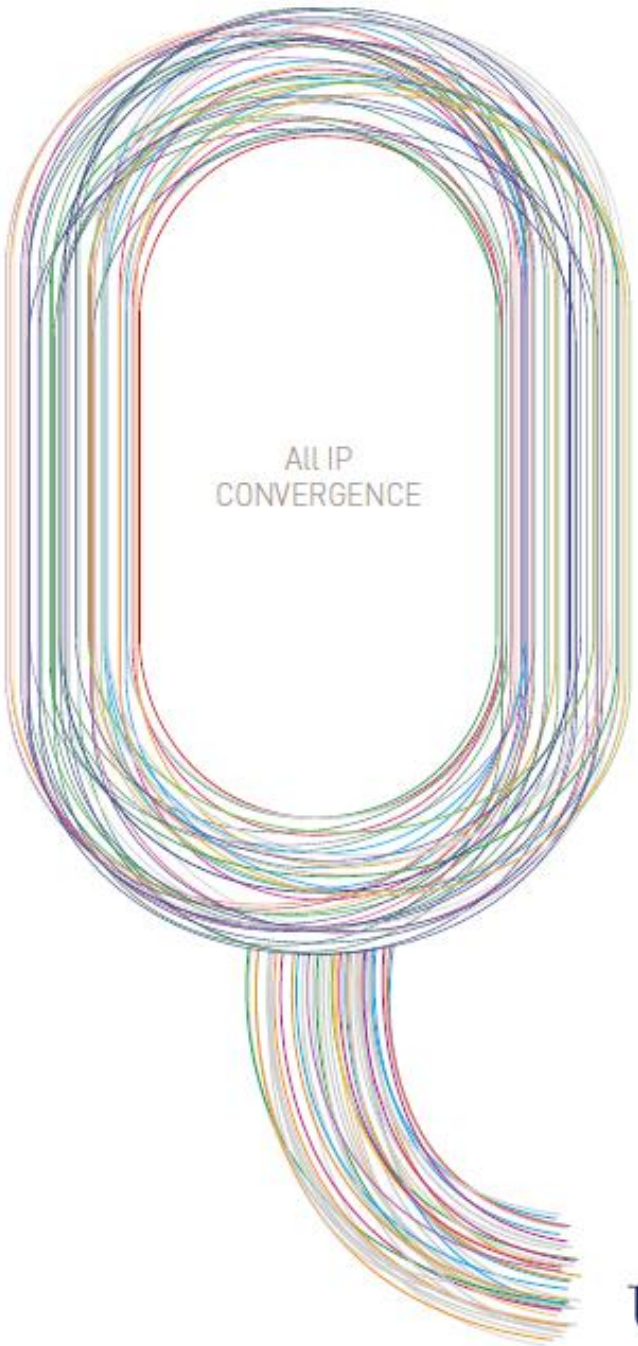
CS3400 Series
User Guide



Published: Mar 2011

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 CS3400 Mobile Backhaul 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
- 캐리어 이더넷 개념
- TCP/IP 프로토콜 개념
- Simple Network Management Protocol (SNMP)

Notice CS3400 Series 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하기 바란다.

1.1.1. 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

1.1.2. 관련 문서

CS3400 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

CS3400 Series 스위치를 포함한 ㈜유비쿼스의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(http://www.ubiquoss.com)를 통하여 다운로드 받거나 서비스를 요청할 수 있다.

본 문서는 CS3400 Series 에 대한 통합 매뉴얼이다.

2

CS3400 Series 스위치 시작하기

본 장은 시스템 운영자가 CS3400 Series Mobile Backhaul 스위치의 운용 환경을 처음 설정할 때 필요한 정보를 제공한다. 스위치 시작의 개요는 다음과 같다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- CS3400 Series 스위치 사용자 인터페이스
- 시스템 로그인과 패스워드 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

다음은 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 ↵
% Incomplete command.
Switch #
```

2.1.2. 명령어 문법 도움말(Command Syntax Helper)

CS3400 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. CS3400 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.

다음은 전체 도움말 기능을 show 명령으로 실행해본 결과이다.
show 명령어 다음에 공백 문자와 함께 '?'를 입력하면 운영자가 입력 할 수 있는 파라미터 및 값의 리스트가 출력된다. 그리고 "Switch# show" 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기한다. 운영자 입력에서 '?'는 화면에 표시되지 않는다.

```
Switch# show ?
  access-list         List IP access lists
  arp                 Internet Protocol (IP)
  bgp                 Border Gateway Protocol (BGP)
  bootvar             Boot and related environment variable
  bridge              Bridge information
  calendar            Display the hardware calendar
  class-map           Class map entry
  cli                 Show CLI tree of current mode
  clock               Display the system clock
  command             shell command
  cpu                 cpu status and configuration
  debugging           Debugging functions (see also 'undebug')
  environment         Temperature and FAN status information
  etherchannel        EtherChannel information
  flash:              display information about flash: file system
  flowcontrol         IEEE 802.3x Flow Control
  fm-status           Show the current status
  history             Display the session command history
  hosts               IP domain-name, lookup style and nameservers
  idprom              show IDPROMs for FRUs
  inet-service        Display enabled internet services
  interface           IP interface status and configuration
  ip                  Internet Protocol (IP)
  ipv6                Internet Protocol version 6 (IPv6)
  lacp                LACP commands
  lacp-counter        LACP commands
  list                Show command lists
  logging             Show the contents of logging buffers
  mac-access-list     List MAC access lists
  mac-address-table   MAC forwarding table
  memory              Memory information
  mirror              Port Mirroring
  mls                 mls global commands
  module              Module Info
  nsm                 NSM
  ntp                 Network time protocol
  policy-map          Policy map entry
```

```
    port                port commands
    port-mib            Port-Mib Count
    power               Switch Power
    pppoe               Point-to-Point over Ethernet (PPPoE)
    privilege           Display your current level of privilege
    processes           Active process statistics
    redundancy          Redundancy Facility (RF) information
    reload              Scheduled reload information
    rmon                Remote Monitoring Protocol (RMON)
    route-map           route-map information
    router-guard        Multicast Router-Guard Commands
    router-id           Router ID
    running-config      Current Operating configuration
    service             Setup miscellaneous service
    service-policy      Serivce Policy entry
    slot                Slot Info
    snmp                Show snmp statistics
    spanning-tree       spanning-tree Display spanning tree information
    startup-config      Contents of startup configuration
    system              Display the system information
    tech-support        Show system information for Tech-Support
    uptime              Display elapsed time since boot
    usbflash:           usbflash: file system
    users               Display information about terminal lines
    version             System software status
    virtual-servers     Virtual-servers
    vlan                Display VLAN information
    vrrp                VRRP information
    whoami              Display information about the current user
Switch #show_
```

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

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

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

```
Switch# show p?
   policy-map  Policy map entry
    port        port commands
    port-mib    Port-Mib Count
    power       Switch Power
    pppoe       Point-to-Point over Ethernet (PPPoE)
```

```
    privilege    Display your current level of privilege
    processes    Active process statistics
Switch# show p_
```

2.1.3. 단축 명령어 입력

CS3400 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 CS3400 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:  "show i"
Switch# show i?
    idprom         show IDPROMs for FRUs
    inet-service   Display enabled internet services
    interface      IP interface status and configuration
    ip             Internet Protocol (IP)
    ipv6           Internet Protocol version 6 (IPv6)
Switch# show i_
```

2.1.4. 명령어 심볼

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

표 2-1. 명령어 구문 심볼

심볼	이름	설명
<>:	Angle brackets	■ 명령어 문법에서 하나의 변수 또는 값을 의미한다. 이렇게 표현된 파라미터는 반드시 입력을 해야 한다. ■ 예를 들어, 다음과 같은 명령어가 있을 때 `access-list <1-99> (deny|permit) address` 표준 IP access control list 번호는 <1-99> 사이의 값으로 반드시 입력해야 한다.
{}:	Braces	■ 명령어 문법에서 사용되는 파라미터 또는 값의 리스트

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

2.1.5. 명령어 라인 편집 키 및 도움말

CS3400 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. 스위치명령어 모드

CS3400 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-fa1/1)#` `Switch(config-if-vlan1)#`	■ 인터페이스의 환경 설정을 변경
Router 모드	`Switch(config-rip)#` `Switch(config-ospf)#`	■ RIP 이나 OSPF 등의 라우팅 프로토콜의 환경 설정을 변경

Notice 명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 CS3400 Series 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 CS3400 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 모드 진입 시 password 설정 가능
`disable`	■ Privileged 모드에서 User 모드로 이동
`configure terminal`	■ Privileged 모드에서 Config 모드로 이동
`interface` *`ifname`*	■ Config 모드에서 Interface 모드로 이동
`Router {rip|ospf}`	■ Config 모드에서 Router 모드로 이동
`exit`	■ 이전의 모드로 이동
`end`	■ User 모드를 제외한 모든 모드에서 Privileged 모드로 이동

2.3. CS3400 Series 스위치가동

CS3400 Series 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS 이미지를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.

Notice CS3400 Series 스위치는 시스템 안정성을 위하여 Primary 및 Secondary 등 두 개의 OS 이미지를 관리한다. 기본적으로 Primary OS 이미지가 로드되도록 설정되어 있으며, 운영자는 스위치의 boot 모드 또는 privileged 모드에서 이를 변경할 수 있다.

2.4. 사용자 인터페이스

시스템 운영자는 스위치의 환경을 설정 및 검증하고 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속할 수 있다. 스위치에 접속하기 위한 가장 기본적인 방법은 CS3400 Series 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것이다(*Out-of-band management*).
스위치로 연결하는 또 다른 방법은 원격지에서 텔넷 프로그램을 이용하는 것이다. 원격지에서 텔넷 연결을 위한 별도의 포트를 지원하지는 않고 서비스 포트를 통하여 접속하도록 한다(*In-band management*).

운영자는 아래의 방법을 사용하여 CS3400 Series 스위치를 관리할 수 있다.

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

CS3400 Series 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결 가능
- 최대 32 개의 텔넷 연결 가능

> **Notice** 단, 한정된 시스템 자원에 의해 텔넷 연결이 최대 32 개에 도달하기 전에 제한 될 수 있다.

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 CS3400 Series 스위치의 경우 후면의 SGIM(Switching, Gigabit ethernet I/O & Management Module) 모듈에 탑재된다.

>과 같이 CS3400 Series 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

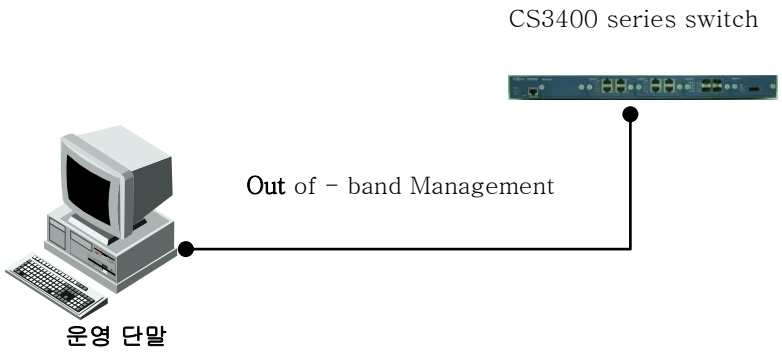


그림 2-1. CS3400 Series 스위치와 운영 단말 연결

> **Notice** 운용 단말의 설정 방법 및 콘솔 포트 핀 설정은 CS3400 Series 스위치 하드웨어 설치 가이드를 참조하기 바란다.

2.4.2. 텔넷 연결

시스템 운영자는 TCP/IP 및 텔넷 접속 기능이 있는 워크스테이션을 통하여 CS3400 Series 스위치에 접속할 수 있다. 운영자는 텔넷 접속에 필요한 ID 및 패스워드를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 한다.

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

텔넷 접속이 성공한 경우 사용자 ID 입력을 요청하는 프롬프트가 화면에 나타난다. 스위치에 설정되어 있는 유효한 사용자 ID 와 패스워드를 입력하여 인증에 성공한 경우 User 모드로 진입할 수 있다.

텔넷 접속 시에 시스템 보안을 위하여 액세스 리스트를 사용하여 텔넷에 접속하는 사용자를 제한할 수 있다. 자세한 정보는 <2.10 ACL(Access Control List)>절을 참조하라.

2.4.3. SNMP(Simple Network Management Protocol)를 통한 연결

네트워크 관리자는 SNMP(Simple Network Management Protocol)를 이용하여 CS3400 Series 스위치의 인터페이스, 환경, 설정 정보 등을 관리할 수 있다. SNMP 에 대한 자세한 정보는 <2.9. SNMP(Simple Network Management Protocol)>절을 참조하라.

2.5. 사용자 관리

2.5.1. 사용자 등록 및 삭제 설정

시스템 운영자는 콘솔 포트나 텔넷을 통해 시스템에 접속할 수 있으며, 사용자 ID 및 패스워드를 설정하여 시스템에 접속 가능한 사용자를 관리를 할 수 있다.
사용자의 privilege level 은 사용자의 권한을 나타내며 privilege level 에 따라 시스템에서 실행할 수 있는 명령을 제한할 수 있다. 사용자를 추가할 때 privilege level 을 설정할 수 있으며 기본 값은 1 로 설정된다. Privilege level 이 1 이상인 사용자는 user 모드 명령을 실행할 수 있으며, user 모드에서 “enable” 명령을 수행하면 privileged 모드로 진입할 수 있다. Privileged 모드로 진입한 사용자의 privilege level 은 15 로 변경된다. 시스템 운영자는 “enable” 명령을 수행할 때 패스워드를 입력하도록 설정하여 privileged 모드로 진입할 수 있는 사용자를 제한할 수 있다.

다음은 각 privilege level 에 대한 설명이다.

- Privilege level 0은 *non-privileged* 상태를 나타낸다.
- Privilege level 1-14는 user 모드 명령을 수행할 수 있다.
- Privilege level 15는 privilege 모드 명령을 수행할 수 있다.

표 2-5. 사용자 등록, 삭제, 관리 명령어

명령어	설명	모드
username *name* {nopassword| password [0|7] *password*| secret [0|5] *password*}	사용자를 등록한다. ■ **nopassword**: 로그인 시 패스워드입력이 요구되지 않는다. ■ **password or secret**: 로그인 시 패스워드입력이 요구되며 password 와 secret 은 암호화 방식에 따라 구분된다. 0 – 암호화 하지 않음. 5 – MD5 암호화 7 – DES 암호화	Config
no username *name*	등록된 사용자를 삭제한다. 사용자가 root 인 경우 패스워드는 초기화 값으로 변경된다.	Config
username *name* privilege <0-15>	사용자의 privilege level 을 변경한다.	Config
username *name* access-class *<1-99>*	사용자에 대해 access-list 를 적용한다. ■ <1-99> : IP standard access list	Config
no username *name* access-class	사용자에 적용된 access-list 를 해제한다.	Config
username *name* user-maxlinks *value*	해당 사용자로 접속 가능한 최대 session 수를 설정한다.	Config
no username *name* user-maxlinks *value*	해당 사용자로 접속 가능한 최대 session 수를 초기화 값으로 변경한다. ■ Default: 32 개	Config
username *name* unlimited-session-ip *A.B.C.D*	Session 접속 수를 제한 받지 않는 사용자 및 IP 주소를 설정한다.	Config
no username *name* unlimited-session-ip	Session 접속 수를 제한 받지 않는 사용자 설정을 해제한다.	Config

2.5.1.1. 사용자 추가

아래 예제는 사용자 등록 및 사용자의 패스워드와 privilege level 을 설정한다. ‘testuser1’ 사용자는 로그인 시 패스워드 입력 프롬프트가 출력되지 않으며 시스템에 접속할 수 있다. ‘testuser2’와 ‘testuser3’ 사용자는 로그인 시 설정한 패스워드를 입력함으로써 시스템에 접속 가능하며, enable 명령을 통해 privileged 모드로 진입할 수 있다.

```
Switch# configure terminal
Switch# configure terminal
Switch(config)# username testuser1 nopassword
Switch(config)# username testuser2 password testpw
Switch(config)# username testuser3 privilege 15 password testpw
```

```
Switch(config)# end
Switch # show running-config
!
username testuser1 nopassword
username testuser2 password 0 testpw
username testuser3 privilege 15 password 0 testpw
!
Switch#
```

아래는 privilege level 이 15 인 **'testuser3'**가 로그인하여 privileged 모드로 진입하는 경우이다.

```
Ubiquoss L3 Switch

Switch login: testuser3
Password: testuser3

Hello.

Switch> enable
Switch#
```

Notice aaa authorization exec 명령이 설정되어 있고, privilege level 이 15 이상인 사용자의 경우 로그인 후 user 모드가 아닌 privileged 모드로 진입한다.

2.5.2. 패스워드 설정

CS3400 series 스위치는 시스템 보안을 위해 사용자 및 enable 패스워드를 설정할 수 있다. 사용자 패스워드 설정은 <2.10 ACL(Access Control List)>를 참고하라.

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

표 2-6. Enable 패스워드 설정 명령

명령어	설명	모드
enable password {password [0|7] *password*| secret [0|5] *password*}	Privileged 모드로 진입하기 위한 패스워드를 설정한다. ■ **password or secret**: Privileged 모드 진입 시 패스워드 입력이 요구되며 password 와 secret 은 암호화 방식에 따라 구분된다. 0 – 암호화 하지 않음. 5 – MD5 암호화	Config

	7 – DES 암호화	
no enable password	Privileged 모드로 진입하기 위한 패스워드 설정을 해제한다.	Config

2.5.2.1. Enable password 설정

Privileged 모드로 진입할 때 패스워드를 입력하도록 설정한다.

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

아래와 같이 설정한 패스워드를 입력하면 privileged 모드로 진입할 수 있다.

```
Ubiquoss L3 Switch

Switch login: root
Password:

Hello.

Switch>enable
Password: testpw
Switch#
```

CS3400 series 스위치는 암호화하지 않은 패스워드를 설정한 경우 `show running-config` 명령으로 설정한 패스워드를 볼 수 있는 문제를 방지하기 위해서 패스워드 암호화 모드를 지원한다. 패스워드 암호화 모드는 service password-encryption 명령으로 설정할 수 있다.

표 2-7. 패스워드 암호화 모드 설정 명령

. 명령어	설명	모드
service password-encryption	시스템에 설정된 패스워드가 암호화되어 보여지도록 패스워드 암호화 모드를 설정한다.	Config
no service password-encryption	패스워드가 암호화 모드를 해제한다.	Config

Notice “**no service password-encryption**” 명령은 보안을 위해 기존에 암호화된 패스워드를 암호화 되기 전의 문자열로 되돌리지는 않는다. 암호화 모드를 해제한 이후에 설정되는 패스워드만 암호화 하지 않도록 설정한다.

2.5.2.2. 패스워드 암호화 모드 설정

패스워드 암호화 모드를 설정하면 기존에 추가되었던 패스워드가 암호화되어 출력된다.

```
Switch# configure terminal
```

```
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJIgc
username testuser1 nopassword
username testuser2 password 7 XX1LtbDbOY4
username testuser3 privilege 15 password 7 XX1LtbDbOY4
!
Switch#
```

2.6. AAA (Authentication, Authorization, Accounting)

2.6.1. 인증 (Authentication)

시스템 보안을 위해 시스템에 접속하는 사용자에 대한 인증이 필요하다. CS3400 series 스위치는 로그 인을 시도하는 사용자에 대한 인증과 privileged 모드로 진입할 때 enable 패스워드에 대한 인증을 수행한다.
다음은 CS3400 series 스위치에서 제공하는 인증 방법으로 Local 시스템의 사용자 정보를 통한 인증과 인증 프로토콜인 RADIUS 및 TACACS+를 통한 인증 방법을 제공한다.

- Local
- RADIUS
- TACACS+

위와 같은 인증 방법은 한 가지 이상 설정될 수 있으며 여러 인증 방법을 설정했을 경우 설정한 순서대로 인증을 시도하게 된다. 사용자는 인증에 대한 성공 또는 실패에 대한 결과를 얻지 못하는 경우에 다른 인증 방법으로 인증을 시도할 수 있도록 여러 인증 방법을 설정해야 한다. Local 시스템으로 인증을 시도하는 경우 로그 인 또는 privileged 모드로 진입하기를 원하는 사용자에 대한 정보가 local 시스템에 없다면 local 인증 방법 다음으로 설정된 인증 방법으로 인증을 시도한다. 마찬가지로 RADIUS 또는 TACACS+ 서버로 인증을 시도하는 경우 해당 서버와 시스템이 연결되지 않는 경우 또는 서버에 사용자에 대한 정보가 없는 경우 등으로 인해 인증 결과를 수신하지 못했다면 다음으로 설정된 인증 방법으로 인증을 시도하게 된다.
Local 인증은 항상 활성화된 상태이며 인증 설정을 명시하지 않은 경우 기본적으로 Local 인증 방법으로 사용자 인증을 수행한다.

2.6.2. 사용자 인증

시스템에 접속하기 위해 로그 인하는 사용자에 대해 사용자 이름과 패스워드로 인증을 시도한다.

Local 시스템의 사용자 정보 또는 RADIUS 및 TACACS+ 서버를 통한 인증이 가능하며 local 시스템을 통해 인증하기 위해서는 먼저 사용자를 등록해야 한다. Local 시스템의 사용자 등록은 <2.5.1 사용자 등록 및 삭제 설정>를 참조하라.

표 2-8. 사용자 인증 설정 명령어

명령어	설명	모드
`aaa authentication login default {local|radius|tacacs+}`	로그인 시 입력된 사용자 이름 및 패스워드에 인증한다.	Config
`no aaa authentication login default`	로그인할 때의 사용자 인증 방법을 초기 값으로 변경한다. ■ Default: Local	Config
`aaa authentication login template-user` *name*	RADIUS 또는 TACACS+ 서버로 인증하는 경우 dummy 사용자를 지정할 수 있다. Dummy 사용자는 local 시스템에 등록되어 있어야 한다.	Config
`no aaa authentication login template-user`	Dummy 사용자 지정을 해제한다.	Config
`aaa authentication login authen-type (chap|pap)`	TACACS+ 서버로 인증하는 경우 인증메시지를 chap 또는 pap 방식으로 전송한다. ■ Default: Ascii	Config
`no aaa authentication login authen-type`	TACACS+ 서버로 인증하는 경우 인증메시지를 ascii 방식으로 전송한다.	Config

2.6.2.1. 사용자 인증 설정

아래의 예제에서 사용자가 로그 인을 시도하는 경우 먼저 TACACS+ 서버로 인증을 시도하며 TACACS+ 서버에서 응답을 받지 못한 경우 RADIUS 서버로 인증을 시도한다. 마찬가지로 RADIUS 서버에서 응답을 받지 못한 경우 디폴트로 제공하는 local 방식을 통해 인증을 시도한다.

```
Switch# configure terminal
Switch(config)# aaa authentication login default tacacs+ radius
Switch(config)# end
Switch#
```

2.6.3. Enable password 인증

사용자가 privileged 모드로 진입을 원할 때 enable 패스워드로 인증할 수 있다. Local 로 인증하는 경우 시스템에 설정한 enable 패스워드를 통해 인증을 수행하며, RADIUS 또는 TACACS+ 서버를 통해 인증을 수행할 수도 있다. Local 로 인증할 때 local 시스템에 enable 패스워드가 설정되지 않은 경우 인증은 항상 성공하게 되므로 privileged 모드로 인증을 수행하기 위해서는 적절한 enable 패스워드를 설정해야 한다. Local 시스템의 enable 패스워드 설정은 <2.5.2 패스워드 설정>을 참조하라.

표 2-9. Privileged 모드 사용자 인증 설정 명령어

명령어	설명	모드
`aaa authentication enable default {enable|radius|tacacs+}`	사용자가 privileged 모드로 진입할 때 enable 패스워드에 대해 인증한다.	Config
`no aaa authentication enable default`	Enable 패스워드에 대한 인증 방법을 초기값으로 변경한다. ■ Default: enable 패스워드(Local 시스템)	Config

2.6.3.1. privileged 모드 사용자 인증 설정

아래의 예제에서 사용자가 privileged 모드로 진입을 원하는 경우 enable 패스워드에 대해 먼저 TACACS+ 서버로 인증을 시도한다. TACACS+ 서버에서 응답을 받지 못한 경우 RADIUS 서버로 인증을 시도한다. 마찬가지로 RADIUS 서버에서 응답을 받지 못한 경우 디폴트로 제공하는 local 방식을 통해 인증을 시도한다.

```
Switch# configure terminal
Switch(config)# aaa authentication enable default tacacs+ radius
Switch(config)# end
Switch#
```

2.6.4. 권한 (Authorization)

CS3400 series 스위치는 privilege level 을 통해 시스템 자원을 사용할 수 있는 권한을 검사할 수 있다. EXEC shell 을 실행할 때 사용자의 privilege level 과 local 시스템 또는 원격 서버(RADIUS 또는 TACACS+)에 설정한 사용자의 privilege level 을 비교한다. 시스템 자원을 사용하고자 하는 사용자의 privilege level 이 설정한 privilege level 보다 낮은 경우 에러 메시지를 출력하며 실행에 실패하게 된다. 또한 특정 명령을 실행할 때 각 명령의 privilege level 과 설정한 privilege level 을 비교하여 해당 명령의 실행 권한을 local 시스템 또는 원격 서버(TACACS+)을 통해 검사할 수 있다.
인증 서버로 접속이 되지 않거나 인증 서버로부터 결과를 수신하지 못하는 경우를 대비해서 항상 local 시스템을 통한 권한 검사 방법을 추가해야 한다. Local 시스템 권한 검사마저 없는 경우 권한 검사는 항상 실패하게 되며, 이 경우 콘솔을 통한 설정 변경이 필요하다. 콘솔을 통해 시스템에 로그 인한 사용자는 권한을 검사하지 않는다.

2.6.5. EXEC 실행 권한

EXEC shell 은 privileged 모드로 진입할 때 실행되는 사용자 정의 쉘이다. EXEC shell 을 실행할 수 있는 권한은 기본적으로 시스템에 등록되어 있는 사용자의 privilege level 로 확인한다. Local 시스템에 등록된 사용자의 privilege level 변경은 <2.5.1. 사용자 추가 및 삭제>를 참조하라. 만약 사용자의 EXEC shell 실행 권한을 local 시스템이 아닌 RADIUS 또는 TACACS+ 서버로 확인할 경우 해당 서버에 권한을 검사할 사용자의 privilege 정보가 설정되어 있어야 한다.

표 2-10. EXEC shell 실행 권한 설정 명령어

명령어	설명	모드
aaa authorization exec default [local|*radius*|*tacacs+*]	EXEC shell 을 실행할 권한을 local 시스템 또는 RADIUS 및 TACACS+ 서버에 설정한 사용자의 privilege level 을 참조하여 검사한다.	Config
no aaa authorization exec default	EXEC shell 을 실행할 권한을 검사하지 않는다.	Config

2.6.5.1. EXEC shell 실행 권한을 TACACS+ 서버로 검사하도록 설정

아래의 예제는 사용자가 EXEC shell 을 실행시킬 때 TACACS+ 서버에 설정된 사용자의 privilege level 을 참조하여 권한을 검사한다. 또한 TACACS+ 서버로부터 결과를 수신한지 못한 경우 local 시스템으로부터 권한을 검사할 수 있다.

```
Switch# configure terminal
Switch(config)# aaa authorization exec default tacacs+ local
Switch(config)#
Switch#
```

TACACS+ 서버에 '**testuser1**` 사용자가 등록되어 있고 privilege level 이 15 로 설정되어 있는 경우 아래와 같이 로그인 후 EXEC shell 을 실행시킬 수 있다. 이 경우 privilege level 이 15 이상이므로 privileged 모드로 바로 진입할 수 있다.

```
Switch login: testuser1
Password: testuser1

Hello.

Switch#
```

2.6.6. 명령 실행 권한

특정 명령을 실행할 때 명령에 주어진 privilege level 로 명령 실행 권한을 검사할 수 있다. 기본적으로 각 명령의 privilege level 은 명령이 실행되는 모드의 privilege level 을 가지며 설정을 통해 변경이 가능하다. Privilege level 변경은 <2.6.4 Privilege level 설정>를 참조하라.

CS3400 series 스위치는 local 시스템 또는 TACACS+ 서버를 이용해 특정 명령의 실행 권한을 검사할 수 있다. <표 2-11 >과 같이 명령이 실행되는 privilege level 을 지정하여 권한을 검사할 명령 집합을 설정할 수 있으며, 해당 privilege level 을 가지는 명령에 대해 local 시스템 또는 TACACS+ 서버로부터 실행 권한을 검사할 수 있다.

표 2-11. 명령어 실행 권한 설정 명령어

명령어	설명	모드
aaa authorization commands <0-15> default (local|tacacs+)	해당 privilege level 을 갖는 명령어를 실행하기 위해 local 시스템 또는 TACACS+ 서버로 권한을 검사할 수 있도록 설정한다. ■ <0-15>: privilege level	Config
no aaa authorization commands <0-15> default	해당 privilege level 을 갖는 명령어를 실행하기 위한 권한을 검사하지 않도록 설정한다. ■ <0-15>: privilege level	Config

2.6.6.1. 명령어 실행 권한을 TACACS+서버로 검사하도록 설정

아래 예제는 config 모드에서 수행하는 **interface** 명령을 실행할 때 TACACS+ 서버로 명령 실행 권한을 검사하도록 한다. **Interface** 명령을 privilege level 2 로 설정한 후 privilege level 2 에 대해 권한 검사를 수행한다.

```
Switch# configure terminal
Switch(config)# privilege config level 2 interface
Switch(config)# aaa authorization commands 2 default tacacs+
Switch(config)# end
Switch#
Switch# show command privilege
COMMAND-MODE         LEVEL    Command
=========================================
config               2        interface
Switch#
```

Interface 명령을 실행했을 때 실행 권한이 없는 경우 아래와 같은 에러가 발생한다.

```
Switch (config)# interface Vlan 1
% Command authorization failed
Switch (config)#
```

2.6.7. 계정(Accounting)

CS3400 series 스위치는 AAA 의 계정 기능을 통해 세션 접속 및 명령 실행 내역을 TACACS+ 서버를 통해 관리할 수 있다.

2.6.8. 세션 접속 관리

시스템에 접속한 내역을 TACACS+ 서버에 기록한다.

표 2-12. 세션 접속 관리 설정 명령어

명령어	설명	모드
aaa accounting exec default	시스템 접속 내역을 TACACS+ 서버로 전송	Config

(start-stop|stop-only) tacacs+	한다. ■ start-stop: 세션 시작과 끝을 모두 기록 ■ stop-only: 세션 끝만 기록.	
no aaa accounting exec default	시스템 접속 내역을 TACACS+ 서버로 전송하지 않는다.	Config

2.6.8.1. 세션 접속 내역을 TACACS+ 서버로 전송하도록 설정

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

2.6.9. 명령 실행 내역 관리

특정 명령을 실행할 때 TACACS+ 서버로 실행 내역을 관리할 수 있다. <표 13> 과 같이 privilege level 을 지정하여 실행 내역을 TACACS+ 서버로 전송할 명령 집합을 설정할 수 있다. 기본적으로 각 명령의 privilege level 은 명령이 실행되는 모드의 privilege level 을 가지며 설정을 통해 변경이 가능하다. Privilege level 변경은 <2.6.4 Privilege level 설정>를 참조하라.

표 2-13. 명령어 실행 내역 설정 명령어

명령어	설명	모드
aaa accounting commands <0-15> default tacacs+	해당 privilege level 을 갖는 명령의 실행 내역을 TACACS+ 서버에 기록한다. ■ <0-15>: privilege level.	Config
no aaa accounting commands <0-15> default	해당 privilege level 을 갖는 명령의 실행 내역을 TACACS+ 서버에 기록하지 않는다. ■ <0-15>: privilege level.	Config

2.6.9.1. 명령어 실행 내역을 TACACS+ 서버로 관리하도록 설정

아래 예제는 EXEC 모드에서 수행하는 모든 **show** 명령의 privilege level 을 15 로 변경하고 실행 내역을 TACACS+ 서버로 전송하도록 한다. 또한 기본적으로 privilege level 을 15 로 가지는 모든 명령들도 실행 내역을 TACACS+ 서버로 전송한다.

```
Switch# configure terminal
Switch(config)# privilege exec level 15 show
Switch(config)# aaa accounting commands 15 default tacacs+
Switch(config)# end
Switch#
Switch# show command privilege
COMMAND-MODE         LEVEL    Command
=========================================
config               15       show
```

```
Switch#
```

2.6.10. Privilege level 설정

CS3400 series 스위치는 privilege level 을 통해 특정 명령에 대한 권한(Authorization) 및 계정(Accounting) 기능을 수행할 수 있다. 특정 명령에 대해 privilege level 을 설정하지 않는 경우 각 명령은 실행되는 모드의 privilege level 을 기본값으로 참조한다.

표 2-14. Privilege level 설정 명령어

명령어	설명	모드
`privilege` *`node`* `level <0-15>` *`command`*	특정 명령에 대해 privilege level 을 부여한다. ■ *node*: 설정할 명령이 실행되는 node ■ <0-15>: privilege level ■ *command*: privilege level 을 부여할 명령	Config
`no privilege` *`node`* `level <0-15>` *`command`*	특정 명령에 대한 privilege level 을 초기값으로 변경한다. ■ Default: 명령이 실행되는 모드의 privilege level	Config
`show command privilege`	설정한 명령들의 privilege level 을 확인할 수 있다.	Privileged

2.7. 서버 설정

CS3400 series 스위치는 RADIUS 또는 TACACS+의 원격 서버를 통한 인증, 권한, 계정 관리 기능을 제공한다. 다음은 RADIUS 와 TACACS+ 서버의 설정 방법이다.

2.7.1. RADIUS 서버 설정

표 2-15. RADIUS 서버 설정 명령어

명령어	설명	모드
`radius-server host` *`A.B.C.D`* `[key [0|7]` *`key-string`*`]`	RADIUS 서버를 설정한다. ■ *A.B.C.D*: RADIUS 서버의 주소 ■ key: 서버에서 사용할 암호 키를 설정한다. 0 – 암호화 하지 않음. 7 – DES 암호화	Config

`no radius-server host` *`A.B.C.D`*	설정된 RADIUS 서버를 삭제한다. ■ *A.B.C.D*: RADIUS 서버의 주소	Config
`radius-server host` *`A.B.C.D`* `[auth-port` *`PORT`*`]`	RADIUS 서버를 설정하며, 서버에서 사용할 auth-port 를 설정한다. ■ *A.B.C.D*: RADIUS 서버의 주소 ■ *PORT*: auth-port 번호	Config
`no radius-server host` *`A.B.C.D`* `auth-port` *`PORT`*	서버에서 사용할 auth-port 를 기본값으로 설정한다. ■ Default: 1812	Config
`radius-server key [0|7]` *`key-string`*	RADIUS 서버에 접속할 때 사용하는 공통 암호 키를 설정한다. Key 가 명시되지 않은 서버는 공통 암호 키를 사용하게 된다.	Config
`no radius-server key`	공통 암호 키를 삭제한다.	Config
`radius-server retransmit` *`count`*	RADIUS 서버로 AAA 정보를 재전송하는 횟수를 설정한다. ■ *count*: 재전송 횟수를 설정	Config
`no radius-server retransmit`	재전송 횟수를 기본값으로 설정한다. ■ Default: 3 회	Config
`radius-server timeout` *`seconds`*	RADIUS 서버로부터 응답을 기다리는 시간을 설정한다. ■ *seconds*: Timeout 시간을 초 단위로 설정	Config
`no radius-server timeout`	응답을 기다리는 시간을 기본값으로 설정한다. ■ Default: 5 초	Config
`ip radius source-interface` *`ifname`*	RADIUS 서버로 전송할 정보의 source IP 주소를 설정한다. ■ *ifname*: 인터페이스 이름 정보	Config
`no ip radius source-interface`	설정한 source IP 주소를 해제한다.	Config

RADIUS 서버 설정

아래 예제는 여러 RADIUS 서버와 공통 암호 키로 test123 을 설정하였다. 192.168.0.1/test123 으로 AAA 정보를 서버로 전송하며 응답을 수신하지 못하는 경우 다음 RADIUS 서버로 전송을 시도 한다.

```
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#
```

2.7.2. TACACS+ 서버 설정

표 2-16. TACACS+ 서버 설정 명령어

명령어	설명	모드
`tacacs-server host A.B.C.D key [0|7] key-string`	TACACS+ 서버를 설정한다. ■ *A.B.C.D*: TACACS+ 서버의 주소 ■ key: 서버에서 사용할 암호 키를 설정한다. 0 – 암호화 하지 않음. 7 – DES 암호화	Config
`no tacacs-server host A.B.C.D`	설정된 TACACS+ 서버를 삭제한다. ■ *A.B.C.D*: TACACS+ 서버의 주소	Config
`tacacs-server host A.B.C.D timeout seconds`	TACACS+ 서버로부터 응답을 기다리는 시간을 설정한다. ■ *seconds*: Timeout 시간을 초 단위로 설정	Config
`tacacs-server host A.B.C.D timeout`	응답을 기다리는 시간을 기본값으로 설정한다. ■ Default: 5 초	Config
`ip tacacs source-interface ifname`	TACACS+ 서버로 전송할 정보의 source IP 주소를 설정한다. ■ *ifname*: 인터페이스 이름 정보	Config
`no ip tacacs source-interface`	설정한 source IP 주소를 해제한다.	Config

TACACS+ 서버 설정

아래 예제는 여러 TACACS+ 서버를 설정하다. 192.168.0.1/lns 로 AAA 정보를 서버로 전송하며 응답을 수신하지 못하는 경우 다음 TACACS+ 서버로 전송을 시도 한다.

```
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#
```

2.8. Hostname 설정

Hostname 은 시스템을 구별하기 위해 사용될 수 있다. 콘솔 또는 텔넷 화면의 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있으며 CS3400 Series 스위치는 기본값으로 시스템의 모델명을 hostname 으로 사용한다.

표 2-17. Hostname 설정 명령어

명령어	설명	모드
`hostname` *`string`*	Hostname 을 변경한다.	Config
`no hostname`	Hostname 을 초기값으로 변경한다.	Config

Hostname 을 설정하는 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# hostname CS3400
CS3400(config)# end
CS3400#
CS3400# configure terminal
CS3400(config)# no hostname
Switch(config)# end
Switch#
```

2.9. SNMP (Simple Network Management Protocol)

SNMP(Simple Network Management Protocol)는 네트워크 관리자가 SNMP 에이전트가 설치된 장비를 MIB(Management Information Base)을 통해 관리할 수 있도록 한다. CS3400 series 스위치에는 SNMPv1, SNMPv2, 그리고 SNMPv3 기능을 제공하는 SNMP 에이전트가 설치되어 있다.

2.9.1. SNMP 환경 설정

다음은 SNMP 에이전트의 시스템 운영자 및 시스템 설치 위치를 지정하는 설정이다.

표 2-18. SNMP 환경 설정 명령

명령어	설명	모드
`snmp-server contact` *`string`*	시스템 운영자 정보를 입력한다.	Config

no snmp-server contact	시스템 운영자 정보를 삭제한다.	Config
snmp-server location *string*	장비가 설치된 위치 정보를 입력한다.	Config
no snmp-server location	장비가 설치된 위치 정보를 삭제한다.	Config

2.9.1.1. 시스템 운영자 정보 입력

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

2.9.1.2. 시스템 구축 위치 입력

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

2.9.2. Community 설정

네트워크 관리자는 SNMP 에이전트에 접속하여 SNMP 로 관리되는 MIB 정보를 읽거나 쓸 수 있다. SNMP 에이전트에 접속할 때 community 로 인증할 수 있으며 community 는 아래와 같은 두 가지 접속 타입을 가진다.

- Read-only community
  - 시스템에 읽기 전용으로 접속한다.
- Read-write community
  - 시스템에 읽기 및 쓰기로 접속한다.

표 2-19. SNMP Community 설정

명령어	설명	모드
snmp-server community *string* [*access-type*| view *view-name*| <1-99>]	SNMP community 를 설정한다. ■ access-type: SNMP 에이전트 접속 타입 ro: read only rw: read write ■ view: MIB 접속 범위를 지정하며, 자세한 내	Config

	용은 snmp-server view 설정을 참조하라. ■ <1-99>: 접속 호스트에 대해 access-list 를 적용할 수 있다.	
no snmp-server community *string*	SNMP community 를 삭제한다.	Config

2.9.2.1. SNMP Community 설정

아래 예제는 read-write 접속 타입의 **'testcom'** community 를 설정한다. 또한 **'testcom'**으로 접속하는 호스트는 access-list 99 를 참조하여 SNMP 를 통한 접속이 permit 또는 drop 될 수 있다.

```
Switch# configure terminal
Switch(config)# snmp-server community testcom rw 99
Switch(config)# end
Switch# show running-config
!
snmp-server community testcom rw access-class 99
!
Switch#
```

2.9.3. Trap host 설정

시스템에서 발생하는 오류 동작 또는 시스템 상태 변경 등의 이벤트는 네트워크 관리자에게 트랩(trap)을 통해 제공될 수 있다. CS3400 series 스위치는 아래와 같은 버전의 트랩을 제공하며, 기본적으로 트랩 호스트 및 "snmp-server enable traps" 명령으로 트랩을 전송하도록 설정하지 않았다면 트랩은 발생하지 않는다.

- **SNMPv1 Trap**
- **SNMPv2c Trap**
  - 기본적으로 전송되는 트랩 버전이다.
- **SNMPv3 Trap**
  - 인증 및 암호 기능을 제공하며, security model 을 설정할 수 있다.
    1) noAuth: 인증 및 암호화를 수행하지 않음.
    2) Auth: 인증 수행
    3) Priv: 인증 및 암호화를 수행함.

표 2-20. SNMP Trap 호스트 설정

명령어	설명	모드
snmp-server trap-host *A.B.C.D* [version 1|2c|3 *sec-level*] *community-string*	트랩을 전송할 호스트를 설정한다. ■ *A.B.C.D*: 트랩 호스트 주소 ■ version: 전송할 트랩의 버전	Config

	(Default: 2c) ■ *sec-level*: 트랩 버전이 3 인 경우 security model 을 설정 ■ *community-string*: community 설정	
no snmp-server trap-host *A.B.C.D* [version 1|2c|3 *sec-level*] *community-string*	설정한 트랩 호스트를 삭제한다.	Config
snmp-server trap-source *ifname*	전송할 트랩의 source IP 주소를 설정한다. ■ *ifname*: 인터페이스 이름 정보	Config
no snmp-server trap-source	설정한 source IP 주소를 해제한다.	Config

표 2-21. SNMP 기본 트랩의 Enable 설정

명령어	설명	모드
(no) snmp-server enable traps alarm [fallingAlarm| risingAlarm]	RMON alarm 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps auto-negotiation	Auto negotiation 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps cfm [pm-event|remote-mep-state]	CFM 관련 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps envmon [ext-supply|fan|supply| temperature]	시스템 환경(fan, power 등) 관련 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps erps [state-change] (no) snmp-server enable traps erps state-change [east-if-state-change|ring-state-change|west-if-state-change]	ERPS 관련 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps fru-ctrl	모듈, slot 등 실/탈장 가능한 unit 의 상태 변경 시 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps interface	Linkup, linkdown 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps port-monitor [crc|drop|error|input-load-monitor|output-load-monitor]	Port 모니터링 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps resource [cpu-load-monitor|	시스템 자원 관련 트랩을 전송하도록 설정한다.	Config

memory-free-monitor]		
(no) snmp-server enable traps snmp [coldStart|warmStart|authFail]	Cold start, warm start, authentication failure 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps vlancreate	Vlan 생성 시 트랩을 전송하도록 설정 또는 해제한다.	Config
(no) snmp-server enable traps vlandelete	Vlan 삭제 시 트랩을 전송하도록 설정 또는 해제한다.	Config

Notice <표 21. SNMP 기본 트랩 및 Enable 설정> 은 CS3400 series 스위치에서 기본적으로 제공하는 트랩의 전송 설정 및 해제 명령을 나타내며 추후에 추가 및 삭제될 수 있다.

2.9.3.1. SNMP Trap 설정

다음 예제는 192.168.0.1 호스트로 팬, 파워, 온도 등의 환경 관련 트랩 및 linkup/linkdown 트랩이 전송되도록 설정한다. 트랩 버전은 기본값인 2c 로 전송된다.

