SFC6000 시리즈

사용자 설명서

SFC6006

SFC6010

목차

19 장. 네트워크 프로토콜 설정

20 장. 라우팅 설정

1장. 설정 준비

이 문서는 포트 번호, 설정 하기 전에 필요한 절차 및 명령어를 입력 할 인터페이스의 소개를 포함하여 스위치를 처음 구성할 때 필요한 정보를 제공 합니다.

1.1 스위치 포트 번호

스위치 실제 포트 번호는 <Type> <Slot>/<Port> 형식으로 되어있으며 다음 비교 표의 유형 및 이름을 적어 놓았습니다.

인터페이스 형태	이름	축약표시
10M Ethernet	Ethernet	E
100M Ethernet	Fast Ethernet	F
1000M Ethernet / 1GigaEthernet	Giga Ethernet	G
10GigaEthernet	TGiga Ethernet	T

표준 구성의 확장 슬롯 번호는 항상 0 입니다. 나머지는 1에서 시작하여 왼쪽에서 오른쪽으로 계속 됩니다.

동일한 확장 슬롯의 포트 번호는 아래에서 위로, 왼쪽에서 오른쪽으로 1부터 시작하여 번호가 매겨 집니다.

Note.

모듈의 포트는 아래에서 위로, 왼쪽에서 오른쪽으로 순서대로 번호가 지정 됩니다.

1.2 시작 전 점검 사항

스위치를 켠 후 설정을 하기 전에 다음단계를 확인하십시오.

- 수동으로 스위치에 설정을 합니다.
- PC 터미널 프로그램을 실행 후 설정 합니다.
- IP 네트워크의 프로토콜에 따라 IP 주소 계획을 세웁니다.

1.3 도움말 얻기

물음표(?) 또는 방향 키를 사용하면서 모든 명령에 대한 관련 정보를 얻을 수 있습니다.

- 현재 명령 모드에서 사용할 수 있는 모든 명령을 나열하려면 물음표를 입력하십시오.

  Switch> ?

- 알고있는 문자를 입력하고 물음표(공백없이)를 입력 하여 현재 알려진 문자로 시작하는 명령어 목록을 얻을 수 있습니다.

Switch> s?

- 명령어를 입력 한 다음 공백과 물음표를 입력 하여 명령 매개변수 목록을 가져옵니다.

Switch> show ?

- 위쪽 화살표 키를 누르면 이전에 입력한 명령어가 표시 됩니다. 위쪽 화살표 키를 계속 누르면 입력한 더 많은 명령어를 볼 수 있으며, 아래쪽 키를 누르면 현재 명령어 다음에 나오는 명령어를 볼 수 있습니다.

1.4 명령어 모드

명령어 라인의 인터페이스에는 다양한 모드가 있습니다. 다른 명령어 모드를 사용하여 스위치의 다른 구성 요소를 구성 할 수 있습니다. 사용 가능한 명령은 현재 사용중인 모드에 따라 다릅니다. 물음표(?)를 입력하면 주어진 모드에서 적용 가능한 명령 목록을 얻을 수 있습니다. 다음 표에서는 자주 사용되는 명령 모드 입니다.

명령어 모드	접근 방법	인터페이스 형식	종료 방법
감시 모드 (Moniter Mode)	전원을 켠 후 "Ctrl+p"를 입력	Monitor#	Type "**quit**"
사용자 모드 (User Mode)	로그인	Switch>	Type "**exit**" or "**quit**"
관리자 모드 (Admin Mode)	사용자 모드에서 "input" 또는 "enable" 명령어를 입력	Switch#	Type "**exit**" or "**quit**"
구성 모드 (Global Mode)	관리자 모드에서 "config" 명령어를 입력	Switch_config#	Type "**exit**" or "**quit**" "**Ctrl+z**"으로 관리자 모드로 돌아갑니다.
인터페이스 설정 모드	구성 모드에서 interface 명령어를 입력 하십시요.	Switch_config_f0/1#	Type "**exit**" or "**quit**" "**Ctrl+z**"으로 관리자 모드로 돌아갑니다.

제한된 명령의 하위 명령어는 각 명령 모드에서 사용할 수 있습니다.

명령어를 입력 하는데 문제가 있으면 인터페이스 형식을 확인하고 물음표(?)를 입력 하여 사용 가능한 명령어 목록을 찾으십시오.

잘못된 명령 모드 이거나 잘못된 구문을 사용 중일 수 있습니다.

다음 예시에서 시스템 프롬프트 변경, 명령모드 변경을 나타냅니다.

Switch> enter

Password: <enter password>

```
Switch# config
Switch_config# interface f0/1
Switch_config_f0/1# quit
Switch_config# quit
Switch#
```

1.5 명령어 취소

명령어를 취소하거나 기본 설정으로 돌아가려면 키워드를 추가 하십시오.

명령어 앞에는 없습니다.

예를 들어, **no ip routing**

1.6 설정 저장

시스템 재시작 또는 전원 차단 시 원래 구성을 복구 할 수 있도록 구성 변경 사항을 저장해야 합니다. **write** 명령어를 사용하여 관리모드 또는 구성 모드에서 구성을 저장 할 수 있습니다.

2장. 기본설정 시스템 관리 설정

2.1.1파일 관리 설정

2.1.1.1 파일 시스템 관리

플래시 메모리에 저장되는 파일의 이름은 20자를 넘지 않으며 파일 이름은 대소문자를 구분하지 않습니다.

2.1.1.2 파일 시스템 명령어

모든 명령어는 굵은 글씨체 이며 기타는 매개변수 입니다.
꺾쇠 괄호"[ ]"의 내용은 선택 사항입니다.

명령어	**설명**
format	파일 시스템을 포맷 하고 모든 데이터를 삭제합니다.
dir [파일명]	파일 및 디렉토리 이름을 표시 합니다. "[]"기호 안의 파일 이름은 여러 문자로 시작하는 파일을 표시하는 것을 의미 합니다. 파일은 다음 형식으로 표시 됩니다. 색인번호 파일이름 <파일> 길이 설정된 시간
delete 파일명	파일을 삭제합니다. 파일이 존재하지 않으면 시스템에서 표현합니다.
md dir이름	디렉토리를 만듭니다.
rd dir이름	디렉토리를 삭제 합니다. 디렉토리가 존재하지 않으면 시스템에서 표현합니다.
more 파일명	파일의 내용을 표시합니다. 파일 내용을 한 페이지로 표시 할 수 없는 경우 페이지별로 표시 됩니다.
cd	현재 파일 시스템의 경로를 변경합니다.
pwd	현재 경로를 표시합니다.

2.1.1.3 수동으로 파일 시작

monitor#boot flash <*local_Filename*>

이전 명령은 여러 스위치 소프트웨어가 포함될 수 있는 플래시에서 스위치 소프트웨어를 시작하는 것입니다.

매개변수 설명

매개변수	**설명**
Local_filename	플래시 메모리에 저장된 파일 이름으로 사용자는 파일 이름을 입력해야 합니다.

설정 예제

monitor#boot flash switch.bin

2.1.1.4 소프트웨어 업데이트

사용자는 이 명령어를 사용하여 스위치 시스템 소프트웨어를 로컬 또는 원격으로

다운로드하여 버전 업데이트 또는 사용자 정의 기능 버전(예: 데이터 암호화 등)을 얻을 수 있습니다. 모니터 모드에서 소프트웨어 업데이트에는 두가지 방법이 있습니다.

1) TFTP를 통한 업데이트

monitor#copy tftp flash [*ip_addr*]

이 명령어는 TFTP 서버의 파일을 시스템의 플래시로 복사하는 것입니다. 명령을 입력하면 시스템은 원격 서버 이름과 원격 파일 이름을 입력하라는 메시지를 표시 합니다.

매개변수 설명

매개변수	**설명**
Ip_addr	TFTP 서버의 ip 주소 입니다. 지정된 IP주소가 없으면 복사명령이 실행된 후 IP주소를 입력하라는 메세지가 나타납니다.

설정 예제

다음 예제는 서버에서 읽은 **main.bin** 파일이 서버에서 읽히고 스위치에 저장되는 파일명은 **switch.bin**으로 변경 하여 저장하는 것을 보여줍니다.

```
monitor#copy tftp flash
Prompt: Source file name[]?main.bin
Prompt: Remote-server ip address[]?192.168.20.1
Prompt: Destination file name[main.bin]?switch.bin
Please wait ....
####################################################################
TFTP:successfully receive 3377 blocks ,1728902 bytes
```

2) 직렬 포트 통신 프로토콜 – zmodem

터미널 프로그램은 WINDOWS 95, NT 4.0의 하이퍼 터미널 프로그램 이거나 WINDOWS 3.X의 터미널 에뮬레이션 프로그램 일 수 있습니다.

monitor#download c0 switch.bin

Prompt: speed[9600]?115200

속도를 115200으로 수정하십시오. 다시 연결한 후 하이퍼터미널(터미널에뮬레이션)의 전송 메뉴에서 파일 전송을 선택하십시오. 파일 보내기 대화상자가 다음과 같이 나타납니다.

그림 1-1. 파일 보내기

자사에서 제공하는 스위치 소프트웨어 "main.bin'의 전체 경로를 파일이름 입력 상자에 입력하고 Zmodem을 프로토콜로 선택하십시오. 파일을 보내려면 보내기를 클릭하십시오,

파일 전송하면 다음 정보가 나타납니다.

ZMODEM: Successfully receive 36 blocks ,18370 bytes

소프트웨어 업데이트가 완료 되었다는 것을 나타내며 하이퍼터미널
(터미널에 뮬레이션)의 전송속도는 9600으로 재설정 되어야 합니다.

2.1.1.5 설정 업데이트(장비의 Configuration Update)

스위치 구성은 파일로 저장되고 파일 이름은 startup-config 입니다. 소프트웨어 업데이트와 유사한 명령을 사용하여 구성을 업데이트 할 수 있습니다.

1) TFTP를 통한 업데이트

monitor # copy tftp flash startup-config

2) 직렬 포트 통신 프로토콜 – zmodem

monitor#download c0 startup-config

2.1.1.6 FTP를 사용하여 소프트웨어 및 설정 업데이트

config #copy ftp flash [*ip_addr* | *option*]

FTP를 사용하여 공식프로그램 관리에서 소프트웨어 및 설정을 업데이트 하십시오. "**copy**" 명령어를 사용하여 FTP서버에서 스위치로 파일을 다운로드 하고, 스위치의 파일 시스템에서 FTP 서버로 파일을 업로드 하십시오. 명령을 입력하면 시스템에서 원격 서버 이름과 원격 파일 이름을 입력하라는 메시지를 표시 합니다.

copy{ftp:[[[//login-name:[login-password]@]location]/directory]/filename}|flash:filename>}{flash<:filename>|ftp:[[[//login-name:[login-password]@]location]/directory]/filename}<blksize><mode><type>

매개변수 설명

매개변수	설명
login-nam	FTP 서버의 사용자 이름 지정된 사용자의 이름이 없으면 **"Copy"** 명령을 실행 한 후 사용자 이름을 입력하라는 메시지가 나타납니다.
login-password	FTP 서버의 비밀번호 지정된 암호가 없으면 **"Copy"** 명령을 실행 한 후 암호를 입력하라는 메세지가 나타납니다.
nchecksize	파일 크기는 서버에서 확인 되지 않습니다.
vfr	MPLS를 지원하는 장치에 대해 vrf 바인딩 기능을 제공합니다.
blksize	데이터 전송 블록의 크기 (기본값: 512)
ip_addr	FTP 서버의 IP 주소 지정된 IP주소가 없으면 **"Copy"** 명령을 실행 한 후 IP 주소를 입력하라는 메시지가 나타납니다.
active	활성 모드에서 FTP서버에 연결하는 것을 의미합니다.
passive	수동 모드로 FTP서버에서 연결하는 것을 의미합니다.
type	데이터 전송 모드 설정합니다.(ascii or binary)

설정 예제

다음 예제는 "main.bin" 파일이 서버에서 읽히고 스위치에서 switch.bin으로 변경되었음을 보여줍니다.

config#copy ftp flash
Prompt: ftp user name[anonymous]? login-nam
Prompt: ftp user password[anonymous]? login-password
Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1
Prompt: Destination file name[main.bin]?switch.bin
or

config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
###
###
FTP:successfully receive 3377 blocks ,1728902 bytes
config#

Note:

1) FTP서버가 작동하지 않을 때 대기 시간이 길어집니다. 이 문제는 TCP 시간 종료 시간(기본 75S)으로 인해 발생하면 TCP 연결 시간을 수정하기 위에 "ip tcp synwait-time" 글로벌 모드에서 명령을 구성 할 수 있습니다.

   하지만. 사용하지 않는 것이 좋습니다.

2) 일부 네트워크 통신의 조건에서 FTP를 사용하면 데이터 전송 속도가 상대적으로 느릴 수 있습니다. 최상의 효과를 얻으려면 전송 블록의 크기를 적절하게 조정 할 수 있습니다. 기본 크기는 512이며 대부분의 네트워크에서 비교적 높은 작동 속도를 보장합니다.

2.1.2 기본 시스템 관리 설정

2.1.2.1 이더넷 IP 주소 설정

monitor#ip address <*ip_addr*> <*net_mask*>

이 명령은 이더넷의 IP 주소를 구성합니다.
기본 주소는 192.168.0.1 이고 <net_mask>는 24bit 입니다.

매개변수 설명

매개변수	설명
ip_addr	이더넷의 IP 주소 입니다.
net_mask	이더넷의 서브넷 마스크 입니다.

설정 예제

monitor#ip address 192.168.1.1 255.255.255.0

2.1.2.2 디폴트 라우트 설정

monitor#ip route default <*ip_addr*>

이 명령은 기본 경로를 구성하는데 사용됩니다. 기본 경로는 하나만 구성 할 수 있습니다.

매개변수 설명

매개변수	설명
ip_addr	게이트웨이의 IP 주소 입니다.

설정 예제

monitor#ip route default 192.168.1.1

!

monitor#ip route default 192.168.0.254

2.1.2.3 Ping을 이용하여 네트워크 연결 상태 테스트

monitor#ping <*ip_address*>

이 명령은 네트워크의 연결 상태를 테스트 하는 것입니다.

매개변수 설명

매개변수	설명
ip_addr	목적지의 IP 주소 입니다.

설정 예제

monitor#ping 192.168.20.100

PING 192.168.20.100: 56 data bytes

64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
----192.168.20.100 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0

2.1.3. HTTP 설정

2.1.3.1 HTTP 설정

- HTTP 서비스의 활성화
- HTTP 서비스의 수신 대기 포트 번호 수정
- HTTP 서비스의 액세스 비밀번호 지정 설정
- HTTP 서비스에 대한 액세스 제어 목록

1) http 서비스를 활성화 합니다.

HTTP 서비스는 기본적으로 비활성화 되어 있습니다.
HTTP 서비스는 다음 명령어를 사용하여 글로벌 모드에서 구성을 활성화 합니다.

명령어	기능
ip http server	http 서버를 활성화 합니다.

2) HTTP 서비스의 수신 대기 포트 번호 수정 합니다.

HTTP 서비스의 수신대기 포트는 80 입니다. HTTP 서비스의 포트 번호는 글로벌 모드에서 다음 명령어를 이용하여 변경/설정이 가능 합니다.

명령어	기능
ip http [port number]	http 서비스의 수신대기포트를 변경 설정 합니다.

3) HTTP 서비스의 password 접속 설정하기

HTTP는 액세스 암호로 enable을 사용합니다. HTTP 액세스에 대한 인증을 수행하려면 암호 사용을 설정해야 합니다. 암호 enable은 다음 명령을 사용하여 글로벌 모드에서 설정 됩니다.

명령어	기능
enable password [line]	HTTP enable 비밀번호를 설정 합니다.

4) HTTP 서비스에 대한 액세스 제어 목록 지정

HTTP 서버에 대한 호스트의 액세스를 제어하기 위해 다음에 대한 액세스 제어 목록을 지정할 수 있습니다. HTTP 서비스의 액세스 제어 목록을 지정하려면 글로벌 모드에서 다음 명령어를 사용하십시오

명령어	기능
Ip http access-class STRING	http에 대한 액세스 제어 목록을 지정합니다.

2.3.1.2 HTTP 설정 예제

다음 예제에서는 http 서비스 포트로 기본 포트(80)을 사용하고 액세스 주소는 192.168.20.0/24로 제한됩니다.

- **Access control List 설정**

  ip access-list standard http-acl
  permit 192.168.20.0 255.255.255.0

- **글로벌 모드에서의 설정**

  ip http access-class http-acl
  ip http server

2-2장. 터미널 설정

2.2.1 VTY 설정

시스템은 **"line"** 명령어를 사용하여 터미널 매개변수를 구성 합니다.
이 명령을 통해 터미널에 화면에 표시되는 구성을 조절 할 수 있습니다.

2.2.2 설정 내용

이 시스템에는 접속 가능한 방법은 4가지의 유형이 있습니다.
: console(콘솔), aid(지원), asynchronous(비동기) and virtual terminal(가상터미널)
시스템마다 다른 유형의 라인이 있습니다. 적절한 구성에 대해서는 다음 소프트웨어 및 하드웨어 구성 안내서를 참조 하십시오.

접속 유형	인터페이스	설명	번호
CON(CTY)	Console	설정을 위해 시스템에 로그인	0
VTY	Virtual and asynchronous	텔넷, X.25 PAD, HTTP, 및 시스템의 포트(예:이더넷 및 직렬 포트)를 통해 로그인 할 수 있습니다.	1~32

2.2.2.1 Line 과 interface 간의 관계

1) 동기 인터페이스와 VTY 라인 간의 관계

가상 터미널 라인은 시스템에서 액세스 하기 위한 동기 인터페이스를 제공 합니다. VTY 라인을 통해 시스템에서 연결하면 실제로 인터페이스의 가상 포트에 연결됩니다. 각 동기 인터페이스에서는 많은 가상 포트가 있을 수 있습니다.
예를 들어, 여러 텔넷이 인터페이스(이더넷 또는 직렬 인터페이스)에 연결하는 경우 VTY 구성을 위해 다음 단계를 수행해야 합니다.

① 회선 구성 모드로 로그인 하십시요.

오류1: 터미널 매개변수를 구성 하십시오.
VTY 구성에 대해서는 2.4절 "VTY 구성 예"를 참조 하십시오.

2.2.3 모니터 및 유지보수

Show line 을 실행하여 VTY 구성 확인 하십시오.

2.2.4 VTY 설정 예제

프롬프트를 표시하지 않고 모든 VTY의 화면 당 회선 수 제한을 취소하는 방법을 보여줍니다.

```
config#line vty 0 32
config_line#length 0
```

2-3장. 네트워크 관리 설정

2.3.1 SNMP 설정

2.3.1.1 소개

SNMP 시스템에는 다음과 같이 파트를 나눌 수 있습니다.

- SNMP 관리를 위한 측면 (NMS)
- SNMP 에이전트 (AGENT)
- 관리를 위한 기본 정보 (MIB)

SNMP는 응용프로그램 계층에서 작동하는 프로토콜 입니다. SNMP 관리 측과 에이전트 간에 패킷 형식을 제공 합니다.
SNMP 관리적인 측면으로 네트워크 관리 시스템(CiscoWorks와 같은 NMS)의 일부가 될 수 있습니다. 에이전트 및 MIB 은 시스템에 저장 됩니다. 시스템 SNMP를 구성하기 전에 네트워크 관리 측과 에이전트 간의 관계를 정의해야 합니다.
SNMP 에이전트는 MIB 변수를 포함합니다.
SNMP 관리 측은 이러한 변수의 값을 확인하거나 수정할 수 있습니다.
관리측은 에이전트에서 변수 값을 가져오거나 변수 값을 에이전트에 저장할 수 있습니다. 에이전트는 MIB에서 데이터를 수집합니다. MIB은 장치 매개 변수로 네트워크 장비의 데이터 베이스 입니다. 또한 에이전트는 관리자의 로딩 또는 데이터 구성 요청에 응답할 수 있습니다.
SNMP 에이전트는 관리 측에 트랩을 보낼 수 있습니다. Trap은 네트워크의 특정 상태를 나타내는 경보 및 각종 정보를 SNMP로 전송합니다. Trap은 부적절한 사용자 인증, 재시작, 링크 계층 상태(활성화/비활성화), TCP 연결 및 종료, 인접 시스템 연결 또는 잃어버릴 수 있는 기타 중요 이벤트를 나타낼 수 있습니다.

1. SNMP 알림

특별한 이벤트가 발생하면 시스템은 SNMP 관리시스템에 "inform"을 보냅니다. 예를 들어, 에이전트 시스템이 비정상 상태를 감지하면 SNMP 관리시스템으로 정보를 보냅니다. SNMP 알림은 Trap으로 처리되거나 요청을 보낸 것을 알릴 수 있습니다. 장비에서는 Trap을 수신할 때 응답을 보내지 않으므로 수신 측은 Trap이 수신 되었다고 확신 할 수 없습니다. 따라서 Trap은 신뢰할 수 없습니다. 이에 비해, SNMP 관리시스템 측에서 "inform request"을 수신하는 SNMP 관리시스템에서 SNMP정보에 대한 응답으로 PDU를 사용합니다. 관리시스템에서 "inform request"이 수신되지 않으면 에코가 전송되지 않습니다. 장비에서는 응답을 보내지 않으면 "inform request"을다시 보낼 수 있습니다. 그런 다음 알림은 관리시스템에 도달 할 수 있습니다.

정보 요청은 보다 신뢰성이 높기 때문에 시스템 및 네트워크의 더 많은 자원을 소비 합니다. 트랩은 전송 될 때 폐기 됩니다. 에코가 수신되거나 요청시간이 초과 될 때까지 "inform request"를 메모리에 저장해야 합니다. 또한 Trap은 한번만 전송되고 "inform request"는 여러 번 재전송 될 수 있습니다. 재전송 "inform request"는 네트워크 통신에 추가가 되므로 더 많은

부하를 유발 합니다. 또한 트랩은 한번만 전송되고 “inform request”은 여러 번 재전송 될 수 있습니다. 따라서 트랩 및 알림 요청은 안정성과 리소스 간에 균형을 유지 합니다. SNMP 관리 시스템에서 모든 통지를 크게 수신해야 하는 경우 “inform request”을 사용할 수 있습니다. 네트워크의 통신량을 우선시 하고 모든 통지를 받을 필요가 없으면 Trap을 사용할 수 있습니다. SFC6000 Series 스위치는 트랩만 지원하지만 “inform request”에 대한 확장을
제공 합니다.

2. SNMP Version

SFC6000 Series 스위치는 다음 SNMP 버전을 지원 합니다:

- SNMPv1 – 간단한 네트워크 관리 프로토콜

  RFC1157에 정의된 인터넷 표준 프로토콜 입니다.

- SNMPv2C – RFC1901에 정의된 SNMPv2의 그룹 기반 관리 프레임워크.

  인터넷 테스트 프로토콜

SFC6000 Series 스위치는 다음 SNMP도 지원 합니다.

- SNMPv3 – RFC4310에 정의된 간단한 네트워크 관리 프로토콜 Version3.

SNMPv1은 그룹 기반 보안 형식을 사용합니다. IP 주소 기반의 액세스 제어목록 및 암호를 이용하여 MIB에 액세스할 수 있는 관리측 그룹을 정의 합니다.

SNMPv3은 네트워크를 통한 패킷 인증 및 암호화의 조합을 통해 장치에 대한 보안 액세스를 제공 합니다.

SNMPv3에서 제공되는 보안 기능은 다음과 같습니다.

- 메시지 무결성 – 패킷이 전송 중에 변조되지 않았는지를 확인 합니다.
- 인증 – 메시지가 유효한 소스인지 확인 합니다.
- 암호화 – 패킷의 내용이 혼합되면 승인되지 않은 출처(대상장비)에서 패킷을 볼 수 없습니다.

SNMPv3은 보안 모델과 보안 레벨을 모두 제공합니다. 보안모델은 사용자 및 사용자가 상주하는 그룹에 대해 설정되는 인증 전략입니다. 보안 레벨은 보안 모델 내에서 허용되는 보안 수준입니다. 보안 모델과 보안 레벨의 조합은 SNMP 패킷을 처리 할 때 사용되는 보안 메커니즘을 결정 합니다. 인증 및 암호화, 인증 및 암호화 없음, 인증 없음의 세가지 보안 모델을 사용 할 수 있습니다.

관리작업 스테이션이 지원하는 SNMP 버전으로 SNMP 에이전트를 구성해야 합니다. 에이전트는 여러 관리적인 측면에서 통신을 할 수 있습니다.

3. MIB 지원

시스템의 SNMP는 모든 MIBII 변수(RFC1213에서 다룰 예정)와 SNMP트랩 (RFC1215에서 다룰 예정)을 지원 합니다. SFC6000 Series 스위치는 각 시스템의 고유 한 MIB 확장을 지원 합니다.

2.3.1.2 SNMP 설정 작업

- SNMP 보기 설정
- SNMP community에 대한 액세스 제어 작성 또는 수정
- 시스템 관리자의 연락 및 시스템 위치 구성
- SNMP 에이전트 데이터 패킷의 최대 길이 정의 SNMP 상태 모니터링
- SNMP trap 설정
- SNMP 바인딩 소스 주소 구성 SNMPv3 그룹 설정
- SNMPv3 사용자 설정
- SNMPv3 EngineID 설정

1. SNMP 보기 설정

SNMP 보기는 MIB에 대한 액세스 권한(incloud / excloud)을 제어하는 것입니다. 다음 명령을 사용하여 설정을 구성하십시오.

명령어	설명
snmp-server view [name oid] [exclude | include]	보기 기능의 이름,OID 지정 MIB의 하위 트리 또는 테이블을 추가하고 이름에 객체 식별자의 액세스 권한을 지정합니다. Exclude : 액세스 거부 Include : 액세스 허용

SNMP 보기 기능에서 액세스 할 수 있는 하위 집합은 MIN개체를 “Exclude” 개체로 지정하고 “Include” 하는 나머지 개체로 나뉩니다. 구성되지 않은 개체는 액세스를 할 수 없습니다.

SNMP 보기기능을 구성한 후 SNMP 액세스 가능한 그룹 이름을 지정한 후 그룹의 액세스 할 수 있는 개체의 하위 집합을 제한 할 수 있습니다.

2. 접근제한을 위한 SNMP community 값의 작성 또는 수정

SNMP community의 문자열을 사용하여 관리시스템과 장비사이의 관계를 정의 할 수 있습니다. Community 문자열은 관리시스템이 장비에 로그인 할 수 있게 하는 암호와 유사합니다. Community 문자열과 관련하여 하나 이상의 속성을 지정할 수 있습니다.

명령어	설명
snmp-server community string [view view-name] [ro | rw] [word]	그룹의 community 값을 정의 합니다.

하나 또는 여러 개의 그룹 문자열을 구성 할 수 있습니다. "no" 명령어를 사용하여 지정된 Community 문자열을 제거하십시오. Community 문자열을 구성하는 방법은 "SNMP 명령" 부분을 참조하십시오.

3. 시스템 관리자의 연락 방법 및 시스템 위치 설명 설정

SysContact와 SysLocation은 시스템 그룹에서의 관리 변수는 MIB 이며 각각의 장비의 ID값과 위치를 정의 합니다. 이 정보는 Config를 통해서 액세스 할 수 있습니다. 글로벌 모드에서 다음 명령을 사용할 수 있습니다.

명령어	설명
snmp-server contact [text]	노드의 링크 관리자에 대한 문자열을 설정합니다.
snmp-server location [text]	노드 위치의 문자열을 설정합니다.

4. 장비에서 보내는 SNMP 데이터 패킷의 최대 길이 정의

요청 또는 응답을 받으면 데이터 패킷의 최대 길이를 구성 할 수 있습니다. 글로벌 모드에서 다음 명령어를 사용 할 수 있습니다.

명령어	설명
snmp-server packetsize byte-count	데이터 패킷의 최대 길이를 설정합니다.

5. SNMP 상태 모니터링

글로벌 모드에서 다음 명령어를 사용하여 잘못된 Community 문자열 항목, 에러 수 및 변수를 비롯한 SNMP 출력/입력 통계를 모니터링 할 수 있습니다.

명령어	설명
show snmp	SNMP의 상태를 모니터링 합니다.

6. SNMP trap 설정

다음 명령어를 사용하여 SNMP trap을 보내도록 시스템에 설정할 수 있습니다.

(두번째 설정은 선택 사항 임)

- Trap을 보내도록 시스템 설정

글로벌 모드에서 다음 명령을 실행하여 트랩을 호스트로 보내도록 설정을 할 수 있습니다.

명령어	설명
snmp-server host host community-string [trap-type]	Trap메시지의 수신자를 지정합니다..
snmp-server host host [traps|informs]{version {v1 | v2c | v3 {auth | noauth | priv } }}community-string [trap-type]	Trap메시지의 수신자, 버전, 사용자 이름을 지정합니다. 참고. SNMPv3의 트랩의 경우 호스트가 트랩 메시지를 수신하도록 구성되지 전에 호스트에 대한 SNMP 엔진 ID를 구성 해야 합니다.

시스템이 시작되면 SNMP 설정은 자동으로 실행 됩니다. 모든 유형의 Trap이 활성화 됩니다. "snmp-server host " 명령어를 사용하여 어떤 호스트가 어떤 종류의 Trap을 수신할 지 지정할 수 있습니다.

일부 Trap은 다른 명령을 통해 제어해야 합니다. 예를 들어, 인터페이스를 열거나 닫을 때 SNMP 링크 트랩을 보내려면 인터페이스 설정창에서 "snmp trap link-status" 명령어를 실행하여 링크 트랩을 활성화 해야 합니다.

Trap을 수신하려면 호스트가 "snmp-server host " 명령을 구성해야 합니다.

- Trap의 실행중인 매개변수 수정하기

선택적인 항목으로 Trap이 시작되는 소스 인터페이스, 메시지 큐의 길이 또는 각 호스트의 재전송 간격 값을 지정할 수 있습니다. Trap의 실행 매개변수를 수정하려면 글로벌모드에서 다음 선택적 명령어를 사용할 수 있습니다.

명령어	설명
snmp-server trap-source [interface]	Trap이 시작되는 소스 인터페이스를 지정하고 메시지의 소스 IP주소를 설정합니다.
snmp-server queue-length [length]	Trap이 있는 각 호스트에 대한 메시지 큐의 길이를 작성합니다. (기본값 : 10)
snmp-server trap-timeout [seconds]	재전송 대기열에서 Trap을 재전송 할 빈도를 정의합니다. (기본값 : 30초)

7. SNMP 바인딩 소스 주소 설정

다음 명령어를 실행하여 SNMP 메시지의 소스 주소를 설정하십시오.

명령어	설명
snmp source-addr [ip address]	SNMP 메시지의 소스 주소를 설정합니다.

8. SNMPv3 그룹의 설정

그룹을 구성하려면 다음 명령어를 실행하십시오.

명령어	설명
snmp-server group [groupname {v1 | v2c |v3 [auth | noauth | priv]}][read readview][write writeview] [notify notifyview] [access access-list]	SNMPv3그룹을 구성합니다. 기본적으로 인터넷 하위 트리의 모든 항목 만 읽을 수 있습니다.

9. SNMPv3 사용자

다음 명령어를 실행하여 로컬 사용자를 구성할 수 있습니다. 관리자가 장치에 로그인하면 장치에 구성된 사용자 이름과 암호를 사용자에게 알려야 합니다. 사용자의 보안 수준은 사용자가 속한 그룹의 보안수준보다 높거나 같아야 합니다. 그렇지 않으면 사용자는 인증을 통과 할 수 없습니다.

명령어	설명
snmp-server user username groupname {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]	SNMPv3의 로컬 사용자를 설정합니다.

다음 명령어를 실행하여 원격 사용자를 구성 할 수 있습니다. 장치가 원격제어 스테이션에 트랩을 보내야하는 경우, 제어 스테이션 ID인증을 수행하면 사용자를 구성해야 합니다. 원격 사용자의 사용자 이름과 암호는 제어스테이션의 사용자 이름과 암호와 같아야 합니다. 그렇지 않으면 Trap을 수신 할 수 없습니다.

명령어	설명
snmp-server user username groupname {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]	SNMPv3의 원격 사용자를 설정합니다. 참고 : 원격사용자를 구성하기 전에 원격 SNMP 엔진 ID를 IP 주소의 제어스테이션에 구성해야 합니다.

10. SNMPv3 엔진ID 설정

SNMP 엔진ID는 SNMP 엔진을 식별하는데 사용됩니다. 기존의 SNMP 관리시스템 및 장비는 SNMPv3 프레임의 SNMP 엔진에 포함되어 있습니다.

명령어	설명
snmp-server engineID remote ip-address [udp-port port-number]	원격 SNMP 엔진의 설정 방법입니다.

engineid-string	

2.3.1.3 설정 예제

1. 예시 (1)

snmp-server community public RO
snmp-server community private RW
snmp-server host 192.168.10.2 public

- 모든 MIB 변수만 읽을 수 있는 공유 문자열을 설정하는 방법
- 모든 MIB 변수를 읽고 쓸수 있는 Community 문자열을 개인용으로 설정하는 방법

Community 문자열을 Public을 사용하여 시스템의 MIB변수를 읽을 수 있습니다. 또한 Community 문자열을 Private하게 설정하여 MIB 변수를 읽어 시스템에 쓰기 가능한 MIB 변수를 입력 할 수 있습니다.

위의 명령은 시스템이 Trap을 보내야 할 때 Community 문자열을 Public 하게 지정하여 Trap을 192.168.10.2으로 보내게 됩니다. 예를 들어, 장비의 포트가 다운상태가 되었다면 장비에서는 192.168.10.2로 링크다운 Trap정보를 보냅니다.

2. 예시 (2)

snmp-server engineID remote 90.0.0.3 80000523015a000003
snmp-server group getter v3 auth
snmp-server group setter v3 priv write v-write
snmp-server user get-user getter v3 auth sha 12345678
snmp-server user set-user setter v3 encrypted auth md5 12345678 snmp-server
user notifier getter remote 90.0.0.3 v3 auth md5 abcdefghi
snmp-server host 90.0.0.3 informs version v3 auth notifier
snmp-server view v-write internet included

위의 예시는 SNMPv3을 사용하여 장비를 관리하는 방법을 보여줍니다. 그룹 Setter는 장치를 설정할 수 있는 반면, 그룹 Getter는 장치정보를 찾아 볼 수 있습니다. 사용자 설정 사용자가 그룹 User가 그룹 Setter에 속할 때 사용자 Get-user는 그룹 getter에 속합니다.
get-user의 경우 보안 수준은 인증되지만 암호화되지 않고 암호는 12345678이며 암호화 방식은 “sha”를 사용하여 암호화를 합니다.

Set-user의 경우 보안 수준은 인증 및 암호화되고 암호는 12345678이며 암호화 방식은 “md5”를 사용하여 암호화를 합니다.
장비에서 Key event가 발생하면 username notifiy를 사용하여 관리자의 호스트는 90.0.0.3에게 알림 메시지를 보냅니다.

2.3.2 RMON 설정

2.3.2.1 RMON 설정 작업

RMON 설정 작업은 다음과 같습니다.

- 스위치에 대한 rMON 경보 기능 설정
- 스위치에 대한 rMON 이벤트 기능 설정
- 스위치에 대한 rMON 통계 기능 설정
- 스위치에 대한 rMON 기록 기능 설정
- 스위치의 rMON 설정 표시

1. 스위치의 rMON 경보 기능 설정

Command line 또는 SNMP NMS를 통해 rMON 경보 기능을 구성 할 수 있습니다.
SNMP NMS를 통해 구성하는 경우 스위치의 SNMP를 구성해야 합니다.
경보 기능이 구성된 후 장치는 시스템의 일부 통계 값을 모니터 할 수 있습니다.
다음 표는 rMON 알람 기능을 설정하는 방법을 보여줍니다.

명령어	설명
configuration	글로벌 모드로 들어갑니다.
rmon alarm index variable interval {absolute | delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string]	RMON 알람 항목을 추가하십시오. **Index**는 경보 항목의 색인입니다. 유효 범위는 1~65535 입니다. **Variable**은 모니터링 되는 MIB의 객체입니다. 시스템에서 유효한 MIB객체여야 하며, Integer, Counter, Gauge 또는 Time Ticks유형의 Objects 만 탐지 할 수 있습니다. **Interva**은 샘플링을 위한 시간 섹션입니다. 단위는 초 단위이며 유효 값은 1에서 4294967295 사이 입니다. **Absolute**는 MIB객체으 값을 직접 모니터링 하는데 사용됩니다. 델타는 두 샘플링 사이에서 MIB 오브젝트의 값 변경을 모니터 하는데 사용됩니다. **Value**는 경보가 생성될 때 임계 값입니다. 이벤트 번호는 임계 값에 도달했을 때 생성되는 이벤트의 index값입니다. 이벤트 번호는 선택사

	항 입니다. **Owner string은** 알람에 대한 정보를 설명합니다.
exit	관리자 모드로 되돌아갑니다.
write	설정을 저장합니다.

rMON 경보 항목이 구성된 후 장치는 지정된 OID 값을 가져옵니다.
획득된 값은 alarm 유형(절대 또는 델타)에 따라 이전 값과 비교됩니다.
획득된 값이 이전 값보다 크고 상승 임계 값으로 지정된 임계 값을 초과하는 경우 이벤트 번호가 index 번호인 이벤트. (이벤트 번호가 0이거나 이벤트 번호가 index 번호가 될때 이벤트가 발생하지 않음)
변수가 지정된 OID를 얻을 수 없으면 이 행의 알람 항목 상대가 무효로 설정됩니다.
동일한 색인으로 경보 항목을 구성하기 위해 rmon alarm을 여러 번 실행하면 마지막 구성만 효과적입니다. 아무런 rmon alarm의 index도 실행하지 않아 인덱스가 동일한 알람 항목을 취소 할 수 있습니다.

2. 스위치용 rMON 이벤트 설정

다음 표에는 rMON 이벤트를 구성하는 단계가 나와있습니다.

명령어	설명
configuration	글로벌 모드로 들어갑니다.
rmon event index [description string] [log] [owner string] [trap community]	RMON 이벤트 항목을 추가하십시오. **Index**는 이벤트 항목의 색인입니다. 유효 범위는 1~65535 입니다. **Description**은 이벤트에 대한 정보를 의미합니다. **Log**는 이벤트가 발생될 때의 로그 테이블에 정보를 추가하는 것을 의미 합니다. Trap은 이벤트가 발생될 때 Trap메시지가 생성됨을 의미 합니다. **Community**는 Community 이름입니다. **Owner string은** 알람에 대한 정보를 설명합니다.
exit	관리자 모드로 되돌아갑니다.
write	설정을 저장합니다.

rMON이벤트가 구성된 후에는 rMON 경보가 발생할 때 rMON 이벤트 항목의 도메인 eventLastTimeSent를 SysUpTime으로 설정해야 합니다.
Log 속성이 rMON 이벤트로 설정되면 메시지가 로그 테이블에 추가 됩니다. Trap 속성이 rMON이벤트로 설정되면 트랩 메시지가 커뮤니티 이름으로 전송됩니다. rMON이벤트를 여러 번 실행하여 동일한 index로 이벤트 항목을 구성하면 마지막 구성만 적용됩니다. rMON이벤트 index를 실행하여 index가 동일한 이벤트 항목을 취소할 수 있습니다.

3. 스위치의 rMON 통계 설정

rMON 통계 그룹은 장치의 모든 포트에 대한 통계 정보를 모니터 하는데 사용됩니다. rMON 통계를 구성하는 단계는 다음과 같습니다.

명령어	설명
configuration	글로벌 모드로 들어갑니다.
interface iftype ifid	포트 모드로 들어갑니다. iftype은 모듈 유형을 의미 합니다. Ifid는 포트의 ID를 의미합니다.
rmon collection stat index [owner string]	포트에서 통계 기능을 활성화 합니다. **index**는 통계의 색인을 의미합니다. **owner string**은 통계에 대한 정보를 설명하는 것입니다.
exit	글로벌 모드로 돌아 갑니다.
exit	관리자 모드로 돌아 갑니다.
write	설정을 저장합니다.

동일한 색인을 사용하여 통계항목을 구성하기 위해 "rmon collection stat " 를 여러 번 실행하면 마지막 구성만 적용이 됩니다. "rmon collection stats index"를 실행하여 index가 동일한 통계 항목을 취소 할 수 있습니다.

4. 스위치에 대한 rMON 기록 설정

rMON 히스토리 그룹은 장치의 포트에서 다른 시간 섹션의 통계 정보를 수집하는데 사용됩니다. rMON 통계 기능은 다음과 같이 구성됩니다.

명령어	설명
configuration	글로벌 모드로 들어갑니다.
interface iftype ifid	포트 모드로 들어갑니다. iftype은 모듈 유형을 의미 합니다. Ifid는 포트의 ID를 의미합니다.
rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	포트에서 통계 기능을 활성화 합니다. **index**는 항목의 색인을 의미합니다. 이력 항목으로 수집된 모든 데이터 중에서 최신 버킷 번호 항목을 저장해야 합니다. 이러한 통계 값을 얻기 위해 이더넷의 히스토리 항목을 찾아 볼 수 있습니다. 기본값은 50개 입니다. 두번째는 격일로 통계 데이터를 확보하는 간격을 의미 합니다. 기본 값은 1800초 입니다. **owner string**은 통계에 대한 정보를 설명하는 것입니다.

exit	글로벌 모드로 돌아 갑니다.
exit	관리자 모드로 돌아 갑니다.
write	설정을 저장합니다.

rMON기록 항목이 추가되면 장치는 지정된 포트에서 2초마다 통계 값을 가져옵니다. 통계 값은 정보 항목으로 이력 항목에 추가 됩니다. rMON 수집, 기록, 색인을 여러 번 실행하여 동일한 색인으로 기록 항목을 구성하면 마지막에 설정 넣은 값만 적용 됩니다.

rMON 히스토리 index를 실행하여 index가 동일한 히스토리 항목을 취소할 수 있습니다.

노트:

버킷 번호의 값이 너무 크거나 간격(초)이 너무 작은 경우 혹은 너무 많은 경우는 시스템의 소스를 사용합니다.

5. 스위치의 rMON 설정 표시

show 명령어를 실행하여 스위치의 rMON구성을 보여줍니다.

명령어	설명
show rmon [alarm] [event] [statistics] [history]	구성 정보를 표시 합니다. **Alarm**은 알랑 항목의 구성을 표시하는 것을 의미 합니다. **Event**는 이벤트 항목의 구성을 표시하고 이벤트 발생에 의해 생성되고 로그테이블에 포함 된 항목을 표시하는 것을 의미 합니다. **Statistics**는 장치가 포트에서 수집하는 통계 항목 및 통계 값의 구성을 표시하는 것을 의미 합니다. **History**는 포트에서 최신 지정된 간격으로 수집하는 기록 항목 및 통계 값의 구성을 표시하는 것을 의미 합니다.

2.3.3 PDP 설정

2.3.3.1 소개

PDP는 네트워크 장치를 탐지하는데 특별히 사용되는 2계층 프로토콜 입니다. PDP는 NMS(Network Management Service)에서 이미 알려진 장치의 모든 인접 장치를 검색하는 데 사용됩니다. PDP를 사용하면 SNMP 상대 주소 및 인접 장치 유형을 알 수 있습니다. PDP를 통해 주변 장치를 감지 한 후 NMS는 네트워크 토폴로지를 얻기 위해 SNMP를 통해 주변 장치를 요구할 수 있습니다.

SFC6000 Series는 PDP를 통해 인접 장치를 탐지 할 수 있지만 SNMP를 통해 인접 장치를 요구할 수는 없습니다. 따라서 이러한 스위치는 네트워크 경계에 위치해야 합니다. 그렇지 않으면 완전한 네트워크 토폴로지를 얻을 수 없습니다. 스위치상의 PDP는 이더넷과 모든 SANP에서 구성될 수 있습니다.

현재 PDP를 지원하는 스위치는 다음과 같은 유형으로 분류 할 수 있습니다.

2.3.3.2 PDP 설정 내용

- 스위치의 기본 PDP 구성
- PDP 클럭 및 정보 저장시간 설정
- PDP의 버전 설정
- 스위치에서 PDP의 사용을 위한 적용 방법
- 스위치 포트에서 PDP의 사용을 위한 적용 방법
- PDP 모니터링 및 관리

1. 스위치의 기본 PDP 구성

기능	기본 설정
PDP 기본 설정 상태	Disable
PDP 포트 설정 상태	Disable
PDP clock (메시지를 보내는 빈도)	60 seconds
PDP information saving	180 seconds
PDP version	2

2. PDP 클럭 및 정보 저장 시간 설정

글로벌 모드에서 다음 명령어를 실행하여 PDP가 메시지를 보내고 PDP 정보 저장 시간을 설정 하십시오.

명령어	설명
pdp timer [seconds]	PDP가 메시지를 보낼 빈도를 설정합니다.
pdp holdtime [seconds]	PDP 정보 저장 시간을 설정합니다.

3. PDP 버전 설정

글로벌 모드에서 다음 명령어를 실행하여 PDP 버전을 설정 하십시오.

명령어	설명
pdp version [1 | 2]	PDP 버전을 설정 합니다.

4. 스위치에서 PDP 적용 하기

PDP는 기본 구성에서 활성화되어 있지 않습니다. PDP를 사용하려면 글로벌 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
pdp run	스위치에서 PDP를 적용 합니다.

5. 스위치의 포트에서 PDP 적용 설정

PDP는 기본 구성에서는 활성화 되어있지 않습니다. 스위치에서 PDP가 활성화 된 후 인터페이스 구성 모드에서 다음 명령을 실행하여 포트에서 PDP를 활성화 할 수 있습니다.

명령어	설명
pdp enable	스위치의 포트에서 PDP를 적용 합니다.

6. PDP의 모니터링 및 관리

관리모드에서 다음 명령어를 실행하여 PDP를 모니터링 합니다.

명령어	설명
show pdp traffic	스위치가 수신 및 전송하는 PDP 메시지 수를 표시 합니다.
show pdp neighbor [detail]	스위치가 인접한 장치를 표시합니다.

2.3.3.3 PDP 설정 예제

예제 1: PDP 활성화

config# pdp run

config# int f0/0

config_f0/0#pdp enable

예제 2: PDP 클럭 및 정보 저장 시간 설정

config#pdp timer 30

config#pdp holdtime 90

예제 3: PDP 버전 설정

config#pdp version 1

예제 4: PDP 정보 모니터링

config#show pdp neighbors

Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r – Repeater

Device ID Local IntrfceHoldtmeCapabilityPlatform Port ID

joeEth 0 133 4500 Eth 0

samEth 0 152 R AS5200 Eth 0

4장. SSH 설정 명령어

2.4.1 개요

2.4.1.1 SSH Server

SSH 서버를 통해 SSH 클라이언트와 장치간 보안 및 암호화된 통신 연결을 생성 할 수 있습니다. 연결에는 텔넷과 같은 기능이 있습니다. SSH서버는 des, 3des 및 blowfish를 포함한 암호화 알고리즘을 지원합니다.

2.4.1.2 SSH client

SSH 클라이언트는 SSH 프로토콜로 실행되는 응용 프로그램입니다. SSH 클라이언트는 인증 및 암호화를 제공 할 수 있으므로 SSH 클라이언트는 안전하지 않은 네트워크 조건에서 실행되는 장치라도 SSH 서버를 지원하는 통신 장치 또는 장치 간의 통신을 보호합니다. SSH 클라이언트는 des, 3des 및 blowfish를 포함한 암호화 알고리즘을 지원합니다.

2.4.1.3 기능

SSH 서버 및 SSH 클라이언트는 버전 1.5를 지원합니다. 둘다 셸 응용 프로그램에서만 지원 합니다.

2.4.2 설정 내용

2.4.2.1 인증 방법 목록 구성

SSH 서버는 로그인 인증 모드를 사용합니다. SSH 서버는 기본적으로 기본 인증 방법 목록을 사용합니다. 글로벌 모드에서 다음 명령을 실행하여 인증 방법 목록을 구성합니다.

명령어	설명
Ip sshd auth_method [STRING]	인증 방법 목록을 구성합니다.

2.4.2.2 접근 제어 목록 구성

장치의 SSH서버에 대한 접근을 제어하려면 SSH서버에 대한 접근 제어 목록을 구성해야 합니다. 글로벌 모드에서 다음 명령을 통해 접근 제어 목록을 구성합니다.

명령어	설명
Ip sshd access-class [STRING]	접근 제어 목록을 설정 합니다.

2.4.2.3 인증 시간 초과 값 구성

클라이언트와 서버 간에 연결이 설정된 후 설정된 시간 내에 인증을 승인 할 수 없으면 서버는 연결을 끊습니다. 다음 명령을 통해 구성 시간 초과 값을 구성합니다.

명령어	설명
Ip sshd timeout [0-65535]	인증 시간 초과 값을 구성합니다

2.4.2.4 인증 재시도 횟수 설정

실패한 인증에 대한 시간이 최대 시간을 초과하면 SSH서버는 새 연결이 설정되지 않는 한 인증을 재시도 하지 않습니다. 최대 재시도 횟수는 기본적으로 3입니다. 글로벌 모드에서 다음 명령어를 실행하여 인증을 다시 시도하는 최대 시간을 설정 하십시오.

명령어	설명
Ip sshd auth-retries [0-65535]	인증을 다시 시도하는 시간을 구성합니다

2.4.2.5 SSH 서버 사용

SSH 서버는 기본적으로 비활성화 되어 있습니다. SSH서버가 활성화 되면 장치는 rsa 암호를 쌍으로 생성 한 다음 클라이언트의 연결 요청을 수신합니다. 과정은 1~2분 정도 소요 됩니다. 글로벌 구성 모드에서 다음 명령어를 실행하여 SSH 서버를 활성화 합니다.

명령어	설명
Ip sshd enable	SSH 서버를 사용 합니다. 암호는 1024bit로 생성 됩니다.

2.4.3 SSH 서버 설정 예시

다음 구성에서는 IP주소가 192.168.20.40인 host만 SSH서버에 접속 할 수 있습니다. 로컬 사용자 데이터베이스는 사용자 ID를 구별하는 데 사용됩니다.

2.4.3.1 접근제어 목록

```
ip access-list standard ssh-acl
permit 192.168.20.40
```

2.4.3.2 글로벌 모드 설정

```
aaa authentication login ssh-auth local
ip sshd auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```

3장 인터페이스 설정

3-1장 소개

이 장에서는 스위치가 구성하는 다양한 종류의 인터페이스를 배우고 다양한 인터페이스 유형에 대한 구성 정보를 참조하는 데 도움이 됩니다. 이 장에서 사용된 모든 인터페이스 명령에 대한 자세한 설명은 인터페이스 구성 명령을 참조 하십시오. 이 장에서 나오는 다른 명령 파일은 설명서의 다른 부분을 참조 하십시오. 소개에는 모든 인터페이스 유형에 적용 할 수 있는 통신 정보가 포함 됩니다.

3.1.1 지원되는 인터페이스 유형

인터페이스 유형에 대한 정보는 다음 표를 참조 하십시오.

타입	작업	참조
Ethernet interface	Configures Ethernet interface. Configures fast Ethernet interface. Configures gigabit Ethernet interface.	이더넷 인터페이스 구성
Logical interface	Loopback interface Null interface VLAN interface SuperVlan interface	논리적 인터페이스 구성 Loopback 인터페이스와 Null 인터페이스는 Layer-3에서만 구성 됩니다. 사용자는 Layer-2스위치에서 VLAN 또는 SuperVLAN인터페이스를 구성할 수 있습니다.
	Aggregation interface	논리적 인터페이스 구성

지원되는 두 종류의 인터페이스는 이더넷 인터페이스와 논리적 인터페이스가 있습니다. 이더넷 인터페이스 유형은 표준 통신 인터페이스 및 스위치에 설치된 인터페이스 카드 또는 인터페이스 모듈에 따라 다릅니다. 논리적 인터페이스는 해당 물리적 장치가 없는 인터페이스로 사용자가 수동으로 설정 합니다.

스위치의 지원 이더넷 인터페이스는 다음과 같습니다.

- Ethernet interface
- Fast Ethernet interface
- Gigabit Ethernet interface

스위치의 지원 논리적 인터페이스는 다음과 같습니다.

- loopback interface
- null interface
- aggregation interface
- VLAN interface

3.1.2 인터페이스 설정 소개

다음 설명은 모든 인터페이스의 구성 프로세스에 적용됩니다. 글로벌 모드에서 인터페이스 구성을 수행하려면 다음 단계를 수행 하십시오.

(1) ‘interface’명령어를 실행하여 인터페이스 구성 모드로 들어가서 구성을 시작 하십시오. 이때 스위치 프롬프트는 ‘config_‘와 단축 인터페이스 형태로 구성 됩니다. 모듈 번호와 인터페이스의 숫자를 사용 하십시오. 번호는 설치(exworks) 또는 인터페이스 카드가 시스템에 추가 될 대 지정 됩니다. 이 인터페이스를 표시하려면 ‘show interface’ 명령어를 실행 하십시오. 장치가 지원하는 각 인터페이스는 다음과 같이 자체 상태를 제공합니다.

```
Switch#show interface
GigaEthernet1/1 is down, line protocol is down
Hardware is Fast Ethernet, Address is 0009.7cf7.7dc1 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Auto-duplex, Auto-speed
 input flow-control is off, output flow-control is off
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output 17:52:52, output hang never Last clearing of "show interface" counters
never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue :0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
  1 packets input, 64 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  input packets with dribble condition detected
  packets output, 64 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
```

gigabit Ethernet interface g1/1을 구성하려면 다음 내용을 입력 하십시오.

Interface gigaEthernet0/1
스위치에서 보여주는 프롬프트는 ‘config_g0/1’ 입니다.

Note :

인터페이스 유형과 인터페이스 번호 사이에 공백을 추가 할 필요가 없습니다. 예를 들어, 위의 행에서 ‘g1/1’ 또는 ‘g 1/1’이 모두 동일합니다.

1. 인터페이스 구성 모드에서 인터페이스 구성 명령을 구성 할 수 있습니다. 다양한 명령은 인터페이스에서 실행될 프로토콜 및 응용 프로그램을 정의 합니다. 이 명령은 사용자가 인터페이스 구성 모드를 종료 하거나 다른 인터페이스로 전환 할 때가지 유지 됩니다.

2. 인터페이스 구성이 완료되면 다음 장의 '인터페이스의 모니터링 및 유지관리' 에서 'show'명령을 사용하여 인터페이스 상태를 테스트 하십시오.

3-2장 인터페이스 설정

3.2.1. 인터페이스의 공통 속성 구성

다음 내용은 모든 유형의 인터페이스에서 실행될 수 있는 명령을 설명하고 인터페이스의 공통 속성을 구성 합니다. 구성할 수 있는 인터페이스의 공통 속성에는 인터페이스 설명, 대역폭, 지연 등이 있습니다.

3.2.1.1 Description 설정

해당 인터페이스에 'Description'을 추가 하여 인터페이스와 연결된 콘텐츠를 기억하는데 도움이 됩니다. 'Description'은 인터페이스의 사용을 식별하는데 도움 되고 인터페이스 참고 용으로만 사용되며 인터페이스의 기능에는 영향을 미치지 않습니다.

명령어	설명
description [string]	현재의 인터페이스에 설명을 추가합니다.

예를 들어, 인터페이스 설명 추가와 관련된 예제는 다음 장 '인터페이스 설명 예'를 참조 하십시오.

3.2.1.2 Bandwidth 설정

상위 프로토콜은 대역폭 정보를 사용하여 작업 결정을 수행 합니다. 다음 명령을 사용하여 인터페이스의 대역폭을 구성 하십시오.

명령어	설명
Bandwidth [kilobps]	현재의 인터페이스에 설명을 추가합니다.

대역폭은 라우팅 매개변수 일 뿐이며 실제 물리적 인터페이스의 통신 속도에는 영향을 미치지 않습니다.

3.2.1.3 Time Delay 설정

상위 프로토콜은 동작 결정을 수행하기 위해 시간 지연 정보를 사용합니다. 인터페이스 구성 모드에서 인터페이스의 시간 지연을 구성하려면 다음 명령을 사용하십시오.

명령어	설명
delay [tensofmicroseconds]	현재 구성된 인터페이스의 시간 지연을 설정합니다.

시간 지연의 구성은 오직 정보 매개변수입니다. 이 명령을 사용하면 인터페이스의 실제 시간지연을 조정 하는 것은 아닙니다.

3.2.2 인터페이스의 모니터링 및 관리

다음 작업은 인터페이스를 모니터링 하고 관리 할 수 있습니다.

- 인터페이스의 상태 확인
- 인터페이스 초기화 및 삭제
- 인터페이스의 활성화 및 종료

3.2.2.1 인터페이스의 상태 확인

스위치는 소프트웨어 및 하드웨어의 버전, 인터페이스 상태 등 인터페이스 정보와 관련된 몇가지 명령을 보여줍니다. 다음 표는 인터페이스 모니터 명령의 일부를 나열합니다. 이 명령에 대한 설명은 '인터페이스 구성 설정'을 참조 하십시오.

명령어는 다음과 같습니다

명령어	설명
show interface [type [slot/port]	인터페이스 상태를 표시합니다.
show running-config	현재 설정 상태를 표시 합니다.

3.2.2.2 인터페이스 초기화 및 삭제

논리 인터페이스를 동적으로 설정하고 삭제 할 수 있습니다. 이는 하위 인터페이스 및 채널화 된 인터페이스에도 적용 됩니다. 글로벌 모드에서 인터페이스를 초기화하고 삭제하려면 다음 명령어를 사용하십시오.

명령어	설명
no interface [type [slot/port]	물리적 인터페이스를 초기화 하거나 가상 인터페이스를 삭제 합니다.

3.2.2.3 인터페이스 활성화 및 비활성화

인터페이스가 비활성화되면 인터페이스의 모든 기능이 사용 불가능하게 되며 인터페이스의 모니터링 명령어로 확인했을 때에 사용 불가능한 인터페이스로 표시 됩니다. 이 정보는 동적 라우팅 프로토콜을 통해 다른 스위치로 전송 될 수 있습니다. 인터페이스 구성 모드에서 인터페이스를 활성화/비활성화 하려면 다음 명령을 사용 하십시오.

명령어	설명
shutdown	인터페이스의 비활성화
no shutdown	인터페이스의 활성화

'show interface'명령과 'show running-config' 명령을 사용하여 인터페이스가 비활성화 되었는지 여부를 확인 할 수 있습니다. 'show interface'명령어를 사용하면 비활성화된 인터페이스는 'administratively down' 으로 표시 됩니다.
자세한 내용은 다음 예제인 '인터페이스 비활성화 예제'를 참조 하십시오.

3.2.3 논리적 인터페이스 설정

이 절에서는 논리적 인터페이스를 설정하는 방법에 대해 설명합니다. 내용은 다음과 같습니다.

- Null 인터페이스 설정
- Loopback 인터페이스 설정
- Aggregation 인터페이스 설정
- Vlan 인터페이스 설정

3.2.3.1 Null 인터페이스 설정

전체 시스템은 하나의 Null 인터페이스만을 지원합니다. 그 기능은 대부분의 운영체제에서 적용되는 Null장치의 기능과 유사 합니다. Null 인터페이스는 항상 사용할 수 있지만 통신 정보를 전송하거나 수신하지는 않습니다. 인터페이스 구성 명령 'no ip unreachable'은 Null 인터페이스에서 사용할 수 있는 유일한 명령입니다. Null 인터페이스는 통신을 필터링 하는 선택적 메소드를 제공합니다. 즉, 원하지 않는 네트워크 통신을 Null인터페이스로 라우팅 할 수 있습니다. Null인터페이스는 접근 제어 목록으로 기능 할 수 있습니다.

글로벌 모드에서 다음 명령어를 실행하여 Null인터페이스를 지정 할 수 있습니다.

명령어	설명
Interface null 0	Null 인터페이스를 생성합니다.

Null 인터페이스는 인터페이스 유형을 매개 변수로 취하는 모든 명령에 적용 할 수 있습니다. 다음 사례는 IP 192.168.20.0 라우팅을 위해 Null 인터페이스를 구성하는 방법을 보여줍니다.

```
ip route 192.168.20.0 255.255.255.0 null 0
```

3.2.3.2 Loopback 인터페이스 설정

Loopback 인터페이스는 가상의 인터페이스 입니다. 외부 인터페이스가 종료된 경우에도 항상 BGP세션을 계속 동작 합니다. Loopback 인터페이스는 BGP 터미널 주소로 사용 될 수 있습니다. 다른 스위치가 Loopback 인터페이스에 도달하려면 Loopback 인터페이스 주소로 라우팅을 Broadcast 하도록 동적 라우팅 프로토콜을 구성해야 합니다. Loopback 인터페이스로 라우팅 된 메시지는 스위치로 재 라우팅 되어 로컬에서 처리 될 수 있습니다. Loopbackㅇ니터페이스로 라우팅 되지만 대상 Loopback 인터페이스의 IP주소가 아닌 경우, 해당 메시지는 삭제됩니다. 즉, Loopback 인터페이스는 Null 인터페이스로 작동 됩니다. 글로벌 모드에서 다음 명령을 실행하여 Loopback 인터페이스를 지정하고 인터페이스 구성 상태를 입력하십시오.

명령어	설명
Interface loopback [number]	Loopback 인터페이스를 생성합니다.

3.2.3.3 Aggregation 인터페이스 설정

오버된 대역복으로 인해 단일 이더넷 인터페이스가 모자랄 경우 Aggregation 인터페이스를 사용 할 수 있습니다. 동일한 속도로 여러 개의 전 이중 인터페이스를 묶어서 대역복을 크게 향상 시킬 수 있습니다.
Aggregation 인터페이스를 정의 하려면 다음 명령을 입력 하십시오.

명령어	설명
Interface port-aggregator [number]	Aggregation 인터페이스를 생성합니다.

3.2.3.4 Vlan 인터페이스 설정

VLAN 인터페이스는 스위치의 라우팅 인터페이스 입니다. 글로벌 모드에서 VLAN 명령은 대상 주소가 VLAN에 있는 IP패킷을 처리하는 방법을 정의하지 않고 Layer-2계층의 VLAN만 시스템에 추가 합니다. VLAN 인터페이스가 없으면 이러한 유형의 패킷이 삭제됩니다. VLAN 인터페이스를 정의하려면 다음 명령을 실행하십시오.

명령어	설명
Interface vlan [number]	VLAN 인터페이스를 생성합니다.

3.2.3.5 Super VLAN 인터페이스 설정

Super VLAN 기술은 다음과 같은 메커니즘을 제공합니다. 동일한 스위치의 다른 VLAN에 있는 호스트를 동일한 IPv4 서브넷에 할당하고 동일한 기본 게이트웨이를 사용 할 수 있습니다. 따라서 많은 IP 주소가 저장 됩니다. Super VLAN 기술은 VLAN이 동일한 관리 인터페이스를 사용하고 호스트가 동일한 IPv4 네트워크 섹션과 게이트웨이를 사용하는 그룹에 다른 VLAN으로 배치 합니다. Super VLAN에 속하는 VLAN을

SubVLAN이라고 합니다. SubVLAN은 IP 주소를 구성하여 관리 인터페이스를 소유 할 수 없습니다.

명령어	설명
[no] Interface Supervlan [index]	SuperVLAN인터페이스 구성 모드로 들어갑니다. 지정된 SuperVLAN인터페이스가 존재하지않으면 시스템에서 SuperVLAN인터페이스를 생성합니다. index는 SuperVLAN 인터페이스의 색인입니다. 유효한 값의 범위는 1에서 32사이 입니다. no 명령어를 이용하여 SuperVLAN 인터페이스를 삭제 할 수 있습니다.
[no] subvlan [setstr] [add addstr] [remove remstr]	SuperVLAN에서 SubVLAN을 구성하십시오. 추가된 하위 VLAN은 관리 인터페이스를 소유 할 수 없거나 다른 SuperVLAN에 속할 수 없습니다. 기본은 SuperVLAN에서 SubVLAN이 포함되어 있지 않습니다. Sub 명령어는 하나만 사용 할 수 있습니다. 'setstr'은 SubVLAN 목록을 설정하는 것을 의미 합니다. 예를 들어, List 2,4,-6은 VLAN2,4,5,6을 나타냅니다. 'add'는 원래의 SubVLAN목록에 VLAN목록을 추가하는 것을 의미 합니다 'addstr'은 위와 같은 형식의 문자열을 의미 합니다. 'remove'는 원래의 SubVLAN목록에서 VLAN 목록을 삭제하는 것을 의미합니다. 'remstr'는 위와 같은 형식의 목록의 문자열입니다. 'no' 명령어는 SuperVLAN에서 SubVLAN을 삭제하는 것을 의미 합니다, 'no'명령어은 하위 명령과 함께 사용할 수 없습니다.

SuperVLAN 인터페이스를 구성한 후 SuperVLAN인터페이스의 IP주소를 구성할 수 있습니다. SuperVLAN인터페이스는 다른 포트와 구성 할 수 있는 라우팅 포트이기도 합니다.

3-3장. 인터페이스 설정 예제

3.3.1 공통 속성의 인터페이스 구성

3.3.1.1 인터페이스 설명 예제

다음 예제에서는 인터페이스와 관련된 설명을 추가하는 방법을 보여줍니다. 이 설명은 구성 파일 및 인터페이스 명령을 디스플레이에서 나타납니다.

```
Interface vlan 1
Ip address 192.168.1.12 255.255.255.0
```

3.3.1.2 인터페이스 비활성화 예제

다음 예제에서는 이더넷 인터페이스 0/1을 비활성화 하는 방법을 보여줍니다.

```
Interface GigaEthernet0/1
shutdown
```

다음 예제에서는 인터페이스를 활성화 하는 방법을 보여줍니다.

```
Interface GigaEthernet0/1
no shutdown
```

4장 포트 특성 추가 설정

4-1장. 포트 보안

4.1.1 소개

포트 보안은 접근기능을 제어할 수 있습니다. 구성에 따라 특정 범위에서 포트를 실행할 수 있습니다. 포트의 보안 MAC 주소를 구성하여 포트의 보안 기능을 활성화 한 경우, 보안 MAC 주소가 안전하지 않으면 포트 보안의 위반이 발생합니다. 다른 위반 모드에 따라 조치를 해야 합니다.

보안 포트에는 다음과 같은 기능이 있습니다.

- 보안 MAC 주소의 개체 수를 설정
- 보안 MAC 주소의 정적 설정

  보안 포트에 고정 MAC 주소의 정적 설정 및 개체수의 지정이 없다면 동적 MAC 주소를 학습합니다.
- 보안 포트 위반이 발생하면 위반된 패킷 삭제

이 절에서는 스위치의 보안 포트를 설정하는 방법에 대해 설명 합니다.

4.1.2 포트 보안 목록 설정

- MAC 주소와 IP 주소를 바인딩 하여 설정 하십시오.

4.1.3 포트 보안 설정

4.1.3.1 MAC 주소와 IP 주소의 바인딩 설정

스위치의 IP 주소와 MAC 주소를 포트에 바인딩 하거나 둘 중 하나만 바인딩 할 수 있습니다.

Note:
IP 주소가 포트의 MAC 주소에 바인딩 된 후 바인딩 된 MAC 주소와 호환되지 않는 IP 주소를 필터링 합니다.

포트 구성 모드로 들어가서 다음 명령어를 실행하여 보안 포트에 대한 설정을 하십시오.

명령어	설명
switchport port-security bind {ip A.B.C.D | mac H.H.H}	IP 주소 / MAC 주소를 포트에 바인딩하십시오.

4-2장 포트 설정

정상적인 경우 이더넷 인터페이스는 알 수 없는 메시지를 이더넷 인터페이스가 있는 VLAN

에 브로드캐스트 합니다. 경우 따라 메시지를 전달 할 수 없습니다.

명령어	설명
switchport block {unicast|multicast|broadcast}	인터페이스는 유니캐스트, 멀티캐스트, 브로드캐스트 메시지를 전달하지 않습니다.
no switchport block {unicast | multicast | broadcast}	인터페이스는 모든 메시지를 전달합니다.

4-3장. 포트 보안

정상적인 경우 스위치의 다른 포트 사이에 패킷을 자유롭게 전달할 수 있습니다. 어떤 경우에는 다른 포트 사이의 패킷을 전달할 수 없습니다. Port isolation 기능은 포트 사이의 패킷 흐름을 차단할 수 있습니다. Port isolation이 있는 포트는 서로 통신할 수 없습니다. 패킷은 Port isolation이 없는 포트 사이 또는 Port isolation 와 non-Port isolation 사이에서 정상적으로 전달될 수 있습니다.

명령어	설명
switchport protected	Port isolation 설정
no switchport protected	Port isolation 설정 해제

4-4장. Storm control 기능 설정

스위치 포트는 유니캐스트(Mac 주소 검색 실패), 멀티캐스트 또는 브로드캐스트 메시지로부터 지속적이고 비정상적인 공격을 받을 수 있습니다. 이 경우 스위치 혹은 전체 스위치 포트에 무리가 됩니다. 현상을 억제하기 위한 설정이 지원 되어야 합니다.

명령어	설명
storm-control {broadcast | multicast | unicast} threshold count	브로드캐스트 | 멀티케스트 | 유니케스트의 지속적인 메시지를 제어합니다.
no storm-control {broadcast | multicast | unicast} threshold	storm-control 설정을 해제 합니다.

4-5장. 포트 속도 제한

구성을 통해 외부/내부 트래픽의 속도를 제어 할 수 있습니다.
글로벌 모드에서 다음 명령을 실행하여 포트의 트래픽 속도를 제어 하십시오.

명령어	설명
Interface g0/1	인터페이스 Gi0/1으로 들어갑니다.
[no] switchport rate-limit band [ingress | egress]	포트에 대한 트래픽 속도 제어를 구성합니다. 'band'는 제어할 트래픽 속도 입니다. 'ingress'는 들어오는 트래픽에 'egress'는 나가는 트래픽에 영향을 미친다는 것을 의미합니다.

4-6장. Port Loop Detection

설정을 하여 포트에서 루프가 발생하는지 여부를 감지 할 수 있습니다.
글로벌 모드에서 포트 구성을 입력하십시오.

명령어	설명
[no] keepalive	[해제] 루프 감지를 실행합니다.
keepalive period	루프 감지 기간을 설정합니다. 유효범위는 0에서 32767 입니다.

5장. 물리적인 포트의 특성 설정

5-1장. 물리적인 인터페이스의 특성 설정

5.1.1 이더넷 인터페이스 설정

이 절에서는 이더넷 인터페이스를 구성하는 방법에 대해 설명합니다. SFC6000 Series 스위치는 10/100/1000Mbps의 고속 이더넷 인터페이스를 지원합니다. 자세한 구성은 다음과 같습니다.
첫번째 단계는 필수 사항이며 다른 단계는 선택 사항입니다.

5.1.1.1 이더넷 인터페이스 설정

글로벌 모드에서 다음 명령을 실행하여 이더넷 인터페이스 구성 상태로 들어갑니다.

명령어	설명
Interface fastethernet [slot/port]	Fastethernet 인터페이스에 접속 합니다.
Interface gigaethernet [slot/port]	Gigaethernet 인터페이스에 접속 합니다.

'show run interface fastethernet' 명령어를 이용하여 이더넷 인터페이스의 상태를 확인 하십시오. 'show run interface gigaethernet' 명령어를 이용하여 기가비트 이더넷 인터페이스의 상태를 확인 하십시오.

5.1.1.2 Rate 설정 (Speed)

이더넷 속도는 자동협상 또는 인터페이스에서 설정을 하여 구현 할 수 있습니다.

명령어	설명
speed [10/100/1000/auto]	이더넷 인터페이스에 10M, 100M, 1000M 혹은 Auto-negotiation의 옵션을 이용하여 Rate값을 설정 합니다
no speed	Rate 옵션을 삭제 합니다. 기본 설정인 auto-negotiation으로 돌아갑니다.

Note:
SFP의 속도는 고정되어 있습니다. 예를 들어, GBIC 및 GE-FX의 속도는 1000M이고 FE-FX의 속도는 100M 입니다. SFP 속도 명령 다음에 자동 매개변수가 있으면 자동협상 기능을 사용할 수 있습니다. 그렇지 않으면 협상 할 수 없습니다. 기본 구성에서는 기가비트 인터페이스의 자동 협상을 활성화 할 수 있지만 100Mbps 인터페이스의 자동협상은 비활성화 입니다.

5.1.1.3 Duplex 모드 설정

기본 구성에서 이더넷 인터페이스는 자동협상을 통해 전 이중 또는 반 이중으로 될 수 있습니다. 이 명령은 SFP 인터페이스의 Duplex 모드는 항상 Auto 입니다.

명령어	설명
duplex [full | half | auto]	이더넷의 Duplex 모드를 설정합니다.
no duplex	기본 구성을 다시 시작 합니다. Duplex 모드는 Auto-negotiation 입니다.

5.1.1.4 Flow-Control 설정

인터페이스가 Full-duplex 일 때, 흐름제어는 802.3x 정의 하여 PAUSE프레임을 통해 실현됩니다. 인터페이스가 반 이중 모드인 경우 Flow-control은 배압을 통해 실현됩니다.

명령어	설명
flow-control on | off	인터페이스의 Flow-control을 실행하거나 끌 수 있습니다.
no flow-control	기본 구성으로 돌아갑니다. 인터페이스에는 flow-control이 없습니다.

6장. 인터페이스 범위 설정

6-1장 인터페이스 범위 설정

6.1.1. 인터페이스 범위 구성

6.1.1.1 인터페이스 범위의 이해

인터페이스를 설정하는 과정에서 같은 유형의 포트에 동일한 속성을 설정 해야 하는 경우가 있습니다. 각 포트에서 반복되는 구성을 피하기 위해 인터페이스 범위 설정 모드를 제공 합니다. 동일한 설정 매개변수로 동일한 유형 및 슬롯 번호 / 포트를 구성 할 수 있습니다. 이렇게 하면 작업량이 줄어 들게 됩니다.

Note :

인터페이스 범위 모드로 들어가면 모드에 포함된 인터페이스가 설정 되어 있어야 합니다.

6.1.1.2 인터페이스 범위 모드로 들어가기

‘interface range’ 모드로 들어가기 위해 다음 명령어를 실행 하십시오.

<table>
<tr><th>명령어</th><th>설명</th></tr>
<tr><td>Interface range type slot/<port1 - port2 | port3>[, <port1 - port2|port3>]</td><td>인터페이스 범위 모드로 시작합니다.
이 모드에 포함 된 모든 포트는 다음 조건에 일치 합니다.
슬롯 번호는 슬롯으로 설정 됩니다.
하이픈 앞뒤의 포트 번호는 port1과 port2 사이이거나 port3과 같아야 합니다. Port2는 port1보다 작아야 합니다.
하이픈 또는 쉼표 앞 뒤에 공백이 있어야 합니다.</td></tr>
</table>

6.1.1.3 설정 예제

슬롯 0 및 이더넷 1,2,3,6,8,10,11,12를 포함하여 다음 명령어를 통해 인터페이스 구성 모드를 시작 하십시오.

