Switch solution

www.ubiquoss.com

P3400 Series Switch
Common 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 3400 Series 2 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
- TCP/IP 프로토콜 개념
- Simple Network Management Protocol (SNMP)

Notice Premier 3400 Series 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하기 바란다.

1.2. 적용 규칙

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

표 1-1. 문자 표시 규칙

문자 표시 규칙	설명
`Screen displays`	■ 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 3400 Series 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 3400 Series 스위치를 포함한 ㈜유비쿼스의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(http://www.ubiqouss.com/)를 통하여 다운로드 받거나 서비스를 요청할 수 있다.

2

Premier 3400 Series 스위치 시작하기

본 장은 다음과 같이 시스템 운영자가 Premier 3400 Series 2 계층 스위치의 운용 환경을 설정하고 처음 다루기 시작할 때 필요한 정보를 제공한다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- Premier 3400 Series 스위치 사용자 인터페이스
- 스위치 로그인과 패스워드의 설정
- SNMP 환경설정
- 스위치의 파일 및 환경 설정의 보기와 저장
- 액세스 리스트
- 텔넷 클라이언트

2.1. 편집 및 도움말 기능

본 장은 명령어 편집기의 편집 기능과 도움말 기능에 대하여 설명한다.

2.1.1. 명령어 문법의 이해

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

명령어 라인 인터페이스를 사용하기 위하여 다음의 단계를 거치도록 한다.

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

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

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

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

다음은 명령어 파라미터를 제대로 입력하지 않은 경우를 보여준다.

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

2.1.2. 명령어 문법 도움말(Command Syntax Helper)

Premier 3400 Series 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 3400 Series 스위치는 다음과 같은 두 가지 도움말 기능을 제공한다.

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

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

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

Switch# show_
```

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

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

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

명령은 다시 표시가 되면서 커서가 깜박이면서 입력을 대기한다.

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

2.1.3. 단축 명령어 입력

Premier 3400 Series 스위치의 CLI 는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행을 지원한다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령을 수행한다.

Notice 단축 명령을 사용할 때, 시스템 운영자는 Premier 3400 Series 스위치가 명령어를 구분하여 인식할 수 있도록 충분하게 입력해야 한다. "% Ambiguous command."라는 메시지를 받을 때가 있다. 이것은 해당 모드에 입력한 문자와 Prefix 가 같은 하나 이상의 명령어가 있음을 의미한다.

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

Switch# show i ?
  interface  Port interface status and configuration
  ip         IP
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

심볼	이름	설명
		반드시 입력해야 한다.
():	Braces	■ 명령어 문법에서 사용되는 파라미터 또는 값의 리스트 ■ 시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 한다. ■ 예를 들어, 다음과 같은 명령어가 있을 때 `qos (cos-queue-map|cos-remarking)` 시스템 운영자는 QoS method 로서 qos-queue-map 또는 qos-remarking 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 interfaces [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 3400 Series 스위치는 Emacs 와 유사한 편집 기능을 제공한다. <표 2-2>는 운영 단말이 제공하는 명령어 라인 편집 명령 및 도움말 기능을 설명한다.

표 2-2. 명령어 라인 편집 명령 및 도움말 기능

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

Tab	■ 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 3400 Series 스위치는 <표 2-3>와 같이 다양한 스위치 명령어 모드를 지원한다. 각 스위치 명령어 모드마다 운영자에게 주어지는 권한에는 차이가 있다.

표 2-3. 스위치 명령어 모드

모드	프롬프트	설명
User 모드	`Switch>`	■ 보통 통계 정보를 디스플레이
Privileged 모드	`Switch#`	■ 시스템 설정을 출력하거나 시스템 관리 명령을 사용
Config 모드	`Switch(config)#`	■ 스위치의 환경 설정 값을 글로벌 하게 변경
Interface 모드	`Switch(config-if-fa1)#` `Switch(config-if-vlan1)#`	■ 인터페이스의 환경 설정을 변경
Interface range 모드	`Switch(config-ifrange)#`	■ 여러 개의 인터페이스를 동시에 설정하기 위한 모드
Range Port 모드	`Switch(config-range-port)#`	■ 여러 개의 인터페이스를 동시에 설정하기 위한 모드

Notice 명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 Premier 3400 Series 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 Premier 3400 Series 스위치의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게 된다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 와 있는 지를 알려준다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 체크 해야만 한다. <표 2-4>은 스위치의 명령어 모드 사이의 이동 방법을 설명한다.

표 2-4. 스위치의 명령어 모드 사이의 이동

명령어	설명
`enable`	■ User 모드에서 Privileged 모드로 이동 ■ Privileged 모드의 패스워드를 입력할 필요
`disable`	■ Privileged 모드에서 User 모드로 이동
`configure terminal`	■ Privileged 모드에서 Config 모드로 이동
`interface` *`ifname`*	■ Config 모드에서 Interface 모드로 이동
`interface range (fastethernet |gigaethernet)` *`ifrange`*	■ Config 모드에서 Interface range 모드로 이동
`range port`	■ Config 모드에서 range port 모드로 이동
`exit`	■ 이전의 모드로 이동
`end`	■ 어느 모드에서든 Privileged 모드로 이동 ■ User 모드에서는 이동하지 않는다.

2.3. Premier 3400 Series 스위치 가동

Premier 3400 Series 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS image 를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.

Notice Premier 3400 Series 스위치는 시스템 안정성을 위하여 두 개 이상의 OS image 를 관리한다. 기본적으로 Primary OS image 가 로드 되도록 설정되어 있으며, 운영자는 스위치의 boot 모드 또는 privileged 모드에서 이를 변경할 수 있다.

2.4. 사용자 인터페이스

시스템 운영자는 스위치의 환경을 설정하고, 환경 설정을 검증하고, 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속할 수 있다. 스위치에 접속하기 위한 가장 기본적인 방법은 Premier 3400 Series 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것이다(*Out-of-band management*).
스위치로 연결하는 또 다른 방법은 원격지에서 telnet 프로그램을 이용하는 것이다. 원격지에서 telnet 연결을 위한 별도의 포트를 지원하지는 않고 서비스 포트를 통하여 접속하도록 한다(*In-band management*).

운영자는 아래의 방법을 사용하여 Premier 3400 Series 스위치를 관리할 수 있다.

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

Premier 3400 Series 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결
- 최대 4 개의 telnet 연결

2.4.1. 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능하다. 이를 위하여 운영 단말(또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9 핀, RS-232 DB9 포트를 지원해야 한다. 콘솔 포트는 Premier 3400 Series 스위치의 경우 전면에 탑재된다.

>과 같이 Premier 3400 Series 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

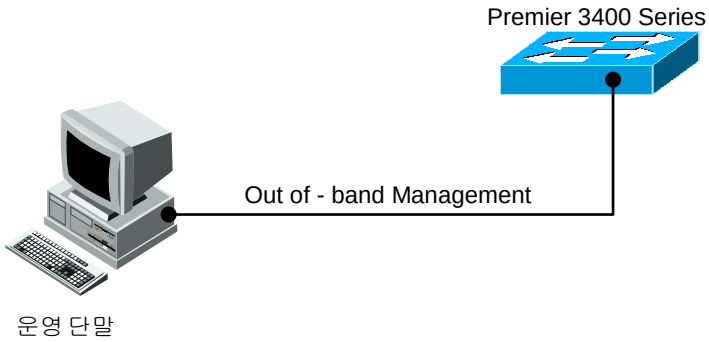


그림 2-1. Premier 3400 Series 스위치와 운영 단말 연결

Notice 운용 단말의 설정 방법 및 콘솔 포트 핀 설정은 Premier 3400 Series 스위치 하드웨어 설치 가이드를 참조하기 바란다.

2.4.2. Telnet 연결

시스템 운영자는 TCP/IP 및 telnet 접속 기능을 가지고 있는 워크스테이션을 통하여 Premier 3400 Series 스위치에 접속할 수 있다. Telnet 을 사용하기 위하여, 운영자는 ID 및 비밀번호를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 한다.

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

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

또한 시스템 보안을 위하여 액세스 리스트를 사용하여 telnet 에 연결하는 사용자를 제한할 수 있다. 이는 <2.9. ACL (Access Control List)>절을 참조하라.

2.4.3. SNMP Network Manager 를 통한 연결

Simple Network Management Protocol (SNMP)를 지원하는 어떠한 네트워크 관리기(Network Manager)를 통해서도 Premier 3400 Series 스위치를 관리할 수 있다.

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

2.5. 사용자 인증

2.5.1. 사용자 추가 및 삭제

시스템 운영자는 콘솔 포트나 telnet 을 통해서 스위치에 로그인 할 수 있다. 로그인을 위해서 사용자 등록이 필요하다. Premier 3400 series 스위치는 사용자를 추가, 삭제 할 수 있고 각각의 사용자에 대해 패스워드와 권한, session timeout 시간, Access List 를 지정할 수 있다.
사용자 권한은 privilege level 로 표현된다. privilege level 은 15 인 경우와 아닌 경우로만 구분하고, 0 에서 14 사이의 privilege level 간의 구분은 사용하지 않는다. privilege level 이 15 인 사용자는 enable mode 로 들어갈 수 있고, 그 외의 privilege level 을 갖는 사용자는 Privileged mode 로 들어갈 수 없다. 새로운 사용자를 등록하면 privilege level 이 1 인 사용자로 등록된다.

Notice Access List 에 대한 추가적인 정보는< 2.8. ACL>절을 참조하라

표 2-5. 스위치의 사용자 추가 및 삭제 명령어

명령어	설명	모드
`username userID nopassword`	■ userID 생성 ■ password 가 없다	Config
`username userID (password | secret) password` `username userID (password |secret) 0 password`	■ userID 생성 ■ 암호화되지 않은 password 를 입력받는다	Config
`username userID (password 7 | secret 5) password`	■ userID 생성 ■ 암호화된 password 를 입력받는다	Config
`username userID privilege <0-15> nopassword`	■ userID 생성 ■ password 가 없다	Config

	■ privilege 15 이면 가장높은 privilege (enable mode 진입허용)를 갖는다.	
username *userID* privilege <0-15> (password | secret) *password* username *userID* privilege <0-15> (password | secret) 0 *password*	■ userID 생성 ■ privilege 15 이면 가장높은 privilege(enable mode 진입허용)를 갖는다. ■ 암호화되지 않은 password 를 입력받는다	Config
username *userID* privilege <0-15> (password 7 | secret 5) *password*	■ userID 생성 ■ privilege 15 이면 가장높은 privilege(enable 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 *access-list-num*	■ 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 passowrd 로 바뀐다.	Config

2.5.1.1. 사용자 추가 및 삭제

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

```
username ubi secret 0 ubi
username admin privilege 15 password 0 admin
username admin timeout 50
!
Switch#
```

2.5.2. 패스워드 설정

Premier 3400 series 스위치는 시스템 보안을 위해 다음과 같은 2 개의 패스워드를 사용한다.

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

표 2-6. 스위치의 Enable 패스워드 설정 명령어

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

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

2.5.2.1. Privileged 모드 패스워드 설정

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

2.5.2.2. 패스워드 encryption 설정

위의 예에서 보듯이 패스워드 설정 후 `show running-config` 명령으로 설정된 패스워드를 볼 수 있다. 이를 방지하기 위하여 Premier 3400 Series 스위치는 패스워드 encryption 모드 설정을 지원한다.

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

2.5.3. 인증 방법 설정

2.5.3.1. 스위치에 login 시 인증 방법 설정

Premier 3400 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. ■ 여러가지 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`	■ 우선적으로 인증받을 인증방식을 설정한	Config

(local | radius | tacacs)	다.	
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
authorization exec tacacs	■ tacacs 로 인증받은경우 tacacs 서버에서 privilege level 을 얻어온다.	Config
no authorization exec tacacs	■ tacacs 서버에서 privilege level 을 얻어오지 않도록 한다.	Config
show authentication login	■ 인증방식의 순서와 사용여부를 보여준다	Enable

사용자 인증 설정

Premier 3400 series 스위치는 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 사용자 ID 와 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 RADIUS 서버를 이용하는 방법, TACACS+ 서버를 이용하는 방법이 있다. 이 3 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다. 한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID 와 패스워드를 다시 요청한다. RADIUS 나 TACACS+ 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID 와 패스워드를 다시 요청한다.

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

Switch#
```

2.5.3.2. privileged mode 진입시 인증 방법 설정

Premier 3400 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 데이터베이스에 기록된 정보를 사용하여 접속 권한이 주어진다.

표 2-8. 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	Enable

사용자 인증 설정

Premier 3400 series 스위치는 privileged mode 로 들어올 때 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 enable 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 TACACS+ 서버를 이용하는 방법이 있다. 이 2 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다.
한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 enable 패스워드를 다시 요청한다. TACACS+ 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 enable 패스워드를 다시 요청한다.

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

```
second          local     enable

Switch#
```

2.5.4. 인증 서버 설정

표 2-9. 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 패킷을 받아야하는 시간을 지정한다.	Config
`no radius-server timeout`	■ 설정된 timeout 시간을 삭제한다.(default 5 초)	Config

2.5.5. 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 2-10. 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 페킷을 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 3400 Series 스위치는 default 로 “Switch”를 hostname 으로 사용하며 운영자가 이를 변경할 수 있다.

표 2-11. 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 P3400
P3400(config)# end
P3400#

P3400# configure terminal
P3400(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 3400 Series 스위치를 관리하고자 할 때는 스위치의 환경 설정이 필요하다.

또한 SNMP 에이전트를 접근하기 위해서는 스위치에 하나 이상의 IP 주소 설정이 필요하다. IP 주소의 설정은 "*P3400 Series_User Guide_제 05 장_IP 환경 설정*" 문서를 참고하라.

표 2-12. SNMP 환경 설정 명령

명령어	설명	모드
`snmp-server agent-address` *`agent-addr`*	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정	Config
`no snmp-server agent-address` *`agent-addr`*	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정하지 않음	Config
`snmp-server contact` *`string`*	■ System contact 정보를 변경	Config
`no snmp-server contact` *`string`*	■ System contact 정보를 삭제	Config
`snmp-server location` *`string`*	■ System location 정보를 변경	Config
`no snmp-server location` *`string`*	■ System location 정보를 삭제	Config
`snmp-server community` *`string`* `[ro|rw [access-class` *`number`*`]]`	■ SNMP community 를 설정 ■ *ro* : read only ■ *rw* : read write ■ *number* : standard IP access-list <1-99>	Config
`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 SNMP trap 을 전송할	Config

	때 사용할 community 를 설정	
`no snmp-server trap-host A.B.C.D`	■ SNMP Trap Host 를 삭제	Config
`snmp-server trap-version 1`	■ SNMPv1 Trap 을 전송하도록 설정	Config
`no snmp-server trap-version`	■ SNMPv2 Trap 을 전송하도록 설정	Config

2.7.1. SNMP Community 설정

Community string 은 시스템과 원격 네트워크 관리자 사이의 간단한 상호 인증 기능을 제공한다. Premier 3400 Series 스위치는 두 가지 형태의 community string 을 지원한다.

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

```
Switch# configure terminal
Switch(config)# snmp-server community public ro
Switch(config)# snmp-server community private rw
Switch(config)# snmp-server community test1 rw access-class 1
Switch(config)# end
Switch# show running-config
!
snmp-server community public ro
snmp-server community private rw
snmp-server community test1 rw access-class 1
!
Switch#
```

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

2.7.2. SNMP Trap 설정

하나 이상의 네트워크 관리 단말이 인증된 trap receiver 로서 설정될 수 있다. Premier 3400 Series 스위치는 모든 trap receiver 에게 SNMP trap 을 전송한다.

```
Switch# configure terminal
Switch(config)# snmp-server trap-version 1
```

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server trap-host 192.168.0.3 community private
Switch(config)# end
Switch# show running-config
!
snmp-server trap-version 1
snmp-server trap-host 192.168.0.3 community private
snmp-server enable traps config slotAdd slotDel GBICAdd GBICDel
powerStatus fanStatus selfLoopDetect fanActivateStatus
snmp-server enable traps environ tempUpRise tempUpFall tempLowRise
tempLowFall
snmp-server enable traps multicast snoop snoopVlan proxyReport
proxyReportVlan
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
!
Switch#
```

Notice Premier 3400 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.

2.7.3. 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#
```

2.7.4. 시스템 담당자 설정

시스템을 관리하는 책임을 가지는 사람을 등록할 수 있다.

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

2.7.5. 시스템 구축 위치 설정

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

2.8. ACL (Access Control List)

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

Premier 3400 Series 는 표준 IP 액세스 리스트를 지원하며, <1-99>의 번호가 할당 될 수 있다.

표 2-13. 액세스 리스트 설정 명령

명령어	설명	모드
access-list <1-99> {**deny|permit**} *address*	■ 표준 IP 액세스 리스트를 설정 ■ *address* ::= {any | A.B.C.D/M}	Config
no access-list <1-199>	■ 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 access-list
Access-List 1
       permit  any
```

2.8.2.2. 모든 액세스 거부

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

2.8.2.3. 특정 호스트에서의 액세스만 허용

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

2.8.2.4. 특정 네트워크에서의 액세스만 허용

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

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

2.8.2.5. 특정 네트워크에서의 액세스만 거부

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

2.8.3. SNMP 연결에 액세스 리스트 설정

엑세스 리스트는 community 별로 적용되며, 설정된 엑세스 리스트는 snmp 를 통한 스위치로의 접속을 허용, 제한한다.
host 10.1.22.247 에서의 접속만을 허용하는 Access list 를 생성하여, snmp 접속을 제한하고자 할 때의 절차는 다음과 같다.

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

2.8.4. Telnet 연결에 액세스 리스트 설정

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 192.168.0.0/24
Switch(config)# username admin access-class 1
Switch# show running-config
!
username admin privilege 15 password 0 admin
username admin access-class 1
!
access-list 1 permit 192.168.0.0/24
!
Switch#
```

2.9. NTP 설정

2.9.1. NTP 개요

NTP (Network Time Protocol)는 네트웍을 통하여 시스템의 시간을 동기화하는 데 사용 되어지는 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 하기위해서는 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 하기위해서는 global 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
ntp master *stratum*	■ NTP master 로 동작하도록 한다.
no ntp master	■ NTP master 로서의 동작을 멈춤다.

2.9.4. NTP time zone 설정

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

명령어	설명
ntp timezone plus *HH:MM*	■ 설정된 Coordinated Universal Time (UTC)에 설정된 시간을 더하여 현제 시간을 표시한다.
ntp timezone minus *HH:MM*	■ 설정된 Coordinated Universal Time (UTC)에 설정된 시간을 빼서 현제 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 한시간 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*	■ 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

ntp server 203.248.240.103 에서 ntp 시간을 받아오려 할 경우 다음과 같이 설정하고 확인한다.

```
Switch#
Switch (config)# ntp server 203.248.240.103
Switch (config)# exit
Switch # show ntp
```

```
-----------------------------------------
Current time    : Thu Jan 12 20:40:25 2008
-----------------------------------------
NTP master             : disable
NTP stratum            : unspecified
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 #
```

timezone 정보를 우리나라에 맞게 변경하려 할 경우 다음과 같이 설정하고 확인한다.

```
Switch#
Switch# configure terminal
Switch(config)# ntp timezone plus 9:0
Switch(config)# end
Switch# show clock
Mon Jan 14 10:58:36 2008  GMT+9:0
Switch# show ntp
-----------------------------------------
Current time    : Mon Jan 14 10:58:39 2008
-----------------------------------------
NTP master             : disable
NTP stratum            : unspecified
Poll interval          : 6 (power of 2)
NTP timezone           : +9:0
NTP summertime         : none
NTP summertime start   : none
NTP summertime end     : none
-----------------------------------------
The list of NTP Server is below.
-----------------------------------------
-----------------------------------------
Switch#
```

3

인터페이스 환경 설정

3.1. 개요

Premier 3400 Series 스위치가 지원하는 인터페이스는 다음과 같다.

표 3-1. Premier 3400 Series 스위치가 지원하는 인터페이스

구분	종류
Physical interfaces	■ Fast Ethernet • 10/100Base-TX (Auto Negotiation) • 100Base-FX ■ Giga Ethernet • 1G-T • 1G-X
port-group interfaces	■ Port-group
VLAN Interfaces	■ VLAN

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.

3.2.1. Interface name

Premier 3400 Series 에서는 인터페이스에 대한 모든 환경 설정에서 interface name을 사용한다. Interface name은 다음과 같이 interface type과id로 구성된다.

표 3-3. Interface name

구분	Interface type	Interface name	예
Physical interface	Fast ethernet	“fa” + port_number	fa1
Physical interface	Giga ethernet	“gi” + port_number	gi1
Port-group interface	Port group	“po” + port-group id	po1
VLAN interface	VLAN	“vlan” + vlan id	vlan10

3.2.2. Interface id

Interface name은interface type과id로 구성되며 interface id는Premier 3400 Series 시리지 스위치 각 모델 마다 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)
P3400	Fast ethernet Giga ethernet Port group VLAN	port id port id port id vlan id	port id: 1-26 port id: 1-2 1 – 7 1 – 4094	fa1, fa26 gi1 po1, po7 vlan1, vlan4094

3.2.3. Interface 모드 프롬프트

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

```
Switch(config)# interface fa1
Switch(config-if-fa1)#
```

3.2.4. Interface-range 모드 프롬프트

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

```
Switch(config)# interface range fastethernet 1-10
Switch(config-ifrange)# speed 100
Switch(config-ifrange)# exit
Switch(config)#
```

위와 같이 설정하는 것은, 다음과 같이 반복 수행하는 것과 동일하다.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# speed 100
Switch(config-if-fa1)# exit
Switch(config)# interface fa2
Switch(config-if-fa2)# speed 100
Switch(config-if-fa2)# exit
(중략)
Switch(config)# interface fa10
Switch(config-if-fa10)# speed 100
Switch(config-if-fa10)# exit
```

3.2.5. range port 모드 프롬프트

range port 명령을 사용하여 range port 모드 사용이 가능하다. 이는 port interface 에 한해서만 가능하며, 현재 vlan 이나 기타 인터페이스는 지원하지 않는다.. Interface range 모드와는 다른 형태로 interface 명령어를 반복 수행한다.

```
Switch(config)# range-port
Switch(config-range-port)#
```

Range-port 모드에서는 모든 port interface 에서 사용 가능한 명령이 수행 가능하다. 단, 포트를 지정하기 위해서 [COMMAND] + [PORTRANGE] 형태로 조합된 명령어 체계를 사용한다.

```
Switch(config)# range port
Switch(config-range-port)# speed 100 fa1
Switch(config-range-port)#
```

이 명령은

```
Switch(config)# interface fa1
Switch(config-if-fa1)# speed 100
Switch(config-if-fa1)#
```

과 동일한 기능을 수행한다.

[PORTRANGE] 에는 단일 포트 뿐만 아니라, 포트 레인지를 조합해서 사용이 가능하다. Port prefix 와 (시작) – (끝) 형태의 레인지 조합으로 여러 포트를 지정할 수 있다. 예를 들어 **fa1-10** 은 fa1 부터 fa10 까지 10 개의 포트를 지칭한다. 또한, comma 를 이용해서 떨어져 있는 여러 포트를 묶어서 사용 가능하다. 예를 들면 **fa1 , fa3-4, fa9-10** 과 같은 형태로 사용이 가능하다.