```
Switch# configure terminal
Switch(config)# snmp-server host 192.168.0.1 public
Switch(config)# snmp-server enable traps envmon
Switch(config)# snmp-server enable traps snmp
Switch#(config)# end
Switch# show running-config
!
snmp-server enable traps interface
snmp-server enable traps envmon fan supply temperature ext-supply
snmp-server host 192.168.0.1 version 2c public
!
Switch#
```

2.9.4. SNMPv3 설정

CS3400 series 스위치는 SNMP 를 통한 시스템 관리에서 더 나은 보완 기능을 제공하기 위해 SNMPv3 를 제공한다. SNMPv3 는 사용자에 대한 인증 및 데이터에 대한 암호화 기능을 제공한다.

표 2-22. SNMPv3 설정

명령어	설명	모드
snmp-server engineID *engineid-string*	SNMP 에이전트를 유일하게 구분하기 위한 engine ID 를 설정한다. SNMP engineID 를 변경하는 경우 기존에 설정한 user 를 다시 설정해야 한다. User 설정은 engine ID 를 이용해 MD5 및 SHA 의 security	Config

	digest 를 생성하기 때문이다.	
`no snmp-server engineID`	Engine ID 를 자동으로 생성되는 기본값으로 설정한다. 기본 값은 자사의 enterprise OID(1.3.6.1.4.1.7800)와 시스템의 첫 번째 MAC 주소로 자동 생성한다.	Config
`show snmp engineID`	Engine ID 를 출력한다.	Privileged
`snmp-server group` *`groupname`* `{v1|v2c|v3` *`sec-level`*`}` `[read` *`read-view`*`|` `write` *`write-view`*`]`	SNMP group 을 설정한다. ■ *group-name*: Group 이름 ■ v1, v2c, v3: Group 버전 ■ *`sec-level`*: 트랩 버전이 3 인 경우 security model 을 설정 ■ read: Read view 설정. Read-view 가 명시되지 않은 경우 기본값으로 **internet** (1.3.6.1)로 설정됨. ■ write: Write view 설정	Config
`no snmp-server group` *`groupname`* `{v1|v2c|v3` *`sec-level`*`}`	SNMP group 을 삭제한다	Config
`show snmp group`	SNMP group 을 출력한다.	Privileged
`snmp-server user` *`username groupname`* `{v1|v2c|v3` `[auth (md5|sha)` *`auth-passwd`*`]` `[priv (des|aes)` *`priv-passwd`*`]` `[access <1-99>]}`	SNMP user 를 설정한다. ■ v1, v2c, v3: User 버전 ■ auth: SNMPv3 인 경우 사용자 인증을 수행할 수 있으며 암호화 방법으로 MD5 또는 SHA 를 설정할 수 있다. *auth-passwd*: 인증을 위한 암호 설정 ■ priv: SNMP PDU 를 암호화할 수 있으며 암호화 방법으로 DES 또는 AES 를 설정할 수 있다. *priv-passwd*: 암호화를 위한 암호 설정 ■ `access`: 사용자에 대해 access-list 를 적용한다. <1-99> : IP standard access list	Config
`no snmp-server user` *`username groupname`* `{v1|v2c|v3}`	SNMP user 를 삭제한다.	Config
`show snmp user`	SNMP user 를 출력한다.	Privileged
`snmp-server view` *`viewname viewoid`* `{excluded|included}`	SNMP view 를 설정한다. ■ *viewoid*: User 또는 community 로 읽기/쓰기 기능을 수행할 수 있는 MIB 의 범위를 지정하며 MIB 이름 또는 OID 로 지정 가능. ■ `excluded` 또는 `included`: *viewoid* 를	Config

	포함하거나 제외하도록 설정	
`no snmp-server view viewname viewoid`	SNMP view 를 삭제한다.	Config

2.9.4.1. SNMP engineID 변경

다음 예제는 시스템의 SNMP engine ID 를 변경한다. 기존에 SNMPv3 사용자가 설정되어 있었다면 engine ID 를 변경한 후 다시 설정해야 네트워크 관리자가 해당 사용자로 접속할 수 있다.

```
Switch# show snmp engineID
Local SNMP engineID: 0x80001f8880236ed0864b7a760f
Switch#configure terminal
Switch(config)# snmp-server engineID 0x1234567890
Switch(config)# exit
Switch#
Switch# show snmp engineID
Local SNMP engineID: 0x1234567890
Switch#
```

2.9.4.2. SNMPv3 사용자 설정

다음 예제는 인증과 암호화를 수행하는 **'testuser'** 사용자를 생성한다. **'testuser'**는 **'testgroup'**에 포함되며 ifEntry(1.3.6.1.2.1.2.2.1)를 읽거나 쓸 수 없는 **'testview'**를 적용한다.

```
Switch# configure terminal
Switch(config)# snmp-server user testuser testgroup v3 auth md5 mysecretpass
priv des myprivpass
Switch(config)# snmp-server group testgroup v3 priv read testview write
testview
Switch(config)# snmp-server view testview 1.3.6.1 included
Switch(config)# snmp-server view testview 1.3.6.1.2.1.2.2.1 excluded
Switch#(config)# end
Switch# show running-config
!
snmp-server group testgroup v3 priv read readview write writeview
snmp-server view testview 1.3.6.1 included
snmp-server view testview 1.3.6.1.2.1.2.2.1 excluded
!
Switch#
Switch# show snmp user

User name : testuser
Engine ID : 0x80001f8880236ed0864b7a760f
storage-type: nonvolatile        active
Authentication Protocol: MD5
Group-name: testgroup
```

Notice SNMPv3 의 패스워드 보완 문제로 user 설정은 "**show running-config**" 명령으로 출력되지 않는다. 위의 예제와 같이 "**show snmp user**" 명령으로 확인할 수 있다.

2.10. ACL(Access Control List)

액세스 리스트(Access Control List)를 사용함으로써 네트워크 관리자는 인터네트워크를 통해 전송되는 트래픽에 대해 상당히 세밀한 통제를 할 수 있다. 시스템 운영자는 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 스위치를 통해 전달되는 패킷을 허용하거나 거부하기 위해 사용할 수도 있고 텔넷(vty)이나 SNMP 를 통한 스위치의 접속에도 적용할 수 있다.

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

표 2-23. 액세스 리스트 설정 명령

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

2.10.1. 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.

2.10.2. 표준 IP 액세스 리스트 설정

2.10.2.1. 모든 액세스 허용

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

2.10.2.2. 모든 액세스 거부

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

2.10.2.3. 특정 호스트에서의 액세스만 허용

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

2.10.2.4. 특정 네트워크에서의 액세스만 허용

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

2.10.2.5. 특정 네트워크에서의 액세스만 거부

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

2.10.3. 텔넷 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, 텔넷 접속을 제한하고자 할 때의 절차는 다음과 같다.

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

2.11. 배너 설정

CS3400 series 스위치는 로그인 배너 및 MOTD 배너를 등록할 수 있다. 로그인 배너는 사용자가 시스템에 접속해서 로그인 하기 전에 출력되는 메시지이며, MOTD 배너는 로그인 한 후 EXEC shell 을 실행하기 전에 출력되는 메시지이다. 배너를 통해 사용자에게 주의 사항과 같은 메시지를 전달할 수 있다.

표 2-24. 로그인 배너 및 MOTD 배너 명령어

명령어	설명	모드
banner login *banner-string* **banner login default**	로그인 배너를 등록한다. ■ *banner-string*: 등록할 로그인 배너 메시지로 시작 문자에 대해 동일한 문자가 나올 때까지 로그인 배너로 지정 ■ default: 기본적으로 등록된 로그인 배너 메시지	Config
no banner login	시스템에 등록한 로그인 배너를 삭제한다.	Config
banner motd *banner-string* **banner motd default**	MOTD 배너를 등록한다. ■ *banner-string*: 등록할 MOTD 배너 메시지로 시작 문자에 대해 동일한 문자가 나올 때까지 MOTD 배너로 지정 ■ default: 기본적으로 등록된 MOTD 배너 메시지	Config
no banner motd	시스템에 등록한 MOTD 배너를 삭제한다.	Config

시스템에는 아래와 같은 로그인 배너와 MOTD 배너가 기본적으로 등록되어 있다.

```
Switch login: root
Password:

Hello.                                  <- MOTD 배너

Switch >enable
Switch #
```

다음은 로그인 배너를 변경하는 예제이다. 배너는 여러 줄로 입력이 가능하며 다만 시작 문자에 대해 동일한 종료 문자가 나타날 때까지 배너로 등록된다. 아래 예제에서는 **'.'** 문자에 대해 시작과 종료 문자로 지정하였고, **'.'** 문자 사이의 공백을 포함한 문자열을 배너로 등록한다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# banner login .
Enter TEXT message. End with the character '.'.

Ubiquoss Mobile Backhaul Switch

Login Banner TEST!

.
Switch(config)#
Switch(config)#exit
Switch#show running-config
…
!
banner login ^C

Ubiquoss Mobile Backhaul Switch

Login Banner TEST!

^C
!
…
```

Notice 'show running-config' 명령으로 등록한 배너를 확인할 때 시작 문자와 종료 문자는 **'^C'**로 지정된다.

위의 예제에서 설정한 로그인 배너는 아래와 같이 출력된다.

```
Ubiquoss Mobile Backhaul Switch

Login Banner TEST!

Switch login: root
Password:
```

```
Hello.

Switch >
```

3

인터페이스 환경 설정

3.1. 개요

CS3400 Series 스위치가 지원하는 인터페이스는 다음과 같다.

표 3-1. CS3400 Series 스위치가 지원하는 인터페이스

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

모든 인터페이스 환경 설정은 다음과 같이 진행된다.

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

3.2. 공통 명령어

인터페이스 환경 설정에 공통으로 적용되는 명령어는 다음과 같다.

표 3-2. 공통 명령어

명령어	설명
interface *IFNAME*	■ Interface 모드로 진입한다. ■ *IFNAME*: 환경을 설정할 특정 인터페이스의 이름.
description *string*	■ 인터페이스에 대한 설명을 등록한다. ■ *string*: 80 자 이내의 문자열의 인터페이스 설명
no description	■ 등록한 인터페이스 설명을 삭제한다.

3.2.1. Interface name

CS3400 Series 스위치에서는 인터페이스에 대한 모든 환경 설정에서 interface name을 사용한다. Interface name은 다음과 같이 interface type과id로 구성된다.

표 3-3. Interface name

구분	Interface type	Interface name	예
Physical interface	Gigabit Ethernet	“Gi” + slot_id + port_id	Gi1/1
	10 Gigabit Ethernet	“Te” + slot_id + port_id	Te1/1
Port-group interface	Port group	“po” + port-group id	po1
VLAN interface	VLAN	“vlan” + vlan id	Vlan10
Loopback interface	Loopback	“lo” + id	Loopback0
Management interface	Fast Ethernet	“eth” + id	eth0

3.2.2. Interface id

Interface name은interface type과id로 구성된다. 다음은 CS3400 Series 스위치의 interface name 표기 방법과 지원 범위를 나타낸다.

표 3-4. Interface ID 및 지원 범위

Model	Interface Type	ID 구성	ID Range	Name(예)
CS3400	Gigabit Ethernet	slot_id + port_id	slot_id: 1-4 port_id: 1-12	Gi1/1
	10 Gigabit Ethernet	slot_id + port_id	slot_id: 1-4 port_id: 1-2	Te1/2
	Port group	port-group id	1 – 256	po1, po30
	VLAN	vlan id	1 – 4094	Vlan1
	LoopBack	interface id	0 – 3	Loopback0
	management	interface id	0	eth0

3.2.3. Interface 모드 프롬프트

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

```
Switch (config-if-Giga1/1)#
```

3.2.4. Description 명령어

운영자의 시스템 운영에 대한 편의를 돕기 위해 각 인터페이스에 대한 설명을 등록할 수 있으며, **show interface description** 명령을 사용하여 조회할 수 있다.

3.3. 인터페이스 정보 및 상태 조회

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

표 3-5. 인터페이스 정보 및 상태 관련 명령어

명령어	설명	모드
show interface *IFNAME*	■ 인터페이스의 설정, 상태 및 통계 정보를 출력한다.	Privileged
show interface status	■ 물리적 인터페이스의 링크 상태, speed, duplex 정보 등을 출력한다.	Privileged
show interface transceiver	■ 물리적 인터페이스의 DDM (Digital	Privileged

[detail|modue <1-6>] show idprom all show idprom *fru-type* show idprom interface *IFNAME*	Diagnostic Monitoring)정보를 출력한다. ■ 시스템 FRU 정보를 출력한다. ■ all: 모든 FRU 타입 정보를 출력 ■ *fru-type*: FRU 타입 별로 정보를 출력 ■ interface *IFNAME*: 인터페이스 정보를 출력	Privileged

Notice 'show interface transceiver' 명령의 자세한 내용은 **CS3400 Series_User Guide_제 22 장_Utilities** 장의 <22.5. DDM>을 참조하라

3.3.1. show interface 명령어

인터페이스에 대한 모든 정보를 확인할 때 **show interface** 명령을 참조한다. 인터페이스의 환경 설정 정보, 링크 상태, 그리고 인터페이스 관련 통계 정보를 출력할 수 있다.

```
Switch# show interface

Giga1/1 is up, line protocol is up (connected)
  Hardware is Ethernet  Current HW addr: 0007.7023.f33a
  Physical:0007.7023.f33a  Logical:(not set)
  index 1001 metric 1 mtu 1500 arp ageing timeout 7200
  Full-duplex, A-100Mb/s, media type is 10/100/1000BaseT
  <UP,BROADCAST,RUNNING,MULTICAST>
  Bandwidth 100m
  inet 10.1.20.224/24 broadcast 10.1.20.255
  Last clearing of "show interface" counters never
  60 seconds input rate 6,568 bits/sec, 6 packets/sec
  60 seconds output rate 0 bits/sec, 0 packets/sec
  L2/L3 in Switched: ucast 159,476 pkt - mcast 847,701 pkt
  L2/L3 out Switched: ucast 127,103 pkt - mcast 0 pkt
    2,731,292 packets input, 310,768,546 bytes
    Received 1,724,115 broadcast pkt (847,701 multicast pkt)
    0 CRC, 0 oversized, 0 dropped
    127,106 packets output, 11,742,727 bytes
    0 collisions
    0 late collisions, 0 deferred
-- More --
```

3.3.2. show interface status 명령어

모든 물리적 포트의 링크 상태, vlan 정보, 현재 speed/duplex, 그리고 interface type을 출력한다.

```
Switch# show interface status

Port     Name               Status       Vlan       Duplex  Speed   Type
-------- ------------------ ------------ ---------- ------- ------- ----------------
Gi1/1                       connected    routed        full   a-100 10/100/1000BaseT
```

```
Gi1/2                     connected    routed        full   a-1000 10/100/1000BaseT
Gi1/3                     connected    1             full   a-1000 10/100/1000BaseT
Gi1/4                     connected    1             full   a-1000 10/100/1000BaseT
Gi3/1                     notconnect   routed        full     auto 10/100/1000BaseT
Gi3/2                     notconnect   routed        full     auto 10/100/1000BaseT
Gi3/3                     notconnect   routed        full     auto 10/100/1000BaseT
Gi3/4                     notconnect   routed        full     auto 10/100/1000BaseT
```

3.3.3. show idprom 명령어

show idprom 명령은 시스템의 FRU(Field Replaceable Unit) 정보를 출력한다. CS3400 series 스위치는 아래와 같은 FRU 타입에 대해 정보를 출력할 수 있다.

- Chassis
- FAN
- FMU
- Module
- Pfe
- PMU
- Power
- Slot
- Tranceiver

다음은 show idprom all 명령으로 시스템의 모든 FRU 타입에 대한 정보를 출력하는 예제이다.

```
Switch# show idprom all
IDPROM for chassis
  Name = 'UbiQuoss Evolution'
  Description = 'UbiQuoss Chassis System'
  SNMP index = '1'

IDPROM for slot 1
  Name = 'Physical Slot 1/1'
  Description = 'UbiQuoss Physical Slot 1/1'
  SNMP index = '10'

IDPROM for slot 3
  Name = 'Physical Slot 1/3'
  Description = 'UbiQuoss Physical Slot 1/3'
  SNMP index = '12'

IDPROM for pwr 2
  Name = 'Power 2'
  Description = 'Power 2'
  SNMP index = '41'

IDPROM for fmu 1
  Name = 'Container of Fan Module 1'
  Description = 'Container of Fan Module 1'
```

```
  SNMP index = '100'

IDPROM for fan 1/1
  Name = 'Fan 1/1'
  Description = 'Fan 1/1'
  SNMP index = '101'

IDPROM for fan 1/2
  Name = 'Fan 1/2'
  Description = 'Fan 1/2'
  SNMP index = '102'

IDPROM for fan 1/3
  Name = 'Fan 1/3'
  Description = 'Fan 1/3'
  SNMP index = '103'
……..
생략
```

3.4. 물리적 포트 환경 설정

다음은 물리적 포트의 환경 설정에 사용되는 명령이다.

표 3-6. 물리적 포트 환경 설정 명령어

명령어	설명	모드
shutdown no shutdown	■ 물리적 포트를 disable/enable	Interface
speed {10|100|1000} speed auto	■ Speed 설정 (단위: Mbps)	Interface
duplex {full |half}	■ Duplex 모드 설정	Interface
flowcontrol (send|receive) (on|off) flowcontrol both no flowcontrol	■ flow-control 설정 및 해제	Interface
carrier-delay <0-60> carrier-delay msec <0-1000>	■ Carrier-delay 를 sec 단위와 ms 단위로 설정	Interface

Notice Gpon interface 노드에서는 해당 명령어들이 표시되지 않는다.

3.4.1. Shutdown

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

```
Switch # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch (config)# interface GigabitEthernet 1/1
Switch (config-if-Giga1/1)# shutdown          <- disable port
Switch (config-if-Giga1/1)# no shutdown       <- enable port
Switch (config-if-Giga1/1)#
```

3.4.2. Speed and duplex

CS3400 Series 스위치의 각 인터페이스에서 지원하는 speed는 다음과 같다.

type	speed	duplex
1000Base-T	10/100/1000/auto	full/half
	1000	full
1000Base-X	1000/auto	full
	1000	full
10GBase-R	10000	full

Speed 또는 duplex를 설정할 때 다 음 사항을 주의하라.

- 10-Gigabit Ethernet 과 1000Base-X Gigabit Ethernet 은 full duplex 만 지원한다.

3.4.3. Flow control

Gigabit Ethernet, 10-Gigabitethernet interface 에 대해서 IEEE 802.3x Flow control 기능을 지원한다. Flow control 은 interface 의 receive buffer 가 가득 찼을 경우 IEEE 802.3x pause frame 을 반대편 interface 에 전송해서 일정시간 동안 패킷을 보내지 않도록 하는 것을 말한다.
다음은 interface 에 IEEE 802.3x pause frame 을 보내는 설정과 받아서 처리하는 설정을 보여주는 예시이다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga1/1
Switch(config-if-Giga1/1)# flowcontrol send on
Switch(config-if-Giga1/1)# flowcontrol receive on
Switch(config-if-Giga1/1)# end
Switch# show flowcontrol
Port     Send FlowControl     Receive FlowControl  RxPause TxPause
         admin    oper        admin    oper
```

```
-----    ------- --------     ------- --------      ------- -------
Giga1/1 on      on           on      off               307     154
Switch#
```

flowcontrol send on 명령은 IEEE 802.3x pause frame 을 보내도록 설정하는 명령이고 **flowcontrol receive on** 는 IEEE 802.3x pause frame 을 받을 경우 일정시간 동안 패킷을 보내지 않도록 설정하는 명령어다. 이러한 설정을 확인하기 위해서 **show flowcontrol (IFNAME)** 명령을 사용한다. 설정을 해제할 경우에는 **no flowcontrol** 명령을 사용한다.

3.4.4. Carrier delay

Interface 에 link up/down event 가 발생할 경우 carrier delay 설정을 통해서 설정 한 시간 보다 작은 시간 사이에 link 가 up -> down -> up 이 될 경우 down 을 인식하지 않도록 설정 할 수 있다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga1/1
Switch(config-if-Giga1/1)# carrier-delay msec 500
Switch(config-if-Giga1/1)# end
Switch#
```

설정을 해지하기 위해서는 **no carrier-delay** 명령을 사용한다.

3.5. Broadcast suppression

Broadcast suppression이란 broadcast storm으로 인한 시스템의 과부하를 방지하기 위하여 브로드캐스트 트래픽이 시스템에 유입되는 것을 제한하는 기능을 말한다. Broadcast storm은 broadcast/multicast 패킷이 서브넷에 flooding되어 과다한 트래픽으로 인한 네트워크의 성능을 저하시키는 현상을 말하며 프로토콜 스택 구현상의 오류나 네트워크 환경 설정의 오류가 이런 현상을 유발시킬 수 있다.
{OFFICIAL_PRODUCT_NAME}는input port의 packet을 양을 측정하여 이를 설정된 threshold와 비교 그 이상의 트래픽은 시스템에 유입 시키지 않고 폐기한다.

명령어	설명	모드
storm-control (broadcast|multicast|unicast)	▪ Multicast, broadcast, unicast,packet 을 suppression	Interface
storm-control level LEVEL no storm-control level	▪ broadcast suppression rate 을 설정	Interface

{OFFICIAL_PRODUCT_NAME}에서는 Broadcast suppression 을 설정하기 위해서 먼저 rate 을 설정해야 한다. 그 후 해당 트래픽에 대한 설정을 한다.
다음은 storm-control 설정에 관한 예시이다.

```
Switch # configure terminal
Switch(config)#
Switch(config)# int GigabitEthernet 1/3
```

```
Switch(config-if-Giga1/3)# storm-control level 50
Switch(config-if-Giga1/3)# storm-control broadcast
Switch(config-if-Giga1/3)# storm-control multicast
Switch# show interface counters storm-control
Port      TotalLevel % UMB UcastDiscards McastDiscards   BcastDiscards
--------- ------------ --- ------------- --------------- ---------
……
Gi1/1        0.00                  0               0               0
Gi1/2        0.00                  0               0               0
Gi1/3       50.00       **         0               0               0
Gi1/4        0.00                  0               0               0
……
Switch#
```

설정을 해지할 경우 **no storm-control** 명령을 사용한다.

3.6. Port mirroring

Port mirroring은 특정 port(source port)의 입출력 트래픽을 운용자가 설정한 목적지 포트에 mirroring하는 기능으로 원하는 포트의 모든 패킷을 감시할 수 있다. {OFFICIAL_PRODUCT_NAME}는rx, tx 트래픽을 각각 여러 소스 포트로부터1개의 port로mirroring 할 수 있다.

명령어	설명	모드
mirror interface IFNAME direction (receive|transmit|both)	■ mirroring 될 port(source port)와 입출력 패킷을 지정	Interface
no mirror interface IFNAME direction (receive|transmit)	■ mirroring 될 port 를 해지	Interface

다음은 port mirroring 에 대한 예시이다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int GigabitEthernet 1/1
Switch(config-if-Giga1/1)# mirror interface gi1/2 direction receive
Switch(config-if-Giga1/1)# mirror interface gi1/3 direction receive
Switch(config-if-Giga1/1)# mirror interface gi1/4 direction receive
Switch(config-if-Giga1/1)# end
Switch# show mirror
Mirror Test Port Name: Giga1/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga1/2
Mirror Test Port Name: Giga1/1
Mirror option: Enabled
Mirror direction: receive
```

```
Monitored Port Name: Giga1/3
Mirror Test Port Name: Giga1/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga1/4
Switch#
```

3.7. 2 계층 인터페이스 환경 설정

2계층 인터페이스는2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 CS3400 Series 스위치에서는 물리적 포트와 port-group 이 2계층 스위칭 모드로 동작한다.
이 절에서는2계층 인터페이스의 설명과 물리적 포트와 port-group을2계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여준다.

3.7.1. VLAN Trunking

트렁크(trunk)란 이더넷 스위치와 다른 네트워킹 장비(router, switch) 사이의 point-to-point 링크로서 단일 링크에 복수의 VLAN 트래픽을 전송할 수 있으며 이를 통하여 VLAN을 전체 네트워크에 확장할 수 있다.
CS3400 Series 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에trunk을 설정할 수 있다.

3.7.2. 2 계층 인터페이스 모드

CS3400 Series 스위치가 지원하는2계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있다.

표 7. CS3400 Series 스위치가 지원하는 2 계층 인터페이스 모드

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

3.7.3. 2 계층 인터페이스 기본 설정 값

CS3400 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

3.7.4. 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 해제되지만 다시 switchport 명령을 통해 2계층 인터페이스가 되면 기존의 설정들이 복원된다.

Notice CS3400 Series 스위치의 초기 설정은 모든 물리적 포트가 3 계층 인터페이스로 되어 있다.

3.7.5. Trunk port 설정

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

표 3-9. Trunk port 설정 명령어

명령어	설명	모드
switchport mode trunk	■ trunk mode 설정	Interface
switchport trunk native *<1-4094>*	■ trunk port native VLAN 설정	Interface
no switchport trunk native	■ trunk port native VLAN 을 default 로 설정	Interface
switchport trunk allowed vlan add *<2-4094>*	■ trunk port tagged VLAN 등록	Interface
switchport trunk remove *<2-4094>* switchport trunk remove all	■ trunk port tagged VLAN 삭제	Interface

다음은 물리적 포트를2계층 트렁크 포트로 설정하는 예이다.

```
Switch# configure terminal
```

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

다음은 port-group 인터페이스를2계층 트렁크 포트로 설정하는 예이다.

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

3.7.6. Access port 설정

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

표 3-10. 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 gi1/1
Switch(config-if-gi1/1)# switchport            ! layer2 interface set
Switch(config-if-gi1/1)# switchport mode access   ! access port set
Switch(config-if-gi1/1)# 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
```

Notice VLAN 에 설정에 관련된 보다 자세한 설명은 가상랜(VLAN) 매뉴얼을 참조하라.

3.8. Port group

3.8.1. Port group 개요

Port group 이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용한다. CS3400 Series 스위치에서 port group 인터페이스는2계층 인터페이스로 사용될 수 있다.

CS3400 Series 스위치의 모델 별 설정 가능한 port group 수는 다음과 같다.

모델	port group 수	그룹 당 최대 port
CS3400 Series	256	8

3.8.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같다.

표 3-11. 포트 그룹 설정 명령어

명령어	설명	모드
Channel-group <1-256> mode on	■ 해당 interface 를 Port group 에 포함시키고 Port group interface 를 생성한다.	interface
no port-group *ifname*	■ port-group 을 삭제한다	config
port-channel load-balance src-dst-mac	■ load-balance 시 MAC 주소를 참조.	config
port-channel load-balance src-dst-ip	■ load-balance 시 ip field 를 참조.	config
port-channel load-balance src-dst-port	■ load-balance 시 tcp/udp port 참조	config
no channel group	■ 해당 interface 를 Port group 에서 제외시킨다.	Interface *
no interface Channel-group <1-256>	■ 해당 Port group interface 를 삭제한다. ■ Port group 에 맴버가 없을 경우 수행된다.	config
show etherchannel	■ port group 설정 출력	Privileged

Notice Port group 에 설정에 관련된 보다 자세한 설명은 LACP 매뉴얼을 참조하라.

4

가상 랜(VLAN)

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

이 장에서는 다음의 내용들을 다룬다:

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

4.1. VLAN 개관

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

4.1.1. VLAN 정의

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

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

4.1.2. VLAN 의 장점

VLAN 을 사용하면 다음과 같은 장점이 있다:

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

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

4.2. VLAN 의 유형

CS3400 Series 스위치는 최대 4094 개의 VLAN 을 지원한다. VLAN 은 다음의 기준에 따라 생성된다:

- 물리적 포트(Physical port)
- 802.1Q 태그(tag)
- 포트기반 VLAN 과 tag 기반 VLAN 의 결합 (Hybrid)

4.2.1. 포트 기반 VLAN(Port-Based VLANs)

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

예를 들면, <**오류! 참조 원본을 찾을 수 없습니다.**>의 CS3400 스위치에서 1/1, 1/2 포트는 VLAN A 의 access 포트이고 2/1, 2/2, 3/3,3/4 포트는 VLAN B 의 access 포트로 할당된다. 그리고 1/3, 1/4, 3/1, 3/2, 4/1, 4/2 포트는 VLAN C 의 access 포트로 정의한다.

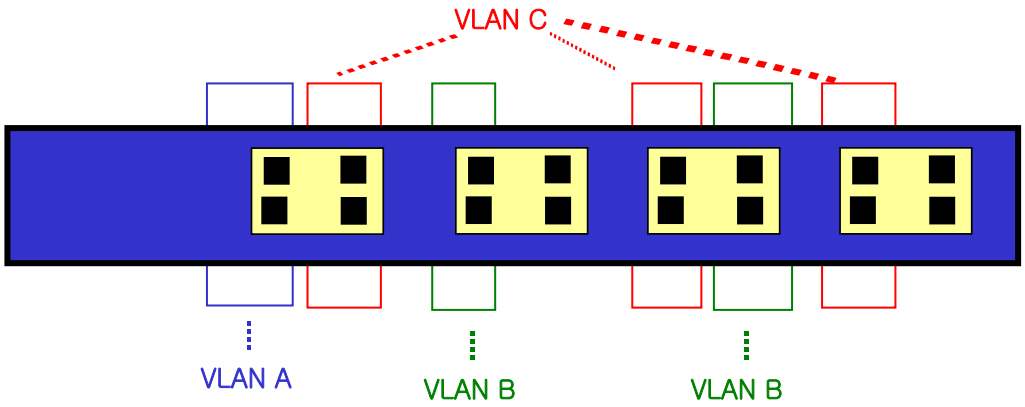


그림 4-1. CS3400 Series 스위치의 포트 기반 VLAN 구성 예

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

4.2.1.1. 포트 기반 VLAN 으로 스위치 묶기

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

7) 각 스위치에서 VLAN 에 대한 access 포트를 할당한다.

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

<그림 2>는 서로 다른 2 개의 CS3400 스위치를 하나의 VLAN 으로 묶는 방법을 보여준다. 먼저 스위치 1 의 4 개의 포트는 VLAN A 로 포함되도록 할당되어 있다. 또한 스위치 2 의 4 개 포트도 VLAN A 의 access 포트로 할당되어 있다. 두 스위치는 <그림 2>와 같이 상호 연결하여 하나의 브로드캐스트 도메인을 형성한다.

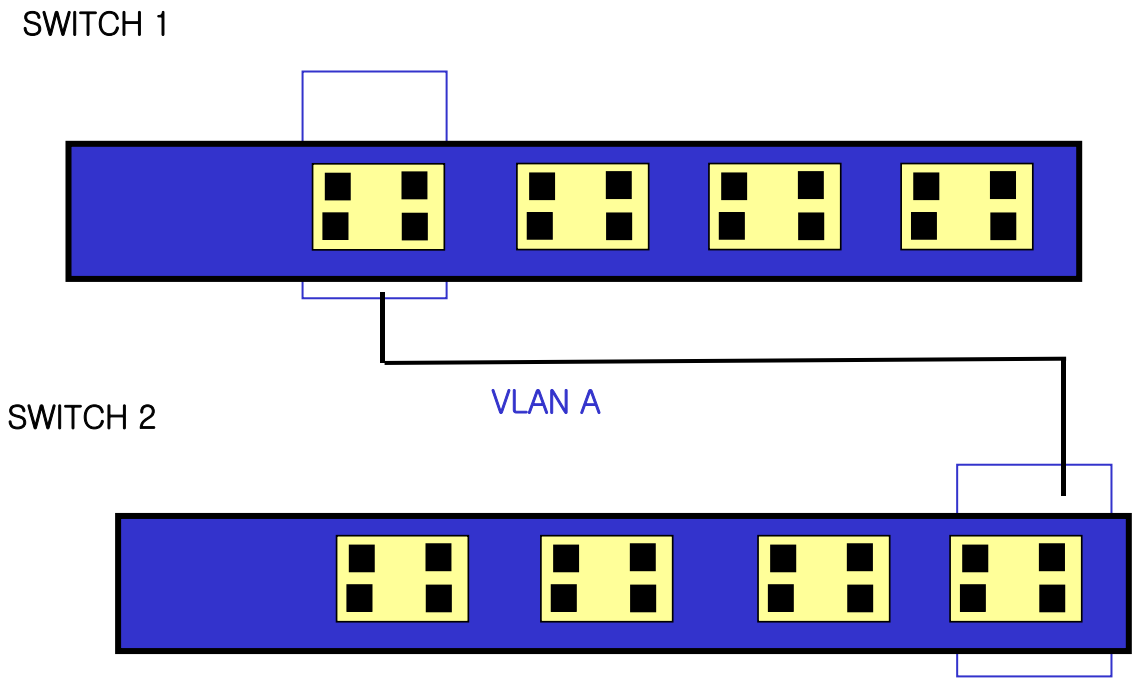


그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

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

<오류! 참조 원본을 찾을 수 없습니다.>은 두 개의 CS3400 스위치에 걸쳐서 설정되는 두 개의 VLAN 을 보여준다. 스위치 1 에서 포트 1/1, 1/2, 1/3, 1/4 포트는 VLAN A 의 access 포트이고 2/3, 2/4, 3/1, 3/2 까지의 포트는 VLAN B 의 access 포트로 할당되어 있다.

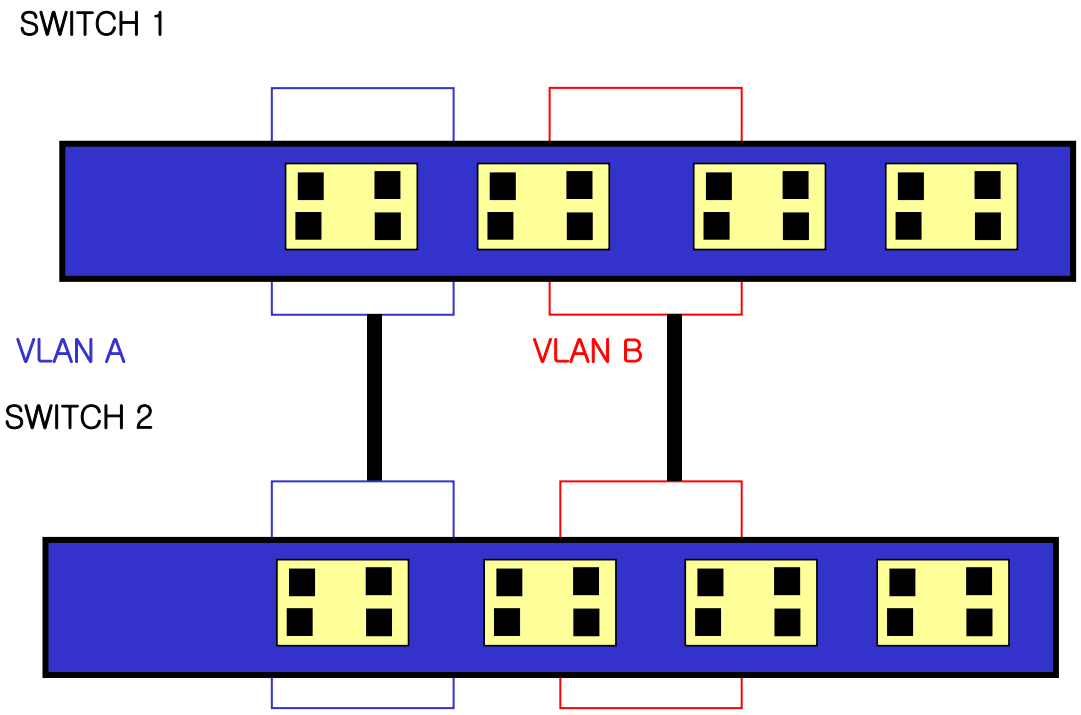


그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

VLAN A 는 스위치 1 의 포트 13 과 스위치 2 의 포트 1 의 연결을 통해 스위치 1 과 스위치 2 를 묶는다. VLAN B 는 스위치 1 의 포트 20 과 스위치 2 의 포트 11 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.

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

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

<오류! 참조 원본을 찾을 수 없습니다.>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.

4.2.2.2. VLAN 태그의 할당(Assigning a VLAN Tag)

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

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

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

<오류! 참조 원본을 찾을 수 없습니다.>는 태그가 붙은 프레임과 태그가 붙지 않은 프레임을 사용하는 네트워크의 물리적인 구성을 보여준다.

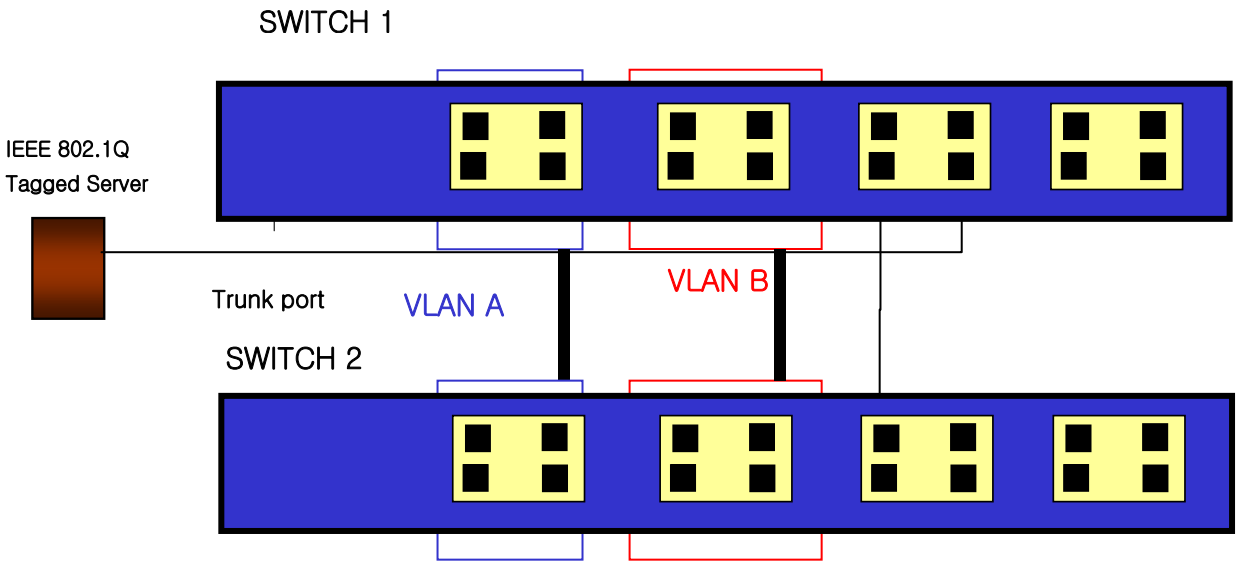


그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<오류! 참조 원본을 찾을 수 없습니다.>는 동일한 네트워크의 논리적인 다이어그램을 보여준다.

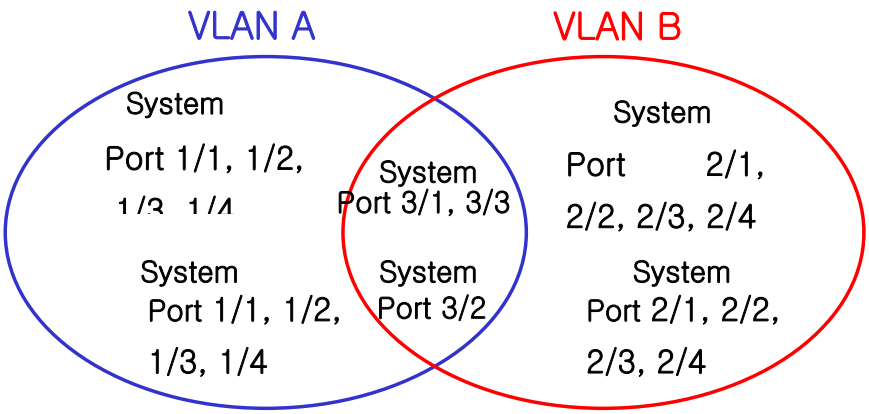


그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

<오류! 참조 원본을 찾을 수 없습니다.>와 <오류! 참조 원본을 찾을 수 없습니다.>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 붙지 않은 프레임을 송수신한다.

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

4.2.3. 포트 기반 VLAN 과 태그 VLAN 의 혼합 (Hybrid)

Hybrid 유형의 VLAN 은 포트 기반의 VLAN 과 태그 VLAN 의 기능을 혼합한 형태이다. Hybrid VLAN 은 포트 기반의 VLAN 과 같이 해당 포트로 들어오는 프레임의 VLAN id 를 결정하고 태그 VLAN 과 같이 태그를 붙여서 송신하거나 태그를 붙이지 않고 송신 하는 것을 결정 할 수 있다.

4.3. VLAN 구성

4.3.1. VLAN ID

VLAN 을 식별하기 위한 VLAN id 의 값으로 1 부터 4,094 사이의 숫자를 사용할 수 있다. 스위치가 초기화되었을 때 기본적으로 하나의 VLAN 이 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.
- 스위치 초기 상태에서 모든 포트는 native VLAN 으로 default VLAN 이 설정되어 있다.

4.3.3. Native VLAN

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

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

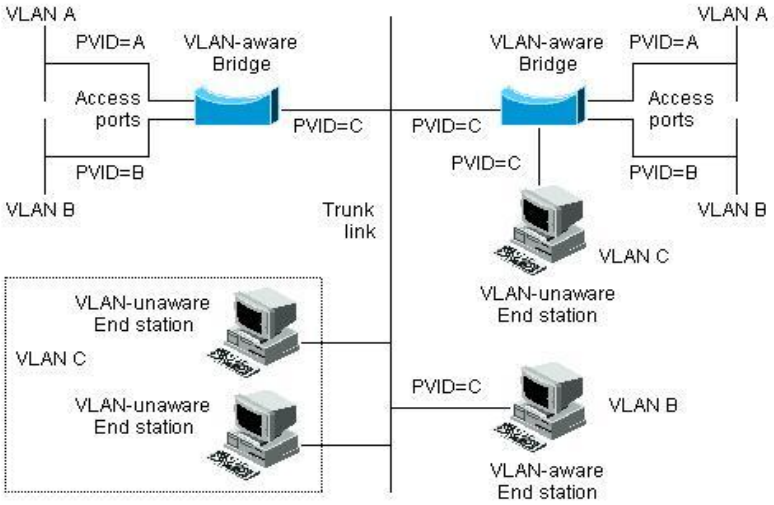


그림 4-6. Native VLAN

예를 들어 <그림 6>의 하단 부분에서처럼 두 달말 장비가 중앙의 트렁크 링크에 연결된 상태를 생각해 보자. 그들은 VLAN 을 인식하지 못하지만, VLAN 을 인식하는 브리지의 PVID 가 VLAN C 와 동일하게 하므로 VLAN C 에 포함될 것이다. VLAN 을 인식하지 못하는 단말 장비는 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 CS3400 series 스위치에 VLAN 을 설정에 사용되는 명령들을 설명한다. VLAN 설정은 다음의 단계로 진행된다.

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

4.4.1. VLAN 설정 명령

<오류! 참조 원본을 찾을 수 없습니다.>은 VLAN 설정에 사용되는 명령들을 설명한다.