```
Switch_config# interface range 1 – 3 , 6 , 8 , 10 – 12
Switch_config_if_range#
```

7장 VLAN 설정

7-1장. VLAN 설정

7.1.1 VLAN 소개

Virtual LAN(VLAN)은 하나 이상의 LAN에 있는 논리적으로 네트워크 화 된 장치 그룹을 말하며 실제로 동일한 링크에 연결되어 있는 것처럼 통신 할 수 있습니다. 실제로 여러 LAN 세그먼트에 위치 합니다. 1999년 IEEE는 VLAN 구현 프로젝트를 표준화 하기 위해 IEEE 802.1Q 프로토콜 표준 초안을 설정했습니다. VLAN은 물리적 연결 대신 논리를 기반으로 하므로 사용자/호스트 관리, 대역폭 할당 및 리소스 최적화에 매우 유연합니다.

Virtual LAN에는 다음과 같은 유형이 있습니다.

- 포트 기반의 VLAN: 각 물리적 스위치 포트는 액세스 목록으로 VLAN원을 지정합니다.
- 802.1Q 트렁크 모드는 인터페이스에서 지원 됩니다.
- 액세스 모드 인터페이스가 지원 됩니다.
  포트 기반 VLAN은 스위치가 지원하는 VLAN의 하위 집합 중 하나의 포트를 할당 하는 것입니다. 이 VLAN하위 집합에 하나의 VLAN만 있는 경우 이 포트는 Access 포트 입니다
- VLAN 서용 범위는 인터페이스에서 지원 됩니다.
  VLAN허용 매개변수는 포트가 속한 VLAN 범위를 제어하는 데 사용됩니다. VLAN 태그가 없는 매개변수는 VLAN 태그가 없는 패킷을 할당 VLAN에 보내도록 포트를 설정하는데 사용됩니다.

7.1.2 VLAN 설정 작업 목록

- VLAN 추가 / 삭제
- 스위치 포트 설정
- VLAN 인터페이스 생성 / 삭제
- SuperVLAN 인터페이스 설정
- VLAN의 설정 및 상태 모니터링

7.1.3 VLAN 설정 작업

7.1.3.1 VLAN 추가 / 삭제

일반적으로 VLAN 이라고 하는 Virtual LAN은 실제 위치에 상관없이 동일한 회선에 연결되어 있는 것처럼 통신하는 일련의 공통 요구사항을 가진 호스트 그룹 입니다.

VLAN은 physical LAN과 동일한 속성을 갖지만 동일한 LAN 세그먼트에 있지 않더라도 종단 스테이션을 함께 그룹화 할 수 있습니다. VLAN에는 여러 개의 포트가 있을 수 있으며 모든 유니캐스트, 멀티캐스트 및 브로드캐스트 메시지는 동일한 VLAN에서 터미널로만 전달 될 수 있습니다. 각 VLAN은 논리적 네트워크 입니다. 데이터가 다른 VLAN에 도달하려면 라우터 또는 브리지로 전달해야 합니다.

다음 명령을 실행하여 VLAN을 설정 하십시오.

명령어	설명
vlan [vlan-id]	VLAN 설정 모드로 들어갑니다.(VLAN을 생성)
name [string]	VLAN의 이름을 설정 합니다.
vlan vlan-range	동시에 여러 개의 VLAN을 생성 할 수 있습니다.
no vlan [vlan-id] vlan-range	하나 이상의 VLAN을 삭제 할 수 있습니다.

VLAN은 VLAN 관리 프로토콜 GVRP를 통해 동적으로 추가 및 삭제를 할 수 있습니다.

7.1.3.2 스위치 포트의 설정

스위치 포트는 액세스 모드, 트렁크 모드 및 dot1q 터널모드를 지원합니다.

- 액세스 모드는 이 포트가 하나의 VLAN에만 종속되며 태그가 없는 이더넷 프레임 만 송수신 함을 나타냅니다
- 트렁크 모드는 이 포트가 다른 스위치에 연결되어 있고 태그가 있는 이더넷 프레임을 보내고 받을 수 있음을 나타냅니다.
- dot1q-tunnel 모드는 수신되지 않은 패킷을 태그가 없는 패킷으로 간주 합니다. 스위치 칩은 자동으로 포트의 pvid를 새 태그로 추가하므로 스위치가 네트워크에 연결된 다른 VLAN 파티션을 무시할 수 있습니다. 그런 다음 패킷은 동일한 고객의 다른 서브 네트워크에 있는 다른 포트로 변경 없이 전달됩니다. 투명 전송은 이러한 방식으로 실현됩니다.

각 포트에는 하나의 기본 VLAN 및 PVID가 있으며 포트에서 수신된 VLAN 태그가 없는 모든 데이터는 VLAN의 데이터 패킷에 속합니다. 트렁크 모드는 포트를 여러 VLAN으로 간주 할 수 있으며 전달할 패킷 종류와 포트에 전송된 패킷의 태그 수 또는 태그가 없는 VLAN 수 및 포트가 속한 VLAN 목록을 설정 할 수 있습니다.

다음 명령을 실행하여 스위치 포트를 설정하십시오.

명령어	설명
switchport pvid [vlan-id]	스위치포트에 PVID를 설정합니다.
switchport mode access | trunk | dot1q-tunnel	스위치포트 모드를 설정합니다.
switchport trunk vlan-allowed [vlan-id | all]	스위치포트에 허용할 VLAN을 지정합니다.
switchport trunk vlan-untagged [vlan-id]	스위치포트에 차단할 VLAN을 지정합니다.

Note : 모든 스위치가 dot1q-tunnel을 지원하는 것은 아닙니다.

일부 스위치는 이 기능을 전역 적으로 활성화/비활성화 하는 기능만 지원하며 다른 포트에 대해 다른 전략을 설정 할 수 없습니다.

dot1q-tunnel을 전역 적으로 활성화 하는 명령어는 다음과 같습니다.

명령어	설명
Double-tagging	스위치 전역으로 활성화 합니다.

7.1.3.3 VLAN 인터페이스 생성 / 삭제

VLAN 인터페이스는 네트워크 관리 또는 Layer-3계층의 라우팅 기능을 실현하기 위해 설정할 수 있습니다. VLAN 인터페이스는 IP 주소와 마스크를 지정하는 데 사용될 수 있습니다. 다음 명령어를 실행하여 VLAN 인터페이스를 설정하십시오.

명령어	설명
[no] interface vlan [vlan-id]	VLAN 인터페이스를 생성 /삭제 합니다.

7.1.3.4 SuperVLAN 인터페이스 설정

SuperVLAN 기술은 다음과 같은 메커니즘을 제공합니다. 동일한 스위치를 실행하는 다른 VLAN의 호스트를 통한 IPv4서브넷에 할당 할 수 있습니다. 따라서 많은 IP 주소가 저장 됩니다. SuperVLAN 기술은 서로 다른 VLAN을 하나의 VLAN 그룹으로 분류 해줍니다. 이 그룹의 VLAN은 동일한 관리 인터페이스를 사용합니다. 호스트는 동일한 IPv4 네트워크 섹션과 게이트웨이를 사용합니다. SuperVLAN에 속하는 VLAN을 SubVLAN이라고 합니다 SubVLAN은 IP 주소를 설정하여 관리 인터페이스를 소유 할 수 없습니다. 명령 줄을 통해 SuperVLAN인터페이스를 설정할 수 있습니다. SuperVLAN 설정하는 절차는 다음과 같습니다.

명령어	설명
[no] interface supervlan [index]	인터페이스 구성모드를 시작/삭제[no] 합니다. 지정된 SuperVlan 인터페이스가 없으며 시스템에서 SuperVlan인터페이스를 생성 합니다. Index는 SuperVlan의 색인입니다. 유효 값의 범위는 1에서 32 사이 입니다.
[no] subvlan [setstr] [add addstr] [remove remstr]	SuperVlan에서 SubVlan을 구성/삭제[no] 합니다. 추가된 하위 VLAN은 관리 인터페이스를 소유 할 수 없습니다. 원래 상태에서 SuperVlan에는 SubVlan이 포함되지 안습니다. 매번 하나의 하위 명령 만 사용할 수 있습니다. 'setstr'은 SubVlan 목록을 설정하는 것을 의미 합니다 예를 들어, List 2,4-6은 VLAN 2,4,5,6을 나타냅니다

	'add'는 원래의 SubVlan목록에서 Vlan목록을 추가 하는 것을 의미 합니다 'addstr'은 위와 같은 형식의 문자열을 의미 합니다. 'remove'는 원래의 SubVlan목록에서 Vlan 목록을 삭제 하는 것을 의미 합니다. 'remstr'은 위와 같은 형식의 목록의 문자열 입니다. SuperVlan에서 모든 SubVlan을 삭제할 수 있는 방법이 없습니다. No 명령어는 다른 하위 명령과 함께 사용할 수 없습니다.

SuperVLAN인터페이스를 구성한 후 SuperVLAN 인터페이스의 IP 주소를 구성 할 수 있습니다. SuperVLAN인터페이스는 다른 포트와 마찬가지로 구성 할 수 있는 라우팅 포트 이기도 합니다.

7.1.3.5 VLAN의 설정 및 상태 모니터링

VLAN의 구성 및 상태를 모니터링 하려면 관리모드에서 다음 명령을 실행하십시오.

명령어	설명
show vlan [id x | interface inff]	VLAN의 설정 값과 상태를 보여줍니다.
show interface [vlan | supervlan] x	VLAN/SuperVLAN의 포트 상태를 보여줍니다.

7.1.4 설정 예제

사용자PC1~PC6은 포트 1~6을 통해 스위치로 연결 합니다. 이 PC의 네트워크는 192.168.1.0/24 입니다. PC1~PC3그룹고 PC4~PC6그룹은 서로 다른 Layer-2 브로드캐스트 도메인에 위치하지만 PC1~PC6은 서로 Ping을 수행하고 IP 192.168.1.100을 통해 스위치를 관리 할 수 있습니다. 이렇게 하려면 포트 1-3은 VLAN1으로 4-6은 VLAN2로 설정해야 합니다. 그런 다음 SubVLAN으로 VLAN1과 VLAN2를 SuperVLAN에 추가해야 합니다. 스위치에서 다음 설정을 수행해야 합니다. (각 인터페이스의 default VLAN은 1으로 설정되어 있습니다)

```
interface fastethernet 0/4
switchport pvid 2
!
interface fastethernet 0/5
switchport pvid 2
!
interface fastethernet 0/6
```

```
switchport pvid 2
!
interface supervlan 1
subvlan 1,2
ip address 192.168.1.100 255.255.255.0
ip proxy-arp subvlan
!
```

8장. STP 설정

8-1장 STP 구성

8.1.1 STP 소개

표준 Spanning-Tree Protocol(STP)은 IEEE802.1D 표준을 기반으로 합니다. 스위치 Stack은 나머지 네트워크에 대한 단일 Spanning-Tree Node로 나타나며 모든 Stack맴버는 동일한 Bridge ID를 사용합니다. 달리 명시하지 않는 한 스위치라는 용어는 독립실행 형 스위치와 스위치 Stack을 나타냅니다. STP는 Spanning-Tree Algorithm을 사용하여 중복된 연결 네트워크의 스위치 하나를 Spanning-Tree Root로 선택합니다. Algorithm은 활성화된 포트의 역할에 따라 각 포트의 영역을 할당하여 Layer-2스위치의 네트워크를 루프 없는 최상의 네트워크 경로를 계산합니다.

STP는 네트워크의 루프를 방지하면서 경로의 중복을 제공하는 Layer-2 Link 관리 프로토콜 입니다. Layer-2 이더넷 네트워크가 제대로 작동하려면 두 Station 사이에 하나의 활성화 경로 만 존재할 수 있습니다. End-station 간의 여러 활성 경로로 인해 네트워크에 루프가 발생합니다. 네트워크에 루프가 있으면 End-Station에 중복된 메시지가 수신 될 수 있습니다. 또한 스위치는 여러 Layer-2 인터페이스에서 End-Station MAC 주소를 학습 할 수 있습니다. 이러한 조건은 불안정한 네트워크를 초래 합니다. Spanning-Tree 작업은 End-Station에서 투명하므로 단일 LAN 세그먼트 또는 여러 세그먼트의 스위치 LAN에 연결되어 있는지 여부를 감지 할 수 없습니다.

STP는 Spanning-Tree Algorithm을 사용하여 중복 연결된 네트워크의 스위치 하나를 Spanning-Tree의 Root로 선택 합니다. 이 Algorithm은 활성 토폴로지의 포트 역할에 따라 각 포트에 역할을 할당하여 Layer-2네트워크의 최상의 루프 없는 경로를 계산 합니다.

표준 Spanning-Tree(STP)는 IEEE802.1D에 정의되어 있습니다. 이는 단일 Spanning-Tree에서 여러 Bridge로 구성된 LAN 토폴로지를 단순화하여 네트워크 루프가 발생하지 않도록 하고 네트워크의 안정적인 작동을 보장 합니다. STP 및 해당 Protocol의 Algorithm은 랜덤 Bridging LAN을 간단한 연결을 사용하는 활성 토폴로지로 구성합니다. 활성 토폴로지에서 일부 Bridging port는 프레임을 전달 할 수 있습니다. 일부 포트는 정체 상태에 있고 프레임을 전송할 수 없습니다 일부 포트는 정체 상태에 있고 프레임을 전송할 수 없습니다. 장애 상태에 있는 포트는 토폴로지에서 종결 될 수 있습니다. 장치가 비효율적이거나 네트워크에 추가되거나 네트워크에서 제거되면 정상적인 포트 전송 상태로 변경이 됩니다. STP 토폴로지에서 Bridge는 Root로 볼 수 있습니다. 모든 LAN섹션에서 Bridging 포트는 네트워크 섹션의 데이터를 루트로 전달합니다. 포트는 네트워크 섹션의 지정된 포트로 표시 합니다. 포트가 있는 브리지는 LAN의 지정된 브리지로 간주됩니다. Root는 Root가 연결하는 모든 네트워크 섹션의 지정된 Bridge 입니다. 각 Bridge의 포트에서 Root에 가장 가까운 포트가 Bridge Root 포트 입니다. Root 포트 및 지정된 포트(사용 가능한 경우)만 전송 상태 입니다. 다른 유형의 포트는 종료되지 않지만 Root포트 또는 지정된 포트가 아닙니다. 우리는 이들 포트를 대기 포트라고 부릅니

다. 다음 매개변수는 안정화된 활성 토폴로지의 구조를 결정합니다.

다음 매개변수는 안정화 된 활성 토폴로지의 구조를 결정 합니다:

(1) 각 브리지의 식별자

(2) 각 포트의 Path Cost

(3) 브리지의 각포트에 대한 포트 식별자

Spanning-Tree 포트의 Priority 값은 네트워크 토폴로지의 포트 위치와 트래픽을 통과시키는 위치를 나타냅니다. 최상위 우선순위(식별자 값이 가장 작은 Bridge)가 Root로 선택 됩니다. 각 Bridge의 포트에 Root Path Cost이 있습니다. 즉, Root에서 Bridge까지의 모든 포트의 경로 비용 합계 중 최소값입니다. 각 네트워크 세그먼트의 지정된 포트는 네트워크 세그먼트에 연결되며 최소 Path Cost를 갖는 포트를 나타냅니다. 스위치의 두 포트가 Loop의 일부분인 경우 Spanning-Tree의 Port Priority 및 Path Cost 설정은 어떤 포트에 전달하고 있는 상태에 있고 어떤 포트가 차단 상태에 있는지를 제어 합니다. Spanning-Tree 포트의 Priority값은 네트워크 토폴로지의 포트 위치와 트래픽을 통과시키는 위치를 나타냅니다. 경로 비용 값은 포트의 속도를 나타냅니다.
SFC6000 Series 스위치는 Spanning-Tree 표준인 802.1D(STP)와 802.1W(RSTP)의 두가지 모드를 지원 합니다. 또한 VLAN 및 MSTP Spanning-Tree 프로토콜에 따라 STP 모드를 설정 하는 것을 지원 합니다.
자세한 내용은 2장의 'STP 모드 및 모델 표'를 참조 하십시오.

이 장에서는 스위치가 지원하는 표준 Spanning-Tree 프로토콜 구성방법을 설명 합니다.

Note: 이 문서는 802.1D(STP) 및 802.1W(RSTP)를 SSTP 및 RSTP로 약칭 합니다.
SSTP는 단일 신장 트리를 의미 합니다.

8.1.2 SSTP 설정 작업 목록

- STP 모드 선택
- STP의 활성화 및 비활성화
- 스위치의 Priority 설정
- Hello time 설정
- Max-Age time 설정
- Forward Delay time 설정
- Port Priority 설정
- Path Cost 설정
- Auto-Designated port 설정
- STP 상태 모니터링

8.1.3 SSTP 설정 작업

8.1.3.1 STP 모드 설정

다음 명령을 실행하여 STP 모드를 구성 하십시오.

명령어	설명
spanning-tree mode (sstp | rstp)	STP의 모드를 설정 합니다.

8.1.3.2 STP의 활성화 및 비활성화

Spanning-Tree는 기본적으로 사용하도록 설정이 되어 있습니다. 네트워크 토폴로지에 루프가 없다고 확신하는 경우에만 Spanning-Tree를 'Disable'하십시오.

Spanning-Tree를 비활성화 하려면 다음 단계를 수행 하십시오:

명령어	설명
no spanning-tree	STP를 비활성화 합니다.

Spanning-Tree를 활성화 하려면 다음 명령을 사용하십시오.

명령어	설명
spanning-tree	STP를 실행 합니다. (기본값 : SSTP)
spanning-tree mode {sstp | rstp}	STP 모드를 설정 합니다.

8.1.3.3 스위치의 우선순위 설정

스위치의 Priority 를 구성하고 Stack의 독립형 스위치 또는 스위치가 Root 스위치로 선택 될 가능성을 높일 수 있습니다.

스위치 Priority를 구성하려면 다음 명령을 사용 하십시오.

명령어	설명
[no] spanning-tree sstp priority [value]	스위치의 Priority 값을 설정 합니다. 'no' 명령어로 기본 설정으로 되돌립니다. (기본값 : 32768)

8.1.3.4 Hello Time 설정

사용자는 Hello time을 변경하 Root스위치가 전송한 STP 데이터 단위 사이의 간격을 설정 할 수 있습니다.

다음 명령을 사용하여 SSTP의 Hello time을 설정 하십시오.

명령어	설명
[no] spanning-tree sstp hello-time [value]	SSTP의 Hello time을 설정 합니다. 'no' 명령어로 기본 설정으로 되돌립니다. (기본값 : 4s)

8.1.3.5 Max-age time 설정

SSTP의 Max-age를 사용하여 재구성을 시도하기 전에 Spanning-tree 설정 메시지를 수신하지 않고 스위치가 대기하는 시간(초)을 구성 합니다.

Maximum-aging time을 설정 하려면 다음 단계를 수행하십시오.

명령어	설명
[no] spanning-tree sstp max-age [value]	SSTP의 Max-age를 설정 합니다. 'no' 명령어로 기본 설정으로 되돌립니다. (기본값 : 20s)

8.1.3.6 Forward Delay 시간 설정

SSTP의 Forward-delay를 구성하여 Spanning-Tree의 Learning 및 수신대기 상태에서 전달 상태로 변경하기 전에 인터페이스가 대기하는 시간(초)을 결정 합니다.

다음 명령을 사용하여 SSTP의 Forward delay time을 설정 하십시오.

명령어	설명
[no] spanning-tree sstp forward-time [value]	SSTP의 Max-age를 설정 합니다. 'no' 명령어로 기본 설정으로 되돌립니다. (기본값 : 15s)

8.1.3.7 포트 우선순위 설정

Loop가 발생하면 Forwarding 상태로 만들 인터페이스를 선택할 때 Spanning-Tree가 Port Priority를 사용하여 우선순위를 사용합니다. 선택한 우선순위가 높은 인터페이스에 더 높은 Priority 값(낮은 값)을 할당하고 마지막에 선택한 우선순위 값(높은 값)을 할당 할 수 있습니다. 모든 인터페이스의 우선 순위 값이 같으면 Spanning-Tree는 가장 낮은 Priority값을 갖고 있는 인터페이스를 Forwarding 상태로 만들고 다른 인터페이스를 차단 합니다.

다음 명령을 이용하여 인터페이스에 Port-Priority 값을 설정 하십시오.

명령어	설명
[no] spanning-tree port-priority [value]	해당 Port의 priority값을 설정 합니다. 'no' 명령어로 설정을 삭제 합니다.
[no] spanning-tree sstp port-priority [value]	해당 port의 SSTP priority값을 설정 합니다. 'no' 명령어로 기본 설정으로 되돌립니다. (기본값 : 128)

8.1.3.8 Path Cost 설정

다음 명령어를 이용하여 각 사용 port에 설정 하십시오:

명령어	설명
[no] spanning-tree cost [value]	해당 port의 Cost를 설정 합니다. 'no' 명령어로 설정을 삭제 합니다.
[no] spanning-tree sstp cost [value]	해당 port의 SSTP Cost 값을 설정 합니다. 'no'명령어로 기본 설정으로 되돌립니다.

8.1.3.9 Auto-Designated Port 설정

자동으로 지정된 포트는 SFC6000 Series 스위치의 특수 기능입니다. 이 기능을 사용하려면 라인카드가 BPDU를 Auto-Designated Port로 자동 전송하여 MSU의 부하를 줄일 수 있습니다. Auto-Designated Port기능은 STP 모드에서 효과적입니다. 글로벌 모드에서 다음 명령을 실행하여 SFC6000 Series 스위치의 Auto-Designated Port의 기능을 설정 하십시오.

명령어	설명

[no] spanning-tree designated-auto	Auto-Designated Port 기능을 활성화 합니다. 'no' 명령어로 기능을 비활성화 합니다..

8.1.3.10 STP 상태 모니터링

STP 구성 및 상태를 모니터링 하려면 관리 모드에서 다음 명령어를 사용하십시오.

명령어	설명
show spanning-tree	사용중인 인터페이스에 대해서만 STP의 정보를 보여줍니다.
show spanning-tree detail	인터페이스 정보에 대해 자세한 요약을 보여줍니다.
show spanning-tree interface	지정된 인터페이스에 대한 spanning-tree 정보를 표시 합니다.

8.1.4 VLAN Spanning-Tree 설정

8.1.4.1 개요

SSTP 모드에서 전체 네트워크에는 하나의 STP 엔트리만 있습니다. STP의 스위치 포트 상태는 모든 VLAN에서 상태를 결정합니다. 네트워크에 여러 VLAN이 있는 경우 단일 STP와 네트워크 토폴로지를 분리하면 네트워크의 일부 통신장애가 발생할 수 있습니다. 스위치는 특정목적의 VLAN에서 독립적인 SSTP를 실행하여 포트가 다른 VLAN에서 다른 상태를 유지하고 VLAN간에 로드 균형이 유지되도록 합니다. 스위치는 최대 30개의 VLAN에서 독립적인 STP를 실행할 수 있습니다. 다른 VLAN 토폴로지는 STP에 의해 제어되지 않습니다.

8.1.4.2 VLAN STP 설정 작업

글로벌 모드에서 다음 명령어를 사용하여 VLAN의 SSTP 설정을 하십시오.

명령어	설명
spanning-tree mod pvst	Vlan 기반의 STP 모드를 시작합니다.
[no] spanning-tree vlan [vlan-id]	지정된 VLAN에 STP를 설정합니다. [no]명령어로 해당 설정을 삭제합니다.
[no] spanning-tree vlan [vlan-id] priority [value]	해당 Vlan의 STP의 우선순위를 설정합니다. [no]명령어로 해당 설정을 삭제합니다.
[no] spanning-tree vlan [vlan-id] forward-time [value]	해당 VLAN에 Forward-time을 설정합니다. [no]명령어로 해당 설정을 삭제합니다.
[no] spanning-tree vlan [vlan-id] max-age [value]	해당 VLAN에 max-age time을 설정합니다. [no]명령어로 해당 설정을 삭제합니다.
[no] spanning-tree vlan [vlan-id] hello-time [value]	해당 VLAN에 hello-time을 설정합니다. [no]명령어로 해당 설정을 삭제합니다.

포트 구성 모드에서 다음 명령어를 사용하여 포트의 속성을 구성합니다.

명령어	설명
[no] spanning-tree vlan [vlan-id] cost [value : 1-200000000]	포트에 지정된 VLAN의 cost 값을 설정합니다. [no]명령어로 해당 설정을 삭제합니다.
[no] spanning-tree vlan [vlan-id] port-priority [value : 0-240]	포트에 지정된 VLAN의 Priority를 구성합니다.. [no]명령어로 해당 설정을 삭제합니다.

모니터모드 또는 구성모드에서 다음 명령어를 실행하여 지정된 VLAN의 STP 상태를 확인합니다.

명령어	설명
show spanning-tree vlan [vlan-id]	VLAN에 설정 되어있는 STP상태를 확인합니다.

8.1.5 RSTP 설정 작업 목록

- 스위치의 RSTP 활성화 및 비활성화
- 스위치의 Priority 설정
- Forward Delay 시간 설정
- Hello 시간 설정
- Max-age 설정
- Path Cost 설정
- Protocol 변환 적용 확인하기

8.1.6 RSTP 설정 방법

8.1.6.1 스위치의 RSTP 활성화 및 비활성화

글로벌 모드에서 다음 설정을 확인 하십시오.

명령어	설명
[no] spanning-tree mode rstp	RSTP를 활성화 합니다.. [no]명령어로 해당 설정을 삭제합니다.

8.1.6.2 스위치의 우선순위 설정

스위치의 Priority를 설정하고 설정 스위치의 Root 스위치로 선택 될 수 있도록 합니다.
스위치의 우선순위를 구성하려면 글로벌 모드에서 다음 명령어를 실행하십시오.

명령어	설명
[no] spanning-tree rstp Priority [value]	RSTP의 우선순위를 설정합니다. [no]명령어로 해당 설정을 삭제합니다.

Note : 전체 네트워크에서 모든 Bridge의 Priority가 동일한 값을 사용하면 가장 작은 MAC 주소를 가진 스위치가 Root Bridge로 선택됩니다. RSTP 프로토콜이 사용되는 상황에서 브리지의 우선순위 값이 수정되면 Spanning-Tree를 다시 계산합니다. (Bridge의 Priority의 기본값 설정은 32768 입니다.)

8.1.6.3 Forward Delay 시간 설정

링크의 오류로 인해 네트워크가 Spanning-tree 구조를 다시 계산하는 경우 최신 구성 메지지는 전체 네트워크로 전달 될 수 없습니다. 새로 선택한 Root-Port와 지정된 Port가 데이터 전달을 즉시 시작 하면 일시적인 경로의 Loop가

발생할 수 있습니다. 따라서 이 Protocol은 일종의 국가 이주 메커니즘을 채택합니다. Root-port와 중간 port가 데이터 전송을 시작하기 전의 상태(Forward-delay 시간)가 지나면 Spanning-tree 정보를 전달하기 시작합니다. 이 Forward-delay 시간은 새로 구성된 메시지가 전체 네트워크로 전달되도록 합니다. Bridge의 Forward-delay 특성은 스위치 네트워크의 크기와 관련됩니다. 일반적으로 네트워크 크기가 클수록 Forward-delay 시간의 값을 길게 설정 해야 합니다.

명령어	설명
[no] spanning-tree rstp forward-time [value]	RSTP의 forward-delay 시간을 설정합니다. [no]명령어로 해당 설정을 삭제합니다.

Note : Forward-delay 시간을 비교적 작은 값으로 구성하면 일시적인 경로가 더 길어질 수 있습니다. Forward-delay 시간을 큰 값으로 구성하면 시스템이 오랫동안 연결을 재개하지 못할 수 있습니다. 사용자는 기본 값을 사용하는 것이 좋습니다. (기본값 : 15초)

8.1.6.4 Hello 시간 설정

적절한 Hello 시간을 사용하면 Bridge가 많은 네트워크 리소스를 차지하지 않고도 네트워크의 링크 오류를 감지할 수 있습니다.
글로벌 모드에서 다음 명령어를 사용하십시오.

명령어	설명
[no] spanning-tree rstp hello-time [value]	RSTP의 hello 시간을 설정합니다. [no]명령어로 해당 설정을 삭제합니다.

Note : 사용자는 기본 값을 사용하는 것이 좋습니다 (기본값 : 4초)

8.1.6.5 Max-age 설정

Max-age는 스위치가 재구성을 시도하기 전에 Spanning-tree 설정 메시지를 수신하지 않고 대기하는 시간(초) 입니다.
글로벌 모드에서 다음 명령어를 사용하십시오.

명령어	설명
[no] spanning-tree rstp max-age	RSTP의 max-age를 설정합니다.

[value]	[no]명령어로 해당 설정을 삭제합니다.

기본값을 사용하는 것을 권장합니다.

Note : Max-age를 작은 값으로 구성하면 Spanning-tree 계산이 빈번해지며 Spanning-tree 링크의 Block상태를 장애로 간주 할 수 있습니다. Max-age를 큰 값으로 구성하면 링크 상태를 명확하게 확인 할 수 없습니다. (기본값 : 20초)

8.1.6.6 Path Cost 설정

Spanning-tree의 Path Cost는 인터페이스의 속도에 확인 할 수 있습니다. Loop가 발생하면 Forwarding 상태로 마들 인터페이스를 선택할 때 Spanning-Tree가 Cost를 사용합니다. 먼저 선택한 인터페이스에 낮은 Cost값을 할당하고 마지막으로 선택한 인터페이스에 높은 Cost를 지정 할 수 있습니다. 모든 인터페이스의 Cost 값이 같으면 Spanning-Tree는 가장 낮은 Cost값을 갖는 인터페이스를 전달 상태로 만들고 다른 인터페이스를 차단 합니다.

인터페이스 설정 모드에서 인터페이스의 Cost값을 설정할 수 있습니다.

명령어	설명
[no] spanning-tree rstp cost [value]	RSTP의 cost를 설정합니다. [no]명령어로 해당 설정을 삭제합니다.

Note : 이더넷 포트의 우선순위를 수정하면 Spanning-tree를 다시 계산합니다.
사용자는 기본값을 사용하고 RSTP 프로토콜이 현재 이더넷의 경로비용을 계산하도록 할 것을 권장합니다.
포트의 속도가 10Mbps이면 이더넷 인터페이스의 Path Cost는 2000000 입니다.
포트의 속도가 100Mbps이면 이더넷 인터페이스의 Path Cost는 200000 입니다.

8.1.6.7 Port Priority 설정

루프가 발생하면 Forwarding 상태로 만들 인터페이스를 선택할 때 Spanning-tree가 포트의 우선순위를 사용합니다. 먼저 선택한 인터페이스에 우선순위가 낮은 값을 지정하고 마지막에 선택한 인터페이스에 우선순위가 높은 값을 지정 할 수 있습니다. 모든 인터페이스의 우선순위 값이 같으면 Spanning-Tree는 가장 낮은 인터페이스 번호(MAC)를 가진 인터페이스를 전달 상태로 만들고 다른 인터페이스를 차단 합니다.

해당 인터페이스 설정 모드에서 Port-priority 값을 설정 할 수 잇습니다.

명령어	설명
[no] spanning-tree rstp port-priority [value]	RSTP의 port-priority를 설정합니다. [no]명령어로 해당 설정을 삭제합니다.

Note : 이더넷 인터페이스에 Port-Priority를 수정하면 Spanning-Tree를 다시 계

산합니다. (기본값 : 128)

8.1.6.8 프로토콜 변환 사용 확인

RSTP 프로토콜을 통해 스위치는 일종의 프로토콜 변환 메커니즘을 이용하여 기존의 802.1D(STP) 스위치와 연결 할 수 있습니다. 스위치의 한 인터페이스가 STP의 구성 정보를 수신하면 인터페이스는 STP 패킷만 전송하는 인터페이스로 변환됩니다. 인터페이스가 STP 호환 상태가 되면 이 인터페이스가 더 이상 802.1D STP BPDU를 수신하지 않더라도 인터페이스가 RSTP 상태로 돌아가지 않습니다. 인터페이스를 RSTP 모드로 되돌리려면 'spanning-Tree rstp migration-check' 명령을 사용하여 다음을 수행할 수 있습니다. 인터페이스에서 프로토콜 변환검사 프로세스를 활성화 합니다.

Note: IEEE 802.1D 2004 RSTP를 지원하는 스위치만 'migration-check' 명령어를 지원 합니다.

글로벌 모드에서 다음 명령어를 실행하여 RSTP 변환 확인을 재시작 하십시오.

명령어	설명
spanning-tree rstp migration-check	프로토콜 변환 체크 확인을 모든 포트에서 재시작 합니다.

포트구성모드에서 해당 포트의 프로토콜 변환 검사를 수행 할 수 있습니다.

명령어	설명
spanning-tree rstp migration-check	프로토콜 변환 체크 확인을 해당 포트에서 재시작 합니다.

8-2장 MSTP 설정

8.2.1 MSTP 개요

8.2.1.1 소개

MSTP(Multiple Spanning Tree Protocol)는 Bridge LAN에서 간단하고 완벽한 토폴로지를 만드는 데 사용됩니다. MSTP는 STP(Spanning Tree Protocol) 및 RSTP(Rapid Spanning Tree Protocol)와 호환 될 수 있습니다. STP와 RSTP 모두 단독 STP 토폴로지로 만들 수 있습니다. 모든 VLAN메시지는 유일한 STP를 통해 전달 됩니다. STP는 너무 느리게 인식되고 RSTP는 Handshake 메커니즘을 통해 빠르고 안정적인 네트워크 토폴로지를 보장 합니다. MSTP는 RSTP의 빠른 Handshake 메커니즘을 사용합니다. 동시에 MSTP는 다른 VLAN을 다른 STP에 배포 하여 네트워크에 여러 토폴로지를 생성 할 수 있습니다. MSTP에 의해 생성된 네트워크에서 다른 VLAN의 프레임을 다른 경로를 통해 전달할 수 있으므

로 VLAN 데이터의 균형을 실현 할 수 있습니다. VLAN이 STP를 배포하는 메커니즘과 달리 MSTP는 여러 VLAN을 하나의 STP 토폴로지에 분산시켜 많은 VLAN을 지원하는데 필요한 STP를 효과적으로 줄일 수 있습니다.

8.2.1.2 MSTP Domain

MSTP에서 VLAN과 STP간의 관계는 MSTP 구성 테이블을 통해 설명됩니다 MSTP 설정 테이블, 설정 이름 및 설정번호는 MSTP 구성의 식별자 역할을 합니다.
네트워크에서 동일한 MSTP구성 식별자가 있는 상호 연결된 브리지는 동일한 MSTP 영역으로 포함 됩니다. 동일한 MSTP 영역의 Bridge는 항상 동일한 VLAN의 구성을 갖게 되므로 VLAN프레임이 MSTP 영역에 전송되도록 합니다.

8.2.1.3 IST, CST, CIST and MSTI

그림2.1은 3개의 MSTP 영역과 802.1D(STP)를 실행하는 스위치를 포함하는 MSTP 네트워크를 보여줍니다.

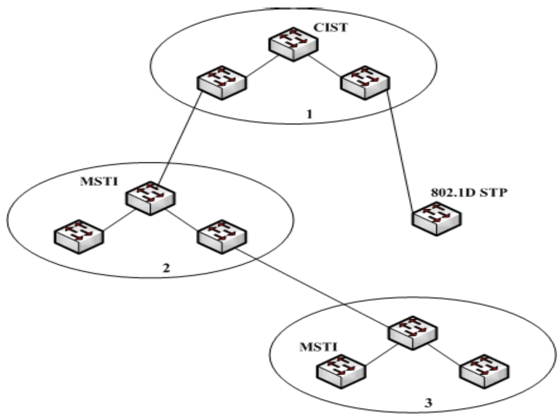


그림 2.1 MSTP 토폴로지

(1) CIST

공통 및 내부 Spanning-Tree(CIST)는 모든 단일 스위치 및 상호 연결된 LAN으로 구성된 Spanning-Tree를 의미 합니다. 이러한 스위치는 다른 MSTP영역에 속할 수 있습니다. 전통적인 STP 또는 RSTP를 실행하는 스위치 일 수 있습니다. MSTP영역에서 STP 또는 RSTP를 실행하는 스위치는 해당 지역에 있는 것으로 간주 됩니다. 네트워크 토폴로지가 안정된 후에 전체 CIST가 CIST Root Bridge를 선택합니다. 내부 CIST Root Bridge는 각 영역에서 선택되며, 이는 영역중심에서 CIST Root까지 최단 경로 입니다.

(2) CST

각 MSTP 영역을 단말 스위치로 보는 CST(Common Spanning Tree)는 모든 "단일스위치"를 연결하는 Spanning-Tree 입니다. 그림2.1에서 볼 수 있듯이 영역1, 2 및 3과 STP 스위치는 네트워크 CST를 구성합니다.

(3) IST

IST(Internal Spanning Tree)는 MSTP 영역에 있는 Cost의 일부, 즉 IST와 CST가 CIST를 구성하는 부분을 나타냅니다.

(4) MSTI

MSTP를 통해 서로 다른 VLAN을 다른 Spanning-tree에 분산시킬 수 있습니다. 그러면 여러 Spanning-tree 인스턴스가 만들어집니다. 일반적으로 No.0 Spanning-tree인스턴스는 전체 네트워크로 확장될 수 있는 CIST를 의미 합니다. No.1에서 시작하는 모든 Spanning-tree 인스턴스는 특정 영역에만 있습니다. 각 Spanning-tree 인스턴스는 여러 VLAN과 함께 분산 될 수 있습니다. 원래 상태에서는 모든 VLAN이 CIST에 분산되어 있습니다.
MSTP 영역의 MSTI는 독립적입니다. 각각의 스위치는 자신을 Root Bridge로 만들 수 있습니다.

8.2.1.4 포트 역할

MSTP에서 포트는 RSTP와 비슷한 역할을 하며 각각의 다른 역할을 합니다.

(1) Root Port

Root-port는 현재 스위치와 Root-bridge 사이의 경로를 나타내며 Root의 Path Cost는 최소 입니다.

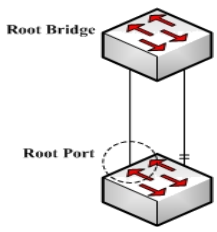


그림 2.2 Root port

(2) Alternate port

Alternate port는 현재 스위치와 Root-bridge 사이의 백업 경로 입니다. Root-port의 연결이 유효하지 않은 Alternate port는 작업 중단 없이 즉시 새로운 Root-port로 전환 할 수 있습니다.

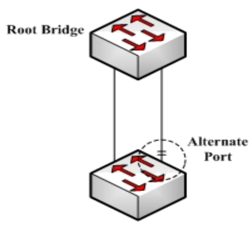


그림 2.3 Alternate port

(3) Designated port

Designated port는 다음 지역의 스위치 또는 LAN을 연결할 수 있습니다. 현재 LAN과 Root-Bridge사이의 경로 입니다.

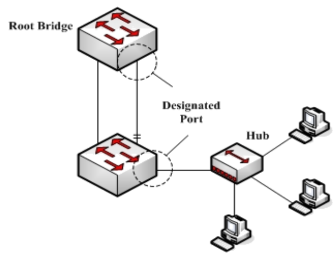


그림 2.4 Designated port

(4) Backup port

2개의 스위치 포트가 직접 연결되거나 둘 모두가 동일한 VLAN에 연결될 때 우선순위가 낮은 포트는 Backup port가 되고 다른 포트는 Designated port가 됩니다. Designated port가 장애가 발생할 경우 Backup port는 Designated port로 작동하여 작업을 계속 합니다.

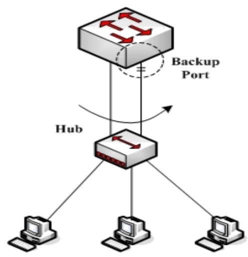


그림 2.5 Backup port

(5) Master port

Master port는 MSTP 영역과 CIST Root-bridge 사이의 최단 경로 입니다. Master port는 CIST 영역에서 Root-bridge의 Root-port 입니다.

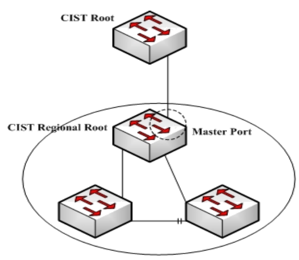


그림 2.6 Master port

(6) Boundary port

CIST의 경계 포트의 개념은 MSTI의 경계 포트와 약간 다릅니다. MSTI에서 경계 포트의 역할은 Spanning-tree 인스턴스가 포트에서 확장되지 않음을 의미합니다.

(7) Edge port

RSTP 또는 MSTP에서 Edge-port는 네트워크 호스트에 직접 연결되는 포트를 의미 합니다. 이 포트는 네트워크에서 루프를 유발하지 않고 직접 포워딩 상태로 들어갈 수 있습니다.

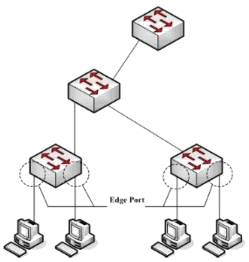


그림 2.7 Edge port

원래 상태에서 MSTP 및 RSTP는 모든 포트를 Edge-port로 사용하지 않으므로 네트워크 토폴로지를 신속하게 만들 수 있습니다. 이 경우 포트가 다른 스위치에서 BPDU를 수신하면 포트가 Edge 상태에서 정상 상태로 재개 됩니다. 포트가 802.1D STP BPDU를 수신하면 포트는 두배의 전달 지연 시간을 기다린 다음 전달 상태로 들어갑니다.

8.2.1.5 MSTP BPDU

STP와 RSTP와 마찬가지로 MSTP를 실행하는 스위치는 BPDU(Bridge protocol data unit)를 통해 서로 통신 할 수 있습니다. CIST 및 MSTI에 대한 모든 구성 정보는 BPDU에서 전달할 수 있습니다. 다음 표 2.1과 표 2.2는 MSTP에서 사용하는 BPDU의 구조를 나열합니다.

표 2.1 MSTP BPDU

Field Name	Byte Number
Protocol Identifier	1 – 2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6– 13
CIST External Root Path Cost	14 – 17
CIST Regional Root Identifier	18 – 25
CIST Port Identifier	26 – 27
Message Age	28 – 29
Max Age	30 – 31
Hello Time	32 – 33
Forward Delay	34 – 35

Version 1 Length	36
Version 3 Length	37 – 38
Format Selector	39
Configuration Name	40 – 71
Revision	72 – 73
Configuration Digest	74 – 89
CIST Internal Root Path Cost	90 – 93
CIST Bridge Identifier	94 – 101
CIST Remaining Hops	102
MSTI Configuration Messages	103 ~

표 2.2 MST configuration 정보

Field Name	Byte Number
MSTI FLAGS	1
MSTI Regional Root Identifier	2– 9
MSTI Internal Root Path Cost	10 – 13
MSTI Bridge Priority	14
MSTI Port Priority	15
MSTI Remaining Hops	16

8.2.1.6 안정 상태 확인

MSTP 스위치는 계산을 수행하고 수신된 BPDU에 따라 작업을 비교하고 마지막으로 다음을 보장합니다.

- 하나의 스위치가 전체 네트워크의 CIST Root로 선정 됩니다.
- 각 스위치 및 VLAN 세그먼트는 CIST Root에 대한 최소 Path cost 경로를 결정하여 완벽한 연결을 보장하고 Loop를 방지할 수 있습니다.
- 각 영역은 CIST 영역 Root로 전환됩니다. 스위치에는 CIST Root에 대한 최소 Path cost 경로가 있습니다.
- 각 MSTI는 스위치를 MSTI 영역 Root로 독립적인 선택을 할 수 있습니다.
- 영역 및 LAN 세그먼트의 각 스위치는 MSTI Root에 대한 최소 Path cost를 결정할 수 있습니다.
- CIST의 Root-port는 CIST 영역 Root와 CIST Root 사이의 최소 Path cost 경로를 제공 합니다.
- CIST의 Designated-port는 LAN에 CIST Root에 대한 최소 Path cost 경로를 제공 합니다.

- Alternated port와 Backup port는 스위치, 포트 또는 LAN이 작동하지 않거나 제거될 때 연결을 제공 합니다.
- MSTI Root-port는 MSTI 영역 Root에 대한 최소 Path cost 경로를 제공 합니다.
- Master port는 영역과 CIST Root 사이의 연결을 제공합니다. 이 지역에서 CIST 영역 Root의 CIST Root-port는 해당 지역의 모든 MSTI의 Master port로 동작합니다.

8.2.1.7 Hop 계산

MSTP를 사용하면 스위치가 프로토콜 변환 메커니즘을 통해 기존의 STP 스위치와 함께 작동 할 수 있습니다. 스위치의 한 포트가 STP 구성 메시지를 수신하면 포트는 STP 메시지만 전송합니다. 동시에 STP 정보를 수신하는 포트는 경계 포트로 간주 됩니다.

Note : 포트가 STP 호환 상태에 있으면 포트가 STP 메시지를 더 이상 수신하지 않더라도 포트는 자동으로 MSTP 상태로 재개되지 않습니다. 이 경우 'spanning-tree mstp migration-check' 명령어를 실행하여 포트가 학습한 STP 메시지를 지우고 포트를 MSTP 상태로 되돌릴 수 있습니다. RSTP 프로토콜을 실행하는 스위치는 MSTP 메시지를 식별하고 처리할 수 있습니다. 따라서 MSTP 스위치는 RSTP 스위치와 함께 작도할 때 프로토콜 변환이 필요하지 않습니다.

8.2.2 MSTP 설정 작업 목록

- 기본 MSTP 설정
- MSTP의 활성화 및 비활성화
- MSTP의 영역 설정
- 네트워크 Root 설정
- Secondary Root 설정
- Bridge priority 설정
- STP의 시간 매개변수 설정
- 네트워크의 크기 설정
- 최대 Hop-Count 설정
- Port priority 설정
- 포트의 Path cost 설정

- 포트의 연결 타입 설정
- MST 호환 모드 활성화

8.2.2.1 MST-호환모드 활성화

스위치가 지원하는 MSTP 프로토콜은 IEEE802.1S를 기반으로 합니다. 다른 MSTP, 특히 시스코 스위치가 지원하는 MSTP와 호환 되도록 MSTP 프로토콜은 MST 호환 모드에서 작동 할 수 있습니다. MSTP 호환모드에서 실행중인 스위치는 다른 MSTP의 메시지 구조를 식별하고 포함 된 MST영역의 식별자를 확인하고 MST 영역을 설정 할 수 있습니다. MST 호환모드 및 STP 호환모드는 MSTP 프로토콜 변환 메커니즘을 기반으로 합니다. 스위치의 한 포트가 호환모드에서 BPDU를 수신하면 포트는 자동으로 모드를 변경하고 BPDU를 호환 모드로 보냅니다. 표준 MST 모드로 포트를 다시 시작하려면 'spanning-tree mstp migration-check' 명령어를 실행하면 됩니다.
글로벌 모드에서 다음 명령을 실행하여 MST 호환모드를 활성화 하거나 비활성화 합니다.

명령어	설명
[no] spanning-tree mstp mst-compatible	스위치에 대해 MST 호환모드를 활성화합니다. No 명령어로 MST 호환모드를 비활성화합니다.

Note: 호환모드의 주요기능은 스위치 및 기타 MSTP 실행스위치 MST영역을 만드는 것입니다. 실제 네트워킹에서 스위치의 구성이름과 편집번호가 동일한지 확인하십시오. 다른 MSTP 프로토콜을 실행하는 스위치를 CIST루트에 구성하여 스위치가 메시지를 수신하여 호환모드가 되도록 하는 것이 좋습니다. MST 호환모드가 활성화되어 있지 않으면 스위치가 전체 BPDU 호환 내용을 확인하지 않고 그 내용을 일반 RSTP BUDU로 가져옵니다. 이렇게 하면 스위치가 연결된 MST 호환 스위치가 같은 영역에 스위치를 배치할 수 없습니다. 호환모드의 포트는 글로벌 모드 구성에서 호환모드가 종료 된 경우에도 표준 MST BPDU를 보내도록 자동으로 재개 할 수 없습니다. 이 경우 'migration-check'를 하십시오.

- 프로토콜 변환 확인을 다시 하십시오
- MSTP 메시지를 확인하십시오.

8.2.3 MSTP 설정 작업

8.2.3.1 기본 MSTP 설정

특성	기본 설정 (기본값 Setting)
STP mode	SSTP(PVST, RSTP, MSTP 사용 X)
Area name	MAC 주소의 문자열
Area edit level	0
MST configuration list	모든 VLAN은 CIST(MST00)에 맵핑됩니다.
Spanning-tree priority(CIST & all MSTI)	32768

Spanning-tree port priority(CIST & all MSTI)	128
Path cost of the spanning-tree port (CIST & all MSTI)	1000Mbps : 20000 100Mbps : 200000 10Mbps : 2000000
Hello Time	2초
Forward Delay	15초
Maximum-aging Time	20초
Maximum hop count	20

8.2.3.2 MSTP의 활성화 및 비활성화

STP프로토코로은 기본적으로 PVST 또는 SSTP 모드에서 시작합니다. Spanning-tree 가 필요하지 않을 때 실행을 중지 할 수 있습니다.
다음 명령을 실행하여 STP를 MSTP 모드로 설정 하십시오.

명령어	설명
spanning-tree	Spanning-tree를 기본 모드로 활성화 합니다.
spanning-tree mode mstp	모드를 MSTP로 설정 합니다.
no spanning-tree	모든 Spanning-tree 설정을 비활성화 합니다.

8.2.3.3 MSTP Area설정

스위치의 MST 영역은 구성 이름, 편집 번호, VLAN과 MSTI 간의 매핑 관계의 세가지 속성으로 결정 됩니다. 영역 구성 명령을 통해 구성 할 수 있습니다. 세 가지 속성 중 하나를 변경하면 스위치가 있는 영역이 변경 됩니다. 원래 상태에서 |MST 구성 이름은 스위치의 MAC주소의 문자열입니다. 편집 번호는 0이고 모든 VLAN은 CIST(MST00)에 매핑이 됩니다. 모든 스위치에는 고유의 MAC주소를 갖고 있으므로 MSTP를 실행하는 스위치는 원래 상태의 다른 영역에 있는 것입니다. Spanning-tree mstp instance <instance-id> vlan <vlan-list> 를 실행하여 새 MSTI를 만들고 지정된 VLAN을 여기에 매핑할 수 있습니다. MSTI가 삭제되면 이러한 모든 VLAN이 CIST에서 다시 매핑됩니다. 다음 명령을 실행하여 MST 영역 정보를 설정하십시오.

명령어	설명
[no] spanning-tree mstp name <string>	MSTP 이름을 설정 합니다. <string>은 문자열을 의미 합니다. 최대 32자의 문자를 사용할 수 있으며 기본값은 MAC 주소 입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.
[no] spanning-tree mstp revision <value>	MSTP 번호를 설정 합니다. <value>는 0~65535 이며 기본 값은 0 입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.
[no] spanning-tree mstp instance <instance-id> vlan <vlan-list>	VLAN을 MSTI에 매핑합니다. <instance-id>는 MSIT를 의미하는 spanning-tree의 독립적인 인스턴스 번호 입니다. 범위는 1~15입니다. <vlan-list>는 spanning-tree에 매핑되는 VLAN 목록을 의미합니다. 범위는 1~409 입니다. “1,2,3”, “1-5”, 1,2,5-10”과 같은 Vlan그룹을 나타냅니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

다음 명령을 실행하여 MSTP영역의 설정을 확인하십시오.

명령어	설명
show spanning-tree mstp region	MSTP 영역의 설정을 보여줍니다.

8.2.3.4 네트워크 Root 설정

MSTP에서 각 spanning-tree instance에는 우선순위 값과 스위치의 MAC 주소가 포함된 브리지 ID가 있습니다. spanning-tree 토폴로지를 설정하는 동안 상대적으로

적은 브릿지ID를 가진 스위치가 네트워크 Root로 선택 됩니다. MSTP는 설정을 통해 스위치를 네트워크 Root 스위치로 설정 할 수 있습니다.

spanning-tree mstp <instance-id> root primary 명령어를 이용하여 spanning-tree instance의 스위치 우선순위 값에서 가장 작은 값으로 수정하여 스위치가 Root스위치가 되도록 할 수 있습니다. 일반적으로 이전 명령이 실행 된 후 프로토콜은 현재 네트워크 Root 브리지ID를 자동으로 확인한 다음 값 24576인 현재 스위치가 Spanning-tree의 Root가 되도록 할 때 브리지ID의 우선수위 필드를 24576으로 설정 합니다. 네트워크 Root은 우선순위 값이 24576값보다 작은 경우 MSTP는 현재 브리지의 spanning-tree 우선순위를 Root의 우선순위 값인 4096으로 자동 설정 합니다. 4096이라는 숫자는 네트워크 우선 순위 값의 단계 길이입니다. Root를 설정할 때 직경 하위 명령을 Spanning-tree네트워크의 네트워크 지름으로 실행할 수 있습니다. 이 키워드는 스패닝 트리 인스턴스 ID가 0 일 때만 유효합니다. 네트워크 지름이 설정되면 MSTP는 적절한 STP 시간 매개 변수를 자동으로 계산하여 네트워크 수렴의 안정성을 보장합니다. 시간 매개 변수에는 Hello 시간, 전달 지연 및 최대 수명이 포함됩니다. Hello-time 부속 명령을 사용하여 기본 설정을 대체 할 새로운 hello 시간을 설정할 수 있습니다.

스위치를 네트워크 루트로 설정하려면 다음 명령을 실행하십시오.

명령어	설명
[no] spanning-tree mstp <instance-id> root primary <diameter <net-diameter> hello-time <seconds>>	지정된 Spanning-tree instance에서 스위치를 Root로 설정 합니다. <instance-id>는 0~15 범위의 Spanning-tree instance 번호를 나타냅니다. <net-diameter>는 선택적 매개변수인 네트워크의 크기를 나타냅니다. <instance-id>가 0일 때 효과적입니다 범위는 2-7입니다. <hello-time>은 1~10초 사이의 시간단위를 나타냅니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

다음 명령을 실행하여 MSTP 메시지를 확인 하십시오.

명령어	설명
show spanning-tree mstp [instance <instance-id>]	MSTP Instance 메시지를 확인 합니다.

8.2.3.5 Secondary Root 설정

네트워크 Root가 구성된 후에는 spanning-tree mstp instance-id root secondary를 실행하여 하나 이상의 스위치를 Secondary Root 또는 Backup Root 로 설정할 수 있습니다. 특정 이유로 Root가 작동하지 않는다면 Secondary Root가 네트워크의 Root가 됩니다. 기본 Root 구성과 달리 기본 Root 구성 명령이 실행 된 후 MSTP는 스위치의 spanning-tree Priority를 28672로 설정 합니다. 다른 스위치의 Priority

기본 값이 32768인 경우, 현재 스위치는 Secondary Root가 될 수 있습니다. Secondary Root를 구성할 때 보조명령인 diameter 및 hello-time을 실행하여 STP 시간 매개변수를 업데이트 할 수 있습니다. Secondary Root가 Primary Root가 되어 작업을 시작하면 모든 매개변수가 작동하기 시작합니다.

스위치를 네트워크의 Secondary Root로 설정하려면 다음 명령을 실행하십시오.

명령어	설명
[no] spanning-tree mstp <instance-id> root secondary <diameter <net-diameter> hello-time <seconds>>	지정된 Spanning-tree instance에서 스위치를 secondary Root로 설정 합니다. <instance-id>는 0~15 범위의 Spanning-tree instance 번호를 나타냅니다. <net-diameter>는 선택적 매개변수인 네트워크의 크기를 나타냅니다. <instance-id>가 0일 때 효과적입니다 범위는 2-7입니다. <hello-time>은 1~10초 사이의 시간단위를 나타냅니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

다음 명령을 실행하여 MSTP 메시지를 확인 하십시오.

명령어	설명
show spanning-tree mstp [instance <instance-id>]	MSTP Instance 메시지를 확인 합니다.

8.2.3.6 Bridge Priority 설정

경우에 따라 브리지 우선순위를 구성하여 스위치를 네트워크 Root에 직접 설정할 수 있습니다. 하위 명령 루트를 실행하지 않고 스위치를 네트워크 루트로 설정할 수 있음을 의미 합니다. 스위치의 우선순위 값은 각 spanning-tree instance에서 독립적으로 운영됩니다. 따라서 스위치의 우선순위를 독립적으로 설정할 수 있습니다.

다음 명령을 실행하여 Spanning-tree의 Priority를 설정 하십시오.

명령어	설명
[no] spanning-tree mstp <instance-id> priority <value>	스위치의 우선순위를 설정합니다. <instance-id>는 0 - 15 범위의 스패닝 트

	리 인스턴스의 번호를 나타냅니다. <value>는 브리지의 우선 순위를 나타냅니다. 다음 값 중 하나 일 수 있습니다. 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 no 명령어를 이용하여 설정을 제거 할 수 있습니다.

8.2.3.7 STP 시간 매개변수 설정

STP의 시간 매개변수는 다음과 같습니다.

- Hello Time
  스위치가 네트워크 Root로 작동 할 때 Designated port로 설정 메시지를 보내는 간격 입니다.

- Forward Delay
  STP mode - Block 에서 Learning으로 Forwarding 상태로 변경 될 때 Port가 필요로 하는 시간

- Max Age
  Spanning-tree에 대한 구성 정보의 최대 활성화 시간입니다. 네트워크 토폴로지의 부화를 줄이려면 시간 매개변수에 대한 다음 요구사항을 충족해야 합니다.
  2 x (fwd_delay-1.0) ≥ Max_age
  Max_age ≥ (hello_time +1) x 2

명령어	설명
[no] spanning-tree mstp hello-time seconds	Hello time 매개 변수를 설정합니다. 매개 변수 초는 Hello time 단위이며 1 - 10 초 사이입니다. 기본값은 2 초입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.
[no] spanning-tree mstp forward-time seconds	Forward Delay 매개 변수를 설정합니다. 매개 변수의 범위는 4 ~ 30 초입니다. 기본값은 15 초입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.
[no] spanning-tree mstp max-age seconds	Max Age 매개 변수를 설정합니다.

	매개 변수는 6 ~ 40 초입니다. 기본값은 20 초입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

Root 또는 Network Diameter를 설정하여 STP 시간 매개변수를 수정하는 것이 좋습니다. 새로 설정된 시간 매개 변수는 이전 수식의 요구사항을 준수하지 않더라도 유효합니다. 구성을 수행 할 때 Console의 알람에 주의 하십시오.

8.2.3.8 Network Diameter 설정

Network Diameter는 네트워크 규모를 나타내는 네트워크의 두 호스트 사이의 최대 스위치 수를 나타냅니다. Spanning-tree mstp diameter net-diameter 명령을 실행하여 MSTP Network Diameter을 설정 할 수 있습니다.
매개변수 <net-diameter>는 CIST에만 유효합니다. 구성 후 3개의 STP 시간 매개변수를 자동으로 비교하여 상위 값으로 업데이트 합니다.
다음 명령을 실행하여 net-diameter를 구성하십시오.

명령어	설명
[no] spanning-tree mstp diameter <net-diameter>	net-diameter를 설정하십시오. 매개 변수 net-diameter 범위는 기본값에서 7입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

매개변수 net-diameter는 스위치의 독립 설정으로 저장되지 않습니다. Network Diameter을 수정하여 수정할 때만 시간 매개변수를 저장할 수 있습니다.

8.2.3.9 Maximum Hop Count 설정

최대 Hop Count를 구성하려면 다음 명령을 실행합니다.

명령어	설명
[no] spanning-tree mstp max-hops <hop-count>	최대 홉을 설정하십시오. hop-count의 범위는 1 - 40입니다. 기본값은 20입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

8.2.3.10 Port Priority 설정

스위치 두 포트 사이에 루프가 발생하면 우선순위가 높은 포트가 Forwarding 상태

가 되고 낮은 포트는 Block 상태가 됩니다. 모든 포트의 우선순위가 같으면 더 작은 포트 번호를 가진 포트가 먼저 Forwarding 상태가 됩니다.
포트 설정모드에서 다음 명령어를 실행하여 STP 포트의 우선순위를 설정합니다.

명령어	설명
[no] spanning-tree mstp <instance-id> port-priority <priority>	STP Port의 Priority를 설정합니다. <instance-id>는 0 - 15 범위의 Spanning-tree instance Num을 나타냅니다. <priority>는 포트 우선 순위를 나타냅니다. 다음 값 중 하나입니다. 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 no 명령어를 이용하여 설정을 제거 할 수 있습니다.
[no] spanning-tree port-priority <value>	모든 Spanning-tree의 instance에서 포트 우선순위를 설정합니다. <value>는 포트 우선순위를 나타냅니다. 다음 값중에 하나 입니다. 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 no 명령어를 이용하여 설정을 제거 할 수 있습니다.

다음 명령을 실행하여 MSTP 포트에 대한 정보를 확인하십시오.

명령어	설명
show spanning-tree mstp interface <interface-id>	MSTP 포트 정보를 확인하십시오. interface-id는 포트 이름을 나타냅니다. (예 : "F0/1"및 "FastEtnernet0/3").

8.2.3.11 포트의 Path Cost 설정

MSTP에서 포트의 Path Cost의 기본값은 연결 속도를 기반으로 합니다. 두 스위치 간에 루프가 발생하면 Path Cost이 적은 포트가 Forwarding 상태가 됩니다. Path Cost이 적을수록 포트의 비율이 높아집니다. 모든 포트의 경로 비용이 같으면 더 작은 포트 번호를 가진 포트가 먼저 Forwarding 상태가 됩니다.
포트 설정 모드에서 다음 명령을 실행하여 포트의 Path Cost을 설정 합니다.

명령어	설명
[no] spanning-tree mstp <instance-id> cost <cost>	Port의 path cost 값을 설정 합니다. <instance-id>는 0에서 15사이의 Spanning-tree instance번호를 나타냅니다.

	<cost>는 port의 Path cost를 나타내며 1에서 200000000 입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.
[no] spanning-tree cost <value>	모든 Spanning-tree instance에서 포트의 Path cost을 설정합니다. 값은 포트의 경로 비용을 나타내며, 범위는 1에서 200000000입니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

8.2.3.12 Port Connection Type 설정

MSTP지원 스위치 사이에 연결이 직접 연결인 경우 스위치는 Handshake 메커니즘을 통해 신속하게 연결을 설정할 수 있습니다. Port Connection Type을 구성 할 때 포트 연결을 각각의 유형으로 설정 하십시오. 프로토콜은 양방향 속성에 따라 각각의 연결을 사용할지 여부를 결정합니다. 포트가 전 이중 모드에서 작동하는 경우 프로토콜은 연결이 지점간 프로토콜이라고 간주 합니다. 포트가 반 이중 모드에서 작동하면 프로토콜은 연결이 공유 된 것으로 간주합니다. 포트가 연결하는 스위치가 RSTP 프로토콜 또는 MSTP 프로토콜을 실행하는 경우 Port Connection Type을 각각(Point-to-point)로 설정하여 handshake가 빠르게 설정 되도록 할 수 있습니다. 포트 설정모드에서 다음 명령어를 이용하여 Port Connection Type을 설정 하십시오.

명령어	설명
spanning-tree mstp point-to-point force-true	포트 연결 유형을 지점 간 (point-to-point)으로 설정합니다.
spanning-tree mstp point-to-point force-false	포트 연결 유형을 공유로 설정합니다.
spanning-tree mstp point-to-point auto	자동으로 포트 연결 유형을 확인합니다.
no spanning-tree mstp point-to-point	No 명령어로 기본 설정으로 돌아갑니다.

8.2.3.13 MSTP 호환모드 활성화

스위치가 지원하는 MSTP 프로토콜은 IEEE802.1s를 기반으로 합니다. 다른 MSTP, 특히 Cisco사에서 지원하는 MSTP와 호환되도록 MSTP프로토콜은 MST 호환모드에서 작동할 수 있습니다. MST 호환모드 에서 실행중인 스위치는 다른 MSTP의 메시지 구조를 식별하고, 포함된 MST 지역 식별자를 확인하고 MST 영역을 설정할 수 있습니다. MST 호환모드 및 STP 호환모드는 MSTP 프로토콜 변환 메커니즘을 기반으로 합니다. 스위치의 한 포트가 MST 호환모드 에서 BPDU를 수신하면 포트는 자동으로 Mode를 변경하고 BPDU를 MST 호환모드로 보냅니다. 표준 MST Mode로 포트를 다시 시작하려면 spanning-tree mstp migration-check를 실행하면 됩니다.

글로벌 모드에서 다음 명령어를 이용하여 MST 호환모드를 설정 합니다.

명령어	설명
[no] spanning-tree mstp mst-compatible	MST 호환모드를 활성화 합니다. no 명령어를 이용하여 설정을 제거 할 수 있습니다.

Note. 호환모드의 주요기능은 스위치 및 기타 MSTP 실행 스위치의 MST영역을 만드는 것입니다. 실제 네트워킹에서는 스위치의 구성, 이름과 편집번호가 동일한 지 확인하십시오. 다른 MSTP 프로토콜을 실행하는 스위치를 CIST Root에 구성하여 메시지를 수신하여 스위치가 호환모드로 들어가도록 하는 것이 좋습니다. MST 호환모드 가 활성화 되어있지 않으면 스위치가 전체 BPDU 호환 컨텐츠를 해결하지 않고 컨텐츠를 일반 RSTP BPDU로 가져옵니다. 이렇게 하면 스위치가 연결된 MST 호환스위치와 같은 영역에 스위치를 배치할 수 없습니다. MST 호환모드의 포트는 글로벌모드에서 호환모드가 종료된 경우 표준 MST BPDU를 내보내도록 자동으로 재개할 수 없습니다. 이 경우 Migration-Check를 실행 하십시오.

8.2.3.14 Protocol Conversion 확인 및 Restarting

MSTP를 사용하면 스위치가 프로토콜 변환 메커니즘을 통해 기존의 STP스위치와 함께 작동 할 수 있습니다. 스위치의 한 포트가 STP 구성 메시지를 수신하면 포트는 STP메시지만 전송합니다. STP 정보를 수신하는 포트는 경계 포트로 간주 됩니다. Note. 포트가 STP호환 상태에 있으면 포트가 STP 메시지를 더이상 수신하지 않더라도 포트는 자동으로 MSTP 상태로 재개되지 않습니다. 이 경우 'spanning-tree mstp migration-check'를 실행하여 포트가 STP 메시지를 지우고 포트를 MSTP 상태로 복구 합니다. RSTP 프로토콜을 실행하는 스위치는 MSTP 메시지를 식별하고 처리 합니다. MSTP 스위치는 RSTP 스위치와 함께 작동할 때 프로토콜 변환이 불필요합니다.

글로벌 모드에서 다음 명령을 실행하여 스위치의 모든 포트에서 감지되는 모든 STP 정보를 지웁니다. (포트가 감지한 STP정보를 지울 경우 포트 설정모드에서 실행)

명령어	설명
spanning-tree mstp migration-check	스위치의 모든 포트에서 감지되는 모든 STP정보를 삭제 합니다. (포트가 감지한 STP정보도 삭제)

8.2.3.15 MSTP 정보 확인

모니터링과 구성 명령 또는 포트 구성명령에서 다음 명령을 실행하여 MSTP에 대한 정보를 확인합니다.

명령어	설명
show spanning-tree	MSTP 정보를 확인합니다. (SSTP, PVST, RSTP 및 MSTP에 대한 정보를 확인할 수 있음)
show spanning-tree detail	MSTP 정보의 세부 사항을 확인합니다. (SSTP, PVST, RSTP 및 MSTP에 대한 정보를 확인할 수 있음)
show spanning-tree interface <interface-id>	STP 인터페이스 정보를 확인합니다. (SSTP, PVST, RSTP 및 MSTP에 대한 정보를 확인할 수 있음)
show spanning-tree mstp	모든 MST 인스턴스를 검사합니다.
show spanning-tree mstp region	MST 영역 구성을 확인합니다.
show spanning-tree mstp interface <interface-id>	MST 인스턴스에 대한 정보를 확인합니다.
show spanning-tree mstp detail	MST 정보를 확인합니다.

9장. Port Mirroring 설정

9-1장 Port Mirroring 설정

9.1.1 Port Mirroring 설정 작업 목록

- Port Mirroring 설정
- Port Mirroring 정보 표시

9.1.2 Port Mirroring 설정 작업

9.1.2.1 Port Mirroring 설정

명령어	설 명
[no] mirror session <session_number> destination interface <interface-id> | source interface <interface-id [, | -] [both | rx | tx] >	Port Mirroring을 설정 합니다. Session-Number는 Port Mirroring 번호입니다. Destination은 출력 interface Port 입니다. Source는 Mirroring 대상 Interface Port 입니다. Both | tx | rx 로 Data의 흐름을 설정 가능하며, tx는 입력, rx는 출력 데이터를 의미 합니다. no명령어로 설정을 삭제 할 수 있습니다.

Port Mirroring을 구성하면 스위치의 한 포트를 사용하여 포트 그룹의 트래픽을 확인 할 수 있습니다.

Port Mirroring을 구성하려면 Config 모드에서 다음 단계를 수행하십시오.

9.1.2.2 Port Mirroring 정보 표시

Show 명령어를 사용하여 Port Mirroring의 설정 정보를 표시합니다.

명령어	설 명
show mirroring [session session_num]	Port mirroring에 대한 구성 정보를 표시합니다. Session_num은 Mirroring 번호 입니다.

10 장 MAC 주소 테이블 배열 설정

10-1장 Mac address 속성 설정

10.1.1 MAC address 설정 작업 목록

- Static MAC Address 설정
- MAC Address Aging Time 설정
- VLAN 공유 MAC Address 설정
- MAC Address 보여주기
- Dynamic MAC Address 지우기

10.1.2 MAC Address 설정 작업

10.1.2.1 Static MAC address 설정

Static MAC Address 항목은 스위치가 경과하지 않고 수동으로 만 삭제할 수 있는 MAC Address 항목입니다. 작업 프로세스 중 실제 요구 사항에 따라 Static MAC Address를 추가 및 삭제할 수 있습니다.
Config 모드에서 다음 명령을 사용하여 Static MAC Address를 추가하고 삭제 하십시오.

명령어	설 명
[no] mac address-table static <mac-addr> vlan <vlan-id> interface <interface-id>	정적 MAC Address를 추가/삭제 합니다. mac-addr은 MAC Address를 나타내며, vlan-id는 Vlan 번호(1~4094), interface-id는 Interface의 이름을 의미 합니다. No 명령어로 삭제 할 수 있습니다.

10.1.2.2 MAC Address Aging Time 설정

지정된 Aging Time 동안 동적 MAC Address가 사용되지 않으며 스위치는 이 MAC Address를 MAC Address Table에서 삭제를 합니다. 스위치 MAC Address의 Aging Time은 필요에 따라 구성 할 수 있습니다(기본값: 300sec). Config 모드에서 다음 명령어를 사용하여 MAC Address의 Aging Time을 설정 하십시오.

명령어	설 명
[no] mac address-table aging-time [0 | 10-1000000]	MAC Address의 Aging Time을 설정합니다. 0은 MAC이 없음을 나타냅니다. 유효한 값은 초단위로 10~100000까지 입니다. No 명령어로 삭제 할 수 있습니다.

10.1.2.3 VLAN 공유 MAC Address 설정

Port가 VLAN 공유 MAC Address로 구성되면 Port에서 학습한 MAC Address는 모든 VLAN에 공유가 됩니다. 즉, 다른 VLAN에서도 MAC Address를 인식 합니다. VLAN에 의해 공유되는 MAC Address를 구성하려면 Config 모드에서 다음 명령어를 수행 하십시오

명령어	설 명
interface Gi 0/1 switchport shared-learning [no] switchport shared-learning	설정할 interface를 입력 합니다. Port의 MAC을 공유하는 설정을 합니다. No 명령어로 삭제 할 수 있습니다.

10.1.2.4 MAC Address 보여주기

운영 프로세스에서 디버깅 및 관리가 필요하기 때문에 스위치 MAC Address Table의 내용이 필요 합니다. 스위치의 MAC Address Table의 내용을 표시하려면 Show를 이용하여 다음 명령어를 실행 하십시오.

명령어	설 명
show mac address-table {dynamic [interface <interface-id> | vlan <vlan-id>] | static}	설정할 interface를 입력 합니다. Port의 MAC을 공유하는 설정을 합니다. No 명령어로 삭제 할 수 있습니다.

10.1.2.5 Dynamic Mac Address 지우기

저장되어 있는 MAC Address는 경우에 따라 삭제가 가능해야 합니다.
다음 명령을 사용하여 Enable 모드에서 Dynamic MAC Address를 삭제 하십시오.

명령어	설 명
clear mac address-table dynamic [address mac-addr | interface interface-id | vlan vlan-id]	Dynamic MAC Address 항목을 삭제합니다. Dynamic은 동적으로 획득하는 MAC Address를 나타냅니다. Interface/VLAN에 공유된 MAC Address 를 삭제 합니다. Interface-id는 interface 번호입니다. Vlan-id는 1~4094 입니다.

11 장 Link Aggregating 설정

11-1장 Port Aggregation 설정

11.1.1 개요

Trunking이라고도 하는 Link Aggregation은 이더넷 스위치에서 사용할 수 있는 옵션 기능이며 Layer 2 Bridging 과 함께 사용 됩니다. Link Aggregation은 단일 Link에서 여러 포트의 논리적 병합을 허용합니다. 각 물리적 링크의 전체 대역폭을 사용할 수 있으므로 비효율적인 트래픽 라우팅으로 대역폭이 낭비되지 않습니다. 결과적으로 전체 클러스터보다 효율적으로

활용됩니다. Link Aggregation은 트래픽이 많은 서버에 높은 대역폭을 제공하고 단일 포트 또는 케이블 장애가 발생할 경우 라우팅 기능을 제공 합니다.

지원되는 기능

- Static Aggregation Control를 지원합니다.
  논리적포트에 실제로 바인딩 할 수 있는지 여부에 관계없이 물리적 포트를 논리적 포트에 바인딩 합니다. LACP Dynamic Aggregation의 Aggregation Control이 지원 됩니다. LACP 프로토콜 협상을 통화하는 물리적 포트 만 논리 포트에 바인딩 할 수 있습니다. 다른 포트는 논리적포트에 바인딩 되지 않습니다.
- LACP의 Aggregation Control은 Dynamic 연동을 지원합니다.
  물리적 포트가 논리적 포트에 바인딩 되도록 구성되면 LACP 협상을 사용하는 물리적 포트를 논리적 포트에 바인딩 합니다. 다른 포트는 논리 포트에 바인딩 될 수 없습니다.
- Port Aggregation의 Traffic 흐름의 load balance가 지원됩니다.
  Port Aggregation 연결 후에는 Aggregation Port의 데이터 흐름이 물리적 포트에 분산 됩니다.

11.1.2 Port Aggregation 설정 작업

- Aggregation에 사용되는 논리 Channel 설정
- 물리적 포트의 Aggregation
- Port Aggregation 후 Load Balance 설정
- Port Aggregation 설정 후 상태 모니터링

11.1.3 Port Aggregation 설정 방법

11.1.3.1 Aggregation의 논리적인 Channel 설정

물리적 포트를 바인딩 하기 전에 논리 포트를 설정 해야 합니다. 논리적 포트는 이러한 물리적 포트를 바인딩에 의해 형성된 Channel을 제어하는 데 사용 됩니다. 논리적인 Channel을 구성 하려면 다음 명령어를 사용하십시오.

명령어	설명

Interface port-aggreagator <id>	논리적인 체널 그룹을 생성합니다.

11.1.3.2 물리적인 포트에 Aggregation 설정

여러 물리적 Port를 논리적 채널로 Aggregation하려면 Static 혹은 LACP Protocol을 사용할 수 있습니다. Static Aggregation을 사용되는 경우 물리적 포트의 링크가 동작을 해야 하며 Aggregation Port와 물리적 Port의 VLAN 설정이 동일해야 하며, 현재 Port가 Aggregation Port의 조건과 일치하는지 여부 및 물리적 포트와 연결된 포트가 Aggregation 조건과 일치하는지 여부와 관계 없이 포트는 논리적 채널에 Aggregation 되어야 합니다

Aggregation 설정의 선행 조건:

- 포트의 링크가 작동해야 하며 포트는 Full-Duplex Mode로 협상이 되어있어야 합니다.
- 모든 물리적 Port의 속도는 Aggregation Process 동안 동일해야 합니다. 즉, 성공적으로 집계된 물리적 포트 하나 있는 경우 두번째 물리적 포트의 속도는 처음 구성된 포트와 동일해야 합니다. 또한 모든 물리적 포트의 VLAN속성은 집계된 포트와 동일해야 합니다.

LACP 패킷을 다음 모드에서 연결된 포트간 교환 됩니다:

- Active – 포트를 Active negotiating status로 만듭니다. 이 상태에서는 포트를 LACP 패킷을 보내 원격 포트와 협상을 시작합니다.
- Passive – 포트를 수동 협상 상태로 지정 합니다. 이 상태 에서 포트가 수신하는 LACP 패킷에 응답하지만 LACP 협상을 시작하지 않습니다. 이 모드에서 포트채널 그룹은 인터페이스를 연결 합니다.

  두 포트가 패시브 방식을 사용하면 Aggregation이 연결되지 않습니다. 이는 양쪽 포트가 Aggregation 프로세스를 시작하기를 기다릴 것이기 때문입니다.
  VLAN 속성: PVID, Trunk 속성, VLAN 허용범위 및 VLAN 비 허용범위
  다음 명령을 사용하여 물리적 Port에서 Aggregation을 설정 하십시오.

명령어	설명
Aggregator-Group <ID> mode (lacp / static)	물리적 포트의 Aggregation옵션을 구성합니다.

11.1.3.3 Port Aggregation 설정 후 Load Balance 설정

Load의 분배 방법을 선택하여 모든 포트가 모든 물리적 포트를 선택하여 데이터 트래픽을 공유 할 수 있도록 합니다. 스위치는 최대 6가지의 Load Balance 방식을 제공 합니다.

- src-mac
  Source-MAC 주소에 따라 Data Traffic을 공유 합니다. 즉, 동일한 MAC주소를 갖고있는 메시지는 물리적 포트를 통과 합니다.

- dst-mac
  Destination-MAC주소에 따라 데이터 트래픽을 공유 하는 것입니다. 즉, 동일한 MAC 주소 속성을 갖고있는 메시지는 물리적 포트를 통과 합니다.

- both-mac
  원본 및 대상 MAC주소에 따라 데이터 트래픽을 공유 합니다. 즉, 동일한 MAC 주소 특성을 갖고있는 메시지를 물리적 포트를 통과 합니다.

- src-ip
  Source IP주소에 따라 데이터 트래픽을 공유 합니다. 즉, 동일한 IP주소를 갖고 있는 메시지는 물리적 포트를 통과 합니다.

- des-ip
  Destination IP주소에 따라 데이터 트래픽을 공유 합니다. 즉, 동일한 IP주소를 갖고있는 메시지는 물리적 포트를 통과합니다.

- both-ip
  대상의 Source IP, Destination IP에 따라 데이터 트래픽을 공유 하는 것입니다. 즉, IP 주소 속성을 갖고있는 메시지는 물리적 포트를 통과 합니다.

Load Balance 방식을 구성하려면 다음 명령을 사용하십시오.

명령어	설명
Aggregator-Group load-balance	Load balance의 방식을 설정 합니다.

Note :

이 명령은 Load-Balance 방법을 지원하지 않거나 하나의 방법만 지원하는 스위치에서는 사용할 수 없습니다. 이 명령을 사용하는 스위치는 자체적으로 지원되는 Load-Balance 만 선택 합니다.

11.1.3.4 Port aggregation의 모니터링

EXEC모드에서 Aggregation 상태를 모니터링 하려면 다음 명령을 사용하십시오.

명령어	설명
show aggregator-group	Port aggregation 상태를 보여줍니다.

12장. GVRP 설정

12-1장 GVRP 설정

12.1.1 소개

GVRP(GARP VLAN Registration Protocol GARP VLAN)는 802.1Q 트렁크 포트에서 IEEE 802.1Q 호환 VLAN running & dynamic VLAN생성을 제공하는 GARP(GARP VLAN Registration Protocol GARP VLAN) 응용프로그램 입니다.

GVRP를 사용하면 스위치가 VLAN 구성정보를 다른 GVRP스위치와 교환하고 불필요한 브로드캐스트 및 알수없는 유니캐스트 트래픽을 제거하고 802.1Q Trunk port를 통해 연결된 스위치에서 VLAN을 동적으로 생성 및 관리 할 수 있습니다.

12.1.2 설정 목록

12.1.2.1 GVRP 설정 목록

- GVRP 전역 활성화 / 비활성화
- 인터페이스에서 GVRP 활성화 / 비활성화
- GVRP의 모니터링 및 유지관리

12.1.3 GVRP 설정 목록

12.1.3.1 GVRP 전역 활성화 / 비활성화

글로벌 모드에서 다음 구성을 수행하십시오.

명령어	설명
[no] gvrp	GVRP를 활성화/비활성화 합니다.

기본 설정은 Disable 입니다.

12.1.3.2 인터페이스에서 GVRP 활성화 / 비활성화

인터페이스 구성 모드에서 다음 명령을 실행 하십시오.

명령어	설명
[no] gvrp	Interface의 GVRP를 활성화/비활성화 합니다.

포트의 GVRP를 활성화 하려면 전역모드의 GVRP가 활성화 되어있어야 하며 포트는 802.1Q Trunk port여야 합니다. 이 포트는 기본적으로 활성화 되어있습니다.

12.1.3.3 GVRP의 모니터링 및 점검

Exec 모드에서 다음 작업을 수행 하십시오.

명령어	설명
show gvrp statistics [interface port_list]	GVRP Statistics를 표시 합니다.
show gvrp status	GVRP 전체 상태정보를 표시합니다.
[no] debug gvrp [packet | event]	GVRP 데이터 패킷 및 이벤트 Debug를 활성화/비활성화 합니다.

GVRP 정보 표시 :

switch#show gvrp statistics interface Tthernet0/1

GVRP statistics on port Ethernet0/1

GVRP Status: Enabled

GVRP Failed Registrations: 0

GVRP Last Pdu Origin: 0000.0000.0000

GVRP Registration Type: Normal

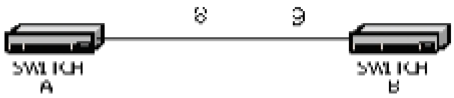
GVRP 전역 상태 정보 표시 :

switch#show gvrp statu

gvrp is enabled!

12.1.4 설정 예제

Switch A와 Switch B의 VLAN 구성 정보를 동일하게 만들려면 Switch A와 Switch B에서 GVRP를 활성화 할 수 있습니다. 네트워크 구성은 다음과 같습니다.



1) Switch A가 Switch B와 연결하는 interface 8로 Trunk 구성 합니다.

   SwitchA_config_g0/8# switch mode trunk

2) Switch A의 전역 GVRP를 활성화 합니다.

   SwitchA_config# gvrp

3) Switch A의 interface 8에 GVRP를 활성화 합니다.

   Switch_config_g0/8# gvrp

4) Switch A에 VLAN 10, 20, 30을 구성 합니다.

   SwitchA_config# vlan 10
   SwitchA_config# vlan 20
   SwitchA_config# vlan 30

5) Switch B가 Switch A와 연결되는 interface 9로 Trunk 구성 합니다.

   SwitchB_config_g0/9# switch mode trunk

6) Switch B의 전역 GVRP를 활성화 합니다.

   SwitchB_config# gvrp

7) Switch B의 interface 9에 GVRP를 활성화 합니다.

   SwitchB_config_g0/9# gvrp

8) Switch B에 VLAN 40, 50, 60을 구성합니다.

   SwitchB_config# vlan 40
   SwitchB_config# vlan 50
   SwitchB_config# vlan 60

   구성이 완료되면 Switch A와 Switch B에 VLAN 구성 정보가 각각 표시 됩니다.
   (즉, 두 스위치의 VLAN10, 20, 30, 40, 50, 60을 확인 할 수 있습니다)

13장 GMRP 설정

13-1장 GMRP 설정

13.1.1 개요

GARP 멀티케스트 등록 프로토콜(GMRP)는 GARP(Generic Attribute Registration Protocol)을 기반으로 합니다. 스위치의 멀티캐스트 MAC Table을 유지 관리 하는 GARP 메커니즘을 채택하여 멀티캐스트 메시지가 브로드캐스트 되지 못하도록 하기 때문에 네트워크 자원을 절약합니다. 모든 GMRP지원 스위치는 다른 스위치로부터 멀티캐스트 MAC 주소 등록 정보를 수신 할 수 있으며 포트에 현재 저장된 멀티캐스트 MAC 주소 등록정보를 포함하여 로컬 멀티 캐스트 MAC 주소 등록 정보를 동적으로 업데이트 할 수 있습니다. 동시에 GMRP 지원 스위치는 로컬 멀티 캐스트 MAC 주소 등록 정보를 다른 스위치로 보낼 수 있습니다.

13.1.2 설정 작업 목록

GMRP 설정 작업 목록은 다음 작업이 포함 됩니다.

- 글로벌 설정 모드에서 GMRP 활성화 / 비활성화
- 포트에서 GMRP 활성화 / 비활성화
- GMRP 모니터링 및 관리

13.1.2 GMRP 설정 목록

13.1.2.1 글로벌 설정 모드에서 GMRP 활성화 / 비활성화

글로벌 설정 모드에서 다음 설정을 수행 하십시오.

명령어	설명
[no] gmrp	GMRP를 활성화/비활성화 합니다. No 명령어를 이용하여 기본상태로 되돌립니다.

GMRP는 기본적으로 비활성화 입니다.

13.1.2.2 Port에서 GMRP 활성화 / 비활성화

포트설정모드에서 다음 설정을 수행하십시오.

명령어	설명
[no] gmrp	GMRP를 활성화/비활성화 합니다. No 명령어를 이용하여 기본상태로 되돌립니다.

port에서 GMRP를 활성화 하기 전에 글로벌 설정모드에서 GMRP를 활성화하십시오. 그렇지 않으면 포트의 GMRP가 작동하지 않습니다. GMRP는 Trunk Port에서 설정 되어야 합니다.
Port의 GMRP는 기본적으로 사용하도록 설정 되어 있습니다.

13.1.3.3 GMRP 모니터링 및 관리

관리모드에서 다음 명령어를 실행하십시오.

명령어	설명
show gmrp statistics [interface port_list]	GMRP 통계 정보를 표시 합니다.
show gmrp status	글로벌 모드에서 GMRP 정보를 표시합니다.
[no] debug gmrp [packet | event]	GMRP 패킷 및 이벤트의 Debug 확인 합니다.

- GMRP 통계 정보 표시 내용

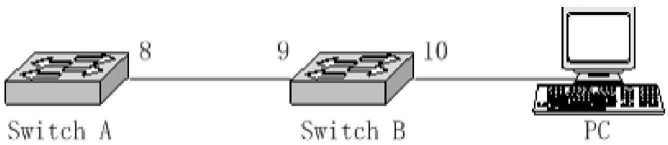
  switch# show gmrp statistics interface fastethernet0/6
  GMRP statistics on port FastEthernet0/6
  GMRP Status: Enabled
  GMRP Frames Received: 54
  GMRP Frames Transmitted: 27
  GMRP Frames Discarded: 0
  GMRP Last Pdu Origin: 1234.5678.9abc

- 글로벌 모드에서 GMRP 정보 표시 내용

  switch# show gmrp status
  GMRP is disable

13.1.4 설정 예제

다음 그림은 네트워크 연결을 보여줍니다.



스위치A의 VLAN 구성정보를 스위치B의 VLAN 구성정보와 동일하게 만들려면 스위치A 및 스위치B에서 GMRP를 활성화 하십시오. 구성은 다음과 같습니다.

1) 다음 명령어를 실행하여 글로벌모드에서 스위치A의 GMRP를 활성화 합니다.
   switch_config# gmrp
2) 다음 명령어를 실행하여 스위치A의 8번 포트에서 GMRP를 활성화 합니다.
   switch_config_f0/8# gmrp
3) 다음 명령어를 실행하여 글로벌모드에서 스위치B의 GMRP를 활성화 합니다.
   switch_config# gmrp
4) 다음 명령어를 실행하여 스위치B의 9번 포트에서 GMRP를 활성화 합니다.

switch_config_f0/9# gmrp

5) 다음 명령어를 실행하여 스위치B의 10번 포트에서 GMRP를 활성화 합니다.
   switch_config_f0/10# gmrp

6) 스위치 B의 컴퓨터 연결 포트 10에서 스위치 B로 gmrp join 메시지를 보냅니다. 메시지에 등록 된 멀티 캐스트 MAC 주소는 01.00.00.00.00.99입니다.

7) 스위치 A의 멀티 캐스트 MAC 주소 테이블을 확인하여 MAC 주소 01.00.00.00.00.99에 대한 레코드를 찾습니다.

Note:

1) 스위치A의 포트8이 속한 VLAN과 스위치B의 포트9의 VLAN은 모두 동일한 VLAN을 포함 합니다. 서로 다른 VLAN은 서로 직접 통신을 할 수 없습니다.

모든 타이머가 종료되기 전에 스위치A에서 멀티캐스트 MAC 주소테이블을 확인 하십시오. 쉽게 관찰 할 수 있도록 garp timer leaveall을 실행하여 두 스위치의 종료 타이머 시간 초과 값을 동시에 증가 시킵니다. (기본값: 10초)

14장 IGMP-Snooping 설정

14-1장 IGMP-snooping 설정

14.1.1 IGMP-snooping 설정 목록

IGMP-snooping의 임무는 VLAN과 그룹 주소 간의 관계를 유지하고 Multicast 변경과 동시에 업데이트하여 multi-Layer 그룹의 토폴로지 구조에 따라 Layer2 스위치가 데이터를 전달할 수 있게 하는 것입니다.
IGMP-snooping의 주요 기능은 다음과 같습니다.

- Listening IGMP message
- VLAN과 그룹주소 간의 연결 테이블을 유지 관리 합니다.
- Flooding이 발생하지 않도록 호스트의 IGMP entity와 Router의 IGMP entity를 동일한 상태로 유지 합니다.

Note.
IGMP-snooping은 query message를 듣고 IGMP의 메시지를 보고 위의 기능을 작동 하기 때문에 IGMP-snooping은 Multicast router에서 작동 할 때문 제대로 작동할 수 있습니다. 즉, 스위치는 주기적으로 라우터에서 IGMP query 정보를 수신해야 합니다. IGMP-snooping의 router-age timer는 IGMP-snooping을 연결하는 Multicast router의 query 시간 보다 큰 시간 값으로 설정 되어야 합니다. "show ip igmp-snooping"을 실행하여 각 VLAN의 Multicast router 정보를 확인 할 수 있습니다.

- VLAN에 IGMP-snooping 설정 활성화/비활성화
- VLAN에 Static Multicast 주소 추가 / 삭제
- VLAN의 제외 설정
- 등록된 대상 주소 없이 Multicast 메시지를 필터링 하는 기능 설정
- IGMP-snooping의 Router-age 설정
- IGMP-snooping의 응답시간 타이머 구성
- IGMP-snooping의 쿼리 작성 설정
- IGMP-snooping의 모니터링 및 관리
- IGMP-snooping 설정 예제

14.1.1.1 VLAN에 IGMP-snooping 설정 활성화/비활성화

글로벌 모드에서 다음 설정을 실행 하십시오.

명령어	설명
[no] ip igmp-snooping [vlan vlan-id]	VLAN에 igmp-snooping을 활성화 합니다. no 명령어로 기본설정으로 합니다.

VLAN을 지정하지 않으면 나중에 생성된 VLAN을 포함하여 시스템의 모든 VLAN을 활성화 하거나 비활성화 할 수 있습니다. 기본 설정에서 ip igmp-snooping 명령이 구성된 것처럼 VLAN의 IGMP-snooping이 활성화 됩니다.

Note: IGMP-snooping은 최대 16개의 VLAN에서 실행 될 수 있습니다.
VLAN3에서 IGMP-snooping을 활성화 하려면 먼저 no ip igmp-snooping을 실행하여 모든 VLAN의 IGMP-snooping을 비활성화 한 다음 ip igmp-snooping vlan3으로 설정 한 후 저장 해야 합니다.

14.1.1.2 VLAN에 Static Multicast 주소 추가 / 삭제

IGMP를 지원하지 않는 호스트는 static multicast 주소를 설정하여 해당 multicast 메시지를 수신 할 수 있습니다.
글로벌모드에서 다음 설정을 수행하십시오.

명령어	설명
[no] ip igmp-snooping vlan vlan_id static A.B.C.D interface intf	VLAN에 static multicast 주소를 설정 합니다. no 명령어로 설정을 삭제 합니다.

14.1.1.3 VLAN의 제외 설정

특성으로 제외가 필요한 VLAN이 구성된 경우 스위치는 제외 메시지를 받은 후 Multicast Group의 포트 목록에서 포트를 삭제 할 수 있습니다. 따라서 스위치는 타이머가 다른 호스트가 Multicast에 포함 되기를 기다릴 필요가 없습니다.
같은 포트에 있는 다른 호스트가 같은 그룹에 속해 있고 사용자가 그룹을 떠나고 싶지 않은 경우 이 사용자의 Multicast 통신에 영향을 줄 수 있습니다. 이 경우 제외 설정 기능을 사용 할 수 없습니다.

명령어	설명
[no] ip igmp-snooping vlan vlan_id immediate-leave	VLAN의 제외 설정을 구성 합니다. no 명령어로 설정을 삭제 합니다.

VLAN의 제외 설정은 기본적으로 비활성화 되어 있습니다.

14.1.1.4 등록된 대상 주소 없이 Multicast 메시지를 필터링 하는 기능 설정

Multicast 메시지 대상을 찾을 수 없으면 (DHL, 대상주소가 igmp-snooping을 통해 스위치 칩셋에 등록되지 않음) 기본 처리 방법은 VLAN의 모든 포트에서 메시지를 보내는 것입니다. 설정을 통해 프로세스 방법을 변경 할 수 있습니다. 목적지 주소가 어떤 포트에도 등록되지 않은 모든 Multicast 메시지는 삭제 됩니다.

명령어	설명
[no] ip igmp-snooping dlf-frames filter	VLAN의 제외 설정을 구성 합니다. no 명령어로 설정을 삭제 합니다.

Note:

1) 모든 VLAN에 대해 속성이 구성됩니다.

2) 이 유형의 메시지를 처리하기 위한 스위치의 기본은 Forward 입니다.
(이 유형의 메시지는 VLAN 내에서 브로드캐스팅 됩니다.)

14.1.1.5 IGMP-snooping의 Router-age 설정

Router-age 타이머는 IGMP query의 사용 여부를 모니터링 하는데 사용됩니다. IGMP 메시지를 보내 Multicast address를 유지 합니다. IGMP-snooping은 IGMP query 와 호스트 간의 통신을 통해 작동합니다.
글로벌 모드에서 다음 설정을 수행하십시오.

명령어	설명
[no] ip igmp-snooping timer router-age timer_value	IGMP-snooping의 Route-Age값을 구성합니다. no 명령어로 기본값으로 다시 시작합니다.

Note.

타이머 설정 방법은 IGMP 요청자와 요청 시간 설정을 참조 하십시오.
타이머는 쿼리 기간보다 작게 설정할 수 없습니다. 타이머는 쿼리 기간의 세배로 설정하는 것이 좋습니다. IGMP-snooping의 Router-age 기본값은 260초 입니다.

14.1.1.6 IGMP-snooping의 Response Time 타이머 설정

Response Time 타이머는 IGMP 요청자가 메시지를 보낸 후 호스트가 Multicast 를 보고 하는 상한 시간입니다. 타이머가 지난 후 보고서 메시지가 수신되지 않으면 스위치는 Multicast 주소를 삭제 합니다.
글로벌 모드에서 다음 설정을 하십시오.

명령어	설명
[no] ip igmp-snooping timer response-time timer_value	IGMP-snooping의 응답시간 값을 설정합니다. no 명령어로 기본값으로 다시 시작합니다.

Note.

타이머 값은 너무 작으면 Multicast 통신이 불안정해집니다. IGMP-snooping의 응답시간 기본값은 10초로 설정 되어있습니다.

14.1.1.7 IGMP-snooping의 querier 설정

IGMP-snooping이 활성화 된 VLAN에 멀티 캐스트 라우터가 없으면 IGMP-snooping의 querier 기능을 사용하여 멀티 캐스트 라우터를 모방하여 IGMP querier 메시지를 정기적으로 전송할 수 있습니다. (이 기능은 전체에 적용됩니다. 즉, IGMP-snooping이 전체 적용으로 활성화 된 VLAN에서 활성화 또는 비활성화 할 수 있습니다.)
멀티 캐스트 라우터가 LAN에 존재하지 않고 멀티 캐스트 흐름에 라우팅이 필요하지 않은 경우 IGMP-snooping을 통해 스위치의 자동 querier 기능을 활성화 할 수 있으므로 IGMP-snooping이 제대로 작동합니다.
글로벌 설정 모드에서 다음 구성을 수행하십시오.

명령어	설명
[no] ip igmp-snooping querier [address [ip_addr]	IGMP-snooping의 querier를 구성합니다. 선택적 매개 변수 address는 조회 메시지의 소스 IP 주소입니다. no 명령어로 기본값으로 다시 시작합니다.

IGMP-snooping의 querier 기능은 기본적으로 비활성화 되어있습니다.
가짜 쿼리 메시지의 IP주소의 Default값은 10.0.0.200 입니다.

Note.
querier 기능이 활성화 되면 VLAN에 멀티캐스트 라우터가 있는 경우 해당 기능이 비활성화 됩니다. 멀티캐스트 라우터가 시간 초과되면 기능이 자동 활성화 됩니다..

14.1.1.8 IGMP-snooping의 모니터링 및 관리

명령어	설명
show ip igmp-snooping	igmp-snooping 설정 정보를 표시
show ip igmp-snooping timer	igmp-snooping의 시간 정보를 표시.
show ip igmp-snooping groups	igmp-snooping의 멀티캐스트 그룹에 대한 정보를 표시
show ip igmp-snooping statistics	igmp-snooping에 대한 통계 정보를 표시
[no] debug ip igmp-snooping [packet | timer | event | error]	igmp-snooping의 패킷, 시간, 이벤트, 에러의 표시를 활성화 및 비활성화 합니다.

15장. 802.1x 설정

15-1장 802.1x 설정

15.1.1 802.1x 설정 목록

- 802.1x 포트 인증 설정
- 802.1x 다중 포트 인증 설정
- 802.1x ID 인증 최대 시간 설정
- 802.1x 재 인증 설정
- 802.1x 전송 빈도 설정
- 802.1x 사용자 바인딩 설정
- 802.1x 포트에 대한 인증 방법 설정
- 802.1x 포트에 대한 인증 유형 선택 및 설정
- 802.1x 계정 설정
- 802.1x Guest VLAN 설정
- 다중 네트워크 카드 사용을 방지 설정
- 기본 802.1x 설정 및 다시 시작
- 802.1x 인증 설정 및 상태 모니터링

15.1.2 802.1x 설정

15.1.2.1 802.1x 포트 인증 설정

802.1x는 강제 인증 승인, 필수 인증 거부, 802.1x인증 시작 등의 세가지 제어 방법을 정의합니다.필수 인증 승인이란 포트가 이미 인증을 통과했음을 의미합니다. 포트는 더 이상 인증이 필요하지 않으며, 모든 사용자는 포트를 통해 데이터 액세스 제어를 수행할 수 있습니다. 인증 방법이 포트에 의해 감압됩니다. 강제 인증 거부는 어떠한 종류의 방법이 적용되어도 포트 인증이 통과되지 않음을 의미합니다. 포트를 통해 데이터 액세스 제어를 수행할 수 없습니다. 802.1x인증 시작이란 포트가 802.1x인증 프로토콜을 실행하는 것을 의미합니다. 포트에 액세스 하는 사용자에게 802.1x인증이 적용됩니다. 인증을 통과한 사용자만이 포트를 통해 데이터 액세스 제어를 수행할 수 있습니다. 802.1x인증을 시작한 후에는 AAA인증 방법을 구성해야 합니다.
802.1x를 구성하기 전에 다음 명령을 실행하여 802.1x기능을 실행하십시오.

명령어	설명
dot1x enable	802.1x를 활성화

다음 명령어를 실행하여 802.1x인증을 시작 합니다.

명령어	설명
dot1x port-control auto	포트에서 802.1x 프로토콜제어 방법을 설정
aaa authentication dot1x {default | list name} method	AAA 인증을 802.1q로 설정

포트 설정모드에서 다음 명령어 중 하나를 실행하여 802.1x 제어방법을 선택합니다.

명령어	설명
dot1x port-control auto	802.1x 인증을 방법을 시작
dot1x port-control force-authorized	강제 포트 인증을 승인
dot1x port-control force-unauthorized	강제 포트 인증을 해제

15.1.2.2 802.1x 다중 포트 인증 설정

802.1x인증은 단일 호스트 사용자의 인증을 위한 것입니다. 이 경우 스위치를 사용하면 한명의 사용자만 인증 및 액세스 제어를 수행할 수 있습니다. 이전 사용자가 인증 및 액세스를 종료하지 않으면 다른 사용자가 인증 및 액세스 할 수 없습니다. 포트가 802.1x스위치를 지원하지 않는 스위치 디바이스를 통해 포트를 여러 호스트에 연결하는 경우 여러 포트 액세스 기능을 시작하여 모든 호스트 사용자가 액세스 할 수 있도록 할 수 있습니다. 포트가 802.1x호스트 인증으로 구성된 후 이 스위치는 여러 호스트 사용자를 인증합니다. 인증이 승인되면 호스트가 스위치를 통해 액세스 할 수 있습니다(호스트의 MAC주소는 제어용으로 사용됨). 이론적으로 802.1x는 호스트 사용자 수를 제한할 수 없습니다. 사용자가 사용자의 MAC주소를 통해 사용자 인증을 제어하기 때문에 호스트 사용자의 수는 스위치의 MAC주소 테이블의 크기에 따라 제한됩니다. 인터페이스 구성 모드에서 다음 명령을 실행하여 802.1x다중 호스트 인증을 활성화합니다.

명령어	설명
dot1x multiple-hosts	802.1x의 다중 포트 인증을 설정

15.1.2.3 802.1x ID 인증 최대 시간 설정

802.1x인증 시작 또는 802.1x인증을 다시 수행하면 802.1x가 게스트 호스트에 ID인증 요청을 전송합니다. 네트워크 문제가 발생하여 요청 메시지가 삭제되거나 지연되면 요구 사항 메시지가 다시 전송됩니다. 메시지가 특정 시간에 발생하면 메시지를 보내기 위해 802.1x,stop중지 및 ID인증이 실패합니다. 다른 네트워크 조건에 따라 ID인증 요청의 최대 횟수를 재설정하여 인증 서버가 인증 서버에 의해 인증되었는지 확인할 수 있습니다.

인터페이스 구성 명령에서 다음 명령을 실행하여 ID인증 요청의 최대 시간을 설정합

니다.

명령어	설명
dot1x max-reg [count]	802.1x ID인증 요청 최대시간 설정

15.1.2.4 802.1x 재 인증 설정

첫번째 인증이 승인되면 클라이언트의 합법성을 보장하기 위해 클라이언트가 특정 시간마다 인증됩니다. 이 경우에는 재 인증 기능을 활성화해야 합니다. 다시 인증 기능을 사용하도록 설정한 후 802.1x가 주기적으로 인증 요청을 호스트에 전송합니다.
다음 명령을 실행하여 재 인증 기능을 구성할 수 있습니다.

명령어	설명
dot1x re-authentication	재 인증 기능을 활성화
dot1x timeout re-authperiod time	재 인증 기간을 설정
dot1x reauth-max time	다시 인증이 실패할 경우 재시도 횟수 설정

15.1.2.5 802.1x 전송 빈도 설정

802.1x인증 프로세스에서 데이터 텍스트가 호스트로 전송됩니다. 호스트 응답이 성공적으로 완료되도록 802.1x전송 빈도를 제어하여 데이터 전송을 조정할 수 있습니다.
다음 명령을 실행하여 전송 빈도를 구성합니다.

명령어	설명
dot1x timeout tx-period [time]	802.1x 의 전송 빈도를 설정

15.1.2.6 802.1x 사용자 바인딩 설정

802.1x인증을 수행할 때 사용자를 특정 포트에 바인딩 하여 포트 액세스 보안을 보장할 수 있습니다. 인터페이스 구성 모드에서 다음 명령을 실행하여 802.1x사용자 바인딩을 시작합니다.

명령어	설명
dot1x user-permit [xxxyyy]	포트에 바인딩할 사용자를 설정

15.1.2.7 802.1x 포트에 대한 인증 방법 설정

802.1x인증은 서로 다른 포트에서 서로 다른 방법으로 수행할 수 있습니다. 기본 구성에서 802.1x인증은 기본 메서드를 사용합니다. 인터페이스 구성 모드에서 다음 명령을 실행하여 802.1x인증 방법을 구성합니다.

명령어	설명
dot1x authentication method [xxx]	802.1x 인증 방법을 설정 합니다.

15.1.2.8 802.1x 포트에 대한 인증 유형 선택 및 설정

802.1x인증의 유형을 선택할 수 있습니다. 802.1x인증 유형은 AAA인증이 CHAP인증 또는 Eap인증을 사용하는지 여부를 결정합니다. Eap인증은 MD5가 지원하는 모드와 대기 모드를 지원합니다. CHAP인증이 채택된 경우에는 CHAP인증이 로컬에서 생성되고 CHAP인증이 채택될 때 인증 서버에서 문제가 발생합니다. 각 포트는 하나의 인증 유형만 사용합니다. 글로벌 구성의 인증 유형은 기본적으로 채택됩니다. 포트가 인증 유형으로 설정된 후에는 기본 값을 다시 실행하지 않으면 포트가 인증 유형을 사용하여 인증 유형을 사용합니다. Eaff-tis는 전자 인증서를 인증 영장으로 가져가고, 변환 계층 보안(tls)의 핸드 셰이크 규칙을 준수합니다. 따라서 보안이 보장됩니다.
글로벌 구성 모드에서 다음 명령을 실행하여 인증 유형을 구성하십시오.

명령어	설명
dot1x authen-type {chap | eap}	CHAP 또는 EAP 로 설정 합니다.

또한 인터페이스 설정 모드에서 다음 명령을 실행합니다.

명령어	설명
dot1x authentication type {chap | eap}	글로벌 모드에서 CHAP 또는 EAP로 인증 유형을 선택 합니다.

15.1.2.9 802.1x 계산 설정

802.1x인증 및 802.1x계산는 동시에 수행할 수 있습니다. 작동 메커니즘이 승인된 경우, 인증 기능이 인증 인터페이스에서 활성화되었는지 여부를 판단하고, 계산 함수가 활성화된 경우 AAA인터페이스를 통해 계산 요청을 전송합니다. AAA인터페이스가 성공적인 요청을 전달할 수 있습니다. 계산은 AAA모듈에 구성된 다양한 계산 방법을 채택할 수 있습니다. 자세한 내용은 AAA구성을 참조하십시오. 계산이 시작된 후, 자막은 정확한 계산 정보를 얻기 위해 AAA인터페이스를 통해 서버로 업데이트 메시지를 정기적으로 전송합니다. AAA구성에 따라 AAA모듈이 업데이트 메시지를 보낼지 여부를 결정합니다. 동시에 스위치가 비정상적으로 비정상적일 때는 스위치가 정상적으로 작동할 수 있도록 하기
위해 X1인증 기능을 사용하도록 설정해야 합니다.
인터페이스 구성 모드에서 다음 명령을 실행하여 dot1x계산을 활성화하고 계산 방법을 구성합니다.

명령어	설명
dot1x accounting enable	802.1x 계산을 활성화합니다.
dot1x accounting method {method name}	계산 방법을 설정합니다.

15.1.2.10 802.1x Guest VLAN 설정

Guest-VLAN은 클라이언트가 응답하지 않을 때 클라이언트 소프트웨어의 일부 액세스 권한(예:클라이언트 소프트웨어 다운로드)를 제공합니다. Guest-VLAN은 시스템에 구성 되어있을 수 있습니다.

참고: 인증 실패 하면 액세스 권한이 없습니다.

전역 모드에서 다음 명령을 실행하여 게스트-vlan을 사용하도록 설정합니다.

명령어	설명
dot1x guest-vlan	모든 포트에 Guest-VLAN을 설정

각 포트에서 Gust-VLAN ID의 값이 0이면 Guest-VLAN이 글로벌 모드에서 활성화 되어있더라도 Guest-VLAN이 작동하지 않을 수 있습니다. 포트 설정 모드에서 Guest-VLAN ID가 구성된 경우에만 Guest-VLAN이 동작 할 수 있습니다.

포트 구성 모드에서 다음 명령을 실행하여 Guest-VLAN ID를 설정합니다.

명령어	설명
dot1x guest-vlan {id(1-4094)}	해당 포트에 Guest-VLAN을 사용하도록 설정

15.1.2.11 다중 네트워크 카드 사용 방지 설정

다수의 네트워크 어댑터를 사용하여 에이전트를 방지합니다. 포트 설정 모드에서 다음 명령어를 실행합니다.

명령어	설명
dot1x forbid multi-network-adapter	다수의 네트워크 어댑터를 사용하도록 설정

15.1.2.12 기본 802.1x 설정 및 다시 시작

다음 명령을 실행하여 모든 글로벌 구성을 기본 구성으로 재시작 합니다.

명령어	설명
dot1x default	모든 글로벌 구성을 기본 구성으로 재시작

15.1.2.13 802.1x 인증 설정 및 상태 모니터링

802.1x인증의 구성 및 상태를 모니터링 하고 조정해야 하는 802.1x 매개변수를 확인 하려면 관리모드에서 다음 명령을 실행하십시오.

명령어	설명
show dot1x {interface ..... }	802.1x 인증의 구성 및 상태를 모니터링

15.1.2.14 802.1x 설정 예제

호스트A는 스위치의 F0/10 포트에 연결 합니다. 호스트B는 F/0/12 포트에 연결 합니다. 무선 서버 호스트의 IP 주소는 192.168.20.2 입니다. Radius 설정 Key값은 TST 입니다. Port F0/10은 접속 Radius 인증 및 사용자 바인딩을 설정 합니다. Port F0/12는 eap 유형의 로컬 인증을 설정하고 Port F0/12에서 멀티캐스트를 사용하도록 설정 합니다

전역 구성

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-F0/10 radius
aaa authentication dot1x TST-F0/12 local
interface VLAN1
ip address 192.168.20.24 255.255.255.0
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813 radius-server key TST
```