```
Switch(config)# range-port
Switch(config-range-port)# speed 100 fa1 , fa3-4, fa9-10
Switch(config-range-port)#
```

fa1, fa3, fa4, fa9, fa10 포트에 각각 speed 100 이라는 명령을 수행하게 된다.

특정 포트에 대한 설정은 interface, interface range, range-port 의 3 가지 방법으로 설정이 가능하다. 그리고, show running-config 명령에 의해서 최종적으로 range-port 와 interface 의 2 가지로 구분되어 출력된다.

1. 여러 포트에 공통적으로 설정된 명령은 port range 를 이용해서 묶여서 출력된다.
2. 특정한 포트에만 설정된 명령은 interface 를 이용해서 출력된다.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# speed 100
Switch(config-if-fa1)# exit
Switch(config)# interface fa2
Switch(config-if-fa2)# speed 100
Switch(config-if-fa2)# exit
Switch(config)# interface fa3
Switch(config-if-fa3)# speed 10
Switch(config-if-fa3)# exit
Switch(config)# exit
Switch#
Switch# show running-config
!
range port
  speed 100 fa1-2
!
interface fa3
 speed 10
```

```
!
Switch#
```

fa1 과 fa2 에 공통적으로 설정된 speed 100 이라는 명령은, range port 기능을 이용해서 묶여서 출력되며, fa3 에 설정된 speed 10 이라는 명령은 fa3 에만 존재하는 명령이므로, interface 를 이용해서 출력된다.

이와 같은 range port 기능을 도입함에 따라, 동일한 설정이 반복적으로 수행되는 L2 스위치의 특성에 따라 아래와 같이 port interface 에 대한 show run 출력이 크게 감소하게 되며, 현재 설정에 대한 파악이 용이하다.

Range port 미사용시	Range port 사용시
interface fa1 shutdown switchport access vlan 100 ! interface fa2 shutdown switchport access vlan 100 description // fa2 is reserved // ! interface fa3 shutdown switchport access vlan 100 ! interface fa4 shutdown switchport access vlan 100 ! interface fa10 shutdown ! interface gi1 shutdown !	! range port shutdown fa1-4,fa10,gi1 switchport access vlan 100 fa1-4 ! interface fa2 description // fa2 is reserved // !

Notice PORT-GROUP 과 VLAN 에 대한 Interface Node 는 기존과 동일하게 유지한다.

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 interfaces [*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 interfaces 명령어

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

```
Switch# show interfaces
fa1 is up
 type 100Base-TX
 auto-negotiation
 speed set auto, current 100M
 duplex set full, current full

 Last clearing of counters 1w0d
 1 minutes input  rate 13,119 bytes/sec, 198 packets/sec
 1 minutes output rate 1,586 bytes/sec, 24 packets/sec
   1,396,695 packets input, 148,951,819 bytes
   Received 796,623 broadcasts, 96,388 multicasts
   0 CRC, 0 oversize, 0 dropped
   4,747 packets output, 455,150 bytes
   Sent 1 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
shutdown : (A)admin, (S)sld, (L)llcf
 ------------------------------------------------------------------------------
  ifname type  shutdown block link  nego  set-speed cur-speed flow-ctl link-cnt
 ------------------------------------------------------------------------------
```

```
fa1   FE-TX    .    .    up  auto   auto/full 100M/full    .        0
fa2   FE-TX    .    .    down auto   auto/full     .     .        0
fa3   FE-TX    .    .    down auto   auto/full     .     .        0
fa4   FE-TX    .    .    down auto   auto/full     .     .        0
fa5   FE-TX    .    .    down auto   auto/full     .     .        0
fa6   FE-TX    .    .    down auto   auto/full     .     .        0
fa7   FE-TX    .    .    down auto   auto/full     .     .        0
fa8   FE-TX    .    .    down auto   auto/full     .     .        0
fa9   FE-TX    .    .    down auto   auto/full     .     .        0
fa10  FE-TX    .    .    down auto   auto/full     .     .        0
fa11  FE-TX    .    .    down auto   auto/full     .     .        0
fa12  FE-TX    .    .    down auto   auto/full     .     .        0
fa13  FE-TX    .    .    down auto   auto/full     .     .        0
fa14  FE-TX    .    .    down auto   auto/full     .     .        0
fa15  FE-TX    .    .    down auto   auto/full     .     .        0
fa16  FE-TX    .    .    down auto   auto/full     .     .        0
fa17  FE-TX    .    .    down auto   auto/full     .     .        0
fa18  FE-TX    .    .    down auto   auto/full     .     .        0
fa19  FE-TX    .    .    down auto   auto/full     .     .        0
fa20  FE-TX    .    .    down auto   auto/full     .     .        0
fa21  FE-TX    .    .    down auto   auto/full     .     .        0
fa22  FE-TX    .    .    down auto   auto/full     .     .        0
fa23  FE-TX    .    .    down auto   auto/full     .     .        0
fa24  FE-TX    .    .    down auto   auto/full     .     .        0
gi1   GI-X     .    .    down manual 1G  /full     .     .        0
--------------------------------------------------------------------------------
```

Notice 이후부터 각 설정 사례에 대한 **CLI** 캡쳐화면은 **Premier 3400 series** 중심으로 했으므로 다른 모델 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
IFNAME   SWMODE N-VLAN TAGGED-VLAN-LIST
--------------------------------------------------------------------------------
fa1     access     1
fa2     access    10
fa3     access     1
fa4     access    20
fa5     access     1
fa6     trunk    100   10   20
fa7     access     1
```

```
fa8     access     1
fa9     access     1
fa10    access     1
fa11    access     1
fa12    access     1
fa13    access     1
fa14    access     1
fa15    access     1
fa16    access     1
fa17    access     1
fa18    access     1
fa19    access     1
fa20    access     1
fa21    access     1
fa22    access     1
fa23    access     2
fa24    access     2
fa25    access     1
fa26    access     1
po7     access     1
--------------------------------------------------------------------------------
```

3.4. 물리적 포트 환경 설정

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

표 3-6. 물리적 포트 환경 설정 명령어

명령어	설명	모드
shutdown **no shutdown**	■ 물리적 포트를 disable/enable	interface
block **no block**	■ 물리적 포트를 block/unblock	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 (on|off)	■ flow-control 설정/해제	interface

3.4.1. Shutdown

물리적 포트를 disable시킨다.

물리적 포트의 shutdown상태를 확인하려면 **show interface** 또는 **show port status** 명령을 사용한다.

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

3.4.2. Block

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

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

3.4.3. Speed / duplex

Premier 3400 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	auto	full
1000Base-X	on	1000	full
	off	1000	full

speed, duplex 설정시 다음 사항을 주의하라.

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

3.5. Port mirroring

Port mirroring은 특정 port(source port)의 입출력 트래픽을 운용자가 설정한 목적지 포트에 mirroring하는 기능으로 원하는 포트의 모든 패킷을 감시할 수 있다.
Premier 3400 Series는rx, tx 트래픽을 각각 여러 소스 포트로부터1개의 port또는 cpu로mirroring할 수 있다.

명령어	설명	모드
mirroring target (*ifname* | cpu)	■ 입력/출력 패킷이 mirroring 될 port 를 지정	config
mirroring rx-traffic	■ 해당 포트의 입력 패킷을 mirroring 토록 설정	interface
mirrorint tx-traffic	■ 해당 포트의 출력 패킷을 mirroring 토록 설정	interface

3.6. 2 계층 인터페이스 환경 설정

2계층 인터페이스는2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 Premier 3400 Series 스위치에서는 물리적 포트와 port-group interface가 이 모드로 동작한다.
이 절에서는2계층 인터페이스의 설명과 물리적 포트와 port-group을2계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여준다.

3.6.1. VLAN Trunking

트렁크(trunk)란 이더넷 스위치와 다른 네트워킹 장비(router, switch) 사이의 point-to-point 링크로서 단일 링크에 복수의 VLAN 트래픽을 전송할 수 있으며 이를 통하여 VLAN을 전체 네트워크에 확장할 수 있다.
Premier 3400 Series 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에trunk을 설정할 수 있다.

3.6.2. 2 계층 인터페이스 모드

Premier 3400 Series 스위치가 지원하는2계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있다.

표 7. Premier 3400 Series 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

3.6.3. 2 계층 인터페이스 기본 설정 값

Premier 3400 Series 스위치는 물리적 포트 또는 port-group이layer2 interface로 설정될 때 다음과 같은 기본(default) 설정 값을 가진다.

표 3-7. 2 계층 인터페이스 기본 설정 값

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

3.6.4. 2 계층 인터페이스 설정/해제

2계층 인터페이스로 설정 및 해제하기 위한 명령어는 다음과 같다.

표 3-8. 2 계층 인터페이스 설정 및 해제 명령어

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

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

3.6.5. Trunk port 설정

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

표 3-9. Trunk port 설정 명령어

명령어	설명	모드
switchport mode trunk	■ trunk mode 설정	interface
switchport trunk native vlan *<1-4094>*	■ trunk port native VLAN 설정	interface
no switchport trunk native vlan	■ 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>*	■ trunk port tagged VLAN 삭제	interface
switchport trunk remove all		

다음은 물리적 포트를2계층 트렁크 포트로 설정하는 예이다.

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

다음은 port-group 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
```

3.6.6. Access port 설정

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

표 3-10. Access port 설정 명령어

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

다음은 물리적 포트를2계층 access port로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# switchport          ! layer2 interface set
Switch(config-if-fa1)# switchport mode access     ! access port set
Switch(config-if-fa1)# switchport access vlan 5   ! native vlan set
```

다음은 port-group 인터페이스를2계층 access port로 설정하는 예이다.

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

3.7. Port group

3.7.1. Port group 개요

Port group 이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용한다. Premier 3400 Series 스위치에서 port group 인터페이스는2계층 인터페이스로 사용될 수 있다.
Premier 3400 Series 스위치의 모델 별 설정 가능한 port group 수는 다음과 같다.

모델	port group 수	그룹 당 최대 port
P3400	7	8

3.7.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같다.

표 3-11. 포트 그룹 설정 명령어

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

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

3.8. MAC Filtering

3.8.1. MAC Filtering 개요

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

3.8.2. MAC Filtering 설정

MAC Filtering 설정을 위한 기본 명령어는 다음과 같다.

표 3-12. mac-filter 설정 명령어

명령어	설명	모드
mac-filter *vlan-id mac-addr*	■ MAC Filter add	config
no mac-filter *vlan-id mac-addr*	■ MAC Filter delete	config

3.9. Traffic-control

3.9.1. Traffic-control 개요

특정 포트에서 과다한 트래픽이 유입되는 것을 방지하기 위한 port flood guard 의 한 방법이다. 정해진 트래픽 이상의 트래픽이 유입되면 해당 포트의 트래픽을 차단하거나 알람을 발생시키고. 트래픽 양이 정해진 양 이하로 줄어 들게 되면 정상 상태로 복귀한다.

3.9.2. Traffic-control 설정

Traffic-control 설정을 위한 기본 명령어는 다음과 같다. Traffic-control 을 pps 단위와 kbps 단위로 걸 수 있으며, inbound 또는 outbound 트래픽을 기준으로 설정할 수도 있다. 또한, pps 의 경우는 트래픽 유형별로 unicast, multicast, broadcast를 구분하여 설정이 가능하며, 모든 트래픽 총량으로도 설정이 가능하다. 만약 여러 가지 항목에 대해서 설정한 경우, 한가지 경우에만 해당되어도, 트래픽 차단 기능이 동작한다.

Block-mode 에서는 해당 포트를 차단하여, 트래픽을 제한하고, 알람을 발생시키며, alarm-only 모드에서는 포트는 차단하지 않은 채 알람만 발생시킨다.

Report-interval 을 해당 포트의 트래픽 양을 기준으로 알람을 발생 또는 해제시키는 시간 간격이며 분 단위로 설정한다.

Observing-period 는 트래픽 집계를 하기 위해서 보는 기준이다. 예를 들어 10으로 설정하면 과거 10분간의 트래픽량을 기준으로 통계를 낸다.

Alarm-mode 는 high threshold 에 대해서는 once / repeatable / disable 의 세가지 모드가 설정 가능하며 low threshold 에 대해서는 once / disable 의 두 가지 모드가 설정 가능하고, 이 둘을

조합하여 설정한다. 만약 트래픽이 설정치를 초과했을 때 1회, 해제되었을 때 1회씩만 발생하게 하려면 high once low once 로 설정하면 된다. 만약 트래픽이 설정치를 초과해 있는 동안에 매 report-interval 마다 반복적으로 알람이 발생하고, 해제 알람은 발생하지 않도록 하고 싶을 경우는 high repeatable low disable로 설정하면 된다. 만약 차단은 시키고자 하나 알람을 발생시키지 않고자 할 때는 high disable low disable로 설정한다.

표 3-13. traffic-control 설정 명령어

명령어	설명	모드
traffic-control pps <all|unicast|multicast|broadcast> <inbound|outbound> <1-1500000> <1-1500000> block-mode	해당 포트의 트래픽을 inbound 또는 outbound 트래픽의 해당 유형별 트래픽량을 기준으로 pps 단위로 설정하며, block-mode 로 설정한다..	interface
traffic-control pps <all|unicast|multicast|broadcast> <inbound|outbound> <1-1500000> <1-1500000> alarm-only	해당 포트의 트래픽을 inbound 또는 outbound 트래픽의 해당 유형별 트래픽량을 기준으로 pps 단위로 설정하며, alarm-only 로 설정한다..	interface
no traffic-control pps <all|unicast|multicast|broadcast> <inbound|outbound>	해당 설정을 해제한다.	interface
traffic-control kbps all <inbound|outbound> <1-1000000> <1-1000000> block-mode	해당 포트의 트래픽을 inbound 또는 outbound 트래픽 총량을 기준으로 kbps 단위로 설정하며, block-mode 로 설정한다..	interface
traffic-control kbps all <inbound|outbound> <1-1000000> <1-1000000> alarm-only	해당 포트의 트래픽을 inbound 또는 outbound 트래픽 총량을 기준으로 kbps 단위로 설정하며, alarm-only 로 설정한다..	interface
no traffic-control kbps all <inbound|outbound>	해당 설정을 해제한다.	Interface
traffic-control report-interval <1-1440>	알람을 몇 분마다 발생시킬지 설정한다.	Config
traffic-control observing-period <1-1440>	트래픽 통계를 내기 위해 집계하기 위한 시간 설정	Config
Traffic-control alarm-mode high <once|repeatable|disable> low <once|disable>	High threshold 과 low threshold 에서 알람을 1 회발생/반복발생/발생안함 중 어떤 모드로 동작 시킬지 설정	Config
show traffic-control	현재의 설정 및 상태를 보여준다.	Privileged

```
Switch(config)# traffic-control report-interval 2
Switch(config)# traffic-control oberserving-period 2
Switch(config)# interface fa1
Switch(config-if-fa1)# traffic-control pps unicast inbound 100000 50000 alarm-only
Switch(config-if-fa1)# traffic-control pps broadcast inbound 100000 50000 alarm-only
Switch(config-if-fa1)# end
```

```
Switch# show traffic-control
Traffic Contorl Status

 Report Interval  : 1 minutes
 Observing Period : 1 minutes
 Alarm Mode       : High - Once , Low - Once

 Interface : fa1
  Status   : Normal
                    High       Low   Average  1 Minute   Alarm
                Threshold Threshold      Rate      Rate   Count Last Alarm Time
-------------------------------------------------------------------------------
 PPS
       All  In :        -         -         -         -       -
   Unicast  In :   100000     50000         0         0       0
  Broadcast  In :   100000     50000         0         0       0
  Multicast  In :        -         -         -         -       -
       All Out :        -         -         -         -       -
    Unicast Out :        -         -         -         -       -
  Broadcast Out :        -         -         -         -       -
  Multicast Out :        -         -         -         -       -

 KBPS
       All  In :        -         -         -         -       -
       All Out :        -         -         -         -       -
-------------------------------------------------------------------------------
 total 1 entries found
```

4

가상 랜(VLAN)

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

이 장에서는 다음의 내용들을 다룬다:

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

4.1. VLAN 개관

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

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 촉약, 그리고 트래픽 흐름 제어를 제공한다. 정의된 그룹내의 스위치는 두 VLAN 사이에서 브로드캐스트 프레임뿐 아니라 어떠한 프레임도 전달하지 않는다.

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 3400 Series 스위치는 최대 256 개의 VLAN 을 지원한다. VLAN 은 다음의 기준에 따라 생성된다:

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

4.2.1. 포트 기반 VLAN(Port-Based VLANs)

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

예를 들면, <그림 4-1>의 Premier 3400 Series 스위치에서 1, 2, 3, 4 포트는 VLAN A 의 access 포트이고, 21, 22, 23, 24 포트는 VLAN B 의 access 포트로 할당된다. 그리고 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18 포트는 VLAN C 의 access 포트로 정의한다.

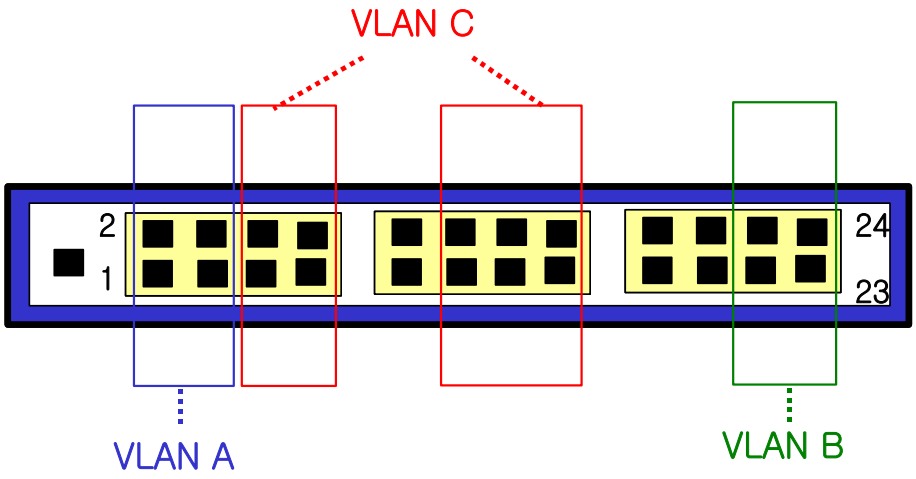


그림 4-1. Premier 3400 Series 스위치의 포트 기반 VLAN 구성 예

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

포트 기반 VLAN 으로 스위치 묶기

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

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

<그림 4-2>는 서로 다른 2 개의 Premier 3400 series 스위치를 하나의 VLAN 으로 묶는 방법을 보여준다. 먼저 스위치 1 의 4 개의 포트는 VLAN A 로 포함되도록 할당되어 있다. 또한 스위치 2 의 4 개 포트도 VLAN A 의 access 포트로 할당되어 있다. 두 스위치는 <그림 4-2>와 같이 상호 연결하여 하나의 브로트 캐스트 도메인을 형성한다.

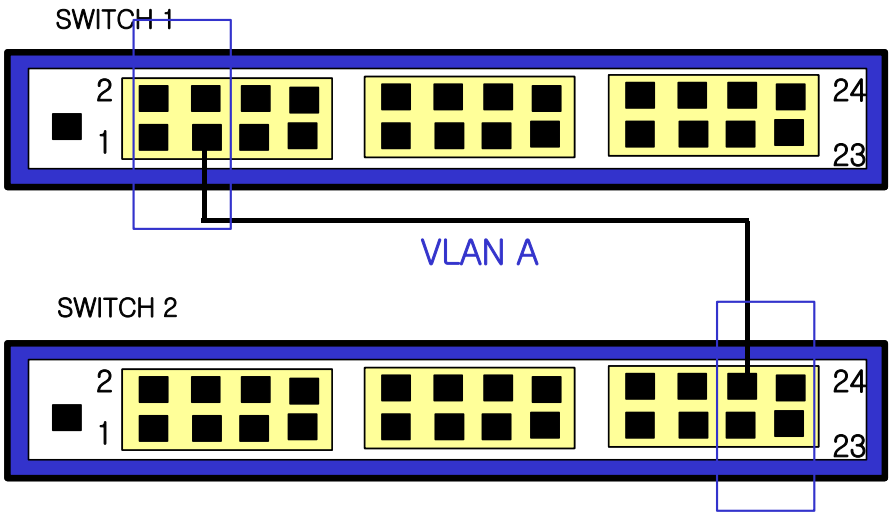


그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

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

<그림 4-3>은 두개의 Premier 3400 Series 스위치에 걸쳐서 설정되는 두개의 VLAN 을 보여준다. 스위치 1 에서 포트 3, 4, 5, 6 포트는 VLAN A 의 access 포트이고 9, 10, 11, 12, 13, 14 까지의 포트는 VLAN B 의 access 포트로 할당되어 있다.

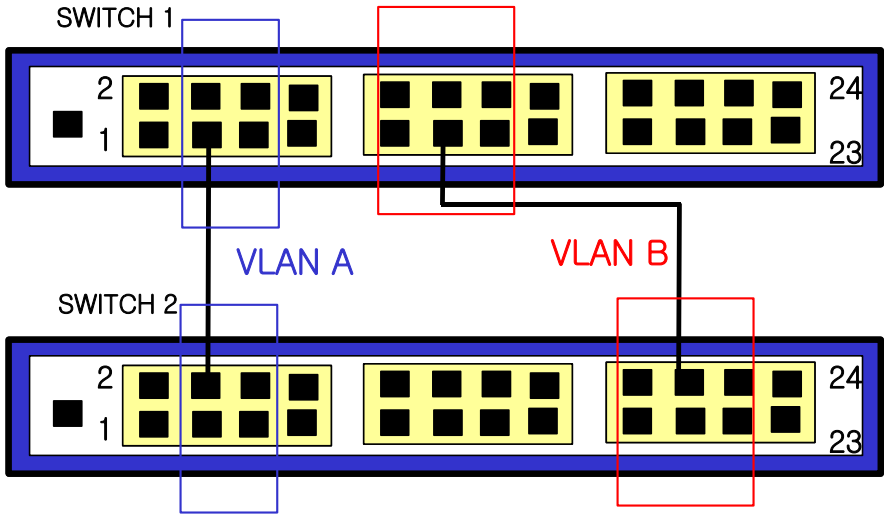


그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

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

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

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

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

VLAN 태그의 할당(Assigning a VLAN Tag)

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

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

Notice VLAN 이 설정되지 않은 포트로 그 VLAN 의 태그 프레임이 수신되면, 프레임은 폐기된다. 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 붙지않은 프레임을 사용하는 네트워크의 물리적인 구성을 보여준다.

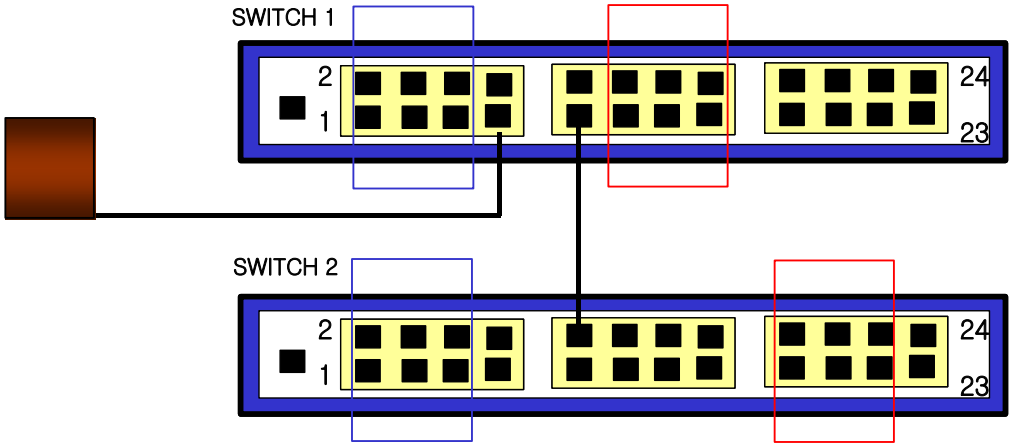


그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<

그림 4-5>은 동일한 네트워크의 논리적인 다이어그램을 보여준다.

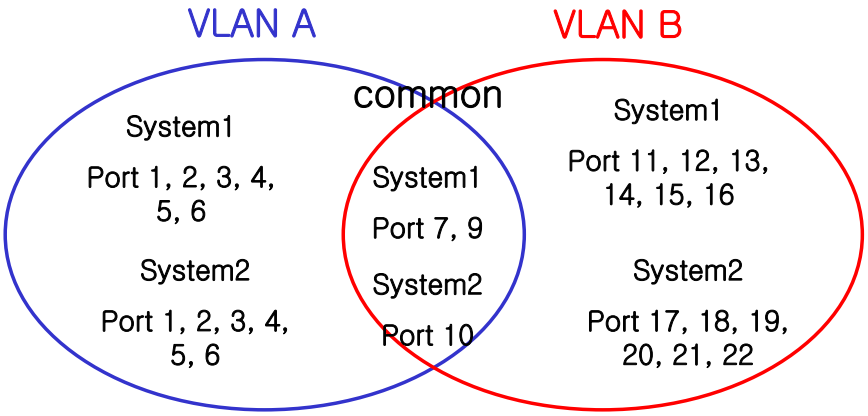


그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

< 그림 4-4>와 <그림 4-5>에서:

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

프레임이 스위치를 지나갈 때, 스위치는 목적지 포트에 대해 태그가 붙은 프레임을 사용할 지 태그가 붙지 않은 프레임을 사용할지를 결정한다. 서버로부터 송수신되는 모든 프레임과 트렁크 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 식별하기위한 VLAN id 의 값으로 1 부터 4,094 사이의 숫자를 사용할 수 있다. 스위치가 초기화되었을 때 기본적으로 하나의 VLAN 이 생성되어 있으며(*default VLAN*), 이 VLAN 이 VLAN id 의 값으로 1 을 사용한다. 따라서 새로 만들어지는 VLAN 은 VLAN id 의 값으로 1 을 사용할 수 없다.

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

4.3.2. Default VLAN

스위치에는 다음과 같은 특성을 가지는 default VLAN 이 설정되어 있다.

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

4.3.3. Native VLAN

각 물리적 포트는 PVID(Port VLAN ID)를 가지고 있다. 모든 802.1Q 포트에는 자신의 native VLAN 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 붙지않은 프레임이 수신된다면, 프레임에 포함된 PVID 값을 태그로 간주한다.

<그림 4-6>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.

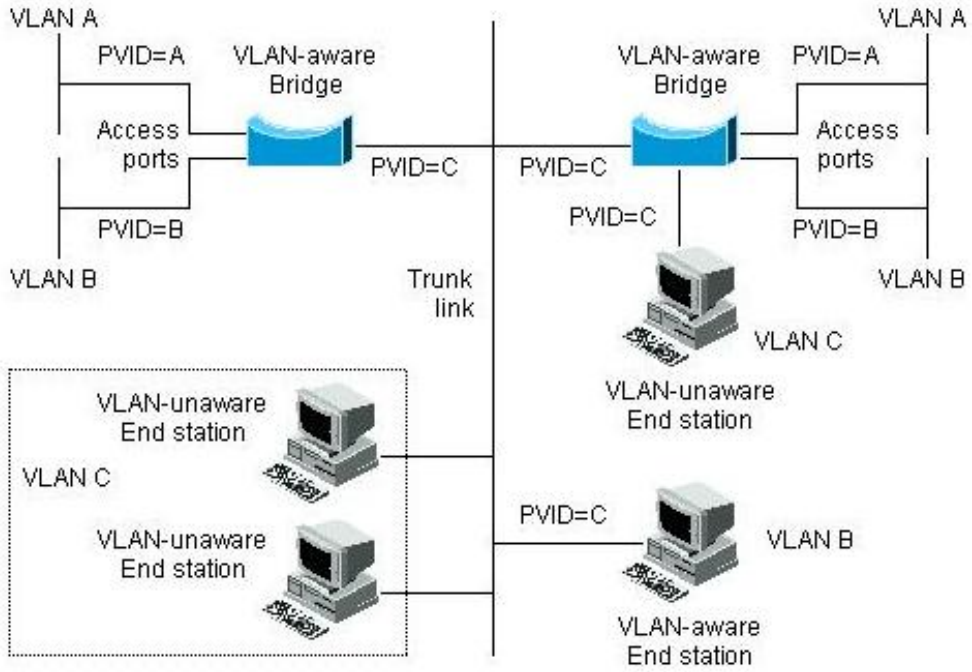


그림 4-6. Native VLAN

예를 들어 <그림 4-6 >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 3400 Series 스위치에 VLAN 을 설정에 사용되는 명령들을 설명한다. VLAN 설정은 다음의 단계로 진행된다.

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

4.4.1. VLAN 설정 명령

<표 4-1>은 VLAN 설정에 사용되는 명령들을 설명한다.

표 4-1. VLAN 설정 명령어

명령어	설명	모드
`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(태크 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 4049 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

명령어	설명	모드
`switchport trunk native` *`vlanid`*	■ 포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 붙지않고 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

4.5. VLAN 설정 예제

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

