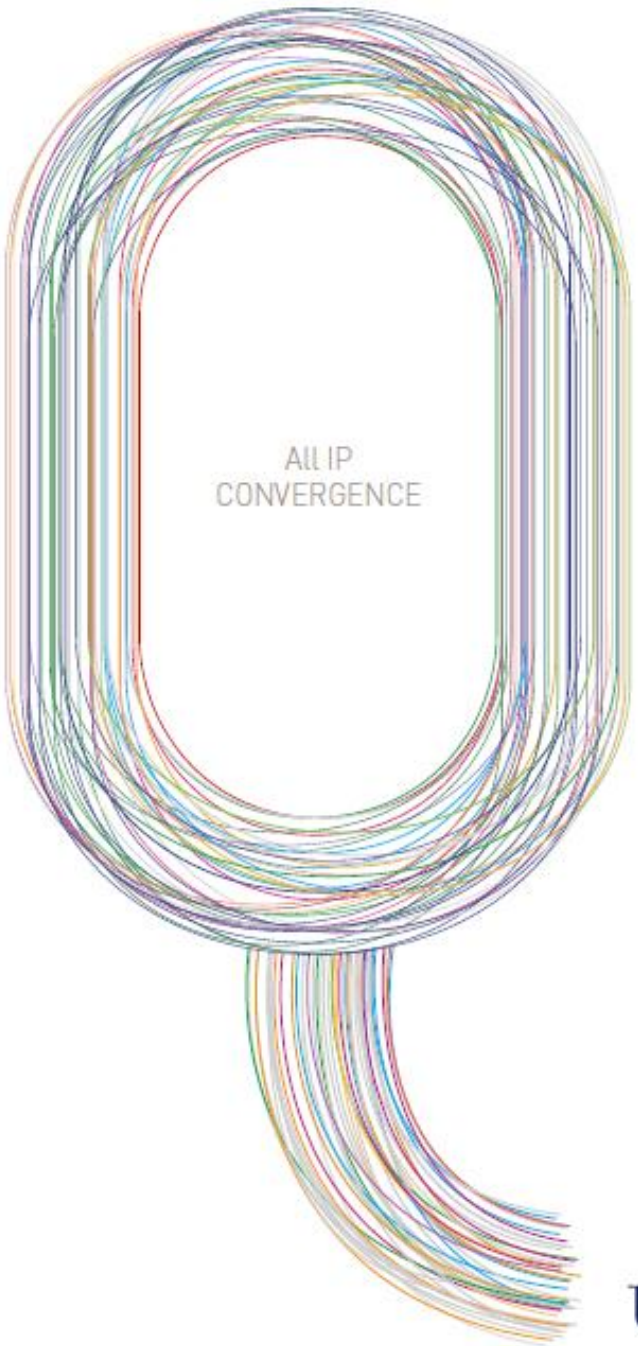
E5224 Series Switch
Common User Guide



Published: Feb 2012

ubiQuoss

목차

표 목차

그림 목차

1 서문

1.1. 개요

본 가이드는 E5224 Ethernet Layer 2 스위치를 설치한 다음 네트워크 환경을 설정하고 운영하는 데 필요한 정보 제공을 목적으로 합니다.

본 가이드는 이더넷 기반의 네트워크 운영자 및 관련 엔지니어를 대상으로 합니다. 네트워크 운영자는 본 가이드를 통하여 최적의 네트워크를 구성하고 보다 효율적으로 운영 관리할 수 있습니다. 또한 네트워크 운영 중 발생할 수 있는 문제를 해결하는 방법을 제공합니다. 본 가이드의 독자는 다음 항목들에 대한 기본적인 지식을 가지고 있다고 가정합니다.

- 근거리 통신망(Local Area Networks, LAN) 및 매트로 네트워크(Metro Area Network, MAN)
- 이더넷, 고속 이더넷, 기가비트 이더넷 개념
- 이더넷 스위칭 및 브리징 개념
- TCP/IP 프로토콜 개념
- Simple Network Management Protocol (SNMP)

Notice

E5224 Series 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하세요.

1.2. 적용 규칙

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

표 1-1. 문자 표시 규칙

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

표 1-2. 알림 및 경고 아이콘

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

1.3. 관련 문서

E5224 Series 스위치 매뉴얼은 다음과 같이 구성됩니다. 본 장비에 대한 추가 적인 정보는 다음의 매뉴얼들을 통하여 알 수 있습니다.

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

E5224 Series 스위치를 포함한 ㈜유비쿼스의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(http://www.ubiquoss.com)를 통하여 다운로드 받거나 서비스를 요청할 수 있습니다.

본 문서는 E5224 Series 에 대한 통합 매뉴얼입니다.

2

E5224 Series 스위치 시작하기

본 장은 시스템 운영자가 E5224 Series Ethernet Layer 2 스위치의 운용 환경을 처음 설정할 때 필요한 정보를 제공합니다. 스위치 시작의 개요는 다음과 같습니다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- E5224 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 설명합니다.

2.1.1. 명령어 문법의 이해

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

명령어 라인 인터페이스를 사용하려면 다음의 단계를 거칩니다.

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

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

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

Notice	명령어를 입력하고 실행했을 때 "% Command incomplete." 메시지를 출력될 때가 있습니다. 이는 명령어 실행에 필요한 파라미터가 제대로 입력되지 않았음을 의미하며, 이 경우 입력한 명령은 실행되지 않습니다. 이 때 위쪽 화살표를 누르면 마지막에 입력한 명령이 표시됩니다.

다음은 명령어 파라미터를 제대로 입력하지 않은 경우에 대한 예제입니다.

```
Switch# show ↵
% Incomplete command.
Switch #
```

2.1.2. 명령어 문법 도움말(Command Syntax Helper)

E5224 Series 스위치의 CLI 는 명령어 문법 도움말 기능을 자체적으로 내장하고 있습니다. 시스템 운영자는 명령어 입력 중 완전한 문법을 모르는 경우, 어느 위치에서든지 '?' 를 입력해서 도움말을 제공받을 수 있습니다. E5224 Series 스위치는 다음과 같은 두 가지 도움말 기능을 제공합니다.

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

다음의 예제는 전체 도움말 기능을 show 명령으로 실행해본 결과입니다.
show 명령어 다음에 공백 문자와 함께 '?'를 입력하면 운영자가 입력 할 수 있는 파라미터 및 값의 목록이 출력됩니다. 그리고 "Switch# show" 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 기다립니다. 운영자 입력에서 '?'는 화면에 표시되지 않습니다.

```
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_
```

다음은 부분 도움말 기능에 대한 예제입니다. show 명령어 입력 후 공백 없이 '?'를 입력하면 다음과 같이 show 명령어에 대한 설명이 표시되고 커서가 깜박이면서 다음 명령 입력을 기다립니다.

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

위의 예제에서 운영자는 포트의 상태를 알고 싶지만 정확한 명령을 모른다고 가정합시다. 그러면 'p'를 치고 공백 없이 '?'를 치면 'p'로 시작하는 서브 명령어의 목록이 다음과 같이 출력됩니다. 물론 운영자가 입력한 명령은 다시 표시가 되고 커서가 깜박이면서 입력을 기다립니다.

```
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

E5224 Series 스위치의 CLI 는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행기능을 지원합니다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령을 수행합니다.

Notice

단축 명령을 사용할 때, 시스템 운영자는 E5224 Series 스위치가 명령어를 구분하여 인식할 수 있도록 충분하게 입력해야 합니다. "% Ambiguous command"라는 메시지가 출력될 때가 있습니다. 이것은 해당 모드에 입력한 문자와 prefix 가 같은 하나 이상의 명령어가 존재함을 의미합니다.

```
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 사용됩니다. 명령어 심벌은 명령어 수행을 위해서 파라미터들이 어떻게 입력되어야 하는 지를 설명합니다. <표 2-1> 시스템 명령어 문법에 적용된 심볼 및 각각의 심벌의 의미를 설명합니다.

표 2-1. 명령어 구문 심볼

심볼	이름	설명
<>:	Angle brackets	명령어 문법에서 하나의 변수 또는 값을 의미합니다. 이렇게 표현된 파라미터는 반드시 입력을 해야 합니다. 예를 들어, 다음과 같은 명령어가 있을 때 `access-list <1-99> (deny|permit) address` 표준 IP access control list 번호는 반드시 <1-99> 사이의 값을 입력해야 합니다.
{ }:	Braces	명령어 문법에서 사용되는 파라미터 또는 값의 리스트 시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 합니다. 예를 들어, 다음과 같은 명령어가 있을 때 `router {rip|ospf}` 시스템 운영자는 라우팅 프로토콜로서 RIP 와 OSPF 중의 하나를 반드시 명시해야 합니다.
[ ]:	Square brackets	명령어 문법에서 사용되는 파라미터 또는 값의 리스트 시스템 운영자는 리스트에 포함된 항목 중에서 필요한 항목을 선택적으로 입력합니다. 경우에 따라서는 하나도 입력을 하지 않을 수도 있습니다. 예를 들어, 다음과 같은 명령어가 있을 때 `show interface [ifname]` 인터페이스의 이름을 명시하지 않아도 됩니다.
|:	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

E5224 Series 스위치는 Emacs 와 유사한 편집 기능을 제공합니다. <표 2-2>는 운영 단말이 제공하는 명령어 라인 편집 명령 및 도움말 기능을 설명합니다.

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 입력하고 [tab]을 입력하면 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

E5224 Series 스위치는 <표 2-3>과 같이 다양한 스위치 명령어 모드를 지원합니다. 각 스위치 명령어 모드마다 운영자에게 주어지는 권한에는 차이가 있습니다.

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 글로벌하게 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 E5224 Series 스위치의 이름을 호스트 이름으로 사용합니다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용합니다.

시스템 운영자는 E5224 Series 스위치의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게 됩니다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 있는 지를 알려줍니다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 체크 해야 합니다. <표 2-4>은 스위치의 명령어 모드 사이의 이동 방법을 설명합니다.

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. E5224 Series 스위치가동

E5224 Series 스위치는 처음 가동될 때, 플래시 메모리에 저장된 OS 이미지를 메모리에 로드 하여 시스템을 시작합니다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩합니다.

Notice	E5224 Series 스위치는 플래시 메모리 용량의 한도 내에서 여러 개의 OS 이미지를 관리할 수 있습니다. 플래시 메모리에 다수의 OS 이미지가 존재할 경우 운영자는 사용할 OS 를 선택할 수 있습니다.

2.4. 사용자 인터페이스

시스템 운영자는 스위치 환경의 설정 및 검증, 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속할 수 있습니다. 스위치에 접속하기 위한 가장 기본적인 방법은 E5224 Series 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 방법입니다(*Out-of-band management*).
스위치로 연결하는 또 다른 방법은 원격지에서 텔넷 프로그램을 이용하는 방법입니다. 원격지에서 텔넷 연결을 위한 별도의 포트를 제공하지는 않고 서비스 포트를 통하여 접속할 수 있습니다(*In-band management*).

운영자는 다음의 방법을 사용하여 E5224 Series 스위치를 관리할 수 있습니다.

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

E5224 Series 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원합니다.

- 1 개의 콘솔 연결 가능
- 최대 8 개의 텔넷 연결 가능

Notice	단, 한정된 시스템 자원에 의해 텔넷 연결이 최대 8 개에 도달하기 전에 제한 될 수 있습니다.

2.4.1. 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능합니다. 이를 위하여 운영 단말(또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9 핀, RS-232 DB9 포트를 지원해야 합니다. 콘솔 포트는 E5224 Series 스위치의 전면에 위치합니다.

>과 같이 E5224 Series 스위치가 제공하는 콘솔 포트에 운영 단말을 연결합니다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행합니다.

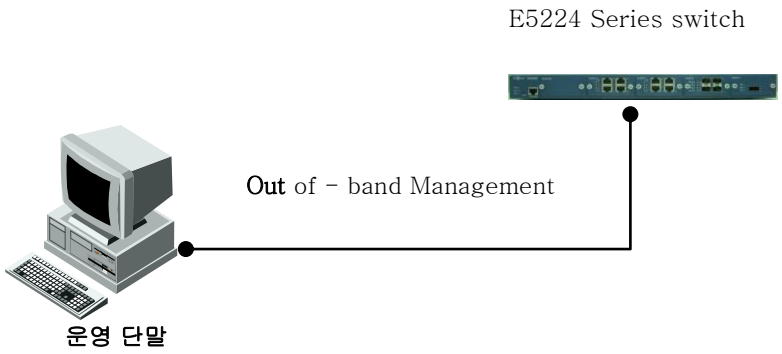


그림 2-1. E5224 Series 스위치와 운영 단말 연결

Notice	운용 단말의 설정 방법 및 콘솔 포트 핀 설정은 E5224 Series 스위치 하드웨어 설치 가이드를 참조하세요.

2.4.2. 텔넷 연결

시스템 운영자는 TCP/IP 및 텔넷 접속 기능이 있는 워크스테이션을 통하여 E5224 Series 스위치에 접속할 수 있습니다. 운영자는 텔넷 접속에 필요한 ID 및 패스워드를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 합니다.

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

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

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

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

네트워크 관리자는 SNMP(Simple Network Management Protocol)를 이용하여 E5224 Series 스위치의 인터페이스, 환경, 설정 정보 등을 관리할 수 있습니다. SNMP 에 대한 자세한 정보는 <2.9. SNMP(Simple Network Management Protocol)>절을 참조하세요.

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 있습니다.
사용자의 privilege level 은 사용자의 권한을 나타내며 privilege level 에 따라 시스템에서 실행할 수 있는 명령을 제한할 수 있습니다. 사용자를 추가할 때 privilege level 을 설정할 수 있으며 기본 값은 1 로 설정됩니다. Privilege level 이 1 이상인 사용자는 user 모드 명령을 실행할 수 있으며, user 모드에서 “enable” 명령을 수행하면 privileged 모드로 진입할 수 있습니다. Privileged 모드로 진입한 사용자의 privilege level 은 15 로 변경됩니다. 시스템 운영자는 “enable” 명령을 수행할 때 패스워드를 입력하도록 설정하여 privileged 모드로 진입할 수 있는 사용자를 제한할 수 있습니다.

다음은 각 privilege level 에 대한 설명입니다.

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

표 2-5. 사용자 등록, 삭제, 관리 명령어

명령어	설명	모드
`username name {nopassword| password [0|7] password| secret [0|5] password}`	사용자를 등록합니다. **nopassword**: 로그인 시 패스워드입력이 요구되지 않습니다. **password or secret**: 로그인 시 패스워드입력이 요구되며 password 와 secret 은 암호화 방식에 따라 구분됩니다. 0 – 암호화 하지 않음. 5 – MD5 암호화 7 – DES 암호화	Config
`no username name`	등록된 사용자를 삭제합니다. 사용자가 root 인 경우 패스워드는 초기화 값으로 변경됩니다.	Config

username *name* privilege <0-15>	사용자의 privilege level 을 변경합니다.	Config
username *name* access-class *<1-99>*	사용자에 대해 access-list 를 적용합니다. <1-99> : IP standard access list	Config
no username *name* access-class	사용자에 적용된 access-list 를 해제합니다.	Config
username *name* user-maxlinks *value*	해당 사용자로 접속 가능한 최대 session 수를 설정합니다.	Config
no username *name* user-maxlinks *value*	해당 사용자로 접속 가능한 최대 session 수를 초기화 값으로 변경합니다. Default: 32 개	Config
username *name* unlimited-session-ip *A.B.C.D*	Session 접속 수를 제한 받지 않는 사용자 및 IP 주소를 설정합니다.	Config
no username *name* unlimited-session-ip	Session 접속 수를 제한 받지 않는 사용자 설정을 해제합니다.	Config

2.5.1.1. 사용자 추가

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

```
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#
```

다음은 privilege level 이 15 인 **'testuser3'**가 로그인하여 privileged 모드로 진입하는 예제입니다.

```
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 진입합니다.

2.5.2. 패스워드 설정

E5224 Series 스위치는 시스템 보안을 위해 사용자 및 enable 패스워드를 설정할 수 있습니다. 사용자 패스워드 설정은 <2.10 ACL(Access Control List)>를 참고하세요.

- 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 설정합니다. **password or secret**: Privileged 모드진입 시 패스워드 입력이 요구되며 password 와 secret 은 암호화 방식에 따라 구분됩니다. 0 – 암호화 하지 않음. 5 – MD5 암호화 7 – DES 암호화	Config
`no enable password`	Privileged 모드로 진입하기 위한 패스워드 설정을 해제합니다.	Config

2.5.2.1. Enable password 설정

Privileged 모드로 진입할 때 패스워드를 입력하도록 설정합니다.

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

다음과 같이 설정한 패스워드를 입력하면 privileged 모드로 진입할 수 있습니다.

```
Ubiquoss L3 Switch

Switch login: root
Password:

Hello.

Switch>enable
Password: testpw
Switch#
```

E5224 Series 스위치는 암호화하지 않은 패스워드를 설정한 경우 show running-config 명령으로 설정한 패스워드를 볼 수 있는 문제를 방지하기 위해서 패스워드 암호화 모드를 지원합니다. 패스워드 암호화 모드는 service password-encryption 명령으로 설정할 수 있습니다.

표 2-7. 패스워드 암호화 모드 설정 명령

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

Notice

"**no service password-encryption**" 명령은 보안을 위해 기존에 암호화된 패스워드를 암호화 되기 전의 문자열로 되돌리지는 않습니다. 암호화 모드를 해제한 이후에 설정되는 패스워드만 암호화 하지 않도록 설정합니다.

2.5.2.2. 패스워드 암호화 모드 설정

패스워드 암호화 모드를 설정하면 기존에 추가되었던 패스워드가 암호화되어 출력됩니다.

```
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#
```

2.5.3. 패스워드 복원

E5224 Series 스위치는 사용자 및 enable 패스워드를 초기 상태로 되돌리는 패스워드 복원 기능을

제공합니다. 단, 사용자 패스워드 복원은 root 사용자로 제한됩니다. 사용자 및 enable 패스워드 설정은 <2.5.2 패스워드 설정>을 참고하십시오.
패스워드 복원 기능을 활성화하기 위해서 시스템 부팅 후 < Ctrl + C > 키를 눌러서 부트로더에 진입해야 합니다. 부트로더 진입 후 아래 명령으로 패스워드 복원과 관련된 ***"epasswd"*** 환경 변수를 설정 또는 해제할 수 있습니다.

표 2-8. 부트로더 환경 변수 설정 명령

.명령어	설명	모드
setenv	환경 변수를 설정한다.	Bootloader
saveenv	환경 변수를 저장한다.	Bootloader
printenv	환경 변수를 출력한다.	Bootloader

아래 예제는 패스워드 복원 기능을 설정하는 내용입니다. 시스템 부팅 후에 < Ctrl + C > 키를 눌러서 부트로더에 진입하며, 부트로더 프롬프트가 출력되면 *"epasswd"* 환경 변수를 yes 로 설정해야 합니다. 패스워드 복원 기능 설정 후 부팅을 계속하려면 부트로더 프롬프트에서 reset 명령을 실행하며, 시스템 부팅 완료 후에 사용자 및 enable 패스워드 설정이 초기화되었는지 확인합니다.

```
/* 생략 */
   Bus 0: ......not available
   Bus 1: ......not available

Image Booting From Flash
 Hit Ctrl_C to stop autoboot:  0
=> <INTERRUPT>
=>
=> setenv epasswd yes
=> saveenv
=> printenv
bootdelay=1
baudrate=9600
/* 생략 */
epasswd=yes
=> reset
```

위와 같이 패스워드가 초기화 된 상태를 유지하기 위해서는 startup configuration 에 변경된 내용을 반드시 저장해주어야 합니다.

```
Switch#copy running-config startup-config
Overwrite 'flash: 0 test.cfg'? [y/n]y
Building configuration...
[OK]
Switch#
```

패스워드 복원 기능은 명시적으로 해제하지 않으면 시스템이 부팅될 때마다 사용자 및 enable 패스워드를 계속 초기화하게 됩니다. 패스워드 복원 기능 해제를 위해서 부트로더에서 *"epasswd"* 환경 변수

를 아래와 같이 삭제할 수 있습니다.

```
=> setenv epasswd
=> saveenv
```

Notice

환경 변수 *"epasswd"*를 해지하지 않으면 시스템 부팅 시 패스워드가 계속 초기화될 수 있으니 명시적으로 해제해야 합니다.

2.6. AAA (Authentication, Authorization, Accounting)

2.6.1. 인증 (Authentication)

시스템 보안을 위해 시스템에 접속하는 사용자에 대한 인증이 필요합니다. E5224 Series 스위치는 로그 인을 시도하는 사용자에 대한 인증과 privileged 모드로 진입할 때 enable 패스워드에 대한 인증을 수행합니다.
다음은 E5224 Series 스위치에서 제공하는 인증 방법으로 Local 시스템의 사용자 정보를 통한 인증과 인증 프로토콜인 RADIUS 및 TACACS+를 통한 인증 방법을 제공합니다.

- Local
- RADIUS
- TACACS+

위와 같은 인증 방법은 한 가지 이상 설정될 수 있으며 여러 인증 방법을 설정했을 경우 설정한 순서대로 인증을 시도하게 됩니다. 사용자는 인증에 대한 성공 또는 실패에 대한 결과를 얻지 못하는 경우에 다른 인증 방법으로 인증을 시도할 수 있도록 여러 인증 방법을 설정해야 합니다. 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 시도합니다. 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 됩니다.
Local 인증은 항상 활성화된 상태이며 인증 설정을 명시하지 않은 경우 기본적으로 Local 인증 방법으로 사용자 인증을 수행합니다.

2.6.2. 사용자 인증

시스템에 접속하기 위해 로그 인하는 사용자에 대해 사용자 이름과 패스워드로 인증을 시도합니다. Local 시스템의 사용자 정보 또는 RADIUS 및 TACACS+ 서버를 통한 인증이 가능하며 local 시스템을 통해 인증하기 위해서는 먼저 사용자를 등록해야 합니다. Local 시스템의 사용자 등록은 <2.5.1 사용자 등록 및 삭제 설정>를 참조하세요.

표 2-9. 사용자 인증 설정 명령어

명령어	설명	모드
`aaa authentication login default {local|radius|tacacs+}`	로그인 시 입력된 사용자 이름 및 패스워드에 대해 인증합니다.	Config
`no aaa authentication login default`	로그인할 때의 사용자 인증 방법을 초기 값으로 변경합니다. Default: Local	Config
`aaa authentication login template-user` *`name`*	RADIUS 또는 TACACS+ 서버로 인증하는 경우 dummy 사용자를 지정할 수 있습니다. Dummy 사용자는 local 시스템에 등록되어 있어야 합니다.	Config
`no aaa authentication login template-user`	Dummy 사용자 지정을 해제합니다.	Config
`aaa authentication login authen-type (chap|pap)`	TACACS+ 서버로 인증하는 경우 인증메시지를 chap 또는 pap 방식으로 전송합니다. Default: Ascii	Config
`no aaa authentication login authen-type`	TACACS+ 서버로 인증하는 경우 인증메시지를 ascii 방식으로 전송합니다.	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 시도합니다. 마찬가지로 RADIUS 서버에서 응답을 받지 못한 경우 디폴트로 제공하는 local 방식을 통해 인증을 시도합니다.

```
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 있습니다. Local 로 인증하는 경우 시스템에 설정한 enable 패스워드를 통해 인증을 수행하며, RADIUS 또는 TACACS+ 서버를 통해 인증을 수행할 수도 있습니다. Local 로 인증할 때 local 시스템에 enable 패스워드가 설정되지 않은 경우 인증은 항상 성공하게 되므로 privileged 모드로 인증을 수행하기 위해서는 적절한 enable 패스워드를 설정해야 합니다. Local 시스템의 enable 패스워드 설정은 <2.5.2 패스워드 설정>을 참조하세요.

표 2-10. Privileged 모드 사용자 인증 설정 명령어

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

2.6.3.1. privileged 모드 사용자 인증 설정

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

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

2.6.4. 권한 (Authorization)

E5224 Series 스위치는 privilege level 을 통해 시스템 자원을 사용할 수 있는 권한을 검사할 수 있습니다. EXEC shell 을 실행할 때 사용자의 privilege level 과 local 시스템 또는 원격 서버(RADIUS 또는 TACACS+)에 설정한 사용자의 privilege level 을 비교합니다. 시스템 자원을 사용하고자 하는 사용자의 privilege level 이 설정한 privilege level 보다 낮은 경우 에러 메시지를 출력하며 실행에 실패하게 됩니다. 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 있습니다.
인증 서버로 접속이 되지 않거나 인증 서버로부터 결과를 수신하지 못하는 경우를 대비해서 항상 local 시스템을 통한 권한 검사 방법을 추가해야 합니다. Local 시스템 권한 검사마저 없는 경우 권한 검사는 항상 실패하게 되며, 이 경우 콘솔을 통한 설정 변경이 필요합니다. 콘솔을 통해 시스템에 로그 인한 사용자는 권한을 검사하지 않습니다.

2.6.5. EXEC 실행 권한

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

표 2-11. 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 검사합니다.	Config
`no aaa authorization exec default`	EXEC shell 을 실행할 권한을 검사하지 않습니다.	Config

2.6.5.1. EXEC shell 실행 권한을 TACACS+ 서버로 검사하도록 설정

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

```
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 다음과 같이 로그인 후 EXEC shell 을 실행시킬 수 있습니다. 이 경우 privilege level 이 15 이상이므로 privileged 모드로 바로 진입할 수 있습니다.

```
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 있습니다. 기본적으로 각 명령의 privilege level 은 명령이 실행되는 모드의 privilege level 을 가지며 설정을 통해 변경이 가능합니다. Privilege level 변경은 <2.6.4 Privilege level 설정>를 참조하세요.
E5224 Series 스위치는 TACACS+ 서버를 이용해 특정 명령의 실행 권한을 검사할 수 있습니다. <표 11>과 같이 명령이 실행되는 privilege level 을 지정하여 권한을 검사할 명령 집합을 설정할 수 있으며, 해당 privilege level 을 가지는 명령에 대해 TACACS+ 서버로부터 실행 권한을 검사할 수 있습니다.

표 2-12. 명령어 실행 권한 설정 명령어

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

2.6.6.1. 명령어 실행 권한을 TACACS+서버로 검사하도록 설정

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

```
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 발생합니다.

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

2.6.7. 계정(Accounting)

E5224 Series 스위치는 AAA 의 계정 기능을 통해 세션 접속 및 명령 실행 내역을 TACACS+ 서버를 통해 관리할 수 있습니다.

2.6.8. 세션 접속 관리

시스템에 접속한 내역을 TACACS+ 서버에 기록합니다.

표 2-13. 세션 접속 관리 설정 명령어

명령어	설명	모드
`aaa accounting exec default (start-stop|stop-only) tacacs+`	시스템 접속 내역을 TACACS+ 서버로 전송합니다. start-stop: 세션 시작과 끝을 모두 기록 stop-only: 세션 끝만 기록.	Config
`no aaa accounting exec default`	시스템 접속 내역을 TACACS+ 서버로 전송하지 않습니다.	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 있습니다. <표 13> 과 같이 privilege level 을 지정하여 실행 내역을 TACACS+ 서버로 전송할 명령 집합을 설정할 수 있습니다. 기본적으로 각 명령의 privilege level 은 명령이 실행되는 모드의 privilege level 을 가지며 설정을 통해 변경이 가능합니다. Privilege level 변경은 <2.6.4 Privilege level 설정>를 참조하세요.

표 2-14. 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 기록합니다. <0-15>: privilege level.	Config
`no aaa accounting commands <0-15> default`	해당 privilege level 을 갖는 명령의 실행 내역을 TACACS+ 서버에 기록하지 않습니다. <0-15>: privilege level.	Config

2.6.9.1. 명령어 실행 내역을 TACACS+ 서버로 관리하도록 설정

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

```
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

E5224 Series 스위치는 privilege level 을 통해 특정 명령에 대한 권한(Authorization) 및 계정(Accounting) 기능을 수행할 수 있습니다. 특정 명령에 대해 privilege level 을 설정하지 않는 경우 각 명령은 실행되는 모드의 privilege level 을 기본값으로 참조합니다.

표 2-15. Privilege level 설정 명령어

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

2.7. 서버 설정

E5224 Series 스위치는 RADIUS 또는 TACACS+의 원격 서버를 통한 인증, 권한, 계정 관리 기능을 제공합니다. 다음은 RADIUS 와 TACACS+ 서버를 설정하는 방법입니다.

2.7.1. RADIUS 서버 설정

표 2-16. RADIUS 서버 설정 명령어

명령어	설명	모드
`radius-server host A.B.C.D [key [0|7] key-string]`	RADIUS 서버를 설정합니다. *A.B.C.D*: RADIUS 서버의 주소 key: 서버에서 사용할 암호 키를 설정합니다. 0 – 암호화 하지 않음. 7 – DES 암호화	Config
`no radius-server host A.B.C.D`	설정된 RADIUS 서버를 삭제합니다. *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 설정합니다. *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 설정합니다. Default: 1812	Config
`radius-server key [0|7] key-string`	RADIUS 서버에 접속할 때 사용하는 공통 암호 키를 설정합니다. Key 가 명시되지 않은 서버는 공통 암호 키를 사용하게 됩니다.	Config
`no radius-server key`	공통 암호 키를 삭제합니다.	Config
`radius-server retransmit count`	RADIUS 서버로 AAA 정보를 재전송하는 횟수를 설정합다. *count*: 재전송 횟수를 설정	Config
`no radius-server retransmit`	재전송 횟수를 기본값으로 설정합니다. Default: 3 회	Config
`radius-server timeout seconds`	RADIUS 서버로부터 응답을 기다리는 시간을 설정합니다. *seconds*: Timeout 시간을 초 단위로 설정	Config
`no radius-server timeout`	응답을 기다리는 시간을 기본값으로 설정합니다. Default: 5 초	Config

`ip radius source-interface` *`ifname`*	RADIUS 서버로 전송할 정보의 source IP 주소를 설정합니다. *ifname*: 인터페이스 이름 정보	Config
`no ip radius source-interface`	설정한 source IP 주소를 해제합니다.	Config

RADIUS 서버 설정

다음 예제는 여러 RADIUS 서버와 공통 암호 키로 test123 을 설정합니다. 192.168.0.1/test123 으로 AAA 정보를 서버로 전송하며 응답을 수신하지 못하는 경우 다음 RADIUS 서버로 전송을 시도하게 됩니다.

```
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 2-17. TACACS+ 서버 설정 명령어

명령어	설명	모드
`tacacs-server host` *`A.B.C.D`* `key [0|7]` *`key-string`*	TACACS+ 서버를 설정합니다. *A.B.C.D*: TACACS+ 서버의 주소 key: 서버에서 사용할 암호 키를 설정합니다. 0 – 암호화 하지 않음. 7 – DES 암호화	Config
`no tacacs-server host` *`A.B.C.D`*	설정된 TACACS+ 서버를 삭제합니다. *A.B.C.D*: TACACS+ 서버의 주소	Config
`tacacs-server host` *`A.B.C.D`* `timeout` *`seconds`*	TACACS+ 서버로부터 응답을 기다리는 시간을 설정합니다. *seconds*: Timeout 시간을 초 단위로 설정	Config
`tacacs-server host` *`A.B.C.D`*	응답을 기다리는 시간을 기본값으로 설정합니	Config

timeout	다. Default: 5 초	
ip tacacs source-interface *ifname*	TACACS+ 서버로 전송할 정보의 source IP 주소를 설정합니다. *ifname*: 인터페이스 이름 정보	Config
no ip tacacs source-interface	설정한 source IP 주소를 해제합니다.	Config

TACACS+ 서버 설정

다음 예제는 여러 TACACS+ 서버를 설정합니다. 192.168.0.1/lns 로 AAA 정보를 서버로 전송하며 응답을 수신하지 못하는 경우 다음 TACACS+ 서버로 전송을 시도하게 됩니다.

```
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 있습니다. 콘솔 또는 텔넷 화면의 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있으며 E5224 Series 스위치는 기본값으로 Switch 를 hostname 으로 사용합니다.

표 2-18. Hostname 설정 명령어

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

다음은 hostname 을 설정하는 절차입니다.

```
Switch# configure terminal
Switch(config)# hostname E52
E52(config)# end
E52#
E52# configure terminal
E52(config)# no hostname
```

```
Switch(config)# end
Switch#
```

2.9. SNMP (Simple Network Management Protocol)

SNMP(Simple Network Management Protocol)를 사용하면 네트워크 관리자는 SNMP 에이전트가 설치된 장비를 MIB(Management Information Base)을 통해 관리할 수 있습니다. E5224 Series 스위치는 SNMPv1, SNMPv2 그리고 SNMPv3 기능을 지원합니다.

2.9.1. SNMP 환경 설정

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

표 2-19. SNMP 환경 설정 명령

명령어	설명	모드
snmp-server contact *string*	시스템 운영자 정보를 입력합니다.	Config
no snmp-server contact	시스템 운영자 정보를 삭제합니다.	Config
snmp-server location *string*	장비가 설치된 위치 정보를 입력합니다.	Config
no snmp-server location	장비가 설치된 위치 정보를 삭제합니다.	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 변경할 수 있

습니다. SNMP 에이전트에 접속할 때 community 로 인증할 수 있으며 community 는 아래와 같은 두 가지 접속 타입을 가집니다.

- Read-only community
  - 시스템에 읽기 전용으로 접속합니다.
- Read-write community
  - 시스템에 읽기 및 쓰기 모드로 접속합니다.

표 2-20. SNMP Community 설정

명령어	설명	모드
`snmp-server community` *`string`* `[`*`access-type`*`| view` *`view-name`*`| <1-99>]`	SNMP community 를 설정합니다. access-type: SNMP 에이전트 접속 타입 ro: read only rw: read write view: MIB 접속 범위를 지정하며, 자세한 내용은 snmp-server view 설정을 참조하세요. <1-99>: 접속 호스트에 대해 access-list 를 적용할 수 있습니다.	Config
`no snmp-server community` *`string`*	SNMP community 를 삭제합니다.	Config

2.9.2.1. SNMP Community 설정

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

```
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 있습니다. E5224 Series 스위치는 다음과 같은 버전의 트랩을 제공하며, 트랩 호스트 및 "snmp-server enable traps" 명령으로 설정해야 트랩이 발생합니다.

- **SNMPv1 Trap**

- **SNMPv2c Trap**
  - 기본적으로 전송되는 트랩 버전입니다.

- **SNMPv3 Trap**
  - 인증 및 암호 기능을 제공하며, security model 을 설정할 수 있습니다.
    1) noAuth: 인증 및 암호화를 수행하지 않습니다.
    2) Auth: 인증 수행합니다.
    3) Priv: 인증 및 암호화를 수행합니다.

표 2-21. SNMP Trap 호스트 설정

명령어	설명	모드
`snmp-server host A.B.C.D [version 1|2c|3 sec-level] community-string [PORT]`	트랩을 전송할 호스트를 설정합니다. *A.B.C.D*: 트랩 호스트 주소 version: 전송할 트랩의 버전 (Default: 2c) *sec-level*: 트랩 버전이 3 인 경우 security model 을 설정 *community-string*: community 설정 *PORT* (Default:162)	Config
`no snmp-server host A.B.C.D [version 1|2c|3 sec-level] community-string`	설정한 트랩 호스트를 삭제합니다.	Config
`snmp-server trap-source ifname`	전송할 트랩의 source IP 주소를 설정합니다. *ifname*: 인터페이스 이름 정보	Config
`no snmp-server trap-source`	설정한 source IP 주소를 해제합니다.	Config

표 2-22. SNMP 기본 트랩의 Enable 설정

명령어	설명	모드
`(no) snmp-server enable traps alarm [fallingAlarm| risingAlarm]`	RMON alarm 트랩을 전송하도록 설정 또는 해제합니다.	Config

(no) snmp-server enable traps auto-negotiation	Auto negotiation 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps cfm [pm-event|remote-mep-state]	CFM 관련 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps envmon [ext-supply|fan|supply|temperature]	시스템 환경(fan, power 등) 관련 트랩을 전송하도록 설정 또는 해제합니다.	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 해제합니다.	Config
(no) snmp-server enable traps fru-ctrl	모듈, slot 등 실/탈장 가능한 unit 의 상태 변경 시 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps interface	Linkup, linkdown 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps port-monitor [crc|drop|error|input-load-monitor|output-load-monitor]	Port 모니터링 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps resource [cpu-load-monitor|memory-free-monitor]	시스템 자원 관련 트랩을 전송하도록 설정합니다.	Config
(no) snmp-server enable traps snmp [coldStart|warmStart|authFail]	Cold start, warm start, authentication failure 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps vlancreate	Vlan 생성 시 트랩을 전송하도록 설정 또는 해제합니다.	Config
(no) snmp-server enable traps vlandelete	Vlan 삭제 시 트랩을 전송하도록 설정 또는 해제합니다.	Config

Notice

<표 2-21 SNMP 기본 트랩 및 Enable 설정> 은 E5224 Series 스위치에서 기본적으로 제공하는 트랩의 전송 설정 및 해제 명령을 나타내며 추후에 추가 및 삭제될 수 있습니다.

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 설정하는 예제입니다. 트랩 버전은 기본값인 2c 로 전송됩니다.

```
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

E5224 Series 스위치는 SNMP 를 통한 시스템 관리에서 더 나은 보완 기능을 제공하기 위해 SNMPv3 기능을 제공합니다. SNMPv3 는 사용자에 대한 인증 및 데이터에 대한 암호화 기능을 제공합니다.

표 2-23. SNMPv3 설정

명령어	설명	모드
`snmp-server engineID` *`engineid-string`*	SNMP 에이전트를 유일하게 구분하기 위한 engine ID 를 설정합니다. SNMP engineID 를 변경하는 경우 기존에 설정한 user 를 다시 설정해야 합니다. User 설정은 engine ID 를 이용해 MD5 및 SHA 의 security digest 를 생성하기 때문입니다.	Config
`no snmp-server engineID`	Engine ID 를 자동으로 생성되는 기본값으로 설정합니다. 기본 값은 자사의 enterprise OID(1.3.6.1.4.1.7800)와 시스템의 첫 번째 MAC 주소로 자동 생성됩니다.	Config
`show snmp engineID`	Engine ID 를 출력합니다.	Privileged
`snmp-server group` *`groupname`* `{v1|v2c|v3` *`sec-level`*`}` `[read` *`read-view`*`|` `write` *`write-view`*`]`	SNMP group 을 설정합니다. *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 설	Config

	정됨. write: Write view 설정	
`no snmp-server group` *`groupname`* `{v1|v2c|v3` *`sec-level`*`}`	SNMP group 을 삭제합니다	Config
`show snmp group`	SNMP group 을 출력합니다.	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 설정합니다. v1, v2c, v3: User 버전 auth: SNMPv3 인 경우 사용자 인증을 수행할 수 있으며 암호화 방법으로 MD5 또는 SHA 를 설정할 수 있습니다. *auth-passwd*: 인증을 위한 암호 설정 priv: SNMP PDU 를 암호화할 수 있으며 암호화 방법으로 DES 또는 AES 를 설정할 수 있습니다. *priv-passwd*: 암호화를 위한 암호 설정 `access`: 사용자에 대해 access-list 를 적용합니다. <1-99> : IP standard access list	Config
`no snmp-server user` *`username groupname`* `{v1|v2c|v3}`	SNMP user 를 삭제합니다.	Config
`show snmp user`	SNMP user 를 출력합니다.	Privileged
`snmp-server view` *`viewname viewoid`* `{excluded|included}`	SNMP view 를 설정합니다. *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 포함하거나 제외하도록 설정	Config
`no snmp-server view` *`viewname viewoid`*	SNMP view 를 삭제합니다.	Config

2.9.4.1. SNMP engineID 변경

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

```
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 생성합니다. **'testuser'**는 **'testgroup'**에 포함되며 ifEntry(1.3.6.1.2.1.2.2.1)를 읽거나 쓸 수 없는 **'testview'**를 적용합니다.

```
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 않습니다. 위의 예제와 같이 "**show snmp user**" 명령으로 확인할 수 있습니다.

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 있습니다. 시스템 운영자는 패킷의 전송 상태에 대한 기본적인 통계 자료를 얻을 수 있고 이를 통해 보안 정책을 수립할 수 있습니다. 또한 인증되지 않은 액세스로부터 시스템을 보호할 수 있습니다. 액세스 리스트는 스위치를 통해 전달되는 패킷을 허용하거나 거부하기 위해 사용할 수도 있고 텔넷(vty)이나 SNMP 를 통한 스위치의 접속에도 적용할 수 있습니다.

액세스 리스트는 표준 IP 액세스 리스트가 있으며, <1-99>의 번호를 할당 할 수 있습니다.

표 2-24. 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 선언합니다.
- 빈번히 조건을 만족시킬만한 것을 먼저 선언합니다.
- Access-list 의 조건을 여러 줄에 선언을 하는데 임의의 줄과 줄 사이의 것을 지우거나 수정할 수 없고, 새로 추가하는 필터는 마지막에 추가됩니다.

Notice

E5224 series 의 경우 Access-list 마지막에 특별히 'deny any'가 명시 되지 않습니다. 특정 엑세스 외에 모든 traffic 을 drop 하기 위해서 'deny any'를 명시 해주어야 합니다.

ACL 설정에 관한 자세한 정보는 **<E5224 Series_user guide 제 15 장 QoS 및 ACL>** 을 참고해 주시기 바랍니다.

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

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

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)# end
Switch#  show running-config
!
access-list 1 deny 192.168.0.0 255.255.255.0
!
```

2.10.3. 텔넷 연결에 액세스 리스트 설정

엑세스 리스트는 user 별로 적용되며, 설정된 엑세스 리스트는 외부에서 스위치로의 접속을 허용하거나 제한합니다.

다음은 192.168.0.0/24 네트워크에서의 접속만을 허용하는 Access list 를 생성하여, 텔넷 접속을 제한하는 예제입니다.

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

2.11. 배너 설정

E5224 Series 스위치는 로그인 배너 및 MOTD 배너를 등록할 수 있습니다. 로그인 배너는 사용자가 시스템에 접속해서 로그인 하기 전에 출력되는 메시지이며, MOTD 배너는 로그인 한 후 EXEC shell 을 실행하기 전에 출력되는 메시지입니다. 배너를 통해 사용자에게 주의 사항과 같은 메시지를 전달할 수 있습니다.

표 2-25. 로그인 배너 및 MOTD 배너 명령어

명령어	설명	모드
banner login *banner-string* **banner login default**	로그인 배너를 등록합니다. *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 삭제합니다.	Config
banner motd *banner-string* **banner motd default**	MOTD 배너를 등록합니다. *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 삭제합니다.	Config

다음은 시스템의 기본 로그인 배너와 MOTD 배너 메시지 입니다.

```
Switch login: root
Password:

Hello.                              <- MOTD 배너

Switch >enable
```

```
Switch #
```

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

```
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 지정됩니다.

위의 예제에서 설정한 로그인 배너는 다음과 같이 출력됩니다.

```
Ubiquoss Mobile Backhaul Switch

Login Banner TEST!

Switch login: root
Password:

Hello.

Switch >
```

3

환경설정 저장 및 소프트웨어 업그레이드

본 장에서는 시스템의 Flash File System 의 관리 방안 및 USB, Compact Flash(CF) File System 의사용에 대해서 설명합니다. E5224 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 됩니다. 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 설명합니다..
(주. 본 매뉴얼에서 설명된 기능은 당사의 사정에 의해 변경될 수 있습니다.)

3.1. 파일 시스템

E5224 Series 스위치는 OS image 파일 저장 및 환경 설정의 저장을 위해 기본적으로 Flash 파일 시스템을 구축합니다. 이 장에서 본 제품의 파일 시스템에 대해 설명합니다.

Flash 파일 시스템은 OS image 파일과 장비의 설정을 파일로 저장하기 위해 사용합니다. 각 파일은 Flash 메모리의 영역에서 기록되고, 저장할 때 또는 **rename** 명령어로 저장이름을 설정할 수 있습니다. 또한 사용자의 요구사항에 따라 이미 Flash File System 에 저장된 파일을 **erase** 명령어로 지울 수 있습니다. 단 지우거나 변경할 파일이 다음 부팅 때 사용될 OS image 또는 설정 파일인지 주의해야 합니다.

시스템 파일 관리를 위한 기본 명령어는 다음과 같습니다.

표 3-1. 파일 관리를 위한 명령어

명령어	설명	모드
show flash:	Flash 파일의 상태를 보여줍니다.	Privileged
dir flash:	해당 파일 시스템의 상태를 보여줍니다.	Privileged

erase flash:	Flash 메모리에 저장된 파일을 삭제합니다.	Privileged
rename flash: *filename* flash: *change*	파일의 이름 및 파일 시스템의 위치를 변경합니다.	Privileged

다음은 E5224 Series 스위치에서 File System 의 정보를 보는 예시입니다. 파일 이름과 파일 사이즈, 그리고 현재(B) 및 다음 부팅 모드(*)에 대한 정보와 함께 그 파일의 종류를 표시합니다.

```
Switch# show flash:


-length- -----------type/info------------ CN path
2216     text file                         B* cot.cfg
33344665 [E5224]3.3.7                     -- mvl2.r337
33238012 [E5224]3.3.8                     B* mvl2.r338
…

194148 Kbytes available (66972 Kbytes used, 26% used)
```

다음은 Flash 파일 시스템에 있는 파일을 지우는 예제입니다.

```
Switch#show flash:


-length- -----------type/info------------ CN path
2216     text file                         B* cot.cfg
33344665 [E5224]3.3.7                     -- mvl2.r337
33238012 [E5224]3.3.8                     B* mvl2.r338
…
194148 Kbytes available (66972 Kbytes used, 26% used)

Switch#erase flash: mvl2.r337
Switch#show flash:

-length- -----------type/info------------ CN path
2216     text file                         B* cot.cfg
33238012 [E5224]3.3.8                     B* mvl2.r338
…
227492 Kbytes available (66972 Kbytes used, 26% used)
Switch#
```

3.2. Image/Configuration/BSP Down/Up Load

E5224 Series 스위치는 운영하면서 필요한 OS Image, Configuration 파일 및 Bootloader 에 대해서 FTP 또는 TFTP 를 이용해서 다운로드 또는 업로드 할 수 있습니다. 이는 새로운 파일을 Flash 파일에 저장하거나, 적용으로 사용될 수도 있고, 운용상 필요한 Backup 을 FTP/TFTP 서버에 할 수 있습니다. 또한 새로운 BSP 파일을 다운로드 하여 적용할 수 있습니다. 이 장에서는 어떻게 FTP/TFTP 를 통해서 파일을 다운로드 또는 업로드 하는지 설명합니다. 아래에서 기술한 running-config 및 startup-config 에 대한 설명은 <Configuration 파일 관리>를 참조하시기 바랍니다.

Warning

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

Warning

FTP/TFTP 를 통해 적용되는 configuration 은 현재 시스템의 configuration 에 추가되거나 변경됩니다. 즉 현재 시스템의 configuration 이 완전히 없어지고 다운로드 되는 configuration 으로 완전히 바뀌지는 않습니다.

3.2.1. FTP 를 통한 Down/Up Load

아래는 FTP 를 이용한 파일 다운로드 또는 업로드 방법에 대한 명령어에 대해서 표로 설명해 놓은 것 입니다.

표 3-2. FTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy ftp: flash:	FTP 서버에 있는 OS Image 파일을 Flash 에 저장합니다.	Privileged
copy flash: ftp	Flash 에 있는 OS Image 파일을 FTP 서버에 저장합니다.	Privileged
copy ftp: config-file	FTP 서버에 있는 Configuration 파일을 Flash 에 저장합니다.	Privileged
copy ftp: running-config	FTP 서버에 있는 Configuration 파일을 현재의 running-config 로 적용시킵니다.	Privileged
copy running-config flash: *filename*	Running-config 를 해당 파일 시스템에 filename 으로 저장합니다	Privileged
copy running-config ftp:	시스템에서 운용중인 현재 running-config 를 FTP 서버에 저장합니다.	Privileged

copy ftp: bootloader	FTP 서버에 있는 BSP 파일을 Flash 에 저장합니다.	Privileged

아래는 FTP 를 이용한 파일 다운 방법에 대한 예를 보여줍니다.

```
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_mvl21.0.6.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 배포합니다.

3.2.2. TFTP 를 통한 Down/Up Load

아래는 TFTP 를 이용한 파일 다운 방법에 대한 명령어에 대해서 표로 설명해 놓은 것 입니다.

표 3-3. 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 저장합니다.	Privileged
copy (usbflash:|disk1:| flash:) (<0-9>|) tftp:	Flash 에 있는 OS Image 파일을 TFTP 서버에 저장합니다.	Privileged

copy tftp: config-file	TFTP 서버에 있는 Configuration 파일을 Flash 에 저장합니다.	Privileged
copy tftp: running-config	TFTP 서버에 있는 Configuration 파일을 현재의 running-config 로 적용시킵니다.	Privileged
copy running-config tftp:	시스템에서 운용중인 현재 running-config 를 TFTP 서버에 저장합니다.	Privileged
copy tftp: bootloader	TFTP 서버에 있는 BSP 파일을 Flash 에 저장합니다.	Privileged

아래는 TFTP 서버에서 파일을 다운로드 하는 방법에 대한 예를 보여줍니다.

```
shu#copy tftp: usbflash:
IP address of remote host ? 10.1.13.4
Source file name ? mvl2l.r330
Destination file name ? mvl2.r330

TFTP::10.1.13.4// mvl2.r330 --> usbflash: 0 [mvl2.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)
```

3.3. Configuration 파일 관리

환경 설정은 시스템 운영자가 E5224 Series 스위치를 운영하면서 설정된 다양한 파라미터의 집합입니다. E5224 Series 스위치에서 사용하는 Configuration 에는 startup-config 와 running-config 가 있습니다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration 을 startup-config 라고 하며, DRAM 내에서 구동하는 환경설정 값을 running-config 라고 합니다. 여기서는 Configuration File Management 에 필요한 저장, 삭제 및 다운로드 방법을 설명합니다.

표 3-4. Configuration Management 명령어

명령어	설명	모드
show startup-config	Flashs, USB, CF 메모리 중 Booting configuration 으로 설정된 파일의 정보를 보여줍니다.	Privileged
show running-config	현재의 환경 설정 정보를 보여줍니다.	Privileged
copy running-config startup-config	현재 시스템에서 운용중인 Running configuration 파일을 startup 파일로 저장합니다.	Privileged
erase startup-config	현재 설정된 startup configuration 파일을 지웁니다.	Privileged

3.3.1. Configuration 파일 저장

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

```
Switch# show running-config
!
interface Giga0/1
 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 Giga0/1
 no switchport
 ip address 192.168.51.1/24
```

```
     ... <생략> ....
SWITCH#
```

3.3.2. Configuration 파일 삭제

E5224 Series 스위치는 시스템 재시동 시 Flash 메모리에 저장되어 있는 startup-config 를 재 로딩합니다. 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 됩니다.

