

# User Manual

# 4MI-SG2400Series

---

4MI-SG2424TFM, 4MI-SG2406TFM, 4MI-SG2416TFM, 4MI-SG2448TFM, 4MI-SG2448TPFM

㈜포엠아이텍 경기도 수원시 영통구 신원로 296-21
현대테라타워영통패스트웍스 514-515호
www.4mitech.co.kr

# 목차


1. 개요 ..... 11

1.1. 운용환경 ..... 11

1.2. 운영체계 버전 ..... 12

1.3. 칩셋 및 SDK 정보 ..... 12

1.4. 접속 방법 ..... 12

2. 기본 명령어 설명 ..... 13

3. 구성 준비 ..... 14

3.1. 스위치 포트 번호 ..... 14

3.2. 시작 전 점검 사항 ..... 14

3.3. 도움말 ..... 15

3.4. 명령어 모드 ..... 15

3.5. 명령어 취소 ..... 16

3.6. 구성 저장 ..... 16

3.7. 기본구성 ..... 16

4. 계정 관리 ..... 17

4.1. 최초 로그인 ..... 17

4.2. 관리자 비밀번호 변경 ..... 17

4.3. 계정 비밀번호 규칙 구성 ..... 17

4.4. 비밀번호 규칙 생성하기 ..... 18

4.5. 로컬 계정에 비밀번호 규칙 적용하기 ..... 19

4.6. 운영모드 변경용 비밀번호에 규칙 적용하기 ..... 19

4.7. RADIUS 계정에 비밀번호 규칙 적용하기 ..... 20

4.8. TACACS 계정에 비밀번호 규칙 적용하기 ..... 20

5. 시스템 관리 구성 ..... 21

5.1. 파일 관리 구성 ..... 21

5.2. 기본 시스템 관리 구성 ..... 25

5.3. VTY 구성 안내 ..... 27

6. 네트워크 관리 구성 ..... 29

6.1. SNMP 구성 ..... 29

6.2. SNMP 구성 업무 ..... 31

6.3. RMON Configuration Commands ..... 60

7. MAC Access List 설정 명령 ..... 65

7.1. MAC Access List Configuration Commands ..... 65
8. SSH ..... 69
8.1. 개요 ..... 69
8.2. 구성 작업 ..... 69
8.3. SSH 동시 접속 세션 제한 ..... 71
8.4. SSH 서버 구성 예제 ..... 71
8.5. SSH 클라이언트 기능 사용 ..... 71
9. Telnet 구성 ..... 72
9.1. Telnet 서비스 구성 ..... 72
9.2. Telnet 서비스 인증 실패 대응 구성 ..... 72
9.3. Telnet 동시 접속 세션 제한 ..... 72
9.4. 관리자 접근 제어 ACL 적용 ..... 72
10. 인증(AAA) 구성 ..... 74
10.1. AAA 개요 ..... 74
10.5. AAA 구성 작업 목록 ..... 77
10.6. AAA 인증 구성 작업 ..... 77
11. RADIUS 구성 ..... 88
11.1. 개요 ..... 88
12. 인터페이스 ..... 94
12.1. 지원되는 인터페이스 유형 ..... 94
12.2. 인터페이스 구성 개요 ..... 95
13. 인터페이스 구성 ..... 97
13.1. 인터페이스 공통 속성 구성 ..... 97
13.3. 논리 인터페이스 구성 ..... 99
14. 인터페이스 구성 예 ..... 102
14.1. 공용 속성의 인터페이스 구성 ..... 102
14.2. 인터페이스 구성 명령 ..... 102
14.3. 설정 예제 ..... 108
15. 인터페이스 범위 구성 ..... 110
15.1. 인터페이스 범위 구성 ..... 110
16. 물리적인 인터페이스 특성 구성 ..... 111
16.1. 인터페이스 구성하기 ..... 111
17. 보안 포트 구성 ..... 113

18. 포트 미러링 구성하기 ..... 115
18.1. 포트 미러링 작업 목록 구성 ..... 115
18.2. 포트 미러링 구성 작업 ..... 115
18.3. 포트 미러링 구성 ..... 115
19. 802.1x 구성 ..... 116
19.1. 802.1x 구성 작업 목록 ..... 116
20. POE (Power Over Ethernet) 설정 명령 ..... 120
20.1. POE Configuration Commands ..... 120
21. VLAN 구성 ..... 138
21.1. VLAN 개요 ..... 138
22. Private VLAN ..... 143
22.1. Private VLAN Configuration Commands ..... 143
23. GVRP 설정 명령 ..... 151
23.1. GVRP Configuration Commands ..... 151
23.2. GARP Configuration Commands ..... 155
24. LACP ..... 162
24.1. 개요 ..... 162
24.2. 포트 집합 구성 작업 목록 ..... 162
25. LLDP (Link Layer Discovery Protocol) ..... 165
25.1. LLDP 개요 ..... 165
25.2. LLDP 구성 작업 목록 ..... 165
25.3. LLDP 구성 작업 ..... 165
26. PDP 설정 명령 ..... 169
26.1. PDP 설정 명령어 ..... 169
27. STP 설정 명령어 ..... 174
27.1. SSTP 설정 명령어 ..... 174
27.2. VLAN STP 설정 명령어 ..... 184
28. RSTP 설정 명령 ..... 193
28.1. RSTP 설정 명령어 ..... 193
29. MSTP 설정 명령 ..... 200
29.1. MSTP 설정 명령어 ..... 200
30. STP Optional Characteristic Configuration Commands ..... 220
30.1. STP Optional Characteristic Configuration Commands ..... 220

31. 이더넷 자동보호절체(EAPS) ..... 229
31.1. 개요 ..... 229
31.2. EAPS 개념 ..... 229
31.3. EAPS 패킷의 종류 ..... 231
31.4. 패스트 이더넷 링 보호 메커니즘 ..... 232
32. 이더넷 자동보호절체(EAPS) 구성 ..... 234
32.1. 기본 EAPS 구성 ..... 234
32.2. 구성 전 요구 사항 ..... 234
32.3. MEAPS 구성 작업 ..... 235
32.4. 고속 이더넷 링 보호 구성 ..... 235
32.5. MEAPS 구성 ..... 237
33. DHCP Snooping ..... 239
33.1. 개요 ..... 239
34. IGMP 설정 명령어 ..... 243
34.1. IGMP 설정 명령어 ..... 243
35. IGMP Snooping ..... 257
35.1. IGMP Snooping 구성 작업 ..... 257
36. PIM-DM 설정 명령어 ..... 264
36.1. PIM-DM 설정 명령어 ..... 264
37. PIM-SM 설정 명령 ..... 278
37.1. PIM-SM 설정 명령어 ..... 278
38. QoS 구성 ..... 341
38.1. QoS 개념 ..... 341
38.2. P2P QoS 모델 ..... 341
38.3. QoS 큐의 QoS 큐 알고리즘 ..... 342
39. QoS 구성 업무 ..... 343
39.1. QoS 작업 구성하기 ..... 343
39.2. QoS 구성 예제 ..... 348
40. DoS 공격 방지 구성 ..... 349
40.1. DoS 공격 개요 ..... 349
40.2. DoS 공격 방지 구성 작업 목록 ..... 350
40.3. DoS 공격 방지 구성 작업 ..... 350
40.4. DoS 공격 방지 구성 예 ..... 351

41. Anti-Attack 설정 명령 ..... 352
41.1. Anti-Attack 설정 명령어 ..... 352
42. Access List 구성하기 ..... 364
42.1. IP 메시지 필터링 ..... 364
42.2. 표준 및 확장 가능 IP 엑세스 목록 만들기 ..... 364
42.3. 인터페이스에 Access list 적용 ..... 365
43. 물리적인 포트를 기반으로 IP Access-list 구성 ..... 367
43.1. IP 메시지 필터링 ..... 367
43.2. 표준 및 확장 IP Access List 생성 ..... 367
43.3. 인터페이스에 Access List 적용 ..... 368
44. IP 엑세스 제어 목록 적용 ..... 370
44.1. IP Access Control List 적용 ..... 370
45. VRRP (Virtual Router Redundancy Protocol) ..... 371
45.1. VRRP 명령어 ..... 371
46. 라우팅 프로토콜 개요 ..... 379
46.1. IP 라우팅 프로토콜 (IP Routing Protocol) ..... 379
46.2. 라우팅 프로토콜 선택 ..... 379
47. VRF 설정 ..... 381
47.1. 개요 ..... 381
47.2. VRF 구성 작업 목록 ..... 381
47.3. 구성 작업 ..... 381
47.4. VRF 구성 예제 ..... 384
48. 정적 라우팅 구성 ..... 386
48.1. 개요 ..... 386
48.2. 정적 라우팅 구성 작업 목록 ..... 386
48.3. 정적 라우팅 구성 작업 ..... 386
49. RIP 설정 ..... 388
49.1. 개요 ..... 388
49.2. RIP 구성 작업 목록 ..... 388
49.3. RIP 구성 작업 ..... 389
49.4. RIP 설정 예제 ..... 395
50. BEIGRP 설정 ..... 397
50.1. 개요 ..... 397

50.2. BEIGRP 구성 작업 목록 ..... 397
50.3. BEIGRP 설정 예시 ..... 403
51. OSPF 설정 ..... 404
51.1. 개요 ..... 404
51.2. OSPF 구성 작업 목록 ..... 404
51.3. OSPF 설정 작업 ..... 405
51.4. OSPF 설정 예시 ..... 413
52. BGP 설정 ..... 424
52.1. 개요 ..... 424
52.2. BGP 구성 작업 목록 ..... 425
52.3. 기본 BGP 기능 구성 작업 ..... 426
52.4. BGP 모니터링 및 유지관리 ..... 438
52.5. BGP 구성 예시 ..... 441
53. 기본 멀티캐스트 명령 ..... 452
53.1. 기본 멀티캐스트 명령어 ..... 452
54. NTP ..... 466
54.1. NTP master ..... 466
54.2. NTP authentication enable ..... 466
54.3. NTP authentication key ..... 467
54.4. NTP authentication trusted-key ..... 468
54.5. NTP server ..... 469
54.6. NTP peer ..... 470
54.7. show NTP ..... 471
54.8. Debug NTP ..... 472
54.9. Time zone ..... 472

이 설명서는 SG2400Series 를 구입하신 사용자에게 제품 설정 방법을 알려 드립니다. 사용자는 본 제품 취급 전에 반드시 설명서를 잘 읽은 후 지침에 따라 제품을 바르게 설정해 주십시오. 또한, 설명서를 읽으신 후에는 잘 보관하여 관리자가 바뀔 때에는 반드시 후임 관리자에게 전달하여 제품을 바르게 사용할 수 있도록 하십시오.

이 설명서는 SG2400Series 를 설정하고 관리할 네트워크 관리자를 위한 것입니다. 따라서 이 설명서를 이용할 네트워크 관리자는 네트워크 장비에 대한 전문적인 지식과 LAN(Local Area Network) 구축 및 운영에 대한 경험이 요구됩니다.

※ 본 설명서의 내용과 그림 등은 제품의 기능 향상 및 그 밖의 이유로 별도의 공지 없이 변경될 수 있습니다.

※ 본 설명서의 내용은 저작권법으로부터 보호를 받습니다. 따라서 ㈜포엠아이텍의 허가 없이 안내서의 내용을 변경할 수 없습니다.

Copyright 2025 ⓒ 4MITECH Co., Ltd.

경기도 수원시 영통구 신원로 296-21 현대테라타워영통패스트웍스 514-515호
www.4mitech.co.kr

## Release for Update

**Summary: Issue 1**

**Details:**

| Chapter/Section | Reasons for update |
|---|---|
| All | |

**Version history:**

| Status | Date of release | Reasons for change |
|---|---|---|
| 1 | 2024.05.22 | Initial release |

# 1. 개요

4MI-SG2400Series 는 4MI-SG2424TFM, 4MI-SG2406TFM, 4MI-SG2416TFM, 4MI-SG2448TFM, 4MI-SG2448TPFM 으로 구성됩니다.

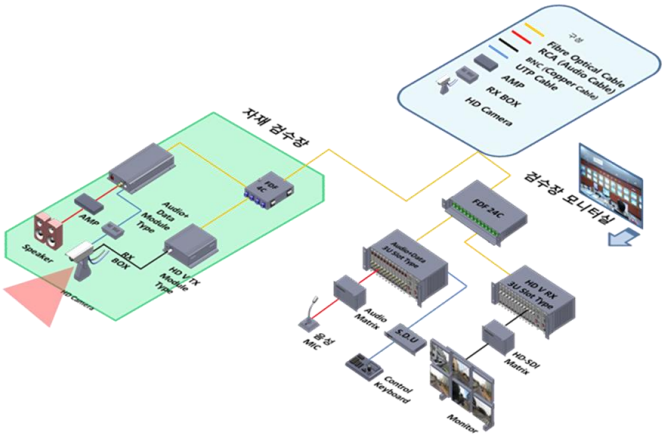
대상 제품들은 LAN 통신 매체를 이용하여 출발지 단말부터 목적지 단말로 2 개 이상의 네트워크 단말이 통신하도록 네트워크 패킷을 전달해주는 장비입니다. 즉, 네트워크상에서 PC, 프린터, 노트북, 서버, 파일스토리지 등 다양한 IT 기기들과 통신할 수 있도록 전송 및 제어하는 장비입니다.

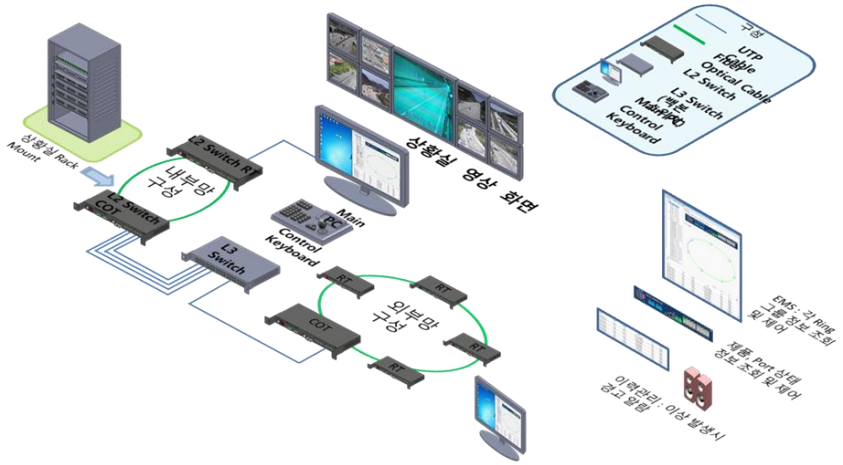
스위치는 OSI 2 계층에서 패킷을 전달하고 라우터는 스위치들을 서로 연결하여 최적 라우팅 경로를 설정한 후 OSI 3계층에서 패킷을 전달합니다. 스위치(Switch)는 MAC Address를 MAC Address테이블에 보관합니다. 이 MAC 주소는 네트워크상에서 다양한 기기를 구분하기 위해 사용하는 고유한 주소입니다. 지정된 단말과 연결된 포트로만 전송하는 방식을 취하며, 고속 통신 연결이 가능합니다. 이는 통신기기가 통신을 하기 위해 필수적으로 지정되어야 하는 기준점이자 의무사항입니다. 이러한 스위치는 ISO(국제표준화기구, International Organization for Standardization)가 규정한 네트워크 프로토콜인 OSI(open systems interconnection) 7 계층에 따라 레이어별로 L1 부터 L7 까지 나뉩니다. 기본적으로 네트워크 스위치는 전원을 이중화해 1 개의 전원 공급이 중단되더라도 별도의 전원을 이용해 통신 유지가 가능합니다. L3 스위치는 2 계층의 스위칭 기능과 3 계층의 라우팅 기능을 함께 수행 가능 하며 모듈 형태의 라우터를 탑재한 스위치와 카드형태의 라우터를 탑재한 스위치로 구분할 수 있습니다.

일반적으로 L3 스위치와 라우터 모두 IP 주소를 기반으로 목적지와 연결된 포트로 패킷을 전송하나, 하드웨어 기반으로 라우팅 및 패킷을 처리하는 L3 스위치와는 달리 라우터는 장비에 탑재된 소프트웨어를 기반으로 라우팅과 패킷을 판정합니다. 또한 L3 스위치와 라우터는 멀티캐스트, 브로드캐스트 기능을 제공하고 목적지를 알 수 없는 유니캐스트 패킷을 수신하면 모두 차단하는 기능을 제공합니다.

## 1.1. 운용환경

▶ L3 장비 설치 운영 구성도






## 1.2. 운영체계 버전

▶ 리눅스 커널 버전 5.4.226

제품에 사용하는 3rd party 라이브러리 및 소프트웨어는 아래의 최신 보안패치가 적용된 버전을 사용합니다.

▶ OpenSSH 버전 9.6

▶ OpenSSL 버전 3.1.4

## 1.3. 칩셋 및 SDK 정보

▶ 칩셋 및 SDK 정보

▶ CHIPSET: Realtek RTL9311

▶ SDK: rtk_sdk_3.6.7

## 1.4. 접속 방법

스위치 장비에 접속할 수 있는 경로는 CLI(Command line Interface)의 console, telnet, ssh 입니다.

▶ 초기 계정 정보

Username = admin / Password = admin

# 2. 기본 명령어 설명

▶ 명령어 형식 규약

| 구문 | 의미 |
|---|---|
| **Bold** | 명령 행에서 키워드를 나타냅니다. 변경되지 않고 그대로 입력해야합니다. 명령 줄에서 굵게 표시됩니다. |
| *{italic}* | 명령 행에서 매개 변수를 나타내며 실제 값으로 대체해야합니다. 중괄호 안에 기울임 꼴로 표시됩니다. |
| *⟨italic⟩* | 명령 행에서 매개 변수를 나타내며 실제 값으로 대체해야합니다. 괄호 안에 기울임 꼴로 표시됩니다. |
| [ ] | 대괄호 안에있는 선택적 매개 변수를 나타냅니다. |
| { x \| y \| ... } | 둘 이상의 옵션에서 하나의 옵션을 선택할 수 있음을 의미합니다. |
| [ x \| y \| ... ] | 둘 이상의 옵션에서 하나의 옵션을 선택할 수도 있고없는 옵션을 의미합니다. |
| { x \| y \| ... } * | 두 가지 이상의 옵션 중에서 하나 이상의 옵션을 선택하거나 모든 옵션을 선택해야한다는 의미입니다. |
| [ x \| y \| ... ] * | 두 가지 이상의 옵션 중에서 여러 옵션을 선택할 수도 있고 아무것도 선택할 수도 없다는 의미입니다. |
| &⟨1-n⟩ | "&"기호 앞에있는 매개 변수를 n 번 입력할 수 있음을 나타냅니다. |
| # | "#"기호로 시작하는 줄이 설명 줄임을 나타냅니다. |

# 3. 구성 준비

이 장에서는 처음 장비를 구성할 경우 다음과 같은 준비 작업을 설명한다.

- 스위치의 포트 수
- 시작 전 점검 사항
- 도움말 얻기
- 명령어 모드
- 명령어 취소
- 구성 저장

## 3.1. 스위치 포트 번호

스위치 실제 포트 번호는 〈Type〉 〈Slot〉/〈Port〉 형식으로 되어 있으며, 다음 비교 표에 유형 및 이름을 표기하였습니다.

| 인터페이스 형식 | 이름 | 약자 |
|---|---|---|
| 1000M Ethernet | GigaEthernet | G |
| 10Giga Ethernet | TGigaethernet | TG |
| 40Giga Ethernet | QGigaethernet | QG |
| 100Giga Ethernet | CGigaethernet | CG |

표준 구성의 확장 슬롯 번호는 아래쪽에서 1 부터 시작하여 위쪽으로 이어집니다. 장치의 포트 번호는 아래에서 위로, 왼쪽에서 오른쪽으로 1 부터 시작하여 번호가 부여 되어있습니다.

## 3.2. 시작 전 점검 사항

스위치를 구동하고 구성하기 전에 다음 사항을 확인하십시오.

- 하드웨어 설치 설명서에 따라 스위치 하드웨어를 구성합니다.
- 최초 접속은 콘솔 포트와 PC 를 연결합니다.

  (콘솔 포트 구성 정보: 속도-9600, 데이터비트-8, 정지비트-1, 패리티-none)
- PC 터미널 에뮬레이션 프로그램을 구성합니다.
- IP 네트워크 프로토콜에 따라 IP 주소, 사용자 계정 및 비밀번호에 대한 계획을 세웁니다.

## 3.3. 도움말

물음표(?) 또는 방향 키를 사용하여 모든 명령에 대한 구성 정보를 얻을 수 있습니다.

- 현재 명령에서 사용 가능한 모든 명령을 나열하려면 물음표를 입력하십시오.
Switch〉?

- 알고 있는 문자를 입력하고 물음표(공백없이)를 입력하여 현재 알려진 문자로 시작하는 명령어 목록을 얻을 수 있습니다.
Switch〉 s?

- 명령어를 입력한 다음 공백과 물음표를 입력하여 명령 매개변수 목록을 가져옵니다.
Switch〉 show ?

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

## 3.4. 명령어 모드

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

| 모드 | 명령어 | 프롬프트 형식 | 종료방법 |
|---|---|---|---|
| 부트 모드 | 장비 구동 직후 “Ctrl+p” 입력 | monitor# | “quit” |
| 사용자 모드 | 로그인 | Switch〉 | “exit” or “quit” |
| 관리 모드 | 사용자 모드에서 “enter” or “enable” 입력 | Switch# | “exit” or “quit” |
| 구성 모드 | 관리자 모드에서 “config” 입력 | Switch_config# | “exit”, “quit” or Ctrl-z |
| 포트 구성 모드 | 구성 모드에서 interface 명령어를 입력 | Switch_config_g1/1# | “exit”, “quit” or Ctrl-z |

제한된 명령의 하위 명령어는 각 명령 모드에서 사용할 수 있습니다. 명령어를 입력하는데 문제가 있으면 인터페이스 형식을 확인하고 물음표(?)를 입력하여 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 g 1/1
Switch_config_g1/1# quit
Switch_config# quit
Switch#

## 3.5. 명령어 취소

명령어를 취소하거나 기본 구성으로 돌아가려면 키워드를 추가하십시오. 명령어 앞에는 'no'를 추가합니다.

Switch_config# no ip telnet enable

## 3.6. 구성 저장

시스템 재시작 또는 전원 차단 시 원래 구성을 복구할 수 있도록 구성 변경 사항을 저장해야 합니다. Write 명령어를 사용하여 관리모드 또는 구성 모드에서 구성을 저장할 수 있습니다.

Switch# write

## 3.7. 기본구성

| 항목 | 기본값 | 비고 |
|---|---|---|
| 관리자 계정 | admin | |
| 관리자 비밀번호 | admin | |
| 콘솔 | 활성화 | 9600, 8, 1, N |
| SNMP | 비활성화 | |
| Telnet | 비활성화 | |
| SSH | 비활성화 | |
| 기본 IP 주소 | 192.168.0.1/24 | |
| 물리적 포트 상태 | 활성화 | |

# 4. 계정 관리

## 4.1. 최초 로그인

최초 장비에 접속을 할 경우 비밀번호를 설정할 수 있는 기능을 제공하며, 최초 장비 기본 구성은 Console 접속만 가능하다. 비밀번호는 9 자리 이상의 영문 대문자, 숫자, 특수문자 조합으로 구성하여야 한다.

| 명령어 | 내용 |
|---|---|
| username: admin<br>password: | 초기 계정(admin) 및 비밀번호(admin)로 로그인<br>(비밀번호는 화면에 표시 안됨) |
| please input password:<br>please input the password AGAIN: | 새로운 비밀번호를 입력 및 재입력.<br>프롬프트에 각각 입력한다. |

## 4.2. 관리자 비밀번호 변경

관리자 계정의 비밀번호를 변경하려면 아래 표에 명령 및 절차를 따른다.

| 명령어 | 내용 |
|---|---|
| Username 〈username〉 password 5 | 계정 비밀번호 변경 시작 |
| please input password:<br>please input the password AGAIN: | 새로운 비밀번호를 입력 및 재입력.<br>프롬프트에 각각 입력한다. |
| no username 〈username〉 | 생성 되어있는 사용자 계정을 삭제 |

관리자/사용자 비밀번호는 Salt 및 비밀번호 입력으로 마스터 키를 발생하는 알고리즘과 대칭형 알고리즘(AES256)으로 암호화되어 안전하게 생성/저장된다.

## 4.3. 계정 비밀번호 규칙 구성

관리자/사용자 인증 및 운용모드 변경에 사용되는 비밀번호의 규칙과 관련된 구성을 함으로써 통일된 보안 규칙에 따라 계정을 관리하기 위해 아래의 기능을 제공한다.

- 로컬 비밀번호 규칙 이름 생성
- 비밀번호의 규칙(준수 사항, 금지 항목)을 구성
- 비밀번호 규칙 구성 항목

| 명령어 | 내용 |
|---|---|
| 준수 사항 | 최소 9 자리 이상 |
| | 숫자, 대문자(영문), 소문자(영문), 특수문자 조합<br>(각 1 개 이상 포함) |
| 금지 항목 | 사용자 계정(ID)과 동일한 비밀번호 구성 금지 |
| | 동일한 문자, 숫자 연속/반복 사용 금지(3 회 이상) |
| | 키 장치의 연속된 문자 또는 숫자의 3 글자 이상 순차적 나열 금지(qwe, asd, abc, 123 등) |
| | 직전 사용된 비밀번호 재사용 금지 |
| | 비밀번호의 유효기간 구성(일, 시간, 분, 초 단위 가능) |

## 4.4. 비밀번호 규칙 생성하기

아래의 절차에 따라 로컬 계정의 비밀번호 규칙을 구성한다.

| 명령어 | 내용 |
|---|---|
| Localpass 〈name〉 | 로컬 비밀번호 규칙의 이름 구성 |
| Min-length 〈1~127〉 | 비밀번호의 최소 길이 구성(범위: 1~127 글자) |
| Element {upper-case \| lower-case \| number \| special character} | 비밀번호 조합 규칙의 필수 요소를 입력 |
| Non-user | 사용자 계정과 동일한 비밀번호 구성 금지 |
| Non-repeat | 동일한 문자, 숫자 연속/반복사용 금지(3 회 이상) |

| 명령어 | 내용 |
|---|---|
| non-seqlisting | 키 장치의 연속된 문자 또는 숫자의 순차적 나열 금지(qwe, asd, abc, 123 등) |
| non-history | 직전 사용된 비밀번호 재사용 금지 |
| local pass-group 〈group-name〉 | 이후에 입력되는 사용자 계정에 대한 비밀번호에 로컬 비밀번호 그룹 규칙을 적용하는 구성 |
| no local pass-group 〈name〉 | Local pass-group 의 구성을 해제 |
| no localpass 〈name〉 | Localpass 규칙 삭제 |

## 4.5. 로컬 계정에 비밀번호 규칙 적용하기

(방법 1) 생성된 비밀번호 규칙을 적용하려면 아래의 절차를 따른다.

| 명령어 | 내용 |
|---|---|
| local pass-group 〈group-name〉 | 이후에 입력되는 사용자 계정에 대한 비밀번호에 로컬 비밀번호 그룹 규칙을 적용하는 구성 |
| username 〈username〉 password 5 | 〈username〉은 사용할 사용자/관리자명으로 입력, 적용하여 비밀번호 구성. 정의된 pass-group 〈name〉의 규칙 적용 |
| Please input the password:<br>please input the password AGAIN: | 새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력 |

(방법 2) 생성된 비밀번호 규칙을 적용하려면 아래의 절차를 따른다.

| 명령어 | 내용 |
|---|---|
| username 〈username〉 pass-group | 〈username〉은 사용할 사용자/관리자명으로 입력, pass-group 〈name〉의 규칙을 이 계정에만 적용하여 비밀번호 구성 |
| please input password:<br>please input the password AGAIN: | 새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력 |

## 4.6. 운영모드 변경용 비밀번호에 규칙 적용하기

생성된 비밀번호 규칙을 적용하려면 아래의 절차를 따른다.

| 명령어 | 내용 |
|---|---|
| Enable pass-group 〈name〉 | 운영모드 변경 비밀번호에 생성된 로컬 비밀번호 규칙을 적용 |
| Enable level 〈1-15〉 password 5 | 운영모드 변경용 비밀번호와 권한(level 15 최상위)을 입력 |
| Please input the password:<br>please input the password AGAIN: | 새로운 비밀번호를 프롬프트에 입력 및 재입력 |

운영모드 변경 비밀번호는 Salt 및 비밀번호 입력으로 마스터 키를 발생하는 알고리즘과 대칭형 알고리즘(AES256)으로 암호화되어 안전하게 생성/저장됩니다.

## 4.7. RADIUS 계정에 비밀번호 규칙 적용하기

생성된 비밀번호 규칙을 적용하려면 아래의 절차를 따른다.

| 명령어 | 내용 |
|---|---|
| radius-server pass-group 〈name〉 | 생성된 로컬 비밀번호 규칙을 적용한다. (선택) |
| Radius-server key 5 | RADIUS 키 입력 모드 |
| Please input the password:<br>please input the password AGAIN: | 새로운 비밀번호를 프롬프트에 입력 및 재입력 |

## 4.8. TACACS 계정에 비밀번호 규칙 적용하기

생성된 비밀번호 규칙을 적용하려면 아래의 절차를 따른다.

| 명령어 | 내용 |
|---|---|
| tacacs-server pass-group 〈name〉 | 생성된 로컬 비밀번호 규칙을 적용한다. (선택) |
| tacacs-server key 5 | TACACS 키 입력 모드 |
| Please input the password:<br>please input the password AGAIN: | 새로운 비밀번호를 프롬프트에 입력 및 재입력 |

# 5. 시스템 관리 구성

## 5.1. 파일 관리 구성

### 5.1.1. 파일 시스템 관리

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

| 명령어 | 설명 |
|---|---|
| **format** | 파일 시스템을 포맷하고 모든 데이터를 삭제 |
| **dir** [filename] | 파일 및 디렉터리 이름을 표시.<br>대괄호 "[]" 안의 파일 이름은 여러 문자로 시작하는 파일을 표시하는 것을 의미. |
| **delete** filename | 파일을 삭제. 파일이 존재하지 않으면 시스템에서 별도 표현. |
| md dirname | 디렉터리를 생성 |
| rd dirname | 디렉터리를 삭제. 디렉터리가 존재하지 않으면 시스템에서 별도 표현. |
| more 〈filename〉 | 파일의 내용을 표시합니다. 파일 내용을 한 페이지로 표시할 수 없는 경우 페이지 별로 표시 |
| cd | 현재 파일 시스템의 경로를 변경 |
| pwd | 현재 경로를 표시 |

### 5.1.2. 부트롬(모니터모드) 진입하기

시스템(장비) 기동 후 키 입력 장치의 "Control + p" 수차례 입력

### 5.1.3. 시스템 부트 파일 구성

monitor#boot flash 〈local_filename〉

이 명령에 지정한 파일명으로 플래시에서 시스템을 부팅 하는 명령입니다. 기본 시스템 파일 이름은 switch.bin 입니다. 파일명은 대소문자를 구분하지 않습니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| *local_filename* | 플래시 메모리에 저장된 파일 이름으로 사용자는 파일 이름을 입력 |

〈예제〉
monitor#boot flash switch.bin

### 5.1.4. 이더넷 IP 주소 구성

monitor#ip address 〈ip_addr〉 〈net_mask〉

이 명령은 관리용 이더넷 포트의 IP 주소를 구성합니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| *Ip_addr* | IP 주소 |
| *Net_mask* | subnet mask |

〈예제〉
monitor#ip address 192.168.1.1 255.255.255.0

### 5.1.5. 기본 경로 구성

monitor#ip route default 〈ip_addr〉

이 명령은 기본 경로를 구성하여 사용합니다. 기본 경로는 하나만 구성할 수 있습니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| *Ip_addr* | 게이트웨이 IP 주소 |

〈예제〉
monitor#ip route default 192.168.1.254

### 5.1.6. Ping 을 이용하여 네트워크 연결 상태 시험

monitor#ping 〈ip_address〉

이 명령어는 네트워크 연결을 확인합니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|

| | |
|---|---|
| *Ip_address* | 도착지 IP 주소 |

〈예제〉
monitor#ping 192.168.1.2
PING 192.168.1.2: 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0, time=0, ms
64 bytes from 192.168.1.2: icmp_seq=1, time=0, ms
64 bytes from 192.168.1.2: icmp_seq=2, time=0, ms
64 bytes from 192.168.1.2: icmp_seq=3, time=0, ms
64 bytes from 192.168.1.2: icmp_seq=4, time=0, ms
----192.168.1.2 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
Round-trip (ms) min/avg/max = 0/0/0

### 5.1.7. 소프트웨어 업데이트

사용자는 이 명령어를 사용하여 스위치의 부트롬 또는 시스템 소프트웨어(펌웨어)를 원격으로부터 로컬로 다운로드하여 업데이트 할 수 있습니다. 또한, 설정 초기화 구성 파일을 복사할 때도 사용할 수 있습니다.

**TFTP 를 이용한 부트롬 업데이트**

monitor#copy tftp: rom: [A.B.C.D]

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| A.B.C.D | TFTP 서버의 IP 주소. 지정된 IP 주소가 없으면 복사 명령이 실행된 후, 서버의 IP 주소를 입력하라는 메시지 출력 |
| source file name | TFTP 서버에 있는 받을 파일의 이름 입력 |
| destination file name | 로컬 플래시에 저장할 파일의 이름을 입력 |

**TFTP 를 이용하여 시스템 소프트웨어 업데이트 하기**

monitor#copy tftp: flash: [A.B.C.D]

이 명령어는 TFTP 서버의 파일을 시스템의 플래시로 복사합니다. 명령을 입력하면 시스템은 원격 서버 이름과 원격 파일 이름을 입력하라는 메시지를 표시합니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|

| | |
|---|---|
| A.B.C.D | TFTP 서버의 IP 주소. 지정된 IP 주소가 없으면 복사 명령이 실행된 후, 서버의 IP 주소를 입력하라는 메시지 출력 |
| source file name | TFTP 서버에 있는 받을 파일의 이름 입력 |
| destination file name | 로컬 플래시에 저장할 파일의 이름을 입력 |

〈예제〉
다음 예제는 TFTP 서버에서 읽은 파일을 스위치에 switch.bin 으로 저장하는 것을 보여줍니다.

monitor#copy tftp: flash: 192.168.0.254
prompt: source file name[ ]? 4MI-G2416TFM-L3_interAptiv_2.2.0F_110667.bin
prompt: destination file name[4MI-G2416TFM-
L3_interAptiv_2.2.0F_110667.bin]? switch.bin
##########################################################################
##########
(생략)
TFTP:successfully receive 14053 blocks, 7195135 bytes
Flush to flash…..*
**********

### 5.1.8. 사용자 구성 업데이트(선택)

스위치 구성은 저장(write) 명령에 의해 파일로 저장되고 파일 이름은 startup-config 입니다. 소프트웨어 업데이트와 유사하게 아래의 명령을 사용하여 사용자의 선택에 따라 백업된 구성 파일을 업로드 하여 구성을 복원할 경우 사용할 수 있습니다.

**TFTP 이용**

monitor# copy tftp: startup-config [A.B.C.D]

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| A.B.C.D | TFTP 서버의 IP 주소. 지정된 IP 주소가 없으면 복사 명령이 실행된 후, 서버의 IP 주소를 입력하라는 메시지 출력 |
| source file name | TFTP 서버에 있는 받을 파일의 이름 입력 |
| destination file name | 로컬 플래시에 저장할 파일의 이름을 입력 |

### 5.1.9. 시스템 재시작

부트롬 모드에서 부트롬, 시스템 소프트웨어, 구성 파일 등을 업데이트 하고 스위치를 재시작 하려면 아래의 명령을 입력합니다.

monitor# reboot
prompt: Do you want to reboot the Switch(y/n)? y
Please wait…
(생략)
Starting kernel …
(생략)
Loading switch.bin……
Start Decompress switch.bin
(생략)
Please wait for loading startup-config to be finished.
(생략)
Jan 1 00:01:07 Switch system started -

Welcom to 4MI 4MI-G2416TFM-L3 Ethernet Switch
Switch〉

## 5.2. 기본 시스템 관리 구성

### 5.2.1. FTP 를 통한 소프트웨어 및 구성 업데이트

**FTP 서버에서 스위치로 파일을 다운로드**

운용 중 FTP 를 이용하여 소프트웨어 및 구성을 업데이트 하십시오. copy 명령어를 사용하여 FTP 서버에서 스위치로 파일을 다운로드 합니다.

copy ftp: flash: {〈64-1024〉 | A.B.C.D | -w | type 〈1 | 2〉 | 〈active / passive〉 | ncheckсize}

copy ftp: flash: 명령만 입력하면 시스템에서 계정, 비밀번호 원격 서버 주소, 소스 파일 목적지 파일 이름을 입력하라는 메시지를 출력하며 그에 따라 입력합니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| A.B.C.D | FTP 서버의 IP 주소. 지정된 IP 주소가 없으면 “copy” 명령을 실행한 후 IP 주소를 입력하라는 메시지가 출력됩니다. |
| ftp user name | FTP 서버의 사용자 이름. “copy” 명령을 실행한 후 사용자 이름을 입력하라는 메시지가 출력됩니다. |
| ftp user password | FTP 서버의 비밀번호. “copy” 명령을 실행한 후 암호를 입력하라는 메시지가 출력됩니다. |

| | |
|---|---|
| 〈64-1024〉 | 데이터 블록 크기 값. 선택 사항. (기본값=512) |
| -w | 파일을 받고 해시값 검사 없이 파일을 플래시에 씀. 선택 사항 |
| 〈active \| passive〉 | FTP 연결 모드를 활성 모드(active)와 수동 모드(passive) 중에서 선택. 선택사항. |
| type 〈1 \| 2〉 | 데이터 전송 모드 구성(1: ascii, 2: binary) |
| Nchecksize | 서버의 파일 크기를 확인하지 않음. 선택 사항 |

**스위치의 파일 시스템에서 FTP 서버로 파일을 업로드**

스위치의 파일 시스템에서 FTP 서버로 파일을 업로드 하십시오.

copy flash: ftp: {〈64-1024〉 | A.B.C.D | -w | type 〈1 | 2〉 | 〈active / passive〉 | nchecksize}

copy ftp: flash: 명령만 입력하면 시스템에서 계정, 비밀번호 원격 서버 주소, 소스 파일 목적지 파  일 이름을 입력하라는 메시지를 출력하며 그에 따라 입력합니다.

〈매개변수 구성〉

| 매개변수 | 설명 |
|---|---|
| A.B.C.D | FTP 서버의 IP 주소. 지정된 IP 주소가 없으면 “copy” 명령을 실행한 후 IP 주소를 입력하라는 메시지가 출력됩니다. |
| ftp user name | FTP 서버의 사용자 이름. “copy” 명령을 실행한 후 사용자 이름을 입력하라는 메시지가 출력됩니다. |
| ftp user password | FTP 서버의 비밀번호. “copy” 명령을 실행한 후 암호를 입력하라는 메시지가 출력됩니다. |
| 〈64-1024〉 | 데이터 블록 크기 값. 선택 사항. (기본값=512) |
| -w | 파일을 받고 해시값 검사 없이 파일을 플래시에 씀. 선택 사항 |
| 〈active \| passive〉 | FTP 연결 모드를 활성 모드(active)와 수동 모드(passive) 중에서 선택. 선택사항. |
| type 〈1 \| 2〉 | 데이터 전송 모드 구성(1: ascii, 2: binary) |
| Nchecksize | 서버의 파일 크기를 확인하지 않음. 선택 사항 |

〈예제〉
다음은 “main.bin” 파일이 서버에서 읽히고 스위치에서 switch.bin 으로 변경되었음을 보여줍니다.

config#copy ftp: flash:
prompt: ftp user name[anonymous]? login-name

prompt: ftp user password [anonymous] ? login-password
prompt: source file name [] ? main.bin
prompt: remote-server ip address [] ? 192.168.0.1
prompt: destination file name [main.bin] ? switch.bin

〈참조〉
FTP 서버가 작동하지 않을 때 대기 시간이 길어집니다. 이 문제는 TCP 종료시간 (기본:75sec)으로 인해 발생하면 TCP 연결 시간을 수정하기 위해 "ip tcp synwait-time" 글로벌 모드에서 명령을 구성합니다.

일부 네트워크 통신의 조건에서 FTP 를 사용하면 데이터 전송 속도가 상대적으로 느릴 수 있습니다. 최상의 효과를 얻으려면 전송 블록의 크기를 적절하게 조정할 수 있습니다. 기본 크기는 512 이며 대부분의 네트워크에서 비교적 높은 작동 속도를 보장합니다.

## 5.3. VTY 구성 안내

시스템은 "line" 명령어를 사용하여 터미널 매개변수를 구성합니다.
이 명령을 통해 화면에 표시된 터미널을 통해 구성을 할 수 있습니다.

### 5.3.1. 유형

시스템에 접속 가능한 방법은 2 가지의 유형이 있습니다.

console(콘솔), virtual terminal(가상터미널)

시스템마다 다른 유형의 라인이 있습니다. 적절한 구성에 대해서는 다음 소프트웨어 및 하드웨어 구성 안내서를 참조 하십시오.

| Line 유형 | 인터페이스 | 설명 | 번호 |
|---|---|---|---|
| CON(CTY) | Console | 구성을 위해 시스템에 로그인 | 0 |
| VTY | 가상 단말 | SSH 및 시스템의 포트(예: 이더넷 및 직렬 포트)를 통해 로그인 할 수 있습니다. | 0-31 |

### 5.3.2. Line console

| 명령어 | 설명 |
|---|---|
| Config | 구성 모드로 진입 |
| line console 0 | 라인 콘솔 모드로 전환 |

| | |
|---|---|
| Pass-group 〈group-name〉 | 비밀번호 규칙 그룹을 적용하는 구성 |
| Password 5 | 비밀번호 입력 |
| please input password:<br>please input the password AGAIN: | 사용할 비밀번호 입력 및 확인까지 2 회 입력.<br>(인증 피드백 보호기능 제공) |
| no password | 콘솔에 생성되어있는 비밀번호를 삭제 |
| No pass-group | 콘솔에 적용된 비밀번호 규칙 그룹을 해제 |

### 5.3.3. Line VTY

| **명령어** | **설명** |
|---|---|
| config | 구성 모드로 진입 |
| line vty 〈0-31〉〈0-31〉 | 라인 VTY 모드로 전환 |
| pass-group 〈group-name〉 | 비밀번호 규칙 그룹을 적용하는 구성 |
| password 5 | 비밀번호 입력 |
| Please input the password:<br>Please input the password AGAIN: | 사용할 비밀번호 입력 및 확인까지 2 회 입력<br>(인증 피드백 보호기능 제공) |
| no password | VTY에 생성되어있는 비밀번호를 삭제 |
| no pass-group | VTY에 적용된 비밀번호 규칙 그룹을 해제 |

show line 을 실행하여 VTY 구성을 확인합니다.

# 6. 네트워크 관리 구성

## 6.1. SNMP 구성

### 6.1.1. 개요

SNMP 시스템은 다음과 같이 나눌 수 있습니다.

- SNMP management side (NMS)
- SNMP agent (AGENT)
- Management information base (MIB)

SNMP 는 응용프로그램 계층에서 작동하는 프로토콜입니다. SNMP 관리 측과 에이전트 간에 패킷 형식을 제공합니다.

SNMP 관리 측은 네트워크 관리 시스템(CiscoWorks 와 같은 NMS)의 일부가 될 수 있습니다. Agent 및 MIB 은 시스템에 저장됩니다. 시스템 SNMP 를 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 MIB 에서 데이터를 수집합니다. MIB 은 장치 매개 변수로 네트워크 장비의 데이터 베이스입니다. 또한 에이전트는 관리자의 로딩 또는 데이터 구성 요청에 응답할 수 있습니다.

SNMP 에이전트는 관리 측에 트랩을 보낼 수 있습니다. Trap 은 네트워크의 특정 상태를 나타내는 경보 및 각종 정보를 SNMP 로 전송합니다. Trap 은 부적절한 사용자 인증, 재시작, 링크 계층상태(활성화/비활성화), TCP 연결 및 종료, 인접 시스템 연결 또는 잃어버릴 수 있는 기타 중요 이벤트를 나타낼 수 있습니다.

**〈SNMP 알림〉**
특별한 이벤트가 발생하면 시스템은 SNMP 관리시스템에 “inform”을 보냅니다. 예를 들어, 에이전트 시스템이 비정상 상태를 감지하면 SNMP 관리시스템으로 정보를 보냅니다. SNMP 알림은 Trap 으로 처리되거나 요청을 보낸 것을 알릴 수 있습니다. 장비에서는 Trap 을 수신할 때 응답을 보내지 않으므로 수신 측은 Trap 이 수신되었다고 확신할 수 없습니다. 따라서 Trap 은 신뢰할 수 없습니다. 이에 비해, SNMP 관리시스템 측에서 “inform request”을 수신하는 SNMP 관리시스템에서 SNMP 정보에 대한 응답으로 PDU 를 사용합니다. 관리시스템에서

"inform request"이 수신되지 않으면 echo 가 전송되지 않습니다. 장비에서는 응답을 보내지 않으면 "inform request"을 다시 보낼 수 있습니다. 그런 다음 알림은 관리시스템에 도달할 수 있습니다 "inform request"은 보다 신뢰성이 높기 때문에 시스템 및 네트워크의 더 많은 자원을 소비합니다. 트랩은 전송될 때 폐기됩니다. 에코가 수신되거나 요청시간이 초과될 때까지 "inform request"를 메모리에 저장해야 합니다. 또한 Trap 은 한 번만 전송되고 "inform request"는 여러 번 재전송 될 수 있습니다. 재전송 "inform request"는 네트워크 통신에 추가가 되므로 더 많은 부하를 유발합니다. 또한 트랩은 한 번만 전송되고 "inform request"은 여러 번 재전송 될 수 있습니다. 따라서 트랩 및 알림 요청은 안정성과 리소스 간에 균형을 유지합니다. SNMP 관리시스템에서 모든 알림을 대량 수신해야 하는 경우 "inform request"을 사용할 수 있습니다. 네트워크의 통신량을 우선시하고 모든 통지를 받을 필요가 없으면 Trap 을 사용할 수 있습니다. 이 스위치는 트랩을 지원하지만 "inform request"에 대한 확장도 제공합니다.

**〈SNMP 버전〉**

다음과 같은 SNMP 버전을 스위치 시스템은 지원합니다.

- SNMPv1---간단한 네트워크 관리 프로토콜 RFC1157 에 정의된 인터넷 표준 프로토콜입니다.
- SNMPv2C---SNMPv2 그룹 기반 관리 프레임 워크로 RFC1901 에 정의된 표준 프로토콜입니다.
- SNMPv3---RFC3410 에 정의된 간단한 네트워크 관리 프로토콜 버전 3

SNMPv1 은 그룹 기반 보안 형식을 사용하고, IP 주소 접근 제어 및 암호를 사용하여 에이전트 MIB 에 접근할 수 있는 관리 측 그룹을 정의합니다.

SNMPv3 는 네트워크를 통한 패킷 인증 및 암호화의 조합을 통해 장치에 대한 보안 접근을 제공합니다. SNMPv3 가 제공하는 보안 기능은 다음과 같습니다.

- 메시지 무결성— 패킷이 전송 중에 변조되지 않았는지를 확인합니다
- 인증—메시지가 유효한 소스 주소 인지 확인합니다.
- 인증—메시지가 유효한 소스 주소 인지 확인합니다.

SNMPv3 은 보안 모델과 보안 수준을 모두 제공합니다. 보안 모델은 사용자 및 사용자가 상주하는 그룹에 대해 구성되는 인증 정책입니다. 보안 수준은 보안 모델 내에서 허용되는 보안 수준입니다. 보안 모델과 보안 수준의 조합은 SNMP 패킷을 처리할 때 사용되는 보안 메커니즘을 결정합니다. 인증 및 암호화, 인증 및 암호화 없음, 인증 없음의 세 가지 보안 모델을 사용할 수 있습니다

관리 작업 스테이션이 지원하는 SNMP 버전으로 SNMP 에이전트를 구성해야합니다. 에이전트는 많은 관리 측과 통신할 수 있습니다.

**〈MIB 지원〉**
우리 시스템의 SNMP 는 모든 MIBII 변수 (RFC 1213)와 SNMP 트랩 (RFC 1215)을 지원합니다. 스위치 시스템은 각 시스템에 대해 고유 MIB 확장을 제공합니다.

## 6.2. SNMP 구성 업무

- SNMP 보기 구성
- SNMP community 접근 제어 구성 및 수정
- 시스템 관리자의 호출 및 시스템 위치 구성
- SNMP agent 데이터 패킷의 최대 길이 정의 SNMP 상태 모니터링
- SNMP 상태 모니터링
- SNMP trap 구성
- SNMP 바인딩 소스 주소 구성
- SNMPv3 그룹
- SNMPv3 사용자
- SNMPv3 EngineID 구성

**〈SNMP 뷰 구성〉**
SNMP 보기는 MIB 에 대한 액세스 권한(include/exclude)을 제어하는 것입니다. 다음 명령을 사용하여 구성하십시오.

| 명령어 | 설명 |
|---|---|
| snmp-server enable | snmp 구성을 활성화 |
| snmp-server view name oid [exclude \| include] | 보기 기능의 이름, OID 지정 MIB 의 하위 트리 또는 테이블을 추가하고 이름에 객체 식별자의 액세스 권한을 지정합니다.<br>Exclude: 액세스 거부<br>Include: 액세스 허용 |

SNMP 보기에서 액세스 할 수있는 하위 집합은 MIB 개체를 "exclude" 개체로 "include"는 나머지 개체입니다. 구성되지 않은 개체는 기본적으로 액세스 할 수 없습니다. SNMP 보기를 구성한 후 SNMP 그룹 이름을 구성하는 SNMP 보기를 구현하여 그룹 이름에서 액세스 할 수있는 개체의 하위 집합을 제한할 수 있습니다.

**〈SNMP Community 에 대한 접근 제어 구성 또는 수정〉**

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

| 명령어 | 기능 |
|---|---|
| **snmp-server community** string [**view** viewname] [ro \| rw] [word] | 그룹의 community 값을 정의합니다. |

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

**〈시스템 관리자의 호출 방법 및 시스템의 위치 설명 구성〉**

SysContact 와 SysLocation 은 시스템 그룹에서의 관리 변수는 MIB 이며 각각의 장비의 ID 값과 위치를 정의합니다. 이 정보는 Config 를 통해서 액세스 할 수 있습니다. 글로벌 모드에서 다음 명령을 사용할 수 있습니다.

| 명령어 | 기능 |
|---|---|
| **snmp-server contact** text | 노드의 링크 관리자에 대한 문 자열을 구성합니다. |
| **snmp-server location** text | 노드 위치의 문자열을 구성합니다. |

**〈장비에서 보내는 SNMP 데이터 패킷의 최대 길이 정의〉**

요청 또는 응답을 받으면 데이터 패킷의 최대 길이를 구성할 수 있습니다. 글로벌 모드에서 다음 명령어를 사용할 수 있습니다.

| 명령어 | 기능 |
|---|---|
| **snmp-server packetsize** byte-count | 데이터 패킷의 최대 길이를 구 성합니다. |

**〈SNMP 상태 모니터링〉**

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

| 명령어 | 기능 |
|---|---|
| **show snmp** | SNMP 상태 모니터 |

**〈SNMP trap 구성〉**

다음 명령어를 사용하여 SNMP trap 을 보내도록 시스템에 구성할 수 있습니다.

- trap 을 보내도록 시스템 구성

전역모드에서 다음을 실행하여 트랩을 호스트로 보내도록 구성합니다.

| 명령어 | 기능 |
|---|---|
| **snmp-server host** host community-string [trap-type] | Trap 메시지의 수신자를 지정합니다. |
| **snmp-server host** host [traps\|informs] {version {v1 \| v2c \| v3 {auth \| noauth \| priv}}} communitystring [trap-type] | Trap 메시지의 수신자, 버전, 사용자 이름을 지정합니다. SNMPv3 trap 의 경우 호스트가 트랩 메시지를 수신하도록 호스트에 대한 SNMP engine ID 를 구성해야 합니다. |

시스템이 시작되면 SNMP 구성은 자동으로 실행됩니다. 모든 유형의 Trap 이 활성화됩니다. "snmp-server host "명령어를 사용하여 어떤 호스트가 어떤 종류의 Trap 을 수신할 지 지정할 수 있습니다.
일부 Trap 은 다른 명령을 통해 제어해야 합니다. 예를 들어, 인터페이스를 열거나 닫을 때 SNMP 링크 트랩을 보내려면 인터페이스 구성창에서 "snmp trap link-status" 명령어를 실행하여 링크 트랩을 활성화해야 합니다.

Trap 을 수신하려면 호스트가 "snmp-server host "명령을 구성해야 합니다.

- Trap 의 실행중인 매개변수 수정하기

선택적 항목으로 Trap 이 시작되는 소스 인터페이스, 메시지 큐의 길이 또는 각 호스트의 재전송 간격 값을 지정할 수 있습니다. Trap 의 실행 매개변수를 수정하려면 전역모드에서 다음 선택적 명령어를 사용할 수 있습니다.

| 명령어 | 기능 |
|---|---|
| **snmp-server trap-source null** | Trap 메시지의 소스 를 null interface 로 지정한다 |
| **snmp-server queue-length** length | Trap 이 있는 각 호스트에 대한 메시지 큐의 길이를 작성합니다. (기본값: 10) |
| **snmp-server trap-timeout** seconds | 재전송 대기열에서 Trap 을 재전송 할 빈도를 정의합니다. (기본값: 30 초) |

**〈SNMP 바인딩 소스 주소 구성〉**
전역모드에서 다음 명령어를 실행하여 SNMP 메시지의 소스 주소를 구성하십시오.

| 명령어 | 기능 |
|---|---|
| **snmp source-addr** ipaddress | SNMP 메시지의 출발지를 구성합니다. |

**〈SNMPv3 group 구성하기〉**
그룹을 구성하려면 다음 명령어를 실행하십시오.

| 명령어 | 기능 |
|---|---|
| **snmp-server group** [groupname **v3** {**auth** \| **noauth** \| **priv**} [**read** readview] [**write** writeview] [**notify** notifyview] [**access** access-list] | SNMPv3 그룹을 구성합니다. 기본적으로 인터넷 하위 트리의 모든 항목 만 읽을 수 있습니다. Priv: SNMP v3 전송 패킷 인증 및 암호화. (권장) Auth: SNMP v3 전송 패킷 인증, 암호화는 미적용. Noauth: SNMP v3 전송 패킷 미인증, 암호화는 미적용 |

**〈SNMPv3 사용자 구성하기〉**

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 통과할 수 없습니다.

| 명령어 | 기능 |
|---|---|
| **snmp-server user** 〈name〉 〈group〉 **v3 priv** 〈aes128 \| aes256 \| aes256-c **auth** 〈sha \| sha256〉 **5** | SNMP v3 사용자 이름, 그룹, 암호화, 인증 방식 구성 5 암호화 방식(PBKDF2 + AES256) 평문 (구성 후, 9 암호문 형태로 표시) |
| input priv:<br>comfirm priv:<br>input auth:<br>comfirm auth: | Priv: 암호화 비밀번호 입력(9 ~32 글자) Auth: 사용자 인증 비밀번호 입력(9~32 글자) |

**〈SNMPv3 Engine ID 구성하기〉**

SNMP EngineID 는 SNMP Engine 을 식별하는데 사용됩니다. 기존의 SNMP 관리시스템 및 장비는 SNMPv3 프레임의 SNMP Engine 에 포함되어 있습니다.

| 명령어 | 기능 |
|---|---|
| **snmp-server engineID local** engineid-string | 자체 SNMP 엔진의 구성 방법입니다. (선택) |

### 6.2.1. 구성 예제

**〈예제 1〉**

snmp-server community 5 public RO
snmp-server community 5 private RW
snmp-server host 192.168.10.2 public

위는 다음과 같은 예를 나타냅니다:

- 모든 MIB 변수를 읽을 수 있는 공유 문자열을 구성하는 방법
- 모든 MIB 변수를 읽고 쓸수 있는 Community 문자열을 개인 구성하는 방법

Community 문자열을 Public 을 사용하여 시스템의 MIB 변수를 읽을 수 있습니다.

또한 Community 문자열을 Private 하게 구성하여 MIB 변수를 읽어 시스템에 쓰기 가능한 MIB 변수를 입력할 수 있습니다.
위의 명령은 시스템이 Trap 을 보내야 할 때 Community 문자열을 Public 하게 지정하여 Trap 을 192.168.10.2 으로 보내게 됩니다. 예를 들어, 장비의 포트가 다운상태가 되었다면 장비에서는 192.168.10.2 로 링크다운 Trap 정보를 보냅니다.

**〈예제 2〉**

```
Switch# show running-configuration non-interface
snmp-server engineID local 15a000003800005230
snmp-server group getter v3 auth
snmp-server group setter v3 priv write v-write
snmp-server user get-user getter v3 auth sha 9
45cc14e33f29f2dac965c3e7a86399065c56fa86d73fd879fb424419cac7a3ff
snmp-server user set-user setter v3 auth sha 9
3cf40643b26872e556b053bf190dbdba5 2aa1ce594605fd77247f3322f88b48f
snmp-server user test admin_g v3 priv aes256 auth sha256 9
65c03eaf2ea90e0cdb8cf
68572b690fcec03713d31f1e566738db3e2dbe0fdaed3ec854a04c12dacc1ca380d
999afe8d0054e02370c8069000c8efd3ea112227
snmp-server host 90.0.0.3 informs version v3 auth notifier
snmp-server view v-write internet included
```

위의 예시는 SNMPv3 을 사용하여 장비를 관리하는 방법을 보여줍니다.

그룹 Setter 는 장치를 구성할 수 있는 반면, 그룹 Getter 는 장치정보를 찾아볼 수 있습니다.
사용자 구성 사용자가 그룹 User 가 그룹 Setter 에 속할 때 사용자 Get-user 는 그룹 getter 에 속합니다.

get-user 의 경우 보안 수준은 인증은 되지만 암호화되지 않습니다.

Set-user 의 경우 보안 수준은 인증 및 암호화합니다.

장비에서 Key event 가 발생하면 username notifier 를 사용하여 관리자의 호스트는 90.0.0.3 에게 알림 메시지를 보냅니다.

### 6.2.2. Snmp-server community

다음 명령어는 특정 커뮤니티를 삭제하는 방법을 보여줍니다.
**no snmp-server community string**

다음 명령어는 모든 커뮤니티를 삭제하는 방법을 보여줍니다.

**no snmp-server community**

| 매개변수 | 설명 |
|---|---|
| 0 | 평문(텍스트) 형태로 커뮤니티 문자열을 설정합니다. |
| 7 | 암호화된 커뮤니티 문자열을 설정합니다. |
| *String* | 접근 가능한 SNMP 프로토콜의 커뮤니티 문자열(비밀번호와 유사)입니다. |
| *view view-name* | (옵션) 사전에 정의된 뷰의 이름을 나타냅니다. 이 뷰 내에서 커뮤니티에 유효한 MIB 객체가 정의됩니다. |
| *Ro* | (옵션) 읽기 전용(read-only) 권한을 지정합니다. 권한이 있는 워크스테이션은 MIB 객체를 읽을 수만 있습니다. |
| *Rw* | (옵션) 읽기 및 쓰기(read-write) 권한을 지정합니다. 권한이 있는 워크스테이션은 MIB 객체를 읽고 수정할 수 있습니다. |
| *Word* | (옵션) 커뮤니티 문자열을 통해 액세스할 수 있는 SNMP 프록시의 IP ACL 이름을 지정합니다. |

**(1) 기본값**

기본적으로 SNMP 커뮤니티 문자열은 모든 객체에 대한 읽기 전용 권한을 부여합니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

접근 가능한 SNMP 프로토콜의 커뮤니티 액세스 문자열을 설정하려면 전역 설정 모드에서 snmp-server community 명령을 실행합니다.

**snmp-server community [0|7] string [view view-name] [ro | rw] [word]**
**no snmp-server community string**
**no snmp-server community**

**(4) 예제**

"comaccess"라는 문자열을 SNMP 에 배포하고, 읽기 전용 액세스를 허용하며, 특정 IP ACL 을 지정하는 예제:
snmp-server community comaccess ro allowed

"mgr"라는 문자열을 SNMP 에 배포하고, "restricted" 뷰 내에서 읽기 및 쓰기 권한을 부여하는 예제:
snmp-server community mgr view restricted rw

"comaccess" 커뮤니티를 삭제하는 예제:
no snmp-server community comaccess

**(5) 관련 명령어**

access-list
snmp-server view

### 6.2.3. snmp-server contact

이 명령어는 시스템 그룹의 MIB 변수인 sysContact 에 해당합니다.

| 매개변수 | 설명 |
|---|---|
| *text* | 담당자 정보 문자열입니다. |

**(1) 기본값**

기본적으로 담당자 정보는 설정되지 않습니다.

**(2) 명령어 모드**

전역 설정 모드

**(3) 구문**

관리 노드의 담당자 정보를 설정하려면 다음 명령어를 실행합니다
**snmp-server contact** *text*
**no snmp-server contact**

**(4) 예제**

노드의 담당자 정보를 설정하는 예제

snmp-server contact Dial_System_Operator_at_beeper_#_27345

### 6.2.4. snmp-server engineID local

이 명령어는 로컬 에이전트의 SNMP 엔진 ID 를 설정하는 데 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *engineID* | SNMP 엔진 ID |

**(1) 기본값**

기본적으로 설정되지 않습니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

로컬 에이전트의 SNMP 엔진 ID 를 구성하려면 다음 명령어를 실행합니다.
기본 설정으로 돌아가려면 no 형식의 명령을 사용합니다.

**snmp-server engineID local** *engineID*
**no snmp-server engineID local** engineID

**(4) 예제**

snmp-server engineID local 80000cf80300e00f3f56e3

### 6.2.5. snmp-server group

이 명령어는 해당 그룹 내 사용자의 접근 권한을 지정하는 데 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| groupname | 생성하거나 수정할 SNMP 그룹의 이름입니다. |
| v3 | SNMP 프로토콜의 버전 ID 를 나타냅니다. |
| auth\|noauth\|priv | SNMPv3 그룹의 최소 보안 수준을 지정합니다. |
| readview | GET 작업의 접근 권한을 정의하는 뷰입니다. |
| writeview | SET 작업의 접근 권한을 정의하는 뷰입니다. |
| notifyview | 트랩 패킷 전송 중 접근 권한을 정의하는 뷰입니다. |
| access-list | SNMP 그룹의 사용자가 IP 액세스 제어 목록을 통과하도록 허용합니다. |

**(1) 기본값**

기본적으로 readview 는 인터넷 서브 트리의 모든 리프에 대한 접근을 허용합니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 그룹을 생성하거나 업데이트하려면 다음 명령어를 실행합니다.
SNMP 그룹을 삭제하려면 두 번째 명령어를 실행합니다.

**snmp-server group** [groupname { **v3** [**auth** | **noauth** | **priv**]}] [**read** readview] [**write** writeview] [**notify** notifyview] [**access** access-list]

**(4) 예제**

다음 예제에서는 SNMP 그룹이 설정되며, 그룹 이름은 setter 입니다. SNMP 프로토콜의 버전 ID 는 3, 보안 수준은 **인증 및 암호화(authentication and encryption)**이며, set 연산으로 접근할 수 있는 뷰(view)는 v-write 입니다.

snmp-server group setter v3 priv write v-write

**(5) 관련 명령어**

snmp-server view
snmp-server user

### 6.2.6. snmp-server [host|host6]

이 명령어를 입력하지 않으면 트랩이 전송되지 않습니다. 스위치에서 SNMP 트랩을 전송하도록 설정하려면 snmp-server host 명령어를 실행해야 합니다. trap-type 키워드가 포함되지 않은 경우, 해당 호스트의 모든 종류의 트랩이 활성화됩니다.

trap-type 키워드가 포함된 경우, 해당 키워드와 관련된 모든 트랩 유형이 활성화됩니다.
각 호스트에 대해 이 명령어에서 여러 개의 트랩 유형을 지정할 수 있습니다.

동일한 호스트에 대해 여러 개의 snmp-server host 명령어를 설정하는 경우, 해당 호스트로 전송되는 SNMP 트랩 메시지는 커뮤니티 문자열과 트랩 유형 필터링에 의해 결정됩니다.
(동일한 호스트와 동일한 커뮤니티 문자열에 대해 하나의 트랩 유형만 설정할 수 있습니다.)
trap-type 옵션의 사용 가능 여부는 스위치 유형 및 해당 스위치에서 지원하는 라우팅 소프트웨어의 속성에 따라 달라질 수 있습니다.

| 매개변수 | 설명 |
|---|---|
| **host\|hostv6** | IPv4 또는 IPv6 호스트를 설정합니다. |
| *Host* | 호스트의 이름 또는 인터넷 주소를 의미합니다. |
| **[vrf** *word***]** | (선택) VRF 를 바인딩합니다. |

| | |
|---|---|
| **[udp-port** *port-num***]** | (선택) 트랩을 전송하는 UDP 포트의 ID 를 지정합니다. |
| **[permit\|deny** *event-id***]** | (선택) 특정 이벤트 전송을 허용하거나 차단합니다. |
| **{version [v1\|v2c\|v3]}** | (선택) 트랩 전송에 사용되는 SNMP 프로토콜의 버전 ID 를 의미합니다. |
| **[informs \| traps]** | (선택) 버전 v2c 에서 트랩 유형을 지정합니다.<br>Informs: 트랩 유형이 "informs"입니다.<br>Traps: 트랩 유형이 "traps"입니다. |
| **[auth \|noauth]** | 버전 v3 에서 트랩 인증 모드를 지정합니다.<br>auth: 인증 필요<br>noauth: 인증 없음 |
| *community-string/user* | 버전 1 및 2c 에서 트랩 작업과 함께 전송되는 암호와 유사한 커뮤니티 문자열을 의미하며, 버전 3 에서는 사용자 이름을 의미합니다. |
| **[authentication \| configure\| snmp]** | 특정 트랩이 지정되지 않은 경우, 생성된 모든 트랩이 호스트로 전송됩니다.<br>**authentication** 인증 오류 트랩 전송을 허용합니다.<br>**configure** SNMP 설정 관련 트랩 전송을 허용합니다.<br>**snmp** SNMP 트랩 전송을 허용합니다. |

**(1) 기본값**

이 명령은 기본적으로 비활성화되어 있으며, 기본 설정에서는 트랩이 전송되지 않습니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 트랩 수신자를 지정하려면 전역 설정 모드에서 다음 첫 번째 명령을 실행하십시오. 지정된 호스트를 취소하려면 두 번째 명령을 실행하십시오.

**snmp-server host|hostv6** host [**vrf** word] [**udp-port** port-num] [**permit|deny** event-id] {{version **[v1 | v2c | v3]**} | **{[informs | traps]** | **[auth |noauth]**}} community-string/user **[authentication | configure| snmp]**

**no snmp-server host** *host community-string*

**(4) 예제**

다음은 SNMP 트랩을 특정 호스트로 전송하는 예제입니다.

1. RFC1157 에서 정의한 SNMP 트랩을 호스트 10.20.30.40 으로 전송하는 경우 커뮤니티 문자열을 comaccess 로 설정하고 SNMP 트랩을 전송합니다.

   snmp-server host 10.20.30.40 comaccess snmp

2. 스위치가 public 커뮤니티 문자열을 사용하여 모든 유형의 트랩을 호스트 10.20.30.40 으로 전송하는 경우

   snmp-server host 10.20.30.40 public

3. 오직 인증 트랩(authentication traps)만 활성화하여 호스트 bob 으로 전송하는 경우

   snmp-server host bob public authentication

**(5) 관련 명령어**

snmp-server queue-length
snmp-server trap-source
snmp-server trap-timeout
snmp-server event-id
snmp-server user

### 6.2.7. snmp-server location

시스템 그룹 내의 MIB 변수인 'sysLocation'에 해당합니다.

| 매개변수 | 설명 |
|---|---|
| *text* | 노드의 위치 정보를 나타내는 문자열 |

**(1) 기본값**

위치 문자열이 기본적으로 설정되지 않음.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

노드의 위치 문자열을 설정하려면 다음 첫 번째 명령을 실행하십시오. 기존 설정을 취소하려면 두 번째 명령을 실행하십시오.

**snmp-server location text**
**no snmp-server location**

**(4) 예제**

스위치의 실제 위치를 "Building_3/Room_214"로 설정하는 명령.
snmp-server location Building_3/Room_214

**(5) 관련 명령어**

snmp-server contact

### 6.2.8. snmp-server packetsize

이 명령은 SNMP 패킷의 최대 크기를 설정합니다.

| 매개변수 | 설명 |
|---|---|
| *byte-count* | **byte-count**: 484 에서 17940 사이의 정수 바이트를 나타냅니다. 기본값은 **3000 바이트**입니다. |

**(1) 기본값**

3000 바이트

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 서버가 요청을 수신하거나 응답을 보낼 때 최대 패킷 크기를 정의하려면 다음 명령을 실행하십시오.

**snmp-server packetsize** *byte-count*
**no snmp-server packetsize**

**(4) 예제**

최대 패킷 크기를 1024 바이트로 설정.

**snmp-server packetsize** 1024

**(5) 관련 명령어**

snmp-server queue-length

### 6.2.9. snmp-server queue-length

이 명령은 각 트랩 호스트의 대기열 길이를 설정하는 데 사용됩니다. 트랩 메시지가 성공적으로 전송되면 스위치는 대기열을 비웁니다.

| 매개변수 | 설명 |
|---|---|
| *Length* | 저장할 수 있는 트랩 이벤트의 개수를 나타내며, 범위는 **1~1000** 입니다. |

**(1) 기본값**

10 트랩 이벤트

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

각 트랩 호스트의 대기열 길이를 설정하려면 다음 명령을 실행하십시오.

**snmp-server queue-length** *length*
**no snmp-server queue-length**

**(4) 예제**

다음 예제는 네 개의 이벤트를 저장할 수 있는 메시지 대기열을 설정하는 방법을 보여줍니다.

snmp-server queue-length 4

**(5) 관련 명령어**

snmp-server packetsize

### 6.2.10. snmp-server trap-source

SNMP 서버가 SNMP 트랩을 전송할 때, 해당 트랩에는 트랩 주소가 포함됩니다.
트랩 주소를 추적하는 데 사용하려면 이 명령을 사용할 수 있습니다.

| 매개변수 | 설명 |
|---|---|
| *Interface* | SNMP 트랩이 생성되는 인터페이스를 나타냅니다.<br>이 매개변수에는 특정 플랫폼의 구문 모드에 따른 인터페이스 유형과 인터페이스 ID 가 포함됩니다. |

**(1) 기본값**

인터페이스 미지정.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

트랩의 소스 주소로 사용할 인터페이스를 지정하려면 전역 설정 모드에서 다음 첫 번째 명령을 실행하십시오. 이 인터페이스 지정을 취소하려면 두 번째 명령을 실행하십시오.

**snmp-server trap-source** *interface*
**no snmp-server trap-source**

**(4) 예제**

다음 예제는 모든 트랩의 소스 주소로 인터페이스 vlan1 을 지정하는 방법을 보여줍니다.

snmp-server trap-source vlan1

**(5) 관련 명령어**

snmp-server queue-length
snmp-server host

### 6.2.11. snmp-server trap-timeout

스위치 소프트웨어가 트랩을 전송하기 전에 대상 주소의 경로를 검색합니다. 경로가 없으면 트랩은 재전송 대기열에 저장됩니다.

이 명령은 트랩의 재전송 간격을 결정합니다.

| 매개변수 | 설명 |
|---|---|
| *seconds* | 트랩 재전송 간격(단위: 초). 범위: 1~1000 초 |

**(1) 기본값**

30 초

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 트랩 재전송의 타임아웃 값을 설정하려면 다음 명령을 실행합니다.

**snmp-server trap-timeout** seconds
**no snmp-server trap-timeout**

**(4) 예제**

다음 예제는 재전송 간격을 20 초로 설정하는 방법을 보여줍니다:
snmp-server trap-timeout 20

**(5) 관련 명령어**

snmp-server host
snmp-server queue-length

### 6.2.12. snmp-server user

이 명령은 SNMP 사용자 이름과 비밀번호를 설정하는 데 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *Username* | 생성하거나 수정할 SNMP 사용자의 이름 |
| *Groupname* | 사용자가 속한 그룹 이름 |
| **v3** | 사용되는 SNMP 프로토콜의 버전을 나타냅니다. |

| | |
|---|---|
| **[ encrypted \| auth ]** | **Encryption Type**:<br>**Encrypted**: 패킷 암호화<br>**auth**: 패킷 인증 |
| **[ md5 \| sha ]** | 암호화 인증 방법을 나타냅니다. |
| *auth-password* | 사용자의 인증 비밀번호를 나타냅니다.<br>이 비밀번호가 로컬화될 경우, SNMPv3 의 인증 키 및 암호화 키로 사용됩니다 |

**(1) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(2) 구문**

SNMP 사용자를 생성하거나 업데이트하려면 전역 설정 모드에서 다음 명령어를 실행하십시오. SNMP 사용자를 삭제하려면 두 번째 명령어를 실행하십시오. 원격(remote) 매개변수를 지정하면 원격 사용자가 설정됩니다. 원격 사용자가 설정될 경우, 해당 관리 스테이션의 IP 주소에 해당하는 SNMP 엔진 ID 가 반드시 존재해야 합니다. 명령어 형식은 아래와 같습니다.

**snmp-server user** *username groupname* **{ v3 [ encrypted | auth ] [ md5 | sha ]** *auth-password*}

**(3) 예제**

다음 예제는 SNMP 사용자 set-user 를 생성하는 방법을 보여줍니다.

- 사용자 이름: set-user
- 그룹: setter
- SNMP 프로토콜 버전: 3
- 보안 수준: 인증 및 암호화 (authentication and encryption)
- 비밀번호: 12345678
- 해시 알고리즘: MD5.

snmp-server user set-user setter v3 encrypted auth md5 12345678

**(4) 관련 명령어**

snmp-server view
snmp-server group

### 6.2.13. snmp-server view

다른 SNMP 명령에서 뷰를 매개변수로 필요로 하는 경우, 이 명령을 사용하여 뷰를 생성할 수 있습니다. 기본적으로 뷰를 정의할 필요가 없으며, 모든 뷰를 볼 수 있습니다. 이는 Cisco 에서 사전 정의한 "everything" 뷰와 동일합니다.

| 매개변수 | 설명 |
|---|---|
| *view-name* | 뷰의 레이블을 업데이트하거나 생성합니다. |
| *oid-tree* | ASN.1 서브트리의 개체 ID(Object ID)를 나타내며, 뷰에 포함되거나 제외되어야 합니다. 식별자 서브트리는 숫자로 구성된 문자열(예: 1.3.6.2.4) 또는 시스템 서브트리를 지정하는 데 사용됩니다. 서브트리 이름은 모든 MIB 트리에서 확인할 수 있습니다. |
| **included \| excluded** | 뷰 유형을 나타냅니다. "included"(포함) 또는 "excluded"(제외) 매개변수를 지정해야 합니다. |

**(1) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(2) 구문**

MIB 뷰를 생성하거나 업데이트하려면 다음 두 개의 명령어 중 첫 번째 명령어를 전역 설정 모드에서 실행하십시오.

SNMP 서버에서 뷰를 삭제하려면 두 번째 명령어를 실행하십시오.

**snmp-server** *view view-name oid-tree* **{included | excluded}**
**no snmp-server view** *view-name*

**(3) 예제**

MIB-II 서브트리의 모든 객체를 포함하는 뷰 생성:
snmp-server view mib2 mib-2 included

시스템 그룹을 포함하는 뷰 생성:
snmp-server view phred system included

시스템 그룹을 포함하지만 system.7 및 인터페이스 1 을 제외하는 뷰 생성:
snmp-server view agon system included
snmp-server view agon system.7 excluded

**(4) 관련 명령어**

snmp-server community

### 6.2.14. snmp-server source-addr

SNMP 서버가 요청을 전송할 때 사용할 소스 주소를 지정할 수 있습니다.

| 매개변수 | 설명 |
|---|---|
| *a.b.c.d* | SNMP 요청 응답에 사용할 소스 주소 |

**(1) 기본값**

가장 가까운 라우팅 주소.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 요청에 대한 응답을 위한 소스 주소를 지정하려면 다음 명령을 실행합니다.

**snmp-server source-addr** *a.b.c.d*
**no snmp-server source-addr**

**(4) 예제**

IP 주소 1.2.3.4 를 모든 SNMP 패킷의 소스 주소로 지정.
snmp-server source-addr 1.2.3.4

### 6.2.15. snmp-server udp-port

기본적으로 SNMP 에이전트는 포트 162 에서 수신 대기.

| 매개변수 | 설명 |
|---|---|
| *udp-port* | SNMP 트랩이 전송될 대상 포트 ID (명령 포트 ID 는 사용할 수 없음) |

**(1) 기본값**

기본적으로 SNMP 에이전트는 포트 162 에서 수신 대기.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 에이전트가 패킷을 수신할 포트 번호를 지정하려면 다음 명령을 실행합니다.

**snmp-server udp-port** *portnum*
**no snmp-server udp-port**

**(4) 예제**

SNMP 에이전트가 포트 1234 에서 수신 대기하도록 설정.
snmp-server udp-port 1234

### 6.2.16. snmp-server encryption

이 명령은 SNMP 커뮤니티, SHA 암호화 비밀번호 및 MD5 암호화 비밀번호를 일반 텍스트로 표시하는 데 사용됩니다. 이를 통해 비밀번호의 보안이 보장됩니다.

**(1) 기본값**

기본 설정은 SNMP 커뮤니티, SHA 암호화 비밀번호 및 MD5 암호화 비밀번호를 일반 텍스트로 표시하는 것입니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 커뮤니티, SHA 암호화 비밀번호 및 MD5 암호화 비밀번호를 표시하려면 글로벌 모드에서 snmp-server encryption 명령을 실행합니다. 이 명령은 한 번만 실행되는 명령이며, 저장되거나 부정 명령어를 통해 취소될 수 없습니다.

**snmp-server encryption**

**(4) 예제**

다음 예제는 호스트 90.0.0.3 에 설정된 SNMP 커뮤니티, SHA 암호화 비밀번호 및 MD5 암호화 비밀번호를 일반 텍스트로 표시하는 방법을 보여줍니다.

snmp-server encryption

**(5) 관련 명령어**

snmp-server community
snmp-server user

### 6.2.17. snmp-server trap-add-hostname

**(1) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(2) 구문**

snmp-server trap-add-hostname
no snmp-server trap-add-hostname

### 6.2.18. Snmp-server trap-logs

**(1) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(2) 구문**

snmp-server trap-logs
no snmp-server trap-logs

### 6.2.19. snmp-server set-snmp-dos-max

이 명령은 SNMP 호스트가 장치의 커뮤니티를 무차별적으로 추측하는 것을 방지하여 장치의 불필요한 CPU 사용을 줄이는 데 사용됩니다.

**(1) 매개변수**

The retry times 은 5 분 내에 잘못된 커뮤니티 로그인 재시도 허용 횟수.

**(2) 기본값**

잘못된 커뮤니티 로그인 횟수에는 제한이 없습니다.

**(3) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(4) 구문**

SNMP 서버에서 5 분 내에 잘못된 커뮤니티 로그인 재시도 횟수를 설정하려면 다음 두 가지 명령 중 첫 번째를 실행합니다.

**snmp-server set-snmp-dos-max** *retry times*
**no snmp-server set-snmp-dos-max**

**(5) 예제**

다음 예제는 5 분 내에 최대 재시도 횟수를 10 으로 설정하는 방법을 보여줍니다:
Router_config# snmp-server set-snmp-dos-max 10

### 6.2.20. Snmp-server keep-alive

이 명령은 snmp-server host 명령과 함께 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *Times* | 하트비트 트랩 전송 간격 |

**(1) 기본값**

이 명령은 기본적으로 존재하지 않으며, 하트비트 트랩이 전송되지 않습니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

장치가 하트비트 트랩을 전송하는 간격을 설정하려면 글로벌 모드에서 다음 두 가지 명령 중 첫 번째를 실행합니다.

**snmp-server keep-alive** *times*
**no snmp-server keep-alive**

**(4) 예제**

다음 예제는 하트비트 트랩을 3 초마다 전송하도록 설정하는 방법을 보여줍니다.
snmp-server keep-alive 3

**(5) 관련 명령어**

snmp-server host
snmp-server hostv6

### 6.2.21. snmp-server necode

이 명령은 개인 SNMP MIB 변수 값과 대응됩니다.

| 매개변수 | 설명 |
|---|---|
| *text* | 관리 노드(고유 장치 ID)에 대한 정보 |

**(1) 기본값**

관리 노드는 설정되지 않습니다.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

관리 노드(고유 장치 ID)를 설정하려면 글로벌 모드에서 다음 두 가지 명령 중 첫 번째를 실행합니다.

**snmp-server necode** *text*
**no snmp-server necode**

**(4) 예제**

다음 예제는 관리 노드에 대한 정보를 설정하는 방법을 보여줍니다:
snmp-server necode Dial_System_Operator_at_beeper_#_27345

### 6.2.22. snmp-server event-id

이 명령어는 호스트 설정에서 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *number* | 이벤트 ID 의 고유 코드 |
| *oid* | 이벤트 ID 에 포함된 트랩 OID |

**(1) 기본값**

이벤트 목록이 설정되지 않음.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

이벤트 목록을 생성하고 설정하려면 글로벌 모드에서 다음 두 명령어 중 하나를 실행하십시오.

**snmp-server event-id** *number* **trap-oid** *oid*
**no snmp-server event-id** *number* [**trap-oid** *oid*]

**(4) 예제**

다음 예제는 트랩 OID 1.2.3.4.5 를 이벤트 ID 1 로 설정하는 방법을 보여줍니다:
snmp-server event-id 1 trap-oid 1.2.3.4.5

### 6.2.23. snmp-server getbulk-timeout

이 명령어는 GetBulk 요청의 최대 타임아웃 시간을 설정하는 데 사용됩니다.
설정된 시간 내에 모든 GetBulk 요청을 처리하지 못하면 기존 결과를 반환합니다.

| 매개변수 | 설명 |
|---|---|
| *Seconds* | GetBulk 요청을 처리하는 최대 타임아웃 시간 |

**(1) 기본값**

GetBulk 요청의 최대 타임아웃 시간이 설정되지 않음

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

GetBulk 요청의 최대 타임아웃 시간을 설정하려면 글로벌 모드에서 다음 두 명령어 중 하나를 실행하십시오.

**snmp-server getbulk-timeout** *seconds*
**no snmp-server getbulk-timeout**

**(4) 예제**

GetBulk 요청의 최대 타임아웃 시간을 설정하려면 글로벌 모드에서 다음 두 명령어 중 하나를 실행하십시오.

snmp-server getbulk-timeout seconds
no snmp-server getbulk-timeout

### 6.2.24. snmp-server getbulk-delay

SNMP 에이전트가 GetBulk 요청을 처리하는 동안 CPU 점유율이 높아지는 경우, getbulk-delay 를 설정해야 합니다.

| 매개변수 | 설명 |
|---|---|
| *Ticks* | GetBulk 요청을 처리할 때 CPU 간격을 설정 |

**(1) 기본값**
CPU 가 최대 부하 상태에서 GetBulk 요청을 처리할 때 CPU 간격이 적용되지 않음.

**(2) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(3) 구문**

SNMP 에이전트가 GetBulk 요청을 처리할 때 CPU 점유율이 너무 높아지는 것을 방지하려면 다음 두 명령어 중 하나를 실행하십시오.

**snmp-server getbulk-delay** *ticks*
**no snmp-server getbulk-delay**

**(4) 예제**

다음 예제는 getbulk-delay 를 1 로 설정하는 방법을 보여줍니다:
snmp-server getbulk-delay 1

### 6.2.25. show snmp

show snmp 명령어는 SNMP 출력 및 입력 통계를 나열하는 데 사용됩니다.

- show snmp engineID 명령어는 SNMP 엔진에 대한 정보를 표시하는 데 사용됩니다.
- show snmp host 명령어는 SNMP 트랩 호스트에 대한 정보를 표시하는 데 사용됩니다.
- show snmp view 명령어는 SNMP 뷰를 표시하는 데 사용됩니다.
- show snmp mibs 명령어는 MIB 등록 정보를 표시하는 데 사용됩니다.
- show snmp group 명령어는 SNMP 그룹을 표시하는 데 사용됩니다.
- show snmp user 명령어는 SNMP 사용자를 표시하는 데 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *engineID* | SNMP 엔진 정보를 표시 |
| *Host* | SNMP 트랩 호스트 정보를 표시 |
| *View* | SNMP 뷰 정보를 표시 |
| *Mibs* | SNMP MIB 등록 정보를 표시 |
| *Group* | SNMP 그룹 정보를 표시 |
| *User* | SNMP 사용자 정보를 표시 |

**(1) 명령어 모드**

EXEC 또는 전역 설정 모드

**(2) 구문**

SNMP 입력 및 출력을 모니터링하려면 show snmp 명령어를 실행하십시오.

- SNMP 엔진 정보를 표시하려면: show snmp engineID
- SNMP 트랩 호스트 정보를 표시하려면: show snmp host
- SNMP 뷰 정보를 표시하려면: show snmp view

- MIB 등록 정보를 표시하려면: show snmp mibs
- SNMP 그룹 정보를 표시하려면: show snmp group
- SNMP 사용자 정보를 표시하려면: show snmp user.

show snmp [engineID |host | view | mibs |group|user]

**(3) 예제**

다음 예제는 SNMP 패킷의 입출력 통계를 조회하는 방법을 보여줍니다.

