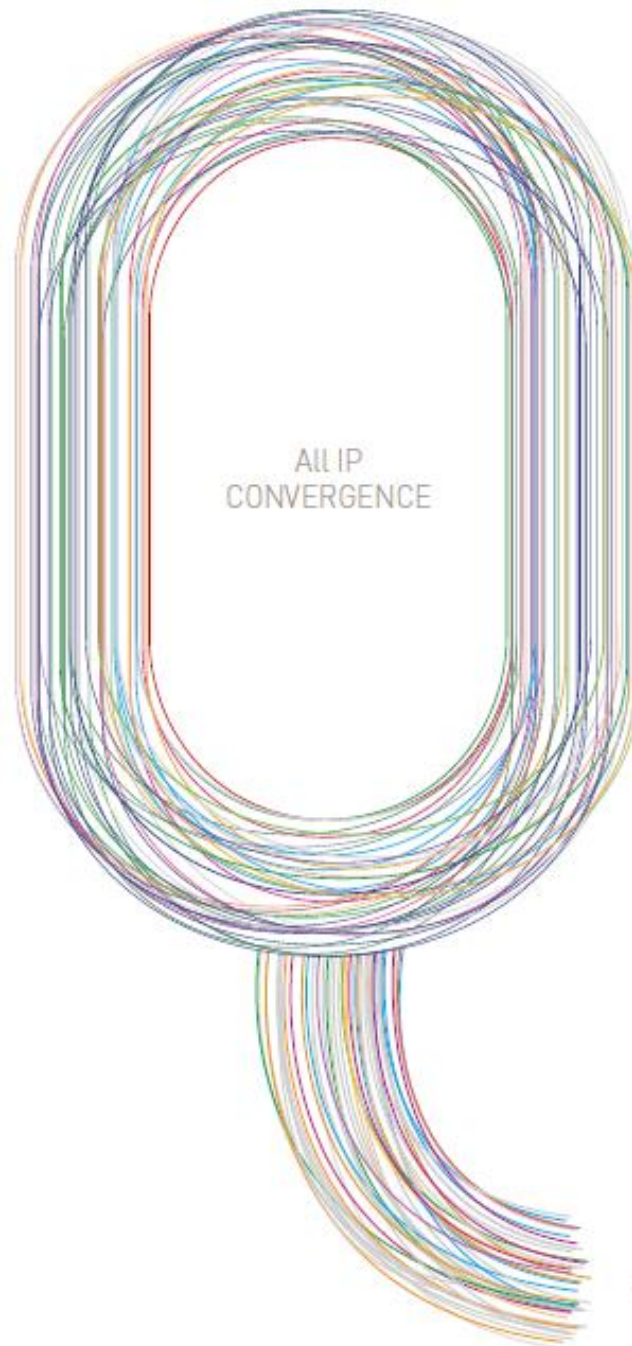


# U3000 Series DSLAM Common User Guide



Published: Oct 2006

ubiQuoss

# 목차

목차 .....	2
표 목차 .....	8
그림 목차 .....	10
<b>1. 서문 .....</b>	<b>11</b>
1.1. 개요 .....	11
1.2. 적용 규칙 .....	12
1.3. 관련 문서 .....	13
<b>2. U3000 SERIES 스위치 시작하기 .....</b>	<b>14</b>
2.1. 편집 및 도움말 기능 .....	14
2.1.1. 명령어 문법의 이해 .....	14
2.1.2. 명령어 문법 도움말(Command Syntax Helper) .....	15
2.1.3. 단축 명령어 입력 .....	17
2.1.4. 명령어 심볼 .....	17
2.1.5. 명령어 라인 편집 키 및 도움말 .....	18
2.2. 스위치 명령어 모드 .....	19
2.3. U3000 SERIES 스위치 가동 .....	20
2.4. 사용자 인터페이스 .....	20
2.4.1. 콘솔 연결 .....	21
2.4.2. Telnet 연결 .....	21
2.4.3. SNMP Network Manager 를 통한 연결 .....	22
2.5. 사용자 인증 .....	22
2.5.1. 사용자 추가 및 삭제 .....	22
2.5.1.1. 사용자 추가 및 삭제 .....	23
2.5.2. 패스워드 설정 .....	24
2.5.2.1. Privileged 모드 패스워드 설정 .....	24
2.5.2.2. 패스워드 encryption 설정 .....	25
2.5.3. 인증 방법 설정 .....	25
2.5.3.1. 스위치에 login 시 인증 방법 설정 .....	25
2.5.3.2. privileged mode 진입시 인증 방법 설정 .....	27
2.5.4. 인증 서버 설정 .....	28
2.6. HOSTNAME 설정 .....	30
2.7. SNMP(SIMPLE NETWORK MANAGEMENT PROTOCOL) .....	30
2.7.1. SNMP Community 설정 .....	31

2.7.2.	SNMP Trap 설정 .....	32
2.7.3.	시스템 담당자 설정 .....	32
2.7.4.	시스템 구축 위치 설정 .....	33
2.8.	ACL(ACCESS CONTROL LIST).....	33
2.8.1.	액세스 리스트 생성 규칙.....	33
2.8.2.	표준 IP 액세스 리스트 설정 .....	34
2.8.2.1.	모든 액세스 허용 .....	34
2.8.2.2.	모든 액세스 거부 .....	34
2.8.2.3.	특정 호스트에서의 액세스만 허용 .....	34
2.8.2.4.	특정 네트워크에서의 액세스만 허용.....	34
2.8.2.5.	특정 네트워크에서의 액세스만 거부.....	34
2.8.3.	SNMP 연결에 액세스 리스트 설정.....	35
2.8.4.	Telnet 연결에 액세스 리스트 설정.....	35
2.9.	NTP 설정 .....	36
2.9.1.	NTP 개요.....	36
2.9.2.	NTP client mode 설정 .....	36
2.9.3.	NTP Server mode 설정 .....	36
2.9.4.	NTP time zone 설정 .....	36
2.9.5.	NTP 기타 명령어.....	36
2.9.6.	NTP 설정 예제 .....	37
2.10.	AFSMGR(ALARM FAULT STATUS MANAGER).....	37
2.10.1.	AFS Alarm Event 해제 .....	38
2.10.2.	AFS history 삭제.....	39
2.10.3.	AFS Masking 기능 설정 .....	39
2.10.4.	AFS Severity 변경 설정.....	40
2.10.5.	AFS SNMP Trap 설정.....	40
3.	인터페이스 환경 설정 .....	42
3.1.	개요 .....	42
3.2.	공통 명령어 .....	43
3.2.1.	Interface name .....	43
3.2.2.	Interface id .....	44
3.2.3.	Interface 모드 프롬프트 .....	44
3.2.4.	Interface-range 모드 프롬프트.....	44
3.3.	인터페이스 정보 및 상태 조회.....	45
3.3.1.	Show interfaces 명령어 .....	45
3.3.2.	Show port status 명령어 .....	45
3.3.3.	Show switchport 명령어.....	46
3.4.	물리적 포트 환경 설정 .....	47
3.4.1.	Shutdown .....	48
3.4.2.	Block .....	48
3.4.3.	Speed an duplex.....	48
3.5.	PORT MIRRORING .....	49

3.6.	2 계층 인터페이스 환경 설정 .....	49
3.6.1.	VLAN Trunking.....	49
3.6.2.	2 계층 인터페이스 모드.....	49
3.6.3.	2 계층 인터페이스 기본 설정 값.....	50
3.6.4.	2 계층 인터페이스 설정/해제 .....	50
3.6.5.	Trunk port 설정.....	50
3.6.6.	Access port 설정.....	51
3.7.	PORT GROUP .....	52
3.7.1.	Port group 개요.....	52
3.7.2.	Port group configuration .....	52
3.8.	MAC FILTERING .....	53
3.8.1.	MAC Filtering 개요.....	53
3.8.2.	MAC Filtering 설정.....	53
3.9.	TRAFFIC-CONTROL .....	53
3.9.1.	Traffic-control 개요.....	53
3.9.2.	Traffic-control 설정.....	53
<b>4.</b>	<b>가상 LAN(VLANS) .....</b>	<b>55</b>
4.1.	VLAN 개관.....	55
4.1.1.	VLAN 정의.....	56
4.1.2.	VLAN 의 장점.....	56
4.2.	VLAN 의 유형 .....	57
4.2.1.	포트 기반 VLAN(Port-Based VLANs) .....	57
4.2.1.1.	포트 기반 VLAN 으로 스위치 묶기.....	58
4.2.2.	태그 VLAN(Tagged VLANs).....	59
4.2.2.1.	태그 VLAN 의 사용(Uses of Tagged VLANs).....	59
4.2.2.2.	VLAN 태그의 할당(Assigning a VLAN Tag) .....	60
4.2.3.	포트 기반 VLAN 과 태그 VLAN 의 혼합 .....	62
4.3.	VLAN 구성.....	62
4.3.1.	VLAN ID.....	62
4.3.2.	Default VLAN .....	62
4.3.3.	Native VLAN .....	63
4.4.	VLAN 설정 .....	64
4.4.1.	VLAN 설정 명령 .....	64
4.5.	VLAN 설정 예제.....	65
4.6.	VLAN 설정 정보 확인.....	67
<b>5.</b>	<b>IP 환경 설정.....</b>	<b>68</b>
5.1.	개요.....	68
5.2.	네트워크 인터페이스에 IP 주소 할당 .....	68
5.3.	ARP(ADDRESS RESOLUTION PROTOCOL) .....	70
5.4.	DEFAULT GATEWAY 설정.....	70
5.5.	IP 설정 예제.....	71

<b>6. DHCP RELAY .....</b>	<b>72</b>
6.1. DHCP RELAY 환경 설정.....	72
6.1.1. DHCP Relay 기능 개요.....	72
6.1.1.1. U3000 Series 스위치를 DHCP relay agent 로 사용.....	73
6.1.2. DHCP relay agent 설정.....	74
6.1.2.1. DHCP relay agent 에서 서버 설정.....	74
6.1.2.2. Relay information option 재중계 정책 설정.....	75
6.1.3. Premier DHCP relay 기능 활성화.....	76
6.2. DHCP RELAY 모니터링 및 관리.....	76
6.3. DHCP 설정 예제.....	76
6.3.1. DHCP Relay Agent 설정.....	77
<b>7. IGMP SNOOPING.....</b>	<b>78</b>
7.1. IGMP SNOOPING 개요.....	78
7.2. IGMP SNOOPING 설정.....	78
7.2.1. Enable Global IGMP Snooping.....	79
7.2.2. Configure IGMP Snooping Functionality.....	79
7.2.2.1. report-suppression 설정.....	79
7.2.2.2. fast-leave 설정.....	80
7.2.2.3. mrouter 설정.....	82
7.2.2.4. aging time 설정.....	83
7.2.2.5. last-member-join-interval 설정.....	84
7.2.2.6. tcn (Topology Change Notification) 설정.....	85
7.2.2.7. igmp filtering 설정.....	86
7.2.2.8. igmp max-group-count 설정.....	87
7.2.2.9. igmp max-reporter-count 설정.....	88
7.3. IGMP PROXY-REPORTING 개요.....	90
7.4. IGMP PROXY-REPORTING 설정.....	91
7.4.1. Enable IGMP Proxy-Reporting.....	91
7.4.2. Enable IGMP Proxy-Reporting on a VLAN.....	91
7.4.3. Configure IGMP Proxy-Reporting Functionality.....	92
7.4.3.1. Multicast Router Port 지정.....	92
7.4.3.2. IGMP Static-Group 지정.....	93
7.4.4. Display System and Network Statistics.....	95
<b>8. STP(SPANNING TREE PROTOCOL) &amp; SLD(SELF-LOOP DETECTION).....</b>	<b>96</b>
8.1. UNDERSTANDING SPANNING-TREE FEATURES.....	96
8.1.1. STP Overview.....	97
8.1.2. Bridge Protocol Data Units.....	97
8.1.3. Election of Root Switch.....	98
8.1.4. Bridge ID, Switch Priority, and Extended System ID.....	99
8.1.5. Spanning-Tree Timers.....	99
8.1.6. Creating the Spanning-Tree Topology.....	100
8.1.7. Spanning-Tree Interface States.....	100
8.2. UNDERSTANDING RSTP.....	104

8.2.1.	<i>RSTP Overview</i> .....	104
8.2.2.	<i>Port Roles and the Active Topology</i> .....	104
8.2.3.	<i>Rapid Convergence</i> .....	105
8.2.4.	<i>Bridge Protocol Data Unit Format and Processing</i> .....	107
8.3.	CONFIGURING SPANNING-TREE FEATURES .....	108
8.3.1.	<i>Default STP Configuration</i> .....	108
8.3.2.	<i>STP Configuration Guidelines</i> .....	108
8.3.3.	<i>Enabling STP</i> .....	108
8.3.4.	<i>Disable per VLAN STP</i> .....	109
8.3.5.	<i>Configuring the Port Priority</i> .....	110
8.3.6.	<i>Configuring the Path Cost</i> .....	110
8.3.7.	<i>Configuring the Switch Priority of a VLAN</i> .....	111
8.3.8.	<i>Configuring the Hello Time</i> .....	112
8.3.9.	<i>Configuring the Forwarding-Delay Time for a VLAN</i> .....	112
8.3.10.	<i>Configuring the Maximum-Aging Time for a VLAN</i> .....	113
8.3.11.	<i>Configuring the Port as Edge Port</i> .....	113
8.3.12.	<i>Configuring the RSTP Mode</i> .....	114
8.3.13.	<i>Specifying the Link Type to Ensure Rapid Transitions</i> .....	114
8.3.14.	<i>Restarting the Protocol Migration Process</i> .....	115
8.4.	DISPLAYING THE SPANNING-TREE STATUS .....	115
8.5.	SELF-LOOP DETECTION .....	116
8.5.1.	<i>Understanding Self-loop Detection</i> .....	116
8.5.2.	<i>Configuring Self-loop Detection</i> .....	117
8.5.2.1.	<i>Enabling Self-loop Detection</i> .....	117
8.5.2.2.	<i>Changing The Service Status of Port</i> .....	118
8.5.2.3.	<i>Disabling Self-loop Detection</i> .....	118
8.5.3.	<i>Displaying Self-loop Status</i> .....	119
<b>9.</b>	<b>STACKING</b> .....	<b>121</b>
9.1.	STACKING OVERVIEW .....	121
9.2.	CONFIGURING STACKING FEATURE.....	121
9.2.1.	<i>Configuring the Stack VLAN</i> .....	122
9.2.2.	<i>Configuring the Stack Member</i> .....	122
9.2.3.	<i>Enabling the Stack</i> .....	123
9.2.4.	<i>Connecting to Slave Switch</i> .....	124
9.3.	DISPLAYING THE STACKING STATUS.....	125
<b>10.</b>	<b>상태 모니터링 및 통계</b> .....	<b>126</b>
10.1.	상태 모니터링 .....	126
10.2.	포트 통계 .....	127
10.3.	CPU 트래픽 통계 .....	130
10.4.	LOGGING.....	132
10.4.1.	<i>시스템 로그 메시지 내용</i> .....	133
10.4.2.	<i>디폴트 Logging 설정 값</i> .....	134
10.5.	RMON(REMOTE MONITORING).....	135
10.5.1.	<i>RMON 개요</i> .....	135

10.5.2.	<i>RMON</i> 의 Alarm 과 Event 그룹 설정 .....	137
10.6.	QoS 및 PACKET FILTERING .....	141
10.6.1.	MFC(Multi-Field Classifier).....	142
10.6.1.1.	Flow-Rule 생성/삭제/모드설정 .....	142
10.6.1.2.	Flow-Rule 설정/해제 .....	142
10.6.1.3.	mask-calculator .....	145
10.6.1.4.	policy-map 생성/추가.....	146
10.6.2.	Qos 관련 파라미터 .....	149
10.6.3.	Scheduling .....	150
10.6.4.	Congestion Avoidance .....	152
10.6.5.	Filtering.....	152
<b>11.</b>	<b>환경 설정 및 소프트웨어 업그레이드 .....</b>	<b>153</b>
11.1.	FLASH 파일 시스템 .....	153
11.2.	IMAGE/CONFIGURATION FILE DOWN/UP LOAD .....	155
11.2.1.	FTP 를 통한 Down/Up Load.....	155
11.2.2.	TFTP 를 통한 Down/Up Load .....	156
11.3.	CONFIGURATION FILE 관리.....	156
11.3.1.	Configuration file 의 저장 .....	157
11.3.2.	Configuration file 의 삭제 .....	158
11.4.	BOOT MODE 설정 및 시스템 재시동 .....	158
11.4.1.	Boot Mode 설정 .....	159
11.4.2.	시스템 재시동 .....	159
<b>12.</b>	<b>CPU_FILTER &amp; SYSCTL.....</b>	<b>160</b>
12.1.	CPU FILTERING.....	160
12.1.1.	CPU-Filtering Rule 설정/해제.....	160
12.1.2.	CPU-FILTER Group 설정 .....	161
12.1.2.1.	INPUT Group 설정/해제 .....	161
12.1.2.2.	FORWARD Group 설정/해제 .....	162
12.1.2.3.	CPU-FILTER service 의 활성화 .....	162
12.1.3.	CPU-FILTER 의 설정 예.....	162
12.2.	SYSCTL 개요 .....	163
12.3.	SYSCTL 명령어 .....	163
<b>13.</b>	<b>VDSL 설정 .....</b>	<b>165</b>
13.1.	프로파일 개요 .....	165
13.2.	LINE 프로파일 설정 .....	166
13.2.1.	Default 설정.....	166
13.2.2.	Assigning a Profile to a Specific VDSL Port.....	166
13.2.3.	Configuring a New Line Profile .....	166
13.2.4.	Reset VDSL Port with Updated Profile .....	167
13.2.5.	Line profile 설정 .....	167
13.2.5.1.	pbo-config 설정 .....	168

13.2.5.2.	Optionnal band 설정 .....	168
13.2.5.3.	band-modifier 설정 .....	169
13.2.5.4.	G.HS 설정 .....	170
13.2.5.5.	ife-tx-filter, ife-rx-filter 설정 .....	170
13.2.5.6.	line type 설정 .....	171
13.2.5.7.	power-mode 설정 .....	171
13.2.5.8.	rate-adaptation-mode 설정 .....	172
13.2.5.9.	upstream / downstream 설정 .....	172
13.2.6.	<b>System profile 설정</b> .....	177
13.2.6.1.	band-plan 설정 .....	177
13.2.6.2.	rfi-band 설정 .....	179
13.2.6.3.	adsl-safe-mode, tlan-safe-mode 설정 .....	179
13.2.6.4.	psd-mask-level 설정 .....	180
13.2.6.5.	Ham-band 설정 .....	180
13.2.8.	<b>Interface 설정</b> .....	181
13.3.	<b>VDSL 설정 정보 확인</b> .....	182
13.3.1.	<b>Alarm-profile 정보 확인</b> .....	182
13.3.2.	<b>line-profile 정보 확인</b> .....	183
13.3.3.	<b>system-profile 정보 확인</b> .....	185
13.3.4.	<b>Interface 정보 확인</b> .....	186

## 표 목차

---

표 1-1.	문자 표시 규칙 .....	12
표 1-2.	알림 및 경고 아이콘 .....	12
표 2-1.	명령어 구문 심볼 .....	17
표 2-2.	명령어 라인 편집 명령 및 도움말 기능 .....	18
표 2-3.	스위치 명령어 모드 .....	19
표 2-4.	스위치의 명령어 모드 사이의 이동 .....	20
표 2-5.	스위치의 사용자 추가 및 삭제 명령어 .....	22
표 2-6.	스위치의 ENABLE 패스워드 설정 명령어 .....	24
표 2-7.	HOSTNAME 설정 명령어 .....	30
표 2-8.	SNMP 환경 설정 명령 .....	31
표 2-9.	액세스 리스트 설정 명령 .....	33
표 2-10.	AFS 설정 명령 .....	37
표 3-1.	U3000 SERIES 스위치가 지원하는 인터페이스 .....	42
표 3-2.	공통 명령어 .....	43



표 3-3. INTERFACE NAME.....	43
표 3-4. INTERFACE ID 및 지원 범위.....	44
표 3-5. 인터페이스 정보 및 상태 관련 명령어.....	45
표 3-6. 물리적 포트 환경 설정 명령어.....	47
표 3-7. U3000 SERIES 스위치가 지원하는 2 계층 인터페이스 모드.....	49
표 3-8. 계층 인터페이스 설정 및 해제 명령어.....	50
표 3-9. TRUNK PORT 설정 명령어.....	50
표 3-10. ACCESS PORT 설정 명령어.....	51
표 3-11. 포트 그룹 설정 명령어.....	52
표 3-12. MAC-FILTER 설정 명령어.....	53
표 3-13. TRAFFIC-CONTROL 설정 명령어.....	53
표 4-1. VLAN 설정 명령어.....	64
표 5-1. 사용 가능한 IP 주소.....	68
표 5-2. IP 주소 할당 명령어.....	70
표 5-3. ARP 환경 설정을 위한 명령어.....	70
표 5-4. DEFAULT GATEWAY 설정 명령어.....	70
표 7-1. IGMP SNOOPING 관련 모니터링 명령어.....	95
표 7-2. IGMP PROXY-REPORTING 관련 모니터링 명령어.....	95
표 8-1. SWITCH PRIORITY VALUE AND EXTENDED SYSTEM ID.....	99
표 8-2. SPANNING-TREE TIMERS.....	99
표 8-3. PORT STATE COMPARISON.....	105
표 8-4. RSTP BPDU FLAGS.....	107
표 8-5. DEFAULT STP CONFIGURATION.....	108
표 10-1. 상태 모니터링 명령어.....	126
표 10-2. 포트 통계조회 조회 명령.....	128
표 10-3. 포트 통계조회 설정 명령.....	130
표 10-4. 포트 통계 초기화 명령.....	130
표 10-5. CPU 트래픽 통계 초기화 명령.....	130
표 10-6. U3000 SERIES 스위치의 로그 레벨.....	132
표 10-7. 시스템 로그 기본 설정 값.....	134
표 10-8. 시스템 메시지 로깅 환경 설정 명령.....	134
표 10-9. RMON 항목.....	136
표 10-10. RMON ALARM AND EVENT 설정 명령.....	137
표 10-11. RMON STATISTICS AND HISTORY 설정 명령.....	139
표 10-12. FLOW-RULE 생성/삭제/모드설정 명령.....	142
표 10-13. FLOW-RULE CLASSIFICATION 명령.....	143
표 10-14. FLOW-RULE 정책 적용 명령.....	144
표 10-15. MASK-CALCULATOR 명령.....	145
표 10-16. POLICY-MAP 생성 및 추가 명령.....	146
표 10-17. POLICY-MAP 삭제 및 특정 FLOW-RULE 삭제 명령.....	146
표 10-18. POLICY-MAP 적용/해제 명령.....	146

표 10-19. FLOW-RULE 조회 명령 .....	147
표 10-20. QoS 관련 MARKING/REMARKING 테이블 셋팅 명령.....	149
표 10-21. QoS 관련 MARKING/REMARKING 테이블 조회명령 .....	149
표 11-1. 파일 관리를 위한 명령어.....	154
표 11-2. FTP 를 통한 DOWN/UP LOAD 명령어 .....	155
표 11-3. TFTP 를 통한 DOWN/UP LOAD 명령어 .....	156
표 11-4. CONFIGURATION MANAGEMENT 명령어 .....	157
표 11-5. BOOT MODE 설정 및 시스템 재 시동 명령어 .....	158
표 12-1. SYSCTL 명령어.....	164

## 그림 목차

---

그림 2-1. U3000 SERIES 스위치와 운영 단말 연결.....	21
그림 4-1. U3000 SERIES 스위치의 포트 기반 VLAN 구성 예.....	57
그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN.....	58
그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN.....	59
그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램.....	61
그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램.....	61
그림 4-6. NATIVE VLAN.....	63
그림 4-7. VLAN 설정 예제 – TAGGED AND UNTAGGED VLAN .....	66
그림 6-1. DHCP RELAY AGENT 로서 DHCP 서버의 메시지 전달 .....	73
그림 6-2. 예제 네트워크 – DHCP RELAY AGENT 환경 설정 .....	77
그림 8-1 SPANNING-TREE TOPOLOGY .....	100
그림 8-2 SPANNING-TREE INTERFACE STATES .....	101
그림 8-3. PROPOSAL AND AGREEMENT HANDSHAKING FOR RAPID CONVERGENCE .....	106
그림 8-4. SELF-LOOP 발생 환경 .....	117
그림 10-1. RMON MANAGER 와 RMON PROBE .....	136
그림 10-2. SPQ(STRICT PRIORITY QUEUE) METHOD .....	150
그림 10-3. WRR / WFQ METHOD .....	150
그림 13-1. OPTION BAND 와 6BAND.....	169
그림 13-2. SNR 마진에 따른 전송 속도 결정 .....	173
그림 13-3. INTERLEAVE 의 예 .....	175

# 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 U3000 Series VDSL 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
- TCP/IP 프로토콜 개념
- Simple Network Management Protocol (SNMP)

**Notice**

U3000 Series 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하기 바란다.



## 1.2. 적용 규칙

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

표 1-1. 문자 표시 규칙

문자 표시 규칙	설명
Screen displays	<ul style="list-style-type: none"> <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

U3000 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**

U3000 Series 스위치를 포함한 (주)유비쿼스의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(<http://www.ubiquoss.com/>)를 통하여 다운로드 받거나 서비스를 요청할 수 있다.

# 2

## U3000 Series 스위치 시작하기

본 장은 다음과 같이 시스템 운영자가 U3000 Series VDSL 스위치의 운용 환경을 설정하고 처음 다루기 시작할 때 필요한 정보를 제공한다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- U3000 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)

U3000 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. U3000 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 “Switch# show” 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기한다. 운영자 입력에서 ‘?’는 화면에 표시되지 않는다.

```
Switch# show ?
access-list      access list entry
arp              Display ARP table entries
clock            show current system's time
config           Show config file information
cpu              CPU information
debugging        Debugging functions
filter           filter setting
flash            display information about flash file system
flow-rule        flow-rule
interface        Interface status and configuration
ip               IP information
logging          Show all contents of logging buffers
mac-address-table Display MAC address table entries
mac-count        MAC count configuration
memory           Memory statistics
mirroring        Port mirroring configuration
ntp              show current ntp status
port             Port status and configuration
port-group       Port-group configuration
privilege        Display your current level of privilege
qos              Qos configuration
rate-limit       Display rate-limit control parameters
rmon             Remote Monitoring
running-config   Current operating configuration
service-policy   service-policy information
spanning-tree    Spanning tree topology
stack            Show stacking information
startup-config   Show startup config file information
switchport       Switching port configuration
system           Display the system information
uptime           Display elapsed time since boot
users            Display information about terminal lines
version          Display the system version
vlans            VLAN information

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?
port                Display port configuration
port-group          Port group information
privilege           Display your current level of privilege
Switch# show p_
```

### 2.1.3. 단축 명령어 입력

U3000 Series 스위치의 CLI 는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행을 지원한다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령어를 수행한다.



#### Notice

단축 명령어를 사용할 때, 시스템 운영자는 U3000 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 하</li> </ul>



심볼	이름	설명
		<p>나 이상을 입력해야 한다.</p> <ul style="list-style-type: none"> <li>■ 예를 들어, 다음과 같은 명령어가 있을 때</li> </ul> <pre>qos (cos-queue-map cos-remark)</pre> <p>시스템 운영자는 <b>QoS method</b>로서 <b>qos-queue-map</b> 또는 <b>qos-remark</b> 중의 하나를 반드시 명시해야 한다.</p>
[:	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</li> </ul> <pre>show interfaces [ifname]</pre> <p>인터페이스의 이름을 정의하지 않을 수도 있다.</p>
:	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>
A.B.C.D		<ul style="list-style-type: none"> <li>■ IP 주소 또는 서브넷 마스크를 의미</li> </ul>
A.B.C.D/M		<ul style="list-style-type: none"> <li>■ IP prefix 를 의미 (예. 192.168.0.0/24)</li> </ul>

### 2.1.5. 명령어 라인 편집 키 및 도움말

U3000 Series 스위치는 Emacs 와 유사한 편집 기능을 제공한다. <표 2-2>는 운영 단말이 제공하는 명령어 라인 편집 명령 및 도움말 기능을 설명한다.

표 2-2. 명령어 라인 편집 명령 및 도움말 기능

명령어	설명
[Ctrl] + [A]	<ul style="list-style-type: none"> <li>■ 커서를 줄의 처음으로 이동</li> </ul>
[Ctrl] + [E]	<ul style="list-style-type: none"> <li>■ 커서를 줄의 끝으로 이동</li> </ul>
[Ctrl] + [B]	<ul style="list-style-type: none"> <li>■ 커서를 한 단어 뒤로 이동</li> </ul>
[Ctrl] + [F]	<ul style="list-style-type: none"> <li>■ 커서를 한 글자 앞으로 이동</li> </ul>
Backspace	<ul style="list-style-type: none"> <li>■ 커서 앞의 한 글자를 삭제</li> </ul>
[Ctrl] + [K]	<ul style="list-style-type: none"> <li>■ 현재 커서로부터 줄의 끝까지 문자를 삭제</li> </ul>
[Ctrl] + [U]	<ul style="list-style-type: none"> <li>■ 현재 커서로부터 줄의 처음까지 문자를 삭제</li> </ul>
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 	<ul style="list-style-type: none"> <li>마지막 입력 명령어부터 차례 대로 20 개까지의 명령어 입력에 대한 이력을 표시</li> </ul>
[Ctrl] + [N] 또는 	<ul style="list-style-type: none"> <li>다음 명령어를 표시</li> </ul>
?	<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

U3000 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>	<ul style="list-style-type: none"> <li>보통 통계 정보를 디스플레이</li> </ul>
Privileged 모드	Switch#	<ul style="list-style-type: none"> <li>시스템 설정을 출력하거나 시스템 관리 명령을 사용</li> </ul>
Config 모드	Switch(config)#	<ul style="list-style-type: none"> <li>스위치의 환경 설정 값을 글로벌 하게 변경</li> </ul>
Interface 모드	Switch(config-if-fal) # Switch(config-if-vlan1) #	<ul style="list-style-type: none"> <li>인터페이스의 환경 설정을 변경</li> </ul>



**Notice**

명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 U3000 Series 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 U3000 Series 스위치의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게 된다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 와 있는 지를 알려준다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 체크 해야만 한다. <표 2-4>은 스위치의 명령어 모드 사이의 이동 방법을 설명한다.

표 2-4. 스위치의 명령어 모드 사이의 이동

명령어	설명
enable	<ul style="list-style-type: none"> <li>■ User 모드에서 Privileged 모드로 이동</li> <li>■ Privileged 모드의 패스워드를 입력할 필요</li> </ul>
disable	<ul style="list-style-type: none"> <li>■ Privileged 모드에서 User 모드로 이동</li> </ul>
configure terminal	<ul style="list-style-type: none"> <li>■ Privileged 모드에서 Config 모드로 이동</li> </ul>
interface ifname	<ul style="list-style-type: none"> <li>■ Config 모드에서 Interface 모드로 이동</li> </ul>
exit	<ul style="list-style-type: none"> <li>■ 이전의 모드로 이동</li> </ul>
end	<ul style="list-style-type: none"> <li>■ 어느 모드에서든 Privileged 모드로 이동</li> <li>■ User 모드에서는 이동하지 않는다.</li> </ul>

## 2.3. U3000 Series 스위치 가동

U3000 Series 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS image 를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.



### Notice

U3000 Series 스위치는 시스템 안정성을 위하여 두 개 이상의 OS image 를 관리한다. 기본적으로 Primary OS image 가 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 U3000 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 U3000 Series 스위치를 관리할 수 있다.

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

U3000 Series 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결
- 최대 4 개의 telnet 연결

### 2.4.1. 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능하다. 이를 위하여 운영 단말 (또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9 핀, RS-232 DB9 포트를 지원해야 한다. 콘솔 포트는 U3000 Series 스위치의 경우 새시나 SCU 모듈에 탑재된다.

>과 같이 U3000 Series 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

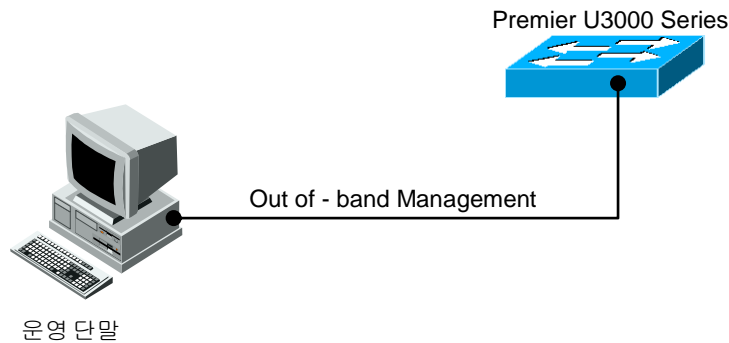


그림 2-1. U3000 Series 스위치와 운영 단말 연결



**Notice**     운용 단말의 설정 방법 및 콘솔 포트 핀 설정은 U3000 Series 스위치 하드웨어 설치 가이드를 참조하기 바란다.

### 2.4.2. Telnet 연결

시스템 운영자는 TCP/IP 및 telnet 접속 기능을 가지고 있는 워크스테이션을 통하여 U3000 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 <2.9. 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 U3000 Series 스위치를 관리할 수 있다.