```
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
```

3.4. Boot Mode 설정 및 시스템 재시동

E5224 Series 스위치는 운영하면서 필요한 OS Image 와 configuration 파일에 대해서 다음 부팅 파일로 설정할 수 있습니다. 이렇게 설정된 OS Image 와 configuration 파일은 시스템의 재 시동 시 적용되므로 각별한 주의가 필요합니다. 아래에서는 OS Image 와 configuration 파일에 대해서 어떻게 다음 부팅 모드로 설정하는 지와 시스템 재 시동 방법에 대해서 설명해 놓은 것 입니다.

표 3-5. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
boot system flash *filename*	다음 부팅 시 적용될 OS Image 를 설정합니다.	Privileged
boot system tftp *filename* A.B.C.D	다음 부팅 시 적용될 OS Image 를 tftp booting 으로 합니다.	Privileged
boot config *filename*	다음 부팅 시 적용될 Configuration 파일을 설정합니다.	Privileged
reload	시스템을 재 시동 시킵니다.	Privileged

3.4.1. Boot Mode 설정

E5224 Series 스위치에서 OS Image 와 configuration 파일에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요합니다. **boot flash** 명령어를 실행할 때에는 E5224 Series 스위치에서 사용할 수 있는 OS Image 파일에 대해서만 적용하도록 해야 하며, 또 **boot config** 명령어를 시행할 때에는 E5224 Series 스위치에서 사용할 수 있는 configuration 파일에 대해서만 적용하도록 해야 됩니다. 그리고 현재 Flash File System 에 있는 파일에 대해서만 적용하도록 하여야 합니다.

```
Switch#
Switch# boot system flash mv12.r090
Switch#
Switch# boot config lns.cfg
Switch#
```

3.4.2. 시스템 재시동

E5224 Series 스위치의 전원 On/Off 또는 **reload** 명령으로 시스템 재 시작이 가능합니다. 또한 reload 명령의 in 또는 at 서브 명령으로 시스템 재 시작에 대한 예약도 가능합니다. 만일 reload at 명령으로 시스템 재 시작을 예약한다면 show clock 명령의 현재 시간을 참조하여 설정해야 합니다.

표 3-6. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
reload	시스템을 즉시 재 시작합니다.	Privileged
reload {in *time*|at *time [day]* [*month*]} [*reason*]	시스템 재 시작을 예약합니다. ▪ 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 취소합니다. 시스템 재 시작의 취소 내용은 모든 터미널로 출력됩니다.	Privileged
show reload	시스템 재 시작 예약 내용을 출력합니다.	Privileged

아래 예제는 reload at 명령으로 시스템 재 시작을 예약하는 설정하고 reload cancel 명령으로 예약을 취소하는 설정입니다.

```
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 합니다. Configure terminal 모드로 진입한 후 reload 명령을 실행하면 아래와 같은 설정 저장 여부를 항상 확인합니다.

```
System configuration has been modified. Save? [y/n]: y
```

Warning

시스템이 Flash File System 에 파일을 저장하고 있을 때는 시스템을 강제적으로 재시동 시켜서는 안 됩니다.

4 인터페이스 환경 설정

4.1. 개요

E5224 Series 스위치가 지원하는 인터페이스는 다음과 같습니다.

표 4-1. E5224 Series 스위치가 지원하는 인터페이스

구분	종류
Physical interfaces	Fast Ethernet ● 100Base-T Gigabit Ethernet ● 1000Base-T ● 1000Base-X
port-group interfaces	Port-group
VLAN Interfaces	VLAN
Loopback interface	Loopback

모든 인터페이스 환경 설정은 다음과 같이 진행됩니다.

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

4.2. 공통 명령어

인터페이스 환경 설정에 공통으로 적용되는 명령어는 다음과 같습니다.

표 4-2. 공통 명령어

명령어	설명
interface *IFNAME*	Interface 모드로 진입합니다. *IFNAME*: 환경을 설정할 특정 인터페이스의 이름.
description *string*	인터페이스에 대한 설명을 등록합니다. *string*: 80 자 이내의 문자열의 인터페이스 설명
no description	등록한 인터페이스 설명을 삭제합니다.

4.2.1. Interface name

E5224 Series 스위치에서는 인터페이스에 대한 모든 환경 설정에서 interface name을 사용합니다. Interface name은 다음과 같이 interface type과id로 구성됩니다.

표 4-3. Interface name

구분	Interface type	Interface name	예
Physical interface	Fast Ethernet	”Fa” + slot_id + port_id	Fa0/1
	Gigabit Ethernet	“Gi” + slot_id + port_id	Gi0/1
Port-group interface	Port group	“po” + port-group id	po1
VLAN interface	VLAN	“vlan” + vlan id	Vlan10
Loopback interface	Loopback	“lo” + id	Loopback0

4.2.2. Interface id

Interface name은interface type과id로 구성됩니다. 다음은 E5224 Series 스위치의 interface name 표기 방법과 지원 범위를 나타냅니다.

표 4-4. Interface ID 및 지원 범위

Model	Interface Type	ID 구성	ID Range	Name(예)
E5224	Fast Ethernet	slot_id + port_id	slot_id: 0 port_id: 1-24	Fa0/1
	Gigabit Ethernet	slot_id + port_id	slot_id: 0 port_id: 1-24	Gi0/1

	Port group	port-group id	1 – 32	po1, po30
	VLAN	vlan id	1 – 4094	Vlan1
	LoopBack	interface id	0 – 3	Loopback0

4.2.3. Interface 모드 프롬프트

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

```
Switch (config-if-Giga0/1)#
```

4.2.4. Description 명령어

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

4.3. 인터페이스 정보 및 상태 조회

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

표 4-5. 인터페이스 정보 및 상태 관련 명령어

명령어	설명	모드
show interface *IFNAME*	인터페이스의 설정, 상태 및 통계 정보를 출력합니다.	Privileged
show interface status	물리적 인터페이스의 링크 상태, speed, duplex 정보 등을 출력합니다.	Privileged
show interface transceiver [detail|modue <1-6>]	물리적 인터페이스의 DDM (Digital Diagnostic Monitoring)정보를 출력합니다.	Privileged
show idprom all show idprom *fru-type* show idprom interface *IFNAME*	시스템 FRU 정보를 출력합니다. 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 **E5224 Series_User Guide_제 20 장_Utilities** 장의 <20.5 DDM>을 참조하시기 바랍니다

4.3.1. show interface 명령어

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

```
Switch# show interface

Giga0/1 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 --
```

4.3.2. show interface status 명령어

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

```
Switch# show interface status

Port      Name               Status       Vlan       Duplex  Speed   Type
--------- ------------------ ------------ ---------- ------- ------- ----------------
Gi0/1                        connected    routed        full   a-100 10/100/1000BaseT
Gi0/2                        connected    routed        full  a-1000 10/100/1000BaseT
Gi0/3                        connected    1             full  a-1000 10/100/1000BaseT
Gi0/4                        connected    1             full  a-1000 10/100/1000BaseT
Gi0/5                        notconnect   routed        full    auto 10/100/1000BaseT
Gi0/6                        notconnect   routed        full    auto 10/100/1000BaseT
```

```
Gi0/7                          notconnect   routed       full     auto 10/100/1000BaseT
Gi0/8                          notconnect   routed       full     auto 10/100/1000BaseT
```

4.3.3. show idprom 명령어

show idprom 명령은 시스템의 FRU(Field Replaceable Unit) 정보를 출력합니다. E5224 Series 스위치는 아래와 같은 FRU 타입에 대해 정보를 출력할 수 있습니다.

Chassis
FAN
FMU
Module
Pfe
PMU
Power
Slot
Tranceiver

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

```
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
```

4.4. 물리적 포트 환경 설정

다음은 물리적 포트의 환경 설정에 사용되는 명령입니다.

표 4-6. 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 {auto|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 않습니다.

4.4.1. Shutdown

물리적 포트를 disable시킵니다.
물리적 포트의 shutdown상태를 확인하려면 **show interface**명령을 사용합니다.

```
Switch # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch (config)# interface GigabitEthernet 0/1
Switch (config-if-Giga0/1)# shutdown          <- disable port
Switch (config-if-Giga0/1)# no shutdown       <- enable port
Switch (config-if-Giga0/1)#
```

4.4.2. Speed and duplex

E5224 Series 스위치의 각 인터페이스에서 지원하는 speed는 다음과 같습니다.

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

Speed 또는 duplex를 설정할 때 다 음 사항을 주의하시기 바랍니다.

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

4.4.3. Flow control

Fast Ethernet, Gigabit Ethernet interface 에 대해서 IEEE 802.3x Flow control 기능을 지원합니다. 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 말합니다.
다음은 interface 에 IEEE 802.3x pause frame 을 보내는 설정과 받아서 처리하는 설정을 보여주는 예시입니다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga0/1
Switch(config-if-Giga0/1)# flowcontrol send on
```

```
Switch(config-if-Giga0/1)# flowcontrol receive on
Switch(config-if-Giga0/1)# end
Switch# show flowcontrol
Port     Send FlowControl     Receive FlowControl  RxPause TxPause
         admin    oper        admin    oper
-----    -------  --------    -------  --------     -------  -------
Giga0/1  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 명령어 입니다. 이러한 설정을 확인하기 위해서 **show flowcontrol (IFNAME)** 명령을 사용합니다. 설정을 해제할 경우에는 **no flowcontrol** 명령을 사용합니다.

4.4.4. 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 있습니다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga0/1
Switch(config-if-Giga0/1)# carrier-delay msec 500
Switch(config-if-Giga0/1)# end
Switch#
```

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

4.5. Broadcast suppression

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

표 4-7. E5224 Series 스위치의 Storm-control 설정 명령어

명령어	설명	모드
storm-control	Multicast, broadcast, unicast,packet 을	Interface

(broadcast|multicast|unicast) storm-control level LEVEL no storm-control level	suppression broadcast suppression rate 을 설정	Interface

{OFFICIAL_PRODUCT_NAME}에서는 Broadcast suppression 을 설정하기 위해서 먼저 rate 을 설정해야 합니다. 그 후 해당 트래픽에 대한 설정을 합니다.

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

4.6. Protected Port

Protected Port 는 switch 의 port 들 간의 traffic 이 forwarding 되는 것을 방지 할 수 있는 기능입니다. 하나의 VLAN 내에서도 각각의 port 간에 통신을 원치 않는 경우 혹은 VLAN 으로 설정하기에 너무 번거로울 경우 Protected port 기능을 사용 할 수 있습니다.
Protected 로 설정된 port 들 간에는 unicast, multicast, 그리고 broadcast 를 비롯한 그 어떠한 traffic 도 Layer-2 상에서 forwarding 하지 않게 됩니다.
그러나 PIM (protocol-independent multicast) 와 같이 cpu 에 의해 처리되는 패킷은 forwarding 될 수 있습니다.
또한 protected 로 설정된 port 와 일반 non protected port 사이에서는 일반적인 forwarding 동작을 수행하게 됩니다.

표 4-8. E5224 Series 스위치의 protected port 설정 명령어

명령어	설명	모드
Switchport protected	Configure an interface to be a protected port	Interface
No switchport protected	Protected port 설정 해제	Interface

4.7. Port block

L2 스위치 장비의 경우 기본적으로 unknown destination mac 주소를 가지는 packet 에 대해 flooding 동작을 하게 됩니다.
이는 보안상에 많은 이슈를 발생 시킬 수 있으며, 이러한 문제점을 해결 하기 위해 port block 기능을

사용할 수 있습니다. Port block 기능은 Unknown unicast / multicast traffic 이 특정 포트로 유입 되었을 때 다른 포트들로의 flooding 을 방지 하게 됩니다.
Port block 기능 사용을 위해선 egress port 에 다음은 명령어를 입력 합니다.

표 4-9. E5224 Series 스위치의 port block 설정 명령어

명령어	설명	모드
Switchport block unicast	Block unknown unicast address	Interface
No switchport block unicast	Port block 설정 해제	Interface

4.8. Port mirroring

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

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 예시입니다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int GigabitEthernet 0/1
Switch(config-if-Giga0/1)# mirror interface gi0/2 direction receive
Switch(config-if-Giga0/1)# mirror interface gi0/3 direction receive
Switch(config-if-Giga0/1)# mirror interface gi0/4 direction receive
Switch(config-if-Giga0/1)# end
Switch# show mirror
Mirror Test Port Name: Giga0/1
Mirror option: Enabled
Mirror direction: receive
```

```
Monitored Port Name: Giga0/2
Mirror Test Port Name: Giga0/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga0/3
Mirror Test Port Name: Giga0/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga0/4
Switch#
```

4.9. 2 계층 인터페이스 환경 설정

2계층 인터페이스는2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 E5224 Series 스위치에서는 물리적 포트와 port-group 이 2계층 스위칭 모드로 동작합니다.
이 절에서는2계층 인터페이스의 설명과 물리적 포트와 port-group을2계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여줍니다.

4.9.1. 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 있습니다.
E5224 Series 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에trunk을 설정할 수 있습니다.

4.9.2. 2 계층 인터페이스 모드

E5224 Series 스위치가 지원하는2계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있습니다.

표 4-10. E5224 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

4.9.3. 2 계층 인터페이스 기본 설정 값

E5224 Series 스위치는 물리적 포트 또는 port-group이layer2 interface로 설정될 때 다음과 같은 기본(default) 설정 값을 가집니다.

표 4-11. 2 계층 인터페이스 기본 설정 값

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

4.9.4. 2 계층 인터페이스 설정/해제

2계층 인터페이스로 설정 및 해제하기 위한 명령어는 다음과 같습니다.

표 4-12. 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 복원됩니다.


Notice

E5224 Series 스위치의 초기 설정은 모든 물리적 포트가 3 계층 인터페이스로 되어 있습니다.

4.9.5. Trunk port 설정

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

표 4-13. 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 예입니다.

```
Switch# configure terminal
Switch(config)# interface gi0/1
Switch(config-if-gi0/1)# switchport                ! layer2 interface
set
Switch(config-if-gi0/1)# switchport mode trunk     ! trunk port set
Switch(config-if-gi0/1)# switchport trunk native 2 ! native vlan set
Switch(config-if-gi0/1)# switchport trunk add 3    ! tagged vlan 등록
Switch(config-if-gi0/1)# switchport trunk add 4
Switch(config-if-gi0/1)# end
```

다음은 port-group 인터페이스를2계층 트렁크 포트로 설정하는 예입니다.

```
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
```

4.9.6. Access port 설정

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

표 4-14. 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 예입니다.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-gi0/1)# switchport              ! layer2 interface set
Switch(config-if-gi0/1)# switchport mode access   ! access port set
Switch(config-if-gi0/1)# switchport access vlan 5 ! native vlan set
```

다음은 port-group 인터페이스를2계층 access port로 설정하는 예입니다.

```
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 참조하시기 바랍니다.

4.10. Port group

4.10.1. Port group 개요

Port group 이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용합니다. E5224 Series 스위치에서 port group 인터페이스는2계층 인터페이스로 사용될 수 있습니다.
E5224 Series 스위치의 모델 별 설정 가능한 port group 수는 다음과 같습니다.

모델	port group 수	그룹 당 최대 port
E5224 Series	32	8

4.10.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같습니다.

표 4-15. 포트 그룹 설정 명령어

명령어	설명	모드
Channel-group <1-32> mode on	해당 interface 를 Port group 에 포함시키고 Port group interface 를 생성합니다.	interface
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 Port-channel <1-32>	해당 Port group interface 를 삭제 합니다. Port group 에 맴버가 없을 경우 수행됩니다.	config
show etherchannel	port group 설정 출력	Privileged

Notice

Port group 에 설정에 관련된 보다 자세한 설명은 **E5224 Series_User Guide 제 10 장** LACP 매뉴얼을 참조하시기 바랍니다.

5

가상 랜(VLAN)

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

이 장에서는 다음의 내용들을 다룹니다:

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

5.1. VLAN 개관

물리적으로 동일 LAN 상에 위치하여 통신하는 것처럼 보이는 장치들의 그룹을 “가상 LAN(VLAN)”이란 용어로 표현합니다. 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 도메인입니다. 즉 VLAN 을 사용하면 VLAN 세그먼트(segment)가 하드웨어의 물리적인 연결에 의해 구분되지 않고, 관리자가 만든 논리적인 그룹에 의해 유연하게 구분됩니다.

5.1.1. VLAN 정의

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

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

5.1.2. VLAN 의 장점

VLAN 을 사용하면 다음과 같은 장점이 있습니다:

- **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 수신합니다. 반면 다른 VLAN 에 속하는 스위치의 포트로는 브로드캐스트 트래픽이 전송되지 않습니다. 따라서 VLAN 을 사용하면 브로드캐스트 트래픽이 인접 네트워크로 퍼져나가는 것을 방지하고 네트워크의 효율을 증가시킬 수 있습니다.
- **네트워크 보안 강화**
  전통적인 네트워크에서는 네트워크에 접근하는 누구라도 네트워크 리소스에 접근할 수 있습니다. 또한, 사용자가 허브를 통하여 네트워크 분석기를 접속하게 되면 네트워크의 모든 흐름을 볼 수 있게 됩니다. 하지만 VLAN 을 사용하면 VLAN 에 포함된 장비들은 오직 같은 VLAN 의 구성원들과 통신할 수 있으며, 스위치 포트에 컴퓨터를 접속하는 것으로는 더 이상 모든 네

트워크 리소스에 접근할 수 없습니다. 만약 VLAN A 에 속한 장비가 다른 VLAN B 의 장비와 통신해야 한다면, 트래픽은 반드시 라우팅 장비를 거쳐야 합니다.

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

5.2. VLAN 의 유형

E5224 Series 스위치는 최대 128 개의 VLAN 생성을 지원합니다. VLAN 은 다음의 기준에 따라 생성됩니다:

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

5.2.1. 포트 기반 VLAN(Port-Based VLANs)

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

예를 들면, <그림 5-1>의 E5224 스위치에서 0/3, 0/4 포트는 VLAN A 의 access 포트이고 0/7, 0/8, 0/17,0/18 포트는 VLAN B 의 access 포트로 할당됩니다. 그리고 0/13, 0/14, 0/23, 0/24 포트는 VLAN C 의 access 포트로 정의합니다.

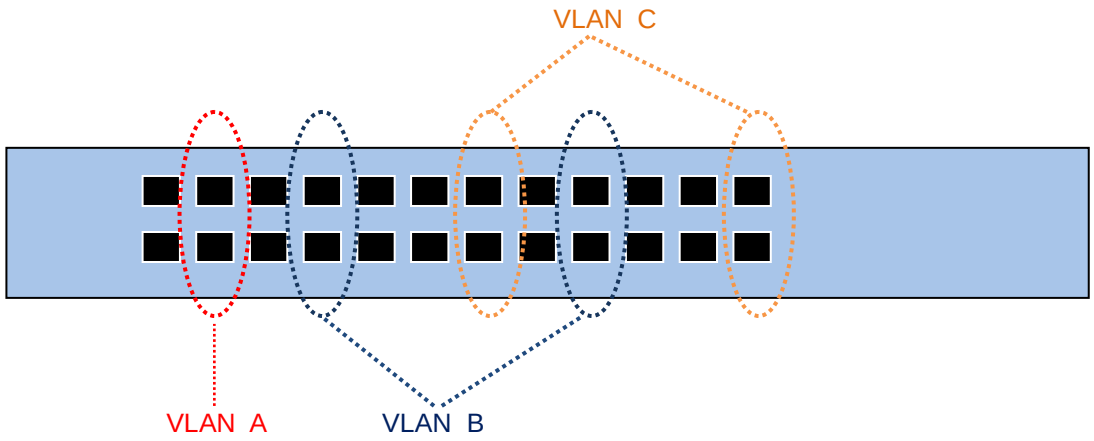


그림 5-1. E5224 Series 스위치의 포트 기반 VLAN 구성 예

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

5.2.1.1. 포트 기반 VLAN 으로 스위치 묶기

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

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

<그림 5-2>는 서로 다른 2 개의 E5224 스위치를 하나의 VLAN 으로 묶는 방법을 나타냅니다. 먼저 스위치 1 의 4 개의 포트는 VLAN A 로 포함되도록 할당되어 있습니다. 또한 스위치 2 의 4 개 포트도 VLAN A 의 access 포트로 할당되어 있습니다. 두 스위치는 <그림 5-2>와 같이 상호 연결하여 하나의 브로드캐스트 도메인을 형성합니다.

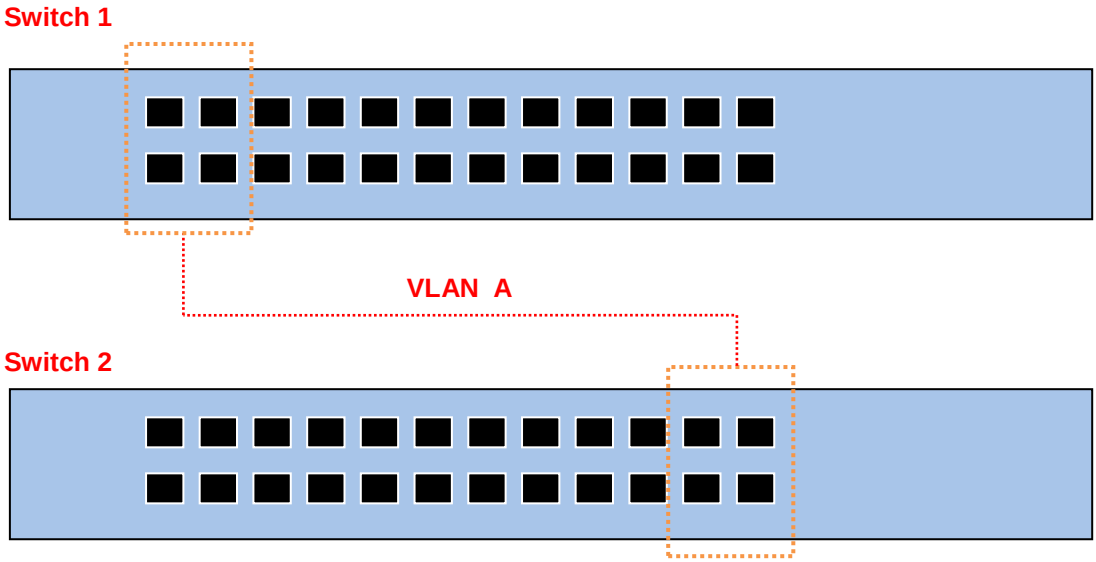


그림 5-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

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 합니다. 그리고 각 스위치에서 적어도 하나의 포트는 각 VLAN 의 access 포트로 할당되어 있어야 합니다.

<그림 5-3 >은 두 개의 E5224 스위치에 걸쳐서 설정되는 두 개의 VLAN 을 나타냅니다. 스위치 1 에서 포트 0/1, 0/2, 0/3, 0/4 포트는 VLAN A 의 access 포트이고 0/9, 0/14 까지의 포트는 VLAN B 의 access 포트로 할당되어 있습니다.

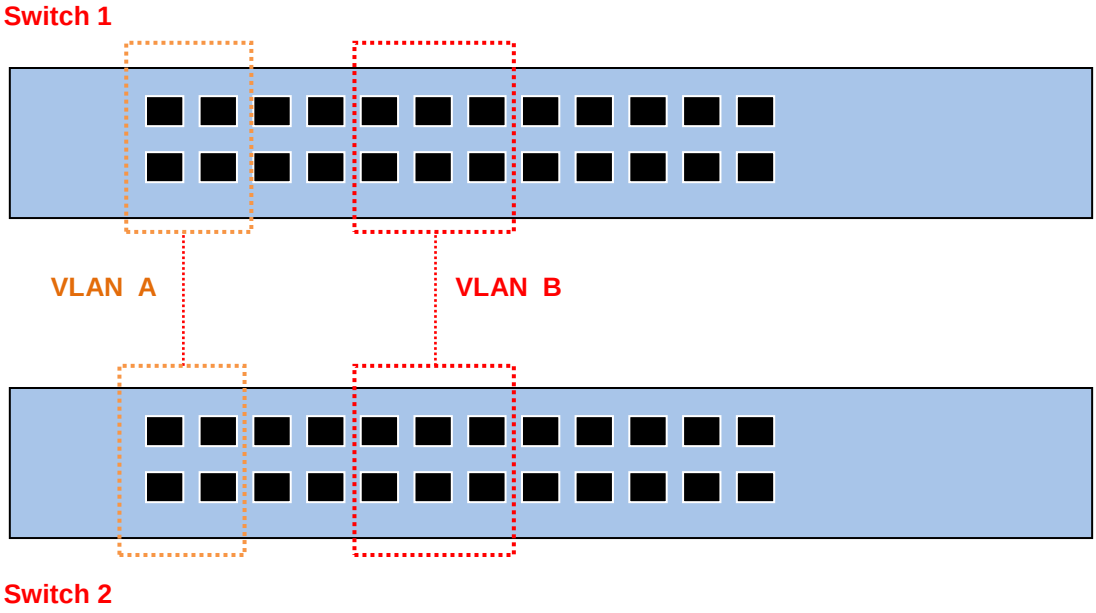


그림 5-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

VLAN A 는 스위치 1 의 포트 1 과 스위치 2 의 포트 1 의 연결을 통해 스위치 1 과 스위치 2 를 묶는다. VLAN B 는 스위치 1 의 포트 9 와 스위치 2 의 포트 9 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 있습니다. 각 스위치는 각각의 VLAN 의 연결을 위한 전용 access 포트를 가지며, 전용 access 포트는 다음 스위치에서 VLAN 의 access 포트와 연결됩니다.

5.2.2. 태그 VLAN(Tagged VLANs)

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

Notice	802.1Q 태그 프레임을 사용하면 IEEE 802.3/Ethernet 프레임의 최대 크기인 1,518 바이트보다 약간 큰 프레임을 발생시킬 수 있습니다. 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 있습니다.

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

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

<그림 5-3 >에서 설명한 것처럼 포트 기반 VLAN 에서는 각 VLAN 별로 하나의 포트를 할당하여 두 스위치를 연결해야 합니다. 하지만 태그 VLAN 을 사용하면 하나의 트렁크만을 사용하여 두 스위치를 묶는 여러 개의 VLAN 을 생성할 수 있습니다.

태그 VLAN 의 또 다른 장점은 하나의 포트가 여러 VLAN 의 멤버가 될 수 있습니다는 점입니다. 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 합니다.

5.2.2.2. 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 사용합니다. 이 경우 태그 VLAN 의 VLANid 가 프레임의 태그로 사용됩니다.

VLAN 의 모든 포트에 반드시 태그가 붙는 것은 아닙니다. 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 결정합니다. 스위치는 VLAN 에 대한 포트 설정에 따라 프레임에 태그를 추가하거나 삭제합니다.

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

<그림 5-4 >는 태그가 붙은 프레임과 태그가 붙지 않은 프레임을 사용하는 네트워크의 물리적인 구성을 나타냅니다.

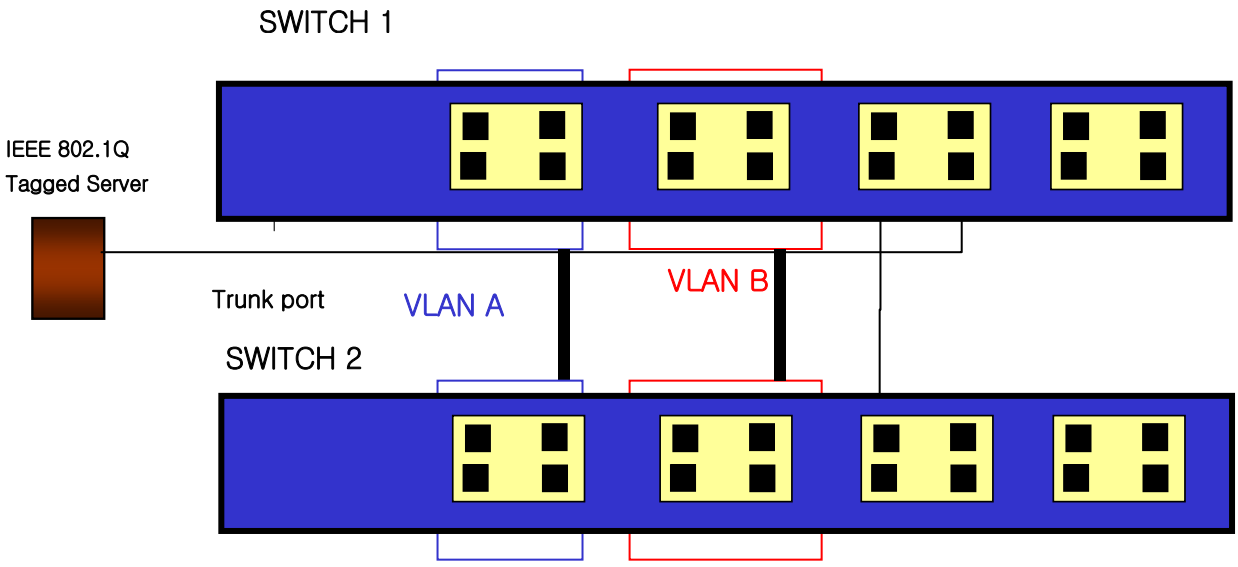


그림 5-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<그림 5-5 >는 동일한 네트워크의 논리적인 다이어그램을 나타냅니다.

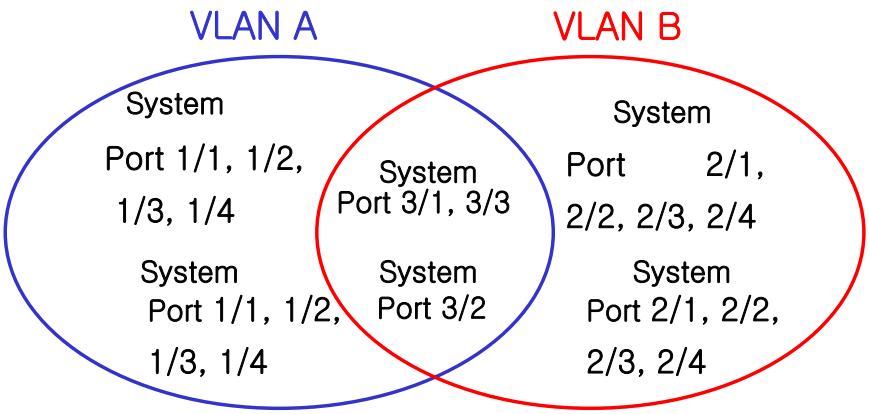


그림 5-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

<그림 5-4 >와 <그림 5-5 >에서:

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

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

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

Hybrid 유형의 VLAN 은 포트 기반의 VLAN 과 태그 VLAN 의 기능을 혼합한 형태입니다. 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 있습니다.

5.3. VLAN 구성

5.3.1. VLAN ID

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

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

5.3.2. Default VLAN

스위치에는 다음과 같은 특성을 가지는 default VLAN 이 설정되어 있습니다.

- Default VLAN 은 VLANid 값으로 1 을 사용합니다.
- 스위치 초기 상태에서 모든 포트는 native VLAN 으로 default VLAN 이 설정되어 있습니다.

5.3.3. Native VLAN

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

<그림 5-6>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 있습니다.

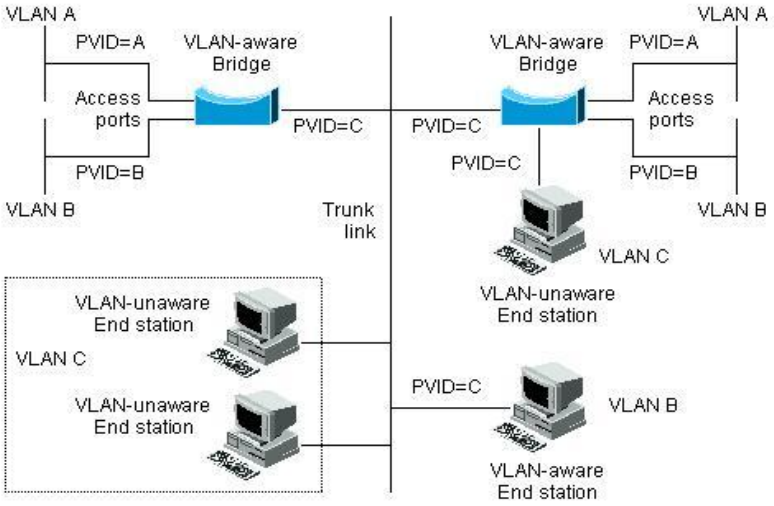


그림 5-6. Native VLAN

예를 들어 <그림 5-6>의 하단 부분에서처럼 두 달말 장비가 중앙의 트렁크 링크에 연결된 상태를 생각해보겠습니다. 그들은 VLAN 을 인식하지 못하지만, VLAN 을 인식하는 브리지의 PVID 가 VLAN C 와 동일하게 하므로 VLAN C 에 포함될 것입니다. 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 송신합니다.

5.4. VLAN 설정

본 절에서는 E5224 Series 스위치에 VLAN 을 설정에 사용되는 명령들을 설명합니다. VLAN 설정은 다음의 단계로 진행됩니다.

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

5.4.1. VLAN 설정 명령

<표 5-1 >은 VLAN 설정에 사용되는 명령들을 설명합니다.

표 5-1. 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 사용합니다	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 있습니다.	vlan database
`vlan` *`vlanid`* `bridge <1-32> 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 있습니다.	
`switchport`	포트의 type 을 L2 로 변경합니다. L2 포트로 변경되면 default 로 access 모드에 VLAN 1 의 맴버가 됩니다.	Interface
`switchport mode {access|hybrid|trunk}`	포트의 VLAN 타입을 설정합니다. `access` – 포트를 access 모드(포트 기반 VLAN)로 설정합니다. 설정된 포트는 태그가 붙지 않은 프레임을 송수신하는 단일 VLAN 의 인터페이스로 동작합니다. Hybrid – 포트를 hybrid 로 설정합니다. `trunk` – 포트를 트렁크(태그 VLAN)로 설정합니다. 설정된 포트는 태그가 붙은 프레임을 송수신합니다.태그가 붙지 않은 프레임의 경우 native VLAN id 로 인식합니다.	Interface
`switchport access vlan` *`vlanid`*	포트를 VLAN 의 access 포트로 설정합니다. 모드가 access 로 설정되면, 설정된 포트는 VLAN 의 멤버 포트로 동작합니다. *vlanid* : 2 부터 4094 사이의 값을 사용합니다.	Interface
`Switchport hybrid vlan` *`vlanid`*	설정된 포트는 VLAN 의 멤버 포트로 동작합니다. 수신되는 프레임이 untagged 일 경우 vlan id 에 해당하는 프레임으로 인식하도록 설정합니다. *vlanid* : 2 부터 4094 사이의 값을 사용합니다.	Interface

명령어	설명	모드
`switchport trunk allowed vlan (add|all|except) vlanid`	포트를 VLAN 의 트렁크 포트로 설정합니다. 특정 VLAN 을 트렁크 포트로 설정하려면 add, 설정된 VLAN 을 모두 설정 하려면 all, 특정 vlan 만 제외 하려면 except 명령을 사용합니다. *vlanid* : 2 부터 4094 사이의 값을 사용합니다.	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 설정합니다. native VLAN 을 설정하지 않으면 default VLAN(VLANid = 1)이 native VLAN 으로 설정 native VLAN 이 설정이 되어 있어도 해당 VLAN 이 트렁크 포트에 add 되어야 정상 동작 합니다. *vlanid* : 2 부터 4094 사이의 값을 사용합니다.	Interface
`switchport trunk (remove|none) vlanid`	포트를 명시한 VLAN 의 멤버에서 제외시킨다. *vlanid* : 2 부터 4094 사이의 값을 사용합니다. none: 모든 VLAN 으로부터 멤버에서 제외	Interface

5.5. 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 할당합니다.

```
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 0/1
Switch(config-if-Giga0/1)#switchport
Switch(config-if-Giga0/1)#switchport mode access
Switch(config-if-Giga0/1)#switchport access vlan 1000
Switch(config-if-Giga0/1)#interface GigabitEthernet 0/2
Switch(config-if-Giga0/2)#switchport
Switch(config-if-Giga0/2)#switchport mode access
Switch(config-if-Giga0/2)#switchport access vlan 1000
Switch(config-if-Giga0/2)#end
Switch#show vlan

VLAN Name                              Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/3  ~ Gi0/24
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    Gi0/1  Gi0/2
...

Switch#
```

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

```
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 0/4
Switch(config-if-Giga0/4)#switchport
Switch(config-if-Giga0/4)#switchport mode trunk
Switch(config-if-Giga0/4)#switchport trunk allowed vlan add 2000
Switch(config-if-Giga0/4)#interface GigabitEthernet 0/1
Switch(config-if-Giga0/1)#switchport
Switch(config-if-Giga0/1)#switchport mode trunk
Switch(config-if-Giga0/1)#switchport trunk allowed vlan add 2000
Switch(config-if-Giga0/1)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- --------------- ------- -------------------------------
-
0               1       default         ACTIVE  Gi0/1 (u) Gi0/4 (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   ?
0                2000     VLAN2000          ACTIVE   Gi0/4 (t) Gi0/2 (t)
shu#
```

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

```
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 0/1
Switch(config-if-Giga0/1)#switchport
Switch(config-if-Giga0/1)#switchport mode hybrid
Switch(config-if-Giga0/1)#switchport hybrid vlan 3000
Switch(config-if-Giga0/1)#switchport hybrid allowed vlan add 4000 egress-tagged
enable
Switch(config-if-Giga0/1)#interface GigabitEthernet 0/2
Switch(config-if-Giga0/2)#switchport
Switch(config-if-Giga0/2)#switchport mode hybrid
Switch(config-if-Giga0/2)#switchport hybrid vlan 3000
Switch(config-if-Giga0/2)#switchport hybrid allowed vlan add 4000 egress-tagged
enable
Switch(config-if-Giga0/2)#end
Switch#show vlan all
Bridge           VLAN ID  Name            State   Member ports
                                                  (u)-Untagged, (t)-Tagged
---------------- ------- ---------------- ------- --------------------------------
-
0                1        default          ACTIVE  Gi0/3 ~ Gi0/24
0                3000     VLAN3000         ACTIVE  Gi0/1 (u) Gi0/2 (u)
0                4000     VLAN4000         ACTIVE  Gi0/1 (t) Gi0/2 (t)
Switch#
```

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

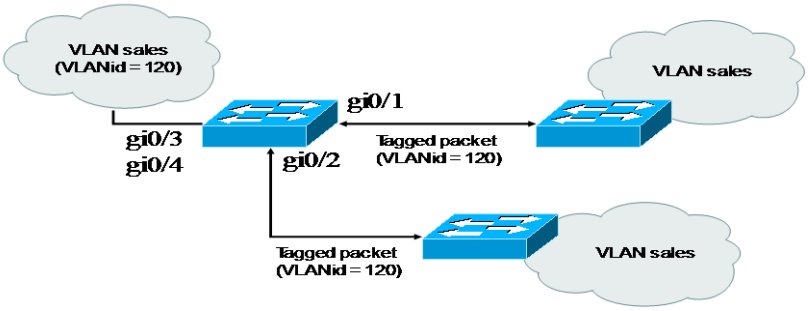


그림 5-7. VLAN 설정 예제 – Tagged and Untagged VLAN

```
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 0/1
Switch(config-if-Giga0/1)#switchport
Switch(config-if-Giga0/1)#switchport mode trunk
Switch(config-if-Giga0/1)#switchport trunk allowed vlan add 120
Switch(config-if-Giga0/1)#interface GigabitEthernet 0/2
Switch(config-if-Giga0/2)#switchport
Switch(config-if-Giga0/2)#switchport mode trunk
Switch(config-if-Giga0/2)#switchport trunk allowed vlan add 120
Switch(config-if-Giga0/2)#interface GigabitEthernet 0/3
Switch(config-if-Giga0/3)#switchport
Switch(config-if-Giga0/3)#switchport access vlan 120
Switch(config-if-Giga0/3)#interface GigabitEthernet 0/4
Switch(config-if-Giga0/4)#switchport
Switch(config-if-Giga0/4)#switchport access vlan 120
Switch(config-if-Giga0/4)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- ---------------- ------- --------------------------------
-
0               1       default          ACTIVE  Gi0/1 (u) Gi0/2 (u)

0               120     VLAN0120         ACTIVE  Gi0/1 (t) Gi0/2 (t)
                                                 Gi1/3 (u) Gi1/4 (u)

Switch#
```

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

```
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 0/1
Switch(config-if-Giga0/1)#switchport mode trunk
Switch(config-if-Giga0/1)#switchport trunk allowed vlan add 200
Switch(config-if-Giga0/1)#switchport trunk native vlan 200
Switch(config-if-Giga0/1)#switchport trunk allowed vlan add 400
Switch(config-if-Giga0/1)#end
Switch#show vlan all
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
--------------- ------- --------------- ------- ------------------------------
-
0               1       default         ACTIVE  Gi0/1 (t)
0               200     VLAN0200        ACTIVE  Gi0/1 (u)
0               400     VLAN0400        ACTIVE  Gi0/1 (t)
Switch#
```

포트 gi0/1 으로 태그가 붙지 않은 프레임이 수신되면 스위치는 VLAN *marketing* 의 멤버 포트로 프레임을 전달합니다.

5.6. VLAN 설정 정보 확인

VLAN 설정 정보를 보려면 다음의 명령을 사용합니다.

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

```
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#
```

6

IP 환경 설정

6.1. 개요

본 장에서는 IP 주소를 설정하는 방법을 설명합니다.

IP 를 설정하기 위해 요구되는 기본 작업은 IP 주소를 네트워크 인터페이스에 할당하는 것입니다. IP 주소를 할당함으로써 인터페이스는 3 계층 인터페이스로 동작합니다.

E5224 Series 스위치는 다음의 인터페이스에 IP 를 할당할 수 있습니다.

- VLAN interface
- Loopback interface

6.2. 네트워크 인터페이스에 IP 주소 할당

IP 주소는 수신된 IP 데이터그램이 보내질 지역을 식별합니다. 어떤 IP 주소들은 특별한 용도로 예약되어 있어 호스트, 서브넷, 네트워크 주소로 사용할 수 없습니다. <표 6-1 >은 IP 주소의 범위를 열거하였고, 어떤 주소들이 예약되었으며 어떤 주소들을 사용할 수 있는지 보여줍니다.

표 6-1. 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 참고 하시기 바랍니다.

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

E5224 Series 스위치는 인터페이스에 IP 주소 할당 기능을 지원합니다. 각 인터페이스는 Primary IP 주소 한 개와 개수 제한이 없는 Secondary IP 주소 설정이 가능합니다. 다양한 상황에서 복수개의 IP 주소가 유용하게 사용됩니다.

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

표 6-2. IP 주소 할당 명령어

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

6.3. ARP(Address Resolution Protocol)

ARP 테이블의 정보를 확인하려면, privilege 모드에서 다음 <표 6-3>의 명령어를 사용합니다.
E5224 Series 에서는 Static ARP 를 설정할 수 있습니다.

표 6-3. ARP 환경 설정을 위한 명령어

명령어	설명	모드
`Show arp`	ARP 테이블의 엔트리를 출력합니다.	Privileged
`clear arp-cache`	ARP 테이블의 엔트리를 삭제합니다.	Privileged
`Clear arp-cache`	해당 interface 의 ARP 엔트리를 삭제합니다	Privileged

interface IFNAME		
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 삭제합니다.	config
arp-ageing-timeout <1-14400>	해당 interface 의 ARP entry 의 소멸 시간을 설정합니다	interface
no arp-ageing-timeout	해당 interface 의 ARP entry 소멸 시간을 default 값으로 설정합니다 (default : 7200 sec)	interface

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

```
Switch#
Switch #configure terminal
Switch (config)#int GigabitEthernet 0/1
Switch (config-if-Giga0/1)#ip address 192.168.1.3/24
Switch (config-if-Giga0/1)#exit
Switch (config)#arp 192.168.1.3 0111.1111.1213
Switch (config)#end

Switch #show arp
Protocol  Address          Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
Internet  192.168.1.3      0111.1111.1213 static    Giga0/1
Internet  10.1.17.104      0022.1926.2db3 dynamic   eth0
Internet  10.1.17.254      0007.7045.a36f dynamic   eth0

Switch #configure terminal
Switch (config)#no arp 192.168.1.3
Switch (config)#end

Switch #show arp
Protocol  Address          Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
Internet  10.1.17.254      0007.7045.a36f dynamic   eth0

Switch #configure terminal
Switch (config)#interface GigabitEthernet 0/1
Switch (config-if-Giga0/1)#arp-ageing-timeout 2000
Switch (config-if-Giga0/1)#
```

6.4. Default gateway 설정

Default gateway 는 라우팅 기능이 없는 L2 장비에서 다른 네트워크상에 있는 장비와의 통신하기 위해 사용됩니다.
L2 스위치는 default gateway IP 로 명시된 라우터 혹은 L3 장비를 통해 외부 네트워크와의 통신이 가능하게 되며 이를 명시 하지 않을 경우 외부 네트워크 장비와의 통신은 불가능합니다.
Telnet 이나 SSH 와 같은 원격접속을 통해 스위치 장비를 제어 / 관리하기 위해서도 default gateway 설정이 필요합니다.

Default gateway 를 설정하려면 Config 모드에서 다음의 명령을 사용합니다.

표 6-4. Default gateway 설정 명령어

명령어	설명
`ip default-gateway A.B.C.D`	Default-gateway IP 주소를 명시합니다.
`no ip default-gateway A.B.C.D`	Default-gateway ip 주소값을 기본 값으로 설정한다. (default : 0.0.0.0)

Default gateway 정보를 확인하려면 privileged 모드에서 다음의 명령을 사용하시기 바랍니다.

명령	목적
show ip route static	IP route 정보를 출력합니다.

6.5. IP 설정 예제

이 절에서는 IP 주소 설정 예제를 제공합니다:

- Assign IP address to network interface
- Assign Secondary IP address to network interface
- ARP
- Assign default-gateway IP address

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

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

다음의 예제는 하나의 vlan interface 에 주 IP address 와 secondary IP address 를 할당합니다.

```
Switch(config)# interface  vlan100
```

```
Switch(config-if-vlan100)# ip  address  192.5.10.1/24
Switch(config-if-vlan100)# ip  address  131.108.3.1/24 secondary
```

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제입니다.

```
Switch# show arp
Protocol  Address          Hardware Addr  Type      Interface
--------- ---------------- -------------- --------- ----------------
Internet  10.1.2.254       0007.7089.1123  dynamic   vlan100
Internet  10.1.11.46       0006.2bfc.146e  dynamic   vlan100
Internet  10.1.13.1        0001.0281.f775  dynamic   vlan100
Internet  10.1.13.190      0000.f083.f6d4  dynamic   vlan100
```

다음의 명령은 ARP 테이블에 static ARP 엔트리를 등록합니다.

```
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    Giga0/1
```

다음의 명령은 ARP 테이블에서 static ARP 엔트리를 삭제합니다.

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

다음의 예제는 192.168.1.10 네트워크에 연결된 호스트가 자신이 속한 네트워크 외에 다른 네트워크 워크로의 통신을 위해 default gateway (IP 192.168.1.254) 를 설정합니다.

```
Switch(config)# interface vlan 100
Switch(config-if-vlan100)# ip default-gateway 192.168.1.254
```

7 UDLD (UniDirectional Link Detection)

이 장에서는 Unidirectional Link Detection (UDLD)를 위한 설정 방법에 대해 설명합니다.

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

이 장은 다음의 절로 구성됩니다.

- Unidirectional Link Detection
- Unidirectional Link Detection Operation
- Unidirectional Link Detection configuration

7.1. Understanding Unidirectional Link Detection

Unidirectional Link Detection (이하 UDLD)는 Layer2 protocol 입니다. Device 에 enable 하면, 연결된 두 port 에 모두 UDLD 기능이 동작해야 감지 할 수 있습니다. 연결된 port 의 Physical Link 에 이상이 생기면 이것을 감지해 알려주는 기능을 하는 protocol 입니다. UDLD 로 인해 port 가 Unidirectional 상태임을 알게 되면 해당 port 는 disable 됩니다. (Unidirectional link 는 STP loop 등의 여러 가지 문제의 원인이 될 수 있습니다.)

7.2. UniDirectional Link Detection Operation

7.2.1. UniDirectional Link Detection

UDLD 동작에는 두 가지 mechanisms 이 사용됩니다.

- Neighbor database maintenance

  UDLD 는 연결된 Link port 의 UDLD 가 주기적으로 보내는 Probe(Hello) message 를 통해 상태를 확인 합니다.

  새로 수신된 정보를 Neighbor table 에 entry 로서 지정된 Hold time 동안 저장, 유지하게 됩니다. 해당 정보가 이미 entry 에 저장 되어 있는 정보 이면, 새로 수신한 정보를 저장, 유지하고, 이미 등록 되어 있던 기존의 정보는 table 에서 삭제 하게 됩니다. 이때 Hold time 은 reset 되게 됩니다. 이 Hold time 동안 해당 정보의 새로운 packet 을 받지 못하면 Neighbor table 에서 해당 entry 를 삭제 하게 됩니다.

  UDLD 가 동작하고 있는 Port 의 UDLD 가 disable 되거나, switch 가 reset 될 경우 해당 port 들은 Flush message 를 전송하고, 모든 UDLD 동작을 중지하게 됩니다.

- Event-driven detection and echoing

  UDLD 는 언제든, 새로운 device 의 정보를 받아, 새로운, Neighbor 를 알게 되면, echo message 를 전송하게 됩니다. 이때, 하나가 아닌 다수의 echo message 를 보내게 되고, 상대편으로부터의 응답 echo message 를 기다리게 됩니다. Reply echo message 를 받게 되면, bidirectional Link 상태로 인지 하게 됩니다. 만약, 해당 message 를 받지 못하면 Link 는 Unidirectional 상태로 여겨져 해당 Port 는 err-disable 상태가 됩니다.

만약 Advertisement 상태에서 모든 neighbor 의 정보가 aged out 되면, UDLD 는 Link-up 시 수행하는 sequence 를 restart 하게 됩니다. 이때, 최초 Link Up 때와 달리 Message 를 기다리는 시간에 제약을 주게 됩니다. 이 제약된 시간 내에 message 를 받지 못하면, 해당 Link 는 UDLD mode 에 따라 처리 됩니다. Normal mode 는 해당 Port 가 잘못된 Port 라는 information 만을 줍니다. Aggressive mode 는 해당 Port 를 err-disable 처리하게 됩니다.

<그림 7-1>은 Unidirectional Link 상태의 한 예를 보여 줍니다.

그림 7-1 UDLD detection of a Unidirectional Link

Switch B 는 switch A 로 부터의 Packet 을 정상적으로 수신할 수 있습니다.
Switch A 를 switch A 로 부터의 Packet 을 정상적으로 수신할 수 없습니다. 만약 UDLD 의 mode 가 aggressive 라면, 해당 port 는 상대 Port 를 인지 할 수 없는 상태가 되고 해당 port 는 err-disable 상태가 됩니다. 만약 UDLD 의 mode 가 normal 이라면, 해당 Link 는 상대방을 알 수 없는 상태로 port 를 disable 시킨다는 정보만을 UDLD 에서 보여 줍니다.

7.2.2. UniDirectional Link Detection Mode

UDLD 는 두 가지 mode 를 지원합니다. Default mode 인 normal mode 와 aggressive mode 두 가지 입니다. 기본적으로 normal mode 를 사용하게 되면, 감지한 결과에 대해 information 을 주고, 추가적으로 aggressive mode 를 사용하면, 해당 port 의 상태를 err-disable 처리하여 Port 를 shutdown 상태로 만듭니다.
Normal mode 와 aggressive mode 모두 Layer1 mechanism 과 함께 동작합니다. Layer1 의 auto negotiation 기능이 동작하지 않을 경우 UDLD 는 Link 의 상태를 감지하게 됩니다.

