제품 설명서

SFC5200AT

솔텍인포넷주식회사

목차

개 요

제품 개요

최근 인터넷 사용자는 폭발적으로 증가하고 있습니다. 사용자는 전화망에 근거한 통신에 만족하지 않습니다. 통신사들이 오디오, 데이터, 사진과 같은 멀티미디어 서비스를 제공하는 것을 원하며 기존의 통신 서비스로는 요건을 충족시킬 수 없습니다. 대역폭 접근 기술은 사람들의 삶과 일에 큰 변화를 가져올 수 있습니다.
ADSL 및 HFC 와 비교했을 때, 이더넷 접근 방식은 높은 대역폭, 낮은 비용 등의 장점을 가지며, IP 는 높은 대역폭의 도시권 통신망 (MAN)의 주요 서비스이고 이더넷은 IP 서비스를 수용하는 직접적인 방법입니다. 네트워크와 사용자를 위해 다른 기기를 추가할 필요가 없으므로 프로토콜 변환 비용이 절감 되며, 이더넷 네트워크는 광을 이용하여 네트워크 망에 수 많은 사용자가 서비스를 이용 할 수 있습니다.
이러한 추세에 SOLTECH 은 비즈니스 지향 이더넷 액세스 솔루션을 제공 합니다.
제품은 사용자 관리, 멀티레이어 스위칭, 유선 속도 사용자 접속 관리, 다중 접속 모드 등을 제공하여 사용자와 관리자에게 유연한 네트워킹을 제공합니다.
제품은 장치 및 전원을 추가할 수 있어 사용자 요구사항을 충족할 수 있습니다.

- 광대역 인터넷 접속
- 캠퍼스 네트워킹에서 대용량 데이터 교환

제품의 특징

- L2 / L3 스위칭 및 유선 속도의 접속
- ASIC을 통한 유선 속도 처리 및 네트워크 프로세서를 통한 유연성 및 고성능 확보
- 적절한 스위칭 용량 및 높은 포트 밀도
- 다중 접속 방식 지원
- 통일된 사용자 관리기능 지원
- 유연성 있는 전원 메커니즘
- RADIUS 기반 사용자 광대역 관리 및 권한 제어

제품의 외관

SFC5200AT 제품의 외관은 아래와 같습니다.

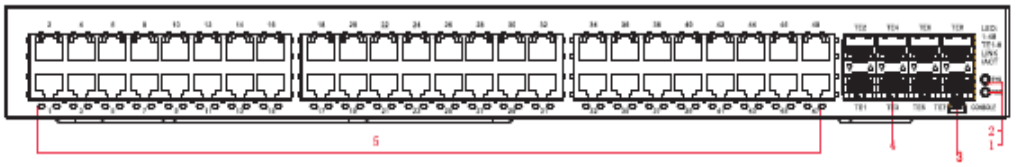


그림 1-1 SFC5200AT 전면

번호	이름	설명
1	PWR	PWR 표시등이 켜져 있으면 장치에 전원이 공급되는것입니다.
2	SYS	SYS 표시등이 켜져 있으면 시스템이 구동 중이거나, 구동에 문제가 있는 것입니다. SYS 표시등이 깜박이면 시스템이 정상적으로 작동하는 것입니다.
3	Console	MINI USB 콘솔포트(RS232), 9600bps의 전송 속도
4	Link/Act	SFP+ 포트 링크 시 켜지고, 데이터 송수신 시 깜박입니다.
5	Link/Act	RJ45 포트 링크 시 켜지고, 데이터 송수신 시 깜박입니다.

SFC5200AT 제품의 후면 외관은 아래와 같습니다.

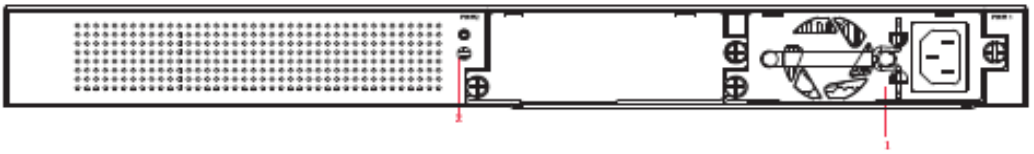


그림 1-3 SFC5200A Series 제품의 후면

번호	**약어**	**이름**	**설명**
1	POWER1	AC 전원공급기 1	입력 전압: AC100~240V
2	GND	접지(Ground)	접지 단자에 연결.