**Notice** SNMP 에 대한 추가적인 정보는 <ACL(Access Control List)>절을 참조하라.

## 2.5. 사용자 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. U3000 series 스위치는 사용자를 추가, 삭제 할 수 있고 각각의 사용자에 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 <[2.8. 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>■ userID 생성</li> <li>■ password 가 없다</li> </ul>	Config
username <i>userID</i> password	<ul style="list-style-type: none"> <li>■ userID 생성</li> </ul>	Config

<code>password</code> <code>username userID password</code> <code>0 password</code>	<ul style="list-style-type: none"> <li>■ 암호화되지 않은 <code>password</code> 를 입력받는다</li> </ul>	
<code>username userID password</code> <code>7 password</code>	<ul style="list-style-type: none"> <li>■ userID 생성</li> <li>■ 암호화된 <code>password</code> 를 입력받는다</li> </ul>	Config
<code>username userID privilege</code> <code>&lt;0-15&gt; nopassword</code>	<ul style="list-style-type: none"> <li>■ userID 생성</li> <li>■ password 가 없다</li> <li>■ privilege 15 이면 가장높은 <code>privilege(enable mode 진입허용)</code>를 갖는다.</li> </ul>	Config
<code>username userID privilege</code> <code>&lt;0-15&gt; password password</code> <code>username userID privilege</code> <code>&lt;0-15&gt; password 0</code> <code>password</code>	<ul style="list-style-type: none"> <li>■ userID 생성</li> <li>■ privilege 15 이면 가장높은 <code>privilege(enable mode 진입허용)</code>를 갖는다.</li> <li>■ 암호화되지 않은 <code>password</code> 를 입력받는다</li> </ul>	Config
<code>username userID privilege</code> <code>&lt;0-15&gt; password 7</code> <code>password</code>	<ul style="list-style-type: none"> <li>■ userID 생성</li> <li>■ privilege 15 이면 가장높은 <code>privilege(enable mode 진입허용)</code>를 갖는다.</li> <li>■ 암호화된 <code>password</code> 를 입력받는다</li> </ul>	Config
<code>username userID timeout</code> <code>&lt;0-600&gt;</code>	<ul style="list-style-type: none"> <li>■ user 별 <code>session timeout</code> 시간(분) 설정(default 20 분)</li> </ul>	Config
<code>no username userID</code> <code>timeout</code>	<ul style="list-style-type: none"> <li>■ user 별 <code>session timeout</code> 시간(분) 삭제</li> <li>■ 초기 <code>session timeout</code> 시간(20 분)으로 되돌린다.</li> </ul>	Config
<code>username userID access-</code> <code>class access-list-num</code>	<ul style="list-style-type: none"> <li>■ 해당 user 에 Access List 를 적용</li> <li>■ <code>access-list-num</code> : &lt;1-99&gt; 이며, standard ip access list 를 의미</li> </ul>	Config
<code>no username userID</code> <code>access-class</code>	<ul style="list-style-type: none"> <li>■ 해당 user 에 적용된 Access List 를 해제.</li> </ul>	Config
<code>no username userID</code>	<ul style="list-style-type: none"> <li>■ userID 삭제</li> <li>■ userID 가 root 이면 삭제되지않고 password 가 default passowrd 로 바뀐다.</li> </ul>	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
!

```

```
username lns nopassword
username test password 0 test
username admin privilege 15 password 0 admin
username admin timeout 50
!
Switch#
```

## 2.5.2. 패스워드 설정

U3000 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 패스워드 설정 명령어

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



**Notice** 사용자 패스워드 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 U3000 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 XX1LtbDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
!
Switch#
```

### 2.5.3. 인증 방법 설정

#### 2.5.3.1. 스위치에 login 시 인증 방법 설정

U3000 series 스위치는 시스템에 접속하는 사용자에게 대한 인증 방법을 다양하게 설정할 수 있다. 일반적으로는 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.

#### 사용자 인증 설정 명령어

명령어	설명	모드
<code>authentication login authen-type chap</code>	■ tacacs server 를 사용하여 인증할 경우 password 를 chap 방식으로 암호화하여 전송한다.	Config
<code>no authentication login authen-type</code>	■ tacacs server 를 사용하여 인증할 경우 password 를 암호화하지 않는다.	Config
<code>authentication login enable (local   radius   tacacs)</code>	■ 사용할 인증방식(local, radius, tacacs)을 선택한다. ■ 여러가지 인증방식을 선택할 수 있다.	Config
<code>no authentication login enable (radius   tacacs)</code>	■ 사용하도록 설정된 인증방식을 사용하지 않도록 설정한다. ■ local 인증방식은 항상 사용한다.	Config
<code>authentication login primary (local   radius   tacacs)</code>	■ 우선적으로 인증받을 인증방식을 설정한다.	Config

<code>no authentication login primary (local   radius   tacacs)</code>	<ul style="list-style-type: none"> <li>우선적으로 인증받도록 설정한 인증방식을 해제한다.</li> </ul>	Config
<code>authentication login template-user userID</code>	<ul style="list-style-type: none"> <li>radius 나 tacacs 로 인증받은 경우 Dummy user 를 지정할 수 있다.</li> <li>지정하는 Dummy user 는 local database 에 등록되어 있어야 한다.</li> </ul>	Config
<code>no authentication login template-user</code>	<ul style="list-style-type: none"> <li>설정된 Dummy user 를 해제한다.</li> </ul>	Config
<code>authorization exec tacacs</code>	<ul style="list-style-type: none"> <li>tacacs 로 인증받은 경우 tacacs 서버에서 privilege level 을 얻어온다.</li> </ul>	Config
<code>no authorization exec tacacs</code>	<ul style="list-style-type: none"> <li>tacacs 서버에서 privilege level 을 얻어오지 않도록 한다.</li> </ul>	Config
<code>show authentication login</code>	<ul style="list-style-type: none"> <li>인증방식의 순서와 사용여부를 보여준다</li> </ul>	Enable

### 사용자 인증 설정

U3000 series 스위치는 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 사용자 ID 와 패스워드를 사용하여 접속 권한 여부를 확인하는 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 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#
```

### 2.5.3.2. privileged mode 진입시 인증 방법 설정

U3000 series 스위치는 privileged mode 로 들어올 때 사용자에게 대한 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.

#### 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>■ 여러가지 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 인증받을 인증방식을 설정한다.</li> </ul>	Config
no authentication enable primary (local   tacacs)	<ul style="list-style-type: none"> <li>■ 우선적으로 인증받도록 설정한 인증방식을 해제한다.</li> </ul>	Config
show authentication enable	<ul style="list-style-type: none"> <li>■ 인증방식의 순서와 사용여부를 보여준다</li> </ul>	Enable

#### 사용자 인증 설정

U3000 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#

## 2.5.4. 인증 서버 설정

### RADIUS 서버 설정 명령어

명령어	설명	모드
radius-server host A.B.C.D	<ul style="list-style-type: none"> <li>radius-server 설정한다.</li> </ul>	Config
no radius-server host A.B.C.D	<ul style="list-style-type: none"> <li>설정된 radius-server 삭제한다.</li> </ul>	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 받아야하는 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#
```

## 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 받아야하는 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 받아야하는 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 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있다. U3000 Series 스위치는 default 로 “Switch”를 hostname 으로 사용하며 운영자가 이를 변경할 수 있다.

표 2-7. Hostname 설정 명령어

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

Hostname 을 설정 및 변경하는 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# hostname P3000
P3000(config)# end
P3000#

P3000# configure terminal
P3000(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 U3000 Series 스위치를 관리하고자 할 때는 스위치의 환경 설정이 필요하다.

또한 SNMP 에이전트를 접근하기 위해서는 스위치에 하나 이상의 IP 주소 설정이 필요하다. IP 주소의

설정은 <IP>절을 참고하라.

표 2-8. SNMP 환경 설정 명령

명령어	설명	모드
snmp-server agent-address <i>agent-addr</i>	■ 장비에서 전송하는 snmp 패킷의 출발지 IP 를 지정	Config
no snmp-server agent-address <i>agent-addr</i>	■ 장비에서 전송하는 snmp 패킷의 출발지 IP 를 지정하지 않음	Config
snmp-server community <i>string</i> [ro rw [access-class <i>number</i> ]]	■ SNMP community 를 설정 ■ ro : read only ■ rw : read write ■ <i>number</i> : Standard IP access-list <1-99>	Config
no snmp-server community <i>string</i>	■ SNMP Community 를 삭제	Config
snmp-server contact <i>string</i>	■ System contact 정보를 변경	Config
no snmp-server contact <i>string</i>	■ System contact 정보를 삭제	Config
snmp-server location <i>string</i>	■ System location 정보를 변경	Config
no snmp-server location <i>string</i>	■ System location 정보를 삭제	Config
snmp-server trap-host <i>A.B.C.D</i> community <i>string</i>	■ SNMP Trap Host 와 trap 을 보낼 때 사용할 community 를 설정	Config
no snmp-server trap-host <i>A.B.C.D</i>	■ SNMP Trap Host 를 삭제	Config
snmp-server trap-version 1	■ snmp trap 의 version 을 SNMPv1 으로 변경	Config
no snmp-server trap-version	■ trap version 을 default 값인 SNMPv2C 로 변경	Config

### 2.7.1. SNMP Community 설정

Community string 은 시스템과 원격 네트워크 관리자 사이의 간단한 상호 인증 기능을 제공한다. U3000 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 locuse ro access-class 1
Switch(config)# end
Switch# show running-config
!
snmp-server community public ro
snmp-server community private rw
snmp-server community locuse ro access-class 1
!
Switch#
```

---



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

---

## 2.7.2. SNMP Trap 설정

하나 이상의 네트워크 관리 단말은 인증된 trap receiver 로써 설정될 수 있다. U3000 Series 스위치는 모든 trap receiver 에게 SNMP trap 을 전송한다.

---

```
Switch# configure terminal
Switch(config)# snmp-server trap-host 192.168.0.3 community private
Switch(config)# snmp-server trap-host 10.1.22.12 community ubi
Switch(config)# end
Switch# show running-config
!
snmp-server trap-host 192.168.0.3 community private
snmp-server trap-host 10.1.22.12 community ubi
!
Switch#
```

---

## 2.7.3. 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@ubiqoss.com"
Switch#
```

---



## 2.7.4. 시스템 구축 위치 설정

```
Switch# configure terminal
Switch(config)# snmp-server location "Dogok-Dong, GangNam-gu, Seoul."
Switch(config)# end
Switch# show running-config
!
snmp-server location "Dogok-Dong, GangNam-gu, Seoul."
!
Switch#
```

## 2.8. ACL(Access Control List)

액세스 리스트(Access Control List)를 사용함으로써 네트워크 관리자는 인터넷네트워크를 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 SNMP 를 통한 라우터의 접속에도 적용할 수 있다.

U3000 Series 는 표준 IP 액세스 리스트를 지원하며, <1-99>의 번호가 할당 될 수 있다.

표 2-9. 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>address ::= {any   A.B.C.D/M}</li> </ul>	Config
<b>no access-list &lt;1-199&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 access-list
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 access-list
Access-List 1
    deny any
```

---

### 2.8.2.3. 특정 호스트에서의 액세스만 허용

---

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.3/32
Switch(config)# end
Switch# show access-list
Access-List 1
    permit 192.168.0.3/32
```

---

### 2.8.2.4. 특정 네트워크에서의 액세스만 허용

---

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0/24
Switch(config)# end
Switch# show access-list
Access-List 1
    permit 192.168.0.0/24
```

---

### 2.8.2.5. 특정 네트워크에서의 액세스만 거부

---

```
Switch# configure terminal
Switch(config)# access-list 1 deny 192.168.0.0/24
Switch(config)# access-list 1 permit any
Switch(config)# end
```

---

---

```
Switch# show access-list
Access-List 1
  deny 192.168.0.0/24
  permit any
```

---

### 2.8.3. SNMP 연결에 액세스 리스트 설정

액세스 리스트는 community 별로 적용되며, 설정된 액세스 리스트는 snmp 를 통한 스위치로의 접속을 허용, 제한한다.

host 10.1.22.247 에서의 접속만을 허용하는 Access list 를 생성하여, snmp 접속을 제한하고자 할 때의 절차는 다음과 같다.

---

```
Switch# configure terminal
Switch(config)# access-list 1 permit 10.1.22.247/32
Switch(config)# snmp-server community lns ro access-class 1
Switch# show running-config
!
snmp-server community lns ro access-class 1
!
access-list 1 permit 10.1.22.247/32
!
Switch#
```

---

### 2.8.4. 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 192.168.0.0/24
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 192.168.0.0/24
!
Switch#
```

---

## 2.9. NTP 설정

### 2.9.1. NTP 개요

NTP (Network Time Protocol)는 네트워크를 통하여 시스템의 시간을 동기화하기 위한 프로토콜이다. NTP는 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
<code>ntp server address</code>	<ul style="list-style-type: none"> <li>NTP server 를 설정한다. (5 개까지 설정가능)</li> </ul>

### 2.9.3. NTP Server mode 설정

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

명령어	설명
<code>ntp master stratum</code>	<ul style="list-style-type: none"> <li>NTP master 로 동작하도록 한다.</li> </ul>

### 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
<code>ntp timezone plus HH:MM</code>	<ul style="list-style-type: none"> <li>설정된 Coordinated Universal Time (UTC)에 설정된 시간을 더하여 현재 시간을 표시한다.</li> </ul>
<code>ntp timezone minus HH:MM</code>	<ul style="list-style-type: none"> <li>설정된 Coordinated Universal Time (UTC)에 설정된 시간을 빼서 현재 시간을 표시한다.</li> </ul>

### 2.9.5. NTP 기타 명령어

명령어	설명
<code>ntp poll-interval number</code>	<ul style="list-style-type: none"> <li>NTP client mode 로 동작할 시, 설정된 NTP server 로 NTP</li> </ul>

request message 를 전송하는 간격, 2 의 배수로 동작하며 <4-17>의 범위를 가진다.

**show ntp**

- NTP 에 대한 사항을 보여준다.

### 2.9.6. NTP 설정 예제

```
Switch#
Switch (config)# ntp server 203.248.240.103
Switch (config)# exit
Switch # show ntp
-----
Current time      : Thu Jan 12 20:40:25 2005
-----
NTP master       : disable
NTP stratum      : unspecified
Poll interval    : 6 (power of 2)
NTP timezone     : GMT
-----
The list of NTP Server is below.
-----
[1] 203.248.240.103
-----
Switch #
```

## 2.10. AFSMGR(Alarm Fault Status Manager)

AFS Manager 는 시스템에서 발생하는 SNMP Trap 이벤트에서 Alarm, Status, Fault 메시지에 대한 관리, 장애 등급 설정 및 log masking, report masking 기능을 제공한다. 또한 현재 발생된 장애 및 과거 이력에 대한 검색을 제공한다.

표 2-10. AFS 설정 명령

명령어	설명	모드
<code>afs current clear [alarm-index]</code>	<ul style="list-style-type: none"> <li>■ AFS 이벤트중 현재 해제되지 않은 alarm 에 대해서 사용자가 강제 해제.</li> <li>■ <i>alarm-index</i> : 발생된 alarm 의 index &lt;1-99999&gt;</li> </ul>	Config
<code>afs history clear</code>	<ul style="list-style-type: none"> <li>■ AFS 이벤트에 대한 history 를 삭제</li> </ul>	Config
<code>afs mask enable disable afs-id</code>	<ul style="list-style-type: none"> <li>■ AFS 이벤트에 대한 masking 기능을 설정 및 해제. Masking 이 enable 이면 이벤트가</li> </ul>	Config

	발생되지 않음	
	<ul style="list-style-type: none"> <li>■ <i>afs-id</i>: A01001, S01001, F01001,...</li> </ul>	
<i>afs severity</i> <i>critical major minor</i> <i>afs-id</i>	<ul style="list-style-type: none"> <li>■ AFS 이벤트에 대한 등급 변경</li> <li>■ <i>afs-id</i>: A01001, S01001, F01001,...</li> </ul>	Config
<i>afs snmp enable disable</i> <i>[afs-id afs-type [event-type]]</i>	<ul style="list-style-type: none"> <li>■ AFS 이벤트에 대한 snmp trap reporting 기능을 설정 및 해제. Snmp trap reporting 이 enable 이면 SNMP Trap 이 발생되지 않음</li> <li>■ <i>afs-id</i>: A01001, S01001, F01001,...</li> <li>■ <i>afs-type</i>: message 종류 (alarm, fault, status)</li> <li>■ <i>event-type</i>: event 의 종류. (communications, environment, equipment, processing, protocol, qos, security)</li> </ul>	Config

### 2.10.1. AFS Alarm Event 해제

발생된 AFS Event 중 장애가 해제되지 않은 Alarm 에 대해서 사용자가 강제 해제 할 수 있는 기능이다.

```
Switch# show afs current
-----
no      id      type      level     date
-----
3       A04003  processing major     2006-09-07 10:43:59
-----

Switch# show afs current 3
-----
Probable Cause      MEMORY OVERLOAD ALARM
ID                  A04003
Type                processing
Level               major
Date                2006-09-07 10:43:59
Physical Location   sys<1>
Logical Location
Additional Text     vlaue<45> thres<50>
-----

Switch# configure terminal
Switch(config)# afs current clear
Switch# show afs current
-----
no      id      type      level     date
-----
-----

Switch#
```

## 2.10.2. AFS history 삭제

발생된 AFS history 에 대하여 사용자가 삭제할 수 있는 기능이다.

```
Switch# show afs history
2006-08-06 09:21:22 A04002 processing maj on sys<1> vlaue<4> thres<1>
2006-08-06 09:21:22 A04001 processing maj on sys<1> vlaue<4> thres<3>
2006-08-06 09:21:22 A04003 processing maj on sys<1> vlaue<49> thres<50>
2006-08-06 09:21:23 A01002 equipment maj off sys<1>
Switch# configure terminal
Switch(config)# afs history clear
Switch# show afs history
##### start history #####
Switch#
```

## 2.10.3. AFS Masking 기능 설정

AFS 이벤트중 특정 이벤트에 대하여 Masking 을 할 수 있다. Masking 이 설정된 이벤트는 Masking 이 해제되기 전까지는 어떠한 메시지도 발생하지 않는다.

```
Switch# show afs running-config
-----
ID          Type          Level      Mask      Snmp      Desc
-----
A01001     equipment     critical   disable   enable    system cold start alarm
A01002     equipment     major     disable   enable    system warm start alarm
Switch# configure terminal
Switch(config)# afs mask enable A01001
Switch(config)# end
Switch# show running-config
!
afs mask enable A01001
!
Switch# show afs running-config
-----
ID          Type          Level      Mask      Snmp      Desc
-----
A01001     equipment     critical   enable    enable    system cold start alarm
A01002     equipment     major     disable   enable    system warm start alarm
Switch#
```



### Notice

Masking 설정에서 default 값이 disable 이며, AFS 의 default-config 의 설정 값을 따른다.

## 2.10.4. AFS Severity 변경 설정

AFS 이벤트중 Alarm 이벤트에 대하여 알람 등급을 변경 할 수 있다.

```
Switch# show afs running-config
-----
ID          Type          Level      Mask      Snmp      Desc
-----
A01001     equipment     critical   disable   enable    system cold start alarm
A01002     equipment     major     disable   enable    system warm start alarm
Switch# configure terminal
Switch(config)# afs severity major A01001
Switch(config)# end
Switch# show running-config
!
afs severity major A01001
!
Switch# show afs running-config
-----
ID          Type          Level      Mask      Snmp      Desc
-----
A01001     equipment     major     disable   enable    system cold start alarm
A01002     equipment     major     disable   enable    system warm start alarm
Switch#
```



**Notice** 장애등급은 AFS의 default-config의 설정값을 따른다.

## 2.10.5. AFS SNMP Trap 설정

AFS 이벤트 대하여 SNMP Trap 발생 여부를 설정 할 수 있다. AFS의 모든 이벤트에 대하여 설정하거나, AFS 타입별, 이벤트 타입별, 각각 이벤트별로 설정 가능하다.

```
Switch# show afs running-config
-----
ID          Type          Level      Mask      Snmp      Desc
-----
A01001     equipment     critical   disable   enable    system cold start alarm
A01002     equipment     major     disable   enable    system warm start alarm
S01003     equipment     warning    disable   enable    slot status change
S01006     equipment     warning    disable   enable    gbic status change
F03023     QoS           warning    disable   enable    crc count threshold alarm
Switch# configure terminal
Switch(config)# afs snmp disable alarm
Switch(config)# afs snmp disable status equipment
Switch(config)# afs snmp disable fault qos F03023
```



```
Switch(config)# end
Switch# show running-config
!
```

```
afs snmp disable A01001
afs snmp disable A01002
afs snmp disable S01003
afs snmp disable S01006
afs snmp disable F03023
```

```
Switch# show afs running-config
```

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	disable	system cold start alarm
A01002	equipment	major	disable	disable	system warm start alarm
S01003	equipment	warning	disable	disable	slot status change
S01006	equipment	warning	disable	disable	gbic status change
F03023	QoS	warning	disable	disable	crc count threshold alarm



**Notice**

Snmp trap 설정에서 default 값이 enable 이다. AFS 의 default-config 의 설정값을 따른다.

# 3

## 인터페이스 환경 설정

### 3.1. 개요

U3000 Series 스위치가 지원하는 인터페이스는 다음과 같다.

표 3-1. U3000 Series 스위치가 지원하는 인터페이스

구분	종류
Physical interfaces	<ul style="list-style-type: none"> <li>■ Fast Ethernet                             <ul style="list-style-type: none"> <li>• 10/100Base-TX (Auto Negotiation)</li> </ul> </li> <li>■ 100Base-FX</li> <li>■ VDSL</li> </ul>
port-group interfaces	<ul style="list-style-type: none"> <li>■ Port-group</li> </ul>
VLAN Interfaces	<ul style="list-style-type: none"> <li>■ VLAN</li> </ul>

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>

### 3.2.1. Interface name

U3000 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	Fast Ethernet	"fa" + port_number	fa1
VDSL line interface	VDSL	"vd" + port_number	vd1
Port-group interface	Port group	"po" + port-group id	po1
VLAN interface	VLAN	"vlan" + vlan id	vlan10

### 3.2.2. Interface id

Interface name은 interface type과 id로 구성되며 interface id는 U3000 Series 시리즈 스위치 각 모델마다 다르다. <표 3-4>은 각 모델별 interface id의 표기 방법과 지원하는 범위를 보여준다.

표 3-4. Interface ID 및 지원 범위

Model	Interface Type	ID 구성	ID Range	Name(예)
U3024	Fast Ethernet VDSL	port id port id	port id: 1-26 port id: 1-24	fa1, fa26 vd1, vds24
	Port group VLAN	port id vlan id	1 – 7 1 – 4094	po1, po7 vlan1, vlan4094
U3048	Fast Ethernet VDSL	port id port id	port id: 1-26 port id: 1-48	fa1, fa26 vd1, vd48
	Port group VLAN	port id vlan id	1 – 7 1 – 4094	po1, po7 vlan1, vlan4094

### 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-fa1) #
```

---

### 3.2.4. Interface-range 모드 프롬프트

**Interface range** 명령을 사용하여 interface range 모드 사용이 가능하다. 이는 port interface 에 한해서만 가능하며, 현재 vlan 이나 기타 인터페이스는 지원하지 않는다.. Interface range 모드는 해당되는 interface를 looping 하면서 반복 수행한다.

---

```
Switch(config-ifrange) #
```

---

### 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 interfaces</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 interfaces 명령어

인터페이스의 환경 설정(configuration) 정보, 링크 상태(link status) 및 인터페이스 관련 통계를 보고자 할 경우 사용한다. **show interfaces** 명령은 정의 되어 있는 모든 인터페이스에 대한 정보를 출력한다.

```
Switch# show interfaces
fa1 is up
type 100Base-TX
ifindex 23(k25) BROADCAST multicast
auto-negotiation
speed set auto, current 100M
duplex set full, current full

Last clearing of counters 26:03:20
0 seconds input rate 55495 bytes/sec, 53 packets/sec
0 seconds output rate 6006 bytes/sec, 50 packets/sec
38548078 packets input, 4007497659 bytes
Received 0 broadcasts, 0 multicasts
0 CRC, 0 oversize, 0 dropped
33191196 packets output, 1784705803 bytes
Sent 7141 broadcasts, 0 multicasts
```

#### 3.3.2. Show port status 명령어

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

```
Switch# show port status
Switch# show port status
```

ifname	type	shutdown	link	nego	set-speed	cur-speed	flow-control
fa1	FE-TX	.	down	auto	auto/full	.	.
fa2	FE-TX	.	down	auto	auto/full	.	.
fa3	FE-TX	.	down	auto	auto/full	.	.
fa4	FE-TX	.	down	auto	auto/full	.	.
fa5	FE-TX	.	down	auto	auto/full	.	.
fa6	FE-TX	.	down	auto	auto/full	.	.
fa7	FE-TX	.	down	auto	auto/full	.	.
fa8	FE-TX	.	down	auto	auto/full	.	.
fa9	FE-TX	.	down	auto	auto/full	.	.
fa10	FE-TX	.	down	auto	auto/full	.	.
fa11	FE-TX	.	down	auto	auto/full	.	.
fa12	FE-TX	.	down	auto	auto/full	.	.
fa13	FE-TX	.	down	auto	auto/full	.	.
fa14	FE-TX	.	down	auto	auto/full	.	.
fa15	FE-TX	.	down	auto	auto/full	.	.
fa16	FE-TX	.	down	auto	auto/full	.	.
fa17	FE-TX	.	down	auto	auto/full	.	.
fa18	FE-TX	.	down	auto	auto/full	.	.
fa19	FE-TX	.	down	auto	auto/full	.	.
fa20	FE-TX	.	down	auto	auto/full	.	.
fa21	FE-TX	.	down	auto	auto/full	.	.
fa22	FE-TX	.	down	auto	auto/full	.	.
fa23	FE-TX	.	down	auto	auto/full	.	.
fa24	FE-TX	.	up	auto	auto/full	100	/full
fa25	FE-FX	.	down	manual	100	/full	.
fa26	FE-FX	.	down	manual	100	/full	.



**Notice**

이후부터 각 설정 사례에 대한 CLI 캡처화면은 U3000 series 중심으로 했으므로 다른 모델 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**

IFNAME	SWMODE	N-VLAN	TAGGED-VLAN-LIST
fa1	access	1	
fa2	access	10	
fa3	access	1	

fa4	access	20		
fa5	access	1		
fa6	trunk	100	10	20
fa7	access	1		
fa8	access	1		
fa9	access	1		
fa10	access	1		
fa11	access	1		
fa12	access	1		
fa13	access	1		
fa14	access	1		
fa15	access	1		
fa16	access	1		
fa17	access	1		
fa18	access	1		
fa19	access	1		
fa20	access	1		
fa21	access	1		
fa22	access	1		
fa23	access	2		
fa24	access	2		
fa25	access	1		
fa26	access	1		
po7	access	1		

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

### 3.4.1. Shutdown

물리적 포트를 disable시킨다.

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

---

```
Switch# configure terminal
Switch(config) #
Switch(config) # interface fa1
Switch(config-if-fa1) # shutdown                <- disable port
Switch(config-if-fa1) # 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 fa1
Switch(config-if-fa1) # block                    <- block port
Switch(config-if-fa1) # no block                <- unblock port
```

---

### 3.4.3. Speed and duplex

U3000 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	1000	full
1000Base-X	on	1000	full
	off	1000	full

speed, duplex 설정시 다음 사항을 주의하라.

- 1000Base-FX 의 경우 speed 설정은 없고 단지 auto-negotiation off/off 만 설정가능하며 auto-negotiation on 시 광케이블이 하나만 단절되도 양쪽에 모두 link down 이 감지됨 (remote fault 감지)
- 만일 라인의 양쪽 끝이 auto-negotiation 을 지원한다면, 가급적 auto-negotiation 을 사용할 것을 강력히 권한다.
- 만일 한쪽 인터페이스만 auto-negotiation 을 지원한다면 양쪽 끝의 두 인터페이스 모두 “duplex”와 “speed” 에서 auto-negotiation 을 사용하면 안 된다.



### 3.5. Port mirroring

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

U3000 Series는rx, tx 트래픽을 각각 여러 소스 포트로부터1개의 port로mirroring할 수 있다.

명령어	설명	모드
<b>mirroring target ifname</b>	<ul style="list-style-type: none"> <li>입력/출력 패킷이 mirroring 될 port 를 지정</li> </ul>	config
<b>mirroring rx-traffic</b>	<ul style="list-style-type: none"> <li>해당 포트의 입력 패킷을 mirroring 토록 설정</li> </ul>	interface
<b>mirroring tx-traffic</b>	<ul style="list-style-type: none"> <li>해당 포트의 출력 패킷을 mirroring 토록 설정</li> </ul>	interface

### 3.6. 2 계층 인터페이스 환경 설정

2계층 인터페이스는2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 U3000 Series 스위치에서는 물리적 포트와 port-group interface가 이 모드로 동작한다.

이 절에서는2계층 인터페이스의 설명과 물리적 포트와 port-group을2계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여준다.

#### 3.6.1. 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 네트워킹에 확장할 수 있다.

U3000 Series 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에trunk를 설정할 수 있다.

#### 3.6.2. 2 계층 인터페이스 모드

U3000 Series 스위치가 지원하는2계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있다.

표 3-7. U3000 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>

### 3.6.3. 2 계층 인터페이스 기본 설정 값

U3000 Series 스위치는 물리적 포트 또는 port-group이 layer2 interface로 설정될 때 다음과 같은 기본(default) 설정 값을 가진다.

표 8. 계층 인터페이스 기본 설정 값

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

### 3.6.4. 2 계층 인터페이스 설정/해제

2계층 인터페이스로 설정 및 해제하기 위한 명령어는 다음과 같다.

표 3-8. 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-grouping하거나 하고자 할 때 적용한다.

### 3.6.5. Trunk port 설정

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

표 3-9. Trunk port 설정 명령어

명령어	설명	모드
<b>switchport mode trunk</b>	■ trunk mode 설정	interface
<b>switchport trunk native vlan &lt;1-4094&gt;</b>	■ trunk port native VLAN 설정	interface
<b>no switchport trunk native vlan</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 2계층 트렁크 포트에 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# switchport ! layer2 interface set
Switch(config-if-fa1)# switchport mode trunk ! trunk port set
Switch(config-if-fa1)# switchport trunk native 2 ! native vlan set
Switch(config-if-fa1)# switchport trunk add 3 ! tagged vlan 등록
Switch(config-if-fa1)# switchport trunk add 4
Switch(config-if-fa1)# end
```

다음은 port-group 인터페이스를 2계층 트렁크 포트에 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
```

### 3.6.6. Access port 설정

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

표 3-10. Access port 설정 명령어

명령어	설명	모드
<b>switchport mode access</b>	■ access mode 설정	interface
<b>switchport access vlan &lt;14094&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 fa1
Switch(config-if-fa1)# switchport ! layer2 interface set
Switch(config-if-fa1)# switchport mode access ! access port set
Switch(config-if-fa1)# switchport access vlan 5 ! native vlan set
```

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

```
Switch# configure terminal
Switch(config)# interface po2
Switch(config-if-po2)# switchport ! layer2 interface
```

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

## 3.7. Port group

### 3.7.1. Port group 개요

Port group 이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용한다. U3000 Series 스위치에서 port group 인터페이스는 2계층 인터페이스로 사용될 수 있다.

U3000 Series 스위치의 모델별 설정 가능한 port group 수는 다음과 같다.

모델	port group 수	그룹 당 최대 port
PU3000	7	8

### 3.7.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같다.

표 3-11. 포트 그룹 설정 명령어

명령어	설명	모드
<b>port-group create ifname protocol none</b>	■ static port group 을 생성한다.	config
<b>no port-group ifname</b>	■ port-group 을 삭제한다	config
<b>lb-mode layer2 (src dst mix)</b>	■ load-balance 시 (source, destination, mixed) mac 을 참조.	interface
<b>lb-mode layer3 (src dst mix)</b>	■ load-balance 시 (source, destination, mixed) IP 를 참조	interface
<b>port-group ifname</b>	■ port group member 등록	interface *
<b>no port-group ifname</b>	■ port group 해제	
<b>show port-group</b>	■ port group 설정 출력	Privileged

```
Switch(config) # port-group create po1 protocol none ! port-group create
Switch(config) # interface range fastethernet 7-8 ! interface range set
Switch(config-ifrange) # no switchport ! no switchport set
Switch(config-ifrange) # port-group po1
Switch(config-ifrange) # exit
```

## 3.8. MAC Filtering

### 3.8.1. MAC Filtering 개요

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

### 3.8.2. MAC Filtering 설정

MAC Filtering 설정을 위한 기본 명령어는 다음과 같다.

표 3-12. mac-filter 설정 명령어

명령어	설명	모드
<code>mac-filter vlan-id mac-addr</code>	■ MAC Filter add	config
<code>no mac-filter vlan-id mac-addr</code>	■ MAC Filter delete	config

## 3.9. Traffic-control

### 3.9.1. Traffic-control 개요

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

### 3.9.2. Traffic-control 설정

Traffic-control 설정을 위한 기본 명령어는 다음과 같다. Traffic-control을 pps 단위로 kbps 단위로 걸 수 있으며, 두 가지 모두 설정할 수도 있다. 만약 두가지 모두 설정한 경우, 한가지 경우에만 해당되어도, 트래픽 차단 기능이 동작한다.

표 3-13. traffic-control 설정 명령어

명령어	설명	모드
<code>traffic-control pps &lt;1-1500000&gt; &lt;1-1500000&gt;</code>	해당 포트의 트래픽을 pps 단위로 설정한다.	interface
<code>traffic-control pps &lt;1-1500000&gt; &lt;1-1500000&gt; led-only</code>	해당 포트의 트래픽을 pps 단위로 설정하되, led만 켜고, 트래픽 차단은 하지 않는다.	interface
<code>no traffic-control pps</code>	해당 포트의 pps 트래픽 제한을 해제한다.	interface
<code>traffic-control kpps &lt;1-</code>	해당 포트의 트래픽을 kbps 단위로 설정한다.	interface

<b>1000000&gt; &lt;1-1000000&gt;</b>		
<b>traffic-control kbps &lt;1-1000000&gt; &lt;1-1000000&gt; led-only</b>	해당 포트의 트래픽을 kbps 단위로 설정하되, led 만 켜고, 트래픽 차단은 하지 않는다.	interface
<b>no traffic-control kbps</b>	해당 포트의 kbps 트래픽 제한을 해제한다.	interface
<b>show traffic-control</b>	현재의 설정 및 상태를 보여준다.	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 구분 되어 다른 VLAN 으로는 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 구분된다.

### 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

U3000 Series 스위치는 최대 256 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 할당 된 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 U3000 Series 스위치에서 1, 2, 3, 4 포트는 VLAN A 의 access 포트이고, 21, 22, 23, 24 포트는 VLAN B 의 access 포트에 할당된다. 그리고 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18 포트는 VLAN C 의 access 포트에 정의한다.

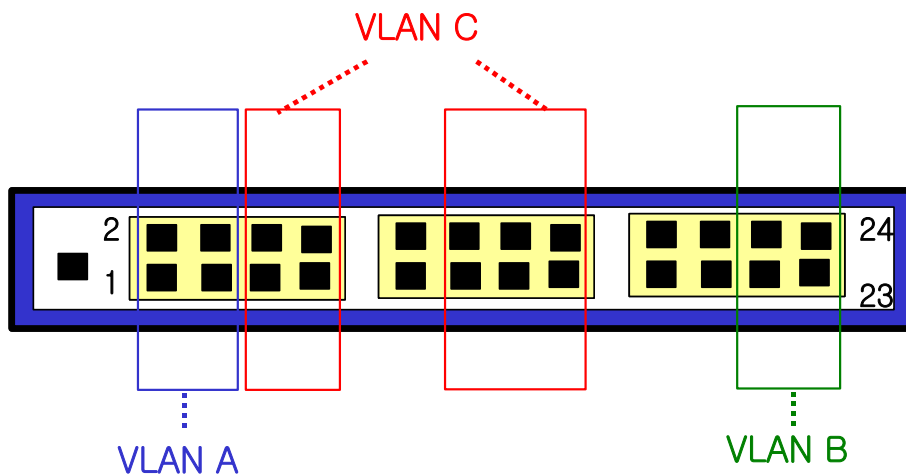


그림 4-1. U3000 Series 스위치의 포트 기반 VLAN 구성 예

서로 다른 VLAN 의 구성원들이 통신하기 위해서는, 비록 그들이 물리적으로 같은 I/O 모듈의 일부가더라도 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 VLAN 에 할당된 access 포트 중 하나씩을 사용하여 두 스위치를 케이블로 연결한다. 여러 개의 VLAN 을 연결하려면, 각각의 VLAN 마다 케이블로 스위치를 연결해야 한다.

