

EJBD-000324

Ed. 01

OpticGear™

OG-1100 운용 매뉴얼



저작권

이 매뉴얼의 저작권은 삼성전자(주)에 있습니다.

이 매뉴얼은 삼성전자(주)의 서면동의 없이 어떤 형태로도 재생산·배포·변경할 수 없습니다.

등록상표

이 매뉴얼에 언급된 등록상표는 그 해당 회사 소유의 등록상표입니다.

제품을 설치 및 운용하기 전에 이 매뉴얼을 반드시 읽고, 매뉴얼의 내용에 따라 제품을 안전하고 올바르게 사용하여 주십시오.

이 매뉴얼은 제품의 기능 향상, 설계 변경에 따라 내용이 수정될 수 있습니다. 수정된 매뉴얼이 필요하거나 매뉴얼의 내용에 대해 궁금한 사항이 있으면 아래의 주소나 홈페이지로 문의 바랍니다.

주소 : 경기도 수원시 영통구 매탄3동 동수원우체국 사서함 105호 정보통신연구소 18층 Document Center ☎ 442-600

홈페이지 : <http://www.samsungdocs.co.kr>

제품에 대한 불만 사항이나 요청 사항이 있으면 **Call Center** 로 문의 바랍니다.

전화 : 1588-4141

들어가며

매뉴얼 소개

이 매뉴얼은 OG-1100 을 설치하고, 네트워크 환경을 설정하여 운영하는 방법에 대해서 설명합니다.

매뉴얼 구성

이 매뉴얼은 3 장(章), 약어, 찾아보기로 구성되어 있습니다.

1 장. 사용자 인터페이스 에서는

시스템 운영자가 OG-1100 의 운용 환경을 설정하고 처음 시작하기 위해 필요한 정보에 대해서 설명합니다.

2 장. 시스템 초기환경 설정 에서는

명령어를 이용하여 시스템의 초기 환경을 설정하는 방법에 대해서 설명합니다.

3 장. 시스템 설정 및 조회 에서는

명령어를 이용하여 시스템 운용 환경을 설정하고 조회하는 방법에 대해서 설명합니다.

약어 에서는


이 매뉴얼에 사용하는 약어에 대한 풀이를 제공합니다.

찾아보기 에서는

이 매뉴얼의 주요 정보에 대한 색인을 제공합니다.

기호 설명

다음은 이 매뉴얼에서 사용되는 기호입니다. 이 기호와 함께 제공되는 정보는 시스템을 안전하고 올바르게 사용하기 위해 반드시 숙지해야 합니다.

	참고할 내용
참고	본문 내용에 대한 부가적인 정보를 제공합니다.

화면 출력 표시

- 콘솔 화면에 출력되는 내용은 본문과 구별하기 위해 박스를 사용하며, ‘Courier New’ 폰트로 표기합니다.
- 사용자가 콘솔 화면에 직접 입력하는 값은 진한 ‘**Courier New**’ 폰트로 표기합니다.

관련 자료

OpticGear 시스템 설명서

OpticGear 시스템 설명서는 OpticGear 시스템에 대한 기본적인 소개, 하드웨어 및 기능, 시스템 유닛, 주요기술 등 OpticGear 시스템을 이해하기 위해 필요한 모든 정보에 대해 설명합니다.

OpticGear CLI 설명서

OpticGear CLI 설명서에는 OpticGear 시스템에서 제공하는 명령어와 입력한 명령어에 대한 결과로 출력되는 메시지에 대해 설명합니다.

OpticGear 설치 매뉴얼

OpticGear 설치 매뉴얼은 OpticGear 시스템의 각 형상별로 하드웨어 설치 절차, 케이블 연결 절차 등 OpticGear 시스템을 설치하는 방법에 대해 절차별로 설명합니다.

OpticGear AceMAN 사용자 매뉴얼

OpticGear AceMAN 사용자 매뉴얼은 OpticGear 시스템의 EMS 시스템인 AceMAN의 운용방법에 대해 설명합니다.

OpticGear 유지보수 매뉴얼

OpticGear 유지보수 매뉴얼은 OpticGear 시스템의 유지보수 방법에 대해서 설명합니다.

연혁

판차	작성일	비고
00	2006. 03.	최초 작성
01	2006. 05.	분당 TP 용으로 내용 보완



이 면에는 내용이 없습니다.

목차

들어가며	I
매뉴얼 소개.....	I
매뉴얼 구성.....	I
기호 설명	II
화면 출력 표시.....	II
관련 자료	II
연혁	III
1 장. 사용자 인터페이스	1-1
1.1 CLI 명령어의 편집과 도움말 기능.....	1-1
1.1.1 명령어 문법의 이해	1-1
1.1.2 명령어 문법 도움말	1-2
1.1.3 단축 명령어 입력.....	1-4
1.1.4 명령어 기호.....	1-5
1.1.5 명령어 라인 편집 키 및 도움말	1-6
1.2 시스템 명령어 모드	1-7
1.3 OG-1100 시스템 가동	1-8
1.3.1 사용자 인터페이스	1-8
1.3.2 콘솔 연결	1-8
1.3.3 Telnet 연결	1-9
1.3.4 시스템 초기 화면 및 가동	1-9
1.3.5 SNMP Network Manager 를 통한 연결	1-10
1.4 비밀번호 설정.....	1-11
1.4.1 Enable 모드 비밀번호 설정	1-11
1.4.2 비밀번호 encryption 설정.....	1-11
1.4.3 운영자 비밀번호 설정	1-12
1.5 Hostname 설정	1-12
1.6 콘솔/Telnet 환경 설정	1-13
1.6.1 세션 설정	1-13
1.6.2 타임 아웃 설정.....	1-14
1.6.3 인증 방법 설정.....	1-14

1.7	현재 세션 환경 설정.....	1-16
1.8	SNMP	1-16
1.9	Access Permit 과 ACL	1-17
1.9.1	Access Permit 설정	1-17
1.9.2	ACL 설정	1-20
1.10	Management IP 설정	1-21
1.11	운영자 설정	1-22
1.11.1	운영자 추가 및 삭제	1-22
1.11.2	운영자 privilege 변경	1-22
1.11.3	운영자 비밀번호 변경	1-23
1.12	관리자 인증 설정	1-23
1.12.1	관리자 인증 리스트 설정	1-23
1.12.2	관리자 인증 서버 설정	1-25
1.13	세션 강제 종료	1-28
1.14	배너 설정	1-28
1.15	외부 접속	1-29
1.16	시스템 조회	1-29
1.16.1	시스템 접속 정보 조회	1-29
1.16.2	명령어 이력 조회	1-30
1.17	소프트웨어 업그레이드하기	1-31
1.18	설정정보 파일 관리하기	1-32
1.19	성능 정보 collection 및 monitoring 설정	1-32
1.20	Rmon 정보 설정	1-33
1.21	Rmon 및 pm 정보 조회	1-34
1.22	pm count 삭제 및 rmon log 삭제	1-35

2 장. 시스템 초기 환경 설정	2-1
--------------------------	------------

2.1	랙의 정보 설정 및 조회.....	2-1
2.2	시스템의 정보 설정 및 조회	2-2
2.3	시스템의 자원 상태 설정 및 조회	2-3
2.4	시스템의 경보 등급 설정 및 발령 조회.....	2-4
2.5	가칭 경보 설정 및 조회.....	2-6
2.6	SLOT 상태 설정 및 조회.....	2-6
2.7	PON OLT, ONU/ONT 의 상태 설정/조회	2-8
2.8	PON 의 ONT 등록 및 조회	2-9
2.8.1	ONT 의 등록 및 조회	2-9

2.8.2	ONU/ONT 의 정보 변경 및 삭제	2-10
2.9	SWU 포트 설정 및 상태 조회	2-11
2.9.1	물리적 포트 상태 변경 및 조회	2-12
2.9.2	물리적 포트상태 변경	2-13
2.9.3	포트의 흐름 제어 (IEEE 802.3x) 설정	2-13

3 장. 시스템 설정 및 조회

3-1

3.1	PON 환경 설정.....	3-1
3.1.1	PON OLT 환경 설정	3-1
3.1.2	PON ONU 환경 설정	3-8
3.2	Layer 2 환경 설정	3-20
3.2.1	VLAN (Virtual LAN).....	3-20
3.2.2	STP/RSTP	3-24
3.2.3	Trunk/LACP	3-26
3.2.4	MAC Filtering 설정	3-34
3.2.5	mirroring 설정.....	3-35
3.2.6	tcpdump 설정	3-36
3.2.7	packet sampling.....	3-37
3.3	Layer 3 환경 설정	3-40
3.3.1	IP 어드레스/subnet 설정 및 조회	3-40
3.3.2	Secondary IP 어드레스/subnet 설정 및 조회.....	3-41
3.3.3	IP 어드레스/subnet 삭제.....	3-41
3.3.4	Static ARP 설정 및 ARP 조회	3-42
3.3.5	Static routing 설정 및 조회	3-43
3.3.6	ARP Proxy 설정 및 조회	3-46
3.4	멀티캐스팅 환경 설정.....	3-47
3.4.1	IGMP snooping	3-47
3.4.2	PIM-SM 설정 및 조회.....	3-59
3.4.3	IGMP 설정 및 조회	3-73
3.4.4	Static Join Group 설정 및 조회	3-78
3.5	DHCP 환경 설정.....	3-80
3.5.1	DHCP server 설정 및 조회	3-80
3.5.2	DHCP relay agent 설정 및 조회	3-84
3.5.3	DHCP blocking 설정 및 조회.....	3-86
3.5.4	DHCP 통계 정보 설정 및 조회.....	3-88
3.6	QoS 환경 설정.....	3-89
3.6.1	QoS 개요	3-89
3.6.2	QoS 정책 적용 순서.....	3-91

3.7 Security 환경 설정	3-116
3.7.1 DoS Attack Filter.....	3-117
3.7.2 Netbios Filter	3-120
3.7.3 Martian Filter.....	3-121
3.7.4 Auto Rate-Limit (Broadcast/Multicast)	3-121
3.7.5 ICMP Unreachable 제한 기능	3-123
3.7.6 TCP rst 패킷 제한 기능	3-123
3.7.7 DHCP 패킷 필터.....	3-123
3.7.8 IPX 패킷 필터	3-124
3.7.9 Security 정보 조회.....	3-124

약어

I

A ~ O	I
P ~ W	II

찾아보기

I

ㄱ ~ ㄴ	I
ㄷ ~ ㄹ	II
ㅁ ~ ㅎ	III
ㅑ ~ ㅓ	IV
ㅕ ~ ㅗ	V

그림 목차

그림 3.1 QoS 구조.....	3-89
그림 3.2 Policy-map 구조.....	3-91

1장. 사용자 인터페이스

이 장은 다음과 같이 시스템 운영자가 OG-1100 의 운용 환경을 설정하고 처음 다루기 시작할 때 필요한 정보를 제공합니다.

- 편집 및 도움말 기능
- 명령어 모드의 이해
- 시스템가동
- OG-1100 사용자 인터페이스
- 로그인과 비밀번호의 설정
- SNMP 환경설정
- 스위치의 파일 및 환경 설정의 보기와 저장

1.1 CLI 명령어의 편집과 도움말 기능

명령어 편집기의 편집 기능과 도움말 기능에 대하여 설명합니다.

1.1.1 명령어 문법의 이해

운영자가 시스템 운영을 위한 명령어를 입력하는 단계를 설명합니다.(명령어 인터페이스 사용에 대한 자세한 정보는 다음 장에서 설명합니다.)

CLI 를 사용하기 위해서는 다음의 단계를 거칩니다.

- 1) 명령어 프롬프트에서 명령어를 입력하기 전에, 먼저 적절한 권한을 가지고 있는 프롬프트 수준에 있는지 먼저 확인합니다.(대부분의 환경 설정 관련 명령어들은 시스템 운영자 수준의 권한을 필요로 합니다.)수행하고자 하는 명령어를 입력합니다. 만약 명령어가 파라미터를 가지고 있으면 파라미터를 입력합니다.
- 2) 명령어에 따르는 파라미터에 따라서 숫자, 문자열, 또는 어드레스 등이 값으로 설정됩니다.
- 3) 명령어 입력 완료 후 [Enter]키를 눌러서 명령어를 실행합니다.



참고

CLI 명령어 입력할 때 출력 메시지

명령어를 입력하고 실행했을 때 ‘% Command incomplete.’ 메시지가 나오는 경우가 있습니다. 이는 명령어 실행에 필요한 파라미터가 제대로 입력되지 않았음을 의미하며, 입력한 명령어는 실행되지 않습니다. 이 때 위쪽 화살표를 누르면 마지막에 입력한 명령어 표시됩니다.

다음은 명령어 파라미터를 정상적으로 입력하지 않은 경우입니다.

```
OG1100# show
% Incomplete command.

OG1100#
```

1.1.2 명령어 문법 도움말

CLI 는 명령어 문법 도움말 기능을 자체적으로 내장하고 있습니다. 시스템 운영자는 명령어 입력 중 완전한 문법을 모르는 경우, 어느 위치에서든지 ‘?’를 입력해서 도움말을 볼 수 있습니다.

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

다음은 명령어 프롬프트에서 ‘help’ 명령어를 입력하면 다음과 같이 실행됩니다.

```
OG1100# help
ZebOS CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g., 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g., 'show ve?'.)

OG1100#
```

전체 도움말 기능을 ‘show’ 명령어를 통하여 보면 다음과 같습니다. ‘show’ 명령어 다음에 공백 문자와 함께 ‘?’를 입력하면 운영자가 입력 할 수 있는 파라미터와 값의 리스트가 출력됩니다. 그리고 다시 ‘OG1100# show’ 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기합니다. 운영자 입력에서 ‘?’는 화면에 표시되지 않습니다.

OG1100# show	
Aaa	Authentication, Authorization and Accounting
access-list	List IP access lists
access-permit	List access permit lists
aco	ACO control state
alarm	Alarms
arp	Address Resolution Protocol (ARP)
auto-negotiation	Auto Negotiation
bcn	Show daemon connection status
class-map	class-map information
date	Show system time
debugging	Debugging functions (see also 'undebug')
dhcp-filter	DHCP filter
dhcpcd	DHCP daemon
dot1x	IEEE 802.1X Port-Based Access Control
duplex	Port Duplex
dyncell	Dyncelllimit Configuration information
etherchannel	LACP etherchannel
fdb	Display forwarding database information
flowcontrol	IEEE 802.3x Flow Control
history	Display the session command history
interface	Interface status and configuration
ip	Internet Protocol (IP)
jumbo	Jumbo Frame Status
lACP	LACP commands
list	Show command lists
mirror	Port Mirroring
multicast-filter	multicast-filter
nsm	NSM
ntp	Network time protocol
packet	packet dump debugging
policy-map	policy-map information
pon	PON Information
port	port commands
port-bridging	Display one port bridging n
portstat	Ports Configuration
privilege	Show current privilege level
process	Process
rack	rack configuration
rmon	rmon configuration
route-map	route-map information
router-id	Router ID
running-config	Current Operating configuration
security	Security Configuration information
service-policy	Apply policy-map to interface
sflow	show sflow status
snmp-config-block	SNMP config mode blocking
software	software
spanning-tree	spanning-tree Display spanning tree information
speed	Port Speed
startup-config	Contents of startup configuration
static-channel-group	Static channel commands
statistics	statistics

storm-control	The layer2 interface
subscriber	Subscriber Switch Information
syslog	syslog
system	system information
timezone	time zone
traffic-class-table	Display traffic class table
traffic-monitor	show traffic-monitor capture status
uipc	Configure UIPC inband
user-priority	Display the default user priority associated with the layer2 interface
users	Display information about connection
vlan	Display VLAN information
vrrp	VRRP information
OG1100# show	

부분 도움말 기능을 ‘show’ 명령어를 통하여 보면 다음과 같습니다. ‘show’ 명령어 입력 후 공백 없이 ‘?’를 입력하면 다음과 같이 ‘show’ 명령어에 대한 설명이 표시되고 커서가 깜박이면서 다음 명령 입력을 기다립니다.


```
OG1100# show?
show Show running system information
OG1100# show_
```

위 예에서 운영자는 VLAN 의 상태를 알고 싶지만 정확한 명령어를 모르는 경우에는 ‘v’를 입력하고, ‘?’를 입력하면 ‘v’로 시작하는 서브 명령어의 리스트가 다음과 같이 출력됩니다. 물론 운영자가 입력한 명령은 다시 표시가 되면서 커서가 깜박이면서 입력을 대기합니다.

```
OG1100# show v
vlan DisplayVLAN information
vrrp VRRP information
OG1100# show v_
```

1.1.3 단축 명령어 입력

CLI 는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행을 지원합니다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령어를 수행합니다.



참고 단축 명령어를 사용할 때, 시스템 운영자는 OG-1100 시스템이 명령어를 구분하여 인식할 수 있도록 충분히 입력해야 합니다. ‘% Ambiguous command.’라는 메시지를 받는 경우가 있습니다. 이것은 해당 모드에 입력한 문자와 Prefix 가 같은 하나 이상의 명령어가 있음을 의미합니다.

```

OG1100#show s
% Ambiguous command : "show s"

OG1100#show s
security      service-policy      sflow      snmp-config-block
software      spanning-tree        speed      startup-config
static-channel-group statistics    storm-control subscriber
syslog        system
OG1100#show s
    
```

1.1.4 명령어 기호

이 설명서에서 설명하는 시스템 명령어 문법에는 다양한 기호가 사용됩니다. 명령어 심벌은 명령어 수행을 위해서 파라미터들이 어떻게 입력되어야 하는 지를 설명합니다. 시스템 명령어 문법에 적용된 기호와 각각의 기호의 의미는 다음과 같습니다.



기호	이름	설명
<>:	Angle brackets	<ul style="list-style-type: none"> - 명령어 문법에서 하나의 변수 또는 값 의미(이렇게 표현된 파라미터는 반드시 입력을 해야 함) - 예를 들어, 다음과 같은 명령어가 있을 때 access-list <1-99> {deny permit} address 표준 IP access control list 번호는 <1-99> 사이의 값으로 반드시 입력해야 합니다.
{ }:	Braces	<ul style="list-style-type: none"> - 명령어 문법에서 사용되는 파라미터 또는 값의 리스트로 시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 함 - 예를 들어, 다음과 같은 명령어가 있을 때 router {rip ospf} 시스템 운영자는 라우팅 프로토콜로서 RIP 또는 OSPF 중의 하나를 반드시 명시해야 합니다.
[]:	Square brackets	<ul style="list-style-type: none"> - 명령어 문법에서 사용되는 파라미터 또는 값의 리스트로 시스템 운영자는 리스트에 포함된 항목 중에서 필요한 항목을 선택적으로 입력(경우에 따라서는 하나도 입력을 하지 않을 수도 있습니다.) - 예를 들어, 다음과 같은 명령어가 있을 때 show port [iftype] 인터페이스의 형태를 정의하지 않을 수도 있습니다.
():	Parentheses	<ul style="list-style-type: none"> - 명령어 문법에서 사용되는 파라미터 또는 값의 리스트로 시스템 운영자는 리스트에 포함된 항목 중 하나를 선택하거나 아무것도 선택하지 않을 수 있음 - 예를 들어, 다음과 같은 명령어가 있을 때 show history (log) 시스템 운영자는 log 를 선택하여 입력하거나 아무것도 입력하지 않을 수 있습니다.

(계속)

기호	이름	설명
:	Vertical bar	파라미터 리스트에서 상호 배타적인 항목들을 표현
<i>Italic 체</i>	-	입력할 변수들
Bold 체	-	운영자가 입력해야 하는 명령어
A.B.C.D	-	IP 어드레스 또는 서브넷 마스크를 의미
A.B.C.D/M	-	IP prefix 를 의미(예. 192.168.0.0/24)

1.1.5 명령어 라인 편집 키 및 도움말

CLI 명령어가 제공하는 명령어 라인 편집 명령과 도움말 기능은 다음과 같습니다.

명령어	설명
[Ctrl] + [A]	커서를 줄의 처음으로 이동
[Ctrl] + [E]	커서를 줄의 끝으로 이동
[Ctrl] + [B]	커서를 한 단어 뒤로 이동
[Ctrl] + [F]	커서를 한 글자 앞으로 이동
[Ctrl] + [D]	한 글자를 삭제
Backspace	커서 앞의 한 글자를 삭제
[Ctrl] + [K]	현재 커서로부터 줄의 끝까지 문자를 삭제
[Ctrl] + [U]	현재 커서로부터 줄의 처음까지 문자를 삭제
[Ctrl] + [Z]	환경 설정 모드를 끝내고 privileged 모드로 전환
Tab	- 명령어의 일부분을 치고 [tab]을 치면 그 prompt 에서 같은 prefix 를 가진 명령어가 여러 개 있을 경우 리스트를 표시 - 한 개의 명령어만 있을 경우 명령어 나머지 부분을 완성
[Ctrl] + [P] 또는 	마지막 입력 명령어부터 차례 대로 20 개까지의 명령어 입력에 대한 이력을 표시
[Ctrl] + [N] 또는 	다음 명령어를 표시
?	- prompt 상에서 사용 가능한 명령어의 리스트와 설명을 표시 - 명령어 다음에 '?'를 쳤을 경우, 해당 명령어 다음에 입력해야 할 파라미터 리스트를 표시 - 부분적인 명령어에 바로 붙여서 '?'를 입력했을 경우 같은 prefix 를 가진 명령어의 리스트를 표시
Return 또는 Spacebar 또는 Q	-- More -- 에서 Return 키를 누르면 다음 한 line 이 표시 - Spacebar 를 누르면 다음 페이지가 표시되며, Q 를 누르면 종료하고 prompt 상태로 전환

1.2 시스템 명령어 모드

CLI 명령어는 다음과 같이 다양한 시스템 명령어 모드를 지원합니다. 각 시스템 명령어 모드마다 운영자에게 주어지는 권한에는 차이가 있습니다.

모드	프롬프트	설명
User 모드	OG1100 >	보통 통계 정보를 디스플레이
Enable 모드	OG1100 #	Show 나 debug 명령어를 사용
Config 모드	OG1100(config) #	시스템의 환경 설정 값을 글로벌 하게 변경
Interface 모드	OG1100(config-if)#	시스템 인터페이스 설정값을 개별적으로 변경
System 모드	OG1100(config-sys)#	시스템 slot 및 management 값을 개별적으로 변경
Pon 모드	OG1100(config-pon)#	PON 에 관계된 값을 개별적으로 변경
QoS 모드	OG1100(config-qos)#	SWU 의 QoS 를 개별적으로 변경
security 모드	OG1100(config-security)#	SWU 의 security 를 개별적으로 변경
Line 모드	OG1100(config-line)#	콘솔이나 vty(Telnet)에 대한 환경 설정 변경



참고

명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 OG-1100 시스템의 이름을 호스트 이름으로 사용합니다. 이 설명서에서는 'OG1100' 프롬프트를 공통의 호스트 이름으로서 사용합니다.

시스템 운영자는 OG-1100 시스템의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게 됩니다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 와 있는 지를 알려줍니다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 확인 해야만 합니다.

아래는 스위치의 명령어 모드 사이의 이동 방법을 설명합니다.

명령어	설명
enable	User 모드에서 Privileged 모드로 이동 (Privileged 모드의 비밀번호 입력 필요)
disable	Privileged 모드에서 User 모드로 이동
configure terminal	Privileged 모드에서 Config 모드로 이동
line {console vty <1-4> [<1-4>]}	Config 모드에서 Line 모드로 이동
exit	이전의 모드로 이동
[CTRL] + [Z] 또는 end	어느 모드에서든 Privileged 모드로 이동 (User 모드에서는 이동하지 않습니다.)

1.3 OG-1100 시스템 가동

OG-1100 시스템은 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS image 를 찾아서 메모리에 로드 하여 시스템을 시작합니다. 시스템 부팅이 완료되면 플래시 메모리 에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩합니다.

1.3.1 사용자 인터페이스

시스템 운영자는 스위치의 환경을 설정하고, 환경 설정을 검증하고, 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속합니다. 스위치에 접속하기 위한 가장 기본적인 방법은 OG-1100 시스템이 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것입니다.(Out-of-band management).

시스템로 연결하는 또 다른 방법은 원격지에서 telnet 프로그램을 이용하는 것입니다. 원격지에서 telnet 연결을 위한 별도의 포트 및 별도의 포트를 지원하지는 않고 서비스 포트를 통하여 접속합니다.(Out-of-band management /In-band management).

운영자는 아래의 방법을 사용하여 OG-1100 시스템을 관리할 수 있습니다.

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

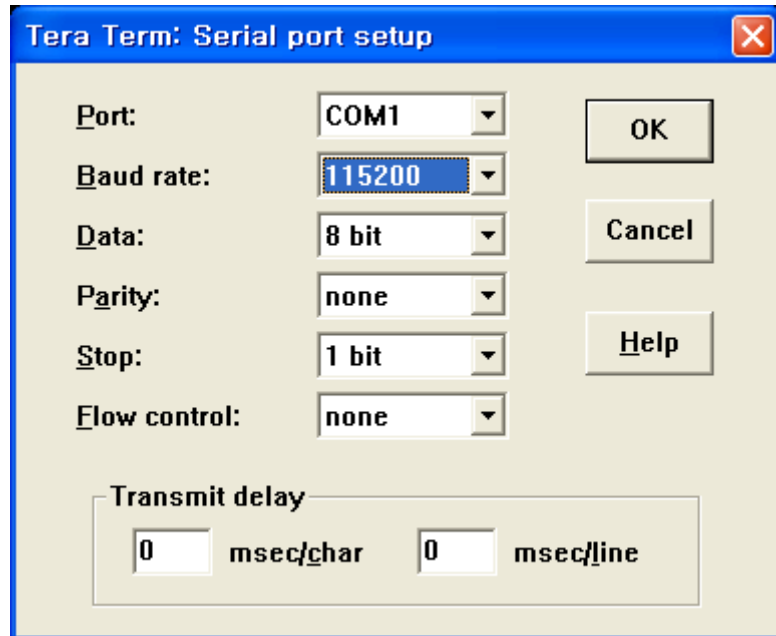
OG-1100 시스템은 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원합니다.

- 1 개의 MgmT(RJ45) 및 콘솔 연결
- 최대 5 개의 telnet 연결

1.3.2 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능합니다. 이를 위하여 운영 단말(또는 terminal emulation 소프트웨어가 탑재된 PC)은 9 핀, RS-232 DB9 포트를 지원해야 합니다. OG-1100 시스템의 콘솔 포트는 전면에 있습니다.

Baud rate 을 ‘115200’에 맞추어야 합니다. 아래 그림은 ‘Tera Term Pro’ 프로그램을 사용한 예입니다.



1.3.3 Telnet 연결

시스템 운영자는 TCP/IP 및 telnet 접속 기능을 가지고 있는 PC/워크스테이션을 통하여 OG-1100 시스템에 접속할 수 있습니다. Telnet 을 사용하기 위하여, 운영자는 telnet 비밀번호를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 어드레스를 가지고 있어야 합니다.

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

Telnet 연결이 성공적으로 설정되며 사용자 비밀번호를 입력 프롬프트가 실행되며, telnet 사용자 비밀번호를 입력하면 됩니다.

1.3.4 시스템 초기 화면 및 가동

콘솔 및 telnet 이 연결이 성공하면, 운용자 ID 및 Password (슈퍼 유저는 ID 는 'admin', Password 는 'epon' 으로 초기화되어 있음)를 차례로 입력한 후, [Enter] 키를 치면 '>' 프롬프트가 나타나며, User Exec Mode 로 접속됩니다.

Exec mode 는 user level 에서 실행되며 사용가능한 명령조회를 위해 '?' 를 내리면 리스트가 조회됩니다.

Exec_mode 에서 'enable' 명령어를 입력하면, 프롬프트가 '#' 으로 변하며 Operating parameters 들에 대한 입력이 가능한 enable mode 가 됩니다. 시스템의 모든 설정에 대한 정보는 enable mode 에서 조회가 됩니다.

시스템에 대한 새로운 설정을 하거나 기존 설정을 수정하려면 Global Configuration mode 로 변환해야 하며, 이 모드는 enable 모드에서 'configure terminal' 명령어를 입력하면 됩니다.

```

      / _ | / \ | \ / / _ | | | | \ | / _ | / / / _ \ | | | | _ |
     \ \ \ _ \ | \ | \ _ \ | | | | . | ( _ | / / | ( ) | | _ | |
    | _ / / \ \ | | | _ \ \ _ / | \ \ \ \ \ / / \ \ / | _ _ | |

User Access Verification

Username: admin
Password:
Last login: Mon Dec 26 08:50:09 from 165.213.224.50
FTTP/H EPON SYSTEM, Samsung Electronics Co. Ltd. 12/24/05 10:04:03
OG1100>
OG1100>?
Exec commands:
  clear          Reset functions
  debug          Debugging functions (see also 'undebug')
  disable        Turn off privileged mode command
  enable         Turn on privileged mode command
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  logout         Exit from the EXEC
  no             Negate a command or set its defaults
  opr            Operate
  packet         enable packet dump debugging
  quit           Exit current mode and down to previous mode
  show           Show running system information
  tcpdump        Execute tcpdump
  terminal        Set terminal line parameters
  traffic-monitor traffic-monitor
OG1100>enable
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#exit
OG1100#
```

1.3.5 SNMP Network Manager 를 통한 연결

SNMP(Simple Network Management Protocol)를 지원하는 네트워크에서도 관리기 (Network Manager)를 통해서 OG-1100 시스템을 관리할 수 있습니다.

1.4 비밀번호 설정

시스템 운영자는 콘솔 포트나 telnet 을 통해서 스위치에 로그인 할 수 있습니다. OG-1100 시스템은 시스템 보안을 위해 다음과 같은 2 개의 비밀번호를 사용합니다.

- Enable 비밀번호: Privileged 모드의 보안을 목적으로 사용
- 사용자 ID/비밀번호: 콘솔이나 telnet 을 통해 사용자 모드로 액세스 할 때 사용

비밀번호 설정과 관련된 명령어는 다음과 같습니다.

(no) service password-encryption 과 username 명령어는 ‘admin 운영자만이 설정할 수 있습니다. ‘admin[k1]’ 이외의 운용자에게는 명령어가 나타나지 않습니다.



참고

운영자 설정에 대한 구체적인 사항은 ‘1.11 운영자 설정’을 참조합니다.

명령어	설명	모드
service password-encryption	비밀번호 encryption mode 를 설정	Config
no service password-encryption	비밀번호 encryption mode 를 삭제	Config
enable password <i>PASSWORD</i>	Privileged 모드 비밀번호를 지정	Config
no enable password	Privileged 모드 비밀번호를 삭제	Config
username <i>USERNAME</i> password <i>PASSWORD</i>	콘솔이나 원격 접속을 통한 사용자 ID 와 비밀번호 설정 및 변경	Config

1.4.1 Enable 모드 비밀번호 설정

```
OG1100# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#enable password epon
OG1100(config)#end
OG1100(config)#show running-config
!
enable password epon
!
```

1.4.2 비밀번호 encryption 설정

위의 예에서 보듯이 비밀번호 설정 후 show running-config 명령어로 설정된 비밀번호를 볼 수 있습니다. 이를 방지하기 위하여 OG-1100 시스템은 비밀번호 encryption 모드 설정을 지원합니다.

```

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#service password-encryption
OG1100(config)#show running-config
!
service password-encryption
enable password 8 8FxbVXpaypPMs
    
```

1.4.3 운영자 비밀번호 설정

운영자 비밀번호를 설정 및 변경합니다.

```

OG1100#con t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#username epon password epon
OG1100(config)#show running-config
!
service password-encryption
!
username epon password 8 FlR76NDMHlrYA
!
    
```

1.5 Hostname 설정

Hostname 은 운영 시 시스템을 구별하기 위해 사용될 수 있으며 따라서 콘솔/Telnet 화면의 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있습니다. OG-1100 시스템은 기본적으로 시스템의 모델명을 hostname 으로 사용하며 운영자가 이를 변경할 수 있습니다.

명령어	설명	모드
hostname WORD	Hostname 을 변경	Config
no hostname	Hostname 을 기본 값으로 변경	Config

Hostname 을 설정 및 변경하는 절차는 다음과 같습니다.

```

OG1100# configure terminal
OG1100(config)# hostname EPON
EPON(config)# end
EPON#

EPON# configure terminal
EPON(config)# no hostname
OG1100(config)# end
OG1100#
    
```

1.6 콘솔/Telnet 환경 설정

콘솔과 Telnet 의 화면 출력 환경을 설정하거나 Telnet 접근 제어를 위하여 다음 명령어를 사용합니다.

명령어	설명	모드
line vty <0-15> (<0-15>)	telnet terminal line 설정 모드	Config
no line vty <0-15> (<0-15>)	telnet terminal session 을 삭제	Config
line console <0-0>	console line 설정 모드	Config
exec-timeout <0-35791> (<0-2147483>)	현재 세션의 타임 아웃 시간을 분, 초 단위로 설정	Line
no exec-timeout	현재 세션의 타임 아웃 시간을 기본값으로 변경 (기본값 : 10 분)	Line
login authentication(default AUTHLISTNAME)	현재 세션의 인증 방법을 설정	Line
no login authentication	현재 세션의 인증 방법을 기본값으로 설정	Line

1.6.1 세션 설정

콘솔 세션에 대한 환경 설정은 'line console' 로 설정할 수 있습니다.

원격 접속으로 시스템에 접속할 수 있는 터미널 수는 'line vty' 명령으로 설정할 수 있으며, 삭제는 'no line vty'(으)로 설정합니다.

OG-1100 시스템에서는 1 개의 콘솔과 최대 16 개 원격 접속을 동시에 허용합니다. 원격 접속은 기본값으로 5 개의 동시 접속을 허용합니다.

```
OG1100(config)#line ?
  console Primary terminal line
  vty      Virtual terminal

OG1100(config)#line vty ?
  <0-15>   First Line number
  <cr>

OG1100(config)#line vty 0 ?
  <0-15>   Last Line number
  <cr>

OG1100(config)#line vty 0 4
OG1100(config-line)#?
Line configuration commands:
  exec-timeout Set the EXEC timeout
  exit          End current mode and down to previous mode
  help         Description of the interactive help system
  login        Enable password checking
  no           Negate a command or set its defaults
  show        Show running system information
```

```
OG1100(config)#no line ?
  vty Virtual terminal

OG1100(config)#no line vty ?
  <0-15> First Line number

OG1100(config)#no line vty 5 ?
  <0-15> Last Line number
  <cr>

OG1100(config)#no line vty 5
```

1.6.2 타임 아웃 설정

일정 시간이상 입력이 없으면, 해당 세션은 접속이 끊어지게 됩니다. 세션의 타임 아웃을 분, 초 단위로 설정합니다. 설정된 타임 아웃을 취소하려면, ‘no exec-timeout’ 을 설정하면 되며, 기본값으로 타임 아웃이 설정됩니다. OG-1100 시스템의 타임 아웃 기본값은 10 분 입니다.

타임 아웃 기능을 해제하려면 ‘exec-timeout 0 0’ 로 설정 됩니다.

타임 아웃 설정전에 접속된 세션에는 타임 아웃이 적용되지 않습니다. 설정 후 새로 접속되는 세션에 대해서 적용됩니다.

```
OG1100(config)#line vty 0 4
OG1100(config-line)#exec-timeout ?
  <0-35791> Timeout in minutes

OG1100(config-line)#exec-timeout 0 ?
  <0-2147483> Timeout in seconds
  <cr>

OG1100(config-line)#exec-timeout 0 0
```

1.6.3 인증 방법 설정

인증 리스트에서 설정된 인증 방법을 콘솔과 원격 접속에 각각 다르게 설정할 수 있습니다. 단, 원격 접속의 인증 방법 설정은 ‘line vty’ 명령으로 터미널 범위를 설정하지 않으며, 모든 원격 접속 세션에 동일하게 적용됩니다.

인증 리스트에 존재하는 것만 인증 방법 설정에 사용할 수 있습니다. 설정 취소는 ‘no login authentication’ 명령어를 사용하며, 기본값으로 설정됩니다. 인증 기본값은 ‘default’ 로 표기되며, 시스템에 설정된 운영자 ID 및 비밀번호만 확인하는 것입니다.

```
OG1100(config)#line vty
OG1100(config-line)#login authentication ?
  AUTHLISTNAME AAA authenticaion method list name
  default AAA authentcation default method
OG1100(config-line)#no login authentication default
```



```
OG1100(config-line)#show running-config aaa
!
aaa authentication login default local
!
line con 0
  login authentication default
line vty 0 4
  login authentication default
!

OG1100(config-line)#no login authentication
```

1.7 현재 세션 환경 설정

콘솔/Telnet 으로 로그인 한 후 임시적으로 화면 출력 환경을 변경하고자 할 경우 다음 명령어를 사용합니다. 단 다음 명령은 현재 세션에만 적용되며 로그 아웃 후 재 적용되지 않습니다.

명령어	설명	모드
<code>terminal length <0-512></code>	Screen Line 설정 0 : no pause	EXEC
<code>terminal no length</code>	Screen Line 을 기본 값(22)으로 변경	EXEC
<code>terminal message(unblock block)</code>	이벤트 메시지가 터미널에 표시되도록 활성화/비활성화('show users' 명령으로 설정 상태를 조회할 수 있습니다.)	EXEC

시스템에 접속하는 모든 터미널의 출력 line 수를 일괄적으로 적용하려면, config 모드에서 'service terminal-length <0-512>' 명령어를 사용합니다.

1.8 SNMP

SNMP(Simple Network Management Protocol)는 MIB(Management Information Base)을 제공하는 스위치를 관리할 수 있습니다. 각각의 네트워크 관리자는 관리의 편의를 위해서 사용자 인터페이스를 제공합니다. SNMP manager 로 OG-1100 시스템 OLT 를 관리하고자 할 때는 OLT 의 환경 설정이 필요합니다. 또한 SNMP 에이전트를 접근하기 위해서는 OLT 에 하나 이상의 IP 어드레스 설정이 필요합니다.

명령어	설명	모드
<code>snmp community(rw ro) NAME</code> <code>no snmp community(rw ro) NAME</code>	SNMP community 를 설정 - ro : read only - rw : read write	System
<code>snmp-config-block(diable enable)</code>	SNMP 로 시스템 환경 설정 가능여부를 설정	Enable
<code>snmp traphost EMSNAME A.B.C.D (PORT)</code> <code>no snmp traphost EMSNAME</code>	SNMP Trap Host 를 추가 혹은 삭제	System
<code>snmp trapport EMSNAME PORT</code>	SNMP Trap port number 를 수정	System
<code>show snmp community</code>	SNMP Community 를 디스플레이	Enable
<code>show snmp traphost</code>	SNMP Trap Host 정보 리스트를 디스플레이	Enable

1.9 Access Permit 과 ACL

Access Permit 과 ACL(access-list)를 사용함으로써 네트워크 관리자는 인터넷워크를 통해 전송되는 트래픽에 대해 상당히 세밀한 통제를 할 수 있습니다. 관리자는 패킷의 전송 상태에 대한 기본적인 통계 자료를 얻을 수 있고 이를 통해 보안 정책을 수립할 수 있습니다. 또한 인증되지 않은 시스템 접속으로부터 시스템을 보호할 수 있습니다.

Access Permit 는 OG-1100 에서는 관리자의 접속에 대한 보안정책으로 사용하며, ACL 는 표준을 지원합니다. 이것을 통해서 DB 를 관리하는 기능만으로 사용되며, 이 에 따른 정책 의 시행은 별도로 QoS 의 classMap 에서 수행하도록 되었었습니다.

1.9.1 Access Permit 설정

Access-permit 은 시스템에 Incoming 되는 패킷에 대하여, 패킷의 Source IP 어드레스와 접속 프로토콜을 검사하여 시스템 접속을 허용합니다.

Access-permit-enable 명령으로 access-permit 리스트 중 하나를 선택하여 활성화 합니다. 단, Access-permit 이 활성화되면, 선택된 리스트외의 IP 어드레스와 프로토콜은 접속이 끊어지므로 주의해야 합니다.

명령어	설명	모드
access-permit LISTNAME A.B.C.D(A.B.C.D(telnet ssh snmp ftp tftp all) (telnet ssh snmp ftp tftp all))	<ul style="list-style-type: none"> - LISTNAME Access-permit List Name - A.B.C.D IP Address - A.B.C.D Subnet Mask - all All(Telnet, SSH, SNMP, FTP, TFTP) connection - telnet Telnet connection - ssh SSH connection - snmp SNMP connection - ftp FTP connection - tftp TFTP connection 	Config
no access-permit(all LISTNAME(all A.B.C.D (A.B.C.D(telnet ssh snmp ftp tftp all) (telnet ssh snmp ftp all))))	<ul style="list-style-type: none"> - all All Access-permit List - LISTNAME Access-permit List Name - all All IP address - A.B.C.D IP address - A.B.C.D Subnet Mask - all All(Telnet, SSH, SNMP, FTP, TFTP) connection - telnet Telnet connection - ssh SSH connection - snmp SNMP connection - ftp FTP connection - tftp TFTP connection 	Config
access-permit-enable LISTNAME in	특정 Access-permit List 를 시스템에 적용	Config
no access-permit enable in	Access-permit 기능을 비활성화 시킴	Config
show access-permit	Access-permit List 및 Access-permit-enable 설정 정보를 디스플레이	EXEC or Config

Access Permit 생성 및 적용 순서는 다음과 같습니다.

- 접속을 허용하고자 하는 IP 및 protocol 을 고려하여, access-permit 리스트를 생성합니다.
- Access-permit-enable 명령어로 access-permit 리스트 중 하나를 선택하여, 시스템에 적용합니다.

Access-permit List 생성

```

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#access-permit ap3 10.89.24.145 all
OG1100(config)#show running-config access-permit
Building configuration...
!
access-permit ap3 10.89.24.145 all
access-permit ap1 10.89.24.0 255.255.255.0 all
access-permit ap2 10.89.23.0 255.255.255.0 all
access-permit ap2 10.89.24.0 255.255.255.0 all
OG1100(config)#end
OG1100#show access-permit
-----
Enabled Access-permit List (Incoming) : None
-----

The number of Access-permit List : 3
List Num Num List Name IP Subnet Protocol
1 1 ap3 10.89.24.145
2 2 ap3 10.89.24.145 ssh
3 3 ap3 10.89.24.145 snmp
4 4 ap3 10.89.24.145 ftp
5 5 ap3 10.89.24.145 tftp
2 1 ap1 10.89.24.0 255.255.255.0 telnet
2 2 ap1 10.89.24.0 255.255.255.0 ssh
3 3 ap1 10.89.24.0 255.255.255.0 snmp
4 4 ap1 10.89.24.0 255.255.255.0 ftp
5 5 ap1 10.89.24.0 255.255.255.0 tftp
3 1 ap2 10.89.23.0 255.255.255.0 telnet
2 2 ap2 10.89.23.0 255.255.255.0 ssh
3 3 ap2 10.89.23.0 255.255.255.0 snmp
4 4 ap2 10.89.23.0 255.255.255.0 ftp
5 5 ap2 10.89.23.0 255.255.255.0 tftp
6 6 ap2 10.89.24.0 255.255.255.0 telnet
7 7 ap2 10.89.24.0 255.255.255.0 ssh
8 8 ap2 10.89.24.0 255.255.255.0 snmp
9 9 ap2 10.89.24.0 255.255.255.0 ftp
10 10 ap2 10.89.24.0 255.255.255.0 tftp
-----
OG1100#
    
```

Access-permit List 삭제

```

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#no access-permit ?
  LISTNAME  Access-permit list name
  all       All entries
OG1100(config)#no access-permit all
OG1100(config)#no access-permit ap3 ?
  A.B.C.D   Source IP address
  all       All entries
OG1100(config)#no access-permit ap3 all
OG1100(config)#no access-permit ap3 ?
  A.B.C.D   Source IP address
  all       All entries
OG1100(config)#no access-permit ap3 10.89.24.145 ?
  A.B.C.D   Subnet Mask
  all       All(Telnet, SSH, SNMP, FTP, TFTP) connection
  ftp       FTP connection
  snmp      SNMP connection
  ssh       SSH connection
  telnet    Telnet connection
  tftp      TFTP connection
OG1100(config)#no access-permit ap3 10.89.24.145 snmp ?
<cr>

```

Access-permit 활성화

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#access-permit-enable ap1 in

OG1100(config)#show running-config access-permit
Building configuration...
!
access-permit ap3 10.89.24.145 all
access-permit ap1 10.89.24.0 255.255.255.0 all
access-permit ap2 10.89.23.0 255.255.255.0 all
access-permit ap2 10.89.24.0 255.255.255.0 all
access-permit-enable ap1 in
!

OG1100(config)#show access-permit
-----
Enabled Access-permit List (Incoming) : ap1
-----

The number of Access-permit List : 3
List Num Num List Name      IP          Subnet      Protocol
   1     1     ap3    10.89.24.145
   2     2     ap3    10.89.24.145
   3     3     ap3    10.89.24.145
   4     4     ap3    10.89.24.145
   5     5     ap3    10.89.24.145
   2     1     ap1    10.89.24.0    255.255.255.0

```

	2	ap1	10.89.24.0	255.255.255.0	ssh
	3	ap1	10.89.24.0	255.255.255.0	snmp
	4	ap1	10.89.24.0	255.255.255.0	ftp
	5	ap1	10.89.24.0	255.255.255.0	tftp
3	1	ap2	10.89.23.0	255.255.255.0	telnet
	2	ap2	10.89.23.0	255.255.255.0	ssh
	3	ap2	10.89.23.0	255.255.255.0	snmp
	4	ap2	10.89.23.0	255.255.255.0	ftp
	5	ap2	10.89.23.0	255.255.255.0	tftp
	6	ap2	10.89.24.0	255.255.255.0	telnet
	7	ap2	10.89.24.0	255.255.255.0	ssh
	8	ap2	10.89.24.0	255.255.255.0	snmp
	9	ap2	10.89.24.0	255.255.255.0	ftp
	10	ap2	10.89.24.0	255.255.255.0	tftp

1.9.2 ACL 설정

명령어	설명	모드
Access-list {<1-99> /<1300-1999>/word}{deny/permit/remark}{ip}A.B.C.D/M/any/host[k2]	<ul style="list-style-type: none"> - <1-99> IP standard access list - <1300-1999> IP standard access list (expanded range) - WORD IP [k3]access-list name - A.B.C.D Network Address to match - A.B.C.D/M Prefix to match - any Any source host - host A single host address 	Config

```

OG1100# configure terminal
OG1100(config)#access-list 100 permit ip 10.0.0.1 0.0.0.255 any
OG1100(config)#end
OG1100#show access-list
Extended IP access list 100
    permit ip 10.0.0.0 0.0.0.255 any
    
```

1.10 Management IP 설정

OG-1100 시스템에서는 운용자의 관리를 위해 management IP 를 out/in-band 모드로 설정할 수 있도록 합니다. 이를 위해서는 시스템의 기본 설정을 위한 설정 모드로 변경하기 위해 아래와 같이 CONFIG_MODE 에서 'system'을 입력하여 SYSTEM_MODE 로 변경합니다.

명령어	설명	모드
system ipconfig ipaddr <i>A.B.C.D</i> [subnet] <i>A.B.C.D</i>	- ipconfig IP configuration - ipaddr IP address - subnet subnet mask - A.B.C.D dotted decimal or host,network names	Config-system
system route {add/del} {host/net} <i>A.B.C.D gw A.B.C.D</i>	- Route provision routing table - Add add a new route - Del delete a route - host A single host address - gw gateway	Config-system

설정된 상태를 조회하기 위해서는 EANBLE_MODE 로 빠져나간 후 'show system ipconfig' 와 'show system route' 명령어로 설정 상태를 조회할 수 있습니다.