```
Switch(config)# vlan 1000
Switch(config)# interface vlan1000
Switch(config-int-vlan)# ip address 132.15.121.1/24
Switch(config-int-vlan)# interface fa2
Switch(config-int-fa2)# switchport mode access
Switch(config-int-fa2)# switchport access vlan 1000
Switch(config-int-fa2)# interface fa4
Switch(config-int-fa4)# switchport mode access
Switch(config-int-fa4)# switchport access vlan 1000
```

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

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

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

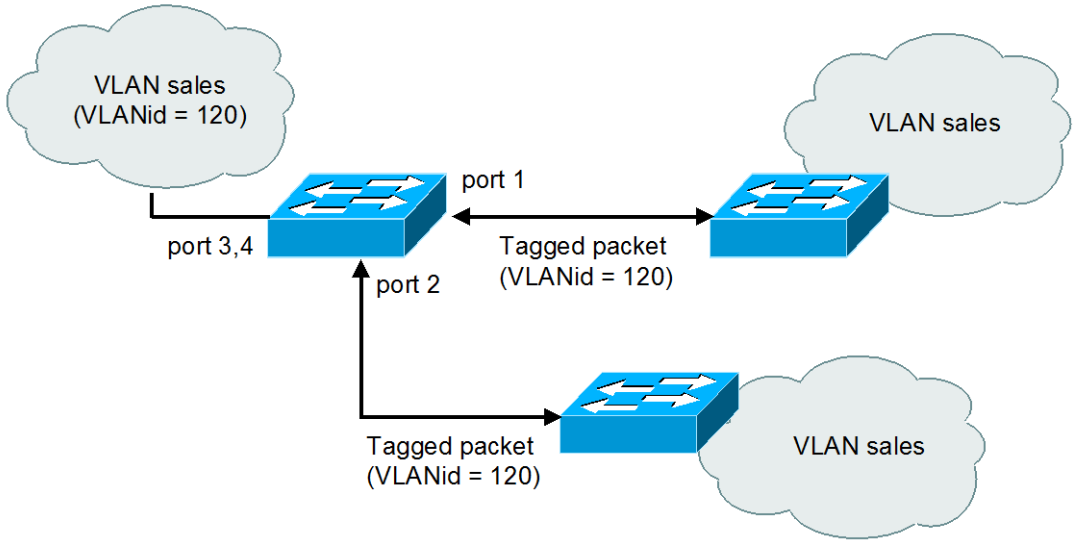


그림 4-7. VLAN 설정 예제 – Tagged and Untagged VLAN

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

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

```
Switch(config)# vlan  200
Switch(config)# vlan  400
Switch(config-vlan)# exit
Switch(config)# interface  fa1
Switch(config-int-fa1)# switchport  mode  trunk
Switch(config-int-fa1)# switchport  trunk  native  200
Switch(config-int-fa1)# switchport  trunk  add  400
```

포트 fa1 로 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 fa1   fa2  fa3  fa4  fa5  fa6  fa7  fa8  fa9  fa10  fa11  fa12
   2 fa13  fa14  fa15
  11 fa16  fa17  fa18  fa19  fa19  fa20  fa21  fa22  fa23  fa24
--------------------------------------------------------------------------------
Switch#
```

5

IP 환경 설정

5.1. 개요

본 장에서는 IP 주소를 설정하는 방법을 설명한다.

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

Premier 3400 Series 스위치는 다음의 인터페이스에 IP 를 할당 할 수 있다.

- VLAN interface

5.2. 네트워크 인터페이스에 IP 주소 할당

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

표 5-1. 사용 가능한 IP 주소

Class	주소 범위	상태
A	0.xxx.xxx.xxx	예약
	1.xxx.xxx.xxx ~ 126.xxx.xxx.xxx	사용가능
	127.xxx.xxx.xxx	예약 (loopback)
B	128.0.xxx.xxx	예약

	129.0.xxx.xxx ~ 191.254.xxx.xxx	사용가능
	191.255.xxx.xxx	예약
C	192.0.0.xxx	예약
	192.0.1.xxx ~ 223.255.254.xxx	사용 가능
	223.255.255.xxx	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 3400 Series 스위치는 하나의 인터페이스에 복수의 IP 주소를 할당하는 기능을 지원한다. Premier 3400 Series 스위치는 인터페이스 당 최대 2 개의 IP 주소를 설정할 수 있다. 다양한 상황에서 복수개의 IP 주소가 유용하게 사용된다. 다음은 가장 일반적인 응용이다:

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

- 많은 오래된 네트워크들은 계층 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 네트웍을 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
show arp	■ ARP 테이블의 엔트리를 출력한다.

5.4. Default Gateway 설정

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

표 5-4. Default gateway 설정 명령어

명령어	설명
ip default-gateway *gateway-ipaddress*	■ Default gateway 를 등록한다. ■ gateway-ipaddress : 게이트웨이 장치의 IP 주소를 명시한다.

Default gateway 정보를 확인하려면 privileged 모드에서 다음의 명령을 사용하라.

명령	설명
show ip default-gateway **show ip route**	■ Default gateway 정보를 출력한다.

5.5. IP 설정 예제

이 절에서는 IP 주소 설정 예제를 제공한다:

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

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

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

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제이다.

```
Switch# show arp
------------------------------------------------------------------------
 IP Address      MAC Address     IPF      PORT   Flags
------------------------------------------------------------------------
192.10.25.190   0000.f083.f6d4  vlan5   fa2    S
------------------------------------------------------------------------
 total 1 entries found
```

다음의 예제는 스위치의 default gateway 로 192.10.25.254 를 설정한다.

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

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

6 DHCP RELAY

6.1. DHCP Relay 기능 및 설정

6.1.1. 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 3400 스위치가 DHCP Relay Agent 로서 DHCP 클라이언트의 IP 요청 메시지를 DHCP Server 로 전달하는 절차이다.

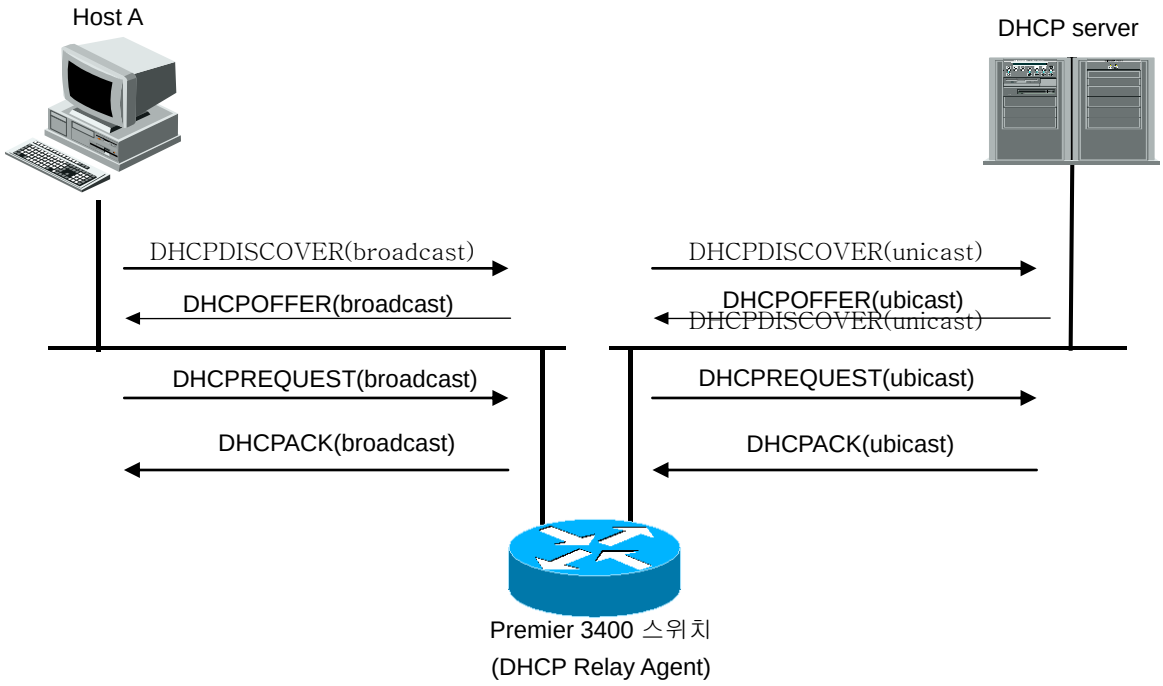


그림 6-1. DHCP Relay Agent 로서 DHCP Server 의 메시지 전달

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

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

14) 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.

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

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

6.2. DHCP relay agent 설정

Premier 3400 series 를 DHCP relay agent 로 사용하면 DHCP 클라이언트로부터의 DHCP 요구를 설정된 DHCP Server 로 중계하게 된다.

6.2.1. Premier 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
```

6.2.2. DHCP relay agent 에서 서버 설정

DHCP relay agent 에서 DHCP Server 를 설정하기 위해서는 Global 설정 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 ■ DHCP Server 의 삭제는 이 명령의 **no** 형태를 사용

Notice Premier 3400 series 의 DHCP relay Agent 는 helper-address 를 최대 20 개까지 설정 가능하다.

다음의 예제는 DHCP Relay Agent 에서 Server 주소를 지정하는 예제이다.

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

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

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

6.2.3. 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. 예를들어 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.

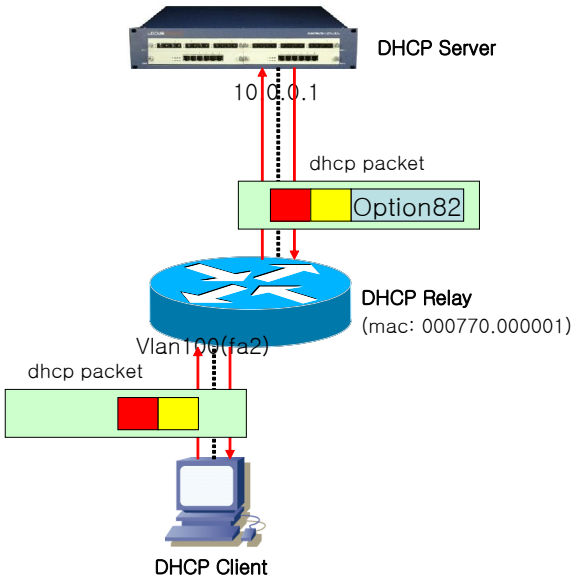


그림 6-2. DHCP Relay Option82

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.

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
```

Relay information option 재중계 정책 설정

기본적으로, Premier 3400 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
```

6.2.4. 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.

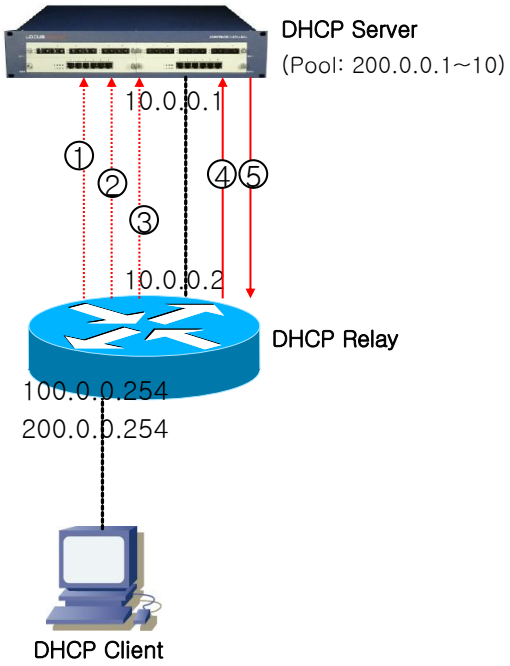


그림 6-3. DHCP Smart-Relay 동작 절차

1) 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.
2) 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.
3) 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)#
```

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

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

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

6.2.5. 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
```

6.2.6. 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.

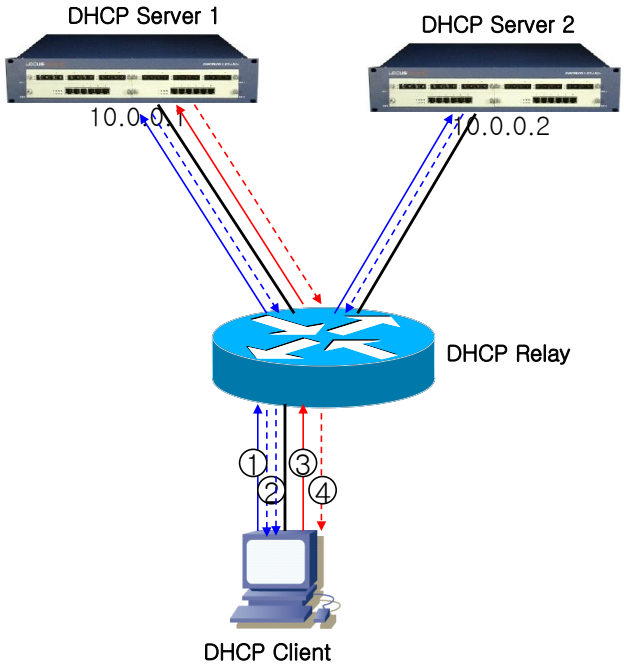


그림 6-4. DHCP Relay Server-Id-Relay 동작 절차

4) DHCP Client 로부터 DHCPDISCOVER 패킷을 받은 DHCP Relay Agent 는 자신에게 등록된 DHCP Server 1, DHCP Server 2 에게 패킷을 각각 포워딩한다.
5) 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.
6) 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.
7) 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
```

6.3. DHCP relay 모니터링 및 관리

표 6-1. DHCP relay 모니터링 및 관리 명령어

명령어	설명
show ip dhcp relay	■ DHCP Relay Confiuration 을 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

6.4. DHCP Relay 설정 예제

이 절에서는 다음의 설정 예를 제공한다.

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

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

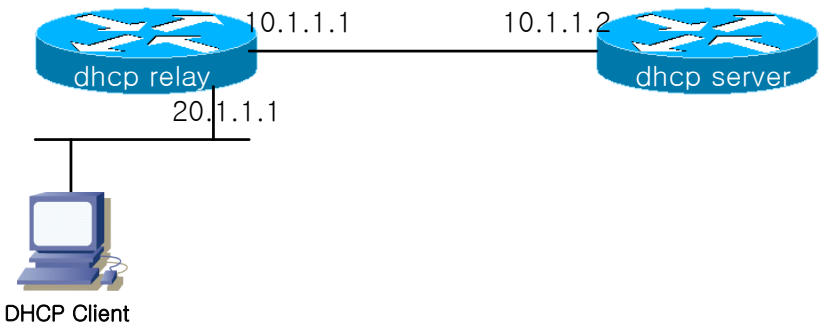


그림 6-5. 예제 네트워크 – DHCP Relay agent 환경 설정

```
Switch(config)# configure terminal
Switch(config)# ip dhcp-server 10.1.1.2
Switch(config)# service dhcp relay
Switch(config)# end
Switch#
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 maximum hop count        : 10

DHCP helper-address is configured on following servers:
  10.1.1.2

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
```

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)

6.5. DHCP Snooping 기능

6.5.1. 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.

6.5.1.1. 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.

6.5.1.2. 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.

6.5.1.3. 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.

6.5.1.4. 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.

6.6. DHCP Snooping 설정

Premier 3400 Switch 에서 DHCP Snooping 을 동작 시키면, 장비를 통과하는 모든 DHCP 패킷을 Snooping 하여 DHCP Client 정보 및 IP Lease 정보, Client 가 연결되어 있는 인터페이스 정보 등을 가지는 DHCP Snooping Binding Entry 를 생성한다.

6.6.1. 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
```

6.6.2. 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)#
Switch(config)#
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
```

```
Verification of hwaddr field is enabled
Insertion of option 82 is disabled
DHCP snooping is configured on following VLANs:
 vlan1
```

6.6.3. 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.