7.3. configuring Unidirectional Link Detection

7.3.1. Default UDLD Configuration

feature	Default setting
UDLD global enable state	Globally disabled
UDLD per-port enable state for fiber-optic media	Disabled on all Ethernet fiber-optic ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX ports
UDLD aggressive mode	Disabled

7.3.2. UDLD Restriction

UDLD 기능 enable 할 때 다음 사항을 주의 해야 합니다.
연결된 Port 는 동일 모드로 설정되어야 합니다. Global configuration 과 Interface configuration 은 동일 모드로 설정 되어야 합니다.

7.3.3. Enabling UDLD Globally

UDLD Global configuration 이 있어야 UDLD 기능이 동작 합니다. UDLD global 설정은 aggressive mode 와 normal mode 로 설정 가능 합니다.

Global 에서 가능한 모드

Mode	Description
udld enable	udld normal mode 를 설정 합니다
udld aggressive	udld aggressive mode 를 설정 합니다.

UDLD Globally
UDLD 의 mode 뿐 아니라 Message Interval time 도 설정 할 수 있습니다. Message Interval time 은 모든 port 에 설정 되게 됩니다.

	Command	Purpose
Step1	Configure terminal	Global configuration 모드로 진입합니다.
Step2	udld {aggressive | enable | message time message-timer-interval}	UDLD mode of operation * aggressive – aggressive 모드로 설정 합니다. * enable – normal 모드로 설정 합니다. * message time message-timer-interval – Advertisement, Bidirectional phase 가 된 후 보내는 Probe message 간의 interval 값으로 설정 됩니다. 설정 가능한 범위는 7-90 값을 설정 할 수 있습니다. Default 값은 15 seconds 입니다. Note UDLD interface 설정이 있어야 각 port 별로 UDLD 기능을 동작시킬 수 잇습니다.
Step3	end	Privileged EXEC mode 로 돌아갑니다.
Step4	show udld	설정 내용을 확인합니다.

UDLD global 설정을 disable 하려면 다음과 같은 명령을 합니다. no udld enable 은 udld enable 설정을, no udld aggressive 는 udld aggressive 설정을 삭제해 줍니다.
Message interval 설정은 no udld message timer 로 삭제할 수 있습니다.

7.3.4. Enabling UDLD on an Interface

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	interface interface-id	Interface configuration 모드로 진입합니다.
Step3	udld port [aggressive]	UDLD interface 설정입니다 * udld port – UDLD normal mode 로 설정 합니다. * udld port aggressive – UDLD aggressive mode 로 설정 합니다. NOTE no udld port [aggressive]를 사용하여 설정을 삭제 합니다.
Step4	end	Privileged EXEC mode 로 돌아갑니다.
Step5	show udld	설정 내용을 확인합니다.

Fa0/9 번 port 에서 UDLD 를 사용하기 위해 설정 하는 방법을 설명합니다.

```
Switch (config)# udld enable
Switch (config)# udld message time 20
Switch (config)# interface fa0/9
Switch (config-if)# udld port
Switch (config-if)# end
```

7.3.5. Resetting an Interface Disabled by UDLD

Privileged EXEC mode 에서 설정 해 줍니다.

	Command	Purpose
Step1	udld reset	Reset all ports disabled by UDLD
Step2	show udld	변경된 UDLD 상태를 확인합니다..

7.3.6. Displaying UDLD status

UDLD 는 모든 port 또는 각 port 별로 상태를 display 해 줄 수 있습니다. show udld [interface-id] 명령을 사용하여 확인 할 수 있습니다.

아래는 P14C07010027 의 gi0/9 와 FCQ1520Z0Y8 의 fa0/16 가 연결된 상태를 보여 줍니다.

```
switch #show udld gi0/9

Interface Gi0/9
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 38
    Device ID: FCQ1520Z0Y8
    Current neighbor state: Bidirectional
    Device name: C2960_214
    Port ID: Fa0/16
    Neighbor echo 1 device: P14C07010027
    Neighbor echo 1 port: Gi0/6

    Message interval: 15
    Time out interval: 5
```

8

STP(Spanning Tree Protocol)

이 장에서는 Spanning Tree Protocol(STP)과 Rapid Spanning Tree Protocol(RSTP), Multiple Spanning Tree(MSTP), Rapid Per Vlan Spanning Tree Plus (RPVST+)를 설정하는 방법과 Bridge 에서의 프레임 전송에 대해 설명합니다.

Notice

이 장에서 사용되는 명령의 완전한 형식 및 사용법은 command reference 를 참고하시기 바랍니다.

이 장은 다음의 절들로 구성됩니다.

- Understanding Spanning-Tree Features
- Understanding RSTP
- Understanding MSTP
- Understanding RPVST+
- Configuring Spanning-Tree Features
- Displaying the Spanning-Tree Status
- Configuring Bridge Mac Forwarding

8.1. Understanding Spanning-Tree Features

이 절에서는 다음의 STP 기능에 대해 설명합니다.

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

8.1.1. STP Overview

STP 는 네트워크에서 루프를 방지하고 경로의 이중화를 제공하는 Layer 2 링크 관리 프로토콜입니다. Layer 2 이더넷(Ethernet) 네트워크가 정상적으로 동작하려면, 임의의 두 단말 사이에는 오직 하나의 활성 경로만 존재해야 합니다. Spanning-tree 의 동작은 종단 단말(end station)들에 대해 투명하기 때문에, 종단 단말들은 단일 LAN 에 연결되었는지 여러 개의 조각으로 구성된 switched LAN 에 연결되었는지 감지할 수 없습니다.

고장에 견고한 네트워크 형상을 구성하려면, 네트워크의 모든 노드들 사이에는 루프가 없어야 합니다. Spanning-tree 알고리즘은 switched Layer 2 네트워크를 통해 루프가 없는 최적의 경로를 계산합니다. 스위치는 주기적으로 bridge protocol data unit(BPDU)라 불리는 spanning-tree 프레임을 송수신합니다. 스위치는 이 프레임들을 forward 하지 않고, 루프가 없는 경로를 생성하기 위해 사용합니다.

두 종단 단말 사이에 여러 개의 활성화된 경로가 존재하면 네트워크에 루프가 발생합니다. 네트워크에 루프가 존재한다면 종단 단말은 중복된 프레임을 수신할 것입니다. 스위치에서는 한 종단 단말의 MAC 주소가 여러 개의 Layer 2 인터페이스에 등록됩니다. 이런 상황은 네트워크를 불안정하게 만듭니다.

Spanning tree 는 Layer 2 네트워크에서 root 스위치와 root 스위치로부터 모든 스위치까지 루프가 없는 경로를 가진 tree 를 정의합니다. Spanning tree 는 중복된 데이터 경로를 standby(blocked) 상태로 만듭니다. 중복된 경로가 존재하는 네트워크에 고장이 발생하면, spanning-tree 알고리즘은 spanning-tree 형상을 새로 계산하고 standby 경로를 활성화시킵니다.

스위치의 두 인터페이스가 루프의 일부라면, spanning-tree port priority 와 path cost 설정이 인터페이스의 forwarding 상태와 blocking 상태를 결정합니다. port priority 값은 네트워크에서 인터페이스의 위치와 트래픽을 위해 얼마나 잘 위치하고 있는가를 나타냅니다. path cost 값은 매체의 속도를 나타냅니다.

8.1.2. Bridge Protocol Data Units

다음의 요소들에 의해 spanning-tree 의 안정된 active 형상이 결정됩니다.

- 각 VLAN과 연관된 유일한 BridgeID(스위치 priority와 MAC 주소)
- root 스위치로의 spanning-tree path cost
- 각 Layer 2 인터페이스에 할당된 포트 식별자(포트 priority와 포트 번호)

스위치에 전원이 들어왔을 때, 스위치는 root 스위치처럼 동작합니다. 각 스위치는 자신의 모든 포트로 configuration BPDU 를 전송합니다. 스위치들은 BPDU 를 서로 교환하고 BPDU 로 spanning-tree 형상을 계산합니다. 각 configuration BPDU 는 다음의 정보를 포함합니다.

- root 스위치의 BridgeID
- root 까지의 spanning-tree path cost
- BPDU를 전송하는 스위치의 BridgeID
- Message age
- BPDU를 전송하는 스위치의 인터페이스 식별자
- hello, forward-delay, max-age 프로토콜 타이머의 값

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

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

다음은 BPDU 교환으로 인한 결과입니다.

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

8.1.3. Election of Root Switch

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

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

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

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

Root 스위치는 switched 네트워크에서 spanning-tree 형상의 논리적인 중심입니다. Switched 네트워크에서 root 스위치로 닿을 필요가 없는 경로들은 spanning-tree blocking 상태가 됩니다.

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

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

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

Premier 8700 Series 스위치는 802.1T spanning-tree extensions 를 지원합니다. 표와 같이 스위치 priority 로 사용되던 2 바이트가 4 비트 priority 값과 VLAN ID 와 동일한 12 비트 extended system ID 값으로 재할당 됩니다.

표 8-1 Switch Priority Value and Extended System ID

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

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

8.1.5. Spanning-Tree Timers

표는 spanning-tree 의 성능에 영향을 미치는 타이머들을 나타냅니다.

표 8-2 Spanning-Tree Timers

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

8.1.6. Creating the Spanning-Tree Topology

그림에서 모든 스위치들의 스위치 priority 가 default(32768)이고 스위치 A 가 가장 낮은 MAC 주소를 가진다고 가정하면 스위치 A 가 root 스위치가 됩니다. 하지만, forwarding 인터페이스의 개수 혹은 link-type 때문에 스위치 A 는 이상적인 root 스위치가 아닙니다. Root 스위치로 만들려는 스위치의 priority 를 증가시킴으로써(낮은 숫자 값을 사용), spanning-tree 의 형상을 재계산하여 이상적인 스위치를 root 로 만들 수 있습니다.

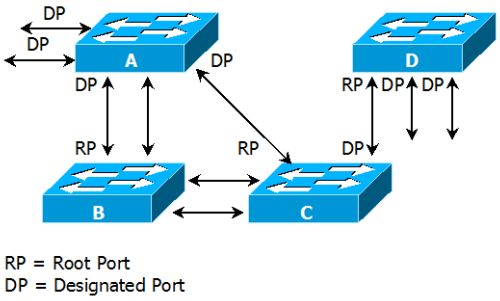


그림 8-1 Spanning-Tree Topology

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

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

8.1.7. Spanning-Tree Interface States

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

Spanning tree 가 활성화된 스위치의 각 Layer 2 인터페이스는 다음 상태 중 하나입니다.

- Blocking - 인터페이스는 프레임을 forwarding하지 않습니다..
- Listening - 인터페이스가 프레임을 forwarding해야 한다고 결정되었을 때, blocking state 다음의 천이 상태.
- Learning – 인터페이스가 프레임을 forwarding하기 위해 준비합니다. MAC learning이 수행됩니다.
- Forwarding – 인터페이스가 프레임을 forward 합니다.
- Disabled – 포트가 shutdown 상태이거나 포트에 링크가 없거나, 포트에 실행중인 spanning-tree instance가 없기 때문에 인터페이스는 spanning tree에 참여하지 않습니다..

인터페이스들은 다음의 상태로 이동합니다.

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

다음의 그림은 인터페이스의 상태천이를 보여줍니다.

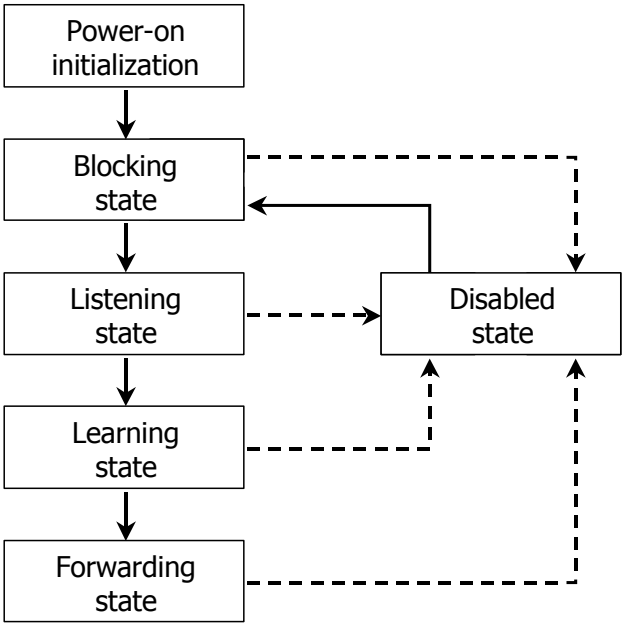


그림 8-2 Spanning-Tree Interface States

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

Spanning-tree 알고리즘이 Layer 2 인터페이스를 forwarding 상태로 만들기로 결정했다면 다음의 과정이 발생합니다.

1. 인터페이스가 forwarding 상태가 되어야 한다는 프로토콜 정보를 수신하면 인터페이스는 listening 상태가 됩니다.
2. forward-delay 타이머가 만료되었을 때, spanning tree는 인터페이스를 learning 상태로 만들고 forward-delay 타이머를 재설정합니다.
3. learning 상태에서, 인터페이스는 종단 단말의 MAC learning은 수행하면서 프레임의 forwarding은 차단합니다.
4. forward-delay 타이머가 만료되면, spanning tree는 인터페이스를 forwarding 상태로 만들고, learning 과 프레임의 forwarding이 모두 가능합니다.

Blocking State

Blocking state 의 Layer 2 인터페이스는 프레임을 forwarding 하지 않습니다.. 스위치는 초기화 후에 스위치의 각 인터페이스로 BPDU 를 전송합니다. 스위치는 다른 스위치와 BPDU 를 교환할 때까지 자신이 root 스위치 인 것처럼 동작합니다. 이러한 BPDU 의 교환은 네트워크의 한 스위치를 root 스위치로 결정합니다. 네트워크에 오직 하나의 스위치만 있다면 스위치 간의 BPDU 교환은 발생하지 않으며, forward-delay 타이머는 종료되면 인터페이스는 listening 상태에 놓입니다. 인터페이스는 스위치 초기화 후에 항상 blocking 상태로 설정됩니다.

인터페이스는 blocking 상태에서 다음과 같이 동작합니다.

- 포트로 수신된 프레임을 폐기합니다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기합니다
- 주소를 learning 하지 않습니다.
- BPDU를 수신합니다

Listening State

listening state 는 blocking 상태 다음의 천이 상태입니다. 인터페이스가 프레임을 forwarding 해야 한다고 결정되면, 인터페이스는 listening 상태가 됩니다.

인터페이스는 listening 상태에서 다음과 같이 동작합니다.

- 포트로 수신된 프레임을 폐기합니다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기합니다
- 주소를 learning 하지 않습니다.
- BPDU를 수신합니다

Learning State

learning 상태의 Layer 2 인터페이스는 프레임 forwarding 을 준비합니다. 인터페이스는 listening 상태에서 learning 상태로 들어갑니다.

인터페이스는 learning 상태에서 다음과 같이 동작합니다.

- 포트로 수신된 프레임을 폐기합니다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기합니다
- 주소를 learning 합니다
- BPDU를 수신합니다

Forwarding State

forwarding 상태의 Layer 2 인터페이스는 프레임을 forward 합니다. 인터페이스는 learning 상태에서 forwarding 상태로 들어갑니다.

인터페이스는 forwarding 상태에서 다음과 같이 동작합니다.

- 포트로 수신된 프레임들을 forward 합니다
- 다른 인터페이스로부터 스위칭된 프레임들을 forward 합니다
- 주소를 learning 합니다
- BPDU를 수신합니다

Disable State

disabled 상태의 Layer 2 인터페이스는 프레임 forwarding 이나 spanning tree 에 참여하지 않습니다..

disable 된 인터페이스는 다음과 같이 동작합니다.

- 포트로 수신된 프레임을 폐기합니다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기합니다
- 주소를 learning 하지 않습니다.
- BPDU를 수신하지 않습니다..

8.2. Understanding RSTP

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

이 절은 RSTP가 어떻게 동작하는 지를 설명합니다.

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

8.2.1. RSTP Overview

RSTP 는 스위치, 스위치 포트 혹은 LAN 에 장애가 발생했을 경우, 재빠른 연결의 복구(약 1 초 이내)를 제공합니다. 새로운 root 포트로 선택된 포트는 바로 forwarding 상태로 천이할 수 있고, 스위치 사이의 명시적인 acknowledgement 를 통해 designated 포트도 forwarding 상태로 바로 천이할 수 있습니다.

8.2.2. Port Roles and the Active Topology

RSTP 는 active 형상을 결정하기 위한 port role 을 할당함으로써 spanning tree 의 빠른 복구를 제공합니다. RSTP 는 STP 처럼 가장 높은 스위치 priority(가장 낮은 priority 값)를 가진 스위치를 root 스위치로 선택합니다. 그리고 RSTP 는 각각의 포트에 다음과 같은 port role 을 할당합니다.

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

root 혹은 designated 포트 역할을 가진 포트는 active 형상에 포함됩니다. alternate 혹은 backup 포트 역할을 가진 포트는 active 형상에서 제외됩니다.

네트워크 전체가 일관된 port role 을 가진 안정된 형상에서, RSTP 는 모든 root 포트와 designated 포트가 바로 forwarding 상태로 천이하는 것을 보장합니다. 반면 모든 alternate 포트와 backup 포트는 항

상 discarding 상태(802.1D 의 blocking 과 동등한 상태)에 놓입니다. 포트의 상태는 forwarding 과 learning 과정의 동장을 제어합니다. 다음의 표는 802.1D 와 RSTP 의 포트 상태를 비교합니다.

표 8-3 Port State Comparison

Operational Status	STP Port State	RSTP Port State	Is Pot Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

STP 구현과의 일관성을 위해, 이 문서에서는 포트 상태에서 discarding 대신 blocking 을 사용합니다. Designated port 는 listening 상태에서 시작합니다.

8.2.3. Rapid Convergence

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

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

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

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

  스위치 B 의 agreement 메시지를 수신한 후에, 스위치 A 는 자신의 designated 포트를 forwarding 상태로 천이합니다. 스위치 B 가 자신의 모든 non-edge port 를 block 시키고, 스위치 A 와 스위치 B 사이는 point-to-point 링크로 연결되었기 때문에 네트워크에 루프가 발생하지 않습니다..

스위치 C 가 스위치 B 와 연결될 때, 유사한 협상 메시지가 교환됩니다. 스위치 C 는 스위치 B 와 연결된 포트를 root 포트로 선택하고, 두 스위치의 두 포트는 forwarding 상태로 천이합니다. 협상 과정에서 하나 이상의 스위치가 active 형상에 참여합니다. 네트워크의 복구에서 이런 proposal-agreement 협상은 spanning tree 의 root 에서 잎 방향으로 진행됩니다.

스위치는 포트의 duplex 모드로 link-type 을 결정합니다. full-duplex 포트는 point-to-point 연결로 고려되고; half-duplex 포트는 공유 연결로 고려됩니다. interface configuration 명령 spanning-tree link-type 명령으로 duplex 모드에 의해 결정되는 default 설정을 변경할 수 있습니다.

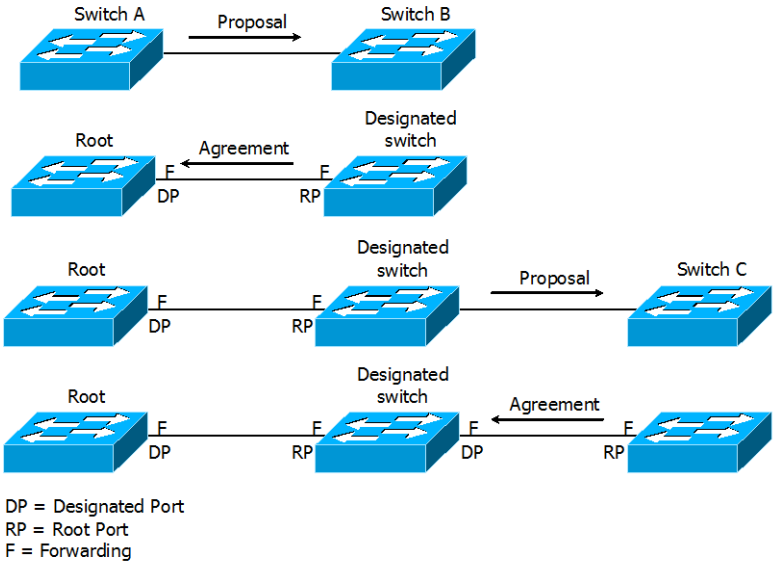


그림 8-3 Proposal and Agreement Handshaking for Rapid Convergence

8.2.4. Bridge Protocol Data Unit Format and Processing

protocol version 필드의 값이 2 로 설정되는 것을 제외하고 RSTP BPDU 의 형식은 IEEE 802.1D BPDU 형식과 같습니다. 새로운 1 바이트 version 1 Length 필드는 0 으로 설정됩니다; 이는 version 1 프로토콜 정보를 포함하지 않는다는 의미입니다. 다음의 표는 RSTP flag 필드를 보여줍니다.

표 8-4. RSTP BPDU Flags

Bit	Function
0	Topology change (TC)
1	Proposal
2-3: 00	Port role: Unknown

01 10 11	Alternate port Root port Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

자신을 LAN 의 designated 스위치로 제안하려는 스위치는 RSTP BPDU 의 proposal flag 를 설정해서 전송합니다. proposal 메시지의 port role 은 항상 designated 포트로 설정됩니다.

다른 스위치에 의한 제안을 받아들이는 스위치는 RSTP BPDU 의 agreement flag 를 설정해서 전송합니다. agreement 메시지의 port role 은 항상 root port 로 설정됩니다.

RSTP 는 독립적인 topology change notification (TCN) BPDU 를 사용하지 않습니다.. topology change 를 알리기 위해 RSTP BPDU flag 의 topology change (TC) flag 를 사용합니다. 하지만 802.1D 스위치와의 연동을 위해 TCN BPDU 를 생성하고 처리합니다.

전송하는 포트의 상태에 따라 learning 과 forwarding flag 가 설정됩니다.

8.3. Understanding MSTP

MSTP (Multiple Spanning Tree Protocol)은 IEEE 802.1s 에 정의된 프로토콜이며, 복수개의 VLAN 을 하나의 그룹으로 묶어 스패닝 트리를 동작시킵니다. MSTP 에서는 인스턴스라고 하는 VLAN 그룹당 하나의 스패닝 트리가 동작하므로 많은 수의 스패닝 트리를 계산할 필요가 없어 스위치의 부하를 줄일 수 있습니다.. 예를 들어, 2000 개의 VLAN 을 사용하는 네트워크에서 PVST 를 사용하면 스위치들이 2000 개의 스패닝 트리를 계산해야 합니다. 그러나 MSTP 를 사용하여 2000 개의 VLAN 을 2 개의 그룹으로 나눈다면 스패닝 트리는 2 개만 사용하게 됩니다. 뿐만 아니라 MSTP 가 동작하면 BPDU 전송량도 획기적으로 줄어든다. 이처럼 MSTP 를 사용하여 스패닝 트리의 수를 줄일 수 있는 것은 대부분의 스위치 네트워크에서 밑의 그림에서 나타내듯 로드 밸런싱 시킬 수 있는 경로 수만큼의 스패닝 트리만 필요하기 때문입니다.

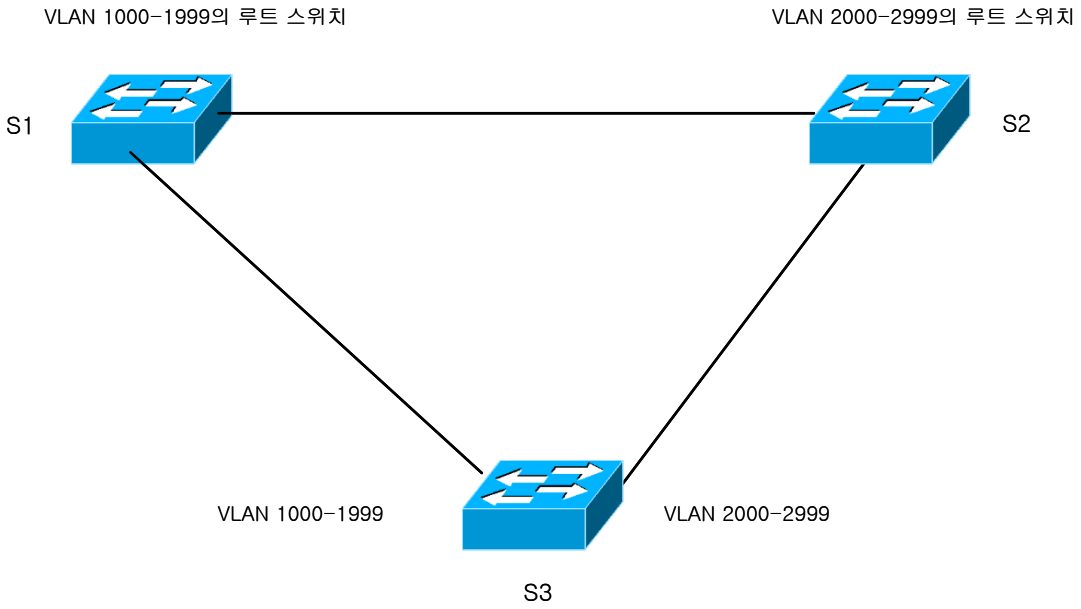


그림 8-4 VLAN 에 대한 load balance

즉, 스위치 S3 에서 사용되는 VLAN 이 1000-2999 까지 2000 개라 하여도 스패닝 트리가 2 개만 동작하면 S1, S2 로 로드 밸런싱 시킬 수 있습니다.

8.3.1. MST 영역

동일한 MST 설정값을 가진 스위치의 집합을 하나의 MST 영역 (region)이라고 합니다. MST 설정값 중에서 MST name, MST revision 및 instance 의 VLAN list 값이 일치하는 스위치들을 동일한 MST 영역에 있다고 합니다.

8.3.2. IST, CST 및 CIST

MSTP 에서는 2 가지 종류의 스패닝 트리가 사용됩니다. 하나의 MST 영역내에서는 IST (Internal Spanning Tree)가 동작 합니다. 동일 MST 영역에서 모두 63 개의 스패닝 트리를 동작시킬 수 있습니다. 각각의 스패닝 트리 인스턴스에 0 에서 63 까지의 번호를 사용할 수 있으며, 이중에서 인스턴스 0 을 IST 라고 합니다. MST 에서는 IST 만 BPDU 를 송수신 합니다. 따라서 다른 인스턴스의 스패닝 트리 정보가 모두 IST 의 BPDU 에 포함되어 있으며, 스위치가 처리해야 하는 BPDU 의 수가 더욱 줄어든다. MST 영역을 포함한 전체 스위치 네트워크에서 공통으로 CIST (common and Internal Spanning Tree)가 동작합니다. CIST 는 IST 와 CST 의 집합입니다. IEEE 802.1Q 에서는 복수개의 VLAN 이 존재해도 스패닝 트리는 하나만 동작하며, 이 스패닝 트리를 CST (common Spanning Tree)라고 합니다. IST, CST 및 CIST 의 관계를 그림으로 나타내면 다음과 같습니다.

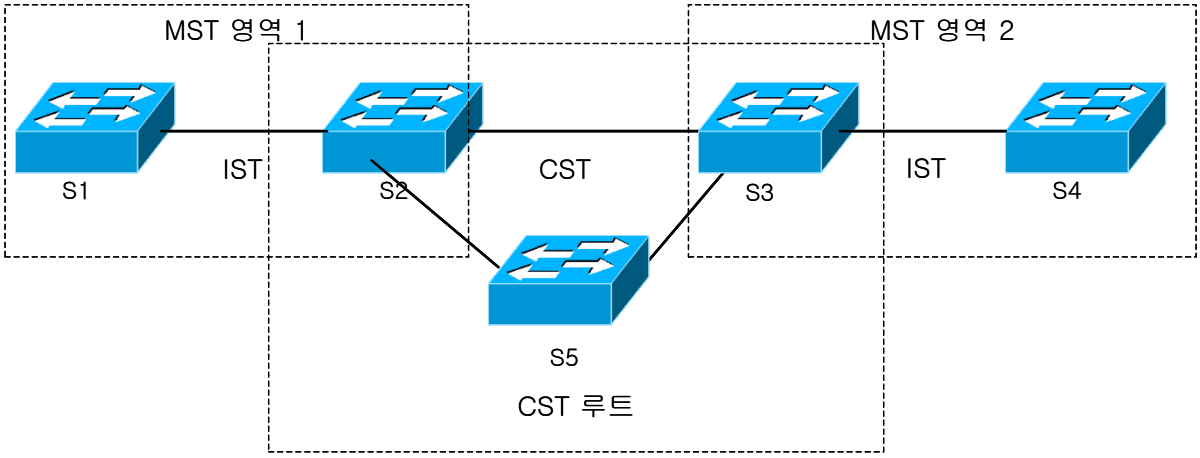


그림 8-5 CST, IST, CIST

MST 영역이 다르면 IST 도 서로 별개로 동작합니다. 서로 다른 MST 영역 사이에는 IST 가 아닌 CST 가 동작합니다. 따라서 그림에서 스위치 S1, S2 의 MST 영역이 스위치 S3, S4 와 서로 다르므로 각각의 MST 영역에서 동작하는 IST 는 별개로 동작하며, 두 영역을 연결하는 스위치 S2 와 S3 사이에는 CST 가 동작합니다. 각 MST 영역내에서 CST 루트 스위치까지의 경로값, 브리지 ID, 포트 ID 값이 가장 작은 스위치를 IST master 라고 합니다. 위의 그림처럼 S5 가 CST 루트 스위치라면 S2 와 S3 이 각각의 MST 영역에서 IST master 스위치로 동작합니다 CST 루트 스위치가 MST 영역 밖에 있다면, IST 마스터는 항상 CST 와 MST 의 경계상에 있게 됩니다. 만약 스위치 네트워크가 하나의 MST 영역으로 구성된 경우에는 동일한 스위치가 CST 루트와 IST 마스터로 동작합니다. CST 는 서로 다른 MST 영역 간 뿐만 아니라 802.1D 로 동작하는 스위치 사이 또는 MST 와 802.1D 스위치 사이에서도 동작합니다. CST 의 관점에서 하나의 MST 영역 전체를 하나의 스위치로 간주합니다. 따라서 위와 같은 네트워크를 CST 에서는 다음 그림과 같이 인식합니다.

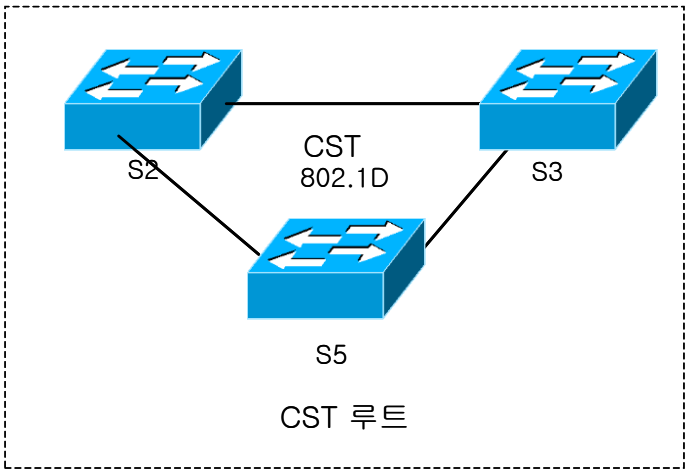


그림 8-6 CST 에서 인식하는 네트워크

8.4. Understanding RPVST+

VLAN trunk 에 관한 표준인 IEEE 802.1Q 는 trunk 에 허용된 모든 VLAN 에 대해 오직 하나의 spanning-tree instance 만 요구하고 있습니다. 그리고 기존의 PVST (Per Vlan Spanning-Tree)의 경우 각 VLAN 별로 spanning-tree instance 를 제공 하지만 IEEE 802.1D 와는 다른 frame 포멧을 사용하기 때문에 연동 되지 않습니다.. RPVST+ (Rapid Per Vlan Spanning-tree plus)는 이러한 문제를 해결하기 위해서 VLAN trunk 에서 BPDU 를 전송 할 때 0100.0CCC.CCCD 의 Multicast MAC 주소를 이용합니다. VLAN ID 가 1 이고 native 인 경우 untagged 로 전송되고 VLAN ID 가 1dl 아닌 native 의 경우 tagged 로 전송됩니다. 이를 통해 VLAN trunk 의 각 vlan 마다 존재하는 spanning-tree instance 가 IEEE 802.1Q 만을 지원하는 스위치를 지나도 BPDU 를 올바로 전송 할 수 있습니다.

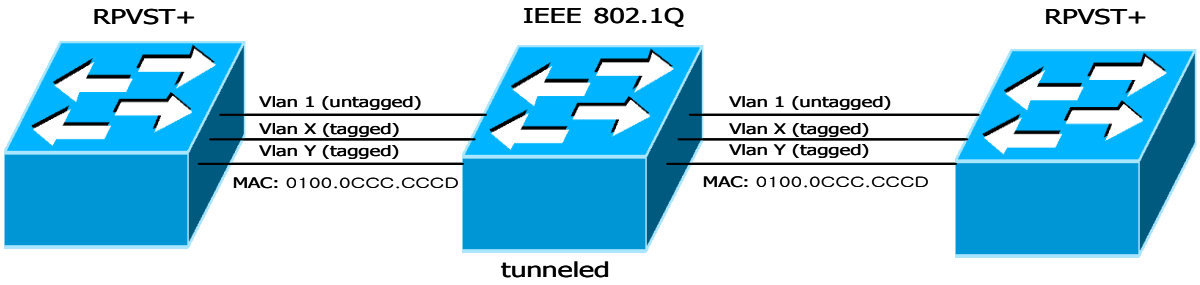


그림 8-7 PVST+ switch 와 IEEE 802.1Q 연동

8.5. Configuring Spanning-Tree Features

이 절에서는 spanning-tree 를 설정하는 방법에 대해 설명합니다. Spanning-tree 의 설정 방법은 mode 에 따라 차이가 있습니다. RSTP 와 STP 의 경우 같은 방법으로 설정되고 MSTP, RPVST+의 경우 다른 설정방법을 같습니다.

8.5.1. Default STP Configuration

다음의 표는 STP 의 default 설정을 보여줍니다.

표 8-5. Default STP Configuration

Feature	Default Setting
Enable state	모든 bridge 에 대해 비활성 되어 있음. 기본적으로 RPVST+ 모드가 설정되어 있는 상황에서 disable 로 되어있어서 enable 시킬 경우 RPVST+ 가 시작됨
Spanning-tree mode	Rapid Per-VLAN Spanning Tree+(RPVST+)
System priority	32768.
Spanning-tree port priority (configurable on a per-port)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	10000 Mbps: 2. 1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello time	2 초.
Forward-delay time	15 초.
Maximum-aging time	20 초.

8.5.2. STP Configuration Guidelines

'spanning-tree enable' 하고 port 에 VLAN 을 추가 하면 VLAN 별로 독립적인 STP 가 동작하게 된다.

8.5.3. Enabling STP

E5224 Series 에서 처음에 STP 는 동작하지 않습니다.. 네트워크에 루프가 존재할 가능성이 있다면 STP 를 활성화 시키도록 합니다. STP 를 활성화 시키면 기본적으로 RPVST+가 구동 됩니다.

Warning

STP 가 비활성 되어있고 형상에 루프가 존재한다면, 과도한 트래픽과 무한의 패킷 중첩이 발생하여 네트워크의 성능을 감소시킵니다.

STP 를 활성화시키려면 privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	spanning-tree enable	Default Bridge 에 대해 STP 를 구동합니다
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show spanning-tree	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

STP 를 비활성 하려면, global configuration 명령 spanning-tree shutdown 를 사용합니다.
다음은 STP 를 활성화하고 비활성화하는 예를 보여줍니다.

```
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree enable
MVL2(config)#end
MVL2#show spanning-tree

Default  Bridge up - Spanning Tree Enabled rpvst+
  Root ID    Priority    32768
             Address     000770b2a7c9
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300
```

```
Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Desg FWD 200000    128.122  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree shutdown
MVL2(config)#end
MVL2#show spanning-tree

MVL2#
```

8.5.4. Enable STP in not default Bridge

E5224 Series 는 Bridge 별로 spanning-tree 를 운영할 수 있습니다. Bridge 를 생성하고 여기에 spanning-tree 로 동작되길 원하는 interface 를 포함 시킨 후 해당 Bridge 의 spanning-tree 를 활성화 시키면 됩니다.

	Notice	Bridge 에 spanning-tree 를 구동하기 위해 포함 시키는 interface 는 직접 Bridge 에 넣을 수 없고 VLAN 에 넣은 후 그 VLAN 을 Bridge 에 넣어야 합니다.

Default Bridge 이외의 Bridge 의 STP 기능을 활성 시키려면, privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	Bridge <1-256> protocol vlan-bridge	Bridge 를 생성합니다.
Step3	bridge <1-256> spanning-tree enable	Bridge 의 STP 를 enable 합니다.
Step4	Bridge-group <1-256>	Vlan 을 Bridge 에 포함시킵니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

Default Bridge이외의 Bridge의 STP기능을 비활성화 하려면, global configuration 명령 bridge shutdown <1-256> 명령을 사용하시기 바랍니다. Bridge를 삭제 하기 위해서는 no bridge <1-256> 명령을 사용합니다.

```
MVL2#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#bridge 1 protocol vlan-bridge
MVL2(config)#bridge 1 spanning-tree enable
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#bridge-group 1
MVL2(config-if-Giga0/23)#end
MVL2#show running-config
!
bridge 1 protocol vlan-bridge
bridge 1 spanning-tree enable
!

MVL2#show spanning-tree
1  Bridge up - Spanning Tree Enabled rpvst+
  Root ID    Priority    32768
             Address     000770b2a7c9
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23    Deg FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#bridge shutdown 1
MVL2(config)#no bridge 1
MVL2(config)#end
MVL2#show running-config!
!
!
MVL2#
```

8.5.5. Configuring the Port Priority

루프가 발생하면 spanning tree 는 포트의 priority 를 사용하여 forwarding 상태의 인터페이스를 결정합니다. 먼저 선택될 인터페이스에는 높은 priority 의 값(낮은 수)을, 나중에 선택될 인터페이스에는 낮은 priority 의 값(높은 수)를 할당할 수 있습니다. 모든 인터페이스가 같은 priority

값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킵니다.

인터페이스의 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹입니다.
Step3	spanning-tree port-priority priority	인터페이스의 포트 priority 를 설정합니다. ● priority 의 범위는 0~240 사이의 16의 배수입니다. default는 128 입니다. 낮은 수가 높은 priority를 의미합니다. 유효한 값은 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224와 240입니다. 이외의 다른 값들은 거부됩니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show spanning-tree	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

인터페이스의 default 설정으로 복구하려면, interface configuration 명령 no spanning-tree priority를 사용합니다. Default Bridge가 아닌 경우에는 spanning-tree 대신 bridge <1-256> 을 사용합니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        122 (Giga0/24)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/24      Root FWD 200000    128.122  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree port-priority 0
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
```

```
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000      0.123  P2

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree port-priority
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost        200000
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.6. Configuring the Path Cost

spanning-tree 의 path cost 의 default 값은 인터페이스의 속도로부터 결정됩니다. 루프가 발생하면 spanning tree 는 포트의 cost 를 사용하여 forwarding 상태의 인터페이스를 결정합니다. 먼저 선택될 인터페이스에는 낮은 cost 값을, 나중에 선택될 인터페이스에는 높은 cost 값을 할당할 수 있습니다. 모든 인터페이스가 같은 cost 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킵니다.

Notice

port group 일 경우 path cost 의 값을 인터페이스의 속도로부터 결정할 수 없습니다. 각각의 멤버 포트가 서로 다른 속도를 가질 수 있습니다. 따라서 port group 에 대해서는 수동으로 path cost 를 설정해서 사용하시기 바랍니다.

인터페이스의 path cost 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

Command	Purpose

Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹입니다.
Step3	spanning-tree path-cost cost	cost 를 설정합니다. 루프가 발생했을 때 forwarding 상태의 포트를 결정하기 위해 spanning tree 는 path cost 를 사용합니다. path cost 값이 낮을 수록 고속의 전송이 가능함을 의미합니다. ● cost 의 범위는 1~200000000 입니다. default 값은 인터페이스의 전송속도로부터 결정됩니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show spanning-tree	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

인터페이스의 default 설정으로 복구하려면, interface configuration 명령 no spanning-tree path- cost 를 사용합니다. Default Bridge가 아닌 경우에는 spanning-tree 대신 bridge <1-256> 을 사용합니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
 Root ID    Priority    4097
            Address     5835d97ea600
            Cost        200000
            Port        123 (Giga0/23)
            Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

 Bridge ID  Priority    32768
            Address     000770b2a7c9
            Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
            Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree path-cost 10
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
 Root ID    Priority    4097
            Address     5835d97ea600
            Cost        10
            Port        123 (Giga0/23)
            Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

 Bridge ID  Priority    32768
            Address     000770b2a7c9
            Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
```

```
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 10        128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree path-cost
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost        200000
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.7. Configuring the Switch Priority of a VLAN

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

VLAN 에 대한 스위치 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	spanning-tree priority priority	● priority 의 범위는 0~61440 사이의 4096의 배수입니다. default는 32768 입니다. 낮은 수일수록 root 스위치로 선택될 가능성이 높다. 유효한 priority 값은 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344과 61440 입니다. 다른 값들은 거부됩니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show spanning	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

스위치의 default 설정으로 복구하려면, global configuration 명령 no spanning-tree priority 명령을 사용하시기 바랍니다. . Default Bridge가 아닌 경우에는 spanning-tree 대신 bridge <1-256> 을 사용합니다.

```
MVL2#show spanning-tree

Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree priority 0
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    0
             Address     000770b2a7c9
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    0
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Desg FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#no spanning-tree priority
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
```

```
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.8. Configuring the Hello Time

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

hello time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	spanning-tree hello-time seconds	hello time 은 root 스위치가 configuration 메시지를 전송하는 주기입니다. 이 메시지는 스위치가 살아있음을 의미합니다. • seconds 의 범위는 1~10 입니다. default 는 2 입니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show spanning-tree	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

스위치의 default 설정으로 복구하려면, global configuration 명령 no spanning-tree hello-time 명령을 사용하시기 바랍니다. Default Bridge가 아닌 경우에는 spanning-tree 대신 bridge <1-256> 을 사용합니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree hello-time 9
MVL2(config)#end
MVL2#show spanning-tree

Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
```

```
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  9  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#no spanning-tree hello-time
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost        200000
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.9. Configuring the Forwarding-Delay Time for a VLAN

VLAN 의 forwarding-delay time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	spanning-tree forward-time seconds	forward delay 는 포트가 spanning-tree 의 listening 혹은 learning 상태에서 forwarding 상태로 천이하기 위해 기다리는 시간입니다. ● seconds 의 범위는 4~30 입니다. default는 15 입니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show spanning-tree	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

스위치의 default 설정으로 복구하려면, global configuration 명령 no spanning-tree forward-time 명령을 사용하시기 바랍니다. Default Bridge가 아닌 경우에는 spanning-tree 대신 bridge <1-256> 을 사용합니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree forward-time 20
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  20 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#no spanning-tree forward-time
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
```

```
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.10. Configuring the Maximum-Aging Time for a VLAN

maximum-aging time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	spanning-tree max-age seconds	maximum-aging time 을 설정합니다. maximum-aging time 은 스위치가 재구성을 하기 전에 spanning-tree 정보를 수신하지 않고 기다리는 최대 시간입니다. ● seconds 의 범위는 6~40 입니다. default는 20 입니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show spanning-tree	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

스위치의 default 설정으로 복구하려면, global configuration 명령 no spanning-tree max-age 명령을 사용하시기 바랍니다. Default Bridge가 아닌 경우에는 spanning-tree 대신 bridge <1-256> 을 사용합니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree max-age 15
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        200000
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
```

```
 Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 15 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#no spanning-tree max-age
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
 Root ID    Priority    4097
          Address     5835d97ea600
          Cost        200000
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

 Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.11. Changing the Spanning-Tree mode for switch

E5224 Series 는 STP, RSTP, MSTP, RPVST+ mode 를 지원하고 mode 가 정해지면 모든 Bridge 는 정해진 mode 로 변경 되고 disable 상태로 변합니다.

스위치의 spanning-tree 모드를 변경하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	spanning-tree mode {rstp|stp|mstp|rpvst+}	스위치의 spanning-tree 모드를 변경합니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show running-config	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
 Root ID    Priority    4097
          Address     5835d97ea600
          Cost        200000
```

```
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p


MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree mode stp-vlan-bridge
MVL2(config)#end
MVL2#show spanning-tree

Default  Bridge up - Spanning Tree Enabled stp-vlan-bridge
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost        19
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 19        128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree mode mstp
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled mstp
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost        200000
          Port        123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
MVL2(config)#spanning-tree mode rpvst+
MVL2(config)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rpvst+
  Root ID    Priority    32768
             Address     000770b2a7c9
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Disb FWD 200000    128.123  P2p
```

8.5.12. Configuring the Port as Edge Port

RSTP 를 사용할 때, 단일 호스트와 연결된 포트에 대해서 edge port 로 설정합니다. 만약 포트를 edge 포트로 설정하지 않으면, 그 포트는 forwarding 상태로 천이하는데 2 x Forward Time 이 소요됩니다.

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

포트를 edge port 로 설정하려면, privileged EXEC 모드부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	Interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹입니다.
Step2	spanning-tree edgeport	포트를 edge port로 설정합니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show running-config	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

스위치의 default 설정으로 복구하려면, interface configuration 명령 no spanning-tree edgeport 명령을 사용하시기 바랍니다.

```
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
             Address     5835d97ea600
```

```
          Cost       200000
          Port       123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree edgeport
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree
Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost       200000
          Port       123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p    edge port

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree edgeport
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree

Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    4097
          Address     5835d97ea600
          Cost       200000
          Port       123 (Giga0/23)
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
          Address     000770b2a7c9
          Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
          Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
```

8.5.13. Specifying the Link Type to Ensure Rapid Transitions

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

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

Notice

port group 의 경우 duplex 모드로부터 링크의 종류를 판단할 수 없습니다. 각각의 멤버 포트가 서로 다른 duplex 모드를 가질 수 있습니다. 따라서 port group 에 대해서는 수동으로 링크 종류를 설정해서 사용하시기 바랍니다.

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

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Stpe3	spanning-tree link-type point-to-point	포트의 링크 종류를 point-to-point 로 설정합니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 설정으로 복구하려면, interface configuration 명령 no spanning-tree link-type 명령을 사용합니다.

8.6. Configuring MSTP Features

이 절에서는 multiple spanning-tree(MSTP)를 설정하는 방법에 대해 설명합니다. MSTP 의 경우 instance 별로 spanning-tree 가 구성 되기 때문에 instance 를 생성하고 여기에 VLAN 을 포함 시키는 부분과 STP 나 RSTP 와 같이 hello time, port priority 등을 설정하는 부분으로 나뉩니다.

8.6.1. Instance 생성 및 VLAN 연결

Instance 를 생성하고 여기에 VLAN 을 넣기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거칩니다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	Spanning-tree mst configuration	Instance 를 생성하고 vlan 과 연결시키기 위해 mst configuration 모드로 진입합니다.
Stpe3	instance instance-id vlan vlan-id	Instance id 를 생성하고 여기에 vlan-id 에 있는 vlan 을 포함시킵니다
Step4	exit	Global configuration 모드로 진입합니다.
Step5	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step6	Spanning-tree instance instance-id	Instance 에 해당 포트를 넣는다
Step7	end	privileged EXEC 모드로 변경합니다.
Step8	show running-config	설정 내용을 확인합니다.
Step9	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

생성되어 있는 instance 를 삭제할 경우에는 no instance instance-id 명령을 사용하시기 바랍니다.

```
MVL2#show spanning-tree mst configuration
name      [Default]
Revision  0     Instances configured 0

%   Instance        VLAN
%   0:              1, 22, 44, 4094
shu#show spanning-tree mst configuration

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree mst configuration
MVL2(config-mst)#instance 1 vlan 22
MVL2(config-mst)#exit
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree instance 1
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree mst configuration
name      [Default]
Revision  0     Instances configured 0

%   Instance        VLAN
%   0:              1, 44, 4094
%   1:              22

MVL2#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree mst configuration
MVL2(config-mst)#no instance 1 vlan 22
MVL2(config-mst)#end
MVL2#show spanning-tree mst configuration
name      [Default]
Revision  0     Instances configured 0

%   Instance       VLAN
%   0:             1, 22, 44, 4094
```

8.6.2. Instance and port configuration

MSTP 에서는 각 instance 마다 spanning-tree 가 동작하기 때문에 instance 별로 priority 를 설정합니다. 여기서 사용되는 명령어 들은 STP, RSTP 에서 사용되는 명령어에 instance 가 붙어서 사용됩니다. Instance 에 priority 를 설정하기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	Spanning-tree instance instance-id priority priority	Instance 에 priority 를 설정합니다
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show running-config	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 값으로 복구하려면 no spanning-tree instance instance-id priority 명령을 사용합니다.

```
MVL2#show spanning-tree mst
#### MST1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      32769   (32768   sysid
1)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Mstr      FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree mst configuration
MVL2(config-mst)#instance 1 priority 4096
```

```
MVL2(config-mst)#end
MVL2#show spanning-tree mst
#### MST1    vlans mapped:22
Bridge      address 0007.70b2.a7c9  priority     4096    (4096    sysid 0)
Regional Root       this switch for the Instance  10
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23        Mstr      FWD 200000    128.123  P2p
```

port 에 관한 설정도 마찬가지로 instance instance-id 가 추가 됩니다.
port 의 priority 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step3	Spanning-tree instance instance-id priority priority	port 에 priority 를 설정합니다
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 값으로 복구하려면 no spanning-tree instance instance-id priority 명령을 사용합니다.

```
MVL2#show spanning-tree mst
#### MST1    vlans mapped:22
Bridge          address 0007.70b2.a7c9  priority     32768   (32768    sysid 0)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23        Mstr      FWD 200000    128.123  P2p

MVL2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree instance 1 priority 0
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree mst
```

```
#### MST1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      4097    (4096    sysid
1)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Mstr      FWD 200000      0.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree instance 1 priority
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree mst
#### MST1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      4097    (4096    sysid
1)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Mstr      FWD 200000    128.123  P2p
```

port 의 path cost 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step3	Spanning-tree instance instance-id path-cost path-cost	port 에 path cost 를 설정합니다
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 값으로 복구하려면 no spanning-tree instance instance-id path-cost 명령을 사용합니다.

```
MVL2#show spanning-tree mst
```

```
#### MST1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      4097    (4096    sysid
1)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Mstr      FWD 200000    128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree instance 1 path-cost 1
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree mst
#### MST1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      4097    (4096    sysid 1)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Mstr      FWD 1         128.123  P2p

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree instance 1 path-cost
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree mst
#### MST1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      4097    (4096    sysid
1)
Regional Root       this switch for the Instance  1
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Mstr      FWD 200000    128.123  P2p
```

Notice

MSTP 에서 instance 와 port 에 설정을 하기 위해서는 instance 생성이 먼저 이루어 저야 합니다.