Switch#show snmp
37 SNMP packets input
0 Bad SNMP version errors
4 Unknown community name
0 Illegal operation for community name supplied
0 Snmp encoding errors
24 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
28 Get-next PDUs
0 Set-request PDUs
78 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
24 Get-response PDUs PDUs
13 SNMP trap PDUs

다음 목록은 SNMP 에이전트가 전송 및 수신한 패킷에 대한 정보에서 각 도메인의 의미를 나타냅니다.

| 표시 정보 | 의미 |
|---|---|
| Unknown community name | 식별할 수 없는 커뮤니티 이름을 의미합니다. |
| Illegal operation for community name supplied | 불법적인 작업을 의미합니다. |
| Encoding errors | 잘못된 인코딩을 의미합니다. |
| Get-request PDUs | Get-Request 패킷을 의미합니다. |
| Get-next PDUs | Get-Next 패킷을 의미합니다. |
| Set-request PDUs | Set-Request 패킷을 의미합니다. |
| Too big errors | 관련 패킷이 너무 커서 응답할 수 없음을 의미합니다. |

| | |
|---|---|
| No such name errors | 지정된 인스턴스가 존재하지 않음을 의미합니다. |
| Bad values errors | 설정된 값의 유형이 잘못되었음을 의미합니다. |
| General errors | 일반적인 오류를 의미합니다. |
| Get-response PDUs | Get-Response 패킷을 의미합니다. |
| Trap PDUs | SNMP 트랩 패킷을 의미합니다. |

다음 예제는 SNMP 트랩 호스트를 표시하는 예제입니다.
Switch# show snmp host
Notification host: 192.2.2.1 udp-port: 162 type: trap
user: public security model: v1

다음 예제는 SNMP 뷰를 표시하는 예제입니다.
Switch# show snmp view
mib2 mib-2 - included permanent active

**(4) 관련 명령어**

snmp-server host
snmp-server view

### 6.2.26. debug snmp

SNMP 디버깅이 활성화되면 SNMP 이벤트, 패킷 송수신 및 오류가 표시되며, 이를 통해 SNMP 문제를 진단할 수 있습니다.

| 매개변수 | 설명 |
|---|---|
| *Error* | SNMP 이벤트 디버깅을 활성화합니다. |
| *Event* | SNMP 이벤트 디버깅을 활성화합니다. |
| *Packet* | SNMP 송수신 패킷 디버깅을 활성화합니다. |

**(1) 명령어 모드**

EXEC

**(2) 구문**

SNMP 이벤트, 패킷 송수신 및 패킷 오류를 표시하려면 다음 명령어를 실행합니다.
**debug snmp** [ *error* | *event* | *packet* ]
**no debug snmp** *[ error | event | packet* ]

**(3) 예제**

다음 예제는 SNMP 패킷을 디버깅하는 방법을 보여줍니다.

```
switch#debug snmp packet
Received 49 bytes from 192.168.0.29:1433
0000: 30 82 00 2D  02 01 00 04  06 70 75 62  6C 69 63 A0   0..-.....public.
0016: 82 00 1E 02  02 7D 01 02  01 00 02 01  00 30 82 00   .....}.......0..
0032: 10 30 82 00  0C 06 08 2B  06 01 02 01  01 03 00 05   .0.....+........
0048: 00                                                   .
Sending 52 bytes to 192.168.0.29:1433
0000: 30 82 00 30  02 01 00 04  06 70 75 62  6C 69 63 A2   0..0.....public.
0016: 82 00 21 02  02 7D 01 02  01 00 02 01  00 30 82 00   ..!..}.......0..
0032: 13 30 82 00  0F 06 08 2B  06 01 02 01  01 03 00 43   .0.....+.......C
0048: 03 00 F4 36                                          ...6
Received 51 bytes from 192.168.0.29:1434
0000: 30 82 00 2F  02 01 00 04  06 70 75 62  6C 69 63 A0   0../.....public.
0016: 82 00 20 02  02 6B 84 02  01 00 02 01  00 30 82 00   .. ..k.......0..
0032: 12 30 82 00  0E 06 0A 2B  06 01 02 01  02 02 01 02   .0.....+........
0048: 01 05 00                                             ...
Sending 62 bytes to 192.168.0.29:1434
0000: 30 82 00 3A  02 01 00 04  06 70 75 62  6C 69 63 A2   0..:.....public.
0016: 82 00 2B 02  02 6B 84 02  01 00 02 01  00 30 82 00   ..+..k.......0..
0032: 1D 30 82 00  19 06 0A 2B  06 01 02 01  02 02 01 02   .0.....+........
0048: 01 04 0B 45  74 68 65 72  6E 65 74 30  2F 31         ...Ethernet0/1
```

| **표시 정보** | **의미** |
|---|---|
| Received | **SNMP 수신 패킷** |
| 192.168.0.29 | **소스 IP 주소** |
| 1433 | **소스 주소의 포트 ID** |
| 51 bytes | **수신된 패킷의 길이** |
| 30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0<br>82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00<br>10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05<br>00 | **SNMP ASN 으로 인코딩된 패킷** |
| 0..-.....public.<br>.....}.......0..<br>.0.....+........<br>. | **패킷 수신의 ASCII 코드 표현**<br>(ASCII 코드 범위를 벗어난 문자는 "."으로 표시됨) |
| sending | **SNMP 전송 패킷** |

| | |
|---|---|
| 192.168.0.29 | **대상 IP 주소** |
| 1433 | **대상 주소의 포트 ID** |
| 52 bytes | **전송된 패킷의 길이** |
| 30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2<br>82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00<br>13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43<br>03 00 F4 36 | **SNMP ASN 으로 인코딩된 패킷** |
| 0..0.....public.<br>..!..}.....0..<br>.0.....+.....C<br>...6 | 패킷 수신의 ASCII 코드 표현<br>(ASCII 코드 범위를 벗어난<br>문자는 "."으로 표시됨) |

아래는 SNMP 이벤트 디버깅 예제 이다.

switch#debug snmp event
Received SNMP packet(s) from 192.2.2.51
SNMP: GETNEXT request
-- ip.ipReasmFails.0
SNMP: Response
〉〉 ip.ipFragOKs.0 = 1
Received SNMP packet(s) from 192.2.2.51

SNMP: GETNEXT request

-- ip.ipFragOKs.0

SNMP: Response

〉〉 ip.ipFragFails.0 = 0
Received SNMP packet(s) from 192.2.2.51

SNMP: GETNEXT request

-- ip.ipFragFails.0

SNMP: Response

〉〉 ip.ipFragCreates.0 = 2

| **표시 정보** | **의미** |
|---|---|
| SNMP | 현재 디버깅 중인 SNMP |

| | |
|---|---|
| GETNEXT request | SNMP GetNext 요청 |
| RESPONSE | SNMP 응답 |
| -- | 수신한 패킷 |
| 〉〉 | 전송한 패킷 |
| ip.ipReasmFails.0 | 요청된 MIB OID |
| ip.ipFragOKs.0 = 1 | MIB OID 와 반환값 |

## 6.3. RMON Configuration Commands

RMON 관련 명령어는 다음과 같습니다:

- rmon alarm
- rmon event
- show rmon

### 6.3.1. RMON alarm

#### (1) 구문

rmon alarm index variable interval {absolute | delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [repeat] [owner string]

RMON 알람 항목을 설정하려면 위 명령어를 실행합니다.

#### (2) 매개변수 (Parameter)

| 매개변수 (Parameter) | 설명 |
|---|---|
| index | 이벤트 항목의 인덱스 (1~65535) |
| *variable* | 모니터링할 대상 (테스트할 객체의 OID) |
| *interval* | 샘플링 주기 (1~2147483647 초) |
| *value* | 알람 임계값 (-2147483648 ~ 2147483647) |
| *eventnumber* | 임계값 초과 시 트리거되는 이벤트 인덱스 (1~65535) |
| *repeat* | 이벤트를 반복 트리거할지 여부 |
| *string* | 설정을 소유하는 사용자 설명 (1~31 자) |

#### (3) 기본값 (Default value)

Eventnumber 기본값이 아님.
repeat 기본값이 아님.

**(4) 사용지침 (Usage guidelines)**

이 명령어는 글로벌 모드에서 설정되며, 특정 객체의 값을 모니터링합니다. 만약 값이 임계값을 초과하면 해당 이벤트가 트리거됩니다.

**(5) 예제 (Example)**

다음 예제는 ifInOctets.2 객체를 모니터링하며, 샘플링 주기는 10 초입니다.
값이 15 를 초과하면 이벤트 1 이 트리거됨
값이 25 미만으로 떨어지면 이벤트 2 가 트리거됨.

rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1 falling-threshold 25 2 repeat owner switch

### 6.3.2. RMON collection stats

**(1) 구문 (Syntax)**

RMON 통계를 설정하려면 아래 명령어를 실행합니다.
rmon collection stats index [owner string]

**(2) 매개변수 (Parameter)**

| 매개변수 (Parameter) | 설명 |
|---|---|
| *index* | 통계 항목의 인덱스를 나타냅니다. 값 범위: 1~65535. |
| *string* | 소유자 문자열을 나타냅니다. 값 범위: 문자열 길이는 1~31. |

**(3) 기본값 (Default value)**

None

**(4) 사용 지침 (Usage guidelines)**

이 명령어는 인터페이스 모드에서 설정해야 합니다.

**(5) 예제 (Example)**

다음 예제는 기가비트 이더넷 g0/1 인터페이스에서 RMON 통계를 활성화하는 방법을 보여줍니다.

int g0/1
rmon collection stats 2 owner switch

### 6.3.3. RMON collection history

#### (1) 구문

RMON 히스토리 컨트롤 항목을 설정하려면 아래 명령어를 실행합니다.

**rmon collection history** *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]

#### (2) 매개변수 (Parameter)

| 매개변수 (Parameter) | 설명 |
|---|---|
| *index* | 인덱스를 나타냅니다. 값 범위: 1~65535. |
| *bucket-number* | 가 가장 가까운 bucket-number 의 모든 히스토리 기록 제어 항목을 보존해야 합니다. 값 범위: 1~65535. |
| *second* | 시간 간격을 나타냅니다. 값 범위: 1~3600. |
| *owner-name* | 소유자 문자열을 나타냅니다. 값 범위: 문자열 길이는 1~31. |

#### (3) 기본값 (Default value)

bucket-number: 50 , second: 1800 (30 분).

#### (4) 사용 지침 (Usage guidelines)

이 명령어는 인터페이스 모드에서 설정해야 합니다. 히스토리 제어 테이블에 하나의 항목을 추가하는 데 사용됩니다.

#### (5) 예제 (Example)

다음 예제는 기가비트 이더넷 g0/1 에서 10 초마다 샘플링하여 최근 20 개의 기록을 저장하는 방법을 보여줍니다.(각 시간 간격은 10 초)
int g0/1
rmon collection history 2 buckets 20 interval 10 owner switch

### 6.3.4. RMON event

**(1) 구문**

**rmon event** index [description des-string] [log] [owner owner-string] [trap community] [ifctrl interface]

위 명령어를 실행하면 RMON 이벤트 항목을 설정할 수 있습니다.

**(2) 매개변수 (Parameter)**

| 매개변수 (Parameter) | 설명 |
|---|---|
| *index* | 이벤트 항목의 인덱스 (1~65535) |
| *des-string* | 이벤트 설명 문자열 (1~127 자) |
| *owner-string* | 이벤트 소유자 문자열 (1~31 자) |
| *community* | 트랩(Trap) 생성 시 사용될 커뮤니티 이름 (1~31 자) |
| interface | 이벤트 발생 시 제어할 종료된 포트 |

**(3) 기본값 (Default value)**

None

**(4) 사용 지침 (Usage guidelines)**

이 명령어는 알람을 사용하는 RMON 이벤트 항목을 설정하는 데 사용됩니다.

**(5) 예제 (Example)**

다음 예제는 RMON 이벤트를 설정하는 방법을 보여줍니다.

- 이벤트 인덱스: 6
- 설명 문자열: "example"
- 이벤트 트리거 시: 로그 리스트에 기록됨
- 트랩 생성 시: 커뮤니티 이름이 "public" 인 트랩이 전송됨.

rmon event 6 log trap public description example owner switch

### 6.3.5. show RMON

**(1) 구문**

show rmon [alarm] [event] [statistics] [history]
위 명령어를 실행하면 현재 RMON 설정을 확인할 수 있습니다.

**(2) 매개변수 (Parameter)**

None

**(3) 기본값 (Default value)**

None

**(4) 사용 지침 (Usage guidelines)**

이 명령어는 현재 설정된 RMON 항목을 확인하는 데 사용됩니다.

**(5) 예제 (Example)**

다음 예제는 현재 설정된 RMON 설정을 표시하는 방법을 보여줍니다.
show rmon

# 7. MAC Access List 설정 명령

## 7.1. MAC Access List Configuration Commands

- mac access-list
- permit
- deny
- mac access-group

### 7.1.1. mac access-list

#### (1) 구문

MAC 액세스 리스트를 추가하려면 mac access-list 명령어를 사용합니다.
MAC 액세스 리스트를 삭제하려면 no mac access-list 명령어를 사용합니다.

[no] **mac access-list** *name*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *name* | MAC 액세스 리스트의 이름. |

#### (3) 기본값

없음

#### (4) 명령어 모드

전역 설정

#### (5) 예제

다음 예제는 "mac-acl"이라는 MAC 액세스 리스트를 생성하는 명령입니다:
Switch-config_# mac access-list mac-acl
Switch-config-macl#

### 7.1.2. permit

**(1) 구문**

MAC 액세스 리스트에 허용(permit) 항목을 추가하려면 permit 명령어를 사용합니다. 허용 항목을 삭제하려면 no permit 명령어를 사용합니다.

**[no] permit {any** | **host** *src-mac-addr* | *src-mac-addr src-mac-addr-mask*} {**any | host** *dst-mac-addr* | *dst-mac-addr dst-mac-addr-mask } [ethertype*]

**(2) 매개변수**

| 매개변수 | 설명 | 값 범위 |
|---|---|---|
| any | 모든 값 허용 | - |
| host | 단일 호스트 | - |
| src-mac-addr | 소스 MAC 주소 | H.H.H |
| src-mac-addr-mask | 소스 MAC 주소 마스크 | H.H.H |
| dst-mac-addr | 목적지 MAC 주소 | H.H.H |
| dst-mac-addr-mask | 목적지 MAC 주소 마스크 | H.H.H |
| ethertype | 매칭되는 이더넷 데이터 패킷 유형 | 0-0xFFFF |

**(3) 기본값**

설정된 항목이 없으면 명령어가 비활성화됨
하나의 항목이 설정되고 permit any any 가 포함되지 않으면 자동으로 deny any any 가 추가되어 모든 트래픽이 차단됨.

**(4) 명령어 모드**

MAC 액세스 리스트 설정 모드

**(5) 예제**

다음 예제는 소스 MAC 주소가 5491.af78.abcd 인 호스트를 허용하는 설정입니다:
Switch-config-macl#permit host 5491.af78.abcd any 0x806

### 7.1.3. deny

**(1) 구문**

MAC 액세스 리스트에 차단(deny) 항목을 추가하려면 deny 명령어를 사용합니다.

차단 항목을 삭제하려면 no deny 명령어를 사용합니다.
**[no] deny {any | host** *src-mac-addr* / *src-mac-addr src-mac-addr-mask*}
{**any | host** *dst-mac-addr* / *dst-mac-addr dst-mac-addr-mask*} [*ethertype*]

**(2) 매개변수**

| 매개변수 | 설명 | 값 범위 |
|---|---|---|
| any | 모든 값 허용 | - |
| host | 단일 호스트 | - |
| src-mac-addr | 소스 MAC 주소 | H.H.H |
| src-mac-addr-mask | 소스 MAC 주소 마스크 | H.H.H |
| dst-mac-addr | 목적지 MAC 주소 | H.H.H |
| dst-mac-addr-mask | 목적지 MAC 주소 마스크 | H.H.H |
| ethertype | 매칭되는 이더넷 데이터 패킷 유형 | 0-0xFFFF |

**(3) 기본값**

설정된 항목이 없으면 명령어가 비활성화됨
하나의 항목이 설정되고 permit any any 가 포함되지 않으면 자동으로 deny any any 가 추가되어 모든 트래픽이 차단됨.

**(4) 명령어 모드**

MAC 액세스 리스트 설정 모드

**(5) 예제**

다음 예제는 소스 MAC 주소가 5491.af78.abcd 인 호스트를 차단하는 설정입니다:
Switch-config-macl#deny host 5491.af78.abcd any 0x806

### 7.1.4. mac access-group

**(1) 구문**

전역 설정 모드에서 설정된 MAC 액세스 리스트를 적용하려면 mac access-group 명령어를 사용합니다. MAC 액세스 리스트를 삭제하려면 no mac access-group 명령어를 사용합니다.

**[no] mac access-group** *name*

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *name* | MAC 액세스 리스트의 이름 |

**(3) 기본값**

적용된 MAC 액세스 리스트 없음.

**(4) 명령어 모드**

PON 포트 또는 업링크 인터페이스 설정 모드

**(5) 예제**

다음 예제는 macacl 이라는 MAC 액세스 리스트를 g0/1 인터페이스에 적용하는 명령입니다:
Switch_config_g0/1#mac access-group macacl

# 8. SSH

## 8.1. 개요

### 8.1.1. SSH 서버

스위치는 SSH 서버기능을 제공하며 SSH 클라이언트와 장치간 보안 및 암호화된 통신 연결을 생성할 수 있습니다. SSH 연결에는 텔넷과 유사한 원격접속 기능이 있습니다. SSH 서버는 암호화 알고리즘을 지원합니다. (자세한 사항은 보안기능 설명서 참조)

### 8.1.2. 클라이언트

SSH 클라이언트는 SSH 프로토콜로 통신하는 응용 프로그램입니다. SSH 클라이언트는 인증 및 암호화를 제공할 수 있으므로 SSH 클라이언트는 안전하지 않은 네트워크 조건에서 실행되는 장치라도 SSH 서버를 지원하는 통신 장치 또는 장치간의 통신을 보호합니다. SSH 클라이언트는 암호화 알고리즘을 지원합니다.

### 8.1.3. 기능

SSH 서버 및 SSH 클라이언트는 버전 2.0 을 지원합니다.

## 8.2. 구성 작업

### 8.2.1. 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 방법의 목록을 구성합니다. |

### 8.2.2. ACL 구성하기

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

| 명령어 | 설명 |
|---|---|
| ip sshd access-class STRING | ACL 을 구성합니다. |

### 8.2.3. 인증 시간 초과 값 구성

클라이언트와 서버간에 연결이 구성된 후 구성된 시간 내에 인증을 승인할 수 없으면 서버는 연결을 끊습니다. 글로벌 구성 모드에서 다음 명령을 통해 구성 시간 초과 값을 구성합니다.

| 명령어 | 설명 |
|---|---|
| ip sshd timeout 〈60-65535〉 | 인증 시간 초과 값을 구성 |

### 8.2.4. 인증 재시도 횟수 구성

실패한 인증에 대한 시간이 최대 시간을 초과하면 SSH 서버는 새 연결이 구성되지 않는 한 인증을 재시도 하지 않습니다. 최대 재시도 횟수는 기본적으로 3 입니다. 글로벌 모드에서 다음 명령어를 실행하여 인증을 다시 시도하는 최대 횟수를 구성하십시오:

| 명령어 | 설명 |
|---|---|
| ip sshd auth-retries 〈0-65535〉 | Configures the maximum times for retrying authentication. |

### 8.2.5. SSH 서버 활성화

SSH 서버는 기본적으로 비활성화 되어 있습니다. SSH 서버가 활성화되면 장치는 rsa 암호를 쌍으로 생성한 다음 클라이언트의 연결 요청을 수신합니다. 과정은 1~2 분 정도 소요됩니다. 글로벌 구성 모드에서 다음 명령어를 실행하여 SSH 서버를 활성화합니다.

| 명령어 | 설명 |
|---|---|
| ip sshd enable | SSH 서버를 사용합니다. 암호는 2048bit 로 생성됩니다. |

### 8.2.6. SSH 버전 구성

SSH 버전을 구성합니다.

| 명령어 | 설명 |
|---|---|
| ip sshd version 2 | SSH 는 기본 값으로 버전 2 만 지원합니다. |

### 8.2.7. SSH 키 저장

SSH 활성화후 생성된 키를 플래시 메모리에 저장하기 위해 다음 명령어를 실행합니다.

| 명령어 | 설명 |
|---|---|
| ip sshd save | SSH 키를 플래시 메모리에 파일로 저장합니다. |

#### 8.2.8. SFTP 활성화

SSH 활성화후 SFTP 를 활성화하기 위해 다음 명령어를 실행합니다.

| 명령어 | 설명 |
|---|---|
| ip sshd sftp | SFTP 기능을 활성화합니다. |

## 8.3. SSH 동시 접속 세션 제한

| 명령어 | 설명 |
|---|---|
| Max-lines ssh 〈0-31〉 | SSH 동시 접속 세션을 제한하도록 설정한다.<br>동시 접속 제한: 0~31 (기본값: 0) |
| no max-lines SSH | SSH 동시 접속 세션 설정을 취소한다. |

## 8.4. SSH 서버 구성 예제

다음 구성에서는 IP 주소가 192.168.20.40 인 host 만 SSH 서버에 접속할 수 있습니다. 로컬 사용자 데이터베이스는 사용자 ID 를 구별하는 데 사용됩니다.

Access control list (ACL)

```
ip access-list standard ssh-acl permit 192.168.20.40
!
aaa authentication login ssh-auth local
ip sshd auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```

## 8.5. SSH 클라이언트 기능 사용

SSH 클라이언트 기능을 사용하려면 아래 명령을 참조하십시오.

| 명령어 | 설명 |
|---|---|
| ssh -l userid -d ip_address | 옵션에 주어진 계정과 IPv4 목적지(A.B.C.D)로 ssh 접속을 시작합니다. |
| ssh -l userid -ipv6 ip_address | 옵션에 주어진 계정과 IPv6 목적지(X:X:X:X::X)로 ssh 접속을 시작합니다. |

# 9. Telnet 구성

## 9.1. Telnet 서비스 구성

| 명령어 | 설명 |
|---|---|
| ip telnet enable | Telnet 를 사용할 수 있도록 활성화 |
| ip telnet sour-interface vlan *⟨interface-id⟩* | ip telnet sour-interface vlan |
| ip telnet listen-port ⟨3001-3999⟩ | Telnet 포트를 변경. (기본값: 23) |
| Ip telnet max-user ⟨0-31⟩ | 최대 Telnet 사용자 수 지정 |
| no ip telnet enable | Telnet 를 사용할 수 없도록 비활성화 |

## 9.2. Telnet 서비스 인증 실패 대응 구성

| 명령어 | 설명 |
|---|---|
| ip telnet attack-defense ⟨count num: 3-10⟩ ⟨time num: 30-86400s⟩ | 접속 횟수 제한 및 재 접속 대기시간을 구성.<br>접속 횟수 제한: 3~10 회<br>재 접속 대기 시간: 30~86400 초. |
| no ip telnet attack-defense | 접속횟수 및 재접속 대기시간 구성 삭제 |

## 9.3. Telnet 동시 접속 세션 제한

| 명령어 | 설명 |
|---|---|
| max-lines telnet ⟨0-31⟩ | Telnet 동시 접속 세션을 제한하도록 설정한다.<br>동시 접속 제한: 0~31 (기본값: 0) |
| no max-lines telnet | Telnet 동시 접속 세션 설정을 취소한다. |

## 9.4. 관리자 접근 제어 ACL 적용

Telnet 서버에 대한 접근을 제어하려면 전역설정모드에서 표준 ACL 을 구성하고 아래 명령으로 Telnet 서비스에 적용합니다.

| 명령어 | 설명 |
|---|---|
| ip telnet access-class 〈acl_name〉 | 관리자 접근제어 ACL 을 Telnet 서비스에 적용합니다. |

## 9.5. Telnet 접속자 확인

| 명령어 | 설명 |
|---|---|
| show telnet | Telnet 접속자 정보를 표시한다. 접속 IP, TCP 포트정보 |
| show tcp brief | TCP 접속 세션 정보를 표시한다. |

# 10. 인증(AAA) 구성

## 10.1. AAA 개요

### 10.1.1. AAA 보안 서비스

AAA 는 세 가지 독립적인 보안 기능을 일관된 방식으로 구성하기위한 기술적인 프레임 워크입니다. AAA 는 다음 서비스를 수행하는 모듈 방식을 제공합니다.

- Authentication - 로그인 및 암호 대화 상자, 요청 및 응답, 메시징 지원 및 선택한 보안 프로토콜에 따라 암호화를 비롯한 사용자 식별 방법을 제공합니다.

Authentication 은 네트워크 및 서비스에 대한 접근이 허용되기 전에 사용자가 식별되는 방식입니다. 명명된 인증 방법 목록을 정의한 다음 해당 목록을 다양한 인터페이스에 적용하여 AAA 인증을 구성합니다. 메소드 목록은 수행할 인증 유형 및 수행할 인증 순서를 정의합니다. 정의된 인증 메소드가 수행되기 전에 특정 인터페이스에 적용되어야 합니다. 예외는 기본 메소드 목록 ("default"라는 이름)입니다. 기본 메소드 목록은 다른 메소드 목록이 정의되지 않은 경우 모든 인터페이스에 자동으로 적용됩니다. 정의된 메소드 목록이 기본 메소드 목록을 중복 사용합니다. 로컬, 회선 암호 및 사용 가능 인증을 제외한 모든 인증 방법은 AAA 를 통해 정의해야합니다. AAA 보안 서비스 외부에서 구현되는 방법을 포함하여 모든 인증 방법 구성에 대한 자세한 내용은 "인증 구성"장을 참조하십시오.

- Authorization — 각 서비스, 사용자 별 계정 목록 및 프로필, 사용자 그룹 지원, IP, IPX, ARA 및 Telnet 지원에 대한 일회성 권한 부여 또는 권한 부여를 비롯하여 원격 접근 제어 방법을 제공합니다.

AAA 권한 부여는 사용자의 수행 권한이 무엇인지 설명하는 일련의 속성을 조합하여 적용합니다. 이러한 속성은 주어진 사용자에 대한 데이터베이스에 포함된 정보와 비교되며 결과는 사용자의 실제 기능 및 제한 사항을 결정하기 위해 AAA 로 반환됩니다. 데이터베이스를 액세스 서버 또는 라우터에 로컬로 배치하거나 RADIUS 또는 TACACS + 보안 서버에서 원격으로 호스팅 할 수 있습니다. RADIUS 및 TACACS +와 같은 원격 보안 서버는 해당 권한을 해당 사용자와 정의하는 AV (Attribute-Value) 쌍을 연결하여 특정 권한을 사용자에게 부여합니다. 모든 인증 방법은 AAA 를 통해 정의해야합니다.

- Accounting— 사용자 ID, 시작 및 정지시간, 실행된 명령 (예: PPP), 패킷 수 및 바이트 수와 같이 요청, 감시 및 보고에 사용되는 보안 서버 정보를 수집하고 보내는 방법을 제공합니다.

계정을 사용하면 사용자가 액세스하는 서비스는 물론 사용중인 네트워크 리소스의 양을 추적할 수 있습니다. AAA 계정이 활성화되면 네트워크 접근 서버는 계정 활동의 형태로 사용자 활동을 RADIUS 또는 TACACS + 보안 서버 (구현한 보안 방법에 따라 다름)에보고합니다. 각 계정

레코드는 계정 AV 쌍으로 구성되며 접근 제어 서버에 저장됩니다. 이 데이터는 네트워크 관리, 클라이언트 청구 및 / 또는 감사를 위해 분석 될 수 있습니다. 모든 Accounting 방법은 AAA 를 통해 정의되어야합니다. 인증 및 권한 부여와 마찬가지로 AAA 계정을 명명된 계정 방법 목록을 정의한 다음 다양한 인터페이스에 적용하여 AAA 계정을 구성합니다. AAA 를 사용하여 계정을 구성하는 방법에 대한 자세한 내용은 "계정 구성"장을 참조하십시오.

## 10.2. AAA 사용 이점

- 구성의 유연한 접근 및 제어 향상
- 확장성
- RADIUS, TACACS+, Kerberos 와 같은 표준화된 인증방법
- 다중 백업 시스템

### 10.2.1. AAA 원리

AAA 는 라인 단위 (사용자 별) 또는 서비스 별 (예: IP, IPX 또는 VPDN) 단위로 원하는 유형의 인증 및 권한 부여를 동적으로 구성할 수 있도록 설계되었습니다. 메소드 목록을 작성한 다음 특정 메소드 또는 인터페이스에 해당 메소드 목록을 적용하여 원하는 인증 및 권한 유형을 정의합니다.

## 10.3. 메소드 목록

메소드 목록은 사용자를 인증하는 데 사용되는 인증 방법을 정의하는 순차적 목록입니다. 메서드 목록을 사용하면 인증에 사용할 보안 프로토콜을 하나 이상 지정할 수 있으므로 초기 메소드가 실패할 경우를 대비하여 인증을 위한 백업 시스템을 보장할 수 있습니다. Cisco IOS 소프트웨어는 나열된 첫 번째 방법을 사용하여 사용자를 인증합니다. 해당 방법이 응답하지 않으면 Cisco IOS 소프트웨어는 메소드 목록에서 다음 인증 방법을 선택합니다. 이 프로세스는 나열된 인증 방법과의 성공적인 통신이 있거나 인증 방법 목록이 모두 소모될 때까지 계속됩니다. 이 경우 인증이 실패합니다.
소프트웨어는 이전 메소드의 응답이 없는 경우에만 다음 나열된 인증 방법으로 인증을 시도합니다. 이 주기의 어느 시점에서든 인증이 실패하면 (즉, 보안 서버 또는 로컬 사용자 이름 데이터베이스가 사용자 액세스를 거부하여 응답함) 인증 프로세스가 중지되고 다른 인증 방법이 시도되지 않습니다. 다음 그림은 4 개의 보안 서버를 포함하는 일반적인 AAA 네트워크 구성을 보여줍니다. R1 과 R2 는 RADIUS 서버이고 T1 과 T2 는 TACACS + 서버입니다.

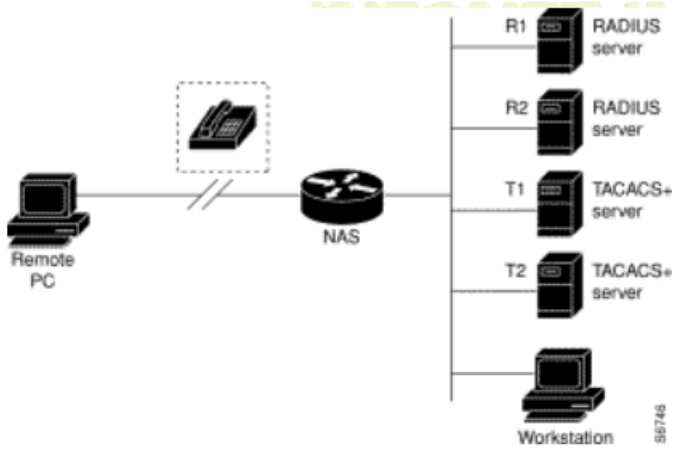



그림 0-1 전형적인 AAA 네트워크 구성

시스템 관리자가 먼저 R1 이 인증 정보, 그 다음 R2, T1, T2 및 마지막으로 액세스 서버 자체의 로컬 사용자 이름 데이터베이스에 연결되는 방법 목록을 정의했다고 가정합니다. 원격 사용자가 네트워크에 전화 접속을 시도하면 네트워크 액세스 서버는 먼저 R1 에 인증 정보를 쿼리합니다. R1 이 사용자를 인증하면 네트워크 액세스 서버에 PASS 응답을 보내고 사용자는 네트워크에 액세스 할 수 있습니다. R1 이 FAIL 응답을 반환하면 사용자의 액세스가 거부되고 세션이 종료됩니다. R1 이 응답하지 않으면 네트워크 액세스 서버는 이를 오류로 처리하고 R2 에 인증 정보를 질문합니다. 이 패턴은 사용자가 인증되거나 거부될 때까지 또는 세션이 종료될 때까지 나머지 지정된 메소드를 통해 계속됩니다. 모든 인증 방법이 오류를 반환하면 네트워크 액세스 서버가 세션을 오류로 처리하고 세션이 종료됩니다.

FAIL 응답은 ERROR 와 다릅니다. FAIL 은 사용자가 해당 인증 데이터베이스에 포함된 기준을 충족하지 못했음을 의미합니다. 인증은 FAIL 응답으로 끝납니다. ERROR 는 보안 서버가 인증 쿼리에 응답하지 않았음을 의미합니다. 이 때문에 인증이 시도되지 않았습니다. ERROR 가 탐지된 경우에만 AAA 는 인증 방법 목록에 정의된 다음 인증 방법을 선택합니다.

## 10.4. AAA 구성 과정

먼저 어떤 종류의 보안 솔루션을 구현할지 결정해야합니다. 특정 네트워크에서 보안 위험을 평가하고 권한이 없는 진입 및 공격을 방지할 수있는 적절한 방법을 결정해야합니다.

### 10.4.1. 구성 과정 개요

AAA 구성은 관련된 기본 프로세스를 이해하면 비교적 간단합니다. AAA 를 사용하여 Cisco 라우터 또는 연동 서버에서 보안을 구성하려면이 프로세스를 따르십시오:

- 별도의 보안 서버를 사용하려면 RADIUS, TACACS + 또는 Kerberos 와 같은 보안 프로토콜 매개 변수를 구성하십시오.
- AAA 인증 명령을 사용하여 인증을위한 메소드 목록을 정의하십시오.

- 필요한 경우 특정 인터페이스 나 회선에 메소드 목록을 적용하십시오.
- (선택사항) 권한명령을 사용하여 권한을 구성합니다.
- (선택사항) 계정명령을 이용하여 계정을 구성합니다.

## 10.5. AAA 구성 작업 목록

- AAA 를 이용하여 로그인 인증을 구성합니다.
- AAA 를 이용하여 PPP 를 구성합니다.
- 권한 단계별 암호를 보호합니다.
- AAA 인증 배너 메시지를 구성합니다.
- AAA 사용자 이름 인증
- AAA 사용자 비밀번호 인증
- 사용자 이름 인증 구성
- 비밀번호 활성화

## 10.6. AAA 인증 구성 작업

인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

(1) 별도의 보안 서버를 사용하려면 RADIUS, TACACS + 또는 Kerberos 와 같은 보안 프로토콜 매개 변수를 구성하십시오.

(2) AAA 인증 명령을 사용하여 인증을 위한 메소드 목록을 정의합니다.

(3) 필요한 경우 메서드 목록을 특정 인터페이스 또는 행에 적용합니다.

### 10.6.1. AAA 를 이용한 인증 로그인 구성

AAA 보안 서비스는 다양한 로그인 인증 방법을 용이하게합니다. 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 생성합니다. 이 목록은 login authentication line configuration 명령을 사용하여 적용됩니다.

AAA 를 사용하여 로그인 인증을 구성하려면 전역 구성 모드에서 시작하는 다음 명령을 사용하십시오:

| 명령어 | 설명 |
|---|---|
| **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] | 전역 AAA 를 활성화합니다. |
| **line** [ **console** \| **vty**] line-number [endingline-number] | 인증 목록을 적용할 회선에 대한 회선 구성 모드를 시작합니다. |
| **login authentication** {**default** \| *list-name*} | 인증 목록을 한 줄 또는 여러 줄에 적용합니다. |

list-name 은 작성중인 목록의 이름을 지정하는 데 사용되는 문자열입니다. 메소드 인수는 인증 알고리즘이 시도하는 실제 메소드를 나타냅니다. 추가 인증 방법은 이전 메소드가 오류를 리턴하는 경우에만 사용되며, 실패하지 않은 경우에는 사용되지 않습니다. 모든 메소드가 오류를 리턴하더라도 인증이 성공하도록 지정하려면 명령 행에서 마지막 메소드로 none 을 지정하십시오.

예를 들어 RADIUS 서버가 오류를 반환하더라도 로컬 계정을 사용하여 인증이 성공하도록 지정하려면 다음 명령을 추가하십시오.

aaa authentication login default local group radius

참조:

none 키워드는 모든 사용자 로그인이 성공적으로 인증되도록하기 때문에 인증의 백업 방법으로만 사용해야합니다.

다음 표는 지원되는 로그인 인증 방법을 나열합니다.

| 키워드 | 설명 |
|---|---|
| enable | 인증에 사용할 암호를 사용합니다. |
| group *name* | 인증을 위해 지정된 서버 그룹을 사용합니다. |
| group radius | 인증을 위해 Radius 서버 목록을 사용합니다. |
| line | 회선 인증에 암호를 사용합니다. |
| local | 인증에 로컬 사용자 이름 데이터베이스를 사용합니다. |
| local-case | 대/소문자를 구분하는 로컬 사용자이름을 인증합니다. |
| none | 인증을 사용하지 않습니다. |

(1) 로그인 인증 암호 활성화

aaa authentication login 명령에 enable method 키워드를 사용하여 로그인 인증 방법으로 활성화 암호를 지정합니다. 예를 들어 다른 메소드 목록이 정의되지 않은 경우 로그인시 사용자 인증 방법으로 사용 가능 암호를 지정하려면 다음 명령을 입력하십시오.

aaa authentication login default enable

(2) 로그인 인증용 라인 암호

aaa authentication login 명령을 line method 키워드와 함께 사용하여 회선 암호를 로그인 인증 방법으로 지정하십시오. 예를 들어 로그인 할 때 다른 메소드 목록이 정의되지 않은 경우 사용자 인증 방법으로 라인 암호를 지정하려면 다음 명령을 입력하십시오:

aaa authentication login default line

로그인 인증 방법으로 라인 암호를 사용하려면 먼저 라인 암호를 정의해야합니다.

(3) 로컬 암호를 사용한 로그인 인증

aaa authentication login 명령을 local method 키워드와 함께 사용하여 Cisco 라우터 또는 액세스 서버가 인증에 로컬 사용자 이름 데이터베이스를 사용하도록 지정합니다. 예를 들어 다른 메소드 목록이 정의되지 않은 경우 로그인시 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 내용은 이 장의 "사용자 인증 구성"절을 참조하십시오.

(4) RADIUS 그룹을 사용한 로그인 인증

aaa 인증 로그인 명령을 그룹 radius 메소드와 함께 사용하여 RADIUS 를 로그인 인증 방법으로 지정하십시오. 예를 들어 다른 메소드 목록이 정의되지 않은 경우 로그인시 사용자 인증 방법으로 RADIUS 를 지정하려면 다음 명령을 입력하십시오:

aaa authentication login default group radius

로그인 인증 방법으로 RADIUS 를 사용하려면 먼저 RADIUS 보안 서버와의 통신을 활성화해야합니다. RADIUS 서버와의 통신 구성에 대한 자세한 내용은 " RADIUS 구성." 장을 참조하십시오.

### 10.6.2. 권한 단계별 비밀번호 보호 활성화

aaa 인증 활성화 기본 명령을 사용하여 사용자가 권한있는 EXEC 명령 수준에 액세스 할 수 있는지 여부를 결정하는 데 사용되는 일련의 인증 방법을 만듭니다. 최대 네 가지 인증 방법을 지정할 수 있습니다. 추가 인증 방법은 이전 메소드가 오류를 리턴하는 경우에만 사용되며, 실패하지 않은 경우에는 사용되지 않습니다. 모든 메소드가 오류를 리턴하더라도 인증이 성공하도록 지정하려면 명령 행에서 마지막 메소드로 none 을 지정하십시오.

다음 명령어를 전역모드에서 사용합니다:

| 명령어 | 설명 |
|---|---|
| **aaa authentication enable default** *method1 [method2...]* | 권한 단계를 요구하는 사용자 ID 및 암호 확인을 사용 가능하게 합니다. |

method 인수는 인증 알고리즘이 시도하는 메소드의 실제 목록을 입력된 순서로 참조합니다. 다음 표는 지원되는 사용 가능 인증 방법을 나열합니다.

| 키워드 | 설명 |
|---|---|
| enable | 인증에 암호를 사용합니다. |
| group *group-name* | aaa 그룹 서버 radius 또는 aaa 그룹 서버 tacacs + 명령에 정의 된대로 인증을 위해 RADIUS 또는 TACACS + 서버의 하위 집합을 사용합니다. |
| group radius | 인증을 위해 Radius 호스트 목록을 사용합니다. |
| line | 회선에 인증 암호를 사용합니다. |
| none | 인증을 사용하지 않습니다. |

### 10.6.3. AAA 인증 배너 메시지 구성

AAA 는 구성 가능한 개인화 된 로그인 및 실패한 로그인 배너의 사용을 지원합니다. 사용자가 시스템에 로그인하여 AAA 를 사용하여 인증되고 어떤 이유로 든 인증에 실패할 때 표시될 메시지 배너를 구성할 수 있습니다.

〈로그인 배너 구성하기〉
사용자가 로그인 할 때마다 표시될 배너를 구성하려면 (로그인 용 기본 메시지 대체) 전역 구성 모드에서 다음 명령을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| **aaa authentication banner** *delimiter text-string delimiter* | 지정 로그인 배너를 만듭니다. |

〈로그인 실패 배너 구성하기〉
사용자가 로그인에 실패할 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* | 사용자가 로그인에 실패할 때 표시할 메시지를 작성합니다. |

로그인 배너를 만들려면 다음 문자 문자열이 배너로 표시되고 텍스트 문자열 자체에 시스템이 있음을 알리는 구분 문자를 구성해야 합니다. 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.

### 10.6.4. AAA 사용자 이름 인증

사용자에게 사용자 이름을 입력하라는 메시지가 표시될 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. 전역구성모드에서 구성하려면 다음 명령을 사용하십시오:

| 명령어 | 설명 |
|---|---|
| **aaa authentication username-prompt** text-string | 사용자 이름을 입력하라는 메시지가 표시될 텍스트 문자열입니다. |

### 10.6.5. AAA 사용자 비밀번호 인증

사용자에게 암호를 묻는 메시지가 표시될 때 표시되는 텍스트를 변경하려면 전역 구성 모드에서 aaa authentication password-prompt 명령을 사용하십시오. 기본 암호 프롬프트 텍스트로 돌아가려면이 명령의 no 형식을 사용하십시오.

aaa authentication password-prompt 명령은 원격 TACACS + 서버가 제공하는 대화 상자를 변경하지 않습니다. 전역 구성 모드에서 다음 명령을 사용하십시오:

| 명령어 | 설명 |
|---|---|
| **aaa authentication password-prompt** *text-string* | 사용자가 암호를 입력하라는 메시지가 표시될 때 표시할 문자열입니다. |

### 10.6.6. 사용자 이름 인증 구성

다음 상황에서 유용하게 사용할 수있는 사용자 이름 기반 인증 시스템을 만들 수 있습니다.

- TACACS 를 지원할 수 없는 네트워크에 대해 TACACS 와 유사한 사용자 이름 및 암호화된 암호 인증 시스템을 제공합니다.
- 액세스 목록 확인, 암호 확인, 로그인시 자동 명령 실행 및 "no escape"과 같은 특수 사례 로그인을 제공합니다.

사용자 이름 인증을 구성하려면 시스템 구성에 필요한대로 전역 구성 모드에서 다음 명령을 사용하십시오. 사용자 이름을 삭제하려면이 명령의 no 형식을 사용하십시오.

**username** name {**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** line-number]

**username** name [**noescape**] [**nohangup**]

**username** name [**maxlinks** number]

**no username** name

#### 10.6.7. 비밀번호 활성화

여러 권한 레벨에 대한 액세스를 제어하기 위해 로컬 암호를 구성하려면, 전역 구성 모드에서 enable password 명령을 사용하십시오. 암호 요구 사항을 제거하려면이 명령의 no 형식을 사용하십시오.

**enable level password encryption-type** encrypted-password
**no enable** [**level** level] **password**

## 10.7. AAA 인증 구성 예제

RADIUS 인증 예제
이 절에서는 RADIUS 를 사용한 하나의 샘플 구성을 제공합니다.
다음 예에서는 RADIUS 를 사용하여 인증하고 권한을 부여하도록 스위치를 구성하는 방법을 보여줍니다.

```
aaa authentication login radius-login group radius local
aaa authorization network radius-network radius
line vty 0
login authentication radius-login
```

이 샘플 RADIUS 인증 및 권한 부여 구성의 줄은 다음과 같이 정의됩니다:

- aaa authentication login radius-login radius local 명령은 로그인 프롬프트에서 인증을 위해 RADIUS 를 사용하도록 라우터를 구성합니다. RADIUS 가 오류를 반환하면 사용자는 로컬 데이터베이스를 사용하여 인증됩니다.
- aaa authentication ppp radius-ppp radius 명령은 사용자가 아직 로그인하지 않은 경우 CHAP 또는 PAP 를 사용하여 PPP 인증을 사용하도록 소프트웨어를 구성합니다. EXEC 기능이 사용자를 인증한 경우 PPP 인증이 수행되지 않습니다.
- aaa authorization network radius-network radius 명령은 RADIUS 에 네트워크 인증, 주소 할당 및 기타 액세스 목록을 쿼리합니다.

- login authentication radius-login 명령은 3 번 라인에 대한 radius-login 메소드 목록을 활성화합니다.

## 10.8. AAA 권한 구성 작업 목록

- AAA 를 사용하여 EXEC 권한 구성

## 10.9. AAA 권한 구성 작업

AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

(1) AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

(2) AAA 권한 부여 명령을 사용하여 권한 부여를 위한 방법 목록을 정의하십시오.

(3) 필요한 경우 메서드 목록을 특정 인터페이스 또는 행에 적용합니다.

### 10.9.1. AAA 를 사용한 EXEC 권한 구성

aaa authorization 명령을 사용하여 권한 부여를 활성화하십시오.

aaa authorization exec 명령을 사용하여 권한 부여를 실행하여 사용자가 EXEC 쉘을 실행할 수 있는지 확인하십시오. 이 기능은 자동 명령 정보와 같은 사용자 프로파일 정보를 반환할 수 있습니다.

라인 구성 명령 로그인 권한을 사용하십시오. 전역 구성모드에서 다음을 사용하십시오:

| 명령어 | 설명 |
|---|---|
| **aaa authorization exec {default** \| *list-name} method1* [*method2*...] | 전역 권한 부여 목록을 구성합니다. |
| **line** [**console** \| **vty**] *line-number* [*ending-line-number*] | 인증 방법 목록을 적용할 라인에 대한 구성 모드를 시작합니다. |
| **login authorization** {**default** \| *list-name*} | 권한을 행이나 행 구성에 적용합니다. |

키워드 list-name 은 권한 부여 메소드 목록의 이름을 지정하는 데 사용되는 문자열입니다. 키워드 메소드는 권한 부여 프로세스 중 실제 메소드를 지정합니다. 방법 목록을 사용하면 하나 이상의 보안 프로토콜을 지정하여 인증에 사용할 수 있으므로 초기 방법이 실패할 경우 백업 시스템을 보장할 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 권한 부여 메소드와의 성공적인 통신이있을 때까지 또는 정의된 모든 메소드가 모두 소진될 때까지 계속됩니다.

지정된 모든 메소드가 응답하지 않고 시스템이 EXEC 쉘에 들어가기를 원하는 경우 명령 행에서 마지막 인증 메소드로 none 을 지정해야합니다.

기본 매개 변수를 사용하여 기본 목록을 구성하면 기본 목록이 모든 인터페이스에 자동으로 적용됩니다. 예를 들어 다음 명령을 사용하여 radius 를 exec 의 기본 인증 방법으로 지정합니다.

aaa authorization exec default group radius

참조:
메소드 목록이 정의되지 않으면 로컬 권한 서비스를 사용할 수 없으며 권한이 미전달됩니다. 다음 표는 현재 지원되는 EXEC 인증 모드를 나열합니다.

| **명령어** | **설명** |
|---|---|
| group *WORD* | 권한 부여를 위해 지정된 서버 그룹을 사용합니다. |
| group radius | Radius 권한을 사용합니다. |
| local | 권한 부여에 로컬 DB 를 사용합니다. |
| if-authenticated | 사용자가 인증된 경우 요청된 기능에 접근이 가능합니다. |
| none | 권한 부여를 수행하지 않습니다. |

## 10.10. AAA 권한 예제

```
aaa authentication login default local
aaa authorization exec default local
!
username exec1 password 9 ciphertext
username exec4 password 9 ciphertext maxlinks 10
!
```

이 샘플 RADIUS 인증 구성의 명령어는 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 을 입력해야하는 모든 사용자에게 자동으로 적용됩니다.
- 사용자 이름은 exec1, 로그인 암호는 abc, EXEC 권한 수준은 15 (가장 높은 수준)입니다. 즉, exec 쉘에 로그인 한 권한 수준이 15 인 사용자 exec1 이 있으면 모든 명령을 검사하고 수행할 수 있습니다.
- 사용자 이름은 exec4, 로그인 암호는 abc, 사용자의 최대 링크는 10 입니다.

## 10.11. AAA 계정 구성 작업 목록

- AAA 사용 계정 연결 구성
- AAA 네트워크 계정 구성

## 10.12. AAA 계정 구성 작업

AAA 계정을 구성하려면 다음 구성 프로세스를 수행하십시오.

(1) 별도의 보안 서버를 사용하려면 RADIUS, TACACS + 또는 Kerberos 와 같은 보안 프로토콜 매개 변수를 구성하십시오.

(2) AAA 계정 명령을 사용하여 계정에 대한 방법 목록을 정의하십시오.

(3) 필요한 경우 메서드 목록을 특정 인터페이스 또는 행에 적용합니다.

### 10.12.1. AAA 계정 연동 사용 구성

aaa accounting 명령을 사용하여 AAA 계정 사용 가능.

네트워크 액세스 서버에서 이루어진 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* | 계정 목록을 만듭니다. |

키워드 list-name 은 구성 목록의 문자열을 명명하는 데 사용됩니다. 키워드는 Accounting 프로세스 중에 채택된 실제 방법을 지정합니다.

다음 표는 현재 지원되는 연결 계정 방법을 나열합니다.

| 키워드 | 설명 |
|---|---|
| group *WORD* | 계정에 대하여 명명된 서버 그룹을 사용 가능하게 합니다. |
| group radius | radius 계정을 활성화합니다. |
| none | 인터페이스 활성화를 비활성화 합니다. |
| stop-only | 요청한 사용자 프로세스가 끝날 때 "중지"기록 Accounting 통지를 보냅니다. |

| | |
|---|---|
| start-stop | RADIUS 또는 TACACS +는 요청된 프로세스가 시작될 때 "시작"계정 알림을 보내고 프로세스가 끝날 때 "중지"계정 알림을 보냅니다. |

### 10.12.2. AAA 네트워크 계정 연동

aaa accounting 명령을 사용하여 AAA 계정을 활성화합니다.

SLIP, PPP, NCP 및 ARAP 세션에 대한 계정 정보를 제공하는 방법 목록을 만들려면 글로벌 구성 모드에서 aaa accounting network 명령을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| **aaa accounting network** {**default** \| *list-name*} {**start-stop \| stop-only \| none**} **group** *groupname* | 네트워크 전역 계정 활성화 |

키워드 list-name 은 구성 목록의 문자열을 명명하는 데 사용됩니다. 키워드는 Accounting 프로세스 중에 채택된 실제 방법을 지정합니다.

다음 표는 현재 지원되는 네트워크 계정 방법을 나열합니다.

| 명령어 | 설명 |
|---|---|
| group *WORD* | 계정에 대해 명명된 서버 그룹 사용가능 하게 합니다. |
| group radius | radius 계정 활성화합니다. |
| none | 계정 서비스를 비활성화 합니다. |
| stop-only | 요청한 사용자 프로세스가 끝날 때 "중지"기록 Accounting 통지를 보냅니다. |
| start-stop | RADIUS 또는 TACACS +는 요청된 프로세스가 시작될 때 "시작"계정 알림을 보내고 프로세스가 끝날 때 "정지" 계정 알림을 보냅니다. |

### 10.12.3. AAA 계정 업데이트

정기적인 임시 계정 레코드를 계정 서버로 보내려면 글로벌 구성 모드에서 aaa accounting update 명령을 사용하십시오. 임시 계정 업데이트를 사용하지 않으려면이 명령의 no 형식을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| **aaa accounting update** [**newinfo**] [**periodic** *number*] | AAA 계정 업데이트 활성화 |

새 정보 키워드를 사용하면 보고할 새 Accounting 정보가 있을 때마다 중간 계정 레코드가 계정 서버로 보내집니다. 예를 들면, IPCP (IP Control Protocol)가 원격 피어와의 IP 주소 협상을 완료할 때입니다. 임시 계정 레코드에는 원격 피어에서 사용하는 협상 된 IP 주소가 포함됩니다.

periodic 키워드와 함께 사용하면 중간 계정 레코드가 인수 번호에 정의 된대로 주기적으로 전송됩니다. 임시 계정 레코드에는 계정 레코드가 전송될 때까지 해당 사용자에 대해 기록된 모든 계정 정보가 들어 있습니다.

newinfo 및 periodic 키워드를 모두 사용하는 경우 보고할 새 계정 정보가 있을 때마다 임시 계정 레코드가 계정 서버로 보내지고 계정 레코드는 인수 번호로 정의 된대로 정기적으로 계정 서버로 보내집니다. 예를 들어, aaa accounting update newinfo periodic number 명령을 구성하면 현재 로그인 한 모든 사용자가 주기적인 임시 계정 레코드를 계속 생성하고 새 사용자는 newinfo 알고리즘을 기반으로 계정 레코드를 생성합니다.

#### 10.12.4. AAA 계정 사용 이름 제어

AAA 시스템이 사용자 이름 문자열이 NULL 인 사용자에 대한 계정 레코드를 보내지 않도록하려면 글로벌 구성 모드에서 aaa accounting suppress null-username 명령을 사용하십시오. 사용자 이름이 NULL 인 사용자에게 레코드를 보내려면이 명령의 no 형식을 사용하십시오.

- aaa accounting suppress null-username

# 11. RADIUS 구성

이 장에서는 Remote Authentication Dial-In User Service (RADIUS) 보안 시스템에 대해 설명하고 RADIUS 의 작동을 정의하며 RADIUS 기술을 사용하기에 적절하고 부적절한 네트워크 환경을 식별합니다. "RADIUS 구성 작업 목록"절에서는 AAA (authentication, authorization, 과 accounting) 명령 집합으로 RADIUS 를 구성하는 방법에 대해 설명합니다.

## 11.1. 개요

### 11.1.1. RADIUS 개요

RADIUS 는 권한이 없는 액세스로부터 네트워크를 보호하는 분산 클라이언트 / 서버 시스템입니다. 구현시 RADIUS 클라이언트는 스위치에서 실행되며 모든 사용자 인증 및 네트워크 서비스 액세스 정보가 포함된 중앙 RADIUS 서버로 인증 요청을 보냅니다.

RADIUS 는 원격 사용자에 대한 네트워크 액세스를 유지하면서 높은 수준의 보안이 필요한 다양한 네트워크 환경에서 구현되었습니다.

액세스 보안이 필요한 다음 네트워크 환경에서 RADIUS 를 사용하십시오.

- RADIUS 를 지원하는 여러 공급 업체 액세스 서버가있는 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 사용자는 Kerberos 보안 시스템과 함께 작동하도록 사용자 지정된 RADIUS 서버를 통해 인증됩니다.
- 사용자가 단일 서비스에만 액세스해야 하는 네트워크. RADIUS 를 사용하면 단일 호스트, 텔넷과 같은 단일 유틸리티 또는 PPP (Point-to-Point Protocol)와 같은 단일 프로토콜에 대한 사용자 액세스를 제어할 수 있습니다. 예를 들어 사용자가 로그인하면 RADIUS 는이 사용자를 IP 주소 10.2.3.4 를 사용하여 PPP 를 실행할 수있는 권한으로 식별하고 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 시점에 데이터를 전송할 수 있으며 세션 중에 사용된 리소스 (시간, 패킷, 바이트 등)의 양을 나타냅니다. 인터넷 서비스 공급자 (ISP)는 프리웨어 기반 버전의 RADIUS 액세스 제어 및 Accounting 소프트웨어를 사용하여 특별한 보안 및 청구 요구 사항을 충족시킬 수 있습니다.

다음 네트워크 보안 상황에서는 RADIUS 가 적합하지 않습니다.

- 멀티 프로토콜 액세스 환경, RADIUS 는 다음 프로토콜을 지원하지 않습니다.

  AppleTalk Remote Access (ARA)

NetBIOS Frame Control Protocol (NBFCP)

- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD 연동
- 스위치-대-스위치인 경우. RADIUS 는 두 가지 인증을 제공하지 않습니다.
- 다양한 서비스를 사용하는 네트워크. RADIUS 는 일반적으로 사용자를 하나의 서비스 모델에 바인딩합니다.

### 11.1.2. RADIUS 운영

사용자가 RADIUS 를 사용하여 액세스 서버에 로그인하고 인증하려고 하면 다음 단계가 발생합니다.

(1) 사용자는 정확한 아이디와 비밀번호를 입력해야 합니다.

(2) RADIUS 서버에 네트워크를 넘어 사용자 이름과 보안 비밀번호를 보냅니다.

(3) RADIUS 서버로부터 사용자가 받는 응답 중 하나가 됩니다.

a. ACCEPT—사용자 인증이 된 경우.

b. REJECT—사용자 인증이 아이디 및 비밀번호 오류로 인해 되지 않은 경우.

c. CHALLENGE— RADIUS 서버에서 챌린지가 발생합니다. 챌린지는 사용자로부터 추가 데이터를 수집합니다.

d. CHANGE PASSWORD— 사용자에게 새 암호를 선택하라는 요청이 RADIUS 서버에 의해 발행됩니다.

ACCEPT 또는 REJECT 응답은 EXEC 또는 네트워크 권한 부여에 사용되는 추가 데이터와 함께 제공됩니다. RADIUS 인증을 사용하려면 먼저 RADIUS 인증을 완료해야합니다. ACCEPT 또는 REJECT 패킷에 포함된 추가 데이터는 다음과 같이 구성됩니다.

텔넷, rlogin 또는 LAT (로컬 영역 전송) 연결, PPP, SLIP (회선 인터넷 프로토콜) 나 EXEC 서비스를 비롯하여 사용자가 액세스 할 수있는 서비스. 호스트 또는 클라이언트 IP 주소, 액세스 목록 및 사용자 시간 초과를 포함한 연결 매개 변수

## 11.2. RADIUS 구성 작업 목록

스위치 또는 액세스 서버에 RADIUS 를 구성하려면 다음 작업을 수행해야합니다.

- RADIUS 인증을위한 방법 목록을 정의하려면 aaa authentication 전역 구성 명령을 사용하십시오. aaa authentication 명령 사용에 대한 자세한 정보는 "인증 구성"장을 참조하십시오.
- 정의된 메소드 목록을 사용하려면 line 및 interface 명령을 사용하십시오. 자세한 정보는 "인증

구성"장을 참조하십시오.

- 다음 구성 작업은 선택 사항입니다.
- 특정 사용자 기능을 인증하려면 aaa authorization global 명령을 사용할 수 있습니다. aaa authorization 명령 사용에 대한 자세한 내용은 "권한 구성"장을 참조하십시오.
- RADIUS 연결에 대한 계정을 활성화하려면 aaa accounting 명령을 사용할 수 있습니다. aaa accounting 명령 사용에 대한 자세한 내용은 "계정 구성"장을 참조하십시오.

RADIUS 구성 작업 목록

- RADIUS 서버 통신으로 전환 구성
- 공급 업체별 RADIUS 특성을 사용하도록 스위치 구성
- RADIUS 인증 지정
- RADIUS 권한 지정
- RADIUS 계정 지정

## 11.3. RADIUS 구성 작업

### 11.3.1. RADIUS 서버 통신으로 전환 구성

RADIUS 호스트는 일반적으로 Livingston, Merit, Microsoft 또는 다른 소프트웨어 제공 업체의 RADIUS 서버 소프트웨어를 실행하는 다중 사용자 시스템입니다.

RADIUS 서버와 시스코 라우터는 공유 암호 텍스트 문자열을 사용하여 암호를 암호화하고 응답을 교환합니다.

RADIUS 가 AAA 보안 명령을 사용하도록 구성하려면 RADIUS 서버 데몬을 실행하는 호스트와 라우터와 공유하는 비밀 텍스트 (키) 문자열을 지정해야 합니다.

서버 별 RADIUS 서버 통신을 구성하려면 글로벌 구성 모드에서 다음 명령을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| **radius-server host** *ip-address* [**auth-port** *port-number*] [**act-port** *portnumber*] | 원격 RADIUS 서버 호스트의 IP 주소 또는 호스트 이름을 지정하고 인증 및 계정 대상 포트 번호를 할당합니다. |
| **radius-server key** string | 라우터와 RADIUS 서버간에 사용되는 공유 비밀 텍스트 문자열을 지정합니다. |

라우터와 RADIUS 서버 간의 전역 통신 구성을 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 지정합니다. |
| **radius-server deadtime** *minutes* | RADIUS 인증 요청에 응답하지 않는 RADIUS 서버가 몇 분 동안 전달되는지 지정합니다. |

### 11.3.2. 특정 업체별 RADIUS 특성을 사용하도록 스위치 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 통해 공급 업체는 일반적인 용도에 적합하지 않은 자체 확장 특성을 지원할 수 있습니다.

공급 업체 ID 및 VSA 에 대한 자세한 내용은 RFC 2138, RADIUS (Remote Authentication Dial-In User Service)를 참조하십시오. VSA 를 인식하고 사용하도록 네트워크 액세스 서버를 구성하려면 전역 구성 모드에서 다음 명령을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| **radius-server vsa send** [authentication] | 네트워크 액세스 서버가 RADIUS IETF 속성 26 에 정의 된대로 VSA 를 인식하고 사용할 수 있습니다 |

### 11.3.3. 특정 RADIUS 인증

RADIUS 서버를 식별하고 RADIUS 인증 키를 정의한 후에는 RADIUS 인증을 위한 방법 목록을 정의해야합니다. RADIUS 인증은 AAA 를 통해 용이하므로 RADIUS 를 인증 방법으로 지정하여 aaa authentication 명령을 입력해야 합니다. 자세한 내용은 "인증 구성"장을 참조하십시오.

### 11.3.4. 특정 RADIUS 권한

AAA 권한을 통해 네트워크에 대한 사용자 액세스를 제한하는 매개 변수를 구성할 수 있습니다. RADIUS 를 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 제어를위한 한 가지 방법을 제공합니다. RADIUS 인증은 AAA 를 통해 용이하므로 RADIUS 를 인증 방법으로 지정하여 aaa authorization 명령을 실행해야합니다. 자세한 내용은 "인증 구성"장을 참조하십시오.

#### 11.3.5. 특정 RADIUS 계정

AAA 계정 기능을 사용하면 사용자가 액세스하는 서비스는 물론 사용중인 네트워크 리소스의 양을 추적할 수 있습니다. RADIUS 계정은 AAA 를 통해 쉽게 처리되므로 RADIUS 를 계정 방법으로 지정하여 aaa accounting 명령을 실행해야합니다. 자세한 내용은 "계정 구성"장을 참조하십시오.

## 11.4. RADIUS 구성 예제

### 11.4.1. RADIUS 인증 및 권한 부여 예제

다음 예에서는 RADIUS 를 사용하여 인증하고 권한을 부여하도록 라우터를 구성하는 방법을 보여줍니다.

aaa authentication login use-radius group radius local

이 샘플 RADIUS 인증 및 권한 부여 구성의 줄은 다음과 같이 정의됩니다.

aaa authentication login use-radius radius local 로그인 프롬프트에서 인증을 위해 RADIUS 를 사용하도록 라우터를 구성합니다. RADIUS 가 오류를 반환하면 사용자는 로컬 데이터베이스를 사용하여 인증됩니다. 이 예에서 use-radius 는 RADIUS 를 지정한 다음 로컬 인증을 지정하는 메소드 목록의 이름입니다.

**RADIUS 인증, 권한, 계정 예제**

다음 예에서는 AAA 명령 집합과 함께 RADIUS 를 사용하는 일반 구성을 보여줍니다.

```
radius-server host 1.2.3.4
radius-server key 5 myRaDiUSpassWoRd
username root password 5 AlongPassword
aaa authentication login admins radius local
line vty 1 16
login authentication admins
```

이 예제의 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 반경 로컬 명령은 RADIUS 인증 및 RADIUS 서버가 응답하지 않는 경우 로컬 인증이 PPP 를 사용하는 직렬 회선에서 사용됨을 지정하는 인증 방법 목록 "dial-ins"을 정의합니다.

login authentication admins 명령은 로그인 인증을 위해 "admins"메소드 목록을 적용합니다.

### 11.4.2. RADIUS 적용 예제

다음 예는 AAA 명령 세트를 통해 일반 구성을 정의하는 방법을 보여줍니다.

```
radius-server host 1.2.3.4
radius-server key 5 myRaDiUSpassWoRd
username root password 5 AlongPassword
aaa authentication login admins radius local
line vty 1 16
login authentication admins
```

위의 예에서 각 명령 행에는 고유 한 의미가 있습니다. 다음 내용을 참조하십시오. 명령 radius-server host 는 RADIUS 서버의 IP 주소를 정의합니다. 명령 radius-server key 는 네트워크 액세스 서버와 RADIUS 서버 간의 공유 핀을 정의합니다.

aaa authentication login admins radius local 명령은 먼저 인증 방법 목록 admins 를 정의합니다. 관리자 목록은 먼저 RADIUS 를 인증 방법으로 지정한 다음 RADIUS 서버가 응답하지 않는 경우 로컬 인증을 사용합니다.

login authentication admins 명령은 로그인 인증 방법으로 admins 메소드 목록을 지정합니다.

# 12. 인터페이스

이 섹션은 스위치가 지원하는 다양한 종류의 인터페이스를 배우고 다양한 인터페이스 유형에 대한 구성 정보를 참조하는 데 도움이 됩니다.

모든 인터페이스 명령에 대한 자세한 설명은 인터페이스 구성 명령을 참조하십시오. 이 섹션에 나오는 다른 명령 파일은 설명서의 다른 부분을 참조하십시오.

개요에는 모든 인터페이스 유형에 적용할 수 있는 통신 정보가 포함됩니다.

## 12.1. 지원되는 인터페이스 유형

인터페이스 유형에 대한 자세한 내용은 다음 표를 참조하십시오.

| 인터페이스 유형 | 명령어 | 참고 |
|---|---|---|
| Ethernet interface | 이더넷 인터페이스를 구성합니다.<br>고속 이더넷 인터페이스를 구성합니다.<br>기가비트 이더넷 인터페이스를 구성합니다. | 이더넷 인터페이스 구성 |
| Logical Interface | 루프백 인터페이스<br>Null 인터페이스<br>VLAN 인터페이스 | 논리 인터페이스 구성<br>루프백 인터페이스와 널 (null) 인터페이스는 3 계층 스위치에서만 구성됩니다. 사용자는 레이어 2 스위치에서 VLAN 인터페이스를 구성할 수 있습니다. |
| | 집계 인터페이스 | 논리 인터페이스 구성 |

종류의 인터페이스: 이더넷 인터페이스와 논리적 인터페이스. 이더넷 인터페이스 유형은 표준 통신 인터페이스 및 스위치에 설치된 인터페이스 카드 또는 인터페이스 모듈에 따라 하나의 장치에 따라 다릅니다. 논리적 인터페이스는 해당 물리적 장치가 없는 인터페이스로 사용자가 수동으로 구성합니다.

스위치의 지원 이더넷 인터페이스는 다음과 같습니다.

- 이더넷 인터페이스
- 고속 이더넷 인터페이스
- 기가비트 이더넷 인터페이스

스위치의 지원되는 논리적 인터페이스는 다음과 같습니다.

- 루프백 인터페이스
- null 인터페이스

- aggregation 인터페이스
- VLAN 인터페이스

## 12.2. 인터페이스 구성 개요

다음 설명은 모든 인터페이스의 구성 프로세스에 적용됩니다. 전역 구성 모드에서 인터페이스 구성을 수행하려면 다음 단계를 수행하십시오.

(1) interface 명령을 실행하여 인터페이스 구성 모드로 들어가서 인터페이스 구성을 시작합니다. 이 때 스위치 프롬프트는 'config_'와 단축된 인터페이스 형식으로 구성됩니다. 이 인터페이스를 번호로 사용하십시오. 번호는 설치 (exworks) 또는 인터페이스 카드가 시스템에 추가될 때 지정됩니다. 이 인터페이스를 표시하려면 show interface 명령을 실행하십시오. 장치가 지원하는 각 인터페이스는 다음과 같이 자체 상태를 제공합니다.

노트:
인터페이스 유형과 인터페이스 번호 사이에 공백을 추가할 필요가 없습니다. 예를 들어, 위의 행에서 g 1/1 또는 g 1/1 이 둘 다 해당합니다.

(2) 인터페이스 구성 모드에서 인터페이스 구성 명령을 구성할 수 있습니다. 다양한 명령은 인터페이스에서 실행될 프로토콜 및 응용 프로그램을 정의합니다. 이 명령은 사용자가 인터페이스 구성 모드를 종료하거나 다른 인터페이스로 전환할 때까지 유지됩니다.

(3) 인터페이스 구성이 완료되면 다음 장의 '모니터링 및 유지 관리 인터페이스'에서 show 명령을 사용하여 인터페이스 상태를 테스트하십시오.

```
switch# show interface
GigaEthernet1/1 is down, line protocol is down
Hardware is Fast Ethernet, Address is 5491.aff7.7dc1
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
0 input packets with dribble condition detected
1 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
To configure gigabit Ethernet interface g1/1, enter the following content:
interface GigaEthernet0/1
The switch prompts “config_g1/1”.

# 13. 인터페이스 구성

## 13.1. 인터페이스 공통 속성 구성

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

### 13.1.1. 설명 추가

관련 인터페이스에 대한 설명을 추가하면 인터페이스에 첨부된 콘텐츠를 기억하는 데 도움이 됩니다. 이 설명은 인터페이스 사용을 식별하는 데 도움이 되는 인터페이스 참고 사항으로 만 사용되며 인터페이스의 기능에는 영향을 미치지 않습니다. 이 설명은 **show running-config** 및 **show interface** 명령의 출력에 나타납니다. 사용자가 인터페이스에 설명을 추가하려는 경우 인터페이스 구성 모드에서 다음 명령을 사용하십시오.

| 명령 | 기술 |
|---|---|
| **description** string | 현재 구성된 인터페이스에 설명을 추가합니다. |

### 13.1.2. 대역폭 구성

상위 프로토콜은 대역폭 정보를 사용하여 작업 결정을 수행합니다. 다음 명령을 사용하여 인터페이스 대역폭을 구성합니다.

| 명령 | 기술 |
|---|---|
| **bandwidth** *kilobps* | 현재 구성된 인터페이스의 대역폭을 구성합니다. |

대역폭은 라우팅 매개 변수 일뿐이며 실제 물리적 인터페이스의 통신 속도에는 영향을 미치지 않습니다.

### 13.1.3. 시간 지연 구성

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

| 명령 | 기술 |
|---|---|
| **delay** *tensofmicroseconds* | 현재 구성된 인터페이스의 시간 지연을 구성합니다. |

시간 지연의 구성은 단지 정보 매개 변수 일뿐입니다. 이 명령을 사용하면 인터페이스의 실제 시간 지연을 조정할 수 없습니다.

## 13.2. 인터페이스 모니터링 및 유지 보수

다음 작업은 인터페이스를 모니터하고 유지 보수할 수 있습니다.

- 인터페이스 상태 점검
- 인터페이스 초기화 및 삭제
- 인터페이스 다운 및 활성화

### 13.2.1. 인터페이스 상태 확인

우리의 스위치는 소프트웨어 및 하드웨어의 버전 번호, 인터페이스 상태 등 인터페이스 정보와 관련된 몇 가지 명령을 표시할 수 있습니다. 다음 표는 인터페이스 모니터 명령의 일부를 나열합니다. 이 명령에 대한 설명은 '인터페이스 구성 명령'을 참조하십시오. 다음 명령을 사용하십시오.

| 명령 | 기술 |
|---|---|
| **show interface** [**type** [slot/port]] | 인터페이스 상태를 표시합니다. |
| **show running-config** | 현재 구성을 표시합니다. |

### 13.2.2. 인터페이스 초기화 및 삭제

논리 인터페이스를 동적으로 구성하고 삭제할 수 있습니다. 이는 하위 인터페이스 및 채널화 된 인터페이스에도 적용됩니다. 전역 구성 모드에서 인터페이스를 초기화하고 삭제하려면 다음 명령을 사용하십시오.

| 명령 | 기술 |
|---|---|
| **no interface type** [*slot*/*port*] | 물리적 인터페이스를 초기화하거나 가상 인터페이스를 삭제합니다. |

### 13.2.3. 인터페이스 활성화 및 비활성화

인터페이스가 종료되면 인터페이스의 모든 기능이 사용 불가능하게 되며 이 인터페이스는 모든 모니터 명령 디스플레이에서 사용 불가능한 인터페이스로 표시됩니다. 이 정보는 동적 라우팅 프로토콜을 통해 다른 스위치로 전송될 수 있습니다.

인터페이스 구성 모드에서 인터페이스를 종료하거나 활성화하려면 다음 명령을 사용하십시오.

| 명령 | 기술 |
|---|---|
| **shutdown** | no shutdown |
| **no shutdown** | no shutdown |

사용할 수있는 show interface 명령과 show 실행-구성 인터페이스가 종료되었는지 여부를 확인하는 명령을 종료된 인터페이스는 show interface 명령을 출력에 'administratively down'으로 표시됩니다. 자세한 내용은 '인터페이스 종료 예제'의 다음 예제를 참조하십시오.

## 13.3. 논리 인터페이스 구성

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

- 널 인터페이스 구성
- 루프백 인터페이스 구성.
- 집계 인터페이스 구성
- VLAN 인터페이스 구성

### 13.3.1. Null 인터페이스 구성

전체 시스템은 하나의 null 인터페이스 만 지원합니다. 그 기능은 대부분의 운영 체제에서 적용되는 널 (null) 장치의 기능과 유사합니다. null 인터페이스는 항상 사용할 수 있지만 통신 정보를 전송하거나 수신하지 않습니다. 인터페이스 구성 명령 no ip unreachable 은 널 인터페이스에서 사용할 수있는 유일한 명령입니다. null 인터페이스는 통신을 필터링하는 선택적 메소드를 제공합니다. 즉, 원하지 않는 네트워크 통신을 널 (null) 인터페이스로 라우트 할 수 있습니다. null 인터페이스는 액세스 제어 목록으로 기능할 수 있습니다.

전역 구성 모드에서 다음 명령을 실행하여 null 인터페이스를 지정할 수 있습니다.

| 명령 | 기술 |
|---|---|
| **interface null** *0* | null 인터페이스 구성 상태로 전환합니다. |

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

ip route 192.168.20.0 255.255.255.0 null 0

### 13.3.2. Loopback 인터페이스 구성

루프백 인터페이스는 논리 인터페이스입니다. 외부 인터페이스가 종료된 경우에도 BGP 세션은 항상 작동하고 계속됩니다. 루프백 인터페이스는 BGP 세션의 터미널 주소로 사용될 수 있습니다. 다른 스위치가 루프백 인터페이스에 도달하려고 하면 루프백 인터페이스 주소로 경로를 Broadcasting 하도록 동적 라우팅 프로토콜을 구성해야 합니다. 루프백 인터페이스로 라우팅 된 메시지는 스위치로 재 라우팅되어 로컬에서 처리될 수 있습니다. 루프백 인터페이스로 라우팅되지만 대상이 루프백 인터페이스의 IP 주소가 아닌 경우, 해당 메시지는 삭제됩니다. 이것은 루프백 인터페이스가 널 (null) 인터페이스로서 기능함을 의미합니다.

전역 구성 모드에서 다음 명령을 실행하여 루프백 인터페이스를 지정하고 인터페이스 구성 상태를 입력하십시오.

| 명령 | 기술 |
|---|---|
| **interface loopback** *number* | 루프백 인터페이스 구성 상태를 입력하십시오 |

### 13.3.3. Aggregation 인터페이스 구성

단일 이더넷 인터페이스의 부적절한 대역폭으로 인해 집합 인터페이스가 탄생합니다. 동일한 속도로 여러 개의 전 이중 인터페이스를 묶어서 대역폭을 크게 향상시킬 수 있습니다. 집계 인터페이스를 정의하려면 다음 명령을 실행하십시오.

| 명령 | 기술 |
|---|---|
| **Interface port-aggregator** *number* | 집계 인터페이스 구성 |

### 13.3.4. VLAN 인터페이스 구성

VLAN 인터페이스는 스위치의 라우팅 인터페이스입니다. 글로벌 구성 모드의 VLAN 명령은 대상 주소가 VLAN 에있는 IP 패킷을 처리하는 방법을 정의하지 않고 계층 2 VLAN 만 시스템에 추가합니다. VLAN 인터페이스가 없으면 이러한 종류의 패킷이 삭제됩니다.

VLAN 인터페이스를 정의하려면 다음 명령을 실행하십시오.

| 명령 | 기술 |
|---|---|
| **Interface vlan** *number* | VLAN 인터페이스를 구성합니다 |

### 13.3.5. 슈퍼 VLAN 인터페이스 구성

슈퍼 VLAN 기술은 다음과 같은 메커니즘을 제공합니다. 동일한 스위치의 다른 VLAN 에있는 호스트를 동일한 IPv4 서브넷에 할당하고 동일한 기본 게이트웨이를 사용할 수 있습니다. 따라서

많은 IP 주소가 저장됩니다. Super VLAN 기술은 VLAN 이 동일한 관리 인터페이스를 사용하고 호스트가 동일한 IPv4 네트워크 섹션과 게이트웨이를 사용하는 그룹에 다른 VLAN 을 배치합니다. Super VLAN 에 속한 VLAN 을 SubVLAN 이라고합니다. SubVLAN 은 IP 주소를 구성하여 관리 인터페이스를 소유할 수 없습니다.

명령 줄을 통해 Super VLAN 인터페이스를 구성할 수 있습니다. Super VLAN 인터페이스를 구성하는 절차는 다음과 같습니다.

| **명령** | **기술** |
|---|---|
| [**no**] **interface supervlan** *index* | Super VLAN 인터페이스 구성 모드로 들어갑니다. 지정된 수퍼 VLAN 인터페이스가 존재하지 않으면 시스템은 수퍼 VLAN 인터페이스를 생성합니다.<br>**index** 는 Super VLAN 인터페이스의 색인입니다. 유효 값의 범위는 1 에서 32 사이입니다.<br>슈퍼 VLAN 인터페이스를 삭제할 수 없습니다 . |
| [**no**] **subvlan** [*setstr*] [**add** *addstr*] [**remove** *remstr*] | 슈퍼 VLAN 에서 SubVLAN 을 구성합니다. 추가된 하위 VLAN 은 관리 인터페이스를 소유할 수 없거나 다른 수퍼 VLAN 에 속할 수 없습니다. 원래 상태에서 Super VLAN 에는 Sub VLAN 이 포함되어 있지 않습니다. 매 서브 명령 하나만 사용할 수 있습니다.<br><br>**setstr** 은 Sub VLAN 목록을 구성하는 것을 의미합니다. 예를 들어 List 2,4-6 은 VLAN 2, 4, 5 및 6 을 나타냅니다.<br><br>**add** 는 원래의 SubVLAN 목록에 VLAN 목록을 **추가**하는 것을 의미합니다. **addstr** 은 위와 같은 형식의 문자열을 의미합니다.<br><br>**제거**는 원래의 SubVLAN 목록에서 VLAN 목록을 삭제하는 것을 의미합니다. remstr 는 위와 같은 형식의 목록의 문자열입니다.<br><br>SuperVLAN 에서 모든 SubVLAN 을 삭제할 수 없습니다. |

인터페이스를 구성한 후 Super VLAN 인터페이스의 IP 주소를 구성할 수 있습니다. Super VLAN 인터페이스는 다른 포트와 마찬가지로 구성할 수 있는 라우팅 포트이기도 합니다.

# 14. 인터페이스 구성 예

## 14.1. 공용 속성의 인터페이스 구성

### 14.1.1. 인터페이스 설명 예

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

```
interface vlan 1
ip address 192.168.1.23 255.255.255.0
```

### 14.1.2. 인터페이스 종료 예제

다음 예에서는 interface GigaEthernet 0/1 을 종료하는 방법을 보여줍니다.

```
interface GigaEthernet0/1
shutdown
```

다음 예제에서는 인터페이스를 활성화하는 방법을 보여줍니다.

```
interface GigaEthernet0/1
no shutdown
```

## 14.2. 인터페이스 구성 명령

다음은 인터페이스 설정 명령어입니다:

- Interface
- description
- bandwidth
- delay
- shutdown
- show interface
- show running-config interface

### 14.2.1. 인터페이스

#### (1) 구문

**[no] interface** *port*
인터페이스 설정 모드로 들어가기 위한 명령어입니다. 논리 포트가 존재하지 않는 경우 먼저 생성한 후에 포트 모드로 진입해야 합니다. 물리 포트가 존재하지 않으면 명령어 실행이 실패합니다.

`no interface` 명령어는 물리 포트와 논리 포트에 따라 다르게 동작합니다.

- `no interface 물리포트` → 물리 포트를 기본 설정으로 되돌립니다.
- `no interface 논리포트` → 논리 포트를 삭제합니다.

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *Port* | 존재하는 물리 또는 논리 포트를 나타냅니다. |

**(3) 기본값**

기본 모드는 포트 모드가 아닙니다.

**(4) 사용지침**

이 명령어는 설정 모드에서 실행됩니다. 명령어 실행 후 포트 설정 모드에 들어가야 합니다. 포트 설정을 마친 후에는 `exit` 명령어를 사용하여 포트 모드에서 나갈 수 있습니다.

**(5) 예제**

다음 예제는 포트 G0/1 의 포트 모드로 진입하는 방법을 보여줍니다.
Switch_config#
Switch_config#interface gigaEthernet0/1
Switch_config_g0/1#exit
Switch_config#

### 14.2.2. Description

**(1) 구문**

**[no] description** *line*
포트의 설명 정보를 설정하려면 위에 언급된 명령어를 실행하십시오.

(2) **매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *Line* | 설명 정보의 문자열을 나타내며, 공백이 포함될 수 있습니다 |

**(3) 기본값**

기본적으로 설명 정보가 없습니다.

**(4) 사용지침**

이 명령어는 포트 설정 모드에서 설정됩니다.

**(5) 예제**

다음 예제는 포트 G0/1 의 설명 정보를 "uplink"로 설정하는 방법을 보여줍니다.

Switch_config# interface gigaEthernet0/1
Switch_config_g0/1# description uplink

### 14.2.3. Bandwidth

**(1) 구문**

**[no] bandwidth** *kilobps*
포트의 대역폭을 설정하려면 위 명령어를 실행하십시오.

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *Kilobps* | 포트의 대역폭(kbps)으로, 1 에서 10,000,000 kbps 범위 내에서 설정 가능합니다 |

**(3) 기본값**

100M 포트, 기가비트 포트, 10G 포트 및 100G 포트의 기본 대역폭은 각각 100,000 kbps, 1,000,000 kbps, 10,000,000 kbps 및 100,000,000 kbps 입니다.

**(4) 사용지침**

이 명령어는 포트 설정 모드에서 설정됩니다.

참고:

설정된 대역폭은 실제 포트 대역폭이 아니라, 일부 프로토콜에서 포트 비용을 계산하는 데 사용됩니다

**(5) 예제**

다음 예제는 포트 G0/1 의 대역폭을 10,000,000 kbps 로 설정하는 방법을 보여줍니다.

Switch_config # interface gigaEthernet0/1
Switch_config_g0/1# bandwidth 10000000

### 14.2.4. Delay

**(1) 구문**

**[no] delay** *tensofmicroseconds*
포트의 지연 시간을 설정하려면 위 명령어를 실행하십시오.

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *tensofmicroseconds* | 포트 지연 시간으로, 1~10,000,000 (10 마이크로초 단위) 범위에서 설정할 수 있습니다 |

**(3) 기본값**

기본 지연 시간은 1 입니다.

**(4) 사용지침**

이 명령어는 포트 설정 모드에서 설정됩니다.

**(5) 예제**

다음 예제는 포트 G0/1 의 지연 시간을 10 으로 설정하는 방법을 보여줍니다.

Switch_config_g0/1# delay 10

### 14.2.5. Shutdown

**(1) 구문**

**[no] shutdown**
포트를 비활성화하려면 shutdown, 다시 활성화하려면 no shutdown 을 실행하십시오.

**(2) 매개변수**

해당 없음 N/A

**(3) 기본값**

기본적으로 물리적 포트는 활성화된 상태입니다.

**(4) 사용지침**

이 명령어는 포트 모드에서 포트를 활성화하거나 비활성화하는 데 사용됩니다.

**(5) 예제**

다음 예제는 포트 G0/1 을 활성화하는 방법을 보여줍니다.

```
Switch_config_g0/1#
Switch_config_g0/1# no shutdown
Switch_config_g0/1#
```

### 14.2.6. Show interface

**(1) 구문**

**show interface** *〈port〉*
포트 상태를 확인하려면 위 명령어를 실행하십시오.

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *Port* | 특정 인터페이스의 이름을 나타냅니다. 특정 포트를 입력하지 않으면 모든 포트의 상태가 표시됩니다. |

**(3) 기본값**

해당 없음 N/A

**(4) 사용지침**

이 명령어는 EXEC 및 설정 모드에서 사용 가능하며, 포트의 물리적 상태 및 패킷 수신 통계를 확인하는 데 사용됩니다.

**(5) 예제**

다음 예제는 포트 G0/1 의 정보를 표시하는 방법을 보여줍니다:

```
Switch_config# show interface gigaEthernet 0/1
GigaEthernet0/1 is administratively down, line protocol is down
 Hardware is Giga-Combo-FX, address is 5491.af10.d083 (bia
5491.af10.d083)
 MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec
 Encapsulation ARPA
 Auto-duplex,  Auto-speed
 flow-control off
 5 minutes input rate 0 bits/sec, 0 packets/sec
 5 minutes output rate 0 bits/sec, 0 packets/sec
   Received 0 packets, 0 bytes
   0 broadcasts, 0 multicasts
   0 discard, 0 error, 0 PAUSE
   0 align, 0 FCS, 0 symbol
   0 jabber, 0 oversize, 0 undersize
   0 carriersense, 0 collision, 0 fragment
   0 L3 packets, 0 discards, 0 Header errors
   Transmited 0 packets, 0 bytes
   0 broadcasts, 0 multicasts
   0 discard, 0 error, 0 PAUSE
   0 sqettest, 0 deferred
   0 single, 0 multiple, 0 excessive, 0 late
   0 L3 forwards
```

### 14.2.7. Show running config interface

**(1) 구문**

**show running-config interface** *port*
포트 설정을 확인하려면 위 명령어를 실행하십시오.

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *Port* | 기존 포트를 나타냅니다. |

**(3) 기본값**

해당 없음 N/A

**(4) 사용지침**

이 명령어는 EXEC 또는 설정 모드에서 실행하여 포트 설정을 확인할 수 있습니다.

**(5) 예제**

다음 예제는 포트 G0/1 의 설정을 표시하는 방법을 보여줍니다:

```
Switch_config#show running-config interface g0/1
Building configuration...

Current configuration:
!
interface GigaEthernet0/1
 shutdown
 description uplink
 bandwidth 10000000
 delay 10
Switch_config#
```

## 14.3. 설정 예제

다음 예제는 VLAN 포트를 생성하고, 설명 정보 및 IP 주소를 설정한 후, 해당 포트의 상태와 설정을 확인하는 방법을 보여줍니다.

```
Switch_config#
Switch_config# interface vlan1
Switch_config_v1# description uplink
Switch_config_v1#
Switch_config_v1# ip address 192.168.1.1 255.255.255.0
Switch_config_v1# exit
Switch_config#
Switch_config# show running-config interface vlan1
```

```
Building configuration...
Current configuration:
!
interface VLAN1
 description uplink
 ip address 192.168.1.1 255.255.255.0
Switch_config# show interface vlan1
```

위 명령어를 실행하면 VLAN1 포트의 상태와 설정을 확인할 수 있습니다.

```
 Description uplink
 Hardware is EtherSVI, Address is 5491.afe4.d06a (5491.afe4.d06a)
 Interface address is 192.168.1.1/24
 MTU 1500 bytes, BW 1000000 kbit, DLY 2000 usec
 Encapsulation ARPA
 ARP type: ARPA, ARP timeout 04:00:00
 Peak input rate 0 pps, output 0 pps
   0 packets input, 0 bytes
   Received 0 broadcasts, 0 multicasts
   0 mpls unicasts, 0 mpls multicasts, 0 mpls input discards
   0 input errors, 0 input discards
   0 packets output, 0 bytes
   Transmited 0 broadcasts, 0 multicasts
   0 mpls unicasts, 0 mpls multicasts, 0 mpls output discards
   0 output errors, 0 discards
Switch_config#
```

# 15. 인터페이스 범위 구성

## 15.1. 인터페이스 범위 구성

### 15.1.1. 인터페이스 범위의 이해

인터페이스를 구성하는 과정에서 같은 유형의 포트에 동일한 속성을 구성해야 하는 경우가 있습니다. 각 포트에서 반복되는 구성을 피하기 위해 인터페이스 범위 구성 모 드를 제공합니다. 동일한 구성 매개변수로 동일한 유형 및 슬롯 번호/포트를 구성할 수 있습니다. 이렇게 하면 작업량이 줄어 들게 됩니다.

Note:
인터페이스 범위 모드로 들어가면 모드에 포함된 인터페이스가 구성되어야 합니다.

### 15.1.2. 인터페이스 범위 모드로 들어가기

'interface range' 모드로 들어가기 위해 다음 명령어를 실행하십시오.

| 명령 | 기술 |
|---|---|
| Interface range type slot/〈port1 - port2 \| port3〉[ , 〈port1 - port2\|port3〉] | 인터페이스 범위 모드로 시작합니다.<br><br>이 모드에 포함된 모든 포트는 다음 조건에 일치합니다.<br><br>슬롯 번호는 슬롯으로 구성됩니다.<br>하이픈 앞뒤의 포트 번호는 port1 과 port2 사이이거나 port3 과 같아야 합니다. Port2 는 port1 보다 작아야 합니다. 하이픈 또는 쉼표 앞 뒤에 공백이 있어야 합니다. |

### 15.1.3. 구성 예제

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

Switch_config# interface range giga1 - 3,6,8,10 - 12
Switch_config_if_range#

# 16. 물리적인 인터페이스 특성 구성

## 16.1. 인터페이스 구성하기

이 절에서는 이더넷 인터페이스를 구성하는 방법에 대해 설명합니다. 스위치는 10/100/1000Mbps 의 고속 이 더넷 인터페이스를 지원합니다. 자세한 구성은 다음과 같습니다.

첫 번째 단계는 필수 사항이며 다른 단계는 선택 사항입니다.

### 16.1.1. 이더넷 인터페이스 구성

전역모드에서 다음 명령을 실행하여 이더넷 인터페이스 구성 상태로 들어갑니다

| 명령 | 기술 |
|---|---|
| **interface gigaethernet** [*slot*/*port*] | Gigaethernet 인터페이스에 접속합니다 |
| **interface gigaethernet** [*slot*/*port*] | Gigaethernet 인터페이스에 접속합니다. |

show run interface gigaethernet' 명령어를 이용하여 이더넷 인터페이스의 상태를 확인하십시 오. 'show run interface gigaethernet' 명령어를 이용하여 기가비트 이더넷 인터페이스의 상태를 확인하십시오.