제품 사양

Technology	Standard	IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.1Q VLAN Tagging IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.1w Rapid Spanning tree protocol	IEEE 802.3z Gigabit SX/LX IEEE 802.1x Port Authentication Network Control IEEE 802.3ab Gigabit 1000T IEEE 802.1p Class of Service
Interface	RJ45 Ports	10/100/1000Mbps TP 48-Ports, Auto-Negotiation, Auto MDI-X	
	Fiber Port	10G SFP+ 8-Slots	
	LED Indication	System: Power, System Ports: 10/100/1000Mbps Link/Act, SFP Link/Act	
Performance	Basic	SWITCH FABRIC : 176Gbps ADDRESS TABLE : 32K entries VLAN TABLE : 4K ROUTING TABLE : 32K JUMBO FRAME : 9Kbytes	THROUGHPUT : 130.9Mpps@64Bytes SHARE DATA BUFFER : 3.0Mbytes ACL TABLE : 1K LAYER 3 INTERFACE : 4K Port Queues : 8
	Layer 3	IPv4 Routing Protocol : Static Route, RIPv1v2, OSPFv1v2, BGP4 IPv6 Routing Protocol : Static Route, RIPng, OSPFv3, BGP4+ Multicast Routing Protocol : IGMP v1/v2/v3, PIM-DM, PIM-SM Layer 3 Protocol : VRRP v2, ARP, ARP Proxy Routing interface : Per VLAN	
Operating Environment	Temperature	Operating: 0℃ ~ 50℃, Storage: -20℃ ~ 70℃	
	Humidity	5 ~ 90% (Non-condensing)	
Power Supply	Input Power	100~240VAC, 50/60Hz	
	Power Consumption	Power Consumption Max. 64 watts	
Dimension		440mm(W) x 350mm(D) x 44mm(H), 1U	

Management:

- Console, Telnet, SSH v2
- SNMP v1/v2/v3, RMON
- TFTP Client, FTP Client, SFTP Client
- NTP, Mirror
- sFlow

위에 명시된 관리용 프로토콜 및 암호화 알고리즘은 관리자가 제품을 OAM(운영/관리/보수) 목적으로만 사용되고, 제품을 통과하는 사용자 데이터 플레인에 대한 암호화 기능은 제공하지 않는다.

설치 준비

안전 수칙

사람이 다치거나 장치가 손상되지 않도록 제품 스위치를 설치하기 전에 설명서의 안전 수칙을 확인하십시오.

다음 안전 수칙은 모든 잠재적 위험을 다루지는 않습니다.

시스템 설치 안전 수칙

- 깨끗하고 먼지가 없는 상태로 유지하십시오.
- 도보 지역에 장치를 두지 마십시오.
- 설치 및 유지 보수 중에 헐거운 옷이나 기계 장비로 인해 넘어 질 수 있는 다른 것을 착용하지 마십시오.
- 장비를 해체하기 전에 모든 전원을 끄고 전원 공급 장치와 케이블을 분리하십시오.

제거 안전 수칙

운반하는 동안 다음 요구 사항을 따르십시오.

- 기기를 움직일 때 발이나 허리를 조심합니다.
- 장치를 옮기기 전에 모든 전원 공급 장치를 분리하고 모든 케이블을 뽑으십시오.
- 장치를 옮길 때 양쪽 측면에 손잡이를 사용하십시오.

전기 안전 수칙

- 접지되지 않은 전원 공급 장치, 신뢰할 수 없는 전원 접지 및 습식 접지와 같은 작업 영역의 잠재적

위험을 확인하십시오.