8.7. Configuring RPVST+ Features

이 절에서는 rapid per vlan spanning-tree plus (RPVST+)를 설정하는 방법에 대해 설명합니다. RPVST+모드의 경우 하나의 VLAN 별로 다른 인스턴스로 spanning-tree 를 구성합니다. 그래서 VLAN 을 생성하고 그 VLAN 에 대한 인스턴스를 만드는 설정이 필요합니다. 또한 port 에 VLAN 을 추가 했을 경우 해당 VLAN 이 RPVST+인스턴스에 등록 되어 있다면 해당 port 에서 그 VLAN 에 대해 자동으로 RPVST+가 동작합니다. RPVST+를 설정하는 방법은 크게 VLAN 생성, 인스턴스 생성, port 에 VLAN 추가, 3 단계로 나눌 수 있습니다. E5224 에서는 VLAN 을 생성하면 자동으로 인스턴스를 생성합니다. 단 32 개의 인스턴스만 허용합니다. 따라서 32 개를 초과한 VLAN 들은 디폴트 인스턴스에 속하게 됩니다. 그 밖에 VLAN 별로 hello time, port priority 등 설정이 있습니다.

8.7.1. VLAN 인스턴스 생성

VLAN 을 생성 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거칩니다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	Spanning-tree rpvst+ configuration	VLAN 를 생성하기 위해 rpvst+ configuration 모드로 진입합니다.
Stpe3	vlan vlan-id	vlan-id 에 해당하는 vlan 을 생성시킵니다
Step4	exit	Global configuration 모드로 진입합니다.
Step5	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step6	Spanning-tree vlan vlan-id	VLAN 에 해당 포트를 넣는다
Step7	end	privileged EXEC 모드로 변경합니다.
Step8	show running-config	설정 내용을 확인합니다.
Step9	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

이때 각각의 port 에 이미 vlan 이 추가 되어 있어야 하며, port 의 mode(access or trunk)와 상관없이 동작합니다.
그리고 생성되어 있는 instance 를 삭제할 경우에는 no vlan vlan-id 명령을 사용하면 됩니다.

```
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree rpvst+ configuration
MVL2(config-rpvst+)#vlan 22
MVL2(config-rpvst+)#end
MVL2#show spanning-tree rpvst+
#### MST1    vlans mapped:22
Bridge          address 0007.70b2.a7c9  priority      32790   (32768    sys-id-ext 22)
Regional Root    address 5835.d97e.a600  priority      4097    (4096    sysid 1)
```

```
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Root      FWD 200000    128.123  P2p
```

8.7.2. Port 에 vlan 추가 및 삭제

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Stpe3	switchport trunk allowed vlan add vlan-id (access port 에서 switchport access vlan vlan-id)	VLAN 에 해당 포트를 넣는다. spanning-tree vlan vlan-id 가 자동으로 등록됩니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show spanning-tree rpvst+	RPVST 설정 내용을 확인합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

```
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/24
MVL2(config-if-Giga0/24)#switchport mode trunk
MVL2(config-if-Giga0/24)#switchport trunk allowed vlan add 22
MVL2(config-if-Giga0/24)#end
MVL2#show spanning-tree rpvst+
#### MST1    vlans mapped:22
Bridge          address 0007.70b2.a7c9  priority      32790   (32768    sys-id-ext 22)
Regional Root   address 5835.d97e.a600  priority      4118    (4096     sysid 22)
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Root      FWD 200000    128.123  P2p
Giga0/24         Desg      FWD 200000    128.122  P2p
```

port 에서 vlan 에 대한 STP 동작 및 중지할 때는 다음과 같습니다.(vlan 에는 계속 포함) 단, spanning-tree vlan vlan-id 가 default 이므로 no spanning-tree vlan vlan-id 만 show run 시 표시됩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Stpe3	spanning-tree vlan vlan-id (no spanning-tree vlan vlan-id)	해당 포트에서 VLAN 에 대한 RPVST+를 동작시킵니다.(또는 중지 시킵니다.) – 단 이 때 vlan 은 포함되어 있습니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

```
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/24
MVL2(config-if-Giga0/24)#no spanning-tree vlan 22
MVL2(config-if-Giga0/24)#end
MVL2#show spanning-tree rpvst+
#### RPVST+ 1    vlans mapped:22
Bridge            address 0007.70b2.a7c9  priority      32790   (32768    sys-id-ext 22)
Regional Root     address 5835.d97e.a600  priority      4118    (4096     sysid 22)
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface         Role    Sts Cost      Prio.Nbr Type
---------------- ---------- --- --------- -------- ----------------------
Giga0/23         Root      FWD 200000    128.123  P2p
```

8.7.3. 다른 모드와 호환을 위한 CIST 동작

RPVST+에서는 다른 모드로 동작하는 스위치와 호환을 위해 CIST 를 동작시킵니다. 이때 CIST 는 mstp 의 그것과 동일합니다. CIST 를 동작시키기 위해서는 VLAN 1 의 인스턴스를 등록해야 합니다. 등록과정은 다른 VLAN 과 동일합니다. 단 vlan 1 은 default vlan 이고 인스턴스로 등록할 경우 특별히 다른 vlan 설정이 되지 않은 port 들은 자동으로 CIST 가 동작합니다. 이 때 CIST 를 VLAN1 에 대한 인스턴스라고 생각하면 됩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	Spanning-tree rpvst+ configuration	VLAN 를 생성하기 위해 rpvst+ configuration 모드로 진입합니다.
Stpe3	vlan 1	vlan 1 에 해당하는 인스턴스를 생성합니다.
Step4	exit	Global configuration 모드로 진입합니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Stpe3	switchport trunk allowed vlan add 1	VLAN1 에 해당 포트를 넣는다. spanning-tree vlan 1 가 자동으로 등록됩니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

```
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree rpvst+ configuration
MVL2(config-rpvst+)#vlan 1
MVL2(config-rpvst+)#exit
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#switchport trunk allowed vlan add 1
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree

Default  Bridge up - Spanning Tree Enabled rpvst+
  Root ID    Priority    4097
             Address     5835d97ea600
             Cost        0
             Port        123 (Giga0/23)
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     000770b2a7c9
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/23      Root FWD 200000    128.123  P2p
```

8.7.4. VLAN and port configuration

RPVST+에서는 각 VLAN 마다 spanning-tree 가 동작하기 때문에 VLAN 별로 priority 를 설정합니다. 여기서 사용되는 명령어 들은 STP, RSTP 에서 사용되는 명령어에 vlan 이 붙어서 사용됩니다.
vlan 에 priority 를 설정하기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거칩니다

Command	Purpose

Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	Spanning-tree vlan vlan-id priority priority	VLAN 에 priority 를 설정합니다
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show running-config	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 값으로 복구하려면 no spanning-tree vlan vlan-id priority 명령을 사용합니다.

```
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 0
% 0: MSTI Root Id 0016000770b2a7c9
% 0: MSTI Bridge Id 0016000770b2a7c9
% Giga0/23: Port Number123 -Ifindex123- Port Id 807b - Role Designated - State Forwarding
%   Giga0/23: Designated Internal Path Cost 0  - Designated Port Id 807b
%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
%   Giga0/23: Designated Root 0016000770b2a7c9
%   Giga0/23: Designated Bridge 0016000770b2a7c9
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#spanning-tree vlan 22 priority 4096
MVL2(config)#end
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 1016000770b2a7c9
%Giga0/23: Port Number123 -Ifindex123 - Port Id 807b - Role Designated - State Forwarding
%   Giga0/23: Designated Internal Path Cost 0  - Designated Port Id 807b
%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
%   Giga0/23: Designated Root 1016000770b2a7c9
%   Giga0/23: Designated Bridge 1016000770b2a7c9
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0%
```

```
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#no spanning-tree vlan 22 priority
MVL2(config)#end
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 44604237 - MSTI Root Port 123 - MSTI Bridge Priority 32768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - State Forwarding
%   Giga0/23: Designated Internal Path Cost 44404237  - Designated Port Id 8017
%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
%   Giga0/23: Designated Root 1016000770b2a7c9
%   Giga0/23: Designated Bridge 10165835d97ea600
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0
```

port 에 관한 설정도 마찬가지로 vlan vlan-id 가 추가 됩니다.

port 의 priority 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step3	Spanning-tree vlan vlan-id priority priority	port 에 priority 를 설정한다(이때 priority 는 4096 배수로 하여야 합니다.)
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 값으로 복구하려면 no spanning-tree vlan vlan-id priority 명령을 사용합니다.

```
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 285627132 - MSTI Root Port 123 - MSTI Bridge Priority 32768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%   Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - State Forwarding
```

```
%   Giga0/23: Designated Internal Path Cost 285427132  - Designated Port Id 8017
%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
%   Giga0/23: Designated Root 1016000770b2a7c9
%   Giga0/23: Designated Bridge 10165835d97ea600
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0shu#configure terminal

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree vlan 22 priority 0
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 336031920 - MSTI Root Port 123 - MSTI Bridge Priority 32768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%   Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - State Forwarding
%   Giga0/23: Designated Internal Path Cost 335831920  - Designated Port Id 8017
%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 0
%   Giga0/23: Designated Root 1016000770b2a7c9
%   Giga0/23: Designated Bridge 10165835d97ea600
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree vlan 22 priority
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 336031920 - MSTI Root Port 123 - MSTI Bridge Priority 32768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%   Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - State Forwarding
%   Giga0/23: Designated Internal Path Cost 335831920  - Designated Port Id 8017
%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
```

```
%  Giga0/23: Designated Root 1016000770b2a7c9
%  Giga0/23: Designated Bridge 10165835d97ea600
%  Giga0/23: Message Age 1 - Max Age 20
%  Giga0/23: Hello Time 2 - Forward Delay 15
%  Giga0/23: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1
```

port 의 path cost 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step3	Spanning-tree vlan vlan-id path-cost path-cost	port 에 path cost 를 설정합니다
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

default 값으로 복구하려면 no spanning-tree vlan vlan-id priority 명령을 사용합니다.

```
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 1182112290 - MSTI Root Port 123 - MSTI Bridge Priority 3
2768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%  Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - Stat
e Forwarding
%  Giga0/23: Designated Internal Path Cost 1181912290  - Designated Port Id 8017

%  Giga0/23: Configured Internal Path Cost 200000
%  Giga0/23: Configured CST External Path cost 200000
%  Giga0/23: CST Priority 128  - MSTI Priority 128
%  Giga0/23: Designated Root 1016000770b2a7c9
%  Giga0/23: Designated Bridge 10165835d97ea600
%  Giga0/23: Message Age 1 - Max Age 20
%  Giga0/23: Hello Time 2 - Forward Delay 15
%  Giga0/23: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0

MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#spanning-tree vlan 22 path-cost 1
```

```
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 1233717192 - MSTI Root Port 123 - MSTI Bridge Priority 3
2768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%   Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - Stat
e Forwarding
%   Giga0/23: Designated Internal Path Cost 1233517192  - Designated Port Id 8017

%   Giga0/23: Configured Internal Path Cost 1
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
%   Giga0/23: Designated Root 1016000770b2a7c9
%   Giga0/23: Designated Bridge 10165835d97ea600
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1
%
MVL2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MVL2(config)#interface GigabitEthernet 0/23
MVL2(config-if-Giga0/23)#no spanning-tree vlan 22 path-cost
MVL2(config-if-Giga0/23)#end
MVL2#show spanning-tree rpvst+ vlan 22
% vlan 22 Instance 1 configured
% 0: MSTI Root Path Cost 1233717192 - MSTI Root Port 123 - MSTI Bridge Priority 3
2768
% 0: MSTI Root Id 1016000770b2a7c9
% 0: MSTI Bridge Id 8016000770b2a7c9
%   Giga0/23: Port Number 123 - Ifindex 123 - Port Id 807b - Role Rootport - Stat
e Forwarding
%   Giga0/23: Designated Internal Path Cost 1233517192  - Designated Port Id 8017

%   Giga0/23: Configured Internal Path Cost 200000
%   Giga0/23: Configured CST External Path cost 200000
%   Giga0/23: CST Priority 128  - MSTI Priority 128
%   Giga0/23: Designated Root 1016000770b2a7c9
%   Giga0/23: Designated Bridge 10165835d97ea600
%   Giga0/23: Message Age 1 - Max Age 20
%   Giga0/23: Hello Time 2 - Forward Delay 15
%   Giga0/23: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1
```

	Notice	RPVST+에서 VLAN 와 port 에 설정을 하기 위해서는 VLAN 생성이 먼저 이루어 저야 합니다.

8.8. Displaying the Spanning-Tree Status

spanning-tree 상태를 조회하려면, 다음 표에 명시된 privileged EXEC 명령 중 하나를 사용하시기 바랍니다.

Command	Purpose
show spanning-tree	전체 인터페이스의 spanning-tree 정보를 출력합니다.
show spanning-tree interface interface-id	특정 인터페이스의 spanning-tree 정보를 출력합니다.
show spanning-tree detail	포트 상태를 자세하게 보여줍니다.

privileged EXEC 명령 show spanning-tree 명령의 다른 키워드에 관한 정보는 command reference를 참고하시기 바랍니다.

```
shu#show spanning-tree

Default  Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID    Priority    32768
             Address     00077074ff01
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec

  Bridge ID  Priority    32768
             Address     00077074ff01
             Hello Time  2  sec  Max Age 20 sec  Foward Delay  15 sec
             Aging Time  300

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Giga0/1     Disb BLK 4         128.611  Shared

shu#show spanning-tree interface gi0/1
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 800000077074ff01
% Default: Bridge Id 800000077074ff01
% Default: last topology change Thu Jan  1 00:00:00 1970
% 0: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970
```

```
% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   Giga0/1: Port 101 - Id 8263 - Role Disabled - State Discarding
%   Giga0/1: Designated Path Cost 0
%   Giga0/1: Configured Path Cost 4  - Add type Explicit ref count 1
%   Giga0/1: Designated Port Id 0 - Priority 128  -
%   Giga0/1: Root 000000077074ff01
%   Giga0/1: Designated Bridge 000000077074ff01
%   Giga0/1: Message Age 0 - Max Age 0
%   Giga0/1: Hello Time 0 - Forward Delay 0
%   Giga0/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   Giga0/1: forward-transitions 0
%   Giga0/1: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   Giga0/1: No portfast configured - Current  portfast off
%   Giga0/1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   Giga0/1: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   Giga0/1: no root guard configured      - Current root guard off
%   Giga0/1: Configured Link Type point-to-point - Current  shared
%
%
shu#show spanning-tree detail

Defaultis executing the  rstp-vlan-bridgecompatible Spanning Tree protocol
  Bridge Identifier has priority 8000 address 00077074ff01
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flagnot set
  Number of topology changes 0 last change occurred Thu Jan  1 00:00:00 1970
  Times:  hold 6, topology change 0, notification 5
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change25, notification 0, aging 300
 Port 611 (Giga0/1)of Default is Discarding
   Port path cost 0 Port priority 128 ,128.611.
   Designated root has priority 1280, address 0007.7074.ff01
   Designated bridge has priority 8000, address 0007.7074.ff01
   Designated port id is 0, designated path cost 4 Hello is not pending
   Number of transitions to forwarding state: 0
   Link type is Shared
   BPDU: sent 0

shu#
```

8.9. Configuring Bridge MAC Forwarding

Layer 2 이더넷(Ethernet) 네트워크가 정상적으로 동작하려면 프레임에 있는 MAC 주소를 MAC address table 에 있는 주소와 비교해서 해당 interface 로 전송해야 합니다. 그러기 위해서는 Bridge 의 MAC address table 이 설정이 되어야 하고 이를 MAC learning 이라 합니다. MAC learning 은 장비에 들어온 프레임을 검사해서 설정하는 동적 방법과 관리자가 직접 입력하는 정적 방법이 있습니다.

MAC learing 을 하기 위해서 Config 모드에서 다음 명령을 수행합니다

Command	Purpose
spanning-tree acquire	Default Bridge 의 MAC learning 을 동적으로 하도록 설정합니다. (default 로 enable 되어있습니다)
no spanning-tree acquire	Default Bridge 의 MAC learning 을 동적으로 하지 않도록 설정합니다.
bridge <1-32> acquire	Default Bridge 가 아닌 Bridge 의 MAC learning 을 동적으로 하도록 설정합니다. (default 로 enable 되어있습니다)
no bridge <1-32> acquire	Default Bridge 가 아닌 Bridge 의 MAC learning 을 동적으로 하지 않도록 설정합니다.
mac-address-table static MAC (forward|discard) IFNAME	해당 Bridge 에 MAC 주소를 IFNAME interface 로 forwarding 하거나 discard 합니다
no mac-address-table static MAC (forward|discard) IFNAME	MAC 주소에 해당하는 forwarding entry 를 삭제 합니다

Default Bridge 가 아닌 경우에는 bridge <1-256> mac-address-table static MAC (forward|discard) IFNAME 명령을 사용합니다.

다음은 정적으로 MAC learing 을 하는 예시입니다.

```
Switch#configure terminal
Switch(config)#mac-address-table static 1111.1111.1111 forward gi0/1
Switch(config)#end
Switch#show mac-address-table

  vlan   mac address     type     fwd          ports
------+---------------+--------+-----+-------------------------
    1  1111.1111.1111    static     1 Gi0/1
Switch(config)#no mac-address-table static 1111.1111.1111 forward gi0/1
Switch(config)#end
Switch#show mac-address-table
  vlan   mac address     type     fwd          ports
------+---------------+--------+-----+-------------------------
No entries present.
```

```
Switch#
```

E5224 Series 는 MAC address table 에서 동적인 entry 와 정적 entry 를 삭제하는 설정을 할 수 있습니다.

Command	Purpose
clear mac-address-table (dynamic|multicast|static)	해당 Bridge 에 정적, 동적, multicast MAC 주소 entry 를 삭제합니다.
clear mac-address-table (static|multicast|dynamic) (address MACADDR | interface IFNAME | vlan Vlan-id)	해당 Bridge 에있는 Vlan 이나 물리적 포트의 정적, 동적, multicast MAC 주소 entry 를 삭제합니다.

Default Bridge 가 아닌 경우에는 clear mac-address-table (dynamic|multicast|static) (address MACADDR | interface IFNAME | vlan Vlan-id) bridge <1-256> 명령을 사용합니다.

다음은 정적 MAC 주소 entry 를 삭제하는 예시입니다.

```
Switch# show mac-address-table

  vlan   mac address     type     fwd          ports
------+---------------+--------+-----+-------------------------
    1  1111.1111.1111    static     1 Gi0/1
Switch# clear mac-address-table static
Switch# show mac-address-table

  vlan   mac address     type     fwd          ports
------+---------------+--------+-----+-------------------------
No entries present.
```

MAC 주소 entry 를 조회 하기 위해 다음과 같은 명령을 Exec 모드에서 수행합니다.

Command	Purpose
show mac-address-table	MAC address table 정보를 보여줍니다.
show mac-address-table (static|dynamic|multicast|) (address MACADDR | interface IFNAME | vlan Vlan-id)	MAC address table 정보를 정적, 동적, multicast, vlan 에 대해서 보여줍니다
show mac-address-table count (vlan vlan-id)	MAC address table 에서 정적 동적 multicast 주소의 개수를 보여줍니다

9

802.1X Port-Based Authentication

이 장에서는 IEEE 802.1X port-based authentication을 위한 설정 방법에 대해 설명합니다.

> **Notice** 이 장에서 사용되는 명령어에 대한 문법과 사용방법에 관한 정보는 command reference 를 참조하시기 바랍니다.

이 장은 다음의 절로 구성됩니다.

- 802.1X 개념
- 802.1X Authentication with Guest VLAN
- 802.1X authentication with Dynamic VLAN Authentication
- 802.1X authentication with Restricted VLAN
- 802.1X authentication with MAC-Authentication Bypass
- 802.1X authentication with Auth-MAC

9.1. Understanding 802.1X

IEEE 802.1X standard 는 client, server-based access control, authentication protocol 을 정의 합니다. 802.1X port-based authentication 은 EAPOL 을 사용하는 인증 방식입니다. Authentication server 는 switch port 에 연결된 각각의 client 들을 authenticate 해주고, 인증에 성공한 port 를 VLAN 에 assign 해줍니다.

Client 가 authenticated 되기 전까지 Extensible Authentication Protocol over LAN (EAPOL) traffic 만 client 와 연결된 port 사이를 오갈 수 있습니다. Authentication 이 success 되었을 경우, 일반 traffic 들을 주고 받을 수 있습니다.

Workstation 과 switch 사이는 EAP 가 EAPOL frame 으로 송수신 되고, switch 와 Authentication server 사이에는 EAP 가 RADIUS packet 으로 encapsulation 되어 송수신 됩니다.

이 절에서는 다음 항목을 설명합니다.

- Understanding 802.1X Device Roles
- 802.1X Port-based Authentication process
- Authentication Initiation and Message Exchange

9.1.1. Understanding 802.1X Device Roles

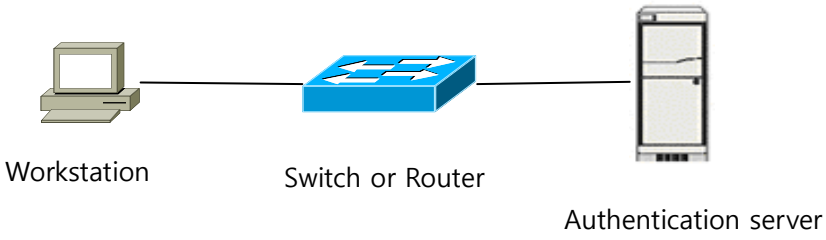


그림 9-1 802.1X Device Role

802.1X port-based authentication 의 device 들은 그림 1 과 같이 구성되어 있습니다.

- Client (supplicant) – workstation 은 LAN 또는 switch services 로의 access request 를 하거나, switch 에서 받은 request 에 대한 response 를 합니다. Workstation 의 경우 802.1X-compliant client software (Microsoft Windows XP operating system 등) 가 서비스 되어있어야 합니다. (IEEE 802.1X standard 에 따르면 client 는 supplicant 로 표현됩니다.)

- Authentication server – client 에 실질적으로 authentication 을 하기 위한 동작을 합니다. Authentication server 는 identity 를 검사하여 client 를 authorized 할 것인지 알려줍니다.

- Switch (authenticator and back-end- authenticator) – switch 는 authentication server 와 client 사이에서 proxy 로 동작합니다. Client 의 identity request 정보를 전송하고 그에 대한 응답을 전송해 줍니다. 또한 Switch 는 RADIUS 의 client 가 되어서 Authentication server 와 통신하기 위해서 EAP frame 들을 encapsulating, decapsulating 하는 역할을 담당합니다.

9.1.2. 802.1X Port-based Authentication process

802.1X port-based authentication 을 enable 하면 다음과 같은 event 가 발생할 수 있습니다.

- client 가 802.1X-compliant client software 를 지원해 주고, client 의 identity 가 valid 한 값인 경우, 802.1X authentication success 가 됩니다.
- 802.1X authentication 이 times out 되면 해당 client 는 Guest VLAN 에 assign 됩니다. (Guest VLAN 설정이 되어 있을 경우에만 assign 됩니다.)
- switch 가 client 로부터 invalid 한 identity 를 받고, Restricted VLAN 이 설정되어 있는 경우, client 는 Restricted VLAN 에 assign 됩니다.

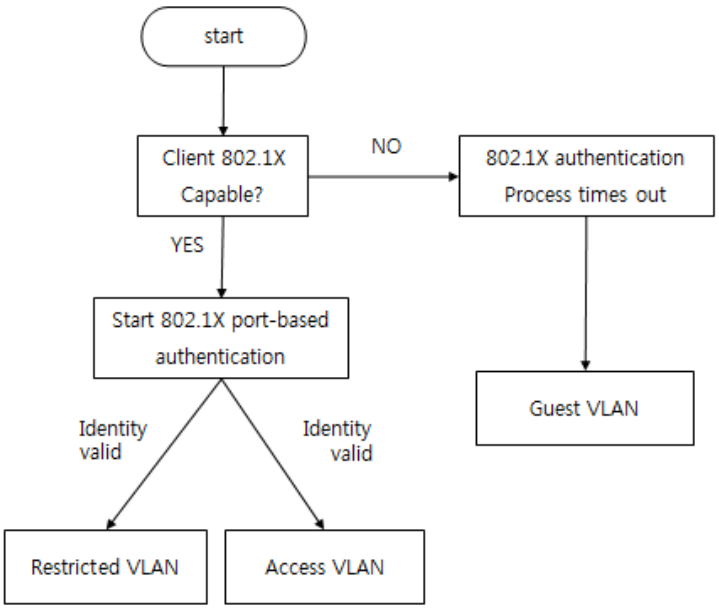


그림 9-2 Authentication flowchart

다음과 같은 상황이 되면 client 는 re authentication 을 진행 됩니다.

- Re-authentication 설정이 되어 있고 re-authentication timer 가 완료 될 경우 진행 됩니다.

9.1.3. Authentication Initiation and Message Exchange

Authentication port-control auto 를 이용하여 port 에 authentication 을 enable 하면, switch 는 link down 에서 up 상태가 되면서 initiate 됩니다. Switch 는 client 에게 EAP-request/identity frame 을 보냅니다. client 에서 이 frame 을 받으면, EAP-response/identity frame 을 보냅니다.

Client 가 switch 로부터 EAP-request/identity frame 을 받지 못하면, client 는 EAPOL-start frame 을 전송하게 됩니다.
Identity 작업이 끝나면 switch 는 authentication server 와 authentication 을 진행 하게 됩니다. Success 일 경우 port 는 authorized 상태가 됩니다. Fail 일 경우 제한된 service 를 제공하기 위한 VLAN 에 assign 되거나, network access 가 거절 됩니다.

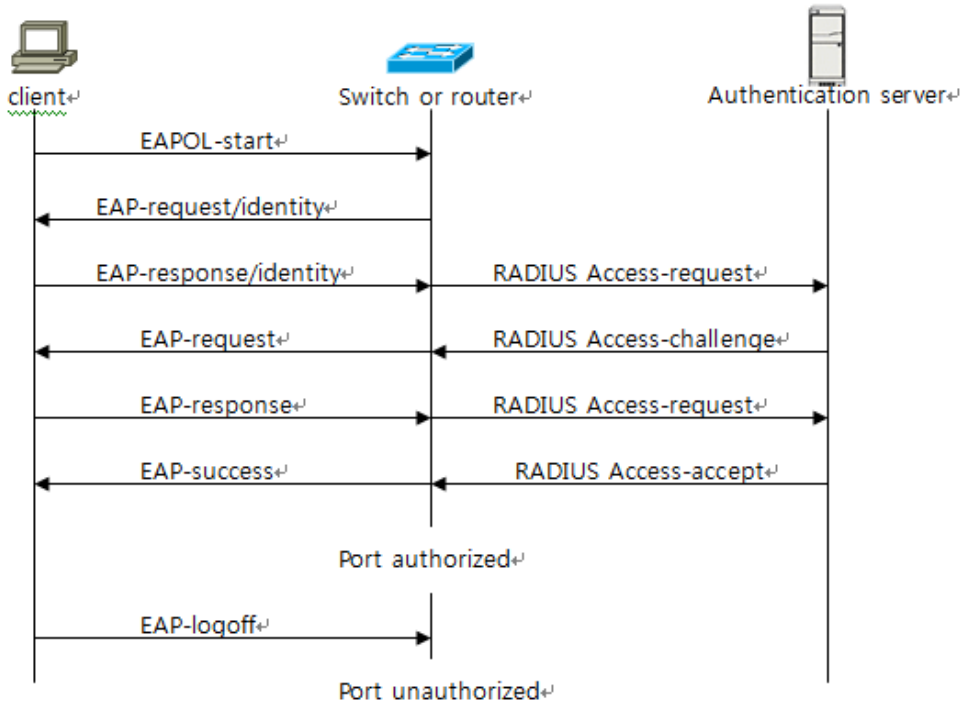


그림 **9-3 Message Exchange**

9.2. configuring 802.1X port-based Authenti-cation

9.2.1. Default 802.1X Authentication Configuration

feature	Default setting
Global 802.1X enable state	Disable
Per-port 802.1X enable state	Disable (force-authorized)
RADIUS server * IP address * authentication port * key	 * None * 1812 * None
Control direction	Bidirectional control
Re-authentication	Disable
Re-authentication attempts	3600 seconds
Quiet period	60 seconds
Server timeout	30 secons
Request period	30 seconds
Guest VLAN	Disable
Restricted VLAN	Disable
Dynamic VLAN assignment	Disable
MAB authentication bypass	Disable
Mac-Based Authentication	Disable

9.2.2. 802.1X Restriction

802.1X 기능을 PC 등의 HOST 에서 사용할 경우 802.1X 기능을 지원해 주는 S/W 가 service 되어야 정상적으로 지원 됩니다. 또한 802.1X 기능을 정상적으로 사용하기 위해서는 최소 하나의 authentication server 가 존재해야 합니다.
802.1X 는 access port 에서만 정상적으로 지원되며, 802.1Q trunk port 에서는 설정이 불가 합니다. 또한 802.1X 는 Port Group 과 함께 사용이 불가 합니다. 현재 802.1X 기능은 single host 로만 지원 합니다.
MAC authentication bypass 는 port security 와 같이 사용이 불가 합니다. 802.1X 와 MAC-Based authentication 기능은 동시에 사용할 수 없습니다. (Dot1X 또는 MAC-Based authentication 중 하나의 인증 방법만 설정 할 수 있습니다.)

기능	사용 가능 여부
HOST MODE	Only single mode
Port type	Only access port
Port Group	사용 불가
Port security	MAC authentication bypass 와 사용 불가
MAC-Based authentication	Dot1X 와 사용 불가

9.2.3. 802.1X port-based authentication enable

802.1X port-based authentication 을 사용하기 위해서는 반드시 authentication server 를 설정해 주어야 합니다. Authentication server 를 다수로 설정 할 수 있습니다. Authentication success 가 될 때까지 authentication server list 를 순차적으로 시도합니다.

Port-control 에서 가능한 모드

Mode	Description
auto	IEEE802.1X authentication 을 port 에 enable 해줍니다.
force-authorized	IEEE802.1X authentication 을 port 에서 disable 해줍니다. Port 는 authentication 과정 없이 authorized 상태가 됩니다.
force-unauthorized	Port 로 진입하는 모든 client 를 deny 합니다. Port 의 상태는 unauthorized 상태가 되고, client 의 authentication 시도를 무시한다. Switch 는 authentication service 를 제공할 수 없습니다.

802.1X 는 access port 에서만 정상적으로 지원됩니다.
802.1X Port-Based authentication 을 설정하려면 다음과 같은 과정을 거치게 됩니다.

	Command	Purpose
Step1	Configure terminal	Global configuration 모드로 진입합니다.
Step2	dot1x system-auth-control	802.1X port-based authentication enable.
Step3	radius-server host ip-address key key	RADIUS server 설정합니다. (RADIUS server address, encryption key)
Step4	interface type slot/port	interface 모드로 진입합니다.
Step5	switchport mode access	access port 로 설정합니다.
Step6	authentication port-control auto	Port 에 authentication 을 enable 합니다.
Step7	end	Privileged EXEC mode 로 돌아갑니다.
Step8	show dot1x all	설정 내용을 확인합니다.

802.1X port-based authentication 을 fastethernet 0/3 에 enable 하는 방법을 설명합니다.

```
Switch (config)# dot1x system-auth-control
Switch (config)# interface fastethernet 0/3
Switch (config-if)# switchport mode access
Switch (config-if)# authentication port-control auto
Switch (config-if)# end
Switch#show dot1x all
802.1X Port-Based Authentication Enabled
Dynamic VLAN Assignment config is Disabled
  RADIUS server address: 10.1.20.7:1812
  Next radius message id: 0
  RADIUS client address: not configured
802.1X info for interface Giga0/3
  Supplicant address: 0000.0000.0000
  portEnabled: false - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  Guest VLAN is not configured
  Restricted VLAN is not configured
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Disconnected - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Invalid - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: both
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

9.3. 802.1X Authentication with Guest VLAN

이 절에서는 Guest VLAN 을 구성하는 방법을 설명합니다:

- Guest VLAN 개념
- Guest VLAN 설정

9.3.1. Guest VLAN 개념

802.1X 를 지원하지 않는 client 에게 한정된 service 를 제공하기 위해서 switch 의 각 port 별로 Guest VLAN 설정을 할 수 있습니다. Guest VLAN 에 assign 되면 802.1X client software 를 다운 받는 등의 한정된 service 를 사용할 수 있게 됩니다.

Guest VLAN 을 802.1X port 에 설정하게 되면, client 가 EAP request/identity frame 에 대한 응답이 없을 경우, client 는 Guest VLAN 에 assign 됩니다.
그리고, switch 는 EAPOL packet history 를 가지고 있게 됩니다. Link 가 살아 있는 동안 interface 에 EAPOL packet 이 들어올 경우, switch 는 802.1X 의 supplicant 로 인지하고, Guest VLAN state 로 변경 되지 않습니다. Interface 의 Link 가 down 되면 가지고 있는 packet history 를 삭제하게 됩니다.

802.1X-incapable client 는 port 를 guest VLAN 에 assign 되도록 하는데, 같은 port 에 802.1X-capable client 가 join 되어 있다면, 이 port 는 unauthorized 상태가 되고, authentication 은 재 시작 됩니다.

Guest VLAN 에 assign 된 경우, HELD state 가 되고 port 는 unauthorized 상태가 되게 됩니다. 이때, Guest VLAN 으로 assign 된 port 는 guest VLAN 설정이 삭제 되거나, interface 가 link down 될 경우에만 Guest VLAN 에서 assign 이 취소됩니다.

9.3.2. Guest VLAN 설정

Guest VLAN 을 설정하기 위해서 아래와 같은 행동을 취합니다.

	Command	Purpose
Step1	interface type slot/port	interface 모드로 진입합니다.
Step2	switchport mode access	access port 로 설정합니다.
Step3	authentication port-control auto	Port 에 authentication 을 enable 합니다.
Step4	authentication event no-response action authorize vlan vlan-id	Guest VLAN 설정을 enable 합니다. 범위 1~4094
Step5	end	Privileged EXEC mode 로 돌아갑니다.
Step5	show dot1x interface type slot/port	설정 내용을 확인합니다.

다음은 VLAN6 을 802.1X guest VLAN 으로 설정하는 방법입니다.

```
Switch (config)# interface fastethernet 0/3
Switch (config-if)# authentication port-control auto
Switch (config-if)# authentication event no-response action authorize vlan 6
```

9.4. 802.1X authentication with Dynamic VLAN Assignment

이 절에서는 Dynamic VLAN Assignment 를 구성하는 방법을 설명합니다:

- Dynamic VLAN Assignment개념
- Dynamic VLAN Assignment설정

9.4.1. Dynamic VLAN Assignment 개념

802.1X authentication 이 success 되면, RADIUS server 는 설정되어 있는 VLAN assignment 를 보내게 됩니다. RADIUS server 는 user-name 과 match 되는 VLAN ID 를 database 에 기억하고 있어서 username 에 해당되는 VLAN 에 client 를 assign 해 주게 됩니다. 이것은 network 에 access 할 수 잇는 user 들을 관리하는 조건이 됩니다.

Dynamic VLAN assignment 가 설정되어 있고, RDIUS server 가 동작한다면 아래와 같은 특징을 보입니다.

- 802.1X 가 enable 되어 있고, RADIUS server 로부터 가져온 값이 모두 valid 하다면, port 는 RADIUS server-assigned VLAN 에 assign 됩니다.
- RADIUS server 로부터 받아온 VLAN 정보가 invalid 하다면, port 의 상태는 unauthorized 가 되고 authentication fail 상태가 됩니다.
- RADIUS server 에서 지정된 VLAN 이 없을 경우 authentication 에 success 하고 access VLAN 에 assign 된다. 모든 통신은 이 access VLAN 을 통해 이루어 집니다.
- 802.1X authentication 이 disable 되면 port 는 access VLAN 으로 돌아갑니다.

Port 가 force-authorized, force-unauthorized, unauthorized 이거나 shutdown 상태이면 port 는 설정되어 있는 access VLAN 에 포함됩니다.

RADIUS server-assigned VLAN 에 할당 된 상태에서 port 의 access VLAN 을 변경하여도 port 의 VLAN 할당 상태에 영향을 주지 않습니다.

9.4.2. Dynamic VLAN Assignment 설정

Dynamic VLAN Assignment 를 사용하기 위해서 아래와 같은 동작을 취합니다.

Step 1

	Command	Purpose
Step1-1	config terminal	Config mode 에 진입한다
Step1-2	aaa authorization network default group radius	RADIUS server 로부터 정보를 가져오기 위해 enable 해준다. (dynamic VLAN assignment enable)

Step 2
802.1X authentication enable
Step 3
RADIUS server 의 attribute 값을 설정 해 준다.

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-ID = VLAN ID

9.5. 802.1X authentication with Restricted VLAN

이 절에서는 Restricted VLAN 을 구성하는 방법을 설명합니다:

- Restricted VLAN개념
- Restricted VLAN설정

9.5.1. Restricted VLAN 개념

Authentication 에 fail 된 client 에게 한정된 service 를 제공하기 위해서 Restricted VLAN 을 설정할 수 있습니다. Authentication 시 invalid 한 값을 이용하여 authentication 을 진행한 경우 EAP-reject 가 된다. 이때 fail 된 supplicant 는 Restricted VLAN 에 assign 됩니다.

Notice

Guest VLAN 과 Restricted VLAN 에 같은 service 를 제공할 것이라면, 같은 VID 에 두 설정을 모두 제공할 수 있습니다.

Port 의 결과가 fail 일 경우 바로 Restricted VLAN 에 assign 되는 것이 아니라 fail count 를 설정 할 수 있습니다. 이 count 는 RADIUS-server 로부터 EAP-reject packet 을 받거나 EAP packet 을 받지 못할 경우 증가 합니다. Count 가 maximum 값이 되면 해당 supplicant 는 Restricted VLAN 에 assign 되고 count 는 다시 0 이 됩니다.

Restricted VLAN 에 assign 되면 switch 는 supplicant 로 EAP success message 를 보내야 합니다. supplicant 에게 notify 를 주지 않으면 supplicant 에서 매 시간 마다 EAP-start message 를 보내서 authentication 을 시도하기 때문입니다.

Restricted VLAN 에 할당된 port 는 다음 re authentication 시도가 있기 전까지 Restricted VLAN 을 유지합니다. 설정된 시간이 지나면 re authentication 을 진행하게 되는데 이때, authentication 에 fail 되면, Restricted VLAN 을 유지하고, success 되면, 설정된 VLAN 에 assign 됩니다.
Re authentication 이 설정 되어 있지 않다면, Restricted VLAN 에서 해제 되는 방법은 link down, 또는 EAP logoff event 를 받았을 경우만 가능합니다.

9.5.2. Restricted VLAN 설정

Restricted VLAN 을 설정하기 위해서 아래와 같은 행동을 취합니다.

	Command	Purpose
Step1	interface type slot/port	interface 모드로 진입합니다.
Step2	switchport mode access	access port 로 설정합니다.
Step3	authentication port-control auto	Port 에 authentication 을 enable 합니다.
Step4	authentication event fail [retry retries] action authorize vlan vlan-id	Restricted VLAN 설정을 enable 합니다. 범위 1~4094 (옵션) authentication 중 Restricted VLAN 으로 assign 되기 전 retry 수를 정해 줄 수 있습니다.
Step5	end	Privileged EXEC mode 로 돌아갑니다.
Step5	show dot1x interface type slot/port	설정 내용을 확인합니다.

Restricted VLAN 설정을 삭제 하면 port 는 unauthorized 상태가 됩니다.

다음은 VLAN 6 을 Restricted VLAN 으로 설정하는 방법입니다.
Switch (config)# interface fastethernet 0/3

Switch (config-if)# authentication port-control auto
Switch (config-if)# authentication event fail action authorize vlan 6

다음은 VLAN 5 를 Restricted VLAN 으로 설정하고 retry 를 2 번으로 설정하는 방법입니다.
Switch (config)# interface fastethernet 0/3
Switch (config-if)# authentication port-control auto
Switch (config-if)# authentication event fail retry 2 action authorize vlan 5

9.6. 802.1X Authentication with MAC-Authentication Bypass

이 절에서는 MAC-Authentication Bypass 방법에 대해 설명합니다.

- MAC-Authentication Bypass 개념
- MAC-Authentication Bypass 설정

(MAC-Authentication bypass 이하 MAB으로 표현)

9.6.1. MAB 개념

switch 에서 supplicant 의 MAC address 를 이용 하여 인증 받는 기능을 이야기 합니다. Printer 등과 같이 802.1X 를 service 할 수 없는 장비가 802.1X port 에 연결되어 있는 경우 사용하게 됩니다.
802.1X 가 EAPOL-response packet 을 기다리다 time out 되면 switch 는 MAC authentication bypass 를 사용하여 인증을 시도하게 됩니다.
MAC authentication bypass 가 802.1X port 에 enable 되어 있으면 supplicant 의 identity 로 MAC address 를 사용하게 됩니다. Authentication server 는 인증해 주고자 하는 MAC address 들을 user-name 으로 등록한 database 를 가지고 있어야 합니다. Switch 는 server 로 MAC address 를 user-name 과 password 로 하여 RADIUS-access/request frame 을 보내게 됩니다. 인증에 성공하게 되면 해당 VLAN 에 access 하게 되고, 인증에 실패하면 Guest VLAN 에 할당 되게 됩니다 (if Guest VLAN configured).
MAB 을 사용하여 인증 중이거나 인증이 완료 된 후에 EAPOL packet 을 받는 다면, 인증을 재 시작 하게 됩니다.
MAB 을 이용하여 authorized 된 port 도 re authentication 을 진행할 수 있습니다. 802.1X 로 인증 받은 port 와 동일한 re authentication process 를 거치게 됩니다. Re authentication 을 진행하는 동안 해당 port 는 이미 assign 된 VLAN 을 유지하게 됩니다. 만약 Re authentication 이 성공하면 port 는 상태를 유지하고, re authentication 이 실패하면 port 는 Guest VLAN 에 assign 됩니다 (If Guest VLAN if configured).

9.6.2. MAB flow

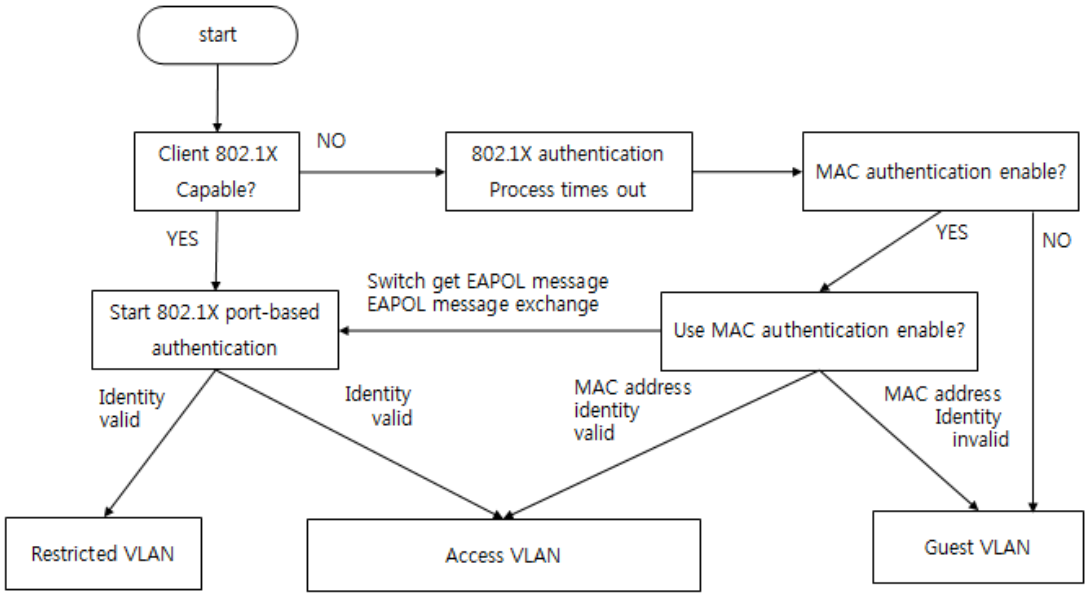


그림 9-4 Authentication Flowchart (MAB)

9.6.3. MAB 설정

MAB 을 설정하기 위해서는 아래와 같은 행동을 취합니다.

	Command	Purpose
Step1	configure terminal	Configure mode 에 진입합니다.
Step2	dot1x system-auth-ctrl	Dot1x global enable.
Step3	interface type slot/port	Interface mode 에 진입합니다.
Step4	authentication port-control auto	Port 에 authentication 을 enable 합니다.
Step5	mab [eap]	MAB enable * eap – RADIUS attribute 값으로 EAP 를 사용합니다.

다음은 interface gi0/5 번에 MAB 을 설정 하는 방법입니다.
Switch (config)# dot1x system-auth-ctrl
Switch (config)# interface gi0/5
Switch (config-if)# authentication port-control auto
Switch (config-if)# mab

다음은 interface gi0/5 번에 MAB with EAP 를 설정 하는 방법입니다.
Switch (config)# dot1x system-auth-ctrl
Switch (config)# interface gi0/5
Switch (config-if)# authentication port-control auto
Switch (config-if)# mab eap

MAB 을 설정을 삭제 하기 위해서는 아래와 같은 행동을 취합니다.

	Command	Purpose
Step1	configure terminal	Configure mode 에 진입합니다.
Step2	dot1x system-auth-ctrl	Dot1x global enable.
Step3	interface type slot/port	Interface mode 에 진입합니다.
Step4	authentication port-control auto	Port 에 authentication 을 enable 합니다.
Step5	no mab [eap]	MAB disable * eap – MAB 설정은 유지하고 EAP 설정만 disable 합니다.

9.7. MAC-Based Authentication

이 절에서는 MAC-Based Authentication 방법에 대해 설명합니다.

- MAC-Based Authentication 개념
- MAC-Based Authentication 설정

9.7.1. MAC-Based Authentication 개념

MAC authentication 은 인증 받고자 하는 supplicant 가 자신의 MAC 정보를 사용하여 인증을 진행하는 방식입니다. Supplicant 의 MAC 주소를 user-name 과 password 로 사용하여 인증을 받게 됩니다. Supplicant 의 MAC 정보를 RADIUS server 가 가지고 있는 경우, 인증에 통과하게 되고, 등록되어 있지 않는 경우 인증에 실패하게 됩니다. 그러므로 RADIUS server 는 인증을 통과 시키고자 하는 MAC 주소를 가지고 있어야 합니다.

Condition for MAC-Based Authentication
Access VLAN port 에서만 지원합니다.
하나의 PC 를 인증 할 수 있습니다.
PC 는 IEEE 802.1X service 를 제공해야 합니다.
Dot1X 기능과 함께 사용할 수 없습니다 (dot1x or MAC authentication).

MAC address Authentication
MAC address 를 이용하여 authentication 을 진행 하면 RADIUS server 가 가진 database 를 사용하게 됩니다. 이 database 는 유효한 user 들을 가지고 있게 됩니다. Interface 에 mac-auth enable 설정이 되면 port 로 들어오는 EAPOL frame 의 source MAC address 는 인증을 위해 RADIUS server 로 보내게 됩니다. 이때 MAC address 를 username 과 password 로 사용하게 되는데, 이 정보가 RADIUS server 에 등록되어 있다면 인증에 통과하게 되고, 아닐 경우에는 인증에 실패하게 됩니다. 인증에 성공하게 되면, MAC address 는 forwarding table 에 forwarding 상태로 등록 되고, 실패할 경우에는 forwarding table 에 discard 상태로 등록되게 됩니다.

9.7.2. MAC-Based Authentication 설정

MAC authentication 을 설정하기 위해서는 아래와 같은 행동을 취합니다.

	Command	Purpose
Step1	configure terminal	Configure mode 에 진입합니다.
Step2	auth-mac system-auth-ctrl	MAC authentication global enable * dot1x 설정이 있는 경우에는 설정 되지 않습니다.
Step3	interface type slot/port	Interface mode 에 진입합니다.
Step4	auth-mac enable	Port 에 MAC authentication 을 enable 합니다. * global 설정이 없는 경우에는 port 별로 enable 이 되지 않습니다.

다음은 interface gi0/5 번에 MAC authentication 을 설정 하는 방법입니다.
Switch (config)# auth-mac system-auth-ctrl
Switch (config)# interface gi0/5
Switch (config-if)# auth-mac enable

MAC authentication 설정을 삭제하기 위해서는 아래와 같은 행동을 취합니다.

	Command	Purpose
Step1	configure terminal	Configure mode 에 진입합니다.
Step2	interface type slot/port	Interface mode 에 진입합니다.
Step3	auth-mac disable	Port 에 MAC authentication 을 disable 합니다.
Step4	exit	Interface mode 에서 configure mode 로 나갑니다.
Step5	no auth-mac system-auth-ctrl	Disable MAC authentication globally

* port 에 MAC authentication enable 설정이 있는 상태에서 global 설정을 삭제하면, port 에 설정된 MAC authentication enable 설정도 함께 삭제 됩니다.

10

Link Aggregation Control Protocol

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

> Notice
> 이 장에서 사용되는 명령어에 대한 문법과 사용방법에 관한 정보는 command reference 를 참조하시기 바랍니다.

이 장은 다음의 절로 구성됩니다:

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

10.1. 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 해줍니다. 상대편 장비와 연결된 interface 에서 서로 LACP 패킷 (LACPDU)을 주고 받으며 해당 interface 가 logical interface 에 포함되는 여부를 판단합니다.

이 절에서는 다음 항목을 설명합니다:

- LACP 동작 원리
- LACP Modes
- LACP Parameters

10.1.1. LACP 동작 원리

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

10.1.2. 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 비교합니다. 다음 표는 LACPDU 에 포함되는 정보들을 나타냅니다.

표 10-1. LACPDU 에 포함되는 정보

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

10.1.3. LACP Modes

E5224 Series 는 port group 을 수동으로 구성할 수 있고, IEEE 802.3ad LACP(Link Aggregation Control Protocol)를 사용하여 자동으로 구성할 수도 있습니다.

LACP 로 port group 을 구성하려면, active 나 passive 모드를 사용하면 됩니다. 적어도 링크의 한쪽은 active 모드로 설정되어 있어야 합니다. Passive 모드의 포트는 LACP 패킷을 먼저 전송하지 않고

LACP 패킷을 수신했을 경우에 LACP 패킷을 전송하기 시작합니다.

LACP 에서 가능한 모드

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

10.1.4. LACP 에 사용되는 정보

LACP 의 설정에 사용되는 인자들은 다음과 같습니다:

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

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

- 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 있습니다.

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

10.2. 802.3ad Link Aggregation Control Protocol and Static Link Aggregation 설정

이 절에서는 LACP 로 port group 을 구성하는 방법을 설명합니다:

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

10.2.1. System Priority 설정

System priority 의 값은 1 과 65535 사이의 정수 값이어야 합니다. 숫자가 클수록 낮은 우선순위를 나타냅니다. default priority 는 32768 입니다.

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

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Step2	lacp system-priority priority	system priority 를 설정합니다.
Step3	end	privileged EXEC 모드로 변경합니다.
Step4	show lacp sys-id	설정 내용을 확인합니다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

설정한 system priority 를 default 설정으로 복구하려면 global configuration 명령 no lacp system-priority 를 사용하시기 바랍니다

다음은 system priority 를 20000 으로 설정하는 방법을 보여줍니다:

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

10.2.2. Port Priority 설정

Port priority 의 값은 1 과 65535 사이의 정수 값이어야 합니다. 숫자가 클수록 낮은 우선순위를 나타냅니다. default priority 는 32768 입니다.

Notice LACP protocol 의 Channel-group 에 속하는 Port 만 Port Priority 설정이 가능합니다.

Port priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.
Stpe2	interface interface-id	LACP 를 port priority 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step3	lacp port-priority priority	port priority 를 설정합니다.
Step4	end	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

설정한 port priority 를 default 설정으로 복구하려면 interface configuration 명령 no lacp port-priority 를 사용하시기 바랍니다

다음은 인터페이스 gi0/1 의 port-priority 를 10 으로 설정하는 예입니다:

```
Switch# configure terminal
Switch(config)# interface Giga0/1
Switch(config-if-Giga0/1)# lacp port-priority 10
Switch(config)# end
```

10.2.3. Timeout Value 설정

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

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

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

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입합니다.

Stpe2	Interface interface-id	LACPDU 전송주기를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입합니다.
Step3	lacp timeout {short|long}	LACPDU 전송주기를 설정합니다.
Step4	End	privileged EXEC 모드로 변경합니다.
Step5	show running-config	설정 내용을 확인합니다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장합니다.

설정한 LACPDU 전송주기를 default 로 복구하려면, interface configuration 명령 no lacp timeout 을 사용하시기 바랍니다.

다음은 인터페이스 gi0/1 과 연결된 상태 시스템의 LACPDU 전송주기를 short 로 설정하는 예입니다:

```
Switch# configure terminal
Switch(config)# interface Giga0/1
Switch(config-if- Giga0/1)# lacp timeout short
Switch(config)# end
```

10.2.4. LACP and static port group 설정

인터페이스에서 LACP 를 설정할 수 있습니다.

LACP 모드를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거칩니다.

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

다음은 인터페이스 Giga0/1 를 port-group 1 의 맴버로 등록 하는 예입니다.