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
```

DHCP Snooping information option 재중계 정책 설정

기본적으로, Premier 3400 스위치의 DHCP Snooping information 정책은 DHCP 클라이언트로부터 수신한 패킷 내에 information Option 정보가 있으면 패킷을 Drop 시킨다. Premier 3400 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 패

	킷은 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
```

6.6.4. 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 ‘fa1’을 Trust Port 로 설정한다.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# ip dhcp snooping trust
Switch(config-if-fa1)# end
Switch# show ip dhcp snooping interface
Interface          Trust State    Max Entry
---------------    -----------    ------------
fa1                Trusted               2000  0
fa2                Untrusted             2000  1
fa3                Untrusted             2000  2
fa4                Untrusted             2000  3
fa5                Untrusted             2000  4
```

```
fa6                 Untrusted               2000   5
fa7                 Untrusted               2000   6
fa8                 Untrusted               2000   7
fa9                 Untrusted               2000   8
fa10                Untrusted               2000   9
fa11                Untrusted               2000   10
fa12                Untrusted               2000   11
fa13                Untrusted               2000   12
fa14                Untrusted               2000   13
fa15                Untrusted               2000   14
fa16                Untrusted               2000   15
fa17                Untrusted               2000   16
gi1                 Untrusted               2000   17
```

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

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# ip dhcp snooping max-entry 100
Switch(config-if-fa1)# end
Switch# show ip dhcp snooping interface
Interface           Trust State    Max Entry
---------------     -----------    ------------
fa1                 Trusted                 100   0
fa2                 Untrusted              2000   1
fa3                 Untrusted              2000   2
fa4                 Untrusted              2000   3
fa5                 Untrusted              2000   4
fa6                 Untrusted              2000   5
fa7                 Untrusted              2000   6
fa8                 Untrusted              2000   7
fa9                 Untrusted              2000   8
fa10                Untrusted              2000   9
fa11                Untrusted              2000   10
fa12                Untrusted              2000   11
fa13                Untrusted              2000   12
fa14                Untrusted              2000   13
fa15                Untrusted              2000   14
fa16                Untrusted              2000   15
fa17                Untrusted              2000   16
```

```
gi1                 Untrusted               2000   17
Switch#
```

6.6.6. 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
  <5-65535>  Minutes
Switch(config)# ip dhcp snooping entry-time 10
Switch(config)# ex
Switch# sh ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
 vlan1
```

6.6.7. 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
  <1-100>  DHCP Packet rate-limit in pps
Switch(config)# ip dhcp snooping rate-limit 100
```

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

6.6.8. 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
```

6.6.9. 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 fa2 포트에 연결되어 IP 100.0.0.10 을 사용하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping binding 1111.2222.3333 vlan 1 100.0.0.10
interface fa2
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
             (H) - Invalid Client HW Address, (R) - Rate Limit Dropped
             (M) - Mac Validation Check Dropped

Mac Address    IP Address        State                  Lease(sec) Vlan Interface
-------------- --------------- ------------------- ---------- ---- ---------
1111.2222.3333 100.0.0.10      Manual                 Infinite      1 fa2
total 4 bindings found
```

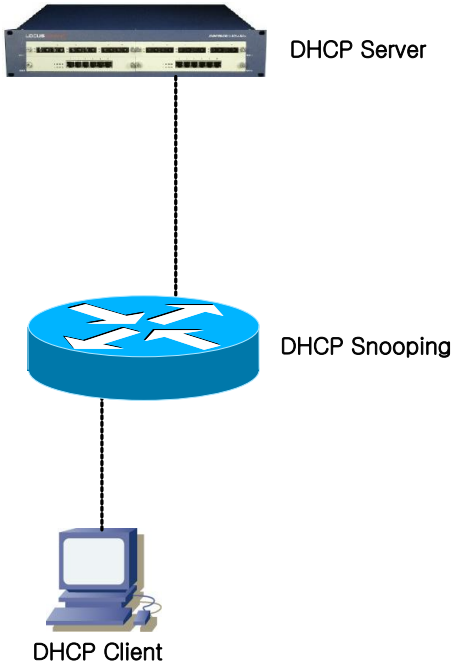
6.7. DHCP Snooping 모니터링 및 관리

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

6.8. DHCP Snooping 설정 예제

다음 예제는 DHCP Server 와 DHCP Client 사이에 위치한 Premier DHCP Snooping Switch 가 DHCP 패킷을 Snooping 하여 DHCP Snooping Binding Entry 를 생성한다.




```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 200
Switch(config)# ip dhcp snooping
Switch (config-if-vlan200)# end
Switch# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
                (H) - Invalid Client HW Address, (D) - Rate Limit Dropped

   MacAddress       IpAddress        State       Lease(sec)     VlanId      Port
   -----------      ---------       -------      ---------     ------      ----
 0000.864a.c185   100.0.0.100       Ack             87          200        fa1/8
```

6.9. Reference

[1] RFC2131 - Dynamic Host Configuration Protocol

[2] RFC3046 - DHCP Relay Agent Information Option

[3] Configuring the Cisco IOS DHCP Relay Agent

7

IGMP Snooping

본 장에서는 Premier 3400 Series 스위치에서의 IGMP Snooping 설정에 대해 설명한다.

7.1. IGMP Snooping 개요

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

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

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

7.2. IGMP Snooping 설정

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

7.2.1. Enable Global IGMP Snooping

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

명령어	설명
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 Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED


_____________________________________________________________
total : 0
```

7.2.2. 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 fa1
Switch (config-if-fa1)# igmp-trap
Switch (config-if-fa1)# end
Switch # show running-configure
…
!
interface fa1
 igmp-trap
!
…
```

7.2.3. Enable IGMP Snooping on a VLAN

본 장비에서는 IGMP Snooping 을 VLAN 별로 enable/disable 해야 한다.

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)# exit
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
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4

_____________________________________________________________
total : 1
```

7.2.4. Configure IGMP Snooping Functionality

IGMP Snooping 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행한다.

7.2.4.1. 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, IGMPv2 Report 메시지에 한해서 적용된다.

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

```
Switch # configure terminal
Switch (config)# ip igmp snooping report-suppression
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4

_____________________________________________________________
total : 1
```

7.2.4.2. fast-leave 설정

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

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

명령	설명
ip igmp snooping vlan *<1-4096>* **fast-leave**	특정 VLAN 에 fast-leave 기능을 설정한다.
no ip igmp snooping vlan *<1-4096>* **fast-leave**	특정 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 fa1
Switch (config)# ip igmp snooping vlan 1 fast-leave fa2
Switch(config)# exit
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
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4
_____________________________________________________________
total : 1
```

7.2.4.3. 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 등록이 되며, Multicast Traffic 뿐만 아니라 Host 에서 전송하는 IGMP Join 메시지도 Mrouter 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*	mrouter port 의 설정을 삭제한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter interface fa1
Switch(config)# exit
Switch# show ip igmp snooping mrouter
  VLAN      MULTICAST-ROUTER-PORT
  0001      fa1

_____________________________________________________________
total : 1
```

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>* **mrouter learn pim-dvmrp**	PIM/DVMRP 프로토콜을 Snooping 하여 mrouter port 를 감지하도록 설정한다.
no ip igmp snooping vlan *<1-4096>* **mrouter learn pim-dvmrp**	설정된 mrouter port 감지 방법을 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Switch(config)# exit
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
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4

_____________________________________________________________
total : 1
```

7.2.4.4. 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 관리되어진다. IGMP Snooping 은 이러한 IGMP 프로토콜 메시지들을 이용하여 Multicast Forwarding Table Entry 의 outgoing port 들을 추가/삭제한다.

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

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

명령어	설명
ip igmp snooping aging *<30-3600>*	aging time 을 설정한다. (default : 300 초)
no ip igmp snooping aging	설정된 aging time 을 default aging time 으로 변경한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping aging 250
Switch(config)# exit
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 250 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit         : DISABLED
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4

_____________________________________________________________
total : 1
```

7.2.4.5. 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 aging time 이후에 Multicast Forwarding Table Entry 에서 삭제된다.
설정된 aging time 의 종료전에 좀 더 빨리 Multicast Membership 관리가 이루어 질수 있도록 last-member-join-interval 을 설정할 수 있다.

만약, last-member-join-interval 이 설정되어 있지 않다면 last-member-join-interval 은 aging time 과 동일하게 자동으로 설정되며, 해당 포트는 IGMP Snooping 의 aging time 에 준하여 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 : 300 초)
no ip igmp snooping last-member-join-interval	설정된 last-member-join-interval 을 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping last-member-join-interval 5
Switch(config)# exit
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval            : 250 sec
 - Last Member Join Interval : 5 sec
 - TCN Query Solicit         : DISABLED
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : DISABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4

_____________________________________________________________
total : 1
```

7.2.4.6. 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 삭제한다.

```
Switch # configure terminal
Switch (config)# ip igmp snooping tcn query-solicit
Switch(config)# exit
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval             : 250 sec
 - Last Member Join Interval  : 5 sec
 - TCN Query Solicit          : ENABLED
 - IGMP Report Suppression    : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host        : DISABLED
 - Query Interval             : 60s
 - Query Based Port           : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
             fa1   fa2   fa3   fa4

_____________________________________________________________
total : 1
```

7.2.4.7. igmp filtering 설정

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

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

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

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

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

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

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

7.2.4.8. 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 적용한다.
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 fa1 10
Switch # show running-configure

…
ip igmp snooping
ip igmp snooping max-group-count fa1 10
…
```

7.2.4.9. 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 VLANinterface 에서 해제한다.

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

…
ip igmp snooping
ip igmp snooping max-reporter-count vlan 1 10
…
```

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 fa1 10
Switch (config)# exit
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-reporter-count port fa1 10
…
```

7.2.4.10. 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
…
```

7.2.4.11. 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 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 snooping ignore-mpkt-upstream-forward
Switch(config)# exit
Switch # show running-configure

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

7.3. 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. 따라서 Multicast Router 로부터 IGMP Query 를 수신한 경우, IGMP Host 로서 IGMP Report 를 전송하고, 가입자의 IGMP Membership 을 관리하기 위해서 주기적으로 IGMP General Query 가 전송되며, IGMP Leave 를 수신시 IGMP Specific Query 가 발생된다.

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.

7.4. IGMP Proxy-Reporting 설정

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

7.4.1. Enable IGMP Proxy-Reporting

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

명령어	설명
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)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval             : 250 sec
 - Last Member Join Interval  : 5 sec
 - TCN Query Solicit          : ENABLED
 - IGMP Report Suppression    : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host        : ENABLED
 - Query Interval             : 60s
 - Query Based Port           : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
             fa1   fa2   fa3   fa4   gi1   gi2

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

7.4.2. Enable IGMP Proxy-Reporting on a VLAN

본 장비에서는 IGMP Proxy-Reporting 을 VLAN 별로 enable/disable 할 수 있다.
실제 IGMP Proxy-Reporting 기능이 적용될 VLAN 을 설정하기 위해서는 다음의 명령을 global configuration mode 에서 사용한다.
IGMP Proxy-Reporting 기능이 적용된 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 vlan 1
Global IGMP Snooping configuration:
 - Aging Interval            : 250 sec
 - Last Member Join Interval : 5 sec
 - TCN Query Solicit         : ENABLED
 - IGMP Report Suppression   : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host       : ENABLED
 - Query Interval            : 60s
 - Query Based Port          : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is ENABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
             fa1  fa2  fa3  fa4

_____________________________________________________________
total : 1
```

7.4.3. Configure IGMP Proxy-Reporting Functionality

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

7.4.3.1. 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 (config)# exit
Switch # show running-configure
!
ip igmp snooping proxy-reporting
ip igmp snooping proxy-reporting vlan 1
ip igmp snooping proxy-reporting vlan 1 static-group 224.1.1.1
!
```

7.5. 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 *<1-4094>*	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 *<1-4094>*	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 *<1-4094>*	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 *<1-4094>*	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 statistics	Igmp packet 에 대한 통계 정보를 보여준다.

표 2 설정 예제

```
interface fa1
  igmp-trap
  ip igmp snoop-filter 1
!
flow-rule mcast_deny classify ip any 224.0.0.0/4
flow-rule mcast_deny match drop
!
policy-map iptv_filter flow-rule mcast_deny
!
service-policy downonly iptv_filter
!
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 deny igmp_query
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
```

8

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

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

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

이 장은 다음의 절들로 구성된다:

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

8.1. Understanding Spanning-Tree Features

이 절에서는 다음의 STP 기능에 대해 설명한다:

- STP Overview
- Bridge Protocol Data Units
- Election of the Root Switch
- Bridge ID, Switch Priority, and Extended System ID
- Spanning-Tree Timers
- Creating the Spanning-Tree Topology
- Spanning-Tree Interface States

8.1.1. STP Overview

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 활성화 시킨다.

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.

8.1.2. 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 인터페이스의 식별자
- hello, forward-delay, max-age 프로토콜 타이머의 값

스위치가 자신보다 우월한 정보(낮은 BridgeID, 낮은 path cost, 등등)를 가진 BPDU 를 수신했을 경우, 그 정보를 BPDU 를 수신한 포트에 저장한다. BPDU 를 수신한 포트가 root 포트라면, 스위치는 메시지를 갱신해서 자신의 designated LAN 으로 전달한다.

스위치가 현재 포트의 정보보다 열등한 정보를 포함한 BPDU 를 수신하면 그 BPDU 를 버린다. 스위치가 designated LAN 으로부터 열등한 메시지를 수신했다면, 포트에 저장된 정보로 갱신된 BPDU 를 LAN 으로 전송한다. 이런 방식으로 열등한 정보는 버려지고 우월한 정보가 네트워크에 전파된다.

다음은 BPDU 교환으로 인한 결과이다:

- 네트워크의 한 스위치가 root 스위치로 선택된다.
- Root 스위치를 제외한 각 스위치에서 root 포트가 선택된다. 이 포트는 스위치가 root 스위치로 패킷을 전송할 때 최적의 경로(가장 낮은 비용)를 제공한다.
- 각 스위치는 path cost를 기반으로 root 스위치까지의 최단 거리를 계산한다.
- 각각의 LAN을 위한 designated 스위치가 결정된다. designated 스위치는 LAN에서 root 스위치로 패킷을 전달할 때 가장 낮은 path cost를 제공한다. LAN과 연결된 designated 스위치의 포트를 designated 포트라 부른다.
- Spanning-tree 에 포함되는 인터페이스들이 결정된다. root 포트와 designated 포트는 forwarding 상태에 놓인다.
- Spanning-tree에 포함되지 않는 모든 인터페이스들은 blocked 된다.

8.1.3. Election of Root Switch

Layer 2 네트워크의 spanning tree 에 참여하는 모든 스위치는 BPDU 의 교환을 통해 다른 스위치들에 관한 정보를 모은다. 이러한 메시지의 교환은 다음의 행위를 야기한다:

- 각 spanning-tree instance에 대한 유일한 root 스위치 선출
- 모든 switched LAN 조각을 위한 designated 스위치의 선출
- 중복된 링크로 연결된 Layer 2 인터페이스의 차단에 의한 switched 네트워크의 루프 제거

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

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

Root 스위치는 switched 네트워크에서 spanning-tree 형상의 논리적인 중심이다. Switched 네트워크에서 root 스위치로 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.

8.1.4. Bridge ID, Switch Priority, and Extended System ID

IEEE 802.1D 표준에 따르면 각 스위치는 root 스위치를 선택하기 위해 사용되는 유일한 브리지 식별자(BridgeID)를 가진다. 각 VLAN 은 논리적으로 서로 다른 브리지로 간주되므로 스위치는 VLAN 별로 서로 다른 BridgeID 를 가질 수 있다. 스위치는 8 바이트의 BridgeID 를 가진다; 최상위 2 바이트는 스위치 priority 로 사용되고, 나머지 6 바이트는 스위치의 MAC 주소이다.

Premier 3400 Series 스위치는 802.1T spanning-tree extensions 를 지원한다. 표와 같이 스위치 priority 로 사용되던 2 바이트가 4 비트 priority 값과 VLAN ID 와 동일한 12 비트 extended system ID 값으로 재할당 되었다.

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

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

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

8.1.5. Spanning-Tree Timers

표는 spanning-tree 의 성능에 영향을 미치는 타이머들을 나타낸다.

표 8-2. Spanning-Tree Timers

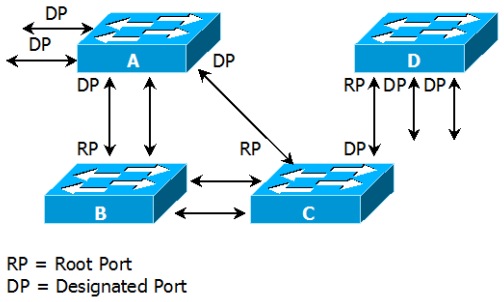
Variable	Description
Hello timer	스위치가 다른 스위치로 얼마나 자주 hello 메시지를 전송할 것인가를 결정한다.
Forward-delay timer	인터페이스가 forwarding 상태가 되기 전에 listening 과 learning 상태에서 각각 얼마나 머물 것인가를 결정한다.
Maximum-age timer	인터페이스로 수신한 프로토콜 정보를 얼마동안 저장할 것인가를 결정한다.

8.1.6. Creating the Spanning-Tree Topology

그림에서 모든 스위치들의 스위치 priority 가 default(32768)이고 스위치 A 가 가장 낮은 MAC

주소를 가진다고 가정하면 스위치 A 가 root 스위치가 된다. 하지만, forwarding 인터페이스의 개수 혹은 link-type 때문에 스위치 A 는 이상적인 root 스위치가 아니다. Root 스위치로 만들려는 스위치의 priority 를 증가시킴으로써(낮은 숫자 값을 사용), spanning-tree 의 형상을 재계산하여 이상적인 스위치를 root 로 만들 수 있다.

그림 8-1. Spanning-Tree Topology



default 인자를 기반으로 spanning-tree 형상을 계산하면, 시작 단말과 목적지 단말 사이의 경로는 이상적이지 않다. 예로, root 포트보다 높은 포트 번호를 가진 인터페이스에 연결된 고속의 링크는 스위치의 root 포트 변경을 야기할 수 있다. 목표는 가장 빠른 링크를 root 포트로 만드는 것이다.

예를 들어 스위치 B 의 한 포트가 기가비트 이더넷 링크이고, 스위치 B 의 다른 포트(10/100 링크)가 현재 root 포트라고 가정하자. 네트워크 트래픽이 기가비트 이더넷 링크를 통해 전달되는 것이 더 효과적이다. 기가비트 이더넷 인터페이스의 port priority 를 root 포트보다 더 높은 priority(낮은 숫자 값)를 가지도록 변경함으로써, 기가비트 이더넷 인터페이스를 새로운 root 포트로 만들 수 있다.

8.1.7. Spanning-Tree Interface States

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

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

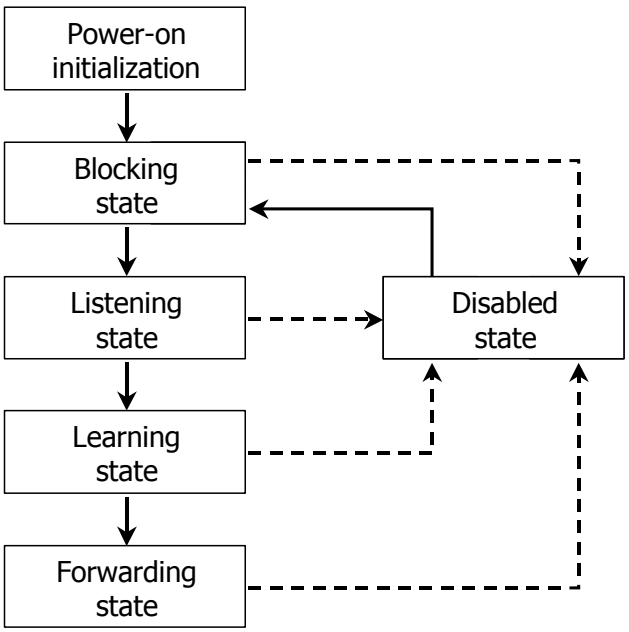
- Blocking – 인터페이스는 프레임을 forwarding하지 않는다.
- Listening – 인터페이스가 프레임을 forwarding해야 한다고 결정되었을 때, blocking state 다음의 천이 상태.
- Learning – 인터페이스가 프레임을 forwarding하기 위해 준비한다. MAC learning이 수행된다.
- Forwarding – 인터페이스가 프레임을 forward 한다.
- Disabled – 포트가 shutdown 상태이거나 포트에 링크가 없거나, 포트에 실행중인 spanning-tree instance가 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.

표 8-3. 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.

8.2. Understanding RSTP

RSTP는 point-to-point 연결에 대해 spanning tree의 빠른 복구를 제공하는 장점을 가진다. Spanning tree의 재구성은 1초(802.1D spanning tree의 default 설정에서 최대 50초가 소요되는 것과는 대조적으로) 이내에 완료된다. 이것은 음성과 영상과 같은 지연에 민감한 트래픽을 전송하는 네트워크에 유효하다.

이 절은 RSTP가 어떻게 동작하는 지를 설명한다:

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

8.2.1. 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.

8.2.2. 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 8-4. 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.

8.2.3. Rapid Convergence

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

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

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

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

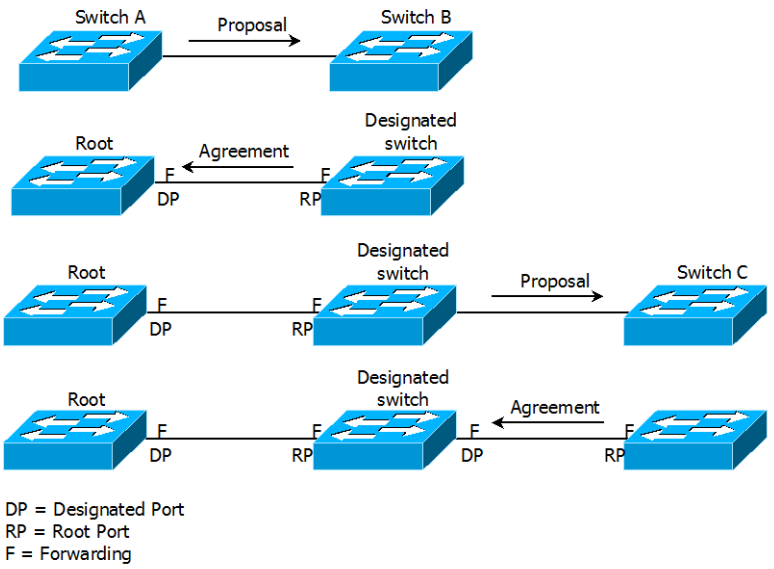
  스위치 B 의 agreement 메시지를 수신한 후에, 스위치 A 는 자신의 designated 포트를

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 8-2. Proposal and Agreement Handshaking for Rapid Convergence



8.2.4. 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 8-5. 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.

8.3. Configuring Spanning-Tree Features

이 절에서는 spanning-tree 를 설정하는 방법에 대해 설명한다.

8.3.1. Default STP Configuration

다음의 표는 STP 의 default 설정을 보여준다.

표 8-6. Default STP Configuration

Feature	Default Setting
Enable state	비활성 되어 있음.
Spanning-tree mode	STP
System priority	32768.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	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.

8.3.2. STP Configuration Guidelines

Premier 3400 Series 는 IEEE 802.1w RSTP 를 지원한다. 또한, 802.1w 는 802.1D STP 를 내부적으로 포함하므로 802.1D 와의 하위 호환성을 제공한다.

8.3.3. Enabling STP

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

시키도록 한다.

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

	Command	Purpose
Step1	**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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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#
```

8.3.4. Disable per VLAN STP

Premier 3400 Series 스위치는 VLAN 별로 spanning-tree 를 운영할 수 있다. 즉, VLAN trunk 포트의 각 VLAN 별로 STP state 를 설정하는 것이 가능하다. 만약 스위치에 32 개 이상의 VLAN 이 있다면, per VLAN STP 기능을 비활성 시키고, 전체 VLAN 을 제어하기 위한 하나의 spanning-tree instance 를 사용하도록 한다.

Notice Per VLAN STP 기능이 비활성된 상태에서 여러 VLAN 에 대해 STP 를 활성시킨다면, VLAN trunk port 의 STP 상태는 안정적이지 않을수 있다.

스위치의 per VLAN STP 기능을 비활성 시키려면, pivileged 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 활성시키려면, 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#
```

8.3.5. Configuring the Port Priority

루프가 발생하면 spanning tree 는 포트의 priority 를 사용하여 forwarding 상태의 인터페이스를 결정한다. 먼저 선택될 인터페이스에는 높은 priority 의 값(낮은 수)을, 나중에 선택될 인터페이스에는 낮은 priority 의 값(높은 수)를 할당할 수 있다. 모든 인터페이스가 같은 priority 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.