- 설치하기 전에 비상 전원 스위치의 실내 위치를 확인하십시오. 문제가 발생하면 전원을 차단하십시오.
- 장치를 혼자 유치하지 마십시오.
- 전원이 차단되면 장치를 주의 깊게 확인하십시오.
- 장치를 습한 환경에 두거나 액체 물질을 장비에 넣지 마십시오.
- DC전원을 사용하기 전에 지침에 따라 양극 / 음극을 연결하십시오.

정전기 예방

정전기 방지를 위해 제품에서 다양한 조치를 취하지만 정전기가 특정 볼륨에 도달하면 회로와 장치에 나쁜 영향을 미칩니다.
다음은 제품이 통신 네트워크에 연결될 때 정적의 주요 리소스입니다.

- 실외 고전압 와이어 및 천둥과 같은 외부 전기장
- 바닥재 및 기계의 구조와 같은 내부 시스템

정전기의 손상을 방지하려면 다음과 같이하십시오.

- 장치와 바닥이 잘 접지되어 있습니다.
- 실내 먼지 방지.
- 적절한 습도 유지.
- 회로 장치를 만지기 전에 정전기 방지 팔걸이를 착용하십시오.

장치를 교체하거나 설치할 때 다음과 같이하십시오:

- 모든 부품, 특히 회로 장치를 설치하기 전에 정전기 방지 팔걸이를 착용하십시오.
- 회로 장치를 잡아야 할 경우 가장자리를 잡으십시오. 회로 내부를 직접 만지지 마십시오.
- 옷이 회로 장치에 닿지 않도록 하십시오. 정전기 방지 팔걸이는 신체의 정전기로 인해 회로 장치가 손상되는 것을 방지 할 수 있지만 의류의 정전기는 방지 할 수 없습니다.

레이저 안전 수칙

- 레이저 변환기가 작동하면 포트가 광섬유 케이블을 연결하고 포트가 먼지 방지 덮개로 채워져 있는지 확인해야 합니다.
- 레이저 인터페이스를 눈으로 보지 마십시오.

설치 장소 요구 사항

스위치는 실내에 설치해야 합니다. 정상적인 작동을 적용하고 수명을 연장하려면 설치 장소에 대한 다음 요구 사항을 충족해야 합니다.

스탠드 설치 요구 사항

랙에 제품을 설치하고 다음 요구 사항을 충족하는지 확인하십시오.

- 랙에 설치를 한 경우 통풍이 잘되는지 확인하십시오.
- 랙이 제품 및 해당 액세서리를 지탱할 수 있을 정도로 견고해야 합니다.
- 제품을 설치 한 후 열 냉각을 위한 공간이 확보되도록 크기가 적절한 지 확인하십시오.
- 장비는 접지가 되어야 합니다.

환기 요구 사항

장치의 환기 구멍에 공간을 확보하여 냉각 시스템이 정상적으로 작동하도록 합니다. 모든 유형의 케이블을 연결 한 후에는 통풍구를 막지 않도록 합니다.

메모:
장비 냉각 공기 흐름이 매끄럽도록 장치 슬롯에 핸들 바가 완전히 눌러져 있어야 합니다.

온도와 습도

제품의 정상적인 기능과 수명을 보장하려면 기계실의 특정 온도와 습도를 유지해야 합니다.
기계실의 온도와 습도가 오랫동안 적합하지 않으면 장치가 손상 될 수 있습니다.

- 비교적 습한 환경에서는 절연 재료가 잘 절연되지 않거나 전류 누출이 발생할 수 있습니다.

경우에 따라 부품의 침식이 발생할 수 있습니다.

- 비교적 낮은 습한 환경에서, 절연 될 제품은 건조되고 수축되며 쉽게 정전기를 발생시킬 수 있습니다. 따라서 장치의 회로가 손상될 수 있습니다.
- 온도가 높을수록 위험이 커집니다. 그러면 스위치의 신뢰성에 큰 영향을 미치며 스위치의 부식과정이 크게 가속화됩니다.

이 장치는 전원 공급 장치의 다중화 기능을 제공합니다. 장치의 지속적인 작동을 보장하여 갑작스러운 전원 종료를 방지하기 위해 다중 전원 공급 장치를 적용하는 것이 좋습니다.