<그림 2>는 서로 다른 2 개의 U3000 series 스위치를 하나의 VLAN 으로 묶는 방법을 보여준다. 먼저 스위치 1 의 4 개의 포트는 VLAN A 로 포함되도록 할당되어 있다. 또한 스위치 2 의 4 개 포트도 VLAN A 의 access 포트로 할당되어 있다. 두 스위치는 <그림 2>와 같이 상호 연결하여 하나의 브로트 캐스트 도메인을 형성한다.

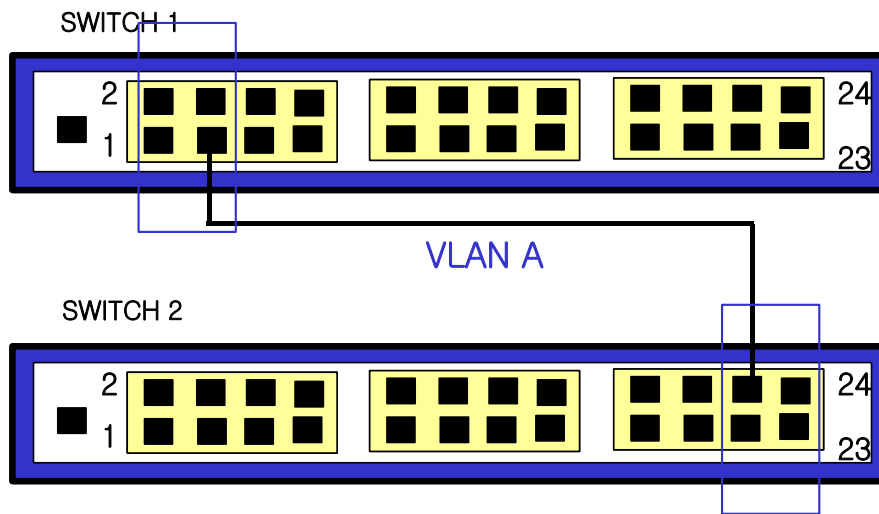


그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

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

<그림 4-3>은 두개의 U3000 Series 스위치에 걸쳐서 설정되는 두개의 VLAN 을 보여준다. 스위치 1 에서 포트 3, 4, 5, 6 포트는 VLAN A 의 access 포트이고 9, 10, 11, 12, 13, 14 까지의 포트는 VLAN B 의 access 포트가 할당되어 있다.

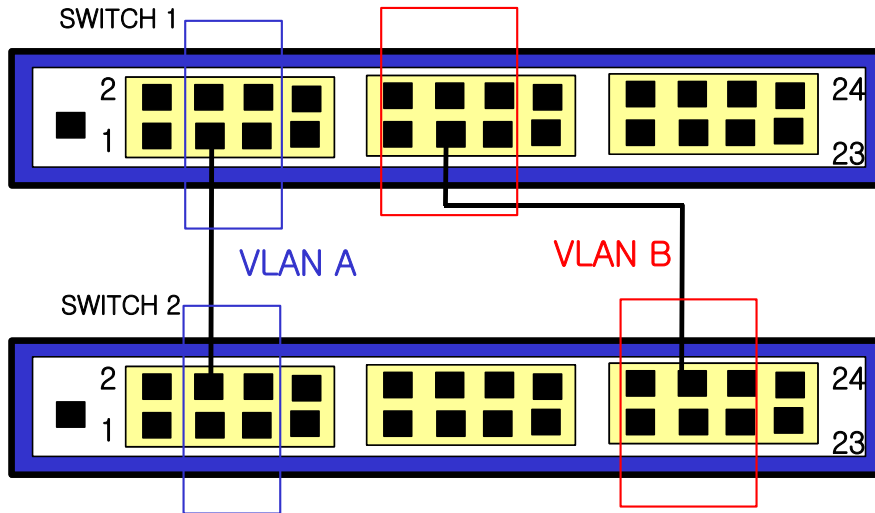


그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

VLAN A 는 스위치 1 의 포트 3 과 스위치 2 의 포트 4 의 연결을 통해 스위치 1 과 스위치 2 를 묶는다. VLAN B 는 스위치 1 의 포트 11 과 스위치 2 의 포트 20 사이를 연결하여 스위치 1 과 스위치 2 를 묶는다.

이런 설정 방법을 사용하면, 여러 개의 스위치를 데이지 체인(daisy-chain)으로 연결하는 다중 VLAN 을 생성할 수 있다. 각 스위치는 각각의 VLAN 의 연결을 위한 전용 access 포트를 가지며, 전용 access 포트는 다음 스위치에서 VLAN 의 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 VLAN 을 식별하기 위한 VLANid 가 포함된다.



**Notice**

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

### 4.2.2.1. 태그 VLAN 의 사용(Uses of Tagged VLANs)

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

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

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

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

#### 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 포트로 할당되어 사용될 때, 포트는 802.1Q VLAN 태그가 붙은 프레임을 사용한다. 이 경우 태그 VLAN 의 VLANid 가 프레임의 태그로 사용된다.

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



#### Notice

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

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

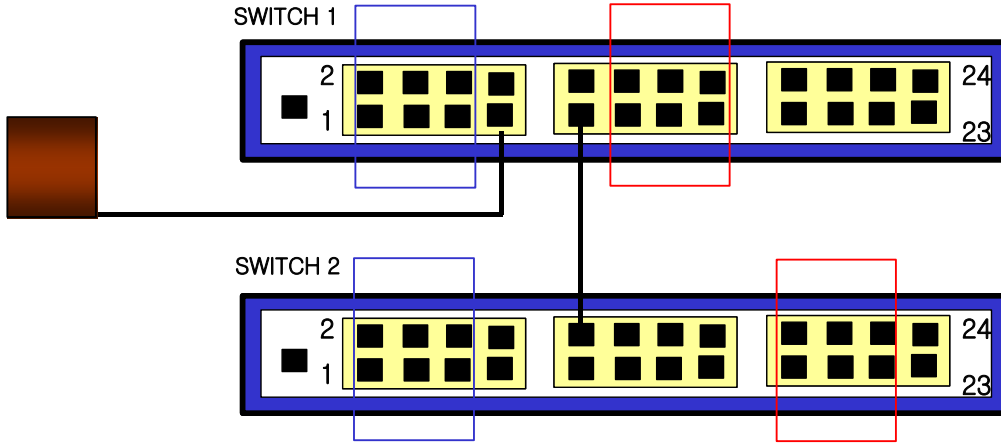


그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<그림 4-5 >은 동일한 네트워크의 논리적인 다이어그램을 보여준다.

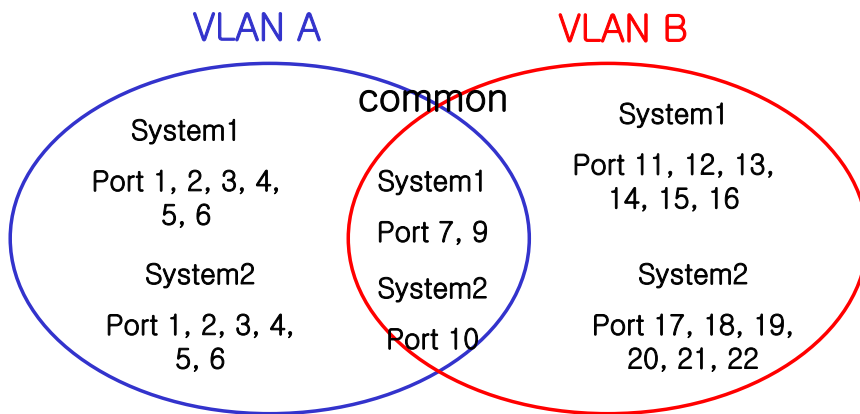


그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

<그림 4-4>와 <그림 4-5>에서:

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

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

### 4.2.3. 포트 기반 VLAN 과 태그 VLAN 의 혼합

한 스위치에서 포트 기반 VLAN 과 태그 VLAN 을 혼합해서 사용할 수 있다. 한 포트가 속하는 포트 기반 VLAN 은 오직 하나라는 조건 아래서 포트는 여러 VLAN 의 멤버가 될 수 있다. 즉, 포트는 동시에 하나의 포트 기반 VLAN 과 여러 개의 태그 VLAN 의 멤버가 될 수 있다.

## 4.3. VLAN 구성

### 4.3.1. VLAN ID

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

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

### 4.3.2. Default VLAN

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

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

### 4.3.3. Native VLAN

각 물리적 포트는 PVID(Port VLAN ID)를 가지고 있다. 모든 802.1Q 포트에는 자신의 native VLAN 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 4-6>처럼 태그가 붙지 않은 프레임과 PVID가 붙은 프레임이 공존하는 것이 허용되므로, VLAN을 지원하는 브리지가 end station과 VLAN을 지원하지 못하는 브리지가 end station들이 케이블로 연결될 수 있다.

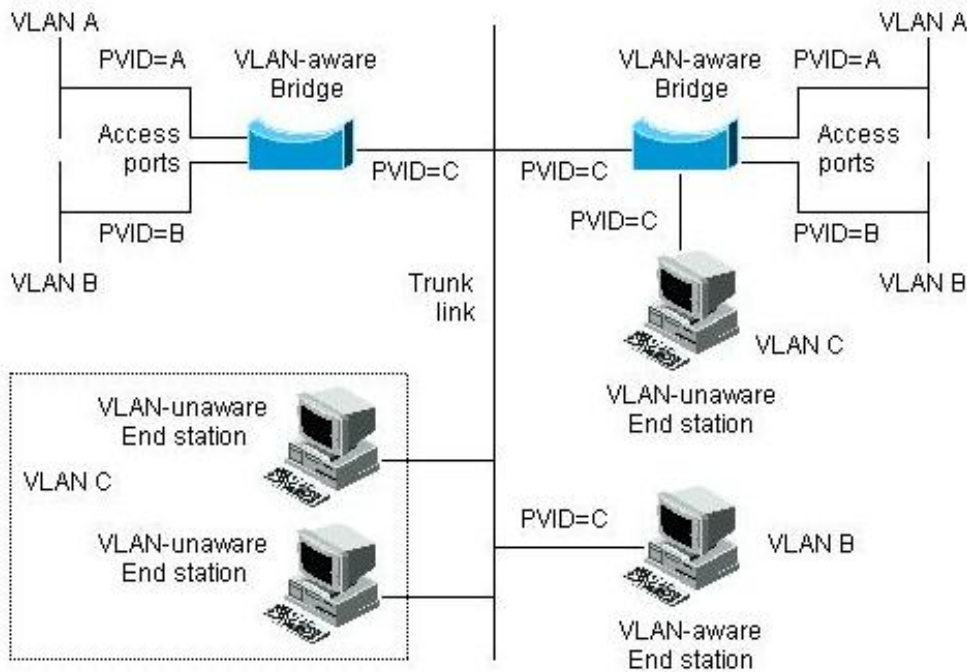


그림 4-6. Native VLAN

예를 들어 <그림 4-6>의 하단 부분에서처럼 두 end station이 중앙의 트렁크 링크에 연결된 상태를 생각해 보자. 그들은 VLAN을 인식하지 못하지만, VLAN을 인식하는 브리지의 PVID가 VLAN C와 동일하게 하므로 VLAN C에 포함될 것이다. VLAN을 인식하지 못하는 end station은 태그가 붙지 않은 프레임만 송신하므로, VLAN을 인식하는 브리지 장비가 이러한 태그가 붙지 않은 프레임을 수신했을 경우, 이를 VLAN C로 송신한다.

## 4.4. VLAN 설정

본 절에서는 U3000 Series 스위치에 VLAN 을 설정에 사용되는 명령들을 설명한다. VLAN 설정은 다음의 단계로 진행된다.

- 9) 생성된 VLAN 과 관련된 값을 설정한다.
- 10) 포트가 할당될 VLAN 의 종류에 따라 포트의 모드를 설정한다.
- 11) 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 4099 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



명령어	설명	모드
switchport trunk native <i>vlanid</i>	<ul style="list-style-type: none"> <li>■ 포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 붙지않고 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
switchport trunk remove { <i>vlanid</i>  all}	<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

## 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-int-vlan)# ip address 132.15.121.1/24
Switch(config-int-vlan)# interface fa2
Switch(config-int-fa2)# switchport mode access
Switch(config-int-fa2)# switchport access vlan 1000
Switch(config-int-fa2)# interface fa4
Switch(config-int-fa4)# switchport mode access
Switch(config-int-fa4)# switchport access vlan 1000
```

다음의 예제에서는 태그 기반 VLANid 로 2000 을 할당하고, 포트 1 와 포트 2 을 트렁크 포트 로 VLAN 에 추가한다.

```
Switch(config)# vlan 2000
Switch(config)# interface fa1
Switch(config-int-fa1)# switchport mode trunk
Switch(config-int-fa1)# switchport trunk add 2000
Switch(config-int-fa1)# interface fa2
Switch(config-int-fa2)# switchport mode trunk
Switch(config-int-fa2)# switchport trunk add 2000
```

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

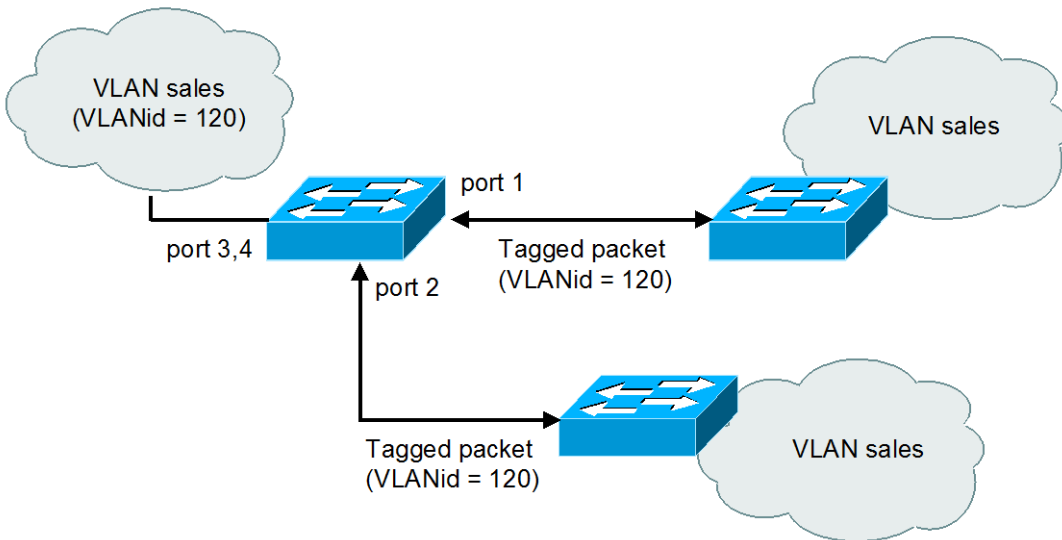


그림 4-7. VLAN 설정 예제 – Tagged and Untagged VLAN

```
Switch(config)# vlan 120
Switch(config)# interface fa1
Switch(config-int-fa1)# switchport mode trunk
Switch(config-int-fa1)# switchport trunk add 120
Switch(config-int-fa1)# interface fa2
Switch(config-int-fa2)# switchport mode trunk
Switch(config-int-fa2)# switchport trunk add 120
Switch(config-int-fa2)# interface fa3
Switch(config-int-fa3)# switchport access vlan 120
Switch(config-int-fa3)# interface fa4
Switch(config-int-fa4)# 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-vlan)# exit
Switch(config)# interface fa1
Switch(config-int-fa1)# switchport mode trunk
Switch(config-int-fa1)# switchport trunk native 200
Switch(config-int-fa1)# switchport trunk add 400
```

포트 fa1/1 으로 태그가 붙지 않은 프레임이 수신되면 스위치는 VLAN *marketing* 의 멤버 포트에 프레임을 전달한다.

## 4.6. VLAN 설정 정보 확인

VLAN 설정 정보를 보려면 다음의 명령을 사용한다.

명령어	설명	모드
show vlans	<ul style="list-style-type: none"> <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 fa1  fa2  fa3  fa4  fa5  fa6  fa7  fa8  fa9  fa10  fa11  fa12
 2 fa13  fa14  fa15
11 fa16  fa17  fa18  fa19  fa19  fa20  fa21  fa22  fa23  fa24
-----
Switch#
```

## 5

## IP 환경 설정

## 5.1. 개요

본 장에서는 IP 주소를 설정하는 방법을 설명한다.

IP를 설정하기 위해 요구되는 기본 작업은 IP 주소를 네트워크 인터페이스에 할당하는 것이다. IP 주소를 할당함으로써 인터페이스는 layer 3 interface로 활성화 된다.

U3000 Series 스위치는 다음의 인터페이스에 IP를 할당할 수 있다.

- VLAN 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.

U3000 Series 스위치는 하나의 인터페이스에 복수의 IP 주소를 할당하는 기능을 지원한다. U3000 Series 스위치는 인터페이스 당 최대 2 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 두개의 논리적인 서브넷을 구성할 수 있다.
- 많은 오래된 네트워크들은 계층 2의 브리지를 사용하여 구성되어 있으며, 서브넷으로 구성되어 있지 않다. 복수개의 주소의 적절한 사용은 서브넷으로의 전환과 라우터 기반 네트워크로 전환을 돕는다. 오래된 브리지 세그먼트에 속한 라우터는 그 세그먼트에 많은 서브넷이 존재한다는 사실을 쉽게 인식할 수 있다.
- 한 네트워크의 두 서브넷은 다른 네트워크에 의해 분리될 수 있다. 복수개의 주소를 사용하는 다른 네트워크에 의해 물리적으로 분리된 서브넷으로부터 하나의 네트워크를 구성할 수 있다. 이 예에서, 첫 네트워크는 확장되거나, 두 번째 네트워크의 상위에 위치한다. 서브넷은 라우터의 하나 이상의 활성화된 인터페이스에 동시에 나타날 수 없다.

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

표 5-2. IP 주소 할당 명령어

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



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

## 5.3. ARP(Address Resolution Protocol)

ARP 테이블의 정보를 확인하려면, `privilege` 모드에서 다음 < 표 5-3>의 명령어를 사용한다.

표 5-3. ARP 환경 설정을 위한 명령어

명령어	설명
<code>show arp</code>	■ ARP 테이블의 엔트리를 출력한다.

## 5.4. Default Gateway 설정

IP 패킷의 특정 목적지에 대한 경로를 구성할 수 없다면 `default gateway` 는 매우 중요하게 사용된다. 라우팅 될 수 없는 패킷들이 보내질 `Default gateway` 를 설정하려면 `Config` 모드에서 다음의 명령을 사용한다.

표 5-4. Default gateway 설정 명령어

명령어	설명
<code>ip default-gateway gateway-ipaddress</code>	<ul style="list-style-type: none"> <li>■ <code>Default gateway</code> 를 등록한다.</li> <li>■ <code>gateway-ipaddress</code> : 게이트웨이 장치의 IP 주소를 명시한다.</li> </ul>

`Default gateway` 정보를 확인하려면 `privileged` 모드에서 다음의 명령을 사용하라.

명령	설명
<code>show ip default-gateway</code>	■ <code>Default gateway</code> 정보를 출력한다.

## 5.5. IP 설정 예제

이 절에서는 IP 주소 설정 예제를 제공한다:

- Assign IP address to network interface
- ARP
- Default gateway

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

---

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

---

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제이다.

---

```
Switch# show arp
```

```
-----
```

IP Address	MAC Address	IPF	PORT	Flags
192.10.25.190	0000.f083.f6d4	vlan5	fa2	S

```
-----
total 1 entries found
```

---

다음의 예제는 스위치의 `default gateway` 로 `192.10.25.254` 를 설정한다.

---

```
Switch(config)# ip default-gateway 192.10.25.254
Switch(config)# end
Switch# show ip default-gateway
```

```
default gateway information
gateway: 192.10.25.254, vlan5, active
```

---

## 6

## DHCP RELAY

## 6.1. DHCP Relay 환경 설정

### 6.1.1. DHCP Relay 기능 개요

DHCP(Dynamic Host Configuration Protocol)는 IP 네트워크의 다른 IP 호스트(DHCP 클라이언트)들에게 재사용 가능한 IP 주소와 설정 파라미터를 동적으로 할당하는 방법을 제공한다. DHCP는 규모가 큰 네트워크 환경과 복잡한 TCP/IP 소프트웨어 설정을 위해 설계되었으며, 이는 IP 네트워크 관리자에게 요구되는 작업을 감소시킨다. 클라이언트가 서버로부터 수신하는 설정 정보 중 가장 중요한 것은 클라이언트의 IP 주소이다.

DHCP는 BOOTP의 확장이지만 DHCP와 BOOTP 사이에는 다음과 같은 두 가지 큰 차이점이 있다.

- DHCP는 클라이언트가 한정된 시간 동안만 IP 주소를 할당 받도록 하여, 후에 다른 클라이언트에게 그 IP 주소를 재할당하여 사용할 수 있는 방법을 제공한다.
- DHCP는 클라이언트가 TCP/IP 네트워크에서 동작하기 위해 필요한 추가적인 IP 설정 파라미터들을 설정할 수 있는 방법을 제공한다.



### 6.1.1.1. U3000 Series 스위치를 DHCP relay agent 로 사용

<그림 6-1>는 Premier DHCP 서버가 DHCP relay agent 로서 다른 네트워크의 DHCP 서버로 DHCP 클라이언트의 요구 메시지를 전달하는 절차이다.

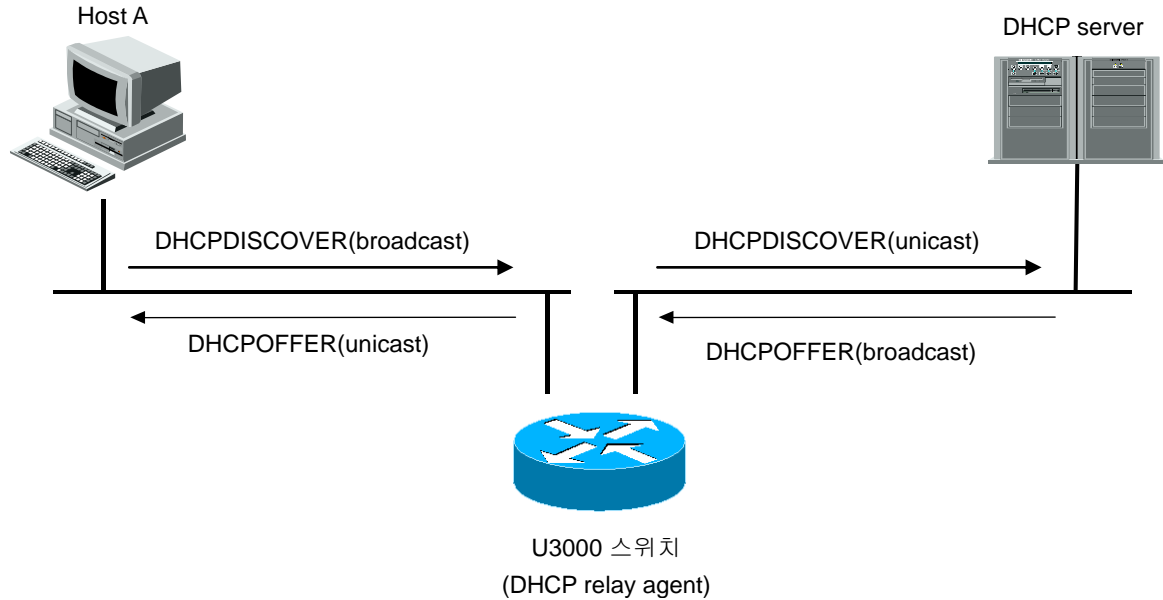


그림 6-1. DHCP relay agent 로서 DHCP 서버의 메시지 전달

DHCP 클라이언트는 브로드캐스트 메시지 **DHCPDISCOVER** 를 서버에게 전송한다.

- 1) Premier DHCP 서버가 클라이언트의 요구를 만족시킬 수 없다면, 운영자가 설정한 DHCP 서버로 유니 캐스트 메시지 **DHCPDISCOVER** 메시지를 사용하여 요구를 전달한다.
- 2) DHCP relay agent 로부터 메시지를 수신한 DHCP 서버는 클라이언트를 위한 IP 주소, 기본 라우터 등의 정보를 유니 캐스트 메시지 **DHCPOFFER** 를 사용하여 DHCP relay agent 에게 전송한다.
- 3) DHCP relay agent 는 수신한 **DHCPOFFER** 메시지를 클라이언트에게 전송한다.
- 4) DHCP 서버와 클라이언트 사이의 **DHCPREQUEST** 와 **DHCPACK** 메시지도 동일한 과정으로 DHCP relay agent 에 의해 전달된다.

## 6.1.2. DHCP relay agent 설정

U3000 series 를 DHCP relay agent 로 사용하면 DHCP 클라이언트로부터의 DHCP 요구를 설정된 DHCP 서버로 중계하게 된다.

### 6.1.2.1. DHCP relay agent 에서 서버 설정

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

명령어	설명
<b>ip dhcp helper-address</b> address <i>IFNAME(option)</i>	<ul style="list-style-type: none"> <li>▪ DHCP relay agent 가 DHCP 요청 패킷을 중계할 때 DHCP 서버의 IP 주소를 설정</li> <li>▪ <i>IFNAME</i>은 선택 항목으로 DHCP 요청 패킷을 수신한 Interface 별로 helper-address 를 설정할 때 사용한다.</li> <li>▪ DHCP 서버의 삭제는 이 명령의 <b>no</b> 형태를 사용</li> </ul>



#### Notice

DHCP Relay Agent 는 DHCP 요청 패킷을 수신한 인터페이스에 helper-address 가 설정되어 있으면 설정된 helper-address 로 DHCP 요청 패킷을 중계하고, 인터페이스에 helper-address 가 설정되어 있지 않으면 *IFNAME(option)*이 지정되지 않은 모든 helper-address 로 패킷을 중계한다.



#### Notice

U3000 series 의 DHCP relay Agent 는 helper-address 를 최대 20 개까지 설정 가능하다.

## 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 클라이언트에 대한 정보를 포함할 수 있도록 DHCP relay information option 기능을 제공한다.

### 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>

### 6.1.2.2. Relay information option 재중계 정책 설정

기본적으로, U3000 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 {append drop keep replace}</b>	<ul style="list-style-type: none"> <li>■ 기본 값은 replace 이다.</li> <li>■ append : 기존의 relay information 에 switch 의 relay information 을 더한다.</li> <li>■ drop : relay information 이 삽입되어 있는 패킷은 폐기한다.</li> <li>■ keep : 기존의 relay information 을 유지한다.</li> <li>■ replace : 기존의 relay information 을 Premier switch 의 relay information 으로 대체한다.</li> </ul>

### DHCP Smart Relay 설정

DHCP Relay Agent 에 smart-relay 기능을 활성화 하면, DHCP Server 로부터 BOOTPREPLY message 를 일정횟수(default : 3) 수신하지 못했을 때 gateway address 를 next ip address 로 변경한다.

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>

### DHCP relay server selection 설정

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

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

### 6.1.3. Premier DHCP relay 기능 활성화

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

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

## 6.2. DHCP relay 모니터링 및 관리

표 5. DHCP relay 모니터링 및 관리 명령어

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

### 6.3. DHCP 설정 예제

이 절에서는 다음의 설정 예를 제공한다.

- DHCP Relay Agent 설정 예제
- DHCP Relay Agent 모니터링 및 관리 예제

### 6.3.1. DHCP Relay Agent 설정

다음의 예제는 스위치의 DHCP Relay Agent 가 클라이언트의 DHCP 요청 패킷을 DHCP Server 에게 중계하도록 설정한다.

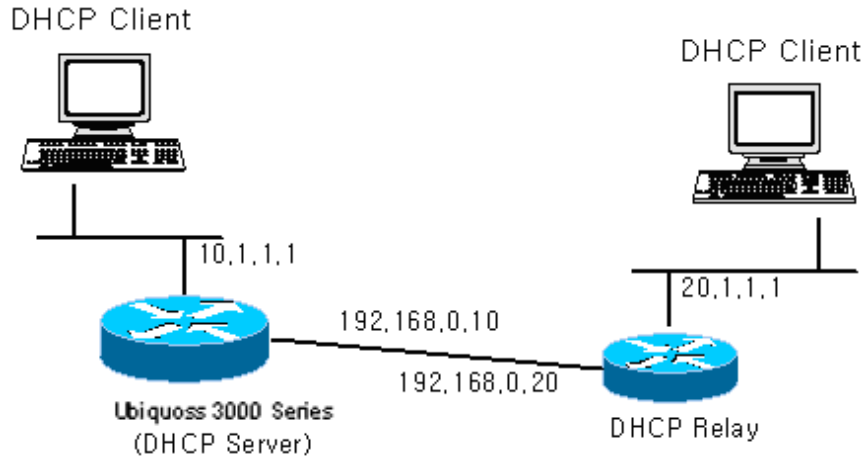


그림 6-2. 예제 네트워크 - DHCP Relay agent 환경 설정

```
Switch(config)# ip dhcp helper-address 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 서브네트워크에 위치한 DHCP 서버로 DHCP 메시지를 전달하려면, 해당 네트워크에 대한 라우팅 경로 정보가 설정되어 있어야 한다.

## 7

# IGMP Snooping

본 장에서는 U3000 Series 스위치에서의 IGMP Snooping 설정에 대해 설명한다.

## 7.1. IGMP Snooping 개요

일반적으로 스위치에서 Multicast Traffic 은 Unknown MAC address 나 Broadcast Frame 으로 처리되어 VLAN 에 속한 모든 포트들로 flooding 된다.

IGMP Snooping 은 VLAN 내의 모든 Member-Port 들로 Multicast Traffic 을 Forwarding 하지 않고, Multicast Traffic 을 Forwarding 할 Port 들을 동적으로 추가/삭제함으로써 Network 의 Bandwidth 를 효율적으로 사용할 수 있도록 해준다. IGMP Snooping 이 활성화된 스위치는 호스트와 라우터간의 IGMP Traffic 을 snooping 하여, Multicast Group 과 Member-Port 들에 대한 정보를 얻어낸다.

IGMP Snooping 의 절차에 대해서 간략히 설명하면 다음과 같다. 특정 Multicast Group 에 대한 IGMP Join 메시지를 받으면, 관련된 Multicast Forwarding Table Entry 에 그 호스트가 연결된 Port 를 추가한다. 호스트로부터 IGMP Leave 메시지를 받으면 반대로 그 호스트가 연결된 Port 를 Table Entry 에서 제거한다. 또한, Multicast Router 로부터의 IGMP Query 를 VALN 내의 포트들로 Forwarding 한 후, IGMP Join 메시지를 받지 못한 포트들은 삭제된다.

## 7.2. IGMP Snooping 설정

IGMP Snooping 은 Global 하게 모든 VLAN 에 enable/disable 이 가능하다.

## 7.2.1. Enable Global IGMP Snooping

Global 하게 IGMP Snooping 을 enable 하기 위해서는 다음의 명령을 global configuration mode 에서 사용한다.

명령어	설명
<b>ip igmp snooping</b>	IGMP Snooping 을 enable 한다.
<b>no ip igmp snooping</b>	IGMP Snooping 을 disable 한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit       : DISABLED
- IGMP Report Suppression  : DISABLED

vlan1
  IGMP snooping is ENABLED on this interface
  IGMP snooping fast-leave is DISABLED on this interface
  IGMP snooping mr-learn is DISABLED on this interface
  Vlan Members :
      vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2
```

## 7.2.2. Configure IGMP Snooping Functionality

IGMP Snooping 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행한다.

### 7.2.2.1. report-suppression 설정

기본적으로 IGMP Snooping 의 IGMP report-suppression 은 Disable 상태이며, 수신된 모든 IGMP

Report 들은 Multicast Router 로 Forward 되어진다. IGMP report-suppression 을 Enable 하면, IGMP Snooping 은 Multicast Membership Group 마다 하나의 IGMP Report 만 Multicast Router 로 Forward 된다.

이 기능은 IGMPv1, IGMPv2 Report 메시지에 한해서 적용된다.

명령	설명
<b>ip igmp snooping report-suppression</b>	IGMP report-suppression 을 설정한다.
<b>no ip igmp snooping report-suppression</b>	IGMP report-suppression 을 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping report-suppression
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit       : DISABLED
- IGMP Report Suppression  : ENABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is DISABLED on this interface
    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members :
        vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2
```

### 7.2.2.2. fast-leave 설정

IGMP Snooping 의 fast-leave 기능을 enable 하면 스위치가 호스트로부터 IGMPv2 Leave 메시지를 받았을 때 해당 포트를 포워딩 테이블에서 즉시 제거하게 된다.

이 기능은 VLAN 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.

Fast-Leave 는 아래의 설정과 같이 VLAN 별 및 PORT 별로 적용할 수 있으며, 만약 VLAN 별로 Fast-Leave 가 설정되면 VLAN 의 member 인 PORT 의 설정보다 우선한다.

명령	설명
----	----



<b>ip igmp snooping vlan &lt;1-4096&gt; fast-leave</b>	특정 VLAN 에 fast-leave 기능을 설정한다.
<b>no ip igmp snooping vlan &lt;1-4096&gt; fast-leave</b>	특정 VLAN 에 fast-leave 기능을 해제한다.
<b>ip igmp snooping vlan &lt;1-4096&gt; fast-leave IFNAME</b>	특정 VLAN 의 PORT 에 fast-leave 를 설정한다.
<b>no ip igmp snooping vlan &lt;1-4096&gt; fast-leave IFNAME</b>	특정 VLAN 의 PORT 에 설정된 fast-leave 를 해 제한다.

