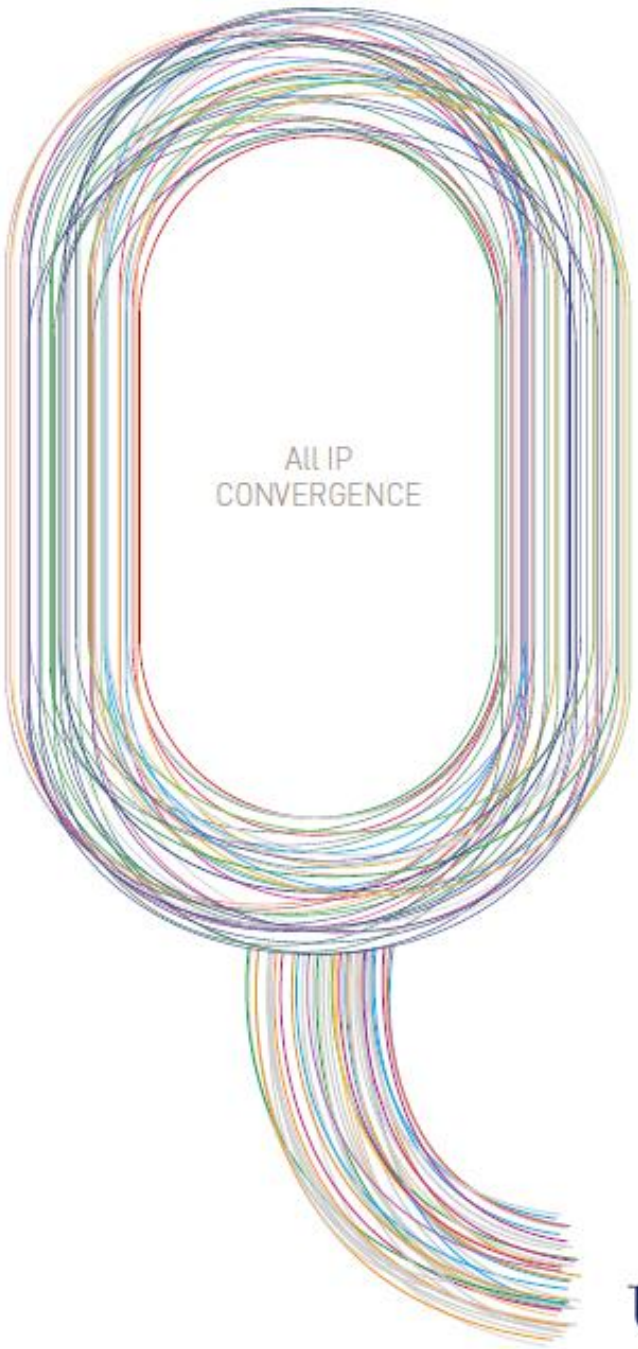
P8624XG Switch
User Guide



Published: May 2008

ubiQuoss

목차

표 목차

그림 목차

1 서문

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

1.1. 개요

본 가이드는 Premier 8624XG 3 계층 스위치 하드웨어를 설치한 다음 네트워크 환경을 설정하고 운영하는 데 필요한 정보를 제공함을 목적으로 한다.

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

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

Notice Premier 8624XG 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하기 바란다.

1.2. 적용 규칙

다음의 < 표 1-1>과 <표 1-2>는 본 가이드에서 사용된 문자 표시 규칙 및 아이콘들을 설명한다.

표 1-1. 문자 표시 규칙

문자 표시 규칙	설명
`Screen displays`	■ 명령 수행 등의 결과로 운영 단말에 표현되는 정보 ■ CLI 명령어 문법
`Screen displays bold`	■ 운영자가 운영 단말에 직접 입력한 명령어
[Key] 입력	■ 키보드의 키 입력을 나타내는 경우 [Enter] 또는 [Ctrl]과 같이 대괄호와 함께 사용 ■ 둘 이상의 키를 동시에 입력하는 경우 [Ctrl] + [z]와 같이 키를 “+”로 연결하여 표현
이탤릭체	■ 강조하는 부분이나 문장에서 새로 정의될 때 사용 ■ 시스템 명령어 문법에서 사용자가 입력해야 하는 파라미터

표 1-2. 알림 및 경고 아이콘

아이콘	종류	설명
	Notice	■ 중요한 기능이나 특징, 명령어, Tip
	Warning	■ 사람에 대한 상해, 데이터 손실, 또는 시스템 손상을 가져올 수 있는 위험

1.3. 관련 문서

Premier 8624XG 스위치 매뉴얼은 다음과 같이 구성된다. 본 장비에 대한 추가 적인 정보는 다음의 매뉴얼들을 통하여 알 수 있다.

매뉴얼 종류	주요 내용
Hardware Installation Guide	■ 스위치 하드웨어 설치 ■ 초기 운용 환경 설정
User Guide	■ 서비스 제공을 위한 운용 환경 설정 ■ 시스템 운용 관리 및 유지보수 ■ 문제 해결(Trouble shooting)

Notice

Premier 8624XG 스위치를 포함한 ㈜유비쿼스 네트웍스의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(http://www.ubiquoss.com)를 통하여 다운로드 받거나 서비스를 요청할 수 있다.

본 문서는 Premier 8624XG Series 에 대한 통합 매뉴얼이다.

2

Premier 8624XG 스위치 시작하기

본 장은 다음과 같이 시스템 운영자가 Premier 8624XG 3 계층 스위치의 운용 환경을 설정하고 처음 다루기 시작할 때 필요한 정보를 제공한다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- Premier 8624XG 스위치 사용자 인터페이스
- 스위치 로그인과 패스워드의 설정
- SNMP 환경설정
- 스위치의 파일 및 환경 설정의 보기와 저장
- 액세스 리스트
- 텔넷 클라이언트

2.1. 편집 및 도움말 기능

본 장은 명령어 편집기의 편집 기능과 도움말 기능에 대하여 설명한다.

2.1.1. 명령어 문법의 이해

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

명령어 라인 인터페이스를 사용하기 위하여 다음의 단계를 거치도록 한다.

1) 명령어 프롬프트에서 명령어를 입력하기 전에, 먼저 적절한 권한을 가지고 있는 프롬프트 수준에 있는지 먼저 확인하라. 대부분의 환경 설정 관련 명령어들은 시스템 운영자 수준의 권한을 필요로 한다.

2) 수행하고자 하는 명령어를 입력하라. 만약 명령어가 추가적인 명령어(sub-command) 또는 파라미터 값을 입력할 필요가 없으면 3 단계로 간다.
   a. 만약 명령어가 파라미터를 가지고 있으면 파라미터 이름 및 값을 입력하라.
   b. 명령어에 따르는 파라미터에 따라서 숫자, 문자열, 또는 주소 등이 값으로 설정된다.

3) 명확하게 명령어 입력을 완료 하였으면, [Return]키를 눌러서 명령을 실행한다.

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

다음은 명령어 파라미터를 제대로 입력하지 않은 경우를 보여준다.

```
Switch# show ↵
% Command incomplete.
Switch #
```

2.1.2. 명령어 문법 도움말(Command Syntax Helper)

Premier 8624XG 스위치의 CLI 는 명령어 문법 도움말 기능을 자체적으로 내장하고 있다. 시스템 운영자는 명령어 입력 중 완전한 문법을 모르는 경우, 어느 위치에서든지 '?'를 쳐서 도움말을 제공받을 수 있다. Premier 8624XG 스위치는 다음과 같은 두 가지 도움말 기능을 제공한다.

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

전체 도움말 기능을 show 명령어를 통하여 보면 다음과 같다. show 명령어 다음에 공백 문자와 함께 '?'를 입력하면 운영자가 입력 할 수 있는 파라미터 및 값의 리스트가 출력된다. 그리고 다시 "f8624XG Series# show" 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기한다. 운영자 입력에서 '**?**'는 화면에 표시되지 않는다.

```
Switch# show ?
  arp                   Display ARP table entries
  authentication        Authentication configurations parameters
  boot                  When system booting, physical port shutdown or not
  clock                 show current system's time
  config                Show config file information
  config-list           display config file list
  cpu                   CPU information
  cpu-filter            CPU Filter
  cpu-mac-filter        MAC Blocking Table based on CPU load
  cpu-packet-counter    CPU packet-counter
  cpuload               CPU load information
  debugging             Debugging functions
  dump                  dump-traffic
  dump-file             tcpdump log file
  environment           Temperature and FAN status information
  flash:                display information about flash file system
  flow                  flow-rule
  flow-rule             flow-rule
  history               Show all contents of command history buffers
  hostkeepalive         Check the keepalive for the specific host
  inet-service          Display enabled internet services
  interface             Interface status and configuration
  ip                    IP information
  lacp                  Port group information
  license               Set enhanced software feature license
  llcf-group            Link Loss Carry Forward group
  logging               Show all contents of logging buffers
  loop-detect           Enable self-loop detection
  mac                   Display MAC address table entries
  mac-address-table     Display MAC address table entries
  mac-count             MAC count configuration
  mac-threshold         MaxMac Threshold information
  max-hosts             MAC count (max-hosts) configuration
  memory                Memory statistics
  mirroring             Port mirroring configuration
  mode                  command mode
```

```
  ntop                  NTOP Web service
  ntp                   show current ntp status
  policy                Policy Map Table
  policy-map            Policy Map Table
  port                  Port status and configuration
  port-group            Port-group configuration
  port-mib              Port-Mib Count
  private-edge-vlan     Private edge vlan configuration
  privilege             Display your current level of privilege
  processes             Active process statistics
  qos                   Qos configuration
  rate-limit            Display rate-limit control parameters
  rmon                  Remote Monitoring
  route-map             route-map information
  running-config        Current operating configuration
  sdm                   Show SDM configuration
  self-loop-detection   Enable self-loop detection
  service-policy        service-policy information
  sflow                 sFlow
  snmp                  display snmp configuration
  spanning-tree         Spanning tree topology
  startup-config        Show startup config file information
  switchport            Switching port configuration
  syslog                syslog
  system                Display the system information
  tc-table              traffic-conditioner-table
  tech-support          Display general information about the switch
  temperature           Temperature and Threshold information
  track                 Tracking information
  uptime                Display elapsed time since boot
  users                 Display information about terminal lines
  version               Display the system version
  vlans                 VLAN information
  vrrp                  Virtual Router Redundancy Protocol (VRRP)
  whoami                Display information about the current user
Switch# show_
```

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

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

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

```
Switch# show p?
  pdp                   Global PDP configuration subcommands
  port                  Display port configuration
  port-group            Port group information
Switch# show p_
```

2.1.3. 단축 명령어 입력

Premier 8624XG 스위치의 CLI는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행을 지원한다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령을 수행한다.

Notice 단축 명령을 사용할 때, 시스템 운영자는 Premier 8624XG 스위치가 명령어를 구분하여 인식할 수 있도록 충분하게 입력해야 한다. "% Ambiguous command."라는 메시지를 받을 때가 있다. 이것은 해당 모드에 입력한 문자와 Prefix가 같은 하나 이상의 명령어가 있음을 의미한다.

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

Switch# show i ?
  ip                    IP information
  logging               Show all contents of logging buffers
Switch# show i_
```

2.1.4. 명령어 심볼

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

표 2-1. 명령어 구문 심볼

심볼	이름	설명
<>:	Angle brackets	■ 명령어 문법에서 하나의 변수 또는 값을 의미한다. 이렇게 표현된 파라미터는 반드시 입력을 해야 한다. ■ 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 한다.
{}:	Braces	■ 명령어 문법에서 사용되는 파라미터 또는 값의 리스트

심볼	이름	설명
		■ 시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 한다. ■ 예를 들어, 다음과 같은 명령어가 있을 때 `router {rip|ospf}` 시스템 운영자는 라우팅 프로토콜로서 RIP 또는 OSPF 중의 하나를 반드시 명시해야 한다.
[]:	Square brackets	■ 명령어 문법에서 사용되는 파라미터 또는 값의 리스트 ■ 시스템 운영자는 리스트에 포함된 항목 중에서 필요한 항목을 선택적으로 입력한다. 경우에 따라서는 하나도 입력을 하지 않을 수도 있다. ■ 예를 들어, 다음과 같은 명령어가 있을 때 `show interface [ifname]` 인터페이스의 이름을 정의하지 않을 수도 있다.
|:	Vertical bar	■ 파라미터 리스트에서 상호 배타적인 항목들을 표현
Italic 체		■ 입력할 변수들
Bold 체		■ 운영자가 입력해야 하는 명령어
A.B.C.D		■ IP 주소 또는 서브넷 마스크를 의미
A.B.C.D/M		■ IP prefix 를 의미 (예. 192.168.0.0/24)

2.1.5. 명령어 라인 편집 키 및 도움말

Premier 8624XG 스위치는 Emacs 와 유사한 편집 기능을 제공한다. <표 2-2>는 운영 단말이 제공하는 명령어 라인 편집 명령 및 도움말 기능을 설명한다.

표 2-2. 명령어 라인 편집 명령 및 도움말 기능

명령어	설명
[Ctrl] + [A]	■ 커서를 줄의 처음으로 이동
[Ctrl] + [E]	■ 커서를 줄의 끝으로 이동
[Ctrl] + [B]	■ 커서를 한 단어 뒤로 이동
[Ctrl] + [F]	■ 커서를 한 글자 앞으로 이동
Backspace	■ 커서 앞의 한 글자를 삭제
[Ctrl] + [K]	■ 현재 커서로부터 줄의 끝까지 문자를 삭제
[Ctrl] + [U]	■ 현재 커서로부터 줄의 처음까지 문자를 삭제
Tab	■ 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

2.2. 스위치 명령어 모드

Premier 8624XG 스위치는 <표 2-3>와 같이 다양한 스위치 명령어 모드를 지원한다. 각 스위치 명령어 모드마다 운영자에게 주어지는 권한에는 차이가 있다.

표 2-3. 스위치 명령어 모드

모드	프롬프트	설명
User 모드	`Switch >`	■ 보통 통계 정보를 디스플레이
Privileged 모드	`Switch #`	■ 시스템 설정을 출력하거나 시스템 관리 명령을 사용
Config 모드	`Switch (config) #`	■ 스위치의 환경 설정 값을 글로벌 하게 변경
Interface 모드	`Switch(config-if-gi1)#` `Switch(config-if-vlan1)#`	■ 인터페이스의 환경 설정을 변경
Router 모드	`Switch(config-rip)#` `Switch(config-ospf)#`	■ RIP 이나 OSPF 등의 라우팅 프로토콜의 환경 설정을 변경
DHCP pool 모드	`Switch(config-dhcp)#`	■ DHCP 주소 pool 을 설정

Notice 명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 Premier 8624XG 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 Premier 8624XG 스위치의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게

된다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 와 있는 지를 알려준다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 체크 해야만 한다. <표 2-4>은 스위치의 명령어 모드 사이의 이동 방법을 설명한다.

표 2-4. 스위치의 명령어 모드 사이의 이동

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

2.3. Premier 8624XG 스위치 가동

Premier 8624XG 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS image 를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.

Notice Premier 8624XG 스위치는 시스템 안정성을 위하여 Primary 및 Secondary 등 두 개의 OS image 를 관리한다. 기본적으로 Primary OS image 가 로드 되도록 설정되어 있으며, 운영자는 스위치의 boot 모드 또는 privileged 모드에서 이를 변경할 수 있다.

2.4. 사용자 인터페이스

시스템 운영자는 스위치의 환경을 설정하고, 환경 설정을 검증하고, 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속할 수 있다. 스위치에 접속하기 위한 가장 기본적인 방법은 Premier 8624XG 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것이다(*Out-of-band management*).

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

운영자는 아래의 방법을 사용하여 Premier 8624XG 스위치를 관리할 수 있다.

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

Premier 8624XG 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결
- 최대 10 개의 telnet 연결

2.4.1. 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능하다. 이를 위하여 운영 단말(또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9 핀, RS-232 DB9 포트를 지원해야 한다. 콘솔 포트는 Premier 8624XG 스위치의 경우 후면의 SGIM(Switching, Gigabit ethernet I/O & Management Module) 모듈에 탑재된다.

>과 같이 Premier 8624XG 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

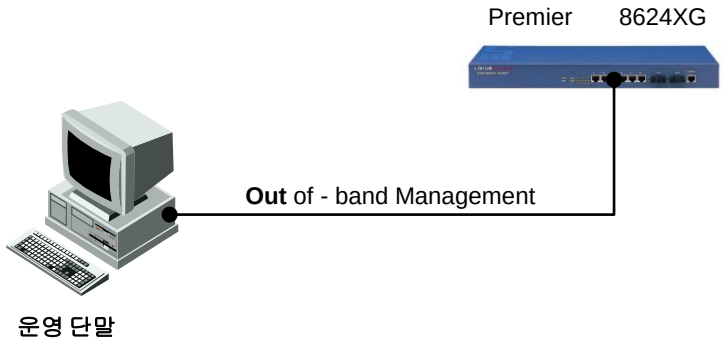


그림 2-1. Premier 8624XG 스위치와 운영 단말 연결

	Notice	운용 단말의 설정 방법 및 콘솔 포트 핀 설정은 Premier 8624XG 스위치 하드웨어 설치 가이드를 참조하기 바란다.

2.4.2. Telnet 연결

시스템 운영자는 TCP/IP 및 telnet 접속 기능을 가지고 있는 워크스테이션을 통하여 Premier 8624XG 스위치에 접속할 수 있다. Telnet 을 사용하기 위하여, 운영자는 ID 및 비밀번호를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 한다.

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

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

또한 시스템 보안을 위하여 액세스 리스트를 사용하여 telnet 에 연결하는 사용자를 제한할 수 있다. 이

는 <2.13. ACL(Access Control List)>절을 참조하라.

2.4.3. SNMP Network Manager 를 통한 연결

Simple Network Management Protocol (SNMP)를 지원하는 어떠한 네트워크 관리기(Network Manager)를 통해서도 Premier 8624XG 스위치를 관리할 수 있다.

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

2.5. 계정 관리 및 인증

2.5.1. 사용자 추가 및 삭제

시스템 운영자는 콘솔 포트나 telnet 을 통해서 스위치에 로그인 할 수 있다. 로그인을 위해서 사용자 등록이 필요하다. Premier 8624XG 스위치는 사용자를 추가, 삭제 할 수 있고 각각의 사용자에 대해 패스워드와 권한, session timeout 시간, Access List 를 지정할 수 있다.
사용자 권한은 privilege level 로 표현된다. privilege level 은 15 인 경우와 아닌 경우로만 구분하고, 0 에서 14 사이의 privilege level 간의 구분은 사용하지 않는다. privilege level 이 15 인 사용자는 enable mode 로 들어갈 수 있고, 그 외의 privilege level 을 갖는 사용자는 Privileged mode 로 들어갈 수 없다. 새로운 사용자를 등록하면 privilege level 이 1 인 사용자로 등록된다.

Notice Access List 에 대한 추가적인 정보는<2.8.ACL(Access Control List)>을 참조하라

표 2-5. 스위치의 사용자 추가 및 삭제 명령어

명령어	설명	모드
`username userID nopassword`	■ userID 생성 ■ password 가 없다	Config
`username userID password password` `username userID password 0 password`	■ userID 생성 ■ 암호화되지 않은 password 를 입력받는다	Config
`username userID password 7 password`	■ userID 생성 ■ 암호화된 password 를 입력받는다	Config

`username userID privilege <0-15> nopassword`	■ userID 생성 ■ password 가 없다 ■ privilege 15 이면 가장높은 privilege(privileged mode 진입허용)를 갖는다.	Config
`username userID privilege <0-15> password password` `username userID privilege <0-15> password 0 password`	■ userID 생성 ■ privilege 15 이면 가장높은 privilege(privileged mode 진입허용)를 갖는다. ■ 암호화되지 않은 password 를 입력받는다	Config
`username userID privilege <0-15> password 7 password`	■ userID 생성 ■ privilege 15 이면 가장높은 privilege(privileged mode 진입허용)를 갖는다. ■ 암호화된 password 를 입력받는다	Config
`username userID timeout <0-600>`	■ user 별 session timeout 시간(분) 설정(default 20 분)	Config
`no username userID timeout`	■ user 별 session timeout 시간(분) 삭제 ■ 초기 session timeout 시간(20 분)으로 되돌린다.	Config
`username userID access-class <1-99>`	■ 해당 user 에 Access List 를 적용 ■ *access-list-num* : <1-99> 이며, standard ip access list 를 의미	Config
`no username userID access-class`	■ 해당 user 에 적용된 Access List 를 해제.	Config
`no username userID`	■ userID 삭제 ■ userID 가 root 이면 삭제되지않고 password 가 default password 로 바뀐다.	Config

사용자 추가 및 삭제

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

```
username lns nopassword
username test password 7 xx1LtbDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
username admin timeout 50
!
Switch#
```

2.5.2. 패스워드 설정

Premier 8624XG 스위치는 시스템 보안을 위해 다음과 같은 2 개의 패스워드를 사용한다.

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

표 2-6. 스위치의 Enable 패스워드 설정 명령어

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

Notice 사용자 패스워드 설정명령은 <2.5.1. 사용자 추가 및 삭제>를 참고하라

Privileged 모드 패스워드 설정

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

패스워드 encryption 설정

위의 예에서 보듯이 패스워드 설정 후 `show running-config` 명령으로 설정된 패스워드를 볼 수 있다. 이를 방지하기 위하여 Premier 8624XG 스위치는 패스워드 encryption 모드 설정을 지원한다.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJIgc
username lns nopassword
username test password 7 XX1LtbDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
!
Switch#
```

2.5.3. 인증 방법 설정

2.5.3.1. 스위치에 login 시 인증 방법 설정

Premier 8624XG series 스위치는 시스템에 접속하는 사용자에 대한 인증 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 사용자의 ID 와 패스워드를 사용하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 RADIUS 와 TACACS+등을 이용하도록 설정하면 각각의 서버가 가지고 있는 데이터베이스에 기록된 사용자 정보를 사용하여 접속 권한이 주어진다.

표 2-7. 사용자 인증 설정 명령어

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

`no authentication login primary (local | radius | tacacs)`	■ 우선적으로 인증받도록 설정한 인증방식을 해제한다.	Config
`authentication login template-user` *`userID`*	■ radius 나 tacacs 로 인증받은 경우 Dummy user 를 지정할 수 있다. ■ 지정하는 Dummy user 는 local database 에 등록되어 있어야 한다.	Config
`no authentication login template-user`	■ 설정한 Dummy user 를 해제한다.	Config
`show authentication login`	■ 인증방식의 순서와 사용여부를 보여준다	Privileged

사용자 인증 설정

Premier 8624XG 스위치는 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 사용자 ID 와 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 RADIUS 서버를 이용하는 방법, TACACS+ 서버를 이용하는 방법이 있다. 이 3 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다.
한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID 와 패스워드를 다시 요청한다. RADIUS 나 TACACS+ 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID 와 패스워드를 다시 요청한다.

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

Switch#
```

2.5.3.2. privileged mode 진입시 인증 방법 설정

Premier 8624XG series 스위치는 privileged mode 로 들어올 때 사용자에 대한 인증 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 enable 패스워드를 사용하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 TACACS+를 이용하도록 설정하면 각각의 서버가 가지고 있는 데이터

베이스에 기록된 정보를 사용하여 접속 권한이 주어진다.

표 2-8. privileged mode 사용자 인증 설정 명령어

명령어	설명	모드
`authentication enable enable (local | tacacs)`	■ 사용할 인증방식(local, tacacs)을 선택한다. ■ 여러가지 인증방식을 선택할 수 있다.	Config
`no authentication enable enable (tacacs)`	■ 사용하도록 설정된 인증방식을 사용하지 않도록 설정한다. ■ local 인증방식은 항상 사용한다.	Config
`authentication enable primary (local | tacacs)`	■ 우선적으로 인증받을 인증방식을 설정한다.	Config
`no authentication enable primary (local | tacacs)`	■ 우선적으로 인증받도록 설정한 인증방식을 해제한다.	Config
`show authentication enable`	■ 인증방식의 순서와 사용여부를 보여준다	Privileged

privileged mode 사용자 인증 설정

Premier 8624XG 스위치는 privileged mode 로 들어올 때 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 enable 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 TACACS+ 서버를 이용하는 방법이 있다. 이 2 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다.
한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 enable 패스워드를 다시 요청한다. TACACS+ 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 enable 패스워드를 다시 요청한다.

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

Switch#
```

2.5.4. 권한 부여

2.5.4.1. 사용자 권한 부여

Premier 8624XG series 스위치는 시스템에 접속하는 사용자에 대한 권한 부여 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 사용자의 privilege level 을 따르지만, 사용자 인증 프로토콜인 RADIUS 와 TACACS+등을 이용하여 login 한 경우 각각의 서버가 가지고 있는 데이터베이스에 기록된 사용자 정보를 사용하여 privilege level 이 주어진다.

표 2-9. 사용자 권한 부여 설정 명령어

명령어	설명	모드
`authorization exec (tacacs | radius)`	■ tacacs 또는 radius 서버를 통하여 인증받은 경우 해당 서버에서 privilege level 을 얻어온다. ■ local 방식은 항상 사용한다.	Config
`no authorization exec (tacacs | radius)`	■ tacacs 또는 radius 서버에서 privilege level 을 얻어오지 않도록 한다. ■ local 방식은 항상 사용한다.	Config

사용자 권한 부여 설정

Premier 8624XG 스위치는 사용자 권한 부여 방법으로 기존의 스위치에 등록되어 있는 사용자 privilege 를 받는 방법과 RADIUS 서버를 이용하는 방법, TACACS+ 서버를 이용하는 방법이 있다. 이 3 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다
한가지 이상의 방법을 사용할 경우 우선순위는 <2.5.3.1. 스위치에 login 시 인증 방법 설정>의 우선순위를 따른다.

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

2.5.4.2. 명령어 권한 허가

Premier 8624XG series 스위치는 명령어 실행 전에 TACACS+ 서버로 권한 허가를 요청 할 수 있다.

표 2-10. 명령어 모드 권한 설정 명령어

명령어	설명	모드
privilege (user-mode | privileged-mode | config-mode | interface-mode | router-mode | dhcp-mode) level <0-15>	■ 해당 모드에서 실행되는 명령어의 privilege level 을 변경한다. ■ <0-15> : 명령어의 privilege level 을 의미.	Config
no privilege (user-mode | privileged-mode | config-mode | interface-mode | router-mode | dhcp-mode) level	■ 해당 모드에서 실행되는 명령어의 privilege level 을 기본값으로 복원한다.	Config
show mode privilege	■ 명령어 모드 별로 설정된 privilege level 을 보여준다.	Privileged

표 2-11. 명령어 권한허가 설정 명령어

명령어	설명	모드
authorization commands <0-15> tacacs	■ 해당 privilege level 을 갖는 명령어를 실행하기 전에 tacacs+ 서버에 권한 허가를 요청하도록 설정한다. ■ <0-15> : 명령어의 privilege level 을 의미.	Config
no authorization commands <0-15> tacacs	■ tacacs+ 서버에 권한 허가를 요청하지 않도록 설정한다. ■ <0-15> : 명령어의 privilege level 을 의미.	Config

명령어 권한 허가 설정

Premier 8624XG 스위치는 명령어 권한 허가 방법으로 TACACS+ 서버를 이용한다.
명령어 모드 별로 privilege level 을 부여하고, 부여한 privilege level 별로 권한 허가 요청 여부를 설정한다.

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

```
interface-mode          15
router-mode             15
dhcp-mode               15
Switch#
```

2.5.5. 계정 관리

2.5.5.1. 세션 관리

Premier 8624XG series 스위치는 TACACS+ 서버에 시스템 접속 내역을 기록할 수 있다.

표 2-12. 세션 관리 설정 명령어

명령어	설명	모드
accounting exec (start-stop | stop-only) tacacs	■ 시스템 접속 내역을 tacacs+ 서버에 기록 한다. ■ start-stop : 세션 시작과 끝을 모두 기록 ■ stop-only : 세션 끝만 기록.	Config
no accounting exec	■ tacacs 시스템 접속 내역을 tacacs+ 서버에 기록하지 않는다.	Config

세션 관리 설정

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

2.5.5.2. 명령어 관리

Premier 8624XG series 스위치는 TACACS+ 서버에 명령어 실행 내역을 기록할 수 있다.

표 2-13. 명령어 관리 설정 명령어

명령어	설명	모드
accounting commands <0-15> stop-only tacacs	■ 해당 privilege level 을 갖는 명령어의 실행 내역을 tacacs+ 서버에 기록 한다. ■ <0-15> : 명령어의 privilege level 를 의	Config

	미.	
no accounting commands <0-15>	■ 해당 privilege level 을 갖는 명령어의 실행 내역을 tacacs+ 서버에 기록하지 않는다. ■ <0-15> : 명령어의 privilege level 를 의미.	Config

명령어 관리 설정

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

2.5.6. 인증 서버 설정

표 2-14. RADIUS 서버 설정 명령어

명령어	설명	모드
radius-server host A.B.C.D	■ radius-server 설정한다.	Config
no radius-server host A.B.C.D	■ 설정된 radius-server 삭제한다.	Config
radius-server host A.B.C.D key *encryption-key*	■ radius-server 설정한다. ■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.	Config
radius-server host A.B.C.D auth-port <0-65536>	■ radius-server 설정한다. ■ 해당 server 에 접속할 때 사용하는 auth-port 를 설정한다.	Config
no radius-server host A.B.C.D auth-port	■ 해당 server 에 접속할 때 사용하는 auth-port 를 삭제한다.(삭제되면 default auth-port 를 사용한다.)	Config
radius-server host A.B.C.D auth-port <0-65536> key *encryption-key*	■ radius-server 설정한다. ■ 해당 server 에 접속할 때 사용하는 auth-port 를 설정한다. ■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.	Config
radius-server key *encryption-key*	■ radius-server 에 접속할 때 사용하는 general key 설정한다. ■ server 에 key 가 지정되지 않으면 이 general key 를 사용한다.	Config

`no radius-server key`	■ 설정된 general key 를 삭제한다.	Config
`radius-server retransmit <1-5>`	■ radius-server 에 접속할 때의 재시도 횟수를 설정한다.	Config
`no radius-server retransmit`	■ 설정된 재시도 횟수를 삭제한다.(default 3 회)	Config
`radius-server timeout <1-1000>`	■ 응답 페킷을 받아야하는 시간을 지정한다.	Config
`no radius-server timeout`	■ 설정된 timeout 시간을 삭제한다.(default 5 초)	Config

RADIUS 서버 설정

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

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

표 2-15. TACACS+ 서버 설정 명령어

명령어	설명	모드
`tacacs-server host A.B.C.D key` *`encryption-key`*	■ tacacs -server 설정한다. ■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.	Config
`no tacacs-server host A.B.C.D`	■ 설정된 tacacs -server 삭제한다.	Config
`tacacs-server host A.B.C.D timeout <1-1000> key` *`encryption-key`*	■ tacacs -server 설정한다. ■ 응답 페킷을 받아야하는 시간 `timeout` 을 지정한다. ■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다	Config

`tacacs-server host A.B.C.D timeout <1-1000>`	■ tacacs -server 설정한다. ■ 응답 패킷을 받아야하는 시간 `timeout` 을 지정한다.	Config

TACACS+ 서버 설정

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

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

2.6. Hostname 설정

Hostname 은 운영 시 시스템을 구별하기 위해 사용될 수 있으며 따라서 콘솔/Telnet 화면의 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있다. Premier 8624XG 스위치는 default 로 시스템의 모델명을 hostname 으로 사용하며 운영자가 이를 변경할 수 있다.

표 2-16. Hostname 설정 명령어

명령어	설명	모드
`hostname` *`string`*	■ Hostname 을 변경	Config
`no hostname`	■ Hostname 을 default 값으로 변경	Config

Hostname 을 설정 및 변경하는 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# hostname P8624XG
P8624XG(config)# end
P8624XG#
  .....

P8624XG# configure terminal
P8624XG(config)# no hostname
Switch(config)# end
Switch#
```

2.7. SNMP(Simple Network Management Protocol)

SNMP Network Manager 는 Management Information Base(MIB)을 제공하는 스위치를 관리할 수 있다. 각각의 Network Manager 는 관리의 편이를 위해서 사용자 인터페이스를 제공한다. SNMP manager 로 Premier 8624XG 스위치를 관리하고자 할 때는 스위치의 환경 설정이 필요하다.

또한 SNMP 에이전트를 접근하기 위해서는 스위치에 하나 이상의 IP 주소 설정이 필요하다. IP 주소의 설정은 "*P8624XG Series_User Guide_제 05 장_IP 환경 설정*" 문서를 참고하라.

표 2-17. SNMP 환경 설정 명령

명령어	설명	모드
`snmp-server contact` *string*	■ System contact 정보를 변경	Config
`snmp-server location` *string*	■ System location 정보를 변경	Config

`snmp-server community` *string*
`[ro|rw`
`[host` *A.B.C.D/M*`]|`
`[access-class` *<1-99>*`]]`
	■ SNMP community 를 설정
	■ *ro* : read only
	■ *rw* : read write
	■ *A.B.C.D /M* : host IP address / prefix length
		Config

	■ <*1-99*> : standard IP access-list	
`no snmp-server community` *`string`*	■ SNMP Community 를 삭제	Config
`snmp-server enable traps` [*`notification-type`*] [*`notification-option`*]	■ SNMP Trap 을 Trap-Host 에게 전송하도록 설정 ■ *`notification-type`*: trap 그룹 (config, environ, multicast, other, perform, resource, security, snmp) ■ *`notification-option`*: 각 trap 그룹에 속한 개별 trap 항목	Config
`no snmp-server enable traps`	■ SNMP Trap 을 Trap-Host 에게 전송하지 않도록 설정	Config
`snmp-server trap-host` *`A.B.C.D community string`*	■ SNMP Trap Host 와 trap 을 전송할 때 사용할 community 를 설정	Config
`no snmp-server trap-host` *`A.B.C.D`*	■ SNMP Trap Host 를 삭제	Config
`snmp-server agent-address` *`A.B.C.D`*	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정	Config
`no snmp-server agent-address`	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정하지 않음	Config
`snmp-server trap-enterprise-oid lnsNotificationMIB`	■ SNMP Trap 의 enterprise OID 를 `lnsNotificationMIB` 으로 설정	Config
`no snmp-server trap-enterprise-oid`	■ SNMP Trap 의 enterprise OID 를 개별 trap 항목으로 설정	Config
`snmp-server trap-version 2`	■ SNMPv2 Trap 을 전송하도록 설정	Config
`no snmp-server trap-version`	■ SNMPv1 Trap 을 전송하도록 설정	Config
`show snmp [trap]`	■ snmp 설정을 출력 ■ trap: snmp trap 설정 출력	Privileged

Notice Premier 8624XG Series 에서 'show snmp [trap]]'명령을 지원하지 않는 스위치가 있을 수 있다.

SNMP Community 설정

Community string 은 시스템과 원격 Network Manager 사이의 간단한 상호 인증 기능을 제공한다. Premier 8624XG 스위치는 두 가지 형태의 community string 을 지원한다.

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

- 시스템에 읽기 및 쓰기(read and write) 접속
- 기본 읽기 및 쓰기 설정은 private

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

Notice access-class 설정은 < 2.9.ACL >절을 참고하라

SNMP Trap 설정

하나 이상의 네트워크 관리 단말이 인증된 trap receiver 로서 설정될 수 있다. Premier 8624XG 스위치는 모든 trap receiver 에게 SNMP trap 을 전송한다.

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

```
Switch#
```

Notice

Premier 8624XG Series 에서 지원하는 SNMP Trap 은 모든 스위치를 포괄한다. 'snmp-server enable traps' 명령으로 모든 SNMP Trap 을 설정할 경우 현재 스위치에서 지원하지 않는 SNMP Trap 의 내용도 running-config 에 포함될 수 있다.

SNMP 패킷의 출발지 IP 설정

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

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

SNMP Trap enterprise - oid 설정

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

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

시스템 담당자 설정

시스템을 관리하는 책임을 가지는 사람을 등록할 수 있다.

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

시스템 구축 위치 설정

```
Switch# configure terminal
```

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

2.8. ACL(Access Control List)

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

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

표 2-18. 액세스 리스트 설정 명령

명령어	설명	모드
access-list <1-99> {**deny|permit**} *address*	■ 표준 IP 액세스 리스트를 설정 ■ Source address/network 만을 설정 ■ *address* ::= {any | A.B.C.D A.B.C.D | host A.B.C.D}	Config
no access-list <1-99>	■ 액세스 리스트를 삭제	Config

2.8.1. 액세스 리스트 생성 규칙

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

2.8.2. 표준 IP 액세스 리스트 설정

2.8.2.1. 모든 액세스 허용

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

2.8.2.2. 모든 액세스 거부

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

2.8.2.3. 특정 호스트에서의 액세스만 허용

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

2.8.2.4. 특정 네트워크에서의 액세스만 허용

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

2.8.2.5. 특정 네트워크에서의 액세스만 거부

```
Switch# configure terminal
Switch(config)# access-list 1 deny 192.168.0.1 255.255.255.0
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch#  show running-config
!
access-list 1 deny 192.168.0.0 255.255.255.0
access-list 1 permit any
!
```

2.8.3. Telnet 연결에 액세스 리스트 설정

엑세스 리스트는 user 별로 적용되며, 설정된 엑세스 리스트는 외부에서 스위치로의 접속을 허용, 제한한다.
192.168.0.0/24 네트워크에서의 접속만을 허용하는 Access list 를 생성하여, telnet 접속을 제한하고자 할 때의 절차는 다음과 같다.

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

2.9. NTP 설정

2.9.1. NTP 개요

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

2.9.2. NTP client mode 설정

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

명령어	설명
ntp server *address*	■ NTP server 를 설정한다. (5 개까지 설정가능)
no ntp server *address*	■ NTP server 를 삭제한다.

2.9.3. NTP Server mode 설정

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

명령어	설명
ntp master *stratum <1-15>*	■ NTP master 로 동작하도록 한다.
no ntp master	■ NTP master 로서의 동작을 멈춘다.

2.9.4. NTP time zone 설정

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

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

2.9.5. NTP summer time 설정

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

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

2.9.6. NTP 기타 명령어

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

2.9.7. NTP 설정 예제

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

```
-----------------------------------------
[1] 203.248.240.103
-----------------------------------------
Switch #
```

3

인터페이스 환경 설정

3.1. 개요

Premier 8624XG 스위치가 지원하는 인터페이스는 다음과 같다.

표 3-1. Premier 8624XG 스위치가 지원하는 인터페이스

구분	종류
Physical interfaces	■ Gigabit Ethernet • 100Base-TX • 100Base-FX • 1000Base-T • 1000Base-X ■ 10 Gigabit Ethernet • 10000Base-X
port-group interfaces	■ Port-group
VLAN Interfaces	■ VLAN
Loopback interface	■ Loopback
Management interface	■ Out of band interface for management

모든 인터페이스 환경 설정은 다음과 같이 진행된다.

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

3.2. 공통 명령어

인터페이스 환경 설정에 공통으로 적용되는 명령어는 다음과 같다.

표 3-2. 공통 명령어

명령어	설명
interface *ifname*	■ Interface 모드로 진입. ■ *ifname*: 환경을 설정할 특정 인터페이스의 이름.
Description *string*	■ Interface comment ■ *string*: 인터페이스에 대한 주석으로 80 자 이내의 문자열

3.2.1. Interface name

Premier 8624XG Series 에서는 인터페이스에 대한 모든 환경 설정에서 interface name을 사용한다. Interface name은 다음과 같이 interface type과id로 구성된다.

표 3-3. Interface name

구분	Interface type	Interface name	예
Physical interface	Gigabit Ethernet	“gi” + port_id	gi1
	10 Gigabit Ethernet	“gi” + port_id	gi25
Port-group interface	Port group	“po” + port-group id	po1
VLAN interface	VLAN	“vlan” + vlan id	vlan10
Loopback interface	Loopback	“lo” + id	lo0
Management interface	Fast Ethernet	“eth” + id	eth0

3.2.2. Interface id

Interface name은interface type과id로 구성되며 interface id는Premier 8624XG 스위치 각 모델마다 다르다. <표3-4>은 각 모델별 interface id의 표기 방법과 지원하는 범위를 보여준다.

표 3-4. Interface ID 및 지원 범위

Model	Interface Type	ID 구성	ID Range	Name(예)
P8024XG	Fast ethernet	slot id /port id	slot id: 1-6 port id: 1-4	fa1/1, fa1/4, fa6/1, fa6/4
	Gigabit ethernet	slot id/port id	slot: 7-8 port id: 1-2	gi7/1, gi7/2
	Port group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	Loopback	interface id	0 – 3	lo0, lo3
	management	interface id	0	eth0
P8024G	Fast ethernet	slot id /port id	slot id: 2 port id: 1-24	fa2/1, fa2/24

	Gigabit ethernet	slot id/port id	slot: 1 port id: 1-2	gi1/1, gi1/2
	Port group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	Loopback	interface id	0 – 3	lo0, lo3
	management	interface id	0	eth0
P808FG	Fast Ethernet	slot id /port id	FE-TX slot id: 1 port id: 1-6	fa1/1, fa1/6
	Gigabit Ethernet	slot id /port id	slot id : 2-3 port id : 1	gi2/1, gi3/1
	Port group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	Loopback	interface id	0 – 3	lo0, lo3
	management	interface id	eth0	eth0
P8124XG	Fast ethernet	slot id /port id	slot id: 2-4 port id: 1-8	fa2/1 fa4/8
	Gigabit ethernet	slot id/port id	slot id: 1 port id: 1-2	gi1/1, gi1/2
	Port group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	Loopback	interface id	0 – 3	lo0, lo3
	management	interface id	0	eth0
P8524XG	Gigabit ethernet	slot id /port id	slot id: 1-3 port id: 1-8	gi1/1 gi3/8
	Port group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	Loopback	interface id	0 – 3	lo0, lo3
	management	interface id	0	eth0
P8624XG	Gigabit ethernet	port id	port id: 1-24	gi1, gi24
	10Gigabit ethernet	port id	port id: 25-26	gi25, gi26
	Porg group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	LoopBack	interface id	0 – 3	lo0, lo3
	management	interface id	0	eth0

3.2.3. Interface 모드 프롬프트

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

```
Switch(config-if-gi1)#
```

3.2.4. Description 명령어

각 인터페이스에 대한 설명을 추가한다. 이는 단지 운영자의 기억을 돕기 위한 comment에 불과하며 **show interfaces** 명령을 사용하면 그 결과를 볼 수 있다.

3.3. 인터페이스 정보 및 상태 조회

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

표 3-5. 인터페이스 정보 및 상태 관련 명령어

명령어	설명	모드
show interface [*ifname*]	■ interface 의 status, configuration 출력	Privileged
show port status	■ 모든 physical interface 의 status 출력	Privileged
show switchport	■ physical/port-group interface 의 switchport 정보 출력	Privileged

3.3.1. show interface 명령어

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

```
Switch# show interface
gi1 is down
type 1000Base-GBIC,LC, 10,000M, 1,490nm
gbic inserted
vendor EZCONN
part name ETB43341-8LNT
Rev No Info
SN R00169
Date 061218
gbic diagnostic
temperature 47.0 'C   vcc 3.25 Volt
rx power -inf dBm   tx power -6.10 dBm
bias   14.1 mA
no auto-negotiation
speed set 1G
duplex set full
vlan ingress check enabled

Last clearing of counters 00:03:54
```

```
1 minutes input rate 0 bytes/sec, 0 packets/sec
1 minutes output rate 0 bytes/sec, 0 packets/sec
0 packets input, 0 bytes
Received 0 broadcasts, 0 multicasts
0 CRC, 0 oversize, 0 dropped
       0 packets output, 0 bytes
       Sent 0 broadcasts, 0 multicasts
```

3.3.2. show port status 명령어

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

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

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

3.3.3. show switchport 명령어

Switchport란2계층 스위칭 모드로 동작하는 port및port-group을 말한다. **Show switchport** 명령어는 물리적 포트 및port-group의switchport 정보가 출력된다. Switchport 정보에는 mode, native및tagged vlan list 등이 포함된다.

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

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

3.4. 물리적 포트 환경 설정

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

표 3-6. 물리적 포트 환경 설정 명령어

명령어	설명	모드
shutdown **no shutdown**	■ 물리적 포트를 disable/enable	interface
auto-negotiation **no auto-negotiation**	■ Enable/Disable speed auto-negotiation.	Interface
speed (10|100|1000) **speed auto**	■ speed 설정	interface
duplex (full-duplex|half-duplex) **duplex auto**	■ duplex mode 설정	interface
flow-control **no flow-control**	■ flow-control 설정/해제	interface

3.4.1. Shutdown

물리적 포트를 disable시킨다.

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

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface gi1
Switch(config-if-gi1)# shutdown              <- disable port
Switch(config-if-gi1)# no shutdown           <- enable port
```

3.4.2. Block

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

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface gi1
Switch(config-if-gi1)# block              <- block port
Switch(config-if-gi1)# no block           <- unblock port
```

3.4.3. Speed an duplex

Premier 8624XG Series에서 각 interface 지원하는 speed는 다음과 같다.

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

speed, duplex 설정시 다음 사항을 주의하라.

- 100Base-FX 의 경우 speed 설정은 없다.
- 1000Base-X 의 경우 speed 설정은 없고 단지 auto-negotiation off/off 만 설정가능하며 auto-negotiation on 시 광케이블이 하나만 단절되어도 양쪽에 모두 link down 이 감지된다. (remote fault 감지)
- 만약에 양쪽이 auto-negotiation 을 지원하면, auto-nego 를 권장한다. 단, 한쪽이라도 auto 모드를 지원하지 않으면 양쪽 모두 manual 로 사용한다.

3.4.4. Media Type

Premier 8624XG Series 의 gi21, gi22, gi23, gi24 포트들은 RJ45 와 SFP 을 지원하는 Combo 포트이다. Combo 포트의 media type 을 결정하기 위해, 각 인터페이스 모드에서 media-type 명령어를 사용한다. 물리적 포트의 media type 을 확인하려면 show port status 명령어를 사용한다. Combo 포트의 디폴트 media type 은 RJ45 이다.

표 3-7. media-type 설정 명령어

명령어	설명	모드
media-type *type*	■ Combo 포트의 media type 을 *type* (rj45 | sfp) 으로 변경	interface
no media-type	■ Combo 포트의 media type 을 디폴트 type 인 rj45 로 변경	interface

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

3.5. Storm Control

Storm Control이란 broadcast/multicast/unicast storm으로 인한 시스템의 과부하를 방지하기 위하여 브로드캐스트/멀티캐스트/유니캐스트 트래픽이 시스템에 유입되는 것을 제한하는 기능을 말한다. Broadcast/multicast/unicast storm은broadcast/multicast/unicast 패킷이 서브넷에 flooding되어 과다한 트래픽으로 인한 네트워크의 성능을 저하시키는 현상을 말하며 프로토콜 스택 구현상의 오류나 네트워크 환경 설정의 오류가 이런 현상을 유발시킬 수 있다.
Premier 8624XG Series는input port의broadcast/multicast/unicast packet을 양을 측정하여 이를 설정된 threshold와 비교 그 이상의 브로드캐스트/멀티캐스트/유니캐스트 트래픽은 시스템에 유입시키지 않고 폐기한다.

명령어	설명	모드
storm-control level *value*	■ Storm Control 의 레벨을 총 Bandwidth 의 퍼센트로 설정	interface
no storm-control	■ Storm Control 해제	interface
storm-control broadcast	■ Storm Control 대상에 Broadcast packet 를 포함	interface
no storm-control broadcast	■ Storm Control 대상에서 Broadcast packet 를 제거	interface
storm-control multicast	■ Storm Control 시 Multicast packet 를 포함	interface
no storm-control multicast	■ Storm Control 대상에서 Broadcast packet 를 제거	interface
storm-control unicast	■ Storm Control 시 Unicast packet 를 포함	interface
no storm-control unicast	■ Storm Control 대상에 Unicast Packet 를 제거	interface

3.6. Port mirroring

Port mirroring은 특정 port(source port)의 입출력 트래픽을 운용자가 설정한 목적지 포트에 mirroring하는 기능으로 원하는 포트의 모든 패킷을 감시할 수 있다.
Premier 8624XG Series는rx, tx 트래픽을 각각 여러 소스 포트로부터1개의 port 혹은 cpu로mirroring할 수 있다.

명령어	설명	모드
mirroring rx-target *ifname <0-7>*	■ 입력 패킷이 mirroring 될 port 를 지정	config
mirroring tx-target *ifname <0-7>*	■ 출력 패킷이 mirroring 될 port 를 지정	config
mirroring rx-target cpu	■ 입력되는 패킷을 cpu 로 mirroring	config
mirroring tx-target cpu	■ 출력되는 패킷을 cpu 로 mirroring	config
mirroring rx-traffic	■ 해당 포트의 입력 패킷을 mirroring	interface

mirroring tx-traffic	하도록 설정 ■ 해당 포트의 출력 패킷을 mirroring 하도록 설정 interface

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

3.7. 2 계층 인터페이스 환경 설정

2계층 인터페이스는2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 Premier 8624XG 스위치에서는 물리적 포트와 port-group interface가 이 모드로 동작한다.
이 절에서는2계층 인터페이스의 설명과 물리적 포트와 port-group을2계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여준다.

3.7.1. VLAN Trunking

트렁크(trunk)란 이더넷 스위치와 다른 네트워킹 장비(router, switch) 사이의 point-to-point 링크로서 단일 링크에 복수의 VLAN 트래픽을 전송할 수 있으며 이를 통하여 VLAN을 전체 네트워크에 확장할 수 있다.
Premier 8624XG 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에trunk을 설정할 수 있다.

3.7.2. 2 계층 인터페이스 모드

Premier 8624XG 스위치가 지원하는2계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있다.

표 7. Premier 8624XG 스위치가 지원하는 2 계층 인터페이스 모드

모드	설명
switchport mode access	■ non trunking mode. ■ native vlan 만 설정 가능
switchport mode trunk	■ trunking mode. ■ 하나의 native VLAN 과 다수의 tagged VLAN 설정 가능

3.7.3. 2 계층 인터페이스 기본 설정 값

Premier 8624XG 스위치는 물리적 포트 또는 port-group이layer2 interface로 설정될 때 다음과 같은 기본(default) 설정 값을 가진다.

표 3-8. 2 계층 인터페이스 기본 설정 값

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

3.7.4. 2 계층 인터페이스 설정/해제

2계층 인터페이스로 설정 및 해제하기 위한 명령어는 다음과 같다.

표 3-9. 2 계층 인터페이스 설정 및 해제 명령어

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

인터페이스가 최초로2계층 인터페이스로 설정되면2계층 인터페이스 기본 설정 값을 가지게 되며2계층 인터페이스 설정이 해제되면 VLAN 설정 값은 모두 해제된다. 2계층 인터페이스 해제는 물리적 포트를 port-grouping하고자 할 때 적용한다.

Notice **Premier 8624XG 스위치의 초기 설정은 모든 물리적 포트가 2 계층 인터페이스로 되어 있다.**

3.7.5. Trunk port 설정

물리적 포트 또는 port-group 인터페이스를2계층 트렁크 포트(layer2 trunk port)로 설정하기 위한 명령어는 다음과 같다.

표 3-10. Trunk port 설정 명령어

명령어	설명	모드
switchport mode trunk	■ trunk mode 설정	interface
switchport trunk native *<1-4094>*	■ trunk port native VLAN 설정	interface
no switchport trunk native	■ trunk port native VLAN 을 default 로 설정	interface
switchport trunk add *<2-4094>*	■ trunk port tagged VLAN 등록	interface

switchport trunk remove *<2-4094>* **switchport trunk remove all**	■ trunk port tagged VLAN 삭제	interface

다음은 물리적 포트를2계층 트렁크 포트로 설정하는 예이다.

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

다음은 port-group 인터페이스를2계층 트렁크 포트로 설정하는 예이다.

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

3.7.6. Access port 설정

물리적 포트 또는 port-group 인터페이스를2계층 access port로 설정하기 위한 명령어는 다음과 같다.

표 3-11. Access port 설정 명령어

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

다음은 물리적 포트를2계층 access port로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport             ! layer2 interface set
Switch(config-if-gi1)# switchport mode access    ! access port set
Switch(config-if-gi1)# switchport access vlan 5  ! native vlan set
```

다음은 port-group 인터페이스를2계층 access port로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface po2
```

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

3.8. Port group

3.8.1. Port group 개요

Port group 이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용한다. Premier 8624XG 스위치에서 port group 인터페이스는2계층 인터페이스로 사용될 수 있다.
Premier 8624XG 스위치의 모델별 설정 가능한 port group 수는 다음과 같다.

모델	port group 수	그룹 당 최대 port
P8624XG Series	30	8

3.8.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같다.

표 3-12. 포트 그룹 설정 명령어

명령어	설명	모드
port-group *ifname* **protocol none**	■ static port group 을 생성한다.	config
port-group *ifname* **protocol lacp**	■ LACP 로 동작하는 port group 을 생성한다.	config
no port-group *ifname*	■ port-group 을 삭제한다	config
port-group lb-mode layer2	■ load-balance 시 MAC 주소를 참조.	config
port-group lb-mode layer3	■ load-balance 시 ip field 를 참조.	config
port-group lb-mode layer4	■ load-balance 시 tcp/udp port 참조	config
port-group *ifname* **no port-group**	■ port group 설정 ■ port group 해제	Interface *
show port-group	■ port group 설정 출력	Privileged

3.9. MAC Filtering

3.9.1. MAC Filtering 개요

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

3.9.2. MAC Filtering 설정

MAC Filtering 설정을 위한 기본 명령어는 다음과 같다.

표 3-13. 3 계층 인터페이스 환경 설정 명령어

명령어	설명	모드
mac-filter *vlan-id mac-addr* **(all-drop | dst-drop | trap)**	■ MAC Filter add	config
no mac-filter *vlan-id mac-addr*	■ MAC Filter delete	config

3.10. CPU Load 에 따른 MAC Filtering

3.10.1. CPU Load 에 따른 MAC Filtering 개요

8624XG Series에서 현재 CPU상태에 따라서 설정된 VLAN에 MAC Filtering 기능을 수행할 수 있다. 이로 인해서 특정 Rate가 넘는 Source MAC에 대해서 지정된 시간만큼 트래픽을 허용하지 않는다. 따라서 특정 트래픽이 과도한 Rate를 점유하는 등의 비정상적인 행동에 대해서 사전에 미리 차단할 수 있게 된다.

3.10.2. CPU Load 에 따른 MAC Filtering 설정

표 3-14. CPU-MAC-FILTER 관련 명령어

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

no cpu-mac-filter (broadcat|multicast)	■ 특정 vlan 에 대해서 broadcast/multicast 패킷에 대한 cpu-mac-filter 기능을 Disable 시킨다.	Interface
cpu-mac-filter cpu-load <1-99>	■ MAC-filtering 을 적용시킬 CPU Load threshold 를 설정한다.	config
no cpu-mac-filter cpu-load	■ MAC-filtering 을 적용시킬 CPU Load threshold 를 default 로 설정한다.	config
cpu-mac-filter packet-threshold <1-5000>	■ MAC-filtering 을 적용시킬 MAC 에 대한 Threshold Rate 를 설정한다.	config
no cpu-mac-filter packet-threshold	■ MAC-filtering 을 적용시킬 MAC 에 대한 Threshold Rate 를 default 로 설정한다.	config
cpu-mac-filter duration <1-1440>	■ MAC-filtering 을 적용시킬 blocking duration time 에 대해서 분단위로 설정한다.	config
no cpu-mac-filter duration	■ MAC-filtering 을 적용시킬 blocking duration time 에 대해서 default 로 설정한다.	config
clear cpu-mac-filter <1-4094>	■ Cpu-mac-filter 가 설정된 vlan Interface 에 대한 Filtering 정보를 초기화 시킨다.	privileged
show cpu-mac-filter information	■ Cpu-mac-filter 의 설정정보 및 설정된 Interface 에 대해서 보여준다.	privileged
show cpu-mac-filter table	■ 현재 mac-filtering 이 적용된 source mac 에 대한 정보를 보여준다.	privileged

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

3.11. Switching Database Manager

3.11.1. SDM 개요

TCAM은 8624XG Series에서 고속으로 Forwarding Table Lookup하기 위한 특별한 메모리로 볼 수 있고, Switching Database Manager (SDM)은 Ternary Content Addressable Memory (TCAM)에 저장되어 지는 Layer2와 Layer3의 Switching Information에 대해서 관리하는 역할을 한다. 이 장에서는 TCAM의 자원을 효과적으로 관리하기 위한 SDM의 설정 방법에 대해서 알아본다.

3.11.2. SDM 설정

8624XGSevies 에서는 4 종류의 SDM 모드를 지원하며, 각 모드는 각각의 특별한 Forwarding Entry 에 더 많은 Memory 를 할당 하게 된다. 예를 들어 “qos mode”의 경우 는 Traffic Conditioner 를 통해 전달되는 Entry 에 더 많은 Memory 를 할당 하게 되고, “route mode”의 경우는 Next Hop 을 통해 전달되는 Entry 에 더 많은 Memory 를 할당 하게 된다. 특히 “sram mode”의 경우는 routing entry 를 통해 전달 되는 mode 를 줄임으로써 자원의 소요를 가장 적게 하였다. 설정된 SDM 모드는 다음 부팅 시 적용된다. 다음은 SDM 에서 사용되는 명령어에 대해서 설명해 놓았다.

표 3-15. SDM 관련 명령어

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

3.12. Traffic-control

3.12.1. Traffic-control 개요

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

3.12.2. Traffic-control 설정

Traffic-control 설정을 위한 기본 명령어는 다음과 같다

표 3-16. traffic-control 설정 명령어

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

3.13. 포트 버퍼 설정

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

표 3-17. traffic-control 설정 명령어

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

3.14. LLCF (Link Loss Carry Forward)

Premier 8624XG Series 의 LLCF 기능은 LLCF Group 으로 관리하며, 물리적 포트는 하나의 LLCF Group 의 Uplink 멤버 또는 Downlink 멤버가 될 수 있다. LLCF Group 은 각 Group 에 설정된 모드(Uplink mode, Downlink mode, Bi-Direction mode)에 따라서 멤버들의 링크 업/다운을 관리한다.

표 3-18. LLCF mode 별 동작

LLCF Group mode	Case	Action
Uplink mode	Group 의 모든 Downlink 멤버들이 링크 다운되었을 때	Group 의 모든 Uplink 멤버들을 링크 다운 시킨다.
	Group 의 Downlink 멤버가 링크 업되었을 때	LLCF 기능으로 링크 다운된 Uplink 멤버들을 링크 업 시킨다.
Downlink mode	Group 의 모든 Uplink 멤버들이 링크 다운되었을 때	Group 의 모드 Downlink 멤버들을 링크 다운시킨다.
	Group 의 Uplink 멤버들이 링크 업되었을 때	LLCF 기능으로 링크 다운된 Downlink 멤버들을 링크 업 시킨다.
Bi-Direction mode	Uplink mode + Downlink mode	

표 3-19. LLCF 설정 명령어

명령어	설명	모드
llcf-group *group-id* **enable**	*group-id* 을 갖는 LLCF Group 을 enable 한다. 8624XG Series 는 최대 12 개의 Group 을 지원한다.	config
llcf-group *group-id* **disable**	*group-id* 을 갖는 LLCF Group 을 disable 한다.	config
llcf-group *group-id* **set-mode** *mode*	*group-id* 을 갖는 LLCF Group 을 *mode* 로 설정한다.	config
llcf-group *group-id* **uplink**	해당 포트를 group-id 을 갖는 LLCF Group 의 uplink 멤버로 등록한다.	interface
llcf-group *group-id* **downlink**	해당 포트를 group-id 을 갖는 LLCF Group 의 downlink 멤버로 등록한다.	interface
no llcf-group	해당 포트를 소속된 LLCF Group 에서 제거한다.	interface
show llcf-group	LLCF Group 과 멤버 포트의 관계를 출력한다.	privileged

4

가상 랜(VLAN)

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

이 장에서는 다음의 내용들을 다룬다:

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

4.1. VLAN 개관

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

4.1.1. VLAN 정의

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

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

4.1.2. VLAN 의 장점

VLAN 을 사용하면 다음과 같은 장점이 있다:

- **트래픽 제어**
  전통적인 네트워크에서는 각 장비의 데이터 수신 여부와 상관없이 모든 네트워크 장비로 전송되는 브로드캐스트 트래픽 때문에 혼잡을 발생시킨다. VLAN 내의 모든 장치는 같은 브로드캐스트 도메인에 속해 있는 구성원이며 모든 브로드캐스트 패킷을 수신한다. 반면 다른 VLAN 에 속하는 스위치의 포트로는 브로드캐스트 트래픽이 전송되지 않는다. 따라서 VLAN 을 사용하면 브로드캐스트 트래픽이 인접 네트워크로 퍼져나가는 것을 방지하고 네트워크의 효율을 증가시킬 수 있다.
- **네트워크 보안 강화**
  전통적인 네트워크에서는 네트워크에 접근하는 누구라도 네트워크 리소스에 접근할 수 있다. 또한, 사용자가 허브를 통하여 네트워크 분석기를 접속하게 되면 네트워크의 모든 흐름을 볼 수 있게 된다. 하지만 VLAN 을 사용하면 VLAN 에 포함된 장비들은 오직 같은 VLAN 의 구성원들과 통신할 수 있으며, 스위치 포트에 컴퓨터를 접속하는 것으로는 더 이상 모든 네트워크 리소스에 접근할 수 없다. 만약 VLAN A 에 속한 장비가 다른 VLAN B 의 장비와 통신해야 한다면, 트래픽은 반드시 라우팅 장비를 거쳐야 한다.

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

4.2. VLAN 의 유형

Premier 8624XG Series 스위치는 최대 4094 개의 VLAN 을 지원한다. VLAN 은 다음의 기준에 따라 생성된다:

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

4.2.1. 포트 기반 VLAN(Port-Based VLANs)

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

예를 들면, <그림 4-1>의 Premier 8700 스위치에서 1, 2, 3, 4 포트는 VLAN A 의 access 포트이고 9, 10, 11, 12 포트는 VLAN B 의 access 포트로 할당된다. 그리고 5, 6, 7, 8, 17, 18, 19, 20 포트는 VLAN C 의 access 포트로 정의한다.

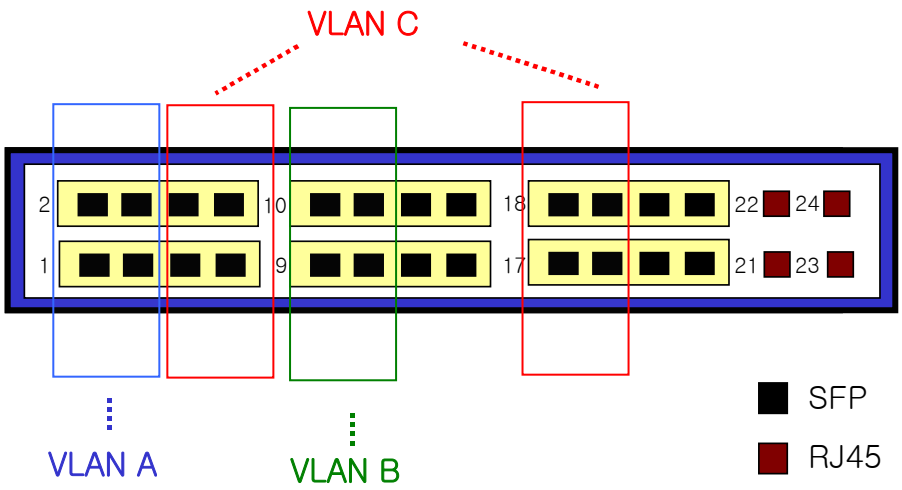


그림 4-1. Premier 8624XG 스위치의 포트 기반 VLAN 구성 예

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

포트 기반 VLAN 으로 스위치 묶기

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

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

<그림 2>는 서로 다른 2 개의 Premier 8624XG 스위치를 하나의 VLAN 으로 묶는 방법을 보여준다. 먼저 스위치 1 의 4 개의 포트는 VLAN A 로 포함되도록 할당되어 있다. 또한 스위치 2 의 4 개 포트도 VLAN A 의 access 포트로 할당되어 있다. 두 스위치는 <그림 2>와 같이 상호 연결하여 하나의 브로드캐스트 도메인을 형성한다.

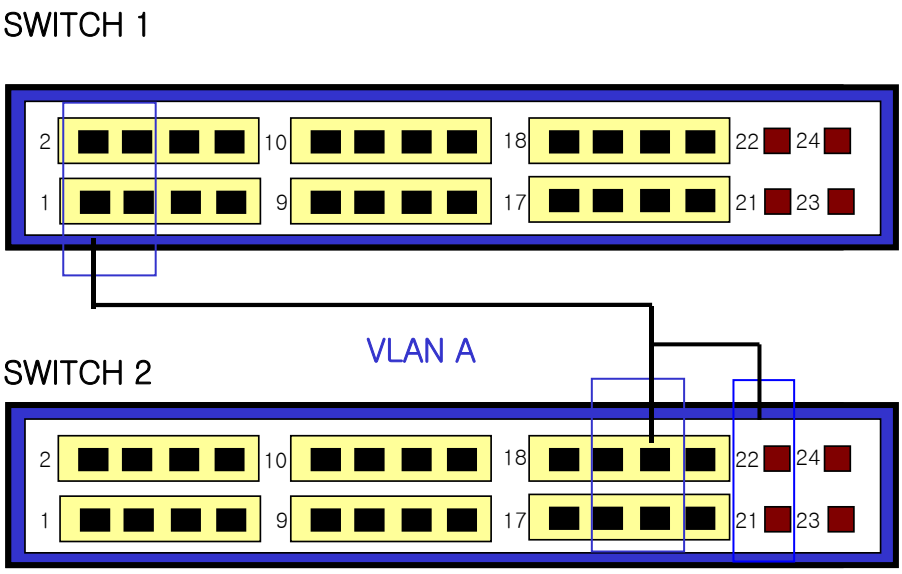


그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

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

<그림 4-3>은 두 개의 Premier 8624XG Series 스위치에 걸쳐서 설정되는 두 개의 VLAN 을 보여준다. 스위치 1 에서 포트 1, 2, 3, 4 포트는 VLAN A 의 access 포트이고 11, 12, 13, 14 까지의 포트는 VLAN B 의 access 포트로 할당되어 있다.

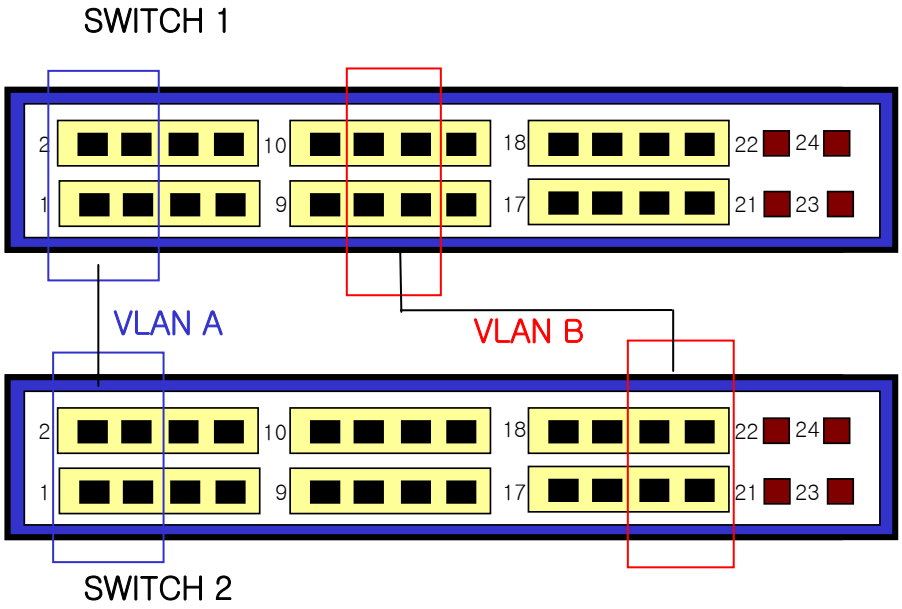


그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

VLAN A 는 스위치 1 의 포트 1 과 스위치 2 의 포트 2 의 연결을 통해 스위치 1 과 스위치 2 를 묶는다. VLAN B 는 스위치 1 의 포트 11 과 스위치 2 의 포트 22 사이를 연결사여 스위치 1 과 스위치 2 를 묶는다.

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

4.2.2. 태그 VLAN(Tagged VLANs)

태깅(tagging)은 Ethernet 프레임에 태그(tag)라는 표지(marker)를 삽입하는 작업이다. 태그에는 각각의 VLAN 을 식별하기 위한 VLANid 가 포함된다.

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

태그 VLAN 의 사용(Uses of Tagged VLANs)

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

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

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

VLAN 태그의 할당(Assigning a VLAN Tag)

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

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

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

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

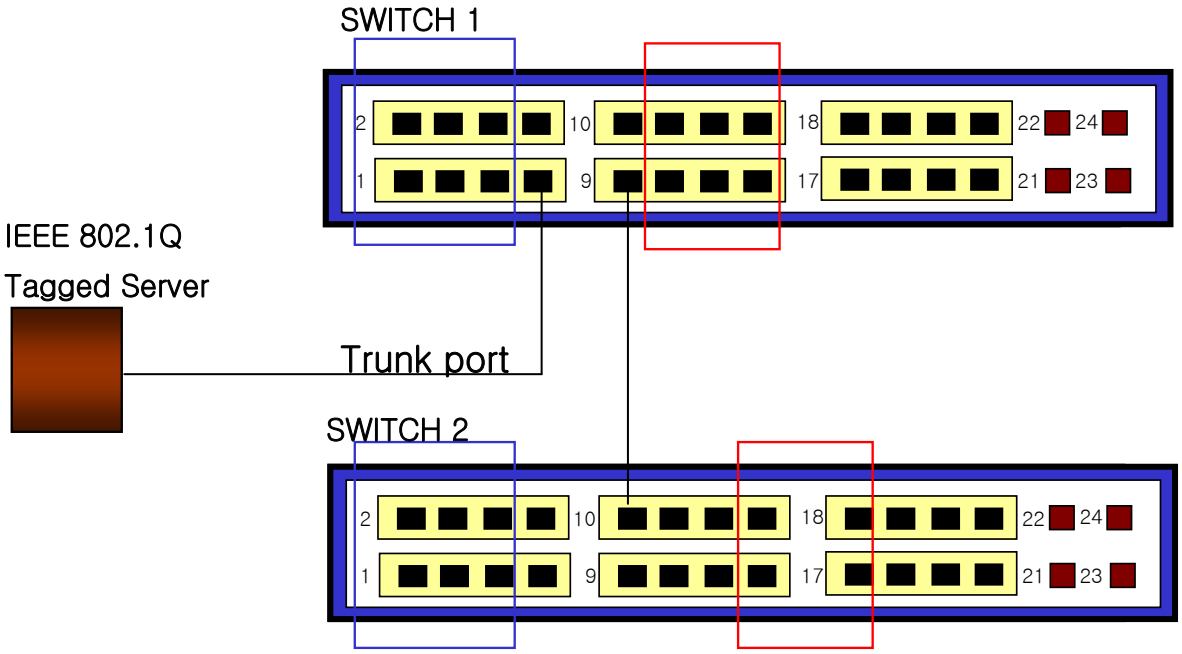


그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<그림 4-5>는 동일한 네트워크의 논리적인 다이어그램을 보여준다.

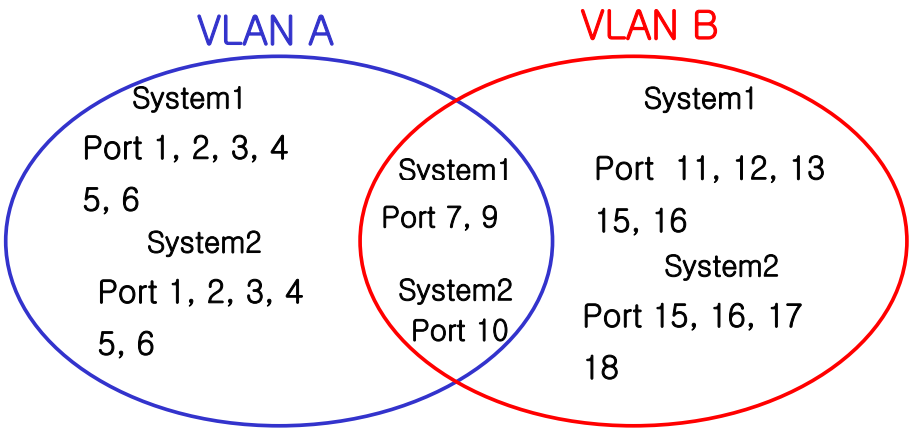


그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

<그림 4-4>와 <그림 4-5>에서:

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

착하고 있으며 VLAN A 와 VLAN B 의 멤버이다.

- 다른 단말들은 태그가 붙지 않은 프레임을 송수신한다.

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

4.2.3. 포트 기반 VLAN 과 태그 VLAN 의 혼합

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

4.3. VLAN 구성

4.3.1. VLAN ID

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

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

4.3.2. Default VLAN

스위치에는 다음과 같은 특성을 가지는 default VLAN 이 설정되어 있다.

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

4.3.3. Native VLAN

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

<그림 6>처럼 태그가 붙지 않은 프레임과 PVID 가 붙은 프레임이 공존하는 것이 허용되므로, VLAN 을 지원하는 브리지나 end station 과 VLAN 을 지원하지 못하는 브리지나 end station 들이 케이블로 연결될 수 있다.

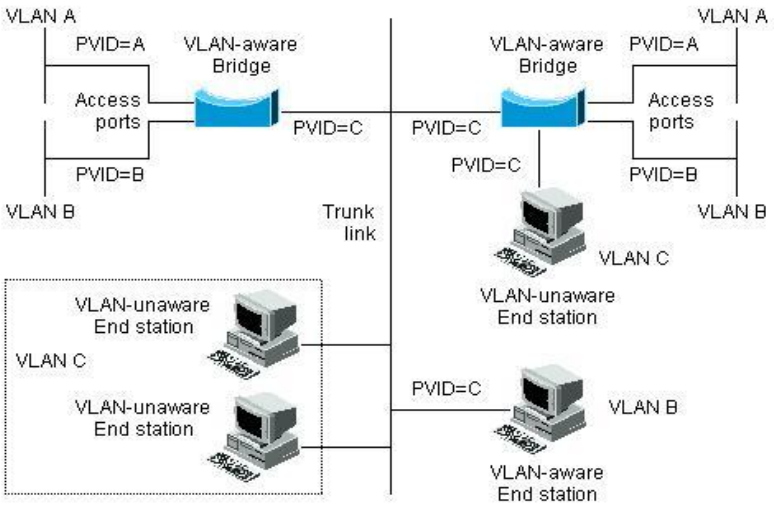


그림 4-6. Native VLAN

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

4.4. VLAN 설정

본 절에서는 Premier 8624XG 스위치에 VLAN 을 설정에 사용되는 명령들을 설명한다. VLAN 설정은 다음의 단계로 진행된다.

1) 생성된 VLAN 과 관련된 값을 설정한다.
2) 포트가 할당될 VLAN 의 종류에 따라 포트의 모드를 설정한다.

3) VLAN 에 하나 이상의 포트를 할당한다. VLAN 에 포트를 추가할 때, 802.1Q 태그의 사용 여부를 결정한다.

4.4.1. VLAN 설정 명령

<표 4-1>은 VLAN 설정에 사용되는 명령들을 설명한다.

표 4-1. VLAN 설정 명령어

명령어	설명	모드
`vlan vlanid`	■ VLAN 과 관련된 값들을 생성, 삭제, 변경한다. ■ 1 은 default VLAN 의 값으로 사용 ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다.	config
`switchport mode {access|trunk}`	■ 포트의 VLAN 타입을 설정한다. ■ `access` – 포트를 access 모드(포트 기반 VLAN)로 설정한다. 설정된 포트는 태그가 붙지 않은 프레임을 송수신하는 단일 VLAN 의 인터페이스로 동작한다. ■ `trunk` – 포트를 트렁크(태그 VLAN)로 설정한다. 설정된 포트는 태그가 붙은 프레임을 송수신한다.	Interface
`switchport access vlan vlanid`	■ 포트를 VLAN 의 access 포트로 설정한다. ■ 모드가 access 로 설정되면, 설정된 포트는 VLAN 의 멤버 포트로 동작한다. ■ *vlanid* : 1 부터 4094 사이의 값을 사용한다.	Interface
`switchport trunk add vlanid`	■ 포트를 VLAN 의 트렁크 포트로 설정한다. ■ 포트를 여러 VLAN 의 트렁크 포트로 설정하려면, 각 VLAN 에 대해 이 명령을 반복 사용한다. ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다. ■ Default VLAN(VLANid=1)은 포트 기반 VLAN 으로 사용	Interface
`switchport trunk native vlanid`	■ 포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 붙지 않고 송수신되는 트래픽을 위한 native VLAN 을 설정한다. ■ native VLAN 을 설정하지 않으면 default VLAN(VLANid = 1)이 native VLAN 으로 설정 ■ *vlanid* : 1 부터 4094 사이의 값을 사용한다.	Interface
`switchport trunk remove {vlanid|all}`	■ 포트를 명시한 VLAN 의 멤버에서 제외시킨다. ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다. ■ all : 모든 VLAN 으로부터 멤버에서 제외	Interface

명령어	설명	모드
(no) untagged-packet-drop	■ 포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 없는 packet 은 drop 시키는 기능이다. No 를 통해서 해제 가능하다.	Interface

4.5. VLAN 설정 예제

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

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

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

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

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

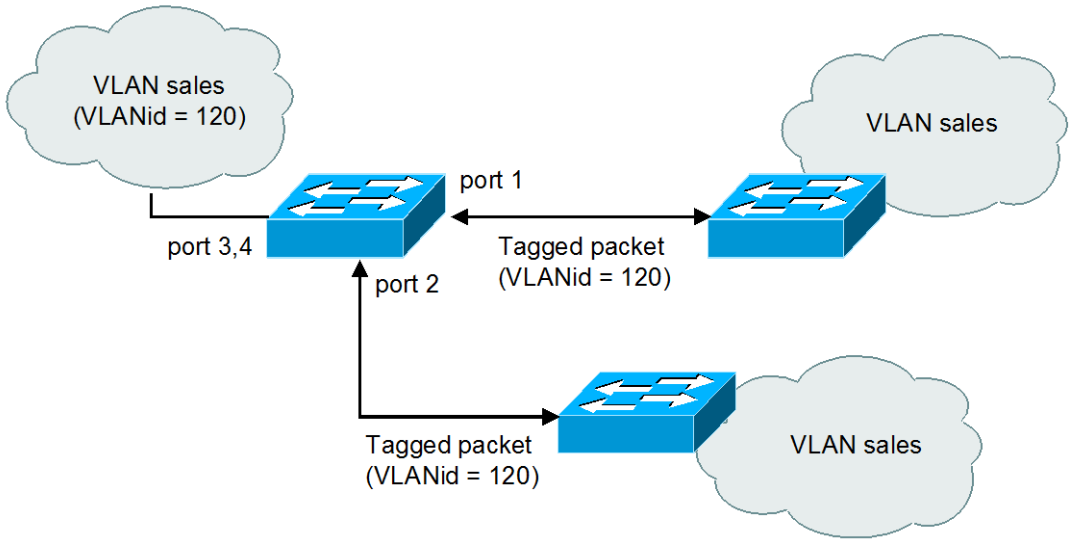


그림 4-7. VLAN 설정 예제 – Tagged and Untagged VLAN

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

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

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

포트 gi1 으로 태그가 붙지 않은 프레임이 수신되면 스위치는 VLAN *marketing* 의 멤버 포트로 프레임을 전달한다.

4.6. VLAN 설정 정보 확인

VLAN 설정 정보를 보려면 다음의 명령을 사용한다.

명령어	설명	모드
show vlans	■ VLAN 와 관련된 다음의 요약 정보를 출력한다. • VLANid • 멤버 포트	Privileged

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

4.7. 802.1QinQ

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

1. 전체 시스템에 QinQ를 적용하기 위한 결정을 내린다. 이것을 적용하기 위해서는 사용자 포트 트래픽의 마지막에 4바이트에 추가를 한다.

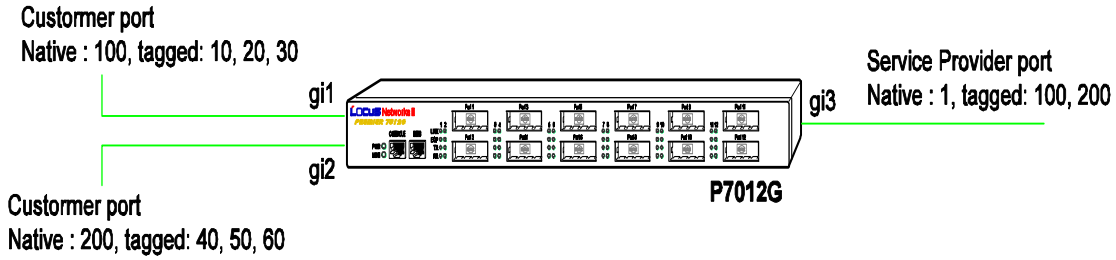
2. Service Provider Ethertype: Set up ethertype of an outer tag (디폴트 값 0x8100).

3. Service Provider VLAN ID: Use the native VLAN ID value of customer port for outer tag VLAN ID

4. 포트모드: Q in Q를 적용하기 위해서는 각 포트마다 모드 세팅을 하는 것은 필요하다. 포트모드는 사용자포트에 outer tag를 추가해야 하고 서비스를 제공하는 포트는 outer tag를 제거 해야 한다.

표 4-2. 802.1 QinQ 명령어 사용법 테이블

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



Example gi1 → gi3

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

그림 8. 802.1 QinQ 설정

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

Switch# show switchport
U : untagged packet drop
--------------------------------------------------------------------------
 IFNAME    SWMODE N-VLAN TAGGED-VLAN-LIST
--------------------------------------------------------------------------
 gi1       trunk     100    10   20   30
 gi2       trunk     200    40   50   60
 gi3       trunk       1   100  200
.
--------------------------------------------------------------------------
total 12 interfaces listed

Switch# configure terminal
Switch(config)# encapsulation q-in-q
```

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

4.8. Private Edge VLAN

Private edge VLAN 은 하나의 세그먼트 즉 VLAN 내에 존재하는 포트들이지만 허용된 포트간에만 통신을 할 수 있고, 나머지 포트들간에는 layer 2 상에서 통신을 차단시키는 기술이다. 다시 말하면 vlan 안에 다시 vlan 을 나누는 개념이라고 보면 된다. 따라서 Private Edge VLAN 은 스위치에 있는 지역성이 중요하다. 그리고 서로 다른 스위치간에 보호되고 있는 두 포트 사이간의 독립이다. 보호되는 포트는 다른 포트에게 어떠한 트래픽(유니캐스트, 멀티캐스트, 브로드캐스트)도 발생시키지 않으며 동일 스위치에서 다른 포트들 역시 보호되는 포트에게는 어떠한 트래픽도 발생시키지 않는다.
L2 에서 보호되어 있는 포트들에게는 트래픽을 전달할 수 없고, 모든 트래픽은 L3 장치를 통해서만 보호되는 포트들간에 통신을 할 수 있다.