포트 F0/10 설정

```
interface FastEthernet0/10
  dot1x port-control auto
  dot1x authentication method TST-F0/10
  dot1x user-permit radius-TST
```

포트 F0/12 설정

```
interface FastEthernet0/12
  dot1x multiple-hosts
  dot1x port-control auto
  dot1x authentication method TST-F0/12
  dot1x authentication type eap
```

16장. MAC 주소 목록 설정

16-1장 Mac address List 설정

16.1.1 MAC List 설정 구성

16.1.1.1 MAC List생성

포트에 MAC List을 적용하려면 먼저 MAC List을 생성해야 합니다. MAC List가 생성되면 MAC List 설정 모드에서 다음 MAC Access List을 설정할 수 있습니다. 다음 작업을 수행하여 권한 모드에서 MAC List을 추가하고 삭제합니다.

명령어	설명
[no] mac access-list [name]	Mac list를 추가하거나 삭제 합니다. [name]은 Mac List의 이름을 의미합니다. no 명령어를 이용하여 삭제 할 수 있습니다.

16.1.1.2 Mac List 생성

Permit/Deny 명령어를 사용하여 Mac List의 허용 또는 거부 List를 설정 할 수 있습니다. Mac List에서 여러 개의 Permit/Deny List를 설정 할 수 있습니다. Mac List에 설정된 여러 항목의 MAC목록에 구성된 여러 항목의 마스크는 동일해야 합니다. 그렇지 않으면 구성이 잘못되었을 수 있습니다(다음 예시 참조). 동일한 항목은 동일한 MAC주소로만 구성할 수 있습니다.

MAC목록 구성 모드에서 다음 작업을 수행하여 MAC목록의 항목을 구성합니다.

명령어	설명
[no] {deny | permit} {any | host src-mac-addr} {any | host dst-mac-addr}[ethertype]	Mac list의 항목을 추가 삭제 합니다. no 명령어를 이용하여 삭제 할 수 있습니다 모든 Mac-address를 호환할 수 있음을 의미. Src-mac-addr은 source Mac 주소입니다. Dst-mac-addr은 destination Mac 주소입니다. Ethertype은 이더넷 패킷 유형을 의미합니다.

Mac list configuration 예시

Switch_config#mac acce 1

Switch-config-macl#permit host 1.1.1 any

Switch-config-macl#permit host 2.2.2 any

위의 설정은 source mac address 주소를 비교하는 것이므로 마스크가 동일합니다. 설정이 정상적으로 되었습니다.

Switch_config#mac acce 1

Switch-config-macl#permit host 1.1.1 any

Switch-config-macl#permit any host 1.1.2

Switch-config-macl#2003-11-19 18:54:25 rule conflict, all the rule in the acl should match!

위의 설정은 첫번째 행은 source Mac-address를 비교하는 반면 두번째 행은 destination Mac-address를 비교하는 것입니다. 따라서 Mask가 동일하지 않으므로 설정이 정상적으로 되지 않습니다.

16.1.1.3 MAC List 적용하기

생성된 Mac list는 모든 물리적 포트에 적용할 수 있습니다.
동일한 Mac-list를 하나의 포트 또는 여러 포트에 적용할 수 있습니다.
포트 설정 모드에서 다음 명령어를 사용하여 Mac-list를 설정 합니다.

명령어	설명
interface f0/1 [no] mac access-group name	설정할 포트에서 생성된 Mac-list를 포트에 적용 하거나 적용된 Mac-list를 삭제 할 수 있습니다.

17 장. Vlan Access List 설정

17-1장 VLAN Access List 설정

이 기능은 사용자가 VLAN에서 불필요한 메시지를 필터링 하도록 도움을 줄 수 있습니다. 위의 설정은 높은 보안을 제공 합니다.
각각의 VLAN Access List는 서로 다른 우선순위를 가진 여러 Access 제어 목록(VLAN ACL)으로 구성 됩니다. 각 Access 제어 목록은 일치 항목과 작업 항목으로 구성 됩니다. 일치 항목은 IP Access 제어목록 또는 MAC Access 제어 목록입니다. 일치항목이 설정되어 있지 않은 것은 모든 Flow가 일치 한다는 뜻이며 일치 항목에 대해 Null IP/Mac access control list가 설정 되어있는 것은 일치 하지 않음을 의미 합니다. 일치항목에 대한 IP/MAC Access control list가 설정이 되어있으면 VLAN ACL 항목이 정상적으로 작동하지 않습니다. 하나의 IP/MAC Access control list가 설정된 경우 마지막이 유효하고. 하나의 permit되는 항목만 IP/MAC Access Control List에 있습니다. VLAN ACL이 VLAN에 적용 될 경우 문제가 발생하지 않습니다. 여러 번에 VLAN ACL을 구성하여 여러 개의 permit 항목을 생성할 수 있습니다. 이 기능으로 Forward 또는 Drop을 할 수 있습니다. 이 기능은 기본적으로 Forward 입니다. VLAN ACL은 IP/MAC Access control list와 일치하는 Flow의 작업 항목에 정의된 작업을 수행 합니다. VLAN ACL은 VLAN ACL의 직렬 번호에 따라 각 VLAN ALC을 사용하며 VLAN ACL과 일치하지 않는 Flow를 줄일 수 있습니다. 이러한 방식으로 Access control이 이루어집니다. 지정된 Flow를 Deny 하려면 모든 Flow를 전달할 수 있는 VLAN ACL을 설정하고. 위와 같은 방식으로 Deny되지 않은 Flow를 전달 할 수 있습니다.

다음 명령을 실행하여 VLAN Access Control List를 설정 합니다.

명령어	설명
Vlan access-map name seq	VLAN 기반 Access Control List를 생성합니다. 동일한 매개변수 이름을 가진 모든 설정은 동일한 VLAN ACL에 속합니다. 매개변수 seq는 VLAN ACL에서 우선순위를 의미합니다. 기본값은 VLAN ACL+5의 가장 높은 우선순위입니다.
match <ip-acl | mac-acl> name	일치되는 항목이 지정된 VLAN에 대해 IP 할당 또는 MAC을 설정 합니다.
action <drop | forward>	VLAN ACL의 Drop 혹은 Forward를 설정 합니다. 기본 값은 Forward 입니다..
vlan filter name vlan	VLAN의 이름이 지정된 VLAN ACL을 적용합니다. 매개변수 VLAN은 ARP가 적용되는 VLAN을 의미 합니다.

18장. IP Access List 설정

18-1장 물리적인 포트기반의 IP Access List 설정

18.1.1 IP 메시지 필터링

메시지 필터링은 네트워크에 패킷의 실행을 제어하도록 합니다 이 제어기능은 네트워크에서 전송을 제한하거나 사용자 또는 장치를 통해 제한 할 수 있습니다. 교차된 지정포트에 패킷을 활성화하거나 비활성화하려면 라우팅 스위치가 다음을 안내합니다.
Access list는 다음과 같이 사용할 수 있습니다.

- 포트에서 패킷 전송 제어
- 가상 터미널 라인의 접근 제어
- 라우팅 업데이트 내용 제한

이 단계에서는 IP Access List를 만들고 사용하는 방법에 대하여 설명합니다..

IP Access List는 IP 주소의 허용 및 금지 조건을 적용하기 위해 규칙적으로 설정된 IP입니다. 라우팅 스위치의 ROS 소프트웨어 (*ROS소프트웨어는 로봇 운영체제를 의미)는 Access List의 주소를 하나씩 테스트합니다. 첫 번째 매치에서는 소프트웨어가 주소를 수락할지 거부 할지를 결정합니다. ROS 소프트웨어는 첫 번째 매치 이후 경기 규칙을 중지하기 때문에 조건에 관한 순서가 매우 중요합니다. 매치된 규칙이 없다면, 주소가 거부됩니다

Access List를 사용하기전에 다음과 같은 단계를 수행해야합니다.

(1) Access List 이름과 접근경로를 지정하여 IP엑세스 목록을 만듭니다.

20 포트에 IP Access List를 적용합니다.

18.1.2 Access List의 표준 및 확장기능

문자열을 사용하여 IP Access List를 만듭니다.

Note :

표준 IP Access List과 확장 가능 IP Access List 은 같은 이름을 사용할 수 없습니다.

Global configuration 모드에서 다음 명령을 실행하여 IP Access List를 생성합니다..

명령어	설명
IP Access-List 표준 이름	표준 IP access list의 이름을 정의.

deny {source [source-mask] | **any**} or **permit** {source [source-mask] | **any**}	하나이상의 **permit/reject** 지정 패킷이 승인되었는지 여부를 결정하는 표준 IP Access-List 구성 모드의 조건.
Exit(종료)	IP Access-List의 구성모드 로그아웃

Global 구성 모드에서 다음 명령을 실행하여 확장 가능한 IP Access-List를 만듭니다.

명령어	실행
IP access-list 확장된 이름	ip access-list를 이름을 사용하여 확장 가능 하도록 정의
{**deny** | **permit**} protocol source source-mask destination destination-mask [**precedence** precedence] [**tos** tos] {**deny | permit**} protocol **any any**	**하나 이상의 deny** or **permit 정의.** 확장 Access-list 조건은 IP 패킷의 통과 여부를 결정하는 구성 모드 (우선 순위는 IP 패킷의 우선 순위를 의미하며, TOS는 서비스 유형의 단순화 된 형태입니다). 프로토콜이 TCP / UDP이면 특정 범위의 단일 포트 또는 포트 14번을 지정할 수 있습니다. 자세한 내용은 "Extensible Access List Example"을 참조 바랍니다.
Exit(종료)	Access-list에서 로그아웃

액세스 목록이 만들어진 후에는 추가 된 부분이 (터미널에 접속허용한다면) 목록 끝에 추가됩니다. 즉, 명령 줄에 지정 Access-list를 추가 할 수 없습니다.

그러나 항목을 삭제하려면 허용 제한과 거부 제한을 실행할 수 있습니다.

Note:

Access-list을 만들 때 Access-list의 끝 부분에 보이지 않는 허용되지않은 문장이 있다는 것을 기억하십시오. 마스크가 관련 IP 주소 Access-list에 지정되지 않은 경우 255.255.255.255가 마스크로 간주됩니다.

Access-list을 만든 후에는 회선이나 포트에 적용해야 합니다.

18.1.3 "포트에 Access-list 적용"

Access-list 을 만든 후에 하나 이상의 포트 또는 항목에 적용 할 수 있습니다.

포트 구성 모드에서 다음 명령을 실행합니다.

명령어	실행
ip access-group name	Access-list에 포트를 적용.

기존 전체 Access-list 의 경우 패킷 수신 Access-list에 검사 패킷의 원본 주소가 확인됩니다. 확장형 Access-list 의 경우 라우팅 스위치는 대상 주소도 확인합니다. 액세스 목록에 대상 주소가 허용되면 소프트웨어는 패킷을 계속 처리합니다. 액세스 목록이 대상 주소를 거부하면 소프트웨어는 패킷을 삭제하고 ICMP 호스트에 도달 할 수 없다는 메시지를 반환합니다.

지정된 액세스 목록이 없으면 모든 패킷이 통과 할 수 있습니다.

18.1.4 확장 Access-list의 예제

18.1.4.1 포트기반 IP Access List의 TCP/UDP 포트에 관한 지원 필터링

다음과 같은 예를 들 수 있습니다.

{**deny | permit**} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt } port] }]

[**precedence** precedence] [**tos** tos]

이 경우 TCP 및 UDP의 포트 l4는 Access-list을 통해 제어 할 수 있습니다. 포트 범위를 정의하여 Access-list을 구성 할 때 다음에 주의하십시오.

(1) 포트를 지정하여 Source 및 destination 에서 Access-list를 구성한 경우 범위 내에 있으면 구성중에 많은 source가 사용되기 때문에 일부 구성이 실패 할 수 있습니다. 이 문제를 해결하려면 한 포트 범위와 다른 포트의 범위를 지정하는 것이 좋습니다.

(2) 포트 범위 필터링을 사용하면 많은 리소스가 필요합니다. 액세스 목록은 포트 범위 필터링이 다른 응용 프로그램에 지원됩니다. 너무 많은 범위에 필터링을 사용하기 때문입니다.

18.1.4.2 포트 기반 IP 액세스의 필터링을 지원하는 포트 기반 IP 액세스 목록 TCP / UDP 지정

포트 목록 필터링 지원합니다.

다음과 같은 경우 첫 번째 명령 줄에서 새로 오는 TCP가 호스트 130.2.1.2의 SMTP에 연결할 수 있습니다.

ip access-list extended aaa

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface g0/10

ip access-group aaa

19 장 네트워크 프로토콜 구성

19-1장 IP 주소 설정

19.1.1 IP 소개

19.1.1.1 IP 라우팅 프로토콜

Internet Protocol (IP)는 네트워크에서 문자형식으로 데이터를 교환하는 프로토콜입니다. IP에는 주소 지정, 분산화, 재그룹화 및 다중화와 같은 기능이 있습니다. 다른 IP 프로토콜 (IP Protocol Cluster)은 IP를 기반으로 합니다. 네트워크 계층에 작동하는 프로토콜로서 IP는 주소 지정 정보와 제어 정보를 포함하고 라우팅에 사용됩니다.

Transmission Control Protocol (TCP)는 IP를 기반으로 합니다. TCP는 데이터 전송 시 데이터 및 정보의 형식을 규제하는 연결 지향 프로토콜입니다. 또한 TCP는 데이터에 성공적으로 도달했음을 알리는 방법을 제공합니다. TCP는 시스템의 여러 응용 프로그램이 수신 된 데이터를 각각의 응용 프로그램에 각각 보낼 수 있기 때문에 동시에 통신 할 수 있게 합니다.

주소 해석 프로토콜과 같은 IP 주소 지정은 1.3 절 "IP 주소 지정 구성"에서 설명합니다. ICMP, HSRP, IP 통계 및 성능 매개 변수와 같은 IP 서비스는 4 장 "구성IP 서비스입니다. "

19.1.1.2 IP 라우팅 프로토콜

우리의 라우팅 스위치는 각 프로토콜의 소개에서 설명 될 여러 IP 라우팅 동적 프로토콜을 지원합니다. IP 라우팅 프로토콜은 두 가지 그룹 Interior Gateway Routing Protocol (IGRP) 및 Exterior Gateway Routing Protocol (EGRP)으로 구분됩니다. 우리의 라우팅 스위치는 RIP, OSPF, BGP 및 BEIGRP를 지원하며 요구사항에 따라 RIP, OSPF, BGP 및 BEIGRP를 각각 구성 할 수 있습니다. 또한 우리의 스위치는 다중 라우팅 프로토콜을 동시에 구성하는 프로세스, OSPF 프로세스의 임의의 수 (메모리를 분배할 수 는 경우), BGP 프로세스, RIP 프로세스 및 임의의 수의 BEIGRP 프로세스를 지원합니다. redistribute 명령을 실행하여 다른 라우팅 프로토콜의 경로를 현재 라우팅 프로세스의 데이터베이스에 재분배하고 여러 프로토콜 프로세스의 경로를 연결할 수 있습니다.

IP 동적 라우팅 프로토콜을 구성하려면 먼저 관련 프로세스를 구성해야 합니다.

관련 네트워크 포트를 동적 라우팅 프로세스와 상호 작용하도록 만든 다음

포트에서 시작될 라우팅 프로세스를 지정합니다. 이를 위해 구성 명령 문서의 구성 단계를 점검 할 수 있습니다.

(3) 라우팅 프로토콜을 선택한다.

- 네트워크의 규모와 복잡성
- 깊이가 다양한 네트워크가 지원 될 필요가 있는지 여부
- 네트워크 트래픽
- 안전 요구사항
- 신뢰성 요구사항
- 다양한 방법
- 기타

위 항목에 대한 자세한 내용은이 절에서 설명하지 않습니다. 라우팅 프로토콜들을 선택할 때 네트워크 요구 사항이 충족되어야 다는 것을 알려드립니다.

(4) IGRP

Interior Gateway Routing Protocol (IGRP)는 자치 시스템의 네트워크 대상에 사용됩니다. 모든 IP IGRP는 시작될 때 네트워크와 연결되어야 합니다. 각 라우팅 프로세스는 네트워크의 다른 라우팅 스위치에서 업데이트 메시지를 모니터링하고 해당 라우팅 메시지를 같은 시간 네트워크에서 Broadcast 합니다.

라우팅 스위치가 지원하는 IGRP는 다음과 같습니다.

- RIP
- OSPF
- BEIGRP

(5) EGRP

Exterior Gateway Routing Protocol (EGRP) 서로 다른 자율 시스템 간의 라우팅 정보를 교환하는 데 사용됩니다. 경로를 교환하는 이웃, 도달 가능한 네트워크 및 지역치 시스템 번호는 일반적으로 구성되어야 합니다. 스위치가 지원하는 EGRP 프로토콜은 BGP입니다.

19.1.2 IP 작업 목록 구성

IP 구성을 위한 필수적인 요구 사항은 라우팅 스위치의 네트워크 인터페이스에 IP 주소를 구성하는 것입니다. 이 경우에만 네트워크 인터페이스를 활성화 할 수 있으며 IP 주소는 다른 시스템과 통신 할 수 있습니다. 동시에 IP 네트워크 마스크를 확인해야합니다. IP 주소 지정을 구성하려면 다음 작업을 완료해야 합니다.

첫번째 일은 의무 사항이며 다른 일은 선택 사항입니다. 네트워크에서 IP 주소 지정을 만들려면 1.4 "IP 주소 지정 예제"를 참조하십시오.

다음은 IP 주소 구성 작업 목록입니다.

- 네트워크 인터페이스에서 IP 주소 구성
- 네트워크 인터페이스에서 다중 IP 주소 구성
- 주소 해석
- 라우팅 프로세스 구성
- Broadcast text 관리 구성
- IP 주소 감지 및 유지 관리

19.1.3 IP 주소 구성

19.1.3.1 네트워크 인터페이스 IP 주소 구성

P 주소는 IP 메시지를 보낼 대상을 결정합니다. 일부 IP 특수 주소는 예약되어 있으며 호스트 IP 주소 또는 네트워크 주소로 사용할 수 없습니다. 표 1에는 IP 주소 범위, 예약 된 IP 주소 및 사용 가능한 IP 주소입니다.

형태	**주소와 범위**	**상태**
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	지정 유효 지정
B	128.0.0.0 to 191.254.0.0 191.255.0.0	유효 지정
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	지정 유효 지정
D	224.0.0.0 to 239.255.255.255	Multicast 주소

E	240.0.0.0 to 255.255.255.254 255.255.255.255	예약 주소 Broadcast 주소

IP 주소에 대한 공식적인 설명은 RFC 1166 "Internet Digit" 참조하며 Internet Service Provider(ISP)에 문의 할 수 있습니다. 인터페이스에는 기본 IP주소가 하나만 있으며 인터페이스 구성 모드에서 다음 명령을 실행하여 네트워크 인터페이스의 기본 IP 주소와 네트워크 마스크를 구성하십시오.

명령어	설명
ip address ip-address mask	인터페이스에 메인 IP 주소를 구성

마스크는 네트워크를 나타내고 IP주소의 일부입니다.

Note : 우리의 스위치는 네트워크 문자 순서에 따라 가장 높은 바이트에서 연속적으로 설정된 마스크 만 지원합니다.

.1.3.2 네트워크 인터페이스 다중 IP 주소구성

각 인터페이스는 기본 IP 주소와 여러 하위 IP 주소를 포함하여 여러 IP 주소를 소유 할 수 있습니다. 다음 두 가지 경우에 하위 IP 주소를 구성해야 합니다.

- 네트워크 세그먼트에 IP 주소가 충분하지 않은 경우

예를 들어 특정 논리 서브넷에는 254 개의 사용 가능한 IP 주소 만 있지만 물리적 네트워크를 연결하려면 300 개의 호스트가 필요합니다. 이 경우 스위치 또는 서버에서 하위 IP 주소를 구성하여 두 개의 논리 서브넷이 동일한 실제 서브넷을 사용할 수 있게 할 수 있습니다. 2계층 브리지를 기반으로 하는 초기 단계 네트워크의 대부분은 여러 서브넷으로 분할되지 않습니다. 하위 IP 주소를 올바르게 사용하여 초기 단계 네트워크를 여러 경로 기반 서브넷으로 나눌 수 있습니다. 구성된 종속 IP 주소를 통해 네트워크의 라우팅 스위치는 동일한 실제 네트워크를 연결하는 여러 서브넷을 인식 할 수 있습니다.

- 다른 네트워크에 의하여 물리적으로 분리된 하나의 네트워크에 2 개의 서브넷이 있는 경우

이 경우 네트워크의 주소를 종속 IP 주소로 사용할 수 있습니다. 따라서 물리적으로 분리 된 논리적 네트워크의 두 서브넷은 논리적으로 함께 연결됩니다.

Note : 네트워크 세그먼트의 라우팅 스위치에 대한 하위 주소를 구성하는 경우 같은 네트워크 세그먼트의 다른 라우팅 스위치에 대해 이 작업을 수행해야 합니다.

인터페이스 설정 모드에서 다음 명령을 실행하여 네트워크 인터페이스에서 여러 IP 주소를 구성하십시오.

실행	설명
ip address ip-address mask **secondary**	네트워크 인터페이스에서 다중 IP 주소를 넣을 수 있다.

Note: IP 라우팅 프로토콜이 경로 업데이트 정보를 전송하는 데 사용될 때 하위 IP 주소는 다른 방식으로 처리 될 수 있습니다

◆ 주소 설정 해결법

IP는 IP 주소 분석과 같은 기능을 구현할 수 있습니다. 다음은 주소 구성을 확인하는 방법을 나타냅니다.

◆ 주소 해결법 만들기

IP 장치는 로컬 주소(로컬 네트워크 세그먼트 와 LAN으로 특별히 구별 된 장치) 와 네트워크 주소(장치에 위치를 나타내는 네트워크) 두가지를 가지고 있습니다. 로컬 주소는 링크 계층의 메시지 헤더에 포함되어 있으며 링크 계층의 장치에서 읽고 사용하므로 로컬 계층주소는 링크계층의 주소입니다. 전문가들은 항상 MAC 주소라고 부릅니다. 이는 링크 계층의 MAC 하위계층이 주소를 처리하는 데 사용되기 때문입니다.

예를 들어 호스트가 이더넷의 장치와 통신하도록 하려면 장치의 48 비트 MAC주소 또는 링크 계층의 로컬 주소를 알아야합니다. IP 주소에서 링크 계층의 로컬주소를 얻는 방법을 ARP (Address Resolution Protocol)라고 합니다. 링크 계층의 로컬주소에서 IP 주소를 얻는 방법을 RARP (Reverse Address Resolution)라고 합니다.

우리의 시스템은 두가지 유형의 주소 해결법을 ARP와 Proxy ARP 적용한다. ARP와 Proxy ARP는 RFC(860)과 RFC(1027)에 각각 정의되어 있습니다. ARP는 IP주소를 미디어 매체나 MAC주소에 매핑하는데 사용하고 IP주소로 ARP는 해당하는 MAC주소를 찾습니다. MAC 주소를 알고 있으면 IP 주소와 MAC 주소 간의 매핑 관계가 빠른 액세스를 위해 ARP 캐시에 저장됩니다. 그러면 IP 메시지는 링크계층의 메시지에 패키징 되어 마지막으로 네트워크로 전송됩니다.

● Static ARP 캐시 정의

ARP 와 다른 주소 확인 프로토콜은 IP 주소와 MAC 주소 사이의 Dynamic mapping 을 제공합니다. 대부분의 호스트가 동적 주소 확인을 지원하므로 정적 ARP 캐시 항목은 일반적으로 필요하지 않습니다. 필요한 경우 전체 구성 모드로 정의 할 수 있습니다. 시스템은 Static ARP 캐시 항목을 사용하여 32 비트 IP 주소를 48 비트 MAC 주소로 변환합니다. 또한 라우팅 스위치를 지정하여 다른 호스트에 대한 ARP 요청에 응답 할 수 있습니다.

ARP 항목을 영구적으로 존재하지 않으려면 ARP 항목의 활성 기간을 설정할 수 있습니다. 다음 두 유형은 고정 IP 주소와 MAC 주소 간의 매핑을 구성하는 방법을 보여줍니다.

전체 구성 모드에서 다음과 같은 명령어를 수행할 수 있습니다.

명령어	설명
arp ip-address hardware-address	ARP 캐시의 IP주소를 전체적으로 MAC주소로 매핑합니다.
arp ip-address hardware-address **alias**	라우팅의 MAC주소를 통해 지정된 IP 주소의 ARP 요청에 응답하도록 라우팅 스위치를 지정합니다.

인터페이스 구성모드에서 명령어를 실행합니다

명령어	설명
arp timeout *seconds*	ARP 캐시에서 ARP 캐시 항목의 시간의 초과 시간을 설정하십시오.

명령어 show interface는 지정 인터페이스의 ARPM timeout을 나타냅니다.

명령어 show arp는 ARP 캐시의 내용을 확인합니다

명령어 Clear arp는 모든 항목의 arp 캐시를 지웁니다.

- Proxy ARP 활성화

시스템 proxy ARP (RFC 1027으로 정의)를 사용하여 다른 네트워크에 해당경로가 없는 호스트를 MAC주소로 가져옵니다. 예를 들어 라우팅 스위치가 ARP 요청을 수신하고 기존 호스트와 대상 호스트가 동일한 인터페이스에 연결되어 있지 않아 라우팅 스위치가 대상 호스트에 도달하는 모든 경로에 ARP 요청을 수신하여 인터페이스를 통과하지 않는 경우, 링크 계층의 주소를 포함하는 프록시 ARP 응답을 보냅니다. 그 다음 기존 호스트는 메시지를 라우팅 스위치로 보내고 스위치는 대상 호스트로 메시지를 전달합니다. 프록시 ARP는 기본적으로 활성화됩니다.

프록시 ARP를 활성화하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip proxy-arp	Proxy-ARP를 인터페이스에서 활성화

- 자유로운 ARP 기능 구성

스위치는 자유로운 메시지를 전송하여 다른 장치의 IP 주소가 IP 주소와 충돌하는지 여부를 알 수 있습니다. 자유로운 ARP 메시지에 포함 된 소스 IP 주소와 대상 IP 주소는 모두 스위치의 로컬 주소입니다. 메시지의 소스 MAC 주소는 로컬 MAC 주소입니다.

스위치는 기본적으로 자유로이 ARP 메시지를 처리합니다. 스위치가 장치에서 자유로운 ARP 메시지를 수신하고 메시지에 포함 된 IP 주소가 자체 IP 주소와 충돌하면 장치에 ARP 응답을 반환하여 IP 주소가 서로 충돌 함을 알립니다. 동시에 스위치는 IP 주소가 충돌한다는 것을 로그

로 사용자에게 알려줍니다.

자유로운 ARP 메시지를 보내는 스위치의 기능은 기본적으로 비활성화되어 있습니다. 다음 명령을 실행하여 스위치의 포트에서 사용 가능한 ARP 기능을 구성하십시오.

명령어	설명
arp send-gratuitous	인터페이스에서 ARP 메시지 시작
arp send-gratuitous interval *value*	자동 ARP 메시지 간격을 선택 기본값은 120초 입니다.

◆ IP주소에 Host 이름을 매핑

특정 IP 주소는 호스트 이름과 일치 할 수 있습니다. 시스템은 telnet 또는 ping을 수행 할 수 있는 호스트 이름 - 주소 매핑 캐시를 저장합니다.

전체 구성 모드에서 다음 명령을 실행하여 호스트 이름과 IP 주소 간의 매핑을 지정하십시오.

명령어	설명
ip host *name address*	IP주소에 호스트이름을 고정시킨다.

19.1.3.4 라우팅 프로세스 구성

네트워크 요구 사항에 따라 하나 이상의 라우팅 프로토콜을 구성 할 수 있습니다. 라우팅 프로토콜은 네트워크 토폴로지에 대한 정보를 제공합니다. BGP, RIP 및 OSPF와 같은 IP 라우팅 프로토콜 구성에 대한 내용은 다음 절에 소개합니다.

19.1.3.5 Broadcast 메시지 처리 구성

Broadcast 메시지의 대상 주소는 모두 실제 네트워크의 모든 호스트입니다. 호스트는 특별한 주소를 통해 Broadcast 메시지를 식별 할 수 있습니다. 일부 중요한 인터넷 프로토콜을 포함한 일부 프로토콜은 일부 Broadcast 메시지를 사용합니다. IP 네트워크 관리자의 주요 임무 중 하나는 Broadcast 메시지를 제어하는 것입니다. 이 시스템은 지정 Broadcast, 즉 지정된 네트워크의 Broadcast를 지원합니다. 시스템이 네트워크의 모든Subnet Broadcast를 지원하지 않습니다.

일부 초기 단계 IP는 현재 Broadcast 주소 표준을 채택하지 않습니다. 이러한 IP에 의해 채택 된 Broadcast 주소는 완전히 숫자 "0"으로 표시됩니다. 시스템은 두 가지 유형의 메시지를 동시에 식별하고 수신 할 수 있습니다.

1. 지정된 Broadcast에서 물리적인 Broadcast로 허용된 변환

지정 IP Broadcast 메시지는 기본적으로 삭제되어 스위치가 "서비스 거부 됨" 메시지에 의한 공격을 차단합니다. 지정 Broadcast가 실제 메시지로 변환되는 인터페이스에서 지정 IP Broadcast 전달 기능을 활성화 할 수 있습니다. 전달 기능이 활성화되면 인터페이스를 연결하는 네트워크의 모든 지정 Broadcast 메시지가 인터페이스로 전달됩니다. 그런 다음 메시지가 실제 Broadcast 메시지로 전송됩니다. Broadcast 메시지의 전달을 제어하는 액세스 테이블을 지정할 수 있습니다.액세스 테이블이 지정되면 액세스 테이블에서 허용하는 IP 메시지만 지정Broadcast에서 물리적인 Broadcast로 변환 될 수 있다.