```

Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave vd25
Switch (config)# ip igmp snooping vlan 1 fast-leave vd26
Switch (config)# exit
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit       : DISABLED
- IGMP Report Suppression  : DISABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is ENABLED on vd25 vd26
    26    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members :
            vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2

Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave
Switch (config)# exit
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit       : DISABLED
- IGMP Report Suppression  : DISABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is ENABLED on this interface
    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members :
            vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2

```

### 7.2.2.3. mrouter 설정

Switch 는 VLAN 내의 모든 Multicast Traffic 이 다른 Network 으로 Forwarding 하기 위해서 모든 Multicast Traffic 을 Multicast Router 로 전달한다. 따라서, Multicast Router 가 연결된 Port 는 모든 Multicast Forwarding Table Entry 에 outgoing port 로 추가 된다.

기본적으로 IGMP Snooping 은 IGMP Traffic 만을 Snooping 하여 Multicast Router 와 연결된 Port 를 감지하며, PIM/DVMRP 프로토콜을 수동으로 enable 하여 mrouter port 를 감지할 수 있다.

위와 같은 방법으로 알게 된 mrouter port 들은 새로운 Multicast Forwarding Table Entry 가 생성될 때 마다 항상 outgoing 포트로 등록이 되어지게 되며, Multicast Traffic 뿐만 아니라 Host 에서 전송하는 IGMP Join 메시지도 Mrouter 로 Forwarding 되어 진다.

수동으로 Multicast Router Port 를 설정하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping vlan &lt;1-4096&gt; mrouter interface IFNAME</b>	mrouter port 를 수동으로 설정한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.
<b>no ip igmp snooping vlan &lt;1-4096&gt; mrouter interface IFNAME</b>	mrouter port 의 설정을 삭제한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter interface gi1
Switch (config)# exit
Switch # show ip igmp snooping mrouter
VLAN      MULTICAST-ROUTER-PORT
0001      gi1
```

동적으로 PIM/DVMRP 프로토콜을 통하여 Multicast Router Port 를 감지하기 위한 설정은 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping vlan &lt;1-4096&gt;</b>	PIM/DVMRP 프로토콜을 Snooping 하여 mrouter port 를

<b>mrouter learn pim-dvmrp</b>	감지하도록 설정한다.
<b>no ip igmp snooping vlan &lt;1-4096&gt;</b> <b>mrouter learn pim-dvmrp</b>	설정된 mrouter port 감지 방법을 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter learn pim-dvm
Switch (config)# exit
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
- Aging Interval          : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit      : DISABLED
- IGMP Report Suppression : DISABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is DISABLED on this interface
    IGMP snooping mr-learn is ENABLED on this interface
    Vlan Members :
        vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2
```

#### 7.2.2.4. aging time 설정

IGMP 프로토콜에서는 IGMP Querier 로 동작하는 Multicast Router 가 주기적으로 IGMP Query 메시지를 전송하고, 호스트들은 이에 대한 응답으로 IGMP Join 메시지를 전송함으로써 Multicast Group에 대한 Membership 이 관리되어진다. IGMP Snooping 은 이러한 IGMP 프로토콜 메시지들을 이용하여 Multicast Forwarding Table Entry 의 outgoing port 들을 추가/삭제한다.

만약, 설정된 aging 시간동안 IGMP Join 메시지를 받지 못해 Multicast Forwarding Table Entry 의 갱신이 되지 않으면 해당 포트는 outgoing 포트로부터 Multicast Forwarding Table Entry 에서 삭제 되어진다.

aging time 의 기본값은 300 초이며, 다음의 명령을 global configuration mode 에서 수행하여 설정 한다.

명령어	설명
<b>ip igmp snooping aging &lt;30-3600&gt;</b>	aging time 을 설정한다. (default : 300 초)
<b>no ip igmp snooping aging</b>	설정된 aging time 을 default aging time 으로 변경한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping aging 250
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
Global IGMP Snooping configuration:
- Aging Interval           : 250 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit       : DISABLED
- IGMP Report Suppression  : DISABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is DISABLED on this interface
    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members :
        vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2
```

#### 7.2.2.5. last-member-join-interval 설정

VLAN 에 IGMP Snooping 의 fast-leave 기능이 설정되어 있지 않은 경우에 IGMP Leave 메시지를 수신하게 되면 즉시 해당 포트를 제거하지 않으며, 설정된 aging time 이후에 Multicast Forwarding Table Entry 에서 삭제된다.

설정된 aging time 의 종료전에 좀 더 빨리 Multicast Membership 관리가 이루어 질수 있도록 last-member-join-interval 을 설정할 수 있다.

만약, last-member-join-interval 이 설정되어 있지 않다면 last-member-join-interval 은 aging time 과 동일하게 자동으로 설정되며, 해당 포트는 IGMP Snooping 의 aging time 에 준하여 제거되어진다. 이 기능은 VLAN 에 fast-leave 기능이 설정되어 있지 않은 경우에만 유효하다.

last-member-join-interval 의 설정은 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping last-member-join-interval &lt;5-300&gt;</b>	last-member-join-interval 을 설정한다. (default : 300 초)
<b>no ip igmp snooping last-member-join-interval</b>	설정된 last-member-join-interval 을 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping last-member-join-interval 5
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 5 sec
- TCN Query Solicit       : DISABLED
- IGMP Report Suppression  : DISABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is DISABLED on this interface
    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members :
        vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2
```

#### 7.2.2.6. tcn (Topology Change Notification) 설정

기본적으로 IGMP Snooping은 spanning-tree Topology Change Notification(TCN)을 수신하였을 때, Multicast Forwarding Table Entry를 모두 초기화한다. 이후, Multicast Router의 IGMP Query에 의해서 Multicast Forwarding Table Entry가 새로 생성되게 된다.

본 장비에서 제공되는 tcn 설정은 spanning-tree Topology Change Notification(TCN)을 수신하였을 때, Multicast Router에게 "0.0.0.0" Group에 대해서 IGMP Leave 메시지를 전송한다. Multicast Router는 "0.0.0.0" Group에 대한 IGMP Leave 메시지를 수신한 후, IGMP Query 메시지를 전송하게 되며, 빠른 시간내에 Topology가 변경된 Network의 Multicast Forwarding Table Entry가 새로 생성되게 된다.

tcn의 설정은 spanning-tree로 형성된 모든 장비에 설정 가능하며, 다음의 명령을 global configuration mode에서 수행한다.

명령어	설명
<b>ip igmp snooping tcn query-solicit</b>	TCN Query Solicit을 설정한다.
<b>no ip igmp snooping tcn query-solicit</b>	설정된 TCN Query Solicit을 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping tcn query-solicit
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit      : ENABLED
- IGMP Report Suppression  : DISABLED

vlan1
    IGMP snooping is ENABLED on this interface
    IGMP snooping fast-leave is DISABLED on this interface
    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members :
        vd25 vd26 vd27 vd28 vd29 vd30 vd31 vd32 gi1 gi2
```

### 7.2.2.7. igmp filtering 설정

igmp filtering 은 스위치 포트에 속한 사용자의 IGMP Packet 들을 filtering 한다. 따라서 특정 Network 환경의 Service 계획이나 신청에 의한 서비스 제공등과 같은 Multicast 서비스의 분배를 관리할 수 있다.

각각의 Switch Port 들은 filtering 에 대한 IGMP Profile 을 가지며, IGMP Profile 은 하나이상의 Multicast Group 들과 해당 Group 에 대한 차단과 허용을 포함하고 있다.

Igmp filtering 을 설정하기 위해서는 먼저 IGMP Profile 을 설정해야 되며, IGMP Profile 의 설정은 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping profile &lt;1-99&gt; permit &lt;multicast address&gt; range &lt;multicast address&gt;</b>	IGMP Filtering 을 허용하는 IGMP Profile 을 설정한다.
<b>ip igmp snooping profile &lt;1-99&gt; deny {&lt;multicast address&gt;   &lt;all&gt;} range &lt;multicast address&gt;</b>	IGMP Filtering 을 차단하는 IGMP Profile 을 설정한다.
<b>no ip igmp snooping profile &lt;1-99&gt;</b>	설정된 IGMP Profile 을 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping profile 1 deny 224.1.0.0/16
Switch (config)# ip igmp snooping profile 2 deny 224.1.0.0/16 range 224.2.0.0/16
Switch (config)# ip igmp snooping profile 3 permit 224.0.0.0/8
Switch (config)# exit
Switch # show ip igmp snooping profile
IGMP Profile 1
    deny
    range : 224.1.0.0/16 224.1.0.0/16
IGMP Profile 2
    deny
    range : 224.1.0.0/16 224.2.0.0/16
IGMP Profile 3
    permit
    range : 224.0.0.0/8 224.0.0.0/8
```

IGMP Profile 을 생성한 후, igmp filtering 을 적용하려면 다음의 명령을 interface mode 에서 수행한다.

명령어	설명
<b>ip igmp snoop-filter &lt;1-99&gt;</b>	IGMP Filtering 을 스위치 포트에 적용한다.
<b>no ip igmp snoop-filter &lt;1-99&gt;</b>	설정된 IGMP Filtering 을 스위치 포트에서 삭제한다.

```
Switch # configure terminal
Switch (config)# interface fa1
Switch (config-if-fa1)# ip igmp snoop-filter 1
Switch (config-if-fa1)# end
Switch # show running-configure
...
!
interface fa1
    ip igmp snoop-filter 1
...
```

### 7.2.2.8. igmp max-group-count 설정

각 가입자별로 multicast service 를 구분하여 제공하기 위해서 Multicast Group 개수를 제한할 수 있다. Multicast Group 의 개수를 제한하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping max-group-count</b> <i>IFANME</i> <count>	max-group-count 를 스위치 포트에 적용한다.
<b>no ip igmp snooping max-group-count</b> <i>IFANME</i>	설정된 max-group-count 를 스위치 포트에서 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-group-count vd25 10
Switch # show running-configure

...
ip igmp snooping
ip igmp snooping max-group-count vd25 10
...

Switch #
```

### 7.2.2.9. igmp max-reporter-count 설정

각 VLAN interface 별로 가입자의 수를 제한하여 multicast service 를 제공하기 위해서 Host 의 개수를 제한할 수 있다.

Host 의 개수를 제한하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping max-reporter-count</b> <i>vlan</i> <vlan-id> <count>	max-reporter-count 를 VLAN interface 에 적용한다.
<b>no ip igmp snooping max-reporter-count</b> <i>vlan</i> <vlan-id>	설정된 max-reporter-count 를 VLANinterface 에서 해제한다.



```
Switch # configure terminal
Switch (config)# ip igmp snooping max-reporter-count vlan 1 10
Switch #
Switch # show running-configure

...
ip igmp snooping
ip igmp snooping max-reporter-count vlan 1 10
...

Switch #
```

## 7.3. IGMP Proxy-Reporting 개요

일반적으로 Network 장비들의 처리능력은 한정되어 있지만, 다양한 Multicast Service의 증가와 Multi-Accessed Network 환경 등으로 인해 동시에 처리되어지는 IGMP의 Membership 요청이 증가되고 있다. 이러한 IGMP HOST들의 IGMP Membership 요청은 상위 Network에 위치한 장비의 과부하를 초래할 수 있으며, Multicast Service의 지연 또는 단절을 초래할 수 있다.

이러한 이유로 인해 DSL Forum에서는 IGMP Proxy-Reporting의 기능을 정의한 문서를 제공하고 있으며, 본 장비에서는 DSL Forum에서 정의한 IGMP Proxy-Reporting 기능을 포함하고 있다.

IGMP Proxy-Reporting은 IGMP에서 규정된 모든 기능을 제공한다. IGMP Proxy-Reporting은 IGMP Proxy-Reporting이 활성화된 VLAN interface에 IP Address가 존재하는 경우 IGMP Report 및 IGMP Query 메시지의 IP Source Address를 지정된 VLAN의 IP Address를 사용하며, VLAN의 IP Address가 지정되지 않는 경우에는 IGMP Membership에서 관리되는 가장 최신의 IGMP Host Address를 사용한다.

## 7.4. IGMP Proxy-Reporting 설정

IGMP Proxy-Reporting 의 서비스는 Global 하게 enable/disable 이 가능하며, VLAN Interface 별로 IGMP Proxy-Reporting 의 기능을 적용할 수 있다.

기본적으로 IGMP Proxy-Reporting 은 IGMP Querier Selection 이 이루어지지 않는다. 따라서 VLAN interface 에 IGMP Proxy-Reporting 의 기능을 적용하기 위해서는 Multicast Router Port 를 반드시 지정해야 한다.

### 7.4.1. Enable IGMP Proxy-Reporting

Global 하게 IGMP Proxy-Reporting 을 enable 하기 위해서는 다음의 명령을 global configuration mode 에서 사용한다.

명령어	설명
<b>ip igmp snooping proxy-reporting</b>	IGMP Proxy-Reporting 을 enable 한다.
<b>no ip igmp snooping proxy-reporting</b>	IGMP Proxy-Reporting 을 disable 한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting
Switch (config)#
Switch # show ip igmp snooping proxy-reporting interface
IGMP Proxy Interface

IGMP Gateway is DISABLED on ALL interface.

-----
total : 0
Switch #
Switch #
```

### 7.4.2. Enable IGMP Proxy-Reporting on a VLAN

본 장비에서는 IGMP Proxy-Reporting 을 VLAN 별로 enable/disable 할 수 있다.

실제 IGMP Proxy-Reporting 기능이 적용될 VLAN 을 설정하기 위해서는 다음의 명령을 global configuration mode 에서 사용한다.

IGMP Proxy-Reporting 기능이 적용된 VLAN에서는 IGMP Snooping을 통한 IGMP 패킷 Forwarding이 이루어지지 않는다.

VLAN에 IGMP Proxy-Reporting 기능을 적용하기 위해서는 먼저 Multicast Router Port를 지정해야 한다.

명령어	설명
<b>ip igmp snooping proxy-reporting vlan &lt;1-4096&gt;</b>	특정 VLAN에 IGMP Proxy-Reporting을 enable한다.
<b>no ip igmp snooping proxy-reporting vlan &lt;1-4096&gt;</b>	특정 VLAN에 IGMP Proxy-Reporting을 disable한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1
Switch (config)#
Switch # show ip igmp snooping proxy-reporting interface
IGMP Proxy Interface

vlan1
    IGMP Proxy is ENABLED on this interface
    IGMP Query-Interval is 60 seconds.
    IGMP Leave-Timeout is 10 seconds.
    IGMP Query-Max-Response-Time is 10 seconds.
    Multicast Router Port : NOT CONFIGURED!
    VLAN Members :
        fa1 fa2 fa3 fa4 fa5 fa6 fa7 fa8

total : 1

Switch #
```

### 7.4.3. Configure IGMP Proxy-Reporting Functionality

IGMP Proxy-Reporting 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행한다.

#### 7.4.3.1. Multicast Router Port 지정

IGMP Proxy-Reporting에서 관리되는 IGMP Membership의 정보와 상위 Multicast Router와의 연동을 위해서 반드시 Multicast Router Port를 지정해야 한다. Multicast Router Port가 지정되지 않은 VLAN은 IGMP Proxy-Reporting 기능을 적용할 수 없다.

명령어	설명
<b>ip igmp snooping proxy-reporting vlan &lt;1-4096&gt; mrouter-port IFNAME</b>	특정 VLAN 에 IGMP Proxy-Reporting 을 위한 Multicast Router Port 를 지정한다.
<b>no ip igmp snooping proxy-reporting vlan &lt;1-4096&gt; mrouter-port IFNAME</b>	지정된 특정 VLAN 에 IGMP Proxy-Reporting 을 위한 Multicast Router Port 를 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 mrouter-port fa1
Switch (config)#
Switch # show ip igmp snooping proxy-reporting interface
IGMP Proxy Interface

vlan1
    IGMP Proxy is ENABLED on this interface
    IGMP Query-Interval is 60 seconds.
    IGMP Leave-Timeout is 10 seconds.
    IGMP Query-Max-Response-Time is 10 seconds.
    Multicast Router Port : fa1
    VLAN Members :
        fa1 fa2 fa3 fa4 fa5 fa6 fa7 fa8

total : 1

Switch #
```

### 7.4.3.2. IGMP Static-Group 지정

IGMP Proxy-Reporting 에서는 특정한 Multicast Group 의 Traffic 을 수신하기 위해서 소요되는 Join Delay Time 을 최소화하기 위해서 Static-Group 기능을 제공한다.

Static-Group 은 Multicast-Router Port 로 지정된 IGMP Report 를 주기적으로 전송하여 Multicast Traffic 을 계속해서 수신하기 위해서 제공된다.

이 기능은 반드시 IGMP Snooping 과 함께 동작하여야 하며, 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
<b>ip igmp snooping proxy-reporting vlan &lt;1-4096&gt; static-group A.B.C.D</b>	특정 VLAN 에 IGMP Proxy-Reporting 를 통한 IGMP Static-Group 을 지정한다.
<b>no ip igmp snooping proxy-reporting vlan &lt;1-4096&gt; static-group A.B.C.D</b>	지정된 IGMP Static-Group 을 해제한다.

```

Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 static-group
224.1.1.1
Switch # show ip igmp snooping proxy-reporting group
  VLAN          GROUP          LAST-REPORTER    EXPIRE-TIME
  0080  224.1.1.1      0.0.0.0          00:04:03  STATIC-GROUP
-----
total : 1

Switch #

```

## 7.4.4. Display System and Network Statistics

표 7-1. IGMP Snooping 관련 모니터링 명령어

명령어	설명
<b>show ip igmp snooping</b>	모든 VLAN 에 대한 IGMP snooping 의 상태를 보여준다.
<b>show ip igmp snooping vlan &lt;1-4096&gt;</b>	특정 VLAN 에 대한 IGMP snooping 의 상태를 보여준다
<b>show ip igmp snooping mrouter</b>	모든 mrouter 에 대한 정보를 보여준다.
<b>show ip igmp snooping mac-entry</b>	설정된 Multicast Forwarding Table Entry 에 대한 정보를 보여준다.
<b>show ip igmp snooping mac-entry vlan &lt;1-4096&gt;</b>	특정 VLAN 에 대한 설정된 Multicast Forwarding Table Entry 에 대한 정보를 보여준다.
<b>show ip igmp snooping querier</b>	Multicast Router 의 모든 IGMP Querier 에 대한 정보를 보여준다.
<b>show ip igmp snooping querier vlan &lt;1-4096&gt;</b>	특정 VLAN 에 대한 Multicast Router 의 모든 IGMP Querier 에 대한 정보를 보여준다.
<b>show ip igmp snooping reporter</b>	모든 IGMP Reporter 에 대한 정보를 보여준다.
<b>show ip igmp snooping reporter vlan &lt;1-4096&gt;</b>	특정 VLAN 에 대한 모든 IGMP Reporter 에 대한 정보를 보여준다.
<b>show ip igmp snooping profile</b>	설정된 IGMP Profile 에 대한 정보를 보여준다.
<b>show ip igmp snooping suppression-forwarder</b>	suppression 된 multicast group 의 forwarder 에 대한 정보를 보여준다.

표 7-2. IGMP Proxy-Reporting 관련 모니터링 명령어

명령어	설명
<b>show ip igmp snooping proxy-reporting interface</b>	모든 VLAN 에 대한 IGMP Proxy-Reporting 의 상태를 보여준다.
<b>show ip igmp snooping proxy-reporting group</b>	관리되는 모든 IGMP Membership 정보를 보여준다.
<b>show ip igmp snooping proxy-reporting querier</b>	인식된 모든 IGMP Querier 정보를 보여준다.

## 8

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

이 장에서는 Spanning Tree Protocol(STP)과 Rapid Spanning Tree Protocol(RSTP)를 설정하는 방법과 자신이 전송한 패킷이 되돌아 오는 현상을 감지하는 self-loop 감지 기능을 설정하는 방법에 대해 설명한다.

**Note**

이 장에서 사용되는 명령의 완전한 형식 및 사용법은 `command reference` 를 참고하라.

이 장은 다음의 절들로 구성된다:

- Understanding Spanning-Tree Features
- Understanding RSTP
- Configuring Spanning-Tree Features
- Displaying the Spanning-Tree Status
- Self-loop Detection

## 8.1. Understanding Spanning-Tree Features

이 절에서는 다음의 STP 기능에 대해 설명한다:

- STP Overview
- 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 States

### 8.1.1. 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 활성화 시킨다.

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.

### 8.1.2. 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 포트로 configuration BPDU를 전송한다. 스위치들은 BPDU를 서로 교환하고 BPDU로 spanning-tree 형상을 계산한다. 각 configuration BPDU는 다음의 정보를 포함한다:

- root 스위치의 BridgeID

- root 까지의 spanning-tree path cost
- BPDU를 전송하는 스위치의 BridgeID
- Message age
- BPDU를 전송하는 스위치의 인터페이스의 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.

### 8.1.3. 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 스위치의 선출
- 중복된 링크로 연결된 Layer 2 인터페이스의 차단에 의한 switched 네트워크의 루프 제거

각 VLAN 에서 가장 높은 스위치 priority(작은 숫자 값을 가진)를 가진 스위치가 root 스위치로 결정된다. 모든 스위치가 default priority(32768)로 설정되었다면, VLAN 에서 가장 낮은 MAC 주소를 가진 스위치가 root 스위치가 된다. 스위치 priority 는 BridgeID 의 최상위 비트에 포함된다.

스위치의 스위치 priority 의 값을 변경함으로써 그 스위치가 root 스위치가 될 가능성을 변경할 수 있다. 스위치 priority 를 큰 값으로 설정하면 가능성이 낮아지고, 작은 값으로 설정하면 가능성이 높아진다.

Root 스위치는 switched 네트워크에서 spanning-tree 형상의 논리적인 중심이다. Switched 네트워크에서 root 스위치로 달을 필요가 없는 경로들은 spanning-tree blocking 상태가 된다.

BPDU 는 BPDU 를 전송하는 스위치와 포트, 스위치의 MAC 주소, 스위치 priority, port priority, path cost 등의 정보를 포함한다. Spanning tree 는 이 정보를 사용하여 root 스위치와 root 포트, designated 포트를 결정한다.

### 8.1.4. 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.

U3000 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.

**표 8-1. Switch Priority Value and Extended System ID**

Switch Priority Value				Extended System ID(Set Equal to the VLAN ID)											
Bit16	Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8	Bit7	Bit6	Bit5	Bit 4	Bit3	Bit2	Bit1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Spanning tree 는 extended system ID 와 스위치 priority, 그리고 MAC 주소로 BridgeID 를 만든다.

### 8.1.5. Spanning-Tree Timers

표는 spanning-tree 의 성능에 영향을 미치는 타이머들을 나타낸다.

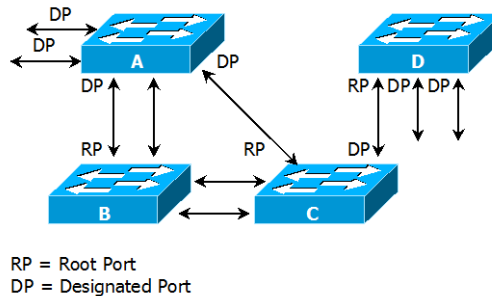
**표 8-2. Spanning-Tree Timers**

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 얼마동안 저장할 것인가를 결정한다.

### 8.1.6. 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 8-1 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.

### 8.1.7. Spanning-Tree Interface States

프로토콜 정보가 switched LAN 을 통해 전달될 때 전파지연이 발생한다. 그 결과 다른 시각, 다른 장소에서 switched LAN 의 형상변화가 발생한다. Spanning-tree 에 참여하지 않는 Layer 2 인터페이스가 바로 forwarding 상태가 된다면 일시적인 데이터 루프가 발생할 수 있다. 그러므로 스위치는 프레임을 forwarding 하기 전에 switched LAN 을 통해 전파되는 새로운 형상 정보를 기다려야 한다.

Spanning tree 가 활성화된 스위치의 각 Layer 2 인터페이스는 다음 상태 중 하나이다:

- Blocking - 인터페이스는 프레임을 forwarding 하지 않는다.
- Listening - 인터페이스가 프레임을 forwarding 해야 한다고 결정되었을 때, blocking state 다음의 천이 상태.
- Learning - 인터페이스가 프레임을 forwarding 하기 위해 준비한다. MAC learning이

수행된다.

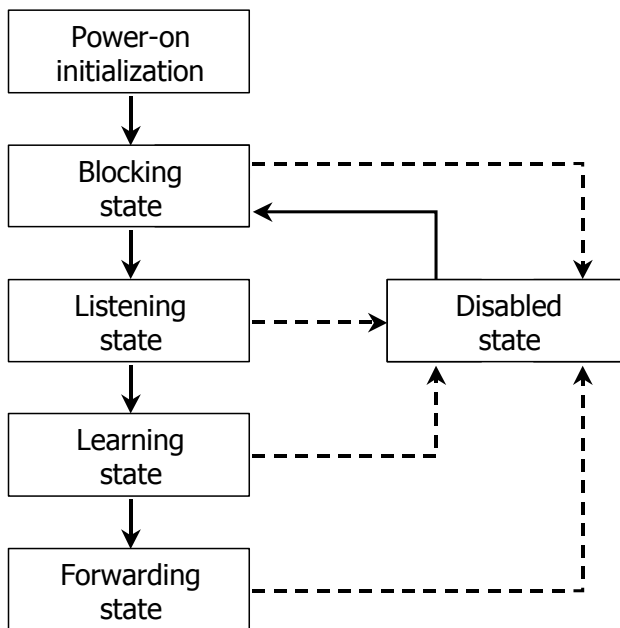
- Forwarding – 인터페이스가 프레임을 forward 한다.
- Disabled – 포트가 shutdown 상태이거나 포트에 링크가 없거나, 포트에 실행중인 spanning-tree instance가 없기 때문에 인터페이스는 spanning tree에 참여하지 않는다.

인터페이스들은 다음의 상태로 이동한다:

- 초기상태에서 blocking 상태로
- blocking 상태에서 listening 혹은 disabled 상태로
- listening 상태에서 learning 혹은 disabled 상태로
- learning 상태에서 forwarding 혹은 disabled 상태로
- forwarding 상태에서 disabled 상태로

다음의 그림은 인터페이스의 상태천이를 보여준다.

**그림 8-2 Spanning-Tree Interface States**



STP 가 활성화 되었을 때, 스위치의 모든 인터페이스는 blocking 상태가 되고 listening 과 learning 의 일시적인 상태를 지난다. 안정화된 spanning tree 에서 각 인터페이스는 forwarding 혹은 blocking 상태로 설정된다.

Spanning-tree 알고리즘이 Layer 2 인터페이스를 forwarding 상태로 만들기로 결정했다면 다음의 과정이 발생한다:

1. 인터페이스가 forwarding 상태가 되어야 한다는 프로토콜 정보를 수신하면 인터페이스는 listening 상태가 된다.
2. forward-delay 타이머가 만료되었을 때, spanning tree는 인터페이스를 learning 상태로 만들고 forward-delay 타이머를 재설정한다.
3. learning 상태에서, 인터페이스는 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.

## 8.2. 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

### 8.2.1. 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.

### 8.2.2. 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 forward 할 때 최적의 경로(가장 낮은 cost)를 제공한다.
- Designated port – designated 스위치와 연결되어, LAN에서 root 스위치로 패킷을 forward 할 때 가장 낮은 비용을 제공한다. LAN과 연결되어 있는 designated 스위치의 포트를 designated port라 부른다.
- Alternate port – 현재 root 포트가 제공하는 root 스위치로의 대체 경로를 제공한다.
- Backup port – spanning tree의 앞쪽으로 향한 designated 포트에 의해 제공되는 경로의 backup으로 동작한다. Backup 포트는 두 포트가 point-to-point 링크로 loopback으로 연결되었거나 스위치가 공유 LAN 조각에 대해 둘 이상의 연결이 있을 경우에만 존재한다.
- Disabled port – spanning tree의 동작에서 아무런 역할도 가지지 않는다.

root 혹은 designated 포트 역할을 가진 포트는 active 형상에 포함된다. alternate 혹은 backup 포



트 역할을 가진 포트는 active 형상에서 제외된다.

네트워크 전체가 일관된 port role 을 가진 안정된 형상에서, RSTP 는 모든 root 포트와 designated 포트가 바로 forwarding 상태로 천이하는 것을 보장한다. 반면 모든 alternate 포트와 backup 포트는 항상 discarding 상태(802.1D 의 blocking 과 동등한 상태)에 놓인다. 포트의 상태는 forwarding 과 learning 과정의 동장을 제어한다. 다음의 표는 802.1D 와 RSTP 의 포트 상태를 비교한다.

**표 8-3. Port State Comparison**

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

STP 구현과의 일관성을 위해, 이 문서에서는 포트 상태에서 *discarding* 대신 *blocking* 을 사용한다. Designated port 는 listening 상태에서 시작한다.

### 8.2.3. Rapid Convergence

RSTP 는 다음과 같은 스위치, 포트 혹은 LAN 의 장애에 대해 빠른 연결의 복구를 제공한다. edge 포트와 새로운 root 포트, 그리고 point-to-point 링크로 연결된 포트에 대해 빠른 복구를 제공한다:

- Edge ports – RSTP 스위치에서 포트를 edge 포트로 설정하면, edge 포트는 forwarding 상태로 바로 천이한다. edge 포트는 STP에서 PortFast가 설정된 포트와 동일하고, 하나의 종단 단말과 연결된 포트에만 설정해야 한다.
- Root ports – RSTP가 새로운 root 포트를 선택하면, 이전의 root 포트는 block 상태가 되고, 새로운 root 포트는 바로 forwarding 상태가 된다.
- Point-to-point links – 포트를 다른 포트와 point-to-point 링크로 연결한다면, 로컬 포트는 designated 포트가 되고 루프를 제거하기 위해 다른 포트와 proposal-agreement 교환을 통한 빠른 천이를 협상한다.

다음 그림에서, 스위치 A 는 스위치 B 와 point-to-point 링크로 연결되어 있고 모든 포트는 blocking 상태이다. 스위치 A 의 priority 가 스위치 B 의 priority 보다 낮은 수의 값을 가진다고 가정하자. 스위치 A 는 proposal 메시지(proposal flag 가 설정된 BPDU)를 스위치 B 로 전송하고 자신을 designated 스위치로 제안한다.

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

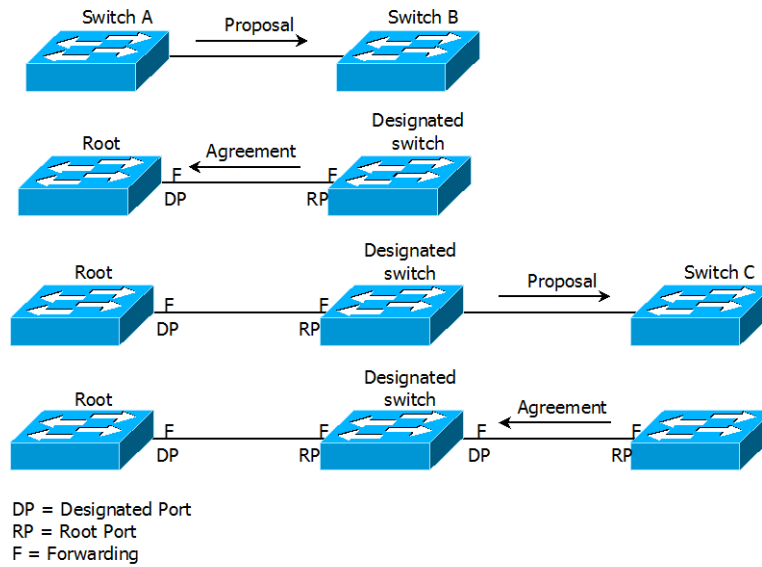
스위치 B 의 agreement 메시지를 수신한 후에, 스위치 A 는 자신의 designated 포트를

forwarding 상태로 천이한다. 스위치 B가 자신의 모든 non-edge port를 block 시키고, 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 포트로 선택하고, 두 스위치의 두 포트는 forwarding 상태로 천이한다. 협상 과정에서 하나 이상의 스위치가 active 형상에 참여한다. 네트워크의 복구에서 이런 proposal-agreement 협상은 spanning tree의 root에서 앞 방향으로 진행된다.

스witch는 포트의 duplex 모드로 link-type을 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 8-3. Proposal and Agreement Handshaking for Rapid Convergence



## 8.2.4. Bridge Protocol Data Unit Format and Processing

protocol version 필드의 값이 2로 설정되는 것을 제외하고 RSTP BPDU의 형식은 IEEE 802.1D BPDU 형식과 같다. 새로운 1 바이트 version 1 Length 필드는 0으로 설정된다; 이는 version 1 프로토콜 정보를 포함하지 않는다는 의미이다. 다음의 표는 RSTP flag 필드를 보여준다.

**표 8-4. 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 LAN의 designated 스위치로 제안하려는 스위치는 RSTP BPDU의 proposal flag를 설정해서 전송한다. proposal 메시지의 port role은 항상 designated 포트로 설정된다.

다른 스위치에 의한 제안을 받아들이는 스위치는 RSTP BPDU의 agreement flag를 설정해서 전송한다. agreement 메시지의 port role은 항상 root port로 설정된다.

RSTP는 독립적인 topology change notification (TCN) BPDU를 사용하지 않는다. topology change를 알리기 위해 RSTP BPDU flag의 topology change (TC) flag를 사용한다. 하지만 802.1D 스위치와의 연동을 위해 TCN BPDU를 생성하고 처리한다.

전송하는 포트의 상태에 따라 learning과 forwarding flag가 설정된다.

## 8.3. Configuring Spanning-Tree Features

이 절에서는 spanning-tree 를 설정하는 방법에 대해 설명한다.

### 8.3.1. Default STP Configuration

다음의 표는 STP 의 default 설정을 보여준다.

**표 8-5. Default STP Configuration**

Feature	Default Setting
Enable state	비활성 되어 있음.
Spanning-tree mode	STP
System priority	32768.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello time	2 초.
Forward-delay time	15 초.
Maximum-aging time	20 초.

### 8.3.2. STP Configuration Guidelines

U3000 Series 는 IEEE 802.1w RSTP 를 지원한다. 또한, 802.1w 는 802.1D STP 를 내부적으로 포함하므로 802.1D 와의 하위 호환성을 제공한다.

### 8.3.3. Enabling STP

default 로 STP 는 비활성 상태이다. 네트워크에 루프가 존재할 가능성이 있다면 STP 를 활성화 시키도록 한다.

VLAN 기반으로 STP 를 활성화시키려면 privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree vlan <i>vlan-id</i></b>	VLAN 별로 STP 를 활성화 한다. VLAN 의 범위는 1~4094 이다.
Step3	<b>end</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning-tree vlan <i>vlan-id</i></b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

STP 를 비활성 하려면, global configuration 명령 **no spanning-tree vlan *vlan-id*** 를 사용한다.

### 8.3.4. Disable per VLAN STP

U3000 Series 스위치는 VLAN 별로 spanning-tree 를 운영할 수 있다. 즉, VLAN trunk 포트의 각 VLAN 별로 STP state 를 설정하는 것이 가능하다. 만약 스위치에 32 개 이상의 VLAN 이 있다면, per VLAN STP 기능을 비활성 시키고, 전체 VLAN 을 제어하기 위한 하나의 spanning-tree instance 를 사용하도록 한다.



**Note**

Per VLAN STP 기능이 비활성된 상태에서 여러 VLAN 에 대해 STP 를 활성화시킨다면, VLAN trunk port 의 STP 상태는 안정적이지 않을 수 있다.

스위치의 per VLAN STP 기능을 비활성 시키려면, privileged EXEC 모드에서부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree one-for-all-vlans</b>	Per VLAN STP 기능을 비활성 시킨다.
Step3	<b>End</b>	privileged EXEC 모드로 변경한다.
Step4	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 per VLAN STP 기능을 활성화시키려면, global configuration 명령 **no spanning-tree one-for-all-vlans** 명령을 사용하라.

### 8.3.5. 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)를 할당할 수 있다. 모든 인터페이스가 같은 priority 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.

인터페이스의 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface interface-id</b>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	<b>spanning-tree vlan vlan-id port-priority priority</b>	인터페이스의 VLAN 포트 priority 를 설정한다. <ul style="list-style-type: none"> <li>• <i>vlan-id</i> 의 범위는 1~4094 이다.</li> <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>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show spanning-tree interface interface-id or show spanning-tree vlan vlan-id</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 vlan vlan-id port-priority** 를 사용한다.

### 8.3.6. 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.



**Note**

port group 일 경우 path cost 의 값을 인터페이스의 속도로부터 결정할 수 없다: 각각의 멤버 포트가 서로 다른 속도를 가질 수 있다. 따라서 port group 에 대해서는 수동으로 path cost 를 설정해서 사용하라.

인터페이스의 path cost 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<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 vlan</b> <i>vlan-id</i> <b>cost</b> <i>cost</i>	VLAN 의 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>vlan-id</i> 의 범위는 1~4094 이다. ● <i>cost</i> 의 범위는 1~200000000 이다. default 값은 인터페이스의 전송속도로부터 결정된다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show spanning-tree</b> <b>interface</b> <i>interface-id</i> or <b>show spanning-tree</b> <b>vlan</b> <i>vlan-id</i>	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 vlan *vlan-id* cost** 를 사용한다.

### 8.3.7. 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 vlan</b> <i>vlan-id</i> <b>priority</b> <i>priority</i>	VLAN 의 스위치 priority 를 설정한다. ● <i>vlan-id</i> 의 범위는 1~4094 이다. ● <i>priority</i> 의 범위는 0~61440 사이의 4096의 배수이다. default는 32768 이다. 낮은 수일수록 root 스위치로 선택될 가능성이 높다. 유효한 priority 값은 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344과 61440 이다. 다른 값들은 거부된다.
Step3	<b>end</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning-tree</b> <b>vlan</b> <i>vlan-id</i>	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 vlan vlan-id priority` 명령을 사용하라.

### 8.3.8. Configuring the Hello Time

hello time 을 변경함으로써 root 스위치가 전송하는 configuration BPDU 의 주기를 설정할 수 있다.

VLAN 의 hello time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<code>configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>spanning-tree vlan <i>vlan-id</i> hello-time <i>seconds</i></code>	VLAN 의 hello time 을 설정한다. hello time 은 root 스위치가 configuration 메시지를 전송하는 주기이다. 이 메시지는 스위치가 살아있음을 의미한다. • <i>vlan-id</i> 의 범위는 1~4094 이다. • <i>seconds</i> 의 범위는 1~10 이다. default 는 2 이다.
Step3	<code>end</code>	privileged EXEC 모드로 변경한다.
Step4	<code>show spanning-tree vlan <i>vlan-id</i></code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 `no spanning-tree vlan vlan-id hello-time` 명령을 사용하라.

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

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

	Command	Purpose
Step1	<code>configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i></code>	VLAN 의 forward time 을 설정한다. forward delay 는 포트가 spanning-tree 의 listening 혹은 learning 상태에서 forwarding 상태로 천이하기 위해 기다리는 시간이다. ● <i>vlan-id</i> 의 범위는 1~4094 이다. ● <i>seconds</i> 의 범위는 4~30 이다. default는 15 이다.
Step3	<code>end</code>	privileged EXEC 모드로 변경한다.
Step4	<code>show spanning-tree vlan <i>vlan-id</i></code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.



스위치의 default 설정으로 복구하려면, global configuration 명령 `no spanning-tree vlan vlan-id forward-time` 명령을 사용하라.

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

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

	Command	Purpose
Step1	<code>configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i></code>	VLAN 의 maximum-aging time 을 설정한다. maximum-aging time 은 스위치가 재구성을 하기 전에 spanning-tree 정보를 수신하지 않고 기다리는 최대 시간이다. <ul style="list-style-type: none"> <li>● <i>vlan-id</i> 의 범위는 1~4094 이다.</li> <li>● <i>seconds</i> 의 범위는 6~40 이다. default는 20 이다.</li> </ul>
Step3	<code>end</code>	privileged EXEC 모드로 변경한다.
Step4	<code>show spanning-tree vlan <i>vlan-id</i></code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 `no spanning-tree vlan vlan-id max-age` 명령을 사용하라.

### 8.3.11. Configuring the Port as Edge Port

U3000 Series 에서 STP 를 활성화시킬 경우, 단일 호스트와 연결된 포트에 대해서 edge port 로 설정한다. 만약 포트를 edge 포트로 설정하지 않으면, 그 포트는 forwarding 상태로 천이하는데 2 x Forward Time 이 소요된다.



**Note**

단말과 연결된 포트에 대해서는 반드시 edge port 로 설정해야 한다. 그렇지 않으면, 네트워크의 STP 형상에 변화가 발생할 때 단말이 연결된 포트의 STP 상태도 영향을 받게된다.

포트를 edge port 로 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<code>configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>Interface <i>interface-id</i></code>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	<code>spanning-tree admin-edge-port</code>	포트를 edge port로 설정한다.

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

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

### 8.3.12. Configuring the RSTP Mode

VLAN의 spanning-tree instance 별로 프로토콜 동작 모드를 설정할 수 있다. 일반적인 RSTP에서는 RSTP BPDU만을 사용해서 spanning-tree를 구성하고, 802.1D BPDU를 수신했을 경우에만 호환을 위해 802.1D BPDU를 사용한다. 하지만 STP 호환 모드에서는 RSTP BPDU를 사용하지 않고 오직 802.1D BPDU만을 사용한다. 또한 RSTP가 제공하는 빠른 복구 기능을 사용할 수 없게 된다.

STP의 프로토콜 모드를 변경하려면, privileged EXEC 모드에서부터 다음의 과정을 거친다.

	<b>Command</b>	<b>Purpose</b>
<b>Step1</b>	<b>configure terminal</b>	Global configuration 모드로 진입한다.
<b>Step2</b>	<b>spanning-tree vlan <i>vlan-id</i> force-version rstp</b>	특정 VLAN의 RSTP instance의 프로토콜 동작모드를 RSTP 모드로 설정한다. <i>vlan-id</i> 의 범위는 1~4094이다. default는 STP 모드이다.
<b>Step3</b>	<b>end</b>	privileged EXEC 모드로 변경한다.
<b>Step4</b>	<b>show running-config</b>	설정 내용을 확인한다.
<b>Step5</b>	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

default 설정으로 복구하려면, global configuration 명령 `no spanning-tree vlan vlan-id force-version` 명령을 사용한다.

### 8.3.13. Specifying the Link Type to Ensure Rapid Transitions

포트를 다른 포트와 point-to-point 링크로 연결한다면, 로컬 포트는 designated 포트가 된다.

기본적으로 link-type은 인터페이스의 duplex 모드에 의해 결정된다: full-duplex 포트는 point-to-point 연결로 간주되고; half-duplex 모드는 공유 연결로 간주된다. 물리적으로 point-to-point로 상대 스위치의 포트와 연결된 half-duplex 링크를 가지고 있다면, link-type의 default 설정을 변경함으로써 forwarding 상태로의 빠른 천이를 가능하게 할 수 있다.



**Note** port group 의 경우 duplex 모드로부터 링크의 종류를 판단할 수 없다: 각각의 멤버 포트가 서로 다른 duplex 모드를 가질 수 있다. 따라서 port group 에 대해서는 수동으로 링크 종류를 설정해서 사용하라.

default link-type 를 변경하려면, privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
<b>Step1</b>	<b>configure terminal</b>	Global configuration 모드로 진입한다.
<b>Step2</b>	<b>interface interface-id</b>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
<b>Step3</b>	<b>spanning-tree link-type point-to-point</b>	포트의 링크 종류를 point-to-point 로 설정한다.
<b>Step4</b>	<b>end</b>	privileged EXEC 모드로 변경한다.
<b>Step5</b>	<b>show running-config</b>	설정 내용을 확인한다.
<b>Step6</b>	<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.

### 8.3.14. Restarting the Protocol Migration Process

RSTP 를 지원하는 스위치는 802.1D STP 를 구동하는 스위치와의 연동이 가능하도록 protocol migration 메커니즘을 지원한다. 스위치가 Configuration BPDU(protocol version 이 0 으로 설정된 BPDU)를 수신한다면, 스위치는 그 포트에 오직 802.1D BPDU 만을 전송한다

스위치가 더 이상 802.1D BPDU 를 수신하지 않더라도 자동으로 RSTP 모드로 전환되지 않는다. 왜냐하면 네트워크에서 STP 스위치가 제거되었는지 혹은 802.1D 스위치가 더 이상 designated 스위치가 아닌지를 판단할 수 없기 때문이다. 그러므로 스위치는 여전히 802.1D BPDU 만을 사용하게 된다.

특정 스위치 포트에서 protocol migration 절차(이웃 스위치들과 협상을 시도함)를 시작하려면, interface configuration 명령 **spanning-tree mcheck** 를 사용한다.

## 8.4. Displaying the Spanning-Tree Status

spanning-tree 상태를 조회하려면, 다음 표에 명시된 privileged EXEC 명령 중 하나를 사용하라:

Command	Purpose
<code>show spanning-tree active</code>	활성 인터페이스의 spanning-tree 정보만을 출력한다.
<code>show spanning-tree interface <i>interface-id</i></code>	특정 인터페이스의 spanning-tree 정보를 출력한다.
<code>show spanning-tree summary</code>	포트 상태를 요약해서 보여준다.

privileged EXEC 명령 `show spanning-tree` 명령의 다른 키워드에 관한 정보는 `command reference`를 참고하라.

## 8.5. Self-loop Detection

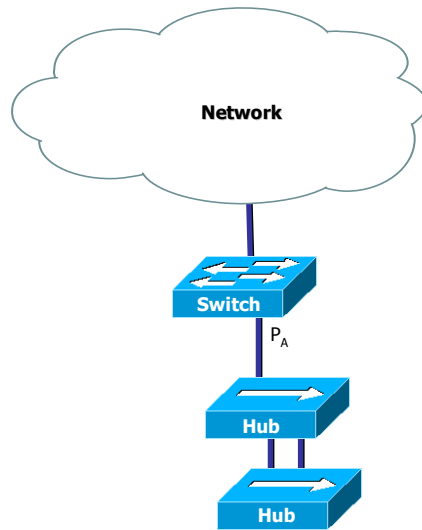
자신이 전송한 패킷이 되돌아 오는 현상을 감지하는 self-loop 감지 기능을 설정하는 방법을 설명한다.

### 8.5.1. 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 8-4. 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).

## 8.5.2. Configuring Self-loop Detection

이 절에서는 스위치에 self-loop 감지 기능을 설정하는 방법을 설명한다:

- Enabling Self-loop Detection
- Changing The Service Status of Port

### 8.5.2.1. 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, 단위로 0 부터 1440 까지 지정할 수 있으며 0 으로 설정하면 수동으로 no shutdown 하기 전까지

port 가 shutdown 상태로 있다.

Self-loop 감지 기능을 활성화 하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<i>Configure terminal</i>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-name</i>	Interface configuration 모드로 진입한다.
Step3a	<b>self-loop-detection</b>	Self-loop 감지 기능을 활성화 한다. Self loop 에 의해 shutdown 되면 5 minutes 후에 자동으로 no shutdown 한다.
Step3b	<b>self-loop-detection limit_time</b> <0-1440>	Self-loop 감지 기능을 활성화 한다. Self loop 에 의해 shutdown 되면 설정된 minutes 후에 자동으로 no shutdown 한다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5a	<b>show running-config</b>	설정 내용을 확인한다.
Step5b	<b>show self-loop-detection</b>	Self-loop 설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

다음은 포트 fa1 에 self-loop 감지 기능을 default limit time 으로 활성화 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# self-loop-detection
Switch(config-if-fa1)# end
Switch#
```