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

- IFNAME
  업 링크를 포트네임으로 지정(ex. gi1, gi2, po1…)

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

표 3. Private Edge VLAN 설정표

명령어	설명	모드
(no) private-edge-vlan	Private-edge-vlan을 설정/해제한다.	Config
(no) private-edge-vlan *IFNAME*	특정 인터페이스에 private edge vlan의 uplink로 설정할 IFNAME을 입력한다.	Interface

(no) private-edge-vlan stp-root-port *VLANID*	특정 인터페이스에 private edge vlan의 uplink를 VLANID의 root 포트로 설정한다.	Interface
Show private-edge-vlan	Private-edge-vlan의 설정 정보를 조회한다.	Privileged

[예제1]

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

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

[예제2]

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

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

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

4.9. 비정상적 MAC 차단기능

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

표 4. 비정상 MAC 차단 명령어

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

5

IP 환경 설정

5.1. 개요

본 장에서는 IP 주소를 설정하는 방법을 설명한다.

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

Premier 8624XG 스위치는 다음의 인터페이스에 IP 를 할당할 수 있다.

- VLAN interface
- Loopback interface
- Management interface

5.2. 네트워크 인터페이스에 IP 주소 할당

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

표 5-1. 사용 가능한 IP 주소

Class	주소 범위	상태
A	0.0.0.0	예약
	1.0.0.0 ~ 126.0.0.0	사용가능
	127.0.0.0	예약

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

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

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

Premier 8624XG 스위치는 하나의 인터페이스에 복수의 IP 주소를 할당하는 기능을 지원한다. Premier 8624XG 스위치는 인터페이스 당 최대 10 개의 IP 주소를 설정할 수 있다. 다양한 상황에서 복수개의 IP 주소가 유용하게 사용된다. 다음은 가장 일반적인 응용이다:

- 특정 네트워크 세그먼트를 위한 충분한 호스트 주소가 마련되어 있지 않다. 예를 들어, 300 개의 호스트 주소를 필요로 하는 하나의 물리적인 서브넷 위에, 논리적인 서브넷마다 254 개의 호스를 허용하도록 서브넷을 구성한다고 가정하자. 라우터나 access 서버에서 복수개의 IP 주소를 사용한다면 하나의 물리적 서브넷을 가지고 두`개의 논리적인 서브넷을 구성할 수 있다.

- 많은 오래된 네트워크들은 계층 2 의 브리지를 사용하여 구성되어 있으며, 서브넷으로 구성되어 있지 않다. 복수개의 주소의 적절한 사용은 서브넷으로의 전환과 라우터 기반 네트워크로 전환을 돕는다. 오래된 브리지 세그먼트에 속한 라우터는 그 세그먼트에 많은 서브넷이 존재한다는 사실을 쉽게 인식할 수 있다.

- 한 네트워크의 두 서브넷은 다른 네트워크에 의해 분리될 수 있다. 복수개의 주소를 사용하는 다른 네트워크에 의해 물리적으로 분리된 서브넷으로부터 하나의 네트워크를 구성할 수 있다. 이 예에서, 첫 네트워크는 확장되거나, 두 번째 네트워크의 상위에 위치한다. 서브넷은 라우터의 하나 이상의 활성화된 인터페이스에 동시에 나타날 수 없다.

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

표 5-2. IP 주소 할당 명령어

명령어	설명
`ip address ipaddress/prefixlen`	■ 인터페이스에 사용될 IP 주소를 설정한다.

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

5.3. ARP(Address Resolution Protocol)

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

표 5-3. ARP 환경 설정을 위한 명령어

명령어	설명	모드
`show arp`	■ ARP 테이블의 엔트리를 출력한다.	Privileged
`show arp IFNAME`	■ ARP 테이블의 내용을 vlan 혹은 port 별로 조회한다.	Privileged
`show arp static`	■ “arp” 명령어를 통해 static 으로 설정한 엔트리를 출력한다.	Privileged
`show arp dhcp-unbinding`	■ Dhcp 에 의해 unbinding 된 arp 엔트리만을 출력한다.	Privileged
`arp ip-address mac-address vlan-name port-name`	■ ARP 테이블에 static ARP 엔트리를 설정 ■ Ip-address: ARP 엔트리의 IP 주소를 나타낸다; ■ Mac-address : ARP 엔트리의 48bit Ethernet 주소를 나타낸다. ■ vlan-name : ARP 의 목적지 IP interface 의 이름을 나타낸다. ■ Port-name: ip interface (즉 VLAN)의 member port 중 ARP 의 목적지 physical port name 을 나타낸다.	config

5.4. Static Routes 설정

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

Static route 를 설정하려면 Config 모드에서 다음의 명령을 사용한다.

표 5-4. Static route 경로 설정 명령어

명령어	설명
`ip route {destination-prefix mask | destination-ipaddress/mask} {gateway-ipaddress | null0} [distance-value]`	■ Static route 를 등록한다. ■ `destination-prefix` : 목적지의 네트워크 번호를 명시한다. ■ `mask` : 목적지 네트워크의 마스크를 명시한다. ■ `gateway-ipaddress` : 게이트웨이 장치의 IP 주소를 명시한다. ■ `null` : null 인터페이스를 게이트웨이로 설정한다. ■ `distance-value` : 1 부터 255 사이의 숫자를 사용

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

표 5-5. 동적 라우팅 프로토콜의 default administrative distances

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

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

static route 정보를 확인하려면 privileged 모드에서 다음의 명령을 사용하라.

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

5.5. IP 설정 예제

이 절에서는 IP 주소 설정 예제를 제공한다:

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

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

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

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

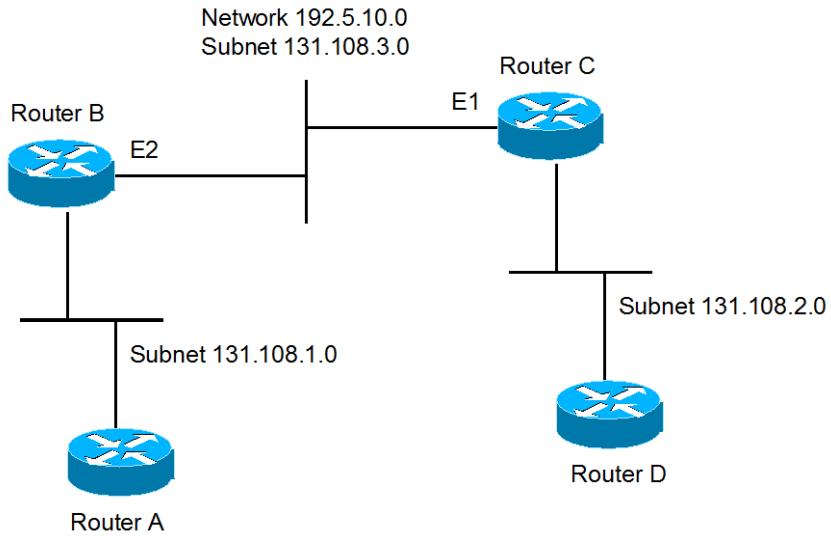


그림 5-1. 네트워크 설정 예 – 복수 IP address

라우터 B 설정

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

라우터 C 설정

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

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제이다.

```
Switch# show arp
Flags>> R: reachable P: permanent K: H/W only B: dhcp unbind drop
-----------------------------------------------------------------------
 IP Address      MAC Address     Interface   PORT     RefCnt  Flags
-----------------------------------------------------------------------
 10.1.2.254      0007.7089.1123  vlan2       gi1      1       R
 10.1.11.46      0006.2bfc.146e  vlan11      gi7      1       R
 10.1.13.1       0001.0281.f775  vlan13      gi2      1       R
 10.1.13.190     0000.f083.f6d4  vlan13      gi6      1       K
```

다음의 명령은 ARP 테이블에 static ARP 엔트리를 등록한다.

```
Switch(config)# arp 142.10.52.196 0010.073c.0514 vlan1 gi2
Switch# show arp
-----------------------------------------------------------------------
 IP Address      MAC Address     Interface   PORT     RefCnt  Flags
-----------------------------------------------------------------------
 142.10.52.196   0010.073c.0514  vlan1       gi2      1       P
```

다음의 명령은 ARP 테이블에서 static ARP 엔트리를 삭제한다.

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

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

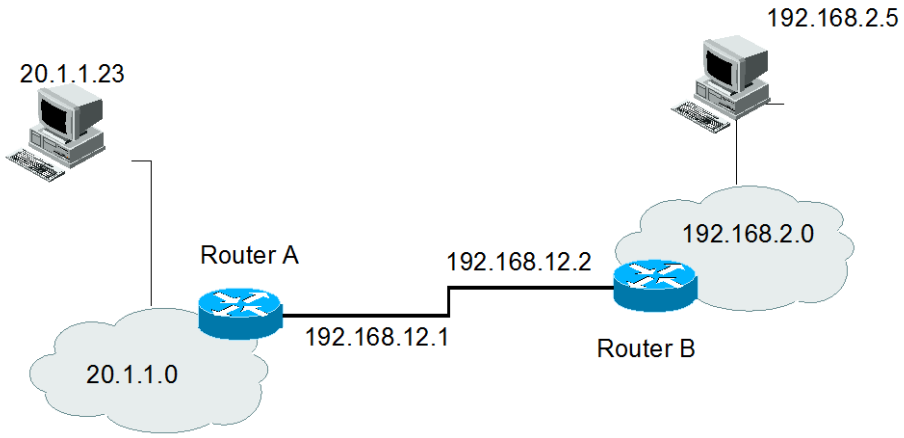


그림 5-2. 네트워크 설정 예 – Static route

라우터 A 설정

```
Switch(config)# ip  route  192.168.2.0/24  192.168.12.2
Switch# show ip route static database
Codes: K - kernel route, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area,
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2,
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, > - selected route, * - FIB route
S>* 192.168.2.0/24 [1/0] via 192.168.12.2 vlan2
Switch#
```

라우터 B 설정

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

6 DHCP

6.1. DHCP Server 기능 및 설정

6.1.1. DHCP Server 기능 개요

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

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

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

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

6.1.1.1. DHCP Server 의 Address 할당 방법

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

- 자동 할당(automatic allocation) – DHCP 가 Client 에게 영구적인 IP Address 를 할당한다.

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

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

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

6.1.1.2. Premier 8624XG 스위치를 DHCP Server 로 사용

<그림 6-1>는 DHCP Client 가 DHCP Server(Premier 8624XG 스위치)에게 IP Address 를 요구했을 때의 기본 절차이다.

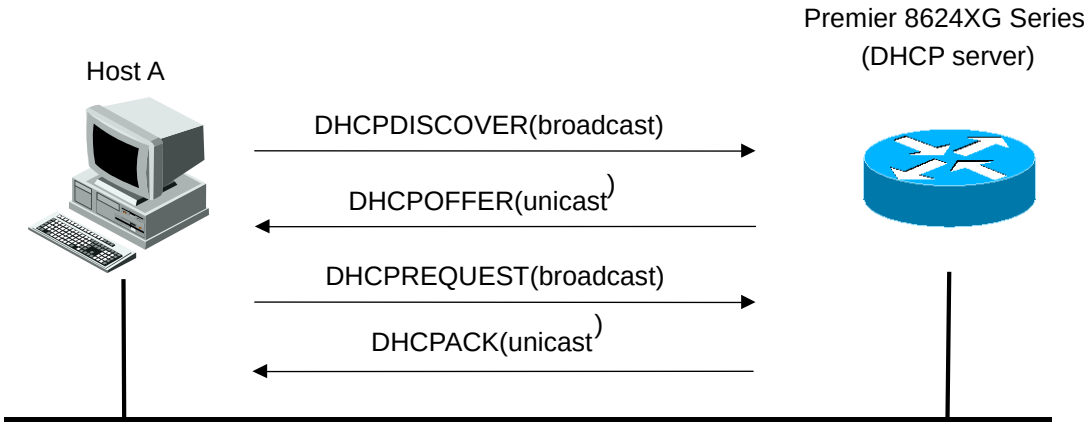


그림 6-1. Premier 8624XG 스위치를 DHCP Server 로 사용

4) Client Host A 는 브로드캐스트 메시지 *DHCPDISCOVER* 를 DHCP Server 로 전송한다.

5) DHCP Server 는 IP Address, 도메인 이름, IP Address 의 임대 기간 등의 설정 파라미터를 Client 에게 유니 캐스트 메시지 *DHCPOFFER* 를 사용하여 전송한다.

Notice DHCP Client 는 하나 이상의 DHCP Server 로부터 *DHCPOFFER* 메시지를 받을 수 있다. Client 는 일반적으로 가장 먼저 수신된 하나의 메시지만 수용한다. 하지만 DHCP Server 의 IP Address 제공 메시지인 *DHCPOFFER* 메시지를 수신했다고 해서 DHCP Server 가 Address 할당을 보장하는 것은 아니다. DHCP Server 는 Client 가 다시 공식적으로 Address 할당을 요구할 때까지 Address 사용을 예약한다.

6) Client 는 제공된 IP Address 에 대한 형식적인 요청을 DHCP Server 에게 브로드캐스트 메시지

DHCPREQUEST 를 사용하여 전송한다.

7) DHCP Server 는 Client 에게 유니 캐스트 메시지 *DHCPACK* 를 전송함으로써 IP Address 가 Client 에게 할당되었음을 확인한다.

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

6.1.1.3. DHCP Server 의 장점

Premier DHCP Server 는 다음의 이점을 제공한다.

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

6.1.2. DHCP Server 기능 활성화

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

명령	설명
`service dhcp server`	■ 스위치의 DHCP Server 기능을 활성화 ■ DHCP Server 기능을 비활성 시키려면, 이 명령의 `no` 형태를 사용

다음의 예제는 DHCP Server 기능을 활성화 시킨다.

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

```
. . .
!
```

6.1.3. DHCP Address Pool

Premier DHCP Server 는 Network Pool 과 Host Pool 의 두 가지 Pool 을 지원한다.

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

6.1.4. DHCP Network Pool 설정

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

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

6.1.4.1. DHCP Network Pool 이름 설정 및 DHCP 설정 모드 진입

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

명령어	설명
`ip dhcp network-pool` *name*	■ DHCP Network Pool 을 위한 이름을 생성 ■ “`config-dhcp#`” 프롬프트로 식별되는 DHCP 네크워크 Pool 설정 모드로 진입

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

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

```
!
ip dhcp network-pool network_pool1
!
. . .
```

6.1.4.2. DHCP 서브넷 및 Network 마스크 설정

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

명령어	설명
network *network-number/prefix-length*	■ DHCP 네크워크 Pool 내의 포함될 서브 Network 번호와 마스크를 설정

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

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

6.1.4.3. Network Pool 에서 할당 할 IP Address 범위 설정

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

명령어	설명
range *lowest-address highest-address*	■ 서브넷에서 클라언트들에게 할당할 Address 범위를 지정한다. ■ 이 명령어는 DHCP Subnet 및 Network Mask 를 설정한 이후에 설정해야 한다.

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

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

```
!
. . .
```

6.1.4.4. DHCP Server 부트 파일 설정

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

명령어	설명
bootfile *filename*	■ 부트 이미지로 사용될 파일의 이름을 명시

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

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

6.1.4.5. Client 를 위한 기본 라우터 설정

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

명령어	설명
default-router *address*	■ DHCP Client 를 위한 기본 라우터의 IP Address 를 명시

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

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# default-router 100.0.0.1
Switch(config-dhcp)# exit
Switch# show running-config
. . .
```

```
!
ip dhcp network-pool network_pool1
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
...
```

6.1.4.6. Client 를 위한 DNS IP Server 설정

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

명령	설정
dns-server *address1 address2 address3*	■ DHCP Client 가 이용할 수 있는 DNS Server 의 IP Address 를 설정 ■ DHCP Client 하나의 IP Address 만 요구하지만, 명령 라인에서 최대 3 개의 IP Address 를 설정할 수 있다.

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

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

6.1.4.7. Client 를 위한 도메인 이름 설정

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

명령어	설명
domain-name *domain*	■ Client 를 위한 도메인 이름을 명시

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

```
Switch# configure terminal
```

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

6.1.4.8. 네크워크 Pool 을 위한 그룹 설정

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

명령어	설명
group *group-name*	■ 그룹 이름을 명시

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

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

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

6.1.4.9. Address 임대 기간 설정

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

명령어	설명
lease {days [hours] [minutes]}	■ 임대 기간을 명시 ■ 기본값은 한 시간으로 설정 ■ infinite: Host 에게 영구적으로 IP Address 를 임대하는 자동 할당방식으로 설정

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

```
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# lease 0 0 20
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
dns-server 200.0.0.1 200.0.0.2
lease 0 0 20
domain-name ubiquoss.com
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group ubiquoss_pool
!
...
```

6.1.4.10. Client 를 위한 NetBios WINS IP Server 설정

WINS(Windows Internet Naming Service)는 일반적인 Network 그룹 내에서 Microsoft DHCP Client 가 Host 이름을 IP Address 를 변환하기 위해 사용하는 이름 해석 서비스이다. Microsoft DHCP Client 가 이용할 수 있는 NetBIOS WINS Server 를 설정하기 위해, DHCP 네크워크 Pool 설정 모드에서 다음의 명령을 사용한다.

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

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

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# netbios-name-server 210.0.0.1
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
```

```
dns-server 200.0.0.1 200.0.0.2
domain-name ubiquoss.com
default-router 100.0.0.1
netbios-name-server 210.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group ubiquoss_pool
!
...
```

6.1.4.11. Client 를 위한 NetBIOS 노드 타입 설정

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

명령어	설명
`netbios-node-type` *type*	■ Microsoft DHCP Client 의 NetBIOS 노드 타입을 명시

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

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

6.1.5. DHCP Host Pool 설정

수동 바인딩은 IP Address 와 Client 의 MAC(Media Access Control) Address 사이의 매핑이다. Client 의 IP Address 는 Network 관리자에 의해서 수동으로 할당되거나 DHCP Server 의 Pool 로부터 자동으

로 할당될 수 있으며, Host Pool 은 수동 Address 할당을 위한 특별한 형태의 Address 할당 형태이다. DHCP Host Pool 설정은 IP, MAC 등의 파라미터를 설정할 수 있는 DHCP Host Pool 설정 모드로 진입한다. DHCP Host Pool 을 설정하기 위해서는 다음 절에서 요구되는 작업들을 완료해야 한다.

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

6.1.5.1. DHCP Host Pool 이름 설정 및 DHCP 설정 모드 진입

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

명령어	설명
`ip dhcp host-pool` *`name`*	■ DHCP Host Pool 을 위한 이름을 생성 ■ "`config-dhcp#`" 프롬프트로 식별되는 DHCP Host Pool 설정 모드로 진입

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

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

표 2. Host Pool 설정 명령어

명령어	설명
`bootfile` *`filename`*	■ 부트 이미지로 사용될 파일의 이름을 명시
`default-router` *`address`*	■ DHCP Client 를 위한 기본 라우터의 IP Address 를 명시
`dns-server` *`address1 address2 address3`*	■ DHCP Client 가 이용할 수 있는 DNS Server 의 IP Address 를 설정 ■ DHCP Client 하나의 IP Address 만 요구하지만, 명령 라인에서 최대 3 개의 IP Address 를 설정할 수 있다.
`domain-name` *`domain`*	■ Client 를 위한 도메인 이름을 명시
`netbios-name-server` *`address`*	■ Microsoft DHCP Client 가 이용할 수 있는 NetBIOS WINS Server 의 IP Address 를 설정

`netbios-node-type` *type*	■ Microsoft DHCP Client 의 NetBIOS 노드 타입을 명시
`network` *ipaddr/prefix-len*	■ 하나의 Host Pool 내에서 설정할 수동 바인딩 IP 의 네크워크

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

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

6.1.5.2. DHCP 수동 바인딩을 위한 Client 설정

Host Pool 내에 수동 바인딩을 제공할 Client 들을 생성한다.

명령어	설명
host *ip-address netmask*	■ Client 에게 할당할 IP Address 와 제공할 Network 마스크를 설정한다. ■ "`config-dhcp-host#`" 프롬프트로 식별되는 DHCP gHost 설정 모드로 진입

표 3. 수동 바인딩 명령어

명령어	설명
`hardware-address` *hardware-address*	■ Client 의 하드웨어 Address 를 명시
`client-name` *name*	■ 선택적으로 수행되며 표준 ASCII 문자를 사용하여 Client 의 이름을 명시 ■ Client 이름은 도메인 이름을 포함하지 않는다. 예로 mars 는 mars.ubiquoss.com 으로 명시하지 않는다.

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

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

```
ip dhcp host-pool host_pool1
 network 110.0.0.0/24
 host 110.0.0.1 255.255.255.0
  hardware-address 0011.2233.4455
!
```

6.1.6. 기타 Global 명령어

표 4. Global 명령어 리스트

명령어	설명
ip dhcp default-lease {days [hours] [minutes]|infinite}	■ 임대 기간을 명시 ■ 기본값은 한 시간으로 설정 ■ infinite: Host 에게 영구적으로 IP Address 를 임대하는 자동 할당방식으로 설정. Premier 스위치는 1 시간을 기본 값으로 갖는다. ■ DHCP Pool 내에 Lease time 이 설정된 경우, Pool 내의 Lease time 이 default-lease time 보다 우선한다.
ip dhcp max-lease {days [hours] [minutes]|infinite}	■ DHCP Client 에서 Lease time 에 대한 요청이 있는 경우, DHCP Server 는 max-lease time 값 이상의 임대시간을 DHCP Client 에게 할당하지 않는다. Premier 스위치는 1 일을 기본 값으로 갖는다.
ip dhcp unbindig-user drop	■ Premier 스위치로부터 IP 를 할당 받지 않은 사용자들이 스위치를 통해 서비스를 받으려고 시도할 경우 해당 패킷을 폐기할 수 있는 기능을 지원한다.
ip dhcp unbindig-user drop delay	■ DHCP Server Daemon start 또는 새로운 Network-pool 추가 시, 기존 DHCP Client 의 서비스 연속성을 보장하기 위해 unbinding-user drop 기능을 일정시간(default : 30 분) 지연시킨다.

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

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

6.2. DHCP Relay 기능 및 설정

6.2.1. DHCP Relay 기능 개요

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

다음은 Premier 8624XG 스위치가 DHCP Relay Agent 로서 DHCP 클라이언트의 IP 요청 메시지를 DHCP Server 로 전달하는 절차이다.

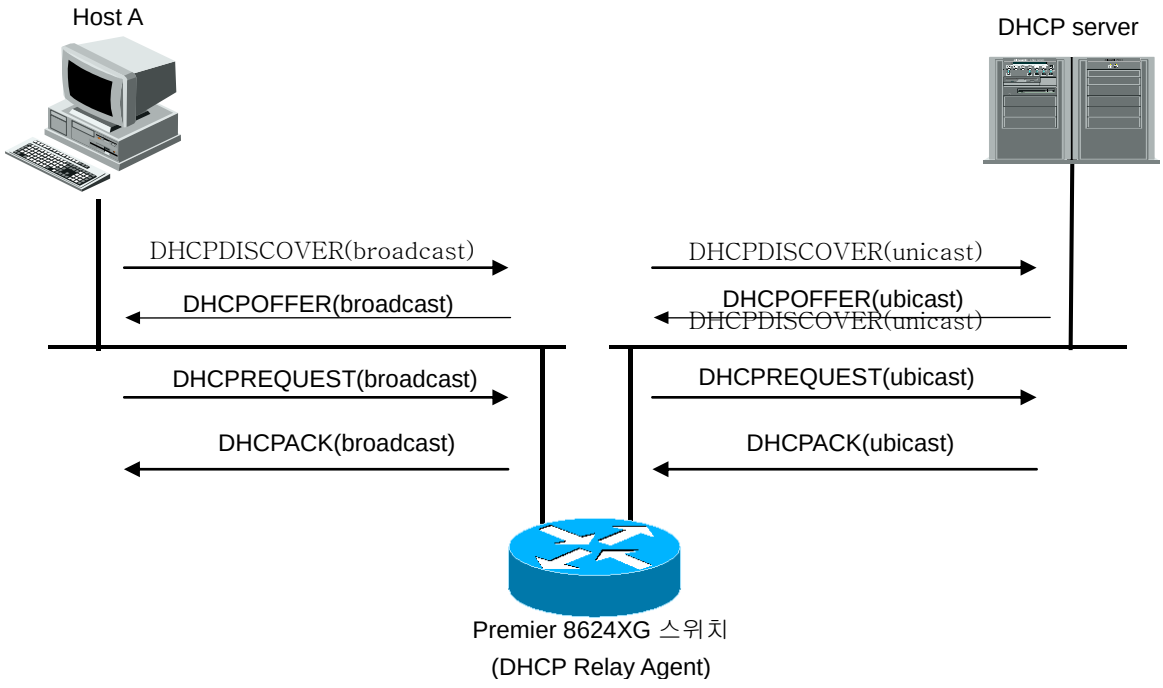


그림 6-2. DHCP Relay Agent 로서 DHCP Server 의 메시지 전달

1) DHCP 클라이언트는 IP 를 요청하기 위해 DHCPDISCOVER 메시지를 Broadcast 전송한다.

2) DHCP Relay Agent 는 DHCP 클라이언트의 IP 요청 메시지를 수신하여 DHCP Server 에게 해당 메시지를 Unicast 로 전달한다.

3) DHCP Relay Agent 로부터 메시지를 수신한 DHCP Server 는 클라이언트를 위한 IP 주소, 기본 라우터 등의 정보를 가진 DHCPOFFER 를 Unicast 로 DHCP Relay Agent 에게 전송한다.

4) DHCP Relay Aent 는 수신한 DHCPOFFER 메시지를 클라이언트에게 Broadcast 전송한다.

5) DHCP Server 와 클라이언트 사이의 DHCPREQUEST 와 DHCPACK 메시지도 동일한 과정으로 DHCP relay agent 에 의해 전달된다.

6.2.2. DHCP relay 기능 활성화

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

명령	설명
`service dhcp relay`	■ 스위치의 DHCP relay 기능을 활성화 ■ DHCP 릴레이 기능을 비활성화 하려면, 이 명령의 `no` 형태를 사용

다음의 예제는 DHCP Relay 기능을 활성화하는 예제이다.

```
Switch# configure terminal
Switch(config)# service dhcp relay
Switch(config)# exit
Switch# show ip dhcp relay

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

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

6.2.3. DHCP relay agent 에서 서버 설정

DHCP relay agent 에서 DHCP Server 를 설정하기 위해서는 Global 설정 모드 또는 Vlan Interface 모드에서 다음의 명령을 사용한다.

명령어	설명
ip dhcp-server *address*	■ DHCP relay agent 가 DHCP 요청 패킷을 중계할 때

DHCP Server 의 IP 주소를 설정

- Vlan Interface 모드에서 이 명령을 설정한 경우, 해당 Vlan Interface 에서 수신한 DHCP 패킷만 지정된 DHCP Server 중계함
- DHCP Server 의 삭제는 이 명령의 **no** 형태를 사용

Notice Premier 8624XG series 의 DHCP relay Agent 는 helper-address 를 최대 100 개까지 설정 가능하다.

다음의 예제는 DHCP Relay Agent 에서 Server 주소를 지정하는 예제이다.

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

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

DHCP helper-address is configured on following servers:
  192.168.0.254

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

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

6.2.4. DHCP relay information option(OPTION82) 설정

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

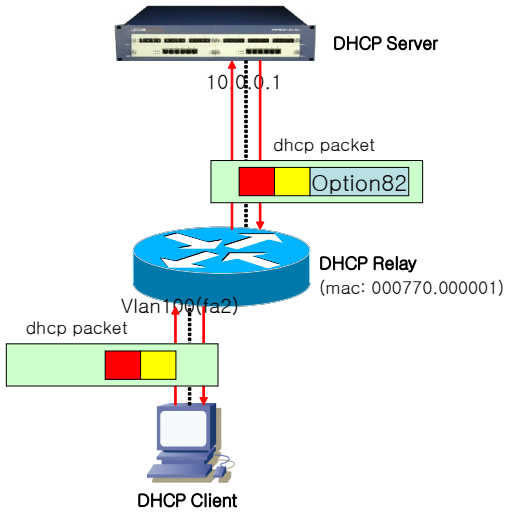


그림 6-3. DHCP Relay Option82

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

6.2.4.1. DHCP relay information option 기능의 활성화

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

명령어	설명
ip dhcp relay information option	■ DHCP relay information(option-82 field) 기능을 활성화 ■ 기본적으로, 이 특성은 비활성화 되어 있다.

다음은 DHCP Relay 의 Option82 기능을 활성화 시키는 예제이다.

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

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

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

6.2.4.2. Relay information option 재중계 정책 설정

기본적으로, Premier 8624XG 시리즈의 재중계 정책은 DHCP 클라이언트로부터 수신한 패킷 내에 기존의 relay information 을 Premier 스위치의 relay information 으로 대체한다. Premier 스위치의 기본 정책을 변경하기 원한다면, Global 모드에서 다음의 명령을 사용한다.

명령어	설명
ip dhcp relay information policy {drop|keep|replace}	■ 기본 값은 replace 이다. ■ drop : relay information 이 삽입되어 있는 패킷은 폐기한다. ■ keep : 기존의 relay information 을 유지하며, 기존의 relay information 이 없으면 switch 의 relay information 을 더한다. ■ replace : 기존의 relay information 을 Premier switch 의 relay information 으로 대체한다.

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

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

DHCP relay                     : Enabled
DHCP Smart Relay feature       : Disabled
DHCP Smart Relay retry count   : 3
DHCP server-id based relay     : Disabled
Verification of MAC address    : Enabled
```

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

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

6.2.5. DHCP Smart Relay 설정

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

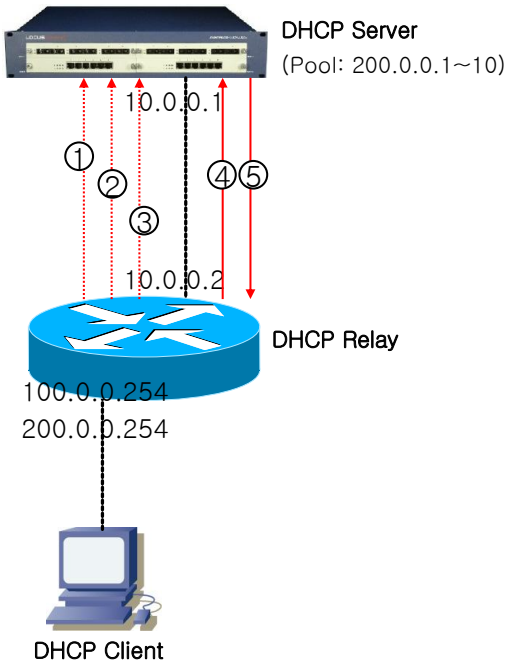


그림 6-4. DHCP Smart-Relay 동작 절차

8) DHCP Client 로부터 IP 요청 패킷을 수신한 DHCP Relay 는 giaddr 에 '100.0.0.254'를 삽입하여 '1' 번 패킷을 DHCP Server 에게 포워딩 한다. DHCP Server 는 이 패킷의 giaddr 를 보고 자신의 Pool 영역이 아니므로 해당 패킷을 Drop 한다.

6) Reply 패킷을 받지못한 DHCP Client 는 다시 한번 IP 를 요청한다. 이 패킷을 수신한 Relay Agent 는 해당 DHCP Client 에 대한 IP 요청 Retry Count 를 증가시킨다.

7) IP 요청 Retry Count 가 3 회이면('4' 번 패킷), DHCP Relay 는 giaddr 를 '200.0.0.254'로 변경한다. DHCP Server 는 이 패킷의 giaddr 를 보고 자신의 Pool 영역에 있으므로 Reply 패킷을 Relay

Agent 에게 전송한다.

명령어	설명
ip dhcp smart-relay	■ DHCP smart-relay 기능을 활성화 ■ 기본적으로, 이 특성은 비활성화 되어 있다.

다음의 예제는 DHCP Smart-Relay 기능을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# ip dhcp smart-relay
Switch(config)# exit
Switch# show ip dhcp relay

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

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

6.2.6. DHCP Relay Verify MAC-Address 설정

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

명령어	설명
ip dhcp snooping verify mac-address	■ DHCP Client Identifier 또는 Client HW Address 가 변조된 경우, 이 패킷을 Drop 시킨다. ■ 기본적으로, 이 특성은 활성화 되어 있다.

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

```
Switch# configure terminal
Switch(config)# no ip dhcp relay verify mac-address
```

```
Switch(config)# exit
Switch# show ip dhcp relay

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

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

6.2.7. DHCP relay server-id-relay 설정

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

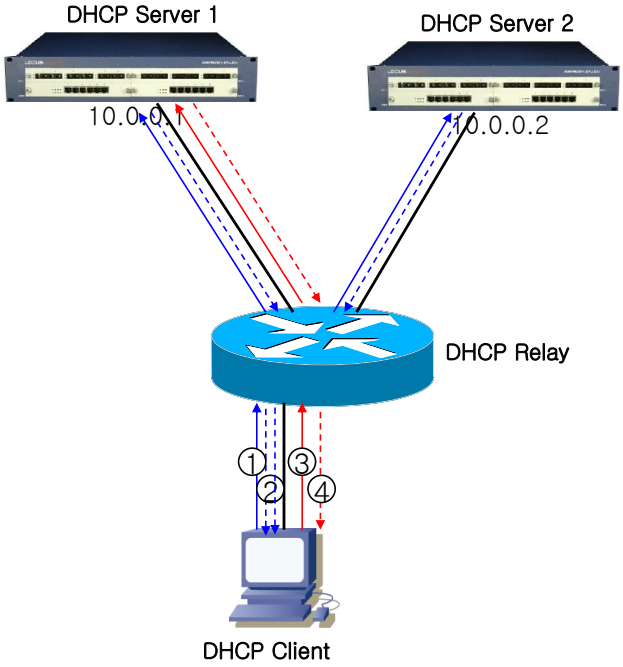


그림 6-5. DHCP Relay Server-Id-Relay 동작 절차

1) DHCP Client 로부터 DHCPDISCOVER 패킷을 받은 DHCP Relay Agent 는 자신에게 등록된 DHCP Server 1, DHCP Server 2 에게 패킷을 각각 포워딩한다.
2) DHCP Server 1 과 DHCP Server 2 는 DHCPDISCOVER 패킷을 받고 각각 DHCPOFFER 패킷으로 Reply 한다. DHCPOFFER 패킷에는 DHCP Server Identifier Option Filed 에 Server IP 주소가 삽입되어 있다.
3) DHCP Client 는 DHCP Server 1 과 DHCP Server 2 로부터 DHCPOFFER 패킷을 받고 이 중에 하나를 선택하여(ex. DHCP Server 1) DHCPREQUEST 패킷을 전송한다. DHCPREQUEST 패킷에도 DHCP Server Identifier Option 이 있다.
4) DHCPREQUEST 패킷을 수신한 DHCP Relay Agent 는 DHCPREQUEST 의 Server Idnetifier Option 을 보고 DHCP Server 1 에게만 DHCPREQUEST 패킷을 전송한다. 만약 DHCP Server Selection 기능이 활성화 되어 있지 않으면 DHCP Relay Agent 는 자신에게 등록된 모든 DHCP Server 에게 패킷을 전송한다.

명령	설명
ip dhcp relay server-id-relay	■ DHCP relay server-id-relay 기능을 활성화 ■ 기본적으로 이 특성은 비 활성화 되어 있다.

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

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

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

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

6.2.8. DHCP Class 기반 DHCP 패킷 Relay

Premier DHCP relay agent 는 DHCP Client 에서 전송된 DHCP 패킷의 Class 값에 따라 DHCP Server 를 선택하는 기능을 제공한다.

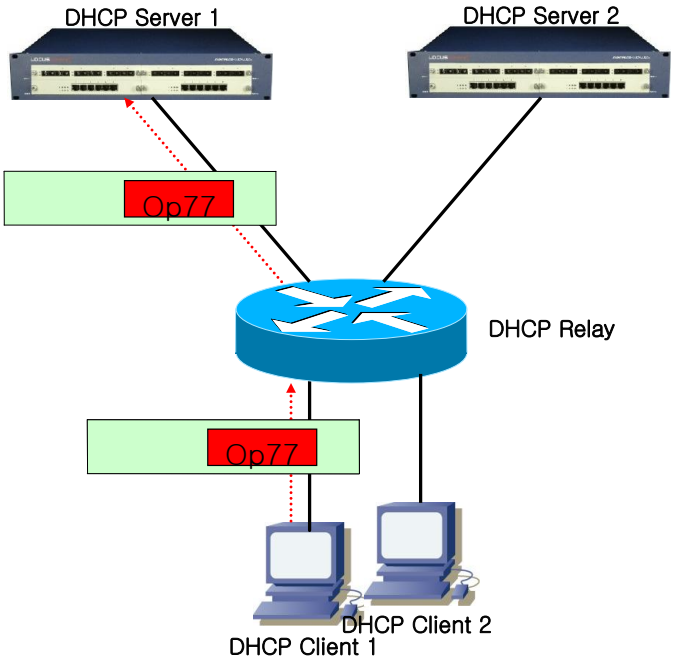


그림 6-6. DHCP Class 기반 DHCP 패킷 Relay

DHCP Class 설정

Premier DHCP relay agent 에서 DHCP Class Data 를 설정하기 위해 Global Node 및 DHCP Class Node 에서 다음의 명령어를 사용한다.

명령어	설명
ip dhcp class *class-name*	■ DHCP Class Name 지정 ■ "(dhcp-class)#" 로 식별되는 DHCP Class Node 로 진입
option <*1-255*> **{ascii|hex}** *WORD*	■ DHCP Option77 Data 설정

다음의 예제는 DHCP Class Data 로 class option77 에 "ubiquoss" 라는 Data 를 설정하는 예제이다.

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

DHCP Relay-Pool 설정

Premier DHCP relay agent 에서 DHCP Relay-Pool 을 설정하여 지정된 Network 로부터 수신한 DHCP 패킷에 DHCP Class 가 있는 경우, 특정 DHCP Server 로 패킷을 중계하기 위해 Global Node 및 DHCP Relay-Pool Node 에서 다음의 명령어를 사용한다.

명령어	설명
ip dhcp relay-pool	■ DHCP Relay-Pool 을 위한 이름 생성

	■ “(dhcp-pool)#” 로 식별되는 DHCP Relay-Pool Node 로 진입
relay source *A.B.C.D/M*	■ DHCP Relay-Pool 을 위한 네트워크 설정
class *class-name*	■ DHCP Relay-Pool 을 위한 class 지정

다음의 예제는 ‘100.0.0.0/24’ 네트워크로부터 Option 77 (“ubiquoss”) 포함한 DHCP 패킷을 수신했을 때 DHCP Server 200.0.0.254 에게 DHCP 패킷을 전송하는 예제이다.

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

6.3. DHCP Snooping 기능

6.3.1. DHCP Snooping 기능 개요

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

6.3.1.1. Trust and Untrust Source

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

6.3.1.2. DHCP Snooping Binding Database

DHCP Snooping은 DHCP Message를 가로 챈 정보를 사용하여 database를 동적으로 만들고 유지한다. Database는 DHCP Snooping이 활성화 되어 있는 Vlan의 untrusted host에 관한 entry를 포함한다. Database Entry는 DHCP Server, Client로부터 받은 모든 DHCP message를 Validation check 후 추가하고, Validation check 값은 state 항목에 기록한다. 또한 동일한 DHCP Client로부터 시작된 일련의 정상 DHCP message 는 가장 최근의 message 1개만 Database Entry에 기록된다. IP Address lease time이 경과되거나 host로부터 DHCPRELEASE message를 받았을 때는 state 항목에 time expired, released로 기록되며, Database의 Entry가 최대값을 넘었을 때는 가장 오래된 Invalid Entry가 삭제되고, 새로운 Entry가 추가된다.
DHCP Snooping binding database는 host의 MAC Address, Client Hardware Address, Client Identifier, leased IP address, lease time, received time, State, Vlan ID, host가 연결된 interface port 정보를 포함한다.

6.3.1.3. Packet Validation

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

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

6.3.1.4. Packet Rate-limit

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

6.3.2. DHCP Snooping 기능의 활성화

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

명령	설명
`ip dhcp snooping`	■ 스위치의 DHCP Snooping 기능을 활성화 ■ DHCP Snooping 기능을 비활성화 하려면, 이 명령의 `no` 형태를 사용

다음의 예제는 DHCP Snooping 기능을 활성화 하는 예제이다.

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

6.3.3. DHCP Snooping Vlan 설정

DHCP 패킷을 Snooping 할 Vlan 을 설정한다. 설정된 Vlan 이외의 Vlan 을 통과하는 DHCP 패킷은 Snooping 되지 않는다.

명령어	설명
ip dhcp snooping vlan *vlan_ID*	■ DHCP 패킷을 Snooping 할 Vlan 설정 ■ DHCP Snooping Vlan 삭제는 이 명령의 **no** 형태를 사용

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

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

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

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

6.3.4. DHCP Snooping information option(OPTION82) 설정

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

6.3.4.1. DHCP Snooping information option 기능의 활성화

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

명령어	설명
ip dhcp snooping information option	■ DHCP Snooping information(option-82 field) 기능을 활성화 ■ 기본적으로, 이 특성은 비활성화 되어 있다.

다음의 예제는 DHCP Snooping Information Option 기능을 활성화 시킨다.

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

6.3.4.2. DHCP Snooping information option 재중계 정책 설정

기본적으로, Premier 8624XG 스위치의 DHCP Snooping information 정책은 DHCP 클라이언트로부터 수신한 패킷 내에 information Option 정보가 있으면 패킷을 Drop 시킨다. Premier 8624XG 스위치의 기본 정책을 변경하기 원한다면, Global 모드에서 다음의 명령을 사용한다.

명령어	설명
ip dhcp snooping information policy {drop|keep|replace}	■ 기본 값은 drop 이다. ■ drop : DHCP Snooping information 이 삽입되어 있는 패킷은 폐기한다. ■ keep : 기존의 DHCP Snooping information 을 유지한다. ■ replace : 기존의 DHCP Snooping information 을 Premier switch 의 DHCP Snooping information 으로 대체한다.

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

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

6.3.5. DHCP Snooping Trust Port 설정

네트워크 관리자가 신뢰할 수 있는 포트(ex, DHCP Server 방향 포트)는 다음의 명령어를 사용하여 Trust Port 로 설정한다. Trust Port 를 설정하면 Host 로부터의 Request 패킷이 Trust Port 로만 포워딩

된다.

명령어	설명
ip dhcp snooping trust	■ 지정된 포트를 Trust Port 로 설정한다. Trust Port 에서 수신한 DHCP 패킷은 Validation check 하지 않는다. ■ Host 로부터의 Request 패킷이 Trust Port 로만 포워딩된다. ■ 기본적으로, 모든 포트는 untrust 포트이다.

다음의 예제는 포트 'gi1'을 Trust Port 로 설정한다.

```
Switch(config)# interface gi1
Switch(config-if-gi1)# ip dhcp snooping trust
Switch(config-if-gi1)# end
Switch# show ip dhcp snooping interface
Interface           Trust State     Max Entry
---------------     -----------     ------------
gi1                 Trusted                 2000  0
gi2                 Untrusted               2000  1
gi3                 Untrusted               2000  2
gi4                 Untrusted               2000  3
gi5                 Untrusted               2000  4
gi6                 Untrusted               2000  5
gi7                 Untrusted               2000  6
gi8                 Untrusted               2000  7
gi9                 Untrusted               2000  8
gi10                Untrusted               2000  9
gi11                Untrusted               2000  10
gi12                Untrusted               2000  11
gi13                Untrusted               2000  12
gi14                Untrusted               2000  13
gi15                Untrusted               2000  14
gi16                Untrusted               2000  15
gi17                Untrusted               2000  16
gi18                Untrusted               2000  17
. . .
```

6.3.6. DHCP Snooping max-entry 설정

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

명령어	설명
ip dhcp snooping max-entry	■ 포트별로 DHCP Snooping max-entry 개수를 설정한다. 단, valid(현재 IP 를 사용중인)한 entry 는 Max entry 개수를 초과하여도 삭제하지 않는다. ■ 기본적으로, 포트별 Max-entry 개수는 2000 개이다.

다음은 예제는 'gi1'의 DHCP Snooping Max-Entry 를 '100'개로 설정한다.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# ip dhcp snooping max-entry 100
Switch(config-if-gi1)# end
Switch# show ip dhcp snooping interface
Interface           Trust State     Max Entry
---------------     -----------     ------------
gi1                 Trusted                  100  0
gi2                 Untrusted               2000  1
gi3                 Untrusted               2000  2
gi4                 Untrusted               2000  3
gi5                 Untrusted               2000  4
gi6                 Untrusted               2000  5
gi7                 Untrusted               2000  6
gi8                 Untrusted               2000  7
gi9                 Untrusted               2000  8
gi10                Untrusted               2000  9
gi11                Untrusted               2000  10
gi12                Untrusted               2000  11
gi13                Untrusted               2000  12
gi14                Untrusted               2000  13
gi15                Untrusted               2000  14
gi16                Untrusted               2000  15
gi17                Untrusted               2000  16
gi18                Untrusted               2000  17
...
Switch#
```

6.3.7. DHCP Snooping Entry Time 설정

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

명령어	설명
ip dhcp snooping entry-time	■ Invalid(IP 를 현재 사용하고 있지 않는)한 DHCP Snooping Binding Entry 를 저장하고 있는 시간을 설정한다. 단위는 분이다. ■ 기본적으로, 14400 분(10 일)으로 설정된다.

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping entry-time 10
Switch(config)# exit
Switch# show ip dhcp snooping
```

```
Switch DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
 vlan1
```

6.3.8. DHCP Snooping Rate-Limit 설정

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

명령어	설명
ip dhcp snooping rate-limit	■ 매 1 초당 동일한 DHCP Client 로부터 Packet type 이 같은 DHCP Packet 의 허용 개수를 설정한다. ■ 기본적으로, 초당 2 개의 패킷을 허용한다.

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping rate-limit 100
Switch(config)# end
Switch#
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
 vlan1
```

6.3.9. DHCP Snooping Verify MAC-Address 설정

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

명령어	설명
ip dhcp snooping verify mac-address	■ DHCP Client Identifier 또는 Client HW Address 가 변조된 경우, 이 패킷을 Drop 시킨다. ■ 기본적으로, 이 특성은 활성화 되어 있다.

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

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

6.3.10. DHCP Snooping Manual Binding 설정

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

명령어	설명
ip dhcp snooping binding *H.H.H* **vlan** *<1-4094>* *A.B.C.D* **interface** *IFNAME*	■ MAC-Address 가 *H.H.H* 인 DHCP Client 를 지정된 Interface 에서 IP *A.B.C.D* 를 사용하며, lease time 은 Infinite 이다.

다음의 예제는 MAC 이 1111.2222.333 인 가입자가, Vlan 1 의 **gi2** 포트에 연결되어 IP 100.0.0.10 을 사용하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping binding 1111.2222.3333 vlan 1 100.0.0.10
interface gi2
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
             (H) - Invalid Client HW Address, (R) - Rate Limit Dropped
             (M) - Mac Validation Check Dropped

Mac Address    IP Address        State                Lease(sec) Vlan Interface
-------------- --------------- -------------------    ---------- ---- ---------
1111.2222.3333 100.0.0.10      Manual               Infinite      1 gi2
total 4 bindings found
```

6.4. DHCP Server 모니터링 및 관리

6.4.1. DHCP Server Pool 정보 조회

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

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

6.4.2. DHCP Server 바인딩 정보 조회

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

명령	목적
show ip dhcp binding	■ DHCP Server 에 생성된 모든 바인딩을 출력
show ip dhcp binding detail	■ DHCP Server 에 생성된 모든 바인딩를 좀 더 상세한 형태로 출력
show ip dhcp binding network-pool {address |name}	■ DHCP Server 에 생성된 바인딩 정보 중 네크워크 Pool 에 속하는 바인딩 정보를 출력 ■ address : Address 에 해당하는 바인딩 정보 출력 ■ name : 이름에 해당하는 Network Pool 내의 모든 바인딩 정보 출력
show ip dhcp binding host-pool {address|name}	■ DHCP Server 에 생성된 바인딩 정보 중 Host Pool 에 속하는 바인딩 정보를 출력 ■ address : Address 에 해당하는 바인딩 정보 출력 ■ name : 이름에 해당하는 Host Pool 내의 모든 바인딩 정보 출력

6.4.3. DHCP Server 통계 정보 조회

명령	목적
show ip dhcp server statistics	■ Server 의 통계와 송수신한 메시지와 관련된 카운터 정보를 출력

6.4.4. DHCP Server 충돌 정보 조회

명령	목적
show ip dhcp conflict *{poolname}*	■ DHCP Server 에 의해 기록된 모든 Address 충돌을 출력 ■ 특정 Pool 에서 발생한 충돌 정보 출력

6.4.5. DHCP Server 변수 초기화 명령어

명령어	설명
`clear ip dhcp binding {address|*}`	■ DHCP 데이터베이스로부터 자동 Address 바인딩을 삭제 ■ *address* 를 명시하면 명시된 IP Address 의 자동 바인딩을, "*"를 사용하면 모든 자동 바인딩을 삭제
`clear ip dhcp server statistics`	■ DHCP Server 의 모든 통계 카운터를 초기화

6.4.6. DHCP Server 디버그 명령어

명령어	설명
`debug ip dhcp server {events|packets}`	■ DHCP Server 의 디버깅 기능을 활성화

6.5. DHCP relay 모니터링 및 관리

표 5. DHCP relay 모니터링 및 관리 명령어

명령어	설명
`show ip dhcp helper-address`	■ DHCP Server 의 목록을 출력
`show ip dhcp relay information option`	■ DHCP relay information option 의 활성화 및 재중계 정책을 출력
`show ip dhcp relay statistics`	■ relay 의 통계와 송수신한 메시지와 관련된 카운터 정보를 출력
`debug ip dhcp relay {events|packets}`	■ DHCP relay 의 디버깅 기능을 활성화

6.6. DHCP Snooping 모니터링 및 관리

DHCP Snooping 모니터링 및 관리 명령어

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

6.7. DHCP 설정 예제

이 절에서는 다음의 설정 예를 제공한다.

- DHCP Network Pool 설정 예제
- DHCP Host Pool 설정 예제
- DHCP Server 모니터링 및 관리 예제
- DHCP Relay Agent 설정 예제
- DHCP Relay Agent 모니터링 및 관리 예제

6.7.1. DHCP Network Pool 설정 예제

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

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

```
Switch(config-dhcp)# range 192.168.1.10 192.168.1.100
Switch(config-dhcp)# range 192.168.1.150 192.168.1.230
```

다음의 예제는 하나의 vlan 이 192.168.2.0/24 와 192.168.3.0/24 를 갖는 인터페이스에 대한 Network Pool 및 그룹 설정 과정이다. 192.168.2.0/24 Network 의 default-router 는 192.168.2.1 이며, 할당 Address 범위로 192.168.2.10~192.168.240 을 사용하며, 192.168.3.0/24 Network 의 default-router 는 192.168.3.1 이며, 할당 Address 범위는 192.168.3.10~192.168.3.50 과 192.168.3.100~192.168.3.230 을 사용한다. 그리고, DNS Server 는 모두 1.2.3.4 와 1.2.3.5 를 사용한다. 각 Client 는 IP Address 의 임대를 12 시간까지 보장 받는다.

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

6.7.2. DHCP Host Pool 설정 예제

다음 예는 192.168.4.0/24 Network 에 속하는 Host Pool 의 구성을 보여준다. default-router 로 192.168.4.1 사용하며, ubiquoss.com 을 domain name 으로, 192.168.4.10 과 192.168.4.11 을 dns-server 로 사용하는 Client 들을 위한 Host Pool 이다. 그리고, Client 의 MAC Address 가 00:01:02:94:77:d7, 00:01:02:94:77:d8, 00:01:02:94:77:d9 인 Client 에게 192.168.4.114, 192.168.4.115, 192.168.4.116 의 IP Address 와 255.255.255.0 의 Network 마스크가 할당된다. 수동 바인딩으로 할당된 IP Address 는 영구적으로 사용된다.

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

```
Switch(config-dhcp-host)# exit
Switch(config-dhcp)# host  192.168.4.115 255.255.255.0
Switch(config-dhcp-host)# hardware-address  00:01:02:94:77:d8
Switch(config-dhcp-host)# exit
Switch(config-dhcp)# host  192.168.4.116 255.255.255.0
Switch(config-dhcp-host)# hardware-address  00:01:02:94:77:d9
```

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

6.7.3. DHCP Server 모니터링 및 관리 예제

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

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

```
Switch# show ip dhcp pool network-pool sales1
Address pool Name             Sales
Type                          Network
Default router                192.168.2.1
Lease                         0 days, 12 hours, 0 minutes
DNS server                    1.2.3.4   1.2.3.5
Network                       192.168.2.0      255.255.255.0
Range(s)
                              192.168.2.10  ~  192.168.2.240
group                         vlan10
```

```
Switch# show ip dhcp pool host-pool mars
Address pool Name              Sales
Type                           Host
Lease                          infinite
Default router                 192.168.4.1
DNS server                     192.168.4.10 192.168.4.11
Domain name                    ubiquoss.com
Network                        192.168.4.0/24

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

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

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

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

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

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

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

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

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

```
------------------------------------------------------------------------
TYPE                    : Manual
IP addr                 : 192.168.4.116
HW addr                 : 00:01:02:94:77:d9
Client ID               : -
Host Name               : -
Lease                   : Infinite
------------------------------------------------------------------------
total 3 bindings found
```

다음의 예제는 Client 에게 이미 바인딩 된 IP Address 를 DHCP Server 가 사용할 수 있도록(다른 Client 의 IP Address 로 사용하도록 시도), DHCP Server 의 바인딩 정보를 삭제한다.

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

다음의 예제는 DHCP Server 의 통계자료를 보여준다.

```
Switch# show ip dhcp server statistics
Message                                 Received
Malformed messages                      0
BOOTREQUEST                             0
DHCPDISCOVER                            200
DHCPREQUEST                             178
DHCPDECLINE                             0
DHCPRELEASE                             0
DHCPINFORM                              0
ICMPECHO

Message                                 Sent
BOOTREPLY                               0
DHCPOFFER                               190
DHCPACK                                 172
DHCPNAK                                 6
```

6.7.4. DHCP Relay Agent 설정

다음의 예제는 스위치의 DHCP Relay Agent 가 Client 의 요구를 전달한 DHCP Server 를 설정한다. Client 의 요구를 만족시키는 DHCP Address Pool 이 없을 경우에 스위치는 다른 서브 Network 에 위치한 DHCP Server 로 Client 의 요구를 전달한다.

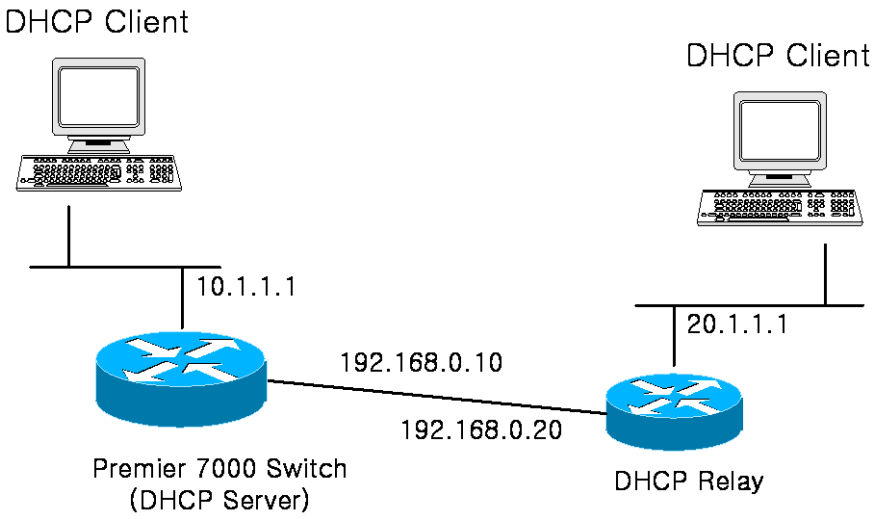


그림 6-7. 예제 Network – DHCP Relay agent 환경 설정

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

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

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

Notice 다른 서브 Network 에 위치한 DHCP Server 로 DHCP 메시지를 전달하려면, 해당 Network 에 대한 라우팅 경로 정보가 설정되어 있어야 한다.

Client-packets relayed	클라이언트가 전송한 패킷을 서버로 포워딩하는데 성공함
Client-packets errored	클라이언트가 전송한 패킷을 서버로 포워딩하는데 실패함
Server-packets relayed	서버가 전송한 패킷을 클라이언트로 포워딩한는데 성공함
Server-packets errored	서버가 전송한 패킷을 클라이언트로 포워딩하는데 실패함
Giaddr errored	서버로부터 수신한 DHCP Packet 에 giaddr 가 없음
Corrupt agent options	Agent 장비에 Option82 이 Enable 되어 있을 때, 서버로부터 수신 한 DHCP 패킷에 Option82 정보에 오류가 있음(Option82 Length 정보와 실제 Option82 Length 가 서로 다름)
Missing agent options	Relay Agent 장비에 Option82 이 Enable 되어 있을 때, 서버로부터 수신 한 DHCP 패킷에 Option82 정보가 없음
Bad circuit id	Relay Agent 장비에 Option82 이 Enable 되어 있을 때, 서버로부터 수신 한 DHCP 패킷 Option82 정보 중 circuit id(가입자 Interface 정보)에 오류가 있음 (DHCP 패킷의 circuit Id 정보가 DHCP Relay 장비의 circuit id list 에 없음)
Missing circuit id	Relay Agent 장비에 Option82 이 Enable 되어 있을 때, 서버로부터 수신 한 DHCP 패킷 Option82 정보 중 circuit id(가입자 Interface 정보가 없음)

7

NAT

본 장에서는 Premier 8624XG 스위치에서의 NAT 설정에 대해 설명한다.

7.1. NAT 개요

Network Address Translation (NAT)는 인터넷의 폭발적인 성장으로 인한 IP 주소 부족 문제에 대한 해결책의 하나로 생겨나게 되었다. NAT 는 어떤 조직의 IP 네트웍이 실제로 사용되는 IP 주소 공간이 아닌 다른 IP 주소 공간으로 외부에 보이게끔 한다. 이리하여, 사설 IP 주소를 사용하는 특정 조직은 이러한 주소를 공인 IP 주소로 변환하여 인터넷에 접속이 가능하게 된다. NAT 는 RFC 1631 에 기술되어진다.

7.2. NAT 설정

NAT translation 을 설정을 시작하기 전에 private 네트워크에서 사용할 inside address 와 public 네크워크에서 사용할 outside address 를 미리 알고 있어야만 한다.

Premier 8624XG 스위치에서는 다음과 같은 세 가지 NAT 변환 방식이 가능하다.

- static translation : 특정 inside address 를 특정 outside address 로 변환.
- dynamic translation : 여러 inside address 들에 대해 하나 이상의 outside address 로 IP 주소로 변환. Premier 8624XG Series 는 사용할 outside address 의 선택 방법에 따라 세가지의 dynamic translation 을 제공한다.
  - MASQUERADE : outside address 를 특별히 지정하지 않고, outside interface 에 해당하

는 address 를 사용한다.

- PAT : 하나의 outside address 만을 사용한다.
- NAT : 두개 이상의 outside address 를 사용한다.

- local translation : Premier 스위치로부터 발생되는 트래픽의 source IP 를 변경하는 방식으로 각 프로토콜별, 포트별, 목적지별로 설정 가능하다.

Premier 8624XG 스위치에서의 각각의 NAT 설정에 대해서 설명한다.

7.2.1. Static NAT 설정

특정 하나의 private IP 주소를 다른 하나의 공인 IP 주소로 변경하여 전송하는 방식으로 Global mode 에서 다음의 명령어를 수행한다.

명령어	설명
ip nat static inside *IFNAME address* **outside** *IFNAME address*	▪ static nat 를 위한 private 네트워크와 publice 네크워크 구성

설정 예제는 다음과 같다.

```
Switch# configure terminal
Switch(config)# ip nat static inside vlan1 192.168.0.1 outside
vlan2 200.1.1.1
```

7.2.2. Dynamic NAT 설정

주소 변환 방식 중 하나인 dynamic translation 을 적용하기 위해서 다음의 명령어를 이용하여 설정한다.

7.2.2.1. Dynamic NAT 를 Masquerade mode 로 설정

Dynamic NAT 를 Masquerade 로 설정 할 경우 inside 네트워크에 속하는 패킷의 source IP 는 outside IFNAME 에 해당하는 주소로 변경하여 전송된다.

명령어	설명
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME*	▪ inside 네트워크를 위한 pool 구성 ▪ outside 인터페이스 설정

Masquerade mode 를 설정하는 예제는 다음과 같다. private 으로 vlan1 과 192.168.1.0/24 네트워크를

정의하며, outgoing 인터페이스로 vlan2 를 정한다.

```
SWITCH# configure terminal
SWITCH(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2
```

7.2.2.2. Dynamic NAT 를 PAT mode 로 설정

Global mode 에서 다음의 명령어를 이용하여 PAT(Port Address Translation) mode 로 NAT 를 설정한다. Dynamic NAT 를 PAT 로 설정 할 경우 inside 네트워크에 속하는 패킷의 source IP 는 outside address 로 설정된 하나의 IP 로 변경하여 전송된다.

명령어	설명
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME address*	■ inside 네트워크를 위한 pool 구성 ■ outside 인터페이스 설정과 변환될 IP 설정

다음은 Dynamic NAT 를 PAT mode 로 설정하도록 하며, vlan1 에서 발생하는 트래픽 중에 source IP 가 192.168.1.0/24 에 해당하는 패킷의 소스 IP 를 200.1.1.1 로 변환하여 전송한다.

```
SWITCH# configure terminal
SWITCH(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2 200.1.1.1
```

7.2.2.3. Dynamic NAT 를 NAT mode 로 설정

Globla mode 에서 다음의 명령어를 이용하여 NAT mode 로 Dynamic NAT 를 설정한다. Dynamic NAT 를 NAT mode 로 설정 할 경우 inside 네트워크에 속하는 패킷의 source IP 는 outside 풀로 설정된 여러 IP 중에 하나로 변경하여 전송된다.