```
OG1100# configure terminal
OG1100(config)# system
OG1100(config-sys)# system ipconfig ipaddr 165.213.224.212 subnet
255.255.255.0
OG1100(config-sys)# system route add net 165.213.224.0 netmask
255.255.255.0 gw 165.213.224.1
OG1100(config)# exit
OG1100# show ip interface
OG1100# show system ipconfig
DEVICE NAME      : lo
IP ADDRESS       : 127.0.0.1
NETMASKS         : 255.0.0.0

DEVICE NAME      : eth0
IP ADDRESS       : 165.213.224.212
NETMASKS         : 255.255.0.0

DEVICE NAME      : eth1
IP ADDRESS       : 192.168.0.1
NETMASKS         : 255.255.255.0

OG1100# show system route
DESTINATION      GATEWAY      SUBNET      FLAGS METRIC REF  USE  IFACE
-----
165.213.0.0      *            255.255.0.0  U    0    0    0  eth0
192.168.0.0      *            255.255.255.0  U    0    0    0  eth1
```

1.11 운용자 설정

OG-1100 시스템에서는 운용자의 관리를 위해 user 를 추가, 삭제 변경 할 수 있습니다. 슈퍼 사용자인 ‘admin[k4]’ 는 오직 하나만 존재하며, ID 를 삭제할 수 없으며, 오직 비밀번호만 변경 가능합니다. ‘service password-encryption’, ‘username’ 등 일반 user 는 접근 권한이 없는 모든 설정이 가능합니다. 그 외 운용자는 privilege 1, 14, 15 를 할당받을 수 있습니다.

Privilege 1 는 EXEC 모드(enable 모드)의 명령어만 권한이 있으며, 조회만 가능합니다. Privilege 14 는 Privilege EXEC 모드(enable 모드)접근 권한을 얻을 수 있으며, 슈퍼 유저에게만 권한이 할당된 명령어 이외의 명령어는 접근 권한이 있습니다. Privilege 15 는 시스템에 접속하자마자 바로 Privileged EXEC 모드(enable 모드) 권한을 얻습니다.

운용자를 삭제할 때는 ‘no username’ 을 사용합니다. 단, 현재 접속중인 운용자는 삭제 할 수 없습니다.

명령어	설명	모드
username USERNAME privilege (1 14 15) password PASSWORD	운용자를 추가	Config
username USERNAME privilege (1 14 15)	운용자의 privilege 변경	Config
username USERNAME password PASSWORD	운용자의 password 변경	Config
no username USERNAME	운용자를 삭제	Config

1.11.1 운용자 추가 및 삭제

운용자를 새로 추가할 때는 ID, 비밀번호, privilege 를 모두 설정해 주어야 합니다. 만약, 운용자를 처음 추가할 때, privilege 를 생략하면 privilege 는 1 이 할당됩니다.

```
OG1100(config)#username cliuser privilege 14 password epon

OG1100(config)#username epon password epon

OG1100(config)# no username admin
% Super user is not allowed to delete

OG1100(config)# no username epon
% user 'admin' is currently logged in
```

1.11.2 운용자 privilege 변경

운용자의 privilege 를 변경합니다.

```
OG1100(config)#username epon privilege 14
```


1.11.3 운용자 비밀번호 변경

운용자의 비밀번호를 변경합니다.

```
OG1100(config)#username cliuser password ftth
```

1.12 관리자 인증 설정

Line 모드의 'login authentication' 명령으로 관리자 인증을 시스템에서 활성화 시키기 전, 관리자 인증 리스트 및 관리자 인증 서버를 설정해야 합니다.

1.12.1 관리자 인증 리스트 설정

관리자 접속(로그인)에 대해 인증 리스트를 설정할 수 있습니다. 인증 리스트는 시스템 로그인 ID 및 비밀번호를 검사하는 local, RADIUS(Remote Authentication Dial In User Service) 서버로부터 관리자 인증을 받는 radius, TACACS+(Terminal Access Controller Access Control System+) 서버로부터 관리자 인증을 받는 tacacs 를 조합하여 리스트를 구성할 수 있습니다. 리스트 구성시 반드시 local 은 순서에 상관없이 포함되어야 합니다. 기본적으로 생성된 default 는 local 로만 구성되어 있으며, 삭제할 수 없습니다. 현재 시스템에서 활성화된 리스트는 삭제할 수 없습니다.

명령어	설명	모드
<code>aaa authentication login AUTHLISTNAME {local radius tacacs}</code>	관리자 인증 리스트 생성 - AUTHLISTNAME : 관리자 인증 리스트 이름 - local : 시스템의 로그인 ID 및 비밀번호 검사 - radius : RADIUS 서버로부터 인증 - tacacs : TACACS+ 서버로부터 인증	Config
<code>no aaa authentication login AUTHLISTNAME</code>	관리자 인증 리스트 삭제	Config
<code>show aaa</code>	관리자 인증 리스트를 디스플레이	EXEC

관리자 인증 리스트 생성

```
OG1100(config)#aaa authentication login ?
  AUTHLISTNAME Named authentication list
OG1100(config)#aaa authentication login a3 ?
  local Local
  radius RADIUS
  tacacs TACACS+
OG1100(config)#aaa authentication login a3 radius ?
  local Local
  tacacs TACACS+
<cr>
OG1100(config)#aaa authentication login a3 radius local ?
  tacacs TACACS+
<cr>
```

```
OG1100(config)#aaa authentication login a3 radius local tacacs

OG1100(config)#show running-config aaa
Building configuration...
!
aaa authentication login default local
aaa authentication login a1 local radius
aaa authentication login a2 local tacacs
aaa authentication login a3 radius local tacacs
!
line con 0
  login authentication default
line vty 0 4
  login authentication default
!

OG1100#show aaa
----- Administrator Authentication -----
[Adapted AAA List] console - default
[Adapted AAA List] vty - default
-----
[AAA List] default      - local
[AAA List] a1          - local radius
[AAA List] a2          - local tacacs
[AAA List] a3          - radius local tacacs
-----
[RADIUS]
[TACACS+]
-----
```

관리자 인증 리스트 삭제

```
OG1100(config)#no aaa authentication login default
% Default authentication list is not allowed to delete

OG1100(config)#no aaa authentication login a3
% This authentication method is currently used

OG1100(config)#show running-config aaa
Building configuration...
!
aaa authentication login default local
aaa authentication login a1 local radius
aaa authentication login a2 local tacacs
aaa authentication login a3 radius local tacacs
radius-server retransmit 0
radius-server host 10.89.24.102 key test
tacacs-server host 10.89.24.102 key test
!
line con 0
  login authentication default
line vty 0 4
  login authentication a3
!
```

1.12.2 관리자 인증 서버 설정

관리자 인증 RADIUS 서버 및 TACACS+ 서버를 설정합니다.

명령어	설명	모드
<code>radius-server retransmit <0-3></code>	- RADIUS 서버에 인증 재시도 횟수 설정 - 기본 값 : 0	Config
<code>radius-server host A.B.C.D {authen-port <1-65535> key KEY timeout <1-1000>}</code>	- RADIUS 서버 설정 authen-port : RADIUS 서버 포트 기본 값 : 1812 - key : Shared key string - timeout : RADIUS 서버로 부터의 time out(sec) 기본 값 : 3 sec	Config
<code>no radius-server (host A.B.C.D all)</code>	RADIUS 서버 삭제	Config
<code>tacacs-server host HOSTNAME {port <1-65535> key KEY timeout <1-1000>}</code>	- TACACS+ 서버 설정 - port : TACACS+ 서버 포트 기본 값 : 49 - key : Shared key string - timeout : TACACS+ 서버로 부터의 time out(sec) 기본 값 : 5 sec	Config
<code>no tacacs-server (host HOSTADDRESS ALL)</code>	TACACS+ 서버 삭제	Config
<code>show aaa</code>	관리자 인증 서버를 디스플레이	EXEC

RADIUS 서버 설정

```

OG1100(config)#radius-server retransmit 1
OG1100(config)#radius-server host ?
  A.B.C.D RADIUS server address (dotted ip notation)
OG1100(config)#radius-server host 10.89.24.102 ?
  auth-port RADIUS server authentication port number
  key      Encryption key shared with the RADIUS server
  timeout  Time to wait for a RADIUS server to reply
OG1100(config)#radius-server host 10.89.24.102 key ?
  KEY Shared key
OG1100(config)#radius-server host 10.89.24.102 key test ?
  auth-port RADIUS server authentication port number
  timeout  Time to wait for a RADIUS server to reply
  <cr>
OG1100(config)#radius-server host 10.89.24.102 key test

OG1100#show running-config aaa
Building configuration...
!
aaa authentication login default local
aaa authentication login a1 local radius
aaa authentication login a2 local tacacs
    
```

```
aaa authentication login a3 radius local tacacs
radius-server retransmit 1
radius-server host 10.89.24.102 key test
!
line con 0
  login authentication default
line vty 0 4
  login authentication default
!

OG1100#show aaa
----- Administrator Authentication -----
[Adapted AAA List] console - default
[Adapted AAA List] vty - default
-----
[AAA List] default      - local
[AAA List] a1           - local radius
[AAA List] a2           - local tacacs
[AAA List] a3           - radius local tacacs
-----
[RADIUS]
RADIUS Server retransmit=1
RADIUS Server addr=10.89.24.102  authn-port=1812  key=test  timeout=3
[TACACS+]
-----
```

TACACS+ 서버 설정

```
OG1100(config)#tacacs-server ?
  host Specify a TACACS+ server
OG1100(config)#tacacs-server host ?
  A.B.C.D TACACS+ server address (dotted ip notation)
OG1100(config)#tacacs-server host 10.89.24.102 ?
  key      Encryption key shared with the TACACS+ server
  port     TACACS+ server port number
  timeout  Time to wait for a TACACS+ server to reply
OG1100(config)#tacacs-server host 10.89.24.102 key ?
  KEY     Shared key
OG1100(config)#tacacs-server host 10.89.24.102 key test ?
  port     TACACS+ server port number
  timeout  Time to wait for a TACACS+ server to reply
  <cr>
OG1100(config)#tacacs-server host 10.89.24.102 key test

OG1100#show running-config aaa
Building configuration...
!
aaa authentication login default local
aaa authentication login a1 local radius
aaa authentication login a2 local tacacs
aaa authentication login a3 radius local tacacs
radius-server retransmit 1
```

```
radius-server host 10.89.24.102 key test
tacacs-server host 10.89.24.102 key test
!
line con 0
  login authentication default
line vty 0 4
  login authentication default
!

OG1100#show aaa
----- Administrator Authentication -----
[Adapted AAA List] console - default
[Adapted AAA List] vty - default
-----
[AAA List] default      - local
[AAA List] a1          - local radius
[AAA List] a2          - local tacacs
[AAA List] a3          - radius local tacacs
-----
[RADIUS]
RADIUS Server retransmit=1
RADIUS Server addr=10.89.24.102 authen-port=1812 key=test timeout=3
[TACACS+]
TACACS+ Server addr=10.89.24.102 port=49 key=test timeout=5
-----
```

1.13 세션 강제 종료

현재 연결된 세션을 강제로 종료시킬 수 있습니다. ‘show users’ 명령어를 사용하여 현재 접속자 정보를 조회한 후, 접속자의 연결을 시스템에서 강제로 끊어버릴 수 있습니다.

명령어	설명	모드
disconnect(all console vty <0-15> vty all) [k5]	접속 세션을 종료 - all : 모든 세션을 종료 - console : 콘솔 세션을 종료 - vty : 원격 세션을 종료	Enable

‘disconnect’ 명령어 사용은 다음과 같습니다.

```

OG1100#show users
  Line LoginID  TTY      IP address      Login Time
Event&Debug MSG
* vty 0 admin   pts/0      10.89.24.145    2000-05-22 21:59 PERMITTED
  vty 1 epon    pts/2      10.89.24.145    2000-05-22 23:18

OG1100#disconnect ?
  all      All connections
  console  Console
  vty      VTY (remote connection)
OG1100#disconnect vty ?
  <0-15>  VTY number
  All     All VTY connections[k6]
OG1100#disconnect vty 1
    
```

1.14 배너 설정

로그인 후 출력 메시지를 설정합니다.

명령어	설명	모드
banner motd(LINE default)	- 로그인 출력 메시지를 설정 - 기본 값 : 기본 출력 메시지	Config
no banner motd	로그인 메시지를 출력하지 않음	Config

‘banner’ 명령어 사용은 다음과 같습니다.

```

OG1100(config)#
OG1100(config)#banner motd Hello!!!

Hello!!!
OG1100>

OG1100(config)#banner motd default
    
```

```

FTTP/H EPON SYSTEM, Samsung Electronics Co. Ltd. 01/03/06 14:13:00
OG1100>

OG1100(config)#no banner motd

OG1100>

```

1.15 외부 접속

시스템에서 외부로 접속할 수 있는 수단을 제공합니다.

명령어	설명	모드
ping WORD	- ping - WORD : IP 어드레스 또는 Hostname	Enable
telnet WORD(PORT)	- 텔넷 클라이언트 - WORD : IP 어드레스 또는 Hostname - PORT : TCP 포트 번호	Enable
ssh WORD(WORD)	SSH 클라이언트 - WORD : IP 어드레스 또는 Hostname - WORD : Login ID	Enable
ftp WORD	- FTP 클라이언트 - WORD : 어드레스 또는 Hostname	Enable

1.16 시스템 조회

시스템의 접속 현황, 명령어 이력 등을 조회할 수 있습니다.

1.16.1 시스템 접속 정보 조회

현재 시스템에 접속한 사용자 정보 및 과거 접속 이력을 조회할 수 있습니다.

명령어	설명	모드
show users	현재 접속 정보 디스플레이	EXEC
shlow users history	접속 이력 디스플레이	Enable

현재 접속 정보

지금 현재 시스템에 접속중인 사용자의 정보만 조회할 수 있습니다.
본인은 '*' 로 표시됩니다.

```
OG1100#show users
  Line LoginID   TTY      IP address      Login Time
Event&Debug MSG
* vty 0 admin   pts/0     10.89.24.145   2000-05-22 21:59 PERMITTED
  vty 1 epon    pts/2     10.89.24.102   2000-05-22 21:57
```

접속 이력

시스템의 접속 이력을 조회할 수 있습니다.

```
OG1100#show users history
LoginID   TTY      IP address      Login          Logout Period
admin     pts/0    10.89.24.145   2000-05-22 21:59 still logged in
epon      pts/2    10.89.24.145   2000-05-22 21:57 still logged in
admin     pts/0    10.89.24.145   2000-05-22 21:56 - 21:58 (00:02)
```

1.16.2 명령어 이력 조회

현재 사용자가 수행한 명령어 및 과거 수행한 명령어 이력을 조회할 수 있습니다.

명령어	설명	모드
show history	시스템에 접속해 있는 동안 수행한 명령어 디스플레이	EXEC
show history log	시스템에 접속한 모든 사용자가 수행한 명령어 이력을 디스플레이(단, 최근 수행한 명령어부터 500 개까지만 조회 가능)	Enable

show history

사용자가 시스템에 접속해 있는 동안 수행한 명령어를 조회합니다. 시스템에서 로그 아웃 되면, 정보는 저장되지 않고 없어집니다.

조회되는 명령어는 화살표 키(↑, ↓)를 이용하여 선택한 후 실행할 수 있습니다.

```
OG1100#show history
 1 en
 2 show pon lpbk-state link
 3 show ip route
 4 show snmp-config-block
 5 snmp-config-block disable
 6 show snmp-config-block
 7 snmp-config-block disable
 8 show snmp-config-block
 9 snmp-config-block enable
10 show snmp-config-block
11 show users
12 show history
OG1100#
```


show history log

```

OG100#show history log
Num Login ID TTY Host Time Result
Command
 1 epon pts/1 165.213.224.228 10/05/05 11:10:13 -- show
history log
 2 admin pts/2 165.213.224.227 10/05/05 11:08:42 -- show
software version swu
 3 admin pts/2 165.213.224.227 10/05/05 11:08:30 -- show
who
 4 admin pts/2 165.213.224.227 10/05/05 11:08:25 success end
 5 admin pts/2 165.213.224.227 10/05/05 11:08:24 success
software download swu os
 6 admin pts/2 165.213.224.227 10/05/05 11:08:17 success sys
 7 epon pts/1 165.213.224.228 10/05/05 11:07:44 -- show
history
 8 epon pts/1 165.213.224.228 10/05/05 11:06:14 -- show
history log
 9 admin pts/2 165.213.224.227 10/05/05 11:05:21 success con t
10 admin pts/2 165.213.224.227 10/05/05 11:05:12 success en

```

1.17 소프트웨어 업그레이드하기

OG-1100 시스템에서는 TFTP 서버를 이용하여 최신 버전의 소프트웨어를 다운로드 받아 업그레이드 할 수 있습니다. 현재 OG-1100 시스템에서 운용하고 있는 소프트웨어의 버전을 확인하고 TFTP 서버로부터 최신 버전의 소프트웨어를 다운로드하는 방법을 알아봅니다.

명령어	설명	모드
software download(MCU swu) FILENAME HOST	MCU 또는 swu 소프트웨어 이미지를 업그 레이드	Config
software download(ponolt pononu onu) (address IF_NAME) FILENAME HOST	Ponlt, pononu, 또는 onu 소프트웨어 이미 지를 업그레이드	Config
show software version (MCU swu ponolt)	MCU, swu, 또는 ponolt 소프트웨어 버전 정보 확인	Enable
show software version(pononu onu) IF_NAME	Pononu 또는 onu 소프트웨어 버전 정보 확인	Enable

1.18 설정정보 파일 관리하기

OG-1100 시스템에서는 현재 설정정보를 파일로 저장하거나, TFTP 서버를 이용하여 업로드할 수 있습니다. 반대로 TFTP 서버를 이용하여 업로드하였던 설정정보를 다운로드 받아 현재 설정정보 파일을 덮어 쓸수 있습니다.

명령어	설명	모드
copy running-config startup-config	현재 시스템의 설정정보 파일 저장	Enable
copy running-config tftp HOST CONFIG_NAME	현재 시스템의 설정정보 원격서버에 업로드	Enable
copy startup-config tftp HOST CONFIG_NAME	현재 시스템에 저장된 설정정보 파일을 원격서버로 업로드	Enable
copy tftp HOST CONFIG_NAME startup-config	원격서버의 설정정보 파일을 다운로드	Enable
copy factory-default startup-config	설정정보 파일을 factory 기본 값 파일로 교체	Enable

1.19 성능 정보 collection 및 monitoring 설정

OG-1100 시스템에서는 현재 성능 정보를 조회할 수 있습니다.

조회하기 위해서는 시스템의 성능조회 포인트를 enable 해주어야 성능 count 가 collection 되어 성능 정보가 증가하게 됩니다. 또한, 5sec/1mim/10min 평균 성능값을 조회하기 위해서는 monitoring 상태를 enable 해주어야 합니다. 이런 status 를 설정한 후 각각의 조회 명령어로 성능을 조회 해 볼수가 있게 됩니다.

명령어	설명	모드
Statistics collection(enable disable) IFNAME	성능 조회하기위한 해당 IFNAME 의 collection status 를 enable/disable	SYSTEM_MODE
Statistics monitoring(enable disable)	5sec/1mim/10min 평균 성능값을 조회 하기 위한 명령어	SYSTEM_MODE

1.20 Rmon 정보 설정

Rmon(alarm/event/history/statistics) 정보를 설정 및 해제 및 활성화/비활성화 하는명령어 입니다.

명령어	설명	모드
Rmon history <1-128> IFNAME (buckets <1-10000>) (interval <1-3600>) (owner STRING)	Rmon history 설정	SYSTEM_MODE
No rmon history <1-128>	Rmon history 삭제	SYSTEM_MODE
Rmon history <1-128> (active deactive)	Rmon history 활성화/비활성	SYSTEM_MODE
Rmon event <1-128> (log trap log-and-trap) community STRING description STRING(owner STRING)	Rmon event 설정	SYSTEM_MODE
No rmon event <1-128>	Rmon event 삭제	SYSTEM_MODE
Rmon event <1-128> (active deactive)	Rmon event 활성화/비활성	SYSTEM_MODE
Rmon statistics <1-128> IFNAME (owner STRING)	Rmon statistics 설정	SYSTEM_MODE
No rmon statistics <1-128>	Rmon statistics 삭제	SYSTEM_MODE
Rmon statistics <1-128> (active deactive)	Rmon statistics 활성화/비활성	SYSTEM_MODE
Rmon alarm <1-128> IFNAME (ethernetlike(dot3StatsInternal MACReceiveErrors dot3StatsFrameTooLongs dot3StatsAlignmentErrors dot3StatsFCSErrors dot3StatsInternalMACTransmitErrors dot3StatsSingleCollisionFrames dot3StatsMultipleCollisionFrames dot3StatsDeferredTransmissions dot3StatsLateCollision dot3StatsExcessiveCollision dot3StatsCarrierSenseErrors) bridge(dot1dTpPortInDiscards dot1dTpPortInFrames dot1dTpPortOutFrames) mibII (ifInDiscards ifInOctets ifInBroadcastPkts ifInMulticastPkts ifInUcastPkts ifInErrors ifInUnknownProtos ifOutDiscards ifOutOctets ifOutBroadcastPkts ifOutMulticastPkts ifOutUcastPkts ifOutErrors) rmon(etherStatsOctets etherStatsBroadcastPkts	Rmon alarm 설정	SYSTEM_MODE

(계속)

명령어	설명	모드
etherStatsMulticastPkts etherStatsUndersizePkts etherStatsOversizePkts etherStatsFragments etherStatsJabbers etherStatsCollisions etherStatsPkt64Octets etherStatsPkt65to127Octets etherStatsPkt128to255Octets etherStatsPkt256to511Octets etherStatsPkt512to1023Octets etherStatsPkt1024to1522Octets etherStatsDropEvents etherStatsCRCAlignErrors)) (absolute delta) <1-4294729695> rising-threshold VALUE <1-128> falling-threshold VALUE <1-128> startup(falling rising rising-and-falling)(owner STRING)	-	-
No alarm <1-128>	Rmon alarm 삭제	SYSTEM_MODE
Rmon alarm <1-128> (active deactive)	Rmon alarm 활성화/비활성	SYSTEM_MODE

1.21 Rmon 및 pm 정보 조회

Rmon(alarm/history/event/statistics) 정보를 조회 및 각종 PM 정보를 조회할수 있습니다.

명령어	설명	모드
Show rmon alarm <1-128>	설정된 성능정보 alarm 조회	EXEC_MODE
Show rmon event <1-128>	설정된 성능정보 event 조회	EXEC_MODE
Show rmon history <1-128>	설정된 성능정보 history 조회	EXEC_MODE
Show rmon statistics <1-128>	설정된 성능정보 statistics 조회	EXEC_MODE
Show statistics bridge IFNAME	성능 정보 중 bridge 정보 조회	EXEC_MODE
Show statistics etherlike IFNAME	성능 정보 중 etherlike 정보 조회	EXEC_MODE
Show statistics interface IFNAME	성능 정보 중 인터페이스 정보 조회	EXEC_MODE
Show statistics collection status	성능 정보 중 collection status 정보 조회	EXEC_MODE
Show statistics interface	OLT PM 인터페이스 count 조회	EXEC_MODE
Show statistics average IFNAME	설정된 과거 5 초/ 1 분/10 분 상태정보 조회	EXEC_MODE
Show rmon log	rmon log 이력 조회	EXEC_MODE
Show rmon history-total	설정된 total history table 조회	EXEC_MODE

1.22 pm count 삭제 및 rmon log 삭제

pm count 를 reset 시키는 기능 및 rmon log 를 삭제하는 기능입니다.

명령어	설명	모드
Clear rmon log	과거의 rmon log 정보 삭제	EXEC_MODE
Clear statistics counter (IFNAME OLT ONU)	port 의 성능 정보를 모두 초기화	EXEC_MODE



이 면에는 내용이 없습니다.

2장. 시스템 초기 환경 설정

2.1 랙의 정보 설정 및 조회

랙의 정보 조회 및 랙의 위치 설정이 가능합니다. 랙 ID 는 셸프 뒤에 있는 DIP 스위치로 설정할 수 있습니다. 조회 명령은 Enable-mode 에서 수행되며, 설정 명령은 system-mode 에서 수행됩니다.

명령어	설명	모드
show rack info	랙의 정보를 표시합니다.	Enable
Rack info loc LINE	LINE : 랙의 위치를 입력합니다.	Config-system

```
OG1100#show rack info
  RACK INFORMATION
=====
RACK ID           : 1
RACK TYPE         : Default Rack
RACK LOCATION     :
=====
```

```
OG1100#
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#system
OG1100(config-sys)#rack info loc FTTH-Lab
OG1100#show rack info
  RACK INFORMATION
=====
RACK ID           : 1
RACK TYPE         : Default Rack
RACK LOCATION     : FTTH-Lab
=====
```

2.2 시스템의 정보 설정 및 조회

시스템의 셸프 번호, 시스템 이름, 위치, 연락처, 부팅 시간, 부팅 경과시간등의 정보 조회가 가능합니다. 시스템의 이름, 위치, Contact 정보등의 설정이 가능합니다. 시스템 ID 는 셸프 뒤에 있는 DIP 스위치로 설정할 수 있습니다. 조회 명령은 Enable-mode 에서 수행되며, 설정 명령은 system-mode 에서 수행됩니다.

명령어	설명	모드
Show system info	시스템의 정보 표시	Enable
System info contact LINE	LINE : system 관리자의 연락처 입력	Config-system
System info loc LINE	LINE : system 의 위치 입력	Config-system
System info name LINE	LINE : system 의 이름 입력	Config-system

```
OG1100#show system info
  SYSTEM INFORMATION
=====
SHELF NUMBER           : 2
SYSTEM NAME            : OG-1100
SYSTEM LOCATION        : FTTH-LAB
SYSTEM CONTACT INFO    : gildong@samsung.com
SYSTEM BOOTING TIME    : 2006-02-20,07:32:35
SYSTEM TIME ELAPSED    : 2 Days 8 Hours 43 Minutes
=====
```

```
OG1100#
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#system
OG1100(config-sys)#system info contact FTTH-LAB
OG1100(config-sys)#system info contact gildong@samsung.com
OG1100#show system info
  SYSTEM INFORMATION
=====
SHELF NUMBER           : 2
SYSTEM NAME            : OG-1100
SYSTEM LOCATION        : FTTH-LAB
SYSTEM CONTACT INFO    : gildong@samsung.com
SYSTEM BOOTING TIME    : 2006-02-20,07:32:35
SYSTEM TIME ELAPSED    : 2 Days 9 Hours 16 Minutes
=====
```


2.3 시스템의 자원 상태 설정 및 조회

MCU, SWU 에서 사용하고 있는 CPU 와 메모리의 자원 상태를 설정하고 조회하는 방법입니다. 조회는 ENABLE_MODE 에서 수행되며, 설정은 System-mode 에서 수행됩니다.

Duration 은 일정기간의 평균 값을 보여주기위한 값으로 CPU 는 5-300 초, 메모리는 1 분-10 분까지 입력가능 하며 단위시간은 CPU 는 초, 메모리는 분입니다.

High Watermark, Low Watermark 는 경보를 발령/해제하는 기준값으로 현재 이용률이 High Watermark 보다 높으면 경보를 발령하고, Low Watermark 보다 낮으면 해제합니다. Low Watermark 는 High Watermark 보다 작은 값을 갖어야 합니다.

명령어	설명	모드
show system resource	MCU/SWU 의 자원 정보 조회	Enable
System [MCU swu] [cpu memory] threshold <1-100> <1-100>	처음 <1-100>이 high watermark, 나중 <1-100>이 low watermark	Config-system
System [MCU swu] (cpu duration <5-300> memory duration <1-10>)	Cpu 의 duration 은 5 초~300 초, 메모리의 duration 은 1 분~10 분까지 설정할 수 있음	-

```

OG1100#show system resource
  MCU RESOURCE STATUS INFORMATION
=====
RESOURCE                CPU                MEMORY
-----
CURRENT UTILIZATION     0.0 %             56.0 %
DURATION                 60 Secs           5 Mins
AVERAGE UTILIZATION     0.7 %             56.0 %
HIGH WATERMARK           90                 80
LOW WATERMARK            80                 60
-----

  SWU RESOURCE STATUS INFORMATION
=====
RESOURCE                CPU                MEMORY
-----
CURRENT UTILIZATION     0.0 %             40.8 %
DURATION                 60 Secs           5 Mins
AVERAGE UTILIZATION     0.0 %             40.8 %
HIGH WATERMARK           90                 80
LOW WATERMARK            80                 60
=====
    
```

```

OG1100(config-sys)#system MCU cpu threshold 88 77
OG1100(config-sys)#system MCU memory threshold 89 78
OG1100(config-sys)#system MCU cpu duration 34
OG1100(config-sys)#system MCU memory duration 2
OG1100(config-sys)#system swu cpu threshold 77 66
OG1100(config-sys)#system swu memory threshold 78 67
OG1100(config-sys)#system swu cpu duration 23
OG1100(config-sys)#system swu memory duration 3
    
```

```

OG1100#show system resource
  MCU RESOURCE STATUS INFORMATION
=====
RESOURCE                CPU                MEMORY
-----
CURRENT UTILIZATION    0.5 %            56.0 %
DURATION                34 Secs          2 Mins
AVERAGE UTILIZATION    0.2 %            56.0 %
HIGH WATERMARK          88                89
LOW WATERMARK           77                78
=====

  SWU RESOURCE STATUS INFORMATION
=====
RESOURCE                CPU                MEMORY
-----
CURRENT UTILIZATION    0.0 %            40.8 %
DURATION                23 Secs          3 Mins
AVERAGE UTILIZATION    0.1 %            40.8 %
HIGH WATERMARK          77                78
LOW WATERMARK           66                67
=====
    
```

2.4 시스템의 경고 등급 설정 및 발령 조회

시스템 운영중 발생하는 경고에 대해 경고 등급(Critical, Major, Minor)을 설정 할 수 있으며 해당 등급에 대한 경보를 조회할 수 있습니다.

경보 등급은 critical, major, minor, intermenate 로 구분 되면 서비스에 미치는 영향에 따라 NSA(None Service Affect)와 SA(Service Affect)로 구분됩니다.

명령어	설명	모드
Show alarm [critical major minor]	현재 발령중인 경고에 대해 각 등급별로 조회	Enable
show alarm log	경보의 발령/해제에 대한 과거 정보 조회	Enable
Show alarm severity	시스템에서 정의 되어 있는 모든 경고에 대해 등급 조회	Enable
Alarm severity (cardRemove fanFail feLinkFault gbeLinkFault gbeModuleOut gbeModuleRxFail geModuleTxFail hardwareFail ipcFail oltLinkFault oltOpticFail onuCriticalEvt onuDyingGasp onuLinkFault pwrFail typeMismatch) (critical major minor intermenate) (nsa sa)	시스템에서 정의 되어 있는 모든 alarm 에 대해 등급을 변경하거나 설정	Config-system

```

OG1100#show alarm
IF_NAME      UNIT TYPE  ALARM              SEVERITY  SA      DATE&TIME
-----
EPU          cardRemove
7/1          SWU        gbeModuleOut      CRITICAL  SA      2006-02-21,09:45:14
5/2          EPU        oltLinkFault      CRITICAL  SA      2006-02-20,18:00:19
4            EPU        cardRemove        CRITICAL  SA      2006-02-20,17:59:51
PWU-B       PWU        cardRemove        CRITICAL  SA      2006-02-20,07:33:11
OG1100#show alarm critical
IF_NAME      UNIT TYPE  ALARM              SEVERITY  SA      DATE&TIME
-----
3            EPU        cardRemove        CRITICAL  SA      2006-02-22,08:22:36
7/1          SWU        gbeModuleOut      CRITICAL  SA      2006-02-21,09:45:14
5/2          EPU        oltLinkFault      CRITICAL  SA      2006-02-20,18:00:19
4            EPU        cardRemove        CRITICAL  SA      2006-02-20,17:59:51
PWU-B       PWU        cardRemove        CRITICAL  SA      2006-02-20,07:33:11
OG1100#show alarm major
IF_NAME      UNIT TYPE  ALARM              SEVERITY  SA      DATE&TIME
-----
OG1100#show alarm minor
IF_NAME      UNIT TYPE  ALARM              SEVERITY  SA      DATE&TIME
-----

```

```

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#system
OG1100(config-sys)#alarm severity cardRemove major nsa

OG1100#show alarm critical
IF_NAME      UNIT TYPE  ALARM              SEVERITY  SA      DATE&TIME
-----
7/1          SWU        gbeModuleOut      CRITICAL  SA      2006-02-21,09:45:14
5/2          EPU        oltLinkFault      CRITICAL  SA      2006-02-20,18:00:19
7/5          SWU        gbeLinkFault      CRITICAL  SA      2006-02-20,08:43:03
7/4          SWU        gbeModuleRxFail   CRITICAL  SA      2006-02-20,07:33:20
OG1100#show alarm
IF_NAME      UNIT TYPE  ALARM              SEVERITY  SA      DATE&TIME
-----
3            EPU        cardRemove        MAJOR     NSA     2006-02-22,18:50:53
4            EPU        cardRemove        MAJOR     NSA     2006-02-22,18:50:53
9            EPU        cardRemove        MAJOR     NSA     2006-02-22,18:50:53
8            EPU        cardRemove        MAJOR     NSA     2006-02-22,18:50:53
PWU-B       PWU        cardRemove        MAJOR     NSA     2006-02-22,18:50:53
7/1          SWU        gbeModuleOut      CRITICAL  SA      2006-02-21,09:45:14
5/2          EPU        oltLinkFault      CRITICAL  SA      2006-02-20,18:00:19
7/5          SWU        gbeLinkFault      CRITICAL  SA      2006-02-20,08:43:03
7/4          SWU        gbeModuleRxFail   CRITICAL  SA      2006-02-20,07:33:20

```

2.5 가청 경보 설정 및 조회

시스템에서 경보가 발생하면 랙에서 부저가 울려 경보 발생을 알립니다. 토글 스위치가 off에 놓여 있을 때에만 가청 경보가 발생합니다. 가청 경보 발령시 토글스위치를 ACO 로 토글시키거나 토글 스위치를 LOCK 에 놓아 가청 경보를 해제할 수 있습니다. ACO 로 토글시키는 방법은 가청 경보를 일회성 해제시킵니다.

랙에 여러 개의 셸프가 있을 때, 어느 하나의 셸프의 토글 스위치만 Lock 에 놓여 있어도 가청경보는 발생하지 않습니다.

콘솔 터미널을 통하여 토글 스위치를 사용하는 것과 동일한 기능을 수행할 수 있습니다.

명령어	설명	모드
show aco	현재 aco 의 상태를 조회합니다.	Enable
Opr aco	가청 경보를 해제합니다.	Config-system
Aco(lock unlock)	가청 경보를 lock[unlock]합니다.	Config-system

```

OG1100#show aco
=====
ACO CONTROL STATE : UNLOCK
=====
OG1100#opr aco
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#system
OG1100(config-sys)#aco lock
OG1100#show aco
=====
ACO CONTROL STATE : LOCK
=====
    
```

2.6 SLOT 상태 설정 및 조회

시스템의 인터페이스 카드를 실장할 슬롯의 Administrative State 를 설정하는 방법입니다. Factory Default 상태의 시스템은 슬롯의 상태가 ‘disable’상태로 설정되어 있습니다.

명령어	설명	모드
show system slot	시스템의 slot 의 상태 표시	Enable
no shutdown slot epu<1~9>	epu1~epu8 : 사용하고자 하는 epu # 을 enable	Config-system
shutdown slot epu<1~9>	epu1~epu8 : 사용하고자 하는 epu # 을 disable	Config-system

```

OG1100#show system slot
SLOT INFORMATION
=====
SLOT (NO/TYPE)      MODULE TYPE      ADMIN STATE      OPER STATE
-----
1    PWU-A           PWU-DC           ENABLE           NORMAL
2    EPU1            EPU-A            DISABLE          NORMAL
3    EPU2            ----             DISABLE          ALARM
4    EPU3            ----             DISABLE          ALARM
    
```

5	EPU4	----	DISABLE	ALARM
6	MCU	MCU	ENABLE	NORMAL
7	SWU	SWU-B8	ENABLE	NORMAL
8	EPU5	----	DISABLE	ALARM
9	EPU6	EPU-A	DISABLE	NORMAL
10	EPU7	----	DISABLE	ALARM
11	EPU8	EPU-A	DISABLE	NORMAL
12	PWU-B	PWU-DC	ENABLE	NORMAL

1	FAN-1	FAN	ENABLE	NORMAL
2	FAN-2	FAN	ENABLE	NORMAL
3	FAN-3	FAN	ENABLE	NORMAL
=====				

슬롯의 Administrative State 설정은 SYSTEM_MODE 에서 수행하며 명령어는 다음과 같습니다. 설정이 가능한 슬롯은 EPU1~EPU8 이며 나머지 슬롯은 기본 값으로 Enable 상태로 설정되어 있으며 변경할 수 없습니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#system
OG1100(config-sys)#no shutdown slot epul
OG1100#show system slot
SLOT INFORMATION
=====
SLOT (NO/TYPE)      MODULE TYPE      ADMIN STATE      OPER STATE
-----
1    PWU-A          PWU-DC          ENABLE          NORMAL
2    EPU1           EPU-A          ENABLE          NORMAL
3    EPU2           ----           DISABLE         ALARM
4    EPU3           ----           DISABLE         ALARM
5    EPU4           ----           DISABLE         ALARM
6    MCU            MCU            ENABLE          NORMAL
7    SWU            SWU-B8        ENABLE          NORMAL
8    EPU5           ----           DISABLE         ALARM
9    EPU6           EPU-A        DISABLE         NORMAL
10   EPU7           ----           DISABLE         ALARM
11   EPU8           EPU-A        DISABLE         NORMAL
12   PWU-B          PWU-DC        ENABLE          NORMAL
-----
1    FAN-1         FAN           ENABLE          NORMAL
2    FAN-2         FAN           ENABLE          NORMAL
3    FAN-3         FAN           ENABLE          NORMAL
=====

```

2.7 PON OLT, ONU/ONT 의 상태 설정/조회

PON 의 중요한 역할을 담당하는 EPU 인터페이스 카드에 대해서 Administrative State 를 설정하는 방법입니다. PON_MODE 에서 수행되며, CONFIG_MODE 에서 ‘pon’명령어를 수행하면 됩니다. Factory Default 상태의 시스템의 PON 의 OLT 의 상태가 ‘disable’상태로 되어 있으며 변경 및 조회하는 명령은 다음과 같습니다.

명령어	설명	모드
show pon topology olt	OLT 의 모든 pon 상태 출력	Enable
[no] shutdown olt IF_NAME	- OLT 의 PON 의 administrative 상태를 [disable] enable 상태로 변경 - IF_NAME slot/port 설정	Config-pon
[no] shutdown onu IF_NAME	IF_NAME slot/port-onu 설정	Config-pon

```

OG1100#show pon topology olt
PON NETWORK OLT TOPOLOGY INFORMATION
=====
IF_NAME      MAC ADDR          ADMIN  OPER   IPC STATE
-----
2/1          54:4B:37:21:00:78  DISABLE DOWN   UP
2/2          54:4B:37:21:00:79  DISABLE DOWN   UP
3/1          54:4B:37:21:00:00  DISABLE DOWN   UP
3/2          54:4B:37:21:00:47  DISABLE DOWN   UP
4/1          54:4B:37:21:00:98  DISABLE DOWN   UP
4/2          54:4B:37:21:00:99  DISABLE DOWN   UP
5/1          54:4B:37:21:00:62  DISABLE DOWN   DOWN
5/2          54:4B:37:21:00:63  DISABLE DOWN   DOWN
8/1          54:4B:37:21:00:9C  DISABLE DOWN   UP
8/2          54:4B:37:21:00:9D  DISABLE DOWN   UP
9/1          54:4B:37:21:00:3E  DISABLE DOWN   UP
9/2          54:4B:37:21:00:3F  DISABLE DOWN   UP
=====
OG1100# configure terminal
OG1100(config)# pon
OG1100(config-pon)# no shutdown olt 2/1
OG1100(config-pon)# end
OG1100# show pon topology olt
=====
IF_NAME      MAC ADDR          ADMIN  OPER   IPC STATE
-----
2/1          54:4B:37:21:00:78  ENABLE  DOWN   UP
2/2          54:4B:37:21:00:79  DISABLE DOWN   UP
3/1          54:4B:37:21:00:00  DISABLE DOWN   UP
3/2          54:4B:37:21:00:47  DISABLE DOWN   UP
4/1          54:4B:37:21:00:98  DISABLE DOWN   UP
4/2          54:4B:37:21:00:99  DISABLE DOWN   UP
5/1          54:4B:37:21:00:62  DISABLE DOWN   DOWN
5/2          54:4B:37:21:00:63  DISABLE DOWN   DOWN
8/1          54:4B:37:21:00:9C  DISABLE DOWN   UP
8/2          54:4B:37:21:00:9D  DISABLE DOWN   UP
9/1          54:4B:37:21:00:3E  DISABLE DOWN   UP
9/2          54:4B:37:21:00:3F  DISABLE DOWN   UP
=====
    
```

2.8 PON 의 ONT 등록 및 조회

ONU/ONT 를 시스템의 자원으로 사용하기 위해서 특정 인덱스를 부여하여 ONU/ONT 정보를 등록해야 합니다. 등록되지 않은 ONU/ONT 의 트래픽은 차단됩니다.

PON_MODE 에서 수행되며, 이 모드에서는 PON 을 OLT/ONU 로 구분합니다. 현재 수용 가능한 ONT 종류는 OG-3500AB, OG-3500DB 두 종류입니다.

2.8.1 ONT 의 등록 및 조회

등록하고자하는 ONU/ONT 의 인터페이스 이름, MAC 어드레스, ONU/ONT 유형, 위치정보 등을 입력합니다.

이러한 수동 등록 절차를 거치지 않으면 시스템의 자원으로 사용할 수 없습니다. SLOT 및 PON OLT 의 Administrative State 가 ‘enable’상태일 경우, 수동 등록 절차를 거치지 않아 Blocking 된 ONU/ONT 에 대한 정보 조회가 가능하며, Blocking 된 ONU/ONT 에 대한 등록 절차를 수행하면 시스템의 자원으로 사용할 수 있게 됩니다. 등록된 ONU/ONT 의 Administrative State 는 ‘enable’상태가 됩니다.

명령어	설명	모드
Topology onu <i>IF_NAME</i> MAC_ADDR onotype(og-3500ab og-3500db) loc LOCATION	ONU/ONT 를 시스템의 자원으로 등록 - IF_NAME : Index(slot/port-onu) - MAC_ADDR : xx:xx:xx:xx:xx - og-3500ab : Premium ONT, 4 FE - og-3500db : Megapass ONT, 1 FE - LOCATION : 위치 정보 문자열	Config-pon
show pon topolgy onu <i>IF_NAME</i>	ONU 의 등록상태 조회 - IF_NAME : OLT Index(slot/port)	Enable
show pon blocked-links <i>IF_NAME</i>	등록 절차를 거치지 않아 Blocking 된 ONU/ ONT 조회 - IF_NAME : OLT Index(slot/port)	Enable

```

OG1100# show pon blocked-links 2/2
LIST OF BLOCKED LINKS INFORMATION
=====
IF NAME      MAC ADDRESS
-----
              54:4B:37:10:00:18
=====
OG1100# configure terminal
OG1100(config)# pon
OG1100(config-pon)# topology onu 2/2-1 54:4B:37:10:00:18 onotype
og3500-ab
OG1100(config-pon)# end
OG1100# show pon topology onu 2/2
PON NETWORK ONU TOPOLOGY FOR OLT(2/2) INFORMATION
=====
IF_NAME      MAC ADDR      ADMIN  OPER   ONU TYPE
              LOCATION
    
```

```

-----
2/2-1      54:4B:37:10:00:18  ENABLE  up    OG35000-AB
=====
OG1100#
    
```

2.8.2 ONU/ONT의 정보 변경 및 삭제

운영자가 ONU/ONT의 변경 및 삭제를 하기 위해서는 PON_MODE에서 먼저, ONU/ONT의 administrative status의 'disable'로 변경해야 합니다. 수행은 'shutdown'명령어를 사용해야 합니다.