인터페이스 구성모드에서 지정된 Broadcast의 전달을 활성화하세요

명령어	설명
ip directed-broadcast [*access-list-name*]	인터페이스에서 지정->물리적인 Broadcast 변환을 허용합니다

2. UDP Broadcast 메시지 전달

호스트는 일부 UDP Broadcast 메시지를 주소, 구성 및 이름 등에 대한 정보를 결정합니다. 호스트가 있는 네트워크에 UDP 메시지를 전달할 서버가 없는 경우 호스트는 UDP 메시지를 수신 할 수 없습니다.

이 문제를 해결하기 위해 해당 인터페이스에서 일부 구성을 수행하여 일부 유형의 Broadcast 메시지를 보조 주소로 전달할 수 있습니다. 인터페이스에 대해 여러 개의 보조 주소를 구성 할 수 있습니다.

UDP 대상 포트를 지정하여 전달할 UDP 메시지를 결정할 수 있습니다. 현재 시스템의 기본 전달 대상 포트는 포트 137입니다.

메시지 전달을 허용하고 대상 주소를 지정하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip helper-address *address*	UDP는 Broadcast 메시지를 허용. 대상주소를 지정합니다.

전체 구성 모드에서 다음 명령을 실행하여 전달할 프로토콜을 지정하십시오.

명령어	설명
ip forward-protocol udp [*port*]	전달할 UDP 프로토콜을 지정하십시오.

19.1.3.6 IP 주소 지정 및 유지

네트워크를 탐지하고 유지 관리하려면 다음 작업을 수행하십시오.

1. 캐시와 기록 과 데이터베이스 지우기

캐시, 목록 또는 데이터베이스의 모든 내용을 지울 수 있습니다. 일부 콘텐츠가 효과적이지 않다고 생각하면 콘텐츠를 지울 수 있습니다.

관리 모드에서 다음 명령을 실행하여 캐시, 목록 및 데이터베이스를 지우십시오.

명령어	**설명**
clear arp-cache	IP와 ARP의 캐시를 제거합니다.

2. 시스템 및 네트워크에 대한 통계 데이터 표시
 시스템은 IP 라우팅 테이블, 캐시 및 데이터베이스와 같은 지정된 통계 데이터를 표시 할 수 있습니다. 이러한 모든 정보는 체계적인 자원의 사용법을 알고 네트워크 문제를 해결하는 데 도움이 됩니다. 시스템은 메시지가 네트워크에서 실행될 때 포트가 도달 할 수 있는 경로와 메시지가 걸리는 경로를 표시 할 수도 있습니다.

모든 관련 작업은 다음과 같은 표에 나열 되어있습니다. 사용법에 대해서는 "IP 주소 명령 지정"장을 참조하십시오.

관리자 모드에서 다음 명령을 실행하십시오.:

명령어	**설명**
show arp	ARP table의 내용을 나타냅니다.
show hosts	Hostname - IP매핑에 관한 캐시테이블
show ip interface [*type number*]	인터페이스 상태를 나타냅니다.
show ip route [*protocol*]	라우팅 테이블의 현 상태를 나타냅니다.
ping {**host | address**}	네트워크 노드에 도달상태를 나타냅니다.

19.1.4 IP 주소화 예제

다음은 Interface VLAN 11에 IP 주소가 설정되는 경우를 나타냅니다.

interface vlan 11

Ip address 202.96.2.3 255.255.255.0

19-2장 DHCP 설정

19.2.1 소개

DHCP (Dynamic Host Configuration Protocol)는 인터넷 호스트의 망 구성 매개 변수를 제공합니다. DHCP는 RFC 2131에 설명되어 있습니다. DHCP의 가장 중요한 기능은 인터페이스에 IP 주소를 배분하는 것입니다. DHCP는 IP 주소를 배포하는 세 가지 방법을 지원합니다.

- 자동 분배

  DHCP 서버는 영구 IP 주소를 클라이언트에 자동으로 배포합니다..

- 동적 배포

  DHCP 서버는 클라이언트가 특정 기간 동안 사용하기 위해 또는 클라이언트가 사용하지 않을 때까지 IP 주소를 분배합니다.

- 수동 배포

  DHCP 서버의 관리자는 IP 주소를 수동으로 지정하고 DHCP 프로토콜을 통해이를 클라이언트에 보냅니다

19.2.1.1 DHCP 적용

DHCP에는 여러 종류의 응용프로그램이 있는데, 다음과 같은 경우 사용가능 합니다.

DHCP 클라이언트를 구성하여 IP 주소, 네트워크 세그먼트 및 관련 소스 (관련 게이트웨이 등)를 이더넷 인터페이스에 배포 할 수 있습니다. DHCP에 액세스 할 수 있는 스위치가 여러 호스트를 연결하면 스위치는 DHCP 릴레이를 통해 DHCP 서버에서 IP 주소를 가져온 다음 호스트에 주소를 배포 할 수 있습니다.

19.2.1.2 DHCP 이점

현재 소프트웨어 버전에서는 이더넷 인터페이스의 DHCP 클라이언트 또는 DHCP 클라이언트가 지원됩니다. DHCP 클라이언트를 지원하는 기능에는 다음과 같은 이점이 있습니다.

- 구성 시간 단축
- 구성 오류 감소
- DHCP 서버를 통해 일부 장치포트의 IP 주소 제어

19.2.1.3 DHCP 용어

DHCP는 서버와 클라이언트 기반으로 하며 각각은 실행 조건이 존재합니다.

- DHCP-서버

  IP 주소 및 임대시간과 같은 DHCP 관련 소스를 배포하고 재생을 합니다.

- DHCP-클라이언트

  IP 주소 정보와 같은 로컬 시스템의 장치에 대한 정보를 DHCP 서버에서 얻는데, 임대 시간은 DHCP 동적 분배의 절차에 나타나는 개념이다.

- 임대 시간 - 분배 이후 IP 주소의 유효 기간.

  유효 기간이 끝나면 IP 주소는 DHCP 서버에 의해 재생됩니다. IP 주소를 계속 사용하려면 DHCP 클라이언트가 IP 주소를 다시 적용해야 합니다.

19.2.2 DHCP 클라이언트 구성

19.2.2.1 DHCP 클라이언트 구성 업무

- IP 주소 배정
- DHCP 서버의 주소 지정
- DHCP 매개변수 구성
- DHCP 모니터링

1. IP 주소 배정

VLAN 인터페이스에서 다음 명령을 실행하여 인터페이스에 대한 DHCP 프로토콜을 통해 IP 주소를 얻습니다.

명령어	설명
ip address dhcp	DHCP 프로토콜을 지정하여 이더넷 인터페이스의 IP 주소를 구성합니다.

2. DHCP서버에 주소를 지정

일부 DHCP 서버의 주소를 알고있는 경우 스위치에서 이러한 DHCP 서버의 주소를 지정하여 프로토콜 상호 작용 시간을 줄일 수 있습니다. 전역 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
ip dhcp-server *ip-address*	DHC서버의 IP주소를 지정합니다.

이 명령어는 IP 주소 입력을 위해 선택적인 작업입니다.

3. DHCP 매개변수 구성

요구 사항에 따라 DHCP 프로토콜이 상호 작용의 매개 변수를 조정할 수 있습니다. 전역 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
ip dhcp client minlease *seconds*	최소 임대 시간 설정입니다.
ip dhcp client retransmit *count*	프로토콜메시지의 재전송시간 설정
ip dhcp client select *seconds*	간격을 선택하여 지정하세요.

이 명령은 IP 주소를 얻기 위한 조작을 수행 할 때 선택적인 작업입니다.

4. DHCP 모니터링

스위치에서 찾은 DHCP 서버에 대한 정보를 확인하려면 관리 모드에서 다음 명령을 실행하십시오.

명령어	설명
show dhcp server	라우팅 스위치가 아는 DHCP 서버 정보를 표시합니다.

관리모드에서 명령어를 실행하여 라우팅 스위치에 사용중인 IP주소를 확인합니다..

명령어	설명
show dhcp lease	라우팅 스위치에서 현 사용중인 IP주소 리소스 및 정보를 표시.

DHCP 프로토콜을 사용하여 이더넷 인터페이스의 IP 주소를 분배하는 경우
"show interface"를 실행하여 이더넷 인터페이스에 필요한 IP 주소를 성공적으로 얻었는지 확인할 수 있습니다.

19.2.2.2 DHCP 클라이언트 구성 예시

1. IP주소를 받는 경우

The following example shows Ethernet1/1 obtains an IP address through DHCP.

!

interface vlan 11

ip address dhcp

19.2.3 DHCP 서버 설정

19.2.3.1 DHCP 서버 구성 내용

DHCP 서버 사용

DHCP 서버 비활성화

ICMP 감지 매개 변수 구성

데이터베이스 저장 영역 매개 변수 구성

DHCP 서버의 주소 풀 구성

DHCP 서버의 주소 풀에 대한 매개 변수 구성

DHCP 서버 모니터링

DHCP 서버 정보 지우기

19.2.3.2 DHCP 서버 구성

1. DHCP 서버 사용

DHCP 서버를 활성화하고 IP 주소와 같은 매개 변수를 배포하려면
DHCP 클라이언트가 전역 구성 모드에서 다음 명령을 실행합니다 (DHCP 서버는 연속적인 작업도 지원합니다. 일반 DHCP 서버가 배포 할 수 없는 주소의 경우에는 ip helper-address가 구성된 포트는 DHCP 요청을 전달하는 것입니다).

명령어	설명
ip dhcpd enable	DHCP 서버 사용

2. DHCP 서버 비활성화

다음은 DHCP 서버를 사용 가능하도록 하고 DHCP 클라이언트에 대한 IP주소 매개 변수와 같은 변수를 중지하려면 다음과 같은 명령어를 입력하십시오.

명령어	설명
no ip dhcpd enable	DHCP서버 비활성화

3. ICMP 감지 매개 변수 구성

서버가 전송 될 때 보낼 ICMP 메시지의 매개 변수를 조정할 수 있습니다

주소 검색을 수행합니다. 전역 구성 모드에서 다음 명령을 실행하십시오.

보낼 ICMP 메시지 수를 구성하려면 다음을 수행하십시오.

명령어	설명
ip dhcpd ping packets *pkgs*	ICMP 메시지의 수로 주소 검색의 시간을 지정하십시오.

전역 구성모드에서 명령을 실행하여 ICMP메시지 응답시간 초과시간을 구성합니다.

명령어	설명
ip dhcpd ping timeout *timeout*	ICMP 메시지 응답의 시간 초과 시간을 지정하십시오.

4. 데이터베이스 저장 영역 매개 변수 구성

주소 분배 정보가 에이전트 데이터베이스에 저장 될 간격을 구성하려면
전역 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip dhcpd write-time *time*	주소 분포 정보가 에이전트 D에 저장되는 간격을 지정하십시오.

5. DHCP 서버의 주소 풀 구성

전역 구성 모드에서 다음을 실행하여 DHCP에 주소풀을 추가합니다.

명령어	설명
ip dhcpd pool *name*	DHCP 서버의 주소풀을 추가하고 구성모드를 입력하십시오.

6. DHCP 서버의 주소 풀에 대한 매개 변수 구성

주소 풀 구성모드에서 명령어로 주소 풀의 망 주소를 구성합니다.

명령어	설명
network *ip-addr netsubnet*	자동 분류에 사용된 주소 풀의 망주소를 구성하십시오.

자동 분류에 사용되는 주소 범위를 구성하는 경우 다음 명령을 실행하세요.

명령어	설명
range *low-addr high-addr*	자동 분배에 사용되는 주소범위를 구성하십시오

다음 명령어는 클라이언트에 배포되는 기본경로를 구성합니다.

명령어	설명
default-router *ip-addr …*	기본 경로를 구성하십시오. 클라이언트에게 배포됩니다.

다음 명령어는 클라이언트에 배포되는 DNS서버 주소를 구성합니다.

명령어	설명
dns-server *ip-addr …*	DNS서버 주소를 구성합니다.

다음 명령어는 클라이언트에 배포되는 도메인을 구성합니다.

명령어	설명
domain-name *name*	Client에 분배되는 도메인을 구성합니다.

다음 명령어는 클라이언트에 배포되는 주소 임대시간을 구성합니다.

명령어	설명
lease {*days* [*hours*][*minutes*] | *infinite* }	Client에 분배하는 주소 임대 시간을 구성합니다.

다음 명령어는 클라이언트에서 배포되는 Netbios 서버주소를 구성합니다.

명령어	설명
netbios-name-server *ip-addr…*	Client에 부류된 Netbios서버를 구성합니다

다음 명령어는 MAC 주소가 하드웨어인 호스트에 IP 주소를 배포하기 위해 거부하려면 다음 명령을 실행합니다.

명령어	설명
hw-access deny hardware-address	하드웨어 주소로 인한 IP주소 배포를 거부합니다.

7. DHCP 서버 모니터링

관리 모드에서 다음 명령을 실행하여 DHCP 서버에 대한 현재 주소 배포 정보를 확인하십시오.

명령어	설명
show ip dhcpd binding	현 사태 주소 분포 표시합니다.

관리 모드에서 다음 명령을 실행하여 DHCP 서버에 대한 현재 메시지 통계 정보를 확인하십시오.

명령어	설명
show ip dhcpd statistic	DHCP 서버에 통계정보를 삭제합니다

8. DHCP 서버 정보 지우기

다음 명령을 실행하여 DHCP 서버에 대한 현재 주소 배포 정보를 삭제하십시오.

명령어	설명
clear ip dhcpd binding {*ip-addr*|*}	지정된 주소분배정보를 삭제합니다.

다음 명령을 실행하여 DHCP 서버에 대한 현재 메시지 통계 정보를 삭제하십시오.

명령어	설명
clear ip dhcpd statistic	현재 DHCP 서버 메시지 통계정보를 삭제합니다.

19.2.3.3 DHCP 서버 구성 예시

다음 예시문에 ICMP 탐지 패킷의 시간에 초과 시간은 200ms로 설정됩니다. 주소 풀 1이 구성되고 DHCP 서버가 사용됩니다.

```
ip dhcpd ping timeout 2
ip dhcpd pool 1
 network 192.168.20.0 255.255.255.0
 range 192.168.20.211 192.168.20.215
 domain-name my315
 default-router 192.168.20.1
 dns-server 192.168.1.3 61.2.2.10
 netbios-name-server 192.168.20.1
 lease 1 12 0
ip dhcpd enable
```

19-3장 IP 서비스 구성

IP서비스를 선택적으로 구성하는 방법을 설명합니다. 보다 더 자세한 내용은 "IP 서비스 명령어" 절을 참조하십시오.

19.3.1 IP 서비스 구성하기

IP 서비스를 선택적으로 구성하는 방법은 다음과 같습니다.:

- IP 연결관리하기
- 매개 변수에 대한 기능 구성하기
- 기본 게이트웨이 구성하기
- IP 망 탐지하고 유지하기

위의 작업이 필수는 아니지만 요구 사항에 따라 작업을 수행 할 수 있습니다.

19.3.1.1 IP 연결 관리하기

IP 프로토콜은 IP 연결을 제어하고 관리하는 일련의 서비스를 제공합니다. 이러한 서비스의 대부분은 ICMP에 의해 제공됩니다. 라우팅 스위치 또는 액세스 서버가 IP 메시지 헤더에서 오류를 감지하면 ICMP 메시지가 호스트 또는 다른 라우팅 스위치로 전송됩니다. ICMP는 RFC 792에서 정의됩니다.

다른 IP 연결 조건에 따라 다음과 같은 작업을 수행하십시오.

1. ICMP 연결 해제 메시지 보내기

시스템이 메시지를 수신하여 경로 없음과 같은 메시지를 대상으로 보낼 수 없는 경우, 시스템은 소스 호스트에 ICMP연결 해제 메시지를 보냅니다. 시스템 기능은 기본적으로 활성화되어 있습니다.

이 기능이 비활성화된 경우 인터페이스 구성 모드에서 다음 명령을 실행하여 해당 기능을 사용하도록 설정할 수 있습니다.

명령어	설명
ip unreachables	ICMP연결 해제 메시지를 전송하려면 이 기능을 사용하도록 설정합니다.

2. ICMP 경로 수정 메시지 보내기

가끔 호스트가 이상한 경로를 선택합니다. 라우팅 스위치의 경로가 호스트에서 메시지를 받으면 라우팅 테이블을 확인한 다음 메시지를 수신메시지-인터페이스를 통해 다른 라우팅 스위치에 전달합니다

호스트와 같은 네트워크 세그먼트인 경우 입니다. 이 경우 라우팅 스위치는 대상과 함께 메시지를 직접 다른 라우팅 스위치에 보내는 방법을 소스 호스트에 알려주고 리디렉션 메시지에는 소스 호스트가 원래 경로를 삭제하고 메시지에 표시된 보다 정확한 경로를 사용해야 합니다. 대부분의 호스트 운영 체제는 라우팅 테이블에 호스트 경로를 추가합니다. 그러나 라우팅 스위치는 라우팅 프로토콜을 통해 얻은 정보를 더 신뢰할 수 있습니다. 따라서 라우팅 스위치의 정보에 따라 호스트 경로를 추가하지 않습니다.

이 기능은 기본적으로 사용하도록 설정되어 있습니다.

HSRP(Hot Standby Routing Protocol) =상시 대기 라우터 프로토콜

HSRP가 인터페이스에 구성된 경우 자동으로 비활성화됩니다. 하지만 이기능은 자동으로 실행되지 않으며 프로토콜이 임의로 취소 된 경우에도 자동으로 활성화되지 않습니다.

이 기능을 사용하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip redirects	ICMP 방향 수정 메시지 전송 허용

3. ICMP mask 응답 메시지 전송

가끔 호스트는 네트워크 마스크를 알아야합니다. 정보를 얻기 위해 호스트는 ICMP 마스크 요청 메시지를 보낼 수 있습니다. 라우팅 스위치가 호스트의 마스크를 확인할 수 있으면 ICMP 마스크 응답 메시지로 응답합니다. 기본적으로 라우팅 스위치는 ICMP 마스크 응답 메시지를 보낼 수 있습니다.

ICMP mask 요청 메시지를 보내려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip mask-reply	ICMP mask 응답메시지를 보냅니다.

4. 지원경로 MTU 탐지

시스템은 RFC 1191에 정의 된 IP 경로의 MTU 감지 장치를 지원합니다. IP 경로 MTU 감지 장치를 사용하면 호스트가 서로 다른 경로의 최대 전송 단위 (MTU)를 자동으로 찾고 조정할 수 있습니다. 빈번히 라우팅 스위치는 수신 된 IP 메시지 길이가 메시지 전달 인터페이스에 설정된 MTU보다 큰 경우를 감지합니다.
IP 메시지는 분할화 되어야 하지만 IP 메시지의 "세분화 되지 않은"비트는 재설정 됩니다. 따라서 메시지는 분할 할 수 없습니다. 메시지를 삭제해야 합니다. 이 경우 라우팅 스위치는 ICMP 메시지를 전송하여 실패한 전달 이유 및 전달 인터페이스의 MTU를 기존 호스트에 알립니다. 그런 다음 기존 호스트는 대상에 보내는 메시지의 길이를 줄여 경로의 최소 MTU를 조정합니다.

경로의 연결이 끊어지면 메시지는 다른 선택하는 것입니다. MTU 최소값은 원래 경로와 다를 수 있습니다. 그런 다음 라우팅 스위치는 소스 호스트에 새 경로의 MTU를 알립니다. IP 메시지는 가능한 한 경로의 최소 MTU로 패키징 되어야 합니다. 이러한 방식으로, 분할이 진행되고 보다 적은 메시지가 보내게 되어 통신 효율이 향상됩니다. 관련 호스트는 IP 경로MTU 감지를 지원해야합니다. 그런 다음 라우팅 스위치에 의해 통보 된 MTU 값에 따라 IP 메시지의 길이를 조정하여 전달 과정에서 분할을 방지 할 수 있습니다.

관련 호스트는 IP 경로 MTU 감지를 지원해야합니다. 그런 다음 라우팅 스위치에 의해 통보 된 MTU 값에 따라 IP 메시지의 길이를 조정하여 전달 과정에서 분할을 방지 할 수 있습니다.

5. MTU IP 설정

Maximum Transmission Unit (MTU)는IP메시지로 전송이 가능한 최대 길이를 말합니다. IP 메시지 길이가 MTU를 초과하는 경우는 라우팅 스위치에서 분할합니다. 인터페이스의 MTU 값을 변경하면 IP MTU 값에 영향을 줍니다. IP MTU가 MTU와 같으면 IP MTU는 자동으로 MTU가 변경 될 때 새로운 MTU와 동일하게 조정됩니다. 그러나 IP MTU의 변경은 MTU에 영향을 미치지 않습니다. IP MTU는 현재 인터페이스에 구성된 MTU보다 클 수 없습니다. 동일한 물리적 미디어를 연결하는 모든 장치가 동일한 MTU 프로토콜을 가져야하는 경우에만 정상적인 통신을 생성 할 수 있습니다.

특정 인터페이스에서 IP MTU를 설정하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
ip mtu *bytes*	인터페이스의 IP MTU를 설정하십시오.

6. IP 소스 경로 인증

라우팅 스위치는 모든 메시지의 IP 헤더를 확인합니다. RFC 791에 정의 된 IP Header 옵션을 지원합니다. 정확한 소스 경로, 순항 소스 경로, 시간 스탬프와 경로에 대한 기록 그리고 스위치가 옵션을 잘못 선택했다면 ICMP 매개 변수문제에 대한 메시지를 소스 호스트에 보내고 메시지를 삭제합니다. 소스경로에서 문제가 발생하면 라우팅 스위치는 소스 호스트로 ICMP 연결 불가 (소스 경로에 실패를 인지하는 글)을 보냅니다. IP는 소스 호스트가 메시지에 대한 IP 네트워크의 경로를 지정할 수 있게 합니다. 지정된 경로가 소스 경로로 호출됩니다. IP 헤더 옵션에서 소스 경로를 선택하여 지정할 수 있습니다. 라우팅 스위치는 옵션에 따라 IP 메시지를 전달하거나 보안 요구 사항에 따라 메시지를 삭제해야 합니다. 그런 다음 라우팅 스위치는 ICMP 연결할 수 없는 메시지를 소스 호스트로 보냅니다. 라우팅 스위치는 기본적으로 소스 경로를 지원합니다.

IP 원본 경로가 비활성화 된 경우 전역 구성 모드에서 다음 명령을 실행하여 IP 원본 경로를 인증합니다.

명령어	설명
ip source-route	IP 소스 경로 권한 부여

7. IP 의 빠른 교섭 허용

IP 빠른 교섭은 캐시를 사용하여 IP 메시지를 전달합니다. 스위치가 특정 대상으로 메시지를 전달하기 전에 시스템은 라우팅 테이블을 확인한 다음 경로에 따라 메시지를 전달합니다. 선택한 경로는 시스템 소프트웨어의 라우팅 캐시에 저장됩니다. 후자의 메시지가 동일한 호스트로 보내지면 스위치는 라우팅 캐시에 저장된 경로에 따라 후자의 메시지를 전달합니다. 메시지가 전달 될 때마다 해당 경로 항목의 적중 횟수 값이 1 씩 증가합니

다. 적중 횟수가 설정 값과 같으면 소프트웨어 라우팅 캐시가 하드웨어 라우팅 캐시에 저장됩니다. 동일한 호스트에 대한 다음 메시지는 하드웨어에 의해 직접 전달됩니다. 일정 시간 동안 캐시를 사용하지 않으면 캐시가 삭제됩니다. 소프트웨어 / 하드웨어 캐시 항목이 상한 값에 도달하면 새 대상 호스트는 더 이상 캐시에 저장되지 않습니다. 빠른 교섭을 허용하거나 금지하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오:

명령어	**설명**
ip route-cache	빠른 교섭을 허용합니다
no ip route-cache	빠른 교섭을 허용하지 않습니다.

소프트웨어 캐시 항목이 하드웨어 캐시에 저장 될 때 필요한 적중 횟수를 구성하려면 전역 구성에서 다음 명령을 실행하십시오.

명령어	설명
ip route-cache hit-numbers *hitnumber*	소프트웨어 캐시에서 라우팅 항목의 적중 횟수가 hitnumber의 값에 도달하면 소프트웨어 캐시의 라우팅 항목이 하드웨어 캐시에 라우팅 항목으로 저장됩니다.

8. 같은 인터페이스에서 빠른 IP 교섭 지원

스위치가 수신 인터페이스를 송신 인터페이스와 동일하게 함으로써 빠른 IP 교섭을 지원할 수 있습니다. 일반적으로 라우터의 재설정 기능과 충돌하기 때문에 이 기능을 사용하지 않는 것이 좋습니다.

동일한 인터페이스에서 IP 라우팅 캐시를 허용하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip route-cache *same-interface*	같은 수신/전송 인터페이스를 가진 IP 메시지를 라우팅 캐시에 저장합니다.

19.3.1.2 매개 변수 구성 성능

1. TCP 연결 대기 시간 설정

라우팅 스위치는 TCP 연결을 수행 할 때 대기 시간 동안 TCP 연결이 만들어지지 않으면 TCP 연결이 실패한 것으로 간주합니다. 그런 다음 라우팅 스위치는 실패한 TCP 연결의 상위 레벨 프로그램에 알립니다. TCP 연결 대기 시간을 설정할 수 있습니다. 시스템의 기본값은 75 초입니다. 이전 구성은 스위치가 전달하는 TCP 연결에 영향을 미치지 않습니다. 스위치 자체에서 생성 된 TCP 연결에만 영향을 줍니다.

글로벌 구성 모드에서 다음 명령을 실행하여 TCP 연결 대기 시간을 설정하십시오.:

명령어	설명
ip tcp synwait-time *seconds*	TCP 연결 대기 시간을 설정하십시오.

2. TCP windows의 크기 설정하기

기본 크기는 2000 바이트입니다. 전역 구성 모드에서 다음 명령을 실행하여 기본 TCP windows 크기를 변경하십시오.

명령어	설명
ip tcp window-size *bytes*	TCP 창의 크기를 설정하십시오.

19.3.1.3 IP 네트워크 유지 및 탐지

1. 캐시와 데이터베이스 목록을 제거합니다.

캐시, 목록 또는 데이터베이스의 모든 내용을 지울 수 있습니다. 캐시, 목록 또는 데이터베이스의 잘못된 데이터를 지울 필요가 있습니다.

잘못된 데이터를 지우려면 다음 명령을 실행하십시오.

명령어	설명
clear tcp statistics	TCP 통계 데이터를 지웁니다.

2. TCP 연결 해제

TCP 연결을 끊으려면 다음 명령을 실행하십시오.:

명령어	설명
clear tcp {**local** host-name **remote** host-name | **tcb** address}	지정된 TCP연결을 지웁니다. TCB는 TCP 제어 블록을 나타냅니다.

3. 시스템 및 네트워크에 대한 통계 데이터 표시

시스템은 캐시, 목록 및 데이터베이스에 내용을 표시 할 수 있습니다. 이러한 통계 데이터는 체계적인 출처의 사용법을 파악하고 네트워크 문제를 해결하는 데 도움이 됩니다.

다음 명령을 실행하십시오. 자세한 내용은 "IP 명령 서비스"를 참조하십시오.

명령어	설명
show ip access-lists *name*	모든 엑세스 목록의 내용을 표시합니다
show ip cache [mask] [type number]	IP 메시지교환 된 캐시를 표시합니다.

show ip sockets	스위치에 소켓 정보를 표시합니다.
show ip traffic	IP프로토콜에 대한 통계 데이터를 표시합니다
show tcp	모든 TCP 연결 상태에 대한 정보를 표시합니다.
show tcp brief	TCP에 대한 정보를 간략히 나타냅니다.
show tcp statistics	TCP 통계 데이터를 표시합니다.
show tcp tcb	지정 TCP 연결상태 정보를 표시합니다.

4. 디버깅 정보 표시.

네트워크에서 문제가 발생하면 디버그를 실행하여 디버깅 정보를 표시 할 수 있습니다.

다음 명령을 실행하십시오. 자세한 내용은 "IP 명령 서비스"를 참조하십시오.

명령어	설명
debug arp	ARP에 대한 상호작용 정보를 표시합니다
debug ip icmp	ICMP에 대한 상호작용 정보를 표시합니다.
debug ip raw	수신/발신 된 IP 메시지에 대한 정보를 표시합니다.
debug ip packet	IP에 대한 상호 작용 정보를 표시합니다.
debug ip tcp	TCP에 대한 상호 작용 정보를 표시합니다.
debug ip udp	UDP에 대한 상호 작용 정보를 표시합니다.

19.3.2 Access List 구성하기

19.3.2.1 IP 메시지 필터링

필터링 메시지는 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 방법은 특정 사용자 또는 장치를 통해 네트워크 전송 및 네트워크 사용을 제한 할 수 있습니다. 교차 지정 인터페이스를 통해 패킷을 유효하거나 무효로 만들기 위해 라우팅 스위치는 Access-List을 제공합니다. Access-List는 다음 모드에서 사용할 수 있습니다.

인터페이스에서 패킷 전송 제어

가상 터미널 회선 접근 제어

경로 업데이트 내용 제한

이 절에서는 IP 액세스 목록을 만드는 방법과 IP Access-list을 사용하는 방법에 대해 설명합니다.

IP Access-list은 IP 주소를 적용하기위한 허가 / 금지 조건의 규칙적인 집합입니다. 스위치의 ROS 소프트웨어는 규정에 따라 Access-List에서 주소를 하나씩 테스트합니다. 첫 번째 일치는 ROS가 주소를 수락 또는 거절하는지 여부를 결정합니다. 첫 번째 경기가 끝나면 ROS 소프트웨어가 경기 규칙을 종료합니다. 따라서 조건의 순서가 중요합니다. 규정이 일치하지 않으면 주소가 거부됩니다.

다음 항목에 따라 Access-list를 사용하십시오.

(1) Access list 의 이름과 조건을 지정하여 작성합니다.

(2) Access list 를 인터페이스에 적용합니다.

19.3.2.2 표준 및 확장 가능 IP 액세스 목록 만들기

문자열을 사용하여 IP 액세스 목록을 만듭니다.

Note:

표준 Access-list 과 확장 Access-list에는 같은 이름을 사용할 수 없습니다.

전역 구성 모드에서 다음 명령을 실행하여 표준 Access-list만듭니다.

명령어	설명
ip access-list standard *name*	Access-List의 이름을 정의합니다.
deny {*source* *[source-mask]* | **any**}[**log**] or **permit** {*source* *[source-mask]* | **any**}[**log**]	하나 이상의 허용 및 거부 조건을 지정하고 패킷의 승인 여부를 결정합니다.
Exit	Access-List에서 로그아웃 합니다.

전역 구성 모드에서 다음 명령을 실행하여 확장 가능한 Access-List만듭니다.

명령어	설명
ip access-list extended *name*	확장 Access-List이름을 정의합니다.

{**deny** | **permit**} *protocol source source-mask destination destination-mask*	하나 이상의 허용 및 거부 조건을 지정하고 패킷 승인여부를 결정합니다. 서비스약관(TOS)는 서비스유형을 의미합니다.
Exit	Access-List 모드에서 로그아웃 합니다

Access-List을 만든 후에는 나중에 추가되는 부분을 목록 끝에 넣을 수 있습니다. 즉, 지정된 Access-List 명령 줄을 추가 할 수 없습니다. 그러나 액세스 허용 목록에서 항목을 삭제하려면 허용 안 함과 거부 안 함을 실행할 수 있습니다.

Note:

Access-List를 만들면 Access-List의 끝 부분에 기본적으로 암시적 거부 문장이 포함됩니다. 마스크가 상대 IP 호스트 주소 Access-list에서 생략되면 255.255.255.255가 마스크로 간주됩니다.

Access-List를 만든 후에는 경로 또는 인터페이스에 액세스 목록을 적용해야 합니다. 자세한 내용은 3.2.3 "인터페이스에 Access-List적용" 장을 참조하십시오

19.3.2.3 인터페이스에 Access-list 적용

Access-List을 만든 후에 입력 인터페이스 와 출력 인터페이스를 포함하여 하나 이상의 인터페이스에 적용 할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip access-group *name* **{in | out}**	Access list를 적용합니다.

Access-list은 입력 인터페이스와 출력 인터페이스에서 사용할 수 있습니다. 입력 인터페이스의 표준 Access-List의 경우 패킷 수신 후 Access-list에 따라 패킷의 손상된 주소를 확인해야합니다. 확장형 Access-list의 경우 라우팅 스위치는 대상을 확인합니다. Access-list에서 주소를 허용하면 소프트웨어는 패킷 처리를 계속합니다. Access-list에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달 할 수 없는 메시지를 반환합니다.

외부 인터페이스의 표준 Access-list의 경우 패킷이 수신되거나 제어 인터페이스로 라우팅 된 후 소프트웨어는 Access-list에 따라 패킷의 원본 주소를 확인합니다. 확장형 Access-list의 경우 라우팅 스위치도 수신 측의 Access-List를 체크합니다. Access-list에서 주소를 허용하면 소프트웨어가 패킷을 보냅니다. Access-list에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달 할 수 없는 메시지를 반환합니다.

지정된 Access-list이 없으면 모든 패킷이 통과 할 수 있습니다.

19.3.2.4 확장 가능한 Access-list 의 예

적용된 aaa 다음 첫 번째 줄은 새 TCP가 포트 1023 다음에 대상 포트를 연결할 수 있게 합니다. 두 번째 줄은 새 TCP가 호스트 130.2.1.2의 SMTP 포트에 연결할 수 있도록 합니다.

```
ip access-list extended aaa

permit tcp any 130.2.0.0 255.255.0.0 gt 1023

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in
```

확장 가능한 액세스 목록을 적용하는 또 다른 예제가 제공됩니다. 네트워크가 인터넷에 연결된다고 가정하면 이더넷의 모든 호스트가 인터넷의 호스트와 TCP 연결을 만들 수 있습니다. 그러나 인터넷의 호스트가 메일 호스트의 SMTP 포트를 연결하지 않으면 이더넷의 호스트와 TCP 연결을 만들 수 없습니다.

연결 기간 동안 동일한 두 포트 번호가 사용됩니다. 인터넷 메일 패킷에는 대상 포트 즉 포트 25가 있습니다. 보내는 패킷에는 반대 포트 번호가 있습니다. 사실, 라우팅 스위치 뒤에 있는 보안 시스템은 항상 포트 25에서 메일을 받습니다. 들어오는 서비스와 나가는 서비스를 고유하게 제어 할 수 있는 정확한 이유입니다. Access-list은 발신 서비스 또는 수신 서비스로 구성 될 수 있습니다.

다음과 같은 경우, 이더넷은 주소가 130.20.0.0 인 B 유형 네트워크입니다. 메일 호스트의 주소는 130.20.1.2입니다. "established" 키워드는 TCP 프로토콜에만 사용됩니다. 즉, 연결이 생성됩니다. TCP 데이터에 ACK 또는 RST 숫자가 설정되어 있으면 패킷이 기존 연결에 속해 있음을 나타내는 매치가 발생합니다..

```
ip access-list aaa

permit tcp any 130.20.0.0 255.255.0.0 established

permit tcp any 130.20.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in
```

19.3.3 물리적인 포트를 기반으로 IP Access-list 구성

19.3.3.1 IP 메시지 필터링

필터링 메시지는 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 이 방법은 특정 사용자 또는 장치를 통해 네트워크 전송 및 네트워크 사용을 제한 할 수 있습니다. 교차로 지정 인터페이스를 통해 패킷을 유효하거나 무효로 만들기 위해 라우팅 스위치는 Access-List을 제공합니다. Access-List는 다음 모드에서 사용할 수 있습니다

- 인터페이스에서 패킷 전송 제어

- 가상 터미널 회선 액세스 제어

- 경로 업데이트 내용 제한

이 절에서는 IP 액세스 목록을 만드는 방법과 IP Access-list을 사용하는 방법에 대해 설명합니다.

IP Access-list은 IP 주소를 적용하기위한 허가 / 금지 조건의 규칙적인 집합입니다. 스위치의 ROS 소프트웨어는 규정에 따라 Access-List에서 주소를 하나씩 테스트합니다. 첫 번째 일치는 ROS가 주소를 수락 또는 거절하는지 여부를 결정합니다. 첫 번째 경기가 끝나면 ROS 소프트웨어가 경기 규칙을 종료합니다. 따라서 조건의 순서가 중요합니다. 규정이 일치하지 않으면 주소가 거부됩니다.

Access list의 사용은 다음과 같은 단계가 있습니다.

(1) access list의 이름과 조건을 지정하여 작성합니다.
(2) 인터페이스에 Access-list를 저장합니다.

19.3.3.2 표준 및 확장 IP Access List 생성

문자열을 사용하여 IP access list를 만듭니다.

Note:

표준 Access-list과 확장 Access-list에는 동일한 이름을 사용할 수 없습니다.

전역 구성 모드에서 다음 명령을 실행하여 표준 Access-list을 만듭니다.

명령어	설명
ip access-list standard *name*	Access-list에 이름을 적용합니다.
deny {*source* *[source-mask]* | **any**}[**log**] or **permit** {*source* *[source-mask]* | **any**}[**log**]	하나이상의 허가/거부 지정하며 조건 이전 설정은 패킷의 승인여부를 결정합니다.
Exit	구성모드에서 로그아웃 합니다.

전역 구성 모드에서 다음 명령을 실행하여 확장 가능한 Access-list를 만듭니다.

명령어	설명
ip access-list extended *name*	Access-list에 이름을 적용합니다.

{**deny** | **permit**} *protocol source source-mask destination destination-mask*	하나이상의 허가/거부 지정하며 조건 이전 설정은 패킷의 승인여부를 결정합니다. 서비스약관(TOS)는 서비스유형을 의미합니다.
Exit	구성 모드에서 로그 아웃합니다.

Access-List을 만든 후에는 나중에 추가되는 부분을 목록 끝에 넣을 수 있습니다. 즉, 지정된 Access-List 명령 줄을 추가 할 수 없습니다. 그러나 액세스 허용 목록에서 항목을 삭제하려면 허용 안 함과 거부 안 함을 실행할 수 있습니다.

Note:

Access-List을 만들면 Access-List의 끝 부분에 기본적으로 암시적 거부 문장이 포함됩니다. 마스크가 상대 IP 호스트 주소 액세스 목록에서 생략되면 255.255.255.255가 마스크로 간주됩니다.

액세스 목록을 만든 후에는 경로 또는 인터페이스에 Access-List을 적용해야 합니다. 자세한 내용은 4.2.3 " 인터페이스에 Access-List적용 " 단원을 참조하십시오.

19.3.3.3 인터페이스에 Access-List 적용

Access list를 만든 후에 입력 인터페이스와 출력 인터페이스에 적용 할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip access-group *name* **{in | out}**	Access그룹의이름을 입출력한다

Access-list는 입력 인터페이스와 출력 인터페이스에서 사용할 수 있습니다. 입력 인터페이스의 표준 액세스 목록의 경우 패킷 수신 후 Access-List에 따라 패킷의 손상된 주소를 확인해야합니다. 확장형 Access-List의 경우 라우팅 스위치는 대상을 확인합니다. Access-List에서 주소를 허용하면 소프트웨어는 패킷 처리를 계속합니다. 액세스 목록에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달 할 수 없는 메시지를 반환합니다.

외부 인터페이스의 표준 Access-list의 경우 패킷이 수신되거나 제어 인터페이스로 라우팅 된 후 소프트웨어는 액세스 목록에 따라 패킷의 원본 주소를 확인합니다. 확장형 액세스 목록의 경우 라우팅 스위치도 수신 측의 액세스리스트를 체크한다. 액세스 목록에서 주소를 허용하면 소프트웨어가 패킷을 보냅니다. 액세스 목록에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달 할 수 없는 메시지를 반환합니다.

지정된 액세스 목록이 없으면 모든 패킷이 통과 할 수 있습니다.

3 1. TCP / UDP 포트 필터링을 지원하는 포트 기반 IP Access-List

{**deny | permit**} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt }

port] }] [**precedence** *precedence*] [**tos** *tos*]

포트 범위를 정의하여 Access-List를 구성하는 경우 다음 사항에 주의하십시오.

- 출발지의 범위와 목적지 입장에서 Access-List 를 구성하기위해 포트 범위를 지정하는 방법을 사용하면 대량의 리소스가 소비되기에 일부 구성이 실패 할 수 있다. 이 경우 한쪽에서 포트 범위를 지정 하는 방식을 사용해야 하고 다른 포트에서 포트를 지정하는 방식을 사용해야합니다.
- 포트 범위 필터링을 수행하면 많은 리소스가 사용됩니다. 포트 범위 필터링을 너무 많이 사용할 경우에는 Access-list 에서 이전과 다른 프로그램을 지원할 수 없습니다.

4 TCP / UDP 포트 필터링을 지원하는 포트 기반 IP Access-List.

다음의 예제에서 첫 번째 줄은 새 TCP가 호스트130.2.1.2.의 SMTP에 연결하도록 합니다.

ip access-list extended aaa

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface f0/10

ip access-group aaa

20장. 라우팅 설정

20-1장　　RIP 구성하기

20.1.1 개요

이 섹션에서는 RIP명령을 구성하는 방법을 설명합니다. RIP명령에 대한 자세한 내용은 "네트워크 프로토콜 명령 참조"의 "RIP명령"을 참조하십시오.

라우팅 정보 프로토콜 (RIP)은 아직 일반적으로 사용되는 내부 게이트웨이 프로토콜 (IGP)이며 주로 같은 유형의 소규모 네트워크에 적용됩니다. RIP는 RFC 1058에 나오는 고전적인 거리 벡터 라우팅 프로토콜입니다.

RIP는 UDP 패킷의 Broadcast를 사용하여 라우팅 정보를 교환합니다. 라우팅 스위치에서 라우팅 정보의 업데이트는 30초마다 수행됩니다. 스위치가 180 초 내에 인접 스위치의 업데이트 정보를 받지 못하면 스위치는 인접 스위치의 라우팅 테이블에 있는 경로를 "사용할 수 없음"으로 표시합니다. 업데이트 정보가 다음 120 초 내에 여전히 수신되지 않으면 스위치는 라우팅 테이블에서 경로를 삭제합니다.

RIP는 홉의 개수를 사용하여 여러 경로의 가중치의 균형을 조정합니다. 홉 수는 패킷이 정보 소스 및 정보 싱크에서 가져 오는 스위치 수입니다. 직접 연결된 네트워크의 라우팅 가중치는 0입니다. 도달 할 수 없는 네트워크의 라우팅 가중치는 16입니다. RIP를 사용하는 라우팅 가중치의 범위가 작기 때문에 대규모 네트워크에는 적합하지 않습니다.

스위치에 기본 경로가 있는 경우 RIP는 네트워크에 대한 경로를 선언합니다 0.0.0.0. 사실 네트워크 0.0.0.0은 존재하지 않습니다. 기본 경로를 구현하기 위해 RIP에만 사용됩니다

RIP는 라우팅 업데이트 정보를 지정된 네트워크 인터페이스로 보냅니다. 인터페이스가 상주하는 네트워크가 지정되지 않은 경우 RIP 업데이트 정보에서 네트워크를 선언 할 수 없습니다.

RIPv2는 일반 텍스트, MD5 인증, 라우팅 요약, CIDR 및 VLSM을 지원합니다.

20.1.2　RIP 작업 목록 구성

RIP를 구성하려면 먼저 다음 작업을 완료해야 합니다. RIP를 활성화하는 작업은 필수이며 다른 작업은 선택 사항입니다.

- RIP을 시작합니다.
- RIP 경로가 단일 프로그램 broadcast를 업데이트하도록 허용한다
- 라우팅 가중치에 Offset 적용
- 타이머 조정하기
- RIP 버전 번호 지정하기
- RIP 인증 활성화
- 라우팅 요약 금지하기
- 소스주소의 인증 금지하기
- 최대 경로 수 구성
- Split-Horizon 활성화 또는 금지
- RIP 모니터링 및 유지보수

20.1.3 RIP 설정작업

20.1.3.1 RIP 시작하기

전역 구성 모드에서 다음 명령을 실행하여 RIP를 활성화합니다.

명령어	설명
router rip	RIP 라우팅 프로세스를 활성화하고 스위치 구성 모드를 시작합니다.
network *network-number* <network-mask>	RIP 라우팅 프로세스와 관련된 네트워크 번호를 지정합니다.

20.1.3.2 단일 프로그램 broadcast를 업데이트 하도록 RIP라우팅을 허용하기

일반적으로 RIP는 Broadcast protocol입니다. Broadcast 아닌 경우 네트워크에 도달하기 위해 RIP 라우팅 업데이트를 활성화하려면 스위치가 라우팅 정보를 교환 할 수 있도록 스위치를 구성해야 합니다.

라우팅 정보 교환을 사용하려면 스위치 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
neighbor *ip-address*	인접 스위치를 정의하여 알려진 스위치와 라우팅 정보를 교환합니다..

또한 **“ip rip passive”** 실행하여 포트를 지정하여 업데이트를 제한 할 수 있습니다..

20.1.3.3 라우팅 가중치에 Offset 적용

오프셋 목록은 나가는 경로 또는 RIP에서 습득 한 들어오는 경로에 대한 오프셋을 추가하는 데 사용됩니다. 라우팅 가중치를 추가하는 방법을 제공합니다. 또한 Access-list 나 인터페이스를 사용하여 Offset List을 제한 할 수 있습니다. 스위치 구성 모드에서 다음 명령을 실행하여 라우팅 가중치를 추가하십시오.

명령어	설명
offset {[interface-type number]|* } {**in**|**out**} access-list-name offset	라우팅 가중치에 offset을 추가합니다.

20.1.3.4 타이머 조정하기

라우팅 프로토콜은 몇 가지 타이머를 사용하여 경로 업데이트 정보를 전송하는 빈도, 경로가 비효율적으로 는 데 필요한 시간 및 기타 매개 변수를 판단합니다. 이러한 것들로 인하여 타이머를 조정하여 라우팅 프로토콜의 성능을 향상시킬 수 있습니다. 또한 라우팅 프로토콜을 조정하여 모든 IP 라우팅 연산의 수렴 시간을 단축하고 신속하게 중복 스위치를 백업하며 빠른 복구의 경우 최소 고장 시간을 보장 할 수 있습니다. 구성 모드에서 다음 명령을 실행하여 타이머를 조정하십시오.

명령어	설명
timers holddown *value*	라우팅 테이블에서 경로가 삭제되는 데 필요한 시간을 나타냅니다.
timers expire *value*	이는 경로가 비효율적으로 선언되기 위해 필요한 간격을 의미합니다.
timers update *value*	라우팅 업데이트 정보의 전송빈도를 의미합니다.

20.1.3.5 RIP 버전 번호 지정하기

스위치의 RIP-2는 인증, PIN 관리, 라우팅 요약, CIDR 및 VLSM을 지원합니다. 기본적으로 스위치는 RIP-1 및 RIP-2를 수신하지만 스위치는 RIP-1 만 보냅니다. 구성을 통해 스위치는 패킷 RIP-1 또는 패킷 RIP-2 만 수신하고 보낼 수 있습니다.
이전 요구 사항을 충족 시키려면 스위치 구성 모드에서 다음 명령을 실행하십시오.:

명령어	설명
version {1 | 2}	스위치는 RIP-1 또는 RIP-2 만 송수신합니다.

이전 작업은 RIP의 기본 동작을 제어합니다. 특정 인터페이스를 구성하여 기본 동작을 변경할 수도 있습니다.

다음 명령을 실행하여 RIP-1 또는 RIP-2를 전송여부를 제어합니다.

명령어	설명
ip rip send version 1	구성된 인터페이스는 RIP-1 만 보냅니다.
ip rip send version 2	구성된 인터페이스는 RIP-2 만 보냅니다.
ip rip send version compatibility	RIP-2 업데이트 메시지를 broadcast 형태로 보냅니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 패킷 RIP-1 또는 패킷 RIP-2를 수신할지 여부를 인터페이스를 제어합니다.

명령어	설명
ip rip receive version 1	구성된 인터페이스는 RIP-1 만 수신합니다.
ip rip receive version 2	구성된 인터페이스는 RIP-2 만 수신합니다.
ip rip receive version 1 2	구성된 인터페이스는 RIP-1 과 RIP-2를 수신합니다.

20.1.3.6 RIP 인증 활성화

RIP-1은 인증을 지원하지 않습니다. RIP-2 패킷을 수신하고 보내려면 인터페이스에서 RIP 인증을 활성화 할 수 있습니다.

활성화 된 인터페이스에는 일반 텍스트 인증과 MD5 인증의 두 가지 인증 모드가 제공됩니다. 각 RIP-2 패킷은 기본적으로 일반 인증을 사용합니다.

노트:

보안을 위해 암호화되지 않은 인증 PIN이 각 RIP-2 패킷으로 전송되므로 RIP 패킷에서 인증을 사용하지 마십시오. 보안 문제없이 일반 인증을 사용할 수 있습니다.

VLAN 구성 모드에서 다음 명령을 실행하여 RIP 일반 텍스트 인증을 구성합니다.

명령어	설명
ip rip authentication simple	일반 인증을 사용하도록 인터페이스를 구성합니다.
ip rip password [string]	일반 인증의 PIN을 구성합니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 RIP의 MD5 인증을 구성합니다.

명령어	설명
ip rip authentication message-digest	MD5 인증을 사용하여 구성합니다.
ip rip message-digest-key [*key-ID*] **md5** [*key*]	MD5 인증의 PIN 및 ID를 구성합니다

20.1.3.7 라우팅 요약 제한

RIP-2는 기본적으로 자동 라우팅 요약을 지원합니다. RIP-2 경로는 다른 네트워크의 경계를 지날 때 수집됩니다. RIP-1 자동 수집 기능은 능동적인 상태입니다.

분리 된 서브넷이 있는 경우 라우팅 요약 기능이 서브넷을 선언하지 라우팅 요약 기능이 비활성화 된 경우 스위치는 다른 네트워크의 경계를 통과 할 때 Subnet 및 호스트의 라우팅 정보를 전송합니다. 스위치 구성 모드에서 다음 명령을 실행하여 자동 라우팅 요약 기능을 비활성화하십시오.

명령어	설명
no auto-summary	자동 경로요약 기능을 비활성화합니다.

20.1.3.8 소스 IP 주소의 인증 금지

기본적으로 스위치는 RIP 라우팅 업데이트 정보에서 소스 IP 주소를 인증합니다. 주소가 잘못된 경우 라우팅 업데이트가 삭제됩니다.

스위치가 자체 업데이트 정보를 수신하려 하고 수신 측의 스위치에 네트워크 및 인접 항목이 구성되어 있지 않으면 원본 IP 주소의 인증을 금지 할 수 있습니다. 일반적으로 들어오는 라우팅 정보의 원본 IP 주소를 인증하는 것을 금지하려면 스위치 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
no validate-update-source	들어오는 라우팅 정보의 소스 IP 주소를 인증하는 것을 금지합니다.

20.1.3.9 최대 경로의 수 구성

기본적으로 로컬 RIP 라우팅 테이블에는 최대 1024 개의 경로가 포함됩니다. 경로 번호가 최대 수를 초과하면 라우팅 테이블에 새 경로를 추가 할 수 없습니다. 시스템은 경로 번호가 이미 라우팅 테이블에 설정된 최대 수에 도달했음을 알립니다. 스위치 구성 모드에서 다음 명령을 실행하여 로컬 RIP 라우팅 테이블의 최대 경로 수를 구성합니다.

명령어	설명
maximum-count *number*	로컬 RIP 경로의 최대 수를 설정합니다.
no maximum-count	기본 최대 경로의 수를 재개합니다.

20.1.3.10 Split-Horizon 활성화 와 비활성화

일반적으로 Broadcast IP 네트워크에 연결하고 원거리 벡터 라우팅 프로토콜을 채택하는 스위치는 라우팅 경로의 가능성을 줄이기 위해 Split-Horizon을 채택합니다.

Split-Horizon 의 라우팅 루프에 대한 정보는 라우팅 정보를 수신하는 인터페이스로 자기자신을 선언합니다. 이러한 방식으로, 특히 루프가 끊어 질 때 여러 라우팅 스위치 간의 통신이 향상됩니다. 그러나 Broadcast가 없는 네트워크만큼 좋지는 않습니다. 이 시점에서 Split-Horizon을 금지 할 수 있습니다.

보조 IP 주소가 인터페이스에 구성되어 있고 split-horizon 이 활성화 된 경우 라우팅 업데이트의 소스 IP 주소가 모든 보조 주소를 결론 지을 수 없습니다. 하나의 라우팅 업데이트의 소스 IP 주소에는 하나의 네트워크 수만 포함됩니다.

다음 명령을 실행하여 Split-Horizon을 활성화하거나 비활성화 하세요

명령어	설명
ip rip split-horizon	Split-Horizon를 활성화합니다
no ip rip split-horizon	Spli7t-Horizon를 활성화하지 않습니다.

기본적으로 수평 분할은 지점 간 인터페이스에서 활성화됩니다. 그만큼

point-to-multiple 인터페이스는 금지되어 있습니다.

적의 세부 사항은 "split-horizon 예제"섹션을 참조하십시오.

Note:

정상적인 경우 프로그램이 상태를 변경해야 한다는 확신이 없는 경우 기본 구성을 변경하지 마십시오. Split-Horizon 이 패킷 교환망을 연결하는 직렬 포트에서 금지 되어있는 경우 Split-Horizon을 금지 해야 합니다.

네트워크의 상대적 다중 프로그램 그룹의 스위치에서.

20.1.3.11 Rip를 유지보수 및 모니터링하기

모니터링 및 유지 관리 RIP는 RIP 매개 변수 구성, 실시간 네트워크 트랙과 같은 네트워크 통계 정보를 표시해야 합니다. 이 정보는 네트워크 사용을 판단하고 망 문제 및 네트워크 노드의 도달 범위를 해결하는 데 도움이 됩니다.

모든 라우팅 통계 정보를 표시하려면 관리모드에서 다음명령을 실행하십시오:

명령어	설명
show ip rip	RIP 프로토콜의 현재 상태를 표시합니다.
show ip rip database	모든 RIP 경로를 표시합니다.
show ip rip protocol	모든 RIP 관련 정보를 표시합니다.

라우팅 프로토콜 정보를 추적하려면 관리 모드에서 다음 명령을 실행하십시오.:

명령어	설명
debug ip rip database	라우팅 테이블에 RIP 경로 추가 제거 및 경로 변경에 대한 정보를 추적합니다.
debug ip rip protocol	RIP 메시지를 추적합니다.

20.1.4 RIP 구성 예제

A와 B의 설정은 다음과 같습니다.

장치 A:

```
interface vlan 11
ip address 192.168.20.81 255.255.255.0
!interface loopback 0
ip address 10.1.1.1 255.0.0.0!
router rip
network 192.168.20.0
network 10.0.0.0
```

장치 B:

```
  interface vlan 11
 Ip address 192.168.20.82 255.255.255.0
interface loopback 0
Ip address 20.1.1.1 255.0.0.0
!
router rip
network 192.168.20.0
network 20.0.0.0
```

20.2.1 개요

BEIGRP에서 사용되는 기술은 거리 벡터 프로토콜과 유사합니다.

- 라우터는 라우터가 제공 한 정보에 따라 라우팅을 결정합니다.
- 라우터는 직접 연결하는 Neighbor에게 라우팅 정보를 제공합니다.
- 라우터는 직접 연결하는 Neighbor에게 라우팅 정보를 제공합니다.
  그러나 BEIGRP는 거리 벡터 프로토콜 보다 더 은 장점을 가지고 있습니다.
- BEIGRP는 목적지에 접근 할 수 없고 교체 가능한 경로가 없을 때 Neighbor 을 질의 할 수 있다. 따라서 BEIGRP의 수렴 속도는 최상의 링크 상태 프로토 콜이다.

BEIGRP의 확산 된 업데이트 알고리즘 (DUAL)은 BEIGRP가 다른 전통적인 거리 벡터 프로토콜보다 우수한 핵심적인 이유입니다. 항상 활성 상태이며 목적지에 액세스 할 수 없고 교체 가능한 경로가 없는 경우 인접 라우터에 질의합니다. 따라서 BEIGRP의 수집 속도가 빠릅니다.
BEIGRP는 EIGRP 요구 사항을 기반으로 설계된 특수 전송 프로토콜입니다.
BEIGRP는 IP 프로토콜에서 생성됩니다. BEIGRP는 다음의 요구 사항들을 만족시켜야 합니다.

- Neighbor들의 새로운 경로나 오래된 경로들의 사라짐은 Hello 메시지를 통해 동적으로 감지됩니다.
- 모든 데이터 전송이 안정적입니다.
- 전송 프로토콜은 단일 프로그램 또는 다중 프로그램 전송을 허용합니다.
- 전송 프로토콜은 네트워크 상태 및 Neighbor 응답의 변화에 적응할 수 있습니다.
- BEIGRP는 요구 사항에 따라 대역폭 점유율을 제한 할 수 있습니다.

20.2.2 BEIGRP 구성 업무 목록

BEIGRP 구성에는 다음과 같은 작업이 포함됩니다. BEIGRP를 활성화하는 작업은 필수입니다. 필요에 따라 다른 작업을 선택적으로 수행 할 수 있습니다.

- BEIGRP 활성화
- BEIGRP 복합 거리에 대한 규정 계수
- Offset 을 통합 복합 거리 조정
- 자동 경로 요약 비활성화
- 경로 요약 사용자 정의
- 전달 경로 구성
- 다른 BEIGRP의 매개변수 구성
- BEIGRP의 실행 모니터링과 유지관리

20.2.3 BEIGRP 구성 작업

20.2.3.1 BEIGRP 활성화하기

BEIGRP 프로세스를 작성하려면 다음을 수행하십시오.

명령어	설명
router beigrp *as-number*	전역 모드에 BEIGRP 프로세스를 추가합니다.
network *network-number network-mask*	경로 모드에서 망 분배를 BEIGRP 프로세스에 추가합니다.

위의 구성이 완료되면 BEIGRP는 네트워크 세그먼트의 모든 인터페이스에서 실행되기 시작합니다. BEIGRP는 hello 메시지를 통해 새로운 Neighbor을 찾고 업데이트 정보를 통해 원래의 경로와 상호 작용합니다.

20.2.3.2 대역폭 점유율 구성하기

기본 상태에서 BEIGRP는 대역폭의 최대 50 %를 차지합니다. VLAN 인터페이스 구성 모드에서 다음 명령을 실행하여 대역폭을 조정할 수 있습니다.

명령어	설명
ip beigrp bandwidth-percent *percent*	BEIGRP의 최대 대역폭 백분율을 구성합니다.

20.2.3.3 BEIGRP 복합 거리에 대한 규정 계수

어떤 경우에는 BEIGRP 복합 거리의 계수가 최종적으로 라우팅 전략에 영향을 미칠 필요가 있다. BEIGRP가 사용하는 기본 계수는 대부분의 네트워크 조건에 적합

하지만 일부 특수한 경우에는 규제해야 합니다. 규제로 인해 전체 네트워크가 크게 변경 될 수 있습니다. 이 규정을 수행 할 때 주의하십시오.

경로 구성모드에서 다음명령을 실행하십시오.

명령어	설명
metric weights *k1 k2 k3 k4 k5*	BEIGRP 복합거리의 계수를 조절합니다.

20.2.3.4 Offset을 통한 복합 거리 조정하기

Offset 테이블을 사용하여 요구 사항에 따라 모든 수신 및 발신 경로를 의도적으로 추가하거나 여러 가지 적합한 경로의 종합 거리를 추가 할 수 있습니다. 목적은 라우터의 라우팅 결과에 영향을 미치는 것입니다. 구성 프로세스에서 Offset-List에 액세스 목록 또는 응용 프로그램 인터페이스를 선택적으로 지정하여 Offset이 추가된 경로를 추가로 확인할 수 있습니다.

명령어	설명
offset{type number | *} {**in** | **out**} access-list-name offset	Offset 테이블을 적용합니다.

20.2.3.5 자동 요약 기능 비활성화

BEIGRP의 자동 수집은 다른 동적 라우팅 프로토콜과 다릅니다.
다음 규정을 준수합니다.

- BEIGRP 프로세스의 여러 네트워크가 정의되면 네트워크의 하나 이상의 서브넷이 BEIGRP 토폴로지 테이블에 있으면 네트워크의 요약 경로가 생성됩니다.
- 생성 된 요약 경로는 모든 서브넷의 최소 거리를 갖는 Null0 인터페이스를 지향합니다. 요약 경로는 기본 IP 라우팅 테이블에도 추가됩니다. 관여 거리는 5 (구성 할 수 없음)입니다.
- 업데이트 정보가 다른 주 IP 네트워크의 Neighbor 노드로 전송되면 룰 1과 룰 2의 요약 라우트 서브넷이 취소됩니다. 요약 경로만 전송됩니다.
- BEIGRP 절차에서 정의 된 망에 속하지 않는 서브넷은 수집되지 않습니다.

일부 네트워크 환경에서는 각 세부 경로를 Neighbor에게 알릴 수 있습니다. 이 경우 다음 명령을 실행해야 합니다.

명령어	설명
no auto-summary	자동 요약 경로를 실행하지 않습니다.

20.2.3.6 라우팅 요약 사용자 정의

경로 요약이 요구 사항을 충족 할 수 없는 경우 BEIGRP가 실행되는 인터페이스에

서 라우팅 요약을 구성하고 라우팅 요약을 수행 할 대상 네트워크 세그먼트를 지정할 수 있습니다. 라우팅 요약이 구성된 인터페이스는 라우팅 요약 망 분할에 속하는 상세한 라우팅 업데이트 정보를 보내지 않습니다. 다른 인터페이스는 영향을 받지 않습니다.

라우팅 요약 작업은 다음 규정을 준수합니다.

- 라우팅 요약 명령이 인터페이스에 구성된 후, 네트워크에 적어도 하나의 서브넷이 BEIGRP 토폴로지 테이블에 있으면 정의 된 네트워크의 요약 된 경로가 생성됩니다.
- 생성 된 요약 경로는 모든 서브넷의 최소 거리를 갖는 Null0 인터페이스를 지향합니다. 요약 된 경로는 기본 IP 라우팅 테이블에도 추가됩니다. 관리 거리는 5 (구성 할 수 없음)입니다.
- 라우팅 업데이트 정보가 라우팅 요약이 구성된 인터페이스에서 전송되면 라우팅 요약 네트워크 세그먼트에 속한 세부 경로가 취소됩니다. 다른 라우팅 업데이트 정보는 영향을받지 않습니다.

명령어	설명
ip beigrp summary-address *ip address address mask*	인터페이스에 경로 요약을 구성합니다.

20.2.3.7 전송 경로 구성하기

BEIGRP가 다른 유형의 경로를 전달할 때, 다음 규정을 준수합니다.

- 현재 경로가 정적 또는 직접 연결되어있는 경우, 명령 default-metric을 구성할 필요가 없으며 다른 복합 거리 매개 변수 (대역폭, 지연, 신뢰성, 유효로드 및 MTU)를 현재 포트에서 직접 가져올 수 있습니다.
- 현재 경로가 다른 BEIGRP 프로세스의 경로 인 경우 default-metric 명령을 구성 할 필요가 없으며 BEIGRP 프로세스에서 복합 매개 변수 매개 변수를 직접 가져올 수 있습니다.
- default-metric 명령은 rip 및 ospf와 같은 다른 프로토콜의 라우트가 전송 될 때 구성되어야합니다. 경로 전달의 적절한 거리는 구성 값에 의해 결정됩니다. 명령이 구성되어 있지 않으면 경로 전달이 작동하지 않습니다.

BEIGRP와 RIP가 동시에 실행되는 스위치에서 BEIGRP Neighbor 라우터가 로컬 스위치의 RIP 프로토콜에 대해 학습 한 경로를 알리려면 다음 명령을 실행합니다.

명령어	설명
default-metric bandwidth delay reliability loading mtu	경로 전달의 기본 백터 거리를 구성합니다.
redistribute *protocol* [**route-map** *name*]	경로를 BEIGRP 프로토콜로 전달합니다.

20.2.3.8 다른 BEIGRP 매개 변수 구성하기

다른 네트워크 조건에 BEIGRP를 효율적으로 만들려면 다음을 수정해야합니다.

- BEIGRP가 hello 메시지와 Neighbor 시간 초과를 보낼 간격을 수정하십시오.
- Split-Horizon 비활성화

0. BEIGRP가 Hello메시지와 인접과의 Timeout 일 경우 보내기 위한 간격을 생성 합니다.

올바른 BEIGRP 작업을 수행하기 위해 BEIGRP hello 프로토콜에 필요한 다음과 같은 정보가 나열됩니다.

- 새로운 접근 가능한 Neighbor을 발견 할 수 있으며 Neighbor 검출은 구성없는 자동 프로세스입니다.
- Neighbor 구성을 인증하고 호환 모드로 구성된 Neighbor 간의 통신만 허용합니다.
- Neighbor의 유용성을 지속적으로 모니터링하고 Neighbor들 실종을 감지합니다.

라우터는 BEIGRP가 실행되는 인터페이스에서 hello 멀티프로그램 Broadcast 패킷을 보냅니다. 각 BEIGRP 지원 라우터는 이러한 멀티프로그램 Broadcast 패킷을 수신합니다. 따라서 모든 Neighbor을 찾을 수 있습니다.

Hello 프로토콜은 두 개의 타이머를 사용하여 Neighbor의 소멸을 감지합니다. hello 간격은 라우터의 인터페이스에서 BEIGRP hello 메시지의 전송 빈도를 지정합니다. hold timer는 라우터가 지정된 Neighbor으로부터 데이터를 수신 할 수 없을 때 Neighbor이 죽었다 고 선언 할 시간을 지정합니다. Neighbor 라우터로부터 어떤 종류의 BEIGRP 패킷이 수신 된 후에는 홀드 타이머의 값을 리셋 해야 합니다.

다른 네트워크 유형 과 대역폭은 hello Timer의 다른 기본값을 채택합니다.

Interface Type Packaging	**상태**	**Hello Timer (초)**	**Hold Timer (초)**
LAN 인터페이스	Any	5	15

Hello 프로토콜에서 타이머의 다른 기본값으로 동일한 IP 서브넷을 연결하는 BEIGRP Neighbor 라우터가 다른 hello 타이머 와 Hold 타이머를 사용 할 수 있습니다. 에러가 발생하지 않도록 하려면 각 라우터의 hello 패킷에 hold 타이머를 지정해야 합니다. 각 BEIGRP 라우터는 Neighbor 라우터의 hello 패킷에 지정된 hold 타이머를 사용하여 Neighbor 라우터가 시간 초과되는지 여부를 판단합니다. 이러한 방식으로 하나의 WAN 토폴로지에서 서로 다른 Neighbor의 장애 감지 타이머가 나타납니다. 특별한 경우 타이머의 기본값은 실제 요구 사항을 충족시킬 수 없습니다.

hello 메시지를 보낼 간격을 수정하려면 다음 명령을 실행하십시오.

명령어	설명
ip beigrp hello-interval *seconds*	인터페이스에 Hello-interval 메시지를 보내는 간격을 수정합니다

Neighbor의 시간 초과 타이머를 수정하려면 다음 명령을 실행하십시오.

명령어	설명
ip beigrp hold-time *seconds*	Neighbor의 시간에 초과시간을 정합니다

0. Split-Horizon 비활성화

Split-Horizon 기능이 일반적으로 적용됩니다. 수신 된 라우팅 정보가 동일한 인터페이스에서 Broadcast 되지 않게 경로에 반복현상을 방지합니다. 어떤 경우에는 Split-Horizon 함수가 좋지 않을 경우 다음 명령을 실행하여 Split-Horizon 함수를 비활성화 할 수 있습니다.

명령어	설명
no ip beigrp split-horizon	Split-Horizon 기능을 비활성화 합니다.

20.2.3.9 BEIGRP 모니터링과 유지보수하기

다음 명령어를 실행하여 neighbor의 관계를 정리 할 수 있습니다.

명령어	설명
clear ip beigrp neighbors [*interface*]	Neighbor의 관계를 정리합니다.

모든 BEIGRP 통계 정보를 표시하려면 다음 명령을 실행하십시오:

명령어	설명
show ip beigrp interfaces [*interface*] [*as-number*]	인터페이스에 대한 정보를 표시합니다.
show ip beigrp neighbors [*as-number* | *interface*]	인접 항목에 대한 정보를 표시합니다.
show ip beigrp topology [*as-number* | all-link | summary | active]	토폴로지 테이블에 대한 정보를 표시합니다

20.2.4 BEIGRP 구성 예제

다음의 예는 VLAN11에서 네트워크 세그먼트 10.0.0.0/8을 보내는 요약 경로를 구성합니다. 네트워크 세먼트의 모든 서브넷 경로는 neighbor을 통보 받지 않습니다. 동시에, BEIGRP 프로세스의 자동 요약이 비활성화됩니다.

```
interface vlan 11
ip beigrp summary-address 1 10.0.0.0 255.0.0.0
router beigrp 1
network 172.16.0.0 255.255.0.0
no auto-summary
```

20.3.1 개 요

이 장에서는 OSPF를 구성하는 방법에 대해 설명합니다. OSPF 명령에 대한 자세한 내용은 OSPF 명령에 대한 상대 섹션을 참조하십시오.

OSPF는 IETF의 OSPF 팀에서 개발한 IGP 라우팅 프로토콜입니다. IP 네트워크 용으로 설계된 OSPF는 IP 서브넷 및 외부 라우팅 정보 식별자, 메시지 인증 및 IP 멀티 캐스트를 지원합니다.

우리 스위치의 OSPF 기능은 OSPF V2 (RFC2328 참조)의 요구 사항을 준수합니다. 다음 표에는 실제의 주요 기능이 나와 있습니다.

중요 특징	**설명**
Stub domain	남은 도메인을 지원합니다.
Rout forwarding	모든 라우팅 프로토콜에 의해 학습 된 경로는 다른 라우팅 프로토콜 도메인으로 전달 될 수 있습니다. 즉, OSPF는 자동 도메인에서 RIP가 학습 한 경로를 입력 할 수 있습니다. 그 경로 또한 OSPF는 RIP로 내보낼 수 있음을 알게 됩니다.
Authentication	도메인의 인접한 스위치 중 텍스트 및 MD5 인증이 지원됩니다.
Routing interface parameters	구성 가능한 인터페이스 매개 변수에는 출력 비용, 재전송 간격, 인터페이스 출력 지연, 스위치의 우선 순위, 스위치의 종료를 판단하는 간격, hello 패킷의 간격 및 인증 PIN이 포함됩니다.
Virtual link	가상의 링크를 지원합니다
NSSA area	RFC 1587 참조 하십시오
OSPF in the on-demand circuit	RFC 1793 참조 하십시오.

20.3.2 OSPF 작업 목록 구성하기

OSPF는 전체 도메인에서 스위치,ABR 및 ASBR간에 라우팅 데이터 교환이 필요합니다. 구성을 단순화하기 위해 인증없이 기본 설정으로 실행되도록 할 수 있습니다. 그러나 특정 매개 변수를 수정하는 경우 수정 된 매개 변수가 모든 스위치에서 동일해야 합니다. OSPF를 구성하려면 다음 작업을 완료해야 합니다. OSPF를 활성화하는 작업은 필수이며 다른 구성은 선택 사항입니다.