명령어	설명
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME lowest-address highest-address*	■ inside 네트워크를 위한 pool 구성 ■ outside 인터페이스 설정과 변환될 IP pool 설정

다음은 Dynamic NAT 를 NAT mode 로 설정하도록 하며, vlan1 에서 발생하는 트래픽 중에 source IP 가 192.168.1.0/24 에 해당하는 패킷의 소스 IP 를 200.1.1.1~ 200.1.1.4 중의 하나로 변환하여 전송한다.

```
SWITCH# configure terminal
SWITCH(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2 200.1.1.1
```

Notice NAT 설정 후 flow-rule(매뉴얼 12 장, 1.5 절 참조)을 설정하여야 한다.

```
SWITCH# configure terminal
SWITCH(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2 200.1.1.1
SWITCH(config)# flow-rule nat classfy ip 192.168.1.0/24 any
SWITCH(config)# flow-rule nat match trapcpu
SWITCH(config)# policy-map nat flow-rule nat
SWITCH(config)# interface vlan10
SWITCH(config-if-vlan10)# service-policy nat
SWITCH(config-if-vlan10)# exit
SWITCH(config)# exit
```

Notice 기존 vlan10 에 policy-map 이 이미 적용되어진 경우에는 해당 policy-map 에 NAT flow-rule 를 추가하여야 한다.

7.2.3. local NAT 설정

local NAT 는 Premier 스위치로부터 발생되는 트래픽의 소스 IP 를 변환하는 방식으로 다음의 명령어를 이용하여 설정한다.

명령어	설명
ip nat local inside *source-netnum/prefix-len protocol portnum destionation-netnum/prefix-len* **outside** *address*	■ protocol : tcp, udp, icmp, 특정 설정이 없는 경우는 any ■ portnum : 적용할 포트 번호 또는 특정 포트를 구분하지 않을 경우는 any ■ destionation-netnum/prefix : 특정 목적지로 향하는 트래픽의 변환, 특별히 구분하지 않을 경우는 any ■ address : 변경 할 IP

다음 예제는 Premier 스위치에서 발생하는 트래픽 중 소스 IP 가 10.1.1.0/24 인 트래픽 중 ftp 서버 20.1.1.1 로 향하는 트래픽의 소스 IP 변환 예이다.

```
SWITCH# configure terminal
SWITCH(config)# ip nat local inside 10.1.1.0/24 tcp 21 20.1.1.1/32
outside 200.1.1.1
```

```
Switch# show ip nat static
MODE     Private IP       Public IP                    Direction
STATIC 10.2.2.10          200.1.1.101                  vlan3->vlan2
total 1 pools found
```

Notice 포트 번호는 프로토콜로서 TCP 또는 UDP 가 설정된 경우에만 설정 가능하다. 또한, 특정하게 정하기를 원치않는 필드는 any 로 설정하면 된다.

7.2.4. NAT 활성화

먼저, NAT 가 동작하기 위해서는 Global mode 에서 다음의 명령어를 이용하여 NAT 엔진을 활성화시킨다.

명령어	설명
service nat	NAT 엔진을 활성화시키다.

```
Switch# configure terminal
Switch(config)# service nat
Switch(config)# exit
```

7.3. NAT 설정 보기

7.3.1. Static NAT 설정 정보 조회

명령어	설명
show ip nat static	Static NAT 의 현재 설정 정보를 출력

다음은 vlan3 인터페이스를 10.2.3.0/24 로 설정한 후에, static nat 를 설정했을 때의 설정 정보이다.

7.3.2. Dynamic NAT 설정 정보 조회

명령어	설명
show ip nat dynamic	Dynamic NAT 의 현재 설정 정보를 출력

다음은 vlan1 인터페이스를 10.1.1.0/16 으로 설정한 후에, dynamic nat 를 각각 다른 대역에 대해 Masquerade, PAT 그리고 NAT 모드로 설정했을 때의 설정 정보이다.

```
Switch# show ip nat dynamic
MODE     Private IP       Public IP                    Direction
MASQ     10.1.0.0/25      -                            vlan1->vlan2
PAT      10.1.0.128/26    200.1.1.100                  vlan1->vlan2
NAT      10.1.0.192/26    200.1.1.200-200.1.1.204      vlan1->vlan2
total 3 pools found
```

7.3.3. Local NAT 설정 정보 조회

명령어	설명
show ip nat local	Local NAT 의 현재 설정 정보를 출력

```
Switch# show ip nat local
MODE       SRC-IP           PROTO   PORT  DEST-IP              PUB-IP
LOCAL      10.1.1.0/24      tcp     23    210.108.10.0/24      200.1.1.99
LOCAL      10.1.1.0/24      tcp     21    20.1.1.1/32          200.1.1.1
total 2 pools found
```

8

IGMP Snooping

본 장에서는 Premier 8624XG 스위치에서의 IGMP Snooping 설정에 대해 설명한다.

8.1. IGMP Snooping 개요

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

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

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

8.2. IGMP Snooping 설정

IGMP Snooping 은 Global 하게 enable/disable 이 가능하며, 또한, VLAN 별로 역시 enable/disable 이 가능하다. 기본적으로 IGMP Snooping 이 Global 하게 enable 되어 있어야 동작하게 된다.

8.2.1. Enable Global IGMP Snooping

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

명령어	설명
ip igmp snooping	IGMP Snooping 을 enable 한다.
no ip igmp snooping	IGMP Snooping 을 disable 한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping
Switch (config)#
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED

IGMP snooping is DISABLED on ALL interface
IGMP snooping fast-leave is DISABLED on ALL interface
```

8.2.2. Enable IGMP-TRAP on an interface

Switch 에서 IGMP Snooping 이 동작중인 동안에는 IGMP packet 들을 수신할 수 있도록 각 port interface 에서 IGMP-TRAP 을 반드시 enable 해야 한다.

IGMP-TRAP 을 설정하기 위해서는 다음의 명령을 Interface configuration mode 에서 사용한다.

명령어	설명
igmp-trap	해당 인터페이스에 igmp-trap 를 enable 한다.
no igmp-trap	igmp-trap 를 Disable 한다.

```
Switch # configure terminal
Switch (config)# interface gi1
Switch (config-if-gi1)# igmp-trap
Switch # show running-configure

…
!
interface gi1
 igmp-trap
!
…
Switch #
```

8.2.3. Enable IGMP Snooping on a VLAN

본 장비에서는 IGMP Snooping 을 VLAN 별로 enable/disable 할 수 있다.

실제 IGMP Snooping 이 적용 될 VLAN 을 설정하기 위해서는 다음의 명령을 global configuration mode 에서 사용한다.

명령어	설명
ip igmp snooping vlan *<1-4096>*	특정 VLAN 에 IGMP Snooping 을 enable 한다.
no ip igmp snooping vlan *<1-4096>*	특정 VLAN 에 IGMP Snooping 을 disable 한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping
Switch (config)# ip igmp snooping vlan 1
Switch (config)#
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is DISABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
Switch #
```

8.2.4. Configure IGMP Snooping Functionality

IGMP Snooping 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행한다.

8.2.4.1. report-suppression 설정

기본적으로 IGMP Snooping 의 IGMP report-suppression 은 Disable 상태이며, 수신된 모든 IGMP Report 들은 Multicast Router 로 Forward 된다. IGMP report-suppression 을 Enable 하면, IGMP Snooping 은 Multicast Membership Group 마다 하나의 IGMP Report 만 Multicast Router 로 Forward 된다.
이 기능은 IGMPv1 및 IGMPv2 Report 메시지에 한해서 적용된다.

명령	설명
ip igmp snooping report-suppression	IGMP report-suppression 을 설정한다.
no ip igmp snooping report-suppression	설정된 IGMP report-suppression 을 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping report-suppression
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED
 - IGMP Report Suppression   : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is DISABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
```

8.2.4.2. fast-leave 설정

IGMP Snooping 의 fast-leave 기능을 enable 하면 스위치가 호스트로부터 IGMPv2 Leave 메시지를 받

았을 때 해당 포트를 포워딩 테이블에서 즉시 제거하게 된다.
이 기능은 VLAN 의 각 포트에 호스트가 하나인 경우에만 사용하여야 한다. 만약, 포트에 여러 호스트가 속해 있는 경우에 이 기능을 사용하면. IGMPv2 Leave 메시지를 보내지 않은 호스트들도 일정시간 동안 Leave 가 된 멀티캐스트 그룹에 대한 트래픽을 받지 못하게 되는 경우가 발생하게 된다. 또한, 이 기능은 모든 호스트들이 Leave 메시지가 지원되는 IGMPv2 를 사용하는 경우에만 유효하다.

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

명령	설명
ip igmp snooping vlan *<1-4096>* **fast-leave**	특정 VLAN 에 fast-leave 기능을 설정한다.
no ip igmp snooping vlan *<1-4096>* **fast-leave**	설정된 VLAN 에 fast-leave 기능을 해제한다
ip igmp snooping vlan *<1-4096>* **fast-leave** *IFNAME*	특정 VLAN 의 PORT 에 fast-leave 를 설정한다.
no ip igmp snooping vlan *<1-4096>* **fast-leave** *IFNAME*	특정 VLAN 의 PORT 에 설정된 fast-leave 를 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave gi1
Switch (config)# ip igmp snooping vlan 1 fast-leave gi2
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is ENABLED on gi1 gi2
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4

Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
Switch #
```

8.2.4.3. mrouter 설정

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

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

위와 같은 방법으로 알게 된 mrouter port 들은 새로운 Multicast Forwarding Table Entry 가 생성될 때마다 항상 outgoing 포트로 등록되며, Multicast Traffic 뿐만 아니라 Host 에서 전송하는 IGMP Join 메시지도 Mrouter port 로 Forwarding 된다.

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

명령어	설명
ip igmp snooping vlan *<1-4096>* **mrouter interface** *IFNAME*	mrouter port 를 수동으로 설정한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.
no ip igmp snooping vlan *<1-4096>* **mrouter interface** *IFNAME*	설정된 mrouter port 를 해제한다.

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

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

명령어	설명
ip igmp snooping vlan *<1-4096>*	PIM/DVMRP 프로토콜을 Snooping 하여 mrouter port 를

mrouter learn pim-dvmrp	감지하도록 설정한다.
no ip igmp snooping vlan *<1-4096>* **mrouter learn pim-dvmrp**	설정된 PIM/DVMRP 프로토콜을 이용한 mrouter 감지를 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is DISABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
```

8.2.4.4. aging time 설정

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

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

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

명령어	설명
ip igmp snooping aging *<30-3600>*	aging time 을 설정한다. (Default : 300 초)
no ip igmp snooping aging	aging time 을 기본값으로 설정한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping aging 250
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 250 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is DISABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
```

8.2.4.5. last-member-join-interval 설정

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

만약, last-member-join-interval 이 설정되어 있지 않다면 last-member-join-interval 은 default 10 초로 자동 설정되며, 해당 포트는 IGMP Snooping 의 last-member-join-interval 에 준하여 제거된다. 이 기능은 VLAN 에 fast-leave 기능이 설정되어 있지 않은 경우에만 유효하다.

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

명령어	설명
ip igmp snooping last-member-join-interval *<5-300>*	last-member-join-interval 을 설정한다. (Default : 10 초)
no ip igmp snooping last-member-join-interval	last-member-join-interval 을 기본값으로 설정한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping last-member-join-interval 50
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 50 sec
 - TCN Query Solicit         : DISABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is DISABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
```

8.2.4.6. tcn (Topology Change Notification) 설정

기본적으로 IGMP Snooping 은 spanning-tree Topology Change Notification(TCN)을 수신하였을 때, Multicast Forwarding Table Entry 를 모두 초기화한다. 이후, Multicast Router 의 IGMP Query 에 의해서 Multicast Forwarding Table Entry 가 새로 생성되게 된다.

본 장비에서 제공되는 tcn 설정은 spanning-tree Topology Change Notification(TCN)을 수신하였을 때, Multicast Router 에게 “0.0.0.0” Group 에 대해서 IGMP Leave 메시지를 전송한다. Multicast Router 는 “0.0.0.0” Group 에 대한 IGMP Leave 메시지를 수신한 후, IGMP Query 메시지를 전송하게 되며, 빠른 시간내에 Topology 가 변경된 Network 의 Multicast Forwarding Table Entry 가 새로 생성되게 된다.

tcn 의 설정은 spanning-tree 로 형성된 모든 장비에 설정 가능하며, 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping tcn query-solicit	TCN Query-Solicit 을 설정한다.
no ip igmp snooping tcn query-solicit	설정된 TCN Query-Solicit 을 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping tcn query-solicit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP snooping fast-leave is DISABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members : gi1 gi2 gi3 gi4
```

8.2.4.7. igmp filtering 설정

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

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

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

명령어	설명
ip igmp snooping profile <*1-99*> permit <*multicast address*> range <*multicast address*>	IGMP Filtering 을 허용하는 IGMP Profile 을 설정한다.
ip igmp snooping profile <*1-99*> deny *{*<*multicast address*> | <*all*>*}* range <*multicast address*>	IGMP Filtering 을 차단하는 IGMP Profile 을 설정한다.
no ip igmp snooping profile <*1-99*>	설정된 IGMP Profile 을 삭제한다.

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

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

명령어	설명
ip igmp snoop-filter *<1-99>*	IGMP Filtering 을 스위치 포트에 적용한다.
no ip igmp snoop-filter *<1-99>*	설정된 IGMP Filtering 을 해제한다.

```
Switch # configure terminal
Switch (config)# interface gi1
Switch (config-if-gi1)# ip igmp snoop-filter 1
Switch # show running-configure
…
!
interface gi1
   ip igmp snoop-filter 1
!
…
Switch #
```

8.2.4.8. igmp max-group-count 설정

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

명령어	설명
ip igmp snooping max-group-count *IFANME <count>*	max-group-count 를 스위치 포트에 적용

	한다.
no ip igmp snooping max-group-count *IFANME*	설정된 max-group-count 를 스위치 포트에서 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-group-count gi1 10
Switch # show running-configure

…
ip igmp snooping
ip igmp snooping max-group-count gi1 10
…

Switch #
```

8.2.4.9. igmp max-reporter-count 설정

각 VLAN interface 별로 가입자의 수를 제한하여 multicast service 를 제공하기 위해서 Host 의 개수를 제한할 수 있다.
Host 의 개수를 제한하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

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

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

명령어	설명
ip igmp snooping max-reporter-count port *IFNAME* <*count*>	max-reporter-count 를 Port 에 적용한다.
no ip igmp snooping max-reporter-count port *IFNAME*	설정된 max- reporter -count 를 PORT 에서 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-reporter-count port gi1 10
Switch #
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-reporter-count port gi1 10
…
Switch #
```

8.2.4.10. drop-igmp-ttl-over 설정

비 정상 packet 을 제한하여 multicast service 를 제공하기 위해서 TTL 을 제한할 수 있다.
허용된 TTL 을 초과하는 packet 을 제한하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping drop-igmp-ttl-over *<1-255>*	drop-igmp-ttl-over 를 적용한다.
no ip igmp snooping drop-igmp-ttl-over	설정된 drop-igmp-ttl-over 를 해제한다.

```
Switch # configure terminal
Switch(config)# ip igmp snooping drop-igmp-ttl-over 1
Switch(config)# exit
Switch # show running-configure

…
ip igmp snooping
ip igmp snooping drop-igmp-ttl-over 1
…
```

8.2.4.11. snooping ignore-mpkt-upstream-forward 설정

mrouter port 가 아닌 port 에서 multicast traffic 이 발생한경우, multicast traffic 은 mrouter port 로 전달된다. 네트워크 관리상의 이유로 mrouter port 로의 multicast traffic 전달을 제한할 수 있다.
Multicast traffic 의 전달을 제한하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping ignore-mpkt-upstream-forward	snooping ignore-mpkt-upstream-forward 를 적용한다.
no ip igmp snooping snooping ignore-mpkt-upstream-forward	설정된 snooping ignore-mpkt-upstream-forward 를 해제한다.

```
Switch # configure terminal
Switch(config)# ip igmp snooping ignore-mpkt-upstream-forward
Switch(config)# exit
Switch # show running-configure

…
ip igmp snooping
ip igmp snooping ignore-mpkt-upstream-forward
…
```

8.3. IGMP Proxy-Reporting 개요

일반적으로 Network 장비들의 처리능력은 한정되어 있지만, 다양한 Multicast Service 의 증가와 Multi-Accessed Network 환경 등으로 인해 동시에 처리되어야 하는 IGMP 의 Membership 요청이 증가되고 있다. 이러한 IGMP HOST 들의 IGMP Membership 요청은 상위 Network 에 위치한 장비의 과부하를 초래할 수 있으며, Multicast Service 의 지연 또는 단절을 초래할 수 있다.
이러한 이유로 인해 DSL Forum 에서는 IGMP Proxy-Reporting 의 기능을 정의한 문서를 제공하고 있으며, 본 장비에서는 DSL Forum 에서 정의한 IGMP Proxy-Reporting 기능을 포함하고 있다.

IGMP Proxy-Reporting 은 IGMP 에서 규정된 모든 기능을 제공한다. IGMP Proxy-Reporting 은 IGMP Proxy-Reporting 이 활성화된 VLAN interface 에 IP Address 가 존재하는 경우 IGMP Report 및 IGMP Query 메시지의 IP Source Address 를 지정된 VLAN 의 IP Address 를 사용하며, VLAN 의 IP Address 가 지정되지 않는 경우에는 IGMP Membership 에서 관리되는 가장 최신의 IGMP Host Address 를 사용한다.

8.4. IGMP Proxy-Reporting 설정

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

8.4.1. Enable IGMP Proxy-Reporting

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

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

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


IGMP Gateway is DISABLED on ALL interface.

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

8.4.2. Enable IGMP Proxy-Reporting on a VLAN

본 장비에서는 IGMP Proxy-Reporting 을 VLAN 별로 enable/disable 할 수 있다.
실제 IGMP Proxy-Reporting 기능이 적용될 VLAN 을 설정하기 위해서는 다음의 명령을 global configuration mode 에서 사용한다.
IGMP Proxy-Reporting 기능이 적용된 VLAN 에서는 IGMP Snooping 을 통한 IGMP 패킷 Forwarding 이 이루어지지 않는다.

명령어	설명
ip igmp snooping proxy-reporting vlan *<1-4096>*	특정 VLAN 에 IGMP Proxy-Reporting 을 enable 한다.
no ip igmp snooping proxy-reporting vlan *<1-4096>*	특정 VLAN 에 IGMP Proxy-Reporting 을 disable 한다.

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

vlan1
        IGMP Proxy is ENABLED on this interface
        IGMP Query-Interval is 60 seconds.
        IGMP Leave-Timeout  is 10 seconds.
        IGMP Query-Max-Response-Time is 10 seconds.
        Multicast Router Port : NOT CONFIGURED!
        VLAN Members :
             gi1 gi2 gi3 gi4

_____________________________________________________________________
total : 1

Switch #
```

8.4.3. Configure IGMP Proxy-Reporting Functionality

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

8.4.3.1. Multicast Router Port 지정

IGMP Proxy-Reporting 에서 관리되는 IGMP Membership 의 정보와 상위 Multicast Router 와의 연동을 위해서 Static 하게 Multicast Router Port 를 지정할 수 있다. Proxy-Reporting 이 enable 된 VLAN 은 Dynamic 하게 IGMP Query Packet 이 수신된 Port 를 Multicast Router Port 로 인식한다.

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

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 mrouter-port
 gi1
Switch (config)#
Switch # show ip igmp snooping proxy-reporting interface
IGMP Proxy Interface

vlan1
        IGMP Proxy is ENABLED on this interface
        IGMP Query-Interval is 60 seconds.
        IGMP Leave-Timeout  is 10 seconds.
        IGMP Query-Max-Response-Time is 10 seconds.
        Multicast Router Port : gi1
        VLAN Members :
             gi1 gi2 gi3 gi4

------------------------------------------------------------------
total : 1
```

8.4.3.2. IGMP Static-Group 지정

IGMP Proxy-Reporting 에서는 특정한 Multicast Group 의 Traffic 을 수신하기 위해서 소요되는 Join Delay Time 을 최소화하기 위해서 Static-Group 기능을 제공한다.
Static-Group 은 Multicast-Router Port 로 지정된 IGMP Report 를 주기적으로 전송하여 Multicast

Traffic 을 계속해서 수신하기 위해서 제공된다.
이 기능은 반드시 IGMP Snooping 과 함께 동작하여야 하며, 다음의 명령을 global configuration mode 에서 수행한다.

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

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

_____________________________________________________________
total : 1

Switch #
```

명령어	설명
ip igmp snooping proxy-reporting vlan <*1-4096*> **static-group** *A.B.C.D* to <*count*>	특정 VLAN 에 IGMP Proxy-Reporting 를 통한 IGMP Static-Group 을 count 만큼 지정한다.
no ip igmp snooping proxy-reporting vlan <*1-4096*> **static-group** *A.B.C.D* to <*count*>	지정된 IGMP Static-Group 을 count 만큼 해제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 static-group
224.1.1.1 to 2
Switch # show ip igmp snooping proxy-reporting group
  VLAN       GROUP         LAST-REPORTER    EXPIRE-TIME
  0080  224.1.1.1        0.0.0.0             00:04:03  STATIC-GROUP
  0080  224.1.1.2        0.0.0.0             00:04:03  STATIC-GROUP
_____________________________________________________________
total : 2

Switch #
```

8.5. Display System and Network Statistics

표 1 IGMP Snooping 관련 모니터링 명령어

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

표 2 IGMP Proxy-Reporting 관련 모니터링 명령어

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

표 3 설정 예제

```
interface gi1
  igmp-trap
  ip igmp snoop-filter 1
!
ip igmp snooping proxy-reporting
ip igmp snooping proxy-reporting vlan 1
!
ip igmp snooping
ip igmp snooping vlan 1
ip igmp snooping profile 1 permit 224.1.1.1/24 range 224.3.1.1/24
ip igmp snooping profile 1 permit 224.5.1.1/24 range 224.6.1.1/24
ip igmp snooping profile 1 deny all
```

9

IP 멀티캐스트 라우팅

본 장에서는 IP 멀티캐스트 라우팅의 구성요소와 Premier 8624XG 스위치에서의 IP 멀티캐스트 라우팅 설정에 대해 설명한다.

9.1. IP 멀티캐스트 라우팅 개요

IP 멀티캐스팅은 하나의 IP 호스트가 여러 IP 호스트들로 구성된 하나의 그룹으로 패킷을 전송할 수 있게 하는 기능이다. 이 호스트들의 그룹은 로컬 네트웍에 있는 장비들, 사설망내에 있는 장비들, 또는 로컬 네트웍 바깥의 장비들을 포함할 수 있다. 트래픽을 생성하는 호스트에서는 트래픽을 받고자하는 호스트들에 대해 각각의 패킷을 전송하는 것이 아니라 하나의 패킷만을 그 그룹으로 전송하는 것이다.

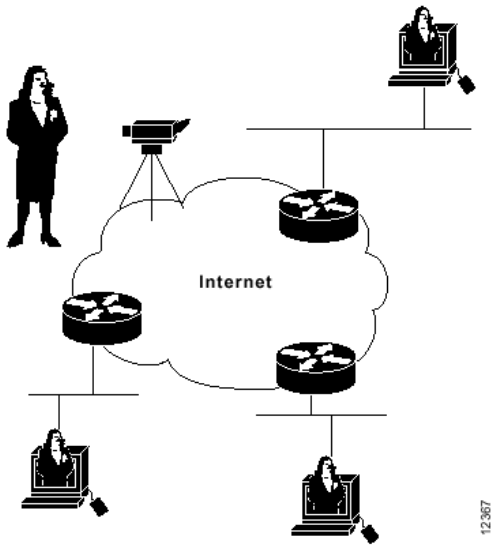


그림 9-1. 여러 목적지에 트래픽을 전달하는 방법을 제공하는 멀티캐스팅

여러 멀티캐스트 라우팅 프로토콜들은 멀티캐스트 그룹을 발견하고 각 그룹에 대한 경로를 생성하기

위해 사용된다. 예를 들면, Protocol-Independent Multicast (PIM), Distance-Vector Multicast Routing Protocol(DVMRP), Multicast Open Shortest Path First (MOSPF)와 같은 것들이 있다. 다음 <표-1 >은 각 프로토콜의 유니캐스트에 대한 요구 사항과 flooding 알고리즘을 요약한 것이다.

표 9-1. 멀티캐스트 프로토콜

프로토콜	유니캐스트 프로토콜	**flooding** 알고리즘
PIM-dense mode	Any	Reverse path flooding (RPF)
PIM-sparse mode	Any	RPF
DVMRP	Internal	RPF
MOSPF	OSPF	Shortest-path first

9.2. IGMP 개요

IGMP 는 IP 호스트가 IP 멀티캐스트 그룹 맴버쉽을 라우터에 등록하기 위해 사용되는 프로토콜이다. 라우터는 등록된 그룹의 맴버쉽 상태를 갱신하기 위하여 주기적으로 맴버쉽 질의를 한다. IP 호스트가 질의에 응답을 하면 그 그룹의 등록은 유지된다.

IP 멀티캐스트에서 사용되는 멀티캐스트 그룹 주소로 class D IP 주소가 사용되며 IGMPv2 는 RFC1112 에 정의되어 있다.

9.3. PIM-SM 개요

PIM-SM 은 다수의 멀티캐스트 데이터 스트림에 대해서 비교적 적은 수의 LAN 들을 연결하기위해 최적화된 멀티캐스트 라우팅 프로토콜이다. PIM-SM 은 rendezvous point 을 정의하는데 이것은 멀티캐스트 패킷의 라우팅을 편리하게 하기 위한 등록점으로 사용된다.

특정 멀티캐스트 서버가 인접한 멀티캐스트 라우터로 멀티캐스트 패킷을 전송하면, 인접한 멀티캐스트 라우터는 이 멀티캐스트 패킷을 rendezvous point 로 보낸다. 멀티캐스트 패킷을 수신하고자 하는 멀티캐스트 라우터는 rendezvous point 로부터 해당 멀티캐스트 패킷을 수신하여 호스트로 전송하게 된다.

9.4. IP 멀티캐스트 라우팅 설정

9.4.1. Enable IP 멀티캐스트 라우팅

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

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

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

9.4.2. Enable IGMP-TRAP on an interface

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

명령어	설명
igmp-trap	해당 인터페이스에 igmp-trap 를 enable 한다.
no igmp-trap	igmp-trap 를 Disable 한다.

```
Router# configure terminal
Router(config)# interface gi1
Router(config-if-gi1)# igmp-trap
```

9.4.3. Enable PIM on an interface

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

명령어	설명
ip pim	해당 인터페이스에 PIM Flag 를 enable 한다.
no ip pim	PIM Flag 를 Disable 한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim
Router# show ip pim interface
     Address      Interface Status Version/Mode   Nbr     JP      MCache CISCO PRI DR
                                                  Count   Intvl   Intvl  ChkSum
10.1.1.254        vlan11    DOWN   v2/Sparse      0       60        110   OFF   1 10.1.1.254
------------------------------------------------------------------------------------
total : 1
```

9.4.4. Enable IGMP on an interface

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

명령어	설명
ip igmp	해당 인터페이스에 IGMP Flag 를 enable 한다.
no ip igmp	IGMP Flag 를 Disable 한다.

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

9.4.5. Configure IGMP Functionality

IGMP 의 다양한 특성들에 대해 설정하기 위해서는 다음에 나오는 작업들을 수행한다.

9.4.5.1. IGMP Access Group

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

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

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

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

9.4.5.2. IGMP filter-receive-query

멀티캐스트 라우터는 query message 를 수신하면 querier selection 을 수행한다. 가입자 VLAN 에서 query message 가 수신되어도 querier selection 을 수행한다. 가입자 VLAN 의 라우터가 querier 로 선출되는 것을 제한하기 위해 query message 를 차단할 수 있다.

가입자 VLAN 에서 수신되는 query message 를 차단하기 위해서는 아래의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip igmp filter-receive-query	가입자 VLAN 에서 수신되는 query message 를 차단한다.
no ip igmp filter-receive-query	filter-receive-query 를 해제한다.

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

9.4.5.3. IGMP Query Transmit Interval

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

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

디폴트로 IGMP Querier Router 는 호스트와 네트웍의 IGMP 오버헤드를 낮게 유지하기 위하여 IGMP host-query 메시지를 125 초마다 보낸다. 이 메시지의 전송 간격을 변경하려면, 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp query-interval *seconds*	IGMP Querier Router 가 IGMP Query 메시지를 전송하는 간격을 설정 (Default : 125 초)
no ip igmp query-interval	설정된 IGMP Query Interval 을 기본값으로 설정한다.

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

9.4.5.4. IGMP Leave Timeout

IGMP Querier Router 는 Host 로부터 특정 Multicast Group 에 대해 탈퇴하는 IGMP Leave 메시지를 수신한 경우, Host 가 포함된 해당 VLAN 에 또다른 Multicast Group 에 가입된 Host 가 있는지 Multicast Membership 을 Checking 하게 된다.
해당 VLAN 의 Membership 을 Checking 한 후, Multicast Group 에 대한 Member 가 더 이상 존재하지 않으면, Multicast Membership 에서 삭제된다.

디폴트로 Multicast Membership Checking 시간은 260 초이다.

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

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

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

9.4.5.5. IGMP Member checking interval

IGMP Querier Router 는 Host 로부터 특정 Multicast Group 에 대해 탈퇴하는 IGMP Leave 메시지를 수신한 경우, Host 가 포함된 해당 VLAN 에 또다른 Multicast Group 에 가입된 Host 가 있는지 Multicast Membership 을 Checking 하게 된다.
Multicast Membership 을 Checking 하기 위해서 전송되는 IGMP Query 메시지는 TTL 을 1 로 하며, all-system-group-address 인 224.0.0.1 로 보내진다.
설정된 Member Checking Interval 은 IGMP Specific-Query Message 에 포함된 Max-Response-Time 으로 사용된다. Member Checking Interval 이 설정되지 않은 경우, IGMP Specific-Query Message 에 포함된 Max-Response-Time 은 Default “1”초이다.

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

명령어	설명
ip igmp member-checking-interval *seconds*	IGMP member checking interval 을 지정한다. (Default : 2 초)
no ip igmp member-checking-interval	설정된 IGMP member checking interval 을 기본값으로 설정한다.

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

9.4.5.6. IGMP Querier Timeout

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

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

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

명령어	설명
ip igmp querier-timeout *seconds*	IGMP Querier timeout 을 지정한다. (Default : 255 초)
no ip igmp querier-timeout	설정된 IGMP Querier timeout 을 기본값으로 설정한다.

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

9.4.5.7. IGMP Maximum Query Response Time

디폴트로 IGMP 에 Query 메시지에 의해 통지되는 maximum query response time 은 10 초이다. 이 값의 변경은 라우터가 IGMPv2 를 사용하고 있는 경우에만 가능하다. Host 는 IGMP query message 를 수신하면 query message 에 설정된 maximum query response time 값 이내의 임의의 시간에 report message 를 전송하게 된다. 이를 통하여 IGMP report 가 분산되어 전달되는 효과를 얻게 되는 것이다. 또한 이 값을 조절하여 Sub-Network 의 multicast traffic 의 flooding 을 tuning 할 수 있다.
설정된 Query-Response-Time 은 IGMP General Query 의 Max-Response-Time 으로만 사용된다.

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

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

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

9.4.5.8. IGMP query-based-port

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

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

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

9.4.6. Configure PIM-SM Functionality

PIM-SM v2 는 PIM-SM v1 에 대해 다음과 같은 개선점이 포함되었다.

- ✓ bootstrap router (BSR)은 fault-tolerant 한, 자동적인 RP discovery 와 distribution 메커니즘을 제공한다. 그러므로, 라우터들은 별도의 설정이 없이도 동적으로 group-to-RP 매핑을 할 수가 있다.
- ✓ PIM Join/Prune 메시지에 여러 address family 에 대한 유연한 인코딩이 가능하다.
- ✓ PIM 패킷은 더 이상 IGMP 패킷에 포함되지 않는다.

PIM-SM 은 PIM-SM 도메인의 모든 라우터들에 대한 각 그룹 prefix 에 대한 RP-set 정보를 발견하고 이를 공고하기 위하여 BSR 을 사용한다.

“Single point of failure”를 방지하기 위하여, PIM-SM 도메인 내에 여러 candidate BSR 를 설정할 수 있다. BSR 은 candidate BSR 들 중에서 자동적으로 선출된다. bootstrap 메시지를 이용하여 가장 우선순위가 높은 BSR 를 알아낸다. BSR 로 선출된 라우터는 PIM 도메인 내의 모든 라우터들에게 자신이 BSR 임을 알린다

Candidate RP 로 설정된 라우터들은 자신이 맡을 group 의 범위를 BSR 에게 유니캐스트로 알린다. BSR 은 bootstrap 메시지에 이 정보를 포함시키고 도메인 내의 모든 PIM 라우터들에 이 메시지를 전송한다. 이 정보를 바탕으로 모든 라우터는 특정 멀티캐스트 그룹에 대한 RP 를 알아낼 수 있게 된다. 라우터가 bootstrap 메시지를 받는 한, 라우터는 현재의 RP map 을 가지게 되는 것이다.

9.4.6.1. PIM-SM Assert Metric

Multi-Access Network 에서 Multicast Packet Originator 혹은 RP 로 평행한 Multicast Routing Path 가 존재할 수 있다. 이러한 Network 에서는 여러 Multicast Router 들로부터 복제된 동일한 패킷을 수신하는 Multicast Group Member 가 발생할 수 있다.
이러한 문제를 해결하기 위해서 PIM-SM 은 지정된 Assert Router 를 결정하기 위해서 PIM-SM Assert 메시지를 사용한다.

만약 모든 Multicast Router 들이 동일한 unicast protocol 을 사용하고 있다면, 최상의 메트릭을 가진 라우터가 Assert Router 로 지정된다. 예를 들어, 만약 모든 라우터가 RIP 를 사용하고 있다면, 가장 적은 홉 수를 지닌 라우터가 선택되며, 메트릭이 같다면, 최상위의 IP 주소를 지닌 라우터가 선택된다.
이러한 Assert 를 위한 Metric 의 기본값은 0xFFFFFFFF 이며, 설정의 변경은 interface configuration mode 에서 실행한다.

Assert Metric 을 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명

ip pim assert-metric *Metric Value*	Assert 메시지의 Metric 을 지정한다. (Default : 0xFFFFFFFF)
no ip pim assert-metric	설정된 Assert Metric 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim assert-metric 10
```

9.4.6.2. PIM-SM Assert Preference

Assert 를 위한 Metric Preference 의 기본값은 0x7FFFFFFF 이며, 가장 큰 Preference 의 값을 가진 Router 가 Assert Router 가 된다.

Metric Preference 를 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim assert-preference *Preference Value*	Assert 메시지의 Metric Preference 를 지정 (Default : 0x7FFFFFFF)
no ip pim assert-preference	설정된 Metric Preference 를 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim assert-Preference 10
```

9.4.6.3. PIM-SM BSR Border

해당 인터페이스로 bootstrap router (BSR) 메시지가 송수신 되는 것을 막고 싶을 때 사용한다

BSR Border 를 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim bsr-border	해당 인터페이스로의 BSR 메시지 송수신을 차단한다.
no ip pim bsr-border	설정된 인터페이스의 BSR 메시지 송수신 차단을 해제한다.

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

9.4.6.4. PIM-SM JoinPrune Interval

Multicast Router 는 Multicast Membership 을 유지하기 위해서 PIM-SM JoinPrune 메시지를 정기적으로 SPT 또는 RPT 의 Routing Path 의 Upstream Multicast Router 로 전송하며, Multicast Traffic 의 전달을 유지한다.

PIM-SM JoinPrune 메시지의 전송 주기의 기본값은 60 초이며, PIM-SM JoinPrune 메시지의 전송 주기를 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim jp-interval *Seconds*	PIM-SM JoinPrune 메시지의 전송주기를 설정 (Default : 60 초)
no ip pim jp-interval	설정된 JoinPrune 메시지의 전송주기를 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim jp-interval 30
```

9.4.6.5. PIM-SM mcache check interval

지정된 시간마다 Multicast Traffic 의 Flooding 유무를 검사한다. Multicast Traffic 이 더 이상 흐르지 않는 경우, Multicast Cache 에서 Multicast Entry 를 삭제하며 Multicast Membership Entry 를 갱신하게 된다.

Multicast Cache Check 주기의 기본값은 110 초이다.

Multicast Cache Check 주기를 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명

ip pim mcache-check-interval *Seconds*	Multicast Cache Check 주기를 설정한다. (Default : 110 초)
no ip pim mcache-check-interval	설정된 Multicast Cache Check 주기를 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim mcache-check-interval 220
```

9.4.6.6. PIM-SM Neighbor Filter

서브넷에 포함된 원하지 않는 PIM-SM Neighbor 로부터의 PIM-SM 프로토콜 메시지를 필터링하기를 원하는 경우 아래의 명령을 실행한다.

명령어	설명
ip pim neighbor-filter *access-list-number*	지정된 access-list 에 의해 PIM-SM 프로토콜 메시지를 차단한다.
no ip pim neighbor-filter	설정된 neighbor-filter 를 해제한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim neighbor-filter 1
```

9.4.6.7. PIM-SM Register Filtering

Multicast Packet 을 수신한 First-Hop Router 는 PIM Register 메시지를 RP 로 전송하여 Multicast Source 정보를 등록한다. 등록되는 Multicast Source 정보들에는 원하지 않은 Source 이거나 Group 에 대한 등록이 포함될 수 있으며, Network 운영자는 RP 또는 First-Hop Router 는 원하지 않은 특정 Source 또는 Group 에 대한 Register Filtering 을 제한할 수 있다.
Register Filtering 이 설정되면, 설정된 VLAN Interface 로의 PIM-SM Register 메시지 전송 또는 수신이 불가능하다.

Group 별 Register Filtering 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip pim register-filter-group *access-list-number*	지정된 access-list 에 의해 Register 되는 Group 을 차단한다.
no ip pim register-filter-group	설정된 register-filter 를 해제한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim register-filter-group 1
```

Source 별 Register Filtering 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip pim register-filter-source *access-list-number*	지정된 access-list 에 의해 Register 되는 Source 를 차단한다.
no ip pim register-filter-source	설정된 register-filter 를 해제한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim register-filter-source 1
```

9.4.6.8. PIM-SM Whole Packet Checksum

멀티캐스트 Originator 로부터 전송된 Multicast Packet 을 수신한 First-Hop 에 위치한 라우터는 RP 로 해당 Packet 을 PIM-SM Register 메시지 내에 포함하여 unicast routing 을 통하여 전달한다. 이 PIM-SM Register 메시지를 수신한 RP 는 메시지 내에 포함된 Multicast Packet 을 Multicast Membership Entry 에 전송하게 된다.

RFC 표준에 의하면, PIM-SM Register 메시지의 Checksum 은 Header 부분만 계산되지만, CISCO 라우터의 경우 Register 메시지 전체가 계산된다.
따라서 CISCO 라우터와 호환하기 위해서는 반드시 Checksum 의 계산은 메시지 전체가 되어야 한다.

Whole Packet Check 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim whole-packet-checksum	해당 Interface 를 CISCO 라우터와 호환하도록 설정한다.
no ip pim whole-packet-checksum	설정된 **whole-packet-checksum** 을 해제한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim whole-packet-checksum
```

9.4.6.9. PIM-SM DR priority

여러 라우터들이 멀티 엑세스 네트워크에 연결된 경우, 이 중 하나는 일정 시간 동안 join/prune 메시지를 RP 로 보내는 DR 로 작동되어야 한다. IP address 가 크거나, DR priority 가 크면 DR 로 선택된다.

DR priority 의 기본값은 1 이며, DR priority 를 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim dr-priority <*priority*>	해당 Interface 의 DR priority 를 설정한다.
no ip pim dr-priority	설정된 DR priority 를 기본값으로 바꾼다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim dr-priority 5
```

9.4.6.10. Candidate BSR

라우터가 candidate BSR 로 동작하기 위해서는 Network 의 Backbone 과 연결이 되어야 한다. 라우터를 Candidate BSR 로 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim bsr-candidate *ifname*	라우터가 BSR candidate 로 동작하도록 설정한다.

[*hash-mask-length*] [*priority*]	
no ip pim bsr-candidate *ifname*	설정된 BSR candidate 를 해제한다.

```
Router(config)# ip pim bsr-candidate vlan1 32 100
Router# show ip pim bsr-router
Local Bootstrap Router Information (state : ELECTED)
 BSR address : 100.1.1.254        Priority : 100   Hash-Mask-Length : 32
 Start-Time  : 00:00:29           Next Bootstrap in 00:00:38
```

9.4.6.11. Candidate RP

라우터가 candidate RP 로 동작하기 위해서는 Network 의 Multicast Backbone 과 연결이 되어야 한다. RP 는 전체 IP 멀티캐스트 주소 공간에 대해서, 또는 일부분에 대해서 서비스를 할 수 있다. Candidate RP 는 candidate RP advertisement 메시지를 BSR 에게 전송한다.

라우터를 Candidate RP 로 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim rp-candidate *ifname [rp-priority] [access-list-number]*	라우터가 RP candidate 로 동작하도록 설정한다.
no ip pim rp-candidate *ifname*	설정된 RP candidate 를 해제한다.

```
Router(config)# access-list 1 permit 224.1.1.0 255.255.255.0
Router(config)# access-list 1 permit 224.2.2.0 255.255.255.0
Router(config)# ip pim rp-candidate vlan10 10 1
Switch# show ip pim rp
SET of Rendezvous Point(RP) Informations.
 RP addr : 2.2.2.2
 Group   : 224.1.1.0  MaskLen : 24  Priority : 10  Holdtime : 150
 Group   : 224.2.2.0  MaskLen : 24  Priority : 10  Holdtime : 150
 Next Cand_RP_Advertisement in 00:00:30
```

9.4.6.12. Static RP

candidate RP 와 BSR 을 설정할 수 없는 Network 의 환경에서 특정 멀티캐스트 라우터의 interface 를 RP interface 로 지정하여 RP candidate 로서 수행하고자 할 때 설정할 수 있다.
설정된 Static RP 의 정보는 Bootstrap 메시지에 포함되지 않으며, 수신된 Bootstrap 의 RP 정보는 항

상 Static RP 의 정보보다 높은 priority 를 갖는다.

라우터에 Static RP 의 정보를 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim rp-address *address access list number*	라우터에 Static RP 정보를 설정한다.
no ip pim rp-address *address access list number*	설정된 Static RP 정보를 해제한다.

```
Router(config)# access-list 1 permit 224.1.1.0 255.255.255.0
Router(config)# access-list 2 permit 224.2.2.0 255.255.255.0
Router(config)# ip pim rp-address 200.1.1.254 1
Router(config)# ip pim rp-address 201.1.1.254 2
Switch# show ip pim rp
SET of Rendezvous Point(RP) Informations.
 RP addr : 200.1.1.254
 Group   : 224.1.1.0  MaskLen : 24   Priority : 196  Holdtime :
65535(Exp:18:12:15)

RP addr : 201.1.1.254
 Group   : 224.2.2.0  MaskLen : 24   Priority : 196  Holdtime :
65535(Exp:18:12:15)
```

9.4.6.13. Static Group

Multicast membership entry 에 IGMP 및 PIM-SM 의 가입시 Join Delay Time 이 발생된다. Static Group 은 RP 혹은 Server 와 연결된 First-Hop-Router 로부터 Static Group 이 설정된 라우터까지 해당 Multicast Traffic 을 미리 수신함으로서 Local Sub-Network 으로의 Traffic 전송을 빠르게 할 수 있다.

라우터에 Static Group 을 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim static-group <*multicast-address*>	라우터에 Static Group 정보를 설정한다.
no ip pim static-group <*multicast-address*>	설정된 Static Group 정보를 해제한다.

명령어	설명
ip pim static-group <*multicast-address*> *to* <*count*>	Static Group 을 지정된 count 만큼 설정한다.
no ip pim static-group <*multicast-address*> *to* <*count*>	Static Group 을 지정된 count 만큼 해제한다.

```
Router(config)# ip pim static-group 224.1.1.1
Router# show ip mroute
IP Multicast Routing Table
Timers: Uptime/Expires
Flags : C - Directly Connected Host, L - Local(Router is member)
        P - Pruned All,              F - Register
        J - Join SPT,                R - RP Bit
        X - Proxy Join Timer flag
Interface state: Interface, Next-Hop, State/Mode

_____________________________________________________________
(*, 224.1.1.1), 00:00:02/00:03:01, RP 192.168.1.254, flags: SRX
 Incoming interface: vlan10,  RPF nbr 10.1.1.2 STATIC-GROUP
 Outgoing interface list: Null

(20.1.1.254, 224.1.1.1) 00:00:02/00:03:01, RP 192.168.1.254, flags: S
 Incoming interface: vlan10,  RPF nbr 10.1.1.2
 Outgoing interface list: Null


_____________________________________________________________
 total    (*, G) : 1, (S, G) : 1
```

9.4.6.14. Static Join

특정한 Multicast Network 의 환경에 따라서 Multicast Membership 에 가입된 Member 가 존재하지 않는 Network 일지라도 Multicast Traffic 을 전송해야 될 경우가 있다.
이러한 경우, Multicast Traffic 을 전송해야 될 Network 의 VLAN Interface 를 Static Join 으로 설정하면 Member 의 존재유무를 검사하지 않고 지정된 Multicast Traffic 이 계속 Forwarding 된다.

라우터에 Static Join 을 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim static-join *multicast-address IFNAME*	라우터에 Static Join 정보를 설정한다.
no ip pim static-join *multicast-address IFNAME*	설정된 Static Join 정보를 해제한다.

명령어	설명
ip pim static-join *multicast-address IFNAME* to *<count>*	라우터에 Static Join 정보를 지정된 count 만큼 설정한다.
no ip pim static-join *multicast-address IFNAME* to *<count>*	설정된 Static Join 정보를 지정된 count 만큼 해제한다.

```
Router(config)# ip pim static-join 224.1.1.1 vlan20
Router# show ip mroute
IP Multicast Routing Table
Timers: Uptime/Expires
Flags : C - Directly Connected Host, L - Local(Router is member)
        P - Pruned All,              F - Register
        J - Join SPT,                R - RP Bit
        X - Proxy Join Timer flag
Interface state: Interface, Next-Hop, State/Mode
_____________________________________________________________
(*, 224.1.1.1), 00:00:02/00:03:01, RP 192.168.1.254, flags: SRX
 Incoming interface: vlan10,  RPF nbr 10.1.1.2
 Outgoing interface list:
   vlan20, Forward/Sparse,  00:00:15/18:12:15  STATIC-JOIN

(20.1.1.254, 224.1.1.1) 00:00:02/00:03:01, RP 192.168.1.254, flags: S
 Incoming interface: vlan10,  RPF nbr 10.1.1.2
 Outgoing interface list:
   vlan20, Forward/Sparse,  00:00:15/18:12:15

 total   (*, G) : 1, (S, G) : 1
```

9.4.6.15. Static Multicast Route Path

PIM-SM 은 Unicast Routing Protocol 을 기반으로 동작한다. 하지만 Network 의 환경이나 라우터의 운용에 따라서 특정한 Multicast Group 이나 Multicast Server 에 대해 Route Path 를 Unicast Routing Protocol 이외의 경로로 지정하여 운용할 경우, 다음과 같이 Multicast Route Path 를 global configuration mode 에서 다음의 명령을 실행한다.

설정된 Multicast Route Path 는 PIM-SM 에서만 유효한 경로이며, Unicast Routing Path 보다 우선한다.

명령어	설명
ip mroute path *<address/prefixlen > <neighbor-address>*	라우터에 multicast route RPT/SPT path 정보를 설정한다.
no ip mroute path *<address/prefixlen > <neighbor-address>*	설정된 multicast route RPT/SPT path 정보를 해제한다.

```
Router(config)# ip mroute path 10.1.1.254/32 20.1.1.1
Router # show ip mroute path
Codes: S - Multicast Route Path, G - Multicast Group Route Path

S> 10.1.1.254/32 via 20.1.1.1, vlan20
```

9.4.6.16. Multicast Route Entry 제한

Multicast 서비스를 제공하는 모든 System 은 System 내의 Resource 가 한정적이다. 따라서 Multicast Route Entry 의 개수를 제한하여야만 안정적인 Multicast 서비스를 지속적으로 제공할 수 있다.

Multicast Route Entry 개수를 제한하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip mroute max-entry *<1-250>*	Maximum mroute entry 개수를 지정한다. (default: 250 개)
no ip mroute max-entry	설정된 multicast route entry 개수를 해제한다.

```
Router(config)# ip mroute max-entry 150
Router(config)# exit
Router# show ip mroute
IP Multicast Routing Table
Timers: Uptime/Expires
Flags : C - Directly Connected Host, L - Local(Router is member)
        P - Pruned All,              F - Register
        J - Join SPT,                R - RP Bit
        X - Proxy Join Timer flag
Interface state: Interface, Next-Hop, State/Mode

_____________________________________________________________________
 total    (*, G) : 0, (S, G) : 0, max : 150
```

9.4.6.17. Switchover Recovery Delay

PIM-SM 은 지정된 mcache-check-interval 마다 주기적으로 Source 또는 RP 에 대한 RPF 를 검사한다. 지정된 RPF 보다 Short-Path-Tree 가 존재하는 경우, PIM-SM 은 Short-Path-Tree 로 즉시 Switchover 한다.

시스템의 Upgrade 를 위한 리부팅 등의 이유로 인하여 Network 장비간 절체 및 복구시 Network 환경으로 인하여 Multicast Traffic 이 중단되는 현상이 발생할 수 있다.

이러한 현상은 절체후 복구시 Network 에 설정된 Unicast Routing 이 Static Routing 일 때 발생할 수 있으며, 이러한 현상을 방지하기 위해서는 Switchover 를 Delay 해야 한다.

Switchover Recovery Delay 를 “0”으로 설정하는 경우, 절체 및 복구후 SPT Switchover 동작을 하지 않는다.

Switchover Recovery Delay 를 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim switchover-recovery-delay <0-300>	절체 후, 복구에 대한 switchover 를 delay 한다.
no ip pim switchover-recovery-delay	설정된 switchover recovery delay 정보를 해제한다.

```
Router(config)# ip pim switchover-recovery-delay 120
Router(config)#
```

9.4.6.18. fast SPT switchover

RPT join 후 Multicast traffic 을 수신하자마자 SPT 로 절체해야 할 경우 global configuration mode 에서 다음 명령을 실행한다.

명령어	설명
ip pim fast-spt-switchover	Multicast traffic 을 수신하자마자 SPT 로 절체하도록 한다.
no ip pim fast-spt-switchover	설정된 fast-spt-switchover 정보를 해제한다.

```
Router(config)# ip pim fast-spt-switchover
Router(config)#
```

9.4.6.19. RPF Load-balance

RPT 혹은 SPT 에 대해 Metric 이 동일한 RPF Interface 가 하나이상 존재할 경우, PIM-SM 은 각 Group 별로 분산하여 Upstream Neighbor 으로부터 해당 Multicast Traffic 을 수신할 수 있다.
이러한 RPF Interface 를 Load-balance 로 지정할 경우, Multicast Traffic 을 여러 Interface 로 분리하여 수신하게 됨으로써 Bandwidth 의 효율을 높일 수 있다.
설정을 위해서는 다음과 같이 Multicast Route Path 를 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim rpf load-balance	라우터에 RPF Load-balance 를 설정한다.
no ip pim rpf load-balance	설정된 RPF Load-balance 정보를 해제한다.

```
Router(config)# ip pim rpf load-balance
Router(config)#
```

9.4.7. Display System and Network Statistics

표 9-2 IP 멀티캐스트 라우팅 관련 모니터링 명령어

명령어	설명
show ip igmp groups	호스트들이 가입한 멀티캐스트 그룹들을 보여준다.
show ip igmp interface	인터페이스들의 멀티캐스트와 관련된 정보들을 보여준다.
show ip mroute	멀티캐스트 라우팅 테이블의 내용을 보여준다.
show ip mroute path	지정된 멀티케스트 라우팅 경로의 내용을 보여준다.
show ip pim interface	PIM 이 설정된 인터페이스에 대한 정보를 보여준다.
show ip pim neighbor	PIM neighbor 들을 보여준다.
show ip pim bsr-router	BSR 라우터에 대한 정보를 보여준다.
show ip pim rp	RP 에 대한 정보를 보여준다.
show ip pim rp-hash	RP-HASH 에 대한 정보를 보여준다.

표 3 IP 멀티캐스트 라우팅 관련 설정 예제

```
vlan 10
!
ip multicast-routing pim-sm
ip multicast-routing igmp-querier
!
interface gi1 ← 가입자 port
 igmp-trap
!
interface gi24
 switchport access vlan 10
!
interface vlan1 ← Outgoing interface
 l2-classifier
 ip address 1.1.1.254/24
 service-policy mcast_traffic_filter ← 가입자 Multicast Traffic 차단
 ip igmp
 ip pim
 ip igmp leave-timeout 300
!
interface vlan10 ← Incoming interface
 l2-classifier
 ip address 10.1.1.254/24
 service-policy mcast_high_queuing ← High Queuing
 ip pim
 ip igmp leave-timeout 300
!
interface eth0
 ip address 192.168.0.102/24
!
flow-rule mcast_high classify ip any 224.0.0.0/4
flow-rule mcast_high match queuing-parameter 7
flow-rule mcast_filter classify ip any 224.0.0.0/4
flow-rule mcast_filter match drop
!
policy-map mcast_high_queuing flow-rule mcast_high
policy-map mcast_traffic_filter flow-rule mcast_filter
!
ip pim bsr-candidate vlan10
ip pim rp-candidate vlan10
!
ip igmp query-based-port
```

10

라우팅 프로토콜 (RIP & OSPF & BGP)

본 장에서는 Premier 8624XG 시리즈 스위치에서 사용 가능한 IP 유니캐스트 라우팅 프로토콜들에 대해서 기술한다. 본 장의 설명들은 사용자가 이미 IP 유니캐스트 라우팅에 대한 익숙함을 가정하고 있다. 만약 IP 유니캐스트 라우팅에 익숙하지 않다면, 다음과 같은 문서들을 참고하기 바란다.

- ✓ RFC 1058 — Routing Information Protocol (RIP)
- ✓ RFC 1256 — ICMP Router Discovery Messages
- ✓ RFC 1723 — RIP Version 2
- ✓ RFC 2178 — OSPF Version 2
- ✓ RFC 1771 — BGP Version 4

10.1. 라우팅 프로토콜 개요

Premier 8624XG 시리즈 스위치는 IP 유니캐스트 라우팅 프로토콜로서 Routing Information Protocol (RIP), Open Shortest Path First (OSPF)를 지원한다. 또한 inter domain 라우팅을 위해 BGP4(RFC 1771)를 지원한다.

RIP 은 Bellman-Ford (또는 distance-vector) 알고리즘을 기반으로 한 distance-vector 프로토콜중의 하나이다. Distance-vector 알고리즘은 수년 동안 사용되어져 왔으며 또한 광범위하게 구축 되었다.

OSPF 는 Dijkstra link-state 알고리즘을 기반으로 한 link-state 프로토콜의 하나이다. OSPF 는 RIP 보

다 늦게 발표된 새로운 Interior Gateway Protocol (IGP) 프로토콜이며, 오늘날의 복잡한 네트워크에서 RIP 를 사용함으로써 발생하는 여러 문제들을 해결하였다.

BGP 는 서로 다른 관리 도메인(Autonomous System:AS) 간에 라우팅 정보를 주고 받을 수 있도록 해주는 프로토콜로서 RIP 와 OSPF 와는 달리 한 도메인 내에서의 라우팅이 아닌 도메인 간의 라우팅을 담당한다. Premier 8624XG 시리즈 스위치에서는 BGP-4 를 지원하고 있다.

10.1.1. RIP 대 OSPF

RIP 와 OSPF 와의 차이점은 distance-vector 프로토콜과 link-state 프로토콜과의 차이점에 있다. Distance-vector 프로토콜을 사용하는 경우에, 각 라우터는 인접 라우터로부터 얻은 정보를 바탕으로 유일한 라우팅 테이블을 생성한다. Link-state 프로토콜을 사용하는 경우에는, 모든 라우터는 AS(Autonomous System) 내의 모든 라우터들로부터 얻은 정보를 바탕으로 생성된 동일한 하나의 라우팅 테이블을 유지한다. 각 라우터는 자신을 루트로 하는 최단 경로 트리(shortest path tree)를 생성한다.

RIP 프로토콜의 가장 큰 장점은 상대적으로 간단하여 이해하기가 쉽고, 구현이 용이하다는 것이다. 이러한 장점들로 인하여 오랜 기간 동안 사실상의 표준으로 많은 네트워크에 적용되어 왔다.

RIP 은 다음과 같은 문제점으로 인하여 규모가 큰 네트워크에 적용되는데 있어서 제한을 가진다.

- ✓ Source network 과 destination network 간의 hop 수가 15 로 제한된다.
- ✓ 전체 라우팅 테이블의 주기적인 브로드캐스팅에 의해 적지 않은 대역폭이 소요된다.
- ✓ 느린 수렴
- ✓ Hop count 에 의하여 라우팅 경로가 결정되며 link cost 및 delay 에 대한 개념이 없다.
- ✓ 계층적인 개념이 없다.

OSPF 는 RIP 에 대해 다음과 같은 장점을 가지고 있다.

- ✓ Hop count 에 제한이 없다.
- ✓ Route update 는 변화가 있을 때에만 멀티캐스트를 수행한다.
- ✓ 빠른 수렴
- ✓ 실제 link 의 cost 를 근거라 한 여러 라우터들 사이의 Load balancing 을 지원한다.
- ✓ 네트워크를 area 들로 나누어 계층적인 토폴로지를 지원한다.

각각의 프로토콜에 대한 세부 사항은 다음 절에서 다루기로 한다.

10.2. RIP 개요

RIP 는 1969 년부터 Advanced Research Projects Agency Network (ARPAnet)에서 처음으로 사용된 Interior Gateway Protocol (IGP)이다. 주로 중간 규모의 homogeneous 한 네트워크간의 사용을 위해 고안되었다.

먼 거리의 네트워크까지의 최적의 경로를 결정하기 위해, RIP 을 사용하는 라우터는 항상 목적지까지 최소의 hop 수를 가지고 있는 경로를 선택한다. 데이터가 전송되는 경로의 각각의 라우터를 하나의 hop 으로 간주한다.

10.1.2. 라우팅 테이블

RIP 를 사용하는 라우터의 라우팅 테이블은 알려진 모든 목적지 네트워크에 대한 엔트리를 가지고 있다. 각 라우팅 테이블의 엔트리는 다음과 같은 정보들을 포함한다.

- ✓ 목적지 네트워크의 IP 주소
- ✓ 목적지 네트워크에 대한 metric (hop count)
- ✓ 다음 라우터의 IP 주소
- ✓ 엔트리가 마지막으로 갱신된 이후의 시간을 기록하는 타이머

라우터는 매 30 초(*default value*)마다 주기적으로, 또는 전체 네트워크 토폴로지에 변경이 발생한 경우(*triggered updates*), 직접 연결되어 있는 인접 라우터들과 update 메시지를 교환한다. 인접한 라우터로부터 라우팅 경로 타임아웃 기간(기본 설정은 180 초)동안 update 메시지를 수신하지 못하면 인접 라우터와의 연결이 더 이상 유효하지 않은 것으로 가정한다.

10.1.3. Route Advertisement of VLANs

VLAN 이 IP 주소를 가지도록 설정되어 있지만 IP 를 라우팅 하도록 설정되어 있지 않거나, RIP 을 라우팅 프로토콜로 사용하지 않도록 설정되어 있으면 RIP 으로 서브넷을 선전할 수 없다. IP 주소를 할당

받았으면서, RIP 을 사용하여 IP 라우팅을 수행하도록 설정되어 있는 VLAN 은 자신의 서브넷을 선전한다.

10.1.4. RIP Version 1 vs. RIP Version 2

RIPv2 는 RIPv1 의 취약점을 개선하여 다음과 같은 기능이 확장되었다.

- ✓ Variable-Length Subnet Mask (VLSMs)
- ✓ Next-hop address
  - ☞ Next-hop address 의 지원은 특정 환경에 대하여 경로의 최적화를 가능하게 한다.
- ✓ 멀티캐스팅
  - ☞ RIP v2 는 라우팅 프로토콜을 지원하지 않는 호스트의 로드를 줄이기 위하여 멀티캐스팅을 지원한다.

10.3. OSPF 개요

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

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

10.3.1. Link-state Database

초기화 시, 각 라우터는 자신의 인터페이스 각각에 대한 link state advertisement (LSA)를 전송한다. LSA 는 각 라우터에 의해서 수집되며 각 라우터의 LSDB 에 들어가게 된다. OSPF 는 라우터간에 LSA 를 분배하기 위해서 flooding 알고리즘을 사용한다. 라우팅 정보의 변화는 네트워크의 모든 라우터들에게 전송 되어 진다. 하나의 area 내의 모든 라우터들은 정확히 동일한 LSDB 를 가진다. 다음 <표 10-1>는 LSA type number 를 보여준다.

표 10-1. LSA Type number

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

10.3.2. Areas

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

OSPF 에서는 다음과 같은 세가지 타입의 라우터를 정의한다.

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

10.1.4.1. AREA 0

하나 이상의 area 를 포함하고 있는 OSPF 기반 네트워크는 백본이라 불리는 area 0 로 설정된 area 를 반드시 가지고 있어야 한다. Autonomous system 의 모든 area 들은 반드시 백본에 연결이 되어야 한다.

네트워크를 설계할 때, area 0 로 시작하여 다른 area 들을 확장 시켜 나가야 한다.

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

10.1.4.2. Stub areas

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

10.1.4.3. Virtual links

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

10.3.3. Route Redistribution

RIP 와 OSPF 는 스위치에서 동시에 사용될 수 있다. Route Redistribution 은 두 라우팅 프로토콜사이에 서로 static route 를 포함한 라우팅 경로를 교환할 수 있도록 한다.

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

10.4. Border Gateway Protocol (BGP)

앞에서도 잠깐 언급 했듯이, BGP 는 외부 네트워크와 연결을 해주는 Exterior Gateway Protocol(EGP) 이다. 즉, 서로 다른 도메인(Autonomous System, AS)간에 라우팅 정보를 주고 받을 수 있도록 네트워크 내부의 정보를 관리한다.

BGP 의 첫 번째 버전은 RFC-1105 로 1989 년 6 월에 발표 되었다. 두 번째 버전은 RFC-1163 으로 1990 년 6 월에 발표 되었으면, 세 번째 버전은 RFC-1267 로 1991 년에, 네 번째 버전은 RFC-1654 로 1994 년 7 월에 발표되어 RFC-1771 로 1995 년 3 월에 개정되었다. 이 버전들은 차례로 BGP-1, BGP-2, BGP-3, BGP-4 로 불리고 있으며, 현재 인터넷에서는 BGP-4 가 사용되고 있으며, P8624XG 시리즈 스위치에서도 BGP-4 를 지원하고 있다.

이러한 BGP-4 설계의 핵심은 네트웍 주소 공간의 급속한 사용을 완화 시키고자 도입된 CIDR (Classless Inter-Domain Routing)을 지원하고, 라우팅 테이블의 폭발적인 증가에 대응하고자 함에 있다.

10.4.1. BGP 동작

BGP 프로토콜은 TCP 위에서 동작된다. 따라서 이런 특성에 따른 장점과 단점을 갖게 된다.

모든 에러 제어 기능들을 TCP 에 의존함으로써 프로토콜이 훨씬 단순해지게 된다. 그리고 TCP 상에서 동작함으로써 라우터들 간에 교환되는 데이터들이 신뢰성 있게 전달되며, 일정 주기로 전체 테이블을 재전송 하는 대신에 “incremental updates”를 사용한다.

BGP 프로토콜 메시지는 19 바이트의 고정 길이 헤더를 갖고 있으며 마지막 한 바이트가 메시지의 타입을 가리키게 되는데, 이러한 메시지 타입으로는

1. OPEN
2. UPDATE
3. NOTIFICATION
4. KEEPALIVE

이 있다.

(1) 초기 동작

BGP 를 지원하는 라우터들은 포트 179 에서 BGP 연결을 기다린다. 연결 설정을 원하는 라우터는 상대방 라우터의 포트 179 로 먼저 TCP 연결을 설정한다. 일단 연결이 설정되면, 각 라우터는 연결의 파라미터들을 현상하기 위해 OPEN 메시지를 주고 받는다. 이 OPEN 메시지의 파라미터들에는 , 버전 넘버, 전송 라우터의 AS 번호, hold-time, identifier, 기타 옵션들이 있다. Identifier 필드는 해당 BGP 라우터의 IP 인터페이스 주소들 중의 하나를 전달하는데, 각 라우터는 하나의 identifier 를 반드시 선택해

야 하고, 모든 BGP 연결에서 BGP 패킷을 전달하는데 사용되는 인터페이스에 상관없이 그 값을 사용한다.

(2) Update

일단 연결이 설정되면, BGP 라우터들은 “update” 메시지들을 주고 받는다. 이 메시지에는 여러 개의 path attribute 들과 도달 가능한 네트워크 정보들로 이루어져 있다. 이 메시지를 수신하면, 알려지는 네트워크에 도달하는데 사용되고 있는 현재 경로와 비교하다. 만일 새 경로가 이전 경로 보다 더 짧다면 라우팅 테이블은 갱신되고 대응하는 업데이트가 네이버들로 보내진다.

(3) Keep-Alive 특성

OSPF 에서처럼 BGP 라우터들은 각 네이버들의 연결여부를 지속적으로 모니터할 필요가 있다. 이를 위해 BGP 는 주기적으로 KEEPALIVE 메시지를 전송한다. 이 메시지는 단순히 19 바이트의 BGP 헤더로만 구성 되어져 있다. 이러한 주기적인 전송 값인 hold-time 은 앞에서 설명한 연결 설정시의 OPEN 메시지 교환 중에 결정된다. 디폴트로 90 초가 설정 되어있다.

(4) Error Notification

만일 BGP 라우터가 잘못 구성되거나 에러가 있는 메시지를 수신하게 되는 경우, 혹은 hold time 이 지나도록 어떤 메시지도 받지 못하는 경우, 상대방에게 notification 메시지를 보냄으로써 에러를 알려주게 된다. 그리하여, 설정된 TCP 연결이 자연스럽게 해제된다.

10.5. RIP 설정

10.5.1. 명령어

P8624XG 시리즈 스위치에서는 RIPv 1/2 가 지원되고 있는데, RIP 프로토콜을 사용하기 위해서는 RIP 를 활성화 시켜야 한다.

RIP 를 활성화 하는 절차는 다음과 같다.

1) Configuration 모드에서 router rip 를 입력한다. 이렇게 하여 rip 모드로 진입한다.

```
router rip
```

2) Rip 모드에서 RIP로 운영할 네트워크를 지정한다.

network ip-address

이 명령어를 이용하여 RIP 가 동작하는 특정 네트워크를 설정할 수 있는데, 예를 들어 192.168. 0.0/24 네트워크에 RIP 가 설정되어 있다면 192.168.0.0 에서 192.168.0.255 사이의 모든 주소가 RIP 로 동작하게 된다. 이렇게 설정된 인터페이스를 통하여 RIP 패킷이 송수신된다.

다음의 명령어들은 RIP 를 구성하기 위해 사용되는 것들이다. 이렇게 하여 RIP 를 활성화 시킨 후에는 사용자의 필요에 따라 다음과 같은 항목들을 설정하여 RIP 프로토콜을 운용할 수 있다.

default-information originate

- RIP 가 하나의 default route 를 알리는 것을 제어한다.

default-metric <*1-16*>

- 하나의 라우터가 하나 이상의 IP 라우팅 프로토콜을 돌리는 경우가 있다. 각각의 라우팅 프로토콜은 각각 서로 다른 metric 을 가지고 있다. 예를 들면 RIP 은 hop count, OSPF 는 dimensionless cost 를 가지고 있다. 하나의 라우팅 프로토콜이 다른 라우팅 프로토콜을 이용하여 경로를 결정하려면 라우트 metric 을 다른 라우팅 프로토콜로 변환 시켜야 한다.
- metric 의 변환을 위해 사용되는 명령이 default-metric 이다. Redistribute routes 의 값을 <1-16> 내에서 선택 정의한다.

distance <*1-255*> [*A.B.C.D/M*] [*WORD*]}

- Administrative distance 의 값을 조정하는데 사용한다. 이 값의 범위는 1~255 이다. RIP 의 기본값은 120 이고, 하나의 라우터 시스템에서 하나 이상의 라우팅 프로토콜이 돌고 있으면 이 administrative distance 값을 사용한다.
- 만약에 라우터에서 RIP 와 OSPF 라우팅 프로토콜이 동작하고 있으면 각각 경로를 결정할 때 RIP 가 아닌 OSPF 로 결정된다. 그 이유는 OSPF 의 distance 값이 110 이고 RIP 는 120 이기 때문에 라우터는 distance 값이 적은 경로를 선택한다. 따라서 필요하다면 이 값을 조절할 필요가 있다. 즉 RIP 의 경로를 설정할 수 있도록 OSPF 보다 적은 값을 설정한다.
- A.B.C.D/M 네트워크를 설정하여 특정 네트워크의 distance 값만 변화 시킬 수도 있다. 이 때는 액세스 리스트를 설정할 수 있다.

distribute-list {*WORD1* | **prefix** *WORD2*} **{in | out}** [*WORD3*]

- Incoming 또는 Outgoing 라우팅 update 시 필터링을 하기 위해 사용한다.
- WORD1 : 액세스 리스트의 이름
- WORD2 : IP prefix-list 의 이름
- WORD3 : interface name
- In : Filter incoming routing updates
- Out : Filter outgoing routing updates

neighbor *A.B.C.D*

- 바로 인접해 있는 인접 라우터의 어드레스를 지정해준다.

network *A.B.C.D/M*

- rip routing 을 활성화 시킬 IP network 지정

no

- 앞에서 설명한 명령들을 해제하거나 디폴트 값으로 만들기 위해 각 명령어 앞에 입력

offset-list *WORD* { **in** | **out** } **<***0-16***>** [*ifname*]

- RIP 의 metric 값을 증가 시키거나 빼는 데 사용한다
- 이 명령은 standard list 를 이용하여 incoming 이나 outgoing RIP update 할 때에 metric, hop count 를 조절하는 데 사용한다
- WORD : 액세스 리스트의 이름
- In : incoming update 시 offset 을 수행
- Out : outgoing update 시 offset 을 수행
- <0-16> : offset 의 값

passive-interface *IFNAME*

- IFNAME 으로 지정된 인터페이스에 라우팅 update 를 억제 시키는데 사용된다.
- 이 명령을 라우터의 특정 인터페이스에 적용시키면 해당 인터페이스는 outgoing 되는 경로를 광고하지 않는다. 그러나 라우팅 정보의 수신은 계속한다.

redistribute ospf [{**metric <***0-16***>**} | {**route-map** *WORD*}]

- OSPF 도메인으로 RIP 라우팅 정보를 Redistribute 하는데 사용된다.
- WORD : route-map 엔트리를 가리키는 이름

route *A.B.C.D/M*

- RIP 의 static route 를 설정하는데 사용된다.

timers basic < *5-2147483647*> < *5-2147483647*> < *5-2147483647*>

- 이 프로토콜에서 사용되는 타이머 값을 조절한다.
- 처음 값은 Routing table update timer 값이고 디폴트 값은 30 이며 단위는 second
- 두 번째 값은 Routing information timeout timer 값이고, 디폴트 값은 180 이며 단위는 second
- 세 번째 값은 Garbage collection timer 값이고, 디폴트 값은 120 이며 단위는 second

version **<***1-2***>**

- RIP 프로토콜의 동작 버전을 설정한다. 기본 설정 값은 버전 2 이다.

10.5.2. RIP 구성

다음 <1>과 같은 네트워크 구성도를 통하여 RIP 프로토콜의 구성 예를 살펴본다.