명령어	설명	모드
Shutdown onu <i>IF_NAME</i> no topology onu <i>IF_NAME</i> topology edit-onu mac <i>IF_NAME</i> <i>MAC_ADDR</i> topology edit-onu loc <i>IF_NAME</i> <i>LOCATION</i>	<ul style="list-style-type: none"> - 해당 Onu의 상태를 'disable'로 변경 - 등록된 ONU/ONT의 삭제 - 등록된 ONU/ONT의 MAC Address 정보 변경 - 등록된 ONU/ONT의 위치 정보 변경 	Config-pon
show pon topolgy onu <i>IF_NAME</i>	ONU의 등록상태 출력 - IF_NAME : OLT Index(slot/port)	Enable

```

OG1100# configure terminal
OG1100(config)# pon
OG1100(config-pon)# topology edit-onu loc 2/2-1 suwon IT BUILDING 24
OG1100(config-pon)# end
OG1100# show pon topology onu 2/2
  PON NETWORK ONU TOPOLOGY FOR OLT(2/2) INFORMATION
=====
IF_NAME      MAC ADDR          ADMIN  OPER   ONU TYPE
  LOCATION
-----
2/2-1      54:4B:37:10:00:18  ENABLE  up    OG35000-AB
  suwon IT BUILDING 24
=====
OG1100(config-pon)# no topology onu 2/2-1 54:4B:37:10:00:18
OG1100(config-pon)# end
OG1100# show pon topology onu 2/2
  PON NETWORK ONU TOPOLOGY FOR OLT(2/2) INFORMATION
=====
IF_NAME      MAC ADDR          ADMIN  OPER   ONU TYPE
  LOCATION
-----
=====
OG1100#
    
```


2.9 SWU 포트 설정 및 상태 조회

24Gbps 스위치인 SWU의 포트의 환경 설정 정보, 상태 정보 및 통계 데이터를 조회하고자 할 경우 다음 명령어를 사용합니다.

명령어	설명	모드
show portstatus	모든 포트의 상태 정보 요약 출력	Enable

시스템 운영자는 다음과 같이 'show portstatus' 명령어를 통하여 SWU 각 포트의 다양한 상태 정보를 볼 수 있습니다.

현재는 Admin status 는 port no shutdown 명령어를 수행한 포트는 enable 으로 보여지고 그렇지 않으면 기본적으로 disable 으로 설정되어 있습니다.

```

OG1100# show port status
-----
      NO          | STATUS |          MODE          | PAUSE | STATE
      |-----| |-----| |-----| |-----|
      | ADM OP | |          | | TX  RX |
-----|-----| |-----| |-----|
EPU  2/1 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  2/2 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  3/1 | EN  DN | AUTO 1000 FD | OFF OFF | DIS
EPU  3/2 | EN  DN | AUTO 1000 FD | OFF OFF | DIS

EPU  4/1 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  4/2 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  5/1 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  5/2 | EN  UP | AUTO 1000 FD | OFF OFF | FWD

EPU  8/1 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  8/2 | EN  UP | AUTO 1000 FD | OFF OFF | FWD
EPU  9/1 | EN  DN | AUTO 1000 FD | OFF OFF | DIS
EPU  9/2 | EN  DN | AUTO 1000 FD | OFF OFF | DIS

EPU 10/1 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
EPU 10/2 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
EPU 11/1 | EN  DN | AUTO 1000 FD | OFF OFF | DIS
EPU 11/2 | EN  DN | AUTO 1000 FD | OFF OFF | DIS

SWU  7/1 | DIS DN | AUTO 1000 FD | OFF OFF | FWD
SWU  7/2 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
SWU  7/3 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
SWU  7/4 | DIS DN | AUTO 1000 FD | OFF OFF | DIS

SWU  7/5 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
SWU  7/6 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
SWU  7/7 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
SWU  7/8 | DIS DN | AUTO 1000 FD | OFF OFF | DIS
-----
ADM      : Port ENable/DISable
OP       : Link UP/DowN
MODE     : AUTO-Nego/FORCEd, Mbps, Full/Half
PAUSE    : TX - Transmit Pause Frame ON/OFF
PAUSE    : RX - Obey Pause Frame ON/OFF
STATE    : FWD / LRN / LIS / BLK / DIS
OG1100#
    
```

2.9.1 물리적 포트 상태 변경 및 조회

SWU의 포트를 사용하기 위해서는 administratvie status 을 변경합니다. ENABLE_MODE 에 서 CONFIG_MODE 에서 INTERFACE_MODE 로 변경 후 'no shutdown'을 실행합니다.

명령어	설명	모드
no shutdown	- 포트의 상태를 enable 로 변경	Config- interface
shutdown	- 포트의 상태를 disable 로 변경	

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface 7/5
OG1100(config-if)#no shutdown
OG1100(config-if)#exit
OG1100(config)#exit
OG1100# show portstatus
-----

```

NO	STATUS		MODE	PAUSE		STATE
	ADM	OP		TX	RX	
EPU 2/1	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 2/2	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 3/1	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 3/2	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 4/1	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 4/2	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 5/1	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 5/2	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 8/1	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 8/2	EN	UP	AUTO 1000 FD	OFF	OFF	FWD
EPU 9/1	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 9/2	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 10/1	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 10/2	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 11/1	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
EPU 11/2	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/1	DIS	DN	AUTO 1000 FD	OFF	OFF	FWD
SWU 7/2	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/3	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/4	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/5	EN	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/6	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/7	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS
SWU 7/8	DIS	DN	AUTO 1000 FD	OFF	OFF	DIS

```

-----
ADM      : Port ENable/DISable
OP       : Link UP/DowN
MODE     : AUTO-Nego/FORCEd, Mbps, Full/Half
PAUSE    : TX - Transmit Pause Frame ON/OFF
PAUSE    : RX - Obey Pause Frame ON/OFF
STATE    : FWD / LRN / LIS / BLK / DIS
OG1100#

```

2.9.2 물리적 포트상태 변경

SWU의 각 포트에서 대한 물리적인 특성을 설정하기 위해서는 INTERFACE_MODE로 들어가서 ‘auto-negotiation on(off)’, ‘speed 1000(10/100)’, ‘duplex full(half)’로 실행합니다.

명령어	설명	모드
Auto-negotiation {on/off} speed {1000/100/10} duplex {full/half}	- Autonegotiation 상태변경 - Speed 상태변경 - Duplex 상태변경	Config-interface

2.9.3 포트의 흐름 제어 (IEEE 802.3x) 설정

OG-1100은 포트의 흐름 제어 기능이 동작하도록 혹은 동작하지 않도록 설정할 수 있습니다. 포트의 흐름 제어 기능은 트래픽 혼잡(congestion)이 발생했을 때 트래픽의 전송 속도를 조절하는 기능입니다. 흐름 제어 기능이 동작하고 있는 포트에서는, 포트의 트래픽이 혼잡 상태가 되어 더 이상의 트래픽을 수신할 수 없게 되는 경우, 다른 포트에 이러한 상태를 알려주고 혼잡상태가 나아질 때까지 패킷을 전송하지 못하도록 요청하게 됩니다.

OG-1100의 포트들은 기본적으로 이러한 흐름 제어 기능이 동작하지 않도록 설정되어 있습니다. 지정한 포트에서 흐름 제어 기능이 동작하도록 하거나 혹은 동작하지 않도록 설정하려면 다음 작업을 수행합니다.

명령어	설명	모드
Interface IFNAME	인터페이스 모드로 변경	config
flowcontrol <receive send> <on off>	흐름 제어 기능의 동 여부 지정	Config-interface

다음은 7번 슬롯에 장착된 모듈의 1번 Gigabit Ethernet 포트의 흐름 제어 기능이 동작하도록 설정하는 예입니다.

```

OG1100(config)#interface 7/1
OG1100(config-if)# flowcontrol receive on
OG1100(config-if)# flowcontrol send on
OG1100(config-if)# exit
OG1100# show flowcontrol
    
```

Port	Send FlowControl admin oper	Receive FlowControl admin oper	RxPause	TxPause
2/1	off off	off off	0	0
2/2	off off	off off	0	0
3/1	off off	off off	0	0
3/2	off off	off off	0	0
4/1	off off	off off	0	0
4/2	off off	off off	0	0

2 장. 시스템 초기 환경 설정

5/1	off	off	off	off	0	0
5/2	off	off	off	off	0	0
7/1	on	on	on	on	0	0
7/2	off	off	off	off	0	0
7/3	off	off	off	off	0	0
7/4	off	off	off	off	0	0
7/5	off	off	off	off	0	0
7/6	off	off	off	off	0	0
7/7	off	off	off	off	0	0
7/8	off	off	off	off	0	0
8/1	off	off	off	off	0	0
8/2	off	off	off	off	0	0
9/1	off	off	off	off	0	0
9/2	off	off	off	off	0	0
10/1	off	off	off	off	0	0
10/2	off	off	off	off	0	0
11/1	off	off	off	off	0	0
11/2	off	off	off	off	0	0

3장. 시스템 설정 및 조회

3.1 PON 환경 설정

이 절에서는 PON OLT 및 ONU 환경 설정에 관한 명령어와 적용 예를 보여줍니다.

PON 설정은 기본적으로 Service Profile 을 작성하고 이를 인터페이스에 적용하는 방식을 따릅니다. OLT 와 ONU Service Profile 작성 및 적용 명령어는 각각 PON_MODE 의 Sub-mode 인 OLT_QOS_MODE 와 ONU_QOS_MODE 에서 수행됩니다.

3.1.1 PON OLT 환경 설정

OLT Service Profile 은 Policy-map, Bridge-map, 그리고 Igmp-map 으로 구성됩니다.

Policy-map 은 Aggregated Bandwidth 설정 및 DBA 환경 설정, Packet Filtering 설정 등의 항목으로 구성되며, Bridge-map 은 Bridging Configuration 설정을 포함하며, Igmp-map 은 IGMP Proxy 설정으로 구성됩니다.

시스템의 초기 설정은 'oltProfile'이라는 Service Profile 로 설정되어 있으며, 이는 Policy-map 으로 'oltPmap'를 Bridge-map 으로 'oltBmap'을, 그리고 Igmp-map 으로 'oltImap'을 포함합니다.

명령어	설명	모드
olt-qos	OLT Service Profile 작성 모드로 변경	Config-pon

3.1.1.1 OLT Service Profile 의 작성 및 적용

OLT Service Profile 을 작성하려면 우선 Policy-map, Bridge-map, Igmp-map 을 먼저 작성해야 합니다. Service Profile 작성 및 삭제, 그리고 OLT 포트 인터페이스에의 적용 명령어는 아래와 같습니다.

명령어	설명	모드
service-map PROFILE_NAME policy-map POLICY_NAME bridge- map BRIDGE_NAME igmp-map IGMP_NAME	OLT Service Profile 작성 - PROFILE_NAME : Service Profile Name - POLICY_NAME : Policy-map Name - BRIDGE_NAME : Bridge-map Name - IGMP_NAME : Igmp-map Name	Config- pon-oltqos
no service-map PROFILE_NAME	OLT Service Profile 삭제 - Default Profile(oltProfil)과 현재 인터페이스 에 적용 중인 Profile 은 삭제 불가	Config- pon-oltqos

(계속)

명령어	설명	모드
no class-map MAP_NAME	OLT Class-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-oltqos
no policy-map MAP_NAME	OLT Policy-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-oltqos
no bridge-map MAP_NAME	OLT Bridge-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-oltqos
no igmp-map MAP_NAME	OLT Igmp-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-oltqos
service-policy IF_NAME service-map PROFILE_NAME	IF_NAME : OLT Port 인터페이스 Name PROFILE_NAME : OLT Service Profile Name	Config-pon-oltqos
show pon service-map olt (PROFILE_NAME)	OLT Service Profile List 조회 또는 특정 Service Profile 의 내용 조회	enable
Show pon service-policy olt (IF_NAME)	OLT Port Interface 에 현재 적용된 Service Profile 조회	enable

3.1.1.2 OLT Class-map 의 작성

OLT Class-map 은 Packet 을 분류하기 위한 Rule 을 설정하는 Map 입니다. 이 Map 은 Policy-map 에서 Packet 을 Drop 하기 위한 조건으로 사용됩니다. 이 Rule 은 Field 와 Lookup Value, 그리고 Operator 로 구성되며, 하나의 Map 은 Rule 을 2 개까지 포함할 수 있으며, 2 개의 Rule 은 ‘AND’ 연산자가 적용되어 ‘Rule Chain’을 구성합니다. OLT_QOS_MODE 에서 ‘class-map’ 명령어를 이용하여 OLT_CMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
olt-qos	OLT Service Profile 작성 모드로 변경	Config-pon
class-map MAP_NAME	Class-map 작성 모드로 변경	Config-pon-oltqos
(no) classrule FIELD LOOKUP_VALUE OPERATOR	Class-map 에 한 개의 Rule 추가 및 삭제 - FIELD, LOOKUP_VALUE, OPERATOR 값은 아래 참조	Config-pon-oltqos-cmap
Map-end	Class-map 작성 완료 및 상위 모드로 전환 이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.	Config-pon-oltqos-cmap
Show pon class-map olt (MAP_NAME)	OLT Class-map List 조회 또는 특정 Class-map 상세 정보 조회	enable

Field Selectors

- l2-da : L2 Destination Address
- l2-sa : L2 Source Address
- llid : Link Index
- ether-type : L2 Length/Type
- vlan : VLAN ID
- l3-da : L3 Destination Address(IPv4)
- l3-sa : L3 Source Address(IPv4)
- l4-dp : L4 Destination Port Number
- l4-sp : L4 Source Port Number
- cos : Class of Service
- tos : Type of Service

Rule Operators

- Never-match : Never match
- Eq : Field Equal to value
- Neq : Field Not equal to value
- Lteq : Field Less than or equal to value
- Gteq : Field Greater than or equal to value
- Exist : True if field exists(value ignored)
- Not-exist : True if field does not exist(value ignored)
- Always : Always match

Lookup Value

Field Selector	Lookup Value String
l2-da, l2-sa	XX:XX:XX:XX:XX:XX(예 : 54:4B:37:11:00:10)
llid	1~4
ether-type	0xXXXX(예 : 0x8100)
vlan	0~4094
l3-da, l3-sa	xxx.xxx.xxx.xxx(예 : 192.168.0.100)
l4-dp, l4-sp	0~65535
cos, tos	0~7

3.1.1.3 OLT Policy-map 의 작성

OLT Policy-map 은 OLT Port 의 Aggregated Bandwidth, DBA 파라미터, Port Filtering Rule 설정 등으로 구성됩니다. OLT_QOS_MODE 에서 ‘policy-map’ 명령어를 이용하여 OLT_PMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
olt-qos	OLT Service Profile 작성 모드로 변경	Config-pon
policy-map MAP_NAME	Policy-map 작성 모드로 변경	Config-pon-oltqos
aggregate bandwidth (upstream downstream) <0-1000000> <0-256>	Aggregated Bandwidth 설정 - Aggregate bandwidth(Kbps) - <0-256> : Max burst size(KB)	Config-pon-oltqos-pmap
bcstsla(enable disable)	Broadcast LLID 에 대한 SLA State 설정	Config-pon-oltqos-pmap
bcstsla control <0-1000000> <0-1000000> (sensitive tolerant) <1-256>	Broadcast LLID 에 대한 SLA 설정 - Minimum Guaranteed Bandwidth(Kbps) - Maximum Allowed Bandwidth(Kbps) - Delay Sensitive - Max burst size(KB)	Config-pon-oltqos-pmap
bcstsla weight <0-255> <0-511> <0-511>	Broadcast LLID 에 대한 SLA Weigh 설정 (단위 : KB) - <0-255> : DBA Tokens - <0-511> : Scheduler Min-tokens - <0-511> : Scheduler Max-tokens	Config-pon-oltqos-pmap
dba drop-down weight <0-16383> <0-16383> <0-16383>	우선순위 레벨에 대한 Upstream Drop-down weight 설정(단위 : KB) - Drop-down for Level 0 - Drop-down for Level 1 - Drop-down for Level 2	Config-pon-oltqos-pmap
dba polling rate <1-65535> <1-65535> <1-65535>	우선순위 레벨에 대한 DBA Polling Rate 설정 (단위 : 65.5 us) - Polling rate at Level 0 - Polling rate at Level 1 - Polling rate at Level 2	Config-pon-oltqos-pmap
priority block size <0-239> <0-239> <1-239>	우선순위 레벨에 허용할 Link 의 최대 개수 - Number of Priority 0 Links - Number of Priority 1 Links - Number of Priority 2 Links	Config-pon-oltqos-pmap
filtering discard olt port (upstream downstream) <0-7> class-map MAP_NAME	OLT Upstream EPON Port 및 Downstream Network Port 에 Packet Filtering Rule 설정 - <0-7> : Priority - MAP_NAME : OLT Class-map Name	Config-pon-oltqos-pmap

(계속)

명령어	설명	모드
Map-end	Policy-map 작성 완료 및 상위 모드로 전환 (이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon-oltqos-pmap
Show pon policy-map olt (MAP_NAME)	OLT Policy-map List 조회 또는 특정 Policy-map 상세 정보 조회	enable

위에서 언급한 우선순위는 세 개의 레벨이 존재하며 각각 0(High), 1(Medium), 2(Low)입니다. 이는 Link 에 대한 SLA 설정 파라미터, 즉 Minimum Guaranteed Bandwidth(MGB), Maximum Allowed Bandwidth(MAB), Delay Sensitive 에 따라 아래와 같은 레벨을 가집니다.

Provisioned Bandwidth	Delay Sensitive	Priority Level
MGB == MAB	Sensitive	0
MGB > 0	Tolerant	1
MGB == 0	Tolerant	2
MGB != MAB	Sensitive	Invalid

3.1.1.4 OLT Bridge-map 의 작성

OLT Bridge-map 은 OLT 포트의 Bridge 관련 설정을 포함합니다. OLT_QOS_MODE 에서 'bridge-map' 명령어를 이용하여 OLT_BMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
olt-qos	OLT Service Profile 작성 모드로 변경	Config-pon
bridge-map MAP_NAME	Bridge-map 작성 모드로 변경	Config-pon-oltqos
Bridgeconfig allow-simple-bridging(on off)	Allow Simple Bridging	Config-pon-oltqos-bmap
Bridgeconfig allow-vlan-tags-on-simple-bridge(on off)	Allow Tagged Frames on Simple Bridge	Config-pon-oltqos-bmap
Bridgeconfig discard-unknown-mac(on off)	Discard Unknown MAC Option	Config-pon-oltqos-bmap
Bridgeconfig downstream-frame-reset-age(on off)	Downstream Frames Reset Age	Config-pon-oltqos-bmap
Bridgeconfig learned-entry-age-limit <0-32768>	Learned entry age limit(단위 : 8.75 ms) - 2 의 거듭제곱 수	Config-pon-oltqos-bmap
Bridgeconfig mac-learning-overwrite(on off)	MAC Learning overwrite	Config-pon-oltqos-bmap
Bridgeconfig number-of-bridged-vlans <0-30>	Number of Bridged VLANs	Config-pon-oltqos-bmap

(계속)

명령어	설명	모드
Map-end	Bridge-map 작성 완료 및 상위 모드로 전환 (이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon-oltqos-bmap
Show pon bridge-map olt (MAP_NAME)	OLT Bridge-map List 조회 또는 특정 Bridge-map 상세 정보 조회	enable

3.1.1.5 OLT Igmp-map 의 작성

OLT Igmp-map 은 OLT Port 의 IGMP Proxy 관련 설정을 포함합니다. OLT_QOS_MODE 에서 'igmp-map' 명령어를 이용하여 OLT_IMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
olt-qos	OLT Service Profile 작성 모드로 변경	Config-pon
igmp-map MAP_NAME	igmp-map 작성 모드로 변경	Config-pon-oltqos
igmp proxy max-igmp-groups <0-4096>	Maximum IGMP Group 수 설정 (0 은 IGMP Proxy Disable)	Config-pon-oltqos-imap
igmp proxy robustness-count <1-16>	Robustness Count	Config-pon-oltqos-imap
igmp proxy query-int	Query Interval(단위 : 10 ms)	Config-pon-oltqos-imap
igmp proxy query-res-timeout <1-2600>	Query Response Time(단위 : 10 ms)	Config-pon-oltqos-imap
igmp proxy query-msg-max-res-time <1-255>	Query Message Maximum Response Time (단위 : 100 ms)	Config-pon-oltqos-imap
igmp proxy startup-query-cnt <0-16>	Startup Query Count	Config-pon-oltqos-imap
igmp proxy startup-query-int <1-65534>	Startup Query Interval(단위 : 10 ms)	Config-pon-oltqos-imap
igmp proxy last-mem-query-cnt <0-16>	Last Member Query Count	Config-pon-oltqos-imap
igmp proxy last-mem-query-int	Last Member Query Interval(단위 : 10 ms)	Config-pon-oltqos-imap
igmp proxy last-mem-query-msg-max-res-time <1-255>	Last Member Query Message Maximum Response Time(단위 : 100 ms)	Config-pon-oltqos-imap
igmp proxy retransmit-cnt <0-3>	Retransmit Count	Config-pon-oltqos-imap
igmp proxy retransmit-int <1-65534>	Retransmit Interval(단위 : 10 ms)	Config-pon-oltqos-imap
igmp proxy vlan-tag <0-65534>	VLAN Tag(0 : IGMP Query 에서 VLAN 을 제거)	Config-pon-oltqos-imap

(계속)

명령어	설명	모드
lgmp proxy igmp-queue-num <1-10>	Number of IGMP Queues	Config-pon-oltqos-imap
lgmp proxy source-ip IP_ADDR	Source IP address in IGMP frames	Config-pon-oltqos-imap
lgmp proxy sla <0-100000> <0-100000> (sensitive tolerant) <1-256>	IGMP SLA - Minimum Guaranteed Bandwidth(Kbps) - Maximum Allowed Bandwidth(Kbps) - Delay Sensitive - Max burst size(KB)	Config-pon-oltqos-imap
Map-end	lgmp-map 작성 완료 및 상위 모드로 전환 (이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon-oltqos-imap
Show pon igmp-map olt (MAP_NAME)	OLT lgmp-map List 조회 또는 특정 lgmp-map 상세 정보 조회	enable

3.1.1.6 OLT IGMP VLAN 설정

IGMP Proxy 는 최대 8 개까지의 VLAN 을 허용합니다. 아래의 명령어는 Proxy 가 처리할 VID 를 설정하고 IGMP Group 별로 Bandwidth 를 설정하는 기능을 수행합니다.

명령어	설명	모드
lgmp vlan fcfs-pool-size IF_NAME <0-1000000>	OLT 포트 인터페이스에 FCFS Pool Size 설정 (단위 : Kbps)	Config-pon
lgmp vlan IF_NAME <0-4093> <0-4093> <0-1000000> <0-1000000> <0-1000000>	OLT 포트 인터페이스에 IGMP VLAN 설정 - Network VLAN ID(0 : untagged) - EPON VLAN ID(0 : strip) - VLAN Min Guaranteed Bandwidth - VLAN Max Allowed Bandwidth - Default Per-channel Bandwidth	Config-pon
lgmp channel single IF_NAME <0-4093> GROUP_IP <1-1000>	'igmp 피우' 명령으로 추가한 IGMP VLAN 에 대하여 단일 Group 의 Bandwidth 를 설정 - Network VLAN ID - Group : 224.0.1.0~239.255.255.255 - Group Bandwidth(Kbps)	Config-pon
lgmp channel range IF_NAME <0-4093> FROM_IP TO_IP <1-1000>	'igmp 피우' 명령으로 추가한 IGMP VLAN 에 대하여 특정 범위에 포함되는 Group 의 Bandwidth 를 동일하게 설정 - Network VALN ID - From Goup IP - To Group IP - Group Bandwidth(Kbps)	Config-pon

(계속)

명령어	설명	모드
Show pon igmp vlan IF_NAME	IGMP VLAN 설정 상태 조회	Enable
Show pon igmp channel IF_NAME <0-4093>	IGMP VLAN 에 대하여 Channel 별 Bandwidth 설정 상태 조회	enable
Show pon igmp cac IF_NAME	설정된 IGMP VLAN 에 대하여 current bandwidth usage 조회	enable
Show pon igmp group-status-for-group IF_NAME <0-4093> GROUP_IP	OLT 가 현재 Forwarding 하고 있는 Group 의 List 조회	enable
Show pon igmp group-status-for-van IF_NAME <0-4093>	OLT 가 현재 Forwarding 하고 있는 Group 의 List 조회	enable

3.1.2 PON ONU 환경 설정

ONU Service Profile 은 Queue-map, Policy-map, Bridge-map, Igmp-map 으로 구성됩니다. Queue-map 은 Upstream Link 및 Downstream Port 에 Queue 를 할당하는 설정으로 구성되며, Policy-map 은 Link 에 SLA 설정, Packet Classification, Filtering 설정 등의 항목으로 구성됩니다.

Bridge-map 은 Bridging Configuration 설정을 포함하며, Igmp-map 은 IGMP Snooping 설정으로 구성됩니다. 시스템의 초기 설정은 ONU 를 등록할 때 입력하는 ONU 종류에 해당하는 Service Profile 로 자동 설정됩니다. 현재 ONU 종류에 따른 Default Profile 은 아래와 같습니다.

ONU 유형	기본 서비스 Profile	
OG-3500AB	onuProfileForOg3500-ab	onuQmapForOg3500-ab onuPmapForOg3500-ab onuBmapForOg3500-ab onulmap
OG-3500DB	onuProfileForOg3500-db	onuQmapForOg3500-db onuPmapForOg3500-db onuBmapForOg3500-db onulmap

ONU Service Profile 작성은 PON_MODE 의 Sub-mode 인 ONU_QOS_MODE 에서 수행합니다.

명령어	설명	모드
onu-qos	ONU Service Profile 작성 모드로 변경	Config-pon

3.1.2.1 ONU Service Profile 의 작성 및 적용

ONU Service Profile 을 작성하려면 우선 Queue-map, Policy-map, Bridge-map, Igmp-map 을 먼저 작성해야 합니다. Service Profile 작성 및 삭제, 그리고 ONU 에의 적용 명령어는 아래와 같습니다.

명령어	설명	모드
service-map PROFILE_NAME queue-map QUEUE_NAME policy-map POLICY_NAME bridge-ap BRIDGE_NAME igmp-map IGMP_NAME (og-3500ab og-3500db)	ONU Service Profile 작성 - PROFILE_NAME : Service Profile Name - QUEUE_NAME : Queue-map Name - POLICY_NAME : Policy-map Name - BRIDGE_NAME : Bridge-map Name - IGMP_NAME : Igmp-map Name - ONU Type	Config-pon-oltqos
no service-map PROFILE_NAME	ONU Service Profile 삭제 - Default Profile 과 현재 인터페이스에 적용 중인 Profile 은 삭제 불가	Config-pon-onuqos
no queue-map MAP_NAME	ONU Queue-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-onuqos
no class-map MAP_NAME	ONU Class-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-onuqos
no policy-map MAP_NAME	ONU Policy-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-onuqos
no bridge-map MAP_NAME	ONU Bridge-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-onuqos
no igmp-map MAP_NAME	ONU Igmp-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-pon-onuqos
service-policy IF_NAME service-map PROFILE_NAME	- IF_NAME : ONU 인터페이스 이름 - PROFILE_NAME : ONU 서비스 Profile 이름	Config-pon-onuqos
show pon service-map onu (PROFILE_NAME)	ONU Service Profile List 조회 또는 특정 Service Profile 의 내용 조회	enable
Show pon service-policy onu (IF_NAME)	ONU 포트 인터페이스에 현재 적용된 서비스 Profile 조회	enable

3.1.2.2 ONU Queue-map 의 작성

ONU(Optical Network Unit) Queue-map 은 ONU 에 Upstream/Downstream Link 및 포트의 Queue 할당 상태를 설정합니다. Upstream 방향으로 4 개의 Link 에 최대 8 개까지 Queue 를 할당할 수 있으며 총 Queue Size 는 240(단위 : 4 KB)입니다. Downstram 방향으로 2 개의 포트에 최대 11 개까지 Queue 를 할당할 수 있으며, 총 Queue Size 는 120(단위 : 1 KB) 이하로 설정해야 합니다. Queue-map 은 ONU_QOS_MODE 에서 ‘queue-map’ 명령어를 이용하여 ONU_QMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
onu-qos	ONU Service Profile 작성 모드로 변경	Config-pon
queue-map MAP_NAME(og-3500ab og-3500db)	queue-map 작성 모드로 변경	Config-pon- onuqos
Queueconfig upstream <1-4> <0-240> <2-240> ...	Upstream Link 에 Queue 할당	Config-pon- oltqos-qmap
Queueconfig downstream <1-2> <0-120> <2-120> ...	Downstream Port 에 Queue 할당	Config-pon- oltqos-qmap
Map-end	queue-map 작성 완료 및 상위 모드로 전환(이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon- oltqos-qmap
Show pon queue-map onu (MAP_NAME)	ONU queue-map List 조회 또는 특정 queue-map 상세 정보 조회	enable

3.1.2.3 ONU Class-map 의 작성

OLT Class-map 은 OLT Class-map 과 같이 Packet 을 분류하기 위한 Rule 을 설정하는 Map 입니다. 이 Map 은 Policy-map 에서 Classification Rule 과 Filtering Rule 의 조건으로 사용됩니다.(Rule 의 구성요소는 OLT Class-map 과 동일하며 각 구성요소에 대한 설명은 OLT Class-map 을 참고합니다.) ONU_QOS_MODE 에서 ‘class-map’ 명령어를 이용하여 ONU_CMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
onu-qos	ONU Service Profile 작성 모드로 변경	Config-pon
class-map MAP_NAME	Class-map 작성 모드로 변경	Config-pon- onuqos
(no) classrule FIELD LOOKUP_VALUE OPERATOR	Class-map 에 한 개의 Rule 추가 및 삭제 - FIELD, LOOKUP_VALUE, OPERATOR 값은 아래 참조	Config-pon- onuqos-cmap
Map-end	Class-map 작성 완료 및 상위 모드로 전환 (이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon- onuqos-cmap
Show pon class-map onu (MAP_NAME)	ONU Class-map List 조회 또는 특정 Class-map 상세 정보 조회	enable

3.1.2.4 ONU Policy-map 의 작성

ONU Policy-map 은 ONU Link 의 SLA 설정 및 Packet Classification Rule 및 Packet Filtering Rule 등으로 구성됩니다. ONU_QOS_MODE 에서 ‘policy-map’ 명령어를 이용하여 ONU_PMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
onu-qos	ONU Service Profile 작성 모드로 변경	Config-pon
policy-map MAP_NAME (og-3500ab og-3500db)	Policy-map 작성 모드로 변경	Config-pon- onuqos
Sla control <1-4> (upstream downstream) <0-1000000> <0-1000000> (sensitive tolerant) <1-256>	ONU Link 의 Upstream/Downstream SLA 설정 - Link Index : 1~4 - Minimum Guaranteed Bandwidth(Kbps) - Maximum Allowed Bandwidth(Kbps) - Delay Sensitive - Max burst size(KB)	Config-pon- onuqos-pmap
Sla weight <1-4> (upstream downstream) <0-255> <0-511> <0-511>	ONU Link 의 Upstream/Downstream SLA Weight 설정	Config-pon- onuqos-pmap
Sla <1-4> (upstream downstream) (enable disable)	ONU Link 의 Upstream/Downstream SLA State 설정	Config-pon- onuqos-pmap
(No) filtering through upstream <1-2> <1-4> <0-7> <4-6> class-map CLASS_MAP	ONU Upstream User Port 에서 수신한 Packet 에 대해 Destination 을 지정하는 Classification Rule 을 설정 또는 삭제 - <1-2> : Ingress User Port Number - <1-4> : Egress Link Number - <0-7> : Egress Upstream Queue Num. - <4-6> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon- onuqos-pmap
(No) filtering through downstream <1-2> <0-10> <4-6> class-map CLASS_MAP	ONU Downstream EPON Port 에서 수신한 Packet 에 대해 Destination 을 지정하는 Classification Rule 을 설정 또는 삭제 - <1-2> : Egress User Port Number - <0-7> : Egress Downstream Queue - <4-6> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon- onuqos-pmap
(no) filtering discard onu port upstream <1-2> <0-7> class- map CLASS_MAP	ONU Upstream User Port 에서 수신한 Packet 을 Discard 하는 Filtering Rule 을 설정 또는 삭제 - <1-2> : Ingress User Port Number - <0-7> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon- onuqos-pmap

(계속)

명령어	설명	모드
(no) filtering discard onu port downstream <0-7> class-map CLASS_MAP	ONU Downstream EPON Port 에서 수신한 Packet 을 Discard 하는 Filtering Rule 을 설정 또는 삭제 - <0-7> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon- onuqos-pmap
(no) filtering discard link <1-4> <0-7> class-map CLASS_MAP	OLT Upstream Link 에서 수신한 Packet 을 Discard 하는 Filtering Rule 을 설정 또는 삭제 - <1-4> : ONU Link Number - <0-7> : Priority of the Rule - CLASS_MAP : ONU Class-map Name	Config-pon- onuqos-pmap
Map-end	Policy-map 작성 완료 및 상위 모드로 전환 이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력 하여 상위 모드로 전환해야 합니다.	Config-pon- onuqos-pmap
Show pon policy-map onu (MAP_NAME)	ONU Policy-map List 조회 또는 특정 Policy-map 상세 정보 조회	Enable

3.1.2.5 ONU Bridge-map 의 작성

ONU Bridge-map 은 ONU User Port 의 Bridge 관련 설정 및 Link 의 Bridge Mode 설정, 그리고 Link 의 데이터 암호화를 위한 Key Exchange Timer 설정 등을 포함합니다. ONU_QOS_MODE 에서 ‘bridge-map’ 명령어를 이용하여 ONU_BMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
onu-qos	ONU Service Profile 작성 모드로 변경	Config-pon
bridge-map MAP_NAME (og-3500ab og-3500db)	Bridge-map 작성 모드로 변경	Config-pon- onuqos
Bridgeconfig <1-2> <0-64> <0-32768>	ONU User Port 에 MAC Limit 설정 - <1-2> : ONU User Port Number - <0-64> : automatic learning entry limit - <0-32768> : learned entry age limit (2 의 거듭제곱 수)	Config-pon- onuqos-bmap
Bridgemode <1-4> (simple-bridge shared-vlan transparent-vlan priority-simple-bridge priority-shared-vlan transparent-priority-shared-vlan) <0-4095>	ONU Link 의 Bridging Mode 설정 - <1-4> : ONU Link Number - Bridging Mode - <0-4095> : mac table entry limit	Config-pon- onuqos-bmap

(계속)

명령어	설명	모드
Key exchange timer <1-4> <0-65535>	ONU Link 의 암호화 시 Key Exchange Timer 값 설정 - <1-4> : ONU Link Number - <0-65535> : Timeout Value(단위 : 초), 0 or 60~65535	Config-pon- onuqos-bmap
Map-end	Bridge-map 작성 완료 및 상위 모드로 전환 (이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon- onuqos-bmap
Show pon bridge-map onu (MAP_NAME)	ONU Bridge-map List 조회 또는 특정 Bridge-map 상세 정보 조회	enable

설정가능한 Bridging Mode 는 아래와 같이 6 종류이며, 각 Mode 의 Upstream/Downstream Bridging Action 은 아래와 같습니다.(Bridge Mode 별로 VLAN 관련 설정은 ‘Link 에 VLAN 설정’ 항목을 참고합니다.)

Simple Bridge

Upstream		
Source MAC 어드레스	Bridging Action	
Unicast	Learn SA Forward	
Multicast	Forward	
Broadcast	Forward	
Downstream		
VLAN Tag	Destination MAC 어드레스	Bridging Action
No	Learned	Forward to Link
No	Unlearned	Flood on broadcast channel
Yes	N/A	Drop

Shared VLAN

Upstream		
Source MAC 어드레스	Bridging Action	
Unicast	Learn SA Add provisioned tag Forward	
Multicast	Forward	
Broadcast	Forward	

(계속)

Downstream	
Destination MAC 어드레스	Bridging Action
Learned	Strip Tag Forward to Link(based on L2 DA + VID)
Unlearned	Strip Tag Broadcast o VLAN(based on VID only)

Transparent VLAN

Upstream	
VLAN Tag Present	Bridging Action
Yes	Forward without modification(based on VID only)
No	Forward without modification(based on VID only)
Downstream	
Bridging Action	
Forward without modification(based on VID only)	

Priority Simple Bridged

Upstream			
Source MAC 어드레스		Bridging Action	
Unicast		Learn SA Forward	
Multicast		Forward	
Broadcast		Forward	
Downstream			
VLAN Tag	Destination MAC 어드레스	Priority	Bridging Action
No	Learned	Within Provisioned Priority Range	Forward to Link
		Outside Provisioned Priority Range	Drop
No	Unlearned	Don't Care	Flood on broadcast channel
Yes	N/A	N/A	Drop

Priority Shared VLAN

Upstream			
VLAN Tag Present		Bridging Action	
Yes		Strip Tag Add Provisioned Tag(VID + Upstream CoS) Forward	
No		Add Provisioned Tag Forward	
Downstream(Switch on ToS)			
ToS in Range	Tx-Non-ToS-Frame	L2 DA Learned	Bridging Action
Yes	N/A	Yes	Strip Tag Forward(based on DA + VID + ToS)
		No	Strip Tag Broadcast on VLAN(based on VID + ToS)
No	Yes	Yes	Strip Tag Forward(based on DA + VID)
		No	Strip Tag Broadcast on VLAN(based on VID)
	No	N/A	Drop
Downstream(Switch on CoS)			
CoS in Range	Tx-Non-ToS-Frame	L2 DA Learned	Bridging Action
Yes	N/A	Yes	Strip Tag Forward(DA + VID + CoS)
		No	Strip Tag Broadcast on VLAN(VID + CoS)
No	N/A	N/A	Drop

Transparent Priority Shared VLAN

Upstream	
VLAN Tag Present	Bridging Action
Yes	Strip Tag Add Provisioned Tag(VID + Upstream CoS) Forward
No	Add Provisioned Tag Forward

(계속)

Downstream(Switch on ToS)			
ToS in Range	Tx-Non-ToS-Frame	L2 DA Learned	Bridging Action
Yes	N/A	Yes	Forward(based on DA + VID + ToS)
		No	Broadcast on VLAN(based on VID + ToS)
No	Yes	Yes	Forward(based on DA + VID)
		No	Broadcast on VLAN(based on VID)
	No	N/A	Drop
Downstream(Switch on CoS)			
CoS in Range	Tx-Non-ToS-Frame	L2 DA Learned	Bridging Action
Yes	N/A	Yes	Forward(DA + VID + CoS)
		No	Broadcast on VLAN(VID + CoS)
No	N/A	N/A	Drop

3.1.2.6 ONU Igmpp-map 의 작성

ONU Igmpp-map 은 ONU 의 IGMP Snooping 관련 설정을 포함합니다. ONU_QOS_MODE 에서 'igmp-map' 명령어를 이용하여 ONU_IMAP_MODE 로 전환하여 작성합니다.

명령어	설명	모드
onu-qos	ONU Service Profile 작성 모드로 변경	Config-pon
igmp-map MAP_NAME	Igmpp-map 작성 모드로 변경	Config-pon- onuqos
igmp snooping onu <1-16> <0-6>	ONU IGMP Snooping Parameter 설정 - <1-16> : robustness count - <0-6> : last member query count	Config-pon- onuqos- imap
igmp snooping port <1-2> <0-32> <0-10>	ONU User Port 에 Snooping 설정 - <1-2> : ONU User Port Number - <0-32> : Number of IGMP groups (0 : snooping disabled) - <0-10> : relative queue for downstream classification	Config-pon- onuqos- imap
Map-end	Igmpp-map 작성 완료 및 상위 모드로 전환 (이 명령어를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 명령어를 입력하여 상위 모드로 전환해야 합니다.)	Config-pon- onuqos- imap
Show pon igmp-map olt (MAP_NAME)	OLT Igmpp-map List 조회 또는 특정 Igmpp-map 상세 정보 조회	enable

3.1.2.7 Link 에 VLAN 설정

이 절은 Link 에 설정된 Bridge Mode 에 따라 VLAN 관련 설정하는 방법입니다. ONU Bridge-map 의 작성에서 언급한바와 같이 Bridge Mode 는 6 종류이며, 각 모드에 대해 VLAN 설정 명령어는 아래와 같습니다.

Link Bridge 모드	VLAN 설정 명령어
Simple Bridge	N/A
Shared VLAN	Vlntag
Transparent VLAN	Vlntag
Priority Simple Bridged	Priority-vlan
Priority Shared VLAN	Priority-vlan
Transparent Priority Shared VLAN	Priority-vlan

명령어	설명	모드
(no) vlntag IF_NAME <1-4> <1-4093>	Shared VLAN, Transparent VLAN Mode 일 경우 Link 에 VLAN tag 을 설정 - IF_NAME : ONU 인터페이스 Name - <1-4> : ONU Link Number - <1-4093> : Network VLAN Tag	Config-pon
(no) priority-vlan IF_NAME <1-4> <1-4093> <0-7> (cos tos) <0-7> <0-7> (on off)	Priority VLAN Mode 일 경우 Link 에 Priority VLAN 을 설정 - IF_NAME : ONU 인터페이스 Name - <1-4> : ONU Link Number - <1-4093> : Network VLAN ID - <0-7> : Upstream CoS(Priority VLAN Group 에 포함되는 모든 Link 는 동일한 값으로 설정해야 합니다.) - (cos tos) : Priority Selector - <0-7> : Minimum Priority Value - <0-7> : Maximum Priority Value - (on off) : Transmit Non-ToS Frame	Config-pon
Show pon vlan-for-link IF_NAME <1-4>	Link 에 설정된 VLAN 조회	Enable
Show pon links-for-vlan IF_NAME <1-4093>	OLT 에 특정 VLAN 으로 설정된 Link List 조회	Enable
Show pon priority-vlan IF_NAME <1-4>	Link 에 설정된 Priority VLAN 조회	Enable

3.1.2.8 ONU Port 에 Advanced Rule 설정

ONU 의 Lookup Engine 에 포함되는 Rule 을 추가 또는 삭제하는 방법입니다. 이 Rule 을 설정함으로써 수신한 Packet 의 VLAN tag 를 변경하거나, CoS 를 변경하는 기능을 수행할 수 있습니다. 이 절에서 기술하는 명령어에 포함되는 Rule 의 Priority 값은 ONU Policy-map 에서 작성한 Classification Rule 이나 Filtering Rule 의 Priority 값의 2 배와 같은 우선순위를 가집니다.

명령어	설명	모드
(no) filtering (add-tag clr-add-tag clr-del-tag clr-replace-tag del-tag replace-tag) onu port upstream IF_NAME <1-2> <0-15> class-map CLASS_MAP	ONU Upstream User Port 에서 수신한 Packet 중 Class-map 조건에 맞는 Packet 에 대하여 VLAN tag 를 변경 - add-tag : Add VLAN tag - clr-add-tag : Clear Add Tag - clr-del-tag : Clear Delete Tag - clr-replace-tag : Clear Replace Tag - del-tag : Delete Tag - replace-tag : Replace Tag - IF_NAME : ONU 인터페이스 Name - <1-2> : ONU User Port Number - <0-15> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon
(no) filtering (add-tag clr-add-tag clr-del-tag clr-replace-tag del-tag replace-tag) onu port downstream IF_NAME <0-15> class-map CLASS_MAP	ONU Downstream EPON Port 에서 수신한 Packet 중 Class-map 조건에 맞는 Packet 에 대하여 VLAN tag 를 변경 - add-tag : Add VLAN tag - clr-add-tag : Clear Add Tag - clr-del-tag : Clear Delete Tag - clr-replace-tag : Clear Replace Tag - del-tag : Delete Tag - replace-tag : Replace Tag - IF_NAME : ONU 인터페이스 Name - <0-15> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon
(no) filtering (set-vid-and-add-tag replace-tag-and-set-vid) onu port upstream IF_NAME <1-2> <0-15> <0-4093> class-map CLASS_MAP	ONU Upstream User Port 에서 수신한 Packet 중 Class-map 조건에 맞는 Packet 에 대하여 VLAN ID 를 설정 - set-vid-and-add-tag : Set VID ; Add Tag - replace-tag-and-set-vid : Replace Tag; Set VID - IF_NAME : ONU 인터페이스 Name - <1-2> : ONU User Port Number - <0-15> : Priority of the rule - CLASS_MAP : ONU Class-map Name	Config-pon

(계속)

명령어	설명	모드
(no) filtering (set-vid-and-add-tag replace-tag-and-set-vid) onu port downstream IF_NAME <0-15> <0-4093> class-map CLASS_MAP	ONU Downstream EPON Port 에서 수신한 Packet 중 Class-map 조건에 맞는 Packet 에 대하여 VLAN ID 를 설정 <ul style="list-style-type: none"> - set-vid-and-add-tag : Set VID ; Add Tag - replace-tag-and-set-vid : Replace Tag ; Set VID - IF_NAME : ONU 인터페이스 Name - <0-15> : Priority of the rule - CLASS_MAP : ONU Class-map Name 	Config-pon
(no) filtering set-cos onu port upstream IF_NAME <1-2> <0-15> <0-7> class-map CLASS_MAP	ONU Upstream User Port 에서 수신한 Packet 중 Class-map 조건에 맞는 Packet 에 대하여 CoS 값을 설정 <ul style="list-style-type: none"> - <1-2> : ONU 인터페이스 Name - <0-15> : Priority of the rule - <0-7> : CoS Value - CLASS_MAP : ONU Class-map Name 	Config-pon
(no) filtering set-cos onu port downstream IF_NAME <0-15> <0-7> class-map CLASS_MAP	ONU Downstream EPON Port 에서 수신한 Packet 중 Class-map 조건에 맞는 Packet 에 대하여 CoS 값을 설정 <ul style="list-style-type: none"> - <0-15> : Priority of the rule - <0-7> : CoS Value - CLASS_MAP : ONU Class-map Name 	Config-pon
Show pon filtering rules onu port upstream IF_NAME <1-2>	ONU Upstream User Port 에 설정된 Rule 조회	Enable
Show pon filtering rules onu port downstream IF_NAME	ONU Downstream EPON Port 에 설정된 Rule 조회	Enable

3.2 Layer 2 환경 설정

2 계층 인터페이스는 2 계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하도록 설정된 인터페이스로서 OG-1100 시스템에서는 물리적 포트가 이 모드로 동작합니다. 이 절에서는 먼저 2 계층 인터페이스를 설명하고 물리적 포트를 2 계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여줍니다.

3.2.1 VLAN (Virtual LAN)

OG-1100 시스템은 모든 이더넷 인터페이스에 802.1Q 을 지원하며, 최대 4k 까지 설정이 가능합니다. VLAN 의 설정은 port/trunk 인터페이스에 설정이 가능합니다.

3.2.1.1 기본 VLAN 구성

OG-1100 시스템의 출하 시 VLAN 구성은 다음과 같습니다.

기본 VLAN 구성

항목	기본값
VLAN 이름	Default, Mgt.
VLAN ID	1, 4094
VLAN 에 속한 포트	모든 포트, PON Side 포트
STP 상태	RSTP, OFF
IP 어드레스	0.0.0.0
Subnet mask	0.0.0.0
태그 처리 방식	Untagged(모든 포트)
VLAN 상태	활성화

위와 같은 VLAN 의 기본구성을 변경하면, 시스템을 리부팅하거나 다른 명령어를 실행하지 않아도 기본 구성이 시스템에 바로 적용됩니다. 하지만, 시스템을 켜다가 켜 후에도 변경된 VLAN 구성을 계속 사용하려면 ENABLE_MODE 에서 write 명령어를 실행하여 VLAN 구성을 메모리에 저장해야 합니다.

3.2.1.2 기본적인 VLAN 구성과정

OG-1100 시스템은 시스템을 시작할 때나 혹은 운용 중에 VLAN 의 구성을 변경할 수 있습니다. 시스템이 운용되는 중에 VLAN 구성을 변경하면, 지금까지 VLAN 에 속한 포트를 통해 습득(Learning)된 모든 MAC 어드레스가 삭제됩니다.

OG-1100 시스템에서 VLAN 을 구성하는 과정은 다음과 같습니다.

- 1) VLAN 을 사용하여 구성할 네트워크의 토폴로지를 디자인합니다.
- 2) VLAN 을 생성합니다.
- 3) 생성한 VLAN 에 포트를 할당합니다(혹은 VLAN 에서 포트를 삭제합니다).
- 4) 변경된 VLAN 구성을 저장하고 시스템에 적용합니다.

이 절에서는 위의 각 과정에 대해 상세하게 살펴봅니다.

3.2.1.3 VLAN 생성하기

기본적으로 OG-1100 시스템의 모든 포트들은 기본 VLAN(이름 : Default, ID : 1)에 할당되어 있고, 하나의 브로드캐스트 도메인(broadcast domain)에 속해 있습니다. 그리고, ONT 단말과의 IPC 통신을 위하여 추가 VLAN(이름 : Mgt., ID : 4094)에 PON Side 포트들이 할당되며, 별도의 브로드캐스트 도메인을 형성합니다. 추가로 VLAN 을 정의하고 포트를 VLAN 에 할당하면 OG-1100 시스템은 여러 개의 가상 브로드캐스트 도메인으로 나눌 수 있습니다.

VLAN 은 ID 와 이름을 통해 다른 VLAN 과 구별됩니다. VLAN ID 와 이름은 VLAN 을 정의할 때 사용자가 원하는 값으로 지정할 수 있습니다. VLAN ID 는 2~4093 중에서 다른 VLAN 이 사용하고 있지 않은 값을 선택하면 됩니다. VLAN 을 정의한다고 하여 브로드캐스트 도메인이 형성되는 것은 아닙니다. 정의된 VLAN 에 포트가 추가되었을 때, VLAN 에 추가된 포트들로 구성된 브로드캐스트 도메인이 형성됩니다.

시스템에 기본적으로 만들어져 있는 기본 VLAN 은 삭제하거나 ID 혹은 이름을 변경할 수 없습니다.

다음은 OG-1100 시스템에서 VLAN 을 생성하는 방법입니다.

3.2.1.4 VLAN 설정 및 변경

- 1) VLAN 을 설정하기 위해서는 맨 처음 CONFIG_MODE 에서 VLAN_MODE 로 변경한 이후 VLAN ID 를 생성해야 합니다.
- 2) 각 INTERFACE_MODE 에 들어가서 hybrid/access/trunk mode 를 설정합니다.
- 3) 각 인터페이스에 PVID 를 변경하거나, VLAN id 를 추가 또는 제거합니다.

명령어	설명	모드
vlan database	VLAN mode 로 변경	config
vlan <2-4093>	VLAN ID 를 설정 <2-4093> VLAN id number 설정	Config-vlan
switch {hybrid/access/trunk}vlan <2~4093>	PVID 변경 - Hybrid : hybrid mode 변경 - Access : access mode 변경 - Trunk : trunk mode 변경 - <2-4093> : VLAN id 번호 설정	Config-interface
no switch hybrid vlan	PVID 를 default VLAN(1)으로 변경	Config-interface
switch {hybrid/access/trunk} allowed vlan {add/remove} <2~4093> egress-tagged {enable/disable}	VLAN id 추가/삭제, tagged 설정 변경 - add : VLAN 추가 - remove : VLAN 삭제 - enable : tagged 로 변경 - disable : untagged 로 변경	Config-interface

아래의 VLAN 10, 20 을 생성하고 인터페이스 7/1 에 추가하는 예제는 다음과 같습니다.