### 16.1.2. 속도 구성

이더넷 속도는 자동협상 또는 인터페이스에서 구성을 하여 구현할 수 있습니다

| 명령 | 기술 |
|---|---|
| **Speed {10\|100\|1000\|auto}** | 이더넷 인터페이스에 10M, 100M, 1000M 혹은 Auto-negotiation 의 옵션을 이용하여 Rate 값을 구 성 합니다 |
| **No speed** | Rate 옵션을 삭제합니다.<br>기본구성 auto-negotiation 으로 돌아갑니다. |

Note:
SFP 의 속도는 고정되어 있습니다. 예를 들어, GBIC 및 GE-FX 의 속도는 1000M 이고 FE-FX 의 속도는 100M 입니다. SFP 속도 명령 다음에 자동 매개변수가 있으면 자동 협상 기능을 사용할 수 있습니다. 그렇지 않으면 협상할 수 없습니다. 기본 구성에서는 기가비트 인터페이스의 자동 협상을 활성화할 수 있지만 100Mbps 인터페이스의 자동협상은 비활성화입니다.

### 16.1.3. 인터페이스에 흐름제어 구성하기

인터페이스가 Full-duplex 일 때, 흐름제어는 802.3x 정의하여 PAUSE 프레임을 통해 실현됩니다. 인터페이스가 반 이중 모드인 경우 Flow-control 은 배압을 통해 실현됩니다.

| 명령 | 기술 |
|---|---|
| **flow-control on/off** | 인터페이스의 Flow-control 을 실행하거나 끌 수 있습니다. |
| **no flow-control** | 기본 구성으로 돌아갑니다. 인터페이스에는 flow-control 이 없습니다. |

# 17. 보안 포트 구성

## 17.1. 개요

보안 포트의 액세스 기능을 제어하여 구성에 따라 포트를 특정 범위에서 실행할 수 있습니다. 포트의 보안 MAC 주소 수를 구성하여 포트의 보안 기능을 활성화한 경우. 보안 MAC 주소의 수가 상위 제한을 초과하고 MAC 주소가 안전하지 않으면 보안 포트 위반이 발생합니다. 다른 위반 모드에 따라 조치를 취해야합니다.

보안 포트에는 다음과 같은 기능이 있습니다.

- 보안 MAC 주소의 수를 구성합니다.
- 정적 보안 MAC 주소 구성

보안 포트에 정적 보안 MAC 주소가 없거나 고정 보안 MAC 주소의 수가 보안 MAC 주소의 번호보다 작은 경우 포트는 동적 MAC 주소를 학습합니다.

- 보안 포트 위반이 발생하면 위반 된 패킷 삭제

이 절에서는 스위치의 보안 포트를 구성하는 방법에 대해 설명합니다.

## 17.2. 보안 포트의 구성 작업

- 보안 포트모드로 구성합니다.
- 보안 포트의 정적 MAC 주소를 구성합니다.

## 17.3. 보안 포트의 구성하기

보안포트 구성 방법
정적 보안 포트 모드에는 수용 및 거부 두 가지가 있습니다. 수신 모드 인 경우 소스 주소가 로컬 MAC 주소와 동일한 흐름 만이 통신 포트로 수신될 수 있습니다. 리 젝트 모드 인 경우 소스 주소가 로컬 MAC 주소와 다른 흐름 만 포트에서 수신할 수 있습니다.

EXEC 모드에서 다음 명령을 실행하여 보안 포트 기능을 활성화 또는 비활성화합니다.

| 명령어 | 설명 |
|---|---|
| **configure** | 전역 구성모드로 진입합니다. |
| **interface** g0/1 | 포트 구성모드로 진입합니다. |
| **[no] switchport port-security mode static {accept \| reject}** | 보안 포트를 구성합니다. |
| **exit** | 전역 모드로 돌아갑니다. |

| | |
|---|---|
| **exit** | EXEC 모드로 돌아갑니다. |
| **write** | 구성을 저장합니다. |

**보안 포트의 고정 MAC 주소 구성하기**

보안 포트의 고정 MAC 주소를 구성한 후 수용 모드에서 소스 주소가 로컬 MAC 주소와 동일한 흐름을 포트에서 수신하여 통신할 수 있습니다. 거부 모드에서는 소스 주소가 로컬 MAC 주소와 다른 흐름을 포트에서 수신할 수 있습니다.

EXEC 모드에서 다음 명령을 실행하여 보안 포트의 정적 MAC 주소를 구성하십시오.

| 명령어 | 설명 |
|---|---|
| **configure** | 전역 구성모드로 진입합니다. |
| **interface** g0/1 | 포트 구성모드로 진입합니다. |
| **[no] switchport port-security static mac-address mac-addr** | 보안 포트를 구성합니다. |
| **exit** | 전역 모드로 돌아갑니다. |
| **exit** | EXEC 모드로 돌아갑니다. |
| **write** | 구성을 저장합니다. |

# 18. 포트 미러링 구성하기

## 18.1. 포트 미러링 작업 목록 구성

- 포트 미러링 구성하기
- 포트 미러링 정보 표시

## 18.2. 포트 미러링 구성 작업

## 18.3. 포트 미러링 구성

포트 미러링을 구성하면 스위치의 한 포트를 사용하여 포트 그룹의 트래픽을 관찰할 수 있습니다.
포트 미러링을 구성하려면 권한 모드로 들어가 다음 단계를 수행하십시오.

| 명령어 | 설명 |
|---|---|
| configure | 전역 구성모드로 진입합니다. |
| **mirror session** *session_number* {**destination** {**interface** *interface-id*} \| **source** {**interface** *interface-id* [, \| -] rx]} | 포트미러링을 구성합니다.<br>**session-number** 는 포트미러링의 수입니다.<br>**destination** 포트의 목적지입니다.<br>**source** 포트의 출발지입니다.<br>**Rx** 미러링 데이터를 넣는 것을 의미합니다. |
| **exit** | 관리 모드로 돌아갑니다. |
| **write** | 구성을 저장합니다. |

### 18.3.1. 포트 미러링 정보 표시

show 를 실행하여 포트 미러링의 구성 정보를 표시합니다

| 명령어 | 설명 |
|---|---|
| show mirror [session *session_number*] | 미러링포트의 구성정보를 표시합니다.<br><br>**session-number:**<br>미러링포트의 수를 나타냅니다. |

# 19. 802.1x 구성

## 19.1. 802.1x 구성 작업 목록

- 802.1x 포트 인증 구성
- 802.1x 재 인증 구성
- 802.1x 전송 주파수 구성
- 802.1x 포트에 대한 인증 유형 선택
- guest-vlan 구성하기
- 기본 802.1x 구성 다시 시작
- 802.1x 인증 구성 및 상태 모니터링

## 19.2. 802.1x 구성 작업

### 19.2.1. 802.1x 인증 구성

802.1x 는 포트에 대한 3 가지 제어 방법, 필수 인증 승인, 필수 인증 비 승인 및 802.1x 인증 시작을 정의합니다.

필수 인증 승인은 포트가 이미 인증을 통과했음을 의미합니다. 포트는 더 이상 인증을 필요하지 않으며, 모든 사용자는 포트를 통해 액세스 제어를 수행할 수 있습니다. 인증 방법은 포트에서 기본값으로 지정됩니다. 필수 인증 비 승인은 어떤 종류의 메소드가 적용되더라도 포트 인증이 통과되지 않음을 의미합니다. 사용자는 포트를 통해 데이터 액세스 제어를 수행할 수 없습니다.

802.1x 인증 시작은 포트가 802.1x 인증 프로토콜을 실행함을 의미합니다. 802.1x 인증은 포트에 액세스하는 사용자에게 적용됩니다. 인증을 통과한 사용자 만 포트를 통해 데이터 액세스 제어를 수행할 수 있습니다. 802.1x 인증이 시작되면 AAA 인증 방법을 구성해야 합니다.

802.1x 를 구성하기 전에 다음 명령을 실행하여 802.1x 기능을 활성화하십시오.

| 명령어 | 설명 |
| --- | --- |
| **dot1x enable** | 802.1x 기능을 활성화합니다. |

### 19.2.2. 802.1x 재 인증 구성

첫 번째 인증이 승인된 후 클라이언트는 특정 시간마다 인증되어 클라이언트의 적법성을 보장합니다. 이 경우 재 인증 기능을 활성화해야 합니다.

재 인증 기능이 활성화되면 802.1x 는 주기적으로 호스트에 인증 요청을 전송합니다. 다음 명령을 실행하여 재 인증 기능을 구성할 수 있습니다.

| 명령어 | 설명 |
|---|---|
| **dot1x re-authentication** | 재 인증 기능을 사용하십시오. |
| **dot1x timeout re-authperiod** *time* | 재 인증 기간을 구성합니다. |
| **dot1x reauth-max** *time* | 재 인증 실패 후 재 시도 시간을 구성합니다. |

### 19.2.3. 802.1x 전송 주파수 구성

802.1x 인증 과정에서 데이터 텍스트가 호스트로 전송됩니다. 데이터 전송은 802.1x 전송 주파수를 제어하여 호스트 응답이 성공적으로 이루어 지도록 조정할 수 있습니다.

다음 명령을 실행하여 전송 빈도를 구성하십시오.

| 명령어 | 설명 |
|---|---|
| **dot1x timeout tx-period** *time* | 802.1x 의 메시지 전송 빈도를 구성하십시오. |

### 19.2.4. 802.1x 포트에 대한 인증 유형 선택

802.1x 인증 유형을 선택할 수 있습니다. 802.1x 인증 유형은 AAA 가 Chap 인증 또는 Eap 인증을 사용하는지 여부를 결정합니다. Eap 인증은 md5-challenge 모드와 eap-tls 모드를 지원합니다. Chap 인증이 채택될 때 MD5 에서 요구되는 챌린지는 로컬에서 생성되는 반면, EAP 인증이 채택되면 챌린지는 인증 서버에서 생성됩니다. 각 포트는 하나의 인증 유형 만 채택합니다. 전역 구성의 인증 유형이 기본적으로 채택됩니다. 포트가 인증 유형으로 구성되면 No 명령을 실행하여 기본값을 다시 시작하지 않는 한 포트는 인증 유형을 사용합니다.

Eap-tls 는 전자 인증서를 인증 영장으로 사용하고 Transport Layer Security (tls)의 핸드 셰이크 규칙을 준수합니다. 따라서 높은 보안이 보장됩니다.

전역 구성 모드에서 다음 명령을 실행하여 인증 유형을 구성합니다.

| 명령어 | 설명 |
|---|---|
| **dot1x authen-type** {chap \| **eap**} | CHAP 또는 EAP 인증 방식을 선택하십시오. |

또한 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **dot1x authentication type** {**chap**\|**eap**} | 전역 모드에서 chap 또는 eap 또는 구성된 인증 유형을 선택하십시오. |

### 19.2.5. 802.1x 게스트 VLAN 구성

Guest-vlan 은 클라이언트가 응답하지 않을 때 관련 포트에 일부 액세스 권한 (예: 클라이언트 소프트웨어 다운로드)을 제공합니다. Guest-vlan 은 시스템에서 구성된 VLAN 일 수 있습니다. 구성된 guest-vlan 이 조건을 충족시키지 않으면 guest-vlan 에서 포트를 실행할 수 없습니다.

Note:
인증에 실패하면 액세스 권한이 없습니다.
전역 모드에서 다음 명령을 실행하여 guest-vlan 을 활성화합니다.

| 명령어 | 설명 |
|---|---|
| **dot1x guest-vlan** | 모든 포트에서 guest-vlan 을 활성화하십시오. |

각 포트에서 guest-vlan id 의 원래 값 이 0 이면 guest-vlan 이 전역 모드에서 활성화되어 있어도 guest-vlan 이 작동하지 않습니다. 포트 구성 모드에서 guest-vlan id 가 구성된 경우에만 guestvlan 이 작동할 수 있습니다.

포트 구성 모드에서 다음 명령을 실행하여 guest-vlan id 를 구성합니다.

| 명령어 | 설명 |
|---|---|
| **dot1x guest-vlan** {id (1-4094)} | 모든 포트에서 guest-vlan 을 활성화하십시오. |

### 19.2.6. 기본 802.1x 구성 다시 시작

모든 글로벌 구성을 기본 구성으로 다시 시작하려면 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **dot1x default** | 모든 글로벌 구성을 기본 구성으로 다시 시작합니다. |

### 19.2.7. 802.1x 인증 구성 및 상태 모니터링

802.1x 인증의 구성 및 상태를 모니터링하고 조정해야 하는 802.1x 매개 변수를 결정하려면 관리 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **show dot1x** {*interface* ….} | 802.1x 인증의 구성 및 상태를 모니터링합니다. |

# 20. POE (Power Over Ethernet) 설정 명령

## 20.1. POE Configuration Commands

### 20.1.1. show poe system

**(1) 구문**

이 명령어는 POE 관련 시스템 정보를 표시하는 데 사용됩니다.
show poe system

**(2) 매개변수**

해당 없음 (N/A)

**(3) 기본값**

해당 없음 (N/A)

**(4) 명령어 모드**

모니터링 모드 (Monitoring mode)

**(5) 사용 지침**

**POE DRIVER**: 칩 드라이버를 의미합니다.
**POE CHIP**: 상세한 칩 유형을 의미합니다.
**POE Port Num**: 최대 POE 포트 수를 의미합니다.
**PSE PowerManagement**: 전원 공급 장치 관리 모드(자동, 선점, 비선점)를 의미합니다.
**PSE Total Power**: 전원 공급 장치의 총 전력입니다.
**PSE Usage Threshold**: 전력 알람(백분율 기준 설정)입니다.
**PSE Alarm Power**: 전력 알람 임계값입니다.
**PSE Lower-Port-Disable Power**: 상대적으로 높은 우선순위를 가진 선점 포트의 전력 공급 임계값(자동 모드에서만 유효)입니다.
**PSE Lower-Port-NoConnect Power**: 동일 또는 낮은 우선순위 포트의 선점을 금지하는 전력 공급 임계값(자동 모드에서만 유효)입니다.
**PSE Consumed Power**: 사용된 전력 소비량입니다.
**PSE Peak Power**: 전원 공급 장치의 최대 전력(전력 통계 활성화 시 유효)입니다.
**PSE Mib Notification**: 포트의 전력 공급 상태 변경 시 MIB 알림이 발생합니다.
**PSE Temperature**: 칩의 온도를 나타냅니다.

**(6) 예제**

Switch#show poe system
POE DRIVER:PETH PD69012 DRV
POE CHIP:PD69012
POE Port Num:24
PSE PowerManagement:Preemptive
PSE Total Power:80000 mW
PSE Usage Threshold:80%
PSE Alarm Power:64000 mW
PSE Lower-Port-Disable Power:62000 mW
PSE Lower-Port-NoConnect Power:44000 mW
PSE Consumed Power:47500 mW
PSE Peak Power:101300 mW
PSE Mib Notification:Disable
PSE Temperature:38 degree

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.2. show poe all

**(1) 구문**

이 명령어는 POE 포트의 정보 설명 테이블을 표시합니다.
show poe all

**(2) 매개변수**

해당 없음 (N/A)

**(3) 기본값**

해당 없음 (N/A)

**(4) 명령어 모드**

모니터링 모드 (Monitoring mode)

**(5) 사용 지침**

포트 활성화/비활성화: 포트의 전원 공급을 활성화하거나 비활성화합니다.
포트 탐색 상태: 포트의 전원 공급 상태를 나타내며, 'disabled', 'searching-power', 'fault' 중 하나일 수 있습니다.

전원 공급 정상 상태:
'delivering-power'는 정상적으로 전원이 공급되고 있음을 의미합니다.

포트 페어:
포트의 전력선 정렬을 의미하며, 'signal'은 신호선을 통해, 'spare'는 예비선을 통해 전력을 공급함을 의미합니다.

포트 우선순위:
포트의 전원 공급 우선순위를 나타내며, 'critical', 'high', 'low' 순으로 우선순위가 높습니다.

**(6) 예제**

Switch#show poe all

| Port | Enable | Status | Pair | Priority |
|---|---|---|---|---|
| f0/3 | enabled | disabled | signal | low |
| f0/4 | enabled | disabled | signal | low |
| f0/2 | enabled | disabled | signal | low |
| f0/1 | enabled | disabled | signal | low |
| f0/5 | enabled | disabled | signal | low |
| f0/6 | enabled | disabled | signal | low |
| f0/7 | enabled | disabled | signal | low |
| f0/8 | enabled | disabled | signal | low |
| f0/9 | enabled | searching | signal | high |
| f0/10 | enabled | searching | signal | high |
| f0/11 | enabled | searching | signal | high |
| f0/12 | enabled | searching | signal | high |
| f0/13 | enabled | delivering-power | signal | high |
| f0/14 | enabled | searching | signal | high |
| f0/15 | enabled | delivering-power | signal | high |
| f0/16 | enabled | searching | signal | high |
| f0/17 | enabled | disabled | signal | low |
| f0/18 | enabled | disabled | signal | low |
| f0/19 | enabled | disabled | signal | low |
| f0/20 | enabled | disabled | signal | low |

```
f0/21  enabled   disabled          signal  low
f0/22  enabled   delivering-power  signal  low
f0/23  enabled   delivering-power  signal  low
f0/24  enabled   delivering-power  signal  critical
```

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.3. Show poe power

**(1) 구문**

이 명령어는 모든 포트의 전력 공급 정보를 표시하는 데 사용됩니다.
show poe power

**(2) 매개변수**

해당 없음 (N/A)

**(3) 명령어 모드**

모니터링 모드 (Monitoring mode)

**(4) 사용 지침**

**Max**: 포트의 최대 전력 제한값을 의미합니다.
**Current**: 포트의 현재 전력 값을 나타냅니다.
**Average**: 포트의 평균 전력(전력 통계 테이블이 활성화된 경우 유효)입니다.
**Peak**: 포트의 피크 전력(전력 통계가 활성화된 경우 유효)입니다.
**Bottom**: 포트의 최저 전력(전력 통계 테이블이 활성화된 경우 유효)입니다.

**(5) 예제**

```
Switch#show poe power
Port   Current   Max        Average   Peak      Bottom
f0/3   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/4   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/2   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/1   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/5   0 mW      30000 mW   0 mW      0 mW      0 mW
```

```
f0/6   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/7   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/8   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/9   0 mW      30000 mW   0 mW      0 mW      0 mW
f0/10  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/11  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/12  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/13  7600 mW   30000 mW   7620 mW   7800 mW   7600 mW
f0/14  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/15  7600 mW   30000 mW   7600 mW   7800 mW   7600 mW
f0/16  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/17  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/18  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/19  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/20  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/21  0 mW      30000 mW   0 mW      0 mW      0 mW
f0/22  15900 mW  30000 mW   15890 mW  16200 mW  14900 mW
f0/23  7700 mW   30000 mW   7780 mW   7800 mW   7700 mW
f0/24  8400 mW   30000 mW   9850 mW   22500 mW  6500 mW
```

**(6) 관련 명령어**

해당 없음 (N/A)

### 20.1.4. Show poe interface

**(1) 구문**

이 명령어는 지정된 포트의 POE 정보를 상세히 표시하는 데 사용됩니다.
show poe interface *type slot/port*

(2) 매개변수

| 매개변수 | 설명 |
|---|---|
| type | 인터페이스 유형 |
| slot | 슬롯 ID |
| port | 포트 ID |

**(3) 기본값**

해당 없음 (N/A)

**(4) 명령어 모드**

모니터링 모드 (Monitoring mode)

**(5) 사용지침**

PSE Port Number: 내부 포트의 ID 입니다.
Port Power Enabled: 포트의 전원 공급 활성화 여부입니다.
Port Force Power: 강제 전원 공급 또는 낮은 우선순위 포트의 전원 공급 활성화 여부입니다.
Port Detection Status: 포트의 전원 공급 상태(비활성화됨, 검색 중, 장애 등)입니다.
Port Fault Status: 포트의 오류 정보입니다.
Port Last Disconnection Reason: 포트의 마지막 전원 차단 원인입니다.
Port Pairs: 포트의 전력 공급 라인 순서(신호선 또는 예비선 사용)입니다.
Port IEEE Class: 포트의 IEEE 클래스입니다.
Port Priority: 포트의 전원 공급 우선순위(critical, high, low)입니다.
Port Current: 인터페이스의 현재 전류입니다.
Port Voltage: 포트의 현재 전압(일부 칩에서는 표시되지 않을 수 있음)입니다.
Port Current Power: 인터페이스의 현재 전력입니다.
Port Average Power: 포트의 평균 전력(전력 통계 활성화 시 유효)입니다.
Port Peak Power: 포트의 최대 전력(전력 통계 활성화 시 유효)입니다.
Port Bottom Power: 포트의 최저 전력(전력 통계 활성화 시 유효)입니다.
Port Max Power: 포트의 최대 전력 제한입니다.
Port PD Description: 포트에 연결된 PD(전력 장치)의 설명입니다.

**(6) 예제**

Switch#show poe interface f0/24
PSE Port Number: 23
Port Power Enabled: enable
Port Force Power: disable
Port Detection Status: delivering-power
Port Fault Status:
Port Last Disconnection Reason: Port was disabled
Port Pairs: signal
Port IEEE Class: 0
Port Priority: critical
Port Current: 163 mA
Port Current Power: 8400 mW
Port Average Power: 8440 mW

Port Peak Power: 22500 mW
Port Bottom Power : 6500 mW
Port Max Power : 30000 mW
Port PD Discription : AP

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.5. poe power management

**(1) 구문**

이 명령어는 스위치의 전력 공급 관리 모드를 설정하는 데 사용됩니다.
poe power-management {auto | preemptive | non-preemptive | lowDisable | lowNoConnect } *value*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| auto | 스위치의 전력 공급 관리 모드를 자동으로 설정합니다. |
| preemptive | 스위치의 전력 공급 관리 모드를 선점 모드로 설정합니다. |
| non-preemptive | 스위치의 전력 공급 관리 모드를 비선점 모드로 설정합니다. |
| lowDisable | 총 전력이 설정된 값 이상이면 포트에 전력이 공급되지 않습니다. 설정 값 이하일 때 다시 공급할수 있다. lowDisable = total power - value |
| lowNoConnect | 총 전력이 설정된 값 이상이면 우선순위가 가장 낮은 포트의 전원이 차단됩니다. supply.lowNoConnect = lowDisable - value |

**(3) 기본값**

기본적으로 전력 공급 관리 모드는 auto 입니다.

**(4) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(5) 사용 지침**

자동(Auto):

포트의 최대 전력 제한을 설정할 수 없으며, 기본적으로 칩이 지원하는 포트의 전력이 최대 전력으로 간주됩니다. 포트의 전원 공급 우선순위를 설정할 수 없으며, 기본 우선순위는 낮음(Low)으로 설정됩니다.

**선점(Preemptive):**
포트의 최대 전력 제한 기능을 활성화합니다. 포트의 전원 공급 우선순위를 활성화합니다.

**비선점(Non-preemptive):**
포트의 최대 전력 제한 기능을 활성화합니다. 포트의 전원 공급 우선순위를 활성화합니다.

**선점(Preempt) 모드:**
새로운 PD(Powered Device) 장치가 높은 우선순위의 전원 공급 포트에 연결될 경우, 해당 포트가 가득 찬 상태에서도 정상적으로 전원이 공급됩니다. 이와 동시에 가장 낮은 전원 공급 우선순위를 가진 포트는 전원이 차단됩니다.

**비선점(Non-preempt) 모드:**
높은 우선순위의 전원 공급 포트가 가득 찬 상태에서 PD 장치가 연결되면, 해당 포트에 PD 장치가 접근했음을 알립니다.

**(6) 예제**

다음 예제는 전원 공급 관리 모드를 선점(Preemptive)으로 설정하는 방법을 보여줍니다.
Switch_config#poe power-management preemptive
Switch_config#poe power-management lowDisable 18000
Switch_config#poe power-management lowNoConnect 18000

**(7) 관련 명령어**

poe max-power
poe priority

### 20.1.6. Poe led-time

**(1) 구문**

이 명령어는 PoE 모드에서 LED 의 지속 시간을 설정하는 데 사용됩니다.
poe led-time *time*
no poe led-time

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| time | 단위: 초(Seconds) |

**(3) 기본값**

PoE 모드에서 LED 의 지속 시간은 기본적으로 30 초입니다.

**(4) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(5) 사용 지침**

no poe led-time 명령어를 사용하면 LED 의 지속 시간을 기본값으로 되돌릴 수 있습니다.

**(6) 예제**

다음 예제는 LED 지속 시간을 10 초로 설정하는 방법을 보여줍니다.

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.7. Poe mib notification-stop

**(1) 구문**

전원 공급 변경 또는 전원 경보 발생 시 사용자에게 트랩(trap) 알림을 보내지 않도록 설정하려면 다음 명령어를 실행합니다:
poe mib notification-stop
no poe mib notification-stop

**(2) 매개변수**

해당 없음 (N/A)

**(3) 기본값**

기본 설정에서는 전원 공급이 변경되거나 전원 경보가 발생하면 시스템이 사용자에게 트랩(trap) 알림을 전송합니다.

**(4) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(5) 사용 지침**

이 명령어에 “no” 값을 사용하면 기본 설정으로 복원할 수 있습니다.

**(6) 예제**

다음 예제는 전원 공급 변경 또는 전원 경보 발생 시 트랩 알림을 중지하는 방법을 보여줍니다:
Switch_config#poe mib notification-stop

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.8. Poe pse-unprotect

**(1) 구문**

포트의 전원 공급 보호 기능을 설정하려면 다음 명령어를 실행합니다:
poe pse-unprotect
no poe pse-unprotect

**(2) 매개변수**

해당 없음 (N/A)

**(3) 기본값**

포트의 전원 공급 보호 기능은 기본적으로 활성화되어 있습니다.

**(4) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(5) 사용 지침**

이 명령어에 “no” 값을 사용하면 기본 설정으로 복원할 수 있습니다.

**(6) 예제**

다음 예제는 전원 공급 보호 기능을 비활성화하는 방법을 보여줍니다:
Switch_config# poe pse-unprotect

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.9. Poe counter value

**(1) 구문**

전역적으로 전력 통계를 활성화하려면 다음 명령어를 실행합니다:
poe counter *value*
no poe counter

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 샘플링 간격 (단위: 초). |

**(3) 기본값**

전력 통계 기능은 기본적으로 비활성화되어 있습니다.

**(4) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(5) 사용 지침**

이 명령어에 “no” 값을 사용하면 기본 설정으로 복원할 수 있습니다.

**(6) 예제**

다음 예제는 전력 통계의 샘플링 간격을 5 초로 설정하는 방법을 보여줍니다.
Switch_config# poe counter 5

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.10. Poe threshold

#### (1) 구문

전원 경보 임계값과 총 전력량 사이의 백분율을 설정하려면 다음 명령어를 실행합니다.
poe threshold value
no poe threshold

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| value | 전원 경보 임계값과 총 전력량 사이의 백분율 설정. |

#### (3) 기본값

기본값은 총 전력량의 100% 입니다.

#### (4) 명령어 모드

전역 설정 모드 (Global configuration mode)

#### (5) 사용 지침

이 명령어에 “no” 값을 사용하면 기본 설정으로 복원할 수 있습니다.

#### (6) 예제

다음 예제는 전원 경보 임계값을 총 전력량의 50%로 설정하는 방법을 보여줍니다:
Switch_config#poe threshold 50

#### (7) 관련 명령어

poe power-management

### 20.1.11. poe standard

#### (1) 구문

PSE(Power Sourcing Equipment) 전원 공급 표준을 설정하려면 다음 명령어를 실행합니다:
poe standard {AF| AT| MAX}

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| AF | AF 표준을 선택하면 포트당 최대 15.4W 까지 전력 공급 가능 |
| AT | AT 표준을 선택하면 포트당 최대 30W 까지 전력 공급 가능 |
| MAX | AF 및 AT 를 모두 지원하는 스위치에서는 AT 표준이 선택되며, AF 만 지원하는 스위치에서는 AF 표준이 선택됨 |

**(3) 기본값**

기본값은 MAX 입니다.

**(4) 명령어 모드**

전역 설정 모드 (Global configuration mode)

**(5) 사용 지침**

AF 표준 선택 시: 포트당 최대 15.4W 공급
AT 표준 선택 시: 포트당 최대 30W 공급
MAX 선택 시 AF 및 AT 를 지원하는 스위치: AT 표준 적용
AF 만 지원하는 스위치: AF 표준 적용.

**(6) 예제**

다음 예제는 PSE 전원 공급 표준을 AF 로 설정하는 방법을 보여줍니다.
Switch_config#poe standard AF

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.12. poe disable

**(1) 구문**

포트의 전원 공급을 비활성화하려면 다음 명령어를 실행합니다.

poe disable { time-range name | 〈cr〉}
no poe disable {time-range | 〈cr〉}

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| time-range name | 전원을 차단할 시간 범위(time range) 이름 |
| 〈cr〉 | poe disable 명령어만 입력하면 해당 포트의 전원을 즉시 차단 |

**(3) 기본값**

포트의 전원 공급은 기본적으로 활성화되어 있으며, 시간 제한 없이 전원을 공급합니다.

**(4) 명령어 모드**

인터페이스 설정 모드 (Interface configuration mode)

**(5) 사용 지침**

poe disable → 포트의 전원 공급 차단
no poe disable → 포트의 전원 공급 활성화.

**(6) 예제**

다음 예제는 포트 f0/1 의 전원 공급을 비활성화하는 방법을 보여줍니다.
Switch_config_f0/1#poe disable

**(7) 관련 명령어**

time-range

### 20.1.13. poe max-power

**(1) 구문**

포트의 최대 전력 공급량을 설정하려면 다음 명령어를 실행합니다.
poe max-power value
no poe max-power

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| value | 포트의 최대 전력 (단위: mW) |

**(3) 기본값**

포트의 기본 최대 전력 공급량은 30000mW(30W) 입니다.

**(4) 명령어 모드**

인터페이스 설정 모드 (Interface configuration mode)

**(5) 사용 지침**

이 명령어에 "no"값을 사용하면 기본 최대 전력 공급량(30000mW)으로 복원할 수 있습니다.

**(6) 예제**

다음 예제는 포트 f0/1 의 최대 전력을 15000mW(15W)로 설정하는 방법을 보여줍니다.
Switch_config_f0/1#poe max-power 15000

**(7) 관련 명령어**

poe power-management

### 20.1.14. poe priority

**(1) 구문**

포트의 전력 공급 우선순위를 설정하려면 다음 명령어를 실행합니다
poe priority {critical | high | low }

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| critical | 가장 높은 우선순위 |
| high | 높은 우선순위 |
| low | 가장 낮은 우선순위 |

**(3) 기본값**

포트의 전력 공급 기본 우선순위는 "low"입니다.

**(4) 명령어 모드**

인터페이스 설정 모드 (Interface configuration mode)

**(5) 사용 지침**

해당 없음 (N/A)

**(6) 예제**

다음 예제는 포트 f0/1 의 전력 공급 우선순위를 "critical"로 설정하는 방법을 보여줍니다.
Switch_config_f0/1#poe priority critical

**(7) 관련 명령어**

poe power-management

### 20.1.15. poe PD discription

**(1) 구문**

포트 설명(PD 장치 설명)을 설정하려면 다음 명령어를 실행합니다.
poe PD-discription string
no poe PD-discription

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| string | 포트 설명(문자열) |

**(3) 기본값**

기본값은 비어 있음(null).

**(4) 명령어 모드**

인터페이스 설정 모드 (Interface configuration mode)

(5) **사용 지침**

이 명령어에 “no”값을 사용하면 포트 설명을 삭제할 수 있습니다.

**(6) 예제**

다음 예제는 포트 설명을 "AP-1"로 설정하는 방법을 보여줍니다.
Switch_config_f0/1#poe PD-discription AP-1

**(7) 관련 명령어**

해당 없음 (N/A)

### 20.1.16. poe force-power

**(1) 구문**

강제 전원 공급을 설정하려면 다음 명령어를 실행합니다.
poe force-power
no poe force-power

**(2) 매개변수**

해당 없음 (N/A)

**(3) 기본값**

기본적으로 강제 전원 공급은 비활성화되어 있습니다.

**(4) 명령어 모드**

인터페이스 설정 모드 (Interface configuration mode)

**(5) 사용 지침**

이 명령어에 “no”값을 사용하면 강제 전원 공급을 비활성화할 수 있습니다.

**(6) 예제**

다음 예제는 PoE 포트의 강제 전원 공급을 설정하는 방법을 보여줍니다.

**(7) 관련 명령어**

poe power-management

# 21. VLAN 구성

## 21.1. VLAN 개요

가상 LAN (VLAN)은 하나 이상의 LAN 에있는 논리적으로 네트워크화 된 장치 그룹을 말하며 실제로 동일한 와이어에 연결되어 있는 것처럼 통신할 수 있습니다. 실제로 여러 LAN 세그먼트에 위치합니다. 1999 년 IEEE 는 VLAN 구현 프로젝트를 표준화하기 위해 IEEE 802.1Q 프로토콜 표준 초안을 구성했습니다. VLAN 은 물리적 연결 대신 논리에 기반하기 때문에 사용자/호스트 관리, 대역폭 할당 및 리소스 최적화에 매우 유연합니다.

가상 LAN 에는 다음과 같은 유형이 있습니다.

- 포트 기반 VLAN: 각 물리적 스위치 포트는 VLAN 세트의 구성원 자격을 지정하는 액세스 목록으로 구성됩니다.
- 인터페이스에서 802.1Q 트렁크 모드가 지원됩니다.
- 액세스 모드 인터페이스가 지원됩니다.

포트 기반 VLAN 은 스위치가 지원하는 VLAN 의 하위 집합 중 하나에 포트를 할당하는 것입니다. 이 VLAN 하위 집합에 하나의 VLAN 만 있는 경우이 포트는 액세스 포트입니다. 이 VLAN 하위 집합에 여러 개의 VLAN 이있는 경우이 포트는 트렁크 포트입니다. 여러 VLAN 중 하나의 기본 VLAN 이 있으며 VLAN ID 는 포트 VLAN ID (PVID)입니다.

- Vlan 허용 범위는 인터페이스에서 지원됩니다.

VLAN 허용 매개 변수는 포트가 속한 VLAN 범위를 제어하는 데 사용됩니다. VLAN 태그 없는 매개 변수는 해당 VLAN 에 VLAN 태그가 없는 패킷을 보내도록 포트를 구성하는 데 사용됩니다.

## 21.2. VLAN 구성 작업 목록

- VLAN 추가/삭제
- 스위치 포트 구성
- VLAN 인터페이스 생성/삭제
- VLAN 의 구성 및 상태 모니터링

## 21.3. VLAN 구성 작업

### 21.3.1. VLAN 추가/삭제

일반적으로 VLAN 이라고하는 가상 LAN 은 실제 위치에 상관없이 동일한 회선에 연결되어 있는 것처럼 통신하는 공통 요구 사항 집합을 가진 호스트 그룹입니다. VLAN 은 물리적 LAN 과 동일한 속성을 갖지만 동일한 LAN 세그먼트에 있지 않더라도 종단 스테이션을 함께 그룹화 할 수 있습니다. VLAN 에는 여러 개의 포트가 있을 수 있으며 모든 유니 캐스트, 멀티 캐스트 및 브로드 캐스트 메시지는 동일한 VLAN 에서 터미널로만 전달될 수 있습니다. 각 VLAN 은 논리 네트워크입니다. 데이터가 다른 VLAN 에 도달하려면 라우터 또는 브리지에 의해 전달되어야 합니다.

다음 명령을 실행하여 VLAN 을 구성합니다

| 명령어 | 설명 |
|---|---|
| **vlan** vlan-id | VLAN 구성 모드로 들어갑니다. |
| **name** str | vlan 구성 모드의 이름 |
| **exit** | vlan 구성 모드를 종료하고 vlan 을 구성합니다. |
| **vlan** vlan-range | 동시에 여러 VLAN 을 구성합니다. |
| **no vlan** vlan-id \| vlan-range | 하나 이상의 VLAN 을 삭제하십시오. |

vlan 은 VLAN 관리 프로토콜 GVRP 를 통해 동적 추가 및 삭제를 수행할 수 있습니다.

### 21.3.2. 스위치 포트 구성

스위치 포트는 액세스 모드, 트렁크 모드 및 dot1q 터널 모드와 같은 모드를 지원합니다.

- 액세스 모드는 이 포트가 하나의 VLAN 에만 종속되며 태그가 없는 이더넷 프레임 만 송수신 함을 나타냅니다
- 트렁크 모드는 이 포트가 다른 스위치에 연결되어 있고 태그가 있는 이더넷 프레임을 송수신 할 수 있음을 나타냅니다.
- dot1q-tunnel 모드는 수신되지 않은 패킷을 비 태그 방식으로 수신합니다. 스위치 칩은 자동으로 포트의 pvid 를 새로운 태그로 추가하므로 스위치가 네트워크에 연결된 다른 VLAN 파티션을 무시할 수 있습니다. 그런 다음 패킷은 동일한 고객의 다른 서브 네트워크에 있는 다른 포트로 변경없이 전달됩니다. 투명 전송은 이러한 방식으로 실현됩니다.

각 포트에는 하나의 기본 vlan 및 pvid 가 있으며 포트에서 수신된 vlan 태그가없는 모든 데이터는 vlan 의 데이터 패킷에 속합니다.

트렁크 모드는 포트를 여러 VLAN 으로 간주할 수 있으며 전달할 패킷 종류와 포트에 전송된 패킷에 태그가 있거나 태그가없는 패킷 수 및 포트가 속한 VLAN 목록을 구성할 수 있습니다.

다음 명령을 실행하여 스위치 포트를 구성하십시오.

| 명령어 | 설명 |
|---|---|
| **switchport pvid** *vlan-id* | 스위치 포트의 pvid 를 구성하십시오 |
| **switchport mode access\|trunk\|dot1q-tunnel** | 스위치의 포트 모드를 구성하십시오. |
| **switchport trunk vlan-allowed …** | 스위치 포트의 VLAN 허용 범위를 구성합니다. |
| **switchport trunk vlan-untagged …** | 스위치 포트의 VLAN 태그없는 범위를 구성합니다. |

참고:
일부 스위치는 dot1q-tunnel 기능을 지원하지 않습니다. 일부 스위치는 이 기능을 전역 적으로 활성화/비활성화하는 기능 만 지원하며 다른 포트에 대해 다른 정책을 구성할 수 없습니다

### 21.3.3. VLAN 인터페이스 생성/삭제

vlan 인터페이스는 네트워크 관리 또는 계층 3 라우팅 기능을 구현하기 위해 구성할 수 있습니다. vlan 인터페이스는 IP 주소와 마스크를 지정하는 데 사용될 수 있습니다. 다음 명령을 실행하여 VLAN 인터페이스를 구성하십시오.

| 명령어 | 설명 |
|---|---|
| **[no] interface vlan** *vlan-id* | VLAN 인터페이스 생성/삭제. |

### 21.3.4. 슈퍼 VLAN 인터페이스 구성

슈퍼 VLAN 기술은 다음과 같은 메커니즘을 제공합니다. 동일한 스위치를 실행하는 다른 VLAN 의 호스트를 동일한 IPv4 서브넷에 할당할 수 있습니다. 따라서 많은 IP 주소가 저장됩니다. Super VLAN 기술은 서로 다른 VLAN 을 하나의 그룹으로 분류합니다. 이 그룹의 VLAN 은 동일한 관리 인터페이스를 사용합니다. 그룹의 호스트는 동일한 IPv4 네트워크 섹션과 게이트웨이를 사용합니다. Super VLAN 에 속한 VLAN 을 SubVLAN 이라고합니다. SubVLAN 은 IP 주소를 구성하여 관리 인터페이스를 소유할 수 없습니다.

명령 줄을 통해 Super VLAN 인터페이스를 구성할 수 있습니다. Super VLAN 인터페이스를 구성하는 절차는 다음과 같습니다.

| 명령어 | 설명 |
|---|---|
| **[no] interface supervlan** *index* | 인터페이스 구성 모드를 시작합니다. 지정된 수퍼 VLAN 인터페이스가 없으면 시스템에서 수퍼 VLAN 인터페이스를 만듭니다.<br><br>**index** 는 슈퍼 VLAN 인터페이스의 색인입니다. 유효 값의 범위는 1 에서 32 사이입니다.<br><br>**no** 는 슈퍼 VLAN 인터페이스를 삭제하는 것을 의미합니다. |

| | |
|---|---|
| [**no**] **subvlan** [*setstr*] [**add** *addstr*] [**remove** *remstr*] | Super VLAN 에서 SubVlan 을 구성합니다. 추가된 하위 VLAN 은 관리 인터페이스를 소유할 수 없습니다. 원래 상태에서는 Super VLAN 에 Sub VLAN 이 포함되지 않습니다. 매번 하나의 하위 명령 만 사용할 수 있습니다.<br><br>**setstr** 은 Sub VLAN 목록을 구성하는 것을 의미합니다. 예를 들어 List 2,4-6 은 VLAN 2, 4, 5 및 6 을 나타냅니다.<br><br>**add** 는 원래의 SubVLAN 목록에 VLAN 목록을 추가하는 것을 의미합니다. **addstr** 은 위와 같은 형식의 문자열을 의미합니다.<br><br>**remove** 는 원래의 SubVLAN 목록에서 VLAN 목록을 삭제하는 것을 의미합니다. remstr 는 위와 같은 형식의 목록의 문자열입니다.<br><br>SuperVLAN 에서 모든 SubVLAN 을 삭제할 수 없습니다. 어떤 명령은 다른 하위 명령과 함께 사용되지 않습니다. |

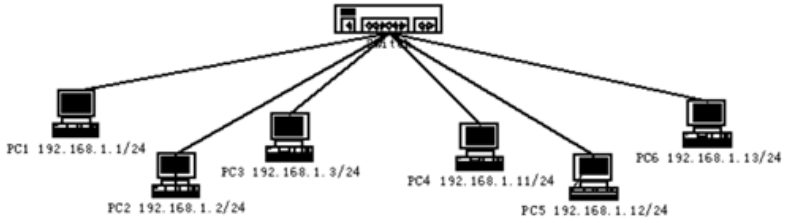
Super VLAN 인터페이스를 구성한 후 Super VLAN 인터페이스의 IP 주소를 구성할 수 있습니다. Super VLAN 인터페이스는 다른 포트와 마찬가지로 구성할 수있는 라우팅 포트이기도합니다.

### 21.3.5. VLAN 의 구성 및 상태 모니터링

VLAN 의 구성 및 상태를 모니터링하려면 EXEC 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **show vlan** [ **id** *x* \| **interface** *intf*] | VLAN 의 구성 및 상태를 표시합니다. |
| **show interface** {**vlan** \| **supervlan**} *x* | VLAN 포트의 상태를 표시합니다. |

## 21.4. 구성 예제



사용자 PC1 ~ PC6 은 포트 1 ~ 6 을 통해 스위치를 연결합니다. 이 PC 의 IP 주소는 네트워크 섹션 192.168.1.0/24 에 속합니다. PC1 ~ PC3 그룹과 PC4 ~ PC6 그룹은 서로 다른 계층 2 브로드 캐스트 도메인에 위치하지만 PC1 ~ PC6 은 서로 ping 을 수행하고 IP 주소 192.168.1.100 을 통해 스위치를 관리할 수 있습니다. 이렇게 하려면 포트 1 ~ 3 을 VLAN1 로, 포트 4 ~ 6 을 VLAN 2 로 구성해야 합니다. 그런 다음 SubVLAN 으로 VLAN 1 과 2 를 SuperVlan 에 추가해야 합니다. 스위치에서 다음 구성을 수행해야 합니다.

```
interface gigaethernet 0/4
switchport pvid 2
!
interface gigaethernet 0/5
switchport pvid 2
!
interface gigaethernet 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
```

# 22. Private VLAN

## 22.1. Private VLAN Configuration Commands

다음은 프라이빗 VLAN 을 설정하는 명령어입니다:

- private-vlan
- private-vlan association
- switchport mode private-vlan
- switchport private-vlan host-association
- switchport private-vlan mapping
- switchport private-vlan
- show vlan private-vlan
- show vlan private-vlan interface

### 22.1.1. Private-vlan

프라이머리 VLAN: 프라이빗 VLAN 에서 단 하나만 존재하며, 프로미스큐어스 포트와 연관됩니다.

아이솔레이티드 VLAN: 같은 VLAN 내의 포트 간 Layer 2 통신이 불가능합니다. 단 하나의 아이솔레이티드 VLAN 만 허용되며, 반드시 프라이머리 VLAN 과 연관되어야 합니다.

커뮤니티 VLAN: 같은 VLAN 내의 포트 간 Layer 2 통신이 가능하지만, 다른 커뮤니티 VLAN 의 포트와는 통신할 수 없습니다. 하나의 프라이빗 VLAN 에 여러 개의 커뮤니티 VLAN 이 존재할 수 있으며, 반드시 프라이머리 VLAN 과 연관되어야 합니다.

| 매개변수 | 설명 |
|---|---|
| *primary* | VLAN 을 프라이머리 VLAN 으로 설정합니다. |
| *community* | VLAN 을 커뮤니티 VLAN 으로 설정합니다. |
| *isolated* | VLAN 을 아이솔레이티드 VLAN 으로 설정합니다. |

**(1) 기본값**

기본적으로 프라이빗 VLAN 이 설정되지 않습니다.

**(2) 명령어 모드**

VLAN 설정 모드

**(3) 구문**

**private-vlan {primary|community|isolated}**
이 명령어는 프라이빗 VLAN 을 설정하는 데 사용됩니다.

**(4) 예제**

VLAN 2 를 프라이머리 VLAN 으로 설정하는 예제입니다.

Switch_config#
Switch_config#vlan 2
Switch_config_vlan2#private-vlan primary

### 22.1.2. Private-vlan association

이 명령어는 기본 VLAN 을 보조 VLAN 과 연결하여 전체 프라이빗 VLAN 에서 VLAN 학습 공유를 가능하게 합니다. 이 명령어는 기본 VLAN 설정 모드에서만 실행됩니다.

svlist 를 사용할 경우, 보조 VLAN 목록을 추가하거나 제거할 수 있습니다. 입력한 목록은 쉼표(,) 또는 하이픈(-)으로 구분됩니다. 예를 들어, "1, 3, 5, 7"은 "VLAN 1, VLAN 3, VLAN 5, VLAN 7"을 의미하며, "1, 3-5, 7"은 "VLAN 1, VLAN 3, VLAN 4, VLAN 5, VLAN 7"을 의미합니다.

전체 프라이빗 VLAN 의 유효성은 프라이빗 VLAN 의 모든 기능이 올바르게 설정되는 것에 따라 달라집니다.

| 매개변수 | 설명 |
|---|---|
| svlist | 연관될 세컨더리 VLAN 을 지정합니다. |

**(1) 기본값**

기본적으로 연관된 세컨더리 VLAN 이 없습니다.

**(2) 명령어 모드**

VLAN 설정 모드

**(3) 구문**

**private-vlan association {svlist | add svlist | remove svlist}**
**no private-vlan association**
이 명령어는 프라이빗 VLAN 의 연관 관계를 설정하는 데 사용됩니다.

**(4) 예제**

다음 예제는 기본 VLAN 2 를 커뮤니티 VLAN 3 및 커뮤니티 VLAN 4 와 연결하는 방법을 보여줍니다.

```
Switch_config#
Switch_config#vlan 2
Switch_config_vlan2#private-vlan association 3-4
```

### 22.1.3. Switchport mode private-vlan

이 명령어는 프라이빗 VLAN 에서 레이어 2 포트의 모드를 설정하는 데 사용됩니다. 모드는 다음과 같이 구분됩니다.

무차별 포트 (Promiscuous Port):
기본 VLAN(Primary VLAN)에 속합니다. 같은 프라이빗 VLAN 내에서 보조 VLAN(Secondary VLAN)의 격리된 포트(Isolated Port) 및 커뮤니티 포트(Community Port)를 포함한 모든 포트와 통신할 수 있습니다.

격리된 포트 (Isolated Port):
격리된 VLAN(Isolated VLAN)의 호스트 포트입니다. 동일한 프라이빗 VLAN 내에서 다른 포트와 완전히 L2 에서 격리됩니다. 무차별 포트와만 통신할 수 있으며, 다른 격리된 포트나 커뮤니티 포트와는 통신할 수 없습니다.

커뮤니티 포트 (Community Port):
커뮤니티 VLAN(Community VLAN)의 호스트 포트입니다.
동일한 커뮤니티 VLAN 내의 다른 커뮤니티 포트 또는 무차별 포트와 L2 통신이 가능합니다.
다른 커뮤니티 VLAN 의 포트나 격리된 VLAN 의 포트와는 통신할 수 없습니다.

| 매개변수 | 설명 |
|---|---|
| host | 레이어 2 포트를 호스트 포트 모드로 설정합니다. |
| promiscuous | 레이어 2 포트를 무차별 포트 모드로 설정합니다. |

**(1) 기본값**

기본적으로 어떤 프라이빗 VLAN 모드도 설정되지 않습니다.

**(2) 명령어 모드**

Port 설정 모드

**(3) 구문**

**switchport mode private-vlan {host | promiscuous}**

레이어 2 포트의 프라이빗 VLAN 모드를 설정하려면 위 명령어를 실행합니다.

**(4) 예제**

다음 예제는 인터페이스 g0/1 을 무차별 포트로 설정하는 방법을 보여줍니다:

Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous

### 22.1.4. Switchport private-vlan host association

이 명령어는 레이어 2 호스트 포트가 기본 VLAN 과 보조 VLAN 을 연계하도록 설정하는 데 사용됩니다. 새로 설정된 호스트 포트는 다음 조건이 충족되어야 정상적으로 동작합니다.

1. 해당 포트가 호스트 포트로 설정되어 있어야 합니다.
2. 두 VLAN 의 프라이빗 VLAN 유형이 올바르게 설정되어 있어야 합니다.
3. 기본 VLAN 과 보조 VLAN 간의 연계가 올바르게 설정되어 있어야 합니다.

| 매개변수 | 설명 |
|---|---|
| p_vid | 연계할 기본 VLAN (Primary VLAN) 의 VLAN ID 를 설정합니다. (범위: 1~4094) |
| s_vid | 연계할 보조 VLAN (Secondary VLAN)의 VLAN ID 를 설정합니다. (범위: 1~4094) |

**(1) 기본값**

기본적으로 어떤 프라이빗 VLAN 연계도 설정되지 않습니다.

**(2) 명령어 모드**

Port 설정 모드

**(3) 구문**

**switchport private-vlan host-association p_vid s_vid**

레이어 2 호스트 포트가 특정 프라이빗 VLAN 과 연계되도록 설정하려면 위 명령어를 실행합니다.

**(4) 예제**

다음 예제는 포트 g0/1 을 기본 VLAN 2 및 보조 VLAN 3 과 연계하는 방법을 보여줍니다.

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#switchport private-vlan host-association 2 3
```

### 22.1.5. Switchport private-vlan mapping

이 명령어는 레이어 2 무차별 포트가 기본 VLAN 과 보조 VLAN 을 연계하도록 설정하는 데 사용됩니다. 새로 설정된 포트는 다음 조건이 충족되어야 정상적으로 동작합니다.

1. 해당 포트가 무차별 포트로 설정되어 있어야 합니다.
2. 두 VLAN 의 프라이빗 VLAN 유형이 올바르게 설정되어 있어야 합니다.
3. 기본 VLAN 과 보조 VLAN 간의 연계가 올바르게 설정되어 있어야 합니다.

svlist 를 사용할 경우, 보조 VLAN 목록을 추가하거나 제거할 수 있습니다.
입력한 목록은 쉼표(,) 또는 하이픈(-)으로 구분됩니다.

예를 들어:
"1, 3, 5, 7" → "VLAN 1, VLAN 3, VLAN 5, VLAN 7"
"1, 3-5, 7" → "VLAN 1, VLAN 3, VLAN 4, VLAN 5, VLAN 7"

| 매개변수 | 설명 |
|---|---|
| *p_vid* | 연계할 기본 VLAN (Primary VLAN) 의 VLAN ID 를 설정합니다. (범위: 1~4094) |
| *svlist* | 연계할 보조 VLAN (Secondary VLAN)의 목록을 설정합니다. |

**(1) 기본값**

기본적으로 어떤 프라이빗 VLAN 연계도 설정되지 않습니다.

**(2) 명령어 모드**

Port 설정 모드

**(3) 구문**

**switchport private-vlan mapping**
**p_vid {svlist | add svlist | remove svlist}**

레이어 2 무차별 포트(promiscuous port)를 특정 프라이빗 VLAN 과 연계하려면 위 명령어를 실행합니다.

**(4) 예제**

다음 예제는 포트 g0/1 을 기본 VLAN 2 및 보조 VLAN 3~5와 연계하는 방법을 보여줍니다.

Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#switchport private-vlan mapping 2 3-5

### 22.1.6. Switchport private-vlan

이 명령어는 프라이빗 VLAN 에서 송출되는 패킷의 태그를 설정하거나, 태그 포함 여부를 결정하는 데 사용됩니다. 이 명령어는 다음 조건이 충족된 후에만 적용됩니다.

프라이빗 VLAN 이 올바르게 설정되어 있어야 합니다. 프라이빗 VLAN 도메인 내에서 VLAN 연계가 올바르게 설정되어 있어야 합니다. 프라이빗 VLAN 내에서 레이어 2 포트 모드가 올바르게 설정되어 있어야 합니다.

레이어 2 포트와 프라이빗 VLAN 간의 연계가 올바르게 설정되어 있어야 합니다.

| 매개변수 | 설명 |
|---|---|
| *p_vid* | VLAN 태그 내 VLAN ID 를 설정합니다. (범위: 1~4094) |
| *priority* | VLAN 태그 내 우선순위 필드를 설정합니다. (범위: 0~7). |
| *untagged* | 송출 패킷이 태그를 포함할지 여부를 설정합니다. |

**(1) 기본값**

기본 VLAN ID 는 1 입니다.
기본 우선순위는 0 입니다.
기본적으로 송출 패킷에는 태그가 없습니다.

**(2) 명령어 모드**

Port 설정 모드

**(3) 구문**

**switchport private-vlan { tag-pvid p_vid | tag-pri priority | untagged }**
**no switchport private-vlan untagged**

프라이빗 VLAN 의 레이어 2 포트에서 송출(Egress) 패킷의 태그 및 필드를 설정하려면 위 명령어를 실행합니다.

### 22.1.7. Show vlan private-vlan

이 명령어는 프라이빗 VLAN 내에서 VLAN 및 레이어 2 포트의 설정을 확인하는 데 사용됩니다.

**(1) 명령어 모드**

Port 설정 모드, VLAN 설정 모드, EXEC 모드

**(2) 예제**

다음 예제는 프라이빗 VLAN 의 설정을 표시하는 방법을 보여줍니다.

```
Switch_config#
Switch_config#show vlan private-vlan
Primary  Secondary  Type          Ports
------------------------- ----------------
2        3     community    G0/1, G0/2, G0/3
   2        4       isolated   G0/1, G0/4
   2        5     community    G0/1, G0/5
```

### 22.1.8. Show vlan private-vlan interface

이 명령어는 프라이빗 VLAN 내 특정 레이어 2 포트의 설정을 확인하는 데 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *Interface* | 조회할 인터페이스를 지정합니다 |

**(1) 명령어 모드**

Port 설정 모드, VLAN 설정 모드, EXEC 모드

**(2) 구문**

**show vlan private-vlan interface interface**

프라이빗 VLAN 에서 특정 레이어 2 포트의 설정을 표시하려면 위 명령어를 실행합니다.

**(3) 예제**

다음 예제는 프라이빗 VLAN 에서 g0/1 인터페이스의 설정을 표시하는 방법을 보여줍니다.

```
Switch_config#
Switch_config#show vlan private-vlan interface g0/1
port type: promiscuous port
private-vlan host-association: primary vlan 2 secondary vlan 3
private-vlan mapping: primary vlan 2 secondary vlan 3-5
Native VLAN tagging enable: untagged
Native VLAN tagging priority 0
Native VLAN tagging pvid: 1
```

# 23. GVRP 설정 명령

## 23.1. GVRP Configuration Commands

### 23.1.1. GVRP

#### (1) 구문

gvrp 명령어를 실행하여 GVRP 를 활성화하거나 비활성화할 수 있습니다. 기본 설정으로 되돌리려면 no gvrp 명령을 실행하십시오.

**no gvrp**

#### (2) 매개변수

없음

#### (3) 기본값

글로벌 GVRP 는 비활성화되어 있으며, 포트의 GVRP 는 활성화되어 있습니다.

#### (4) 사용 지침

GVRP 는 글로벌 또는 포트에서 활성화할 수 있습니다. 따라서 GVRP 는 글로벌과 포트에서 모두 활성화된 후에만 실제로 활성화됩니다.

#### (5) 예제

다음 예제는 GVRP 를 글로벌로 활성화하는 방법을 보여줍니다.
Switch_config#gvrp
Switch_config#

다음 예제는 포트 1 에서 GVRP 를 활성화하는 방법을 보여줍니다.
Switch_config_g0/1#gvrp
Switch_config_g0/1#

### 23.1.2. GVRP dynamic-vlan-pruning

#### (1) 구문

등록된 포트에서 동적 VLAN 을 적용하려면 gvrp dynamic-vlan-pruning 명령을 실행합니다. 기본 설정으로 돌아가려면 no 형식을 사용합니다.
gvrp dynamic-vlan-pruning
no gvrp dynamic-vlan-pruning

**(2) 매개변수**

없음

**(3) 기본값**

기본적으로 dynamic-vlan-pruning 은 비활성화되어 있으며, 즉 동적 VLAN 은 모든 포트에서 적용될 수 있습니다.

**(4) 명령어 모드**

전역 설정 모드

**(5) 사용 지침**

이 명령이 활성화된 경우, 포트가 동적 VLAN 을 등록하지 않았다면 해당 포트는 트렁크 포트(trunk port)이고 동적 VLAN 을 허용하더라도 동적 VLAN 에 속하지 않습니다.

**(6) 예제**

다음 예제는 등록된 포트에서 동적 VLAN 을 적용하는 방법을 보여줍니다.
Switch_config#gvrp dynamic-vlan-pruning
Switch_config#

### 23.1.3. show GVRP statistics

**(1) 구문**

GVRP 통계 정보를 표시하려면 다음 명령을 실행합니다.

**show gvrp statistics** [*interface intf-id*]

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *Intf-id* | 특정 물리적 인터페이스를 나타냅니다. |

**(3) 기본값**

없음

**(4) 사용 지침**

이 명령은 GVRP 통계 정보를 표시하는 데 사용됩니다.

**(5) 예제**

다음 예제는 인터페이스 g0/1 의 GVRP 통계 정보를 표시하는 방법을 보여줍니다.

```
Switch_config#show gvrp statistics interface g0/1
GVRP statistics on port g0/1
    GVRP Status          : Enabled
    GVRP Frames Received  : 0
    GVRP Frames Transmitted : 20
    GVRP Frames Discarded  : 0
    GVRP Last Pdu Origin    : 0000.0000.0000
```

### 23.1.4. show GVRP status

**(1) 구문**

GVRP 상태 정보를 표시하려면 다음 명령을 실행합니다.

**show gvrp status**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 사용 지침**

이 명령은 GVRP 상태 정보를 표시하는 데 사용됩니다.

**(5) 예제**

다음 예제는 스위치의 GVRP 상태 정보를 표시하는 방법을 보여줍니다.

Switch_config#show gvrp status
GVRP is enabled

### 23.1.5. Debug GVRP event

#### (1) 구문

GVRP 디버깅 정보 출력을 활성화하려면 debug gvrp event 명령을 실행합니다. GVRP 디버깅 정보 출력을 중지하려면 no debug gvrp event 명령을 실행합니다.

**debug gvrp event**
**no debug gvrp event**

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 사용 지침

GVRP 디버깅 정보 출력을 활성화하려면 debug gvrp event 를 실행하고, 중지하려면 no debug gvrp event 를 실행합니다.

#### (5) 예제

Switch# debug gvrp event
Switch#

### 23.1.6. Debug GVRP packet

#### (1) 구문

GVRP 패킷 디스플레이를 활성화 또는 비활성화하려면 다음 명령을 실행합니다.

debug gvrp packet
no debug gvrp packet

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 사용 지침**

GVRP 패킷 디스플레이를 활성화 또는 비활성화하려면 이 명령을 실행합니다.

**(5) 예제**

switch# debug gvrp packet
switch#

## 23.2. GARP Configuration Commands

GARP(Generic Attribute Registration Protocol)은 GVRP/GMRP 의 기본 모듈로, GVRP/GMRP 실행을 스케줄링하고 GVRP/GMRP 에 서비스를 제공합니다.

### 23.2.1. Garp timer leaveall

**(1) 구문**

GARP leaveall 타이머를 설정하려면 garp timer leaveall time_value 명령을 실행합니다. 기본 설정으로 복원하려면 no garp timer leaveall 명령을 실행합니다.

**garp timer leaveall** *time_value*
**no garp timer leaveall**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *timer_value* | 글로벌 leaveall 타이머 값 (10~32765 센티초). |

**(3) 기본값**

1000 센티초

**(4) 사용 지침**

leaveall 타이머가 만료되면 브리지가 모든 등록된 VLAN 정보를 취소하고 Leave All 메시지를 외부로 전송합니다.

**(5) 예제**

다음 예제는 스위치에서 leaveall 타이머를 1200 센티초로 설정하는 방법을 보여줍니다.

```
Switch_config# garp timer leaveall 1200
Switch_config#
```

### 23.2.2. Garp timer hold

**(1) 구문**

GARP hold 타이머를 설정하려면 garp timer hold time_value 명령을 실행합니다. 기본 설정으로 복원하려면 no garp timer hold 명령을 실행합니다.

**garp timer hold** *time_value*
**no garp timer hold**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| ***timer_value*** | 포트의 hold 타이머 값 (10~32765 센티초) |

**(3) 기본값**

10 센티초

**(4) 명령어 모드**

포트 설정 모드

**(5) 사용 지침**

없음

**(6) 예제**

다음 예제는 스위치에서 GARP hold 타이머를 15 센티초로 설정하는 방법을 보여줍니다.
Switch_config_g0/1#garp timer hold 15
Switch_config_g0/1#

### 23.2.3. Garp timer join

**(1) 구문**

GARP join 타이머를 설정하려면 garp timer join time_value 명령을 실행합니다. 기본 설정으로 복원하려면 no garp timer join 명령을 실행합니다.

**garp timer join** *time_value*
**no garp timer join**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *timer_value* | 포트의 join 타이머 값 (10~32765 센티초) |

**(3) 기본값**

20 센티초

**(4) 명령어 모드**

포트 설정 모드

**(5) 사용 지침**

없음

**(6) 예제**

다음 예제는 스위치의 포트 g0/1 에서 GARP join 타이머를 25 센티초로 설정하는 방법을 보여줍니다.

```
Switch_config_g0/1#garp timer join 25
Switch_config_g0/1#
```

### 23.2.4. garp timer leave

#### (1) 구문

GARP leave 타이머를 설정하려면 garp timer leave time_value 명령을 실행합니다. 기본 설정으로 복원하려면 no garp timer leave 명령을 실행합니다.

**garp timer leave** *time_value*
**no garp timer leave**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *timer_value* | 포트의 leave 타이머 값 (10~32765 센티초) |

#### (3) 기본값

60 센티초

#### (4) 명령어 모드

포트 설정 모드

#### (5) 사용 지침

없음

#### (6) 예제

다음 예제는 스위치의 포트 g0/1 에서 GARP leave 타이머를 80 센티초로 설정하는 방법을 보여줍니다.

```
Switch_config_g0/1#garp timer leave 80
Switch_config_g0/1#
```

### 23.2.5. show garp timers

**(1) 구문**

GARP 에서 구성된 타이머 정보를 표시하려면 다음 명령을 실행합니다.
**show garp timers** *[ interface intf_id* ]

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *Intf-id* | 특정 물리적 인터페이스를 나타냅니다. |

**(3) 기본값**

없음

**(4) 사용 지침**

이 명령은 GARP 에서 구성된 타이머 정보를 표시하는 데 사용됩니다. 여기에는 글로벌 leaveall 타이머 값과 포트별 hold/join/leave 타이머 값이 포함됩니다.

**(5) 예제**

다음 예제는 인터페이스 g0/1 의 타이머 정보를 표시하는 방법을 보여줍니다.

```
Switch# show garp timers interface g0/1
 GARP  timers on port 1 (G0/1)
     Garp Join Time       : 20 centiseconds
     Garp Leave Time      : 60 centiseconds
     Garp LeaveAll Time   : 1000 centiseconds
     Garp Hold Time       : 10 centiseconds
```

### 23.2.6. show garp status

**(1) 구문**

현재 실행 중인 GARP 애플리케이션 인스턴스를 표시하려면 다음 명령을 실행합니다.
**show garp status**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 사용 지침**

현재 실행 중인 GARP 애플리케이션 인스턴스를 표시하려면 이 명령을 실행합니다.

**(5) 예제**

다음 예제는 실행 중인 GARP 애플리케이션 인스턴스를 표시하는 방법을 보여줍니다.

```
Switch_config#show garp status
No  GARP  application is running.
```

### 23.2.7. debug garp

**(1) 구문**

GARP 이벤트 또는 타이머에 대한 디버그 정보를 활성화 또는 비활성화하려면 다음 명령을 실행합니다.

**debug garp { event | timer }**
**no debug garp { event | timer }**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| event | 이벤트 디버깅을 활성화 |
| timer | 타이머 디버깅을 활성화 |

**(3) 기본값**

없음

**(4) 사용 지침**

GARP 이벤트 또는 타이머의 디버그 정보를 활성화하거나 비활성화하려면 위의 명령을 실행합니다.

**(5) 예제**

다음 예제는 GARP 이벤트 디버깅 정보를 활성화하는 방법을 보여줍니다.

```
Switch# debug garp event
Switch#
```

# 24. LACP

## 24.1. 개요

트렁킹이라고 하는 링크 집합은 이더넷 스위치에서 사용할 수 있는 옵션 기능이며 2 계층 브리징과 함께 사용됩니다. 링크 집합은 단일 링크에서 여러 포트의 논리적 병합을 허용합니다. 각 물리적 링크의 전체 대역폭을 사용할 수 있기 때문에 비효율적 인 트래픽 라우팅으로 대역폭을 낭비하지 않습니다. 결과적으로 전체 클러스터가 보다 효율적으로 활용됩니다. 링크 집합은 트래픽이 많은 서버에 높은 총 대역폭을 제공하고 단일 포트 또는 케이블 장애가 발생할 경우 재 라우팅 기능을 제공합니다.

지원 기능:

정적 집합 제어가 지원됩니다.
논리적 포트에 실제로 바인딩 할 수 있는지 여부에 관계없이 물리적 포트를 논리적 포트에 바인딩합니다.
LACP 동적 협상의 집합 제어가 지원됩니다.
LACP 프로토콜 협상을 전달하는 물리적 포트 만 논리 포트에 바인딩 할 수 있습니다. 다른 포트는 논리 포트에 바인드 되지 않습니다.
LACP 동적 협상의 집합 제어가 지원됩니다.
물리적 포트가 논리적 포트에 바인딩되도록 구성되면 LACP 협상을 사용하는 물리적 포트를 논리적 포트에 바인딩 할 수 있습니다. 다른 포트는 논리 포트에 바인드 될 수 없습니다.
포트 집합의 흐름 균형이 지원됩니다.
포트 집합 후에는 집합 포트의 데이터 흐름이 각 집합된 물리적 포트에 분산됩니다.

## 24.2. 포트 집합 구성 작업 목록

### 24.2.1. 포트 집합에 사용된 논리 채널의 구성

물리적 포트를 모두 바인딩하기 전에 논리 포트를 구성해야 합니다. 논리적 포트는 이러한 바인딩 물리적 포트에 의해 형성된 채널을 제어하는 데 사용됩니다.

논리 채널을 구성하려면 다음 명령을 사용하십시오.

| 명령어 | 설명 |
| --- | --- |
| interface port-aggregator id | 집합된 논리 채널을 구성합니다. |

### 24.2.2. 집합 물리적인 포트

여러 물리적 포트를 논리 채널로 집합하려면 협상에 정적 집합 또는 LACP 프로토콜을 사용할 수 있습니다.

정적 집합이 사용되는 경우 물리적 포트의 링크가 작동해야 하며 집합 포트와 물리적 포트의 VLAN 속성이 동일해야 하며 이 포트는 논리 채널에 집합되어야 하며, 현재 포트가 포트 집합의 조건과 일치하는지 여부 및 물리적 포트와 연결된 포트가 집합 조건과 일치하는지 여부에 관계없이 집합할 포트에 대한 선행 조건:

- 포트의 링크를 올리고 포트를 전 이중 모드로 협상해야 합니다.
- 모든 물리적 포트의 속도는 집합 프로세스 중에 동일해야 합니다. 즉, 성공적으로 집합된 물리적 포트가 하나 있는 경우 두 번째 물리적 포트의 속도는 첫 번째 구성된 포트와 동일해야 합니다. 또한 모든 물리적 포트의 VLAN 속성은 집합된 포트와 동일해야 합니다.

LACP 패킷은 다음 모드에서 포트 간에 교환됩니다.

- 활성 - 포트를 활성 협상 상태로 전환합니다. 이 상태에서 포트는 LACP 패킷을 보내 원격 포트와 협상을 시작합니다.
- 패시브 - 포트를 패시브 협상 상태로 전환합니다. 상태에서 포트는 LACP 패킷에 응답하지만 LACP 협상을 시작하지는 않습니다. 이 모드에서 포트 채널 그룹은 인터페이스를 번들에 연결합니다.

두 포트 모두 패시브 방식을 사용하면 집합이 실패합니다. 이는 양 측이 상대방이 집합 협상 프로세스를 시작하기를 기다릴 것이기 때문입니다.

VLAN 속성: PVID, 트렁크 속성, VLAN 허용 범위 및 VLAN 비 태그 범위. 다음 명령을 사용하여 물리적 포트에서 집합을 수행하십시오.

| 명령어 | 설명 |
|---|---|
| **aggregator-group** *aggid* **mode {lacp \| static}** | 물리적 포트의 집합 옵션을 구성합니다 . |

### 24.2.3. 포트 집합 후의 부하 분산 방법 선택

로드 공유 방법을 선택하여 모든 포트가 모든 물리적 포트를 모은 후에 데이터 트래픽을 공유할 수 있도록 할 수 있습니다. 스위치는 최대 6 가지로드 밸런싱 정책을 제공할 수 있습니다.

- src-mac

원본 MAC 주소에 따라 데이터 트래픽을 공유합니다. 즉, 동일한 MAC 주소 특성을 가진 메시지는 물리적 포트를 통과하는 것입니다.

- dst-mac

대상 MAC 주소에 따라 데이터 트래픽을 공유하는 것입니다. 즉, 동일한 MAC 주소 속성을 가진 메시지는 물리적 포트를 통과하는 것입니다.

- both-mac

원본 및 대상 MAC 주소에 따라 데이터 트래픽을 공유하는 것입니다. 즉, 동일한 MAC 주소 특성을 가진 메시지는 물리적 포트를 통과하는 것입니다.

- src-ip

출발 IP 주소에 따라 데이터 트래픽을 공유하는 것입니다. 즉, 동일한 IP 주소 특성을 가진 메시지는 물리적 포트를 통과하는 것입니다.

- dst-ip

목적 IP 주소에 따라 데이터 트래픽을 공유하는 것입니다. 즉, 동일한 IP 주소 속성을 가진 메시지는 물리적 포트를 통과하는 것입니다.

- both-ip

대상 및 소스 IP 주소에 따라 데이터 트래픽을 공유하는 것입니다. 즉, 동일한 IP 주소 속성을 가진 메시지는 물리적 포트를 통과하는 것입니다.

부하 분산 방법을 구성하려면 다음 명령을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| aggregator-group load-balance | 부하 분산 방법을 구성합니다. |

Note:
이 명령은 부하 분산 방법을 지원하지 않거나 하나의 방법 만 지원하는 스위치에서는 사용할 수 없습니다. 이 명령을 사용하는 스위치는 자체적으로 지원되는 로드 균형 정책 만 선택합니다.

#### 24.2.4. 포트 집합의 구체적인 조건 모니터링

EXEC 모드에서 포트 집합 상태를 모니터링하려면 다음 명령을 사용하십시오.

| 명령어 | 설명 |
|---|---|
| show aggregator-group | 포트 집합 상태를 표시합니다. |

# 25. LLDP (Link Layer Discovery Protocol)

## 25.1. LLDP 개요

802.1AB 에서 링크 계층 탐색 프로토콜 (LLDP) 802.1AB 는 쉽게 네트워크 문제를 감지하고 네트워크 토폴로지를 유지하는 데 도움이 됩니다.

LLDP 는 단방향 프로토콜입니다. 하나의 LLDP 에이전트는 연결된 MSAP 를 통해 상태 정보 및 기능을 전송하거나 이웃에 대한 현재 상태 정보 또는 기능 정보를 수신합니다. 그러나 LLDP 에이전트는 프로토콜을 통해 상대로부터 정보를 요청할 수 없습니다.

메시지 교환 중에는 메시지 송수신이 서로 영향을 미치지 않습니다. 메시지 전송 또는 수신 또는 둘 다를 구성할 수 있습니다.

LLDP 는 관리 인력에게 정확한 네트워크 매핑, 트래픽 데이터 및 문제 감지 정보를 제공하는 유용한 관리 도구입니다.

## 25.2. LLDP 구성 작업 목록

- LLDP 활성화 또는 비활성화
- 대기시간구성
- 타이머구성하기
- 재시작구성
- 보낼 대상 tlv 구성
- 송수신모드구성
- 상대보기명령구성
- 삭제명령구성
- 디버깅명령구성

## 25.3. LLDP 구성 작업

### 25.3.1. LLDP 활성화/비활성화

LLDP 는 기본적으로 비활성화되어 있습니다. 실행하기 전에 LLDP 를 시작해야합니다.
LLDP 를 활성화하려면 전역 구성 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **lldp run** | LLDP 를 실행합니다. |

다음 명령을 실행하여 LLDP 를 비활성화하십시오.

| 명령어 | 설명 |
|---|---|
| **no lldp run** | LLDP 를 비활성화합니다. |

### 25.3.2. 유지 시간 구성

holdtime 수정을 통해 LLDP 메시지를 전송하는 시간 제한을 제어할 수 있습니다.
글로벌 구성 모드에서 다음 명령을 실행하여 LLDP 의 보류 시간을 구성합니다.

| 명령어 | 설명 |
|---|---|
| **lldp holdtime** *time* | LLDP 의 제한 시간을 구성합니다 |
| **no lldp holdtime** | 시간 종료 시간을 기본값 인 120 초로 재개합니다. |

### 25.3.3. 타이머 구성

LLDP 의 타이머를 구성하여 메시지 전송을 위한 스위치 간격을 제어할 수 있습니다.
LLDP 의 타이머를 구성하려면 전역 구성 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **lldp timer** *time* | LLDP 의 메시지 전송 간격을 구성합니다. |
| **no lldp timer** | 기본 간격 즉, 30 초를 재개합니다. |

### 25.3.4. Reinit 구성

LLDP reinit 를 구성하여 스위치의 간격을 제어하여 두 개의 메시지를 계속 전송할 수 있습니다.
글로벌 구성 모드에서 다음 명령을 실행하여 LLDP 의 reinit 를 구성합니다.

| 명령어 | 설명 |
|---|---|
| **lldp reinit** *time* | LLDP 의 간격을 구성하여 메시지를 계속 전송합니다. |
| **no lldp reinit** | 메시지를 계속 전송하는 기본 간격을 다시 시작합니다. 기본 간격 값은 2 초입니다. |

### 25.3.5. 전송할 TLV 구성

LLDP 의 tlv-select 를 구성하여 보내야 하는 TLV 를 선택할 수 있습니다. 기본적으로 모든 TLV 가 전송됩니다.

LLDP 의 tlv 를 추가하거나 삭제하려면 전역 구성 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **lldp tlv-select** *tlv-type* | 추가해야 할 Tlvs 또는 tlv 유형은 다음과 같습니다.<br>chassis-id<br>management-address<br>port-description<br>port-vlan<br>system-capabilities<br>system-description<br>system-name |
| **no lldp tlv-select** *tlv-type* | 삭제해야 할 tlv 또는 tlv 유형은 다음과 같습니다.<br>chassis-id<br>management-address<br>port-description<br>port-vlan<br>system-capabilities<br>system-description<br>system-name |

### 25.3.6. 전송 또는 수신 모드 구성

LLDP 는 전송 전용, 수신 전용 및 전송 및 수신의 세 가지 모드로 작동할 수 있습니다.
기본적으로 LLDP 는 송수신 모드에서 작동합니다. 다음 명령을 통해 LLDP 의 작업 모드를 수정할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 LLDP 의 작동 모드를 구성하십시오.

| 명령어 | 설명 |
|---|---|
| **[no] lldp transmit** | 포트를 송신 전용 모드로 구성하거나 포트의 송신 전용 모드를 비활성화합니다. |
| **[no] lldp receive** | 포트를 수신 전용 모드로 구성하거나 포트의 수신 전용 모드를 사용 불가능하게 합니다. |

### 25.3.7. 표시 관련 명령 구성

Show 연관 명령을 실행하여 LLDP 모듈이 수신한 이웃, 통계 또는 포트 상태에 대한 정보를 볼 수 있습니다.

EXEC 또는 전역 구성 모드에서 다음 명령을 실행합니다.

| 명령어 | 설명 |
|---|---|
| **show lldp errors** | LLDP 모듈에 대한 오류 정보를 표시합니다. |
| **show lldp interface** *interface-name* | 포트 상태, 즉 전송 모드 및 수신 모드에 대한 정보를 표시합니다. |
| **show lldp neighbors** | 이웃에 대한 추상 정보를 표시합니다. |
| **show lldp neighbors detail** | 이웃에 대한 자세한 정보를 표시합니다. |
| **show lldp traffic** | 모든 수신 및 전송된 통계 정보를 표시합니다 |

### 25.3.8. 삭제 명령 구성

EXEC 모드에서 다음 명령을 실행하여 수신된 이웃 목록 및 모든 통계 정보를 삭제할 수 있습니다.

| 명령어 | 설명 |
|---|---|
| **clear lldp counters** | 모든 통계 데이터를 삭제합니다. |
| **clear lldp table** | 수신된 모든 이웃 정보를 삭제합니다. |

### 25.3.9. 디버깅 명령 구성하기

LLDP 모듈을 쉽게 모니터링하려면 EXEC 모드에서 다음 명령을 실행하십시오.

| 명령어 | 설명 |
|---|---|
| **debug lldp errors** | LLDP 모듈에 대한 몇 가지 오류 정보를 보고합니다. |
| **debug lldp events** | LLDP 모듈에 대한 몇 가지 특별 이벤트를 보고합니다. |
| **debug lldp packets** | LLDP 모듈의 메시지 전송 이벤트를 보고합니다. |
| **debug lldp states** | LLDP 포트의 상태에 대한 정보를 보고합니다. |

# 26. PDP 설정 명령

## 26.1. PDP 설정 명령어

다음은 PDP(Peer Discovery Protocol) 관련 명령어 목록입니다:

- pdp timer
- pdp holdtime
- pdp version
- pdp run
- pdp enable
- show pdp traffic
- show pdp neighbor

### 26.1.1. PDP timer

#### (1) 구문

이 명령어는 PDP 타이머 시간을 설정하는 데 사용됩니다.

[no|default] pdp timer seconds

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| seconds | PDP 패킷을 전송하는 간격(범위: 5~254 초) |

#### (3) 기본값

기본 설정값은 60 초입니다.

#### (4) 사용 지침

이 명령어는 전역 설정 모드에서 설정됩니다.

#### (5) 예제

다음 예제는 스위치가 5 초마다 PDP 패킷을 전송하도록 설정하는 방법을 보여줍니다.
pdp timer 5

### 26.1.2. PDP holdtime

#### (1) 구문

이 명령어는 PDP 유지 시간(holdtime)을 설정하는 데 사용됩니다.

[no|default] pdp holdtime seconds

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| seconds | 이웃 정보를 삭제하는 데 필요한 시간(범위: 10~255 초). |

#### (3) 기본값

기본 설정값은 180 초입니다.

#### (4) 사용 지침

이 명령어는 전역 설정 모드에서 설정됩니다.

#### (5) 예제

다음 예제는 이웃 정보를 15 초 동안 유지하도록 설정하는 방법을 보여줍니다.
pdp holdtime 15

### 26.1.3. PDP version

#### (1) 구문

이 명령어는 PDP 버전을 설정하는 데 사용됩니다.

[no] pdp version 〈1|2〉

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| version | PDP 버전(1 또는 2) |

**(3) 기본값**

기본 PDP 버전은 2 입니다.

**(4) 사용 지침**

이 명령어는 글로벌 설정 모드에서 설정됩니다.

**(5) 예제**

다음 예제는 스위치의 PDP 버전을 1 로 설정하는 방법을 보여줍니다.

pdp version 1

### 26.1.4. PDP run

**(1) 구문**

이 명령어는 PDP 를 활성화하는 데 사용됩니다.

[no] pdp run

**(2) 매개변수**

없음

**(3) 기본값**

PDP 프로토콜은 기본적으로 비활성화되어 있습니다.

**(4) 사용 지침**

이 명령어는 글로벌 설정 모드에서 설정됩니다.

**(5) 예제**

다음 예제는 PDP 를 비활성화하는 방법을 보여줍니다.

no pdp run

### 26.1.5. PDP enable

#### (1) 구문

이 명령어는 특정 포트에서 PDP 를 활성화하거나 비활성화하는 데 사용됩니다.

[no] pdp enable

#### (2) 매개변수

해당 없음

#### (3) 기본값

PDP 는 기본적으로 활성화되어 있습니다.

#### (4) 사용 지침

이 명령어는 포트 설정 모드에서 설정되며, PDP 가 글로벌 모드에서 활성화된 경우에만 적용됩니다.

#### (5) 예제

다음 예제는 포트 f0/1 에서 PDP 를 비활성화하는 방법을 보여줍니다.

switch_config_f0/1#no pdp enable

### 26.1.6. Show PDP traffic

#### (1) 구문

이 명령어는 수신된 PDP 패킷의 개수를 확인하는 데 사용됩니다.

show pdp traffic

#### (2) 매개변수

해당 없음

#### (3) 기본값

해당 없음

**(4) 사용 지침**

PDP 의 실행 상태를 확인하는 데 사용됩니다.

**(5) 예제**

Switch_config#show pdp traffic
Packets output: 253491, Input: 0
Hdr 구문: 0, Chksum error: 0
No memory: 0, Invalid packet: 0

### 26.1.7. Show PDP neighbor

**(1) 구문**

이 명령어는 PDP 이웃 정보를 확인하는 데 사용됩니다.

show pdp neighbor

**(2) 매개변수**

해당 없음

**(3) 기본값**

해당 없음

**(4) 사용 지침**

PDP 이웃의 실행 상태를 확인하는 데 사용됩니다.

**(5) 예제**

Switch_config#show pdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID Local-Intf Hldtme Port-ID Platform Capability
Switch Gig0/1 169 Gig0/1 xxcom, RISC R S

# 27. STP 설정 명령어

## 27.1. SSTP 설정 명령어

### 27.1.1. spanning-tree

#### (1) 구문

**spanning-tree**
**no spanning-tree**

기본 STP 모드를 활성화하려면 spanning-tree 명령어를 실행하고, STP 를 비활성화하려면 no spanning-tree 명령어를 실행합니다.

인터페이스 설정 모드에서 STP 를 활성화하거나 비활성화합니다.

#### (2) 매개변수

없음

#### (3) 기본값

기본적으로 RSTP 모드를 활성화합니다.

#### (4) 사용 지침

없음

#### (5) 명령어 모드

전역 설정 모드
물리적 포트 또는 애그리게이션 포트 설정 모드.

#### (6) 예제

없음

### 27.1.2. spanning-tree mode sstp

#### (1) 구문

**spanning-tree mode sstp**
**no spanning-tree mode**

RSTP 와 SSTP 모드를 전환하려면 spanning-tree mode 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**(2) 매개변수**

없음

**(3) 기본값**

RSTP

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 명령어는 SSTP 모드를 활성화하는 방법을 보여줍니다:
Switch_config# spanning-tree mode sstp
Switch_config#

### 27.1.3. Spanning-tree sstp priority

**(1) 구문**

SSTP 브리지 우선순위를 설정하려면 spanning-tree sstp priority 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree sstp priority** *value*
**no spanning-tree sstp priority**

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *value* | 0~61440 사이의 값. |

**(3) 기본값**

32768

**(4) 사용 지침**

우선순위 값을 설정하면 해당 노드를 스패닝 트리의 루트로 지정할 수 있습니다. 설정 가능한 값은 4096 단위로 증가하며, 0, 4096, 8192, 3×4096, 4×4096, ..., 15×4096 과 같은 값만 사용할 수 있습니다.

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 SSTP 우선순위를 4096 으로 설정하는 방법을 보여줍니다:
Switch(config)# spanning-tree sstp priority 4096
Switch(config)#

### 27.1.4. spanning-tree sstp hello-time

**(1) 구문**

Hello-time 지연 타이머를 설정하려면 spanning-tree sstp hello-time 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree sstp hello-time** *time*
**no spanning-tree sstp hello-time**

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *time* | Hello-time 지연 타이머를 설정할 초 단위 값(1~10 초) |

**(3) 기본값**

2 초

**(4) 사용 지침**

로컬 스위치에서 설정한 Hello-time 값은 해당 스위치가 루트 브리지일 때만 유효합니다.

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 SSTP hello-time 을 8 초로 설정하는 방법을 보여줍니다:
Switch(config)# spanning-tree sstp hello-time 8
Switch(config)#

### 27.1.5. spanning-tree sstp max-age

**(1) 구문**

SSTP max-age 타이머를 설정하려면 spanning-tree sstp max-age 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree sstp max-age** *time*
**no spanning-tree sstp max-age**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *seconds* | Max-age 타이머를 설정할 초 단위 값(6~40 초). |

**(3) 기본값**

20 초

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 max-age 타이머를 24 초로 설정하는 방법을 보여줍니다.
Switch(config)# spanning-tree sstp max-age 24
Switch(config)#

### 27.1.6. spanning-tree sstp forward-time

#### (1) 구문

전역 설정 모드에서 포워드 딜레이 타이머를 설정하려면 spanning-tree sstp forward-time 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree sstp forward-time** *time*
**no spanning-tree sstp forward-time**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *time* | 포워드 딜레이 타이머를 설정할 초 단위 값(4~30 초). |

#### (3) 기본값

15 초

#### (4) 사용 지침

없음

#### (5) 명령어 모드

전역 설정 모드

#### (6) 예제

다음 예제는 포워드 딜레이 타이머를 20 초로 설정하는 방법을 보여줍니다:
Switch_config# spanning-tree sstp forward-time 20
Switch_config#

### 27.1.7. spanning-tree sstp cost

#### (1) 구문

SSTP 계산을 위한 인터페이스의 경로 비용(Path Cost)을 설정하려면 spanning-tree sstp cost 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.
**spanning-tree sstp cost** *value*
**no spanning-tree sstp cost**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 경로 비용. 설정 가능한 값은 1~200000000 |

**(3) 기본값**

10M Ethernet:100 .
100M Ethernet: 19 .
1000M Ethernet: 4 .

**(4) 사용 지침**

없음

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

다음 예제는 인터페이스 G0/1 에서 스패닝 트리 VLAN 의 경로 비용을 100 으로 설정하는 방법을 보여줍니다:
Switch_config_g0/1#spanning-tree sstp cost 100
Switch_config_g0/1#

### 27.1.8. spanning-tree cost

**(1) 구문**

STP 계산을 위한 인터페이스의 경로 비용(Path Cost)을 설정하려면 spanning-tree cost 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree cost** *value*
**no spanning-tree cost**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 경로 비용. 설정 가능한 값은 1~200000000 |

**(3) 기본값**

인터페이스의 대역폭 설정을 기준으로 기본 경로 비용이 계산됩니다.

**(4) 사용 지침**

이 명령어의 설정 결과는 모든 스패닝 트리 모드에서 유효합니다.

**STP 모드:**
인터페이스에 있는 모든 VLAN 스패닝 트리의 경로 비용이 업데이트됩니다.

**MSTP 모드:**
모든 스패닝 트리 인스턴스의 경로 비용이 업데이트됩니다. 하지만 이 명령어의 설정 결과는 다양한 모드에서 개별적으로 설정된 구성에 영향을 미치지 않습니다. 예를 들어, 스위치가 SSTP 모드에서 spanning-tree sstp cost 100 과 spanning-tree cost 110 을 각각 설정한 경우, 포트 비용은 100 으로 유지됩니다.

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

다음 예제는 인터페이스 G0/1 에서 스패닝 트리 VLAN 의 경로 비용을 24 로 설정하는 방법을 보여줍니다:
Switch(config_f0/0)# spanning-tree cost 24
Switch_config_g0/1#

### 27.1.9. spanning-tree sstp port-priority

**(1) 구문**

SSTP 모드에서 포트 우선순위 값을 설정하려면 spanning-tree sstp port-priority 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree sstp port-priority** *value*
**no spanning-tree sstp port-priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 포트 우선순위(0~240, 16 단위로 증가) |

**(3) 기본값**

128 (0x80)

**(4) 사용 지침**

포트 우선순위 값은 반드시 16 단위로 설정해야 합니다.

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

다음 예제는 인터페이스 G0/1 에서 포트 우선순위를 32 로 설정하는 방법을 보여줍니다:
Switch_config_g0/1# spanning-tree sstp port-priority 32
Switch_config_g0/1#

### 27.1.10. spanning-tree port-priority

**(1) 구문**

두 개의 브리지가 루트 브리지로 경쟁할 때 인터페이스의 우선순위를 설정하려면 spanning-tree port-priority 명령어를 사용합니다. 동일한 비용을 가진 경로가 있을 때 이 우선순위 값이 우선순위를 결정합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree port-priority** *value*
**no spanning-tree port-priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 포트 우선순위(0~240, 16 단위로 증가) |

**(3) 기본값**

포트 우선 값 128

**(4) 사용 지침**

이 명령어의 설정 결과는 모든 스패닝 트리 모드에서 유효합니다.

STP 모드:
인터페이스에 있는 모든 VLAN 스패닝 트리의 우선순위가 변경됩니다.

MSTP 모드:

모든 스패닝 트리 인스턴스의 우선순위가 변경됩니다.

하지만 이 명령어의 설정 결과는 다양한 모드에서 개별적으로 설정된 구성에 영향을 미치지 않습니다. 예를 들어, 스위치가 SSTP 모드에서 spanning-tree sstp port-priority 128 과 spanning-tree port-priority 48 을 각각 설정한 경우, 포트 우선순위는 128 로 유지됩니다.

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

다음 예제는 인터페이스 G0/1 에서 포트 우선순위를 16 으로 설정하는 방법을 보여줍니다:
Switch_config_g0/1#spanning-tree port-priority 16
Switch_config_g0/1#

### 27.1.11. show spanning-tree

**(1) 구문**

지정된 스패닝 트리 인스턴스의 정보를 표시하려면 show spanning-tree 명령어를 사용합니다.

**show spanning-tree [detail | interface** *intf-i* **| mstp| pvst | interfacevlan]**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *intf-i* | 인터페이스 이름 (예: G5/1) |

**(3) 기본값**

없음

**(4) 사용 지침**

스패닝 트리 상태를 표시합니다.

**(5) 명령어 모드**

EXEC/전역 설정 모드/인터페이스 설정 모드

**(6) 예제**

Switch_config#show spanning-tree

```
Spanning tree enabled protocol SSTP

SSTP
 Root ID    Priority    32768
        Address     5491.AF10.D083
        This bridge is the root
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32768
        Address     5491.AF10.D083
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface       Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------
G5/1            Desg FWD 19        128.16  P2p

Switch_config#
```

### 27.1.12. spanning-tree management trap

#### (1) 구문

STP 트랩을 활성화하려면 spanning-tree management trap [ newroot | topologychange ] 명령어를 실행합니다. 기본 설정으로 되돌리려면 no 형식을 사용합니다.

**[no] spanning-tree management trap [ newroot | topologychange ]**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| newroot | 새로운 루트 트랩 유형 |
| topologychange | 토폴로지 변경 트랩 유형 |

#### (3) 기본값

STP 트랩이 활성화되지 않음.

#### (4) 사용 지침

없음

#### (5) 명령어 모드

전역 설정 모드

**(6) 예제**

없음

## 27.2. VLAN STP 설정 명령어

### 27.2.1. spanning-tree mode pvst

**(1) 구문**

VLAN 기반 STP(PVST) 모드를 활성화하려면 spanning-tree mode pvst 명령어를 실행합니다. 기능을 비활성화하려면 no 형식을 사용합니다.

**spanning-tree mode pvst**
**no spanning-tree mode**

**(2) 매개변수**

없음

**(3) 기본값**

RSTP 모드

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 스위치에서 PVST 모드를 활성화하는 방법을 보여줍니다:

Switch_config# spanning-tree mode pvst
Switch_config#

### 27.2.2. spanning-tree vlan

**(1) 구문**

지정된 VLAN 에서 STP 를 실행하려면 spanning-tree vlan vlan-list 명령어를 사용합니다. 지정된 VLAN 의 스패닝 트리를 취소하려면 no spanning-tree vlan vlan-list 명령어를 실행합니다.

**spanning-tree vlan** *vlan-list*
**no spanning-tree vlan** *vlan-list*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *vlan-list* | VLAN 번호 목록 (예: 1,2,3-10,15) |

**(3) 기본값**

스위치는 특정 VLAN 에만 STP 인스턴스를 할당하며, 초과된 VLAN 은 자동으로 STP 금지 목록에 추가됩니다.

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 VLAN 10, 11, 15-19 에서 STP 를 제거하고, VLAN 40-50 에서 STP 를 활성화하는 방법을 보여줍니다:

```
Switch_config#no spanning-tree vlan 10,11,15-19
Switch_config#spanning-tree vlan 40-50
Switch_config#
```

### 27.2.3. spanning-tree vlan priority

**(1) 구문**

VLAN STP 브리지의 우선순위 값을 지정하려면 spanning-tree vlan priority 명령어를 사용합니다.

**spanning-tree vlan** *vlan-list* **priority** *value*
**no spanning-tree vlan** *vlan-list* **priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| vlan-list | VLAN 번호 목록 (예: 1,2,3-10,15) |
| value | 우선순위 값 (0 ~ 61440, 단위: 4096) |

**(3) 기본값**

각 VLAN 스패닝 트리의 브릿지 기본 우선순위 값은 32768 + VLAN 번호입니다.

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 VLAN 1-3 및 5-10 의 브리지 우선순위를 4096 으로 설정하는 방법을 보여줍니다:

```
Switch_config#spanning-tree vlan 1-3,5-10 priority 4096
Switch_config#
```

### 27.2.4. spanning-tree vlan forward-time

**(1) 구문**

이 명령어는 VLAN 에서 STP 의 Forward Delay 매개변수를 지정하는 데 사용됩니다. 이 기능을 비활성화하려면 no 형식의 명령어를 사용합니다.

**spanning-tree vlan** *vlan-list* **forward-time** *value*
**no spanning-tree vlan** *vlan-list* **forward-time**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| vlan-list | VLAN 번호 목록 (예: 1,2,3-10,15) |
| value | Forward Delay 값 (4 ~ 30 초, 기본값: 15 초) |

**(3) 기본값**

모든 VLAN 의 Forward Delay 기본값은 15 초입니다.

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 VLAN 1-3 및 5-10 의 Forward Delay 값을 19 초로 설정하는 방법을 보여줍니다:

Switch_config#spanning-tree vlan 1-3,5-10 forward-time 19
Switch_config#

### 27.2.5. spanning-tree vlan max-age

#### (1) 구문

이 명령어는 VLAN 에서 STP 의 Max Age 매개변수를 설정하는 데 사용됩니다. 이 기능을 비활성화하려면 no 형식의 명령어를 사용합니다.

**spanning-tree vlan** *vlan-list* **max-age** *value*
**no spanning-tree vlan** *vlan-list* **max-age**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| vlan-list | VLAN 번호 목록 (예: 1,2,3-10,15) |
| value | Max Age 값 (6 ~ 40 초, 기본값: 20 초) |

#### (3) 기본값

모든 VLAN 의 Max Age 기본값은 20 초입니다.

#### (4) 사용 지침

없음

#### (5) 명령어 모드

전역 설정 모드

#### (6) 예제

다음 예제는 VLAN 1-3 및 5-10 의 Max Age 값을 19 초로 설정하는 방법을 보여줍니다:

Switch_config#spanning-tree vlan 1-3,5-10 max-age 19
Switch_config#

### 27.2.6. spanning-tree vlan hello-time

#### (1) 구문

이 명령어는 VLAN 에서 STP 의 hello-time 매개변수를 설정하는 데 사용됩니다. 기본 설정으로 돌아가려면 no 형식의 명령어를 사용하십시오.

**spanning-tree vlan** *vlan-list* **hello-time** *value*
**no spanning-tree vlan** *vlan-list* **hello-time**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *vlan-list* | VLAN 번호 목록, 예: 1,2,3-10,15 |
| *value* | hello-time 값, 범위는 1 초에서 10 초 사이이며 기본값은 2 초입니다. |

**(3) 기본값**

모든 VLAN 의 Hello-Time 은 2 초입니다.

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 VLAN1-3,5-10 의 Hello-Time 을 9 초로 설정하는 방법을 보여줍니다:

Switch_config#spanning-tree vlan 1-3,5-10 hello-time 9
Switch_config#

### 27.2.7. spanning-tree vlan cost

**(1) 구문**

지정된 VLAN 에서 스패닝 트리의 경로 비용을 설정하려면 spanning-tree vlan vlan-list cost value 명령을 실행하십시오. 기본값으로 되돌리려면 no spanning-tree vlan vlan-list cost 명령을 실행하십시오.

**spanning-tree vlan** *vlan-list* **cost** *value*
**no spanning-tree vlan** *vlan-list* **cost**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|

| | |
|---|---|
| *vlan-list* | VLAN 번호 목록, 예: 1,2,3-10,15. |
| *value* | 경로 비용, 범위는 1 에서 200000000 까지입니다 |

**(3) 기본값**

포트의 경로 비용은 포트의 속도에 따라 달라집니다.

10M Ethernet: 100
100M Ethernet: 19
1000M Ethernet: 4.

**(4) 사용 지침**

없음

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

다음 예제는 포트 G0/1 에서 VLAN1-3,5-10 의 경로 비용을 100 으로 설정하는 방법을 보여줍니다:

```
Switch_config_g0/1#spanning-tree vlan 1-3,5-10 cost 100
Switch_config_g0/1#
```

### 27.2.8. spanning-tree vlan port-priority

**(1) 구문**

지정된 VLAN 에서 스패닝 트리의 포트 우선순위를 설정하려면 spanning-tree vlan vlan-list port-priority value 명령을 실행하십시오. 기본값으로 되돌리려면 no spanning-tree vlan vlan-list port-priority 명령을 실행하십시오.

**spanning-tree vlan** *vlan-list* **port-priority** *value*
**no spanning-tree vlan** *vlan-list* **port-priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *vlan-list* | VLAN 번호 목록, 예: 1,2,3-10,15 |
| *value* | 포트 우선순위, 범위는 0 에서 240 까지이며, 증가 값은 16 입니다. |

**(3) 기본값**

128

**(4) 사용 지침**

없음

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

다음 예제는 포트 G0/1 에서 VLAN1-3,5-10 의 포트 우선순위를 32 로 설정하는 방법을 보여줍니다.