스위치의 접지 안내

좋은 접지 환경은 스위치가 안정적으로 작동하기 위한 기반으로 낙뢰 방지 및 전파 피해 방지를 위한 기본 전제입니다. 접지 규정의 요구 사항에 따라 설치 장소의 접지 조건을 주의 깊게 확인하고 실제 상황에 따라 올바르게 접지하십시오.

안전한 접지

AC-적용 장치는 황록색 접지선을 통해 접지 되어야 합니다. 그렇지 않으면 전원 공급 장치와 선체 사이의 절연 저항이 작아지면 감전 될 수 있습니다.

낙뢰 방지 접지

낙뢰 방지 시스템은 피뢰침, 지하 도체 및 접지 시스템용 커넥터로 구성된 시설 중 독립적인 시스템입니다. 접지 시스템은 황록색 안전 접지선의 접지 장치와 함께 사용됩니다. 낙뢰 방전 접지는 장치가 아닌 접지구조물만을 위한 것입니다.

전자기 호환 접지

전자기 호환성을 위한 접지에는 차폐 접지, 필터 접지, 소음 / 차단 제한 및 단계별 참고가 포함됩니다. 접지 저항 값은 1Ω 미만이어야 합니다.
스위치 접지 연결단자는 제품 뒷면에 있습니다.

시스템과의 연결은 모든 장치의 정상적인 작동을 보장하기 위한 것입니다. 시스템의 모든 장치를 연결하기 전에 다음을 읽으십시오.

EMI 지침

모든 종류의 간섭에 대한 근원지는 외부 또는 내부 응용시스템에 관계없이 정전용량의 결합, 인덕턴스 결합 및 전자기파 복사와 같은 다양한 전도 방식을 통해 장치에 영향을 끼칩니다.
전자기 간섭은 두 가지 유형으로 분류됩니다: 확산 경로의 유형에 의해 결정되는 방사선 간섭 및 전도 간섭이 있습니다.

장치에서 배출되는 에너지(전파 에너지)가 여유공간을 통해 센서에 도달하는 과정을 방사선 간섭이라고 한다. 간섭원은 방해된 시스템의 일부일 수도 있고, 또는 전기 장치에서 완전히 격리된 장치일 수도 있습니다. 전도 간섭이 발생하는 이유는 간섭원이 전자파선이나 신호 케이블을 통해 센서를 연결하고 간섭이 된 장치에서 다른 장치로 이루어지기 때문이다. 전도 간섭은 항상 장치의 전원 시스템에 영향을 미친다. 따라서 전도 간섭이 전력 시스템에 영향을 미치지 않도록 하기 위해 파동 필터가 필요하다. 방사선 간섭은 방사선 간섭을 차폐하는 방법이 어려운 반면에 장치의 신호 경로에 영향을 미칠 수 있다.

- 스위치에 전원 공급이 방해되지 않도록 효과적인 조치를 취해야 합니다.
- 전기 장비의 접지 장치와 낙뢰 방지 장치를 스위치가 있는 지면에 두지 않는 것이 좋습니다. 접지 / 낙뢰 방지 장치와 스위치 사이에 거리간격을 유지하십시오.
- 강력한 무선 방출 범위, 레이더 방출 범위 또는 고주파 전기 장치에서 멀리 떨어져 있어야 합니다.
- 정전기 차폐 방법을 사용해야 합니다.

광 선로 연결시주의 사항

광선로를 연결하기 전에 광 커넥터 및 광 선로 유형이 광 인터페이스 유형을 준수하는지 확인하십시오.