표 4-1. VLAN 설정 명령어

명령어	설명	모드
`vlan database`	■ VLAN database 모드로 진입.	config
`vlan` *`vlanid`*	■ Vlanid 에 해당하는 vlan 을 생성 ■ 1 은 default VLAN 의 값으로 사용 ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다	vlan database
`vlan` *`vlanid`* `name WORD (state (enable|disable)|)`	■ Vlanid 에 해당하는 vlan 을 생성 ■ `WORD` 에 해당하는 vlan ascii 값을 설정 ■ vlan 의 상태를 enable disable 할 수 있다.	vlan database
`vlan` *`vlanid`* `bridge <1-256> name WORD (state (enable|disable)|)`	■ Vlanid 에 해당하는 vlan 을 생성 ■ `WORD` 에 해당하는 vlan ascii 값을 설정 ■ 생성하는 `vlan` 을 `bridge` 에 만든다. ■ vlan 의 상태를 enable disable 할 수 있다.	
`switchport`	■ 포트의 type 을 L2 로 변경한다. ■ L2 포트로 변경되면 default 로 access 모드에 VLAN 1 의 맴버가 된다.	Interface
`switchport mode {access|hybrid|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. ■ Hybrid – 포트를 hybrid 로 설정한다. ■ `trunk` – 포트를 트렁크(태그 VLAN)로 설정한다. 설정된 포트는 태그가 붙은 프레임을 송수신한다. 태그가 붙지 않은 프레임의 경우 native VLAN id 로 인식한다.	Interface
`switchport access vlan` *`vlanid`*	■ 포트를 VLAN 의 access 포트로 설정한다. ■ 모드가 access 로 설정되면, 설정된 포트는 VLAN 의 멤버 포트로 동작한다. ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다.	Interface

명령어	설명	모드
`Switchport hybrid vlan vlanid`	■ 설정된 포트는 VLAN 의 멤버 포트로 동작한다. ■ 수신되는 프레임이 untagged 일 경우 vlan id 에 해당하는 프레임으로 인식하도록 설정한다. ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다.	Interface
`switchport trunk allowed vlan (add|all|except) vlanid`	■ 포트를 VLAN 의 트렁크 포트로 설정한다. ■ 특정 VLAN 을 트렁크 포트로 설정하려면 add, 설정된 VLAN 을 모두 설정 하려면 all, 특정 vlan 만 제외 하려면 except 명령을 사용한다. ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다.	Interface
`switchport trunk native vlanid`	■ 포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 붙지 않고 송수신되는 트래픽을 위한 native VLAN 을 설정한다. ■ native VLAN 을 설정하지 않으면 default VLAN(VLANid = 1)이 native VLAN 으로 설정 ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다.	Interface
`switchport trunk (remove|none) vlanid`	■ 포트를 명시한 VLAN 의 멤버에서 제외시킨다. ■ *vlanid* : 2 부터 4094 사이의 값을 사용한다. ■ none: 모든 VLAN 으로부터 멤버에서 제외	Interface

4.5. VLAN 설정 예제

다음의 예제에서는 VLANid 가 1000 인 VLAN 을 생성하고, VLAN 에 IP 주소 132.15.121.1 을 할당하고, 두 포트를 VLAN 에 할당한다.

```
Switch#
Switch #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan database
Switch(config-vlan)#vlan 1000
Switch(config-vlan)#exit
Switch(config)#interface Vlan 1000
Switch(config-if-Vlan1000)#ip address 132.15.121.1/24
Switch(config-if-Vlan1000)#interface GigabitEthernet 1/2
Switch(config-if-Giga1/2)#switchport
Switch(config-if-Giga1/2)#switchport mode access
Switch(config-if-Giga1/2)#switchport access vlan 1000
Switch(config-if-Giga1/2)#interface GigabitEthernet 1/3
Switch(config-if-Giga1/3)#switchport
Switch(config-if-Giga1/3)#switchport mode access
Switch(config-if-Giga1/3)#switchport access vlan 1000
Switch(config-if-Giga1/3)#end
```

```
Switch#show vlan

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                         active    Gi1/1
2    VLAN0002                        active
3    VLAN0003                        active
4    VLAN0004                        active
5    VLAN0005                        active
6    VLAN0006                        active
7    VLAN0007                        active
8    VLAN0008                        active
9    VLAN0009                        active
10   VLAN0010                        active
11   VLAN0011                        active
12   VLAN0012                        active
100  VLAN0100                        active
1000 VLAN1000                        active    Gi1/2  Gi1/3

...

Switch#
```

다음의 예제에서는 태그 기반 Vlanid 로 2000 을 할당하고, 두 포트를 트렁크 포트로 VLAN 에 추가한다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan database
Switch(config-vlan)#vlan 2000
Switch(config-vlan)#exit
Switch(config)#interface GigabitEthernet 2/4
Switch(config-if-Giga2/4)#switchport
Switch(config-if-Giga2/4)#switchport mode trunk
Switch(config-if-Giga2/4)#switchport trunk allowed vlan add 2000
Switch(config-if-Giga2/4)#interface GigabitEthernet 2/1
Switch(config-if-Giga2/1)#switchport
Switch(config-if-Giga2/1)#switchport mode trunk
Switch(config-if-Giga2/1)#switchport trunk allowed vlan add 2000
Switch(config-if-Giga2/1)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- --------------- ------- ------------------------------
-
0               1       default         ACTIVE  Gi1/1 (u) Gi2/4 (u)
                                                Gi2/1 (u)
0               2       VLAN0002        ACTIVE
0               3       VLAN0003        ACTIVE
0               4       VLAN0004        ACTIVE
```

```
0                5       VLAN0005         ACTIVE
0                6       VLAN0006         ACTIVE
0                7       VLAN0007         ACTIVE
0                8       VLAN0008         ACTIVE
0                9       VLAN0009         ACTIVE
0                10      VLAN0010         ACTIVE
0                11      VLAN0011         ACTIVE
0                12      VLAN0012         ACTIVE
0                100     VLAN0100         ACTIVE
0                1000    VLAN1000         ACTIVE  Gi1/2 (u) Gi1/3 (u)
0                2000    VLAN2000         ACTIVE  Gi2/4 (t) Gi2/1 (t)
shu#
```

다음의 예제에서는 Vlanid 로 3000, 4000 을 할당하고, 두 포트를 hybrid 포트로 3000 에 추가하고 4000 에 태그포트로 추가한다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan database
Switch(config-vlan)#vlan 3000
Switch(config-vlan)#vlan 4000
Switch(config-vlan)#exit
Switch(config)#interface GigabitEthernet 1/1
Switch(config-if-Giga1/1)#switchport
Switch(config-if-Giga1/1)#switchport mode hybrid
Switch(config-if-Giga1/1)#switchport hybrid vlan 3000
Switch(config-if-Giga1/1)#switchport hybrid allowed vlan add 4000 egress-tagged
enable
Switch(config-if-Giga1/1)#interface GigabitEthernet 1/2
Switch(config-if-Giga1/2)#switchport
Switch(config-if-Giga1/2)#switchport mode hybrid
Switch(config-if-Giga1/2)#switchport hybrid vlan 3000
Switch(config-if-Giga1/2)#switchport hybrid allowed vlan add 4000 egress-tagged
enable
Switch(config-if-Giga1/2)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- --------------- ------- ------------------------------
-
0               1       default         ACTIVE  Gi1/1 (u) Gi1/4 (u)
0               2       VLAN0002        ACTIVE
0               3       VLAN0003        ACTIVE
0               6       VLAN0006        ACTIVE
0               7       VLAN0007        ACTIVE
0               8       VLAN0008        ACTIVE
0               9       VLAN0009        ACTIVE
0               10      VLAN0010        ACTIVE
0               11      VLAN0011        ACTIVE
0               12      VLAN0012        ACTIVE
0               100     VLAN0100        ACTIVE
0               1000    VLAN1000        ACTIVE  Gi1/2 (u) Gi1/3 (u)
0               2000    VLAN2000        ACTIVE  Gi1/4 (t)
0               3000    VLAN3000        ACTIVE  Gi1/1 (u) Gi1/2 (u)
0               4000    VLAN4000        ACTIVE  Gi1/1 (t) Gi1/2 (t)
Switch#
```

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

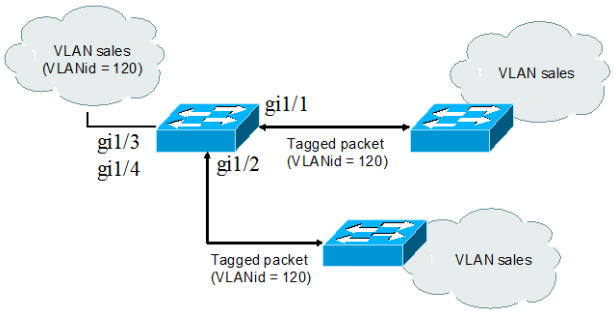


그림 4-7. VLAN 설정 예제 – Tagged and Untagged VLAN

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan database
Switch(config-vlan)#vlan 120
Switch(config-vlan)#exit
Switch(config)#interface GigabitEthernet 1/1
Switch(config-if-Giga1/1)#switchport
Switch(config-if-Giga1/1)#switchport mode trunk
Switch(config-if-Giga1/1)#switchport trunk allowed vlan add 120
Switch(config-if-Giga1/1)#interface GigabitEthernet 1/2
Switch(config-if-Giga1/2)#switchport
Switch(config-if-Giga1/2)#switchport mode trunk
Switch(config-if-Giga1/2)#switchport trunk allowed vlan add 120
Switch(config-if-Giga1/2)#interface GigabitEthernet 1/3
Switch(config-if-Giga1/3)#switchport
Switch(config-if-Giga1/3)#switchport access vlan 120
Switch(config-if-Giga1/3)#interface GigabitEthernet 1/4
Switch(config-if-Giga1/4)#switchport
Switch(config-if-Giga1/4)#switchport access vlan 120
Switch(config-if-Giga1/4)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- ---------------- ------- ------------------------------
-
0               1       default          ACTIVE  Gi1/1 (u) Gi1/2 (u)

0               120     VLAN0120         ACTIVE  Gi1/1 (t) Gi1/2 (t)
                                                 Gi1/3 (u) Gi1/4 (u)
Switch#
```

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#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 200
Switch(config-vlan)#vlan 400
Switch(config-vlan)#exit
Switch(config)#interface GigabitEthernet 1/1
Switch(config-if-Giga1/1)#switchport mode trunk
Switch(config-if-Giga1/1)#switchport trunk allowed vlan add 200
Switch(config-if-Giga1/1)#switchport trunk native vlan 200
Switch(config-if-Giga1/1)#switchport trunk allowed vlan add 400
Switch(config-if-Giga1/1)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- --------------- ------- ------------------------------
-
0               1       default         ACTIVE  Gi1/1 (t)
0               100     VLAN0100        ACTIVE
0               120     VLAN0120        ACTIVE  Gi1/1 (t)
0               200     VLAN0200        ACTIVE  Gi1/1 (u)
0               400     VLAN0400        ACTIVE  Gi1/1 (t)
Switch#
```

포트 gi1/1 으로 태그가 붙지 않은 프레임이 수신되면 스위치는 VLAN *marketing* 의 멤버 포트로 프레임을 전달한다.

4.6. VLAN 설정 정보 확인

VLAN 설정 정보를 보려면 다음의 명령을 사용한다.

명령어	설명	모드
`show vlans`	■ VLAN 와 관련된 다음의 요약 정보를 출력한다. • VLANid • 멤버 포트 • VLAN 이 속한 bridge • Spanning-tree 모드	Exec
`show vlan all`	■ VLAN 와 관련된 다음의 요약 정보를 출력한다. • VLANid • 멤버 포트 • tag, untag	Exec
`show interface trunk (module <1-6>|)`	■ VLAN 와 관련된 다음의 요약 정보를 출력한다. • 포트 • Vlan 모드 • Native vlan, trunk vlan	Exec
`show interface`	■ VLAN 와 관련된 다음의 요약 정보를 출력한다.	Exec

summary vlan	• Vlan id

```
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- ---------------- ------- --------------------------------
-
0               1       default          ACTIVE  Gi1/1 (t) Gi1/2 (u)
0               2       VLAN0002         ACTIVE
0               10      VLAN0010         ACTIVE
0               11      VLAN0011         ACTIVE
0               12      VLAN0012         ACTIVE
0               100     VLAN0100         ACTIVE
0               120     VLAN0120         ACTIVE  Gi1/1 (t) Gi1/2 (t)
                                                 Gi1/3 (u) Gi1/4 (u)
0               200     VLAN0200         ACTIVE  Gi1/1 (u)
0               400     VLAN0400         ACTIVE  Gi1/1 (t)
0               1000    VLAN1000         ACTIVE
0               2000    VLAN2000         ACTIVE
0               3000    VLAN3000         ACTIVE
0               4000    VLAN4000         ACTIVE
Switch#
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- --------------------------------
1    default                          active    Gi1/1  Gi1/2
120  VLAN0120                         active    Gi1/1  Gi1/2  Gi1/3
                                                Gi1/4
200  VLAN0200                         active    Gi1/1
400  VLAN0400                         active    Gi1/1
1000 VLAN1000                         active
2000 VLAN2000                         active
3000 VLAN3000                         active
4000 VLAN4000                         active

VLAN MTU        BridgeNo Stp Enabled  BrdgMode
---- ---------- -------- ------------ ---------------
1    1500       0        Yes          vlan-bridge
120  1500       0        Yes          vlan-bridge
200  1500       0        Yes          vlan-bridge
400  1500       0        Yes          vlan-bridge
1000 1500       0        Yes          vlan-bridge
2000 1500       0        Yes          vlan-bridge
3000 1500       0        Yes          vlan-bridge
4000 1500       0        Yes          vlan-bridge

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 3 계층 인터페이스로 동작한다.

CS3400 Series 스위치는 다음의 인터페이스에 IP 를 할당할 수 있다.

- VLAN interface
- Loopback interface
- Management interface

5.2. 네트워크 인터페이스에 IP 주소 할당

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

표 5-1. 사용 가능한 IP 주소

Class	주소 범위	상태
A	0.0.0.0	예약
	1.0.0.0 ~ 126.0.0.0	사용가능

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

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

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

CS3400 Series 스위치는 인터페이스에 IP 주소 할당 기능을 지원한다. 각 인터페이스는 Primary IP 주소 한 개와 개수 제한이 없는 Secondary IP 주소 설정이 가능하다. 다양한 상황에서 복수개의 IP 주소가 유용하게 사용된다. 다음은 가장 일반적인 응용이다.

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

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

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

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

표 5-2. IP 주소 할당 명령어

명령어	설명
`ip address` *`ipaddress/prefixlen`* `[secondary]`	■ 인터페이스에 사용될 IP 주소를 설정한다. ■ *ipaddress/prefixlen*: 설정할 IP 주소 ■ secondary: Secondary IP 주소로 설정

5.3. ARP(Address Resolution Protocol)

ARP 테이블의 정보를 확인하려면, privilege 모드에서 다음 < 표 5-3>의 명령어를 사용한다. CS3400 Series 에서는 Static ARP 를 설정할 수 있다.

표 5-3. ARP 환경 설정을 위한 명령어

명령어	설명	모드
`Show arp`	■ ARP 테이블의 엔트리를 출력한다.	Privileged
`clear arp-cache`	■ ARP 테이블의 엔트리를 삭제한다.	Privileged
`Clear arp-cache interface IFNAME`	■ 해당 interface 의 ARP 엔트리를 삭제한다	Privileged
`arp` *`ip-address MAC`*	■ ARP 테이블에 static ARP 엔트리를 설정 ■ Ip-address: ARP 엔트리의 IP 주소를 나타낸다; ■ MAC: ARP 엔트리의 48bit Ethernet 주소를 나타낸다. ■ alias	config
`no arp` *`ip-address`*	■ 해당 ip address 의 ARP 엔트리를 삭제한다.	config
`arp-ageing-timeout <1-3000>`	■ 해당 interface 의 ARP entry 의 소멸 시간을 설정한다	interface
`no arp-ageing-timeout`	■ 해당 interface 의 ARP entry 소멸 시간을 default 값으로 설정한다 (default : 7200 sec)	interface

다음은 static ARP 를 설정하고 ARP timeout 을 설정하는 예이다. ARP 설정을 위해서는 설정하는 IP 주소를 가지고 있는 인터페이스가 먼저 존재해야 한다.

```
shu#
shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shu(config)#arp 192.168.1.3 0111.1111.1213
% Interface does not exist
shu(config)#int GigabitEthernet 1/1
shu(config-if-Giga1/1)#ip address 192.168.1.3/24
shu(config-if-Giga1/1)#exit
shu(config)#arp 192.168.1.3 0111.1111.1213
shu(config)#end
```

```
shu#show arp
Protocol  Address         Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
Internet  192.168.1.3     0111.1111.1213 static    Giga1/1
Internet  10.1.17.104     0022.1926.2db3 dynamic   eth0
Internet  10.1.17.254     0007.7045.a36f dynamic   eth0
shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shu(config)#no arp 192.168.1.3
shu(config)#end
shu#show arp
Protocol  Address         Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
Internet  10.1.17.254     0007.7045.a36f dynamic   eth0
shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shu(config)#interface GigabitEthernet 1/1
shu(config-if-Giga1/1)#arp-ageing-timeout 2000
shu(config-if-Giga1/1)#
```

5.4. Static Routes 설정

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

Static route 를 설정하려면 Config 모드에서 다음의 명령을 사용한다.

표 5-4. Static route 경로 설정 명령어

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

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

distance 값을 가진다. Static route 가 동적 라우팅 프로토콜의 정보로 중첩되길 원한다면 static route 의 administrative distance 가 동적 프로토콜의 값보다 더 크면 된다.

표 5-5. 동적 라우팅 프로토콜의 default administrative distances

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

Static route 정보를 확인하려면 privileged 모드에서 다음의 명령을 사용하라.

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

5.5. IP 설정 예제

이 절에서는 IP 주소 설정 예제를 제공한다:

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

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

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

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

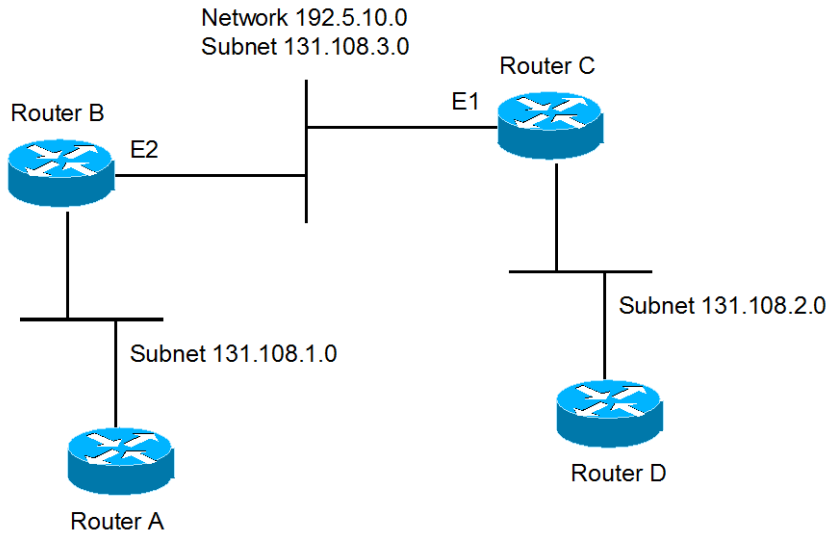


그림 5-1. 네트워크 설정 예 – 복수 IP address

라우터 B 설정

```
Switch(config)# interface  giga1/1
Switch(config-if-Giga1/1)# ip  address  192.5.10.1/24
Switch(config-if-Giga1/1)# ip  address  131.108.3.1/24 secondary
```

라우터 C 설정

```
Switch(config)# interface  vlan2
Switch(config-if-Giga1/1)# ip  address  192.5.10.2/240
Switch(config-if-Giga1/1)# ip  address  131.108.3.2/24 secondary
```

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제이다.

```
Switch# show arp
Protocol  Address          Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
Internet  10.1.2.254       0007.7089.1123  dynamic   Giga1/1
Internet  10.1.11.46       0006.2bfc.146e  dynamic   Giga1/1
Internet  10.1.13.1        0001.0281.f775  dynamic   Giga1/1
Internet  10.1.13.190      0000.f083.f6d4  dynamic   Giga1/1
```

다음의 명령은 ARP 테이블에 static ARP 엔트리를 등록한다.

```
Switch(config)# arp 142.10.52.196 0010.073c.0514
Switch# show arp
Protocol  Address          Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
```

```
Internet  142.10.52.196   0010.073c.0514  static    Giga1/1
```

다음의 명령은 ARP 테이블에서 static ARP 엔트리를 삭제한다.

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

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

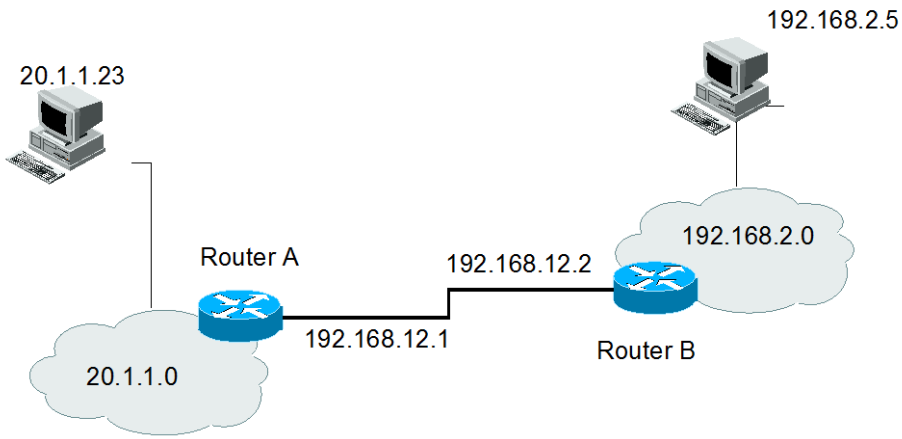


그림 5-2. 네트워크 설정 예 – Static route

라우터 A 설정

```
Switch(config)# ip  route  192.168.2.0/24  192.168.12.2
Switch(config)# show ip route static
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route
S>* 192.168.2.0/24 [1/0] via 192.168.12.2 vlan2
Switch(config)#
```

라우터 B 설정

```
Switch(config)# ip  route  20.1.1.0/8  192.168.12.1
Switch(config)# show ip route static
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route
S   20.1.1.0/8 [1/0] via 192.168.12.1 vlan2
Switch(config)#
```

6 CFM (Connectivity Fault Management)

6.1. CFM 개요

이더넷 OAM(Operations, Administration, Maintenace)은 이더넷 네트워크의 관리를 위하여 고안된 프로토콜이다. 이더넷 OAM 에는 CFM(Connectivity Fault Management), EFM 등이 존재 한다.

CFM (Connectivity Fault Management)는 네트워크 장애를 감지하기 위해서 고안된 프로토콜로써, IEEE 802.1ag 와 ITU-T Y.1731 에 표준화되어 있다. 이 장에서는 CFM 을 설정하는 방법과 절차에 대해서 설명한다.

6.1.1. Understanding CFM

CFM은 VLAN별로 End-to-End로 이루어지는 이더넷 계층의 OAM 프로토콜이다. CFM은 연결상태 감시(connectivity monitoring), 장애 확인(fault verification) 그리고 성능 측정(performance monitoring) 기능을 제공한다

6.1.2. CFM Domain

CFM 관리 도메인 (maintenance domain)은 네트워크 관리를 위해 논리적으로 구분한 관리 공간이다. CFM 도메인은 8(0 ~ 7레벨) 개의 레벨로 나뉘고 각 도메인들은 계층적 관계로 정의 된다. 도메인 레벨의 값이 작을수록 높은 우선순위를 가지며, 도메인 레벨은 그 역할에 따라 다음과 같이 구분된다:

- 0~2 level: 관리자 역할 (Operation role)
- 3~4 level: 서비스 제공자 역할 (Provider role)
- 5~7 level: 사용자 역할 (Customer role)

그림 1은 CFM 도메인을 레벨별로 구성한 예제이다.

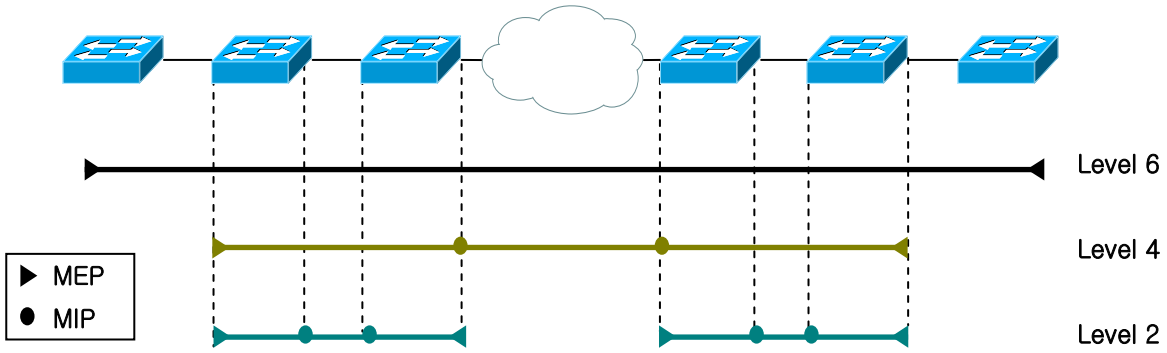


그림 6-1 CFM Maintenace Domain Level

그림 2는 CFM 도메인을 구성할 때의 유의사항을 나타낸다. CFM 도메인은 그림 2 (A)처럼 근접하게 설정할 수 있으며, 그림 2의 (B)처럼 범위가 넓은 도메인 안에 다른 도메인이 포함되게 도메인을 구성 할 수도 있다. 하지만, 그림 2의 (C)와 같이 한 개의 관리 개체(포트)가 서로 다른 도메인이 교차되서 설정 될 수 는 없다.

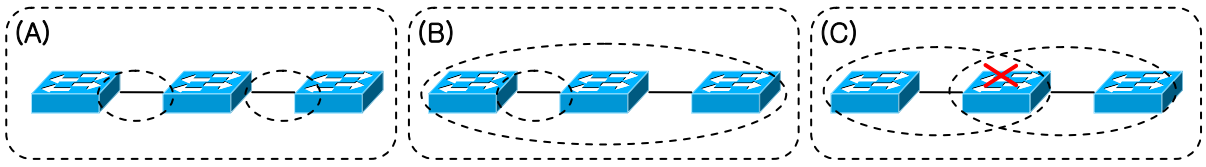


그림 6-2 도메인 구성

6.1.3. CFM Maintenance Association

CFM MA(Mainteneace Association)는 도메인 내에 유일한 MA ID 로 정의된다. MA 에 속한 MEP 들은 MA 가 속한 도메인의 레벨을 가진다. 동일한 도메인 내에 여러 MA 를 설정할 수 있으며, 도메인에 속한 MA 들은 VLAN 별로 MA ID 를 부여할 수 있다.

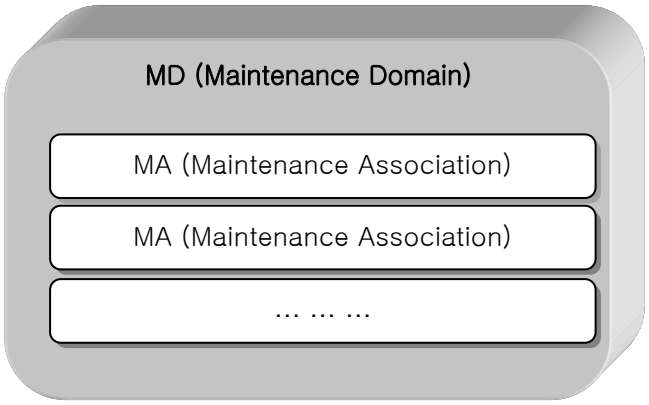


그림 6-3 MD 와 MA 의 관계

6.1.4. Maintenance Points

도메인 내에서 CFM 이 동작하는 인터페이스 경계점을 관리 지점(Maintenance Point)라고 한다. 관리 지점은 하위 레벨의 CFM 프레임을 폐기하거나 상위 레벨의 프레임을 전달하는 역할을 한다. 관리 지점은 두 가지 종류가 있다.

1) MEP (Maintenance end point)

MEP는 도메인의 종단에 자리잡고 있는 경계점이다. 즉, MEP는 도메인의 경계를 의미한다. MEP는 CFM 프레임을 생성하여 송신하고 수신한 CFM 프레임을 처리한다.

2) MIP (Maintenance Intermediate point)

도메인 내부에 위치하는 관리 지점으로서 traceroute, loopback message에 대한 응답만 할 뿐 다른 CFM 프레임에 대해서는 처리하지 않는다.

6.1.5. CFM Message

CFM 프레임을 식별하기 위해 고유의 EtherType(0x8902)과 Group MAC address 를 사용한다. CS3400 스위치에서 지원하는 CFM 메시지의 종류는 다음과 같다:

1) ETH-CC (Ethernet Continuty Check)

2) ETH-LB (Ethernet Loopback)

3) ETH-LT (Ethernet LinkTrace)

4) ETH-LM (Ethernet Loss measurement)

5) ETH-DM (Ethernet Delay measurement)

6.1.6. Ethenret CFM Guidelines

CFM 을 설정할 때 유의할 점은 다음과 같다:

- L2 인터페이스에서만 설정이 가능하다.
- Port-group 인터페이스에는 레벨 0 MEP 를 설정 할 수 없고 UNI-MEP 설정만 가능하다.

6.2. Configuring CFM

본 장에서는 CFM 을 설정하는 방법을 설명한다.

CFM 설정 순서는 다음과 같다:

1) 도메인 생성
2) MA 생성
3) Remote MEP 지정
4) MEP 설정

6.2.1. Preparing the CFM configuration

다음은 CFM 도메인, MA 및 Remote MEP 정보를 설정하는 방법이다.

	Command or Action	***Purpose***
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**ethernet cfm domain-name type** *TYPE* **name** *MDNAME* **level** *<0 – 7>* **mip-creation** (none |	도메인을 생성하고 ethernet cfm mode 로 진입한다.

	default | explicit) **예제:** Switch(config)# **ethernet cfm domain-name type itu-t name CFMMD level 5 mip-creation none**	**NOTE** domain type 을 *itu-t* 또는 *802.1ag* 으로 생성할 수 있다.
Step 3	**service ma-type** *TYPE* **ma-name** *MANAME* **(vlan** *VID* **mip-creation** *permission***)** Switch(config-ether-cfm)# **service ma-type string ma-name MANAME vlan 200 mip-creation none**	MA 를 생성한다.
Step 4	**mep crosscheck rmpid** *RMEP ID (* vlan *VID*) Switch(config-ether-cfm)# **mep crosscheck rmpid 1 vlan 200**	Remote MEP 를 설정한다.
Step 5	**end** **예제:** Switch(config-ether-cfm)# **end**	privileged EXEC 모드로 돌아간다

6.2.2. Configuring MEP

다음은 인터페이스에서 MEP 를 설정하는 방법이다.

	Command or Action	***Purpose***
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**Interface** *IFNAME* **예제:** Switch(config)# **interface gi2/1**	인터페이스 모드로 진입한다.
Step 3	**switchport** **예제:** Switch(config-if-Giga2/1)#**switchport**	인터페이스를 L2 모드로 전환한다.
Step 4	**swtichport access vlan** *VID* **예제:** Switch(config-if-Giga2/1)#**switchport access vlan 200**	인터페이스를 VLAN 에 포함시킨다.
Step 5	**ethernet cfm mep** *direction* **mpid** *MEPID* **active** (ture|false) **domain** *MDNAME* (vlan VID | uni-mep | bridge) **예제:** Switch(config-if-Giga2/1)# **ethernet cfm mep down mpid 2 active true domain MDNAME vlan**	인터페이스에 MEP 를 설정한다.

	200	
Step 6	**end** **예제:** Switch(config-if-Giga2/1)# **end**	privileged EXEC 모드로 돌아간다

6.2.3. Enable Continuity Check

CFM 의 CC(Continutity Check)기능을 사용하기 위해서는 해당 인터페이스에 MEP 가 설정되어 있어야 한다. CC 기능이 설정되면 각 MEP 는 ETH-CC 프레임을 주고 받는다. ETH-CC 프레임의 전송 주기는 변경이 가능하다.

다음은 CFM 의 CC 기능을 설정하는 방법이다.

	Command or Action	***Purpose***
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**Interface *IFNAME*** **예제:** Switch(config)# **interface gi2/1**	인터페이스 모드로 진입한다.
Step 3	**ethernet cfm cc** (multicast |unicast**) state** (enable|disable) **domain** *MDNAME* **mepid** *MEPID* (vlan VID) **예제:** Switch(config-if-Giga2/1)# **ethernet cfm cc multicast state enable domain MDNAME mepid 2 vlan 200**	CC 를 enable 한다. **NOTE** CC type 이 unicast 일 경우 RMEP 생성시에 remote MEP 의 인터페이스에 MAC address 를 설정 한다. **NOTE** CC 를 disable 하려면 state 를 diable 로 변경한다.
Step 4	**exit** **예제:** Switch(config-if-Giga2/1)# **exit**	Global configuration 모드로 돌아간다.
Step 5 **(Optional)**	**ethernet cfm cc domain** *MDNAME* (vlan VID) **interval** (1|2|3|4|5|6|7) **예제:** Switch(config)# **ethernet cfm cc domain MDNAME vlan 200 interval 5**	ETH-CC 프레임 전송 주기를 변경한다. **NOTE** MEP 와 MEP 간에는 ETH-CC 프레임 전송 주기가 반드시 일치해야 CC 상태가 검사된다. **NOTE** default 는 4 (1 second)
Step 6	**end** **예제:** Switch(config-if-Giga2/1)# **end**	privileged EXEC 모드로 돌아간다

6.2.4. Using Ethernet Traceroute and Ethernet Loopback

CFM 의 traceroute 기능과 loopback 기능을 사용하기 위해서는 MEP 가 설정되어 있어야 한다. Remote MEP 로의 traceroute 와 loopback 을 위한 명령은 다음과 같다.

	Command or Action	***Purpose***
	traceroute ethernet *MACADDR* **domain** MDNAME (vlan VID) **예제:** Switch#**traceroute ethernet 1111.1111.1111 domain MDNAME vlan 200**	Remote MEP 인 Target MAC address 까지의 경로를 확인 한다.
	ping ethernet mac *MACADDR* **unicast source** *MEPID* **domain** *MDNAME* (vlan *VID*) **예제:** Switch# **ping ethernet mac 1111.1111.1111 unicast source 2 domain MDNAME vlan 200**	Unicast 형식의 ETH-LB 프레임을 Remote MEP 로 전송하고 그 수신결과를 모니터링한다.
	ping ethernet (multicast | unicast rmepid RMEPID) **mepid** *MEPID* **domain** *MDNAME* (vlan *VID*) **예제:** **ping ethernet multicast mepid 2 domain MDNAME vlan 200**	Unicast / multicast 유형의 ETH-LB 프레임을 Remote MEP 로 전송하고 그 수신결과를 모니터링 한다.

6.2.5. Performance Monitoring

CFM 을 두 MEP 사이의 프레임 손실(frame loss)이나 전달 지연(frame delay)과 같은 네트워크 성능측정에 사용할 수 있다. CFM 의 PM 기능은 CC 로 연결된 두 MEP 사이에서만 올바르게 동작한다.

다음은 PM 기능을 설정하고 결과를 확인하는 방법이다.

	Command or Action	***Purpose***
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**Interface *IFNAME*** **예제:** Switch(config)# **interface gi2/1**	인터페이스 모드로 진입한다.
Step 3	**ethernet cfm pm** (enable|disable) (frame-delay| frame-loss) (multicast|unicast) **mepid** *MEPID* **rmepid** *RMEPID* **domain** *MDNAME* (vlan *VID*)	인터페이스에 performance monitoring 을 설정/해제 한다.

	예제: Switch(config-if-Giga2/1)#**ethernet cfm pm enable frame-delay multicast mepid 2 rmepid 1 domain MDNAME vlan 200**	
Step 4 **(optional)**	**exit** 예제: Switch(config-if-Giga2/1)# **exit**	Global configuration 모드로 돌아간다.
Step 5 **(optional)**	**ethernet cfm pm** (frame-loss|frame-delay) **domain** *MDNAME* (vlan *VID*) **interval** INTV 예제: Switch(config)#**ethernet cfm pm frame-loss domain test vlan 200 interval 10**	Performance monotiring 을 수행하는 주기를 변경한다. Interval 로 설정한 시간을 주기로 PM 을 진행한다.
Step 6	**end** 예제: Switch(config-if-Giga2/1)# **end**	privileged EXEC 모드로 돌아간다

6.2.6. Configuring MIP

MIP 는 MEP 와 MEP 를 연결하는 중간 노드이다. CFM traceroute 기능을 사용할 때 두 MEP 경로사이에 위치한 MIP 는 ETH-LT 메시지에 대한 응답을 해준다.

다음은 MIP 를 설정하는 방법이다.

	Command or Action	***Purpose***
Step 1	**configure terminal** 예제: Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**ethernet cfm domain-name type** *TYPE* **name** *MDNAME* **level** <*0 – 7*> **mip-creation none** 예제: Switch(config)# **ethernet cfm domain-name type itu-t name CFMMD level 5 mip-creation none**	Domain 을 생성하고 ethernet cfm mode 로 진입한다. **NOTE** domain type 을 *itu-t* 또는 *802.1ag* 로 생성할 수 있다.
Step 3	**service ma-type** *TYPE* **ma-name** *MANAME* (vlan *VID* mip-creation *permission*) Switch(config-ether-cfm)# **service ma-type string ma-name MANAME vlan 200 mip-creation none**	MA 를 생성한다.
Step 4 **(optional)**	**exit** 예제: Switch(config-ether-cfm)# **exit**	Global configuration 모드로 돌아간다.
Step 5	**ethernet cfm default-md-level entry vid** *VID*	CFM MIP 를 생성한다.

(optional)	**level** <0-7> **mip-creation** PERMISSION **예제:** Switch(config)# **ethernet cfm default-md-level entry vid 200 level 5 mip-creation default**	
Step 6	**end** **예제:** Switch(config)# end	Privileged EXEC 모드로 돌아간다.

6.2.7. Verifying the CFM configuration

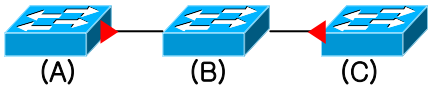
CFM의 설정 정보, CC 상태 그리고 성능 측정 결과 등을 확인할 수 있다.

	Command or Action	***Purpose***
	show ethernet cfm maintenance-points remote	Remote MEP 의 정보와 CC 상태를 확인한다.
	show ethernet cfm maintenance-points local (mep|mip)	장비에 설정되어 있는 MEP / MIP 의 설정 정보를 확인한다.
	show ethernet cfm pm (frame-loss|frame-delay) **mepid** *MEPID* **rmepid** *RMEPID* **domain** *MDNAME* (vlan *VID)*	Performance Monitoring 결과를 확인한다.
	show ethernet cfm traceroute-cache	Traceroute cache 에 있는 ethernet traceroute 의 결과를 확인한다.
	show ethernet cfm ma status domain *MDNAME* **(vlan** *VID***) mep** *MEPID*	설정된 MA 정보와 MA 안에 Remote MEP 설정 개수, MEP 설정정보 및, CC 상태 정보를 모니터링 할 수 있다.

6.3. CFM Configuration Samples

6.3.1. CC configuration

다음의 예제는 도메인의 이름이 test 인 Level 5 의 Vlan200 도메인에서 MEP 를 설정하고 멀티캐스트 CC 기능을 설정하는 방법을 보여준다.



(A) MEP Configuration

```
Switch# conf ter
Switch(config)#ethernet cfm domain-name type itu-t name test level 5 mip-creation none
Switch(config-ether-cfm)#service ma-type string ma-name testma vlan 200 mip-creation none
Switch(config-ether-cfm)# mep crosscheck rmpid 11 vlan 200
Switch(config-ether-cfm)# exit
Switch(config)#interface gi2/1
Switch(config-if-Giga2/1)# ethernet cfm mep down mpid 21 active true domain test vlan 200
Switch(config-if-Giga2/1)# ethernet cfm cc multicast state enable domain test mepid 21 vlan 200
Switch(config-if-Giga2/1)# exit
Switch# show ethernet cfm maintenance-points local mep
```

(A) 장비의 설정을 조회하면 다음과 같다.

```
!
ethernet cfm domain-name type itu-t name test level 5 mip-creation none
 service ma-type string ma-name testma vlan 200 mip-creation none
 mep crosscheck rmpid 11 vlan 200
!
interface Giga2/1
 ethernet cfm mep down mpid 21 active true domain test vlan 200
 ethernet cfm cc multicast state enable domain test mepid 21 vlan 200
!
```

(B) MIP Configuration

```
Switch# conf ter
Switch(config)#ethernet cfm domain-name type itu-t name test level 5 mip-creation none
Switch(config-ether-cfm)#service ma-type string ma-name testma vlan 200 mip-creation none
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm default-md-level entry vid 200 level 5 mip-creation default
Switch(config-if-Giga2/1)# exit
Switch# show ethernet cfm maintenance-points local mep
```

(B) 장비의 설정을 조회하면 다음과 같다.

```
!
ethernet cfm domain-name type itu-t name test level 5 mip-creation none
 service ma-type string ma-name testma vlan 200 mip-creation none
!
ethernet cfm default-md-level entry vid 200 level 5 mip-creation default
!
```

(C) MEP Configuration

```
Switch# conf ter
Switch(config)#ethernet cfm domain-name type itu-t name test level 5 mip-creation none
Switch(config-ether-cfm)#service ma-type string ma-name testma vlan 200 mip-creation none
Switch(config-ether-cfm)# mep crosscheck rmpid 21 vlan 200
Switch(config-ether-cfm)# exit
Switch(config)#interface gi2/1
Switch(config-if-Giga2/1)# ethernet cfm mep down mpid 11 active true domain test vlan 200
Switch(config-if-Giga2/1)# ethernet cfm cc multicast state enable domain test mepid 11 vlan 200
Switch(config-if-Giga2/1)# exit
Switch# show ethernet cfm maintenance-points local mep
```

(C) 장비의 설정을 조회하면 다음과 같다.

```
!
ethernet cfm domain-name type itu-t name test level 5 mip-creation none
 service ma-type string ma-name testma vlan 200 mip-creation none
 mep crosscheck rmpid 21 vlan 200
!
interface Giga2/1
 ethernet cfm mep down mpid 11 active true domain test vlan 200
 ethernet cfm cc multicast state enable domain test mepid 11 vlan 200
!
```

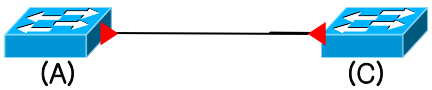
CC 의 상태 정보는 아래와 같이 확인 할 수 있다.

```
Switch# show ethernet cfm maintenance-points remote
MPID    LEVEL    VLAN    ACTIVE    Remote Mac       RDI    FLAGS
-------------------------------------------------------------------------------
 21       0        0       Yes      0007.729e.dfda   False  Configured
```

6.3.2. UNI-MEP configuration

다음의 예제는 물리 인터페이스(Physical interface)에 UNI-MEP 를 생성하는 예제이다. UNI-MEP 를 생성할 경우 CC 는 default 로 설정된다. UNI-MEP 를 설정할 때 유의할 점은 다음과 같다:

- UNI-MEP 의 도메인 레벨은 반드시 0 이어야 한다.
- UNI-MEP 가 설정된 물리 인터페이스의 종단에는 항상 Remote UNI MEP 가 있어야 한다.
- UNI-MEP 는 기본적으로 Untagged 프레임 형식으로 전송되지만, 802.1Q 프레임으로도 전송이 가능하다.



(A) UNI MEP Configuration

```
Switch# conf ter
Switch(config)#ethernet cfm domain-name type itu-t name test level 0 mip-creation none
Switch(config-ether-cfm)#service ma-type string ma-name testma
Switch(config-ether-cfm)# mep crosscheck rmpid 11
Switch(config-ether-cfm)# exit
Switch(config)#interface gi2/1
Switch(config-if-Giga2/1)# ethernet cfm mep down mpid 21 active true domain test uni-mep rmepid
11
Switch(config-if-Giga2/1)# exit
Switch#
Switch# show ethernet cfm maintenance-points local mep
```

(A) 장비의 설정을 조회하면 다음과 같다.

```
!
ethernet cfm domain-name type itu-t name test level 5 mip-creation none
 service ma-type string ma-name testma
 mep crosscheck rmpid 11
```

```
!
interface Giga2/1
 ethernet cfm mep down mpid 21 active true domain test uni-mep rmepid 11
 ethernet cfm cc multicast state enable domain test mepid 21
!
```

(B) UNI MEP Configuration

```
Switch# conf ter
Switch(config)#ethernet cfm domain-name type itu-t name test level 0 mip-creation none
Switch(config-ether-cfm)#service ma-type string ma-name testma
Switch(config-ether-cfm)# mep crosscheck rmpid 21
Switch(config-ether-cfm)# exit
Switch(config)#interface gi2/1
Switch(config-if-Giga2/1)# ethernet cfm mep down mpid 11 active true domain test uni-mep rmepid
21
Switch(config-if-Giga2/1)# exit
Switch#
Switch# show ethernet cfm maintenance-points local mep
```

(B) 장비의 설정을 조회하면 다음과 같다.

```
!
ethernet cfm domain-name type itu-t name test level 0 mip-creation none
 service ma-type string ma-name testma
 mep crosscheck rmpid 21
!
interface Giga2/1
 ethernet cfm mep down mpid 11 active true domain test uni-mep rmepid 21
 ethernet cfm cc multicast state enable domain test mepid 11
!
```

CC 의 상태 정보는 아래와 같이 확인 할 수 있다.