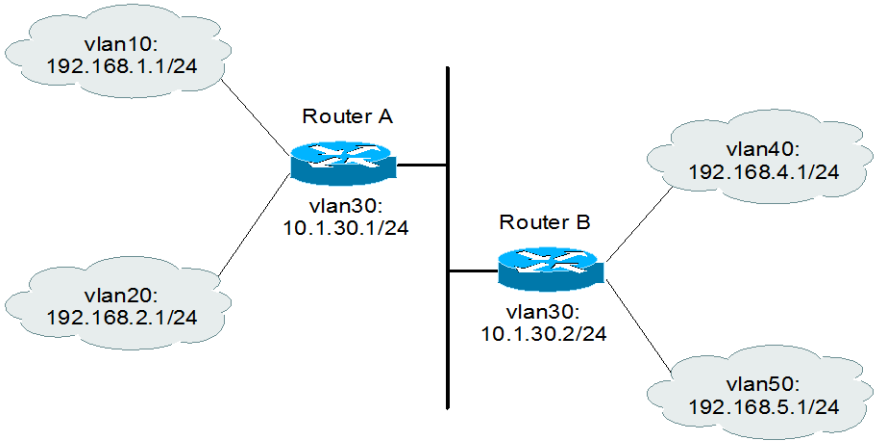


그림 10-1. RIP 을 설정한 네트워크 예제 설정 및 구성도

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

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

Router A 설정

```
Router A(config)# router rip
Router A(config-rip)# network 192.168.1.1/24
Router A(config-rip)# network 192.168.2.1/24
Router A(config-rip)# network 10.1.30.1/24
Router A(config-rip)# end
Router A# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
R>  192.168.4.0/24 [120/1] via 10.1.30.2, vlan30, 00:01:42
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan30, 00:01:42
Router A#
```

Router B 설정

```
Router B(config)# router rip
Router B(config-rip)# network 192.168.4.1/24
Router B(config-rip)# network 192.168.5.1/24
Router B(config-rip)# network 10.1.30.2/24
Router B(config-rip)# end
Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan30
R>* 192.168.1.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Router B#
```

10.5.3. Distance 설정

<그림 1>의 네트워크 구성도에서 라우터 B 의 distance 값(RIP 에서 디폴트로 120 이다)을 distance 명령을 통하여 130 으로 변경해보자.

```
Router B(config)# router rip
Router B(config-rip)# distance 130
Router B(config-rip)# end
Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan30
R>* 192.168.1.0/24 [130/1] via 10.1.30.1, vlan30, 00:02:13
R>* 192.168.2.0/24 [130/1] via 10.1.30.1, vlan30, 00:02:13
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Router B#
```

위에서 보듯이 distance 값이 120 에서 130 으로 바뀐 것을 볼 수 있다. 이제 특정 네트워크의 distance 값을 변경하고자 한다. 이 때의 방법은 다음과 같다. 네트워크의 원래 상태로 설정 값을 되돌리고 다음과 같은 설정 작업을 다시 한다.

Distance 값을 원래대로 하려면 다음과 같다.

```
Router B(config)# router rip
Router B(config-rip)# no distance 130
Router B(config-rip)# distance 130 ?
A.B.C.D/M  IP source prefix
<cr>
Router B(config-rip)# distance 130 192.168.0.0/16 ?
WORD  Access list name
<cr>
Router B(config-rip)# distance 130 192.168.0.0/16 1
Router B(config-rip)# end
```

위와 같이 설정하는 의도는 192.168.1.0 의 distance 값은 130, 192.168.2.0 의 distance 값은 120 으로 설정 하고자 하는 데 있다.

위의 설정이 끝나면 이제 실제로 distance 값을 적용하기 위한 access-list 를 설정한다.

```
Router B(config)# access-list 1 permit 192.168.1.0 255.255.255.0
Router B(config)# end
Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan30
R>* 192.168.1.0/24 [130/1] via 10.1.30.1, vlan30, 00:02:13
R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Router B(config)#
```

10.5.4. Distribute-list 설정

마찬가지로 위의 예제 네트워크에서 라우터 B 는 라우터 A 에서 광고 되는 192.168.1.0 네트워크의 경로를 삭제하고자 한다. 이 경우에 다음과 같은 순서대로 작업하면 된다. 먼저 라우터 B 의 RIP 프로세스에 distribute-list 를 적용시킨다. 그리고 access-list 를 사용해야 한다. 다음 순서대로 설정 한다.

9) Access-list 를 이용하여 라우터 B 로 들어오는 192.168.1.0 네트워크를 막아보자.

```
Router B(config)# router rip
Router B(config-rip)# distribute-list 2 in
Router B(config-rip)# end
```

10) 이제 192.168.1.0 경로를 막는 access-list 를 설정한다. 이렇게 설정하는 이유는 192.168.1.0 경로만 막고 나머지 경로는 허용한다는 의미이다.

```
Router B(config)# access-list 2 deny 192.168.1.0 255.255.255.0
Router B(config)# access-list 2 permit any
Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan30
R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan30, 00:12:15
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Router B#
```

11) 라우터 A 에서 오는 192.168.1.0 경로는 필터링 되었음을 볼 수 있다. “show ip protocol”을 통하여 필터링을 사용함을 알 수 있다.

```
Router B# show ip protocols
Routing Protocol is "rip"
```

```
  Sending updates every 30 seconds with +/-50, next due in 5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is 2
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    vlan30            2     2
    vlan40            2     2
    vlan50            2     2
  Routing for Networks:
    10.1.30.0/24
    192.168.4.0/24
    192.168.5.0/24
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update
    10.1.30.1                 0         20       120   00:00:05
  Distance: (default is 120)
    Address           Distance  List
    192.168.0.0/16         130  1
Router B#
```

12) 이제 라우터 B 가 192.168.4.0 경로가 다른 쪽으로 나가는 것을 막는 경우를 access-list 를 적용하기로 하자.

```
Router B(config)# router rip
Router B(config-rip)# distribute-list 3 out
Router B(config-rip)# exit
Router B(config)# access-list 3 deny 192.168.4.0 255.255.255.0
Router B(config)# access-list 3 permit any
```

13) 이제 라우터 A 의 라우팅 테이블을 보면 192.168.4.0 의 경로가 넘어오지 않는다는 것을 알 수 있다.

```
Router A# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan30, 00:20:04
Router A#
```

10.5.5. Offset-list 설정

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

```
Router A(config)# router rip
Router A(config-rip)# offset-list 4 in 2
Router A(config-rip)# exit
Router A(config)# access-list 4 permit any
Router A(config)# [Ctrl] + [z]
Router A# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

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

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

10.5.6. Passive-interface 설정

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

```
Router A(config)# router rip
Router A(config-rip)# passive-interface vlan30
Router A(config-rip)# end
Router A# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

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

Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

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

10.6. OSPF 설정

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

(1) Config 모드에서 ospf 모드로 진입한다.

router ospf

(2) OSPF 프로토콜을 활성화 시킬 네트워크와 이것이 속할 area를 지정한다.

network ip-address/M **area** (area-id | area-address)

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

10.6.1. 명령어

다음은 OSPF 를 설정하기 위해 사용되는 명령어들이다.

router ospf ☞ OSPF 인스턴스를 생성하기 위한 명령어이다.

```
Router# configure terminal
Router(config)# router ospf
Router(config-ospf)# ?
```

`router ospf` 명령을 수행한 후에 나타나는 명령어들의 리스트는 다음과 같다.

표 10-2. Router ospf 명령어 수행 후의 명령어

명령어	설명
area	OSPF area parameters
auto-cost	Calculate OSPF interface cost according to bandwidth
compatible	OSPF compatibility list
default-information	Control distribution of default information
default-metric	Set metric of redistributed routes
distance	Define an administrative distance

distribute-list	Filter networks in routing updates
end	End configuration mode and return to EXEC mode.
exit	Exit configuration mode or close an active terminal session
Help	Description of the help system
neighbor	Specify neighbor router
network	Enable routing on an IP network
no	Negate a command or set its defaults
ospf	OSPF specific commands
passive-interface	Suppress routing updates on an interface
redistribute	Redistribute information from another routing protocol
refresh	Adjust refresh parameters
router-id	router-id for the OSPF process
timers	Adjust routing timers

다음 절부터 <표 10-2>의 명령어들을 설명하고자 한다.

10.1.4.4. area

다음의 예가 보여주는 것처럼 area 다음에는 area id 를 0~4294967295 사이의 십진수 값이나, A.B.C.D 처럼 IP 주소 포맷으로 나타낼 수 있다.

```
Router(config-ospf)#area ?
<0-4294967295>  OSPF area ID as a decimal value
A.B.C.D         OSPF area ID in IP address format
Router(config-ospf)#
```

area id 를 임의의 값(여기서는 0)으로 주었을 때 나타나는 서브 명령어들은 <표 10-3>과 같다.

표 10-3. Area 값이 임의로 주어졌을 때 나타나는 서브 명령어

명령어	설명
authentication	Enable authentication
default-cost	OSPF area ID as a decimal value
export-list	Set the filter for networks announced to other areas
import-list	Set the filter for networks from other areas announced to the specified one
range	Configure OSPF area range for route summarization
shortcut	Configure the area's shortcutting mode
stub	Configure OSPF area as stub
virtual-link	Configure a virtual link
auto-cost	Calculate OSPF interface cost according to bandwidth
compatible	OSPF compatibility list

default-information	Control distribution of default information
default-metric	Set metric of redistributed routes
distance	Define an administrative distance
distribute-list	Filter networks in routing updates
end	End configuration mode and return to EXEC mode.
exit	Exit configuration mode or close an active terminal session
help	Description of the help system
neighbor	Specify neighbor router
network	Enable routing on an IP network
no	Negate a command or set its defaults
ospf	OSPF specific commands
passive-interface	Suppress routing updates on an interface
redistribute	Redistribute information from another routing protocol
refresh	Adjust refresh parameters
router-id	router-id for the OSPF process
timers	Adjust routing timers

<표 10-3>의 서브 명령들의 각각은 다음과 같다.

- **Authentication**
  area 안에서 인증을 위하여 사용한다. 인증 사용은 단순한 패스워드를 이용한 방법과 암호화를 통한 방법이 있다.

```
Router(config-ospf)#area 0 authentication
  message-digest  Use message-digest authentication
<cr>
Router(config-ospf)#
```

  단순한 패스워드를 이용한 방법은 <cr>값 (enter 를 의미)을 사용하는 것으로서 해당되는 인터페이스에 동시에 다음과 같은 명령을 설정해야 한다. 여기서 AUTH_KEY 부분에 사용할 암호를 넣는다.

```
Router(config-if-fa20/1)# ip ospf authentication-key AUTH_KEY
```

  서로 연결된 두 개의 라우터의 연결 인터페이스에 위의 명령의 패스워드가 일치하지 않으면 해당 인터페이스를 통하여 라우팅 정보가 넘어오지 않는다. 즉, 서로 라우팅 정보를 갖지 못한다. 암호화를 통한 방법은 위와 큰 차이가 없다. 단지 명령의 차이가 있을 뿐이다.

- **Default-cost**
  Stub area 가 알리는 외부 라우터의 metric 값이며, 기본 값은 1 로 설정되어 있다.

- **Export-list**
  다른 area 로 알려지는 경로들을 액세스 리스트를 이용하여 필터링하는 데 사용된다.

- **Import-list**
  다른 area 에서 알려오는 경로들을 액세스 리스트를 이용하여 필터링하는 데 사용된다

- **Range**
  Border router 에서만 이용되는 커맨드로서 매칭되는 주소의 대표 경로를 제공한다.

- **Shortcut**
  해당 area 위 shortcut 모드를 설정하는데 사용된다.

- **Stub**
  Stub area 를 정의하기 위해 사용한다. 다음 명령은 area 2 를 stub area 로 설정한다.
  No-summary 가 추가되면 이 area 로는 inter-area 경로가 전혀 들어오지 않는다.

```
Router(config-ospf)#area 2 stub
  no-summary  Do not inject inter-area routes into stub
<cr>
Router(config-ospf)#
```

- **virtual-link**

  이 명령은 다음과 같이 사용한다.

area <transit area id> **virtual-link** <remote router id>

  <

  그림 10-2>는 이해를 돕기 위한 그림으로 Virtual Link 네트워크를 보여준다. Area 6 은 virtual-link 를 이용하여 area 8 을 transit-area 로 사용하여 백본 area 0 에 접속된다.

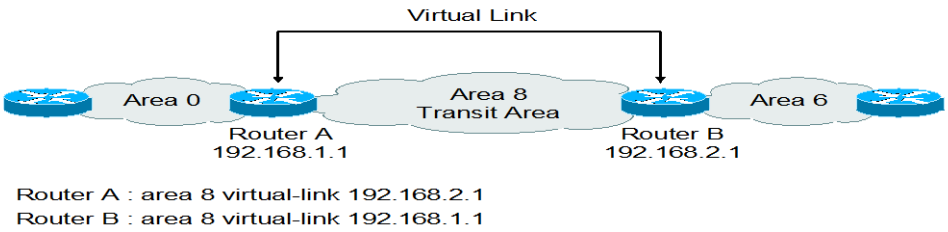


그림 10-2. Virtual Link 네트워크

- **Auto-Cost**

  대역폭에 따라 인터페이스의 OSPF cost 를 계산하기 위해 reference-bandwidth 를 <1-4294967> 범위에서 Mbps 단위로 입력한다.

- **Compatible**

  OSPF 호환되는 리스트. 현재는 RFC1583 이 있다.

- **Default-Information**

  ABR 이 하나의 ospf area 로 디폴트 라우트(0.0.0.0/0)를 생성하여 보내는데 사용되는 명령이다.

default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]

- **default-metric**

  Redistribute 되는 경로의 metric 값을 <0-16777214>에서 선택한다.

- **Distance**

distance *<1-255>* [*A.B.C.D/M*] [*WORD*]}

  Administrative distance 의 값을 조정하는데 사용한다. 이 값의 범위는 1~255 이다. OSPF 의 기본 값은 110 이고, 하나의 라우터 시스템에서 하나 이상의 라우팅 프로토콜이 돌고 있으면 이 administrative distance 값을 사용한다.

  만약에 라우터에서 RIP 와 OSPF 라우팅 프로토콜이 동작하고 있으면 각각 경로를 결정할 때 RIP

이 아닌 OSPF 로 결정된다. 그 이유는 OSPF 의 distance 값이 110 이고 RIP 은 120 이기 때문에 라우터는 distance 값이 적은 경로를 선택한다. 따라서 필요하다면 이 값을 조절할 필요가 있다. 즉 RIP 의 경로를 설정할 수 있도록 OSPF 보다 적은 값을 설정한다.

A.B.C.D/M 네트워크를 설정하여 특정 네트워크의 distance 값만 변화 시킬 수도 있다. 이 때는 액세스 리스트를 설정할 수 있다.

- **distribute-list**

distribute-list {*WORD1* | **prefix** *WORD2*} **{in | out}** [*WORD3*]

Incoming 또는 Outgoing 라우팅 update 시 필터링을 하기 위해 사용한다.
WORD1 : 액세스 리스트의 이름
WORD2 : IP prefix-list 의 이름
WORD3 : interface name
In : Filter incoming routing updates
Out : Filter outgoing routing updates

- **neighbor**

neighbor *A.B.C.D*

바로 인접해 있는 인접 라우터의 어드레스를 지정해준다 단지 이웃 라우터가 살아 있는지 폴링하는 주기를 <0-65535> 초 범위에서 설정할 수 있고, priority 값을 <0-255> 범위에서 설정할 수 있다.

- **network**

network *A.B.C.D/M* **area** *<area id>*

OSPF 를 구동 시키는 네트워크를 지정한다. RIP 과는 달리 이 네트워크가 속하는 area 를 지정해 주어야 한다.

- **Ospf**

OSPF 에 특정한 명령으로 ABR type 설정, RFC1583 compatibility flag 설정, 그리고 router ID 설정 등에 사용된다.

- **passive-interface**

passive-interface *IFNAME*

IFNAME 으로 지정된 인터페이스에 라우팅 update 를 억제 시키는데 사용된다.
이 명령을 라우터의 특정 인터페이스에 적용시키면 해당 인터페이스는 outgoing 되는 경로를 광고하지 않는다. 그러나 라우팅 정보의 수신은 계속한다.

- **redistribute**

redistribute (kernel|connected|static|rip|bgp) [**metric** <0-16777214>] [metric-type (1|2)] [route-map WORD]

다른 라우팅 프로토콜 혹은 정적 정보를 OSPF 의 라우팅 도메인으로 넘겨주기 위해 사용한다. 이렇게 분배된 정보들은 OSPF external route 가 된다.

- **Refresh**

<10-1800> 초 범위 내에서 LSA 의 refresh 주기를 설정한다.

- **router-id**

해당 OSPF 의 router ID 를 설정하는 명령이다.

10.6.2. OSPF 로 예제 네트워크 구성

이제부터 OSPF 라우팅 프로토콜을 이용한 네트워크를 구성 해본다. 다음 <그림 10-3>는 OSPF 로 구성한 예제 네트워크 구성도이다. 이것을 이용하여 OSPF 네트워크로 구성하면 다음과 같다.

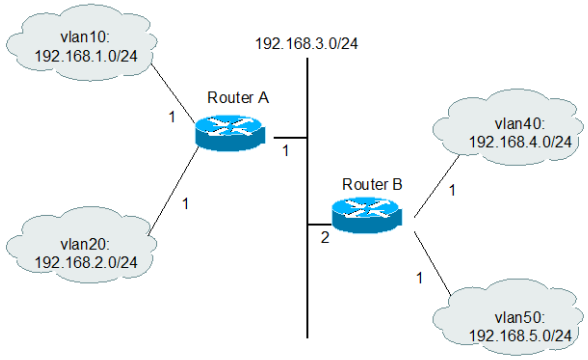


그림 10-3. OSPF 로 구성한 네트워크 샘플 예

위의 그림은 Area 0 의 백본 네트워크(192.168.0.0/24)이다. 위 그림의 네트워크를 OSPF 라우팅 프로토콜로 설정하고자 한다.

14) 먼저 라우터에 OSPF 인스턴스를 생성하여 동작 시킨다.

```
Router A# config terminal
Router A(config)# router ospf
Router A(config-ospf)#
```

15) 이제 OSPF 라우팅 프로세스를 동작 시켰으므로 라우터 주변의 네트워크를 다른 네트워크에 통보해야 한다. 즉, 라우터 A 는 192.168.1.0, 192.168.2.0, 192.168.3.0 을 통보한다. 이를 위해 먼저 네트워크 번호, 네트워크 마스크, 이 네트워크가 속한 area 를 설정한다.

```
Router A(config-ospf)# network 192.168.1.0/24 area 0
Router A(config-ospf)# network 192.168.2.0/24 area 0
Router A(config-ospf)# network 192.168.3.0/24 area 0
```

16) 이제 라우터 B 도 동일한 방식으로 설정한다.

```
Router B# config terminal
Router B(config)# router ospf
Router B(config-ospf)#

Router B(config-ospf)# network 192.168.3.0/24 area 0
```

```
Router B(config-ospf)# network 192.168.4.0/24 area 0
Router B(config-ospf)# network 192.168.5.0/24 area 0
```

17) 이제 두 대의 라우터 모두 OSPF 라우팅 프로세스를 동작 시키고 있다. 이들의 라우팅 테이블을 보면 다음과 같다.

```
Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

C>* 192.168.0.0/24 is directly connected, vlan60
O>* 192.168.1.0/24 [110/20] via 192.168.3.2, vlan30, 00:01:31
O>* 192.168.2.0/24 [110/20] via 192.168.3.2, vlan30, 00:01:31
C>* 192.168.3.0/24 is directly connected, vlan30
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Router B#

Router A# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

C>* 192.168.0.0/24 is directly connected, vlan60
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
C>* 192.168.3.0/24 is directly connected, vlan30
O>* 192.168.4.0/24 [110/20] via 192.168.3.1, vlan30, 00:01:04
O>* 192.168.5.0/24 [110/20] via 192.168.3.1, vlan30, 00:01:04
Router A#
```

위에 표시된 라우팅 정보를 살펴보면, 라우터 A 와 B 에는 각각 3 개의 직접 연결된 경로와 OSPF 로부터 배운 2 개의 경로가 있다. 이들 라우팅 테이블 각각의 정보를 분석하면 다음과 같다.

- ✓ [110/20]은 administrative distance 가 110 이고, cost 20 으로 구성 된다는 의미이다. 그리고 directly connected 는 해당 라우터의 인터페이스에 이 네트워크가 직접 연결 되었음을 의미한다.
- ✓ via 192.168.3.1 은 OSPF 를 넘겨주는 중간 네트워크이다.
- ✓ 00:01:04 는 해당 경로가 생성된 후 지난 시간을 의미한다. OSPF 는 RIP 처럼 주기적으로 라우팅 테이블을 update 시키지 않는다.
- ✓ vlan30 은 목적지 네트워크로 보낼 패킷이 지나가는 인터페이스를 가리킨다.

P8624XG 스위치에서는 기본적으로 OSPF 네트워크 cost 값이 1,000,000,000 (1Gbps)를 해당 링크의 대역폭으로 나눈 값이다. 예로 기가링크의 경우는 cost 가 1 이 되며, 100Mbps 링크는 코스트가 10 으로 설정된다. 현재 각 라우터의 인터페이스에는 이 대역폭에 대한 정보가 있다. 이들 정보는 "`show interface`" 명령을 이용하면 된다.

```
Router A# show interface vlan30
fa2/1 is up
 type 100Base-TX
 speed auto, current 100M
 duplex auto, current full
 ifindex 4(k11)  UP RUNNING BROADCAST MULTICAST

 Last clearing of counters 00:52:14
 1 minutes input rate 0 bytes/sec, 0 packets/sec
 1 minutes output rate 0 bytes/sec, 0 packets/sec
   0 packets input, 0 bytes
   Received 0 broadcasts, 0 multicasts
   0 CRC, 0 oversize, 0 dropped
   49 packets output, 3496 bytes
  Sent 0 broadcasts, 49 multicasts
Router A#
```

동작하고 있는 OSPF 를 모두 disable 시키기 위해서는 `no router` 명령을 수행하면 된다.

```
Router B(config)# no router ospf
```

앞에서 제시한 예제 네트워크 그림처럼 오직 하나의 area 가 있을 경우에 area 0 를 꼭 사용해야 할 필요는 없다. 다른 area 번호를 사용해도 무관하다. 그러나 area 가 1 개 이상일 경우에는 반드시 area 0 가 존재해야 한다.

10.6.3. Route re-distribution

RIP 와 OSPF 는 하나의 시스템에서 동시에 기동 시킬 수 있다. Route re-distribution 은 해당 시스템이 두 개의 라우팅 프로토콜들 간에 정적 경로(static route)를 포함하여, 라우팅 정보를 교환할 수 있게 해 준다.

OSPF 에서 RIP 로, 그리고 RIP 에서 OSPF 로 경로들을 보내기(export) 위해서는, 구성 함수들을 신중하게 사용 하여야 한다. RIP 와 OSPF 를 동시에 수행 하기 위해, 우선은 양쪽 프로토콜을 구성하고, 각각의 독립적인 동작을 확인하여야 한다. 그 후에 OSPF 에서 RIP 로, 그리고 RIP 에서 OSPF 로 경로들을 보내도록 구성 할 수 있다.

10.6.4. Passive-interface 설정

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

```
Router A(config)# router ospf
Router A(config-ospf)# passive-interface vlan30
Router A(config-ospf)# end
Router A# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

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

Router B# show ip route database
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

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

10.7. BGP 설정

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

- ✓ BGP 프로토콜의 활성화
- ✓ BGP neighbor 라우터 설정

10.7.1. BGP 프로토콜의 활성화

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

1) BGP 라우터 설정 모드로의 진입

```
router bgp <1-65535>
```

끝의 숫자는 AS 넘버를 가리킨다. AS 번호는 Autonomous System 번호로 BGP 네트워크를 구분하기 위해 사용되며, 망 운영자에 의해 할당된다.

2) BGP 네트워크를 지정하고 BGP 라우팅 테이블에 등록한다.

```
network A.B.C.D/M
```

BGP 를 통해 알려 줄 네트워크를 지정한다.

10.7.2. Neighbor 설정

BGP 라우팅 정보를 교환하기 위해 TCP 연결을 설정한 두 개의 라우터는 peer 혹은 neighbor(이하 네이버)라 불린다. 그래서 반드시 네이버 설정이 되어 있어야 한다. 이러한 네이버에는 동일한 AS 에 속한 네이버(iBGP Peer)와 다른 AS 에 속한 네이버(eBGP Peer)로 구분된다. 동일 AS 에 속한 네이버들은 직접 연결 되어 있을 필요는 없고 내부 라우팅 프로토콜(IGP, 예로 RIP 혹은 OSPF 등)로 경로 설정이 되어 있으면 된다. 그러나 다른 AS 에 속한 네이버와는 물리적으로 연결이 설정 되어 동일한 서브넷에 속해 있어야 한다.

이러한 bgp neighbor 를 설정하기 위해서는 다음의 명령을 사용한다.

```
neighbor ip-address remote-as number
```

이렇게 bgp 를 활성화 시키고 네이버 설정이 이루어 지면 기본적인 BGP 프로토콜이 동작하게 된다. 여기에 망 운용자는 다음에 설명하는 항목들을 선택적으로 설정할 수 있다.

1) 필터링 기능
2) BGP Attribute 설정
3) Routing policy 변경
4) 기타 기능

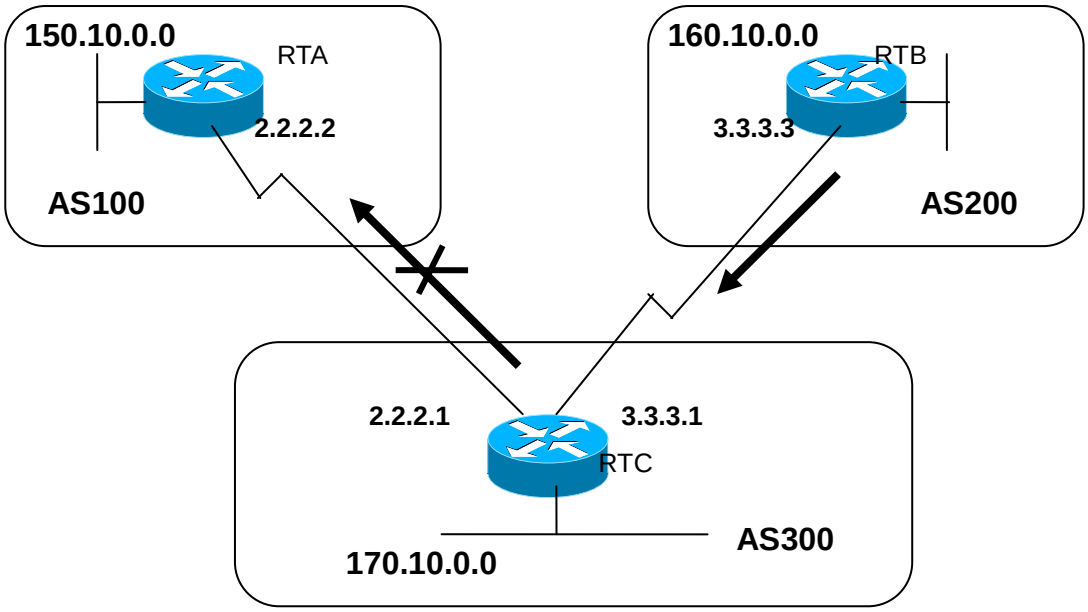
10.7.3. BGP 필터링 기능

BGP update 를 송수신 하는 것은 여러 개의 필터링 방식에 의해 조절할 수 있다. 이러한 필터링 방식에는 route filtering, path filtering, community filtering 이 있다. 이 모든 방법은 동일한 효과를 얻는다. 다만 특정한 네트워크 구성에 따라 적절한 방법을 선택하면 된다.

10.1.4.5. Route Filtering

라우터가 습득하거나 선전하는 라우팅 정보를 제한하기 위해, 특정 네이버로 가거나 오는 라우팅 업데이트에 기반하여 BGP 를 필터링할 수 있다. 이를 위해. Access-list 가 정의되어 특정 네이버로의 입출력 업데이트에 적용된다. 이를 위해 다음의 명령을 사용한다.

neighbor {*ip-address*|*peer-group-name*} **distribute-list** *access-list-number* **{in|out}**



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

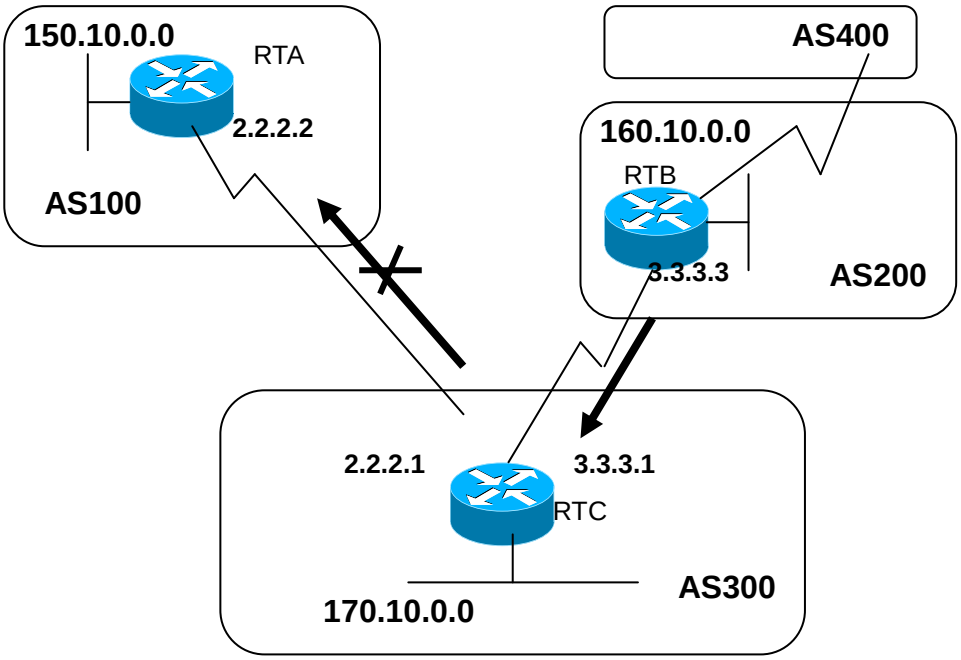
```
RTC#
router bgp 300
network 170.10.0.0
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 distribute-list 1 out

access-list 1 deny 160.10.0.0 0.0.255.255
access-list 1 permit 0.0.0.0 255.255.255.255
!-- filter out all routing updates about 160.10.x.x
```

Path Filtering

또 한가지의 필터링 방식으로, BGP AS path information 에 기반하여 입력과 출력쪽 모두에 access-list 를 설정할 수 있다. 다음 그림의 네트워크 구성도에서, AS 200 에서 생성된 업데이트가 AS 100 으로 가는 것을 막기 위해, RTC 에 access-list 를 정의함으로써, 160.10.0.0 에 대한 정보가 AS100 으로 가는

것을 막을 수 있다. 이를 위해 다음의 명령을 사용한다.

```
ip as-path access-list access-list-number {permit|deny} as-regular-expression
neighbor {ip-address|peer-group-name} filter-list access-list-number {in|out}
```

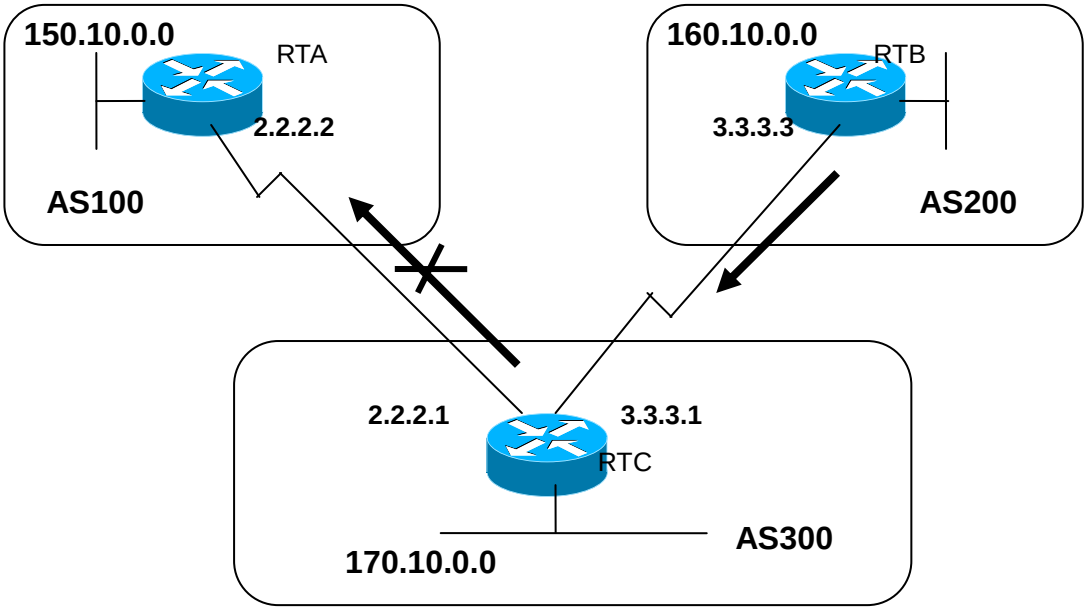


다음의 구성은 위 그림의 RTC 가 RTA 로 160.10.0.0 의 업데이트를 하는 것을 path filtering 을 사용하여 수행하는 구성을 보여준다.

```
RTC#
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 filter-list 1 out
!-- the 1 is the access list number below
ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*
```

1. Community Filtering

Community 는 여러 개의 destination 을 특정 그룹으로 community 화 하여, 이 community 에 routing decision 을 적용하기 위해 사용된다.



위 그림에서, RTC 가 자신의 eBGP peer 로 RTB 가 보내는 라우트들을 업데이트 하지 않도록, RTB 에 community attribute 를 설정하는 예가 다음에 나와 있다. 이를 위해 'no-export' community attribute 가 사용된다.

```
RTB#
router bgp 200
network 160.10.0.0
neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 send-community
neighbor 3.3.3.1 route-map setcommunity out
route-map setcommunity
match ip address 1
set community no-export
access-list 1 permit 0.0.0.0 255.255.255.255
```

시스코 라우터의 경우는 이러한 attribute 를 RTC 로 보내기 위해 **neighbor send-community** 명령을 사용해야 하나, 우리 시스템에서는 이 명령이 default enable 되어 있다. 그래서 위의 구성에서 실제로는 'neighbor 3.3.3.1 send-community' 명령어는 삭제 되어도 된다. 다만 이것을 disable 시키기 위해서는 'no neighbor 3.3.3.1 send-community'를 명시해야 한다.

이렇게 하여 RTC 가 **no-export** attribute 를 가진 update 를 얻는 경우, RTC 는 이 정보들을 자신의 외

부 피어인 RTA 로 전달하지 않는다.
다음의 구성 예에서는, RTB 가 community attribute 를 100 200 을 additive 하는 경우를 보여준다. 이 값 100 200 은 RTC 로 보내지기 전에 현존하는 community value 에 덧붙여 질 것이다. 만일 additive 명령어가 없는 경우는 기존의 community value 를 100 200 우로 대치하게 된다.

```
RTB#
   router bgp 200
   network 160.10.0.0
   neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 route-map setcommunity out

route-map setcommunity
match ip address 2
set community 100 200 additive
access-list 2 permit 0.0.0.0 255.255.255.255
```

community list 는, 서로 다른 community number 의 리스트들에 기반하여 attribute 들을 세팅하거나 필터링하도록 하기 위해 route map 의 **match** 문에 사용하게 되는 일종의 community 들의 그룹을 지칭한다.

ip community-list *community-list-number* **{permit|deny}** *community-number*

예로 다음의 라우트 맵을 정의할 수 있다.

```
route-map match-on-community
match community 10
!-- 10 is the community-list number
set weight 20
ip community-list 10 permit 200 300
!-- 200 300 is the community number
```

이 라우트 맵을 사용하여 특정 업데이트 시에 이 community value 에 기반하여 metric 값이나 weight 같은 특정 파라미터들을 필터링 하거나 세팅할 수 있다. 앞의 예에서, RTB 는 RTC 로 community 100 200 을 가진 업데이트를 보내고 있었다. 만일 RTC 가 이 값에 기반하여 weight 값을 세팅하고자 하는 경우 다음과 같은 구성을 할 수 있다.

```
RTC#
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 route-map check-community in
route-map check-community permit 10
match community 1
set weight 20
```

```
route-map check-community permit 20
match community 2 exact
set weight 10
route-map check-community permit 30
match community 3
ip community-list 1 permit 100
ip community-list 2 permit 200
ip community-list 3 permit internet
```

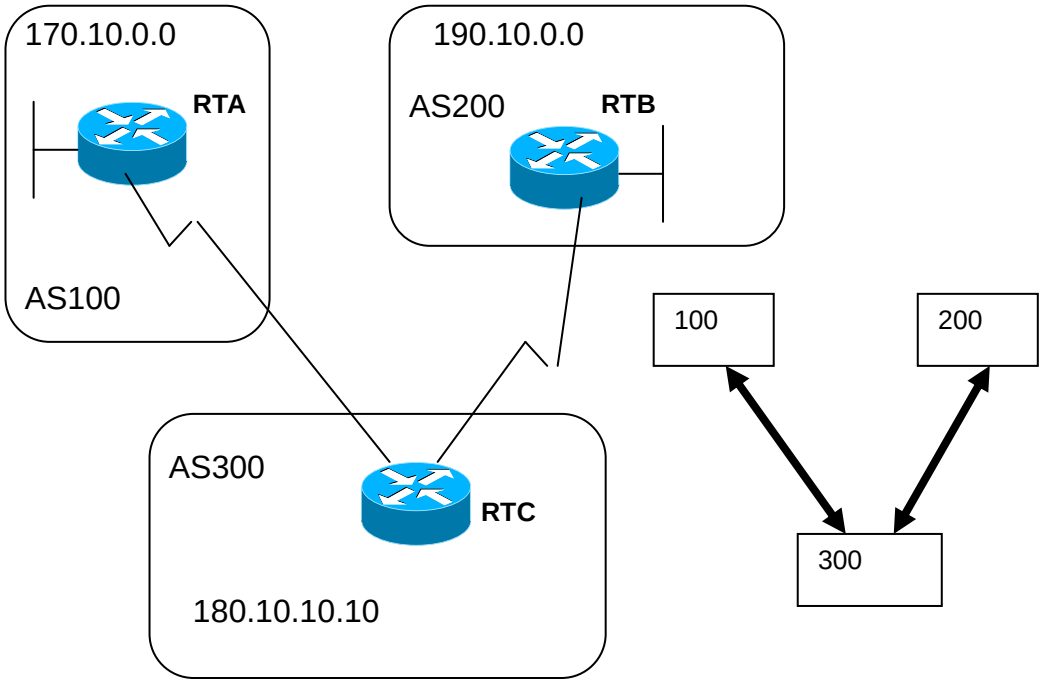
이 구성에서, community attribute 로 100 을 가진 라우트는 리스트 1 에 매치될 것이고 따라서 weight 값이 20 으로 세팅 된다. Community 값으로 200 만을 가진 라우트는 리스트 2 에 매치되어 weight 값 10 을 갖게 된다. 키워드 **exact** 는 community 가 200 만을 가지고 있어야 되면 그 밖의 다른 값은 없어야 됨을 의미한다. 마지막 community list 는 그 외의 업데이트가 drop 되지 않도록 하기 위해 사용된다. 왜냐하면, 매치가 되지 않는 것들은 디폴트로 drop 되기 때문이다. 키워드 **internet** 은 모든 라우트들이 internet community 의 멤버들이기 때문에 모든 라우트들을 의미한다.

10.7.4. BGP Attribute 설정

BGP 에 사용되는 attribute 들에는 다음과 같은 것들이 있다.

- ✓ **As-path attribute**
- ✓ **Origin attribute**
- ✓ **Nexthop attribute**
- ✓ **Local Preference attribute**
- ✓ **Metric attribute**
- ✓ **Community attribute**
- ✓ **Weight attribute**

10.1.4.6. As_path Attribute



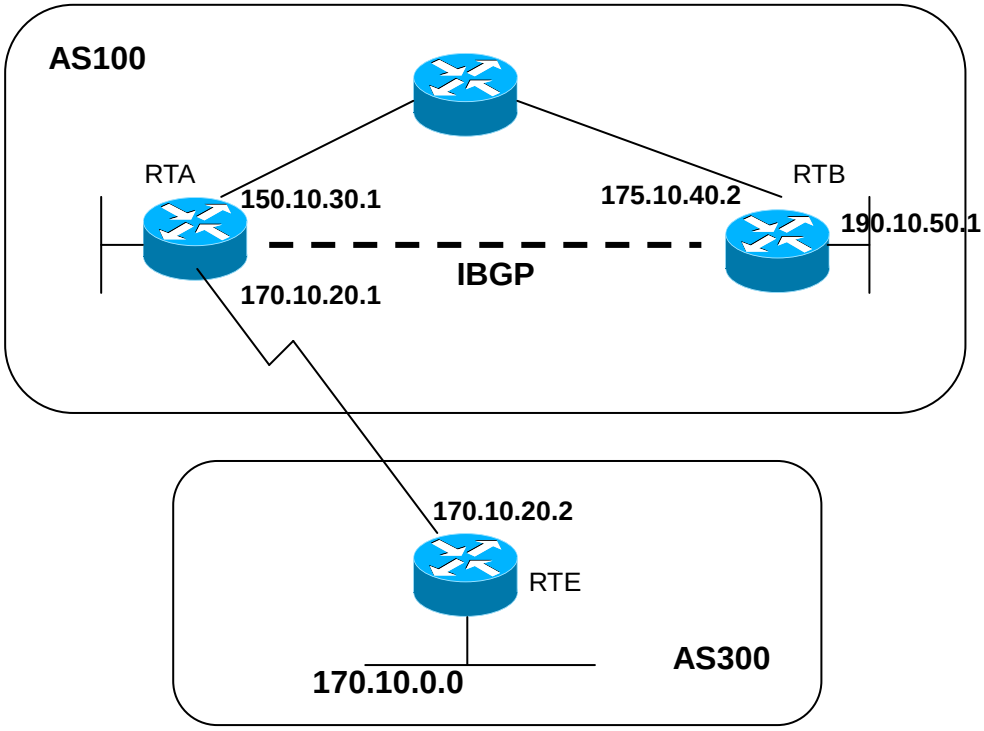
하나의 라우트가 하나의 AS 를 지나갈 때, 이 AS 의 번호가 해당 라우트의 업데이트에 추가된다. **AS_path** attribute 는 하나의 라우트가 특정 목적지에 도달하기 위해 지나온 AS 번호들의 리스트를 가리킨다. **AS-SET** 은 하나의 라우트가 지나온 모든 AS 들의 집합을 가리킨다. 위 그림에서 네트워크 190.10.0.0 은 AS200 에 있는 RTB 에 의해 알려진다. 이 라우트가 AS 300 을 지나갈 때 RTC 는 자신의 AS 번호 300 을 이 라우트의 as-path 에 덧붙인다. 그래서 190.10.0.0 라우트가 RTA 에 도달시 RTA 는 그것에 추가된 2 개의 AS 번호인 200 과 300 을 보게 될 것이다. 그래서 RTA 에 있어서 190.10.0.0 에 도달하기 위한 경로는 (300,200)이 된다.

170.10.0.0 과 180.10.0.0 에 대해서도 마찬가지 경우가 성립한다. RTB 는 170.10.0.0 에 도달하기 위해 AS300 과 AS100 을 지나가야 한다. RTC 는 190.10.0.0 에 도달하기 위해 AS 200 을 지나야 하고, 170.10.0.0 에 도달하기 위해서는 AS 100 을 지나야 한다.

10.1.4.7. Origin Attribute

이것은 패스 정보의 기원을 정의하는 attribute 이다. 이것에는 3 가지 값이 있다.

- ✓ **IGP**: NLRI(Network Layer Reachability Information)가 생성 AS의 내부에 있다. 이것은 보통 bgp network 명령을 사용하거나 IGP 정보가 BGP로 redistribute 될 때에 해당하고, 이 패스 정보의 origin은 IGP가 되고, BGP 테이블에 "i" 로 나타난다.
- ✓ **EGP**: NLRI는 BGP를 통해 습득된다. 이것은 BGP 테이블에 "e"로 표시된다.
- ✓ **INCOMPLETE**: NLRI 가 unknown이거나 기타의 방법으로 습득된다. 보통 static route를 BGP로 redistribute 할 때이다. 이것은 BGP 테이블에 "?"로 표시된다.




```
RTA#
router bgp 100
neighbor 190.10.50.1 remote-as 100
neighbor 170.10.20.2 remote-as 300
network 150.10.0.0
redistribute static

ip route 190.10.0.0 255.255.0.0 null0

RTB#
router bgp 100
neighbor 150.10.30.1 remote-as 100
network 190.10.50.0
RTE#
router bgp 300
neighbor 170.10.20.1 remote-as 100
```

```
network 170.10.0.0
```

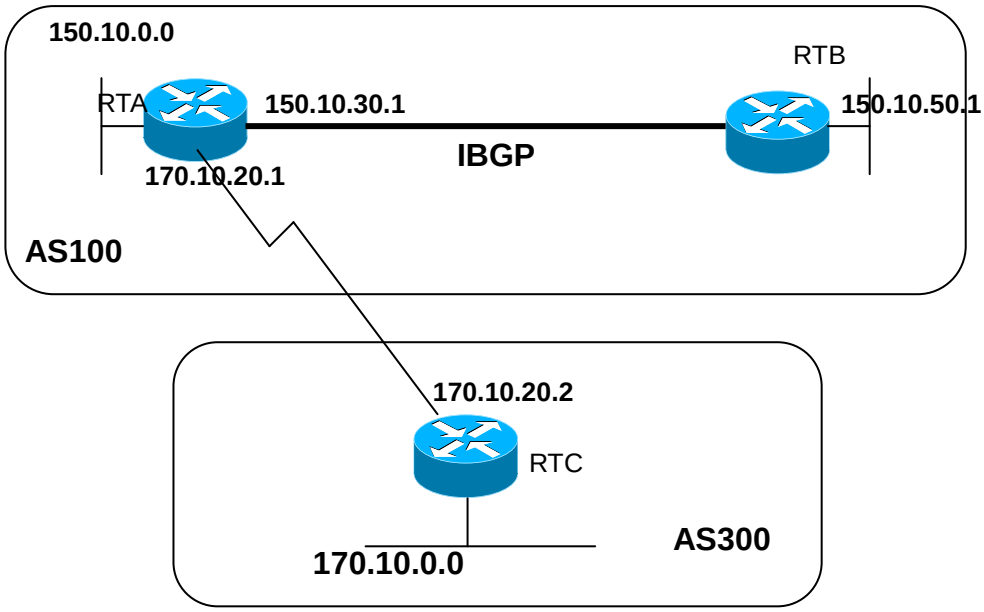
위 그림의 구성에서,

- RTA는 170.10.0.0에 300 i 를 통해 도달된다.
  (이것은 다음의 AS 패스가 300이고 이 라우트의 origin이 IGP임을 의미한다.)
- RTA는 190.10.50.0에 i 를 통해 도달된다.
  (이것은 다음의 AS 패스가 100이고 이 라우트의 origin이 IGP임을 의미한다.)
- RTE는 150.10.0.0에 100 i 를 통해 도달된다.
  (이것은 다음의 AS 패스가 100이고 이 라우트의 origin이 IGP임을 의미한다.)
- RTE는 190.10.0.0에 100 ? 를 통해 도달된다.
  (이것은 다음의 AS 패스가 100이고 이 라우트의 origin이 incomplete임을 의미한다.)

10.1.4.8. BGP Nexthop Attribute

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

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



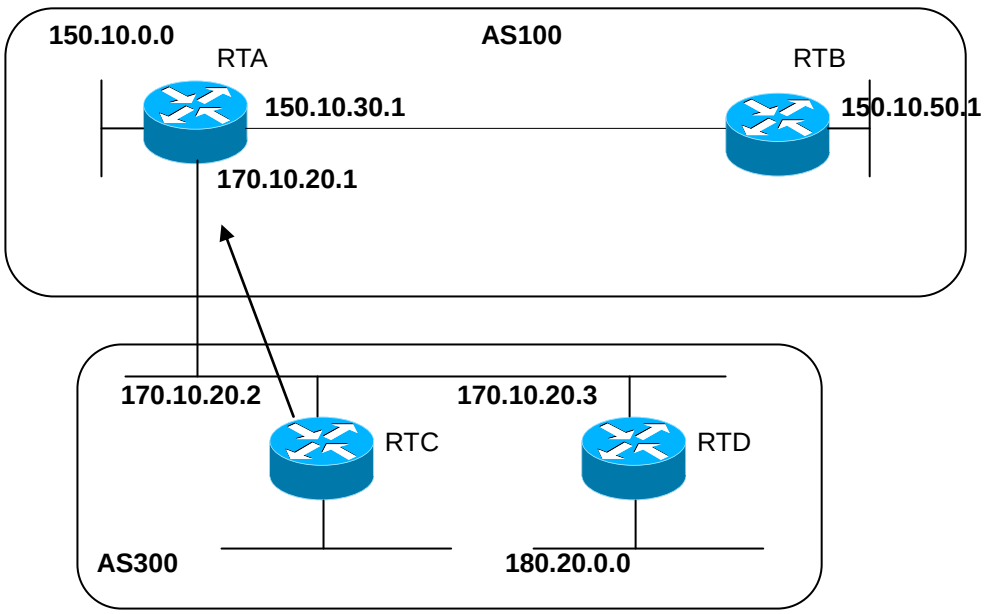

```
RTA#
router bgp 100
neighbor 170.10.20.2 remote-as 300
neighbor 150.10.50.1 remote-as 100
```

```
network 150.10.0.0
RTB#
router bgp 100
neighbor 150.10.30.1 remote-as 100
RTC#
router bgp 300
neighbor 170.10.20.1 remote-as 100
network 170.10.0.0
```

- RTC는 RTA로 170.10.0.0을 전달시 넥스트 홉이 170.10.20.2가 된다.
- RTA가 RTB로 170.10.0.0을 전달시 넥스트 홉이 170.10.20.2가 된다.

멀티액세스 네트워크와 NBMA 망에서는 특별한 주의가 요구되는데 다음에 설명한다.

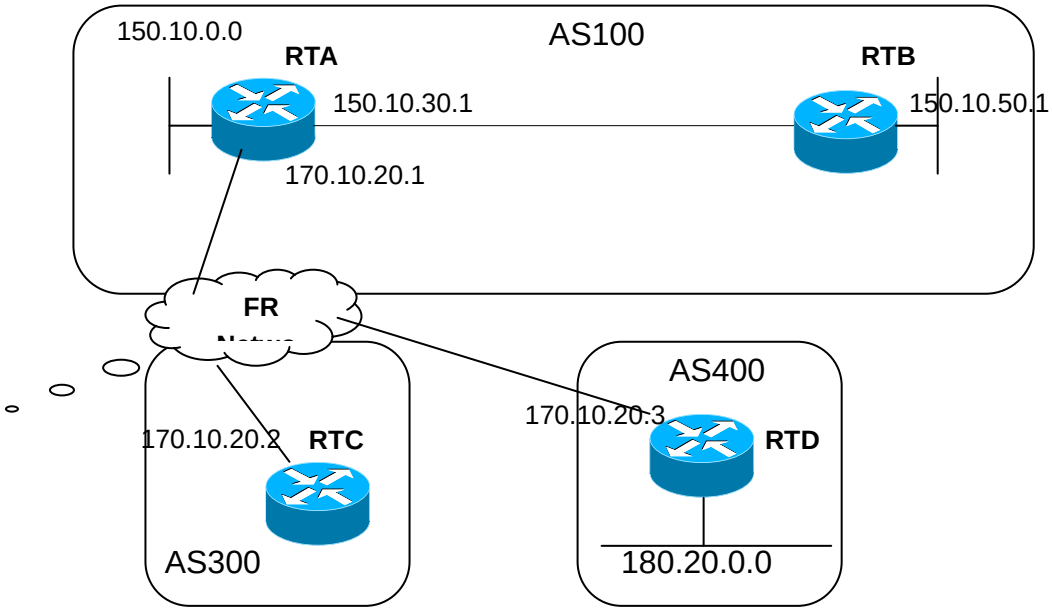
10.1.4.9. BGP Nexthop (Multiaccess Networks)



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

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

10.1.4.10. BGP Nexthop (NBMA)



위 그림에서 보듯이 공통 미디어가 Frame Relay 같은 NBMA 망이라면 앞의 경우와 같은 행동을 하게 된다. 즉 RTC 는 RTA 로 180.20.0.0 의 정보를 전달 시 넥스트 홉으로 170.10.20.3 을 사용한다. 문제는 RTA 가 RTD 로 직접적인 PVC 를 갖고 있지 않아서, 넥스트 홉에 도달할 수 없는 경우이다. 이 경우 라우팅은 실패하게 된다. 이 상황을 위해 nexthopself 명령이 고안 되었다.

10.1.4.11. Nexthopself

next-hop-self 명령은 프로토콜이 넥스트 홉을 지정하게 하지 않고, 지정된 IP 를 강제적으로 넥스트 홉으로 사용할 수 있게 해준다. 이 명령의 구문은 다음과 같다.

neighbor {ip-address|peer-group-name} **next-hop-self**

앞의 예와 같은 경우, 다음의 구성으로 문제를 해결할 수 있다.

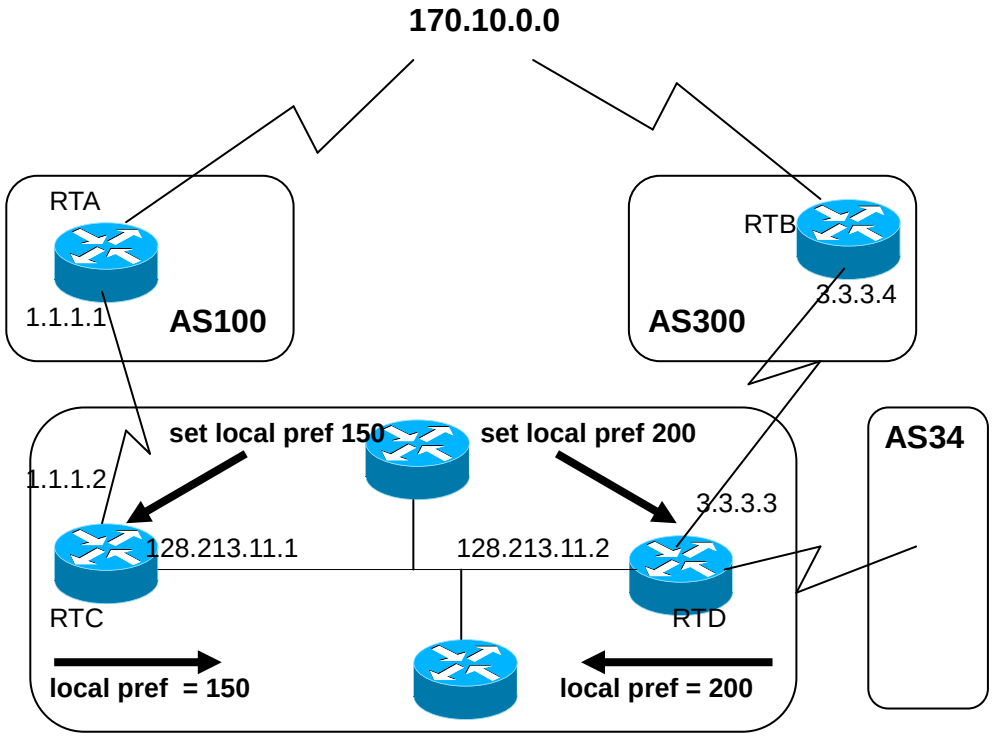
```
RTC#
router bgp 300
neighbor 170.10.20.1 remote-as 100
neighbor 170.10.20.1 next-hop-self
```

RTC 는 180.20.0.0 를 nextHop = 170.10.20.2 로 전송한다.

10.1.4.12. Local Preference Attribute

Local preference 는 특정 네트워크에 도달하기 위해 해당 AS 를 빠져나가는데 어떤 패스를 선호할 지를 AS 에게 알려준다. 더 높은 값을 지닌 local preference 를 가진 패스가 더 선호된다. 디폴트 값은 100 이다. 로컬 라우터에만 적용되는 weight attribute 와 달리, local preference 는 동일 AS 내에 있는 라우터들 간에 교환되는 attribute 이다.
local preference 는 **bgp default local-preference** < *value*> 명령이나 라우트 맵을 통해 세팅되는데, 다음에 그 예를 보여준다.

bgp default local-preference 명령은 동일 AS 내의 피어 라우터로 나가는 업데이트 시의 local preference 값을 모두 바꾼다. 아래 예제 그림에서, AS256 은 서로 다른 2 개의 AS 로부터 170.10.0.0 에 대한 업데이트를 받는다. local preference 는 동일 네트워크에 도달하기 위해 AS256 을 빠져 나가는 방법을 결정하는데 도움을 준다. 그림에서 RTD 가 선호되는 출구점(exit point) 이라고 가정하자. 다음의 구성은 AS 300 에서 오는 업데이트에 대한 local preference 값을 200 으로 세팅하고 AS100 에서 오는 업데이트는 150 으로 세팅한다.




```
RTC#
router bgp 256
neighbor 1.1.1.1 remote-as 100
neighbor 128.213.11.2 remote-as 256
bgp default local-preference 150
RTD#
```

```
router bgp 256
neighbor 3.3.3.4 remote-as 300
neighbor 128.213.11.1 remote-as 256
bgp default local-preference 200
```

위 구성에서 RTC 는 모든 업데이트의 local preference 를 150 으로 세팅하며, RTD 는 모든 업데이트의 local preference 를 200 으로 세팅한다. local preference 는 AS256 내에서 교환되기 때문에, RTC 와 RTD 는 네트워크 170.10.0.0 정보가 AS100 보다는 AS300 에서 오는 정보가 더 높은 local preference 를 갖는다고 인식하게 된다. 그래서 170.10.0.0 으로 지정된 AS256 내의 모든 트래픽은 RTD 로 보내진다.

이와는 달리 라우트 맵을 사용하여 더 많은 융통성을 제공할 수 있다. 위 예에서, RTD 가 수신하는 모든 업데이트는 local preference 200 으로 세팅된다. 이것은 바람직하지 않을 수 있다. 아래 구성에서 보여지는 것처럼 특정 업데이트는 특정 local preference 로 세팅할 필요가 있을 때 라우트 맵을 사용한다.

```
RTD#
router bgp 256
neighbor 3.3.3.4 remote-as 300
neighbor 3.3.3.4 route-map setlocalin in
neighbor 128.213.11.1 remote-as 256
....
ip as-path access-list 7 permit ^300$
...
route-map setlocalin permit 10
match as-path 7
set local-preference 200
route-map setlocalin permit 20
set local-preference 150
```

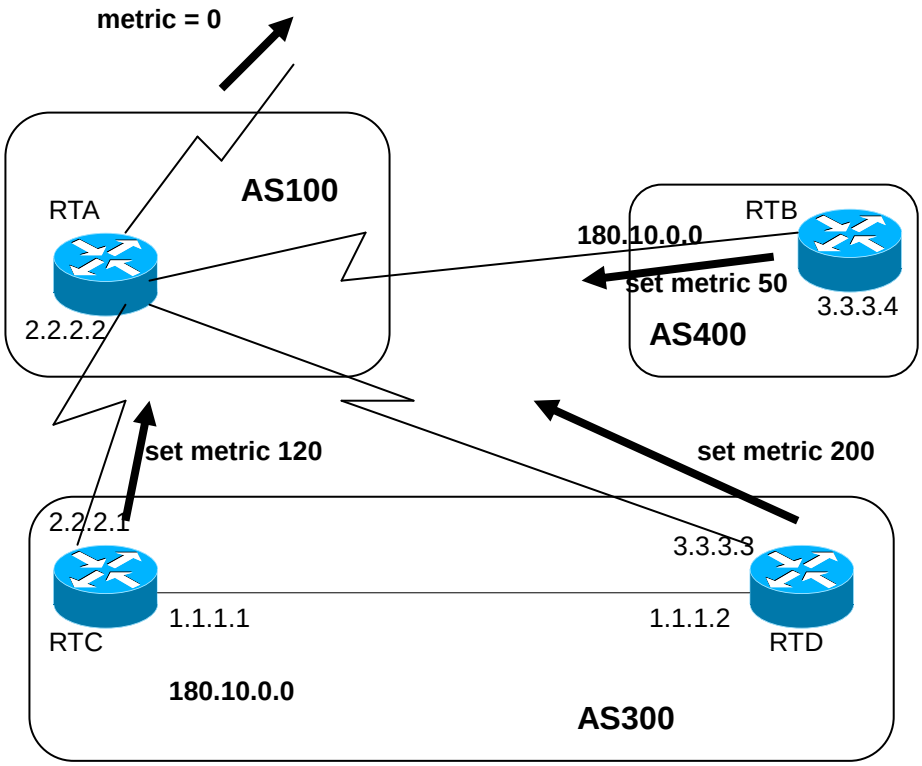
이 구성을 통해, AS300 에서 오는 업데이트는 local preference 200 으로 세팅 되고, AS34 로부터 오는 다른 업데이트들은 local preference 150 으로 세팅된다.

10.1.4.13. Metric Attribute

metric attribute 는 Multi_exit_discriminator(MED)로도 불려지는데, 특정 AS 로 향하는 패스에 대한 선호정보를 외부 네이버에 제공한다. 특정 AS 로의 진입점이 다수 존재시, 그 AS 내의 라우트로 도달하기 위해 어떤 지점을 선택할 지에 대해 타 AS 에 영향을 줄 수 있는 동적인 방법이다. 더 낮은 값을 지닌 경로가 선택된다.

local preference 와 달리, metric 은 AS 들 간에 교환된다. 이 메트릭 값은 하나의 AS 로 전달되지만, 그 AS 를 떠나지는 않는다. 특정 메트릭 값을 지닌 업데이트가 AS 에 들어 왔을 때, 그 메트릭 값은 그 AS 내에서의 경로 선택에 사용된다. 동일한 업데이트 정보가 또 다른 AS 로 전달될 시, 이 메트릭 값은 0 으로 세팅되어 전달된다. 디폴트 값은 0 이다. 다른 특별한 지정이 없는 경우, 동일 AS 상에 있는 네이

버들로부터 온 경로에 대해서만 메트릭 값을 비교한다. 서로 다른 AS 에 있는 네이버들로부터 온 메트릭을 비교하기 위해서는 “bgp always-compare-med" 라는 특별한 구성 명령을 필요로 한다.



위 그림에서, AS100 은 3 개의 서로 다른 라우터 RTC, RTD, RTB 를 통해서 180.10.0.0 의 네트워크 정보를 얻고 있다. RTC 와 RTD 는 AS300 에 있고, RTB 는 AS400 에 있다.

RTC 로부터 오는 메트릭 값을 120 으로 세팅하고 RTD 로부터 오는 메트릭 값은 200 으로 RTB 로부터 오는 메트릭 값은 50 으로 세팅 되어 있는 것으로 가정하자. 디폴트로, 라우터는 동일 AS 에 있는 네이버들로부터 오는 메트릭만을 비교한다. 그래서 RTA 는 RTC 와 RTD 로부터 오는 메트릭만을 비교할 수 있어서 RTC 를 베스트 넥스트 홉으로 선택한다. 왜냐하면 120 이 200 보다 작기 때문이다. RTA 가 RTB 로부터 메트릭 50 을 지닌 정보를 수신 시, RTA 는 이것을 120 과 비교할 수 없다. 왜냐하면 RTC 와 RTB 는 서로 다른 AS 에 있기 때문이다(RTA 는 다른 attribute 들에 기반하여 경로 선택을 한다.).
RTA 가 이 메트릭을 비교할 수 있기 위해서는 RTA 에 **bgp always-compare-med** 명령을 추가한다. 아래에 그 구성이 나와있다.

```
RTA#
   router bgp 100
   neighbor 2.2.2.1 remote-as 300
   neighbor 3.3.3.3 remote-as 300
   neighbor 4.4.4.3 remote-as 400
   ....
RTC#
   router bgp 300
```

```
   neighbor 2.2.2.2 remote-as 100
   neighbor 2.2.2.2 route-map setmetricout out
   neighbor 1.1.1.2 remote-as 300
route-map setmetricout permit 10
   set metric 120
RTD#
   router bgp 300
   neighbor 3.3.3.2 remote-as 100
   neighbor 3.3.3.2 route-map setmetricout out
   neighbor 1.1.1.1 remote-as 300
route-map setmetricout permit 10
   set metric 200
RTB#
   router bgp 400
   neighbor 4.4.4.4 remote-as 100
   neighbor 4.4.4.4 route-map setmetricout out
route-map setmetricout permit 10
   set metric 50
```

위 구성에서, RTA 는 RTC 를 넥스트 홉으로 선택한다.(다른 모든 attribute 들이 동일하다고 가정시). RTB 가 메트릭 비교에 포함되기 위해서는 RTA 를 다음과 같이 구성한다.

```
RTA#
router bgp 100
neighbor 2.2.21 remote-as 300
neighbor 3.3.3.3 remote-as 300
neighbor 4.4.4.3 remote-as 400
bgp always-compare-med
```

이 경우 RTA 는 180.10.0.0 에 도달하기 위한 최적의 넥스트 홉으로 RTB 를 선택한다.
default-metric *number* 명령을 사용하여 BGP 로 라우트를 redistribute 하면서 메트릭 값을 세팅할 수도 있다. 위 예에서 RTB 가 스태틱 정보를 redistribute 한다고 가정할 경우의 구성은 다음과 같다.

```
RTB#
router bgp 400
redistribute static
default-metric 50

ip route 180.10.0.0 255.255.0.0 null 0
!-- Causes RTB to send out 180.10.0.0 with a metric of 50
```

10.1.4.14. Community Attribute

community attribute 는 0 에서 4,294,967,200 까지의 값을 갖는 optional, transitive attribute 이다. community attribute 는 여러 개의 목적지들을 특정 community 로 그룹화하는 방법인데, 이렇게 그룹화된 커뮤니티에 라우팅 결정(accept, prefer, redistribute 등)을 적용 가능하게 된다.
community attribute 를 세팅하기 위해 라우트 맵을 사용할 수 있다. 라우트 맵의 세팅 명령은 다음의

구문을 갖는다.

set community *community-number* **[additive]**

몇 개의 미리 정의된 잘 알려진 커뮤니티들(community-number)로는 다음이 있다.

- **no-export** (Do not advertise to EBGP peers)
- **no-advertise** (Do not advertise this route to any peer)
- **internet** (Advertise this route to the internet community, any router belongs to it)

커뮤니티가 세팅되는 라우트 맵의 예로 다음이 있다.

```
route-map communitymap
match ip address 1
set community no-advertise
```

or

```
route-map setcommunity
match as-path 1
set community 200 additive
```

만일 additive 키워드가 세팅 되지 않은 경우, 200 이 기존에 존재하는 커뮤니티 값을 대체한다. Additive 키워드를 사용하는 경우, 200 이 기존 커뮤니티에 추가된다. 본 시스템에서는 community attribute 를 세팅하면, 이 attribute 는 디폴트로 네이버로 전달된다. 시스코의 경우는 다음의 명령을 사용해야 전달이 된다.

neighbor {*ip-address*|*peer-group-name*} **send-community**

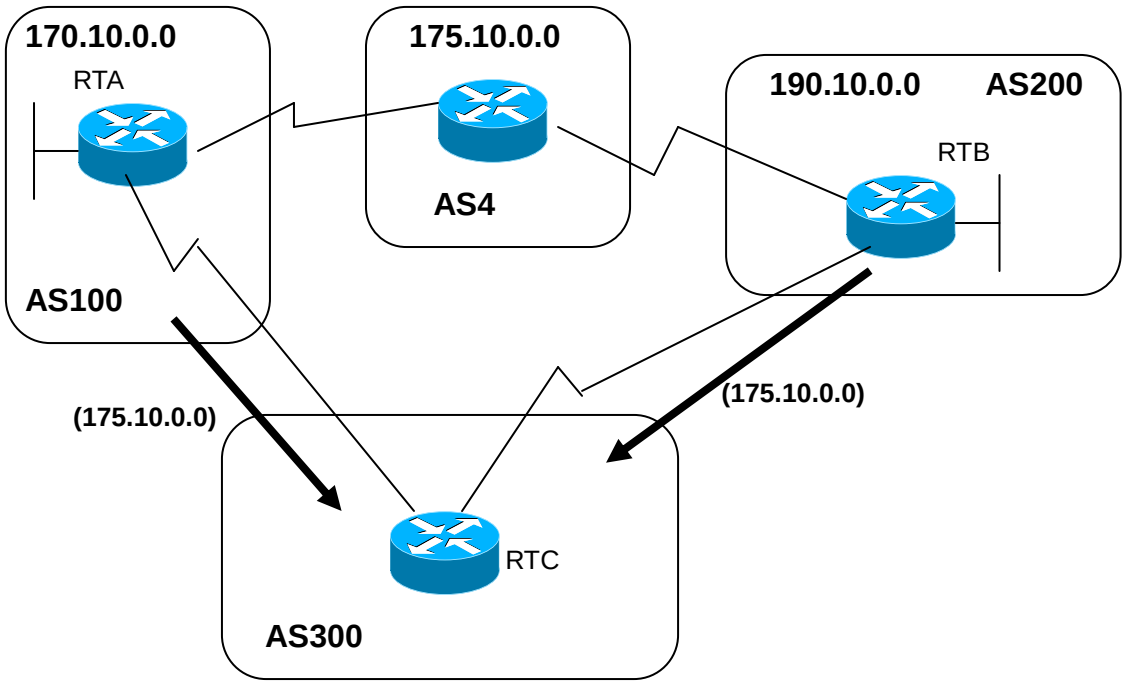
```
RTA#
router bgp 100
neighbor 3.3.3.3 remote-as 300
neighbor 3.3.3.3 send-community
neighbor 3.3.3.3 route-map setcommunity out
```

본 시스템에서는 neighbor send-community 가 디폴트로 활성화 되어 있어 ‘neighbor 3.3.3.3 send-community’ 명령은 필요치 않다.

10.1.4.15. Weight Attribute

weight attribute 는 스펙에는 없는 것이지만 본 시스템에서 정의 하였으며, 시스코 시스템의 weight attribute 와 동일한 기능을 지니고 있다. 이 값은 해당 라우터에만 적용된다. 즉 특정 라우터에만 의미 있는 값이고 다른 라우터로 전달되지 않는다. 이 값은 0 에서 65535 범위 값을 가지며, 자신이 생성한 경로에 대해서는 디폴트로 32768 을 할당한다. 다른 경로들은 0 값을 갖는다.

동일 목적지로 다수의 라우트가 존재시 더 높은 weight 값을 지닌 라우트가 선택된다.



위 그림에서, RTA 는 네트워크 175.10.0.0 에 대한 정보를 AS4 에서 얻었고, 이 정보를 RTC 로 전달한다. RTB 또한 네트워크 175.10.0.0 에 대한 정보를 AS4 에서 얻었고, 이 정보를 RTC 로 전달한다. 이제 RTC 는 네트워크 175.10.0.0 에 도달하는 2 가지 경로를 얻었고 어느 쪽으로 가야할 지를 선택해야 한다. 만일 RTC 에서, RTA 로부터 오는 정보에 RTB 에서 오는 정보 보다 더 높은 weight 값을 주면, RTC 는 네트워크 175.10.0.0 에 도달하기 위한 넥스트 홉으로 RTA 를 선택하도록 할 수 있다. 이것은 여러 가지 방법을 이용하여 수행할 수 있다.

- Using the **neighbor** command: **neighbor** {*ip-address*|*peer-group*} **weight** *weight*.
- Using AS path access-lists: **ip as-path access-list** *access-list-number* **{permit|deny}** *as-regular-expression* **neighbor** *ip-address* **filter-list** *access-list-number* **weight** *weight*.
- Using route-maps.

동일 목적지로의 다수 경로가 존재시, 더 높은 weight 값을 가진 경로가 선택된다. 위의 예제에서 RTA 를 넥스트 홉으로 선택하기 위한 구성을 3 가지 방법을 이용하여 구성하였다.

neighbor weight 명령어 사용

```
RTC#
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 weight 200
!-- route to 175.10.0.0 from RTA has 200 weight
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 weight 100
!-- route to 175.10.0.0 from RTB will have 100 weight
```

IP as-path 와 filter-list 사용

```
RTC#
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 filter-list 5 weight 200
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 filter-list 6 weight 100
...
ip as-path access-list 5 permit ^100$
!-- this only permits path 100
ip as-path access-list 6 permit ^200$
```

라우트 맵 사용

```
RTC#
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 route-map setweightin in
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-map setweightin in
...
ip as-path access-list 5 permit ^100$
...
route-map setweightin permit 10
match as-path 5
set weight 200
!-- anything that applies to access-list 5, such as packets from AS100, have
weight 200
route-map setweightin permit 20
   set weight 100
   !-- anything else would have weight 100
```

10.7.5. Routing Policy 변경

Routing policy 라 함은 네이버 라우터와 라우팅 정보를 주고 받을 때 route-map, filter-list, prefix-list 등을 이용하여 받아들일 정보와 제공할 정보에 대한 취사 선택을 할 수 있도록 해주는 것이다. BGP 에서는 이러한 routing policy 가 변경되는 경우, 기존 정책을 따르는 라우팅 정보를 삭제하거나 원 경로를 복구하여 새로운 정책에 맞는 라우팅 정보를 갖게 된다.

BGP 라우터가 새로운 폴리시에 맞는 정보를 받아들이도록 하려면, inbound reset 을 설정하여주고, 새로운 정보 제공의 경우에는 outbound reset 을 설정한다. 새로운 정책에 맞추어 새로운 정보를 제공하면 네이버 라우터들도 새로운 정보를 받아들인다.

만일 사용자의 망에 위치한 BGP 라우터와 네이버 라우터 모두가 route refresh capability 기능을 지원하는 경우라면 inbound reset 을 이용하여 라우팅 정보를 갱신할 수 있다. 이 방법을 이용한 라우터 재설정은 다음과 같은 장점이 있다.

- ✓ 관리자의 추가 설정 동작이 필요 없다.
- ✓ 라우팅 정보 변경에 따른 추가의 메모리 사용이 없다.

네이버 라우터가 route refresh capability 기능을 지원하는지 확인 하려면 다음의 명령을 사용한다.