```
Switch_config_g0/1#spanning-tree vlan 1-3,5-10 port-priority 32
Switch_config_g0/1#
```

### 27.2.9. show spanning-tree vlan

**(1) 구문**

지정된 VLAN 에서 스패닝 트리 상태를 확인하려면 위 명령어를 실행하십시오.

**show spanning-tree vlan** *vlan-list* **[ detail ]**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *vlan-list* | VLAN 번호 목록, 예: 1,2,3-10,15 |
| *detail* | 자세한 정보를 표시 |

**(3) 기본값**

없음

**(4) 사용 지침**

없음

**(5) 명령어 모드**

EXEC, 전역 설정 모드 또는 인터페이스 설정 모드

**(6) 예제**

다음 예제는 VLAN1-2 에서 스패닝 트리를 확인하는 방법을 보여줍니다:

```
Switch_config#show spanning-tree vlan 1-2

Spanning tree enabled protocol PVST

VLAN0001
 Root ID    Priority    32769
        Address     5491.AF10.D083
        This bridge is the root
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32769
        Address     5491.AF10.D083
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface       Role Sts Cost     Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------
G0/1            Desg FWD 19       128.1  P2p


VLAN0002
 Root ID    Priority    32770
        Address     5491.AF10.D083
        This bridge is the root
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32770
        Address     5491.AF10.D083
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface       Role Sts Cost     Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------
G0/1            Desg FWD 19       128.1  P2p

Switch_config#
```

### 27.2.10. show spanning-tree pvst instance-list

#### (1) 구문

이 명령어는 PVST 인스턴스와 VLAN 간의 관계를 확인하는 데 사용됩니다.

**show spanning-tree pvst instance-list**

#### (2) 매개변수

없음

**(3) 기본값**

없음

**(4) 사용 지침**

없음

**(5) 명령어 모드**

EXEC, 전역 설정 모드 또는 인터페이스 설정 모드

**(6) 예제**

없음

# 28. RSTP 설정 명령

## 28.1. RSTP 설정 명령어

### 28.1.1. spanning-tree mode rstp

#### (1) 구문

RSTP 기능을 활성화하려면 spanning-tree mode rstp 명령을 실행합니다. RSTP 를 비활성화하려면 no spanning-tree mode 명령을 실행합니다.

**spanning-tree mode rstp**
**no spanning-tree mode**

#### (2) 매개변수

없음

#### (3) 기본값

RSTP 가 활성화되어 있습니다.

#### (4) 사용 지침

없음

#### (5) 예제

다음 명령은 스위치에서 RSTP 를 활성화하는 방법을 보여줍니다.

Switch_config# spanning-tree mode rstp
Switch_config#

### 28.1.2. spanning-tree rstp forward-time

#### (1) 구문

RSTP 의 포워딩 지연 시간을 설정하려면 spanning-tree rstp forward-time time 명령을 실행합니다. RSTP 의 기본 포워딩 지연 시간으로 되돌리려면 no spanning-tree rstp forward-time 명령을 실행합니다.

**spanning-tree rstp forward-time** *time*
**no spanning-tree rstp forward-time**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *time* | 포워딩 지연 시간 (범위: 4 초에서 30 초) |

**(3) 기본값**

15 초

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 RSTP 의 포워딩 지연 시간을 20 초로 설정하는 방법을 보여줍니다.

```
Switch_config# spanning-tree rstp forward-time 20
Switch_config#
```

### 28.1.3. spanning-tree rstp hello-time

**(1) 구문**

RSTP 의 업데이트 간격을 설정하려면 spanning-tree rstp hello-time time 명령을 실행합니다. RSTP 의 기본 업데이트 간격으로 되돌리려면 no spanning-tree rstp hello-time 명령을 실행합니다.

**spanning-tree rstp hello-time** *time*
**no spanning-tree rstp hello-time**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *time* | 업데이트 간격 (범위: 1 초에서 10 초) |

**(3) 기본값**

2 초

**(4) 사용 지침**

로컬 스위치가 루트 브리지로 동작할 때만 설정된 Hello-Time 이 유효합니다.

**(5) 예제**

다음 예제는 RSTP 의 업데이트 간격을 8 초로 설정하는 방법을 보여줍니다.

```
Switch_config# spanning-tree rstp hello-time 8
Switch_config#
```

### 28.1.4. spanning-tree rstp max-age

#### (1) 구문

RSTP BPDU 의 최대 수명을 설정하려면 spanning-tree rstp max-age time 명령을 실행합니다. 기본 수명 시간으로 되돌리려면 no spanning-tree rstp max-age 명령을 실행합니다.

**spanning-tree rstp max-age** *time*
**no spanning-tree rstp max-age**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *time* | 최대 수명 시간 (범위: 6 초에서 40 초). |

#### (3) 기본값

20 초

#### (4) 사용 지침

없음

#### (5) 예제

다음 예제는 RSTP 의 최대 수명 시간을 24 초로 설정하는 방법을 보여줍니다.

```
Switch_config# spanning-tree rstp max-age 24
Switch_config#
```

### 28.1.5. spanning-tree rstp priority

#### (1) 구문

RSTP 의 우선순위 값을 설정하려면 spanning-tree rstp priority value 명령을 실행합니다. 기본 우선순위 값으로 되돌리려면 no spanning-tree rstp priority 명령을 실행합니다.

**spanning-tree rstp priority** *value*
**no spanning-tree rstp priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 브리지의 우선순위 값 (범위: 0 에서 61440, 증가 값은 4096) |

**(3) 기본값**

32768

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 RSTP 의 브리지 우선순위 값을 4096 으로 설정하는 방법을 보여줍니다.

Switch_config# spanning-tree rstp priority 4096
Switch_config#

### 28.1.6. spanning-tree rstp cost

**(1) 구문**

포트의 경로 비용을 설정하려면 spanning-tree rstp cost value 명령을 실행합니다. 기본값으로 되돌리려면 no spanning-tree rstp cost 명령을 실행합니다.

**spanning-tree rstp cost** *value*
**no spanning-tree rstp cost**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 경로 비용 값 (범위: 1 에서 200000000 까지). |

**(3) 기본값**

포트의 연결 속도에 따라 경로 비용이 결정됩니다.
10 Mbps: 2000000
100 Mbps: 200000
1000 Mbps: 20000

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 포트 G0/1 의 경로 비용을 24 로 설정하는 방법을 보여줍니다:

```
Switch_config_g0/1# spanning-tree rstp cost 24
Switch_config_g0/1#
```

### 28.1.7. spanning-tree rstp port-priority

**(1) 구문**

포트의 우선순위 수준을 설정하려면 spanning-tree rstp port-priority value 명령을 실행합니다. 기본값으로 되돌리려면 no spanning-tree rstp port-priority 명령을 실행합니다.

**spanning-tree rstp port-priority** *value*
**no spanning-tree rstp port-priority**

(2) **매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 포트의 우선순위 수준 (범위: 0 에서 240 까지, 증가 값은 16) |

**(3) 기본값**

128

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 포트 G0/1 의 우선순위 수준을 16 으로 설정하는 방법을 보여줍니다:

```
Switch_config_g0/1# spanning-tree rstp port-priority 16
Switch_config_g0/1#
```

### 28.1.8. spanning-tree rstp edge

**(1) 구문**

엣지 포트를 설정하려면 spanning-tree rstp edge 명령을 실행합니다. 기본값으로 되돌리려면 no spanning-tree rstp edge 명령을 실행합니다.

**spanning-tree rstp edge**

**no spanning-tree rstp edge**

**(2) 매개변수**

없음

**(3) 기본값**

자동 확인

**(4) 사용 지침**

없음

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

없음

### 28.1.9. spanning-tree rstp point-to-point

**(1) 구문**

포트의 포인트-투-포인트 연결을 force-true, force-false 또는 auto 로 설정하려면 이 명령을 실행합니다.

**spanning-tree rstp point-to-point [ force-true | force-false | auto ]**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *force-true* | 포트의 포인트-투-포인트 연결을 강제로 true 로 설정 |
| *force-false* | 포트의 포인트-투-포인트 연결을 강제로 false 로 설정 |
| *auto* | 포인트-투-포인트 연결을 자동 확인 (기본값) |

**(3) 기본값**

자동 확인

**(4) 사용 지침**

없음

**(5) 명령어 모드**

인터페이스 설정 모드

**(6) 예제**

없음

### 28.1.10. spanning-tree rstp migration-check

**(1) 구문**

RSTP 의 프로토콜 전환을 다시 시작하려면 spanning-tree rstp migration-check 명령을 실행합니다.

**spanning-tree rstp migration-check**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 사용 지침**

이 명령은 포트에서 프로토콜 전환 확인을 다시 시작하고, STP 호환 모드에서 RSTP 모드로 포트를 변경하며, RSTP BPDU 를 전송할 수 있도록 합니다.

**(5) 명령어 모드**

전역과 인터페이스 설정 모드

**(6) 예제**

다음 예제는 인터페이스 G0/1 에서 프로토콜 전환 확인을 실행하는 방법을 보여줍니다:

```
Switch_config_g0/1#spanning-tree rstp migration-check
Switch_config_g0/1#
```

# 29. MSTP 설정 명령

## 29.1. MSTP 설정 명령어

### 29.1.1. spanning-tree mode mstp

#### (1) 구문

STP 의 실행 모드를 MSTP 로 설정하려면 spanning-tree mode mstp 명령을 실행합니다. STP 를 비활성화하려면 no spanning-tree mode 명령을 실행합니다.

**spanning-tree mode mstp**
**no spanning-tree mode**

#### (2) 매개변수

없음

#### (3) 기본값

MSTP 모드는 비활성화되어 있으며, RSTP 모드가 실행됩니다.

#### (4) 사용 지침

없음

#### (5) 예제

다음 예제는 스위치에서 MSTP 프로토콜을 활성화하는 방법을 보여줍니다:

switch(config)# spanning-tree mode mstp
switch(config)#

### 29.1.2. spanning-tree mstp name

#### (1) 구문

STP 의 지역 이름을 설정하려면 spanning-tree mstp name string 명령을 실행합니다. 기본 이름으로 되돌리려면 no spanning-tree mstp name 명령을 실행합니다.

**spanning-tree mstp name** *string*
**no spanning-tree mstp name**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| String | 이 명령은 이름의 문자 문자열을 구성합니다. 문자열은 최대 32 자까지 가능하며 대소문자를 구분합니다. 기본값은 스위치의 MAC 주소 형식의 문자열입니다. |

**(3) 기본값**

스위치의 MAC 주소 형식으로 된 문자열

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 스위치의 STP 이름을 reg-01 로 설정하는 방법을 보여줍니다.

```
switch(config)# spanning-tree mstp name reg-01
switch(config)#
```

### 29.1.3. spanning-tree mstp revision

**(1) 구문**

STP 의 수정 번호를 설정하려면 spanning-tree mstp revision value 명령을 실행합니다. 기본값으로 되돌리려면 no spanning-tree mstp revision 명령을 실행합니다.

**spanning-tree mstp revision** *value*
**no spanning-tree mstp revision**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| Value | 수정 번호 (0 에서 65535 까지) , 기본값은 0. |

**(3) 기본값**

수정 번호 기본값은 0 입니다.

**(4) 사용 지침**

없음

**(5) 예제**

다음 명령은 STP 의 지역 수정 번호를 100 으로 설정하는 방법을 보여줍니다.

```
switch(config)# spanning-tree mstp revision 100
switch(config)#
```

### 29.1.4. spanning-tree mstp instance

**(1) 구문**

VLAN 을 MSTI 에 매핑하려면 spanning-tree mstp instance instance-id vlan vlan-list 명령을 실행합니다. VLAN 을 CIST 로 재매핑하려면 no spanning-tree mstp instance instance-id 명령을 실행합니다.

**spanning-tree mstp instance** *instance-id* **vlan** *vlan-list*
**no spanning-tree mstp instance** *instance-id*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| instance-id | STP 의 인스턴스 번호로, 1 에서 31 사이의 MSTI 를 의미합니다. |
| vlan-list | STP 에 매핑된 VLAN 목록으로, 1 에서 4094 사이의 값입니다. |

**(3) 기본값**

모든 VLAN 은 CIST(MST00)에 매핑됩니다.

**(4) 사용 지침**

instance-id 는 STP 인스턴스를 나타내는 고유한 값입니다.
vlan-list 는 "1,2,3", "1-5", "1,2,5-10"과 같은 VLAN 그룹을 나타냅니다.

**(5) 예제**

다음 명령은 VLAN2 를 STP 의 인스턴스 1 에 매핑하고, VLAN5,7,10-20 을 인스턴스 2 에 매핑한 후, 이러한 VLAN 을 MST00 으로 재매핑하는 방법을 보여줍니다.

```
Switch_config# spanning-tree mstp instance 1 vlan 2
Switch_config# spanning-tree mstp instance 2 vlan 5,7,10-20
Switch_config# no spanning-tree mstp instance 1
Switch_config# no spanning-tree mstp instance 2
```

### 29.1.5. spanning-tree mstp root

#### (1) 구문

지정된 MSTP 인스턴스를 기본 루트/보조 루트로 설정합니다. 해당 명령의 부정형을 실행하면 MSTP 인스턴스의 우선순위가 기본값으로 복원됩니다.

지정된 MSTP 인스턴스를 기본 루트/보조 루트로 설정하려면 spanning-tree mstp instance-id root {primary | secondary} 명령을 실행합니다. 기본 설정으로 되돌리려면 위 명령의 부정형을 실행하십시오.

spanning-tree mstp instance-id root {primary | secondary}
[ diameter net-diameter [ hello-time seconds ] ]
no spanning-tree mstp instance-id root

diameter 명령과 hello-time 명령은 루트를 설정할 때 MSTP 의 네트워크 지름과 HelloTime 매개변수를 수정할 수 있습니다.

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| instance-id | MSTP 인스턴스, 0 에서 31 사이 |
| primary | MSTP 인스턴스를 기본 루트로 설정 |
| secondary | MSTP 인스턴스를 보조 루트로 설정 |
| net-diameter | 네트워크 지름은 선택 사항입니다.<br>instance-id 매개변수가 0일 때만 유효합니다.<br>지름 값은 2 에서 7 사이입니다. |
| seconds | HelloTime, 선택 사항 (1 에서 10 초 사이) |

#### (3) 기본값

모든 MSTP 인스턴스의 기본 루트의 우선순위 값은 32768 입니다.
네트워크 지름은 7, HelloTime 은 2 초입니다.

#### (4) 사용 지침

diameter 명령과 hello-time 명령은 instance-id 가 0 일 때만 유효합니다.

일반적으로 기본 루트를 설정한 후 프로토콜은 현재 네트워크 루트의 ID 를 자동으로 확인하고, 현재 스위치가 MSTP 인스턴스의 루트가 될 수 있도록 루트 식별자의 우선순위 필드를 24576 으로 설정합니다. 루트의 우선순위 값이 24576 보다 작으면, 프로토콜은 MSTP 우선순위를 4096 만큼 작게 자동으로 설정합니다.

기본 루트 구성과 다르게, 보조 루트를 구성하는 명령을 실행하면 프로토콜은 스위치의 MSTP 우선순위를 28672 로 직접 설정합니다. 따라서 다른 스위치들의 기본값인 32768 우선순위일 때 현재 스위치는 보조 루트가 될 수 있습니다.

**(5) 예제**

다음 명령은 스위치를 CIST 의 기본 루트로 설정하고, 네트워크 지름 3 과 HelloTime 3 을 통해 MSTP 의 시간 매개변수를 다시 계산한 후, 마지막으로 스위치를 MST01 의 보조 루트로 설정하는 예제입니다.

```
Switch_config# spanning-tree mstp 0 root primary diameter 3 hello-time 3
Switch_config# spanning-tree mstp 1 root secondary
```

### 29.1.6. spanning-tree mstp priority

**(1) 구문**

MSTP 인스턴스의 브리지 우선순위를 구성하려면 spanning-tree mstp instance-id priority value 명령을 실행합니다. 기본 설정으로 되돌리려면 no spanning-tree mstp instance-id priority 명령을 실행합니다.

**spanning-tree mstp** *instance-id* **priority** *value*
**no spanning-tree mstp** *instance-id* **priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| instance-id | MSTP 인스턴스 번호, 0 에서 31 사이 |
| value | 브리지 우선순위, 가능한 값: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 |

**(3) 기본값**

모든 MSTP 인스턴스의 브리지 기본 우선순위 값은 32768 입니다.

**(4) 사용 지침**

MSTP 인스턴스의 각 우선순위 값은 독립적으로 설정할 수 있습니다.

**(5) 예제**

이 명령어는 CIST 와 MST01 에서 스위치의 우선순위를 각각 4096 과 8192 로 설정하는 데 사용됩니다.

```
Switch_config# spanning-tree mstp 0 priority 4096
Switch_config# spanning-tree mstp 1 priority 8192
```

### 29.1.7. spanning-tree mstp hello-time

#### (1) 구문

이 명령어는 MSTP 의 HelloTime 을 설정하는 데 사용되며, 부정 명령어는 HelloTime 의 기본 설정을 복원하는 데 사용됩니다.

**spanning-tree mstp hello-time** *seconds*
**no spanning-tree mstp hello-time**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| seconds | 1 초에서 10 초까지 설정 가능하며, 기본값은 2 초입니다 |

#### (3) 기본값

2 초

#### (4) 사용 지침

없음

#### (5) 예제

이 명령어는 MSTP 의 HelloTime 을 10 초로 설정하고, 이후 기본값으로 복원합니다.

```
switch(config)# spanning-tree mstp hello-time 10
switch(config)# no spanning-tree mstp hello-time
```

### 29.1.8. spanning-tree mstp forward-time

#### (1) 구문

이 명령어는 MSTP 의 Forward Delay 를 설정하며, 부정 명령어는 기본 설정을 복원하는 데 사용됩니다.

**spanning-tree mstp forward-time** *seconds*
**no spanning-tree mstp forward-time**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| seconds | 4 초에서 30 초까지 설정 가능하며, 기본값은 15 초입니다. |

**(3) 기본값**

15 초

**(4) 사용 지침**

없음

**(5) 예제**

이 명령어는 MSTP 의 Forward Delay 를 10 초로 설정하고, 이후 기본값으로 복원합니다.

```
Switch_config# spanning-tree mstp forward-time 10
Switch_config# no spanning-tree mstp forward-time
```

### 29.1.9. spanning-tree mstp max-age

**(1) 구문**

MSTP 의 Max Age 매개변수를 설정하려면 spanning-tree mstp max-age seconds 명령을 실행하십시오. 기본 설정으로 되돌리려면 명령의 부정형을 실행하십시오.

**spanning-tree mstp max-age** *seconds*
**no spanning-tree mstp max-age**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| Seconds | 범위: 6 - 40 초. 기본값은 20 초입니다 |

**(3) 기본값**

20 초

**(4) 사용 지침**

없음

**(5) 예제**

다음 명령은 MSTP 의 Max Age 매개변수를 10 초로 설정하는 예입니다.

```
Switch_config# spanning-tree mstp max-age 10
Switch_config# no spanning-tree mstp max-age
```

### 29.1.10. spanning-tree mstp diameter

#### (1) 구문

MSTP 의 네트워크 직경을 설정하려면 spanning-tree mstp diameter net-diameter 명령을 실행하십시오. 기본 설정으로 되돌리려면 no spanning-tree mstp diameter 명령을 실행하십시오.

**spanning-tree mstp diameter** *net-diameter*
**no spanning-tree mstp diameter**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| net-diameter | 범위: 2 - 7. 기본값은 7 입니다. |

#### (3) 기본값

네트워크 직경의 기본값은 7 입니다.

#### (4) 사용 지침

net-diameter 매개변수는 스위치에서 독립적인 설정으로 저장되지 않습니다. 네트워크 직경 구성을 통해 수정된 시간 매개변수는 저장될 수 있습니다. net-diameter 매개변수는 CIST 에서 유효하며 설정 후 STP 의 세 가지 시간 매개변수는 자동으로 상대적으로 유리한 값으로 업데이트될 수 있습니다. STP 의 시간 매개변수는 루트 구성 또는 네트워크 직경 구성을 통해 설정하는 것이 좋습니다. 이 방법을 통해 시간 매개변수의 합리성을 보장할 수 있습니다.

#### (5) 예제

다음 첫 번째 명령은 MSTP 의 브리지 직경을 5 로 설정하는 예입니다. 두 번째 명령은 브리지 직경의 기본값을 복원하는 예입니다.

```
Switch_config# spanning-tree mstp diameter 5
Switch_config# no spanning-tree mstp diameter
```

### 29.1.11. spanning-tree mstp max-hops

#### (1) 구문

MSTP BPDU 의 최대 홉 수를 설정하려면 spanning-tree mstp max-hops hop-count 명령을 실행하십시오. 기본 설정으로 되돌리려면 부정형 명령을 실행하십시오.

**spanning-tree mstp max-hops** *hop-count*
**no spanning-tree mstp max-hops**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| hop-count | 범위: 6 - 40. 기본값은 20 입니다. |

**(3) 기본값**

최대 홉 수의 기본값은 20 입니다.

**(4) 사용 지침**

없음

**(5) 예제**

다음 명령은 MSTP BPDU 의 최대 홉 수를 6 으로 설정하는 예입니다. 두 번째 명령은 최대 홉 수의 기본값을 복원하는 예입니다.

Switch_config# spanning-tree mstp max-hops 6
Switch_config# no spanning-tree mstp max-hops

### 29.1.12. spanning-tree mstp port-priority

**(1) 구문**

STP 인스턴스의 포트 우선순위를 지정하려면 spanning-tree mstp instance-id port-priority value 명령을 실행하십시오. 기본 설정으로 되돌리려면 부정형 명령을 실행하십시오.

**spanning-tree mstp** *instance-id* **port-priority** *value*
**no spanning-tree mstp** instance-id **port-priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| instance-id | STP 인스턴스 번호 (0 ~ 31) |
| Value | 포트 우선순위 값 (다음 값 중 하나) : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 |

**(3) 기본값**

모든 STP 인스턴스에서 포트 우선순위의 기본값은 128 입니다.

**(4) 사용 지침**

없음

**(5) 예제**

다음 첫 번째 명령은 CIST 에서 포트 G0/1 의 우선순위를 16 으로 설정하는 예입니다. 두 번째 명령은 기본값을 복원하는 예입니다.

Switch_config_g0/1# spanning-tree mstp 0 port-priority 16
Switch_config_g0/1# no spanning-tree mstp 0 port-priority

### 29.1.13. spanning-tree mstp cost

**(1) 구문**

특정 STP 인스턴스에서 포트의 경로 비용을 설정하려면 spanning-tree mstp instance-id cost value 명령을 실행하십시오. 기본 설정으로 되돌리려면 부정형 명령을 실행하십시오.

**spanning-tree mstp** *instance-id* **cost** *value*
**no spanning-tree mstp** *instance-id* **cost**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| instance-id | STP 인스턴스 번호 (0 ~ 31) |
| value | 포트의 경로 비용 (1 ~ 200,000,000). |

**(3) 기본값**

포트의 연결 속도에 따라 다릅니다:
10 Mbps: 2000000
100 Mbps: 200000
1000 Mbps: 20000

**(4) 사용 지침**

없음

**(5) 예제**

다음 명령은 CIST 에서 포트 G0/1 의 경로 비용을 200 으로 설정하는 예입니다:

Switch_config_g0/1# spanning-tree mstp 0 cost 200

Switch_config_g0/1#

### 29.1.14. spanning-tree mstp edge

#### (1) 구문

엣지 포트를 설정하려면 spanning-tree mstp edge 명령을 실행하십시오. 기본 설정으로 되돌리려면 no spanning-tree mstp edge 명령을 실행하십시오.

**spanning-tree mstp edge**
**no spanning-tree mstp edge**

#### (2) 매개변수

없음

#### (3) 기본값

자동 확인 엣지포트

#### (4) 사용 지침

없음

#### (5) 예제

없음

### 29.1.15. spanning-tree mstp point-to-point

#### (1) 구문

포트의 연결 유형을 설정하려면 spanning-tree mstp point-to-point { force-true | force-false | auto } 명령을 실행하십시오. 연결 유형을 자동 확인 모드로 되돌리려면 no spanning-tree mstp point-to-point 명령을 실행하십시오.

**spanning-tree mstp point-to-point { force-true | force-false | auto }**
**no spanning-tree mstp point-to-point**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| force-true | 포트 연결 모드를 포인트-투-포인트로 설정 |
| force-false | 포트 연결 모드를 공유 모드로 설정 |
| auto | 포트 연결 모드를 자동 확인 모드로 설정 (기본 모드) |

**(3) 기본값**

MSTP 는 기본적으로 포트 연결 모드를 자동으로 확인합니다.

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 포트 G0/1 의 연결 모드를 공유로 설정하는 방법을 보여줍니다.

```
Switch_config_g0/1# spanning-tree mstp point-to-point force-false
Switch_config_g0/1#
```

### 29.1.16. spanning-tree mstp mst-compatible

**(1) 구문**

MST 호환 모드를 활성화/비활성화하려면, 전역 설정 모드.
**spanning-tree mstp mst-compatible**
**no spanning-tree mstp mst-compatible**

MST 호환 모드를 활성화/비활성화하려면, 인터페이스 설정 모드.
**spanning-tree mstp mst-compatible {enable | disable}**
**no spanning-tree mstp mst-compatible**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| **enable** | MST 호환 모드를 활성화합니다 |
| **disable** | MST 호환 모드를 비활성화합니다. |

**(3) 기본값**

MST 호환 모드는 기본적으로 활성화되지 않으며, 스위치는 호환 모드에서 BPDU 를 전송하는 다른 스위치와 영역을 설정할 수 없습니다.

**(4) 사용 지침**

MST 호환 모드를 활성화한 후, 다른 MSTP 프로토콜을 실행하는 연결된 다른 스위치를 CIST 의 루트로 설정하여 스위치가 메시지를 수신하여 MSTP 호환 모드로 진입할 수 있도록 합니다.

**(5) 예제**

다음 명령은 전역 설정 모드에서 MST 호환 모드를 활성화하는 명령입니다:

switch(config)#spanning-tree mstp mst-compatible

### 29.1.17. spanning-tree mstp migration-check

**(1) 구문**

포트에서 체크된 STP 정보를 지우고 프로토콜 변환 프로세스를 다시 시작합니다.
**spanning-tree mstp migration-check**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 사용 지침**

이 명령은 전역 설정 모드와 포트 설정 모드에서 유효합니다.

**(5) 예제**

다음 명령은 모든 포트에서 프로토콜 변환을 먼저 확인하고, 그 후에 G0/1 포트에서 프로토콜 변환을 다시 확인하는 예제입니다.

Switch_config# spanning-tree mstp migration-check
Switch_config# interface g0/1
Switch_config_g0/1# spanning-tree mstp migration-check

### 29.1.18. spanning-tree mstp restricted-role

**(1) 구문**

포트에서 역할 제한을 활성화/비활성화합니다.

**[no] spanning-tree mstp restricted-role**

**(2) 매개변수**

없음

**(3) 기본값**

포트의 역할 제한이 비활성화되어 있습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

역할 제한을 활성화하면, 해당 포트는 루트 포트로 선택되지 않습니다.

**(6) 예제**

없음

### 29.1.19. spanning-tree mstp restricted-tcn

**(1) 구문**

포트에서 TCN 제한을 활성화/비활성화합니다.

**[no] spanning-tree mstp restricted-tcn**

**(2) 매개변수**

없음

**(3) 기본값**

포트에서 TCN 제한이 비활성화되어 있습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

포트에서 TCN 제한을 활성화하면, 토폴로지 변경 사항을 다른 포트로 전송하지 않습니다.

**(6) 예제**

없음

### 29.1.20. show spanning-tree mstp

#### (1) 구문

위 명령은 MSTP 정보를 확인하는 데 사용됩니다. show spanning-tree mstp 명령을 실행하면 모든 STP 인스턴스에 대한 정보가 표시됩니다.

**show spanning-tree mstp [ instance** *instance-id*]

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| instance-id | STP 인스턴스 번호, 0 에서 15 까지의 값 |

#### (3) 기본값

없음

#### (4) 사용 지침

이 명령은 모니터링 모드, 전역 설정 모드 또는 포트 모드에서 유효합니다.

#### (5) 예제

다음 명령은 모든 STP 인스턴스를 확인하는 예제입니다. 여기서 MST00 은 CIST 를 나타내며, Type 필드는 포트 연결 유형을 나타냅니다.
Switch#show spanning-tree mstp

```
MST00      Vlans Mapped:  1,4-4094
Root     Address  5491.AF10.D083  Priority  32768 (32768 mst-id 0)
Root       This root is the CIST and regional root
Configured  Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times  Hello Time 2, Forward Delay 15, Max Age 20

Interface      Role Sts Cost     Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------
F0/1           Desg FWD 200000    128.1   P2p
F0/3           Back BLK 200000    128.3   P2p
F0/47          Desg FWD 200000    128.47  Edge

MST01      Vlans Mapped:  2
Root     Address  5491.AF10.D083 Priority  32769 (32768 mst-id 1)
Root       This root for MST01

Interface      Role Sts Cost     Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------
F0/1           Desg FWD 200000    128.1   P2p
```

```
MST02      Vlans Mapped:  3
Root     Address  5491.AF10.D083  Priority  32770 (32768 mst-id 2)
Root       This root for MST02

Interface       Role Sts Cost     Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------
F0/1            Desg FWD 200000    128.1   P2p
```

### 29.1.21. show spanning-tree mstp region

#### (1) 구문

MSTP 에 대한 지역 구성 정보를 확인하는 명령입니다.

**show spanning-tree mstp region**

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 사용 지침

없음

#### (5) 예제

다음은 VLAN 과 STP 인스턴스 간의 관계를 보여주는 MST 구성 테이블 정보입니다.

```
switch(config)# show spanning-tree mstp region

MST Region:
 Name:   [reg01]
 Revision: [0]

MST Config Table:
 Instance    VLAN IDs
----------   ----------
     0    1,4-4094
     1    2
     2    3
```

### 29.1.22. show spanning-tree mstp detail

#### (1) 구문

이 명령은 MSTP 에 대한 자세한 정보를 확인하는 데 사용됩니다.

**show spanning-tree mstp detail**

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 사용 지침

없음

#### (5) 예제

다음은 show spanning-tree mstp detail 명령 실행 후의 자세한 STP 정보입니다. 포트 연결 유형과 선택적 특성이 포함됩니다:
Switch#show spanning-tree mstp detail

MST00 Vlans Mapped: 1,4-4094
Root Address 5491.AF10.D083 Priority 32768 (32768 mst-id 0)
Root This root is the CIST and regional root
Configured Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times Hello Time 2, Forward Delay 15, Max Age 20

FastEthernet0/1 of MST00 is designated forwarding
Port Info Port ID 128.1 Priority 128 Cost 200000
Designated Root Address 5491.AF10.D083 Priority 32768 Cost 0
CIST Regional Root Address 5491.AF10.D083 Priority 32768 Cost 0
Designated Root Address 5491.AF10.D083 Priority 32768 Port ID 128.1
Edge Port: disabled Link Type: point-to-point (auto)
Bpdu Guard: disabled (default) Root Guard: disabled (default)
Loop Guard: disabled (default)
Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
Bpdu sent 335, received 5

FastEthernet0/3 of MST00 is backup blocking
Port Info Port ID 128.3 Priority 128 Cost 200000
Designated Root Address 5491.AF10.D083 Priority 32768 Cost 0
CIST Regional Root Address 5491.AF10.D083 Priority 32768 Cost 0

Designated Root Address 5491.AF10.D083 Priority 32768 Port ID 128.1
Edge Port: disabled Link Type: point-to-point (auto)
Bpdu Guard: disabled (default) Root Guard: disabled (default)
Loop Guard: disabled (default)
Timers: message expires in 5 sec, forward delay 15 sec, up time 662 sec
Number of transitions to forwarding state: 0
Bpdu sent 5, received 335

FastEthernet0/47 of MST00 is designated forwarding
Port Info Port ID 128.47 Priority 128 Cost 200000
Designated Root Address 5491.AF10.D083 Priority 32768 Cost 0
CIST Regional Root Address 5491.AF10.D083 Priority 32768 Cost 0
Designated Root Address 5491.AF10.D083 Priority 32768 Port ID 128.47
Edge Port: enabled (auto) Link Type: point-to-point (auto)
Bpdu Guard: disabled (default) Root Guard: disabled (default)
Loop Guard: disabled (default)
Timers: message expires in 0 sec, forward delay 0 sec, up time 1485 sec
Number of transitions to forwarding state: 1
Bpdu sent 744, received 0

MST01 Vlans Mapped: 2
Root Address 5491.AF10.D083 Priority 32769 (32768 mst-id 1)
Root This root for MST01

FastEthernet0/1 of MST01 is designated forwarding
Port Info Port ID 128.1 Priority 128 Cost 200000
Designated Root Address 5491.AF10.D083 Priority 32769 Cost 0
Designated Root Address 5491.AF10.D083 Priority 32769 Port ID 128.1
Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

MST02 Vlans Mapped: 3
Root Address 5491.AF10.D083 Priority 32770 (32768 mst-id 2)
Root This root for MST02

FastEthernet0/1 of MST02 is designated forwarding
Port Info Port ID 128.1 Priority 128 Cost 200000
Designated Root Address 5491.AF10.D083 Priority 32770 Cost 0
Designated Root Address 5491.AF10.D083 Priority 32770 Port ID 128.1
Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

### 29.1.23. show spanning-tree mstp interface

#### (1) 구문

이 명령은 MSTP 하에 실행 중인 포트에 대한 정보를 확인하는 데 사용됩니다.

**show spanning-tree mstp interface** *interface-id*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| interface-id | 포트 이름, 예: "G5/1", "GigaEthernet5/2" |

#### (3) 기본값

없음

#### (4) 사용 지침

없음

#### (5) 예제

다음은 show spanning-tree mstp interface g0/1 명령을 실행한 후 G0/1 포트에 대한 정보입니다:

```
GigaEthernet0/1 of MST00 is designated forwarding
Port Info          Port ID 128.1        Priority 128   Cost 200000
Designated Root    Address 5491.AF10.D083  Priority 32768  Cost 0
CIST Regional Root  Address 5491.AF10.D083  Priority 32768  Cost 0
Designated Bridge   Address 5491.AF10.D083  Priority 32768  Port ID 128.1
Edge Port: disabled            Link Type: point-to-point (auto)
Bpdu Guard: disabled (default)     Root Guard: disabled (default)
Loop Guard: disabled (default)
Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
Bpdu sent 430, received 5

GigaEthernet0/1 of MST01 is designated forwarding
Port Info          Port ID 128.1        Priority 128   Cost 200000
Designated Root    Address 5491.AF10.D083  Priority 32769  Cost 0
Designated Bridge   Address 5491.AF10.D083  Priority 32769  Port ID 128.1
Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0

GigaEthernet0/1 of MST02 is designated forwarding
```

```
Port Info           Port ID 128.1         Priority 128    Cost 200000
Designated Root     Address 5491.AF10.D083  Priority 32770  Cost 0
Designated Bridge   Address 5491.AF10.D083 Priority 32770  Port ID 128.1
Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0

Instance Role Sts Cost     Pri.Nbr Vlans Mapped
-------- ---- --- --------- ------- --------------------
0      Desg FWD 200000   128.1   1,4-4094
1      Desg FWD 200000   128.1   2
2      Desg FWD 200000   128.1   3
```

### 29.1.24. show spanning-tree mstp protocol-migration

**(1) 구문**

이 명령은 포트가 MSTP 하에 있을 때 프로토콜 변환 정보를 확인하는 데 사용됩니다.

**show spanning-tree mstp protocol-migration**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 사용 지침**

없음

**(5) 예제**

다음 예제는 show spanning-tree mstp protocol-migration 명령을 실행한 후 프로토콜 변환에 대한 정보를 보여줍니다. 여기서 포트 G0/1 은 802.1D STP 모드로 전환되었습니다:

```
Switch#show spanning-tree mstp protocol-migration

MSTP Port Protocol Migration

Interface      Protocol
-------------- ---------- ------------
G0/1           802.1D
```

# 30. STP Optional Characteristic Configuration Commands

## 30.1. STP Optional Characteristic Configuration Commands

### 30.1.1. spanning-tree portfast

#### (1) 구문

스위치에서 Bridge Protocol Data Unit (BPDU) 필터링을 기본적으로 모든 PortFast 포트에서 활성화하려면, global 설정 모드에서 다음 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

spanning-tree portfast {bpdufilter Default | bpduguard Default | Default}
no spanning-tree portfast {bpdufilter Default | bpduguard Default | Default}

인터페이스가 링크업(Link-Up) 상태가 되자마자 대기 시간 없이 즉시 Forwarding 상태로 전환되도록 PortFast 모드를 활성화하려면, 인터페이스 설정 모드에서 다음 명령어를 사용합니다.

기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree portfast** [disable]
**no spanning-tree portfast**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| bpdufilter | BPDU 필터를 활성화합니다. |
| bpduguard | BPDU 가드를 활성화합니다. |
| default | 기본 설정을 적용합니다. |

#### (3) 기본값

비활성화

#### (4) 사용지침

SSTP/PVST 모드에서 PortFast 기능은 포트가 즉시 Forwarding 상태로 전환되도록 하여, 일반적인 STP 상태 변경 절차를 거치지 않도록 합니다.

하지만, RSTP/MSTP 모드에서는 이 설정이 적용되지 않습니다.

PortFast 가 설정된 포트에는 BPDU Guard 또는 BPDU Filter 를 추가적으로 구성하여 보호하는 것이 권장됩니다.

**(5) 명령어 모드**

전역 과 인터페이스 설정 모드

**(6) 예제**

글로벌 PortFast 모드 활성화 예제:
Switch(config)# spanning-tree portfast Default
Switch(config)#
특정 인터페이스(g0/1)에서 PortFast 모드 활성화 예제:
Switch_config_g0/1# spanning-tree portfast
Switch_config_g0/1#

### 30.1.2. spanning-tree bpduguard

**(1) 구문**

특정 인터페이스에서 BPDU Guard 를 활성화하려면 인터페이스 설정 모드에서 다음 명령어를 사용합니다.

기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree bpduguard {disable | enable}**
**no spanning-tree bpduguard**

**(2) 매개변수**

없음

**(3) 기본값**

비활성화

**(4) 사용 지침**

SSTP/PVST 모드에서 BPDU Guard 및 PortFast 가 설정된 포트가 BPDU 를 수신하면, 해당 포트는 강제로 차단(Shutdown) 됩니다.

사용자는 수동 설정(manual configuration)을 통해 포트를 다시 활성화할 수 있습니다.

RSTP/MSTP 모드에서 BPDU Guard 가 설정된 포트가 BPDU 를 수신하면, 해당 포트는 일정 시간 동안 Blocking 상태로 설정됩니다.

**(5) 명령어 모드**

업링크(Uplink) 인터페이스 설정 모드

**(6) 예제**

인터페이스 g0/1 에서 BPDU Guard 활성화 예제:

```
Switch_config_g0/1# spanning-tree bpduguard enable
Switch_config_g0/1#
```

### 30.1.3. spanning-tree bpdufilter

**(1) 구문**

특정 인터페이스에서 BPDU Filtering 을 활성화하려면 인터페이스 설정 모드에서 다음 명령어를 사용합니다.

기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree bpdufilter {disable | enable}**
**no spanning-tree bpdufilter**

**(2) 매개변수**

없음

**(3) 기본값**

비활성화

**(4) 사용 지침**

SSTP/PVST 모드에서 BPDU Filtering 및 PortFast 가 설정된 포트가 BPDU 를 수신하면, 해당 포트의 BPDU Filtering 및 PortFast 기능이 자동으로 비활성화됩니다.

이후 해당 포트는 일반 포트(Ordinary Port) 로 변경되며, Listening → Learning 단계를 거쳐 Forwarding 상태로 전환됩니다.

RSTP/MSTP 모드에서는 이 기능이 적용되지 않습니다.

**(5) 명령어 모드**

업링크(Uplink) 인터페이스 설정 모드

**(6) 예제**

인터페이스 g0/1 에서 BPDU Filtering 활성화 예제:

```
Switch_config_g0/1# spanning-tree bpdufilter enable
Switch_config_g0/1#
```

### 30.1.4. spanning-tree uplinkfast

#### (1) 구문

Spanning Tree 의 UplinkFast 기능을 활성화하려면 다음 명령어를 사용합니다.

기능을 비활성화하려면 no 형식의 명령어를 사용합니다.

**spanning-tree uplinkfast**
**no spanning-tree uplinkfast**

#### (2) 매개변수

없음

#### (3) 기본값

비활성화

#### (4) 사용 지침

UplinkFast 기능은 SSTP/PVST 모드에서만 유효합니다.

#### (5) 명령어 모드

전역 설정

#### (6) 예제

UplinkFast 기능 활성화 예제:

Switch(config)# spanning-tree uplinkfast
Switch(config)#

### 30.1.5. spanning-tree backbonefast

#### (1) 구문

Spanning Tree 의 BackboneFast 기능을 활성화하려면 다음 명령어를 사용합니다.

기능을 비활성화하려면 no 형식의 명령어를 사용합니다.

**spanning-tree backbonefast**
**no spanning-tree backbonefast**

**(2) 매개변수**

없음

**(3) 기본값**

비활성화

**(4) 사용 지침**

BackboneFast 기능은 SSTP/PVST 모드에서만 유효합니다.

**(5) 명령어 모드**

전역 설정

**(6) 예제**

BackboneFast 기능 활성화 예제:

```
Switch(config)# spanning-tree backbonefast
Switch(config)#
```

### 30.1.6. spanning-tree guard

**(1) 구문**

Guard 모드를 활성화 또는 비활성화하려면 다음 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

**spanning-tree guard** {loop | none | root}
**no spanning-tree guard**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *loop* | Guard loop. |
| *none* | Guard none. |
| root | Guard root. |

**(3) 기본값**

비활성화

**(4) 사용 지침**

Root Guard: 높은 우선순위의 BPDU 를 수신하여 포트가 Root 포트가 되는 것을 방지합니다.

Loop Guard: Root 포트 또는 Alternate 포트가 Designated 포트로 변경될 경우를 보호합니다. BPDU 를 지속적으로 수신하지 못할 경우 루프 발생을 방지합니다.

**(5) 명령어 모드**

업링크(Uplink) 인터페이스 설정 모드

**(6) 예제**

인터페이스 g0/1 에서 Root Guard 활성화 예제:

```
Switch_config_g0/1# spanning-tree guard root
Switch_config_g0/1#
```

### 30.1.7. spanning-tree loopguard

**(1) 구문**

모든 포트에서 기본적으로 Loop Guard 를 활성화하려면 다음 명령어를 사용합니다.
비활성화하려면 no 형식의 명령어를 사용합니다.

**spanning-tree loopguard** Default

**(2) 기본값**

없음

**(3) 사용 지침**

없음

**(4) 명령어 모드**

전역 설정

**(5) 예제**

Loop Guard 활성화 예제:

```
Switch(config)# spanning-tree loopguard Default
Switch(config)#
```

### 30.1.8. spanning-tree loopfast

#### (1) 구문

Loop Fast 를 설정하려면 글로벌 설정 모드에서 다음 명령어를 사용합니다.
**spanning-tree loopfast**

기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다
**spanning-tree loopfast**
**spanning-tree loopfast disable**

이 명령어를 사용하여 Loop Fast 를 설정할 수 있습니다. 기본 설정으로 복원하려면 no 형식의 명령어를 사용하십시오.

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 사용 지침

이 명령어는 기술 지원 담당자의 안내에 따라 설정하십시오.

#### (5) 명령어 모드

전역 설정 과 인터페이스 설정

#### (6) 예제

다음 예제는 글로벌 설정 모드에서 인터페이스 G0/1 에 대해 Loop Fast 를 활성화한 후 비활성화하는 방법을 보여줍니다.

```
Switch_config#spanning-tree loopfast
Switch_config#int g0/1
Switch_config_g0/1#spanning-tree loopfast disable
Switch_config_g0/1#exit
Switch_config#
```

### 30.1.9. spanning-tree fast-aging

#### (1) 구문

이 명령어는 주소 테이블의 빠른 에이징(Fast Aging)을 활성화/비활성화하는 데 사용됩니다.
**spanning-tree fast-aging**

**no spanning-tree fast-aging**

이 명령어는 주소 테이블의 빠른 에이징 보호(Fast Aging Protection)를 활성화/비활성화하는 데 사용됩니다.
**spanning-tree fast-aging protection**
**no spanning-tree fast-aging protection**

이 명령어는 주소 테이블의 에이징 보호 시간을 설정하는 데 사용됩니다.
**spanning-tree fast-aging protection time** *value*
**no spanning-tree fast-aging protection time**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *value* | 에이징 보호 시간(기본값: 15 초, 범위: 10~60 초) |

**(3) 기본값**

기본적으로 빠른 에이징(Fast Aging)이 활성화되며 보호 기능은 비활성화됩니다.

**(4) 사용 지침**

없음

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 빠른 에이징 보호(Fast Aging Protection)를 활성화하고 보호 시간을 30 초로 설정하는 방법을 보여줍니다.

Switch_config#spanning-tree fast-aging protection
Switch_config#spanning-tree fast-aging protection time 30

### 30.1.10. spanning-tree fast-aging flush-fdb

**(1) 구문**

이 명령어는 FDB-Flush 기능을 활성화/비활성화하는 데 사용됩니다.

spanning-tree fast-aging flush-fdb
no spanning-tree fast-aging flush-fdb

**(2) 매개변수**

없음

**(3) 기본값**

기본적으로 FDB-Flush 가 활성화됩니다.

**(4) 사용 지침**

이 명령어는 기술 지원 담당자의 안내에 따라 설정하십시오. FDB-Flush 는 빠른 에이징(Fast Aging) 기능과 독립적으로 동작합니다.

no spanning-tree fast-aging 명령어가 설정되지 않은 상태에서도 FDB-Flush 를 구성할 수 있습니다. 빠른 에이징 보호(Fast Aging Protection)는 FDB-Flush 에 영향을 주지 않습니다.

**(5) 명령어 모드**

전역 설정 모드

**(6) 예제**

다음 예제는 빠른 에이징(Fast Aging)을 비활성화하고 FDB-Flush 를 활성화하는 방법을 보여줍니다:

```
Switch_config#no spanning-tree fast-aging
Switch_config#spanning-tree fast-aging flush-fdb
```

# 31. 이더넷 자동보호절체(EAPS)

## 31.1. 개요

이더넷 자동보호절체 프로토콜은 이더넷 링 토폴로지를 구성하기 위해 특별히 고안된 특별한 유형의 링크 계층 프로토콜입니다. 이더넷 자동보호절체 프로토콜은 완전한 링 토폴로지에서 하나의 링크를 차단하여 데이터 루프가 브로드캐스트 스톰을 형성하는 것을 방지합니다. 링크가 끊어진 경우 프로토콜은 이전에 종료된 링크를 즉시 다시 시작합니다. 이러한 방식으로, 링 네트워크들 사이의 노드들은 서로 통신합니다.

링 보호 프로토콜 및 STP 는 모두 링크 계층의 토폴로지 제어에 사용됩니다. STP 는 네트워크 토폴로지의 변화를 홉 단위로 전송하는 모든 종류의 복잡한 네트워크에 적합합니다. 링 보호 프로토콜은 링 토폴로지에 사용되며 네트워크 토폴로지의 변경을 전송하기위한 메커니즘을 적용합니다. 따라서 링 네트워크에서 링 보호 프로토콜의 수렴은 STP 보다 우수합니다. 사운드 네트워크에서 링 보호 프로토콜은 50ms 이내에 네트워크 통신을 재개할 수 있습니다.

Note:
EAPS 는 스위치를 다수의 물리적 링의 노드로 구성하여 토폴로지를 구성할 수 있도록 지원합니다.

## 31.2. EAPS 개념

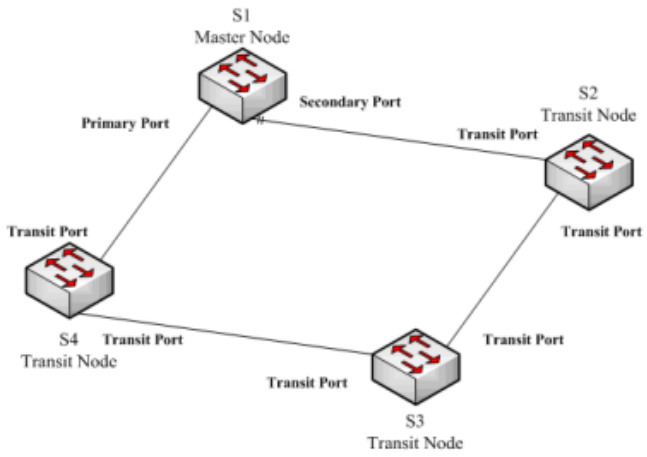



그림 1.1 EAPS 이더넷 링

### 31.2.1. 링 노드의 역할

이더넷 링의 각 스위치는 링 노드입니다. 링 노드는 마스터 노드와 중계 노드로 분류됩니다. 이더넷 링에 있는 스위치 하나만 단순한 마스터 노드로 사용할 수 있고 다른 스위치는 중계 노드로 사용할 수 있습니다.

마스터 노드: 링의 토폴로지가 완료되었는지, 루프백을 제거하는지, 다른 스위치를 제어하여 토폴로지 정보를 업데이트하는지 여부를 확실하게 알 수 있습니다.

중계 노드: 링의 로컬 포트 상태 만 확인하고 마스터 노드에 잘못된 링크를 알립니다.

각 노드의 역할은 구성을 통해 사용자가 지정할 수 있습니다. 문제는 동일한 링의 각 스위치를 한 종류의 노드로만 구성할 수 있다는 것입니다. 그림 1.1 에서 스위치 S1 은 링 네트워크의 마스터 노드이고 스위치 S2, S3 및 S4 는 중계 노드입니다.

### 31.2.2. 링 포트의 역할

EAPS 는 각 스위치가 링 네트워크에 연결할 수 있는 두 개의 포트를 요구합니다. 링 네트워크의 각 포트도 구성을 통해 지정해야 하며 프로토콜은 다음과 같은 종류의 포트 역할을 지원합니다.

기본 포트: 기본 포트는 마스터 노드에서만 구성할 수 있습니다. 마스터 노드는 기본 포트를 통해 링 감지 패킷을 전송합니다.

보조 포트: 마스터 노드에서만 보조 포트를 구성할 수 있습니다. 마스터 노드는 2 차 포트로부터 링 검출 패킷을 수신하고 링 네트워크의 토폴로지가 완료되었는지 여부를 판단한다. 완벽한 토폴로지에서 마스터 노드는 보조 포트에서 데이터 패킷을 차단하고 루프백이 발생하지 않도록 합니다. 링 네트워크상의 링크가 인터럽트 된 후, 마스터 노드는 데이터 패킷을 포워딩하기 위해 제 2 포트를 열 것이다

전송 포트: 전송 포트는 전송 노드에서만 구성할 수 있습니다. 중계 노드가 링 네트워크를 연결하는 두 포트는 모두 중계 포트입니다.

노드의 스위치 역할과 제어 VLAN 이 구성된 후에는 링 네트워크의 각 포트를 하나의 포트 역할로만 구성할 수 있습니다. 그림 1.1 에서와 같이 마스터 노드 S1 이 중계 노드 S4 를 연결하는 포트는 기본 포트이고 S1 을 통해 연결되는 포트는 보조 포트이며 다른 스위치가 링 네트워크를 연결하는 포트는 모든 중계 포트입니다.

Note:
스위치가 여러 개의 링에 속하도록 구성하려면 스위치가 다른 물리적 포트를 통해 다른 링을 연결해야 합니다.

### 31.2.3. 제어 VLAN 및 데이터 VLAN

개인 제어 VLAN 은 마스터 노드와 중계 노드 간에 사용되어 프로토콜 패킷을 전송합니다. 이 제어 VLAN 은 사용자 구성을 통해 지정되며 링의 포트는 사용자가 제어 VLAN 에 추가하므로 프로토콜 패킷이 정상적으로 전달될 수 있습니다. 일반적으로 링 네트워크의 각 포트는 제어 VLAN 에서 전달 상태에 있고 링 네트워크에 속하지 않은 포트는 제어 VLAN 패킷을 전달할 수 없습니다.

Note:
스위치의 각 링에 서로 다른 제어 VLAN 을 지정할 수 있습니다. 제어 VLAN 은 L2/L3 통신이 아닌 링 네트워크의 제어 패킷을 전달하는 데에만 사용됩니다. 예를 들어, 제어 VLAN 에 해당하는 VLAN 포트가 구성된 경우 VLAN 포트의 IP 주소는 다른 장치를 통해 핑 (ping) 될 수 없습니다. 제어 VLAN 을 제외한 VLAN 은 모든 데이터 VLAN 이며 일반 서비스 또는 관리 패킷의 패킷을 전송하는 데 사용됩니다.

Note:
데이터 VLAN 은 일반 L2/L3 통신에 사용될 수 있습니다. 예를 들어 데이터 VLAN 에 해당하는 VLAN 포트를 구성하고 동적 라우팅 프로토콜을 구성할 수 있습니다.

#### 31.2.4. Mac 주소의 에이징

이더넷 링 보호 프로토콜은 토폴로지가 변경될 때 스위치의 MAC 주소 테이블의 에이징을 제어함으로써 데이터 패킷을 올바른 링크로 전송할 수 있습니다. 일반적으로 MAC 주소 테이블에서 MAC 주소의 경과 시간은 300 초입니다. 링 보호 프로토콜은 짧은 시간에 MAC 주소 테이블의 에이징을 제어할 수 있습니다.

#### 31.2.5. 완전한 링 네트워크의 상태

마스터 노드와 중계 노드는 현재 링 네트워크가 상태 기호 "COMPLETE"를 통해 완료되었는지 여부를 표시할 수 있습니다. 마스터 노드에서 링 네트워크의 모든 링크가 정상인 경우에만 기본 포트가 전달 상태에 있고 보조 포트가 차단 상태에 있습니다. "COMPLETE"기호는 실제 상태 일 수 있고, 전송 노드에서는 두 개의 전송 포트가 전달 상태에 있으면 "COMPLETE"기호가 true 가 될 수 있습니다.

링 네트워크의 상태 기호는 사용자가 현재 네트워크의 토폴로지 상태를 판단하는 데 도움이 됩니다.

## 31.3. EAPS 패킷의 종류

EAPS 패킷은 표 1.1 에서와 같이 다음 유형으로 분류할 수 있습니다.

| 패킷유형 | 설명 |
|---|---|
| Loopback detection (HEALTH) | 이것은 링 네트워크의 토폴로지가 완료되었는지를 검출하기 위해 마스터 노드에 의해 전송됩니다. |
| LINK-DOWN | 링에서 링크 중단이 발생했음을 나타냅니다. 이러한 종류의 패킷은 중계 노드에서 전송됩니다. |
| RING-DOWN-FLUSH-FDB | 링 네트워크가 중단된 후 마스터 노드가 전송하고 패킷은 중계 노드의 MAC 주소 에이징 테이블을 표시합니다. |

| | |
|---|---|
| RING-UP-FLUSH-FDB | 링 네트워크가 복구된 후 마스터 노드가 전송하고 패킷은 중계 노드의 MAC 주소 에이징 테이블을 표시합니다. |

## 31.4. 패스트 이더넷 링 보호 메커니즘

### 31.4.1. 마스터 노드의 링 검출 및 제어

마스터 노드는 구성 가능한 기간에 기본 포트를 통해 제어 패킷에 HEALTH 패킷을 전송합니다. 정상적인 경우, HEALTH 패킷은 링 네트워크의 다른 모든 노드를 통과하여 마침내 마스터 노드의 2 차 포트에 도달합니다.

보조 포트는 기본 조건의 모든 데이터 VLAN 을 차단합니다. HEALTH 패킷을 계속 수신하면 보조 포트는 데이터 VLAN 을 차단하고 루프를 차단합니다. 보조 포트가 특정 시간 (구성할 수 있음)의 기본 포트에서 HEALTH 패킷을 수신하지 않으면 링 네트워크가 유효하지 않다고
간주합니다. 그런 다음 마스터 노드는 보조 포트에서 데이터 VLAN 차단을 제거하고 로컬 MAC 주소 표를 오래 사용하고 RING-DOWN-FLUSH-FDB 패킷을 전송하여 다른 노드에 알립니다.

마스터 노드가 데이터 VLAN 에 대해 열린 보조 포트에서 HEALTH 패킷을 수신하면 링 네트워크가 재개됩니다. 이 경우 마스터 노드는 보조 포트에서 데이터 VLAN 을 즉시 차단하고 로컬 토폴로지 정보를 업데이트하고 다른 노드가 RING-UP-FLUSH-FDB 패킷을 통해 MAC 주소 테이블을 에이징 하도록 보고합니다.

Hello-time 노드와 Fail-time 노드에서 관련 명령을 구성하여 주 포트가 HEALTH 패킷을 전송할 간격을 수정하고 보조 포트가 HEALTH 패킷을 대기하는 시간 제한을 수정할 수 있습니다.

### 31.4.2. 중계 노드의 무효 링크 통지

중계 노드의 중계 포트가 효과가 없으면 다른 중계 포트가 LINK-DOWN 패킷을 즉시 전송하여 다른 노드에 알립니다. 정상적인 경우 패킷은 다른 중계 노드를 통과하여 마침내 마스터 노드의 한 포트에 도착합니다.

마스터 노드는 LINK-DOWN 패킷을 수신한 후 링 네트워크가 유효하지 않다고 판단합니다. 이 경우 마스터 노드는 보조 포트에서 데이터 VLAN 차단을 제거하고 로컬 MAC 주소 표를 오래 사용하고 RING-DOWN-FLUSH-FDB 패킷을 전송하고 다른 노드에 알립니다.

### 31.4.3. 중계 노드의 링크 재시작

중계 포트가 재개된 후에는 데이터 VLAN 패킷을 즉시 전송하지 않고 사전 전달 상태가 됩니다. 프리 포워딩 상태의 중계 포트는 제어 VLAN 에서 제어 패킷 만 전송 및 수신합니다.

링 네트워크에서 유효하지 않은 중계 포트가 하나뿐이며 포트가 프리 포워딩 상태가 되면 마스터 노드의 보조 포트는 기본 포트에서 HEALTH 패킷을 다시 수신할 수 있습니다. 이 경우 마스터 노드는 보조 포트의 데이터 VLAN 을 다시 차단하고 에이징 주소 테이블의 알림을 외부로 전송합니다. 프리 포워딩 상태의 중계 포트가 있는 노드가 에이징 주소 테이블의 알림을 수신하면 노드는 먼저 전달 포트에 대한 사전 전달 포트를 수정한 다음 로컬 MAC 주소 테이블을 에이징 합니다.

중계 노드가 마스터 노드에서 에이징 주소 테이블 알림을 받지 못하면 마스터 노드에 대한 링크가 이미 유효하지 않다고 판단하여 중계 노드는 자동으로 전달 전 포트를 전달 중으로 구성합니다. 사전 전달 시간 노드를 통해 관련 명령을 구성하여 전송 포트가 사전 전달 상태를 유지할 시간을 수정할 수 있습니다.

# 32. 이더넷 자동보호절체(EAPS) 구성

## 32.1. 기본 EAPS 구성

Note:
빠른 이더넷 자동보호절체 프로토콜은 STP 와 함께 구성할 수 없습니다. STP 가 비활성화 된 후에 링 노드가 BPDU 를 전달하지 못하게 하려면 spanning-tree bpduterminal 을 실행하는 것이 좋습니다. 그러면 폭풍이 발생합니다. 다음 표를 참조하십시오.

| **스패닝 트리 프로토콜** | **spanning-tree mode rstp** |
|---|---|
| Ethernet Automatic Protection Switching | 구성이 없습니다. |

표 2.1 이더넷 링 보호 프로토콜 및 STP 의 기본 구성.

## 32.2. 구성 전 요구 사항

MEAPS 를 구성하기 전에 다음 항목을 주의 깊게 읽으십시오.

링 보호 프로토콜의 중요한 기능 중 하나는 브로드캐스트 스톰을 중지하는 것이므로 링 링크가 다시 연결되기 전에 모든 링 노드가 구성되었는지 확인하십시오. 구성이 완료되지 않은 경우 링 네트워크가 연결된 경우, 트래픽 폭주가 쉽게 발생할 수 있습니다.

EAPS 는 STP 와 잘 호환되지만 EAPS 가 관리하는 포트는 STP 의 적용을받지 않습니다
링 보호 프로토콜은 다중 링 네트워크를 구성하기위한 스위치를 지원합니다.
링 제어 VLAN 을 구성하면 해당 시스템 VLAN 이 자동으로 구성됩니다.

각 링의 포트는 링의 제어 VLAN 에서 패킷을 전달할 수 있지만 트렁크 모드에서도 다른 포트는 제어 VLAN 에서 패킷을 전달할 수 없습니다.

기본적으로 마스터 노드의 Fail-time 은 Hello-time 보다 3 배 길기 때문에 링 보호 프로토콜에 충격을 주면 패킷 지연이 방지됩니다. Hello-time 이 수정된 후에는 Fail-time 을 적절히 수정해야 합니다.

기본적으로 중계 노드의 Pre-Forward-Time 은 마스터 노드의 Hello-time 보다 3 배 길기 때문에 중계 포트가 사전 전달에 들어가기 전에 마스터 노드가 링 네트워크의 복구를 감지할 수 있습니다 상태. 마스터 노드에 구성된 Hellotime 이 중계 노드의 pre-Forward-Time 보다 길면 루프백이 쉽게 생성되고 브로드캐스트 스톰이 트리거 됩니다.

물리적 인터페이스, 고속 이더넷 인터페이스, 기가비트 이더넷 인터페이스 및 집계 인터페이스는 모두 링의 인터페이스로 구성될 수 있습니다. 링크 집합, 802.1X 또는 포트 보안이 실제 인터페이스에 이미 구성된 경우 물리적 인터페이스를 더 이상 링 인터페이스로 구성할 수 없습니다

## 32.3. MEAPS 구성 작업

- 마스터 노드 구성
- 중계 노드 구성
- 링 포트 구성
- 링 보호 프로토콜의 상태 탐색

## 32.4. 고속 이더넷 링 보호 구성

### 32.4.1. 마스터 노드 구성

다음 단계에 따라 스위치를 링 네트워크의 마스터 노드로 구성하십시오.

| 명령 | 설명 |
|---|---|
| **Switch#config** | 스위치 구성 모드로 들어갑니다. |
| **Switch_config#ether-ring** *id* | 노드를 구성하고 노드 구성 모드로 들어갑니다.<br>id: 인스턴스 ID |
| **Switch_config_ring#control-vlan** *vlan-id* | 제어 VLAN 을 구성합니다.<br>Vlan-id: 제어 VLAN 의 ID |
| **Switch_config_ring#master-node** | 노드 유형을 마스터 노드로 구성합니다. |
| **Switch_config_ring#hello-time** *value* | 이 단계는 선택 사항입니다. 마스터 노드가 HEALTH 패킷을 전송할 주기를 구성합니다.<br>값: 1 – 10 초 범위의 시간 값이고 기본값은 1 초입니다. |
| **Switch_config_ring#fail-time** *value* | 이 단계는 선택 사항입니다. 보조 포트가 HEALTH 패킷을 기다리는 시간을 구성합니다.<br>값: 3 초에서 30 초 사이의 시간 값이고 기본값은 3 초입니다. |
| **Switch_config_ring#exit** | 현재 구성을 저장하고 노드 구성 모드를 종료합니다. |

### 32.4.2. 중계 노드 구성

다음 단계에 따라 스위치를 링 네트워크의 중계 노드로 구성합니다.

| 명령 | 설명 |
|---|---|
| **Switch#config** | 스위치 구성 모드로 들어갑니다 |
| **Switch_config#ether-ring** *id* | 노드를 구성하고 노드 구성 모드로 들어갑니다.<br>id: 인스턴스 ID |

| | |
|---|---|
| **Switch_config_ring#control-vlan** *vlan-id* | 제어 VLAN 을 구성합니다.<br>Vlan-id: 제어 VLAN 의 ID |
| **Switch_config_ring#transit-node** | 노드 유형을 중계 노드로 구성합니다 |
| **Switch_config_ring#pre-forward-time** *value* | 이 단계는 선택 사항입니다. 전송 포트에서 사전 전달 상태를 유지하는 시간을 구성합니다.<br>값: 3 초에서 30 초 사이의 시간 값이고 기본값은 3 초입니다. |
| **Switch_config_ring#exit** | 현재 구성을 저장하고 노드 구성 모드를 종료합니다. |

Note:
ID 값과 관련 없는 명령어를 넣은 경우 이더넷 링의 구성포트가 취소될 수 있습니다.

### 32.4.3. 링 포트 구성

다음 단계에 따라 스위치의 포트를 이더넷 링의 포트로 구성하십시오.

| 명령 | 설명 |
|---|---|
| **Switch#config** | 스위치 구성 모드로 들어갑니다. |
| **Switch_config#interface** *intf-name* | 인터페이스 구성 모드를 시작합니다.<br>intf-name: 인터페이스 이름을 나타냅니다. |
| **Switch_config_intf#ether-ring** id **{primary-port \| secondary-port \| transit-port}** | 이더넷 링의 포트 유형을 구성합니다.<br>이더넷 링의 노드 ID |
| **Switch_config_intf#exit** | 인터페이스 구성 모드를 종료합니다. |

Note:
ID 값과 관련 없는 명령어를 넣은 경우 이더넷 링의 구성포트가 취소될 수 있습니다.

### 32.4.4. 보호 프로토콜의 상태 탐색

다음 명령을 실행하여 링 보호 프로토콜의 상태를 찾습니다.

| 명령 | 설명 |
|---|---|
| **show ether-ring** *id* | 링 보호 프로토콜 및 이더넷 링의 포트에 대한 요약 정보를 탐색합니다.<br>id: 이더넷 링의 ID |
| **show ether-ring** *id* **detail** | 링 보호 프로토콜 및 이더넷 링 포트에 대한 자세한 정보를 검색합니다. |
| **show ether-ring** *id* **interface** *intf-name* | Ether-ring 포트 또는 공통 포트의 상태를 탐색합니다. |

## 32.5. MEAPS 구성

### 32.5.1. 구성 예

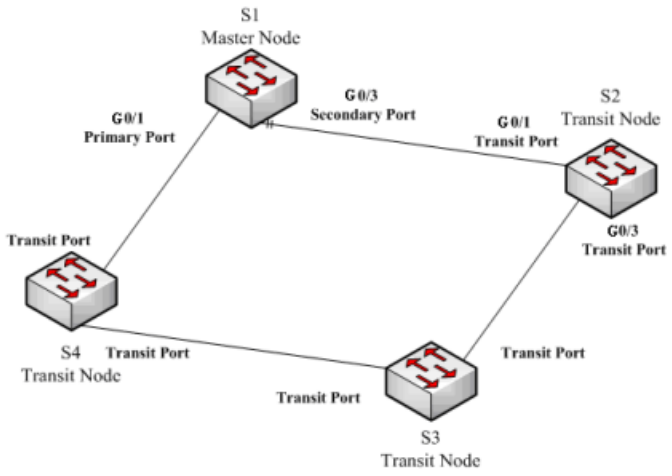



그림 2.1 에서와 같이 마스터 노드 S1 과 중계 노드 S2 는 다음과 같이 구성됩니다. 다른 노드의 구성은 S2 의 구성과 동일합니다.

**스위치 S1 구성:**

**STP 를 종료하고 Ether-ring 노드를 구성합니다.**

S1_config#no spanning-tree
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node

**다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.**
S1_config_ring1#hello-time 2
S1_config_ring1#fail-time 6
노드 구성 모드를 종료합니다.
S1_config_ring1 # exit

**기본 포트와 보조 포트를 구성합니다.**
S1_config#interface gigaEthernet 0/1
S1_config_g0/1#ether-ring 1 primary-port
S1_config_g0/1#exit
S1_config#interface gigaEthernet 0/3
S1_config_g0/3#ether-ring 1 secondary-port

S1_config_g0/3#exit

**제어 VLAN 을 구성합니다.**

S1_config#vlan 2
S1_config_vlan2#exit
S1_config#interface range g0/1 , 3
S1_config_if_range#switchport mode trunk
S1_config_if_range#exit

**스위치 S2 구성**

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 gigaEthernet 0/1
S2_config_g0/1#ether-ring 1 transit-port
S2_config_g0/1#exit
S2_config#interface gigaEthernet 0/3
S2_config_g0/3#ether-ring 1 transit-port
S2_config_g0/3#exit
S2_config#vlan 2
S2_config_vlan2#exit
S2_config#interface range gigaEthernet 0/1, 3
S2_config_if_range#switchport mode trunk
S2_config_if_range#exit

# 33. DHCP Snooping

## 33.1. 개요

VLAN 에서 DHCP 스누핑이 활성화된 경우 VLAN 의 모든 신뢰할 수 없는 물리적 포트에서 수신된 DHCP 패킷이 합법적으로 검사됩니다. VLAN 의 신뢰할 수 없는 물리적 포트에서 수신된 DHCP 응답 패킷은 삭제되어 가짜 또는 잘못 구성된 DHCP 서버가 주소 분배 서비스를 제공하지 못하게 합니다. 신뢰할 수 없는 포트의 DHCP 요청 패킷의 경우 DHCP 요청 패킷의 하드웨어 주소 필드가 이 패킷의 MAC 주소와 일치하지 않으면 DHCP 요청 패킷은 DHCP DOS 의 공격 패킷으로 사용되는 가짜 패킷으로 간주됩니다 스위치가 그것을 버립니다.

전역 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **Ip dhcp-relay snooping vlan** *vlan_id* | VLAN 에서 DHCP 스누핑을 활성화합니다. |
| **no ip dhcp-relay snooping vlan** *vlan_id* | VLAN 에서 DHCP 스누핑을 비활성화합니다 |

### 33.1.1. DHCP trust 인터페이스 구성

인터페이스가 DHCP trusting 인터페이스로 구성된 경우이 인터페이스에서 수신한 DHCP 패킷은 확인되지 않습니다.

물리적 인터페이스 구성 모드에서 다음 명령을 실행하십시오

| 명령 | 설명 |
|---|---|
| **dhcp snooping trust** | 인터페이스를 DHCP trusting 인터페이스로 구성합니다. |
| **no dhcp snooping trust** | DHCP- 신뢰할 수 없는 인터페이스에 대한 인터페이스를 다시 시작합니다. |

인터페이스는 기본적으로 신뢰할 수 없는 인터페이스입니다.

### 33.1.2. VLAN 에서 DAI 활성화

VLAN 의 모든 물리적 포트에서 동적 ARP 모니터링이 수행되면 이 패킷의 소스 MAC 주소와 소스 IP 주소가 구성된 MAC-IP 바인딩 관계와 일치하지 않으면 수신된 ARP 패킷이 거부됩니다. 인터페이스의 바인딩 관계는 DHCP 에 의해 동적으로 바인딩되거나 수동으로 구성될 수 있습니다. 물리적 인터페이스의 IP 주소에 MAC 주소가 바인딩되어 있지 않으면 스위치는 모든 ARP 패킷을 전달하지 않습니다.

| 명령 | 설명 |
|---|---|
| **ip arp inspection vlan vlanid** | VLAN 의 모든 불신 포트에서 동적 ARP 모니터링을 활성화합니다. |
| **no ip arp inspection vlan vlanid** | VLAN 의 모든 불신 포트에서 동적 ARP 모니터링을 비활성화합니다. |

### 33.1.3. ARP trust 인터페이스 구성

신뢰할 수 있는 인터페이스에서는 ARP 모니터링을 사용할 수 없습니다. 인터페이스는 기본적으로 신뢰할 수 없는 인터페이스입니다.

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **arp inspection trust** | 인터페이스를 ARP trusting 인터페이스에 구성합니다. |
| **no arp inspection trust** | ARP 불신 인터페이스에 대한 인터페이스를 재개합니다. |

### 33.1.4. VLAN 에서 소스 IP 주소 모니터링 활성화

VLAN 에서 소스 IP 주소 모니터링이 활성화된 후에는 소스 MAC 주소와 소스 IP 주소가 구성된 MAC-IP 바인딩 관계와 일치하지 않으면 VLAN 의 모든 물리적 포트에서 수신된 IP 패킷이 거부됩니다. 인터페이스의 바인딩 관계는 DHCP 에 의해 동적으로 바인딩되거나 수동으로 구성될 수 있습니다. 물리적 인터페이스의 IP 주소에 MAC 주소가 바인딩되어 있지 않으면 스위치는 물리적 인터페이스에서 수신한 모든 IP 패킷을 전달하지 않습니다. 전역 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **ip verify source vlan vlanid** | VLAN 의 모든 불신 인터페이스에서 소스 IP 주소 검사를 활성화합니다. |
| **no ip verify source vlan vlanid** | VLAN 의 모든 인터페이스에서 소스 IP 주소 검사를 비활성화합니다. |

참고:
DHCP 패킷 (IP 패킷)이 수신되면 전역 스누핑이 구성되어 전달됩니다.

### 33.1.5. IP source trust 인터페이스 구성

인터페이스에 신뢰할 수 있는 원본 IP 주소가 있는 경우 원본 주소 검사가 인터페이스에서 활성화되어 있지 않습니다

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| ip-source trust | 신뢰할 수 있는 원본 IP 주소가 있는 인터페이스를 구성합니다. |
| no Ip-source trust | 신뢰할 수 없는 소스 IP 주소가 있는 인터페이스를 다시 시작합니다. |

### 33.1.6. 수동으로 인터페이스 바인딩 구성

호스트가 DHCP 를 통해 주소를 얻지 못하면 스위치의 인터페이스에 바인딩 항목을 추가하여 호스트가 네트워크에 액세스 할 수 있게 할 수 있습니다. 해당 바인딩 목록에서 항목을 삭제할 IP 원본 바인딩 MAC IP 를 실행할 수 없습니다.

수동으로 구성된 바인딩 항목은 동적으로 구성된 바인딩 항목보다 우선 순위가 높습니다. 수동으로 구성된 바인딩 항목과 동적으로 구성된 바인딩 항목이 동일한 MAC 주소를 갖는 경우 수동으로 구성된 항목은 동적으로 구성된 항목을 업데이트합니다. 인터페이스 바인딩 항목은 MAC 주소를 고유 색인으로 사용합니다.

전역 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| ip source binding *MAC IP* interface *name* | 인터페이스 바인딩을 수동으로 구성합니다. |
| no ip source binding *MAC IP* vlan | 인터페이스 바인딩 항목을 취소합니다. |

### 33.1.7. DHCP 스누핑 모니터링 및 유지 관리

EXEC 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **show ip dhcp-relay snooping** | DHCP 스누핑 구성에 대한 정보를 표시합니다. |
| **show ip dhcp-relay snooping binding** | 인터페이스에 유효한 주소 바인딩 항목을 표시합니다. |
| **show ip dhcp-relay snooping binding all** | DHCP 스누핑에 의해 생성된 모든 바인딩 항목을 표시합니다. |
| [no] **debug ip dhcp-relay** [ **snooping** \| binding \| **event**] | DHCP 릴레이 스누핑의 전환을 활성화 또는 비활성화합니다. |

다음은 DHCP 스누핑 구성에 대한 정보를 보여줍니다.

switch#show ip dhcp-relay snooping
ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:

Gigaethernet0/1
ARP Inspect interface:
Gigaethernet0/11

다음은 dhcp-relay snooping 에 대한 바인딩 정보를 보여줍니다.

switch#show ip dhcp-relay snooping binding
Hardware Address IP Address remainder time Type VLAN interface 54-91-af-10-23-89 192.2.2.101 86400 DHCP_SN 3 Gigaethernet0/3

다음은 DHCP 릴레이 스누핑에 대한 모든 바인딩 정보를 보여줍니다.

switch#show ip dhcp-relay snooping binding all
Hardware Address IP Address remainder time Type VLAN interface
54-91-af-10-1c-59 192.2.2.1 infinite MANUAL 1 Gigaethernet0/2
54-91-af-10-23-89 192.2.2.101 86400 DHCP_SN 3 Gigaethernet0/3

다음은 dhcp-relay snooping 에 대한 정보입니다.

switch#debug ip DHCP-snooping packet
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface Gigaethernet0/3
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 Gigaethernet0/3
DHCPR: IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue

# 34. IGMP 설정 명령어

## 34.1. IGMP 설정 명령어

### 34.1.1. clear ip igmp group

#### (1) 구문

IGMP 를 지원하는 멀티캐스트 라우터에서 저장된 멀티캐스트 그룹 멤버 정보를 삭제하려면 “clear ip igmp group” 명령을 사용할 수 있습니다.

**clear ip igmp group** *type-number group-address*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *type-number* | 포트 유형과 포트 번호입니다. |
| *group-address* | 정보를 삭제할 멀티캐스트 그룹의 주소입니다. |

#### (3) 기본값

**없음**

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

이 명령어를 사용하면 저장된 멀티캐스트 그룹 정보에 문제가 있을 때 멀티캐스트 라우터에 저장된 멤버 정보를 삭제할 수 있습니다.

#### (6) 예제

다음 예제는 e1/0 포트에서 멀티캐스트 그룹 233.33.1.1 의 정보를 삭제하는 방법을 보여줍니다.

clear ip igmp group e1/0 233.33.1.1

**(7) 연관 명령어**

없음

### 34.1.2. debug ip igmp

**(1) 구문**

IGMP-라우터 끝 프로토콜의 처리 과정을 추적하려면 “debug ip igmp” 명령을 사용할 수 있으며, “no” 형태의 명령을 사용하여 디버그 정보를 종료할 수 있습니다.

**debug ip igmp**
**no debug ip igmp**

**(2) 매개변수**

**없음**

**(3) 기본값**

디버그 정보 출력이 비활성화됨

**(4) 명령어 모드**

슈퍼바이저 모드

**(5) 사용 지침**

이 명령어를 사용하여 IGMP-라우터 끝 프로토콜의 주요 처리 과정을 추적하고, 프로토콜 처리 실패의 원인을 찾을 수 있습니다.

**(6) 예제**

IGMP-라우터 기능 모듈의 디버그 정보는 자연어로 설명되며, 간단하게 이해할 수 있으므로 모든 디버그 정보를 나열하지는 않습니다.

### 34.1.3. debug ip igmph

#### (1) 구문

IGMP-호스트 끝 프로토콜의 처리 과정을 추적하려면 “debug ip igmph” 명령을 사용할 수 있으며, “no” 형태의 명령을 사용하여 디버그 정보를 종료할 수 있습니다.

**debug ip igmph** *group-address*
**no debug ip igmph**

#### (2) 매개변수

없음

#### (3) 기본값

디버그 정보 출력이 비활성화됨

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

이 명령어를 사용하여 IGMP-호스트 끝 프로토콜의 주요 처리 과정을 추적하고, 프로토콜 처리 실패의 원인을 찾을 수 있습니다.

#### (6) 예제

IGMP-호스트 기능 모듈의 디버그 정보는 자연어로 설명되며, 간단하게 이해할 수 있으므로 모든 디버그 정보를 나열하지는 않습니다.

### 34.1.4. ip igmp helper-address

#### (1) 구문

IGMP 패킷을 전송하려면 이 명령어를 사용하여 포트를 설정할 수 있습니다. 한 포트는 이 명령어를 한 번만 설정할 수 있으며, 이후 설정되는 명령어는 이전 명령어를 덮어씁니다.

**ip igmp helper-address** *destination-address*
**no ip igmp helper-address** *destination-address*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *destination-address* | IGMP 패킷을 전송할 대상 주소입니다 |

**(3) 기본값**

포트는 IGMP 패킷을 전송하지 않습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

"ip igmp helper-address" 명령을 사용하여 수신된 모든 IGMP 패킷을 전송할 수 있습니다.

**(6) 예제**

ip igmp helper-address 192.168.20.10

### 34.1.5. ip igmp join-group

**(1) 구문**

포트에 멀티캐스트 그룹을 추가하려면 이 명령어를 사용할 수 있습니다.

**ip igmp join-group** *group-address* **[{include|exclude}** *source-address***]**
**no ip igmp join-group group-address [{include|exclude} source-address]**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *group-address* | 포트에 추가하려는 멀티캐스트 그룹 주소입니다. |
| **include** | SSM 모드에서 멀티캐스트 그룹을 추가할 때 "include"를 사용합니다. |
| **exclude** | SSM 모드에서 멀티캐스트 그룹을 추가할 때 "exclude"를 사용합니다. |
| *source-address* | 멀티캐스트 그룹에 추가된 포트의 소스 필터 주소입니다. |

**(3) 기본값**

포트에 멀티캐스트 그룹이 추가되지 않습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

“ip igmp join-group” 명령을 사용하여 멀티캐스트 그룹을 동적으로 포트에 추가할 수 있습니다.

**(6) 예제**

ip igmp join-group 230.0.0.1
ip igmp join-group 230.0.0.1 exclude 192.168.20.10

### 34.1.6. ip igmp immediate-leave group-list

**(1) 구문**

IGMP 버전 2 를 실행하는 라우터 포트에서 멀티캐스트 그룹 기능을 "Exit Now"로 실행하려면 “ip igmp immediate-leave group-list” 명령을 사용하여 설정할 수 있습니다. 또한, “no” 형식을 사용하여 IGMP 호스트가 “exit now”를 사용하지 않도록 설정할 수 있습니다.

**ip igmp immediate-leave** *group-list list-name*
**no ip igmp immediate-leave** *group-list*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *list-name* | 미리 구성된 IP 표준 접근 목록의 이름입니다 |

**(3) 기본값**

IGMP 호스트는 "Exit Now" 기능을 사용할 수 없습니다.

**(4) 명령어 모드**

전역 설정 모드/인터페이스 설정 모드

**(5) 사용 지침**

이 명령은 IGMP 버전 2 를 실행하는 포트에서만 사용할 수 있습니다. 네트워크가 해당 포트와 연결된 상태에서 IGMP 호스트가 하나만 있을 때 사용할 수 있습니다. 이 명령을

설정하면 호스트는 라우터에서 패킷 교환 및 지연 처리 과정 없이 멀티캐스트 그룹에서 즉시 탈퇴할 수 있습니다. 이 명령은 "전역 설정 모드"와 "인터페이스 설정 모드"에서 구성할 수 있으며, "전역 설정 모드"에서 구성된 명령이 우선 적용됩니다. "인터페이스 설정 모드"에서 구성된 명령은 무시됩니다. 반대로, "전역 설정 모드"에서 구성된 명령은 "인터페이스 설정 모드"에서 설정된 명령을 덮어씁니다.

**(6) 예제**

"멀티캐스트 라우팅 구성" 참조.

**(7) 연관 명령어**

ip access-list

### 34.1.7. ip igmp last-member-query-interval

**(1) 구문**

현재 포트에서 마지막 그룹 멤버 쿼리 간격을 변경하려면 "ip igmp last-member-query-interval" 명령을 사용할 수 있습니다. "no" 형식을 사용하여 기본값으로 복원할 수 있습니다.

**ip igmp last-member-query-interval** *time*
**no ip igmp last-member-query-interval**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *time* | 포트에서 구성된 마지막 멤버 쿼리 간격 값입니다. 단위는 밀리초입니다 |

**(3) 기본값**

포트에서 마지막 그룹 멤버 쿼리 간격의 기본값은 1000ms 입니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령어는 포트에서 마지막 그룹 멤버 쿼리 간격을 수정하는 데 사용됩니다.

**(6) 예제**

다음 예제는 포트에서 마지막 멤버 쿼리 간격을 2 초로 수정하는 방법을 보여줍니다.
interface ethernet 0/0

ip igmp last-member-query-interval 2000

### 34.1.8. ip igmp querier-timeout

#### (1) 구문

이 명령어 “ip igmp querier-timeout”을 사용하여 다른 라우터의 IGMP 쿼리 타임아웃을 수정할 수 있습니다. “no” 형식을 사용하여 기본값으로 복원할 수 있습니다.

**ip igmp querier-timeout** *time*
**no ip igmp querier-timeout**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *time* | 다른 쿼리 타임아웃 값입니다. 단위는 초입니다 |

#### (3) 기본값

125 초

#### (4) 명령어 모드

인터페이스 설정 모드

#### (5) 사용 지침

이 명령어를 사용하여 다른 라우터의 쿼리 타임아웃을 수정할 수 있습니다. 이 명령은 IGMP 버전 2 를 실행하는 포트에서만 사용할 수 있습니다.

#### (6) 예제

다음 예제는 Ethernet 0/0 인터페이스에서 쿼리 타임아웃을 100 초로 지정하는 방법을 보여줍니다.

interface ethernet 0/0
ip igmp querier-timeout 100

### 34.1.9. ip igmp query-interval

#### (1) 구문

포트에서 IGMP 일반 쿼리 패킷 전송 간격을 설정하려면 “ip igmp query-interval” 명령을 사용할 수 있습니다. "no" 형식을 사용하여 기본값으로 복원할 수 있습니다.

**ip igmp query-interval** *time*
**no ip igmp query-interval**

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *time* | 일반 쿼리 패킷 전송 간격입니다. 단위는 초입니다. |

**(3) 기본값**

60 초

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령어를 사용하여 포트에서 IGMP 일반 쿼리 패킷 전송 간격을 설정할 수 있습니다.

**(6) 예제**

다음 예제는 Ethernet 0/0 포트에서 일반 쿼리 패킷 전송 간격을 50 초로 지정하는 방법을 보여줍니다.