```
Switch# show ethernet cfm maintenance-points remote
MPID    LEVEL    VLAN    ACTIVE    Remote Mac       RDI    FLAGS
--------------------------------------------------------------------------------
 21        0        0        Yes     0007.729e.11ab     False   Configured
```

7

ERPS

본 장에서는 CS3400 Series 스위치에서 사용 되는 ERPS 프로토콜에 대해서 기술한다. ERPS 프로토콜은 ITU-T G.8032/Y.1344 에 서술되어 있다.

7.1. ERPS 개요

ERPS 는 이더넷 링 (Ethernet Ring topology) 환경에서 사용 된다. ERPS 는 ITU-T G8032/Y.1344 에 서술되어 있는 Automatic Protection Switching (APS) 프로토콜로써 이더넷 링을 보호한다. 트래픽 Loop 방지를 위해 RPL(Ring Protection Link)을 차단(Block) 하고, RPL 이 아닌 다른 Link 에 장애가 발생했을 때 RPL 의 차단을 해제한다.

이더넷 링 노드 중 RPL Owner 는 PRL 의 트래픽을 차단하고, Link 장애가 발생하면 RPL 의 트래픽 차단을 해제하여 서비스가 가능하도록 한다.

7.1.1. ERPS Terms

- ✓ **Ring Protection Link (RPL)**
  이더넷 링에서 Loop 방지를 위하여 임의로 지정하여 차단된 Link.
- ✓ **RPL Owner**
  RPL 에 연결되어 있는 링 노드가 Idle 상태이면 RPL 을 차단하고, 링 장애가 발생했을 때 RPL 의 차단을 해제한다.
- ✓ **Signal Fail (SF)**
  Link 장애가 감지되면 Signal Fail 이 발생한다.
- ✓ **No Request (NR)**
  Idle 상태 혹은 Link 장애가 복구 되면 No Request 가 발생한다.
- ✓ **Ring APS (R-APS) Message**
  Y.1731/G8032 에 정의되어 있는 링의 상태를 전달/확인 하는 프로토콜 메시지.
- ✓ **Manual/Force switch**
  관리자가 임의로 링 포트를 차단하는 것

7.1.2. ERPS timers

- ✓ **Wait To Restore (WTR) Timer**
  Link flapping 을 방지하기 위해 RPL Owner 에 설정되는 타이머. Link 장애가 복구되면 WTR 동안 기다린 후 원래(Idle) 상태(RPL 이 차단된 상태)로 되돌아 간다.
- ✓ **Guard Timer**
  Link 장애가 복구 되었을 때 Guard 타이머가 시작된다. Guard 타이머 만료 전까지는 수신한 R-APS 를 처리하거나 전달하지 않는다. 이와 같은 동작으로 유효하지 않은 R-APS 메시지를 처리하지 않도록 한다.
- ✓ **Hold-off Timer**
  Link 장애가 감지 되었을 때 Hold-off 타이머가 시작 된다. Hold-off 타이머 만료 전 까지 ERPS 는 Link 장애에 대한 동작을 하지 않고, hold-off 타이머가 만료 되었을 때 Link 장애에 대한 동작을 한다. 이는 Link flapping 이 심하게 발생 할 경우 불필요한 ERPS 상태 변화를 방지 한다.
- ✓ **Wait To Block (WTB) Timer**
  WTB 와 유사하다. EPRS 의 상태가 Manual/Force Switch 에서 관리자가 Manual/Force Switch 를 clear 하면 WTB 타이머가 시작되고, WTB 타이머가 만료되면 PRL 차단(Idle) 상태로 되돌아 온다.

7.1.3. ERPS 모드

- ✓ **복귀 모드 (Revertive mode)**
  Link 의 장애가 복구되면 WTR 타이머가 시작되어 타이머가 만료되면 다시 RPL 이 차단되어 원래(Idle) 상태로 되돌아 가게 되는데, 이렇게 Link 장애가 복구되면 원래 상태로 되돌아 가는

ERPS 모드를 복귀 모드라고 한다.

- ✓ **비복귀 모드 (Non-revertive mode)**
  비복귀 모드에서는 Link 장애가 복구되어도 WTR 타이머가 시작되지 않고 현 상태를 계속 유지한다.

7.1.4. ERPS 상태

- ✓ **Idle**
  Link 장애가 없고 RPL 이 차단된 상태
- ✓ **Protection**
  Link 장애가 발생하여 RPL 의 차단이 해제된 상태
- ✓ **Manual Switch**
  관리자에 의해 하나의 링 포트가 차단된 상태
- ✓ **Force Switch**
  관리자에 의해 하나 이상의 링 포트가 차단된 상태
- ✓ **Pending**
  Link 장애는 없지만 RPL 이 차단해제 상태이고 RPL 이 아닌 다른 링 포트가 차단된 상태

7.1.5. ERPS 기본 동작

ERPS 는 모든 장비가 물리적으로 연결되어 있는 이더넷 링 환경에서 동작 하고, Automatic Protection Switching(APS) 프로토콜을 사용하여 이더넷 링을 보호한다. 각 노드는 인접한 각 노드와 각각 링 포트로 연결 되고, 표준 FDB (Filtering database) MAC learning, forwarding, port blocking/unblocking(포트 차단/해제)을 지원한다.
Loop 을 방지하기 위해 Idle 상태에서는 RPL 이 항상 차단 된 상태 이다. Link 장애를 감지하면 다른 링 노드에 Link 장애를 알리기 위해 SF(Signal Failure) 메시지를 전송한다. 이런 상태를 'Protection' 상태라고 한다. Protection 상태에서는 PRL 의 차단이 해제되어 트래픽 전달 경로가 변경된다. 이렇게 PRL 의 상태를 차단/해제 하는 링 노드를 RPL Owner 라고 한다.

7.2. ERPS 설정

7.2.1. ERPS 기본 설정

ERPS 가 동작 하기 위해서는 Bridge 와 이 Bridge 에 VLAN 생성이 필요하다. Bridge 와 VLAN 생성은 VLAN 설정과 Provider Bridge 설정 매뉴얼을 참조하라. ERPS 는 2 개의 이더넷 인터페이스가 필요하며 g8032-config-vlan 노드에서는 Control plane VLAN 과 Data plane VLAN 을 설정하고, g8032-config-switch 노드에서 ERPS 동작과 관련된 기능을 설정한다. ERPS 를 동작시키려면 아래와 같이 설정 한다.

표 7-1. ERPS 기본 설정

	명령어	*설명*
Step 1	Switch (config) # **bridge 1 protocol provider-bridge**	Bridge 를 생성 한다.
Step 2	Switch (config) # **vlan database**	VLAN 을 설정하기 위해 VLAN 노드로 진입한다.
Step 3	Switch (config-vlan) # **vlan 10 type service point-point bridge 1** Switch (config-vlan) # **vlan 20 type service point-point bridge 1**	Bridge 에 VLAN 을 생성한다.
Step 4	Switch (config) # **bridge 1 g8032 ring-id 1 east-interface gi2/1 west-interface gi2/2 instance 1**	생성된 Bridge 에 Ring ID 와 Ring port 를 지정하여 Ring instance 를 생성 한다.
Step 5	Switch (config) **# g8032 configure vlan ring-id 1 bridge 1**	Ring 의 control-vlan, service-vlan 을 설정하기 위해 g8032 vlan 노드로 진입한다.
Step 5	Switch (g8032-config-vlan) # **g8032 control-vlan 10** Switch (g8032-config-vlan) # **g8032 service-vlan 20**	Ring 프로토콜 통신 목적의 control-vlan 과 traffic service 목적의 service-vlan 을 설정 한다.
Step 7	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 8	Switch (g8032-config-switch) **# g8032 meg-level 7**	MEG level 을 설정 한다.
Step 9	Switch (g8032-config-switch) **# g8032 rpl owner east-interface** or Switch (g8032-config-switch) **# g8032 rpl non-owner**	RPL owner 또는 RPL non-owner 설정을 한다.

7.2.2. Wait-to-Restore(WTR) Timer 설정

Wait-to-Restore(WTR) 타이머 값은 Link 장애상태에서 장애가 복구 되었을 때 RPL Owner 가 RPL 을 다시 차단할 때까지 기다리는 시간이다. WTR 은 Link flapping 에 의한 불필요한 트래픽 경로 변경을 방지 한다. WTR 의 default 값은 5 분이고 1 분 단위로 설정 할 수 있다. Wait-to-Restore 타이머는 다음과 같이 설정 한다.

표 7-2. WTR timer 설정

	명령어	*설명*
Step 1	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 2	Switch (g8032-config-switch) **g8032 timer wait-to-restore 1**	WTR timer 를 1 분으로 설정 한다.
Step 3	Switch (g8032-config-switch) **# end**	

7.2.3. Guard Timer 설정

Guard 타이머가 동작하는 동안은 수신 한 모든 R-APS 메시지를 처리하지 않는다. 이는 이더넷 링에 존재하는 유효하지 않은 R-APS 메시지 처리를 방지한다. Guard 타이머의 default 값은 500ms 이며 10ms 단위로 설정 할 수 있다. Guard 타이머는 다음과 같이 설정 한다.

표 7-3. Guard timer 설정

	명령어	*설명*
Step 1	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 2	Switch (g8032-config-switch) **g8032 g8032 timer guard-timer 100**	Guard timer100 100ms 로 설정 한다.
Step 3	Switch (g8032-config-switch) **# end**	

7.2.4. ERPS 모드 설정

ERPS 는 Protection 상태에서 장애가 복구 되었을 때 RPL 을 차단하는 복귀 모드와 현재 상태를 계속 유지하는 비복귀 모드 두 가지가 있다. ERPS 모드는 Default 복귀 모드이며 다음과 같이 설정 한다.

표 7-4. ERPS 모드 설정

	명령어	*설명*
Step 1	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 2	Switch (g8032-config-switch) **no g8032 revertive-mode**	ERPS 모드를 비복귀(Non-revertive) 모드로 설정한다.
Step 3	Switch (g8032-config-switch) **g8032 revertive-mode**	ERPS 모드를 복귀(Revertive mode)로 설정한다.
Step 4	Switch (g8032-config-switch) **# end**	

7.2.5. CFM CCM 연동 설정

ERPS 는 CCM Fail/OK 에 의해서 Link Fail/OK 를 감지 할 수 있다. ERPS 는 Down MEP 만 연동 가능하며 Port-channel 또는 VLAN 인터페이스가 아닌 링 포트에 모두 MEP 설정이 있어야 한다. MEP 설정은 CFM 매뉴얼을 참고 한다. CCM 연동 설정은 Default Disable 이다.

표 7-5. CFM CCM 연동 설정

	명령어	*설명*
Step 1	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 2	Switch (g8032-config-switch) **g8032 md-name TEST service-id TESTMA**	Ring port 와 MEP Binding 설정을 한다.
Step 3	Switch (g8032-config-switch) **g8032 ethoam-event**	CCM 연동 설정을 한다.
Step 4	Switch (g8032-config-switch) **# end**	

7.2.6. Manual/Force switch 설정

ERPS 는 임의로 링 포트를 차단 상태로 만들 수 있다. Manual switch 는 이더넷 링에서 한 Link 만 차단 상태로 설정 할 수 있지만, Force switch 는 여러 Link 를 차단 상태로 설정 할 수 있다. Manual/Force switch 는 다음과 같이 설정 한다.

표 7-6. Manual/Force switch 설정

	명령어	*설명*
Step 1	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 2	Switch (g8032-config-switch) **g8032 manual east-interface**	East Ring port 에 manual switch 설정을 한다.
Step 3	Switch (g8032-config-switch) **g8032 force west-interface**	West Ring port 에 force switch 설정을 한다.
Step 4	Switch (g8032-config-switch) **# end**	

7.3. 이종(Metro) Ring 연동 설정

CS3400 의 ERPS 는 Sub ring 설정을 통해 ERPS 를 사용하지 않는 링 네트워크와 연동이 가능 하다. 그림 1 과 같은 이더넷 링 구성에서 MRT A 와 COT1, MRT B 와 COT2 사이에 Sub Ring 을 구성하면 Normal(Idle) 상태에서 MRT A - COT1 또는 MRT B - COT2 Link 가 차단 상태이기 때문에 Loop 를 방지할 수 있다.

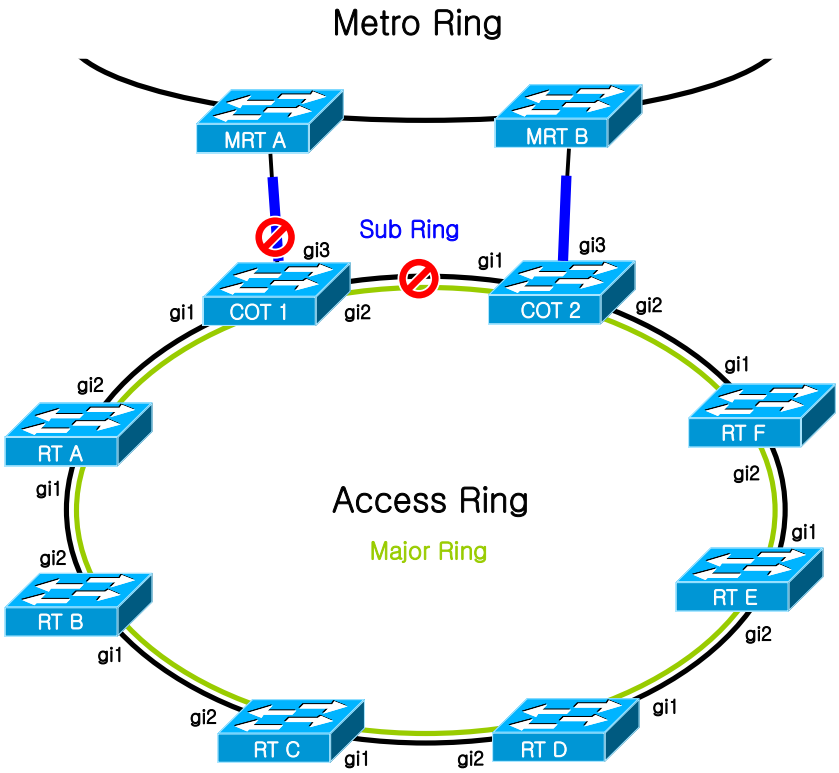


그림 7-1. 이종 Ring 과의 연동

그림 1 과 같이 링 구성을 하려면 먼저 Access Ring(Major Ring)에 ERPS 설정하고 COT1 과 COT2 에 ERPS(Sub Ring)를 설정 한다.

7.3.1. COT 노드 설정

Major Ring 설정

COT 노드의 Major Ring 에는 COT 노드의 명시적 설정과 COT Neighbor port 에 대한 명시적 설정을 해야 한다. 이 것은 이종(Metro) Ring 과의 회선 이중화를 위한 정보이며 반드시 COT 노드 Major ring 에 설정 해야 한다. 그림 1 의 COT1 Major Ring 은 아래와 같이 설정 한다.

표 7-7. Major Ring 설정

	명령어	*설명*
Step 1	Switch (config) # **bridge 1 g8032 ring-id 1 east-interface gi1 west-interface gi2 instance 1**	생성된 Bridge 에 Ring ID 와 Ring port 를 지정하여 Ring instance 를 생성 한다.
Step 2	Switch (config) **# g8032 configure vlan ring-id 1 bridge 1**	Ring 의 control-vlan, service-vlan 을 설정하기 위해 g8032 vlan 노드로 진입한다.
Step 3	Switch (g8032-config-vlan) # **g8032 control-vlan 10** Switch (g8032-config-vlan) # **g8032 service-vlan 100**	Ring 프로토콜 통신 목적의 control-vlan 과 traffic service 목적의 service-vlan 을 설정 한다.
Step 4	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 5	Switch (g8032-config-switch) **# g8032 meg-level 7**	MEG level 을 설정 한다.
Step 6	Switch (g8032-config-switch) **# g8032 rpl owner east-interface**	RPL owner 설정을 한다.
Step 7	Switch (g8032-config-switch) **# g8032 cot-node**	COT 노드 설정을 한다.
Step 8	Switch (g8032-config-switch) **# g8032 cot-neighbour-port west-interface**	COT Neighbor port 를 COT2 와 인접한 port 로 설정 한다.
Step 9	Switch (g8032-config-switch) **# end**	

Sub Ring 설정

COT 노드의 Sub Ring 에는 연동 할 Major Ring 을 명시하고, Sub Ring topology 가 변경 되었을 경우 Major Ring 에 topology 변화를 알려주기 위한 설정을 해야 한다. 그림 1 의 COT1 의 Sub Ring 은 아래와 같이 설정 한다.

표 7-8. Sub Ring 설정

	명령어	*설명*
Step 1	Switch (config) # **bridge 1 g8032 ring-id 2 east-interface gi3 west-interface vlan20 instance 2**	생성된 Bridge 에 Ring ID 와 Ring port 를 지정하여 Ring instance 를 생성 한다.
Step 2	Switch (config) **# g8032 configure vlan ring-id 2 bridge 1**	Ring 의 control-vlan, service-vlan 을 설정하기 위해 g8032 vlan 노드로 진입한다.
Step 3	Switch (g8032-config-vlan) # **g8032 control-vlan 20** Switch (g8032-config-vlan) # **g8032 service-vlan 100**	Ring 프로토콜 통신 목적의 control-vlan 과 traffic service 목적의 service-vlan 을 설정 한다.
Step 4	Switch (config) **# g8032 configure switching ring-id 2 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 5	Switch (g8032-config-switch) **# g8032 meg-level 7**	MEG level 을 설정 한다.
Step 6	Switch (g8032-config-switch) **# g8032 rpl owner east-interface**	RPL owner 설정을 한다.
Step 7	Switch (g8032-config-switch) **# g8032 major-ring 1**	Major Ring 을 Ring ID 1 로 설정한다.
Step 8	Switch (g8032-config-switch) **# g8032 propagate-tc**	Sub Ring Topology 가 변화 하였을 때 Major Ring 으로 알려주는 Propagation Topology Change 설정을 한다.
Step 9	Switch (g8032-config-switch) **# end**	

Notice	Sub Ring 의 다른 한 포트는 Sub Ring control-vlan 인터페이스로 설정 한다. Sub Ring 의 control-vlan 을 Traffic service 목적으로 사용하거나 Major Ring 의 service-vlan 으로 설정 해서는 안 된다.

7.3.2. COT Neighbor 노드 설정

COT 에 바로 인접한 노드(RT A, RT B)에는 COT Neighbor 포트 설정을 해 주어야 한다. COT Neighbor 노드는 COT 노드가 Down 되었을 때 다른 COT 노드로 COT Down 을 알려주어서 Traffic service 가 계속 유지 되도록 해 준다. 그림 1 의 RT A Ring 을 다음과 같이 설정 한다.

표 7-9. COT Neighbor 노드 설정

	명령어	*설명*
Step 1	Switch (config) # **bridge 1 g8032 ring-id 1 east-interface gi1 west-interface gi2 instance 1**	생성된 Bridge 에 Ring ID 와 Ring port 를 지정하여 Ring instance 를 생성 한다.
Step 2	Switch (config) **# g8032 configure vlan ring-id 1 bridge 1**	Ring 의 control-vlan, service-vlan 을 설정하기 위해 g8032 vlan 노드로 진입한다.
Step 3	Switch (g8032-config-vlan) # **g8032 control-vlan 10** Switch (g8032-config-vlan) # **g8032 service-vlan 100**	Ring 프로토콜 통신 목적의 control-vlan 과 traffic service 목적의 service-vlan 을 설정 한다.
Step 4	Switch (config) **# g8032 configure switching ring-id 1 bridge 1**	Ring 동작설정을 위해 g8032 switching 노드로 진입한다.
Step 5	Switch (g8032-config-switch) **# g8032 meg-level 7**	MEG level 을 설정 한다.
Step 6	Switch (g8032-config-switch) **# g8032 rpl non-owner**	RPL Non-owner 설정을 한다.
Step 7	Switch (g8032-config-switch) **# g8032 cot-neighbour-port west-interface**	COT Neighbor port 를 COT1 와 인접한 port 로 설정 한다.
Step 8	Switch (g8032-config-switch) **# end**	

7.4. ERPS 상태 조회

표 7-10. ERPS 상태 조회 CLI

명령어	설명
Switch # **show g8032** [***bridge*** <1-32>] [***ring-id*** <1-65535>]	ERPS Overall 정보를 조회 한다..
Switch # **show g8032 brief**	ERPS brief 정보를 조회 한다.
Switch # **show g8032 traffic** [***bridge*** <1-32>] [***ring-id*** <1-65535>]	ERPS R-APS 통계 정보를 조회 한다.

7.4.1. ERPS Overall 정보 조회

ERPS Overall 정보를 조회 하려면 Exec 노드에서 **"show g8032"** 명령어를 입력 한다. 표시 되는 정보는 다음과 같다.

```
Switch#show g8032

RING3
  Node ID 0007.729e.0002                                    → 노드 ID
  This node is RPL Owner                                    → RPL Owner 유무를
나타냄
  DNF status is False                                       → DNF의 상태를 나타냄
  ERPS version 2                                             → ERPS 버전 정보
  This ring is operated in Non-Revertive mode             → ERPS 모드
  This ring is Sub-Ring of Ring 1                           → Sub Ring을 나타냄
  Topology Change Propagation is Enabled                  → TC 설정

  Control VLAN is Vlan4013                                  → Control Vlan
  Service VLAN  Vlan1012 Vlan1011 Vlan1200 Vlan1100       → Service Vlan

  Timer    Wait-to-restore    0 sec                         → WTR time
           Wait-to-block      5 sec                         → WTB time
           Holdoff Timer      0 msec                        → Hold-off time
           Guard Timer        500 msec                      → Guard Time

  Current  Node state is Idle                               → 현재 ERPS 상태
           Event is WTR Expires                             → 이전에 발생한
Event

Name                 Port Role  Link Sts  Shared  Node ID          BPR
---------------- ---- ----  ---- ---  ------  -------------- -------
Port-channel1     East  RPL   up   BLK          0000.0000.0000 0(east)
Vlan4013           West        up   FWD          0000.0000.0000 0(east)
```

7.4.2. ERPS 요약 정보 조회

ERPS 의 요약된 정보를 조회 하려면 Exec 노드에서 **“show g8032 brief”** 명령어를 입력 한다. 표시 되는 정보는 다음과 같다.

```
Switch#Show g8032 brief

Bridge   RING  VLAN State RPL  East      Sts  West      Sts  WTR WTB Guard Holdoff
10         1     4011 Pend        Gi2/1!   FWD  Gi3/1     FWD  0    0    0      0


Brige     : ERPS가 설정된 Bridge
RING      : Ring ID
VLAN      : Control Vlan
State     : ERPS의 현재 상태
RPL       : RPL Owner 표시
East      : East Ring port
West      : West Ring port
Sts       : Ring port의 상태
WTR       : 남은 WTR time
WTB       : 남은 WTB time
Guard     : 남은 Guard time
Holdoff : 남은 Holdoff time
```

7.4.3. ERPS R-APS 통계 정보 조회

ERPS R-APS 통계 정보를 조회 하려면 Exec 노드에서 **“show g8032 traffic”** 명령어를 입력 한다. 표시 되는 정보는 다음과 같다.

```
Switch#Show g8032 brief

Bridge 10

Ring 1

 East Gi2/1
        SF          NR          FS          MS          Event
Rx   : 193         12621       0           3324        0
Tx   : 0           3            0           0           0

 West Gi3/1
        SF          NR          FS          MS          Event
Rx   : 214         12621       0           3327        0
Tx   : 0            3           0           0           0
```

8 LLDP

(Link Layer Discovery Protocol)

이 장에서는 LAN 에 연결된 네트워크 장비의 정보를 수집하기 위해 IEEE 802.1AB LLDP (Link Layer Discovery Protocol)를 설정하는 방법에 대해 설명한다.

8.1. Information About LLDP

8.1.1. LLDP overview

LLDP (Link Layer Discovery Protocol)는 Layer 2 data-link 계층에서 사용하는 프로토콜로장비의 정보를 네트워크로 전송한다. LLDP는 단방향 프로토콜로서 LLDP가 설정된 장비는 현재 장비의 상태, 인터페이스 상태 그리고 장비의 capability와 같은 정보들을 전송한다.
LLDP는 네트워크 장비 정보를 수집하기 위해 LLDPDU(LLDP Data Unit)를 사용한다. LLDPDU는 TLV(Type, Length, Value)들로 구성되어 있다. TLV들은 IEEE 802.1AB에 정의되어 있다.
LLDPDU에 반드시 포함되어야 하는 세개의 필수 TLV는 아래와 같다. 이 세개의 TLV는 반드시 순서대로 포함되어야 한다.

1) Chassis ID TLV

2) Port ID TLV

3) Time To Live TLV

세 개의 필수 TLV를 포함시키고 그 뒤로는 필요에 따라 TLV를 선택해서 포함 시킬 수 있다.

8.2. LLDP Guidelines and Limitations

LLDP를 설정할 때 유의할 점은 다음과 같다::

- ✓ 인터페이스 별로 LLDP 를 활성/비활성 할 수 있다.
- ✓ 물리 인터페이스에서만 LLDP 를 지원한다.
- ✓ L2 인터페이스에만 설정이 가능하다.

8.3. Default Settings

다음의 표는 default LLDP 설정을 나타낸다:

Feature	*Default Setting*
LLDP receive	Disable
LLDP transmit	Disable
LLDP timer	30 seconds
LLDP TLV	Disable

8.4. Configuring LLDP

LLDP 는 인터페이스 설정 모드에서 기능을 활성/비활성할 수 있다.

이 장에서는 다음과 같은 절차를 설명한다:

- LLDP enable or disable
- Configuring Optional LLDP parameters
- Verifying the LLDP configuration

8.4.1. LLDP enable or disable

다음은 인터페이스에서 LLDP 기능을 활성/비활성 하는 방법을 설명한다.

	Command or Action	*Purpose*
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입한다
Step 2	**interface** *interface-name*	Interface configuration 모드로 진입한다.

	예제: Switch(config)# **interface gi2/1**	
Step 3	**switchport** 예제: Switch(config-if-Gi2/1)# **switchport**	인터페이스를 L2 모드로 설정한다. **NOTE** 자세한 설정 정보는 "제 03 장 인터페이스 환경 설정" chapter 에서 참고할 수 있다
Step 4	**lldp transmit** 예제: Switch(config-if-Giga2/1)# **lldp transmit**	인터페이스에 LLDP 전송을 enable 한다.
Step 4	**lldp receive** 예제: Switch(config-if-Giga2/1)# **lldp receive**	인터페이스에 LLDP 수신을 enable 한다.
Step 5	**end** 예제: Switch(config-if-Giga2/1)# **end**	privileged EXEC 모드로 돌아간다

8.4.2. Configuring optional LLDP parameters

LLDP 정보를 전송하는 시간 주기와 같은 LLDP parameter 를 설정 할 수 있다.

	Command or Action	***Purpose***
	configure terminal 예제: Switch# **configure terminal**	Global configure 모드로 진입한다
	lldp timer 예제: Switch(config)# **lldp timer 10**	LLDP Data Unit 전송 주기를 변경한다. 이 설정으로 LLDP update 정보 주기를 변경할 수 있다.
	lldp system-name *NAME* 예제: Switch(config)# **lldp system-name LLDP**	LLDP 에서 사용할 system name 을 지정한다.
	interface *interface-name* 예제: Switch(config)# **interface gi2/1**	Interface configuration 모드로 진입한다.
	lldp tlv-select *tlv* 예제: Switch(config-if-Giga2/1)# **lldp tlv-select system-name**	LLDP 로 전송할 TLV 를 선택한다. **NOTE** lldp 를 enable 하면 default 로 mandatory TLV 인 lldp tlv-select chassis-id port-id ttl 가 설정된다.
	end	privileged EXEC 모드로 돌아간다

	예제: Switch(config-if-Giga2/1)# **end**

8.4.3. Verifying the LLDP configuration

LLDP 의 설정 정보나, LLDP 를 통해 수집한 네트워크 장치에 대한 정보를 확인 할 수 있다.

	Command or Action	*Purpose*
	show lldp interface *IFNAME*	인터페이스에 LLDP 설정 여부와, 인터페이스 mac address 정보를 보여준다.
	show lldp neighbor interface *IFNAME*	인터페이스와 연관 있는 LLDP neighbor 정보를 보여준다.
	Show lldp traffic *(IFNAME)*	인터페이스 별로 LLDP traffic 통계 정보를 보여준다.

8.5. LLDP Configuration Samples

다음의 예제는 CS3400 인터페이스에 LLDP 를 설정하고, LLDP 정보를 update 하기 위해서 LLDP 프레임 전송 주기를 변경하는 방법을 보여준다.

```
Switch# configure terminal
Swtich(config)# interface gi2/1
Switch(config-if-Giga2/1)# lldp receive
Switch(config-if-Giga2/1)# lldp transmit
Switch(config-if-Giga2/1)# exit
Switch(config)# lldp timer 60
```

스위치의 설정을 조회하면 다음과 같다.

```
!
lldp timer 60
!
interface Giga2/1
 lldp receive
 lldp transmit
 lldp tlv-select chassis-id port-id ttl
!
```

인터페이스에 LLDP 설정 정보를 조회하면 결과는 다음과 같다.

```
Switch#show lldp interface GigabitEthernet 2/1
```

```
Interface Information:
  Enable (TX/RX): Y/Y
  Port MAC address: 0007.729e.ab17
  Neighbors count: 1
```

Remote LLDP 로부터 수신한 정보를 조회하면 다음과 같다.

```
Switch#show lldp neighbor GigabitEthernet 2/1
Remote LLDP Neighbor Information:
MAC Address: 0007.729e.11ab
Chassis MAC Address: 0007.729e.11ab
  TTL: 120 (113 second(s) expired)
Interface Number: 0
  Port Vlan ID: 0
  AutoNego Support:
  AutoNego Capability: 0
  Operational MAU Type: 0
  Link Aggregation Capability:
  Link Aggregation Status: Disabled
  Link Aggregation Port ID: 0
  Max Frame Size: 0
  System Capabilities:
  System Capabilities Enabled:
```

9

Link Aggregation Control Protocol

이 장에서는 port-group을 구성하기 위해 스위치에 IEEE 802.3ad Link Aggregation Control Protocol(LACP)를 설정하는 방법을 설명한다.

Notice 이 장에서 사용되는 명령어에 대한 문법과 사용방법에 관한 정보는 command reference 를 참조하라.

이 장은 다음의 절로 구성된다:

- Link Aggregation Control Protocol 개관
- 802.3ad LACP, static link aggregation 설정
- 802.3ad 통계 및 상태 표시

9.1. Link Aggregation Control Protocol 개관

Link Aggregation Control Protocol (LACP)는 IEEE 802.3ad 에 기술 되어 있는 프로토콜로 여러 개의 물리적 interface 를 하나의 logical interface 로 묶어서 사용할 수 있게 해준다. 상대편 장비와 연결된 interface 에서 서로 LACP 패킷 (LACPDU)을 주고 받으며 해당 interface 가 logical interface 에 포함되는 여부를 판단한다.

이 절에서는 다음 항목을 설명한다:

- LACP 동작 원리
- LACP Modes
- LACP Parameters

9.1.1. LACP 동작 원리

LACP 는 연결된 두 장비 모두 설정이 되어 있어서 LACPDU 를 주고 받으며 interface 의 상태를 정하고 Link Aggregation 을 결정한다. LACP 가 설정된 interface 는 LACPDU 를 통해 여러 상태를 지나게 되고 두 장비가 서로 조건이 맞을 경우 Link Aggregation 이 일어 난다. LACP 가 설정이 되면 logical interface 가 생성 된다. LACPDU 를 받은 interface 는 연결된 장비가 LACP 가 설정 되어 있다는 것을 파악한 후 자신의 LACPDU 전송 주기를 확인하고 그에 맞게 LACPDU 를 전송한다. 그리고 LACPDU 를 통해 받은 정보와 interface 가 가지고 있는 정보가 일치하는 지를 확인하고 일치 할 경우 logical interface 에 해당 물리적 interface 를 연결한다.

9.1.2. LACPDU 구성

LACPDU 는 전송하는 interface 의 정보와 상대편의 정보를 가진다. 이 정보들을 이용해서 각 interface 에서 정보를 저장하고 이 값을 다음에 도착하는 LACPDU 와 비교한다. 다음 표는 LACPDU 에 포함되는 정보들을 나타낸다.

field	*description*
Actor_System_Priority	장비에 설정된 priority
Actor_System	장비의 MAC 값과 priority 로 만든 ID
Actor_Key	logical interface 의 ID
Actor_Port_Priority	Port 의 priority
Actor_Port	Port 의 index
Actor_State	Port 의 상태를 bit 으로 나타낸 값
Partner_System_Priority	상대편 장비의 system priority
Partner_System	상대편 장비의 system ID
Partner_Key	상대편 장비의 logical interface 의 ID
Partner_Port_Priority	상대편 Port 의 priority
Partner_Port	상대편 Port 의 index
Partner_State	상대편 Port 의 상태

표 9-1 LACPDU 에 포함되는 정보

9.1.3. LACP Modes

CS3400 series 는 port group 을 수동으로 구성할 수 있고, IEEE 802.3ad LACP(Link Aggregation Control Protocol)를 사용하여 자동으로 구성할 수도 있다.

LACP 로 port group 을 구성하려면, active 나 passive 모드를 사용하면 된다. 적어도 링크의

한쪽은 active 모드로 설정되어 있어야 한다. Passive 모드의 포트는 LACP 패킷을 먼저 전송하지 않고 LACP 패킷을 수신했을 경우에 LACP 패킷을 전송하기 시작한다.

LACP 에서 가능한 모드

Mode	Description
on	LACP 에 의해 포트 그룹이 생성되지 않고 static 한 포트 그룹이 생성된다.
passive	포트를 passive 협상 모드로 설정한다. Passive 모드의 포트는 먼저 LACP 패킷을 전송하여 협상을 시작하지 않고, LACP 패킷을 수신했을 때 응답만 한다.
active	포트를 active 협상 모드로 설정한다. Active 모드의 포트는 LACP 패킷을 전송함으로써 협상을 시작한다.

9.1.4. LACP 에 사용되는 정보

LACP 의 설정에 사용되는 인자들은 다음과 같다:

- System Priority
  LACP 가 동작하는 각 스위치에는 자동으로 혹은 CLI 를 통해서 system priority 를 할당해야 한다. System priority 는 스위치의 MAC 주소와 같이 사용되어 system ID 를 구성하고, 다른 시스템과의 협상에 사용된다.

- Port Priority
  스위치의 각 포트에는 자동으로 혹은 CLI 를 통해서 port priority 를 할당해야 한다. Port priority 는 포트 번호와 함께 port identifier 를 구성한다. Port priority 는 하드웨어의 제약 때문에 적합한 모든 포트가 통합될 수 없을 때, standby 모드로 만들 포트를 결정하기 위해 사용된다.

- Administrative key
  - 스위치의 각 포트는 그 포트의 성질에 따라 자동으로 administrative key 값을 할당 받는다. Administrative key을 결정하는 성질은 bandwidth, vlan id, duplex, mtu 등이 있고 이 값이 같은 경우에만 같은 logical interface에 속할 수 있다.

LACP 가 활성화되면, LACP 는 항상 통합 가능한 최대 개수의 포트를 통합하려 시도한다. 만약 통합 가능한 모든 포트들을 통합할 수 없다면, 통합되지 않은 모든 포트들은 hot standby 상태에 놓이게 되며 통합된 다른 포트에 고장이 발생했을 경우에만 사용된다.

9.2. 802.3ad Link Aggregation Control Protocol

and Static Link Aggregation 설정

이 절에서는 LACP 로 port group 을 구성하는 방법을 설명한다:

- System Priority 설정
- Port Priority 설정
- Administrative Key Value 설정
- Timeout Value 설정
- LACP and static port group 설정
- LACP Statistics 삭제

9.2.1. System Priority 설정

System priority 의 값은 1 과 65535 사이의 정수 값이어야 한다. 숫자가 클수록 낮은 우선순위를 나타낸다. default priority 는 32768 이다.

LACP System priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Step2	**lacp system-priority** *priority*	system priority 를 설정한다.
Step3	**end**	privileged EXEC 모드로 변경한다.
Step4	**show lacp sys-id**	설정 내용을 확인한다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

설정한 system priority 를 default 설정으로 복구하려면 global configuration 명령 **no lacp system-priority** 를 사용하라

다음은 system priority 를 20000 으로 설정하는 방법을 보여준다:

Switch# **configure terminal**
Switch(config)# **lacp system-priority 20000**
Switch(config)# **end**

9.2.2. Port Priority 설정

Port priority 의 값은 1 과 65535 사이의 정수 값이어야 한다. 숫자가 클수록 낮은 우선순위를 나타낸다. default priority 는 32768 이다.

Port priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	LACP 를 port priority 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	**lacp port-priority** *priority*	port priority 를 설정한다.
Step4	**end**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

설정한 port priority 를 default 설정으로 복구하려면 interface configuration 명령 **no lacp port-priority** 를 사용하라

다음은 인터페이스 gi1/1 의 port-priority 를 10 으로 설정하는 예이다:

Switch# **configure terminal**
Switch(config)# **interface Giga1/1**
Switch(config-if-Giga1/1)# **lacp port-priority 10**
Switch(config)# **end**

9.2.3. Timeout Value 설정

포트별로 LACPDU 의 전송 주기를 설정할 수 있다. 전송주기는 short (1 초)나 long (30 초)으로 설정할 수 있다.

Notice **lacp timeout** 명령은 설정하는 스위치가 아닌 상대 스위치의 LACPDU 전송 주기에 영향을 미친다.

LACPDU 의 전송 주기를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**Interface** *interface-id*	LACPDU 전송주기를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.

Step3	**lacp timeout {short|long}**	LACPDU 전송주기를 설정한다.
Step4	**End**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

설정한 LACPDU 전송주기를 default 로 복구하려면, interface configuration 명령 **no lacp timeout** 을 사용하라.

다음은 인터페이스 gi1/1 과 연결된 상태 시스템의 LACPDU 전송주기를 short 로 설정하는 예이다:

Switch# **configure terminal**
Switch(config)# **interface Giga1/1**
Switch(config-if- Giga1/1)# **lacp timeout short**
Switch(config)# **end**

9.2.4. LACP and static port group 설정

인터페이스에서 LACP 를 설정할 수 있다.

LACP 모드를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	**Purpose**
Step1	**Configure terminal**	Global configuration 모드로 진입한다.
Stpe2	**interface** *interface-id*	LACP 모드를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	**Channel-group** *po-id* **mode {active|on|passive}**	Port group 모드를 설정한다. Active 와 Passive 는 LACP mode 이고 on 은 static port group 이다.
Step4	**End**	privileged EXEC 모드로 변경한다.
Step5	**show running-config**	설정 내용을 확인한다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장한다.

다음은 인터페이스 Giga1/1 를 port-group 1 의 맴버로 등록 하는 예이다.

Switch# **configure terminal**
Switch(config)# **interface Giga1/1**
Switch(config-if- Giga1/1)# **channel-group 1 mode active**
Switch(config)# **end**

LACP 에 의해서가 아닌 static 으로 port-group 을 생성 할 경우는 다음과 같다

Switch# **configure terminal**
Switch(config)# **interface Giga1/1**
Switch(config-if- Giga1/1)# **channel-group 1 mode on**
Switch(config)# **end**

9.2.5. LACP Statistics 삭제

LACP 의 통계 정보를 삭제하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	**clear lacp** [*aggregator-id*] **counters**	해당 port group 의 LACP 통계 정보를 삭제한다.
Stpe2	**show lacp counters**	변경 내용을 확인한다.

다음은 port group 1 의 LACP 를 통계정보를 삭제하는 예이다:

Switch# **clear lacp 1 counters**

9.3. 802.3ad 통계 및 상태 표시

CS3400 series 는 모든 포트 그룹에 대한 정보를 확인하는 여러 명령어를 제공한다.

Command	Purpose
show etherchannel	port group 의 ID 연결된 포트의 수 등 전반적인 정보를 제공.
show etherchannel summary	Port group 과 연결된 포트의 정보를 간결하게 제공
show etherchannel detail	Port group 과 연결된 포트의 정보를 자세하게 제공

다음은 static 한 port group 이 설정된 정보를 확인하는 예이다

```
shu#show etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 1   Max Maxports = 8
Port-channels: 1 Max Port-channels = 8
Protocol=    -


shu#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
Number of channel-groups in use: 1
```

```
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------------------
1      Po1(SD)         -        Gi1/1(D)

shu#show etherchannel detail
               Channel-group listing:
               ----------------------

Group: 1
----------
Group state = L2
Ports: 1   Max Maxports = 8
Port-channels: 1 Max Port-channels = 8
Protocol=    -
               Ports in the group:
               -------------------
Port: Gi1/1
------------

Port state    = Down Not-in-Bndl
Channel group = 1              Mode = On         Gcchange = -
Port-channel  = NULL           GC   = -          Pseudo port-channel= Port-chan
nel1
Port index    = 0              Load = 0x00
Protocol      = -

Age of the port in the current state: 0d:16h44m24s


               Port-channels in the group:
               ----------------------
Port-channel: Port-channel1
-------------
Age of the Port-channel = 0d:0h0m18s
Number of ports = 0
GC              = 0x00000000   HotStandBy port= null
Port state      = Down Ag-Not-Inuse
Protocol        = -
shu#
```

모든 포트 그룹에 대한 LACP 통계를 조회하려면, privileged EXEC 명령 **show lacp counters** 를 사용하라.

특정 포트 그룹에 대한 LACP 통계를 조회하려면, privileged EXEC 명령 **show lacp** *aggregator-id* **counters** 를 사용하라.

스위치의 LACP 프로토콜 정보와 상태를 조회하려면, privileged EXEC 명령 **show lacp internal** 을 사용하라. 상대 시스템의 LACP 프로토콜 정보와 상태를 조회하려면, privileged EXEC 명령 **show lacp neighbor** 을 사용하라.

출력 결과물의 항목에 대한 상세정보는 command reference 를 참고하라.

10

IGMP Snooping

본 장에서는 IGMP Snooping 설정에 대해 설명한다.

10.1. IGMP Snooping 개요

멀티캐스트 트래픽은 Unknown MAC address 나 브로드캐스트 프레임으로 처리되어 VLAN 에 속한 모든 포트로 플러딩(flooding) 된다.

IGMP Snooping 은 멀티캐스트 트래픽을 VLAN 에 포함된 모든 포트로 전달하지 않고, 멀티캐스트 트래픽을 전달할 인터페이스들을 동적으로 추가/삭제함으로써 네트워크 대역폭을 효율적으로 사용할 수 있도록 해준다. IGMP Snooping 은 IGMP 호스트와 멀티캐스트 라우터 사이에서 송수신되는 IGMP 메시지를 snooping 하여, 멀티캐스트 그룹과 VLAN 포트 정보를 수집한다.

IGMP Snooping 의 절차에 대해서 간략히 설명하면 다음과 같다. 특정 멀티캐스트 그룹에 대한 IGMP Join 메시지를 받으면, 해당 IGMP 호스트가 연결된 VLAN 포트를 Multicast Forwarding Table Entry 에 추가한다. 그 IGMP 호스트로부터 IGMP Leave 메시지를 받으면 반대로 그 IGMP 호스트와 연결된 VLAN 포트를 Multicast Forwarding Table Entry 에서 제거한다. 또한, 멀티캐스트 라우터로부터 수신되는 IGMP Query 메시지를 VALN 의 모든 포트로 전달한 후, IGMP Join 메시지를 받지 못해서 갱신되지 않은 Multicast Forwarding Table Entry 들을 삭제한다.

10.2. IGMP Snooping 설정

10.2.1. Enable IGMP Snooping on a VLAN

IGMP Snooping 은 VLAN 별로 설정할 수 있으며, 다음의 명령을 interface configuration mode 에서 사용한다.

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

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ip igmp snooping
Switch(config-if-Vlan22)# end
Switch# show ip igmp interface
......
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
    IGMP interface has 10 group-record states
     IGMP activity: 0 joins, 0 leaves
    IGMP querying router is 0.0.0.0
    IGMP query interval is 125 seconds
     IGMP querier timeout is 262 seconds
     IGMP max query response time is 25 seconds
     Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
  IGMP Last member query count is 2
     IGMP Snooping is enabled on this interface
     IGMP Snooping fast-leave is not enabled
     IGMP Snooping querier is not enabled
     IGMP Snooping report suppression is enabled
......
Switch#
```

10.2.2. Configure IGMP Snooping Functionality

다양한 IGMP Snooping 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행한다.