- OSPF의 매개변수 인터페이스 구성하기
- 서로 다른 물리적 네트워크에서 OSPF 구성
- OSPF Area 매개변수 구성
- OSPF의 NSSA 도메인 구성
- OSPF Area에서 경로 요약 구성
- 전달된 경로 요약 구성
- 기본 경로 생성
- Loopback 인터페이스에서 경로 ID 선택
- OSPF의 관리 범위 구성
- 경로 계산을 위한 타이머 설정
- OSPF 모니터링 및 유지 보수

경로 구성의 경우 IP 라우팅 프로토콜 구성에 대한 관련 내용을 참조하십시오.

20.3.3 OSPF 작업 구성하기

20.3.3.1 OSPF 시작하기

다른 라우팅 프로토콜과 마찬가지로 OSPF를 활성화하기 전에 OSPF 라우팅 프로세스를 만들어야 합니다. 라우팅 프로세스를 생성 할 때 처리와 관련된 IP 주소
범위와 관련 도메인 ID를 배포 해야 합니다.

전역 구성 모드에서 다음 명령을 실행하여 OSPF를 시작합니다.

명령어	설명
router ospf *process-id*	OSPF 라우팅 프로토콜을 활성화와 스위치 구성 모드를 시작합니다.
network *address mask* **area** *area-id*	OSPF 및 관련 인터페이스 도메인 ID의 실행중인 인터페이스를 구성합니다.

20.3.3.2 OSPF 인터페이스 매개변수 구성하기

실제 요구 사항에 따라 인터페이스의 OSPF 매개 변수를 수정할 수 있습니다. 매개 변수를 수정할 때 상호 연결된 네트워크의 모든 스위치에서 매개 변수가 동일한 지 확인하십시오.

인터페이스 구성 모드에서 다음 명령을 실행하여 인터페이스 매개 변수를 구성하십시오.

명령어	**설명**
ip ospf cost *cost*	OSPF 인터페이스에서 전송 패킷의 값을 구성합니다.
ip ospf retransmit-interval *seconds*	동일한 OSPF 인터페이스에서 neighbor 사이의 LSA 재전송 시간 (초)을 구성합니다.
ip ospf transmit-delay *seconds*	OSPF 인터페이스에서 LSA를 보낼 시간을 구성합니다 (단위: 초).
ip ospf priority *number*	라우팅 스위치가 OSPF 에서 DR이 되도록 되도록 우선 순위 번호를 구성합니다.
ip ospf hello-interval *seconds*	OSPF 인터페이스에서 hello 패킷을 보내는 간격을 구성합니다.
ip ospf dead-interval *seconds*	Dead-interval 을 구성합니다. 소정의 간격에서, neighbor들로부터 hello 패킷이 수신되지 않으면, 인접 스위치는 shutdown 상태로 간주합니다.
ip ospf authentication-key *key*	네트워크 세그먼트에서 인접 라우터의 인증 암호를 나타냅니다. OSPF 인증 암호가 채택됩니다.
ip ospf message-digest-key *keyid* md5 *key*	MD5 인증을 사용하려면 OSPF가 필요합니다
ip ospf passive	포트에서 hello 메시지의 상태를 구성합니다.

20.3.3.3 서로 다른 물리적 네트워크에서 OSPF 구성

OSPF는 네트워크의 물리적 미디어를 다음과 같은 클래스로 나눕니다.

- Broadcast 네트워크 (Ethernet, Token Ring, FDDI)
- Non-broadcast 와 다중 접속 네트워크(SMDS, Frame Relay, X.25)
- Point-to-point 네트워크(HDLC, PPP)

X.25 및 Frame-relay 네트워크는 선택적 broadcast 기능을 제공합니다. map 명령을 통해 broadcast 네트워크에서 실행되도록 OSPF를 구성합니다.. map 명령에 대한 자세한 내용은 WAN 명령어 참조안에 map 명령에 대한 설명을 참조하십시오

20.3.3.4 OSPF 네트워크 유형 구성

네트워크가 속한 물리적 미디어 유형에 상관없이 네트워크를 Broadcast 네트워크 또는 non-Broadcast 및 다중 접근성 네트워크로 구성 할 수 있습니다. 이 기능을 사용하면 네트워크를 유연하게 구성 할 수 있습니다. Broadcast 네트워크를 non-Broadcast 및 멀티 액세스 네트워크로 구성 할 수 있습니다. Broadcast 네트워크에 X.25, 프레임 릴레이 및 SMDS와 같은 non-Broadcast 네트워크를 구성 할 수도 있습니다. 이 기능은 neighbor의 구성을 용이하게 합니다. 자세한 내용은 non-Broadcast 네트워크의 OSPF 구성에 대한 내용을 참조하십시오.

Broadcast 네트워크 또는 non-Broadcast 네트워크에 non-Broadcast 및 멀티 액세스 네트워크를 구성하는 것은 두 개의 랜덤 스위치 간에 가상 링크가 존재한다고 가정하거나 네트워크가 그물형 네트워크라고 가정하는 것입니다. 이전 구성은 비용이 너무 많이 들기 때문에 비현실적입니다. 부분 Broadcast 및 다중 액세스 네트워크를 부분적으로 그물형 된 네트워크로 구성 할 수 있습니다. 비용을 절약하기 위해 non-Broadcast 및 멀티 액세스 네트워크를 지점 간 네트워크로 구성 할 수 있습니다. 분리 된 스위치는 가상 링크를 통해 라우팅 정보를 서로 교환 할 수 있습니다.

OSPF 지점을 다른 지점에 연결하는 인터페이스는 지점 간 (point-to-multipoint) 네트워크 인터페이스로 정의됩니다. 그것은 많은 호스트 경로를 만듭니다. 비교

Non-broadcast 및 멀티 액세스 네트워크 또는 지점 간 네트워크의 경우 OSPF

point-to-multipoint 네트워크에는 다음과 같은 이점이 있습니다.

- point-to-multipoint network는 쉽게 구성 할 수 있습니다.
- Point-to multipoint network는 전체 메시 네트워크의 토폴로지가 필요하지 않으므로 비용이 적다
- 더 신뢰할 수 있습니다. 가상 링크가 실패하더라도 연결은 계속 작동 할 수 있습니다. 인터페이스 구성 모드에서 다음 명령을 실행하여 OSPF 네트워크 유형을 구성합니다.

인터페이스 설정 모드에서 명령을 실행하여 OSPF 네트워크의 유형을 설정하십시오

명령어	설명
ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] }}	OSPF의 형태의 네트워크로 구성한다.

Broadcast network는 하나의 스위치의 네트워크이다.

20.3.3.5 매개변수 지역 구성하기

구성 가능한 Area 매개 변수에는 인증, 스텁 Area 및 기본 라우팅 요약 값이 포함됩니다. 인증은 암호 보호를 기반으로 합니다. 스텁 Area은 외부 경로가 전송되지 않는 Area입니다. ABR은 기본값을 생성합니다.

스터브 Area에 들어가기 한 외부 경로. 자동 Area 외부의 외부 네트워크에 스텁 Area을 연결할 수 있습니다. OSPF 스텁이 지원하는 기능을 사용하려면 스텁 Area에서 기본 경로를 사용해야합니다. 스텁 Area에 들어가기 위해 LSA를 추가로 줄이려면 ABR에서 옵션 없음을 선택해야합니다.
스위치 매개 변수를 설정하려면 스위치 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
area *area-id* **authentication simple**	OSPF Area의 인증을 활성화합니다.
area *area-id* **authentication message-digest**	MD5 인증을 인증OSPF로 지정합니다.
area *area-id* **stub** [no-summary]	Stub Area을 정의합니다.
area *area-id* **default-cost** *cost*	스텁 Area의 기본 경로 값을 설정합니다.

20.3.3.6 OSPF Area에서의 라우팅 요약 구성

이 기능을 사용하면 ABR은 다른 지역으로 요약 경로를 Broadcast 할 수 있습니다. OSPF에서 ABR은 모든 네트워크를 다른 Area으로 Broadcast합니다. 일부 방법에 따라 네트워크 번호가 순차적으로 분배되는 경우 ABR을 구성하여 요약 경로를 다른 Area에 broadcasting 요약 경로는 특정 범위의 모든 네트워크를 포괄 할 수 있습니다.

스위치 구성 모드에서 다음 명령을 실행하여 주소 범위를 설정하십시오.

명령어	설명
area *area-id* **range** *address mask*	요약 Area의 주소 범위를 설정합니다.

20.3.3.7 전달 된 라우팅 요약 구성

경로가 다른 Area에서 OSPF Area으로 분배 될 때, 각 경로는 외부 LSA 방법으로 고유하게 Broadcast됩니다. 그러나 특정 주소 Area을 포함 할 수 있는 경로를 Broadcast하도록 스위치를 구성 할 수 있습니다. 이 방법은 OSPF 연결 상태 데이터베이스의 크기를 줄입니다.

스위치 구성 모드에서 다음 명령을 실행하여 요약 경로를 구성하십시오.

명령어	설명
summary-address *prefix* *mask* [not advertise]	분산 경로를 다루는 주소와 마스크를 설명합니다. 하나요약 라우트는 broadcast됩니다.

20.3.3.8 기본 경로 생성

ASBR에서는 OSPF 경로 Area에 들어가기 위해 기본 경로를 생성해야 합니다.

OSPF Area에 경로를 배포하도록 스위치를 구성하면 경로가 자동으로 ASBR이 됩니다. 그러나 기본 ASBR은 기본 경로를 생성하지 않아 OSPF 라우팅 Area에 들어갑니다.

ASBR이 기본 경로를 생성하도록 스위치 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
default-information originate [always] [route-map *map-name*]	목표 ASBR 기본 경로를 생성하도록 합니다.

20.3.3.9 Loopback 인터페이스를 통한 경로 ID선택

OSPF는 인터페이스에 구성된 최대의 값을 IP 주소를 스위치 ID로 사용합니다. IP 주소를 연결하는 인터페이스가 다운 상태로 변경되거나 IP 주소가 취소 된 경우 OSPF 프로세스는 새 스위치 ID를 다시 계산하고 모든 인터페이스에서 라우팅 정보를 다시 보냅니다.

인터페이스가 IP 주소로 구성되면 스위치는 IP 주소를 ID로 사용합니다. Loopback 인터페이스는 절대로 다운 상태가 되지 않습니다. 따라서 라우팅 테이블은 안정적입니다. 스위치는 우선적으로 Loopback 인터페이스를 스위치 ID로 사용합니다. 또한 스위치 ID로 최대 IP 주소를 선택합니다. Loopback 인터페이스가 없으면 스위치의 큰 값의 IP 주소가 스위치 ID로 간주됩니다. 특수 인터페이스를 사용하려고 OSPF를 지정하는 건 불가능합니다.

글로벌 루프 모드에서 다음 명령을 실행하여 IP Loopback 인터페이스를 구성하십시오.

명령어	설명
interface loopback 0	Loopback 인터페이스를 생성하고 인터페이스 구성 모드를 시작합니다.
ip address *ip-address mask*	인터페이스의 IP주소를 분배합니다.

20.3.3.10 OSPF 관리 공간 구성

관리 공간은 단일 스위치 또는 스위치 그룹과 같은 라우팅 소스정보의 신용 수준을 나타냅니다. 일반적으로 관리 공간은 0 에서 255 사이의 정수입니다. 숫자가
클수록 신용도가 낮아집니다. 만약 관리 공간이 255 인 경우 라우팅 소스 정보가
신뢰 되지 않거나 생략되어야 합니다.

OSPF는 세 가지 종류의 서로 다른 관리 공간 (Area 간 및 내-외부)를 사용

합니다. 한 지역의 경로를 **intra-area 경로**라고 부릅니다. 다른 지역으로 가는 경로를 **inter-area 경로**라고 부릅니다. 다른 라우팅 프로토콜 Area에서 분산 된 경로를 **external-area 경로**라고 합니다. 각 경로의 유형 기본값은 110입니다.

스위치 구성 모드에서 다음 명령을 실행하여 OSPF의 거리 값을 구성하십시오.

명령어	설명
distance ospf [intra-area *dist1*] [inter-area *dist2*] [external *dist3*]	Area 내 경로, Area 간 경로 및 외부 경로의 관리 거리 값을 수정합니다.

20.3.3.11 경로 계산을 위한 타이머구성

OSPF가 토폴로지 변경 정보를 수신하고 계산이 시작될 때까지 지연 시킬 수 있습니다. 연속적으로 SPF를 계산하는 간격을 구성 할 수도 있습니다. 스위치 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
timers delay *delaytime*	라우팅 계산의 지연시간을 설정합니다.
timers hold *holdtime*	라우팅 계산의 최소 간격을 설정합니다.

20.3.3.12 OSPF 모니터링 및 유지보수하기

네트워크 통계정보에는 IP 라우팅 테이블, 캐시 및 데이터베이스의 내용이
포함됩니다. 모든 정보는 네트워크 리소스 사용을 판단하고 네트워크 문제를 해결하며 네트워크 노드의 연결 가능성을 확인하고 패킷이 네트워크를
통과하는 경로를 찾는데 도와줍니다.

모든 라우팅 통계 정보를 표시하려면 다음 명령을 실행하십시오.

명령어	설명
Show ip ospf [*process-id*]	OSPF 프로세스의 정보를 표시합니다.

Show ip ospf [*process-id*] **database** **show ip ospf** [*process-id*] **database [router]** [*link-state-id*] **show ip ospf** [*process-id*] **database [router] [self-originate]** **show ip ospf** [*process-id*] **database [router] [adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database [network]** [*link-state-id*] **show ip ospf** [*process-id*] **database [summary]** [*link-state-id*] **show ip ospf** [*process-id*] **database [asbr-summary]** [*link-state-id*] **show ip ospf** [*process-id*] **database [external]** [*link-state-id*] **show ip ospf** [*process-id*] **database**	OSPF 데이터베이스에 대한 상대적 정보를 표시합니다.
show ip ospf border-routers	ABR과 ASBR 간의 라우팅 테이블에 내부 항목을 표시합니다.
show ip ospf interface	OSPF 인터페이스 정보를 표시합니다.
show ip ospf neighbor	인터페이스에 따라 OSPF의 neighbor에 대한 정보를 표시합니다.
debug ip ospf adj	OSPF 인접 구축 절차를 모니터링합니다.
debug ip ospf events	OSPF 인터페이스 및 인접 이벤트를 모니터합니다.
debug ip ospf flood	OSPF 데이터베이스의 초과를 모니터합니다.
debug ip ospf lsa-generation	OSPF의 LSA 생성을 모니터링합니다.
debug ip ospf packet	OSPF 메시지를 모니터합니다.
debug ip ospf retransmission	OSPF의 메시지 재전송을 모니터합니다.
debug ip ospf spf **debug ip ospf spf intra** **debug ip ospf spf inter** **debug ip ospf spf external**	OSPF의 SPF 계산 경로를 모니터링합니다.
debug ip ospf tree	OSPF의 SPF 트리 설정을 모니터링합니다.

20.3.4 OSPF 구성 예제

20.3.4.1 VLSM 구성 예제

OSPF 및 고정 경로는 VLSM을 지원합니다. VLSM을 통해 서로 다른 인터페이스의 다른 마스크에서 동일한 네트워크 번호를 사용할 수 있습니다. 따라서 IP 주소가 저장되고 주소 공간이 효과적으로 활용됩니다. 다음 예에서는 30자리 서브넷 마스크가 사용됩니다. 2 자리 주소 공간은 직렬 포트의 호스

트 주소 용으로 예약되어 있습니다. 두 개의 호스트 주소로 충분합니다.

```
interface vlan 10
  ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernets
interface vlan 11
  ip address 131.107.254.1 255.255.255.252
! 2 bits of address space reserved for serial lines
! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
  network 131.107.0.0 0.0.255.255 area 0.0.0.0
```

20.3.4.2 OSPF 경로와 경로 분배의 구성 예

OSPF는 내부 스위치, ABR(Area Bounder Router) 및 ASBR(Autonomous System Border Router) 간에 정보를 교환해야 합니다. 최소 구성에서 OSPF 기반 스위치는 기본 매개 변수 설정으로 작동 할 수 있습니다. 인증을 요구하지 않습니다.

다음은 세 가지 구성 예입니다.

첫 번째 예는 기본적인 OSPF 명령을 보여줍니다.

두 번째 예는 자동 라우팅 스위치, ABR 및 ASBR을 자동 시스템에 구성하는 방법을 보여줍니다.

세 번째 예는 모든 종류의 OSPF 도구를 사용하는 방법을 보여줍니다.

0. 기본 OSPF 구성 예

다음 예에서는 간단한 OSPF를 구성하는 방법을 보여줍니다. 라우팅 프로세스 활성화 번호 90과 이더넷 인터페이스 0을 Area 0.0.0.0에 연결하십시오. 한편 RIP를 OSPF로 보내거나 OSPF를 RIP로 보냅니다.

```
interface vlan 10
ip address 130.130.1.1 255.255.255.0
ip ospf cost 1
interface vlan 10
ip address 130.130.1.1 255.255.255.0
router ospf 90
```

```
network 130.130.0 .0 255.255.0.0 area 0
redistribute rip
router rip
network 130.130.0.0
redistribute ospf 90
```

0. 내부 라우팅 스위치, ABR 및 ASBR의 기본 구성 예제

다음 예제에서는 네 개의 IP 주소 범위에 네 개의 Area ID가 배포됩니다. 라우팅 프로세스 (109)가 활성화된다. 네 개의 area는 area10.9.50.0, area 0, area 2 및 area 3입니다. Area 10.9.50.0, 2 및 3의 마스크는 주소 범위로 지정됩니다.
Area 0에는 모든 네트워크가 포함됩니다.

```
router ospf 109
  network 131.108.20.0 255.255.255.0 area 10.9.50.0
  network 131.108.0.0 255.255.0.0 area 2
  network 131.109.10.0 255.255.255.0 area 3
  network 0.0.0.0 0.0.0.0 area 0
! Interface vlan10 is in area 10.9.50.0:
interface vlan 10
  ip address 131.108.20.5 255.255.255.0
! Interface vlan11 is in area 2:
interface vlan 11
  ip address 131.108.1.5 255.255.255.0
! Interface vlan12 is in area 2:
interface vlan 12
  ip address 131.108.2.5 255.255.255.0
! Interface vlan13 is in area 3:
interface vlan 13
  ip address 131.109.10.5 255.255.255.0
! Interface vlan14 is in area 0:
interface vlan 14
  ip address 131.109.1.1 255.255.255.0
! Interface vlan 100 is in area 0:
interface vlan 100
  ip address 10.1.0.1 255.255.0.0
```

네트워크 Area 구성 명령의 기능은 순서가 있으므로 명령 순서가 중요합니다. 스위치는 순서에 따라 IP 주소 / 마스크의 짝을 일치시킵니다. 자세한 내용은 OSPF 명령 섹션을 참조하십시오.

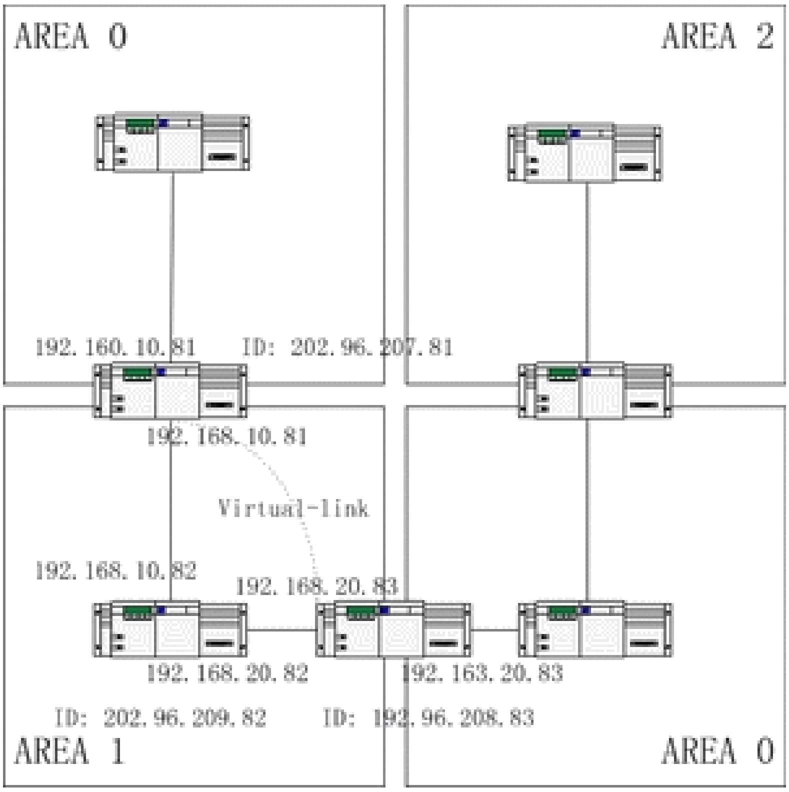
첫 번째 네트워크 Area을 확인하십시오. Area ID 10.9.50.0에 대해 구성된 인터페이스 Subnet 131.108.20.0은 131.108.20.0입니다. 이더넷 인터페이스는 0으로 설정됩니다. 따라서 인터페이스는 10.9.50.0 Area에 있습니다.

두 번째 Area에서는 다른 인터페이스를 분석하기 위해 이전 프로세스가 채택되면 인터페이스가 1로 일치합니다. 따라서 인터페이스 1은 Area 2를 연결합니다.

다른 네트워크 Area을 계속 일치시킵니다. 마지막 네트워크 Area 명령은 예외이며, 이는 나머지 모든 인터페이스가 네트워크 Area 0에 연결된다는 것을 의미합니다.

0. 내부스위치에서의 ABR 과 ASBR의 복잡한 구성

다음 예는 단일 OSPF 자동 시스템에 여러 스위치를 구성하는 방법을 보여줍니다. 다음
그림은 구성 예에 대한 네트워크 토폴로지를 보여줍니다.



위의 그림에 따라 스위치를 구성하십시오.

```
RTA：
interface loopback 0
  ip address 202.96.207.81 255.255.255.0
!
interface vlan 10
  ip address 192.168.10.81 255.255.255.0
!
interface vlan 10
  ip address 192.160.10.81 255.255.255.0
!
router ospf 192
  network 192.168.10.0 255.255.255.0 area 1
  network 192.160.10.0 255.255.255.0 area 0
!
RTB：
interface loopback 0
  ip address 202.96.209.82 255.255.255.252
!
interface vlan 10
  ip address 192.168.10.82 255.255.255.0
!
interface vlan 11
  ip address 192.160.20.82 255.255.255.0
!
router ospf 192
  network 192.168.20.0 255.255.255.0 area 1
  network 192.168.10.0 255.255.255.0 area 1
!
RTC：
interface loopback 0
ip address 202.96.208.83 255.255.255.252
!
interface vlan 10
ip address 192.163.20.83 255.255.255.0
!
interface vlan 11
ip address 192.160.20.83 255.255.255.0
!
```

```
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.163.20.0 255.255.255.0 area 0
```

20.3.5 복잡한 OSPF 를 ABR 스위치에서 구성하기

다음은 ABR 구성 작업에 대한 설명입니다.

- 기본 OSPF 구성하기
- 경로 분배하기

다음은 기본 구성 작업입니다.

(1) 이더넷 0 ~3 에 대한 주소 범위 구성

(2) 모든 인터페이스에서 OSPF 활성화

(3) 각 Area 및 네트워크의 인증 비밀번호 설정

(4) 링크 상태 값 및 기타 인터페이스 매개 변수 설정

노트:
하나의 영역 명령을 각각 사용하여 인증 매개 변수와 Stub 영역을 설정하세요 하나의 명령을 사용하여 이러한 매개변수를 설정할 수 있습니다.

- 백본 영역 설정(Area 0).

배포와 관련된 구성 작업은 다음과 같습니다.

- IGRP 경로와 RIP 경로를 배포하여 OSPF 매개 변수 설정 (매트릭, 매트릭 유형, 태그 및 서브넷 포함)을 입력합니다.
- IGRP 경로와 OSPF 경로를 RIP에 배포하십시오. .

다음은 OSPF의 설정의 예시입니다.

```
interface vlan 10
  ip address 192.168.20.81 255.255.255.0
  ip ospf password GHGHGHG
  ip ospf cost 10
interface vlan 11
  ip address 192.168.30.81 255.255.255.0
  ip ospf password ijklmnop
  ip ospf cost 20
  ip ospf retransmit-interval 10
  ip ospf transmit-delay 2
```

```
   ip ospf priority 4
!
interface vlan 12
   ip address 192.168.40.81 255.255.255.0
   ip ospf password abcdefgh
   ip ospf cost 10
!
interface vlan 13
   ip address 192.168.0.81 255.255.255.0
   ip ospf password ijklmnop
   ip ospf cost 20
   ip ospf dead-interval 80
!
router ospf 192
   network 192.168.0.0 255.255.255.0 area 0
   network 192.168.20.0 255.255.255.0 area 192.168.20.0
   network 192.168.30.0 255.255.255.0 area 192.168.30.0
   network 192.168.40.0 255.255.255.0 area 192.168.40.0
   area 0 authentication simple
   area 192.168.20.0 stub
   area 192.168.20.0 authentication simple
   area 192.168.20.0 default-cost 20
   area 192.168.20.0 authentication simple
   area 192.168.20.0 range 36.0.0.0 255.0.0.0
   area 192.168.30.0 range 192.42.110.0 255.255.255.0
   area 0 range 130.0.0.0 255.0.0.0
   area 0 range 141.0.0.0 255.0.0.0
   redistribute rip
```

RIP 은 네트워크 192.168.30.0. 주소

```
router rip
   network 192.168.30.0
   redistribute ospf 192
 !
```

20-4장 BGP 구성하기

이 장에서는 경계 게이트웨이 프로토콜 (BGP)을 구성방법에 대해 설명합니다.
BGP 명령에 대한 자세한 내용은 "BGP 명령" 섹션을 참조하십시오. BGP는 RFC1163, 1267 및 1771에 정의 된 Exterior Gateway Protocol (EGP)입니다. BGP를 사용하면 자치 시스템(AS) 간에 라우팅 선택 방법을 만들 수 있습니다. 라우팅 선택 방법을 사용하면 루프없이 자동 관리 시스템 간에 라우팅 선택 정보를 자동으로 교환 할 수 있습니다.

20.4.1 개요

20.4.1.1 BGP 소개

BGP에서 각 경로는 네트워크 번호, 경로가 통과하는 자동 관리 시스템 목록 (as-path) 및 기타 속성 목록을 포함합니다. 우리의 스위치 소프트웨어는 BGP 4 버전을 지원합니다. BGP는 RFC1771에 정의되어 있습니다. BGP의 기본 기능은 네트워크를 교환하는 것입니다.
AS 라우팅 테이블에 대한 정보를 포함하여 다른 BGP 시스템과 연결 가능한 정보. AS 라우팅 테이블에 대한 정보는 AS 연결 그림을 구성하고 AS 연결 그림을 통해 AS 레벨 라우팅 전략을 적용하는 데 사용될 수 있습니다. BGP 버전 4는 CIDR을 지원합니다. CIDR은 요약 경로를 만들어 라우팅 테이블의 크기를 줄입니다. 따라서 수퍼 네트워크가 생성됩니다. CIDR은 BGP 네트워크 클래스의 개념을 취소하고 IP 고정-Broadcast를 지원합니다. CIDR은 OSPF, IGRP 및 RIP2를 통해 전송합니다.

EGP는 향상된 제어 기능으로 IGP와 다릅니다. BGP는 경로를 제어하기위한 여러 가지 선택적 방법을 제공합니다.

- 인접한 라우터들의 Access-list를 사용하여 유동경로의 의하여 고정경로를 필터링합니다.

- 로컬 환경설정 및 용량 MED 같은 BGP라우트들의 속성을 경로를 설정하여 수정하십시오.

- ospf 및 rip과 같은 동적 IGRP와 상호 작용하려면 distribute 명령을 사용하여 경로를 재분배합니다. 따라서 BGP 라우팅 정보가 자동 생성됩니다. BGP 경로는 수동으로 네트워크 및 집합을 구성하여 생성 할 수도 있습니다.
  BGP 경로가 생성되면 route-map을 사용하여 경로의 속성을 설정합니다.

- 시스템에서 BGP 경로의 우선 순위를 조정하여 BGP 경로의 관리 범위를 distance 명령어를 사용하여 설정하십시오.

20.4.1.2 BGP 경로 선택

BGP의 진행 절차는 경로 속성 비교에 기반합니다. 동일한 네트워크에 도달하는 경로가 여러 개인 경우 BGP는 최적의 경로를 선택합니다. 최적 경로를 선택하는 BGP 절차는 다음과 같습니다.

- 다음 홉에 도달 할 수 없는 경우, 최적 경로가 고려하게 됩니다.
- 경로가 내부 경로이고 동기화가 활성화 된 경우, 경로가 IGP에 없을 때 최적의 경로는 고려되지 않습니다.
- 최대 무게의 경로가 우선적으로 선택됩니다..
- 모든 경로의 가중치가 동일하면 우선 순위가 가장 높은 경로가 우선적으로 선택됩니다.
- 모든 경로가 동일한 로컬 우선순위를 가지면 로컬에 의해 생성 된 경로가 우선적으로 생성된 것으로 선택됩니다. 예를 들어 라우터가 네트워크 명령 또는 집계 명령을 실행하거나 IGP 경로가 전달 될 때 경로가 생성 될 수 있습니다.
- 로컬 우선 순위가 같거나 로컬 라우터에 의해 라우트가 생성되지 않으면 가장 짧은 AS 경로를 가진 라우트가 먼저 선택됩니다.
- AS 경로가 동일하면 Origin 속성 값이 가장 작은 경로 (IGP <EGP <INCOMPLETE)가 먼저 선택됩니다.
- Origin 속성 값이 같으면 MED 값이 가장 작은 경로가 먼저 선택됩니다. bgp always-compare-med가 활성화되어 있지 않으면 MED 값 비교는 동일한 인접 AS의 경로에 대한 것입니다.
- 모든 경로의 MED 값이 같으면 EBGP가 먼저 선택됩니다. 자율 시스템의 모든 경로는 IBGP로 사용됩니다.

각 경로 동일한 연결 속성을 갖는 경우 가장 작은 router-id를 가진 경로가 먼저 선택됩니다..

20.4.2 BGP 작업 구성

20.4.2.1 BGP 기본 특성 설정

BGP 구성 작업은 기본 작업과 고급 작업의 두 그룹으로 분류 할 수 있습니다. 기본 작업의 처음 두 항목은 BGP 구성에 필수 항목입니다. 기본 작업 및 고급 작업의 다른 항목은 선택 사항입니다.

0. B G P 경 로 선 택 활 성 화 하 기

글로벌 구성 모드에서 다음 명령을 실행하여 BGP 경로 선택을 활성화합니다.

명령어	설명
router bgp *autonomous-system*	라우터 설정 모드에서 BGP 라우팅 프로세스를 활성화합니다.
network *network-number/masklen [route-map route-map-name]*	네트워크를 로컬 자치 시스템으로 표시하고 BGP 테이블에 추가합니다.

노트:

1) EGP의 경우 라우터 구성 네트워크의 명령어 사용하여 IP 네트워크를 구성 할 때 어떤 네트워크가 알림을 받을 수 있는지 제어 할 수 있습니다. 그것은 IGP와 반대입니다. 예를 들어, RIP 프로토콜은 네트워크 명령을 사용하여 업데이트가 전송되는 위치를 결정합니다.

2) network 명령을 사용하여 IGP 경로를 BGP 라우팅 테이블에 추가 할 수 있습니다. 구성된 RAM과 같은 라우터 리소스가 사용 가능한 네트워크 명령의 상한을 결정합니다. 추가 선택 사항으로 redistribute 명령을 실행할 수도 있습니다.

0. BGP Neighbor 설정

외부와 라우팅 정보를 교환하려면 BGP 네이버를 설정해야 합니다.

BGP는 IBGP와 EBGP의 두 neighbor을 지원합니다. 내부 Neighbor은 같은 AS에 있습니다. 외부 Neighbor은 다른 AS가 있습니다. 일반적으로 외부 Neighbor은 밀접하게 인접 해 있으며 서브넷을 공유합니다. 내부 Neighbor는 같은 AS의 어느 곳에 나 있습니다.

라우터 명령을 사용하여 BGP neighbors를 구성합니다.

명령어	설명
neighbor {*ip-address* } **remote-as** *number*	BGP neighbor를 설계합니다.

자세한 사항은 “BGP Neighbor 설정 예제”를 참조하시기 바랍니다.

0. BGP Soft 재구성 설정

일반적으로 BGP neighbor 라우터는 연결이 생성 될 때만 모든 경로를 교환합니다. 그런 다음 변경된 경로 만 나중에 교환합니다. 구성된 라우팅 정책이 변경된 경우 변경된 라우팅 정책을 수신 된 경로에 적용하기 전에 BGP 세션을 지워야 합니다. 그러나 BGP 세션을 지우면 고속 캐시를 비활성화하고 네트워크 실행을 손상시킬 수 있습니다. BGP 세션을 지우지 않고 정책을 구성하고 활성화하는 데 도움이 되기

때문에 Soft 재구성 기능을 채택하는 것이 좋습니다. 현재, 새로운 Soft 재구성 기능은 각각의 neighbor에 적용될 수 있다. 새로운 소프트 재구성은 neighbor에 의해 생성 된 수신 업데이트에 적용되며 수신 소프트 재구성이라고 합니다. 새로운 소프트 재구성을 사용하여 출력되는 업데이트를 neighbor로 전송하는 경우 이를 출력 소프트 재구성 이라고 합니다. 입력 소프트 재구성을 실행 한 후 새 입력 정책이 유효한지 확인합니다. 출력 소프트 재구성을 실행 한 후에는 새 로컬 출력 정책이 BGP 세션을 재설정하지 않고 유효성을 검사합니다.

BGP 세션을 리셋 하지 않고 입력 된 업데이트를 생성하기 위해 로컬 BGP 세션의 라우터는 수정없이 수신 된 들어오는 업데이트를 복원해야 합니다. 입력 된 업데이트가 현재 들어오는 정책에 의해 수신되거나 거부되는지 여부는 고려 대상이 아닙니다. 이 경우 메모리가 많이 사용됩니다. 발신 재구성에는 추가 메모리 비용이 없으므로 항상 유효합니다. BGP의 다른 쪽에서 나가는 소프트 재구성을 트리거 할 수 있습니다

세션을 사용하여 새 로컬 들어오는 정책의 유효성을 검사합니다. 들어오는 소프트 재구성을 허용하려면 수신 된 모든 라우팅 업데이트를 복원하도록 BGP를 구성해야 합니다. 발신 소프트 재구성에는 사전 구성이 필요하지 않습니다.

BGP SOFT 재구성을 구성하려면 다음 명령을 실행하십시오.

명령어	설명
Neighbor { ip-address } soft-reconfiguration [inbound]	BGP soft 를 재구성하여 설정합니다.

0. BGP 연결

두 개의 라우터가 BGP Neighbor로 정의되면 BGP 연결을 만들고 경로 선택 정보를 교환합니다. BGP 라우팅 정책이 나중에 수정되거나 다른 설정이 변경되면 BGP 연결을 재설정하여 변경된 구성의 유효성을 검사해야 합니다. 다음 명령 중 하나를 실행하여 BGP 연결을 재설정하십시오

명령어	설명
clear ip bgp *	Resets 모든 BGP 연결을 재설정합니다.
clear ip bgp *address*	특정 BGP 연결을 재설정합니다.

0. BGP 와 IGPs 간의 동기화 구성

AS가 자신의 AS를 통해 세 번째 AS에서 정보를 보내는 경우, AS의 내부 라우팅 상태는 AS가 다른 AS에 boradcasting하는 라우팅 정보와 일치 해야합니다. 예를 들어, AS의 모든 라우터가 IGP를 통해 경로를 학습하기 전에 AS는 BGP에서 일부 라우터가 라우팅 할 수 없는 라우팅 정보를 수신 할 수 있습니다. BGP와 IGP 사이의 동기화는 AS 내의 모든 IGP 라우터가 라우팅 정보를 알아낼 때까지 BGP가 라우팅 정보를 Broadcast 안 한다는 것입니다. 동기화는 기본적으로 활성화됩니다.

어떤 경우에는 BGP와 IGP 간의 동기화를 수행 할 필요가 없습니다. 다른 AS가

AS를 통해 데이터를 전송하도록 허용되지 않거나 AS의 모든 라우터가 BGP를 실행하는 경우 동기화가 취소됩니다. 동기화가 취소 된 후 IGP는 몇 개의 경로를 수행 할 수 있으며 BGP는 더 빨리 집계됩니다.

동기화를 취소하려면 다음 명령을 실행하십시오.

명령어	설명
no synchronization	BGP 와 IGP. 사이에 동기화를 취소한다.

동기화를 취소 할 때 BGP 세션을 지우려면 “clear ip bgp” 명령을 실행해야 합니다.

자세한 내용은 " Neighbor 기반 BGP 경로 필터링 예제" 섹션을 참조하십시오.

일반적으로 하나 또는 두 개의 경로 만 IGP로 전달되고 IGRP의 외부 경로가 되거나 BGP 세션 스폰서가 기본 AS 경로를 생성합니다. BGP에서 IGP로 경로가 전달되면 EBGP를 통해 얻은 경로 만 전달할 수 있습니다. 대부분의 경우 IGP는 BGP에 재 배포되지 않습니다. AS에있는 네트워크는 라우터 구성 네트워크 명령어를 실행하여 나열됩니다. 따라서 네트워크가 Broadcast 됩니다. 이 방법으로 나열된 네트워크를 로컬 네트워크라고 합니다. BGP는 IGP의 origin 속성을 가집니다. 직접 연결된 경로, 고정 경로 또는 IGP에서 학습 한 경로와 같은 이러한 경로는 주 IP 라우팅 테이블에 있어야 유효합니다. BGP 라우팅 과정에서 주 IP 라우팅 테이블은 주기적으로 스캔 되어 로컬 네트워크가 존재하는지 여부를 탐지하고 이후에 BGP 라우팅 테이블이 업데이트됩니다. BGP가 경로를 포워드 할 때 주의하십시오. IGP의 경로는 BGP를 통해 다른 라우터에 전달 될 수 있습니다. BGP는 잠재적으로 정보를 IGP로 보내고 IGP는 정보를 다시 BGP로 보냅니다.

0. BGP 경로 크기 구성

BGP 경로 크기는 경로 선택 프로세스를 제어하기 위해 BGP 경로에 부여되는 번호입니다. 무게는 라우터에 대해 로컬입니다. 가중치 범위는 0에서 65535입니다. 로컬 BGP 경로의 기본 크기는 32768입니다. Neighbor에서 얻은 경로 크기는 0입니다. 관리자는 경로 크기를 수정하여 라우팅 정책을 수행 할 수 있습니다.

경로 중량을 구성하려면 다음 명령을 실행하십시오.

명령어	설명
neighbor {*ip-address* } **weight** *weight*	**모든 라우터의 크기 값을 지정합니다.**

라우트 맵을 통한 경로의 크기를 설정가능 합니다.

0. Neighbor 기반의 BGP 라우팅 필터링 구성

라우터 소프트웨어는 다음과 같은 방법으로 지정된 Neighbor 의 BGP 라우트를 필터링합니다

(1) **ip as path-list** 와 **neighbor filter-list**과 함께 **aspath** 목록 필터를 사용합니다.

명령어	설명
ip aspath-list *aspaths-list-name* {**permit | deny**} *as-regular-expression*	BGP 관련 Access-table 정의합니다.
router bgp *autonomous-system*	라우터 구성 모드를 시작합니다
neighbor {*ip-address* } **filter-list** *aspath-list-name* {**in | out** }	BGP 필터를 설정합니다.

(5) **ip access-list** 및 **neighbor distribute-list** 을 사용하여 액세스 목록을 사용합니다.

명령어	설명
ip access-list standard *access-list-name*	Defines an access list.
router bgp *autonomous-system*	Enters the router configuration mode.
neighbor {*ip-address* } **distribute-list** *access-list-name* {**in | out** }	Establishes a BGP filter.

(6) 접두사 목록을 **ip prefix-list** 및 **neighbor prefix-list**와 함께 사용하십시오.

명령어	설명
ip prefix-list *prefixs-list-name* |*sequence number* ｛**permit |deny**｝A.B.C.D/n **ge** x **le** y	prefix list를 정의합니다..
router bgp *autonomous-system*	라우터 BGP설정모드로 들어갑니다
neighbor {*ip-address* } **prefix-list**	BGP filter를 만듭니다..
prefix-list-name {**in | out**}	고정 리스트 이름의 입출력을 설정합니다.

(7) route-map 및 neighbor route-map 명령을 사용하여 route mapping을 사용합니다.

라우트 맵핑은 라우팅 속성을 필터링하고 변경할 수 있습니다.

자세한 내용은 "네이버 기반 BGP 경로 필터링 예제" 섹션을 참조하십시오.

0. 포트기반 BGP 라우트 필터링 구성하기

Access-list 이나 prefix-list를 사용하여 포트 기반 BGP 라우트 필터링을 구성 할 수 있습니다. 경로의 네트워크 번호 또는 게이트웨이 주소를 필터링 할 수 있습니다. Access-list를 사용하도록 Access-list 옵션을 지정하거나 prefix-list 을 사용하여 경로의 네트워크 번호를 필터링하려면 prefix-list 옵션을 지정할 수 있습니다. 또한 게이트웨이 옵션을 지정하여 Access-list를 사용하여 경로의 Nexthop 속성을 필터링 할 수 있습니다. access-list 옵션과 prefix-list 옵션은 함께 사용할 수 없습니다. 별표 (*)를 지정하여 모든 포트의 경로를 필터링 할 수 있습니다.

다음 명령을 실행하여 포트 기반 BGP 라우트 필터링을 구성하십시오

명령어	설명
filter interface ｛**in | out**｝〔**access-list** access-list-name〕 〔**prefix-list** prefix-list-name〕〔**gateway**	포트 기반 BGP 라우트 필터링을 구성합니다.

자세한 내용은 "포트 기반 BGP 라우트 필터링 예제" 섹션을 참조하십시오.

0. BGP-Updated Next Hop 진행중 취소하기

Neighbor 라우터의 BGP 업데이트에 대한 다음 홉 처리를 취소 할 수 있습니다. 구성은 프레임 릴레이 또는 X.25와 같은 non-broadcast 네트워크에서 유용합니다. 프레임 릴레이 또는 X.25에서 BGP 출력 라우터는 동일한 IP 서브넷의 다른 모든 neighbor 라우터에 직접 액세스 할 수 없습니다. 다음 방법은 다음 홉 처리를 취소 할 수 있습니다.

- BGP연결을 사용하는 로컬 IP주소는 출력경로의 다음 홉 주소를 사용합니다..
- 라우팅 맵을 사용하여 나가는 경로 또는 들어오는 경로의 다음 홉주소를 하십시오.

다음 홉 처리를 취소하려면 다음 명령을 실행하십시오.

명령어	**설명**
neighbor {*ip-address* } **next-hop-self**	BGP neighbor 가 업데이트 될 때 다음 홉 처리를 취소합니다.

이전 명령이 사용되면 현재 라우터는 라우트의 다음 홉으로 인식하도록 스스로 알립니다. 따라서 다른 BGP 이웃 라우터는 패킷을 현재 라우터로 보냅니다. 현재 Broadcast 라우터에서 지정된 이웃 라우터로의 경로이기 때문에 non-broadcast 네트워크에서 유용합니다. 그러나 불필요한 여분의 홉 (hop)이 발생하기 때문에 broadcast 네트워크에서는 사용빈도가 낮습니다.

20.4.2.2상위 BGP 특징 설정

0. Route map 을 통한 Route Update 필터링 및 수정

경로 맵은 각 이웃에서 경로 업데이트를 필터링하고 매개 변수의 속성을 수정하는 데 사용할 수 있습니다. 경로 맵은 들어오는 업데이트와 나가는 업데이트에 모두 적용 할 수 있습니다. 경로 업데이트를 보내거나 받을 때 경로 맵을 통과 한 경로 만 처리됩니다. 라우트 맵은 들어오는 업데이트와 나가는 업데이트가 AS 경로, 커뮤니티 및 네트워크 번호를 기반으로 한다는 것을 지원합니다. aspath-list 명령은 AS 일치에 사용되어야 합니다. 커뮤니티 일치에는 커뮤니티 목록 명령어가 필요합니다. 네트워크 옵션 맞추기 위해서는ip access-list 명령이 필요합니다

다음 명령을 실행하여 경로 맵을 통해 경로 업데이트를 필터링하고 수정하십시오.

명령어	**설명**

neighbor {*ip-address* } **route-map** *route-map-name* **{in | out}**	들어오는 경로 나 나가는 경로에 경로 맵을 적용합니다.

BGP 라우터 맵 예제로

0. aggregate 주소 속성

비 유형 필드 간 라우트는 라우팅 테이블을 최소화하기 위해 집계 라우트 (및 수퍼 네트워크)를 작성할 수 있습니다. 집계 경로를 BGP에 재분배하거나 다음 표에 설명 된 집계 속성을 사용하여 구성 할 수 있습니다. BGP 테이블에 적어도 하나 이상의 자세한 레코드가 있으면 BGP 테이블에 집계 주소를 추가하십시오.

다음 명령 중 하나 이상을 사용하여 라우팅 테이블에 집계 주소를 만듭니다.

명령어	설명
aggregate network/len	라우팅 테이블에 집계 주소를 만듭니다.
aggregate network/len **summary-only**	요약주소만 Broadcast 합니다.
aggregate network/len **route-map** map-name	라우트 맵을 통해 지정된 집계 주소를 생성합니다.

"BGP 경로 집계 예" 섹션을 참조하십시오.

0. BGP 커뮤니티 설정하기

BGP가 지원하는 라우팅 정책은 BGP 라우팅 정보에 대해 다음 세 가지 값 중 하나를 기반으로 합니다.

- 경로 망 번 호
- **AS_PATH** 속성의 값
- Value of the **COMMUNITY 속성의 값**

1. 라우트는 COMMUNITY 속성을 통해 커뮤니티로 분류 될 수 있으며 커뮤니티 기반 라우팅 정책은 라우트에 적용될 수 있습니다. 따라서
2. 라우팅 정보 제어의 구성이 간단 해진다.
3. 커뮤니티는 동일한 속성을 갖는 라우트 그룹입니다. 각 경로는 여러 커뮤니티에 속할 수 있습니다. AS 관리자는 경로가 속한 커뮤니티를 결정할 수 있습니다.
4. COMMUNITY 속성은 선택적이고 전송 가능하며 전역 적이며 범위는 다음과 같습니다.
5. 0 ~ 4,294,967,200 인터넷에서 미리 정의 된 유명한 커뮤니티는 다음 표에 나열되어 있습니다

명령어	설명

no-export	자율 시스템의 EBGP 피어를 포함하여 EBGP 피어에 대한 경로를 Broadcast 하지 않습니다.
no-advertise	모든 Peer에게 경로를 Broadcast 하지 않습니다.
local-as	자치시스템 외부로 경로를 Broadcast하지 않습니다

BGP 세션 스폰서는 라우트를 생성, 수신 또는 전달할 때 라우트 커뮤니티 속성을 설정, 추가 또는 수정할 수 있습니다. 라우트가 집계 된 후, 집계에는 모든 원래 라우트의 COMMUNITY 속성이 포함됩니다.

COMMUNITY 속성은 기본적으로 인접 항목에 전송되지 않습니다. 다음을 실행하십시오.

명령을 사용하여 COMMUNITY 속성을 지정된 neighbor으로 보냅니다.

명령어	설명
neighbor {*ip-address* } **send-community**	지정된 Neighbor에 COMMUNITY 특성을 보냅니다.

커뮤니티 속성을 설정하려면 다음 조작을 수행하십시오.

명령어	설명
route-map *map-name* *sequence-number* **{deny | permit}**	경로 맵을 구성합니다
set community *community-value*	설정 규칙을 구성합니다.
router bgp *autonomous-system*	라우터 구성 모드를 시작합니다.
neighbor {*ip-address* } **route-map** *access-list-name* {**in | out** }	경로 맵을 적용합니다.

다음 작업을 수행하여 커뮤니티 속성 기반 라우팅 정보 필터링을 구성합니다.

명령어	설명
ip community-list standard | expended *community-list-name* {**permit | deny**} *communtiy-expression*	커뮤니티 목록을 정의합니다.
route-map *map-name* *sequence-number* **{deny | permit}**	경로 맵을 구성합니다.
match *community-list-name*	일치하는 규칙을 구성합니다.
router bgp *autonomous-system*	라우터 구성모드를 시작합니다.
neighbor {*ip-address* } **route-map** *route-map-name* {**in | out** }	경로 맵을 적용합니다.

"BGP 커뮤니티 속성을 통한 라우트 맵 예제" 섹션을 참조하십시오.

0. A S A (Autonomous System Alliance) 자치 연합 시스템 구성하기

IBGP 연결을 줄이는 방법은 하나의 AS를 여러 개의 하위 AS로 나누고 이를 자치 연합시스템으로 분류하는 것입니다. 외부에 관해서는, 동맹은 AS처럼 보인다. 동맹

내부에 관해서는, 각각의 하위 AS는 완전 접속되어 있으며 동일한 연합관계에 있는 다른 하위 AS를 연결합니다. EBGP 세션이 다른 하위 AS의 Peer에 존재하더라도 IBGP peer와 마찬가지로 경로 선택 정보를 교환합니다. 즉, 다음 홉, MED 및 로컬 우선 순위 정보를 저장합니다.

BGP 자치 연합 시스템을 구성하려면 동맹 식별자를 지정해야 합니다. 연합식별자는 AS 번호입니다. 외부에 관해서는, AS는 동맹 식별자를 AS 번호로 취하는 단일 AS처럼 보입니다.

다음 명령을 실행해 자치 연합 시스템의 식별자를 구성합니다.

명령어	설명
bgp confederation0 identifier *autonomous-system*	자치 연합 시스템 의 식별자를 구성합니다.

다음 명령을 실행해 자치 연합 시스템에 속한 자치 시스템 번호를 지정합니다

명령어	설명
bgp confederation peers autonomous-system [autonomous-system ...]	자치 연합 시스템 에 속한 AS를 지정합니다.

“BGP 연합 자치 시스템 예제” 섹션을 참조하십시오.

0. Route Reflector 구성하기

IBGP 연결을 줄이는 또 다른 방법은 reflector를 구성하는 것입니다.

Route reflector의 피어는 클라이언트 peer와 AS의 다른 라우터 (비-클라이언트 피어)의 두 그룹으로 나뉩니다. Route reflector는 두 그룹 사이의 경로를 반영합니다. Route reflector 및 클라이언트 피어는 클러스터로 구성됩니다. 비-클라이언트 피어는 완전히 연결되어야 합니다. 클라이언트 피어는 완전히 연결될 필요는 없습니다. 클러스터의 클라이언트는 다른 클러스터의 IBGP 세션 스폰서와 통신하지 않습니다.

Route reflector가 라우팅 정보를 수신하면 다음 작업을 수행합니다.

- 외부 BGP 세션 스폰서의 경로를 모든 클라이언트와 비-클라이언트 피어로 Broadcast 합니다.
- 비 클라이언트 경로에서 모든 클라이언트로 경로를 Broadcast 합니다.
- 클라이언트에서 모든 클라이언트 피어 및 클라이언트 peer로 경로를 broadcast 합니다. 클라이언트 피어는 완전히 연결될 필요는 없습니다.

다음 명령을 실행하여 로컬 라우터를 Reflector로 설정하고 이웃 라우터를 클라이언트로 지정하십시오.

명령어	설명

neighbor *ip-address* **route-reflector-client**	로컬 라우터를 route-reflector로 설정하고 neighbor 클라이언트로 지정합니다.

하나의 AS에는 다중 경로 reflector가 있습니다. 경로 reflector는 IBGP 세션 스폰서를 처리 할 때 다른 **route-reflector** 를 처리합니다. 일반적으로 동일한 클러스터의 클라이언트에는 하나의 **route-reflector** 만 있습니다. 클러스터는 **route-reflector** 의 라우터 ID로 식별됩니다. 이중화를 추가하고 단일 노드의 장애를 피하려면 하나의 클러스터에 여러 개의 **route-reflector** 가 있을 수 있습니다. 이 경우 클러스터의 모든 경로 reflector를 4 비트 클러스터 ID로 설정해야 경로 reflector가 동일한 클러스터의 다른 경로 reflector의 업데이트 정보를 식별 할 수 있습니다. 동일한 클러스터의 모든 **route-reflector** 는 완전히 연결되어 있고 동일한 클라이언트 피어 및 비 클라이언트 peer를 가지고 있어야합니다.

route-reflector 가 클러스터에 있으면 다음 명령을 실행하여 ID를 구성하십시오.

명령어	설명
bgp cluster-id *cluster-id*	cluster ID를 구성합니다..

“BGP Route Reflector 구성 예제”섹션을 참조하십시오.

0. peers 종료하기

BGP neighbors에 shutdown 명령어를 실행합니다.

명령어	설명
neighbor {ip-address } **shutdown**	BGP neighbor에 shutdown을 실행합니다..

Run the following command to activate the neighbor:

명령어	설명
no neighbor {ip-address } **shutdown**	BGP neighbor.활성화합니다.

0. 멀티-홉 외부의 피어 구성하기

외부 피어는 기본적으로 직접 연결된 망에 있어야합니다.
다음 명령을 실행하여 멀티 홉 외부 피어를 구성합니다.

명령어	설명
neighbor {ip-address } **ebgp-multihop** ttl	BGP의 neighbor를 멀티 홉 외부 peer로 설정합니다.

0. BGP 관리 경로 설정하기

관리 거리는 라우팅 프로토콜의 우선 순위를 측정하는 단위입니다. BGP는 외부 거리, 내부 거리 및 로컬 거리 등 3 가지 종류의 관리 거리를 사용합니다. 외부 BGP에서 학습 한 경로는 외부 거리를 보여줍니다.

내부 BGP에서 학습 한 경로는 내부 거리를 보여줍니다. 로컬 경로에는 로컬 거리가 표시됩니다. BGP 경로 관리 거리를 설정하려면 다음 명령을 실행하십시오.

명령어	설명
distance bgp external-distance internal-distance local-distance	BGP route 관리 거리를 설정합니다..

BGP 경로의 관리 거리를 수정하는 것은 위험합니다. 외부 거리는 모든 동적라우팅 프로토콜의 거리보다 짧아야 합니다. 내부 거리는 모든 동적 라우팅 프로토콜의 거리보다 길어야 합니다.

0. BGP timer 수정하기

BGP keepalive 및 hold-time timer를 수정하려면 다음 명령을 실행하십시오.

명령어	설명
neighbor *[ip-address | peer group-name]* **timers** *keepalive holdtime*	설계된 피어 또는 피어 그룹의 keepalive 및 holdtime 타이머를 설정합니다 (단위 : 초).

no neighbor timer 명령을 실행하여 BGP neighbor 또는 피어 그룹의 타이머를 기본값으로 다시 시작합니다.

0. 다른 AS의 경로 MED 비교

MED는 여러 경로 중에서 최적의 경로를 선택해야 할 때 고려되는 매개 변수입니다. 비교적 작은 MED 값을 가진 경로가 먼저 고려됩니다.

기본적으로 최상의 경로가 선택 될 때 MED 비교는 동일한 AS의 경로 중에서 만 수행됩니다. 경로 선택에 상관없이 MED를 비교할 수 있도록 구성 할 수 있습니다.

다른 AS의 경로 간 MED 비교를 수행하려면 다음 명령을 실행하십시오.

명령어	설명
bgp always-compare-med	AS의 경로 간 MED 비교를 수행합니다.

20.4.3 BGP 모니터링과 유지보수하기

관리자는 BGP의 라우팅 테이블이나 다른 데이터베이스의 내용을 찾아보고 삭제할 수 있습니다. 세부 통계 정보의 값을 표시 할 수 있습니다.

0. BGP 라우팅 테이블 및 데이터베이스 지우기

관리 모드에서 다음 명령을 실행하여 고속 캐시, 테이블 또는 BGP 데이터베이스 지우기 관련 작업을 수행합니다.

명령어	설명
clear ip bgp *	모든 BGP 연결을 재설정합니다.
clear ip bgp *as-number*	지정된 자율 시스템의 BGP 연결을 재설정합니다.
clear ip bgp *address*	지정된 이웃의 BGP 연결을 재설정합니다.
clear ip bgp *address* **soft** {**in|out**}	지정된 이웃의 들어오는 또는 나가는 데이터베이스를 지웁니다.
clear ip bgp *aggregates*	경로 집계 중에 생성 된 경로를 지웁니다.
clear ip bgp *networks*	네트워크 명령에 의해 생성 된 경로를 지웁니다.
clear ip bgp *redistribute*	프로세서 전달중 생성 된 경로를 지웁니다.

0. 라우팅 테이블 및 시스템 통계 정보 표시

BGP 라우팅 테이블 및 데이터베이스와 같은 자세한 통계 정보를 나타낼 수 있습니다. 이러한 통계 정보는 네트워크 리소스를 완전히 사용하고 네트워크 문제를 해결하는 데 도움이 됩니다.

다른 통계 정보를 표시하려면 다음 명령을 실행하십시오.

명령어	설명
show ip bgp	시스템에 BGP route table을 보여줍니다..
show ip bgp prefix	접두부 일치하는 목록과 일치하는 경로를 표시합니다.
show ip bgp community	커뮤니티 속성에 대한 통계 정보를 표시합니다.
show ip bgp regexp *regular-expression*	정규 표현식과 일치하는 경로를 표시합니다.
show ip bgp *network*	지정된 BGP 경로를 표시합니다.
show ip bgp neighbors *address*	지정된 이웃의 TCP 연결 및 BGP 연결에 대한 자세한 정보를 표시합니다.
show ip bgp neighbors *[address]* [received-routes | routes | advertised-routes]	특정한 BGP neighbor로부터 배운 경로를 표시합니다.
show ip bgp paths	모든 BGP 경로 정보를 데이터베이스에 표시합니다.
show ip bgp summary	모든 BGP 연결 상태를 표시합니다.

0. BGP 정보 추적하기

오류를 찾아서 문제를 해결하려면 BGP 연결 추적, BGP 정보를 추적하여 경로 수신 및 경로 전달을 관찰해야 합니다. 다음 작업을 수행하십시오.

Command	설명
debug ip bgp *	일반적인 BGP 정보를 추적합니다
debug ip bgp all	모든 BGP 정보를 추적합니다
debug ip bgp fsm	BGP 기계 상태를 추적합니다
debug ip bgp keepalive	BGP Keepalive 메시지를 추적합니다
debug ip bgp open	BGP open 메시지를 추적합니다
debug ip bgp update	BGP 업데이트 메시지를 추적합니다.

20.4.4 BGP 구성 예제

0. BGP route-map 예제

다음 예에서는 route-map을 사용하여 들어오는 경로의 속성을 이웃 라우터에서 수정하는 방법을 보여줍니다. 인접 라우터 140.222.1.1에서 수신 한 모든 경로의 가중치를 설정하고 ASPATH 액세스 목록 aaa를 200으로 일치시킵니다. 로컬 우선 순위를 250으로 설정합니다. 경로가 거부되면 다른 경로가 거부됩니다.

router bgp 100

!

```
 neighbor 140.222.1.1 route-map fix-weight in
 neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight permit 10
 match as-path aaa
 set local-preference 250
 set weight 200
!
ip aspath-list aaa permit ^690$
ip aspath-list aaa permit ^1800
```

다음 예에서 경로 맵 freddy의 첫 번째 항목은 자치 시스템 690에서 시작하는 모든 경로의 MED 속성을 127로 설정합니다. 두 번째 항목은 이전 조건을 만족하지 않는 경로를 인접 라우터 1.1.1.1로 전송합니다.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
ip aspath-list abc permit ^690_
ip aspath-list xyz permit .*
!
route-map freddy permit 10
 match as-path abc
 set metric 127
!
route-map freddy permit 20
match as-path xyz
```

다음은 route-map을 통해 전달해서 생성 된 경로를 수정하는 방법을 보여줍니다.

```
router bgp 100
 redistribute rip route-map rip2bgp
!
 route-map rip2bgp
 match ip address rip
 set local-preference 25
 set metric 127
 set weight 30000
 set next-hop 192.92.68.24
 set origin igp
!
```

```
ip access-list standard rip
 permit 131.108.0.0 255.255.0.0
 permit 160.89.0.0 255.255.0.0
 permit 198.112.0.0 255.255.128.0
```

0. BGP neighbor 설정 예

다음 예에서 BGP 라우터는 AS109에 속합니다. AS109는 두 개의 네트워크를 구축합니다. 라우터에는 외부 이웃 (다른 AS에 있음), 내부 이웃 (동일한 AS 번호로) 및 외부 이웃 등 3 개의 이웃이 있습니다.

```
router bgp 109
 network 131.108.0.0
 network 192.31.7.0
 neighbor 131.108.200.1 remote-as 167
 neighbor 131.108.234.2 remote-as 109
 neighbor 150.136.64.19 remote-as 99
```

0. neighbor-기반 BGP 경로필터의 예

다음은 neighbor 기반 BGP 경로 필터링의 예입니다. as-path의 액세스 목록 test1을 통과하는 라우트는 가중치 100을 얻습니다. as-path의 액세스 목록 test2를 통해 도달하는 라우트만 이웃 193.1.12.10으로 전송 될 수 있습니다.

마찬가지로 액세스 목록 test3을 통과하는 경로는 이웃 라우터 193.1.12.10에서 허용 할 수 있습니다.

```
router bgp 200
 neighbor 193.1.12.10 remote-as 100
 neighbor 193.1.12.10 filter-list test1 weight 100
 neighbor 193.1.12.10 filter-list test2 out
 neighbor 193.1.12.10 filter-list test3 in
ip aspath-list test1 permit _109_
ip aspath-list test2 permit _200$
ip aspath-list test2 permit ^100$
ip aspath-list test3 deny _690$
ip aspath-list test3 permit .*
```

0. 포 트 -based BGP의 route필터 예

다음 예에서는 포트 e1 / 0의 경로가 액세스를 통해 필터링 됨을 보여줍니다.

```
router bgp 122
 filter vlan10 in access-list acl
```

다음 예에서는 액세스 목록 filter-network 및 액세스 목록 filter-gateway를 사용하여 포트 번호 e1 / 0에서 경로를 동시에 필터링하여 네트워크 번호와 게이트웨이 주소를 각각 필터링하는 방법을 보여줍니다.

```
router bgp 100
 filter vlan100 in access-list filter-network gateway filter-gateway
```

다음 예는 prefix list filter-prefix와 prefix list filter-gateway를 사용하여 네트워크 번호와 게이트웨이 주소를 각각 필터링하여 포트에서 동시에 경로를 필터링하는 방법을 보여줍니다.

```
router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway
```

0. prefix-list 기반 경로 필터 구성 예

다음 예는 기본 경로 0.0.0.0 /0가 거부되었음을 보여 줍니다.

```
ip prefix-list abc deny 0.0.0.0/0
```

다음 예는 prefix- 35.0.0.0/8과 일치하는 경로가 허용됨을 보여줍니다.

```
ip prefix-list abc permit 35.0.0.0/8
```

다음 예제에서는 / 8에서 / 24 사이의 길이를 가진 prefix만 BGP 프로세스에서 허용됩니다.

```
router bgp
 network 101.20.20.0
 filter * in prefix max24
!
 ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

다음 예에서 라우터는 모든 경로를 필터링하고 prefix 길이가 8~ 24 사이 인 경로 만 허용합니다.

```
router bgp 12
 filter * in prefix-list max24
 !
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

다음 예는 prefix 길이가 24 이하인 경로가 망 192/8에서 허용됨을 보여줍니다.

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

다음 예는 prefix 길이가 25를 초과하는 경로가 망 192/8에서 허용됨을 보여줍니다.

ip prefix-list abc deny 192.0.0.0/8 ge 25

다음 예는 prefix 길이가 8보다 크고 24보다 작은 경로가 허용됨을 보여줍니다.

ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24

다음 예는 접두사 길이가 25를 초과하는 경로가 거부되었음을 보여줍니다.

ip prefix-list abc deny 0.0.0.0/0 ge 25

다음 예는 네트워크 10/8의 모든 경로가 거부되었음을 보여줍니다.
A 클래스 네트워크 10.0.0.0/8의 마스크가 32 비트보다 작거나 같으면
모든 경로가 거부됩니다.

ip prefix-list abc deny 10.0.0.0/8 le 32

다음 예에서는 네트워크 204.70.1 / 24의 마스크 길이가 25를 초과하므로 모든 경로가 거부되었음을 보여줍니다.

ip prefix-list abc deny 204.70.1.0/24 ge 25

다음 예는 모든 경로가 허용됨을 보여줍니다.:

ip prefix-list abc permit any

0. BGP 집합 경로 예

다음 예는 경로 전달 또는 조건부 경로 집계 기능을 통해 BGP에서 집계 경로를 생성하는 방법을 보여줍니다.

다음 예는 명령어 **redistribute static 는 통합경로** 193. * . * . * 으로 전송하는데 사용됩니다.

```
ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

라우팅 테이블의 하나 이상의 경로가 지정된 범위에 속하면 다음 구성에 따라

BGP 라우팅 테이블에 집계 경로가 만들어집니다. 집계 경로는 사용자 AS의 것으로 간주되며 표시 정보에서 손실 될 수 있는 atomic 속성을 가집니다.

router bgp 100

aggregate 193.0.0.0/8

다음 예는 집계 경로 193. *. *. *을 만드는 방법과 Broadcast 에서 모든 Neighbor 라우터에 대한 자세한 경로를 제한하는 방법을 보여줍니다.

router bgp 100

aggregate 193.0.0.0/8 summary-only

0. BGP 경로 reflector 구성 예

다음은 경로 reflector 구성의 예입니다. RTA, RTB, RTC 및 RTE는 동일한 자치 시스템 AS 200에 속합니다. RTA는 경로 reflector 역할을 하지만 RTB 및 RTC는 경로 reflector 기능을 담당합니다. RTE는 일반적인 IBGP 이웃입니다. RTD는 AS100에 속하며 RTA와의 EBGP 연결을 설정합니다. 구성은 다음과 같습니다.

RTA 구성:

```
interface vlan110
ip address 2.0.0.1 255.0.0.0
!
interface vlan111
ip address 3.0.0.1 255.0.0.0
!
interface vlan112
ip address 4.0.0.1 255.0.0.0
!
interface vlan113
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200    /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200    /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200    /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100    /*RTD EBGP*/
network 11.0.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

RTB 구성 :

```
interface vlan110
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200    /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

RTC 구성 :

```
interface vlan110
  ip address 2.0.0.2 255.0.0.0
  !
```

```
router bgp 200
neighbor 2.0.0.1 remote-as 200    /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

RTD 구성:

```
interface vlan110
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200    /*RTA EBGP*/
network 14.0.0.0/8
 !
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

RTE구성:

```
interface vlan110
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200    /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12
```

0. BGP 자율 결합 시스템의 예

다음 그림은 자치 결합 시스템 구성을 보여줍니다. RTA, RTB 및 RTC는 IBGP 연결을 만듭니다. RTA, RTB 및 RTC는 사설 자치 시스템 65010에 속합니다. RTE는 사설 자치 시스템 65020에 속합니다. RTE 및 RTA는 자치 결합 시스템 에서 EBGP 연결을 설정합니다.

AS65010 및 AS65020은 자치 결합 시스템을 구성합니다. 자치 결합 시스템 의 번호는 AS 200입니다. RTD는 AS100에 속합니다. RTA를 통해 RTD와 AS200 간에 EBGP 연결이 설정됩니다.

RTA 구성:

```
interface vlan110
ip address 1.0.0.1 255.0.0.0
```

```
!
interface vlan111
ip address 2.0.0.1 255.0.0.0
!
interface vlan112
ip address 4.0.0.1 255.0.0.0
!
interface vlan113
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010   /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010   /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020   /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100     /*RTD EBGP*/
```

RTB 구성:

```
interface vlan110
ip address 1.0.0.2 255.0.0.0
!
interface vlan111
ip address 3.0.0.1 255.0.0.0
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.1 remote-as 65010   /*RTA IBGP*/
neighbor 3.0.0.2 remote-as 65010   /*RTC IBGP*/
```

RTC 구성:

```
interface vlan110
ip address 2.0.0.2 255.0.0.0
!
interface vlan111
ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
```

```
bgp confederation peers 65020
neighbor 2.0.0.1 remote-as 65010   /*RTA IBGP*/
neighbor 3.0.0.1 remote-as 65010   /*RTB IBGP*/
```

RTD 구성:

```
interface vlan110
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200   /*RTA EBGP*/
```

RTE 구성:

```
interface vlan110
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010   /*RTA EBGP*/
```

0. route-map BGP community 특성의 예

다음의 예는 명령어 **route map set-community** 을 neighbor의 나가는 경로 171.69.232.50를 사용합니다. 특정 커뮤니티 속성 값 no-export는액세스 목록 aaa의 경로를 통해 설정할 수 있습니다. 다른 경로는 정상적인 Broadcast를 수행합니다. 특정 속성 값은 AS200의 BGP가 자동으로 자율 시스템 외부로 경로를 Broadcasting 하는 것을 방지합니다.