```
neighbor capability route-refresh
```

이 명령을 사용하면, 네이버 라우터에 route refresh capability 기능을 알려주고 네이버 라우터도 이 기능을 지원하는 경우, “ Received route refresh capability from peer” 메시지가 출력된다.

만일 모든 BGP 라우터가 route refresh capability 기능을 지원한다면, 사용자는 soft reset 을 이용하여 이전에 보낸 경로 정보를 받아 볼 수 있다. 새로운 정책에 부합하는 라우팅 정보를 설정하려면 다음과 같은 명령을 사용한다.

```
clear ip bgp [* | AS | address] soft in
```

반면에 outbound reset 기능은 별도의 사전 설정을 필요로 하지 않고, soft 라는 명령어를 사용하여 라우팅 정보를 다시 전송한다. 라우팅 정보를 다시 제공하려면, 다음의 명령을 사용한다.

```
clear ip bgp [* | AS | address] soft out
```

관리자가 변경된 라우팅 정책을 초기 상태로 복구시에는 route refresh capability 기능을 사용한다. 이 기능을 사용하면 각각의 변경된 내용을 하나씩 삭제하지 않아도 된다.

route refresh capability 기능을 지원하지 않는 장비의 경우에는 neighbor soft-reconfiguration 명령어를 사용하여 기존에 주고 받던 라우팅 정보를 삭제해야 한다. 그러나 이것은 네트워크에 문제가 발생할

수 있는 소지가 있으므로 가능한 사용하지 않는 것이 좋다.

BGP 정보를 재설정하지 않고 새로운 정보를 생성하려면 라우팅 정보를 선별적으로 처리하지 않고 BGP 네트워크로 들어오는 모든 정보를 저장해야 한다. 이 방법은 메모리 부하를 야기 시키기 때문에 가능한 사용하지 않는 것이 좋다. 그러나 변경된 정보를 제공하는 것은 메모리를 요구하지 않는다. BGP 라우터가 새로운 변경된 정보를 전달하면 연쇄적으로 네이버 라우터들이 변경된 정보를 받아들이게 된다.

설정된 routing policy 를 이용하여 BGP 설정을 바꾸기 위한 절차는 다음과 같다.

1) BGP 라우터를 재설정 한 후, 네이버 라우터가 보내온 모든 정보를 저장하도록 설정한다. 이 시점부터 BGP 라우터에 들어오는 모든 정보는 저장된다.

neighbor *ip-address* **soft-reconfiguration inbound**

2) 저장된 정보를 이용하여 새롭게 변경된 정보를 테이블에 등록한다.

clear ip bgp [* | AS | address] **soft in**

라우팅 테이블과 bgp 네이버 라우터를 통해 라우팅 정보가 제대로 변경 되었는지 확인하려면 다음의 명령을 사용한다.

show ip bgp neighbors *ip-address* **[advertised-routes|received-routes|routes]**

10.7.6. BGP Peer Groups

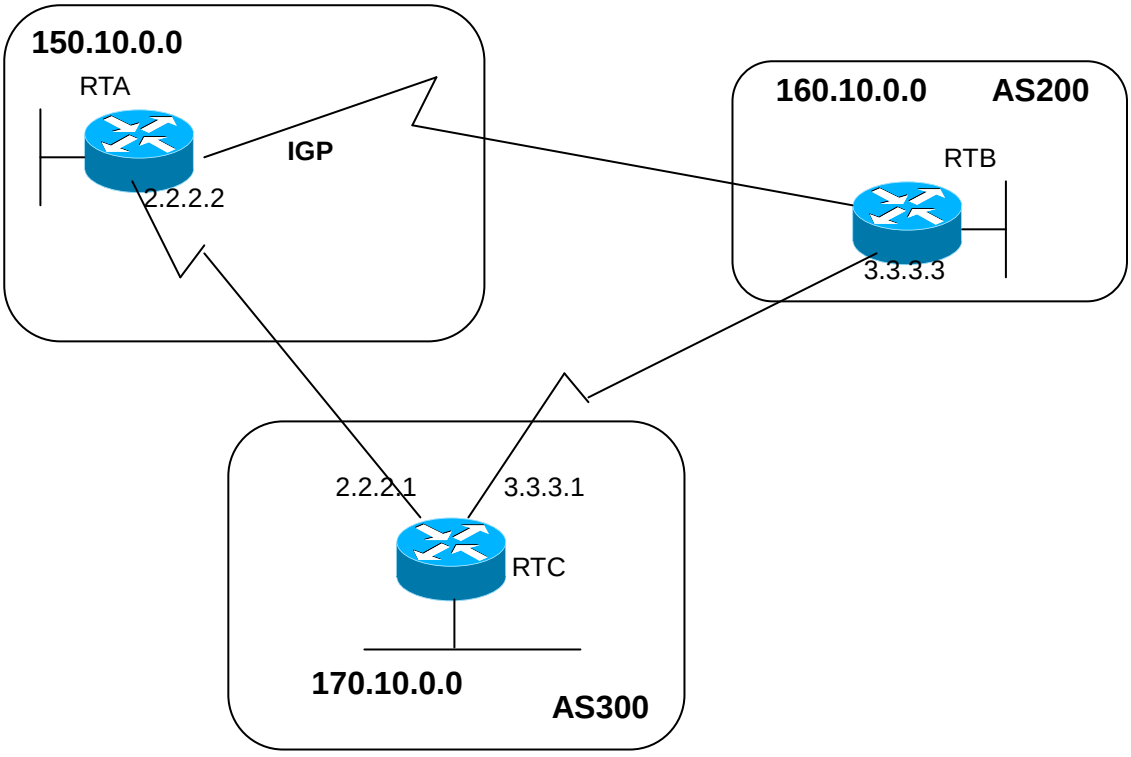
동일한 업데이트 policy 가 적용되는 BGP 네이버들의 그룹을 의미한다. 업데이트 폴리시는 주로 라우트 맵, distribute-list, filter-list 에 의해 세팅된다. 각각의 별도 네이버에 동일한 폴리시를 정의하는 데 신에. Peer group name 을 정의하여 그 피어 그룹에 이러한 폴리시들을 적용한다.

피어 그룹의 멤버들은 그 피어 그룹의 configuration option 모두를 계승한다. 멤버들은 또한 출력 업데이트에 영향을 미치지 않는 옵션이라면 새로운 옵션들을 정의하여 피어그룹의 옵션을 오버라이드 할 수 있다. 그러나 inbound 쪽에만 옵션들을 오버라이드 할 수 있음을 명심해야 한다.

피어 그룹의 정의를 위해 다음이 사용된다.

neighbor *peer-group-name* **peer-group**

BGP backdoor



위의 그림에서 RTA 와 RTC 는 EBGP 로 연결되어 있고, RTB 와 RTC 간에도 EBGP 연결이 되어있다. RTA 와 RTB 는 IGP 프로토콜(OSPF, RIP 등)을 돌리고 있다. EBGP 업데이트는 IGP distance 값보다 작은 20 의 distance 값을 갖는다. 참고로 RIP 경우는 디폴트 디스턴스 값이 120 이고, OSPF 는 110 의 값을 갖는다.

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

디폴트로, BGP 는 다음의 디스턴스 값을 갖지만 다음의 distance command 에 의해 변경될 수 있다.

distance bgp *external-distance internal-distance local-distance*
external-distance:20
internal-distance:200
local-distance:200

RTA 는 더 낮은 디스턴스 값을 지닌 RTC 를 통해 받은 EBGP 업데이트 정보를 선택한다. 만일 RTA 가 160.10.0.0 에 대한 정보를 RTB 를 통해(즉, IGP 를 통해) 받기를 원한다면, 두 가지 행동을 취할 수 있다.

- ✓ EBGP의 external distance 값이나 IGP의 external distance 값을 바꾼다.(바람직하지 않음)
- ✓ BGP backdoor 사용

이처럼 BGP backdoor 는 IGP 라우트를 선호 라우트로 만들어 준다. 이를 위해 다음의 명령을 사용한다.

network *address* **backdoor**

지정되는 주소 값은 IGP 를 통해 수신하고자 하는 네트워크 주소이다. BGP 의 경우, 이 네트워크는 BGP 업데이트에서 전달되지 않는다는 점을 제외하면 로컬리 할당된 네트워크처럼 취급된다.

```
RTA#
router ospf

router bgp 100
neighbor 2.2.2.1 remote-as 300
network 160.10.0.0 backdoor
```

네트워크 160.10.0.0 은 로컬 엔트리로 취급되지만. 보통의 네트워크 엔트리처럼 전달되지 는 않는다. RTA 는 디스턴스 값 110 을 가진 OSPF 를 통해 RTB 로부터 160.10.0.0 에 대한 정보를 취득한다. 그리고 동시에 디스턴스 값 20 을 지닌 EBGP 를 통해 RTC 로부터도 취득한다. 보통은 EBGP 가 선호되지만 backdoor 명령 때문에 OSPF 정보가 선택된다.

10.7.7. BGP Multipath

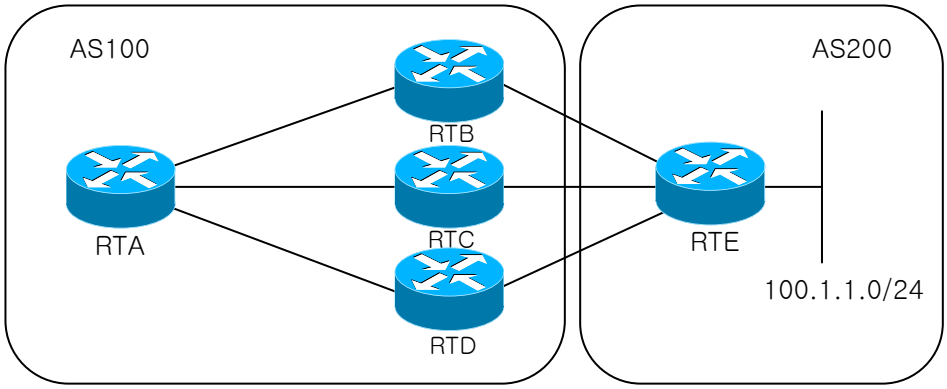
BGP Multipath 는 동일한 목적지에 대해서 여러 BGP 경로를 갖는 것을 허락한다. 이 경로들은 Load Sharing 을 위해서 best path 와 함께 라우팅 테이블에 설정된다. BGP Multipath 는 best path 를 선정하는데 영향을 주지 않는다. 예를 들어서, 라우터는 Multi-Path 중에서 하나를 best path 로서 지정한다. 그리고 그 best path 를 neighbors 에게 advertise 한다.

Multipath의 후보가 되기 위해서, 동일한 목적지를 갖는 path들은 best path와 다음의 조건들이 동일해야 한다.

Weight
Local preference
AS-PATH length
Origin
MED
One of these:
Neighboring AS or sub-AS (before the addition of the eiBGP Multipath feature)
AS-PATH (after the addition of the eiBGP Multipath feature)

몇몇 BGP Multipath 특징들은 multipath 후보들에 추가적인 요구사항이 있다.
다음은 eBGP multipath에 대한 추가적인 요구사항이다.
그 경로는 external or confederation-external neighbor로부터 배워야 한다.
BGP nexthop에 대한 IGP metric은 best path의 IGP metric과 동일해야 한다.

다음은 iBGP multipath에 대한 추가적인 요구사항이다.
그 경로는 internal neighbor로부터 배워야 한다.
BGP nexthop에 대한 IGP metric은 best path의 IGP metric과 동일해야 한다.



위의 그림에서 RTA 는 네트워크 100.1.1.0/24 를 RTB, RTC, RTD 로부터 받게 된다. 라우터는 디폴트로 multipath 기능이 disable 되어 잇다. 따라서 multipath 기능을 사용하기 위해서 다음의 명령어를 사용한다.

maximum-path *[ibgp|ebgp|eibgp] number*

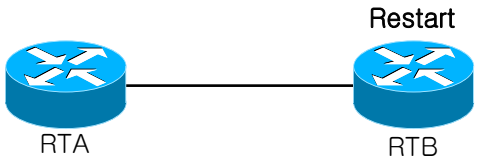
Multipath 기능을 사용하기 위해 RTA 에서 다음과 같이 설정을 한다.

```
RTA#
router bgp 100
 maximum-paths ibgp 3
 neighbor 10.1.1.1 remote-as 200  /* RTB */
```

```
neighbor 20.1.1.1 remote-as 200  /* RTC */
neighbor 30.1.1.1 remote-as 200  /* RTD */
```

10.7.8. BGP graceful-restart

보통, 어떤 라우터의 BGP 가 restart 했을 때, 그 BGP 와 연결된 모든 BGP Peer 들은 session 이 down 되었다 다시 up 되는 것을 감지한다. 이러한 “down/up”은 “routing flap”을 초래하고, BGP route 의 재계산을 야기시킨다. 또한, “routing flaps”은 일시적으로 forwarding black hole 과 forwarding loop 을 발생시킬 수 있다. 이러한 것들로 인해, 전체 네트워크의 성능에 부정적인 영향을 끼치게 된다.
BGP graceful restart 는 BGP restart 에 의해서 야기되는 부정적인 영향들을 최소화 시키는 것 것들 돕는 메커니즘이다. 이 메커니즘은 BGP 가 restart 하는 동안, BGP speaker 가 forwarding state 를 보존시키도록 한다.



위 그림은 RTB 가 BGP restart 를 하고 RTA 가 BGP graceful-restart 를 처리하도록 한다. BGP graceful-restart 는 default 로 disable 되어 있다. 따라서 이 기능을 사용하기 위해서 다음의 명령어를 설정해야 한다. stalepath-time 은 Local BGP 가 restarting Peer 에 대해, stale-path 를 hole 하고 있는 최대 시간이다. stalepath-time 에 명세된 시간 동안 restarting Peer 가 route 를 update 하지 않으면 stale path 는 지워진다.

bgp graceful-restart [**stalepath-time** *seconds*]

BGP graceful-restart 기능을 사용하기 위해 RTA 에서 다음과 같이 설정을 한다.

```
RTA#
router bgp 100
 bgp graceful-restart stalepath-time 200
 neighbor 10.1.1.1 remote-as 200  /* RTB */
```

10.7.9. BGP default-metric

default metric은 incompatible metric과 함께 재분배 되는 라우트들의 문제를 해결하기 위해 사용된다. 이 값은 MED(Multi Exit Discriminator)으로써 best path selection 을 계산하는데 영향을 준다. MED는 Local AS에서만 처리되는 non-transitive 값이다. 따라서 External AS에는 이 값이 전달되지 않는다.

다음은 이 기능이 설정 되지 않았을 때, 기본적인 metric 설정을 나타낸다.

- 재분배된 IGP 라우트의 metric 은 interior BGP metric 과 동일하게 설정된다.
- 재분배된 connected 와 static 라우트의 metric 은 0 으로 설정된다.
- 그리고 이 기능이 설정되었을 때 재분배된 connected 라우트의 metric 은 0 으로 설정된다.

이 기능을 사용하기 위해서 다음의 명령어를 설정해야 한다.

default-metric *number*

10.7.10. BGP redistribute-internal

OSPF, RIP와 같은 IGP에서 redistribute bgp 가 설정되어있는 경우 iBGP로 얻은 route 가 같은 IGP인 OSPF나 RIP에 redistribute이 되어 loop 이 발생할 수 있게 된다.. 이러한 상황을 방지하기 위해 default로 redistribute bgp 가 설정되어 있어도 iBGP route은 redistribute을 하지 않도록 한다. 강제적으로 iBGP route가 redistribute 되기를 원하는 경우 이 명령어를 사용한다.

bgp redistribute-internal

10.7.11. Use of set as-path prepend Command

어떤 상황에서는 BGP decision process 를 조절하기 위해 경로 정보를 조정해야만 할때가 있다. 이를 위해 라우트 맵과 함께 사용되는 명령은 다음과 같다.

set as-path prepend <As-path#><As-path#> ...

10.7.12. 기타 기능

neighbor 명령은 입력 혹은 출력되는 업데이트에 대해 필터링을 하거나 파라미터 세팅을 수행하기 위해 route map 과 함께 사용될 수 있다.

네이버 문과 연관된 라우트 맵은 IP address 에 기반하여 매치를 수행할 때, 입력되는 업데이트에 대해서는 영향을 미치지 않는다.

neighbor ip-address **route-map** route-map-name

neighbor 에 password 를 지정하여, TCP connection 에 대한 인증 기능을 사용할 수 있다. Password 가 일치하면, neighbor 끼리는 TCP connection 이 되고 메시지 통신을 하게 된다.

neighbor ip-address **password** KEY **neighbor** ip-address **password 0** KEY **neighbor** ip-address **password 7** KEY

neighbor 의 password 는 encryption 가능하며, 암호화 전에 설정된 password 의 level 은 0 이고, 암호 후에 7 로 변경 된다.
단, 사용자가 암호화 전에 password 를 level 7 로 설정할 수는 없다.

10.8. Route Flap Dampening

route dampening 은 라우트 플래핑과 네트워크 상의 오실레이션에 의해 야기되는 불안정성을 최소화하고자 하는 메커니즘이다. 이를 위해 부적절하게 동작하는 라우트들을 정의하는 원칙이 정의된다. 플래핑 하는 라우트는 각 플랩마다 패널티 값(디폴트 1000)을 얻는다. 이렇게 축적된 패널티 값이 미리 정의된 “suppress-limit” 값을 넘으면, 이 라우트의 전달은 중지된다. 이 패널티 값은 미리 정의된 “half-time”에 도달하면 절반씩 감소되는데, 5 초마다 절반씩 감소된다. 감소된 패널티 값이 미리 정의된 “reuse-limit” 값 이하에 도달하면, 이 라우트는 다시 전달된다.

IBGP 를 통해 습득된 외부 라우트들은 dampening 되지 않음을 유의해야 한다. 그리고 dampening 정보는 패널티 값이 “reuse-limit” 값의 절반 이하가 될 때까지는 계속해서 라우터에 유지가 된다.

초기에 route dampening 은 디폴트로 오프상태이다. 다음의 명령들이 route dampening 을 조절하는데 사용된다.

- **bgp dampening** (will turn on dampening)
- **no bgp dampening** (will turn off dampening)
- **bgp dampening** <*half-life-time*> (will change the half-life-time)

동시에 모든 파라미터들을 바꾸는 명령은,

- **bgp dampening** <*half-life-time*> <*reuse*> <*suppress*> <*maximum-suppress-time*>
- <*half-life-time*> (range is 1-45 min, current default is 15 min)
- <*reuse-value*> (range is 1-20000, default is 750)
- <*suppress-value*> (range is 1-20000, default is 2000)
- <*max-suppress-time*> (maximum duration a route can be suppressed, range is 1-255, default is 4 times half-life-time)

다음은 route dampening 에 사용되는 용어를 정리한 표이다.

표 10-4. route dampening 에 사용되는 용어

항목	내용
History state	해당 route 에 대한 best path 를 갖고 있지는 않지만, 여전히 해당 라우트 플래핑에 대한 정보는 존재하는 상태
Damp state	패널티 값이 한계치를 초과 한 상태로 네이버에게 정보 전달이 안된다.
Penalty	라우트 플래핑이 발생시 마다 이 라우트에 부과되는 점수로 디폴트 값이 1000 이다. 이 점수는 누적되고, 한계치(suppress limit)가 초과되면 상태가 'history'에서 'damp' 상태로 변한다
Suppress limit	route 에 부과되는 패널티 값의 한계치로 디폴트 2000 이다
Half-life-time	route 에 부과된 패널티 값은 half-life-time 에 설정된 시간(디폴트 15 분)이 지나면 반으로 줄어드는데, 이러한 감소는 5 초마다 행해진다.
Reuse-limit	플래핑에 부과된 패널티 값이 줄어 들어서 이 값을 밑돌게 되면 무효화된 경로는 복구된다. 해당 라우트가 다시 BGP 테이블에 복구되어 전달되어진다. 디폴트 값은 750 이고, 경로 무효화를 해제하는 절차는 10 초마다 수행된다
Maximum suppress limit	라우트가 무효화될 수 있는 최대 시간이고, 기본 값은 half-lif-time 의 4 배이다.

11 Link Aggregation Control Protocol

이 장에서는 port-group을 구성하기 위해 스위치에 IEEE 802.3ad Link Aggregation Control Protocol(LACP)를 설정하는 방법을 설명한다.

> **Note** 이 장에서 사용되는 명령어에 대한 문법과 사용방법에 관한 정보는 command reference 를 참조하라.

이 장은 다음의 절로 구성된다:

- Understanding the Link Aggregation Control Protocol
- Configuring 802.3ad Link Aggregation Control Protocol
- Displaying 802.3ad Statistics and Status

11.1. Understanding Link Aggregation Control Protocol

이 절에서는 다음 항목을 설명한다:

- LACP Modes
- LACP Parameters

11.1.1. LACP Modes

Premier 8624XG Series switch 는 port group 을 수동으로 구성할 수 있고, IEEE 802.3ad

LACP(Link Aggregation Control Protocol)를 사용하여 자동으로 구성할 수도 있다.

LACP 로 port group 을 구성하려면, active 나 passive 모드를 사용하면 된다. 적어도 링크의 한쪽은 active 모드로 설정되어 있어야 한다. Passive 모드의 포트는 LACP 패킷을 먼저 전송하지 않고 LACP 패킷을 수신했을 경우에 LACP 패킷을 전송하기 시작한다.

LACP 에서 가능한 모드

Mode	Description
off	LACP 에 의해 포트가 포트 그룹으로 구성되지 않도록 한다
passive	포트를 passive 협상 모드로 설정한다. Passive 모드의 포트는 먼저 LACP 패킷을 전송하여 협상을 시작하지 않고, LACP 패킷을 수신했을 때 응답만 한다.
active	포트를 active 협상 모드로 설정한다. Active 모드의 포트는 LACP 패킷을 전송함으로써 협상을 시작한다.

11.1.2. LACP Parameters

LACP 의 설정에 사용되는 인자들은 다음과 같다:

- System Priority
  LACP 가 동작하는 각 스위치에는 자동으로 혹은 CLI 를 통해서 system priority 를 할당해야 한다. System priority 는 스위치의 MAC 주소와 같이 사용되어 system ID 를 구성하고, 다른 시스템과의 협상에 사용된다.

- Port Priority
  스위치의 각 포트에는 자동으로 혹은 CLI 를 통해서 port priority 를 할당해야 한다. Port priority 는 포트 번호와 함께 port identifier 를 구성한다. Port priority 는 하드웨어의 제약 때문에 적합한 모든 포트가 통합될 수 없을 때, standby 모드로 만들 포트를 결정하기 위해 사용된다.

- Administrative key
  스위치의 각 포트에는 자동 혹은 CLI 통해서 administrative key 값을 할당해야 한다. 포트가 다른 포트와 통합될 수 있는 능력은 administrative key 에 의해 정의 된다. 다른 포트와 통합될 수 있는 포트의 능력은 다음의 요소에 의해 결정된다:
  - 전송률(data rate), duplex 모드, point-to-point 혹은 공유 매체와 같은 포트의 물리적 특성
  - 설정 제약

LACP 가 활성화되면, LACP 는 항상 통합 가능한 최대 개수의 포트를 통합하려 시도한다. 만약

통합 가능한 모든 포트들을 통합할 수 없다면, 통합되지 않은 모든 포트들은 hot standby 상태에 놓이게 되며 통합된 다른 포트에 고장이 발생했을 경우에만 사용된다.

11.2. Configuring 802.3ad Link Aggregation Control Protocol

이 절에서는 LACP 로 port group 을 구성하는 방법을 설명한다:

- Specifying the System Priority
- Specifying the Port Priority
- Specifying an Administrative Key Value
- Specifying the Timeout Value
- Changing the LACP Mode
- Clearing LACP Statistics

11.2.1. Specifying the System Priority

System priority 의 값은 1 과 65535 사이의 정수 값이어야 한다. 숫자가 클수록 낮은 우선순위를 나타낸다. default priority 는 32768 이다.

LACP System priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	**Purpose**
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Step2	**lacp system-priority** *priority*	system priority 를 설정한다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show lacp sys-id**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

설정한 system priority 를 default 설정으로 복구하려면 global configuration 명령 **no lacp system-priority** 를 사용하라

다음은 system priority 를 20000 으로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# lacp system-priority 20000
Switch(config)# end
```

11.2.2. Specifying the Port Priority

Port priority 의 값은 1 과 65535 사이의 정수 값이어야 한다. 숫자가 클수록 낮은 우선순위를 나타낸다. default priority 는 32768 이다.

Port priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	LACP 를 port priority 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	**lacp port-priority** *priority*	port priority 를 설정한다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

설정한 port priority 를 default 설정으로 복구하려면 interface configuration 명령 **no lacp port-priority** 를 사용하라

다음은 인터페이스 gi1 의 port-priority 를 10 으로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp port-priority 10
Switch(config)# end
```

11.2.3. Specifying an Administrative Key Value

포트나 시스템의 administrative key 값을 설정할 수 있다. admin-key 값을 설정하지 않는 다면 자동으로 값이 설정된다. 두 경우 모두 유효한 admin-key 값의 범위는 1~1024 이다.

administrative key 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	administrative key 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	**lacp admin-key** *key*	administrative key 를 설정한다.
Step4	**end**	privileged EXEC 모드로 변경한다.

Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

인터페이스에 자동으로 administrative key 값을 할당하려면, interface configuration 명령 **no lacp admin-key** 를 사용하라.

다음은 인터페이스 gi1 의 administrative key 를 10 으로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp admin-key 10
Switch(config)# end
```

11.2.4. Specifying the Timeout Value

포트별로 LACPDU 의 전송 주기를 설정할 수 있다. 전송주기는 short (1 초)나 long (30 초)으로 설정할 수 있다.

Note **lacp timeout** 명령은 설정하는 스위치가 아닌 상대 스위치의 LACPDU 전송 주기에 영향을 미친다.

LACPDU 의 전송 주기를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	**Purpose**
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	LACPDU 전송주기를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	**lacp timeout** {**short**|**long**}	LACPDU 전송주기를 설정한다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

설정한 LACPDU 전송주기를 default 로 복구하려면, interface configuration 명령 **no lacp timeout** 을 사용하라.

다음은 인터페이스 gi1 과 연결된 상태 시스템의 LACPDU 전송주기를 short 로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp timeout short
Switch(config)# end
```

11.2.5. Changing the LACP Mode

인터페이스의 LACP 동작 모드를 설정할 수 있다.

LACP 모드를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	LACP 모드를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	**lacp mode {active|off|passive}**	LACP 모드를 설정한다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

다음은 인터페이스 gi1 의 LACP 를 disable 하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp mode off
Switch(config)# end
```

11.2.6. Clearing LACP Statistics

LACP 의 통계 정보를 삭제하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**clear lacp** [*aggregator-id*] **counters**	해당 port group 의 LACP 통계 정보를 삭제한다.
Stpe2	**show lacp counters**	변경 내용을 확인한다.

다음은 port group 1 의 LACP 를 통계정보를 삭제하는 예이다:

```
Switch# clear lacp 1 counters
```

11.3. Displaying 802.3ad Statistics and Status

모든 포트 그룹에 대한 LACP 통계를 조회하려면, privileged EXEC 명령 **show lacp counters** 를 사용하라.

특정 포트 그룹에 대한 LACP 통계를 조회하려면, privileged EXEC 명령 **show lacp** *aggregator-id* **counters** 를 사용하라.

스위치의 LACP 프로토콜 정보와 상태를 조회하려면, privileged EXEC 명령 **show lacp internal** 을 사용하라. 상대 시스템의 LACP 프로토콜 정보와 상태를 조회하려면, privileged EXEC 명령 **show lacp neighbor** 을 사용하라.

출력 결과물의 항목에 대한 상세정보는 command reference 를 참고하라.

12

통계 모니터링 및 QoS

본 장은 현재 운영중인 Premier 8624XG 스위치의 상태를 파악하고, 로그의 정보를 화면에 표시하고, RMON(Remote Monitoring)을 통한 운영 관리 기능에 대하여 설명한다.

또한 Premier 8624XG 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 한다. 만일 주기적으로 통계 데이터를 관리한다면, 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있다.

12.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. Premier 8624XG 스위치는 `show` 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공한다.

표 12-1. 상태 모니터링 명령어

명령어	설명
`show logging`	■ 시스템이 현재 관리하고 있는 로그를 보여 준다.
`show memory usage`	■ 현재 시스템의 메모리 사용 상태를 보여 준다.
`show cpu usage`	■ 현재 CPU 점유율을 보여 준다.
`show version`	■ 스위치의 H/W 와 S/W 의 버전 정보를 보여 준다.

12.2. 포트 통계

Premier 8624XG 스위치는 포트의 통계 정보를 제공한다. 포트의 통계 정보는 시스템의 현재 운용 중인 모듈의 각 포트의 현재 카운터 값을 보여준다.

포트 통계를 보기 위해서는 다음의 명령을 사용한다.

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

Premier 8624XG 스위치는 운용자에게 다음의 포트 통계 정보를 제공한다.

- **Link Status** – 링크의 현재 상태
- **Received Packet Count (Rx Pkt Count)** – The total number of good packets that have been received by the port.
- **Received Byte Count (Rx Byte Count)** – The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- **Transmit Packet Count (Tx Pkt Count)** – The number of packets that have been successfully transmitted by the port.
- **Transmit Byte Count (Tx Byte Count)** – The total number of data bytes successfully transmitted by the port.
- **Received Broadcast (Rx Bcast)** – The total number of frames received by the port that are addressed to a broadcast address.
- **Received Multicast (Rx Mcast)** – The total number of frames received by the port that are addressed to a multicast address.
- **Transmit Collisions (Tx Coll)** – The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Received Bad CRC Frames (RX CRC)** – The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Oversize)** – The total number of good frames received by the ports that were of greater than the supported maximum length of 1,522 bytes.
- **Receive Dropped Frames (Rx Drop)** – The total number of dropped frames due to lack of system resources.

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

```
Switch # show interface
gi1 is up
 type 1000Base-GBIC,LC, 10,000M, 1,310nm
 gbic inserted
   vendor LUMINENTOIC
   part name SPGBLXCNA
```

```
    Rev A
    SN 5426120096
    Date 061212
  gbic diagnostic not supported
  no auto-negotiation
  speed set 1G, current 1G
  duplex set full, current full
  vlan ingress check enabled

  Last clearing of counters 06:12:47
  1 minutes input rate 85,673,635 bytes/sec, 1,338,650 packets/sec
  1 minutes output rate 42,836,918 bytes/sec, 669,325 packets/sec
    14,836,928,874 packets input, 949,563,504,371 bytes
    Received 3 broadcasts, 5,790,151,331 multicasts
    0 CRC, 0 oversize, 0 dropped
    6,526,551,009 packets output, 417,700,052,349 bytes
    Sent 49 broadcasts, 14,033 multicasts

gi2 is up
  type 1000Base-GBIC,LC, 500M, 850nm
  gbic inserted
    vendor CORETEK
    part name CT-1250NSP-SB1L
    Rev 0000
    SN CF0008FC100017
    Date 061219
  gbic diagnostic not supported
  no auto-negotiation
  speed set 1G, current 1G
  duplex set full, current full
  vlan ingress check enabled

 --More--
```

표 12-2. 포트 통계조회 조회 명령

명령어	설명	모드
show port counter (detail)	시스템의 모든 인터페이스의 In/Out packet 의 누적치를 보여준다.	Privileged
show port counter egress-queue (packet)	시스템의 모든 인터페이스의 Egress Queue 당 pass/drop byte/(packet) count 를 보여준다.	Privileged
show port counter pps	시스템의 모든 인터페이스의 In/Out packet 의 누적치를 pps(packet per second) 단위로 보여준다.	Privileged
show port statistics *IFNAME*	해당 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bit/s, bytes/s, pkts/s 를 보여준다.	Privileged
show port statistics all	모든 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bit/s, bytes/s, pkts/s 를 보여준다.	Privileged
show port statistics avg (all|range|type) (fastethernet|gigabitethernet) *PORTRANGE*	모든/해당 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bits/s, pkts/s 를 보여주면, type 추가시 Unicast/Multicast/Broadcast 의 pkts/s 를 보여준다.	Privileged
show port statistics interface *IFNAME*	해당 인터페이스의 In/Out Octets/UcastPkts/McastPkts BcastPkts/Discards/Errors/PauseFrame 등을 보여준다.	Privileged
show port statistics range (fastethernet|gigabitethernet) *PORTRANGE*	해당 범위의 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bit/s, bytes/s, pkts/s 를 보여준다. IFRANGE : ex) 1/1-2, 1/1-5/2, 1/1,2/1-5/2	Privileged
show port statistics rmon *IFNAME*	해당 인터페이스의 RMON 의 Ether 통계 정보를 보여준다.	Privileged
show port-mib *IFNAME*	해당 인터페이스의 mib 정보에 대해 현재 정보와 누적치를 보여준다.	Privileged

다음은 show port counter 를 이용하여 전체 포트의 패킷 누적치와 특정 인터페이스(gi1)의 5 초, 1 분, 5 분 통계치를 보여준다.

```
Switch # show port counter

ifname      I-Kbps      O-Kbps            InOctets          InPkts           OutOctets         OutPkts
-------------------------------------------------------------------------------------------------------
gi1         685,355     342,678   903,299,486,156  14,114,053,597   394,567,989,806  6,165,113,228
gi2               0           0     3,975,780,187      62,120,332     3,941,783,961     61,589,202
gi3         342,678     685,354   395,100,015,742   6,173,425,595   842,492,363,856  13,163,942,876
gi4               0           0                0               0                0               0
gi5               0           0                0               0                0               0
gi6               0           0                0               0                0               0
gi7               0           0                0               0                0               0
gi8               0           0                0               0                0               0
gi9               0           0                0               0                0               0
gi10              0           0                0               0                0               0
gi11              0           0                0               0                0               0
gi12              0           0                0               0                0               0
gi13              0           0                0               0                0               0
```

gi14	0	0	0	0	0	0
gi15	0	0	0	0	0	0
gi16	0	0	0	0	0	0
gi17	0	0	0	0	0	0
gi18	0	0	0	0	0	0
gi19	0	0	0	0	0	0
gi20	0	0	0	0	0	0
gi21	0	0	0	0	0	0
gi22	0	0	0	0	0	0
gi23	0	0	0	0	0	0
gi24	0	0	0	0	0	0
gi25	0	0	0	0	0	0
gi26	0	0	0	0	0	0

R2# **show port counter pps**

ifname	I-PPS	O-PPS	InPkts	OutPkts
gi1	1,338,628	669,314	14,167,600,498	6,191,886,696
gi2	0	0	62,120,341	61,589,210
gi3	669,314	1,338,628	6,200,199,061	13,217,489,788
gi4	0	0	0	0
gi5	0	0	0	0
gi6	0	0	0	0
gi7	0	0	0	0
gi8	0	0	0	0
gi9	0	0	0	0
gi10	0	0	0	0
gi11	0	0	0	0
gi12	0	0	0	0
gi13	0	0	0	0
gi14	0	0	0	0
gi15	0	0	0	0
gi16	0	0	0	0
gi17	0	0	0	0
gi18	0	0	0	0
gi19	0	0	0	0
gi20	0	0	0	0
gi21	0	0	0	0
gi22	0	0	0	0
gi23	0	0	0	0
gi24	0	0	0	0
gi25	0	0	0	0
gi26	0	0	0	0

Switch # **show port statistics gi1**

Last clearing of counters 06:05:16

```
---------------------------------------------------------------------------
                                     TX |                             RX
                      bits/s       pkts/s |       bits/s          pkts/s
---------------------------------------------------------------------------
 5sec :          342,168,984       668,298     684,337,984       1,336,597
 1min :          342,723,768       669,380     685,446,000       1,338,761
 5min :          342,680,360       669,295     685,359,336       1,338,591
R2#

Switch # show port statistics range gigabitethernet 1-3

---------------------------------------------------------------------------
                                     TX |                             RX
                      bits/s       pkts/s |       bits/s          pkts/s
---------------------------------------------------------------------------
 gi1  ---------------------------------------------------------------------
 5sec :          342,648,776       669,236     685,297,400       1,338,471
 1min :          342,615,352       669,169     685,229,104       1,338,337
 5min :          342,669,056       669,273     685,336,528       1,338,547
 gi2  ---------------------------------------------------------------------
 5sec :                    0             0               0               0
 1min :                   88             0              88               0
 5min :                   96             0              96               0
 gi3  ---------------------------------------------------------------------
 5sec :          685,296,736     1,338,470     342,648,320         669,235
 1min :          685,229,184     1,338,338     342,615,384         669,169
 5min :          685,336,536     1,338,547     342,669,048         669,273
Switch #
```

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

표 12-3. 포트 통계조회 설정 명령

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

Show port traffic-control	PPS 의 현재 상태를 조회한다.	privileged

다음 명령은 통계치에 대한 누적치를 초기화시키는 명령어이다.

표 12-4. 포트 통계 초기화 명령

명령어	설명	모드
clear counters	시스템의 모든 인터페이스의 통계 누적치를 초기화한다.	privileged
clear counters *IFNAME*	특정 인터페이스의 통계 누적치를 초기화한다.	privileged
clear counters snmp	시스템의 모든 인터페이스의 snmp 를 위한 통계 누적치를 초기화한다.	privileged

12.3. Logging

Premier 8624XG 스위치 로그는 모든 환경 설정 정보와 경보 발생 정보를 보여 준다. 시스템 메시지 로깅 소프트웨어는 스위치의 메모리에 로그 메시지를 저장하며, 다른 디바이스로 메시지를 보낼 수 있다. 시스템 메시지 로깅 기능은 다음을 지원한다.

- 사용자에게 수집할 로깅 타입을 선택할 수 있도록 한다.
- 사용자에게 수집한 로깅을 보낼 디바이스를 선택할 수 있도록 한다.

Premier 8624XG 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI 를 사용하여 로깅되는 시스템 메시지를 제어할 수 있다. 시스템 운영자는 시스템 메시지를 Telnet 이나 콘솔을 통해서, 또는 syslog server 의 로그를 봄으로써 원격으로 모니터 할 수 있다.

Premier 8624XG 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

표 12-5. Premier 8624XG 스위치의 로그 레벨

Severity 레벨	설명
Emergencies (0)	시스템 사용 불가.
Alerts (1)	즉각적인 조치가 필요한 상태
Critical (2)	Critical 상태.
Errors (3)	에러 메시지.
Warnings (4)	경고 메시지.
Notifications (5)	정상적인 상태지만 중요한 정보.
Informational (6)	사용자에게 제공하는 정보 메시지.
Debugging (7)	디버깅 메시지.

12.3.1. 시스템 로그 메시지 내용

Premier 8624XG 스위치의 시스템 로그 메시지는 다음과 같은 내용을 제공된다.

- **Timestamp**
  - Timestamp 는 이벤트가 발생한 월, 날짜, 연도 및 구체적인 시간 정보를 Month Day HH:MM:SS 와 같이 기록한다.
- **Severity level**
  - **<오류! 참조 원본을 찾을 수 없습니다.5>**에서 정의한 Premier 8624XG Series 의 로그 메시지의 레벨
  - 0-7 까지의 숫자
- **Log description**
  - 발생한 이벤트에 대한 상세한 정보를 포함하는 텍스트 문자열

다음은 시스템 부팅 시의 로그 메시지 이다.

```
May  6 11:53:48  [5] %REMOTE-CONNECT: login from console as lns
May  6 11:54:01  [5] IFM-NOTICE: Rate limit ra creation
May  7 02:10:24  [5] %REMOTE-CONNECT: login from console as lns
May  7 02:10:40  [5] IFM-NOTICE: Flow xx classified
May  7 02:10:48  [5] IFM-NOTICE: Flow xx match rate 10
May  7 05:17:56  [5] %REMOTE-CONNECT: login from console as lns
May  7 05:23:10  [5] IFM-NOTICE: Service pa add interface gi1
```

12.3.2. 디폴트 Logging 설정 값.

표 12-6. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	enabled
Telnet 세션으로의 로깅 출력	disable.
로깅 버퍼 사이즈	1MB
Time-Stamp 출력	enabled
Logging Server	disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings(4)
콘솔의 Severity	Debuggings(7)
Telnet 의 Severity	info (6)
Flash 로의 로깅 저장	disable

Flash 버퍼 사이즈	25KB

표 12-7. 시스템 메시지 로깅 환경 설정 명령

명령어	설명
`logging console {enable|disable|level}`	■ 콘솔로의 로깅 출력 여부 설정 및 환경 설정.
`logging facility {auth|cron|daemon|kernel|local0| local1|local2local3|local4|local5| local6|local7|lpr|mail|news|syslog| user|uucp}`	■ syslog 메시지를 보낼 Facility parameter 를 설정.
logging flash `{enable|disable|level|size}`	■ syslog 메시지를 flash 에 저장할지 여부 설정 및 환경 설정.
logging server `A.B.C.D`	■ syslog 메시지를 외부 syslog 서버에 보낼지 설정
`logging session {enable|disable|level }`	■ 현 세션으로의 로깅 출력 여부 설정.
logging size BYTE	■ 저장할 syslog 의 size 설정
logging source-ip `A.B.C.D`	■ syslog packet 의 source ip 를 설정
`logging trap {<0-7>|alert|crit|debug|emerg|err| info|notice|warn}`	■ syslog server 의 logging level 설정
`show logging {<0-7>|back|flash }`	■ 로깅 버퍼 출력 및 로깅 설정 확인.

12.3.3. Logging 설정 예.

Console 로 접속한 경우 Log level notice(5) 이하의 log message 만을 console 로 출력하고자 할 때 다음과 같이 설정한다. console 로 log message 출력을 중단하고자 할 경우 “logging console disable” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging console enable
Switch(config)# logging console level notice
Switch(config)#
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# logging console disable
Switch(config)#
```

Telnet 으로 접속한 경우 Log level warn(4) 이하의 log message 만을 telnet session 에 출력하고자 할

때 다음과 같이 설정한다. Telnet session 으로 log message 출력을 중단하고자 할 경우 “logging session disable” command 를 사용한다.

```
Switch#
Switch# configure terminal
Switch(config)# logging session enable
Switch(config)# logging session level warn
Switch(config)#
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# logging session disable
Switch(config)#
```

Log level err(3) 이하의 log message 를 flash 에 저장하고자 할 경우 다음과 같이 설정한다. flash 에 log message 의 저장을 중단하고자 할 경우 “logging flash disable” command 를 사용한다.

```
Switch#
Switch# configure terminal
Switch(config)# logging flash enable
Switch(config)# logging flash level err
Switch(config)#
Switch (config)# end
Switch# configure terminal
Switch(config)# logging flash disable
Switch(config)#
```

Log server 100.10.1.1 에 이 switch 에서 발생하는 log 중 Log level err(5) 이하의 log message 를 보내고자 할 경우 다음과 같이 설정한다. log server 로 log message 보내는 것을 중단하고자 할 경우 “no logging server” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging server 100.10.1.1
Switch(config)# logging trap err 100.10.1.1
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging server 100.10.1.1
Switch(config)#
```

12.4. RMON(Remote MONitoring)

시스템 운영자는 Premier 8624XG 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다.

다음 절에서는 RMON 개념 및 Premier 8624XG 스위치가 지원하는 RMON 서비스 기능에 대하여 자세히 설명한다.

12.4.1. RMON 개요

RMON 은 IETF(Internet Engineering Task Force)의 RFC 1271 와 RFC 1757 에 정의되어 있는 국제 표준 규격으로 시스템 운영자가 네트워크를 원격으로 관리하는 기능을 제공한다. 일반적으로 RMON 은 다음의 두 가지 구성 요소로 구성된다.

- **RMON probe**
  - 원격으로 제어되면서 지속적으로 LAN 세그먼트 또는 VLAN 의 통계 정보를 수집하는 지능형 디바이스 또는 소프트웨어 agent
  - 수집한 정보를 운영자의 요구가 있을 때 또는 미리 정의한 환경에 따라서 자동으로 관리 호스트에게 전송

- **RMON Manager**
  - RMON probe 와 통신하면서 통계 정보를 수집
  - 반드시 RMON probe 와 동일한 네트워크에 있을 필요는 없으며, RMON probe 를 in-band 또는 out-of-band 연결을 통하여 제어

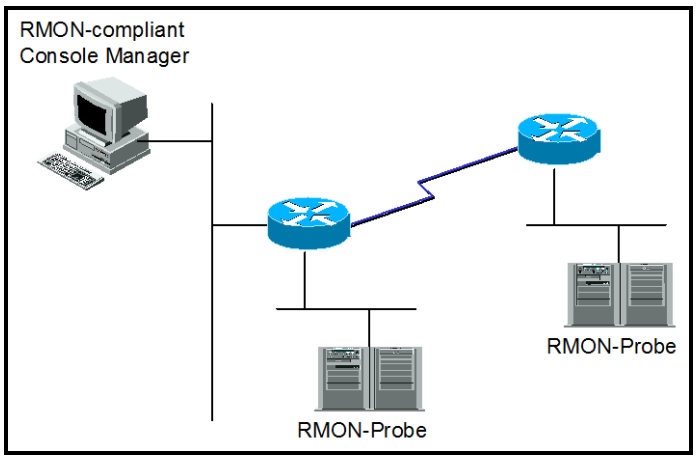


그림 12-1. RMON Manager 와 RMON Probe

기존의 SNMP MIBs 가 SNMP agent 가 탑재된 장비 자체를 관리 대상으로 보고 있는데 반하여 RMON MIBs 는 관리 대상을 장비에 연결된 LAN 세그먼트로 한다. 즉 LAN 세그먼트의 전체 발생 트래픽, 세그먼트에 연결된 각 호스트의 트래픽, 호스트들 사이의 트래픽 발생 현황을 알려준다.

RMON Agent 는 전체 통계 데이터, 이력 데이터, 호스트 관련 데이터, 호스트 매트릭스와 사전에 문제 예측 및 제거를 위해서 특정 패킷을 필터링하는 기능과 임계치를 설정, 이에 도달하면 자동으로 알려주는 경보 기능 및 사건 발생 기능을 보유하고 있어야 한다.

Premier 8624XG 스위치에서는 **<오류! 참조 원본을 찾을 수 없습니다.>**에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON 은 디폴트로 모든 설정이 disabled 이다.

표 12-8. RMON 항목

항목	설명
통계	■ 한 세그먼트에서 발생한 패킷/바이트 수, 브로드캐스트/멀티캐스트 수, 충돌 수 및 패킷 길이별 수 그리고 각종 오류(fragment, CRC Alignment, jabber, 길이 미달, 길이 초과)에 대한 통계를 제공.
이력	■ 관리자가 설정한 시간 간격 내에 발생한 각종 트래픽 및 오류에 대한 정보를 제공 ■ 기본적으로 단기/장기적으로 간격을 설정 가능하고 1-3.600 초를 간격으로 제한 ■ 이 자료를 통해 시간대별 이용 현황 및 다른 세그먼트와 비교 가능
경보	■ 주기적으로 특정한 값을 체크 해 기준치에 도달하면 관리자에 보고하고 대리인이 자신의 기록을 보유 ■ 기준치는 절대값 및 상대값으로 정할 수 있고 계속적인 경보 발생을 막기 위해서 상/하한치를 설정해서 넘나드는 경우에만 경보가 발생.
호스트	■ 세그먼트에 연결된 각 장비가 발생시킨 트래픽, 오류 수를 호스트별로 관리
상위 n 개의 호스트	■ 위 호스트 테이블에 발견될 호스트 중에서 일정시간 동안 가장 많은 트래픽을 발생시킨 호스트 검색 ■ 관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 수집
트래픽 메트릭스	■ 데이터 링크 계층, 즉 MAC 어드레스를 기준으로 두 호스트간에 발생한 트래픽 및 오류에 대한 정보를 수집 ■ 이 정보를 이용해서 특정 호스트에 가장 많은 이용자가 누구인지를 어느 정도는 판별 가능함 ■ 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없음.
필터	■ 관리자가 특정한 패킷의 동향을 감시하기 위해서 이용
패킷 수집	■ 세그먼트에 발생한 패킷을 수집해서 관리자가 분석.
사건	■ 특정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고 메시지를 전송. 트랩 발생 및 기록보관은 선택적임.

12.4.2. RMON 의 Alarm 과 Event 그룹 설정.

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

표 12-9. RMON Alarm and Event 설정 명령

명령어	설명	모드
rmon alarm *index* ifEntry *variable ifIndex interval* {delta|absolute} rising-threshold *value* [*event-number*] falling-threshold *value* [*event-number*] [owner *string*]	■ RMON 의 alarm table 에 alarm 을 추가 ■ *Index*: alarm table 의 유일한 인덱스 ■ *Variable*: alarm variable 을 관찰할 MIB object ■ *IfIndex:* 물리적 인터페이스를 지정 ■ *Interval*: alarm variable 을 관찰한 시간 간격으로 초 단위. ■ Delta: MIB variable 값의 샘플간의 값의 차이를 관찰함. ■ Absolute: MIB variable 의 절대값 ■ Rising-threshold, falling-threshold *value*: alarm 을 발생시킬 설정 값. ■ *Event-number*: alarm variable 의 delta 값이나 absolute 값이 rising-threshold 나, falling threshold 값에 도달했을 때 각각 해당 Event 가 발생. ■ Owner *string*: Alarm 의 owner 를 명시	Config
rmon event *index* [log] [trap *community*] [owner *string*] [description *string*]	■ RMON event table 에 event 를 추가 ■ log: event 가 발생했을 때, RMON log 를 생성할 것인지를 명시. ■ Trap community: event 가 발생했을 때, 설정한 community *string* 과 함께 trap 을 전송하도록 명시. ■ Owner *string*: Event 의 owner 를 명시. ■ Description *string:* Event 에 대한 설명	Config
no rmon alarm *alarm-index*	■ RMON alarm table 에서 alarm 을 삭제	Config
no rmon event *event-index*	■ RMON event table 에서 event 를 삭제.	Config
show rmon alarms	■ RMON alarm table 을 출력.	Privileged
show rmon events	■ RMON event table 을 출력.	Privileged
show rmon log	■ RMON log table 을 출력	Privileged

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

```
         Alarm Configurations
--------------------------------------

The index of alarm    : 10
The interval          : 20
The type of Packets   : inErrors
The interface         : gi1
The type of Sample    : deltaValue
alarmValue            : 0
The status of starting: RISING_FALLING_ALARM
alarmRisingThreshold  : 15
alarmFallingThreshold : 0
alarmRisingEventIndex  : 1
alarmFallingEventIndex : 1
alarmOwner            : hong
Switch# show rmon event
--------------------------------------
         Event Configurations
--------------------------------------

The Index of event : 1
eventDescription   : "Noti:TooMuchInErrors"
eventType          : log and trap
Community          : rmontrap
eventOwner         : hong
```

표 12-10. RMON History 설정 및 statistics 명령

명령어	설명	모드
rmon history *index* ifEntry *ifIndex* [buckets *bucket-number*] [interval *seconds*] [owner *string*]	■ 물리적 인터페이스에 대하여 이력을 수집 ■ *Index*: history table 의 유일한 인덱스, ■ Buckets *bucket-number*: 수집할 이력의 수를 지정 ■ IfEntry *ifIndex*: 물리적 인터페이스를 지정 ■ Interval *seconds*: 이력을 수집할 시간 간격으로 초 단위 ■ Owner *string:* History 의 owner 를 명시.	Config
no rmon history *index* ifEntry *ifindex*	■ History 수집을 Disable 함	Config
show rmon history	■ RMON history table 을 출력.	Privileged
show rmon statistics [*IFNAME*]	■ RMON statistics table 을 출력. ■ *IFNAME:* 특정 인터페이스를 지정	Privileged
show port statistics rmon [IFNAME]	■ RMON statistics table 을 출력.	Privileged

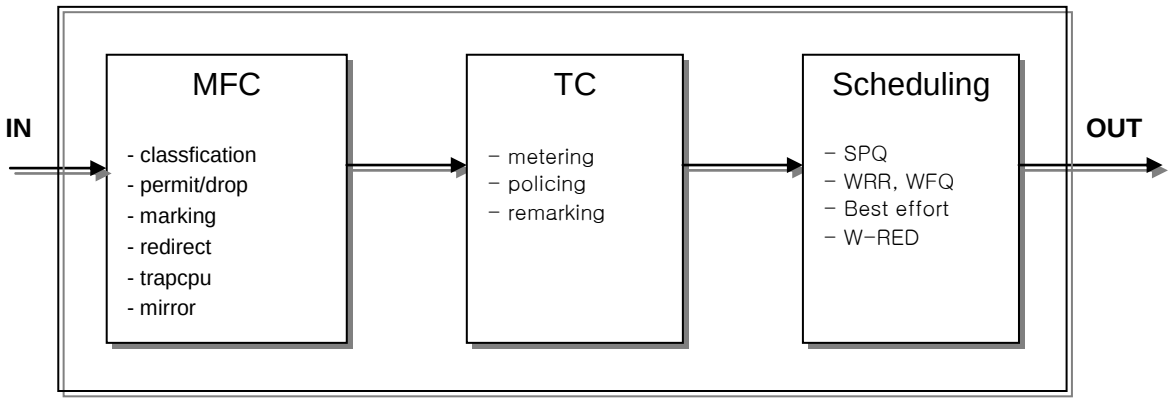
■ *IFNAME:* 특정 인터페이스를 지정

Notice ‘show rmon statistics’ 명령은 ‘show port statistics rmon’명령과 동일한 내용을 출력한다.

```
Switch# configure terminal
Switch(config)# rmon history 1 ifEntry 9 buckets 100 interval 5 owner park
Swtich(config)# end
Switch# show rmon history
-------------------------------------
         SHOW HISTORY
-------------------------------------


====== gi2 ======
Control-index     : 1
ifindex           : 9
interval          : 5
buckets           : 50
owner             : park

--- gi2 : bucket 1 ---
DropEvents        : 0
Octets            : 0
       (생략)
P8624XG_86# show rmon statistics
-------------------------------------
         SHOW STATISTICS
-------------------------------------

The Index of stats   : 1
Interface            : gi1
Drop Events          : 0
Total Octets         : 0
Total Packets        : 0
Broadcast Packets    : 0
Multicast Packets    : 0
CRC errors           : 0
Under Size Packets   : 0
Over Size Packets    : 0
Fragments            : 0
Jabbers              : 0
Collisions           : 0
Pkts 64 Octets       : 0
Pkts 65 to 127 Oct   : 0
Pkts 128 to 255 Oct  : 0
Pkts 256 to 511 Oct  : 0
Pkts 512 to 1023 Oct : 0
Pkts 1024 to 1518 Oct: 0
```

```
Owner                 : ubiquoss
       (생략)
Switch# show rmon statistics gi2
--------------------------------------------------------------------------------
         RMON STATISTICS
--------------------------------------------------------------------------------

The Index of stats    : 3 (gi2)
DropEvents            :               0  Jabbers             :               0
Octets                :               0  Collisions          :               0
Pkts                  :               0  Pkts64Octets        :               5
BroadcastPkts         :               0  Pkts65to127Octets   :           10562
MulticastPkts         :               0  Pkts128to255Octets  :               0
CRCAlignErrors        :               0  Pkts256to511Octets  :               0
UndesizePkts          :               0  Pkts512to1023Octets :               0
OversizePkts          :               0  Pkts1024to1518Octets:               0
Fragments             :               0
--------------------------------------------------------------------------------
```

12.5. QoS 및 Packet Filtering



본 Premier 8624XG 스위치에서는 QoS 와 Packet filtering 을 위해 다음과 같은 기능을 수행을 한다.

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

  프로토콜, src/dest IP, UDP/TCP Port, dscp, Tcp sync 등의 지정된 값에 의해 다양하게 classification 하여 flow-rule 을 결정한 후 permit/drop, redirect, trapcpu, mirror 등의 특정 정책(action)을 수행하거나, QoS 를 위해 특정 필드를 Marking 한다. 또한 이를 이용하여 다양하게 filtering 기능을 수행하는데 이용되기도 한다.

- **TC(Traffic Conditioner)**

특정 Flow-rule 과 Binding 하여 통계치를 내거나, 대역폭을 제한하거나, QoS 필드들을 Remarking 하는데 이용된다. 여러 flow-rule 이 하나의 TC 에 Binding 될 수 있기 때문에 다양하게 통계치를 내거나 대역폭을 제한할 수 있다.

- **Scheduling**

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

- SPQ(Strict Priority Queuing Method)

이 알고리즘은 중요한 데이터를 가장 빨리 처리하려고 할 때 사용된다. 모든 데이터를 우선순위대로 처리하여 우선순위가 높은 데이터를 빨리 처리되지만 우선도가 낮은 데이터는 처리순서가 밀리면서 대역폭이 우선순위 높은 데이터로 채워지면 한번도 나가지 못하고 대기 상태에 놓이는 단점을 지니고 있는 방식이다.

- WRR(Weighted Round Robin Method), WFQ(Weighted Fair Queuing Method)

일정 비율을 기반으로 데이터를 처리하는 방식으로 SPQ 방식의 단점을 보완할 수 있는 알고리즘으로서 큐에 일정한 크기의 대역폭을 할당하는 대신에 일정한 처리 비율을 사용자가 자신의 환경에 맞게 설정할 수 있다.

12.5.1. MFC(Multi-Field Classifier)

12.5.1.1. Flow-Rule 설정/해제

패킷을 처리하는 정책을 설정하기 위해 적용할 대상이 되는 규칙을 설정하여야 하는데 이는 Flow-rule 을 classification 설정으로 가능하다.
Flow-rule 은 프로토콜, src/dest IP, UDP/TCP Port, dscp, Tcp sync 등의 지정된 값에 의해 다양하게 classification 할 수 있다. 또한, 특수 목적의 필터링을 위한 netbios-filter, nbt-filter, dhcp-filter 등의 classification 을 지원하는데 이는 다른 action 을 적용하지 못하며 오직 Filtering(drop)만을 위해 사용된다.

표 12-11. Flow-rule Classification 명령

명령어	설명	모드
flow-rule *NAME* **classify** { *<0-255>* | **icmp | igmp | ip | ospf | pim | tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** }	rule 이 적용된 포트의 특정 프로토콜에 대한 모든 혹은 지정된 src/dest ip 에 대해 적용	Config

flow-rule *NAME* **classify** { *<0-255>* | **icmp | igmp | ip | ospf | pim | tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } **dscp** *VALUE*	flow-rule 이 적용된 포트의 특정 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 지정된 dscp 에 대해 적용	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*}	flow-rule 이 적용된 포트의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 에 대해 적용	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **dscp** *VALUE*	flow-rule 이 적용된 포트의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 와 지정된 dscp 에 대해 적용	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **cos** *VALUE*	flow-rule 이 적용된 포트의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 와 지정된 cos 에 대해 적용	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **tos** *VALUE*	flow-rule 이 적용된 포트의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 와 지정된 tos(ip-precedence)에 대해 적용	Config
flow-rule *NAME* **classify tcp** { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **sync**	flow-rule 이 적용된 포트의 tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 와 sync 에 대해 적용	Config
flow-rule *NAME* **classify** { *H.H.H* | **any** } { *H.H.H* | **any** }	flow-rule 이 적용된 포트의 모든 혹은 지정된 src/dest Mac address 에 대하여 적용	Config
flow-rule *NAME* **classify** { *H.H.H* | **any** } { *H.H.H* | **any** } **cos** *VALUE*	flow-rule 이 적용된 포트의 모든 혹은 지정된 src/dest Mac address 와 지정된 cos 에 대하여 적용	Config
flow-rule *NAME* **classify dhcp-filter**	flow-rule 이 적용된 포트의 dhcp 프로토콜에 대한 필터 적용	Config
flow-rule *NAME* **classify nbt-filter**	flow-rule 이 적용된 포트의 nbt 프로토콜에 대한 필터 적용	Config
flow-rule *NAME* **classify netbios-filter**	flow-rule 이 적용된 포트의 netbios 프로토콜에 대한 필터 적용	Config
flow-rule *NAME* **classify sync**	flow-rule 이 적용된 포트의 tcp sync 에 대해 적용.	Config
flow-rule *NAME* **classify tos** *<0-7>*	flow-rule 이 적용된 포트의 tos 에 대해 적용.	Config
flow-rule *NAME* **classify cos** *<0-7>*	flow-rule 이 적용된 포트의 cos 에 대해 적용.	Config
flow-rule *NAME* **classify dscp** *<0-63>*	flow-rule 이 적용된 포트의 dscp 에 대해 적용	Config

각 조건에 의해 Classification 된 Flow-Rule 에 특정 정책(action)을 적용시킬 수가 있다.
QoS 를 위해 Cos, DP(Drop precedence), Dscp, Tos(Ip Precedence), Queue 필드를 marking 할 수도 있으며, redirect, mirror, trapcpu, rate-limit 등의 정책을 적용할 수도 있다.
또한, TC(Traffic Conditioner)와 binding 하여 QoS 필드의 remark, rate-limit, 통계기능 등을 수행할 수 있다.

Notice dhcp-filter, nbt-filter, netbios-filter 등의 특수 flow-rule 은 다른 정책을 match 시킬 수 없다. 또한 이 flow-rule 은 특정 정책(action)이 match 되지 않으면 아무 의미가 없다.

Notice src/dest Mac address 를 지정하는 flow-rule 에 대해서는 l2-default 의 profile 를 가지는 policy-map 에만 포함된다. 또한 l3 에 관련된 flow-rule 중 cos 를 지정하는 flow-rule 은 l3cos profile 를 가지는 policy-map 에 포함될 수 있다.

표 12-12. Flow-rule 정책 적용 명령

명령어	설명	모드
flow-rule *NAME* **match** { **permit | drop** }	규칙과 일치하는 패킷을 허용 혹은 불허한다.	Config
flow-rule *NAME* **match** { **cos | dropprecedence | dscp | queue-parameter** } *VALUE*	규칙과 일치하는 패킷의 해당값을 지정된 값으로 mark 한다.	Config
flow-rule *NAME* **match mirror**	규칙과 일치하는 패킷의 사본을 mirror 포트로 전송한다.	Config
flow-rule *NAME* **match redirect** VNAME *IFNAME*	규칙과 일치하는 패킷을 지정된 vlan 의 포트로 전송한다.	Config
flow-rule *NAME* **match rate-limit** *<1-100000>*	규칙과 일치하는 패킷을 지정된 속도로 rate-limit 한다.	Config
flow-rule *NAME* **match tc-table** *TBLNAME*	규칙과 일치하는 패킷을 지정된 tc-table 로 바인딩한다.	Config
flow-rule *NAME* **match trapcpu**	규칙과 일치하는 패킷을 CPU 로 전달한다.	Config
flow-rule *NAME* **match trapcpu-high**	규칙과 일치하는 패킷을 CPU 로 들어가는 높은 우선순위 큐에 전달한다	Config
flow-rule *NAME* **match counting**	규칙과 일치하는 패킷을 패킷 통계정보를 계산한다.	Config
flow-rule *NAME* **match nexthop** *A.B.C.D*	규칙과 일치하는 패킷의 nexthop 을 변경한다.	Config
flow-rule *NAME* **match outer-tag-vlan** *<1-4096>*	규칙과 일치하는 패킷의 vlan id 을 변경한다.	Config
flow-rule *NAME* **match queuing-parameter** *<0-7>*	규칙과 일치하는 패킷의 queuing 순서를 변경한다.	Config

Notice marking 을 제외한 정책(action)은 하나의 flow-rule 에 여러 정책이 match 될 수 없다.

특정 Flow-rule 에 적용된 정책을 해제하기 위해서는 다음의 명령어가 사용된다.

표 12-13. Flow-rule 정책 해제 명령

명령어	설명	모드
no flow-rule *NAME* **match** { **permit | drop** }	규칙에 대한 정책을 해지한다.	Config
no flow-rule *NAME* **match** { **cos | droppprecedence | dscp | queue-parameter** }		
no flow-rule *NAME* **match mirror**		
no flow-rule *NAME* **match redirect**		
no flow-rule *NAME* **match rate-limit**		
no flow-rule *NAME* **match tc-table**		
no flow-rule *NAME* **match trapcpu**		
no flow-rule *NAME* **match trapcpu-high**		
no flow-rule *NAME* **match counting**		
no flow-rule *NAME* **match nexthop**		
no flow-rule *NAME* **match outer-tag-vlan**		

다음은 특정 flow-rule 을 삭제하는 명령어이다.

표 12-14. flow-rule 삭제 명령

명령어	설명	모드
no flow-rule *NAME*	NAME 의 flow-rule 을 삭제한다.	Config

12.5.1.2. policy-map 생성/추가

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

표 12-15. Policy-map 생성 및 추가 명령

명령어	설명	모드
policy-map *PNAME* **flow-rule** *FNAME*	PNAME 이 없는 경우는 새로이 생성하고 PNAM 의 policy 가 기존에 있는 경우는 FNAME 의 flow 가 마지막으로 추가된다.	Config
policy-map *PNAME* **flow-rule** *FNAME1* **above flow-rule** *FNAME2*	FNAME1 의 flow 가 FNAME2 의 위로 추가된다.	Config
policy-map *PNAME* **flow-rule** *FNAME1* **below flow-rule** *FNAME2*	FNAME1 의 flow 가 FNAME2 의 아래로 추가된다.	Config

표 12-16. Policy-map 삭제 및 특정 flow-rule 삭제 명령

명령어	설명	모드
no policy-map *PNAME*	PNAME 의 policy-map 을 삭제한다.	Config
no policy-map *PNAME* **flow-rule** *FNAME*	PNAME 의 policy-map 에서 FNAME 의 특정 flow-rule 를 삭제한다.	Config

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

표 12-17. policy-map 적용/해제 명령

명령어	설명	모드
service-policy *PNAME*	특정 vlan 인터페이스에 PNAME 의 policy-map 을 적용한다.	Interface
no service-policy	적용된 policy-map 을 해제한다.	Interface

Notice policy-map 은 vlan 인터페이스에 내려지며 하나의 vlan 인터페이스에는 하나의 policy-map 만이 적용되므로 순서에 주의하면서 다수의 flow-rule 을 적용 가능한 policy-map 을 생성하여야 한다.

다음의 명령을 사용하여 flow-rule 관련 설정을 조회할 수 있다.

표 12-18. Flow-rule 조회 명령

명령어	설명	모드
show flow-rule	flow-rule 의 세부정보 및 policy-map 의 정보를 보여준다.	Privileged
show service-policy	현재 적용되어있는 policy-map 을 vlan 인터페이스와 함께 보여준다.	Privileged

이해를 돕기 위해 다음의 조건을 만족시키기 위한 두 가지 예를 나타내었다.

예 1)

조건 : vlan3
srcip : 210.222.57.0/24 중 텔넷만 허용 후 나머지 drop
netbios filter 설정

```
Switch# configure terminal
Switch(config)# flow-rule telnet23 classify ip 210.222.57.0/24 any
Switch(config)# flow-rule telnet23 match permit
Switch(config)# flow-rule droprule classify ip 210.222.57.0/24 any
Switch(config)# flow-rule droprule match drop
```

```
Switch(config)# flow-rule netbiosfilter classify netbios-filter
Switch(config)#
Switch(config)# policy-map example1 flow-rule telnet23
Switch(config)# policy-map example1 flow-rule droprule
Switch(config)# policy-map example1 flow-rule netbiosfilter
Switch(config)#
Switch(config)# int vlan3
Switch(config-if-vlan3)#
Switch(config-if-vlan3)# service-policy example1
Switch(config-if-vlan3)# end
Switch# show flow-rule

   < flow table >
flow-rule telnet23 classify ip 210.222.57.0/24 any
          telnet23 match permit
flow-rule droprule classify ip 210.222.57.0/24 any
          droprule match drop
flow-rule netbiosfilter classify netbios-filter

   < policy table >
policy-map  example1 flow-rule telnet23
            example1 flow-rule droprule
            example1 flow-rule netbiosfilter

Switch#
Switch# show service-policy
<vlan3>
  service-policy example1
Switch#
```

예 2)

12.5.2. TC(Traffic Conditioner)

앞서 언급한 바, Premier 8624XG 스위치에서는 TC(Traffic Conditioner)를 이용하여 Binding 된 Flow-rule 의 대역폭을 제한하는 기능을 제공할 수 있다.

> **Notice** 다수의 Flow-rule 이 하나의 TC 에 적용될 수 있으나 반대로 하나의 flow-rule 이 다수의 TC 에 binding 되지는 못한다.

12.5.2.1. TC 생성/삭제

표 12-19. Traffic Conditioner 생성 명령

명령어	설명	모드
tc-table *TNAME* **noratelimit**	Ratelimit 를 하지 않는 Traffic-conditioner 를 생성한다.	Config
tc-table *TNAME* <1-999999> { **drop | nodrop** }	특정 ratelimit 위한 Traffic-conditioner 를 생성한다.	Config

> **Notice** drop/nodrop 의 옵션의 경우 DP(Drop Precedence)가 Green, Yellow, Red 의 패킷 중 Red 패킷의 drop 여부를 결정하게 된다.

생성된 TC 를 삭제하기 위해서는 다음의 명령이 사용되며, Flow-rule 이 binding 되어 있는 TC 는 삭제되지 않는다.

표 12-20. Traffic Conditioner 삭제 명령

명령어	설명	모드
no tc-table *TNAME*	특정 Traffic-conditioner 를 삭제한다. 단, binding 된 flow 가 존재할 시에는 삭제되지 않는다.	Config

12.5.2.2. TC 조회

다음의 명령을 통해 생성된 tc-table 과 binding 된 flow-rule 정보를 조회할 수 있다.

표 12-21. Traffic Conditioner Table 조회 명령

명령어	설명	모드
show tc-table	Traffic-conditioner 의 정보 및 binding 되어 있는 flow-rule 을 보여준다.	Privileged

```
Switch(config)# tc-table tc1 1000 drop
Switch(config)# flow-rule fa classify ip 10.1.1.0/24 20.1.1.0/24
Switch(config)# flow-rule fa match tc-table tc1
Switch(config)#
Switch(config)# policy-map ra flow-rule fa
Switch(config)#
Switch(config)# int vlan2
Switch(config-if-vlan2)# service-policy ra
Switch(config-if-vlan2)#
Switch(config-if-vlan2)# end
Switch# sh flow-rule

   < flow table >
flow-rule fa classify ip 10.1.1.0/24 20.1.1.0/24
          fa match tc-table tc1

   < policy table >
policy-map ra flow-rule fa

Switch# sh service-policy
<vlan2>
  service-policy ra
Switch# sh tc-table

   < tc table >
tc-table tc1  1000  nodrop
    flow-rule fa applied
```

12.5.3. QoS 관련 파라메터

다음의 그림은 Premier 8624XG 스위치에서 QoS 를 위해 쓰이는 필드들의 Ethernet Packet 에서의 필드를 나타내고 있다.

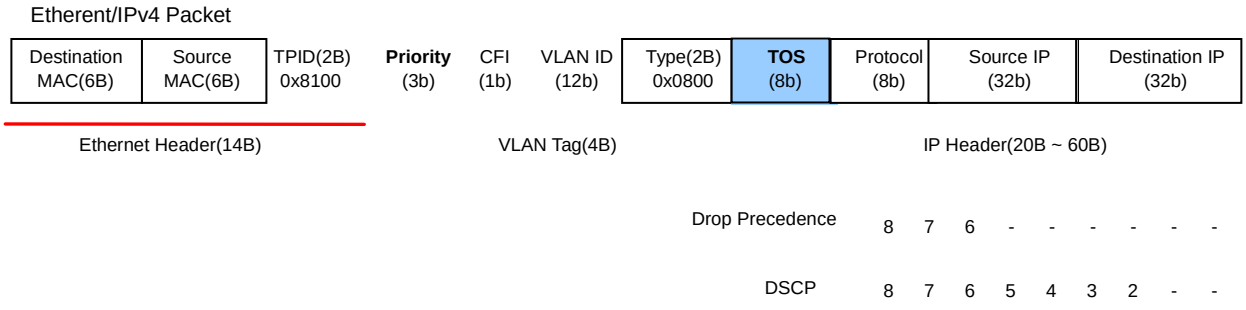


그림 12-2. QoS 관련 파라메터 필드

QoS 를 위해 다음의 필드들을 marking/remarking 을 하게 되는데 주로 marking 은 MFC 나 L2 레벨에서 강제로 특정 필드로 조건에 의해 변경하는 것을 말하며, remarking 은 TC 를 거치며 해당 필드를 다시 변경해 주는 것을 의미한다. 다음은 그 기준이 테이블을 조회하는 명령어들이다.