10.2.2.1. IGMP Report-Suppression

특정 VLAN Interface 에 IGMP Snooping 을 적용하면, IGMP Report-suppression 은 기본적으로 Enable 된 상태이며, IGMP Membership 마다 하나의 IGMP Report 만 Multicast Router 로 Forwarding 된다. IGMP Report-suppression 을 Disable 하면, 수신하는 모든 IGMP Report 들을 Multicast Router

로 Forwarding 한다.

이 기능은 IGMPv1 및 IGMPv2 메시지에 한해서 적용되며, 아래의 명령을 interface configuration mode 에서 실행한다.

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

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# no ip igmp snooping report-suppression
Switch(config-if-Vlan22)# end
Switch# show ip igmp interface
......
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
    IGMP interface has 10 group-record states
    IGMP activity: 0 joins, 0 leaves
    IGMP querying router is 0.0.0.0
    IGMP query interval is 125 seconds
    IGMP querier timeout is 262 seconds
    IGMP max query response time is 25 seconds
    Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
  IGMP Last member query count is 2
    IGMP Snooping is enabled on this interface
    IGMP Snooping fast-leave is not enabled
    IGMP Snooping querier is not enabled
    IGMP Snooping report suppression is disabled
......

Switch#
```

10.2.2.2. IGMP Fast-Leave

IGMP Fast-Leave 기능을 enable 하면 호스트로부터 IGMPv2 Leave 메시지를 받았을 때 해당 VLAN 의 Membership interface 를 Multicast forwarding table 에서 즉시 제거한다.

IGMP Fast-Leave 기능은 VLAN interface 의 각 포트에 호스트가 하나인 경우에만 사용하여야 한다.

만약, 포트에 여러 호스트가 속해 있는 경우에 이 기능을 사용하면. IGMPv2 Leave 메시지를 보내지 않은 호스트들도 일정시간 동안 Leave 가 된 멀티캐스트 그룹에 대한 트래픽을 받지 못하게 되는 경우가 발생하게 된다. 또한, 이 기능은 모든 호스트들이 Leave 메시지가 지원되는 IGMPv2 를 사용하는 경우에만 유효하다.

명령	설명
ip igmp snooping fast-leave	해당 VLAN 에 fast-leave 기능을 설정한다.
no ip igmp snooping fast-leave	해당 VLAN 에 설정된 fast-leave 를 해제한다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ip igmp snooping fast-leave
Switch(config-if-Vlan22)# end
Switch# show ip igmp interface
......
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
    IGMP interface has 10 group-record states
    IGMP activity: 0 joins, 0 leaves
   IGMP querying router is 0.0.0.0
   IGMP query interval is 125 seconds
    IGMP querier timeout is 262 seconds
    IGMP max query response time is 25 seconds
   Last member query response interval is 1000 milliseconds
   Group Membership interval is 275 seconds
  IGMP Last member query count is 2
    IGMP Snooping is enabled on this interface
    IGMP Snooping fast-leave is enabled
    IGMP Snooping querier is not enabled
   IGMP Snooping report suppression is enabled
......

Switch#
```

10.2.2.3. IGMP Mrouter-Port

VLAN interface 내의 Mrouter Port 를 제외한 모든 Member port 로부터 수신되는 Multicast Traffic 들과 IGMP 메시지들은 Multicast Router 로 전달되어야 한다. 따라서, Multicast Router 와 연결된 VLAN Interface 의 Mrouter Port 는 모든 Multicast Forwarding Table Entry 의 Traffic forwarding port 로 추가된다.

기본적으로 IGMP Snooping 은 IGMP 메시지를 Snooping 하여 Multicast Router 와 연결된 Mrouter Port 를 감지한다.

새로운 Multicast Forwarding Table Entry 가 생성될 때마다 Mrouter port 는 항상 traffic forwarding port 로 등록되며, Multicast Traffic 뿐만 아니라 IGMP Host 에서 전송하는 IGMP 메시지도 전달된다.

Multicast Router Port 를 Static 하게 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping mrouter interface *IFNAME*	해당 VLAN 에 mrouter port 를 수동으로 설정한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.
no ip igmp snooping mrouter interface *IFNAME*	해당 VLAN 에 설정된 mrouter port 를 해제한다.

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ip igmp snooping mrouter interface gi2/2
Switch(config-if-Vlan22)# end
Switch# show ip igmp snooping mrouter vlan22
VLAN    Interface
22      Giga2/2

Switch#
```

customer bridge type 의 VLAN 에 IGMP HOST 를 구성하고, service point-point bridge type 의 VLAN 의 Member-Port 를 Mrouter-Port 로 구성하기 위해서는 다음의 명령을 수행한다.

명령어	설명
ip igmp snooping mrouter interface *IFNAME* **svlan** *<vlan-id>*	해당 VLAN 에 mrouter port 를 수동으로 설정한다. IFNAME 은 service VLAN 내의 Member-Port 여야 한다.
no ip igmp snooping mrouter interface *IFNAME* **svlan** *<vlan-id>*	해당 VLAN 에 설정된 mrouter port 를 해제한다.

```
Switch#configure terminal
Switch#interface Vlan 200
Switch(config-if-Vlan200)#ip igmp snooping mrouter interface gi2/1 svlan 1200
Switch(config-if-Vlan200)#ip igmp snooping mrouter interface gi3/1 svlan 1200
Switch(config-if-Vlan200)#end
```

```
Switch#show ip igmp snooping mrouter vlan200
VLAN     Interface
200      Giga2/1                (Mapped SVLAN1200)
200      Giga3/1                (Mapped SVLAN1200)
```

10.2.2.4. IGMP Access-Group

IGMP Snooping 은 특정 인터페이스에서 수신되는 IGMP Host 들의 특정 그룹을 제한할 수 있다. IGMP Host 의 멀티캐스트 그룹을 제한하기 위해서는 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping access-group <*access-list*>	해당 포트에 수신되는 호스트들의 멀티캐스트 그룹에 대한 등록을 제한한다.
no ip igmp snooping access-group <*access-list*>	해당 포트에 수신되는 제한된 호스트들의 멀티캐스트 그룹에 대한 등록을 해제한다.

```
Switch# configure terminal
Switch(config)# access-list 10 permit 225.1.1.1
Switch(config)# access-list 10 deny any
Switch(config)# interface gi3/1
Switch(config-if-Giga3/1)# ip igmp snooping access-group 10
Switch(config-if-Giga3/1)# end
Switch#
```

해당 인터페이스가 여러 VLAN interface 의 member 인 경우, 특정 VLAN interface 에서만 IGMP Host 들의 멀티캐스트 그룹을 제한할 수 있으며 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping access-group <*access-list*> **vlan** <*vlan-id*>	IGMP 호스트에서 지정된 VLAN Interface 로 수신되는 멀티캐스트 그룹에 대한 등록을 제한한다.
no ip igmp snooping access-group <*access-list*> **vlan** <*vlan-id*>	IGMP 호스트에서 지정된 VLAN Interface 로 수신되는 멀티캐스트 그룹에 대한 등록 제한을 해제한다.

```
Switch# configure terminal
Switch(config)# access-list 10 permit 225.1.1.1
Switch(config)# access-list 10 deny any
```

```
Switch(config)# interface gi3/1
Switch(config-if-Giga3/1)# ip igmp snooping access-group 10 vlan 22
Switch(config-if-Giga3/1)# end
Switch#
```

10.2.2.5. IGMP Group-Limit

IGMP Snooping 은 각각의 interface 별로 Multicast Group 의 개수를 제한할 수 있다.
Multicast Group 의 개수를 제한하기 위해서는 다음의 명령을 interface configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping limit <*count*>	해당 포트에 수신되는 Multicast Group 의 개수를 제한한다.
ip igmp snooping limit <*count*> **except** <*access-list*>	해당 포트에 수신되는 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.
no ip igmp snooping limit <*count*>	해당 포트에 설정된 Multicast Group 의 개수 제한을 해제한다.

```
Switch# configure terminal
Switch(config)# interface gi3/1
Switch(config-if-Giga3/1)# ip igmp snooping limit 10
Switch(config-if-Giga3/1)# end
Switch#
```

해당 인터페이스가 여러 VLAN interface 의 member 인 경우, 특정 VLAN interface 에서만 Multicast Group 의 개수를 제한할 수 있으며 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping limit <*count*> **vlan** <*vlan-id*>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한한다.
ip igmp snooping limit <*count*> **vlan** <*vlan-id*> **except** <*access-list*>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.
no ip igmp snooping limit <*count*> **vlan** <*vlan-id*>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수 제한을 해제한다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi3/1
Switch(config-if-Giga3/1)# ip igmp snooping limit 10 vlan 22
Switch(config-if-Giga3/1)# end
Switch#
```

Multicast Group 수의 제한 범위는 각각의 interface 구분 없이, 전체적으로 설정할 수 있다. 해당 명령은 아래와 같으며, config mode 에서 실행한다.

명령어	설명
ip igmp limit <*count*>	전체 Multicast Group 의 개수를 제한한다.
ip igmp limit <*count*> **except** <*access-list*>	전체 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip igmp limit 10
Switch(config)# end
Switch#
```

10.2.2.6. IGMP snooping forced-source-ip

IGMP Snooping 동작 시에 Mrouter port 로 전달되는 IGMP Message 에 대하여 Source address 를 지정할 수 있다. 이 기능은 IP address 를 설정하지 않은 VLAN 에 Static Group 을 설정한 경우, Mrouter Port 로 전송하는 Message 의 source address 를 지정하는데 활용이 가능하다.

명령어	설명
ip igmp snooping forced-source-ip <*ip-address*>	해당 VLAN 의 Report 및 Leave Message 의 Source Address 를 지정한다.
no ip igmp snooping forced-source-ip	해당 VLAN 의 Report 및 Leave Message 의 Source Address 를 해제한다.

```
Switch# configure terminal
RT#F_211(config)#interface Vlan 200
Switch(config-if-Vlan200)#ip igmp snooping forced-source-ip 22.1.1.1
Switch# end
```

10.2.2.7. IGMP querier timeout

IGMP Snooping 이 설정된 interface 는 Query 수신 시 Dynamic Mrouter-Port 의 결정에 필요한 Querier 정보를 가지고 있다. 이 정보를 유지하는 시간은 설정이 가능하며 그 시간 동안 Query 를 수신하지 못하면, Mrouter-Port 정보는 삭제된다. timeout 시간을 설정하는 명령은 아래와 같으며 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping querier-timeout *<60-300>*	해당 VLAN 의 Querier timeout 시간을 설정한다.
no ip igmp snooping querier-timeout	해당 VLAN 의 Querier timeout 시간을 해제한다.

```
Switch# configure terminal
Switch (config)#interface Vlan 200
Switch(config-if-Vlan200)#ip igmp querier-timeout 60
Switch#show ip igmp interface
Interface Vlan200 (Index 2200)
  IGMP Enabled, Inactive, Version 2 (default)
    IGMP interface has 0 group-record states
    IGMP activity: 0 joins, 0 leaves
   IGMP querying router is 0.0.0.0
    IGMP query interval is 125 seconds
    IGMP querier timeout is 60 seconds
    IGMP max query response time is 25 seconds
    Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
  IGMP Last member query count is 2
    IGMP Snooping is enabled on this interface
    IGMP Snooping fast-leave is enabled
    IGMP Snooping querier is not enabled
    IGMP Snooping report suppression is enabled
```

10.2.3. Configure IGMP Static Group Functionality

10.2.3.1. IGMP Static Group

특정한 Multicast 네트워크의 환경에 따라서 Multicast Membership 에 가입된 Member 가 존재하지 않아도 Multicast 트래픽을 수신해야 되는 경우가 있다.
이러한 경우, Multicast 트래픽을 수신 할 Network 의 VLAN Interface 에 Static Group 을 설정하면, 해당 VLAN 으로 지정된 Multicast Traffic 이 계속 전달된다. 또, Static Group 설정 시에 VLAN 의 Member-port 를 명시하면, IGMP JOIN 여부와 상관없이 해당 port 로 Multicast Traffic 이 전달된다.

IGMP static-group 명령은 interface configuration mode 에서 실행하며, 각 명령에 대한 설명은 아래와

같다.

명령어	설명
ip igmp static-group <*group-address*>	<*group-address*>으로 Static Group 을 설정한다.
ip igmp static-group <*class-map*>	Static Group 의 Group-address 를 class-map 으로 설정한다.
ip igmp static-group <*group-address*> **interface** *IFNAME*	Static Group 을 설정한다. 명시된 interface 로 해당 Multicast Traffic 이 전달된다.
no ip igmp static-group <*group-address*>	<*group-address*>으로 Static Group 을 해제한다.
no ip igmp static-group <*class-map*>	Static Group 의 Group-address 를 class-map 으로 해제한다.
no ip igmp static-group <*group-address*> **interface** *IFNAME*	해당 Group 및 interface 의 Static Group 을 해제한다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan 200
Switch(config-if-Vlan200)#ip igmp static-group 225.1.1.1
Switch(config-if-Vlan200)#end
Switch#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime   Expires  Last Reporter
225.1.1.1          Vlan200            00:00:03   static      0.0.0.0
```

10.2.3.2. multicast-flows class-map

IGMP Static Group 을 설정할 때, 명시하는 Group 주소는 class-map 으로도 지정이 가능하다. 이 class-map 은 멀티캐스트용으로 별도로 지정하여야 하며, 설정하는 명령은 아래와 같다.

명령어	설명
class-map type multicast-flows <*class-map*>	Static Group 지정을 위한 class-map 을 등록한다. config mode 에서 수행이 가능하다.

class-map 을 등록하면 class-map config mode 가 되어 class-map 의 추가적인 정보 등록이 가능하다. class-map config mode 에서 실행이 가능한 명령은 아래와 같다.

명령어	설명
description <*description*>	class-map 에 대한 description 을 등록한다.
group <*group-address*>	class-map 에 해당 Group 주소를 등록한다.
group <*group-address*> **to** <*group-address*>	class-map 에 해당 Group 주소를 범위를 지정하여 등록한다.
group <*group-address*> **source** <*source-address*>	class-map 에 해당 Group 주소를 Source-

	address 를 지정하여 등록한다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#class-map type multicast-flows MCAST_CLASS
Switch(config-mcast-flows-cmap)#group 225.1.1.101 to 225.1.1.103
Switch(config-mcast-flows-cmap)#end
Switch#show ip igmp static-group class-map

Class-map MCAST_CLASS
  description : -
  Group address range 225.1.1.101 to 225.1.1.103
```

10.3. Display System and Network Statistics

표 1 IGMP Snooping 관련 모니터링 명령어

명령어	설명
show ip igmp groups	IGMP JOIN 정보를 보여준다.
show ip igmp interface	IGMP snooping 설정 정보를 보여준다.
show ip igmp static-group class-map	static-group 등록을 위해 지정한 class-map 의 정보를 보여준다.
show ip igmp snooping statistics	IGMP snooping 의 통계 정보를 보여준다
show ip igmp snooping mrouter *<IFNAME>*	해당 VLAN 에 대한 mrouter port 를 보여준다.
show ip igmp snooping reporter	IGMP JOIN 이 되어 있는 호스트들의 목록을 보여준다.

11 Provider Bridging

이 장에서는 Provider Bridging 기능을 설정하는 방법에 대해 설명한다. Provider Bridging 을사용해서 ISP 는 Provider Bridge Network 라는 하나의 Layer2 Network 를 고객이 VLAN ID 로 구별되는 여러개의 LAN segment 와 같이 사용할 수 있도록 하는 Service 를 제공할 수 있다. 고객은 Provider Bridging 을사용하기위해 Customer Network 의 구성이나 설정에 최소한의 변경만을 하면 되며, Provider Bridging 을사용하기위한 고객간의 협조는 필요하지않다.

이 장은 다음과 같은 내용으로 구성된다:

- Provider Bridging 에 대한 이해
- Provider Bridging 기본 설정
- Provider Bridging 설정
- Provider Bridging 설정 예제

11.1. Provider Bridiging 에 대한 이해

11.1.1. 소개

Provider Bridiging 은 IEEE 802.1AD 규격에 정의되어 있다. IEEE 802.1AD 규격은 Metro Ethernet 과 같은 대규모의 LAN 에서 12-bit VID 의 한계를 극복하는 방법을 기술하고 있다. 이를 위해서 규격문서에서는 Service VLAN(S-VLAN)tag 가 도입되었다. Service VLAN tag 와 대비하여 기존의 tag 는 Customer VLAN(C-VLAN) tag 라고 부른다.

추가적인 S-VLAN tag(S-tag)의 도입으로 Provider Bridge Network 는 C-VLAN tag(C-tag)에 의해 frame 의 switching 이 이루어지는 Customer Network, S-tag(S-tag)에 의해 frame 이 switching 되는 Provider Network 로 나누어지게된다. 이러한 계층적인 구조를 통해 ISP 는 Network 를 보다많은 VLAN 으로 세분화 할수 있다. 또한 Provider Network 내에서 Customer Network 에서 전송된 frame 의 C-tag 는 S-tag 내에 쌓여서 손실없이 반대쪽 Customer Network 에 전달된다. 따라서 고객은 VLAN ID 가 다른 고객이 사용하는 VLAN-ID 와 겹치는것에 대한 우려없이 여러개의 VLAN 을 사용할 수 있게된다.

Provider Bridiging 을이용하는 네트워크에서 frame 의 switching 은 Customer Netork 내에서는 C-tag 를 통해 이루어지고 Provider Network 에서는 S-tag 를 통해 이루어진다.

11.1.2. 802.1AD Ethernet frame

S-tag 는 Service Provider Domain(Provider Network)에서 Ethernet frame 의 switching 을 위해 사용되며 C-tag 는 Customer Network 에서 사용된다. C-tag 와 S-tag 는 서로다른 Ethernet Type 을 가질 수 있다. 다음은 802.1AD 규격의 Ethernet frame 이다.

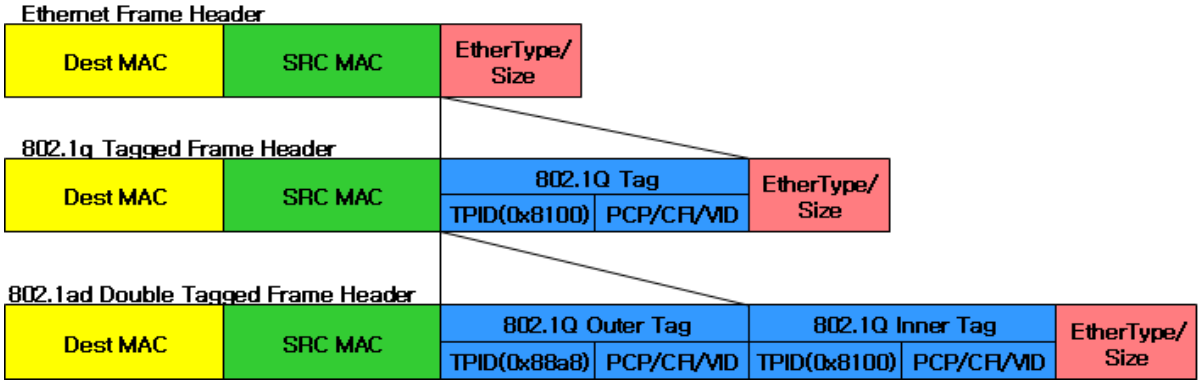


그림 11-1. 802.1ad Double Tagged frame Header

11.1.3. Provider Bridge Network 구성 개요

아래의 그림은 Provider Bridge Network 의 일반적인 구성을 보여준다

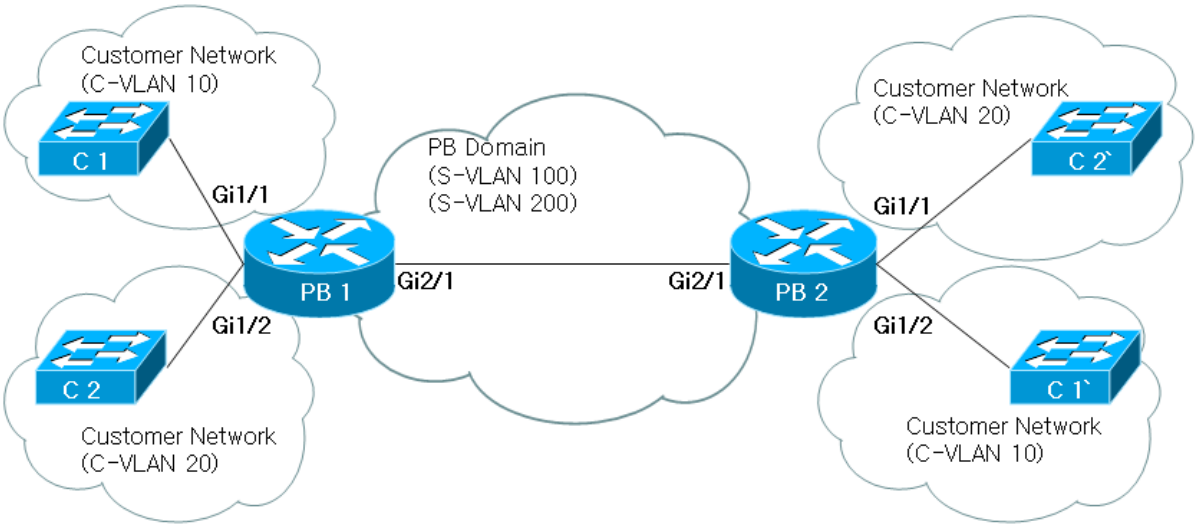


그림 11-2. Provider Bridge Network 구성 개요

Customer Network C1, C2 는 Provider Network 을 통해 연결되어 있으며 PB1 에 연결된 Customer Device C1 과 이에 연결된 Customer Network, C1`과 이에 연결된 Customer Network 는 802.1Q VLAN 에 연결된것처럼 작동한다.
C1->PB1 으로 전달된 Packet 에는 하나의 tag(C-tag)만 달려있고 PB1->PB2 로 전달되면서 대응되는 S-tag 를 달게되며 PB2->C1`으로 전달되면서 S-tag 가 삭제되고 적당한 port 를 통해 C1`으로 Switching 된다.

11.2. Provider Bridging 기본설정

다음의 표는 Provider Bridging 기본설정을 보여준다.

표 11-1. Provider Bridige port 기본설정

Feature	*Default Setting*
port 가 속한 Bridge port 의 ingress-filter 설정	Default Bridge(VLAN Bridge) 비활성 상태이다
Customer-Edge, Customer Network port 의 Native VLAN	0

11.3. Provider Bridging 설정

이 절에서는 다음과 같은 Provider Bridging 설정 방법에 대해 설명한다:

- Bridge 생성

- CVLAN, SVLAN 생성
- port 설정
- C-VLAN Registration Table 설정
- Provider Bridiging 설정 조회

11.3.1. Bridge 생성

Provider Bridiging 설정을 위해서는 먼저 Provider Bridge Network 에 연관된 port, VLAN 이 속할 Bridge 를 만들어줘야한다.

명령어	설명
`bridge <1-32> protocol [provider-bridge | provider-bridge edge]`	■ Brige 를 생성한다. ■ 설정 mode: (Global Config Mode) ■ protocol: 아래에 정리

다음은 각 Bridge Protocol 의 특성을 정리한것이다.

provider-bridge	■ *S-tag 만 보고 frame 을 switching* ■ *포함할 수 있는 VLAN:S-VLAN* ■ *포함할 수 있는 port:* *Provider Network port / Customer Network port*
provider-bridge edge	■ C-tag, S-tag 를 보고 frame 을 switching ■ 포함할수 있는 VLAN: C-VLAN , S-VLAN ■ 포함할 수 있는 port: Customer Edge port / Provider Network port / Customer Network port

Notice CS3400 은 Bridge 0 을 Default Bridge 로 사용하고 있으며 이 Bridge 는 Provider Bridiging 용으로 사용할 수 없다. 따라서 이 Bridge 에는 CE, CN, PN port 가 소속될 수 없으며, Service type 의 VLAN 도 소속될 수 없다.

다음은 Provider Edge Bridige 2 를 생성하는 예제이다.

```
Switch#configure terminal
Switch(config)#bridge 2 protocol provider-bridge edge
Switch(config)#exit
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   G.8031 does not initialized.
   G.8032 does not initialized.
```

Bridge 를 삭제하기 위해서는 다음 명령을 사용한다.

명령어	설명
`no bridge <1-32>`	■ Brige 를 삭제한다. ■ 설정 mode: (Global Config Mode)

Bridge 삭제시 동작은 다음과 같다.

VLAN	*Bridge 에 속한 VLAN 은 모두 삭제된다.*
port	Bridge 에 속한 port 는 모두 Default Bridge 로 이동한다. port 의 mode 는 “access”로 변경된다.
C-VLAN Registration table	Bridge 에 속한 C-VLAN Registration table 은 삭제된다.

no bridge 사용예

```
Switch#config terminal
Switch(config)#no bridge 2
Switch(config)#exit
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   port 2 (Giga1/2) of bridge group 0 is enabled
   port 3 (Giga1/3) of bridge group 0 is enabled
   G.8031 does not initialized.
   G.8032 does not initialized.
```

11.3.2. CVLAN, SVLAN 생성

Customer Network 와 연결될 CVLAN, Provider Network 에 연결될 SVLAN 을 생성해야 한다.

명령어	설명
vlan VLANID [type customer] bridge <1-32> vlan VLANID type service [point-point|multipoint-multipoint] bridge <1-32>	■ VLAN 을 생성한다. ■ 설정 mode: (VLAN Config Mode) ■ type: VLAN type customer: C-VLAN[type 생략시 default] service: S-VLAN ■ bridge: VLAN 이 소속될 bridge C-VLAN: vlan-bridge, Provider Edge Bridige 에 소속가능 S-VLAN: Provider Bridge, Provider Edge Bridige 에 소속가능

Notice VLAN 의 type, 소속된 Bridge 는 생성후 변경불가능하다. 변경이 필요하다면 VLAN 을 삭제후 재생성해야한다.

Notice VLAN 1 은 CS3400 의 System Default VLAN 으로 Default Bridge 에 속하며 Default Bridge 와 마찬가지로 PB 에 사용할 수 없다.

다음은 bridge 2 에 속하는 C-VLAN 들을 생성하는 예제이다.

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 91 type customer bridge 2
Switch(config-vlan)#vlan 92 type customer bridge 2
Switch(config-vlan)#vlan 93 type customer bridge 2
Switch(config-vlan)#exit
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge
   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   Vlan91 of bridge group 2 is up
    Vlan92 of bridge group 2 is up
    Vlan93 of bridge group 2 is up
   G.8031 does not initialized.
   G.8032 does not initialized.
```

다음은 bridge 2 에 속하는 S-VLAN 들을 생성하는 예제이다.

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 101 type service point-point bridge 2
Switch(config-vlan)#vlan 102 type service point-point bridge 2
Switch(config-vlan)#vlan 103 type service point-point bridge 2
Switch(config-vlan)#exit
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   Vlan91 of bridge group 2 is up
   Vlan92 of bridge group 2 is up
   Vlan93 of bridge group 2 is up
   Vlan101 of bridge group 2 is up
   Vlan102 of bridge group 2 is up
   Vlan103 of bridge group 2 is up
   G.8031 does not initialized.
   G.8032 does not initialized.
```

VLAN 을 삭제하기 위해서는 다음 명령을 사용한다.

명령어	설명
no vlan VLANID [type customer] bridge <1-32> no vlan VLANID type service bridge <1-32>	■ VLAN 을 삭제한다. ■ 설정 mode: (VLAN Config Mode) ■ type S-VLAN 은 삭제시 type 을 명시해야 한다. ■ bridge Default Bridge 에 속하지 않은 VLAN 은 삭제시 bridge 를 명시해야 한다.

Notice VLAN 이 C-VLAN Registration Table 에 등록되어있으면 삭제할 수 없다.

VLAN 을 삭제하는 예제이다.

```
Switch#config terminal
Switch(config)#vlan database
Switch(config-vlan)#no vlan 91 bridge 2
Switch(config-vlan)#no vlan 101 type service bridge 2
Switch(config-vlan)#do show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   Vlan92 of bridge group 2 is up
   Vlan93 of bridge group 2 is up
   Vlan102 of bridge group 2 is up
   Vlan103 of bridge group 2 is up
   G.8031 does not initialized.
   G.8032 does not initialized.
```

11.3.3. port 설정

Provider Bridge Network 상의 port 들은 다음의 순서대로 설정을 해주어야 한다.

- port 와 Bridge 를 연결
- port Mode 설정
- Vlan 을 port 의 Member set 에 추가.

11.3.3.1. port 와 Bridge 를 연결

명령어	설명
bridge-group <1-32>	■ port 를 Bridge 와 연결한다. ■ 설정 mode: (Interface Config Mode)

11.3.3.2. port Mode 설정

다음은 Bridge/VLAN Type 별로 연결가능한 port 의 mode 를 정리한 것이다.

표 11-2. Bridge/VLAN Type 별로 소속가능한 port mode

BRiDGE / *VLAN*	*Provider Bridge*	*Provider Edge Bridge*
Customer		Customer Edge Access Customer Edge Trunk Customer Edge Hybrid
Service	Customer Network	Customer Network
	Provider Network	Provider Network

명령어	설명
switchport mode customer-edge [access | hybrid | trunk]	■ Customer Network 와 연결된 port 의 mode 를 설정한다. ■ mode: (Interface Config Mode) access: non Trunking mode native VLAN 만 설정가능 hybrid: 하나의 native VLAN 설정가능 다수의 tagged/untagged VLAN 설정가능 trunk: trunking mode 하나의 native VLAN 설정가능 다수의 tagged VLAN 설정가능

명령어	설명
switchport mode [provider-network|customer-network]	■ Provider Network 쪽에 연결된 port 를 provider-network 또는 customer-network mode 로 설정한다. ■ 설정 mode: (Interface Config Mode) ■ provider-network 802.1AD 규격에 명시된 Provider Network port 로 동작

	■ customer-network 802.1AD 규격에 명시된 Customer Network port 로 동작

11.3.3.3. VLAN 을 port 의 member set 에 추가.

명령어	설명
switchport customer-edge [access|hybrid] vlan VLANID switchport customer-network vlan VLANID	■ VLAN 을 port 의 member set 에 추가하고 port 의 native VLAN 을 설정. ■ 설정 mode: (Interface Config Mode)
switchport customer-edge hybrid allowed vlan [all|none] switchport customer-edge hybrid allowed vlan add VLANID egress-tagged [enable|disable] switchport customer-edge hybrid allowed vlan remove VLANID	■ VLAN 을 Customer Network 와 연결된 hybrid port 의 member set 에서 추가하거나 삭제한다. ■ 설정 mode: (Interface Config Mode) ■ all: Bridge 의 모든 VLAN 들이 이 port 를 사용해서 frame 을 주고 받도록 설정한다. ■ none: Bridge 의 어떤 VLAN 에서도 이 port 를 사용해서 frame 을 주고 받지 못하도록 설정한다. ■ add: VLAN 을 port 의 member set 에 추가한다. ■ remove: VLAN 을 port 의 member set 에서 삭제한다. ■ egress-tagged: enable: port 에서 Tx 되는 frame 에는 VLAN tag 를 삽입한다. disable: port 에서 Tx 되는 frame 에 VLAN tag 를 삽입하지 않는다.
switchport customer-edge trunk allowed vlan [all|none] switchport customer-edge trunk allowed vlan [add|remove] VLANID	■ VLAN 을 Customer Network 와 연결된 trunk port 의 member set 에서 추가하거나 삭제한다. ■ 설정 mode: (Interface Config Mode) ■ all: Bridge 의 모든 VLAN 들이 이 port 를 사용해서 frame 을 주고 받도록 설정한다. ■ none: Bridge 의 어떤 VLAN 에서도 이 port 를 사용해서 frame 을 주고 받지 못하도록 설정한다. ■ add: VLAN 을 port 의 member set 에 추가한다. ■ remove: VLAN 을 port 의 member set 에서 삭제한다.

명령어	설명
switchport [provider-network |customer-network] allowed vlan [all|none] switchport [provider-network |customer-network] allowed vlan [add| remove|except] VLANID	■ VLAN 을 Customer Network 또는 Provider Network port 의 member set 에서 추가하거나 삭제한다. ■ 설정 mode: (Interface Config Mode) ■ all: Bridge 의 모든 VLAN 들이 이 port 를 사용해서 frame 을 주고 받도록 설정한다. ■ none: Bridge 의 어떤 VLAN 에서도 이 port 를 사용해서 frame 을 주고 받지 못하도록 설정한다. ■ add: VLAN 을 port 의 member set 에 추가한다. ■ remove: VLAN 을 port 의 member set 에서 삭제한다.

	■ except: 지정된 VLAN 을 제외한 Bridge 의 모든 VLAN 을 이 port 의 member set 에 추가한다.

다음은 CE port 를 Provider Edge Bridige 2 와 연결하고 C-VLAN 들을 CE port 의 member set 에 추가하는 예제이다.

```
Switch#configure terminal
Switch(config)#interface gi1/2
Switch(config-if-Giga1/2)#switchport
Switch(config-if-Giga1/2)#bridge-group 2
Switch(config-if-Giga1/2)#switchport mode customer-edge trunk
Switch(config-if-Giga1/2)#switchport customer-edge trunk allowed vlan add 91-93
Switch(config-if-Giga1/2)#exit
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   Vlan91 of bridge group 2 is up
   Vlan92 of bridge group 2 is up
   Vlan93 of bridge group 2 is up
   Vlan101 of bridge group 2 is up
   Vlan102 of bridge group 2 is up
   Vlan103 of bridge group 2 is up
   port 2 (Giga1/2) of bridge group 2 is enabled
   G.8031 does not initialized.
   G.8032 does not initialized.

Switch#show interface switchport bridge 2
Interface name          : Giga1/2
 Switchport mode         : customer-edge
 Ingress filter           : enable
 Acceptable frame types   : vlan-tagged only
 Default Vlan             : 0
 Configured Vlans          :    91   92   93
```

다음은 Provider Network 에 연결된 port 를 Provider Edge Bridige 2 에 삽입하고 S-VLAN 100 에 삽입하는 예제이다.

```
Switch#configure terminal
Switch(config)#interface gi1/3
Switch(config-if-Giga1/3)#switchport
Switch(config-if-Giga1/3)#bridge-group 2
Switch(config-if-Giga1/3)#switchport mode provider-network
Switch(config-if-Giga1/3)#switchport provider-network allowed vlan add 101-103
Switch(config-if-Giga1/3)#exit
```

```
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   Vlan91 of bridge group 2 is up
   Vlan92 of bridge group 2 is up
   Vlan93 of bridge group 2 is up
   Vlan101 of bridge group 2 is up
   Vlan102 of bridge group 2 is up
   Vlan103 of bridge group 2 is up
   port 2 (Giga1/2) of bridge group 2 is enabled
   port 3 (Giga1/3) of bridge group 2 is enabled
   G.8031 does not initialized.
   G.8032 does not initialized.

Switch#show interface switchport bridge 2
Interface name          : Giga1/2
 Switchport mode         : customer-edge
 Ingress filter           : enable
 Acceptable frame types   : vlan-tagged only
 Default Vlan             : 0
 Configured Vlans          :    91   92   93
 Interface name          : Giga1/3
 Switchport mode         : provider-network
 Ingress filter           : enable
 Acceptable frame types   : vlan-tagged only
 Default Vlan             : 0
 Configured Vlans          :   101  102  103
```

VLAN 을 port 의 member set 에서 삭제하고 port 의 native VLAN 설정을 삭제하려면 다음 명령을 입력하면 된다.

명령어	설명
no switchport customer-edge [access|hybrid] vlan no switchport customer-network vlan	■ VLAN 을 port 의 member set 에서 삭제하고 port 의 native VLAN 설정을 삭제. ■ 설정 mode: (Interface Config Mode)

11.3.4. C-VLAN Registration Table 설정

Customer Network 에서 Provider Network 로 인입되는 frame 에 올바른 S-tag 를 달고 Provider Network 에서 Customer Network 로 나가는 frame 을 S-tag 에 따라 올바른 Bridge 와 port 로 switching 하기위해서 C-VLAN Registration Table 이 설정되어야 한다.

명령어	설명

cvlan registration table WORD cvlan registration table WORD bridge <1-32>	■ C-VLAN Registration Table WORD 생성 ■ 설정 mode: (Global Config Mode) ■ bridge: registration table 을 등록할 bridge 를 선택(선택하지 않으면 default bridge 가 선택됨)
cvlan VLAN_ID svlan VLAN_ID	■ C-VLAN 과 S-VLAN 사이에 Mapping 을 생성 ■ 설정 mode: (C-VLAN Registration Mode)

Notice 여러개의 C-VLAN 을 하나의 S-VLAN 으로 Mapping 할 수 있으나 반대로 여러개의 S-VLAN 을 하나의 C-VLAN 으로 Mapping 할 수는 없다.

C-VLAN Registration Table 을 생성한 후에는 이를 다시 CE port 에 등록해야한다.

명령어	설명
switchport customer-edge vlan registration WORD	■ C-VLAN Registration Table 을 CE port 에 등록 ■ 설정 mode: (InterfaceConfig Mode) ■ WORD: registration table 이름

다음은 PBE 2 에 C-VLAN Registration Table 'test' 생성하고 여기에 C-VLAN 99, S-VLAN 100 간의 Mapping 을 생성하고 이 table 을 port gi1/2 에 등록하는 예제이다.

```
Switch#configure terminal
Switch(config)#cvlan registration table test bridge 2
Switch(config-cvlan-registration)#cvlan 91 svlan 101
Switch(config-cvlan-registration)#cvlan 92 svlan 102
Switch(config-cvlan-registration)#cvlan 93 svlan 103
Switch(config-cvlan-registration)#exit
Switch(config)#interface gi1/2
Switch(config-if-Giga1/2)#switchport customer-edge vlan registration test
Switch(config-if-Giga1/2)#exit
Switch#show cvlan registration table bridge 2
Bridge          Table Name       port List
======          ==========       =========
2               test             Giga1/2

CVLAN ID        SVLAN ID
========        ========
91              101
92              102
93              103
```

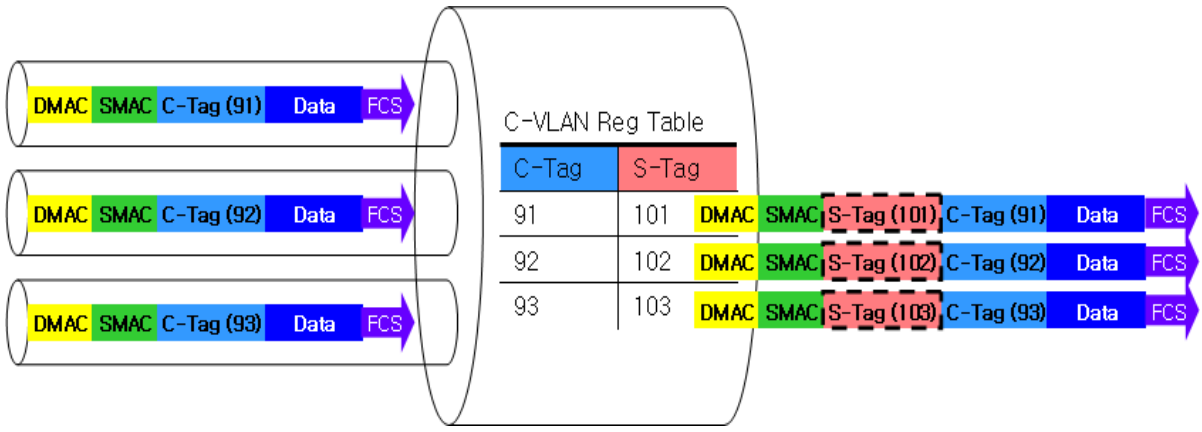


그림 11-3. C-VLAN Registration table

port 에 등록된 C-VLAN Registration table 에 의해 CS3400 에 도달한 frame 은 다음과 같이 처리된다.

- Customer Network->CS3400 방향의 frame
  CS3400 은 Packet 의 802.1q tag 를 보고 C-VLAN Registration table 에서 대응되는 S-tag 를 frame 에 추가한다. Tag 가 삽입된 frame 은 C-VLAN Registration table 에서 선택된 S-VLAN 으로 switching 한다.
- CS3400->Customer Network frame
  CS3400 은 Packet 의 S-tag 를 보고 대응되는 C-VLAN 으로 frame 을 switching 한다. 이때 frame 의 S-tag 는 삭제된다.

interface 에 등록되어 있는 C-VLAN Registration table 을 삭제하기 위해서는 다음 명령을 사용한다.

명령어	설명
switchport customer-edge vlan registration	■ C-VLAN Registration Table 을 CE port 에서 삭제 ■ 설정 mode: (InterfaceConfig Mode)

port gi1/2 에 C-VLAN Registration table 등록을 해제하는 예제이다.

```
Switch#configure terminal
Switch(config)#interface gi1/2
Switch(config-if-Giga1/2)#no switchport customer-edge vlan registration test
Switch(config-if-Giga1/2)#exit
Switch#show cvlan registration table bridge 2
Bridge          Table Name       port List
======          ==========       =========
2               test

CVLAN ID        SVLAN ID
========        ========
91              101
92              102
93              103
```

C-VLAN ~ S-VLAN Mapping 을 삭제하려면 다음 명령을 사용한다.

명령어	설명
no cvlan VLAN_ID no svlan VLAN_ID	■ C-VLAN 과 S-VLAN 사이의 Mapping 을 삭제 ■ 설정 mode: (C-VLAN Registration Mode)

C-VLAN ~ S-VLAN Mapping 을 삭제하는 예제이다.

```
Switch#config terminal
Switch(config)#cvlan registration table test bridge 2
Switch(config-cvlan-registration)#no cvlan 91
Switch(config-cvlan-registration)#do show cvlan registration table bridge 2
Bridge          Table Name       port List
======          ==========       =========
2               test             Giga1/2

CVLAN ID        SVLAN ID
========        ========
92              102
93              103
Switch(config-cvlan-registration)#no svlan 103
Switch(config-cvlan-registration)#do show cvlan registration table bridge 2
Bridge          Table Name       port List
======          ==========       =========
2               test             Giga1/2

CVLAN ID        SVLAN ID
========        ========
92              102
```

C-VLAN Registration Table 을 삭제하려면 다음 명령을 사용한다.

명령어	설명
no cvlan registration table WORD [bridge <1-32>]	■ C-VLAN Registration Table WORD 삭제 ■ 설정 mode: (Global Config Mode) ■ bridge: registration table 을 등록할 bridge 를 선택(선택하지 않으면 default bridge 가 선택됨)

C-VLAN Registration Table 을 삭제예제이다. gi1/2 에 등록되어 있던 table 이 삭제된것을 볼 수 있다.

```
Switch#config terminal
Switch(config)#no cvlan registration table test bridge 2
Switch(config-cvlan-registration)#no cvlan 91
Switch(config-cvlan-registration)#do show cvlan registration table bridge 2
Switch#show running-config | begin Giga1/2

...skipping
interface Giga1/2
 no shutdown
 switchport
 bridge-group 2
 switchport mode customer-edge trunk
 switchport customer-edge trunk allowed vlan add 91
 switchport customer-edge trunk allowed vlan add 92
 switchport customer-edge trunk allowed vlan add 93
!
... 생략 ...
```

11.3.5. Provider Bridiging 설정 조회

명령어	설명
show bridge group	■ 설정된 bridge 목록을 조회

show bridge group 사용예

```
Switch#show bridge group

Bridge Group 0 is running the vlan-bridge

   Vlan1 of bridge group 0 is up
   G.8031 does not initialized.
   G.8032 does not initialized.