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

	Command	**Purpose**
Step1	**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-priority 를 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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# interface fa5
Switch(config-if-fa5)# spanning-tree vlan 1 port-priority 240
Switch(config-if-fa5)# 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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        240.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch#
Switch# configure terminal
Switch(config-if-fa5)# no spanning-tree vlan 1 port-priority
Switch(config-if-fa5)# 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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch#
```

8.3.6. Configuring the Path Cost

spanning-tree 의 path cost 의 default 값은 인터페이스의 속도로부터 결정된다. 루프가 발생하면 spanning tree 는 포트의 cost 를 사용하여 forwarding 상태의 인터페이스를 결정한다. 먼저 선택될 인터페이스에는 낮은 cost 값을, 나중에 선택될 인터페이스에는 높은 cost 값을 할당할 수 있다. 모든 인터페이스가 같은 cost 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진

인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.

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

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

	Command	Purpose
Step1	**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 (fa5)
              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              Altn BLK 19        128.6    P2p

Switch# configure terminal
Switch(config)# interface fa5
```

```
Switch(config-if-fa5)# spanning-tree vlan 1 cost 100
Switch(config-if-fa5)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    0
              Address     0007.70bc.cdde
              Cost        19
              Port        6 (fa6)
              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Altn BLK 100       128.5    P2p
fa6              Root FWD 19        128.6    P2p

Switch# configure terminal
Switch(config)# interface fa5
Switch(config-if-fa5)# no spanning-tree vlan 1 cost
Switch(config-if-fa5)# end
Switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    0
              Address     0007.70bc.cdde
              Cost        19
              Port        5 (fa5)
              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              Altn BLK 19        128.6    P2p

Switch#
```

8.3.7. Configuring the Switch Priority of a VLAN

스위치가 root 스위치가 될 가능성을 높이기 위해 스위치 priority 를 변경할 수 있다.

VLAN 에 대한 스위치 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	**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 (fa5)
              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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 (fa5)
              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              Altn BLK 19        128.6    P2p

Switch#
```

8.3.8. Configuring the Hello Time

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

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

	Command	Purpose
Step1	**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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch#
```

8.3.9. Configuring the Forwarding-Delay Time for a VLAN

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

	Command	Purpose
Step1	**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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch#
```

8.3.10. Configuring the Maximum-Aging Time for a VLAN

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

	Command	Purpose
Step1	**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-config**	(옵션) 설정을 configuration 파일에 저장한다.

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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch#
```

8.3.11. Configuring the Port as Edge Port

Premier 3400 Series 에서 STP 를 활성화시킬 경우, 단일 호스트와 연결된 포트에 대해서 edge port 로 설정한다. 만약 포트를 edge 포트로 설정하지 않으면, 그 포트는 forwarding 상태로 천이하는데 2 x Forward Time 이 소요된다.

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

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

	Command	Purpose
Step1	**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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
fa7              down DIS 0         128.7    P2p Edge

Switch#
```

8.3.12. Configuring the RSTP Mode

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.

STP 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 rstp**	특정 VLAN 의 RSTP instance 의 프로토콜 동작모드를 RSTP 모드로 설정한다. *vlan-id* 의 범위는 1~4094 이다. default 는 STP 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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch#
```

8.3.13. Specifying the Link Type to Ensure Rapid Transitions

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

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

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

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

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Stpe3	**spanning-tree link-type**	포트의 링크 종류를 point-to-point 로 설정한다.

	point-to-point	
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.

8.3.14. Restarting the Protocol Migration Process

RSTP 를 지원하는 스위치는 802.1D STP 를 구동하는 스위치와의 연동이 가능하도록 protocol migration 메커니즘을 지원한다. 스위치가 Configuration BPDU(protocol version 이 0 으로 설정된 BPDU)를 수신한다면, 스위치는 그 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 fa5
Switch(config-if-fa5)# spanning-tree vlan 1 mcheck
Switch(config-if-fa5)#
```

8.4. 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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              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
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p

Switch# show spanning-tree interface fa5
 Port 5 (fa5) 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#
```

8.5. Self-loop Detection

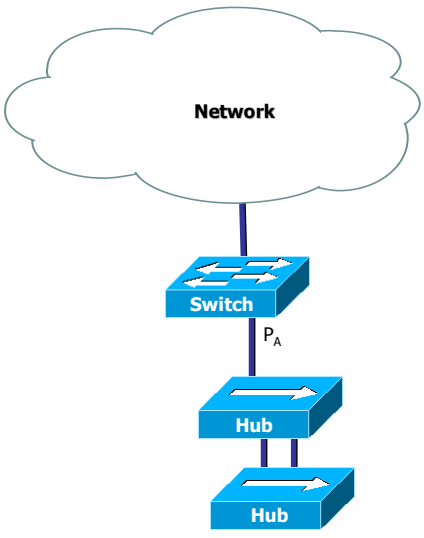
자신이 전송한 패킷이 되돌아 오는 현상을 감지하는 self-loop 감지 기능을 설정하는 방법을 설명한다.

8.5.1. Understanding Self-loop Detection

사용자의 스위치에 이중 경로가 존재하지 않아도 네트워크 구성이나 스위치에 연결된 케이블의 상태 등에 따라 loop 가 발생할 수 있다.

스위치가 자신의 한 포트로 전송한 패킷이 다시 그 포트로 되돌아왔을 때, 이런 현상을 self-loop 이라 한다. 다음의 그림은 self-loop 이 발생한 환경에 대한 예제이다.

그림 8-3. self-loop 발생 환경



그림에서 두 hub 사이에 이중 경로에 의한 loop 이 존재한다. STP 가 활성화 되지 않은 상태이기 때문에 hub 사이의 loop 은 제거되지 않으며 network 의 불안정을 초래하게 된다. 이 경우 스위치가 포트 PA 를 통해 전송한 패킷은 다시 PA 로 수신된다. 스위치에 self-loop 감지 기능이 활성화되어 있다면, 포트 PA 에 self-loop 이 있다는 것을 감지하고 포트 PA 를 서비스 불가능 상태(Administrative disable)로 만들어 스위치와 포트 PA 와 연결되지 않은 다른 네트워크를 보호하게 된다. 포트 PA 에 연결된 장비와 네트워크에 여전히 loop 은 존재한다(네트워크에서 완전한 loop 의

제거를 원한다면 STP 를 사용하라).

8.5.2. Configuring Self-loop Detection

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

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

8.5.2.1. Enabling Self-loop Detection

Self-loop 감지 기능은 스위치의 각 포트 별로 기능의 활성화가 가능하다. 또는 Port 의 range 선택 상태에서도 활성화가 가능하다. default 는 self-loop 감지 기능이 비활성화 되어 있다.

Self-loop 감지 기능이 활성화 된 후 이 기능에 의하여 port 가 shutdown 상태가 되면 설정된 limit time 이 지난 후 자동으로 no shutdown 상태로 바뀐다. Limit time 의 default 값은 5 분이고, 분 단위로 0 부터 1440 까지 지정할 수 있으며 0 으로 설정하면 수동으로 no shutdown 하기 전까지 port 가 shutdown 상태로 있는다.

Self-loop 감지 기능을 활성화 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	**self-loop-detection**	Self-loop 감지 기능을 활성화 한다. Self loop 에 의해 shutdown 되면 5 minutes 후에 자동으로 no shutdown 한다.
Step3b	**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.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5a	**show running-config**	설정 내용을 확인한다.
Step5b	**show self-loop-detection**	Self-loop 설정 내용을 확인한다.
Step5c	**show loop-detect**	Self-loop 설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

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

```
Switch(config-if-fa1)# end
Switch# show self-loop-detection
--------------------------------------------------------------------------------
 ifname sld  link  shutdown set_time remain_time count      last-occur
--------------------------------------------------------------------------------
 fa1    set   up       .       5 min       .         0           .
 fa2     .   down      .       .           .         0           .
 fa3     .   down      .       .           .         0           .
 fa4     .   down      .       .           .         0           .
 fa5     .    up       .       .           .         0           .
……
 gi1     .   down      .       .           .         0           .
 gi2     .   down      .       .           .         0           .
Switch#
```

8.5.2.2. Changing The Service Status of Port

Self-loop 감지 기능에 의해 서비스 불가능 상태가 된 포트가 limit time 이 0 으로 설정된 상태라면 수동으로만 서비스 가능 상태로 만들 수 있다.

포트를 서비스 가능 상태로 만들려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	*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.

8.5.2.3. Disabling Self-loop Detection

Self-loop 감지 기능은 스위치의 각 포트 별로 또는 Port 의 range 선택 상태에서 기능의 비활성화가 가능하다.

만약 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	**end**	privileged EXEC 모드로 변경한다.
Step5a	**show running-config**	설정 내용을 확인한다.

Step5b	**show self-loop-detection**	Self-loop 설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# no self-loop-detection
Switch(config-if-fa1)# end
Switch# show self-loop-detection
-------------------------------------------------------------------------------
 ifname sld  link  shutdown set_time remain_time count      last-occur
-------------------------------------------------------------------------------
 fa1     .    up       .       .          .        0          .
 fa2     .   down      .       .          .        0          .
 fa3     .   down      .       .          .        0          .
 fa4     .   down      .       .          .        0          .
 fa5     .    up       .       .          .        0          .
……
 gi1     .   down      .       .          .        0          .
 gi2     .   down      .       .          .        0          .
Switch#
```

8.5.3. Displaying Self-loop Status

포트의 self-loop 감지 기능 설정 상태를 조회하려면, privileged EXEC 명령 **show running-config** 나 **show self-loop-detection** 을 사용하라.

show self-loop-detection 에서

- ifname : Interface name (Port name)
- 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 fa5 에 SLD 가 default time 인 5 분으로 설정되어 있는 것을 보여준다. Port fa5 는 May

29 04:48:39 2006 에 SLD 에 의해 self loop 이 감지되어 shutdown 된 적이 한번 있었다는 것을 알 수 있다.

```
Switch# show running-config
!
interface fa5
 self-loop-detection
!
interface vlan1
 ip address 100.1.1.1/24
!
Switch#
Switch# show self-loop-detection
-------------------------------------------------------------------------------
 ifname sld  link  shutdown set_time remain_time count      last-occur
-------------------------------------------------------------------------------
 fa1     .   down      .       .           .         0           .
 fa2     .    up       .       .           .         0           .
 fa3     .   down      .       .           .         0           .
 fa4     .   down      .       .           .         0           .
 fa5    set   up      block      5 min      .         1  May 29 04:48:39 2007
 fa6     .   down      .       .           .         0           .
 fa7     .   down      .       .           .         0           .
 fa8     .   down      .       .           .         0           .
Switch#
```

9 Stacking

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

이 장은 다음의 절들로 구성된다:

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

9.1. Stacking Overview

Premier 3400 Series 스위치는 하나의 IP 주소로 여러 대의 스위치를 관리할 수 있다. 이 때, 관리 IP 주소를 가진 스위치를 *Master 스위치*, Master 스위치를 통해 관리되는 스위치 그룹내의 나머지 스위치들을 *Slave 스위치*라 칭한다.

Premier 3400 Series 스위치는 Master 스위치와 Slave 스위치가 통신할 수 있는 공통의 VLAN 으로 연결만 되어 있으면, 네트워크 형상(Network topology)과 무관하게 stacking 될 수 있다. 이 때, Master 스위치와 Slave 스위치를 연결하는 VLAN 을 *Stack VLAN* 이라 부른다.

9.2. Configuring Stacking Feature

이 절에서는 Stacking 을 설정하는 방법을 설명한다:

- Configuring the Stack VLAN
- Configuring the Stack Member
- Enabling the Stack
- Connecting to Slave Switch

9.2.1. Configuring the Stack VLAN

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

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

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

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**stack vlan** *vlan-id*	Stack VLAN 을 설정한다. *vlan-id* 의 범위는 1~4094 이다. default 는 VLAN 1 이다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

```
Switch# configure terminal

Switch(config)# stack vlan 200

Switch(config)# end

Switch#

Switch# show running-config

!

stack vlan 200

!
```

9.2.2. Configuring the Stack Member

Master 스위치에서 관리할 Slave 스위치들을 Master 스위치에 등록해주어야 한다.

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

Slave 스위치를 등록하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**stack member** *node-id mac-address*	Slave 스위치를 등록한다. ● *node-id* 의 범위는 2~8 이다. ● *mac-address* 는 AABB.CCDD.EEFF 형식이다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

```
Switch# configure terminal

Switch(config)# stack member 3 0007.70BC.CDDE

Switch(config)# end

Switch# show running-config

!

stack vlan 200

stack member 3 0007.70bc.cdde

!
```

9.2.3. Enabling the Stack

스위치는 Master 스위치 혹은 Slave 스위치로 Stack 기능이 활성화 된다.

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

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**stack role {master|slave}**	스위치의 Stack 기능을 활성화한다. ● master – Master 스위치로 동작한다. ● slave – Slave 스위치로 동작한다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

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

master switch 의 경우 다음과 같다.

```
Switch# configure terminal

Switch(config)# stack role master

Switch(config)# end

Switch# show running-config

!

stack vlan 200

stack member 3 0007.70bc.cdde

stack role master

!

Switch# show stack

Node   Mac address      Status     Platform     VLAN

   1   0007.7012.2932   active     P4624FG       200

   3   0007.70bc.cdde   active     P4624FG       200
```

```
Switch#
```

slave switch 의 경우 다음과 같다.

```
Switch _1# configure terminal

Switch _1(config)# stack role slave

Switch _1(config)# end

Switch _1# show stack

Stacking VLAN : 200

Node ID       : 3

Master switch : P3624FG(0007.7012.2932) on VLAN0200

Switch _1#
```

9.2.4. Connecting to Slave Switch

Master 스위치와 Slave 스위치가 성공적으로 stacking 되었다면, Master 스위치를 통해 Slave 스위치에 접속할 수 있다. Premier 3400 Series 스위치는 Slave 스위치의 shell 을 사용할 수 있는 방법을 제공한다.

Notice 이 명령은 Master 스위치에서만 동작한다

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

	Command	Purpose
Step1	**rcommand** *node-id*	Master 스위치에서 Slave 스위치에 접속한다. *node-id* 의 범위는 2~8 이다.

```
Switch# show stack

Node   Mac address      Status     Platform     VLAN

   1   0007.7012.2932   active     P3624FG       200

   3   0007.70bc.cdde   active     P3624FG       200

Switch# rcommand 3


Entering character mode

Escape character is '^]'.



Ubiquoss L2 Switch
```

```
Hello.


Switch _1>
```

9.3. Displaying the Stacking Status

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

Command	**Purpose**
show stack	stack 상태 정보를 출력한다

다음은 Master 스위치에서의 show stack 명령에 대한 출력 결과이다:

```
Switch# show stack

Node  Mac address     Status    Platform    VLAN
1     0007.7000.100a  active    P3624FG     10
2     0007.7000.100c  active    P3624FG     10
```

다음은 Slave 스위치에서의 show stack 명령에 대한 출력 결과이다:

```
Switch# show stack

Stacking VLAN : 10
Node ID       : 2
Master switch : P3624FG(0007.7000.100a) on VLAN 10
```

10 통계 모니터링 및 Qos

본 장은 현재 운영중인 Premier 3400 Series 스위치의 상태를 파악하고, 로그의 정보를 화면에 표시하고, RMON(Remote Monitoring)을 통한 운영 관리 기능에 대하여 설명한다.

또한 Premier 3400 Series 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 한다. 만일 주기적으로 통계 데이터를 관리한다면, 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있다.

10.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. Premier 3400 Series 스위치는 `show` 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공한다.

표 10-1. 상태 모니터링 명령어

명령어	설명
`show log`	■ 시스템이 현재 관리하고 있는 로그를 보여 준다. ■ 최대 500 개까지의 로그를 저장할 수 있다.
`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.

10.2. 포트 통계

Premier 3400 Series 스위치는 포트의 통계 정보를 제공한다. 포트의 통계 정보는 시스템의 현재 운용

중인 모듈의 각 포트의 현재 카운터 값을 보여준다.

포트 통계를 보기 위해서는 다음의 명령을 사용한다.

`show interface [interface name]`

Premier 3400 Series 스위치는 운용자에게 다음의 포트 통계 정보를 제공한다.

- **Link Status** – 링크의 현재 상태
- **Received Packet Count (Rx Pkt Count)** – The total number of good packets that have been received by the port.
- **Received Byte Count (Rx Byte Count)** – The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- **Transmit Packet Count (Tx Pkt Count)** – The number of packets that have been successfully transmitted by the port.
- **Transmit Byte Count (Tx Byte Count)** – The total number of data bytes successfully transmitted by the port.
- **Received Broadcast (Rx Bcast)** – The total number of frames received by the port that are addressed to a broadcast address.
- **Received Multicast (Rx Mcast)** – The total number of frames received by the port that are addressed to a multicast address.
- **Transmit Collisions (Tx Coll)** – The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Received Bad CRC Frames (RX CRC)** – The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Oversize)** – The total number of good frames received by the ports that were of greater than the supported maximum length of 1,522 bytes.
- **Receive Dropped Frames (Rx Drop)** – The total number of dropped frames due to lack of system resources.

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

```
Switch# show interface
fa1 is link down.
 type 100Base-TX
 auto-negotiation
 speed set auto
 duplex set full
 cpu-mac-filter disable

 Last clearing of counters 02:47:05
 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

fa2 is link down.
 type 100Base-TX
 auto-negotiation
 speed set auto
 duplex set full
 cpu-mac-filter disable

 Last clearing of counters 02:47:05
 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
--More--
```

표 10-2. 포트 통계조회 조회 명령

명령어	설명	모드
show port counter	시스템의 모든 인터페이스의 In/Out packet 의 누적치를 보여준다.	privileged
show port counter detail	시스템의 모든 인터페이스의 In/Out packet 과 octet 의 누적치를 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 allports	모든 인터페이스의 5 초, 1 분, 5 분 단위로 Rx/Tx 의 bit/s, bytes/s, pkts/s 를 보여준다.	privileged

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

```
Switch# show port counter

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

```
 fa7          0       0              0              0              0              0
 fa8          0       0              0              0              0              0
 fa9          0       0              0              0              0              0
 fa10         0       0              0              0              0              0
 fa11         0       0              0              0              0              0
 fa12         0       0              0              0              0              0
 fa13         0       0              0              0              0              0
 fa14         0       0              0              0              0              0
 fa15         0       0              0              0              0              0
 fa16         0       0              0              0              0              0
 fa17         0       0              0              0              0              0
 fa18         0       0              0              0              0              0
 fa19         0       0              0              0              0              0
 fa20         0       0              0              0              0              0
 fa21         0       0              0              0              0              0
 fa22         0       0              0              0              0              0
 fa23         0       0              0              0              0              0
 fa24         0       0              0              0              0              0
--------------------------------------------------------------------------------
Switch#
Switch#
Switch# show port statistics fa24

Last clearing of counters :  0 days and 00:06:24 before

-----------------------------------------------------------------
                                TX |                        RX
                  bits/s       pkts/s |     bits/s       pkts/s
-----------------------------------------------------------------
     5sec :            0            0            0            0
     1min :            0            0            0            0
     5min :            0            0            0            0
-----------------------------------------------------------------
Switch#
```

다음 명령은 통계치에 대한 누적치를 초기화시키는 명령어이다.

표 10-3. 포트 통계 초기화 명령

명령어	설명	모드
clear counters	시스템의 모든 인터페이스의 통계누적치를 초기화한다.	privileged
clear counters *IFNAME*	특정 인터페이스의 통계누적치를 초기화한다.	privileged
clear counters snmp	시스템의 모든 인터페이스의 snmp 를 위한 통계누적치를 초기화한다.	privileged

10.3. CPU 트래픽 통계

Premier 3400 series 스위치는 cpu 로 올라오는 수많은 packet 을 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 초동안의 CPU packet count, 최근 1 분 동안의 CPU packet count, 최근 5 분 동안의 CPU packet count 를 보여 준다.

10.3.1. 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.

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

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.

표 10-4. packet type 추가

	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#
```

Notice Ethertype 은 “unsigned short”, IP protocol 은 “unsigned char”, TCP/UDP port 는 “unsigned short” 값으로 입력해야 한다.

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.

표 10-5. packet type 삭제

	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.

10.3.2. 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.

표 10-6. display cpu packet counter

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-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-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.

10.4. Logging

Premier 3400 series 스위치 로그는 모든 환경 설정 정보와 경보 발생 정보를 보여 준다. 시스템 메시지 로깅 소프트웨어는 스위치의 메모리에 로그 메시지를 저장하며, 다른 디바이스로 메시지를 보낼 수 있다. 시스템 메시지 로깅 기능은 다음을 지원한다.

- ✓ 사용자에게 수집할 로깅 타입을 선택할 수 있도록 한다.
- ✓ 사용자에게 수집한 로깅을 보낼 디바이스를 선택할 수 있도록 한다.

Premier 3400 series 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI 를 사용하여 로깅되는 시스템 메시지를 제어할 수 있다. 최대 500 개의 로그 메시지를 시스템 버퍼에 저장한다. 시스템 운영자는 시스템 메시지를 Telnet 이나 콘솔을 통해서, 또는 Syslog server 의 로그를 봄으로써 원격으로 모니터 할 수 있다.

Premier 3400 series 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

표 10-7. Premier 3400 series 스위치의 로그 레벨

Severity 레벨	설명
Emergencies (0)	시스템 사용 불가.
Alerts (1)	즉각적인 조치가 필요한 상태
Critical (2)	Critical 상태.
Errors (3)	에러 메시지.

Warnings (4)	경고 메시지.
Notifications (5)	정상적인 상태지만 중요한 정보.
Informational (6)	사용자에게 제공하는 정보 메시지.
Debugging (7)	디버깅 메시지.

10.4.1. 시스템 로그 메시지 내용

Premier 3400 series 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
  - <표 1>에서 정의한 Premier 3400 스위치의 로그 메시지의 레벨
  - 0~7 까지의 숫자
- ✓ Log description
  - 발생한 이벤트에 대한 상세한 정보를 포함하는 텍스트 문자열

다음은 시스템 부팅 시의 로그 메시지 이다.

```
May  6 11:53:48  [5] %REMOTE-CONNECT: login from console as lns
May  6 11:54:01  [5] IFM-NOTICE: Rate limit ra creation
May  7 02:10:24  [5] %REMOTE-CONNECT: login from console as lns
May  7 02:10:40  [5] IFM-NOTICE: Flow xx classified
May  7 02:10:48  [5] IFM-NOTICE: Flow xx match rate 10
May  7 05:17:56  [5] %REMOTE-CONNECT: login from console as lns
May  7 05:23:10  [5] IFM-NOTICE: Service pa add interface fa1
```

10.4.2. 디폴트 Logging 설정 값.

표 10-8. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	enabled
Telnet 세션으로의 로깅 출력	disabled.
로깅 버퍼 사이즈	250kb
Time-Stamp 출력	enabled
Logging Server	disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings(4)
콘솔의 Severity	Debuggings(7)
Telnet 의 Severity	info(6)
Flash 로의 로깅 저장	disable
Flash 버퍼 사이즈	25KB

표 10-9. 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 저장할지의 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 configuration 확인.

10.4.3. 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)#
```

10.5. RMON(Remote MONitoring)

시스템 운영자는 Premier 3400 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다.

다음 절에서는 RMON 개념 및 Premier 3400 Series 스위치가 지원하는 RMON 서비스 기능에 대하여 자세히 설명한다.