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
 route-map set-community 10 permit
 match ip address aaa
 set community no-export
 !
 route-map set-community 20 permit
```

다음 예에서 route map set-community 명령어는 neighbor 171.69.232.90의 출력 경로를 업데이트하는 데 사용됩니다. 현재 값을 커뮤니티 속성 값 200으로 설정하십시오. 다른 경로는 정상 Broadcasting를 수행합니다.

route-map bgp 200

neighbor 171.69.232.90 remote-as 100

neighbor 171.69.232.90 send-community

neighbor 171.69.232.90 route-map set-community out

route-map set-community 10 permit

match as-path test1

set community-additive 200 200

route-map set-community 20 permit

match as-path test2

ip aspath-list test1 permit 70$

ip aspath-list test2 permit .*

다음 예는 경로의 MED 및 로컬 우선 순위를 인접 라우터에서 설정합니다.

커뮤니티 속성 값에 따라 171.69.232.55. 커뮤니티 목록 com1과 일치하는 모든 경로의 MED를 8000으로 설정합니다. 이 경로에는 커뮤니티 값이 "100 200 300"및 "900 901"인 경로가 포함될 수 있습니다. 이러한 경로에는 다른 속성 값이 있을 수 있습니다.

커뮤니티 목록 com2를 보내는 경로의 로컬 우선 순위를 500으로 설정합니다.

다른 경로의 로컬 우선 순위를 50으로 설정하십시오. 따라서 이웃 171.69.232.55의 나머지 모든 경로의 모든 로컬 우선 순위 값은 50입니다.

router bgp 200

neighbor 171.69.232.55 remote-as 100

neighbor 171.69.232.55 route-map filter-on-community in

route-map filter-on-community 10 permit

match community com1

set metric 8000

route-map filter-on-community 20 permit

match community com2

set local-preference 500

route-map filter-on-community 30 permit

set local-preference 50

ip community-list com1 permit 100 200 300

ip community-list com1 permit 900 901

ip community-list com2 permit 88

ip community-list com2 permit 90

21장. VRRP 구성

21-1장 VRRP 구성

21.1.1 개요

VRRP (Virtual Router Redundancy Protocol)는 기본 정적 라우팅 조건에서 성공적인 단일 노드 서비스를 보장합니다. VRRP는 정적으로 지정된 게이트웨이의 결함을 방지합니다. 스위치 그룹은 VRRP를 통해 가상 스위치로 함께 작동 할 수 있습니다. 가상 스위치에는 외부 IP 주소 및 가상 MAC 주소가 있습니다. VRRP는 스위치 그룹에서 하나의 스위치를 마스터 스위치로 선택하여 패킷 전달을 담당합니다. 마스터 스위치에 문제가 발생하면 대기 스위치는 기본 게이트웨이 주소를 변경하지 않고 즉시 마스터 스위치의 작업을 인계합니다. 전체 인계 프로세스는 터미널 시스템에 투명합니다. 이 메커니즘은 문제가 발생했을 때 빠르고 효과적인 해결책을 제공 할 수 있습니다.

21.1.2 VRRP 작업 구성

- 포트에서 VRRP 활성화 / 비활성화
- VRRP 인증 모드 구성
- VRRP 우선 순위 선점 구성
- VRRP 우선 순위 구성
- VRRP 클럭 값 구성
- VRRP 모니터링 및 유지 관리

21.1.3 VRRP 작업 구성

21.1.3.1 포트에서 VRRP의 활성화와 비활성화

포트 구성 모드에서 다음 명령을 실행하십시오.

명령어	**설명**
vrrp *vrid* **associate** *virtual-address*	포트에 VRRP를 삽입합니다.
no vrrp *vrid*	VRRP를 기본 상태로 다시 시작합

VRRP의 가상 주소가 구성된 후에 가상 스위치가 활성화됩니다. 포트의 가상 주소와 기본 IP 주소는 동일한 네트워크 세그먼트에 있어야합니다. 그렇지 않으면 가상 스위치가 Init 상태로 유지됩니다. 가상 스위치는 포트의 기본 마스크를 마스크로 사용하기 때문에 가상 주소에 대한 마스크를 구성 할 필요가 없습니다. 포트의 가상 주소와 기본 IP 주소가 같으면 시스템은 가상 스위치의 우선 순위를 자동으로 255로 설정합니다.

VRRP 기능은 기본적으로 비활성화되어 있습니다.

21.1.3.2 VRRP 인증 모드 구성

포트 구성 모드에서 다음 명령을 실행하십시오.

명령어	**설명**

vrrp *vrid* **authentication** {**no-authen**|**simple-text** *string*} **(word)**	VRRP 인증 모드를 구성하십시오.
no vrrp ***vrid*** **authentication**	VRRP 인증 모드를 기본 상태로 다시 시작합니다.

단순 텍스트 인증 모드에서는 인증 문자열이 메시지에 명확한 코드로 포함되어 전달됩니다. 수신자는 메시지의 인증 문자열을 확인하여 로컬로 구성된 인증 문자열과 일치하는지 확인합니다. 기본 상태에서 VRRP의 인증 모드는 no-authen입니다.(인증문자열은 최대 8자 입니다)

21.1.3.3 VRRP 우선 순위 선점 구성

포트 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
vrrp *vrid* **preempt** {**on** | **off | delay**}	VRRP 우선 순위 선점을 구성하십
no vrrp *vrid* **preempt**	기본 VRRP 우선 순위 우선 모드를 다시 시작하십시오.

우선 순위 선점은 백업 스위치에만 유효합니다. 백업 스위치가 마스터 스위치에서 알림 메시지를 받으면 마스터 스위치의 우선 순위를 검사합니다. 마스터 스위치의 우선 순위 수준이 로컬로 구성된 우선 순위 수준보다 낮고 백업 스위치가 우선 선점 방식으로 구성된 경우 백업 스위치는 백업 상태에서 마스터 상태로 실행하고 알림 메시지를 외부로 보냅니다. 그렇지 않으면 백업 스위치가 백업 상태로 유지됩니다.

기본 모드는 우선 순위 선점입니다.

21.1.3.4 VRRP 우선순위 구성하기

포트 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
vrrp *vrid* **priority** *value* **(1~254)**	VRRP의 우선순위를 구성합니다.
no *vrid* **priority**	기본값으로 다시 시작하십시오.

가상 주소와 포트가 같으면 VRRP는 자동으로 우선순위 값을 255로 증가시킵니다.
가상 주소 나 포트가 변경되면 우선 순위 값이 자동으로 원래 값으로 재개됩니다.

기본값은 100입니다.

21.1.3.5 VRRP 클럭 값 구성

포트 구성 모드에서 다음 명령을 실행하십시오

명령어	설명
vrrp *vrid* **timer advertisement** *value*	VRRP 클럭 값을 구성하십시오.
no vrrp *vrid* **timer advertisement**	VRRP 클럭 값을 기본값으로 다시 시작하십시오.

클럭 값은 가상 스위치가 문제로부터 생존하는 데 필요한 최단 시간을 결정합니다. 마스터 스위치가 고장 나면 백업 스위치는 3 * advertisement + skew_time 간격 후에 마스터 스위치로 작동합니

다. 광고하는 클럭의 값이 크면 시스템
복구에 좋지 않습니다. 기본값이 권장됩니다.

기본값은 1 초입니다.

21.1.3.6 VRRP을 유지하고 모니터링하기

포트 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
show vrrp *vrid* [**interface** *vlan_intf*]	VRRP 정보를 표시합니다.
[**no**] **vrrp** { **packet** | **event** }	VRRP 패킷 및 이벤트에 대한 디버깅 켜기 / 끄기를 활성화 또는 비활성화합니다.

다음과 같은 VRRP 정보를 나타낸다:

switch#show vrrp 1

VLAN1 (192.168.20.118, 255.255.255.0 00e0.0f42.0000)
group id: 1

state: Master

virtual mac address: 0000.5e00.0101

priority: 100

preempt: on

authentication: no-authen

advertisement interval: 1

associate IP address: 192.168.20.110

advertisement timer expiry: 1

21.1.3.7 VRRP 구성의 예

네트워크 토폴로지는 그림 1-1에 나와 있습니다

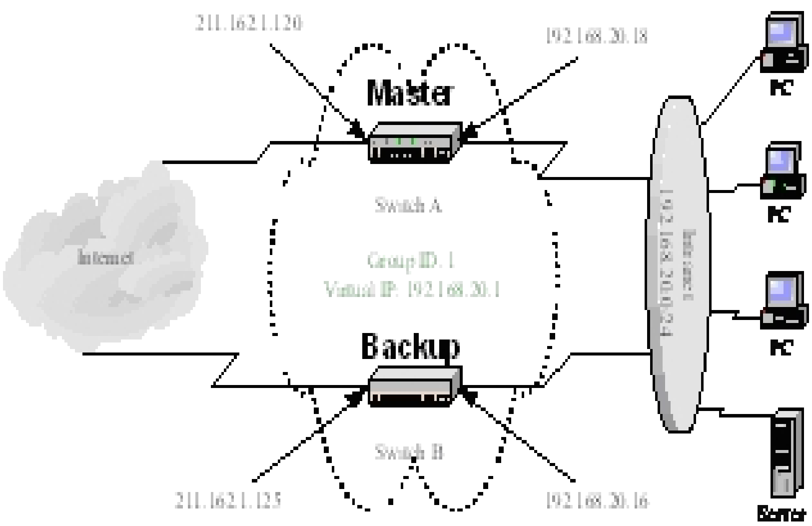


그림 1-1 네트워크 토폴로지

1. 스위치 A 구성하기

사설 네트워크의 인터페이스에 대한 주소를 구성하십시오.

Switch_config_v1# ip address 192.168.20.18 255.255.255.0

공용 네트워크의 인터페이스에 대한 주소를 구성하십시오.

Switch_config_v2#ip address 211.162.1.120 255.255.255.0

개인 네트워크의 인터페이스에서 가상 스위치 그룹 1을 구성합니다.
가상 주소는 192.168.20.1입니다. 우선 순위 값은 120입니다.

Switch_config_v1#vrrp 1 associate 192.168.20.1 Switch_config_v1#vrrp 1 priority 120

가상 스위치에 대한 정보를 표시합니다.

Switch_config# show vrrp

VLAN1 (192.168.20.18,255.255.255.0 00e0.0f42.0000)

group id: 1

state: Master

virtual mac address: 0000.5e00.0101

priority: 120

preempt: on

authentication: no-authen

advertisement interval: 1

associate IP address: 192.168.20.1

advertisement timer expiry: 1

2. 스위치 B 구성하기

(1) 사설 네트워크의 인터페이스에 대한 주소를 구성하십시오.

Switch_config_v1# ip address 192.168.20.16 255.255.255.0

(2) 공용 네트워크의 인터페이스에 대한 주소를 구성하십시오.

Switch_config_v2#ip address 211.162.1.125 255.255.255.0

개인 네트워크의 인터페이스에서 가상 스위치 그룹 1을 구성합니다. 가상 주소는 192.168.20.1입니다. 우선 순위 값이 기본값입니다.

Switch_config_v1#vrrp 1 associate 192.168.20.1 Display information about the virtual switch:

Switch_config#show vrrp

VLAN1 (192.168.20.16,255.255.255.0 00e0.0f42.0000)

group id: 1

state: Backup

virtual mac address: 0000.5e00.0101

priority: 100

preempt: on

authentication: no-authen

advertisement interval: 1

associate IP address: 192.168.20.1

advertisement timer expiry: 1

3. 사설 네트워크의 PC 및 서버 구성

사설 네트워크의 각 PC 및 서버에 대한 기본 게이트웨이를 192.168.20.1로 구성하십시오.

22장 Multicast 개요

22-1장 Multicast 개요

이 장에서는 Multicast 라우팅 프로토콜을 구성하는 방법에 대해 설명합니다. Multicast 라우팅 명령에 내용은 " Multicast 라우팅 명령" 부분을 참조하십시오.

전통적인 IP 전송은 하나의 호스트 만 단일 호스트와 통신하거나 (unicast 통신) 모든 호스트와 통신 할 수 있습니다 (Broadcast 통신). Multicast 기술을 사용하면 한 호스트가 일부 호스트에 메시지를 보낼 수 있습니다. 이 호스트는 그룹 구성원 이라고 합니다.

그룹 구성원에게 전송 된 메시지의 대상 주소는 D 클래스 주소 (224.0.0.0 ~ 239.255.255.255)입니다. Multicast 메시지는 UDP와 같이 전송됩니다. TCP처럼 신뢰할 수 있는 전송 및 오류 제어를 제공하지 않습니다. 발신자와 수신자는 Multicast 응용 프로그램을 구성합니다. 보낸 사람은 그룹에 가입하지 않고 Multicast 메시지를 보낼 수 있습니다. 그러나 수신자는 그룹의 메시지를 받기 전에 그룹에 가입해야 합니다. 그룹 구성원 간의 관계는 동적입니다. 호스트는 언제든지 그룹에 가입하거나 그룹에서 탈퇴 할 수 있습니다. 그룹 회원의 위치와 번호에는 제한이 없습니다. 필요한 경우 호스트는 여러 그룹의 구성원이 될 수 있습니다. 따라서 그룹의 상태와 그룹 구성원의 수는 시간에 따라 다릅니다.

IP Multicast 기술은 일 대 다 멀티미디어 응용 프로그램에 적합합니다.

22.1.1 Multicast 라우팅 인식

우리 라우터의 라우터 소프트웨어에서 Multicast 라우팅에 다음 사항이 포함됩니다.

- IGMP는 LAN에서 라우터와 호스트 간에 실행되며 그룹 구성원 관계를 추적하는 데 사용됩니다.
- OLNK는 간단한 토폴로지에서 사용되는 정적 Multicast 기술입니다. Multicast 포워딩을 실현하고 CPU와 대역폭을 효과적으로 절약합니다.
- PIM-DM, PIM-SM 및 DVMRP는 동적 Multicast 라우팅 프로토콜입니다. 라우터 간에 실행되며 Multicast 라우팅 테이블을 만들어 Multicast 전달을 실현합니다.

22.1.2 Multicast 구성 작업 목록

22.1.2.1 기본 Multicast 구성 작업 목록

- Multicast 라우팅 시작 (필수)
- TTL 임계 값 구성 (선택 사항)

- 고속 multicast 전달 취소 (선택 사항)
- 정적 multicast 경로 구성 (선택 사항)
- Multicast 경계 구성 (선택 사항)
- Multicast 도움 구성 (선택 사항)
- Stub Multicast 경로 구성 (선택 사항)
- Multicast 경로 모니터링과 유지 관리 (선택 사항)

22.1.2.2 IGMP 구성 작업 목록

- 현재 버전의 IGMP 수정
- IGMP 쿼리 간격 구성
- IGMP Querier 간격 구성
- IGMP의 최대 응답 시간 구성
- 마지막 IGMP 그룹 구성원의 쿼리 간격 구성
- 정적 IGMP 구성
- IGMP 즉시 제거 목록 구성

22.1.2.3 PIM-DM 구성 작업 목록

- 타이머 조절하기
- PIM-DM 버전 지정
- 상태 다과 구성하기
- 여과 목록 구성
- DR 우선 순위 설정
- 정보 (S, G) 삭제

22.1.2.4 PIM-SM 구성 작업 목록

- 정적 RP 구성
- 대기 BSR 구성

- 대기 RP 구성
- PIM-SM Multicast 라우팅 표시
- PIM-SM에서 학습한 Multicast 경로 지우기

22.1.2.5 DVMRP 구성 작업 목록

- 경로 요약 구성
- 포트의 필수적인 leaf-node 구성
- 경로 필터 구성
- DVMRP Unicast 경로 표시
- DVMRP multicast 경로 표시
- DVMRP에서 학습한 multicast경로 지우기

22-2장 기본 Multicast 라우팅 구성

22.2.1 Multicast 라우팅 시작하기

라우터 소프트웨어가 Multicast 메시지를 전달할 수 있게 하려면 Multicast 라우팅을 시작해야 합니다. 전역 구성 모드에서 다음을 실행하여 Multicast 메시지 전달을 시작합니다.

명령어	설명
ip multicast-routing	IP 라우팅 Multicast 시작하기

22.2.2 포트에서 Multicast 기능 설정하기

Multicast 라우팅 프로토콜이 포트에서 실행되면 IGMP가 해당 포트에서 활성화됩니다. Multicast 라우팅 프로토콜에는 OLNK, PIM-DM, PIM-SM 및 DVMRP가 포함됩니다.
하나의 Multicast 라우팅 프로토콜 만 동일한 포트에서 실행되도록 허용됩니다. 라우터가 여러 Multicast 도메인을 연결하면 다른 포트에서 다른 Multicast 프로토콜을 실행합니다.
라우터 소프트웨어가 Multicast 경계 라우터 (MBR)로 작동 할 수는 있지만. 가능하다면 여러 Multicast 라우팅 프로토콜을 동일한 라우터에서 동시에 실행하지 마십시오.
일부 Multicast 라우팅 프로토콜의 경우 심각한 영향을 받을 수 있습니다.
예를 들어, PIM-DM과 BIDIR PIM-SM이 동시에 실행되면 혼동이 발생합니다.

22.2.2.1 OLNK 시작하기

포트 구성 모드에서 다음 명령을 실행하여 Multicast 라우팅을 시작합니다.

명령어	설명
ip olnk	Multicast 라우팅을 시작합니다..

22.2.2.2 PIM-DM 시작하기

다음 실행하여 포트에서 PIM-DM으로 multicast dense 기능을 활성화합니다.

명령어	설명
ip pim-dm	PIM-DM이 실행중인 포트를 입력 한 다음 포트 구성 모드에서 PIM-DM Multicast 라우팅 프로세스를 활성화합니다.

22.2.2.3 PIM-SM 시작하기

포트에 PIM-DM을 실행하고 PIM-DM Multicast를 활성화하려면 다음 작업을 수행하십시오.

명령어	설명

ip pim-sm	PIM-SM을 실행해야 하는 포트로 들어가고 포트 구성 모드에서 PIM-SM Multicast 라우팅 프로세스를 활성화합니다.

22.2.3 TTL 임계 값 구성

ip multicast ttl-threshold 명령을 실행하여 포트를 통과 할 수 있는 Multicast 메시지의 TTL 임계 값을 구성합니다. 기본 임계 값 1을 사용하려면 no ip multicast ttl-threshold 명령을 실행하십시오.

명령어	설명
ip multicast ttl-threshold *ttl-value*	포트에 TTL 임계 값을 구성합니다.

예제

다음 예에서는 관리자가 포트에서 TTL 임계 값을 구성하는 방법을 보여줍니다.

interface ethernet 1/0

ip multicast ttl-threshold 200

22.2.4 빠른 Multicast 전달기능을 취소하기

ip multicast mroute-cache 명령을 실행하여 포트에서 빠른 Multicast 전달 기능을 구성합니다. 빠른 Multicast 전달 기능을 취소하려면 no ip multicast mroute-cache 명령을 실행하십시오.

명령어	설명
ip multicast mroute-cache	포트에 빠른 Multicast 전달을 실행합니다.

예제

다음 예는 관리자가 포트에서 고속 Multicast 전달 기능을 취소하는 방법을 보여 줍니다.

interface ethernet 1/0

no ip mroute-cache

22.2.5 수동 Multicast 경로 구성

정적 Multicast 경로는 Multicast 전달 경로가 Unicast 경로와 다른 것을 허용합니다. RPF 검사는 Multicast 메시지가 전달 될 때 수행됩니다. 메시지를 받는 실제 포트는 예상했던 수신되는 포트입니다. 즉, 포트는 보낸 사람에게 도달하는 Unicast 경로의 Next-hop 포트입니다. Unicast 토폴로지가 Multicast 토폴로지와 동일하면 RPF 검사가 합리적입니다. 경우에 따라 Unicast 경로는 Multicast 경로와 달라야 합니다. 터널 기술을 예로 들어 보겠습니다. 경로의 라우터가 Multicast 프로토콜을 지원하지 않을 경우 해결 방법은 두 개의 경로 사이에 GRE 터널을 구성하는 것입니다. 다음 그림에서 각 Unicast 라우터는 Unicast 메시지 만 지원합니다. 각 Multicast 라우터는 Multicast 메시지만 지원합니다. 소스 호스트는 MR1 및 MR2를 통해 대상 호스트에 Multicast 메시지를 전송합니다. MR2는 터널을 통해 수신 된 경우에만 Multicast 메시지를 전달합니다.

대상 호스트가 Unicast 메시지를 원본 호스트로 보내면 터널도 사용됩니다. 터널 기술을 채택한 경우 메시지 전송 속도는 직접 메시지 전송 속도보다 느립니다. 정적 Multicast 라우팅이 구성된 후에 라우터는 구성 정보에 따라 RPF 검사를 수행 할 수 있습니다. RPF 검사는 더 이상 Unicast 라우팅 테이블을 기반으로 하지 않습니다. 따라서 Multicast 메시지는 터널을 통과하지만 Unicast 메시지는 터널을 통과하지 않습니다. 정적 Multicast 경로는 로컬 위치에만 있습니다. 알려지거나 전달되지 않습니다.

전역 구성 모드에서 다음 명령을 실행하여 정적 Multicast 경로를 구성합니다.

명령어	설명
ip mroute *source-address mask rpf-address* **type** *number*[**distance**]	정적 multicast 경로 구성합니다.

22.2.6 경계 IP Multicast 구성하기

ip multicast boundary 명령을 실행하여 포트의 경계 Multicast 를 구성합니다. 구성된 경계를 취소하려면 no ip multicast boundary 명령을 실행하십시오. 두 번째 구성에서 사용된 명령은 첫 번째 구성에서 사용 된 명령을 대체합니다.

명령어	설명
ip multicast boundary *access-list*	포트에 경계 multicast를 구성합니다.

예제

다음 예는 포트의 관리 경계를 구성하는 방법을 보여줍니다.

```
interface ethernet 0/0
ip multicast boundary acl
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

22.2.7 IP Multicast 속도 제어 구성

ip multicast rate-limit 명령을 실행하여 소스 / 그룹 범위에서 Multicast 메시지 수신 및 전송 속도를 제한하십시오.
속도 제한을 취소하려면 no ip multicast rate-limit 명령을 실행하십시오.

다음 명령을 실행하여 Multicast 흐름의 입력 속도를 nkbps로 제한하십시오.

명령어	설명
ip multicast rate-limit in group-list *access-list*1 source-list *access-list*2 nkbps	특정 범위의 multicast 흐름에 대한 최대 입력 속도 제한을 구성합니다.

다음 명령을 실행하여 Multicast 흐름의 출력 속도를 n kbps로 제한하십시오.

명령어	설명
ip multicast rate-limit out *group-list access-list*1 *source-list access-list*2 kbps	특정 범위의 Multicast 흐름에 대한 최대 출력 속도 제한을 구성합니다.

22.2.8 IP Multicast 도움 구성하기

ip multicast helper-map 명령을 실행하여 Multicast 경로를 사용하여 Multicast 네트워크에서 두 개의 Broadcast 네트워크를 연결합니다.
명령을 취소하려면 no ip multicast helper-map 명령을 실행하십시오.

명령어	설명
interface *type number*	인터페이스 구성 모드를 시작합니다
ip multicast helper-map broadcast *group-address access-list*	ip multicast helper 명령을 구성하여 Broadcast 메시지를 Multicast 메시지로 변환합니다.
ip directed-broadcast	지향성 Broadcast를 허용합니다.
ip forward-protocol [*port*]	메시지를 전달하도록 번호를 구성합니다.

Broadcast 네트워크의 목적지를 연결하는 마지막-홉 라우터에 다음을 수행하십시오.

명령어	설명
interface *type number*	인터페이스 구성 모드를 시작합니다.
ip directed-broadcast	지향성 broadcast를 허용합니다.
ip multicast helper-map *group-address broadcast-address access-list*	ip multicast helper 명령을 구성하여 multicast 메시지를 Broadcast 메시지로 변환합니다.
ip forward-protocol [port]	메시지를 전달하도록 포트번호를 구성합니다.

예제

다음 예는 ip multicast helper 명령을 구성하는 방법을 보여줍니다.

라우터 구성은 다음과 같습니다. 지향성 메시지를 처리하기 위해 첫 번째 홉 라우터의 e0 포트에 ip directed-broadcast 명령을 구성합니다. ip multicast helper-map Broadcast 230.0.0.1 구성

testacl1을 사용하여 소스 주소 192.168.20.97/24에서 대상 주소 230.0.0.1의 Multicast 메시지로 전송 된 포트 번호 4000의 UDP Broadcast 메시지를 변환 할 수 있습니다.

방향 메시지를 처리하기 위해 마지막 홉 라우터의 e1 포트에 ip directed-broadcast 명령을 구성합니다. ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2를 구성하여 포트 번호가 4000이고 소스 주소가 192.168.20.97/24 인 대상 주소 230.0.0.1을 대상이 있는 Broadcast 메시지로 변환 할 수 있습니다 address 172.10.255.255.

소스 Broadcast 네트워크를 연결하는 첫 번째 홉 라우터에서 다음 작업을 수행하십시오.

(라우터가 VLAN 포트에 구성되어 있음)

interface ethernet 0

ip directed-broadcast

ip multicast helper-map broadcast 230.0.0.1 testacl

ip pim-dm

!

ip access-list extended testacl   permit udp 192.168.20.97 255.255.255.0 any ip forward-protocol udp 4000

Broadcast 네트워크의 목적지를 연결하는 마지막-홉 라우터에 다음을 수행합니다..

interface ethernet 1

ip directed-broadcast

ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2

ip pim-dm

!

ip access-list extended testacl2   permit udp 192.168.20.97 255.255.255.0 any ip forward-protocol udp 4000

Stub Multicast 경로 구성하기

ip igmp helper-address 및 ip pim-dm neighbor-filter 명령을 실행하여 stub multicast 경로를 구성합니다.

stub 라우터와 호스트가 연결된 포트에서 다음 작업을 수행하십시오.

명령어	설명
interface *type number*	인터페이스 구성모드를 시작합니다.
ip igmp helper-address *destination-address*	Configures the command **ip igmp helper-address** to forward the multicast message to the central router

중앙 라우터와 stub 라우터가 연결된 포트에서 다음 작업을 수행합니다.

명령어	설명
interface *type number*	인터페이스 구성 모드를 입력합니다
ip pim neighbor-filter *access-list*	Stub 라우터에서 모든 PIM 메시지를 필터링합니다

예제

다음과 같이 라우터 A와 B를 구성합니다.

Stub 라우터 A 구성

ip multicast-routing

ip pim-dm

ip igmp helper-address 10.0.0.2

중심 라우터 B 구성

ip multicast-routing

ip pim-dm

ip pim-dm neighbor-filter stubfilter

ip access-list stubfilter

deny 10.0.0.1

22.2.9 Multicast 경로 모니터링 및 유지보수하기

1. Multicast 캐시와 라우팅 테이블 지우기

특정 캐시 또는 라우팅 테이블이 유효하지 않은 경우 해당 내용을 지워야 합니다.

관리모드에서 다음을 실행하십시오.

명령어	설명
clear ip igmp group [*type number*] [*group-address* | *<cr>*]	IGMP 캐시의 항목을 지 웁니다.
clear ip mroute *[* | group-address | source-address]*	Multicast 라우팅 테이블의 항목을 지 웁니다.

2. Multicast 라우팅 테이블 및 시스템 통계 정보 표시.

IP Multi 라우팅 테이블, 캐시 또는 데이터베이스에 대한 자세한 정보는 리소스 사용 방법을 판단하고 네트워크 문제를 해결하는 데 도움이 됩니다.

다음 명령을 실행하여 multicast 라우팅에 대한 통계 정보를 표시합니다.:

명령어	설명
show ip igmp groups [*type number* | *group-address*] [detail]	Displays the information about the multicast group in the IGMP cache.
show ip igmp interface [*type number*]	Displays the IGMP configuration information on the interface.
show ip mroute mfc	Displays the multicast forwarding cache.
show ip rpf [**ucast | mstatic | pim-dm** | **pim-sm** | **dvmrp**] *source-address*	Displays the RPF information.

22-3 장 IGMP 구성하기

22.3.1 소개

1. IGMP

IGMP (Internet Group Management Protocol)는 Multicast group 구성원을 관리하는데 사용되는 프로토콜입니다. IGMP는 호스트 측과 스위치 측을 포함하는 비대칭형 프로토콜입니다. 호스트 측에서 IGMP 프로토콜은 호스트, Multicast 그룹 구성원이 자신이 속한 Multicast 그룹을 보고하는 방법과 호스트가 스위치의 쿼리 메시지에 응답하는 방법을 규정합니다. 스위치 측면에서 IGMP 프로토콜은 IGMP 지원 스위치가 로컬 네트워크에 있는 호스트의 Multicast 그룹 구성원 ID를 학습하는 방법과 호스트의 보고 메시지에 따라 저장된 Multicast 그룹 구성원 정보를 수정하는 방법을 규정합니다.

스위치가 IGMP 라우터 프로토콜을 지원하기 때문에 multicast 라우팅 프로토콜에 현재 네트워크의 multicast 그룹 구성원에 대한 정보가 제공 될 수 있으며 스위치는 Multicast 메시지를 전달할지 여부를 결정합니다. 즉, 스위치가 IP 메시지의 Multicast 프로세스를 지원할 수 있게 하려면 Multicast 라우팅 프로토콜과 IGMP 라우터 프로토콜을 지원하도록 스위치를 구성해야 합니다. 현재 AAA 스위치는 최신 버전 인 IGMP 라우터 프로토콜과 버전 3 IGMP를 지원합니다.

IGMP에 대한 독립적 인 시작 명령이 없습니다. IGMP-Router 프로토콜의 기능은 Multicast 라우팅 프로토콜을 통해 시작됩니다.

2. OLNK

정확히 말하면 IGMP의 유일한 링크 프로토콜 (OLNK)은 다른 프로토콜처럼 상호 작용 프로세스가 없기 때문에 Multicast 라우팅 프로토콜이 아닙니다. 그러나 일부 특수한 경우 OLNK를 단순 토폴로지에서 실행하면 좋은 결과를 얻을 수 있습니다. 협상 프로세스가 없는 PIM-DM 프로토콜과 마찬가지로 OLNK는 IGMP 그룹 구성원의 변경을 처리하고 토폴로지 변경에 따라 RPF 인터페이스를 즉시 조정할 수 있습니다. 이러한 방식으로 OLNK는 Multicast 전달을 보장하고 Multicast 라우팅 프로토콜의 제어 메시지가 대역폭을 차지하는 것을 방지합니다.

22.3.2 IGMP 구성하기

IGMP 라우터의 속성을 구성하는 명령은 주로 IGMP 매개 변수를 조정하는 명령입니다. 다음은 이러한 명령을 설명합니다. 자세한 내용은 IGMP 명령과 관련된 설명 문서를 참조하십시오.

22.3.2.1 현재 IGMP 버전 변경

지금까지 IGMP 프로토콜에는 세 가지 정식 버전이 있습니다. 해당 RFC는RFC1112, RFC2236 및 RFC3376입니다. IGMP V1은 Multicast 그룹 구성원을 기록하는 기능만 지원합니다. IGMP V2는 지정된 Multicast 그룹 구성원을 쿼리하고, IGMP 호스트가 Multicast 그룹을 떠날 때 유휴 메시지를 생성하고 그룹 구성원의 변경 지연을 단축 할 수 있습니다. IGMP V3에는 소스 호스트 주소에 해당하는 Multicast 그룹 구성원 ID를 업데이트하고 유지 관리하는 추가 기능이 있습니다. IGMP V3의 IGMP 라우터 프로토콜은 IGMP V1 및 IGMP V2의 호스트 측과 완벽하게 호환됩니다. AAA의 스위치 소프트웨어는 3 개의 IGMP 버전의 IGMP 라우터 프로토콜을 지원합니다.

서로 다른 인터페이스에서 IGMP-Router 기능을 구성 할 수 있습니다 (서로 다른 인터페이스에 구성된 Multicast 라우팅 프로토콜이 IGMP 라우터 기능을 시작함). 그리고 다른 버전의 IGMP를 다른 인터페이스에서 실행할 수 있습니다.

Multicast 스위치는 동일한 네트워크를 연결하는 포트 중 하나에서만 IGMP 라우터 기능을 시작 할 수 있습니다.

다음 명령을 실행하여 포트에서 IGMP-Router 프로토콜의 버전을 변경합니다.

명령어	설명
ip igmp version *version_number*	포트에서 실행중인 IGMP 버전을 변경합니다.

22.3.2.2 IGMP 쿼리 간격 구성

현재 IGMP 라우터 프로토콜의 버전 번호가 무엇이든 관계없이 Multicast 스위치는 IGMP 라우터 기능이 시작된 포트에서 특정 시간마다 IGMP 일반 쿼리 메시지를 보낼 수 있습니다. 전송 주소는 224.0.0.1입니다. Multicast 스위치의 목적은 IGMP 호스트에서 보고 메시지를 가져 와서 네트워크의 각 IGMP 호스트가 속한 Multicast 그룹을 파악하는 것입니다. 일반 쿼리 메시지를 보내는 간격을 IGMP 쿼리 간격이라고 합니다. IGMP Query Interval (IGMP 쿼리 간격) 매개 변수가 큰 값으로 설정된 경우 스위치는 현재 IGMP 호스트가 속한 Multicast 그룹에 대한 정보를 즉시 수신 할 수 없습니다. IGMP Query Interval (IGMP 쿼리 간격) 매개 변수가 작은 값으로 설정된 경우 현재 네트워크에서 IGMP 메시지의 흐름이 증가합니다.

다음 명령을 실행하여 포트에서 IGMP 쿼리 간격을 수정합니다.

명령어	설명
ip igmp query-interval *time*	현재 인터페이스에서 IGMP 쿼리 간격을 수정합니다 (단위 : 초).

22.3.2.3 IGMP 쿼리의 간격 구성하기

IGMP 라우터 프로토콜의 버전 2 및 버전 3에 대해 IGMP 라우터 프로토콜을 실행하는 다른 스위치가 동일한 네트워크에 있으면 쿼리 프로그램을 선택해야합니다.

Querier는 쿼리 메시지를 보낼 수 있는 스위치를 의미합니다 (사실 IGMP-Router 프로토콜이 활성화 된 스위치의 포트입니다). 보통은 하나의 네트워크에는 하나의 쿼리가 있습니다. 즉, 하나의 스위치만 IGMP 쿼리 메시지를 보냅니다. Multicast 라우팅 프로토콜은 IGMP-Router V1에서 IGMP 쿼리 메시지를 보낼 스위치를 결정하기 때문에 IGMP-Router V1에 대한 쿼리 작성자 선택이 없습니다.

IGMP-Router V2 및 IGMP-Router V3에는 동일한 querier 선택 방법이 있습니다. 즉, 최소 IP 주소를 가진 스위치가 네트워크의 querier 입니다. querier가 아닌 스위치는 querier의 존재를 기록하기 위해 시계를 저장해야 합니다. 클록 시간이 초과되면 더 작은 IP 주소로 스위치에서 IGMP 쿼리 메시지를 수신 할 때까지 비 쿼리 스위치가 querier로 변합니다.

IGMP-Router V2 경우 다음을 사용하여 다른 쿼리 간격을 구성 할 수 있습니다

명령어	설명
ip igmp querier-timeout *time*	다른 queriers의 간격을 구성합니다 (단위: 초).

IGMP-Router V1의 경우 다른 쿼리의 간격은 쓸모가 없습니다. IGMP-Router V3의 경우, 프로토콜 자체에 의해 결정되기 때문에 간격을 구성 할 수 없습니다.

22.3.3 최대 IGMP 응답 시간 구성

IGMP-Router V2 및 IGMP-Router V3의 경우 전송 된 IGMP 일반 쿼리 메시지의 특수 데이터 필드는 IGMP 호스트의 최대 응답 시간을 조절합니다. 즉, IGMP 호스트는 규정 된 최대 응답 시간이 만료되기 전에 응답 메시지를 보내야 하며 이는 일반 쿼리 메시지가 수신되었음을 나타냅니다. 최대 응답 시간이 큰 값으로 설정된 경우 Multicast 그룹 구성원의 변경이 지연됩니다. 최대 응답 시간을 작은 값으로 설정하면 현재 네트워크에서 IGMP 메시지의 흐름이 증가합니다.

Note:

최대 IGMP 응답 시간은 IGMP 쿼리 간격보다 짧아야 합니다. 최대 응답 시간 값이 쿼리 간격보다 크면 시스템은 query-interval-1에 대한 최대 응답 시간을 자동으로 설정합니다. IGMP-Router V2 및 IGMP-Router V3의 경우 인터페이스 구성 모드에서

다음 명령을 실행합니다 최대 IGMP 응답 시간을 설정하려면 다음을 수행하십시오.

명령어	설명
ip igmp query-max-response-time *time*	최대 IGMP 응답 시간 (단위:초)을 구성합니다.

IGMP-Router V1의 경우, 최대 IGMP 응답 시간은 프로토콜 자체에 의해 결정됩니다. 따라서 이전 명령은 IGMP-Router V1에서는 쓸모가 없습니다.

22.3.4 마지막 그룹 구성원에 대한 IGMP 쿼리 간격 구성하기

IGMP-Router V2 및 IGMP-Router V3의 경우 특정 Multicast 그룹에 대한 그룹 별 쿼리 메시지가 전송되면 마지막 그룹 구성원의 쿼리 간격이 호스트의 최대 응답 시간으로 사용됩니다. 즉, IGMP 호스트는 그룹 특정 쿼리 메시지가 수신되었음을 나타내는 마지막 그룹 구성원의 최대 응답 시간이 만료되기 전에 응답 메시지를 보내야합니다. IGMP 호스트가 쿼리 메시지에 응답할 필요가 없다는 것을 발견하면 기존 간격 이후에 메시지에 응답하지 않습니다. 이 경우 Multicast 스위치는
저장된 Multicast 그룹 구성원 정보를 업데이트합니다. 마지막 그룹 구성원의 쿼리 간격이 큰 값으로 설정된 경우 Multicast 그룹 구성원의 변경이 지연됩니다. 마지막 그룹 구성원의 쿼리 간격이 작은 값으로 설정된 경우 현재 네트워크에서 IGMP 메시지의 흐름이 증가합니다.

IGMP-Router V2 및 IGMP-Router V3의 경우 인터페이스 구성 모드에서 다음을 실행하여 마지막 그룹 구성원의 IGMP 쿼리 간격을 구성합니다.

명령어	설명
ip igmp last-member-query-interval *time*	마지막 그룹 구성원의 IGMP 쿼리 간격 (단위: 밀리 초)을 구성합니다.

앞의 명령은 IGMP-Router V1에서는 유효하지 않습니다.

22.3.5 정적 IGMP 구성

IGMP-Router 프로토콜에 의해 규제되는 기능 외에도 BODCOM의 스위치는 포트상의 정적 Multicast 그룹 구성을 지원합니다. IGMP 호스트의 경우 Multicast 그룹 구성원 관계가 다를 수 있습니다. IGMP 호스트가 Multicast 그룹 group1에만 속하고, Multicast 메시지를 수신 시 Multicast 그룹 group1에 Multicast 메시지를 보냅니다. 일정 시간이 지나면 Multicast 그룹 인 그룹 2에 속할 수 있으며 Multicast 그룹 2에 Multicast 메시지를 전송하여 Multicast 그룹 2에 보냅니다. 다른 시간이 지나면 IGMP 호스트는 Multicast 그룹에 속하지 않을 수 있습니다. 따라서, Multicast 그룹 할당 정보는 다양하다.

위의 "동적 Multicast 그룹"과 달리 포트가 정적 Multicast 그룹에 속하도록 구성된경우 Multicast 라우팅 프로토콜은 포트를 Multicast 그룹의 Multicast 메시지를 항상 수신하고 보내는 포트로 사용합니다. IGMP-Router V3와 더 잘 호환되도록 정적 Multicast 그룹은 지정된 소스 주소에서 Multicast 메시지를 수신하도록 구성 할 수 있습니다. 즉, Multicast 메시지가 수신될 때 소스 필터 기능이 추가됩니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 포트에 대한 정적 Multicast 그룹을 구성합니다.

명령어	설명
ip igmp static-group { * | *group-address*} {**include** *source-address* | <*cr*> }	포트의 정적 Multicast 그룹 속성을 구성합니다.

22.3.6 IGMP 즉시-방출 목록 구성

스위치의 포트에서 IGMP V2가 시작되고 포트가 연결된 네트워크에 IGMP 호스트가 하나만 있는 경우 IGMP 즉시-방출 목록을 구성하여 IGMP 호스트의 즉시-방출기능을 구현할 수 있습니다. IGMP V2의 규정에 따르면 호스트가 특정 Multicast 그룹을 떠날 때 호스트는 모든 Multicast 스위치에 Leave 메시지를 보냅니다. Leave 메시지를 수신 한 후 Multicast 스위치는 그룹 별 메시지를 보내 호스트에서 Multicast 그룹과 주고받는 Multicast 메시지가 포트에 있는지 여부를 확인합니다. 즉시 방출 기능이 구성되어 있으면 IGMP 호스트와 Multicast 스위치 간에 메시지를 상호 작용할 필요가 없으므로 Multicast 그룹 구성원 ID의 변경가능 합니다.

Note:

명령어는 전역 구성 모드와 인터페이스 구성 모드에서 모두 구성 할 수 있습니다. 전역 구성 모드에서 구성된 명령의 우선 순위는 인터페이스 구성 모드에서 구성된 명령의 우선 순위보다 높습니다. 전역 구성 모드에서 명령을 처음 구성하면 인터페이스 구성 모드에서 구성된 명령이 생략됩니다. 명령이 인터페이스 구성 모드에서 처음 구성되면 전역 구성 모드에서 구성된 명령은 인터페이스 구성 모드에 구성된 명령을 삭제합니다.

IGMP-Router V2의 경우 인터페이스 구성 모드에서 다음 명령을 실행하여 IGMP 즉시-방출 목록을 구성합니다.

명령어	설명
ip igmp immediate-leave group-list *list-name*	IGMP 호스트에 대한 Multicast 그룹에서 즉시 나가는 기능을 구현하는 액세스 목록을 구성합니다.
ip access-list standard *list-name*	list-name이라는 표준 IP Access-list를 만듭니다.
permit *source-address*	표준 Access-list구성 모드에서 즉석 탈퇴 기능을 구현하는 IGMP 호스트의 IP 주소를 구성합니다.

이전 명령은 IGMP-Router V1 및 IGMP-Router V3에는 유효하지 않습니다.

22.3.7 IGMP 특성 구성 예

모든 구성은 Vlan 포트에서 IGMP 특성을 수행합니다.

1. IGMP 버전 변경의 예

상위 버전의 IGMP-라우터 프로토콜은 하위 버전의 IGMP호스트와 호환되지만, 이전 버전의 IGMP-라우터 프로토콜과 호환되지 않는다. 따라서 현재 네트워크에 있는 이전 버전의 IGMP-라우터 프로토콜을 실행하는 스위치가 있는 경우 최신 버전의 IGMP-라우터 프로토콜을 초기 버전이 같은 IGMP-라우터 프로토콜로 변경해야 합니다.

관리자가 IGMP-라우터 V1및 IGMP-라우터 V2를 실행하는 스위치가 로컬 스위치가 연결된 네트워크에 있다는 것을 알고 있다고 가정하면, 관리자는 IGMP-라우터 프로토콜 버전의 V2버전을 IGMP-라우터 2에서 변경해야 합니다.

```
interface ethernet 1/0
ip igmp version 1
```

2. 모든 IGMP쿼리 간격 구성 예

다음 예는 인터페이스 ethernet 1/0에서 IGMP 쿼리 간격을 50 초로 수정하는

방법을 보여줍니다.

```
interface ethernet 1/0
ip igmp query-interval 50
```

3. IGMP Querier 간격 구성 예

다음 예는 인터페이스 ethernet 1/0에서 IGMP Querier 간격을 100초로 수정하는 방법을 보여줍니다.

```
interface ethernet 1/0
ip igmp querier-timeout 10
```

4. IGMP 최대 응답 시간 예제

다음 예는 인터페이스 ethernet 1/0에서 최대 IGMP 응답 시간을 15 초로 수정하는 방법을 보여줍니다.

```
interface ethernet 1/0
ip igmp query-max-response-time 15
```

5. 마지막 그룹 구성원에 대한 IGMP 쿼리 간격 구성의 예

다음 예에서는 인터페이스 ethernet 1/0에서 마지막 그룹 구성원의 IGMP 쿼리 간격을 2000ms로 수정하는 방법을 보여줍니다.

interface ethernet 1/0

ip igmp last-member-query-interval 2000

6. 정적 IGMP 구성 예제

정적 Multicast 그룹의 구성 명령은 다른 매개 변수를 채택하여 정적 클래스의 다른 클래스를 정의 할 수 있습니다. 다음 예제는 다른 명령 매개 변수를 실행 한 결과를 보여줍니다.

interface ethernet 1/0

ip igmp static-group *

이전 구성 명령은 인터페이스 ethernet 1/0에서 모든 정적 Multicast 그룹을 구성합니다. Multicast 라우팅 프로토콜은 모든 IP multicast 메시지를 인터페이스 ethernet 1/0으로 전달하는 것입니다.

interface ethernet 1/0

ip igmp static-group 224.1.1.7

이전 구성 명령은 인터페이스 ethernet 1/0에 정적 multicast 그룹 224.1.1.7을 구성합니다. 즉, 인터페이스는 multicast 그룹 224.1.1.7에 속합니다. Multicast 라우팅 프로토콜은 마침내 Multicast 그룹 224.1.1.7로 전송 된 모든 IP Multicast 메시지를 인터페이스 ethernet 1/0으로 전달하는 것입니다.

interface ethernet 1/0

ip igmp static-group 224.1.1.7 include 192.168.20.168

기존 명령 구성은 인터페이스 ethernet 0/0에 정적 Multicast 그룹 224.1.1.7을 구성하고 Multicast 그룹의 source-filter를 192.168.20.168로 정의합니다. 즉, 인터페이스는 Multicast 그룹 224.1.1.7에 속하지만 192.168.20.168의 IP Multicast 메시지 만 수신합니다. Multicast 라우팅 프로토콜은 192.168.20.168에서 수신되고 마침내 Multicast 그룹 224.1.1.7로 전송 된 IP Multicast 메시지를 인터페이스 이더넷 0/0으로 전달하는 것입니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 192.168.20.169에서 마지막으로 Multicast 그룹 224.1.1.7로 전송 된 IP Multicast 메시지를 수신합니다.

ip igmp static-group 224.1.1.7 include 192.168.20.169

기존 명령은 여러 소스 주소를 정의하기 위해 여러 번 실행될 수 있습니다.

Note:

Multicast 그룹에서 Multicast 그룹 정보는 특정 소스 주소와 모든 소스 주소에 대해 동시에 구성 할 수 없습니다. 이후 구성에서 사용되는 명령은 생략됩니다. 예를 들어 ip igmp static-group 224.1.1.7 명령을 실행 한 후 ip igmp static-group 224.1.1.7 include 192.168.20.168 명령을 실행하면 ip igmp 명령이 실행됩니다

정적 그룹 224.1.1.7 포함 192.168.20.168은 생략 됩니다.

7. IGMP 즉시-방출 목록 구성 예시

다음 예에서는 immediate-leave 기능을 사용하여 ethernet 1/0 인터페이스에서 일시 중지되도록 Access-list를 설정하고 IGMP 호스트의 IP 주소 192.168.20.168을 Access-list에 추가하는 방법을 보여줍니다. 이 구성을 사용하면 IP 주소가 192.168.20.168 인 IGMP 호스트에서 즉석 탈퇴 기능을 사용할 수 있습니다.

```
interface ethernet 1/0
ip igmp immediate-leave imme-leave
exit
ip access-list standard imme-leave
permit 192.168.20.168
```

22.4.1 PIM-DM 소개

Protocol Independent Multicast Dense Mode (PIM-DM)는 결합 모드의 Multicast 라우팅 프로토콜입니다. 기본적으로 Multicast 소스가 Multicast 데이터를 보내기 시작하면 도메인의 모든 네트워크 노드가 데이터를 수신합니다. 따라서 PIM-DM은 Multicast 패킷을 Broadcast 전정 모드로 전달합니다. Multicast 소스가 데이터를 보내기 시작하면 스위치는 RPF 인터페이스를 제외한 모든 PIM 활성화 인터페이스로 Multicast 패킷을 전달합니다. 이러한 방식으로 PIM-DM 도메인의 모든 네트워크 노드는 이러한 Multicast 패킷을 수신 할 수 있습니다. Multicast 포워딩을 완료하기 위해 스위치는 그룹 G와 소스 S에 해당하는 Multicast 라우팅 항목 (S, G)을 생성해야 합니다. 라우팅 항목 (S, G)에는 Multicast 소스 주소, Multicast 그룹 주소, 발신 인터페이스 목록, 타이머 및 로고를 포함합니다.

특정 네트워크 세그먼트에 Multicast 그룹 구성원이 없으면 PIM-DM은 pruning 정보를 보내고 네트워크 세그먼트를 연결하는 전달 인터페이스를 정리 한 다음 pruning 상태를 설정합니다. pruning 상태는 제한 시간 타이머에 해당합니다. 타이머가 시간 초과되면 pruning 상태가 다시 전달 상태가 되며 Multicast 데이터는 이 분기를 따라 전달 될 수 있습니다. 또한 pruning 상태에는 Multicast 소스 및 Multicast 그룹에 대한 정보가 들어 있습니다. pruning 영역에 Multicast 그룹 구성원이 나타나면 PIM-DM은 상위 필드의 pruning 상태가 시간 초과되어 pruning 상태가 전달이 될 때까지 기다리지 않고 관여 메시지를 상위 필드로 변환합니다

소스 S가 여전히 그룹 G에 정보를 보내는 한, 첫 번째-홉 위치는 라우팅 항목 (S, G)의 새로 고침 정보를 주기적으로 원래 Broadcast 트리로 보내서 새로 고침을 마칩니다. PIM-DM의 상태 새로 고침 방법은 다운 스트림 상태를 새로 고침 하여 Broadcast 트리의 pruning이 시간 초과되지 않도록 합니다.

다중 액세스 네트워크에서 DR 선택에도 PIM-DM은 다음과 같은 법을 도입합니다.

- 반복적으로 전달되는 Multicast 패킷을 방지하기 위해 고유의 전달자를 선택하는 주장 메커니즘을 사용합니다.
- add / prune 억제 메커니즘을 사용하여 중복 추가 / 정리 정보를 줄이십시오.
- 부적절한 가지 치기 작업을 거부하는 메커니즘을 치기를 거부합니다.

PIM-DM 도메인에서 PIM-DM을 주기적으로 실행하는 스위치는 Hello 정보를 주기적으로 보내 다음과 같은 목적을 달성합니다.:

- 인접하는 PIM 스위치를 찾습니다.
- 결정 리프 네트워크와 리프 스위치.
- Multi-access 네트워크에서 지정된 라우터(DR)를 선택합니다.

IGMP v1과 호환되도록 PIM-DM은 DR 선택을 합니다. 인터페이스의 모든 PIM 인접 라우터가 DR 우선 순위를 지원하면 우선 순위가 높은 인접 라우터가 DR으로 선택됩니다. 우선 순위가 같으면 인터페이스 IP 값이 최대 인 인접 라우터가 DR으로 선택됩니다. 우선 순위가 여러 라우터의 Hello 메시지에 표시되지 않으면 인터페이스가 가장 큰 IP 값을 가진 라우터가 DR으로 선택됩니다.

DBCOM 스위치의 PIM-DM v2는 CIDR, VLSM 및 IGMP v1-v3을 지원합니다.

22.4.2 PIM-DM 구성하기

22.4.2.1 타이머 수정하기

라우팅 프로토콜은 Hello 메시지와 State-Refresh 제어 메시지의 전송 빈도를 판단하기 위해 여러 개의 타이머를 사용한다. Hello 메시지를 전송하는 간격은 인접 관계가 올바르게 생성 될 수 있는지 여부에 영향을 미칩니다.

스위치 구성 모드에서 다음 명령을 실행하여 타이머를 조절하십시오:

명령어	설명
ip pim-dm hello-interval	인터페이스 및 neighbor으로부터 Hello 메세지를 송신하는 간격 (초 단위)을 설정합니다.
ip pim-dm state-refresh origination-interval	소스를 직접 연결하는 첫 번째-홉 스위치의 상태 새로 고침 메시지를 보내는 간격은 업스트림 포트의 구성에만 유효합니다. 다음 스위치의 경우 간격은 상태 새로 고침 메시지를 수신하고 처리하는 기간입니다.

22.4.2.2 상태 새로 고침 구성

PIM-DM의 상태 새로 고침 제어 정보는 기본적으로 관리 모드에서 전달됩니다. 인터페이스 구성 모드의 구성 명령은 소스를 직접 연결하는 첫 번째 홉 스위치가 주기적으로 상태 새로 고침 메시지를 보낼 때 업스트림 포트의 구성에만 적용됩니다. 다음 스위치의 경우 간격은 상태 새로 고침 메시지를 처리 기간입니다.

명령어	설명
no ip pim-dm state-refresh disable	포트에서 상태 새로 고침 메시지를 보내고 받을 수 있습니다.
ip pim-dm state-refresh origination-interval	포트에서 상태 새로 고침 메시지를 보내고 받을 간격을 구성합니다.

22.4.2.3 필터 구성 목록

PIM-DM은 기본적으로 필터링 목록을 설정하지 않습니다. 참조 된 필터링 목록은 인접 필터링 목록 및 Multicast 경계 필터링 목록을 포함합니다. 여과 목록은 인터페이스 구성 모드에서 구성해야 합니다.

네트워크 세그먼트의 스위치 또는 스위치가 PIM-DM 협상에 참가하는 것을 금지하려면 인접 필터링 목록을 구성해야 합니다. 일부 그룹이 로컬 영역을 통과하는 것을 금지하거나 허용하려면 Multicast 경계 필터링 목록을 구성해야 합니다.

명령어	설명
ip pim-dm neighor-filter	인접 필터링 목록을 구성합니다.
ip multicast boundary	Multicast 경계에서 필터링 목록 만듭니다.

22.4.2.4 DR 우선순위 설정하기

IGMP v1과 호환성에는 DR 선택이 필요합니다. 기본적으로 DR의 우선 순위는 1로 설정됩니다. 인터페이스의 모든 PIM 인접 라우터가 DR 우선 순위를 지원하면 높은 우선 순위를 가진 인접 라우터가 DR으로 선택됩니다. 우선 순위가 같으면 인터페이스 IP 값이 최대 인 인접 라우터가 DR으로 선택됩니다. 우선 순위가 여러 라우터의 Hello 메시지에 표시되지 않으면 인터페이스가 가장 큰 IP 값을 가진 라우터가 DR으로 선택됩니다.
인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip pim-dm dr-priority	지정된 포트에서 로컬 DR에 대한 우선 순위를 구성합니다.

22.4.2.5 항목 (S,G) 지우기

일반적으로 로컬 MRT의 항목 (S, G) 또는 항목 (S, G)을 통해 전달 된 Multicast 메시지 번호의 통계 값을 지울 필요가 있습니다. 관리 모드에서 다음 명령을 실행하십시오.

명령어	설명
clear ip mroute pim-dm {***** | *group* [*source*]}	로컬 MRT에서 품목 (S, G)을 지웁니다. 작업은 라우팅 테이블의 항목 삭제하는 것입니다. 명령은 업스트림 포트에서 PIM-DM Multicast 라우팅 프로토콜에 의해 생성 된 (S, G) 항목 만 삭제하는 데 사용됩니다.
clear ip pim-dm interface	PIM-DM 포트에서 (S, G)로 전달 된 Multicast 메시지의 통계 값을 재설정합니다. 이 명령은 업스트림 포트에서 PIM-DM Multicast 라우팅 프로토콜에 의해 생성 된 (S, G) 항목 만 재설정하는 데 사용됩니다.

22.4.3 PIM-DM 상태 새로 고침 구성 예

4.2.2 "상태 새로 고침 구성" 단원을 참조하십시오.

22.5.1 PIM-SM 소개

Protocol Independent Multicast Spare Mode (PIM-SM)는 스파 스 모드의 Multicast 라우팅 프로토콜입니다. PIM-SM 도메인에서 PIM-SM을 실행하는 스위치는 주기적으로 Hello 정보를 전송하여 다음과 같은 목적을 달성합니다.

- 인접한 PIM-SM 스위치를 발견하십시오.
- 다중 액세스 네트워크에서 지정된 라우터 (DR)를 선택합니다.

다음 그림과 같이 DR은 조인 / 정리 메시지를 Multicast 트리의 방향으로 직접 연결된 그룹 구성원을 연결하거나 직접 연결된 multicast 소스의 데이터를 multicast 분배 트리로 보냅니다.

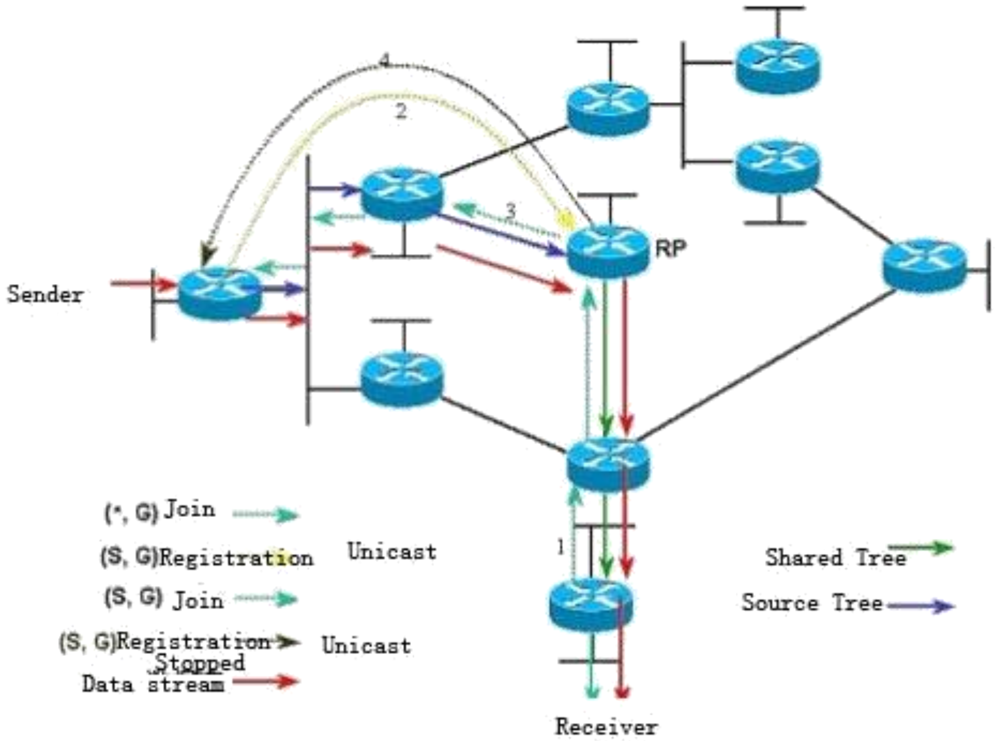


그림 5-1 PIM-SM의 참여 방법

PIM-SM은 Multicast 배포 트리를 만들어 Multicast 패킷을 전달합니다. Multicast 분포 트리는 공유 트리와 최단 경로 트리의 두 그룹으로 분류 할 수 있습니다. Shared Tree는 그룹 G의 RP를 루트로 사용하고 Shortest Path Tree는 Multicast 소스를 루트로 사용합니다. PIM-SM은 표시된 join / prune 모드를 통해 Multicast 배포 트리를 만들고 유지 관리합니다. 그림 5-1과 같이 DR이 수신 측에서 Join 메시지를 수신하면 DR은 그룹 B의 RP에 대한 각 홉에서 (*, G) - 가입 메시지 공유 트리에 가입시킵니다. 소스 호스트 Multicast 메시지를 그룹에 전송하면 소스 호스트의 패킷은 등록 메시지에 패키지화 되고 DR에 의해 RP에 Unicast 됩니다.

그런 다음 RP는 소스 호스트의 패키지 되지 않은 패킷을 공유 트리를 따라 그룹 구성원에게 보냅니다. RP는 소스의 최단 경로 트리에 참여하기 위해 (S, G) - 조인 메시지를 소스 방향으로 첫 번째 홉 스위치로 보냅니다. 이 방법으로 소스의 패킷은 패키징 되지 않고 최단 경로 트리를 따라 RP로 전송됩니다. 첫 번째 Multicast 데이터가 도착하면 RP는 등록 중지 메시지를 소스의 DR에 보내고 DR은 등록 패키지 프로세스를 중지합니다. 이후 소스의 Multicast 데이터는 더 이상 패키징 되지 않지만 소스의 최단 경로 세 개를 따라 RP로 전송 된 다음 RP가 공유 트리를 따라 각 그룹 멤버에게 전송합니다. Multicast 데이터가 필요하지 않은 경우 DR은 Prune 메시지를 그룹 G의 RP를 향해 Multicast하여 공유 트리를 제거합니다.

PIM-SM은 RP 선택 방법도 인지합니다. 하나 이상의 후보 BSR이 PIM-SM 도메인에서 구성됩니다. 특정 규정에 따라 후보 BSR 중에서 BSR을 선택할 수 있습니다. 후보 RP도 PIM-SM 도메인에서 구성됩니다. 이러한 후보 RP는 RP의 주소와 Multicast 그룹을 포함하는 패킷을 BSR에 Uni-casting합니다. BSR은 일련의 후보 RP 및 대응하는 그룹 어드레스를 포함하는 부트스트랩 메시지를 규칙적으로 생성한다. 부트스트랩 메시지는 전체 도메인에서 홉 단위로 전송됩니다. 스위치는 부트스트랩 메시지를 수신하여 저장합니다. DR이 직접 연결된 호스트와 그룹 구성원의 관계에 대한 보고서를 받은 후 DR에 그룹의 라우팅 항목이 없으면 DR은 해시 알고리즘을 통해 그룹 주소를 후보 RP에 매핑합니다. 그런 다음 DR은 Join / prune 메시지를 RP쪽으로 호프별로 Multicast합니다. 마지막으로, DR은 등록 메시지에 Multicast 데이터를 패키징하고 이를 RP에 Uni-casting합니다.

22.5.2 PIM-SM 구성하기

22.5.2.1 PIM-SM 시작하기

다음 명령을 실행하여 인터페이스에서 PIM-SM을 실행하여 sparse 모드에서 멀티 캐스트 기능을 활성화합니다.

명령어	설명
ip pim-sm	PIM-SM을 실행하고 인터페이스 구성 모드에서 PIM-SM 멀티 캐스트 라우팅 프로세스를 인터페이스 활성화를 시작합니다.

22.5.2.2 정적 RP 구성하기

네트워크 규모가 작은 경우 PIM-SM을 사용하도록 정적 RP를 구성 할 수 있습니다. PIM-SM 도메인에 있는 모든 라우터의 RP 구성은 동일해야 합니다.

PIM-SM Multicast 경로가 정확합니다. PIM-SM 도메인의 일부 라우터가 BSR을 행하면 RP가 순서를 따르므로 재정의가 구성된 정적 RP가 우선적으로 사용됩니다. RP는 BSR에 의해 배포되는 RP 매핑 목록의 RP가 선호됩니다. 다음 명령을 실행합니다.

명령어	설명
ip pim-sm rp-address rp-add [**override|acl-name**] **no ip pim-sm rp-address** rp-add	로컬 스위치에 대한 정적 RP를 구성합니다.

22.5.2.3 예비 BSR 구성하기

후보 RP의 구성은 PIM-SM 도메인에서 고유 BSR 글로벌을 생성 할 수 있습니다. 전역 BSR은 도메인에서 RP를 수집과 배포하여 RP 매핑이 고유한지 확인합니다.

전역 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
ip pim-sm bsr-candidate *type number* [*hash-mask-length*] [**priority**] **no ip pim-sm bsr-candidate** *type number*	예비 BSR와 로컬 스위치 그리고 전역 BSR BSM메시지를 학습하고 전역 BSR이다.

22.5.2.4 예비 RP 구성하기

후보 RP를 주기적으로 BSR로 설정 한 다음

도메인의 모든 PIM-SM 라우터로 분산되어 RP 매핑이 고유한지 확인합니다.

전역 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
ip pim-sm rp-candidate [**type** *number*] [**interval**|*group-list acl-name*] **no ip pim-sm rp-candidate** [**type** *number*]	로컬 스위치를 후보 RP로 구성합니다. RP를 구성한 후 주기적으로 BSR로 보냅니다. BSR은 모든 PIM-SM 라우터를 PIM-SM 도메인으로 broadcast합니다.

22.5.2.5 PIM-SM Multicast 경로를 나타냅니다.

명령어	설명
show ip mroute pim-sm [*group-address*] [*source-address*] [**type** *number*] [**summary**] [**count**] [**active** *kbps*]	다음 명령을 실행하여 PIM-SM에서 학습 한 multicast 경로 정보를 확인합니다.

22.5.2.6 Multicast 라우트 습득 by PIM-SM 지우기

다음 명령을 실행하여 PIM-SM에서 학습 한 멀티 캐스트 경로를 지 웁니다.

명령어	설명
clear ip mroute pim-sm [* | group-address] [source-address]	PIN-SM 대한 정보에 대한 자세한 정보

22.5.3 구성 예제

22.5.3.1 PIM-SM 구성 예제

다음은 두 스위치가 PIM-SM Multicast 경로를 배우고 전달하는 방법을 보여줍니다

장치 A:

```
ip multicast-routing
interface Loopback0
ip address 192.166.100.142 255.255.255.0
ip pim-sm
interface Ethernet1/1
ip address 192.166.1.142 255.255.255.0
ip pim-sm
ip pim-sm dr-priority 100
interface Serial2/0
ip address 192.168.21.142 255.255.255.0
physical-layer speed 128000
ip pim-sm
router rip
network 192.168.21.0
network 192.166.1.0
network 192.166.100.0
version2
ip pim-sm bsr-candidate Loopback0 30 201
ip pim-sm rp-candidate Loopback0
```

장치 B:

```
ip multicast-routing
interface Ethernet0/1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
ip pim-sm dr-priority 200
interface Serial0/0

ip address 192.168.21.144 255.255.255.0
ip pim-sm
```

22.5.3.2 BSR 설정 예(Vlan 포트에 스위치 설정이 되어있다.

다음 예는 두 스위치의 BSR 구성을 보여줍니다.

장치 A:

ip multicast-routing

interface Loopback0

ip address 192.166.100.142 255.255.255.0

ip pim-sm

interface Ethernet1/1

ip address 192.166.1.142 255.255.255.0

ip pim-sm

interface Serial2/0

ip address 192.168.21.142 255.255.255.0

physical-layer speed 128000

ip pim-sm

router rip

network 192.168.21.0

network 192.166.100.0

ip pim-sm bsr-candidate Loopback0 30 201

장치 B:

ip multicast-routing

interface Loopback0

ip address 192.168.100.144 255.255.255.0

ip pim-sm

interface Ethernet0/1

ip address 192.168.200.144 255.255.255.0

ip pim-sm

interface Serial0/0

ip address 192.168.21.144 255.255.255.0

ip pim-sm

ip pim-sm bsr-candidate Loopback0 30

23장. QoS 구성

23-1장 QoS 구성

완벽한 라인의 대역폭을 사용하고 효과적으로 네트워크 리소스를 사용하는 방법에 대하여 걱정한다면, 서비스 품질에 대하여 구성을 해야 합니다.

23.1.1 개요

23.1.1.1 QoS 개념

스위치는 일반적으로 최선의 노력을 다하는 서빙 모드에 있습니다. 이 모드에서 스위치는 모든 플로우를 동등하게 처리하고 모든 플로우를 전달하도록 최선을 다합니다. 이 경우, 모든 플로우는 정체가 발생하면 동일한 기회가 삭제됩니다. 실제 네트워크 조건에서 다른 흐름은 다른 중요성을 갖습니다. 스위치의 QoS 기능은 흐름의 중요성에 따라 다른 흐름에 다른 서비스를 제공하여 더 중요한 흐름을 보다 신중히 제공합니다.

현재 네트워크는 흐름의 중요성을 구별하는 두 가지 방법을 제공합니다.

- 802.1Q 프레임의 태그를 기준으로 중요성을 구별합니다. 태그에는 2 바이트가 있습니다. 가장 높은 바이트의 세 비트는 우선 순위 수준을 나타냅니다. 8 개의 우선 순위 레벨 0과 7이 각각 가장 낮은 우선 순위와 가장 높은 우선 순위 레벨을 나타냅니다.

- IP 메시지의 IP 헤더에서 DSCP 필드를 기반으로 중요성을 구별합니다. DSCP 필드는 IP 헤더의 TOS 도메인에서 6 비트를 차지합니다.

실제 네트워크 어플리케이션에서 발신 스위치는 중요도에 따라 다른 우선 순위를 다른 플로우에 분배합니다. 다른 스위치는 흐름에 포함 된 우선 순위 정보에 따라 다른 서비스를 제공합니다. peer-to-peer (P2P) QoS 서비스가 실현됩니다.

또한 네트워크를 구성하여 특정 메시지로 전환 할 수 있습니다. 동작은 하나의 홉으로 불리는 동작으로 수행됩니다.

스위치의 QoS 기능은 네트워크 대역폭을 효과적으로 만들어 성능을 향상시킵니다.

23.1.1.2 P2P QoS 모델

P2P QoS 서비스 모델은 다른 Peer to Peer 메시지를 전송할 수 있습니다. QoS 소프트웨어는 Best-effort served service와 differentiated service의 두 가지 유형의 서비스 모델을 지원합니다.

1. Best-effort 서비스

단일 서비스 모델입니다. 응용 프로그램이 네트워크의 허가 또는 이전 알림을 적용하지 않고 필요한 시간에 원하는 수의 데이터를 보낼 수 있습니다. 최선형 서비스의 경우, 네트워크는 신뢰성, 지연 범위 또는 통과를 요구하지 않고 데이터를 전송할 수 있습니다. 베스트에 포트 서비스 모델에서 스위치의 QoS 기능은 "선착순" 주문을 준수합니다.

2. Differentiated 서비스

차별화 된 서비스의 경우 서비스가 특수한 경우 각 패킷에 해당 QoS 레이블을 지정해야 합니다. 지정 된 다른 모드로 구체화 될 수 있습니다 .IP 패킷의 IP 주소. 스위치는 QoS 규칙을 사용하여 서비스를 분류하고 지능형 대기열을 수행합니다. 스위치의 QoS 기능은 엄격한 우선 순위, 가중 라운드 로빈 (WRR) 및 "선착순 우선" (FCFS)를 통해 차별화 된 서비스를 전송할 수 있습니다.

23.1.1.3 QoS 큐의 QoS 큐 알고리즘

QoS 큐의 QoS 큐 알고리즘은 QoS 실현을 보장합니다. 우리의 스위치는 엄격한 우선 순위, WRR (Weighted Round Robin) 및 FCFS (First come, first served)에 대한 대기 열 알고리즘을 제공합니다.

1 엄격한 우선순위

최우선 원칙은 존재하지 않습니다. 큐 알고리즘은 우선 순위가 높은 플로우에 대해 더 나은 서비스를 제공합니다. 단점은 우선 순위가 낮은 흐름입니다.

2 Round Robin 가중치

WRR 알고리즘은 엄격한 우선 순위의 큐 알고리즘의 단점을 해결하는 효과적인 방법입니다. 특정 대역폭이 각 우선 순위 큐에 분산됩니다. 각 우선 순위 큐는 높은 우선 순위에서 낮은 우선 순위에 따라 제공됩니다. 우선 순위가 높은 대기열이 이미 시작된 경우 WWW 알고리즘은 우선 순위가 낮은 대기열로 바뀌고 서비스를 제공합니다.

3 선착순 (첫번째로 온 것이 첫번째로 서비스 받는다)

FCFS 알고리즘은 메시지를 전달하는 순서를 엄격하게 따르고 메시지에 서비스가 제공됩니다.

22.1.2 QoS 설정 업무 목록

일반적으로 스위치는 모든 메시지를 전달하기 위해 최선을 다합니다. 정체가 발생하면 모든 메시지가 삭제 될 수 있습니다. 실제로, 다른 메시지는 다른 중요성을 가지고 있습니다. 중요한 메시지는 더 나은 서비스와 함께 제공 되어야 합니다. QoS 기능은 서로 다른 서비스를 제공하기 위해 서로 다른 우선 순위를 갖는 다른 메시지를 제공합니다. 따라서 네트워크 성능이 향상되어 효과적으로 사용합니다.

이번 장에서는 스위치의 기능을 구성하는 방법을 설명합니다.

- 전역 CoS 우선 순위 대기열 구성
- CoS 우선 순위 대기열의 대역폭 구성
- CoS 우선 순위 대기열에 대한 일정 전략 구성
- CoS 우선 순위 대기열에 대한 일정 표준 구성
- 포트의 기본 CoS 값 구성
- 포트의 CoS 우선 순위 대기열 구성
- QoS 전략 매핑 설정
- QoS 전략 매핑 설명 구성
- QoS 전략 매핑의 일치 된 데이터 흐름 구성
- QoS 전략 매핑의 일치 된 데이터 흐름에 대한 작업 구성
- 포트에 QoS 전략 적용
- QoS 전략 매핑 테이블 표시
- 포트 유량 제한 구성

22.1.3 QoS 작업 구성하기

22.1.3.1 전역 우선순위 Queue 구성하기

QoS 우선 순위 큐를 구성하는 것은 IEEE802.1p에 정의 된 8 개의 CoS 값을 우선 순위 큐에 매핑하는 것입니다. 스위치에는 8 개의 우선 순위 대기열이 있습니다. 스위치는 다른 대기열에 따라 해당 전략을 채택하고 QoS 서비스를 실

현합니다.

전역 구성 모드에서 CoS 우선 순위 대기열을 구성하면 CoS 우선 순위 맵이 영향을 받습니다. 우선 순위 큐가 구성되면 포트는 우선 순위 큐를 사용하려고 합니다. 그렇지 않으면 전역 구성이 사용됩니다.

전역 CoS 우선 순위 대기열을 구성하려면 다음을 수행하십시오.

명령어	설명
configure	전역 구성모드로 들어갑니다.
[**no**] **cos map** *quid cos1..cosn* **(1~8)**	COS 우선순위 큐를 설정합니다. **quid** 는 COS 우선순위의 ID 입니다 **cos1..cosn** 는 IEEE802.1p에 정의 된 cos값입니다.
Exit	관리 모드로 돌아갑니다.
Write	구성을 저장합니다.