```
Switch# configure terminal
Switch(config)# interface Giga0/1
Switch(config-if- Giga0/1)# channel-group 1 mode active
Switch(config)# end
```

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

```
Switch# configure terminal
Switch(config)# interface Giga0/1
```

```
Switch(config-if- Giga0/1)# channel-group 1 mode on
Switch(config)# end
```

10.2.5. LACP Statistics 삭제

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

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

다음은 port group 1 의 LACP 를 통계정보를 삭제하는 예입니다:

```
Switch# clear lacp 1 counters
```

10.3. 802.3ad 통계 및 상태 표시

E5224 Series 는 모든 포트 그룹에 대한 정보를 확인하는 여러 명령어를 제공합니다.

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
show etherchannel load-balance	Port group 에 적용되는 load balance mode 정보를 제공

다음은 static 한 port group 이 설정된 정보를 확인하는 예입니다

```
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)         -        Gi0/1(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: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1               Mode = On          Gcchange = -
Port-channel  = Port-channel1    GC   = -          Pseudo port-channel= Port-channel1
Port index    = 0               Load = 0xFF
Protocol      = -

Age of the port in the current state: 0d:00h:00m:31s

                Port-channels in the group:
                -----------------------

Port-channel: Port-channel1
-----------------------

Age of the Port-channel = 0d:00h:05m:06s
Number of ports = 1
GC              = 0x00000000   HotStandBy port= null
Port state      = Up Mstr In-Bndl
Protocol        = -

Ports in the Port-channel:
Index   Load      Port         EC state       No of bits
------+------+------------+------------------+-----------
 0      FF         Gi0/1              On   4

Time since last port bundled:    0d:00h:00m:31s    Giga0/1
```

Time since last port un-bundled: 0d:00h:00m:34s Giga0/1

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

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

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

출력 결과물의 항목에 대한 상세정보는 command reference 를 참고하시기 바랍니다.

11

IGMP Snooping

본 장에서는 IGMP Snooping 설정에 대해 설명합니다.

11.1. IGMP Snooping 개요

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

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 해줍니다. IGMP Snooping 은 IGMP 호스트와 멀티캐스트 라우터 사이에서 송수신되는 IGMP 메시지를 snooping 하여, 멀티캐스트 그룹과 VLAN 포트 정보를 수집합니다.

IGMP Snooping 의 절차에 대해서 간략히 설명하면 다음과 같습니다. 특정 멀티캐스트 그룹에 대한 IGMP Join 메시지를 받으면, 해당 IGMP 호스트가 연결된 VLAN 포트를 Multicast Forwarding Table Entry 에 추가합니다. 그 IGMP 호스트로부터 IGMP Leave 메시지를 받으면 반대로 그 IGMP 호스트와 연결된 VLAN 포트를 Multicast Forwarding Table Entry 에서 제거합니다. 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 삭제합니다.

11.2. IGMP Snooping 설정

11.2.1. Enable IGMP Snooping on a VLAN

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

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

```
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#
```

11.2.2. Configure IGMP Snooping Functionality

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

11.2.2.1. 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 됩니다. IGMP Report-suppression 을 Disable 하면, 수신하는 모든 IGMP Report 들을 Multicast Router 로 Forwarding 합니다.

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

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

```
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#
```

11.2.2.2. 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 제거합니다.

IGMP Fast-Leave 기능은 VLAN interface 의 각 포트에 호스트가 하나인 경우에만 사용하여야 합니다. 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 됩니다. 또한, 이 기능은 모든 호스트들이 Leave 메시지가 지원되는 IGMPv2 를 사용하는 경우에만 유효합니다.

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

```
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#
```

11.2.2.3. IGMP Mrouter-Port

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

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

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 전달됩니다.

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

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

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ip igmp snooping mrouter interface gi0/2
Switch(config-if-Vlan22)# end
Switch# show ip igmp snooping mrouter vlan22
VLAN    Interface
22      Giga0/2

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 수행합니다.

명령어	설명

ip igmp snooping mrouter interface *IFNAME* **svlan** <*vlan-id*>	해당 VLAN 에 mrouter port 를 수동으로 설정합니다. IFNAME 은 service VLAN 내의 Member-Port 여야 합니다.
no ip igmp snooping mrouter interface *IFNAME* **svlan** <*vlan-id*>	해당 VLAN 에 설정된 mrouter port 를 해제합니다.

```
Switch#configure terminal
Switch#interface Vlan 200
Switch(config-if-Vlan200)#ip igmp snooping mrouter interface gi0/1 svlan 1200
Switch(config-if-Vlan200)#ip igmp snooping mrouter interface gi0/2 svlan 1200
Switch(config-if-Vlan200)#end
Switch#show ip igmp snooping mrouter vlan200
VLAN     Interface
200      Giga0/1               (Mapped SVLAN1200)
200      Giga0/2               (Mapped SVLAN1200)
```

11.2.2.4. IGMP Access-Group

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

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

```
Switch# configure terminal
Switch(config)# access-list 10 permit 225.1.1.1
Switch(config)# access-list 10 deny any
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip igmp snooping access-group 10
Switch(config-if-Giga0/1)# 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 실행합니다.

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

```
Switch# configure terminal
Switch(config)# access-list 10 permit 225.1.1.1
Switch(config)# access-list 10 deny any
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip igmp snooping access-group 10 vlan 22
Switch(config-if-Giga0/1)# end
Switch#
```

11.2.2.5. IGMP Group-Limit

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

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

```
Switch# configure terminal
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip igmp snooping limit 10
Switch(config-if-Giga0/1)# 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 실행합니다.

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

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip igmp snooping limit 10 vlan 22
Switch(config-if-Giga0/1)# end
Switch#
```

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

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

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

11.2.2.6. IGMP snooping forced-source-ip

IGMP Snooping 동작 시에 Mrouter port 로 전달되는 IGMP Message 에 대하여 Source address 를 지정할 수 있습니다. 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 가능합니다.

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

```
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
```

11.2.2.7. IGMP querier timeout

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

명령어	설명
ip igmp querier-timeout <*60-300*>	해당 VLAN 의 Querier timeout 시간을 설정합니다.
no ip igmp querier-timeout	해당 VLAN 의 Querier timeout 시간을 해제합니다.

```
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
```

11.2.2.8. IGMP Snooping querier

interface 에 가상의 IGMP querier 를 생성하여, 해당 VLAN 의 member port 에 주기적으로 Query 를 전송하는 기능입니다.

IGMP Snooping querier 가 설정되었을 때 다른 장비로부터 Query 를 수신한 경우 IGMP Snooping querier 기능은 일시적으로 중지됩니다.

다른 장비로부터의 Query 로 인해 non-querier 가 된 상태에서 other-querier timeout 시간 동안 다른 Query 를 수신하지 못했다면 다른 querier 의 정보를 삭제하고 IGMP Snooping querier 기능이 다시 시작되어 Query 를 전송하게 됩니다.

또한 snooping querier 가 송신하는 query 의 max-response-time, query-interval, source-ip, version 값을 사용자가 설정할 수 있습니다.

IGMP snooping querier 명령은 interface configuration mode 에서 실행하며, 각 명령에 대한 설명은 아래와 같습니다.

명령어	설명
ip igmp snooping querier	해당 VLAN 에 가상 querier 를 생성합니다.
no ip igmp snooping querier	해당 VLAN 에 가상 querier 를 해제합니다.
ip igmp snooping querier max-response-time *<1-240>*	querier 가 송신하는 query 의 max-response-time 값을 지정합니다.
no igmp snooping querier max-response-time	설정한 query 의 max-response-time 값을 해제하여 default 값(25)으로 돌아갑니다.
ip igmp snooping querier query-interval *<1-18000>*	querier 가 송신하는 query 의 query-interval 값을 지정합니다.
no igmp snooping querier query-interval	설정한 query 의 query-interval 값을 해제하여 default 값(125)으로 돌아갑니다.
ip igmp snooping querier source-ip *<ip-address>*	querier 가 송신하는 query 의 source ip 를 지정합니다.
no ip igmp snooping querier source-ip	설정한 query 의 source ip 를 해제하여 default 값(VLAN IP)으로 돌아갑니다.
ip igmp snooping querier version *<1-2>*	querier 가 송신하는 query 의 version 을 지정합니다.

no ip igmp snooping querier version	설정한 query 의 version 을 해제하여 default 값 (2)으로 돌아갑니다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan 200
Switch(config-if-Vlan200)#ip igmp snooping querier
Switch(config-if-Vlan200)#ip igmp snooping querier source-ip 1.1.1.1
Switch(config-if-Vlan200)#ip igmp snooping querier max-response-time 30
Switch(config-if-Vlan200)#ip igmp snooping querier query-interval 45
Switch(config-if-Vlan200)#ip igmp snooping querier version 1
Switch(config-if-Vlan200)#end
```

11.2.3. Configure IGMP Static Group Functionality

11.2.3.1. IGMP Static Group

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

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

명령어	설명
ip igmp stat ic-group <*group-address*>	<*group-address*>으로 Static Group 을 설정합니다.
ip igmp static-group class-map <*class-map name*>	Static Group 의 Group-address 를 class-map 으로 설정합니다.
ip igmp static-group <*group-address*> **interface** *IFNAME*	Static Group 을 설정합니다. 명시된 interface 로 해당 Multicast Traffic 이 전달됩니다.
no ip igmp static-group <*group-address*>	<*group-address*>으로 Static Group 을 해제합니다.
no ip igmp static-group class-map <*class-map name*>	Static Group 의 Group-address 를 class-map 으로 해제합니다.
no ip igmp static-group <*group-address*> **interface** *IFNAME*	해당 Group 및 interface 의 Static Group 을 해제합니다.

```
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
```

11.2.3.2. multicast-flows class-map

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

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

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

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

```
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
```

11.3. Display System and Network Statistics

표 11-1. IGMP Snooping 관련 모니터링 명령어

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

12

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 설명합니다.

12.1. Information About LLDP

12.1.1. LLDP overview

LLDP (Link Layer Discovery Protocol)는 Layer 2 data-link 계층에서 사용하는 프로토콜로 장비의 정보를 네트워크로 전송합니다. LLDP는 단 방향 프로토콜로서 LLDP가 설정된 장비는 현재 장비의 상태, 인터페이스 상태 그리고 장비의 capability와 같은 정보들을 전송합니다.
LLDP는 네트워크 장비 정보를 수집하기 위해 LLDPDU(LLDP Data Unit)를 사용합니다. LLDPDU는 TLV(Type, Length, Value)들로 구성되어 있습니다. TLV들은 IEEE 802.1AB에 정의되어 있습니다.
LLDPDU에 반드시 포함되어야 하는 세개의 필수 TLV는 아래와 같습니다. 이 세 개의 TLV는 반드시 순서대로 포함되어야 합니다.

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 있습니다.

12.2. LLDP Guidelines and Limitations

LLDP를 설정할 때 유의할 점은 다음과 같습니다::

- ✓ 인터페이스 별로 LLDP 를 활성/비활성 할 수 있습니다.
- ✓ 물리 인터페이스에서만 LLDP 를 지원합니다.
- ✓ L2 인터페이스에만 설정이 가능합니다.

12.3. Default Settings

다음의 표는 default LLDP 설정을 나타냅니다:

Feature	Default Setting
LLDP run	Enable
LLDP receive	Enable
LLDP transmit	Enable
LLDP timer	30 seconds
LLDP TLV	Chassis ID/Port ID/TTL TLV transmit

12.4. Configuring LLDP

LLDP 는 기능을 활성화 시켜준 이후, 인터페이스 에서 활성/비활성 할 수 있습니다.

이 장에서는 다음과 같은 절차를 설명합니다:

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

12.4.1. LLDP global enable or disable

다음은 장비에 LLDP 기능을 활성/비활성 하는 방법을 설명합니다. LLDP 의 인터페이스 상에 LLDP 가 활성화 되어 있어도 다음의 작업을 해주지 않으면 LLDP 의 기능을 사용할 수 없으므로 반드시 설정해 주어야 합니다.

	Command or Action	Purpose
Step 1	**configure terminal** **예제:** Switch# **configure terminal**	Global configure 모드로 진입합니다

Step 2	**lldp run** 예제: Switch(config)# **lldp run**	시스템에서 lldp 기능을 활성화 합니다.
Step 3	**end** 예제: Switch(config-)# **end**	privileged EXEC 모드로 돌아갑니다

12.4.2. LLDP enable or disable

다음은 인터페이스에서 LLDP 기능을 활성/비활성 하는 방법을 설명합니다.

	Command or Action	**Purpose**
Step 1	**configure terminal** 예제: Switch# **configure terminal**	Global configure 모드로 진입합니다
Step 2	**interface** *interface-name* 예제: Switch(config)# **interface gi0/1**	Interface configuration 모드로 진입합니다.
Step 3	**switchport** 예제: Switch(config-if-Gi0/1)# **switchport**	인터페이스를 L2 모드로 설정합니다. **NOTE** 자세한 설정 정보는 “제 03 장 인터페이스 환경 설정” chapter 에서 참고할 수 있습니다
Step 4	**lldp transmit** 예제: Switch(config-if-Giga0/1)# **lldp transmit**	인터페이스에 LLDP 전송을 enable 합니다.
Step 4	**lldp receive** 예제: Switch(config-if-Giga0/1)# **lldp receive**	인터페이스에 LLDP 수신을 enable 합니다.
Step 5	**end** 예제: Switch(config-if-Giga0/1)# **end**	privileged EXEC 모드로 돌아갑니다

12.4.3. Configuring optional LLDP parameters

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

Command or Action	Purpose
configure terminal 예제: Switch# **configure terminal**	Global configure 모드로 진입합니다
lldp timer 예제: Switch(config)# **lldp timer 10**	LLDP Data Unit 전송 주기를 변경합니다. 이 설정으로 LLDP update 정보 주기를 변경할 수 있습니다.
lldp system-name *NAME* 예제: Switch(config)# **lldp system-name LLDP**	LLDP 에서 사용할 system name 을 지정합니다.
interface *interface-name* 예제: Switch(config)# **interface gi0/1**	Interface configuration 모드로 진입합니다.
lldp tlv-select *tlv* 예제: Switch(config-if-Giga0/1)# **lldp tlv-select system-name**	LLDP 로 전송할 TLV 를 선택합니다. **NOTE** lldp 를 enable 하면 default 로 mandatory TLV 인 lldp tlv-select chassis-id port-id ttl 가 설정된다.
end 예제: Switch(config-if-Giga0/1)# **end**	privileged EXEC 모드로 돌아갑니다

12.4.4. Verifying the LLDP configuration

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

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

12.5. LLDP Configuration Samples

다음의 예제는 E5224 series switch 의 LLDP 프레임 전송 주기를 60 초로 변경하고, 인터페이스에 특정 인터페이스에 LLDP 를 비활성화 하는 방법을 보여줍니다.

```
Switch# configure terminal
Switch(config)# lldp timer 60
Swtich(config)# interface gi0/1
Switch(config-if-Giga0/1)#no lldp receive
Switch(config-if-Giga0/1)#no lldp transmit
Switch(config-if-Giga0/1)# exit
```

스위치의 설정을 조회하면 다음과 같습니다.

```
!
lldp timer 60
!
interface Giga0/1
 no lldp receive
 no lldp transmit
!
```

LLDP 가 활성화 되어 있는 인터페이스에 LLDP 설정 정보를 조회하면 결과는 다음과 같습니다.

```
Switch#show lldp interface GigabitEthernet 0/1
Interface Information:  Giga0/1
  Enable (TX/RX): Y/Y
  Port MAC address: 0007.729e.ab17
  Neighbors count: 1
```

Remote LLDP 로부터 수신한 정보를 조회하면 다음과 같습니다.

```
Switch#show lldp neighbor GigabitEthernet 0/2
Remote LLDP Neighbor Information:
  MAC Address: 0007.709e.dfdb
  Chassis IP Address: 192.168.1.203
  TTL: 120 (100 second(s) expired)
  Interface Numbering subtype: 2
    Interface Identification: 104
  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 enabled Capabilities:
Management MAC Address: 0007.709e.dfdb
```

장비와 연동되는 LLDP 의 모든 neighbor 의 목록을 조회하면 다음과 같습니다.

```
Switch#show lldp neighbor
MAC ADDRESS        Local Intf    Hold-time
0007.729e.ab15     Giga0/1       115
0007.729e.ab11     Giga0/3       35

Total entries displayed: 2
```

13 DHCP Relay

13.1. DHCP relay agent 기능 및 설정

13.1.1. DHCP relay agent 개요

- DHCP relay 는 서로다른 subnet 상에 위치한 DHCP client, DHCP server 사이에서 DHCP packet 을 forwarding 해주는 host 입니다. IP 망에서의 일반적인 packet forwarding 과는 달린 relay agent 는 DHCP packet 을 RX 하면 RX 받은 packet 에 몇몇 field 가 추가되거나 변경된 packet 을 생성하여 Forwarding 합니다. DHCP relay agent 는 gateway address 에 값을 기록(DHCP packet 의 giaddr field)하고 relay agent information option (option82)를 DHCP packet 에 삽입하여 server 에 전달하도록 설정할 수 있습니다.

E5224 를 DHCP relay agent 로 설정하면 아래와 같이 DHCP client, DHCP server 간 DHCP packet 을 forwarding 합니다.

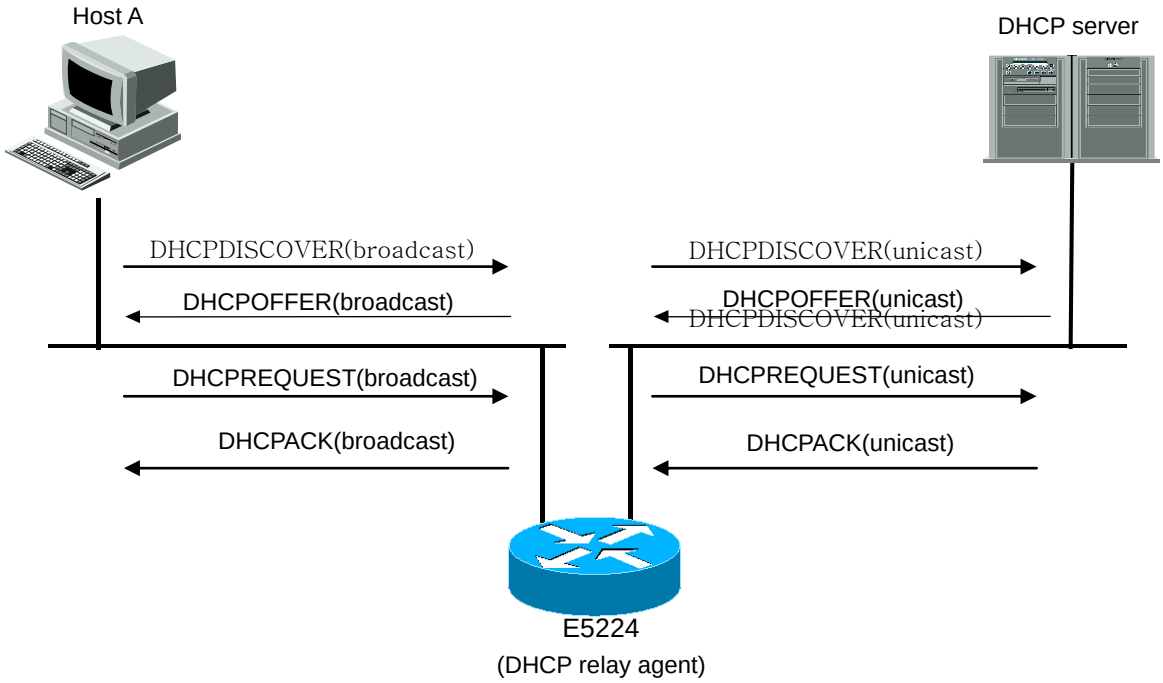


그림 13-1. DHCP relay agent 로서 DHCP server 의 message 전달

1) DHCP client 는 IP 를 요청하기 위해 DHCP DISCOVER message 를 broadcast 로 전송합니다.

2) DHCP relay agent 는 DHCP client 의 IP 요청 message 를 수신하여 DHCP server 에게 해당 message 를 unicast 로 전달합니다.

3) DHCP relay agent 로부터 message 를 수신한 DHCP server 는 client 의 IP address, default gateway 등의 정보를 가진 DHCP OFFER message 를 unicast 로 DHCP relay agent 에게 unicast 로 전송합니다.(이때의 destination IP 로는 giaddr field 에 기록된 IP 를 사용합니다.)

Notice	일반적으로 DHCP server 는 DHCP DISCOVERY/REQUEST message 의 giaddr field 가 설정되어있다면 server 가 가진 address pool 중 giaddr 과 같은 subnet 에 속하는 address pool 에서 IP address 를 선택하여 이를 offer 하거나 할당하는 DHCP OFFER/ACK message 를 relay agent 에게 전송하고 giaddr 에 해당하는 addree pool 이 없는경우 응답하지 않지만 이는 DHCP 의 RFC (RFC 2131)에서 강제 하는 사항은 아닙니다.

4) DHCP relay agent 는 수신한 DHCPOFFER message 를 client 에게 broadcast 로 전송합니다.

5) DHCP server 와 client 사이의 DHCPREQUEST 와 DHCPACK message 도 동일한 과정을 통해 DHCP relay agent 에 의해 전달됩니다.

13.1.2. DHCP relay 기능 활성화

기본적으로 스위치의 DHCP relay agent 는 비활성화 되어 있습니다. global 설정 mode 에서 다음의 명령을 사용하여 DHCP relay agent 를 활성화 할 수 있습니다.

명령	설명
`service dhcp relay`	Switch 의 DHCP relay 기능을 활성화 DHCP relay 기능을 비활성화 하려면, 이 명령의 `no` 형태를 사용

> **Notice** E5224 의 DHCP relay 는 DHCP server 와 같이 설정될 경우의 동작을 보장하지 않습니다. 이는 반대의 경우에도 마찬가지 입니다.

DHCP Relay agent 를 통해서 DHCP packet 을 forwarding 하려면 router 의 switching chip 이 packet 을 forwarding 하지않고 CPU 로 packet 을 trap 해서 relay agent 가 packet 을 처리할 수 있도록 설정할 필요가 있습니다.
다음은 가입자가 Vlan10 에 속한 port 에 연결되어있고 gi1/1 을 통해 DHCP server 가 연결 되어있을때 DHCP relay agent 를 활성화하는 예제입니다.

```
Switch#config terminal
Switch(config)#class-map dhcp_user_class
Switch(config-cmap)#match protocol udp
Switch(config-cmap)#match layer4 source-port 68
Switch(config-cmap)#exit
Switch(config)#class-map dhcp_server_class
Switch(config-cmap)#match protocol udp
Switch(config-cmap)#match layer4 source-port 67
Switch(config-cmap)#end
Switch#show class-map

    CLASS-MAP-NAME: dhcp_user_class (match-all)
      Match Source Port: 68
      Match Protocol: udp

    CLASS-MAP-NAME: dhcp_user_class (match-all)
      Match Source Port: 67
      Match Protocol: udp

Switch#config terminal
Switch(config)#policy-map dhcp_user_map
Switch(config-pmap)#class dhcp_user_class
Switch(config-pmap-c)#trap-cpu
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#policy-map dhcp_server_map
Switch(config-pmap)#class dhcp_user_class
```

```
Switch(config-pmap-c)#trap-cpu
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#int vlan10
Switch(config-if-Vlan10)#service-policy input dhcp_user_map
Switch(config-if-Vlan10)#int gi1/1
Switch(config-if-Giga0/1)service-policy input dhcp_user_map
Switch(config-if-Giga0/1)end
Switch#show policy-map

  POLICY-MAP-NAME: dhcp_user_map
    State: attached

    CLASS-MAP-NAME: dhcp_user_class (match-all)
      Trap-cpu

  POLICY-MAP-NAME: dhcp_server_map
    State: attached

    CLASS-MAP-NAME: dhcp_server_class (match-all)
      Trap-cpu

Switch#show service-policy
 Interface  Giga0/1   : input  dhcp_server_map
 Interface     Vlan10 : input  dhcp_user_map
Switch# configure terminal
Switch(config)# service dhcp relay
Switch(config)# exit
Switch# show ip dhcp relay

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

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

13.1.3. DHCP Relay Agent 에서 DHCP Server 설정

DHCP relay agent 가 작동하기 위해서는 DHCP client 로 부터온 DHCP DISCOVER/REQUEST message 를 forwarding 할 DHCP server 를 설정해야 합니다. relay agent 는 DHCP packet 을 RX 한 interface 별로 forwarding 할 server 를 설정하거나 packet 을 RX 한 interface 에 무관하게 forwarding 할 server 를 설정할 수 있습니다.

DHCP message 를 RX 한 interface 별로 DHCP server 를 설정하려면 다음의 명령을 사용합니다.

명령어	설명
ip dhcp helper-address *address*	interface 에서 RX 한 DHCP DISCOVER/REQUEST message 를 forwarding 할 DHCP server 의 IP address 를 설정 interface 에서 수신한 DHCP packet 만 지정된 server 로 forwarding 함. 설정을 해제하려면 명령의 **no** 형태를 사용

DHCP message 를 RX 한 interface 와 관계없이 DHCP server 를 설정하려면 다음의 명령을 사용합니다.

명령어	설명
ip dhcp-server *address*	DHCP relay agent 가 DHCP DISCOVER/REQUEST message 를 forwarding 할 DHCP server 의 IP address 를 설정 설정을 해제하려면 명령의 **no** 형태를 사용

Notice

E5224 의 DHCP relay Agent 는 helper-address 를 최대 256 개까지 설정 가능합니다.

다음은 DHCP relay agent 에서 server 주소를 지정하는 예제입니다.

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

DHCP relay                    : Enabled
DHCP Smart Relay feature      : Disabled
DHCP Smart Relay retry count  : 3
DHCP server-id based relay    : Disabled
Verification of MAC address   : Enabled
Insertion of option 82        : Disabled
```

```
DHCP Option82 Management-IP    : 0.0.0.0
DHCP maximum hop count         : 10

DHCP helper-address is configured on following servers:
  192.168.0.254

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

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

13.1.4. DHCP Relay Agent Information option(OPTION82) 설정

일반적으로 DHCP protocol 에 의한 IP address 의 할당은 gateway IP address (DHCP packet 의 giaddr field)나 packet 을 RX 한 interface 의 IP address 에 의해 결정되지만 network 구성에 따라 IP 할당이나 가입자별 network 이용정책 설정을 위한 추가적인 정보가 요구되는 경우가 있습니다.
E5224DHCP relay agent 는 client 에서 RX 한 DHCP packet(DHCP DISCOVER/REQUEST message)를 DHCP server 로 forwarding 할 때, packet 을 RX 한 E5224 의 port/Interface 정보를 포함할 수 있도록 relay agent 가 DHCP relay agent information option 을 client 로부터 받은 packet 에 삽입할 수 있는 기능을 제공합니다. server 는 이 정보를 가입자의 IP 할당, 가입자에 대한 access controll 수행, QoS 및 보안정책 설정 등에 이용할 수 있습니다.

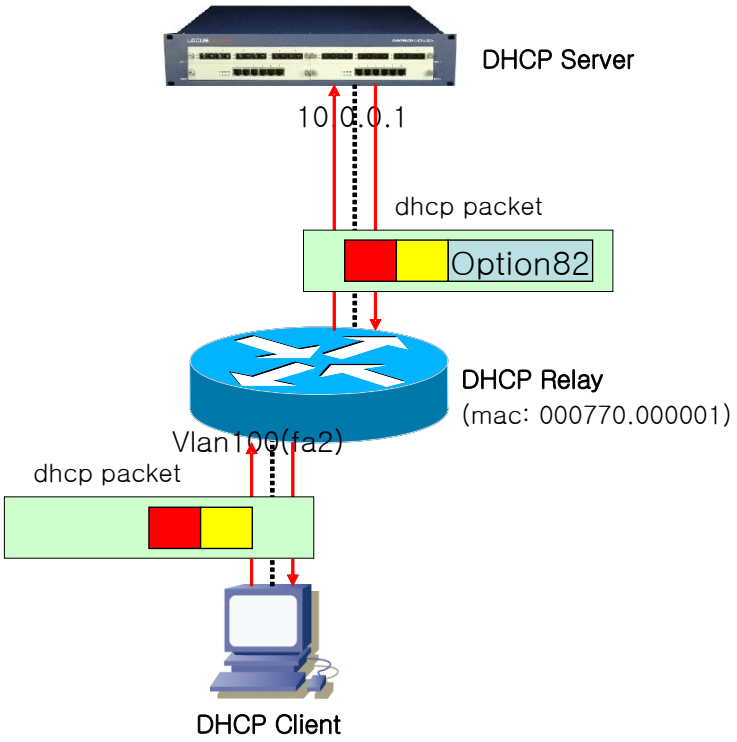


그림 13-2. DHCP Relay Option82

위 그림에서처럼 DHCP relay agent information option 은 DHCP relay agent 와 DHCP server 사이에서만 사용됩니다. relay agent 는 client 가 전송한 packet 을 server 로 forwarding 할 때 DHCP relay agent information option 를 삽입하며, server 가 전송한 packet 을 client 에게 forwarding 할 때 DHCP relay agent information option 를 제거합니다.

DHCP relay agent information option 기능의 활성화

E5224DHCP relay agent 에서 relay agent information option 기능을 활성화시키기 위해서는 다음의 명령을 사용합니다.

명령어	설명
ip dhcp relay agent information option	DHCP relay agent information option 기능을 활성화 기본적으로, 이 특성은 비활성화 되어 있습니다. router 에서 relay agent information option 을 삽입하지 않으려면 이 명령의 no 형식을 사용합니다.

다음은 DHCP relay agent 의 relay agent information option 삽입 기능을 활성화 시키는 예제입니다.

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

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

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

Relay agent information option reforwarding 정책 설정

기본적으로, E5224 의 relay agent information option reforwarding 정책은 DHCP client(또는 DHCP relay agent)로부터 수신한 packet 에 기존의 relay agent information option 이 이미 삽입되어 있는 경우 router 의 relay agent information option 으로 이를 대체합니다. 기본 정책을 변경하기 원한다면, global 설정 mode 에서 다음의 명령을 사용합니다.

명령어	설명
ip dhcp relay agent information option policy {drop|keep|replace}	기본 값은 replace 입니다. drop : relay agent information option 이 삽입되어 있는 packet 은 폐기합니다. keep : 기존의 relay agent information option 을 유지하며, 기존의 relay agent information option 이 없으면 router 의 relay agent information option 을 삽입합니다. replace : 기존의 relay agent information option 을 router 의 relay agent information option 으로 대체합니다. 기본 설정으로 돌아가려면 이 명령의 no 형태를 사용합니다.

다음의 예제는 DHCP Relay Information Option reforwarding 설정을 Drop 으로 설정합니다.

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

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

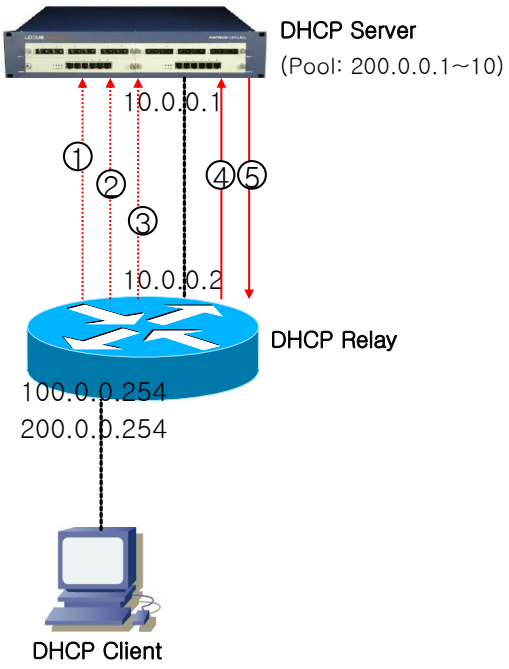
```
DHCP helper-address is configured on following servers:
  192.168.0.254
```

13.1.5. DHCP Smart Relay 설정

E5224DHCP relay agent 는 기본적으로 DHCP client 로 부터 DHCP packet 을 받은 interface 의 primary IP address 를 DHCP packet 의 giaddr field 로 설정하여 DHCP server 로 packet 을 forwarding 합니다.

일반적인 network 구성에서 giaddr field 에 설정된 IP 는 server 가 client 에게 IP address 를 할당하는데 사용할 address pool 을 결정하기 위해 참조되고 server 가 relay agent 로부터 forwarding 받은 packet 에 대한 응답을 전송할 때 destination IP 로 사용됩니다.

smart-relay 기능은 router 가 client 로부터 DHCP packet 을 RX 받은 interface 에 두 개 이상의 IP 가 설정되어 있고 relay agent 가 interface 에 설정된 IP address 중 하나를 사용하여 giaddr field 를 설정하여 server 로 forwarding 한 DHCP DISCOVER/REQUEST message 에 대한 응답이 일정횟수이상 오지않는다면 interface 에 설정된 다른 IP address 를 giaddr field 에 설정하고 DHCP DISCOVER/REQUEST message 를 forwarding 하여 client 가 server 의 다른 address pool 또는 다른 server 를 통해 IP address 를 할당 받을 수 있게 하는 기능입니다



.

그림 13-3. DHCP Smart-Relay 동작 절차

4) client 로부터 DHCP DISCOVER/REQUEST message 를 수신한 relay agent 는 giaddr field 에 DHCP packet 을 RX 한 interface 의 primary IP 인 '100.0.0.254'를 삽입하여 packet 을 server 에게 forwarding 합니다.(1) server 에 설정된 address pool 중 giaddr field 의 IP 와 같은 subnet 상의 address pool 이 없으므로 server 는 relay agent 가 보낸 message 에 응답하지 않습니다.
5) DHCP OFFER/ACK message 를 받지못한 client 는 다시 한번 IP 를 요청합니다. 이 message 를 수신한 relay agent 는 그 client 에서 giadr field 값으로 100.0.0.254 를 사용한 IP 요청 시도횟수를 기억합니다.
6) IP 요청 시도 횟수가 3 회(기본설정) 이상이면 (2) (3)('4' 번 packet), relay agent 는 다음부터는 giaddr 를 '200.0.0.254'로 변경하여 server 로 message 를 forwarding 합니다.(4) server 에 설정된 address pool 중 200.0.0.254 와 같은 network 에 속한 pool 이 있으므로 server 로부터 정상적으로 응답을 받습니다.

Notice	E5224DHCP relay agent 는 smart-relay 에 사용하기 위해 interface 당 최대 500 개의 client 의 IP 요청 시도횟수를 유지하기 위해 내부적인 database 를 사용합니다. 만약 한 interface 상에 IP 할당을 요청했으나 server 로 부터 응답을 받지못한 client 가 500 개 이상 존재한다면 relay agent 는 database 를 삭제합니다.

DHCP smart-relay 를 활성화 하기 위해 아래의 명령을 사용합니다.

명령어	설명
ip dhcp smart-relay	DHCP smart-relay 기능을 활성화 기본적으로, 이 특성은 비활성화 되어 있습니다. 해제하기 위해서는 이 명령의 no 형식을 사용합니다.

DHCP relay agent 가 giaddr field 에 설정할 IP address 를 변경하는 client 의 IP 요청 시도횟수는 아래의 명령어로 설정할 수 있습니다.

명령어	설명
ip dhcp smart-relay retry *<1-10>*	<1-10> giaddr field 에 설정할 IP 를 relay agent 가 변경하는 client 의 IP 요청 시도횟수 기본값은 3 입니다. 기본값으로 돌아가기 위해서는 이 명령의 no 형식을 사용합니다.

다음은 DHCP Smart-Relay 기능을 설정하는 예제입니다.

```
Switch# configure terminal
Switch(config)# ip dhcp smart-relay
Switch(config)# ip dhcp smart-relay retry 5
Switch(config)# exit
Switch# show ip dhcp relay

DHCP relay                      : Enabled
DHCP Smart Relay feature        : Enabled
DHCP Smart Relay retry count    : 5
DHCP server-id based relay      : Disabled
Verification of MAC address     : Enabled
Insertion of option 82          : Enabled
DHCP relay agent information option policy : drop
DHCP Option82 Management-IP     : 0.0.0.0
DHCP maximum hop count          : 10

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

13.1.6. DHCP Relay Agent Verify MAC-Address 설정

DHCP relay agent 는 IP 요청을 시작한 DHCP client 를 인식하기 위한 수단으로 DHCP packet 의 field 중 다음 세가지를 사용합니다.

1) source MAC address
2) client hardware address(chaddr field)
3) client identifier option (option61)

E5224DHCP relay agent 는 악의적인 client 로부터의 IP 할당요청을 막기위해 DHCP DISCOVER message 의 위 세 field 를 검사하여 세 field 가 동일하지 않을 경우 DHCP DISCOVER message 를 server 로 forwarding 하지 않도록 설정할 수 있습니다.

client hardware address 또는 client Identifier option 이 변조된 DHCP DISCOVER message 를 drop 하기 위해 다음 명령어를 사용합니다.

명령어	설명
ip dhcp relay verify mac-address	DHCP DHCP DISCOVER message 의 client hardware address 또는 client Identifier option 이 변조된 경우, 이 message 를 server 로 forwarding 하지 않습니다. 기본적으로, 이 특성은 활성화 되어 있습니다. 비활성화 시키기 위해서는 이 명령어의 no 형식을 사용하면 됩니다.

다음은 DHCP relay agent verify MAC-address 기능 설정을 해제하는 예제입니다.

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

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

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

13.1.7. DHCP Class 기반 DHCP packet forwarding

E5224DHCP relay agent 는 client 로부터 RX 한 DHCP DISCOVER/REQUEST message 에 options 60, 77, 124 또는 125 가 삽입되었다면 (packet 이 수신된 Network/DHCP option/option 값)과 DHCP message 를 RX 한 interface 가 속한 subnet 에 따라 DHCP message 를 forwarding 할 server 를 선택하는 기능을 가지고 있습니다. 이 기능은 ip dhcp-server, ip dhcp helper-address 명령어와 같이 client 로 부터 RX 한 DHCP message 를 어떤 DHCP server 로 forwarding 할지 선택하는 기능입니다.

Notice	E5224DHCP relay agent 는 RX 한 DHCP DISCOVER/REQUEST message 가 relay agent 에 설정된 DHCP class 중 하나로 분류되어 message 를 forwarding 할 DHCP server 를 알게 되면 그 server 로만 message 를 forwarding 하고 ip dhcp-server, ipdhcp helper-address 명령에 의해 지정된 server 로는 message 를 forwarding 하지 않습니다.

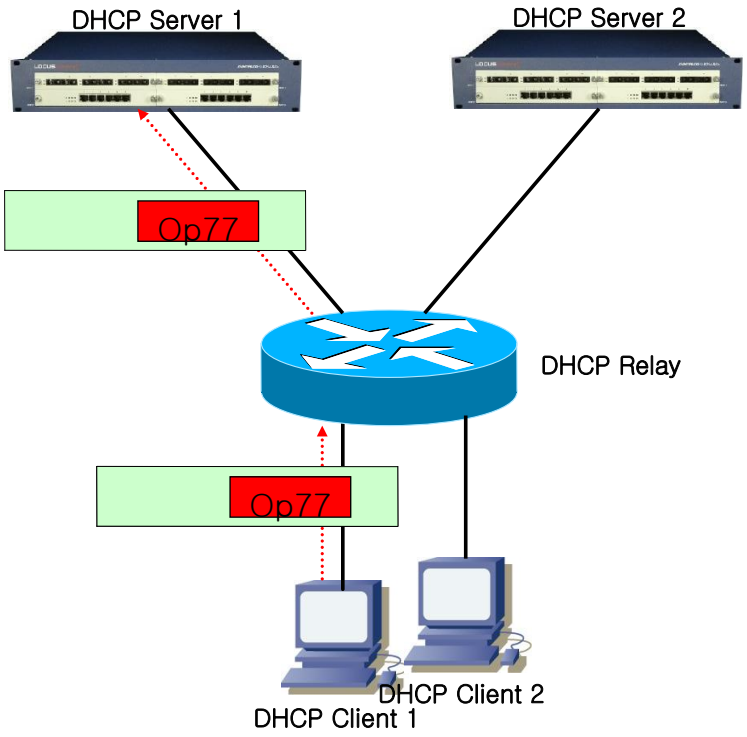


그림 13-4. DHCP Class 기반 DHCP packet Relay

DHCP Class 설정

E5224DHCP relay agent 에서 DHCP class 를 설정하기 위해 다음의 명령어를 사용합니다.

명령어	설명
ip dhcp class *class-name*	DHCP Class Name 지정 "(dhcp-class)#" 로 식별되는 DHCP class 설정 mode 로 진입 class 를 삭제하기 위해서는 이 명령의 no 형식을 사용.
option <*1-255*> **{ascii|hex}** *WORD*	client 가 보낸 DHCP message 가 이 class 로 분류되기위해 가지고 있어야할 option-option value 를 설정합니다. <1-255>: DHCP option 번호 {ascii|hex}: DHCP option 값 형식 (ascii 문자열, hexadecimal) WORD: option 값, Notice: 형식이 hexadecimal 일 경우 반드시 짝수개의 digit 를 사용해야 합니다. EX) ip dhcp option 60 hex 1 -> 설정 안 됨 ip dhcp option 60 hex 01 -> 설정 됨

다음은 DHCP Class "test" 를 설정하는 예제입니다. client 로 부터 RX 된 DHCP DISCOVER/REQUEST message 중 option 77 을 가지고 그 값이 ascii 문자열 77 인 message 는 이 class 로 분류됩니다.

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

DHCP Relay-Pool 설정

E5224DHCP relay agent 의 DHCP relay-pool 은 DHCP client 로 부터 RX 한 DHCP DHCP DISCOVER/REQUEST message 가 분류된 class, message 를 RX 한 interface 가 속한 subnet 을 보고 message 를 forwarding 할 DHCP server 를 선택하는데 사용됩니다. 아래의 명령어를 통해 DHCP relay-pool 을 설정할 수 있습니다.

명령어	설명
ip dhcp relay-pool *WORD*	DHCP relay-pool 을 생성하고 "(dhcp-pool)#" 로 식별되는 DHCP relay-pool 모드로 진입 WORD: relay-pool 의 이름

	relay-pool 을 삭제하려면 이 명령의 no 형식을 사용합니다.
relay source *A.B.C.D/M*	relay-pool 의 subnetwork 를 설정 DHCP DISCOVER/REQUEST message 를 RX 한 interface 가 여기서 지정된 subnetwork 에 속하면 message 가 어떤 DHCP class 로 분류되는지 찾는다. 이 명령의 no 형식을 사용하여 설정을 해제할 수 있습니다.
class *class-name*	이 relay-pool 에 설정된 server 로 message 가 forwarding 되려면 client 가 보낸 DHCP DISCOVER/REQUEST message 가 어떤 DHCP class 로 분류되어야 하는지 설정합니다. 하나이상의 class 를 지정할 수 있으며 해제하려면 이 명령의 no 형식을 사용합니다.
relay target *A.B.C.D/M*	DHCP DISCOVER/REQUEST message 를 forwarding 할 server 를 설정합니다. 이 명령의 no 형식을 사용하여 설정을 해제할 수 있습니다.

이전 예제에나온 “test” DHCP class 를 설정한후 다음 예제에서 나오는 DHCP relay-pool “test-pool”을 설정하면 DHCP relay agent 는 subnetwork ‘100.0.0.0/24’ 에 속한 IP address 를 가진 interface 가 RX 한 DHCP DISCOVER/REQUEST message 중 DHCP Option 77 을 가지고 그 option 값으로 ascii 문자열 “ubiquoss”를 포함한 message 를 DHCP server 200.0.0.254 로 forwarding 합니다.

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

13.2. DHCP Snooping 기능

13.2.1. DHCP Snooping 기능 개요

DHCP snooping 기능 은 DHCP client 와 DHCP server 간에 교환되는 DHCP message 들을 보고 DHCP server 에서 생성되는 것과 유사한 addreess binding table 을 작성합니다. 이 binding table 은 DAI 에서 악의적인 사용자를 차단하기 위해 database 로 사용됩니다. 또한 snoop 은 설정에 따라 client-server 간에 주고받는 message 를 통제할 수 있습니다. snoop 은 DHCP relay agent 와 같이 활성화 될 수 있으며 DHCP server 와는 같이 사용될 수 없습니다.

13.2.1.1. Trust and Untrust Source

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

13.2.1.2. DHCP Snooping Binding Database

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

13.2.1.3. Packet Validation

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

- 스위치가 untrusted interface로부터 source MAC address와 DHCP client Identifier 또는 DHCP client Hardware Address가 일치하지 않는 DHCPDISCOVER packet을 받습니다.

13.2.1.4. Packet Rate-limit

DHCP Snooping 은 동일한 DHCP client 로부터 오는 DHCP Packet 에 대하여 Rate-limit 을 수행합니다. DHCP Snooping 은 기본적으로 동일한 DHCP client 로부터 오는 동일한 타입의 DHCP Packet 을 초당 2 개까지 허용합니다.

13.2.2. DHCP Snooping 기능의 활성화

기본적으로 스위치의 DHCP Snooping 의 기능은 비활성화 되어 있습니다. global 설정 mode 에서 다음의 명령어를 사용하여 DHCP Snooping 기능을 활성화 시킬 수 있습니다.

Notice

DHCP Snooping 을 활성화할때도 relay agent 기능과 마찬가지로 class-map 과 policy-map 설정을 통해 DHCP packet 이 CPU 로 trap 되도록 해야 합니다. 설정방법은 6.2.2 절을 참조하면 됩니다.

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

다음의 예제는 DHCP Snooping 기능을 활성화 하는 예제입니다.

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

13.2.3. DHCP Snooping Vlan 설정

DHCP packet 을 Snooping 할 Vlan 을 설정합니다. 설정된 Vlan 이외의 Vlan 을 통과하는 DHCP packet 은 Snooping 되지 않습니다.

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

Notice

DHCP Snooping 을 DHCP Relay 와 함께 사용할 경우, DHCP Relay 가 packet 을 forwarding 하게 됩니다.

Notice

DHCP Snooping 을 DHCP Relay 와 함께 사용할 경우, DHCP server 와 연결된 vlan, DHCP client 와 연결된 vlan 양 쪽 모두 Snooping vlan 으로 지정해야 합니다.

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

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

13.2.4. DHCP Snooping information option(OPTION82) 설정

DHCP Snooping 은 DHCP client 로부터의 DHCP request 를 Snooping 할 때, DHCP client 가 연결된 Interface 및 장비에 대한 정보를 포함할 수 있도록 DHCP Snooping information option 기능을 제공합니다.

13.2.4.1. DHCP Snooping information option 기능의 활성화

E5224Snooping 에서 information option 기능을 활성화시키기 위해서는 다음의 명령을 사용합니다.

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

다음의 예제는 DHCP Snooping Information Option 기능을 활성화 시킵니다.

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

13.2.4.2. DHCP Snooping information option reforwarding 정책 설정

기본적으로, E5224 스위치의 DHCP Snooping information 정책은 DHCP client 로부터 수신한 packet 내에 information Option 정보가 있으면 packet 을 Drop 시킵니다. E5224 스위치의 기본 정책을 변경하기 원한다면, global 설정 mode 에서 다음의 명령을 사용합니다.

명령어	설명
ip dhcp snooping information policy {drop|keep|replace}	기본 값은 drop 입니다. drop : DHCP Snooping information 이 삽입되어 있는 packet 은 폐기합니다. keep : 기존의 DHCP Snooping information 을 유지합니다. replace : 기존의 DHCP Snooping information 을 Premier router 의 DHCP Snooping information 으로 대체합니다.

다음의 예제는 DHCP Snooping Information Option reforwarding 정책을 Keep 으로 설정합니다.

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

13.2.5. DHCP Snooping Trust Port 설정

네트워크 관리자가 신뢰할 수 있는 포트(ex, DHCP server 방향 포트)는 다음의 명령어를 사용하여 Trust Port 로 설정합니다. Trust Port 를 설정하면 Host 로부터의 Request packet 이 Trust Port 로만 forwarding 됩니다.

명령어	설명
ip dhcp snooping trust	지정된 포트를 Trust Port 로 설정합니다. Trust Port 에서 수신한 DHCP packet 은 Validation check 하지 않습니다. Host 로부터의 Request packet 이 Trust Port 로만 forwarding 됩니다. 기본적으로, 모든 포트는 untrust 포트입니다.

다음은 포트 ‘gi0/1’을 Trust Port 로 설정하는 예제입니다.

```
Switch(config)# interface gi0/1
```

```
Switch(config-if-Giga0/1)# ip dhcp snooping trust
Switch(config-if-Giga0/1)# end
Switch# show ip dhcp snooping interface
Interface           Trust State     Max Entry
---------------     -----------     ------------
Giga0/1             Trusted                 2000
```

13.2.6. DHCP Snooping max-entry 설정

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

명령어	설명
ip dhcp snooping max-entry <*10-10000*>	포트별로 DHCP Snooping max-entry 개수를 설정합니다. 단, Max entry 개수를 초과하여 binding entry 가 생겨도 기존 entry 중 valid(현재 IP 를 사용중인)한 entry 는 삭제하지 않습니다. 기본적으로, 포트별 Max-entry 개수는 2000 개입니다.

다음은 'gi1/1/1'의 DHCP Snooping Max-Entry 를 '100'개로 설정하는 예제입니다.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga0/1)# ip dhcp snooping max-entry 100
Switch(config-if-Giga0/1)# end
Switch# show ip dhcp snooping interface
Interface           Trust State     Max Entry
---------------     -----------     ------------
Giga0/1            Trusted                 100
```

13.2.7. DHCP Snooping Entry Time 설정

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

명령어	설명
ip dhcp snooping entry-time <*5-65535*>	Invalid(IP 를 현재 사용하고 있지 않는)한 DHCP Snooping Binding Entry 를 저장하고 있는 시간을 설정합니다. 단위는 분입니다. 기본적으로, 14400 분(10 일)으로 설정됩니다.