10.5.1. 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

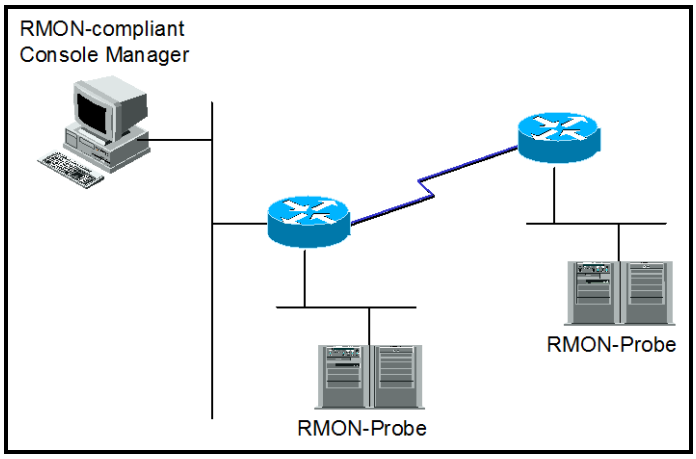


그림 10-1. RMON Manager 와 RMON Probe

기존의 SNMP MIBs 가 SNMP agent 가 탑재된 장비 자체를 관리 대상으로 보고 있는데 반하여 RMON MIBs 는 관리 대상을 장비에 연결된 LAN 세그먼트로 한다. 즉 LAN 세그먼트의 전체 발생 트래픽, 세그먼트에 연결된 각 호스트의 트래픽, 호스트들 사이의 트래픽 발생 현황을 알려준다.

RMON Agent 는 전체 통계 데이터, 이력 데이터, 호스트 관련 데이터, 호스트 매트릭스와 사전에 문제 예측 및 제거를 위해서 특정 패킷을 필터링하는 기능과 임계치를 설정, 이에 도달하면 자동으로 알려주는 경보 기능 및 사건 발생 기능을 보유하고 있어야 한다.

Premier 3400 Series 스위치에서는 **<오류! 참조 원본을 찾을 수 없습니다.>**에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON 은 디폴트로 모든 설정이 disabled 이다.

표 10-10. 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 관

	리
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 지를 전송. 트랩 발생 및 기록보관은 선택적임.

10.5.2. 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 10-11. 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 인테페이스를 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 해	Config

	당 Event 가 발생. ■ Owner *string*: Alarm 의 owner 를 명시.	
`rmon event index [log] [trap community string] [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 alarm`	■ RMON alarm table 을 출력.	Privileged
`show rmon event`	■ 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         : fa1/1
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
Switch#
```

표 10-12. 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. ■ *IFNAME:* 특정 인터페이스를 지정	Privileged

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
--------------------------------------


====== gi2/1 ======
Control-index     : 1
ifindex           : 9
interval          : 5
```

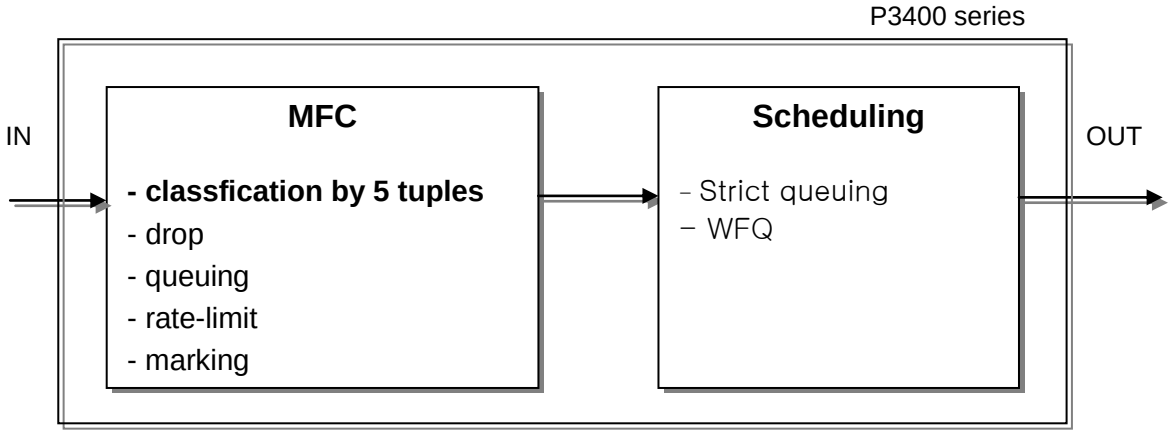
```
buckets            : 50
owner              : park

--- gi2/1 : bucket 1 ---
DropEvents         : 0
Octets             : 0
       (생략)
P808FG_85# show rmon statistics
--------------------------------------
         SHOW STATISTICS
--------------------------------------

The Index of stats    : 1
Interface             : fa1/1
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 fa2/1
--------------------------------------------------------------------------------
         RMON STATISTICS
--------------------------------------------------------------------------------

The Index of stats    : 3 (fa2/1)
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
--------------------------------------------------------------------------------
```

10.6. Qos 및 Packet Filtering



본 Premier 3400 Series 스위치에서는 Qos 와 Packet filtering 을 위해 다음과 같은 기능을 수행을 한다.

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

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

- **Scheduling**

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

  - Strict Queuing Method

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

  - WRR(Weighted Round Robin Method)

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

  - WFQ(Weighted Fair Queuing Method)

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

10.6.1. MFC(Multi-Field Classifier)

10.6.1.1. Flow-Rule 설정/해제

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

표 10-13. Flow-rule Classification 명령

명령어	설명	모드
flow-rule NAME classify { <0-255> | icmp | igmp | ip | ospf | pim | tcp | udp } { *SRCIP/M* **| any } {** *DSTIP/M* **| any }**	flow-rule 이 적용된 인터페이스의 특정 프로토콜에 대한 모든 혹은 지정된 src/dest ip 에 대해 적용(L3 기본 classify)	Config
flow-rule NAME classify <0-255> mask MASK *SRCIP/M DSTIP/M*	flow-rule 이 적용된 인터페이스의 특정 range 의 프로토콜에 대한 지정된 src/dest ip 에 대해 적용(L3 기본 classify)	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP/M* | **any** } { *DSTIP/M* | **any** } { *<0-65535>* | *SRCPORT* } { *<0-65535>* | *DSTPORT*}	flow-rule 이 적용된 인터페이스의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 에 대해 적용(L3 기본 classify)	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP/M* | **any** } { *DSTIP/M* | **any** } **mask** *SRCPORT SPORTMASK DSTPORT DSTPORTMASK*	flow-rule 이 적용된 인터페이스의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 mask range 의 src/dest port 에 대하여 적용. 이 경우 Port 도 16 진수로 입력해야 함(L3 기본 classify) * Mask-calculator 참조	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP/M* | **any** } { *DSTIP/M* | **any** } { *l4port-range-checker <1-16>* | *SRCPORT* } { *l4port-range-checker <1-16>* | *DSTPORT*}	flow-rule 이 적용된 인터페이스의 udp/tcp 프로토콜에 대한 모든 혹은 지정된 src/dest ip 와 모든 혹은 지정된 src/dest port 에 대해 적용(L3 기본 classify). 이 경우 port 의 classification 을 l4port-range-checker 을 사용.	Config
flow-rule *NAME* **classify** { *H.H.H* | **any** } { *H.H.H* | **any** }	flow-rule 이 적용된 인터페이스의 모든 혹은 지정된 src/dest Mac address 에 대하여 적용(L2 기본 classify)	Config
flow-rule *NAME* **classify** *H.H.H* **mask** *H.H.H H.H.H* **mask** *H.H.H*	flow-rule 이 적용된 인터페이스의 모든 혹은 지정된 mask range 의 src/dest Mac address 에 대하여 적용(L2 기본 classify)	Config

flow-rule *NAME* **classify tcp-control** *{ack|fin|psh|rst|syn|urg|VALUE MASK}*	Tcp control flag 를 이용한 classification 설정	Config
(no) flow-rule *NAME* **classify dscp** *VALUE*	flow-rule 이 적용된 인터페이스의 해당 dscp 값의 패킷에 대하여 적용/해제	Config
(no) flow-rule *NAME* **classify tos** *VALUE*	flow-rule 이 적용된 인터페이스의 해당 tos 값의 패킷에 대하여 적용/해제	Config
(no) flow-rule *NAME* **classify cos** *VALUE*	flow-rule 이 적용된 인터페이스의 해당 cos 값의 패킷에 대하여 적용	Config
(no) flow-rule *NAME* **classify vlan <1-4094>**	Vlan 을 이용한 classification 설정	Config
(no) flow-rule *NAME* **classify ethertype** *VALUE*	flow-rule 이 적용된 인터페이스의 특정 ethertype 패킷에 대하여 적용	Config
(no) flow-rule *NAME* **classify ethertype** *VALUE* **mask** *MASK*	flow-rule 이 적용된 인터페이스의 특정 ethertype mask range 패킷에 대하여 적용	Config
(no) flow-rule *NAME* **classify tag-type (tagged | untagged)**	flow-rule 이 적용된 인터페이스의 패킷이 untagged packet 혹은 tagged packet 에 대하여 적용	Config

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

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

표 10-14. Flow-rule 정책 적용 명령

명령어	설명	모드
flow-rule *NAME* **match drop**	규칙과 일치하는 패킷을 불허한다.	Config
flow-rule *NAME* **match queuing <0-7>**	규칙과 일치하는 패킷을 지정된 우선순위의 Queue 에 할당한다.	Config
flow-rule *NAME* **match marking cos <0-7>**	규칙과 일치하는 패킷의 해당값을 할당된 Cos 값으로 패킷에 marking 한다.	Config
flow-rule *NAME* **match marking dscp <0-63>**	규칙과 일치하는 패킷의 해당값을 할당된 dscp 값으로 패킷에 marking 한다.	Config
flow-rule *NAME* **match marking tos <0-7>**	규칙과 일치하는 패킷의 해당값을 할당된 tos 값으로 패킷에 marking 한다.	Config
flow-rule *NAME* **match cos-to-tos**	규칙과 일치하는 패킷의 tos 값을 패킷의 cos 값을 참조하여 패킷에 marking 한다.	Config
flow-rule *NAME* **match tos-to-cos**	규칙과 일치하는 패킷의 cos 값을 패킷의 tos 값을 참조하여 패킷에 marking 한다.	Config
flow-rule *NAME* **match mirror**	규칙과 일치하는 패킷을 지정된 mirror 포트에 복사한다.	Config

flow-rule *NAME* **match redirect {all|unicast|broadcast|BPDU|DLF|known-multicast|unknown-multicast}** *INTERFACE* **{ tag | untag }**	규칙과 일치하는 패킷을 지정된 INTERFACE 로 redirect 한다.	Config
flow-rule *NAME* **match trap-cpu**	규칙과 일치하는 패킷을 CPU 로 트랩시킨다.	Config
flow-rule *NAME* **match control-cpu-trap**	규칙과 일치하는 패킷을 CPU 에 high priority 로 트랩시키며, 동시에 drop 시킨다.	Config
flow-rule *NAME* **match drop-precedence**	규칙과 일치하는 패킷에 drop-precedence 를 부여한다.	Config
flow-rule *NAME* **match metering**	규칙과 일치하는 패킷을 카운팅한다.	Config
flow-rule *NAME* **match rate-limit** <64-1048576>	규칙과 일치하는 패킷에 rate-limit 를 적용한다.	Config
flow-rule *NAME* **match tos-to-cos-and-queue**	규칙과 일치하는 패킷에 tos 값을 참조하여 cos 와 queue 값에 markinig 한다.	Config
flow-rule *NAME* **match cos-and-queue** *<1-7>*	규칙과 일치하는 패킷에 cos 와 queue 값에 지정된 값을 marking 한다.	Config
flow-rule *NAME* **match rate-limit aggregator** *WORD*	규칙과 일치하는 패킷에 지정한 rate-limit aggregator 를 적용한다.	Config
flow-rule *NAME* **match cpu-queuing** *<1-6>*	규칙과 일치하는 패킷에 cpu-queuing 값을 지정한 값을 할당한다.	Config
no flow-rule *NAME* **match drop**	규칙과 일치하는 패킷을 불허를 취소한다.	Config
no flow-rule *NAME* **match queuing**	규칙과 일치하는 패킷의 queuing 을 취소한다.	Config
no flow-rule *NAME* **match marking cos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match marking dscp**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match marking tos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match cos-to-tos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match tos-to-cos**	규칙과 일치하는 패킷의 marking 을 취소한다.	Config
no flow-rule *NAME* **match mirror**	규칙과 일치하는 패킷의 mirror 를 취소한다.	Config
no flow-rule *NAME* **match redirect**	규칙과 일치하는 패킷의 redirect 를 취소한다.	Config
no flow-rule *NAME* **match trap-cpu**	규칙과 일치하는 패킷의 trap-cpu 를 취소한다.	Config
no flow-rule *NAME* **match control-cpu-trap**	규칙과 일치하는 패킷의 trap-cpu 를 취소한다.	Config
no flow-rule *NAME* **match drop-precedence**	규칙과 일치하는 패킷의 drop-precedence 를 취소한다.	Config
no flow-rule *NAME* **match metering**	규칙과 일치하는 패킷의 metering 를 취소한다.	Config
no flow-rule *NAME* **match rate-limit**	규칙과 일치하는 패킷의 rate-limit 를 취소한다.	Config
no flow-rule *NAME* **match tos-to-cos-and-queue**	규칙과 일치하는 패킷의 tos-to-cos-and-queue 를 취소한다.	Config
no flow-rule *NAME* **match cos-and-queue**	규칙과 일치하는 패킷의 cos-and-queue 를 취소한다.	Config
no flow-rule *NAME* **match rate-limit aggregator**	규칙과 일치하는 패킷의 rate-limit aggregator 를 취소한다.	Config
no flow-rule *NAME* **match cpu-queuing**	규치과 일치하는 패킷의 cpu-queuing 을 취소한다.	Config

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

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

10.6.1.2. mask-calculator

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

표 10-15. mask-calculator 명령

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

이해를 돕기위해 다음의 조건을 만족시키기 위한 한가지 예를 나타내었다.

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

```
Switch# mask-calculator 4000 4100

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

Required number of mask = 4

Switch#
```

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

10.6.1.3. port range checker

port range checker 는 L4port range 를 classification 하는 경우 쉽게 할 수 있도록 지원하는 기능이다.

L4port range 를 classification 하기 전에 먼저 port range 를 다음 명령어를 통해 정의 한다.

표 10-16. port range checker 명령어

명령어	설명	모드
flow-rule l4port-range-checker *<1-16>* (*src*|*dst*) *<0-65535> <0-65535>*	L4port-range-checker 의 identify 는 1-16 이고 port 의 direction, range 를 설정한다.	Privileged

l4port-range-checker 는 최대 16 개까지 정의 할 수 있다. 그리고 각 l4pot-range-checker 는 source port 또는 destination port 둘 중에 하나만 설정 할 수 있다.

이해를 돕기위해 다음의 조건을 만족시키기 위한 한가지 예를 나타내었다.

예 1) fa1 포트에 다음과 같이 적용한다.
tcp src 6000~10000 번 포트 drop

```
Switch#configure terminal
Switch(config)# flow-rule l4port-range-checker 1 src 6000 10000
Switch(config)# flow-rule f1 classify tcp any any l4port-range-checker 1 any
Switch(config)# flow-rule f1 match drop
Switch(config)#
Switch(config)# policy-map p1 flow-rule f1
Switch(config)#
Switch(config)# service-policy fa1 ingress p1
Switch(config)#
```

10.6.1.4. policy-map 생성/추가

인터페이스에 Flow-rule 을 적용하기위해 Policy-map 을 만들어 적용하며, Policy-map 에는 다수의 Flow-rule 이 포함될 수 있어, 한 인터페이스에 다수의 정책이 적용될 수 있으며 Policy-map 에 추가되는 순서에 의해 Flow-rule 이 적용되므로 그 순서가 대단히 중요하다.
적용된 순서는 **show flow-rule** 을 통해 확인할 수 있다.

표 10-17. 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 전체를 삭제하거나, 적용된 하나의 Flow-rule 을 삭제하기 위해서는 다음의 명령어들이 사용된다.

표 10-18. 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 10-19. policy-map 적용/해제 명령

명령어	설명	모드
service-policy *IFNAME* **ingress** *PNAME*	특정 포트 인터페이스의 해당 direction 으로 PNAME 의 policy-map 을 적용한다.	Config
no service-policy *IFNAME*	해당 인터페이스 적용된 policy-map 을 해제한다.	Config

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

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

다음의 명령을 사용하여 flow-rule 관련 설정을 조회할수 있다.

표 10-20. Flow-rule 조회 명령

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

이해를 돕기위해 다음의 조건을 만족시키기 위한 두가지 예를 나타내었다.

예 1) fa1 포트에 다음과 같이 적용한다.

tcp 6000 번 포트 drop

Src ip 20.1.1.0/24 queuing 2

Tcp 23 포트에 queuing 7 (highest) 및 marking

```
Switch#configure terminal
Switch(config)# flow-rule f1 classify tcp any any 6000 any
Switch(config)# flow-rule f1 match drop
Switch(config)# flow-rule f2 classify ip 20.1.1.0/24 any
Switch(config)# flow-rule f2 match queuing 2
Switch(config)# flow-rule f3 classify tcp any any 23 any
Switch(config)# flow-rule f3 match cos-and-queue 7
Switch(config)#
Switch(config)# policy-map p1 flow-rule f1
Switch(config)# policy-map p1 flow-rule f2
Switch(config)# policy-map p1 flow-rule f3
Switch(config)#
Switch(config)# service-policy fa1 ingress p1
Switch(config)#
```

예 2) fa2 포트에 다음과 같이 적용한다.

tcp 4010 포트에 rate limit 10Mbps

tcp 5010 포트에 rate limit 20Mbps

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

10.6.2. Qos 관련 파라메터

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

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

Premier 3400 시리즈는 각 인터페이스별로 8 개의 queue 를 가지고 있으며, 이들 사이의 mapping

table 을 system wide 하게 유지하고 있다.

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

표 10-21. 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
qos cos-remarking *<0-7> <0-7>*	규칙에 적용된 패킷의 queue 값에 의해 remarking 될 새로운 Cos 값을 설정한다.	Config
qos dscp-dp-map *<0-63> <0-1>*	규칙에 적용된 패킷의 dscp 값에 의해 mapping 될 새로운 dp 값을 설정한다. 이는 show qos dscp 로 확인 가능하다.	Config
qos dscp-pri-map *<0-63> <0-7>*	규칙에 적용된 패킷의 dscp 값에 의해 mapping 될 새로운 pri 값을 설정한다. 이는 show qos dscp 로 확인 가능하다.	Config

표 10-22. Qos 관련 Marking/Remarking 테이블 조회명령

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

10.6.3. Scheduling

Premier 3400 Series 스위치에서는 Scheduling 을 위해 SPQ(Strict Priority Queue) Method 와 WRR(Weighted Round Robin) , WFQ(Weighted Fair Queing) Mothod 를 제공하며 디폴트는 SPQ 이다.
다음 그림은 SPQ 와 WFQ 의 차이점을 나타내고 있다.

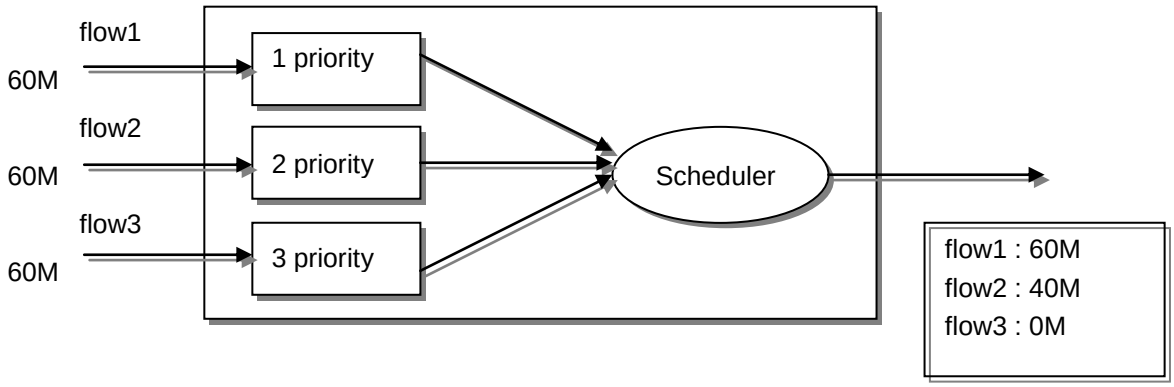


그림 10-2. SPQ(Strict Priority Queue) Method

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

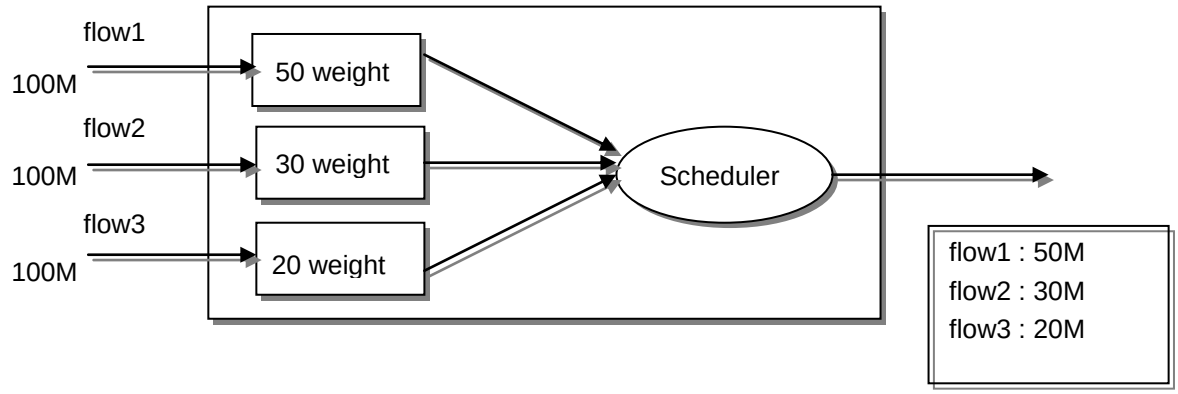


그림 10-3. WRR / WFQ Method

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

weight 에 따른 균등 분배는 아니기 때문에, 트래픽의 상태에 따라서 높은 우선순위의 Queue 에 weight 값 보다 더 많은 트래픽이 할당될 수 있다는 장점이 있다.
Premier 3400 Series 스위치의 경우 8 개의 sheduling 을 위한 Queue 를 제공하며 다음은 특정 인터페이스의 Queue 방식을 결정하는 명령어이다.

표 10-23. Queue-mode 변경 명령

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

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

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

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

표 10-24. Wrr-method Queue weight 변경 명령

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

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

다음은 각 포트의 scheduling 관련 상태를 한눈에 알수 있게 하여준다.

표 10-25. 전체 interface 의 queue-method 및 weight 조회명령

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

10.6.4. Congestion Avoidance

출력쪽의 큐에서 나타나는 혼잡은 실지 네트웍에서 입력 링크와 출력 링크사이에서 속도의 불협화로 출력쪽의 큐가 넘치면서 빈번히 발생한다. 큐의 혼잡이 발생했을 때 버퍼의 자원을 가용하게 하기 위해서 버퍼안에 있는 패킷을 버리는 것과 패킷의 지연시간이 원하는 값 이하로 유지하도록 하는 것이 중요하다.
Premier 3400 Series 스위치는 Flow Classifier 나 Traffic Conditioner 에 의해서 마크된 높은 순위에 있는 패기할 패킷을 우선적으로 버린다. Premier 3400 Series 에서 이를 위한 파라메타은 트래픽 종류에 따라 큐별로 서로 다르게 설정될 수 있다.

10.6.5. Filtering

Netbios 필터는 개별 인터페이스 별로 설정이 가능하며,. Netbios 필터를 설정하면, Netbios / Netbeui / NBT 프로토콜이 모두 차단된다. Dhcp 필터는 개별 인터페이스 별로 설정이 가능하며, 이 필터를 설정하면 해당 인터페이스의 DHCP server 패킷이 차단된다. 또한, 사설 IP 와 loopback IP 를 차단할 수 있다.