```

OG1100(config)#vlan database
OG1100(config-vlan)#vlan 10 (VLAN 10을 생성하는 경우)
OG1100(config-vlan)#vlan 20 (VLAN 20을 생성하는 경우)
OG1100(config-vlan)#exit
OG1100(config)#interface 7/1
OG1100(config-if)# switch hybrid vlan 10 (PVID 10으로 변경)
OG1100(config-if)# switch hybrid allowed vlan add 10 egress-tagged
disable
OG1100(config-if)# switch hybrid allowed vlan add 20 egress-tagged
enable
OG1100(config-if)#end
OG1100#show vlan
-----

```

SLOT	EPU				EPU				SWU	LACP/TRUNK
	2	3	4	5	8	9	10	11	7	AGGREGATOR
PORT
	12	12	12	12	12	12	12	12	12	34 56 78
SWITCHPORT	HH	HH	HH	HH	HH	HH	HH	HH	HH	HH
PRIORITY	00	00	00	00	00	00	00	00	00	00
INGRESS FILTER	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
ACCEPT. FRAME	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
default (1)	UU	UU	UU	UU	UU	UU	UU	UU	UU	UU
VLAN0010 (10)	U.	..
VLAN0020 (20)	t.	..
Mgt. (4094)	tt	tt	tt	tt	tt	tt	tt	tt

```

-----
OG1100#

```

Untagged/tagged VLAN 으로 설정 및 변경 시는 ‘egress-tagged enable/diable’으로 재 설정해 주면 변경됩니다.

VLAN 을 삭제하려면 할려면 위에 명령에서 ‘remove’ 명령어를 사용합니다.

```

OG1100(config)#interface 7/1
OG1100(config-if)# switch hybrid allowed vlan remove 10
OG1100(config-if)# end
OG1100# show vlan
OG1100(config-if)#end
OG1100#show vlan
-----

```

SLOT	EPU				EPU				SWU	LACP/TRUNK
	2	3	4	5	8	9	10	11	7	AGGREGATOR
PORT
	12	12	12	12	12	12	12	12	12	34 56 78
SWITCHPORT	HH	HH	HH	HH	HH	HH	HH	HH	HH	HH
PRIORITY	00	00	00	00	00	00	00	00	00	00

```

-----

```

```

INGRESS FILTER | YY YY YY YY | YY YY YY YY | YY YY YY YY | .. .. ..
ACCEPT. FRAME | AA AA AA AA | AA AA AA AA | AA AA AA AA | .. .. ..
-----+-----+-----+-----+
default ( 1) | UU UU UU UU | UU UU UU UU | UU UU UU UU | .. .. ..
VLAN0010 ( 10) | .. .. .. .. | .. .. .. .. | P. .. .. .. | .. .. ..
VLAN0020 ( 20) | .. .. .. .. | .. .. .. .. | t. .. .. .. | .. .. ..
Mgt. (4094) | tt tt tt tt | tt tt tt tt | .. .. .. .. | .. .. ..
-----+-----+-----+-----+
OG1100#
    
```

그런데, 위의 예제처럼 PVID 을 10 으로 설정하고 VLAN 10 을 제거하면 PVID 는 변경이 되지 않아서 위와 같이(P) 표시됩니다. PVID 를 default VLAN 1 로 변경하기 위해서는 ‘no switch hybrid vlan’ 명령어를 사용합니다. 또한, 다른 PVID 를 설정하기 위해서는 아래와 같은 예제로 사용하면 됩니다.

```

OG1100(config)#interface 7/1
OG1100(config-if)# no switch hybrid vlan
OG1100(config-if)# switch hybrid vlan 20
OG1100(config-if)#end
OG1100# show vlan

-----+-----+-----+-----+
SLOT          | EPU          | EPU          | SWU          | LACP/TRUNK
              | 2 3 4 5     | 8 9 10 11   | 7            | AGGREGATOR
-----+-----+-----+-----+
PORT          | .. .. .. .. | .. .. .. .. | .. .. .. .. |
              | 12 12 12 12 | 12 12 12 12 | 12 34 56 78 | 12 34 56 78
-----+-----+-----+-----+
SWITCHPORT    | HH HH HH HH | HH HH HH HH | HH HH HH HH | .. .. ..
PRIORITY      | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | .. .. ..
INGRESS FILTER| YY YY YY YY | YY YY YY YY | YY YY YY YY | .. .. ..
ACCEPT. FRAME | AA AA AA AA | AA AA AA AA | AA AA AA AA | .. .. ..
-----+-----+-----+-----+
default ( 1) | UU UU UU UU | UU UU UU UU | UU UU UU UU | .. .. ..
VLAN0010 ( 10) | .. .. .. .. | .. .. .. .. | .. .. .. .. | .. .. ..
VLAN0020 ( 20) | .. .. .. .. | .. .. .. .. | T. .. .. .. | .. .. ..
Mgt. (4094) | tt tt tt tt | tt tt tt tt | .. .. .. .. | .. .. ..
-----+-----+-----+-----+
OG1100#
    
```

3.2.1.5 VLAN 조회

설정된 VLAN 을 조회하는 명령은 ENABLE_MODE 에서 할 수 있습니다.

명령어	설명	모드
Show vlan	VLAN 상태 조회	Enable

```

OG1100# show vlan
-----
          | EPU          | EPU          | SWU          | LACP/TRUNK
SLOT      | 2 3 4 5     | 8 9 10 11   | 7           | AGGREGATOR
-----+-----+-----+-----+-----
PORT      | .. .. .. .. | .. .. .. .. | .. .. .. .. |
          | 12 12 12 12 | 12 12 12 12 | 12 34 56 78 | 12 34 56 78
-----+-----+-----+-----+-----
SWITCHPORT | HH HH HH HH | HH HH HH HH | HH HH HH HH | .. .. .. ..
PRIORITY   | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | .. .. .. ..
INGRESS FILTER | YY YY YY YY | YY YY YY YY | YY YY YY YY | .. .. .. ..
ACCEPT. FRAME | AA AA AA AA | AA AA AA AA | AA AA AA AA | .. .. .. ..
-----+-----+-----+-----+-----
default ( 1) | UU UU UU UU | UU UU UU UU | UU UU UU UU | .. .. .. ..
Mgt. (4094) | tt tt tt tt | tt tt tt tt | .. .. .. .. | .. .. .. ..
-----+-----+-----+-----+-----
SWITCHPORT      : A(Access) H(Hybrid) T(Trunk)
PRIORITY        : IEEE 802.1P Default User-Priority <0-7>
INGRESS FILTER  : Y(Enable) N(Disable)
ACCEPT. FRAME   : Acceptable Frame Type
                  A - All frame receive.
                  T - Only VLAN Tagged frame receive.
                  U - Only VLAN Untagged frame receive.
VLANNAME ( VID) : IEEE 802.1q Port based VLAN information
                  U - Untagged VLAN (PVID = VID)
                  u - Untagged shared VLAN (PVID != VID)
                  T - Tagged VLAN (PVID = VID)
                  t - Tagged shared VLAN (PVID != VID)
                  P - Only PVID
OG1100#
    
```

각 포트에 VLAN 를 설정하거나 특성을 변경 후에 VLAN 에 관한 모든 정보를 조회할 수 있습니다.

당사에 제공하는 VLAN 은 hybrid/access/trunk mode 를 제공하며 기본적으로는 hybrid mode 로 설정되어 있습니다. 특히, PVID 설정 및 tagged VLAN(802.1Q)을 제공합니다.

3.2.2 STP/RSTP

Switching Loop 차단과 경로 이중화를 위한 STP(Spanning Tree Protocol)/RSTP(Rapid Spanning Tree Protocol)을 지원하며, VLAN 을 고려하여 다양한 Topology 를 구현할 수 있는 MSTP(Multiple Spanning Tree Protocol)/PVST(Per VLAN Spanning Tree)도 지원을 합니다.

네트워크상에서 하나의 목적지에 대하여 여러경로를 가질 수 있습니다. 하지만, 같은 BroadCast 도메인에서 경로가 여러 개인 경우 loop 가 발생할 수 있게 되고, 트래픽 폭주에 의한 네트워크를 불안정하게 합니다. STP 는 여러 개의 경로를 가진 네트워크상에서 루프를 방지해 주는 프로토콜이며, 하나의 스위치를 루트로 하는 tree 를 정의합니다.

OG-1100 시스템은 기본적으로 RSTP 가 활성화 되 있는 상태입니다.

3.2.2.1 설정 및 조회

당 시스템의 STP/RSTP/MSTP/PVST 를 설정하기 위해서는 configure mode 에서 ‘bridge protocol ‘이라는 명령어를 이용하여 사용하고자 하는 프로토콜을 선택하게 됩니다. 이 명령은 SWU 의 상위 7/1~7/8 의 8 개 포트 전체에 동시에 적용되는 명령입니다.

명령어	설명	모드
bridge protocol {stp rstp mstp pvst} {enable disable}	STP/RSTP/MSTP/PVST 를 global 하게 설정하도록 변경	config
show spanning-tree [ieee][mst][pvst- mode][rstp][instance]	설정된 STP/RSTP/MSTP/PVST 상태를 조회	Enable

간단한 예를 들어보면 다음과 같습니다.

```
OG1100# configure terminal
OG1100(config)# bridge protocol stp enable
OG1100(config)# exit
OG1100# show spanning-tree
% Spanning-Tree Running Status

% IEEE 802.1D : Enabled (stp가 enable 된 것을 확인)
% IEEE 802.1w : Disabled
% IEEE 802.1s : Disabled
% PerVLAN STP : Disabled OG1100#
```

STP 에서 RSTP/MSTP/PVST 로 변경하고자 하면 먼저 해당 프로토콜을 ‘disable’한 후 변경하고자 하는 프로토콜로 변경합니다.

```
OG1100(config)#bridge protocol rstp enable
% other stp already running!! (stp가 활성화된 상태이기 때문)
OG1100(config)#bridge protocol stp disable (stp 비활성화)
OG1100(config)#bridge protocol rstp enable (rstp 활성화)
OG1100(config)#exit
OG1100#show spanning-tree rstp

bridge name      : default bridge(1)
protocol(1w)    : enabled
ageing time      : 300 (sec)
bridge id        : 8000-0000f00400eb ( priority : 32768 )
root id          : 8000-0000000000000
root port 0      : / path cost 0
forward delay 15 (sec) / bridge forward delay 15 (sec)
hello time 2 (sec) / bridge hello time 2 (sec)
max age 20 (sec) / bridge max age 20 (sec)

7/1: portid 8015 - path cost 20000 - role designated - forwarding
7/2: portid 8016 - path cost 20000 - role disabled - discarding
7/3: portid 8017 - path cost 20000 - role disabled - discarding
7/4: portid 8018 - path cost 20000 - role disabled - discarding
```

```

7/5: portid 8019 - path cost 20000 - role disabled - discarding
7/6: portid 801a - path cost 20000 - role disabled - discarding
7/7: portid 801b - path cost 20000 - role disabled - discarding
7/8: portid 801c - path cost 20000 - role disabled - discarding
    
```

3.2.2.2 인터페이스 별 설정 및 조회

STP/RSTP 인 경우에 개별 인터페이스별로 설정하는 것은 STP/RSTP 가 설정된 상태에서 설정하는 인터페이스를 STP/RSTP 그룹에 포함할 것인지 말것인지를 결정하는 것으로 INTERFACE_MODE 에서 설정하면 됩니다.

명령어	설명	모드
spanning-tree {enable disable port-fast}	해당 인터페이스에 STP/RSTP 에 그룹에 포함여부 결정 - Port-fast : port-fast-enable	Config-interface
show spanning-tree ieee <i>interface</i>	각 인터페이스별 STP/RST 상태조회	Enable

```

OG1100(config)#interface 7/1
OG1100(config-if)#spanning-tree enable
OG1100(config-if)#end
OG1100#show spanning-tree ieee interface 7/1

intf name      : 7/1 in default bridge(1)
protocol(1d)  : enabled
designated root 8000-0000f00400eb
designated bridge 8000-0000f00400eb
state disabled / priority 128
port id 8015   / designated port id 8015
path cost 20000 / designated path cost 0
config bpdu tx 0 / config bpdu rx 0
tcn bpdu tx 0 / tcn bpdu rx 0
portfast disabled / forward-transitions 2
currnet remaining timer
forward time 0 (sec) - hold time 0 (sec) - max age 0 (sec)
    
```

3.2.3 Trunk/LACP

상위 장비와 연동하여 네트워크를 구성할 경우, 트래픽의 병목현상이나, 분산을 위하여 여러 개의 물리적인 링크를 하나의 논리적인 링크로 구성할 수 있으며, 이러한 기능을 port trunking 또는 link aggregation 이라 하며, 이 포트들의 집합이 port group 이라고 합니다. 당 장비는 이러한 기능을 지원하는 방법으로 고정적으로 trunk 그룹을 지정하여 사용하는 static trunk 와 IEEE802.3ad 의 LACP(Link Aggregation Control Protocol)을 지원합니다.

3.2.3.1 Static trunk 설정 및 조회

Static trunk 은 INTEFACE_MODE 에서 지정한 trunk 에 속할 논리적 링크인 ‘static-channel-group’에 설정하며, 최대 group 수는 8 개입니다. 같은 group number 로 지정하면 trunk 의 한 멤버로 지정되어, 지정한 논리적 링크의 멤버가 되는 것입니다. 지정된 인터페이스는 aggn 의 aggregation 인터페이스가 되며, 인터페이스와 동일하게 간주하며 설정 할 수 있게 됩니다.

명령어	설명	모드
<code>static-channel-group <1-8></code>	Static channel group 지정 및 변경 <1-8> group number 변경	Config-interface
<code>show static-channel-group</code>	설정된 static channel group 조회	Enable

다음은 인터페이스에 대해서 static trunk group 으로 설정하는 예입니다.

```

OG1100(config)#interface 7/3
OG1100(config-if)#static-channel-group 1 (group 1에 지정)
OG1100(config-if)#exit
OG1100(config)#interface 7/4
OG1100(config-if)#static-channel-group 1 (group 1 지정 7/3와 동일 링크)
OG1100(config-if)#end
OG1100#show static-channel-group
-----
AGGREGATOR for | SWU
STATIC TRUNK   | 7/1 7/2 7/3 7/4 7/5 7/6 7/7 7/8
-----+-----
agg1 (STATIC)  | . . O O . . . . (설정한)
agg2 (NO EXIST)| . . . . . . . .
agg3 (NO EXIST)| . . . . . . . .
agg4 (NO EXIST)| . . . . . . . .
-----+-----
agg5 (NO EXIST)| . . . . . . . .
agg6 (NO EXIST)| . . . . . . . .
agg7 (NO EXIST)| . . . . . . . .
agg8 (NO EXIST)| . . . . . . . .
-----+-----
. : Not Configured
O : Configured for Static Trunk
OG1100#
    
```

설정된 static channel group 을 해지 하기 위해서는 ‘no’ 명령어를 사용합니다.

명령어	설명	모드
<code>no static-channel-group</code>	Static channel group 해지	Config-interface

```

OG1100(config)#interface 7/3
OG1100(config-if)#no static-channel-group
OG1100(config-if)#end
OG1100#show static-channel-group

-----
AGGREGATOR for | SWU
STATIC TRUNK   | 7/1 7/2 7/3 7/4 7/5 7/6 7/7 7/8
-----
agg1 (STATIC)  | . . . 0 . . . . . (삭제 확인)
agg2 (NO EXIST)| . . . . .
agg3 (NO EXIST)| . . . . .
agg4 (NO EXIST)| . . . . .
-----
agg5 (NO EXIST)| . . . . .
agg6 (NO EXIST)| . . . . .
agg7 (NO EXIST)| . . . . .
agg8 (NO EXIST)| . . . . .
-----
. : Not Configured
0 : Configured for Static Trunk
OG1100#
    
```

위에서 agg1 으로 설정된 것은 aggregation 인터페이스를 의미하며, ‘static’ 또는 ‘LACP’ 로 표시됩니다. Interface 7/1, 7/2 와 같은 인터페이스로 취급되며, 인터페이스에 할 수 있는 모든 설정을 aggregation 인터페이스에 마찬가지로 설정합니다. 즉, aggregation INTERFACE_MODE 로 설정하기 위해서 ‘interface aggn ‘으로 설정 및 조회를 하면 됩니다.

설정된 aggregation 인터페이스는 default 가 admin. 상태가 ‘shutdown’으로 사용하기 위해서는 ‘no shutdown’의 명령어를 사용하면 됩니다.

3.2.3.2 LACP 설정 및 조회

LACP 는 trunk 으로 설정된 논리적 링크에 표준 프로토콜에 의하여 자동적으로 다른 장비와 메시지를 통하여 포트 trunk 으로 동작하는 것은 LACP 를 지원하는 장비와 상호연동이 가능하도록 하는 것입니다.

Static trunk 와 비슷하게 INTERFACE_MODE 에서 설정하게 되며, ‘channel-group’명령어를 사용하게 되며, static trunk 와 달리 ‘mode {active|passive} 설정을 해야 합니다. 즉, aggregation port 를 수동적일 지정할지 아니면, 능동적으로 메시지를 상대방 스위치에게 메시지를 먼저 전달할 지에 대한 모드를 결정하는 것입니다. LACP 의 group 은 etherchannel 로 정의됩니다.

명령어	설명	모드
channel-group mode {active passive} <1-8>	LACP channel group 설정 및 변경	Config-interface
show etherchannel <1~8> [summary][load-balance][detail]	Etherchannel 설정 상태 조회	Enable

예제는 다음과 같습니다.

```

OG1100(config)#interface 7/3
OG1100(config-if)#channel-group 1 mode active
OG1100(config-if)#exit
OG1100(config)#interface 7/4
OG1100(config-if)#channel-group 1 mode active
OG1100(config-if)#end
OG1100#show etherchannel

-----
AGGREGATOR for | SWU
LACP            | 7/1 7/2 7/3 7/4 7/5 7/6 7/7 7/8
-----+-----
agg1 (STATIC)   | . . . . . . . .
agg2 (NO EXIST) | . . . . . . . .
agg3 (LACP)     | . . 0 0 . . . .
agg4 (NO EXIST) | . . . . . . . .
-----+-----
agg5 (NO EXIST) | . . . . . . . .
agg6 (NO EXIST) | . . . . . . . .
agg7 (NO EXIST) | . . . . . . . .
agg8 (NO EXIST) | . . . . . . . .
-----+-----
. : Not Configured
0 : Configured for LACP

OG1100#
OG1100#show etherchannel 3

-----
AGGREGATOR  agg3(38)                00:00:f0:bb:00:03
-----+-----
SYSTEM ID   Actor                    | 0x8000, 00:00:f0:bb:00:03
             Partner                  | 0x8000, 00:00:f0:cd:cd:01
OPER. KEY   Actor                    | 0003, 0003(Admin)
             Partner                  | 0003
DEBUGGING   Individual               | 0
             Ready                    | 1
             Link Count                | 2
             Ref. Count                | 2
             Rx Link                   | 1
             Tx Link                   | 1
-----+-----
LINK INFO.  7/3 (15)                 | In SYNC (1)
             7/4 (16)                 | In SYNC (1)
-----+-----

OG1100#
OG1100#show etherchannel detail

```

(설정확인)

```

-----
AGGREGATOR  agg3(38)                00:00:f0:bb:00:03
-----
SYSTEM ID   Actor      | 0x8000, 00:00:f0:bb:00:03
            Partner   | 0x8000, 00:00:f0:cd:cd:01
OPER. KEY   Actor      | 0003, 0003(Admin)
            Partner   | 0003
DEBUGGING   Individual | 0
            Ready     | 1
            Link Count | 2
            Ref. Count | 2
            Rx Link    | 1
            Tx Link    | 1
-----+-----
LINK INFO.  7/3 (15) | In SYNC (1)
            7/4 (16) | In SYNC (1)
-----

OG1100#
OG1100#show etherchannel summary
% Aggregator agg3 38
% Admin Key: 0003 - Oper Key 0003
% Link: 7/3 (15) sync: 1
% Link: 7/4 (16) sync: 1
OG1100#
OG1100#show port etherchannel 9/3

-----
-----
LACP Link 7/3(15)
-----
SYSTEM ID   |
Actor Oper  | 0x8000(32768), 00:00:f0:bb:00:03
Partner Admin | 0x8000(32768), 00:00:00:00:00:00
Partner Oper  | 0x8000(32768), 00:00:f0:cd:cd:01
LAG Link ID  |
Actor Oper   | Port 15, 0x8000(32768), 00:00:f0:bb:00:03
Partner Admin | Port 00, 0x0000(00000), 00:00:00:00:00:00
Partner Oper  | Port 27, 0x8000(32768), 00:00:f0:cd:cd:01
KEY INFO     |
Actor Admin  | 0x0003(0003)
Actor Oper   | 0x0003(0003)
Actor Physical | 0x0004(0000)
Partner Admin | 0x0000(0000)
Partner Oper  | 0x0003(0003)
STATE INFO   |
Actor Admin  | 0x45 ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1
EXP:0
Actor Oper   | 0x3d ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0
EXP:0
Partner Admin | 0x45 ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1
EXP:0

```

```

Partner Oper          | 0x3f ACT:1 TIM:1 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
MACHINE STATE        |
Receive SM           | CURRENT
Periodic Tx SM       | FAST PERIODIC
MUX SM                | COLLECTING/DISTRIBUTING
ETC                   |
LACP En/Disable      | ENABLE
Port En/Disable      | ENABLE
NTT                   | FALSE
Begin                 | FALSE
Ready N               | TRUE
Selected              | SELECTED
Port Moved           | FALSE
AGGREGATOR INFO      |
ID                    | 38
Name                  | agg3
-----
ACT(Activity)         0:Passive          1:Active
TIM(Time-Out)         0:Long Time-Out      1:Short Time-Out
AGG(Aggregation)      0:Individual         1:Aggregatable
SYN(Synchronization) 0:Out of Sync.       1:In Sync.
COL(Collecting)       0:Disable            1:Enable
DIS(Distributing)     0:Disable            1:Enable
DEF(Defaulted)        0:Not Defaulted     1:Defaulted
EXP(Expired)           0:Not Expired        1:Expired

OG1100#
    
```

설정된 인터페이스를 해지 하는 것은 static trunk 와 마찬가지로 ‘no’ 명령어를 L2 INTERFACE_MODE 에서 사용하면 됩니다.

LACP 는 연결된 상대편 스위치와 능동적으로 메시지를 주고 받아서 load-balancing 을 수행합니다.

3.2.3.3 Aggregation 인터페이스의 기능 설정 및 조회

Aggregation 인터페이스는 L2 인터페이스와 동일하게 모든 것을 설정할 수 있으며, 설정된 값은 aggregation 인터페이스에서 확인할 수 있습니다. 먼저, ‘show vlan’을 실행하면 다음과 같습니다.

```

OG1100#show vlan

-----
SLOT          | EPU          | EPU          | SWU          | LACP/TRUNK
              | 2 3 4 5     | 8 9 10 11   | 7            | AGGREGATOR
-----+-----+-----+-----+-----
PORT          | .. .. .. .. | .. .. .. .. | .. .. .. .. |
              | 12 12 12 12 | 12 12 12 12 | 12 34 56 78 | 12 34 56 78
-----+-----+-----+-----+-----
    
```

```

SWITCHPORT      | HH HH HH HH | HH HH HH HH | HH HH HH HH | .. .. .
PRIORITY        | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 0. .. .
INGRESS FILTER  | YY YY YY YY | YY YY YY YY | YY YY YY YY | N. .. .
ACCEPT. FRAME   | AA AA AA AA | AA AA AA AA | AA AA AA AA | .. .. .
-----+-----+-----+-----+
default ( 1)    | UU UU UU UU | UU UU UU UU | UU UU UU UU | .. .. .
VLAN0010 ( 10) | .. .. .. .. | .. .. .. .. | u. .. .. .. | .. .. .
VLAN0020 ( 20) | .. .. .. .. | .. .. .. .. | .t .. .. .. | .. .. .
VLAN0030 ( 30) | .. .. .. .. | u. .. .. .. | .. .. .. .. | .. .. .
Mgt. (4094)    | tt tt tt tt | tt tt tt tt | .. .. .. .. | .. .. .
-----+-----+-----+-----+
SWITCHPORT      : A(Access) H(Hybrid) T(Trunk)
PRIORITY        : IEEE 802.1P Default User-Priority <0-7>
INGRESS FILTER  : Y(Enable) N(Disable)
ACCEPT. FRAME   : Acceptable Frame Type
    A - All frame receive.
    T - Only VLAN Tagged frame receive.
    U - Only VLAN Untagged frame receive.
VLANNAME ( VID) : IEEE 802.1q Port based VLAN information
    U - Untagged VLAN (PVID = VID)
    u - Untagged shared VLAN (PVID != VID)
    T - Tagged VLAN (PVID = VID)
    t - Tagged shared VLAN (PVID != VID)
    P - Only PVID
OG1100#
    
```

위에 보듯이 aggregation 인터페이스에 대한 switchport/accept. Frame 이 지정되지 않았고, ingress filter 도 ‘N’로 설정되어 있습니다. 이것은 아직 bridge-group 이 형성되지 않기 때문입니다. 따라서, 먼저 agg1에 대해서 bridge-group 을 형성하여야 합니다. INTERFACE_MODE 에서 ‘bridge-group’(STP/RSTP 인 경우)을 실행하면 됩니다.

명령어	설명	모드
bridge-group [instance] [path-cost][priority]	Bridge group 설정 및 변경 - Instance : MSTP instance - Path-cost : 포트 path cost 설정 - Priority : bridge 의 포트우선순위설정	Config-interface

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface agg1
OG1100(config-if)#bridge-group
OG1100(config-if)#end
OG1100#show vlan
-----+-----+-----+-----+
SLOT          | EPU          | EPU          | SWU          | LACP/TRUNK
              | 2 3 4 5     | 8 9 10 11   | 7            | AGGREGATOR
-----+-----+-----+-----+
    
```

```

PORT          | .. .. . | .. .. . | .. .. . |
              | 12 12 12 12 | 12 12 12 12 | 12 34 56 78 | 12 34 56 78
-----+-----+-----+-----+
SWITCHPORT    | HH HH HH HH | HH HH HH HH | HH HH HH HH | H. . . . .
PRIORITY      | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 0. . . . .
INGRESS FILTER| YY YY YY YY | YY YY YY YY | YY YY YY YY | Y. . . . .
ACCEPT. FRAME | AA AA AA AA | AA AA AA AA | AA AA AA AA | A. . . . .
-----+-----+-----+-----+
default ( 1)  | UU UU UU UU | UU UU UU UU | UU UU UU UU | U. . . . .
VLAN0010 ( 10)| .. .. . | .. .. . | u. . . . . | .. .. .
VLAN0020 ( 20)| .. .. . | .. .. . | .t .. .. . | .. .. .
VLAN0030 ( 30)| .. .. . | u. . . . . | .. .. . | .. .. .
Mgt. (4094)  | tt tt tt tt | tt tt tt tt | .. .. . | .. .. .
-----+-----+-----+-----+
SWITCHPORT    : A(Access) H(Hybrid) T(Trunk)
PRIORITY      : IEEE 802.1P Default User-Priority <0-7>
INGRESS FILTER : Y(Enable) N(Disable)
ACCEPT. FRAME : Acceptable Frame Type
    A - All frame receive.
    T - Only VLAN Tagged frame receive.
    U - Only VLAN Untagged frame receive.
VLANNAME ( VID) : IEEE 802.1q Port based VLAN information
    U - Untagged VLAN (PVID = VID)
    u - Untagged shared VLAN (PVID != VID)
    T - Tagged VLAN (PVID = VID)
    t - Tagged shared VLAN (PVID != VID)
    P - Only PVID
OG1100#
    
```

위의 예제처럼 switch 포트에 포함되어 다른 L2 인터페이스와 초기 설정값이 동일함을 알 수 있습니다.

Aggregation 인터페이스는 L2 인터페이스와 동일하게 모든 것을 설정 및 조회를 알 수 있으며, 동일한 기능을 제공하게 됩니다.

반면에 일반적인 L2 인터페이스 에서 사용할 수 있는 명령어 이외에 Aggregation 인터페이스에만 설정 및 조회할 수 있는 명령어는 다음과 같습니다.

명령어	설명	모드
Load-balance src-mac dst-mac src-ip dst-ip No load-balance Show etherchannel load-balance	Load balance 설정, 취소, 조회	Config-interface

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface agg2
OG1100(config-if)#load-balance ?
    dst-ip  Destination IP address based load balancing
    dst-mac Destination Mac address based load balancing
    
```

```

src-ip Source IP address based load balancing
src-mac Source Mac address based load balancing

OG1100(config-if)#load-balance src-mac
OG1100(config-if)#q
OG1100(config)#interface agg3
OG1100(config-if)#load-balance src-ip
OG1100(config-if)#q
OG1100(config)#ex
OG1100#show etherchannel load-balance

-----
AGGREGATOR | LOAD SHARING ALGORITHM
-----+-----
agg1 | NONE
agg2 (36) | 0x1: Source MAC address
agg3 (38) | 0x4: Source IP address
agg4 | NONE
-----+-----
agg5 | NONE
agg6 | NONE
agg7 | NONE
agg8 | NONE
-----

OG1100#
    
```

3.2.4 MAC Filtering 설정

사용자 장비 MAC 어드레스 확인을 통한 특정 그룹 접속 제어 및 접속 차단을 목적으로 MAC Table 에 Static Entry 를 추가 또는 삭제 가능합니다. MAC entry 는 동일 브로드캐스트 도메인 즉, 단 VLAN 내에서 단일해야 합니다.

명령어	설명	모드
Mac address MAC(discard forward) IFNAME(vlan <1-4094>)	Static Entry 추가 - MAC : HHHH.HHHH.HHHH format - Discar forward : Entry status - IFNAME : 인터페이스 이름 - VLAN : VLAN ID	config
No mac address MAC(discard forward) IFNAME(vlan <1-4094>)	Static Entry 삭제	config

다음은 각 포트에 특정 MAC 어드레스에 대해 Filtering 하는 설정 및 해제를 보여줍니다.

```

OG1100(config)# mac address 0000.0000.1111 discard 7/1 vlan 10
OG1100(config)# mac address 0000.0000.2222 forward 7/2 vlan 10
OG1100(config)# end
OG1100#show fdb
TOTAL NUMBER OF MAC ENTRY = 5
-----
NUM.      | VLAN  PORT | MAC ADDRESS          | FWD/DIS | STATIC
-----
   1      |   10  7/2  | 00:00:00:00:22:22   | FORWARD | STATIC
   2      |   10  7/1  | 00:00:00:00:11:11   | DISCARD | STATIC
   3      |  4094 CPU | 00:00:F0:BB:00:03   | FORWARD | STATIC
   4      |   10  CPU | 00:00:F0:BB:00:03   | FORWARD | STATIC
   5      |    1  CPU | 00:00:F0:BB:00:03   | FORWARD | STATIC
-----

OG1100#config terminal
OG1100(config)# no mac address 0000.0000.1111 discard 7/1 vlan 10
OG1100(config)# no mac address 0000.0000.2222 forward 7/2 vlan 10
OG1100(config)# end
    
```

3.2.5 mirroring 설정

mirroring 은 특정 포트에 들어오거나 나가는 패킷을 다른 포트에 내보내고자 할 경우에 사용되는 기능입니다. 예를 들어 1/1 번 포트에 들어오는 패킷들을 2/1 번 포트에 내보내어 어떤 패킷들이 1/1 번 포트에 들어오는지를 확인할 수 있습니다.

mirroring 기능은 일반적으로 포트에서 포트에 스위칭 되어 들어오거나 나가는 패킷들이 어떠한 패킷들로 구성되어 있는지를 확인하고자 할 때 자주 사용됩니다. 설정 과정은 먼저 패킷이 mirroring 되어 나갈 포트의 인터페이스 모드로 들어간 후 mirror CLI 를 이용하여 설정합니다.

명령어	설명	모드
mirror interface IFNAME direction (both receive transmit)	Mirroring 할 인터페이스 설정 - IFNAME : 인터페이스 이름 - direction : 방향 설정	interface
no mirror interface IFNAME	Mirroring 설정 삭제	interface

```

OG1100(config)#interface 2/1
OG1100(config-if)#mirror interface 2/2 direction both
OG1100(config-if)#end
OG1100#show mirror
OG1100#show mirror

=====
MTP(Mirror-to-port) | Mirrored port | Direction
-----
                2/1                2/2                Both
-----
    
```

```
Total mirror count : 1
=====

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface 2/1
OG1100(config-if)#no mirror interface 2/2
OG1100(config-if)#
```

3.2.6 tcpdump 설정

tcpdump 는 특정 포트 혹은 VLAN 인터페이스로 들어오는 패킷들 중 스위칭되어 나가는 패킷들이 아닌 CPU 로 전달되는 패킷들(예-ARP, ICMP 패킷)의 패킷 정보를 덤프하여 화면으로 출력하는 기능입니다. 특별한 옵션이 사용되지 않을경우 CPU 로 전달되는 모든 패킷을 덤프하며, 옵션에 따라 원하는 패킷(예-IP 어드레스, Port number)들만을 출력하도록 설정할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다.

- arp : Monitor only ARP packet
- bpdud : Monitor only Layer2 BPDU packet
- ether : Monitor only ethernet frame
- icmp : Monitor only ICMP packet
- igmp : Monitor only IGMP packet
- ip : Monitor only IP
- pim : Monitor only PIM packet
- rarp : Monitor only RARP packet
- tcp : Monitor only TCP
- udp : Monitor only UDP packet

명령어	설명	모드
tcpdump interface IFNAME (arp bpdud ether icmp ip pim rarp tcp udp)	Mirroring 할 인터페이스 설정 - IFNAME : 인터페이스 이름 - Option parameter	EXEC

```
OG1100#tcpdump interface 7/1

tcpdump: WARNING: 7/1: no IPv4 address assigned
tcpdump: listening on 7/1
0:0:f0:12:12:8 1:80:c2:0:0:0 002b 57: 802.1d unknown version
0:0:f0:12:12:8 1:80:c2:0:0:0 002b 57: 802.1d unknown version

2 packets received by filter
0 packets dropped by kernel
OG1100#
```



```

OG1100#tcpdump interface vlan1 arp

tcpdump: WARNING: vlan1: no IPv4 address assigned
tcpdump: listening on vlan1

0 packets received by filter
0 packets dropped by kernel
OG1100#
    
```

3.2.7 packet sampling

패킷 샘플링 기능은 특정 포트로 들어오는 패킷들 중 일정한 확률로 패킷을 캡처하여 저장하거나, 실시간으로 캡처링된 패킷들의 내용을 확인하고자 할 때 사용됩니다. 특정 포트가 가능한 대역폭을 모두 사용하는 정도의 패킷이 유입되고 있을 경우 유입되는 패킷들 전체를 확인하기란 현실적으로 불가능 하기 때문에, 일정한 비율로 샘플링하여 샘플링된 결과만을 확인하여도 현재 트래픽의 상태를 예측하거나 분석할 수 있습니다. 패킷 샘플링 기능은 이와 같은 목적으로 사용됩니다.

3.2.7.1 packet sampling 설정 및 조회

샘플링 기능의 설정은 인터페이스 단위로 이루어지고, 샘플링된 결과를 실시간으로 확인하거나 저장할 수 있습니다. 저장된 결과는 위 tcpdump CLI 를 통하여 확인할 수 있습니다.

명령어	설명	모드
sflow(ingress egress) <1-65535	샘플링 빈도수 설정 - (ingress egress)는 입력 패킷을 샘플링할 것인지, 출력 패킷을 샘플링할 것인지를 결정 - <1-65535> : 샘플링 빈도수를 지정하는 것으로 값이 클수록 더 많은 패킷이 샘플링 되도록 보장합니다.	INTERFACE
no sflow(ingress egress)	샘플링 설정을 삭제	INTERFACE
show sflow status	샘플링 설정 상태를 조회	EXEC

```

OG1100#
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface 7/1
OG1100(config-if)#sflow ?
    egress  Egress
    ingress  Ingress

OG1100(config-if)#sflow ingress ?
    <1-65535> Sample Rate <1-65535> ( 65535 means 0.4% sample rate )

OG1100(config-if)#sflow ingress 10
    
```

```

OG1100(config-if)#end
OG1100#show sflow status
=====
INTF.      INGRESS_RATE    EGRESS_RATE
-----
 2/1        DISABLED        DISABLED
 2/2        DISABLED        DISABLED
 3/1        DISABLED        DISABLED
 3/2        DISABLED        DISABLED
 4/1        DISABLED        DISABLED
 4/2        DISABLED        DISABLED
 5/1        DISABLED        DISABLED
 5/2        DISABLED        DISABLED
 8/1        DISABLED        DISABLED
 8/2        DISABLED        DISABLED
 9/1        DISABLED        DISABLED
 9/2        DISABLED        DISABLED
10/1        DISABLED        DISABLED
10/2        DISABLED        DISABLED
11/1        DISABLED        DISABLED
11/2        DISABLED        DISABLED
 7/1                10        DISABLED
 7/2        DISABLED        65535
 7/3        DISABLED        DISABLED
 7/4        DISABLED        DISABLED
 7/5        DISABLED        DISABLED
 7/6        DISABLED        DISABLED
 7/7        DISABLED        DISABLED
 7/8        DISABLED        DISABLED
=====
OG1100#
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface 7/1
OG1100(config-if)#no sflow ingress
OG1100(config-if)#

```

3.2.7.2 packet sampling monitor

위 패킷 샘플링을 통해 설정된 포트는 설정된 값에 따라 패킷을 CPU 쪽으로 샘플링하여 전달합니다. 전달된 패킷은 실시간으로 확인하거나 시스템 내에 저장할 수 있습니다. 샘플링된 패킷의 실시간 확인은 tcpdump CLI를 모니터링 할 수 있습니다.

```

OG1100#tcpdump traffic-monitor realtime

0:0:0:0:0:20 0:0:0:0:0:19 8100 132: 802.1Q vlan#1 P0 198.19.1.2 >
198.19.1.1: ip-proto-114 90
0:0:0:0:0:20 0:0:0:0:0:19 8100 132: 802.1Q vlan#1 P0 198.19.1.2 >
198.19.1.1: ip-proto-114 90
0:0:0:0:0:20 0:0:0:0:0:19 8100 132: 802.1Q vlan#1 P0 198.19.1.2 >
198.19.1.1: ip-proto-114 90

```

```

0:0:0:0:0:20 0:0:0:0:0:19 8100 132: 802.1Q vlan#1 P0 198.19.1.2 >
198.19.1.1: ip-proto-114 90
0:0:0:0:0:20 0:0:0:0:0:19 8100 132: 802.1Q vlan#1 P0 198.19.1.2 >
198.19.1.1: ip-proto-114 90
0:0:0:0:0:20 0:0:0:0:0:19 8100 132: 802.1Q vlan#1 P0 198.19.1.2 >
198.19.1.1: ip-proto-114 90
0:0:0:0:0:20 0:0:0:0:0:19 8100 10:0:0:0:0:20 0:0:0:0:0:19 8100 132:
802.1Q vlan#1 P0 198.19.1.2 > 198.19.1.1: ip-proto-114 90
OG1100#
    
```

sflow 의 설정에 의해 샘플링된 패킷은 다음 CLI 를 통하여 시스템에 저장됩니다. 최대 60000 개의 패킷을 저장할 수 있으며, 지정된 개수 이상이 되면 자동으로 패킷 저장을 중지합니다. 패킷 캡처를 중지하였을 경우 현재까지 저장된 패킷들만 시스템에 저장되고 그 이후의 패킷은 저장되지 않습니다.

명령어	설명	모드
Traffic-monitor capture start <1-60000>	샘플링된 패킷을 저장할 때 저장할 패킷 개수 설정	EXEC
Traffic-monitor capture stop	저장을 중지함.	EXEC
show traffic-monitor capture status	현재까지 저장된 패킷 개수를 출력합니다.	EXEC

```

OG1100#traffic-monitor capture start 10
OG1100#
OG1100#show traffic-monitor capture status
=> [ 2476 ] packets were captured...
OG1100#traffic-monitor capture stop
% STOP Packet capture engine.
OG1100#
    
```

저장된 패킷은 tcpdump CLI 를 이용하여 그 내용을 확인할 수 있습니다.