Bridge Group 2 is running the provider-brdige

   Vlan91 of bridge group 2 is up
   Vlan92 of bridge group 2 is up
   Vlan93 of bridge group 2 is up
   Vlan101 of bridge group 2 is up
   Vlan102 of bridge group 2 is up
   Vlan103 of bridge group 2 is up
   port 2 (Giga1/2) of bridge group 2 is enabled
   port 3 (Giga1/3) of bridge group 2 is enabled
   G.8031 does not initialized.
   G.8032 does not initialized.
```

명령어	설명
show interface swichport bridge <1-32>	■ bridge 에 소속된 port 정보를 표시

show interface switchport bridge 사용예

```
Switch#show interface switchport bridge 2
Interface name          : Giga1/2
 Switchport mode         : customer-edge
 Ingress filter           : enable
 Acceptable frame types   : vlan-tagged only
 Default Vlan             : 0
 Configured Vlans          :    91   92   93
 Interface name          : Giga1/3
 Switchport mode         : provider-network
 Ingress filter           : enable
 Acceptable frame types   : vlan-tagged only
 Default Vlan             : 0
 Configured Vlans          :   101  102  103
```

명령어	설명
show cvlan registration table [bridge <1-32>]	■ C-VLAN Registration Table 을 Bridge 별로 표시 ■ bridge: 선택한 bridge 의 C-VLAN Registration Table 만 표시

show cvlan registration table 사용예

```
Switch# show cvlan registration table bridge 2
Bridge          Table Name       port List
======          ==========       =========
2               test             Giga1/2

CVLAN ID        SVLAN ID
========        ========
91              101
92              102
93              103
```

11.4. Provider Bridge Network 에서 ACL/QoS 를 이용한 frame 전송

이 절은 다음과 같이 Provider Bridge Network 에서의 frame 전송에 대해 설명한다.

- Provider Bridge Network에서 분류된 frame의 전송
- frame의 분류 및 VLAN tag 설정

11.4.1. Provider Bridge Network 에서 분류된 frame 의 전송

Provider Bridiging 을이용하는 네트워크에서는 VLAN 에 따라 MAC table 이 구성 되고 MAC table 에 의해 frame 의 switching 이 이루어 진다. 그래서 frame 의 VLAN tag 와 목적지 MAC 주소에 따라 frame 의 경로가 결정된다.

frame 에 대한 VLAN 분류는 여러가지 방법이 있는데 기본적으로 port-based VLAN 분류 방식이 사용된다. 해당 frame 이 들어온 port 에 따라 frame 을 switching 할 VLAN 이 결정 되는 방식으로 frame 에 VLAN tag 가 없을 경우 포트에 지정된 vid 값으로 VLAN 을 인식하고 frame 에 VLAN tag 가 존재 할 경우 tag 값에 해당하는 VLAN 으로 분류한다. 이렇게 분류된 frame 은 VLAN 의 MAC table 에 따라 switching 된다.

CS3400 serise 는 QoS/ACL 을 이용해서 특정 frame 에 대해 사용자가 VLAN tag 값을 설정해서 다른 VLAN MAC table 에 의해 frame switching 이 일어나도록 하는 기능을 제공한다. PB 에서 사용하는 C-VLAN tag 와 S-VLAN tag 를 frame 에 설정 할 수 있고 이를 이용해서 frame 의 ip, 프로토콜, 포트 번호에 따라 다른 VLAN tag 를 할당 해서 기존의 경로와는 다른 경로를 갖도록 설정 할 수 있다.

11.4.2. frame 의 분류 및 VLAN tag 설정

특정 frame 에 대한 분류를 위해서 QoS/ACL 을 이용한다. IP 나 L4 포트번호에 대한 분류를 위해서 ACL 을 이용하고 프로토콜에 대한 분류를 위해서 QoS 를 사용 한다. 이에 대한 설정 명령은 다음과 같다.

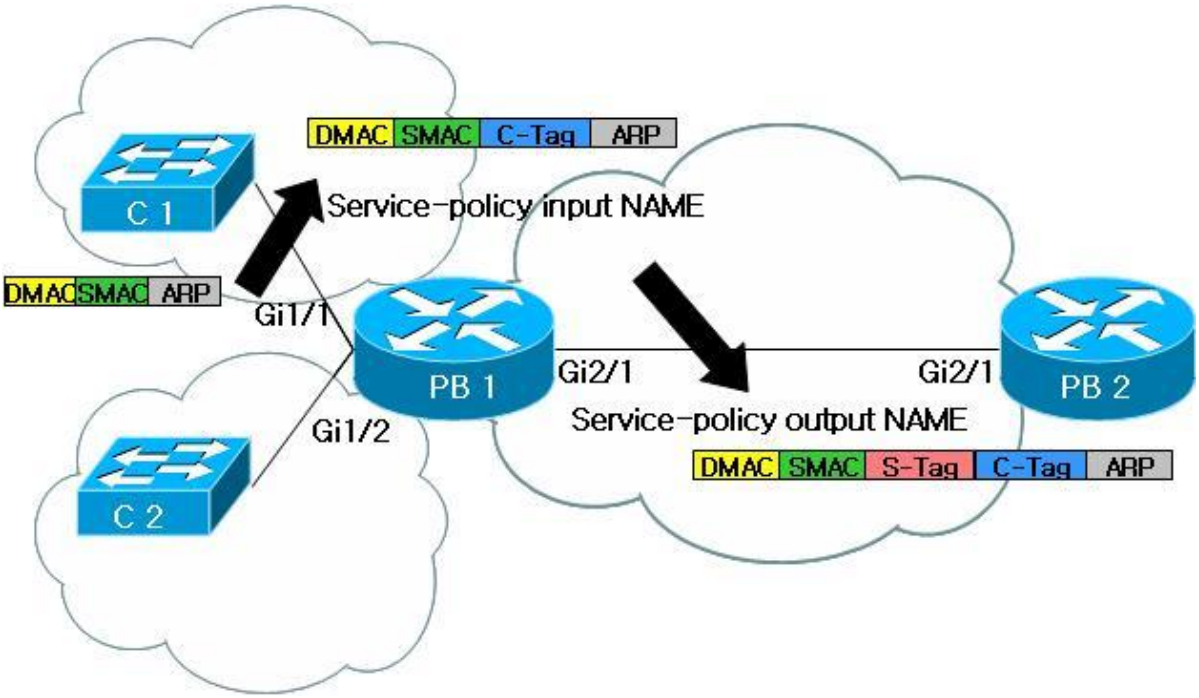


그림 11-4 분류된 frame 에 VLAN tag 설정

PB1(config)# access-list standard C10 *permit 12.1.1.0 0.0.0.255* *PB1(config)# class-map C10* *PB1 (config-cmap)# match protocol arp 12.1.1.0/24 12.1.1.0/24* *PB1(config)# class-map C10_0* *PB1 (config-cmap)# match access-group C10* *PB1(config)# class-map C10_1* *PB1 (config-cmap)# match access-group C10*	*12.1.1.0/24 에 해당하는 IP 주소를 갖는 frame 에 대해서 classify* *ARP frame 중 src 와 dst 주소가 12.1.1.0/24 에 속하는 frame 에 대해서 classify*
PB1(config-cmap)# exit PB1(config)# policy-map RTA_CVLAN PB1(config-pmap)#class C10 PB1(config-pmap-c)# set inner-tag-vlan 10 outer-tag-vlan 100 PB1(config-pmap)#class C10_0 PB1(config-pmap-c)#set tag-vlan 10 PB1(config-pmap-c)# exit PB1(config-pmap)# exit	Policy-map 을 설정해서 12.1.1.0/24 에 해당하는 IP 주소를 갖는 frame 에 대해서 C-VLAN tag 를 10 이 되도록 설정 ARP frame 중 src 와 dst 주소가 12.1.1.0/24 에 속하는 frame 에 대해서 C-VLAN tag 를 10 이 되고 S-VLAN tag 를 100 으로 설정

PB1(config)# policy-map RTA_SVLAN PB1(config-pmap-c)# class C10_1 PB1(config-pmap-c)#set tag-vlan 100 PB1(config-pmap-c)#exit	
PB1(config-pmap)#exit **PB1(config)# interface Gi1/1** **PB1(config-if-Giga1/1)#service-policy input RTA_CVLAN** **PB1(config)# interface Gi2/1** **PB1(config-if-Giga2/1)#service-policy output RTA_SVLAN**	위에서 설정한 RTA_CVLAN policy-map 을 interface gi1/1 에 설정 위에서 설정한 RTA_SVLAN policy-map 을 interface gi1/2 에 설정

앞에 표에서 보는 명령은 우선 class-map 을 생성하고 ACL 이나 class-map 의 frame 구별 명령을 사용한 후 이를 policy-map 에 적용해서 해당 interface 에 설정하도록 되어 있다.

그림 4 에서 보는 바와 같이 QoS/ACL 설정은 다음과 같다.

C-VLAN tag 를 설정할 경우에는 set tag-vlan 명령을 사용하고 이를 반드시 service-policy input NAME 설정을 통해 interface 의 input 방향으로 설정해야 한다.

S-VLAN tag 의 경우 set tag-vlan 명령을 사용하고 service-policy output NAME 설정을 통해 interface 의 output 방향으로 설정해야 한다.

ARP frame 에 대한 설정은 service-policy input 을 사용하고 policy-map 에서 S-VLAN 과 C-VLAN 을 동시에 설정하는 set inner-tag-vlan id outer-tag-vlan id 명령을 사용한다.

11.5. Provider Bridging 설정 예제

이 절은 다음과 같은 예제들을 포함한다:

- 예제 1: 기본구성
- 예제 2: Provider Bridge Network 망에서 QoS와 ACL을 이용한 frame switching 설정

11.5.1. 예제 1: 기본구성

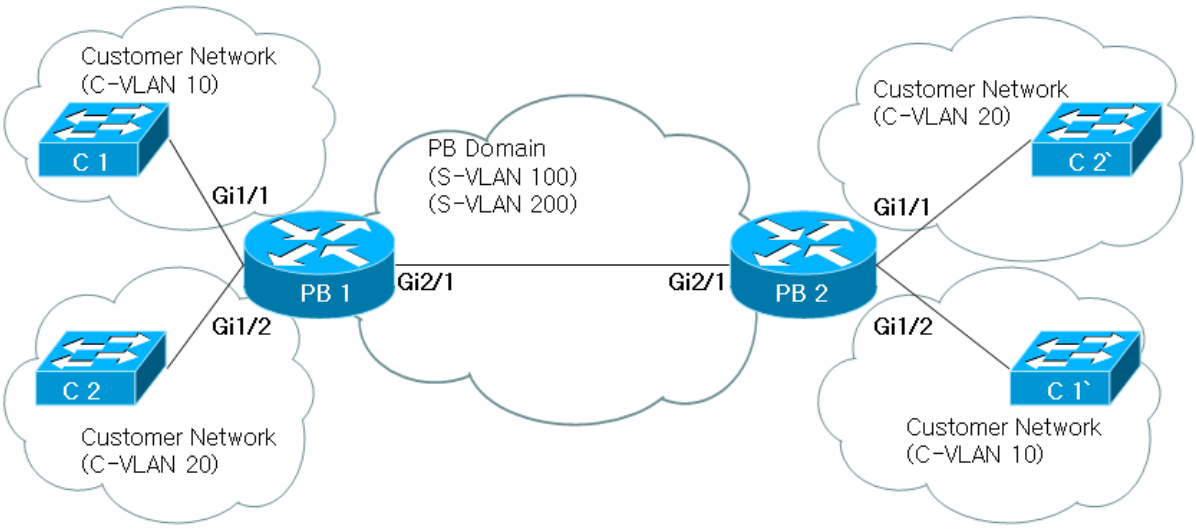


그림 11-5. 예제 1: 기본구성

PB 1 설정

PB1# configure terminal *PB1(config)# bridge 2 protocol provider-bridge edge*	*Provider Edge Bridige 생성*
PB1(config)# vlan database PB1(config-vlan)# vlan 10 type customer bridge 2 PB1(config-vlan)# vlan 20 type customer bridge 2 PB1(config-vlan)# vlan 100 type service point-point bridge 2 PB1(config-vlan)# vlan 200 type service point-point bridge 2 PB1(config-vlan)#exit	C-VLAN 생성 S-VLAN 생성
PB1(config)# interface gi1/1 PB1(config-if-Giga1/1)#switchport PB1(config-if-Giga1/1)#bridge-group 2 PB1(config-if-Giga1/1)#switchport mode customer-edge trunk PB1(config-if-Giga1/1)#switchport customer-edge trunk allowed vlan add 10	Customer Network 와 연결된 gi1/1 설정
PB1(config-if-Giga1/1)#interface gi1/2 PB1(config-if-Giga1/2)#switchport PB1(config-if-Giga1/2)#bridge-group 2	Customer Network 와 연결된 gi1/2 설정

PB1(config-if-Giga1/2)#switchport mode customer-edge trunk PB1(config-if-Giga1/2)#switchport customer-edge trunk allowed vlan add 20 PB1(config-if-Giga1/2)#interface gi2/1 PB1(config-if-Giga2/1)#switchport PB1(config-if-Giga2/1)#bridge-group 2 PB1(config-if-Giga2/1)#switchport mode provider-network PB1(config-if-Giga2/1)#switchport provider-network allowed vlan add 100,200 PB1(config-if-Giga2/1)#exit PB1(config)# cvlan registration table c1 bridge 2 PB1(config-cvlan-registration)# cvlan 10 svlan 100 PB1(config-cvlan-registration)# exit PB1(config)# interface gi1/1 PB1(config-if-Giga1/1)# switchport customer-edge vlan registration c1	Provider Network 와 연결된 gi2/1 설정 Customer Network 'C1'을 위한 C-VLAN Registration table 'c1'을 생성하고 gi1/1 과 연결
PB1(config-if-Giga1/1)#exit **PB1(config)# cvlan registration table c2 ridge 2** **PB1(config-cvlan-registration)# cvlan 20 vlan 200** **PB1(config-cvlan-registration)# exit** **PB1(config)# interface gi1/2** **PB1(config-if-Giga1/2)#switchport customer-edge vlan registration c2**	Customer Network 'C2 을 위한 C-VLAN Registration table 'c2 을 생성하고 gi1/2 와연결

PB 2 설정

PB2# configure terminal *PB2(config)# bridge 2 protocol provider-bridge edge*	*Provider Edge Bridige 생성*
PB2(config)# vlan database PB2(config-vlan)# vlan 10 type customer bridge 2 PB2(config-vlan)# vlan 20 type customer bridge 2 PB2(config-vlan)# vlan 100 type service point-point bridge 2 PB2(config-vlan)# vlan 200 type service point-point bridge 2 PB2(config-vlan)#exit PB2(config)# interface gi1/1 PB2(config-if-Giga1/1)#switchport PB2(config-if-Giga1/1)#bridge-group 2 PB2(config-if-Giga1/1)#switchport mode customer-edge trunk PB2(config-if-Giga1/1)#switchport customer-edge trunk allowed vlan add 20 PB2(config-if-Giga1/1)#interface gi1/2 PB2(config-if-Giga1/2)#switchport PB2(config-if-Giga1/2)#bridge-group 2 PB2(config-if-Giga1/2)#switchport mode	C-VLAN 생성 S-VLAN 생성 Customer Network 와 연결된 gi1/1 설정 Customer Network 와 연결된 gi1/2 설정

customer-edge trunk PB2(config-if-Giga1/2)#switchport customer-edge trunk allowed vlan add 10 PB2(config-if-Giga1/2)#interface gi2/1 PB2(config-if-Giga2/1)#switchport PB2(config-if-Giga2/1)#bridge-group 2 PB2(config-if-Giga2/1)#switchport mode provider-network PB2(config-if-Giga2/1)#switchport provider-network allowed vlan add 100,200 PB2(config-if-Giga2/1)#exit PB2(config)# cvlan registration table c1 bridge 2 PB2(config-cvlan-registration)# cvlan 10 svlan 100 PB2(config-cvlan-registration)# exit PB2(config)# interface gi1/2 PB2(config-if-Giga1/2)# switchport customer-edge vlan registration c1	Provider Network 와 연결된 gi2/1 설정 Customer Network 'C1'을 위한 C-VLAN Registration table 'c1'을 생성하고 gi1/1 과 연결
PB2(config-if-Giga1/2)#exit **PB2(config)# cvlan registration table c2 ridge 2** **PB2(config-cvlan-registration)# cvlan 20 vlan 200** **PB2(config-cvlan-registration)# exit** **PB2(config)# interface gi1/1** **PB2(config-if-Giga1/1)#switchport customer-edge vlan registration c2**	Customer Network 'C2 을 위한 C-VLAN Registration table 'c2 을 생성하고 gi1/2 와 연결

11.5.2. 예제 2: QoS 와 ACL 을 이용한 frame switching 설정예제

다음 예제는 12.1.1.1 호스트와 12.1.1.5 인 호스트가 통신하기 위한 설정을 보여준다. 두 호스트가 통신하기 위해서 우선 arpframe 을 주고 받아야 하는데 tag 가 붙어있지 않은 ARP frame 을 QoS 와 ACL 설정을 이용해서 ARP frame 의 목적지까지 전송되어 MAC 주소를 받아올 수 있도록 tag 를 붙이는 설정을 보여준다.

아래 그림은 그림 4 에 나와 있는 설정에서 QoS/ACL 설정을 추가 해서 12.1.1.5 인 호스트가 12.1.1.1 호스트와 통신을 하기 위해서 ARP frame 을 보낼 경우 PB1 에서 C-VLAN tag 와 S-VLAN tag 를 과정을 나타낸다. 이와 관련된 설정은 아래 표와 같다.

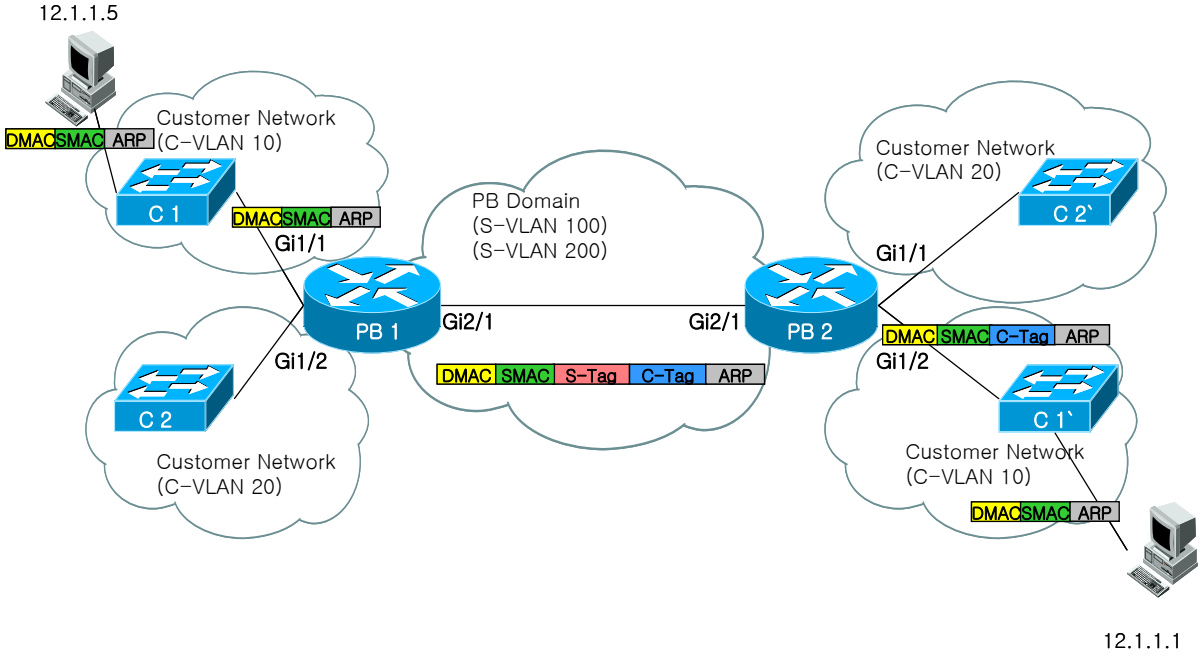


그림 11-6. 예제 2: Setting C-tag and S-tag in ARP packet

PB 1 설정

PB1# configure terminal *PB1(config)# bridge 2 protocol provider-bridge edge*	*Provider Edge Bridige 생성*
PB1(config)# vlan database PB1(config-vlan)# vlan 10 type customer bridge 2 PB1(config-vlan)# vlan 20 type customer bridge 2	C-VLAN 생성
PB1(config-vlan)# vlan 100 type service point-point bridge 2 PB1(config-vlan)# vlan 200 type service point-point bridge 2 PB1(config-vlan)#exit	S-VLAN 생성
PB1(config)# interface gi1/1 PB1(config-if-Giga1/1)#switchport PB1(config-if-Giga1/1)#bridge-group 2	Customer Network 와 연결된 gi1/1 설정

PB1(config-if-Giga1/1)#switchport mode customer-edge trunk PB1(config-if-Giga1/1)#switchport customer-edge trunk allowed vlan add 10 PB1(config-if-Giga1/1)#interface gi1/2 PB1(config-if-Giga1/2)#switchport PB1(config-if-Giga1/2)#bridge-group 2 PB1(config-if-Giga1/2)#switchport mode customer-edge trunk PB1(config-if-Giga1/2)#switchport customer-edge trunk allowed vlan add 20	Customer Network 와 연결된 gi1/2 설정
PB1(config-if-Giga1/2)#interface gi2/1 PB1(config-if-Giga2/1)#switchport PB1(config-if-Giga2/1)#bridge-group 2 PB1(config-if-Giga2/1)#switchport mode provider-network PB1(config-if-Giga2/1)#switchport provider-network allowed vlan add 100,200 PB1(config-if-Giga2/1)#exit	Provider Network 와 연결된 gi2/1 설정
PB1(config)# cvlan registration table c1 bridge 2 PB1(config-cvlan-registration)# cvlan 10 svlan 100 PB1(config-cvlan-registration)# exit PB1(config)# interface gi1/1 PB1(config-if-Giga1/1)# switchport customer-edge vlan registration c1	Customer Network 'C1'을 위한 C-VLAN Registration table 'c1'을 생성하고 gi1/1 과 연결
PB1(config-if-Giga1/1)#exit PB1(config)# cvlan registration table c2 ridge 2 PB1(config-cvlan-registration)# cvlan 20 vlan 200 PB1(config-cvlan-registration)# exit PB1(config)# interface gi1/2 PB1(config-if-Giga1/2)#switchport customer-edge vlan registration c2	Customer Network 'C2 을 위한 C-VLAN Registration table 'c2 을 생성하고 gi1/2 와 연결
PB1(config-if-Giga1/1)#exit PB1(config)# access-list standard C10 permit 12.1.1.0 0.0.0.255 PB1(config)# class-map C10 PB1 (config-cmap)# match protocol arp 12.1.1.0/24 12.1.1.0/24 PB1(config)# class-map C10_0 PB1 (config-cmap)# match access-group C10 PB1(config)# class-map C10_1 PB1 (config-cmap)# match access-group C10	12.1.1.0/24 에 해당하는 IP 주소를 갖는 frame 에 대해서 classify ARP frame 중 src 와 dst 주소가 12.1.1.0/24 에 속하는 frame 에 대해서 classify
PB1(config-cmap)# exit PB1(config)# policy-map RTA_CVLAN	Policy-map 을 설정해서 12.1.1.0/24 에 해당하는 IP 주소를 갖는 frame 에 대해서 C-VLAN

PB1(config-pmap)#class C10 PB1(config-pmap-c)# set inner-tag-vlan 10 outer-tag-vlan 100 PB1(config-pmap)#class C10_0 PB1(config-pmap-c)#set tag-vlan 10 PB1(config-pmap-c)# exit PB1(config-pmap)# exit PB1(config)# policy-map RTA_SVLAN PB1(config-pmap-c)# class C10_1 PB1(config-pmap-c)#set tag-vlan 100 PB1(config-pmap-c)#exit	tag 를 10 이 되도록 설정 ARP frame 중 src 와 dst 주소가 12.1.1.0/24 에 속하는 frame 에 대해서 C-VLAN tag 를 10 이 되고 S-VLAN tag 를 100 으로 설정
PB1(config-pmap)#exit **PB1(config)# interface Gi1/1** **PB1(config-if-Giga1/1)#service-policy input RTA_CVLAN** **PB1(config)# interface Gi1/2** **PB1(config-if-Giga1/2)#service-policy output RTA_SVLAN**	위에서 설정한 RTA_CVLAN policy-map 을 interface gi1/1 에 설정 위에서 설정한 RTA_SVLAN policy-map 을 interface gi1/2 에 설정

%PB2 의 설정은 Sample one 의 설정을 참조하면 된다.

12

시스템 및 통계 모니터링

본 장은 현재 운영중인 CS3400 Series 스위치의 시스템 및 통계 모니터링 기능에 대해 설명한다.

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

CS3400 Series 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 한다. 주기적으로 통계 데이터를 관리하면 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있다.

12.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. CS3400 Series 스위치는 **show** 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공한다.

표 12-1. 상태 모니터링 명령어

명령어	설명	모드
show logging	시스템이 현재 관리하고 있는 로그를 보여 준다.	Privileged
show memory usage	현재 시스템의 메모리 사용 상태를 보여 준다.	Privileged
show cpu usage	현재 CPU 점유율을 보여 준다.	Privileged
show environment [cooling|temperature|status]	시스템의 파워, FAN, 온도에 대한 환경 정보를 출력한다. ■ cooling: FAN 정보 ■ temperature: 온도 정보 ■ status: 파워, FAN, 온도의 상태 정보 출력	Privileged
show environment alarm [status]	시스템 환경 정보에 대한 알람 이력을 출력한다. ■ status: 알람 이력 출력	Privileged
show version	시스템의 버전 정보를 보여 준다.	Privileged

12.2. 시스템 임계치 설정

CS3400 Series 스위치는 시스템 모듈 온도, CPU 및 메모리 사용률 등에 대해 임계치(threshold)를 설정할 수 있다. 임계치는 상한 임계치와 하한 임계치로 설정할 수 있으며, 설정한 범위를 벗어나는 경우 syslog 및 SNMP 트랩을 발생시킬 수 있다.

12.2.1. 온도 설정

시스템의 각 모듈에 대해 온도의 상한 및 하한 임계치를 설정할 수 있다. 임계치 범위를 벗어나는 경우 알람이 발생하며 발생한 알람에 대한 이력을 관리를 할 수 있다.

표 12-2. 온도 설정 관련 명령어

명령어	설명	모드
`facility-alarm temperature major` *value* `minor` *value*	모든 모듈에 대해 온도 임계치(major/minor)를 설정한다.	Config
`no facility-alarm temperature`	온도 임계치를 기본값으로 설정한다.	Config
`show environment alarm`	파워, FAN, 온도의 알람 임계치 정보를 출	Privileged

thresholds	력한다.	
clear facility-alarm [major|minor]	알람 이력을 삭제한다.	Privileged

다음은 major 및 minor 온도 임계치를 설정한 예제이다.

```
Switch# configure terminal
Switch(config)# facility-alarm temperature major 65 minor 45
Switch(config)# exit
Switch# show environment alarm thresholds

Temperature    : 35.0 (`C)
Fan threshold : 40 (`C)
Fan ON/OFF     : De-activated by threshold.
  threshold #1 for Module 1 temperature:
    (sensor value >= 65'C) is system major alarm
  threshold #2 for Module 1 temperature:
    (sensor value >= 45'C) is system minor alarm
```

12.2.2. Cpu usage 설정

장비에 CPU 사용율에 대한 임계치를 설정하고, 임계치 초과시 syslog 와 SNMP 트랩으로 이를 알린다.

표 12-3. CPU usage threshold 관련 명령어

명령어	설명	모드
cpu usage threshold low *<30-100>* high *<40-100>*	CPU usage 의 임계치를 설정하는 명령어이다. CPU 사용률이 임계치 보다 높아지거나(high) 다시 낮아지면(low) syslog 를 발생한다.	Config
cpu usage time-period (<300>|<5>|<60>)	CPU 사용률(average) 기준이 되는 시간을 설정한다.	Config
snmp-server enable traps resource cpu-load-monitor	CPU 사용률이 임계치보다 높아지거나(high) 다시 낮아지면(low) snmp trap 을 발생 한다.	Config
show cpu usage	현재의 CPU usage 를 조회한다.	Privileged

12.2.3. Memory Usage 설정

장비에 memory 에 대한 임계치를 설정하고, 사용 가능한 memory 의 사용 가능한 양이 임계치 보다 낮아지면 syslog 와 SNMP 트랩으로 이를 알린다.

표 12-4. Memory usage 관련 명령어

명령어	설명	모드
memory free low-watermark *<10-70>*	사용 가능한 memory 량의 임계치를 설정하는 명령어이다. 사용 가능한 memory 가 임계치 보다 낮아지거나 다시 높아지면 syslog 를 발생한다.	Config
snmp-server enable traps resource memory-free-monitor	사용 가능한 memory 가 임계치 보다 낮아지거나 다시 높아지면 SNMP 트랩을 발생 한다.	Config
show memory usage	현재의 memory usage 를 조회한다.	Privileged

12.2.4. Application memory 사용 display

각 application 들이 사용하는 memory 관련 정보를 보여주기 위해 다음과 같은 명령을 사용한다

표 12-5. Memory display 관련 명령어

명령어	설명	모드
show memory (imi|lacp|nsm|onm|zas|zifm)	각 application 의 memory 사용정보를 조회한다.	Privileged

Notice 조회 가능한 application 은 추후에 추가 및 삭제 될 수 있다.

12.3. 포트 통계

CS3400 Series 스위치는 각 포트의 통계 정보를 제공하며, 다양한 포트 통계 조회 명령들을 통해 아래와 같은 포트 통계 정보를 조회할 수 있다.

표 12-6. 포트 통계 정보

항목	설명
수신 패킷 통계	■ 포트에서 수신한 패킷의 수이다.
수신 바이트 통계	■ 포트에서 수신한 바이트의 수이다.
전송 패킷 통계	■ 포트에서 전송한 패킷의 수이다.
전송 바이트 통계	■ 포트에서 전송한 바이트의 수이다.
브로드캐스트 통계	■ 포트에서 수신 및 전송한 브로드캐스트 주소를 가지는 패킷의 수

	이다.
멀티캐스트 통계	■ 포트에서 수신 및 전송한 멀티캐스트 주소를 가지는 패킷의 수이다.
Transmit Collisions 통계	■ 포트에서 패킷 전송 시 발생한 충돌 횟수이다.
불량 CRC 프레임 통계	■ 포트에서 수신한 양호한 길이의 프레임 중 불량 CRC 를 포함한 프레임의 수이다.
Oversize 프레임 통계	■ 포트에서 수신한 프레임 중 MRU 사이즈보다 큰 프레임의 수이다.
Drop 프레임 통계	■ 포트에서 수신한 프레임 중 시스템 자원이 부족해서 버려진 프레임의 수이다.

포트 통계 정보를 포함한 포트 정보를 출력하기 위해 아래의 명령을 수행할 수 있다.

show interface [*IFNAME*]

다음 예제는 **show interface** 명령으로 출력한 내용이다.

```
Switch# show interface GigabitEthernet 1/1

Giga1/1 is up, line protocol is up (connected)
  Hardware is Ethernet  Current HW addr: 0007.709e.ab12
  Physical:0007.709e.ab12  Logical:(not set)
  index 1001 metric 1 mtu 1500 arp ageing timeout 7200
  Full-duplex, A-100Mb/s, media type is 10/100/1000BaseT
  <UP,BROADCAST,RUNNING,MULTICAST>
  Bandwidth 100m
  inet 192.168.1.229/24 broadcast 192.168.1.255
  Last clearing of "show interface" counters never
  60 seconds input rate 2,048 bits/sec, 2 packets/sec
  60 seconds output rate 1,424 bits/sec, 1 packets/sec
  L2/L3 in Switched: ucast 95,982 pkt - mcast 37,694 pkt
  L2/L3 out Switched: ucast 54,356 pkt - mcast 0 pkt
    185,326 packets input, 124,235,006 bytes
    Received 51,650 broadcast pkt (37,694 multicast pkt)
    0 CRC, 0 oversized, 0 dropped
    54,359 packets output, 3,873,276 bytes
    0 collisions
    0 late collisions, 0 deferred
```

표 12-7. 포트 통계 조회 명령들

명령어	설명	모드
show port counter [detail]	아래 항목에 대해 모든 인터페이스의 누적 통계 정보를 출력한다. ■ I-Kbps/ O-Kbps ■ InOctets/ OutOctets ■ InPkts/ OutPkts	Privileged
show port statistics {all | *IFNAME*}	아래 항목에 대해 인터페이스의 누적 통계 정보를 5 초/1 분/5 분 단위로 출력한다. ■ TX: bits/s, pkts/s ■ RX: bits/s, pkts/s	Privileged
show port statistics avg type *[IFNAME]*	트래픽 타입 기반의 항목에 대해 인터페이스의 평균 통계 정보를 5 초/1 분/5 분 단위로 출력한다. ■ TX: Unicast/Multicast/Broadcast s ■ RX: Unicast/Multicast/Broadcast	Privileged
show port statistics interface *[IFNAME]*	아래 항목에 대한 인터페이스의 통계 정보를 출력한다. ■ InOctets/ OutOctets ■ InUcastPkts/ OutUcastPkts ■ InMcastPkts/ OutMcastPkts ■ InBcastPkts/ OutBcastPkts ■ IfInDiscards ■ IfInErrors	Privileged
show port-mib *IFNAME*	해당 인터페이스의 현재 통계와 누적 통계 정보를 상세하게 출력한다.	Privileged

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

```
Switch# show interface counters

 Port           I-Kbps      O-Kbps                    InOctets
 --------- ---------- ---------- --------------------------
 Gi1/1               1          0                 126,601,563
 Gi1/2               0          0                           0
 Gi1/3               0          0                           0
 Gi1/4               0          0                           0
 Gi2/1               0          0                           0
 Gi2/2               0          0                           0
 Gi2/3               0          0                           0
 Gi2/4               0          0                           0


        InPkts                   OutOctets        OutPkts
 ------------- -------------------------- -------------
       197,556                3,926,576         54,874
             0                        0              0
             0                        0              0
```

```
                0                       0               0
                0                       0               0
                0                       0               0
                0                       0               0
```

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

```
Switch# show port statistics gi1/1
Last clearing of counters 55:17:10
================================================================================
 Port                                    TX|                                RX
                     bits/s          pkts/s|          bits/s          pkts/s
--------------------------------------------------------------------------------
 Gi1/1    ------------------------------------------------------------------------
    5 sec.               96               0             1,048               1
    1 min.              160               0             1,008               0
    5 min.              336               0             1,088               0
================================================================================
```

인터페이스의 통계 정보는 현재 값을 나타내는 평균 값과 누적 값으로 보여진다. 아래 명령을 사용하여 인터페이스의 평균 통계 정보를 갱신하는 시간 설정을 바꾸거나 해당 인터페이스에 대해 일정 기간 동안 High/Low threshold 값을 설정하여 모니터링 할 수 있다. .

표 12-8. 포트 통계 설정 명령

명령어	설명	모드
load-interval *interval*	인터페이스의 평균 통계 정보를 갱신하는 시간을 설정한다.	interface
no load-interval	인터페이스의 평균 통계 정보를 갱신하는 시간을 기본 값으로 변경한다.	interface
input-load-monitor *interval low-threshold high-threshold*	해당 인터페이스에 대해 일정한 시간 동안 low 및 high 임계 값을 설정하여 수신 트래픽이 해당 임계 값을 벗어나는 경우를 모니터링 할 수 있다.	interface
no input-load-monitor	해당 인터페이스에 대한 모니터링 설정을 해제한다.	interface
show port input-load-monitor	인터페이스에 대한 모니터링 설정을 출력한다.	interface

다음 명령은 포트 통계에 대해 누적 값을 초기화시키는 명령어이다.

표 12-9. 포트 통계 초기화 명령

명령어	설명	모드
clear counters	모든 인터페이스의 통계 누적 값을 초기화한다.	privileged
clear counters *IFNAME*	특정 인터페이스의 통계 누적 값을 초기화한다.	privileged
clear counters snmp	모든 인터페이스의 snmp 통계 정보를 초기화한다.	privileged

clear counters *IFNAME* snmp	특정 인터페이스의 snmp 통계 정보를 초기화한다.	privileged

12.4. RMON (Remote MONitoring)

시스템 운영자는 CS3400 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다. 다음 절에서는 RMON 개념 및 CS3400 Series 스위치가 지원하는 RMON 기능에 대하여 자세히 설명한다.

12.4.1. RMON 개요

RMON 은 IETF(Internet Engineering Task Force)의 RFC 1271 와 RFC 1757 에 정의되어 있는 국제 표준 규격으로 시스템 운영자가 네트워크를 원격으로 관리하는 기능을 제공한다. 일반적으로 RMON 은 다음의 두 가지 구성 요소를 가진다.

- **RMON probe**
  - 원격으로 제어되면서 지속적으로 LAN 세그먼트 또는 VLAN 의 통계 정보를 수집하는 지능형 디바이스 또는 소프트웨어 에이전트
  - 수집한 정보를 운영자의 요구가 있을 때 또는 미리 정의한 환경에 따라서 자동으로 관리 호스트에게 전송

- **RMON Manager**
  - RMON probe 와 통신하면서 통계 정보를 수집
  - 반드시 RMON probe 와 동일한 네트워크에 있을 필요는 없으며, RMON probe 를 in-band 또는 out-of-band 연결을 통하여 제어

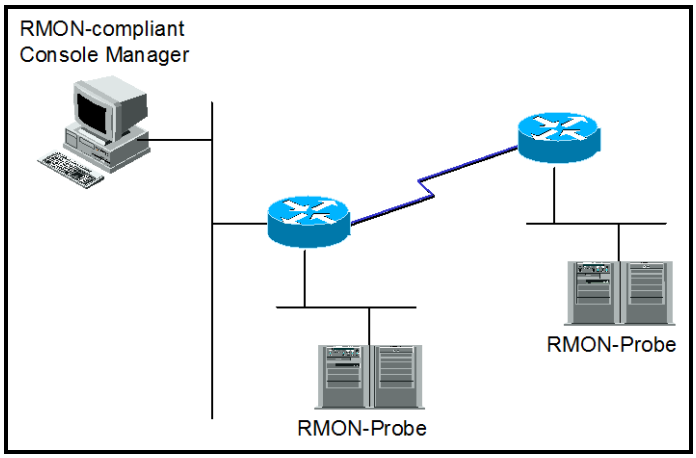


그림 12-1. RMON Manager 와 RMON Probe

기존의 SNMP MIBs 이 SNMP agent 가 탑재된 장비 자체를 관리 대상으로 보고 있는데 반하여 RMON MIBs 는 관리 대상을 장비에 연결된 LAN 세그먼트로 한다. 즉 LAN 세그먼트의 전체 발생 트래픽, 세

그먼트에 연결된 각 호스트의 트래픽, 호스트들 사이의 트래픽 발생 현황을 알려준다.

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

CS3400 Series 스위치에서는 아래 표에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON 은 디폴트로 모든 설정이 disabled 이다.

표 12-10. 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, 길이 미달, 길이 초과 등) 에 대한 통계를 제공.
이력	■ 관리자가 설정한 시간 간격 내에 발생한 각종 트래픽 및 오류에 대한 정보를 제공 ■ 기본적으로 단기/장기적으로 간격을 설정 가능하고 1-3600 초를 간격으로 제한 ■ 이 자료를 통해 시간대별 이용 현황 및 다른 세그먼트와 비교 가능
경보	■ 주기적으로 특정한 값을 체크 해 기준치에 도달하면 관리자에 보고하고 대리인이 자신의 기록을 보유 ■ 기준치는 절대값 및 상대값으로 정할 수 있고 계속적인 경보 발생을 막기 위해서 상/하한치를 설정해서 넘나드는 경우에만 경보가 발생.
호스트	■ 세그먼트에 연결된 각 장비가 발생시킨 트래픽, 오류 수를 호스트별로 관리
상위 n 개의 호스트	■ 위 호스트 테이블에 발견될 호스트 중에서 일정시간 동안 가장 많은 트래픽을 발생시킨 호스트 검색 ■ 관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 수집
트래픽 메트릭스	■ 데이터 링크 계층, 즉 MAC 어드레스를 기준으로 두 호스트간에 발생한 트래픽 및 오류에 대한 정보를 수집 ■ 이 정보를 이용해서 특정 호스트에 가장 많은 이용자가 누구인지를 어느 정도는 판별 가능함 ■ 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없음.
필터	■ 관리자가 특정한 패킷의 동향을 감시하기 위해서 이용
패킷 수집	■ 세그먼트에 발생한 패킷을 수집해서 관리자가 분석.
사건	■ 특정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고 메시지를 전송. 트랩 발생 및 기록보관은 선택적임.

12.4.2. RMON 의 Alarm 과 Event 그룹 설정.

사용자는 CLI 또는 SNMP 관리자에 의해서 RMON 을 설정할 수 있다.

표 12-11. RMON Alarm and Event 설정 명령

명령어	설명	모드
rmon alarm *index variable* interval *seconds* {absolute |delta} rising-threshold *value* event *num* falling-threshold *value* event *num* [owner *string*]	RMON alarm 을 추가한다. ■ *Index*: Alarm 인덱스 ■ *Variable*: Alarm 발생 대상으로 SNMP mib 인스턴스를 지정 *Example)* etherStatsEntry.4.1001: ifindex 가 1001 인 인터페이스의 etherStatsOctets (etherStatsEntry.4)를 지정 ■ Interval: 샘플링 시간 간격 (단위: 초). ■ Absolute: 샘플링 되는 alarm value 에 대해 절대값을 관찰하도록 설정 ■ Delta: 샘플링 되는 alarm value 에 대해 현재 값과 이전 값의 차이를 관찰하도록 설정 ■ Rising-threshold, falling-threshold *value*: alarm 을 발생시킬 설정 값 ■ event: Delta 나 absolute 로 샘플링 되는 alarm value 가 rising-threshold 또는 falling -threshold 값에 도달했을 때 각각 해당 Event 가 발생하도록 설정 ■ owner: Alarm 의 owner 를 등록	Config
rmon event *index* [log] [trap *community*] [description *string*] [owner *string*]	RMON event 를 추가한다. ■ *Index*: Event 인덱스 ■ log: Event 가 발생한 경우 log 를 생성하도록 설정 ■ trap: Event 가 발생한 경우 설정한 community 와 함께 trap 을 전송하도록 설정 ■ owner: Event 의 owner 를 등록 ■ description*:* Event 에 대한 설명을 등록	Config
no rmon alarm *alarm-index*	설정한 RMON alarm 설정을 삭제한다.	Config
no rmon event *event-index*	설정한 RMON event 설정을 삭제한다	Config
show rmon alarms	RMON alarm 정보 출력한다.	Privileged
show rmon events	RMON event 정보 출력한다.	Privileged

아래 예제는 GigabitEthernet 1/1 에 대해 rmon alarm 을 설정한다. GigabitEthernet 1/1 의 inOctets 값

을 30 초마다 샘플링하며 rising-threshold 및 falling-threshold 를 벗어나면 각 설정된 event 를 발생시키도록 한다. RMON alarm 의 alarm variable 설정 시 인터페이스 인덱스(ifindex)를 설정해야 하며, 인터페이스 인덱스 값은 “show interface [*IFNAME*]” 명령을 통해 참조할 수 있다.

Rmon alarm 을 설정할 때 아래와 같이 event 및 stats 을 먼저 설정 해야 한다.