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

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

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

13.2.8. DHCP Snooping Rate-Limit 설정

동일한 DHCP client 로부터 전송되는 DHCP Packet 의 Rate-limit 를 설정하기 위해 다음의 명령어를 사용합니다.

명령어	설명
ip dhcp snooping rate-limit	매 1 초당 동일한 DHCP client 로부터 Packet type 이 같은 DHCP Packet 의 허용 개수를 설정합니다. 기본적으로, 초당 2 개의 packet 을 허용합니다.

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

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

13.2.9. DHCP Snooping Verify MAC-Address 설정

DHCP client Identifier 또는 Client HW Address 가 변조된 경우, 이 packet 을 Drop 시키기 위해 다음 명령어를 사용합니다.

명령어	설명
ip dhcp snooping verify mac-address	DHCP client Identifier 또는 Client HW Address 가 변조된 경우, 이 packet 을 Drop 시킵니다. 기본적으로, 이 특성은 활성화 되어 있습니다.

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

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

13.2.10. DHCP Snooping Manual Binding 설정

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

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

다음은 MAC 이 1111.2222.333 인 가입자가, Vlan 1 의 **gi**1/1/1 포트에 연결되어 IP 100.0.0.10 을 사용하는 예제입니다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping binding 1111.2222.3333 vlan 1 100.0.0.10
interface gi1/1
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
             (H) - Invalid Client HW Address, (R) - Rate Limit Dropped
             (M) - Mac Validation Check Dropped

Mac Address    IP Address        State                Lease(sec) interface
-------------- --------------- -------------------    ---------- ---- ---------
1111.2222.3333 100.0.0.10      Manual               Infinite      Giga0/1
total 4 bindings found
```

13.3. DHCP server 모니터링 및 관리

DHCP server Pool 정보 조회

DHCP server 에 생성된 DHCP Address Pool 정보를 조회하려면, privileged EXEC mode 에서 다음의 명령을 사용합니다.

명령	목적
show ip dhcp pool	DHCP server 의 DHCP Address Pool 정보를 출력
show ip dhcp pool pool [name]	DHCP server 의 Network Pool 내의 정보 출력

DHCP server 바인딩 정보 조회

DHCP server 에서 Client 에게 제공한 Address 의 바인딩 정보를 조회하려면, privileged EXEC mode 에서 다음의 명령을 사용합니다.

명령	목적
show ip dhcp binding	DHCP server 에 생성된 모든 바인딩을 출력
show ip dhcp binding detail	DHCP server 에 생성된 모든 바인딩를 좀 더 상세한 형태로 출력

DHCP server 통계 정보 조회

명령	목적
show ip dhcp server statistics	Server 의 통계와 송수신한 message 와 관련된 카운터 정보를 출력

DHCP server 충돌 정보 조회

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

DHCP server 변수 초기화 명령어

명령어	설명
`clear ip dhcp binding {address|*}`	DHCP 데이터베이스로부터 자동 Address 바인딩을 삭제 *address* 를 명시하면 명시된 IP Address 의 자동 바인딩을, "*"를 사용하면 모든 자동 바인딩을 삭제

`clear ip dhcp server statistics`	DHCP server 의 모든 통계 카운터를 초기화

DHCP server 디버그 명령어

명령어	설명
`debug ip dhcp server on`	DHCP server 의 디버깅 기능을 활성화

13.4. DHCP relay 모니터링 및 관리

표 13-1. DHCP relay 모니터링 및 관리 명령어

명령어	설명
`show ip dhcp helper-address`	DHCP server 의 목록을 출력
`show ip dhcp relay agent information option`	DHCP relay agent information option 의 활성화 및 reforwarding 정책을 출력
`show ip dhcp relay statistics`	relay 의 통계와 송수신한 message 와 관련된 카운터 정보를 출력
`debug ip dhcp relay {events|packets}`	DHCP relay 의 디버깅 기능을 활성화

13.5. DHCP Snooping 모니터링 및 관리

DHCP Snooping 모니터링 및 관리 명령어

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

13.6. DHCP 설정 예제

이 절에서는 다음의 설정 예를 제공합니다.

- DHCP Network Pool 설정 예제
- DHCP Host Pool 설정 예제
- DHCP server 모니터링 및 관리 예제
- DHCP relay agent 설정 예제
- DHCP relay agent 모니터링 및 관리 예제

13.6.1. DHCP Network Pool 설정 예제

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

```
Switch(config)# configure terminal
Switch(config)# ip dhcp pool  marketing
Switch(config-dhcp)# domain-name  ubiquoss.com
Switch(config-dhcp)# lease  1
Switch(config-dhcp)# network  192.168.1.0/24
Switch(config-dhcp)# default-router 192.168.1.1
Switch(config-dhcp)# range 192.168.1.10 192.168.1.100
Switch(config-dhcp)# range 192.168.1.150 192.168.1.230
```

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

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

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

13.6.2. DHCP Host Pool 설정 예제

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

```
Switch(config)# ip dhcp pool mars
Switch(config-dhcp)# default-router  192.168.4.1
Switch(config-dhcp)# dns-server  192.168.4.10
Switch(config-dhcp)# dns-server  192.168.4.11
Switch(config-dhcp)# domain-name  ubiquoss.com
Switch(config-dhcp)# host  192.168.4.114/13
Switch(config-dhcp)# hardware-address  00:01:02:94:77:d7
Switch(config-dhcp)# exit
```

Notice

수동 바인딩으로 설정된 Client 에게는 항상 동일한 IP Address 가 할당됩니다.

13.6.3. DHCP server 모니터링 및 관리 예제

다음은 DHCP server 에 생성된 DHCP Address Pool 정보를 출력하는 예제입니다.

```
shu# show ip dhcp pool
Pool network :
  network: 44.1.1.0/24
  address range(s):
    add: 44.1.1.1 to 44.1.1.200
  lease <days:hours:minutes> <0:0:1>
  no domain is defined
  no dns-servers
  no default-routers

Pool host:
host 3.1.1.1/24
  hardware Ethernet 31:11:11:11:11:11
  no domain is defined
  no dns-servers
  no default-routers
  shu#
```

Notice

show running-config 명령을 사용하면 운영자가 설정한 모든 정보를 볼 수 있습니다.

다음은 DHCP server 가 Client 에게 할당한 IP Address 를 보여주는 예제입니다.

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

다음은 DHCP server 가 Client 에게 할당한 IP Address 를 자세히 보여주는 예제입니다.

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

Lease                   : Infinite
------------------------------------------------------------------------
```

```
TYPE                        : Manual
IP addr                     : 192.168.4.115
HW addr                     : 00:01:02:94:77:d8
Client ID                   : -
Host Name                   : -
Lease                       : Infinite
------------------------------------------------------------------------
TYPE                        : Manual
IP addr                     : 192.168.4.116
HW addr                     : 00:01:02:94:77:d9
Client ID                   : -
Host Name                   : -
Lease                       : Infinite
------------------------------------------------------------------------
total 3 bindings found
```

다음은 Client 에게 이미 바인딩 된 IP Address 를 DHCP server 가 사용할 수 있도록(다른 Client 의 IP Address 로 사용하도록 시도), DHCP server 의 바인딩 정보를 삭제하는 예제입니다..

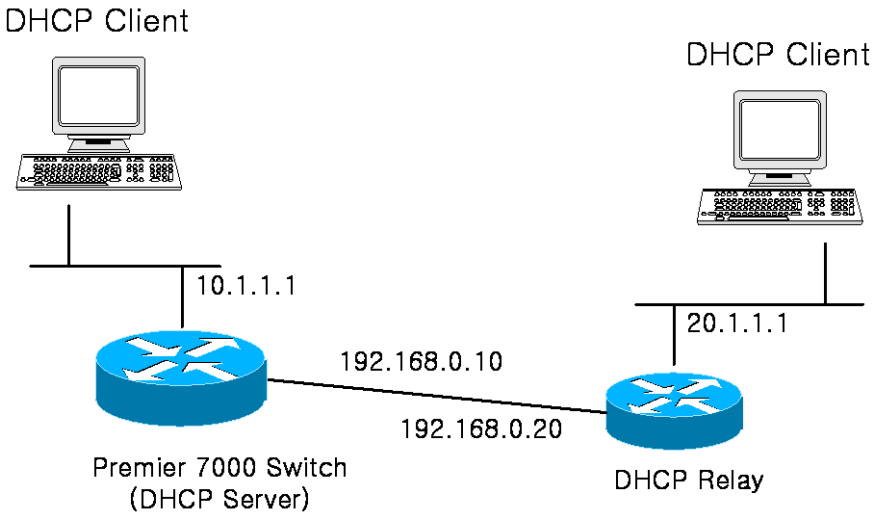
```
Switch(Config)# clear ip dhcp binding 192.168.3.10
Switch(Config)# show ip dhcp binding
IP address         Hardware address      Lease expiration            Type
192.168.4.114     00:01:02:94:77:d7      Infinit                      Maunal
```

다음은 DHCP server 의 통계자료를 보여주는 예제입니다.

```
Switch# show ip dhcp server statistics
Message                                 Received
Malformed messages                      0
BOOTREQUEST                             0
DHCPDISCOVER                            200
DHCPREQUEST                             178
DHCPDECLINE                             0
DHCPRELEASE                             0
DHCPINFORM                              0
ICMPECHO
Message                                 Sent
BOOTREPLY                               0
DHCPOFFER                               190
DHCPACK                                 172
DHCPNAK                                 6
```

13.6.4. DHCP relay agent 설정

다음의 예제는 스위치의 DHCP relay agent 가 Client 의 요구를 전달한 DHCP server 를 설정하는 예제입니다. Client 의 요구를 만족시키는 DHCP Address Pool 이 없을 경우에 스위치는 다른 서브 Network 에 위치한 DHCP server 로 Client 의 요구를 전달합니다.



. 예제 Network – DHCP Relay agent 환경 설정

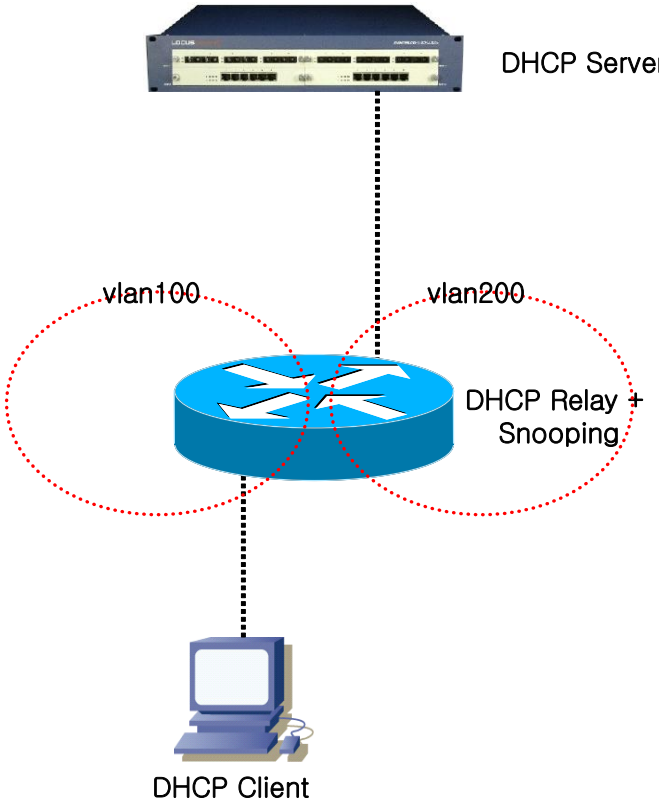
```
Switch(config)# configure terminal
Switch(config)# ip dhcp-server 10.1.1.2
Switch(config)# service dhcp relay
Switch (config)# end
Switch# show ip dhcp helper-address
Server's  IP address : 10.1.1.2
Switch #
Switch # show ip dhcp relay statistics

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

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

Notice 다른 서브 Network 에 위치한 DHCP server 로 DHCP message 를 전달하려면, 해당 Network 에 대한 라우팅 경로 정보가 설정되어 있어야 합니다.

Client-packets relayed	DHCP client 가 TX 한 packet 을 DHCP server 로 forwarding 하는데 성공함
Client-packets errored	DHCP client 가 TX 한 packet 을 DHCP server 로 forwarding 하는데 실패함
Server-packets relayed	DHCP server 가 TX 한 packet 을 DHCP client 로 forwarding 하는데 성공함
Server-packets errored	DHCP server 가 TX 한 packet 을 DHCP client 로 forwarding 하는데 실패함
Giaddr errored	DHCP server 로부터 RX 한 DHCP Packet 에 giaddr 가 없음
Corrupt agent options	DHCP relay agent또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP server로부터 RX 한 DHCP packet의 Option82 정보에 오류가 있음(DHCP Option82의 Length field값과 실제 DHCP Option82 Length 가 서로 다름)
Missing agent options	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP server로부터 RX 한 DHCP packet에 Option82 정보가 없음
Bad circuit id	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP server로부터 RX 한 DHCP packet Option82 정보 중 circuit id(가입자 Interface 정보)에 오류가 있음 (DHCP packet에 있는 option82 의 circuit id를 통해 장비에서 circuit id에 해당하는 port를 찾을수 없음.)
Missing circuit id	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP relay(snoop)은 이전에 DHCP Request packet을 받았을 때 RX한 port에 해당하는 circuit id를 buffering하는데 이 buffer에 없는 circuit id를 포함한 DHCP packet을 DHCP server로부터 받음.

13.6.5. DHCP Snooping 설정 예제

다음 예제는 DHCP Server 와 DHCP Client 사이에 위치한 E5224 를 DHCP Snoop 으로 사용한 예제입니다. Premier 8700 DHCP Snoop 은 Switch 를 통하는 DHCP 패킷을 Snooping 하여 DHCP Snooping Binding Entry 를 생성합니다. 예제 화면은 gi1/1/1 port 에 물린 DHCP Client(0000.864a.c185)가 DHCP Server 100.0.0.254 로 DHCP Request 패킷을 보내 IP 100.0.0.100 을 받은 것을 보여줍니다.




```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 100
Switch(config)# ip dhcp snooping vlan 200
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp-server 100.0.0.254
Switch(config)# service dhcp relay
Switch# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
             (H) - Invalid Client HW Address, (D) - Rate Limit Dropped

   MacAddress       IpAddress        State       Lease(sec)     VlanId      Port
   -----------      ---------       -------      ---------     ------      ----
 0000.864a.c185    100.0.0.100       Ack            87           100     Giga0/1
```

14 Dynamic ARP Inspection

문서버전 History
E52-DAI-2
마지막 수정 날짜: 2012-02-22
적용가능 장비: E5224 Series

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

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

이 장은 다음과 같은 내용으로 이루어져 있습니다:

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

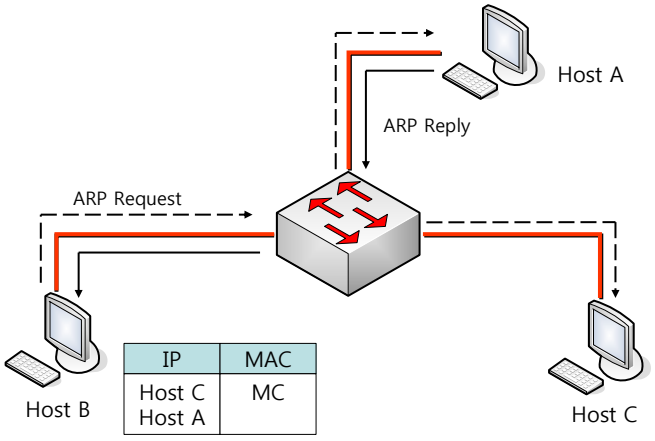
14.1. Understanding DAI

이 절에서는 DAI 에 대한 설명과 DAI 기능을 사용해서 ARP spoofing 공격 [attack] 을 방어하는 방법에 대해 설명합니다. 이 절은 다음과 같은 내용으로 이루어져 있습니다:

- Understanding ARP
- Understanding ARP Spoofing Attacks
- Understanding DAI and ARP Spoofing Attacks
- Interface Trust States and Network Security
- Rate Limiting of ARP Packets
- Relative Priority of ARP ACLs and DHCP Snooping Entries
- Logging of Dropped Packets

14.1.1. Understanding ARP

ARP 는 IP 주소와 MAC 주소를 매핑 mapping 해서 Layer 2 브로드캐스트 broadcast 도메인에서 IP 통신이 가능하게 합니다. 예를 들어, 호스트 B 가 호스트 A 로 정보를 전송하려고 하는데 호스트 B 의 ARP 테이블에 호스트 A 에 대한 MAC 주소가 등록되어 있지 않다고 가정합니다.

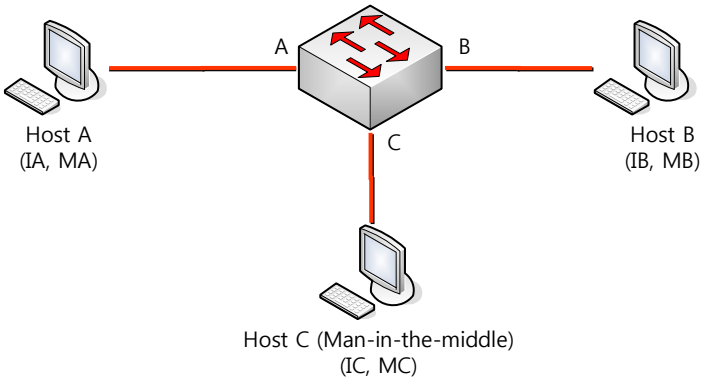


호스트 B 는 호스트 A 의 IP 주소에 대응하는 MAC 주소를 알아내기 위해서, 브로드캐스트 도메인 내부의 모든 호스트들에게 브로드캐스트 메시지 (ARP request)를 전송합니다. 브로드캐스트 도메인 내부의 모든 호스트들은 호스트 B 가 전송한 ARP request 를 수신하고, 호스트 A 는 자신의 MAC 주소를 응답합니다.

14.1.2. Understanding ARP Spoofing Attacks

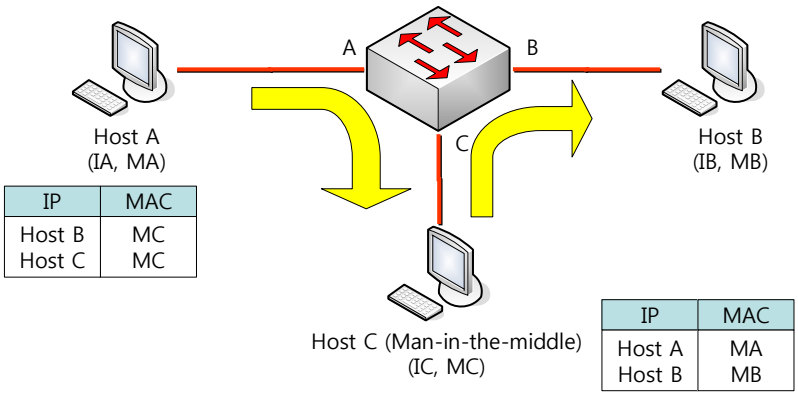
ARP 는 ARP request 를 수신하지 않은 호스트가 전송한 gratuitous reply 로 ARP 테이블이 변경되는 것을 허용합니다. 이로 인해 ARP spoofing 공격과 ARP cache poisoning 이 발생할 수 있습니다. 공격 이후에는 공격 당한 장비의 모든 트래픽은 공격자의 컴퓨터를 통해 라우터, 스위치 또는 호스트로 전달됩니다.

ARP spoofing 공격은 Layer 2 네트워크에 연결된 호스트, 스위치, 라우터의 ARP 캐시 cache 을 조작합니다. 그리고 다른 호스트로 전달되어야 할 트래픽을 가로챈다. 다음의 그림은 ARP cache poisoning 의 예를 보여줍니다.



호스트 A, B, C 는 각각 스위치의 인터페이스 A, B, C 에 연결되어 있으며, 모두 같은 서브넷에 위치합니다. IP 주소와 MAC 주소를 괄호 안에 나타내었다: 예를 들어, 호스트 A 는 IP 주소 IA 와 MAC 주소 MA 를 사용합니다. 호스트 A 가 IP 계층에서 호스트 B 와 통신할 필요가 있을 때, IP 주소 IB 와 연관된 MAC 주소를 알기 위해 ARP request 를 브로드캐스트로 전송합니다. 스위치와 호스트 B 는 이 ARP request 를 수신하면, IP 주소 IA 와 MAC 주소 MA 를 가진 호스트의 ARP 캐시를 갱신합니다: 예를 들어, IP 주소 IA 는 MAC 주소 MA 에 매핑되어 있습니다. 호스트 B 가 응답하면, 스위치와 호스트 A 는 IP 주소 IB 와 MAC 주소 MB 를 가진 호스트의 ARP 캐시를 갱신합니다.

호스트 C 는 IP 주소 IA (또는 IB)에 대한 MAC 주소로 MC 를 사용하는 ARP response 를 브로드캐스트함으로써 스위치, 호스트 A, 호스트 B 의 ARP 캐시를 오염시킬 수 있습니다. ARP 캐시가 오염된 호스트들은 IA 또는 IB 로 향하는 트래픽의 목적지 MAC 주소로 MC 를 사용하게 됩니다. 이것은 호스트 C 가 트래픽을 가로챈다는 것을 의미합니다. 호스트 C 는 IA, IB 와 연관된 진짜 MAC 주소를 알고 있기 때문에, 올바른 MAC 주소를 목적지 MAC 주소로 사용해서 가로챈 트래픽을 원래 호스트들에게로 포워딩 [forwarding] 합니다. 호스트 C 는 호스트 A 와 호스트 B 의 트래픽 사이에 자신을 집어 넣게 되고, 이런 형상을 *man-in-the middle* attack 이라 합니다.



14.1.3. Understanding DAI and ARP Spoofing Attacks

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

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

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

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

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

ARP 패킷을 수신한 인터페이스의 특성에 따라 스위치는 다음과 같이 동작합니다:

- trusted 인터페이스로 수신한 ARP 패킷은 검사하지 않습니다.
- untrusted 인터페이스에 대해서는 오직 유효한 패킷만 허용합니다.

DAI 는 정적으로 할당된 IP 주소를 가진 호스트에 대해서는 운용자가 정의한 ARP access control lists (ACLs)를 사용할 수도 있습니다. 스위치는 폐기된 패킷에 대해 로그를 남길 수도 있습니다.

또한 다음과 같은 경우 DAI 가 ARP 패킷을 폐기하도록 설정할 수도 있습니다:

- 패킷의 IP 주소가 유효하지 않습니다 – 예를 들어, 0.0.0.0, 255.255.255.255 또는 IP 멀티캐스트 주소.
- ARP 패킷의 body 에 포함된 MAC 주소와 Ethernet 헤더의 주소가 일치하지 않습니다.

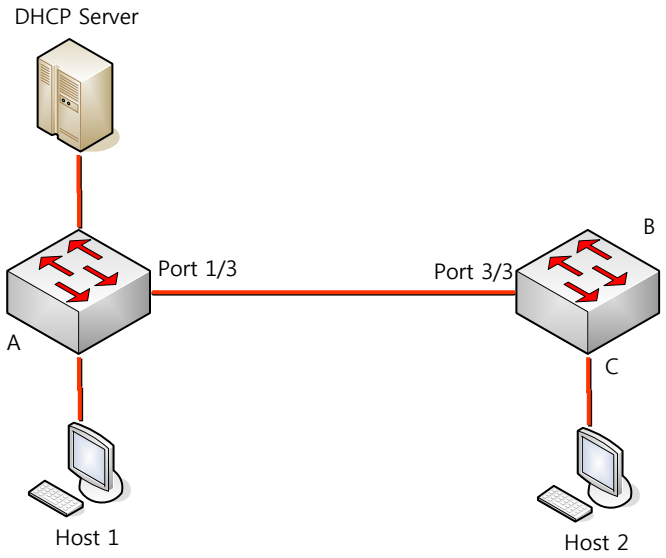
14.1.4. Interface Trust States and Network Security

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

전형적인 네트워크 구성에서, 호스트와 연결된 스위치 포트를 untrusted 로 설정하고 스위치에 연결된 포트는 trusted 로 설정합니다. 이런 설정에서, 이 스위치를 통해 네트워크로 유입되는 모든 ARP 패킷은 보안검사를 받게 됩니다. VLAN 이나 네트워크의 다른 장소에서 더 이상의 유효성 검사가 필요하지는 않습니다. trust 설정은 인터페이스 설정 명령인 **ip arp inspection trust** 를 사용하면 됩니다.

Warning	네트워크 보안을 위해 스위치가 모든 ARP 패킷을 검사하도록 하려면, 특별한 기능이 필요합니다. 즉, DAI 가 스위치의 포워딩 엔진 forwarding engine 을 통해 포워딩되는 유니캐스트 ARP 패킷도 검사할 수 있도록 스위치의 CPU 로 trap 할 수 있어야 합니다. 유니캐스트 ARP 패킷을 검사하도록 설정하는 방법은 19.4.1 절에서 설명하도록 하겠습니다.

다음 그림에서 스위치 A 와 스위치 B 에서 호스트 1 과 호스트 2 를 포함하는 VLAN 에 대해 DAI 가 실행 중이라고 가정합니다. 호스트 1 과 호스트 2 가 스위치 A 와 연결된 DHCP 서버 server 로부터 IP 주소를 할당 받았다면, 오직 스위치 A 는 호스트 1 에 대한 IP-to-MAC 주소 매핑을 가지고 있습니다. 그러므로, 스위치 A 와 스위치 B 사이의 인터페이스가 untrusted 라면, 호스트 1 이 전송한 ARP 패킷은 스위치 B 에서 폐기됩니다. 즉, 호스트 1 과 호스트 2 는 통신을 할 수 없게 됩니다.



인터페이스를 trusted 로 설정했을 때, 신뢰할 수 없는 장비가 존재한다면 네트워크 보안에 허점이 발생합니다. 스위치 A 에서 DAI 를 실행하고 있지 않으면, 호스트 1 은 스위치 B (그리고 스위치 사이의 인터페이스가 trusted 로 설정되어 있다면 호스트 2 까지)의 ARP 캐시를 오염시킬 수 있습니다. 이런 현상은 스위치 B 에서 DAI 를 실행시키더라도 발생합니다.

DAI 가 실행중인 스위치는 연결된 호스트가 네트워크의 다른 호스트들의 ARP 캐시를 오염시키는 행위를 방지합니다. 그러나, DAI 는 DAI 가 실행중인 다른 네트워크의 호스트의 ARP 캐시를 오염시키는 것을 방지하지는 못합니다.

이 경우에 DAI 를 실행중인 스위치에서는 DAI 를 실행시키지 않는 스위치와 연결된 인터페이스를 untrusted 로 설정하십시오. 그리고 DAI 가 설정되지 않는 스위치로부터의 packet 을 검사하기 위해 DAI 를 실행중인 스위치에서 ARP ACLs 를 설정하십시오. 이런 설정이 불가능하다면, Layer 3 에서 DAI 를 사용중인 스위치와 사용하지 않는 스위치를 분리해야 합니다.

Notice	E5224 Series 는 DAI 가 모든 ARP 패킷을 검사하는 네트워크를 보호 기능을 제공합니다.

14.1.5. Rate Limiting of ARP Packets

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

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

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

14.1.6. Relative Priority of ARP ACLs and DHCP Snooping Entries

DAI 는 IP-to-MAC 주소 매핑을 검사할 때, DHCP snooping binding 데이터베이스를 사용합니다.

ARP ACLs 은 DHCP snooping binding 데이터베이스보다 먼저 검사에 사용됩니다. 스위치는 **ip arp inspection filter** 명령으로 설정이 되었을 경우에만 ACLs 을 사용합니다. 스위치는 먼저 사용자가 설정한 ARP ACLs 로 ARP 패킷을 검사합니다. 만약 ARP 패킷이 ARP ACLs 의 deny 조건과 일치하면, DHCP snooping 에 의해 유효한 binding 이 존재하더라도 그 패킷은 폐기됩니다.

14.1.7. Logging of Dropped Packets

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성합니다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제됩니다. 각각의 로그에는 flow 정보 (수신한 VLAN, port 번호, source 와 destination IP 주소, source 와 destination MAC 주소)가 포함됩니다.

Global 설정 명령 **ip arp inspection log-buffer** 로 버퍼의 크기를 설정할 수 있으며, 단위 시간 동안 필요한 로그의 개수를 설정해서 시스템 메시지의 생성 량을 조절할 수 있습니다. 그리고, Global 설정 명령 **ip arp inspection vlan logging** 으로 로그할 패킷의 종류를 지정할 수도 있습니다.

14.2. Default DAI Configuration

다음의 표는 default DAI 설정을 보여줍니다.

Feature	Default Setting
DAI	모든 VLAN 에 대해 비활성 상태입니다.
Interface trust state	모든 인터페이스들은 untrusted 상태입니다.
Rate limit of incoming ARP packets	초당 15 개의 새로운 호스트가 등록되는 Layer 2 네트워크라 가정하고, untrusted 인터페이스 에 대해 15 pps 로 설정됩니다. Trusted 인터페이스에 대해서는 rate 를 제한하지 않습니다. burst interval 은 1 초입니다. 인터페이스의 rate limit 기능은 disable 되어 있습니다.
ARP ACLs for non-DHCP environments	ARP ACLs 은 정의되어 있지 않습니다.
Validation checks	어떤 검사도 수행하지 않습니다.
Log buffer	DAI 가 활성화되면, deny 되거나 drop 되는 모든 ARP 패킷 정보가 로깅됩니다. log entry 의 개수는 32 개. 생성되는 시스템 메시지의 개수는 초당 5 개. logging-rate 주기는 1 초.
Per-VLAN logging	deny 되거나 drop 되는 모든 ARP 패킷이 로깅됩니다.

14.3. DAI Configuration Guidelines and Restrictions

DAI를 설정할 때, 다음의 사항을 준수하십시오:

- ✓ DAI는 기본적으로 스위치 자신의 ARP 테이블만 보호합니다. 네트워크를 보호하기 위해서는 모든 ARP 패킷을 CPU로 trap할 수 있는 기능이 필요합니다.
- ✓ DAI는 입구 보안[ingress security] 기능입니다; 출구 검사[egress check]에 사용하지 마십시오.
- ✓ DAI는 DAI를 지원하지 않는 스위치에 연결된 호스트에 대해서는 효과적이지 않습니다. man-in-the-middle attack은 단일 Layer 2 브로드캐스트 도메인에 제한되기 때문에, DAI를 사용하는 도메인을 그렇지 않은 도메인으로부터 분리하십시오. 이것은 DAI가 활성화된 도메인에 위치한 호스트의 ARP 테이블을 보호해줍니다.
- ✓ DAI는 유입된 ARP request와 ARP response 패킷의 IP-to-MAC 주소 binding을 검사하기 위해 DHCP snooping binding 데이터베이스를 사용합니다. 동적으로 할당되는 IP 주소에 대한 ARP 패킷을 허용하기 위해서는 반드시 DHCP snooping을 활성하십시오.
- ✓ DHCP snooping이 비활성 상태이거나 DHCP 환경이 아니라면, 패킷을 permit하거나 deny하기 위해 ARP ACL을 사용하십시오.
- ✓ 포트의 특성을 고려해서 ARP 패킷의 rate를 설정하십시오.

14.4. Configuring DAI

이 절에서는 DAI 를 설정하는 방법에 대해 설명합니다:

- Enabling DAI on VLANs (필수)
- Configuring the DAI Interface Trust State (옵션)
- Applying ARP ACLs for DAI Filtering (옵션)
- Configuring ARP Packet Rate Limiting (옵션)
- Enabling DAI Error-Disabled Recovery (옵션)
- Enabling Additional Validation (옵션)
- Configuring DAI Logging (옵션)
- Displaying DAI Information

14.4.1. Enabling DAI on VLANs

VLAN 에 DAI 를 enable 하면, 스위치는 해당 VLAN 을 통해 수신한 다음과 같은 ARP 패킷들을 검사합니다:

- 브로드캐스트되는 ARP 패킷
- 스위치의 MAC 주소를 요청하는 ARP request 패킷
- 스위치가 요청한 ARP request 에 대한 응답 패킷
- 단말들 사이에 송수신되는 모든 unicast ARP 패킷

이 패킷들을 검사해서, 유효한 패킷에 대해서만 응답하고 ARP 테이블을 변경합니다.

VLAN 에 DAI 를 enable 하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **ip arp inspection vlan** *vlan-id* Switch(config)# **no ip arp inspection vlan** *vlan-id*	VLAN 에 DAI 를 enable 합니다. VLAN 에 DAI 를 disable 합니다.
Switch# **show ip arp inspection**	설정을 확인합니다.

Notice

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

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

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

다음의 예는 설정을 확인하는 방법을 보여줍니다:

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

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

유니캐스트 ARP 패킷에 대해 DAI 기능을 사용하도록 할려면 class-map 과 policy-map 을 사용하여 ARP 패킷을 CPU 로 trap 되도록 해야합니다.

다음은 Vlan200 에서 수신한 ARP 패킷을 CPU 로 trap 되도록 설정하는 예제입니다.

```
Switch(config)#class-map arp_trap_class
Switch(config-cmap)#match ethertype 0806
Switch(config-cmap)#end
Switch#show class-map

   CLASS-MAP-NAME: arp_trap_class (match-all)
     Match Ethertype: 0806

Switch#config terminal
Switch(config)#policy-map arp_trap_map
Switch(config-pmap)#class arp_trap_class
Switch(config-pmap-c)#trap-cpu
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#int vlan200
Switch(config-if-Vlan200)#service-policy input dhcp_user_map
Switch#show policy-map

 POLICY-MAP-NAME: arp_trap_map
   State: attached

   CLASS-MAP-NAME: arp_trap _class (match-all)
     Trap-cpu

Switch#show service-policy
Interface     Vlan200 : input  dhcp_user_map
```

14.4.2. Configuring the DAI Interface Trust State

스위치는 trusted 인터페이스로부터 수신한 ARP 패킷은 검사하지 않습니다.

Untrusted 인터페이스를 통해 수신한 ARP 패킷은 유효한 IP-to-MAC 주소 매핑을 가지고 있는지 검사됩니다. 스위치는 유효하지 않은 패킷은 폐기하고, **ip arp inspection vlan logging** 설정에 따라 로그 버퍼에 패킷 로그를 저장합니다.

인터페이스의 trust 상태를 설정하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **interface** *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입합니다.
Switch(config-if-Giga0/1)# **ip arp inspection trust** Switch(config-if-Giga0/1)# **no ip arp inspection trust**	스위치와 연결된 인터페이스를 trusted 로 설정합니다. (default: untrusted) 스위치와 연결된 인터페이스를 untrusted 로 설정합니다.
Switch(config-if-Giga0/1)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection interfaces**	설정을 확인합니다.

다음의 예는 Gigabit 포트 1 을 trusted 로 설정하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip arp inspection trust
Switch(config-if-Giga0/1)# end
Switch# show ip arp inspection interfaces
Interface       Trust State  Rate (pps)  Burst Interval  Auto Recovery
--------------- -----------  ----------  --------------  -------------
Giga0/1         Trusted          None            1       Disabled
```

14.4.3. Applying ARP ACLs for DAI Filtering

ARP ACL 을 사용하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정로 진입합니다.
Switch(config)# **ip arp inspection filter** *arp_acl_name* **vlan** *vlan-id* [**static**]	VLAN 에 ARP ACL 을 적용합니다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection**	설정을 확인합니다.

ARP ACL 을 적용할 때, 다음의 사항에 유의하십시오:

- ARP ACL 의 implicit deny 를 explicit deny 처럼 다루고 ACL 의 어떤 조건과도 일치하지 않는 패킷을 폐기하려면, **static** 키워드를 사용하십시오. 이 경우에 DHCP binding 은 사용되지 않습니다.
  static 키워드를 사용하지 않으면, ACL 에 일치하는 조건이 없는 패킷에 대해서는 DHCP binding 을 사용해서 패킷을 permit 할 것이지 deny 할 것인지를 결정합니다.
- IP-to-MAC 주소 매핑을 포함하고 있는 ARP 패킷만 ACL 로 검사합니다. Access list 가 permit 하는 패킷들만 permit 됩니다.

다음의 예는 이름이 example_arp_acl 인 ARP ACL 을 VLAN 200 에 적용하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection filter example_arp_acl vlan 200
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Disabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled

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

14.4.4. Configuring ARP Packet Rate Limiting

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

Notice

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

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

Command	Purpose
Switch# **configure terminal**	global 설정으로 진입합니다.
Switch(config)# **interface** *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입합니다.
Switch(config-if-Giga0/1)# **ip arp inspection**	(옵션) ARP packet rate limit 를 설정합니다.

limit {**rate** *pps* [**burst interval** *seconds*] **| none**} Switch(config-if-Giga0/1)# **no ip arp inspection limit**	default 설정으로 복원합니다.
Switch(config-if-Giga0/1)# **ip arp inspection limit enable** Switch(config-if-Giga0/1)# **no ip arp inspection limit enable**	인터페이스의 ARP rate limit 기능을 enable 시킨다. 인터페이스의 ARP rate limit 기능을 disable 시킨다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection interfaces**	설정을 확인합니다.

ARP packet rate limit 를 설정할 때, 다음의 사항에 유의하십시오:

- 디폴트로 untrusted 인터페이스에 대해서는 15 pps (packet per second), trusted 인터페이스에 대해서는 rate 를 제한하지 않습니다.
- **rate** *pps* 로 초당 처리할 수 있는 상한을 설정합니다. 범위는 0 부터 2048 입니다.
- **rate none** 키워드는 수신되는 ARP 패킷의 rate 에 제한을 하지 않음을 명시합니다.
- (옵션) **burst interval** *seconds* (default 는 1)는, ARP 패킷의 rate 가 상한을 초과하는지 관측하는 시간입니다. 즉, **rate** 로 설정한 값을 **burst interval** 초 동안 초과할 때 해당 포트로 유입되는 ARP 패킷을 제한합니다. 값의 범위는 1 ~ 15 입니다.
- 유입되는 ARP 패킷의 rate 가 설정 값을 초과하면, 스위치는 해당 포트로 수신한 모든 ARP 패킷을 폐기합니다. 운영자가 설정을 변경할 때까지 이 상태가 유지됩니다.
- 인터페이스의 rate-limit 값을 변경하지 않고, 인터페이스의 trust 상태를 변경해도 인터페이스에 대한 rate-limit 의 default 값이 변경됩니다. rate-limit 값을 변경한 후에는, trust 상태를 변경하더라도 설정한 값이 그대로 보존됩니다. 인터페이스 설정 명령 **no ip arp inspection limit** 을 사용하면, 인터페이스의 rate-limit 값은 default 값으로 복원됩니다.
- **ip arp inspection limit enable** 명령을 설정해야, ARP 패킷 rate limit 가 동작합니다.

다음은 gi0/1 에 ARP packet rate limit 를 설정하는 예입니다:

```
Switch# configure terminal
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-Giga0/1)# ip arp inspection limit enable
Switch(config-if-Giga0/1)# end
Switch# show ip arp inspection interfaces
Interface        Trust State  Rate (pps)  Burst Interval  Auto Recovery
---------------  -----------  ----------  --------------  -------------
Giga0/1          Untrusted          20               2  Disabled
```

14.4.5. Enabling DAI Error-Disabled Recovery

ARP 패킷에 대한 rate limit 때문에, ARP 패킷의 수신이 제한된 포트를 자동으로 복구하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **interface** *ifname*	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드 로 진입합니다.
Switch(config-if-Giga0/1)# **ip arp inspection limit auto-recovery** *seconds* Switch(config)# **no ip arp inspection limit auto-recovery**	(옵션) 자동 복구 기능을 활성화 시킨다. 자동 복구 기능을 해제합니다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection interfaces**	설정을 확인합니다.

다음은 인터페이스 gi0/1 이 ARP rate limit 에 의해 ARP 패킷 수신이 차단되었을 경우, 10 초 후에 자동으로 복구되도록 설정하는 예입니다.

```
Switch# configure terminal
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-Giga0/1)# ip arp inspection limit enable
Switch(config-if-Giga0/1)# end
Switch# show ip arp inspection interfaces
Interface       Trust State  Rate (pps)  Burst Interval  Auto Recovery
--------------- -----------  ----------  --------------  -------------
Gi0/1           Untrusted    20          2               10
Gi0/2           Untrusted    15          1               Disabled
```

14.4.6. Enabling Additional Validation

DAI 로 ARP 패킷의 destination MAC 주소, sender 와 target IP 주소, source MAC 주소에 대한 유효성 검사를 할 수 있습니다.

IP 주소 또는 MAC 주소에 대한 유효성 검사를 하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **ip arp inspection validate {dst-mac** | **ip** | **src-mac}** Switch(config)# **no ip arp inspection validate**	(옵션) 추가적인 유효성 검사를 enable 합니다. (default: none) 추가적인 유효성 검사를 disable 합니다.

{**dst-mac** | **ip** | **src-mac**}	
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection**	설정을 확인합니다.

추가적인 유효성 검사를 enable 하려면, 다음의 사항에 유의하십시오:

- 다음의 키워드 중 적어도 하나를 사용해야 합니다.
- 각 **ip arp inspection validate** 명령은 이전의 명령을 삭제합니다. 만약, **ip arp inspection validate** 명령으로 **src-mac** 와 **dst-mac** 검사를 enable 하고, 두 번째 **ip arp inspection validate** 명령으로 **ip** 검사만을 enable 했다면, **src-mac** 와 **dst-mac** 검사는 disable 되고 **ip** 검사만이 enable 됩니다.
- 추가적인 유효성 검사는 다음과 같다:
  - **dst-mac** - ARP response 패킷에 대해 Ethernet 헤더의 destination MAC 주소와 ARP body 의 target MAC 주소를 비교합니다.
  - **ip –** ARP body 의 유효하지 않은 IP 주소를 검사합니다. 0.0.0.0 또는 255.255.255.255 또는 멀티캐스트 IP 주소는 폐기됩니다. ARP request 의 sender IP 주소, ARP response 의 sender/target IP 주소를 검사합니다
  - **src-mac** – 모든 ARP 패킷에 대해 Ethernet 헤더의 source MAC 주소와 ARP body 의 sender MAC 주소를 비교합니다.

다음의 예는 src-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Enabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled

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

다음의 예는 dst-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac
Switch(config)# end
```

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

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

다음의 예는 ip 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate ip
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Disabled
Destination MAC Validation : Disabled
IP Address Validation      : Enabled
ARP Field Validation       : Disabled

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

다음의 예는 src-mac 과 dst-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Enabled
Destination MAC Validation : Enabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled

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

14.4.7. Configuring DAI Logging

이 절에서는 DAI 의 로깅 [logging] 에 대해 설명합니다:

- DAI Logging Overview
- Configuring the DAI Logging Buffer Size
- Configuring the DAI Logging System Messages
- Configuring DAI Log Filtering

14.4.7.1. DAI Logging Overview

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성합니다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제됩니다. 각각의 로그에는 flow 정보(수신한 VLAN, port 번호, source 와 destination IP 주소, source 와 destination MAC 주소)가 포함됩니다.

하나의 로그 버퍼 entry 는 하나 이상의 패킷에 대한 정보를 표시할 수 있습니다. 예를 들어, 같은 VLAN 에서 같은 ARP 인자 [parameter] 를 가진 패킷을 동일한 인터페이스를 통해 많이 수신한다면, DAI 는 이 패킷에 대한 로그 버퍼 entry 를 하나 생성하고, 하나의 시스템 메시지를 생성합니다.

14.4.7.2. Configuring the DAI Logging Buffer Size

DAI 로그 버퍼의 크기를 설정하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **ip arp inspection log-buffer entries** *number* Switch(config)# **no ip arp inspection log-buffer entries**	DAI 의 로그 버퍼 크기를 설정합니다. (범위는 0 ~ 1024). default 버퍼 크기로 복원합니다. (32)
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection log**	설정을 확인합니다.

다음의 예는 DAI 의 로그 버퍼 크기를 64 개로 설정합니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
```

14.4.7.3. Configuring the DAI Logging System Messages

DAI 가 생성하는 로그 메시지를 설정하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **ip arp inspection log-buffer logs** *number_of_messges* **interval** *length_in_seconds* Switch(config)# **no ip arp inspection log-buffer logs**	DAI 로그 버퍼를 설정합니다. default 로 복원합니다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show ip arp inspection log**	설정을 확인합니다.

DAI 의 로깅 시스템 메시지를 설정하려면, 다음의 사항에 유의하십시오:

- **logs** *number_of_messges* (default 는 5) 에서, 값의 범위는 0 ~ 1024 입니다. 0 으로 설정하면 로그 메시지가 생성되지 않습니다.
- **interval** *length_in_seconds* (default 는 1) 에서, 값의 범위는 0 ~ 86400 초 (1 일)입니다. 0 으로 설정하면, 로그 메시지가 바로 생성됩니다 (즉, 로그 버퍼는 항상 비어있습니다).
- 시스템 로그 메시지는 *length_in_seconds* 초당 *number_of_messages* 의 비율로 생성됩니다.

다음의 예는 매 2 초마다 12 개의 DAI 로그 메시지를 생성하도록 설정합니다:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 12 entries per 2 seconds.
No entries in log buffer.
```

14.4.7.4. Configuring the DAI Log Filtering

ARP 패킷을 검사한 후, 그 결과에 대한 시스템 메시지를 선택적으로 생성할 수 있습니다.

DAI 의 log filtering 기능을 설정하려면, 다음의 작업을 수행하십시오:

Command	Purpose
Switch# **configure terminal**	global 설정 모드로 진입합니다.
Switch(config)# **ip arp inspection vlan** *vlan-id* {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	각 VLAN 에 대해 log filtering 을 설정합니다.
Switch(config)# **end**	Enable 모드로 돌아간다.
Switch# **show running-config**	설정을 확인합니다.

DAI 의 로깅 시스템 메시지를 설정하려면, 다음과 같은 사항에 유의하십시오:

- Default 로 모든 deny 되는 패킷은 로깅됩니다.
- **acl-match matchlog** — ACL 설정을 기반으로 로깅합니다. 이 명령에 **matchlog** 키워드를 명시했고, ARP access-list 설정의 **permit** 또는 **deny** 명령에 **log** 키워드가 사용되었다면, ACL 에 의해 permit 되거나 deny 되는 ARP 패킷들이 로깅됩니다.
- **acl-match none** — ACL 과 일치하는 패킷에 대해 로깅하지 않습니다.
- **dhcp-bindings all** — DHCP binding 과 일치하는 모든 패킷들을 로깅합니다.
- **dhcp-bindings none** — DHCP binding 과 일치하는 패킷들을 로깅하지 않습니다.
- **dhcp-bindings permit** — DHCP binding 에 의해 허용된 패킷들을 로깅합니다

다음의 예는 VLAN 200 에 대해 ACL 과 일치하는 패킷에 대한 로그 메시지를 생성하지 않도록 설정합니다.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200 logging acl-match none
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap       : Disabled
Source MAC Validation      : Disabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled

Vlan  Config    Operation  ACL Match           Static ACL  ACL Log   DHCP Log
----  --------  ---------  ------------------  ----------  --------- --------
 200  Enabled   Active                    No         None      Deny
```

14.4.8. Displaying DAI Information

DAI 의 정보를 조회하려면, 다음의 명령을 사용하십시오:

Command	Description
show arp access-list	ARP ACL 에 대한 정보를 출력합니다.
show ip arp inspection interfaces	인터페이스의 trust 상태 정보를 출력합니다.
show ip arp inspection vlan [*vlan-id*]	VLAN 에 대한 DAI 설정과 동작 상태 정보를 출력합니다.
show ip arp inspection arp-rate	인터페이스의 ARP 패킷 수신 rate 정보를 출력합니다.

DAI 통계정보를 조회하거나 초기화하려면, 다음의 명령을 사용하십시오:

Command	Description
clear ip arp inspection statistics	DAI 통계 정보를 초기화 합니다.
show ip arp inspection statistics [**vlan** *vlan-id*]	DAI 가 처리한 ARP 패킷에 대한 통계정보를 출력합니다.

DAI logging 정보를 조회하거나 초기화하려면, 다음의 명령을 사용하십시오:

Command	Description
clear ip arp inspection log	DAI 로그 버퍼를 초기화 합니다.
show ip arp inspection log	DAI 로그 버퍼의 설정과 로그 버퍼의 내용을 출력합니다.

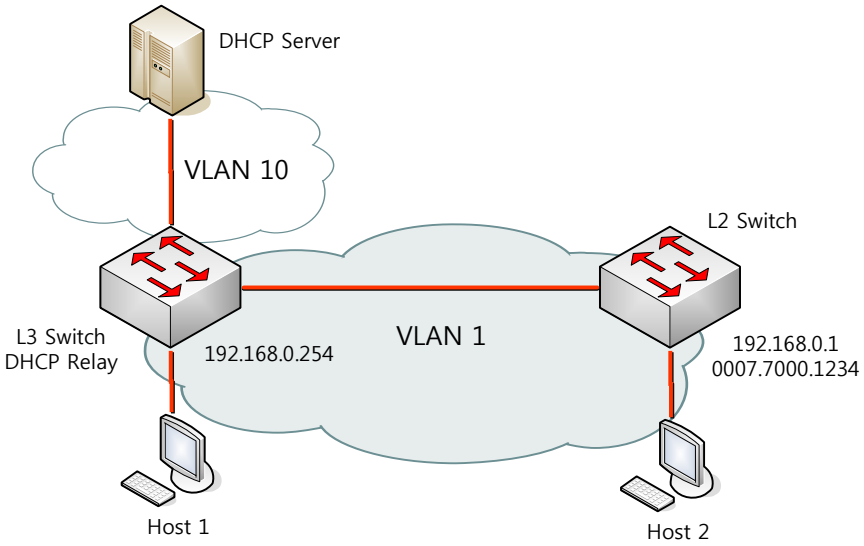
14.5. DAI Configuration Samples

이 절은 다음과 같은 예제들을 포함합니다:

- Sample One: Interoperate with DHCP Relay
- Sample Two: Interoperate with DHCP Server

14.5.1. Sample: Interoperate with DHCP Relay

이 예제는 DHCP relay 기능을 사용하는 스위치에 DAI 를 설정하는 방법을 설명합니다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정합니다:



L3 스위치는 VLAN 10 을 통해 DHCP 서버로 DHCP 메시지를 중계하며, 호스트 또는 L2 스위치가 연결됩니다. L3 스위치에 연결된 L2 스위치는 고정 IP 주소를 사용합니다. 호스트 1 과 호스트 2 는 DHCP 를 통해 IP 주소를 할당 받습니다. 그리고 모든 스위치와 호스트들은 VLAN 1 에 위치합니다.