```

OG1100#tcpdump traffic-monitor captured

10:22:54.120042 802.1Q vlan#1 P0 198.19.1.2 > 198.19.1.1: ip-proto-114
90
10:22:54.120056 802.1Q vlan#1 P0 198.19.1.2 > 198.19.1.1: ip-proto-114
90
10:22:54.120062 802.1Q vlan#1 P0 198.19.1.2 > 198.19.1.1: ip-proto-114
90
10:22:54.120068 802.1Q vlan#1 P0 198.19.1.2 > 198.19.1.1: ip-proto-114
90

0 packets received by filter
0 packets dropped by kernel
OG1100#
    
```

3.3 Layer 3 환경 설정

당 시스템은 L2/L3 switching 을 동시에 지원하고 L3 switching 은 현재 static routing 을 지원합니다. L3 Interface 는 VLAN 을 설정할 때 동시에 생성되며, L3 관련 설정이 VLAN 인터페이스에서 설정 됩니다.

3.3.1 IP 어드레스/subnet 설정 및 조회

먼저 VLAN 인터페이스를 생성합니다. 위의 예제에서 VLAN10 을 생성하면, 동시에 L3 인터페이스인 VLAN10 이 생성됩니다. 따라서, configure mode 에서 L3 INTERFACE_MODE 로 들어가기 위하여 ‘interface vlanID’을 주면 됩니다.

INTERFACE_MODE 에서 다음과 명령으로 IP 어드레스/subnet 을 설정할 수 있습니다.

또한, 사용하기 위해서는 ‘shutdown’ 이 기본임으로 admin status 를 enable 로 변경하여야 합니다.

명령어	설명	모드
ip address A.B.C.D/M [secondary]	IP 어드레스 및 subnet 설정 및 변경	Config-interface
[no] shutdown	인퍼페이스의 administrativ status 변경	Config-interface
show ip interface [IFNAME] brief	설정된 IP 어드레스/subnet 조회 IFNAME : 인터페이스 이름	Enable

```

OG1100(config)# interface vlan10
OG1100(config-if)# ip address 10.0.0.1/24
OG1100(config-if)# no shutdown
OG1100(config-if)# end
OG1100# show ip interface vlan10 brief
=====
Interface                IP-Address            Admin  OP
-----
vlan10                    10.0.0.1/24          up     down
=====
OG1100# show ip interface brief  (전체 인터페이스 조회)
=====
Interface                IP-Address            Admin  OP
-----
lo                        127.0.0.1/8          up     up
vlan1                     unassigned            down   down
vlan4094                  192.168.200.1/18     up     up
vlan10                    10.0.0.1/24          up     down
vlan20                    unassigned            down   down
=====
OG1100#

```

3.3.2 Secondary IP 어드레스/subnet 설정 및 조회

각 인터페이스에서 secondary IP 를 설정할 수 있습니다. 위의 IP 설정과 동일하게 configure mode 에서 설정하고, 단지 ‘secondary’를 더 추가하면 됩니다. 최대 10 개까지 입력이 가능합니다.

```

OG1100(config-if)# ip address 10.0.1.1/24 secondary
OG1100(config-if)# end
OG1100# show ip interface brief
=====
Interface                IP-Address      Admin  OP
-----
lo                        127.0.0.1/8    up     up
vlan1                     unassigned     down   down
vlan4094                  192.168.200.1/18 up     up
vlan10                    10.0.0.1/24    up     up
                        10.0.1.1/24    up     up (secondary IP)
vlan20                    unassigned     down   down
=====
OG1100#
    
```

3.3.3 IP 어드레스/subnet 삭제

설정된 IP 어드레스/subnet 을 삭제할 경우 L3 INTERFACE_MODE 에서 ‘no’ 명령어를 사용합니다. Secondary IP 인 경우에는 secondary 를 입력하면 됩니다.

명령어	설명	모드
no ip address A.B.C.D/M [secondary]	IP 어드레스 및 subnet 설정 삭제	Config-interface

```

OG1100(config-if)# no ip address 10.0.1.1/24 secondary (secondary IP
삭제)
OG1100(config-if)# end
OG1100# show ip interface vlan10 brief
=====
Interface                IP-Address      Admin  OP
-----
vlan10                    10.0.0.1/24    up     up
=====
OG1100#
    
```

3.3.4 Static ARP 설정 및 ARP 조회

L3 인터페이스의 IP 설정하고 나서 entry 에 접속된 router/host 의 MAC 을 어드레스를 요청하기 위해서 arp 패킷이 사용되며, 특정한 router/host 의 IP/MAC 을 고정하여 사용할 수 있으며, 설정된 arp 를 flushing 할 수 있습니다. 설정은 configure mode 에서 할 수 있으며, 삭제할 때는 'no'명령어를 사용하면 됩니다.

명령어	설명	모드
<code>arp A.B.C.D Macadd IFNAME PORT</code>	Static arp 등록 - Macadd : AA:BB:CC:DD:EE:FF 어드레스 - IFNAME : 인터페이스 이름 - Port : 설정한 포트	Config
<code>No arp A.B.C.D Macadd IFNAME PORT</code>	Static arp 등록 삭제 - Macadd : AA:BB:CC:DD:EE:FF 어드레스 - IFNAME : 인터페이스 이름 - Port : 설정한 포트	Config
<code>arp aging time-out <1-3000></code>	Aging timeout 설정 및 변경	Config
<code>Arp flush [IFNAME]</code>	Dynamic Arp table 을 clear	Config
<code>Show arp [IFNAME][aging-timeout]</code>	설정된 arp table 조회	Enable

```

OG1100#show arp
=====
IP address      Mac Address      PORT      IfName
-----
10.1.1.2        00:00:f0:bb:00:01  9/1      vlan10

Total count : 1
(T) : Trunk Port      (S) : Static entry
=====

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#arp 10.0.0.10 00:00:f0:00:00:01 vlan10 9/1
OG1100(config)#exit
OG1100#show arp vlan10
=====
IP address      Mac Address      PORT      IfName
-----
10.1.1.2        00:00:f0:bb:00:01  9/1      vlan10
10.0.0.10       00:00:f0:00:00:01  9/1      vlan10      S (고정 arp)

Total count : 2
(T) : Trunk Port      (S) : Static entry
=====

OG1100#show arp aging-timeout
arp aging-timeout : 300
    
```

3.3.5 Static routing 설정 및 조회

목적지 IP 어드레스 A.B.C.D/M 을 가진 Packet Traffic 을 A.B.C.D 어드레스 또는 인터페이스로 Static Routing 하도록 설정하는데 사용됩니다. Distance 는 목적지의 도착에 대한 링크 distance 를 설정하여 동일 목적지에 대한 다수개의 Routing Path 가 존재할 경우 distance 가 낮은 Routing Path 를 선택하게 됩니다. 각 route 설정을 조회하려면 ‘show ip route []’ 으로 설정 값을 조회할 수 있습니다. 각 특성에 따라서 조회가 가능합니다.

명령어	설명	모드
<code>ip route {A.B.C.D/M A.B.C.D M.M.M.M} {A.B.C.D IFNAME} [distance <1-255>] [weight<1-32>]</code>	Static IP route 설정 변경 - A.B.C.D/M : routing 될 경로 - A.B.C.D : routing 될 연결된 IP 어드레스 - M.M.M.M : subnet mask - IFNAME : 인터페이스 이름 - Distance : cost 값 변경 - Weigh : 경로의 우선순위설정	Config
<code>ip route A.B.C.D/M null</code>	null 인터페이스를 route path 로 설정 시 사용	Config
<code>show ip route [database] [connected] [A.B.C.D] [A.B.C.D/M][static][system]</code>	설정된 IP route 조회	Enable

여기서 ‘weight’는 ECMP 인 경우에는 설정이 필요하지 않으나, WCMP(Weighted Cost MultiPath)에서 weight 를 설정할 경우 사용합니다. Multiple Path 에 할당에 WCMP 의 weight 총합은 32 를 넘을 수 없습니다.

```

OG1100# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       > - selected route, * - FIB route, p - stale info

C   *> 10.0.0.0/24 is directly connected, vlan10
C   *> 127.0.0.0/8 is directly connected, lo
C   *> 192.168.192.0/18 is directly connected, vlan4094

OG1100(config)# ip route 20.1.1.0/24 10.0.0.2
OG1100(config)# exit
OG1100# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
    
```

```

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
> - selected route, * - FIB route, p - stale info

C  *> 10.0.0.0/24 is directly connected, vlan10
S  *> 20.1.1.0/24 [1/0] via 10.0.0.2, vlan10 (static route 설정된 값)
C  *> 127.0.0.0/8 is directly connected, lo
C  *> 192.168.192.0/18 is directly connected, vlan4094
OG1100#

```

설정된 static route 를 삭제하려면 앞에서 설명한 route 설정명령 앞에 ‘no’를 추가하여 명령어를 사용하면 됩니다.

```

OG1100(config)# no ip route 20.1.1.0/24 10.0.0.2
OG1100(config)# exit
OG1100# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
> - selected route, * - FIB route, p - stale info

C  *> 10.0.0.0/24 is directly connected, vlan10
C  *> 127.0.0.0/8 is directly connected, lo => static route 설정이
삭제됨.
C  *> 192.168.192.0/18 is directly connected, vlan4094

OG1100#

```

L3 load balancing 을 하기 위하여 제공되는 프로토콜이 ECMP 입니다. ECMP 를 설정하기 위해서는 기본 값인 weight 1 인 경우로 따로 설정이 필요하지 않고 각 L3 인터페이스에 대해서 같은 gateway 를 설정해 주면 됩니다.

```

OG1100(config)# ip route 20.1.1.0/24 10.0.0.2
OG1100(config)# ip route 20.1.1.0/24 30.0.0.2
OG1100(config)# exit
OG1100# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
> - selected route, * - FIB route, p - stale info

C  *> 10.0.0.0/24 is directly connected, vlan10
C  *> 30.0.0.0/24 is directly connected, vlan20

```



```

S   *> 20.1.1.0/24 [1/0] via 10.0.0.2, vlan10
    *>           [1/0] via 30.1.1.2, vlan20 (ECMP가 추가 설정됨)
C   *> 127.0.0.0/8 is directly connected, lo
C   *> 192.168.192.0/18 is directly connected, vlan4094
OG1100#

```

ECMP 의 설정을 해지하려면 위의 static routing 해지와 같이 해당되는 설정에 대해 ‘no’ 명령어를 사용하면 됩니다.

시스템에서 수용할수 있는 Multipule Path Rouing Entry 개수는 63 개로 제한 되어 있으며, 각 Multiple Path Routing Entry 는 최대 32 개의 Multiple Path 를 가집니다.

모든 L3 packet 에 대해서 모든 경로에 대해서 static route 를 설정할 수 없기 때문에 default gateway 를 설정할 필요가 있습니다. 현재 default gateway 는 두 개 이상 설정이 가능합니다. Route 설정에서 destination ip prefix 을 ‘0.0.0.0/0’으로 설정하면 됩니다.

```

OG1100(config)#ip route 0.0.0.0/0 10.0.0.2 => default gateway설정
OG1100(config)#end
OG1100#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       > - selected route, * - FIB route, p - stale info

S   *> 0.0.0.0/0 [1/0] via 10.0.0.2, vlan10 (default gateway조회)
C   *> 10.0.0.0/24 is directly connected, vlan10
C   *> 10.0.0.0/24 is directly connected, vlan10
S   *> 20.1.1.0/24 [1/0] via 10.0.0.2, vlan10
    *>           [1/0] via 30.1.1.2, vlan20
C   *> 127.0.0.0/8 is directly connected, lo
C   *> 192.168.192.0/18 is directly connected, vlan4094
OG1100#

```

3.3.6 ARP Proxy 설정 및 조회

서로 다른 포트에 대해서 같은 subnet 이 존재할 경우 ARP(Address Resolution Protocol) 의 learning 이 되지 않습니다. 이 문제를 해결하기 위하여 ‘arp proxy’ 명령어를 사용하게 되며, OG-1100 시스템의 한 EPU 포트에 연결되어 있는 ONT 간의 통신을 할 수 없게 되어 있습니다. 따라서, 한 EPU 포트에 있는 ONT 간의 통신을 하기 위해서 ‘arp proxy-plus’ 라는 특정기능을 사용할 수 있습니다. 명령은 L3 INTERFACE_MODE 에서 설정할 수 있습니다.

명령어	설명	모드
arp proxy	해당 인터페이스에 arp proxy enable 로 변경	Config-interface
arp proxy plus	한 EPU 내에 ONT 간의 L3 통신 enable 로 변경	Config-interface

```

OG1100(config)#interface vlan30
OG1100(config-if)#ip address 103.10.10.1/24
OG1100(config-if)#arp proxy
OG1100(config-if)#no arp proxy
OG1100(config-if)#arp proxy-plus
OG1100(config-if)#end
OG1100#show running-config interface vlan30
Building configuration...
!
interface vlan30
 ip address 103.10.10.1/24
 shutdown
 arp_proxy_plus
OG1100#

```

3.4 멀티캐스팅 환경 설정

OG-1100 시스템에서는 IP 멀티캐스팅을 위해 다음과 같은 기능을 지원합니다.

- IGMP snooping
- PIM-SM(Protocol Independent Multicast Sparse-Mode 버전 2 지원)
- IGMP(Internet Group Management Protocol 버전 1, 2 지원)

3.4.1 IGMP snooping

일반적인 L2 스위치의 경우, 멀티캐스트 트래픽을 수신하면 모든 포트로 트래픽을 flooding 합니다. OG-1100은 L2 스위치로 동작할 경우에도 수신되는 IGMP packet의 정보를 확인, L2 멀티캐스트 테이블을 설정함으로써, 대역 낭비 없이 해당 멀티캐스트 트래픽을 원하는 포트로만 전송할수 있도록 하는 IGMP snooping 기능을 지원합니다.

OG-1100 시스템에서 IGMP snooping 과 관련 설정은 다음과 같이 크게 다섯가지 항목으로 나눌수 있습니다.

- IGMP snooping 기능 활성화
- IGMP snooping proxy 기능 설정
- IGMP snooping querier 기능 설정
- 멀티캐스트 그룹에 멤버포트 사용자 추가
- 멀티캐스트 트래픽 포워딩 정책 설정

3.4.1.1 IGMP snooping 기능 설정

시스템 및 각 VLAN 별 IGMP snooping 활성화

OG-1100 시스템의 멀티캐스트 기능은 초기 부팅시 L3 멀티캐스팅을 하도록 설정되어 있습니다.

따라서, L2 멀티캐스트인 IGMP snooping 을 동작시키기 위해서는 다음 명령어를 이용해서 먼저 L3 멀티캐스트 기능을 해제해야 합니다.

명령어	설명	모드
no ip multicast-routing	-	Config

OG-1100 시스템에서의 IGMP snooping 기능의 활성화는 **ip igmp snooping** 명령어를 실행하면 설정되는데, 이 명령어는 시스템의 IGMP snooping 의 기능을 활성화하는 것이고, 원하는 각 VLAN 에서 IGMP snooping 을 동작시키기 위해서는 각 VLAN 별로 활성화를 해주어야 합니다.

명령어	설명	모드
ip igmp snooping [vlan ID] no ip igmp snooping [vlan ID]	시스템의 IGMP snooping 기능 활성화 및 각 VLAN 별 기능 활성화	Config
show ip igmp snooping [vlan ID]	설정된 IGMP snooping 조회	Enable

다음은 VLAN 10에 IGMP snooping 기능을 활성화하는 예입니다.

```

OG1100(config)#no ip multicast-routing
OG1100(config)#ip igmp snooping
OG1100(config)#ip igmp snooping vlan 10
OG1100(config)#end
OG1100#show ip igmp snooping
IGMP Snooping is globally enabled
IGMP Snooping Proxy is disabled
VLAN 1
    IGMP Snooping is disabled
VLAN 10
    IGMP Snooping is enabled
    IGMP snooping query interval is 60000 ms
    IGMP snooping max query response time is 10000 ms
    IGMP Snooping last member query interval is 1000 ms
    IGMP snooping other querier timeout interval is 120000 ms
    IGMP snooping group membership interval is 260000 ms
    IGMP snooping v1 router present timeout is 400000 ms
    IGMP snooping interface 9/1 version 2
VLAN 20
    IGMP Snooping is disabled
VLAN 30
    IGMP Snooping is disabled
VLAN 4094
    IGMP Snooping is disabled
OG1100#
    
```

멀티캐스트 라우터 포트 지정

VLAN 의 IGMP snooping 기능이 활성화 되면, 상위 멀티캐스트 라우터가 연결되어 있는 포트에 IGMP Query 메시지가 수신 될 경우, 기본적으로 해당 포트를 mrouter 포트에 자동으로 등록하게 됩니다. 하지만, Query 메시지를 받지 못하거나, Query 메시지를 받기 전에 하위 포트에 IGMP report 메시지가 올라오면, mrouter 포트가 지정되어 있지 않기 때문에 IGMP Report 를 멀티캐스트 라우터로 전송하지 못하는 상황이 발생할수 있습니다. 따라서, IGMP snooping 기능을 활성화 한 후, **ip igmp snooping mrouter** 명령어를 사용해 서포트를 직접 지정해 주는 방식이 권장됩니다. 지정된 mrouter 포트를 해제할 경우는 **no ip igmp snooping mrouter** 명령어를 사용합니다. .

명령어	설명	모드
ip igmp snooping mrouter interface <port> no ip igmp snooping mrouter interface <port>	<port> 를 mrouter 포트에 지정 지정된<port>를 mrouter 포트에서 해제	Config
show ip igmp snooping mrouter	Mrouter 포트정보 출력	Enable

다음은 7/1 포트를 mrouter 포트로서 설정 및 조회하는 예입니다.

```
OG1100(config)#ip igmp snooping mrouter interface 7/1
OG1100#show ip igmp snooping mrouter
  VLAN: 10  Igmp Snooping Enabled
    Mrouter -> 7/1 (Configured)
  VLAN: 20  Igmp Snooping Disabled
  VLAN: 30  Igmp Snooping Disabled
  VLAN: 4094 Igmp Snooping Disabled
OG1100#
```

IGMP Group Membership Interval 변경

IGMP 그룹 멤버십 인터벌(IGMP Group Membership Interval)은 멀티캐스트 그룹을 테이블에서 삭제하기 전에 IGMP 응답메시지(IGMP report 메시지)를 기다리는 최대시간입니다. IGMP Query 메시지를 각 포트로 전송한 후, IGMP 그룹 멤버십 인터벌 동안 IGMP Report 메시지를 받지 못하면 해당포트에 멤버가 없다고 간주하여 그룹 멤버십에서 그 포트를 삭제합니다.

OG-1100 시스템에서 IGMP 그룹 멤버십 인터벌의 기본값은 260000(ms) 입니다. 이 값을 변경하고 조회하는 명령어는 다음과 같습니다.

명령어	설명	모드
ip igmp snooping group-membership-interval <interval> vlan <vlan ID>	- ID 가 <vlan ID>인 VLAN 의 그룹 멤버십 인터벌 값을 <interval>ms 로 설정	Config
no ip igmp snooping group-membership-interval <interval> vlan <vlan ID>	- VLAN <vlan ID>의 그룹 멤버십 인터벌값을 기본값으로 설정	
show ip igmp snooping group-membership-interval [vlan ID]	Mrouter 포트 정보 출력	Enable

다음은 OG-1100 시스템에서 VLAN10 의 IGMP snooping group membership interval 값을 300000(ms)로 변경하는 예입니다.

```
OG1100(config)#ip igmp snooping group-membership-interval 300000 vlan 10
OG1100(config)#end
OG1100#show ip igmp snooping group-membership-interval
  VLAN 1
    IGMP Snooping group-membership-interval is 260000 ms
  VLAN 10
    IGMP Snooping group-membership-interval is 300000 ms
  VLAN 20
    IGMP Snooping group-membership-interval is 260000 ms
  VLAN 4094
    IGMP Snooping group-membership-interval is 260000 ms
OG1100#
```

IGMP Snooping 의 Group Membership Interval 값을 설정할 때는, IGMP Query 의 주기와 Max Respons Time 값에 주의하여 설정해야 합니다.

Last member query interval 설정

호스트가 특정 그룹 멤버쉽에서 탈퇴하기 위해 IGMP Leave 메시지를 보내면, 멀티캐스트 라우터는 그 호스트가 연결되어 있는 포트를 테이블에서 바로 삭제하지 않고, 그 그룹에 가입되어 있는 다른 호스트가 있는지 확인하기 위해 Specific Query 메시지를 해당 포트로 전송합니다. 이 때, 응답이 없으면 비로서 그룹멤버쉽에서 해당 포트를 삭제하게 됩니다. 이 때, Specific Query 메시지를 전송한 후, 응답을 기다리는 시간이 Last Member Query Interval 입니다.

OG-1100 시스템에서는 기본적으로 Last Member Query Interval 이 1000ms 로 설정이 되어있습니다. 이 값을 변경하고 조회하는 명령어는 다음과 같습니다.

명령어	설명	모드
<pre>ip igmp snooping last-member-query-interval <interval> vlan <vlan ID></pre>	- ID 가 <vlan ID>인 VLAN 의 last-member-query-interval 값을 <interval>ms 로 설정	Config
<pre>no ip igmp snooping last-member-query- interval <interval> vlan <vlan ID></pre>	- VLAN <vlan ID>의 last-member-query-interval 을 기본 값으로 설정	
<pre>show ip igmp snooping last-member-query- interval [vlan ID]</pre>	last-member-query-interval 정보 출력	Enable

다음은 IGMP Snooping 에서 VLAN10 에 대한 Last Member Query Interval 을 2000(ms) 로 변경 및 조회하는 예입니다..

```
OG1100(config)#ip igmp snooping last-member-query-interval 2000 vlan
10
OG1100(config)#end
OG1100#show ip igmp snooping last-member-query-interval
VLAN 1
    IGMP Snooping last-member-query-interval is 1000 ms
VLAN 10
    IGMP Snooping last-member-query-interval is 2000 ms
VLAN 20
    IGMP Snooping last-member-query-interval is 1000 ms
VLAN 4094
    IGMP Snooping last-member-query-interval is 1000 ms
OG1100#
```

Immediate-leave 기능 설정

호스트로부터 IGMP Leave 메시지를 받았을 때, 곧 바로 그룹멤버십에서 해당 포트를 삭제하도록 하는 기능입니다. 즉, 이 기능을 활성화 하면 호스트로부터 Leave 메시지를 받았을 때, Specific Query 메시지를 전송하지 않습니다.

따라서 Last member Query Interval 동안 기다림 없이 바로 해당 포트를 멤버십테이블에서 삭제합니다.

OG-1100 시스템에서 immediate-leave 기능을 설정하기 위해서는 다음과 같은 명령어를 사용합니다.

명령어	설명	모드
ip igmp snooping immediate-leave vlan <vlan ID>	- VLAN 의 immediate-leave 기능 활성화	Config
no ip igmp snooping immediate-leave vlan <vlan ID>	- VLAN 의 immediate-leave 기능 비활성화	
show ip igmp snooping immedaite-leave vlan <vlan ID>	Mrouter 포트정보 출력	Enable

OG-1100 시스템에서 VLAN10 에 immediate-leave 기능을 활성화 하고 조회하는 예는 다음과 같습니다.

```
OG1100(config)#ip igmp snooping immediate-leave vlan 10
OG1100(config)#end
OG1100#show ip igmp snooping immediate-leave
VLAN 1
    IGMP Snooping immediate-leave is disabled
VLAN 10
    IGMP Snooping immediate-leave is enabled
VLAN 20
    IGMP Snooping immediate-leave is disabled
VLAN 4094
    IGMP Snooping immediate-leave is disabled
OG1100#
```

3.4.1.2 IGMP Snooping Proxy 기능 설정

IGMP Proxy 기능이란, 시스템이 상위 멀티캐스트 라우터에 대해서는 하나의 호스트로서 동작하고, 하위 호스트들에 대해서는 마치 멀티캐스트 라우터처럼 동작하는 기능을 말합니다. 즉, 멀티캐스트 라우터처럼 주기적으로 query 메시지를 보내어 하위 호스트들에 대한 멤버십 관리를 하다가가 상위 멀티캐스트 라우터에서 query 메시지를 받으면, 관리하고 있던 멤버십 테이블을 참고하여, 마치 하나의 호스트처럼 그에 대한 report 를 보내는 기능을 말합니다.

IGMP Snooping Proxy 기능 활성화

OG-1100 시스템의 IGMP snooping 기능에서도 Proxy 기능이 있는데, 이를 설정하는 명령어는 다음과 같습니다.

명령어	설명	모드
ip igmp snooping proxy	IGMP proxy 기능 활성화	Config
no ip igmp snooping proxy	IGMP proxy 기능 비활성화	

IGMP Proxy 기능이 활성화 되었는지에 대한 확인은 **show ip igmp snooping** 명령어를 통해 확인할 수 있습니다.

Proxy 의 IP 어드레스 설정

일반적으로 L2 멀티캐스팅에서는 IP 가 필요하지 않지만, IGMP Snooping Proxy 로 동작할 때에는 상위 멀티캐스트 라우터에서 보내는 Query 메시지에 대한 Report 메시지를 보내야 하기 때문에 IP 어드레스를 필요로 합니다.

상위 라우터에 보내는 메시지의 Source IP 어드레스는 기본값으로 192.168.0.5 로 설정되어 있습니다. Proxy 의 IP 어드레스를 바꿀 때에는 Config 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
ip igmp snooping proxy ip addr A.B.C.D	IGMP proxy IP 어드레스 설정 A.B.C.D IP 어드레스	Config

IGMP Proxy 의 IP 어드레스 확인은 **show ip igmp snooping** 명령어를 통해 확인할 수 있습니다.

다음은 OG-1100 시스템에서 시스템의 IGMP Snooping Proxy 기능을 활성화하고 Proxy 의 IP 어드레스를 192.168.100.2 로 설정하는 예입니다.

```

OG1100(config)#ip igmp snooping proxy
OG1100(config)#ip igmp snooping proxy ipaddr 192.168.100.2
OG1100(config)#end
OG1100#show ip igmp snooping
IGMP Snooping is globally enabled
IGMP Snooping Proxy is enabled
IGMP Snooping Proxy IP is 192.168.100.2
VLAN 1
    IGMP Snooping is disabled
VLAN 10
    IGMP Snooping is enabled
    IGMP Snooping querier enabled
    IGMP Snooping immediate-leave is enabled
    IGMP snooping query interval is 125000 ms
    IGMP snooping max query response time is 2000 ms
    IGMP Snooping last member query interval is 2000 ms
    
```



```

IGMP snooping other querier timeout interval is 300000 ms
IGMP snooping group membership interval is 300000 ms
IGMP snooping vl router present timeout is 400000 ms
IGMP snooping interface 1/2 version 2
IGMP snooping interface 9/1 version 2
IGMP snooping interface 9/2 version 2
IGMP snooping interface 9/3 version 2
IGMP snooping interface 9/4 version 2
VLAN 20
    IGMP Snooping is disabled
VLAN 4094
    IGMP Snooping is disabled
OG1100#

```

Proxy 기능이 활성화 되었을 때는, 상위 멀티캐스트에서 전송되는 Query 메시지에 대해 OG-1100 시스템에서 직접 응답(Report)하기 때문에 호스트에는 Query 메시지가 전송되지 않습니다. 따라서 OG-1100 시스템에서 Proxy 기능을 활성화 했을때는 IGMP Snooping Querier 기능 역시 활성화 해 주어야 합니다.

3.4.1.3 IGMP Snooping Static Group 설정

일반적으로 IGMP snooping 기능이 활성화 되면, IGMP 메시지에 따라 멀티캐스트 그룹에 호스트들이 동적으로(자동적으로) 가입되고 탈퇴되도록 동작하지만, 필요한 경우 원하는 포트를 원하는 그룹에 등록할 수 있고, 또는 특정 멀티캐스트 트래픽이 시스템까지 전송되도록 설정할 수 있습니다.

OG-1100 시스템에서는 **ip igmp snooping static-group** 명령어를 사용해서 static group 에 등록합니다. 이때 Group 어드레스만 지정을 하면 상위 멀티캐스트 라우터로 IGMP Report 메시지를 보냄으로서 해당 Group 의 멀티캐스트 트래픽이 OG-1100 시스템까지 전송되도록 합니다. 여기에 특정 포트까지 지정을 하게되면 해당 트래픽이 지정한 포트로 전송되도록 그룹 멤버십 테이블을 설정합니다.

OG-1100 시스템에서 Static Group 을 등록 및 해제하는 명령은 다음과 같습니다.

명령어	설명	모드
ip igmp snooping static-group A.B.C.D vlan <vlan ID> [interface <PORT>]	Static Group 및 포트 등록 - VLAN ID - PORT	Config
no ip igmp snooping static-group A.B.C.D vlan <vlan ID> [interface <PORT>]	등록된 Static Group 및 포트 해제	

등록된 Static Group 정보는, group 만을 지정한 경우 **show ip igmp snooping static-group** 을 사용해 확인할 수 있고, 포트까지 지정한 경우는 멀티캐스트 포워딩 테이블에 등록되기 때문에 **show ip igmp snooping forwarding table** 명령어를 통해 확인할 수 있습니다.

명령어	설명	모드
show ip igmp snooping static-group	등록된 Static Group 확인	enable
show ip igmp snooping forwarding table	등록된 static member 확인	

Static Group 을 등록하면 상위 멀티캐스트 라우터의 Query 에 대한 응답을 호스트가 아닌 시스템에서 직접하기 때문에 IP 어드레스를 필요로 합니다. 따라서 Static Group 에 등록했을 경우는 적절한 IP 어드레스를 **ip igmp snooping proxy ipaddr** 사용해서 설정해 주어야 합니다.

다음은 멀티캐스트 그룹 225.1.1.10 에 해당하는 트래픽이 OG-1100 시스템까지 전송되어 지도록 VLAN10 에 멀티캐스트 그룹을 등록하는 예입니다.

```

OG1100(config)#ip igmp snooping static-group 225.1.1.10 vlan 10
OG1100(config)#ex
OG1100#show ip igmp snooping static-group

-----
VLAN   Group Address      Group MAC Address
-----
10     225.001.001.010   0100.5e01.010a

OG1100#
    
```

아래 예는 멀티캐스트 그룹 225.1.1.20 을 VLAN10 의 포트 3/1 에 등록하는 예입니다. 이 경우 225.1.1.20 에 해당하는 멀티캐스트 트래픽이 VLAN10 의 3/1 포트로 전송하도록 OG-1100 시스템의 멀티캐스트 포워딩 테이블이 설정됩니다.

```

OG1100(config)#ip igmp snooping static-group 225.1.1.20 vlan 10
interface 3/1
OG1100(config)#ex
OG1100#show ip igmp snooping forwarding table

-----
VLAN   Group Address      Group MAC-Addr    Member-Ports (Aging time)
-----
10     225.001.001.020   0100.5e01.0114   3/1 (static)

OG1100#
    
```

3.4.1.4 IGMP Snooping Querier 기능 설정

주변에 IGMP Querier 가 없는 경우, 즉 IGMP Query 메시지를 받을 수 없는 경우, OG-1100 시스템은 그룹 멤버십을 유지하기 위해 IGMP Querier 로 동작할 수 있습니다.

Querier 활성화

OG-1100 시스템은 VLAN 별로 querier 를 동작시킬수 있습니다. VLAN 별로 IGMP Querier 를 활성화하고 조회하는 명령어는 다음과 같습니다.

명령어	설명	모드
ip igmp snooping querier vlan <vlan ID>	VLAN 의 IGMP querier 기능 활성화	Config
no ip igmp snooping querier vlan <vlan ID>	VLAN 의 IGMP querier 기능 비활성화	
show ip igmp snooping querier	IGMP Querier 조회	Enable

Query Interval 설정

OG-1100 시스템에서 IGMP Snooping Querier 의 IGMP Query 메시지 전송주기는 125000(ms)이 기본값을 설정되어 있습니다. 이값을 변경하기 위해서는 다음 명령어를 사용합니다.

명령어	설명	모드
ip igmp snooping query-interval <INTERVAL> vlan <vlan ID>	VLAN 의 Query 메시지 전송주기 설정	Config
no ip igmp snooping query-interval <INTERVAL> vlan <vlan ID>	VLAN 의 Query 메시지 전송주기를 기본값(125000 ms)로 설정	
show ip igmp snooping	Query 전송주기 조회	Enable

Max Response Time 설정

Max Response Time 은 호스트로 IGMP Query 메시지를 전송한 후 호스트로부터 응답 (IGMP Report 메시지)를 기다리는 시간입니다. 만약 Max Response Time 내 Report 메시지가 도착하지 않으면 Query 메시지가 전송된 포트에 해당 멀티캐스트 그룹의 멤버가 없는 것으로 간주합니다.

OG-1100 시스템의 Max Response Time 의 기본값은 10000(ms)로 설정되어 있습니다. 이 값을 변경하려면 config 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
ip igmp snooping max-response-time <INTERVAL> vlan <vlan ID>	해당 VLAN 의 max-response-time 값 변경	Config
no ip igmp snooping max-response-time <INTERVAL> vlan <vlan ID>	해당 VLAN 의 max-response-time 값을 기본값(1000ms)으로 설정	
show ip igmp max-response-time	Max-response-time 설정값 조회	Enable

다음은 IGMP Snooping Querier 의 Max-response-time 값을 2000(ms)로 설정하는 예입니다.

```
OG1100(config)#ip igmp snooping max-response-time 2000 vlan 10
OG1100(config)#end
OG1100#show ip igmp snooping max-response-time
VLAN 1
    IGMP Snooping max-response-time is 10000 ms
VLAN 10
    IGMP Snooping max-response-time is 2000 ms
VLAN 20
    IGMP Snooping max-response-time is 10000 ms
VLAN 4094
    IGMP Snooping max-response-time is 10000 ms
OG1100#
```

Other Querier Timeout 설정

OG-1100 시스템에서 IGMP snooping 의 Querier 가 동작하고 있을 때 다른 IGMP Querier 로부터 IGMP Query 메시지를 받으면 IGMP Querier 기능을 일단 중지합니다. 중지 후 일정시간 동안 Query 메시지를 받지 않으면 주변에 Querier 가 없는 것으로 간주하여 다시 Querier 기능을 시작하게 되는데, 이 기다리는 시간이 Other Querier Timeout 입니다.

OG-1100 시스템에서 Other Querier Timeout 값은 기본적으로 255000(ms)로 설정되어 있습니다. 이 값을 Config 모드에서 다음 명령어를 이용하여 변경할 수 있습니다.

명령어	설명	모드
ip igmp snooping other-querier-interval <INTERVAL> vlan <vlan ID> no igmp snooping other-querier-interval <INTERVAL> vlan <vlan ID>	해당 VLAN 의 other-querier-timeout 값 변경 해당 VLAN 의 other-querier-timeout 값을 기본값(255000ms)으로 설정	Config
show ip igmp snooping other-querier-interval	other-querier-timeout 설정값 조회	Enable

다음은 VLAN10 의 other-querier-timeout 값을 30000(ms)로 설정하는 예입니다.

```
OG1100(config)#ip igmp snooping other-querier-interval 300000 vlan 10
OG1100(config)#end
OG1100#show ip igmp snooping other-querier-interval
VLAN 1
    IGMP Snooping other-querier-interval is 255000 ms
VLAN 10
    IGMP Snooping other-querier-interval is 300000 ms
VLAN 20
    IGMP Snooping other-querier-interval is 255000 ms
VLAN 4094
    IGMP Snooping other-querier-interval is 255000 ms
OG1100#
```

3.4.1.5 멀티캐스트 트래픽 포워딩 정책 설정

OG-1100 시스템은 멀티캐스트 트래픽이 들어올 경우 해당 멀티캐스트 그룹의 멤버십 등록 여부에 따라(트래픽이 들어온 포트가 속하는) VLAN 내의 포트에 대해 트래픽을 어떤 식으로 처리할 것인지에 대한 정책을 설정할 수 있습니다.

OG-1100 시스템의 멀티캐스트 트래픽에 대한 기본정책(초기설정정책)은, 해당 멀티캐스트 그룹이 멤버십에 등록되어 있지 않으면(트래픽을 들어온 포트가 속하는) VLAN 내 모든 포트로 플러딩(flooding)하고 멤버십에 등록되어 있으면 멤버십에 등록되어 있는 포트만 포워딩(forwarding) 하도록(**multicast-flood-known**) 설정되어 있습니다. 이 외에, 멀티캐스트 그룹의 등록 여부와 관계없이 VLAN 내 모든 포트 플러딩 하는 정책(**multicast-flood-all**)과, 그룹에 등록되어 있으면 멤버인 포트만 포워딩(forwarding)하고 그룹에 등록되어 있지 않으면 트래픽을 드랍(drop)하도록 하는 정책(**multicast-flood-none**)을 설정할 수 있습니다.

각 VLAN 별 멀티캐스트 트래픽 처리 정책은 config 모드에서 다음 명령어를 사용하여 변경할 수 있습니다.

명령어	설명	모드
<code>multicast-filter mode {multicast-flood-none multicast-flood-all multicast-flood-known} vlan <vlan ID></code>	멀티캐스트 처리정책을 변경함 - Multicast-flood-none : L2MC 테이블에 등록된 group 에 해당 하는 multicast traffic 에 대해서는 해당 포트로 forwarding 을 하고 그 외의 multicast traffic 은 drop 시킨다. - Multicast-flood-all : multicast traffic 을 VLAN 내의 모든 포트로 flooding 합니다. - Multicast-flood-known : L2MC 테이블에 등록된 group 에 해당 하는 multicast traffic 에 대해서는 해당 포트로 forwarding 을 하고 그 외의 multicast traffic 은 VLAN 내의 모든 포트로 flooding 합니다.	Config
<code>Show multicast-filter</code>	설정된 multicasting 정책을 조회	Enable

다음은 VLAN 10 의 멀티캐스트 트래픽 처리 정책을 multicast-flood-none 으로 설정하는 예입니다.

```

OG1100(config)#multicast-filter mode multicast-flood-none vlan 10
OG1100(config)#end
OG1100#show multicast-filter

-----
VLAN      Multicast filtering Mode
-----
1         multicast-flood-unknown
10        multicast-flood-none
    
```

```

20      multicast-flood-unknown
4094    multicast-flood-unknown
-----
OG1100#
    
```

3.4.1.6 IGMP Snooping 정보 조회

IGMP Snooping 설정 정보 조회

OG-1100 시스템에서 IGMP snooping의 설정정보는 enable 모드에서 **show ip igmp snooping** 을 이용해서 조회할 수 있습니다.

명령어	설명	모드
Show ip igmp snooping [<i>vlan ID</i>]	시스템(혹은 VLAN) 의 igmp snooping 정보 확인 vlan ID : VLAN 번호	Enable

다음은 **show ip igmp snooping** 명령어를 사용하여 OG-1100 시스템의 IGMP snooping 설정 정보를 조회하는 예입니다.

```

OG1100#show ip igmp snooping
IGMP Snooping is globally enabled
IGMP Snooping Proxy is enabled
IGMP Snooping Proxy IP is 192.168.100.2
VLAN 1
    IGMP Snooping is disabled
VLAN 10
    IGMP Snooping is enabled
    IGMP Snooping querier enabled
    IGMP Snooping immediate-leave is enabled
    IGMP snooping query interval is 125000 ms
    IGMP snooping max query response time is 2000 ms
    IGMP Snooping last member query interval is 2000 ms
    IGMP snooping other querier timeout interval is 300000 ms
    IGMP snooping group membership interval is 300000 ms
    IGMP snooping vl router present timeout is 400000 ms
    IGMP snooping interface 1/2 version 2
    IGMP snooping interface 9/1 version 2
    IGMP snooping interface 9/2 version 2
    IGMP snooping interface 9/3 version 2
    IGMP snooping interface 9/4 version 2
VLAN 20
    IGMP Snooping is disabled
VLAN 4094
    IGMP Snooping is disabled
OG1100#
    
```

IGMP Snooping 포워딩 테이블 정보 조회

OG-1100 시스템에서 IGMP 를 통해 구성된 멤버십 정보는 다음 명령어를 통해 조회할 수 있습니다.

명령어	설명	모드
Show ip igmp snooping forwarding table	IGMP snooping 멤버십 테이블 정보조회	Enable

다음은 show ip igmp snooping forwarding 명령어를 사용하여 OG-1100 시스템의 IGMP snooping 멤버십 정보를 조회하는 예입니다.

```
OG1100#show ip igmp snooping forwarding table
```

VLAN	Group Address	Group MAC-Addr	Member-Ports (Aging time)
10	225.001.001.003	0100.5e01.0103	9/1 (210 sec)
	225.001.001.004	0100.5e01.0104	9/1 (210 sec)
	225.001.001.005	0100.5e01.0105	9/1 (211 sec)
	225.001.001.020	0100.5e01.0114	3/1 (static)

```
OG1100#
```

3.4.2 PIM-SM 설정 및 조회

PIM-SM 은 dynamic multicasting routing protocol 이며, 본 시스템에서 PIM-SM ver2 를 지원합니다. 먼저 'ip multicast-routing'이 실행되어 있어야 합니다. PIM 인터페이스는 L3 인터페이스별 생성할 수 있으며, L3 인터페이스가 down 일 경우에 자동적으로 PIM 인터페이스도 down 됩니다.

PIM 인터페이스는 생성하면 PIM 메시지인 hello 메시지를 주고 받게 되며, 각 router 의 역할인 DR, RP, BSR 로써의 역할을 수행하게 됩니다. PIM 인터페이스는 L3 INTERFACE_MODE 에서 설정하게 되며, DR/RP/BSR 에 대한 설정은 configure mode 에서 수행하게 됩니다.

3.4.2.1 PIM-SM 기능 활성화

IP Multicast-Routing 활성화

OG-1100 시스템에서 인터페이스의 PIM-SM 기능을 활성화 해주기 위해서는 IP multicast-routing 이 설정되어 있어야 합니다. ip multicast-routing 은 L3 multicast routing protocol 활성화를 위한 명령어으로써, OG-1100 시스템은 PIM-SM, IGMP protocol 을 위해서 선행적으로 수행하여야 합니다. 다만, L2 IGMP Snooping 설정을 위해서는 ip multicast-routing 은 비활성화 되어야 합니다.

OG-1100 시스템은 IP multicast-routing 을 지원하도록 초기설정이 되어 있지만, 이전에 L2 멀티캐스트인 IGMP Snooping 을 실행했었거나, 다른 이유로 IP multicast-routing 기능이 비활성화 되어있을 경우는 config 모드에서 다음과 같은 명령어를 사용해 활성화 해주어야 합니다.

명령어	설명	모드
ip multicast-routing	시스템을 L3 멀티캐스트 모드로 설정	Config
no ip multicast-routing	시스템을 L3 멀티캐스트 모드에서 해제	

다음은 시스템의 IP multicast-routing 을 활성화 하는 예입니다.

```
OG1100(config)#ip multicast-routing
OG1100(config)#end
OG1100#
```

PIM-SM 기능 활성화

OG-1100 시스템에서 PIM-SM 기능은 인터페이스 별로 활성화할 수 있습니다. 호스트가 연결되어 있는 인터페이스의 경우, PIM-SM passive 모드로 설정하면 hello 메시지등의 무의미한 패킷의 전송을 막을 수 있습니다.

OG-1100 시스템에서 인터페이스 별 PIM-SM 활성화는 인터페이스 모드에서 다음 명령어를 사용하여 설정할 수 있습니다.

명령어	설명	모드
ip pim-sparse [passive]	Pim 인터페이스 설정 - Passive : passive mode 로 설정 (이경우 hello 메시지 보내지 않음)	Config-interface
no ip pim-sparse	Pim 인터페이스 해지	
show ip pim sparse-mode interface [detail]	설정된 pim 인터페이스 조회	Enable



참고

인터페이스의 PIM-SM 기능이 활성화 되기 위해서는 해당 인터페이스의 operation status 가 'up' 상태이어야 합니다. L3 인터페이스의 status 는 enable 모드에서 **show ip interface brief** 명령어를 통해 확인할 수 있습니다.

다음은 인터페이스 VLAN10 의 PIM-SM 을 활성화시키는 예입니다.

```
OG1100(config)# interface vlan10
OG1100(config-if)#ip pim sparse-mode
OG1100(config)#end
OG1100# show ip pim sparse-mode interface
```

Address	Interface	VIFindex	Ver/	Nbr	DR	DR	
		Mode		Count	Prior		
10.1.1.1	vlan10	0		v2/S	1	1	10.1.1.1

```
OG1100#
```


3.4.2.2 Hello 메시지 전송주기/Holdtime 설정

PIM-SM 라우터는 Hello 메시지를 다른 PIM 라우터(PIM neighbor)로 전송함으로써 자신의 존재를 알리고 PIM neighbor와의 관계를 유지합니다.

Hello 메시지 전송주기 설정

OG-1100 시스템에서 기본적으로 설정되어 있는 Hello 메시지의 전송주기(Hello-interval)은 30 초이며, 이 값을 변경하고자 할 때에는 인터페이스 모드에서 다음 명령어를 사용합니다.

명령어	설명	모드
<code>ip pim hello-interval <INTERVAL></code>	인터페이스의 Hello 메시지 전송주기 설정 INTERVAL : 전송주기(초)	Config-interface
<code>no ip pim hello-interval <INTERVAL></code>	인터페이스의 Hello 메시지 전송주기를 기본값으로 설정	

현재 설정되어 있는 Hello interval은 enable 모드에서 `show ip pim sparse-mode detail` 명령으로 확인할 수 있습니다.

다음은 인터페이스 VLAN10의 Hello 메시지 전송주기를 60 초 변경하는 예입니다.

```
OG1100(config)#interface vlan10
OG1100(config-if)#ip pim hello-interval 60
OG1100(config-if)#end
OG1100#show ip pim sparse-mode interface detail
vlan10 (vif 2): Passive mode
  Address 10.10.10.1, DR 10.10.10.1
  Hello period 60 seconds
  Triggered Hello period 5 seconds
  Neighbors:

vlan20 (vif 0): Passive mode
  Address 10.10.100.1, DR 10.10.100.1
  Hello period 30 seconds
  Triggered Hello period 5 seconds
  Neighbors:
OG1100#
```

Hello 메시지 Hold Time 설정

Hello Hold Time은 Hello 메시지의 유효시간을 말하며, OG-1100에서는 105 초가 기본값으로 설정되어 있습니다. 이값은 인터페이스 모드에서 다음 명령어를 사용하여 변경할 수 있습니다.

명령어	설명	모드
ip pim hello-holdtime <TIME>	인터페이스 Hello 메시지의 유효시간 설정 <Time> Hello 메시지 유효시간(초)	Config-interface
no ip pim hello-holdtime	인터페이스 Hello 메시지의 유효시간 을 기본값으로 설정	

현재 설정되어 있는 Hello interval 은 enable 모드에서 **show ip pim sparse-mode detail** 명령으로 확인할 수 있습니다

다음은 인터페이스 VLAN10 의 Hello Holdtime 을 200 초로 변경하는 예입니다

```
OG1100(config)#interface vlan10
OG1100(config-if)#ip pim hello-holdtime 200
```

3.4.2.3 Join/Prune 메시지 전송주기 설정

Join 메시지는 상위 PIM 라우터에게 해당 그룹의 멀티캐스트 트래픽을 전송해 줄것을 요청하는 메시지 이고, Prune 메시지는 상위 PIM 라우터에게 해당 그룹의 트래픽 전송을 중지하도록 요청하는 메시지 입니다.

OG-1100 시스템에서 Join/Prune 메시지의 전송주기는 기본적으로 60 초로 설정되어 있습니다. 이 주기의 변경을 원하면 config 모드에서 다음 명령어를 사용합니다.

명령어	설명	모드
ip pim jp-timer <INTERVAL>	인터페이스의 Join/Prune 전송주기 설정 < INTERVAL> 전송주기(초)	Config
no ip pim jp-timer	인터페이스의 Join/Prune 전송주기를 기본값으로 설정	

다음은 인터페이스 VLAN20 의 Join/Prune 메시지의 주기를 120 초로 변경하는 예입니다.