```
Switch# configure terminal
Switch(config)# rmon event 1 log trap rmon_test description RisingAlarm
Switch(config)# rmon event 2 log trap rmon_test description
FallingAlarm
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if-Giga2/2/8)# rmon collection stats 1
Switch(config-if-Giga2/2/8)# end
Switch#show interface GigabitEthernet 1/1

Giga1/1 is up, line protocol is up (connected)
  Hardware is Ethernet  Current HW addr: 0007.7023.f33a
  Physical:0007.7023.f33a  Logical:(not set)
  index 1001 metric 1 mtu 1500 arp ageing timeout 7200
  Full-duplex, A-100Mb/s, media type is 10/100/1000BaseT
  <UP,BROADCAST,RUNNING,MULTICAST>
  Bandwidth 100m
  inet 10.1.21.224/24 broadcast 10.1.21.255
  Last clearing of "show interface" counters never
  60 seconds input rate 368 bits/sec, 0 packets/sec
  60 seconds output rate 344 bits/sec, 0 packets/sec
  L2/L3 in Switched: ucast 24,996 pkt - mcast 32,624 pkt
  L2/L3 out Switched: ucast 24,574 pkt - mcast 0 pkt
    149,785 packets input, 46,520,411 bytes
    Received 92,165 broadcast pkt (32,624 multicast pkt)
    0 CRC, 0 oversized, 0 dropped
    24,584 packets output, 1,604,647 bytes
    0 collisions
    0 late collisions, 0 deferred
Switch# configure terminal
Switch(config)# rmon alarm 1 etherStatsEntry.4.1001 interval 30
absolute rising-threshold 50000000 event 1 falling-threshold 1000000
event 2
Switch(config)# exit
Switch# show rmon alarm
Alarm 1 is active, owned by RMON_SNMP
 Monitors etherStatsOctets.1001 every 30 second(s)
 Taking Absolute samples, last value was 046479224
 Rising threshold is 50000000, assigned to event 1
 Falling threshold is 1000000, assigned to event 2
 On startup enable rising or falling alarm
Switch# show rmon event
event Index = 1
```

```
        Description RisingAlarm
         Event type Log & Trap
          Event community name rmon_test
        Last Time Sent = 10923:30:00
        Owner  RMON_SNMP

 event Index = 2
        Description FallingAlarm
         Event type Log & Trap
          Event community name rmon_test
        Last Time Sent = 10921:50:00
        Owner  RMON_SNM
Switch# show rmon statistics
Collection 1 on Giga1/1 is active, and owned by RMON_SNMP,
 Monitors ifEntry.1.1001 which has
 Received 046507231 octets, 0149624 packets,
  092102 broadcast and 032603 multicast packets,
  00 undersized and 00 oversized packets,
  00 fragments and 00 jabbers,
  00 CRC alignment errors and 00 collisions.
  # of dropped packet events (due to lack of resources): 00
  # of packets received of length (in octets):
  64: 081018, 65-127: 054779, 128-255: 014978
  256-511: 0573,  512-1023: 064, 1024-1518: 022731
```

Notice

RMON alarm 의 variable 설정 시 etherStatsTable(1.3.6.1.2.1.16.1.1)의 하위 항목만 설정 가능하며, 자세한 설정 방식은 다음과 같다. 아래 예제는 ifindex 가 1001 인 인터페이스의 etherStatsOctets(etherStatsEntry.4) 값을 alarm 모니터링 하도록 설정하는 두 가지 방법을 나타낸다.

1) etherStatsOctets.1001
2) etherStatsEntry.4.1001

표 12-12. RMON History 설정 및 statistics 명령

명령어	설명	모드
rmon collection stats *index* [owner *string*]	물리적 인터페이스의 통계 값을 수집한다. ■ *Index*: etherStats 인덱스,	Interface
rmon collection history *index* [buckets *number*] [interval *seconds*] [owner *string*]	물리적 인터페이스에 대하여 이력을 수집한다. ■ *Index*: History 인덱스, ■ buckets: 수집할 이력의 수 ■ Interval: 이력 수집 간격 (단위: 초) ■ owner: History 의 owner 를 등록.	Interface

no rmon collection stats *index*	물리적 인터페이스의 통계 값을 수집하지 않도록 설정한다.	Interface
no rmon collection history *index*	물리적 인터페이스의 이력을 수집하지 않도록 설정한다.	Interface
show rmon history	RMON history 정보를 출력한다.	Privileged
show rmon statistics	RMON statistics 정보를 출력한다.	Privileged
rmon clear counters	해당 인터페이스의 statistics 값을 초기화한다.	Interface

아래 예제는 GigabitEthernet 2/2/8 에 대해 10 초 마다 최대 30 개의 bucket 을 이용해 RMON 이력을 수집하도록 설정한다.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 2/2/8
Switch(config-if-Giga2/2/8)# rmon collection stats 1
Switch(config-if-Giga2/2/8)# rmon collection history 1 buckets 30
interval 10
Switch(config-if-Giga2/2/8)# end
Switch# show rmon history
Entry 1 is active, and owned by RMON_SNMP
 Monitors ifIndex 1001 every 10 second(s)
 Requested # of time intervals, ie buckets, is 30,
   Sample # 1 began measuring    Received 46570622 octets, 150301
packets,
    92511 broadcast and 32678 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions.
    # of dropped packet events is 0
   Sample # 2 began measuring    Received 46572230 octets, 150326
packets,
    92511 broadcast and 32679 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions.
    # of dropped packet events is 0
   Sample # 3 began measuring    Received 46575144 octets, 150368
packets,
    92523 broadcast and 32683 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions.
    # of dropped packet events is 0
```

12.5. Logging

CS3400 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.

CS3400 Series 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI 를 사용하여 로깅되는 시스템 메시지를 제어할 수 있다. 최대 약 1000 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.

CS3400 Series 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

표 12-13. CS3400 Series 스위치의 로그 레벨

Severity 레벨	설명
Emergencies (0)	시스템 사용 불가.
Alerts (1)	즉각적인 조치가 필요한 상태
Critical (2)	Critical 상태.
Errors (3)	에러 메시지.
Warnings (4)	경고 메시지.
Notifications (5)	정상적인 상태지만 중요한 정보.
Informational (6)	사용자에게 제공하는 정보 메시지.
Debugging (7)	디버깅 메시지.

12.5.1. 시스템 로그 메시지 내용

CS3400 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 12>에서 정의한 CS3400 Series 의 로그 메시지의 레벨
  - 0-7 까지의 숫자

- **Log description**
  - 발생한 이벤트에 대한 상세한 정보를 포함하는 텍스트 문자열

다음은 시스템 부팅 시의 로그 메시지 이다.

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

12.5.2. 디폴트 Logging 설정 값.

표 12-14. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	disable
Telnet 세션으로의 로깅 출력	disable.
로깅 버퍼 사이즈	1MB
Time-Stamp 출력	enabled
Logging Server	disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings(4)
콘솔의 Severity	Debuggings(7)
Telnet 의 Severity	info (6)

표 12-15. 시스템 메시지 로깅 환경 설정 명령

명령어	설명
`logging console {<0-7> |alerts|critical|debugging|emergencies|errors| informations|notifications|warnings}`	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 *A.B.C.D*	syslog 메시지를 외부 syslog 서버

	에 보낼지 설정
`logging monitor |alerts|critical|debugging|emergencies|errors| informations|notifications|warnings}`	현 세션으로의 로깅 출력 여부 설정.
logging source-ip *A.B.C.D*	syslog packet 의 source ip 를 설정
`logging trap |alerts|critical|debugging|emergencies|errors| informations|notifications|warnings}`	syslog server 의 logging level 설정
`show logging`	로깅 버퍼 출력 및 로깅 설정 확인.

12.5.3. Logging 설정 예.

Console 로 접속한 경우 Log level notice(5) 이하의 log message 만을 console 로 출력하고자 할 때 다음과 같이 설정한다. console 로 log message 출력을 중단하고자 할 경우 “no logging console” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging console notifications
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging console
Switch(config)#
```

Telnet 으로 접속한 경우 Log level warn(4) 이하의 log message 만을 telnet session 에 출력하고자 할 때 다음과 같이 설정한다. Telnet session 으로 log message 출력을 중단하고자 할 경우 “logging session disable” command 를 사용한다.

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

Log server 100.10.1.1 에 이 switch 에서 발생하는 log 중 Log level err(5) 이하의 log message 를 보내고자 할 경우 다음과 같이 설정한다. log server 로 log message 보내는 것을 중단하고자 할 경우 “no logging A.B.C.D” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging 100.10.1.1
Switch(config)# logging trap errors
Switch(config)# end
```

```
Switch#
Switch# configure terminal
Switch(config)# no logging 100.10.1.1
Switch(config)#
```

12.5.4. Login logging 설정

CS3400 Series 스위치의 기본 동작은 사용자의 로그인 성공 또는 실패 이벤트가 발생했을 때 로그를 출력하지 않으며 아래 명시한 명령으로 로그 출력 동작을 설정할 수 있다.

표 12-16. Login logging 설정 명령들

명령어	설명
login [on-failure|on-success] every <1-65535>	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 주기적으로 로그가 발생하도록 설정한다.
(no) login [on-failure|on-success] every	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 주기적으로 발생하는 로그 설정을 해제한다.
login [on-failure|on-success] log	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 로그를 출력하도록 설정한다.
(no) login [on-failure|on-success] log	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 로그 출력 설정을 해제한다.

다음 예제는 사용자 로그인에 성공한 경우 3 번 주기로 로그인 성공 로그를 출력하도록 설정한 내용이다.

```
Switch# configure terminal
Switch(config)#login on-success every 3
Switch(config)#exit
```

위 예제의 설정으로 사용자가 3 번 로그인에 성공하였다면 아래와 같은 로그 메시지를 출력한다.

Feb 10 18:59:23 [5] %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: root] [Source: 10.1.21.59] [localport: 23] at 18:59:23 UTC Thu Feb 10 2000

아래 예제는 사용자 로그인에 실패한 경우 로그를 출력하도록 설정한 내용이다.

```
Switch# configure terminal
Switch(config)# login on-failure log
Switch(config)#exit
```

위 예제의 설정으로 사용자가 3 번 로그인에 성공하였다면 아래와 같은 로그 메시지를 출력한다.

Feb 10 19:07:30 [4] %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: root] [Source: 10.1.21.59] [localport: 23] [Reason: Login Authentication Failed] at 19:07:30 UTC Thu Feb 10 2000

13

QoS 및 ACL

본 장은 현재 운영중인 CS3400 Series 스위치의 QOS (Quality of Service)설정 및 ACL (access-list) 설정에 대해서 다룬다.

13.1. QOS

13.1.1. 전역 설정

본 장비의 qos 에 대한 전역 설정을 활성화 시키는 명령어는 다음과 같다.

표 13-1. QOS 전역 설정 명령어

명령어	설명	모드
mls qos	QOS 전역 설정을 활성화 한다.	Config
no mls qos	QOS 전역 설정을 비활성화 한다.	Config
show mls qos	QOS 전역 설정 상태를 조회한다	Exec

CS3400 장비의 QOS 관련 설정은 위의 전역 설정이 되어 있다는 것을 기본 전제하에 동작한다. Mls qos 가 활성화 되어 있지 않은 경우 대부분의 QOS 관련 명령어는 설정이 불가능하다.

13.1.2. TX Scheduling 설정

CS3400 Series 스위치에서는 Scheduling 을 위해 SPQ (Strict Priority Queue) Method 와 WRR (Weighted Round Robin) Method 를 제공하며 디폴트는 SPQ 이다. 이 둘은 서로 혼재해서 사용하는 것이 가능하며, 2 개의 WRR 그룹을 가져서 이들 사이에서의 우선 순위도 가진다.

이 장비에서 제공되는 WRR 은 정확하게는 SDWRR (Shaped Deficit Weighted Round Robin) Method 이다. DWRR 은 일반 WRR 에서 quota 관리를 더 해주는 방식으로 동작하며, 이를 통해서 꾸준히 들어오는 트래픽과, burst 하게 몰려 들어 오는 트래픽의 데이터량을 조절해주는 기능을 포함한다. SDWRR 은 여기에 데이터의 흐름에 latency 를 줄기이 위한 shaping 기능이 포함된다. 5:3 비율로 2 개의 queue 에 weight 가 주어졌다고 할 때, WRR (혹은 DWRR) 은 1,1,1,1,1,0,0,0, 1,1,1,1,1,0,0,0 순서로 queue 배분이 이루어진다면, SDWRR 를 쓰는 경우에는 1,0,1,0,1,0,1,1, 1,0,1,0,1,0,1,1 순서로 queue 배분이 이루어지면서 weight 에 따라 패킷양을 조절함과 동시에 트래픽의 latency 도 줄이도록 노력한다.

각 포트는 모두 8 개의 queue 를 가지고 있으며 7 번 큐가 가장 높은 우선순위를 가지고, 0 번 큐가 가장 낮은 우선 순위를 가진다.

Queue 7	*SPQ*
Queue 6	SPQ
Queue 5	WRR group 1 (50)
Queue 4	WRR group 1 (30)
Queue 3	WRR group 1 (20)
Queue 2	WRR group 2 (60)
Queue 1	WRR group 2 (40)
Queue 0	SPQ

위의 표는 큐 별 스케줄링에 대해서 한가지 예시를 적용한 것이다.

- Q7 과 Q6 은 SPQ 로 설정되었다. Q7 은 가장 높은 우선순위이며 동시에 SPQ 이므로, 모든 트래픽중 가장 높은 우선순위로 처리된다. 그다음으로 Q6 이 처리된다.

- Q5,4,3 은 WRR group 1 으로 설정되어 있으며 각각의 weight 은 50:30:20 으로 분배되었다. WRR group 1 은 SPQ 보다 우선순위가 낮지만, WRR group 2 보다는 높으며 이 둘 사이에는 SPQ 와 마찬가지로 절대적인 우선순위 차이를 가진다.

- Q2,1 은 WRR group 2 로 설정되어 있으며, 이 둘 사이에는 60:40 의 weight 배분을 가진다. WRR group 2 는 위의 모든 큐에서 데이터가 처리된 후에나 처리된다.

- Q0 은 SPQ 로 선언되었지만, 제일 낮은 우선순위를 가진다, Q7~1 의 모든 큐가 처리되어야만 Q0 이 동작한다.

Notice 2 개의 WRR group 을 섞어서 사용하거나 (예: Q5 와 Q2 에 WRR1 을 설정하고, Q4 와 Q1 에 WRR2 를 설정하여 사용하는 경우) WRR group 사이 또는 더 낮은 큐에 SPQ 를 사용하는 것은 권장사항이 아니며, 이렇게 설정할 경우에 스케줄링 동작에 대해서는 설정과 다르게 동작할 수 있다.

본 장비에서는 스케줄링 설정은 tx-scheduling 이라는 mapping table 을 생성한 뒤, 포트에 적용하는 방식으로 동작하며, 모듈당 7 개 의 map 을 적용해서 사용할 수 있다. 실제로는 총 8 개의 map 을 설정할 수 있으나, 0 번은 default SPQ 로 사용되며 변경이 불가능하므로, 운용자가 설정할 수 있는 것은 7 개이다.

표 13-2. Tx-scheduling map 설정 명령어

명령어	설명	모드
mls qos map tx-scheduling NAME queueing-method <0-7> (strict|wrr1|wrr2)	해당 이름을 가지는 mapping table 의 n 번째 큐에 대한 queueing-method 를 설정한다. 해당 이름을 가지는 mapping table 이 없는 경우에는 새로 생성한다.	Config
mls qos map tx-scheduling NAME queueing-method <0-7> (wrr1|wrr2) <1-100>	wrr1 또는 wrr2 를 설정할 경우는 wrr weight 를 동시에 설정이 가능하다. Weight 값이 주어지지 않으면 1 로 설정된다.	Config
mls qos map tx-scheduling NAME wrr-weight <0-7> <1-100>	Wrr 로 설정된 큐의 weight 를 설정한다.	Config
no mls qos map tx-scheduling NAME queueing-method <0-7>	해당 큐의 queueing-method 를 해제한다. 해제할 경우 디폴트인 strict 로 바뀐다.	Config
no mls qos map tx-scheduling NAME wrr-weight <0-7>	Wrr 로 설정된 큐의 weight 를 해제한다. 디폴트인 1 로 설정된다.	Config
no mls qos map tx-scheduling NAME	해당 이름을 가지는 mapping table 을 삭제한다.	Config
show mls qos map tx-scheduling	Tx-scheduling 설정 정보를 보여준다.	Exec

위와 같이 만들어진 tx-scheduling 에 대한 mapping table 을 원하는 포트에 다음과 같이 설정하여 사용한다.

표 13-3. Tx-scheduling 설정 명령어

명령어	설명	모드
mls qos tx-scheduling NAME	해당 이름을 가지는 mapping table 을 해당 포트 인터페이스에 설정한다.	interface
no mls qos tx-scheduling NAME	해당 이름을 가지는 mapping table 을 해당 포트 인터페이스에서 해제한다.	interface

13.1.3. Port trust 모드

포트에 인입되는 트래픽에 대해서 QOS 를 수행하기 위해서는 패킷의 COS 또는 DSCP 값을 확인한 뒤, 이를 바탕으로 패킷의 우선 순위를 정하게 되어 있다. 하지만, 인입되는 트래픽의 COS 또는 DSCP

값이 믿을 수 있는지를 결정해 주어야 한다.

아무런 설정이 없는 경우에는 COS 또는 DSCP 값을 참조하지 않으며, 이 경우에는 포트에 설정된 default COS 값을 이용하여 동작하게 되어 있다. 참고로 이 default COS 값은 COS 또는 DSCP 가 없는 패킷 (예:untagged packet) 에 대한 기본 동작을 정의하는 용도로도 사용된다.

Trust mode 는 COS 또는 DSCP 에 대해서 설정할 수 있으며, 둘 다 설정할 수도 있고, 둘 다 설정하지 않을 수도 있다.

- trust DSCP (또는 BOTH) 모드이며, 패킷에 DSCP 값이 있다면 이를 이용한다.
- trust COS (또는 BOTH) 모드이며, 패킷에 COS 값이 있다면 이를 이용한다.
- trust COS (또는 BOTH) 모드이며, 패킷에 COS 값이 없다면, 포트에 설정된 default COS 값을 이용한다.
- 그 외의 경우에는 default COS 값을 이용한다.

Trust DSCP 모드이며, 패킷에 DSCP 값이 있는 경우라면, 해당 패킷은 DSCP 를 바탕으로 QOS 가 진행되며, 그렇지 않은 경우는 COS 를 바탕으로 QOS 가 진행된다.

표 13-4. port trust 설정 명령어

명령어	설명	모드
mls qos trust (cos|dscp|both)	해당 포트 인터페이스에 trust mode 를 설정한다.	interface
no mls qos trust	해당 포트 인터페이스에 trust mode 를 해제한다. 이 경우 none 으로 설정된다.	interface
mls qos cos <0-7>	포트의 디폴트 cos 값을 설정	interface
no mls qos cos	포트의 디폴트 cos 값 설정을 해제함.	interface

13.1.4. DSCP 변환 map 설정

Trust DSCP 모드에 의해서 해당 패킷이 DSCP 를 기준으로 동작하게 될 경우, 이 패킷은 다음과 같이 동작한다.

- DSCP 값에 따른 queueing 동작
- DSCP 값에 따른 COS marking(or remarking) 동작
- DSCP 값에 따른 DSCP remarking 동작

13.1.4.1. DSCP to queue 설정

DSCP 값에 따라 해당 패킷은 queueing 동작을 수행하는데, 이는 enable/disable 설정이 없이 항시 동작한다. 이 동작에 필요한 DSCP-queue map 값은 전역 설정으로 유지된다.

```
Switch#show mls qos map dscp-queue
  DSCP-TO-QUEUE MAP
    d1 :   d2  0   1   2   3   4   5   6   7   8   9
    ------------------------------------------------
     0 :       0   0   0   0   0   0   0   0   1   1
     1 :       1   1   1   1   1   1   2   2   2   2
     2 :       2   2   2   2   3   3   3   3   3   3
     3 :       3   3   4   4   4   4   4   4   4   4
     4 :       5   5   5   5   5   5   5   5   6   6
     5 :       6   6   6   6   6   6   7   7   7   7
     6 :       7   7   7   7
```

표 13-5. dscp-queue map 설정 명령어

명령어	설명	모드
mls qos map dscp-queue <0-63> … <0-63> to <0-7>	Dscp-queue map 을 설정한다.	config
no mls qos map dscp-queue	Dscp-queue map 을 초기화 한다..	config
show mls qos map dscp-queue	현재 dscp-queue map 설정을 보여준다.	Exec

13.1.4.2. DSCP to COS 설정

DSCP 값에 따라 해당 패킷은 COS marking (or remarking)동작을 수행할 수 있다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 DSCP to COS map 값은 전역 설정으로 유지된다.

```
Switch#show mls qos map dscp-cos
  DSCP-TO-COS MAP
    d1 :   d2  0   1   2   3   4   5   6   7   8   9
    ------------------------------------------------
     0 :       0   0   0   0   0   0   0   0   1   1
     1 :       1   1   1   1   1   1   2   2   2   2
     2 :       2   2   2   2   3   3   3   3   3   3
     3 :       3   3   4   4   4   4   4   4   4   4
     4 :       5   5   5   5   5   5   5   5   6   6
     5 :       6   6   6   6   6   6   7   7   7   7
     6 :       7   7   7   7
```

표 13-6. dscp-cos map 설정 명령어

명령어	설명	모드
mls qos map dscp-cos <0-63> … <0-63> to <0-7>	Dscp-cos map 을 설정한다.	config
no mls qos map dscp-cos	Dscp-cos map 을 초기화 한다..	config
mls qos dscp-cos	해당 포트 인터페이스에 dscp-cos marking 을 수행하도록 설정한다.	interface
no mls qos dscp-cos	해당 포트 인터페이스에 dscp-cos marking 을 수행하지 않도록 설정한다.	interface
show mls qos map dscp-cos	현재 dscp-cos map 설정을 보여준다.	Exec

13.1.4.3. DSCP to DSCP 설정

DSCP 값에 따라 해당 패킷은 DSCP remarking 동작을 수행할 수 있다. 이는 자기 자신의 DSCP 값을 변경한다는 의미에서 mutation 이란 표현을 사용한다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 DSCP to DSCP map 값은 전역 설정으로 유지된다. 디폴트는 1:1 이 기본이므로, 의미 있게 사용하기 위해서는 map 을 변경후에 포트 인터페이스에 적용해야 한다.

```
Switch#show mls qos map dscp-mutation
  DSCP MUTATION MAP
    d1 :   d2  0   1   2   3   4   5   6   7   8   9
    ----------------------------------------------------
     0 :        0   1   2   3   4   5   6   7   8   9
     1 :       10  11  12  13  14  15  16  17  18  19
     2 :       20  21  22  23  24  25  26  27  28  29
     3 :       30  31  32  33  34  35  36  37  38  39
     4 :       40  41  42  43  44  45  46  47  48  49
     5 :       50  51  52  53  54  55  56  57  58  59
     6 :       60  61  62  63
```

표 13-7. dscp-mutation map 설정 명령어

명령어	설명	모드
mls qos map dscp-mutation <0-63> … <0-63> to <0-63>	Dscp-mutation map 을 설정한다.	config
no mls qos map dscp-mutation	Dscp-mutation map 을 초기화 한다..	config
mls qos dscp-mutation	해당 포트 인터페이스에 dscp remarking 을 수행하도록 설정한다.	interface
no mls qos dscp-mutation	해당 포트 인터페이스에 dscp remarking 을 수행하지 않도록 설정한다.	interface

show mls qos map dscp-mutation	현재 dscp-mutation map 설정을 보여준다.	Exec

13.1.5. COS 변환 map 설정

Trust COS 모드에 의해서 해당 패킷이 COS 를 기준으로 동작하게 될 경우, DSCP 와 비슷하게 이 패킷은 다음과 같이 동작한다.

- COS 값에 따른 queueing 동작
- COS 값에 따른 DSCP marking(or remarking) 동작
- COS 값에 따른 COS remarking 동작

13.1.5.1. COS to queue 설정

COS 값에 따라 해당 패킷은 queueing 동작을 수행하는데, 이는 enable/disable 설정이 없이 항시 동작한다. 이 동작에 필요한 COS-queue map 값은 전역 설정으로 유지된다.

```
Switch#show mls qos map cos-queue
  COS-TO-QUEUE MAP
    COS  :   0   1   2   3   4   5   6   7
    ----------------------------------------
    Queue:   2   1   0   3   4   5   6   7
```

표 13-8. cos-queue map 설정 명령어

명령어	설명	모드
mls qos map cos-queue <0-7> <0-7>	Cos-queue map 을 설정한다.	config
no mls qos map cos-queue	Cos-queue map 을 초기화 한다..	config
show mls qos map cos-queue	현재 cos-queue map 설정을 보여준다.	Exec

13.1.5.2. COS to DSCP 설정

COS 값에 따라 해당 패킷은 DSCP marking (or remarking)동작을 수행할 수 있다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 COS to DSCP map 값은 전역 설정으로 유지된다.

```
Switch# show mls qos map cos-dscp
  COS-TO-DSCP MAP
    COS :   0   1   2   3   4   5   6   7
    ---------------------------------------
    DSCP:   0   8  16  24  32  40  48  56
```

표 13-9. cos-dscp map 설정 명령어

명령어	설명	모드
mls qos map cos-dscp <0-7> <0-63>	Cos-dscp map 을 설정한다.	config
no mls qos map cos-dscp	Cos-Dscp map 을 초기화 한다..	config
mls qos cos-dscp	해당 포트 인터페이스에 cos-dscp marking 을 수행하도록 설정한다.	interface
no mls qos cos-dscp	해당 포트 인터페이스에 cos-dscp marking 을 수행하지 않도록 설정한다.	interface
show mls qos map cos-dscp	현재 cos-dscp map 설정을 보여준다.	Exec

13.1.5.3. COS to COS 설정

COS 값에 따라 해당 패킷은 COS remarking 동작을 수행할 수 있다. 이는 자기 자신의 COS 값을 변경한다는 의미에서 mutation 이란 표현을 사용한다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 DSCP to DSCP map 값은 전역 설정으로 유지된다. 디폴트는 1:1 이 기본이므로, 의미 있게 사용하기 위해서는 map 을 변경후에 포트 인터페이스에 적용해야 한다.

```
Switch#show mls qos map cos-mutation
  COS MUTATION MAP
    In COS  :   0   1   2   3   4   5   6   7
    ----------------------------------------
    Out cos :   0   1   2   3   4   5   6   7
```

표 13-10. cos-mutation map 설정 명령어

명령어	설명	모드
mls qos map cos-mutation <0-7> <0-7>	Cos-mutation map 을 설정한다.	config
no mls qos map cos-mutation	Cos-mutation map 을 초기화 한다..	config
mls qos cos-mutation	해당 포트 인터페이스에 cosremarking 을 수행하도록 설정한다.	interface
no mls qos cos-mutation	해당 포트 인터페이스에 cos remarking 을 수행	interface

	하지 않도록 설정한다.	
show mls qos map cos-mutation	현재 cos-mutation map 설정을 보여준다.	Exec

13.2. ACL 설정

CS3400 장비는 다양한 ACL 설정이 가능하며 이를 이용해서, 쉽게 허용하고자 하는 패킷과 그렇지 않는 패킷을 구분할 수 있다.

본 장비에서 제공되는 ACL 은 크게 분류하여 standard IP ACL, extended IP ACL, MAC ACL 로 구분할 수 있다.

Standard IP ACL 은 source IP 로만 패킷을 구분한다. Standard IP ACL 을 위해서는 <1-99>, <1300-1999> 의 번호 대역이 할당되어 있으며, 그 외 번호가 아닌 이름으로도 생성하는 것이 가능하다.

Extended IP ACL 은 source IP, destination IP, protocol type 을 이용해서 패킷을 구분할 수 있다. 또한, TCP, UDP 패킷인 경우는 L4 src 및 dst port 를 이용해서 구분하는 것도 가능하며, ICMP 패킷의 경우는 icmp-type 을, IGMP 패킷인 경우는 igmp-type 을 이용해서 구분하는 것도 가능하다. <100-199> <2000-2699> 의 번호 대역이 할당되어 있으며, 그 외 번호가 아닌 이름으로도 생성하는 것이 가능하다.

MAC ACL 은 mac 주소를 이용해서 패킷을 구분하며, mac-access-list 라는 명령어로 분리 되어 있다. MAC ACL 용으로는 <1100-1199> 의 번호 대역이 할당되어 있다.

13.2.1. Standard IP ACL

Standard IP ACL 은 패킷의 source IP 로 패킷을 분류한다. 하나의 번호 또는 이름에 여러 개의 access-list 가 연결될 수 있으며, 개별의 조건마다 permit 또는 deny 동작을 수행할 수 있다.

Standard IP ACL 은 원래 <1-99> 의 99 개의 ACL 을 설정할 수 있도록 할당되었는데, 필요한 ACL 의 개수가 늘어나면서 <1300-1999> 의 700 개의 expanded 영역이 추가되었다. 또한, 문자로 이름을 정해서 사용할 수 있게 ACL 의 이름에 구애 받지 않고 만들 수 있다.

표 13-11. standard IP ACL 설정 명령어

명령어	설명	모드
access-list <1-99> (permit|deny) SRC_IP_ADDRESS	Standard IP ACL 을 설정한다.	config
no access-list <1-99> (permit|deny) SRC_IP_ADDRESS	Standard IP ACL 을 해제한다.	config

no access-list <1-99>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
access-list <1-99> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list <1300-1999> (permit|deny) SRC_IP_ADDRESS	Expanded range 의 Standard IP ACL 을 설정한다.	config
no access-list <1300-1999> (permit|deny) SRC_IP_ADDRESS	Expanded range 의 Standard IP ACL 을 해제한다.	config
no access-list <1300-1999>	해당 번호를 가지는 ACL 전부를 삭제한다.	config
access-list <1300-1999> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list standard WORD (permit|deny) SRC_IP_ADDRESS	Named Standard IP ACL 을 설정한다.	config
no access-list standard WORD (permit|deny) SRC_IP_ADDRESS	Named Standard IP ACL 을 해제한다.	config
no access-list standard WORD	해당 이름을 가지는 ACL 전부를 삭제한다.	config
access-list WORD remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
Show access-list	ACL 설정을 조회한다	Exed

위 명령어중에서 **SRC_IP_ADDRESS** 는 다음과 같은 방법으로 설정할 수 있다.

A.B.C.D A.B.C.D	*IP 대역을 wildcard 형태로 설정이 가능하다. 일반적인 IP 설정과는 반대로 masking 되는 부분이 0 이다.*
host A.B.C.D **A.B.C.D**	단 하나의 IP 주소만을 가르킬때는 host prefix 를 붙혀서 사용한다. 하나의 IP 만 주어진 경우는 host A.B.C.D 과 동일하게 처리된다.
any	모든 IP 주소를 지정하는 경우는 any 를 사용한다.

Notice 일반적으로 IP 대역을 의미할 경우 10.1.1.0/24 와 같은 표현은 10.1.1.0 255.255.255.0 과 동일한 의미를 가지며 이는 10.1.1.0 ~ 10.1.1.255 의 IP 구간을 의미한다.
하지만, ACL 설정에서는 wildcard 는 이와 반대로 설정되며 10.1.1.0 ~ 10.1.1.255 IP 구간을 지정하기 위해서는 10.1.1.0 0.0.0.255 로 지정해야 한다.

13.2.2. Extended IP ACL

Standard IP ACL 이 src ip 주소만으로 패킷을 구분하는데 반해, extended ip acl 을 src ip 와 dest ip 를 모두 사용한다. 뿐만 아니라 protocol type 을 이용해서 패킷을 구분할 수 있다. 또한, TCP, UDP 패킷인 경우는 L4 src 및 dst port 를 이용해서 구분하는 것도 가능하며, ICMP 패킷의 경우는 icmp-type 을, IGMP 패킷인 경우는 igmp-type 을 이용해서 구분하는 것도 가능하다.

Extended IP ACL 은 원래 <100-199> 의 100 개의 ACL 을 설정할 수 있도록 할당되었는데, 필요한 ACL 의 개수가 늘어나면서 <2000-2699> 의 700 개의 expanded 영역이 추가되었다. 또한, standard IP ACL 과 마찬가지로 문자로 이름을 정해서 사용할 수 있게 되었다.

표 13-12. extended IP ACL 설정 명령어

명령어	설명	모드
access-list <100-199> (permit|deny) (<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Extended IP ACL 을 설정한다.	config
access-list <100-199> (permit|deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	ICMP type 의 Extended IP ACL 을 설정한다.	config
access-list <100-199> (permit|deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Extended IP ACL 을 설정한다.	config
access-list <100-199> (permit|deny) (tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536>	TCP / UDP type 의 Extended IP ACL 을 설정한다.	config
no access-list <100-199> (permit|deny) (<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Extended IP ACL 을 해제한다.	config
no access-list <100-199>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
access-list <100-199> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list <2000-2699> (permit|deny) (<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Expanded range 의 Extended IP ACL 을 설정한다.	config
access-list <2000-2699> (permit|deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	ICMP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
access-list <2000-2699> (permit|deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
access-list <2000-2699> (permit|deny) (tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536>	TCP / UDP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
no access-list <2000-2699> (permit|deny) (<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Extended IP ACL 을 해제한다.	config
no access-list <2000-2699>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
access-list <2000-2699> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list extended WORD (permit|deny) (<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Named Extended IP ACL 을 설정한다.	config
access-list extended WORD (permit|deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS	ICMP type 의 Extended IP ACL 을 설정한다.	config

ICMP-TYPE		
access-list extended WORD (permit|deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Extended IP ACL 을 설정한다.	config
no access-list extended WORD (permit|deny) (<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Named Extended IP ACL 을 해제한다.	config
no access-list extended WORD	해당 이름을 가지는 ACL 전부를 삭제한다.	config
access-list WORD remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
Show access-list	ACL 설정을 조회한다	Exec

위 명령어중에서 **SRC_IP_ADDRESS** 와 **DST_IP_ADDRESS** 다음과 같은 방법으로 설정할 수 있다.

A.B.C.D A.B.C.D	*IP 대역을 wildcard 형태로 설정이 가능하다. 일반적인 IP 설정과는 반대로 masking 되는 부분이 0 이다.*
host A.B.C.D	단 하나의 IP 주소만을 가르킬때는 host prefix 를 붙혀서 사용한다.
any	모든 IP 주소를 지정하는 경우는 any 를 사용한다.

Notice A.B.C.D 는 명령어 상의 혼돈을 피하기 위해서 extended IP ACL 에서는 지원하지 않으며, 단일 IP 을 지정하는 경우는 host A.B.C.D 를 사용한다.

Notice 일반적으로 IP 대역을 의미할 경우 10.1.1.0/24 와 같은 표현은 10.1.1.0 255.255.255.0 과 동일한 의미를 가지며 이는 10.1.1.0 ~ 10.1.1.255 의 IP 구간을 의미한다.
하지만, ACL 설정에서는 wildcard 는 이와 반대로 설정되며 10.1.1.0 ~ 10.1.1.255 IP 구간을 지정하기 위해서는 10.1.1.0 0.0.0.255 로 지정해야 한다.

13.2.3. MAC ACL

MAC 주소를 이용하여 패킷을 구분하는 것이 가능하다. MAC ACL 은 원래 <1100-1199> 의 ACL 번호가 할당되어 있다. MAC ACL 은 IP ACL 과 달리 mac-access-list 라는 명령어를 사용한다.

표 13-13. standard IP ACL 설정 명령어

명령어	설명	모드
mac-access-list <1100-1199> (permit|deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS <1-8>	MAC ACL 을 설정한다.	config

no mac-access-list <1100-1199> (permit|deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS <1-8>	MAC ACL 을 해제한다.	config
no mac-access-list <1100-1199>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	
Show mac-access-list	MAC ACL 설정 상태를 조회한다.	Exec

위 명령어중에서 **SRC_MAC_ADDRESS** 와 **DST_MAC_ADDRESS** 다음과 같은 방법으로 설정할 수 있다. 단 SRC_MAC 과 DST_MAC 둘다 any 가 될 수는 없다.

H.H.H H.H.H	*MAC 대역을 wildcard 형태로 설정이 가능하다..*
any	모든 MAC 주소를 지정하는 경우는 any 를 사용한다.

13.2.4. ACL 의 인터페이스 적용

위와 같이 설정된 ACL 은 다음과 같이 인터페이스에 적용이 가능하다. 여기서 인터페이스는 다음 Physical 인터페이스를 의미하며, router port, switchport 로 지정된 포트 인터페이스에 적용이 가능하다.

Input 방향과 output 방향에 걸 수 있으며, 해당 인터페이스로 들어 오는 또는 나가는 패킷에 대해서 ACL 을 설정할 수 있다.

표 13-14. ACL 의 인터페이스 적용 설정 명령어

명령어	설명	모드
ip access-group { <1-199> | <1300>2699> | WORD) } {in|out}	해당 인터페이스에 acl 을 설정한다.	Interface
no ip access-group { <1-199> | <1300>2699> | WORD) } {in|out}	해당 인터페이스에 acl 을 해제한다.	Interface

Notice Router port 란 no switchport 상태인 port 를 의미한다.

Notice Service-policy 는 ACL 과 합쳐서 최대 input 방향으로 1500 개, output 방향으로 1500 개의 rule 을 설정할 수 있다.

Notice Input 방향으로는 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능하다, output 방향으로는 둘중 하나만 설정이 가능하다.

13.3. Service-policy 설정

단순한 ACL 설정 이외에 더 복잡한 형태의 QOS 설정을 위해서는 class-map 과 policy-map 을 이용해서 다양한 형태의 rule 과 action 을 설정하는 것이 가능하다. Class-map 에서는 ACL 또는 특정한 패킷의 성질을 이용해서 패킷을 분류하고, policy-map 에서는 이렇게 분류된 패킷에 특정한 동작을 수행할 수 있도록 해준다.

Class-map 에서는 ACL 을 통한 패킷 분류 뿐만 아니라 ethertype, cos, vlan, protocol, dscp, ip-preedence(TOS), l4 port, tcp flag, mlps flag 등 다양한 방법으로 패킷을 분류하는 것이 가능하다. Class-map 은 ACL 을 이용할 수 있을 뿐만 아니라, AND OR 조합으로 ACL 과 다른 항목을 조합하여 사용하는 것도 가능하다.

이러한 class-map 으로 분류된 트래픽은 기본적인 permit / drop 동작이외에도 queueing, cos marking / remarking, dscp marking / remarking, rate-limit 등의 동작을 수행하는 것이 가능하다. 또한 nexthop 을 연동하여 PBR (Policy based routing) 이 가능하게 할 수 있다. QOS 와 상관 없지만, trap-cpu, mirror, redirect, netflow 등의 동작을 수행하게 하여 장비 운용에 필요한 다양한 동작을 수행토록 할 수도 있다.

이렇게 선언된 policy-map 은 service-policy 라는 명령을 통해서 switchport, router port interface 에 input 또는 output 방향에 적용하여 사용할 수 있다.

13.3.1. Class-map

Class-map 은 패킷을 분류하기 위한 목적으로 생성된다. 패킷의 분류는 기본적으로 ACL 을 사용하여 할수 있으며, 그외에도 ethertype, cos, vlan, protocol, dscp, ip-preedence(TOS), l4 port, tcp flag, mlps flag 등 다양한 방법으로 패킷을 분류하는 것이 가능하다.

ACL 은 ip acl 과 mac-acl 을 모두 사용 할 수 있지만, 1 개의 ACL 만 연동할 수 있다. 1 개의 ACL 이 가질 수 있는 세부 항목의 최대 개수는 750 개이며, 750 개 이상의 ACL 을 적용하고자 하면, 여러 개의 ACL 로 분리 한 뒤 class-map 도 각각 따라 만들어 연동해 주어야 한다.

ACL 을 비롯한 다른 분류 조건은 기본적으로 AND 연산을 수행하는데, 예를 들어 ACL 과 DSCP 를 같이 설정하면, 두 개의 조건이 모두 해당되는 패킷만 분류 할 수 있다. Class-map 을 선언할 때 match-any 옵션을 명시적으로 선언 하는 경우는 OR 연산을 수행하여, 둘중 하나만 만족하더라도 패킷이 분류 된다.

표 13-15. Class-map 설정 명령어

명령어	설명	모드
class-map WORD	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
class-map match-all WORD	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
class-map match-any WORD	OR 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
no class-map WORD	Class-map 을 삭제한다..	Config
match access-group NAME	ACL 을 이용한 분류 조건을 설정한다.	cmap
match cos <0-7>	Cos 을 이용한 분류 조건을 설정한다.	cmap
match ethertype WORD	Ethertype 을 이용한 분류 조건을 설정한다.	cmap
match ip-dscp <0-63>	Dscp 을 이용한 분류 조건을 설정한다.	cmap
match ip-precedence <0-7>	Ip-precedence 을 이용한 분류 조건을 설정한다.	cmap
match protocol (<0-255>|icmp|igmp|ip|ospf|ospf|pim|tcp|udp)	Ip protocol 를 이용한 분류 조건을 설정한다.	cmap
match protocol arp (|A.B.C.D/M A.B.C.D/M)	Arp 를 이용한 분류 조건을 설정한다	cmap
match layer4 {source-port|destination-port} <1-65536>	L4 port 을 이용한 분류 조건을 설정한다.	cmap
match mpls exp-bit topmost <0-7>	Mpls flag 을 이용한 분류 조건을 설정한다.	cmap
match tcp-control VALUE	Tcp-control 을 이용한 분류 조건을 설정한다.	cmap
match vlan <1-4095>	VLAN 을 이용한 분류 조건을 설정한다.	cmap

Notice Ethertype 의 분류는 4 자리 hexadecimal 로 분류한다. 예를 들어 ARP 타입인 경우 0806 으로 지종하면 된다.

Notice Tcp-control 을 6 자리 2 진수로 분류한다. 예를 들어 5 번째 자리인 SYN flag 를 보고자 할때는 000010 으로 선언하면 된다.

13.3.2. Policy-map

Class-map 으로 분류된 트래픽은 기본적인 permit / drop 동작이외에도 queueing, cos marking / remarking, dscp marking / remarking, rate-limit 등의 동작을 수행하는 것이 가능하다. 또한 nexthop 을 연동하여 PBR (Policy based routing) 이 가능하게 할 수 있다. QOS 와 상관 없지만, trap-cpu, mirror, redirect, netflow 등의 동작을 수행하게 하여 장비 운용에 필요한 다양한 동작을 수행토록 할 수도 있다.

하나의 policy-map 에는 최대 100 개의 class-map 에 대해서 동작을 지정하는 것이 가능하다. Class-map 당 1000 개의 항목을 가지는 ACL 이 사용될 수 있기에, 이론상 10 만개의 ACL 항목을 하나의 policy-map 에서 제어가 가능하지만, 실제 H/W 의 제약으로 이렇게 많은 수를 rule 을 사용할 수는 없

다.

각 class-map 별로 패킷에 대한 동작을 수행할 수 있는데, 다음과 같은 것들을 지정할 수 있으며, 동작의 조건에 따라 중복 적용도 가능하다. 예를 들어 하나의 class-map 에 대해서 queueing 7 을 주며, cos marking 6 을 하고, dscp marking 54 를 동시에 수행하도록 할 수도 있다. 동작의 특성상 drop 같은 경우는 다른 동작과 중복되지 않는다.

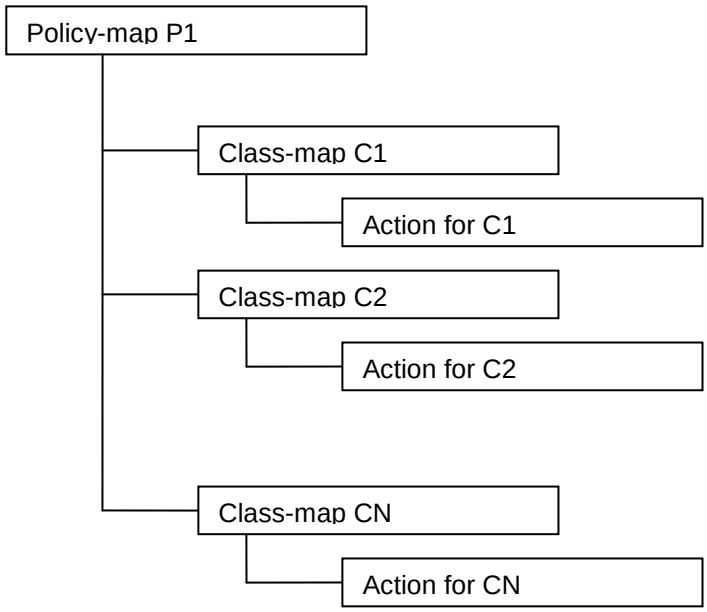


그림 13-1. policy-map 의 계층도

Marking 과 remarking 은 별다른 구분없이 사용되는데, 들어오는 패킷에 해당 필드가 없으면 자동으로 marking 을 수행하고, 해당 필드가 있으면 remarking 으로 동작한다. Trap-cpu, mirror, redirect, netflow 등의 동작은 QOS 와는 직접적인 상관은 없지만, class-map 과 policy-map 을 이용해서 제어하는 것이 가능하다.

표 13-16. policy-map 설정 명령어

명령어	설명	모드
policy-map NAME	해당 이름의 policy-map 을 생성하고 해당 노드로 이동한다.	Config
no policy-map NAME	해당 이름의 policy-map 을 삭제한다..	Config
class NAME	Class-map 의 동작을 지정하는 sub node 로 이동한다	pmap
no class NAME	해당 class-map 동작 설정을 삭제한다.	pmap
drop	해당 class-map 으로 분류된 트래픽을 drop 한	pmap-c

	다.	
set cos <0-7>	Cos marking 설정	pmap-c
set drop-precedence <0-2>	Drop precedence 설정	pmap-c
set ip-dscp <0-63>	Dscp marking 설정	pmap-c
set ip-precedence <0-7>	Ip precedence (tos) 설정	pmap-c
set queueing <0-7>	Queueing 설정	pmap-c
set tag-vlan <1-4094>	vlan id 를 설정	pmap-c
set inner-tag-vlan <2-4094> outer-tag-vlan <2-4094>	q-in-q 에서 inner vlan id 와 outer vlan id 를 설정	pmap-c
police <1-10000000> <1-10000000> exceed-action drop	Rate-limit 설정	pmap-c
police aggregate NAME	Aggregated rate-limit 설정	pmap-c
nexthop A.B.C.D { priority <1-8> | }	PBR nexthop 설정 및 nexthop priority 설정	pmap-c
netflow	Netflow 설정	pmap-c
redirect IFNAME	Redirect 설정	pmap-c
mirror	Mirror 설정	pmap-c
trap-cpu { high-priority| }	CPU trap 설정	pmap-c

13.3.3. Service-policy

위와 같은 방법으로 설정된 policy-map 은 switchport 또는 router port interface 에 적용이 가능하다. ACL 과 마찬가지로 input 과 output 방향에 설정할 수 있다. 단, output 방향으로는 service-policy 와 ACL 중 하나만 설정이 가능하며, input 방향은 두 가지 설정을 동시에 적용이 가능하다.