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

DHCP relay 로 사용되는 스위치에서 DAI 기능을 사용하려면, 다음과 같이 설정합니다:

Step 1 **DHCP relay 기능을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 10.1.1.1
Switch(config)# service dhcp relay
```

Step 2 **DHCP 로 IP 를 할당 받는 호스트의 IP-to-MAC binding 정보를 구축하기 위해, DHCP server 와의 통신에 사용되는 인터페이스 VLAN 10 과 호스트가 연결된 인터페이스 VLAN 1 에 DHCP snooping 을 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping
```

Step 3 **고정 IP 를 사용하는 스위치의 ARP 패킷을 허용하기 위해 ARP ACL 을 설정합니다.**

```
Switch# configure terminal
Switch(config)# arp access-list permit-switch
Switch(config-arp-nacl)# permit ip host 192.168.0.1 mac host 0007.7000.1234
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection filter permit-switch vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인합니다.

```
Switch# show ip arp inspection vlan 1
```

Step 4 **호스트가 연결된 VLAN 1 에 DAI 를 활성화 시킨다.**

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인합니다.

```
Switch# show ip arp inspection vlan 1
```

L3 스위치의 설정을 조회하면 다음과 같다.

```
!
arp access-list permit-switch
  permit ip host 192.168.0.1 mac host 0007.7000.1234
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
ip dhcp helper-address 10.1.1.1
service dhcp relay
!
ip dhcp snooping vlan 1
ip dhcp snooping vlan 10
ip dhcp snooping
!
```

15

QoS 및 ACL

본 장은 현재 운영중인 E5224 Series 스위치의 QOS (Quality of Service)설정 및 ACL (access-list) 설정에 대해서 다룹니다.

15.1. QOS

15.1.1. 전역 설정

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

표 15-1. QOS 전역 설정 명령어

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

E5224 장비의 QOS 관련 설정은 위의 전역 설정이 되어 있다는 것을 기본 전제하에 동작합니다. Mls qos 가 활성화 되어 있지 않은 경우 대부분의 QOS 관련 명령어는 설정이 불가능합니다.

15.1.2. TX Scheduling 설정

E5224 Series 스위치에서는 Scheduling 을 위해 SPQ (Strict Priority Queue) Method 와 WRR (Weighted Round Robin) Method 를 제공하며 디폴트는 SPQ 입니다. 이 둘은 서로 혼재해서 사용하는 것이 가능하며, 2 개의 WRR 그룹을 가져서 이들 사이에서의 우선 순위도 가집니다.

이 장비에서 제공되는 WRR 은 정확하게는 SDWRR (Shaped Deficit Weighted Round Robin) Method 입니다. DWRR 은 일반 WRR 에서 quota 관리를 더 해주는 방식으로 동작하며, 이를 통해서 꾸준히 들

어오는 트래픽과, burst 하게 몰려 들어 오는 트래픽의 데이터량을 조절해주는 기능을 포함합니다. SDWRR 은 여기에 데이터의 흐름에 latency 를 줄기이 위한 shaping 기능이 포함됩니다. 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 노력합니다.

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

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 것입니다.

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

- 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 가집니다.

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

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

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 있습니다.

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 있습니다. 실제로는 총 8 개의 map 을 설

정할 수 있으나, 0 번은 default SPQ 로 사용되며 변경이 불가능하므로, 운용자가 설정할 수 있는 것은 7 개입니다.

표 15-2. 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 설정합니다. 해당 이름을 가지는 mapping table 이 없는 경우에는 새로 생성합니다.	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 가능합니다. Weight 값이 주어지지 않으면 1 로 설정됩니다.	Config
mls qos map tx-scheduling NAME wrr-weight <*0-7*> <*1-100*>	Wrr 로 설정된 큐의 weight 를 설정합니다.	Config
no mls qos map tx-scheduling NAME queueing-method <*0-7*>	해당 큐의 queueing-method 를 해제합니다. 해제할 경우 디폴트인 strict 로 바뀐다.	Config
no mls qos map tx-scheduling NAME wrr-weight <*0-7*>	Wrr 로 설정된 큐의 weight 를 해제합니다. 디폴트인 1 로 설정됩니다.	Config
no mls qos map tx-scheduling NAME	해당 이름을 가지는 mapping table 을 삭제합니다.	Config
show mls qos map tx-scheduling	Tx-scheduling 설정 정보를 보여줍니다.	Exec

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

표 15-3. Tx-scheduling 설정 명령어

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

15.1.3. 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 있습니다. 하지만, 인입되는 트래픽의 COS 또는 DSCP 값이 믿을 수 있는지를 결정해 주어야 합니다.

아무런 설정이 없는 경우에는 COS 또는 DSCP 값을 참조하지 않으며, 이 경우에는 포트에 설정된

default COS 값을 이용하여 동작하게 되어 있습니다. 참고로 이 default COS 값은 COS 또는 DSCP 가 없는 패킷 (예:untagged packet) 에 대한 기본 동작을 정의하는 용도로도 사용됩니다.

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

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

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

표 15-4. port trust 설정 명령어

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

15.1.4. DSCP 변환 map 설정

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

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

15.1.4.1. DSCP to queue 설정

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

```
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 15-5. dscp-queue map 설정 명령어

명령어	설명	모드
mls qos map dscp-queue *<0-63> … <0-63>* **to** *<0-7>*	Dscp-queue map 을 설정합니다.	config
no mls qos map dscp-queue	Dscp-queue map 을 초기화 합니다..	config
show mls qos map dscp-queue	현재 dscp-queue map 설정을 보여줍니다.	Exec

15.1.4.2. DSCP to COS 설정

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

```
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 15-6. dscp-cos map 설정 명령어

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

15.1.4.3. DSCP to DSCP 설정

DSCP 값에 따라 해당 패킷은 DSCP remarking 동작을 수행할 수 있습니다. 이는 자기 자신의 DSCP 값을 변경한다는 의미에서 mutation 이란 표현을 사용합니다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 입니다. 이 동작에 필요한 DSCP to DSCP map 값은 전역 설정으로 유지됩니다. 디폴트는 1:1 이 기본이므로, 의미 있게 사용하기 위해서는 map 을 변경 후에 포트 인터페이스에 적용해야 합니다.

```
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 15-7. dscp-mutation map 설정 명령어

명령어	설명	모드
mls qos map dscp-mutation *<0-63> … <0-63>* **to** *<0-63>*	Dscp-mutation map 을 설정합니다.	config
no mls qos map dscp-mutation	Dscp-mutation map 을 초기화 합니다..	config
mls qos dscp-mutation	해당 포트 인터페이스에 dscp remarking 을 수행하도록 설정합니다.	interface
no mls qos dscp-mutation	해당 포트 인터페이스에 dscp remarking 을 수행하지 않도록 설정합니다.	interface
show mls qos map dscp-mutation	현재 dscp-mutation map 설정을 보여줍니다.	Exec

15.1.5. COS 변환 map 설정

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

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

15.1.5.1. COS to queue 설정

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

```
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 15-8. cos-queue map 설정 명령어

명령어	설명	모드
mls qos map cos-queue *<0-7> <0-7>*	Cos-queue map 을 설정합니다.	config
no mls qos map cos-queue	Cos-queue map 을 초기화 합니다..	config
show mls qos map cos-queue	현재 cos-queue map 설정을 보여줍니다.	Exec

15.1.5.2. COS to DSCP 설정

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

```
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 15-9. cos-dscp map 설정 명령어

명령어	설명	모드
mls qos map cos-dscp *<0-7> <0-63>*	Cos-dscp map 을 설정합니다.	config
no mls qos map cos-dscp	Cos-Dscp map 을 초기화 합니다..	config
mls qos cos-dscp	해당 포트 인터페이스에 cos-dscp marking 을 수행하도록 설정합니다.	interface

no mls qos cos-dscp	해당 포트 인터페이스에 cos-dscp marking 을 수행하지 않도록 설정합니다.	interface
show mls qos map cos-dscp	현재 cos-dscp map 설정을 보여줍니다.	Exec

15.1.5.3. COS to COS 설정

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

```
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 15-10. cos-mutation map 설정 명령어

명령어	설명	모드
mls qos map cos-mutation *<0-7> <0-7>*	Cos-mutation map 을 설정합니다.	config
no mls qos map cos-mutation	Cos-mutation map 을 초기화 합니다..	config
mls qos cos-mutation	해당 포트 인터페이스에 cosremarking 을 수행하도록 설정합니다.	interface
no mls qos cos-mutation	해당 포트 인터페이스에 cos remarking 을 수행하지 않도록 설정합니다.	interface
show mls qos map cos-mutation	현재 cos-mutation map 설정을 보여줍니다.	Exec

15.2. ACL 설정

E5224 장비는 다양한 ACL 설정이 가능하며 이를 이용해서, 쉽게 허용하고자 하는 패킷과 그렇지 않는 패킷을 구분할 수 있습니다.

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

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

Extended IP ACL 은 source IP, destination IP, protocol type 을 이용해서 패킷을 구분할 수 있습니다. 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 가능합니다. <100-199> <2000-2699> 의 번호 대역이 할당되어 있으며, 그 외 번호가 아닌 이름으로도 생성하는 것이 가능합니다.

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

15.2.1. Standard IP ACL

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

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 있습니다.

표 15-11. standard IP ACL 설정 명령어

명령어	설명	모드
access-list *<1-99>* **(permit|deny) SRC_IP_ADDRESS**	Standard IP ACL 을 설정합니다.	config
no access-list *<1-99>* **(permit|deny) SRC_IP_ADDRESS**	Standard IP ACL 을 해제합니다.	config
no access-list *<1-99>*	해당 이름(번호)를 가지는 ACL 전부를 삭제합니다.	config
access-list *<1-99>* **remark LINE**	해당 ACL 에 대한 설명을 추가합니다.	config
access-list *<1300-1999>* **(permit|deny) SRC_IP_ADDRESS**	Expanded range 의 Standard IP ACL 을 설정합니다.	config
no access-list *<1300-1999>* **(permit|deny)**	Expanded range 의 Standard IP ACL 을 해제합	config

SRC_IP_ADDRESS	니다.	
no access-list *<1300-1999>*	해당 번호를 가지는 ACL 전부를 삭제합니다.	config
access-list *<1300-1999>* **remark LINE**	해당 ACL 에 대한 설명을 추가합니다.	config
access-list standard WORD (permit|deny) SRC_IP_ADDRESS	Named Standard IP ACL 을 설정합니다.	config
no access-list standard WORD (permit|deny) SRC_IP_ADDRESS	Named Standard IP ACL 을 해제합니다.	config
no access-list standard WORD	해당 이름을 가지는 ACL 전부를 삭제합니다.	config
access-list WORD remark LINE	해당 ACL 에 대한 설명을 추가합니다.	config
Show access-list	ACL 설정을 조회합니다	Exed

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

A.B.C.D A.B.C.D	IP 대역을 wildcard 형태로 설정이 가능합니다. 일반적인 IP 설정과는 반대로 masking 되는 부분이 0 입니다.
host A.B.C.D	단 하나의 IP 주소만을 가르킬때는 host prefix 를 붙혀서 사용합니다.
A.B.C.D	하나의 IP 만 주어진 경우는 host A.B.C.D 과 동일하게 처리됩니다.
any	모든 IP 주소를 지정하는 경우는 any 를 사용합니다.

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 의미합니다.
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 합니다.

15.2.2. Extended IP ACL

Standard IP ACL 이 src ip 주소만으로 패킷을 구분하는데 반해, extended ip acl 을 src ip 와 dest ip 를 모두 사용합니다. 뿐만 아니라 protocol type 을 이용해서 패킷을 구분할 수 있습니다. 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 가능합니다.

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 15-12. 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 설정합니다.	config
access-list *<100-199>* **(permit|deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE**	ICMP type 의 Extended IP ACL 을 설정합니다.	config
access-list *<100-199>* **(permit|deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE**	IGMP type 의 Extended IP ACL 을 설정합니다.	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 설정합니다.	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 해제합니다.	config
no access-list *<100-199>*	해당 이름(번호)를 가지는 ACL 전부를 삭제합니다.	config
access-list <100-199> remark LINE	해당 ACL 에 대한 설명을 추가합니다.	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 설정합니다.	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 설정합니다.	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 설정합니다.	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 설정합니다.	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 해제합니다.	config
no access-list *<2000-2699>*	해당 이름(번호)를 가지는 ACL 전부를 삭제합니다.	config
access-list *<2000-2699>* **remark LINE**	해당 ACL 에 대한 설명을 추가합니다.	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 설정합니다.	config
access-list extended WORD (permit|deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	ICMP type 의 Extended IP ACL 을 설정합니다.	config
access-list extended WORD (permit|deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Extended IP ACL 을 설정합니다.	config
no access-list extended WORD (permit|deny) (*<0-255>***|icmp|igmp|ip|ospf|pim|tcp|udp)**	Named Extended IP ACL 을 해제합니다.	config

SRC_IP_ADDRESS DST_IP_ADDRESS		
no access-list extended WORD	해당 이름을 가지는 ACL 전부를 삭제합니다.	config
access-list WORD remark LINE	해당 ACL 에 대한 설명을 추가합니다.	config
Show access-list	ACL 설정을 조회합니다	Exec

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

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

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 사용합니다.

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 의미합니다.
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 합니다.

15.2.3. MAC ACL

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

표 15-13. 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 설정합니다.	config
no mac-access-list *<1100-1199>* **(permit|deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS** *<1-8>*	MAC ACL 을 해제합니다.	config
no mac-access-list *<1100-1199>*	해당 이름(번호)를 가지는 ACL 전부를 삭제합니다.	

Show mac-access-list	MAC ACL 설정 상태를 조회합니다.	Exec

위 명령어중에서 **SRC_MAC_ADDRESS** 와 **DST_MAC_ADDRESS** 다음과 같은 방법으로 설정할 수 있습니다. 단 SRC_MAC 과 DST_MAC 둘다 any 가 될 수는 없습니다.

H.H.H H.H.H	MAC 대역을 wildcard 형태로 설정이 가능합니다..
any	모든 MAC 주소를 지정하는 경우는 any 를 사용합니다.

15.2.4. ACL 의 인터페이스 적용

위와 같이 설정된 ACL 은 다음과 같이 인터페이스에 적용이 가능합니다. 여기서 인터페이스는 다음 Physical 인터페이스를 의미하며, router port, switchport 로 지정된 포트 인터페이스에 적용이 가능합니다.

Input 방향과 output 방향에 걸 수 있으며, 해당 인터페이스로 들어 오는 또는 나가는 패킷에 대해서 ACL 을 설정할 수 있습니다.

표 15-14. ACL 의 인터페이스 적용 설정 명령어

명령어	설명	모드
ip access-group { *<1-199>* | *<1300>2699>* | WORD) } {in|out}	해당 인터페이스에 acl 을 설정합니다.	Interface
no ip access-group { *<1-199>* | *<1300>2699>* | WORD) } {in|out}	해당 인터페이스에 acl 을 해제합니다.	Interface


Notice

Router port 란 no switchport 상태인 port 를 의미합니다.


Notice

Service-policy 는 ACL 과 합쳐서 최대 input 방향으로 1500 개, output 방향으로 1500 개의 rule 을 설정할 수 있습니다.


Notice

Input 방향으로는 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능합니다, output 방향으로는 둘중 하나만 설정이 가능합니다.

15.3. 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 가능합니다. Class-map 에서는 ACL 또는 특정한 패킷의 성질을 이용해서 패킷을 분류하고, policy-map 에서는 이렇게 분류된 패킷에 특정한 동작을 수행할 수 있도록 해줍니다.

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 가능합니다. Class-map 은 ACL 을 이용할 수 있을 뿐만 아니라, AND OR 조합으로 ACL 과 다른 항목을 조합하여 사용하는 것도 가능합니다.

이러한 class-map 으로 분류된 트래픽은 기본적인 permit / drop 동작이외에도 queueing, cos marking / remarking, dscp marking / remarking, rate-limit 등의 동작을 수행하는 것이 가능합니다. 또한 nexthop 을 연동하여 PBR (Policy based routing) 이 가능하게 할 수 있습니다. QOS 와 상관 없지만, trap-cpu, mirror, redirect, netflow 등의 동작을 수행하게 하여 장비 운용에 필요한 다양한 동작을 수행토록 할 수도 있습니다.

이렇게 선언된 policy-map 은 service-policy 라는 명령을 통해서 switchport, router port interface 에 input 또는 output 방향에 적용하여 사용할 수 있습니다.

15.3.1. Class-map

Class-map 은 패킷을 분류하기 위한 목적으로 생성됩니다. 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 가능합니다.

ACL 은 ip acl 과 mac-acl 을 모두 사용 할 수 있지만, 1 개의 ACL 만 연동할 수 있습니다. 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 합니다.

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 있습니다. Class-map 을 선언할 때 match-any 옵션을 명시적으로 선언 하는 경우는 OR 연산을 수행하여, 둘중 하나만 만족하더라도 패킷이 분류 됩니다.

표 15-15. Class-map 설정 명령어

명령어	설명	모드
class-map WORD	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동합니다.	Config
class-map match-all WORD	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동합니다.	Config
class-map match-any WORD	OR 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동합니다.	Config
no class-map WORD	Class-map 을 삭제합니다..	Config
match access-group NAME	ACL 을 이용한 분류 조건을 설정합니다.	cmap
match cos *<0-7>*	Cos 을 이용한 분류 조건을 설정합니다.	cmap
match ethertype WORD	Ethertype 을 이용한 분류 조건을 설정합니다.	cmap
match ip-dscp *<0-63>*	Dscp 을 이용한 분류 조건을 설정합니다.	cmap
match ip-precedence *<0-7>*	Ip-precedence 을 이용한 분류 조건을 설정합니다.	cmap
match protocol *(<0-255>*|**icmp|igmp|ip|ospf|ospf|pim|tcp|udp)**	Ip protocol 를 이용한 분류 조건을 설정합니다.	cmap
match protocol arp (|A.B.C.D/M A.B.C.D/M)	Arp 를 이용한 분류 조건을 설정합니다	cmap
match layer4 {source-port|destination-port} *<1-65536>*	L4 port 을 이용한 분류 조건을 설정합니다.	cmap
match mpls exp-bit topmost *<0-7>*	Mpls flag 을 이용한 분류 조건을 설정합니다.	cmap
match tcp-control VALUE	Tcp-control 을 이용한 분류 조건을 설정합니다.	cmap
match vlan *<1-4095>*	VLAN 을 이용한 분류 조건을 설정합니다.	cmap

Notice

Ethertype 의 분류는 4 자리 hexadecimal 로 분류합니다. 예를 들어 ARP 타입인 경우 0806 으로 지정하면 됩니다.

Notice

Tcp-control 을 6 자리 2 진수로 분류합니다. 예를 들어 5 번째 자리인 SYN flag 를 보고자 할때는 000010 으로 선언하면 됩니다.

15.3.2. Policy-map

Class-map 으로 분류된 트래픽은 기본적인 permit / drop 동작이외에도 queueing, cos marking / remarking, dscp marking / remarking, rate-limit 등의 동작을 수행하는 것이 가능합니다. 또한 nexthop 을 연동하여 PBR (Policy based routing) 이 가능하게 할 수 있습니다. QOS 와 상관 없지만, trap-cpu, mirror, redirect, netflow 등의 동작을 수행하게 하여 장비 운용에 필요한 다양한 동작을 수행토록 할 수도 있습니다.

하나의 policy-map 에는 최대 100 개의 class-map 에 대해서 동작을 지정하는 것이 가능합니다. 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 없습니다.

각 class-map 별로 패킷에 대한 동작을 수행할 수 있는데, 다음과 같은 것들을 지정할 수 있으며, 동작의 조건에 따라 중복 적용도 가능합니다. 예를 들어 하나의 class-map 에 대해서 queueing 7 을 주며, cos marking 6 을 하고, dscp marking 54 를 동시에 수행하도록 할 수도 있습니다. 동작의 특성상 drop 같은 경우는 다른 동작과 중복되지 않습니다.

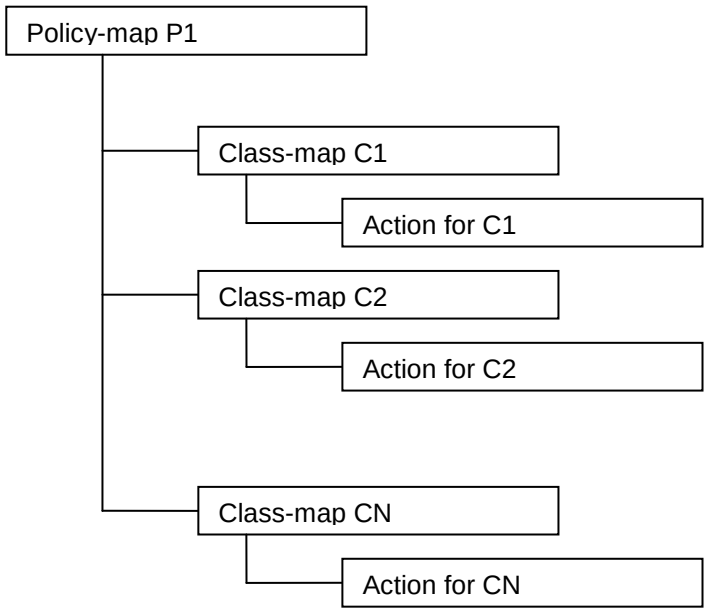


그림 15-1. policy-map 의 계층도

Marking 과 remarking 은 별다른 구분없이 사용되는데, 들어오는 패킷에 해당 필드가 없으면 자동으로 marking 을 수행하고, 해당 필드가 있으면 remarking 으로 동작합니다. Trap-cpu, mirror, redirect, netflow 등의 동작은 QOS 와는 직접적인 상관은 없지만, class-map 과 policy-map 을 이용해서 제어하는 것이 가능합니다.

표 15-16. policy-map 설정 명령어

명령어	설명	모드
policy-map NAME	해당 이름의 policy-map 을 생성하고 해당 노드로 이동합니다.	Config
no policy-map NAME	해당 이름의 policy-map 을 삭제합니다..	Config
class NAME	Class-map 의 동작을 지정하는 sub node 로 이동합니다	pmap
no class NAME	해당 class-map 동작 설정을 삭제합니다.	pmap
drop	해당 class-map 으로 분류된 트래픽을 drop 합니다.	pmap-c
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
redirect IFNAME	Redirect 설정	pmap-c
mirror	Mirror 설정	pmap-c
trap-cpu { high-priority| }	CPU trap 설정	pmap-c

15.3.3. Service-policy

위와 같은 방법으로 설정된 policy-map 은 switchport 또는 router port interface 에 적용이 가능합니다. ACL 과 마찬가지로 input 과 output 방향에 설정할 수 있습니다. 단, output 방향으로는 service-policy 와 ACL 중 하나만 설정이 가능하며, input 방향은 두 가지 설정을 동시에 적용이 가능합니다.

표 15-17. service-policy 설정 명령어

명령어	설명	모드
service-policy { input | output } NAME	해당 이름의 policy-map 을 인터페이스에 적용합니다.	interface
no service-policy { input | output } NAME	해당 이름의 policy-map 을 인터페이스에서 삭제합니다.	interface

Notice	Router port 란 no switchport 상태인 port 를 의미합니다.

Notice	Service-policy 는 ACL 과 합쳐서 최대 input 방향으로 1500 개, output 방향으로 1500 개의 rule 을 설정할 수 있습니다.

Notice	Input 방향으로는 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능합니다, output 방향으로는 둘 중 하나만 설정이 가능합니다.

15.4. COPP

COPP 는 Control Plane Policing 라는 의미로 CPU 로 유입되는 트래픽에 대한 rate-limit 및 QOS 정책을 적용하는 것을 의미합니다. 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 있습니다. 그러므로, 패킷별 우선순위 설정 및 rate-limit 설정을 통해 트래픽을 정리해주는 기능이 필요합니다.

15.4.1. Service-policy on COPP

Control Plane 에 service-policy 를 적용해서 CPU 로 유입되는 트래픽에 대해 Policing 을 수행할 수 있습니다.

표 15-18. service-policy 의 control-plane 적용 설정 명령어

명령어	설명	모드
control-plane	Control-plane 모드로 진입합니다	configure
service-policy input NAME	해당 이름의 policy-map 을 control-plane 에 적용합니다.	Control-plane
no service-policy input NAME	해당 이름의 policy-map 을 control-plane 에 적용을 해지합니다.	Control-plane

Notice	Control-plane 에서 Service-policy 가 사용되는 경우에는 policy-map 에서 설정하는 동작 중 **police**, **drop**, **set queueing** 의 동작만 수행이 됩니다.

15.4.2. Rate-limit on COPP

CPU 로 유입되는 특정 트래픽에 대해서 rate-limit 을 설정 할 수 있습니다.

표 15-19. 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 선택합니다	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 선택합니다	Control-plane
rate-limit igmp <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 igmp 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택합니다	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 선택합니다	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 선택합니다	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 선택합니다	Control-plane
rate-limit mld <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 mld 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택합니다	Control-plane
rate-limit multicast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 multicast 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택합니다	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 선택합니다	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 선택합니다	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 선택합니다	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 선택합니다	Control-plane

16 Setting Time and Calendar

E5224 시리즈 스위치는 time-of-day 서비스를 제공합니다. 이 서비스는 여러 장비들이 같은 시각으로 동기화를 맞추거나, 다른 시스템에 시간 서비스를 제공할 수 있도록 스위치가 정확한 현재 시간을 유지하도록 합니다.

16.1. Understanding Time Sources

E5224 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) 입니다. 이 두 개의 클락은 각각 관리됩니다.

시스템이 사용하는 기본 시간 소스는 소프트웨어 클락입니다. 소프트웨어 클락은 시스템 시작 후부터 현재 시각을 유지합니다. 소프트웨어 클락은 여러 가지 소스로부터 설정할 수 있고, 다양한 방법을 통해 다른 시스템으로 전달됩니다. 소프트웨어 클락은 시스템이 초기화되거나 리부트 될 때 하드웨어 클락을 사용해서 초기화됩니다. 그리고 나서 다음의 소스들을 사용해서 변경할 수 있습니다:

- Network Time Protocol (NTP)
- 수동 설정 (하드웨어 클락 사용)

소프트웨어 클락은 내부적으로 Coordinated Universal Time (UTC), 또는 Greenwich Mean Time (GMT) 기반으로 시간 정보를 관리합니다. 장비가 사용되는 지역의 시간 정보를 반영할 수 있도록 지역 시간대 (time zone)과 서머 타임 (daylight savings time)을 설정할 수 있습니다.

16.1.1. Network Time Protocol

NTP 는 네트워크에 연결된 장비들의 시간 동기화를 위해 설계된 프로토콜입니다. NTP 는 IP/UDP 서비스를 이용해서 동작합니다. RFC1305 에 NTP 버전 3 에 대해 정의되어 있습니다.

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 획득합니다. NTP 는 이 시간 정보를 네트워크를 통해 분배합니다. NTP 는 두 시스템 사이에 밀리초 단위의 시간 동기화를 맞추는데 분당 하나의 패킷을 사용할 정도로 매우 효과적인 프로토콜입니다.

NTP 는 신뢰성있는 타임 소스로까지 얼마나 많은 NTP “hops”이 존재하는 지를 나타내는 “stratum”이란 개념을 사용합니다. 일반적으로 “stratum 1” 타임 서버에는 타임 소스가 직접 연결 되어 있습니다. “stratum 2” 타임 서버는 “stratum 1” 타임 서버로부터 NTP 를 통해 시간 정보를 수신합니다. NTP 는 사용할 수 있는 타임 서버중 가장 작은 stratum 을 가진 타임 서버를 자신의 시간 소스로 선택합니다.

NTP 는 의심스러운 시간 정보로 동기화를 하지 않기 위해 다음 두 가지 방법을 제공합니다.

- NTP 는 자신을 소스로 동기화한 장비와는 동기화하지 않습니다.
- NTP 는 여러 장비에서 얻은 시간을 비교하고 다른 것과 큰 시간차를 보이는 장비와는 stratum 이 작아도 동기화하지 않습니다.

16.1.2. Hardware Clock

E5224 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 사용됩니다.

16.2. Configuring NTP

이 장에서는 시스템에서 NTP 를 사용할 수 있도록 다음과 같은 절차에 대해 설명합니다:

- 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

16.2.1. Configuring Poll-Based NTP Associations

NTP 를 사용하는 네트워크 장비는 시간 소스와 동기화를 맞추는데 여러 가지 동작 모드를 제공합니다. 장비가 네트워크로부터 시간 정보를 획득하는 방법으로는 호스트 서버에게 시간 정보를 요청(poll-based association)하거나 브로드 캐스트되는 NTP 정보를 청취하는 두 가지 방법이 있습니다. 이 장에서는 서버에게 요청하는 모드에 대해 설명합니다.

다음은 가장 많이 사용되는 서버 요청 모드입니다:

- Client mode
- Symmetric active mode

Client 와 Symmetric active 모드는 NTP 에 높은 수준의 시간 정밀도가 요구될 때 사용됩니다.

클라이언트 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사합니다. 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 않습니다. 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 됩니다.

Symmetric active 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사하고, 로컬 호스트에게는 시간 정보를 제공합니다. 이 모드는 peer-to-peer 관계이기 때문에 장비는 자신이 통신하는 로컬 네트워크 장비의 시간 정보도 함께 저장합니다. 이 모드는 복잡한 네트워크 경로를 통해 연결된 상호 중복된 서버가 존재할 경우에 사용되어야 합니다. 대부분의 stratum 1 과 stratum 2 서버는 이런 형태의 네트워크 설정을 사용합니다. Symmetric active 모드를 사용하려면 **ntp peer** 명령을 사용합니다.

NTP 의 동작 모드를 결정하는 것은 장비의 역할 (서버 또는 클라이언트)과 stratum 1 서버 설정입니다.

Command	Purpose

Switch(config)# **ntp server** *ip-adress*	Client 모드로 NTP 설정
Switch(config)# **ntp peer** *ip-adress*	Symmetric active 모드로 NTP 설정

16.2.2. Configuring NTP Authentication

암호화된 NTP 인증은 인증 키와 NTP 패킷의 정보를 사용하기 전에 신뢰할 수 있는 장비로부터 전송된 패킷인지를 검사하는 인증 절차를 사용합니다.

인증 절차는 NTP 패킷이 생성되는 순간부터 시작됩니다. MD5 message digest 알고리즘에 의해 암호화된 체크섬(checksum) 키가 생성되고 NTP 패킷에 포함되어 클라이언트에게 전송됩니다. 패킷을 수신한 클라이언트는 패킷의 암호화된 체크섬 키를 해독한 후 자신의 trusted 키와 비교합니다. 패킷이 유효한 인증 키를 포함하고 있다면 클라이언트는 이 패킷의 시간 정보를 허용합니다. 클라이언트와 일치하는 인증 키를 포함하고 있지 않는 NTP 패킷은 폐기됩니다.

NTP 인증이 올바르게 설정된 후부터 장비는 오직 신뢰할 수 있는 시간 소스와 시간을 동기화 시킵니다. 장비에서 암호화된 NTP 패킷을 송수신하게 하려면, 글로벌 설정 모드에서 다음의 명령을 사용합니다:

	Command or Action	**Purpose**
Step 1	Switch(config)# **ntp authenticate**	NTP 의 인증 기능을 활성화 시킵니다.
Step 2	Switch(config)# **ntp authentication-key** *key-number* **md5** *value*	인증 키를 정의합니다. 각 키는 키 번호와 종류 그리고 값을 가진다. 현재 지원되는 키 종류는 MD5 입니다.
Step 3	Switch(config)# **ntp trusted-key** *key-number*	신뢰하는 인증 키를 정의합니다. 만약 인증키가 신뢰하는 키라면, 시스템은 NTP 패킷에 이 키를 사용하는 시스템과 시간 동기를 시도합니다.
Step 4	Switch(config)# **ntp server** *ip-address* **key** *key-number*	소프트웨어 클락이 NTP 타임 서버와 동기화 되도록 허용합니다.

16.2.3. Configuring the Source IP Address for NTP Packets

시스템이 NTP 패킷을 전송할 때, NTP 패킷의 소스 IP 주소는 NTP 패킷을 전송하는 인터페이스의 주소로 설정됩니다. NTP 패킷의 소스 IP 주소로 특정 인터페이스의 IP 주소를 사용하고 싶다면 글로벌 설정 모드에서 다음의 명령을 사용합니다:

Command	**Purpose**
Switch(config)# **ntp source** *interface*	IP 주소를 빌려올 인터페이스를 지정합니다.

16.2.4. Configuring the System as an Authoritative NTP Server

시스템이 외부의 시간 소스와 동기화가 되지 않더라도 시스템을 NTP 서버로 사용하려면 글로벌 설정 모드에서 다음의 명령을 수행합니다:

Command	Purpose
Switch(config)# **ntp master** [*stratum*]	시스템을 NTP 서버로 설정합니다.

E5224 시리즈 스위치는 stratum 1 서비스를 지원합니다. 하지만 장비 내부에 연결 가능한 라디오 혹은 원자 클락이 존재하지는 않으므로 E5224 시리즈 스위치를 stratum 1 로 설정하는 것은 권장하지 않습니다.

16.2.5. Updating the Hardware Clock

하드웨어 클락을 가진 장비에서, 소프트웨어 클락으로 하드웨어 클락을 주기적으로 업데이트 하도록 설정할 수 있습니다. NTP 로 설정되는 소프트웨어 클락이 하드웨어 클락보다 더 정확하기 때문에 NTP 를 사용하는 장비에서는 이렇게 설정하는 것이 바람직합니다.

하드웨어 클락을 NTP 시각과 동기화시키려면 글로벌 설정 모드에서 다음의 명령을 사용합니다:

Command	Purpose
Switch(config)# **ntp update-calendar**	시스템의 하드웨어 클락을 주기적으로 소프트웨어 클락으로 업데이트 하도록 설정합니다.

16.3. Configuring Time and Date Manually

사용 가능한 타임 소스가 없다면, 시스템이 시작된 후에 현재 시각을 직접 설정할 수 있습니다.

16.3.1. Configuring the Time Zone

시간대 정보를 설정하려면 글로벌 설정 모드에서 다음의 명령을 사용합니다:

Command	Purpose
Switch(config)# **clock timezone** *zone hours-offset* [*minutes-offset*]	시간대를 설정합니다. 인자 zone 은 시간대의 이름을 표시합니다 (보통 표준 시간대 이름을 사용). 인자 *hours-offset* 은 UTC 와의 시차를 명시합니다. 인자 *minutes-offset* 은 UTC 와의 분차를 명시합니다.

16.3.2. Configuring Summer Time (Daylight Savings Time)

매년 특정 날짜에 시작되고 끝나는 서머 타임 (daylight savings time)을 설정하려면 글로벌 설정 모드에서 다음의 명령을 사용합니다:

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 표시합니다.

서머 타임이 매년 동일하게 반복되지 않는다면, 글로벌 설정 모드에서 다음의 명령으로 다음 서머타임이 시작되는 정확한 날짜를 설정할 수 있습니다:

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 표시합니다.

16.3.3. 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 사용합니다. 이 명령으로 설정되는 시간은 시간대의 영향을 받습니다. 소프트웨어 클락을 직접 설정하려면, EXEC 모드에서 다음의 명령을 사용합니다:

Command	Purpose
Switch# **clock set** *hh:mm:ss day month year* 또는 Switch# **clock set** *hh:mm:ss month day year*	소프트웨어 클락 설정.

16.4. Using the Hardware Clock

E5224 시리즈 스위치는 소프트웨어 기반의 클락과는 독립된 하드웨어 기반의 클락을 추가로 가지고 있습니다. 하드웨어 클락은 충전이 가능한 배터리를 가진 칩(chip)으로 장비가 리부트 되더라도 시각 정보를 유지할 수 있습니다.

소프트웨어 클락은 정확한 시각 정보를 유지하기위해 네트워크의 권위있는 타임 소스로부터의 시간 업데이트 정보를 수신해야 합니다. 그리고 시스템이 동작중인 동안 소프트웨어 클락은 하드웨어 클락을 주기적으로 업데이트 해줘야 합니다.

하드웨어 클락을 설정하기 위해 다음의 작업을 할 수 있습니다:

- Setting the Hardware Clock
- Setting the Software Clock from the Hardware Clock
- Setting the Hardware Clock from the Software Clock

16.4.1. Setting the Hardware Clock

하드웨어 클락은 소프트웨어 클락과 별도로 시간을 관리합니다. 하드웨어 클락은 시스템이 재시작되거나 전원이 꺼진 상태에서도 계속 동작합니다. 일반적으로 하드웨어 클락은 시스템이 설치될 때 한 번만 설정하면 됩니다.

믿을 수 있는 외부 시간 소스를 사용하고 있다면 하드웨어 클락을 직접 설정하지 않도록 합니다. 시간 동기는 NTP 를 이용해서 이뤄질 것입니다.

만약 사용할 수 있는 외부 시간 소스가 없다면 하드웨어 클락을 설정하기 위해 EXEC 모드에서 다음의 명령을 사용합니다:

Command	**Purpose**
Switch# **calendar set** *hh:mm:ss day month year* 또는 Switch# **calendar set** *hh:mm:ss month day year*	하드웨어 클락 설정.

16.4.2. Setting the Software Clock from the Hardware Clock

새로운 하드웨어 클락 설정으로 소프트웨어 클락을 설정하려면, EXEC 모드에서 다음의 명령을 상용합니다:

Command	**Purpose**
Switch# **clock read-calendar**	하드웨어 클락으로 소프트웨어 클락 설정.

16.4.3. Setting the Hardware Clock from the Software Clock

새로운 소프트웨어 클락 설정으로 하드웨어 클락을 설정하려면, EXEC 모드에서 다음의 명령을 사용합니다:

Command	Purpose
Switch# **clock update-calendar**	스프트웨어 클락으로 하드웨어 클락 설정.

16.5. Monitoring Time and Calendar Services

클락, 카렌더 그리고 NTP 정보를 조회하려면 다음의 명령들을 사용합니다.

Command	Purpose
Switch# **show calendar**	현재 하드웨어 클락 조회
Switch# **show clock**	현재 소프트웨어 클락 조회
Switch# **show ntp associations** [**detail**]	NTP association 상태 조회
Switch# **show ntp status**	NTP 상태 조회

16.6. Configuration Examples

16.6.1. Clock, Calendar, and NTP Configuration Examples

다음 예에서 하드웨어 클락을 가진 스위치는 두 개의 다른 시스템과 서버 관계를 가지고 있고, 주기적으로 하드웨어 클락을 업데이트 합니다.

clock timezone KST 9
ntp update-calendar
ntp server 192.168.13.57
ntp server 192.168.11.58

17

MLD Snooping

본 장에서는 MLD Snooping 설정에 대해 설명합니다.

17.1. MLD Snooping 개요

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

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

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

17.2. MLD Snooping 설정

17.3. Enable MLD Snooping on a VLAN

MLD Snooping 은 VLAN 별로 설정할 수 있으며, 다음의 명령을 interface configuration mode 에서 사용합니다.

명령어	설명
Ipv6 mld snooping	해당 VLAN 에 MLD Snooping 을 enable 합니다.
no ipv6 mld snooping	해당 VLAN 에 MLD Snooping 을 disable 합니다.

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ipv6 enable
Switch(config-if-Vlan22)# ip mld snooping
Switch(config-if-Vlan22)# end
Switch# show ipv6 mld interface
......
Interface Vlan22 (Index 2022)
  MLD Enabled, Active, Non-Querier, Version 1 (default)
  MLD interface has 10 group-record states
    MLD activity: 0 joins, 0 leaves
    MLD querying router is ::
    MLD query interval is 125 seconds
     MLD querier timeout is 262 seconds
     MLD max query response time is 25 seconds
     Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
    MLD Snooping is enabled on this interface
     MLD Snooping fast-leave is not enabled
     MLD Snooping querier is not enabled
     MLD Snooping report suppression is enabled
......
Switch#
```

17.4. Configure MLD Snooping Functionality

다양한 MLD Snooping 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행합니다.

17.4.1.1. MLD Report-Suppression

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

이 기능은 MLDv1 메시지에 한해서 적용되며, 아래의 명령을 interface configuration mode 에서 실행합니다.

명령	설명
Ipv6 mld snooping report-suppression	VLAN interface 에 MLD report-suppression 을 설정합니다.
no ipv6 mld snooping report-suppression	VLAN interface 에 설정된 MLD report-suppression 을 해제합니다.

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# no ipv6 mld snooping report-suppression
Switch(config-if-Vlan22)# end
Switch# show ipv6 mld interface
......
Interface Vlan22 (Index 2022)
  MLD Enabled, Active, Non-Querier, Version 1 (default)
    MLD interface has 10 group-record states
    MLD activity: 0 joins, 0 leaves
    MLD querying router is ::
    MLD query interval is 125 seconds
    MLD querier timeout is 262 seconds
    MLD max query response time is 25 seconds
    Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
    MLD Snooping is enabled on this interface
    MLD Snooping fast-leave is not enabled
    MLD Snooping querier is not enabled
    MLD Snooping report suppression is disabled
......

Switch#
```

17.4.1.2. MLD Fast-Leave

MLD Fast-Leave 기능을 enable 하면 호스트로부터 MLDv1 Done 메시지를 받았을 때 해당 VLAN 의 Membership interface 를 Multicast forwarding table 에서 즉시 제거합니다.

MLD Fast-Leave 기능은 VLAN interface 의 각 포트에 호스트가 하나인 경우에만 사용하여야 합니다. 만약, 포트에 여러 호스트가 속해 있는 경우에 이 기능을 사용하면. MLDv1 Done 메시지를 보내지 않은 호스트들도 일정시간 동안 Done 이 된 멀티캐스트 그룹에 대한 트래픽을 받지 못하게 되는 경우가 발생하게 됩니다.

명령	설명
Ipv6 mld snooping fast-leave	해당 VLAN 에 fast-leave 기능을 설정합니다.
no ipv6 mld snooping fast-leave	해당 VLAN 에 설정된 fast-leave 를 해제합니다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ipv6 mld snooping fast-leave
Switch(config-if-Vlan22)# end
Switch# show ipv6 mld interface
......
Interface Vlan22 (Index 2022)
  MLD Enabled, Active, Non-Querier, Version 1 (default)
    MLD interface has 10 group-record states
    MLD activity: 0 joins, 0 leaves
    MLD querying router is ::
    MLD query interval is 125 seconds
    MLD querier timeout is 262 seconds
    MLD max query response time is 25 seconds
    Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
    MLD Snooping is enabled on this interface
    MLD Snooping fast-leave is enabled
    MLD Snooping querier is not enabled
    MLD Snooping report suppression is enabled
......
```

```
Switch#
```

17.4.1.3. MLD Mrouter-Port

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

기본적으로 MLD Snooping 은 MLD 메시지를 Snooping 하여 Multicast Router 와 연결된 Mrouter Port 를 감지합니다.

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

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

명령어	설명
Ipv6 mld snooping mrouter interface *IFNAME*	해당 VLAN 에 mrouter port 를 수동으로 설정합니다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 합니다.
no ipv6 mld snooping mrouter interface *IFNAME*	해당 VLAN 에 설정된 mrouter port 를 해제합니다.

```
Switch# configure terminal
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ipv6 mld snooping mrouter interface gi0/2
Switch(config-if-Vlan22)# end
Switch# show ipv6 mld snooping mrouter vlan22
VLAN    Interface
22      Giga0/2

Switch#
```

17.4.1.4. MLD Access-Group

MLD Snooping 은 특정 인터페이스에서 수신되는 MLD Host 들의 특정 그룹을 제한할 수 있습니다. MLD Host 의 멀티캐스트 그룹을 제한하기 위해서는 아래의 명령을 interface configuration mode 에서 실행합니다.

명령어	설명
Ipv6 mld snooping access-group *<access-list>*	해당 포트에 수신되는 호스트들의 멀티캐스트 그룹에 대한 등록을 제한합니다.
no ipv6 mld snooping access-group *<access-list>*	해당 포트에 수신되는 제한된 호스트들의 멀티캐스트 그룹에 대한 등록을 해제합니다.

```
Switch# configure terminal
Switch(config)# ipv6 access-list test permit ff05::e100:1
Switch(config)# access-list 10 deny any
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ipv6 mld snooping access-group test
Switch(config-if-Giga0/1)# end
Switch#
```

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

명령어	설명
Ipv6 mld snooping access-group *<access-list>* **vlan** *<vlan-id>*	해당 포트에서 해당 VLAN 으로 수신되는 호스트들의 멀티캐스트 그룹에 대한 등록을 제한합니다.
no Ipv6 mld snooping access-group *<access-list>* **vlan** *<vlan-id>*	해당 포트에서 해당 VLAN 으로 수신되는 제한된 호스트들의 멀티캐스트 그룹에 대한 등록을 해제합니다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ipv6 mld snooping limit 10 vlan 22
Switch(config-if-Giga0/1)# end
Switch#
```

17.4.1.5. MLD Group-Limit

MLD Snooping 은 각각의 interface 별로 Multicast Group 의 개수를 제한할 수 있습니다.
Multicast Group 의 개수를 제한하기 위해서는 다음의 명령을 interface configuration mode 에서 수행합니다.

명령어	설명
Ipv6 mld snooping limit <*count*>	해당 포트에 수신되는 Multicast Group 의 개수를 제한합니다.
Ipv6 mld snooping limit <*count*> **except** <*access-list*>	해당 포트에 수신되는 Multicast Group 의 개수를 제한합니다. 제한하지 않을 Group 은 access-list 로 만들어 지정합니다.
no ipv6 mld snooping limit <*count*>	해당 포트에 설정된 Multicast Group 의 개수 제한을 해제합니다.

```
Switch# configure terminal
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ipv6 mld snooping limit 10
Switch(config-if-Giga0/1)# 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 실행합니다.

명령어	설명
Ipv6 mld snooping limit <*count*> **vlan** <*vlan-id*>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한합니다.
Ipv6 mld snooping limit <*count*> **vlan** <*vlan-id*> **except** <*access-list*>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한합니다. 제한하지 않을 Group 은 access-list 로 만들어 지정합니다.
no ipv6 mld snooping limit <*count*> **vlan** <*vlan-id*>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수 제한을 해제합니다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi0/1
Switch(config-if-Giga0/1)# ipv6 mld snooping limit 10 vlan 22
Switch(config-if-Giga0/1)# end
Switch#
```

Multicast Group 수의 제한 범위는 VLAN Interface 별로 설정할 수 있습니다. 해당 명령은 아래와 같으며, interface configuration mode 에서 실행합니다.

명령어	설명
Ipv6 mld limit <*count*>	해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한합니다.
Ipv6 mld limit <*count*> **except** <*access-list*>	해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한합니다. 제한하지 않을 Group 은 access-list 로 만들어 지정합니다.
no Ipv6 mld limit	전체 Multicast Group 의 개수 제한을 해제합니다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface vlan22
Switch(config-if-Vlan22)# ipv6 mld limit 10
Switch(config-if-Vlan22)# end
Switch#
```

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

명령어	설명
Ipv6 mld limit <*count*>	전체 Multicast Group 의 개수를 제한합니다.
Ipv6 mld limit <*count*> **except** <*access-list*>	전체 Multicast Group 의 개수를 제한합니다. 제한하지 않을 Group 은 access-list 로 만들어 지정합니다.
no Ipv6 mld limit	전체 Multicast Group 의 개수 제한을 해제합니다.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld limit 10
Switch(config)# end
Switch#
```

17.4.1.6. MLD snooping forced-source-ip

MLD Snooping 동작 시에 Mrouter port 로 전달되는 MLD Message 에 대하여 Source address 를 지정할 수 있습니다. 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 가능합니다.

명령어	설명
Ipv6 mld snooping forced-source-ip *<ip-address>*	해당 VLAN 의 Report 및 Done Message 의 Source Address 를 지정합니다.
no ipv6 mld snooping forced-source-ip	해당 VLAN 의 Report 및 Done Message 의 Source Address 를 해제합니다.

```
Switch# configure terminal
RT#F_211(config)#interface Vlan 200
Switch(config-if-Vlan200)#ipv6 mld snooping forced-source-ip
ff05::e100:1
Switch# end
```

17.4.1.7. MLD snooping querier timeout

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

명령어	설명
Ipv6 mld querier-timeout *<60-300>*	해당 VLAN 의 Querier timeout 시간을 설정합니다.
no ipv6 mld querier-timeout	해당 VLAN 의 Querier timeout 시간을 해제합니다.

```
Switch# configure terminal
Switch (config)#interface Vlan 200
Switch(config-if-Vlan200)#ipv6 mld querier-timeout 60
Switch#show ipv6 mld interface
Interface Vlan200 (Index 2200)
  MLD Enabled, Inactive, Version 1 (default)
    MLD interface has 0 group-record states
    MLD activity: 0 joins, 0 leaves
   MLD querying router is ::
    MLD query interval is 125 seconds
```

```
    MLD querier timeout is 60 seconds
    MLD max query response time is 25 seconds
    Last member query response interval is 1000 milliseconds
    Group Membership interval is 275 seconds
   MLD Snooping is enabled on this interface
    MLD Snooping fast-leave is enabled
    MLD Snooping querier is not enabled
    MLD Snooping report suppression is enabled
```

17.4.1.8. MLD Snooping querier

interface 에 가상의 IGMP querier 를 생성하여, 해당 VLAN 의 member port 에 주기적으로 Query 를 전송하는 기능입니다.

MLD Snooping querier 가 설정되었을 때 다른 장비로부터 Query 를 수신한 경우 MLD Snooping querier 기능은 일시적으로 중지됩니다.

다른 장비로부터의 Query 로 인해 non-querier 가 된 상태에서 other-querier timeout 시간 동안 다른 Query 를 수신하지 못했다면 다른 querier 의 정보를 삭제하고 MLD Snooping querier 기능이 다시 시작되어 Query 를 전송하게 됩니다.

또한 snooping querier 가 송신하는 query 의 max-response-time, query-interval, source-ip, version 값을 사용자가 설정할 수 있습니다.

MLD snooping querier 명령은 interface configuration mode 에서 실행하며, 각 명령에 대한 설명은 아래와 같습니다.

명령어	설명
Ipv6 mld snooping querier	해당 VLAN 에 가상 querier 를 생성합니다.
no ipv6 mld snooping querier	해당 VLAN 에 가상 querier 를 해제합니다.
Ipv6 mld snooping querier max-response-time *<1-240>*	querier 가 송신하는 query 의 max-response-time 값을 지정합니다.
no ipv6 mld snooping querier max-response-time	설정한 query 의 max-response-time 값을 해제하여 default 값(25)으로 돌아갑니다.
ipv6 mld snooping querier query-interval *<1-18000>*	querier 가 송신하는 query 의 query-interval 값을 지정합니다.
No ipv6 mld snooping querier query-interval	설정한 query 의 query-interval 값을 해제하여 default 값(125)으로 돌아갑니다.
ip ipv6 mld snooping querier source-ip *<ip-address>*	querier 가 송신하는 query 의 source ip 를 지정합니다. (source ip 주소는 link-local scope)
no ipv6 mld snooping querier source-ip	설정한 query 의 source ip 를 해제하여 default 값

	(VLAN link-local IP)으로 돌아갑니다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan 200
Switch(config-if-Vlan200)#ipv6 mld snooping querier
Switch(config-if-Vlan200)#ipv6 mld snooping querier source-ip
ff05::e100:1
Switch(config-if-Vlan200)#ipv6 mld snooping querier max-response-time 30
Switch(config-if-Vlan200)#ipv6 mld snooping querier query-interval 45
Switch(config-if-Vlan200)#end
```

17.5. Configure MLD Static Group Functionality

17.5.1.1. MLD Static Group

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

MLD static-group 명령은 interface configuration mode 에서 실행하며, 각 명령에 대한 설명은 아래와 같습니다.