```
OG1100(config)#ip pim jp-timer 120
OG1100(config)#end
OG1100#
```

3.4.2.4 Candidate BSR 설정

BSR(Bootstrap Router)는 RP(Rendezvous Point)의 정보를 도메인 내의 다른 라우터로 전송하는 역할을 합니다. BSR 은 각 PIM-SM 도메인에 하나만이 동작할 수 있기 때문에 여러 candidate BSR 중에서 우선순위와 IP 어드레스를 토대로 자동으로 선택됩니다.

OG-1100 시스템을 candidate BSR 로 설정하기 위해서는 config 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
ip pim bsr-candidate <IFNAME> <HASH> <PRIORITY> no ip pim bsr-candidate <IFNAME> <HASH> <PRIORITY>	해당 인터페이스를 candidate BSR 로 설정. <IFNAME> 인터페이스 이름 <HASH> Hash 값 <PRIORITY> 우선순위 해당 인터페이스의 candidate BSR 설 정을 해제합니다.	Config
show ip pim sparse-mode bsr-router	BSR 정보 확인	Enable

다음은 인터페이스 VLAN20 을 Hash mask length 30, priority 100 인 candidate BSR 로 지정하는 예입니다

```

OG1100(config)#ip pim bsr-candidate vlan20 30 200
OG1100(config)#end
OG1100#show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 10.10.100.1
  Uptime   : 00:00:06, BSR Priority: 200, Hash mask length: 30
  Expires  : 00:02:04
  Role     : Candidate BSR
  State    : Pending BSR
OG1100#
    
```

3.4.2.5 Candidate RP 설정

멀티캐스트 라우터가 candidate RP 로 설정되면 candidate RP 메시지를 BSR 로 전송합니다. BSR 은 candidate RP 들로부터 수신된 candidate RP 메시지의 내용(라우터의 IP 어드레스 와 priority)를 참고로 RP 를 선출합니다.

OG-1100 시스템을 candidate RP 로 지정하기 위해서는 config 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
ip pim rp-candidate <IFNAME> priority <PRIORITY> [interval <INTERVAL> group- list <LIST>] no ip pim rp-candidate <IFNAME>	해당 인터페이스를 candidate RP 로 설정 <IFNAME> <PRIORITY> <INTERVAL> <LIST> 해당 인터페이스의 candidate RP 설정 해제	Config
show ip pim sparse-mode -rp mapping	RP 설정정보 확인	Enable

다음은 인터페이스 VLAN20 을 priority 255 인 candidate RP 로 설정한 후 조회하는 예입니다.

```
OG1100(config)#ip pim rp-candidate vlan20 priority 255
OG1100#show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 10.10.100.1
    Info source: 10.10.100.1, via bootstrap, priority 255
    Uptime: 00:00:13, expires: 00:02:17
Group(s): 224.0.0.0/4, Static
  RP: 10.10.100.1
    Uptime: 01w00d08h
OG1100#
```

3.4.2.6 Static RP 설정

일반적인 경우, RP 는 Candidate RP 의 IP 어드레스와 Priority 를 토대로 candidate RP 중 에서 자동으로 선출됩니다. 하지만 비교적 작고 복잡하지 않은 네트워크의 경우는 직접 RP 를 지정하는 것이 효율적입니다.

OG-1100 시스템에서 특정 인터페이스를 RP 로 지정하기 위해서는 config 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
ip pim rp – address A.B.C.D	A.B.C.D RP 어드레스 로 설정	Config
no ip pim rp – address A.B.C.D	설정된 RP 어드레스 A.B.C.D 해제	
show ip pim sparse-mode –rp mapping	RP 설정정보 확인	Enable

다음은 IP 어드레스 가 10.10.100.2 인 인터페이스를 RP 로 지정하는 하는 예입니다.

```
OG1100(config)#ip pim rp-address 10.10.100.2
OG1100(config)#end
OG1100#show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4, Static
  RP: 10.10.100.2
    Uptime: 00:00:56
  RP: 10.10.100.1
    Uptime: 01w00d08h
OG1100#
```

3.4.2.7 RP Reachability 검사 여부 설정 (register-rp-reachability)

DR 에서 PIM register processing 을 위해 RP reachability 를 check 할 것인지를 설정합니다. OG-1100 시스템은 기본적으로 RP reachability 검사를 수행하지 않도록 설정되어 있습니다.

RP reachability 검사를 수행하려면 config 모드에서 다음 명령어를 실행합니다

명령어	설명	모드
ip pim register-rp-reachability	PIM register 의 RP Reachability 검사하도록 설정	Config
no ip pim register-rp-reachability	PIM register 의 RP Reachability 검사하지 않도록 설정	

다음은 OG-1100 시스템에서 PIM Register 의 RP reachability 를 체크하도록 설정하는 예입니다.

```
OG1100(config)#ip pim register-rp-reachability
OG1100(config)#end
OG1100#
```

3.4.2.8 RP register-kat 설정

O1100 의 RP Register KAT 값을 설정하려면 다음 명령어를 사용합니다.

명령어	설명	모드
ip pim rp-register-kat <TIME>	시스템의 RP Register KAT 값 설정	Config
no ip pim rp-register-kat	TIME : KAT Time(초) RP Register KAT 값을 기본값으로 설정	

다음은 OG-1100 시스템에서 RP register KAT 값을 변경하는 예입니다.

```
OG1100(config)#ip pim rp-register-kat 100
OG1100(config)#
```

3.4.2.9 STP Threshold 설정

해당 group list 에 대해 last-hop PIM router 가 SPT 로 전환되도록 할것인지를 설정합니다. OG-1100 시스템은 기본적으로 STP 로 전환되도록 설정 되어 있습니다.

명령어	설명	모드
ip pim spt-threshold [group-list]	Group list 에 대해 STP 로 전환되도록 설정	Config
no ip pim spt-threshold [group-list]	group-list : Multicast Group List Group list STP 로 전환되지 않도록 설정	

다음은 STP 로 전환될수 있도록 한 기본설정에서 RTP 를 유지하도록 변경하는 예입니다

```
OG1100(config)#no ip pim spt-threshold
OG1100(config)#end
OG1100#
```

3.4.2.10 DR 우선순위 설정

여러 라우터들이 연결되어 있는 multi-access network 의 경우, 이중 하나의 라우터가 일정 시간동안 Join/Prune 메시지를 전송하는 DR(Designated Router)로 동작해야 합니다. DR 을 선택하기 위해 네트워크의 각 PIM 라우터는 수신한 hello 메시지의 IP 어드레스를 검사해서 네트워크 환경들이 수신한 Hello 메시지와 비교합니다. 비교 결과 가장 높은 Priority 를 가지는 라우터가 DR 로 선정되고, Priority 가 동일하면 최상위 어드레스를 가진 라우터가 DR 이 됩니다.

이렇게 정해진 DR 로부터 지정된 시간동안 Hello 메시지를 받을 수 없다면 같은 방식에 의해 다른 라우터가 다시 DR 로 선정됩니다.

OG-1100 시스템에서 DR 의 우선순위는 0 이 기본값으로 설정되어 있습니다. 이 우선순위는 인터페이스 모드에서 다음 명령어를 통해 변경할 수 있습니다.

명령어	설명	모드
ip pim rp-priority <PRIORITY> no ip pim rp-priority	인터페이스의 DR Priority 를 설정 - PRIORITY : 우선순위 값 설정된 DR Priority 를 기본값(1)으로 설정	Config

현재 설정되어 있는 Hello interval 은 enable 모드에서 **show ip pim interface** 명령으로 확인할 수 있습니다.

다음은 OG-1100 시스템에서 인터페이스 VLAN20 의 DR Priority 를 255 로 변경하는 예입니다

```
OG1100(config)#interface vlan20
OG1100(config-if)#ip pim dr-priority 255
OG1100(config-if)#end
OG1100#show ip pim sparse-mode interface
Address          Interface VIFindex Ver/  Nbr    DR    DR
                  Mode     Count  Prior
10.10.10.1       vlan10   2      v2/S   0      1     10.10.10.1
10.10.100.1      vlan20   0      v2/S   0      255  10.10.100.1
OG1100#
```

3.4.2.11 Cisco 라우터와 호환을 위한 설정

OG-1100 시스템은 RFC 2362 에 정의 되어 있는 PIM-SM version 2 프로토콜을 지원합니다.

만약 RFC 2362 를 지원하지 않는 Cisco 라우터와 OG-1100 시스템을 연동하려면, 다음과 같은 기능에 대해 설정을 해야 합니다.

Register Checksum 계산 설정

Cisco 라우터에 맞도록 PIM 헤더와 register 메시지의 데이터 부분에 대해 checksum 을 계산하도록 설정합니다.

OG-1100 시스템은 기본적으로 Cisco 라우터를 위한 checksum 을 계산하지 않도록 설정되어 있습니다. 계산하도록 설정하려면 config 모드에서 다음 명령어를 사용합니다.

명령어	설명	모드
ip pim cisco-register-checksum [group-list <LIST>] no ip pim cisco-register-checksum [group-list <LIST>]	(특정한 group-list 에 대해) Checksum 계산 설정 LIST : Access list 번호	Config

다음은 시템을 Cisco 라우터를 위한 checksum 을 계산하도록 설정하는 예입니다.

```
OG1100(config)#ip pim cisco-register-checksum
OG1100(config)#end
OG1100#
```

프리픽스 (prefix)가 0 이 아닌 Candidate RP 메시지 전송 설정

RFC 2362 를 지원하지 않는 Cisco PIM-SM BSR 은 그룹 프리픽스 번호가 0 인 candidate RP 를 허용하지 않습니다. 따라서 Cisco 라우터와 호환을 위해서는 그룹 프리픽스가 0 이 아닌 Candidate RP 메시지를 전송하도록 설정해야 합니다.

OG-1100 시스템은 기본적으로 프리픽스가 0 인 Candidate RP 메시지도 전송되도록 되어 있습니다. 프리픽스가 0 이 아닌 CRP 메시지 전송을 설정하려면 config 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
ip pim crp-cisco-prefix no ip pim crp-cisco-prefix	프리픽스가 0 인 CRP 메시지를 전송하도록 설정	Config

다음은 OG-1100 시스템에서 0 이 아닌 Candidate RP 메시지를 전송하도록 설정하는 예입니다.

```
OG1100(config)#ip pim crp-cisco-prefix
OG1100(config)#end
OG1100#
```

Hash 를 이용한 RP 선정방식 설정

Candidate RP 에 지정된 우선순위 대신 hash 방식을 사용하여 RP 를 선정하도록 설정합니다.

명령어	설명	모드
ip pim ignore-rp-set-priority	Hash 방식의 RP 선정방법 설정	Config
no ip pim ignore-rp-set-priority	Hash 방식의 RP 선정방법 설정 해지	

다음은 OG-1100 시스템에서 hash 방식을 사용하여 RP 를 선정하도록 설정하는 예입니다.

```
OG1100(config)#ip pim ignore-rp-set-priority
OG1100(config)#end
OG1100#
```

GenID (Generation ID) 필드 제외 설정

Cisco ISO 버전의 라우터와 호환을 위해 Hello 메시지에서 Generation ID(GenID) 필드를 제외하고 전송하도록 설정합니다.

명령어	설명	모드
ip pim exclude-genid	Hello 메시지에서 GenID 옵션을 제외하도록 설정	Config
no ip pim exclude-genid	Hello 메시지에서 GenID 옵션을 포함하도록 설정	

다음은 Hello 메시지에서 Generation ID 필드를 제외하고 전송하도록 기본설정을 변경하는 예입니다.

```
OG1100(config)#ip pim exclude-genid
OG1100(config)#end
OG1100#
```

3.4.2.12 PIM-SM 정보 조회

멀티캐스트 라우팅 정보 조회

OG-1100 시스템에서 멀티캐스트 라우팅 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
show ip mrouter	멀티캐스트 라우팅 정보 조회	enable

다음은 OG-1100 시스템에서 **show ip mroute** 명령어를 수행하는 예입니다.

```

OG1100#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.10.30, 225.1.1.1), uptime 00:03:36, stat expires 00:01:50
Owner PIM-SM, Flags: TF
  Incoming interface: vlan10
  Outgoing interface list:
    vlan20 (1)
    Register (1)

(10.10.10.30, 225.1.1.2), uptime 00:03:36, stat expires 00:01:50
Owner PIM-SM, Flags: TF
  Incoming interface: vlan10
  Outgoing interface list:
    Register (1)

(10.10.10.30, 225.1.1.3), uptime 00:03:36, stat expires 00:01:50
Owner PIM-SM, Flags: TF
  Incoming interface: vlan10
  Outgoing interface list:
    vlan20 (1)
    Register (1)

OG1100#

```

PIM-SM 멀티캐스트 라우팅 정보 조회

OG-1100 시스템에서 PIM-SM 라우팅 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
show ip pim sparse-mode mroute	PIM SM 라우팅 정보 조회	Enable

다음은 OG-1100 시스템에서 **show ip pim sparse-mode mrouter** 명령어를 사용하여 멀티캐스트 라우트 정보를 조회하는 예입니다.

```

OG1100#show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 255
(S,G) Entries: 255
(S,G,rpt) Entries: 255
FCR Entries: 0

```

```
(10.10.10.30, 225.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
Local .....
Joined .j.....
Asserted .....
Outgoing .o.....

(10.10.10.30, 225.1.1.2)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
Local .....
Joined .j.....
Asserted .....
Outgoing .o.....
```

인터페이스의 PIM-SM 설정정보 조회

OG-1100 시스템에서 PIM-SM 라우팅 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
<code>show ip pim sparse-mode interface [detail]</code>	PIM SM 인터페이스 조회	enable

다음은 OG-1100 시스템에서 `show ip pim sparse-mode interface` 명령어를 사용하여 PIM 인터페이스의 정보를 조회하는 예입니다.

```
OG1100#show ip pim sparse-mode interface
Address          Interface VIFindex Ver/  Nbr  DR    DR
                  Mode  Count Prior
10.10.10.1      vlan10   2      v2/S  0     1    10.10.10.1
10.10.100.1     vlan20   0      v2/S  0    255  10.10.100.1
OG1100#show ip pim sparse-mode interface ?
  detail Detailed interface information
  |      Output modifiers
  <cr>

OG1100#show ip pim sparse-mode interface detail
vlan10 (vif 2): Passive mode
  Address 10.10.10.1, DR 10.10.10.1
  Hello period 60 seconds
  Triggered Hello period 5 seconds
  Neighbors:
vlan20 (vif 0): Passive mode
  Address 10.10.100.1, DR 10.10.100.1
  Hello period 30 seconds
  Triggered Hello period 5 seconds
  Neighbors:

OG1100#
```

PIM-SM RP 정보 조회

OG-1100 시스템에서 RP 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
show ip pim sparse-mode rp-mapping	RP 정보 조회	Enable

다음은 show ip pim sparse-mode rp-mapping 명령어를 사용하여 OG-1100 시스템의 RP 정보를 조회하는 예입니다.

```
OG1100#show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4, Static
  RP: 10.10.100.2
      Uptime: 14:58:57
  RP: 10.10.100.1
      Uptime: 01w00d23h
OG1100#
```

PIM-SM Neighbor 정보 조회

OG-1100 시스템에서 PIM-SM Neighbor 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
show ip pim sparse-mode neighbor [detail]	PIM-SM Neighbor 정보 조회	enable

다음은 show ip pim sparse-mode neighbor detail 명령어를 사용하여 OG-1100 시스템의 RP 정보를 조회하는 예입니다.

```
OG1100#show ip pim sparse-mode neighbor
OG1100#show ip pim sparse-mode neighbor detail
```

PIM-SM BSR (Bootstrap Router) 정보 조회

OG-1100 시스템에서 BSR 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
show ip pim sparse-mode bsr-router	PIM-SM BSR 정보 조회	enable

다음은 `show ip pim sparse-mode bsr-router` 명령어를 사용하여 BSR 정보를 조회하는 예입니다.

```
OG1100#show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 10.10.100.1
  Uptime:      01d17h59m, BSR Priority: 10, Hash mask length: 2
  Next bootstrap message in 00:00:26
  Role: Candidate BSR
  State: Elected BSR
```

PIM-SM Next Hop 정보 조회

OG-1100 시스템에서 Next Hop 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
<code>show ip pim sparse-mode next-hop</code>	PIM-SM Next Hop 정보 조회	enable

다음은 `show ip pim sparse-mode neighbor detail` 명령어를 사용하여 OG-1100 시스템의 RP 정보를 조회하는 예입니다.

```
OG1100# show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination   Type  Nexthop  Nexthop  Nexthop  Nexthop Metric Pref
Refcnt
              Num   Addr     Ifindex   Name
-----
100.1.1.1     .R..  1        100.1.2.1  32        0         1    100
100.1.1.11    ..S.  1        100.1.2.1  32        0         1    100
100.1.2.10    .R..  1        0.0.0.0   32        0         0    105
OG1100#
```

PIM-SM RP Hash 정보 조회

OG-1100 시스템에서 특정 그룹에 대한 RP Hash 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
<code>show ip pim sparse-mode rp-hash <A.B.C.D></code>	그룹 A.B.C.D의 RP Hash 정보 조회	enable

다음은 OG-1100 시스템에서 그룹 225.1.1.1 의 RP Hash 정보를 조회하는 예입니다.

```
OG1100#show ip pim sparse-mode rp-hash 224.1.1.30
RP: 10.10.10.1
Info source: 20.20.20.1, via bootstrap
```

3.4.3 IGMP 설정 및 조회

OG-1100 시스템은 해당 인터페이스에 PIM-SM 이 설정되면 추가적인 구성작업 필요 없이 IGMP 가 동작하도록 설정되어 있습니다. 시스템 전체 또는 특정 인터페이스의 IGMP 설정 정보는 다음 명령어를 통해 확인할 수 있습니다.

명령어	설명	모드
<code>show ip igmp interface {IFNAME}</code>	설정된 전체 igmp 및 개별인터페이스 조회	Enable

OG-1100 시스템에서는 필요한 경우 기본설정된 다음의 IGMP 설정값들을 변경할 수 있습니다.

- Access 멀티캐스트 그룹 지정
- IGMP Querier 설정
- Querier Timeout 값 변경
- Max Response Time 변경
- Last Member Query Interval 변경
- Last Member Query Count 변경
- Robustness Variable 값 변경

3.4.3.1 IGMP Query 메시지 전송주기 설정

인터페이스에 IGMP Querier 가 활성화 되면, Querier 는 인터페이스에 연결되어 있는 호스트에 주기적으로 Query 메시지를 전송합니다. 호스트들은 이 Query 메시지에 대해 자신이 가입되어 있는 멀티캐스트 그룹을 Report 하고, Querier 는 이를 토대로 해당 인터페이스의 멀티캐스트 그룹 멤버십을 관리하게 됩니다.

OG-1100 시스템에서는 특정 인터페이스에 PIM 기능을 활성화 하면 자동으로 IGMP Querier 가 동작하도록 되어있고 이때 Query 메시지를 보내는 주기는 125 초로 설정되어 있습니다. Query 전송주기는 인터페이스 모드에서 다음 명령어를 입력함으로써 변경할 수 있습니다.

명령어	설명	모드
<code>ip igmp query-interval <INTERVAL></code>	IGMP Query 메시지 전송주기 설정 <INTERVAL> 메시지 전송주기	Interface
<code>no ip igmp query-interval</code>	IGMP Query 메시지 전송주기를 초기값 (125 초)로 설정 I	

현재 설정되어 있는 Query Interval 은 enable 모드에서 `show ip igmp interface` 명령으로 확인할 수 있습니다.

다음은 인터페이스 VLAN20 의 Query Interval 을 200 초로 변경하는 예입니다.

```
OG1100(config)#interface vlan20
OG1100(config-if)#ip igmp query-interval 200
OG1100(config-if)#end
```


```
OG1100#show ip igmp interface vlan20
Interface vlan20 (Index 32)
IGMP Enabled, Active, Querier, Default version 2
Internet address is 10.10.100.1
IGMP query interval is 200 seconds
IGMP querier timeout is 405 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 410 seconds
OG1100#
```

3.4.3.2 Query Max Response Time 설정

Max Response Time 은 Query 메시지를 전송한 후 호스트로부터 Report 메시지를 기다리는 시간으로, 이 시간(Max Response Time) 내 호스트로부터 응답(IGMP Report)가 없으면 해당 인터페이스에 특정 멀티캐스트 그룹의 멤버가 없는 것으로 간주합니다.

OG-1100 시스템은 Max Response TIME 이 10 초로 설정되어 있고, 이 값을 변경하기 위해서는 인터페이스 모드에서 다음 명령어를 실행 합니다.

명령어	설명	모드
<code>ip igmp query-max-response-time <TIME></code>	인터페이스의 max response time 설정	Interface
<code>no ip igmp query-max-response-time</code>	<TIME> max-response-time 값(초) 인터페이스의 max response time 을 초기값으로 설정	



현재 설정되어 있는 Query Interval 은 enable 모드에서 **show ip igmp interface** 명령으로 확인할 수 있습니다.

참고

다음은 인터페이스 VLAN20 의 Query Max Response Time 을 15 초로 변경하는 예입니다.

```
OG1100(config)#interface vlan20
OG1100(config-if)#ip igmp query-max-response-time 15
OG1100(config-if)#end
OG1100#show ip igmp interface vlan20
Interface vlan20 (Index 32)
IGMP Enabled, Active, Querier, Default version 2
Internet address is 10.10.100.1
IGMP query interval is 200 seconds
IGMP querier timeout is 407 seconds
IGMP max query response time is 15 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 265 seconds
OG1100#
```

3.4.3.3 Querier Timeout 설정

하나의 LAN 에 여러 개의 IGMP 시스템이 있더라도 IGMP Querier 는 하나만 존재합니다. 만약 querier 가 어떤 이유에서든 동작하지 않으면 다른 non-Querier 중 IP 어드레스가 가장 낮은 시스템이 Querier 로 동작해야 하는데 이때 non-Querier 였다가 Querier 로 동작하는 시점을 Querier Timeout 값을 통해 결정합니다. 즉 Non-Querier 는 Query 메시지를 받은 후 Querier Timeout 동안 기다려도 Query 메시지를 수신하지 못하면 자신이 Querier 로 동작하게 됩니다.

OG-1100 시스템은 기본적으로 Querier Timeout 이 255 초로 설정되어 있습니다. 이 값을 변경하기 위해서는 인터페이스 모드에서 다음 명령어를 실행 합니다.

명령어	설명	모드
ip igmp querier-timeout <TIME>	인터페이스의 querier-timeout 값 설정 <TIME> querier-timeout 값(초)	Interface
no ip igmp querier-timeout	인터페이스의 querier-timeout 을 초기값으로 설정	

현재 설정되어 있는 Query Timeout 은 enable 모드에서 **show ip igmp interface** 명령으로 확인할 수 있습니다.

다음은 인터페이스 VLAN20 의 Query Timeout 을 300 초로 변경하는 예입니다

```
OG1100(config)#interface vlan20
OG1100(config-if)#ip igmp querier-timeout 300
OG1100(config-if)#end
OG1100#show ip igmp interface vlan20
Interface vlan20 (Index 32)
  IGMP Enabled, Active, Querier, Default version 2
  Internet address is 10.10.100.1
  IGMP query interval is 200 seconds
  IGMP querier timeout is 300 seconds
  IGMP max query response time is 15 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 415 seconds
OG1100#
```

3.4.3.4 Last Member Query Interval 및 count 설정

멀티캐스트 라우터가 호스트로부터 특정 그룹에 대한 IGMP Leave 메시지를 수신했을때, 멀티캐스트 라우터는 Leave 메시지를 받은 인터페이스에 그 특정 그룹에 가입된 호스트가 남아 있는지 확인하기 위해 Specific Query 를 해당 인터페이스의 호스트들에게 전송합니다. 이 때 호스트로부터 응답(Report 메시지)을 받지 못하면 더 이상 그 그룹에 가입된 호스트 없다고 판단해서 그룹을 해당 인터페이스에서 삭제합니다. 이 때, specific query 메시지를 전송한 후, 응답을 기다리는 시간이 Last Member Query Interval 입니다.

OG-1100 시스템은 기본적으로 2 번의 Specific Query 를 보내서 응답이 없을경우, 즉 last-member query interval 이 2 번 지나간 시간 만큼 기다려서 멀티캐스트 그룹에 대한 멤버가 있는지 확인을 합니다.

OG-1100 시스템의 last member query interval 기본값은 1 초, last member query count 의 기본값은 2 로 설정되어 있습니다. 이 값을 변경하기 위해서는 인터페이스 모드에서 다음 명령어를 실행 합니다.

명령어	설명	모드
ip igmp last-member-query-interval <INTERVAL>	인터페이스의 last member query interval 값 설정	Interface
ip igmp last-member-query-count <COUNT>	querier-timeout 값 설정 - <INTERVAL> last member query interval(ms)	
no ip igmp last-member-query-interval <INTERVAL>	인터페이스의 last member query count 값 설정	
no ip igmp last-member-query-count <COUNT>	- <COUNT> last member query count 인터페이스의 last member query interval 을 초기값으로 설정 인터페이스의 last member query count 를 초기값으로 설정	

현재 설정되어 있는 Last member Query Interval 및 last mameber query count 값은 enable 모드에서 **show ip igmp interface** 명령으로 확인할 수 있습니다.

다음은 인터페이스 VLAN20 의 Last Member Query Interval 은 2 초, last member query count 는 3 으로 변경하는 예입니다.

```

OG1100(config)#interface vlan10
OG1100(config-if)#ip igmp last-member-query-interval 2000
OG1100(config-if)#ip igmp last-member-query-count 3
OG1100(config-if)#end
OG1100#show ip igmp interface vlan20
Interface vlan20 (Index 32)
IGMP Enabled, Active, Querier, Default version 2
Internet address is 10.10.100.1
IGMP query interval is 125 seconds
IGMP querier timeout is 300 seconds
IGMP max query response time is 15 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 265 seconds
OG1100#
    
```

3.4.3.5 Immediate Leave 설정

OG-1100 시스템에서 Immeidate leave 기능을 활성화 하면, 호스트로부터 특정 그룹에 대한 IGMP Leave 메시지를 수신했을때, Leave 메시지를 받은 인터페이스에 그 특정 그룹에 가입된 호스트가 남아 있는지에 대한 확인작업 없이 바로 해당 그룹을 삭제합니다.

OG-1100 시스템은 기본적으로 immediate leave 기능 작동되지 않도록 되어 있습니다. immediate leave 기능을 동작시키기 위해서는 인터페이스 모드에서 다음 명령어를 실행 합니다.

명령어	설명	모드
ip igmp immediate-leave group-list <LIST> no ip igmp immediate-leave group <LIST>	해당 group list에 대해 immediate leave 기능 적용 해당 group list에 대해 immediate leave 기능 해제	Interface

다음은 인터페이스 Access-list 10에 대해서 VLAN10의 immediate leave 기능을 동작시키는 예입니다.

```
OG1100(config)#interface vlan10
OG1100(config-if)#ip igmp immediate-leave group-list 10
```

3.4.3.6 IGMP 정보 조회

IGMP 인터페이스 설정정보 조회

OG-1100 시스템에서 인터페이스의 IGMP 인터페이스 설정 정보를 조회하려면 enable 모드에서 다음 명령어를 실행합니다.

명령어	설명	모드
show ip igmp interface [IFNAME]	인터페이스의 IGMP 설정정보 조회 [IFNAME] 인터페이스 이름	enable

다음은 **show ip igmp interface** 명령어를 사용하여 OG-1100 시스템의 IGMP 설정 정보를 조회하는 예입니다.

```
OG1100#show ip igmp interface
Interface vlan10 (Index 31)
  IGMP Enabled, Active, Querier, Default version 2
  Internet address is 10.10.10.1
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 2000 milliseconds
  Group Membership interval is 260 seconds
Interface vlan20 (Index 32)
  IGMP Enabled, Active, Querier, Default version 2
  Internet address is 10.10.100.1
  IGMP query interval is 200 seconds
  IGMP querier timeout is 300 seconds
  IGMP max query response time is 15 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 265 seconds
OG1100#
```

IGMP 멤버십 정보 조회

OG-1100 시스템에서 IGMP 를 통해 구성된 멤버십 정보는 다음 명령어를 통해 조회할 수 있습니다.

명령어	설명	모드
show ip igmp group [/IFNAME]	Join/leave 된 group 를 조회 IFNAME : 인터페이스 이름	Enable

다음은 show ip igmp group 명령어를 사용하여 OG-1100 시스템의 IGMP 멤버십 정보를 조회하는 예입니다.

```
OG1100#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
225.10.1.1         vlan10            02:46:02 00:03:29 10.1.1.2
225.10.1.2         vlan10            02:45:58 00:03:23 10.1.1.3
225.10.1.3         vlan10            02:46:04 00:03:20 10.1.1.4
OG1100#
```

3.4.4 Static Join Group 설정 및 조회

PIM-SM network 에서는 host 단에서의 join/leave message 를 전달받아 SPT/RPT 의 경로를 따라 multicast traffic 을 전송하게 됩니다. mulitcast application 에 따라서는 이러한 경로 설정을 위한 지연시간이 매우 중요한 요소로 작용되는 것이 있습니다. 따라서, OG-1100 에서는 특정 pim router 까지 해당 multicast group traffic 을 미리 전송하도록 설정하는 기능을 가지고 있습니다. 이렇게 함으로써 PIM router 간의 전송 지연시간을 최소화하거나 인위적인 traffic 전송 경로를 설정 가능하게 됩니다.

OG-1100 에서는 PIM router 간의 join latency 를 줄이기 위하여 igmp static-join group 을 사용할 수 있습니다. Static-join group 으로 설정된 multicast group 은 mroute 에 해당하는 PIM interface 로 join 신호를 지속적으로 static 하게 내보내서 multicast traffic 이 OG1100 까지 내려오도록 하는 것이다. Host 단의 join/leave 에 의해서 multicast traffic 이 ONT 쪽으로 traffic 이 forwarding 되며, 해당하는 전 group 에 대해서 ONT 에서 leave 를 보내더라도 mroute 의 path 에는 변함이 없이 OG-1100 의 mroute PIM interface 까지 multicast traffic 이 내려와 있습니다.

3.4.3.1 IGMP static-join group 설정

OG-1100 시스템에서 igmp static-join group 을 설정하는 명령은 다음과 같습니다.

명령어	설명	모드
ip igmp static-join group [WORD]	Static-join group 설정 WORD : static-access list 의 이름	Config

먼저, static join 을 할 multicast group 을 access-list 을 이용하여 구성한다.
이 때, access-list 는 공인된 숫자가 아닌 word 인 subnet base 로 생성한다.

```
OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#access-list static_1 permit 225.10.1.11/32
OG1100(config)#ip igmp static-group-join static_1
OG1100(config)#
```

3.4.3.2 IGMP static-join group 조회

Static-join group 을 설정한 것을 확인하는 것은 이전 멀티캐스팅 라우팅 정보 조회인 mroute 를 조회하면 알 수 있습니다.

Static-join group 으로 설정된 것은 flag 상에서 ‘ s ’ 라고 표시를 하였으므로 알 수 있습니다.

```
OG1100#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, S
- STATIC Group Join
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(104.1.1.2, 225.10.1.11), uptime 02:37:36, stat expires 00:03:08
Owner PIM-SM, Flags: TFS (S가 static join group 표시)
  Incoming interface: vlan400
  Outgoing interface list:
```

3.5 DHCP 환경 설정

DHCP(Dynamic Host Configuration Protocol)는 네트워크 관리자들이 조직 내의 네트워크 상에서 IP 어드레스를 중앙에서 관리하고 할당해줄 수 있도록 해주는 프로토콜입니다. DHCP 와 관련된 기능으로는 IP 를 할당하기 위한 DHCP server, 외부의 DHCP server 와 DHCP client 를 DHCP Relay Agent, DHCP 환경에서 고정 IP 사용을 차단하는 DHCP Blocking 기능이 있습니다.

3.5.1 DHCP server 설정 및 조회

DHCP server 기능을 활성화 시키기 위해서는 DHCP client 에게 IP 어드레스를 할당하기 위한 DHCP pool 을 생성해야 합니다. Pool 을 생성하기 위해서는 ‘ip dhcp pool <Pool Name>’을 사용합니다. Pool 을 생성한 후에는 DHCP client 에게 IP 어드레스를 할당하기 위한 IP subnet network number 와 mask 를 설정합니다. 그리고 설정한 subnet 에 속하는 IP range 를 설정합니다.

명령어	설명	모드
ip dhcp pool <Pool Name>	DHCP pool 이름 설정	Config
network A.B.C.D/M	DHCP client 에게 IP 어드레스를 할당하기 위한 네트워크 번호 및 mask 설정	dhcp-config
range A.B.C.D A.B.C.D	DHCP client 에게 IP 어드레스를 할당할 IP 어드레스 할당 범위 설정	dhcp-config
show ip dhcp pool	설정된 DHCP pool 조회	Enable

```

OG1100(config)#ip dhcp pool POOL1          (DHCP pool 설정)
OG1100(dhcp-config)#network 40.40.40.0/24 (Pool에 해당하는 network 설정)
OG1100(dhcp-config)#range 40.40.40.11 40.40.40.100 (할당 IP 범위 설정)
OG1100(dhcp-config)#end
OG1100#show ip dhcp pool

Pool POOL1 :
  network: 40.40.40.0/24
  address range(s):
    add: 40.40.40.11 to 40.40.40.100
  lease <days:hours:minutes> <1:0:0>
  no domain is defined
  no dns-servers
  no default-routers
  no fixed address
  no usage-threshold
OG1100#

```

DHCP client 에게 IP 어드레스를 할당할 때 client 에게 DNS server, default gateway 와 domain 명과 같은 네트워크 설정에 대한 정보를 동시에 줄 수 있습니다.

명령어	설명	모드
domain-name <domain name>	DHCP client 의 domain 이름 설정	dhcp-config
dns-server <DNS server address>	DHCP client 에게 IP 어드레스를 할당하기 위한 네트워크 번호 및 mask 설정	dhcp-config
default-router <default router address>	DHCP client 에게 IP 어드레스를 할당할 IP 할당 범위 설정	dhcp-config

```

OG1100(dhcp-config)#domain-name POOL1
OG1100(dhcp-config)#dns-server 100.100.100.10
OG1100(dhcp-config)#default-router 40.40.40.1
OG1100(dhcp-config)#end
OG1100#show ip dhcp pool

Pool POOL1 :
  network: 40.40.40.0/24
  address range(s):
    add: 40.40.40.11 to 40.40.40.100
  lease <days:hours:minutes> <1:0:0>
  domain: POOL1
  dns-server(s): 100.100.100.10
  default-router(s): 40.40.40.1
  no fixed address
  no usage-threshold
    
```

DHCP server 를 이용해 특정 DHCP client 에게 ‘fixedaddr <Hostname> <MAC address> <IP address>’를 이용해 고정된 IP 어드레스를 할당하도록 설정할 수 있습니다.

명령어	설명	모드
fixedaddr <Hostname> <MAC address> <IP address>	DHCP client 에게 고정 IP 어드레스를 할당하도록 설정	dhcp-config

```

OG1100(dhcp-config)#fixedaddr client_1 0000.0c12.12a8 40.40.40.105
OG1100(dhcp-config)#end
OG1100#show ip dhcp pool

Pool POOL1 :
  network: 40.40.40.0/24
  address range(s):
    add: 40.40.40.11 to 40.40.40.100
  lease <days:hours:minutes> <1:0:0>
  domain: POOL1
    
```

```

dns-server(s): 100.100.100.10
default-router(s): 40.40.40.1
fixed address client_1 0000.0C12.12A8 40.40.40.105
no usage-threshold
    
```

DHCP pool의 할당할 수 있는 IP 어드레스 범위 중 사용량이 일정 수준 이상이 되면 운용자에게 메시지로 알려주는 기능은 ‘usage-threshold <IP pool usage in percent>’를 이용해 설정할 수 있습니다.

명령어	설명	모드
usage-threshold <IP pool usage in percent>	Usage threshold 설정	dhcp-config

```

OG1100(dhcp-config)#usage-threshold 85
OG1100(dhcp-config)#end
OG1100#show ip dhcp pool

Pool POOL1 :
  network: 40.40.40.0/24
  address range(s):
    add: 40.40.40.11 to 40.40.40.100
  lease <days:hours:minutes> <1:0:0>
  domain: POOL1
  dns-server(s): 100.100.100.10
  default-router(s): 40.40.40.1
  fixed address client_1 0000.0C12.12A8 40.40.40.105
  usage-threshold: 85
    
```

‘dhcp-config’mode 에서의 설정이 끝나면, ‘config-mode’에서 ‘service dhcp’를 이용해 DHCP server 기능을 활성화 할 수 있습니다. DHCP server 기능을 비활성화 하기 위해서는 ‘no service dhcp’를 이용하며, DHCP server 전체 설정을 삭제하려는 경우에는 ‘no ip dhcp pool’을 이용합니다.

명령어	설명	모드
service dhcp	DHCP server 기능 활성화	config
no service dhcp	DHCP server 기능 비활성화	
show ip dhcp	DHCP server 상태 조회	enable
show ip dhcp pool usage	DHCP server 의 pool 상태 조회	enable
show ip dhcp fixed-ip host	고정 IP 어드레스 할당 host 설정 조회	enable

```

OG1100(config)#service dhcp
OG1100(config)#end
OG1100#show ip dhcp
dhcp server enabled.
dhcp pool list: POOL1
OG1100#show ip dhcp pool usage
Pool Name      Type      IP Address      Total      Used      Usage
-----
POOL1          Network  40.40.40.0/24   90         0         0.00%
OG1100#show ip dhcp fixed-ip host
=====
Pool           Host      MAC Address      IP Address
-----
POOL1         client_1  0000.0C12.12A8  40.40.40.105
-----
Total Count: 1
=====
    
```

DHCP server 를 통해 DHCP client 에 할당된 IP 어드레스 내역은 ‘show ip dhcp pool binding’ 을 이용하여 조회할 수 있습니다.

명령어	설명	모드
show ip dhcp pool binding	DHCP server 에 의해 DHCP client 에게 할당된 IP 어드레스 내역 조회	enable

```

OG1100#show ip dhcp pool binding
IP Address      Hardware Address      Lease Expiration      Type
-----
40.40.40.243    00:60:f3:01:00:09    2006/02/22 11:32:15  Network
40.40.40.244    00:60:f3:01:00:08    2006/02/22 11:32:15  Network
40.40.40.245    00:60:f3:01:00:07    2006/02/22 11:32:15  Network
40.40.40.246    00:60:f3:01:00:06    2006/02/22 11:32:15  Network
40.40.40.247    00:60:f3:01:00:05    2006/02/22 11:32:15  Network
40.40.40.248    00:60:f3:01:00:04    2006/02/22 11:32:15  Network
40.40.40.249    00:60:f3:01:00:03    2006/02/22 11:32:15  Network
40.40.40.250    00:60:f3:01:00:02    2006/02/22 11:32:15  Network
40.40.40.251    00:60:f3:01:00:01    2006/02/22 11:32:15  Network
40.40.40.252    00:60:f3:01:00:00    2006/02/22 11:32:15  Network
-----
Total Count: 10
-----
    
```

3.5.2 DHCP relay agent 설정 및 조회

DHCP server 와 DHCP client 가 다른 subnet 에 있는 경우, DHCP relay agent 를 이용해 둘 사이를 중계하도록 합니다.

DHCP relay agent 설정은 'configure mode'에서 'ip dhcp-relay' 명령어를 이용해 'dhcp-relay' mode 에서 할 수 있습니다. DHCP relay agent 를 실행시키기 위해서는 DHCP client 와 DHCP server 의 인터페이스, DHCP server IP 어드레스 혹은 server 이름에 대한 설정을 필요로 합니다. DHCP relay agent 를 활성화하려면 'config-mode'에서 'service dhcp-relay'를 이용하고, 비활성화 하려면 'no service dhcp-relay'를 이용합니다. DHCP relay agent 의 전체 설정을 삭제하려면 'no ip dhcp-relay'를 입력합니다.

명령어	설명	모드
ip dhcp-relay	DHCP relay agent 설정 mode 로 변경	config
interface-list <interface name>	DHCP client/server 의 인터페이스 설정	dhcp-relay
server-list ip <DHCP server ip> server-list name <DHCP server name>	DHCP client 의 DHCP packet 을 보낼 DHCP server 설정	dhcp-relay
service dhcp-relay no service dhcp-relay	DHCP relay agent 기능 활성화 DHCP relay agent 기능 비활성화	config
show ip dhcp-relay	DHCP relay agent 관련 설정 확인	enable

```

OG1100(config)#ip dhcp-relay
OG1100(dhcp-relay)#interface-list vlan40 (DHCP client 쪽 인터페이스)
OG1100(dhcp-relay)#interface-list vlan60 (DHCP server 쪽 인터페이스)
OG1100(dhcp-relay)#server-list ip 60.60.60.60
OG1100(dhcp-relay)#server-list name DHCP_SERVER
OG1100(dhcp-relay)#exit
OG1100(config)#service dhcp-relay
OG1100(config)#end
OG1100#show ip dhcp-relay
dhcp-relay enabled.
dhcp-relay listen interface:
vlan40 vlan60
dhcp-server ip:
60.60.60.60
dhcp-server name:
DHCP_SERVER
OG1100#

```


DHCP relay agent 를 활성화하게 되면, DHCP relay agent option 기능(option 82)을 이용할 수 있게 됩니다. Option 82 와 관련된 명령은 ‘option 82(enable|forward|append|replace)’입니다. Option82 field 는 agent circuit id 와 agent remote id 두 부분으로 구성되어 있으며, agent circuit id 는 client 로부터 DHCP packet 이 인가된 OLT port 의 정보를, agent remote id 는 OLT 장비의 MAC 어드레스 정보를 제공해 줍니다.

명령어	설명	모드
option82(append enable forward replace)	DHCP relay agent 의 option82 상태 설정	dhcp-relay

```

OG1100(dhcp-relay)#option82 enable
OG1100(dhcp-relay)#end
OG1100#show ip dhcp-relay
dhcp-relay enabled.
option82 status enable
dhcp-relay listen interface:
vlan40 vlan60
dhcp-server ip:
60.60.60.60
dhcp-server name:
DHCP_SERVER
OG1100#
    
```

OG1100 에는 DHCP relay agent 를 통해 DHCP server 로부터 IP 어드레스를 할당받은 client 에 대한 정보를 조회할 수 있는 기능이 있습니다. 이 기능을 실행하기 위해서는 ‘dhcp-relay mode’ 에서 ‘relay-binding enable’ 명령어를 이용하면 됩니다. DHCP relay agent 를 통해 IP 어드레스를 할당받은 client 에 대한 조회는 ‘show ip dhcp-relay binding-list’를 이용합니다.

명령어	설명	모드
relay-binding enable	DHCP relay agent 를 통해 IP 어드레스를 할당받은 client 조회 기능 활성화	dhcp-relay
show ip dhcp-relay binding-list	DHCP relay agent 를 통해 IP 어드레스를 할당 받은 client 조회	dhcp-relay

```

OG1100(dhcp-relay)#relay-binding enable
OG1100(dhcp-relay)#end
OG1100#show ip dhcp-relay binding-list
=====
Mac Address          IP Address          VLAN          Lease(sec)
-----
00:60:f3:01:00:09    40.40.40.243       vlan40        600
00:60:f3:01:00:08    40.40.40.244       vlan40        600
00:60:f3:01:00:07    40.40.40.245       vlan40        600
    
```

```

00:60:f3:01:00:06    40.40.40.246    vlan40          600
00:60:f3:01:00:05    40.40.40.247    vlan40          600
00:60:f3:01:00:04    40.40.40.248    vlan40          600
00:60:f3:01:00:03    40.40.40.249    vlan40          600
00:60:f3:01:00:02    40.40.40.250    vlan40          600
00:60:f3:01:00:01    40.40.40.251    vlan40          600
00:60:f3:01:00:00    40.40.40.252    vlan40          600
-----
Total Count: 10
=====

```

3.5.3 DHCP blocking 설정 및 조회

DHCP client 가 DHCP server 를 통해 IP 어드레스를 할당 받는 환경에서, 단말의 host 가 DHCP server 가 할당한 IP 어드레스가 아닌 다른 고정 IP 어드레스를 사용한다면, 불법으로 IP 어드레스를 사용하는 host 로 간주할 수 있습니다.

이런 단말의 통신을 막기 위해 사용하는 것이 dhcp blocking 기능입니다. DHCP blocking 과 관련된 설정은 'config-mode'의 'ip dhcp-block' 명령어를 통해 'dhcp-config mode'에서 설정할 수 있습니다. DHCP blocking 설정을 위해서는 blocking 기능을 수행할 인터페이스와 고정 IP 어드레스 사용 host 에 대한 검사 주기 설정이 필요합니다. 설정이 완료되면 'config-mode'에서 'service dhcp-block'을 이용해 기능을 활성화 할 수 있으며, 'no service dhcp-block'을 통해 기능을 비활성화 할 수 있습니다. DHCP blocking 관련 설정을 모두 삭제하려면 'config-mode'에서 'no ip dhcp-block'을 사용합니다.

명령어	설명	모드
ip dhcp-block	DHCP blocking 설정 mode 로 변경	config
interface-list <interface name>	DHCP blocking 을 수행할 인터페이스 설정	dhcp-block
interval <5-10 Min.>	고정 IP 어드레스 사용 host 검사를 위한 주기 설정(기본 : 5 분)	dhcp-block
service dhcp-block	DHCP blocking 기능 활성화	config
no service dhcp-block	DHCP blocking 기능 비활성화	
Show ip dhcp-block	DHCP blocking 관련 설정 확인	enable

```

OG1100(config)#ip dhcp-block
OG1100(dhcp-block)#interface-list vlan60
OG1100(dhcp-block)#interface-list vlan40
OG1100(dhcp-block)#interval 8
OG1100(dhcp-block)#ex
OG1100(config)#service dhcp-block
OG1100(config)#end
OG1100#show ip dhcp-block
Static IP-blocking enabled.
Static IP-blocking listen interface:
  vlan40  vlan60
Static IP-blocking interval: 8 minute.

```

DHCP blocking 을 통해 차단된 IP 어드레스에 대한 정보는 ‘show ip dhcp-block list’를 통해서 확인할 수 있습니다.

명령어	설명	모드
show ip dhcp-block list	DHCP blocking 을 통해 차단된 IP 어드레스 정보	enable

```

OG1100#show ip dhcp-block list
=====
IP address      Mac Address      PORT    IfName
-----
60.60.60.60    00:00:f0:12:12:08    9/6    vlan60
-----
Total count : 1
=====
    
```

DHCP blocking 기능은 L3 인터페이스를 기준으로 고정 IP 어드레스를 사용하는 단말 host 를 차단하게 됩니다. 그런데 DHCP blocking 을 실행시킬 인터페이스에 secondary IP 어드레스가 설정되어 있을 때, 특정 secondary IP 어드레스 대역에 대해서는 고정 IP 어드레스 사용을 허용하려면 ‘dhcp-block mode’에서 ‘limited-subnet <A.B.C.D/M>’을 이용해 해당 인터페이스의 특정 대역에 대해서는 blocking 기능을 수행하지 않도록 설정할 수 있습니다.