12.5.3.1. QoS 관련 파라미터 조회

표 12-22. QoS 테이블 조회명령

명령어	설명	모드
Show Qos cos	규칙에 적용된 패킷의 cos 값에 의해 mapping/remaking 테이블을 보여준다.	Privileged

12.5.3.2. QoS 관련 파라미터 변경

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

표 12-23. QoS 관련 Marking/Remarking 테이블 셋팅 명령

명령어	설명	모드

Qos cos-queue-map *<0-7> <0-7>*	규칙에 적용된 패킷의 cos 값에 의해 mapping 될 새로운 queue 값을 설정한다. 이는 **show QoS cos** 로 확인 가능하다.	Config

12.5.4. Scheduling

Premier 8624XG 스위치에서는 Scheduling 을 위해 SPQ(Strict Priority Queue) Method 와 WRR(Weighted Round Robin) Method 를 제공하며 디폴트는 SPQ 이다.
다음 그림은 SPQ 와 WRR 의 차이점을 나타내고 있다.

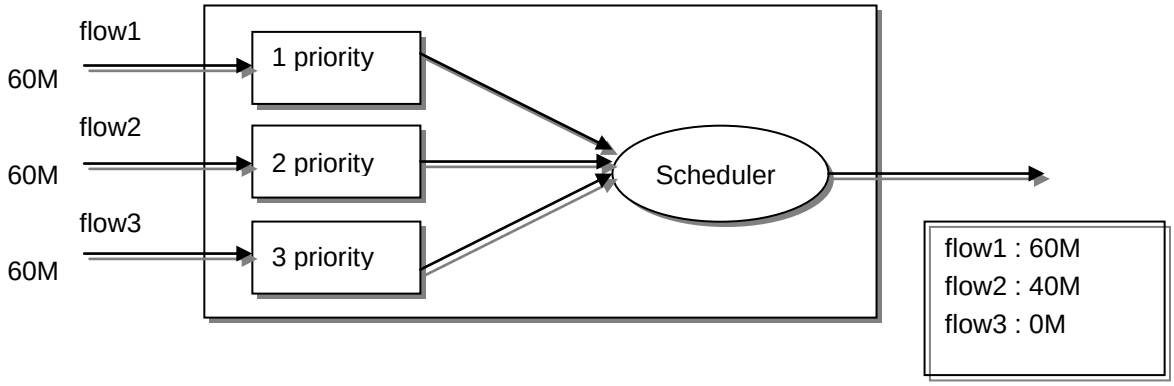


그림 12-3. SPQ(Strict Priority Queue) Method

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

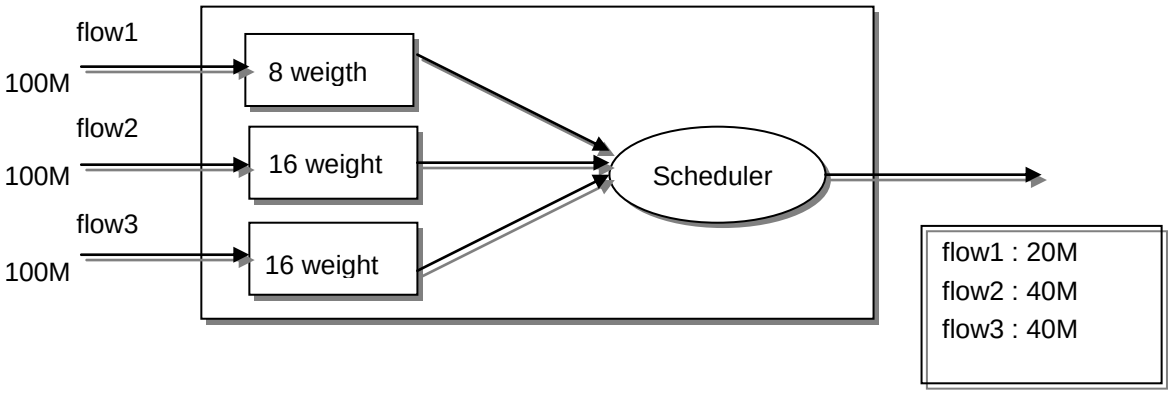


그림 12-4. WRR(Weighted Round Robin) Method

위의 그림은 WRR(Weighted Round Robin) Method 의 예인데 SPQ 와 달리 포트에 설정된 weight 에 비율만큼 내보내게 된다.
Premier 8624XG 스위치의 경우, 0-7 의 8 개의 profile 을 제공하며, 각 profile 에 0-7 의 8 개의

scheduling 을 위한 Queue 를 제공한다. 다음은 특정 인터페이스의 Queue 방식을 결정하는 명령어이다.

표 12-24. Queue-method 변경 명령

명령어	설명	모드
tx-scheduling-profile *profile-id* **queueing-method** *queue-id* **(strict|wrr1|wrr2)**	*profile-id*(1~7) Profile 의 *queue-id*(0~7) Queue Queue-method 를 Strict 방식 혹은 WRR1(Weight-Round-Robin)방식 혹은 WRR2 으로 변경한다. Default 모드는 Strict 방식이다.	Config

Notice SPQ 에서의 우선순위는 8 개(0-7) Queue 중 숫자가 클수록 우선순위가 높다.

다음은 해당 profile 이 WRR1(Weighted Round Robin) 또는 WRR2 Method 로 설정되었을 경우에 해당 Queue 에 Weight 를 변경해 주는 명령어이다.

표 12-25. WRR-method Queue weight 변경 명령

명령어	설명	모드
tx-scheduling-profile *profile-id* **wrr-profile** *queue-id weitht*	*profile-id*(1~7) Profile 의 *queue-id*(0~7) Queue WRR Weight 를 *weight* 로 변경한다. 변경 후 이는 **show port Qos** 명령으로 확인 가능하다. default WRR Weight 값은 8 이다.	Config
no tx-scheduling-profile *profile-id* **wrr-profile** *queue-id*	*profile-id*(1~7) Profile 의 *queue-id*(0~7) Queue WRR Weight 를 default weight 인 8 로 변경한다.	Config

다음은 해당 포트에 적용할 profile 를 지정하고 해제하는 명령어이다.

표 12-26. tx-scheduling 변경 명령

명령어	설명	모드
tx-scheduling *profile-id*	해당 포트에 적용될 profile 을 *profile-id* 로 설정한다. 디폴트 profile-id 는 0 이다.	Interface
no tx-scheduling *profile-id*	*profile-id*(1~7) Profile 의 *queue-id*(0~7) Queue WRR Weight 를 default weight 인 8 로 변경한다..	Interface

다음은 각 포트의 scheduling 관련 상태를 한눈에 알 수 있게 하여 준다.

표 12-27. 전체 interface 의 queue-method 및 weight 조회명령

명령어	설명	모드

show port qos	시스템의 모든 인터페이스의 queue-method 및 WRR 방식인 경우의 weight 값을 보여준다.	Privileged

다음은 WRR 의 그림에서 input 포트를 gi1, gi2, gi3 으로 가정하고 output 포트를 gi4 로 가정할 경우에 그림과 같은 결과를 얻기 위한 과정을 예로 설명하였다. 0-7 의 8 개의 queue 중 1, 2, 3 Queue 를 사용한 경우이다. 여기서 port-priority 명령은 해당 Queue 로 marking 하는 명령어이다.

```
Switch(config)# tx-scheduling-profile 1 queueing-method 1 wrr1
Switch(config)# tx-scheduling-profile 1 queueing-method 2 wrr1
Switch(config)# tx-scheduling-profile 1 queueing-method 3 wrr1
Switch(config)# tx-scheduling-profile 1 wrr-profile 1 8
Switch(config)# tx-scheduling-profile 1 wrr-profile 2 16
Switch(config)# tx-scheduling-profile 1 wrr-profile 3 16
Switch(config)# int gi4
Switch(config-if-gi4)# tx- scheduling 1
Switch(config-if-gi4)# int gi1
Switch(config-if-gi1)# port-priority 1
Switch(config-if-gi1)# int gi2
Switch(config-if-gi2)# port-priority 2
Switch(config-if-gi2)# int gi3
Switch(config-if-gi3)# port-priority 3
Switch(config-if-gi3)# end
Switch# show port qos
 IFNAME   Pri   Q0     Q1     Q2     Q3     Q4     Q5     Q6     Q7
-------------------------------------------------------------------------------
 gi1      P-1 st-    st-    st-    st-    st-    st-    st-    st-
 gi2      P-2 st-    st-    st-    st-    st-    st-    st-    st-
 gi3      P-3 st-    st-    st-    st-    st-    st-    st-    st-
 gi4       .  st-    w1-  8 w1- 16 w1- 16 st-    st-    st-    st-
 gi5       .  st-    st-    st-    st-    st-    st-    st-    st-
 gi6       .  st-    st-    st-    st-    st-    st-    st-    st-
 gi7       .  st-    st-    st-    st-    st-    st-    st-    st-
 gi8       .  st-    st-    st-    st-    st-    st-    st-    st-
 gi9       .  st-    st-    st-    st-    st-    st-    st-    st-
 gi10      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi11      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi12      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi13      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi14      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi15      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi16      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi17      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi18      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi19      .  st-    st-    st-    st-    st-    st-    st-    st-
 gi20      .  st-    st-    st-    st-    st-    st-    st-    st-
```

```
  gi21      .  st-    st-    st-    st-    st-    st-    st-    st-
  gi22      .  st-    st-    st-    st-    st-    st-    st-    st-
  gi23      .  st-    st-    st-    st-    st-    st-    st-    st-
  gi24      .  st-    st-    st-    st-    st-    st-    st-    st-
  gi25      .  st-    st-    st-    st-    st-    st-    st-    st-
  gi26      .  st-    st-    st-    st-    st-    st-    st-    st-
Switch#
```

12.5.5. CPU Rate-limit

Premier 8624XG Series 스위치에서는 시스템 전체에 대한 cpu rate limit 를 적용할 수 있다. No cpu rate limit 로서 Default 값을 적용시킬 수 있다

표 12-28. CPU Rate-limit 관련 명령

명령어	설명	모드
rate-limit cpu <1-999999>	CPU Rate limit 값을 설정한다<Kbps>.	Config
no rate-limit cpu	CPU Rate limit 값을 Default 로 설정한다 <2048Kbps>.	Config
show rate-limit cpu	설정된 Rate limit 값을 보여 준다.	Privileged

12.5.6. 기타 filtering

Source-ip, Ipx-netbios 필터링을 위해 해당 인터페이스에 다음과 같은 명령어를 사용하여 적용할 수 있다.

표 12-29. 기타 Filtering 관련 명령

명령어	설명	모드
source-ip-filter	특정 인터페이스에 source-ip Filtering 을 설정한다.	Interface
no source-ip-filter	특정 인터페이스에 source-ip Filtering 을 해제한다.	Interface
ipx_netbios	특정 인터페이스에 Ipx_netbios Filtering 을 설정한다.	Interface
no ipx_netbios	특정 인터페이스에 Ipx_netbios Filtering 을 해제한다.	Interface

12.6. sFlow

본 Premier 8624XG 스위치에서는 각 interface 의 Traffic flow 별 모니터링과 statistics 에 대한 정보를 수집하기 위해 sFlow 를 지원한다. Premier 8624XG Series 에서 sFlow 를 지원하는 interface 의 범위는 physical port 에 한한다. sFlow 는 switch 또는 router 에 있는 상태 및 통계 정보를 수집해 주는

sFlow agent 와 이 정보를 sorting 하여 운영자에게 보여주는 sFlow collector 가 있다. 아래는 sFlow 개념에 대해 설명한 그림이다.

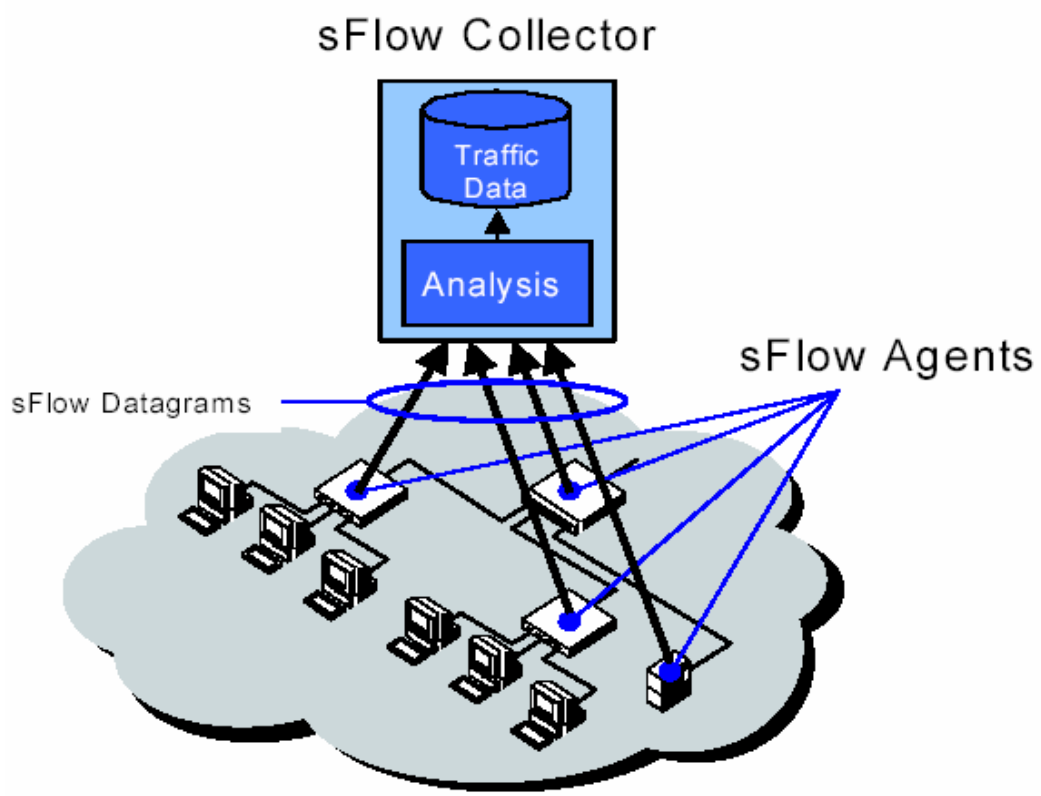


그림 12-5. sFlow 개념도(sFlow agent 와 collector)

12.6.1. sFlow agent

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

표 12-30. sFlow 관련 명령어

명령어	설명	모드
show sflow	sflow 설정과 관련된 명령어를 보여준다	Privileged
service sflow	sampling 이 enable 된 interface 의 flow sampling 및 statistics sampling 을 시작하게 된다. Disable 은 no 형태를 취한다.	Config
sflow forwarding	해당 interface 를 통과하는 패킷에 대해서 sampling 을 할 것인지 설정한다. Disable 은 no 형태를 취한다.	Interface
sflow sample *<10-65530>*	Interface 를 통과하는 패킷 중 몇 패킷마다 을 sampling 을 취할지를 설정한다. no 형태로 Default 값을 취한다.	Interfac, Config
sflow polling-interval *<20-120>*	몇 초마다 statistics sample 을 sampling 할지 결정한다.	Config
sflow agent *A.B.C.D*	sflow agent 의 ip address 를 설정한다. No 형태로 Default 값을 취한다	Config
sflow destination *A.B.C.D*	sflow collector 의 ip address 를 설정한다. No 형태로 Default 값을 취한다	Config

12.6.2. sFlow collector

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

12.6.2.1. sflowtool 설정

1) port 6343으로 수신된 sFlow sampling packet을 출력한다.

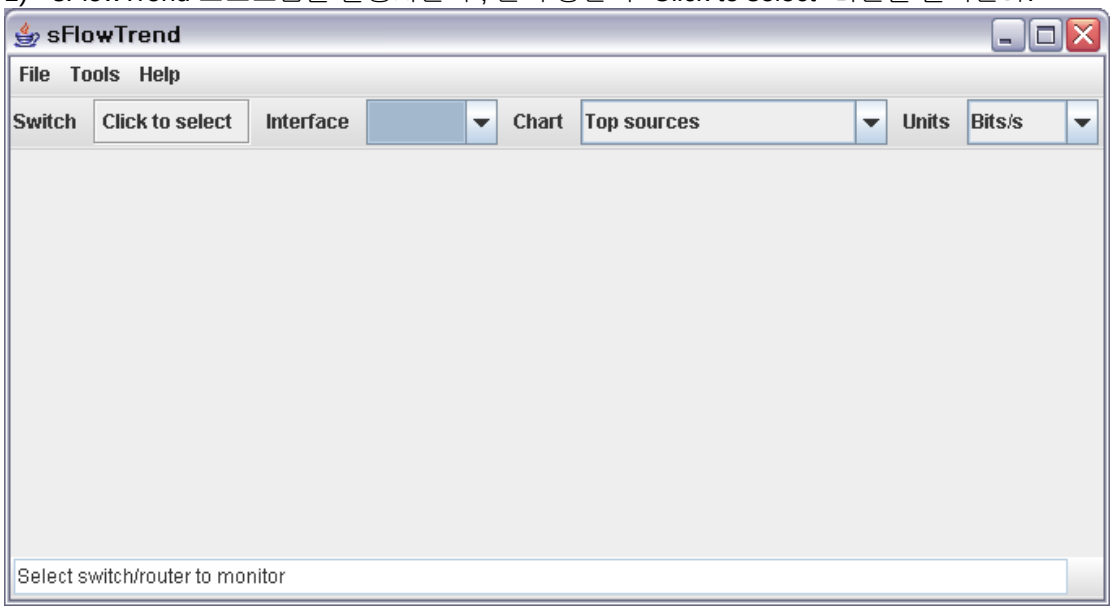
```
[lns:/home/lns] sflowtool -p 6343
startDatagram =================================
datagramSourceIP 192.168.0.212
datagramSize 144
unixSecondsUTC 1136381882
datagramVersion 5
agentSubId 0
agent 192.168.0.212
```

packetSequenceNo 9512
sysUpTime 190157000
samplesInPacket 1
startSample ----------
sampleType_tag 0:2
sampleType COUNTERSSAMPLE
. . . . . .
endSample ----------
endDatagram ==========

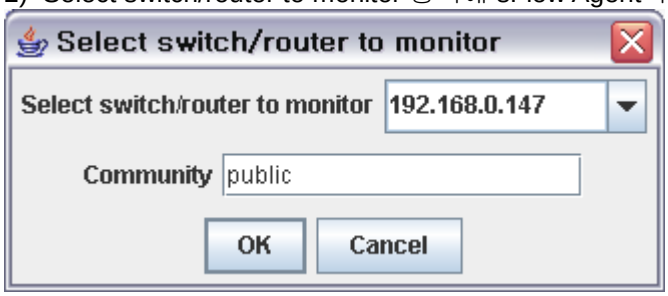
2) sFlow sampling packet을 line 단위로 출력한다.
[lns:/home/lns] **sflowtool -l**
CNTR,10.0.0.254,17,6,100000000,0,2147483648,175283006,136405187,2578019,297011,0,3,0,0,0,0,0
,0,0,1
FLOW,10.0.0.254,0,0,00902773db08,001083265e00,0x0800,0,0,10.0.0.1,10.0.0.254,17,0x00,64,3569
0,161,0x00,143,125,80

12.6.2.2. sFlowTrend 설정

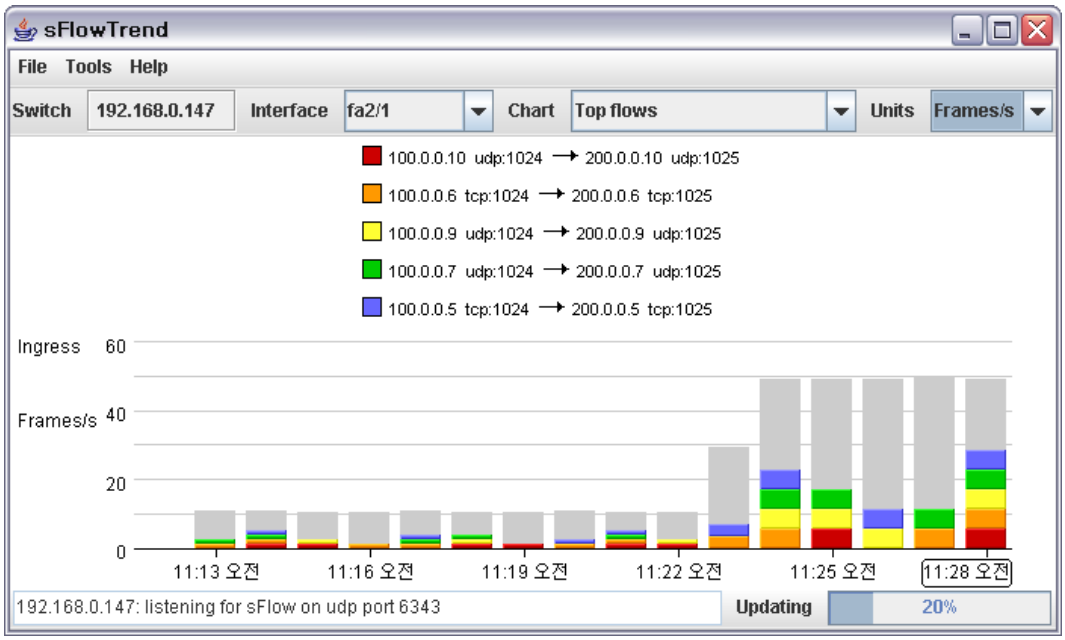
1) sFlowTrend 프로그램을 실행시킨 후, 왼쪽 상단의 “Click to select” 버튼을 클릭한다.



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



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



12.6.3. sFlow Network 구성

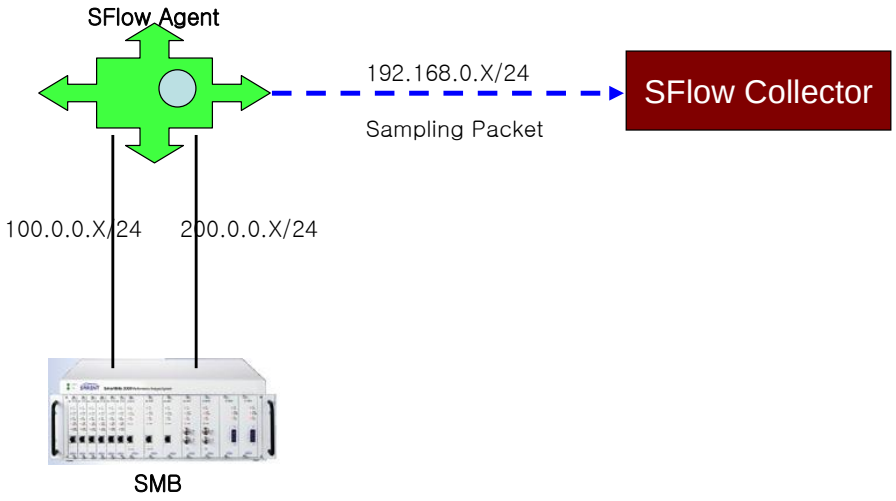


그림 **12-6. sFlow** 를 설정한 네트워크 예제 설정 및 구성도

12.6.3.1. sFlow sampling 시험

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

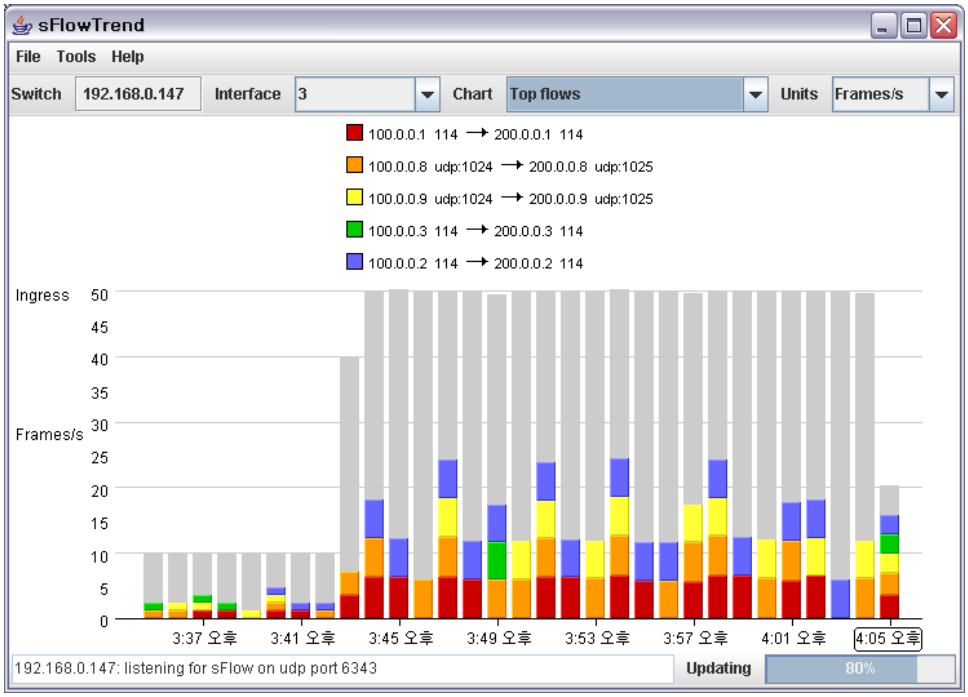
1. SMB 를 사용하여 다양한 flow(TCP, UDP, IP, 여러개의 IP Address)별 트래픽을 생성하여, Sflow Agent 에게 송신한다.

2. Sflow Agent 에서 SMB 와 연결된 포트의 트래픽을 샘플링하고, 이 트래픽을 SFlow Collector 에게 전송하기 위하여 SFlow Collector 와 SFlow Agent 의 IP Address 를 설정한다. SFlow Service 를 활성화 시킨다.

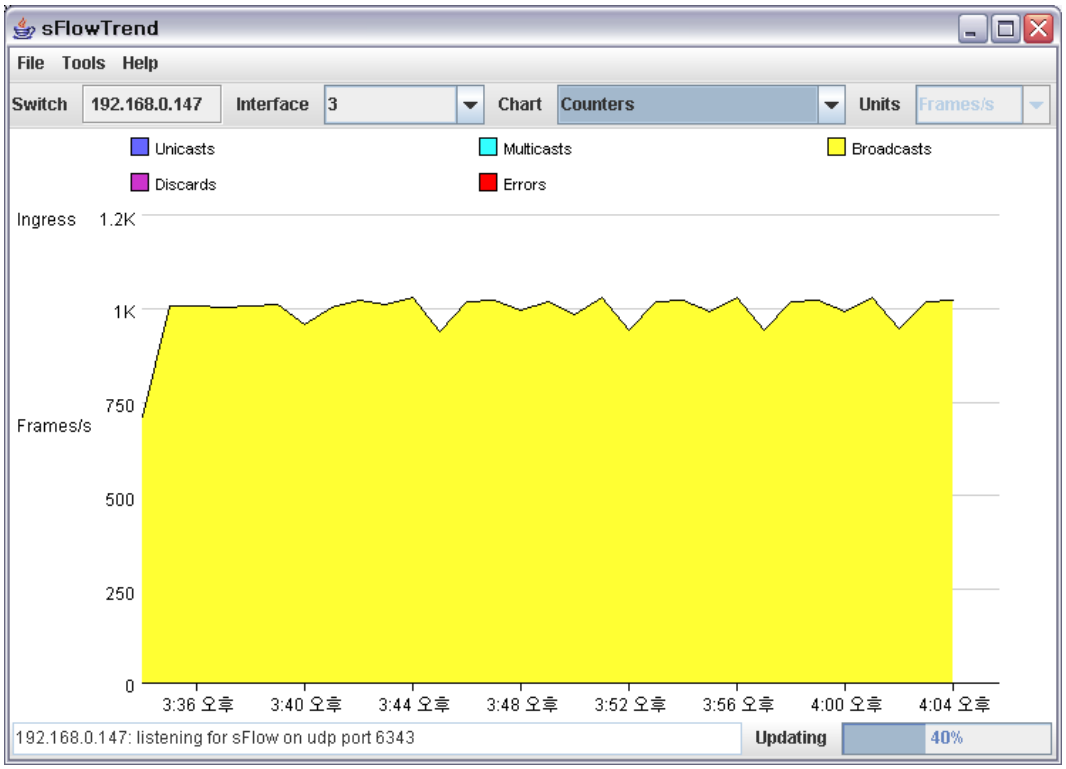
```
Switch(config)# interface gi1
  Switch(config-if-gi1)# sflow forwarding
 Switch(config-if-gi1)# exit
  Switch(config)# sflow agent 192.168.0.147
  Switch(config)# sflow destination 192.168.0.200
  Switch(config)# service sflow
```

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

4.



※ Traffic flow sampling



※ Interface statistics sampling

12.7. 임계치 설정

Premier 8624XG 스위치에는 임계치(threshold)를 설정하고 이를 초과하면 이를 log 에 저장하고 운용자에게 이를 알리는 기능이 있다.

12.7.1. 온도 설정

다음은 온도에 대한 임계치를 설정, 조회하는 명령어이며, FAN 의 경우 온도의 low-threshold 임계치 이하로 떨어지면 FAN 을 off 하는 기능을 가진다.

표 12-31. 온도설정 관련 명령어

명령어	설명	모드
`temperature threshold` *`HIGHVAL LOWVAL`*	온도의 임계치를 설정하는 명령어로 임계치를 초과하면 syslog 와 snmp trap 을 발생한다.	config

`temperature fan-check-time <0-9999>`	주기적으로 fan 을 체크하여 fan fail 일 시에 이를 알리고 fan “ON”을 2 회 시도한다. Default 60 분이며 0 으로 셋팅시 위의 동작을 시도하지 않는다. 단위는 분이다..	config
`show temperature`	현재의 온도와 임계치를 조회하며 FAN 을 지원하는 모델의 경우 FAN 의 상태도 조회가능하다.	Privileged

12.7.2. Mac count 설정

장비에 등록되어 있는 Mac count 에 대한 임계치를 설정하고, 임계치 초과시 syslog 로 이를 알린다.

표 12-32. mac threshold 관련 명령어

명령어	설명	모드
`mac-threshold <1- 32768>`	Mac count 의 임계치를 설정하는 명령어로 임계치를 초과하면 syslog 를 발생한다.	config
`show mac-threshold`	현재의 mac-count 의 총 합과 threshold 를 조회한다.	Privileged

12.7.3. Cpu usage 설정

장비에 cpu usage 사용율에 대한 임계치를 설정하고, 임계치 초과시 syslog 와 snmp trap 으로 이를 알린다.

표 12-33. cpu usage threshold 관련 명령어

명령어	설명	모드
`cpu usage low-threshold <30-100> high-threshold <40-100>`	Cpu usage 의 임계치를 설정하는 명령어로 임계치를 초과하면 syslog 와 snmp trap 을 발생한다.	config
`show cpu usage`	현재의 cpu usage 를 조회한다.	Privileged

12.7.4. User Priority 설정

장비에서 생성된 패킷의 User Priority(802.1P) 값을 임의로 설정(Marking)하는 기능이다.

표 12-34. user priority 관련 명령어

명령어	설명	모드
`user-priority <0-7>`	장비에서 생성된 패킷의 user-priority 값을 설정(Marking)한다. 디폴트값은 7 이다.	Interface
`no user-priority`	user-priority 값을 디폴트값으로 설정한다.	Interface

13

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

이 장에서는 Spanning Tree Protocol(STP)과 Rapid Spanning Tree Protocol(RSTP)를 설정하는 방법에 대해 설명한다.

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

이 장은 다음의 절들로 구성된다:

- Understanding Spanning-Tree Features
- Understanding RSTP
- Configuring Spanning-Tree Features
- Displaying the Spanning-Tree Status

13.1. Understanding Spanning-Tree Features

이 절에서는 다음의 STP 기능에 대해 설명한다:

- STP Overview
- Supported Spanning-Tree Instances
- Bridge Protocol Data Units
- Election of the Root Switch
- Bridge ID, Switch Priority, and Extended System ID
- Spanning-Tree Timers
- Creating the Spanning-Tree Topology
- Spanning-Tree Interface States
- STP and IEEE 802.1Q Trunks

13.1.1. STP Overview

STP 는 네트워크에서 루프를 방지하고 경로의 이중화를 제공하는 Layer 2 링크 관리 프로토콜이다. Layer 2 이더넷(Ethernet) 네트워크가 정상적으로 동작하려면, 임의의 두 단말 사이에는 오직 하나의 활성 경로만 존재해야 한다. Spanning-tree 의 동작은 종단 단말(end station)들에 대해 투명하기 때문에, 종단 단말들은 단일 LAN 에 연결되었는지 여러 개의 조각으로 구성된 switched LAN 에 연결되었는지 감지할 수 없다.

고장에 견고한 네트워크 형상을 구성하려면, 네트워크의 모든 노드들 사이에는 루프가 없어야 한다. Spanning-tree 알고리즘은 switched Layer 2 네트워크를 통해 루프가 없는 최적의 경로를 계산한다. 스위치는 주기적으로 bridge protocol data unit(BPDU)라 불리는 spanning-tree 프레임을 송수신한다. 스위치는 이 프레임들을 forward 하지 않고, 루프가 없는 경로를 생성하기 위해 사용한다.

두 종단 단말 사이에 여러 개의 활성화된 경로가 존재하면 네트워크에 루프가 발생한다. 네트워크에 루프가 존재한다면 종단 단말은 중복된 프레임을 수신할 것이다. 스위치에서는 한 종단 단말의 MAC 주소가 여러 개의 Layer 2 인터페이스에 등록된다. 이런 상황은 네트워크를 불안정하게 만든다.

Spanning tree 는 Layer 2 네트워크에서 root 스위치와 root 스위치로부터 모든 스위치까지 루프가 없는 경로를 가진 tree 를 정의한다. Spanning tree 는 중복된 데이터 경로를 standby(blocked) 상태로 만든다. 중복된 경로가 존재하는 네트워크에 고장이 발생하면, spanning-tree 알고리즘은 spanning-tree 형상을 새로 계산하고 standby 경로를 활성화시킨다.

스위치의 두 인터페이스가 루프의 일부라면, spanning-tree port priority 와 path cost 설정이 인터페이스의 forwarding 상태와 blocking 상태를 결정한다. port priority 값은 네트워크에서 인터페이스의 위치와 트래픽을 위해 얼마나 잘 위치하고 있는가를 나타낸다. path cost 값은 매체의 속도를 나타낸다.

13.1.2. Supported Spanning-Tree Instances

Premier 8624XG 스위치는 VLAN 별 spanning tree 와 최대 128 개의 spanning-tree instance 를 지원한다. 128 개의 VLAN 에 대해 독립적으로 spanning-tree 를 활성화 할 수 있다.

13.1.3. Bridge Protocol Data Units

다음의 요소들에 의해 spanning-tree 의 안정된 active 형상이 결정된다:

- 각 VLAN과 연관된 유일한 BridgeID(스위치 priority와 MAC 주소)
- root 스위치로의 spanning-tree path cost

- 각 Layer 2 인터페이스에 할당된 포트 식별자(포트 priority와 포트 번호)

스위치에 전원이 들어왔을 때, 스위치는 root 스위치처럼 동작한다. 각 스위치는 자신의 모든 포트로 configuration BPDU 를 전송한다. 스위치들은 BPDU 를 서로 교환하고 BPDU 로 spanning-tree 형상을 계산한다. 각 configuration BPDU 는 다음의 정보를 포함한다:

- root 스위치의 BridgeID
- root 까지의 spanning-tree path cost
- BPDU를 전송하는 스위치의 BridgeID
- Message age
- BPDU를 전송하는 스위치의 인터페이스 식별자
- hello, forward-delay, max-age 프로토콜 타이머의 값

스위치가 자신보다 우월한 정보(낮은 BridgeID, 낮은 path cost, 등등)를 가진 BPDU 를 수신했을 경우, 그 정보를 BPDU 를 수신한 포트에 저장한다. BPDU 를 수신한 포트가 root 포트라면, 스위치는 메시지를 갱신해서 자신의 designated LAN 으로 전달한다.

스위치가 현재 포트의 정보보다 열등한 정보를 포함한 BPDU 를 수신하면 그 BPDU 를 버린다. 스위치가 designated LAN 으로부터 열등한 메시지를 수신했다면, 포트에 저장된 정보로 갱신된 BPDU 를 LAN 으로 전송한다. 이런 방식으로 열등한 정보는 버려지고 우월한 정보가 네트워크에 전파된다.

다음은 BPDU 교환으로 인한 결과이다:

- 네트워크의 한 스위치가 root 스위치로 선택된다.
- Root 스위치를 제외한 각 스위치에서 root 포트가 선택된다. 이 포트는 스위치가 root 스위치로 패킷을 전송할 때 최적의 경로(가장 낮은 비용)를 제공한다.
- 각 스위치는 path cost를 기반으로 root 스위치까지의 최단 거리를 계산한다.
- 각각의 LAN을 위한 designated 스위치가 결정된다. designated 스위치는 LAN에서 root 스위치로 패킷을 전달할 때 가장 낮은 path cost를 제공한다. LAN과 연결된 designated 스위치의 포트를 designated 포트라 부른다.
- Spanning-tree 에 포함되는 인터페이스들이 결정된다. root 포트와 designated 포트는 forwarding 상태에 놓인다.
- Spanning-tree에 포함되지 않는 모든 인터페이스들은 blocked 된다.

13.1.4. Election of Root Switch

Layer 2 네트워크의 spanning tree 에 참여하는 모든 스위치는 BPDU 의 교환을 통해 다른 스위치들에 관한 정보를 모은다. 이러한 메시지의 교환은 다음의 행위를 야기한다:

- 각 spanning-tree instance에 대한 유일한 root 스위치 선출
- 모든 switched LAN 조각을 위한 designated 포트 결정
- 중복된 링크로 연결된 Layer 2 인터페이스의 차단에 의한 switched 네트워크의 루프 제거

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

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

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

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

13.1.5. Bridge ID, Switch Priority, and Extended System ID

IEEE 802.1D 표준에 따르면 각 스위치는 root 스위치를 선택하기 위해 사용되는 유일한 브리지 식별자(BridgeID)를 가진다. 각 VLAN 은 논리적으로 서로 다른 브리지로 간주되므로 스위치는 VLAN 별로 서로 다른 BridgeID 를 가질 수 있다. 스위치는 8 바이트의 BridgeID 를 가진다; 최상위 2 바이트는 스위치 priority 로 사용되고, 나머지 6 바이트는 스위치의 MAC 주소이다.

Premier 8624XG 스위치는 802.1T spanning-tree extensions 를 지원한다. 표와 같이 스위치 priority 로 사용되던 2 바이트가 4 비트 priority 값과 VLAN ID 와 동일한 12 비트 extended system ID 값으로 재할당 되었다.

표 13-1. Switch Priority Value and Extended System ID

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

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

13.1.6. Spanning-Tree Timers

표는 spanning-tree 의 성능에 영향을 미치는 타이머들을 나타낸다.

표 13-2. Spanning-Tree Timers

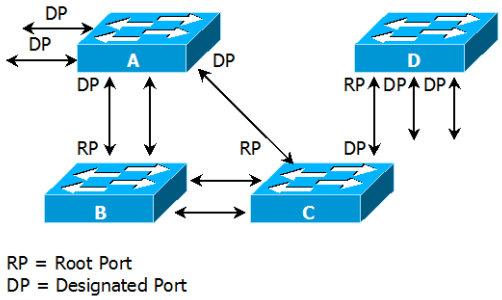
Variable	Description
Hello timer	스위치가 다른 스위치로 얼마나 자주 hello 메시지를 전송할 것인가를 결정한다.

Forward-delay timer	인터페이스가 forwarding 상태가 되기 전에 listening 과 learning 상태에서 각각 얼마나 머물 것인가를 결정한다.
Maximum-age timer	인터페이스로 수신한 프로토콜 정보를 얼마 동안 저장할 것인가를 결정한다.

13.1.7. Creating the Spanning-Tree Topology

그림에서 모든 스위치들의 스위치 priority 가 default(32768)이고 스위치 A 가 가장 낮은 MAC 주소를 가진다고 가정하면 스위치 A 가 root 스위치가 된다. 하지만, forwarding 인터페이스의 개수 혹은 link-type 때문에 스위치 A 는 이상적인 root 스위치가 아니다. Root 스위치로 만들려는 스위치의 priority 를 증가시킴으로써(낮은 숫자 값을 사용), spanning-tree 의 형상을 재계산하여 이상적인 스위치를 root 로 만들 수 있다.

그림 13-1 Spanning-Tree Topology



default 인자를 기반으로 spanning-tree 형상을 계산하면, 시작 단말과 목적지 단말 사이의 경로는 이상적이지 않다. 예로, root 포트보다 높은 포트 번호를 가진 인터페이스에 연결된 고속의 링크는 스위치의 root 포트 변경을 야기할 수 있다. 목표는 가장 빠른 링크를 root 포트로 만드는 것이다.

예를 들어 스위치 B 의 한 포트가 기가비트 이더넷 링크이고, 스위치 B 의 다른 포트(10/100 링크)가 현재 root 포트라고 가정하자. 네트워크 트래픽이 기가비트 이더넷 링크를 통해 전달되는 것이 더 효과적이다. 기가비트 이더넷 인터페이스의 port priority 를 root 포트보다 더 높은 priority(낮은 숫자 값)를 가지도록 변경함으로써, 기가비트 이더넷 인터페이스를 새로운 root 포트로 만들 수 있다.

13.1.8. Spanning-Tree Interface States

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

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

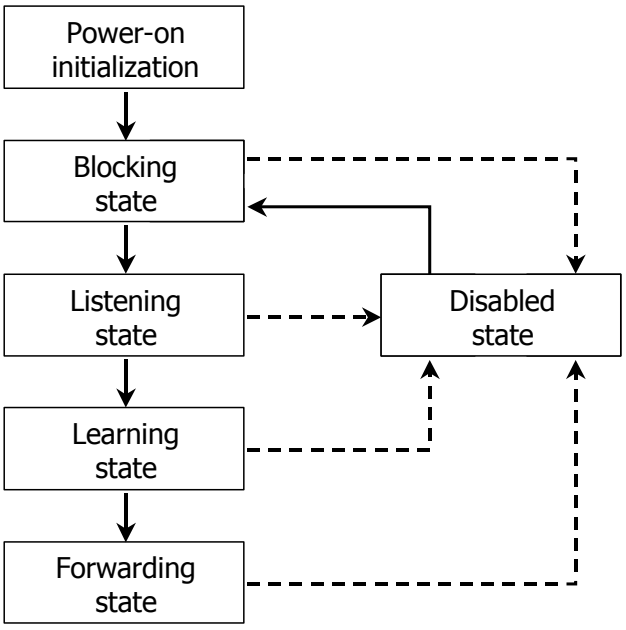
- Blocking – 인터페이스는 프레임을 forwarding하지 않는다.
- Listening – 인터페이스가 프레임을 forwarding해야 한다고 결정되었을 때, blocking state 다음의 천이 상태.
- Learning – 인터페이스가 프레임을 forwarding하기 위해 준비한다. MAC learning이 수행된다.
- Forwarding – 인터페이스가 프레임을 forward 한다.
- Disabled – 포트가 shutdown 상태이거나 포트에 링크가 없거나, 포트에 실행중인 spanning-tree instance가 없기 때문에 인터페이스는 spanning tree에 참여하지 않는다.

인터페이스들은 다음의 상태로 이동한다:

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

다음의 그림은 인터페이스의 상태천이를 보여준다.

그림 13-2 Spanning-Tree Interface States



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

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

1. 인터페이스가 forwarding 상태가 되어야 한다는 프로토콜 정보를 수신하면 인터페이스는

listening 상태가 된다.

2. forward-delay 타이머가 만료되었을 때, spanning tree는 인터페이스를 learning 상태로 만들고 forward-delay 타이머를 재설정한다.
3. learning 상태에서, 인터페이스는 종단 단말의 MAC learning은 수행하면서 프레임의 forwarding은 차단한다.
4. forward-delay 타이머가 만료되면, spanning tree는 인터페이스를 forwarding 상태로 만들고, learning 과 프레임의 forwarding이 모두 가능하다.

Blocking State

Blocking state 의 Layer 2 인터페이스는 프레임을 forwarding 하지 않는다. 스위치는 초기화 후에 스위치의 각 인터페이스로 BPDU 를 전송한다. 스위치는 다른 스위치와 BPDU 를 교환할 때까지 자신이 root 스위치 인 것처럼 동작한다. 이러한 BPDU 의 교환은 네트워크의 한 스위치를 root 스위치로 결정한다. 네트워크에 오직 하나의 스위치만 있다면 스위치 간의 BPDU 교환은 발생하지 않으며, forward-delay 타이머는 종료되면 인터페이스는 listening 상태에 놓인다. 인터페이스는 스위치 초기화 후에 항상 blocking 상태로 설정된다.

인터페이스는 blocking 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 하지 않는다
- BPDU를 수신한다

Listening State

listening state 는 blocking 상태 다음의 천이 상태이다. 인터페이스가 프레임을 forwarding 해야 한다고 결정되면, 인터페이스는 listening 상태가 된다.

인터페이스는 listening 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 하지 않는다
- BPDU를 수신한다

Learning State

learning 상태의 Layer 2 인터페이스는 프레임 forwarding 을 준비한다. 인터페이스는 listening 상태에서 learning 상태로 들어간다.

인터페이스는 learning 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 한다
- BPDU를 수신한다

Forwarding State

forwarding 상태의 Layer 2 인터페이스는 프레임을 forward 한다. 인터페이스는

learning 상태에서 forwarding 상태로 들어간다.

인터페이스는 forwarding 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임들을 forward 한다
- 다른 인터페이스로부터 스위칭된 프레임들을 forward 한다
- 주소를 learning 한다
- BPDU를 수신한다

Disable State

disabled 상태의 Layer 2 인터페이스는 프레임 forwarding 이나 spanning tree 에 참여하지 않는다.

disable 된 인터페이스는 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 하지 않는다
- BPDU를 수신하지 않는다.

13.1.9. STP and 802.1Q Trunks

VLAN trunk 에 관한 표준인 IEEE 802.1Q 는 trunk 에 허용된 모든 VLAN 에 대해 오직 하나의 spanning-tree instance 만 요구하고 있다. 하지만 Premier 8624XG 스위치는 802.1Q trunk 로 구성된 네트워크에서 trunk 에 허용된 각각의 VLAN 당 하나의 spanning-tree instance 를 운용한다. IEEE 802.1D spanning-tree 프레임을 802.1Q tagged 프레임 형식으로 사용함으로써 trunk 의 각 VLAN 별로 spanning-tree 프레임을 송수신 할 수 있다.

Cisco 스위치는 VLAN trunk 에서 spanning-tree 의 상호 연동을 위해 per-VLAN spanning tree(PVST) 를 사용한다. PVST/PVST+는 IEEE 802.1D 와는 다른 프레임 포맷을 사용하는데, 이로 인해 Cisco 스위치와 non-Cisco 스위치는 상호 연동하지 못하고 분리된다.

Premier 8624XG 스위치는 Cisco 의 PVST spanning-tree 프레임을 송수신할 수 있다. 일반적으로 Premier 8624XG 스위치는 VLAN trunk 에 대해 VLAN tag 가 붙은 IEEE 802.1D BPDU 프레임을 사용하지만, 만약 trunk 포트가 PVST 프레임을 수신하면 그 포트로는 PVST 포맷의 BPDU 를 전송한다. 이 기능은 PVST 프레임을 수신한 802.1Q trunk 에서 자동으로 활성화되며, 사용자의 설정을 필요로 하지 않는다.

13.2. Understanding RSTP

RSTP는 point-to-point 연결에 대해 spanning tree의 빠른 복구를 제공하는 장점을 가진다. Spanning tree의 재구성은 1초(802.1D spanning tree의 default 설정에서 최대 50초가 소요되는 것과는 대조적으로) 이내에 완료된다. 이것은 음성과 영상과 같은 지연에 민감한 트래픽을 전송하는 네트워크에 유효하다.

이 절은 RSTP가 어떻게 동작하는 지를 설명한다:

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

13.2.1. RSTP Overview

RSTP 는 스위치, 스위치 포트 혹은 LAN 에 장애가 발생했을 경우, 재빠른 연결의 복구(약 1 초 이내)를 제공한다. 새로운 root 포트로 선택된 포트는 바로 forwarding 상태로 천이할 수 있고, 스위치 사이의 명시적인 acknowledgement 를 통해 designated 포트도 forwarding 상태로 바로 천이할 수 있다.

13.2.2. Port Roles and the Active Topology

RSTP 는 active 형상을 결정하기 위한 port role 을 할당함으로써 spanning tree 의 빠른 복구를 제공한다. RSTP 는 STP 처럼 가장 높은 스위치 priority(가장 낮은 priority 값)를 가진 스위치를 root 스위치로 선택한다. 그리고 RSTP 는 각각의 포트에 다음과 같은 port role 을 할당한다:

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

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

트 역할을 가진 포트는 active 형상에서 제외된다.

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

표 3. Port State Comparison

Operational Status	STP Port State	RSTP Port State	Is Pot Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

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

13.2.3. Rapid Convergence

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

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

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

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

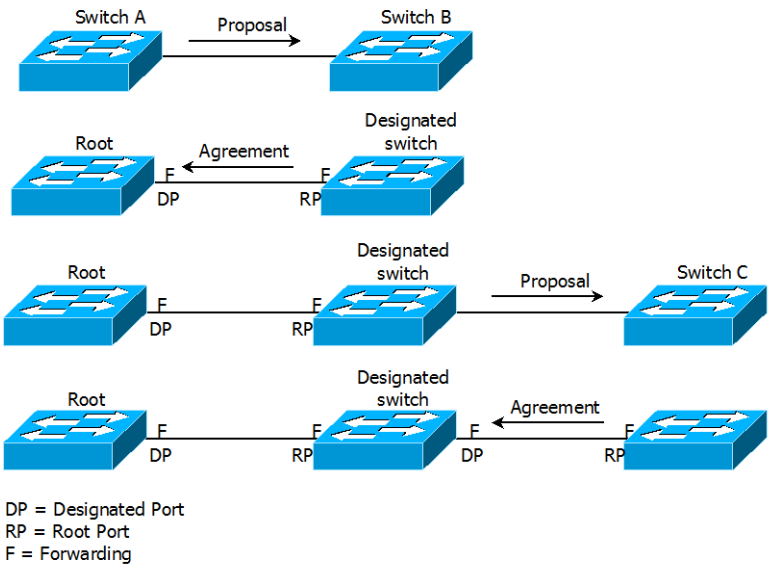
  스위치 B 의 agreement 메시지를 수신한 후에, 스위치 A 는 자신의 designated 포트를

forwarding 상태로 천이한다. 스위치 B 가 자신의 모든 non-edge port 를 block 시키고, 스위치 A 와 스위치 B 사이는 point-to-point 링크로 연결되었기 때문에 네트워크에 루프가 발생하지 않는다.

스위치 C 가 스위치 B 와 연결될 때, 유사한 협상 메시지가 교환된다. 스위치 C 는 스위치 B 와 연결된 포트를 root 포트로 선택하고, 두 스위치의 두 포트는 forwarding 상태로 천이한다. 협상 과정에서 하나 이상의 스위치가 active 형상에 참여한다. 네트워크의 복구에서 이런 proposal-agreement 협상은 spanning tree 의 root 에서 잎 방향으로 진행된다.

스위치는 포트의 duplex 모드로 link-type 을 결정한다: full-duplex 포트는 point-to-point 연결로 고려되고; half-duplex 포트는 공유 연결로 고려된다. interface configuration 명령 spanning-tree link-type 명령으로 duplex 모드에 의해 결정되는 default 설정을 변경할 수 있다.

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



13.2.4. Bridge Protocol Data Unit Format and Processing

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

표 4. RSTP BPDU Flags

Bit	Function

0	Topology change (TC)
1	Proposal
2-3: 00 01 10 11	Port role: Unknown Alternate port Root port Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

자신을 LAN 의 designated 스위치로 제안하려는 스위치는 RSTP BPDU 의 proposal flag 를 설정해서 전송한다. proposal 메시지의 port role 은 항상 designated 포트로 설정된다.

다른 스위치에 의한 제안을 받아들이는 스위치는 RSTP BPDU 의 agreement flag 를 설정해서 전송한다. agreement 메시지의 port role 은 항상 root port 로 설정된다.

RSTP 는 독립적인 topology change notification (TCN) BPDU 를 사용하지 않는다. topology change 를 알리기 위해 RSTP BPDU flag 의 topology change (TC) flag 를 사용한다. 하지만 802.1D 스위치와의 연동을 위해 TCN BPDU 를 생성하고 처리한다.

전송하는 포트의 상태에 따라 learning 과 forwarding flag 가 설정된다.

13.3. Configuring Spanning-Tree Features

이 절에서는 spanning-tree 를 설정하는 방법에 대해 설명한다:

13.3.1. Default STP Configuration

다음의 표는 STP 의 default 설정을 보여준다.

표 5. Default STP Configuration

Feature	Default Setting
Enable state	모든 VLAN 에 대해 비활성 되어 있음. 최대 128 개의 spanning-tree instance 를 활성화 할 수 있음.
Spanning-tree mode	IEEE 802.1D STP.
System priority	32768.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	10000 Mbps: 2. 1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello time	2 초.
Forward-delay time	15 초.
Maximum-aging time	20 초.

13.3.2. STP Configuration Guidelines

아무리 많은 VLAN 이 생성되어 있어도 오직 128 개의 VALN 에만 STP 를 활성화 할 수 있다.

이미 128 개의 spanning tree instance 가 동작 중 이라면, 그 VLAN 중 하나의 STP 를 비활성하고 사용하고 싶은 VLAN 의 STP 를 활성화하면 된다. 특정 VLAN 의 STP 를 비활성 하려면 global configuration 명령 **no spanning-tree vlan** *vlan-id* 를 사용하라. 원하는 VLAN 의 STP 를 활성화하려면 global configuration 명령 **spanning-tree vlan** *vlan-id* 를 사용한다.

Caution VLAN 에서 spanning-tree 를 실행중인 스위치들이 루프를 방지할 수 있도록, spanning tree 를 사용하지 않는 스위치도 수신한 BPDU 를 forward 한다. 그러므로, 네트워크에서 모든 루프를 방지하기에 충분한 만큼의 스위치에서 spanning tree 가 실행되어야 한다; 예로, VLAN 에서 각 루프에서 오직 하나의 스위치만 spanning tree 를 사용하면 된다. VLAN 의 모든 스위치들이 반드시 spanning tree 를 실행할 필요는 없다; 그러나 최소한의 스위치에서만 spanning tree 를 사용한다면, VLAN 에 루프를 발생시키는 네트워크의 부주의한 변화가 broadcast storm 을 야기할 수 있다.

13.3.3. Enabling STP

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

Caution STP 가 비활성 되어있고 형상에 루프가 존재한다면, 과도한 트래픽과 무한의 패킷 중첩이 발생하여 네트워크의 성능을 감소시킨다.

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

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

STP 를 비활성 하려면, global configuration 명령 **no spanning-tree vlan** *vlan-id* 를 사용한다.
다음은 VLAN 1 에 STP 를 활성화하고 비활성화하는 예를 보여준다

```
Switch#
Switch# configure terminal
Switch(config)# spanning-tree vlan 1
Switch(config)#
Switch(config)# end
Switch#
Switch# show spanning-tree

VLAN0001
```

```
 Spanning tree enabled protocol ieee
 Root ID    Priority    32768
            Address     0007.7012.2932
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
            Address     0007.7012.2932
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1
Switch(config)# end
Switch# show spanning-tree vlan 1

Spanning tree instance(s) for vlan 1 does not exist

Switch#
```

13.3.4. Disable per VLAN STP

Premier 8624XG 스위치는 VLAN 별로 spanning-tree 를 운영할 수 있다. 즉, VLAN trunk 포트의 각 VLAN 별로 STP state 를 설정하는 것이 가능하다. 만약 스위치에 128 개 이상의 VLAN 이 있다면, per VLAN STP 기능을 비활성 시키고, 전체 VLAN 을 제어하기 위한 하나의 spanning-tree instance 를 사용하도록 한다.

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

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

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

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

```
Switch#
Switch# show spanning-tree

Spanning tree instance(s) does not exist

Switch# configure terminal
Switch(config)# spanning-tree one-for-all-vlans
%Warning: you may enable only one spanning-tree instance per port.
Switch(config)# spanning-tree vlan 1
Switch(config)# end
Switch# show running-config
!
spanning-tree one-for-all-vlans
spanning-tree vlan 1
!
Switch#
Switch#
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1
Switch(config)# no spanning-tree one-for-all-vlans
Switch(config)# end
Switch# show running-config
!
!
Switch#
```

13.3.5. Configuring the Port Priority

루프가 발생하면 spanning tree 는 포트의 priority 를 사용하여 forwarding 상태의 인터페이스를 결정한다. 먼저 선택될 인터페이스에는 높은 priority 의 값(낮은 수)을, 나중에 선택될 인터페이스에는 낮은 priority 의 값(높은 수)를 할당할 수 있다. 모든 인터페이스가 같은 priority 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.

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

	Command	**Purpose**
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	**spanning-tree vlan** *vlan-id* **port-priority** *priority*	인터페이스의 VLAN 포트 priority 를 설정한다. ● *vlan-id* 의 범위는 1~4094 이다. ● *priority* 의 범위는 0~240 사이의 16의 배수이다. default는 128 이다. 낮은 수가 높은 priority를 의미한다. 유효한 값은 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224와 240이다. 이 외의 다른 값들은 거부된다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

인터페이스의 default 설정으로 복구하려면, interface configuration 명령 no spanning-tree vlan *vlan-id* port-priority를 사용한다.

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
```

```
gi6             Desg FWD 19       128.6    P2p

Switch# configure terminal
Switch(config)# interface gi5
Switch(config-if-gi5)# spanning-tree vlan 1 port-priority 240
Switch(config-if-gi5)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19       240.5    P2p
gi6              Desg FWD 19       128.6    P2p

Switch#
Switch# configure terminal
Switch(config-if-gi5)# no spanning-tree vlan 1 port-priority
Switch(config-if-gi5)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19       128.5    P2p
gi6              Desg FWD 19       128.6    P2p

Switch#
```

13.3.6. Configuring the Path Cost

spanning-tree 의 path cost 의 default 값은 인터페이스의 속도로부터 결정된다. 루프가 발생하면 spanning tree 는 포트의 cost 를 사용하여 forwarding 상태의 인터페이스를 결정한다. 먼저 선택될 인터페이스에는 낮은 cost 값을, 나중에 선택될 인터페이스에는 높은 cost 값을 할당할 수 있다. 모든 인터페이스가 같은 cost 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.

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

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

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	**spanning-tree vlan** *vlan-id* **cost** *cost*	VLAN 의 cost 를 설정한다. 루프가 발생했을 때 forwarding 상태의 포트를 결정하기 위해 spanning tree 는 path cost 를 사용한다. path cost 값이 낮을수록 고속의 전송이 가능함을 의미한다. ● *vlan-id* 의 범위는 1~4094 이다. ● *cost* 의 범위는 1~200000000 이다. default 값은 인터페이스의 전송속도로부터 결정된다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

인터페이스의 default 설정으로 복구하려면, interface configuration 명령 no spanning-tree vlan *vlan-id* cost 를 사용한다.

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
             Address     0007.70bc.cdde
             Cost        19
             Port        5 (gi5)
```

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

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
          Address     0007.7012.2932
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Root FWD 19        128.5    P2p
gi6              Altn BLK 19        128.6    P2p

Switch# configure terminal
Switch(config)# interface gi5
Switch(config-if-gi5)# spanning-tree vlan 1 cost 100
Switch(config-if-gi5)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
          Address     0007.70bc.cdde
          Cost        19
          Port        6 (gi6)
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
          Address     0007.7012.2932
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Altn BLK 100       128.5    P2p
gi6              Root FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# interface gi5
Switch(config-if-gi5)# no spanning-tree vlan 1 cost
Switch(config-if-gi5)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
          Address     0007.70bc.cdde
          Cost        19
          Port        5 (gi5)
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
```

```
          Address     0007.7012.2932
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Root FWD 19        128.5    P2p
gi6              Altn BLK 19        128.6    P2p

Switch#
```

13.3.7. Configuring the Switch Priority of a VLAN

스위치가 root 스위치가 될 가능성을 높이기 위해 스위치 priority 를 변경할 수 있다.

VLAN 에 대한 스위치 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	**Purpose**
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Step2	**spanning-tree vlan** *vlan-id* **priority** *priority*	VLAN 의 스위치 priority 를 설정한다. ● *vlan-id* 의 범위는 1~4094 이다. ● *priority* 의 범위는 0~61440 사이의 4096의 배수이다. default는 32768 이다. 낮은 수일수록 root 스위치로 선택될 가능성이 높다. 유효한 priority 값은 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344과 61440 이다. 다른 값들은 거부된다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show spanning-tree vlan** *vlan-id*	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 **no spanning-tree vlan** *vlan-id* **priority** 명령을 사용하라.

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
             Address     0007.70bc.cdde
             Cost        19
             Port        5 (gi5)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Root FWD 19        128.5    P2p
gi6              Altn BLK 19        128.6    P2p

Switch# configure terminal
Switch(config)# spanning-tree vlan 1 priority 0
Switch(config)# end
Switch#
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    0      (priority 0 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 priority
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    0
             Address     0007.70bc.cdde
             Cost        19
             Port        5 (gi5)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

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

```
gi5             Root FWD 19        128.5    P2p
gi6             Altn BLK 19        128.6    P2p

Switch#
```

13.3.8. Configuring the Hello Time

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

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

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

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

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p
```

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 hello-time 5
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time  5 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time  5 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 hello-time
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
```

13.3.9. Configuring the Forwarding-Delay Time for a VLAN

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

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

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

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# spanning-tree vlan 1 forward-time 20
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 20 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
```

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

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 forward-time
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
```

13.3.10. Configuring the Maximum-Aging Time for a VLAN

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

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Step2	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	VLAN 의 maximum-aging time 을 설정한다. maximum-aging time 은 스위치가 재구성을 하기 전에 spanning-tree 정보를 수신하지 않고 기다리는 최대 시간이다. ● *vlan-id* 의 범위는 1~4094 이다. ● *seconds* 의 범위는 6~40 이다. default는 20 이다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show spanning-tree vlan** *vlan-id*	설정 내용을 확인한다.
Step5	**copy running-config startup-**	(옵션) 설정을 configuration 파일에 저장한다.

config	

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

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# spanning-tree vlan 1 max-age 10
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 10 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 10 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 max-age
Switch(config)# end
Switch# show spanning-tree

VLAN0001
```

```
 Spanning tree enabled protocol ieee
 Root ID    Priority    32768
            Address     0007.7012.2932
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
            Address     0007.7012.2932
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
```

13.3.11. Changing the Spanning-Tree mode for switch

스위치의 spanning-tree 모드를 변경하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Step2	**spanning-tree mode {rstp|stp}**	스위치의 spanning-tree 모드를 변경한다. ● rstp 는 IEEE 802.1w 모드로 동작한다. ● stp 는 IEEE 802.1D 모드로 동작한다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 no spanning-tree mode 명령을 사용하라.

```
Switch# show spanning-tree

VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    32768
            Address     0007.7012.2932
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
            Address     0007.7012.2932
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# spanning-tree mode rstp
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# spanning-tree mode stp
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
```

13.3.12. Configuring the Port as Edge Port

RSTP 를 사용할 때, 단일 호스트와 연결된 포트에 대해서 edge port 로 설정한다. 만약 포트를 edge 포트로 설정하지 않으면, 그 포트는 forwarding 상태로 천이하는데 2 x Forward Time 이 소요된다.

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

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

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Step2	**Interface** *interface-id*	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	**spanning-tree admin-edge-port**	포트를 edge port로 설정한다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p
fa7              down DIS 0         128.7    P2p
```

```
Switch# configure terminal
Switch(config)# interface fa7
Switch(config-if-fa7)# spanning-tree admin-edge-port
Switch(config-if-fa7)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p
fa7              down DIS 0         128.7    P2p Edge

Switch#
```

13.3.13. Configuring the 802.1D STP Compatible Mode

각 VLAN 의 spanning-tree instance 별로 프로토콜 동작 모드를 설정할 수 있다. 일반적인 RSTP 에서는 RSTP BPDU 만을 사용해서 spanning-tree 를 구성하고, 802.1D BPDU 를 수신했을 경우에만 호환을 위해 802.1D BPDU 를 사용한다. 하지만 STP 호환 모드에서는 RSTP BPDU 를 사용하지 않고 오직 802.1D BPDU 만을 사용한다. 또한 RSTP 가 제공하는 빠른 복구 기능을 사용할 수 없게 된다.

RSTP instance 의 프로토콜 모드를 변경하려면, privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	**Purpose**
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**spanning-tree vlan** *vlan-id* **force-version stp**	특정 VLAN 의 RSTP instance 의 프로토콜 동작모드를 STP 호환 모드로 설정한다. *vlan-id* 의 범위는 1~4094 이다. default 는 RSTP 모드이다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show running-config**	설정 내용을 확인한다.

Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# spanning-tree vlan 1 force-version rstp
Switch(config)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 force-version
Switch(config)# end
```

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch#
```

13.3.14. Specifying the Link Type to Ensure Rapid Transitions

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

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

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

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

	Command	**Purpose**
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Stpe3	**spanning-tree link-type point-to-point**	포트의 링크 종류를 point-to-point 로 설정한다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.

Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

13.3.15. Restarting the Protocol Migration Process

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

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

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

```
Switch# configure terminal
Switch(config)# interface gi5
Switch(config-if-gi5)# spanning-tree vlan 1 mcheck
Switch(config-if-gi5)#
```

13.4. Displaying the Spanning-Tree Status

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

Command	**Purpose**
show spanning-tree active	활성 인터페이스의 spanning-tree 정보만을 출력한다.
show spanning-tree interface *interface-id*	특정 인터페이스의 spanning-tree 정보를 출력한다.
show spanning-tree summary	포트 상태를 요약해서 보여준다.

privileged EXEC 명령 **show spanning-tree** 명령의 다른 키워드에 관한 정보는 command reference를 참고하라.

```
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
```

```
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# show spanning-tree active

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0007.7012.2932
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0007.7012.2932
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
----
gi5              Desg FWD 19        128.5    P2p
gi6              Desg FWD 19        128.6    P2p

Switch# show spanning-tree interface gi5
 Port 5 (gi5) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.5.
   Designated root has priority 32768, address 0007.7012.2932
   Designated bridge has priority 32768, address 0007.7012.2932
   Designated port id is 128.5, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
```

```
  Number of transmition to forwarding state: 1
  BPDU: sent 627, received 7
Switch#
```

13.5. Self-loop Detection

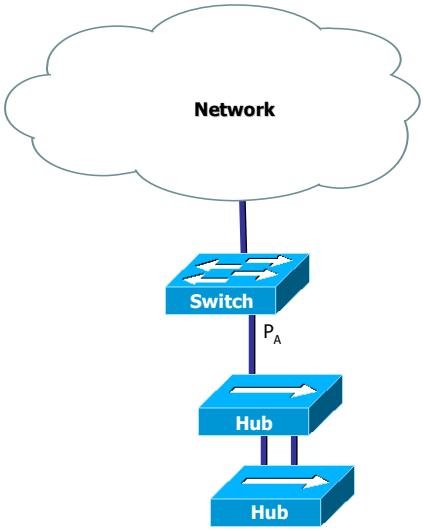
자신이 전송한 패킷이 되돌아 오는 현상을 감지하는 self-loop 감지 기능을 설정하는 방법을 설명한다.

13.5.1. Understanding Self-loop Detection

사용자의 스위치에 이중 경로가 존재하지 않아도 네트워크 구성이나 스위치에 연결된 케이블의 상태 등에 따라 loop 가 발생할 수 있다.

스위치가 자신의 한 포트로 전송한 패킷이 다시 그 포트로 되돌아왔을 때, 이런 현상을 self-loop 이라 한다. 다음의 그림은 self-loop 이 발생한 환경에 대한 예제이다.

그림 13-4. self-loop 발생 환경



그림에서 두 hub 사이에 이중 경로에 의한 loop 이 존재한다. STP 가 활성화 되지 않은 상태이기 때문에 hub 사이의 loop 은 제거되지 않으며 network 의 불안정을 초래하게 된다. 이 경우 스위치가 포트 PA 를 통해 전송한 패킷은 다시 PA 로 수신된다. 스위치에 self-loop 감지 기능이 활성화되어 있다면, 포트 PA 에 self-loop 이 있다는 것을 감지하고 포트 PA 를 서비스 불가능 상태(Administrative disable)로 만들어 스위치와 포트 PA 와 연결되지 않은 다른 네트워크를 보호하게 된다. 포트 PA 에 연결된 장비와 네트워크에 여전히 loop 은 존재한다(네트워크에서 완전한 loop 의 제거를 원한다면 STP 를 사용하라).

13.5.2. Configuring Self-loop Detection

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

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

13.5.2.1. Enabling Self-loop Detection

Self-loop 감지 기능은 스위치의 각 포트 별로 기능의 활성화가 가능하다. 또는 Port 의 range 선택 상태에서도 활성화가 가능하다. default 는 self-loop 감지 기능이 비활성화 되어 있다.

Self-loop 감지 기능이 활성화 된 후 이 기능에 의하여 port 가 shutdown 상태가 되면 설정된 limit time 이 지난 후 자동으로 no shutdown 상태로 바뀐다. Limit time 의 default 값은 5 분이고, 분

단위로 0 부터 1440 까지 지정할 수 있으며 0 으로 설정하면 수동으로 no shutdown 하기 전까지 port 가 shutdown 상태로 있는다.

Notice P8624XG 에서는 기존의 SLD 와는 다르게 Self-loop 감지 하고자 하는 포트가 속한 vlan 에 self-loop-detection 을 활성화 한 이후에 실제 Self-loop 감지 하고자 하는 포트에 self-loop-detection 을 활성화해야 SLD 가 정상적으로 동작 한다.

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

	Command	**Purpose**
Step1	**Configure terminal**	Global configuration 모드로 진입한다.
Step2	**interface** *vlan-name*	Slef-loop 을 걸고자 하는 포트가 속한 vlan
Step3	**self-loop-detection**	해당 vlan 에 Self-loop 감지 기능을 활성화 한다.
Step4	**interface** *interface-name*	Interface configuration 모드로 진입한다.
Step5a	**self-loop-detection**	Self-loop 감지 기능을 활성화 한다. Self loop 에 의해 shutdown 되면 5 minutes 후에 자동으로 no shutdown 한다.
Step5b	**self-loop-detection limit_time** *<0-1440>*	Self-loop 감지 기능을 활성화 한다. Self loop 에 의해 shutdown 되면 설정된 minutes 후에 자동으로 no shutdown 한다.
Step6	**end**	privileged EXEC 모드로 변경한다.
Step7a	**show running-config**	설정 내용을 확인한다.
Step7b	**show self-loop-detection**	Self-loop 설정 내용을 확인한다.
Step7c	**show loop-detect**	Self-loop 설정 내용을 확인한다.
Step8	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

다음은 포트 gi1 에 self-loop 감지 기능을 default limit time 으로 활성화 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if-vlan1)# self-loop-detection
Switch(config-if-vlan1)# interface gi1
Switch(config-if-gi1)# self-loop-detection
Switch(config-if-gi1)# end
Switch# show self-loop-detection
-------------------------------------------------------------------------------
 ifname  ld  link  shutdown set_time remain_time count      last-occur
-------------------------------------------------------------------------------
 gi1    set   up       .      5 min      .        0          .
 gi2     .   down      .       .         .        0          .
 gi3     .   down      .       .         .        0          .
 gi4     .   down      .       .         .        0          .
 gi5     .    up       .       .         .        0          .
.....
 gi25    .   down      .       .         .        0          .
 gi26    .   down      .       .         .        0          .
Switch#
```

13.5.2.2. Changing The Service Status of Port

Self-loop 감지 기능에 의해 서비스 불가능 상태가 된 포트가 limit time 이 0 으로 설정된 상태라면 수동으로만 서비스 가능 상태로 만들 수 있다.

포트를 서비스 가능 상태로 만들려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**Configure terminal**	Global configuration 모드로 진입한다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입한다.
Step3	**no shutdown**	포트를 서비스 가능 상태로 만든다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show port status**	포트의 상태정보를 확인한다.

13.5.2.3. Disabling Self-loop Detection

Self-loop 감지 기능은 스위치의 각 포트 별로 또는 Port 의 range 선택 상태에서 기능의 비활성화가 가능하다.

만약 비활설화할 Port 가 Self-loop 감지기능에 의해 자동으로 shutdown 된 상태라면 no shutdown 으로 설정 후 Self-loop 감지 기능을 비활성화 한다.