```
interface ethernet 0/0
ip igmp query-interval 50
```

### 34.1.10. ip igmp query-max-response-time

**(1) 구문**

IGMP 호스트가 일반 쿼리 패킷에 응답하는 최대 시간을 지정하려면 “ip igmp query-max-response-time” 명령을 사용할 수 있습니다. "no" 형식을 사용하여 기본값으로 복원할 수 있습니다.

**ip igmp query-max-response-time** *time*
**no ip igmp query-max-response-time**

**(2) 매개변수**

| 매개변수 | 설명 |
| --- | --- |
| *time* | 포트에서 구성된 최대 응답 시간 값입니다. |

**(3) 기본값**

10 초

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령어를 사용하여 IGMP 호스트가 일반 쿼리 패킷에 응답하는 최대 시간을 지정할 수 있습니다. 이 명령은 IGMP 버전 2 와 3 을 실행하는 포트에서만 사용할 수 있습니다.

**(6) 예제**

다음 예제는 Ethernet 0/0 포트에서 IGMP 최대 응답 시간을 15 초로 설정하는 방법을 보여줍니다.

```
interface ethernet 0/0
ip igmp query-max-response-time 15
```

### 34.1.11. ip igmp static-group

**(1) 구문**

포트에서 정적 멀티캐스트 그룹을 구성하려면 “ip igmp static-group” 명령을 사용할 수 있습니다. "no" 형식을 사용하여 기본값으로 복원할 수 있습니다.

**ip igmp static-group** { ***** | *group-address* } {**include** *source-address* }
**no ip igmp static-group** { ***** | *group-address* } {**include** *source-address*}

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *** | 모든 멀티캐스트 그룹 |
| *group-address* | 지정된 멀티캐스트 그룹 주소 |
| source-address | 지정된 호스트 소스 주소 |

**(3) 기본값**

기본적으로 포트에는 정적 멀티캐스트 그룹이 구성되지 않습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

현재 포트에서 정적 IGMP 멀티캐스트 그룹 정보를 구성할 수 있습니다.

참고:
동일한 group-address 에 대해 여러 개의 include source-address 명령을 구성하여 여러 개의 소스 주소가 존재하도록 할 수 있습니다. 그러나 동일한 group-address 에 대해 include source-address 가 있는 명령과 없는 명령을 동시에 구성할 수는 없습니다.

**(6) 예제**

"멀티캐스트 라우팅 구성" 참조

### 34.1.12. Ip igmp version

**(1) 구문**

포트에서 실행 중인 IGMP 버전 번호를 설정하려면 "ip igmp version" 명령을 사용할 수 있습니다. "no" 형식을 사용하여 기본값으로 복원할 수 있습니다.

**ip igmp version** *version-number*
**no ip igmp version**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *version-number* | IGMP 버전 번호. 1, 2, 3 중 하나를 선택할 수 있습니다 |

**(3) 기본값**

이 명령을 구성하지 않으면, 포트에서 실행 중인 IGMP-Router 프로토콜의 기본 버전 번호는 3 입니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 예제**

다음 예제는 Ethernet 0/0 포트에서 IGMP 버전 번호를 2 로 지정하는 방법을 보여줍니다.
interface ethernet 0/0
ip igmp version 2

### 34.1.13. show ip igmp groups

**(1) 구문**

현재 라우터에서 저장된 멀티캐스트 그룹 멤버 정보를 확인하려면 다음 명령어를 사용할 수 있습니다.

**show ip igmp groups** *{interface | group-address | detail}*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *interface* | 멀티캐스트 그룹 정보를 보고 싶은 포트입니다. 이 매개변수를 추가하지 않으면 포트에서 모든 멀티캐스트 그룹 정보를 표시합니다 |
| group-address | 확인하려는 멀티캐스트 그룹 주소입니다. 이 매개변수를 추가하지 않으면 라우터에서 모든 멀티캐스트 그룹 정보를 표시합니다. |
| detail | 멀티캐스트 그룹에 대한 자세한 정보를 볼지 여부입니다. |

**(3) 기본값**

없음

**(4) 명령어 모드**

슈퍼바이저 모드/전역 설정 모드/인터페이스 설정 모드

**(5) 사용 지침**

이 명령어를 사용하여 라우터에 저장된 멀티캐스트 그룹 멤버 정보를 확인할 수 있습니다.

**(6) 예제**

show ip igmp groups e0/0 detail
이 명령어를 실행하면 다음과 같은 메시지가 표시됩니다:
…….
Interface: Ethernet0/0
Group address: 233.33.1.3
Uptime: 00:03:46
Group status: Static
Group filter mode: INCLUDE
Last reporter: 0.0.0.0
Group source-list: (Flags: S-Static, R-Remote)
Source address: Uptime Timer Fwd Flags
192.168.20.5 00:03:46 stopped Yes S

Interface: Ethernet0/0
Group address: 233.33.1.1
Uptime: 00:03:46
Group status: Static
Group filter mode: INCLUDE
Last reporter: 0.0.0.0
Group source-list: (Flags: S-Static, R-Remote)
Source address: Uptime Timer Fwd Flags
192.168.20.5 00:03:46 stopped Yes S

192.168.20.3 00:03:46 stopped Yes S
192.168.20.1 00:03:46 stopped Yes S
…….
show ip igmp groups 233.33.1.1 detail
이 명령어를 실행하면 다음과 같은 메시지가 표시됩니다:
Interface: Ethernet0/0
Group address: 233.33.1.1
Uptime: 00:02:42
Group status: Static
Group filter mode: INCLUDE
Last reporter: 0.0.0.0
Group source-list: (Flags: S-Static, R-Remote)
Source address: Uptime Timer Fwd Flags
192.168.20.5 00:02:42 stopped Yes S
192.168.20.3 00:02:42 stopped Yes S
192.168.20.1 00:02:42 stopped Yes S
show ip igmp groups
이 명령어를 실행하면 다음과 같은 메시지가 표시됩니다:
Interface Group address Uptime Expires Last Reporter Flags
Ethernet0/0 239.255.255.250 00:01:08 00:02:05 192.168.20.141 R
Ethernet0/0 224.2.127.254 00:01:09 00:02:00 32.1.1.67 R
Ethernet0/0 224.1.1.1 00:01:24 stopped 0.0.0.0 S
Ethernet0/0 233.33.1.5 00:01:24 stopped 0.0.0.0 S
Ethernet0/0 233.33.1.3 00:01:24 stopped 0.0.0.0 S
Ethernet0/0 233.33.1.1 00:01:24 stopped 0.0.0.0 S

Interface Group address Uptime Expires Last Reporter Flags
Loopback10 239.255.255.250 00:01:08 00:02:05 192.168.20.141 R
Loopback10 224.2.127.254 00:01:09 00:02:00 32.1.1.67 R

### 34.1.14. show ip igmp interface

#### (1) 구문

IGMP 가 활성화된 현재 라우터의 포트 정보를 확인하려면 다음 명령어를 사용할 수 있습니다.

**show ip igmp interface** *interface*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *interface* | 정보를 표시할 지정된 포트입니다. 이 매개변수를 추가하지 않으면 IGMP 가 활성화된 모든 포트 정보를 표시합니다. |

#### (3) 기본값

없음

**(4) 명령어 모드**

슈퍼바이저 모드/전역 설정 모드/인터페이스 설정 모드

**(5) 사용 지침**

이 명령어를 사용하여 IGMP 가 활성화된 포트에 대한 정보를 확인할 수 있습니다.

**(6) 예제**

show ip igmp interface e0/0
이 명령어를 실행하면 다음과 같은 정보가 표시됩니다:
Ethernet0/0 is up, line protocol is up
 Internet address is 192.168.20.167
 Current IGMP router version is 3
 Router plays role of querier on the interface now
 IGMP is enable on the interface
 IGMP query-interval is 60 seconds
 IGMP max query response time is 10 seconds
 IGMP Last member query response time is 1000 milliseconds
 IGMP querier timeout is 125 seconds
 Multicast routing is enabled on the interface

### 34.1.15. show ip igmph

**(1) 구문**

현재 라우터의 포트에서 IGMP 호스트 정보를 확인하려면 다음 명령어를 사용할 수 있습니다.

**show ip igmph { *interface* } detail**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| ***interface*** | 정보를 표시할 지정된 포트입니다 |
| **detail** | IGMP 호스트에 대한 자세한 정보를 표시할지 여부입니다. |

**(3) 기본값**

없음

**(4) 명령어 모드**

슈퍼바이저 모드/전역 설정 모드/인터페이스 설정 모드

**(5) 사용 지침**

이 명령어를 사용하여 지정된 포트에서 IGMP 호스트의 기본 정보를 확인할 수 있습니다.

**(6) 예제**

show ip igmph interface e0/0
이 명령어를 실행하면 다음과 같은 정보가 표시됩니다:
IGMP host Mode is IGMP_V3_ROUTER
IGMP host Query Interval is 23 second
IGMP host Query Response Interval is 125
IGMP host Query Robustness Variable is 2
IGMP host Last Query Interval is 0
IGMP interface timer is 0
IGMP host group joined(number of users):
230.0.0.1(1)

# 35. IGMP Snooping

## 35.1. IGMP Snooping 구성 작업

IGMP-Snooping 의 임무는 VLAN 과 그룹 주소 간의 관계를 유지하고 멀티 캐스트 변경과 동시에 업데이트하여 멀티 레이어 그룹의 토폴로지 구조에 따라 레이어 2 스위치가 데이터를 전달할 수 있게 하는 것입니다.

IGMP-Snooping 의 주요 기능은 다음과 같습니다.

- IGMP 메시지를 받습니다.
- VLAN 과 그룹 주소 간의 관계 테이블을 유지 보수합니다.
- 플러딩이 발생하지 않도록 호스트의 IGMP 엔티티와 라우터의 IGMP 엔티티를 동일한 상태로 유지합니다.

Note:
igmp-Snooping 은 질의 메시지를 받고 igmp 의 메시지를 보고 위의 기능을 실현하기 때문에 igmp-Snooping 은 멀티캐스트 라우터에서 작동할 때만 제대로 작동할 수 있습니다. 즉 스위치는 주기적으로 라우터에서 igmp 쿼리 정보를 수신해야 합니다. igmp-Snooping 의 라우터 수명 타이머는 igmp-Snooping 을 연결하는 멀티 캐스트 라우터의 그룹 쿼리 기간보다 큰 시간 값으로 구성되어야합니다. show ip igmp-Snooping 을 실행하여 각 VLAN 의 멀티 캐스트 라우터 정보를 확인할 수 있습니다.

- VLAN 의 IGMP-Snooping 활성화/비활성화
- VLAN 의 정적 멀티 캐스트 주소 추가/삭제
- VLAN 의 즉시 탈퇴 구성
- 등록된 대상 주소 가없는 멀티 캐스트 메시지를 필터링하는 기능 구성
- IGMP-Snooping 의 라우터 에이지 타이머 구성
- IGMP-Snooping 의 응답 시간 타이머 구성
- IGMP-Snooping 의 IGMP Querier 구성
- IGMP-Snooping 모니터링 및 유지 관리
- IGMP-Snooping 구성 예제

### 35.1.1. VLAN 의 IGMP Snooping 활성화/비활성화

전역 구성 모드에서 다음 구성을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **ip igmp-Snooping** [vlan *vlan_id*] | VLAN 의 IGMP-Snooping 을 활성화합니다. |
| **no ip igmp-Snooping** [vlan *vlan_id*] | 기본 구성을 다시 시작합니다. |

vlan 을 지정하지 않으면 나중에 생성된 VLAN 을 포함하여 시스템의 모든 VLAN 을 활성화 또는 비활성화 할 수 있습니다. 기본 구성에서 ip igmp-Snooping 명령이 구성된 것처럼 모든 VLAN 의 IGMP-Snooping 이 활성화됩니다.

Note:
IGMP-Snooping 은 최대 16 개의 VLAN 에서 실행될 수 있습니다.
VLAN3 에서 IGMP-Snooping 을 활성화하려면 먼저 no ip IGMP-Snooping 을 실행하여 모든 VLAN 의 IGMP-Snooping 을 비활성화 한 다음 ip igmp-Snooping vlan 3 을 구성하고 구성을 저장해야 합니다

### 35.1.2. VLAN 의 정적 멀티캐스트 주소 추가/삭제

IGMP 를 지원하지 않는 호스트는 정적 멀티 캐스트 주소를 구성하여 해당 멀티 캐스트 메시지를 수신할 수 있습니다.

전역 구성 모드에서 다음 구성을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **ip igmp-Snooping vlan** *vlan_id* **static** *A.B.C.D* **interface** *intf* | VLAN 의 정적 멀티 캐스트 주소를 추가합니다. |
| **no ip igmp-Snooping vlan** *vlan_id* **static** *A.B.C.D* **interface** *intf* | VLAN 의 정적 멀티 캐스트 주소를 삭제합니다. |

### 35.1.3. VLAN 의 즉시 종료 기능

즉시 방치가 구성된 경우 스위치는 특정 메시지를 받은 후 멀티 캐스트 그룹의 포트 목록에서 포트를 삭제할 수 있습니다. 따라서 스위치는 타이머가 다른 호스트가 멀티 캐스트에 참석하기를 기다릴 필요가 없습니다. 같은 포트에 있는 다른 호스트가 같은 그룹에 속해 있고 사용자가 그룹을 떠나고 싶지 않으면 이 사용자의 멀티 캐스트 통신이 영향을 받을 수 있습니다. 이 경우 즉각적인 종료 기능을 사용할 수 없습니다.

전역 구성 모드에서 다음 구성을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **ip igmp-Snooping vlan** *vlan_id* **immediate-leave** | VLAN 의 즉시종료 기능을 구성합니다 . |

| | |
|---|---|
| **no ip igmp-Snooping vlan** *vlan_id* **immediate-leave** | VLAN 의 즉각적인 종료를 기본값으로 구성합니다. |

VLAN 의 즉시 종료 특성은 기본적으로 비활성화되어 있습니다.

### 35.1.4. 등록된 대상 주소 없이 멀티캐스트 메시지를 필터링하는 기능 구성

멀티 캐스트 메시지 대상을 찾을 수 없으면 (DLF, 대상 주소가 igmp-Snooping 을 통해 스위치 칩에 등록되지 않음) 기본 처리 방법은 VLAN 의 모든 포트에서 메시지를 보내는 것입니다. 구성을 통해 프로세스 방법을 변경할 수 있습니다 목적지 주소가 어떤 포트에도 등록되지 않은 모든 멀티 캐스트 메시지는 삭제됩니다.

| 명령 | 설명 |
|---|---|
| **ip igmp-Snooping dlfdrop vlan** *vlan_id* | 대상을 찾을 수 없는 멀티 캐스트 메시지를 삭제합니다. |
| **no ip igmp-Snooping dlfdrop vlan** *vlan_id* | 오류 구성을 다시 시작합니다. (앞에서부터). |

Note:
1) 모든 VLAN 에 대해 속성이 구성됩니다.

2) 스위치가 유형의 메시지를 처리하는 기본 방법은 정방향입니다.
(이 유형의 메시지는 VLAN 에서 브로드 캐스팅됩니다).

### 35.1.5. IGMP Snooping 의 구성 Router age 타이머

Router-age 는 IGMP 쿼리어 이 존재하는지 여부를 모니터링하는 데 사용됩니다. IGMP 질의는 질의 메시지를 보내 멀티 캐스트 주소를 유지합니다. IGMP-Snooping 은 IGMP 쿼리어와 호스트 간의 통신을 통해 작동합니다.

전역 구성 모드에서 다음 구성을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **ip igmp-Snooping timer router-age** *timer_value* | IGMP-Snooping 의 Router Age 값을 구성합니다. |
| **no ip igmp-Snooping timer router-age** | IGMP-Snooping 의 Router Age 의 기본값을 다시 시작합니다. |

Note:
타이머 구성 방법은 IGMP 질의 자의 질의 기간 구성을 참조하십시오. 타이머는 쿼리 기간보다 작게 구성할 수 없습니다. 타이머는 쿼리 기간의 세 배로 구성하는 것이 좋습니다.
IGMP-Snooping 의 Router Age 의 기본값은 260 초입니다.

### 35.1.6. IGMP Snooping 응답 시간 타이머 구성

응답 시간 타이머는 IGMP 의 지망생이 전송한 후 호스트가 멀티 캐스트를 보고 상한 시간 쿼리 메시지를. 는 만약 보고서 메시지가 타이머 세 이후에 수신되지 않는 스위치는 멀티 캐스트 주소를 삭제합니다.

전역 구성 모드에서 다음 구성을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **ip igmp-Snooping timer response-time** *timer_value* | IGMP-Snooping 의 응답 시간 값을 구성합니다 . |
| **no ip igmp-Snooping timer response-time** | IGMP-Snooping 응답 시간의 기본값을 다시 시작합니다. |

Note:
타이머 값은 너무 작을 수 없습니다. 그러면 멀티 캐스트 통신이 불안정 해집니다.
IGMP-Snooping 의 응답 시간 값은 10 초로 구성됩니다

### 35.1.7. IGMP Snooping 의 쿼리 작성 구성

멀티 캐스트 라우터가 IGMP-Snooping 이 활성화 된 VLAN 에 존재하지 않으면 IGMP-Snooping 의 쿼리 기능을 사용하여 멀티 캐스트 라우터를 모방하여 정기적으로 IGMP 쿼리 메시지를 보낼 수 있습니다.(이 기능은 전역 적입니다. 즉, IGMP-Snooping 이 전역 적으로 활성화된 VLAN 에서 기능을 활성화 또는 비활성화 할 수 있습니다)

멀티 캐스트 라우터가 LAN 에 존재하지 않고 멀티 캐스트 플로우에 라우팅이 필요 없는 경우 IGMP-Snooping 을 통해 스위치의 자동 쿼리 기능을 활성화할 수 있으므로 IGMP-Snooping 이 제대로 작동합니다.

전역 구성 모드에서 다음 구성을 수행하십시오.

| 명령 | 설명 |
|---|---|
| [**no**] **ip igmp-Snooping querier** [**address** [*ip_addr*] | IGMP-Snooping 의 쿼리를 구성합니다. 선택적 매개 변수 address 는 조회 메시지의 소스 IP 주소입니다. |

IGMP Snooping-querier 기능은 기본 비활성화되어 있습니다. 가짜 쿼리 메시지의 원본 IP 주소는 기본적으로 10.0.0.200 입니다.

Note:
만약 쿼리어 기능이 활성화되고 기능이 적용되지 않으면 멀티캐스트 라우터가 vlan 에 존재하며 이기능은 자동적으로 멀티캐스트 타임아웃때 활성화됩니다.

### 35.1.8. IGMP Snooping 모니터링

관리 모드에서 다음 작업을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **show ip igmp-Snooping** | IGMP-Snooping 구성 정보를 표시합니다. |
| **show ip igmp-Snooping timer** | IGMP-Snooping 의 시계 정보를 표시합니다. |
| **show ip igmp-Snooping groups** | IGMP-Snooping 의 멀티 캐스트 그룹에 대한 정보를 표시합니다. |
| **show ip igmp-Snooping statistics** | IGMP-Snooping 에 대한 통계 정보를 표시합니다. |
| [**no**] **debug ip igmp-Snooping** [ **packet** \| **timer** \| **event** \| **error**] | IGMP-Snooping 의 패킷/클럭 디버그/이벤트/실수 인쇄 스위치를 활성화 및 비활성화합니다. 디버그 스위치를 지정하지 않으면 모든 디버그 스위치가 활성화되거나 비활성화됩니다. |

**IGMP-Snooping 실행에 대한 VLAN 정보 표시:**

switch#show ip igmp-Snooping
igmp-Snooping response time:10 s
vlan 1
------------
running
router: 90.0.0.120(F0/2)

**IGMP-Snooping 의 멀티 캐스트 그룹에 대한 정보 표시:**

switch#show ip igmp-Snooping groups
Vlan Source Group Type Port(s)
---- --------------- --------------- ---- ------------------------
1 0.0.0.0 234.5.6.6 IGMP F0/2
1 0.0.0.0 239.255.255.250 IGMP F0/2

**IGMP-Snooping 타이머 표시:**

switch#show ip igmp-Snooping timers
vlan 1 router age: 251 Indicating the timeout time of the router age timer
vlan 1 multicast address 0100.5e00.0809 response time: 1 Indicating the period from when the last multicast group query message is received to the current time; if no host on the port respond when the timer times out, the port will be deleted..

**IGMP-Snooping 통계 표시:**

switch#show ip igmp-Snooping statistics
vlan 1
------------
v1_packets:0 IGMP v1 packet number

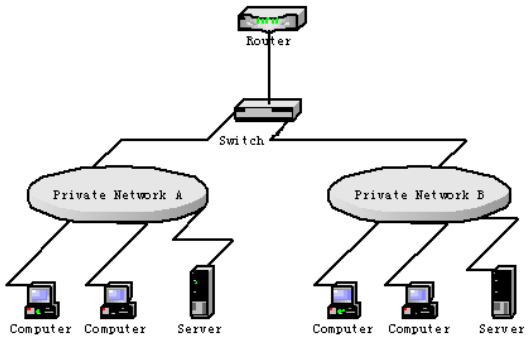
v2_packets:6 IGMP v2 packet number
v3_packets:0 IGMP v3 packet number
general_query_packets:5 General query of the packet number
special_query_packets:0 Special query of the packet number
join_packets:6 Number of report packets
leave_packets:0 Number of Leave packets
send_query_packets:0 Reserved statistics option
err_packets:0 Number of incorrect packets

**IGMP-Snooping 의 메시지 타이머 디버그:**
switch#debug ip igmp-Snooping packet
rx: s_ip:90.0.0.3, d_ip:224.0.8.9 Source and destination IP addresses where packets are received
type:16(V2-Report), max resp:00, group address:224.0.8.9 Type and content of packet
rx: s_ip:90.0.0.90, d_ip:224.0.0.1
type:11(Query), max resp:64, group address:0.0.0.0
rx: s_ip:90.0.0.3, d_ip:224.0.8.9
type:16(V2-Report), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.3, d_ip:224.0.0.2
type:17(V2-Leave), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.90, d_ip:224.0.8.9
type:11(Query), max resp:0a, group address:224.0.8.9

**Snooping 의 메시지 타이머 디버그:**
switch#debug ip igmp-Snooping timer
tm: vlan 1 igmp router age expiry at port 2(F0/2)
tm: multicast item 0.0.0.0->224.0.8.9(0100.5e00.0809) response time expiry at port F0/4 Inquiring the response timer expiry

### 35.1.9. IGMP Snooping 구성 예제

그림 1 은 예제의 네트워크 연결을 보여줍니다.



(1) 사설망 A 를 연결하는 VLAN 1 의 IGMP-Snooping 을 활성화합니다.
Switch_config # ip igmp-Snooping VLAN 1

(2) 사설망 B 를 연결하는 VLAN 2 의 IGMP-Snooping 을 활성화합니다.
Switch_config # ip igmp-Snooping VLAN 2

# 36. PIM-DM 설정 명령어

## 36.1. PIM-DM 설정 명령어

### 36.1.1. clear ip mroute pim-dm

#### (1) 구문

다음 명령어를 슈퍼바이저 모드에서 사용하여 PIM-DM 이 제출한 (S, G) 라우팅 목록 항목을 MROUTING 에서 삭제할 수 있습니다:

**clear ip mroute pim-dm** *{* | *group [source]}*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| * | PIM-DM 이 제출한 모든 멀티캐스트 라우팅 목록 항목을 삭제합니다. |
| *group* | 지정된 그룹에서 PIM-DM 이 제출하고 만족하는 모든 항목을 삭제합니다. |
| *source* | (선택사항) 지정된 그룹의 소스에서 PIM-DM 이 제출하고 만족하는 모든 항목을 삭제합니다. |

#### (3) 기본값

없음

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

이 명령어는 로컬 멀티캐스트 라우터 테이블의 모든 또는 일부 목록을 삭제하며, 이는 정상적인 멀티캐스트 패킷 전달에 영향을 줄 수 있습니다. 이 명령어는 PIM-DM 멀티캐스트 라우팅 프로토콜로 생성된 업스트림 포트를 가진 (S, G) 항목만 삭제할 수 있으며, mrouting 에 알리고 mrouting 은 해당 (S,G)를 다시 설정해야 하는지 결정합니다.

#### (6) 예제

예제 1:
Router#clear ip mroute pim-dm *
PIM-DM 에 의해 생성된 미들스트림/업스트림 포트를 가진 모든 (S, G) 항목들이 로컬 MRT 에서 삭제됩니다.

예제 2:
Router#clear ip mroute pim-dm 239.1.1.1
그룹 주소 239.1.1.1 을 가진 모든 (S, G) 항목들이, PIM-DM 에 의해 생성된 미들스트림/업스트림 포트를 가진 항목들이 로컬 MRT 에서 삭제됩니다.

예제 3:
Router#clear ip mroute pim-dm 239.1.1.1 192.168.20.131
주소 (192.168.20.131, 239.1.1.1)을 가진 모든 (S, G) 항목들이, PIM-DM 에 의해 생성된 미들스트림/업스트림 포트를 가진 항목들이 로컬 MRT 에서 삭제됩니다.

### 36.1.2. clear ip pim-dm interface

#### (1) 구문

PIM-DM 포트를 통해 전달된 (S, G) 멀티캐스트 패킷 통계 값을 초기화합니다. 이 명령어는 슈퍼바이저 모드에서 사용할 수 있습니다:

**clear ip pim-dm interface {count |** *type number {count}***}**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| count | (선택 사항) PIM-DM 포트에서 모든 멀티캐스트 패킷 통계 값을 삭제합니다 |
| *type number* | (선택 사항) 지정된 포트에서 멀티캐스트 패킷 통계 값을 삭제합니다. |

#### (3) 기본값

없음

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

이 작업은 로컬 멀티캐스트 라우팅 목록에서 PIM-DM 포트를 통해 전달된 멀티캐스트 패킷 수 통계 값을 초기화합니다. 이 명령어는 PIM-DM 멀티캐스트 라우팅 프로토콜로 생성된 업스트림 포트를 가진 (S, G) 항목에 대해서만 초기화할 수 있습니다.

#### (6) 예제

예제 1:
Router#clear ip pim-dm interface count
로컬 MRT 에서 PIM-DM 으로 전달된 모든 (S, G) 항목의 멀티캐스트 패킷 수 통계 값을 초기화합니다.

예제 2:
Router#clear ip pim-dm interface Ethernet1/1 count
로컬 MRT 에서 Ethernet1/1 포트를 통해 전달된 모든 (S, G) 항목의 멀티캐스트 패킷 수 통계 값을 초기화합니다.

### 36.1.3. debug ip pim-dm

#### (1) 구문

이 명령어는 입력/출력 PIM 패킷과 발생한 이벤트를 추적하는 데 사용됩니다. 추적을 중지하려면 이 명령어를 "no"로 설정하십시오.

**debug ip pim-dm [group|alert]**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| group | (선택 사항) 지정된 그룹 상태를 추적합니다. |
| alert | (선택 사항) mrouting 에서 받은 경고 상태를 추적합니다. |

#### (3) 기본값

없음

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

mrouting 에서 알림을 수신하고, 다른 구성 요소로 알림을 전송합니다.

#### (6) 예제

예제 1, 출력 정보:
Hello packet sent to each port.
Hello packet received from each port.
A new neighbor is found.
Delete neighbor.
Port sending status refresh packet.
Port receiving status refresh packet.
Port is sending Assert packet.
Port is receiving Assert packet.
Port is sending prune packet.
Port is receiving prune packet.
Port is sending graft ack packet.

Port is receiving graft ack packet.
Port is sending graft packet.
Port is receiving graft packet.
Port is sending join/prune packet.
Port is receiving join/prune packet.
When a new (S,G) is created
When deleting (S,G)
Router#debug ip pim-dm
2003-3-26 11:45:17 received V2 hello packet on Ethernet2/1 from 192.168.20.133(GenID = 3539)
2003-3-26 11:45:17 Ethernet2/1 create new nbr 192.168.20.133
2003-3-26 11:45:25 send hello packet to 224.0.0.13 on Loopback1
2003-3-26 11:50:29 Ethernet2/1 delete nbr 192.168.20.133
2003-3-26 11:50:51 received V2 hello packet on Ethernet2/1 from 192.168.20.152
2003-3-26 11:50:51 send hello packet to 224.0.0.13 on Ethernet2/1
2003-3-26 12:04:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success
2003-3-26 12:04:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful
2003-3-26 12:04:39 PIM-DM: ignored V2 packet on Ethernet2/1 from 192.168.10.204 (validate source address failed)
2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream:192.168.20.132 Adding in MRT success
2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

예제 2 출력 경고 메시지:
Router#debug ip pim-dm alert
2003-3-26 12:09:51 receive alert_rt_change alert from mroute
2003-3-26 12:09:54 receive alert_rt_change alert from mroute
2003-3-26 12:11:08 PIM-DM: send sg_deletion alert
2003-3-26 12:11:19 receive alert_sg_creation alert from mroute
2003-3-26 12:11:20 receive alert_sg_prune alert from mroute
2003-3-26 12:11:56 receive alert_group_report alert from mroute
2003-3-26 12:11:56 receive alert_sg_join alert from mroute

예제 3, 지정된 그룹 상태 추적:
Router#deb ip pim-dm 239.1.1.1
Router#2003-3-26 12:35:27 PIM-DM: clear (192.168.20.138, 239.1.1.1) forwd pkt count success
2003-3-26 12:35:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success
2003-3-26 12:35:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful
2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream: 192.168.20.132 Adding in MRT success
2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 1.1.1.1 create success

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 192.167.20.132 create success
2003-3-26 12:35:42 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

### 36.1.4. ip pim-dm

#### (1) 구문

이 명령어는 포트에서 PIM-DM 을 실행하는 데 사용됩니다. 이 명령어를 "no"로 설정하여 포트에서 PIM-DM 을 비활성화할 수 있습니다.

**ip pim-dm**
**no ip pim-dm**

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 명령어 모드

인터페이스 설정 모드

#### (5) 사용 지침

"ip multicast-routing" 미설정 시, 이 명령을 설정하면 다음 경고가 표시됩니다: 경고: "ip multicast-routing"이 설정되지 않았습니다. IP 멀티캐스트 패킷은 전달되지 않습니다.

이 기능이 비활성화되면: PIM-DM 은 포트에서 실행되지 않지만, 다른 PIM-DM 설정에는 영향을 미치지 않습니다. 다시 PIM-DM 을 포트에서 실행하면 모든 PIM-DM 설정은 여전히 유효합니다.

이 기능을 활성화하면: 해당 포트에서 멀티캐스트 패킷 전달이 가능하지만, 먼저 글로벌 멀티캐스트 패킷 전달 기능을 활성화해야 합니다.

#### (6) 예제

Router_config#ip multicast-routing
Router_config#interface Ethernet1/1

Router_config_e1/1#ip pim-dm

**(7) 연관 명령어**

ip multicast-routing
show ip pim-dm interface

### 36.1.5. ip pim-dm dr-priority

**(1) 구문**

지정된 라우터를 우선 순위가 높은 라우터(DR)로 설정합니다. 이 명령을 "no"로 설정하여 포트에서 기본값 DR 우선 순위를 복원할 수 있습니다.

**ip pim-dm dr-priority** priority
**no pim-dm dr-priority**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *priority* | 포트 DR 우선 순위입니다. 값이 클수록 우선 순위가 높습니다. 범위는 0 에서 4294967294 까지이며, 기본값은 1 입니다. |

**(3) 기본값**

PIM 포트에서 기본값 DR 우선 순위는 1 입니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

모든 PIM 이웃이 해당 포트에서 DR 우선 순위를 지원하는 경우, 가장 높은 우선 순위를 가진 라우터를 DR 로 선택합니다. 모든 라우터의 우선 순위가 동일하면 가장 높은 포트 IP 값을 가진 라우터를 DR 로 선택합니다.

라우터가 HELLO 패킷에서 우선 순위를 광고하지 않고 여러 라우터가 동일한 상황이라면, 가장 높은 포트 IP 값을 가진 라우터를 DR 로 선택합니다.

### 36.1.6. ip pim-dm hello-interval

**(1) 구문**

이 명령은 포트에서 정기적으로 전송되는 PIM-Hello 패킷의 간격을 구성하는 데 사용됩니다. 이 명령을 "no"로 설정하여 기본값 간격을 복원할 수 있습니다.

**ip pim-dm hello-interval** *interval*
**no ip pim-dm hello-interval**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *interval* | 정기적으로 전송되는 PIM-Hello 패킷의 간격입니다. 범위는 0 에서 65535 까지이며, 기본값은 30 초입니다 |

**(3) 기본값**

30 초

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

주기적으로 Hello 패킷을 보내면 이웃이 존재하는지 확인할 수 있습니다. 일반적으로 이웃에서 설정한 hello-interval 의 3.5 배 시간 동안 Hello 패킷을 받지 못하면 해당 이웃은 사라진 것으로 간주됩니다.

IGMP v1 에서는 PIM-DM Hello 패킷을 통해 지정된 라우터(DR)를 선택할 수 있습니다.

**(6) 예제**

Router_config#interface Ethernet1/1
Router_config_e1/1#ip pim-dm hello-interval 30

**(7) 연관 명령어**

ip igmp query-interval

### 36.1.7. ip pim-dm state-refresh origination-interval

**(1) 구문**

이 명령어는 라우터가 원본 PIM-DM 상태 갱신 패킷을 생성하고 갱신 간격을 구성할 수 있도록 합니다. 원본 PIM-DM 상태 갱신 패킷 생성을 취소하려면 이 명령어를 “no”로 설정하십시오.

**ip pim state-refresh origination-interval [***interval***]**
**no ip pim state-refresh origination-interval**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| interval | 소스와 직접 연결된 첫 번째 포트 라우터의 상태 갱신 패킷 전송 간격입니다. 이후 라우터에서는 포트에서 상태 갱신 패킷을 받는 간격입니다. 이 매개변수는 선택적으로 구성할 수 있으며, 범위는 4 초에서 100 초 사이입니다. 기본값은 60 초입니다. |

**(3) 기본값**

이 매개변수는 선택적입니다. 기본값은 60 초입니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령어는 멀티캐스트 소스와 직접 연결된 첫 번째 라우터의 수신 포트에서 구성하십시오. 기본값으로 상태 갱신 패킷을 생성합니다. 이후 라우터의 포트에서 이 명령어를 구성할 때는 상태 갱신 패킷을 받는 간격을 제한할 수 있습니다.

**(6) 예제**

Router_config_e1/1#ip pim-dm state-refresh origination-interval 80

**(7) 연관 명령어**

ip pim-dm state-refresh 바활성화

### 36.1.8. ip pim-dm neighbor-filter

**(1) 구문**

이 명령어는 특정 라우터가 PIM-DM 작업에 참여하지 않도록 차단합니다. "no"로 설정하면 제한을 취소합니다.

**ip pim-dm neighbor-filter** access-list-name
**no ip pim-dm neighbor-filter** access-list-name

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *access-list-name* | PIM 패킷을 지정된 소스에서 거부하는 표준 액세스 리스트입니다. |

**(3) 기본값**

필터 기능 없음

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

여러 개의 필터 리스트를 사용할 수 있습니다. 이 리스트 중 하나라도 거부된 라우터는 로컬 PIM-DM 의 이웃이 될 수 없습니다.

**(6) 예제**

router_config_e1/1#ip pim-dm neighbor-filter nbr_filter
router_config#ip access-list standard nbr_filter
router_config_std_nacl#deny 192.167.20.132 255.255.255.255
router_config_std_nacl#permit 192.168.20.0 255.255.255.0

**(7) 연관 명령어**

access-list

### 36.1.9. ip pim-dm state-refresh 비활성화

**(1) 구문**

이 명령어는 PIM-DM 멀티캐스트 프로토콜을 실행하는 라우터에서 상태 갱신 제어 메시지를 전달하지 않도록 합니다. 이 명령어를 "no"로 설정하면 전달 기능을 복원할 수 있습니다.

ip pim-dm state-refresh 바활성화
no ip pim-dm state-refresh 바활성화

**(2) 매개변수**

없음

**(3) 기본값**

기본적으로 PIM Dense Mode 상태 갱신 제어 메시지 전달이 허용됩니다.

**(4) 명령어 모드**

슈퍼바이저 모드

**(5) 사용 지침**

이 명령어를 설정하면 PIM-DM 의 Hello 메시지에 상태 갱신 제어 옵션이 포함되지 않으며, 상태 갱신 제어 패킷을 받거나 보낼 수 없습니다.

**(6) 예제**

다음 명령어는 PIM Dense Mode 의 다운스트림 이웃에 상태 갱신 제어 메시지를 전달하지 못하도록 설정합니다.

ip pim-dm state-refresh 바활성화

**(7) 연관 명령어**

ip pim-dm state-refresh origination-interval

### 36.1.10. show ip mroute pim-dm

**(1) 구문**

PIM-DM 멀티캐스트 라우팅 목록 정보를 표시하려면 다음 명령어를 실행하십시오.

**show ip mroute pim-dm** *group-address source*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *group-address* | (선택 사항) 그룹 주소 |
| **source** | (선택 사항) 소스 주소 |

**(3) 기본값**

없음

**(4) 명령어 모드**

사용자 모드를 제외한 모든 모드

**(5) 사용 지침**

이 명령어는 로컬 MRT 에서 모든 (S,G) 또는 지정된 (S,G)만 표시할 수 있습니다.

**(6) 예제**

예제 1: 로컬 MRT 에서 모든 (S,G)를 표시합니다.
Router#show ip mroute pim-dm
PIM-DM Multicast Routing Table

Timers: Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1), 00:00:03 /00:03:27
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1 NoInfo 00:00:07 /00:00:00

(192.168.20.138, 239.1.1.1), 00:00:03 /00:03:27
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1 NoInfo 00:00:07 /00:00:00
Ethernet1/1 NoInfo 00:02:43 /00:00:00

예제 2: 지정된 (S,G)를 로컬 MRT 에서 표시합니다.
Router#show ip mroute pim-dm 224.1.1.1
PIM-DM Multicast Routing Table
Timers: Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1), 00:00:01 /00:03:29
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1 NoInfo 00:03:50 /00:00:00

예제 3: 로컬 MRT 에서 지정된 (S,G)를 표시합니다.
Router#show ip mroute pim-dm 224.1.1.1 192.168.20.131
PIM-DM Multicast Routing Table

### 36.1.11. show ip pim-dm neighbor

#### (1) 구문

PIM-DM 이웃과 선택된 DR(디자이네이티드 라우터)을 표시하려면 다음 명령어를 실행하십시오:
**show ip pim-dm neighbor [***interface-type interface-number***]**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| ***interface-type*** *interface-number* | 인터페이스의 유형과 ID (예: Ethernet1/1, serial 11/0) |

**(3) 기본값**

없음

**(4) 명령어 모드**

사용자 모드를 제외한 모든 모드

**(5) 사용 지침**

이 명령어는 PIM-DM 또는 PIM-SM 이 구성된 LAN 라우터를 확인하는 데 사용됩니다.

**(6) 예제**

예제 1:

```
Router#show ip pim-dm neighbor
    PIM-DM Neighbor Table
Neighbor       Interface      Uptime/Expires    Ver   DR Prior/Mode
Address
192.167.20.132  Ethernet1/1    03:13:34 / 00:00:00  v2   4/D    (DR)
1.1.1.1        Loopback1      03:52:30 / 00:00:00  v2   1/D    (DR)
192.168.20.132  Ethernet2/1    19:35:56 / 00:00:00  v2   1/D
192.168.20.152  Ethernet2/1    00:00:04 / 00:01:41  v2   1/D
192.168.20.204  Ethernet2/1    00:00:36 / 00:01:44  v2   20/D   (DR)
```

예제 2:

```
Router# show ip pim-dm neighbor Ethernet2/1
PIM-DM Neighbor Table
Neighbor       Interface      Uptime/Expires    Ver   DR Prior/Mode
Address
192.168.20.132  Ethernet2/1    19:39:22 / 00:00:00  v2   1/D
192.168.20.152  Ethernet2/1    00:00:30 / 00:01:15  v2   1/D
192.168.20.204  Ethernet2/1    00:00:04 / 00:02:16  v2   20/D   (DR)
```

**(7) 연관 명령어**

ip pim-dm
ip pim-dm dr-priority
ip pim-dm hello-interval
ip pim version
ip pim-dm neighbor-filter
show ip pim-dm interface

### 36.1.12. show ip pim-dm interface

**(1) 구문**

PIM-DM 인터페이스 상태를 표시하려면 다음 명령어를 실행하십시오:

**show ip pim-dm interface [interface-*type* *interface-number*] *[count] [detail]***

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| ***interface-type*** ***interface-number*** | 인터페이스의 유형과 ID (예: Ethernet1/1, serial 11/0) |

**(3) 기본값**

없음

**(4) 명령어 모드**

사용자 모드를 제외한 모든 모드

**(5) 사용 지침**

이 명령어는 PIM-DM 인터페이스 상태만 표시합니다. PIM-DM 인터페이스가 지정되지 않은 경우, 모든 PIM-DM 인터페이스 상태 정보가 표시됩니다.

**(6) 예제**

예제 1:

```
Router#show ip pim interface
address        Interface      Ver/  Nbr   Hello  DR    DR
                              Mode  Count  intvl  Prior
192.167.20.132  Ethernet1/1     v2/D 0     30    4     192.167.20.132
1.1.1.1         Loopback1       v2/D 0     30    1     1.1.1.1
192.168.20.132  Ethernet2/1     v2/D 2     30    1     192.168.20.204
```

예제 2:

```
Router#show ip pim interface Ethernet2/1
address        Interface      Ver/  Nbr   Hello  DR    DR
                              Mode  Count  intvl  Prior
192.168.20.132  Ethernet2/1     v2/D 2     30    1     192.168.20.204
```

**(7) 연관 명령어**

ip pim-dm
ip pim-dm dr-priority
ip pim-dm hello-interval
ip pim version
ip pim-dm neighbor-filter
show ip pim-dm neighbor

### 36.1.13. show ip rpf pim-dm

#### (1) 구문

멀티캐스트 라우트가 Reverse Path Forwarding (RPF)을 수행하는 방식을 표시하려면 다음 명령어를 실행하십시오:
**show ip rpf pim-dm** *source-address*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *source-address* | 지정된 소스 주소에 대한 RPF 정보를 표시합니다. |

#### (3) 기본값

없음

#### (4) 명령어 모드

사용자 모드를 제외한 모든 모드

#### (5) 사용 지침

PIM-DM 프로토콜은 여러 유형의 라우팅 테이블에서 RPF 정보를 얻을 수 있습니다. 이 명령어는 RPF 정보가 어디에서 가져오는지 알려줍니다.

#### (6) 예제

Router#show ip rpf pim 4.1.1.1
RPF information for (4.1.1.1)
RPF interface: Ethernet2/1
RPF neighbor: 192.168.20.80
RPF route/mask: 192.168.20.0/24
RPF type: unicast
Metric preference: 120
Metric: 1

#### (7) 연관 명령어

없음

# 37. PIM-SM 설정 명령

## 37.1. PIM-SM 설정 명령어

### 37.1.1. ip pim-sm

#### (1) 구문

ip pim-sm
no ip pim-sm

#### (2) 매개변수

없음

#### (3) 기본값

PIM-SM 비활성화

#### (4) 명령어 모드

인터페이스 설정 모드

#### (5) 사용 지침

PIM-SM 기능을 인터페이스에서 활성화하려면 이 명령어를 사용하십시오. 처음 라우터에서 PIM-SM 을 구성할 때 인터페이스에서 PIM-SM 을 활성화하고, 마지막 인터페이스에서 PIM-SM 구성을 취소하여 PIM-SM 실행을 중지할 수 있습니다.

#### (6) 연관 명령어

없음

### 37.1.2. ip pim-sm admin-scope

#### (1) 구문

멀티캐스트 관리자 범위를 설정하려면 ip pim-sm admin-scope gaddr gmask 명령어를 실행합니다. 지정된 멀티캐스트 주소 범위는 239.0.0.0 에서 239.255.255.255 사이입니다. 이 명령은 다른 SZ 와 상호 작용하는 엣지 라우터에서만 설정됩니다.

**ip pim-sm admin-scope** *gaddr gmask*
**no ip pim-sm admin-scope**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 설명 |
|---|---|---|
| admin-scope | admin-scope - pim-sm 관리자 범위 | C-BSR 과 ZBR 만 이 범위를 인식하도록 설정해야 합니다. 다른 라우터는 C-RP 를 포함하여 Bootstrap 메시지에서 범위의 존재를 알게 됩니다. |
| gaddr | A.B.C.D - 개인 그룹 주소 접두사 | 239.0.0.0 에서 239.255.255.255 까지 |
| gmask | gmask - sz 그룹 마스크 | |

**(3) 기본값**

전역 도메인은 기본값으로 224.0.0.0/4 입니다.

**(4) 명령어 모드**

포트 구성 모드

**(5) 사용 지침**

이 명령은 PIM-SM 관리자 범위의 경계를 설정하며, 관리자 범위 외부에서 수신한 BSM 정보를 확인하는 데 사용됩니다. 수신한 BSM 정보의 SZ 범위가 로컬에서 설정한 관리자 범위보다 작거나 같으면, 해당 BSM 정보는 폐기됩니다. 그렇지 않으면, 수신된 BSM 정보는 로컬 관리자 범위로 들어갑니다. BSM 정보가 로컬로 전달될 때도 동일한 원칙이 적용됩니다.

SZ1 의 RP 는 C-RP-ADV 정보를 전역 SZ 에 알리지 그러나 전역
BSM 정보는 들어올 수 있습니다.

**(6) 예제**

다음 예제는 라우터 A 에서 경계 범위를 pim-sm sz1 (239.1.1.1/24)로 설정하는 방법을 보여줍니다.

RouterA_config_f0/0#ip pim-sm admin-scope 239.1.1.1 255.255.255.0
RouterB_config_ps# c-bsr interface lo1
RouterB_config_ps# c-bsr admin-scope 239.1.1.1 255.255.255.0

**(7) 연관 명령어**

ip pim-sm bsr-border
c-bsr intf_type intf_name

### 37.1.3. ip pim-sm asrt-hold

#### (1) 구문

포트에 대해 assert 상태의 홀드 타임을 설정하려면 다음 명령어를 실행합니다.

**ip pim-sm asrt-hold intvl**
**no ip pim-sm asrt-hold [intvl]**

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 설명 |
|---|---|---|
| pim-sm | pim-sm | PIM 스패스 모드 작업을 활성화 |
| asrt-hold | asrt-hold - assert 상태 홀드 타이머 | |
| intvl | 〈7-65535〉 - 시간 값(초) | 기본값은 180 초입니다. |

#### (3) 기본값

180 초

#### (4) 명령어 모드

포트 구성 모드

#### (5) 사용 지침

없음

#### (6) 예제

다음 예제는 포트 f0/0 에서 assert 상태의 타임아웃 시간을 200 초로 설정하는 방법을 보여줍니다.

Router_config_f0/0#ip pim-sm holdtimer assert 200

### 37.1.4. ip pim-sm bsr-border

#### (1) 구문

ip pim-sm bsr-border
no ip pim-sm bsr-border

#### (2) 매개변수

없음

**(3) 기본값**

Non-BSR 경계

**(4) 명령어 모드**

전역 설정 모드

**(5) 사용 지침**

이 명령은 인터페이스를 BSR 경계로 설정할 수 있습니다. 이 인터페이스는 BSM 메시지를 송수신하지 않으며, "no" 명령을 사용하여 기본값으로 복구할 수 있습니다.

이 명령은 BSR 경계의 정의를 변경하여 서로 다른 PIM-SM 도메인에서 BSM 메시지가 영향을 미치지 않도록 합니다.

**(6) 연관 명령어**

없음

### 37.1.5. ip pim-sm dr-pri

**(1) 구문**

**ip pim-sm dr-pri** *pri-value*
**no ip pim-sm dr-pri** *pri-value*

**(2) 매개변수**

| 이름 | 영어 프롬프트 |
|---|---|
| dr-pri | dr-pri - pim-sm 인터페이스 DR 우선순위 |
| pri-value | 〈0-4294967294〉 - DR 우선순위, 더 큰 값이 우선 |

**(3) 기본값**

전역 모드에서 DR 우선순위는 기본값으로 1 입니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

인터페이스 DR 우선순위를 변경하려면 "no" 명령을 사용하여 기본값으로 복구할 수 있습니다.

우선순위가 가장 높은 라우터가 DR 이 되며, 우선순위가 같으면 주소가 가장 높은 라우터가 DR 이 됩니다.

**(6) 연관 명령어**

없음

### 37.1.6. ip pim-sm hello-intvl

**(1) 구문**

**ip pim-sm hello-intvl** seconds
**no pim-sm hello-intvl** [seconds]

**(2) 매개변수**

| 이름 | 영어 프롬프트 |
|---|---|
| hello-intvl | hello-intvl - pim-sm hello 광고 간격 |
| Seconds | 〈1-65535〉 - 주기적인 pim hello 메시지 전송 주기(단위: 초) |

**(3) 기본값**

Hello 메시지를 보내는 간격은 30 초입니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

Hello 메시지 전송 간격을 설정하려면 "no" 명령을 사용하여 기본값으로 갱신할 수 있습니다. 이웃 라우터의 홀드 타임을 변경하려면, 홀드 타임은 hello 메시지 전송 간격의 3.5 배입니다.

**(6) 연관 명령어**

없음

### 37.1.7. ip pim-sm holdtime

**(1) 구문**

PIM-SM 포트의 hello 타이머 간격을 설정하려면, 먼저 아래 명령어를 실행합니다. 간격 값은 4 에서 65535 사이입니다.

**ip pim-sm holdtime** seconds
**no pim-sm holdtime** [seconds]

**(2) 매개변수**

| 이름 | 영어 프롬프트 |
|---|---|
| Holdtime | holdtime - 이웃과의 keep-alive 시간 |
| *Seconds* | 〈4-65535〉 - keep-alive 시간 값 |

**(3) 기본값**

105 초

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령은 포트 구성 모드에서 먼저 실행한 후 전역 설정 모드에서 설정할 수 있습니다. 또는 기본값을 선택할 수 있습니다. Holdtime 값이 Hello 간격 값보다 작으면, 설정된 값은 무효가 됩니다. Holdtime 값은 hello-intvl * 3.5 입니다.

**(6) 예제**

다음 예제는 pimsm 구성을 위해 인터페이스의 holdtime 값을 100 으로 설정하는 방법을 보여줍니다.
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm holdtime 100

**(7) 연관 명령어**

ip pim-sm hold-intvl
intvl-time hello hlo-intvl

### 37.1.8. ip pim-sm horizon-split

**(1) 구문**

BSM 패킷의 Horizon split 전략을 포트에서 설정하려면 다음 명령어를 실행합니다.

**ip pim-sm horizon-split**
**no ip pim-sm horizon-split**

**(2) 매개변수**

| 이름 | 영어 프롬프트 |
|---|---|
| horizon-split | Horizon-split - 인터페이스의 horizon split 허용 |

**(3) 기본값**

수평 분할은 기본값으로 비활성화되어 있습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령이 적용된 후, PIM-SM 포트의 해당 레이블 비트를 설정할 수 있습니다. 해당 포트에서 수신한 BSM 패킷은 다른 포트로 전송되지 않습니다.

**(6) 예제**

다음 예제는 인터페이스 f0/0 에서 Horizon split 기능을 활성화하는 방법을 보여줍니다.
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm horizon-split

**(7) 연관 명령어**

bsm policy

### 37.1.9. ip pim-sm jp-hold

**(1) 구문**

PIM-SM 과 관련된 포트에서 join-prune 상태에 대한 holdtime 을 설정하려면, 먼저 아래 명령어를 실행합니다.

**ip pim-sm jp-hold *intvl***
**no ip pim-sm jp-hold [*intvl*]**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|

| | | |
|---|---|---|
| pim-sm | pim-sm - PIM sparse mode 동작 활성화 | |
| jp-hold | Join-prune - join-prune 상태 hold 타이머 | |
| intvl | 〈1-65535〉 - 시간 값(초) | 기본값 은 210 초. |

**(3) 기본값**

210 초

**(4) 명령어 모드**

포트 구성 모드

**(5) 사용 지침**

없음

**(6) 예제**

다음 예제는 f0/0 포트에서 join 상태의 타임아웃 시간을 200 초로 설정하는 방법을 보여줍니다.

Router_config_f0/0#ip pim-sm jp-hold 200

### 37.1.10. ip pim-sm jp-intvl

**(1) 구문**

정기적으로 join 또는 prune 패킷을 전송하는 간격을 설정하려면, 먼저 아래 명령어를 실행합니다. 간격은 초 단위로 1 에서 65535 사이입니다.

**ip pim-sm jp-intvl [s*econds*]**
**no ip pim-sm jp-intvl**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | pim-sm - PIM sparse mode 동작 활성화 | |
| jp-intvl | jp-intvl - 정기적인 Join/Prune 메시지 전송 간격 (단위: 초) | |

| | | |
|---|---|---|
| ***Seconds*** | 〈1-65535〉 - 시간 값(초) | 기본값 60 초. |

**(3) 기본값**

60 초

**(4) 명령어 모드**

포트 구성 모드

**(5) 사용 지침**

각 구성이 있을 때마다 PIM-SM 데이터베이스는 (s, g) 쌍 또는 (*, g) 쌍에 대해 완전히 검색해야 합니다. 만약 구성된 포트가 업스트림 포트라면, 해당 (s, g) 또는 (*, g) 쌍의 jp 타이머 간격은 리셋됩니다. 포트 구성 모드에서 설정된 간격은 전역 모드에서 설정된 join/prune 간격보다 우선합니다. 다운스트림 이웃으로부터 Join 패킷이 세 번의 JP 타임아웃 기간 동안 수신되지 않으면, 해당 멀티캐스트 항목에 대한 다운스트림은 prune 상태로 전환됩니다. 기본 holdtime 은 3 분입니다. 이 값을 임의로 변경하면 CPU 충격 및 서비스 전달 충격이 발생할 수 있습니다.

**(6) 예제**

다음 예제는 PIM join 메시지 간격을 90 초로 변경하는 방법을 보여줍니다:
Router_config_f0/0# ip pim-sm jp-intvl 90

**(7) 연관 명령어**

ip pim-sm jp-hold

### 37.1.11. ip pim-sm lan-delay

**(1) 구문**

PIM-SM 포트에서 prune 지연 시간을 지정하려면, 먼저 아래 명령어를 실행합니다.

**ip pim-sm lan-delay** *delay-intvl*
**no pim-sm lan-delay**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|

| | | |
|---|---|---|
| lan-delay | lan-delay - PIM-SM prune 지연 | |
| delay-intvl | 〈1-32767〉 - prune 지연 타이머 간격(단위: ms) | 기본값 500 milli 초. |

**(3) 기본값**

500ms

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

로컬 포트가 다운스트림 포트인 경우, 최종적으로 계산된 prune 지연 시간은 다운스트림 이웃이 보고한 모든 최대 값에 기반합니다. 이 경우, 업스트림 이웃에게 join 패킷을 전송하는 타이머가 영향을 받습니다. 만약 prune_delay 옵션이 모든 다운스트림 이웃에서 지원되지 않으면, 기본값이 prune 대기 타이머의 초과 시간으로 사용됩니다. prune 지연 타이머의 간격이 로컬에서 설정되면, 이는 HELLO 패킷을 통해 업스트림 이웃에게 보고됩니다.

**(6) 예제**

다음 예제는 pim-sm 인터페이스 f0/0 에서 prune 지연 값을 20ms 로 설정하는 방법을 보여줍니다:
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm lan-delay 20

**(7) 연관 명령어**

ip pim-sm override

### 37.1.12. ip pim-sm nbma-mode

**(1) 구문**

모든 NBMA 인터페이스에 대해 아래 명령어를 구성하면, 중앙 노드는 서브 노드에서 전송된 모든 정보를 전달하고, 다른 서브 노드는 해당 정보를 얻을 수 있습니다.

**ip pim-sm nbma-mode**
**no ip pim-sm nbma-mode**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| nbma-mode | nbma-mode - 인터페이스에서 Non-Broadcast Multi-Access (NBMA) 모드 사용 | 현재 우리 제품은 이 기능을 지원하지 않습니다 |

**(3) 기본값**

비활성화

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

전통적인 NBMA 네트워크(프레임 릴레이, ATM, SMDS)는 포인트-투-다중모드(Point-to-multipoint mode)를 채택합니다. 서브 노드가 잘리기를 원할 때, 이 정보는 중앙 노드에 직접 보고되며, 다른 서브 노드는 이 정보를 받을 수 없습니다. 이 경우 다른 서브 노드는 응답할 수 없으며, 중앙 노드의 인터페이스가 잘못 잘리게 됩니다.

위 명령어를 모든 NBMA 인터페이스에 구성하면, 중앙 노드는 서브 노드에서 전송된 모든 정보를 전달하고, 다른 서브 노드는 해당 정보를 얻을 수 있습니다.

이 명령어는 Ethernet 이나 FDDI 와 같은 멀티캐스트 LAN 에서는 사용할 수 없습니다.

**(6) 예제**

다음 예제는 인터페이스를 NBMA 모드로 구성하는 방법을 보여줍니다:
Router_config#interface s1/0
Router_config_s1/0#ip address 10.0.1.2 255.255.255.0
Router_config_s1/0#ip pim-sm nbma-mode

**(7) 연관 명령어**

없음

### 37.1.13. ip pim-sm nbr-filter

**(1) 구문**

PIM 에 장치를 추가하는 것을 차단하려면 아래 첫 번째 명령어를 실행하고, 이 기능을 취소하려면 두 번째 명령어를 실행합니다.

**ip pim-sm nbr-filter** *acl-name*
**no ip pim-sm nbr-filter**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| nbr-filter | nbr-filter - PIM 피어링 필터 | |
| acl-name | WORD - IP 표준 액세스 목록 이름 | |

**(3) 기본값**

비활성화

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령어를 구성하면, Hello 패킷을 수신할 때 이웃이 필터링되어 새로운 이웃을 만들 수 있습니다. 만약 필터링이 거부 상태이면, 해당 새로운 이웃은 만들어지지 않습니다. 여러 개의 이웃 액세스 목록을 구성할 수 있습니다(새로운 CISCO 바이너리에서는 이웃 액세스 목록 하나만 구성할 수 있음; 오래된 바이너리에서는 여러 개의 이웃 액세스 목록을 구성할 수 있음). 이웃이 필터링되면, 해당 이웃은 거부됩니다.

**(6) 예제**

다음 예제는 라우터 A 에서 스텁 멀티캐스트 라우팅을 구성하고, 라우터 B 가 액세스 목록 1 을 사용하여 라우터 A 의 모든 PIM 정보를 필터링하는 방법을 보여줍니다.

**Router A 설정:**
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.1 255.255.255.0
Router_config#interface f0/1
Router_config_f0/1# ip igmp-helper 10.0.0.2

**Router B 설정:**

```
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.2 255.255.255.0
Router_config_f0/0# ip pim-sm nbr-filter 1
Router_config#ip access-list standard 1
Router_config_std_nacl# deny 10.0.0.1
Router_config_std_nacl# permit any
```

**(7) 연관 명령어**

ip pim-sm jp-intvl

### 37.1.14. ip pim-sm nbr-track

**(1) 구문**

JOIN 패킷의 제한을 전역적으로 금지하고, 이웃 추적을 활성화하려면 아래 명령어를 실행하세요:

**ip pim-sm nbr-track**

**no ip pim-sm nbr-track**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **nbr-track** | nbr-trackPIM-SM 인터페이스 이웃 추적 | |

**(3) 기본값**

전역 설정 모드가 구성되지 않으면, 이웃 추적은 금지됩니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 명령어는 JOIN 패킷의 제한 기능을 금지하고 이웃 추적을 활성화하는 데 사용됩니다.

**(6) 예제**

다음 예제는 인터페이스 f0/0 에서 이웃 추적 기능을 활성화하는 방법을 보여줍니다.

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm nbr-track
```

**(7) 연관 명령어**

없음

### 37.1.15. ip pim-sm override

**(1) 구문**

PIM-SM 포트의 프룬 거부 시간을 지정하려면 아래 명령어를 실행하세요.

**ip pim-sm override** *override-intvl*
**no ip pim-sm override**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **override** | override PIM-SM override 타이머 | |
| ***override-intvl*** | 〈1-65535〉 - override 타임아웃 간격(단위: 100ms) | |

**(3) 기본값**

2.5 초

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

최종적으로 계산된 프룬 거부 시간은 모든 이웃들이 보고한 최대 값에 기반합니다. 일부 이웃이 프룬 거부를 지원하지 않으면 기본값이 선택됩니다. OT 가 활성화되면, 값은 랜덤이 될 수 있습니다. 프룬 거부 타이머의 간격이 로컬로 설정되면, 해당 값은 HELLO 패킷을 통해 업스트림 이웃에게 보고됩니다.

**(6) 예제**

다음 예제는 pim-sm 인터페이스 f0/0 에 대해 override 값을 2000ms 로 설정합니다:
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm override 200

**(7) 연관 명령어**

ip pim-sm lan-delay

### 37.1.16. router pim-sm

**(1) 구문**

전역 PIM-SM 뷰에 진입하려면 아래 명령어를 실행하세요:
**router pim-sm**
**no router pim-sm**

**(2) 매개변수**

없음

**(3) 기본값**

시스템은 기본적으로 PIM-SM 뷰를 생성하지 않습니다.

**(4) 명령어 모드**

전역 설정 모드

**(5) 사용 지침**

router pim-sm 명령어가 전역적으로 구성되거나, PIM-SM 관련 설정이 포트에 처음 구성되면 전역 PIM-SM 뷰가 생성됩니다. 포트에 PIM-SM 관련 설정이 있으면, 전역 뷰를 삭제할 수 없습니다.

**(6) 예제**

다음 명령어는 전역 PIM-SM 뷰를 생성하는 방법을 보여줍니다:

Router_config#router pim-sm
Router_config_ps#

**(7) 연관 명령어**

ip pim-sm

### 37.1.17. hello-option

**(1) 구문**

전역 PIM-SM 뷰에서 글로벌 DR 우선순위, 프룬 지연 시간, HELLO 패킷의 전송 간격, 프룬 거부 시간, 이웃 추적 및 이웃 타임아웃 시간을 설정하려면 아래 명령어를 실행하세요:
hello-option { dr-pri pri-value | lan-delay delay-intvl |
override override-intvl | nbr-track | holdtime hold-intvl }
no hello-option [dr-pri | lan-delay | override | nbr-track | holdtime]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **dr-pri** | dr-pri - PIM-SM 글로벌 DR 우선순위 | |
| *pri-value* | 〈0-4294967294〉 - DR 우선순위 값, 더 큰 값에 우선순위 부여 | 이 명령이 설정되지 않은 경우, 이 프로세스의 기본값 DR 우선순위는 1 입니다 |
| **lan-delay** | lan-delay - PIM-SM 프룬 지연 시간 설정 | 프룬 지연 시간을 설정합니다. |
| **override** | Override - 수신한 프룬에 대한 거부 설정 | 프룬 거부를 설정합니다. |
| ***delay-intvl*** | **〈0-32767〉** - 프룬 지연 시간 값 | 기본값 프룬 지연 시간은 500ms 입니다. |
| ***override-intvl*** | **〈0-65535〉** 오버라이드 지연 시간 | 기본값 프룬 거부 시간은 2500ms 입니다. |
| **nbr-track** | **nbr-track - 이웃 추적 활성화 설정** | 이 명령이 설정된 경우, JOIN 패킷은 제한되지 않습니다 |
| **holdtime** | **holdtime - 이웃 유지 시간 타이머** | |
| ***hold-intvl*** | **〈4-65535〉** - 이웃 타임아웃 시간 값 | 일반적으로, 해당 값은 포트의 Hello 간격보다 3.5 배 더 큽니다.<br>기본값 이웃 홀드타임은 105 초입니다. |

**(3) 기본값**

위의 표를 참조하세요.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

포트에 해당하는 설정 항목이 없으면 전역적으로 구성된 속성이 포트에 적용됩니다. 글로벌 DR 우선순위 변경은 새로운 DR 선택에 영향을 미칠 수 있습니다. DR 선택 규칙은 다음과 같습니다:

포트에서 가장 높은 DR 우선순위가 해당 포트가 속한 네트워크 세그먼트의 DR 로 선택됩니다. 동일한 DR 값이 여러 개 있으면, 로컬 포트의 주요 IP 주소와 이웃의 주요 IP 주소 중 상대적으로 큰 IP 주소가 DR 로 선택됩니다.

포트에 이웃이 있거나 DR 우선순위가 지원되지 않는 경우, 상대적으로 큰 주요 IP 주소가 DR 로 선택됩니다.

**(6) 예제**

다음 예제는 글로벌 PIM-SM 구성에서 DR 우선순위 값을 200 으로 설정하는 방법을 보여줍니다:
Router_config#Router pim-sm
Router_config_ps#dr-priority 200

### 37.1.18. accept bsm-adv

**(1) 구문**

글로벌 모드에서 accept bsm-adv 를 실행하여 필터링 리스트를 설정할 수 있습니다. 이 필터링 리스트 설정은 특정 BSM 소스 주소를 필터링하고 지정된 BSM 소스 주소만 받도록 설정하는 데 사용됩니다. 필터링을 취소하려면 no accept bsm-adv [list std-acl]를 실행하세요.

**accept bsm-adv list** *std-acl*
**no accept bsm-adv [***list std-acl***]**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **accept** | Accept 수락 정책 구성 | |
| bsm-adv | bsm-adv - BSM 패킷 소스 주소 수락 필터 | |
| list | list - BSM 소스 리스트를 위한 IP 접근 리스트 | |
| *std-acl* | WORD -- 표준 접근 리스트 이름 | 이것은 BSM 소스 주소의 범위를 제한하는 데 사용됩니다. |

**(3) 기본값**

기본적으로 필터링은 비활성화되어 있습니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

하나의 필터링 명령만 설정할 수 있습니다.

**(6) 예제**

다음 예제는 네트워크 세그먼트 192.2.2.0/30 에서 오는 BSM 알림만 수신하도록 설정하는 방법을 보여줍니다.

```
Router_config#router pim-sm
Router_config_ps#accept bsm-adv list adv-src
Router_config_ps#exit
Router_config#ip access-list stand adv-src
Router_config_std_nacl#permit 192.2.2.0 255.255.255.252
```

### 37.1.19. accept crp-adv

**(1) 구문**

특정 그룹의 주소 범위를 필터링하고, 특정 후보 RP 유니캐스트에서만 C-RP-ADV 패킷을 받도록 설정하려면, ACL 을 통해 수신된 패킷에서 그룹 주소 범위를 지정하여 필터링할 수 있습니다. 필터링을 취소하려면 no accept crp-adv *.*.*.* [std-acl]를 실행하세요.

accept crp-adv *.*.*.* [std-acl]
no accept crp-adv *.*.*.* [std-acl]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **accept** | Accept - 수락 정책 구성 | |
| **c-rp-adv** | crp-adv - C-RP-ADV 수락 필터 | |
| *A.B.C.D* | A.B.C.D - 그룹에 대한 후보 RP 의 IP 주소 | |
| *std-acl* | WORD 그룹을 위한 IP 표준 접근 리스트 이름 | |

**(3) 기본값**

기본적으로 C-RP-ADV 패킷을 필터링하지 않습니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

이 명령어가 설정된 후, BSR 은 RP 에서 오는 C-RP-ADV 만 처리합니다. 또한, 그룹 주소의 범위는 표준 ACL 에 의해 허용되어야 합니다.

**(6) 예제**

다음 예제는 라우터가 224.2.2.2 멀티캐스트 그룹에 대해 RP 주소가 100.1.1.1 인 C-RP 메시지를 수락하도록 설정하는 방법을 보여줍니다:
Router_config#router pim-sm
Router_config_ps#accept crp-adv 100.1.1.1 grp-acl
Router_config#ip access-list stand grp-acl
Router_config_std_nacl#permit 224.2.2.2 255.255.255.255

### 37.1.20. accept rp-addr

#### (1) 구문

accept-rp 는 전역 설정 모드에서 특정 그룹 주소 범위를 필터링하여 (*, G) 조인/프룬을 허용할지 여부를 결정하고, 특정 대상 그룹 주소의 등록 정보를 응답하는 필터링 리스트를 설정할 수 있습니다. 이 설정을 취소하려면 이 명령어의 "no" 형식을 실행하세요.

accept rp-addr A.B.C.D [std-acl]
no accept rp-addr A.B.C.D [std-acl]

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **accept** | Accept - 수락 정책 구성<br>Accept - 패킷 수신 정책 구성. | |
| **rp-addr** | rp-addr - RP 주소 수락 필터<br>rp-addr - 수락 가능한 RP 주소 필터 구성. | |
| *A.B.C.D* | A.B.C.D - 그룹에 대한 RP 의 IP 주소<br>A.B.C.D - 멀티캐스트 그룹의 RP 주소 지정 | |
| *std-acl* | WORD - 그룹에 대한 ip 표준 액세스 목록 이름<br>WORD - 멀티캐스트 그룹 필터링에 사용되는 표준 액세스 목록을 나타냅니다. | 이를 생략하면, 라우터는 RP 에 매핑된 모든 그룹에 대해 PIM-SM 메시지를 처리합니다. |

#### (3) 기본값

비활성화 (기본적으로 모든 Join, Prune 또는 Register 패킷은 처리됩니다)

#### (4) 명령어 모드

PIM-SM 전역 뷰

#### (5) 사용 지침

이 명령어가 설정되면 라우터는 지정된 RP 에 매핑된 Join 패킷만 처리합니다. 중요한 점은 그룹 주소 범위가 표준 접근 리스트에 의해 허용되어야 하며, 해당 그룹의 집합체가 계산된 RP 여야만 접근 필터링 리스트가 적용될 수 있다는 것입니다. 그룹 주소가 거부되면 RP 는

Join 및 Register 패킷을 거부하고, Register 패킷을 수신한 후 RP 는 Register Stop 패킷을 등록 패킷 생성기로 반환합니다.

이 명령어는 rp-addr 매개변수가 다를 경우 여러 번 설정할 수 있습니다. 그룹 주소가 매핑된 RP 가 설정된 범위에 포함되지 않으면 RP 는 이를 거부합니다.

**(6) 예제**

다음 예제는 라우터가 100.1.1.1 주소에 대한 RP 에 대해 224.2.2.2 멀티캐스트 그룹을 위한 Join 또는 Prune 메시지를 수락하도록 설정하는 방법을 보여줍니다:
Router_config#router pim-sm
Router_config_ps#accept rp 100.1.1.1 no-ssm-range
Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#permit 224.2.2.2

%PIM-6-INVALID_RP_JOIN: Received (*, 238.1.1.1) Join from 192.17.20.173 for invalid RP 1.1.1.1
Router#show ip mroute
(*, 238.1.1.1), 00:02:52/00:00:07, RP 1.1.1.1, flags: S
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
 FastEthernet0/0, Forward/Sparse, 00:02:52/00:00:07
It can be seen that the previous address, *.238.1.1.1, ages after the filtration is set.

### 37.1.21. accept register

**(1) 구문**

C-RP 에서 Register 범위 리스트가 설정되고, RP 가 선택되어 PIM-SM Register 패킷이 수신되면, 필터링 리스트를 사용하여 Register 패킷을 필터링해야 합니다. 이 경우 accept-register 를 실행하고, 필터링을 취소하려면 이 명령어의 "no" 형식을 실행합니다.

accept register {list ext-acl | route-map map-name}
no accept register [list ext-acl | route-map map-name]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **accept** | Accept - 수락 정책 구성<br>Accept - 패킷 수신 정책 구성 | |

| | | |
|---|---|---|
| **register** | register – 수락 필터 등록<br>Register - Register 메시지 수신 필터를 나타냅니다. | |
| *list* | list - 액세스 목록<br>list - 액세스 목록을 나타냅니다. | |
| *route-map* | Route-map - 라우트 맵<br>route-map - 라우트 맵 목록을 나타냅니다 | |
| *ext-acl* | WORD - IP 확장 액세스 목록 이름<br>WORD - 확장 가능한 IP 액세스 제어 목록의 이름을 나타냅니다. | |
| *map-name* | WORD - 라우트 맵 이름<br>WORD - 라우트 맵 목록의 이름을 나타냅니다 | |

**(3) 기본값**

기본적으로 Register 패킷에 대한 접근 리스트 필터링 또는 경로 맵 필터링이 수행되지 않습니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

이 명령어는 인증되지 않은 데이터 소스가 Register 패킷을 RP 로 보내는 것을 방지하는 데 사용됩니다. 인증되지 않은 데이터 소스가 Register 패킷을 RP 로 보내면, RP 는 즉시 Register Stop 패킷을 반환합니다. 이 명령어는 RP 로 실행되는 장치에서만 유효합니다.

**(6) 예제**

다음 예제는 라우터가 Source Specific Multicast (SSM) 주소 범위의 소스가 RP 에 등록되지 않도록 제한하는 방법을 보여줍니다.

```
Router_config#router pim-sm
Router_config_ps#accept register list no-ssm-range
Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#deny ip any 232.0.0.0 0.255.255.255
Router_config_std_nacl#permit ip any any
```

**(7) 연관 명령어**

reg-src

### 37.1.22. anycast-rp

#### (1) 구문

anycast-rp 와 해당 이웃 주소를 설정하여 RP 의 부하를 분담할 수 있는 해당 피어 이웃을 지정할 수 있습니다. 이 설정을 취소하려면 이 명령어의 "no" 형식을 실행하세요.

anycast-rp A.B.C.D nbr *.*.*.*
no anycast-rp A.B.C.D nbr *.*.*.*

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **anycast-rp** | anycast-rp - PIM-SM 의 Anycast RP 설정 | |
| *A.B.C.D* | *A.B.C.D - Anycast RP 주소* | |
| ***nbr*** | nbr - Anycast RP 이웃 | |
| ***.*.*.** | *A.B.C.D - Anycast RP 이웃 주소* | |

#### (3) 기본값

기본적으로 이 명령어는 영향을 미치지 않습니다.

#### (4) 명령어 모드

PIM-SM 전역 뷰

#### (5) 사용 지침

PIM-SM 은 단일 RP 의 기준을 규제하지만, 큰 데이터 흐름은 단일 RP 에 과부하를 일으킬 수 있습니다. 이 경우 anycast-rp 명령어를 사용하여 PIM-SM 도메인 내에서 RP 의 과부하 문제를 해결할 수 있습니다.

참조:
이 명령어는 PIM 도메인의 백본 네트워크에서 좋은 연결성을 가진 장비에서 구성하는 것이 좋습니다. 즉, 다이얼업을 통해 다른 PIM 장비와 연결하는 무음 터미널 라우터에서는 이 명령어를 설정하는 것이 적합하지 않습니다.

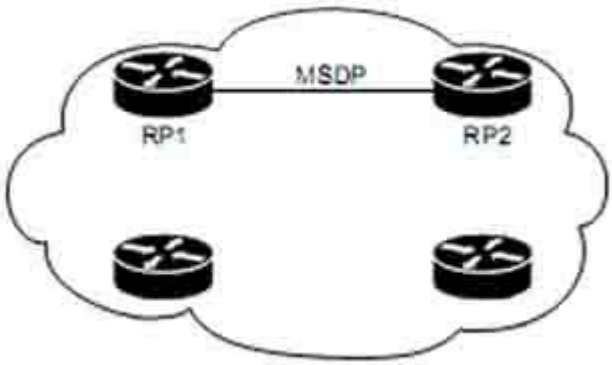
내부 도메인에서 MSDP 가 사용되지 않으면, anycast rp 를 지정하는 장치는 동일한 RP 주소를 가진 이웃의 주소도 동시에 지정해야 Register 처리에 도움이 됩니다.

anycast-rp A.B.C.D nbr 명령어는 MSDP 설정이 없는 장치에서 사용되며, 정적 RP 로 주소를 제공할 때 사용됩니다. 모든 피어 이웃을 지정해야 하며, 이웃은 서로 연결 가능해야 합니다.

MSDP 가 설정된 경우, 장치가 정적 RP 주소를 제공한 경우 anycast rp nbr 을 지정할 필요가 없습니다.

**(6) 예제**

MSDP 가 사용되는 경우 anycast-rp 주소 설정 예.




RP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
!
ip msdp peer 10.1.1.2 connect-source loopback 1
ip msdp originator-id loopback 1

RP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
!
ip msdp peer 10.1.1.1 connect-source loopback 1

ip msdp originator-id loopback 1
다른 장치에서 정적 RP 주소를 지정하는 예:
Ra:
router pim-sm
static-rp 10.0.0.1
2. MSDP 를 사용하지 않는 경우 anycast-rp 주소 설정 예.
RP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1

RP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1
다른 장치에서 정적 RP 주소를 지정하는 예:

Ra:
router pim-sm
static-rp 10.0.0.1

**(7) 연관 명령어**

없음

### 37.1.23. reg-rate-limit

**(1) 구문**

(s, g)로 지정된 멀티캐스트 그룹에서 PIM-SM 등록 패킷의 생성 비율을 설정하려면 reg-rate-limit 명령어를 사용하십시오. 이 설정을 취소하려면 no reg-rate-limit [rate]를 실행하십시오.

reg-rate-limit rate
no reg-rate-limit [rate]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **reg-rate-limit** | reg-rate-limit - PIM 등록 패킷의 비율 제한 설정 | |
| *rate* | 〈1-65535〉 초당 패킷 수 | |

**(3) 기본값**

모든 (s,g) 등록 패킷의 생성 비율은 초당 1 개의 패킷으로 제한됩니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

이 명령어는 DR 라우터에서 (s, g)의 등록 패킷 생성 비율을 제한하는 데 사용됩니다. 이 명령어가 활성화되면 DR 라우터의 부하가 제한됩니다. 멀티캐스트 경로를 처음 설정할 때, 멀티캐스트 소스의 갑작스러운 대량 트래픽 발생으로 인해 패킷 손실이 발생할 수 있습니다.

**(6) 예제**

다음 예제는 각 (s, g)가 초당 2 개의 등록 패킷을 생성하도록 설정하는 방법을 보여줍니다.

Router_config#router pim-sm
Router_config_ps#reg-rate-limit 2

### 37.1.24. reg-src

**(1) 구문**

PIM-SM 등록 패킷을 전송하기 위해 DR 이 소스로 사용할 IP 주소를 지정하려면 reg-src 명령어를 사용하십시오. 기본적으로 데이터 소스에 연결된 포트의 주소가 사용됩니다. 이 설정을 취소하려면 no reg-src [intf-type intf-number]를 실행하십시오.

reg-src intf-type intf-number
no reg-src [intf-type intf-number]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **reg-src** | reg-src - PIM Register 의 소스 주소 설정 | |
| *intf-type* | 지정된 포트의 유형 | 포트에 주요 IP 주소나 ID 가 없으면 설정이 적용되지 않습니다. 지정된 포트의 L3 프로토콜은 활성화되어야 합니다 |
| *intf-number* | 포트 번호 | |

**(3) 기본값**

기본값에서는 DR 과 데이터 소스를 연결하는 포트가 Register 패킷의 소스 주소로 사용되어 패킷 캡슐화를 수행합니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

Register 패킷의 기본 소스 주소가 RP 가 Register Stop 패킷을 반환할 수 있는 유일한 라우팅 가능한 대상 주소가 아닐 경우, 이 명령어를 사용하여 Register 패킷의 새로운 소스 주소를 설정해야 합니다. 예를 들어, Register 패킷의 소스 주소가 RP 에서 ACL 로 필터링되거나, 소스 주소가 유일한 IP 주소가 아닐 경우, RP 에서 반환한 Register Stop 패킷이 해당 DR 에 제대로 도달하지 않으면 PIM-SM 등록이 실패할 수 있습니다.

소스 주소가 지정되지 않거나 지정된 소스 주소가 효과가 없다면, DR 은 데이터 소스와 연결된 포트를 소스 주소로 사용하여 Register 패킷을 보냅니다. 따라서 PIM-SM 도메인에 고유한 라우팅 가능한 주소를 루프백 포트에서 소스 주소로 설정하는 것이 좋습니다.

**(6) 예제**

다음 예제는 DR 의 loopback3 포트를 Register 패킷의 소스 주소로 지정하는 방법을 보여줍니다.

Router_config#router pim-sm
Router_config_ps#reg-src loopback 3

### 37.1.25. spt-threshold

#### (1) 구문

PIM-SM 구성 모드에서 흐름이 최단 경로 트리로 전환되는 트래픽 임계값을 설정하려면 spt-threshold 명령어를 사용합니다. 기본 설정으로 되돌리려면 no spt-threshold 를 실행하십시오.

spt-threshold {infinity/kbps} [stand-acl]
no spt-threshold

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **spt-threshold** | spt-threshold - 소스 트리 전환 임계값 설정 | |
| infinity | Infinity - 소스 트리로 절대 전환하지 않음 | 포트에 주요 IP 주소나 ID 가 없으면 설정이 적용되지 않습니다. 지정된 포트의 L3 프로토콜은 활성화되어야 합니다 |
| *kbps* | 〈0-4294967〉 초당 킬로비트로 트래픽 속도 | |
| *stand-acl* | *stand-acl - 그룹에 대한 IP 표준 접근 제어 목록 이름* | |

#### (3) 기본값

전환에 대한 트래픽 제한이 없습니다. 다운스트림 수신기가 데이터 소스를 조인하려고 할 때, 데이터 소스는 데이터를 수신하면 SPT 전환을 시작합니다.