### 8.5.2.2. 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	<i>Configure terminal</i>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-name</i>	Interface configuration 모드로 진입한다.
Step3	<b>no shutdown</b>	포트를 서비스 가능 상태로 만든다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show port status</b>	포트의 상태정보를 확인한다.

### 8.5.2.3. 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	<code>Configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>interface interface-name</code>	Interface configuration 모드로 진입한다.
Step3a	<code>no self-loop-detection</code>	Self-loop 감지 기능을 비활성화 한다. Self loop 에 의해 shutdown 되면 5 minutes 후에 자동으로 no shutdown 한다.
Step4	<code>end</code>	privileged EXEC 모드로 변경한다.
Step5a	<code>show running-config</code>	설정 내용을 확인한다.
Step5b	<code>show self-loop-detection</code>	Self-loop 설정 내용을 확인한다.
Step6	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

다음은 포트 fa1 에 self-loop 감지 기능을 비 활성화 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# no self-loop-detection
Switch(config-if-fa1)# end
Switch#
```

### 8.5.3. 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)
- sld : self-loop-detection 설정 (set)
- link : link 의 상태 (up, down)
- shutdown : SLD 에 의한 shutdown (set)
- 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 fa5 에 SLD 가 default time 인 5 분으로 설정되어 있는 것을 보여준다. Port fa5 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 fa5
  self-loop-detection
!
interface vlan1
  ip address 100.1.1.1/24
!
Switch#
Switch# show self-loop-detection
-----
ifname sld link shutdown set_time remain_time count last-occur
-----
fa1 . down . . . 0 .
fa2 . up . . . 0 .
fa3 . down . . . 0 .
fa4 . down . . . 0 .
fa5 set up set 5 min . 1 May 29 04:48:39 2006
fa6 . down . . . 0 .
fa7 . down . . . 0 .
fa8 . down . . . 0 .
Switch#
```



## 9

# Stacking

이 장에서는 여러 대의 스위치를 하나의 IP 주소로 관리할 수 있는 Stacking 기능에 대해 설명한다.

이 장은 다음의 절들로 구성된다:

- Stacking Overview
- Configuring Stacking Features
- Displaying the Stacking Status

## 9.1. Stacking Overview

U3000 Series 스위치는 하나의 IP 주소로 여러 대의 스위치를 관리할 수 있다. 이 때, 관리 IP 주소를 가진 스위치를 *Master 스위치*, Master 스위치를 통해 관리되는 스위치 그룹내의 나머지 스위치들을 *Slave 스위치*라 칭한다.

U3000 Series 스위치는 Master 스위치와 Slave 스위치가 통신할 수 있는 공통의 VLAN 으로 연결만 되어 있으면, 네트워크 형상(Network topology)과 무관하게 stacking 될 수 있다. 이 때, Master 스위치와 Slave 스위치를 연결하는 VLAN 을 *Stack VLAN*이라 부른다.

## 9.2. Configuring Stacking Feature

이 절에서는 Stacking 을 설정하는 방법을 설명한다:

- Configuring the Stack VLAN
- Configuring the Stack Member
- Enabling the Stack

- Connecting to Slave Switch

## 9.2.1. Configuring the Stack VLAN

Stacking 을 하려면 Master 스위치와 Slave 스위치가 통신할 수 있는 공통의 VLAN, Stack VLAN 을 설정해야 한다.



**Note** 일반 트래픽과 Stacking 트래픽의 분리를 위해 VLAN 을 분리할 것을 권장한다. 즉, 별도의 Trunk VLAN 을 생성해서 Stack VLAN 으로 지정하라.

Stack VLAN 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>stack vlan <i>vlan-id</i></b>	Stack VLAN 을 설정한다. <i>vlan-id</i> 의 범위는 1~4094 이다. default 는 VLAN 1 이다.
Step3	<b>end</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

Stack VLAN의 default 설정으로 복구하려면, global configuration 명령 **no stack vlan** 을 사용한다.

## 9.2.2. Configuring the Stack Member

Master 스위치에서 관리할 Slave 스위치들을 Master 스위치에 등록해주어야 한다.



**Note** 이 명령은 Master 스위치에서만 의미를 가지며, Slave 스위치에서는 설정하더라도 동작에 영향을 미치지 않는다. 등록하는 스위치는 Master 스위치와 같은 VLAN(Stack VLAN)에 존재해야 한다.

Slave 스위치를 등록하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>stack member <i>node-id mac-address</i></b>	Slave 스위치를 등록한다. <ul style="list-style-type: none"> <li>● <i>node-id</i> 의 범위는 2~5 이다.</li> <li>● <i>mac-address</i> 는 AABB.CCDD.EEFF 형식이다.</li> </ul>

<b>Step3</b>	<b>end</b>	privileged EXEC 모드로 변경한다.
<b>Step4</b>	<b>show running-config</b>	설정 내용을 확인한다.
<b>Step6</b>	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

등록된 스위치를 삭제하려면, global configuration 명령 **no stack member** 를 사용한다.

### 9.2.3. Enabling the Stack

스위치는 Master 스위치 혹은 Slave 스위치로 Stack 기능이 활성화 된다.

스위치의 Stack 기능을 활성화 하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	<b>Command</b>	<b>Purpose</b>
<b>Step1</b>	<b>configure terminal</b>	Global configuration 모드로 진입한다.
<b>Step2</b>	<b>stack role {master slave}</b>	스위치의 Stack 기능을 활성화한다. <ul style="list-style-type: none"> <li>● <b>master</b> - Master 스위치로 동작한다.</li> <li>● <b>slave</b> - Slave 스위치로 동작한다.</li> </ul>
<b>Step3</b>	<b>end</b>	privileged EXEC 모드로 변경한다.
<b>Step4</b>	<b>show running-config</b>	설정 내용을 확인한다.
<b>Step6</b>	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

Stack 기능을 해제하려면, global configuration 명령 **no stack role** 을 사용한다.

## 9.2.4. Connecting to Slave Switch

Master 스위치와 Slave 스위치가 성공적으로 stacking 되었다면, Master 스위치를 통해 Slave 스위치에 접속할 수 있다. U3000 Series 스위치는 Slave 스위치의 shell 을 사용할 수 있는 방법을 제공한다.



**Note** 이 명령은 Master 스위치에서만 동작한다

스위치의 Stack 기능을 활성화 하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
<b>Step1</b>	<code>rcommand node-id</code>	Master 스위치에서 Slave 스위치에 접속한다. <i>node-id</i> 의 범위는 2~5 이다.

## 9.3. Displaying the Stacking Status

Stack 상태를 조회하려면, 다음 표에 명시된 privileged EXEC 명령을 사용하라:

Command	Purpose
show stack	stack 상태 정보를 출력한다

다음은 Master 스위치에서의 **show stack** 명령에 대한 출력 결과이다:

```
Switch# show stack
```

Node	Mac address	Status	Platform	VLAN
1	0007.7000.100a	active	U3024	10
2	0007.7000.100c	active	U3024	10

다음은 Slave 스위치에서의 **show stack** 명령에 대한 출력 결과이다:

```
Switch# show stack
```

```
Stacking VLAN : 10
Node ID       : 2
Master switch : U3024(0007.7000.100a) on VLAN 10
```

# 10

## 통계 모니터링 및 Qos

본 장은 현재 운영중인 U3000 Series 스위치의 상태를 파악하고, 로그의 정보를 화면에 표시하고, RMON(Remote Monitoring)을 통한 운영 관리 기능에 대하여 설명한다.

또한 U3000 Series 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 한다. 만일 주기적으로 통계 데이터를 관리한다면, 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있다.

### 10.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. U3000 Series 스위치는 show 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공한다.

표 10-1. 상태 모니터링 명령어

명령어	설명
show log	<ul style="list-style-type: none"> <li>■ 시스템이 현재 관리하고 있는 로그를 보여 준다.</li> <li>■ 최대 500 개까지의 로그를 저장할 수 있다.</li> </ul>
show memory usage	<ul style="list-style-type: none"> <li>■ 현재 시스템의 메모리 사용 상태를 보여 준다.</li> </ul>
show cpu usage	<ul style="list-style-type: none"> <li>■ 현재 CPU 점유율을 보여 준다.</li> </ul>
show version	<ul style="list-style-type: none"> <li>■ 스위치의 HW 와 SW 의 버전 정보를 보여 준다.</li> </ul>

## 10.2. 포트 통계

U3000 Series 스위치는 포트의 통계 정보를 제공한다. 포트의 통계 정보는 시스템의 현재 운용 중인 모듈의 각 포트의 현재 카운터 값을 보여준다.

포트 통계를 보기 위해서는 다음의 명령을 사용한다.

```
show interface [interface name]
```

U3000 Series 스위치는 운용자에게 다음의 포트 통계 정보를 제공한다.

- **Link Status** – 링크의 현재 상태
- **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.

Show interface 명령을 사용하면 다음과 같이 다양한 통계 데이터를 확인할 수 있다.

---

```
Switch# show interface
fa1 is down
type 100Base-TX
ifindex 0(k2) BROADCAST multicast
auto-negotiation
speed set auto
duplex set full
```

---

```

Last clearing of counters 17:31:00
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 oversized, 0 dropped
  0 packets output, 0 bytes
  Sent 0 broadcasts, 0 multicasts
    
```

```

fa2 is down
type 100Base-TX
ifindex 1(k3) BROADCAST multicast
auto-negotiation
speed set auto
duplex set full
    
```

```

Last clearing of counters 17:31:00
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 oversized, 0 dropped
  0 packets output, 0 bytes
    
```

--More--

**표 10-2. 포트 통계조회 조회 명령**

명령어	설명	모드
<b>show port counter</b>	시스템의 모든 인터페이스의 In/Out packet의 누적치를 보여준다.	Interface
<b>Show port statistics IFNAME</b>	해당 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx의 bit/s, bytes/s, pkts/s를 보여준다.	Config

다음은 **show port counter**를 이용하여 전체 포트의 패킷 누적치와 특정 인터페이스(**fa1/1**)의 5 초, 1 분, 5 분 통계치를 보여준다.

```
Switch# show port counter
```

```

ifname I-Kbps O-Kbps  InOctets  InUpkt  InNUpkt  OutOctets  OutUpkt  OutNUpkt
-----
fa1      0      0      0      0      0      0      0      0
fa2      0      0      0      0      0      0      0      0
fa3      0      0      0      0      0      0      0      0
fa4      0      0      0      0      0      0      0      0
fa5      0      0      0      0      0      0      0      0
fa6      0      0      0      0      0      0      0      0
fa7      0      0      0      0      0      0      0      0
    
```



---

fa8	0	0	0	0	0	0	0	0
fa9	0	0	0	0	0	0	0	0
fa10	0	0	0	0	0	0	0	0
fa11	0	0	0	0	0	0	0	0
fa12	0	0	0	0	0	0	0	0
fa13	0	0	0	0	0	0	0	0
fa14	0	0	0	0	0	0	0	0
fa15	0	0	0	0	0	0	0	0
fa16	0	0	0	0	0	0	0	0
fa17	0	0	0	0	0	0	0	0
fa18	0	0	0	0	0	0	0	0
fa19	0	0	0	0	0	0	0	0
fa20	0	0	0	0	0	0	0	0
fa21	0	0	0	0	0	0	0	0
fa22	0	0	0	0	0	0	0	0
fa23	0	224	2266323	11646	120	1779661246	19781	1528642
fa24	224	0	1779736598	20000	1528693	2279097	11857	120
fa25	0	0	0	0	0	0	0	0
fa26	0	0	0	0	0	0	0	0

Switch#

Switch#

Switch# **show port statistics fa24**

Last clearing of counters 17:31:45

---

	RX				TX		
	bits/s	bytes/s	pkts/s		bits/s	bytes/s	pkts/s
5sec :	222656	27832	23		0	0	0
1min :	223912	27989	23		40	5	0
5min :	222840	27855	23		80	10	0

Switch#

---

또한 다음의 명령을 사용하여 **show interface** 시 보여주는 통계에 대한 설정을 바꾸거나 해당 인터페이스의 특정 기간의 **High/Low threshold** 값을 설정하여 **log** 로 남길수 있다.

표 10-3. 포트 통계조회 설정 명령

명령어	설명	모드
<b>load interval</b> <5-100>	Show interface 시 보여주는 평균값의 기간을 셋팅한다.	interface
<b>no load interval</b>	Show interface 시 보여주는 평균값의 기간을 디폴트값으로 변경한다.(60 초)	interface
<b>input-load-monitor</b> <5-100> <1-1000> <1-1000>	해당 인터페이스의 특정 기간 동안의 low/high threash 설정 하여 syslog, snmp trap 을 통해 보고한다.	interface
<b>no input-load-monitor</b>	Input-load-monitor 를 해제한다.	interface

다음 명령은 통계치에 대한 누적치를 초기화시키는 명령어이다.

표 10-4. 포트 통계 초기화 명령

명령어	설명	모드
<b>clear counters</b>	시스템의 모든 인터페이스의 통계누적치를 초기화한다.	privileged
<b>clear counters</b> IFNAME	특정 인터페이스의 통계누적치를 초기화한다.	privileged
<b>clear counters snmp</b>	시스템의 모든 인터페이스의 snmp 를 위한 통계누적치를 초기화한다.	privileged

## 10.3. CPU 트래픽 통계

U3000 series 스위치는 cpu 로 인입되는 패킷에 대한 통계를 보여 준다.

표 10-5. CPU 트래픽 통계 초기화 명령

명령어	설명	모드
<b>show cpu-packet-counter ( all   ip_icmp   tcp   udp )</b>	Cpu 로 인입되는 패킷 들에 대한 통계를 보여준다.	privileged

예제

```
Switch# show cpu-packet-counter all
Ip:
  15368 total packets received
  0 forwarded
  0 incoming packets discarded
  15181 incoming packets delivered
  15103 requests sent out
Icmp:
  3 ICMP messages received
  0 input ICMP message failed.
ICMP input histogram:
  echo requests: 3
  3 ICMP messages sent
  0 ICMP messages failed
```

---

ICMP output histogram:

echo replies: 3

Tcp:

0 active connections openings  
 1 passive connection openings  
 0 failed connection attempts  
 0 connection resets received  
 1 connections established  
 2158 segments received  
 2075 segments send out  
 10 segments retransmited  
 0 bad segments received.  
 1 resets sent

Udp:

13012 packets received  
 0 packets to unknown port received.  
 0 packet receive errors  
 13025 packets sent

TcpExt:

1 invalid SYN cookies received  
 ArpFilter: 0  
 2 delayed acks sent  
 1 packets directly queued to recvmsg prequeue.  
 3 packets directly received from prequeue  
 19 packets header predicted  
 1 packets header predicted and directly queued to user  
 TCPPureAcks: 4  
 TCPHPAcks: 2047  
 TCPRecovery: 0  
 TCPSackRecovery: 0  
 TCPSACKReneging: 0  
 TCPFACKReorder: 0  
 TCPSACKReorder: 0  
 TCPReorder: 0  
 TCPTSReorder: 0  
 TCPFullUndo: 0  
 TCPPartialUndo: 0  
 TCPDSACKUndo: 0  
 TCPLossUndo: 0  
 TCPLoss: 0  
 TCPLostRetransmit: 0  
 TCPRecoveryFailures: 0  
 TCPSackFailures: 0  
 TCPLossFailures: 0  
 TCPFastRetrans: 0  
 TCPForwardRetrans: 0  
 TCPSlowStartRetrans: 0  
 TCPTimeouts: 2  
 TCPRecoveryFail: 0  
 TCPSackRecoveryFail: 0  
 TCPSchedulerFailed: 0  
 TCPRcvCollapsed: 0

---

---

```

TCPDSACKOldSent: 0
TCPDSACKOfoSent: 0
TCPDSACKRecv: 2
TCPDSACKOfoRecv: 0
TCPAbortOnSyn: 0
TCPAbortOnData: 0
TCPAbortOnClose: 0
TCPAbortOnMemory: 0
    
```

---

## 10.4. Logging

U3000 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.

U3000 series 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI 를 사용하여 로깅되는 시스템 메시지를 제어할 수 있다. 최대 500 개의 로그 메시지를 시스템 버퍼에 저장한다. 시스템 운영자는 시스템 메시지를 Telnet 이나 콘솔을 통해서, 또는 Syslog server 의 로그를 봄으로써 원격으로 모니터 할 수 있다.

U3000 series 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

**표 10-6. U3000 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.

## 10.4.1. 시스템 로그 메시지 내용

U3000 series 스위치의 시스템 로그 메시지는 다음과 같은 내용을 제공한다.

- ✓ **Timestamp**
  - Timestamp 는 이벤트가 발생한 월, 날짜, 연도 및 구체적인 시간 정보를 HH:MM:SS MM/DD/YYYY 과 같이 기록한다.
- ✓ **Severity level**
  - <표 1>에서 정의한 U3000 스위치의 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
```

## 10.4.2. 디폴트 Logging 설정 값.

표 10-7. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	enabled
Telnet 세션으로의 로깅 출력	disabled.
로깅 버퍼 사이즈	250kb
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 10-8. 시스템 메시지 로깅 환경 설정 명령

명령어	설명
logging console {enable disable level}	<ul style="list-style-type: none"> <li>콘솔로의 로깅 출력 여부 및 환경 설정.</li> </ul>
logging facility {auth cron daemon kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp}	<ul style="list-style-type: none"> <li>syslog 메시지를 보낼 Facility parameter 를 설정.</li> </ul>
logging flash {enable disable level size}	<ul style="list-style-type: none"> <li>syslog 메시지를 flash 에 저장할지의 여부 설정 및 환경 설정.</li> </ul>
logging server A.B.C.D	<ul style="list-style-type: none"> <li>syslog 메시지를 외부 syslog 서버에 보낼지 설정</li> </ul>
logging session {enable disable level }	<ul style="list-style-type: none"> <li>현 세션으로의 로깅 출력 여부 설정.</li> </ul>
logging source-ip A.B.C.D	<ul style="list-style-type: none"> <li>syslog packet 의 source ip 를 설정</li> </ul>
logging trap {<0-7> alert crit debug emerg err info notice warn}	<ul style="list-style-type: none"> <li>syslog server 의 logging level 설정</li> </ul>

---

```
show log
```

- 로깅 버퍼 출력 및 로깅 설정 확인.

```
{<0-7>|back|flash }
```

```
logging console {enable|disable}
```

- 콘솔로의 로깅 출력 여부 설정.
- 

## 10.5. RMON(Remote MONitoring)

시스템 운영자는 U3000 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다.

다음 절에서는 RMON 개념 및 U3000 Series 스위치가 지원하는 RMON 서비스 기능에 대하여 자세히 설명한다.

### 10.5.1. 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 요소로 구성된다.

- **RMON probe**

- 원격으로 제어되면서 지속적으로 LAN 세그먼트 또는 VLAN의 통계 정보를 수집하는 지능형 디바이스 또는 소프트웨어 agent
- 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

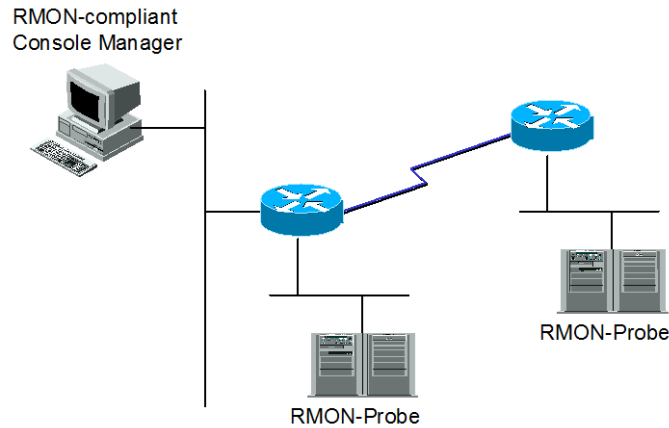


그림 10-1. RMON Manager 와 RMON Probe

기존의 SNMP MIBs 가 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 임계치를 설정, 이에 도달하면 자동으로 알려주는 경보 기능 및 사건 발생 기능을 보유하고 있어야 한다.

U3000 Series 스위치에서는 <오류! 참조 원본을 찾을 수 없습니다.>에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON 은 디폴트로 모든 설정이 disabled 이다.

표 10-9. 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, jabber, 길이 미달, 길이 초과)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 1-3.600 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> </ul>



	<ul style="list-style-type: none"> <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 호스트를 찾는다.</li> <li>■ 관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 얻을 수 있다.</li> </ul>
트래픽 매트릭스	<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 알 수 있다.</li> <li>■ 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없다.</li> </ul>
필터	<ul style="list-style-type: none"> <li>■ 관리자가 특정한 패킷의 동향을 감시하기 위해서 이용한다.</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 보낸다. 트랩 발생 및 기록보관은 선택적이다.</li> </ul>

## 10.5.2. RMON의 Alarm 과 Event 그룹 설정.

사용자는 CLI 또는 SNMP Manager 에 의해서 RMON 의 Configuration 을 설정할 수 있다. 이는 Privileged 모드에서 설정되며, 명령어는 다음과 같다.

표 10-10. RMON Alarm and Event 설정 명령

명령어	설명	모드
<pre>rmon alarm index ifEntry variable ifIndex interval {delta absolute} rising- threshold value [event- number] falling-threshold value [event-number] [owner string]</pre>	<ul style="list-style-type: none"> <li>■ RMON 의 Alarm Table 에 Alarm 을 추가</li> <li>■ Index : 1 부터 65535 의 정수 값.</li> <li>■ Variable 은 MIB object</li> <li>■ interval 은 alarm variable 을 관찰한 시간 간격으로 초 단위</li> <li>■ delta 는 MIB variable 값의 샘플간의 값의 차이를 관찰함을 말하며, absolute 는 MIB</li> </ul>	Config

	variable의 절대값을 말한다.	
	<ul style="list-style-type: none"> <li>rising-threshold와 falling-threshold의 값을 각각 설정한다.</li> <li>event의 설정은 option이며, alarm variable의 delta 값이나 absolute 값이 rising-threshold나, falling threshold 값에 도달했을 때 각각 해당 Event가 발생한다.</li> <li>Alarm의 owner를 명시할 수 있다.</li> </ul>	
rmon event <i>index</i> [log] [trap community <i>string</i> ] [owner <i>string</i> ] [description <i>string</i> ]	<ul style="list-style-type: none"> <li>RMON Event table에 Event를 추가한다.</li> <li>log는 event가 발생했을 때, RMON log를 생성할 것인지를 명시한다. Trap은 Event가 발생했을 때, trap을 보낼 것인지를 명시한다.</li> </ul>	Config
no rmon alarm <i>alarm-index</i>	RMON Alarm table에서 alarm을 삭제한다.	Config
no rmon event <i>event-index</i>	RMON Event Table에서 event를 삭제한다.	Config
show rmon alarm	RMON alarm table을 보여준다.	Privileged
show rmon event	RMON event table을 보여준다.	Privileged
show rmon log	RMON log table을 보여준다.	Privileged

```
Switch# configure terminal
Switch(config)# rmon alarm 10 ifEntry inErrors 1 20 delta rising-threshold 15 1
falling-threshold 0 owner mijiook
Switch(config)# rmon event 1 log trap community rmonTrap owner mijiook
description "Noti : Too Much InErrors"
Switch(config)# exit
Switch# show rmon alarm
```

-----  
Alarm Configurations  
-----

```
The index of alarm      : 10
The interval            : 20
The type of Packets     : inErrors
The interface           : fa1
The type of Sample      : deltaValue
alarmValue              : 0
The status of starting: RISING_FALLING_ALARM
alarmRisingThreshold    : 15
alarmFallingThreshold   : 0
alarmRisingEventIndex   : 1
alarmFallingEventIndex  : 1
alarmOwner               : mijiook
```