22.1.3.2 CoS 우선 순위 대기열의 대역폭 구성

CoS 우선 순위 큐는 WRR입니다.

이 명령을 사용하면 모든 포트에서 CoS 우선 순위 대기열의 대역폭에 영향을 줍니다. 이 명령은 스케줄 전략이 WRR 일 때만 유효합니다. 이 명령은 일정을 사용할 때 우선 순위 대기열의 대역폭 값을 결정합니다.

다음 작업을 수행하여 CoS 우선 순위 대기열의 대역폭을 구성합니다.

명령어	**설명**
configure	전역 구성 모드를 시작합니다.
[**no**] **scheduler wrr bandwidth** *weight1...weightn* **(1~8)**	CoS 우선 순위 큐의 대역폭을 설정합니다. Weight(1~n)에서 8개의 CoS 우선순위 값을 나타냅니다.
exit	관리 구성 모드로 돌아갑니다.
write	구성을 저장합니다.

22.1.3.3 CoS 우선 순위 대기열에 대한 일정 계획 전략 구성

스위치의 각 포트에는 여러 개의 출력 대기열이 있습니다. 이 스위치에는 8 개의 우선 순위 대기열이 있습니다. 다음을 사용하여 출력 대기열을 예약이 가능합니다.

- SP (Sheer Priority): 완벽한 우선 순위 일정. 우선 순위가 낮은 대기열의 패킷은 우선 순위가 높은 대기열이 비어 있는 경우에만 전달됩니다. 우선 순위가 높은 대기열에 패킷이 있으면 이 패킷이 먼저 전송됩니다.

- WRR (Weighted Round Robin): 각 큐에 가능한 한 많이 할당하는 것입니다.

권한 모드에서 다음 작업을 수행하여 CoS 우선 순위 대기열의 일정을 구성합니다

명령어	설명
configure	전역 구성 모드를 시작하십시오.
[**no**] **scheduler policy** { **sp** | **wrr** }	QoS 우선 순위 대기열에 대한 일정 전략을 설정합니다 **sp 는** sp 스케줄 수립을 나타냅니다. **wrr 은 wrr** 스케줄 수립을 나타냅니다.
exit	관리 모드로 돌아갑니다.
write	구성을 저장합니다.

22.1.3.4 QoS 우선 순위 대기열에 대한 스케줄 표준 구성

COS 우선 순위 큐는 WRR입니다. 스케줄에는 두 가지 유형이 있습니다.

- 패킷-카운트 : 표현할 패킷의 수를 사용합니다.
- 대기 시간: 전송 된 시간에 세그먼트를 사용하여 점유 대역폭을 나타냅니다.

일련의 스위치는 패킷 수만 지원합니다. 패킷 수는 기본 스케줄 표준입니다.
따라서 표준 스케줄 전략을 선택하라는 명령은 없습니다.

22.1.3.5 포트의 기본 CoS 값 구성

포트가 레이블이 없는 프레임을 수신하면 스위치는 기본 COS 우선 순위를 레이블에 추가하려고 합니다. 기본 CoS 값 구성은 레이블이 없는 프레임의 기본값입니다.

특정 모드에서 다음 포트의 기본 CoS 값 조작을 수행하십시오.

명령어	설명
configure	전역 구성 모드를 시작하십시오
interface g0/1	구성 할 포트에 로그인합니다
[**no**] **cos default** *cos* **(0~7)**	레이블이 없는 프레임의 CoS값을 구성하고 CoS는 cos값을 나타냅니다. 기본 값으로 cos (0~7) 설정이 가능합니다.
exit	전역 구성 모드로 돌아갑니다
exit	관리 모드로 돌아갑니다
write	구성을 저장합니다

22.1.3.6 포트의 CoS 우선 순위 대기열 구성

우선 순위 큐가 레이어 2 포트에 설정되면 포트는 구성된 우선 순위 대기열을 사용합니다. 그렇지 않으면 글로벌 COS 우선 순위 대기열 구성이 채택됩니다.

기본 CoS 값을 구성하려면 권한 모드에서 다음 작업을 수행하십시오.

명령어	설명
configure	전역 구성 구성 모드를 시작합니다
interface g0/1	구성 할 포트에 로그인합니다.
[**no**] **cos map** *quid cos1..cosn* **(1~8)**	CoS 우선도 큐를 설정합니다. Quid는 우선순위 ID입니다. Cos(1~n)은 IEEE802.1p에 정의 된 cos 값입
exit	전역 구성 모드로 돌아갑니다
exit	관리 모드로 돌아갑니다.

22.1.3.7 Qos 매핑 전략 설정하기

QoS 매핑 전략은 헤더에서 지정 작업을 구별하기에 특정 기능을 채택하는 것입니다.

하나의 규칙 만 사용하여 데이터 액세스의 IP 액세스 목록 및 MAC Access-list를 일치시킬 수 있습니다. 그렇지 않으면 구성이 실패합니다. 작업이 허가 인 경우
규칙은 다음 작업을 수행하는 데 사용됩니다.

데이터 흐름을 구분합니다. 조치가 거부되면 규칙은 데이터 플로우를 일치시키기 위해 사용되지 않습니다. IP 액세스 목록의 포트 번호는 고정되어 있어야합니다.

QoS 매핑 전략을 만들려면 권한 모드에서 다음 작업을 수행하십시오.

명령어	설명
configure	전역 구성 모드를 시작합니다.
[no]policy-map *name*	QoS 전략 테이블 구성 모드를 시작합니다. name은 전략테이블의 이름을 나타냅니다.
description description-text	QoS의 전략을 설명을 구성합니다.. **description-text** 는 전략을 설명하는 Text입니다

[**no**]**classify** {**ip access-group** *access-list-name* | **dscp** *dscp-value* | **mac access-group** *mac-access-name* | **vlan** *vlan-id* | **cos** ***cos*** **| any** }	QoS 전략 표의 일치된 데이터 흐름을 구성합니다 access-list-name는 일치하는 IP Access list의 이름입니다. **dscp-value 이란** IP 메시지에 다른 서비스를 의미합니다. **mac-list-name** Mac 주소 리스트의 일치하는 주소 목록 이름이다.. **vlan-id** vlan과 일치하는 ID이다 **cos 는** 일치하는 서비스 등급 값을 나타냅니다. **any** 어떤 패킷과 일치 방법을 찾습니다.
action{**bandwidth** *max-band* | **cos**	일치하는 데이터 흐름 전략을 구성합니다.
cos-value **| dscp** *dscp-value* | **redirect** *interface-id* | **drop | monitor** }	QoS 전략 테이블. **max-band** 데이터흐름에 의해 최대 대역폭이 발생합니다, **cos-value** 일치된 서비스 등급을 cos-value으로 설정하는 것을 의미합니다. **dscp-value** 는 흐름의 맞춘 **dscp 필드 dscp-value**. 값을 매칭시킵니다. **interface-id** 지향성에 맞춘 흐름의 종료를 나타냅니다. **Drop** 드롭 메시지를 삭제합니다.. **Stat** 통계 정보를 나타냅니다 **monitor** 패킷을 미러링 포트로 전송을 의미합니다
exit	전역 구성모드로 돌아갑니다
exit	관리모드로 돌아갑니다.

22.1.3.8 QoS 전략 매핑 구성 설명

다음 작업을 수행하여 QoS전략 매핑에 대한 설명을 구성합니다.

명령어	설명
configure	전역 구성 모드로 들어갑니다.

[**no**]**policy-map** *name*	QoS 전략 목록 구성 모드를 입력합니다.. **name** 전략 이름을 나타냅니다.
description description-text	Qos 전략 설명을 구성합니다 **description-text** 는 전략을 설명하는 텍스트 입니다.
exit	글로벌 구성 모드로 돌아갑니다
exit	관리 모드로 돌아갑니다.

22.1.3.9 QoS 매핑 전략의 일치하는 데이터 흐름 구성하기

QoS 데이터 흐름의 분류 규칙은 요구 사항에 따라 구성한 필터링 규칙입니다.
다음 작업을 일치하는 전략 데이터 흐름을 구성하십시오.

명령어	설명
configure	전역 구성 모드로 들어갑니다.
[**no**]**policy-map** *name*	QoS 전략 목록에 구성을 합니다. **name** 전략이름을 나타냅니다
[**no**]**classify** {**ip** **access-group** *access-list-name* **|** **dscp** *dscp-value* | **mac** **access-group** *mac-access-name* **|** **vlan** *vlan-id* **|** **cos** *cos* **|** **any** }	QoS 전략 표의 일치 하는 데이터흐름을 구성합니다. **access-list-name** 일치하는 IP ac-list 이름입니다. **dscp-value** stands for the **diffserv** field in the IP message. **mac-list-name** 는 일치하는 MAC ac-list 이름 입니다. **vlan-id** Vlan 아이디를 나타냅니다. [illegible]
exit	전역 구성 모드로 돌아갑니다
exit	관리 모드로 돌아갑니다

22.1.3.10 QoS 매핑 전략의 일치하는 데이터 흐름을 일치하는 구성하기

데이터 흐름의 작용을 정의한다는 것은 대역 폭 제한, 메시지 삭제, 도메인 업데이트 등 필터링 규칙을 데이터 흐름에 따라 작업을 수행한다는 것을 의미합니다.
다음 작업을 수행하여 일치하는 데이터 흐름에 대한 작업을 구성하십시오.

명령어	설명
configure	전역 구성 모드를 사용합니다.
[**no**]**policy-map** *name*	Qos 전략 구성 모드를 실행합니다. **name** 전략-맵의 이름을 나타냅니다

action {**bandwidth** *max-band* | **cos** *cos-value* **| dscp** *dscp-value* | **vlanID** *vlanid-value* | **redirect** *interface-id* **| drop |** **stat | monitor** }	QoS전략 표에 일치하는 데이터 흐름 전략을 구성합니다. **max-band**: 최대값을 나타냅니다. **cos-value** 흐름의 서비스 등급 필드를 cos-value로 설정하는 것을 의미합니다. **dscp-value** 일치하는 흐름의 dscp필드를 VSE-값으로 설정하는 방법입니다. **vlanid-value** 일치된 흐름의 VLANID필드를 vlanid-value로 설정하는 것을 의미합니다. **interface-id** 방향성 일치 항목 흐름의 종료를 나타냅니다. **drop** 드롭 된 메시지를 나타냅니다 **Stat** 스위치에 의해 수집된 통계 정보를 나타냅니다. **monitor** 패킷을 미러링 포트에 전송하는 것을 의미합니다
exit	전역 구성 모드로 돌아갑니다.
exit	관리모드로 돌아갑니다.

22.1.3.11 포트에 QoS 전략을 적용하기

QOS 전략을 포트에 적용 할 수 있습니다. 하나의 전략이 다중 포트에도 적용될 수 있습니다. 포트에 적용된 전략에는 우선 적용되는 전략이 최우선 순위를 차지합니다. 메시지가 동시에 두 가지 전략을 구성하고 구성 작업이 충돌하는 경우 먼저 일치 전략을 표준으로 취하십시오. 전략이 포트에 적용되면 스위치는 통과가 허용되지 않는 전략에 흐름을 추가합니다. 포트의 모든 전략이 삭제되면 스위치는 포트에서 기본값의 기본 전략을 자동으로 삭제합니다.

QoS 전략을 적용하려면 권한 모드에서 다음 작업을 수행하십시오.:

명령어	설명
configure	전역 구성 모드를 시작합니다
interface g0/1	구성 할 포트에 로그인합니다.

[**no**] **qos policy** *name* { **ingress**|**egress**}	포트에 QoS 전략을 적용합니다. **name** QoS 전략을 적용합니다. **ingress** Qos 전략의 수신의 영향을 끼친다는 것을 의미합니다. **egress** Qos 전략이 발신에 영향을 끼친다는 것을 의미합니다.
exit	전역 구성 모드로 돌아갑니다.
exit	관리 모드로 돌아갑니다.

22.1.3.12 QoS 매핑 전략 테이블 표시

show QoS strategy 매핑 테이블을 실행할 수 있습니다.

QoS 전략 매핑 테이블을 표시하려면 권한 모드에서 다음 작업을 수행하십시오.

명령어	설명
show policy-map [*policy-map-name*]	모든 또는 지정된 QoS 전략 매핑 테이블을 표시합니다. **policy-map-name** 매핑 테이블의 이름을 나타냅니다.

22.1.3.13 포트 속도 흐름 제한 구성하기

포트의 속도의흐름은 제한하려면 다음 작업을 수행하십시오.

명령어	설명
configure	전역 구성 모드로 들어갑니다
interface g0/1	포트 구성 모드로 들어갑니다.
[**no**] **switchport rate-limit** *band* **(1~1000)** { ingress|egress}	포트 속도 흐름을 제한합니다. **band** 흐름 속도를 제한합니다. **Ingress** 흐름 제한이 입구에 영향을 끼칩니다. **egress** 흐름 제한이 출구에 영향을 끼칩니다.
exit	전역 구성 모드로 돌아갑니다.
exit	관리 모드로 돌아갑니다.

22.1.4 QoS 구성 예제

22.1.4.1 포트에 QoS 전략 예제 적용하기

포트에서 메시지의 COS 값을 2로 변경하는 전략을 구성합니다. 그렇지 않으면 다른 전략을 적용해야 합니다. 모든 데이터 흐름을 통과 할 수 없습니다.

```
ip access-list extended ipacl

permit ip 192.168.20.2 255.255.255.255 192.168.20.210
255.255.255.255 policy-map any

classify any

policy-map pmap

classify ip access-group ipacl

action cos 2

interface GigaEthernet0/2

  qos policy pmap ingress

  qos policy any ingress (pay attention to the order of two strategies applied)
```

24장. 2 계층 프로토콜 터널 구성하기

1.1 소개

2 계층 프로토콜 터널은 스위치의 양면 사이에 사용자가 스위치의 관련 2 계층 소프트웨어 모듈에 의해 영향을 받지 않고 자신의 네트워크에 지정된 2 계층 프로토콜을 전송 할 수 있습니다.
스위치는 사용자를 위한 명확한 미디어입니다.

1.2 2 계층 프로토콜 터널 계층 구성하기

스위치 인터페이스에서 명령어를 사용하여 계층 2 프로토콜의 터널 기능을 구성하십시오. 구성 단계는 다음과 같습니다.

명령어	설명
configure	전역 구성 모드를 시작합니다.
interface *<intf_name>*	스위치의 인터페이스 구성모드를 시작합니다.
[**no**] **l2protocol-tunnel** *[stp]*	현재 stp 프로토콜의 터널기능을 스위치가 지원하며 2계층을 사용합니다.
[CTRL] + Z	EXEC 모드로 나갑니다.
write	구성을 저장합니다.

1.3 2 계층 프로토콜 터널 구성 예제

A1 / A2 /는 코어 네트워크에 속하며, C1 / C2는 두 곳에서 분산 된 스위치입니다. 고객은 자사의 네트워크 중 두 가지를 하나로 결합하고자 합니다. 즉, 네트워크는 고객을 위한 명백한 전송 채널입니다. 사용자가 STP의 명백한 전송을 실현하려면 각 스위치에서 다음 구성을 수행해야합니다

1 스 위 치 A1의 f0/2, f0/1과 f0/2이 모이고, 스 위 치 A2 f0/1 와 f0/2가 트렁크 모드로 구성됩니다.

2 STP 프로토콜의 터널기능과 A2 의 f0/2 와 A1 의 0/1 이 접근하도록 구성되어 있습니다.

25장. 하드웨어 IP Subnet 라우팅 구성

25.1.1 하드웨어 IP Subnet 경로 구성 작업

25.1.1.1 개요

하드웨어 IP Subnet 경로는 IP의 빠른 교환과 유사합니다. 하드웨어 IP Subnet 경로가 활성화되지 않은 경우 IP 주소가 포함 된 전달 메시지 앞에 표시됩니다. 항목이 있으면 메시지가 하드웨어를 통해 전달됩니다. 해당 항목이 없으면 메시지가 CPU로 전송 된 다음 소프트웨어를 통해 처리됩니다.
하드웨어 IP Subnet 경로 항목에는 대상 Subnet, 마스크, 다음 홉의 IP 주소, 인터페이스 등이 포함됩니다. 하드웨어 IP Subnet 경로가 활성화되면 IP 캐시가 실패한 후 시스템은 하드웨어 IP Subnet 경로 항목을 확인합니다. 일치 항목이 발견되면 메시지는 다음 홉 IP 주소와 일치 항목에 지정된 인터페이스를 통해 직접 전달됩니다. 하드웨어 IP Subnet 경로 항목이 없으면 처리를 위해 메시지가 CPU로 전송됩니다.

하드웨어 IP Subnet 경로에는 자동 및 수동의 두 가지 모드가 있습니다. 수동 모드에서는 하드웨어 IP Subnet 경로를 수동으로 구성 해야 합니다. 목적지 서브넷의 더 긴 마스크가 있는 라우팅 항목은 먼저 구성되어야 합니다. 자동 모드에서 시스템은 알려진 경로를 하드웨어 Subnet 경로에 자동으로 추가합니다. 하드웨어 Subnet 경로가 시작되면 모든 절차가 자동으로 수행됩니다.

25.1.1.2 하드웨어 IP Subnet 경로 구성하기

하드웨어 IP Subnet 경로 구성하려면 다음 단계를 수행하십시오.

단계	명령어	설명
1	[**no**] **ip exf** {**default** | *destination mask*} {**cpu** | *nexthop* vlan *vlanid*}	하드웨어 Subnet 경로에 대상 네트워크와 마스크를 지정하여 추가하거나 삭제하고 이 경우 다음 홉은 이 명령은 수동 구성 모드에서만 유효합니다.
2	[**no**] **ip exf**	하드웨어 IP Subnet 라우팅을 활성화 또는 비활성화합니다.

25.1.1.3 하드웨어 IP Subnet 경로 구성의 상태 확인하기

명령어	설명
show ip exf	현재 경로 구성상태를 보여줍니다.

25.1.2 구성 예제

라우팅 항목을 구성 할 때 다음 내용에 주의하십시오.

직접 연결 된 라우팅과 관련하여 다음 홉은 CPU입니다. 다음 홉이 IP 주소가 아닌 라우팅 인터페이스 인 경우 직접 연결 라우팅입니다.
하드웨어 IP Subnet 경로는 하드웨어 IP Subnet 경로의 항목입니다.
서로 prefix 인 두 개 이상의 경로는 하드웨어 IP Subnet 경로가 채택 될 때 함께 사용되어야 합니다. 다른 항목의 경우 하드웨어 Subnet 라우팅 테이블에 트래픽이 많은 항목을 추가하는 것이 좋습니다.
다음 홉 IP 주소의 ARP가 없으면 시스템은 ARP 요청을 보내고 일시적으로 다음 홉 라우팅 항목을 CPU로 지정합니다. 시스템이 ARP 응답을 수신하면 시스템은 다음 홉을 사용자 지정 주소로 업데이트합니다. VLAN 인터페이스가 다음 홉이 있는 곳이면 경로의 다음 홉이 CPU로 지정됩니다. 사용자는 구성을 수정해야합니다.
Next-hop 인터페이스 또는 인터페이스 프로토콜이 없으면 항목이 하드웨어 서브넷 라우팅 테이블에 추가되지 않습니다.

스위치에 다음 항목이 있다고 가정합니다.

4 192.168.0.0/16 next hop 192.168.26.3/vlan1

5 192.168.20.0/24 next hop 192.168.26.1/vlan1

6 192.168.1.0/24 direct-connecting routing

7 192.168.26.0/24 direct-connecting routing

8 10.0.0.0/8 next hop 192.168.1.4/vlan2

9 0.0.0.0/0 next hop 192.168.1.6/vlan2

경로 항목 1의 대상 Subnet 은 Subnet 2, 3 및 4의 prefix입니다. 따라서 이러한 항목은 하드웨어 Subnet 라우팅 테이블에 함께 추가 되어야합니다.
항목 3과 4는 직접 연결 라우팅이고 다음 홉은 CPU입니다.

다음은 상대적인 구성입니다

```
ip exf 192.168.20.0 255.255.255.0 nexthop 192.168.26.1 vlan 1
ip exf 192.168.1.0 255.255.255.0 cpu
ip exf 192.168.26.0 255.255.255.0 cpu
ip exf 192.168.0.0 255.255.0.0 nexthop 192.168.26.3 vlan 1
ip exf 10.0.0.0 255.0.0.0 nexthop 192.168.1.4 vlan 2
ip exf 0.0.0.0 0.0.0.0 nexthop 192.168.1.6 vlan 2
```

26장. 공격 예방 구성

26.1.1 개요

스위치는 네트워크 대역폭의 유용성을 보장하기 위해 트래픽이 사용되는 것을 방지하는 기능을 제공합니다. 현재의 공격 모드에 비추어 우리 호스트는 일정 기간 동안 ARP, IGMP 또는 IP 메시지를 많이 보내고 이러한 호스트에 서비스를 제공하지 않습니다. 이 기능은 악의적 인 메시지가 많은 네트워크 대역폭을 차지하는 것을 막을 수 있습니다. 따라서 네트워크가 정체 될 수 없습니다.

26.1.2 공격 예방 구성 작업

임계 값을 초과하는 지정된 간격으로 호스트에서 보낸 IGMP, ARP 또는 IP 메시지의 수는 호스트가 네트워크를 공격한다고 생각합니다.

공격 방지 유형 (ARP, IGMP 또는 IP), 공격 방지 포트 및 공격 탐지 매개 변수를 선택할 수 있습니다. 다음과 같은 구성 작업이 있습니다.

- 공격 방지 유형 구성
- 공격 탐지 매개 변수 구성

26.1.3 공격 예방 구성

26.1.3.1 공격 탐지 매개변수 구성하기

명령어	설명
filter period *time*	공격 탐지 기간을 초단위로 설정합니다.
filter threshold *value*	공격 탐지 임계 값을 value로 설정합니다. 매개 변수 값은 임계 값에서의 메시지 수를 나타냅니다.
filter block-time *time*	공격 소스의 서비스 중단 시간을 설정합니다. 단위는 초입니다.

26.1.3.2 공격 방지 유형 구성

명령어	설명
filter igmp	igmp 공격을 탐지합니다.
fileter ip source-ip	IP 주소를 기반으로 공격을 감지합니다.
interface f x/y	인터페이스 y에 슬롯 x에 들어갑니다..
filter arp	Arp 공격을 탐지합니다

ARP 공격은 호스트의 MAC 주소와 소스 포트를 공격 소스로 사용합니다. IGMP 공격과 IP 공격은 호스트의 IP 주소와 소스 포트를 공격 소스로 사용합니다. IGMP 공격 방지와 IP 공격 방지는 함께 시작할 수 없습니다.

26.1.3.3 공격 예방 기능 시작하기

공격 예방을 위한 모든 매개 변수가 끝나면 공격 방지 기능을 시작할 수 있습니다. 공격 방지 기능이 시작됩니다.

명령	설명
filter enable	공격 방지 기능을 시작합니다.

공격 방지 기능을 비활성화하고 모든 공격 소스로 차단을 제거하려면
no filter enable 명령을 사용하십시오.

26.1.3.4 공격 예방 상태 점검

공격 방지가 시작되면 다음 명령을 실행하여 공격 방지 상태를 확인할 수 있습니다:

명령	설명
show filter	공격 예방 상태 점검.

26.1.4 공격 방지 구성 예

포트 1/2에서 IGMP 공격 방지 및 ARP 공격 방지를 사용하려면 공격 소스로 15 초 내에 1200 개 이상의 메시지를 보내고 공격 소스에 대한 네트워크 서비스를 차단하는 호스트를 고려하십시오..

```
filter period 15
filter threshold 1200
filter block-time 600
interface f1/2
filter arp
exit
filter enable
```

27장. 보안 구성 (AAA 구성)

27.1.1 AAA 개요

액세스 제어는 네트워크와 서비스에 액세스하는 방법입니다. 인증 (Authentication), 권한 부여(authorization) 및 계정(accounting) (AAA) 네트워크 보안 서비스는 라우터 와 액세스 서버에 대한 액세스 제어를 설정하는 프레임 워크를 제공합니다.

27.1.1.1 AAA 보안 서비스

AAA는 세 가지 독립적 인 보안 기능을 일관된 방식으로 구성하기위한 건축 프레임 워크입니다. AAA는 다음 서비스를 수행하는 모듈 식 방법을 제공합니다.

• 인증— 로그인 및 암호 대화 상자, 요청 및 응답, 메시징 지원 및 선택한 보안 프로토콜에 따라 암호화를 비롯한 사용자 식별 방법을 제공합니다.

인증은 네트워크 및 네트워크 서비스에 대한 액세스입니다. 지정된 인증 방법 목록을 정의한 다음 다양한 인터페이스에 적용하여 AAA 인증을 구성합니다. 메서드 목록은 시퀀스를 수행하고 반복하도록 설정됩니다. 특정 인터페이스에 적용되어야 합니다. 유일한 예외는 기본 메소드 목록 ("default"라는 이름)입니다. 기본 방법은 모든 인터페이스에 자동으로 적용됩니다. 정의 된 메소드 목록은 기본 메소드 목록과 겹쳐집니다. 로컬, 회선 암호 및 활성화 인증을 제외한 모든 인증 방법은 AAA에 의해 정의 되어야 합니다. AAA 보안 서비스 외부에서 구현되는 것을 포함하여 모든 인증 방법 구성에 대한 자세한 내용은 "인증 구성"장을 참조하십시오.

• 권한 부여 각 서비스, 사용자 별 계정 목록 및 프로필, 사용자 그룹 지원, IP, IPX, ARA 및 텔넷 지원에 대한 일회성 권한 부여 또는 권한 부여를 비롯하여 원격 액세스 제어 방법을 제공합니다.

AAA 권한 부여는 사용자가 수행 할 수 있는 권한을 설명하는 일련의 속성을 조합하여 작동합니다. 이러한 속성은 주어진 사용자에 대한 데이터베이스에 포함 된 정보와 비교되고 결과가 리턴 됩니다. 데이터베이스는 RADIUS 또는 TACACS + 보안 서버에서 원격으로 액세스 할 수 있습니다. RADIUS 및 TACACS +로 검색하는 원격 보안 서버는 해당 사용자와 해당 권한을 정의하는 연관 속성 - 값 (AV) 쌍으로 특정 권한을 사용자에게 부여합니다.
모든 인증 방법은 AAA에 의해 정의되어야 합니다.

인증 방법의 명명 된 목록을 정의한 다음이를 다양한 인터페이스에 적용하여 AAA 권한을 얻습니다. AAA를 사용하여 권한을 구성하는 방법에 대한 자세한 내용은 "권한 구성"장을 참조하십시오.

계정 - 청구, 감사 및 보고, 사용자 ID 검색, 시작 및 중지 시간, 실행 된 명령 (PPP로 검색), 패킷 수 및 바이트 수에 사용되는 보안 서버 정보를 수집하고 보내는 방법을 제공합니다.

계정을 사용하면 사용자가 액세스하고있는 서비스는 물론 사용중인 네트워크 리소스의 양을 추적 할 수 있습니다. AAA 계정이 활성화되면 네트워크 액세스 서버는 계정이 레코드의 형태로 RADIUS 또는 TACACS + 보안 서버 (구현 한 보안 방법에 따라 다름)에 사용자 작업을 보고합니다. 각 계정에서 레코드는 AV 쌍에 포함되며 액세스 제어 서버에 저장됩니다. 이 데이터는 네트워크 관리, 클라이언트 청구 및 / 또는 감사를 위해 분석 될 수 있습니다. 모든 회계 방법은 AAA에 의해 정의 되어야 합니다. 회계 방법의 명명 된 목록을 정의한 다음이를 다양한 인터페이스에 적용하여 AAA 계정 관리. AAA를 사용하여 계정을 구성하는 방법에 대한 자세한 내용은 "계정 구성" 장을 참조하십시오.

27.1.1.2 AAA를 사용하는 이점

AAA는 다음과 같은 이점을 제공합니다.

- 향상된 유연성 및 접근 구성 제어
- 확장성
- RADIUS, TACACS + 와 Kerberos 와 같은 표준화 된 인증 방법
- 다중 백업 시스템

27.1.1.3 AAA 원리

AAA는 라인 단위 (사용자 별) 또는 서비스 별 (예 : IP, IPX 또는 VPDN) 단위로 필요한 인증 및 권한 유형을 동적으로 구성 할 수 있도록 설계되었습니다. 메소드 목록을 작성한 다음 특정 메소드 또는 인터페이스에 해당 메소드 목록을 적용하여 원하는 인증 및 권한 유형을 정의하십시오.

27.1.1.4 메서드 목록

메서드 목록는 사용자를 인증 시에 사용한 인증 방법을 정의하는 순차 목록입니다. 메서드 목록을 사용하면 인증에 사용할 보안 프로토콜을 하나 이상 지정할 수 있으므로 초기 메서드가 실패 할 경우를 대비하여 인증을 위한 백업 시스템을 보장 할 수 있습니다. Cisco IOS 소프트웨어는 나열된 첫 번째 방법을 사용하여 사용자를 인증합니다. Cisco IOS 소프트웨어는 방법 목록에서 다음 인증 방법을 선택합니다. 인증 방법이 고갈되면 인증에 실패합니다.

이전 방법의 응답이 없는 경우에만 다음에 나열된 인증 방법을 사용하는 인증 방법입니다. 인증이 사이클 의미의 어느 지점에서 실패 할 경우 보안 서버 또는 로컬 사용자 이름 데이터베이스를 중지하고 다른 인증 방법이 시도되지 않은 사용자 액세스 인증 프로세스를 거부하여 응답했다. 4 개의 보안 서버를 포함하는 AAA 네트워크 구성: R1과 R2는 RADIUS 서버이고 T1과 T2는 TACACS + 서버입니다.

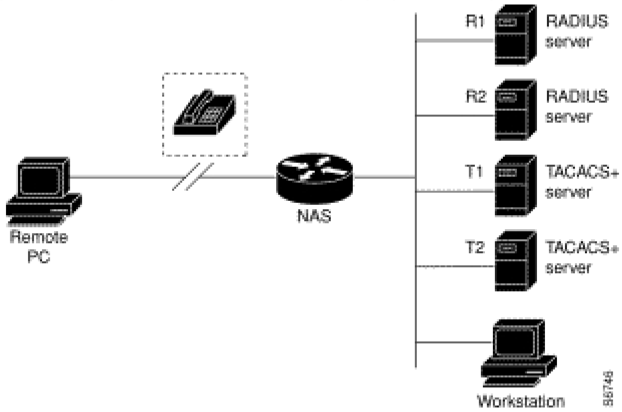


그림 1-1 전형적인 AAA 네트워크 구성

시스템 관리자가 R1이 먼저 인증 정보에 대해 연락을 취하고 R2, T1, T2 및 마지막으로 서버 접근 자체의 로컬 사용자 이름 데이터베이스에 연결하려는 방법을 정의했다고 가정합니다. 원격 사용자가 네트워크에 전화 접속을 시도하면 네트워크 액세스 서버는 우선 R1에 인증 정보를 쿼리합니다. R1이 사용자를 인증하면 네트워크 서버 접근에 PASS 응답을 보내고 사용자는 네트워크에 접근 할 수 있습니다. R1이 FAIL 응답을 반환하면 사용자의 접근이 거부되고 세션이 종료됩니다. R1이 응답하지 않으면 네트워크 서버 접근은 이를 ERROR로 처리하고 R2에 인증 정보를 쿼리합니다. 이 패턴은 계속 인증되거나 거부되거나 세션이 종료 될 때까지 계속됩니다. 네트워크 서버 접근에 세션을 오류로 처리하려고 할 때 세션이 종료됩니다. FAIL 응답은 ERROR와 상당히 다릅니다. FAIL은 사용자가 인증하지 않았음을 의미합니다. 인증은 FAIL 응답으로 끝납니다. ERROR에서 보안 서버가 인증 쿼리에 응답하지 않았습니다. 이 때문에 인증이 시도되지 않았습니다. ERROR가 탐지 된 경우에만 AAA는 인증 방법 목록에 정의 된 다음 인증 방법을 선택합니다.

27.1.2AAA 구성 프로세스

먼저 어떤 종류의 보안 솔루션을 구현할지 결정해야합니다. 무단 진입 및 공격을 방지합니다.

27.1.2.1 AAA 구성 프로세스 의 개요

AAA 구성은 관련된 기본 프로세스를 이해 한 후 비교적 간단합니다. AAA를 사용하여 시스코 라우터 또는 액세스 서버에서 보안을 구성하려면 다음 절차를 따르십시오.

- 별도의 보안 서버를 사용하려면 보안 프로토콜 매개 변수를 구성하고 RADIUS, TACACS + 또는 Kerberos로 검색하십시오.
- AAA 인증 명령을 사용하여 인증을 위한 방법 목록을 정의하십시오. 필요한 경우 특정 인터페이스 또는 회선에 메소드 목록을 적용하십시오.
- (선택 사항) aaa authorization 명령을 사용하여 권한을 구성합니다.
- (선택 사항) aaa accounting 명령을 사용하여 계정을 구성합니다.

27.1.3 AAA 인증 구성 작업 목록

- AAA를 사용하여 로그인 인증 구성
- AAA를 사용하여 PPP 인증 구성
- 권한 수준에서 암호 보호 활성화
- AAA 인증을 위한 메시지 배너 구성
- AAA 인증 사용자 이름 - 프롬프트
- AAA 인증 암호 프롬프트
- 사용자 이름 인증 설정
- 비밀번호 사용

27.1.4 AAA 인증 구성 작업

AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

1 별도의 보안 서버를 사용하려면 보안 프로토콜 매개 변수를 구성하고 RADIUS, TACACS+ 또는 Kerberos로 검색하십시오.

2 AAA 인증을 사용하여 인증을 위한 메소드 명령어 목록 정의.

3 필요한 경우 메서드 목록을 특정 인터페이스나 행에 적용합니다.

27.1.4.1 AAA를 사용하여 로그인 인증 구성

AAA 보안 서비스는 다양한 로그인 인증 방법을 용이하게 합니다. aaa authentication login 명령을 사용하여 지원되는 로그인 인증 방법에 상관없이 AAA 인증을 활성화합니다. aaa authentication login 명령을 사용하여 로그인 할 때 시도되는 인증 방법 목록을 하나 이상 작성합니다. 이 목록은 로그인 인증 라인 구성 명령을 사용하여 적용됩니다.

AAA를 사용하여 다음 명령을 사용하십시오.

명령어	설명
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	전역적으로 AAA를 활성화합니다.
line [**console** | **vty**] *line-number* [*ending-line-number*]	인증 목록을 적용 할 회선에 대한 회선 구성 모드를 시작합니다.
login authentication {**default** | *list-name*}	인증 목록을 한 줄 이상에 적용합니다.

list-name은 작성중인 목록의 이름을 지정하는 데 사용되는 문자열입니다. 메소드 인수는 인증 알고리즘이 시도하는 실제 메소드를 나타냅니다. 추가 메소드 인증은 이전 메소드가 실패 할 경우에만 오류를 반환하는 경우에만 사용됩니다. 모든 메소드가 오류를 반환하더라도 인증이 성공하도록 지정하려면 명령 행에서 마지막 메소드로 none을 지정하십시오. 예를 들어 (이 예제에서) TACACS + 서버가 오류를 반환하더라도 인증이 성공하도록 지정하려면 다음 명령을 입력하십시오.

aaa authentication login default group radius

Note:
none 키워드는 사용자가 성공적으로 인증하기 위해 로그인 할 수 있게 하므로 인증의 백업 방법으로 만 사용해야합니다.
다음 표는 지원되는 로그인 인증 방법을 나열합니다.

단어	설명
enable	인증에 사용 할 암호를 사용합니다.
group *name*	인증을 위해 지정 된 서버 그룹을 사용합니다.
group radius	인증을 위해 모든 RADIUS 서버 목록을 사용합니다.
line	인증에 회선 암호를 사용합니다.
local	인증에 로컬 사용자이름의 데이터베이스를 사용합니다.

local-case	대/소문자를 구분하는 로컬 사용자 이름 인증을 사용합니다.
none	인증을 사용하지 않습니다.

(1) 사용 암호를 사용하여 로그인 인증

enable method 키워드와 함께 aaa authentication login 명령을 사용하여 사용 가능 암호를 로그인 인증 방법으로 지정하십시오. 예를 들어 다른 메소드 목록이 정의되지 않은 경우 로그인 시 사용자 인증 방법으로 사용 가능 암호를 지정하려면 다음 명령을 입력하십시오.

aaa authentication login default enable

(2) 회선 암호를 사용한 로그인 인증

aaa authentication login 명령을 line method 키워드와 함께 사용하여 회선 암호를 로그인 인증 방법으로 지정하십시오. 예를 들어 다른 메소드 목록이 정의되지 않은 경우 로그인 할 때 사용자 인증 방법으로 라인 암호를 지정하려면 다음 명령을 입력하십시오.

aaa authentication login default line

로그인 인증 방법으로 회선 암호를 사용하려면 회선 암호를 정의합니다.

(2) 로컬 암호를 사용한 로그인 인증

aaa authentication login 명령을 local method 키워드와 함께 사용하여 시스코 라우터 또는 액세스 서버가 인증에 로컬 사용자 이름의 데이터베이스를 사용하도록 지정합니다. 예를 들어 다른 메소드 목록이 정의되지 않은 경우에는 로그인 시 사용자 인증 방법으로 로컬 사용자 이름 데이터베이스를 지정하려면 다음 명령을 입력하십시오.

aaa authentication login default local

로컬 사용자 이름 데이터베이스에 사용자를 추가하는 방법에 대한 자세한 내용은이 장의 "사용자 이름 인증 설정"절을 참조하십시오.

(3) 그룹 RADIUS를 사용한 로그인 인증

aaa authentication login 명령을 group radius 메소드와 함께 사용하여 RADIUS를 로그인 인증 방법으로 지정하십시오. 예를 들어 다른 메소드 목록이 정의되지 않은 경우 로그인 시 사용자 인증 방법으로 RADIUS를 지정하려면 다음 명령을 입력하십시오.

aaa authentication login default group radius

로그인 인증 방법으로 RADIUS를 사용하려면 먼저 RADIUS 보안 서버와의 통신을 활성화 해야 합니다. RADIUS 서버와의 통신 설정에 대한 자세한 내용은 "RADIUS 구성"장을 참조하십시오.

27.1.4.2 권한 단계에서 비밀번호 보호를 활성화하기

aaa authentication enable default 명령을 사용하여 사용자가 권한 있는 EXEC 명령 수준에 액세스 할 수 있는지 여부를 결정하는 데 사용되는 일련의 인증 방법을 만듭니다. 최대 네 가지 인증 방법을 지정할 수 있습니다. 추가 메소드 인증은 이전 메소드가 실패 할 경우에만 오류를 반환하는 경우에만 사용됩니다. 모든 메소드가 오류를 반환하더라도 인증이 성공하도록 지정하려면 명령 행에서 마지막 메소드로 none을 지정하십시오.

전역 구성 모드에서 다음 명령을 사용하십시오.

명령어	설명
aaa authentication enable default *method1* [*method2...*]	특정 단계를 요구하는 사용자에 대한 사용자 ID 및 암호 확인을 사용합니다.

method 인수는 인증 알고리즘이 시도하는 메소드의 실제 목록을 입력 된 순서대로 참조합니다.

다음 표는 지원되는 사용 가능 인증 방법을 나열합니다.

단어	설명
enable	인증할 경우 사용할 입장 암호를 사용합니다.
group *group-name*	aaa group server radius 또는 aaa group server tacacs + 명령에 정의 된 인증을 위해 RADIUS 또는 TACACS + 서버의 하위 집합을 사용합니다.
group radius	인증을 위해 모든 RADIUS 호스트 목록을 사용합니다.
line	인증에 회선 암호를 사용합니다.
none	인증을 사용하지 않습니다.

27.1.4.3 AAA 인증 배너 메시지 구성

AAA는 구성 가능한 개인화 및 실패한 로그인 배너의 사용을 지원합니다. 사용자가 AAA를 사용하여 인증되도록 시스템에 로그인 할 때 및 어떤 이유로 든 인증에 실패 할 때 표시 될 메시지 배너를 구성 할 수 있습니다.

로그인 배너 구성하기

사용자가 로그인 할 경우 표시 될 배너를 구성하려면 (로그인 용 기본 메시지 교체) 전역 구성 모드에서 다음 명령을 사용하십시오.

명령어	설명
aaa authentication banner *delimiter text-string delimiter*	개인적인 로그인 배너를 만듭니다

로그인 배너 구성 실패

사용자가 로그인에 실패 할 때마다 표시되는 메시지를 구성하려면 (로그인 실패에 대한 기본 메시지 대체) 전역 구성 모드에서 다음 명령을 사용하십시오.

명령어	설명
aaa authentication fail-message *delimiter text-string delimiter*	로그인 실패 메시지를 나타냅니다.

설명

로그인 배너를 만들려면 구분 문자를 구성해야 합니다. 이 문자는 다음 텍스트 문자열이 배너로 표시되고 텍스트 문자열 자체에 표시되도록 시스템에 알립니다. 구분 문자는 텍스트 문자열의 끝에서 반복되어 배너의 끝을 나타냅니다. 분리 문자는 확장 ASCII 문자 세트의 단일 문자 일 수 있지만 일단 분리 문자로 정의되면 해당 문자는 배너를 구성하는 텍스트 문자열에 사용할 수 없습니다.

27.1.4.4 AAA 빠른 사용자 이름 인증

사용자에게 사용자 이름을 입력하라는 메시지가 표시 될 때 표시되는 텍스트를 변경하려면 전역 구성 모드에서 aaa authentication username-prompt 명령을 사용하십시오. 기본 사용자 이름 프롬프트 텍스트로 돌아가려면 이 명령의 no 형식을 사용하십시오.

aaa authentication username-prompt 명령은 원격 TACACS + 서버가 제공하는 대화 상자를 변경하지 않습니다. 전역 구성 모드에서 구성하려면 다음 명령을 사용하십시오.

명령어	설명
aaa authentication username-prompt *text-string*	사용자의 이름을 입력하라는 메시지가 표시 될 때 표시할 문자열입니다.

27.1.4.5 AAA 빠른 비밀번호 인증

사용자에게 암호를 묻는 메시지가 표시 될 때 표시되는 텍스트를 변경하려면 글로벌 구성 모드에서 aaa authentication password-prompt 명령을 사용하십시오. 기본 암호 프롬프트 텍스트로 돌아가려면 이 명령의 no 형식을 사용하십시오.

aaa authentication password-prompt 명령은 원격 TACACS + 서버가 제공하는 대화 상자를 변경하지 않습니다. 구성하려면 다음을 사용하십시오.

명령어	설명
aaa authentication password-prompt *text-string*	사용자 암호의 문자열을 입력합니다.

27.1.4.6 사용자 인증 만들기

다음과 같은 경우에 유용한 사용자 이름 기반 인증 시스템을 생성할 수 있습니다.

- TACACS를 지원할 수 없는 네트워크에 TACACS와 유사한 사용자 이름 및암호화 된 암호 인증 시스템을 제공합니다.
- 특별한 경우 로그인을 제공하기 위해 : 예를 들어 액세스 목록 검증, 패스워드 검증, 로그인 시 자동 명령 실행, "탈출 불가"상황

사용자 이름 인증을 설정하려면 시스템 구성에 필요한대로 전역 구성 모드에서 다음 명령을 사용하십시오.

이 명령의 no 형식을 사용하여 사용자 이름을 삭제하십시오.

username *name* {**nopassword** **|** **password** *password* **|** **password encryption-type** *encrypted-password*}

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty | aux**] *line-number* [*ending-line-number*]]

username *name* [**noescape**] [**nohangup**]

username *name* [**privilege** *level*]

username *name* [**user-maxlinks** *number*]

no username *name*

27.1.4.7 비밀번호 넣기

여러 권한 레벨에 대한 액세스를 제어하기 위해 로컬 암호를 설정하려면,
전역 구성 모드에서 enable password 명령을 사용하십시오. 암호 요구 사항을 제거하려면 이 명령의 no 형식을 사용하십시오.

enable password { [***encryption-type***] *encrypted-password*} [**level** *level*]

no enable password [**level** *level*]

27.1.5 AAA 인증 구성 예제

- RADIUS 인증 예제

이 절에서는 RADIUS를 사용한 하나의 구성 예를 제공합니다.

다음은 RADIUS를 인증하고 권한을 부여하는 방법을 보여줍니다.

aaa authentication login radius-login group radius local

aaa authorization network radius-network radius

line vty

login authentication radius-login

이 샘플 RADIUS 인증 및 권한 부여 구성의 행은 다음과 같이 정의됩니다

aaa authentication login radius-login radius local 명령은 로그인 프롬프트에서 인증을 위해 RADIUS를 사용하도록 라우터를 구성합니다. RADIUS가 오류를 반환하면 사용자는 로컬 데이터베이스를 사용하여 인증됩니다.
aaa authentication ppp radius-ppp radius 명령은 사용자가 아직 로그인하지 않은 경우 CHAP 또는 PAP를 사용하여 PPP 인증을 사용하도록 소프트웨어를 구성합니다. EXEC 기능이 사용자를 인증 한 경우 PPP 인증이 수행되지 않습니다.

aaa authorization network radius-network radius 명령 명령은 RADIUS에 네트워크 인증, 주소 할당 및 기타 액세스 목록을 쿼리합니다.

login authentication radius-login 명령은 3 행에 radius-login 메소드 목록을 사용 가능하게 합니다.

27.1.6 AAA 작업 구성 허가 목록

AAA를 사용하여 EXEC 기능을 허가합니다.

27.1.7 AAA 작업 구성 허가

AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

3. 별도의 보안 서버를 사용하려면 RADIUS, TACACS + 또는 Kerberos와 같은 보안 프로토콜 매개 변수를 구성하십시오.
4. AAA 인증 명령을 사용하여 인증을 위한 방법 목록을 정의합니다.
5. 필요한 경우 메서드 목록을 특정 인터페이스 또는 행에 적용합니다.

27.1.7.1 AAA를 사용하여 EXEC 권한 구성

aaa authorization 명령을 사용하여 권한 부여를 활성화하십시오.

aaa authorization exec 명령을 사용하여 권한 부여를 실행하여 사용자가 EXEC 쉘을 실행할 수 있는지 여부를 판별하십시오. 이 기능은 자동 명령 정보와 같은 사용자 프로파일 정보를 리턴 할 수 있습니다.

라인 구성 명령 로그인 권한을 사용하여 다음의 명령을 사용하십시오.

명령어	설명
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	전역 권한을 부여하는 목록을 설정합니다.
line [**console** | **vty**] *line-number* [*ending-line-number*]	인증 방법 목록을 적용 할 회선에 대한 회선 구성 모드를 시작합니다.
login authorization {**default** | *list-name*}	권한리스트를 행 또는 행 세트에 적용합니다. (행 구성 모드에서)

키워드 list-name은 권한 부여 메소드 목록의 이름을 지정하는 데 사용되는 문자열입니다. 키워드 메소드는 권한 부여 프로세스 중 실제 메소드를 지정합니다.
메소드 목록을 사용하면 하나 이상의 보안 프로토콜을 지정하여 인증에 사용할 수 있으므로 초기 방법이 실패 할 경우 백업 시스템을 보장 할 수 있습니다. 시스템은 나열된 첫 번째 방법을 사용하여 특정 네트워크 서비스에 대해 사용자에게 권한을 부여합니다. 해당 메소드가 응답하지 않으면 시스템은 메소드 목록에 나열된 다음 메소드를 선택합니다. 이 프로세스는 나열된 권한이 부여 된 메소드와의 성공적인 통신이 이루어 지거나 정의 된 모든 메소드가 모두 사용될 때까지 계속됩니다. 지정된 모든 메소드가 응답하지 않고 시스템이 EXEC 쉘에 들어가기를 원하면 명령 행에서 마지막 인증 메소드로 none을 지정해야 합니다.

기본 매개 변수를 사용하여 기본 목록을 설정하면 기본목록이 모든 인터페이스에 자동으로 적용됩니다. 예를 들어, 다음 명령을 사용하여 반지름을 지정하십시오.

aaa authorization exec default group radius

노트:

메소드 목록이 정의되지 않으면 로컬 서비스를 사용할 수 없으며 권한이 전환됩니다.

다음 표에는 현재 지원되는 EXEC 인증 모드가 나열되어 있습니다.

단어	설명
group *WORD*	권한 부여를 위해 지정 된 서버 그룹을 사용합니다.
group radius	Radius 사용을 승인합니다.
local	로컬 데이터베이스 사용을 허가합니다.

if-authenticated	사용자가 인증 된 경우 사용자가 요청 된 기능에 엑세스가 가능합니다.
none	권한 부여는 수행되지 않습니다.

27.1.8 AAA 허용 예제

1 EXEC 로컬 허가 예제

```
aaa authentication login default local
aaa authorization exec default local
!
username exec1 password 0 abc privilege 15
username exec2 password 0 abc privilege 10
username exec3 nopassword
username exec4 password 0 abc user-maxlinks 10
username exec5 password 0 abc autocommand telnet 172.16.20.1
!
```

이 샘플 RADIUS 인증 구성의 줄은 다음과 같이 정의됩니다

aaa authentication login default local 명령은 로그인 인증의 기본 메소드 목록을 정의합니다. 이 방법 목록은 모든 로그인 인증 서버에 자동으로 적용됩니다.

aaa authorization exec default local 명령은 exec 권한 부여의 기본 메소드 목록을 정의합니다. 메소드 목록은 exec 쉘을 입력해야 하는 모든 사용자에게 자동으로 적용됩니다.

사용자 이름은 exec1이고 로그인 암호는 abc입니다. EXEC 권한 수준은 15 (가장 높은 수준)입니다. 즉, 권한 수준이 15 인 exec1 사용자가 exec 셸에 로그인하면 모든 명령을 검사하고 수행 할 수 있습니다.

사용자 이름은 exec2이고, 로그인 암호는 abc이며, EXEC 권한 레벨은 10입니다. 즉, 권한 레벨이 10 인 사용자 exec2가 EXEC 쉘에 로그인하면 명령

특정 레벨이 10 미만인 것을 확인하고 수행 할 수 있습니다.

사용자 이름은 exec3이며 로그인에 암호가 필요하지 않습니다.

사용자 이름은 exec4, 로그인 암호는 abc, 사용자의 최대 링크 수는 10입니다.

사용자 이름은 exec5이고 로그인 암호는 abc이며 사용자는 exec 쉘에 로그인
할 때 즉시 telnet 172.16.20.1을 수행합니다..

27.1.9 AAA 구성 작업 목록 계산하기

AAA를 사용하여 연결 계정 구성

AAA를 사용하여 네트워크 계정 구성

27.1.9 AAA 구성 작업 계산하기

AAA계정을 구성하려면 다음 구성 프로세스를 수행하십시오

1 별도의 보안 서버를 사용하려면 RADIUS, TACACS + 또는 Kerberos와 같은 보안 프로토콜 매개 변수를 구성하십시오.

2 AAA 계정 명령을 사용하여 계정에 대한 방법 목록을 정의합니다..

3 필요한 경우 메서드 목록을 특정 인터페이스 또는 행에 적용합니다.

27.1.10.1 AAA를 사용하여 계정 연결 구성

aaa accounting 명령을 사용하여 AAA 계정을 활성화하십시오.

네트워크 액세스 서버에서 만들어진 모든 아웃 바운드 연결에 대한 계정 정보를 제공하는 방법 목록을 만들려면 aaa accounting connection 명령을 사용하십시오.

명령어	설명
aaa accounting connection {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} **group** *groupname*	전역 계정 목록을 만듭니다

list-name 키워드는 설정 목록의 문자열을 명명하는 데 사용됩니다.

키워드는 회계 프로세스 중에 채택 된 실제 방법을 지정합니다.

다음 표는 현재 지원되는 연결 계정 방법 목록입니다.

단어	설명
group *WORD*	그룹 서버에 계정의 이름을 만듭니다
group radius	Radius 계정에 접속합니다.
none	지정된 행 또는 인터페이스에 대한 계정 서비스를 비활성화합니다.
stop-only	요청한 사용자 프로세스가 끝날 때 "중지"기록 지를 보냅니다.
start-stop	RADIUS 또는 TACACS +는 요청 된 프로세스가 시작될 때 "시작"계정 알림을 보내고 프로세스가 끝날 때 "중지"계정 알림을 보냅니다.

27.1.10.2 AAA를 사용하는 네트워크 계정의 구성

aaa accounting 명령을 사용하여 AAA 계정을 활성화하십시오.

SLIP, PPP, NCP 및 ARAP 세션에 대한 계정 정보를 제공하는 방법 목록을 만들려면 전역 구성 모드에서 aaa accounting network 명령을 사용하십시오.

명령어	설명
aaa accounting network {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} **group** *groupname*	전역모드에서 계정을 들어갑니다.

list-name 키워드는 설정 목록의 문자열을 명명하는 데 사용됩니다. 키워드 키워드는 회계 프로세스 중에 채택 된 실제 방법을 지정합니다.

다음 표는 현재 지원되는 네트워크 계정 방법을 나열합니다.

단어	설명
group *WORD*	계정에 대해 명명 된 서버 그룹을 사용 가능하게 합니다.
group radius	radius 계정에 들어갑니다.
none	지정된 행 또는 인터페이스에 대한 계정 서비스를 비활성화합니다.
stop-only	요청한 사용자 프로세스가 끝날 때 "중지"기록 회계 통지를 보냅니다.
start-stop	RADIUS 또는 TACACS +는 요청 된 프로세스가 시작될 때 "시작"계정 알림을 보내고 프로세스가 끝날 때 "중지"계정 알림을 보냅니다.

27.1.10.3 AAA 계정 업데이트

정기적 인 임시 계정 레코드를 계정 서버로 보낼 수 있게 하려면 전역구성 모드에서 aaa accounting update 명령을 사용하십시오. 임시 계정 업데이트를 사용하지 않으려면 이 명령의 no 형식을 사용하십시오.

명령어	설명
aaa accounting update [**newinfo**] [**periodic** *number*]	AAA 계정을 업데이트 합니다.

newinfo 키워드가 사용되면 보고 할 새 계정 정보가 있을 때마다 계정 레코드가 계정 서버로 보냅니다. 예를 들면, IPCP (IP Control Protocol)가 원격 peer와의 IP 주소 협상을 완료 할 때입니다. 임시 계정 레코드에는 원격 peer에서 사용하는 협상 된 IP 주소가 포함됩니다..

periodic 키워드와 함께 사용하면 임시 계정 레코드가 인수 번호에 정의 된 대로 주기적으로 전송됩니다. 임시 계정 레코드에는 계정 레코드가 전송 될 때까지 해당 사용자에 대해 기록 된 모든 계정 정보가 들어 있습니다.

newinfo 및 periodic 키워드를 모두 사용하는 경우보고 할 새 계정 정보가 있을 때

마다 임시 계정 레코드가 계정 서버로 보내 인수 레코드에 정의 된 대로 계정 레코드가 정기적으로 계정 서버로 보내 집니다. 예를 들어, aaa accounting update newinfo periodic number 명령을 구성하면 현재 로그인 한 모든 사용자가 주기적인 임시 계정 레코드를 생성하고 새 사용자는 newinfo 알고리즘을 기반으로 계정 레코드를 생성합니다.

27.1.10.4 AAA 사용하지 않는 계정 억제

AAA 시스템이 사용자 이름 문자열이 NULL 인 사용자에 대한 계정 레코드를 보내지 않게 하려면 글로벌 구성 모드에서 aaa accounting suppress null-username 명령을 사용하십시오. 사용자 이름이 NULL 인 사용자에게 레코드를 보내려면 이 명령의 no 형식을 사용하십시오.

aaa accounting suppress null-username

27-2장 RADIUS 구성하기

이 장에서는 원격 인증 다이얼 인 사용자 서비스 (RADIUS) 보안 시스템에 대해 설명하고 해당 작업을 정의하며 RADIUS 기술을 사용하기에 적절하고 부적합한 네트워크 환경을 식별합니다. "RADIUS 구성 작업 목록"절에서는 AAA (authentication, authorization, and accounting) 명령 집합으로 RADIUS를 구성하는 방법에 대해 설명합니다.

27.2.1소개

27.2.1.1 RADIUS 안내

이 장에서는 원격 인증 다이얼 인 사용자 서비스 (RADIUS) 보안 시스템에 대해
설명하고 해당 작업을 정의하며 RADIUS 기술을 사용하기에 적절하고 부적절한
네트워크 환경을 식별합니다. "RADIUS 구성 작업 목록"절에서는 AAA (authentication, authorization, and accounting) 명령 집합으로 RADIUS를 구성하는 방법에 대해 설명합니다

RADIUS를 지원하는 여러 공급 업체 서버가 있는 네트워크 예를 들어 여러 공급 업체의 액세스 서버는 단일 RADIUS 서버 기반 보안 데이터베이스를 사용합니다. 여러 공급 업체의 액세스 서버가 있는 IP 기반 네트워크에서 전화 접속 로그인 사용자는 Kerberos 보안 시스템과 함께 작동하도록 사용자 지정된 RADIUS 서버를 통해 인증됩니다.

사용자가 단일 서비스에만 접근하는 네트워크입니다. RADIUS를 사용하면
단일 호스트, 텔넷과 같은 단일 유틸리티 또는 PPP (Point-to-Point Protocol)와 같은 단일 프로토콜에 대한 사용자 접근을 제어 할 수 있습니다. 예를 들어 사용자가 로그인하면 RADIUS는이 사용자가 IP 주소 10.2.3.4를 사용하여 PPP를 실행할 수 있는 권한을 확인하고 정의된 액세스 목록을 시작합니다.

리소스 사용 통계가 필요한 네트워크. RADIUS 인증이나 권한 부여와 상관없이 RADIUS 계정을 사용할 수 있습니다. RADIUS 계정 기능을 사용하면 서비스 시작 및 종료 할 경우 데이터를 전송할 수 있으며 세션 중에 사용 된 리소스 (시간, 패킷, 바이트 등)의 양을 나타냅니다. 인터넷 서비스 공급자 (ISP)는 프리웨어 기반 버전의 RADIUS 액세스

제어 및 회계 소프트웨어를 사용하여 특별한 보안 및 청구 요구 사항을 충족시킬 수 있습니다.

다음 네트워크 보안 상황에서는 RADIUS가 적합하지 않습니다.

멀티 프로토콜 액세스 환경인 경우
RADIUS는 다음 프로토콜을 지원하지 않습니다.

- AppleTalk Remote Access (ARA)
- NetBIOS Frame Control Protocol (NBFCP)
- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD 연동
- 스위치-스위치 인 상황. RADIUS는 양방향의 인증을 제공하지 않습니다..
- 네트워크의 다양한 서비스. RADIUS 는 일반적으로 하나의 서비스로만 사용자와 바인딩합니다

27.2.1.2 RADIUS 작동

사용자가 RADIUS를 사용하여 액세스 서버에 로그인하고 인증하려고 하면 다음 단계가 발생합니다.

1 사용자에게 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.

2 사용자의 암호화 된 비밀번호는 네트워크를 통해 RADIUS서버로 전송됩니다.

3 사용자가 RADIUS 서버에서 다음 응답 중 하나를 받습니다.

a. ACCEPT— 사용자가 인증되었습니다.

b. REJECT—사용자가 인증되지 않았으며 사용자 이름과 암호를 다시 입력하라는 메시지가 표시되거나 접근이 거부됩니다.

c. CHALLENGE—RADIUS 서버에서 발생하는 사용자로부터 추가 데이터를 수집합니다.

d. CHANGE PASSWORD—사용자가 새 암호를 선택하도록 요청하는 RADIUS 서버에 요청합니다.

ACCEPT 또는 REJECT 응답은 EXEC 또는 네트워크 인증에 사용되는 추가 데이터와 함께 제공됩니다. RADIUS 인증을 사용하려면 먼저 RADIUS 인증을 완료해야 합니다. ACCEPT 또는 REJECT 패킷에 포함

된 추가 데이터는 다음과 같이 구성됩니다.

• 호스트 또는 클라이언트 IP 주소, 액세스 목록 및 사용자 시간 초과를 포함한 연결 매개 변수.

27.2.2 RADIUS 작업 그룹 구성

스위치 또는 액세스 서버에 RADIUS를 구성하려면 다음 작업을 수행해야합니다.

RADIUS 인증을 한 방법 목록을 정의하는 aaa authentication 전역 구성 명령 aaa authentication 명령 사용에 대한 자세한 정보는 "인증 구성"장을 참조하십시오.

정의 된 메소드 목록을 사용하려면 line 및 interface 명령을 사용하십시오. 자세한 정보는 "인증 구성"장을 참조하십시오.

1. 다음 구성 작업은 선택 사항입니다.

aaa authorization global 명령을 사용하여 특정 사용자에게 권한을 부여 할 수 있습니다

기능. aaa authorization 명령 사용에 대한 자세한 정보는,"인증 구성"장을 참조하십시오.

aaa accounting 명령을 사용하여 RADIUS 연결에 대한 계정을 활성화 합니다.

aaa accounting 명령 사용에 대한 자세한 내용은 "계정구성"장을 참조하십시오.

27.2.3 RADIUS 구성 작업 목록

- RADIUS 서버 통신으로 전환 구성 벤더 특정
- RADIUS 특성을 사용하도록 스위치 구성
- RADIUS 인증 지정
- RADIUS 인증 지정
- RADIUS 계정 지정

27.2.4 RADIUS 작업 구성

27.2.4.1 RADIUS 서버 통신을 스위치 구성하기

RADIUS 호스트는 일반적으로 Livingston, Merit, Microsoft 또는 다른 소프트웨어 제공 업체의 RADIUS 서버 소프트웨어를 실행하는 다중 사용자 시스템입니다.

RADIUS 서버와 Cisco 라우터는 공유 암호 텍스트 문자열을 사용하여 암호를 암호화하고 응답을 교환합니다.

RADIUS가 AAA 보안 명령을 사용하도록 구성하려면 RADIUS 서버 데몬을 실행하는 호스트와 라우터와 공유하는 비밀 텍스트 (키) 문자열을 지정해 니다.

서버 별 RADIUS 서버 통신을 구성하려면 글로벌 구성 모드에서 다음 명령을 사용하십시오

명령어	설명
radius-server host *ip-address* [**auth-port**	원격 RADIUS 서버 호스트의 IP 주소 와 호스트 이름을 지정하고 인증 및 계정 대상 포
radius-server key *string*	라우터와 a RADIUS 서버 작업

라우터와 RADIUS 서버 간의 전역 통신 설정을 구성하려면 전역 구성 모드에서 다음 radius-server 명령을 사용하십시오.

명령어	설명
radius-server retransmit *retries*	**포기하기 전에 스위치가 각 RADIUS 요청을 서버에 전송하는 횟수를 지정합니다 (기본값은 2).**
radius-server timeout *seconds*	요청을 재전송하기 전에 스위치가 RADIUS 요청에 대한 응답을 기다리는 시간 (초)을
radius-server deadtime *minutes*	RADIUS 인증 요청에 응답하지 않는 RADIUS 서버가 몇 분 동안 전달되는지 지정합니다.

27.2.4.2 공급 업체별 RADIUs 특성을 사용하도록 스위치를 구성

IETF (Internet Engineering Task Force) 초안 표준은 공급 업체별 특성 (특성 26)을 사용하여 네트워크 액세스 서버와 RADIUS 서버간에 공급 업체별 정보를 전달하는 방법을 지정합니다.

공급 업체별 특성 (VSA)을 사용하면 공급 업체는 일반적인 용도에 적합하지 않은 자체 확장 특성을 지원할 수 있습니다.

공급 업체 ID 및 VSA에 대한 자세한 내용은 RFC 2138, RADIUS (Remote Authentication Dial-In User Service)를 참조하십시오. VSA를 인식하고 사용하도록 네트워크 액세스 서버를 구성하려면 다음 명령을 사용하십시오.

명령어	설명
radius-server vsa send [authentication]	서버가 RADIUS IETF 속성 26에 정의 된 대로 VSA를 인식하고 사용할 수 있습니다.

27.2.4.3 특정 RFADIUS 인증

RADIUS 서버를 식별하고 RADIUS 인증 키를 정의한 후에는 RADIUS 인증을 위한 방법 목록을 정의해야 합니다. RADIUS 인증은 AAA를 통해 용이하므로 RADIUS를 인증 방법으로 지정하여 aaa authentication 명령을 입력해야 합니다. 자세한 내용은 "인증 구성"장을 참조하십시오.

27.2.4.4 특정 RADIUS 허가

AAA 권한을 통해 사용자가 네트워크에 액세스하는 것을 제한하는 매개 변수를
설정할 수 있습니다. RADIUS를 통한 권한 부여는 각 서비스, 사용자 별 계정 목록 및 프로필, 사용자 그룹 지원, IP, IPX, ARA 및 텔넷 지원에 대한 일회성 권한 부여 또는 권한 부여를 포함하여 원격 액세스 제어를 위한 한 가지 방법을 제공합니다. RADIUS 인증은 AAA를 통해 용이하므로 RADIUS를 인증 방법으로 지정하여 aaa authorization 명령을 실행해야 합니다. 자세한 내용은 "인증 구성"장을
참조하십시오.

27.2.4.5 RADIUS 계정 지정하기

AAA 계정 기능을 사용하면 사용자가 액세스하는 서비스는 물론 사용중인 네트워크 리소스의 양을 추적 할 수 있습니다. RADIUS 계정은 AAA를 통해 쉽게 처리되므로 RADIUS를 계정 방법으로 지정하여 aaa accounting 명령을 실행해야 합니다.
자세한 내용은 "계정 구성"장을 참조하십시오.

27.2.5 RADIUS 구성 예제

27.2.5.1 RADIUS 인증과 허가의 예제

다음 예에서는 RADIUS를 사용하여 인증하고 권한을 부여하도록 라우터를 구성하는 방법을 보여줍니다.

aaa authentication login use-radius group radius local

RADIUS 인증 및 권한 부여 구성의 줄은 다음과 같이 정의됩니다

aaa authentication login use-radius radius local 로그인 프롬프트에서 인증을 위해 RADIUS를 사용하도록 라우터를 구성합니다. RADIUS가 오류를 반환하면 사용자는 로컬 데이터베이스를 사용하여 인증됩니다.
use-radius는 RADIUS 및 로컬 인증을 지정하는 메소드 목록의 이름입니다.

RADIUS 인증,권한 부여 및 계정 예제

다음 예에서는 RADIUS를 AAA 명령어와 함께 사용하는 일반 구성을 보여줍니다

radius-server host 1.2.3.4

radius-server key myRaDiUSpassWoRd

username root password AlongPassword

aaa authentication login admins radius local

line vty 1 16

login authentication admins

RADIUS 인증, 권한 부여 및 계정 구성은 다음과 같이 정의됩니다.
radius-server host 명령은 RADIUS 서버 호스트의 IP 주소를 정의합니다.

radius-server key 명령은 네트워크 액세스 서버와 RADIUS 서버 호스트 사이의 공유 비밀 텍스트 문자열을 정의합니다. aaa authentication login admins 그룹 로컬 명령은 RADIUS 인증 및 RADIUS 서버가 응답하지 않는 경우 로컬 인증이 직렬 회선에서 PPP를 사용하도록 지정하는 인증 방법 목록 "dialins"을 정의하고 login authentication admins 명령을 적용합니다 로그인 인증을 위한 "admins"메소드 목록입니다.

27-3장 웹 인증

이 절에서는 웹 인증의 개념과 웹 인증의 구성 및 사용법에 대해 설명합니다.

27.3.1 개요

27.3.1.1 웹 인증

스위치의 웹 인증은 PPPoE 및 802.1x와 같은 연결 제어 모드입니다. 웹 인증을 사용하면 브라우저와 브라우저의 내장 포털 서버의 상호 작용을 통해 로그인 및 로그 아웃 작업을 성공적으로 수행 할 수 있습니다. 로그인 및 로그 아웃 작업중에는 다른 클라이언트 소프트웨어를 설치할 필요가 없습니다.

1. 장치 역할

웹 인증 중에 네트워크 장치가 수행하는 역할은 그림 3-1에 나와 있습니다.

Client: 스위치를 통해 네트워크에 액세스하는 사용자 컴퓨터입니다. 사용자 컴퓨터는 네트워크 브라우저, DHCP 클라이언트의 기능 및 DNS 쿼리를 시작하는 기능을 구성해야 합니다.

DHCP server: 사용자의 IP 주소를 배포하는 것입니다.

AAA server: 사용자 권한 정보를 저장하고 네트워크 접근을 위해 요금을 부과합니다.

Switch: 웹 인증을 사용하는 스위치입니다. 그것은 사용자의 액세스 권한을 제어하고 사용자와 AAA 서버 사이의 에이전트로 작동합니다.

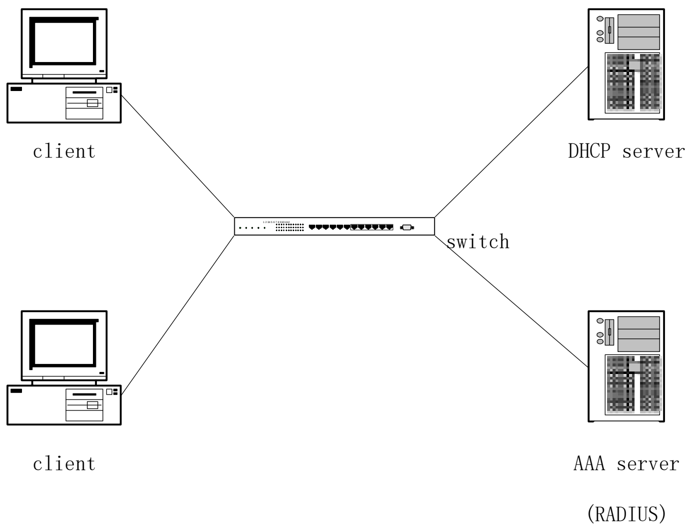


그림 3-1 웹 인증 네트워크

2. 진행 인증

다른 구성 전략에 따라 스위치의 웹 인증 흐름은 DHCP 및 DNS와 같은 프로토콜과 관련 될 수 있습니다. 그것의 전형적인 흐름은 그림 3-2. 웹 인증 흐름에는 일반적으로 다음 단계가 포함됩니다.

DHCP 서버는 사용자가 DHCP 주소 분배 프로세스를 시작한 후 스위치를 통해 DHCP 확인 요청을 사용자에게 전송합니다. 그런 다음 스위치는 사용자를 식별하고 기록합니다. 사용자는 브라우저를 통해 웹 사이트에 액세스합니다 (브라우저의 URL 열의 호스트 부분에 IP 주소가 아닌 도메인 이름을 적어 둡니다). 그러면 사용자 컴퓨터의 DNS 요청이 활성화됩니다.
DNS 서버는 사용자에게 요청 응답을 반환합니다. 스위치는 요청 응답 메시지를 캡처하고 확인 된 주소를 스위치의 내장 포털 서버 주소로 변경합니다.

브라우저에서 DNS 확인을 캡처하면 DHCP 확인 프로세스가 계속됩니다. 스위치는 스위치가 요청을 받은 후에 다른 인증 방법에 따라 해당 인증 페이지를 반환합니다. 사용자가 인증 요청을 제출합니다. 스위치는 사용자가 제출 한 정보를 스위치가 받은 후에 AAA 서버를 통해 사용자를 인증합니다. 인증이 성공하면 AAA 서버에 요금 청구를 시작하라는 통지를 받습니다. 스위치는 사용자에게 네트워크 액세스 권한을 제공하고 인증이 성공한 페이지를 사용자에게 반환합니다. 그 사이에, 스위치는 또한 주기적으로 사용자 온라인 알림을 스위치로 보내는 활성 페이지를 반환합니다.