#### (4) 명령어 모드

PIM-SM 전역 뷰

#### (5) 사용 지침

멀티캐스트 소스의 전송 속도가 지정된 임계값에 도달하거나 이를 초과하면, 리프 노드는 (s,g) 조인 패킷을 멀티캐스트 소스로 보내 최단 경로 트리(SPT)를 구축합니다.
임계값이 infinity 로 설정되면, 지정된 그룹에 대해 모든 멀티캐스트 소스가 공유 트리를 사용하여 패킷을 전달합니다. 데이터 소스의 메시지 흐름이 지정된 임계값 미만일 경우, 리프 노드의 PIM-SM 라우터는 일정 시간이 지난 후 다시 공유 트리로 전환하고 소스 트리에서 프룬 메시지를 전송합니다.

**(6) 예제**

다음 예제는 4 kbps 를 임계값으로 설정하여 소스에서 그룹으로의 트래픽이 해당 임계값을 초과할 경우, 라우터가 해당 소스로 최단 경로 트리로 전환하는 방법을 보여줍니다:
Router_config#router pim-sm
Router_config_ps# spt-threshold 4

**(7) 연관 명령어**

없음

### 37.1.26. ssm

**(1) 구문**

특정 멀티캐스트 그룹의 범위를 설정하려면 ssm {기본값 | range std-acl} 명령어를 사용하십시오. 지정된 SSM 범위를 취소하려면 no ssm 을 실행하십시오.
ssm {기본값 | range std-acl}
no ssm

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **ssm** | ssm - Source Specific Multicast 설정 | |
| **기본값** | 기본값 - 기본적으로 SSM 에 232/8 그룹 범위 사용 | |
| **Range** | range - SSM 에 사용할 그룹 범위의 ACL 설정 | |
| *std-acl* | WORD - *IP 표준 접근 제어 목록 이름* | |

**(3) 기본값**

비활성화

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

PIM-SM 이 활성화되면, 기본값 또는 구성된 멀티캐스트 그룹 주소 범위를 사용할 수 있습니다. 만약 멀티캐스트 그룹이 지정된 SSM 범위에 포함된다면, 해당 그룹에 대해 (*,g)를 취소해야 합니다. 전체 PIM-SM 에서 동일한 SSM 전략이 설정되어야 합니다.

참고:
전체 PIM-SM 에서 동일한 SSM 전략을 설정해야 하며, 그렇지 않으면 지정된 SSM 이 (*,g) 조인을 방지하는 효과가 없을 수 있습니다.

PIM-SM 은 다른 프로토콜과 함께 사용할 수 없습니다. SSM 구성이 (*,g) 조인과 (*,*,rp) 조인의 전송을 방지하며, PMBR 장치는 상위 장치로 특정 (s,g) 조인을 전송할 수 없습니다.

SSM 이 설정되면, MSDP 는 지정된 멀티캐스트 그룹 주소 범위에 해당하는 SA 를 생성하거나 수신할 수 없습니다.

그룹 범위가 BIDIR 그룹 범위를 포함하는 경우, 이전 설정은 유지되며, 후속에 오류 메시지가 표시됩니다 (현재 지원되지 않음)

**(6) 예제**

다음 예제는 액세스 목록 grp_range 에 정의된 IP 주소 범위에 대해 SSM 서비스를 구성하는 방법을 보여줍니다:

```
Router_config#router pim-sm
Router_config_ps# ssm range grp_range
Router_config#ip access-list stand grp_range
Router_config_std_nacl# permit 224.2.151.141
```

**(7) 연관 명령어**

없음

### 37.1.27. c-bsr intf_type intf_name

#### (1) 구문

라우터를 후보 BSR 라우터로 설정하려면 아래 두 명령 중 첫 번째 명령을 실행합니다. 이 설정을 취소하려면 두 번째 명령을 실행합니다.

c-bsr intf_type intf_name [hash-length [priority]]
no c-bsr [intf_type] [intf_name] [hash-length] [priority]

#### (2) 매개변수

없음

#### (3) 기본값

동적 BSR 선택은 비활성화되어 있습니다.

#### (4) 명령어 모드

PIM-SM 전역 뷰

#### (5) 사용 지침

이 명령이 설정되면, 포트의 지정된 주소가 BSR 주소로 사용되며, 이 주소는 로컬 머신의 모든 PIM-SM 이웃에게 BSM(부트스트랩 메시지)을 전송합니다. 각 이웃은 이전에 받은 BSM 과 현재 받은 BSM 을 비교하고, 현재 BSM 에 포함된 BSR 주소가 이전 BSM 의 BSR 주소보다 크거나 같으면 로컬에 저장된 BSM 을 업데이트하고 현재 BSM 을 전달합니다. 그렇지 않으면 현재 BSM 은 직접 폐기됩니다. 후보 BSR 이 더 높은 우선순위의 BSM 을 받기 전까지는 항상 자신을 해당 관리 도메인의 BSR 라우터로 간주합니다.

참고:
이 명령은 PIM 도메인에서 좋은 연결을 가진 장비에 설정하는 것이 좋습니다. 즉, 이 명령은 다이얼업을 통해 다른 PIM 장비와 연결되는 단말 라우터에는 적합하지 않습니다.

C-RP-Adv 를 수락할 때, BSR 은 SZ 범위를 만족하는 내용만 수락하며, 범위를 초과하는 내용은 생략됩니다.

장비에서 하나의 포트만 BSR 주소로 지정할 수 있으며, 여러 명령이 설정되면 이전에 설정된 후보 BSR 은 교체됩니다.

이 명령이 효과를 보기 위한 조건은 지정된 포트의 IP 주소가 PIM-SM 상태이고 프로토콜이 활성화되어 있어야 합니다.

**(6) 예제**

다음 예제는 Ethernet 인터페이스 0의 IP 주소를 후보 BSR로 설정합니다.
해시 마스크 길이는 10, 우선순위는 100으로 지정합니다:
Router_config# router pim-sm
Router_config_ps# c-bsr f0/0 10 100

**(7) 연관 명령어**

c-bsr admin-scope {global |gaddr gmask} [hash-length [priority]]

### 37.1.28. C-bsr admin-scope

**(1) 구문**

관리 도메인 내에서 후보 BSR 을 설정하려면 아래 두 명령 중 첫 번째 명령을 실행합니다. 이 설정을 취소하려면 두 번째 명령을 실행합니다.

c-bsr admin-scope {global |gaddr gmask} [hash-length [priority]]
no c-bsr admin-scope

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **c-bsr** | c-bsr - 후보 부트스트랩 라우터 (후보 BSR) | |
| **admin-scope** | admin-scope - PIM-SM 관리자의 범위 | |
| **global** | global - 글로벌 범위 | 224.0.0.0/240.0.0.0 |
| *gaddr* | gaddr - sz 그룹 주소 (group address) | 239.0.0.0 to 239.255.255.255 |
| *gmask* | gmask - sz 그룹 마스크 (group mask) | |
| ***hash-length*** | 〈0-32〉 RP 선택을 위한 해시 마스크 길이 | |
| ***Priority*** | 〈0-255〉 후보 부트스트랩 라우터의 우선순위 값 | |

**(3) 기본값**

전역 도메인은 224.0.0.0/4 입니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

이 명령은 관리 도메인 내에서 후보 BSR 을 설정하는 데 사용됩니다. 이 명령은 도메인 경계에서의 admin-scope 명령에 해당하며 관리 도메인의 범위를 지정하는 데 사용됩니다.

참조:
c-bsr intf_type intf_name 명령이 설정되지 않은 경우, 이 명령은 효과가 없습니다.

이 명령은 관리 범위(239.0.0.0--239.255.255.255) 내에서 설정하는 것이 좋습니다.

**(6) 예제**

다음 예제는 C-BSR 이 관리 도메인 239.1.1.0/24 에서만 효과를 가지는 방법을 보여줍니다:
Router_config# router pim-sm
Router_config_ps#c-bsr f0/0 10 250
Router_config_ps#c-bsr admin-scope 239.1.1.1 255.255.255.0

**(7) 연관 명령어**

c-bsr intf_type intf_name [hash-length [priority]]

### 37.1.29. Bsm-policy

**(1) 구문**

BSM 수신 정책을 설정하려면, PIM-SM 구성 모드에서 아래 두 명령 중 첫 번째 명령을 실행합니다. 기본값 설정을 복원하려면 두 번째 명령을 실행합니다.

bsm-policy { unicast {rcvd | send}| forward-all | backward}
no bsm-policy { unicast {rcvd | send} | forward-all }

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **bsm** | bsm - BSM 패킷 수신 | |
| ***policy*** | Policy - BSM 수신 및 전달을 위한 정책 | |
| **unicast** | unicast - 유니캐스트 BSM 패킷 | 기본값은 유니캐스트 BSM 패킷의 수신을 허용합니다.<br>이전 버전 호환성은 유니캐스트 BSM 전송을 지원합니다. |
| rcvd | *rcvd*-BSM 메시지 수신 허용 | |
| ***forward-all*** | ***forward-all - 모든 BSM 패킷 전달*** | 수평 분할 포트는 유니캐스트 또는 "no-forward-bit" 리셋 패킷을 포함한 모든 BSM 패킷을 전달하지 않습니다 |
| ***backward*** | ***backward 이전 버전 호환성 지원, 유니캐스트 BSM 전송.*** | |

**(3) 기본값**

BSM 수신 또는 전송 정책은 설정되지 않습니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

이명령어의 설명을 참조.

**(6) 예제**

다음 예제는 로컬 라우터가 이웃으로부터 유니캐스트된 BSM 을 수신할 수 있도록 설정하는 방법을 보여줍니다:
Router_config# router pim-sm
Router_config_ps# bsm-policy unicast rcvd

**(7) 연관 명령어**

없음

### 37.1.30. static-rp

#### (1) 구문

PIM-SM 의 정적 RP 를 설정하려면 아래 두 명령 중 첫 번째 명령을 실행합니다. 기본값 설정을 복원하려면 두 번째 명령을 실행합니다.

static-rp rp-addr [std-acl] [override] [bidir]
no static-rp rp-addr

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **static** | static - PIM-SM 의 정적 RP 주소 설정 | |
| **rp-addr** | A.B.C.D - PIM-SM RP 주소 (Rendezvous Point) | |
| *std-acl* | WORD - IP 표준 액세스 리스트 | |
| **override** | override - 충돌 발생 시, 정적 RP 가 동적 RP 보다 우선됨 | 정적 RP 가 동적 RP 와 충돌할 경우, 매개변수가 지정되지 않으면 동적 RP 가 우선적으로 선택됩니다. 동적 RP 가 존재하지 않거나 동적 RP 가 적용되지 않는 경우에만 정적 RP 가 적용됩니다 |
| **bidir** | bidir - 그룹 범위를 양방향 공유 트리 모드로 처리 | 현재는 지원되지 않습니다 |

#### (3) 기본값

비활성화

#### (4) 명령어 모드

PIM-SM 전역 뷰

#### (5) 사용 지침

정적 RP 의 지정 IP 주소는 합법적인 유니캐스트 주소여야 하며 루프백 주소(127.0.0.0/8)일 수 없습니다. 액세스 목록(ACL)이 지정되면, 구성된 정적 RP 는 일치하는 멀티캐스트 그룹을 제공합니다. ACL 이 지정되지 않으면, 구성된 정적 RP 는 모든

멀티캐스트 그룹(224.0.0.0/4)을 제공합니다. 정적 RP 가 동적 RP 와 충돌할 경우, override 옵션을 지정하면 정적 RP 가 우선적으로 선택됩니다.

PIM-SM 또는 BIDIR 모드에서는 각 그룹에 RP 가 제공됩니다. 동일한 관리 도메인 내의 모든 라우터는 그룹에 대해 동일한 규칙을 따라야 합니다. RP 는 정적 RP 주소 설정 또는 BSR 메커니즘을 통한 동적 학습 두 가지 방법으로 얻을 수 있습니다. static-rp 명령어를 사용하여 RP 를 여러 그룹의 집계 지점으로 설정할 수 있습니다. 정적 RP 에 의해 구성된 ACL 은 RP 적용 범위를 정의합니다. 표준 ACL 이 설정되지 않으면, 지정된 정적 RP 는 모든 그룹에 적용됩니다. 하나의 PIM 라우터는 여러 개의 RP 를 사용할 수 있지만, 특정 그룹에 대해서는 하나의 RP 만 사용할 수 있습니다.

**여러 개의 static-rp 명령어가 설정된 경우, 그룹과 RP 간의 매칭 규칙은 다음과 같습니다:**

그룹이 여러 개의 정적 RP 규칙과 일치하는 경우, 표준 ACL 에 지정된 가장 긴 일치 원칙을 따라 적절한 RP 를 선택할 수 있습니다. ACL 이 지정되지 않은 정적 구성의 경우 모든 그룹에 적용될 수 있지만, ACL 내의 항목이 먼저 설정되어야 합니다.

그룹이 여러 개의 ACL 과 일치하고 가장 긴 매칭 원칙을 따르는 경우, RP 의 IP 주소를 비교하여 더 큰 IP 주소를 가진 RP 가 우선적으로 선택됩니다.

정적 RP 구성을 사용하는 경우, 지정된 RP 에 대한 도달 가능성 테스트는 수행되지 않습니다. RP 가 선택되면, 해당 RP 의 경로가 로컬에 존재하지 않더라도 상대적으로 낮은 RP 는 선택되지 않습니다.

각 명령어는 하나의 정적 RP 주소를 지정하는 데 사용됩니다. 구성 중에 동일한 정적 RP 주소 또는 ACL 규칙이 지정되면, 새로운 설정이 기존 설정을 대체합니다.

**정적 RP 와 동적 RP 가 함께 사용되는 경우, 그룹과 RP 간의 매칭 규칙은 다음과 같습니다:**

override 가 지정되지 않은 경우, BSR 메커니즘을 통해 동적으로 학습된 RP 가 정적 RP 보다 우선합니다.

동적 RP 를 사용하는 경우, c-rp intf_type intf_name 명령어를 설정해야 합니다.

참조:
동일한 RP 는 BIDIR 및 PIM-SM 에서 동시에 사용할 수 없습니다.
정적으로 구성된 RP 는 글로벌 SZ 만 지원하며, 글로벌 SZ 가 생성되지 않았더라도 지원을 제공합니다.

**(6) 예제**

다음 예제는 198.92.37.33 을 정적 RP 주소로 지정하는 방법을 보여줍니다.

Router_config#router pim-sm
Router_config_ps#static-rp 198.92.37.33

**(7) 연관 명령어**

c-rp intf_type intf_name

### 37.1.31. C-rp intf_type intf_name

**(1) 구문**

PIM-SM 도메인에서 지정된 BSR 라우터로 유니캐스트 알림을 주기적으로 전송하는 C-RP 포트를 설정하려면 다음 두 명령 중 첫 번째 명령을 실행하십시오. 기본값으로 복원하려면 두 번째 명령을 실행하십시오.

c-rp intf-type intf-name [group-list std-acl] [bidir] [intvl seconds] [pri pri-value]
no c-rp intf-type intf-name

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **c-rp** | c-rp - PIMv2 RP 후보로 설정 | |
| ***intf-type intf-name*** | 인터페이스 유형 및 인터페이스 이름 지정 | C-RP 에서 PIM-SM 을 활성화해야 합니다. |
| **group-list** | group-list - 그룹 주소에 대한 표준 IP 액세스 목록 | 이는 그룹 주소의 프리픽스입니다. |
| ***std-acl*** | WORD 표준 IP 액세스 목록 | |
| **bidir** | bidir - 양방향 공유 트리 모드에서 그룹 범위를 처리 | 현재는 지원되지 않습니다. |
| **intvl** | Interval - RP 후보 광고 간격 | |
| seconds | 〈1-32767〉 - 초 | |
| **pri** | pri - RP 우선순위 | |
| *pri-value* | 〈0-255〉 - RP 우선순위 값 | 값이 작을수록 우선순위가 높아집니다. 기본값은 192 입니다. |

**(3) 기본값**

Dynamic RP 선택이 비활성화됨

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

이 명령어는 모든 BSR 에 C-RP 를 알리는 데 사용됩니다. 그룹 주소 범위는 표준 ACL 형식으로 나열됩니다.

참조:
C-RP 로 사용되는 포트에서 PIM-SM 이 활성화되어 있어야 합니다.

유사한 라우터나 필요 시 다이얼업 스텁 라우터에서 정적 설정을 방지하려면 주요 PIM-SM 도메인에서 C-RP 를 설정하는 것이 좋습니다.

멀티캐스트 그룹 범위가 지정되지 않으면 C-RP 는 모든 멀티캐스트 그룹을 지원합니다.

여러 그룹 범위에 대해 C-RP 를 설정하려면, STD-ACL 에서 group-list 에 해당하는 여러 규칙을 사용하여 여러 그룹 범위를 나타내야 합니다.

하나의 포트에는 하나의 C-RP 만 설정할 수 있으며, 이후의 설정은 이전 설정(포함된 STD-ACL 포함)을 덮어씁니다.

동일한 PIM-SM 라우터에서 여러 포트에 대해 C-RP 를 설정할 수 있습니다.

여러 C-RP 가 동일한 표준 ACL 을 사용할 수 있습니다.

동일한 인터페이스에서 이 명령어를 여러 번 실행하면 이전 설정이 덮어씌워집니다.

C-RP 에서 여러 SZ(서브존)를 인식하는 경우, 각 SZ 의 BSR 로 유니캐스트 C-RP-Adv 가 전송됩니다. 이때 설정된 그룹 범위가 대상 SZ 의 그룹 범위를 초과할 수 없습니다.

C-RP 자체가 특정 SZ 의 ZBR(존 경계 라우터)인 경우, C-RP-Adv 패킷의 Admin Scope Bit 가 재설정되어야 합니다. 그렇지 않으면 이 비트는 그대로 유지됩니다. 현재 이 기능은 BSR 이 로그를 기록하는 데 사용되며, 프로토콜 확장을 위해 활용될 가능성이 있습니다.

**(6) 예제**

다음 예제는 lo172 와 lo173 을 C-RP 포트로 지정하는 방법을 보여줍니다. lo172 는 239.1/16 프리픽스 그룹에 대해서만 RP 역할을 하도록 제한됩니다.

Router_config#router pim-sm
Router_config_ps# c-rp loopback172 group-list grp-range
Router_config# ip access-list standard grp-range
Router_config_std_nacl# permit 239.1.0.0 255.255.0.0
Router_config_ps# c-rp loopback173

**(7) 연관 명령어**

없음

### 37.1.32. intvl-time

**(1) 구문**

주기적인 Join/Prune 패킷 전송을 활성화하고 Hello, BSM 또는 C-RP-Adv 패킷을 주기적으로 전송하는 간격을 설정하려면 아래 두 명령어 중 하나를 실행합니다:

intvl-time { join-prune jp-intvl | hello hlo-intvl | c-bsr cbsr-intvl |crp-adv crp-intvl| spt-check [spt-intvl]}

no intvl-time {join-prune [jp-intvl] | hello [hlo-intvl] |c-bsr[cbsr-intvl]| crp-adv [crp-intvl] | spt-check [spt-intvl]}

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| **join-prune** | **join-prune** – PIM-SM 정규 Join/Prune 패킷의 주기적 전송 | |
| **jp-intvl** | 〈1-65535〉 – JP 타이머 값 | Join/Prune 패킷 전송 기본값 간격: 60 초. |
| **Hello** | hello – PIM-SM Hello 광고 전송 주기 | Hello 패킷 전송 간격을 설정함. |
| ***hlo-intvl*** | 〈1-65535〉 – Hello 타이머 값 | Hello 패킷 전송 기본값 간격: 30 초 |
| **c-bsr** | c-bsr – 후보 부트스트랩 라우터 (후보 BSR) | |

| | | |
|---|---|---|
| *cbsr-intvl* | 〈1-65535〉 C-BSR 타이머 값 | 자체 선택 패킷 전송 기본값 간격: 60 초 |
| **crp-adv** | crp-adv - PIM-SM C-RP-ADV 전송 주기 | C-RP-Adv 패킷 전송 간격을 설정함 |
| *crp-intvl* | 〈1-65535〉 - CRP 타이머 값 | Report 패킷 전송 기본값 간격: 60 초. |
| *spt-check* | Spt-check - SPT 전환 타이머 | |
| *spt-intvl* | 〈1-65535〉 - SPT 전환 질의 타이머 값 | |

**(3) 기본값**

위에 테이블을 참조

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

Join-prune 패킷의 holdtime 이 설정되지 않고 downstream 이웃에서 Join 패킷을 세 번의 JP 타임아웃 주기 동안 받지 못하면, 해당 downstream 은 multicast 항목에 대해 prune 상태로 전환됩니다. 기본값 holdtime 은 3 분입니다. 포트 구성 모드에서의 간격은 전역 모드에서의 join/prune 간격보다 우선 적용됩니다.

**(6) 예제**

다음 예제는 글로벌 pimsm 구성에서 join/prune 광고 간격 값을 30 으로 설정합니다:
Router_config#Router pim-sm
Router_config_ps#timer join-prune 30

**(7) 연관 명령어**

Holdtime

### 37.1.33. Holdtime

**(1) 구문**

PIM-SM 의 타임아웃 타이머 간격을 설정하려면 다음 두 명령어 중 첫 번째 명령어를 실행합니다. 기본값 설정으로 복원하려면 다른 명령어를 실행합니다.

holdtime {join-prune jp-hold | assert asrt-hold | c-bsr cbsr-hold | crp-adv crp-hold | sz sz-hold}

no holdtime {join-prune [jp-hold] | assert [asrt-hold] | c-bsr [cbsr-hold] | crp-adv [crp-hold] | sz [sz-hold]}

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| holdtime | holdtime - 상태 유지용 hold 타이머 | |
| join-prune | Join-prune - join-prune 상태 hold 타이머 | |
| jp-hold | 〈1-65535〉 - 시간 값 (초) | 기본값은 210 초입니다. |
| assert | assert - assert 상태 hold 타이머 | |
| asrt-hold | 〈7-65535〉 - 시간 값 (초) | 기본값은 180 초입니다. |
| c-bsr | c-bsr - 후보 부트스트랩 라우터 (candidate BSR) | |
| cbsr-hold | 〈1-65535〉 - 시간 값 (초) | 기본값은 다음과 같습니다: holdtime 타임아웃 시간 = holdtime 간격 * 2 + 10. 기본적으로 holdtime 의 간격은 60 초이며, holdtime 의 타임아웃 시간은 130 초입니다. |
| c-rp | c-rp - 후보 RP (candidate RP) | |
| crp-hold | 〈1-65535〉 - 시간 값 (초) | 기본값은 150 초입니다. BSR 가 holdtime 패킷을 통해 타임아웃 시간을 업데이트하므로, C-RP 의 타임아웃 시간은 holdtime 패킷 전송 간격보다 적어서는 안 됩니다. 이상적으로는 2.5 간격 이상이 좋습니다. |
| sz | sz - 스코프 영역 타이머 | |
| sz-hold | 〈10-4294967295〉 - 시간 값 (초) | 기본값은 1300 초입니다. |

**(3) 기본값**

위에 테이블을 참조

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

포트에서 holdtime 이 설정된 경우, 먼저 해당 포트의 구성이 적용되고, 그 다음에 전역 구성이 적용됩니다. 만약 둘 다 설정되지 않으면 기본값 구성이 선택됩니다.

참조:
C-RP 의 holdtime 을 구성할 때, C-RP 의 타임아웃 시간을 2.5 holdtime 전송 간격 이상으로 설정하여 BSR holdtime 패킷에서 C-RP 가 손실되지 않도록 해야 합니다.

SZ 의 타임아웃 시간은 BSR 의 타임아웃 시간보다 길어야 하며, BSR 타임아웃 시간의 10 배로 설정하는 것이 좋습니다.

**(6) 예제**

다음 예제는 C-RP 의 holdtime 을 200 초로 설정하는 방법을 보여줍니다. 여기서 C-RP 와 C-BSR 은 Ra 에서 설정되지 않았습니다.

Ra_config# router pim-sm
Ra_config_ps# holdtime c-rp 200

**(7) 연관 명령어**

Intvl-time

### 37.1.34. Log

**(1) 구문**

DR 의 변경, 이웃의 상태 업/다운, 주소 충돌, 비정상 패킷을 기록하기 위해 로그 스위치를 활성화하려면 다음 두 명령어 중 첫 번째 명령어를 실행합니다:
log { nbr-change | ipaddr-conflict | pkt-conflict }
no log { nbr-change | ipaddr-conflict | pkt-conflict }

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| Log | log - 충돌을 기록하기 위해 사용 | |

| | | |
|---|---|---|
| nbr-change | nbr-change - 이웃 상태 업/다운 또는 DR 변경 | |
| ipaddr-conflict | ipaddr-conflict - 보조 IP 주소가 다른 이웃과 충돌 | |
| pkt-conflict | pkt-conflict - pim-sm mroute 항목이 pimsm 패킷에서 충돌 | |

**(3) 기본값**

로그 기능은 비활성화되어 있습니다.

**(4) 명령어 모드**

PIM-SM 전역 뷰

**(5) 사용 지침**

로그 서버가 있을 경우, 해당 로그는 로그 서버에 기록됩니다.

**(6) 예제**

다음 예제는 보조 IP 주소가 다른 이웃으로부터 수신된 Hello 패킷에 포함된 경우, 충돌을 기록하도록 라우터를 구성하는 방법을 보여줍니다.

Router_config_ps# log ipaddr-conflict

**(7) 연관 명령어**

없음

### 37.1.35. clear ip pim-sm rp-mapping

**(1) 구문**

PIM-SM RP 매핑 테이블 정보를 지우려면 다음 명령어를 실행합니다.

clear ip pim-sm rp-mapping [A.B.C.D]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | pim-sm - PIM sparse mode | PIM sparse 모드에서 사용하는 멀티캐스트 라우팅 프로토콜 |

| | | |
|---|---|---|
| pim-sm | pim-sm - PIM multicast routing protocol in sparse mode | PIM sparse 모드에서 멀티캐스트 라우팅 프로토콜로 사용 |
| rp-mapping | rp-mapping - BSR 에 의해 RP 매핑 테이블을 지웁니다 | BSR 을 통해 RP 매핑 테이블을 삭제 |

**(3) 기본값**

없음

**(4) 명령어 모드**

관리모드

**(5) 사용 지침**

이 명령어는 RP 매핑 테이블을 지우는 데 사용됩니다.

**(6) 예제**

없음

### 37.1.36. clear ip mroute pim-sm

**(1) 구문**

IP 멀티캐스트 라우트 pim-sm 을 지우려면 다음 명령어를 실행합니다.

clear ip mroute pim-sm *
clear ip mroute pim-sm gaddr [saddr]

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | pim-sm - PIM sparse mode | PIM sparse 모드에서 사용하는 멀티캐스트 라우팅 프로토콜 |
| pim-sm | pim-sm - multicast routing protocol of PIM sparse mode | PIM sparse 모드의 멀티캐스트 라우팅 프로토콜 |
| * | * - 모든 PIM-SM 멀티캐스트 라우트를 삭제 | 모든 PIM-SM 멀티캐스트 라우트를 삭제 |
| gaddr | A.B.C.D - 관련된 그룹 멀티캐스트 라우트 삭제 | 관련된 그룹 멀티캐스트 라우트를 삭제 |

**(3) 기본값**

없음

**(4) 명령어 모드**

관리 모드

**(5) 사용 지침**

이 명령어는 ip 멀티캐스트 라우트 pim-sm 을 지우는 데 사용됩니다.

**(6) 예제**

없음

### 37.1.37. show running-configure

**(1) 구문**

전역 PIM-SM 정보와 포트에 대한 주요 구성 정보를 표시하려면 다음 명령어를 실행합니다: show running-configure

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

출력된 정보를 통해 현재 PIM-SM 에 대한 구성 정보를 확인할 수 있습니다.

**(6) 예제**

없음

### 37.1.38. show ip pim-sm bsr-router

**(1) 구문**

show ip pim-sm bsr

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

관리 모드

**(5) 사용 지침**

PIM-SM 라우터 BSR 메시지를 표시합니다.

**(6) 예제**

```
R142#show ip pim-sm bsr-router
PIMv2 BSR information:
I am BSR!
  Address of BSR: 192.166.100.142
  BSR Priority: 201 Hash Mask Length: 30 Uptime: 00:10:56
  Next BSM will be sent in 00:00:04
Candidate-RP: 192.166.100.142(Loopback0)
  Interval of Advertisements: 60 초
  Next Advertisement will be sent in 00:00:04
```

**(7) 연관 명령어**

없음

### 37.1.39. show ip pim-sm sz-info

#### (1) 구문

PIM-SM SZ 정보를 표시하려면, SZ 의 범위, SZ 내의 BSM 패킷 수, SZ 초과 시간, 그리고 iif 인터페이스에서 BSM 이 전달되는 남은 시간을 포함한 정보를 확인할 수 있습니다.

show ip pim-sm sz-info

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | pim-sm -- PIM Sparse mode | pim-sm -- PIM Sparse 모드 |
| sz-info | sz-info -- PIM-SM sz 정보를 표시 | sz-info -- PIM-SM sz 정보를 표시 |

#### (3) 기본값

없음

#### (4) 명령어 모드

사용자 모드를 제외한 다른 모드

#### (5) 사용 지침

이 명령어는 PIM-SM SZ 정보를 표시하는 데 사용됩니다.

#### (6) 예제

명령어 show ip pim-sm sz-info 의 출력 예시:
switch#show ip pim-sm sz-info
PIMv2 administor scope information:
sz range: 224.0.0.0/4
 group range numbers:1
 BSM pkt numbers:0, in current forward queue
 szt not create,for we are c-bsr or BST not expire for no-cbsr
switch #

Definitions of domains above:

| 이름 | **설명** |
|---|---|

| | |
|---|---|
| sz range | SZ 범위 |
| group range numbers | SZ 내 그룹 범위 번호 |

### 37.1.40. show ip pim-sm interface

#### (1) 구문

show ip pim-sm interface [type number]

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| type | 포트 유형 |
| number | 포트 번호 |

#### (3) 기본값

없음

#### (4) 명령어 모드

관리 모드

#### (5) 사용 지침

PIM-SM 라우터 포트 정보를 표시합니다.

#### (6) 예제

```
R142#show ip pim-sm interface
Address       Interface  Ver/   Nbr   Query   DR     DR
                         Mode   Count Intvl   Prior
192.168.21.142  Serial2/0  v2/S   1     30      1     192.168.21.144
192.168.100.142 Ethernet1/1 v2/S   1     30     100    192.168.100.142
192.166.100.142 Loopback0  v2/S   0     30      1     192.166.100.142
```

#### (7) 연관 명령어

없음

### 37.1.41. show ip pim-sm neighbor

#### (1) 구문

show ip pim-sm neighbor [type number]

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| type | 포트 유형 |
| number | 포트 번호 |

#### (3) 기본값

없음

#### (4) 명령어 모드

관리 모드

#### (5) 사용 지침

PIM-SM 라우터 이웃 정보를 표시합니다.

#### (6) 예제

```
R142#show ip pim-sm neighbor
PIM Neighbor Table
Neighbor        Interface    Uptime/Expires     Ver    DR
Address                                         Prio
192.168.21.144    Serial2/0    00:03:53/00:01:22    v2    1
192.168.100.143   Ethernet1/1  00:03:34/00:01:41    v2    1
```

#### (7) 연관 명령어

없음

### 37.1.42. show ip pim-sm rp

#### (1) 구문

show ip pim-sm rp [mapping|metric]

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| mapping | RP-GROUP 매핑 관계를 표시 |
| metric | 각 RP 의 단순 캐스트 라우트 메트릭을 표시 |

**(3) 기본값**

없음

**(4) 명령어 모드**

관리 모드

**(5) 사용 지침**

PIM-SM 라우터 RP 매핑 정보를 표시합니다.

**(6) 예제**

R144#show ip pim-sm rp
GROUP: 225.1.1.10, RP: 9.1.1.1, Version2 Uptime: 1d01h07m, Expires in 00:02:16

**(7) 연관 명령어**

없음

### 37.1.43. show ip pim-sm rp-hash

**(1) 구문**

**show ip pim-sm rp-hash** [*group-address*]

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| group-address | 그룹 주소 |

**(3) 기본값**

없음

**(4) 명령어 모드**

관리 모드

**(5) 사용 지침**

지정된 멀티캐스트 주소의 해시 값을 표시합니다.

**(6) 예제**

```
R142#show ip pim-sm rp-hash 225.1.1.10
 RP: 192.166.100.142
 Info Source: 192.166.100.142, via BSR
 Uptime: 00:00:08, Expires: 00:02:22
```

### 37.1.44. show ip pim-sm anycast-rp

**(1) 구문**

현재 anycast-rp 정보를 표시하려면, 다음 명령어를 실행하십시오.
**show ip pim-sm anycast-rp**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | pim-sm -- PIM Sparse 모드 | pim-sm -- PIM Sparse 모드 |
| anycast-rp | anycast-rp -- anycast-rp 의 등록 패킷 수신 및 전송을 표시 | anycast-rp -- anycast-rp 의 등록 패킷 수신 및 전송을 표시 |

**(3) 기본값**

없음

**(4) 명령어 모드**

사용자 모드를 제외한 다른 모드

**(5) 사용 지침**

이 명령어는 로컬 anycast-rp 가 등록 패킷을 수신 및 전송하는 상태를 표시하는 데 사용됩니다.

**(6) 예제**

show ip pim-sm anycast-rp 명령어의 출력 예시 (그룹 239.1.1.1 에 대한 예시):

switch# show ip pim-sm anycast-rp
anycast-rp 2.2.2.2 nbr 192.168.18.1 status: REG_SEND

| 매개변수 | 설명 |
|---|---|
| anycast-rp | 2.2.2.2 는 anycast-rp 의 주소입니다. |
| nbr | 192.168.18.1 은 이웃 주소입니다. |
| status: REG_SEND | 이웃에게 등록 패킷을 전송 중입니다. |

### 37.1.45. show ip pim-sm protocol

**(1) 구문**

PIM-SM 프로토콜과 관련된 중요한 정보를 표시하려면 다음 명령어를 실행하십시오.
show ip pim-sm protocol

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | pim-sm -- PIM Sparse 모드 | pim-sm -- PIM Sparse 모드 |
| protocol | protocol -- 프로토콜 독립 멀티캐스트 프로토콜 Sparse 모드 | 프로토콜 독립 멀티캐스트 프로토콜 Sparse 모드 |

**(3) 기본값**

없음

**(4) 명령어 모드**

사용자 모드를 제외한 다른 모드

**(5) 사용 지침**

이 명령어는 PIM-SM 프로토콜의 현재 상태, 포트 번호, 이웃 번호, 수신된 패킷 수 및 BSM 구성의 인터벌 정보를 표시합니다.

**(6) 예제**

예제는 show ip pim-sm protocol 을 보여준다:

```
switch# show ip pim-sm protocol
PIM-SM is active
pim-sm interface number:3
pim-sm neighbor number:1
pim-sm receive pkt num:133; bad pkt num:0
PIM-SM current glb jp_intvl: 60(s)
PIM-SM current glb hello intvl: 30(s)
PIM-SM current glb BSM update timer intvl: 60(s)
PIM-SM current glb crp_intvl: 60(s)
PIM-SM current glb spt_intvl: 2(s)
PIM-SM BSM hold timeout: 130(s)
```

### 37.1.46. show ip mroute pim-sm

**(1) 구문**

**show ip mroute pim-sm** *[group-address|source-address]* **[type** *number***] [summary|count] [active** *kbps***]**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| group-address | 그룹 주소 |
| source-address | 소스 주소 |
| type | 포트 유형 |
| number | 포트 번호 |
| summary | PIM-SM 항목 요약 표시 |
| count | (S, G) 통계 정보 표시 |
| active | 활동 중인 데이터 전송 속도 |

**(3) 기본값**

없음

**(4) 명령어 모드**

관리 모드

**(5) 사용 지침**

PIM-SM 멀티캐스트 라우트 정보를 표시합니다.

**(6) 예제**

```
R142#show ip mroute pim-sm
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir group, s - SSM group,
I - IGMP report, R - RP-bit set, F - Register flag, T - SPT-bit set,
J - Join Needed, P - Pruned,
Timers: Uptime/Expires
(*, 225.1.1.10), 00:15:14/00:02:37, RP 9.1.1.1, flags: SRJ
Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143
Outgoing interface list:
Serial2/0, Forward/Sparse, 00:13:23/00:02:37
(192.166.1.253, 225.1.1.10), 00:15:14/00:02:46, flags: STJ
Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143
Outgoing interface list:
Serial2/0, Forward/Sparse, 00:15:14/00:02:46
(192.168.20.141, 225.1.1.10), 00:15:14/00:02:46, flags: STJ
Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143
Outgoing interface list:
Serial2/0, Forward/Sparse, 00:15:14/00:02:46
```

**(7) 연관 명령어**

없음

### 37.1.47. show ip rpf pim-sm

**(1) 구문**

**show ip rpf pim-sm {*source-address*} metric**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| source-address | 소스 주소 |
| metric | 단순 캐스트 라우트 메트릭 |

**(3) 기본값**

없음

**(4) 명령어 모드**

관리 모드

**(5) 사용 지침**

지정된 소스 주소에 대한 역방향 전달 정보를 표시합니다.

**(6) 예제**

R142#show ip rpf pim-sm 192.166.1.143
RPF information for 192.166.1.143
RPF interface: Ethernet1/1
RPF neighbor: 192.168.100.143
RPF route/mask: 192.166.1.0/24
RPF type: unicast (rip)
RPF recursion count: 0
Doing distance-preferred lookups across tables

**(7) 연관 명령어**

없음

### 37.1.48. debug ip pim-sm alert

**(1) 구문**

mrouting 또는 IP 에서 경고 정보를 표시하려면, 아래 두 명령 중 첫 번째 명령을 실행하십시오.

**debug ip pim-sm alert**
**no debug ip pim-sm alert**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

Mrouting 또는 노후화된 알림 정보가 있는 경우 VTY 를 내보냅니다(s,g).

**(6) 예제**

다음 예제는 RIP 의 라우트 이벤트가 모니터링되는 방법을 보여줍니다.

router# debug ip rip database
RIP-DB: Adding summary route 192.1.1.0/24 〈metric 0〉 to RIP database
The fields in the previous 예제 are explained in the following table:

| 매개변수 | 설명 |
|---|---|
| summary | 라우팅 테이블에 추가된 라우트 유형 |
| 192.1.1.0/24 | 라우팅 테이블에 추가된 라우트 |
| 〈metric 0〉 | 라우트의 메트릭 값 |

### 37.1.49. debug ip pim-sm assert

**(1) 구문**

PIM-SM 의 Assert 이벤트를 모니터링하려면 다음 두 명령 중 첫 번째 명령을 실행하십시오:
**debug ip pim-sm assert** [packet | state-machine | A.B.C.D ]

**no debug ip pim-sm assert [packet | state-machine | A.B.C.D ]**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| state-machine | 상태 기계 활동 표시 | |
| packet | 패킷 추적 정보 | |
| A.B.C.D | STM 및 패킷 출력을 위한 그룹 주소 | |

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

출력 정보를 통해 PIM-SM 의 현재 Assert 이벤트를 확인할 수 있습니다.

**(6) 결과**

(S,G) Assert 상태 기계 동작 표시
(*,G) Assert 메시지 상태 기계 동작 표시
타이머 만료 후 활동 표시
패킷 활동 표시

### 37.1.50. debug ip pim-sm bsr

**(1) 구문**

PIM-SM 의 BSM 이벤트, C-RP-ADV 이벤트 또는 BSR 상태 기계를 모니터링하려면, 아래 명령 중 첫 번째 명령을 실행합니다:
**debug ip pim-sm bsr [packet | state-machine]**
**no debug ip pim-sm bsr [packet | state-machine]**

**(2) 매개변수**

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| state-machine | Show state machine activity debug information | 상태 기계 활동 디버그 정보를 표시 |

| | | |
|---|---|---|
| packet | Trace information about packet | 패킷에 대한 정보를 추적 |

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

출력 정보를 통해 PIM-SM 의 BSM 이벤트, C-RP-ADV 이벤트 또는 BSR 상태 기계를 확인할 수 있습니다.

### 37.1.51. debug ip pim-sm rp

**(1) 구문**

PIM-SM-RP-SET 변경에 관한 관련 이벤트와 패킷을 모니터링하려면 다음 두 명령 중 첫 번째 명령을 실행합니다:
**debug ip pim-sm rp**
**no debug ip pim-sm rp**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

이 명령은 C-RP-ADV 수신 및 전송과 RP-SET 변경을 내보내는 데 사용됩니다. 정적 RP 의 변경에 대해서는 현재 디버깅 정보가 내보내지지 않습니다.

### 37.1.52. debug ip pim-sm entry

**(1) 구문**

(,,rp), (*,g), (s,g,rpt), (s,g,spt)의 생성 및 업데이트와 RP 변경 시 이들의 동시 변경을 내보내려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm entry**
**no debug ip pim-sm entry**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

출력 정보를 통해 PIM-SM 멀티캐스트 라우팅 항목의 생성 및 업데이트 정보를 확인할 수 있습니다.

### 37.1.53. debug ip pim-sm event

**(1) 구문**

PIM-SM 의 주요 작업이 수신하는 모든 이벤트를 내보내려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm event**
**no debug ip pim-sm event**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

출력 정보를 통해 현재 PIM-SM 의 모든 이벤트를 확인할 수 있습니다.

### 37.1.54. debug ip pim-sm hello

#### (1) 구문

PIM-SM 이 수신하거나 전송한 Hello 패킷을 표시하여 이웃 정보를 디버깅하려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm hello**
**no debug ip pim-sm hello**

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| pim-sm | Show state machine activity debug information | 상태 기계 활동 디버그 정보 표시 |
| hello | Show information about packet sending and receiving | 패킷 송수신 정보 표시 |

#### (3) 기본값

없음

#### (4) 명령어 모드

EXEC

#### (5) 사용 지침

출력 정보를 통해 PIM-SM 이 수신하거나 전송한 Hello 패킷을 확인할 수 있으며, 로컬 머신이나 이웃에서 발생한 내용을 알 수 있습니다.

#### (6) 결과

현재 수신하거나 전송된 Hello 패킷의 포트, 소스 주소 및 genid 를 표시할 수 있습니다.

### 37.1.55. debug ip pim-sm jp

#### (1) 구문

(*,g) 또는 (s,g)의 Join/Prune 이벤트를 추적하려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm jp [**packet | state-machine | A.B.C.D **]**
**no debug ip pim-sm jp [**packet | state-machine | A.B.C.D **]**

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| state-machine | Show state machine activity debug information | 상태 기계 활동 디버깅 정보 표시 |
| packet | Trace information about packet | 패킷 정보 추적 |
| A.B.C.D | Group address for stm and packet output | stm 및 패킷 출력을 위한 그룹 주소 |

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

없음

### 37.1.56. debug ip pim-sm nbr

**(1) 구문**

이웃과 관련된 이벤트(이웃 추가, 시간 초과 삭제 또는 DR 선택 등)를 추적하려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm nbr**
**no debug ip pim-sm nbr**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

이 명령의 출력 정보를 통해 이웃 변경, 이웃 새로 고침, GENID 변경 및 DR 선택을 확인할 수 있습니다.

### 37.1.57. debug ip pim-sm packet

#### (1) 구문

PIM-SM 이 수신하거나 전송한 프로토콜 제어 패킷을 추적하려면 다음 명령을 실행합니다.

**debug ip pim-sm packet**

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 명령어 모드

EXEC

#### (5) 사용 지침

이 명령을 실행한 후 PIM-SM 패킷의 유형을 표시합니다.

### 37.1.58. debug ip pim-sm register

#### (1) 구문

PIM-SM 의 등록 패킷 및 등록 상태 이벤트를 표시하려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm register** [packet | state-machine | A.B.C.D ]
**no debug ip pim-sm register** [packet | state-machine | A.B.C.D ]

#### (2) 매개변수

| 이름 | 영어 프롬프트 | 주석 |
|---|---|---|
| state-machine | Show state machine activity debug information | 상태 기계 활동 디버깅 정보 표시 |
| packet | Trace information about packet | 패킷 정보 추적 |
| A.B.C.D | Group address for stm and packet output | stm 및 패킷 출력을 위한 그룹 주소 |

#### (3) 기본값

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

출력 정보를 통해 PIM-SM 의 등록 이벤트를 확인할 수 있습니다.

### 37.1.59. debug ip pim-sm timer

**(1) 구문**

모든 PIM-SM 타이머의 변경 사항(생성, 삭제, 정지 및 시간 초과 등)을 표시하려면 다음 두 명령 중 첫 번째 명령을 실행합니다.

**debug ip pim-sm timer**
**no debug ip pim-sm timer**

**(2) 매개변수**

없음

**(3) 기본값**

없음

**(4) 명령어 모드**

EXEC

**(5) 사용 지침**

PIM-SM 타이머에는 Hello 타이머, 이웃 시간 초과 타이머, Join/Prune 타이머, 오버라이드 타이머, 프룬 대기 타이머, Keepalive 타이머, 어설트 타이머, 등록 타이머, 등록 제한 타이머, BSM 타이머 등이 포함됩니다.

# 38. QoS 구성

## 38.1. 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 0 과 7 이 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 포함된 우선 순위 정보에 따라 다른 서비스를 제공합니다. peer-to-peer (P2P) QoS 서비스가 실현됩니다.

또한 네트워크를 구성하여 특정 메시지로 전환할 수 있습니다. 동작은 하나의 홉으로 불리는 동작으로 수행됩니다.

스위치의 QoS 기능은 네트워크 대역폭을 효과적으로 만들어 성능을 향상시킵니다.

## 38.2. P2P QoS 모델

P2P QoS 서비스 모델은 다른 Peer to Peer 메시지를 전송할 수 있습니다. QoS 소프트웨어는 최선의 서비스(Best-effort service)와 차별화 서비스(differentiated service)의 두 가지 유형의 서비스 모델을 지원합니다.

**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. Best-effort 서비스 모델에서 스위치의 QoS 기능은 "선착순" 주문을 준수합니다.

**Differentiated 서비스**
차별화된 서비스의 경우 서비스가 특수한 경우 각 패킷에 해당 QoS 레이블을 지정해야 합니다. 지정된 다른 모드로 구체화될 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 차별화된 서비스를 전송할 수 있습니다.

## 38.3. 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.

**엄격한 우선순위**
최우선 원칙은 존재하지 않습니다. 큐 알고리즘은 우선 순위가 높은 플로우에 대해 더 나은 서비스를 제공합니다. 단점은 우선 순위가 낮은 흐름입니다.

**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 WRR 알고리즘은 우선 순위가 낮은 대기열로 바뀌고 서비스를 제공합니다.

**선착순(첫번째로 온 것이 첫번째로 서비스 받는다.)**
FCFS 알고리즘은 메시지를 전달하는 순서를 엄격하게 따르고 메시지에 서비스가 제공됩니다.

# 39. QoS 구성 업무

일반적으로 스위치는 모든 메시지를 전달하기 위해 최선을 다합니다. 정체가 발생하면 모든 메시지가 삭제될 수 있습니다. 실제로, 다른 메시지는 다른 중요성을 가지고 있습니다. 중요한 메시지는 더 나은 서비스와 함께 제공되어야 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 대기열에 대한 일정 정책 구성
- CoS 우선 순위 대기열에 대한 일정 표준 구성
- 포트의 기본 CoS 값 구성
- QoS 정책 매핑 구성
- QoS 정책 매핑 설명 구성
- QoS 정책 매핑의 일치된 데이터 흐름 구성
- QoS 정책 매핑의 일치된 데이터 흐름에 대한 작업 구성
- 포트에 QoS 정책 적용
- QoS 정책 매핑 테이블 표시
- 포트 유량 제한 구성

## 39.1. QoS 작업 구성하기

### 39.1.1. 전역 우선순위 Queue 구성하기

QoS 우선 순위 큐를 구성하는 것은 IEEE802.1p 에 정의된 8 개의 CoS 값을 우선 순위 큐에 매핑하는 것입니다. 스위치에는 8 개의 우선 순위 대기열이 있습니다. 스위치는 다른 대기열에 따라 해당 정책을 채택하고 QoS 서비스를 실현합니다.

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.

| 명령 | 설명 |
|---|---|

| | |
|---|---|
| **Configure** | 전역 구성모드로 들어갑니다. |
| **[no] cos map quid cos1..cosn (0-7)** | COS 우선순위 큐를 구성합니다.<br>**quid** 는 COS 우선순위의 ID 입니다.<br>**cos1..cosn** 는 IEEE802.1p 에 정의 된 cos 값입니다. |
| **Exit** | 관리 모드로 돌아갑니다. |
| **Write** | 구성을 저장합니다. |

### 39.1.2. CoS 우선 순위 대기열에 대한 일정 계획 정책 구성

스위치의 각 포트에는 여러 개의 출력 대기열이 있습니다. 이 스위치에는 8 개의 우선 순위 대기열이 있습니다. 다음을 사용하여 출력 대기열을 예약이 가능합니다.

- SP (Strict 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.

| **명령** | **설명** |
|---|---|
| **configure** | 전역 구성 모드를 시작하십시오. |
| [no] **scheduler policy** {sp \| **wrr** \| **wfq**\| **fcfs** } | QoS 우선 순위 대기열에 대한 일정 정책을 구성합니다. |
| **Exit** | 관리 모드로 돌아갑니다. |
| **Write** | 구성을 저장합니다. |

### 39.1.3. QoS 우선 순위 대기열에 대한 스케줄 표준 구성

COS 우선 순위 큐는 WRR 입니다. 스케줄에는 두 가지 유형이 있습니다.

- 패킷-카운트: 표현할 패킷의 수를 사용합니다.
- 대기 시간: 전송된 시간에 세그먼트를 사용하여 점유 대역폭을 나타냅니다.

일련의 스위치는 패킷 수만 지원합니다. 패킷 수는 기본 스케줄 표준입니다.
따라서 표준 스케줄 정책을 선택하라는 명령은 없습니다.

### 39.1.4. 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.

| 명령 | 설명 |
|---|---|
| **Configure** | 전역 구성 모드를 시작하십시오. |
| **interface g0/1** | 구성할 포트에 로그인합니다. |
| [**no**] **cos default** *cos* (**0~7**) | 레이블이 없는 프레임의 CoS 값을 구성하고 CoS 는 cos 값을 나타냅니다.<br>기본 값으로 cos (0~7) 구성이 가능합니다. |
| **Exit** | 전역 구성 모드로 돌아갑니다. |
| **Exit** | 관리 모드로 돌아갑니다. |
| **Write** | 구성을 저장합니다. |

### 39.1.5. 매핑 정책 구성하기

QoS 매핑 정책은 헤더에서 지정 작업을 구별하기에 특정 기능을 채택하는 것을 의미합니다. 하나의 규칙 만 사용하여 데이터 액세스의 IP 액세스 목록 및 MAC Access-list 를 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 있어야 합니다.

QoS 매핑 정책을 만들려면 권한 모드에서 다음 작업을 수행하십시오

| 명령 | 설명 |
|---|---|
| Configure | 전역 구성 모드를 시작합니다. |
| [no] policy-map name | QoS 정책 테이블 구성 모드를 시작합니다.<br>name 은 정책테이블의 이름을 나타냅니다. |
| description description-text | QoS 의 정책을 설명을 구성합니다.<br>description-text 는 설명입니다. |
| [**no**] **classify** {**ip access-group** *access-list-name* \| **dscp** *dscp-valu*e \| **mac access-group** *mac-access-name* \| **vlan** *vlan-id* \| **cos cos** \| **any**} | QoS 정책 표의 일치된 데이터 흐름을 구성합니다.<br>access-list-name 는 일치하는 IP Access list 의 이름입니다.<br>**dscp-value** 이란 IP 메시지에 다른 서비스를 의미합니다.<br>**mac-list-name** Mac 주소 리스트의 일치하는 주소 목록 이름이다.<br>**vlan-id** vlan 과 일치하는 ID 이다.<br>**cos** 는 일치하는 서비스 등급 값을 나타냅니다. |
| **action** {**bandwidth** *max-band* \| **cos** | 일치하는 데이터 흐름 정책을 구성합니다 |
| **cos-value** \| **dscp** *dscp-value* \| **redirect** *interface-id* \| **drop** \| **monitor**} | QoS 정책 테이블.<br>**max-band** 데이터흐름에 의해 최대 대역폭이 발생합니다, |

| | |
|---|---|
| | **cos-value** 일치된 서비스 등급을 cos-value 으로 구성하는 것을 의미합니다.<br>**dscp-value** 는 흐름의 맞춘 dscp 필드 dscp-value. 값을 매칭시킵니다.<br>**interface-id** 지향성에 맞춘 흐름의 종료를 나타냅니다.<br>**Drop** 드롭 메시지를 삭제합니다.<br>**Stat** 통계 정보를 나타냅니다.<br>**monitor** 패킷을 미러링 포트로 전송합니다. |
| Exit | 전역 구성모드로 돌아갑니다. |
| Exit | 관리모드로 돌아갑니다. |

### 39.1.6. QoS 정책 매핑 구성

권한 모드에서 다음 작업을 수행하여 QoS 정책 매핑에 대한 설명을 구성합니다

| **명령** | **설명** |
|---|---|
| **Configure** | 전역 구성 모드로 들어갑니다. |
| [**no**] **policy-map** *name* | QoS 정책 목록 구성 모드를 입력합니다.<br>name 정책 이름을 나타냅니다. |
| **description** description-text | Qos 정책 설명을 구성합니다.<br>description-text 는 정책을 설명하는 텍스트입니다. |
| **Exit** | 글로벌 구성 모드로 돌아갑니다. |
| **Exit** | 관리 모드로 돌아갑니다. |

### 39.1.7. QoS 매핑 정책의 일치하는 데이터 흐름 구성하기

QoS 데이터 흐름의 분류 규칙은 요구 사항에 따라 구성한 필터링 규칙입니다.
다음 작업을 일치하는 정책 데이터 흐름을 구성합니다.

| **명령** | **설명** |
|---|---|
| **configure** | 전역 구성 모드로 들어갑니다. |
| [**no**] **policy-map** *name* | QoS 정책 목록에 구성을 합니다.<br>Name 정책이름을 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 정책 표의 일치하는 데이터흐름을 구성합니다.<br>**Access-list-name** 일치하는 IP ac-list 이름입니다.<br>**Dscp-value** stands for the **diffserv** field in the IP message.<br>**Mac-list-name** 는 일치하는 MAC ac-list 이름입니다.<br>**Vlan-id** Vlan 아이디를 나타냅니다.<br>**Cos** 일치하는 서비스 등급 값입니다.<br>**Any** 임의 패킷을 일치는 방법입니다. |
| **Exit** | 전역 구성 모드로 돌아갑니다. |
| **Exit** | 관리 모드로 돌아갑니다. |

### 39.1.8. QoS 매핑 정책의 일치하는 데이터 흐름에 대한 작업 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 구성합니다.

| 명령 | 설명 |
|---|---|
| **configure** | 전역 구성 모드를 사용합니다. |
| [**no**] **policy-map** *name* | Qos 정책 구성 모드를 실행합니다.<br>Name 정책-맵의 이름을 나타냅니다. |
| **Action** {**bandwidth** *max-band* \| **cos** *cos-value* \| **dscp** *dscp-value* \| **vlanID** *vlanid-value* \| **redirect** *interface-id* \| **drop** \| [**stat-packet** \| **stat-byte**] \| **monitor**} | QoS 정책 표에 일치하는 데이터 흐름 정책을 구성합니다.<br>**Max-band**: 최대값을 나타냅니다.<br>**Cos-value** 흐름의 서비스 등급 필드를 cos-value 로 구성하는 것을 의미합니다.<br>**Dscp-value** 일치하는 흐름의 dscp 필드를 dscp-value로 구성하는 방법입니다.<br>**Vlanid-value** 일치된 흐름의 VLANID 필드를 vlanid-value 로 구성하는 것을 의미합니다.<br>**Interface-id** 방향성 일치 항목 흐름의 종료를 나타냅니다.<br>**Drop** 드롭 된 메시지를 나타냅니다.<br>**Stat-packet, Stat-byte** 스위치에 의해 수집된 통계 정보를 패킷 또는 바이트 단위로 나타냅니다.<br>**Monitor** 패킷을 미러링 포트에 전송하는것을 의미합니다. |
| **Exit** | 전역 구성 모드로 돌아갑니다. |
| **Exit** | 관리모드로 돌아갑니다. |

### 39.1.9. 포트에 QoS 정책을 적용하기

QOS 정책을 포트에 적용할 수 있습니다. 하나의 정책이 다중 포트에도 적용될 수 있습니다. 포트에 적용된 정책에는 우선 적용되는 정책이 최우선 순위를 차지합니다. 메시지가 동시에 두 가지 정책을 구성하고 구성 작업이 충돌하는 경우 먼저 일치 정책을 표준으로 취하십시오. 정책이 포트에 적용되면 스위치는 통과가 허용되지 않는 정책에 흐름을 추가합니다. 포트의 모든 정책이 삭제되면 스위치는 포트에서 기본값의 기본 정책을 자동으로 삭제합니다.

QoS 정책을 적용하려면 권한 모드에서 다음 작업을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **Configure** | 전역 구성 모드를 시작합니다. |
| **interface g0/1** | 구성할 포트에 로그인합니다. |
| [**no**] **qos policy** *name* {**ingress**\|**egress**} | 포트에 QoS 정책을 적용합니다.<br>**name** QoS 정책을 적용합니다.<br>**ingress** Qos 정책의 수신의 영향을 끼친다는 것을 의미합니다. |

| | |
|---|---|
| | **egress** Qos 정책이 발신에 영향을 끼친다는 것을 의미합니다. |
| **Exit** | 전역 구성 모드로 돌아갑니다. |
| **Exit** | 관리 모드로 돌아갑니다. |

#### 39.1.10. QoS 매핑 정책 테이블 표시

show QoS strategy 매핑 테이블을 실행할 수 있습니다.
QoS 정책 매핑 테이블을 표시하려면 권한 모드에서 다음 작업을 수행하십시오.

| 명령 | 설명 |
|---|---|
| **show policy-map** [*policy-map-name*] | 모든 또는 지정된 QoS 정책 매핑 테이블을 표시합니다.<br>**policy-map-name** 매핑 테이블의 이름을 나타냅니다. |

## 39.2. QoS 구성 예제

#### 39.2.1. 포트에 QoS 정책 예제 적용하기

포트에서 메시지의 COS 값을 2 로 변경하는 정책을 구성합니다. 그렇지 않으면 다른 정책을 적용해야 합니다. 모든 데이터 흐름을 통과할 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
```

# 40. DoS 공격 방지 구성

## 40.1. DoS 공격 개요

### 40.1.1. DoS 공격의 개념

DoS 공격은 서비스 거부 공격이라고도 합니다. 일반적인 DoS 공격에는 네트워크 대역폭 공격과 연결 공격이 포함됩니다. DoS 공격은 해커가 자주 발생시키는 네트워크 공격 모드입니다. 궁극적인 목적은 합법적 인 사용자에게 일반적인 네트워크 서비스를 제공하지 않으려 고 네트워크를 무너뜨리는 것입니다.

DoS 공격 방지는 Pingflood, SYNflood, Landattack, Teardrop 및 불법 플래그가 포함된 TCP 와 같은 공격을 막기위한 많은 공격 예방 방법을 제공하는 스위치가 필요합니다. 스위치가 공격받고 있을 때 어떤 공격 유형인지 판단해야 하며 이 공격 패킷을 특수하게 처리해야 합니다. (예: 스위치를 CPU 로 보내고 버리는 것)

**DoS 공격 유형**
해커는 다양한 유형의 DoS 공격 패킷을 만들어 서버를 공격합니다. 다음은 일반적인 DoS 공격 패킷입니다.

**Ping of Death**
Ping of Death 는 비정상 Ping 패킷으로, 크기가 ICMP 임계 값을 초과하며 TCP/IP 스택 및 최종적으로 수신 호스트의 고장이 발생한다고 주장합니다.

**TearDrop**
TearDrop 은 TCP/IP 스택의 신뢰할 수 있는 IP 조각의 패킷 헤더에 포함된 정보를 사용하여 공격을 실현합니다. IP 조각에는 원래 패킷의 어느 부분이 포함되어 있는지를 나타내는 정보가 포함되어 있으며 일부 TCP/IP 스택은 겹치는 오프셋이 포함된 가짜 조각을 수신하면 고장납니다.

**SYN Flood**
표준 TCP 연결에는 세 가지 손 - 쉐이크 프로세스가 필요합니다. 클라이언트는 SYN 메시지를 서버로 보내고 서버는 SYN-ACK 메시지를 반환하고 클라이언트는 SYN-ACK 메시지를받은 후 서버에 ACK 메시지를 보냅니다. 이러한 방식으로 TCP 연결이 구성됩니다. SYN flood 는 TCP 프로토콜 스택이 두 호스트 사이에서 손 - 쉐이크 절차를 초기화 할 때 DoS 공격을 트리거 합니다.

**Land Attack**
공격자는 특수 SYN 메시지를 만듭니다 (발신 주소와 수신 주소는 동일한 서비스 주소 임). SYN 메시지는 서버가 SYN-ACK 메시지를 서버 자체로 전송하도록 하므로 이 주소는 또한 ACK 메시지를 보내고 null 링크를 생성합니다. 이러한 각 종류의 링크는 제한 시간까지 유지되므로 서버가 고장납니다. Landattack 은 IPland 와 MACland 로 분류할 수 있습니다.

## 40.2. DoS 공격 방지 구성 작업 목록

글로벌 DoS 공격 방지 구성과 관련하여 관련 하위 기능을 구성한 다음 스위치가 해당 DoS 공격 패킷을 삭제합니다. 따라서 스위치의 대역폭은 사용되지 않도록 보장됩니다.

DoS 공격 방지 구성 작업은 아래와 같습니다.

- DoS 공격 방지 구성
- 모든 DoS 공격 방지 구성

## 40.3. DoS 공격 방지 구성 작업

### 40.3.1. 글로벌 DoS 공격 방지 구성

DoS 공격 방지를 구성하는 것은 global 모드에서 DoS 공격 방지 하위 기능을 구성하는 것을 의미하며 각 하위 기능은 다른 유형의 DoS 공격 패킷을 차단할 수 있습니다. DoS IP 하위 기능은 LAND 공격을 방지할 수 있지만 DoS ICMP 하위 기능은 Ping of Death 를 방지할 수 있습니다.

실제 요구 사항에 따라 해당 하위 기능을 구성할 수 있습니다.

EXEC 모드에서 DoS 공격 방지 기능 구성.

| 명령 | 설명 |
|---|---|
| **config** | Global 구성 모드를 시작합니다. |
| [no] **dos enable** {**all** \| **icmp icmp-value** \| **ip** \| **ipv4firstfrag** \| **l4port** \| **tcpflags** \| **tcpfrag tcpfrag-value**} | 모든 유형의 DoS 공격 패킷을 방지하도록 all 을 구성합니다.<br>ICMP 패킷을 방지하도록 ICMP 를 구성합니다.<br>ICMP 값은 ICMP 패킷의 최대 길이를 의미합니다.<br>출발지 IP 가 목적지 IP 와 동일한 IP 패킷을 방지하도록 ip 를 구성합니다.<br>ipv4 첫 번째 플래그를 구성하여 IP 패킷의 첫 번째 조각을 확인합니다.<br>원본 포트 ID 가 대상 포트 ID 인 TCP/UDP 패킷을 방지하도록 l4port 를 구성합니다.<br>불법 TCP 플래그를 포함하는 TCP 패킷을 방지하도록 tcpflags 를 구성합니다.<br>최소 TCP 헤더가 tcpfrag-value 인 TCP 패킷을 방지하도록 tcpfrag 를 구성합니다. |
| **exit** | EXEC 모드로 돌아갑니다. |
| **write** | 구성을 저장합니다. |

#### 40.3.2. 모든 DoS 공격 방지 구성 표시

show 명령을 통해 Dos 공격 방지 구성을 표시할 수 있습니다.
EXEC 모드에서 다음 명령을 실행하여 구성된 DoS 공격 방지 기능을 표시하십시오.

| 명령 | 설명 |
|---|---|
| **show dos** | DOS 공격 방지 구성을 표시합니다. |

## 40.4. DoS 공격 방지 구성 예

다음 예는 잘못된 플래그가 있는 TCP 패킷의 공격을 막고 사용자의 구성을 표시하도록 구성하는 방법을 보여줍니다.

**config**
dos enable tcpflags
show dos

다음 예제는 글로벌 모드에서 출발지 IP 가 목적지 IP 인 IP 패킷의 공격을 막는 방법을 보여줍니다.

**config**
dos enable ip

다음 예는 최대 길이가 255 보다 큰 ICMP 패킷의 공격을 글로벌 모드에서 방지하는 방법을 보여줍니다.

**config**
dos enable icmp 255

# 41. Anti-Attack 설정 명령

## 41.1. Anti-Attack 설정 명령어

### 41.1.1. Filter period

#### (1) 구문

filter period time
이 명령어는 공격 탐지 주기를 설정하는 데 사용됩니다.

no filter period
이 명령어는 공격 탐지 주기를 설정하는 데 사용됩니다.

#### (2) 매개변수

| 매개변수 | Description |
|---|---|
| *time* | 공격 방어 검사 주기(초 단위). 설정된 시간 동안 공격원이 지정된 패킷 수를 초과하면 공격으로 간주됩니다. (범위: 1~600 초) |

#### (3) 기본값

기본 설정값은 10 초입니다.

#### (4) 명령어 모드

전역 설정 모드

#### (5) 예제

Switch_config# filter period 15

#### (6) 연관 명령어

filter threshold

### 41.1.2. Filter threshold

#### (1) 구문

filter threshold type value
시스템이 공격으로 판단하기 전에 초과해야 하는 임계값을 설정하려면 위 명령어를 실행하십시오. 패킷 유형에 따라 설정을 다르게 지정할 수 있습니다.

no filter threshold type
기본값으로 복원하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

| 매개변수 | Description |
|---|---|
| *type* | 패킷 유형을 지정합니다. ARP, BPDU, DHCP, IGMP, ICMPv6, ICMP 를 포함합니다 |
| *value* | 공격 방지 검사 기간 동안 시스템이 공격으로 인식하기 전에 수신해야 하는 패킷 수를 지정합니다.<br>값 범위: 5~2000 |

**(3) 기본값**

기본값은 1000 패킷입니다.

**(4) 명령어 모드**

전역 설정 모드

**(5) 예제**

Switch_config# filter threshold ip 1500

**(6) 연관 명령어**

filter period

### 41.1.3. Filter block-time

**(1) 구문**

**filter block-time** *value*
공격 원본을 차단하는 시간을 설정하려면 filter block-time value 명령어를 사용하십시오.

**no filter block-time**
기본값으로 복원하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

| 매개변수 | Description |
|---|---|
| *value* | 공격이 감지된 후 공격 원본을 차단하는 시간을 설정합니다.<br>단위: 초<br>값 범위: 1~86400 |

**(3) 기본값**

기본값은 300 초 (5 분) 입니다.

**(4) 명령어 모드**

전역 설정 모드

**(5) 예제**

Switch_config# filter block-time 600

**(6) 연관 명령어**

filter period
filter threshold

### 41.1.4. Filter polling period

**(1) 구문**

**filter polling period** *time*
하이브리드 모드에서 공격 원본을 주기적으로 검사하는 주기를 설정하려면 다음 명령어를 실행하십시오.

**no filter polling period**
기본값으로 복원하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

| 매개변수 | Description |
|---|---|
| *time* | 공격 원본을 차단한 후 수행하는 주기적 폴링 검사 간격을 설정합니다. |

| | |
|---|---|
| | 단위: 초<br>값 범위: 1~600 |

**(3) 기본값**

기본값은 10 초입니다.

**(4) 명령어 모드**

전역 설정 모드

**(5) 예제**

Switch_config# filter polling period 20

**(6) 연관 명령어**

filter polling threshold
filter polling auto-fit

### 41.1.5. Filter polling threshold

**(1) 구문**

**filter polling threshold** type value
하이브리드 모드에서 필터 폴링 임계값을 설정하려면 다음 명령어를 실행하십시오. 패킷 유형에 따라 설정을 다르게 지정할 수 있습니다.

**no filter polling threshold** *type*
기본값으로 복원하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

| 매개변수 | Description |
|---|---|
| *type* | 패킷 유형을 지정합니다. ARP, BPDU, DHCP, IGMP, ICMP, ICMPv6, IP 를 포함합니다. |
| *value* | 특정 폴링 주기 내에 12000개의 패킷이 수신되면 공격 원본이 존재하는 것으로 간주됩니다. 값 범위: 12000 |

**(3) 기본값**

기본값은 750 패킷입니다.

**(4) 명령어 모드**

전역 설정 모드

**(5) 예제**

Switch_config# filter polling threshold ip 1500

**(6) 연관 명령어**

filter polling period
filter polling auto-fit

### 41.1.6. Filter polling auto-fit

**(1) 구문**

**filter polling auto-fit**
폴링 감지 주기와 임계값을 자동으로 조정하려면 위 명령어를 실행하십시오. 이 명령어는 기본적으로 활성화되어 있습니다.

폴링 주기 = 공격 감지 주기
폴링 패킷 임계값 = 공격 감지 패킷 임계값의 3/4

**no filter polling auto-fit**
기본 설정으로 복원하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

전역 설정 모드

**(4) 예제**

Switch_config# filter polling auto-fit

**(5) 연관 명령어**

filter polling period
filter polling threshold

### 41.1.7. Filter IGMP

**(1) 구문**

**filter igmp**
IGMP 공격 감지를 활성화하려면 위 명령어를 실행하십시오.

**no filter igmp**
IGMP 공격 감지를 비활성화하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

전역 설정 모드

**(4) 예제**

Switch_config# filter igmp

**(5) 연관 명령어**

filter enable

### 41.1.8. Filter ip source-ip

**(1) 구문**

**filter ip source-ip**
IP 공격 감지를 활성화하려면 위 명령어를 실행하십시오.

**no filter ip source-ip**
IP 공격 감지를 비활성화하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

전역 설정 모드 와 물리 포트 설정 모드.
이 명령어는 전역 포트와 물리 포트가 모두 설정된 경우에만 적용됩니다.

**(4) 예제**

Switch_config# filter ip source-ip
Switch_config# interface g0/1
switch_config_g0/1# filter ip source-ip

**(5) 연관 명령어**

filter enable

### 41.1.9. Filter ICMP

**(1) 구문**

**filter icmp**
ICMP 공격 감지를 활성화하려면 위 명령어를 실행하십시오.

**no filter icmp**
ICMP 공격 감지를 비활성화하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

전역 설정 모드 와 물리 포트 설정 모드.
이 명령어는 전역 포트와 물리 포트가 모두 설정된 경우에만 적용됩니다.

**(4) 예제**

Switch_config# filter icmp
Switch_config# interface g0/1
switch_config_g0/1# filter icmp

**(5) 연관 명령어**

filter enable

### 41.1.10. Filter DHCP

**(1) 구문**

**filter dhcp**
DHCP 공격 감지를 활성화하려면 위 명령어를 실행하십시오.

**no filter dhcp**
DHCP 공격 감지를 비활성화하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

전역 설정 모드 와 물리 포트 설정 모드.
이 명령어는 전역 포트와 물리 포트가 모두 설정된 경우에만 적용됩니다.

**(4) 예제**

Switch_config# filter dhcp
Switch_config# interface g0/1
switch_config_g0/1# filter dhcp

**(5) 연관 명령어**

filter enable

#### 41.1.11. Filter ARP

**(1) 구문**

**filter arp**
ARP 공격 감지를 활성화하려면 위 명령어를 실행하십시오.

**no filter arp**
ARP 공격 감지를 비활성화하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

물리 인터페이스 설정 모드

**(4) 연관 명령어**

filter enable

#### 41.1.12. Filter BPDU

**(1) 구문**

**filter bpdu**
BPDU 공격 감지를 활성화하려면 위 명령어를 실행하십시오.

**no filter bpdu**
BPDU 공격 감지를 비활성화하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

물리 인터페이스 설정 모드

**(4) 예제**

Switch_config_g0/1# filter bpdu

**(5) 연관 명령어**

filter enable

### 41.1.13. Filter mode

**(1) 구문**

**filter mode [ raw | hybrid ]**
필터 모드를 설정하려면 위 명령어를 실행하십시오.

**(2) 매개변수**

| 매개변수 | Description |
|---|---|
| raw | 필터를 Raw 모드로 설정합니다. |
| hybrid | 필터를 Hybrid 모드로 설정합니다. |

**(3) 기본값**

하이브리드 모드

**(4) 명령어 모드**

전역 설정 모드

**(5) 예제**

Switch_config# filter mode raw

**(6) 연관 명령어**

filter enable

#### 41.1.14. filter enable

**(1) 구문**

**filter enable**
공격 감지 기능을 활성화하려면 위 명령어를 실행하십시오.

**no filter enable**
기본 설정으로 복원하려면 위 명령어의 no 형식을 사용하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

전역 설정 모드

**(4) 예제**

Switch_config# filter enable

**(5) 연관 명령어**

없음

#### 41.1.15. show filter

**(1) 구문**

**show filter**
현재 스위치의 공격 방지 기능 작동 상태를 확인하려면 위 명령어를 실행하십시오

**show filter summary**
현재 스위치의 공격 방지 기능 요약 정보를 확인하려면 위 명령어를 실행하십시오.

**(2) 매개변수**

없음

**(3) 명령어 모드**

비사용자 모드 (Non-user mode)

**(4) 예제**

```
Switch#show filter
Filter period 600 seconds, polling interval 600 seconds
Filter thresholds:
Filter type(major code)  Minor code Threshold   Polling
arp                A             5       3
bpdu               B             1000      750
dhcp               D             1000      750
ip                 I             1000      750
icmp               I             1000      750
igmp               I             1000      750
Filters blocked:
Cause  Address         Seconds  Discard       Rate  Polling Interface
 arp  5491.afcd.1234      7.41       0        0/0   592.59    G0/1

Filters counting:
Cause    Address          Seconds     Count Interface
 arp     5491.afcd.1234       15.59         1     G0/1
```

Filters blocked: 차단된 공격 원본의 MAC 주소, 차단 시간, 원본 인터페이스를 표시합니다.
Filters counting: 공격 원본의 MAC 주소, 감지 시간, 수신 패킷 수, 원본 인터페이스를 표시합니다.

# 42. Access List 구성하기

## 42.1. IP 메시지 필터링

필터링 메시지는 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 방법은 특정 사용자 또는 장치를 통해 네트워크 전송 및 네트워크 사용을 제한할 수 있습니다. 교차 지정 인터페이스를 통해 패킷을 유효하거나 무효로 만들기 위해 라우팅 스위치는 Access-List 을 제공합니다. Access-List 는 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-list 를 사용하는 방법에 대해 설명합니다.

IP Access-list 은 IP 주소를 적용하기위한 허가/금지 조건의 규칙적인 집합입니다. 스위치의 운영 소프트웨어는 규정에 따라 Access-List 에서 주소를 하나씩 테스트합니다. 첫 번째 일치는 장비가 주소를 수락 또는 거절하는지 여부를 결정합니다. 첫 번째 일치가 있으면 장비 소프트웨어가 규칙 검사를 종료합니다. 따라서 조건의 순서가 중요합니다. 규정이 일치하지 않으면 주소가 거부됩니다.

다음 항목에 따라 Access-list 를 사용하십시오.

(1) Access list 의 이름과 조건을 지정하여 작성합니다.

(2) Access list 를 인터페이스에 적용합니다.

## 42.2. 표준 및 확장 가능 IP 액세스 목록 만들기

문자열을 사용하여 IP 액세스 목록을 만듭니다.

Note:
표준 Access-list 과 확장 Access-list 에는 같은 이름을 사용할 수 없습니다.
전역 구성 모드에서 다음 명령을 실행하여 표준 Access-list 만듭니다.

| 명령 | 설명 |
|---|---|
| **ip access-list standard** *name* | Access-List 의 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-List 에서 로그아웃 합니다. |

구성 모드에서 다음 명령을 실행하여 확장 가능한 Access-List 만듭니다.

| 명령 | 설명 |
|---|---|
| **ip access-list extended** *name* | 확장 Access-List 이름을 정의합니다. |
| {**deny** \| **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos**] [established] [log] {deny \| permit} protocol any any | 하나 이상의 허용 및 거부 조건을 지정하고 패킷 승인여부를 결정합니다. TOS는 서비스유형을 의미합니다. |
| **exit** | Access-List 모드에서 로그아웃 합니다. |

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

Note:
Access-List 를 만들면 Access-List 의 끝 부분에 기본적으로 암시적 거부 문장이 포함됩니다. 마스크가 상대 IP 호스트 주소 Access-list 에서 생략되면 255.255.255.255 가 마스크로 간주됩니다.

Access-List 를 만든 후에는 경로 또는 인터페이스에 액세스 목록을 적용해야 합니다. 자세한 내용은 42.3 "인터페이스에 Access-List 적용" 장을 참조하십시오.

## 42.3. 인터페이스에 Access list 적용

Access-List 을 만든 후에 입력 인터페이스 와 출력 인터페이스를 포함하여 하나 이상의 인터페이스에 적용할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **ip access-group** *name* {**in** \| **out**} | Access list 를 적용합니다. |

Access-list 은 입력 인터페이스와 출력 인터페이스에서 사용할 수 있습니다. 입력 인터페이스의 표준 Access-List 의 경우 패킷 수신 후 Access-list 에 따라 패킷의 손상된 주소를 확인해야 합니다. 확장형 Access-list 의 경우 라우팅 스위치는 대상을 확인합니다. Access-list 에서 주소를 허용하면 소프트웨어는 패킷 처리를 계속합니다. Access-list 에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달할 수 없는 메시지를 반환합니다.

외부 인터페이스의 표준 Access-list 의 경우 패킷이 수신되거나 제어 인터페이스로 라우팅 된 후 소프트웨어는 Access-list 에 따라 패킷의 원본 주소를 확인합니다. 확장형 Access-list 의 경우 라우팅 스위치도 수신 측의 Access-List 를 체크합니다. Access-list 에서 주소를 허용하면 소프트웨어가 패킷을 보냅니다. Access-list 에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달할 수 없는 메시지를 반환합니다.

지정된 Access-list 이 없으면 모든 패킷이 통과할 수 있습니다.

**확장 가능한 Access-list 의 예**
적용된 aaa 다음 첫 번째 줄은 새 TCP 가 포트 1023 다음에 대상 포트를 연결할 수 있게 합니다. 두 번째 줄은 새 TCP 가 호스트 130.2.1.2 의 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 25 가 있습니다. 보내는 패킷에는 반대 포트 번호가 있습니다. 사실, 라우팅 스위치 뒤에 있는 보안 시스템은 항상 포트 25 에서 메일을 받습니다. 들어오는 서비스와 나가는 서비스를 고유하게 제어할 수 있는 정확한 이유입니다. Access-list 은 발신 서비스 또는 수신 서비스로 구성될 수 있습니다.

다음과 같은 경우, 이더넷은 주소가 130.20.0.0 인 B 유형 네트워크입니다. 메일 호스트의 주소는 130.20.1.2 입니다. "established" 키워드는 TCP 프로토콜에만 사용됩니다. 즉, 연결이 생성됩니다. TCP 데이터에 ACK 또는 RST 숫자가 구성되어 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
```

# 43. 물리적인 포트를 기반으로 IP Access-list 구성

## 43.1. IP 메시지 필터링

필터링 메시지는 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 이 방법은 특정 사용자 또는 장치를 통해 네트워크 전송 및 네트워크 사용을 제한할 수 있습니다. 지정한 인터페이스를 통해 패킷을 유효하거나 무효로 만들기 위해 라우팅 스위치는 Access-List 을 제공합니다. Access-List 는 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-list 을 사용하는 방법에 대해 설명합니다.

IP Access-list 은 IP 주소를 적용하기위한 허가/금지 조건의 규칙적인 집합입니다. 스위치의 운영 소프트웨어는 규정에 따라 Access-List 에서 주소를 하나씩 테스트합니다. 첫 번째 일치는 장비가 주소를 수락 또는 거절하는지 여부를 결정합니다. 첫 번째 일치가 있으면 장비 소프트웨어가 규칙 검사를 종료합니다. 따라서 조건의 순서가 중요합니다. 규정이 일치하지 않으면 주소가 거부됩니다.

Access list 의 사용은 다음과 같은 단계가 있습니다.

(1) access list 의 이름과 조건을 지정하여 작성합니다.

(2) 인터페이스에 Access-list 를 저장합니다.

## 43.2. 표준 및 확장 IP Access List 생성

문자열을 사용하여 IP access list 를 만듭니다.

Note:
표준 Access-list 과 확장 Access-list 에는 동일한 이름을 사용할 수 없습니다.
전역 구성 모드에서 다음 명령을 실행하여 표준 Access-list 을 만듭니다.

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

구성 모드에서 다음 명령을 실행하여 확장 가능한 Access-list 를 만듭니다.

| 명령 | 설명 |
|---|---|
| **ip access-list extended** *name* | Access-list 에 이름을 적용합니다. |
| {**deny** \| **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** tos] [established] [log] {**deny** \| **permit**} | 하나이상의 허가/거부 지정하며 조건 이전 구성은 패킷의 승인여부를 결정합니다. TOS는 서비스유형을 의미합니다. |
| **exit** | 구성 모드에서 로그 아웃합니다. |

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

Note:
Access-List 을 만들면 Access-List 의 끝 부분에 기본적으로 암시적 거부 문장이 포함됩니다. 마스크가 상대 IP 호스트 주소 액세스 목록에서 생략되면 255.255.255.255 가 마스크로 간주됩니다.

## 43.3. 인터페이스에 Access List 적용

Access list 를 만든 후에 입력 인터페이스와 출력 인터페이스에 적용할 수 있습니다.
인터페이스 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **ip access-group** *name* | Access 그룹의 이름을 입출력한다. |

Access-list 는 입력 인터페이스와 출력 인터페이스에서 사용할 수 있습니다. 입력 인터페이스의 표준 액세스 목록의 경우 패킷 수신 후 Access-List 에 따라 패킷의 손상된 주소를 확인해야 합니다.

확장형 Access-List 의 경우 라우팅 스위치는 대상을 확인합니다. Access-List 에서 주소를 허용하면 소프트웨어는 패킷 처리를 계속합니다. 액세스 목록에서 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 도달할 수 없는 메시지를 반환합니다.

외부 인터페이스의 표준 Access-list 의 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 도달할 수 없는 메시지를 반환합니다.

지정된 액세스 목록이 없으면 모든 패킷이 통과할 수 있습니다.