표 13-17. service-policy 설정 명령어

명령어	설명	모드
service-policy { input | output } NAME	해당 이름의 policy-map 을 인터페이스에 적용한다.	interface
no service-policy { input | output } NAME	해당 이름의 policy-map 을 인터페이스에서 삭제한다.	interface

Notice Router port 란 no switchport 상태인 port 를 의미한다.

Notice Service-policy 는 ACL 과 합쳐서 최대 input 방향으로 1500 개, output 방향으로 1500 개의 rule 을 설정할 수 있다.

Notice Input 방향으로는 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능하다, output 방향으로는 둘 중 하나만 설정이 가능하다.

13.4. COPP

COPP 는 Control Plane Policing 라는 의미로 CPU 로 유입되는 트래픽에 대한 rate-limit 및 QOS 정책을 적용하는 것을 의미한다. CPU 에는 프로토콜에 관련된 다양한 제어 패킷이 유입되는데, 특정한 패킷이 과도하게 유입되는 경우에는 CPU 의 성능 문제가 발생할 수 있으며, 더 중요한 우선순위를 가지는 다른 프로토콜 패킷이 처리되지 않을 수 있는 문제를 야기할 수 있다. 그러므로, 패킷별 우선순위 설정 및 rate-limit 설정을 통해 트래픽을 정리해주는 기능이 필요하다.

13.4.1. Service-policy on COPP

Control Plane 에 service-policy 를 적용해서 CPU 로 유입되는 트래픽에 대해 Policing 을 수행할 수 있다.

표 13-18. service-policy 의 control-plane 적용 설정 명령어

명령어	설명	모드
control-plane	Control-plane 모드로 진입한다	configure
service-policy input NAME	해당 이름의 policy-map 을 control-plane 에 적용한다.	Control-plane
no service-policy input NAME	해당 이름의 policy-map 을 control-plane 에 적용을 해지한다.	Control-plane

Notice Control-plane 에서 Service-policy 가 사용되는 경우에는 policy-map 에서 설정하는 동작 중 **police**, **drop**, **set queueing** 의 동작만 수행이 된다.

13.4.2. Rate-limit on COPP

CPU 로 유입되는 특정 트래픽에 대해서 rate-limit 을 설정 할 수 있다.

표 13-19. rate-limit 의 control-plane 적용 설정 명령어

명령어	설명	모드
rate-limit arp-reply <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 arp-reply 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane

rate-limit arp-request <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 arp-request 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit igmp <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 igmp 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit ip-control-over-multicast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 ip-control 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit ipv6-neib-sol <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 ipv6 ns 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit l4-port (both|tcp|udp) (both|multicast|unicast) <1-65535> <1-65535> <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 L4 트래픽에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit mld <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 mld 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit multicast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 multicast 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit protocol <1-255> <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 특정 protocol 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit ripv1 <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 rip(version 1) 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit tcp-syn <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 tcp-syn 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit udp-broadcast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 udp broadcast 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane

14

IP-OPTION

14.1. IP OPTOIN 개요

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

14.2. IP OPTOIN 명령어

IP OPTION 명령으로 설정 가능한 parameter 들은 다음과 같다.

표 18.1 IP OPTION 명령어

명령어	설명	모드
ip option icmp-drop icmp-type (any|<0-255>|echo-reqeust|echo-reply) length *<1-65535>*	ICMP 패킷 차단을 위한 icmp-type 및 패킷 사이즈를 설정한다.	Config
no ip option icmp-drop	ICMP 패킷 차단 설정을 해제한다.	Config
ip icmp-ttl-exceed-send	TTL Exceed ICMP 에러 전송을 허용 또는 차단한다. **Default) send**	Config
no ip icmp-ttl-exceed-send	TTL Exceed ICMP 에러 전송 설정을 해제한다.	Config
ip option icmp-unreachable-send	ICMP unreachable 에러 전송을 허용 또는 차단한다. **Default) send**	Config

no ip option icmp-unreachable-send	ICMP unreachable 에러 전송 설정을 해제한다.	Config
ip option ip_default_ttl *VALUE*	Default TTL 크기를 설정한다. **Default) 64**	Config
no ip option ip_default_ttl	Default TTL 크기 설정을 기본값으로 변경한다.	Config
ip option ipfrag_time *VALUE*	메모리에서 IP fragment 를 유지하는 시간을 설정한다. **Default) 30**	Config
no ip option ipfrag_time	메모리에서 IP fragment 를 유지하는 시간을 기본값으로 변경한다.	Config
ip option tcp-conn-rate-limit profile-id <*1-128*> (any|*PORT*) period <*1-3600*> count <*1-655535*>	TCP connection rate-limit profile 을 추가한다. TCP 목적지 포트에 대해 period 이내에 count 이상 TCP 연결을 시도하는 경우 로깅 및 차단할 수 있다.	Config
no ip option tcp-conn-rate-limit profile-id <*1-128*>	Profile-id 에 해당하는 TCP connection rate-limit profile 을 삭제한다.	Config
ip option tcp_fin_timeout *VALUE*	FIN-WAIT-2 상태의 소켓 유지 시간을 설정한다. **Default) 60**	Config
no ip option tcp_fin_timeout	FIN-WAIT-2 상태의 소켓 유지 시간을 기본값으로 변경한다.	Config
ip option tcp_keepalive_probes *VALUE*	연결이 끊어졌다고 여길 때까지 발생 시킬 keepalive probe 메시지 수를 설정한다. **Default) 9**	Config
no ip option tcp_keepalive_probes	Keepalive probe 메시지 수를 기본값으로 변경한다.	Config
ip option tcp_keepalive_time *VALUE*	Keepalive 가 활성화되었을 경우 keepalive 메시지 전송 시간을 설정을 설정한다. **Default) 7200**	Config
no ip option tcp_keepalive_time	Keepalive 메시지 전송 시간을 기본값으로 변경한다.	Config
ip option tcp_max_syn_backlog *VALUE*	TCP syn backlog queue 의 최대치 설정이다. **Default) 1024**	Config
no ip option tcp_max_syn_backlog	TCP syn backlog queue 의 최대치 설정을 기본값으로 변경한다.	Config
ip option tcp_max_tw_buckets *VALUE*	Timewait 소켓의 수를 설정한다. **Default) 18700**	Config
no ip option tcp_max_tw_buckets	Timewait 소켓의 수를 기본값으로 변경한다.	Config
ip option tcp_retries1 *VALUE*	의심스러운 TCP session 에 대한 재전송 횟수를 설정한다.	Config

	Default) 3	
no ip option tcp_retries1	의심스러운 TCP session 에 대한 재전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_retries2 *VALUE*	종단전 재전송 횟수를 설정한다. **Default)15**	Config
no ip option tcp_retries2	종단전 재전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_syn_retries *VALUE*	활성 TCP 연결에서 재전송을 위해 지정한 시간만큼 지난 뒤에 초기화 SYN 패킷을 보낸다. **Default) 5**	Config
no ip option tcp_syn_retries	TCP syn 재 전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_syncookies (default|disable|enable)	Syn flood attack 방어를 위해 설정한다. **Default) enable**	Config
ip option telnet-acl access-group <1-99>	Telnet 접속을 access-group 에 대해 허용 및 차단하도록 설정한다.	Config
no ip option telnet-acl acess-group <1-99>	Access-group 에 의한 telnet 접속 제한 설정을 해제한다.	Config

15 Setting Time and Calendar

CS3400 시리즈 스위치는 time-of-day 서비스를 제공한다. 이 서비스는 여러 장비들이 같은 시각으로 동기화를 맞추거나, 다른 시스템에 시간 서비스를 제공할 수 있도록 스위치가 정확한 현재 시간을 유지하도록 한다.

15.1. Understanding Time Sources

CS3400 시리즈 스위치는 두 개의 클락(clock)을 가진다. 하나는 배터리에 의해 유지되는 하드웨어 클락 (“calendar” CLI 명령 참조)이고 나머지 하나는 소프트웨어 클락 (“clock” CLI 명령 참조) 이다. 이 두 개의 클락은 각각 관리된다.

시스템이 사용하는 기본 시간 소스는 소프트웨어 클락이다. 소프트웨어 클락은 시스템 시작 후부터 현재 시각을 유지한다. 소프트웨어 클락은 여러 가지 소스로부터 설정할 수 있고, 다양한 방법을 통해 다른 시스템으로 전달된다. 소프트웨어 클락은 시스템이 초기화되거나 리부트 될 때 하드웨어 클락을 사용해서 초기화된다. 그리고 나서 다음의 소스들을 사용해서 변경할 수 있다:

- Network Time Protocol (NTP)
- 수동 설정 (하드웨어 클락 사용)

소프트웨어 클락은 내부적으로 Coordinated Universal Time (UTC), 또는 Greenwich Mean Time (GMT) 기반으로 시간 정보를 관리한다. 장비가 사용되는 지역의 시간 정보를 반영할 수 있도록 지역 시간대 (time zone)과 서머 타임 (daylight savings time)을 설정할 수 있다.

15.1.1. Network Time Protocol

NTP 는 네트워크에 연결된 장비들의 시간 동기화를 위해 설계된 프로토콜이다. NTP 는 IP/UDP 서비스를 이용해서 동작한다. RFC1305 에 NTP 버전 3 에 대해 정의되어 있다.

NTP 네트워크는 타임 서버(time server)에 연결된 라디오 클락(radio clock) 또는 원자 클락 (atomic

clock)과 같은 신뢰성있는 타임 소스(authoritative time source)로부터 시간 정보를 획득한다. NTP 는 이 시간 정보를 네트워크를 통해 분배한다. NTP 는 두 시스템 사이에 밀리초 단위의 시간 동기화를 맞추는데 분당 하나의 패킷을 사용할 정도로 매우 효과적인 프로토콜이다.

NTP 는 신뢰성있는 타임 소스로까지 얼마나 많은 NTP "hops"이 존재하는 지를 나타내는 "stratum"이란 개념을 사용한다. 일반적으로 "stratum 1" 타임 서버에는 타임 소스가 직접 연결 되어 있다. "stratum 2" 타임 서버는 "stratum 1" 타임 서버로부터 NTP 를 통해 시간 정보를 수신한다. NTP 는 사용할 수 있는 타임 서버중 가장 작은 stratum 을 가진 타임 서버를 자신의 시간 소스로 선택한다.

NTP 는 의심스러운 시간 정보로 동기화를 하지 않기 위해 다음 두 가지 방법을 제공한다.

- NTP 는 자신을 소스로 동기화한 장비와는 동기화하지 않는다.
- NTP 는 여러 장비에서 얻은 시간을 비교하고 다른 것과 큰 시간차를 보이는 장비와는 stratum 이 작아도 동기화하지 않는다.

15.1.2. Hardware Clock

CS3400 시리즈 스위치는 시스템이 재시작되거나 전원이 꺼지더라도 현재 시각을 유지할 수 있도록 배터리에 의해 유지되는 하드웨어 클락을 가진다. 하드웨어 클락은 시스템이 시작할 때 소프트웨어 클락을 초기화하는데 사용된다.

15.2. Configuring NTP

이 장에서는 시스템에서 NTP 를 사용할 수 있도록 다음과 같은 절차에 대해 설명한다:

- Configuring Poll-Based NTP Associations
- Configuring NTP Authetnication
- Configuring the Source IP Address for NTP Packets
- Configuring the System as an Authoritative NTP Server
- Updating the Hardware Clock

15.2.1. Configuring Poll-Based NTP Associations

NTP 를 사용하는 네트워크 장비는 시간 소스와 동기화를 맞추는데 여러 가지 동작 모드를 제공한다. 장비가 네트워크로부터 시간 정보를 획득하는 방법으로는 호스트 서버에게 시간 정보를 요청(poll-based association)하거나 브로드 캐스트되는 NTP 정보를 청취하는 두 가지 방법이 있다. 이 장에서는 서버에게 요청하는 모드에 대해 설명한다.

다음은 가장 많이 사용되는 서버 요청 모드이다:

- Client mode
- Symmetric active mode

Client 와 Symmetric active 모드는 NTP 에 높은 수준의 시간 정밀도가 요구될 때 사용된다.

클라이언트 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사한다. 장비는 조사된 여러 개의 시간 서버들 중 하나를 선택해서 시간 동기를 맞춘다. 이 경우 장비와 시간 서버는 클라이언트-서버 관계를 맺고 있기 때문에, 장비는 다른 클라이언트 장비가 보낸 시간 정보는 사용하지 않는다. 이 모드는 다른 로컬 클라이언트에게로 시간 정보를 제공할 필요가 없는 시스템에 유용하다. 클라이언트 모드에서 시간 동기를 맞추고 싶은 시간 서버를 명시하기 위해 **ntp server** 명령을 사용하면 된다.

Symmetric active 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사하고, 로컬 호스트에게는 시간 정보를 제공한다. 이 모드는 peer-to-peer 관계이기 때문에 장비는 자신이 통신하는 로컬 네트워크 장비의 시간 정보도 함께 저장한다. 이 모드는 복잡한 네트워크 경로를 통해 연결된 상호 중복된 서버가 존재할 경우에 사용되어야 한다. 대부분의 stratum 1 과 stratum 2 서버는 이런 형태의 네트워크 설정을 사용한다. Symmetric active 모드를 사용하려면 **ntp peer** 명령을 사용하라.

NTP 의 동작 모드를 결정하는 것은 장비의 역할 (서버 또는 클라이언트)과 stratum 1 서버 설정이다.

Command	***Purpose***
Switch(config)# **ntp server** *ip-adress*	Client 모드로 NTP 설정
Switch(config)# ntp peer *ip-adress*	Symmetric active 모드로 NTP 설정

15.2.2. Configuring NTP Authentication

암호화된 NTP 인증은 인증 키와 NTP 패킷의 정보를 사용하기 전에 신뢰할 수 있는 장비로부터 전송된 패킷인지를 검사하는 인증 절차를 사용한다.

인증 절차는 NTP 패킷이 생성되는 순간부터 시작된다. MD5 message digest 알고리즘에 의해 암호화된 체크섬(checksum) 키가 생성되고 NTP 패킷에 포함되어 클라이언트에게 전송된다. 패킷을 수신한 클라이언트는 패킷의 암호화된 체크섬 키를 해독한 후 자신의 trusted 키와 비교한다. 패킷이 유효한 인증 키를 포함하고 있다면 클라이언트는 이 패킷의 시간 정보를 허용한다. 클라이언트와 일치하는 인증 키를 포함하고 있지 않는 NTP 패킷은 폐기된다.

NTP 인증이 올바르게 설정된 후부터 장비는 오직 신뢰할 수 있는 시간 소스와 시간을 동기화 시킨다. 장비에서 암호화된 NTP 패킷을 송수신하게 하려면, 글로벌 설정 모드에서 다음의 명령을 사용하라:

	Command or Action	***Purpose***
Step 1	Switch(config)# **ntp authenticate**	NTP 의 인증 기능을 활성화 시킨다.
Step 2	Switch(config)# **ntp athentication-key** *key-*	인증 키를 정의한다.

Step 3	*number* **md5** *value* Switch(config)# **ntp trusted-key** *key-number*	각 키는 키 번호와 종류 그리고 값을 가진다. 현재 지원되는 키 종류는 MD5 이다. 신뢰하는 인증 키를 정의한다. 만약 인증키가 신뢰하는 키라면, 시스템은 NTP 패킷에 이 키를 사용하는 시스템과 시간 동기를 시도한다.
Step 4	Switch(config)# **ntp server** *ip-address* **key** *key-number*	소프트웨어 클락이 NTP 타임 서버와 동기화 되도록 허용한다.

15.2.3. Configuring the Source IP Address for NTP Packets

시스템이 NTP 패킷을 전송할 때, NTP 패킷의 소스 IP 주소는 NTP 패킷을 전송하는 인터페이스의 주소로 설정된다. NTP 패킷의 소스 IP 주소로 특정 인터페이스의 IP 주소를 사용하고 싶다면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	***Purpose***
Switch(config)# ntp source *interface*	IP 주소를 빌려올 인터페이스를 지정한다.

15.2.4. Configuring the System as an Authoritative NTP Server

시스템이 외부의 시간 소스와 동기화가 되지 않더라도 시스템을 NTP 서버로 사용하려면 글로벌 설정 모드에서 다음의 명령을 수행하라:

Command	***Purpose***
Switch(config)# ntp master [*stratum*]	시스템을 NTP 서버로 설정한다.

CS3400 시리즈 스위치는 stratum 1 서비스를 지원한다. 하지만 장비 내부에 연결 가능한 라디오 혹은 원자 클락이 존재하지는 않으므로 CS3400 시리즈 스위치를 stratum 1 로 설정하는 것은 권장하지 않는다.

15.2.5. Updating the Hardware Clock

하드웨어 클락을 가진 장비에서, 소프트웨어 클락으로 하드웨어 클락을 주기적으로 업데이트 하도록 설정할 수 있다. NTP 로 설정되는 소프트웨어 클락이 하드웨어 클락보다 더 정확하기 때문에 NTP 를 사용하는 장비에서는 이렇게 설정하는 것이 바람직하다.

하드웨어 클락을 NTP 시각과 동기화시키려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	***Purpose***
Switch(config)# ntp update-calendar	시스템의 하드웨어 클락을 주기적으로 소프트웨어 클락으로 업데이트

	하도록 설정한다.

15.3. Configuring Time and Date Manually

사용 가능한 타임 소스가 없다면, 시스템이 시작된 후에 현재 시각을 직접 설정할 수 있다.

15.3.1. Configuring the Time Zone

시간대 정보를 설정하려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	***Purpose***
Switch(config)# clock timezone *zone hours-offset* [*minutes-offset*]	시간대를 설정한다. 인자 zone 은 시간대의 이름을 표시한다 (보통 표준 시간대 이름을 사용). 인자 *hours-offset* 은 UTC 와의 시차를 명시한다. 인자 *minutes-offset* 은 UTC 와의 분차를 명시한다.

15.3.2. Configuring Summer Time (Daylight Savings Time)

매년 특정 날짜에 시작되고 끝나는 서머 타임 (daylight savings time)을 설정하려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	***Purpose***
Switch(config)# clock summer-time *zone* recurring [*week day month hh:mm week day month hh:mm* [offset]]	반복되는 서머타임의 시작과 끝을 설정. 인자 *offset* 은 서머 타임 동안 추가되는 분을 표시한다.

서머 타임이 매년 동일하게 반복되지 않는다면, 글로벌 설정 모드에서 다음의 명령으로 다음 서머타임이 시작되는 정확한 날짜를 설정할 수 있다:

Command	***Purpose***
Switch(config)# clock summer-time *zone* date *month date year hh:mm month date year hh:mm* [offset] **또는** **Switch(config)# clock summer-time *zone* date *date onth date year hh:mm date month year hh:mm* [offset]**	특정 서머타임의 시작과 끝을 설정. 인자 *offset* 은 서머 타임 동안 추가되는 분을 표시한다.

15.3.3. Manually Setting the Software Clock

일반적으로 시스템이 NTP 와 같은 유효한 시간 메카니즘에 의해 시간 동기화가 이루어지거나, 시스템이 하드웨어 클락을 가지고 있다면 소프트웨어 클락을 설정할 필요가 없다. 만약 사용가능한 시간 소스가 없다면 이 명령을 사용하라. 이 명령으로 설정되는 시간은 시간대의 영향을 받는다. 소프트웨어 클락을 직접 설정하려면, EXEC 모드에서 다음의 명령을 사용하라:

Command	***Purpose***
Switch# clock set *hh:mm:ss day month year* **또는** **Switch# clock set *hh:mm:ss month day year***	소프트웨어 클락 설정.

15.4. Using the Hardware Clock

CS3400 시리즈 스위치는 소프트웨어 기반의 클락과는 독립된 하드웨어 기반의 클락을 추가로 가지고 있다. 하드웨어 클락은 충전이 가능한 배터리를 가진 칩(chip)으로 장비가 리부트 되더라도 시각 정보를 유지할 수 있다.

소프트웨어 클락은 정확한 시각 정보를 유지하기위해 네트워크의 권위있는 타임 소스로부터의 시간 업데이트 정보를 수신해야 한다. 그리고 시스템이 동작중인 동안 소프트웨어 클락은 하드웨어 클락을 주기적으로 업데이트 해줘야 한다.

하드웨어 클락을 설정하기 위해 다음의 작업을 할 수 있다:

- Setting the Hardware Clock
- Setting the Software Clock from the Hardware Clock
- Setting the Hardware Clock from the Software Clock

15.4.1. Setting the Hardware Clock

하드웨어 클락은 소프트웨어 클락과 별도로 시간을 관리한다. 하드웨어 클락은 시스템이 재시작되거나 전원이 꺼진 상태에서도 계속 동작한다. 일반적으로 하드웨어 클락은 시스템이 설치될 때 한 번만 설정하면 된다.

믿을 수 있는 외부 시간 소스를 사용하고 있다면 하드웨어 클락을 직접 설정하지 않도록 한다. 시간 동기는 NTP 를 이용해서 이뤄질 것이다.

만약 사용할 수 있는 외부 시간 소스가 없다면 하드웨어 클락을 설정하기 위해 EXEC 모드에서 다음의 명령을 사용하라:

Command	*Purpose*
Switch# calendar set *hh:mm:ss day month year* 또는 **Switch# calendar set *hh:mm:ss month day year***	하드웨어 클락 설정.

15.4.2. Setting the Software Clock from the Hardware Clock

새로운 하드웨어 클락 설정으로 소프트웨어 클락을 설정하려면, EXEC 모드에서 다음의 명령을 상용하라:

Command	*Purpose*
Switch# clock read-calendar	하드웨어 클락으로 소프트웨어 클락 설정.

15.4.3. Setting the Hardware Clock from the Software Clock

새로운 소프트웨어 클락 설정으로 하드웨어 클락을 설정하려면, EXEC 모드에서 다음의 명령을 사용하라:

Command	*Purpose*
Switch# clock update-calendar	스프트웨어 클락으로 하드웨어 클락 설정.

15.5. Monitoring Time and Calendar Services

클락, 카렌더 그리고 NTP 정보를 조회하려면 다음의 명령들을 사용하라.

Command	*Purpose*
Switch# **show calendar** Switch# **show clock** Switch# **show ntp associations** [**detail**]	현재 하드웨어 클락 조회 현재 소프트웨어 클락 조회 NTP association 상태 조회
Switch# show ntp status	NTP 상태 조회

15.6. Configuration Examples

15.6.1. Clock, Calendar, and NTP Configuration Examples

다음 예에서 하드웨어 클락을 가진 스위치는 두 개의 다른 시스템과 서버 관계를 가지고 있고, 주기적으로 하드웨어 클락을 업데이트 한다.

```
clock timezone KST 9
ntp update-calendar
ntp server 192.168.13.57
ntp server 192.168.11.58
```

16 Utilities

16.1. 개 요

본 장에서는 시스템 운영에 필요한 기타 기능들에 대해 설명하도록 한다.

16.2. 상태 dump 명령

16.2.1. 명령어

각 모듈들(시스템 환경, MULTICAST, 라우팅, 드라이버 등)의 시스템 로깅 메시지를 dump 하기 위한 목적으로 “show tech-support” 명령을 사용한다.

```
# show tech-support
```

시스템 운영 시 문제가 발생했을 경우, 기존에는 여러 명령을 입력하여 모듈들의 동작 상태를 확인해야 하는 번거로움이 있었지만, 이 명령을 사용함으로써, 미리 정의해 놓은 모듈들의 주요 명령들이 수행되어 그 결과 메시지가 출력되기 때문에, 각 모듈 담당자들이 이 메시지를 통해 좀 더 빠르게 확인할 수 있다.

출력 메시지는 페이징이 되지 않기 때문에, 출력 메시지는 명령의 수행이 끝날 때까지 출력된다. 이 명령의 수행 도중에, 출력을 멈추기 위해서는 Ctrl+C 를 입력하여 중단시켜야 한다.

다음의 예를 살펴보도록 하자.
Show tech 명령의 수행은 CPU 에 상당한 부하를 가하기 때문에, 처리시간도 길다. CPU 가 100% 지속됨에 따라 프로토콜 끊김 현상이 발생할 수 있기 때문에, 다음과 같이 운용자에게 다시 한번 명령을 수행할 것인지에 대한 confirm 을 요청한다.

```
Switch# show tech-support

        --- Display the system information ---
        --------------------------------------

MODEL-NAME         : CS3400
SERIAL-NO          : P00M0000000A
System MAC-ADDRESS: 00:07:70:74:ff:01


        --- Display the system version ---
        ----------------------------------


Ubiquoss Switch Operating System Software
CS3400 Software (CS3400), Version 3.3.7
Technical Support: http://www.ubiquoss.com
Copyright (c) 2001-2011 by Ubiquoss Inc.

BOOTLDR: CS3400 Software (u-boot-cs3400-drg.kw), Version 2010.06

Switch uptime is 2 minutes
Time since Switch switched to active is 2 minutes
System restarted at 22:09:54 UTC Sat Mar 11 2011
System image file is "flash:/csr.r337"

If you require further assistance please contact us by sending email to
spot.team@ubiquoss.com.

Ubiquoss ARM926EJ-S rev 1 (v5l) processor with 512M bytes of memory.
Processor board ID B01MXXXXXXXX
ARM CPU at 796Mhz, Rev 1, 32KB L2 Cache
Last reset from s/w reset
261120K bytes of Flash internal SIMM (Sector size 256K).



        --- Show current system's time ---
        ----------------------------------

22:09:54 UTC Sat Mar 11 2011


        --- Display elapsed time since boot ---
        ---------------------------------------

0 days, 5 hours, 11 mins, 39 secs since boot
```

```
        --- CPU information ---
        ----------------------
...
```

16.3. Command history 기능

운용자에 의해 수행된 명령어를 명령어를 실행한 시간순서 또는 실행한 시간의 역순으로 출력하는 기능이다. 이 기능을 사용하여 운용자가 실행한 명령의 조회가 가능하며 시스템 오동작시 원인 규명 및 복원이 편리하게 된다.

표 1. command history 조회 및 설정 명령어

명령어	설명	모드
show history	■ 실행된 명령어들을 조회한다.	Privileged
show history back	■ 실행된 명령어들을 시간의 역순으로 조회한다.	Privileged
show history detail	■ 명령을 실행한 시간/user/접속 IP 를 추가적으로 표시한다.	Privileged

같은 명령어를 반복하여 입력하는 경우는 한번만 저장된다.

16.4. Output Modifiers

16.4.1. Output Modifiers 개요

장비의 현재 상태 또는 설정을 보는 명령어는 대부분 show 로 시작한다. show 명령은 대부분 한 화면에 보기 편하게 정리해서 보여주는 것이 일반적이나, 그 내용이 방대한 경우도 상당히 많다.

예를 들면, show mac-address-table 명령의 경우 수천 라인의 정보가 보여 질 수 있으며, show interface 명령의 경우에도 상당히 많은 분량의 내용이 출력된다. 출력되는 내용이 많을 경우, 이 내용 중에서 원하는 부분을 찾는 것은 쉽지 않다. 이럴 때 본 장비에서 지원하는 output modifiers 기능을 사용하면 편리하다.

일반적으로 유닉스에서 pipe 라고 부르는 기능과 비슷하며, 본 장비에서는 3 가지의 미리 정의된

output modifiers 를 지원한다. Output modifiers 기능을 사용하기 위해서는 show 명령 이후 bar (|) 를 이어 붙이고, 다음의 명령어를 사용하면 된다.

명령어	설명
| include WORD	■ 특정 단어를 포함하는 문자열을 출력한다.
| exclude WORD	■ 특정 단어를 포함하지 않는 문자열을 출력한다.
| begin WORD	■ 특정 단어를 포함하는 문자열부터 그 이후에 나오는 모든 라인을 출력한다.

16.4.2. Output Modifiers 예제

show mac-address-table 명령은 상당한 양의 결과를 출력하는데, 그 중 원하는 부분이 포함된 mac 주소만 출력하고자 할 때는 **include** 를 사용한다.

```
Switch#
Switch# show run | inc service
service password-encryption
service dhcp
```

show ip interface 명령은 상당한 양의 결과를 출력하는데, 그 중 특정 vlan 인터페이스 이후의결과 만을 원할 때는 begin 을 사용한다.

```
Switch#show ip interface | begin Vlan1

...skipping
Vlan1 is up, line protocol is up
  Internet protocol processing disabled
  IP Flow switching is disabled
Vlan33 is administratively down, line protocol is down
  Internet address is 20.1.3.2/24
  Broadcast address is 20.1.3.255
  MTU is 1500 bytes
  Ingress service-policy is not set.
  Egress service-policy is not set.
  IP Flow switching is disabled
Vlan200 is down, line protocol is down
  Internet address is 200.1.1.236/24
  Broadcast address is 200.1.1.255
  MTU is 1500 bytes
  Ingress service-policy is not set.
  Egress service-policy is not set.
  IP Flow switching is disabled
```

16.5. DDM (Digital Diagnostic Monitoring)

CS3400 은 DDM 을 지원하는 GBIC 의 상태를 상세하게 사용자에게 보여주는 명령어를 지원한다. Monitoring 항목은 다음과 같다.

항목	설명
온도	GBIC Port 온도
전압	GBIC Port 전압
전류	GBIC Port 전류
RxPower	GBIC Port 광 입력 세기
TxPower	GBIC Port 광 출력 세기

16.5.1. GBIC DDM Monitoring

DDM 을 지원하는 gbic 에 한해 다음 명령어를 사용하여 gbic 의 현재 상태를 확인할 수 있다.

명령어	Mode	설명
show interface transceiver	Privileged	DDM 을 지원하는 gbic 의 상태를 확인한다.

```
Switch# show interface transceiver
  If device is externally calibrated, only calibrated values are printed.
  ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
  NA or N/A: not applicable, Tx: transmit, Rx: receive.
  mA: milliamperes, dBm: decibels (milliwatts).

                                          Optical   Optical
           Temperature  Voltage  Current   Tx Power  Rx Power
  Port     (Celsius)    (Volts)  (mA)      (dBm)     (dBm)
  -------  -----------  -------  --------  --------  --------
  Gi2/1      49.2       3.31       0.0 --  -40.0 --   -7.2
  Gi2/2      48.8       3.30       0.0 --  -40.0 --   -6.3
  Gi3/1      50.2       3.32       0.0 --  -40.0 --  -40.0 --
.....................................................................
```

17

환경설정 저장 및 소프트웨어 업그레이드

본 장에서는 시스템의 Flash File System 의 관리 방안 및 USB, Compact Flash(CF) File System 의 사용에 대해서 설명한다. CS3400 series 에서 제공하는 File System 은 시스템 OS Image 와 Configuration 파일을 저장하는 장소로 주로 사용되며, 부팅 시 여기에 저장된 OS Image 와 Configuration 파일을 시스템이 Loading 하게 된다. 이 장에서는 기본적인 File System 운용에 필요한 명령어와 OS Image 와 Configuration File Management 에 필요한 명령어 및 부팅 모드 설정에 필요한 명령어 등을 중심으로 설명한다.
(주. 본 매뉴얼에서 설명된 기능은 당사의 사정에 의해 변경될 수 있다)

17.1. 파일 시스템

CS3400 Series 스위치는 OS image 파일 저장 및 환경 설정의 저장을 위해 기본적으로 Flash 파일 시스템을 구축한다. 이 장에서 본 제품의 파일 시스템에 대해 설명한다.

Flash 파일 시스템은 OS image 파일과 장비의 설정을 파일로 저장하기 위해 사용한다. 각 파일은 Flash 메모리의 영역에서 기록되고, 저장할 때 또는 **rename** 명령어로 저장이름을 설정할 수 있다. 또한 사용자의 요구사항에 따라 이미 Flash File System 에 저장된 파일을 **erase** 명령어로 지울 수 있다. 단 지우거나 변경할 파일이 다음 부팅 때 사용될 OS image 또는 설정 파일인지 주의해야 한다.

시스템 파일 관리를 위한 기본 명령어는 다음과 같다.

표 17-1. 파일 관리를 위한 명령어

명령어	설명	모드
show flash:	Flash 파일의 상태를 보여준다.	Privileged
dir flash:	해당 파일 시스템의 상태를 보여준다	Privileged
erase flash:	Flash 메모리에 저장된 파일을 삭제한다.	Privileged

rename flash: *filename* flash: *change*	파일의 이름 및 파일 시스템의 위치를 변경한다.	Privileged

다음은 CS3400 Series 스위치에서 File System 의 정보를 보는 예시이다. 파일 이름과 파일 사이즈, 그리고 현재(B) 및 다음 부팅 모드(*)에 대한 정보와 함께 그 파일의 종류를 표시한다.

```
Switch# show flash:


-length- -----------type/info------------ CN path
2216     text file                        B* cot.cfg
33344665 [CS3400]3.3.7                    -- csr.r337
33238012 [CS3400]3.3.8                    B* csr.r338
…

194148 Kbytes available (66972 Kbytes used, 26% used)
```

다음은 Flash 파일 시스템에 있는 파일을 지우는 예제이다.

```
Switch#show flash:


-length- -----------type/info------------ CN path
2216     text file                        B* cot.cfg
33344665 [CS3400]3.3.7                    -- csr.r337
33238012 [CS3400]3.3.8                    B* csr.r338
…
194148 Kbytes available (66972 Kbytes used, 26% used)

Switch#erase flash: csr.r337
Switch#show flash:


-length- -----------type/info------------ CN path
2216     text file                        B* cot.cfg
33344665 [CS3400]3.3.7                    -- csr.r337
33238012 [CS3400]3.3.8                    B* csr.r338
…
227492 Kbytes available (66972 Kbytes used, 26% used)
Switch#
```

17.2. Image/Configuration/BSP Down/Up Load

CS3400 Series 스위치는 운영하면서 필요한 OS Image, Configuration 파일 및 Bootloader 에 대해서 FTP 또는 TFTP 를 이용해서 다운로드 또는 업로드 할 수 있다. 이는 새로운 파일을 Flash 파일에 저장하거나, 적용으로 사용될 수도 있고, 운용상 필요한 Backup 을 FTP/TFTP 서버에 할 수 있다. 또한 새로운 BSP 파일을 다운로드 하여 적용할 수 있다. 이 장에서는 어떻게 FTP/TFTP 를 통해서 파일을 다운로드 또는 업로드 하는지 설명한다. 아래에서 기술한 running-config 및 startup-config 에 대한 설명은 <14.3 Configuration 파일 관리>를 참조하라.

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 다운로드 되는 configuration 으로 완전히 바뀌지는 않는다.

17.2.1. FTP 를 통한 Down/Up Load

아래는 FTP 를 이용한 파일 다운로드 또는 업로드 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 17-2. FTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy ftp: flash:	FTP 서버에 있는 OS Image 파일을 Flash 에 저장한다.	Privileged
copy flash: ftp	Flash 에 있는 OS Image 파일을 FTP 서버에 저장한다.	Privileged
copy ftp: config-file	FTP 서버에 있는 Configuration 파일을 Flash 에 저장한다.	Privileged
copy ftp: running-config	FTP 서버에 있는 Configuration 파일을 현재의 running-config 로 적용시킨다.	Privileged
copy running-config flash: *filename*	Running-config 를 해당 파일 시스템에 filename 으로 저장한다	Privileged
copy running-config ftp:	시스템에서 운용중인 현재 running-config 를 FTP 서버에 저장한다.	Privileged

copy ftp: bootloader	FTP 서버에 있는 BSP 파일을 Flash 에 저장한다.	Privileged

아래는 FTP 를 이용한 파일 다운 방법에 대한 예를 보여준다.

```
Switch# copy ftp: flash
IP address of remote host ? 10.1.13.4
User ID ? evolution
Password ?
Source file name ? 0621
Destination file name ? 0621
Warning: There is a file already existing with this name
Do you want to over-write [yes/no]? y
Over-writing 0621 file to flash memory
 (생략)
```

```
Switch# copy ftp bootloader
IP address of remote host ? 192.168.0.1
User ID ? lns
Password ?
Source file name ? u-boot_csr1.0.6.kwb_os
Bootloader key (0xaabb) ? 0x3400106
FTP:: 10.1.13.4//E7xg.bsp --> bootloader
Continue [yes/no]? yes
(생략)
```

Warning Bootloader 적용 시의 key 값은 보완을 위해 사전에 협의 후 배포한다.

17.2.2. TFTP 를 통한 Down/Up Load

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

표 17-3. TFTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy tftp: (usbflash:|disk1:| flash:) (<0-9>|)	TFTP 서버에 있는 OS Image 파일을 Flash, USB, CF 에 저장한다.	Privileged
copy (usbflash:|disk1:| flash:) (<0-9>|) tftp:	Flash 에 있는 OS Image 파일을 TFTP 서버에 저장한다.	Privileged
copy tftp: config-file	TFTP 서버에 있는 Configuration 파일을 Flash 에 저장한다.	Privileged
copy tftp: running-config	TFTP 서버에 있는 Configuration 파일을 현재의	Privileged

	running-config 로 적용시킨다.	
copy running-config tftp:	시스템에서 운용중인 현재 running-config 를 TFTP 서버에 저장한다.	Privileged
copy tftp: bootloader	TFTP 서버에 있는 BSP 파일을 Flash 에 저장한다.	Privileged

아래는 TFTP 서버에서 파일을 다운로드 하는 방법에 대한 예를 보여준다.

```
shu#copy tftp: usbflash:
IP address of remote host ? 10.1.13.4
Source file name ? csr.r330
Destination file name ? csr.r330

TFTP::10.1.13.4// csr.r330 --> usbflash: 0 [csr.r330]
Proceed [yes/no]? y
```

```
Switch# copy tftp bootloader
IP address of remote host ? 10.1.13.4
Source file name ? E7x.bsp
Bootloader key (0xaabb) ? 0x860011

TFTP:: 10.1.13.4// E7x.bsp --> bootloader
Proceed [yes/no]? yes
(생략)
```

17.3. Configuration 파일 관리

환경 설정은 시스템 운영자가 CS3400 Series 스위치를 운영하면서 설정된 다양한 파라미터의 집합이다. CS3400 Series 스위치에서 사용하는 Configuration 에는 startup-config 와 running-config 가 있다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration 을 startup-config 라고 하며, DRAM 내에서 구동하는 환경설정 값을 running-config 라고 한다. 여기서는 Configuration File Management 에 필요한 저장, 삭제 및 다운로드 방법을 설명한다.

표 17-4. Configuration Management 명령어

명령어	설명	모드
show startup-config	Flashs, USB, CF 메모리 중 Booting configuration 으로 설정된 파일의 정보를 보여준다.	Privileged
show running-config	현재의 환경 설정 정보를 보여준다.	Privileged
copy running-config startup-config	현재 시스템에서 운용중인 Running configuration 파일을 startup 파일로 저장한다.	Privileged
erase startup-config	현재 설정된 startup configuration 파일을 지운다.	Privileged

17.3.1. Configuration 파일 저장

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

```
Switch# show running-config
!
interface Giga1/1
 no switchport
 ip address 192.168.51.1/24
     ... <생략> ....
SWITCH#
SWITCH# copy running-config startup-config
Overwrite 'system.cfg'? [yes/no] y
SWITCH# show startup-config
!
interface Giga1/1
 no switchport
 ip address 192.168.51.1/24
```

```
     ... <생략> ....
SWITCH#
```

17.3.2. Configuration 파일 삭제

CS3400 Series 스위치는 시스템 재시동 시 Flash 메모리에 저장되어 있는 startup-config 를 재 로딩한다. 만약 현재 저장되어 있는 configuration 파일을 삭제하고 다른 파일로 시스템을 사용하고자 한다면 다음 예에서 보여주는 것처럼 startup-config 를 지우고 다른 파일로 설정 후 재 부팅하면 된다.

```
SWITCH# erase flash: System1.cfg
Warning: System1.cfg is booting config file
Do you want to erase it [yes/no]? y
SWITCH# boot config System2.cfg
SWITCH# reload
```

17.4. Boot Mode 설정 및 시스템 재시동

CS3400 Series 스위치는 운영하면서 필요한 OS Image 와 configuration 파일에 대해서 다음 부팅 파일로 설정할 수 있다. 이렇게 설정된 OS Image 와 configuration 파일은 시스템의 재 시동 시 적용되므로 각별한 주의가 필요하다. 아래에서는 OS Image 와 configuration 파일에 대해서 어떻게 다음 부팅 모드로 설정하는 지와 시스템 재 시동 방법에 대해서 설명해 놓았다.

표 17-5. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
boot system flash *filename*	다음 부팅 시 적용될 OS Image 를 설정한다.	Privileged
boot system tftp *filename* A.B.C.D	다음 부팅 시 적용될 OS Image 를 tftp booting 으로 한다.	Privileged
boot config *filename*	다음 부팅 시 적용될 Configuration 파일을 설정한다.	Privileged
reload	시스템을 재 시동 시킨다.	Privileged

17.4.1. Boot Mode 설정

CS3400 Series 스위치에서 OS Image 와 configuration 파일에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요하다. **boot flash** 명령어를 실행할 때에는 CS3400 Series 스위치에서 사용할 수 있는 OS Image 파일에 대해서만 적용하도록 해야 하며, 또 **boot config** 명령어를 시행할 때에는 CS3400 Series 스위치에서 사용할 수 있는 configuration 파일에 대해서만 적용하도록 해야 된다. 그리고 현재 Flash File System 에 있는 파일에 대해서만 적용하도록 하여야 한다.

```
Switch#
Switch# boot system flash p8xg.r090
Switch#
Switch# boot config lns.cfg
Switch#
```

17.4.2. 시스템 재시동

CS3400 Series 스위치의 전원 On/Off 또는 **reload** 명령으로 시스템 재 시작이 가능하다. 또한 reload 명령의 in 또는 at 서브 명령으로 시스템 재 시작에 대한 예약도 가능하다. 만일 reload at 명령으로 시스템 재 시작을 예약한다면 show clock 명령의 현재 시간을 참조하여 설정해야 한다.

표 17-6. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
reload	시스템을 즉시 재 시작한다.	Privileged
reload {in *time*|at *time [day]* [*month*]} [*reason*]	시스템 재 시작을 예약한다. ▪ in: 설정한 시간(time)후에 시스템이 재 시작됨 ▪ at: 설정한 시각에 시스템이 재 시작됨 ▪ *time*: HH:MM 형식으로 설정 가능 ▪ *day*: 1 일부터 31 일까지 설정 가능 ▪ *month*: 1 월부터 12 월까지 설정 가능 (ex. Jan or January) ▪ *reason*: 시스템 재 시작 이유를 등록	Privileged
reload cancel	시스템 재 시작 예약을 취소한다. 시스템 재 시작의 취소 내용은 모든 터미널로 출력된다.	Privileged
show reload	시스템 재 시작 예약 내용을 출력한다.	Privileged

아래 예제는 reload at 명령으로 시스템 재 시작을 예약하는 설정하고 reload cancel 명령으로 예약을 취소하는 설정이다.

```
Switch# show clock
23:52:01 KST Thu Feb 18 2010
Switch# reload at 13:00 19 Feb For reload test

System configuration has been modified. Save? [y/n]: y
Building configuration...
[OK]
Reload scheduled for 13:00:00 KST Fri Feb 19 2010 in ( 13 hours 7 minutes )
Reload Reason: For reload test

continue to reboot ? [yes/no]: y

Switch# show reload
Reload scheduled for 13:00:00 KST Fri Feb 19 2010 in ( 13 hours 7 minutes 28
seconds ) on vty/0 (10.1.20.99)
Reload reason: For reload test
Switch#
Switch# reload cancel

***
*** --- SHUTDOWN ABORTED   ---
***

Switch# show reload
No reload is scheduled.
Switch#
```

Warning 시스템의 재 시작 전에는 반드시 현재의 configuration 을 Flash 메모리에 저장하도록 한다. Configure terminal 모드로 진입한 후 reload 명령을 실행하면 아래와 같은 설정 저장 여부를 항상 확인한다.

```
System configuration has been modified. Save? [y/n]: y
```

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