설치 도구

일반 도구	십자 드라이버, UTP 점퍼 코드 및 광 점퍼코드
특정 도구	정전기 방지 도구
기 구	광 파워 미터

표 2-4 도구 및 장치

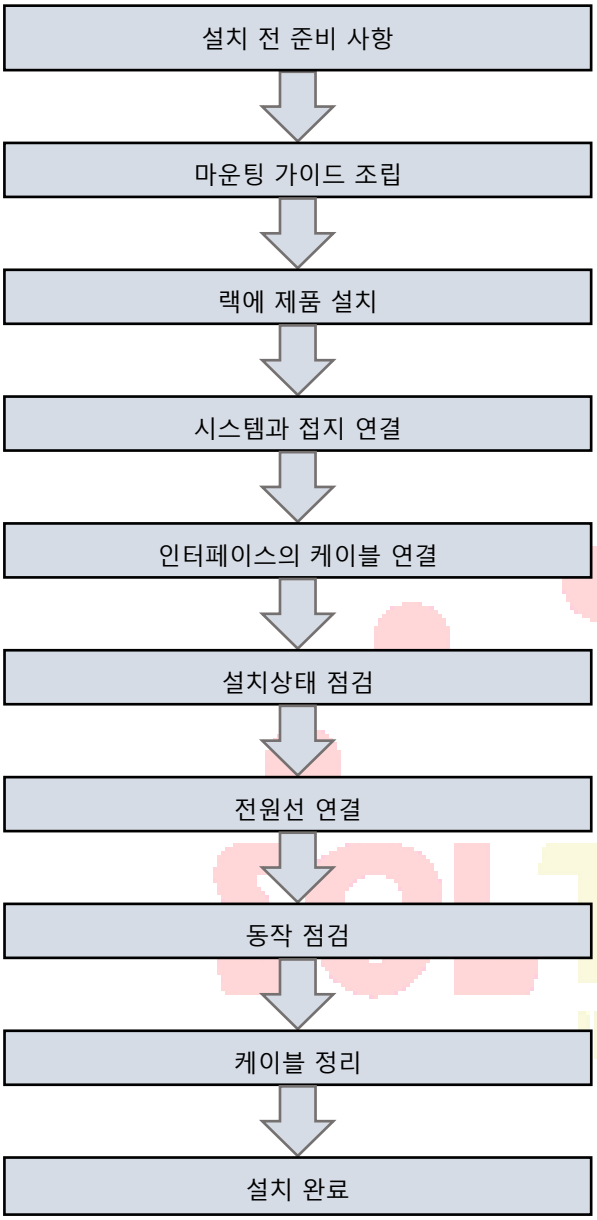
Notes **제품에는 이러한 도구들은 제공되지 않으므로 사용자는 이러한 공구를 준비해야 합니다.**

제품의 설치

Notes

- **제품을 설치하기 전에 앞장의 '설치 준비' 내용을 먼저 읽으십시오.**
- **'설치 준비'에 기술된 요건이 충족되어야 합니다.**

설치 절차



설치 전 준비 사항

제품을 설치하기 전에 공간, 네트워킹 방식, 전원 공급 장치에 대해 확인해야 합니다.
설치하기 전에 다음과 확인하십시오:

- 환기를 위한 장소를 확인하십시오.
- 설치장소의 전원 공급 장치 및 공기 흐름이 해당 요구 사항에 따라 준비되어 있는지 확인하십시오.
- 전원 공급 장치 및 상대 네트워크에 케이블이 잘 준비되어 있는지 확인하십시오.
- AC 전원 또는 DC 전원을 선택할지 여부를 결정하고 정격 전원을 얻을 수 있는지 확인하십시오.

스위치 설치

예방 조치

설치할 때 다음 사항에 유의하십시오.

- 랙을 지면에 고정시키는 모든 볼트가 잘 연결되어 있어야 하며, 평평한 패드, 스프링 패드 및 너트 순서에 따라 볼트를 렌치로 고정해야 합니다.
- 캐비닛에 안정적으로 설치되어야 합니다.
- 설치 장소는 지면과 수직이 되어야 합니다.
- 기계실에 설치된 랙은 일직선 상에 있어야 합니다. 오차는 5mm보다 작아야 합니다.
- 랙의 전면 도어와 후면 도어는 개폐가 편리해야 합니다. 자물쇠 및 열쇠는 준비되었습니다.
- 캐비닛 또는 각 장치에 중복 및 비정상 레이블이 없습니다.
- 보조 손잡이가 잘 설치되어 있어야 합니다.
- 각 장치를 고정하기 위한 나사는 견고 해야 하며, 볼트는 규격이 일치해야 합니다.
- 각 장치를 단단히 설치하고 템플릿을 고정하기 위한 나사를 단단히 조입니다.
- 하단 또는 상단의 모든 코드 콘센트에는 방지망이 설치되어 있어야 합니다. 왼쪽 누출의 직경은 1.5cm를 초과 할 수 없어 쥐나 다른 작은 동물이 캐비닛에 들어 가지 못하게 합니다.
- 정전기 방지 팔목보호대가 설치되어 있어야 합니다.