```

OG1100(dhcp-block)#limited-subnet 60.60.60.0/24 (60.60.60.0/24
blocking 기능 해제)
OG1100(dhcp-block)#end
OG1100#show ip dhcp-block list
No active blocking list (Blocking 되었던 host 해제)
OG1100#show ip dhcp-block
Static IP-blocking enabled.
Static IP-blocking listen interface:
vlan40 vlan60
Static IP-blocking interval: 8 minute.
Limited subnet of static IP blocking:
60.60.60.0/24
    
```

3.5.4 DHCP 통계 정보 설정 및 조회

DHCP server 가 수신한 DHCP discover, request, relase 나 송신한 DHCP offer, ack, nak 등의 패킷과 관련된 통계정보를 조회할 수 있습니다. 'show ip dhcp statistics'를 통해 조회가 가능합니다.

명령어	설명	모드
ip dhcp statistics enable	DHCP 통계 정보 조회 기능 활성화	config
show ip dhcp statistics	DHCP 통계 정보 조회	enable

```

OG1100(config)#ip dhcp statistics enable
OG1100(config)#end
OG1100#show ip dhcp statistics

-----
      DHCP Packet Statistics
-----
MALFORMED_MESSAGE      0
BOOT_REQUEST           0
BOOT_REPLY             0
DHCP_DISCOVER          40
DHCP_OFFER             40
DHCP_REQUEST           40
DHCP_ACK               40
DHCP_NAK               0
DHCP_DECLINE           0
DHCP_INFORM            0
DHCP_RELEASE           30
-----

```

3.6 QoS 환경 설정

QoS 는 트래픽의 특성에 따라 여러 플로우로 구분하여 각 트래픽마다 차등화된 품질의 서비스를 제공할 수 있게 해주는 기술입니다. 즉, QoS 기능을 이용하면 중요한 정보를 전송하는 트래픽이나 혹은 실시간으로 처리되어야 하는 트래픽에 높은 우선 순위를 부여하여 다른 트래픽보다 우선적으로 처리할 수 있고, 우선 순위가 낮은 트래픽은 우선 순위가 높은 트래픽이 처리된 이후에 전송될 수 있도록 할 수 있습니다. 이와 같은 QoS 기능을 이용하여 한정된 대역폭과 네트워크 자원은 효율적으로 사용할 수 있습니다.

3.6.1 QoS 개요

QoS 는 다음과 같이 트래픽을 분류하는 부분(Classifier)과 분류된 트래픽을 처리하는 부분(Traffic Manager)으로 이루어집니다.

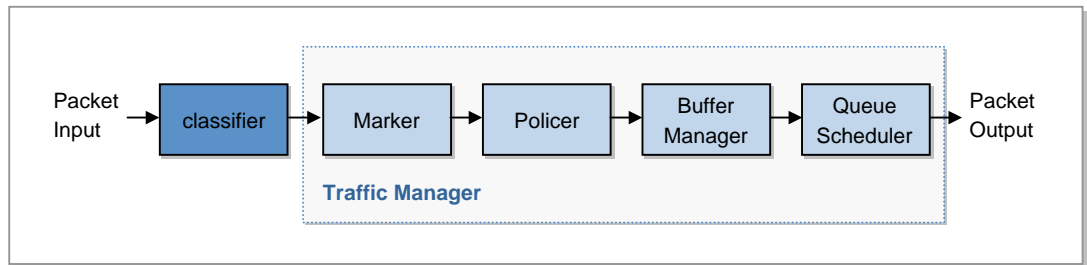


그림 3.1 QoS 구조

Classifier 에서는 수신된 패킷의 헤더정보를 참고하여 패킷을 분류합니다. Traffic Manager 에서는 classifier 에서 분류된 패킷에 CoS, DSCP, ToS 등을 마킹하고, Meter 를 이용하여 약속된 대역폭 이내의 패킷만 처리하거나 congestion 이 발생했을 때 어떤 패킷을 버릴 것인지 선택하거나(Buffer Manager) 혹은 출력 포트를 통해 어떤 패킷을 우선적으로 전송할 것인지(Queue Scheduling) 등의 작업을 수행합니다.

3.6.1.1 Classifier

Classifier 는 패킷 헤더에 있는 정보들을 이용하여 트래픽을 분류하는데 다음 값들을 사용합니다.

- **Layer 1:** 입력/출력 포트 번호
- **Layer 2:** 전송지/목적지 MAC 어드레스, EtherType 필드, 802.1P 필드, VLAN ID
- **Layer 3:** 전송지/목적지 IP 어드레스, 프로토콜 ID, TOS/DSCP 필드, TTL
- **Layer 4:** 전송지/목적지 포트번호, TCP 플래그, 전송지/목적지 포트 범위지정

본 시스템은 class group 을 12 개까지 설정 가능하고 group 당 최대 128 개의 class-entry 를 설정할 수 있습니다. 각 class-entry 는 Layer1~Layer4 중에서 원하는 조합으로 설정이 가능하고 더블매치가 발생할 경우, class-entry ID 가 큰 entry 가 더 높은 우선순위를 갖습니다.

3.6.1.2 Marker

Packet Marker 는 Classifier 에 의해 분류된 패킷에 802.1p 필드나 TOS/DSCP 필드에 표시해주는 기능입니다. 분류된 패킷은 classifier 에 의해 결정된 값을 그대로 사용할 수도 있고, QoS 정책에 의해서 리마킹(remarking)될 수도 있습니다.

3.6.1.3 Policer

Policer 는 사용자가 약속된 대역폭만큼만 사용하도록 대역폭을 제한하는 기능입니다. classifier 에 의해 분류된 플로우(traffic flow)별로 트래픽의 유입율을 미터로 측정하여 정해진 대역폭 이상을 사용할 수 없도록 합니다.

Policer 는 미터링(metering)과 액션 블록(action block)으로 구성됩니다. 미터링은 트래픽의 유입율을 측정하여 측정된 값을 약속되어 있는 대역폭과 비교합니다. 그리고, 그 결과(Green, Yellow, Red)를 액션 블록에 알려줍니다. 액션 블록은 Conform-action, Exceed-action, Violate-action 으로 구분되는데, 미터에 따른 트래픽의 Color 에 따라 적용되는 액션이 결정됩니다. 처리 방법에는 permit(결과에 무관하게 항상 패킷을 그대로 전송), drop(대역폭을 초과한 패킷은 항상 폐기), marking(대역폭을 초과한 패킷에 리마킹)등을 적용할 수 있습니다.

3.6.1.4 Buffer Manager

출력 포트에 있는 CoS 큐의 크기가 한정되어 있기 때문에 큐에 패킷이 가득찬 상태에서 새로운 패킷이 들어오면 일정한 규칙에 따라 패킷을 폐기해야 합니다. 이와 같이 큐의 congestion 을 해결하기 위해서 수신된 패킷을 선택적으로 폐기하는 기능을 Buffer Manager 라고 합니다. OG-1100 시스템은 디폴트로 Tail Drop 방식을 사용하여 Queue Threshold 이상 들어오는 패킷을 모두 폐기됩니다. 그리고 Drop-precedence 를 이용하여 패킷 Color 에 따라 차등적으로 폐기할 수 있습니다.

3.6.1.5 Queue Scheduler

일반적으로 출력 포트는 여러 입력 포트에서 패킷을 수신하기 때문에 Congestion 이 발생하게 됩니다. 출력 포트에는 포트당 하나 이상의 큐가 할당되어 출력 포트를 통해 처리되어야 할 패킷이 저장됩니다. 출력 포트는 큐에 저장되어 있는 패킷이 전송할 수 있는 대역폭보다 많은 경우(congestion 발생시) 어떤 패킷을 우선적으로 처리해야 할 지에 대한 방법이 정해져 있어야 하는데, 이러한 방법을 큐 스케줄링이라고 합니다.

큐 스케줄링 방식에는 여러 가지가 있는데, OG1000 시스템에서는 다음 방식들이 사용됩니다.

Strict Priority Queueing

이 방식은 각 큐에 high, medium, low 의 우선 순위를 지정하고, 우선 순위가 높은 큐에 있는 패킷을 모두 처리한 후 다음 우선 순위 큐의 패킷을 처리하는 방식입니다. 이 방식은 구현하기는 쉽지만, 우선 순위가 높은 큐로 유입되는 패킷의 양이 많을 경우에는 우선 순위가 낮은 큐에 있는 패킷이 처리가 되지 않는 starvation 현상이 발생할 수 있습니다.

RR (Round Robin)

이 방식은 모든 큐가 우선순위를 무시하고 동등하게 서비스 되는 방식입니다.

WRR (Weight Round Robin)

WRR 방식은 SPQ 에서 발생하는 starvation 현상을 없애기 위해 모든 큐를 순차적으로 방문합니다. 대신, 각 큐마다 weight 라는 값을 사용하는데, 이 값은 큐를 통해 서비스될 패킷 개수의 비율을 나타냅니다.

DRR (Deficit Round Robin)

DRR 방식은 WRR 에서 발생할 수 있는 패킷 사이즈에 따른 역전 현상을 없애기 위해서 패킷을 작은 단위로 쪼개서 스케줄링을 수행합니다. 또한 각 큐마다 weight, quantum, deficit counter 를 이용하여 패킷을 서비스 합니다.

3.6.2 QoS 정책 적용 순서

본 시스템에 QoS 정책을 적용하는 순서는 다음과 같습니다.

- 1) Class-Map 정의
QoS 정책을 구성하기 위한 첫 번째 단계로 패킷 분류를 위해서 Class-map 을 정의합니다. Class-map 을 정의하기 위해서 이미 정의되어진 Qset(Qualifier Set : 1~13)중에서 하나를 선택하여 Class-map(=class group)을 생성합니다. 그리고 각 class-map 은 128 개까지 class-entry 를 생성할 수 있는데 Qset 에 정의되어진 Class Key 들을 이용하여 match rule 을 정의해야 합니다.
- 2) Policy-map 정의
QoS 정책을 구성하기 위한 두 번째 단계로 QoS Action 를 적용하기 위해서 Policy-map 을 정의합니다. Class-map 에서 분류된 트래픽에 미터링 결과에 따라서 다양한 Action 을 수행하고 마킹/리마킹을 적용할 수 있습니다.
- 3) Service-Policy 적용 : QoS 정책 구성의 마지막 단계는 위에서 설정한 policy-map 을 실제 포트에 적용합니다.

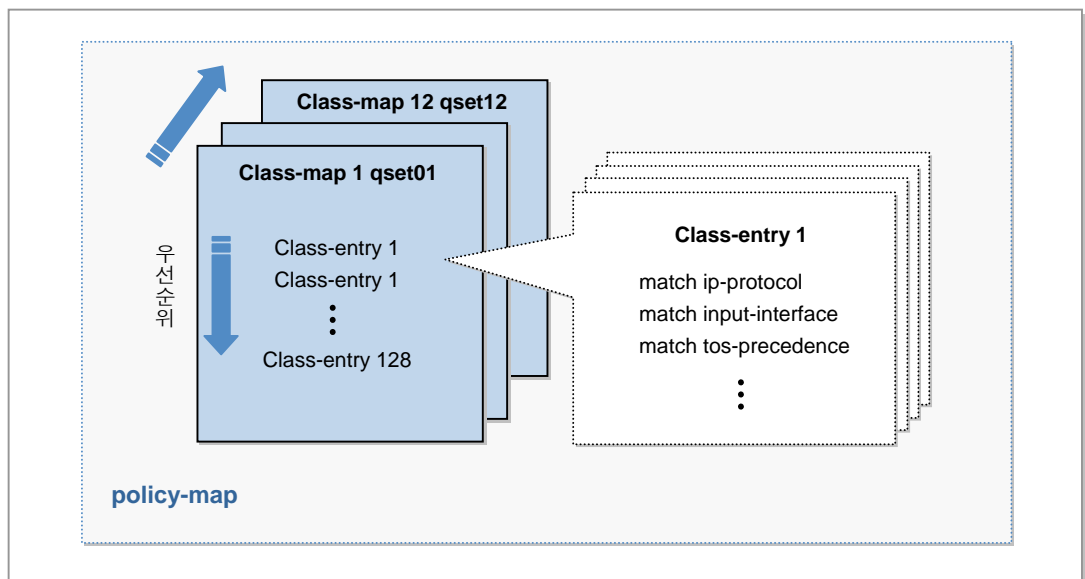


그림 3.2 Policy-map 구조

3.6.2.1 Classifier

OG-1100 시스템 시스템에서 QoS 패킷 분류를 하기 위한 명령어는 다음과 같습니다. 모든 QoS 관련 명령어는 QoS 모드에서 시작합니다.

명령어	설명	모드
Qos	QoS mode 로 변경	Config
Class-map	Class-map mode 로 변경	qos
exit	Config mode 로 이동	
no	설정된 설정을 삭제합니다.	
policy-map	Policy-map mode 로 변경	
port-range	Port-range mode 로 변경	
service-policy	<ul style="list-style-type: none"> - Policy-map 실행 - Input port trust dscp/cos 설정 - Output scheduling - Output port Metering - Output cos rate limit 설정 	

OG-1100 시스템 시스템은 사용자에게 편의성 제공을 위한 Class-map 을 정의하기 위해서 미리 정의한 Qset(Qualifier set)를 선택해야 하는데 다음과 같은 필드 정보를 제공하고 있습니다.

명령어	설명	모드
qset01	<ul style="list-style-type: none"> - Input/Output Interface - Source IP - Destination IP - IP Protocol - ICMP type - Layer 4 source port - Layer 4 destination port - DSCP/TOS - IP Flag - TCP_Control - TTL 	qos
qset02	<ul style="list-style-type: none"> - Input/Output Interface - Source IP - Destination IP - IP Protocol - ICMP type - Layer 4 source port range - Layer 4 destination port - DSCP/TOS - IP Flag - TCP_Control - TTL 	

(계속)

명령어	설명	모드
qset03	<ul style="list-style-type: none"> - Input/Output Interface - Source IP - Destination IP - IP Protocol - ICMP type - Layer 4 source port - Layer 4 destination port range - DSCP/TOS - IP Flag - TCP_Control - TTL 	qos
qset04	<ul style="list-style-type: none"> - This will be implemented in the future. - Input/Output Interface - IP version 6 Source IP address 	
qset05	<ul style="list-style-type: none"> - This will be implemented in the future. - Input/Output Interface - IP version 6 Destination IP address 	
qset06	<ul style="list-style-type: none"> - This will be implemented in the future. - Input/Output Interface - IP version 6 Destination Upper64, NH, TC, FL, TTL, TCP_control 	
qset07	<ul style="list-style-type: none"> - Input/Output Interface - Destination MAC address - Source MAC address - Ether Type - VLAN ID - 802.1p priority 	
qset08	<ul style="list-style-type: none"> - Input/Output Interface - Source MAC address - Source IP address - Ether Type - VLAN ID - 802.1p priority 	
qset09	<ul style="list-style-type: none"> - Input/Output Interface - Destination IP address - Destination MAC address - Ether Type - VLAN ID - 802.1p priority 	
qset10	<ul style="list-style-type: none"> - This will be implemented in the future. - Input/Output Interface - UDF1(user-defined field) 	

(계속)

명령어	설명	모드
qset11	<ul style="list-style-type: none"> - This will be implemented in the future. - Input/Output Interface - UDF2(user-defined field) 	qos
Qset12	qset01 + qset07	

Class-entry 를 정의할 때, match 명령과 함께 사용할 수 있는 분류 기준은 다음과 같습니다.

명령어	설명	모드
diffserv-codepoint	패킷의 DSCP 필드의 값(0~63)	Class-entry
ether-type	패킷의 Ether Type 필드의 값	
icmp-type	패킷의 ICMP Type 필드의 값(0~18)	
input-interface	패킷의 input 인터페이스의 값(범위 설정 가능합니다. 예를 들어 2/1-3/2, 7/8)	
ip-destination-address	패킷의 목적지 IP 어드레스	
ip-destination-port	패킷의 L4 목적지 port 필드의 값 (0~65535)	
ip-fragment-bit	패킷의 IP fragment 필드의 값(0~3)	
ip-protocol	패킷의 IP 프로토콜 필드의 값(0~255)	
ip-source-address	패킷의 전송지 IP 어드레스	
ip-source-port	패킷의 L4 전송지 포트 필드의 값 (0~65535)	
ip-ttl	패킷의 IP TTL 필드의 값(0~255)	
mac-destination-address	패킷의 목적지 MAC 어드레스	
mac-source-address	패킷의 전송지 MAC 어드레스	
out-interface	패킷의 output 인터페이스의 값(Layer 2 에서만 동작)	
prio-tag	패킷의 802.1p 필드의 값(0~7)	
tcp-control	패킷의 TCP control 필드의 값(0~63)	
tos-precedence	패킷의 TOS 필드의 값(0~7)	
vlan-tag	패킷의 VLAN tag 필드의 값(1~4094)	
port-range	패킷의 L4 Port Range ID	

OG-1100 시스템의 port-range 명령어를 이용하여 불필요한 class-entry 수를 줄일 수 있는데, 16 개까지 port-range ID 를 생성할 수 있습니다.(다음 절에서 자세히 설명합니다.)

클래스 맵 설정시 중복 설정이 불가능한 경우와 제약 사항은 아래와 같습니다.

- DSCP 와 tos-precedence 은 중복 설정이 불가능합니다.
- icmp-type 을 설정은 ip-protocol ‘1’(icmp)이 아닌 경우에는 불가능합니다.
- ip-destination-port, ip-source-port, port-range 설정은 ip-protocol 이 TCP/UDP 인 경우에만 가능합니다.
- tcp-control 설정은 IP-protocol 이 TCP 가 아닌 다른 프로토콜인 경우에는 설정이 불가능합니다.
- ‘0x0800’이 아닌 ether-type 설정될 경우, 위 명령어에 제약이 따를 수 있습니다.
- Layer 3 스위칭 되는 트래픽은 out-interface 가 적용되지 않습니다.

Class-map 구성하기

클래스 맵을 생성하면 시스템은 클래스 맵에 있는 분류 기준에 따라 인터페이스의 패킷들이 해당 클래스에 속하는지 여부를 결정하게 되고, 이렇게 분류된 패킷들은 Policy-map 의 정책에 따라 필요한 action 이 적용됩니다.

다음은 class-map 을 생성하고 적용하는 방법입니다.

명령어	작업
configure terminal	1) Global 구성 모드로 들어갑니다.
qos	2) QoS 구성 모드로 들어갑니다.
class-map <class-name> <qset0x>	3) 클래스 맵을 정의하고 class-map 모드로 들어갑니다.
class-entry <1-128>	4) class-entry 모드로 들어간다. qset 에 정의된 필드 정보를 조합하여 class-entry 를 최대 128 개 까지 설정할 수 있습니다.
-	5) 클래스의 분류 기준을 설정합니다.(qset 에 따라 다름)
diffserv-codepoint <dscp-value>	<dscp-value> 패킷의 dscp code point 값
ether-type <ether type>	<ether-type> 패킷의 ethernet type 값
icmp-type <icmp-type>	<icmp> 패킷의 icmp type 값
input-interface <slot>/<port>	패킷의 input 인터페이스 번호 <2/1~11/2> 인터페이스 range 설정이 가능함.
ip-destination-address <ip>/<mask>	패킷의 destination IP 어드레스
ip-destination-port <dest-port>	패킷의 Layer 4 destination port 번호
ip-fragment-bit <frag-num>	<0-3> IP fragment bits 번호(MF : 1, DF : 2)
ip-protocol <protocol-num>	Layer 3 IP protocol 번호

(계속)

명령어	작업
ip-source-address <ip>/<mask>	패킷의 source IP 어드레스
ip-source-port <src-port>	패킷의 Layer 4 source port 번호
ip-ttl <ttl-value>	패킷의 IP ttl 값 <0~255>
mac-destination-address <dest-mac>	<dest-mac> 목적지 MAC 어드레스
mac-source-address <src-mac>	<src-mac> 전송지 MAC 어드레스
out-interface <slot>/<port>	패킷의 output 인터페이스 번호 <2/1~11/2>
prio-tag <cos-value>	<cos-value> 패킷의 802.1p priority 값
tcp-control <ctrl-num>	<ctrl-num> 패킷의 tcp control bits 값 (fin : 1, sync : 2, rst : 4, psh : 8, ack : 16, urg : 32)
tos-precedence <tos-value>	<tos-value> 패킷의 IP precedence 값
vlan-tag <vlan-id>	<vlan-id> 패킷의 VLAN ID <1-4094>
port-range <range-id>	<range-id> Layer 4 src/dst port range ID 번호
End	6) Privileged 모드로 돌아간다.
Show class-map <class-map name>	7) 클래스 맵의 구성 정보를 확인합니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#class-map CLASS_1 qset01
OG1100(config-qos-cmap)#class-entry 1
OG1100(config-qos-cmap-e)#match ?
  diffserv-codepoint      Match diffserv codepoint
  icmp-type               Match icmp type
  input-interface         Match input interface
  ip-destination-address  Match ip destination address
  ip-destination-port     Match ip destination port
  ip-fragment-bit        Match IP fragment bits
  ip-protocol             Match ip protocol
  ip-source-address       Match ip source address
  ip-source-port         Match ip source port
  ip-ttl                 Match ip ttl (time to live)
  out-interface          Match output interface in the L2 FDB entry
  tcp-control            Match TCP control bits
  tos-precedence         Match tos precedence

OG1100(config-qos-cmap-e)#match diffserv-codepoint 8
OG1100(config-qos-cmap-e)#match input-interface 2/1
OG1100(config-qos-cmap-e)#match ip-protocol 1
OG1100(config-qos-cmap-e)#exit
OG1100(config-qos-cmap)#class-entry 2
OG1100(config-qos-cmap-e)#match diffserv-codepoint 32
OG1100(config-qos-cmap-e)#match input-interface 2/2

```

```

OG1100(config-qos-cmap-e)#match ip-protocol 6
OG1100(config-qos-cmap-e)#end
OG1100#sh class-map
CLASS_1, referenced 0 times
  qset: qset01
    1.
      diffserv-codepoint 8
      input-interface 2/1
      ip-protocol 1
    2.
      diffserv-codepoint 32
      input-interface 2/2
      ip-protocol 6

OG1100#
    
```

위 예제는 qset01 을 이용하여 class-map 을 설정하는 방법을 보여줍니다. 먼저 qos 모드로 들어간 다음, CLASS_1 이라는 class-map 을 생성합니다. 하나의 class-map 은 128 개 까지의 entry 를 생성할 수 있는데, entry 1 은 2/1 번 포트에 대해서 icmp 이고 dscp 가 8 인 패킷을 필터링하고 entry 2 는 2/2 번 포트에 대해서 tcp 이고 dscp 가 32 인 패킷을 필터링합니다.

만약 entry 1 과 entry 2 사이에 더블 매치가 발생하면 ID가 큰 entry가 우선순위가 더 높기 때문에 entry 2에 설정된 action이 수행됩니다. 설정된 class rule을 삭제하려면 no match 명령어를 사용합니다. 다른 qset도 동일한 방법으로 설정이 가능합니다.

Port Range 구성하기

OG-1100 시스템은 port-range 를 이용하여 class-entry 중복설정으로 인한 자원의 낭비를 줄입니다. Source-port mode 는 Qset02 와 함께 사용되고 Destinatnon-port mode 는 Qset03 과 함께 사용되며 최대 16 개까지 설정 가능합니다.

명령어	설명	모드
port-range WORD	port-range mode 로 변경	Qos
Exit	상위 mode 로 이동	port-range
Mode	L4 source/destination Port mode	
port <0-65535>	Port-range(0-65535)	
Show	running-config 출력	

```

OG1100(config)#qos
OG1100(config-qos)#port-range PR1
OG1100(config-qos-port-range)#mode source-port
OG1100(config-qos-port-range)#port 1 100
OG1100(config-qos-port-range)#exit
OG1100(config-qos)#port-range PR2
OG1100(config-qos-port-range)#mode destination-port
    
```

```

OG1100(config-qos-port-range)#port 100 200
OG1100(config-qos-port-range)#exit
OG1100(config-qos)#class-map CLASS1 qset02
OG1100(config-qos-cmap)#class-entry 1
OG1100(config-qos-cmap-e)#match port-range PR1
OG1100(config-qos-cmap-e)#end
OG1100#sh class-map
Port range:
  PR1, referenced 1 times
    mode: source port
    start: 1, end: 100
  PR2, referenced 0 times
    mode: destination port
    start: 100, end: 200
CLASS1, referenced 0 times
qset: qset02
  1.
    port-range PR1
    
```

위 예제는 source-port range(1-100) PR1 과 destination-port range(100-200) PR2 를 생성한 후, Qset02 를 이용하여 class-map C1 를 만들고 class-entry 1 에 PR1 을 적용한 결과를 보여줍니다. 만약 IP 프로토콜이 TCP 나 UDP 가 아닐 경우, 정상적으로 적용되지 않기 때문에 항상 IP 프로토콜 설정을 확인한 후에 적용해야 합니다.

3.6.2.2 정책 (Policy-Map) 구성

Policy-map 은 특정 트래픽 클래스로 분류된 패킷에 적용할 QoS action 들을 정의합니다. 하나의 Policy-map 은 최대 12 개까지 서로 다른 Class-map 을 포함할 수 있고 해당 entry 에 적용할 QoS action 을 설정합니다. 그리고, 적용할 인터페이스 선택은 class map 의 'match input-interface/output-interface'를 통해서 정의할 수 있습니다. 이렇게 함으로써 인터페이스마다 각기 다른 flow 별로 정책을 적용할 수 있다는 장점이 있습니다.

명령어	설명	모드
Qos	QoS mode 로 변경	Config
class<class-map-name><1-12>	Class-map mode 로 변경 <class-map-name> class-map 이름 <1-12> sequence 번호 : 클수록 우선 순위가 높다.	policy-map
Exit	상위 모드로 이동	
No	적용된 class-map 삭제	
Remark	policy-map 에 대한 설명	
Show	running-config 출력	
class-entry <1-128>	Class-entry mode 로 이동	pmap-cmap
counter <counter-name>	Counter mode 로 이동 class-map 당 64 개 설정가능하고 한 counter 를 2 개 이상의 class-entry 에 중복 설정 가능	

(계속)

명령어	설명	모드
Exit	상위 모드로 이동	
meter <meter-name>	meter mode 로 이동 class-map 당 64 개 설정가능하고 한 meter 를 2 개 이상의 class-entry 에 중복 설정 가능	
No	설정된 내용을 삭제	
Show	Running config 내용 display	
conform-action	Green 패킷에 대한 action 설정	pmap-cmap-entry
exceed-action	Yellow 패킷에 대한 action 설정	
Exit	상위 모드로 이동	
increase-counter <counter-name>	Counter 설정	
No	설정된 action 을 삭제	
rate-limit <meter-name>	Bandwidth 를 설정	
Show	Show running-config	
violate-action	Red 패킷에 대한 action 설정	

QoS action 을 정의할 때, conform-action(green color 패킷) 명령과 함께 사용할 수 있는 분류 기준은 다음과 같습니다.

명령어	설명	모드
copy-to-cpu	cpu 로 패킷 복사	pmap-cmap-entry
copy-to-mirror {<slot>/<port> cpu}	mirrored port 로 패킷 복사	
Deny	패킷 폐기(permit action 과 동시에 설정 불가)	
drop-precedence	congestion 시 먼저 폐기될 패킷 표시	
insert-dscp <0-63>	새로운 dscp 값으로 리마킹	
insert-priority <0-7>	새로운 cos 값으로 리마킹	
insert-tos <0-7>	새로운 tos 값으로 리마킹	
Permit	패킷을 포워딩	
priority-to-tos	cos 값을 tos 값으로 리마킹	
redirect <slot>/<port>	패킷을 특정 포트로 redirect	
set-priority <0-7>	cos queue 만 적용되고 패킷 리마킹은 하지 않습니다.	
tos-to-priority	tos 값을 cos 값으로 리마킹합니다.	

QoS action 을 정의할 때, exceed-action 명령(yellow color 패킷)과 함께 사용할 수 있는 분류 기준은 다음과 같습니다. 미터가 설정되어 있지 않으면 exceed-action 을 사용할 수 없습니다.

명령어	설명	모드
copy-to-cpu	cpu 로 패킷 복사	Pmap-cmap-entry
Deny	패킷 폐기(permit action 과 동시에 설정 불가)	
drop-precedence	congestion 시 먼저 폐기될 패킷 표시	
insert-dscp <dscp-value>	새로운 dscp 값으로 리마킹	
Permit	패킷을 포워딩	

QoS action 을 정의할 때, violate-action 명령(red color 패킷)과 함께 사용할 수 있는 분류 기준은 다음과 같습니다. 미터가 설정되어 있지 않으면 violate-action 을 사용할 수 없습니다.

명령어	설명	모드
copy-to-cpu	cpu 로 패킷을 복사	Pmap-cmap-entry
Deny	패킷 폐기(permit action 과 동시에 설정 불가)	
drop-precedence	congestion 시 먼저 폐기될 패킷 표시	
insert-dscp <dscp-value>	새로운 dscp 값으로 리마킹	
Permit	패킷을 포워딩	

OG-1100 시스템 시스템은 rate-limit 와 increase-counter QoS action 을 적용하기 위해서 미터와 카운터 설정을 분리합니다.(이는 다수의 class-entry 가 미터와 카운터를 공유하여 설정할 수 있게 하기위해서 입니다.) 즉, class-entry 128 개가 counter 및 meter 64 개를 서로 공유하여 설정이 가능합니다. 미터와 카운터에 대해서는 다음 절에서 자세히 설명합니다.

Policy 맵 설정시 중복 설정이 불가능한 경우와 제약사항은 아래와 같습니다.

- Permit 과 deny 는 동시에 설정할 수 없고 toggle 형태로 되어 있습니다.
- Class-map qset12 로 설정할 경우, sequence 번호가 2 개가 사용됨으로 주의해야 합니다. Sequence number 1 과 12 는 사용불가능하고 sequence 번호로 2, 4, 6, 8, 10 사용 가능 합니다.
- Rate-limit 가 설정되어 있어야 exceed action 과 violate action 적용이 가능합니다.
- Copy-to-mirror action 은 port mirror 와 중복 설정하면 이상 동작을 유발할 수 있습니다.
- Insert-priority, set-priority, tos-to-priority 는 동시에 적용될 수 없습니다.
- Insert-tos, priority-to-tos, insert-dscp 는 동시에 적용될 수 없습니다.

policy-map 구성하기

이 절에서는 정의된 class-map 과 policy-map 을 연결하여 QoS action 을 구성하는 방법에 대해서 설명합니다.

명령어	작업
Configure terminal	1) Global 구성 모드로 들어갑니다.
Qos	2) QoS 구성 모드로 들어갑니다.
policy-map<policy-name>	3) policy-map 을 정의하고 Policy-map 구성 모드로 들어갑니다. <policy-name> 새로 정의할 맵의 이름
class-map <class-name> <1-12>	4) 정책을 적용할 클래스 맵을 지정하고 policy-map class 구성 모드로 들어갑니다. <class-name> 정책을 적용할 class-map 이름 <1-12> class-map 사이의 우선순위, 큰 수가 우선순위가 더 높습니다.
class-entry <1-128>	5) 정책을 적용할 class-entry 를 지정하고 class-entry 모드로 들어갑니다. <1-128> class-entry ID 번호
-	6) class-entry 에 적용할 QoS action 을 추가합니다. 각 QoS action 에 대한 상세한 설명을 다음 절에서 자세히 설명합니다.
Conform-action : green color 패킷에 대한 QoS action 을 추가합니다.	
copy-to-cpu	cpu 로 패킷을 복사합니다.
copy-to-mirror {<slot>/<port> cpu}	mirror 포트에 패킷을 복사합니다.
Deny	패킷을 폐기합니다.
drop-precedence	congestion 시 먼저 폐기될 패킷을 지정합니다.
insert-dscp <dscp-value>	<dscp-value> : dscp 값을 리마킹합니다.
insert-priority <prio-value>	<prio-value> : cos 값을 리마킹합니다.
insert-tos <tos-value>	<tos-value> : tos 값을 리마킹합니다.
Permit	패킷을 포워딩합니다.
priority-to-tos	cos 값을 tos 값으로 리마킹합니다.
redirect <slot>/<port>	패킷을 특정 포트에 redirect 합니다.
set-priority <prio-value>	cos queue 를 지정합니다.
tos-to-priority	tos 값을 cos 값으로 리마킹합니다.
exceed-action : yellow color 패킷에 대한 QoS action 을 추가합니다. Default action 은 Deny 로 설정됩니다.	
copy-to-cpu	cpu 로 패킷을 복사합니다.
Deny	패킷을 폐기합니다.
drop-precedence	congestion 시 먼저 폐기될 패킷을 지정합니다.
insert-dscp <dscp-value>	<dscp-value> : dscp 값을 리마킹합니다.

(계속)

명령어	작업
Permit	패킷을 포워딩합니다.
violate-action : red color	패킷에 대한 QoS action 을 추가합니다. Default action 은 Deny 로 설정됩니다.
copy-to-cpu	cpu 로 패킷을 복사합니다.
Deny	패킷을 폐기합니다.
drop-precedence	congestion 시 먼저 폐기될 패킷을 지정합니다.
insert-dscp <dscp-value>	<dscp-value> : dscp 값을 리마킹합니다.
Permit	패킷을 포워딩합니다.
End	7) Privileged 모드로 돌아갑니다.
Show policy-map <policy-map name>	8) 클래스 맵의 구성정보를 확인합니다.

다음은 policy-map POLICY_1 을 정의하고 정책을 적용할 CLASS_1 을 연결하고 실제 QoS action 을 적용한 결과를 보여줍니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#policy-map POLICY_1
OG1100(config-qos-pmap)#class CLASS_1 1
OG1100(config-qos-pmap-c)#class-entry 1
OG1100(config-qos-pmap-c-e)#?
Policy Map's class entry configuration commands:
  conform-action      Bandwidth conform action
  exceed-action       Bandwidth exceed action
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  increase-counter    Counter
  no                  Negate a command or set its defaults
  rate-limit          Rate limit
  show                Show running system information
  violate-action      Bandwidth violate action

OG1100(config-qos-pmap-c-e)#conform-action ?
  copy-to-cpu        Copy to cpu
  copy-to-mirror     Copy to mirror
  deny               Do not switch
  drop-precedence    Drop precedence
  insert-dscp        Insert DSCP
  insert-priority    Affect COSQ and packet
  insert-tos         Insert TOS
  permit             Do switch
  priority-to-tos    TOS to priority
  redirect           Redirect
  set-priority       Affects COSQ only
  tos-to-priority    Priority to TOS

```

```

OG1100(config-qos-pmap-c-e)#conform-action insert-dscp 32
OG1100(config-qos-pmap-c-e)#conform-action copy-to-cpu
OG1100(config-qos-pmap-c-e)#end
OG1100#show policy-map
POLICY_1, referenced 0 times
  class CLASS_1, sequence 1
  -----
  1.
    Conform action clauses:
      insert-dscp 32
      copy-to-cpu
  2.

OG1100#
    
```

위 예제에서는 미리 정의된 class-map ‘CLASS_1’의 class-entry 1 에 dscp 32 를 마킹하고 cpu 로 보내는 action 을 설정하고 그 결과를 보여줍니다

meter 구성하기

이 절에서는 meter 를 정의하고 policy-map 을 생성하여 QoS action 을 구성하는 방법에 대해서 설명합니다. Meter 는 class-map 당 64 개까지 설정이 가능하고 최대 12 * 64 개까지 설정할 수 있습니다.

명령어	설명	모드
meter <meter-name>	Meter mode 로 변경	Pmap-cmap
exit	상위 mode 로 이동	Pmap-cmap-
mode <meter-mode>	Flow mode - srTCM-color-aware mode - trTCM-color-aware mode - srTCM-color-blind mode - srTCM-color-blind mode	meter mode
commit-rate <rate><burst>	- <rate> 1~1000000 kbps (granularity is 64 Kbps) - <burst> 1~16000 kbit (4 kbit 의 배수로 동작합니다)	
peak-rate	- <rate> 1~1000000kbps (granularity is 64 Kbps) - <burst> 1~16000kbit (4 kbit 의 배수로 동작합니다)	
show	running-config 출력	-

다음은 각 meter mode 에 따른 action 설정방법에 대해서 설명합니다.

- flow mode
in-profile 패킷은 green 으로 마킹되고 out-profile 패킷은 red 로 마킹됩니다.
- srTCM-color-blind mode(Single rate three color blind mode)
commit-rate, peak-rate 는 CIR(Committed Information Rate), CBS(Committed Burst Size)와 EBS(Excess Burst Size)를 결정하고 패킷의 color 는 두 버킷의 상태에 따라서 green, yellow, red 패킷으로 마킹됩니다.
- trTCM-color-blind mode
commit-rate, peak-rate 는 CIR(Committed Information Rate),PIR(Peak Information Rate), CBS(Committed Burst Size)와 EBS(Excess Burst Size)를 결정하고 패킷의 color 는 두 버킷의 상태에 따라서 green, yellow, red 패킷으로 마킹됩니다.
- srTCM-color-aware mode
commit-rate, peak-rate 는 CBS 와 EBS 를 결정하고 패킷의 color 는 두 버킷의 상태와 입력 패킷의 color 에 따라서 green, yellow, red 패킷으로 마킹됩니다.
- trTCM-color-aware mode
commit-rate, peak-rate 는 CIR(Committed Information Rate), PIR(Peak Information Rate), CBS(Committed Burst Size)와 EBS(Excess Burst Size)를 결정하고 패킷의 color 는 두 버킷의 상태와 입력 패킷의 color 에 따라서 green, yellow, red 패킷으로 마킹됩니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#policy-map POLICY_1
OG1100(config-qos-pmap)#class CLASS_1
OG1100(config-qos-pmap-c)#meter METER_1
OG1100(config-qos-pmap-meter)#mode flow
OG1100(config-qos-pmap-meter)#peak-rate 100000 4
OG1100(config-qos-pmap-meter)#exit
OG1100(config-qos-pmap-c)#class-entry 1
OG1100(config-qos-pmap-c-e)#rate-limit METER_1
OG1100(config-qos-pmap-c-e)#violate-action deny
OG1100(config-qos-pmap-c)#class-entry 2
OG1100(config-qos-pmap-c-e)#rate-limit METER_1
OG1100(config-qos-pmap-c-e)#conform-action permit
OG1100(config-qos-pmap-c-e)#violate-action deny
OG1100(config-qos-pmap-c-e)#end
OG1100#sh policy-map
POLICY_1, referenced 0 times
  class CLASS_1, sequence 1
  -----
  meter METER_1, sequence 1, referenced 2 times
  mode: flow
  commit rate: 100000Kbit/s, burst: 4Kbit
  peak rate : 100000Kbit/s, burst: 4Kbit
    
```

```

1.
Meter: METER_1
Conform action clauses:
  copy-to-cpu
  insert-dscp 32
Exceed action clauses:
  deny
Violate action clauses:
  deny
2.
Meter: METER_1
Conform action clauses:
  permit
Exceed action clauses:
  deny
Violate action clauses:
  deny

```

위 예제는 flow mode 인 meter ‘METER_1’을 정의하여 100 Mbps/4 Kbit(peak-rate/burst rate)로 설정하였습니다.(단, Flow mode 에서는 peak-rate 만 의미가 있습니다.) 이렇게 정의된 meter 는 rate-limit action 을 이용하여 class-map ‘CLASS_1’의 class-entry 1 과 class-entry 2 에 적용하였습니다. 100Mbps 이상 패킷이 입력될 경우, red 패킷으로 마킹되고 violate-action ‘deny’에 따라 red 패킷은 폐기됩니다. 여기에서 default exceed-action, violate-action 을 deny 로 설정됩니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#policy-map POLICY_1
OG1100(config-qos-pmap)#class CLASS_1
OG1100(config-qos-pmap-c)#meter METER_2
OG1100(config-qos-pmap-meter)#mode trTCM-color-blind
OG1100(config-qos-pmap-meter)#peak-rate 500000 4
OG1100(config-qos-pmap-meter)#commit-rate 100000 4
OG1100(config-qos-pmap-meter)#exit
OG1100(config-qos-pmap-c)#class-entry 1
OG1100(config-qos-pmap-c-e)#rate-limit METER_2
OG1100(config-qos-pmap-c-e)#exceed-action ?
copy-to-cpu      Copy to cpu
deny             Do not switch
drop-precedence  Drop precedence
insert-dscp      Insert DSCP
permit          Do switch

OG1100(config-qos-pmap-c-e)#exceed-action drop-precedence
OG1100(config-qos-pmap-c-e)#exceed-action permit
OG1100(config-qos-pmap-c-e)#end
OG1100#sh policy-map
POLICY_1, referenced 0 times
  class CLASS_1, sequence 1
  -----

```

```

meter METER_1, sequence 1, referenced 1 times
mode: flow
commit rate : 100000Kbit/s, burst: 4Kbit
peak rate : 100000Kbit/s, burst: 4Kbit

meter METER_2, sequence 2, referenced 1 times
mode: trTCM-color-blind
commit rate : 100000Kbit/s, burst: 4Kbit
peak rate : 500000Kbit/s, burst: 4Kbit

1.
Meter: METER_2
Conform action clauses:
copy-to-cpu
insert-dscp 32
Exceed action clauses:
drop-precedence
permit
Violate action clauses:
deny
2.
Meter: METER_1
Conform action clauses:
permit
Exceed action clauses:
deny
Violate action clauses:
deny

OG1100#
    
```

위 예제는 또 다른 meter mode 인 trTCM-color-blind mode 를 설명합니다. trTCM-color-blind meter ‘METER_2’을 새롭게 정의하고 commit-rate 100Mbps/4Kbit (commit-rate/burst rate), peak-rate 500 Mbps/4 Kbit(peak-rate/burst rate)로 설정하여 class-entry 1 에 적용하였습니다. 여기서 100 Mbps 까지 ‘green color’로 마킹되고 100~500 Mbps 는 ‘yellow color’로 마킹되고, 500 Mbps 이상 유입되는 패킷은 ‘red color’가 마킹됩니다. 위 예제에서 보이는 바와 같이 green 패킷은 cpu 로 복사되고 dscp 를 32 로 리마킹하는 action 이 적용됩니다. yellow 패킷은 congestion 이 발생할 경우 먼저 폐기되는 action 이 적용됩니다. 마지막으로 red 로 마킹된 패킷은 바로 폐기됩니다.

counter 구성하기

이 절에서는 counter 를 정의하고 policy-map 을 생성하여 QoS action 을 구성하는 방법에 대해서 설명합니다. class-map 당 64 개까지 설정이 가능하고 최대 12 * 64 개까지 설정할 수 있습니다.

명령어	설명	모드
counter <counter-name>	counter mode 로 변경	Pmap-cmap
exit	상위 mode 로 이동	Pmap-cmap-counter mode

(계속)

명령어	설명	모드
mode <counter-mode>	green-notgreen green-red green-yellow no-no no-yes red-notred red-yellow yes-no	Pmap-cmap- counter mode
reset	현재 정의된 counter 를 reset 합니다.	
show	running-config 출력	-

각 counter mode 에 따른 차이점에 대해서 설명합니다. 일반적으로 counter 하나를 설정하면 두 가지 color 패킷에 대해 패킷 개수가 누적되는 것을 원칙으로 합니다.

그리고 service-policy 를 재적용하면 모든 counter 가 reset 되는 결과를 얻을 수 있습니다.

- green-notgreen: 첫번째 counter 는 green 패킷을 count 하고 두번째 counter 는 green 이외의 패킷을 count 합니다.
- green-red: 첫번째 counter 는 green 패킷을 count 하고 두번째 counter 는 red 패킷을 count 합니다.
- green-yellow: 첫번째 counter 는 green 패킷을 count 하고 두번째 counter 는 yellow 패킷을 count 합니다.
- no-n : 어떠한 패킷도 count 하지 않습니다.
- no-yes: 첫번째 counter 는 count 하지 않고 두번째 counter 는 class rule 에 매칭되는 모든 패킷을 count 합니다.
- red-notred: 첫번째 counter 는 red 패킷을 count 하고 두번째 counter 는 red 이외의 패킷을 count 합니다.
- red-yellow: 첫번째 counter 는 red 패킷을 count 하고 두번째 counter 는 yellow 패킷을 count 합니다.
- yes-no: 첫번째 counter 는 모든 패킷을 count 하고 두번째 counter 는 어떠한 패킷도 count 하지 않습니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#policy-map POLICY_1
OG1100(config-qos-pmap)#class CLASS_1
OG1100(config-qos-pmap-c)#counter CNT_1
OG1100(config-qos-pmap-counter)#mode yes-no
OG1100(config-qos-pmap-counter)#exit
OG1100(config-qos-pmap-c)#class-entry 1
OG1100(config-qos-pmap-c-e)#increase-counter CNT_1
OG1100(config-qos-pmap-c-e)#exit
OG1100(config-qos-pmap-c)#class-entry 2
    
```

```

OG1100(config-qos-pmap-c-e)#increase-counter CNT_1
OG1100(config-qos-pmap-c-e)#exit
OG1100(config-qos-pmap-c)#exit
OG1100(config-qos-pmap)#exit
OG1100(config-qos)#service-policy POLICY_1
OG1100(config-qos)#end
OG1100#sh policy-map
POLICY_1, referenced 1 times
  class CLASS_1, sequence 1
  -----
  meter METER_1, sequence 1, referenced 1 times
  mode: flow
  commit rate      : 100000Kbit/s, burst: 4Kbit
  peak rate       : 100000Kbit/s, burst: 4Kbit

  meter METER_2, sequence 2, referenced 1 times
  mode: trTCM-color-blind
  commit rate      : 100000Kbit/s, burst: 4Kbit
  peak rate       : 500000Kbit/s, burst: 4Kbit

  counter CNT_1, sequence 1, referenced 2 times
  mode: yes no
  type: packet
  number: (0, 0)

1.
  Meter: METER_2
  Counter: CNT_1
  Conform action clauses:
    copy-to-cpu
    insert-dscp 32
  Exceed action clauses:
    drop-precedence
    permit
  Violate action clauses:
    deny
2.
  Meter: METER_1
  Counter: CNT_1
  Conform action clauses:
    permit
  Exceed action clauses:
    deny
  Violate action clauses:
    deny

```

위 예제는 yes-no mode counter 'CNT_1'을 정의하고 class-entry 1 과 class-entry 2 에 적용하였습니다. 만약 class rule 과 매치되는 패킷이 존재하면 첫 번째 counter 가 증가하게 되고 두 번째 counter 는 사용되지 않습니다.(yes-no mode) 다른 counter 설정 모드도 동일한 방법으로 적용할 수 있습니다.