```
Switch# show rmon event
-----
```

---

Event Configurations

---

```

-----
The Index of event : 1
eventDescription : "Noti:TooMuchInErrors"
eventType : log and trap
Community : rmonTrap
eventOwner : mijiok
Switch#

```

---

**표 10-11. RMON Statistics And History 설정 명령**

명령어	설명	모드
<code>rmon history index ifEntry ifIndex [buckets bucket-number] [interval seconds] [owner string]</code>	<ul style="list-style-type: none"> <li>명시된 bucket 의 수와 interval 간격으로 이력을 수집</li> <li>index 값은 1 부터 65535 까지 할당할 수 있다.</li> <li>Bucket 의 default 개수는 50</li> </ul>	Config
<code>no rmon history index ifEntry ifindex</code>	<ul style="list-style-type: none"> <li>History 수집을 Disable 시킨다..</li> </ul>	Config
<code>show rmon history</code>	<ul style="list-style-type: none"> <li>RMON history table 을 보여준다.</li> </ul>	Privileged
<code>show rmon statistics</code>	<ul style="list-style-type: none"> <li>RMON statistics table 을 보여준다.</li> </ul>	Privileged

---

Switch# **show rmon statistics**

---

SHOW STATISTICS

---

```

-----
The Index of stats : 1
Interface : fa1
Drop Events : 0
Total Octets : 0
Total Packets : 0
Broadcst Packets : 0
Multicast Packets : 0
CRC errors : 0
Under Size Packets : 0
Over Size Packets : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts 64 Octets : 0
Pkts 65 to 127 Oct : 0
Pkts 128 to 255 Oct : 0
Pkts 256 to 511 Oct : 0
Pkts 512 to 1023 Oct : 0

```

---

---

```
Pkts 1024 to 1518 Oct: 0
Owner                : locus
```

```
The Index of stats   : 2
Interface            : fa2
Drop Events          : 0
Total Octets         : 0
Total Packets        : 0
```

```
.....
Switch#
```

---

```
Switch# configure terminal
Switch#(config)# rmon history 1 ifEntry 1 buckets 20 interval 10 owner mijiok
Switch#(config)# exit
Switch# show rmon history
```

```
-----
                SHOW HISTORY
-----
```

```
===== fa1 =====
Control-index       : 1
ifindex             : 1
interval            : 10
buckets             : 20
owner               : hong
```

```
--- fa1 : bucket 1 ---
DropEvents          : 0
Octets              : 0
Pkts                : 0
BroadcastPkts       : 0
MulticastPkts       : 0
CRCAlignErrors      : 0
UndersizePkts       : 0
OversizePkts        : 0
Fragments           : 0
Jabbers             : 0
Collisions           : 0
Utilization         : 0
```

```
--- fa1 : bucket 2 ---
DropEvents          : 0
Octets              : 0
Pkts                : 0
BroadcastPkts       : 0
MulticastPkts       : 0
CRCAlignErrors      : 0
UndersizePkts       : 0
OversizePkts        : 0
Fragments           : 0
Jabbers             : 0
```

---

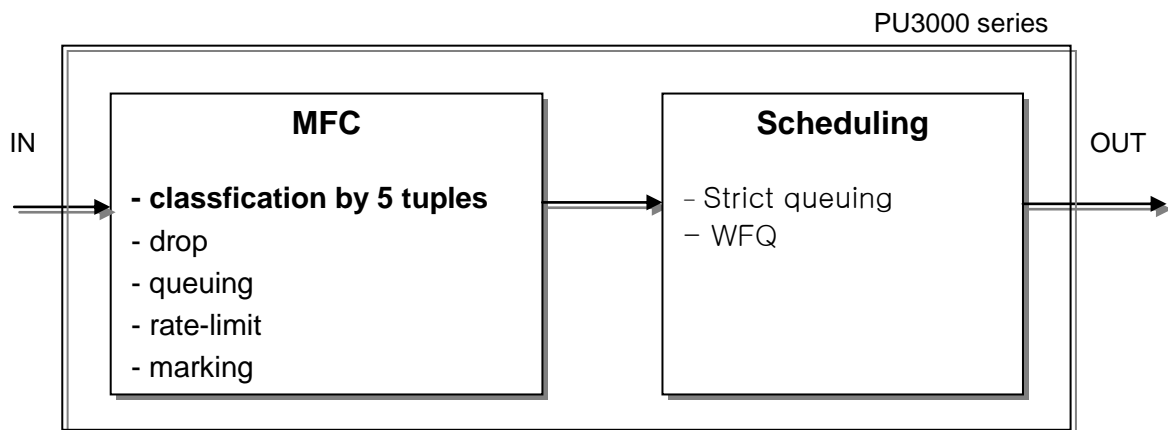
---

```
Collisions      : 0
Utilization     : 0
```

```
--- fa1 : bucket 3 ---
DropEvents     : 0
Octets         : 0
Pkts          : 0
BroadcastPkts : 0
MulticastPkts : 0
CRCAlignErrors : 0
```

---

## 10.6. Qos 및 Packet Filtering



본 U3000 Series 스위치에서는 Qos 와 Packet filtering 을 위해 다음과 같은 기능을 수행을 한다.

- **MFC(Multi-Field Classifier)**

프로토콜, src/dest IP, UDP/TCP Port 등의 지정된값에 의해 다양하게 classification 하여 flow-rule 을 결정한후 drop, queuing, rate-limit, marking 등의 특정 정책(action)을 수행할 수 있다. 또한 이를 이용하여 다양하게 filtering 기능을 수행하는데 이용되기도 한다.

- **Scheduling**

트래픽이 과부하가 일어났을 경우 이를 위한 처리 방식으로 Scheduling 알고리즘을 이용하여 트래픽의 조건에 따라 처리순서를 다르게 하는 방식이다.

- **Strict Queuing Method**

이 알고리즘은 중요한 데이터를 가장 빨리 처리하려고 할 때 사용된다. 모든 데이터를 우선 순위대로 처리하여 우선 순위가 높은 데이터를 빨리 처리되지만 우선도가 낮은 데이터는 처리 순서가 밀린다. 만약 대역폭 전체가 우선 순위 높은 데이터로 채워지면 낮은 우선순위의 트래픽은 전혀 통과하지 못하고 대기 상태에 놓이는 단점을 지니고 있는 방식이다.

**- WRR(Weighted Round Robin Method)**

일정 비율을 기반으로 데이터를 처리하는 방식으로 SPQ 방식의 단점을 보완할수 있는 알고리즘으로서 사용자가 자신의 환경에 맞게 설정한 큐에 지정된 비율에 따라 데이터를 처리한다..

**- WFQ(Weighted Fair Queuing Method)**

일정 비율을 기반으로 데이터를 처리하는 방식으로 SPQ 방식의 단점을 보완할수 있는 알고리즘으로서 큐에 일정한 크기의 처리율을 사용자가 자신의 환경에 맞게 설정할 수 있다.

**10.6.1. MFC(Multi-Field Classifier)**

**10.6.1.1. Flow-Rule 생성/삭제/모드설정**

패킷을 처리하는 정책을 설정하기 위해 적용할 대상이되는 규칙을 설정하여야 하는데, 먼저 이를 위한 flow-rule 을 생성해야 한다. 또한, 이를 위한 적당한 profile-mode 를 설정하여야 한다. L2 모드에서는 Mac/vlan/cos/ethertype/ipaddr/protocol 를 이용해서 classification 을 수행하며, I3 모드에서는 Ipaddr/protocol/dscp/tos/I4port/tcp-control 를 이용해서 classification 을 수행한다. Address 모드는 mac / ip addr / I4 port / protocol 를 이용해서 classification 을 수행한다.

표 10-12. Flow-rule 생성/삭제/모드설정 명령

명령어	설명	모드
flow-rule NAME	해당 flow-rule 생성	Config
no flow-rule NAME	해당 flow-rule 삭제	Config
flow-rule NAME pofile-mode I2	Mac/vlan/cos/ethertype/ipaddr/protocol 를 보는 I2 프로파일 사용	Config
flow-rule NAME pofile-mode I3	Ipaddr/protocol/dscp/tos/I4port/tcp-control 을 보는 I3 프로파일 사용(디폴트)	Config
flow-rule NAME pofile-mode adress	Mac / ip / I4 port / protocol 을 보는 모드	Config

**10.6.1.2. Flow-Rule 설정/해제**

패킷을 처리하는 정책을 설정하기 위해 적용할 대상이되는 규칙을 설정하여야 하는데 이는 Flow-rule 을 classification 설정으로 가능하다. Flow-rule 은 src/dest mac, vlan, cos, ethertype, 프로토콜, src/dest IP, UDP/TCP Port, dscp, tos, Tcp sync 등의 지정된 값에 의해 다양하게 classification 할수 있다.

표 10-13. Flow-rule Classification 명령

명령어	설명	모드
<b>flow-rule</b> NAME classify mac {H.H.H any} {H.H.H any}	Mac 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify mac mask H.H.H H.H.H mask H.H.H H.H.H	Mac mask 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify vlan <1-4094>	Vlan 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify cos <0-7>	Cos 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify ethetype WORD	Ethertype 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify ipaddr {A.B.C.D/M any} {A.B.C.D/M any}	IP address 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify protocol {<0-255> icmp igmp ip ospf pim tcp udp}	Protocol 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify dscp <0-63>	DSCP 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify tos <0-7>	Tos 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify l4port <0-65535> any {<0-65535> any}	L4 port number 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify l4port mask XXXX XXXX mask XXXX XXXX	L4 port mask 을 이용한 classification 설정	Config
<b>flow-rule</b> NAME classify tcp-control VALUE MASK	Tcp control flag 를 이용한 classification 설정	Config
<b>no flow-rule</b> NAME classify mac	Mac 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify vlan	Vlan 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify cos	Cos 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify ethetype	Ethertype 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify ipaddr	IP address 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify protocol	Protocol 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify dscp	DSCP 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify tos	Tos 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify l4port	L4 port numbe 을 이용한 classification 해제	Config
<b>no flow-rule</b> NAME classify tcp-control	Tcp control fla 를 이용한 classification 해제	Config



**Notice** Profile-mode 에 해당하지 않는 classification 무시한다.



**Notice** Flow-rule 을 생성만 하고 아무런 추가적인 classification 을 설정하지 않은 경우는 '모든 패킷' 을 의미한다.



**Notice** Marking dscp , marking tos , cos-to-tos 는 동시에 적용되지 않으며, 동시 설정시 dscp , tos , cos-to-tos 의 우선순위로 한가지만 설정된다.

각 조건에 의해 Classification 된 Flow-Rule 에 특정 정책(action)을 적용시킬 수가 있다.  
Qos 를 위해 Cos, Queue 필드를 marking 할수도 있으며, rate-limit 등의 정책을 적용할수도 있다.

표 10-14. Flow-rule 정책 적용 명령

명령어	설명	모드
<b>flow-rule NAME match drop</b>	규칙과 일치하는 패킷을 불허한다.	Config
<b>flow-rule NAME match queuing &lt;0-7&gt;</b>	규칙과 일치하는 패킷을 지정된 우선순위의 Queue 에 할당한다.	Config
<b>flow-rule NAME match marking cos &lt;0-7&gt;</b>	규칙과 일치하는 패킷의 해당값을 할당된 Cos 값으로 패킷에 marking 한다.	Config
<b>flow-rule NAME match marking dscp &lt;0-63&gt;</b>	규칙과 일치하는 패킷의 해당값을 할당된 dscp 값으로 패킷에 marking 한다.	Config
<b>flow-rule NAME match marking tos &lt;0-7&gt;</b>	규칙과 일치하는 패킷의 해당값을 할당된 tos 값으로 패킷에 marking 한다.	Config
<b>flow-rule NAME match cos-to-tos</b>	규칙과 일치하는 패킷의 tos 값을 패킷의 cos 값을 참조하여 패킷에 marking 한다.	Config
<b>flow-rule NAME match tos-to-cos</b>	규칙과 일치하는 패킷의 cos 값을 패킷의 tos 값을 참조하여 패킷에 marking 한다.	Config
<b>flow-rule NAME match mirror</b>	규칙과 일치하는 패킷을 지정된 mirror 포트에 복사한다.	Config
<b>flow-rule NAME match replace-vlan &lt;1-4094&gt;</b>	규칙과 일치하는 패킷의 vlan 값을 지정된 값으로 패킷에 marking 한다.	Config
<b>flow-rule NAME match redirect {all unicast not-unicast} INTERFACE { tag   untag }</b>	규칙과 일치하는 패킷을 지정된 INTERFACE 로 redirect 한다.	Config
<b>flow-rule NAME match trap-cpu</b>	규칙과 일치하는 패킷을 CPU 로 트랩시킨다.	Config
<b>flow-rule NAME match control-cpu-trap</b>	규칙과 일치하는 패킷을 CPU 에 high priority 로 트랩시키며, 동시에 drop 시킨다.	Config
<b>flow-rule NAME match drop-precedence</b>	규칙과 일치하는 패킷에 drop-precedence 를 부여한다.	Config
<b>flow-rule NAME match metering</b>	규칙과 일치하는 패킷을 카운팅한다.	Config
<b>flow-rule NAME match rate-limit &lt;64-1048576&gt;</b>	규칙과 일치하는 패킷에 rate-limit 를 적용한다.	Config
<b>no flow-rule NAME match drop</b>	규칙과 일치하는 패킷을 불허를 취소한다.	Config
<b>no flow-rule NAME match queuing</b>	규칙과 일치하는 패킷의 queuing 을 취소한다.	Config
<b>no flow-rule NAME match marking cos</b>	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
<b>no flow-rule NAME match marking dscp</b>	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
<b>no flow-rule NAME match marking tos</b>	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
<b>no flow-rule NAME match cos-to-tos</b>	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
<b>no flow-rule NAME match tos-to-cos</b>	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
<b>no flow-rule NAME match mirror</b>	규칙과 일치하는 패킷의 mirror 를 취소한다.	Config
<b>no flow-rule NAME match replace-vlan</b>	규칙과 일치하는 패킷의 replace-vlan 을 취소한다.	Config
<b>no flow-rule NAME match redirect</b>	규칙과 일치하는 패킷의 redirect 를 취소한다.	Config



<b>no flow-rule NAME match trap-cpu</b>	규칙과 일치하는 패킷의 trap-cpu 를 취소한다.	Config
<b>no flow-rule NAME match control-cpu-trap</b>	규칙과 일치하는 패킷의 trap-cpu 를 취소한다.	Config
<b>no flow-rule NAME match drop-precedence</b>	규칙과 일치하는 패킷의 drop-precedence 를 취소한다.	Config
<b>no flow-rule NAME match metering</b>	규칙과 일치하는 패킷의 metering 를 취소한다.	Config
<b>no flow-rule NAME match rate-limit</b>	규칙과 일치하는 패킷의 rate-limit 를 취소한다.	Config



**Notice**

위의 모든 정책은 flow-rule 에 여러 개를 동시에 적용이 가능하지만, action 에 따라서 동시에 적용되지 않을수 있다. 예를 들면 queuing 과 marking cos 는 동시에 적용이 가능하지만, drop 과 queuing 은 한가지로만 동작한다. Action 의 우선 순위는 Broadcom 칩셋을 따른다.



**Notice**

control-cpu-trap 은 해당 패킷을 cpu 의 high-priority 로 trap 하면서, 동시에 drop 을 수행한다. Igmp snooping 을 수행하기 위해서는 해당 packet 에 대해서 이 trap 을 설정해 주는 것을 권장한다.

**10.6.1.3. mask-calculator**

flow-rule NAME classify l4port mask 명령을 사용하기 위해서는 복잡한 16 진수 mask 계산이 필요한 데 이를 쉽게 해결해 주는 명령이다. L4port 의 시작 값과 끝 값을 주면 이에 필요한 mask 개수와 설정에 필요한 mask 값을 출력해 준다.

표 10-15. mask-calculator 명령

명령어	설명	모드
<b>mask-calculator</b> <0-65535> <0-65535>	시작값과 끝값을 주면 필요한 mask 값을 출력한다.	Privileged

이해를 돕기위해 다음의 조건을 만족시키기 위한 한가지 예를 나타내었다.

예 1) port number 4000~4100 까지 100 개의 port 에 대해서 classification 하기 위한 mask 계산

```
Switch# mask-calculator 4000 4100
```

```
mask 0fa0 ffe0 : 4000 ~ 4031 ( 6)
mask 0fc0 ffc0 : 4032 ~ 4095 ( 7)
mask 1000 fffc : 4096 ~ 4099 ( 3)
mask 1004 ffff : 4100 ~ 4100 ( 1)
```

```
Required number of mask = 4
```

Switch#

위와 같이 출력된 4 개의 mask 를 이용해서 classification rule 을 적용하면 된다.

#### 10.6.1.4. policy-map 생성/추가

인터페이스에 Flow-rule 을 적용하기 위해 Policy-map 을 만들어 적용하며, Policy-map 에는 다수의 Flow-rule 이 포함될 수 있어, 한 인터페이스에 다수의 정책이 적용될 수 있으며 Policy-map 에 추가되는 순서에 의해 Flow-rule 이 적용되므로 그 순서가 대단히 중요하다.

적용된 순서는 **show flow-rule** 을 통해 확인할 수 있다.

표 10-16. Policy-map 생성 및 추가 명령

명령어	설명	모드
<b>policy-map</b> PNAME <b>flow-rule</b> FNAME	PNAME 이 없는 경우는 새로이 생성하고 PNAME 의 policy 가 기존에 있는 경우는 FNAME 의 flow 가 마지막으로 추가된다.	Config

Policy-map 전체를 삭제하거나, 적용된 하나의 Flow-rule 을 삭제하기 위해서는 다음의 명령어들이 사용된다.

표 10-17. Policy-map 삭제 및 특정 flow-rule 삭제 명령

명령어	설명	모드
<b>No policy-map</b> PNAME	PNAME 의 policy-map 을 삭제한다.	Config
<b>No policy-map</b> PNAME <b>flow-rule</b> FNAME	PNAME 의 policy-map 에서 FNAME 의 특정 flow-rule 를 삭제한다.	Config

생성된 policy-map 을 vlan 인터페이스에 적용/해제하는 명령어는 다음과 같다.

표 10-18. policy-map 적용/해제 명령

명령어	설명	모드
<b>service-policy</b> IFNAME { <b>ingress</b>   <b>egress</b> } PNAME	특정 포트 인터페이스의 해당 direction 으로 PNAME 의 policy-map 을 적용한다.	Config
<b>no service-policy</b> IFNAME	해당 인터페이스 적용된 policy-map 을 해제한다.	Config



**Notice**

policy-map 은 포트 인터페이스에 내려지며 하나의 포트 인터페이스에는 하나의 policy-map 만이 적용되므로 순서에 주의하면서 다수의 flow-rule 을 적용가능한 policy-map 을 생성하여야 한다.



**Notice**

policy-map 의 flow-rule 중에 drop 과 그 이외의 match rule 이 동시에 적용 될 경우, drop 룰은 우선되어 적용된다.

다음의 명령을 사용하여 flow-rule 관련 설정을 조회할수 있다.

**표 10-19. Flow-rule 조회 명령**

명령어	설명	모드
<b>show flow-rule</b>	flow-rule 및 policy-map 의 정보를 보여준다.	Config
<b>show service-policy</b>	현재 적용되어있는 policy-map 을 vlan 인터페이스와 함께 보여준다.	Config

이해를 돕기위해 다음의 조건을 만족시키기 위한 두가지 예를 나타내었다.

```

예 1) fa1 포트에 다음과 같이 적용한다.
tcp 6000 번 포트 drop
Src ip 20.1.1.0/24 queuing 2
Tcp 23 포트에 queuing 3 (highest) 및 marking
    
```

```

Switch#configure terminal
Switch(config)# flow-rule f1
Switch(config)# flow-rule f1 classify protocol tcp
Switch(config)# flow-rule f1 classify l4port 6000 any
Switch(config)# flow-rule f1 match drop
Switch(config)# flow-rule f2
Switch(config)# flow-rule f2 classify ipaddr 10.1.1.0/24 any
Switch(config)# flow-rule f2 match queuing 3
Switch(config)# flow-rule f3
Switch(config)# flow-rule f3 classify protocol tcp
Switch(config)# flow-rule f3 classify l4port 23 any
Switch(config)# flow-rule f3 match queuing 3
Switch(config)# flow-rule f3 match marking cos 3
Switch(config)#
Switch(config)# policy-map p1 flow-rule f1
Switch(config)# policy-map p1 flow-rule f2
Switch(config)# policy-map p1 flow-rule f3
Switch(config)#
Switch(config)# service-policy fa1
Switch(config)#
    
```

---

예 2) fa2 포트에 다음과 같이 적용한다.

tcp 4010 포트에 rate limit 10Mbps

tcp 5010 포트에 rate limit 20Mbps

---

---

```
Switch# conf t
Switch(config)# flow-rule f4
Switch(config)# flow-rule f4 classify protocol tcp
Switch(config)# flow-rule f4 classify l4port 4010 any
Switch(config)# flow-rule f4 match rate-limit 10000
Switch(config)# flow-rule f5
Switch(config)# flow-rule f5 classify protocol tcp
Switch(config)# flow-rule f5 classify l4port 5010 any
Switch(config)# flow-rule f5 match rate-limit 20000
Switch(config)#
Switch(config)# policy-map p2 flow-rule f4
Switch(config)# policy-map p2 flow-rule f5
Switch(config)#
Switch(config)# service-policy fa2 ingress p2
Switch#
```

---

## 10.6.2. Qos 관련 파라미터

IEEE 802.1p 규약에 의해서 tag 정보를 가지는 L2 패킷에는 패킷 우선순위를 가지는 cos 값이 있고, 이를 이용해서 queuing 할수 있어야 한다. 또한, 적당한 방법에 의해서 cos 값을 설정/재설정이 가능해야 한다. 이 값은 0 부터 7 사이의 값을 가진다.

또한, L3 패킷에는 dscp 값이 있으며, 이에 따른 적당한 queuing 역시 가능해야 한다.

U3000 시리즈는 각 인터페이스별로 8 개의 queue 를 가지고 있으며, 이들 사이의 mapping table 을 system wide 하게 유지하고 있다.

이 테이블은 다음의 명령어를 통해 marking/remarking 될 값을 변경할 수 있다.

표 10-20. Qos 관련 Marking/Remarking 테이블 셋팅 명령

명령어	설명	모드
<b>qos cos-queue-map &lt;0-7&gt; &lt;0-7&gt;</b>	규칙에 적용된 패킷의 cos 값에 의해 mapping 될 새로운 queue 값을 설정한다. 이는 <b>show qos cos</b> 로 확인 가능하다.	Config
<b>qos cos-remarking &lt;0-7&gt; &lt;0-7&gt;</b>	규칙에 적용된 패킷의 queue 값에 의해 remarking 될 새로운 Cos 값을 설정한다.	Config
<b>qos dscp-dp-map &lt;0-63&gt; &lt;0-1&gt;</b>	규칙에 적용된 패킷의 dscp 값에 의해 mapping 될 새로운 dp 값을 설정한다. 이는 <b>show qos dscp</b> 로 확인 가능하다.	Config
<b>qos dscp-pri-map &lt;0-63&gt; &lt;0-7&gt;</b>	규칙에 적용된 패킷의 dscp 값에 의해 mapping 될 새로운 pri 값을 설정한다. 이는 <b>show qos dscp</b> 로 확인 가능하다.	Config

표 10-21. Qos 관련 Marking/Remarking 테이블 조회명령

명령어	설명	모드
<b>show qos cos</b>	규칙에 적용된 패킷의 cos 값에 의해 mapping/remaking 테이블을 보여준다.	Privileged
<b>show qos dscp</b>	규칙에 적용된 패킷의 dscp 값에 의해 mapping 테이블을 보여준다.	Privileged

### 10.6.3. Scheduling

U3000 Series 스위치에서는 Scheduling 을 위해 SPQ(Strict Priority Queue) Method 와 WRR(Weighted Round Robin) , WFQ(Weighted Fair Queing) Method 를 제공하며 디폴트는 SPQ 이다.

다음 그림은 SPQ 와 WFQ 의 차이점을 나타내고 있다.

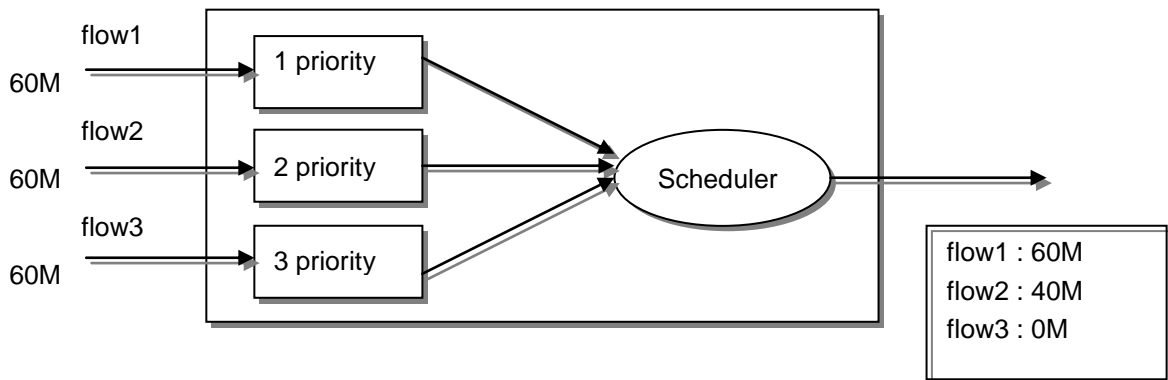


그림 10-2. SPQ(Strict Priority Queue) Method

SPQ(Strict Priority Queue) Method 인 경우 우선순위가 높은 패킷을 우선적으로 처리하기 때문에 flow1 과 같은 경우는 모든 패킷이 전달되지만 가장 낮은순위의 flow3 의 패킷은 하나도 전달되지 않는 경우가 발생한다.

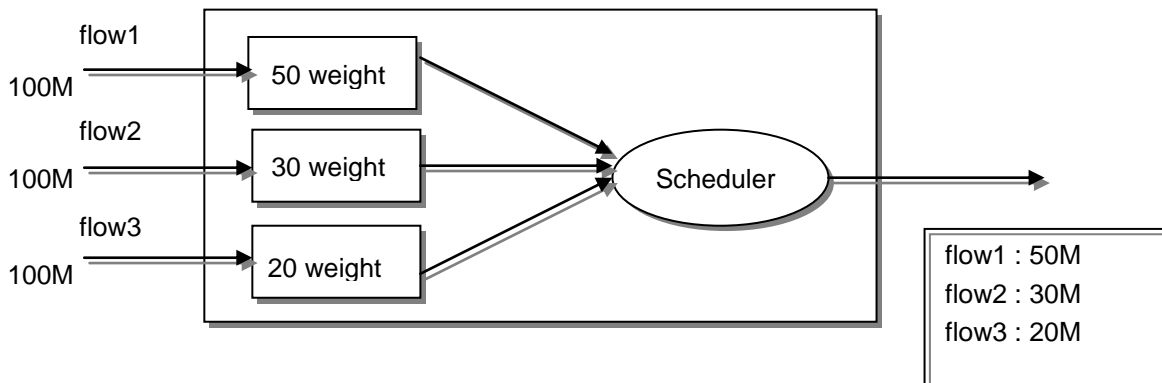


그림 10-3. WRR / WFQ Method

위의 그림은 WRR 과 WFQ Method 의 예인데 SPQ 와 달리 포트에 설정된 weight 를 기준으로 적당한 알고리즘에 의해 적당한 비율만큼 내보내게 된다. WFQ 는 WRR 과 유사하게 동작하지만, WRR 처럼

weight 에 따른 균등 분배는 아니기 때문에, 트래픽의 상태에 따라서 높은 우선순위의 Queue 에 weight 값 보다 더 많은 트래픽이 할당될 수 있다는 장점이 있다.

U3000 Series 스위치의 경우 8 개의 scheduling 을 위한 Queue 를 제공하며 다음은 특정 인터페이스의 Queue 방식을 결정하는 명령어이다.

표 21. Queue-mode 변경 명령

명령어	설명	모드
queueing-mode { strict  rr  wrr  wfq }	해당 Interface 의 Queue-mode 를 Strict 방식 혹은 RR / WRR / WFQ 방식으로 변경한다. Default 모드는 Strict 방식이다.	Interface
queueing-method <0-7> { strict  wrr  wfq }	WRR 또는 WFQ 로 설정한 interface 의 특정 queue 를 strict 로 설정하거나 해제 하기 위해서 사용한다.	Interface



**Notice** SPQ 에서의 우선순위는 8 개 Queue 중 숫자가 높을수록 우선순위가 높다.



**Notice** Queuing-mode 설정은 FX / Giga 포트의 경우 개별 설정이 가능하다. 하지만 TX 포트 인 경우는 8 개 단위로만 설정이 가능하며, 8 포트중 제일 첫 번째 포트에 설정하면 8 개의 포트에 모두 적용이 된다. 예를 들어 fa1 에 설정하면 fa1 ~ fa8 까지 모두 설정된다.

다음은 WRR / WFQ mode 로 설정되었을 경우에 해당 Queue 에 Weight 를 변경해주는 명령어이다.

표 22. Wrr-method Queue weight 변경 명령

명령어	설명	모드
queueing-profile wfq-weight <0-7> <1-2047>	해당 포트가 wfq 모드 일 때, 지정된 queue 의 wfq weight 값을 지정한다.	Interface
no queueing-profile wfq-weight	해당 포트가 wfq 모드 일 때, 지정된 queue 의 wfq weight 값을 디폴트 값으로 설정한다.	Interface
queueing-profile wrr-weight <0-7> <1-15>	해당 포트가 wrr 모드 일 때, 지정된 queue 의 wrr weight 값을 지정한다.	Interface
no queueing-profile wrr-weight	해당 포트가 wrr 모드 일 때, 지정된 queue 의 wrr weight 값을 디폴트 값으로 설정한다.	Interface



**Notice** Wfq 의 경우 100M 포트에서는 weight 1 은 64kbps 의 값을 의미하고, Giga 포트에서는 2Mbps 를 의미한다.

다음은 각 포트의 scheduling 관련 상태를 한눈에 알 수 있게 하여준다.

표 23. 전체 interface 의 queue-method 및 weight 조회명령

명령어	설명	모드
show port qos	시스템의 모든 인터페이스의 queue-method 및 weight 값을 보여준다.	Privileged

### 10.6.4. Congestion Avoidance

출력쪽의 큐에서 나타나는 혼잡은 실지 네트워크에서 입력 링크와 출력 링크사이에서 속도의 불협화로 출력쪽의 큐가 넘치면서 빈번히 발생한다. 큐의 혼잡이 발생했을 때 버퍼의 자원을 가용하게 하기 위해서 버퍼안에 있는 패킷을 버리는 것과 패킷의 지연시간이 원하는 값 이하로 유지하도록 하는 것이 중요하다.

U3000 Series 스위치는 Flow Classifier 나 Traffic Conditioner 에 의해서 마크된 높은 순위에 있는 패킷을 우선적으로 버린다. U3000 Series 에서 이를 위한 파라메타는 트래픽 종류에 따라 큐별로 서로 다르게 설정될 수 있다.

### 10.6.5. Filtering

Netbios 필터는 개별 인터페이스 별로 설정이 가능하며, Netbios 필터를 설정하면, Netbios / Netbeui / NBT 프로토콜이 모두 차단된다.

Dhcp 필터는 개별 인터페이스 별로 설정이 가능하며, 이 필터를 설정하면 해당 인터페이스의 DHCP server 패킷이 차단된다.

명령어들은 다음과 같다.

설정된 내용은 show interface 로 확인이 가능하다.

표 24. 기타 Filtering 관련 명령

명령어	설명	모드
filter netbios	특정 인터페이스에 netbios 필터를 설정한다...	Interface
no filter netbios	특정 인터페이스에 netbios 필터를 해제한다.	Interface
filter dhcp	특정 인터페이스에 dhcp filtering 을 설정한다.	Interface
no filter dhcp	특정 인터페이스에 dhcp filtering 을 해제한다.	Interface



# 11

## 환경 설정 저장 및 소프트웨어 업그레이드

### 11.1. Flash 파일 시스템

본 장에서는 시스템의 Flash File System의 관리에 대해서 설명한다. Flash File System은 시스템 OS Image와 Configuration 파일을 저장하는 장소로 사용되며, 저장된 OS Image와 Configuration File은 시스템 boot시 시스템에 Loading된다.

- Flash File System 운용에 필요한 명령어
- OS Image와 Configuration File Management에 필요한 명령어
- 부팅 모드 설정에 필요한 명령어

U3000 Series 스위치는 OS image 저장 및 환경 설정을 위해 Flash 파일 시스템을 구축한다. 이 장에서 본 제품의 Flash 파일 시스템에 대한 개략적인 설명을 한다.

Flash 파일 시스템은 OS image와 Configuration을 파일 형태로 저장하여 사용한다. 각 파일은 Flash 메모리의 영역에서 기록되고, 저장할 때 또는 rename 명령어로 저장이름을 설정할 수 있다. 또한 사용자의 요구사항에 따라 이미 Flash File System에 저장된 File을 erase 명령어로 지울 수 있다. 단 지우거나 변경할 File이 Reload시 부팅할 Image 또는 Configuration File인지 주의해야 한다.

시스템 파일 관리를 위한 기본 명령어는 다음과 같다.

표 11-1. 파일 관리를 위한 명령어

명령어	설명	모드
show flash	• Flash File 의 상태를 보여준다.	Privileged
erase <i>filename</i>	• Flash 메모리에 저장된 환경 설정 파일을 삭제한다.	Privileged

다음은 show flash 명령어를 시행하였을 때 나타나는 출력문의 예시를 나타낸다. U3000 Series 스위치는 Flash File System 의 정보에 대해서 이름과 그 파일 사이즈, 그리고 현재(-) 및 다음 부팅 모드(\*)에 대한 정보와 함께 그 파일이 OS 인지 Configuration 파일인지 나타낸다.

```
Switch# show flash

flash info
-length- -----type/info----- CN path
6684094 1.0.0          -* p33xx.100
6684094 1.0.0          -* p33xx.100_b
105     Configuration   B* cfg.txt
256 Kbytes available (7124 Kbytes used)

Switch#
```

## 11.2. Image/Configuration File Down/Up Load

U3000 Series 스위치는 운영하면서 필요한 OS Image 와 Configuration File 에 대해서 FTP 또는 TFTP 를 이용해서 Down 또는 Up Load 할 수 있다. 이는 새로운 파일을 Flash 파일에 저장하거나, 재부팅시 OS Image 나 Configuration 으로 적용될 수도 있습니다. 또한 운용상 필요한 OS Image 나 Configuration 을 FTP/TFTP Server 에 저장할 수 있다. 이 장에서는 어떻게 FTP/TFTP 를 통해서 파일을 Down/Up Load 하는지 설명한다. 아래에서 기술한 running-config 및 startup-config 에 대한 설명은 “Configuration File 관리”라는 장에 설명해 놓았다.



**Warning** 업그레이드할 Image 의 선택은 시스템 모델과 버전에 따라 상당히 주의를 요하므로 당사의 지시 사항을 따르기 바란다.



**Warning** FTP/TFTP 를 통해 적용되는 configuration 은 현재 시스템의 configuration 에 추가되거나 변경된다. 즉 현재 시스템의 configuration 이 완전히 없어지고 다운로드되는 configuration 으로 완전히 바뀌지는 않는다.

### 11.2.1. FTP 를 통한 Down/Up Load

아래는 FTP 를 이용한 파일 Down/Up Load 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 11-2. FTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy ftp flash	• FTP Server 에 있는 OS Image File 을 Flash 에 저장한다.	Privileged
copy flash ftp	• Flash 에 있는 OS Image File 을 FTP Server 에 저장한다.	
copy ftp config-file	• FTP Server 에 있는 Configuration File 을 Flash 에 저장한다.	Privileged
copy ftp running-config	• FTP Server 에 있는 Configuration File 을 현재 의 running-config 로 적용시킨다.	Privileged
copy running-config ftp	• System 에서 운용중인 현재 running-config 을 FTP Server 에 저장한다.	Privileged

아래는 FTP 를 이용한 파일 다운 방법에 대한 예를 보여준다.