**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-List 를 구성하는 경우 다음 사항에 주의하십시오.

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

**TCP/UDP 포트 필터링을 지원하는 포트 기반 IP Access-List**

다음의 예제에서 첫 번째 줄은 새 TCP 가 호스트 130.2.1.2 의 SMTP 에 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
```

# 44. IP 액세스 제어 목록 적용

## 44.1. IP Access Control List 적용

### 44.1.1. 포트에 ACL 적용

ACL 이 구성된 후에는 하나 이상의 슬롯 또는 전역 적으로 적용될 수 있습니다. global 또는 포트 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **config** | 글로벌 구성 모드로 들어갑니다. |
| **interface g0/1** | 구성할 포트 입력. |
| [**no**] {**ip** \| **ipv6**} **access-group** *name* [**〈cr〉** \| **egress** \| [**stat-packet** \| **stat-byte**] ] | 구성된 IP/IPv6 액세스 목록을 인터페이스에 적용하거나 인터페이스에서 취소합니다.<br>Egress 는 ACL 이 아웃 바운드 방향으로 적용됨을 의미합니다. |
| exit | 글로벌 구성 모드로 돌아갑니다. |
| exit | EXEC 모드로 돌아갑니다. |
| write | 구성을 저장합니다. |

# 45. VRRP (Virtual Router Redundancy Protocol)

## 45.1. VRRP 명령어

### 45.1.1. VRRP associate

VRRP 의 가상 IP 주소를 구성하려면 다음 명령어를 실행합니다.

vrrp vrid associate virtual-address virtual-mask [secondary]

기본 설정으로 돌아가려면 다음 명령어를 사용합니다.

no vrrp vrid associate [virtual-address virtual-mask] [secondary]

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 ID 입니다. 값 범위는 1 부터 255 까지입니다. |
| virtual-address | 가상 IP 주소 |
| virtual-mask | 가상 IP 주소 마스크 |

가상 IP 주소는 인터페이스 IP 와 동일한 네트워크 범위 내에 있어야 하며, 그렇지 않으면 가상 라우팅 스위치가 작동하지 않습니다.

가상 IP 주소가 인터페이스 IP 주소와 동일한 경우, 시스템은 자동으로 라우팅 스위치를 255 로 설정합니다.

가상 라우터 는 여러 개의 IP 주소를 구성할 수 있으며, 이 중 하나는 기본 주소로, 나머지는 보조 주소로 설정됩니다.

가상 IP 보조 주소는 secondary 매개변수를 사용하여 명령어로 구성됩니다.

다음 예제는 인터페이스 VLAN 1 에서 VRRP 그룹 1 을 활성화하고, 구성된 가상 IP 주소를 192.168.20.100 으로 설정하는 방법을 보여줍니다:

Switch_config# interface vlan 1
Switch_config_v1#vrrp 1 associate 192.168.20.100 255.255.255.0

### 45.1.2. VRRP authentication

인터페이스 VRRP 의 단순 텍스트 인증 방법을 구성하려면 다음 명령어를 실행합니다.

vrrp vrid authentication WORD

기본 설정으로 돌아가려면 다음 명령어를 사용합니다.

no vrrp vrid authentication

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 ID 입니다. 값 범위는 1 부터 255 까지입니다. |
| WORD | 인증 평문입니다. 길이는 8 자를 초과할 수 없습니다. |

VRRP 그룹은 동일한 인증 방법을 가져야 합니다.

다음 예제는 인터페이스 VLAN 1 에서 가상 라우터 1 의 인증 방법을 단순 텍스트(`simple-text`)로 설정하고, 인증 문자열을 `test`로 구성하는 방법을 보여줍니다:

Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 authentication test

### 45.1.3. VRRP description

VRRP 의 설명 정보를 구성하려면 다음 명령어를 실행합니다.

vrrp vrid description WORD

기본 설정으로 돌아가려면 다음 명령어를 사용합니다.

no vrrp vrid description

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 ID 입니다. 값 범위는 1 부터 255 까지입니다. |
| WORD | 인증 평문입니다. 길이는 8 자를 초과할 수 없습니다. |

다음 예제는 VLAN1 인터페이스에서 가상 라우터 1 의 설명 정보를 `GROUP1`으로 설정하는 방법을 보여줍니다.

Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 description GROUP1

### 45.1.4. VRRP preempt

VRRP 선점(Preempt)을 구성하려면 다음 명령어를 실행합니다.

vrrp vrid preempt

기본 설정으로 돌아가려면 다음 명령어를 사용합니다.

no vrrp vrid preempt

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 ID 입니다. 값 범위는 1 부터 255 까지입니다. |

VRRP 선점 기능이 활성화되면, 동일한 그룹 내에서 높은 우선순위를 가진 라우터가 낮은 우선순위를 가진 라우터를 선점합니다.

VRRP 선점 기능이 비활성화되면, 높은 우선순위를 가진 라우터라도 낮은 우선순위를 가진 라우터를 선점하지 않습니다.

다음 예제는 인터페이스 VLAN 1 에서 가상 라우터 1 의 선점 기능을 비활성화하는 방법을 보여줍니다:

Switch_config# interface vlan 1
Switch_config_v1# no vrrp 1 preempt

### 45.1.5. VRRP preempt delay

VRRP 의 우선순위 선점 지연 시간을 구성하려면 다음 명령어를 실행합니다.

vrrp vrid preempt delay second

기본 설정으로 돌아가려면 다음 명령어를 사용합니다.

no vrrp vrid preempt delay

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 ID, 1 에서 255 까지의 범위입니다. 이 ID 는 VRRP 그룹을 식별합니다. |
| delay | 우선 순위 전환 지연 시간, 0 에서 255 까지의 범위입니다. 이 시간은 라우터가 기본 라우터로 전환하기까지 기다리는 시간을 의미합니다. 기본값은 0 초로, 즉 즉시 전환을 의미합니다. |

다음 예시에서는 가상 라우터 1 의 VLAN 인터페이스에서 우선 순위 전환 지연 시간을 10 초로 설정하는 방법을 보여줍니다.

Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 preempt delay 10

### 45.1.6. VRRP priority

Virtual Router Redundancy Protocol (VRRP) 우선순위 값을 설정합니다. 기본 설정으로 되돌리려면 no 형식을 사용합니다.

vrrp vrid priority value
no vrrp vrid priority

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 의 ID. 값 범위는 1 에서 255 입니다. |
| value | 우선순위 값. 값 범위는 1 에서 254 입니다. |

다음 예제는 인터페이스 vlan 1 의 가상 라우터 1 의 우선순위 값을 120 으로 설정합니다.

Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 priority 120

### 45.1.7. VRRP source-mac-use-system

VRRP 프로토콜 패킷의 소스 MAC 주소를 설정하려면 다음 명령을 실행합니다. 기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

vrrp vrid source-mac-use-system
[no] vrrp vrid source-mac-use-system

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 ID 를 지정합니다. 값은 1 부터 255 까지입니다. |

이 명령을 구성한 후, VRRP 패킷은 시스템 MAC 주소를 프로토콜 패킷의 소스 MAC 주소로 사용합니다.
다음 예제는 VLAN1 인터페이스의 가상 라우터 1 이 시스템 MAC 주소로 프로토콜 패킷을 전달하는 방법을 보여줍니다.

Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 source-mac-use-system

### 45.1.8. VRRP timers

VRRP 의 알림 타이머를 설정하려면 다음 명령을 실행합니다.

vrrp vrid timers advertise {second | dsec decisecond | csec centisecond}

기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

no vrrp vrid timers advertise

알림 타이머를 학습 모드로 설정하려면 다음 명령을 실행합니다.

vrrp vrid timers learn

기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

no vrrp vrid timers learn

| 명령 | 설명 |
|---|---|
| vrid | 가상 라우터 의 ID. 값의 범위는 1 에서 255 까지입니다. |
| second | 알림 타이머 값; 단위: 초; 값의 범위는 1 에서 255 까지입니다. |
| decisecond | 알림 타이머 값, 단위: 0.1 초; 값의 범위는 5 에서 360 까지입니다. |
| centisecond | 알림 타이머 값, 단위: 0.01 초; 값의 범위는 1 에서 3600 까지입니다. |

타이머 값은 가상 라우터 가 오류로부터 복구하는 데 걸리는 최소 시간을 결정합니다. 마스터 라우터의 링크가 다운되면 백업 라우터 는 3 * advertisement + skew_time 간격 내에 마스터 라우터 로 전환됩니다. advertisement 값이 클수록 오류 복구에 좋지 않습니다. 사용자는 기본값을 사용하는 것이 좋습니다.

다음 명령은 인터페이스 vlan 1 의 가상 라우터 1 의 알림 타이머 값을 2 초로 설정합니다.

Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 timers advertise 2

### 45.1.9. VRRP track

**VLAN 인터페이스 설정 모드:**

vrrp vrid track interface intf-id value
no vrrp vrid track interface intf-id
vrrp vrid track ip ip-address value
no vrrp vrid track ip ip-address

VRRP 모니터링 기능을 설정하려면 다음 명령을 실행합니다. 기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

**전역 설정 모드:**
BFD 정적 감지를 설정하려면 다음 명령을 실행합니다. 다음 홉에 도달할 수 있으면 대상 노드 경로에 도달할 수 있습니다. 기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

ip route bfd static next-hop
no ip route bfd static next-hop

BFD 감지 정적 라우팅 기능을 설정하려면 다음 명령을 실행합니다. 구성된 게이트웨이 주소에 도달할 수 있으면 대상 노드 경로에 도달할 수 있습니다. 기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

ip route bfd static A.B.C.D
no ip route bfd static A.B.C.D

**사용 지침**
모니터링 기능을 사용하면 VRRP 그룹은 링크 상태 변화에 따라 적절하게 우선순위를 조정하고 주 회선 상태를 백업 회선 상태로 전환할 기회를 제공할 수 있습니다. 여기서 링크 상태 변화는 VRRP 라우터 자체의 링크 상태가 아닌 VRRP 라우터 를 통과하는 대상 링크의 도달
가능 여부를 의미합니다.

VRRP 는 두 가지 모니터링 객체를 지원합니다. 첫째, 인터페이스 상태 모니터링. 모니터링 대상 인터페이스의 링크 상태가 다운되면 자체 우선순위를 능동적으로 낮춥니다. 둘째, 지정된 노드의 정적 라우팅 상태를 모니터링합니다. 모니터링 대상 경로에 도달할 수 없으면 자체 우선순위를 능동적으로 낮춥니다.

지정된 노드의 정적 라우팅 상태를 모니터링하려면 BFD 정적 경로 감지 기능이 필요합니다.

**예제**
다음 예제는 vlan1 가상 라우터 1 이 물리 포트 g5/1 을 모니터링하도록 설정하는 방법을 보여줍니다. 물리 포트 g5/1 의 상태가 다운되면 자체 우선순위를 20 만큼 낮춥니다.
Switch_config# interface vlan 1
Switch_config_v1# vrrp 1 track interface GigaEthernet5/1 20

다음 예제는 vlan1 포트의 가상 라우터 1 이 IP 주소 1.1.1.254 의 정적 라우팅 상태를 모니터링하는 방법을 보여줍니다. 해당 정적 경로와 BFD 가 구성되고 1.1.1.254 의 라우팅 상태가 도달할 수 없게 되면 자체 우선순위를 20 낮춥니다.

Switch_config#ip route 1.1.1.254 255.255.255.255 1.1.1.100
Switch_config#ip route bfd static next-hop
Switch_config# interface vlan 1
Switch_config_v1#vrrp 1 track ip 1.1.1.254 20

### 45.1.10. show VRRP

가상 라우터 이중화 프로토콜(VRRP) 정보를 표시하려면 다음 명령을 실행합니다. 기본 설정으로 되돌리려면 no 형태의 명령을 사용합니다.

show vrrp brief
show vrrp [interface intf-id] detail

| 명령 | 설명 |
|---|---|
| intf-id | 특정 물리 인터페이스. |

이 명령은 VRRP 정보를 표시하는 데 사용됩니다.
다음 예제는 인터페이스 vlan 1 의 VRRP 정보를 표시합니다.

Switch_config# show vrrp interface vlan 1 detail

VLAN1 - Group 1
 VRRP State is Master
 Virtual IP address: 192.168.20.110/24
 Virtual Mac address: 0000.5e00.0101
 Current Priority: 100 (Config 100)
 VRRP timer: Advertise 1.0 s (default) master_down 3.6 s
 VRRP current timer: Advertise 1.0 s master_down 0.0 s preempt after 0.0 s
 Authentication string is not set
 Preempt is set (delay: 0 s)
 Learn Advertise Interval is not set
Master Router IP: 192.168.20.118, priority: 100, advertisement: 1.0 s

### 45.1.11. debug VRRP

VRRP 정보를 디버깅하려면 debug vrrp 명령을 사용합니다. VRRP 정보 디버깅을 비활성화하려면 이 명령의 no 형태를 사용합니다.

debug vrrp [interface intf-id vrid] {errors | events | packets | all}
no debug vrrp

| 명령 | 설명 |
|---|---|
| intf-id | 특정 물리 포트 |
| vrid | 가상 라우터 ID. 값의 범위는 0 에서 255 까지입니다. 기본값은 0 입니다. |

다음 명령은 VRRP 디버깅 스위치를 활성화하는 방법을 보여줍니다.

Switch# debug vrrp packets

# 46. 라우팅 프로토콜 개요

## 46.1. IP 라우팅 프로토콜 (IP Routing Protocol)

회사의 라우터는 여러 IP 동적 라우팅 프로토콜을 구현합니다. 이들은 본 장의 각 프로토콜 설명에서 소개될 것입니다.

IP 라우팅 프로토콜은 내부 게이트웨이 라우터 프로토콜(IGP)과 외부 게이트웨이 라우터 프로토콜(EGP)의 두 가지 범주로 분류됩니다. 라우터는 RIP, OSPF, BGP 및 BEIGRP 를 지원합니다. RIP, OSPF, BGP 및 BEIGRP 는 실제 필요에 따라 개별적으로 구성할 수 있습니다. 라우터는 (메모리가 충분한 경우) 무제한의 OSPF 프로세스, BGP 프로세스, RIP 프로세스 및 무제한의 BEIGRP 프로세스를 포함하여 여러 라우팅 프로토콜의 동시 구성을 지원합니다. "재분배(redistribute)" 명령을 사용하여 다른 라우터 프로토콜을 현재 라우팅 프로토콜의 데이터베이스에 삽입하여 여러 라우팅 프로토콜을 연결할 수 있습니다. IP 동적 라우팅 프로토콜을 구성하려면 해당 프로세스를 시작하고 해당 네트워크 인터페이스와 특정 동적 라우팅 프로세스를 연결하여 라우팅 프로세스가 실행되는 인터페이스를 지정해야 합니다. 이를 위해 구성에 대한 관련 문서를 참조하여 구성 단계를 확인해야 합니다.

## 46.2. 라우팅 프로토콜 선택

라우팅 프로토콜 선택은 복잡한 과정입니다. 라우팅 프로토콜을 선택할 때 다음 요소를 고려해야 합니다.

(1) 네트워크의 규모와 복잡성
(2) VLSM 지원 필요 여부
(3) 네트워크 트래픽
(4) 보안 요구 사항
(5) 신뢰성 요구 사항
(6) 정책
(7) 기타

이 주제는 여기에서 자세히 다루지 않습니다. 선택한 라우팅 프로토콜은 네트워크의 실제 조건을 충족하고 사용자의 요구 사항을 준수해야 합니다.

### 46.2.1. 내부 게이트웨이 라우팅 프로토콜 (IGP, Interior Gateway Protocol)

내부 게이트웨이 라우팅 프로토콜(Interior Gateway Routing Protocol)은 단일 자율 시스템(Autonomous System) 내의 네트워크에서 사용됩니다. 모든 IP 내부 게이트웨이 라우팅 프로토콜은 시작될 때 특정 네트워크와 연결되어야 합니다 (예: network 구성). 각 라우팅 프로세스는 네트워크의 다른 라우터로부터 업데이트 메시지를 수신하고 동시에

네트워크에서 자체 라우팅 정보를 브로드캐스트합니다. 라우터에서 지원하는 내부 게이트웨이 라우터 프로토콜은 다음과 같습니다.

(1) RIP
(2) OSPF
(3) BEIGRP

### 46.2.2. 외부 게이트웨이 라우팅 프로토콜 (EGP, Exterior Gateway Protocol)

외부 게이트웨이 라우팅 프로토콜(Exterior Gateway Routing Protocol)은 서로 다른 자율 시스템(Autonomous System) 간에 라우팅 정보를 교환하는 데 사용됩니다. 일반적으로 경로 교환, 도달 가능한 네트워크 및 로컬 자율 시스템 번호를 위해 해당 이웃을 구성해야 합니다. 라우터에서 지원하는 외부 게이트웨이 라우팅 프로토콜은 BGP 입니다.

# 47. VRF 설정

## 47.1. 개요

VPN 의 핵심 중 하나는 데이터의 보안 유지 및 격리입니다. 동일한 VPN 에 속하지 않은 스테이션 간의 통신을 차단할 수 있어야 합니다. PE 장치에서 어느 로컬 인터페이스를 통해 VPN 사용자 경로가 전송되었는지 구별하기 위해 PE 장치에 가상 경로를 생성합니다. 모든 가상 경로는 자체 라우팅 테이블과 포워딩 테이블을 갖습니다. 이러한 라우팅 테이블과 포워딩 테이블을 VRF(VPN 라우팅 및 포워딩 인스턴스)라고 합니다. 하나의 VRF 는 동일한 스테이션 관련 라우팅 테이블, 인터페이스(서브 인터페이스), 라우팅 인스턴스 및 라우팅 정책을 포함합니다. PE 에서 동일한 VPN 을 가진 물리적 포트 또는 논리적 포트는 하나의 VRF 에 해당합니다.

## 47.2. VRF 구성 작업 목록

VRF 를 구성하려면 다음 작업이 필요합니다.

(1) VRF 테이블 생성
(2) 인터페이스와 VRF 연결
(3) VRF 의 대상 VPN 확장 속성 구성
(4) VRF 설명 구성
(5) VRF 의 정적 경로 구성
(6) VRF 모니터링
(7) VRF 유지 관리
(8) VRF 구성 예제

## 47.3. 구성 작업

### 47.3.1. VRF 테이블 생성

VPN 라우팅 및 포워딩 테이블을 생성하려면 글로벌 구성 모드에서 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| PE_config#**ip vrf** ce | VRF 구성 모드로 진입하여 VRF 테이블을 정의합니다. |
| PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn* | VRF 의 라우팅 태그를 지정하고 VRF 라우팅 및 포워딩 테이블을 생성합니다. |
| PE_config_vrf_ce#**route-target** [**export** \| **import** \| **both** ] *ASN:nn or IP-address:nn* | VRF 의 입력 및 출력 대상 VPN 확장 속성을 생성합니다. |

### 47.3.2. 인터페이스 VRF 연결

인터페이스를 VRF 에 연결하려면 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| PE_config#**interface vlan** 1 | 인터페이스 구성 모드로 진입합니다. |
| PE_config_v1#**ip vrf forwarding** *vrf-name* | 인터페이스를 VRF 에 연결합니다. |
| PE_config_v1#**ip address** *ip-address subnet-mask* | 인터페이스의 IP 주소를 구성합니다. |

### 47.3.3. VRF 의 대상 VPN 확장 속성 구성

VRF 의 대상 VPN 확장 속성을 구성하려면 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| PE_config#**ip vrf** ce | VRF 구성 모드로 진입합니다. |
| PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn* | VRF 라우팅 태그를 구성하고 VRF 테이블을 생성합니다. |
| PE_config_vrf_ce#**route-target** [**export** \| **import** \| **both** ] *ASN:nn or IP-address:nn* | VRF 의 입력 및 출력 대상 확장 속성을 구성합니다. |
| PE_config_vrf_ce#**import map** *WORD* | VRF 라우팅 테이블에 추가되는 경로의 route-map 필터를 구성합니다. |
| PE_config_vrf_ce#**export map** *WORD* | route-map 조건에 맞는 대상 VPN 확장 속성을 VRF 의 출력 대상 VPN 확장 속성에 추가합니다. |

로컬 경로를 다른 PE 라우팅 장치로 게시하기 전에, 진입 PE 는 직접 연결된 스테이션에서 학습한 모든 경로에 경로 대상 속성을 추가합니다. 경로에 연결된 대상 값은 출력 대상 확장 속성에 구성된 VRF 값을 기반으로 합니다.

다른 PE 에서 게시된 원격 경로를 로컬 VRF 에 설치하기 전에, 진입 PE 라우팅 장치의 모든 VRF 는 하나의 입력 대상 확장 속성으로 구성됩니다. PE 라우팅 장치는 VPN-IPv4 가 전달하는 라우팅 대상 속성이 VRF 입력 대상과 일치할 때까지 특정 VRF 에만 설치할 수 있습니다.

### 47.3.4. VRF 설명 구성

VRF 설명 구성을 하려면 다음을 수행합니다.

| 명령 | 설명 |
|---|---|

| | |
|---|---|
| PE_config#**ip vrf** ce | VRF 구성 모드로 진입합니다. |
| PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn* | VRF 라우팅 태그를 구성하고 VRF 테이블을 생성합니다. |
| PE_config_vrf_ce# **description** LINE | VRF 에 대한 설명을 구성합니다. |

### 47.3.5. VRF 의 정적 경로 구성

VRF 의 정적 경로를 구성하려면 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| PE_config#**ip vrf** ce | VRF 구성 모드로 진입합니다. |
| PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn* | VRF 라우팅 태그를 구성하고 VRF 테이블을 생성합니다. |
| PE_config_vrf_ce#**exit** | VRF 구성 모드에서 나옵니다. |
| PE_config#**ip route** [**vrf** vrf-name] dest mask { type num \| nexthop } [distance] | VRF 정적 경로를 구성합니다. |

### 47.3.6. VRF 모니터링

VRF 를 모니터링하려면 VRF 의 통계를 확인합니다. 모니터링하려면 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| PE#**show ip vrf** | VRF 및 관련 포트 정보를 표시합니다. |
| PE#**show ip vrf** [{**brief** \| **detail** \| **interfaces**}] *vrf-name* | VRF 구성 및 관련 포트 정보를 표시합니다. |
| PE#**show ip route vrf** *vrf-name*[A.B.C.D \| all \| beigrp \| bgp \| ospf \| rip \| connect \| static \| summary ] | VRF 라우팅 테이블의 라우팅 정보를 표시합니다. |

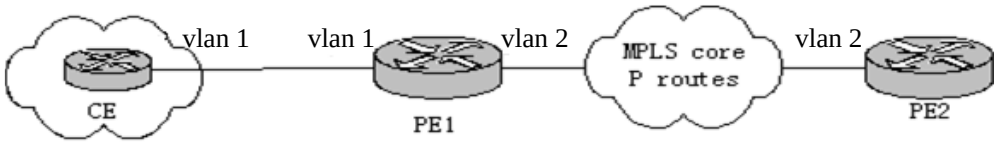
### 47.3.7. VRF 유지 관리

VRF 를 유지 관리하려면 관리 모드에서 기본 라우팅 테이블과 VRF 라우팅 테이블 및 VRF 구성 정보의 변경 사항을 추적하고 다음을 수행합니다.

| 명령 | 설명 |
|---|---|

| | |
|---|---|
| PE#**debug ip routing** | 기본 라우팅 테이블에서 경로의 추가, 삭제 및 변경 사항을 추적합니다. |
| PE **#debug ip routing message** | VRF 가 수신하고 보낸 정보를 추적합니다. |
| PE **#debug ip routing vrf** *vrf-name* | 추가, 삭제 및 변경을 포함하여 지정된 VRF 라우팅 테이블의 변경 사항을 추적합니다. |

## 47.4. VRF 구성 예제




라우팅 장치의 구성은 다음과 같습니다.

```
Routing device CE:
interface loopback 0
 ip address 22.1.1.1 255.255.255.0
!
interface vlan 1
ip address 170.168.20.152 255.255.255.0
!
router ospf 1
 network 170.168.20.0 255.255.255.0 area 0
 network 22.1.1.0 255.255.255.0 area 0
!
Routing device PE1:
ip vrf pe1
    rd 1:1
    route-target 1:1
!
interface vlan 1
ip vrf forwarding pe1
ip address 170.168.20.153 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.152 255.255.255.0
!
router ospf 1 vrf pe1
 network 170.168.20.0 255.255.255.0 area 0
```

```
!
router bgp 1
    neighbor 176.168.20.154 remote-as 2

    address-family vpnv4
    neighbor 176.168.20.154 activate
    exit-address-family

    address-family ipv4 vrf pe1
    no synchronization
    redistribute ospf 1
    exit-address-family
```

Routing device PE2:

```
ip vrf pe2
    rd 1:1
    route-target 1:1
!
interface loopback 0
 ip vrf forwarding pe2
 ip address 44.1.1.1 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.154 255.255.255.0
!
router bgp 2
    neighbor 176.168.20.153 remote-as 1

address-family vpnv4
neighbor 176.168.20.153 activate
exit-address-family

address-family ipv4 vrf pe2
no synchronization
redistribute connected
exit-address-family
```

# 48. 정적 라우팅 구성

## 48.1. 개요

이 장에서는 정적 라우팅을 구성하는 방법을 설명합니다. 이 섹션의 정적 라우팅 명령어에 대한 자세한 설명이 필요하면 "네트워크 프로토콜 명령어 참조"의 "정적 라우팅" 장을 참조합니다. 다른 명령어로 문서를 검색하려면 명령어 마스터 색인을 사용하여 인라인 검색을 수행하면 됩니다.

정적 라우팅은 특별한 라우팅 구성으로, 관리자가 구성합니다. 네트워크 구조가 비교적 단순한 네트워크에서는 네트워크 상호 운용성을 위해 정적 경로만 구성하면 됩니다. 정적 경로를 적절하게 설정하고 사용하면 네트워크 성능을 향상시킬 수 있으며 중요한 네트워크 애플리케이션에 대한 대역폭을 보장할 수 있습니다.

정적 경로의 단점은 네트워크 토폴로지의 변화에 자동으로 적응하지 못한다는 것입니다. 네트워크 장애 또는 토폴로지 변경으로 인해 경로에 도달할 수 없게 되면 네트워크 중단이 발생할 수 있으며, 이 경우 네트워크 관리자가 정적 경로 구성을 수동으로 수정해야 합니다.

라우팅 시 라우터가 일치하는 라우팅 테이블 항목을 찾을 수 없는 경우 기본 경로가 사용됩니다.

(1) 패킷의 목적지 주소가 라우팅 테이블의 어떤 항목과도 일치하지 않으면 패킷은 기본 경로를 선택합니다.
(2) 기본 경로가 없고 패킷의 목적지가 라우팅 테이블에 없으면 패킷은 폐기됩니다.

라우팅 테이블에 나타나도록 정적 라우팅 구성을 통해 0.0.0.0/0.0.0.0 형식의 기본 경로를 네트워크에 설정합니다.

## 48.2. 정적 라우팅 구성 작업 목록

정적 라우팅을 구성하려면 다음 작업이 필요합니다.

(1) 관련 인터페이스의 물리적 매개변수를 구성합니다.
(2) 관련 인터페이스의 링크 계층 속성을 구성합니다.
(3) 관련 인터페이스의 IP 주소를 구성합니다

## 48.3. 정적 라우팅 구성 작업

### 48.3.1. 정적 라우팅 구성

정적 라우팅을 활성화하려면 글로벌 구성 모드에서 다음 단계를 수행해야 합니다.

| 명령 | 설명 |
| --- | --- |
| **ip route** A.B.C.D mask {next-hop \| interface} [distance] [tag tag] [global] [description] | 정적 라우팅을 구성합니다. |

### 48.4. 정적 라우팅 구성 예제

네트워크 세그먼트 10.0.0.0/8 패킷 포트가 인터페이스 GigaEthernet3/0 에 할당되었으며 구성은 다음과 같습니다.

ip route 10.0.0.0 255.0.0.0 gigaEthernet 3/0

# 49. RIP 설정

## 49.1. 개요

이 장에서는 RIP 을 구성하는 방법을 설명합니다. 이 섹션의 RIP 명령어에 대한 자세한 설명이 필요하면 "네트워크 프로토콜 명령어 참조"의 "RIP 명령어" 장을 참조합니다. 다른 명령어로 문서를 검색하려면 명령어 마스터 색인을 사용하여 인라인 검색을 수행하면 됩니다.

RIP(Routing Information Protocol)는 비교적 오래되었지만 여전히 일반적으로 사용되는 내부 게이트웨이 프로토콜(IGP)로, 주로 동일 종류의 소규모 네트워크에서 사용됩니다. RIP 은 RFC 1058 에 명시된 전통적인 거리 벡터 라우팅 프로토콜입니다.

RIP 은 UDP 패킷 브로드캐스팅을 통해 라우팅 정보를 교환합니다. 라우터에서 업데이트된 라우팅 정보는 30 초마다 전송됩니다. 이웃 라우터로부터 180 초 이내에 업데이트 정보를 받지 못하면 라우팅 테이블의 해당 이웃 라우터의 경로는 "사용할 수 없음"으로 표시됩니다. 그리고 이후 120 초 동안 업데이트된 정보가 수신되지 않으면 이러한 경로는 라우팅 테이블에서 삭제됩니다.

홉 수는 RIP 에서 서로 다른 경로를 측정하는 메트릭으로 사용됩니다. 홉 수는 출발지에서 목적지까지 패킷이 통과하는 라우터의 수를 나타냅니다. 네트워크에 직접 연결된 경로의 메트릭은 "0"이고, 네트워크에 도달할 수 없는 경로의 메트릭은 "16"입니다.

RIP 에서 사용하는 경로 메트릭은 비교적 작은 범위에 있으므로 대규모 네트워크에는 적용할 수 없습니다. 라우터에 기본 경로가 있으면 RIP 은 0.0.0.0 의 잘못된 네트워크에 경로를 알립니다. 실제로 0.0.0.0 네트워크는 존재하지 않으며 RIP 에서 기본 경로 기능을 구현하는 데만 사용됩니다. RIP 이 기본 경로를 학습했거나 라우터에 기본 게이트웨이가 구성되어 있고 기본 메트릭으로 구성된 경우 라우터는 기본 네트워크를 알립니다.

RIP 은 지정된 네트워크의 인터페이스로 업데이트를 보냅니다. 인터페이스의 네트워크가 지정되지 않으면 해당 네트워크는 어떤 RIP 업데이트에도 포함되지 않습니다.

라우터의 RIP-2 는 일반 텍스트 및 MD5 인증, 경로 요약, CIDR 및 VLSM 을 지원합니다.

## 49.2. RIP 구성 작업 목록

RIP 을 구성하려면 다음 작업이 필요합니다. RIP 을 먼저 활성화해야 하지만 다른 작업은 선택 사항입니다.

(1) RIP 시작
(2) RIP 경로 업데이트 메시지의 유니캐스팅 활성화
(3) 경로 메트릭에 오프셋 적용

(4) 타이머 조절
(5) RIP 버전 번호 지정
(6) RIP 인증 활성화
(7) 경로 요약 금지
(8) 출발지 IP 주소의 인증 금지
(9) 스플릿 호라이즌 활성화 또는 금지

## 49.3. RIP 구성 작업

### 49.3.1. RIP 시작

RIP 을 활성화하려면 글로벌 구성 모드에서 다음 단계를 수행해야 합니다.

| 명령 | 설명 |
|---|---|
| **router rip** | RIP 라우팅 프로세스를 활성화하고 라우터 구성 모드로 진입합니다. |
| **network** *network-number* *〈network-mask〉* | RIP 라우팅 프로세스와 관련된 네트워크 번호를 지정합니다. |

### 49.3.2. RIP 라우터에 의해 모노 브로드캐스팅 업데이트 허용 및 그룹화

RIP 은 브로드캐스팅 방식의 프로토콜입니다. 만약 경로 업데이트가 브로드캐스팅 방식이 아닌 네트워크에 접근하도록 하려면, 라우터가 정보 교환을 활성화하도록 구성해야 합니다. 이를 위해 라우터 구성 모드에서 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **neighbor** *ip-address* | 라우팅 정보를 교환할 이웃 라우터를 정의합니다. |

또한, 어떤 인터페이스를 사용하여 라우팅 정보를 교환할지 제어하려면 "ip rip passive" 명령을 사용하여 경로 업데이트 전송을 금지하는 특정 인터페이스 또는 여러 인터페이스를 지정할 수 있습니다. 필요한 경우 "IP 라우터 구성의 프로토콜 독립적 명령어" 장의 "라우팅 정보 필터링"에 있는 관련 설명을 참조합니다.

### 49.3.3. 경로 메트릭에 오프셋 사용

오프셋 목록은 RIP 을 통해 학습한 입력 및 출력 경로에 오프셋을 증가시키는 데 사용됩니다. 반면, 접근 목록 또는 인터페이스를 사용하여 오프셋 목록을 제한할 수 있습니다. 경로 메트릭을 증가시키려면 라우터 구성 모드에서 다음 명령을 실행해야 합니다.

| 명령 | 설명 |
|---|---|
| **offset-list** {[**interface-type** *number*]|*} {**in**|**out**} *access-list-name* **offset** | 경로 메트릭에 오프셋을 추가합니다. |

### 49.3.4. RIP 타이머 조절

라우팅 프로토콜은 경로 업데이트 전송 빈도, 라우터가 유효하지 않은 상태가 되는 기간 및 기타 매개변수를 결정하기 위해 여러 타이머를 사용합니다. 이러한 타이머를 조절하여 라우팅 프로토콜의 성능을 네트워크 요구 사항에 더 적합하게 할 수 있습니다.

또한, 모든 종류의 IP 라우팅 계산의 수렴 시간을 단축하고, 신속한 복구를 위한 중복 라우터로 빠르게 백업하여 빠른 복구 시간을 최소화하도록 경로 프로토콜을 조절할 수 있습니다. 타이머를 조절하려면 라우터 구성 모드에서 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **timers holddown** *value* | 특정 경로가 라우팅 테이블에서 삭제되는 데 걸리는 시간(초 단위)을 조절합니다. |
| **timers expire** *value* | 라우터가 유효하지 않다고 알려지는 시간(초 단위)을 조절합니다. |
| **timers update** *value* | 라우터 업데이트 전송 빈도(라우팅 업데이트 전송 간격, 초 단위)를 조절합니다. |

### 49.3.5. RIP 버전 번호 지정

라우터의 RIP-2 는 인증, 비밀번호 관리, 경로 요약, CIDR 및 VLSM 을 지원합니다. 기본적으로 라우터는 RIPv1 및 RIPv2 업데이트를 모두 수신할 수 있지만 RIP-1 업데이트만 전송할 수 있습니다. 구성을 통해 라우터가 RIPv1 업데이트만 수신 및 전송하거나 RIPv2 업데이트만 수신 및 전송하도록 설정할 수 있습니다. 이를 위해 라우터 구성 모드에서 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **version** {1 | 2} | 라우터가 RIPv1 또는 RIPv2 업데이트만 주고받도록 구성합니다. |

위의 작업은 RIP 의 기본 동작을 제어하는 것입니다. 또한 특정 인터페이스를 구성하여 이 기본 동작을 변경할 수 있습니다. 인터페이스가 RIP-1 업데이트 또는 RIP-2 업데이트를 전송하도록 제어하려면 인터페이스 구성 모드에서 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **ip rip send version 1** | 인터페이스가 RIP-1 업데이트만 전송하도록 구성합니다. |
| **ip rip send version 2** | 인터페이스가 RIP-2 업데이트만 전송하도록 구성합니다. |
| **ip rip send version compatibility** | 브로드캐스트를 통해 RIP-2 메시지 업데이트를 전송합니다. |

동시에 인터페이스가 RIP-1 및 RIP-2 업데이트를 모두 수신하도록 제어하려면 인터페이스 구성 모드에서 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **ip rip receive version 1** | 인터페이스가 RIP-1 업데이트만 수신하도록 구성합니다. |
| **ip rip receive version 2** | 인터페이스가 RIP-2 업데이트만 수신하도록 구성합니다. |
| **ip rip receive version 1 2** | 인터페이스가 RIP-1 및 RIP-2 업데이트를 모두 수신하도록 구성합니다. |

### 49.3.6. Enabling RIP Authentication

RIP-1 은 인증을 지원하지 않습니다. RIP-2 업데이트를 주고받으려면 인터페이스에서 RIP 인증 기능을 활성화해야 합니다.

활성화된 RIP 인터페이스에서 일반 텍스트 인증과 MD5 인증의 두 가지 인증 모드를 지원합니다. 일반 텍스트 인증은 기본 상태에서 RIP-2 의 각 하위 그룹에서 사용됩니다.

Note:
보안상의 이유로 RIP 그룹에서 일반 텍스트 인증을 사용하지 마십시오. 암호화되지 않은 인증 키가 각 RIP-2 업데이트로 전송되기 때문입니다. 보안이 큰 문제가 되지 않는 경우(잘못 구성된 호스트가 경로에 참여할 수 없다고 보장되는 경우) 일반 텍스트 인증을 사용할 수 있습니다.

RIP 일반 텍스트 인증을 구성하려면 인터페이스 구성 모드에서 다음 단계를 수행해야 합니다.

| 명령 | 설명 |
|---|---|
| **ip rip authentication simple** | RIP 인증을 활성화합니다. |
| **ip rip password** [*string*] | 인터페이스에 대한 일반 텍스트 인증 키를 구성합니다. |

MD5 인증을 구성하려면 인터페이스 구성 모드에서 다음 단계를 수행해야 합니다.

| 명령 | 설명 |
|---|---|
| **ip rip authentication** *message-digest* | RIP MD5 인증을 활성화합니다. |

| | |
|---|---|
| **ip rip message-digest-key** [*key-ID*] **md5** [*key*] | 인터페이스에 대한 MD5 인증 키를 구성합니다. |

### 49.3.7. 인터페이스의 'Passive' 및 'Deaf' 상태 활성화

기본적으로 RIP 이 적용된 인터페이스는 RIP 프로토콜을 유연하게 적용하여 라우팅 업데이트를 전달하고 받을 수 있습니다.

인터페이스 구성 모드에서 인터페이스의 passive 및 deaf 상태를 구성하려면 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| **Ip rip passive** | 해당 인터페이스는 RIP 프로토콜 그룹핑을 전달하지 않습니다. |
| **ip rip deaf** | 해당 인터페이스는 RIP 프로토콜 그룹핑을 수신하지 않습니다. |

### 49.3.8. RIP 인증 활성화

RIP-1 은 인증을 지원하지 않습니다. RIP-2 그룹핑이 전달 및 수신되는 경우 인터페이스에서 RIP 인증을 활성화할 수 있습니다.

RIP 이 활성화된 인터페이스에서 일반 텍스트 인증, MD5 인증, 동적 인증(md5 및 sha1) 등 다양한 인증 모드가 지원됩니다. 각 RIP-2 그룹핑은 기본적으로 일반 텍스트 인증을 사용합니다.

Note:
보안을 고려한다면 RIP 그룹에서 일반 텍스트 인증을 사용하지 마십시오. 암호화되지 않은 인증 키가 각 RIP-2 그룹에 전달되기 때문입니다. 보안이 중요하지 않은 경우 (예: 잘못 구성된 호스트가 경로에 참여할 수 없는 경우) 일반 텍스트 인증을 사용할 수 있습니다.

RIP 일반 텍스트 인증을 구성하려면 인터페이스 구성 모드에서 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| **ip rip authentication simple** | 인터페이스에 일반 텍스트 인증을 구성합니다. |
| **ip rip password** *string* | 일반 텍스트 인증 키를 구성합니다. |

RIP 의 MD5 인증을 구성하려면 인터페이스 구성 모드에서 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| **ip rip authentication md5** | 인터페이스에 MD5 인증을 구성합니다. |
| **ip rip md5-key** *key-ID* **md5** *key* | MD5 인증 키와 인증 ID 를 구성합니다. |

RIP 의 동적 인증을 구성하려면 인터페이스 구성 모드에서 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| **ip rip authentication dynamic** | 인터페이스에 동적 인증(MD5 및 SHA1)을 구성합니다. |
| **ip rip dynamic-key** *key-ID* { **md5 \| sha1** } *key xxxx-xx-xx-xx:xx xx:xx* | 동적 인증 키와 인증 ID 를 구성합니다. |

RIP 인증 구성을 완료한 후 인터페이스 구성 모드에서 다음을 수행합니다.

| 명령 | 설명 |
|---|---|
| **ip rip authentication commit** | 인증에 실패하면 상대방 피어와 상대방으로부터 학습한 경로를 무효화합니다. |

### 49.3.9. 경로 요약 금지

기본적으로 RIP-2 는 클래스 기반 네트워크 경계를 넘을 때 RIP-2 경로를 요약하는 자동 경로 요약을 지원합니다. 그리고 RIP-1 자동 경로 수집 기능은 항상 활성화되어 있습니다.

분리된 서브넷이 있는 경우 이 서브넷을 선언하려면 경로 요약을 금지해야 합니다. 경로 수집이 금지되면 라우터는 클래스 기반 네트워크 경계를 넘을 때 서브넷 및 호스트의 경로 정보를 전송합니다. 라우터 구성 모드에서 자동 수집을 금지하려면 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **no auto-summary** | 자동 요약을 금지합니다. |

### 49.3.10. 발신지 IP 주소 인증 금지

기본적으로 라우터는 수신된 경로 업데이트의 인증 가능한 발신지 IP 주소를 인증합니다. 이 주소가 유효하지 않으면 라우터 업데이트는 거부됩니다.

업데이트를 수신하려는 라우터가 있지만 수신자에서 해당 "network" 또는 "neighbor"를 구성하지 않은 경우 이 기능을 금지해야 합니다. 그러나 일반적으로 이 명령은 사용하지 않는 것이 좋습니다. 라우터 구성 모드에서 다음 명령은 들어오는 경로 업데이트에서 발신지 IP 주소를 인증하는 기본 기능을 금지합니다.

| 명령 | 설명 |
|---|---|
| **no validate-update-source** | 들어오는 RIP 라우터 업데이트의 발신지 IP 주소 인증을 금지합니다. |

### 49.3.11. 최대 경로 개수

기본적으로 로컬 RIP 라우팅 테이블은 최대 1024 개의 경로를 포함할 수 있습니다. 라우팅 테이블의 경로 수가 최대 개수를 초과하면 경로는 라우팅 테이블에 더 이상 추가되지 않습니다.

동시에 사용자에게 라우팅 테이블의 경로 수가 최대 개수에 도달했음을 알립니다. 라우터 구성 모드에서 다음 표의 명령을 실행하여 로컬 RIP 라우팅 테이블의 최대 경로 수를 구성합니다.

| 명령 | 설명 |
|---|---|
| **maximum-count** *number* | 로컬 RIP 라우팅 테이블의 최대 경로 수를 구성합니다. |
| **no maximum-count** | 로컬 RIP 라우팅 테이블의 기본 최대 경로 수를 복원합니다. |

### 49.3.12. Horizontal Split 기능 활성화 또는 금지

일반적으로 IP 네트워크에 연결되어 거리 벡터 라우팅 프로토콜을 사용하는 라우터는 라우팅 루프 가능성을 줄이기 위해 수평 분할(split-horizon)을 사용합니다. 수평 분할은 해당 경로 정보의 수신 인터페이스에 경로 정보를 알리는 것을 방지합니다. 이러한 방식으로 여러 라우터 간의 통신(특히 루프가 끊어질 때)이 최적화됩니다. 그러나 비브로드캐스팅 네트워크(예: Frame Relay)의 경우 상황은 그렇게 간단하지 않습니다. 그리고 수평 분할을 금지해야 할 수도 있습니다.

인터페이스에 보조 IP 주소가 구성되어 있고 수평 분할이 활성화된 경우, 경로 업데이트의 발신지 IP 주소에 모든 보조 IP 주소가 포함되지 않을 수 있습니다. 하나의 경로 업데이트의 발신지 IP 주소에는 하나의 네트워크 번호만 포함됩니다(수평 분할이 금지되지 않은 경우).

수평 분할을 활성화하거나 금지하려면 인터페이스 구성 모드에서 다음 명령을 사용해야 합니다.

| 명령 | 설명 |
|---|---|
| **ip rip split-horizon** | Split- Horizon 활성화 |
| **no ip rip split-horizon** | Split- Horizon 금지 |

기본적인 상황에서, 점대점(Point-to-Point) 인터페이스의 경우 스플릿 호라이즌(Split-Horizon)이 활성화되고, 점대다점(Point-to-Multipoint) 인터페이스의 경우 스플릿 호라이즌이 금지됩니다.

스플릿 호라이즌 사용에 대한 특정 예제는 이 장의 "스플릿 호라이즌 예제" 섹션을 참조합니다.

Notes:
일반적으로, 애플리케이션이 상태를 변경할 때까지 경로를 올바르게 선언할 수 없다고 확신하지 않는 한 기본 상태를 변경하지 않는 것이 좋습니다. 직렬 인터페이스에서 스플릿 호라이즌이

금지되어 있고 (인터페이스가 패킷 교환 네트워크에 연결되어 있는 경우) 해당 네트워크의 관련 멀티캐스트 그룹에 있는 모든 라우터에 대해 스플릿 호라이즌을 금지해야 합니다.

#### 49.3.13. RIP 의 모니터링 및 유지보수

RIP 를 모니터링하고 유지 관리하면 RIP 프로토콜 매개변수 구성, 네트워크 활용률, 네트워크 통신의 실시간 추적 등과 같은 네트워크 통계를 표시할 수 있습니다. 이러한 정보는 네트워크 리소스 사용을 판단하고 네트워크 문제를 해결하며 네트워크 노드의 도달 가능성을 파악하는 데 도움이 될 수 있습니다. 관리 통계에서 다양한 유형의 경로에 대한 통계 정보를 표시하는 데 다음 명령을 사용할 수 있습니다.

| 명령 | 설명 |
|---|---|
| **show ip rip** | RIP 의 현재 상태 표시 |
| **show ip rip** *database* | RIP 의 모든 경로 표시 |
| **Show ip rip protocol** | RIP 프로토콜의 모든 관련 정보 표시 |

관리 모드에서 다음 명령을 사용하여 경로 프로토콜 정보를 추적해야 합니다.

| 명령 | 설명 |
|---|---|
| **Debug ip rip database** | RIP 라우팅 절차 정보 (예: 라우팅 테이블 삽입, 라우팅 테이블 삭제, 경로 변경 등) 추적 |
| **Debug ip rip protocol** | RIP 프로토콜 메시지 추적 |

## 49.4. RIP 설정 예제

RIP 설정 예제는 이 섹션에 포함되어 있습니다.

**〈RouterA〉**

```
interface ethernet 1/1
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
```

```
!

〈RouterB〉

interface ethernet 1/1
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
```

# 50. BEIGRP 설정

이 장에서는 BEIGRP 동적 라우팅 프로토콜의 구성 과정에 대해 자세히 설명합니다.

## 50.1. 개요

BEIGRP 라우팅 프로토콜 간략 소개합니다.

BEIGRP 는 거리 벡터 라우팅 프로토콜과 유사한 기술을 사용합니다.

(1) 라우터는 직접 연결된 이웃이 제공하는 정보만으로 라우팅 결정을 내립니다.
(2) 라우터는 자신이 사용하는 라우팅 정보만 직접 연결된 이웃에게 제공합니다. 그러나 BEIGRP 는 거리 벡터 라우팅 프로토콜과 몇 가지 주요 차이점이 있어 더 많은 장점을 갖습니다.
(3) BEIGRP 는 지금까지의 최적 경로뿐만 아니라 모든 이웃의 모든 경로를 토폴로지 테이블에 저장합니다.
(4) BEIGRP 는 목적지에 접근할 수 없고 대체 경로가 없을 때 이웃에게 쿼리할 수 있으므로 BEIGRP 의 수렴 속도는 최고의 링크 상태 프로토콜과 경쟁할 수 있습니다.

DUAL(Diffused Update Algorithm)의 도입은 BEIGRP 가 다른 기존 거리 벡터 라우팅 프로토콜보다 뛰어난 이유에 매우 중요합니다. DUAL 은 항상 능동적으로 작동하며 목적지에 접근할 수 없고 대체 경로(실현 가능한 대체)가 없을 때 이웃에게 쿼리합니다. 수렴 과정이 수동적(라우터 시간 초과를 수동적으로 기다리는 것)이 아닌 능동적이므로 BEIGRP 의 수렴 속도는 매우 빠릅니다.

BEIGRP 는 EIGRP 의 요구 사항에 맞게 설계되었으며 IP 를 직접 기반으로 하는 특정 라우팅 프로토콜입니다. BEIGRP 는 다음 요구 사항을 충족합니다.

(1) "Hello" 메시지를 통해 새로운 이웃을 동적으로 검색하고 기존 이웃의 소멸을 감지합니다.
(2) 따라서 데이터 전송은 모두 안정적입니다.
(3) 전송 프로토콜은 유니캐스트 및 멀티캐스트 데이터 전송을 허용합니다.
(4) 전송 프로토콜 자체는 네트워크 상태 및 이웃 응답의 변화에 적응할 수 있습니다.

BEIGRP 는 요구 사항에 따라 대역폭 점유율을 제한할 수 있습니다.

## 50.2. BEIGRP 구성 작업 목록

BEIGRP 구성을 완료하려면 다음 작업을 수행해야 하며, 그 중에서 BEIGRP 활성화는 필수적이지만 다른 작업은 필요에 따라 결정할 수 있습니다.

(1) BEIGRP 프로토콜 활성화
(2) 대역폭 공유율 구성

(3) BEIGRP 복합 거리의 산술 계수 조정
(4) "offset"을 사용하여 라우터의 복합 거리 조정
(5) 자동 요약 끄기
(6) 경로 요약 사용자 정의
(7) BEIGRP 의 기타 매개변수 구성
(8) BEIGRP 감독 및 유지 관리

#### 50.2.1. BEIGRP 활성화

BEIGRP 프로세스를 생성하려면 다음 명령을 실행해야 합니다.

| 명령 | 설명 |
|---|---|
| **router beigrp** *as-number* | 전역 설정 모드에서 BEIGRP 프로세스 추가 |
| **network** *network-number network-mask* | 라우터 설정 모드에서 이 BEIGRP 프로세스에 주소 추가 |

위 구성을 마치면 BEIGRP 는 해당 주소에 속한 모든 인터페이스에서 실행을 시작하고, "Hello"를 통해 새로운 이웃을 검색하며, "update"를 통해 초기 라우팅 상호 작용을 수행합니다.

#### 50.2.2. 대역폭 공유율 구성 설정

기본적으로 BEIGRP 는 최대 대역폭의 50%를 점유할 수 있습니다. 다른 데이터의 정상적인 상호 작용을 보장하기 위해 이 기본값을 변경하거나, 인터페이스가 실제 상황에 맞지 않는 대역폭으로 구성된 경우 명령을 통해 BEIGRP 의 실제로 사용 가능한 대역폭을 조정할 수 있습니다. 이러한 경우 인터페이스 구성 모드에서 다음 명령을 사용할 수 있습니다.

| 명령 | 설명 |
|---|---|
| **ip beigrp bandwidth-percent** *percent* | BEIGRP 메시지가 대역폭에서 점유하는 최대 비율을 구성합니다. |

#### 50.2.3. BEIGRP 복합 거리의 산술 계수 조정

특정 상황에서 BEIGRP 복합 거리의 산술 계수를 조정해야 할 수 있으며, 이는 최종적으로 라우터의 라우팅 정책에 영향을 미칩니다. BEIGRP 의 기본 산술 계수는 대부분의 네트워크를 만족시킬 수 있지만, 특정 조건에서는 조정해야 할 수 있습니다. 그러나 이러한 조정은 전체 네트워크에 큰 변화를 가져올 수 있으므로 가장 숙련된 엔지니어가 수행해야 합니다.

라우터 구성 모드에서 다음 명령을 사용합니다:

| 명령 | 설명 |
| --- | --- |
| **metric weights** *k1 k2 k3 k4 k5* | BEIGRP 복합 거리의 산술 계수를 조정합니다. |

### 50.2.4. "Offset"을 사용하여 라우터의 복합 거리를 조정

우리는 오프셋 목록을 사용하여 필요에 따라 모든 수신 및 발신 경로 또는 요구 사항에 맞는 특정 경로의 복합 거리를 의도적으로 추가합니다. 이러한 접근 방식의 목적은 최종적으로 라우터의 라우팅 결과에 영향을 미치고 우리가 예상한 결과를 충족시키는 것입니다. 구성 과정에서 사용자는 어떤 경로에 오프셋 증가 작업을 수행할지 더 명확하게 알 수 있도록 필요에 따라 오프셋 목록에서 접근 목록 또는 애플리케이션 인터페이스를 선택적으로 지정할 수 있습니다.

다음 명령은 아래와 같습니다:

| 명령 | 설명 |
| --- | --- |
| **offset**{type number \| *} {**in** \| **out**} access-list-name offset | 오프셋 목록을 적용합니다. |

### 50.2.5. 자동 요약 끄기

BEIGRP 의 자동 요약은 다른 동적 라우팅 프로토콜과 다르며 다음 규칙을 따릅니다.

(1) BEIGRP 프로세스가 여러 네트워크를 정의할 때, 해당 네트워크의 서브넷 중 하나 이상이 BEIGRP 토폴로지 목록에 존재하는 한, 정의된 네트워크의 요약 경로를 생성합니다.
(2) 설정된 요약 경로는 인터페이스 Null0 을 가리키며, 경로에 포함된 네트워크의 모든 서브넷의 최소 거리를 갖습니다. 요약 경로는 관리 거리 5(구성 불가)로 기본 IP 라우팅 테이블에 삽입됩니다.
(3) 다른 기본 IP 네트워크의 이웃에게 업데이트를 보낼 때, 규칙 1 과 규칙 2 에 의해 요약된 서브넷은 취소되고 요약 경로만 전송됩니다.
(4) BEIGRP 프로세스 정의에 나열되지 않은 네트워크의 서브넷에 대해서는 요약을 수행하지 않습니다.

특정 네트워크 상황에서는 모든 세부 경로를 이웃에게 보고해야 할 수 있으며, 다음 명령을 사용할 수 있습니다:

| 명령 | 설명 |
| --- | --- |
| **no auto-summary** | 경로의 자동 요약을 끕니다. |

### 50.2.6. 경로 요약 사용자 정의

자동 요약이 요구 사항을 충족하지 못할 때, BEIGRP 를 실행하는 각 인터페이스에서 경로 요약을 구성하고 요약을 수행해야 하는 대상 주소를 지정할 수 있습니다. 요약에 대해 구성된 인터페이스는 이 요약 주소에 속하는 서브넷의 구체적인 업데이트 정보를 보내지 않지만 다른 인터페이스는 영향을 받지 않습니다.

여기서 요약 작업은 다음 규칙을 따릅니다.

(1) 인터페이스가 요약에 대해 구성되면 이 네트워크가 BEIGRP 토폴로지 목록에 하나 이상의 서브넷을 가지고 있는 한 정의된 네트워크의 요약 경로를 생성합니다.
(2) 요약 경로는 인터페이스 Null0 을 가리키며, 경로에 포함된 네트워크의 모든 서브넷의 최소 거리를 갖습니다. 요약 경로는 관리 거리 5(구성 불가)로 기본 IP 라우팅 테이블에 삽입됩니다.
(3) 요약 범위를 사용하여 구성된 인터페이스에서 경로 업데이트를 보낼 때, 요약 주소에 속하는 구체적인 경로는 취소됩니다. 다른 인터페이스에 대한 업데이트는 영향을 받지 않습니다.

| 명령 | 설명 |
|---|---|
| **ip beigrp** *summary-address as-number address mask* | 인터페이스에서 경로 요약을 구성합니다. |

### 50.2.7. 다른 경로 BEIGRP 프로세스 재분배

재분배 작업은 다음 규칙을 따릅니다.

(1) 정적 경로와 연결된 경로를 재분배할 때 "default-metric" 명령을 구성할 필요가 없습니다. 관련 매개변수(예: 대역폭, 지연, 안정성, 부하 및 MTU)는 관련 인터페이스에서 가져옵니다.
(2) 다른 BEIGRP 프로세스의 경로를 재분배할 때 "default-metric" 명령을 구성할 필요가 없습니다. 관련 매개변수는 재분배된 BEIGRP 프로세스에서 가져옵니다.
(3) 다른 프로토콜(예: RIP, OSPF)의 경로를 재분배할 때는 "default-metric" 명령을 구성해야 합니다. 관련 매개변수는 "default-metric" 구성에 의해 검증됩니다. "default-metric" 명령 없이 이러한 유형의 경로를 재분배하면 재분배가 작동하지 않습니다.

BEIGRP 프로토콜과 RIP 프로토콜을 실행하는 라우터에서 RIP 프로토콜의 경로를 BEIGRP 프로토콜로 가져와야 할 때 다음 명령을 구성해야 합니다.

| 명령 | 설명 |
|---|---|
| **default-metric** bandwidth delay reliability loading mtu | 재분배의 기본 매개변수 구성 |

| | |
|---|---|
| **redistribute** protocol [process] [**route-map** name] | 경로를 BEIGRP 프로토콜로 재분배 |

### 50.2.8. BEIGRP 의 다른 매개변수 구성

다양한 네트워크 환경에 적응하고 BEIGRP 가 보다 효과적이고 완전하게 작동하도록 하기 위해 다음 매개변수를 조정해야 할 수 있습니다.

(1) "hello" 메시지를 보내는 BEIGRP 의 시간 간격과 이웃의 타임아웃 소멸 시간 조정
(2) 스플릿 호라이즌 끄기

**"hello" 메시지를 보내는 BEIGRP 의 시간 간격 및 이웃의 타임아웃 소멸 시간 조정**

BEIGRP hello 프로토콜은 올바른 BEIGRP 작동을 가능하게 하기 위해 3 가지 목표를 달성합니다.

(1) 접근 가능한 새로운 이웃을 발견합니다. 검색은 자동이며 수동 구성이 필요하지 않습니다.
(2) 이웃의 구성을 확인하고 호환 모드로 구성된 이웃과의 통신만 허용합니다.
(3) 이웃의 가용성을 계속 유지하고 이웃의 소멸을 감지합니다.

라우터는 BEIGRP 를 실행하는 모든 인터페이스에서 "hello" 멀티캐스트 패킷을 보냅니다. 모든 라우터는 이러한 멀티캐스트 그룹을 수신하는 것을 지원하므로 모든 이웃을 검색할 수 있습니다.

"Hello" 프로토콜은 두 개의 타이머를 사용하여 이웃의 소멸을 감지합니다. hello 간격은 라우터의 인터페이스에서 BEIGRP hello 메시지를 보내는 빈도를 정의하고, hold 타이머는 라우터가 지정된 이웃으로부터 통신 데이터를 기다려야 하는 시간 간격을 정의하며, 이 시간이 지나면 이웃의 소멸을 선언합니다. 우리는 이웃 라우터로부터 BEIGRP 패킷을 받을 때마다 hold 타이머를 재설정하도록 했습니다.

서로 다른 네트워크 유형 또는 네트워크 대역폭은 hello 타이머의 서로 다른 기본값을 사용합니다:

| Interface type encapsulation | | Hello timer (second) | Hold timer (second) |
|---|---|---|---|
| LAN interface | Any | 5 | 15 |
| WAN interface | HDLC or PPP | 5 | 15 |
| | NBMA interface, bandwidth<=T1 | 60 | 180 |
| | NBMA interface, bandwidth>T1 | 5 | 15 |
| | The point-to-point sub-interface of NBMA interface | 5 | 15 |

Hello 프로토콜 타이머의 기본값 차이로 인해 서로 다른 IP 서브넷에 연결된 BEIGRP 이웃이 서로 다른 hello 및 hold 타이머를 사용할 수 있습니다. 이 문제를 해결하기 위해 모든 라우터의 hello 패킷은 자체 hold 타이머를 지정하며, 모든 BEIGRP 라우터는 hello 그룹의 이웃이 지정한 hold 타이머를 사용하여 이웃의 시간 초과를 결정합니다. 이를 통해 동일한 WAN 네트워크의 서로 다른 지점에서 서로 다른 이웃 오류 감지 타이머가 나타날 수 있습니다. 그러나 특정 상황에서는 타이머의 기본값을 충족할 수 없으므로 hello 메시지 전송 간격을 조정하려면 다음 명령을 사용합니다.

| 명령 | 설명 |
|---|---|
| **ip beigrp hello-interval** *seconds* | 이 인터페이스에서 hello 메시지를 보내는 시간 간격을 조정합니다. |

이웃의 타임아웃 타이머를 조정하려면 다음 명령을 사용합니다.

| 명령 | 설명 |
|---|---|
| **ip beigrp hold-time** *seconds* | 이웃의 타임아웃 소멸 시간(또는 연결 끊김 시간)을 조정합니다. |

**스플릿 호라이즌 끄기**

일반적으로 스플릿 호라이즌을 사용하는 것을 선호합니다. 스플릿 호라이즌은 하나의 인터페이스에서 나간 라우팅 정보가 동일한 인터페이스로 다시 브로드캐스트되는 것을 방지하여 라우팅 루프를 피합니다. 그러나 특정 상황에서는 이것이 최적의 선택이 아닐 수 있으며, 이 경우 다음 명령을 사용하여 스플릿 호라이즌을 비활성화할 수 있습니다.

| 명령 | 설명 |
|---|---|
| **no ip beigrp split-horizon** | horizontal split 비활성화 |

### 50.2.9. BEIGRP 모니터링 및 유지 관리

모든 이웃과의 이웃 관계를 지우려면 다음 명령을 사용합니다.

| 명령 | 설명 |
|---|---|
| **clear ip beigrp neighbors** [*as-number* \| *interface*] | 모든 이웃과의 이웃 관계를 삭제합니다. |

BEIGRP 의 다양한 통계 정보를 표시하려면 다음 명령을 실행합니다.

| 명령 | 설명 |
|---|---|
| **show ip beigrp interfaces** [*interface*] *[as-number*] | 인터페이스 정보 표시 |

| | |
|---|---|
| **show ip beigrp neighbors** [*as-number* | *interface*] | 이웃 정보 표시 |
| **show ip beigrp topology** [*as-number* | all-link | summary | active] | 토폴로지 정보 표시 |

## 50.3. BEIGRP 설정 예시

다음 예제에서 이더넷 1/1 인터페이스는 10.0.0.0/8 주소의 요약 경로를 전송하도록 구성되며, 이 주소에 속하는 모든 서브넷 경로는 해당 인터페이스를 통해 이웃에 광고되지 않습니다. 동시에 BEIGRP 프로세스의 자동 요약 기능은 비활성화됩니다.

```
interface Ethernet 1/1
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
```

# 51. OSPF 설정

## 51.1. 개요

이 장에서는 OSPF 구성에 대해 소개합니다. 모든 OSPF 명령에 대한 더 구체적인 자세한 정보는 "네트워크 프로토콜 구성 참조"의 OSPF 명령 관련 섹션을 참조합니다.

OSPF 는 IETF 의 OSPF 워킹 그룹에서 개발한 IGP(Interior Gateway Protocol, 내부 게이트웨이 프로토콜) 라우팅 프로토콜입니다. IP 네트워크용으로 설계된 OSPF 는 IP 서브넷과 외부 경로 정보 레이블을 지원하며, 동시에 메시지 인증을 허용하고 IP 멀티캐스트를 지원합니다.
당사에서 구현한 OSPF 는 OSPF V2 사양(RFC2328 참조)을 준수합니다.

구현의 몇 가지 주요 특징은 다음과 같습니다.

(1) Stub Area(스텁 영역): 스텁 영역 지원
(2) Route redistribution(경로 재분배): 라우팅 프로토콜에 의해 생성되고 학습된 모든 경로는 항상 다른 라우팅 프로토콜 도메인으로 재분배될 수 있습니다. 자율 시스템 내에서 이는 OSPF 가 RIP 에서 학습한 경로를 입력할 수 있음을 의미합니다. 또한 OSPF 에서 학습한 경로는 RIP 으로 재분배될 수 있습니다. 자율 시스템 간에 OSPF 는 BGP 에서 학습한 경로를 입력할 수 있으며, OSPF 경로는 BGP 로도 주입될 수 있습니다.
(3) Authentication(인증): 영역 내의 인접 라우터 간에 일반 텍스트 및 MD5 인증이 지원됩니다.
(4) Router Interface Parameters(라우터 인터페이스 매개변수): 구성 가능한 매개변수에는 Outgoing Cost(나가는 비용), Retransmission Interval(재전송 간격), Interface Transmission Delay(인터페이스 전송 지연), router Priority(라우터 우선순위), Judgement on the router Switching-off Interval(라우터 종료 간격 판단), the Interval of Hello Message(Hello 메시지 간격) 및 Authentication Password(인증 비밀번호)가 포함됩니다.
(5) Virtual Link(가상 링크): 가상 링크 지원
(6) NSSA area(NSSA 영역): RFC 1587 참조
(7) OSPF---가상 회선에 대한 RFC 1793

## 51.2. OSPF 구성 작업 목록

OSPF 는 영역 내의 모든 라우터, ABR 및 ASBR 간에 라우팅 데이터를 교환해야 합니다. 구성을 단순화하기 위해 인증 등을 사용하지 않고 모든 라우터가 기본 매개변수에서 작동하도록 할 수 있지만, 일부 매개변수를 변경하려면 모든 라우터에서 매개변수의 동일성을 보장해야 합니다.

OSPF 를 구성하려면 다음 작업을 완료합니다. OSPF 활성화의 필요성 외에 다른 구성은 모두 선택 사항입니다.

(1) OSPF 시작
(2) OSPF 의 인터페이스 매개변수 구성
(3) 서로 다른 물리적 네트워크에서 OSPF 구성
(4) OSPF 도메인 내에서 경로 요약 구성
(5) 전달 라우터 수집 구성
(6) 기본 경로 생성
(7) LOOPBACK 인터페이스를 통해 라우터 ID 선택
(8) OSPF 의 관리 거리 구성
(9) 경로 계산 타이머 구성
(10) OSPF 감독 및 유지 관리

또한 경로 재분배 구성에 대해서는 "IP 라우팅 프로토콜의 프로토콜 독립적 특징 구성"의 "경로 재분배" 관련 내용을 참조합니다.

## 51.3. OSPF 설정 작업

### 51.3.1. OSPF 시작

다른 라우팅 프로토콜과 마찬가지로 OSPF 를 활성화하려면 OSPF 라우팅 프로세스를 생성하고, 실행 중인 프로세스와 관련된 IP 주소 범위를 할당하며, IP 주소 범위와 관련된 영역 ID 를 할당해야 합니다. 전역 구성 모드에서 다음 명령을 사용합니다.

| 명령 | 설명 |
|---|---|
| **router ospf** *process-id* | 이 명령은 OSPF 라우팅 프로토콜을 활성화하고 라우터 구성 모드로 진입합니다. |
| **network** *address mask* **area** *area-id* | 이 명령은 OSPF 를 실행하는 인터페이스와 인터페이스의 영역 ID 를 구성합니다. |

### 51.3.2. OSPF 인터페이스 매개변수 구성

OSPF 를 구현하는 동안 필요에 따라 인터페이스와 관련된 OSPF 매개변수를 변경할 수 있습니다. 어떤 매개변수도 변경할 필요는 없지만, 연결된 네트워크의 모든 라우터에서 특정 매개변수의 동일성을 보장해야 합니다.

인터페이스 구성 모드에서 다음 명령을 사용하여 인터페이스 매개변수를 구성합니다.

| 명령 | 설명 |
|---|---|
| **ip ospf cost** *cost* | OSPF 인터페이스의 메트릭을 구성하여 패킷을 전달합니다. |

| | |
|---|---|
| **ip ospf retransmit-interval** *seconds* | 동일한 OSPF 인터페이스에 속한 이웃 간에 LSA 를 재전송하는 데 걸리는 시간(초 단위). |
| **ip ospf transmit-delay** *seconds* | OSPF 인터페이스에서 LSA 를 전송하는 데 걸리는 예상 시간(초 단위)을 구성합니다. |
| **ip ospf priority** *number* | DR 라우터가 되기 위한 라우터의 우선순위를 구성합니다. |
| **ip ospf hello-interval** *seconds* | OSPF 인터페이스에서 hello 패킷을 보내는 시간 간격을 구성합니다. |
| **ip ospf dead-interval** *seconds* | 라우터가 정의된 시간 간격 내에 이웃으로부터 "hello" 패킷을 받지 못하면 이웃 라우터가 꺼진 것으로 간주합니다. |
| **ip ospf authentication-key** *key* | OSPF 의 단순 비밀번호 인증을 사용하는 주소의 인접 라우터 인증 비밀번호입니다. |
| **ip ospf message-digest-key** *keyid* **md5** *key* | OSPF 가 MD5 인증을 사용하도록 요구합니다. |
| **ip ospf passive** | 인터페이스에서 "hello" 메시지를 보내지 않습니다. |

### 51.3.3. OSPF 네트워크 유형 구성

네트워크의 물리적 매체 유형에 관계없이 네트워크를 브로드캐스팅 네트워크 또는 비브로드캐스팅, 멀티 액세스 네트워크로 구성할 수 있습니다. 이 기능을 사용하면 네트워크를 유연하게 구성할 수 있습니다. 물리적 브로드캐스팅 네트워크를 비브로드캐스팅, 멀티 액세스 네트워크로 구성할 수 있으며, 비브로드캐스팅 네트워크(X.25, 프레임 릴레이 및 SMDS)를 브로드캐스팅 네트워크로 구성할 수도 있습니다. 이 기능은 이웃 구성을 줄여줍니다. 자세한 내용은 OSPF 의 비브로드캐스팅 네트워크 구성 관련 내용을 참조합니다.

비브로드캐스팅, 멀티 액세스 네트워크를 브로드캐스팅 네트워크 또는 비브로드캐스팅 네트워크로 구성하는 것은 모든 라우터에서 다른 라우터로 가상 링크가 존재한다고 가정하거나, 모든 라우터가 완전 메시 네트워크를 구성한다고 가정하는 것과 같습니다. 비용 제약으로 인해 일반적으로 실용적이지 않거나 부분적으로 완전 메시 네트워크일 수 있습니다. 이러한 상황에서 point-to-multipoint 네트워크를 구성할 수 있습니다. 서로 인접하지 않은 라우터는 가상 링크를 통해 라우팅 정보를 교환할 수 있습니다.

OSPF point-to-multipoint 인터페이스는 여러 개의 호스트 경로를 생성하는 여러 개의 point-to-point 네트워크 인터페이스로 정의할 수 있습니다. OSPF point-to-multipoint 네트워크는 비브로드캐스팅, 멀티 액세스 네트워크 및 point-to-point 네트워크에 비해 다음과 같은 장점이 있습니다.

(1) Point-to-multipoint 네트워크는 구성하기 쉽고, 이웃 구성 명령이 필요하지 않으며, 하나의 IP 만 사용하고 DR 을 생성하지 않습니다.
(2) 완전 메시 네트워크 토폴로지가 필요하지 않으므로 비용이 적게 듭니다.
(3) 안정성이 더 높습니다. 가상 링크가 실패하더라도 연결을 유지할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 사용하여 OSPF 네트워크 유형을 구성합니다.

| 명령 | 설명 |
|---|---|
| **ip ospf network** {**broadcast** \| **non-broadcast** \| {**point-to-multipoint** [**non-broadcast**] }} | 이 명령은 OSPF 의 네트워크 유형을 구성합니다. |

이 장의 마지막 부분에서 OSPF point-to-multipoint 네트워크 구성 예제를 볼 수 있습니다.

### 51.3.4. One-to-Multiple Broadcast 네트워크 설정

point-to-multipoint 네트워크와 브로드캐스팅 네트워크에서는 이웃 관계를 설명할 필요가 없습니다. 그러나 "neighbor" 명령을 사용하여 특정 이웃의 우선순위를 설명할 수 있습니다.

이 명령을 사용하기 전에 일부 OSPF point-to-multipoint 프로토콜 트래픽은 멀티캐스트 트래픽입니다. 따라서 point-to-multipoint 인터페이스의 경우 "neighbor" 명령이 필요하지 않습니다. "hello" 패킷, 업데이트 패킷 및 확인 패킷은 모두 브로드캐스팅 형식을 통해 전송되며, 특히 멀티캐스트 "hello" 패킷은 모든 이웃을 동적으로 검색할 수 있습니다.

point-to-multipoint 네트워크에서 라우터는 모든 이웃이 동일한 메트릭을 가지고 있다고 가정합니다. 이 값은 "ip ospf cost" 명령을 통해 구성할 수 있습니다. 실제로 모든 이웃의 대역폭은 다르므로 값도 달라야 합니다. 이 기능은 point-to-multipoint 인터페이스에만 적용됩니다.

다음 명령을 사용하여 인터페이스를 point-to-multipoint 인터페이스로 구성하고 각 이웃에 대한 메트릭을 할당합니다:

| 명령 | 설명 |
|---|---|
| **ip ospf network point-to-multipoint** | 브로드캐스팅 매체에서 인터페이스를 point-to-multipoint 네트워크로 구성합니다. |
| **Exit** | 전역 구성 모드로 돌아갑니다. |
| **router ospf** *process-id* | OSPF 라우터 프로세스를 구성하고 라우터 구성 모드로 들어갑니다. |
| **neighbor** *ip-address* cost *number* | 이웃을 지정하고 해당 이웃에 메트릭을 할당합니다. |

각 이웃의 메트릭을 지정하려면 4 단계를 반복합니다. 그렇지 않으면 "ip ospf cost" 명령으로 지정된 값을 사용합니다.

### 51.3.5. Non-Broadcasting 네트워크 설정

OSPF 네트워크에는 많은 라우터가 있으므로 네트워크를 위해 DR(Designated Router, 지정 라우터)이 선출되어야 합니다. 브로드캐스팅 기능이 구성되지 않은 경우 선택 프로세스에 대한 매개변수 구성을 수행해야 합니다.
이러한 매개변수는 DR 또는 BDR 이 될 자격이 있는 라우터에서만 구성됩니다.

라우터 구성 모드에서 다음 명령을 사용하여 서로 관련된 비브로드캐스팅 네트워크의 라우터를 구성합니다.

| 명령 | 설명 |
|---|---|
| **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*] | 비브로드캐스팅 네트워크에 연결된 라우터를 구성합니다. |

이웃 라우터에 대해 다음 매개변수를 지정할 수 있습니다.

(1) 이웃 라우터의 우선순위
(2) 비브로드캐스팅 폴링 간격
(3) 이웃에 접근 가능한 인터페이스

point-to-multipoint, 비브로드캐스팅 네트워크에서 "neighbor" 명령을 사용하여 이웃 관계를 지정할 수 있습니다. 선택적 우선순위를 할당합니다.

이전 소프트웨어 버전에서 일부 사용자는 비브로드캐스팅 매체(IP over ATM)에서 point-to-multipoint 연결을 구성했으므로 라우터가 이웃 라우터를 동적으로 검색할 수 없었습니다. 이 기능을 사용하면 point-to-multipoint 인터페이스에서 "neighbor" 명령을 사용할 수 있습니다.

point-to-multipoint 네트워크에서 라우터는 모든 이웃이 동일한 메트릭을 가지고 있다고 가정합니다. 이 값은 "ip ospf cost" 명령을 통해 구성할 수 있습니다. 실제로 각 이웃의 대역폭이 다르므로 값도 달라야 합니다. 이 기능은 point-to-multipoint 인터페이스에만 적용됩니다.

브로드캐스팅을 지원하지 않는 매체에서 point-to-multipoint 인터페이스를 구성하려면 인터페이스 구성 모드에서 다음 명령을 사용하십시오.

| 명령 | 설명 |
|---|---|
| **ip ospf network point-to-multipoint non-broadcast** | 비브로드캐스팅 매체에서 point-to-multipoint 인터페이스를 구성합니다. |
| **Exit** | 전역 구성 모드로 진입합니다. |
| **router ospf** *process-id* | OSPF 라우팅 프로세스를 생성하고 라우터 구성 모드로 진입합니다. |

| | |
|---|---|
| **neighbor** *ip-address* [**cost** *number*] | OSPF 이웃을 지정하고 해당 이웃에 메트릭을 할당합니다. |

각 이웃에 대해 4 단계를 반복합니다.

### 51.3.6. OSPF domain 설정

구성 가능한 영역 매개변수에는 인증, 스텁 영역 지정, 기본 요약 경로에 대한 메트릭 지정이 포함됩니다. 인증은 비밀번호 기반 보호를 채택합니다.

스텁 영역은 외부 경로를 배포하지 않는 영역입니다. 대신 ABR(Area Border Router, 영역 경계 라우터)은 스텁 영역으로 들어가는 기본 외부 경로를 생성하여 스텁 영역이 자율 시스템의 외부 네트워크에 진입할 수 있도록 합니다. OSPF 스텁 지원 기능을 활용하려면 스텁 영역에서 기본 경로를 사용해야 합니다. 스텁 영역으로 전송되는 LSA(Link State Advertisement, 링크 상태 광고) 수를 추가로 줄이기 위해 ABR 수집을 금지하여 스텁 영역으로 들어가는 요약 LSA(type3) 전송을 줄일 수 있습니다.

라우터 구성 모드에서 다음 명령을 사용하여 영역 매개변수를 정의합니다.

| 명령 | 설명 |
|---|---|
| **area** *area-id* **authentication simple** | OSPF 영역 인증을 활성화합니다. |
| **area** *area-id* **authentication message-digest** | OSPF 가 MD5 를 사용하여 인증하도록 설정합니다. |
| **area** *area-id* **stub** [**no-summary**] | 스텁 영역을 정의합니다. |
| **area** *area-id* **default-cost** *cost* | 스텁 영역의 기본 경로에 대한 메트릭을 설정합니다. |

### 51.3.7. OSPF 의 NSSA 구성

NSSA 는 스텁 영역과 유사합니다. 그러나 NSSA 영역은 외부 경로의 진입을 허용합니다. 경로 요약 및 패킷 필터링 또한 전송 중에 지원됩니다. ISP 가 다른 라우팅 프로토콜을 사용하여 원격 네트워크를 사용해야 하는 경우 NSSA 는 관리를 단순화할 수 있습니다.

엔터프라이즈-코어 경계 라우터는 NSSA 가 적용되지 않은 경우 OSPF 의 스텁 영역에서 실행될 수 없습니다. 원격 네트워크의 경로는 스텁 영역으로 전달될 수 없기 때문입니다. RIP 과 같은 단순 라우팅 프로토콜은 광고될 수 있지만 두 종류의 라우팅 프로토콜을 유지해야 합니다. NSSA 는 중앙 라우터와 원격 라우터를 동일한 NSSA 영역에 배치할 수 있으며, OSPF 는 원격 네트워크에 적용될 수 있습니다.

NSSA 영역을 사용할 때 ABR 라우터에서 생성된 경로는 NSSA 가 구성되면 NSSA 영역에 들어갈 수 있습니다. 동일한 영역의 각 라우터는 자신이 NSSA 영역에 있음을 인정해야 하며, 그렇지

않으면 다른 라우터와 통신할 수 없습니다. 라우터의 패킷 전송 혼란을 피하기 위해 ABR 에서 표시된 릴리스를 사용해야 합니다.

OSPF 의 NSSA 영역을 설정하려면 라우터 구성 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| **Area area-id nssa** [**no-redistribution**] [**no-summary**] [**default-information-originate**] | OSPF NSSA 영역을 구성합니다. |

### 51.3.8. OSPF 도메인 내에서 경로 요약 구성

이 기능을 사용하면 ABR 이 다른 영역으로 요약 경로를 브로드캐스트할 수 있습니다. OSPF 에서 ABR 은 모든 네트워크를 다른 영역으로 브로드캐스트합니다. 네트워크 번호를 특정 방법에 따라 할당하고 연속적으로 할당할 수 있는 경우 ABR 이 다른 영역으로 요약 경로를 브로드캐스트하도록 구성할 수 있습니다. 요약 경로는 특정 범위 내의 모든 네트워크를 포함할 수 있습니다.

라우터 구성 모드에서 다음 명령을 사용하여 주소 범위를 정의합니다:

| 명령 | 설명 |
|---|---|
| **area** *area-id* **range** *address mask* | 경로 요약의 주소 범위를 정의합니다. |

### 51.3.9. 전달 라우터 수집 구성

다른 라우터 영역에서 OSPF 라우터 영역으로 경로를 분배할 때 각 라우터는 외부 LSA 형태로 독립적인 브로드캐스팅을 수행합니다. 그러나 특정 주소 범위를 포함하는 경로를 브로드캐스트하도록 라우터를 구성할 수 있습니다. 이 방법을 사용하면 OSPF 링크 상태 데이터베이스의 크기를 줄일 수 있습니다.

라우터 구성 모드에서 다음 명령을 사용하여 라우터 수집을 구성합니다.

| 명령 | 설명 |
|---|---|
| **summary-address** *prefix mask* [**not advertise**] | 분배 경로를 포함하는 주소와 마스크를 설명합니다.<br>하나의 수집 경로만 브로드캐스트됩니다. |

### 51.3.10. 기본 라우팅 생성

ASBR(Autonomous System Boundary Router, 자율 시스템 경계 라우터)이 OSPF 라우팅 영역으로 진입하는 기본 경로를 생성하도록 요청할 수 있습니다. 라우터가 OSPF 도메인으로 진입하는 경로를 분배하도록 구성할 때마다 이 라우터는 자동으로 ASBR 로 변경됩니다. 그러나 ASBR 은 기본적으로 OSPF 라우팅 영역으로 진입하는 기본 경로를 생성하지 않습니다.

라우터 구성 모드에서 다음 명령을 사용하여 ASBR 이 기본 경로를 생성하도록 강제합니다:

| 명령 | 설명 |
|---|---|
| **default-information originate** [**always**] [**route-map** *map-name*] | ASBR 이 OSPF 라우팅 영역으로 진입하는 기본 경로를 생성하도록 강제합니다. |

### 51.3.11. 루프백 인터페이스를 통한 라우터 ID 선택

OSPF 는 인터페이스에 구성된 가장 큰 IP 주소를 라우터 ID 로 사용합니다. 이 IP 주소에 연결된 인터페이스가 DOWN 상태로 변경되거나 IP 주소가 삭제되면 OSPF 프로세스가 다시 시작되어 새 라우터 ID 를 계산하고 모든 인터페이스에서 라우팅 정보를 다시 보냅니다.

루프백 인터페이스가 IP 주소로 구성된 경우 라우터는 해당 IP 주소를 라우터 ID 로 사용합니다. 루프백 인터페이스는 절대 Down 상태가 되지 않으므로 라우팅 테이블이 더욱 안정적으로 유지됩니다.

라우터는 루프백 인터페이스를 라우터 ID 로 사용하는 것을 선호하며, 모든 루프백 인터페이스 중에서 가장 큰 IP 주소를 라우터 ID 로 선택합니다. 루프백 인터페이스가 없으면 라우터의 가장 큰 IP 주소를 사용합니다. OSPF 가 특정 인터페이스를 사용하도록 지정할 수는 없습니다.

전역 모드에서 다음 명령을 사용하여 IP 루프백 인터페이스를 구성합니다.

| 명령 | 설명 |
|---|---|
| **interface loopback 0** | Create a loopback interface and enter into interface configuration mode. |
| **ip address** *ip-address mask* | Allocate an IP address for the interface. |

### 51.3.12. OSPF 관리 거리 구성

관리 거리는 라우터 또는 라우터 그룹과 같은 라우팅 정보 소스의 신뢰도 수준으로 정의됩니다.

일반적으로 관리 거리는 0-255 사이의 정수이며, 값이 클수록 신뢰도 수준이 낮아집니다. 관리 거리가 255 이면 경로 정보 소스를 신뢰할 수 없으므로 무시해야 합니다.

OSPF 는 3 가지 유형의 관리 거리를 사용합니다. 즉, 도메인 간, 도메인 내 및 외부입니다. 영역 내의 경로는 도메인 내 경로이고, 다른 영역으로의 경로는 도메인 간 경로이며, 다른 라우팅 프로토콜 도메인에서 분배된 경로는 외부 경로입니다. 모든 종류의 경로의 기본값은 110 입니다.

라우터 구성 모드에서 다음 명령을 사용하여 OSPF 의 거리 값을 구성합니다:

| 명령 | 설명 |
| --- | --- |
| **distance ospf** [**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*] | OSPF 내부 도메인, 외부 도메인 및 외부 경로의 관리 거리 값을 변경합니다. |

### 51.3.13. 경로 계산 타이머 구성

OSPF 가 토폴로지 변경 정보를 수신한 시점과 SPF 계산을 시작하는 시점 사이의 시간 지연을 구성할 수 있습니다. 또한 두 번의 연속적인 SPF 계산 간의 간격을 구성할 수도 있습니다

라우터 구성 모드에서 다음 명령을 사용하여 구성합니다:

| 명령 | 설명 |
| --- | --- |
| **timers delay** *delaytime* | 영역 내 경로 계산의 시간 지연을 설정합니다. |
| **timers hold** *holdtime* | 영역 내 경로 계산의 최소 시간 간격을 설정합니다. |

### 51.3.14. The On Demand Link 설정

온디맨드 회선상의 OSPF 는 OSPF 의 업그레이드 버전으로, 온디맨드 다이얼링 네트워크 서핑의 경우 프로토콜을 더욱 효율적으로 사용할 수 있도록 합니다. OSPF 프로토콜은 연결이 처음 설정되거나 패킷에 포함된 정보가 변경된 후 연결된 라우터 간에 HELLO 패킷과 링크 상태 브로드캐스트 새로 고침 패킷을 정기적으로 교환합니다. 이는 최소 스패닝 트리가 다시 계산되고 토폴로지가 실제로 변경된 경우에만 패킷이 전송됨을 의미합니다.

라우터 간의 point-to-point 연결인 경우 한쪽 종단에서 구성을 수행해야 합니다. 물론 다른 쪽 종단의 라우터는 이 특성을 지원해야 합니다. 라우터 간의 point-to-multipoint 연결인 경우 multipoint 종단에서 구성을 수행해야 합니다.

스텁 영역에서 온디맨드 다이얼링을 구성하는 것이 좋습니다. 스텁 영역의 각 라우터에서 이 속성이 구성되면 스텁 영역 외부의 라우터는 온디맨드 다이얼링을 지원하지 않아도 됩니다. 온디맨드 다이얼링이 표준 영역에서 구성된 경우 다른 표준 영역은 이 특성을 지원해야 합니다. 두 번째 종류의 외부 링크 상태 브로드캐스트 패킷이 모든 영역에서 브로드캐스트되기 때문입니다.

브로드캐스트 기반 네트워크에서 이 특성이 구성되면 링크 상태 브로드캐스트 패킷은 제한될 수 있지만 HELLO 패킷은 제한될 수 없습니다. HELLO 패킷은 이웃 관계를 유지하고 DR 을 선택하는 데 사용되기 때문입니다.

인터페이스 모드에서 다음 명령을 실행하십시오.

| 명령 | 설명 |
|---|---|
| ip ospf demand-circuit | Configures OSPF on-demand dialing. |

#### 51.3.15. OSPF 모니터링 및 유지관리

네트워크의 통계 정보를 표시할 수 있습니다. 예를 들어 IP 라우팅 테이블, 캐시 및 데이터베이스의 내용에 대한 통계 등이 있습니다. 이 정보는 네트워크 리소스 활용도를 판단하고 네트워크 문제를 해결하는 데 도움이 될 수 있습니다. 또한 네트워크 노드의 가용성을 이해하고 네트워크 데이터 패킷이 네트워크를 통과하는 경로를 파악할 수 있습니다.

다음 명령을 사용하여 다양한 라우팅 통계를 표시합니다.

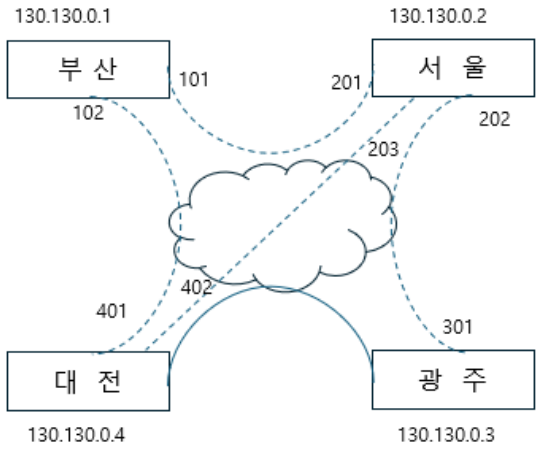
| 명령 | 설명 |
|---|---|
| **show ip ospf** [*process-id*] | OSPF 라우팅 프로세스에 대한 일반 정보를 표시합니다. |
| **show ip ospf** *process-id* [**database** [**router**\|**network**\|**summary**\|**asbr-summary**\|**external**\|**database-summary**]] [*link-state-id*] [**self-originate**] | OSPF 데이터베이스와 관련된 정보를 표시합니다. |
| **show ip ospf border-routers** | ABR 및 ASBR 의 내부 라우팅 테이블 항목을 표시합니다. |
| **show ip ospf interface** | OSPF 인터페이스에 대한 정보를 표시합니다. |
| **show ip ospf neighbor** | 인터페이스에 따라 OSPF 이웃 정보를 표시합니다. |
| **debug ip ospf adj** | OSPF 의 인접 관계 설정을 감시합니다. |
| **debug ip ospf events** | OSPF 의 인터페이스 및 이웃 이벤트를 감시합니다. |
| **debug ip ospf flood** | OSPF 데이터베이스의 플러딩 프로세스를 감시합니다. |
| **debug ip ospf lsa-generation** | OSPF 의 LSA 생성을 감시합니다. |
| **debug ip ospf packet** | OSPF 메시지를 감시합니다. |
| **debug ip ospf retransmission** | OSPF 의 메시지 재전송 프로세스를 감시합니다. |
| **debug ip ospf spf** [**intra**\|**external**] | OSPF 의 SPF 계산 경로를 감시합니다. |
| **debug ip ospf tree** | OSPF 의 SPF 트리 구축을 감시합니다. |

## 51.4. OSPF 설정 예시

다음은 OSPF 구성의 예입니다.

#### 51.4.1. OSPF one to multi Point 설정 예시

서울 DLCI 201 을 사용하여 부산과 통신하고, DLCI 202 를 사용하여 광주와 통신하며, DLCI 203 을 사용하여 대전 과 통신합니다. 부산은 DLCI 101 을 사용하여 서울 과 통신하고, DLCI 102 를 사용하여 대전 과 통신합니다. 대전은 DLCI 401 을 통해 부산 과 통신하고, DLCI 402 를 통해 서울 과 통신할 수 있습니다. 광주는 DLCI 301 을 통해 서울 과 통신할 수 있습니다.




**The configuration of 서울:**

Hostname 서울
!
interface serial 1/0
ip address 130.130.0.2 255.255.0.0
encapsulation frame-relay
frame-relay map 130.130.0.1 pvc 201 broadcast
frame-relay map 130.130.0.3 pvc 202 broadcast
frame-relay map 130.130.0.4 pvc 203 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0

**The configuration of 부산:**

hostname 부산
!
interface serial 1/0
ip address 130.130.0.1 255.0.0.0
encapsulation frame-relay
frame-relay map 130.130.0.2 pvc 101 broadcast
frame-relay map 130.130.0.4 pvc 102 broadcast
ip ospf network point-to-multipoint
!

```
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

**The configuration of 대전:**

```
hostname 대전
!
interface serial 1/0
ip address 130.130.0.4 255.0.0.0
encapsulation frame-relay
physical speed 1000000
frame-relay map 130.130.0.1 pvc 401 broadcast
frame-relay map 130.130.0.2 pvc 402 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

**The configuration of 광주:**

```
hostname 광주
!
interface serial 1/1
ip address 130.130.0.3 255.0.0.0
encapsulation frame-relay
physical speed 2000000
frame-relay map 130.130.0.2 pvc 301 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

### 51.4.2. OSPF point to multipoints, non-broadcasting 설정 예시

```
interface Serial1/0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
frame-relay local-dlci 200
frame-relay map 10.0.1.3 pvc 202
frame-relay map 10.0.1.4 pvc 203
frame-relay map 10.0.1.5 pvc 204
no shut
```

```
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
Here is the configuration of the router on the other side:
interface Serial1/2
ip address 10.0.1.3 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint non-broadcast
no ip mroute-cache
no keepalive
no fair-queue
frame-relay local-dlci 301
frame-relay map 10.0.1.1 pvc 300
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
```

### 51.4.3. VLSM 설정 예시

OSPF 와 정적 라우팅은 가변 길이 서브넷 마스크(VLSM)를 지원합니다. VLSM 을 통해 서로 다른 인터페이스에서 동일한 네트워크 번호에 대해 서로 다른 마스크를 사용할 수 있으므로 IP 주소를 절약하고 네트워크의 주소 공간을 보다 효율적으로 활용할 수 있습니다.

다음 예제에서는 30 비트 서브넷 마스크만 사용하고 직렬 포트의 호스트 주소로 2 비트의 주소 공간을 예약합니다. 두 개의 호스트 주소만 필요한 point-to-point 직렬 링크의 경우 충분합니다.

```
interface ethernet 1/0
ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernets
interface serial 1/1
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
```

### 51.4.4. OSPF route 와 route distribution 설정 예시

OSPF 는 많은 내부 라우터, ABR(Area Border Router, 영역 경계 라우터) 및 ASBR(Autonomous System Boundary Router, 자율 시스템 경계 라우터) 간의 정보 교환을 필요로 합니다. 최소 구성에서 OSPF 기반 라우터는 기본 매개변수에서 작동할 수 있으며 인증이 필요하지 않습니다.

다음은 세 가지 구성 예제입니다.

(1) 첫 번째 예제는 기본적인 OSPF 명령을 연습합니다.
(2) 두 번째 예제는 단일 OSPF 자율 시스템에서 내부 라우터, ABR 및 ASBR 의 구성을 구성합니다.
(3) 세 번째 예제는 다양한 OSPF 도구를 사용한 보다 복잡한 구성 예제를 보여줍니다.