3.6.2.3 Service Policy 구성하기

이 절에서는 Service policy 를 이용하여 policy map 을 적용하고 포트에 input/output 정책 들을 설정하는 방법에 대해서 설명합니다.

명령어	설명	모드
service-policy <policy-map-name>	Policy-map 을 실제 적용합니다. <policy-map-name> 적용할 policy-map 이름.	qos

다음 예제는 위에서 이미 정의된 policy-map 을 실제 하드웨어에 적용하고 조회한 결과를 보여줍니다. 만약 Service-policy 적용후 class-map 이나 policy-map 을 수정할 경우 다시 service-policy 를 재적용해야 합니다.

```
OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#service-policy POLICY_1
OG1100(config-qos)#end
OG1100#sh service-policy
  Policy map: POLICY_1
    Class: CLASS_1, sequence 1
OG1100#
```

3.6.2.4 Service-policy input 구성하기

이 절에서는 service-policy 를 이용하여 input 인터페이스에 정책을 적용하는 방법에 대해서 설명합니다. Service-policy input 은 모두 qos mode 에서 동작합니다.


명령어	설명
service-policy input IFNAME cos-map queue <0-7> prio <0-7>	입력되는 packet 의 802.1p tag 에 대해 특정 egress queue 에 remapping 시키는 기능
service-policy input IFNAME cos-map default	802.1p to cos queue remapping table 을 초기 상태로 돌리는 기능
service-policy input IFNAME trust-dscp(enable disable)	Trust-dscp 를 해당 인터페이스 enable/disable 하는 기능.
service-policy input trust-dscp (all <0-63>) <0-63>	DSCP 값을 remapping 하는 기능.
service-policy input trust-dscp none	DSCP remapping 값은 기본 값 설정
service-policy input trust-dscp <0-63> <0-63> (green yellow red)	DSCP 값을 remapping 하고 three color marking 을 하는 기능
service-policy input trust-dscp <0-63> <0-63> <0-7> (green yellow red)	DSCP 값을 remapping 및 three color marking 을 하고 Prio 를 설정하는 기능.

다음 예제는 interface 2/1 에 대해서 802.1p priority ‘0’을 cos 큐 ‘3’번으로 mapping 하는 과정입니다.

```

OG1100#show service-policy input 2/1
2/1:
  Class of service mapping:
    Prio 0 ==> CoSQ 0
    Prio 1 ==> CoSQ 0
    Prio 2 ==> CoSQ 1
    Prio 3 ==> CoSQ 1
    Prio 4 ==> CoSQ 2
    Prio 5 ==> CoSQ 2
    Prio 6 ==> CoSQ 3
    Prio 7 ==> CoSQ 3
OG1100#
OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#service-policy input 2/1 cos-map prio 0 queue 3
OG1100(config-qos)#end
OG1100#sh service-policy input 2/1
2/1:
  Class of service mapping:
    Prio 0 ==> CoSQ 3
    Prio 1 ==> CoSQ 0
    Prio 2 ==> CoSQ 1
    Prio 3 ==> CoSQ 1
    Prio 4 ==> CoSQ 2
    Prio 5 ==> CoSQ 2
    Prio 6 ==> CoSQ 3
    Prio 7 ==> CoSQ 3
OG1100#
    
```

아래 예제에서는 interface 2/1 에 대해서 trust-dscp 를 설정하는 과정입니다. 모든 DSCP 값에 대해서 DSCP ‘63’으로 remapping 하고 Priority 는 ‘1’, color ‘yellow’를 marking 하여 packet 을 처리하게 됩니다.


Trust-dscp 는 color-aware meter 미터 mode 와 연동하여 동작합니다.

참고

다음 예제는 interface 2/1 에 대해서 trust-dscp 매핑하는 과정을 보여줍니다.

```

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#service-policy input trust-dscp all ?
<0-63> Mapped code point value
    
```

```

OG1100(config-qos)#service-policy input trust-dscp all 63 ?
<0-7>   Priority for mapped code point
green   Green precedence
red     Red precedence
yellow  Yellow precedence
<cr>
OG1100(config-qos)#service-policy input trust-dscp all 63 7 ?
green   Green precedence
red     Red precedence
yellow  Yellow precedence
<cr>

OG1100(config-qos)#service-policy input trust-dscp all 63 7 yellow
OG1100(config-qos)#service-policy input 2/1 trust-dscp enable
OG1100(config-qos)#end
OG1100#show service-policy input trust-dscp
Enabled port list:
  2/1

src      map      prio      cng
-----
all      63          7         yellow
OG1100#

```

인터페이스 2/1 로 입력되는 패킷의 모든 DSCP code 포인트 값에 대해서 DSCP '63'으로 리마킹되고 시스템 내부에서 패킷이 처리될 때, cos 7로 처리됩니다. 그리고 congestion 이 발생하면 yellow 패킷 처리절차를 따릅니다. 또한, 이 결과는 srTCM-color-aware, trTCM-color-aware 미터 모드에서 입력 패킷을 구분하기 위한 인자로써 사용됩니다.

3.6.2.5 Service-policy output 구성하기

이 절에서는 service-policy 를 이용하여 output 인터페이스에 정책을 적용하는 방법에 대해서 설명합니다. Service-policy output 은 모두 qos mode 에서 동작합니다.

명령어	설명
service-policy output IFNAME rate-limit <1-1000000> <1-128000>	Egress Port 에 대해서 rate-limit 설정 <1-1000000> Rate(단위 : Kbit/s), granularity 는 64Kbps. <1-128000> Burst(단위 : Kbit), 32 의 배수로 동작.
service-policy output IFNAME rate-limit <1-1000000> <1-128000> frame-size (64 128 256 512 1024 1280 1518)	Egress Port 에 대해서 rate-limit 설정
service-policy output rate-limit none	Egress Port 에 대해서 rate-limit 해제
service-policy output IFNAME schedule mode(strict round-robin)	Strict-Priority-Queuing 이나 Round-Robin Scheduling mode 를 설정

(계속)

명령어	설명
service-policy output IFNAME schedule mode(weighted-round-robin deficit-round-robin) <0-15> <0-15><0-15> <0-15>	Weighted-round-robin 이나 deficit-round-robin 스케줄링 mode 를 설정
service-policy output IFNAME cos-red-threshold queue <0-3> cng <0-2047>	CNG bit 이 red 로 세팅된 packet 에 대해 queue 내에서의 threshold 값 설정(입력 packet count 가 Threshold 보다 크면 drop)
service-policy output IFNAME cos-red-threshold default	CoS threshold 값 관련 설정을 초기화
service-policy output IFNAME cos-yellow-threshold queue <0-3> cng <0-2047>	CNG bit 이 red 로 세팅된 packet 에 대해 queue 내에서의 threshold 값 설정(입력 packet count 가 Threshold 보다 크면 drop)
service-policy output IFNAME cos-yellow-threshold default	CoS threshold 값 관련 설정을 초기화
service-policy output IFNAME cos-rate-limit queue <0-3> none	Cos Queue 의 rage-limit 값을 초기화
service-policy output IFNAME cos-rate-limit queue <0-3> <1-1000000> <1-1000000>	CoS queue 의 rate-limit 값을 설정. - <1-1000000> Min Rate(단위 : Kbit/s), granularity 는 64Kbps. - <1-1000000> Max Rate(단위 : Kbit/s), granularity 는 64Kbps.



참고

cos threshold 나 rate limit 설정 시 traffic on 이 아니어야 합니다.

다음 예제는 interface 2/1 에 대해서 출력 인터페이스에 Rate Limit 를 설정/해제, color 패킷의 Bandwidth 를 컨트롤하는 방법에 대해서 설명합니다.

```

OG1100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#service-policy output 2/1 ?
  cos-rate-limit           Output CoS rate limit
  cos-red-threshold        Class of service red threshold
  cos-yellow-threshold     Class of service threshold
  rate-limit               Output rate limit
  schedule                 Service policy output scheduling

OG1100(config-qos)#service-policy output 2/1 rate-limit 500000 128
OG1100(config-qos)#service-policy output 2/1 cos-rate-limit queue 0
100000 200000
    
```

```

OG1100(config-qos)#service-policy output 2/1 cos-red-threshold queue
0 100
OG1100(config-qos)#service-policy output 2/1 cos-yellow-threshold
queue 0 200
OG1100(config-qos)#end
OG1100#show service-policy output 2/1
2/1 output
Rate limit:
  rate: 500000 kbit/s
  burst: 128 kbit
Scheduling:
  mode: strict
Class of service queue red threshold:
  CosQ 0 ==> 100
  CosQ 1 ==> 2
  CosQ 2 ==> 2
  CosQ 3 ==> 2
Class of service queue yellow threshold:
  CosQ 0 ==> 200
  CosQ 1 ==> 4
  CosQ 2 ==> 4
  CosQ 3 ==> 4
Class of service queue rate limit:
  CosQ 0 ==> 100000, 200000
  CosQ 1 ==> None
  CosQ 2 ==> None
  CosQ 3 ==> None
OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#qos
OG1100(config-qos)#service-policy output 2/1 rate-limit none
OG1100(config-qos)#service-policy output 2/1 cos-rate-limit queue 0
none
OG1100(config-qos)#service-policy output 2/1 cos-red-threshold
default
OG1100(config-qos)#service-policy output 2/1 cos-yellow-threshold
default
OG1100(config-qos)#end
OG1100#show service-policy output 2/1
2/1 output
Rate limit:
  None
Scheduling:
  mode: strict
Class of service queue red threshold:
  CosQ 0 ==> 2
  CosQ 1 ==> 2
  CosQ 2 ==> 2
  CosQ 3 ==> 2
Class of service queue yellow threshold:
  CosQ 0 ==> 4
  CosQ 1 ==> 4
  CosQ 2 ==> 4
  CosQ 3 ==> 4
Class of service queue rate limit:
OG1100#

```

위 예제의 설정 값은 다음과 같습니다.

- Output Interface: 2/1
- Output Interface Rate-Limit: 500 Mbps/128 kbit(burst)
- Out_IF_CoS_Queue '0' Rate-Limit: 100000 Kbps(min), 200000 Kbps(max)
Min rate 를 기준으로 스케줄링이 적용되고 난 후에 Max rate 를 기준으로 스케줄링이 적용됩니다. 즉, 우선 순위가 낮은 큐도 어느 정도의 대역을 할당해 줄 수 있습니다.
- Out_IF_CoS '0' Red_Threshold : 100(Packet count), CoS Queue '0'에 RED 패킷이 Threshold 이상이면 Drop 됩니다.



참고

Traffic ON 상태에서 적용할 경우, 예상하지 못한 결과를 초래할 수 있습니다. Packet size 가 증가하면 이 값을 줄여야 정상동작 합니다.

- Out_IF_CoS '0' Yellow_Threshold: 100(Packet count), CoS Queue '0'에 Yellow 패킷이 Threshold 이상이면 Drop 됩니다. Traffic ON 이 아니어야 합니다.



참고

Traffic ON 상태에서 적용할 경우, 예상하지 못한 결과를 초래할 수 있습니다. Packet size 가 증가하면 이 값을 줄여줘야 정상동작을 합니다.

다음 예제는 interface 2/1 에 대해서 출력 인터페이스에 Rate Limit 를 설정/해제, color 패킷의 Bandwidth 를 컨트롤하는 방법에 대해서 설명합니다.

```

OG1100(config)#qos
OG1100(config-qos)#service-policy output 2/1 schedule mode ?
  drr Set the scheduling mode as deficit round robin
  rr  Set the scheduling mode as round robin
  spq Set the scheduling mode as strict
  wrr Set the scheduling mode as weighted round robin
OG1100(config-qos)#service-policy output 2/1 schedule mode rr
OG1100(config-qos)#end
OG1100#show service-policy output 2/1
2/1 output
  Rate limit:
  None
  Scheduling:
  mode: round robin
OG1100(config-qos)#service-policy output 2/1 schedule mode wrr 1 2 3
4
OG1100(config-qos)#end
OG1100#show service-policy output 2/1
2/1 output
  Rate limit:
  None
    
```

```

Scheduling:
  mode: weighted round robin
  weight:1 2 3 4
OG1100(config-qos)#service-policy output 2/1 schedule mode drr 1 2 3
4
OG1100(config-qos)#end
OG1100#sh service-policy output 2/1
2/1 output
  Rate limit:
  None
  Scheduling:
  mode: deficit round robin
  weight:1 2 3 4
OG1100#

```

위 예제의 설정 값은 다음과 같습니다.

- 시스템의 Default 스케줄링 모드: SPQ(Strict Priority Queuing)
- Round Robin 일 경우: 4 개의 Queue 가 공평하게 서비스
- Weighted Round-Robin 일 경우: 각 Queue 가 1:2:3:4 의 비율로 서비스 됩니다.
단, 우선 순위가 낮은 큐의 패킷 크기가 클 경우, B/W 역전현상이 발생할 수 있습니다.
- Deficit Round-Robin 일 경우, weight: B/W 는 다음과 같습니다.
(DRR 의 granularity 는 $2^{(n-1)}$ 입니다.)
 - 1 : 10 Kbytes
 - 2 : 20 Kbytes
 - 3 : 40 Kbytes
 - 4 : 80 Kbytes
 - 5 : 160 Kbytes
 - 6 : 320 Kbytes
 - 7 : 640 Kbytes
 - 8 : 1280 Kbytes
 - 9 : 2560 Kbytes
 - 10 : 5120 Kbytes
 - 11 : 10 Mbytes
 - 12 : 20 Mbytes
 - 13 : 40 Mbytes
 - 14 : 80 Mbytes
 - 15 : 160 Mbytes

3.7 Security 환경 설정

OG-1100 시스템은 패킷 필터링 기능을 이용하여 시스템에 Security 기능을 제공하는데 이 절에서는 그 종류와 목적 및 설정 방법에 대해서 설명합니다.

- Dos attack filtering
 시스템으로 유입 및 스위칭 되는 모든 트래픽에 대해서 적용됩니다.
 - IP land attack: Source 및 Destination 이 동일한 IP 어드레스를 이용한 공격 방지 기능
 - Port land attack: Source 및 Destination 이 동일한 Layer 4 포트를 이용한 공격방지 기능
 - ICMP attack: 큰 ICMP 패킷 사이즈를 이용하거나 fragment 된 ICMP 패킷을 이용한 공격 방지 기능
 - TCP attack: 잘못된 TCP 패킷이나 fragment 패킷을 이용하여 공격할 경우 방지하는 기능
 - IP fragment attack: 잘못된 IP fragment 패킷을 이용한 공격 방지 기능
 - ARP attack: ARP 패킷을 이용한 공격 방지 기능
- Netbios filtering
 - 동일한 VLAN 에 속하는 포트에 연결되어 있는 호스트들 간의 파일 및 자원 공유를 방지하기 위한 기능
 - IPX netbios 패킷 필터링: IPX 패킷을 이용한 공격 방지 기능
- Martian filtering
 - VLAN 별 Martian 필터 기능은 다른 Source IP 어드레스를 가지고 외부로 나가는 패킷을 차단하는 기능
- 자동 제한 기능(auto-limit)
 - auto-limit 기능은 broadcast, multicast traffic 이 특정 대역폭 이상, 연속해서 입력 되면 입력 트래픽을 차단하고 대역폭 이하로 내려가면 다시 차단 기능을 해제하여 서비스 시작
- ICMP Unreachable 패킷 제한 기능
 - OG-1100 시스템에서 외부 망으로 icmp destination unreachable 메시지를 전송하는 것을 제한하는 기능
- TCP rst 패킷 제한 기능
 - OG-1100 시스템에서 외부 망으로 TCP reset 플래그가 설정된 패킷 전송을 제한하는 기능
- DHCP 패킷 필터
 - OG-1100 시스템에 연결된 호스트가 DHCP 서버를 동작시키는 경우, OG-1100 시스템에 연결된 다른 호스트들이 비정상적인 IP 어드레스를 할당 가능하며, 이를 방지하기 위해서 지정한 포트를 통해 수신되는 DHCP 서버 패킷을 필터링하는 기능

3.7.1 DoS Attack Filter

3.7.1.1 DoS Attack CPU

시스템의 CPU 로 입력되는 유해 트래픽을 방지하기 위해서 dos-attack 필터를 설정합니다. Security 관련 모든 명령어는 SECURITY MODE 에서 수행됩니다.

명령어	설명
dos-attack cpu icmp prevention no dos-attack cpu icmp prevention	icmp packet 을 이용한 DOS attack 방지 기능 설정/해제
dos-attack cpu land addr prevention no dos-attack cpu land addr prevention	Destination 과 source 가 동일한 IP 어드레스를 이용한 DOS Attack 방지 기능 설정/해제
dos-attack cpu land port prevention no dos-attack cpu land port prevention	Destination 과 source 가 동일한 L4 포트를 이용한 DOS Attack 방지 기능 설정/해제
dos-attack cpu ping-of-death prevention no dos-attack cpu ping-of-death prevention	ping packet 을 이용한 DOS attack 방지 기능 설정/해제
dos-attack cpu tcp prevention no dos-attack cpu tcp prevention	Wrong TCP packet 을 이용한 DOS attack 방지 기능설정/해제
dos-attack cpu tcp-sync prevention no dos-attack cpu tcp-sync prevention	TCP Wrong Sync flag 를 이용한 DOS attack 방지 기능설정/해제
dos-attack cpu tear-drop prevention no dos-attack cpu tear-drop prevention	IP-fragment option 을 이용한 DOS attack 방지 기능설정/해제
dos-attack cpu udp attack prevention no dos-attack cpu udp attack prevention	특정 L4 port 를 사용하는 UDP Traffic 을 이용한 DOS attack 방지 기능설정/해제

아래 예제는 DoS attack 필터링을 설정하여 OG-1100 시스템 시스템의 CPU 로 들어오는 패킷중에서 source/destination IP 어드레스가 같을 경우 패킷을 차단합니다.

아래와 같은 방법으로 다른 DoS attack 필터링도 설정이 가능합니다.

```
OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#security
OG1100(config-security)#dos-attack cpu ?
  icmp          Denial of Service Attack via icmp traffic
  land          Denial of Service Attack via using src ip/port ==
                dst ip/port
  ping-of-death Denial of Service Attack via Ping
  statistics    Statistics
  tcp           Denial of Service Attack via wrong tcp traffic
  tcp-sync     Denial of Service Attack via tcp sync
  tear-drop    Denial of Service Attack via ip fragment
                manipulations
  udp          Denial of Service Attack via udp specific service

OG1100(config-security)#dos-attack cpu land ?
  addr Src IP == Dst IP
  port Src L4 Port == Dst L4 Port
```

```

OG1100(config-security)#dos-attack cpu land
addr port
OG1100(config-security)#dos-attack cpu land addr prevention
OG1100(config-security)#end
OG1100#show security dos-attack
% DoS Attack Configuration :

% [CPU]
% TCP Sync Attack Prevention      : Disabled
% UDP Flood Attack Prevention     : Disabled
% Ping of Death Attack Prevention : Disabled
% Land Addr Attack Prevention     : Enabled
% Land Port Attack Prevention     : Disabled
% Tear Drop Attack Prevention     : Disabled
% ICMP Attack Prevention          : Disabled
% TCP Attack Prevention           : Disabled

% [SYSTEM]
% Land Addr Attack Prevention     : Disabled
% Land Port Attack Prevention     : Disabled
% TCP Attack Prevention           : Disabled
% UDP Flood Attack Prevention     : Disabled
% ICMP Check                      : Disabled
% TCP Fragment Check              : Disabled
% IP Fragment Check               : Disabled

OG1100#
    
```

3.7.1.2 DoS Attack System

시스템을 경유해서 스위칭되는 트래픽에 대해 dos-attack 필터를 설정합니다. Security 관련 모든 명령어는 SECURITY MODE 에서 수행됩니다.

명령어	설명
dos-attack system icmp size check <0-1023> no dos-attack system icmp size check	특정 크기를 넘는 icmp packet 에 대한 drop 기능 설정/해제
dos-attack system land addr prevention no dos-attack system land addr prevention	Destination 과 source 가 동일한 IP 어드레스를 이용한 DOS Attack 방지 기능 설정/해제
dos-attack system land port prevention no dos-attack system land port prevention	Destination 과 source 가 동일한 L4 포트를 이용한 DOS Attack 방지 기능 설정/해제
dos-attack system tcp-fragment check <0-255> no dos-attack system tcp-fragment check	TCP fragment packet 에 대한 dorp 기능 설정/해제, 첫 TCP fragment header 가 설정값보다 작으면 Drop 한다.
dos-attack system tcp prevention no dos-attack system tcp prevention	Wrong TCP packet 을 이용한 DOS attack 방지 기능설정/해제
dos-attack system ip-fragment check no dos-attack system ip-fragment check	Wrong IP fragment packet 에 대한 dorp 기능 설정/해제

(계속)

명령어	설명
dos-attack (system) arp-rate-limit IFNAME <64-1000000> dos-attack (system) arp-rate-limit IFNAME (default)	ARP attack 을 방지하기 위한 port 별 rate-limit 설정 및 해제(default value : 256Kbit/sec)
dos-attack system udp prevention no dos-attack system udp prevention	SIP-DIP : 7-17, 135-135, 7-135, 19-135 를 가진 UDP 패킷을 Drop 한다.

아래 예제는 DoS attack 필터링을 설정하여 스위칭 되는 패킷중에서 source/destination IP 어드레스가 동일한 패킷을 차단합니다.

아래와 같은 방법으로 다른 DoS attack 필터링도 설정이 가능합니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#security
OG1100(config-security)#dos-attack system ?
  icmp-size      ICMP Packet Size
  ip-fragment    IP Fragment
  land           Denial of Service Attack via using src ip/port
==  dst ip/port
  tcp            Denial of Service Attack via wrong tcp traffic
  tcp-fragment  TCP Fragment
  udp           Denial of Service Attack via udp specific
service

OG1100(config-security)#dos-attack system land ?
  addr Src IP == Dst IP
  port Src L4 Port == Dst L4 Port

OG1100(config-security)#dos-attack system land addr prevention
OG1100(config-security)#end
OG1100#show security dos-attack
% DoS Attack Configuration :

% [CPU]
% TCP Sync Attack Prevention      : Disabled
% UDP Flood Attack Prevention     : Disabled
% Ping of Death Attack Prevention : Disabled
% Land Addr Attack Prevention     : Enabled
% Land Port Attack Prevention     : Disabled
% Tear Drop Attack Prevention     : Disabled
% ICMP Attack Prevention         : Disabled
% TCP Attack Prevention          : Disabled

% [SYSTEM]
% Land Addr Attack Prevention     : Enabled
% Land Port Attack Prevention     : Disabled
% TCP Attack Prevention          : Disabled
% UDP Flood Attack Prevention     : Disabled
% ICMP Check                     : Disabled
% TCP Fragment Check             : Disabled
% IP Fragment Check              : Disabled

OG1100#
    
```

3.7.2 Netbios Filter

해당 인터페이스에 Netbios 필터를 설정합니다. Security 관련 모든 명령어는 SECURITY MODE 에서 수행됩니다.

명령어	설명
netbios filter interface all	모든 포트에 netbios filter 설정
netbios filter interface interface	특정 포트에 netbios filter 설정
no netbios filter interace (상기 명령에 대한 disable)	설정된 netbios filter 해제

아래 예제는 인터페이스 7/1 부터 7/8 까지 netbios 필터를 설정하고 그 결과를 보여줍니다. 아래와 같은 방법으로 다른 Netbios 필터링도 설정이 가능합니다.

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#security
OG1100(config-security)#netbios filter interface 7/1-7/8
OG1100(config-security)#end
OG1100#show security netbios-filter
% NetBIOS Filter Configuration :

% Intf      Status
% ----      -
% 2/1      Disabled
% 2/2      Disabled
% 3/1      Disabled
% 3/2      Disabled
% 4/1      Disabled
% 4/2      Disabled
% 5/1      Disabled
% 5/2      Disabled
% 7/1      Enabled
% 7/2      Enabled
% 7/3      Enabled
% 7/4      Enabled
% 7/5      Enabled
% 7/6      Enabled
% 7/7      Enabled
% 7/8      Enabled
% 8/1      Disabled
% 8/2      Disabled
% 9/1      Disabled
% 9/2      Disabled
% 10/1     Disabled
% 10/2     Disabled
% 11/1     Disabled
% 11/2     Disabled

OG1100#

```

3.7.3 Martian Filter

Martian 필터를 이용하여 다른 Source IP 어드레스를 가지고 외부로 나가는 패킷을 차단할 수 있습니다. 단, 해당 VLAN 인터페이스는 L3 인터페이스로 IP 가 설정되어 있어야 하며 하나 이상의 member 포트를 가지고 있어야 합니다. 위의 두 조건이 충족되지 않는 경우 설정이 실제 내부 하드웨어에 반영되지 않습니다.

명령어	설명
martian-filter vlan	모든 VLAN 에 martian filter 설정
no martian-filter vlan	설정된 martian filter 해제

아래 예제는 VLAN10 에 Martian 필터링을 설정하여 10.1.1.1/16 이외의 source IP 어드레스를 가지고 인터페이스 7/1, 7/2 로 들어오는 패킷을 차단합니다. 아래와 같은 방법으로 다른 VLAN 에 대한 설동도 가능합니다.

```
OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#security
OG1100(config-security)#martian-filter vlan10
OG1100(config-security)#end
OG1100#show security martian-filter
% Martian Filter Configuration :

Interface : vlan10 [Applied]
          VID      : 10
          PBMP     : 7/1 7/2
          IP       : 10.1.1.1/16
OG1100#
```

3.7.4 Auto Rate-Limit (Broadcast/Multicast)

auto-limit 기능은 broadcast, multicast traffic 이 특정 대역폭 이상, 연속해서 입력될 경우, 입력 트래픽을 차단하고 대역폭 이하로 내려가면 다시 서비스가 시작됩니다. Security 관련 모든 명령어는 SECURITY MODE 에서 수행됩니다.

명령어	설명
auto-limit(broadcast multicast) interface (all IFNAME) <0-1500000> <0-300>	인터페이스에 auto broadcast/multicast limit 를 설정 Time-out 이 0 인 경우는 traffic 을 monitoring 하여 해당 pps 이하로 입력되는 경우 auto-limit 을 해제
no auto-limit(broadcast multicast) interface (all IFNAME)	설정된 auto limit 를 해제

```

OG1100(config)#security
OG1100(config-security)#auto-limit broadcast interface all ?
<0-1500000> Packet Per Second

OG1100(config-security)#auto-limit broadcast interface all 1000 ?
<0-300> Time Out (0 : auto-toggle through traffic monitoring)

OG1100(config-security)#auto-limit broadcast interface all 1000 300
OG1100(config-security)#auto-limit multicast interface 2/1 1000 200
OG1100(config-security)#end
OG1100#show security auto-limit all
% Auto Broadcast Limit Statistics :

% Intf   Status   Config:                Status:
%        -----   -----   -----   -----   -----
%        pps    time-out   pps    time-out   lock
% -----
% 2/1    Enabled   1000     300      0       0       0
% 2/2    Enabled   1000     300      0       0       0
% 3/1    Enabled   1000     300      0       0       0
% 3/2    Enabled   1000     300      0       0       0

중략 ...

% 10/1   Enabled   1000     300      0       0       0
% 10/2   Enabled   1000     300      0       0       0
% 11/1   Enabled   1000     300      0       0       0
% 11/2   Enabled   1000     300      0       0       0

% Auto Multicast Limit Statistics :

% Intf   Status   Config:                Status:
%        -----   -----   -----   -----   -----
%        pps    time-out   pps    time-out   lock
% -----
% 2/1    Enabled   1000     200      0       0       0
% 2/2    Disabled   0        0        0       0       0
% 3/1    Disabled   0        0        0       0       0
% 3/2    Disabled   0        0        0       0       0
% 4/1    Disabled   0        0        0       0       0

중략 ...

% 11/2   Disabled   0        0        0       0       0

OG1100#
    
```

3.7.5 ICMP Unreachable 제한 기능

OG-1100 시스템에서 외부 망으로 icmp destination unreachable 메시지를 전송하는 것을 제한할 수 있습니다. Security 관련 모든 명령어는 SECURITY MODE 에서 수행됩니다.

명령어	설명
ip icmp destination unreachable disable	OG1100 에서 외부 망으로 icmp destination unreachable 메시지 전송 금지
no ip icmp destination unreachable disable	OG1100 에서 외부 망으로 icmp destination unreachable 메시지 전송 허용

3.7.6 TCP rst 패킷 제한 기능

OG-1100 시스템에서 외부 망으로 TCP reset 플래그가 설정된 패킷전송을 제한할 수 있습니다. Security 관련 모든 명령어는 SECURITY MODE 에서 수행됩니다.

명령어	설명
ip tcp ignore rst-unknown disable	OG1100 에서 외부 망으로 TCP reset flag 설정된 패킷 전송 금지
no ip tcp ignore rst-unknown disable	OG1100 에서 외부 망으로 tcp reset flag 가 설정된 패킷 전송 허용

3.7.7 DHCP 패킷 필터

DHCP server 에 의해 IP 어드레스를 할당받고 있는 환경에서 가입자 단에 IP 공유기 등 또다른 DHCP server 가 될 수 있는 장비가 존재한다면, DHCP client 가 IP 어드레스를 할당받아 가는 DHCP server 가 가입자 단의 사설 DHCP server 가 될 수 있는 상황이 존재하게 됩니다.

이런 현상이 발생하게 되면 가입자인 DHCP client 에는 통신 장애가 발생하게 됩니다. DHCP filtering 은 가입자 포트를 통해 들어왔다가 업링크 포트나 다른 가입자 포트로 나가는 DHCP request 와 가입자 포트로 들어오는 DHCP reply 를 막아줌으로써 DHCP 서비스가 적절하게 이루어질 수 있도록 해줍니다.

DHCP filtering 과 관련된 설정은 ‘interface mode’에서 ‘dhcp-filtering(enable|disable)’을 통해 실행할 수 있으며, DHCP server 나 DHCP relay agent 를 실행시키는 경우에도 자동으로 DHCP filter 가 enable 되게 됩니다. DHCP filter 에 관한 설정은 ‘show dhcp-filter’를 이용하여 조회가 가능합니다.

명령어	설명
dhcp-filter enable	해당 인터페이스를 통해 DHCP 패킷이 전송되지 않도록 설정
dhcp-filter disable	해당 인터페이스를 통해 DHCP 패킷이 전송될 수 있도록 설정
show dhcp-filter interface IFNAME	인터페이스 별로 DHCP Filter 설정 상황을 표시
show dhcp-filter	전체 인터페이스의 DHCP Filter 설정 상황 표시

```

OG1100#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OG1100(config)#interface 2/1
OG1100(config-if)#dhcp-filter enable
OG1100(config-if)#end
OG1100#show dhcp-filter
-----+-----
Port | DHCP Filter
-----+-----
2/1      ON
2/2      OFF
3/1      OFF
3/2      OFF
4/1      OFF

중략 ...

10/2     OFF
11/1     OFF
11/2     OFF
-----+-----
OG1100#
    
```

3.7.8 IPX 패킷 필터

Ethernet Type 이 0x8137 인 패킷을 Drop 하는 기능을 수행한다.

3.7.9 Security 정보 조회

'show security all' 명령어를 통해 모든 Security 정보를 조회할 수 있습니다.

```

OG1100#show security all
% DoS Attack Configuration :

% [CPU]
% TCP Sync Attack Prevention      : Disabled
% UDP Flood Attack Prevention     : Disabled
% Ping of Death Attack Prevention : Disabled
% Land Addr Attack Prevention     : Enabled
% Land Port Attack Prevention     : Disabled
% Tear Drop Attack Prevention     : Disabled
% ICMP Attack Prevention          : Disabled
% TCP Attack Prevention           : Disabled

% [SYSTEM]
% Land Addr Attack Prevention     : Enabled
% Land Port Attack Prevention     : Disabled
% TCP Attack Prevention           : Disabled
% UDP Flood Attack Prevention     : Disabled
% ICMP Check                      : Disabled
% TCP Fragment Check              : Disabled
% IP Fragment Check               : Disabled
    
```



```
% Martian Filter Configuration :

Interface : vlan10 [Applied]
          VID      : 10
          PBMP     : 7/1 7/2
          IP       : 10.1.1.1/16

% Miscellaneous Configuration :

% IP Tcp Ignore Rst-unknown Disable      : Unset
% IP Icmp Destination Unreachable Disable : Unset

% NetBIOS Filter Configuration :

% Intf   Status
% ----  -
% 2/1    Disabled
% 2/2    Disabled
% 3/1    Disabled
% 3/2    Disabled
% 4/1    Disabled
% 4/2    Disabled
% 5/1    Disabled
% 5/2    Disabled
% 7/1    Enabled
% 7/2    Enabled
% 7/3    Enabled
% 7/4    Enabled
% 7/5    Enabled
% 7/6    Enabled
% 7/7    Enabled
% 7/8    Enabled
% 8/1    Disabled
% 8/2    Disabled
% 9/1    Disabled
% 9/2    Disabled
% 10/1   Disabled
% 10/2   Disabled
% 11/1   Disabled
% 11/2   Disabled

% IPX Filter Configuration :

% Intf   Status
% ----  -
% 2/1    Enabled
% 2/2    Enabled
% 3/1    Enabled
% 3/2    Enabled
% 4/1    Enabled
% 4/2    Enabled
% 5/1    Enabled
```

```
% 5/2 Enabled
% 7/1 Enabled
% 7/2 Enabled
% 7/3 Enabled
% 7/4 Enabled
% 7/5 Enabled
% 7/6 Enabled
% 7/7 Enabled
% 7/8 Enabled
% 8/1 Enabled
% 8/2 Enabled
% 9/1 Enabled
% 9/2 Enabled
% 10/1 Enabled
% 10/2 Enabled
% 11/1 Enabled
% 11/2 Enabled
OG1100#
```



약어

A

ACL	access-list
ARP	Address Resolution Protocol

B

BSR	Bootstrap Router
-----	------------------

D

DBA	Dynamic Bandwidth Allocation
DHCP	Dynamic Host Configuration Protocol
DR	Designated Router
DRR	Deficit Round Robin

I

ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol

L

LACP	Link Aggregation Control Protocol
------	-----------------------------------

M

MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol

N

NSA	None Service Affect
-----	---------------------

O

OLT	Optical Line Termination
ONT	Optical Network Termination
ONU	Optical Network Unit

P

PIM-SM	Protocol Independent Multicast Sparse-Mode
PON	Passive Optical Network
PVST	Per VLAN Spanning Tree

R

RADIUS	Remote Authentication Dial In User Service
RP	Rendezvous Point
RR	Round Robin
RSTP	Rapid Spanning Tree Protoco

S

SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System+
---------	---

V

VID	Virtual Identification
-----	------------------------

W

WCMP	Weighted Cost MultiPath
WRR	Weight Round Robin

찾아보기

ㄱ

가청 경보 설정 및 조회2-6
 관리자 인증 리스트 삭제 1-24
 관리자 인증 리스트 생성 1-23
 관리자 인증 리스트 설정 1-23
 관리자 인증 서버 설정 1-25
 관리자 인증 설정 1-23
 기본 VLAN 구성3-23
 기본적인 VLAN 구성과정3-23

ㄴ

단축 명령어 입력 1-4

ㄷ

랙의 정보 설정 및 조회2-1

ㄹ

멀티캐스트 라우터 포트 지정 ...3-51
 멀티캐스트 라우팅 정보 조회 ...3-71
 멀티캐스트 트래픽 포워딩 정책
 설정3-60
 멀티캐스팅 환경 설정3-50
 명령어 기호 1-5
 명령어 라인 편집 키 및 도움말 .1-6
 명령어 문법 도움말 1-2
 명령어 이력 조회 1-30
 물리적 포트 상태 변경 및 조회2-12
 물리적 포트상태 변경2-13

ㅁ

배너 설정 1-28
 비밀번호 설정 1-11
 비밀번호 encryption 설정 1-11

ㅂ

사용자 인터페이스 1-8
 설정정보 파일 관리하기 1-32
 성능 정보 collection 및 monitoring
 설정 1-32
 세션 강제 종료 1-28
 세션 설정 1-13
 소프트웨어 업그레이드하기 1-31
 시스템 명령어 모드 1-7
 시스템 및 각 VLAN 별 IGMP
 snooping 활성화 3-50
 시스템 접속 정보 조회 1-29
 시스템 조회 1-29
 시스템 초기 화면 및 가동 1-9
 시스템의 경보 등급 설정 및 발령
 조회 2-4
 시스템의 자원 상태 설정 및 조회...
 2-3
 시스템의 정보 설정 및 조회 2-2

ㅇ

외부 접속 1-29
 운영자 비밀번호 설정 1-12
 운용자 비밀번호 변경 1-23

운용자 설정 1-22
 운용자 추가 및 삭제 1-22
 운용자 privilege 변경 1-22
 인증 방법 설정 1-14

ㅈ

조회 3-73
 접속 이력 1-30
 정책 (Policy-Map) 구성 3-103

ㅋ

콘솔 연결 1-8
 콘솔/Telnet 환경 설정 1-13

ㅌ

타임 아웃 설정 1-14

ㅍ

포트의 흐름 제어 (IEEE 802.3x)
 설정 2-13
 프리픽스(prefix)가 0 이 아닌
 Candidate RP 메시지 전송 설정
 3-70

ㅎ

현재 세션 환경 설정 1-16
 현재 접속 정보 1-29

A

Access Permit 설정 1-17
 Access-permit 활성화 1-19
 Access-permit List 삭제 1-19
 Access-permit List 생성 1-18
 ACL 설정 1-20
 Aggregation 인터페이스의 기능
 설정 및 조회 3-34

ARP Proxy 설정 및 조회 3-48
 Auto Rate-Limit (Broadcast/Multicast)
 3-126

B

Buffer Manager 3-94

C

Candidate BSR 설정 3-65
 Candidate RP 설정 3-66
 Cisco 라우터와 호환을 위한 설정...
 3-69
 Classifier 3-93, 3-96
 Class-map 구성하기 3-99
 counter 구성하기 3-111

D

DHCP 통계 정보 설정 및 조회 3-91
 DHCP 패킷 필터 3-128, 3-129
 DHCP 환경 설정 3-83
 DHCP blocking 설정 및 조회 3-90
 DHCP relay agent 설정 및 조회 3-88
 DHCP server 설정 및 조회 3-84
 DoS Attack CPU 3-122
 DoS Attack Filter 3-122
 DoS Attack System 3-123
 DR 우선순위 설정 3-69
 DRR (Deficit Round Robin) 3-95

E

Enable 모드 비밀번호 설정 1-11
 Exclude-genid 3-71

F

Field Selectors 3-3

H

Hash 를 이용한 RP 선정방식 설정	3-71
Hello 메시지 전송주기 설정	3-64
Hello 메시지 전송주기/Holdtime 설정	3-64
Hello 메시지 Hold Time 설정	3-64
Hostname 설정	1-12

I

ICMP Unreachable 제한 기능	3-128
IGMP 멤버십 정보 조회	3-82
IGMP 설정 및 조회	3-77
IGMP 인터페이스 설정정보 조회	3-81
IGMP 정보 조회	3-81
IGMP Group Membership Interval 변경	3-52
IGMP Query 메시지 전송주기 설정	3-77
IGMP snooping	3-50
IGMP snooping 기능 설정	3-50
IGMP Snooping 설정 정보 조회	3-61
IGMP Snooping 정보 조회	3-61
IGMP Snooping 포워딩 테이블 정보 조회	3-62
IGMP Snooping Proxy 기능 설정	3-54
.....	3-54
IGMP Snooping Proxy 기능 활성화	3-55
IGMP Snooping Querier 기능 설정	3-58
IGMP Snooping Static Group 설정	3-56
Immediate Leave 설정	3-81
Immediate-leave 기능 설정	3-54
IP 어드레스/subnet 삭제	3-44
IP 어드레스/subnet 설정 및 조회	3-43
IP Multicast-Routing 활성화	3-62

J

Join / Prune 메시지 전송주기 설정	3-65
-----------------------------------	------

L

LACP 설정 및 조회	3-31
Last Member Query Interval 및 count 설정	3-80
Last member query interval 설정	3-53
Layer 2 환경 설정	3-23
Layer 3 환경 설정	3-43
Link 에 VLAN 설정	3-20
Lookup Value	3-3

M

MAC Filtering 설정	3-37
Management IP 설정	1-21
Marker	3-94
Martian Filter	3-126
Max Response Time 설정	3-58
meter 구성하기	3-108
mirroring 설정	3-38

N

Netbios Filter	3-125
----------------------	-------

O

OLT Bridge-map 의 작성	3-5
OLT Class-map 의 작성	3-2
OLT IGMP VLAN 설정	3-8
OLT Igmp-map 의 작성	3-7
OLT Policy-map 의 작성	3-4
OLT Service Profile 의 작성 및 적용	3-1
ONT 의 등록 및 조회	2-9
ONU Bridge-map 의 작성	3-13

ONU Class-map 의 작성 3-11
 ONU Icmp-map 의 작성 3-18
 ONU Policy-map 의 작성 3-12
 ONU Port 에 Advanced Rule 설정 ...
 3-21
 ONU Queue-map 의 작성 3-11
 ONU Service Profile 의 작성 및
 적용 3-10
 ONU/ONT 의 정보 변경 및 삭제 ...
 2-10
 Other Querier Timeout 설정 3-59

P

packet sampling 3-40
 packet sampling 설정 및 조회 .. 3-40
 packet sampling monitor 3-41
 PIM-SM 기능 활성화 3-62, 3-63
 PIM-SM 멀티캐스트 라우팅 정보
 조회 3-72
 PIM-SM 설정 및 조회 3-62
 PIM-SM 정보 조회 3-71
 PIM-SM Neighbor 정보 조회
 3-74, 3-75
 PIM-SM RP 정보 조회 3-74
 pm count 삭제 및 rmon log 삭제.....
 1-35
 Policy-map 구조 3-96
 Policer 3-94
 policy-map 구성하기 3-105
 PON 환경 설정 3-1
 PON OLT 환경 설정 3-1
 PON OLT, ONU/ONT 의 상태
 설정/조회 2-8
 PON ONU 환경 설정 3-9
 PON 의 ONT 등록 및 조회 2-9
 Port Range 구성하기 3-102
 Priority Shared VLAN 3-17
 Priority Simple Bridged 3-15
 Proxy 의 IP 어드레스 설정 3-55

Q

QoS 개요 3-93
 QoS 정책 적용 순서 3-95
 QoS 환경 설정 3-93
 Querier 활성화 3-58
 Querier Timeout 설정 3-79
 Query Interval 설정 3-58
 Query Max Response Time 설정 3-78
 Queue Scheduler 3-94

R

RADIUS 서버 설정 1-25
 Register Checksum 계산 설정 .. 3-70
 Rmon 및 pm 정보 조회 1-34
 Rmon 정보 설정 1-33
 RP Reachability 검사 여부 설정 3-68
 RP register-kat 설정 3-68
 RR (Round Robin) 3-95
 Rule Operators 3-3

S

Secondary IP 어드레스/subnet 설정
 및 조회 3-44
 Security 정보 조회 3-129
 Security 환경 설정 3-121
 Service Policy 구성하기 3-113
 Service-policy input 구성하기 .. 3-114
 Service-policy output 구성하기 3-116
 Shared VLAN 3-14
 show history 1-30
 show history log 1-31
 Simple Bridge 3-14
 SLOT 상태 설정 및 조회 2-6
 SNMP 1-16
 SNMP Network Manager 를 통한
 연결 1-10
 Static ARP 설정 및 ARP 조회 .. 3-45

Static routing 설정 및 조회	3-46
Static RP 설정	3-67
Static trunk 설정 및 조회	3-30
STP Threshold 설정	3-68
STP/RSTP	3-27
Strict Priority Queueing.....	3-94
SWU 포트 설정 및 상태 조회...	2-11

T

TACACS+ 서버 설정	1-26
TCP rst 패킷 제한 기능	3-128
tcpdump 설정	3-39
Telnet 연결	1-9
Transparent Priority Shared VLAN	
.....	3-17
Transparent VLAN	3-15
Trunk/LACP	3-29

V

VLAN 생성하기	3-24
VLAN 설정 및 변경	3-24
VLAN 조회	3-26

W

WRR (Weight Round Robin)	3-95
--------------------------------	------



이 면에는 내용이 없습니다.

OpticGear™
OG-1100 운용 매뉴얼

©2006 Samsung Electronics Co., Ltd.

All rights reserved.

이 매뉴얼의 저작권은 삼성전자(주)에 있습니다.
이 매뉴얼은 삼성전자(주)의 서면동의 없이 어떤 형태로도
재생산·배포·변경할 수 없습니다.