명령어들은 다음과 같다.
설정된 내용은 show interface 로 확인이 가능하다.

표 10-26. 기타 Filtering 관련 명령

명령어	설명	모드
filter netbios	특정 인터페이스에 netbios 필터를 설정한다...	Interface
no filter netbios	특정 인터페이스에 netbios 필터를 해제한다.	Interface
filter dhcp	특정 인터페이스에 dhcp filtering 을 설정한다.	Interface
no filter dhcp	특정 인터페이스에 dhcp fltering 을 해제한다.	Interface
filter private-ip [10|172|192|all]	특정 인터페이스에 사설 IP filtering 을 설정한다.	Interface
no filter private-ip [10|172|192|all]	특정 인터페이스에 사설 IP filtering 을 해제한다.	Interface
filter src-ip-all-f	특정 인터페이스에 src IP 가 all f (255.255.255.255) 인 패	Interface

	킷의 filtering 을 설정한다.	
no filter src-ip-all-f	특정 인터페이스에 src IP 가 all f (255.255.255.255) 인 패킷의 filtering 을 해제한다.	Interface
filter src-ip-loopback	특정 인터페이스에 loopback ip (127.0.0.0/8) 인 패킷의 filtering 을 설정한다.	Interface
no filter src-ip-loopback	특정 인터페이스에 loopback ip (127.0.0.0/8) 인 패킷의 fltering 을 해제한다.	Interface

11

환경 설정 저장 및 소프트웨어 업그레이드

11.1. Flash 파일 시스템

본 장에서는 시스템의 Flash File System 의 관리에 대해서 설명한다. Flash File System 은 시스템 OS Image 와 Configuration 파일을 저장하는 장소로 사용되며, 저장된 OS Image 와 Configuration File 은 시스템 boot 시 시스템에 Loading 된다.

- Flash File System 운용에 필요한 명령어
- OS Image 와 Configuration File Management 에 필요한 명령어
- 부팅 모드 설정에 필요한 명령어

Premier 3400 Series 스위치는 OS image 저장 및 환경 설정을 위해 Flash 파일 시스템을 구축한다. 이 장에서 본 제품의 Flash 파일 시스템에 대한 개략적인 설명을 한다.

Flash 파일 시스템은 OS image 와 Configuration 을 파일 형태로 저장하여 사용한다. 각 파일은 Flash 메모리의 영역에서 기록되어지고, 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 File 이 Reload 시 부팅할 Image 또는 Configuration File 인지 주의해야 한다.

시스템 파일 관리를 위한 기본 명령어는 다음과 같다.

표 11-1. 파일 관리를 위한 명령어

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

다음은 show flash 명령어를 시행하였을 때 나타나는 출력문의 예시를 나타낸다. Premier 3400 Series 스위치는 Flash File System 의 정보에 대해서 이름과 그 파일 사이즈, 그리고 현재(-) 및 다음 부팅 모드(*)에 대한 정보와 함께 그 파일이 OS 인지 Configuration 파일인지 나타낸다.

```
Switch# show flash

-length- -----------type/info------------ CN path
5336443  1.1.1                           B* p36xx.test
5333998  1.1.1                           -- p36xx.test2
2775     text file                       -- test
2595     text file                       B* base.cfg
72098    text file                       -- config.txt

1740 Kbytes available (14762 Kbytes used)

Switch#
```

11.2. Image/Configuration File Down/Up Load

Premier 3400 Series 스위치는 운영하면서 필요한 OS Image 와 Configuration File 에 대해서 FTP 또는 TFTP 를 이용해서 Down 또는 Up Load 할 수 있다. 이는 새로운 파일을 Flash 파일에 저장하거나, 재부팅시 OS Image 나 Configuration 으로 적용될 수도 있습니다. 또한 운용상 필요한 OS Image 나 Configuration 을 FTP/TFTP Server 에 저장할 수 있다. 이 장에서는 어떻게 FTP/TFTP 를 통해서 파일을 Down/Up Load 하는지 설명한다. 아래에서 기술한 running-config 및 startup-config 에 대한 설명은 "Configuration File 관리"라는 장에 설명해 놓았다.

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

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

11.2.1. FTP 를 통한 Down/Up Load

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

표 11-2. FTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy ftp flash	• FTP Server 에 있는 OS Image File 을 Flash 에 저장한다.	Privileged
copy flash ftp	• Flash 에 있는 OS Image File 을 FTP Server 에 저장한다.	Privileged
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

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 ? p36xx.100
Destination file name ? p36xx.100

FTP::192.168.0.1//p36xx.100-->image file[p36xx.100]
Proceed [yes/no]?  yes
.....................................................................
(생략)
```

11.2.2. TFTP 를 통한 Down/Up Load

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

표 11-3. TFTP 를 통한 Down/Up Load 명령어

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

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

```
Switch# copy flash tftp
IP address of remote host ? 192.168.0.1
filename to write on tftp host? p36xx.100

TFTP send: -> 192.168.0.1// p36xx.100
Proceed [yes/no]? yes
.....................................................................
(생략)
```

11.3. Configuration File 관리

환경 설정은 시스템 운영자가 Premier 3400 Series 스위치를 운영하면서 설정된 다양한 파라미터의 집합이다. Premier 3400 Series 스위치에서 사용하는 Configuration 에는 startup-config 와 running-config 가 있다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration 을 startup-config 라 하며, DRAM 내에서 구동하는 환경설정 값을 running-config 라 한다. 여기서는 Configuration File Management 에 필요한 저장, 삭제 및 다운로드 방법을 설명한다.

표 11-4. Configuration Management 명령어

명령어	설명	모드
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 Config
write memory	• copy running-config startup-config 와 동일한 기능을 한다.	Privileged Config
erase startup-config	• 현재 설정된 startup configuration 파일을 지운다.	Privileged

11.3.1. Configuration file 의 저장

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

```
Switch# show running-config

interface vlan1
 ip address 192.168.51.1/24
     ... <생략> ....
Switch#
Switch# copy running-config startup-config
Overwrite 'base.cfg'? [yes/no] y
```

```
Switch# how startup-config

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

11.3.2. Configuration file 의 삭제

Premier 3400 Series 스위치는 시스템 재시동 시 flash 메모리에 저장되어 있는 startup-config 를 재 로딩한다. 만약 현재 저장되어 있는 Configuration file 중에 필요 없는 configuration file 이 있다면 erase command 를 사용해 삭제할 수 있다. 만약 필요 없는 configuration file 이 test.cfg 라면 다음과 같이 한다.

```
Switch# erase test.cfg
Switch#
```

11.4. Boot Mode 설정 및 시스템 재시동

Premier 3400 Series 스위치는 운영하면서 필요한 OS Image 와 Configuration File 에 대해서 다음 부팅 파일로 설정할 수 있다. 이렇게 설정된 OS Image 와 Configuration File 은 시스템의 재 시동 시 적용되므로 각별한 주의가 필요하다. 아래에서는 OS Image 와 Configuration File 에 대해서 어떻게 다음 부팅 모드로 설정하는 지와 시스템 재 시동 방법에 대해서 설명해 놓았다.

표 11-5. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
boot flash *filename*	• 다음 부팅 시 적용될 OS Image 를 설정한다.	Privileged
boot config *filename*	• 다음 부팅 시 적용될 Configuration File 을 설정한다.	Privileged
reload	• 시스템을 재 시동 시킨다.	Privileged

11.4.1. Boot Mode 설정

Premier 3400 Series 스위치에서 OS Image 와 Configuration File 에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요하다. boot flash 명령어를 실행할 때에는 Premier 3400 Series 스위치에서 사용할 수 있는 OS Image File 에 대해서만 적용하도록 해야 하며, 또 boot config 명령어를 시행할 때에는 Premier 3400 Series 스위치에서 사용할 수 있는 Configuration File 에 대해서만 적용하도록 해야 된다. 그리고 현재 Flash File System 에 있는 File 에 대해서만 적용하도록 하여야 한다.

```
Switch#
Switch# boot flash p36xx..r101
Switch#
Switch# boot config lns.cfg
Switch#
```

11.4.2. 시스템 재시동

시스템의 재시동은 Premier 3400 Series 스위치의 전원 On/Off 를 이용하는 H/W 적인 방법이 있으며, 콘솔 또는 원격 접속 후 쉘 상에서 명령어로 하는 S/W 적인 방법이 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#
```

12 Utility

12.1. Packet Dump 기능

본 Premier 3400 Series 스위치에서는 cpu usage 수치가 미리 설정된 threshold 값을 상회할 경우 tcpdump 를 자동 실행하여 트래픽에 대한 로그 파일을 생성하고 조회하는 기능을 제공한다.

12.1.1. 자동 실행 조건

cpu usage 가 미리 설정된 threshold 값을 상회할 경우 tcpdump가 백그라운드로 자동 실행되어 파일로 저장되며, 조건 (설정된 패킷 수 수신 or 실행 후 1분 경과) 에 따라 자동 종료됩니다.

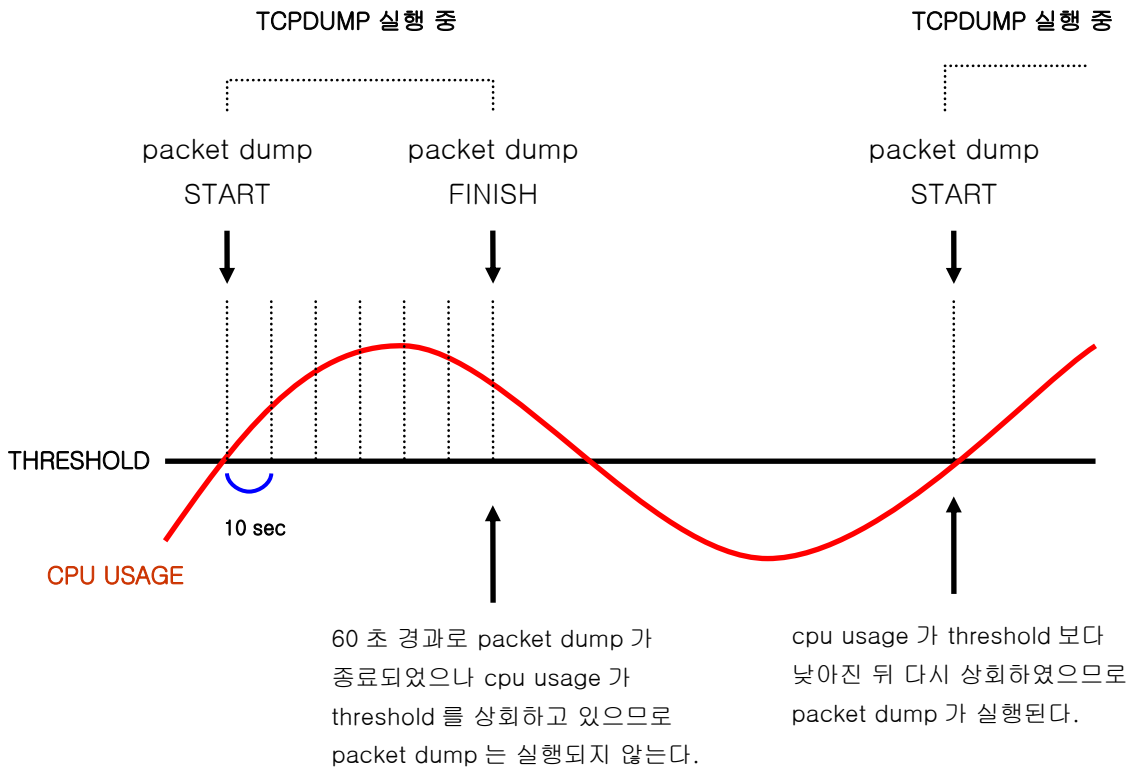
cpu usage가 설정된 threshold 값을 상회할 경우 실행 조건에 따라 tcpdump가 자동 실행되며, 설정된 수신 패킷 수를 모두 수신하거나 자동 실행 후 1분이 경과하면 강제 종료된다. 강제 종료는 사용자가 직접 실행하는 tcpdump 명령과는 간섭이 없으며, 종료 직후에도 cpu usage가 threshold 값을 상회하고 있을 경우 이미 dump된 트래픽과 같은 종류의 트래픽으로 간주하고 cpu usage가 threshold 값보다 낮아질 때까지 실행되지 않는다.

12.1.2. 자동 실행되지 않는 경우

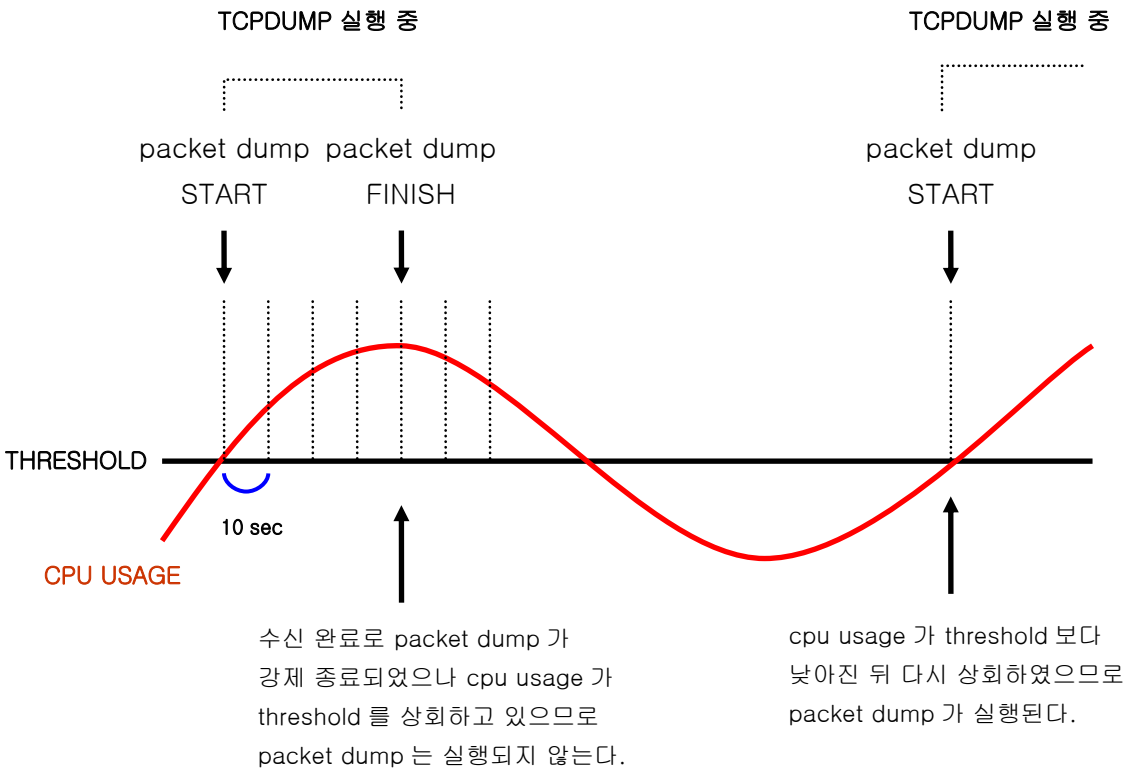
① 자동 실행된 tcpdump 의 중지 혹은 종료 직후에도 cpu usage가 threshold 값을 상회하고 있을 경우, 이전과 같은 종류의 트래픽으로 간주하고 자동 실행하지 않는다. (cpu usage가 threshold 값 이하로 내려간 뒤 다시 상회할 경우에 실행됨.)
② threshold 가 0으로 설정된 경우 자동 실행되지 않는다.

다음은 실행 조건 예이다.

60초 내에 설정한 패킷 수만큼 수신되지 않아 자동 종료되었고, 종료 후에도 cpu usage가 threshold를 상회할 경우



60 초 이전에 설정된 패킷 수만큼 수신하여 강제 종료되었고 (40 초 경과 후 수신이 완료된 것으로 가정함), 종료 후에도 cpu usage 가 threshold 를 상회할 경우



12.1.3. config 설정 및 초기화, 조회

표 12-1. threshold 의 설정 및 해제, 조회 명령어

명령어	설명	모드
dump traffic threshold <0-100>	packet dump 가 실행될 threshold 설정	config
no dump traffic threshold	threshold 의 초기화 (0 으로 설정)	config
dump traffic count <100-500>	실행 1 회 당 dump 할 패킷수 설정	config
no dump traffic count	dump 할 패킷수를 100 으로 설정 (default)	config

dump traffic interface INTERFACE	packet dump 할 interface 를 설정	config
no dump traffic interface	interface 를 any (모든 interface, default)로 설정함	config
dump traffic enable	packet dump 기능을 활성화함	config
dump traffic disable	packet dump 기능을 비활성화함	config
show dump config	threshold 의 조회	Privileged

다음은 threshold 를 20 으로 설정하여 packet dump 를 실행하는 과정이다. (cpu usage 가 20 을 상회할 경우 packet dump 가 실행되며, 100 개의 패킷을 전체 interface 에 대해서 dump 한다.)

```
switch#
switch# configure terminal
switch(config)# dump traffic threshold 20
switch(config)# dump traffic enable
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 100
dump traffic interface is any
dump traffic is enabled
switch#
```

다음은 threshold 를 20 으로, packet count 를 500 으로, interface 를 vlan1 로 설정하여 packet dump 를 실행하는 과정이다. (cpu usage 가 20 을 상회할 경우 실행되며, 500 개의 패킷을 vlan1 interface 에 대해서 dump 한다.) 주의할 점은 interface 설정 시 반드시 ip address 할당이 가능한 인터페이스(vlan, eth0 등)를 설정해야 한다는 것이다.

```
switch#
switch# configure terminal
switch(config)# dump traffic threshold 20
switch(config)# dump traffic count 500
switch(config)# dump traffic interface vlan1
switch(config)# dump traffic enable
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 500
dump traffic interface is vlan1
dump traffic is enabled
```

```
switch#
```

다음은 packet dump 기능을 비활성화하는 과정이다. threshold, count, interface 가 설정되어 있더라도 packet dump 는 실행되지 않는다.

```
switch#
switch# configure terminal
switch(config)# dump traffic disable
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 500
dump traffic interface is vlan1
dump traffic is disable
switch#
```

다음은 설정을 초기화하는 과정이다.

```
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 500
dump traffic interface is vlan1
dump traffic is disabled
switch#
switch# configure terminal
switch(config)# no dump traffic threshold
switch(config)# no dump traffic count
switch(config)# no dump traffic interface
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 0
dump traffic count is 100
dump traffic interface is any
dump traffic is disabled
switch#
```

12.1.4. Log File 의 조회

표 12-2. Log File 조회 명령어

명령어	설명	모드
show dump-file FileName	해당 log file 의 내용을 조회한다.	privileged
show dump-file FileName OPTION	tcpdump 옵션을 추가하여 해당 log file 의 내용을 조회한다. 각 옵션에 해당하는 추가 정보를 출력할 수 있다.	privileged

packet dump 파일은 flash 에 저장되며, show flash 명령을 통해 파일명과 생성된 시간을 확인할 수 있다.

예) **pktdump_1(Jan 14 02:41:50)** : 1 월 14 일 02 시 41 분 50 초에 생성된 dump 파일.

```
Switch# show flash

-length- -----------type/info------------ CN path
5336443  1.1.1                           B* p36xx.test1
5333998  1.1.2                           -- p36xx.test2
2775     text file                       -- test
2595     text file                       B* base.cfg
414      text file                       -- pktdump_1(Jan 14 02:41:50)
72098    text file                       -- config.txt

1696 Kbytes available (14806 Kbytes used)

Switch#
```

다음은 pktdump_1 파일을 조회하는 과정이다.

```
switch#
switch# show dump-file pktdump_1
01:01:39.652358 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:40.662453 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:41.672519 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
```

```
01:01:42.682603 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:43.692650 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:44.702824 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:45.712877 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:46.155500 [fa1(1)] 192.168.0.181 > 224.0.0.5: OSPFv2-hello 44: area
0.0.0.1 dr 192.168.0.181 [tos 0xc0] [ttl 1]
01:01:46.723229 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:47.732996 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:48.743046 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:49.753138 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:50.392509 [fa1(1)] 192.168.0.29.138 > 192.168.0.255.138: udp 201
01:01:50.763271 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:51.773442 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:52.783324 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:53.793428 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:54.803500 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:55.813607 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:56.156198 [fa1(1)] 192.168.0.181 > 224.0.0.5: OSPFv2-hello 44: area
0.0.0.1 dr 192.168.0.181 [tos 0xc0] [ttl 1]
01:01:56.824045 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:57.833789 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
```

✓ dump 된 패킷은 tcpdump raw file 로 저장되므로 조회 시 기본 정보만 출력된다. 다양한 packet 정보를 확인하기 위해서는 다음 13.2.1.3 과 같이 tcpdump 옵션을 추가한다.

다음은 옵션을 추가하여 pktdump_1 파일을 조회하는 과정이다.

```
switch# show dump-file tcpdump_19700116195734 ve
01:01:39.652358 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36074)
01:01:40.662453 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36075)
01:01:41.672519 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36076)
01:01:42.682603 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36077)
01:01:43.692650 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36078)
```

```
01:01:44.702824 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36079)
01:01:45.712877 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36080)
01:01:46.155500 [fa1(1)] 0:7:70:33:11:5 1:0:5e:0:0:5 0800 78:
192.168.0.181 > 224.0.0.5: OSPFv2-hello 44: area 0.0.0.1 E mask
255.255.255.0 int 10 pri 1 dead 40 dr 192.168.0.181 nbrs [tos 0xc0] [ttl
1] (id 4346)
01:01:46.723229 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36081)
01:01:47.732996 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36082)
01:01:48.743046 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36083)
01:01:49.753138 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36084)
01:01:50.392509 [fa1(1)] 0:15:f2:27:e7:1 ff:ff:ff:ff:ff:ff 0800 243:
192.168.0.29.138 > 192.168.0.255.138: udp 201 (ttl 128, id 29631)
01:01:50.763271 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36085)
01:01:51.773442 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36086)
01:01:52.783324 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36087)
01:01:53.793428 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36088)
01:01:54.803500 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36089)
01:01:55.813607 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36090)
01:01:56.156198 [fa1(1)] 0:7:70:33:11:5 1:0:5e:0:0:5 0800 78:
192.168.0.181 > 224.0.0.5: OSPFv2-hello 44: area 0.0.0.1 E mask
255.255.255.0 int 10 pri 1 dead 40 dr 192.168.0.181 nbrs [tos 0xc0] [ttl
1] (id 4347)
01:01:56.824045 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36091)
01:01:57.833789 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 >
224.0.0.18: ip-proto-112 20 (ttl 255, id 36092)
```

✓ 위와 같이 특정 tcpdump option 을 추가할 경우 그에 해당하는 정보를 추가로 출력할 수 있다. 예를 들어, "**show dump-file pktdump_1 evt**" 를 실행할 경우, 해당 파일을 조회하되 각각 패킷의 조회 결과에 link-level header 정보 (e 옵션)와 TTL, identification, total length 등 (v 옵션), timestamp (t 옵션) 등이 추가되어 출력된다. 주의할 점은, tcpdump raw file 조회와 관련되지 않는 옵션이 지정되거나 옵션 형식(evt 와 같이 알파벳으로만 구성되어야 하며 순서는 없음)이 일치하지 않을 경우 로그 파일 내용이 출력되지 않는다.

12.1.5. Log File 의 관리

저장되는 로그 파일의 수는 최대 3 개로 관리된다. 만일 로그 파일의 개수가 3 개를 초과하게 될 경우 가장 이전에 만들어진 파일을 삭제한 뒤 새로 생성된다.

12.2. CPU Packet Counter

이 장에서는 CPU 로 올라오는 packet 의 종류를 구별하여 count 해 주는 Packet Counter 를 설정하는 방법에 대해 설명한다.

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

12.2.1. 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.

12.2.2. 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.

12.2.2.1. 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

12.2.2.2. 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#
```

Notice Ethertype 은 "unsigned short", IP protocol 은 "unsigned char", TCP/UDP port 는 "unsigned short" 값으로 입력해야 한다.