```
Switch# copy ftp flash
```

```

IP address of remote host ? 192.168.0.1
User ID ? Ins
Password ?
Source file name ? vdsl2.r100
Destination file name ? vdsl2.r100

FTP::192.168.0.1//vdsl2.r100-->image file[vdsl2.r100]
Proceed [yes/no]? yes
(생략)
    
```

### 11.2.2. TFTP 를 통한 Down/Up Load

아래는 TFTP 를 이용한 파일 다운 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 11-3. TFTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy tftp flash	• TFTP Server 에 있는 OS Image File 을 Flash 에 저장한다.	Privileged
copy flash tftp	• Flash 에 있는 OS Image File 을 TFTP Server 에 저장한다.	
copy tftp config-file	• TFTP Server 에 있는 Configuration File 을 Flash 에 저장한다.	Privileged
copy tftp running-config	• TFTP Server 에 있는 Configuration File 을 현재의 running-config 로 적용시킨다.	Privileged
copy running-config tftp	• System 에서 운용중인 현재 running-config 을 TFTP Server 에 저장한다.	Privileged

아래는 TFTP 서버에 File 을 Up load 하는 방법에 대한 예를 보여준다.

```

Switch# copy flash tftp
IP address of remote host ? 192.168.0.1
filename to write on tftp host? vdsl2.r100

TFTP send: -> 192.168.0.1// vdsl2.r100
Proceed [yes/no]? yes
(생략)
    
```

## 11.3. Configuration File 관리

환경 설정은 시스템 운영자가 U3000 Series 스위치를 운영하면서 설정된 다양한 파라미터의 집합이

다. U3000 Series 스위치에서 사용하는 Configuration 에는 startup-config 와 running-config 가 있다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration 을 startup-config 라 하며, DRAM 내에서 구동하는 환경설정 값을 running-config 라 한다. 여기서는 Configuration File Management 에 필요한 저장, 삭제 및 다운로드 방법을 설명한다.

**표 11-4. Configuration Management 명령어**

명령어	설명	모드
<code>show startup-config</code>	• Flash 메모리에 저장된 Booting configuration 의 환경 설정 정보를 보여준다.	Privileged
<code>show running-config</code>	• 현재의 환경 설정 정보를 보여준다.	Privileged
<code>copy running-config startup-config</code>	• 현재 시스템에서 운용중인 Running configuration 파일을 startup 파일로 저장한다.	Privileged
<code>erase startup-config</code>	• 현재 설정된 startup configuration 파일을 지운다.	Privileged

### 11.3.1. Configuration file 의 저장

시스템 운영자가 환경 설정을 변경하면 새로운 설정은 DRAM 에 저장된다. DRAM 에 저장된 설정 정보는 시스템 재부팅 시 유지되지 않는다. 따라서 설정 정보를 시스템 재 부팅 시에도 계속 유지하기 위해서는 설정 정보 파일을 Flash 메모리에 저장해야 한다. 다음은 현재의 running configuration 를 보여주는 명령어와 현재의 running-config 를 startup-config 로 저장하는 명령어에 대한 예를 보여 준다.

```
Switch# show running-config
Current configuration...

Building system configuration...

interface vlan1
ip address 192.168.51.1/24
... <생략> ....
Switch#
Switch# copy running-config startup-config
Building system configuration...

Write system configuration to system.cfg...
```

---

```

Saving system configuration to system.cfg completed
Switch# show startup-config
Startup configuration...

interface vlan1
ip address 192.168.51.1/24
... <생략> ....
Switch#
    
```

---

### 11.3.2. Configuration file 의 삭제

U3000 Series 스위치는 시스템 재시동 시 flash 메모리에 저장되어 있는 startup-config 를 재 로딩 한다. 만약 현재 저장되어 있는 Configuration file 를 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# reload
    
```

---

## 11.4. Boot Mode 설정 및 시스템 재시동

U3000 Series 스위치는 운영하면서 필요한 OS Image 와 Configuration File 에 대해서 다음 부팅 파일로 설정할 수 있다. 이렇게 설정된 OS Image 와 Configuration File 은 시스템의 재 시동 시 적용되므로 각별한 주의가 필요하다. 아래에서는 OS Image 와 Configuration File 에 대해서 어떻게 다음 부팅 모드로 설정하는지와 시스템 재 시동 방법에 대해서 설명해 놓았다.

표 11-5. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
<code>boot flash filename</code>	• 다음 부팅시 적용될 OS Image 를 설정한다.	Privileged
<code>boot config filename</code>	• 다음 부팅시 적용될 Configuration File 을 설정한다.	Privileged
<code>reload</code>	• 시스템을 재 시동 시킨다.	Privileged

### 11.4.1. Boot Mode 설정

U3000 Series 스위치에서 OS Image 와 Configuration File 에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요하다. boot flash 명령어를 실행할 때에는 U3000 Series 스위치에서 사용할 수 있는 OS Image File 에 대해서만 적용하도록 해야 하며, 또 boot config 명령어를 실행할 때에는 U3000 Series 스위치에서 사용할 수 있는 Configuration File 에 대해서만 적용하도록 해야 된다. 그리고 현재 Flash File System 에 있는 File 에 대해서만 적용하도록 하여야 한다.

---

```
Switch#  
Switch# boot flash vdsl2.r101  
Switch#  
Switch# boot config start.cfg  
Switch#
```

---

### 11.4.2. 시스템 재시동

시스템의 재시동은 U3000 Series 스위치의 전원 On/Off 또는 콘솔상에서 명령어로 할 수 있다.



**Warning** 시스템의 재시동 전에는 반드시 현재의 Configuration 을 Flash 메모리에 저장하도록 한다.



**Warning** 시스템이 Flash File System 에 파일을 저장하고 있을 때는 시스템을 강제로 재시동 시켜서는 안 된다.

---

```
Switch# reload  
  
WARNING !!!  
You must save current configuration or you will lose it...  
"continue to reboot [yes/no]? yes  
Switch#
```

---

# 12

## CPU-FILTER & SYSCTL

### 12.1. CPU Filtering

본 Ubiquoss 3000 Series 에서는 스위치 자체로 들어오는 트래픽이나 스위치의 CPU 를 이용하여 포워딩되는 트래픽에 대한 필터링 기능을 제공합니다. 이는 IP 주소, 프로토콜, 포트 별로 사용자 설정이 가능하며, 다음의 명령어를 이용하여 필터링 설정을 할 수 있습니다.

#### 12.1.1. CPU-Filtering Rule 설정/해제

패킷을 필터링하기 위해서는 먼저 적절한 Rule 이 설정되어야 한다. CPU-Filtering Rule 은 프로토콜, src/dest IP, UDP/TCP Port 등에 의해 다양하게 적용할 수 있다. CPU-Filtering Rule 을 적용하기 위해서는 Global mode 에서 다음의 명령어를 수행한다.

명령어	설명
<code>cpu-filter rule NAME ip { srcIP   srcIP/M   any } { dstIP   dstIP/M   any } match { permit   deny }</code>	<ul style="list-style-type: none"> <li>IP 프로토콜에 대한 CPU-filter</li> <li>source address 와 destination address 를 기반으로 CPU-filter 를 적용</li> <li>분류되는 패킷을 match 명령어를 통해 허용할 것인가를 결정</li> </ul>
<code>cpu-filter rule NAME tcp { srcIP   srcIP/M   any } { dstIP   dstIP/M   any } { srcPort   any } { dstPort   any } match { permit   deny }</code>	<ul style="list-style-type: none"> <li>TCP 프로토콜에 대한 CPU-filter</li> <li>source/destination address 와 source/destination port 번호에 의한 CPU-filter</li> <li>분류되는 패킷을 match 명령어를 통해 허용할 것인가를 결정</li> </ul>
<code>cpu-filter rule NAME udp { srcIP   srcIP/M   any } { dstIP   dstIP/M   any } { srcPort   any }</code>	<ul style="list-style-type: none"> <li>UDP 프로토콜에 대한 CPU-filter</li> <li>source/destination address 와 source/</li> </ul>



<code>{ dstPort   any } match { permit   deny }</code>	destination port 번호에 의한 CPU-filter <ul style="list-style-type: none"> <li>■ 분류되는 패킷을 match 명령어를 통해 허용할 것을가를 결정</li> </ul>
--	--

위의 CPU-filter rule 을 해제하기 위해서는 **configure mode** 에서 다음의 명령어를 사용한다.

명령어	설명
<code>no cpu-filter rule NAME</code>	<ul style="list-style-type: none"> <li>■ NAME : 설정된 CPU-filter 의 이름</li> </ul>

## 12.1.2. CPU-FILTER Group 설정

CPU-Filter 를 시스템에 적용하기 위해서는 CPU-Filter rule 를 CPU-Filter group 에 추가하여야 한다. Ubiquoss 3000 에는 Input group 과 Output group 의 두 종류 group 을 설정할 수 있다. Input group 은 시스템 자체로 들어오는 트래픽에 대한 filter group 이며, forward group 은 스위치의 CPU 를 통해 라우팅되는 트래픽에 대한 filter group 이다. CPU-Filter group 에는 여러 개의 rule 이 적용될 수 있으며, group 에 추가되는 순서대로 rule 이 적용되므로, rule 적용 순서가 중요하다. 또한, 두 종류의 CPU-Filter group 이 지원되며, 적용된 순서는 **show cpu-filter group** 을 통해 확인할 수 있다.

### 12.1.2.1. INPUT Group 설정/해제

Input CPU-Filtering Group 을 적용하기 위해서는 **Global mode** 에서 다음의 명령어를 수행한다.

명령어	설명
<code>cpu-filter group input add NAME</code>	<ul style="list-style-type: none"> <li>■ NAME : 추가할 rule 의 이름</li> </ul>
<code>cpu-filter group input add NAME1 { above   below } NAME2</code>	<ul style="list-style-type: none"> <li>■ Group 에 이미 삽입된 rule 과 상대적인 위치에 새로운 rule 삽입</li> <li>■ NAME1 : 그룹에 새로 삽입 할 rule 의 이름</li> <li>■ NAME2 : 이미 Group 에 삽입되어 있는 rule 이름</li> <li>■ above : NAME2 의 위에 NAME1 삽입</li> <li>■ below : NAME2 의 아래에 NAME1 삽입</li> </ul>

Input CPU-Filtering Group 에서 rule 을 삭제하기 위해서는 **Global mode** 에서 다음의 명령어를 수행한다.

명령어	설명
<code>cpu-filter group input delete NAME</code>	<ul style="list-style-type: none"> <li>■ NAME : Group 으로부터 삭제할 rule 의 이름</li> </ul>

**cpu-filter group input delete all**

- Group 에 속한 모든 rule 삭제

**12.1.2.2. FORWARD Group 설정/해제**

Forward CPU-Filtering Group 을 적용하기 위해서는 Global mode 에서 다음의 명령어를 수행한다.

명령어	설명
<b>cpu-filter group forward add NAME</b>	<ul style="list-style-type: none"> <li>■ NAME : forward group 에 추가할 rule 의 이름</li> </ul>
<b>cpu-filter group forward add NAME1 { above   below } NAME2</b>	<ul style="list-style-type: none"> <li>■ Group 에 이미 삽입된 rule 과 상대적인 위치에 새로운 rule 삽입</li> <li>■ NAME1 : 그룹에 새로 삽입 할 rule 의 이름</li> <li>■ NAME2 : 이미 Group 에 삽입되어 있는 rule 이름</li> <li>■ above : NAME2 의 위에 NAME1 삽입</li> <li>■ below : NAME2 의 아래에 NAME1 삽입</li> </ul>

**12.1.2.3. CPU-FILTER service 의 활성화**

CPU-Filtering Group 을 설정한 다음, 시스템에 이 RULE 들을 적용하기 위해서는 Global mode 에서 다음의 명령어를 수행한다.

명령어	설명
<b>service cpu-filter</b>	<ul style="list-style-type: none"> <li>■ CPU-FILTER 의 활성화</li> </ul>
<b>no service cpu-filter</b>	<ul style="list-style-type: none"> <li>■ CPU-FILTER 의 비활성화</li> </ul>

**12.1.3. CPU-FILTER 의 설정 예**

다음은 스위치로 들어오는 모든 TELNET 을 허용하지 않도록 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# cpu-filter rule telnet tcp any any any 23 match deny
Switch(config)# cpu-filter group input add telnet
Switch(config)# service cpu-filter
```

다음은 스위치 CPU 라우팅을 이용하는 FTP 트래픽을 허용하지 않도록 하는 설정 예이다.

```
Switch# configure terminal
Switch(config)# cpu-filter rule ftp tcp any any any 20 match deny
```

```
Switch(config)# cpu-filter rule ftp-data tcp any any any 21 match deny
Switch(config)# cpu-filter group forward add ftp
Switch(config)# service cpu-filter
```

다음은 스위치에 설정된 CPU-FILTER group 의 조회를 나타낸다.

```
Switch# show cpu-filter group
-----
INPUT  GROUP-LIST    : telnet
FOWARD GROUP-LIST    : ftp
-----
total 2 group-list found
```

다음은 스위치에 설정된 CPU-FILTER rule 의 조회를 나타낸다.