**OSPF 기본 설정 예시**

다음은 간단한 OSPF 구성의 예입니다. 라우팅 프로세스 90 을 활성화한 다음 이더넷 인터페이스 0 을 영역 0.0.0.0 에 연결합니다. 동시에 RIP 을 OSPF 로, OSPF 를 RIP 으로 재분배합니다.

```
.
interface ethernet 1/0
 ip address 130.130.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1/0
 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
```

**내부 라우터, ABR 및 ASBR 의 기본 구성 예제**

다음 예제는 4 개의 IP 주소 범위를 4 개의 영역 ID 에 할당합니다. 먼저 라우팅 프로세스 109 가 활성화되고, 4 개의 영역은 10.9.50.0, 2, 3, 0 입니다. 영역 10.9.50.0, 2, 3 의 마스크는 주소 범위를 지정하지만, 영역 0 은 모든 네트워크를 포함합니다.

```
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 Ethernet1/0 is in area 10.9.50.0:
interface ethernet 1/0
 ip address 131.108.20.5 255.255.255.0
!
! Interface Ethernet1/1 is in area 2:
interface ethernet 1/1
 ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet1/2 is in area 2:
interface ethernet 1/2
 ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet1/3 is in area 3:
interface ethernet 1/3
 ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet1/4 is in area 0:
interface ethernet 1/4
 ip address 131.109.1.1 255.255.255.0
!
! Interface FastEthernet0/0 is in area 0:
interface FastEthernet0/0
 ip address 10.1.0.1 255.255.0.0
```

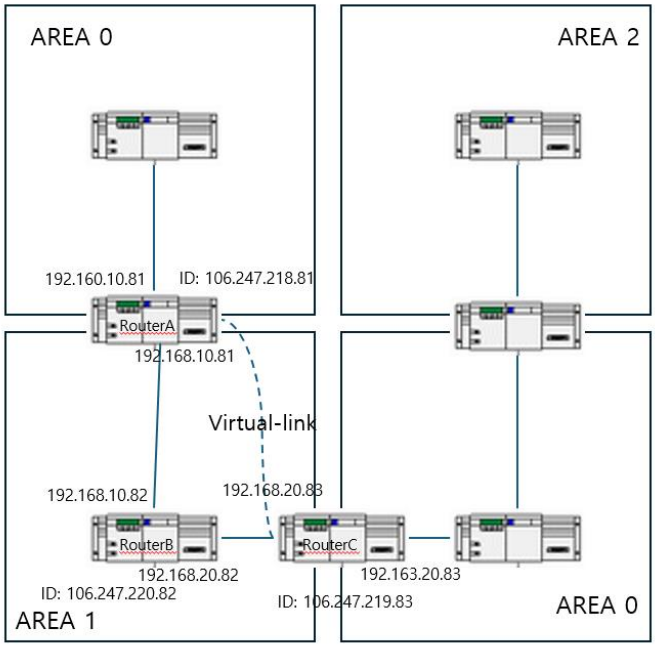
네트워크 영역 구성 명령의 기능은 순차적이며, 명령의 순서가 중요합니다. 라우터는 각 인터페이스의 주소/마스크 쌍을 순서대로 매치합니다. 자세한 내용은 "OSPF 명령"의 관련 네트워크 프로토콜 명령 참조의 관련 내용을 참조하십시오.

위 예제의 첫 번째 네트워크 영역으로 돌아가 보겠습니다. 영역 ID 10.9.50.0 은 인터페이스 서브넷 마스크 131.108.20.0 으로 구성됩니다. 따라서 이더넷 인터페이스 0 이 일치합니다. 따라서 이더넷 인터페이스 0 은 영역 10.9.50.0 에만 존재합니다.

두 번째 영역으로 이동합니다. 인터페이스 0 을 제외하고 다른 인터페이스에서 동일한 프로세스를 적용하면 이더넷 인터페이스 1 이 일치합니다. 따라서 인터페이스 1 은 영역 2 에 연결됩니다. 다른 네트워크 영역의 매칭을 계속합니다. 마지막 네트워크 영역 명령은 나머지 인터페이스가 모두 네트워크 영역 0 에 연결됨을 의미하는 특수한 경우입니다.

내부 라우터, ABR 및 ASBR 의 복잡한 구성 예제.

다음 예제는 단일 OSPF 자율 시스템에서 여러 라우터의 구성을 보여줍니다. 그림 24 는 예제의 네트워크 토폴로지입니다.




위 그림에 따라 라우터를 구성합니다.

**RouterA：**

```
interface loopback 0/0
ip address 106.247.218.81 255.255.255.0
!
interface Ethernet 1/0
ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
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
!
```

**RouterB：**

```
interface loopback 0/0
```

```
ip address 106.247.220.82 255.255.255.252
!
interface Ethernet 1/0
ip address 192.168.10.82 255.255.255.0
!
interface ethernet 1/1
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
!
```

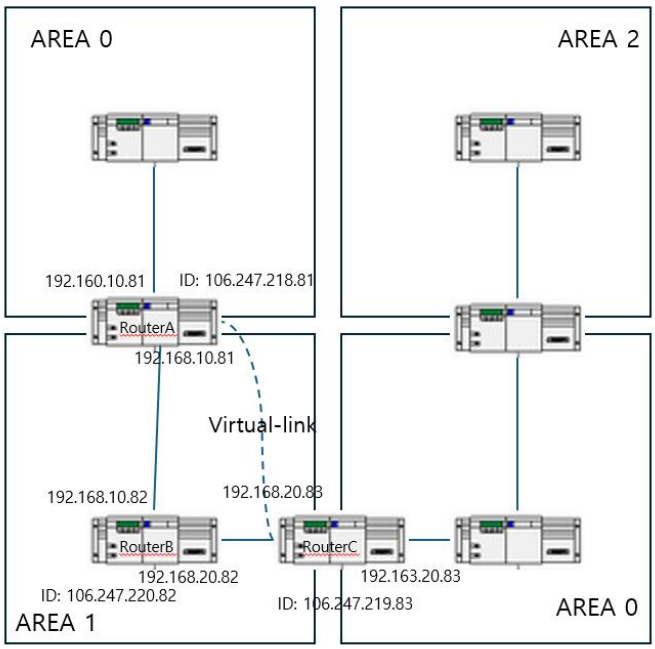
**routerC：**

```
interface loopback 0/0
ip address 106.247.219.83 255.255.255.252
!
interface Ethernet 1/0
ip address 192.163.20.83 255.255.255.0
!
interface ethernet 1/1
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
!
```

**복잡한 내부 라우터, ABR 및 ASBR 구성 예제**

다음 예제는 단일 OSPF 자율 시스템에서 여러 라우터를 구성하는 방법을 보여줍니다.

그림 4-2 는 구성 예제의 네트워크 토폴로지를 보여줍니다.




위 그림에 따라 라우터를 구성합니다.

**Router A:**

interface loopback 0/0
ip address 106.247.218.81 255.255.255.0
!
interface Ethernet 1/0
ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
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
!

**Router B:**

interface loopback 0/0
ip address 106.247.220.82 255.255.255.252
!
interface Ethernet 1/0
ip address 192.168.10.82 255.255.255.0
!

```
interface ethernet 1/1
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
!
```

**Router C:**

```
interface loopback 0/0
ip address 106.247.219.83 255.255.255.252
!
interface Ethernet 1/0
ip address 192.163.20.83 255.255.255.0
!
interface ethernet 1/1
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
!
```

**ABR 라우터의 복잡한 OSPF 구성 예제**

다음은 OSPF 구성의 예입니다.

```
interface ethernet 1/0
ip address 192.168.20.81 255.255.255.0
ip ospf password GHGHGHG
ip ospf cost 10
!
interface ethernet 1/1
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 ethernet 1/2
```

```
ip address 192.168.40.81 255.255.255.0
ip ospf password abcdefgh
ip ospf cost 10
!
interface ethernet 1/3
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 on network 192.168.30.0
router rip
network 192.168.30.0
redistribute ospf 192
```

# 52. BGP 설정

## 52.1. 개요

이 장에서는 BGP(Border Gateway Protocol, 경계 게이트웨이 프로토콜) 구성 방법을 설명합니다. 이 장의 BGP 명령에 대한 자세한 내용은 "BGP 명령"과 관련된 다른 섹션을 참조하십시오. BGP 는 RFC 1163, 1267 및 1771 에 정의된 EGP(Exterior Gateway Protocol, 외부 게이트웨이 프로토콜)입니다. BGP 를 사용하면 서로 다른 자율 시스템 간에 경로 선택 메커니즘을 설정할 수 있으며, 이 메커니즘은 자율 시스템 간에 루프 없는 라우팅 정보 교환을 자동으로 보장할 수 있습니다.

### 52.1.1. 라우터의 BGP 구현

BGP 에서 각 경로는 네트워크 번호, 이 경로가 통과한 자율 시스템 목록(AS-path 라고 함) 및 기타 속성 목록을 포함합니다. 당사의 라우터 소프트웨어는 RFC 1771 에 정의된 BGP v4 를 지원합니다. BGP 의 기본 기능은 AS-path 정보를 포함하여 다른 BGP 시스템과 네트워크 도달 가능성 정보를 교환하는 것입니다. 이 정보는 경로 루프를 제거할 수 있는 AS 연결 그래프를 구성하는 데 사용될 수 있으며, AS 연결 그래프를 사용하여 AS 수준 라우팅 정책을 구현할 수 있습니다. BGP v4 는 CIDR(Classless Inter-Domain Router, 클래스리스 도메인 간 라우터)를 지원하며, CIDR 은 요약 경로를 생성하여 라우팅 테이블의 크기를 줄이고 슈퍼 네트워크를 생성할 수 있습니다. CIDR 은 BGP 에서 네트워크 수준의 개념을 제거하고 IP 접두사 브로드캐스팅을 지원합니다. CIDR 경로는 OSPF, Enhanced IGRP, ISIS-IP 및 RIP2 를 통해 전송될 수 있습니다.

외부 게이트웨이 라우팅과 내부 게이트웨이 라우터의 중요한 차이점은 전자가 더 나은 제어 기능을 갖는다는 것입니다. 경로를 제어하기 위해 BGP 구현은 다음과 같은 여러 가지 선택적 방법을 제공합니다.

(1) 경로를 필터링하기 위해 이웃 기반 액세스 목록, aspath-list, prefix-list 를 기반으로 할 수 있으며, 인터페이스 기반 액세스 목록, prefix-list 를 사용하여 경로 또는 경로의 Nexthop 속성을 필터링할 수도 있습니다.
(2) 경로의 속성을 변경하기 위해 route-map 을 사용하여 MED, Local preference, route value 등을 포함한 BGP 경로의 속성을 수정할 수 있습니다.
(3) 내부 게이트웨이 동적 라우팅 프로토콜(OSPF, RIP 등)과 상호 작용하기 위해 경로를 재분배하여 BGP 라우팅 정보를 자동으로 생성할 수 있습니다. 또한 네트워크, 집계의 수동 구성을 통해 BGP 경로를 생성할 수 있습니다. BGP 경로를 생성하는 동안 route-map 을 사용하여 경로의 속성을 구성할 수 있습니다.

시스템에서 BGP 경로의 우선순위를 제어하기 위해 "distance" 명령을 사용하여 BGP 경로의 관리 거리를 구성할 수 있습니다.

#### 52.1.2. 어떻게 BGP 경로를 선택하는가

BGP 의 경로 결정 과정은 경로 속성 값을 비교하는 것을 기반으로 합니다. 동일한 네트워크에 여러 경로가 있는 경우 BGP 는 목적지에 대한 최적 경로를 선택합니다. 다음은 BGP 가 최적 경로를 선택하는 방법을 요약한 것입니다.

(1) 다음 홉에 도달할 수 없으면 고려하지 않습니다.
(2) 경로가 내부 경로이고 동기화가 활성화되어 있으며 IGP 에 경로가 없으면 고려하지 않습니다.
(3) 최대 우선순위를 가진 선호 경로를 선택합니다.
(4) 각 경로의 값이 동일하면 최대 로컬 우선순위를 가진 경로를 선호합니다.
(5) 각 경로의 로컬 우선순위가 동일하면 로컬 라우터에서 생성된 경로를 선호합니다. 예를 들어, "network, aggregate" 명령을 사용하거나 IGP 경로를 재분배하여 로컬 라우터에서 경로를 생성할 수 있습니다.
(6) 로컬 우선순위가 동일하거나 로컬 라우터에서 생성된 경로가 없으면 가장 짧은 AS 경로를 가진 경로를 선호합니다.
(7) AS 경로 길이가 동일하면 "origin" 속성의 가장 낮은 값을 가진 경로를 선호합니다 (IGP < EGP < INCOMPLETE).
(8) "Origin"의 속성 값이 동일하면 가장 낮은 MED 값을 가진 경로를 선호합니다. "bgp always-compare-med"가 활성화되지 않은 경우 이 비교는 동일한 이웃 AS 의 경로 간에만 수행될 수 있습니다.
(9) 각 경로의 MED 가 동일하면 내부 경로(IBGP)보다 외부 경로(EBGP)를 선호합니다. 자율 시스템 연합 내의 모든 경로는 내부 경로로 간주되지만 IBGP 연합이 아닌 EBGP 연합을 선호합니다.
(10) 각 경로의 연결 속성이 동일하면 더 작은 라우터 ID 를 가진 경로를 선호합니다.

## 52.2. BGP 구성 작업 목록

#### 52.2.1. BGP 기본 설정 작업 목록

BGP 구성 작업은 기본 작업과 고급 작업으로 나눌 수 있습니다. 기본 작업의 처음 두 항목은 BGP 를 구성하는 데 필수적이며, 기본 작업의 다른 항목과 모든 고급 작업은 선택 사항입니다. BGP 의 기본 구성 작업은 다음과 같습니다.

(1) BGP 의 경로 선택을 활성화합니다.
(2) BGP 이웃을 구성합니다.
(3) BGP 소프트 재구성을 구성합니다.
(4) BGP 연결을 재설정합니다.
(5) BGP 와 IGP 간의 동기화를 구성합니다.
(6) BGP 경로 값을 구성합니다.

(7) 이웃을 기반으로 BGP 경로 필터를 구성합니다.
(8) 인터페이스를 기반으로 BGP 경로 필터링을 구성합니다.
(9) BGP 업데이트의 다음 홉 처리를 비활성화합니다.

#### 52.2.2. 고급 BGP 구성 작업 목록

선택적인 고급 BGP 구성 작업은 다음과 같습니다.

(1) route-map 을 사용하여 경로 업데이트를 필터링하고 수정합니다.
(2) 집계 주소를 구성합니다.
(3) BGP 커뮤니티 속성을 구성합니다.
(4) 자율 시스템 연합을 구성합니다.
(5) 경로 반사기를 구성합니다.
(6) 피어 엔터티를 종료합니다.
(7) 멀티홉 외부 피어 본체를 구성합니다.
(8) BGP 경로의 관리 거리를 구성합니다.
(9) BGP 타이머를 조정합니다.
(10) 서로 다른 AS 의 경로의 MED 를 비교합니다.

여러 IP 경로 선택 프로토콜의 속성 구성에 대한 자세한 내용은 "프로토콜과 독립적인 IP 라우팅 속성 구성"을 참조하십시오.

## 52.3. 기본 BGP 기능 구성 작업

#### 52.3.1. 기본 BGP 기능 구성

(1) BGP 경로 선택 활성화

BGP 경로 선택을 활성화하려면 전역 구성 모드에서 다음 명령을 사용합니다:

| 명령 | 설명 |
|---|---|
| **router bgp autonomous-system** | 라우터 구성 모드에서 BGP 경로 선택 프로세스를 활성화합니다. |
| **network** *network-number*[ *masklen*] [**route-map** *route-map-name*] | 네트워크를 로컬 자율 시스템으로 태그하고 BGP 목록에 추가합니다. |

Notes:
외부 게이트웨이 라우팅 프로토콜에서는 `network` 구성 명령어를 사용하여 IP 네트워크를 설정할 때, 단순히 어떤 네트워크 정보를 알릴지를 제어하는 용도로 사용됩니다. 이는 내부 게이트웨이 프로토콜(IGP), 예를 들어 RIP 과는 반대되는 개념으로, RIP 에서는 `network` 명령어를 사용하여 업데이트를 전송할 대상을 결정합니다.

`network` 명령어는 IGP 경로를 BGP 라우팅 테이블로 가져오는 데 사용됩니다. 사용 가능한 `network` 명령어의 상한선은 라우터의 설정된 RAM 과 같은 리소스에 의해 결정됩니다. 대안으로, `redistribute` 명령어를 사용하여 동일한 효과를 얻을 수 있습니다.

(2) BGP neighbour 설정

BGP 이웃을 구성하는 것은 라우팅 정보를 교환하기 위해 피어를 설정하는 과정입니다. 외부 세계와 라우팅 정보를 교환하려면 BGP 이웃을 반드시 구성해야 합니다.

BGP 는 두 가지 유형의 이웃을 지원합니다: 내부 이웃(IBGP)과 외부 이웃(EBGP). 내부 이웃(IBGP)은 동일한 자율 시스템(AS) 내에 있고, 외부 이웃(EBGP)은 서로 다른 AS 에 속합니다. 일반적으로 외부 이웃(EBGP)은 서로 인접하며 동일한 서브넷을 공유하지만, 내부 이웃(IBGP)은 동일한 AS 내에서 어디든 위치할 수 있습니다.

BGP 이웃을 구성하려면 `Neighbor` 구성 명령어를 사용하십시오:

| 명령 | 설명 |
|---|---|
| **neighbor** {*ip-address* \| *peer-group-name*} **remote-as** *number* | BGP 이웃을 지정하십시오. |

예를 들어, BGP 이웃 구성에 대한 내용은 이 장의 하단에 있는 "BGP 이웃 구성 예제" 섹션을 참고하십시오.

(3) BGP 소프트 재구성 설정

일반적으로 BGP 이웃은 연결이 설정될 때 모든 경로를 교환하고, 그 후에는 업데이트된 경로만 교환합니다. 따라서 구성된 라우팅 정책이 변경되면 수신된 경로에 적용하기 위해 BGP 세션을 지워야 합니다. BGP 세션을 지우면 캐시가 무효화되어 네트워크 운영에 큰 영향을 미칩니다. 소프트 재구성 기능을 사용하면 BGP 세션을 지우지 않고 정책을 구성하고 활성화할 수 있습니다. 따라서 소프트 재구성을 사용하는 것이 좋습니다. 현재 이웃을 기준으로 소프트 재구성을 활성화합니다. 소프트 재구성이 이웃에서 생성된 수신 업데이트에 사용될 때 이를 수신 소프트 재구성이라고 하고, 소프트 재구성이 이웃에 대한 발신 업데이트에 사용될 때 이를 발신 소프트 재구성이라고 합니다. 수신 소프트 재구성을 적용하면 새 입력 정책이 적용되고, 발신 소프트 재구성을 적용하면 BGP 세션을 재설정하지 않고 새 로컬 출력 정책이 적용됩니다.

BGP 세션을 재설정하지 않고 새 수신 업데이트를 생성하려면 로컬 BGP 스피커는 현재 수신 정책에 따라 허용되든 거부되든 상관없이 수정 없이 수신된 수신 업데이트를 저장해야 합니다. 이는 메모리 소비가 매우 클 수 있으므로 피해야 합니다. 반면 발신 재구성은 추가 메모리 소비가 없으므로 항상 효과적입니다. BGP 세션의 다른 쪽에서 발신 소프트 재구성을 트리거하여 새 로컬 수신 정책을 적용할 수 있습니다.

수신 소프트 재구성을 허용하려면 BGP 가 모든 허용된 라우팅 업데이트를 저장하도록 구성해야 합니다. 발신 재구성은 미리 구성할 필요가 없습니다.

다음 라우터 구성 명령을 사용하여 BGP 소프트 재구성을 구성합니다:

| 명령 | 설명 |
|---|---|
| **Neighbor** {*ip-address* \| *peer-group-name*} **soft-reconfiguration** [**inbound**] | BGP 소프트 재구성을 구성합니다. |

"peer-community-name" 매개변수를 사용하여 BGP 피어 커뮤니티를 지정하면 해당 커뮤니티의 모든 피어 구성원이 이 명령의 기능을 상속받습니다.

(4) BGP 연결 재설정

두 라우터가 BGP 이웃으로 정의되면 BGP 연결을 생성하고 라우팅 정보를 교환합니다. BGP 라우팅 정책이 변경되었거나 다른 구성이 변경된 경우 구성 변경 사항을 적용하려면 BGP 연결을 재설정해야 합니다.

다음 두 가지 관리 모드 명령 중 하나를 사용하여 BGP 연결을 재설정합니다:

| 명령 | 설명 |
|---|---|
| **clear ip bgp** {***** \| *address}* | BGP 모든 연결 재설정<br>특정 BGP 연결을 다시 만듭니다. (또는 재생성합니다.) |

(5) BGP 와 IGP 간의 동기화 구성

만약 당신의 AS 를 통해 다른 AS 가 제 3 의 AS 로 데이터를 전송하도록 허용한다면, 당신의 AS 내부 라우팅 상태와 다른 AS 에 브로드캐스트하는 라우팅 정보 간의 동기화는 매우 중요합니다. 예를 들어, 당신의 BGP 가 AS 내의 모든 라우터가 IGP 를 통해 경로를 알기 전에 경로를 브로드캐스트하려고 하면, 당신의 AS 는 일부 라우터가 라우팅할 수 없는 일부 정보를 수신할 수 있습니다. 이러한 상황을 방지하기 위해 BGP 는 AS 내부의 모든 IGP 라우터가 해당 라우팅 정보를 알 때까지 기다려야 합니다. 이것이 BGP 와 IGP 간의 동기화이며, 동기화는 기본적으로 활성화되어 있습니다.

특정 상황에서는 동기화가 필요하지 않습니다. 다른 AS 가 당신의 AS 를 통해 데이터를 전송하는 것을 허용하지 않거나 AS 의 모든 라우터가 BGP 를 실행하는 경우 동기화 기능을 취소할 수 있습니다. 이 기능을 취소하면 IGP 에 더 적은 경로를 포함할 수 있고 BGP 의 수렴 속도를 높일 수 있습니다.

다음 라우터 구성 명령을 사용하여 동기화를 취소합니다:

| 명령 | 설명 |
|---|---|
| **no synchronization** | BGP 와 IGP 간의 동기화를 취소합니다. |

동기화를 취소하는 동안 "clear ip bgp" 명령을 사용하여 BGP 대화를 지워야 합니다.
BGP 동기화에 대한 예는 이 장의 맨 아래에 있는 "이웃별 BGP 경로 필터링 예제" 섹션을 참조하십시오.

일반적으로 모든 경로를 IGP 로 재분배하는 것을 기대하지 않습니다. 일반적인 설계는 하나 또는 두 개의 경로를 재분배하여 IGRP 의 외부 경로로 만들거나 BGP 세션이 AS 기본 경로를 생성하도록 하는 것입니다. BGP 가 경로를 IGP 로 재분배할 때 EBGP 를 통해 획득한 경로만 재분배됩니다. 대부분의 상황에서 IGP 를 BGP 에 할당하지 않고 "network" 구성 명령을 사용하여 AS 의 네트워크를 나열하면 네트워크가 브로드캐스트됩니다. 이러한 형식으로 나열된 네트워크를 로컬 네트워크라고 하며 BGP 가 IGP 의 "Origin" 속성을 갖도록 합니다.

이러한 네트워크는 기본 IP 라우팅 테이블에 나타나야 하며 유효해야 합니다. 예를 들어 직접 연결된 경로, 정적 경로 또는 IGP 를 통해 알려진 경로입니다. BGP 라우팅 프로세스는 기본 IP 라우팅 테이블을 주기적으로 검색하여 로컬 네트워크의 존재 여부를 확인하고, 실제로 BGP 가 재분배를 실행하도록 하려면 매우 신중해야 합니다. 이러한 경로는 다른 라우터가 BGP 를 통해 주입한 IGP 의 경로일 수 있으므로 BGP 가 잠재적으로 정보를 IGP 에 주입한 다음 해당 정보를 BGP 로 다시 보내는 일종의 상황을 초래할 수 있습니다. 반대의 경우도 마찬가지입니다.

(6) BGP 경로 값 구성

BGP 경로 값은 경로 선택 프로세스를 제어하기 위해 BGP 경로에 설정된 숫자이며, 값은 라우터에 로컬합니다. 값의 범위는 0 에서 65535 까지입니다. 로컬에서 생성된 BGP 경로는 기본값 32768 을 가지며, 이웃에서 가져온 경로는 값 0 을 가집니다. 관리자는 경로 값을 변경하여 라우팅 정책을 구현할 수 있습니다.

다음 라우터 구성 명령을 사용하여 BGP 경로 가중치를 구성합니다:

| 명령 | 설명 |
|---|---|
| **neighbor** {*ip-address* \| *peer-group-name*} **weight** *weight* | 한 이웃의 각 경로에 값을 지정합니다. |

또한 route-map 을 통해 경로 가중치를 변경할 수 있습니다.

(7) 이웃 기반 BGP 경로 필터 구성

라우터 소프트웨어의 BGP 구현에는 지정된 이웃의 BGP 경로를 필터링하는 4 가지 방법이 있습니다.

ip aspath-list 전역 구성 명령 및 neighbor filter-list 명령과 함께 AS 경로 목록 필터를 사용합니다.

| 명령 | 설명 |
|---|---|
| **ip aspath-list** aspaths-list-name {**permit \| deny**} as-regular-expression | BGP 와 관련된 접근 목록을 정의합니다. |
| **router bgp** autonomous-system | 라우터 구성 모드로 들어갑니다. |
| **neighbor** {ip-address \| peer-group-name} **filter-list** aspath-list-name {**in \| out** } | BGP 필터를 설정합니다. |

접근 목록과 전역 구성 명령 "ip access-list" 및 "neighbor distribute-list" 명령을 함께 사용합니다."

| 명령 | 설명 |
|---|---|
| **ip access-list standard** *access-list-name* | 접근 목록을 정의합니다. |
| **router bgp** *autonomous-system* | 라우터 구성 모드로 진입합니다. |
| **neighbor** {*ip-address* \| *peer-group-name*} **distribute-list** *access-list-name* {**in** \| **out** } | BGP 필터를 설정합니다. |

접두사 목록과 전역 구성 명령 "ip prefix-list" 및 "neighbor prefix-list" 명령을 함께 사용합니다.

| 명령 | 설명 |
|---|---|
| **ip prefix-list** *prefixs-list-name* **{permit \|deny}** A.B.C.D/n **ge** x **le** y | 접두사 목록을 정의합니다. |
| **router bgp** *autonomous-system* | 라우터 구성 모드로 들어갑니다. |
| **neighbor** {*ip-address* \| *peer-group-name*} **prefix-list** *prefix-list-name* {**in \| out** } | BGP 필터를 설정합니다. |

route-map 과 전역 구성 명령 "route-map" 및 "neighbor route-map" 명령을 함께 사용합니다.

route-map 을 사용하면 경로를 필터링할 수 있을 뿐만 아니라 경로 속성도 변경할 수 있으며, 사용법은 다음 장에서 설명합니다.

이웃 기반 경로 필터링에 대한 예는 "이웃 기반 BGP 경로 필터링 예제"를 참조하십시오.

(8) 인터페이스 기반 BGP 경로 필터링 구성

인터페이스 기반 BGP 경로 필터링 구성은 접근 목록과 접두사 목록을 사용하여 수행할 수 있습니다.

경로의 네트워크 번호와 게이트웨이 주소를 필터링할 수 있습니다. "access-list" 옵션을 지정하여 접근 목록을 사용하여 경로의 네트워크 번호를 필터링하고, "prefix-list" 옵션을 지정하여 접두사 목록을 사용하여 경로의 네트워크 번호를 필터링하며, "gateway" 옵션을 지정하여 접근 목록을 사용하여 경로의 "nexthop" 속성을 필터링할 수 있습니다. 네트워크 번호와 경로의 "nexthop" 속성을 동시에 필터링할 수도 있지만 "access-list" 옵션은 "prefix-list" 옵션과 함께 사용할 수 없습니다. "*"를 지정하면 모든 인터페이스의 경로를 필터링할 수 있습니다.

인터페이스 기반 BGP 경로 필터링을 구성하려면 BGP 구성 모드에서 다음 구성을 수행해야 합니다:

| 명령 | 설명 |
|---|---|
| **filter interface** {**in** \| **out**} [**access-list** *access-list-name*] [**prefix-list** *prefix-list-name*][**gateway** *access-list-name*] | 인터페이스를 기반으로 BGP 경로를 필터링합니다. |

인터페이스 기반 경로 필터링 예제는 "인터페이스 기반 BGP 경로 필터링 예제"를 참조합니다.

(9) BGP 업데이트의 다음 홉 처리 비활성화

인접 BGP 업데이트의 다음 홉 처리를 비활성화하도록 구성할 수 있습니다. 이는 FR 또는 X.25 와 같은 비브로드캐스팅 네트워크에서 유용할 수 있습니다. FR 또는 X.25 네트워크에서 BGP 인접 장치가 동일한 IP 서브넷의 다른 모든 인접 장치에 직접 액세스하지 못할 수 있습니다.

다음 홉 처리를 취소하는 두 가지 방법이 있습니다:

a. 나가는 경로의 다음 홉 주소를 이 BGP 연결의 로컬 IP 주소로 바꾸는 방법:
b. route-map 을 사용하여 들어오는 또는 나가는 경로의 다음 홉 주소를 지정하는 방법: (자세한 내용은 다른 장을 참조합니다.)

c. 다음 라우터 구성 명령을 사용하여 다음 홉 처리를 비활성화하고 이 BGP 연결의 로컬 IP 주소를 사용하여 나가는 경로의 다음 홉 주소를 바꾸는 방법:

| 명령 | 설명 |
|---|---|
| **neighbor** {*ip-address* \| *peer-group-name*} **next-hop-self** | BGP 인접 업데이트를 수행하는 동안 다음 홉 처리를 비활성화합니다. |

이 명령을 사용하여 구성하면 현재 라우터가 자신을 경로의 다음 홉으로 알리도록 설정합니다. 따라서 다른 BGP 인접 장치는 이 네트워크로 향하는 패킷을 현재 라우터로 전달합니다. 이는 현재 라우터에서 지정된 인접 장치로 경로가 존재하는 비브로드캐스팅 네트워크 환경에서 매우 유용합니다. 그러나 브로드캐스팅 네트워크 환경에서는 불필요한 추가 홉을 유발하므로 적합하지 않습니다.

### 52.3.2. 고급 BGP 기능 구성

(1) route-map 을 사용하여 경로 업데이트를 필터링하고 수정

route-map 을 사용하여 각 인접 장치를 기반으로 경로 업데이트를 필터링하고 매개변수 속성을 수정할 수 있습니다. route-map 은 들어오는 업데이트와 나가는 업데이트 모두에 적용할 수 있습니다. route-map 을 통과하는 경로만 경로 업데이트를 보내거나 받을 때 처리됩니다.

route-map 은 AS 경로, 커뮤니티 및 네트워크 번호와 일치하도록 들어오는 업데이트와 나가는 업데이트를 지원합니다. AS 매칭에는 "aspath-list" 명령을 사용해야 하고, 커뮤니티 기반 매칭에는 "community-list" 명령을 사용해야 하며, 네트워크 기반 매칭에는 "ip access-list" 명령을 사용해야 합니다.

다음 BGP 구성 명령을 사용하여 경로 업데이트의 필터링 및 수정을 위한 route-map 을 구성합니다:

| 명령 | 설명 |
|---|---|
| **neighbor** {*ip-address* \| *peer-group-name*} **route-map** *route-map-name* **{in \| out}** | Apply route-map on incoming or outgoing routes. |

route-map 을 사용하여 경로 업데이트를 필터링하고 수정하는 예제는 "BGP route-map 예제"를 참조합니다.

(2) Aggregate address 설정

클래스리스(Classless) 인터도메인 라우팅은 라우팅 테이블을 최소화하기 위해 집계 라우팅(및 슈퍼넷)을 생성할 수 있습니다. BGP 에서 집계 라우팅을 구성하는 방법에는 집계 경로를 BGP 로 재분배하거나 다음 작업 목록에 설명된 조건부 집계 속성을 사용하는 두 가지 방법이 있습니다. BGP 라우팅 테이블에 하나 이상의 상세 레코드가 있는 경우 집계 주소를 BGP 라우팅 테이블에 추가합니다.

다음의 하나 이상의 라우터 구성 명령을 사용하여 라우팅 테이블에 집계 주소를 생성합니다:

| **명령** | **설명** |
|---|---|
| **aggregate** *network/len* | BGP 라우팅 테이블에 집계 주소 생성 |
| **aggregate** *network/len* **summary-only** | 요약 주소만 브로드캐스트 |
| **aggregate** *network/len* **route-map** *map-name* | route-map 에서 지정한 조건에 따라 집계 주소 생성 |

BGP 경로 집계 사용에 관한 예제는 이 장의 맨 아래 섹션 "BGP 경로 집계 예제"를 참조하세요.

(3) BGP community attribute 설정

BGP 가 지원하는 라우팅 정책은 주로 BGP 라우팅 정보의 다음 3 가지 값 중 하나를 기반으로 합니다.

a. 경로의 네트워크 번호
b. 경로의 as_path 속성 값
c. 경로의 "community" 속성 값

"community" 속성을 통해 경로를 커뮤니티로 나누고, 커뮤니티를 기반으로 라우팅 정책을 적용함으로써 라우팅 정보 제어 구성을 단순화합니다.

커뮤니티는 공통 속성을 가진 경로 그룹이며, 각 경로는 여러 커뮤니티에 속할 수 있습니다. AS 관리자는 특정 경로가 특정 커뮤니티에 속하도록 정의할 수 있습니다. 커뮤니티 속성은 1 에서 4,294,967,200 까지의 범위를 갖는 선택적이고 전송 가능한 글로벌 속성입니다.

인터넷 커뮤니티에 미리 정의된 유명한 커뮤니티는 다음과 같습니다.

a. No-export: 이 경로를 EBGP 피어(자율 시스템 연합 내부의 EBGP 피어 포함)에 광고하지 않습니다.
b. No-advertise: 이 경로를 어떤 피어에도 광고하지 않습니다.

c. local-as: 이 경로를 자율 시스템 외부로 광고하지 않습니다(자율 시스템 연합의 다른 하위 AS 피어에는 이 경로를 보낼 수 있습니다).

BGP 스피커는 경로를 생성, 수락 또는 전송할 때 경로 커뮤니티 속성을 구성, 추가 또는 수정할 수 있습니다. 경로를 집계할 때 생성된 집계에는 모든 원래 경로의 완전한 커뮤니티의 "community" 속성이 포함됩니다.

기본적으로 "Community" 속성은 이웃에 전송되지 않습니다. 다음 BGP 구성 명령을 사용하여 이웃에게 "community" 속성 전송을 지정합니다:

| 명령 | 설명 |
|---|---|
| **neighbor** {*ip-address* \| *peer-group-name*} **send-community** | 이웃에게 "community" 속성을 보내도록 지정합니다. |

라우터에 커뮤니티 속성을 구성하려면 다음 작업을 수행해야 합니다.

| 명령 | 설명 |
|---|---|
| **route-map** *map-name sequence-number* **{deny \| permit}** | route-map 구성 |
| **set community** *community-value* | 설정 규칙 구성 |
| **router bgp** *autonomous-system* | 라우터 구성 모드 진입 |
| **neighbor** {*ip-address* \| *peer-group-name*} **route-map** *access-list-name* {**in \| out** } | route-map 적용 |

커뮤니티 속성을 기반으로 라우팅 정보를 필터링하려면 다음 작업을 수행해야 합니다.

| 명령 | 설명 |
|---|---|
| **ip community-list** *community-list-*name {**permit \| deny**} **community-expression** | 커뮤니티 목록 정의 |
| **route-map** *map-name* s*equence-number* **{deny \| permit}** | route-map 구성 |
| **match** *community-list-name* | 매칭 규칙 구성 |
| **router bgp autonomous-system** | 라우터 구성 모드 진입 |
| **neighbor** {*ip-address* \| *peer-group-name*} **route-map** *route-map-name* {**in \| out** } | route-map 적용 |

커뮤니티 속성 사용 예제는 "BGP 커뮤니티 속성을 사용하는 route-map 예제"를 참조하세요.

(4) 자율 시스템 연합 구성

IBGP 연결 수를 줄이는 방법은 AS 를 여러 개의 하위 AS 로 나누어 자율 시스템 연합을 구성하는 것입니다. 외부 관점에서 연합은 하나의 AS 처럼 보입니다. 연합 내에서 각 하위 AS 는 내부적으로 완전 메시(full-mesh) 연결되어 있으며 동일한 연합의 다른 하위 AS 와 연결되어 있습니다. 다른 하위 AS 의 피어 간에 EBGP 세션이 있더라도 IBGP 피어와 마찬가지로 라우팅 선택 정보를 교환할 수 있습니다. 구체적으로는 다음 홉, MED 및 로컬 우선 순위 정보를 저장합니다.

BGP 자율 시스템 연합을 구성하려면 연합 식별자를 지정해야 합니다. 연합 식별자는 AS 번호이며, 외부 관점에서 연합은 연합 식별자를 AS 번호로 사용하는 단일 AS 와 같습니다.

다음 BGP 구성 명령을 사용하여 자율 시스템의 연합 식별자를 구성합니다:

| 명령 | 설명 |
|---|---|
| **bgp confederation identifier** *autonomous-system* | 자율 시스템의 연합 식별자를 구성합니다. |

자율 시스템 연합에 속하는 자율 시스템 번호를 지정하려면 다음 BGP 구성 명령을 사용하십시오:

| 명령 | 설명 |
|---|---|
| **bgp confederation peers autonomous-system [autonomous-system ...]** | 자율 시스템 연합에 속하는 AS 를 지정합니다. |

자율 시스템 연합의 예는 "BGP 자율 시스템 연합 예"를 참조하세요.

(5) Route reflector 설정

자율 시스템 연합을 구성하는 대신 IBGP 연결 수를 줄이는 또 다른 방법은 경로 반사기(Route Reflector)를 구성하는 것입니다.

경로 반사기의 내부 피어는 두 그룹으로 나뉩니다. 클라이언트 피어와 다른 모든 라우터(비-클라이언트 피어). 경로 반사기는 두 그룹 간의 경로를 반사합니다. 경로 반사기와 해당 클라이언트 피어는 클러스터를 형성합니다. 비-클라이언트 피어는 완전 메시(full-mesh)로 연결되어야 하지만 클라이언트 피어는 그럴 필요가 없습니다. 클러스터의 클라이언트는 클러스터 외부의 IBGP 스피커와 통신하지 않습니다.

경로 반사기가 라우팅 정보를 수신하면 다음 작업을 완료합니다.

a. 외부 BGP 스피커의 경로를 모든 클라이언트와 비-클라이언트 피어에게 브로드캐스트합니다.
b. 비-클라이언트에서 모든 클라이언트에게 경로를 브로드캐스트합니다.
c. 클라이언트의 경로를 모든 클라이언트와 비-클라이언트 피어에게 브로드캐스트합니다. 따라서 클라이언트 피어는 완전 메시로 연결될 필요가 없습니다.

다음 라우터 구성 명령을 사용하여 로컬 라우터를 반사기로 구성하고 이웃을 경로 반사기 클라이언트로 지정합니다:

| 명령 | 설명 |
|---|---|
| **neighbor** *ip-address* **route-reflector-client** | 로컬 라우터를 경로 반사기로 구성하고 이웃을 클라이언트로 지정합니다. |

하나의 AS 는 여러 개의 경로 반사기를 가질 수 있으며, 경로 반사기가 다른 경로 반사기를 처리하는 방식은 IBGP 스피커를 처리하는 방식과 동일합니다. 일반적으로 클라이언트 클러스터는 하나의 경로 반사기만 가지고 있으며, 클러스터는 경로 반사기의 라우터 ID 로 식별됩니다. 중복성을 높이고 단일 노드의 실패를 방지하기 위해 클러스터는 둘 이상의 경로 반사기를 가질 수 있습니다. 이 경우 클러스터의 모든 경로 반사기는 4 비트 클러스터 ID 로 구성되어야 경로 반사기가 동일 클러스터에 있는 경로 반사기의 업데이트 정보를 식별할 수 있습니다. 동일 클러스터에 속하는 모든 경로 반사기는 완전 메시(full-mesh)로 연결되어야 하며, 동일한 클라이언트 및 비-클라이언트 피어 집합을 가져야 합니다.

클러스터에 둘 이상의 경로 반사기가 있는 경우 다음 BGP 구성 명령을 사용하여 클러스터 ID 를 구성할 수 있습니다.

| 명령 | 설명 |
|---|---|
| **bgp** *cluster-id cluster-id* | cluster-ID 설정 |

Route reflector 구성 예제는 "BGP route reflector 구성 예제"를 참조하십시오.

(6) Peer entity 종료

다음 BGP 구성 명령을 사용하여 BGP neighbor 을 종료하십시오:

| 명령 | 설명 |
|---|---|
| **neighbor** {*ip-address* \| *peer-group-name*} **shutdown** | BGP neighbour 종료 |

이전(에) 종료된 neighbor 를 활성화하려면 다음 BGP 구성 명령을 사용하십시오:

| 명령 | 설명 |
| --- | --- |
| **no neighbor** {*ip-address* \| *peer-group-name*} **shutdown** | BGP neighbour 활성화 합니다. |

(7) 다중 홉 외부 피어(peer) 구성

기본적으로 외부 피어는 직접 연결된 네트워크에 있어야 합니다. 다중 홉 외부 피어를 구성하려면 다음 작업을 수행해야 합니다:

| 명령 | 설명 |
| --- | --- |
| **neighbor** {*ip-address* \| *peer-group-name*} **ebgp-multihop** ttl | BGP neighbor 을 다중 홉 외부 피어로 구성합니다. |

(8) BGP 경로의 관리 거리 구성

관리 거리는 서로 다른 라우팅 프로토콜의 우선 순위를 측정하는 방법의 일종입니다. BGP 는 외부 거리, 내부 거리, 로컬 거리의 세 가지 다른 관리 거리를 사용합니다. 외부 BGP 에서 얻은 경로는 외부 거리가 할당되고, 내부 BGP 에서 얻은 경로는 내부 거리가 할당되며, 로컬 경로는 로컬 거리가 할당됩니다. 다음 BGP 구성 명령을 사용하여 BGP 경로 관리 거리를 구성하십시오:

| 명령 | 설명 |
| --- | --- |
| **distance bgp** {**external-distance**\| **internal-distance**\| **local-distance**} | BGP 경로 관리 거리를 구성합니다. |

BGP 경로의 관리 거리를 변경하는 것은 위험하며 일반적으로 권장되지 않습니다. 외부 거리는 다른 모든 동적 라우팅 프로토콜의 거리보다 짧아야 하고, 내부 거리는 다른 모든 동적 라우팅 프로토콜의 거리보다 길어야 합니다.

(9) BGP 타이머 조정

다음 BGP 구성 명령을 사용하여 특정 이웃의 BGP "keepalive" 및 "holdtime" 타이머를 조정하십시오:

| 명령 | 설명 |
| --- | --- |
| **neighbor** *[ip-address \| peer group-name]* **timers** *keepalive holdtime* | 지정된 피어 또는 피어 커뮤니티에 대한 "keepalive" 및 "holdtime" 타이머 간격(단위: 초)을 설정합니다. |

"no neighbor timers" 명령을 사용하여 BGP 이웃 또는 피어 커뮤니티의 타이머 간격을 기본값으로 재설정합니다.

(10) 서로 다른 AS(Autonomous System)에서 온 경로의 MED 비교

MED 는 여러 경로 중에서 최적의 경로를 선택할 때 고려해야 할 매개변수입니다. MED 값이 낮은 경로가 MED 값이 높은 경로보다 우선적으로 고려됩니다.
기본적으로 최적 경로 선택 과정에서 MED 비교는 동일한 AS 에서 온 경로 간에만 이루어집니다. 경로가 어느 AS 에서 왔는지에 관계없이 라우팅 선택 시 MED 비교를 허용할 수 있습니다.

위의 목적을 달성하려면 다음 BGP 구성 명령을 사용합니다:

| 명령 | 설명 |
|---|---|
| **bgp always-compare-med** | 서로 다른 AS 의 경로 간 MED 비교를 허용합니다. |

(11) BGP 이웃에 대한 MD5 인증 구성

AS 간의 안전한 라우팅 정보 전달을 보장하기 위해 TCP 에서 제공하는 MD5 옵션을 통해 BGP 연결에 대한 비밀번호 인증을 수행합니다.

이전의 목적을 달성하려면 다음 명령을 실행합니다:

| 명령 | 설명 |
|---|---|
| **Neighbor A.B.C.D password LINE** | BGP 이웃의 MD5 인증을 활성화하고 비밀번호를 설정합니다. |

**no neighbor A.B.C.D password** 명령을 실행하여 BGP 이웃의 MD5 인증을 취소할 수 있습니다.

## 52.4. BGP 모니터링 및 유지관리

관리자는 BGP 라우팅 테이블 또는 기타 데이터베이스의 내용을 표시하거나 삭제할 수 있습니다. 물론 상세한 통계 정보도 표시할 수 있습니다.

다음은 관련 작업입니다:

(1) BGP 라우팅 테이블 및 데이터베이스 삭제
(2) 라우팅 테이블 및 시스템 통계 정보 표시
(3) BGP 정보 추적

### 52.4.1. BGP 라우팅 테이블 및 BGP 데이터베이스 삭제

다음 표는 고속 캐시 삭제, 테이블 삭제 또는 BGP 데이터베이스 삭제와 관련된 작업을 나열합니다. 다음 표에 나열된 모든 명령은 EXEC 모드에서 실행됩니다.

| 명령 | 설명 |
|---|---|
| **clear ip bgp *** | Resets all BGP connections. 모든 BGP 연결을 재설정합니다 |
| **clear ip bgp** *as-number* | Resets the BGP connections of the designated autonomous system. 지정된 자율 시스템 (AS)의 BGP 연결을 재설정합니다. |
| **clear ip bgp** *address* | Resets the BGP connections of the designated neighbor. 지정된 이웃의 BGP 연결을 재설정합니다. |
| **clear ip bgp** *address* soft {**in**\|**out**} | Deletes the incoming database or the outgoing database of the designated neighbor. 지정된 이웃의 수신 데이터베이스 또는 송신 데이터베이스를 삭제합니다. |
| **clear ip bgp** *aggregates* | Deletes the routes generated in route aggregation. 경로 집합화에서 생성된 경로를 삭제합니다. |
| **clear ip bgp** *networks* | Deletes the routes generated during the forwarding process. 전달 과정에서 생성된 경로를 삭제합니다. |
| **clear ip bgp** *redistribute* | Deleting the routes generated by the **network** command. 네트워크 명령으로 생성된 경로를 삭제합니다. |

### 52.4.2. 라우팅 테이블 및 시스템 통계 정보 표시

BGP 라우팅 테이블 또는 데이터베이스에 대한 자세한 통계 정보가 표시됩니다. 제공된 정보는 자원 활용도를 결정하고 네트워크 문제 해결에 도움이 될 수 있습니다. 또한 노드 도달 가능성에 대한 정보도 표시될 수 있습니다.

다음 명령을 실행하여 다양한 종류의 라우팅 통계 정보를 표시할 수 있습니다:

| 명령 | 설명 |
|---|---|
| **show ip bgp** | Displays the BGP router in the system. 시스템의 BGP 라우팅 테이블을 표시합니다. |

| | |
|---|---|
| **show ip bgp prefix** | Displays the routes which match the designated prefix list. 지정된 접두사 목록과 일치하는 경로를 표시합니다. |
| **show ip bgp community** | Displays the statistics information about the group attribute. 그룹 속성에 대한 통계 정보를 표시합니다. |
| **show ip bgp regexp** *regular-expression* | Displays the routes which match the designated regular expression. 지정된 정규 표현식과 일치하는 경로를 표시합니다. |
| **show ip bgp** *network* | Displays the designated BGP route. 지정된 BGP 경로를 표시합니다. |
| **show ip bgp neighbors** *address* | Displays the information about the TCP and the BGP connections of the designated neighbor. 지정된 이웃의 TCP 및 BGP 연결에 대한 정보를 표시합니다 |
| **show ip bgp neighbors** *[address]* [**received-routes | routes | advertised-routes**] | Displays the routes learned from the special BGP neighbor. 특정 BGP 이웃으로부터 학습한 경로를 표시합니다. |
| **show ip bgp paths** | Displays the information about all BGP paths in the database. 데이터베이스에 있는 모든 BGP 경로에 대한 정보를 표시합니다. |
| **show ip bgp summary** | Displays the states of all BGP connections. 모든 BGP 연결의 상태를 표시합니다. |

### 52.4.3. BGP 정보 추적

BGP 정보를 추적하여 BGP 연결 설정 및 경로 전송/수신을 관찰할 수 있으며, 이를 통해 문제를 찾고 해결하는 데 도움이 됩니다.

BGP 정보를 추적하는 명령은 다음 표에 나와 있습니다:

| 명령 | 설명 |
|---|---|
| **debug ip bgp *** | Tracks the general BGP information. 일반적인 BGP 정보를 추적합니다. |
| **debug ip bgp all** | Tracks all BGP information. 모든 BGP 정보를 추적합니다. |
| **debug ip bgp fsm** | Tracks the BGP state machine. BGP 상태를 추적합니다. |
| **debug ip bgp keepalive** | Tracks the KeepAlive packets of BGP. BGP 의 KeepAlive 패킷을 추적합니다. |
| **debug ip bgp** *open* | Tracks the OPEN packets of BGP. BGP 의 OPEN 패킷을 추적합니다. |
| **debug ip bgp** *update* | Tracks the UPDATE packets of BGP. BGP 의 UPDATE 패킷을 추적합니다. |

## 52.5. BGP 구성 예시

다음 섹션에서는 BGP 구성 예시를 제공합니다:

### 52.5.1. BGP 라우트 맵 예시

다음 예시는 route-map 을 사용하여 이웃으로부터 들어오는 경로 속성을 변경하는 방법을 설명합니다. 이웃 140.222.1.1 에서 오는 모든 경로 중 ASPATH 접근 리스트 "aaa"의 요구 사항을 충족하는 경로의 가중치를 200 으로 설정하고, 로컬 우선순위 값을 250 으로 설정하며, 해당 경로는 수락됩니다. 그 외의 경로는 모두 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 예시에서, route-map "freddy"의 첫 번째 항목은 자율 시스템 690 에서 시작하는 모든 경로의 MED 속성을 127 로 설정합니다. 두 번째 항목은 위 조건을 충족하지 않는 경로가 이웃 1.1.1.1 로 전송되도록 허용합니다.

```
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
```

다음 예에서는 route-map 을 사용하여 경로 재배포에서 경로를 변경하는 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
```

#### 52.5.2. 이웃 구성 예시

다음 예시에서, BGP 라우터는 AS109 에 속하며 두 개의 네트워크를 생성합니다. 이 라우터는 3 개의 이웃을 가지고 있습니다: 첫 번째 이웃은 외부 이웃(다른 AS 에 속함), 두 번째는 내부 이웃(같은 AS 번호를 사용), 세 번째는 또 다른 외부 이웃입니다.

```
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
```

#### 52.5.3. 이웃을 기준으로 한 BGP 경로 필터링 예시

다음은 이웃을 기준으로 한 BGP 경로 필터링 예시입니다. AS-path 접근 리스트 “test1”을 통과하는 경로는 가중치 값이 100 으로 설정됩니다. 오직 AS-path 접근 리스트 “test2”를 통과하는 경로만 193.1.12.10 으로 전송되며, 마찬가지로 접근 리스트 “test3”을 통과하는 경로만 193.1.12.10 에서 수락됩니다:

```
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 .*
```

#### 52.5.4. 인터페이스를 기준으로 한 BGP 경로 필터링 예시

다음은 인터페이스를 기준으로 한 경로 필터링 구성 예시입니다. 이 구성은 인터페이스 e1/0 에서 오는 경로를 접근 리스트 "acl"을 통해 필터링합니다.

```
router bgp 122
filter e1/0 in access-list acl
```

다음 예시는 접근 리스트 "filter-network"를 사용하여 경로의 네트워크 번호를 필터링하고, 동시에 접근 리스트 "filter-gateway"를 사용하여 s1/0 인터페이스에서 오는 경로의 게이트웨이 주소를 필터링하는 구성입니다.

```
router bgp 100
filter s1/0 in access-list filter-network gateway filter-gateway
```

다음 예시는 접두사 목록 "filter-prefix"를 사용하여 경로의 네트워크 번호를 필터링하고, 동시에 접근 리스트 "filter-gateway"를 사용하여 모든 인터페이스에서 오는 경로의 게이트웨이 주소를 필터링하는 구성입니다.

```
router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway
```

#### 52.5.5. 접두사 목록을 사용한 경로 필터링 구성 예시

다음 예시에서는 기본 경로 0.0.0.0/0 을 거부합니다.

```
ip prefix-list abc deny 0.0.0.0/0
```

다음 예시에서는 접두사 35.0.0.0/8 과 일치하는 경로를 허용합니다:

```
ip prefix-list abc permit 35.0.0.0/8
```

다음 예시에서는 BGP 프로세스가 길이가 /8 에서 /24 사이인 접두어만 수락하도록 구성됩니다.

```
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 구성에서는 라우터가 모든 인터페이스에서 오는 경로를 필터링하며, 접두사가 /8 에서 /24 사이인 경로만 수락합니다.

router bgp 12
filter * in prefix-list max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24

다음은 접두사 목록 구성의 다른 예시들입니다:
다음 예시는 네트워크 192/8 에서 접두사 길이가 24 이하인 경로를 허용합니다:

ip prefix-list abc permit 192.0.0.0/8 le 24

다음 예시는 네트워크 192/8 에서 접두사 길이가 25 보다 큰 경로를 거부합니다:

ip prefix-list abc deny 192.0.0.0/8 ge 25

다음 예시는 모든 주소 공간에서 접두사 길이가 8 보다 크고 24 보다 작은 경로를 허용합니다:

ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24

다음 예시는 모든 주소 공간에서 접두사 길이가 25 보다 큰 모든 경로를 거부합니다:

ip prefix-list abc deny 0.0.0.0/0 ge 25

이 예시는 네트워크 10/8 에서 오는 경로를 거부합니다. 클래스 A 네트워크 10.0.0.0/8 의 마스크가 32 비트보다 작거나 같으면 해당 네트워크에서 오는 모든 경로가 거부됩니다:

ip prefix-list abc deny 10.0.0.0/8 le 32

다음 예시는 네트워크 204.70.1.0/24 에서 접두사 길이가 25 보다 큰 경로를 거부합니다:

ip prefix-list abc deny 204.70.1.0/24 ge 25

다음 예시는 모든 경로를 허용합니다:

ip prefix-list abc permit any

### 52.5.6. BGP 경로 집합화 예시

다음 예시는 BGP 에서 경로 집합화를 생성하는 방법을 설명합니다. 이는 경로 재분배 또는 조건부 경로 집합화 기능을 사용하여 생성할 수 있습니다.

다음 예시에서는 "redistribute static" 명령을 사용하여 집합화된 경로 193.*.*.*:를 재분배합니다.

ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
redistribute static

지정된 범위 내에 라우팅 테이블에 하나 이상의 경로가 있는 경우, 다음 구성은 BGP 라우팅 테이블에 집계 경로를 생성합니다. 집계 경로는 AS 에서 온 것으로 간주되며, 정보 손실 가능성을 나타내기 위해 "원자" 속성을 갖습니다.

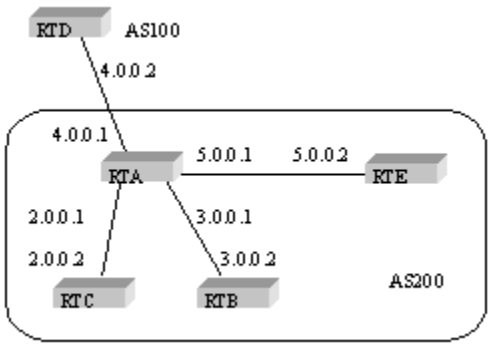
router bgp 100
aggregate 193.0.0.0/8

다음 예제에서는 집계 경로 193.*.*.*을 생성할 뿐만 아니라 보다 구체적인 경로를 모든 이웃에게 브로드캐스트하는 것도 금지합니다:

router bgp 100
aggregate 193.0.0.0/8 summary-only

### 52.5.7. BGP 경로 리플렉터 예시

다음은 경로 반사기 구성의 예입니다. RTA, RTB, RTC, RTE 는 모두 동일한 자율 시스템 AS200 에 속하고, RTA 는 경로 반사기 역할을 하며, RTB 와 RTC 는 경로 반사기 클라이언트이고, RTE 는 일반 IBGP 이웃입니다. RTD 는 AS100 에 속하며, RTA 와 EBGP 연결을 생성하며, 구성은 다음과 같이 설명됩니다:




**RTA 구성:**

```
interface s1/0
ip address 2.0.0.1 255.0.0.0
!
interface s1/1
ip address 3.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.2 remote-as 200 /*RTC IBGP*/
neighbor 2.0.0.2 route-reflector-client
neighbor 3.0.0.2 remote-as 200 /*RTB IBGP*/
neighbor 3.0.0.2 route-reflector-client
neighbor 5.0.0.2 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 s1/0
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 s1/0
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:**

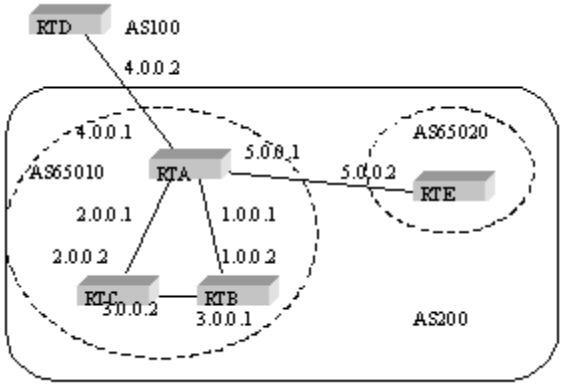
```
interface s1/0
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200   /*RTA EBGP*/
network 14.0.0.0/8
 !
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

**RTE 구성:**

```
interface s1/0
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
```

### 52.5.8. BGP 연합 예시

다음은 연합의 구성입니다. RTA, RTB, RTC 는 IBGP 연결을 생성하고, 개인 자율 시스템 65010 에 속합니다. RTE 는 다른 개인 자율 시스템 65020 에 속합니다. RTE 와 RTA 는 연합의 내부 EBGP 연결을 설정합니다. AS65010 AS65020 은 식별자가 AS200 인 연합을 포함합니다. RTD 는 자율 시스템 AS100 에 속하고, RTD 는 RTA 를 통해 자율 시스템 200 과 EBGP 연결을 설정합니다.




**RTA 구성:**

```
interface s1/0
ip address 1.0.0.1 255.0.0.0
!
interface s1/1
ip address 2.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
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 s1/0
ip address 1.0.0.2 255.0.0.0
!
interface s1/1
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 s1/0
ip address 2.0.0.2 255.0.0.0
!
interface s1/1
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 s1/0
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 s1/0
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*/
```

### 52.5.9. BGP 그룹 속성을 포함한 경로 맵 예시

이 섹션에는 BGP 커뮤니티 속성을 사용한 경로 맵을 사용하는 세 가지 예가 포함되어 있습니다.

첫 번째 예에서 "route map set-community"는 이웃 171.69.232.50 의 결과 업데이트에 적용됩니다. 액세스 목록 aaa 를 통과하는 경로에 대해 값 "no-export"를 갖는 특수 커뮤니티 속성을 설정하고, 다른 경로는 정상적으로 브로드캐스트합니다. 이 특수 커뮤니티 속성은 AS200 의 BGP 스피커가 자율 시스템 외부에서 경로를 광고하는 것을 자동으로 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
```

두 번째 예에서 "route map set-community"는 이웃 171.69.232.90 의 결과 업데이트에 사용됩니다. AS70 에서 시작하는 모든 경로는 커뮤니티 속성 200 에 값 200 을 삽입하고 다른 모든 경로는 정상적으로 광고됩니다.

```
router 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 .*
```

세 번째 예에서, 경로의 커뮤니티 속성 값에 따라 이웃 171.69.232.55 의 경로에 대한 MED 및 로컬 선호도 값을 선택적으로 설정합니다. 커뮤니티 목록 com1 과 일치하는 모든 라우터는 MED 를 8000 으로 설정합니다. 여기에는 커뮤니티 값이 "100 200 300" 또는 "900 901"인 경로가 포함될 수 있습니다. 이러한 경로에는 다른 속성 값이 있을 수 있습니다.

커뮤니티 목록 com2 를 전송하는 모든 경로는 로컬 선호도 값을 500 으로 설정됩니다.

다른 모든 경로는 로컬 우선 순위 값을 50 으로 설정합니다. 따라서 이웃 171.69.232.55 의 나머지 모든 경로는 우선 순위가 50 입니다.

```
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
```

# 53. 기본 멀티캐스트 명령

## 53.1. 기본 멀티캐스트 명령어

### 53.1.1. Debug ip mpacket

#### (1) 구문

멀티캐스트 패킷의 처리를 추적하려면 "debug ip mpacket" 명령을 사용할 수 있으며, "no" 형식을 사용하여 디버그 정보를 종료할 수 있습니다.

**debug ip mpacket** *access-list group-address* **detail**
**no debug ip mpacket**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *access-list* | 추적할 멀티캐스트 패킷의 범위 |
| *group-address* | 추적할 멀티캐스트 패킷 그룹 주소 |
| ***detail*** | 멀티캐스트 패킷 처리에 대한 세부 정보 |

#### (3) 기본값

디버그 정보 출력 종료

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

이 명령은 IGMP-호스트 종료 프로토콜의 주요 프로세스를 추적하는 데 사용됩니다.

#### (6) 예제

다음 예제는 멀티캐스트 패킷 처리 상황을 보여줍니다.
이 내용은 인터페이스 e0/1 에서 100.168.20.151 소스 IP 로부터 224.1.1.1 목적지 IP 로 멀티캐스트 패킷이 수신되었고, 그 후 192.168.20.99 IP 에서 224.0.0.5 로 응답 패킷이 전송되었음을 나타냅니다.

router#debug ip mpacket
MINPUT : IP Ethernet0/1 (100.168.20.151,224.1.1.1) , len=112
MOUTPUT : IP Ethernet0/1 (192.168.20.99,224.0.0.5) , len=64

### 53.1.2. Debug ip mroute-cache

#### (1) 구문

"debug ip mroute-cache" 명령을 사용하여 "mroute-cache" 추적 기능을 활성화하고 멀티캐스트 라우팅 캐시의 변화를 볼 수 있습니다. "no" 형식을 사용하여 추적을 종료할 수 있습니다.

**debug ip mroute-cache** *group-address*
**no debug ip mroute-cache**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *group-address* | 추적할 멀티캐스트 라우팅 캐시 그룹 주소 |

#### (3) 기본값

모든 추적 기능 종료

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

이 명령은 멀티캐스트 라우팅 캐시의 추가/삭제 변화를 확인하는 데 사용됩니다.

#### (6) 예제

다음 예제는 멀티캐스트 라우팅 캐시에서 (192.168.20.97, 230.0.0.1) 캐시의 생성 및 타임아웃을 보여줍니다.

router#debug ip mroute-cache
MRC: create (192.168.20.97,230.0.0.1) mroute-cache
MRC: expired (192.168.20.97,230.0.0.1) mroute-cache

### 53.1.3. Debug ip multicast

#### (1) 구문

"debug ip multicast" 명령을 사용하여 멀티캐스트 이벤트 추적 기능을 활성화하고, 멀티캐스트 프로토콜과 mroute 간의 상호작용을 확인할 수 있습니다. "no" 형식을 사용하여 기능을 종료할 수 있습니다.

**debug ip multicast [alert | border-router]**
**no debug ip multicast [alert | border-router]**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| **alert** | 멀티캐스트 라우팅 구성 요소 간의 경고 상호작용을 추적 |
| **border-router** | 멀티캐스트 경계 라우터 MBR 관련 이벤트 추적 |

#### (3) 기본값

모든 추적 기능 종료

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

"alert"는 멀티캐스트 라우팅 프로토콜과 mroute 간의 표준 이벤트를 정의합니다. 예를 들어, (S, G)의 생성 경고/삭제 경고와 관련된 내용을 추적할 수 있습니다. "debug ip multicast alert" 명령을 사용하여 이러한 경고를 볼 수 있습니다. "border-router"는 각 멀티캐스트 라우팅 프로토콜이 하나의 "구성 요소"로서 MBR 과의 상호작용 정보를 볼 수 있습니다.

#### (6) 예제

다음 예제에서는 alert 라우터가 출력되는 예시입니다:
router#debug ip multicast alert
MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
MBR: [(S, G) creation alert], originated by 없음, sent to all components
MBR:  src = 192.168.20.110, grp = 239.0.0.100

MBR:  sent to owner OLNK first
MBR: [(S, G) join alert], originated by 없음, sent to OLNK
MBR:  src = 192.168.20.110, grp = 239.0.0.100
MBR: [(S, G) firstuse alert], originated by 없음, sent to OLNK
MBR:  src = 192.168.20.110, grp = 239.0.0.100
MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
MBR:  src = 192.168.20.110, grp = 239.0.0.100

#### 53.1.4. ip multicast-statistic

**(1) 구문**

IP 멀티캐스트 패킷 통계를 활성화하려면 다음 명령을 실행합니다. 기본 설정으로 돌아가려면 "no" 형식을 사용합니다.

**ip multicast-statistic**
**no ip multicast-statistic**

**(2) 매개변수**

없음

**(3) 기본값**

비활성화

**(4) 명령어 모드**

전역 설정 모드

**(5) 사용 지침**

멀티캐스트 통계는 PIM-SM 에서 SPT 로 전환되는 증거를 제공합니다. 전환 임계값을 구성하면 이 명령을 활성화해야 합니다. 이 명령이 비활성화되면 스위치는 멀티캐스트 통계를 생성하지 않습니다.

**(6) 예제**

다음 예제는 스위치에서 멀티캐스트 패킷 통계를 구성하는 방법을 보여줍니다:
switch_config#ip multicast-statistic

**(7) 연관 명령어**

없음

### 53.1.5. ip multicast-routing

**(1) 구문**

"ip multicast-routing" 명령을 사용하여 IP 멀티캐스트 패킷 전송 기능을 활성화하고, "no ip multicast-routing" 명령을 사용하여 이 기능을 비활성화합니다.

**ip multicast-routing**
**no ip multicast-routing**

**(2) 매개변수**

없음

**(3) 기본값**

멀티캐스트 패킷을 전송하지 않음.

**(4) 명령어 모드**

전역 설정 모드

**(5) 사용 지침**

이 기능을 비활성화하면 라우터는 더 이상 멀티캐스트 패킷을 전송하지 않으며, 멀티캐스트 라우팅 목록과 멀티캐스트 캐시는 비어 있습니다.

**(6) 예제**

다음 예제는 라우터에서 멀티캐스트 패킷 전송을 활성화하는 방법을 보여줍니다:
router_config#ip multicast-routing

**(7) 연관 명령어**

show ip mroute mfc

### 53.1.6. ip multicast route-limit

#### (1) 구문

"ip multicast route-limit" 명령을 사용하여 멀티캐스트 라우팅 항목의 최대 수를 설정하고, "no ip multicast route-limit" 명령을 사용하여 제한을 해제합니다.

**ip multicast route-limit** *size*
**no ip multicast route-limit** *size*

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *size* | 멀티캐스트 라우팅 항목의 최대 수 |

#### (3) 기본값

멀티캐스트 라우팅 항목 수는 제한이 없습니다.

#### (4) 명령어 모드

전역 설정 모드

#### (5) 사용 지침

이 기능을 구성하면 멀티캐스트 라우팅 항목 수가 제한됩니다.

#### (6) 예제

다음 예제는 멀티캐스트 라우팅 항목 수를 2000 으로 제한하는 방법을 보여줍니다:
router_config#ip multicast route-limit 2000

#### (7) 연관 명령어

show ip mroute mfc

### 53.1.7. ip multicast boundary

#### (1) 구문

"ip multicast boundary" 명령을 사용하여 멀티캐스트 패킷을 처리할 수 있는 포트 범위를 관리할 수 있습니다. 이 명령은 포트에서 입력 및 출력 패킷에 유효합니다. "no ip multicast boundary" 명령을 사용하여 이 명령을 취소할 수 있습니다.

**ip multicast boundary** *access-list*
**no ip multicast boundary**

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| *access-list* | 멀티캐스트 패킷을 처리할 범위를 지정하는 액세스 리스트 이름 |

**(3) 기본값**

모든 멀티캐스트 패킷을 처리합니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

이 기능을 구성하면 포트에서 처리할 수 있는 멀티캐스트 패킷의 범위가 제한됩니다.

**(6) 예제**

다음 예제는 포트 e1/0 에서 처리할 수 있는 멀티캐스트 패킷의 범위를 "testacl" 액세스 리스트에 의해 제한하는 방법을 보여줍니다:
router_config_e1/0#ip multicast boundary testacl

### 53.1.8. ip multicast helper-map

**(1) 구문**

"ip multicast helper-map" 명령을 사용하여 두 개의 브로드캐스트 네트워크를 멀티캐스트 네트워크와 연결하며, "no ip multicast helper-map" 명령을 사용하여 이 명령을 취소할 수 있습니다.

**ip multicast helper-map** {group-address|**broadcast**} {broadcast-*address |multicast-address } access-list*

**no ip multicast helper-map** {group-address|**broadcast**}
{*broadcast-address* / *multicast-address*} *access-list*

**(2) 매개변수**

| 매개변수 | 설명 |
|---|---|
| group-address | 브로드캐스트 패킷으로 변환할 필요가 있는 멀티캐스트 패킷의 그룹 주소. broadcast-address 키워드와 함께 사용됩니다 |
| **broadcast** | 브로드캐스트 패킷을 멀티캐스트 패킷으로 변환합니다. multicast-address 키워드와 함께 사용됩니다. |
| *broadcast-address* | 변환 후 브로드캐스트 패킷의 대상 주소. group-address 키워드와 함께 사용됩니다. |
| *multicast-address* | 변환 후 멀티캐스트 패킷의 대상 주소. broadcast 키워드와 함께 사용됩니다. |
| *access-list* | 패킷 변환을 위해 포트 번호를 지정하는 데 사용할 IP 확장 액세스 리스트 이름 |

**(3) 기본값**

멀티캐스트 패킷과 브로드캐스트 패킷 간의 변환을 수행하지 않습니다.

**(4) 명령어 모드**

인터페이스 설정 모드

**(5) 사용 지침**

두 개의 브로드캐스트 네트워크가 멀티캐스트 네트워크에 연결될 경우, 첫 번째 홉 라우터에서 소스 브로드캐스트 네트워크와 연결된 멀티캐스트 흐름을 변환하여 멀티캐스트 흐름을 브로드캐스트 흐름으로 바꿀 수 있으며, 마지막 홉 라우터에서 대상 브로드캐스트 네트워크와 연결된 멀티캐스트 흐름을 브로드캐스트 흐름으로 변환할 수 있습니다. 이렇게 하면 두 개의 브로드캐스트 네트워크가 서로 연결되는 동안 멀티캐스트 네트워크의 멀티캐스트 특성을 활용할 수 있습니다. 또한 두 브로드캐스트 네트워크 간에 패킷이 반복 전송되는 것을 방지하고 멀티캐스트 네트워크에서 "빠른 전송" 특성을 활용할 수 있습니다. "ip multicast helper-map"을 사용하기 전에 "ip directed-broadcast" 명령을 포트에 설정해야 합니다.

**(6) 예제**

라우터에서의 구성 예시는 다음과 같습니다: 첫 번째 홉 라우터의 e0 포트에서 "ip directed-broadcast" 명령을 설정하면 링크 브로드캐스트 패킷을 처리할 수 있습니다.

"ip multicast helper-map broadcast 230.0.0.1 testacl1"을 설정하면 포트 번호가 4000("ip forward-protocol" 명령에서 지정)이고 소스 주소가 192.168.20.97/24 (testacl1 지정)인 UDP 브로드캐스트 패킷을, 대상 주소가 230.0.0.1 인 멀티캐스트 패킷으로 변환할 수 있습니다.

마지막 홉 라우터의 e1 포트에서 "ip directed-broadcast" 명령을 설정하면 링크 브로드캐스트 패킷을 처리할 수 있습니다.

"ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2"을
설정하면, 포트 번호가 4000("ip forward-protocol" 명령에서 지정), 소스 주소가 192.168.20.97/24 (testacl2 지정), 대상 주소가 230.0.0.1 인 멀티캐스트 패킷을, 대상 주소가 172.10.255.255 인 브로드캐스트 패킷으로 변환할 수 있습니다.

소스 브로드캐스트 네트워크와 연결된 첫 번째 홉 라우터에서:

```
interface ethernet 0
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim dense-mode
!
ip access-list extended testacl  permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

타겟 브로드캐스트 네트워크와 연결된 마지막 홉 라우터에서:

```
interface ethernet 1
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim dense-mode
!
ip access-list extended testacl2  permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

**(7) 연관 명령어**

ip forward-protocol
ip directed-broadcast

### 53.1.9. ip multicast ttl-threshold

#### (1) 구문

"ip multicast ttl-threshold" 명령을 사용하여 포트에서 멀티캐스트 패킷 TTL 의 최대 임계값을 설정하며, "no ip multicast ttl-threshold" 명령을 사용하여 기본값으로 복원합니다.

**ip multicast ttl-threshold** *ttl-value*
**no ip multicast ttl-threshold**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *ttl-value* | 포트에서 멀티캐스트 패킷 TTL 임계값입니다 |

#### (3) 기본값

포트에서 기본 TTL 임계값은 1 입니다.

#### (4) 명령어 모드

인터페이스 설정 모드

#### (5) 사용 지침

수신/송신 패킷의 TTL 값이 설정된 임계값보다 커야 합니다. 이 명령은 라우터를 경계 라우터로 설정하는 데 사용됩니다.

#### (6) 예제

포트 s0 에서 TTL 임계값을 200 으로 설정하면 TTL 값이 200 보다 큰 멀티캐스트 패킷만 포트에서 수신하거나 송신할 수 있습니다.

```
interface serial 0
ip multicast ttl-threshold 200
```

### 53.1.10. show ip mflow

#### (1) 구문

"show ip mflow" 명령을 사용하여 시스템에서 처리된 글로벌 흐름 정보와 포트에서 처리된 멀티캐스트 흐름 정보를 표시합니다.

**show ip mflow** *[group-address|source-address]***interface**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *group-address* | 표시할 멀티캐스트 흐름 정보의 그룹 주소입니다. |
| *source-address* | 표시할 멀티캐스트 흐름 정보의 소스 주소입니다. |
| **interface** | 표시할 포트의 멀티캐스트 흐름 정보입니다. |

#### (3) 기본값

없음

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

처리된 패킷 수, 잘못된 수신 인터페이스의 패킷 수 및 현재 흐름 값을 표시합니다.

#### (6) 예제

다음 예제는 글로벌 멀티캐스트 흐름 정보를 표시합니다:
router#show ip mflow
IP Multicast Flow
(100.168.20.151,224.1.1.1)
total process : 0  wrong_if_count : 0 curr-flux : 0.00
(192.167.20.131,239.1.1.1)
total process : 0  wrong_if_count : 0 curr-flux : 0.00
다음 예제는 포트 멀티캐스트 흐름 정보를 표시합니다:
router#show ip mflow interface e0/1
IP Multicast Flow
(192.168.20.97,230.0.0.1)
total recv : 21180  total send : 0  curr-in-flux : 0.00 curr-out-flux : 0.00

(100.168.20.151,224.1.1.1)
total recv : 16822400 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
(192.168.20.97,232.0.0.1)
total recv : 240 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
(192.167.20.131,239.1.1.1)
total recv : 103264 total send : 0 curr-in-flux : 0.90 curr-out-flux : 0.00

### 53.1.11. show ip mroute-cache

#### (1) 구문

이 명령어 "show ip mroute-cache"를 사용하여 멀티캐스트 라우팅 캐시 정보를 표시할 수 있습니다.

**show ip mroute-cache [group-address]**

#### (2) 매개변수

| 매개변수 | 설명 |
|---|---|
| *group-address* | 표시할 멀티캐스트 라우팅 캐시의 그룹 주소입니다 |

#### (3) 기본값

없음

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

MRC(Multicast Route Cache)는 전역 멀티캐스트 라우팅 캐시이며, 각 MRC 항목은 (S, G)/(*, G) 정보와 멀티캐스트 라우팅에서 수신된 업스트림/다운스트림 인터페이스 정보를 포함합니다.

#### (6) 예제

다음 예제는 멀티캐스트 라우팅 목록 정보를 표시합니다:
router#show ip mroute-cache
IP Multicast Route Cache

(192.168.20.97, 230.0.0.1)|(192.168.20.97,230.0.0.1)
Incoming interface: Ethernet0/2, Last used : 00:00:34
Outgoing interface list:
Loopback0
(192.168.20.97, 230.0.0.2)|(192.168.20.97,230.0.0.2)
Incoming interface: Ethernet0/2, Last used : 00:00:12
Outgoing interface list:
Loopback1

### 53.1.12. show ip mroute mfc

#### (1) 구문

"show ip mroute mfc" 명령을 사용하여 멀티캐스트 전달 목록 정보를 표시하고 멀티캐스트 기능을 활성화할 수 있습니다.

show ip mroute mfc

#### (2) 매개변수

없음

#### (3) 기본값

없음

#### (4) 명령어 모드

슈퍼바이저 모드

#### (5) 사용 지침

MFC(Multicast Forwarding Cache)는 전역 멀티캐스트 전달 목록이며, 멀티캐스트 패킷은 이를 통해 전달됩니다. 각 MFC 항목은 (S, G)/(*, G) 정보와 업스트림/다운스트림 인터페이스 정보를 포함합니다.

#### (6) 예제

다음 예제는 멀티캐스트 전달 목록 정보를 표시합니다:
router#show ip mroute mfc
IP Multicast Forwarding Cache
(192.168.20.110/32, 239.0.0.100/32)

```
 Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
 Outgoing interface list:
   Loopback0, owned by OLNK
(192.168.20.110/32, 239.0.0.101/32)
 Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
 Outgoing interface list:
   Loopback0, owned by OLNK
(192.168.20.138/32, 239.1.1.1/32)
 Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
 Outgoing interface list:
 Loopback0, owned by OLNK
```

**(7) 연관 명령어**

show ip mroute olnk
show ip mroute static

# 54. NTP

## 54.1. NTP master

장치가 NTP 서버로 설정되지 않은 경우 (ntp server 명령어가 설정되지 않은 경우), 반드시 ntp master primary 명령어를 설정해야 합니다. 그렇지 않으면 스위치는 시간 동기화 서비스를 제공할 수 없습니다.

ntp master secondary 명령어는 스위치가 NTP 서버를 설정한 경우 실행해야 합니다.

스위치가 NTP 클라이언트에게 시간 동기화 서비스를 제공하려면 자신의 시간 동기화가 먼저 완료되어야 합니다.

### 54.1.1. 구문

**ntp master primary**
장치를 최상위 NTP 서버(stratum=1) 로 설정하려면 위 명령어를 실행하십시오.

**ntp master secondary**
장치를 보조 NTP 서버로 설정하려면 위 명령어를 실행하십시오.

**no ntp master**
NTP 서버 기능을 비활성화하려면 위 명령어를 실행하십시오.

### 54.1.2. 예제

```
Switch_config#ntp master primary
Switch_config#ntp master secondary
Switch_config#no ntp master
```

### 54.1.3. 연관 명령어

ntp server
ntp peer

## 54.2. NTP authentication enable

보안성이 요구되는 네트워크 환경에서는 반드시 NTP 인증을 활성화해야하며, NTP 인증을 활성화하면, 클라이언트가 인증된 서버와만 동기화할 수 있도록 보장됩니다.

이를 통해 비인가된 서버에서 잘못된 시간 정보를 수신하는 것을 방지할 수 있습니다.

#### 54.2.1. 구문

**ntp authentication enable**

**no ntp authentication enable**

NTP 인증 기능을 활성화하려면 위 명령어를 실행하십시오.

기본 설정으로 되돌리려면 위 명령어의 no 형식을 사용하십시오.

#### 54.2.2. 연관 명령어

ntp authentication key
ntp authentication trusted-key

## 54.3. NTP authentication key

이 명령어는 ID 인증 키를 설정하는 데 사용됩니다.
클라이언트와 서버는 동일한 키 일련 번호와 키 값을 설정해야 하며, 그렇지 않으면 시간 동기화를 수행할 수 없습니다.

NTP 인증 키를 설정한 후, ntp authentication trusted-key 명령어를 사용하여 해당 키를 신뢰할 수 있는 키로 설정하십시오.

신뢰할 수 있는 키가 삭제되면 신뢰할 수 있는 키 목록에서도 자동으로 제거되므로, no ntp authentication trusted-key 명령어를 실행할 필요가 없습니다.

| 매개변수 | 설명 |
|---|---|
| *keyid* | 인증 키의 일련 번호. (값 범위: 1~4,294,967,295) |
| *password* | 인증 키 값 (길이: 1~50 자) |

#### 54.3.1. 구문

**ntp authentication key keyid md5 password**
**no ntp authentication key keyid**

NTP 인증 키를 설정하려면 위 명령어를 실행하십시오. 기본 설정으로 되돌리려면 위 명령어의 no 형식을 사용하십시오.

#### 54.3.2. 예제

Switch_config#ntp authentication key 5 md5 abc123
Switch_config#no ntp authentication key 5

#### 54.3.3. 연관 명령어

ntp authentication enable
ntp authentication trusted-key

## 54.4. NTP authentication trusted-key

NTP 인증 기능이 활성화된 경우, 클라이언트는 신뢰할 수 있는 키를 제공하는 서버와만 동기화할 수 있습니다.

서버가 제공하는 키가 신뢰할 수 없는 경우, 클라이언트는 해당 NTP 서버와 시간 동기화를 수행할 수 없습니다.

이 명령어는 NTP 인증 키를 설정한 후에 실행해야 합니다.

삭제된 신뢰할 수 있는 키는 자동으로 목록에서 제거됩니다.

따라서 no ntp authentication trusted-key 명령어를 따로 실행할 필요가 없습니다.

| 매개변수 | 설명 |
|---|---|
| *keyid* | 신뢰할 수 있는 키의 일련 번호 (값 범위: 1~4,294,967,295) |

#### 54.4.1. 구문

**ntp authentication trusted-key keyid**
**no ntp authentication trusted-key keyid**

생성된 키를 신뢰할 수 있는 키(trusted key) 로 설정하려면 위 명령어를 실행하십시오. 기본 설정으로 되돌리려면 위 명령어의 no 형식을 사용하십시오.

#### 54.4.2. 예제

Switch_config#ntp authentication trusted-key 5
Switch_config#no ntp authentication trusted-key 5

#### 54.4.3. 연관 명령어

ntp authentication enable
ntp authentication key

## 54.5. NTP server

NTP 서버를 설정하면 장치는 서버와 시간 동기화를 수행할 수 있지만, 서버의 시간이 장치로 동기화되지는 않습니다. 여러 개의 ntp server 명령을 설정할 수 있습니다.

공용 네트워크의 NTP 서버를 사용할 경우, 최소 4 개의 서로 다른 NTP 서버를 설정해야 잘못된 시간 소스를 배제할 수 있습니다.

| 매개변수 | 설명 |
|---|---|
| *ip-address* | NTP 서버의 IP 주소 |
| *number* | NTP 버전 번호. 값 범위: 〈1-4〉, 기본값은 4 |
| *keyid* | NTP 서버로 NTP 패킷을 전송할 때, 해당 keyid에 해당하는 키를 사용하여 패킷 정보를 추출하여 인증을 수행합니다. 값 범위: 1~4294967295.<br>이 매개변수를 설정하지 않으면 장치는 서버의 ID 를 인증하지 않으며, 반대로 서버도 장치를 인증하지 않습니다. |

#### 54.5.1. 구문

**ntp server ip-address [version number | key keyid]***
**no ntp server ip-address**

NTP 서버를 설정하려면 위 명령어를 실행하십시오. 기본 설정으로 되돌리려면 위 명령어의 no 형식을 사용하십시오.

#### 54.5.2. 예제

Switch_config#ntp server 1.1.1.1 version 4 key 5

#### 54.5.3. 연관 명령어

ntp authentication enable
ntp authentication key
ntp authentication trusted-key

## 54.6. NTP peer

NTP 피어를 지정하면, 피어가 동기화된 경우에만 장치가 피어와 시간 동기화를 수행할 수 있습니다. 이 명령어는 주로 NTP 서버 간의 상호 백업을 위해 사용되며, 클라이언트에는 적용되지 않습니다.

NTP 서버를 지정하려면 ntp server 명령어를 사용하십시오.

| 매개변수 | 설명 |
|---|---|
| *ip-address* | NTP 피어의 IP 주소 |
| *number* | NTP 버전 번호. 값 범위: 1~4, 기본값은 4 |
| *keyid* | NTP 서버로 NTP 패킷을 전송할 때, 해당 keyid에 해당하는 키를 사용하여 패킷 정보를 추출하여 인증을 수행합니다. 값 범위: 1~4294967295.<br>이 매개변수를 설정하지 않으면 장치는 서버의 ID 를 인증하지 않으며, 반대로 서버도 장치를 인증하지 않습니다. |

#### 54.6.1. 구문

**ntp peer ip-address [version number | key keyid]***
**no ntp peer ip-address**

첫 번째 명령어를 실행하면 장치의 NTP 피어를 지정할 수 있습니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

#### 54.6.2. 예제

Switch_config#ntp peer 1.1.1.2 version 3 key 5

#### 54.6.3. 연관 명령어

ntp authentication enable
ntp authentication key
ntp authentication trusted-key

## 54.7. show NTP

NTP 관련 정보를 표시하는 명령어입니다.

### 54.7.1. 구문

**show ntp [status]**
현재 NTP 상태를 확인하려면 위 명령어를 실행합니다.
**show ntp associations [detail]**
NTP 연관(association) 상태를 확인하려면 위 명령어를 실행합니다.

**show ntp timers**
NTP 타이머 상태를 확인하려면 위 명령어를 실행합니다.

### 54.7.2. 예제

Switch#show ntp

Time-zone: GMT+9:00, Seoul
Current time: 2025-02-05 10:45:26

Clock Status: synchronized
Clock Stratum: 3
Leap Indicator: 0
Reference ID: 211.233.84.186
Clock Jitter: 0.004149
Clock Precision: -18
Clock Offset: 6.561 ms
Root Delay: 172.153 ms
Root Dispersion: 587.873 ms
Packets Sent: 30788
Packets Received: 27969 (bad version: 0)
Reference Time: 2025-02-05 10:41:37
Last Update Time: 2025-02-05 10:37:08

Switch#show ntp associations

ip address reference clock st poll reach delay offset dispersion
==========
====

```
 61.110.197.50  204.123.2.5     2  64    377   59.99  0.96    2.7
 27.114.150.12  193.190.230.65  2  64    377   489.97 -34.56  3.1
*211.233.84.186 204.123.2.5     2  64    377   19.99  9.15    3.0
 198.55.111.50  216.229.0.50    3  64    377   229.98 -40.09  3.4
 199.241.31.224 132.163.4.103   2  64    377   198.04 2.51    3.6
 204.2.134.163  241.199.164.101 2  64    360   169.97 -17.16  942.8
=================================================================
====
Note: * system peer(master), poll(s), delay(ms), offset(ms), dispersion(ms)

Total Associations: 6
```

## 54.8. Debug NTP

이 명령어를 사용하여 NTP 실행 프로세스를 디버깅할 수 있습니다.

### 54.8.1. 구문

**debug ntp packet**
NTP 패킷 디버그 기능을 활성화합니다.

**debug ntp event**
NTP 이벤트 디버그 기능을 활성화합니다.

**debug ntp error**
NTP 오류 디버그 기능을 활성화합니다.

**debug ntp all**
모든 NTP 디버그 기능을 활성화합니다.

**no debug ntp**
모든 NTP 디버그 기능을 비활성화합니다.

## 54.9. Time zone

이 명령어는 UTC 시간을 로컬 시간으로 변환하는 데 사용됩니다.

| 매개변수 | 설명 |
|---|---|
| *name* | 타임존의 이름 |

| | |
|---|---|
| *offset-hour* | UTC 시간과의 차이 (범위: -12~12 시간) |
| *offset-minute* | UTC 시간과의 분 단위 차이 (범위: 0~59, 기본값: 0) |

#### 54.9.1. 구문

**time-zone name offset-hour [offset-minute]**
**no time-zone**

첫 번째 명령어를 실행하면 타임존 설정 기능을 활성화할 수 있습니다.
기본값으로 되돌리려면 no 형식의 명령어를 사용합니다.

#### 54.9.2. 예제

Switch_config#time-zone Seoul 9