명령어	설명
Ipv6 mld stat ic-group *<group-address>*	*<group-address>*으로 Static Group 을 설정합니다.
Ipv6 mld static-group *<group-address>* **interface** *IFNAME*	Static Group 의 Group-address 를 class-map 으로 설정합니다.
no ipv6 mld static-group *<group-address>*	*<group-address>*으로 Static Group 을 해제합니다.
no ipv6 mld static-group *<group-address>* **interface** *IFNAME*	해당 Group 및 interface 의 Static Group 을 해제합니다.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan 200
Switch(config-if-Vlan200)#ipv6 mld static-group ff05::e100:1
Switch(config-if-Vlan200)#end
```

```
Switch#show ipv6 mld groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires  Last Reporter
ff05::e100:1       Vlan200            00:00:03   static      ::
```

17.6. Display System and Network Statistics

표 17-1. IGMP Snooping 관련 모니터링 명령어

명령어	설명
show ipv6 mld groups	MLD JOIN 정보를 보여줍니다.
show ipv6 mld interface	MLD snooping 설정 정보를 보여줍니다.
show ipv6 mld static-group class-map	static-group 등록을 위해 지정한 class-map 의 정보를 보여줍니다.
show ipv6 mld snooping statistics	MLD snooping 의 통계 정보를 보여줍니다
show ipv6 mld snooping mrouter <*IFNAME*>	MLD snooping 의 통계 정보를 보여줍니다
show ipv6 mld snooping reporter	MLD JOIN 이 되어 있는 호스트들의 목록을 보여줍니다.

18 IP-OPTION

18.1. 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 기능입니다

18.2. IP OPTOIN 명령어

IP OPTION 명령으로 설정 가능한 parameter 들은 다음과 같습니다.

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 설정합니다.	Config
no ip option icmp-drop	ICMP 패킷 차단 설정을 해제합니다.	Config
ip icmp-ttl-exceed-send	TTL Exceed ICMP 에러 전송을 허용합니다.	Config
no ip icmp-ttl-exceed-send	TTL Exceed ICMP 에러 전송 설정을 해제합니다.	Config
ip option icmp-unreachable-send	ICMP unreachable 에러 전송을 허용합니다.	Config
no ip option icmp-unreachable-send	ICMP unreachable 에러 전송 설정을 해제합니다.	Config
ip option icmp-unreachable-send too-big	ICMP unreachable (Fragmentation Needed/ DF set) 에러 전송을 허용합니다.	Config
no ip option icmp-unreachable-send too-big	ICMP unreachable (Fragmentation Needed/ DF set) 에러 전송 설정을 해제합니다.	Config
ip option ip_default_ttl *VALUE*	Default TTL 크기를 설정합니다.	Config

	Default) 64	
no ip option ip_default_ttl	Default TTL 크기 설정을 기본값으로 변경합니다.	Config
ip option ipfrag_time *VALUE*	메모리에서 IP fragment 를 유지하는 시간을 설정합니다. **Default) 30**	Config
no ip option ipfrag_time	메모리에서 IP fragment 를 유지하는 시간을 기본값으로 변경합니다.	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 추가합니다. TCP 목적지 포트에 대해 period 이내에 count 이상 TCP 연결을 시도하는 경우 로깅 및 차단할 수 있습니다.	Config
no ip option tcp-conn-rate-limit profile-id <*1-128*>	Profile-id 에 해당하는 TCP connection rate-limit profile 을 삭제합니다.	Config
ip option tcp_fin_timeout *VALUE*	FIN-WAIT-2 상태의 소켓 유지 시간을 설정합니다. **Default) 60**	Config
no ip option tcp_fin_timeout	FIN-WAIT-2 상태의 소켓 유지 시간을 기본값으로 변경합니다.	Config
ip option tcp_keepalive_probes *VALUE*	연결이 끊어졌다고 여길 때까지 발생 시킬 keepalive probe 메시지 수를 설정합니다. **Default) 9**	Config
no ip option tcp_keepalive_probes	Keepalive probe 메시지 수를 기본값으로 변경합니다.	Config
ip option tcp_keepalive_time *VALUE*	Keepalive 가 활성화되었을 경우 keepalive 메시지 전송 시간을 설정을 설정합니다. **Default) 7200**	Config
no ip option tcp_keepalive_time	Keepalive 메시지 전송 시간을 기본값으로 변경합니다.	Config
ip option tcp_max_syn_backlog *VALUE*	TCP syn backlog queue 의 최대치 설정입니다. **Default) 1024**	Config
no ip option tcp_max_syn_backlog	TCP syn backlog queue 의 최대치 설정을 기본값으로 변경합니다.	Config
ip option tcp_max_tw_buckets *VALUE*	Timewait 소켓의 수를 설정합니다. **Default) 18700**	Config
no ip option tcp_max_tw_buckets	Timewait 소켓의 수를 기본값으로 변경합니다.	Config
ip option tcp_retries1 *VALUE*	의심스러운 TCP session 에 대한 재전송 횟수를 설정합니다. **Default) 3**	Config

no ip option tcp_retries1	의심스러운 TCP session 에 대한 재전송 횟수를 기본값으로 변경합니다.	Config
ip option tcp_retries2 *VALUE*	종단전 재전송 횟수를 설정합니다. **Default)15**	Config
no ip option tcp_retries2	종단전 재전송 횟수를 기본값으로 변경합니다.	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 변경합니다.	Config
ip option tcp_syncookies (default|disable|enable)	Syn flood attack 방어를 위해 설정합니다. **Default) enable**	Config
ip option telnet-acl access-group <1-99>	Telnet 접속을 access-group 에 대해 허용 및 차단하도록 설정합니다.	Config
no ip option telnet-acl acess-group <1-99>	Access-group 에 의한 telnet 접속 제한 설정을 해제합니다.	Config
ip option ftp-acl access-group <1-99>	FTP 접속을 access-group 에 대해 허용 및 차단하도록 설정합니다.	Config
no ip option ftp-acl acess-group <1-99>	Access-group 에 의한 FTP 접속 제한 설정을 해제합니다.	Config

19 시스템 및 통계 모니터링

본 장은 현재 운영중인 E5224 Series 스위치의 시스템 및 통계 모니터링 기능에 대해 설명합니다.

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

E5224 Series 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 합니다. 주기적으로 통계 데이터를 관리하면 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있습니다.

19.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공합니다. E5224 Series 스위치는 **show** 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공합니다.

표 19-1. 상태 모니터링 명령어

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

19.2. 시스템 임계치 설정

E5224 Series 스위치는 시스템 모듈 온도, CPU 및 메모리 사용률 등에 대해 임계치(threshold)를 설정할 수 있습니다. 임계치는 상한 임계치와 하한 임계치로 설정할 수 있으며, 설정한 범위를 벗어나는 경우 syslog 및 SNMP 트랩을 발생시킬 수 있습니다.

19.2.1. 온도 설정

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

표 19-2. 온도 설정 관련 명령어

명령어	설명	모드
`facility-alarm temperature major` *`value`* `minor` *`value`*	모든 모듈에 대해 온도 임계치(major/minor)를 설정합니다.	Config
`no facility-alarm temperature`	온도 임계치를 기본값으로 설정합니다.	Config

`show environment alarm thresholds`	파워, FAN, 온도의 알람 임계치 정보를 출력합니다.	Privileged
`clear facility-alarm [major|minor]`	알람 이력을 삭제합니다.	Privileged

다음은 major 및 minor 온도 임계치를 설정한 예제입니다.

```
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
```

19.2.2. Cpu usage 설정

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

표 19-3. CPU usage threshold 관련 명령어

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

19.2.3. Memory Usage 설정

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

표 19-4. Memory usage 관련 명령어

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

19.2.4. Application memory 사용 display

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

표 19-5. Memory display 관련 명령어

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

Notice

조회 가능한 application 은 추후에 추가 및 삭제 될 수 있습니다.

19.3. 포트 통계

E5224 Series 스위치는 각 포트의 통계 정보를 제공하며, 다양한 포트 통계 조회 명령들을 통해 아래와 같은 포트 통계 정보를 조회할 수 있습니다.

표 19-6. 포트 통계 정보

항목	설명
수신 패킷 통계	포트에서 수신한 패킷의 수입니다.
수신 바이트 통계	포트에서 수신한 바이트의 수입니다.
전송 패킷 통계	포트에서 전송한 패킷의 수입니다.
전송 바이트 통계	포트에서 전송한 바이트의 수입니다.
브로드캐스트 통계	포트에서 수신 및 전송한 브로드캐스트 주소를 가지는 패킷의 수입니다.
멀티캐스트 통계	포트에서 수신 및 전송한 멀티캐스트 주소를 가지는 패킷의 수입니다.
Transmit Collisions 통계	포트에서 패킷 전송 시 발생한 충돌 횟수입니다.
불량 CRC 프레임 통계	포트에서 수신한 양호한 길이의 프레임 중 불량 CRC 를 포함한 프레임의 수입니다.
Oversize 프레임 통계	포트에서 수신한 프레임 중 MRU 사이즈보다 큰 프레임의 수입니다.
Drop 프레임 통계	포트에서 수신한 프레임 중 시스템 자원이 부족해서 버려진 프레임의 수입니다.

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

show interface [*IFNAME*]

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

```
Switch# show interface GigabitEthernet 0/1

Giga0/1 is up, line protocol is up (connected)
  Hardware is Ethernet  Current HW addr: 0007.70b2.a7c9
  Physical:0007.70b2.a7c9  Logical:(not set)
  index 101 metric 1 mtu 1500 arp ageing timeout 7200
  A-full-duplex, A-100Mb/s, media type is 10/100/1000BaseT
  <UP,BROADCAST,RUNNING,MULTICAST>
  Bandwidth 100m
  Last clearing of "show interface" counters never
  60 seconds input rate 640 bits/sec, 1 packets/sec
```

```
  60 seconds output rate 104 bits/sec, 0 packets/sec
  L2/L3 in Switched: ucast 25,259 pkt - mcast 61,124 pkt
  L2/L3 out Switched: ucast 12,064 pkt - mcast 2,937 pkt
    97,444 packets input, 23,211,975 bytes
    Received 11,061 broadcast pkt (61,124 multicast pkt)
    0 CRC, 0 oversized, 0 dropped
    15,004 packets output, 1,094,278 bytes
    0 collisions
    0 late collisions, 0 deferred
```

표 19-7. 포트 통계 조회 명령들

명령어	설명	모드
show port counter [detail]	아래 항목에 대해 모든 인터페이스의 누적 통계 정보를 출력합니다. 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 출력합니다. 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 출력합니다. TX: Unicast/Multicast/Broadcast s RX: Unicast/Multicast/Broadcast	Privileged
show port statistics interface *[IFNAME]*	아래 항목에 대한 인터페이스의 통계 정보를 출력합니다. InOctets/ OutOctets InUcastPkts/ OutUcastPkts InMcastPkts/ OutMcastPkts InBcastPkts/ OutBcastPkts IfInDiscards IfInErrors	Privileged
show port-mib *IFNAME*	해당 인터페이스의 현재 통계와 누적 통계 정보를 상세하게 출력합니다.	Privileged

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

```
Switch# show interface counters

 Port           I-Kbps      O-Kbps                    InOctets
 --------- ---------- ---------- -------------------------
 Gi0/1               1           0                126,601,563
```

```
 Gi0/2                0            0                          0
 Gi0/3                0            0                          0
 Gi0/4                0            0                          0
 Gi0/1                0            0                          0
 Gi0/2                0            0                          0
 Gi0/3                0            0                          0
 Gi0/4                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 내용입니다.

```
Switch# show port statistics gi0/1
Last clearing of counters 55:17:10
================================================================================
 Port                                  TX|                                   RX
                     bits/s          pkts/s|          bits/s          pkts/s
--------------------------------------------------------------------------------
 Gi0/1    ------------------------------------------------------------------------
    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 보여집니다. 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 있습니다. .

표 19-8. 포트 통계 설정 명령

명령어	설명	모드
load-interval *interval*	인터페이스의 평균 통계 정보를 갱신하는 시간을 설정합니다.	interface
no load-interval	인터페이스의 평균 통계 정보를 갱신하는 시간을 기본 값으로 변경합니다.	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 값	interface

	을 벗어나는 경우를 모니터링 할 수 있습니다.	
no input-load-monitor	해당 인터페이스에 대한 모니터링 설정을 해제합니다.	interface
show port input-load-monitor	인터페이스에 대한 모니터링 설정을 출력합니다.	interface

다음 명령은 포트 통계에 대해 누적 값을 초기화시키는 명령어입니다.

표 19-9. 포트 통계 초기화 명령

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

19.4. RMON (Remote MONitoring)

시스템 운영자는 E5224 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있습니다. 다음 절에서는 RMON 개념 및 E5224 Series 스위치가 지원하는 RMON 기능에 대하여 자세히 설명합니다.

19.4.1. 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 제공합니다. 일반적으로 RMON 은 다음의 두 가지 구성 요소를 가집니다.

- **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

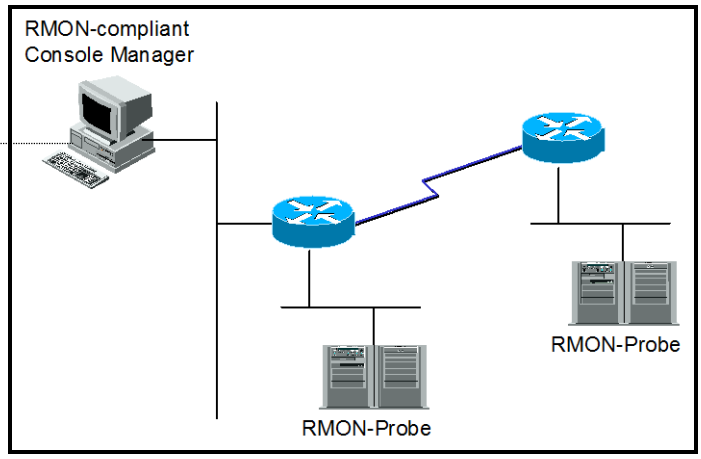


그림 19-1. RMON Manager 와 RMON Probe

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

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 합니다.

E5224 Series 스위치에서는 아래 표에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원합니다. RMON 은 디폴트로 모든 설정이 disabled 입니다.

표 19-10. 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.

19.4.2. RMON 의 Alarm 과 Event 그룹 설정.

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

표 19-11. 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 추가합니다. *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 추가합니다. *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 삭제합니다.	Config
no rmon event *event-index*	설정한 RMON event 설정을 삭제합니다	Config
show rmon alarms	RMON alarm 정보 출력합니다.	Privileged
show rmon events	RMON event 정보 출력합니다.	Privileged

아래 예제는 GigabitEthernet 0/1 에 대해 rmon alarm 을 설정합니다. GigabitEthernet 0/1 의 inOctets 값을 30 초마다 샘플링하며 rising-threshold 및 falling-threshold 를 벗어나면 각 설정된 event 를 발생시키도록 합니다. RMON alarm 의 alarm variable 설정 시 인터페이스 인덱스(ifindex)를 설정해야 하며, 인터페이스 인덱스 값은 “show interface [*IFNAME*]” 명령을 통해 참조할 수 있습니다.

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

```
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 0/1
Switch(config-if-Giga0/1)# rmon collection stats 1
Switch(config-if-Giga0/1)# end
Switch#show interface GigabitEthernet 0/1

Giga0/1 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 Giga0/1 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 같습니다. 아래 예제는 ifindex 가 101 인 인터페이스의 etherStatsOctets(etherStatsEntry.4) 값을 alarm 모니터링 하도록 설정하는 두 가지 방법을 나타낸다.

1) etherStatsOctets.101
2) etherStatsEntry.4.101

표 19-12. RMON History 설정 및 statistics 명령

명령어	설명	모드
rmon collection stats *index* [owner *string*]	물리적 인터페이스의 통계 값을 수집합니다. *Index*: etherStats 인덱스,	Interface
rmon collection history *index* [buckets *number*] [interval *seconds*] [owner *string*]	물리적 인터페이스에 대하여 이력을 수집합니다. *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 설정합니다.	Interface
no rmon collection history *index*	물리적 인터페이스의 이력을 수집하지 않도록 설정합니다.	Interface
show rmon history	RMON history 정보를 출력합니다.	Privileged
show rmon statistics	RMON statistics 정보를 출력합니다.	Privileged
rmon clear counters	해당 인터페이스의 statistics 값을 초기화합니다.	Interface

아래 예제는 GigabitEthernet 0/8 에 대해 10 초 마다 최대 30 개의 bucket 을 이용해 RMON 이력을 수집하도록 설정합니다.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/8
Switch(config-if-Giga0/8)# rmon collection stats 1
Switch(config-if-Giga0/8)# rmon collection history 1 buckets 30
interval 10
Switch(config-if-Giga0/8)# 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
```

19.5. Logging

E5224 Series 스위치 로그는 모든 환경 설정 정보와 경보 발생 정보를 보여 줍니다. 시스템 메시지 로깅 소프트웨어는 스위치의 메모리에 로그 메시지를 저장하며, 다른 디바이스로 메시지를 보낼 수 있습니다. 시스템 메시지 로깅 기능은 다음을 지원합니다.

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

E5224 Series 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI 를 사용하여 로깅되는 시스템 메시지를 제어할 수 있습니다. 최대 약 1000 개의 로그 메시지를 시스템 버퍼에 저장합니다. 시스템 운영자는 시스템 메시지를 Telnet 이나 콘솔을 통해서, 또는 syslog server 의 로그를 봄으로써 원격으로 모니터 할 수 있습니다.

E5224 Series 스위치는 0-7 까지의 Severity 레벨을 가지고 있습니다.

표 19-13. E5224 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.

19.5.1. 시스템 로그 메시지 내용

E5224 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 기록합니다.
- **Severity level**
  - <표 12>에서 정의한 E5224 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 입니다.

```
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
```

19.5.2. 디폴트 Logging 설정 값.

표 19-14. 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 19-15. 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 서버에 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.

19.5.3. Logging 설정 예.

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

```
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 설정합니다. Telnet session 으로 log message 출력을 중단하고자 할 경우 “logging session disable” command 를 사용합니다.

```
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 설정합니다. log server 로 log message 보내는 것을 중단하고자 할 경우 “no logging A.B.C.D” command 를 사용합니다.

```
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)#
```

19.5.4. Login logging 설정

E5224 Series 스위치의 기본 동작은 사용자의 로그인 성공 또는 실패 이벤트가 발생했을 때 로그를 출력하지 않으며 아래 명시한 명령으로 로그 출력 동작을 설정할 수 있습니다.

표 19-16. 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 설정합니다.
(no) login [on-failure|on-success] every	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 주기적으로 발생하는 로그 설정을 해제합니다.
login [on-failure|on-success] log	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 로그를 출력하도록 설정합니다.
(no) login [on-failure|on-success] log	로그인 동작에 대해 실패 또는 성공 이벤트가 발생했을 때 로그 출력 설정을 해제합니다.

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

```
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 출력합니다.

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 내용입니다.

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

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

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

20 Utilities

20.1. 개 요

본 장에서는 시스템 운영에 필요한 기타 기능들에 대해 설명하도록 합니다.

20.2. 상태 dump 명령

20.2.1. 명령어

각 모듈들(시스템 환경, MULTICAST, 라우팅, 드라이버 등)의 시스템 로깅 메시지를 dump 하기 위한 목적으로 “show tech-support” 명령을 사용합니다.

```
# 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 있습니다.

출력 메시지는 페이징이 되지 않기 때문에, 출력 메시지는 명령의 수행이 끝날 때까지 출력됩니다. 이 명령의 수행 도중에, 출력을 멈추기 위해서는 Ctrl+C 를 입력하여 중단시켜야 합니다.

다음의 예를 살펴보도록 합니다.
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 요청합니다.

```
Switch# show tech-support
```

```
        --- Display the system information ---
        --------------------------------------

MODEL-NAME        : E52
SERIAL-NO         : P00M0000000A
System MAC-ADDRESS: 00:07:70:74:ff:01


        --- Display the system version ---
        ---------------------------------


Ubiquoss Switch Operating System Software
E5224Software (E52), Version 3.3.7
Technical Support: http://www.ubiquoss.com
Copyright (c) 2001-2011 by Ubiquoss Inc.

BOOTLDR: E5224Software (u-boot-E52-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 ---
        -----------------------
...
```

20.3. Command history 기능

운용자에 의해 수행된 명령어를 명령어를 실행한 시간순서 또는 실행한 시간의 역순으로 출력하는 기능입니다. 이 기능을 사용하여 운용자가 실행한 명령의 조회가 가능하며 시스템 오동작시 원인 규명 및 복원이 편리하게 됩니다.

표 20-1. command history 조회 및 설정 명령어

명령어	설명	모드
show history	실행된 명령어들을 조회합니다.	Privileged
show history back	실행된 명령어들을 시간의 역순으로 조회합니다.	Privileged
show history detail	명령을 실행한 시간/user/접속 IP 를 추가적으로 표시합니다.	Privileged

같은 명령어를 반복하여 입력하는 경우는 한번만 저장됩니다.

20.4. Output Modifiers

20.4.1. Output Modifiers 개요

장비의 현재 상태 또는 설정을 보는 명령어는 대부분 show 로 시작합니다. show 명령은 대부분 한 화면에 보기 편하게 정리해서 보여주는 것이 일반적이나, 그 내용이 방대한 경우도 상당히 많습니다.

예를 들면, show mac-address-table 명령의 경우 수천 라인의 정보가 보여 질 수 있으며, show interface 명령의 경우에도 상당히 많은 분량의 내용이 출력됩니다. 출력되는 내용이 많을 경우, 이 내용 중에서 원하는 부분을 찾는 것은 쉽지 않다. 이럴 때 본 장비에서 지원하는 output modifiers 기능을 사용하면 편리합니다.

일반적으로 유닉스에서 pipe 라고 부르는 기능과 비슷하며, 본 장비에서는 3 가지의 미리 정의된 output modifiers 를 지원합니다. Output modifiers 기능을 사용하기 위해서는 show 명령 이후 bar (|) 를 이어 붙이고, 다음의 명령어를 사용하면 됩니다.

명령어	설명
| include WORD	특정 단어를 포함하는 문자열을 출력합니다.
| exclude WORD	특정 단어를 포함하지 않는 문자열을 출력합니다.
| begin WORD	특정 단어를 포함하는 문자열부터 그 이후에 나오는 모든 라인을 출력합니다.

20.4.2. Output Modifiers 예제

show mac-address-table 명령은 상당한 양의 결과를 출력하는데, 그 중 원하는 부분이 포함된 mac 주소만 출력하고자 할 때는 **include** 를 사용합니다.

```
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 사용합니다.

```
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
```

20.5. DDM (Digital Diagnostic Monitoring)

E5224 는 DDM 을 지원하는 GBIC 의 상태를 상세하게 사용자에게 보여주는 명령어를 지원합니다. Monitoring 항목은 다음과 같습니다.

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

20.5.1. GBIC DDM Monitoring

DDM 을 지원하는 gbic 에 한해 다음 명령어를 사용하여 gbic 의 현재 상태를 확인할 수 있습니다.

명령어	Mode	설명
show interface transceiver	Privileged	DDM 을 지원하는 gbic 의 상태를 확인합니다.

```
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)
  -------  -----------  -------  --------  --------  --------
  Gi0/1      49.2       3.31       0.0 --  -40.0 --   -7.2
  Gi0/2      48.8       3.30       0.0 --  -40.0 --   -6.3
  Gi0/1      50.2       3.32       0.0 --  -40.0 --  -40.0 --
.....................................................................
```

21 ErrDisable

이 장에서는 Error 발생 시 Interface 를 disable 시키는 Errdisable 기능에 대해서 설명합니다.

Notice

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

이 장은 다음의 절들로 구성됩니다:

- ErrDisable 특징
- ErrDisable Recovery

21.1. ErrDisable

ErrDisable state 와 어떻게 ErrDisable 상태가 되는지에 대해 설명합니다. 또한 ErrDisable state 가 된 Interface 복구 방법에 대해 설명합니다.

21.1.1. Understanding ErrDisable

Configuration 에 Port 가 enable 인 상태이지만, software 에서 Port 에 error 를 발생 시키며, softwarde 는 해당 port 를 shutdown 시킵니다. 즉, Port 는 switch operating system software 로 disable 상태가 되면 error disabled 상태가 되는 것 입니다.

Errdisabled 상태가 되면, Port 는 shut down 되어, traffice 송/수신이 불가능해 집니다. Port status show 는 err-disabled 로 표시 됩니다.

Errdisable 을 사용하는 이유는 아래와 같습니다.

- Administrator 가 언제 어느 port 에 문제가 생겼는지 알기 위해서 사용합니다.
- Error 가 발생한 모듈 때문에 다른 모듈에 영향을 줄 수 있기 때문에 사용합니다.

21.1.2. Causes of errdisable

다음의 원인으로 Errdisable 상태가 됩니다.

- UniDirectional Link Detection (UDLD) condition
- Self-Loop Detection (SLD) condition

Note: Error-disable detection 는 모든 원인에 대해 default 로 enable 되어 있습니다.

21.1.3. Recover a Port from Errdisabled State

Errdisable 상태가 된 Port는 아래 방법으로 Port를 re-enable 시켜야 합니다.

- 운용자가 shutdown 명령을 입력 후, no shutdown 명령을 입력
- errDisable auto recovery 기능을 이용

21.1.3.1. Re-enable (Maually)

Errdisable 상태가 된 Port 를 re-enable 하기 위한 설정을 설명합니다.

- 운용자가 shutdown 명령을 입력 후, no shutdown 명령을 입력

	Command	Purpose
Step1	**Configure terminal**	Global configuration 모드로 진입합니다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입합니다.
Step3	**shutdown**	administrative down 을 설정 합니다.
Step4	**no shutdown**	administrative down 설정을 해제 합니다.
Step5	**end**	privileged EXEC 모드로 변경합니다.

Note: Step3 에서 administarative down 을 설정하면, ErrDisable 정보가 clear 됩니다.

21.1.3.2. ErrDisable Auto Recovery

Errdisable 상태가 된 Port 를 자동으로 Re-enable 시키기 위한 설정을 설명 합니다.

- errDisable auto recovery 기능을 이용

	Command	Purpose
Step1	**Configure terminal**	Global configuration 모드로 진입합니다.
Step2	**errdisable recovery cause** *cause*	errDisable Auto Recovery 기능을 사용할 것인지 설정 합니다. - udld: UDLD 로 인해 errDisable 상태가 되면 Auto Recovery 기능을 사용 합니다. - sld: SLD 로 인해 errDisable 상태가 되면 Auto Recovery 기능을 사용 합니다.
Step3	**errdisable recovery interval** *interval*	(option) Recovery interval 을 설정합니다. (30~86400) 설정 되지 않으면 300 초가 default 값으로 설정 됩니다. 설정 시간 후 Port 는 Re-enable 됩니다.
Step4	**end**	privileged EXEC 모드로 변경합니다.

Note: ErrDisable Auto Recovery 기능은 default 로 disable 상태 입니다.

다음은 UDLD 에 의해 Port state 가 ErrDisable 상태가 되었을 때 Recovery 기능을 사용하겠다는 설정을 보여 줍니다. Recovery 시간은 600 초로 설정 합니다.

```
E52-24D(config)#errdisable recovery interval 600
E52-24D(config)#errdisable recovery cause udld
```

Errdisable Auto Recovery disable 명령에 관한 설명입니다.

	Command	Purpose
Step1	**Configure terminal**	Global configuration 모드로 진입합니다.
Step2	**no errdisable recovery cause** *cause*	errDisable Auto Recovery 기능을 사용하지 않도록 합니다. - udld: UDLD 로 인해 errDisable 상태가 되면 Auto Recovery 기능을 사용하지 않습니다. - sld: SLD 로 인해 errDisable 상태가 되면 Auto Recovery 기능을 사용하지 않습니다.
Step3	**no errdisable recovery interval**	Recovery interval 을 설정을 삭제 합니다.
Step4	**end**	privileged EXEC 모드로 변경합니다.

21.1.4. Displaying Errdisabled state

21.1.4.1. Port state 와 Show running-config

<표 21-1 >는 Port state 에 따라 Show running-config 에 보여지는 상태를 설명합니다.

표 21-1 Port Status 와 show state

State	show running-config
Normal	no shutdown
Administrative down	shutdown
Administrative up	no shutdown
errDisable	no shutdown

21.1.4.2. Displaying Errdisabled state

ErrDisable 의 port 상태를 조회하려면 privileged EXEC 명령 **show interface status err-disabled** 명령을 사용합니다.

```
Switch# show interface status err-disabled

ErrDisable status
Port     Name          Status       Reason
Gi0/13                 err-disabled UDLD
```

21.1.4.3. Displaying Errdisabled Recovery state

ErrDisable 의 Auto Recovery 기능을 사용하면 privileged EXEC **show errdisable recovery** 명령을 사용하여 조회 할 수 있습니다.

- Auto Recovery 기능 사용 전

```
E52-24D#show errdisable recovery
ErrDisable Reason              Timer Status
-----------------              ------------
udld                           Disabled
sld                            Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

- Auto Recovery 기능 사용 후

```
E52-24D#show errdisable recovery
ErrDisable Reason              Timer Status
-----------------              ------------
udld                           Enabled
sld                            Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
Interface      Errdisable reason      Time left(sec)
---------    ---------------------    --------------
Gi0/13       udld                     29
```

22

CPU-MAC-FILTER

이 장에서는 cpu 로 trafiic 이 과도하게 유입되어 시스템 성능이 저하 되는 현상을 방지하기 위해 cpu 의 과 부하를 유발하는 MAC 에 대해 차단 동작 하는 cpu-mac-filter 기능에 대하여 설명합니다.

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

이 장은 다음의 절들로 구성됩니다.

- CPU-MAC-FILTER

22.1. CPU-MAC-FILTER

cpu 의 과부하를 유발하는 traffic 에 대하여 해당 mac 을 filtering 하는 cpu-mac-filter 기능 의 설정 방법에 대하여 설명 합니다.

22.1.1. Understanding cpu-mac-filter

L2 switch 장비는 유입되는 traffic 에 대해 기본적인 flooding 이나 forwarding 동작 외에도 CPU 로 trap 되거나 mirror 시켜야 할 경우가 있습니다.

이러한 traffic 들은 일반적으로 control traffic 이라고도 불리우며 SNMP, HTTP, ICMP 와 같은 IP 관리를 위한 protocol 부터 mac address 정보를 획득하기 위한 ARP, Ipv6 Neighbor Solicitation, IEEE Reserved Multicast 등이 존재합니다.

위와 같은 switch 의 특성은 ICMP attack / mac attack 등 다양한 network 공격에 취약한 결과를 초래하게 됩니다.

따라서 CPU 부하를 야기시키는 mac 을 filtering 하여 시스템을 안정적으로 동작하도록 하는 기능이 CPU-MAC-FILTER 입니다.

22.1.2. Default cpu-mac-filter Configuration

다음의 표는 cpu-mac-filter 의 default 설정을 보여줍니다.

표 22-1 Default cpu-mac-filter Configuration

Feature	Default Setting
Cpu-mac-filter enable	No
Cpu-load	10 [%]
Block duration time	10 [min]
Packet Threshold for Blocking	100 [pkts/sec]

22.1.3. Configuring cpu-mac-filter

이 절에서는 스위치에 cpu-mac-filter 감지 기능을 설정하는 방법을 설명 합니다.

- Changing cpu-mac-filter cpu-load
- Changing cpu-mac-filter duration
- Changing cpu-mac-filter packet-threshold
- Enabling cpu-mac-filter

22.1.3.1. Changing cpu-mac-filter cpu-load

Cpu-load 는 설정은 몇 % 의 usage 부터 cpu 부하로 판단, mac 을 filtering 할 것인가에 대한 기준을 정하는 과정 입니다. 입력된 cpu-load 는 5 분 동안의 평균 cpu usage 와 비교 되어 지며 기본값은 10 [%] 으로 설정 되어 있습니다.

설정을 변경하려면, privileged EXEC 모드에서 다음의 과정을 거칩니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**Cpu-mac-filter cpu-load** *<1-99>*	cpu-load 의 threshold 값을 설정 합니다. 설정된 값은 5 분 동안의 평균 cpu 값과 비교 되어 진다.
Step3	**End**	privileged EXEC 모드로 변경합니다.
Step4	**show running-config**	설정 내용을 확인합니다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

설정을 해체 / 기본값으로 변경 하기 위해서는 config 모드에서 **no cpu-mac-filter cpu-load** 을 입력합니다.

22.1.3.2. Changing cpu-mac-filter duration

Duration 설정은 filtering 된 mac address 를 다시 정상적으로 동작하기까지의 시간을 설정하는 과정입니다.
즉, cpu 부하의 원인이라고 판단 되어진 특정 mac 에 대하여 얼마 시간동안 blocking 시킬 것인가를 정하는 parameter 입니다.

기본값은 10 [min] 이며 설정을 변경하려면, privileged EXEC 모드에서 다음의 과정을 거칩니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**Cpu-mac-filter duration** *<1-1440>*	Packet 을 차단하고자 하는 blocking time 값을 설정 합니다.
Step3	**End**	privileged EXEC 모드로 변경합니다.
Step4	**show running-config**	설정 내용을 확인합니다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

설정을 해체 / 기본값으로 변경 하기 위해서는 config 모드에서 **no cpu-mac-filter duration** 을 입력합니다.

22.1.3.3. Changing cpu-mac-filter packet-threshold

Packet-threshold 는 설정은 몇 초당 몇 개의 packet 이 cpu 로 유입시 mac 을 filtering 할 것인가에 대한 기준을 정하는 과정 입니다. packet-threhold 기본값은 100 [pkts/sec] 입니다.

설정을 변경하려면, privileged EXEC 모드에서 다음의 과정을 거칩니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**Cpu-mac-filter packet-threshold** *<1-5000>*	Packet threshold 를 설정합니다.
Step3	**End**	privileged EXEC 모드로 변경합니다.
Step4	**show running-config**	설정 내용을 확인합니다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

설정을 해체 / 기본값으로 변경 하기 위해서는 config 모드에서 **no cpu-mac-filter packet-threshold** 을 입력합니다.

22.1.3.4. Enabling cpu-mac-filter

Cpu-mac-filter 는 vlan interface 별로 enable / disable 설정이 가능합니다.
또한 packet type 별 (unicast, multicast, broadcast) 설정이 가능하며 3 가지 type 에 대해서 동시에 설정도 가능합니다.
Cpu-mac-filter 를 enable 하는 명령은 다음과 같습니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**interface** *vlan-id*	Vlan interface 로 진입합니다.
Step3	**Cpu-mac-filter** *{multicast / unicast / broadcast}*	각 type 별로 cpu-mac-filter 를 설정 합니다.
Step4	**End**	privileged EXEC 모드로 변경합니다.
Step5	**show running-config**	설정 내용을 확인합니다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

설정을 해체 하기 위해서는 config 모드에서 **no cpu-mac-filter** *{multicast | unicast | broadcast}* 을 입력합니다.

22.1.4. Displaying cpu-mac-filter Status

CPU-MAC-FILTER 설정 정보를 조회하려면, privileged EXEC 명령 **show running-config** 나 **show cpu-mac-filter information** 명령을 사용하세요.

```
Switch# show cpu-mac-filter information


 MAC BLOCKING based on CPU load Information
-----------------------------------------------------------
 Blocking Duration Time         : 10 min
 CPU Load Threshold for Blocking: 10 %[5min avg]
 Packet Threshold for Blocking  : 100[Pkts/sec]


CPU-MAC-FILTER Enabled Interface
      VLAN       ENABLE  BROADCAST  MULTICAST
-----------------------------------------------------------
   Vlan100               ENABLE     ENABLE
```

23

SLD (Self-loop Detection)

이 장에서는 자신이 전송한 패킷이 되돌아 오는 현상을 감지하는 self-loop 감지 기능을 설정하는 방법을 설명합니다.

Notice

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

이 장은 다음의 절들로 구성됩니다:

- Self-loop Detection

23.1. Self-loop Detection

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

23.1.1. Understanding Self-loop Detection

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

스위치가 자신의 한 포트로 전송한 패킷이 다시 그 포트로 되돌아오는 현상을 self-loop 이라고 합니다. 다음의 그림들은 self-loop 이 발생하는 구성에 대한 예제입니다.

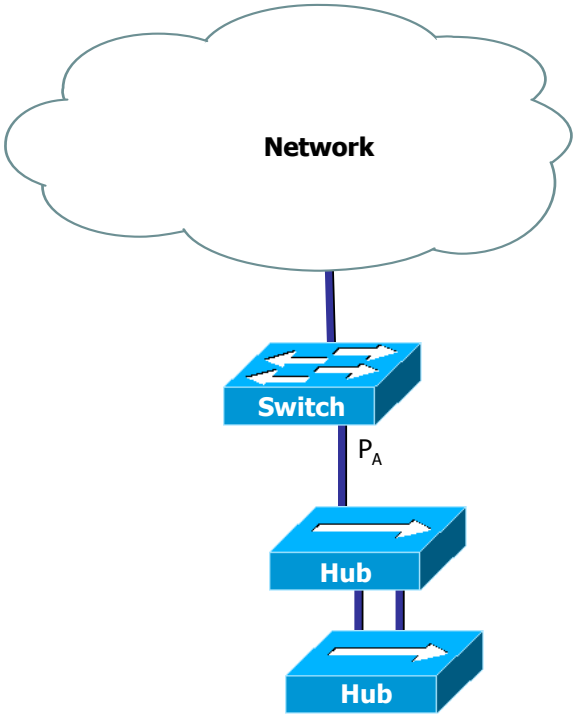


그림 23-1 Self-loop 발생 환경

<그림 23-1> 에서 두 hub 사이에 이중 경로에 의한 loop 이 존재합니다. 네트워크 loop 방지 기능이 사용되지 않은 상태이기 때문에 hub 사이의 loop 은 제거되지 않으며 network 의 불안정을 초래하게 됩니다. 이 경우 스위치가 포트 P_A 를 통해 전송한 패킷은 다시 P_A 로 수신됩니다. 스위치에 self-loop 감지 기능이 활성화되어 있다면, 포트 P_A 에 self-loop 이 있다는 것을 감지하고 포트 P_A 를 서비스 불가능 상태 (Port errDisabled state)로 만들어 스위치와 포트 P_A 와 연결되지 않은 다른 네트워크를 보호할 수 있습니다. 포트 P_A 에 연결된 장비와 네트워크에는 여전히 loop 가존재합니다.
(네트워크에서 완전한 loop 의 제거를 원한다면 장비간 연동이 가능한 표준 loop 방지 프로토콜을 사용해야 합니다).

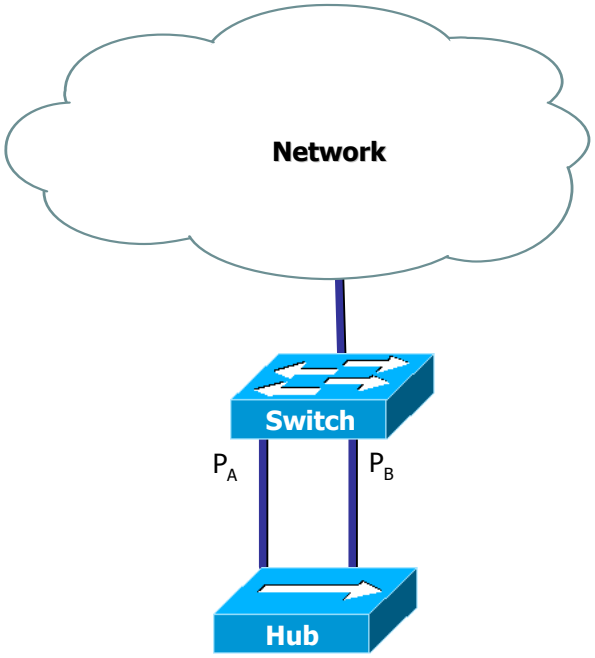


그림 23-2 Self loop 발생 환경 2

그림 2 에서 switch 포트들 간에 loop 이 존재합니다. 네트워크 loop 방지 기능이 활성화 되지 않은 상태일 경우 포트사이의 loop 은 제거되지 않으며 network 의 불안정을 초래하게 됩니다. 이 경우 스위치가 포트 P_A 를 통해 전송한 패킷은 다시 P_B 로 수신되고 포트 P_B 를 통해 전송한 패킷이 다시 P_A 로 수신됩니다. 스위치에 self-loop system 감지 기능이 활성화되어 있다면, 포트 P_A 와 P_B 간에 self-loop 이 있다는 것을 감지하고 포트 P_A 와 P_B 를 서비스 불가능 상태 (port errDisabled state)로 만들어 스위치와 포트 P_A, P_B 와 연결되지 않은 다른 네트워크를 보호하게 됩니다.

23.1.2. Default SLD Configuration

다음의 표는 SLD 의 default 설정을 나타냅니다.

표 23-1 Default SLD Configuration

Feature	Default Setting
System SLD enable	Disable
Interface SLD enable	Disable
Loop detection action	Port shutdown
Port check	Disable
Hello time	2 초

23.1.3. Configuring Self-loop Detection

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

- Configuring SLD PDU Policy-MAP
- Enabling Self-loop Detection on System
- Enabling Self-loop Detection on Interface
- Changing The Service Status of Port
- Disabling Self-loop Detection
- Disabling SLD Port Check (option)
- Changing SLD Interval (option)
- Changing SLD Action (option)

23.1.3.1. Configurring SLD PDU Policy-MAP

스위치가 SLD PDU 를 수신하도록 하기 위해서 policy map 설정이 필요합니다.

자신의 전송한 SLD PDU 만을 수신하기 위해 MAC ACL 을 설정합니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**mac-access-list** *access-group-name* **permit** *source-mac mask destination-mac make* **8**	자신의 MAC 을 soucrce MAC 으로 가진 SLD PDU 만 수신하도록 합니다. - access-group-name: mac-access-list 로 사용 될 이름을 지정합니다. (<1100-1199> extended mac ACL) - source-mac: 장비의 MAC address 로 설정합니다. - Destination-mac: SLD 의 Destination MAC 인 Broadcast 로 설정 합니다. (ffff.ffff.ffff)
Step3	**end**	privileged EXEC 모드로 변경합니다.

SLD PDU 를 수신하기 위한 class-map 을 설정합니다

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**Class-map** *class-map-name*	class-map 을 생성합니다.
Step3	**match access-group** *group-name*	MAC ACL 을 설정합니다.
Step4	**match ethertype *0807***	SLD 의 EtherType 을 설정 합니다.
Step5	**match tag-type *untagged***	SLD 는 항상 untagged 이므로 untagged 를 설정합니다.

policy-map 을 설정합니다:

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**policy-map** *policy-map-name*	policy-map 을 생성합니다.
Step3	**class** *class-map-name*	class-map 을 지정합니다.
Step4	**trap-cpu [high-priority]**	Policy-map action 으로 CPU TRAP 을 설정합니다. * trap-cpu 적용 시 0 번 queue 를 통해 수신됩니다. trap-cpu high-priority 적용 시 6 번 queue 로 수신됩니다.

다음은 0007.701A.2EF3 장비에서 SLD PDU 수신을 위한 policy-map 설정 예제입니다.

```
!
mac-access-list 1100 permit 0007.701a.2ef3 0000.0000.0000 ffff.ffff.ffff 0000.00
00.0000 8
!
class-map U_SLD
 match access-group 1100
 match ethertype 0807
 match tag-type untagged
!
policy-map SLD_PDU
 class U_SLD
  trap-cpu high-priority
```

23.1.3.2. Enabling Self-loop Detection on System

스위치의 SLD 기능을 활성화 하려면, privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**sld enable**	시스템의 SLD 기능을 활성화 합니다. SLD 기능을 활성화 하려면 반드시 이설정을 해야 합니다.
Step3	**end**	privileged EXEC 모드로 변경합니다.
Step4	**show running-config**	설정 내용을 확인합니다.
Step5	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

23.1.3.3. Enabling Self-loop Detection on Interface

SLD 기능은 각 포트 별로 기능의 활성화가 가능합니다. default 는 SLD 기능이 비활성 상태입니다.
SLD 기능을 활성화 하려면 privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입합니다.
Step3	**sld enable**	SLD 기능을 활성화 합니다.
Step4	**service-policy input** *policy-map-name*	policy-map 을 적용 합니다.
Step5	**end**	privileged EXEC 모드로 변경합니다.
Step6	**show running-config**	설정 내용을 확인합니다.
Step7	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

다음은 포트 gi1/1 에 SLD 기능을 활성화 하는 방법을 보여줍니다

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# sld enable
Switch(config-if-Giga1/1)# service-policy input SLD_PDU
Switch(config-if-Giga1/1)# end
Switch# show sld
```

```
Interface  Enable  Flag  Sts   Link  Count  Last change
Gi1/1      yes     PL    ok    up    0      00:00:02
Gi1/2      no      PL    n/a   down  0      n/a
Gi1/3      no      PL    n/a   down  0      n/a
Gi1/4      no      PL    n/a   down  0      n/a
……
Switch#
```

23.1.3.4. Changing The Service Status of Port

SLD 기능에 의해 서비스 불가능 상태가 된 포트를 수동으로 서비스 가능 상태로 만들 수 있습니다.
포트를 서비스 가능 상태로 만들려면 privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	Purpose
Step1	**clear sld** *interface-type portID*	포트를 서비스 가능 상태로 변경합니다.
Step2	**show ip interface brief**	포트의 상태정보를 확인합니다.

23.1.3.5. Disabling Self-loop Detection

SLD 감지 기능을 비활성화 하려면 privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입합니다.
Step3	**no service-policy input** *policy-map-name*	policy-map 을 삭제 합니다.
Step4	**no sld enable**	SLD 감지 기능을 비활성화 합니다. SLD 에 shutdown 된 포트는 shutdown 이 해제됩니다.
Step5	**end**	privileged EXEC 모드로 변경합니다.
Step6	**show running-config**	설정 내용을 확인합니다.
Step7	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

다음은 포트 gi1/1 에 SLD 기능을 비 활성화 하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# no service-policy input SLD_PDU
Switch(config-if-Giga1/1)# no sld enable
Switch(config-if-Giga1/1)# end
Switch# show sld
Interface  Enable  Flag  Sts   Link   Count  Last change
Gi1/1      no      PL    ok    up       0    n/a
Gi1/2      no      PL    n/a   down     0    n/a
Gi1/3      no      PL    n/a   down     0    n/a
Gi1/4      no      PL    n/a   down     0    n/a
……
Switch#
```

23.1.3.6. Disabling SLD Port Check

포트의 SLD port-check 기능을 해제하면 Self-loop 판단시에 SLD 패킷의 송수신 port 검사를 하지 않습니다. 다른 포트에서 전송된 SLD 패킷을 수신했을 경우 loop 으로 감지하려면 관련 포트들의 port-check 기능을 해제해야 합니다. SLD port-check 기능을 비활성화 하려면 privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입합니다.
Step3	**no sld port-check**	SLD port-check 기능을 비 활성화 합니다.
Step4	**end**	privileged EXEC 모드로 변경합니다.
Step5	**show running-config**	설정 내용을 확인합니다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

다음은 포트 gi1/1 에 SLD port-check 기능을 비 활성화 하는 방법을 보여줍니다:

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# no sld port-check
Switch(config-if-Giga1/1)# end
Switch# show sh sld parameters
Global SLD information:
                Protocol version: 1
                SLD is enabled

Interface  Enable  Hello  Action     Option
Gi1/1      yes       2   link down
Gi1/2      no        2   link down  port-check
Gi1/3      no        2   link down  port-check
Gi1/4      no        2   link down  port-check
……
Switch#
```

23.1.3.7. Changing SLD Interval

SLD PDU 의 전송 주기를 변경 하려면 privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	Purpose
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입합니다.
Step3	**sld interval** *<1-10>*	SLD pdu 의 전송 주기를 변경 합니다.
Step4	**end**	privileged EXEC 모드로 변경합니다.
Step5	**show running-config**	설정 내용을 확인합니다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

다음은 포트 gi1/1 에 SLD pud 의 전송 주기를 5 초로 변경하는 방법을 보여줍니다.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# sld interval 5
Switch(config-if-Giga1/1)# end
Switch# show sh sld parameters
Global SLD information:
                Protocol version: 1
                SLD is enabled

Interface  Enable  Hello  Action     Option
Gi1/1      yes       5   link down  port-check
Gi1/2      no        2   link down  port-check
Gi1/3      no        2   link down  port-check
Gi1/4      no        2   link down  port-check
……
Switch#
```

23.1.3.8. Changing SLD Action

Self-loop dictection 시에 포트를 서비스 불능 상태로 하지 않고, 로그만 출력하도록 SLD 동작을 변경하려면 privileged EXEC 모드에서부터 다음의 과정을 수행합니다.

	Command	**Purpose**
Step1	*Configure terminal*	Global configuration 모드로 진입합니다.
Step2	**interface** *interface-name*	Interface configuration 모드로 진입합니다.
Step3	**sld notify-only**	SLD 동작을 로그만 출력하도록 변경합니다.
Step4	**end**	privileged EXEC 모드로 변경합니다.
Step5	**show running-config**	설정 내용을 확인합니다.
Step6	**copy running-config startup-config**	(옵션) 설정을 configuration 파일에 저장합니다.

다음은 포트 gi1/1 에 SLD 동작을 로그만 출력하도록 변경하는 방법을 보여줍니다.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# sld notify-only
Switch(config-if-Giga1/1)# end
Switch# show sh sld parameters
Global SLD information:
                Protocol version: 1
                SLD is enabled

Interface  Enable  Hello  Action     Option
Gi1/1      yes       2   notify     port-check
Gi1/2      no        2   link down  port-check
Gi1/3      no        2   link down  port-check
Gi1/4      no        2   link down  port-check
……
Switch#
```

23.1.4. Displaying Self-loop Status

포트의 SLD 기능 설정 상태를 조회하려면, privileged EXEC 명령 **show running-config** 나 **show sld parameter** 명령을 사용하세요.

show self-loop-detection 에서

- ifname : Interface name (Port name)
- ld : self-loop-detection 설정 (set 또는 sys)
- link : link 의 상태 (up, down)
- shutdown : SLD 에 의한 shutdown (block)
- set_time : SLD 에 의한 limit time (minutes). 만약 0 min 이라면 SLD 에 의해 shutdown 된 후, 수동으로 해당 Port 를 no shutdown 하기 전까지 계속 shutdown 상태로 유지됩니다.
- remain_time : SLD 에 의한 shutdown 시 정상으로 복귀되기 까지 남은 시간(minute:second)
- count : SLD 에 의한 shutdown 횟수
- last-occur : 마지막으로 SLD 에 의해 shutdown 된 시간

```
Switch# show sld parameters
Global SLD information:
                Protocol version: 1
                SLD is enabled

Interface  Enable  Hello Action     Option
Gi1/1      no          2 link down  port-check
Gi1/2      no          2 link down  port-check
Gi1/3      no          2 link down  port-check
Gi1/4      no          2 link down  port-check
……
Switch#
```

SLD 의 동작상태를 조회하려면 privileged EXEC 명령 **show sld** 명령을 사용하세요.

```
Switch# show sld
Interface  Enable  Flag  Sts   Link Count  Last change
Gi1/1      no      PL    n/a   up       0  n/a
Gi1/2      no      PL    n/a   down     0  n/a
Gi1/3      no      PL    n/a   down     0  n/a
Gi1/4      no      PL    n/a   down     0  n/a
……
Switch#
```