```
Switch# show cpu-filter
-----
CPU-FILTER  PROTO SRC-IP      DST-IP      SPORT  DPORT  ACTION
-----
telnet      tcp    any         any         any    23     deny
ftp         tcp    any         any         any    21
deny
ftp-data    tcp    any         any         any    20     deny
```

## 12.2. SYSCTL 개요

SYSCTL 기능은 linux kernel 에서 제공하는 /proc/sys/net/ipv4 아래의 parameter 들 중 Attack 방지와 관련된 parameter 들을 설정/해제 가능 하도록 하여주는 기능이다

## 12.3. SYSCTL 명령어

SYSCTL 명령으로 설정 가능한 parameter 들은 다음과 같다.

표 12-1. SYSCTL 명령어

명령어	설명	모드
<b>sysctl secure_redirect</b> <i>INTERFACE</i> ( <i>default disable enable</i> )	디폴트 게이트웨이 목록에 있는 게이트웨이에만 ICMP 리다이렉트 메시지를 전달, 차단. <b>Default) enable</b>	config
<b>Sysctl send_redirects</b> <i>INTERFACE</i> ( <i>default disable enable</i> )	라우터 기능으로 동작시 다른 호스트로 ICMP 리다이렉트 전달, 차단. <b>Default) enable</b>	config
<b>Sysctl icmp_port_unreach</b> <i>INTERFACE</i> ( <i>default disable enable</i> )	Icmp port unreachable 허용, 차단 <b>Default) disable</b>	config
<b>Sysctl icmp_host_unreach</b> <i>INTERFACE</i> ( <i>default disable enable</i> )	Icmp host unreachable 허용, 차단 <b>Default) disable</b>	config
<b>Sysctl icmp_net_unreach</b> <i>INTERFACE</i> ( <i>default disable enable</i> )	Icmp net unreachable 허용, 차단 <b>Default) disable</b>	config
<b>Sysctl icmp_prot_unreach</b> <i>INTERFACE</i> ( <i>default disable enable</i> )	Icmp prot unreachable 허용, 차단 <b>Default) disable</b>	config
<b>Sysctl tcp_max_syn_backlog</b> <i>VALUE</i>	Tcp syn backlog queue 의 최대치 설정 <b>Default) 1024</b>	config
<b>Sysctl ip_default_ttl</b> <i>VALUE</i>	Default TTL 크기 설정 <b>Default) 64</b>	config
<b>Sysctl ipfrag_time</b> <i>VALUE</i>	플래그멘테이션 된 IP 데이터를 메모리에 갖고 있는 시간 설정 <b>Default) 30</b>	config
<b>Sysctl tcp_syn_retries</b> <i>VALUE</i>	활성 TCP 연결에서 재전송을 위해 지정한 시간만큼 지난 뒤에 초기화 SYN 패킷을 보냄 <b>Default) 5</b>	config
<b>Sysctl tcp_retries1</b> <i>VALUE</i>	의심스러운 tcp session 에 대한 재전송 횟수 설정 <b>Default) 3</b>	config
<b>Sysctl tcp_retries2</b> <i>VALUE</i>	종단전 재전송 횟수 <b>Default) 15</b>	config
<b>Sysctl tcp_keepalive_time</b> <i>VALUE</i>	keepalive 가 활성화되었을 시 keepalive time 설정 <b>Default) 7200</b>	config
<b>Sysctl tcp_fin_timeout</b> <i>VALUE</i>	FIN-WAIT-2 상태의 소켓 유지 시간 설정 <b>Default) 60</b>	config
<b>Sysctl tcp_max_tw_buckets</b> <i>VALUE</i>	timewait 소켓의 수 설정 <b>Default) 18000</b>	config
<b>Sysctl tcp_keepalive_probes</b> <i>VALUE</i>	연결이 끊어졌다고 여길 때까지 발생 시 킬 keepalive probe 메시지 <b>Default) 9</b>	config
<b>Sysctl tcp_syncookies</b> ( <i>default disable enable</i> )	syn flood attack 방어를 위한 설정 <b>Default) enable</b>	config
<b>Sysctl tcp_send_reset</b> ( <i>default disable enable</i> )	Tcp send reset 플래그 설정, 해제 <b>Default) enable</b>	config

# 13

## VDSL 설정

이 장에서는 U3000 스위치에서 VDSL 관련 설정을 하는 방법에 대해 설명합니다. 이 장에서는 설명하는 내용은 다음과 같습니다:

- 프로파일 개요
- Line 프로파일 설정
- CPE firmware upgrade
- Displaying VDSL Status

**Note**

이 장에서 사용되는 CLI 명령어의 상세한 사용방법은 `command reference` 를 참고하십시오.

### 13.1. 프로파일 개요

U3000 시리즈 스위치는 **프로파일profile**이라고 부르는 설정을 사용하여 VDSL link의 상향속도<sup>upstream rate</sup>과 하향속도<sup>downstream rate</sup>를 제어할 수 있습니다. 프로파일에 의해 VDSL link는 약 64Kbps 에서 100 Mbps 사이의 상향/하향 대역을 가질 수 있습니다.

U3000 시리즈 스위치는 미리 정의된 프로파일 (DEFVAL 프로파일)을 가지고 있으며, 새로운 프로파일을 정의할 수도 있습니다. 프로파일은 각 포트 별로 설정할 수 있습니다. 기본적으로 U3000 시리즈 스위치의 모든 VDSL 포트에는 DEFVAL 프로파일이 적용되어 있습니다.

**Note**

DEFVAL 프로파일의 설정 내용은 OS 버전에 따라 달라질 수 있습니다. DEFVAL 프로파일의 내용을 참고하여 환경에 맞는 프로파일을 생성하여 사용하는 것을 권장합니다.

## 13.2. Line 프로파일 설정

이 절에서는 프로파일 설정에 대한 지침과 VDSL 포트에 프로파일을 적용하는 방법에 대해서 설명합니다.

### 13.2.1. Default 설정

다음은 VDSL 포트에 대한 default 설정입니다:

- U3000 시리즈 스위치의 모든 VDSL 포트에는 DEFVAL 프로파일이 설정되어 있습니다.

### 13.2.2. Assigning a Profile to a Specific VDSL Port

각 포트 별로 프로파일을 설정할 수 있습니다. 그래서 스위치의 VDSL 포트들에 같은 프로파일 또는 다른 프로파일을 적용할 수 있습니다. U3000 시리즈 스위치의 모든 VDSL 포트에는 DEFVAL 프로파일이 설정되어 있습니다.

특정 포트에 프로파일을 설정하려면, privileged EXEC 모드에서 다음의 과정을 수행합니다:

	명령어	목적
Step 1	<code>configure terminal</code>	global configuration 모드로 진입한다.
Step 2	<code>interface interface-id</code>	설정할 포트를 명시하고, interface configuration 모드로 진입한다.
Step 3	<code>service-line-profile profile-name</code>	프로파일 이름을 명시한다.

포트에 설정된 프로파일을 삭제하려면, 시스템의 default 프로파일을 사용하려면, interface configuration 명령 `no service-line-profile` 을 사용합니다.

### 13.2.3. Configuring a New Line Profile

U3000 시리즈 스위치는 새로운 Line 프로파일을 생성할 수 있습니다. 새로 생성되는 프로파일은 DEFVAL 프로파일의 값을 상속받습니다.

프로파일을 생성하려면, privileged EXEC 모드에서 다음의 과정을 수행합니다:

	명령어	목적
Step 1	<code>configure terminal</code>	global configuration 모드로 진입한다.
Step 2	<code>line-profile profile-name</code>	프로파일 이름을 명시하고, profile configuration 모드로 진입한다.
Step 3	<code>end</code>	privileged EXEC 모드로 돌아간다.

새로 생성된 프로파일은 DEFVAL 프로파일과 동일한 설정을 가지고 있습니다. 다음에 설명하는 profile configuration 명령을 사용하여 프로파일의 설정 내용을 변경할 수 있습니다.

프로파일을 삭제하려면 global configuration 명령 `no line-profile profile-name` 을 사용합니다.

### 13.2.4. Reset VDSL Port with Updated Profile

프로파일의 설정내용이 변경되었을 때에는, 해당 프로파일을 사용하는 VDSL 포트들을 reset하여 프로파일의 변경내용을 적용해야 합니다. U3000 시리즈 스위치는 프로파일과 관련된 포트들을 한 번에 reset 시킬 수 있습니다.

변경된 프로파일의 설정내용을 VDSL 포트에 적용하려면, privileged EXEC 모드에서 다음의 과정을 수행합니다:

	명령어	목적
Step 1	<code>configure terminal</code>	global configuration 모드로 진입한다.
Step 2	<code>line-profile profile-name</code>	프로파일 이름을 명시하고, profile configuration 모드로 진입한다.
Step 3	<code>apply associated-ports</code>	이 프로파일을 사용하는 VDSL 포트들을 reset 한다.
Step 4	<code>end</code>	privileged EXEC 모드로 돌아간다.

### 13.2.5. Line profile 설정

명령어	Mode	기능
<code>band-modifier</code>		Band Modifier
<code>downstream</code>		Downstream
<code>g-handshake</code>		G.HS (Handshake)
<code>ife-rx-filter</code>		IFE RX filter
<code>ife-tx-filter</code>		IFE TX filter
<code>line-type</code>		VDSL line type
<code>option-band-plan</code>	Line-profile	Option Band Plan
<code>pbo-config</code>		PBO(Power Back Off) config
<code>power-mode</code>		Power Mode
<code>rate-adaptation-mode</code>		Rate adaptation mode
<code>tcn</code>		TCM (Trellis Code Modulation)의 적용 여부를 설정한다
<code>upstream</code>		Upstream
<code>downstream</code>		Downstream

### 13.2.5.1. pbo-config 설정

U3000 시리즈의 VDSL 라인이 CPE와 연결되는 거리는 포트마다 다를 수 있습니다. VDSL 라인의 거리가 다름에도 불구하고 똑 같은 전력량이 제공되면, 가까운 거리에 CPE가 연결되어 있는 라인에 전달되는 전력량은 먼 거리에 CPE가 연결되어 있는 라인에 전달되는 전력량보다 크며 이 때 먼 거리에 CPE가 연결되어 있는 라인에 간섭이 일어날 수도 있습니다. 따라서 U3000 시리즈는 VDSL 라인에 불필요하게 큰 전력량이 전달되는 것을 막기 위해 거리에 따라 전력량을 조절하는 기능을 제공하고 있습니다.

명령어	Mode	기능
<code>pbo-config enable</code>		PBO 기능을 활성화 시킵니다.
<code>pbo-config disable</code>		PBO 기능을 비활성화 시킵니다.
<code>pbo-config length {0,...,900}</code>	line-profile	PBO 기능을 적용할 라인 길이를 100m 단위로 설정합니다.
<code>pbo-config k1[1] k1[2] k1[3] k1[4] k1[5] k1[6]</code>		PBO 기능을 위한 내부적인 항목들이 정해져 있지만 시스템의 설치환경에 따라 맞지 않은 경우가 발생할 수 있는데 이 때 값을 조절하기 위한 명령어입니다. 가급적 시스템에 기본적으로 설정되어 있는 값을 사용하기를 권장합니다.
<code>pbo-config k2[1] k2[2] k2[3] k2[4] k2[5] k2[6]</code>		

### 13.2.5.2. Optionnal band 설정

U3000 시리즈는 단거리에서 6band를, 장거리에서는 3band를 사용합니다. 장거리일 경우에 Downstream에 비해 상대적으로 Upstream의 대역폭이 적은데, U3000 시리즈는 사용자의 요구에 따라 Downstream의 영역, 또는 현재 사용하고 있지 않은 영역 등을 Upstream의 대역폭으로 사용하여 장거리에서 안정적인 전송을 보장하도록 설정할 수 있습니다. 이와 같이 Upstream 대역폭을 늘리기 위해 사용하는 것을 Option band라고 합니다. Option band를 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
<code>optional-band-plan annex-a-25-138</code>	line-profile	25~138Kbps 대역을 optional band 로 사용합니다.
<code>optional-band-plan annex-b-138-276</code>		138~276Kbps 대역을 optional band 로 사용합니다.
<code>optional-band-plan annex-m-25-276</code>		위 2 대역을 모두 포함하는 25~276Kbps 대역을 optional band 로 사용합니다.
<code>exclude</code>		optional band 를 사용하지 않도록 설정합니다.



**Note**

U3000 시리즈는 기본적으로 exclude 로 설정되어 있습니다.



다음은 Option band의 영역에 대한 설명입니다.

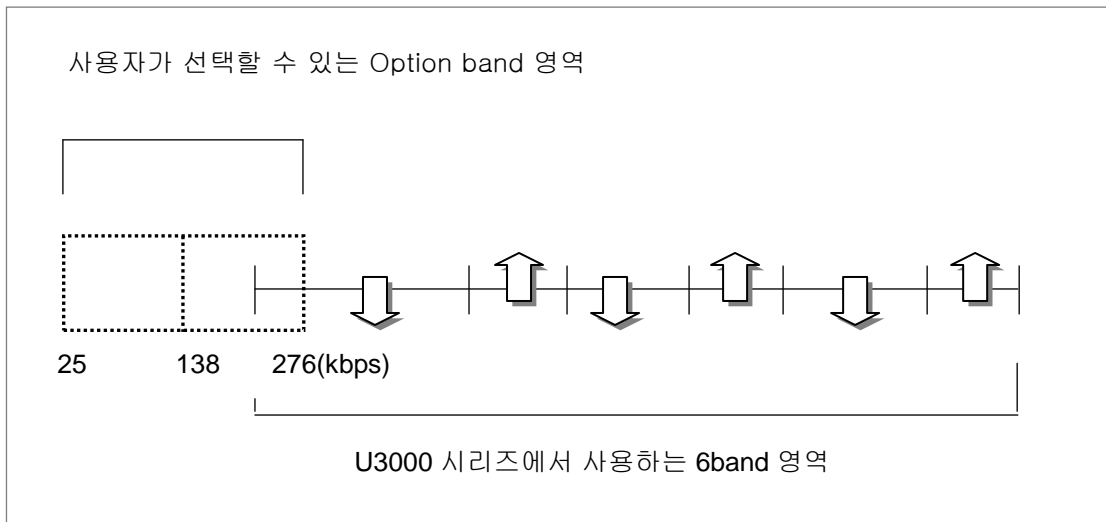


그림 13-1. Option band 와 6band

### 13.2.5.3. band-modifier 설정

U3000 시리즈는 기존 ADSL, ISDN 등의 간섭을 피하기 위하여 특정대역이하의 주파수를 차단하는 필터 기능을 사용할 수 있습니다. band modifier 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기      능
band-modifier rx disable-640k-below		ISDN 대역을 disable 합니다.
band-modifier rx disable-1.1m-below		ISDN, ADSL 대역을 disable 합니다.
band-modifier rx disable-2.2m-below		2.2MHz 이하 대역을 disable 합니다.
band-modifier rx all-tones-on	line-	ISDN, ADSL 주파수 대역 제한 없이 모두 사용합니다.
band-modifier tx disable-640k-below	profile	
band-modifier tx disable-1.1m-below		ISDN, ADSL 대역을 disable 합니다.
band-modifier tx disable-2.2m-below		2.2MHz 이하 대역을 disable 합니다.
band-modifier tx all-tones-on		ISDN, ADSL 주파수 대역 제한 없이 모두 사용합니다.



**Note**

U3000 시리즈는 기본적으로 상하향에 대해 all-tone-on 으로 설정되어 있습니다.

### 13.2.5.4. G.HS 설정

VDSL 장비와 가입자 측 CPE 는 각자가 가진 각종 정보를 상호교환하여 거리, 노이즈 폭, band plan 등에 따라 최적의 설정값을 결정합니다. 이러한 과정을 정의한 것이 G.HS 입니다. U3000 시리즈는 A43, B43, I43, V43 의 방식의 G.HS 를 지원합니다. G.HS 를 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
g-handshake a43 {on off}		Ikanos 사에서 사용하는 a43의 사용유무를 설정합니다.
g-handshake b43 {on off}	line-	Ikanos 사에서 사용하는 b43의 사용유무를 설정합니다.
g-handshake v43 {on off}	profile	G.992, G.993 에서 표준화된 V43 을 사용유무를 설정합니다.
g-handshake i43 {on off}		Ikanos 사에서 사용하는 I43의 사용유무를 설정합니다.



**Note** U3000 시리즈는 기본적으로 V43, B43 이 설정되어 있습니다.

### 13.2.5.5. ife-tx-filter, ife-rx-filter 설정

U3000 시리즈에서 5band, 6band 를 사용할 경우에는 별도의 외부필터(external filter)가 필요없으나, 100/100 band plan 혹은 VLR 를 사용할 경우에는 필요하게 됩니다. Extern filter를 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
ife-tx-filter internal		외부 필터를 사용하지 않습니다.
ife-tx-filter k1_external	line-	K1 필터를 사용합니다.
ife-tx-filter u1_external	profile	U1 필터를 사용합니다.
ife-tx-filter h1_external		H1 필터를 사용합니다.
ife-tx-filter ttc_external		TTC 필터를 사용합니다.

명령어	Mode	기능
ife-rx-filter internal		외부 필터를 사용하지 않습니다.
ife-rx-filter k1_external	line-	K1 필터를 사용합니다.
ife-rx-filter u1_external	profile	U1 필터를 사용합니다.
ife-rx-filter h1_external		H1 필터를 사용합니다.
ife-rx-filter ttc_external		TTC 필터를 사용합니다.



**Note** U3000 시리즈는 기본적으로 tx, rx 에 대하여 internal 로 설정되어 있습니다.

### 13.2.5.6. line type 설정

U3000 시리즈는 지역특성, 거리, 대역폭에 따른 다양한 프로파일을 지원합니다. Line-type 을 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
line-type auto-detect all-xdsl		ADSL 1/2/2+, VDSL 1/2 의 모든 프로파일을 지원합니다.
line-type auto-detect vdsl2-itu	line-profile	ITU 표준인 8A/8B/8C/8D/12A/12B/17A 프로파일을 지원합니다.
line-type auto-detect vdsl2-all		8A/8B/8C/8D/12A/12B/17A과 30A 프로파일을 지원합니다.

명령어	Mode	기능
line-type manual-set adsl-annex-a {on off}		ADSL DMT Annex A 를 설정합니다.
line-type manual-set adsl-annex-b {on off}		ADSL DMT Annex B 를 설정합니다.
line-type manual-set adsl-annex-c {on off}		ADSL DMT Annex C 를 설정합니다.
line-type manual-set adsl2-annex-a {on off}		ADSL2 DMT Annex A 를 설정합니다.
line-type manual-set adsl2-annex-b {on off}		ADSL2 DMT Annex B 를 설정합니다.
line-type manual-set adsl2+-annex-a {on off}		ADSL2+ DMT Annex A 를 설정합니다.
line-type manual-set adsl2+-annex-b {on off}		ADSL2+ DMT Annex B 를 설정합니다.
line-type manual-set adsl2+-annex-m {on off}		ADSL2+ DMT Annex M 를 설정합니다.
line-type manual-set adsl2+-annex-l {on off}		ADSL2+ DMT Annex L 를 설정합니다.
line-type manual-set vdsl-ansi {on off}		VDSL ANSI 를 설정합니다.
line-type manual-set vdsl-etsi {on off}		VDSL ETSI 를 설정합니다.
line-type manual-set vdsl-itu-993-1 {on off}	line-profile	VDSL ITU 993 1 를 설정합니다.
line-type manual-set vdsl-ieee-802-ah {on off}		VDSL IEEE 802 AH 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-8a {on off}		VDSL2 ITU G993 2 8A 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-8b {on off}		VDSL2 ITU G993 2 8B 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-8c {on off}		VDSL2 ITU G993 2 8C 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-8d {on off}		VDSL2 ITU G993 2 8D 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-12a {on off}		VDSL2 ITU G993 2 12A 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-12b {on off}		VDSL2 ITU G993 2 12B 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-17a {on off}		VDSL2 ITU G993 2 17A 를 설정합니다.
line-type manual-set vdsl2-itu-g993-2-30a {on off}		VDSL2 ITU G993 2 30A 를 설정합니다.



**Note**

U3000 시리즈는 거리, 통신선로, CPE 의 라인타입에 따라 최적의 라인타입을 결정하는 auto switching 기능을 가지고 있습니다. 예를 들어 8A, 12A, 30A 가 설정되어 있고 선로의 길이가 3Km 라면 8A 로 결정이 되는데 거리가 100m 로 짧아진다면 자동으로 30A 로 전환되게 됩니다.

### 13.2.5.7. power-mode 설정

U3000 시리즈는 선로의 출력전압을 설정할 수 있습니다. 다음 명령어를 사용하십시오.

명령어	Mode	기능
power-mode 0	line-profile	선로의 출력전압을 8.5 dBm 으로 설정합니다.
power-mode 1		선로의 출력전압을 11.5 dBm 으로 설정합니다.
power-mode 2		선로의 출력전압을 14.5 dBm 으로 설정합니다.
power-mode 3		선로의 출력전압을 17.5 dBm 으로 설정합니다.
power-mode 4		선로의 출력전압을 20.5 dBm 으로 설정합니다.



**Note** U3000 시리즈는 기본적으로 (4) 20.5 dBm 으로 설정되어 있습니다.

### 13.2.5.8. rate-adaptation-mode 설정

U3000 시리즈는 거리 및 선로상태에 따라 최적의 전송 속도를 자동으로 설정하도록 할 수도 있고 고정적인 전송 속도를 설정할 수 있습니다. fixed 모드를 설정하면 설정된 maximum data rate 에서 train 합니다. Synchronization이 실패하더라도 fixed rate에서 계속 train을 시도하도록 되어있어 라인특성이 좋지 않은 상황에서는 통신이 되지 않을 수 있습니다. 반면 startup 모드로 설정하면 거리 및 선로상태에 따라 설정된 Max rate 와 min rate 사이에서 synchronization 되도록 되어 있습니다. rate-adaptation-mode 를 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
rate-adaptation-mode fixed	line-profile	Fixed 모드로 설정합니다.
rate-adaptation-mode startup		Startup 모드로 설정합니다.



**Note** U3000 시리즈는 기본적으로 startup 으로 설정되어 있습니다.

### 13.2.5.9. upstream / downstream 설정

U3000 시리즈에서 상향(upstream)과 하향(downstream) 별로 rate limit, snr margin 등을 설정할 수가 있습니다.

## max-margin, min-noise-margin, target-noise-margin 설정

디지털 통신과 아날로그 통신에서 SNR(Signal to Noise Ratio)는 신호 대 노이즈의 비율을 나타낸 것으로 그 공식은, 신호의 세기를  $V_s$ , 노이즈의 세기를  $V_n$ 이라고 할 때, 「 $SNR(dB) = 20 \log_{10}(V_s/V_n)$ 」로 나타냅니다. 신호의 세기가 노이즈 세기와 같거나 노이즈 세기보다 작으면 안정적인 통신이 이루어질 수 없습니다. 따라서, 안정된 라인을 유지하려면 SNR은 음수이거나 “0”이 되어선 안되고, 이러한 경우에는 신호 수준을 증가시키거나 노이즈의 수준을 감소시키는 조치를 취하지 않으면 안됩니다.

VDSL 라인의 전송 속도는 SNR에 의해 결정됩니다. 그러나 라인 환경은 항상 일정할 수는 없기 때문에 변화될 수 있는 가능성을 고려하여 VDSL 라인의 전송 속도가 결정될 수 있도록 하는 것이 좋습니다. 노이즈가 갑자기 증가하여 노이즈의 세기가 커지면 SNR은 작아지고, 통신은 불안정해집니다. 따라서, 노이즈가 갑자기 증가했을 때 작아진 SNR 값에 적합한 전송 속도를 미리 결정해 두면, 노이즈가 증가했을 때에도 통신에는 문제가 발생하지 않습니다.

U3000 시리즈는 변화될 것으로 예상되는 SNR의 범위의 값을 설정해 두면, 현재 라인 환경의 SNR에서 사용자가 설정해 둔 값을 뺀 후 전송 속도를 적용하게 됩니다. 이 때, 변화될 것으로 예상되는 SNR의 범위의 값을 「SNR 마진」이라고 합니다.

다시 설명하면, SNR 마진을 “6”으로 설정하면, 아래의 그림과 같이 현재 라인 환경의 SNR에서 6을 뺀 SNR 값에 알맞은 전송 속도를 선택하게 되는 것입니다.

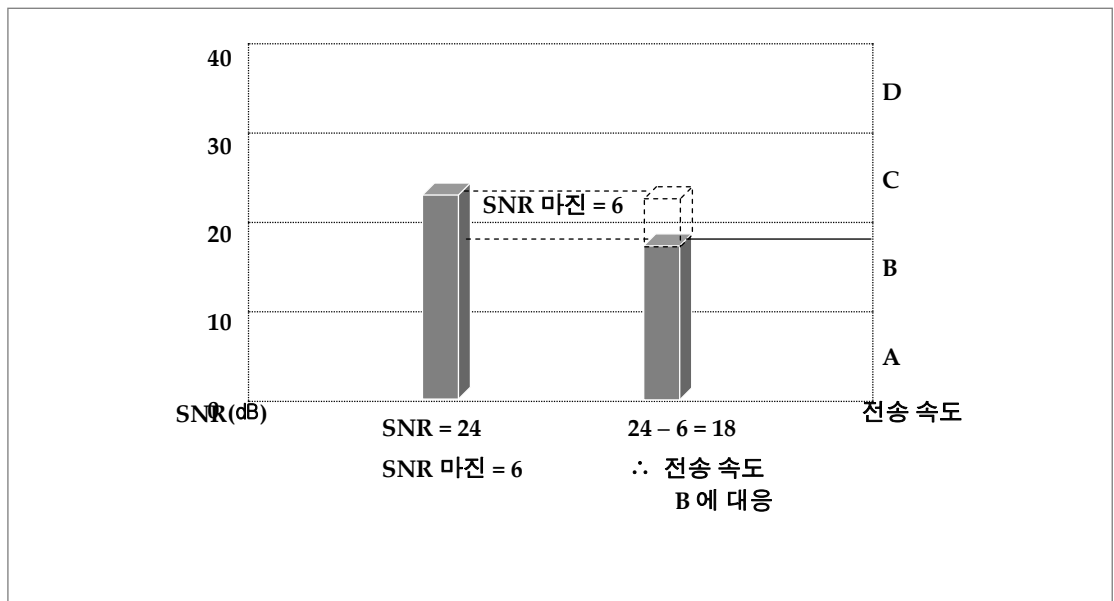


그림 13-2. SNR 마진에 따른 전송 속도 결정

노이즈의 변동이 심할 것으로 예상되는 환경에서는 SNR 마진을 크게 설정합니다. 그러나, SNR 마진을 크게 설정하면 안정된 통신이 보장되긴 하지만, 전송 속도가 느려지는 단점이 있습니다

U3000 시리즈에서 snr margin 을 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
upstream max-margin		snr margin 의 최대값을 설정합니다.
upstream min-noise-margin		snr margin 의 최소값을 설정합니다.
upstream target-noise-margin	line-profile	snr margin 의 목표값을 설정합니다.
downstream max-margin		snr margin 의 최대값을 설정합니다.
downstream min-noise-margin		snr margin 의 최소값을 설정합니다.
downstream target-noise-margin		snr margin 의 목표값을 설정합니다.



**Note**

U3000 시리즈는 기본적으로 max-margin 은 31 dB, min-noise-margin 은 5dB, target-noise-margin 은 6dB 로 설정되어 있습니다.

### VDSL 포트 전송 속도 설정

VDSL 포트 전송 속도는 이더넷 포트의 대역폭을 설정하는 방법과 동일한 방법으로 설정할 수 있습니다. 이러한 기능은 VDSL 가입자에게 차별화된 서비스를 제공할 수 있도록 도와줍니다. Line Rate 은 VDSL 시스템과 가입자 모뎀이 상호간 설정되기 원하는 속도이며, Payload Rate 은 실제로 설정된 Data Rate 입니다. 설정된 Line Rate 은 noise margin, line type 등에 따라서 편차를 갖는 Payload Rate 으로 설정되게 됩니다. 각 Rate 은 최소와 최대 Rate 을 지정할 수 있는데, 선로가 이 범위 내에서 Payload Rate 이 설정되지 않으면 자동적으로 선로가 끊어지게 됩니다. VDSL 포트의 대역폭을 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능
upstream slow-max-rate <0-200000>	line-profile	상향 속도의 최대값을 64Kbps 단위로 설정합니다.
upstream slow-min-rate <0-200000>		상향 속도의 최소값을 64Kbps 단위로 설정합니다.
downstream slow-max-rate <0-200000>		하향 속도의 최대값을 64Kbps 단위로 설정합니다.
downstream slow-min-rate <0-200000>		하향 속도의 최소값을 64Kbps 단위로 설정합니다.



**Note**

U3000 시리즈는 기본적으로 상하향 각각 최대 125Mbps 로 설정되어 있습니다.

## Interleave 설정

디지털 신호를 아날로그 신호로 변조(Modulation)하기 전에 데이터의 에러를 효율적으로 보정하기 위해서 상호 배치(Interleave)하는 과정이 있습니다.

Interleave는 특정한 크기의 데이터가 어느 정도 모이면 모인 데이터를 다시 재배치한 후 다시 특정한 크기로 나누어 전송합니다.

아래의 그림을 보면, 에러가 집중적으로 모여 있는 데이터가 Interleave를 통해 재배치 됨에 따라 에러가 골고루 분산됩니다. 에러가 분산되면서 에러의 크기가 작아지면 에러의 크기가 클 때보다 쉽게 보정할 수 있기 때문에 효율적입니다.

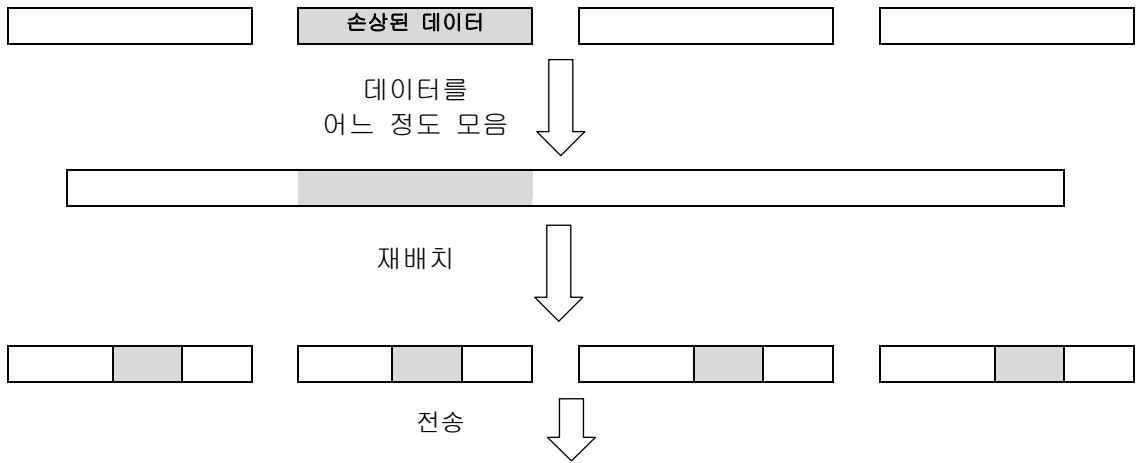


그림 13-3. Interleave 의 예

Interleave 과정을 거치면 에러를 효율적으로 보정할 수 있지만, 데이터가 어느 정도 모일 때까지 기다렸다가 한꺼번에 전송되기 때문에 하나씩 전송될 때보다 시간이 걸리는 단점이 있습니다. 반대로, Interleave 과정을 생략하면 데이터가 전송되는 속도는 빨라지지만, 에러를 보정하는 효율이 떨어지게 됩니다. DMT 변조 방식을 사용하는 U3000 시리즈는 Interleave 단계를 거쳐 데이터를 전송하는 slow channel 모드만 사용됩니다.

한편, 신호 변조 과정에서 Interleave 단계를 거치도록 설정된 상태에서는 데이터를 모았다가 한꺼번에 보내기까지의 시간 간격을 설정할 수 있습니다. 이러한 시간 간격을 Interleave-delay라고 합니다. Interleave-delay를 지정하면, 데이터가 어느 정도 모아지기까지 계속 기다림에 따라 데이터 전송이 더욱 지연되는 것을 방지할 수 있습니다.

Interleave delay 값을 변경하려면 다음 명령어를 사용하십시오.

명령어	Mode	기능	능력
<code>upstream slow-max-interdelay &lt;0-200&gt;</code>	line-	상향 interleave delay 값을 0.5 ms 단위로 설정합니다.	
<code>downstream slow-max-interdelay</code>	profile	하향 interleave delay 값을 0.5 ms 단위로 설정합니다.	



**Note** U3000 시리즈는 기본적으로 상하향 interleaved delay 값이 각각 1.0ms 로 설정되어 있습니다.

### min-ohm-rate 설정

OHM(Over Head Message)은 가입자 모델로부터 관리의 목적으로 정보를 획득하는데 사용하는 방식입니다. 별도의 채널이 아닌 가입자 데이터 채널을 사용하여 정보를 획득하므로 가입자 회선사용에 영향을 줄 수 있습니다. 따라서 OHM 을 사용하는 경우에 가입자 데이터 채널을 사용하는 한도를 정해줄 필요가 있습니다. Min-ohm-rate 는 이에 대한 설정입니다. Min-ohm-rate 를 설정하려면 다음 커맨드를 사용하십시오.

명령어	Mode	기능
upstream min-ohm-rate <1-256>	line-profile	상향 데이터 중 ohm 으로 사용할 속도의 제한폭을 Kbps 단위로 설정합니다.
upstream min-ohm-rate <1-256>		하향 데이터 중 ohm 으로 사용할 속도의 제한폭을 Kbps 단위로 설정합니다.



**Note** U3000 시리즈는 기본적으로 상하향 min-ohm-rate 값이 각각 5Kbps 로 설정되어 있습니다.

### Alarm profile 설정

Alarm profile은 시스템에 오류가 발생하였을 때 SNMP Trap을 사용하여 사용자에게 이를 알리는 Alarm에 대한 내용을 하나의 정책으로 설정하여 서비스 포트에 적용할 수 있도록 하는 것입니다. 이는 서비스 특성에 따라 달라지는 오류 점검 기준을 각 포트에 쉽게 설정할 수 있기 때문에 편리합니다.

Alarm profile은 사용자가 설정한 각 에러의 임계값(Threshold)로 이루어집니다. “4.1.6 (1) 에러 발생 횟수 확인”의 기준과 동일하게 15분 단위로 각각의 에러를 확인하고, 사용자가 설정한 임계값을 넘어서면 SNMP Trap을 내보냅니다.

다음은 Alarm profile을 설정하는 방법입니다. Alarm profile 설정 모드로 들어가려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	Mode	기능
alarm-profile <i>profile-name</i>	Global	Alarm profile 설정 모드로 들어갑니다.

명령어	Mode	기능
-----	------	----



<code>thresh-15min-crc &lt;0-900&gt;</code>	CRC 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-ess &lt;0-900&gt;</code>	ESs 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-fecs &lt;0-900&gt;</code>	RECs 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-lofs &lt;0-900&gt;</code>	LOFS 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-lols &lt;0-900&gt;</code>	Alarm-profile LOLS 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-loss &lt;0-900&gt;</code>	
<code>thresh-15min-lprs &lt;0-900&gt;</code>	LPRs 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-sess &lt;0-900&gt;</code>	SES 지속 시간의 임계값을 설정합니다. 단위는 초입니다.
<code>thresh-15min-uass &lt;0-900&gt;</code>	UAS 지속 시간의 임계값을 설정합니다. 단위는 초입니다.

명령어	Mode	기능
<code>set alarm-profile <i>profile-name</i> add <i>port-number</i></code>	Interface	Profile의 내용을 포트에 적용합니다.

### 13.2.6. System profile 설정

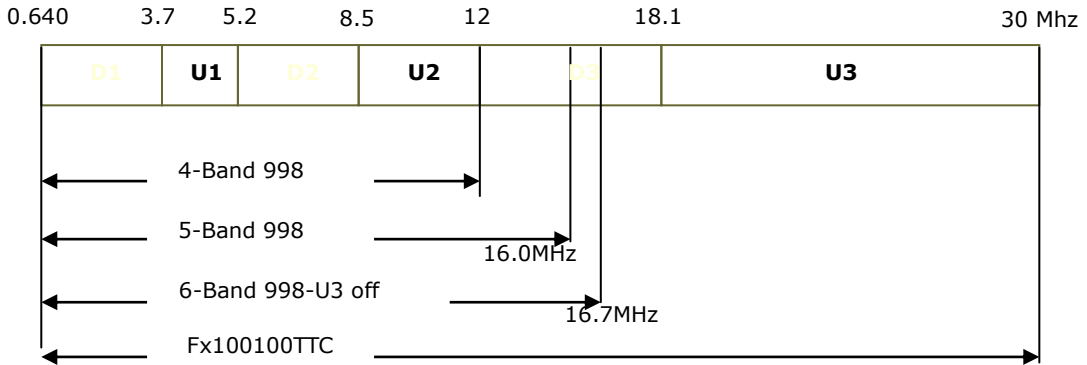
Line profile 이 가입자 포트 단위로 설정하는 것과는 달리 system profile 은 시스템 전반에 걸쳐 적용되는 항목들의 묶음입니다. System-profile 에 설정된 항목은 모든 포트에 공통적으로 적용되게 됩니다.

Profile의 내용을 설정합니다. 다음은 각 내용을 설정할 때 사용하는 명령어입니다.

명령어	Mode	기능
<code>adsl-safe-mode</code>		ADSL safe mode
<code>band-plan</code>		Band Plan
<code>bit-swap</code>	System-profile	Bit Swap
<code>ham-band</code>		HAM Band
<code>psd-mask-level</code>		PSD Mark Level
<code>rfi-band</code>		RFI Band
<code>tlan-safe-mode</code>		TLAN safe mode 의 적용 여부를 결정한다

#### 13.2.6.1. band-plan 설정

U3000 시리즈는 다양한 Band 를 하드웨어 변경 없이 지원 가능하기 때문에 사업자 서비스 조건에 맞는 다양한 속도를 지원할 수 있습니다.



다음은 band plan 을 설정할 때 사용하는 명령어입니다.

명령어	Mode	기능
band-plan 0		Band Plan 998 3 (BP1_998_3)
band-plan 1		Band Plan 998 3 (BP2_998_3 or BP998_3B_8_5M)
band-plan 2		Band Plan 998 4 (BP3_998_4 or BP998_4B_12M)
band-plan 3		Band Plan 997 3 (BP4_997_3 or BP997_3B_7_1M)
band-plan 4		Band Plan 997 3 (BP5_997_3)
band-plan 5		Band Plan 997 4 (BP6_997_4 or BP997_4B_7_1M)
band-plan 6		Band Plan Flex (BP7_MXU_3 or FLEX_3B_8_5M)
band-plan 7		Band Plan Flex (BP8_MXU_2)
band-plan 8		Band Plan 998 6 (BP998_6B_30A)
band-plan 9		Band Plan 998 2 (BP10_998_2 or BP998_2B_3_8M)
band-plan 10		Band Plan 998 2 (BP11_998_2)
band-plan 11		Band Plan 998 3 (BP998_3B_17000_4K)
band-plan 12	system-profile	Band Plan Flex (BP13_MXU_3)
band-plan 13	system-profile	Band Plan Flex (BP14_MXU_3)
band-plan 14		Band Plan 998 (BP15_998_138_32000)
band-plan 15		Band Plan 997 (BP16_997_4B_4P)
band-plan 16		Band Plan 998 138 4400 (BP17_998_138_4400)
band-plan 17		Band Plan 997 138 4400 (BP18_997_138_4000)
band-plan 18		Band Plan 997 32 4400 (BP19_997_32_4000)
band-plan 21		Band Plan 998 138 4400 Option Band
band-plan 22		Band Plan 997 138 4400 Option Band
band-plan 23		Band Plan 998 138 16000
band-plan 24		Band Plan 998 3B 8KHz
band-plan 25		Band Plan 998 138 17600
band-plan 26		Band Plan CH1 3
band-plan 27		Band Plan CH1 4

### 13.2.6.2. rfi-band 설정

HAM 대역의 유입 및 유출 잡음 영향을 줄이기 위해 표준이 정하는 아마추어 주파수 밴드를 사용하지 않도록 설정할 수 있습니다. RFI Band 는 13 개이며 복수로 사용하지 않도록 설정할 수 있습니다. Rfi-band 를 설정하려면 다음 명령어를 사용합니다.

명령어	Mode	기	능
rfi-band 1 {on off}		1.810 - 1.825 MHz:	ANNEX F
rfi-band 2 {on off}		1.810 - 2.000 MHz:	ETSI, T1E1
rfi-band 3 {on off}		1.9075 - 1.9125MHz:	ANNEX F
rfi-band 4 {on off}		3.500 - 3.575 MHz:	ANNEX F
rfi-band 5 {on off}		3.500 - 3.800 MHz:	ETSI
rfi-band 6 {on off}		3.500 - 4.000 MHz:	T1E1
rfi-band 7 {on off}		3.747 - 3.754 MHz:	ANNEX F
rfi-band 8 {on off}		3.791 - 3.805 MHz:	ANNEX F
rfi-band 9 {on off}		7.000 - 7.100 MHz:	ANNEX F, ETSI
rfi-band 10 {on off}		7.000 - 7.300 MHz:	T1E1
rfi-band 11 {on off}	System-	10.100 - 10.150 MHz:	ANNEX F, ETSI, T1E1
rfi-band 12 {on off}	profile	14.000 - 14.350 MHz:	ANNEX F, ETSI, T1E1
rfi-band 13 {on off}		18.068 - 18.168 MHz:	ANNEX F, ETSI, T1E1
rfi-band 14 {on off}		1.800 - 1.825 MHz:	HAM Band 1
rfi-band 15 {on off}		3.500 - 3.550 MHz:	HAM Band 2
rfi-band 16 {on off}		3.790 - 3.800 MHz:	HAM Band 3
rfi-band 17 {on off}		1.800 - 1.810 MHz:	RFI Notch
rfi-band 18 {on off}		21.000 - 21.450 MHz:	ANNEX F, ETSI, T1E1
rfi-band 19 {on off}		24.890 - 24.990 MHz:	ANNEX F, ETSI, T1E1
rfi-band 20 {on off}		28.000 - 29.100 MHz:	ANNEX F, ETSI, T1E1
rfi-band 21 {on off}		28.000 - 29.700 MHz:	ANNEX F, ETSI, T1E1
rfi-band all {on off}			ALL Bands

### 13.2.6.3. adsl-safe-mode, tlan-safe-mode 설정

adsl-safe-mode 는 ADSL과 간섭을, tlan-safe-mode는 TLAN 과의 간섭을 최소화하기 위한 설정입니다. 각각을 Enable로 설정하면 ADSL/TLAN 주파수 대역과 간섭이 일어나는 부분만 Blocking 시키게 되고 간섭이 일어나지 않는 주파수 대역은 사용하게 됩니다.

다음은 adsl-safe-mode, tlan-safe-mode 를 설정할 때 사용하는 명령어입니다.

명령어	Mode	기	능
adsl-safe-mode {enable disable}	System-profile	adsl-safe-mode 의 사용여부 설정	
tlan-safe-mode {enable disable}		tlan-safe-mode 의 사용여부 설정	



**Note**

adsl-safe-mode, tlan-safe-mode 를 enable 로 사용할 경우 특정 대역의 주파수를 blocking 시키므로 data rate 이 설정치 보다 낮게 나올 수 있으므로 기본적으로 disable 하여 사용하시기 바랍니다.

**13.2.6.4. psd-mask-level 설정**

전력 스펙트럼 밀도(PSD ; Power Spectrum Density)는 신호를 주파수 기준으로 나타낸 것으로 이를 조절하면 같은 주파수 대역에서 서로 간섭을 받지 않고 통신을 할 수 있습니다. PSD가 너무 커 버리면 이를 Noise로 인식하여 통신에 간섭이 발생할 수 있습니다. 그래서 이러한 PSD의 상한값(MASK-Level)을 표준으로 정하고 있습니다. U3000 시리즈는 VDSL 라인의 PSD MASK Level을 설정할 수 있습니다.

다음은 PSD MASK Level을 설정할 때 사용하는 명령어입니다.

명령어	Mode	기	능
psd-mask-level default-psd			Default PSD
psd-mask-level etsi-m1-cab			Etsi M1 cab
psd-mask-level etsi-m2-cab			Etsi M2 cab
psd-mask-level itu-t-annex-f			ITU-T Annex F (Japan)
psd-mask-level ansi-m1-ex	System-profile		Ansi M1 Ex
psd-mask-level ansi-m2-ex			Ansi M2 Ex
psd-mask-level etsi-m1-ex-p2			Atsi M1 Ex P1
psd-mask-level etsi-m2-ex-p2			Atsi M2 Ex P2
psd-mask-level ansi-m1-cab			Ansi M1 cab
psd-mask-level psd-china			Psd china
psd-mask-level etsi-m1-ex-p1			Etsi M1 Ex P1

**13.2.6.5. Ham-band 설정**

U3000 시리즈의 VDSL 포트가 사용하는 대역폭에는 Ham band가 포함되어 있습니다. 그러나, Ham band로 인해서 VDSL 라인에 간섭이 일어날 수 있습니다. U3000 시리즈 사용자는 Ham band로부터의 간섭을 피하기 위해 대역폭에 있는 Ham band를 사용하지 않도록 설정할 수 있습니다. 사용자가 선택한 Ham band를 사용하지 않도록 설정하려면 다음 명령어를 사용하십시오.

명령어	Mode	기	능
ham-band 1 {on off}		1.800 - 2.000 MHz:	Amateur Radio
ham-band 2 {on off}		2.173 - 2.191 MHz:	GMDSS
ham-band 3 {on off}		2.850 - 3.155 MHz:	Aeronautical Comm.
ham-band 4 {on off}		3.400 - 3.500 MHz:	Aeronautical Comm.
ham-band 5 {on off}		3.500 - 3.800 MHz:	Amateur Radio
ham-band 6 {on off}		3.800 - 4.000 MHz:	Aeronautical/Broadcasting

---

ham-band 7 {on off}	4.200 - 4.215 MHz: GMDSS
ham-band 8 {on off}	4.650 - 4.850 MHz: Aeronautical Comm.
ham-band 9 {on off}	5.450 - 5.730 MHz: Aeronautical Comm.
ham-band 10 {on off}	5.900 - 6.200 MHz: DRM Radio
ham-band 11 {on off}	6.300 - 6.320 MHz: GMDSS
ham-band 12 {on off}	6.525 - 6.765 MHz: Aeronautical Comm.
ham-band 13 {on off}	7.000 - 7.200 MHz: Amateur Radio
ham-band 14 {on off}	7.200 - 7.450 MHz: DRM Radio
ham-band 15 {on off}	8.405 - 8.420 MHz: GMDSS
ham-band 16 {on off}	8.815 - 9.040 MHz: Aeronautical Comm.
ham-band 17 {on off}	9.400 - 9.900 MHz: DRM Radio
ham-band 18 {on off}	10.005 - 10.100 MHz: Aeronautical Comm.
ham-band 19 {on off}	10.100 - 10.150 MHz: Amateur Radio
ham-band 20 {on off}	11.175 - 11.400 MHz: Aeronautical Comm.
ham-band 21 {on off}	11.600 - 12.100 MHz: DRM Radio
ham-band 22 {on off}	12.570 - 12.585 MHz: GMDSS
ham-band 23 {on off}	13.200 - 13.360 MHz: Aeronautical Comm.
ham-band 24 {on off}	13.570 - 13.870 MHz: DRM Radio
ham-band 25 {on off}	14.000 - 14.350 MHz: Amateur Radio
ham-band 26 {on off}	15.010 - 15.100 MHz: Aeronautical Comm.
ham-band 27 {on off}	15.100 - 15.800 MHz: DRM Radio
ham-band 28 {on off}	16.795 - 16.810 MHz: GMDSS
ham-band 29 {on off}	17.480 - 17.900 MHz: DRM Radio
ham-band 30 {on off}	17.900 - 18.030 MHz: Aeronautical Comm.
ham-band 31 {on off}	18.068 - 18.168 MHz: Amateur Radio
ham-band 32 {on off}	21.000 - 21.450 MHz: Amateur Radio
ham-band 33 {on off}	24.890 - 24.990 MHz: Amateur Radio
ham-band 34 {on off}	26.965 - 27.405 MHz: CB Radio
ham-band 35 {on off}	28.000 - 29.700 MHz: Amateur Radio
all {on off}	1~35 의 모든 대역에 대해 설정합니다.

---

### 13.2.8. Interface 설정

특정 interface에 VDSL과 관련된 설정을 하는 방법입니다

Interface에 관련된 설정을 하기 위해서는 interface 설정 모드로 들어가야 합니다.

명령어	Mode	기능
interface <i>IFNAME</i>	Global	Interface 설정 모드로 들어갑니다.

interface 모드에서 VDSL에 관련된 정보를 설정합니다. 다음은 각 내용을 설정할 때 사용하는 명령어입니다.

명령어	Mode	기능
cpe		Interface에 연결된 가입자 모뎀을 관리합니다.
service-alarm-profile		Interface에 적용할 alarm-profile을 설정합니다
service-line-profile	Line-profile	Interface에 적용할 line-profile을 설정합니다
vdsl-custom-set		VDSL 포트에 관련된 stream의 값을 설정합니다. 이 설정으로 line-profile에서 설정된 값이 아닌 이 값이 사용됩니다

## 13.3. VDSL 설정 정보 확인

### 13.3.1. Alarm-profile 정보 확인

설정된 alarm-profile의 정보를 확인합니다.

명령어	Mode	기능
Show alarm-profile PROFILE_NAME	Enable / Alarm-profile	설정된 alarm-profile의 정보를 확인합니다.

```

VDSL2#1# show alarm-profile

VDSL Alarm Profile
-----
Alarm Profile Name      : DEFVAL
Thresh 15min FECs      : 0
Thresh 15min ESs       : 0
Thresh 15min SESSs     : 0
Thresh 15min LOFs      : 0
Thresh 15min LOSs      : 0
Thresh 15min LPRs      : 0
Thresh 15min LOLs      : 0
Thresh 15min LOMs      : 0
Thresh 15min UASs      : 0
Thresh 15min CRC Count : 0
-----
Alarm Profile Name      : vd-al
Thresh 15min FECs      : 0
Thresh 15min ESs       : 0
Thresh 15min SESSs     : 0
Thresh 15min LOFs      : 0
Thresh 15min LOSs      : 0
Thresh 15min LPRs      : 0

```

```

Thresh 15min LOLs      : 0
Thresh 15min LOMs     : 0
Thresh 15min UASs     : 0
Thresh 15min CRC Count : 0
    
```

### 13.3.2. line-profile 정보 확인

설정된 line-profile의 정보를 확인합니다.

명령어	Mode	기능
Show line-profile PROFILE_NAME	Enable / line-profile	설정된 line-profile의 정보를 확인합니다.

```

VDSL2#1# show line-profile

VDSL Line Profile
-----
Profile Name           : DEFVAL
Line Type              : Auto Detect All xDSL
Option Band Plan      : (0) Exclude Option(USO) Band
Band Modifier TX      : (1) All Tones On
Band Modifier RX      : (1) All Tones On
Rate Adaptation Mode  : StartUp
  Up Slow Rate Ratio   : 0
  Down Slow Rate Ratio : 0
  Up Slow Max Rate     : 200000 Kbps
  Up Slow Min Rate     : 0 Kbps
  Down Slow Max Rate   : 200000 Kbps
  Down Slow Min Rate   : 0 Kbps
  Up Slow Max Interdelay : 1.0 ms (milliseconds)
  Down Slow Max Interdelay : 1.0 ms (milliseconds)
  Up Maximum Margin    : 127.5 dB
  Down Maximum Margin  : 127.5 dB
  Up Min Noise Margin  : 5.0 dB
  Up Target Noise Margin : 6.0 dB
  Down Min Noise Margin : 5.0 dB
  Down Target Noise Margin : 6.0 dB
  Up Max Power         : 63.75 dBm
  Down Max Power       : 63.75 dBm
  Up Slow Min Protection : 0.000 ms (milliseconds)
  Down Slow Min Protection : 0.000 ms (milliseconds)
Power Mode             : (2) 14.5 dBm
IFE RX Filter          : (0) Internal Filter
IFE TX Filter          : (0) Internal Filter
TCM (Trellis Code Modul.) : disable
G.Handshake            : V43 A43
PBO Config             : disable
    
```

PBO Length	: 100 meters
-----	
Profile Name	: 100M
Line Type	: Manual Customized
	VDSL ANSI
	VDSL2 ITU G993 2 8D
	VDSL2 ITU G993 2 12A
	VDSL2 ITU G993 2 17A
	VDSL2 ITU G993 2 30A
Option Band Plan	: (2) Annex M 25 KHz ~ 276 KHz (6-64)
Band Modifier TX	: (1) All Tones On
Band Modifier RX	: (1) All Tones On
Rate Adaptation Mode	: StartUp
Up Slow Rate Ratio	: 0
Down Slow Rate Ratio	: 0
Up Slow Max Rate	: 200000 Kbps
Up Slow Min Rate	: 0 Kbps
Down Slow Max Rate	: 200000 Kbps
Down Slow Min Rate	: 0 Kbps
Up Slow Max Interdelay	: 1.0 ms (milliseconds)
Down Slow Max Interdelay	: 1.0 ms (milliseconds)
Up Maximum Margin	: 127.5 dB
Down Maximum Margin	: 127.5 dB
Up Min Noise Margin	: 5.0 dB
Up Target Noise Margin	: 6.0 dB
Down Min Noise Margin	: 5.0 dB
Down Target Noise Margin	: 6.0 dB
Up Max Power	: 63.75 dBm
Down Max Power	: 63.75 dBm
Up Slow Min Protection	: 0.000 ms (milliseconds)
Down Slow Min Protection	: 0.000 ms (milliseconds)
Power Mode	: (2) 14.5 dBm
IFE RX Filter	: (2) U1 External Filter
IFE TX Filter	: (2) U1 External Filter
TCM (Trellis Code Modul.)	: disable
G.Handshake	: V43 B43
PBO Config	: disable
PBO Length	: 100 meters
-----	



### 13.3.3. system-profile 정보 확인

설정된 system-profile의 정보를 확인합니다.

명령어	Mode	기능
Show system-profile PROFILE_NAME	Enable / system-profile	설정된 system-profile의 정보를 확인합니다.

```

VDSL2#1# show system-profile

VDSL System Profile
-----
Configured                Current Working
-----
Band Plan                  : (8) Band Plan 998 6 (BP998_6B (Same to left)
PSD Mask Level            : (11) PSD K (Korean M1 FTTCab) (Same to left)
TLAN Safe Mode            : disable (Same to left)
ADSL Safe Mode            : disable (Same to left)
Bit Swap                   : disable (Same to left)
HAM Band                   : All Bands Disable (Same to left)
RFI Band                   : All Bands Disable (Same to left)
-----

```

### 13.3.4. Interface 정보 확인

Interface에 설정된 VDSL에 관련된 정보를 확인합니다.

명령어	Mode	기능
show port alarm-profile		Port에 적용된 alarm-profile 정보를 보여줍니다
show port bit-loading		Port에 적용된 bit-loading 정보를 보여줍니다
show port cpe-status		Port에 연결된 CPE의 상태 정보를 보여줍니다
show port cpe-version		Port에 연결된 CPE의 버전과 ID 등에 관한 정보를 보여줍니다
show port line-ewl		각 port의 EWL(Eletronic Wire Length)의 추정치 정보를 보여줍니다
show port line-profile	Enable	Port에 적용된 line-profile 정보를 보여줍니다
show port line-rate		각 port의 line-rate 정보를 보여줍니다
show port line-snr		각 port의 SNR, Authentication, Tx Power에 관한 정보를 보여줍니다
show port vdsl-chan-perf-count		각 port의 시간에 바탕을 둔 VDSL CHAN PERF 통계 정보를 보여줍니다
show port vdsl-major		각 port의 주요한 item에 바탕을 둔 VDSL PERF 통계 정보를 보여줍니다
show port vdsl-perf-count		각 port의 VDSL PERF 통계 정보를 보여줍니다
show port vdsl-perf-second		각 port의 시간에 바탕을 둔 VDSL PERF 통계 정보를 보여줍니다
show port vdsl-ptmf		각 port의 VDSL PTMP 통계 정보를 보여줍니다