12.2.2.3. 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.

12.2.3. 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#
```

13

Dynamic ARP Inspection

이 장에서는 ARP 패킷을 검사하는 dynamic Address Resolution Protocol (ARP) inspection (DAI) 기능에 대한 설정 방법을 설명한다.

Notice 이 장에서 사용되는 명령어에 대한 문법과 사용 방법에 관한 상세한 정보는 command reference 를 참조하라.

이 장은 다음과 같은 내용으로 이루어져 있다:

- DAI에 대한 이해 (Understanding DAI)
- DAI 기본 설정 (Default DAI Configuration)
- DAI 설정 지침과 제약 사항 (DAI Configuration Guidelines and Restrictions)
- DAI 설정 (Configuring DAI)
- DAI 설정 예제 (DAI Configuration Samples)

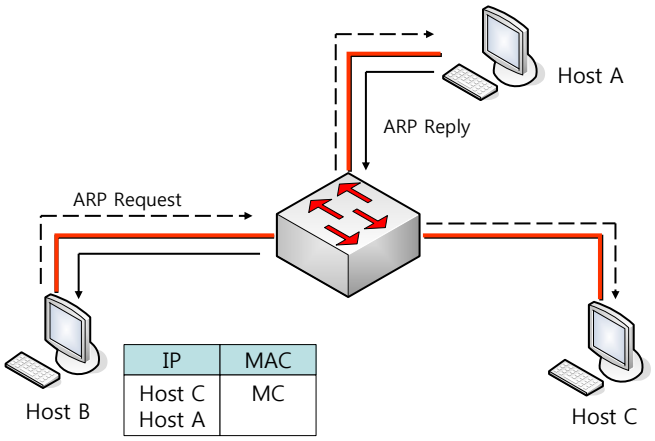
13.1. Understanding DAI

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

13.1.1. 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.

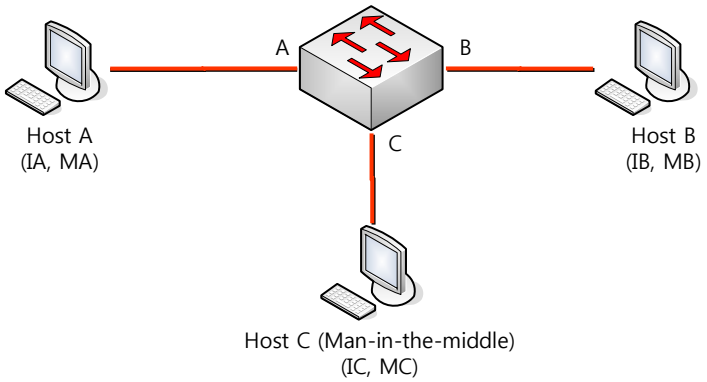


호스트 B 는 호스트 A 의 IP 주소에 대응하는 MAC 주소를 알아내기 위해서, 브로드캐스트 도메인 내부의 모든 호스트들에게 브로드캐스트 메시지 (ARP request)를 전송한다. 브로드캐스트 도메인 내부의 모든 호스트들은 호스트 B 가 전송한 ARP request 를 수신하고, 호스트 A 는 자신의 MAC 주소를 응답한다.

13.1.2. Understanding ARP Spoofing Attacks

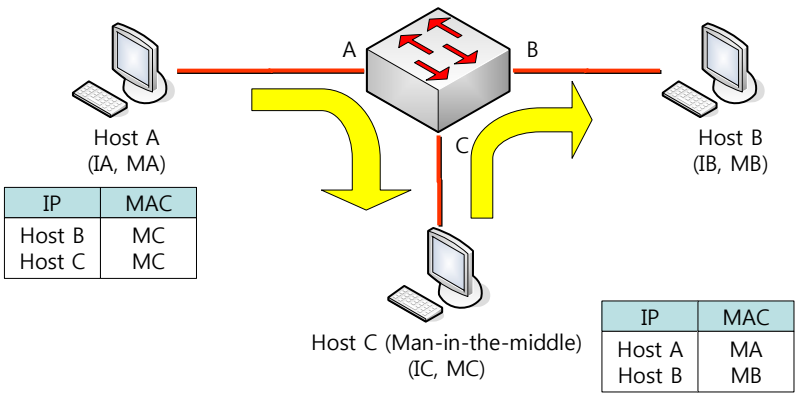
ARP 는 ARP request 를 수신하지 않은 호스트가 전송한 gratuitous reply 로 ARP 테이블이 변경되는 것을 허용한다. 이로 인해 ARP spoofing 공격과 ARP cache poisoning 이 발생할 수 있다. 공격 이후에는 공격 당한 장비의 모든 트래픽은 공격자의 컴퓨터를 통해 라우터, 스위치 또는 호스트로 전달된다.

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.



13.1.3. Understanding DAI and ARP Spoofing Attacks

DAI 는 ARP 패킷을 검사하는 보안 기능이다. DAI 는 유효하지 않은 IP-to-MAC 주소 binding 을 가진 ARP 패킷을 로깅 logging 하고, 폐기 drop 한다. 이 기능은 main-in-the-middle attack 으로부터 네트워크를 보호한다.

DAI 는 ARP 테이블이 오직 유효한 ARP request 와 response 에 의해 변경되도록 동작한다. DAI 기능이 활성화된 스위치는 다음과 같이 동작한다:

- untrusted 포트로 수신한 모든 ARP 패킷을 검사한다.
- 자신의 ARP 캐시를 변경하기 전에, 수신한 패킷이 유효한 IP-to-MAC 주소 binding 을 가지고 있는지 검사한다.
- 유효하지 않은 ARP 패킷을 폐기한다.

DAI 는 ARP 패킷의 유효성을 검사할 때, 신뢰할 수 있는 데이터베이스 database 인 DHCP snooping binding 데이터베이스에 저장된 IP-to-MAC 주소 binding 을 사용한다.

> **Notice** 스위치와 VLAN 에 DHCP snooping 이 활성화 되어 있을 때, DHCP snooping 에 의해 DHCP snooping binding 데이터베이스가 생성된다.

ARP 패킷을 수신한 인터페이스의 특성에 따라 스위치는 다음과 같이 동작한다:

- trusted 인터페이스로 수신한 ARP 패킷은 검사하지 않는다.
- untrusted 인터페이스에 대해서는 오직 유효한 패킷만 허용한다.

DAI 는 정적으로 할당된 IP 주소를 가진 호스트에 대해서는 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.

13.1.4. Interface Trust States and Network Security

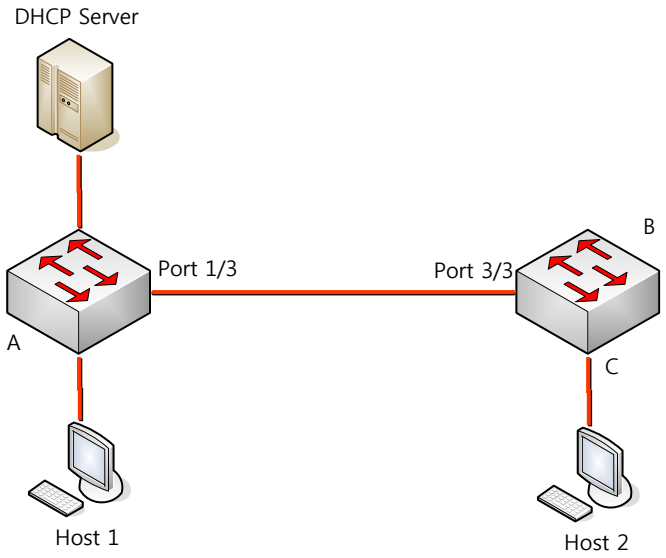
DAI 는 스위치의 각 인터페이스에 대한 trust 상태 state 정보를 유지하고 있다. Trusted 인터페이스를 통해 수신한 패킷에 대해서는 어떤 DAI 검사도 수행하지 않는다. 반면, Untrusted 인터페이스를 통해 수신한 패킷은 DAI 의 검사를 받는다.

전형적인 네트워크 구성에서, 호스트와 연결된 스위치 포트를 untrusted 로 설정하고 스위치에 연결된 포트는 trusted 로 설정한다. 이런 설정에서, 이 스위치를 통해 네트워크로 유입되는 모든 ARP 패

킷은 보안검사를 받게 된다. VLAN 이나 네트워크의 다른 장소에서 더 이상의 유효성 검사가 필요하지는 않다. trust 설정은 인터페이스 설정 명령인 **ip arp inspection trust** 를 사용하면 된다.

Caution 네트워크 보안을 위해 스위치가 모든 ARP 패킷을 검사하도록 하려면, 특별한 기능이 필요하다. 즉, DAI 가 스위치의 포워딩 엔진 forwarding engine 을 통해 포워딩되는 유니캐스트 ARP 패킷도 검사할 수 있도록 스위치의 CPU 로 trap 할 수 있어야 한다.
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 사용중인 스위치와 사용하지 않는 스위치를 분리해야 한다.

Notice Premier 3000 시리즈는 DAI 가 모든 ARP 패킷을 검사하는 네트워크를 보호 기능을 제공한다.

13.1.5. Rate Limiting of ARP Packets

DAI 기능이 활성화된 스위치는 CPU 로 유입되는 ARP 패킷의 rate 를 제한한다. 디폴트로 untrusted 인터페이스에 대해서 초당 15 개 (15 pps)의 ARP 패킷만 허용되며, trusted 인터페이스의 rate 는 제한하지 않는다. 인터페이스 설정 명령 **ip arp inspection limit** 를 사용해서 설정을 변경할 수 있다.

특정 포트를 통해 CPU 로 유입되는 ARP 패킷의 rate 가 설정한 값을 초과하면, 스위치는 이 포트로 수신한 모든 ARP 패킷을 폐기한다. 사용자가 설정을 변경할 때까지 이 상태가 유지된다. 인터페이스 설정 명령 **ip arp inspection limit auto-recovery** 를 사용하면, 일정 시간이 경과한 후 포트를 자동으로 서비스 가능 상태로 만들 수 있다.

Notice ARP 패킷의 rate limit 는 CPU 에서 software 로 처리되기 때문에, Denial-of-Service (DoS) 공격에 대해 큰 효과를 기대할 수 없다.

13.1.6. 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.

13.1.7. 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.

13.2. 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.

13.3. DAIConfigurationGuidelinesand 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.

> **Notice** DAI 가 DHCP 서버와 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.

13.4. 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

13.4.1. 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* Switch(config)# **no ip arp inspection vlan** *vlan-id*	VLAN 에 DAI 를 enable 한다. VLAN 에 DAI 를 disable 한다.
Switch# **show ip arp inspection**	설정을 확인한다.

Notice VLAN 에 DAI 를 enable 하면, 해당 VLAN 을 통해 송수신 되는 모든 ARP 패킷을 검사한다. 다시 말해, 스위치의 ARP 캐시와 네트워크가 함께 보호된다.

다음의 예는 VLAN 200 에 DAI 를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200
```

다음의 예는 설정을 확인하는 방법을 보여준다:

```
Switch# show ip arp inspection
DHCP Snoop Bootstrap        : Disabled
Source MAC Validation       : Disabled
Destination MAC Validation : Disabled
IP Address Validation       : Disabled
ARP Field Validation        : Disabled

Vlan  Config    Operation  ACL Match             Static ACL  ACL Log   DHCP Log
----  --------  ---------  --------------------  ----------  --------- --------
 200  Enabled   Active+                          No          Deny      Deny
```

13.4.2. 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-fa1/1)# **ip arp inspection trust** Switch(config-if-fa1/1)# **no ip arp inspection trust**	스위치와 연결된 인터페이스를 trusted 로 설정한다. (default: untrusted) 스위치와 연결된 인터페이스를 untrusted 로 설정한다.
Switch(config-if-fa1/1)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection interfaces**	설정을 확인한다.

다음의 예는 Fast Ethernet 포트 2/1 을 trusted 로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface fa2/1
Switch(config-if-fa2/1)# ip arp inspection trust
Switch(config-if-fa2/1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
fa2/1            Trusted            None               1       Disabled
fa2/2            Untrusted            15               1       Disabled
```

13.4.3. 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
```

13.4.4. Configuring ARP Packet Rate Limiting

DAI 가 활성화 되면 스위치는 모든 ARP 에 대해 유효성 검사를 하고, 이로 인해 스위치는 ARP 패킷의 DoS 공격에 취약해진다. 스위치의 CPU 에서 ARP 패킷의 rate 를 제한함으로써 CPU 의 부하를 감소시킬 수 있다.

Notice DAI 가 제공하는 ARP rate limit 는 소프트웨어 기능이기 때문에, 스위치의 CPU 사용률을 직접적으로 감소시킬 수는 없다. 하지만 DAI 가 처리하는 ARP 패킷의 양을 조절함으로써, DAI 에 의한 CPU 사용률을 낮출 수는 있다.

포트에 대해 ARP 패킷에 대한 rate limit 를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **configure terminal**	global 설정로 진입한다.
Switch(config)# **interface** *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드 로 진입한다.
Switch(config-if-fa1/1)# **ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] | **none**} Switch(config-if-fa1/1)# **no ip arp inspection limit**	(옵션) ARP packet rate limit 를 설정한다. default 설정으로 복원한다.
Switch(config-if-fa1/1)# **ip arp inspection limit enable** Switch(config-if-fa1/1)# **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 fa2/1 에 ARP packet rate limit 를 설정하는 예이다:

```
Switch# configure terminal
```

```
Switch(config)# interface fa2/1
Switch(config-if-fa2/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-fa2/1)# ip arp inspection limit enable
Switch(config-if-fa2/1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
fa2/1            Untrusted            20               2       Disabled
fa2/2            Untrusted            15               1       Disabled
```

13.4.5. 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-fa1/1)# ip arp inspection limit auto-recovery *seconds* Switch(config)# no ip arp inspection limit auto-recovery	(옵션) 자동 복구 기능을 활성화 시킨다. 자동 복구 기능을 해제한다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection interfaces	설정을 확인한다.

다음은 인터페이스 fa2/1 이 ARP rate limit 에 의해 ARP 패킷 수신이 차단되었을 경우, 10 초 후에 자동으로 복구되도록 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface fa2/1
Switch(config-if-fa2/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-fa2/1)# ip arp inspection limit enable
Switch(config-if-fa2/1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
fa2/1            Untrusted            20               2             10
fa2/2            Untrusted            15               1       Disabled
```

13.4.6. Enabling Additional Validation

DAI 로 ARP 패킷의 destination MAC 주소, sender 와 target IP 주소, source MAC 주소에 대한 유

효성 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
```

13.4.7. 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

13.4.8. DAI Logging Overview

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성한다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제된다. 각각의 로그에는 flow 정보(수신한 VLAN, port 번호, 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.

13.4.9. 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.
```

13.4.10. 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.
```

13.4.11. Configuring the DAI Log Filtering

ARP 패킷을 검사한 후, 그 결과에 대한 시스템 메시지를 선택적으로 생성할 수 있다.
DAI 의 log filtering 기능을 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# **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
```

13.4.12. 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.

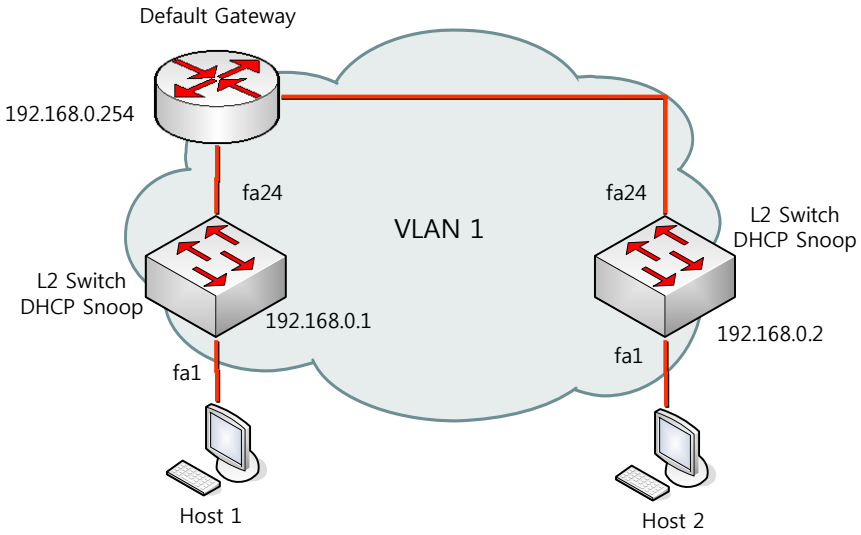
13.5. DAI Configuration Samples

이 절은 다음과 같은 예제들을 포함한다:

- Sample One: Interoperate with DHCP Snoop

13.5.1. Sample One: Interoperate with DHCP Snoop

이 예제는 DHCP snoop 기능을 사용하는 스위치에 DAI 를 설정하는 방법을 설명한다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정하자:



Caution 가입자가 연결된 L2 스위치에서 DAI 를 사용하려면, 연결된 모든 L2 스위치에서 DAI 를 사용해야 한다. DAI 를 제공하지 않는 L2 스위치가 포함되어 있으면 통신 장애가 발생할 수 있다.

DHCP snoop 이 활성화된 L2 스위치에는 같은 VLAN 에 Default gateway 와 L2 스위치 또는 호스트가 연결된다. L3 스위치와 L2 스위치는 고정 IP 주소를 사용한다. 호스트 1 과 호스트 2 는 DHCP 를 통해 IP 주소를 할당 받는다.

Notice 이런 구성에서 DAI 는 IP-to-MAC binding 정보를 전적으로 DHCP snooping binding 정보에 의존한다. DHCP snooping 설정은 DHCP snooping 매뉴얼을 참고하라.

DHCP snoop 기능이 활성화 된 스위치에서 DAI 기능을 사용하려면, 다음과 같이 설정한다:

Step 1 DHCP 로 IP 를 할당 받는 호스트의 IP-to-MAC binding 정보를 구축하기 위해, VLAN 1 에 DHCP snooping 을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# ip dhcp snooping
```

Step 2 스위치가 연결된 포트를 Trust port 로 설정한다. Trust port 로부터 수신된 ARP 패킷은 무조건 허용된다.

```
Switch# configure terminal
Switch(config)# interface fa24
Switch(config-if-fa24)# ip arp inspection trust
```

Step 3 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
```

Step 4 ARP 패킷을 차단하기 위한 flow rule 과 policy map 을 생성한다.

```
Switch# configure terminal
Switch(config)# flow-rule arp classify ethertype 0806
Switch(config)# flow-rule arp match drop
Switch(config)# flow-rule arp match trap-cpu
Switch(config)# policy-map arp-trap flow-rule arp
Switch(config)# end
```

Step 5 가입자가 연결된 포트에 flow rule 을 적용한다.

```
Switch# configure terminal
Switch(config)# service-policy fa1 ingress arp-trap
Switch(config)# end
```

14 ARP Snoop

이 장에서는 특정 IP 주소 영역에 대한 Ethernet 주소 정보를 구축하기 위해 사용되는 ARP snoop 기능의 설정 방법에 대해 설명한다.

Notice 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)

14.1. Understanding ARP Snoop

이 절에서는 ARP snoop 기능에 대해 설명한다.

14.1.1. 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 14-1 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.

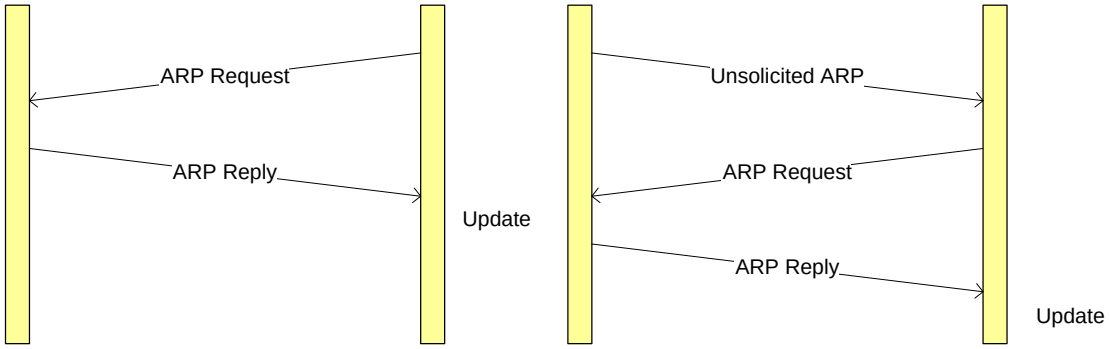


그림 14-1. ARP snoop (3-way handshake)

ARP 패킷 자체에 보안 기능이 없으므로, 여러 개의 ARP Reply 를 수신했을 경우에 어떤 것이 유효한 가를 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.

14.1.2. 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.

14.1.3. 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.

14.1.4. 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.

14.1.5. 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.

Notice 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.

14.1.6. Understanding DAI and ARP Snoop

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.

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.

Notice 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.

14.1.7. 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.

14.2. 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.

14.3. 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

14.3.1. 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
```

14.3.2. 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 마라.

14.3.3. 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
```

14.3.4. 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
```

14.3.5. 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.

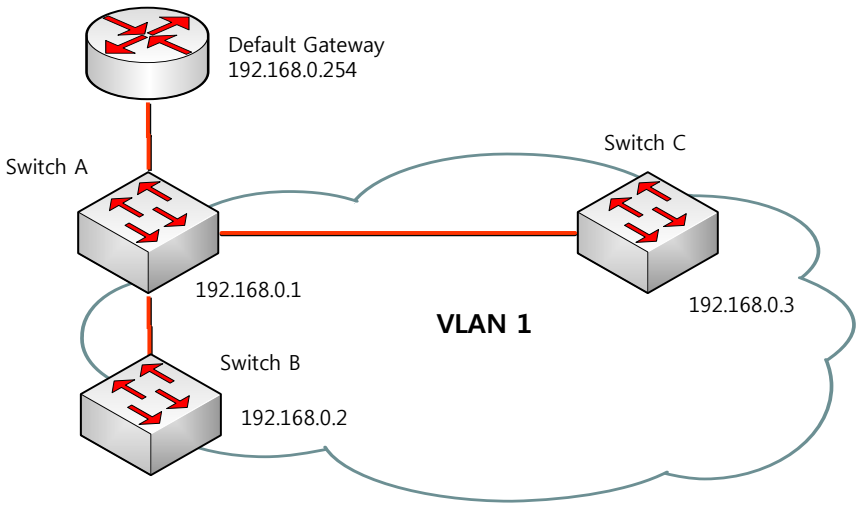
14.4. ARP Snoop Configuration Samples

이 절은 다음과 같은 예제들을 포함한다:

- Sample One: ARP spoofing detection

14.4.1. 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
```

Notice 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.