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

	Command	Purpose
Step1	**Configure terminal**	Global configuration 모드로 진입한다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입한다.
Step3a	**no self-loop-detection**	Self-loop 감지 기능을 비활성화 한다. Self loop 에 의해 shutdown 되면 5 minutes 후에 자동으로 no shutdown 한다.
Step4	**interface** *vlna-name*	vlan configuration 모드로 진입한다.
Step5a	**no self-loop-detection**	Self-loop 감지 기능을 비활성화 한다.
Step6	**end**	privileged EXEC 모드로 변경한다.
Step7a	**show running-config**	설정 내용을 확인한다.
Step7b	**show self-loop-detection**	Self-loop 설정 내용을 확인한다.
Step8	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

다음은 포트 gi1 에 self-loop 감지 기능을 비 활성화 하는 방법을 보여준다:

Switch# **configure terminal**
Switch(config)# **interface vlan1**
Switch(config-if-vlan1)# **self-loop-detection**
Switch(config-if-vlan1)# **interface gi1**

```
Switch(config-if-gi1)# no self-loop-detection
Switch(config-if-gi1)# end
Switch# show self-loop-detection
-------------------------------------------------------------------------
 ifname  ld  link  shutdown set_time remain_time count      last-occur
-------------------------------------------------------------------------
 gi1     .   up       .       .         .        0          .
 gi2     .  down      .       .         .        0          .
 gi3     .  down      .       .         .        0          .
 gi4     .  down      .       .         .        0          .
 gi5     .   up       .       .         .        0          .
.....
 gi25    .  down      .       .         .        0          .
 gi26    .  down      .       .         .        0          .
Switch#
```

13.5.3. Displaying Self-loop Status

포트의 self-loop 감지 기능 설정 상태를 조회하려면, privileged EXEC 명령 **show running-config** 나 **show self-loop-detection** 을 사용하라.

show self-loop-detection 에서

- ifname : Interface name (Port name)
- ld : self-loop-detection 설정 (set)
- link : link 의 상태 (up, down)
- shutdown : SLD 에 의한 shutdown (block)
- set_time : SLD 에 의한 limit time (minutes). 만약 0 min 이라면 SLD 에 의해 shutdown 된 후, 수동으로 해당 Port 를 no shutdown 하기 전까지 계속 shutdown 상태로 있게 된다.
- remain_time : SLD 에 의한 shutdown 시 정상으로 복귀되기 까지 남은 시간(minute:second)
- count : SLD 에 의한 shutdown 횟수
- last-occur : 마지막으로 SLD 에 의해 shutdown 된 시간

다음 예는 Port gi5 에 SLD 가 default time 인 5 분으로 설정되어 있는 것을 보여준다. Port gi5 는 May 29 04:48:39 2006 에 SLD 에 의해 self loop 이 감지되어 shutdown 된 적이 한번 있었다는 것을 알 수 있다.

```
Switch# show running-config
!
interface gi5
```

```
 self-loop-detection
!
interface vlan1
  self-loop-detection
 ip address 100.1.1.1/24
!
Switch#
Switch# show self-loop-detection
-------------------------------------------------------------------------------
 ifname  ld  link  shutdown set_time remain_time count       last-occur
-------------------------------------------------------------------------------
 gi1     .   down      .       .          .        0          .
 gi2     .    up       .       .          .        0          .
 gi3     .   down      .       .          .        0          .
 gi4     .   down      .       .          .        0          .
 gi5    set   up      block     5 min      .        1  May 29 04:48:39 2007
 gi6     .   down      .       .          .        0          .
 gi7     .   down      .       .          .        0          .
 gi8     .   down      .       .          .        0          .
Switch#
```

14

환경설정 저장 및 소프트웨어 업그레이드

본 장에서는 시스템의 Flash File System 의 관리 방안에 대해서 설명한다. Flash File System 은 시스템 OS Image 와 Configuration 파일을 저장하는 장소로 주로 사용되며, 부팅 시 여기에 저장된 OS Image 와 Configuration File 을 시스템이 Loading 하게 된다. 이 장에서는 기본적인 Flash File System 운용에 필요한 명령어와 OS Image 와 Configuration File Management 에 필요한 명령어 및 부팅 모드 설정에 필요한 명령어 등을 중심으로 설명한다.
(주. 본 매뉴얼에서 설명된 기능은 당사의 사정에 의해 변경될 수 있다)

14.1. Flash 파일 시스템

Premier 8624XG 스위치는 OS image 파일 저장 및 환경 설정의 저장을 위해 Flash 파일 시스템을 구축한다. 이 장에서 본 제품의 Flash 파일 시스템에 대해 설명한다.

Flash 파일 시스템은 OS image 파일과 장비의 설정을 파일로 저장하기 위해 사용한다. 각 파일은 Flash 메모리의 영역에서 기록되고, 저장할 때 또는 rename 명령어로 저장이름을 설정할 수 있다. 또한 사용자의 요구사항에 따라 이미 Flash File System 에 저장된 File 을 erase 명령어로 지울 수 있다. 단 지우거나 변경할 파일이 다음 부팅 때 사용될 OS image 또는 설정 파일인지 주의해야 한다.

시스템 파일 관리를 위한 기본 명령어는 다음과 같다.

표 14-1. 파일 관리를 위한 명령어

명령어	설명	모드
show flash:	• Flash File 의 상태를 보여준다.	Privileged
show config-list	• Flash 메모리에 저장된 환경 설정 파일을 보여준다.	Privileged

erase *filename*	• Flash 메모리에 저장된 환경 설정 파일을 삭제한다.	Privileged
rename flash *filename change*	• Flash File 의 이름을 변경한다.	Privileged

다음은 show flash: 명령어를 시행하였을 때 나타나는 출력문의 예시를 나타낸다. Premier 8624XG 스위치는 Flash File System 의 정보에 대해서 파일 이름과 파일 사이즈, 그리고 현재(B) 및 다음 부팅 모드(*)에 대한 정보와 함께 그 파일의 종류를 표시한다.

```
Switch# show flash:

--------filename-------- -----------type/info------------ CN -length-
swcfg                    text file                        --      1681
abc.cfg                  text file                        B*      2213
p8xg.r141g               1.4.1g                           B* 10850005
p8xg.r141h               1.4.1h                           -- 10847225

10076 Kbytes available (22692 Kbytes, 70 % used)
```

14.2. Image/Configuration/BSP Down/Up Load

Premier 8624XG 스위치는 운영하면서 필요한 OS Image, Configuration File 및 Bootloader 에 대해서 FTP 또는 TFTP 를 이용해서 Down 또는 Up Load 할 수 있다. 이는 새로운 파일을 Flash 파일에 저장하거나, 적용으로 사용될 수도 있고, 운용상 필요한 Backup 을 FTP/TFTP Server 에 할 수 있다. 또한 새로운 BSP file 을 download 하여 적용할 수 있다. 이 장에서는 어떻게 FTP/TFTP 를 통해서 파일을 Down/Up Load 하는지 설명한다. 아래에서 기술한 running-config 및 startup-config 에 대한 설명은 “Configuration File 관리”라는 장에 설명해 놓았다.

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

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

14.2.1. FTP 를 통한 Down/Up Load

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

표 14-2. FTP 를 통한 Down/Up Load 명령어

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

아래는 FTP 를 이용한 파일 다운 방법에 대한 예를 보여준다.

```
Switch# copy ftp flash
IP address of remote host ? 192.168.0.1
User ID ? lns
Password ?
Source file name ? p8xg.r089
Destination file name ? p8xg.r089

FTP::192.168.0.1//p8xg.r089 -->image file[p8xg.r089]
Proceed [yes/no]?  yes
(생략)
```

```
Switch# copy ftp bootloader
IP address of remote host ? 192.168.0.1
User ID ? lns
Password ?
Source file name ? p8xg.bsp
Bootloader key (0xaabb) ? 0x8624XG11

FTP::192.168.0.1//p8xg.bsp --> bootloader
Continue [yes/no]? yes
(생략)
```

Warning Bootloader 적용시의 key 값은 보완을 위해 사전에 협의 후 배포한다.

14.2.2. TFTP 를 통한 Down/Up Load

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

표 14-3. TFTP 를 통한 Down/Up Load 명령어

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

copy running-config tftp	• System 에서 운용중인 현재 running-config 을 TFTP Server 에 저장한다.	Privileged
copy tftp bootloader	• TFTP Server 에 있는 BSP File 을 Flash 에 저장한다.	Privileged

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

```
Switch# copy flash tftp
IP address of remote host ? 192.168.0.1
filename to write on tftp host? p8xg.r090

TFTP send: -> 192.168.0.1// p8xg.r090
Proceed [yes/no]? yes
(생략)
```

```
Switch# copy tftp bootloader
IP address of remote host ? 192.168.0.1
Source file name ? p8x.bsp
Bootloader key (0xaabb) ? 0x8624XG11

TFTP::192.168.0.1//p8x.bsp --> bootloader
Proceed [yes/no]? yes
(생략)
```

14.3. Configuration File 관리

환경 설정은 시스템 운영자가 Premier 8624XG 스위치를 운영하면서 설정된 다양한 파라미터의 집합이다. Premier 8624XG 스위치에서 사용하는 Configuration 에는 startup-config 와 running-config 가 있다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration 을 startup-config 라 하며, DRAM 내에서 구동하는 환경설정 값을 running-config 라 한다. 여기서는 Configuration File Management 에 필요한 저장, 삭제 및 다운로드 방법을 설명한다.

표 14-4. Configuration Management 명령어

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

erase startup-config	• 현재 설정된 startup configuration 파일을 지운 Privileged 다.

14.3.1. Configuration file 의 저장

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

```
P8624XG# show running-config
!
hostname P8624XG
!
interface gi1
 ip address 192.168.51.1 255.255.255.0
     ... <생략> ....
SWITCH#
SWITCH# copy running-config startup-config
Overwrite 'system.cfg'? [yes/no] y
SWITCH# show startup-config
!
hostname P8624XG
!
interface gi1
  no switchport
 ip address 192.168.51.1 255.255.255.0
     ... <생략> ....
SWITCH#
```

14.3.2. Configuration file 의 삭제

Premier 8624XG 스위치는 시스템 재시동 시 flash 메모리에 저장되어 있는 startup-config 를 재 로딩한다. 만약 현재 저장되어 있는 Configuration file 를 삭제하고 다른 파일로 시스템을 사용하고자 한다면 다음 예에서 보여주는 것처럼 startup-config 를 지우고 다른 파일로 설정 후 재 부팅하면 된다.

```
SWITCH# erase flash System1.cfg
Warning: System1.cfg is booting config file
Do you want to erase it [yes/no]? y
SWITCH# boot config System2.cfg
SWITCH# reload
```

14.4. Boot Mode 설정 및 시스템 재시동

Premier 8624XG 스위치는 운영하면서 필요한 OS Image 와 Configuration File 에 대해서 다음 부팅 파일로 설정할 수 있다. 이렇게 설정된 OS Image 와 Configuration File 은 시스템의 재 시동 시 적용되므로 각별한 주의가 필요하다. 아래에서는 OS Image 와 Configuration File 에 대해서 어떻게 다음 부팅 모드로 설정하는 지와 시스템 재 시동 방법에 대해서 설명해 놓았다.

표 14-5. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
Boot flash *filename*	• 다음 부팅시 적용될 OS Image 를 설정한다.	Privileged
Boot config *filename*	• 다음 부팅시 적용될 Configuration File 을 설정한다.	Privileged
Reload	• 시스템을 재 시동 시킨다.	Privileged

14.4.1. Boot Mode 설정

Premier 8624XG 스위치에서 OS Image 와 Configuration File 에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요하다. boot flash 명령어를 실행할 때에는 Premier 8624XG 스위치에서 사용할 수 있는 OS Image File 에 대해서만 적용하도록 해야 하며, 또 boot config 명령어를 시행할 때에는 Premier 8624XG 스위치에서 사용할 수 있는 Configuration File 에 대해서만 적용하도록 해야 된다. 그리고 현재 Flash File System 에 있는 File 에 대해서만 적용하도록 하여야 한다.

```
Switch#
Switch# boot flash p8xg.r090
Switch#
Switch# boot config lns.cfg
Switch#
```

14.4.2. 시스템 재시동

시스템의 재시동은 Permier 8624XG Series 스위치의 전원 On/Off 또는 콘솔상에서 명령어로 할 수 있다.

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

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

```
SWITCH# reload
WARNING !!!
 You must save current configuration or you will lose it..

"continue to reboot [yes/no]? yes
SWITCH#
```

15

IP ACCOUNT 및 SNOOP DEVICE

본 장에서는 Premier 8624XG 스위치에서의 IP ACCOUNT 기능과 SNOOP DEVICE 에 대하여 설명한다.

15.1 IP ACCOUNT 개요

IP ACCOUNT 기능은 상용 S/W 인 NTOP 을 통해 IP 별 성능 정보를 CONSOLE 과 WEB 을 통해 관찰할 수 있는 기능이다. 관찰하고자 하는 DEVICE 를 SNOOP DEVICE 로 그룹화 하여 사용할 수 있다.

15.2 IP ACCOUNT 명령어

IP ACCONT 는 CONSOLE 과 WEB 을 통해 확인할 수 있으며 WEB 의 경우 최초 NTOP INSTALL 과정이 필요하다.

15.2.1 Show ip account 명령어

CONSOLE 상에서 IP ACCONT 를 확인하기 위해 **Show ip account IFNAME** 명령어를 사용한다.

표 15.1 Show ip account 명령어

명령어	설명	모드
Show ip account IFNAME	**IFNAME** 에는 gi1,vlan1,snoop 등의 DEVICE 를 사용할 수 있다.	privileged

표 15.2 Show ip account 실행

```
                  lns ntop v.0.1 [p8k] listening on eth0
210 Pkts/27.9 Kb [IP 21.4 Kb/Other 6.5 Kb]              Thpt: 0.0 Kbps/0.0 Kbps
 Host                       Act    -Rcvd-       Sent        TCP        UDP      ICMP
 192.168.0.197               B     9.9 Kb    11.5 Kb        727     9.0 Kb       212
 192.168.0.51                B     9.6 Kb     9.8 Kb          0     9.4 Kb       212
 192.168.0.1                 B     1.9 Kb        727     1.9 Kb          0         0
 00:07:70:42:00:00           S          0     3.9 Kb          0          0         0
 00:07:70:80:01:1B           S          0        414          0          0         0
 00:50:DA:92:A8:0E           S          0         98          0          0         0
```

표 15.3 Show ip account 실행 중 명령어

```
'q' - quit ntop
'r' - reset statistics
'n' - toggle address format (num <-> sym <-> MAC <-> Nw Board Manufact.)
'p' - toggle traffic values (bytes <-> % <-> thpt)
'l' - toggle hosts display (local subnet <-> all)
'd' - toggle idle (idle <-> send/receive)
't' - toggle sort (sent <-> received)
'y' - toggle columns sort
'h' - show this help
' ' - toggle protocol
```

15.2.2 NTOP 설치 및 실행

IP ACCOUNT 를 WEB 상에서 확인하기 위해선 첫 사용시 ntop.conf 다운로드 후 service 를 실행하여야 한다.

Notice NTOP 기능은 단기간 동안의 트래픽 모니터링을 제공하며 일정시간 경과 후 모든 데이터는 초기화된다.

15.2.2.1 ntop.conf 다운받기

copy tftp config-file 또는 copy ftp config-file 명령어를 통해 ntop.conf 파일을 다운 받는다 (14 장 환경설정 및 소프트웨어 업그레이드 참조)

표 15-1 copy 명령어

```
Switch# copy tftp config-file
IP address of remote host ? 192.168.0.1
Source configuration file name ? ntop.conf
Destination configuration file name ? ntop.conf
```

15.2.2.2 SERVICE KEY 등록

제공된 SERVICE KEY 를 **license 명령어를** 이용하여 등록하여야 한다 (license command 참조)

표 15.5 show license 명령어

```
Switch # sh license

Software is licensed for the following features.

 RIP is enabled
 OSPF is enabled
 BGP is enabled
 PIM-SM is enabled
 IPACC is enabled

Switch #
```

15.2.2.3 NTOP 실행

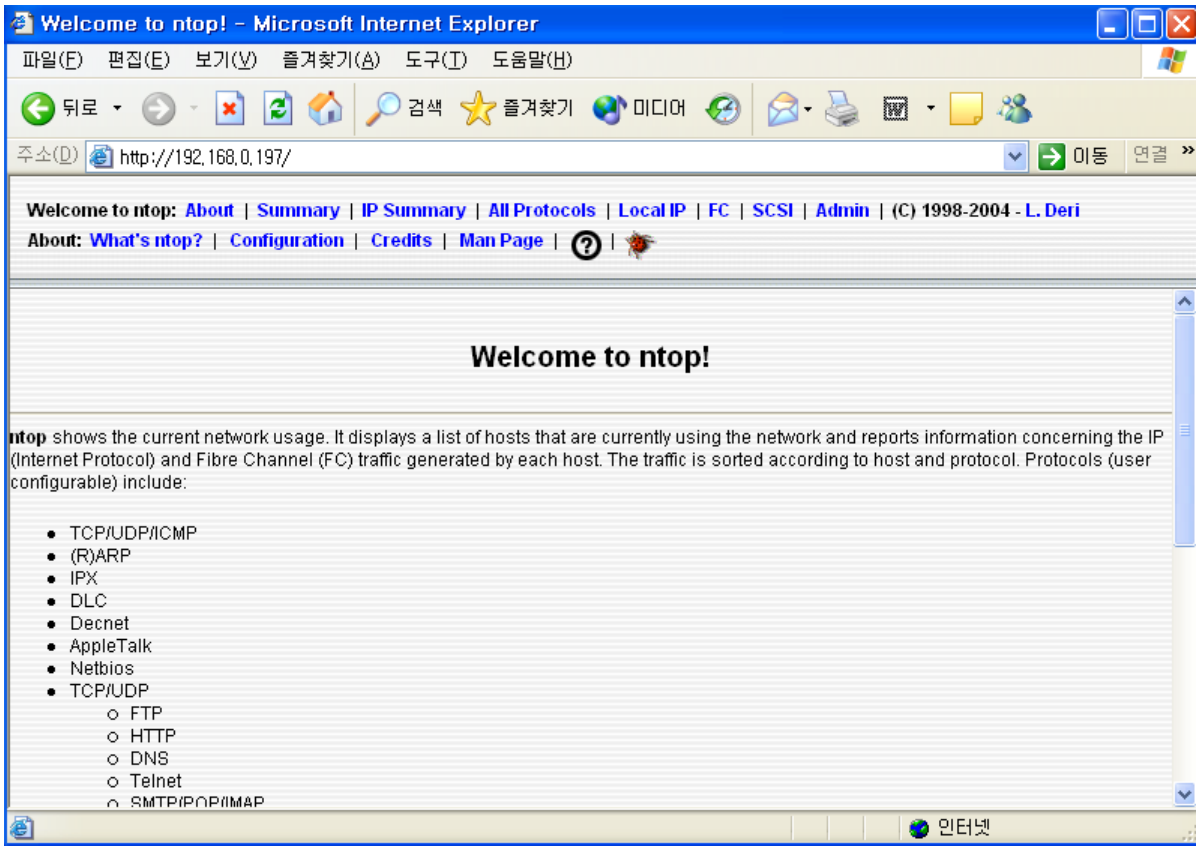
Service ntop IFNAME 명령어를 사용하여 ntop service 를 시작한다. Service 실행 후 웹브라우저를 통해 시스템에 접속하여 성능 정보를 확인한다. 그림 15-1 은 ntop 의 메인 화면이다.

표 15.6 ntop 실행/종료 명령어

명령어	설명	모드
Service ntop IFNAME	Ntop service 시작 명령어. **IFNAME** 에는 gi1,vlan1,snoop1 등의 DEVICE 를 사용할 수 있다.	Config

Service ntop IFNAME local A.B.C.D/M	Local network 의 range 를 포함한 Ntop service 시작 명령어	Config
No service ntop	Ntop service 중지 명령어.	Config

그림 **15-1.** ntop 메인화면



15.2.2.4 PROTOCOL LIST 만들기

PROTOCOL LIST 기능은 NTOP 상에서 사용자가 관찰하고자 하는 protocol 을 생성/삭제 할수 있게 해준다. **ntop protocol-list PROTO_ID_LIST** 에 의해 protocol list 를 선택한 경우 NTOP 서비스시 자동 반영된다.

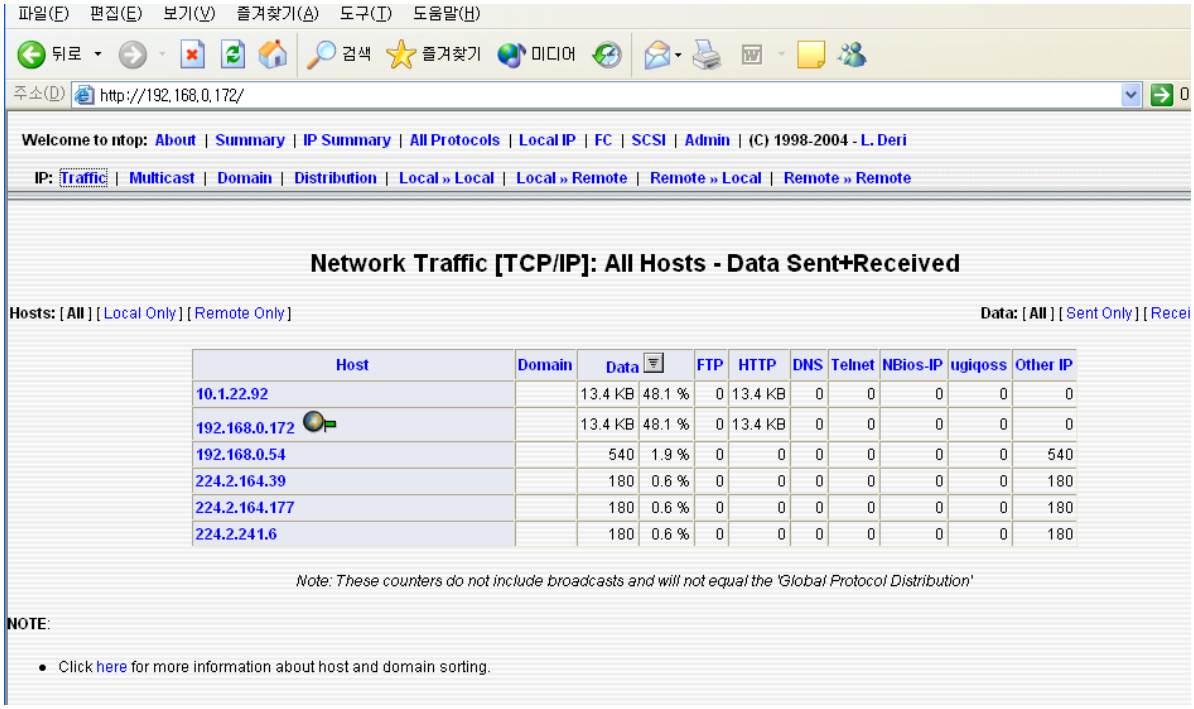
표 15.7 protocol list 명령어

명령어	설명	모드
show ntop protocol-list	Ntop 에서 사용할 수 있는 protocol list 를 보여주는 명령어.	privileged
ntop protocol-list PROTO_ID_LIST	**show ntop protocol-list** 명령어를 참조하여 사용자가 관찰하고자 하는 protocol 들을 선택하는 명령어.	Config
No ntop protocol-list PROTO_ID_LIST	사용자가 선택했던 protocol 들을 해제 하는 명령어	
ntop protocol-list create PROTO_NAME	새로운 protocol list 를 생성하는 명령어 (생성 후 **show ntop protocol-list** 명령어에 반영 됨)	Config
ntop protocol-list delete PROTO_NAME	생성한 protocol list 를 삭제하는 명령어	Config

표 15.8 protocol list 생성 예

```
Switch (config)# ntop protocol-list create ubiquoss
Switch (config)#exit
Switch # show ntop protocol-list
 1.FTP=ftp|ftp-data
 2.HTTP=http|www|https|3128
 3.DNS=name|domain
 4.Telnet=telnet|login
 5.NBios-IP=netbios-ns|netbios-dgm|netbios-ssn
 6.Mail=pop-2|pop-3|pop3|kpop|smtp|imap|imap2
 7.DHCP-BOOTP=67-68
 8.SNMP=snmp|snmp-trap
 9.NNTP=nntp
 10.NFS=mount|pcnfs|bwnfs|nfsd|nfsd-status
 11.X11=6000-6010
 12.SSH=22
 13.Gnutella=6346|6347|6348
 14.Kazaa=1214
 15.WinMX=6699|7730
 16.eDonkey=4661-4665
 17.Messenger=1863|5000|5001|5190-5193
 18.ubiquoss=4000-4001|5000
Switch #con t
Switch (config)# ntop protocol-list 1-5,19
Switch (config)# service ntop snoop1 local 192.168.0.0/24
```

그림 15-2. protocol list 설정시 protocol 항목



15.3 SNOOP DEVICE

IP ACCOUNT 기능을 통해 특정 혹은 다수의 device 를 관찰 하고자 할 때 SNOOP DEVICE 를 사용한다.

표 15.9 SNOOP DEVICE 명령어

명령어	설명	모드
Soop device <1-100>	Snoop device 생성 명령어. Soop device id 1 은 device name ‘snoop1’ 을 갖게된다.	Config

No snoop device <1-100>	Snoop device 삭제 명령어.	Config
Soop device <1-100> add IFNAME	Snoop device 에 interface 를 추가하는 명령어.IFNAME 에는 gi1,vlan1 등이 사용가능하다.	Config
Soop device <1-100> delete IFNAME	Snoop device 에서 interface 를 삭제 하는 명령어	Config

16

CPU-FILTER & IP-OPTION

16.1. CPU Filtering

본 Premier 8624XG 스위치에서는 스위치 자체로 들어오는 트래픽이나 스위치의 CPU 를 이용하여 포워딩되는 트래픽에 대한 필터링 기능을 제공합니다. 이는 IP 주소, 프로토콜, 포트 별로 사용자 설정이 가능하며, 다음의 명령어를 이용하여 필터링 설정을 할 수 있습니다.

16.1.1. CPU-Filtering Rule 설정/해제

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

명령어	설명
cpu-filter rule *NAME* **ip { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } match { permit | deny }**	■ IP 프로토콜에 대한 CPU-filter ■ source address 와 destination address 를 기반으로 CPU-filter 를 적용 ■ 분류되는 패킷을 match 명령어를 통해 허용할 것인가를 결정
cpu-filter rule *NAME* **tcp { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } { *srcPort* | any } { *dstPort* | any } match { permit | deny }**	■ TCP 프로토콜에 대한 CPU-filter ■ source/destination address 와 source/ destination port 번호에 의한 CPU-filter ■ 분류되는 패킷을 match 명령어를 통해 허용할 것인가를 결정
cpu-filter rule *NAME* **udp { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } { *srcPort* | any }**	■ UDP 프로토콜에 대한 CPU-filter ■ source/destination address 와 source/

{ *dstPort* **| any } match { permit | deny }**	destination port 번호에 의한 CPU-filter ■ 분류되는 패킷을 match 명령어를 통해 허용할 것인가를 결정

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

명령어	설명
no cpu-filter rule *NAME*	■ NAME : 설정된 CPU-filter 의 이름

16.1.2. CPU-FILTER Group 설정

CPU-Filter 를 시스템에 적용하기 위해서는 CPU-Filter rule 를 CPU-Filter group 에 추가하여야 한다. Premier 8624XG 스위치에는 Input group 과 Output group 의 두 종류 group 을 설정할 수 있다. Input group 은 시스템 자체로 들어오는 트래픽에 대한 filter group 이며, forward group 은 스위치의 CPU 를 통해 라우팅되는 트래픽에 대한 filter group 이다. CPU-Filter group 에는 여러 개의 rule 이 적용될 수 있으며, group 에 추가되는 순서대로 rule 이 적용되므로, rule 적용 순서가 중요한다. 또한, 두 종류의 CPU-Filter group 이 지원되며, 적용된 순서는 **show cpu-filter group** 을 통해 확인할 수 있다.

16.1.2.1. INPUT Group 설정/해제

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

명령어	설명
cpu-filter group input add *NAME*	■ NAME : 추가할 rule 의 이름
cpu-filter group input add *NAME1* **{ above | below }** *NAME2*	■ Group 에 이미 삽입된 rule 과 상대적인 위치에 새로운 rule 삽입 ■ NAME1 : 그룹에 새로 삽입 할 rule 의 이름 ■ NAME2 : 이미 Group 에 삽입되어 있는 rule 이름 ■ above : NAME2 의 위에 NAME1 삽입 ■ below : NAME2 의 아래에 NAME1 삽입

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

명령어	설명
cpu-filter group input delete *NAME*	■ NAME : Group 으로부터 삭제할 rule 의 이름

cpu-filter group input delete all	■ Group 에 속한 모든 rule 삭제

16.1.2.2. FORWARD Group 설정/해제

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

명령어	설명
cpu-filter group forward add *NAME*	■ NAME : forward group 에 추가할 rule 의 이름
cpu-filter group forward add *NAME1* **{ above | below }** *NAME2*	■ Group 에 이미 삽입된 rule 과 상대적인 위치에 새로운 rule 삽입 ■ NAME1 : 그룹에 새로 삽입 할 rule 의 이름 ■ NAME2 : 이미 Group 에 삽입되어 있는 rule 이름 ■ above : NAME2 의 위에 NAME1 삽입 ■ below : NAME2 의 아래에 NAME1 삽입

16.1.2.3. CPU-FILTER service 의 활성화

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

명령어	설명
service cpu-filter	■ CPU-FILTER 의 활성화
no service cpu-filter	■ CPU-FILTER 의 비활성화

16.1.3. CPU-FILTER 의 설정 예

다음은 스위치로 들어오는 모든 TELNET 을 허용하지 않도록 설정하는 예이다.

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

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

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

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

다음은 스위치에 설정된 CPU-FILTER group 의 조회를 나타낸다.

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

다음은 스위치에 설정된 CPU-FILTER rule 의 조회를 나타낸다.

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

16.2. IP OPTOIN 개요

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

16.3. IP OPTOIN 명령어

IP OPTION 명령으로 설정 가능한 parameter 들은 다음과 같다.

표 18.1 IP OPTION 명령어

명령어	설명	모드
ip option secure_redirect *INTERFACE* **(***default*|*disable*|*enable***)**	디폴트 게이트웨이 목록에 있는 게이트웨이에만 ICMP 리다이렉트 메시지를 전달, 차단. Default) enable	config
ip option send_redirects *INTERFACE* **(***default*|*disable*|*enable***)**	라우터 기능으로 동작시 다른 호스트로 ICMP 리다이렉트 전달,차단. Default) enable	config
ip option icmp_port_unreach *INTERFACE* **(***default*|*disable*|*enable***)**	Icmp port unreachable 허용,차단 Default) disable	config
ip option icmp_host_unreach *INTERFACE* **(***default*|*disable*|*enable***)**	Icmp host unreachable 허용,차단 Default) disable	config
ip option icmp_net_unreach *INTERFACE* **(***default*|*disable*|*enable***)**	Icmp net unreachable 허용,차단 Default) disable	config
ip option icmp_prot_unreach *INTERFACE* **(***default*|*disable*|*enable***)**	Icmp prot unreachable 허용,차단 Default) disable	config
ip option tcp_max_syn_backlog *VALUE*	Tcp syn backlog queue 의 최대치 설정 Default) 1024	config
ip option ip_default_ttl *VALUE*	Default TTL 크기 설정 Default) 64	config
ip option ipfrag_time *VALUE*	플래그멘테이션 된 IP 데이터를 메모리에 갖고 있는 시간 설정 Default) 30	config
ip option tcp_syn_retries *VALUE*	활성 TCP 연결에서 재전송을 위해 지정한 시간만큼 지난 뒤에 초기화 SYN 패킷을 보냄 Default) 5	config
ip option tcp_retries1 *VALUE*	의심스러운 tcp session 에 대한 재전송 횟수 설정 Default) 3	config
ip option tcp_retries2 *VALUE*	종단전 재전송 횟수 Default)15	config
ip option tcp_keepalive_time *VALUE*	keepalive 가 활성화되었을 시 keepalive time 설정 Default) 7200	config
ip option tcp_fin_timeout *VALUE*	FIN-WAIT-2 상태의 소켓 유지 시간 설정 Default) 60	config
ip option tcp_max_tw_buckets *VALUE*	timewait 소켓의 수 설정 Default) 18700	config
ip option tcp_keepalive_probes *VALUE*	연결이 끊어졌다고 여길 때까지 발생 시킬 keepalive probe 메시지 Default) 9	config
ip option tcp_syncookies (*default*|*disable*|*enable***)**	syn flood attack 방어를 위한 설정 Default) enable	config
ip option tcp_send_reset (*default*|*disable*|*enable***)**	Tcp send reset 플래그 설정,해제 Default) enable	config
(no) ip option icmp-ttl-exceed-send	TTL Exceed ICMP 전송 허용, 차단	config

	Default) send	

17 VRRP

(Virtual Router Redundancy Protocol)

Virtual Router Redundancy Protocol (VRRP)는 LAN 에서 여러 개의 접근 경로를 제공하기 위해 여러 라우터가 동일한 가상 IP 주소를 가지도록 허용하고, 그 중 한 라우터를 가상 라우터로 선출하는 프로토콜이다. VRRP 라우터는 LAN 에 연결된 다른 라우터와 통신하기위해 VRRP 프로토콜을 사용한다. VRRP 설정에서, 한 라우터가 마스터 가상 라우터로 선출되면 나머지 라우터들은 마스터 가상 라우터의 장애에 대비해 backup 으로 동작한다.

17.1. Information About VRRP

17.1.1. VRRP Operation

LAN 클라이언트가 특정 목적지에 대한 first hop 라우터를 선택하는 방법은 여러 가지가 있다. 클라이언트는 동적 절차나 정적 설정을 사용할 수 있다. 동적으로 라우터를 결정하는 방법의 예는 다음과 같다:

- Proxy ARP – 클라이언트는 자신의 목적지를 알기 위해 Address Resolution Protocol (ARP)를 사용하고, 라우터는 자신의 MAC 주소를 사용해서 ARP request 에 응답한다.
- Routing protocol – 클라이언트는 dynamic 라우팅 프로토콜의 업데이트 정보를 이용해서 자신의 라우팅 테이블을 구축한다.
- IRDP (ICMP Router Discovery Protocol) client – 클라이언트는 Internet Control Message Protocol (ICMP) router discover 클라이언트를 실행한다.

LAN 클라이언트에 대한 설정과 프로토콜 동작에 대한 부담이 동적 프로토콜의 단점이다. 또한 라우터에 장애가 발생했을 때, 다른 라우터로의 절체가 느려질 수 있다.

동적 프로토콜에 대한 대안은 클라이언트에 default 라우터를 정적으로 설정하는 것이다. 이 방법은 클라이언트의 설정과 동작이 간단하다. 그러나 default gateway 에 장애가 발생하면, LAN 클라이언트는

외부 네트워크와의 통신이 단절된다.

VRRP 는 정적 설정 문제를 해결할 수 있다. VRRP 는 라우터의 그룹이 하나의 가상 라우터를 형성하도록 한다. LAN 클라이언트는 가상 라우터를 자신의 default gateway 로 설정한다. 라우터의 그룹을 표현하는 가상 라우터를 VRRP 그룹이라고 표현하기도 한다.

그림 1 은 VRRP 가 설정된 LAN 형상을 나타낸다. 이 예제에서 라우터 A, B 그리고 C 가 가상 라우터를 구성하는 VRRP 라우터 (VRRP 를 실행하는 라우터)이다. 가상 라우터의 IP 주소는 라우터 A 의 IP 주소 (10.0.0.1)과 동일하게 설정한다.

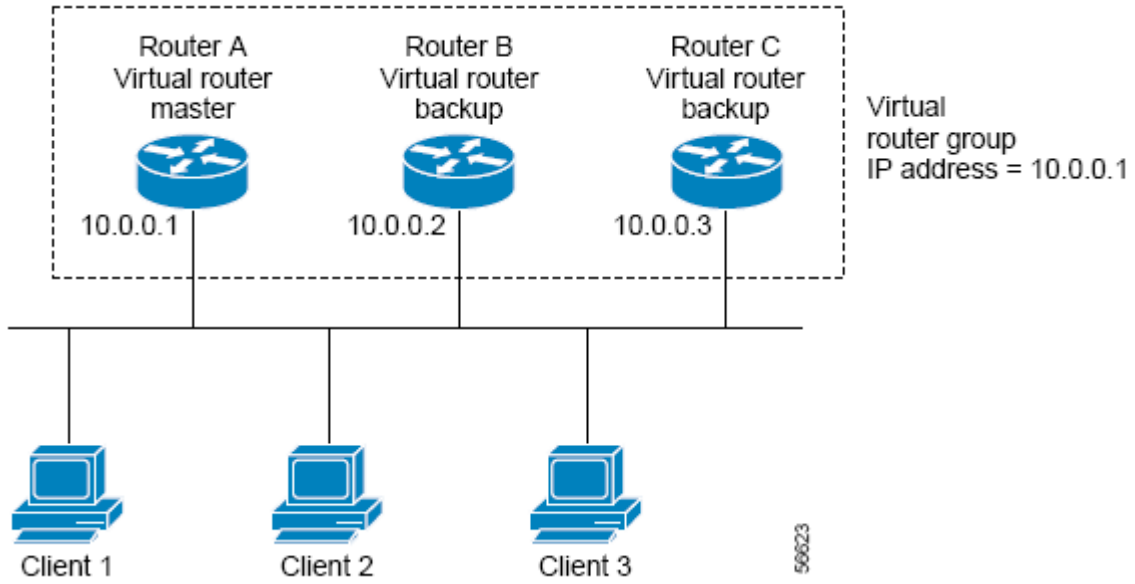


그림 17-1 Basic VRRP Topology

가상 라우터가 라우터 A 의 물리적 주소를 사용하기 때문에, 라우터 A 가 마스터 가상 라우터 의 역할을 담당하고 IP address owner 라 부른다. 라우터 A 는 마스터 가상 라우터로써 가상 라우터의 IP 주소를 제어하고, 이 IP 주소로 전달된 패킷의 포워딩을 담당한다. Client 1 부터 3 은 default gateway 의 IP 주소를 10.0.0.1 로 설정한다.

라우터 B 와 C 는 백업 가상 라우터로 동작한다. 만약 마스터 가상 라우터에 장애가 발생하면, 높은 우선 순위를 가진 라우터가 마스터 가상 라우터가 되어 LAN 호스트들에게 계속 서비스를 제공한다. 라우터 A 가 복구되면, 다시 마스터 가상 라우터가 된다.

그림 2 는 라우터 A 와 B 가 트래픽을 공유하도록 VRRP 를 설정한 예를 보여준다. 라우터 A 와 B 는 서로에 대한 백업 가상 라우터로 동작한다.

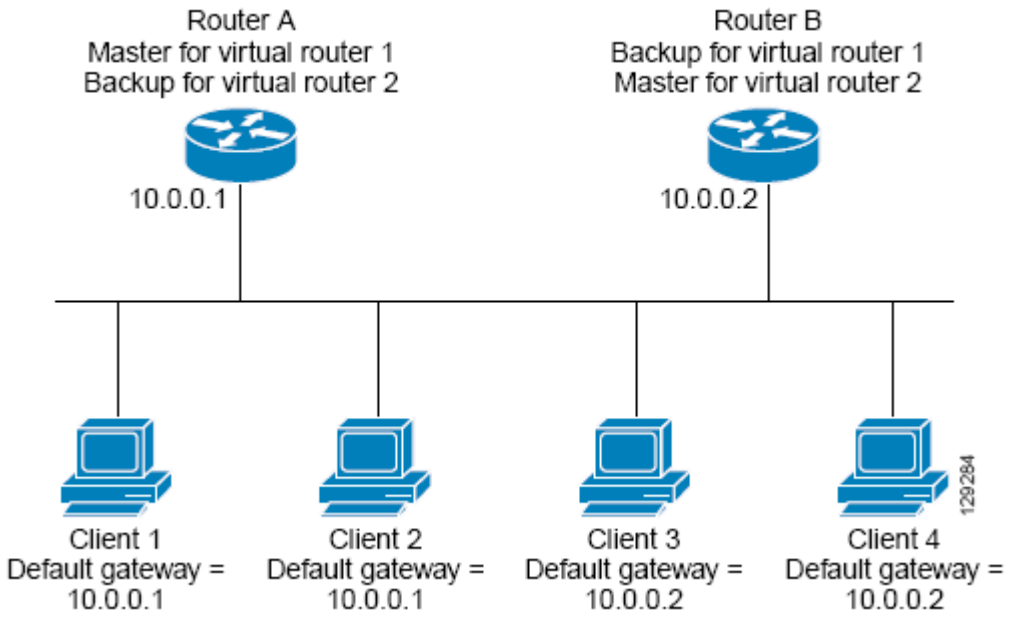


그림 17-2 Load Sharing and Redundancy VRRP Topology

이 형상에서 두 개의 가상 라우터가 설정된다. 가상 라우터 1 에서 라우터 A 가 IP 주소 10.0.0.1 의 주인이자 마스터 가상 라우터이며, 라우터 B 는 라우터 A 에 대한 백업 가상 라우터이다. 클라이언트 1 과 2 는 default gateway 의 IP 주소로 10.0.0.1 을 사용한다.

가상 라우터 2 에서 라우터 B 가 IP 주소 10.0.0.2 의 주인이자 마스터 가상 라우터이며, 라우터 A 는 라우터 B 에 대한 백업 가상 라우터이다. 클라이언트 3 과 4 는 default gateway 의 IP 주소로 10.0.0.2 를 사용한다.

17.1.2. VRRP Benefits

Redundancy
VRRP 는 default gateway 라우터로 여러 개의 라우터를 사용할 수 있게 해준다. 이것은 네트워크의 단일 지점 장애에 대한 위험을 낮춰준다.

Load Sharing
LAN 클라이언트로부터의 트래픽이 여러 라우터에게로 분산되도록 VRRP 를 설정할 수 있다. 이렇게 함으로써 트래픽에 대한 부담을 여러 라우터들에게 분산시킬 수 있다.

Multiple Virtual Routers
VRRP 는 최대 255 개의 가상 라우터 (VRRP 그룹)을 지원한다. 다수의 가상 라우터를 지원함으로써 LAN 구성에서 redundancy 와 load sharing 의 지원이 가능하다.

Preemption
VRRP 의 redundancy scheme 은 높은 우선 순위의 라우터가 사용 가능하게 되었을 때, 백업 가상 라

우터를 대신해서 마스터 가상 라우터가 되는 것을 허용한다.

Advertisement Protocol
VRRP 는 전용의 Internet Assigned Numbers Authority (IANA) 표준 멀티캐스트 주소 (224.0.0.18)를 VRRP advertisement 에 사용한다. IANA 는 VRRP 에게 IP 프로토콜 번호 112 를 할당한다.

VRRP Object Tracking
VRRP object tracking 은 인터페이스 또는 IP route 의 상태에 따라 VRRP 우선 순위를 변경해서, 최적의 VRRP 라우터가 마스터 가상 라우터가 될수 있도록 지원한다.

17.1.3. Multiple Virtual Rouer Support

라우터의 물리 인터페이스에 최대 255 개의 가상 라우터를 설정할 수 있다. 라우터가 지원할 수 있는 실제 가상 라우터의 개수는 다음의 요인에 영향을 받는다:

- 라우터의 프로세스 능력
- 라우터의 메모리 용량
- 라우터의 인터페이스가 제공할 수 있는 최대 MAC 주소 개수

17.1.4. VRRP Router Priority and Preemption

VRRP 이중화 기능에서 중요한 요소는 VRRP 라우터 우선 순위이다. 마스터 가상 라우터에 장애가 발생했을 때, 우선 순위로써 VRRP 라우터의 역할을 결정한다.

만약 VRRP 라우터가 가상 라우터의 IP 주소를 자신의 물리 인터페이스의 IP 주소로 가지고 있다면, 이 라우터는 마스터 가상 라우터로 동작한다.

또한 우선 순위는 마스터 가상 라우터에 장애가 발생했을 때, 백업 가상 라우터로 동작중 인 VRRP 라우터 중에서 마스터 가상 라우터를 선출하는 기준이 된다. **vrrp priority** 명령을 사용해서 백업 가상 라우터의 우선 순위를 1 ~ 254 범위로 설정할 수 있다.

예를 들어, LAN 에서 마스터 가상 라우터인 라우터 A 에 장애가 발생했다면, 선출 프로세스는 백업 가상 라우터 B 와 C 중에서 마스터를 선출해야 한다. 라우터 B 와 C 의 우선 순위가 각각 101 과 100 으로 설정되어 있다면, 라우터 B 의 우선 순위가 더 높으므로 라우터 B 가 마스터 가상 라우터가 된다. 만약 라우터 B 와 C 의 우선 순위가 똑같이 100 으로 설정되었다면, 높은 IP 주소를 가진 백업 가상 라우터가 마스터 가상 라우터로 선출 된다.

높은 우선 순위의 백업 가상 라우터가 마스터 가상 라우터가 될 수 있도록 preemptive scheme 가 적용된다. **no vrrp preempt** 명령을 사용해서 preemptive scheme 를 중지시킬 수 있다. Preemption 이 비활성화 되면, 마스터 가상 라우터가 된 백업 가상 라우터는 원래의 마스터 가상 랑우터가 복구되어 마스터가 될 때까지 계속 마스터의 역할을 수행한다.

17.1.5. VRRP Advetisements

마스터 가상 라우터는 같은 그룹의 다른 VRRP 라우터에게 VRRP advertisement 를 전송한다. Advertisement 에는 마스터 가상 라우터의 우선 순위와 상태 정보가 포함된다. VRRP advertisement 는 IP 패킷으로 만들어져서, VRRP 그룹에 할당된 IPv4 멀티캐스트 주소로 전송된다. Default 로 매 1 초마다 advertisement 가 전송되며, 전송 주기는 설정 가능한다.

17.1.6. VRRP Object Tracking

Object tracking 은 인터페이스의 line-protocol 상태와 같은 객체를 생성하고 모니터링하며, 제거를 관리하는 독립된 프로세스이다. VRRP 와 같은 클라이언트는 상태의 변화를 알고 싶은 객체를 등록한다.

추적할 객체는 tracking comman-line-interface (CLI)에 의해 유일한 번호를 할당 받는다. VRRP 와 같은 클라이언트 프로세스는 이 번호를 사용해서 추적할 객체를 명시한다.

Tracking 프로세스는 주기적으로 객체의 상태를 검사하고 상태 값의 변화를 클라이언트에게 알려준다. 객체의 상태 값은 up 또는 down 으로 표시된다.

Tracking 프로세스를 통해 VRRP 는 모든 객체의 상태 변화를 추적할 수 있다. Tracking 프로세스는 인터페이스의 line protocol 상태, route 의 도달 가능성 등 각 객체의 상태 추적 기능을 제공한다.

각 VRRP 그룹은 VRRP 라우터의 우선 순위에 영향을 미치는 여러 객체를 추적할 수 있다. 추적할 객체 번호를 명시하면 VRRP 는 그 객체의 상태 변화를 감지하게 된다. VRRP 는 추적하는 객체의 상태에 따라 가상 라우터의 우선 순위 값을 감소 시키거나 증가 시킨다.

17.2. How to Configure VRRP

이 장에서는 다음과 같은 절차를 설명한다:

- Enabling VRRP
- Disabling VRRP on an Interface
- Configuring VRRP Object Tracking

17.2.1. Enabling VRRP

VRRP 를 작동시키려면 다음의 작업을 수행한다.

	Command or Action	Purpose
Step 1	**configure terminal** 예제: Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**interface** *interface-name* 예제: Switch(config)# **interface vlan1**	Interface configuration 모드로 진입한다.
Step 3	**ip address** *ip-address/prefix-length* 예제: Switch(config-if-vlan1)# **ip address 172.16.6.5/24**	인터페이스에 IP 주소를 설정한다.
Step 4	**vrrp** *group* **ip address** *ip-address* 예제: Switch(config-if-vlan1)# **vrrp 10 ip 172.16.6.5**	인터페이스에 VRRP 를 작동시킨다. **주의:** VRRP 그룹의 모든 라우터들은 같은 IP 주소로 설정해야 한다. 다른 IP 주소가 설정되면, VRRP 그룹의 라우터들은 서로 통신을 할 수 없게 되고, 잘못 설정된 라우터는 자신이 마스터로 동작한다.
Step 5	**end** 예제: Switch(config-if-vlan1)# **end**	privileged EXEC 모드로 돌아간다
Step 6	**show vrrp** [**brief** | *group*] 예제: Switch# **show vrrp 10**	(옵션) 라우터의 VRRP 그룹의 상태 정보를 조회한다.
Step 7	**show vrrp interface** *interface-name* [**brief**] 예제: Switch# **show vrrp interface vlan1**	(옵션) 특정 인터페이스에 설정된 VRRP 그룹의 정보를 조회한다.

17.2.2. Disabling VRRP on an Interface

인터페이스의 VRRP 를 중단시킴으로써 VRRP 설정은 유지하고 프로토콜 동작만 중지하는 것이 가능하다.

show running-config 명령으로 조회했을 때, VRRP 그룹의 설정 상태와 VRRP 가 동작하는지 중단되었는지를 확인할 수 있다.

	Command or Action	Purpose
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**interface** *interface-name* **예제:** Switch(config)# **interface *vlan1***	Interface configuration 모드로 진입한다.
Step 3	**ip address** *ip-address/prefix-length* **예제:** Switch(config-if-vlan1)**# ip address 172.16.6.5/24**	인터페이스에 IP 주소를 설정한다.
Step 4	**vrrp** *group* **shutdown** **예제:** Switch(config-if-vlan1)# **vrrp 10 shutdown**	인터페이스의 VRRP 를 중단시킨다. **주의:** VRRP 설정은 유지한채 VRRP 를 중단시킬 수 있다.

17.2.3. Configuring VRRP Object Tracking

VRRP object trackingg 을 설정하려면 다음의 작업을 수행하라.

VRRP 그룹이 IP 주소의 소유주라면, VRRP 그룹의 우선 순위는 255 로 고정되고 object tracking 을 통해 우선 순위가 변경되지 않는다.

	Command or Action	Purpose
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**track** *object-number* **interface** *interface-name* { **line-protocol | ip routing** } **예제:** Switch(config)# **track 2 interface vlan1 line-protocol**	인터페이스의 상태가 VRRP 그룹의 우선 순위에 영향을 미치는 인터페이스를 설정한다. - 이 명령으로 인터페이스를 설정하고 **vrrp track** 명령에서는 대응되는 object 번호가 사용된다. - **line-protocol** 키워드는 인터페이스의 상태가 up 인가를 추적한다. **ip routing** 키워드는 IP 주소가 설정되었고 인터페이스의 상태가 up 인가를 검사한다. - **track ip route** 명령을 사용해서 특정 IP route 의 도달성을 검사할 수도 있다.

Step 3	**interface** *interface-name* **예제:** Switch(config)# **interface vlan10**	Interface configuration 모드로 진입한다.
Step 4	**ip address** *ip-address/prefix-length* **예제:** Switch(config-if-vlan10)# **ip address 10.0.1.1/24**	인터페이스에 IP 주소를 설정한다.
Step 5	**vrrp** *group* **ip address** *ip-address* **예제:** Switch(config-if-vlan10)# **vrrp 10 ip 10.0.1.20**	인터페이스에 VRRP 를 작동시키고 가상 라우터의 IP 주소를 설정한다.
Step 6	**vrrp** *group* **priority** *leve* **예제:** Switch(config-if-vlan10)# **vrrp 10 priority 120**	VRRP 라우터의 우선 순위를 설정한다.
Step 7	**vrrp** *group* **track** *object-number* [**decrement** *priority*] **예제:** Switch(config-if-vlan10)# **vrrp 10 track 2 decrement 15**	VRRP 가 object 의 상태를 추적하도록 설정한다.

17.3. Configuration Examples for VRRP

17.3.1. Configuring VRRP: Example

다음의 예제에서 스위치 A 와 스위치 B 는 3 개의 VRRP 그룹에 포함된다.
각 그룹의 설정은 다음과 같다:

- Group 1:
  - 가상 IP 주소는 10.1.0.10
  - 스위치 A 가 우선 순위 값 120 으로 이 그룹의 마스터가 된다
  - Advertising 주기는 3 초이다.
  - Preemption 이 활성화 되어 있다.
- Group 5:
  - 스위치 B 가 우선 순위 값 200 으로 이 그룹의 마스터가 된다.
  - Advertising 주기는 30 초이다.
  - Perrmption 이 활성화 되어 있다.
- Group 100:
  - 스위치 A 가 가장 높은 IP 주소 (10.1.0.2)를 가지고 있기 때문에, 이 그룹의 마스터가 된다.
  - Advertising 주기는 default 1 초이다.

- Preemption 이 비활성화 되어 있다.

Router A

```
interface vlan1
   ip address 10.1.0.2/8
   vrrp 1 priority 120
   vrrp 1 timers advertise 3
   vrrp 1 ip 10.1.0.10
   vrrp 5 timer advertise 30
   vrrp 5 ip 10.1.0.50
   no vrrp 100 preempt
   vrrp 100 ip 10.1.0.100
```

Router B

```
interface vlan1
   ip address 10.1.0.1/8
   vrrp 1 timers advertise 3
   vrrp 1 ip 10.1.0.10
   vrrp 5 priority 200
   vrrp 5 timer advertise 30
   vrrp 5 ip 10.1.0.50
   no vrrp 100 preempt
   vrrp 100 ip 10.1.0.100
```

17.3.2. VRRP Object Tracking: Example

다음의 예제에서, 인터페이스 vlan10 의 line protocol 상태를 추적하도록 tracking 프로세스가 설정된다. 인터페이스 vlan1 의 VRRP 는 인터페이스 vlan10 의 프로토콜 상태 변환에 대한 정보를 전달받을 수 있도록 tracking 프로세스에 등록한다. 인터페이스 vlan10 의 line protocol 상태가 down 이 되면, VRRP 그룹의 우선 순위 값이 15 만큼 감소한다.

```
track 1 interface vlan10 line-protocol
!
interface vlan1
   ip address 10.0.0.2/8
   vrrp 1 ip 10.0.0.3
   vrrp 1 priority 120
   vrrp 1 track 1 decrement 15
```

17.3.3. VRRP Object Tracking Verification: Example

다음의 예제는 “VRRP Object Tracking: Example” 절에서의 설정을 확인한다:

Switch# **show vrrp**

vlan1 – Group 1
State is Master
Virtual IP address is 10.0.0.3
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1 sec
Preemption is enabled
Priority is 105
Track object 1 state Down decrement 15
Master Router is 10.0.0.2 (local) priority is 105
Master Advertisement interval is 1 sec
Master Down interval is 3.531 sec

Switch# **show track**

Track 1
Interface vlan10 line-protocol
Line protocol is Down (hw down)
1 change, lasst change 00:06:53
Tracked by:
VRRP vlan1 1

17.3.4. Disabling a VRRP Group on an Interface: Example

다음의 예는 인터페이스 VRRP 그룹의 설정을 유지하면서 인터페이스 vlan1 의 VRRP 그룹을 중지시키는 방법을 보여준다:

interface vlan1
ip address 10.24.1.1/24
vrrp1 ip 10.24.1.254
vrrp 1 shutdown

18 Utilities

18.1. 개 요

본 장에서는 시스템 운영에 필요한 기타 기능들에 대해 설명하도록 한다.

18.2. 상태 dump 명령

18.2.1. 명령어

각 모듈들(시스템 환경, MULTICAST, 라우팅, 드라이버 등)의 시스템 로깅 메시지를 dump 하기 위한 목적으로 “show tech” 명령을 사용한다.

```
# show tech
```

시스템 운영 시 문제가 발생했을 경우, 기존에는 여러 명령을 입력하여 모듈들의 동작 상태를 확인해야 하는 번거로움이 있었지만, 이 명령을 사용함으로써, 미리 정의해 놓은 모듈들의 주요 명령들이 수행되어 그 결과 메시지가 출력되기 때문에, 각 모듈 담당자들이 이 메시지를 통해 좀 더 빠르게 확인할 수 있다.

출력 메시지는 페이징이 되지 않기 때문에, 출력 메시지는 명령의 수행이 끝날 때까지 출력된다. 이 명령의 수행 도중에, 출력을 멈추기 위해서는 Ctrl+C 를 입력하여 중단시켜야 한다.

다음의 예를 살펴보도록 하자.
Show tech 명령의 수행은 CPU 에 상당한 부하를 가하기 때문에, 처리시간도 길다.
CPU 가 100% 지속됨에 따라 라우팅 끊김 현상이 발생할 수 있기 때문에, 다음과 같이 운용자에게 다시 한번 명령을 수행할 것인지에 대한 confirm 을 요청한다.

```
Switch# show tech

NOTICE !!!
 This may take a few minutes and may take up the CPU resources!!
continue to process [yes/no]?y

================================================================================
                          Display the system information
================================================================================
Model Name         : P8624XGB
Main Memory Size   : 256 MB
Flash Memory Size  : 32 MB
H/W Revision       : Rev 9.1
H/W Address        : 00:07:70:a4:36:a9
RTC Information    : Installed
Serial Number      : P25M05171234

================================================================================
                           Display the system version
================================================================================

P8624XGB Software Version 1.4.1h
Copyright (c) 2001-2008 by Ubiquoss Inc.

...
================================================================================
                                 CPU information
================================================================================
----------------------------------------
  Average CPU load
----------------------------------------
  5 sec :   1.20%
  1 min :  10.36%
  5 min :   3.50%
----------------------------------------
  cpuload threshold (high) :   0%
  cpuload threshold ( low) :   0%
  cpuload time period      : 1 Minutes
----------------------------------------

================================================================================
                          Current operating configuration
================================================================================
!
vlan 33
vlan 44
vlan 2000
```

```
!
interface gi2
 shutdown
 switchport access vlan 33
!
interface gi3
 switchport access vlan 44
!
interface vlan33
 ip address 33.33.33.2/24
!
interface vlan44
 ip address 44.44.44.2/24
!
interface vlan2000
 ip address 198.19.1.250/24
!
interface eth0
 ip address 192.168.0.144/24
!
interface lo0
 ip address 58.229.2.143/32
!
!
ip igmp snooping
ip igmp snooping vlan 2000
!

...
```

18.3. Command history 기능

운용자에 의해 수행된 명령어를 명령어를 수행한 운용자의 id, ip, 수행된 시간 정보와 함께 출력하는 기능이다.
출력하는 대상은 정상적으로 수행된 명령어에 한하며 “exit”, “end”등과 같이 예측 가능한 명령어는 생략하였다.

표 1. command history 조회 및 설정 명령어

명령어	설명	모드
show history	■ 실행된 명령어들을 조회한다.	Privileged
show history back	■ 실행된 명령어들을 시간의 역순으로 조회한다.	Privileged

show history flash	■ Flash memory 에 저장된 실행된 명령어들을 조회한다. 이 경우 시스템 rebooting 이전에 수행된 명령어들도 조회가능 하다.	Privileged
show history flash back	■ Flash memory 에 저장된 실행된 명령어들을 시간의 역순으로 조회한다. 이 경우 시스템 rebooting 이전에 수행된 명령어들도 조회가능 하다.	Privileged
clear history	■ 실행된 명령어들의 리스트를 초기화한다.	Privileged
clear history flash	■ Flash memory 에 저장된 실행된 명령어들의 리스트를 초기화한다.	Privileged
history flash {enable|disable}	■ Flash memory 에 실행된 명령어 저장 여부를 결정한다. Default 는 enable 상태이다.	Config

명령어의 실효성을 높이기위해 시스템이 다운되거나 reboot 되더라도 조회가능하도록 flash 에 저장하도록 하였으며 default 상태는 enable 상태이므로 특별이 disable 되지 않으면 flash memory 에 저장되게 된다.
이 기능을 통해 운용자에 의해 수행된 과거 이력 조회가 가능하며 시스템 오동작시 원인 규명 및 복원이 편리하게 된다.
또한, 같은 명령어를 반복하여 입력하는 경우는 한번만 저장된다.

18.4. Output Post Processing

18.4.1. output post processing 개요

장비의 현재 상태 또는 설정을 보는 명령어는 대부분 show 로 시작한다. show 명령은 대부분 한 화면에 보기 편하게 정리해서 보여주는 것이 일반적이나, 그 내용이 방대한 경우도 상당히 많다.
예를 들면, show mac-address-table 명령의 경우 수천 라인의 정보가 보여 질 수 있으며, show interface 명령의 경우에도 상당히 많은 분량의 내용이 출력된다. 출력되는 내용이 많을 경우, 이 내용 중에서 원하는 부분을 찾는 것은 쉽지 않다. 이럴 때 본 장비에서 지원하는 output post processing 기능을 사용하면 편리하다.
일반적으로 유닉스에서 pipe 라고 부르는 기능과 비슷하며, 본 장비에서는 3 가지의 미리 정의된 output post processing 을 지원한다. Output post processing 기능을 사용하기 위해서는 show 명령 이후 bar (|) 를 이어 붙이고, 다음의 명령어를 사용하면 된다.

명령어	설명
| include WORD	■ 특정 단어를 포함하는 문자열을 출력한다.
| exclude WORD	■ 특정 단어를 포함하지 않는 문자열을 출력한다.
| begin WORD	■ 특정 단어를 포함하는 문자열부터 그 이후에 나오는 모든 라

인을 출력한다.

18.4.2. output post processing 예제

show mac-address-table 명령은 상당한 양의 결과를 출력하는데, 그 중 원하는 부분이 포함된 mac 주소만 출력하고자 할 때는 **include** 를 사용한다.

```
Switch#
Switch# show mac-address-table | include 0007.70
     2    gi1  0007.7089.1123 0-0  F-F  UD.
     3    gi2  0007.709e.000b 0-0  F-F  UD.
    13    gi3  0007.701e.4dac 0-0  F-F  UD.
    13    gi4  0007.7089.1123 0-0  F-F  UD.
    13    gi5  0007.7092.40f6 0-0  F-F  UD.
    13    gi6  0007.7093.cca2 0-0  F-F  UD.
    13    gi7  0007.709e.1000 0-0  F-F  UD.
    13    gi8  0007.709f.5934 0-0  F-F  UD.
    20    gi9  0007.7042.0001 0-0  F-F  UD.
Switch #
```

show ip interface 명령은 상당한 양의 결과를 출력하는데, 그 중 특정 vlan 인터페이스 이후의결과 만을 원할 때는 begin 을 사용한다.

```
Switch#
Switch# show ip interface | begin vlan10
vlan10 is up
 type: vlan interface
 ip address: 10.1.10.1/24 broadcast address 10.1.10.254

 Cpu packet counters since creation
   4 packets input, 208 bytes
   Received 4 unicasts, 0 non-unicasts
   0 dropped, 0 errors
   6 packets output, 309 bytes

vlan11 is up
 type: vlan interface
 ip address: 10.1.11.1/24 broadcast address 10.1.11.255

 Cpu packet counters since creation
   1,057,364 packets input, 54,984,438 bytes
   Received 1,160 unicasts, 1,056,204 non-unicasts
   156 dropped, 0 errors
   6,560 packets output, 311,183 bytes
(하략)

Switch #
```

18.5. DDM(Digital Diagnostic Monitoring)

P8K 는 DDM 을 지원하는 GBIC 의 상태를 상세하게 사용자에게 보여주는 명령어를 지원하며 GBIC Port 의 Monitoring 항목이 설정된 임계 값(Threshold)의 범위를 넘었을 경우 이를 사용자에게 통보 할 수 있도록 임계 값 범위를 설정할 수 있다. Monitoring 항목은 다음과 같다.

항목	설명	임계값 설정범위
온도	GBIC Port 온도	-128°C ~ 128°C
전압	GBIC Port 전압	0V ~ 6.55V
전류	GBIC Port 전류	0mA ~ 131mA
RxPower	GBIC Port 광 입력 세기	- 40dBm ~ 8.0dBm
TxPower	GBIC Port 광 출력 세기	- 40dBm ~ 8.0dBm

각 검사항목마다 Alarm/Warning 2 단계의 임계 값 범위를 가질 수 있으며 스위치는 5 분을 주기로 각 GBIC port 의 상태를 검사하여 사용자가 설정한 임계 값 범위를 벗어난 항목을 사용자에게 통보한다.

18.5.1. DDM Monitoring enable/disable (명령어 없음)

기본적으로 P8K Switch 의 DDM Monitoring 기능은 꺼져있다. DDM 기능을 통해 GBIC 의 상태를 일정 간격으로 LOG 에 표시하려면 DDM Monitoring 기능이 활성화 되어 있어야 한다.

명령어	Mode	설명
gbic-ddm alarm enable	Config	DDM Monitoring 기능을 활성화 한다.
gbic-ddm alarm disable	Config	DDM Monitoring 기능을 비활성화 한다.

```
Router# configure terminal
Router(config)# gbic-ddm alarm enable
Router(config)# gbic-ddm alarm disable
```

DDM Monitoring 기능이 꺼져있는 상태에서도 임계값 범위를 설정하고 GBIC 의 Monitoring 항목의 현재 값을 확인할 수 있다.

18.5.2. GBIC 상태 확인

DDM 을 지원하는 gbic 에 한해 다음 명령어를 사용하여 gbic 의 현재 상태를 확인할 수 있다.

명령어	Mode	설명
show port status gbic-ddm	Privileged	DDM 을 지원하는 gbic 의 상태를 확인한다.

```
Router# show port status gbic-ddm
-------------------------------------------------------------------------------------------------
 ifname gbic    ddm        Temperature      Voltage       Bias Current      Tx Power        Rx Power
                             (state)         (state)         (state)         (state)         (state)
                (warn)    high    low      high    low     high    low     high    low     high    low
               (alarm)    high    low      high    low     high    low     high    low     high    low
-------------------------------------------------------------------------------------------------
 gi1     gbic   ddm           48.5'C          3.5 V          21.7 mA        -6.00 dBm      -40.00 dBm
                             Normal          Normal          Normal         Alarm(H)         Normal
                (warn)  127.0 -128.0      6.6     0.0   131.0     0.0  -12.73 -40.00  -12.73 -40.00
               (alarm)  127.0 -128.0      6.6     0.0   131.0     0.0  -12.73 -40.00  -12.73 -40.00
.................................................................................................
 gi2     .
```

18.5.3. DDM Monitoring 값 설정.

사용자는 개별 GBIC 마다 Alarm/Warning 통보를 위한 임계값 범위를 설정할 수 있다. 설정 값은 GBIC 내에 보존되므로 사용자 configuration 에 반영되지 않으며, GBIC port 를 탈착한 이후에도 보존되어 다음에 다시 GBIC 을 장착할 경우 자동적으로 반영된다.

명령어	Mode	설명
write gbic-ddm-threshold ***<IFNAME>***	Privileged	IFNAME 에 해당하는 GBIC 이 DDM 을 지원할 경우 현재 설정된 온도,전압, 전류, Rx power, Tx power 에 대한 Alarm/Warning 임계값 범위를 보여주고 이를 설정하도록 한다.

```
-------------------------------------------------------------------------------------------------
 ifname gbic   ddm       Temperature     Voltage      Bias Current     Tx Power       Rx Power
                (warn)   high   low     high   low     high   low     high   low     high   low
               (alarm)   high   low     high   low     high   low     high   low     high   low
-------------------------------------------------------------------------------------------------
                (warn)   90.0   -5.0     3.5    3.1    70.0    4.0   -3.00  -9.50   -3.00 -21.02
               (alarm)  100.0  -10.0     3.6    3.0    80.0    2.0   -2.00 -10.50   -2.00 -22.01
-------------------------------------------------------------------------------------------------
Configure Temperature                          [y/n] ? y
    Warning High (128.0'C ~ -128.0'C ) [    90.0'C] ? 128
    Warning Low  (128.0'C ~ -128.0'C ) [    -5.0'C] ? -128
    Alarm   High (128.0'C ~ -128.0'C ) [   100.0'C] ? 128
    Alarm   Low  (128.0'C ~ -128.0'C ) [   -10.0'C] ? -128
Configure Voltage                              [y/n] ? y
    Warning High (  6.55 V ~ 0.00 V  ) [    3.50 V] ? 6.55
    Warning Low  (  6.55 V ~ 0.00 V  ) [    3.10 V] ? 0
    Alarm   High (  6.55 V ~ 0.00 V  ) [    3.60 V] ? 6.55
    Alarm   Low  (  6.55 V ~ 0.00 V  ) [    3.00 V] ? 0
Configure Bias Current                         [y/n] ? y
    Warning High ( 131.0 mA ~ 0.0 mA ) [   70.0 mA] ? 131
    Warning Low  ( 131.0 mA ~ 0.0 mA ) [    4.0 mA] ? 0
    Alarm   High ( 131.0 mA ~ 0.0 mA ) [   80.0 mA] ? 131
    Alarm   Low  ( 131.0 mA ~ 0.0 mA ) [    2.0 mA] ? 0
Configure Tx Power                             [y/n] ? n
Configure Rx Power                             [y/n] ? n
-------------------------------------------------------------------------------------------------
 ifname gbic   ddm       Temperature     Voltage      Bias Current     Tx Power       Rx Power
                (warn)   high   low     high   low     high   low     high   low     high   low
               (alarm)   high   low     high   low     high   low     high   low     high   low
-------------------------------------------------------------------------------------------------
                (warn)  128.0 -128.0     6.6    0.0   131.0    0.0   -3.00  -9.50   -3.00 -21.02
               (alarm)  128.0 -128.0     6.6    0.0   131.0    0.0   -2.00 -10.50   -2.00 -22.01
-------------------------------------------------------------------------------------------------
Do you really want to SAVE [y/n] ? y
```

항목마다 waring / alarm threshold를 순서대로 설정하게 되고 마지막 물음에 'y'를 눌러 입력한 설정을 저장하도록 선택하면 설정이 저장되게 된다.

18.6. CPU Packet Counter

이 장에서는 CPU 로 올라오는 packet 의 종류를 구별하여 count 해 주는 Packet Counter 를 설정하는 방법에 대해 설명한다.

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

18.6.1. CPU Packet Counter 이해

스위치의 cpu 로 수많은 packet 이 들어온다. 때로는 예상하지 못한 packet 이 많이 올라오는 경우도 있다. 이를 모니터링 하기 위해 CPU Packet Counter 를 사용하여 어떤 종류의 packet 이 얼마나 올라오는지 확인할 수 있다.

CPU Packet Counter 는 packet 의 ether type 에 따라, IP protocol 에 따라, TCP port 에 따라, UDP port 에 따라 분류하며, 최근 5 초 동안의 CPU packet count, 최근 1 분 동안의 CPU packet count, 최근 5 분 동안의 CPU packet count 를 보여 준다.

18.6.2. CPU Packet Counter 설정

이 절에서는 스위치에 새로운 packet type 을 추가하거나 삭제하는 방법을 설명한다.

Packet Counter 는 설정된 packet type 에 따라 CPU 로 들어오는 packet 을 분류하며 default 로 설정된 packet type 과 user 에 의해 새로 추가된 packet type 을 지원한다.

18.6.3. Default CPU packet type

CPU Packet Counter 는 default packet type list 를 가지며 이 type 들은 항상 적용되고, list 에서 삭제할 수 없다. Default packet type 은 ethertype, IP protocol, TCP port, UDP port 로 나눌 수 있다.

Ethertype

- ETHERTYPE_IP 0x0800 /* IP protocol */
- ETHERTYPE_ARP 0x0806 /* Addr. resolution protocol */
- ETH_P_IPX 0x8137 /* IPX over DIX */

IP Protocol

- IPPROTO_IP = 0, /* Dummy protocol for TCP */
- IPPROTO_ICMP = 1, /* Internet Control Message Protocol */
- IPPROTO_IGMP = 2, /* Internet Group Management Protocol */
- IPPROTO_TCP = 6, /* Transmission Control Protocol */
- IPPROTO_UDP = 17, /* User Datagram Protocol */
- IPPROTO_IPV6 = 41, /* IPv6-in-IPv4 tunnelling */
- IPPROTO_PIM = 103, /* Protocol Independent Multicast */
- IPPROTO_RAW = 255, /* Raw IP packets */

TCP Port

- 20 : ftp-data
- 21 : ftp
- 22 : ssh
- 23 : telnet
- 25 : smtp
- 42 : nameserver
- 53 : domain
- 80 : www
- 137 : netbios-ns
- 138 : netbios-dgm
- 139 : netbios-ssn
- TCP SYN

UDP Port

- 53 : domain
- 67 : BOOTP server
- 68 : BOOTP client
- 69 : tftp
- 123 : ntp
- 137 : netbios-ns
- 138 : netbios-dgm
- 139 : netbios-ssn
- 161 : snmp
- 162 : snmp-trap

18.6.4. User Added Packet Type

User 가 추가할 수 있는 Packet type 은 default 로 지정된 packet type 을 포함하여 다음과 같이 정해진 수 까지 추가 가능하다. ()안은 default 로 설정된 값이다.

- Ether type : 10 (default 4)
- IP protocol : 15 (default 8)
- TCP/UDP port : 15 (tcp 11, udp 10)

Default 로 설정된 packet type 과는 별도로 사용자의 필요에 의해 새로운 packet type 을 지정하여 count 를 볼 수 있다. 이렇게 추가된 packet type 은 삭제 가능하다.