사용자는 브라우저를 통해 스위치에 로그 아웃 요청을 보냅니다. 그런 다음 스위치는 AAA 서버에 요금 청구를 중지하도록 알리고 사용자로부터 네트워크 액세스 권한을 철회합니다.
성공적인 사용자 인증과 로그 아웃 사이의 기간에 스위치는 주기적으로 사용자 온라인 알림을 감지합니다. 사전 설정된 시간 내에 알림을 받지 못하면 스위치는 사용자가 비정상적으로 로그오프 했다는 사실을 알리고 AAA 서버에 알리지 않고 충전을 중지하고 네트워크 액세스 권한을 사용자로부터 철회합니다..

위의 단계는 구성 전략 및 사용자 작업에 따라 약간 다를 수 있습니다. 예를 들어 인증이 승인되기 전에 사용자가 스위치의 포털 서버에 직접 액세스하면 DNS 관련 프로세스가 활성화되지 않습니다.

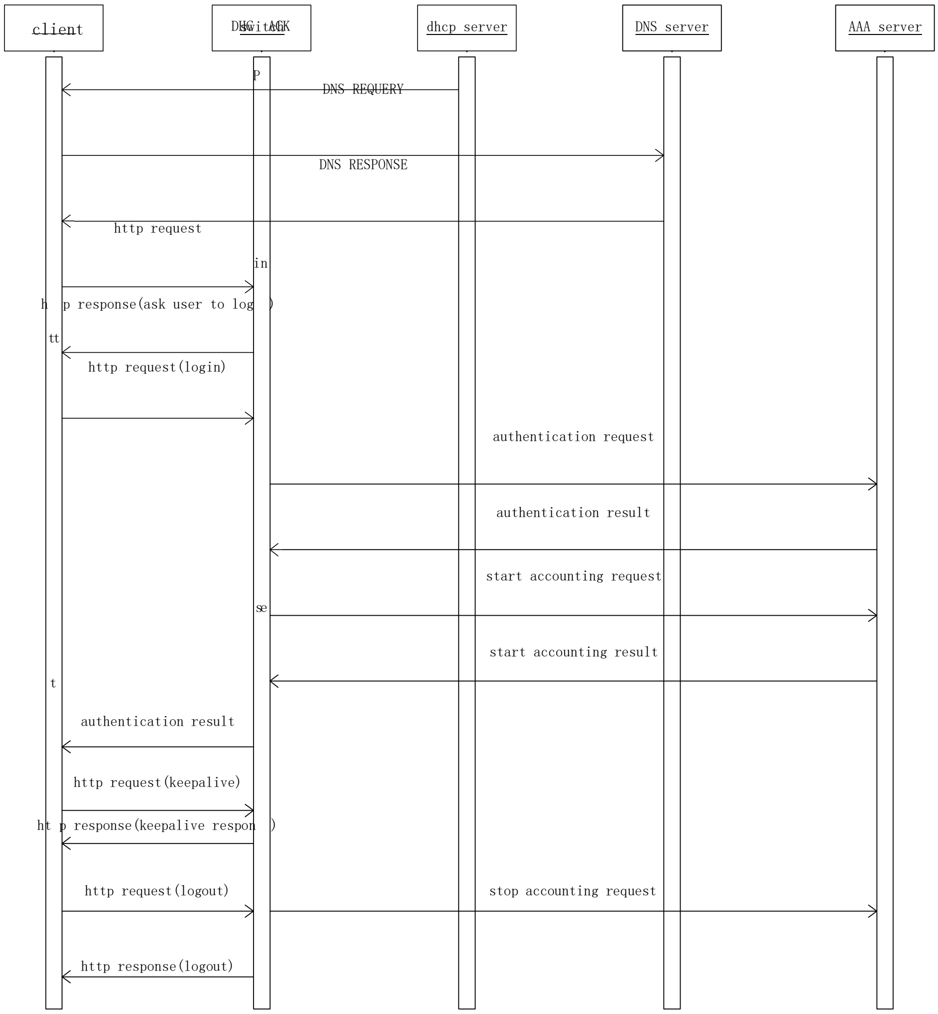


그림 3-2 웹 인증 흐름도

27.3.1.2 웹 인증 계획하기

1. 인증 모드 계획

사용자의 액세스를 제어하는 두 가지 인증 모드가 제공됩니다.

사용자 이름 / 암호 인증 모드: 이 모드에서 스위치는 사용자 이름과 암호를 통해 사용자를 식별하고 사용자 이름에 따라 요금을 부과하기 위해 AAA 서버에
알립니다. 사용자는 브라우저를 통해 사용자 이름과 암호를 입력해야 합니다.

VLAN ID 인증 모드: 이 모드에서 스위치는 사용자가 속한 VLAN ID를 통해 사용자를 식별하고 VLAN ID에 따라 요금을 청구하도록 AAA 서버에 알립니다. 사용자는 네트워크에 액세스하기 전에 웹 페이지에서 해당 작업을 확인해야합니다.
다른 운영 전략은 서로 다른 인증 모드를 채택합니다. 네트워크에 동시에 액세스하는 지원되

는 최대 사용자 수는 인증 모드에 따라 다릅니다. 사용자 이름 / 암호 인증 모드의 경우, 스위치는 동시에 액세스 할 수 있는 사용자의 성능이 허용하는 만큼 지원합니다. VLAN ID 인증 모드의 경우 최대 동시 액세스 사용자 수는 스위치가 지원하는 VLAN 수와 같습니다.

2. 네트워크 토폴로지 계획하기

스위치는 라우팅 인터페이스를 하나의 단위로 사용하여 인증 속성을 설정합니다.
라우팅 인터페이스에서 웹 인증 기능을 사용하는 경우 라우팅 인터페이스를 통한
네트워크 액세스는 모두 웹 인증에 의해 제어됩니다. DHCP 서버, DNS 서버 또는 AAA 서버는 웹 인증 기능이 비활성화 된 인터페이스를 통해 스위치를 연결해야 합니다.
그림 3-3은 상대적으로 일반적인 네트워크 토폴로지를 보여줍니다.

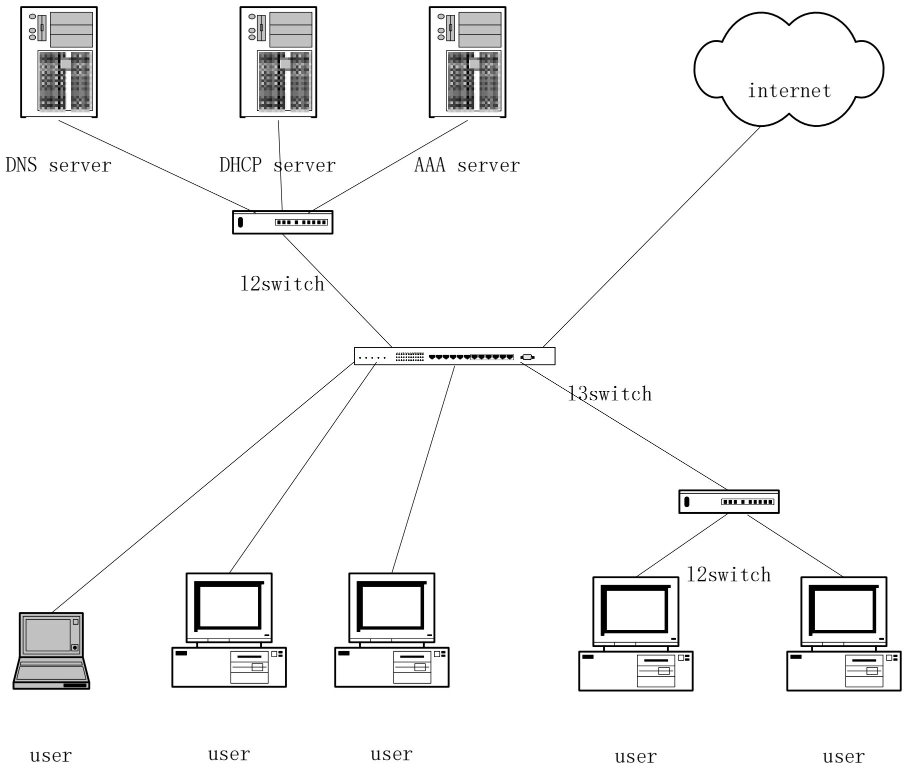


그림 3-3 전형적인 네트워크 토폴로지

27.3.2 웹 인증 구성하기

27.3.2.3 전역 구성

1. 포탈 서버의 주소 구성

전역 구성 모드에서 다음을 이용하여 포털 서버의 주소를 구성하십시오:

명령어	설명
web-auth portal-server *A.B.C.D*	포털 서버의 IP 주소를 구성하십시오.

2. 인증 기간 구성

authtime 매개 변수는 사용자의 인증 최대 시간을 결정합니다. 최대 시간 내에 인증이 승인되지 않으면 스위치는 인증 절차를 종료합니다.

전역 구성 모드에서 다음 명령을 실행하여 인증 기간 (단위: 초)을 구성합니다.

명령어...	설명
web-auth authtime <60-65535>	인증 기간을 구성하십시오.

3. 온라인 알림의 전송 기간 구성

스위치는 브라우저가 보낸 온라인 알림을 통해 사용자가 온라인 상태입니다.

전역 구성 모드에서 다음 명령을 실행하여 전송 기간을 구성하십시오 (단위: 초).

명령어..	설명
web-auth keep-alive <60-65535>	온라인 알림의 전송 기간을 구성합니다.

4. 비정상적인 로그 아웃을 감지하는 기간 설정

스위치가 설정된 기간 동안 브라우저에서 사용자 온라인 알림을 받지 못하면 스위치는 사용자가 비정상적으로 로그 아웃 한 것으로 간주합니다.

전역 구성 모드에서 다음 명령을 실행하여 비정상적인 로그아웃을 감지하는 기간을 구성하십시오.

명령어	설명
web-auth holdtime <60-65535>	비정상적인 로그 아웃 시간을 탐지합니다.

5. VLAN ID 인증을 위한 비밀번호 구성

인증 모드가 VLAN ID로 설정되면 스위치는 사용자 이름으로 vlan n을 취하고 해당 VLAN 일련 번호를 나타내는 n을 사용합니다. 모든 사용자 이름은 동일한 암호를 사용합니다.

전역 구성 모드에서 다음 명령을 실행하여 VLAN ID 인증을 위한 비밀번호를 구성합니다.

명령어	설명
web-auth vlan-password <WORD>	Vlan ID 인증을 위한 암호를 구성하십시오.

27.3.2.2 인터페이스 설정

1. 인증 모드 구성하기

스위치는 두 가지 인증 모드를 제공합니다. 사용자 이름 / 암호 및 VLAN ID

인터페이스 구성 모드에서 다음 명령을 실행하여 인증 모드를 구성하십시오.

명령어...	설명
web-auth mode user | *vlan-id*	인증 모드를 구성하십시오.

2. 인증 방법 목록 구성

서로 다른 인증 방법 목록을 각 인터페이스에 적용 할 수 있습니다. 기본적으로 default라는 인증 방법 목록이 각 인터페이스에 적용됩니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 인증 방법 목록을 구성하십시오.

명령어...	설명
web-auth authentication WORD	인증방법 목록을 구성하십시오.

3. 회계 방법 리스트 구성

각 인터페이스에 다른 회계 방법 목록을 적용 할 수 있습니다. 기본적으로 default 라는 회계 방법 목록이 각 인터페이스에 적용됩니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 계정 방법 목록을 구성합니다.

명령어...	설명
web-auth accounting WORD	게정 메소드 목록을 구성하십시오.

27.3.2.3 웹 인증 실행하기

글로벌 구성 및 인터페이스 구성이 요구 사항을 충족하면 지정된 라우팅 스위치에서 웹 인증을 활성화 할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 웹 인증을 활성화합니다.

명령어...	설명
web-auth enable	웹 인증을 사용합니다.

27.3.3웹 인증 모니터링 및 유지 보수

27.3.3.1 전역 구성 확인하기

권한 모드에서 다음 명령을 실행하시오.

명령어..	설명
show web-auth	전역 구성 모드 확인

27.3.3.2 인터페이스 구성 확인하기

인터페이스 구성 모드에서 다음 명령을 실행하여 인터페이스 구성을 확인하십시오.

명령어...	설명
show web-auth interface [vlan | SuperVlan]	인터페이스 구성 확인

27.3.3.3 사용자 상태 확인하기

권한 모드에서 다음 명령을 실행하여 사용자 상태를 확인하십시오.

명령어...	설명
show web-auth user	사용자 상태를 확인

27.3.3.4 강제적인 사용자 내보내기

권한 모드에서 다음 명령을 실행하여 사용자 상태를 확인하십시오.

명령어	설명
web-auth kick-out user-IP	강제로 사용자를 내보냅니다.

27.3.4 웹 구성 연동 예제

네트워크 토폴로지

그림 참조 3-4:

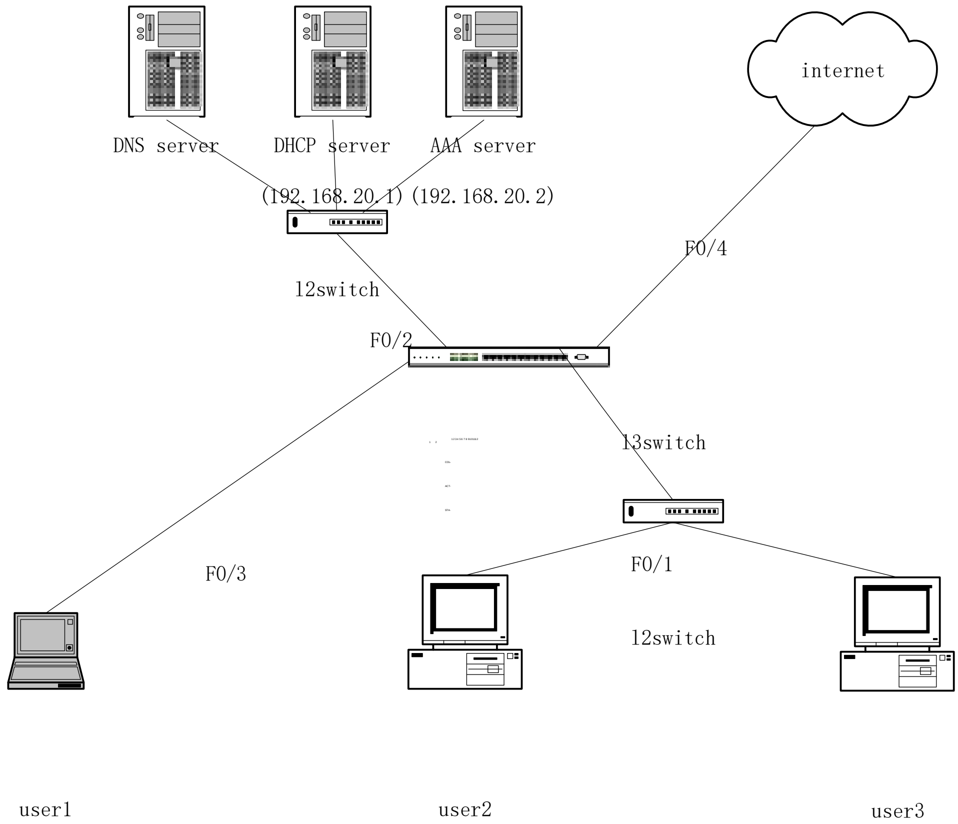


그림 3-4 네트워크 토폴로지

구성도

aaa authentication login auth-weba radius

aaa accounting network acct-weba start-stop radius

!

radius-server host 192.168.20.2 auth-port 1812 acct-port 1813

radius-server key 405.10

!

ip dhcpd enable

ip http server

!

vlan 1-4

!

web-auth portal-server 192.168.20.41

web-auth holdtime 3600

web-auth authtime 600

web-auth keep-alive 180

2 계층의 인터페이스 구성

```
interface FastEthernet0/1
 switchport pvid 1
interface FastEthernet0/2
 switchport pvid 2
interface FastEthernet0/3
 switchport pvid 3
interface FastEthernet0/4
 switchport pvid 4
```

라우팅 인터페이스의 설정

```
interface VLAN1
 no ip directed-broadcast
 ip helper-address 192.168.20.1
 web-auth accounting acct-weba
 web-auth authentication auth-weba
 web-auth mode vlan-id
 web-auth enable
!
interface VLAN2
 ip address 192.168.20.41 255.255.255.0
 no ip directed-broadcast
!
interface VLAN3
 no ip directed-broadcast
 ip helper-address 192.168.20.1
 web-auth accounting acct-weba
 web-auth authentication auth-weba
 web-auth mode user
 web-auth enable
!
interface VLAN4
 no ip directed-broadcast
!
```

28-1장 클러스터 구성 관리

28.1.1 개요

스위치 클러스터는 단일 엔티티로 관리 할 수 있는 스위치 그룹입니다. 클러스터에는 명령 스위치로 작동하는 스위치가 있어야 하며 최대 255 개의 스위치를 동시에 구성원 스위치로 클러스터에 조인 할 수 있습니다. 클러스터의 단일 접근 노드로서 명령 스위치는 구성, 관리 및 모니터하는 데 사용됩니다. 하나의 스위치는 특정 순간에 하나의 클러스터에 속합니다.

28.1.2 클러스터 구성 작업 목록 관리

- 계획 클러스터
- 클러스터 만들기
- 클러스터 구성
- 대기 그룹의 상태 모니터링
- SNMP를 사용하여 클러스터 관리
- 웹을 사용하여 클러스터 관리

28.1.3 클러스터 구성 작업 관리

28.1.3.1 클러스터 계획하기

1 VLAN

클러스터를 통해 스위치를 관리하려면 클러스터의 명령 스위치, 구성원 스위치 및 후보 스위치에 기본 VLAN이 있어야합니다. 이러한 스위치의 기본 VLAN 인터페이스는 이미 존재합니다.

2 스위치 멤버 및 후보 스위치 자동 검색

명령 스위치는 BDP 프로토콜을 사용하여 구성원 스위치, 후보 스위치 및 기타 클러스터를 찾습니다. 또한 명령 스위치는 BDP 프로토콜을 사용하여 네트워크 토폴로지를 찾습니다. 따라서 구성원 스위치, 후보 스위치 및 기타 클러스터에서 BDP 프로토콜을 실행하고 상호 연결된 인터페이스에서 BDP를 활성화 해야 합니다.

3 IP 주소

관리 스테이션이 telnet, http 및 snmp와 같은 TCP / IP 관리 모드를 통해 클러스터에 접근하는 경우 관리 스테이션에서 접근 할 수 있는 명령 스위치의 IP 주소를 구성해야 합니다. 클러스터의 구성 스위치에 IP 주소를 구성하지 않아도 됩니다.

구성원 스위치가 클러스터에서 연결 된 후 명령 스위치는 각 구성원 스위치에 IP 주소를 분배합니다. 이 IP 주소는 명령 스위치에 구성된 클러스터의 IP 풀에서 선택됩니다. 주소 풀을 계획 할 때 서비스 주소는 주소 풀의 주소와 같을 수 없습니다. 주소 풀의 주소 번호는 클러스터의 구성원 스위치 (명령 스위치 포함)의 최대 수보다 작을 수 없습니다.

28.1.3.2 클러스터 만들기

(1)스위치 명령어 활성화

스위치를 명령 스위치로 설정하려면 다음 명령을 실행하십시오.

명령어	설명
cluster mode commander *cluster-name*	현재 스위치를 명령 스위치로 설정합니다.

(2) 대기 스위치 활성화

스위치를 명령 스위치로 설정하려면 다음 명령을 실행하십시오:

명령어	설명
cluster mode commander *member*	현재 스위치를 대기 스위치로 설정합니다.

(3) 스위치에 멤버 추가

다음 명령을 실행하여 MAC 주소가 있는 대기스위치를 클러스터에 추가합니다:

명령어	설명
cluster member [**id** *member-id*] **mac-address** *H.H.H* [**password** *enable-password*]	스위치 멤버를 추가합니다.

28.1.3.3 클러스터 설정

1 IP pool 설정

다음 명령을 실행하여 클러스터 관리를 위해 IP 주소 풀을 구성하십시오.

명령어	설명
cluster address-pool *A.B.C.D A.B.C.D*	Configures the IP address pool.

2 Hellotime 설정

Hellotime (단위 : 초)을 구성하여 명령 스위치와 일반 스위치 간에 핸드 셰이크 메시지를 보내도록 간격을 수정할 수 있습니다.

글로벌 구성 모드에서 다음 명령을 실행하여 클러스터 Hellotime을 구성합니다.

명령어	설명
cluster hellotime *<1-300>*	명령 스위치와 구성원 스위치 사이에 hello 메시지를 보내는 간격을 구성합니다.

3 Holdtime 구성

일반 스위치와 명령 스위치가 일정한 간격으로 peer에서 핸드 셰이크 메시지를 받지 못하면 peer가 다운 상태에 있다고 생각합니다. 구성 할 수 있습니다.

holdtime을 사용하여 간격 값을 변경하십시오.

글로벌 구성 모드에서 다음 명령을 실행하여 클러스터 holdtime을 구성합니다.

명령어	설명
cluster holdtime *<1-300>*	명령 스위치와 일반 스위치 간에 핸드 셰이크 메시지를 보내는 간격을 구성합니

4 탐지 프로토콜의 홉 개수 구성

클러스터는 홉 번호를 사용하여 클러스터에 있는 스위치의 거리를 측정합니다. 명령 스위치에 구성된 검색 프로토콜의 홉 수는 클러스터 경계와 가장 가까운 후보 스위치 사이의 거리와 같습니다.

다음 명령을 실행하여 클러스터에 대한 검색 프로토콜의 홉 번호를 구성합니다.

명령어	설명
cluster discovery *hop-count*	탐지 프로토콜의 PDP 홉 번호를 구성합니다.

28.1.3.4 대기 그룹의 상태 모니터링

클러스터의 구성 및 상태를 모니터링하려면 다음 명령을 실행하십시오.

명령어	설명
show cluster	대기 그룹의 상태를 모니터링합니다
show cluster *member*	클러스터 멤버를 확인합니다.
show cluster candidate	예비 클러스터를 확인합니다
show cluster topo	클러스터 구성도를 확인합니다
show address-pool	클러스터 주소 풀을 확인합니다..

28.1.3.5 SNMP를 사용하여 클러스터 관리

클러스터가 생성되면 명령 스위치를 통해 일반 스위치와 snmp 응용 프로그램 간에 snmp 메시지를 전송할 수 있습니다. 자세한 프로세스는 다음과 같습니다.

snmp 모드에서 N 멤버 스위치에 액세스하려면 snmp 응용 프로그램에서 스위치의 주소로 대상 IP 주소를 지정하십시오.

community string 로 community string + @esN, 명령 스위치에 해당 오른쪽에 속하고. 만약 명령 스위치에 커뮤니티 스트링이면 6번째 스위치의 커뮤니티 스트링은 **public@es6** 이다**.**

28.1.3.6 Web을 사용하여 클러스터 관리

클러스터가 생성 된 후 명령 스위치를 통해 구성원 스위치와 브라우저 간에 http 메시지가 전송 될 수 있습니다. 자세한 작업은 url 앞에 "esN /"과 같은 접두사를 추가하는 것입니다.

명령 스위치의 IP가 192.168.20.1이라고 가정하면, No.6 구성원 스위치의 URL은 http://192.168.20.1/es6/입니다.

29장 Fast Ethernet Ring 구성과 보호법

29.1.1 개요

AAA 이더넷 링 보호 프로토콜은 링크 계층에 적용되는 특수 프로토콜입니다.
이더넷의 링 토폴로지를 위해 특별히 설계되었습니다. 이더넷 보호 프로토콜은
완전한 링 토폴로지에서 하나의 링크를 차단하여 루프를 방지 할 수 있습니다

Broadcast Storm을 형성하는 것에서. 링크가 끊어진 경우 프로토콜은 이전에 종료된 링크를 즉시 다시 시작합니다. 이러한 방식으로, 링 네트워크들 사이의 노드들은 서로 통신 할 수 있다.

링 네트워크 보호 프로토콜과 신장 트리 프로토콜은 모두 링크 계층 토폴로지를 제어하는 데 사용됩니다. 신장 트리 프로토콜은 여러 개의 복잡한 네트워크에서 사용되며 네트워크 토폴로지가 hop-to-hop 방법을 통해 변경되면 전송합니다. 링 네트워크 보호 프로토콜은 링 토폴로지에서 사용되며 링 토폴로지의 변경을 확산 방법을 통해 전송합니다. 그러므로 링 네트워크에서 링 네트워크 보호 프로토콜의 수렴은 신장 트리 프로토콜보다 훨씬 낫습니다. 양호한 네트워크 조건에서 링 네트워크 보호 프로토콜은 50ms 이내에 네트워크 통신을 재개 할 수 있습니다.

노트:

링-네트워크 보호 프로토콜(RNPP)은 하나의 스위치를 여러가지 물리적인 링 네트워크에 대한 노드로 구성이 가능합니다. 따라서 보다 복잡한 토폴로지를 설정할 수 있습니다.

29.1.2 이더넷 링에 관하여 관련 개념

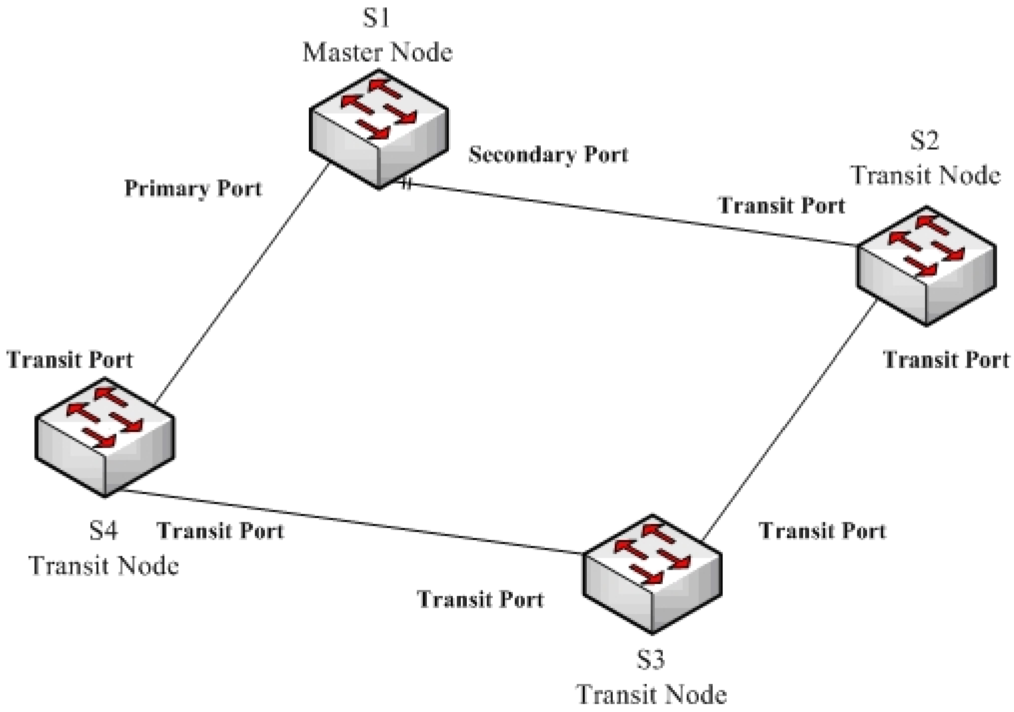


그림 1.1 이더넷 링

29.1.2.1 링-네트워크 노드의 역할

이더넷 링의 각 스위치는 이더넷 링의 노드입니다. 링 - 네트워크 노드는 마스터 노드와 중계 노드로 분류 할 수 있다. 링 네트워크의 스위치 하나가 마스터 노드로 사용되고 다른 스위치는 중계 노드로 사용됩니다.

마스터 노드: 토폴로지를 업데이트 할 때 링 토폴로지가 완료되었는지 확인하고 루프를 제거하고 다른 스위치를 제어합니다.

중계 노드: 링 네트워크의 로컬 포트 상태를 감지하고 링크가 무효화되면 마스터 노드에 알립니다.

각 노드의 역할은 사용자가 지정합니다. 각 스위치는 하나의 역할로만 구성 할 수 있습니다. 그림 1.1에서 스위치 S1은 링 네트워크의 마스터 노드입니다. 스위치 S2, S3 및 S4는 중계 노드입니다.

29.1.2.2 링 네트워크 포트의 역할

이더넷 링 보호 프로토콜은 각 스위치가 링 네트워크에 연결할 수 있는 2 개의 포

트를 요구합니다. 각 포트의 역할은 구성을 통해 지정해야 합니다.
프로토콜이 지원하는 포트 역할에는 다음 클래스가 포함됩니다.
기본 포트: 마스터 노드에서만 구성됩니다. 마스터 노드는 기본 포트를 통해 링 네트워크 탐지 메시지를 보냅니다.

보조 포트 : 마스터 노드에서만 구성됩니다. 마스터 노드는 링 - 망 탐지 메시지를 수신하고 링 토폴로지가 완료되었는지를 판단한다. 링 토폴로지가 완료되면 마스터 노드는 보조 포트에서 데이터 메시지를 차단합니다. 링 토폴로지에서 링크가 끊어진 경우 마스터 노드는 보조 포트를 사용하여 데이터 메시지를 전달할 수 있습니다.

중계 포트 : 중계 노드에서만 구성됩니다. 중계 노드의 두 포트는 전송 포트로 사용할 수 있습니다.

링 네트워크의 각 포트는 하나의 포트 역할로만 구성 할 수 있습니다. 포트 역할은 스위치의 노드 역할이 구성되고 VLAN이 제어 된 후에 구성 할 수 있습니다. 그림 1.1에서 볼 수 있듯이 마스터 노드 S1이 S4를 연결하는 포트는 기본 포트입니다. S1이 S2를 연결하는 포트는 보조 포트입니다. 다른 스위치가 링 네트워크를 연결하는 포트는 중계 포트입니다.

노트:

동일한 스위치를 다중 링으로 구성해야 하는 경우 스위치는 서로 다른 물리적 포트를 통해 서로 다른 링을 연결해야 합니다.

29.1.2.3 VLAN 제어와 데이터 VLAN

마스터 노드와 중계 노드는 사설 제어 VLAN을 통해 프로토콜 메시지를 교환합니다. 구성을 통해 제어 VLAN을 지정할 수 있습니다. 프로토콜 메시지를 정상적으로 수신하고 전송할 수 있도록 제어 네트워크에 링 네트워크의 포트를 추가합니다.
일반적으로 링 네트워크의 각 포트는 제어 VLAN에서 전달 상태에 있습니다. 비 링 포트는 데이터 VLAN 0에서 메시지를 전달할 수 없습니다.

노트:

링마다 다른 제어 VLAN을 지정해야 합니다. 제어 VLAN 링 - 네트워크 제어 메시지를 포워딩 하기 위해서만 사용된다. 제어 VLAN은 사용할 수 없습니다.

2계층 또는 3계층 통신에 사용됩니다. 예를 들어, 제어 VLAN의 VLAN 인터페이스가 생성 된 후에는 다른 장치를 통해 인터페이스의 IP에 ping이 불가능합니다.

제어 VLAN을 제외한 VLAN은 데이터 VLAN입니다. 데이터 VLAN은 공통 서비스 메시지 또는 스위치 관리 메시지를 전달하는 데 사용됩니다. 이더넷 링 보호 프로토콜은 링 네트워크 포트가 데이터 VLAN에서 메시지를 전달할 수 있는지 여부를 결정할 수 있습니다.

모든 non-Ring 네트워크 포트는 데이터 VLAN에서 메시지를 전달합니다.

노트:

데이터 VLAN은 레이어 2 또는 레이어 3 통신에 사용할 수 있습니다.
예를 들어 데이터 VLAN의 해당 VLAN 인터페이스를 생성하고 동적 라우팅 프로토콜을 구성 할 수 있습니다.

29.1.2.4 MAC 주소 테이블 에이징

이더넷 링 보호 프로토콜은 스위치의 MAC 주소 테이블을 제어하여 토폴로지가 변경된 후 데이터 메시지가 올바른 링크로 전송 될 수 있도록 합니다. 일반적으로 MAC 주소는 300 초 후에 MAC 주소 테이블에서 시간이 경과하기 시작합니다. 이더넷 링 보호 프로토콜은 스위치의 MAC 주소가 가장 짧은 시간 내에 오래도록 제어할 수 있습니다.

29.1.2.5 링-네트워크의 완성 상태

마스터 노드와 중계 노드는 COMPLETE 로고를 통해 현재 링 네트워크가 완전한 상태인지 여부를 표시 할 수 있습니다. 마스터 노드와 관련하여 현재 링 네트워크의 모든 링크가 정상 상태에 있고 기본 포트가 전달 상태에 있고 보조 포트가 정체 상태에 있는 경우 COMPLETE 로고가 true입니다. 중계 노드와 관련하여 보조 노드의 두 개의 중계 포트가 전달 상태 일 때만 COMPLETE 로고가 참일 수 있습니다. 링 네트워크 상태 로고는 현재 네트워크 인 경우 토폴로지 상태를 판단하는데 도움이 됩니다.

29.1.3 이더넷 링 보호 프로토콜에 사용되는 메시지 유형

이더넷 링 보호 프로토콜에 사용되는 메시지 유형은 표 1.1에 나와 있습니다.

표1.1 이더넷 링 보호 프로토콜의 메시지 유형

메시지 형태	설명
Loop detection (HEALTH)	링 노드 토폴로지가 완료되었는지를 검출하기 위해 마스터 노드에 의해 전송됩니다.
Link interruption (LINK-DOWN)	중계 노드가 링 네트워크에서 링크 고장이 발생했음을 나타내기 위해 중계 노드에서 전송됩니다.
Aging address table for ring network breakdown (RING-DOWN-FLUSH-FDB)	중계 노드의 에이징 MAC 주소 테이블을 나타내는 링 네트워크의 고장이 감지 된 후 마스터 노드가 전송합니다.
Aging address table for ring network restoration (RING-UP-FLUSH-FDB)	중계 노드의 에이징 MAC 주소 테이블을 나타내는 링 네트워크 복원 후 마스터 노드가 전송합니다.

29.1.4 이더넷 링의 보호법

29.1.4.1 마스터 노드에 대한 루프 탐지 및 제어

마스터 노드는 구성 기간에 기본 포트를 통해 제어 VLAN에 HEALTH 메시지를 전송합니다. 통상적으로, HEALTH 메시지는 링 네트워크 내의 다른 모든 노드들을 통과 한 후에 마스터 노드의 제 2 포트로 전송 될 수 있습니다.

보조 포트는 기본적으로 모든 데이터 VLAN을 차단합니다. HEALTH 메시지가 지속적으로 수신되는 경우 보조 포트는 루프를 피하기 위해 데이터 VLAN을 차단합니다. 보조 포트가 구성된 시간 제한 후 1 차 포트에서 HEALTH 메시지를 받지 못하면 링 네트워크는 유효하지 않은 것으로 간주됩니다. 그런 다음 마스터 노드는 보조 포트를 사용하여 데이터 VLAN을 차단하지 않고 로컬 MAC 주소 테이블을 사용하고 RING-DOWN-FLUSH-FDB 메시지를 전송하여 다른 노드에 알립니다.

마스터 노드가 데이터 VLAN에 열린 보조 포트를 통해 HEALTH 메시지를 수신하면 링 네트워크가 복원됩니다. 이 경우 마스터 노드는 보조 포트를 통해 데이터 VLAN을 차단하고 로컬 토폴로지를 업데이트하고 RING-UP-FLUSH-FDB 메시지를 통해 다른 노드에 에이징 주소 테이블을 알립니다.

hello-time 노드와 fail-time 노드에서 명령을 구성하여 HEALTH 메시지를 보내는 기본 포트의 간격과 HEALTH 메시지를 기다리는 보조 포트의 시간 제한을 수정할 수 있습니다.

29.1.4.2 중계 노드의 링크 다운 메시지

중계 노드에 대한 중계 포트의 링크가 무효가 된 후에 중계 노드는 다른 중계 포트를 통해 링크 다운 메시지를 보냅니다. LINK-DOWN 메시지는 다른 중계 노드를 통과 한 후 마스터 노드의 포트로 전송됩니다.

마스터 노드가 LINK-DOWN 메시지를 수신하면 링 네트워크는 유효하지 않은 것으로 간주됩니다. 그런 다음 마스터 노드는 보조 포트를 사용하여 데이터 VLAN을 차단하지 않고 로컬 MAC 주소 테이블을 오래 사용하고 RING-DOWN-FLUSH-FDB 메시지를 전송하여 다른 노드에 알립니다.

29.1.4.3 중계 노드의 링크 복원

중계 포트가 복원 된 후에는 전달 전 상태가 됩니다. 중계 포트는 제어 포트가 사전 전달 중일 때 제어 메시지를 전달 및 수신합니다.

링 네트워크에서 하나의 중계 포트만이 유효하지 않으면 마스터 노드의 2차 포트는 1 차 포트에서 다시 HEALTH 메시지를 수신 할 수 있습니다. 이 경우 마스터 노드는 보조 포트에서 데이터 VLAN을 다시 차단하고 MAC 주소 테이블 aging에 대한 알림을 다른 노드로 보냅니다. 전송 포트가 사전 전달 상태에 있는 노드는 전송 포트를 전달 상태로 변경하고 로컬 MAC 주소 테이블을

aging합니다. 중계 노드가 구성 가능한 시간 제한 후 마스터 노드에서 주소 aging 알림을 받지 못하면 중계 노드와 마스터 노드 사이의 연결이 끊어진 것으로 간주됩니다. 이 경우 대중 교통 노드가 자동으로 변경됩니다.

포트 상태를 포워딩 전 상태에서 포워딩 상태로 변경합니다.

전송 포트의 시간 제한을 수정하여 사전 전달 상태를 유지할 수 있습니다

사전 전달 시간 노드에서 명령을 구성합니다.

29.2.1 Fast Ethernet-Ring 의 기본 구성

노트:

고속 이더넷 링 보호 프로토콜과 신장 트리 프로토콜은 함께 구성 할 수 없습니다. 신장 트리 프로토콜이 활성화되면 링 노드의 BPDU 전달로 인한 공격을 피하기 위해 신장 트리 bpdu-terminal 기능을 구성하는 것이 좋습니다.

표2.1은 ERP 와 STP의 기본 구성을 보여줍니다..

표 2.1 고속 이더넷 링 보호 프로토콜 및 신장 트리 프로토콜의 기본 설정

Spanning-tree protocol (STP)	**신장-트리 모드를 설정합니다**
fast Ethernet-ring protection protocol	구성 없음

29.2.2 Fast Ethernet-Ring 프로토콜 구성에 대한 참고 사항

이더넷 링 보호 프로토콜을 구성하기 전에 다음 항목을 주의 깊게 읽으십시오.

- Broadcast storm 방지는 이더넷 링 프로토콜의 중요한 기능입니다. 링 링크를 연결하기 전에 모든 링 노드가 구성되어 있는지 확인하십시오. 예를 들어 마스터 노드와 모든 중계 노드가 구성된 후에는 마스터 노드의 보조 포트에 대한 네트워크 케이블을 연결하십시오. 모든 노드가 구성되기 전에 네트워크 케이블을 연결하면 Broadcast storm이 쉽게 발생합니다.

- 이더넷 링 보호 프로토콜을 구성하기 전에 스위치의 신장 트리 프로토콜을 비활성화 하십시오. no spanning-tree 명령을 실행 한 후 모든 링 노드의 BPDU 전달로 인한 영향을 피하려면 신장 트리 bpdu-teminal 기능을 구성하십시오..

- 링 네트워크 노드 인스턴스가 구성된 후에는 모든 링 네트워크 노드의 구성을 삭제하지 않으면 STP 프로토콜을 활성화 할 수 없습니다.

- 이더넷 링 보호 프로토콜은 스위치의 여러 링 네트워크 노드 인스턴스를 지원합니다.

- 해당 시스템 VLAN은 링 네트워크 제어 VLAN이 구성된 후에 자동으로 설정 될 수 없습니다. 전역 VLAN 구성 명령을 실행하여 수동으로 VLAN을 설정해야 합니다.

- 링 네트워크 포트만 링의 제어 VLAN에서 메시지를 전달할 수 있습니다. 다른 포트는 트렁크 모드로 구성되어 있어도 이 작업을 수행 할 수 없습니다.

- 기본적으로 마스터 노드의 Fail-Time은 마스터 노드의 Hello 시간의 3 배입니다. 따라서 메시지 지연으로 인한 이더넷 링 보호 프로토콜의 충격을 피할 수 있습니다. Hello 시간을 수정 한 후에도 Fail-time을 수정해야합니다.

- 본적으로 전송 노드의 미리 전달 시간은 마스터 노드의 Hello 시간의 3 배입니다. 기본 설정은 전송 포트가 전달 상태가 되기 전에 마스터 노드가 링 네트워크 복구를 감지 할 수 있도록 합니다. 마스터 노드에 구성된 hello-time이 중계 노드의 Pre-Forward-Time보다 큰 경우 Broadcast storm 링에서 쉽게 발생할 수 있습니다.

- distributed-mode 및 centralized-mode 명령을 실행하여 이더넷 링 보호 프로토콜의 작동 모드를 수정할 수 있습니다.

- Interface FastEthernet 및 Interface GigaEthernet과 같은 물리적 포트만 링 네트워크의 포트로 구성 할 수 있습니다. 요약 포트는 링 네트워크 포트로 구성 할 수 없습니다. 링크 수렴, 802.1X 또는 포트 보안이 실제 포트에 이미 구성된 경우 포트를 링 네트워크 포트로 구성 할 수 없습니다.

29.2.3 Fast Ethernet-Ring 구성 작업

- 마스터 노드 구성
- 중계 노드 구성
- 링 네트워크 포트 구성
- 링 네트워크 보호 프로토콜의 상태 확인

29.2.4 Fast Ethernet-Ring 보호 구성

29.2.4.1 마스터 노드 구성하기

다음 명령을 실행하여 스위치를 링 네트워크의 마스터 노드로 구성하십시오.

명령어	설명
Switch#**configure**	스위치 구성 모드로 들어갑니다
Switch_config#**no spanning-tree**	현재 STP 프로토콜을 비활성화 합니다
Switch_config#**spanning-tree bpdu-terminal**	스위치가 BPDU의 전달을 금지합니다.
Switch_config#**ether-ring** *id* *ID=인스턴스번호	노드 인스턴스를 구성하고 시작합니다
Switch_config_ring#**control-vlan** *vlan-id*	제어 vlan을 구성합니다.
Switch_config_ring#**master-node**	마스터 형태의 노드를 만듭니다.

Switch_config_ring#**hello-time** *value*	마스터 노드가 탐지 메시지를 전송하는 기간을 구성합니다. 이는 선택 사항입니다. 값 : 1-10 초이며,기본값 : 1s
Switch_config_ring#**fail-time** *value*	선택 사항 인 검색 메시지를 기다리는 보조 포트의 시간 제한을 구성합니다. 값 : 3-30 초이며 기본값 : 3s
Switch_config_ring#**distributed-mode**	이더넷 링 보호 프로토콜 (옵션).
Switch_config_ring#**centralized-mode**	중앙 집중식 이더넷 링 보호 프로토콜 (옵션).
Switch_config_ring#**exit**	구성을 저장하고 구성 모드를 종료합니다.
Switch_config#**vlan** *vlan-id*	해당 제어 VLAN을 설정합니다.

노트:

링 네트워크 및 포트의 구성을 삭제하려면 no ether-ring id 명령을 실행해야 합니다.

29.2.4.2 중계 노드 구성하기

다음 명령을 실행하여 스위치를 링 네트워크의 중계 노드로 구성하십시오.

명령어	설명
Switch#**configure**	스위치 구성 모드로 들어갑니다.
Switch_config#**no spanning-tree**	STP를 비활성화 합니다.
Switch_config#**spanning-tree bpdu-terminal**	STP가 BPDU를 전달하는 것을 금지합니다..
Switch_config#**ether-ring** *id*	노드 인스턴스를 구성하고 노드 구성 모드를 시작합니다. id : 노드의 인스턴스 번호
Switch_config_ring#**control-vlan** *vlan-id*	제어 VLAN을 구성합니다. vlan-id : 제어 VLAN 번호
Switch_config_ring#**transit-node**	전송할 노드 유형을 설정합니다
Switch_config_ring#**pre-forward-time** *value*	전송 포트의 사전 전달 시간을 구성합니다. 작업은 선택 사항입니다. 값 : 3-30 초 기본 3초
Switch_config_ring#**exit**	현재 구성을 저장하고 구성 모드를 종료합니다.
Switch_config#**vlan** *vlan-id*	해당 제어 VLAN을 설정합니다.

29.2.4.3 링 네트워크 포트 구성

다음을 실행하여 스위치의 포트를 링네트워크 포트로 구성하십시오.

명령어	제안
Switch#**configure**	스위치 구성 모드로 들어갑니다
Switch_config#**interface** *intf-name*	포트 구성 모드로 들억압니다. intf-name: 포트이름
Switch_config_intf#**ether-ring** *id* **primary-port** **{ secondary-port | transit-port }**	링 네트워크 포트의 유형을 구성합니다. Id : 링 네트워크 노드의 인스턴스 번호
Switch_config_intf**#exit**	포트 구성 모드를 종료합니다.

노트 :

no ether-ring id 명령을 실행하십시오. primary-port {secondary-port | transit-port}를 사용하여 링 네트워크 포트의 구성을 삭제합니다.

29.2.4.4 링 네트워크 보호 프로토콜의 상태 확인

다음 명령을 실행하여 링 네트워크 보호 프로토콜의 상태를 확인하십시오.

명령어	설명
show ether-ring *id*	링 네트워크 보호 프로토콜 및 링 네트워크 포트에 대한 추출 정보를 확인합니다. Id : 링 네트워크의 인스턴스 번호
show ether-ring *id* **detail**	링 네트워크 보호 프로토콜 및 링 네트워크 포트에 대한 자세한 정보를 확인합니다.
show ether-ring *id* **interface** *intf-name*	링 네트워크 포트 및 공용 포트에 대한 상태 정보를 확인합니다.

29.2.5 Fast Ethernet Ring Protocol의 예

29.2.5.1 예제

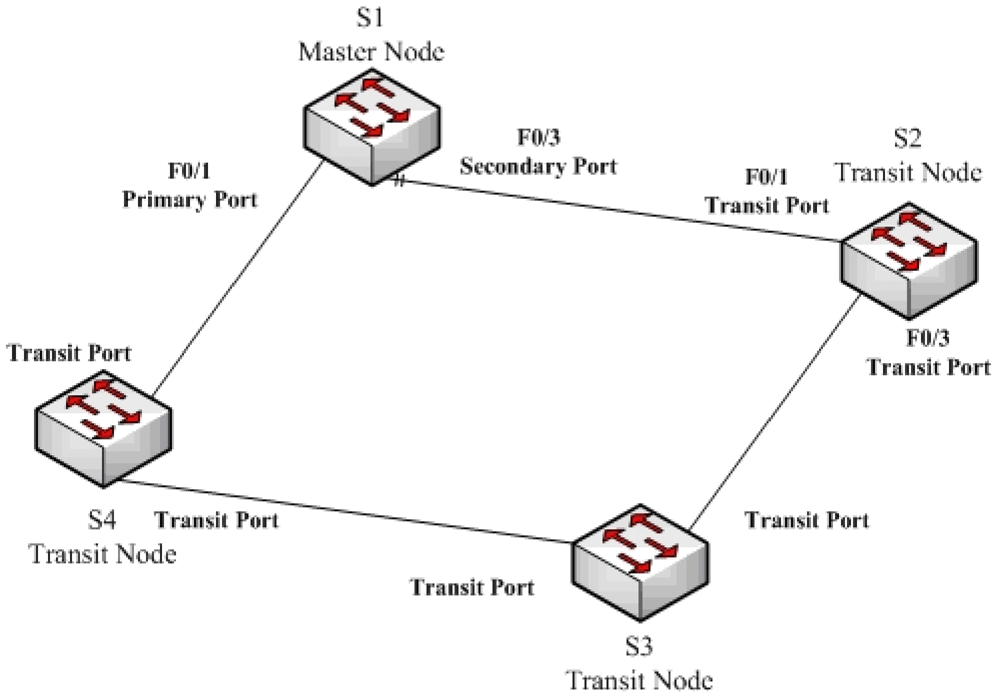


그림 2.1 fast-ethernet ring protection 예제

2.1에 도시 된 바와 같이, 마스터 노드 (S1)와 중계 노드 (S2)는 다음과 같이 구성된다. 다른 노드는 S2와 동일하게 구성됩니다.

스위치 S1 구성하기:

STP 프로토콜을 비활성화하고 링 네트워크 노드를 구성합니

다. S1_config#no spanning-tree

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

S1_config_ring1#master-node

< 시간 매개 변수 구성>

S1_config_ring1#hello-time 2

S1_config_ring1#fail-time 6

<노드 구성모드를 종료합니다>

S1_config_ring1#exit

<기본 포트 및 보조 포트 구성:>

S1_config#interface fastEthernet 0/1

S1_config_f0/1#ether-ring 1 primary-port

S1_config_f0/1#exit

S1_config#interface fastEthernet 0/3

S1_config_f0/3#ether-ring 1 secondary-port

S1_config_f0/3#exit

VLAN 컨트롤 설정:

S1_config#vlan 2

S1_config_vlan2#exit

S1_config#interface range f0/1 , 3

S1_config_if_range#switchport mode trunk

S1_config_if_range#exit

스위치 S2 구성하기:

S2_config#no spanning-tree

S2_config#ether-ring 1

S2_config_ring1#control-vlan 2

S2_config_ring1#transit-node

S2_config_ring1#pre-forward-time 8

S2_config_ring1#exit

S2_config#interface fastEthernet 0/1

S2_config_f0/1#ether-ring 1 transit-port

S2_config_f0/1#exit

S2_config#interface fastEthernet 0/3

S2_config_f0/3#ether-ring 1 transit-port

S2_config_f0/3#exit

S2_config#vlan 2

S2_config_vlan2#exit

S2_config#interface range fastEthernet 0/1- 3

S2_config_if_range#switchport mode trunk

S2_config_if_range#exit

30 장. DHCP-Snooping 구성

30.1.1 IGMP-Snooping 구성 작업

DHCP-Snooping은 DHCP 패킷을 판단하여 가짜의 DHCP 서비스를 예방하여 MAC 주소와 IP 주소 간의 바인딩 관계를 유지합니다. L2 스위치는 MAC 주소와 IP 주소 간의 바인딩 관계에 따라 DAI 기능과 소스 IP 보호 기능을 수행 할 수 있습니다. DHCP-Snooping은 주로 DHCP 패킷을 모니터링하고 MAC-IP 바인딩 목록을 동적으로 유지 관리합니다. L2 스위치는 MAC-IP 바인딩 관계를 충족시키지 않는 패킷을 필터링하여 공격적인 사용자의 네트워크 공격을 방지합니다.

30.1.1.1 DHCP-Snooping의 활성화와 비활성화

전역 구성 모드에서 다음과 같은 명령어를 사용해보시오

명령어	설명
ip dhcp-relay snooping	DHCP-snooping을 활성화합니다.
no ip dhcp-relay snooping	기본값으로 되돌립니다.

이 명령은 전역 구성 모드에서 DHCP-snooping을 활성화하는 데 사용됩니다.
이 명령을 실행하면 스위치가 모든 DHCP 패킷을 모니터링하고 해당 바인딩 관계를 형성합니다.

30.1.1.2 Vlan에서의 DHCP-snooping 활성화

VLAN에서 DHCP-snooping이 활성화 된 경우 우 VLAN에서 제거된 모든 물리적 포트로부터 수신된 DHCP 패킷이 합법적으로 검사됩니다. VLAN의 신뢰할 수 없는 물리적 포트에서 수신 된 DHCP 응답 패킷은 삭제되어 가짜 또는 잘못 구성된 DHCP 서버가 주소 분배 서비스를 제공하지 못하게 합니다. 신뢰할 수 없는 포트의 DHCP-패킷을 요청한 경우
DHCP 요청 패킷의 하드웨어 주소 필드가이 패킷의 MAC 주소와 일치하지 않으면 DHCP 패킷은 DHCP DOS의 공격 패킷으로 사용되는 가짜 패킷으로 간주되어 스위치에서 삭제합니다. 스위치는 DHCP DOS의 공격 패킷을 삭제 할 것입니다.

전역 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip dhcp-relay snooping vlan *vlan_id*	Vlan에서 DHCP-snooping 활성화합니다.
no ip dhcp-snooping vlan *vlan_id*	Vlan에서 DHCP-snooping 비활성화합니다.

30.1.1.3 Vlan에서의 DHCP Clients 최대치 활성화하기

VLAN에서 방어를 활성화하려면 특정 VLAN에 허용되는 최대 DHCP 클라이언트를 구성하고 "선착순" 원칙을 수행해야 합니다. 특정 VLAN의 사용자 수가 최대 값에 도달하면 추가 클라이언트를 배포 할 수 없습니다.

전역 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip dhcp-relay snooping vlan *vlan_ied* **max-client** *number*	Vlan에 DHCP 공격방어를 활성화합니다..
no ip dhcp-snooping vlan *vlan_id* **max-client***r*	Vlan에 DHCP 공격방어를 비활성화합니다..

30.1.1.4 신뢰하는 DHCP 인터페이스를 인터페이스에 설정하기

인터페이스가 신뢰하는 DHCP 인터페이스로 설정된 경우 이 인터페이스에서 수신 한 DHCP 패킷은 확인되지 않습니다. 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
dhcp snooping trust	신뢰하는 인터페이스를 활성화합니다.
no dhcp snooping trust	신뢰하는 인터페이스를 비활성화합니다

기본값은 비활성화로 설정되어 있습니다.

30.1.1.5 바인딩 테이블의 빠른 업데이트 기능 활성화 또는 비활성화

이 기능은 기본적으로 비활성화되어 있습니다. 이 기능이 비활성화되고 포트가 클라이언트 A에 묶인 경우 클라이언트 A가 오프라인 인 경우에도 다른 포트의 동일한 MAC 주소에 대한 DHCP 요청은 가짜 MAC 공격으로 간주됩니다.
이 기능을 사용하면 위의 경우는 발생하지 않습니다.

클라이언트가 DHCP 서버에 의해 배포 된 포트 및 주소 임대를 자주 변경하고 단기간에 수정할 수 없는 경우 이 기능을 사용하는 것이 좋습니다.

명령어	설명
ip dhcp-relay snooping rapid-refresh-bind	바인딩 테이블의 빠른 업데이트 기능을 사용합니다.
no ip dhcp-relay snooping rapid-refresh-bind	바인딩 테이블의 빠른 업데이트 기능을 비활성화합니다.

VLAN

동적 ARP 모니터링이 VLAN의 모든 물리적 포트에서 수행 되면 이 패킷의 소스 MAC 주소와 소스 IP 주소가 구성된 MAC-IP 바인딩 관계와 일치하지 않으면 수신된 ARP 패킷이 거부됩니다. 인터페이스의 바인딩 관계는 DHCP에 의해 동적으로 바인딩 되거나 수동으로 구성 될 수 있습니다. 물리적 인터페이스의 IP 주소에 MAC 주소가 바인딩 되어 있지 않으면 스위치는 모든 ARP 패킷을 전달하지 않습니다.

명령어	설명
ip arp inspection vlan *vlanid*	VLAN의 모든 포트에서 동적 ARP 모니터링을 활성화합니다.
no ip arp inspection vlan *vlanid*	VLAN의 모든 포트에서 동적 ARP 모니터링을 비활성화합니다.

30.1.1.7 신뢰하는 ARP 인터페이스에 대한 인터페이스 설정

인터페이스는 기본적으로 신뢰할 수 없어 ARP 모니터링을 사용할 수 없습니다
인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
arp inspection trust	신뢰하는 ARP 인터페이스에 대한 인터페이스를 설정합니다.
no arp inspection trust	ARP 비신뢰 인터페이스에 대한 인터페이스를 다시 시작합니다.

30.1.1.8 VLAN에서 소스 IP 주소 모니터링 활성화

VLAN에서 소스 IP 주소 모니터링이 활성화 된 후에는 소스 MAC주소와 IP주소가 구성된 MAC-IP 바인딩 관계와 일치하지 않으면 VLAN의 모든 포트에서 수신 IP 패킷이 거부됩니다. 바인딩 관계는 DHCP에 의해 동적 바인딩 되거나 수동으로 구성 될 수 있습니다. 만약 바인딩 되어있지 않으면 스위치는 물리적 인터페이스에서 수신한 모든 IP패킷을 전달하지 않습니다. 다음은 전역모드에 활성화한 명령어입니다.

명령어	설명
ip verify source vlan *vlanid*	VLAN의 비 신뢰 인터페이스에서 소스 IP 주소 검사를 활성화합니다.
no ip verify source vlan *vlanid*	VLAN의 비 신뢰 인터페이스에서 소스 IP 주소 검사를 비활성화합니다.

노트: DHCP패킷(IP패킷도 포함)이 수신된 경우 Snooping이 구성되어 있기 때문에 전달됩니다.

30.1.1.9 VLAN변환 사용(이 기능을 지원하는 장비가 필요함)

VLAN 변환이 활성화 된 VLAN에서 이 VLAN의 모든 물리적 포트 패킷 으로 N 대 1 VLAN 변환이 수행됩니다. 즉, 여러 VLAN을 하나의 VLAN으로 변환 할 수 있습니다. 전역 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip vlan-translate vlan *vlanid*	Vlan의 모든 인터페이스에서 Vlan 변환을 활성화합니다.
no ip vlan-translate vlan *vlanid*	Vlan의 모든 인터페이스에서 Vlan 변환을 비활성화합니다.

노트: 여기서 vlanid는 변환 된 VLAN입니다. VLAN 변환은 전역 DHCP Snooping을 통해 활성화 해야 하며 QinQ 관련 명령을 사용하려면 유효성 검사가 필요합니다..

30.1.1.10 IP 소스 주소 모니터링이 신뢰할 수 있는 인터페이스 설정

인터페이스에 신뢰할 수 있는 원본 IP 주소가 있으면 원본 주소 검사가 인터페이스에서 활성화되어 있지 않습니다.

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip-source trust	신뢰 하는 소스 IP 주소가 있는 인터페이스를 설정합니다.
no ip-source trust	신뢰하지 않는 소스 IP 주소가 있는 인터페이스를 리셋합니다.

30.1.1.11 Vlan 변환을 금지하도록 인터페이스를 지원 (Vlan 변환 지원)

VLAN 변환이 금지 된 인터페이스에서 VLAN 변환을 비활성화합니다.
인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
vlan-translate deny	인터페이스를 VLAN 변환을 금지하는 것으로 설정합니다.
no vlan-translate deny	인터페이스가 VLAN 변환을 금지하지 않도록 설정합니다 (이 인터페이스가 VLAN 변환 활성화 VLAN에 속하면 이 경우 VLAN 변환이 정상적으로 작동 함).

30.1.1.12 DHCP-Snooping 옵션82번 설정하기

옵션 82는 로컬 정보를 서버에 가져오고 서버가 클라이언트에게 주소를 분배하는 데 도움을 줍니다.

전역 구성 모드에서 다음 명령을 실행하십시오..

명령어	설명
ip dhcp-relay snooping information option	기본 형식 인 option82를 다음과 같이 설정합니다. DHCP-Snooping은 DHCP 패킷을 전달합니다.
no ip dhcp-relay snooping information option	DHCP-snooping이 DHCP 패킷을 전달할 때 option82가 전달되지 않도록 설정합니다.

option82의 형식을 지정하려면 전역 모드에서 다음 설정을 수행하십시오.

명령어	설명
ip dhcp-relay snooping information option format snmp-ifindex/manual/hn-type	DHCP-Snooping에 의해 전달 될 때 DHCP 패킷이 전송하는 option82의 형식을 설정합니다.
no ip dhcp-relay snooping information option format snmp-ifindex/manual/hn-type	DHCP-snooping이 DHCP 패킷을 전달할 때 option82가 전달되지 않도록 설정합니다.

옵션 82에서 수동 모드를 입력하도록 설정 한 경우 인터페이스 모드에서 다음 구성을 수행하여 회로 ID를 설정합니다:

명령어	설명
dhcp snooping information circuit-id string [STRING]	option82를 수동 형식으로 설정 한 경우, 옵션 82가있는 DHCP 패킷을 전달하도록 DHCP-Snooping을 설정해야 합니다. 옵션의 내용은 STRING**형식으로** 작성한 문자열입니다. 이 명령은 클라이언트를 연결하는 포트에 설정됩니다.
dhcp snooping information circuit-id **hex [***xx-xx-xx-xx-xx-xx***]**	option82가 수동 형식으로 설정되어있는 경우 내용이 16 진수 시스템 인 옵션 82의 방향으로 DHCP 패킷을 전달하도록 DHCP 스누핑을 설정해야 합니다.이 명령은 클라이언트를 연결하는 포트에 설정됩니다.
no dhcp snooping information circuit-id	수동으로 구성된 option82 circuit-id를 삭제합니다.

옵션 82에서 수동 모드를 입력하도록 설정 한 경우 인터페이스 모드에서 다음 구성을 수행하여 remote-id를 설정하십시오:

dhcp snooping information append first-subop9-param hex [*xx-xx-xx-xx-xx-xx*]	option82 vendor-specific (하위 옵션 9)에 의해 수행 된 첫 번째 매개 변수의 Hex 시스템을 나타냅니다.
dhcp snooping information append second-subop9-param hex [*xx-xx-xx-xx-xx-xx*]	option82 vendor-specific (하위 옵션 9)에 의해 운반되는 두 번째 매개 변수의 Hex 시스템을 나타냅니다.

30.1.1.13 DHCP-snooping Option82 패킷의 정책 설정

이러한 패킷을 수신 한 후 option82와 함께 전달되는 DHCP 요청 패킷에 대한 정책을 설정할 수 있습니다. 정책에는 다음과 같은 정책이 포함됩니다.

"Drop"정책: 포트 모드에서 다음 명령을 실행하여 option82를 사용하여 요청 패킷을 삭제하십시오.

명령어	설명
dhcp snooping information drop	option82가 포함 된 요청 패킷을 삭제합니다.

option82 포함 된 요청 패킷을 삭제하십시오.

30.1.1.14 인터페이스 바인딩을 백업하기 위한 TFTP 서버 구성

스위치 구성을 다시 부팅하면 이전에 구성된 인터페이스 바인딩이 손실됩니다.
인터페이스에는 바인딩 관계가 없습니다. 소스 IP 주소 모니터링이 활성화 후 스위치는 모든 IP 패킷을 전달하는 것을 거부했습니다. TFTP 서버가 인터페이스 바인딩 백업용으로 구성된 후에는 바인딩 관계가 TFTP 프로토콜을 통해 서버에 백업됩니다. 스위치를 다시 시작하면 스위치가 자동으로 TFTP 서버에서 바인딩 목록을 다운로드 하여 정상적인 네트워크 실행을 보장합니다. 다음 명령을 실행하십시오..

명령어	설명
ip dhcp-relay snooping database-agent *ip-address*	인터페이스 바인딩을 백업 할 TFTP 서버의 IP 주소를 구성합니다.
no ip dhcp-relay snooping database-agent	인터페이스 바인딩을 백업하기 위해 TFTP 서버를 취소합니다.

30.1.1.15 인터페이스 바인딩 백업을 위한 파일 이름 구성

인터페이스 바인딩 관계를 백업 할 때 해당 파일 이름이 TFTP 서버에 저장됩니다. 이러한 방식으로 서로 다른 스위치가 동일한 TFTP 서버에 자신의 인터페이스 바인딩 관계를 백업 할 수 있습니다. 다음 명령을 실행하십시오.

명령어	설명
ip dhcp-relay snooping db-file *name*	인터페이스 바인딩 백업을 위한 파일 이름을 구성합니다
no ip dhcp-relay snooping db-file	인터페이스 바인딩 백업을 위한 파일 이름을 취소합니다.

30.1.1.16 인터페이스 바인딩 백업 확인을 위한 간격 구성

인터페이스의 MAC-IP 바인딩 관계는 동적으로 변경됩니다. 따라서 일정한 간격 후에 바인딩 관계가 업데이트되는지 확인해야 합니다. 바인딩 관계가 업데이트되면 다시 백업해야 합니다. 기본 간격은 30 분입니다. 다음 명령을 실행하십시오..

명령어	설명
ip dhcp-relay snooping write *num*	인터페이스 바인딩 백업 검사 간격을 구성합니다.
no ip dhcp-relay snooping write	인터페이스 바인딩 백업을 기본 설정으로 확인하는 간격을 다시 시작합니다.

30.1.1.17 수동으로 인터페이스 바인딩 구성

호스트가 DHCP를 통해 주소를 얻지 못하면 스위치의 인터페이스에 바인딩 항목을 추가하여 호스트가 네트워크에 접근 할 수 있습니다. 어떤 ip 소스도 실행할 수 없습니다.

MAC IP를 바인딩하여 해당 바인딩 목록에서 항목을 삭제합니다.

수동으로 구성된 바인딩 항목은 동적으로 구성된 바인딩 항목보다 우선 순위가 높습니다. 수동으로 구성된 바인딩 항목과 동적으로 구성된 바인딩 항목은 동일한 MAC 주소를 갖습니다. 수동으로 구성된 동적 업데이트는 동적으로 구성된 업데이트를 업데이트합니다. 인터페이스 바인딩 항목은 MAC 주소를 색인으로 사용합니다. 다음 명령을 실행하십시오.

명령어	설명
ip source binding *MAC IP* interface *name*	인터페이스 바인딩을 수동으로 구성합니다.
no ip source binding *MAC IP*	인터페이스 바인딩 항목을 취소합니다.

30.1.1.18 L2 스위치 전달 DHCP 패킷

다음 명령을 사용하여 DHCP 패킷을 지정된 DHCP 서버로 전달하여 DHCP 릴레이를 실현할 수 있습니다. 이 명령의 부정적인 형식은 DHCP 릴레이를 종료하는 데 사용될 수 있습니다.

Note: 명령은 L2 스위치에서 DHCP 릴레이를 활성화하는 데에만 사용합니다. 반면 L3 스위치, DHCP 릴레이는 DHCP 서버에 의해 실현됩니다.

전역 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip dhcp-relay agent	DHCP 릴레이를 사용합니다.
ip dhcp-relay helper-address *address* **vlan** *vlan-id*	릴레이의 대상 주소 및 VLAN을 구성합니다.

30.1.1.19 DHCP-Snooping 모니터링 및 유지 관리

EXEC 모드에서 다음 명령을 실행하십시오.

명령어	설명
show ip dhcp-relay snooping	DHCP-snooping 구성에 대한 정보를 표시합니다.
show ip dhcp-relay snooping binding	인터페이스에 유효한 주소 바인딩 항목을 표시합니다.
show ip dhcp-relay snooping binding all	DHCP-Snooping에 의해 생성 된 모든 바인딩 항목을 표시합니다.
[**no**] **debug ip dhcp-relay** [**snooping** | binding | **event** | all]	DHCP-relay-Snooping 바인딩 또는 이벤트의 전환을 활성화하거나 비활성화합니다.

다음은 DHCP 스누핑 구성에 대한 정보를 표시합니다..

switch#**show ip dhcp-relay snooping**

ip dhcp-relay snooping vlan 3

ip arp inspection vlan 3

DHCP Snooping trust interface:

FastEthernet0/1

ARP Inspect interface:

FastEthernet0/11

다음은 dhcp-relay snooping에 대한 바인딩 정보를 보여줍니다.

switch#**show ip dhcp-relay snooping binding**

Hardware Address	IP Address	remainder time	Type	VLAN	interface
00-e0-0f-26-23-89	192.2.2.101	86400	DHCP_SN	3	FastEthernet0/3

다음은 dhcp-relay snooping에 대한 바인딩 정보를 보여줍니다.

switch#**show ip dhcp-relay snooping binding all**

Hardware Address	IP Address	remainder time	Type	VLAN	interface
00-e0-0f-32-1c-59	192.2.2.1	infinite	MANUAL	1	FastEthernet0/2
00-e0-0f-26-23-89	192.2.2.101	86400	DHCP_SN	3	FastEthernet0/3

다음은 dhcp-relay snooping에 대한 정보입니다.

switch#**debug ip dhcp-relay all**

DHCPR: receive l2 packet from vlan 3, diID: 3

DHCPR: DHCP packet len 277

DHCPR: add binding on interface FastEthernet0/3

DHCPR: send packet continue

DHCPR: receive l2 packet from vlan 3, diID: 1

DHCPR: DHCP packet len 300

DHCPR: send packet continue

DHCPR: receive l2 packet from vlan 3, diID: 3

DHCPR: DHCP packet len 289

DHCPR: send packet continue

DHCPR: receive l2 packet from vlan 3, diID: 1

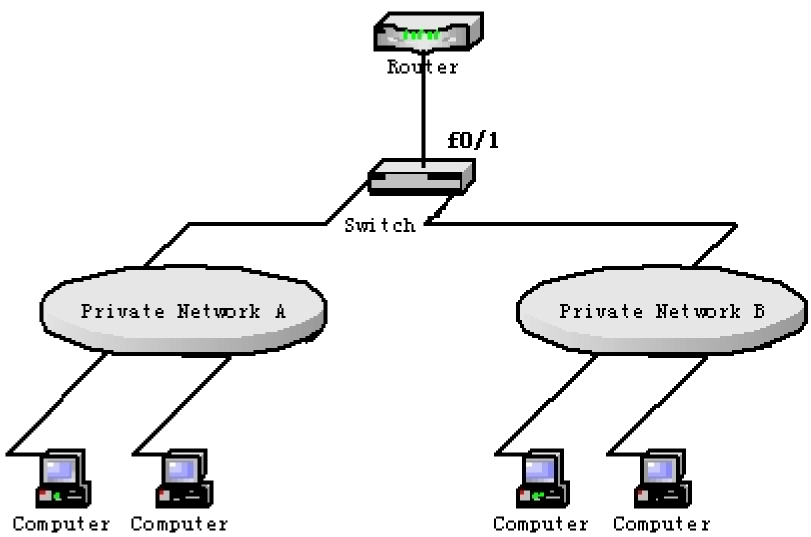
DHCPR: DHCP packet len 300

DHCPR: update binding on interface FastEthernet0/3

DHCPR: IP address: 192.2.2.101, lease time 86400 seconds

DHCPR: send packet continue

30.1.1.20 DHCP - Snooping구성의 예



다음 그림은 네트워크 구성도입니다.

1. 사설망 A를 연결하는 VLAN 1에서 DHCP-Snooping을 사용합니다.

   Switch_config#ip dhcp-relay snooping

   Switch_config#ip dhcp-relay snooping vlan 1

2. 사설망 B를 연결하는 VLAN 2에서 DHCP-Snooping을 활성화합니다.

   Switch_config#ip dhcp-relay snooping Switch_config#ip dhcp-relay snooping vlan 2

3. DHCP 서버를 DHCP- 신뢰 인터페이스에 연결하는 인터페이스를 설정합니다.

   Switch_config_f0/1#dhcp snooping trust

4. option82 인스턴스를 수동으로 설정합니다.

   interface GigaEthernet0/1

   dhcp snooping information circuit-id hex 00-01-00-05

   dhcp snooping information remote-id hex 00-e0-0f-13-1a-50

   dhcp snooping information vendor-specific hex 00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34

   dhcp snooping information append

```
  dhcp snooping information append first-subop9-param hex
61-62-63-61-62-63
interface GigaEthernet0/2
  dhcp snooping trust
  arp inspection trust
  ip-source trust
ip dhcp-relay snooping
ip dhcp-relay snooping vlan  1-100
ip arp inspection vlan  1
ip verify source vlan  1
ip dhcp-relay snooping information option format manual
```