	Command	Purpose
Step1	Configure terminal	Global configuration 모드로 진입한다.
Step2a	**cpu-packet-counter ethertype** *ETHERTYPE*	새로운 ethertype 추가
Step2b	**cpu-packet-counter ip_protocol** *IP_PROTO*	새로운 IP protocol 추가
Step2c	**cpu-packet-counter tcp_port** *PORT_NUM*	새로운 TCP port 추가
Step2d	**cpu-packet-counter udp_port** *PORT_NUM*	새로운 UDP port 추가
Step3	**end**	Privilideged 모드로 진입한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

다음은 TCP port 222 를 추가하는 것을 보여준다.

```
Switch# configure terminal
Switch(config)# cpu-packet-counter tcp_port 222
Switch(config)# end
Switch#
```

Note Ethertype 은 "unsigned short", IP protocol 은 "unsigned char", TCP/UDP port 는 "unsigned short" 값으로 입력해야 한다.

18.6.5. User Deleted Packet Type

Default 로 설정된 packet type 은 삭제할 수 없다.

	Command	Purpose
Step1	Configure terminal	Global configuration 모드로 진입한다.
Step2a	**no cpu-packet-counter ethertype** *ETHERTYPE*	User 가 입력한 ethertype 삭제
Step2b	**no cpu-packet-counter ip_protocol** *IP_PROTO*	User 가 입력한 IP protocol 삭제
Step2c	**no cpu-packet-counter tcp_port** *PORT_NUM*	User 가 입력한 TCP port 삭제
Step2d	**no cpu-packet-counter udp_port** *PORT_NUM*	User 가 입력한 UDP port 삭제
Step3	**end**	Privilideged 모드로 진입한다.
Step4	**show running-config**	설정 내용을 확인한다.

Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

18.6.6. Displaying CPU Packet Counter

User 에 의해 설정된 packet type 을 조회하려면 privileged EXEC 명령 "show running-config"나 show packet-counter type-list"를 사용하라.

CPU packet counter 조회에 관련된 command 는 다음과 같다.

Command	Purpose
show cpu-packet-counter	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 보여준다.
show cpu counter	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 보여준다.
show cpu-packet-counter *IFNAME*	저정된 interface 의 Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 cpu packet count 를 보여준다.
show cpu-packet-counter bps	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 bps 로 보여준다.
show cpu-packet-counter bps *IFNAME*	저정된 interface 의 Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 cpu packet count 를 bps 로 보여준다.
show cpu-packet-counter pps	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 pps 로 보여준다.
Show cpu counter avg	Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 각 interface 별 cpu packet count 를 pps 로 보여준다.
show cpu-packet-counter pps *IFNAME*	저정된 interface 의 Arp, tcp, udp, icmp, igmp, tcp syn 등의 기본 protocol 에 대한 cpu packet count 를 pps 로 보여준다.
show cpu-packet-counter total	CPU 로 올라온 모든 packet count 를 보여준다.
show cpu-packet-counter ethertype *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 ethertype 별로 보여준다.
show cpu-packet-counter ip_protocol *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 IP protocol 별로 보여준다.
show cpu-packet-counter tcp_port *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 TCP port 별로 보여준다.
show cpu-packet-counter udp_port *IFNAME*	입력된 interface 에서 CPU 로 올라온 모든 packet count 를 UDP port 별로 보여준다.
show cpu-packet-counter type-list	CPU 로 올라오는 모든 packet 을 count 하기 위해 가지고 있는 모든 packet 의 type 을 보여준다.
clear cpu-packet-counter	저장된 모든 cpu packet count 를 clear 한다.

다음 예는 tcp port 에 222 라는 새로운 port 가 등록되었음을 보여준다.

```
Switch# show running-config
!
```

```
packet-counter tcp_port 222
!
Switch#
Switch# show cpu-packet-counter type-list
ethertype               default
--------------------------------------------------------------------------------
     0800( IP)             *
     0806(ARP)             *
     8137(IPX)             *
      STP                  *
ip_proto                default
--------------------------------------------------------------------------------
       1(ICMP)             *
       2(IGMP)             *
       6( TCP)             *
      17( UDP)             *
      41(IPv6)             *
     103( PIM)             *
     255( RAW)             *
tcp_port                default
--------------------------------------------------------------------------------
      20(  ftp-data)        *
      21(       ftp)        *
      22(       ssh)        *
      23(    telnet)        *
      25(      smtp)        *
      42(   namesrv)        *
      53(    domain)        *
      80(       www)        *
     137(  netbi-ns)        *
     138( netbi-dgm)        *
     139( netbi-ssn)        *
     222
udp_port                default
--------------------------------------------------------------------------------
      53(    domain)        *
      67( BOOTP_srv)        *
      68( BOOTP_cli)        *
      69(      tftp)        *
     123(       ntp)        *
     137(  netbi-ns)        *
     138( netbi-dgm)        *
     139( netbi-ssn)        *
     161(      snmp)        *
     162( snmp-trap)        *
Switch#
```

19

Dynamic ARP Inspection

이 장에서는 ARP 패킷을 검사하는 dynamic Address Resolution Protocol (ARP) inspection (DAI) 기능에 대한 설정 방법을 설명한다.

Note 이 장에서 사용되는 명령어에 대한 문법과 사용 방법에 관한 상세한 정보는 command reference 를 참조하라.

이 장은 다음과 같은 내용으로 이루어져 있다:

- DAI에 대한 이해 (Understanding DAI)
- DAI 기본 설정 (Default DAI Configuration)
- DAI 설정 지침과 제약 사항 (DAI Configuration Guidelines and Restrictions)
- DAI 설정 (Configuring DAI)
- DAI 설정 예제 (DAI Configuration Samples)

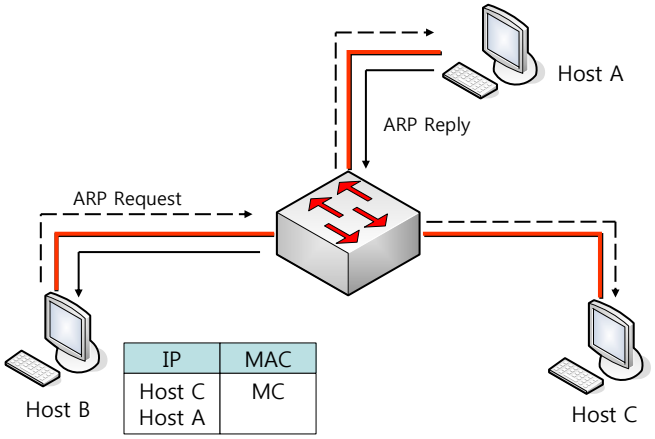
19.1. Understanding DAI

이 절에서는 DAI 에 대한 설명과 DAI 기능을 사용해서 ARP spoofing 공격 attack 을 방어하는 방법에 대해 설명한다. 이 절은 다음과 같은 내용으로 이루어져 있다:

- Understanding ARP
- Understanding ARP Spoofing Attacks
- Understanding DAI and ARP Spoofing Attacks
- Interface Trust States and Network Security
- Rate Limiting of ARP Packets
- Relative Priority of ARP ACLs and DHCP Snooping Entries
- Logging of Dropped Packets

19.1.1. Understanding ARP

ARP 는 IP 주소와 MAC 주소를 매핑 mapping 해서 Layer 2 브로드캐스트 broadcast 도메인에서 IP 통신이 가능하게 한다. 예를 들어, 호스트 B 가 호스트 A 로 정보를 전송하려고 하는데 호스트 B 의 ARP 테이블에 호스트 A 에 대한 MAC 주소가 등록되어 있지 않다고 가정하자.

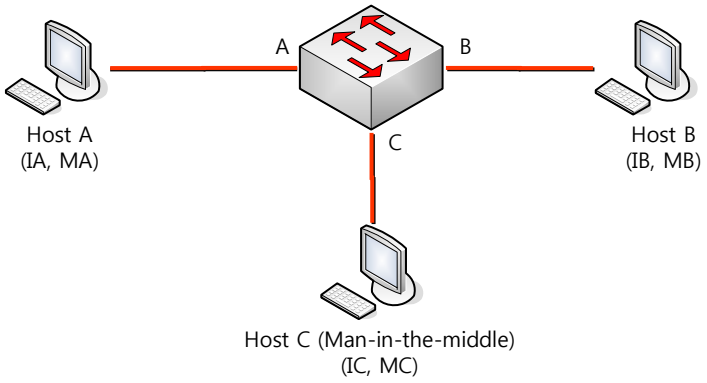


호스트 B 는 호스트 A 의 IP 주소에 대응하는 MAC 주소를 알아내기 위해서, 브로드캐스트 도메인 내부의 모든 호스트들에게 브로드캐스트 메시지 (ARP request)를 전송한다. 브로드캐스트 도메인 내부의 모든 호스트들은 호스트 B 가 전송한 ARP request 를 수신하고, 호스트 A 는 자신의 MAC 주소를 응답한다.

19.1.2. Understanding ARP Spoofing Attacks

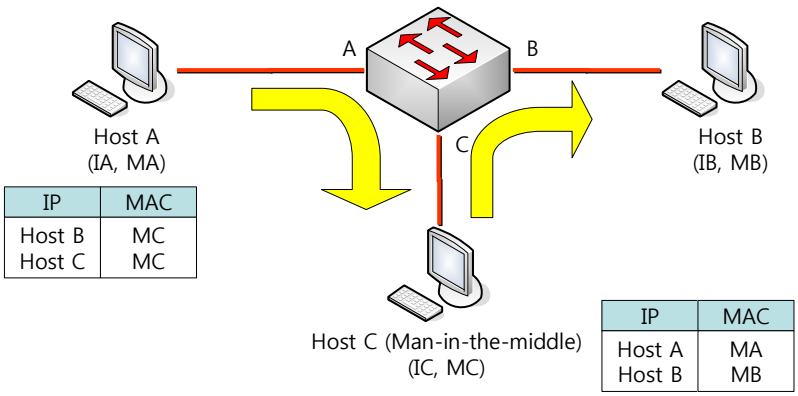
ARP 는 ARP request 를 수신하지 않은 호스트가 전송한 gratuitous reply 로 ARP 테이블이 변경되는 것을 허용한다. 이로 인해 ARP spoofing 공격과 ARP cache poisoning 이 발생할 수 있다. 공격 이후에는 공격 당한 장비의 모든 트래픽은 공격자의 컴퓨터를 통해 라우터, 스위치 또는 호스트로 전달된다.

ARP spoofing 공격은 Layer 2 네트워크에 연결된 호스트, 스위치, 라우터의 ARP 캐시 cache 을 조작한다. 그리고 다른 호스트로 전달되어야 할 트래픽을 가로챈다. 다음의 그림은 ARP cache poisoning 의 예를 보여준다.



호스트 A, B, C 는 각각 스위치의 인터페이스 A, B, C 에 연결되어 있으며, 모두 같은 서브넷에 위치한다. IP 주소와 MAC 주소를 괄호 안에 나타내었다: 예를 들어, 호스트 A 는 IP 주소 IA 와 MAC 주소 MA 를 사용한다. 호스트 A 가 IP 계층에서 호스트 B 와 통신할 필요가 있을 때, IP 주소 IB 와 연관된 MAC 주소를 알기 위해 ARP request 를 브로드캐스트로 전송한다. 스위치와 호스트 B 는 이 ARP request 를 수신하면, IP 주소 IA 와 MAC 주소 MA 를 가진 호스트의 ARP 캐시를 갱신한다: 예를 들어, IP 주소 IA 는 MAC 주소 MA 에 매핑되어 있다. 호스트 B 가 응답하면, 스위치와 호스트 A 는 IP 주소 IB 와 MAC 주소 MB 를 가진 호스트의 ARP 캐시를 갱신한다.

호스트 C 는 IP 주소 IA (또는 IB)에 대한 MAC 주소로 MC 를 사용하는 ARP response 를 브로드캐스트함으로써 스위치, 호스트 A, 호스트 B 의 ARP 캐시를 오염시킬 수 있다. ARP 캐시가 오염된 호스트들은 IA 또는 IB 로 향하는 트래픽의 목적지 MAC 주소로 MC 를 사용하게 된다. 이것은 호스트 C 가 트래픽을 가로챈다는 것을 의미한다. 호스트 C 는 IA, IB 와 연관된 진짜 MAC 주소를 알고 있기 때문에, 올바른 MAC 주소를 목적지 MAC 주소로 사용해서 가로챈 트래픽을 원래 호스트들에게로 포워딩 forwarding 한다. 호스트 C 는 호스트 A 와 호스트 B 의 트래픽 사이에 자신을 집어 넣게 되고, 이런 형상을 *man-in-the middle* attack 이라 한다.



19.1.3. Understanding DAI and ARP Spoofing Attacks

DAI 는 ARP 패킷을 검사하는 보안 기능이다. DAI 는 유효하지 않은 IP-to-MAC 주소 binding 을 가

진 ARP 패킷을 로깅 logging 하고, 폐기 drop 한다. 이 기능은 main-in-the-middle attack 으로부터 네트워크를 보호한다.

DAI 는 ARP 테이블이 오직 유효한 ARP request 와 response 에 의해 변경되도록 동작한다. DAI 기능이 활성화된 스위치는 다음과 같이 동작한다:

- untrusted 포트로 수신한 모든 ARP 패킷을 검사한다.
- 자신의 ARP 캐시를 변경하기 전에, 수신한 패킷이 유효한 IP-to-MAC 주소 binding 을 가지고 있는지 검사한다.
- 유효하지 않은 ARP 패킷을 폐기한다.

DAI 는 ARP 패킷의 유효성을 검사할 때, 신뢰할 수 있는 데이터베이스 database 인 DHCP snooping binding 데이터베이스에 저장된 IP-to-MAC 주소 binding 을 사용한다.

Note 스위치와 VLAN 에 DHCP snooping 이 활성화 되어 있을 때, DHCP snooping 에 의해 DHCP snooping binding 데이터베이스가 생성된다.

ARP 패킷을 수신한 인터페이스의 특성에 따라 스위치는 다음과 같이 동작한다:

- trusted 인터페이스로 수신한 ARP 패킷은 검사하지 않는다.
- untrusted 인터페이스에 대해서는 오직 유효한 패킷만 허용한다.

DAI 는 정적으로 할당된 IP 주소를 가진 호스트에 대해서는 운용자가 정의한 ARP access control lists (ACLs)를 사용할 수도 있다. 스위치는 폐기된 패킷에 대해 로그를 남길 수도 있다.

또한 다음과 같은 경우 DAI 가 ARP 패킷을 폐기하도록 설정할 수도 있다:

- 패킷의 IP 주소가 유효하지 않다 – 예를 들어, 0.0.0.0, 255.255.255.255 또는 IP 멀티캐스트 주소.
- ARP 패킷의 body 에 포함된 MAC 주소와 Ethernet 헤더의 주소가 일치하지 않는다.

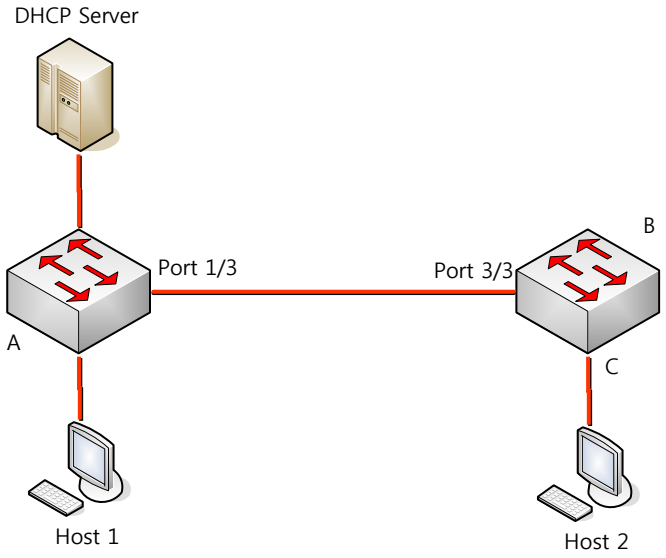
19.1.4. Interface Trust States and Network Security

DAI 는 스위치의 각 인터페이스에 대한 trust 상태 state 정보를 유지하고 있다. Trusted 인터페이스를 통해 수신한 패킷에 대해서는 어떤 DAI 검사도 수행하지 않는다. 반면, Untrusted 인터페이스를 통해 수신한 패킷은 DAI 의 검사를 받는다.

전형적인 네트워크 구성에서, 호스트와 연결된 스위치 포트를 untrusted 로 설정하고 스위치에 연결된 포트는 trusted 로 설정한다. 이런 설정에서, 이 스위치를 통해 네트워크로 유입되는 모든 ARP 패킷은 보안검사를 받게 된다. VLAN 이나 네트워크의 다른 장소에서 더 이상의 유효성 검사가 필요하지는 않다. trust 설정은 인터페이스 설정 명령인 ip arp inspection trust 를 사용하면 된다.

Caution 네트워크 보안을 위해 스위치가 모든 ARP 패킷을 검사하도록 하려면, 특별한 기능이 필요하다. 즉, DAI 가 스위치의 포워딩 엔진 forwarding engine 을 통해 포워딩되는 유니캐스트 ARP 패킷도 검사할 수 있도록 스위치의 CPU 로 trap 할 수 있어야 한다.
플랫폼에 따른 기능의 차이가 있으므로, 관련 제품의 매뉴얼을 숙독하기 바란다.

다음 그림에서 스위치 A 와 스위치 B 에서 호스트 1 과 호스트 2 를 포함하는 VLAN 에 대해 DAI 가 실행 중이라고 가정하자. 호스트 1 과 호스트 2 가 스위치 A 와 연결된 DHCP 서버 server 로부터 IP 주소를 할당 받았다면, 오직 스위치 A 는 호스트 1 에 대한 IP-to-MAC 주소 매핑을 가지고 있다. 그러므로, 스위치 A 와 스위치 B 사이의 인터페이스가 untrusted 라면, 호스트 1 이 전송한 ARP 패킷은 스위치 B 에서 폐기된다. 즉, 호스트 1 과 호스트 2 는 통신을 할 수 없게 된다.



인터페이스를 trusted 로 설정했을 때, 신뢰할 수 없는 장비가 존재한다면 네트워크 보안에 허점이 발생한다. 스위치 A 에서 DAI 를 실행하고 있지 않으면, 호스트 1 은 스위치 B (그리고 스위치 사이의 인터페이스가 trusted 로 설정되어 있다면 호스트 2 까지)의 ARP 캐시를 오염시킬 수 있다. 이런 현상은 스위치 B 에서 DAI 를 실행시키더라도 발생한다.

DAI 가 실행중인 스위치는 연결된 호스트가 네트워크의 다른 호스트들의 ARP 캐시를 오염시키는 행위를 방지한다. 그러나, DAI 는 DAI 가 실행중인 다른 네트워크의 호스트의 ARP 캐시를 오염시키는 것을 방지하지는 못한다.

이 경우에 DAI 를 실행중인 스위치에서는 DAI 를 실행시키지 않는 스위치와 연결된 인터페이스를 untrusted 로 설정하라. 그리고 DAI 가 설정되지 않는 스위치로부터의 packet 을 검사하기 위해 DAI 를 실행중인 스위치에서 ARP ACLs 를 설정하라. 이런 설정이 불가능하다면, Layer 3 에서 DAI 를 사

용중인 스위치와 사용하지 않는 스위치를 분리해야 한다.

Note Premier 8624XG 시리즈는 DAI 가 모든 ARP 패킷을 검사하는 네트워크를 보호 기능을 제공한다.

19.1.5. Rate Limiting of ARP Packets

DAI 기능이 활성화된 스위치는 CPU 로 유입되는 ARP 패킷의 rate 를 제한한다. 디폴트로 untrusted 인터페이스에 대해서 초당 15 개 (15 pps)의 ARP 패킷만 허용되며, trusted 인터페이스의 rate 는 제한하지 않는다. 인터페이스 설정 명령 **ip arp inspection limit** 를 사용해서 설정을 변경할 수 있다.

특정 포트를 통해 CPU 로 유입되는 ARP 패킷의 rate 가 설정한 값을 초과하면, 스위치는 이 포트로 수신한 모든 ARP 패킷을 폐기한다. 사용자가 설정을 변경할 때까지 이 상태가 유지된다. 인터페이스 설정 명령 **ip arp inspection limit auto-recovery** 를 사용하면, 일정 시간이 경과한 후 포트를 자동으로 서비스 가능 상태로 만들 수 있다.

Note ARP 패킷의 rate limit 는 CPU 에서 software 로 처리되기 때문에, Denial-of-Service (DoS) 공격에 대해 큰 효과를 기대할 수 없다.

19.1.6. Relative Priority of ARP ACLs and DHCP Snooping Entries

DAI 는 IP-to-MAC 주소 매핑을 검사할 때, DHCP snooping binding 데이터베이스를 사용한다.

ARP ACLs 은 DHCP snooping binding 데이터베이스보다 먼저 검사에 사용된다. 스위치는 **ip arp inspection filter** 명령으로 설정이 되었을 경우에만 ACLs 을 사용한다. 스위치는 먼저 사용자가 설정한 ARP ACLs 로 ARP 패킷을 검사한다. 만약 ARP 패킷이 ARP ACLs 의 deny 조건과 일치하면, DHCP snooping 에 의해 유효한 binding 이 존재하더라도 그 패킷은 폐기된다.

19.1.7. Logging of Dropped Packets

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성한다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제된다. 각각의 로그에는 flow 정보 (수신한 VLAN, port 번호, source 와 destination IP 주소, source 와 destination MAC 주소)가 포함된다.

Global 설정 명령 **ip arp inspection log-buffer** 로 버퍼의 크기를 설정할 수 있으며, 단위 시간 동안

필요한 로그의 개수를 설정해서 시스템 메시지의 생성 량을 조절할 수 있다. 그리고, Global 설정 명령 ip arp inspection vlan logging 으로 로그할 패킷의 종류를 지정할 수도 있다.

19.2. Default DAI Configuration

다음의 표는 default DAI 설정을 보여준다.

Feature	Default Setting
DAI	모든 VLAN 에 대해 비활성 상태이다.
Interface trust state	모든 인터페이스들은 untrusted 상태이다.
Rate limit of incoming ARP packets	초당 15 개의 새로운 호스트가 등록되는 Layer 2 네트워크라 가정하고, untrusted 인터페이스 에 대해 15 pps 로 설정된다. Trusted 인터페이스에 대해서는 rate 를 제한하지 않는다. burst interval 은 1 초이다. 인터페이스의 rate limit 기능은 disable 되어 있다.
ARP ACLs for non-DHCP environments	ARP ACLs 은 정의되어 있지 않다.
Validation checks	어떤 검사도 수행하지 않는다.
Log buffer	DAI 가 활성화되면, deny 되거나 drop 되는 모든 ARP 패킷 정보가 로깅된다. log entry 의 개수는 32 개. 생성되는 시스템 메시지의 개수는 초당 5 개. logging-rate 주기는 1 초.
Per-VLAN logging	deny 되거나 drop 되는 모든 ARP 패킷이 로깅된다.

19.3. DAI Configuration Guidelines and Restrictions

DAI를 설정할 때, 다음의 사항을 준수하라:

- ✓ DAI는 기본적으로 스위치 자신의 ARP 테이블만 보호한다. 네트워크를 보호하기 위해서는 모든 ARP 패킷을 CPU로 trap할 수 있는 기능이 필요하다.
- ✓ DAI는 입구 보안ingress security 기능이다; 출구 검사egress check에 사용하지 마라.
- ✓ DAI는 DAI를 지원하지 않는 스위치에 연결된 호스트에 대해서는 효과적이지 않다. man-in-the-middle attack은 단일 Layer 2 브로드캐스트 도메인에 제한되기 때문에, DAI를 사용하는 도메인을 그렇지 않은 도메인으로부터 분리하라. 이것은 DAI가 활성화된 도메인에 위치한 호스트의 ARP 테이블을 보호해준다.

✓ DAI는 유입된 ARP request와 ARP response 패킷의 IP-to-MAC 주소 binding을 검사하기 위해 DHCP snooping binding 데이터베이스를 사용한다. 동적으로 할당되는 IP 주소에 대한 ARP 패킷을 허용하기 위해서는 반드시 DHCP snooping을 활성화시켜라.

> **Note** DAI 가 스위치의 DHCP 서버 기능과 함께 사용될 경우, DHCP 서버의 binding 정보를 사용할 수도 있다.

✓ DHCP snooping이 비활성 상태이거나 DHCP 환경이 아니라면, 패킷을 permit하거나 deny하기 위해 ARP ACL을 사용하라.

✓ 포트의 특성을 고려해서 ARP 패킷의 rate를 설정하라.

19.4. Configuring DAI

이 절에서는 DAI 를 설정하는 방법에 대해 설명한다:

- Enabling DAI on VLANs (필수)
- Configuring the DAI Interface Trust State (옵션)
- Applying ARP ACLs for DAI Filtering (옵션)
- Configuring ARP Packet Rate Limiting (옵션)
- Enabling DAI Error-Disabled Recovery (옵션)
- Enabling Additional Validation (옵션)
- Configuring DAI Logging (옵션)
- Displaying DAI Information

19.4.1. Enabling DAI on VLANs

VLAN 에 DAI 를 enable 하면, 스위치는 해당 VLAN 을 통해 수신한 다음과 같은 ARP 패킷들을 검사한다:

- 브로드캐스트되는 ARP 패킷
- 스위치의 MAC 주소를 요청하는 ARP request 패킷
- 스위치가 요청한 ARP request 에 대한 응답 패킷
- 단말들 사이에 송수신되는 모든 unicast ARP 패킷

이 패킷들을 검사해서, 유효한 패킷에 대해서만 응답하고 ARP 테이블을 변경한다.

VLAN 에 DAI 를 enable 하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **ip arp inspection vlan** *vlan-id*	VLAN 에 DAI 를 enable 한다.
Switch(config)# **no ip arp inspection vlan**	VLAN 에 DAI 를 disable 한다.

vlan-id	
Switch# **show ip arp inspection**	설정을 확인한다.

Note VLAN 에 DAI 를 enable 하면, 해당 VLAN 을 통해 송수신 되는 모든 ARP 패킷을 검사한다. 다시 말해, 스위치의 ARP 캐시와 네트워크가 함께 보호된다.

다음의 예는 VLAN 200 에 DAI 를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200
```

다음의 예는 설정을 확인하는 방법을 보여준다:

```
Switch# show ip arp inspection
DHCP Snoop Bootstrap        : Disabled
Source MAC Validation       : Disabled
Destination MAC Validation  : Disabled
IP Address Validation       : Disabled
ARP Field Validation        : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
 200  Enabled   Active+                        No          Deny      Deny
```

19.4.2. Configuring the DAI Interface Trust State

스위치는 trusted 인터페이스로부터 수신한 ARP 패킷은 검사하지 않는다.

Untrusted 인터페이스를 통해 수신한 ARP 패킷은 유효한 IP-to-MAC 주소 매핑을 가지고 있는지 검사된다. 스위치는 유효하지 않은 패킷은 폐기하고, **ip arp inspection vlan logging** 설정에 따라 로그 버퍼에 패킷 로그를 저장한다.

인터페이스의 trust 상태를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **interface** *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.

Switch(config-if-gi1)# **ip arp inspection trust** Switch(config-if-gi1)# **no ip arp inspection trust**	스위치와 연결된 인터페이스를 trusted 로 설정한다. (default: untrusted) 스위치와 연결된 인터페이스를 untrusted 로 설정한다.
Switch(config-if-gi1)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection interfaces**	설정을 확인한다.

다음의 예는 Gigabit 포트 1 을 trusted 로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# ip arp inspection trust
Switch(config-if-gi1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
gi1              Trusted            None               1       Disabled
gi2              Untrusted            15               1       Disabled
```

19.4.3. Applying ARP ACLs for DAI Filtering

ARP ACL 을 사용하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정로 진입한다.
Switch(config)# **ip arp inspection filter** *arp_acl_name* **vlan** *vlan-id* [**static**]	VLAN 에 ARP ACL 을 적용한다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection**	설정을 확인한다.

ARP ACL 을 적용할 때, 다음의 사항에 유의하라:

- ARP ACL 의 implicit deny 를 explicit deny 처럼 다루고 ACL 의 어떤 조건과도 일치하지 않는 패킷을 폐기하려면, **static** 키워드를 사용하라. 이 경우에 DHCP binding 은 사용되지 않는다.

  static 키워드를 사용하지 않으면, ACL 에 일치하는 조건이 없는 패킷에 대해서는 DHCP binding 을 사용해서 패킷을 permit 할 것이지 deny 할 것인지를 결정한다.
- IP-to-MAC 주소 매핑을 포함하고 있는 ARP 패킷만 ACL 로 검사한다. Access list 가 permit 하는 패킷들만 permit 된다.

다음의 예는 이름이 example_arp_acl 인 ARP ACL 을 VLAN 200 에 적용하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection filter example_arp_acl vlan 200
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap        : Disabled
Source MAC Validation       : Disabled
Destination MAC Validation  : Disabled
IP Address Validation       : Disabled
ARP Field Validation        : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
 200  Enabled   Active     example_arp_acl      No          Deny      Deny
```

19.4.4. Configuring ARP Packet Rate Limiting

DAI 가 활성화 되면 스위치는 모든 ARP 에 대해 유효성 검사를 하고, 이로 인해 스위치는 ARP 패킷의 DoS 공격에 취약해진다. 스위치의 CPU 에서 ARP 패킷의 rate 를 제한함으로써 CPU 의 부하를 감소시킬 수 있다.

Note DAI 가 제공하는 ARP rate limit 는 소프트웨어 기능이기 때문에, 스위치의 CPU 사용률을 직접적으로 감소시킬 수는 없다. 하지만 DAI 가 처리하는 ARP 패킷의 양을 조절함으로써, DAI 에 의한 CPU 사용률을 낮출 수는 있다.

포트에 대해 ARP 패킷에 대한 rate limit 를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정으로 진입한다.
Switch(config)# interface *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-gi1)# ip arp inspection limit {rate *pps* [burst interval *seconds*] | none} Switch(config-if-gi1)# no ip arp inspection limit	(옵션) ARP packet rate limit 를 설정한다. default 설정으로 복원한다.
Switch(config-if-gi1)# ip arp inspection limit enable Switch(config-if-gi1)# no ip arp inspection limit enable	인터페이스의 ARP rate limit 기능을 enable 시킨다. 인터페이스의 ARP rate limit 기능을 disable 시킨다.
Switch(config)# end	Enable 모드로 돌아간다.

Switch# **show ip arp inspection interfaces**	설정을 확인한다.

ARP packet rate limit 를 설정할 때, 다음의 사항에 유의하라:

- 디폴트로 untrusted 인터페이스에 대해서는 15 pps (packet per second), trusted 인터페이스에 대해서는 rate 를 제한하지 않는다.
- **rate** *pps* 로 초당 처리할 수 있는 상한을 설정한다. 범위는 0 부터 2048 이다.
- **rate none** 키워드는 수신되는 ARP 패킷의 rate 에 제한을 하지 않음을 명시한다.
- (옵션) **burst interval** *seconds* (default 는 1)는, ARP 패킷의 rate 가 상한을 초과하는지 관측하는 시간이다. 즉, **rate** 로 설정한 값을 **burst interval** 초 동안 초과할 때 해당 포트로 유입되는 ARP 패킷을 제한한다. 값의 범위는 1 ~ 15 이다.
- 유입되는 ARP 패킷의 rate 가 설정 값을 초과하면, 스위치는 해당 포트로 수신한 모든 ARP 패킷을 폐기한다. 운영자가 설정을 변경할 때까지 이 상태가 유지된다.
- 인터페이스의 rate-limit 값을 변경하지 않고, 인터페이스의 trust 상태를 변경해도 인터페이스에 대한 rate-limit 의 default 값이 변경된다. rate-limit 값을 변경한 후에는, trust 상태를 변경하더라도 설정한 값이 그대로 보존된다. 인터페이스 설정 명령 **no ip arp inspection limit** 을 사용하면, 인터페이스의 rate-limit 값은 default 값으로 복원된다.
- **ip arp inspection limit enable** 명령을 설정해야, ARP 패킷 rate limit 가 동작한다.

다음은 gi1 에 ARP packet rate limit 를 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-gi1)# ip arp inspection limit enable
Switch(config-if-gi1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
gi1              Untrusted            20               2       Disabled
gi2              Untrusted            15               1       Disabled
```

19.4.5. Enabling DAI Error-Disabled Recovery

ARP 패킷에 대한 rate limit 때문에, ARP 패킷의 수신이 제한된 포트를 자동으로 복구하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **interface** *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드 로 진입한다.
Switch(config-if-gi1)# **ip arp inspection limit auto-recovery** *seconds*	(옵션) 자동 복구 기능을 활성화 시킨다.

Switch(config)# **no ip arp inspection limit auto-recovery**	자동 복구 기능을 해제한다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection interfaces**	설정을 확인한다.

다음은 인터페이스 **gi1** 이 **ARP rate limit** 에 의해 **ARP** 패킷 수신이 차단되었을 경우, **10** 초 후에 자동으로 복구되도록 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi2
Switch(config-if-gi1)# ip arp inspection limit auto-recovery 10
Switch(config-if-gi1)# ip arp inspection limit enable
Switch(config-if-gi1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
gi1              Untrusted            20               2             10
gi2              Untrusted            15               1       Disabled
```

19.4.6. Enabling Additional Validation

DAI 로 ARP 패킷의 destination MAC 주소, sender 와 target IP 주소, source MAC 주소에 대한 유효성 검사를 할 수 있다.

IP 주소 또는 MAC 주소에 대한 유효성 검사를 하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **ip arp inspection validate {dst-mac | ip | src-mac}** Switch(config)# **no ip arp inspection validate {dst-mac | ip | src-mac}**	(옵션) 추가적인 유효성 검사를 enable 한다. (default: none) 추가적인 유효성 검사를 disable 한다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection**	설정을 확인한다.

추가적인 유효성 검사를 enable 하려면, 다음의 사항에 유의하라:

- 다음의 키워드 중 적어도 하나를 사용해야 한다.
- 각 **ip arp inspection validate** 명령은 이전의 명령을 삭제한다. 만약, **ip arp inspection validate** 명령으로 **src-mac** 와 **dst-mac** 검사를 enable 하고, 두 번째 **ip arp inspection validate** 명령으로 **ip** 검사만을 enable 했다면, **src-mac** 와 **dst-mac** 검사는 disable 되고

ip 검사만이 enable 된다.

- 추가적인 유효성 검사는 다음과 같다:
  - **dst-mac** – ARP response 패킷에 대해 Ethernet 헤더의 destination MAC 주소와 ARP body 의 target MAC 주소를 비교한다.
  - **ip –** ARP body 의 유효하지 않은 IP 주소를 검사한다. 0.0.0.0 또는 255.255.255.255 또는 멀티캐스트 IP 주소는 폐기된다. ARP request 의 sender IP 주소, ARP response 의 sender/target IP 주소를 검사한다
  - **src-mac** – 모든 ARP 패킷에 대해 Ethernet 헤더의 source MAC 주소와 ARP body 의 sender MAC 주소를 비교한다.

다음의 예는 src-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Enabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
 200  Enabled   Active                          No          Deny      Deny
```

다음의 예는 dst-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Disabled
Destination MAC Validation : Enabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
```

```
 200   Enabled   Active                          No          Deny       Deny
```

다음의 예는 ip 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate ip
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap        : Disabled
Source MAC Validation       : Disabled
Destination MAC Validation  : Disabled
IP Address Validation       : Enabled
ARP Field Validation        : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
 200  Enabled   Active                          No          Deny      Deny
```

다음의 예는 src-mac 과 dst-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap        : Disabled
Source MAC Validation       : Enabled
Destination MAC Validation  : Enabled
IP Address Validation       : Disabled
ARP Field Validation        : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
 200  Enabled   Active                          No          Deny      Deny
```

19.4.7. Configuring DAI Logging

이 절에서는 DAI 의 로깅 [logging] 에 대해 설명한다:

- DAI Logging Overview
- Configuring the DAI Logging Buffer Size
- Configuring the DAI Logging System Messages
- Configuring DAI Log Filtering

19.4.7.1. DAI Logging Overview

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성한다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제된다. 각각의 로그에는 flow 정보(수신한 VLAN, port 번호, source 와 destination IP 주소, source 와 destination MAC 주소)가 포함된다.

하나의 로그 버퍼 entry 는 하나 이상의 패킷에 대한 정보를 표시할 수 있다. 예를 들어, 같은 VLAN 에서 같은 ARP 인자 parameter 를 가진 패킷을 동일한 인터페이스를 통해 많이 수신한다면, DAI 는 이 패킷에 대한 로그 버퍼 entry 를 하나 생성하고, 하나의 시스템 메시지를 생성한다.

19.4.7.2. Configuring the DAI Logging Buffer Size

DAI 로그 버퍼의 크기를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **ip arp inspection log-buffer entries** *number* Switch(config)# **no ip arp inspection log-buffer entries**	DAI 의 로그 버퍼 크기를 설정한다. (범위는 0 ~ 1024). default 버퍼 크기로 복원한다. (32)
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection log**	설정을 확인한다.

다음의 예는 DAI 의 로그 버퍼 크기를 64 개로 설정한다:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
```

19.4.7.3. Configuring the DAI Logging System Messages

DAI 가 생성하는 로그 메시지를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose

Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **ip arp inspection log-buffer logs** *number_of_messges* **interval** *length_in_seconds* Switch(config)# **no ip arp inspection log-buffer logs**	DAI 로그 버퍼를 설정한다. default 로 복원한다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection log**	설정을 확인한다.

DAI 의 로깅 시스템 메시지를 설정하려면, 다음의 사항에 유의하라:

- **logs** *number_of_messges* (default 는 5) 에서, 값의 범위는 0 ~ 1024 이다. 0 으로 설정하면 로그 메시지가 생성되지 않는다.
- **interval** *length_in_seconds* (default 는 1) 에서, 값의 범위는 0 ~ 86400 초 (1 일)이다. 0 으로 설정하면, 로그 메시지가 바로 생성된다 (즉, 로그 버퍼는 항상 비어있다).
- 시스템 로그 메시지는 *length_in_seconds* 초당 *number_of_messages* 의 비율로 생성된다.

다음의 예는 매 2 초마다 12 개의 DAI 로그 메시지를 생성하도록 설정한다:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 12 entries per 2 seconds.
No entries in log buffer.
```

19.4.7.4. Configuring the DAI Log Filtering

ARP 패킷을 검사한 후, 그 결과에 대한 시스템 메시지를 선택적으로 생성할 수 있다.
DAI 의 log filtering 기능을 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **ip arp inspection vlan** *vlan-id* {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	각 VLAN 에 대해 log filtering 을 설정한다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show running-config**	설정을 확인한다.

DAI 의 로깅 시스템 메시지를 설정하려면, 다음과 같은 사항에 유의하라:

- Default 로 모든 deny 되는 패킷은 로깅된다.

- **acl-match matchlog** — ACL 설정을 기반으로 로깅한다. 이 명령에 **matchlog** 키워드를 명시했고, ARP access-list 설정의 **permit** 또는 **deny** 명령에 **log** 키워드가 사용되었다면, ACL 에 의해 permit 되거나 deny 되는 ARP 패킷들이 로깅된다.
- **acl-match none** — ACL 과 일치하는 패킷에 대해 로깅하지 않는다.
- **dhcp-bindings all** — DHCP binding 과 일치하는 모든 패킷들을 로깅한다.
- **dhcp-bindings none** — DHCP binding 과 일치하는 패킷들을 로깅하지 않는다.
- **dhcp-bindings permit** — DHCP binding 에 의해 허용된 패킷들을 로깅한다

다음의 예는 VLAN 200 에 대해 ACL 과 일치하는 패킷에 대한 로그 메시지를 생성하지 않도록 설정한다:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200 logging acl-match none
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap        : Disabled
Source MAC Validation       : Disabled
Destination MAC Validation  : Disabled
IP Address Validation       : Disabled
ARP Field Validation        : Disabled

Vlan  Config    Operation  ACL Match            Static ACL  ACL Log   DHCP Log
----  --------  ---------  -------------------  ----------  --------- --------
 200  Enabled   Active                          No          None      Deny
```

19.4.8. Displaying DAI Information

DAI 의 정보를 조회하려면, 다음의 명령을 사용하라:

Command	Description
show arp access-list	ARP ACL 에 대한 정보를 출력한다.
show ip arp inspection interfaces	인터페이스의 trust 상태 정보를 출력한다.
show ip arp inspection vlan [*vlan-id*]	VLAN 에 대한 DAI 설정과 동작 상태 정보를 출력한다.
show ip arp inspection arp-rate	인터페이스의 ARP 패킷 수신 rate 정보를 출력한다.

DAI 통계정보를 조회하거나 초기화하려면, 다음의 명령을 사용하라:

Command	Description
clear ip arp inspection statistics	DAI 통계 정보를 초기화 한다.
show ip arp inspection statistics [vlan *vlan-id*]	DAI 가 처리한 ARP 패킷에 대한 통계정보를 출력한다.

DAI logging 정보를 조회하거나 초기화하려면, 다음의 명령을 사용하라:

Command	Description
clear ip arp inspection log	DAI 로그 버퍼를 초기화 한다.
show ip arp inspection log	DAI 로그 버퍼의 설정과 로그 버퍼의 내용을 출력한다.

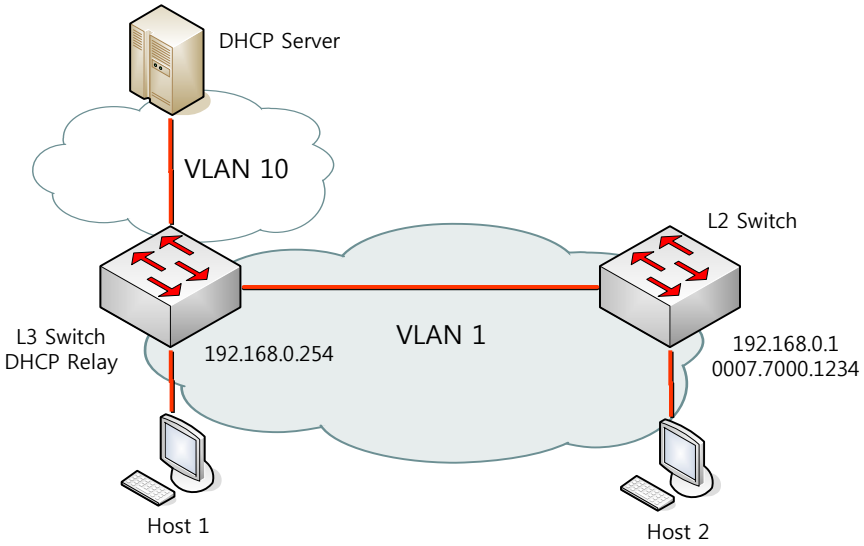
19.5. DAI Configuration Samples

이 절은 다음과 같은 예제들을 포함한다:

- Sample One: Interoperate with DHCP Relay
- Sample Two: Interoperate with DHCP Server

19.5.1. Sample One: Interoperate with DHCP Relay

이 예제는 DHCP relay 기능을 사용하는 스위치에 DAI 를 설정하는 방법을 설명한다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정하자:



L3 스위치는 VLAN 10 을 통해 DHCP 서버로 DHCP 메시지를 중계하며, 호스트 또는 L2 스위치가 연

결된다. L3 스위치에 연결된 L2 스위치는 고정 IP 주소를 사용한다. 호스트 1 과 호스트 2 는 DHCP 를 통해 IP 주소를 할당 받는다. 그리고 모든 스위치와 호스트들은 VLAN 1 에 위치한다.

Note 이런 구성에서 DAI 는 IP-to-MAC binding 정보를 전적으로 DHCP snooping binding 정보에 의존한다. DHCP snooping 설정은 DHCP snooping 매뉴얼을 참고하라.

DHCP relay 로 사용되는 스위치에서 DAI 기능을 사용하려면, 다음과 같이 설정한다:

Step 1 **DHCP relay 기능을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 10.1.1.1
Switch(config)# service dhcp relay
```

Step 2 **DHCP 로 IP 를 할당 받는 호스트의 IP-to-MAC binding 정보를 구축하기 위해, DHCP server 와의 통신에 사용되는 인터페이스 VLAN 10 과 호스트가 연결된 인터페이스 VLAN 1 에 DHCP snooping 을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping
```

Step 3 **고정 IP 를 사용하는 스위치의 ARP 패킷을 허용하기 위해 ARP ACL 을 설정한다.**

```
Switch# configure terminal
Switch(config)# arp access-list permit-switch
Switch(config-arp-nacl)# permit ip host 192.168.0.1 mac host 0007.7000.1234
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection filter permit-switch vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

```
Switch# show ip arp inspection vlan 1
```

Step 4 **호스트가 연결된 VLAN 1 에 DAI 를 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

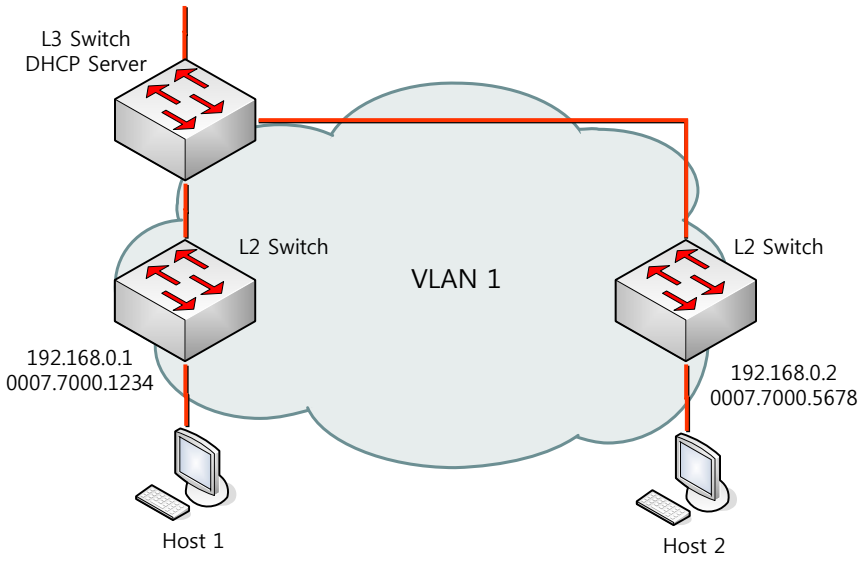
Switch# **show ip arp inspection vlan 1**

L3 스위치의 설정을 조회하면 다음과 같다.

```
!
arp access-list permit-switch
  permit ip host 192.168.0.1 mac host 0007.7000.1234
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
ip dhcp helper-address 10.1.1.1
service dhcp relay
!
ip dhcp snooping vlan 1
ip dhcp snooping vlan 10
ip dhcp snooping
!
```

19.5.2. Sample Two: Interoperate with DHCP Server

이 예제는 DHCP 서버로 사용되는 스위치에 DAI 를 설정하는 방법을 설명한다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정하자:



L3 스위치는 DHCP 서버로 동작하며 L2 스위치가 연결된다. L2 스위치는 고정 IP 주소를 사용한다. 호스트 1 과 호스트 2 는 DHCP 를 통해 IP 주소를 할당 받는다. 그리고 모든 스위치와 호스트들은 VLAN

1 에 위치한다.

> **Note** 이런 구성에서 DAI 는 IP-to-MAC binding 정보를 전적으로 DHCP 서버의 binding 정보에 의존한다. DHCP 서버 설정은 DHCP 서버 매뉴얼을 참고하라.

DHCP 서버로 사용되는 스위치에서 DAI 기능을 사용하려면, 다음과 같이 설정한다:

Step 1 **호스트에게 IP 주소를 할당하기 위해 DHCP server 를 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# service dhcp server
```

> **Note** DHCP 네트워크 pool 설정은 생략한다. DHCP 매뉴얼을 참고하라.

Step 2 **고정 IP 를 사용하는 스위치의 ARP 패킷을 허용하기 위해 ARP ACL 을 설정한다.**

```
Switch# configure terminal
Switch(config)# arp access-list permit-switch
Switch(config-arp-nacl)# permit ip range 192.168.0.1 192.168.0.10 mac host 0007.7000.1234 0000.00ff.ffff
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection filter permit-switch vlan 1
Switch(config)# end
```

> **Note** ARP ACL 은 하나의 조건으로 다수의 패킷을 검사할 수 있도록, IP 주소에 대해서는 range 를 MAC 주소에 대해서는 wildcard 명령을 제공한다.

올바르게 설정되었는지 확인한다.

```
Switch# show ip arp inspection vlan 1
```

Step 3 **호스트와 스위치가 연결된 VLAN 1 에 DAI 를 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

Switch# **show ip arp inspection vlan 1**

L3 스위치의 설정을 조회하면 다음과 같다.

```
!
arp access-list permit-switch
  permit ip host 192.168.0.1 192.168.0.10 mac host 0007.7000.1234 0000.00ff.ffff
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
service dhcp server
!
ip dhcp network-pool
 dns-server 164.124.107.9 203.248.252.2 168.126.63.1
 lease 0 0 30
 domain-name ubiquoss.com
 default-router 192.168.0.254
 network 192.168.0.0/24
 range 192.168.0.50 192.168.0.100
!
```

20 ARP Snoop

이 장에서는 특정 IP 주소 영역에 대한 Ethernet 주소 정보를 구축하기 위해 사용되는 ARP snoop 기능의 설정 방법에 대해 설명한다.

> **Note** 이 장에서 사용되는 명령어에 대한 문법과 사용 방법에 관한 상세한 정보는 command reference 를 참조하라.

이 장은 다음과 같은 내용으로 이루어져 있다:

- ARP Snoop에 대한 이해 (Understanding ARP Snoop)
- ARP Snoop 기본 설정 (Default ARP Snoop Configuration)
- ARP Snoop 설정 (Configuring ARP Snoop)
- ARP Snoop 설정 예제 (ARP Snoop Configuration Samples)

20.1. Understanding ARP Snoop

이 절에서는 ARP snoop 기능에 대해 설명한다.

20.1.1. Understanding ARP Snoop

일반적으로 ARP cache 는 다음과 같은 경우에 생성된다:

- 호스트에서 ARP Request를 전송하거나
- 호스트가 가진 IP 주소에 대한 ARP Request를 수신했을 때

한 번 생성된 ARP cache 는 ARP 패킷에 의해 계속 업데이트 되며, 일정 시간 동안 업데이트 되지 않으면 삭제된다.

다음의 표는 ARP cache 를 변경하는 ARP 패킷 유형을 나타낸다:

ARP op	Target address	Sender address	ARP cache
Request	To me	!= 0	존재하지 않으면 생성
Reply	To me	!= 0	존재하면 업데이트
Request	Any	!= 0	존재하면 업데이트
Reply	Any	!= 0	존재하면 업데이트

표 20-1 ARP cache를 업데이트하는 ARP 유형

ARP 패킷의 sender address 에 대해 ARP cache 가 존재한다면, 어떤 ARP 패킷이라도 호스트의 ARP cache 를 변경하게 된다.

ARP snoop 기능의 기본 개념은 호스트가 요청하지 않은 ARP 패킷에 의해 ARP cache 가 업데이트 되는 것을 방지할 수 있도록 ARP sender 에 대한 정보를 제공하는 것이다. 이를 위해 ARP snoop 은 ARP snoop binding 이라는 (IP 주소, Ethernet 주소) 정보를 관리한다.

ARP snoop 기능이 활성화된 호스트는 unsolicited ARP 를 수신하면, ARP snoop binding 을 생성한 후 ARP 패킷에 명시된 호스트에게 ARP Request 를 전송한다. 이 후, 수신한 ARP Reply 의 sender 정보가 ARP Request 의 정보와 일치할 경우에, 이 ARP snoop binding 정보를 믿을 수 있다고 가정한다.

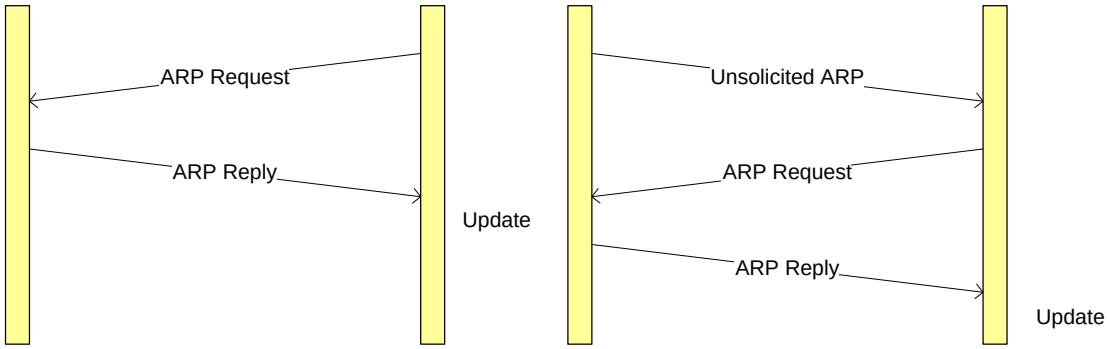


그림 20-1 ARP snoop (3-way handshake)

ARP 패킷 자체에 보안 기능이 없으므로, 여러 개의 ARP Reply 를 수신했을 경우에 어떤 것이 유효한가를 판단할 수 없다. 따라서 이 방법으로 ARP spoofing 공격을 완전히 차단하지는 못한다. 하지만 공격이 시작되기 전에 신뢰할 만한 정보를 생성했다면, 공격의 피해를 감소시킬 수는 있다.

Caution ARP snoop binding 정보를 기반으로 ARP cache 의 업데이트를 차단하려면, DAI 와 ARP ACL 을 함께 사용해야 한다. ARP snoop 은 오직 ARP binding 정보만 제공한다.

20.1.2. ARP Snoop Entry States

ARP snoop 은 ARP snoop binding 정보의 상태를 다음과 같이 유지한다:

State	Description
INIT	ARP snoop entry 가 생성되는 초기 상태
INCOMPLETE	INIT 상태나 UNSOLICITED 상태에서 ARP request 를 전송한 상태 (probe)
REACHABLE	3 Way handshake 과정을 통해 검증된 상태
STALE	REACHABLE 상태에서 age-time 이 경과한 상태
3WAY	ARP request 를 전송하고 ARP reply 를 기다리는 상태
UNSOLICITED	3WAY 상태에서 ARP reply 를 수신하지 못한 상태

ARP snoop 에서 신뢰할 수 있는 것은 REACHABLE 상태의 ARP snoop binding 이다.

20.1.3. ARP Snoop Ageing Time

ARP snoop 은 REACHABLE 상태의 ARP snoop binding 은 ageing-time (default 80 초) 동안 유효하다고 간주한다. ARP Reply 에 의한 업데이트 없이 ageing-time 이 경과한 ARP snoop binding 은 STALE 상태를 거쳐 삭제된다.

한 번 REACHABLE 상태가 된 ARP snoop binding 을 계속 유지하려면 ageing-time 을 사용하지 않으면 된다.

Caution 잘못 생성된 ARP snoop binding 이 계속 유지될 수 있으므로, ageing-time 을 사용하는 것을 권장한다.

20.1.4. ARP Snoop Binding Health Check

ARP snoop 은 주기적으로 ARP snoop binding 의 유효성을 판단할 수 있는 기능인 Health-check 기능을 제공한다. ARP snoop binding 은 비록 REACHABLE 상태라고 하더라도 그 값을 무조건 신뢰할 수 없다. 다음과 같은 경우에 health-check 기능이 유용하게 사용될 수 있다:

- 해당 장비가 네트워크에 더 이상 존재하지 않을 때
- 악의적으로 공격하던 호스트가 사라 졌을 때

Health-check 의 목적은 ARP snoop binding 의 유효성을 주기적으로 검사하고, 유효한 ARP snoop binding 일 경우 계속 유지하기 위함이다.

20.1.5. ARP Snoop Probe

ARP snoop 의 probe 기능은 health check 기능과 유사하다. ARP snoop 의 probe 기능은 INIT 상태와 UNSOLICITED 상태의 ARP snoop binding 에 대해서만 수행된다.

INIT 상태와 UNSOLICITED 상태는 ARP Request 를 전송한 호스트가 존재하지만, ARP snoop 이 송신한 ARP Request 에 대한 ARP Reply 가 없는 경우이다. ARP snoop 은 사용했던 적이 있는 IP 주소에 대해 주기적으로 probe 작업을 수행한다.

Note 모든 IP 대역에 대해 probe 를 하면 ARP request 의 패킷 수가 많아지므로, ARP snoop 이 전송하는 ARP request 의 패킷 수를 줄이기 위해 INIT, UNSOLICITED 상태였던 IP 주소에 대해 probe 를 수행한다.

ARP snoop 은 60 초마다 한번씩 불필요한, INIT 또는 UNSOLICITED 상태의 ARP snoop binding 을 삭제하므로 반복적으로 probe 되는 경우는 드물다.

20.1.6. Understanding DAI and ARP Snoop

DAI 는 ARP 패킷을 검사하는 보안 기능이다. DAI 는 유효하지 않은 IP-to-MAC 주소 binding 을 가진 ARP 패킷을 로깅 logging 하고, 폐기 drop 한다. 이 기능은 main-in-the-middle attack 으로부터 네트워크를 보호한다.

DHCP binding 이 존재하지 않는 IP 주소에 대해서는 DAI 는 다음과 같은 설정을 필요로 한다:

- Static ARP – IP 주소와 해당하는 Ethernet 주소를 운용자가 직접 설정
- ARP ACLs – 허용하거나 폐기할 IP 주소, Ethernet 주소를 ACL 로 설정

DHCP 를 사용하지 않는 고정 IP 에 대한 ARP spoofing 방지 방법은 static ARP 을 사용하거나 ARP ACL 을 사용해서 IP 주소와 Ethernet 주소에 대한 1:1 매핑을 생성하는 것이다. IP 주소와 Ethernet 주소에 대한 1:1 매핑을 사용할 경우 ARP spoofing 에 대한 방어는 완벽하지만, 고정 IP 를 사용하는 호스트의 수가 증가하거나 장비가 교체되면 설정도 변경되어야 한다.

권장하지는 않지만 장비의 증설이나 교체에 대해 설정 변경을 하지 않기 위해 다음과 같이 ARP ACL 의 wildcard 기능을 사용할 수 있다:

- 192.168.0.10 부터 192.168.0.20 까지의 IP 주소에 대해 모든 장비를 허용한다 – permit ip range 192.168.0.10 192.168.0.20 mac any
- 특정 IP 주소 대역은 특정 회사 (Ubiquoss)의 장비를 사용한다 – permit ip range 192.168.0.10 192.168.0.20 mac 0007.7000.0000 0000.00ff.ffff

Caution ARP ACL 을 1:1 매핑으로 사용하지 않는다면, permit 설정과 일치하는 ARP 패킷을 사용한 ARP spoofing 공격으로부터 ARP cache 를 보호할 수 없다.

ARP snoop 이 활성화 되어 ARP snoop binding 정보가 있다면, DAI 는 ARP ACL 에 의해 허용된 ARP 패킷을 ARP snoop binding 정보와 한번 더 비교한다.

Note ARP snoop binding 정보도 100% 신뢰할 수 있는 정보가 아니기 때문에, ARP snoop 과 DAI 를 함께 사용해도 ARP spoofing 공격에 취약하다. 고정 IP 에 대한 신뢰성 있는 ARP spoofing 공격 방지는 IP 주소와 Ethernet 주소에 대한 1:1 매핑을 설정하는 것이다.

20.1.7. Relative Priority of ARP ACLs and ARP Snoop Entries

DAI 는 IP-to-MAC 주소 매핑을 검사하기 위해 ARP snoop binding 도 사용한다.

ARP ACL 과 ARP snoop 이 같이 설정되었을 경우 ARP snoop binding 이 ARP ACLs 보다 먼저 검사에 사용된다. 스위치는 먼저 ARP snoop binding 으로 ARP 패킷을 검사한다. ARP snoop binding 정보와 불일치 되는 ARP 패킷은 폐기된다.

ARP snoop binding 에 의해 허용된 ARP 패킷이라도 ARP ACLs 에 의해 허용되지 않으면 그 패킷은 폐기된다. 즉, DAI 는 ARP snoop binding 을 폐기 조건으로만 사용한다.

20.2. Default ARP Snoop Configuration

다음의 표는 default ARP snoop 설정을 보여준다.

Feature	Default Setting
ARP snoop	Disable.
ARP snoop ip	설정된 IP 주소는 없다.
Ageing Time	80 초
Health check	Enable.
Probe	Enable.
Probe interval	60 초
Wait time	2 초
Gratuitous ARP update	Gratuitous ARP 에 대해서는 검사를 하지 않고 ARP snoop binding 을 update 한다.

20.3. Configuring ARP Snoop

이 절에서는 ARP Snoop 을 설정하는 방법에 대해 설명한다:

- Enabling ARP Snoop (필수)
- Configuring ARP Snoop Ageing-time
- Disabling Gratuitous ARP update without validation (옵션)
- Disabling Health-check (옵션)
- Displaying ARP Snoop Information

20.3.1. Enabling ARP Snoop

스위치에 ARP snoop 을 enable 하면, 스위치는 설정 된 IP 주소 대역에 대해 ARP snoop binding 을 관리한다.

스위치에 ARP snoop 를 enable 하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **arp snoop ip** *ip-address* [*ip-address*]	IP 주소 대역을 설정한다.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	ARP snoop 을 enable 한다. ARP snoop 을 disable 한다.
Switch# **show arp snoop**	설정을 확인한다.

다음의 예는 IP 주소 대역 192.168.0.10 ~ 192.168.0.20 에 대해 ARP snoop 을 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20
Switch(config)# arp snoop
```

다음의 예는 설정을 확인하는 방법을 보여준다:

```
Switch# show arp snoop

ARP Snoop              : Enabled
Gratuitous ARP update  : Enabled
Health Check           : Disabled
Wait Time              : 2 sec
```

```
Probe Interval          : 60 sec
```

20.3.2. Configuring ARP Snoop Ageing-time

ARP snoop 은 REACHABLE 상태의 ARP snoop binding 을 ageing-time 동안 유지한다. Default ageing-time 은 80 초이다.

ARP snoop binding 의 ageing-time 을 변경하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **arp snoop ip** *ip-address* [*ip-address*] [**aging-time** *aging-time*]	IP 주소 대역을 설정하고 ageing-time 을 변경한다.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	ARP snoop 을 enable 한다. ARP snoop 을 disable 한다.
Switch# **show arp snoop**	설정을 확인한다.

다음의 예는 IP 주소 대역 192.168.0.10 ~ 192.168.0.20 에 대해 ARP snoop 을 enable 하고 ageing-time 을 300 초로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20 ageing-time 300
Switch(config)# arp snoop
```

Caution Ageing-timer 의 값을 0 으로 설정하면 REACHABLE 상태의 ARP snoop binding 에 대한 상태 검사 및 변화가 발생하지 않는다. 즉, 잘못 매핑 된 ARP snoop binding 을 계속 사용하게 된다. 올바르게 매핑 된 ARP snoop binding 이 아니라면 ageing-time 을 0 으로 설정하지 않도록 한다.

20.3.3. Disabling Gratuitous ARP Update without Validation

Default 로 ARP snoop 은 gratuitous ARP 를 수신했을 경우, ARP request 를 전송하지 않고 ARP snoop binding 을 업데이트한다.

ARP snoop 이 gratuitous ARP 패킷에 대해서도 ARP request 를 전송한 후 ARP snoop binding 을 업데이트하도록 하려면, 다음의 작업을 수행하라.

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.

Switch(config)# **arp snoop ip** *ip-address* [*ip-address*]	IP 주소 대역을 설정한다.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	ARP snoop 을 enable 한다. ARP snoop 을 disable 한다.
Switch(config)# **no arp snoop gratuitous-arp-update**	Gratuitous ARP 를 수신했을 때, ARP snoop binding 을 바로 업데이트 하지 않는다.
Switch# **show ip arp inspection**	설정을 확인한다.

다음의 예는 IP 주소 대역 192.168.0.10 ~ 192.168.0.20 에 대해 ARP snoop 을 enable 하고, gratuitous ARP 에 대해서도 ARP request 를 전송하도록 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20
Switch(config)# arp snoop
Switch(config)# no arp snoop gratuitous-arp-update
Switch(config)# end
```

20.3.4. Disabling Health-check

ARP snoop 은 REACHABLE 상태의 ARP snoop binding 에 대해 주기적으로 ARP Request 를 전송하고, 수신한 ARP Reply 로 ARP snoop binding 의 상태를 업데이트 한다.

ARP snoop 의 health-check 기능을 사용하지 않으려면, 다음의 작업을 수행하라.

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입한다.
Switch(config)# **arp snoop ip** *ip-address* [*ip-address*]	IP 주소 대역을 설정한다.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	ARP snoop 을 enable 한다. ARP snoop 을 disable 한다.
Switch(config)# **no arp snoop health-check**	Health-check 기능을 disable 한다.
Switch# **show ip arp inspection**	설정을 확인한다.

다음의 예는 IP 주소 대역 192.168.0.10 ~ 192.168.0.20 에 대해 ARP snoop 을 enable 하고, health-check 기능은 사용하지 않는 예를 보여준다:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20
Switch(config)# arp snoop
Switch(config)# no arp snoop health-check
Switch(config)# end
```

20.3.5. Displaying ARP Snoop Information

ARP snoop 의 정보를 조회하려면, 다음의 명령을 사용하라:

Command	Description
show arp snoop	ARP snoop 의 설정 정보를 조회한다.
show arp snoop binding	ARP snoop binding 정보를 조회한다.
show arp snoop interface	ARP snoop 이 송신하는 ARP 패킷의 전송률을 조회한다.

ARP snoop 의 통계정보를 조회하거나 초기화하려면, 다음의 명령을 사용하라:

Command	Description
clear arp snoop statistics	ARP snoop 통계 정보를 초기화 한다.
show arp snoop statistics	ARP snoop 이 송수신한 ARP 패킷에 대한 통계 정보를 출력한다.

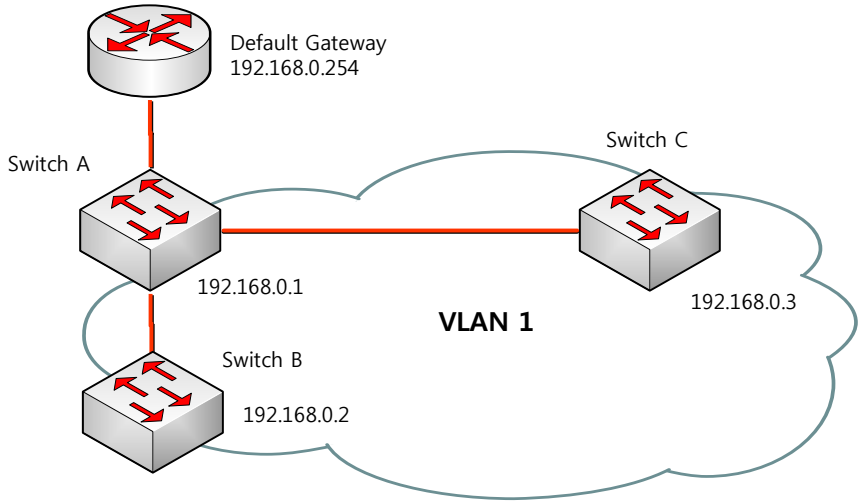
20.4. ARP Snoop Configuration Samples

이 절은 다음과 같은 예제들을 포함한다:

- Sample One: ARP spoofing detection
- Sample Two: Interoperate with DAI on DHCP Relay

20.4.1. Sample One: ARP spoofing detection

이 예제는 ARP snoop 기능을 사용해서 특정 IP 주소 대역에 대한 ARP spoofing 을 감지하는 방법을 설명한다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정하자:



스위치 A 에서 다른 스위치의 Default gateway 나 다른 스위치가 사용하는 IP 주소 대역에 대한 IP-to-MAC binding 정보를 획득하기 위해 ARP snoop 기능을 활성화하려면 다음과 같이 설정한다:

Step 1 **특정 IP 주소 대역에 대한 IP-to-MAC binding 정보를 구축하기 위해 ARP snoop 을 활성화 시킨다.**

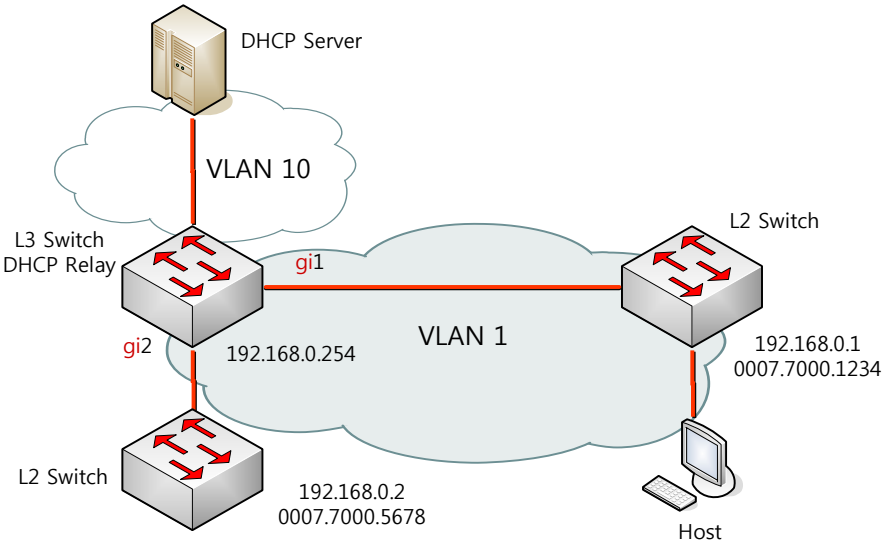
Switch# configure terminal
Switch(config)# arp snoop 192.168.0.1 192.168.0.10
Switch(config)# arp snoop 192.168.0.254
Switch(config)# arp snoop

올바르게 설정되었는지 확인한다.
Switch# show arp snoop

Note ARP snoop 은 IP-to-MAC binding 정보만 구축하기 때문에 ARP 테이블에 대한 보호는 불가능하다. "**show arp snoop binding**" 명령과 "**show arp**" 명령의 결과를 비교하면 ARP spoofing 여부를 감지할 수 있다.

20.4.2. Sample Two: Interoperate with DAI on DHCP Relay

이 예제는 DAI 기능을 사용하는 DHCP relay 에서 ARP snoop 의 IP-to-MAC binding 정보를 사용해서 ARP 패킷을 차단하는 방법을 설명한다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정하자:



L3 스위치는 VLAN 10 을 통해 DHCP 서버로 DHCP 메시지를 중계하며, 호스트 또는 L2 스위치가 연결된다. L3 스위치에 연결된 L2 스위치는 고정 IP 주소를 사용한다. 호스트들은 DHCP 를 통해 IP 주소를 할당 받는다. 그리고 모든 스위치와 호스트들은 VLAN 1 에 위치한다.

Note 이런 구성에서 DAI 는 IP-to-MAC binding 정보를 전적으로 DHCP snooping binding 정보에 의존한다. DHCP snooping 설정은 DHCP snooping 매뉴얼을 참고하라.

DHCP relay 로 사용되는 스위치에서 DAI 기능을 사용하려면, 다음과 같이 설정한다:

Step 1 **DHCP relay 기능을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 10.1.1.1
Switch(config)# service dhcp relay
```

Step 2 **DHCP 로 IP 를 할당 받는 호스트의 IP-to-MAC binding 정보를 구축하기 위해, DHCP server 와의 통신에 사용되는 인터페이스 VLAN 10 과 호스트가 연결된 인터페이스 VLAN 1 에 DHCP snooping 을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping
```

Step 3 **고정 IP 를 사용하는 IP 주소 대역에 대한 IP-to-MAC binding 정보를 구축하기 위해 ARP snoop 을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.1 192.168.0.10
Switch(config)# arp snoop
```

Step 4 **고정 IP 를 사용하는 스위치의 ARP 패킷을 허용하기 위해 ARP ACL 을 설정한다.**

```
Switch# configure terminal
Switch(config)# arp access-list permit-switch
Switch(config-arp-nacl)# permit ip range 192.168.0.1 192.168.0.10 mac any
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection filter permit-switch vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

```
Switch# show ip arp inspection vlan 1
```

Step 5 **호스트가 연결된 VLAN 1 에 DAI 를 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

```
Switch# show ip arp inspection vlan 1
```

L3 스위치의 설정을 조회하면 다음과 같다.

```
!
arp snoop ip 192.168.0.1 192.168.0.10
arp snoop
!
arp access-list permit-switch
  permit ip range 192.168.0.1 192.168.0.10 mac any
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
ip dhcp helper-address 10.1.1.1
service dhcp relay
!
ip dhcp snooping vlan 1
```

```
ip dhcp snooping vlan 10
ip dhcp snooping
!
```