설치 순서

랙을 설치하기 전에 여유공간을 확보하십시오. 유지 관리 및 작동을 위해 랙의 전면 및 후면 도어를 위한 충분한 공간을 확보하십시오.

여유공간에 지정된 위치에 장비를 설치 한 다음 잘 고정하십시오.

연결 선과 케이블들을 설치합니다.

제품의 설치

주의 사항

랙에 제품을 설치하기 전에 전면 및 후면 고정 브래킷이 올바른지 확인하십시오. 고정 브래킷이 올바른 위치에 있지 않으면 장치의 전면 템플릿이 전면 도어에 너무 가까이 있을 수 있습니다. 네트워크 케이블을 꽂은 후 전면 도어가 닫히지 않을 수 있습니다. 제품을 설치 한 후 전면 도어와 장비 전면부 사이의 거리가 10mm 인지 확인하십시오.
또한 설치 전에 다음 사항을 확인해야 합니다:
랙은 잘 고정되어 있으며 랙 또는 장비 옆에 설치에 영향을 주는 장애물이 없어야 합니다.

설치 절차

최소 두 사람이 제품의 가장자리를 수평으로 잡고 천천히 설치 공간 앞에 옮깁니다.

두 사람이 제품을 랙의 받침대 또는 밀어 넣는 위치 보다 약간 높은 위치에 수평으로 이동한 다음 캐비닛에 설치합니다.

랙 볼트를 사용하여 제품을 랙 내부에 고정합니다.

시스템과 접지 연결

제품의 뒷면에는 보호 접지 (PGND- Protection Ground) 단자가 있습니다. 먼저 PGND 와 랙의 접지 열을 연결 한 다음 기계실의 접지 열과 접지 막대를 연결합니다.

주의 사항

- 접지선의 옆면의 크기는 통과 된 최대 전류 부하를 통해 계산합니다. 얇은 도체 및 전도 선을 사용해야 합니다.
- 차폐되지 않은 전도 선은 사용이 금지되어 있습니다.
- 접지 저항 값은 1Ω 미만이어야 합니다.

접지 절차

후면 접지의 육각 나사를 제거 합니다.

접지선의 단자를 접지 기둥에 고정합니다.

스패너로 육각 나사를 고정시킵니다.

연결 안내도에 따라 이전 단계들의 해당 터미널을 연결합니다.

AC 전원 연결

주의 사항

전원 공급 장치를 연결하기 전에 제공된 외부 전원 공급 장치가 제품에 설치된 전원 공급 장치 장치와 일치하는지 확인하십시오.

전원 선을 연결하기 전에 전원 공급 장치의 스위치가 차단(OFF) 상태인지 확인하십시오.

전원 선과 전선 포스트를 같은 색으로 연결하십시오.

연결된 전원 선이 제대로 연결되어 있는지 확인하십시오.

연결 절차

전원 라인의 플러그를 전원에 직접 삽입하십시오.

전원 라인의 다른 쪽 끝을 해당 소켓 또는 커넥터에 연결하십시오

제품의 케이블 연결

연결 절차

이더넷 케이블의 RJ45 끝을 제품의 이더넷 인터페이스에 연결 한 다음 이더넷 케이블의 다른 쪽 끝을 네트워크 관리자 장치 또는 터미널 제어 장치에 연결하십시오.

RS-232 직렬 케이블의 RJ45 끝을 제품의 RS-232 직렬 인터페이스에 연결 한 다음 이더넷 케이블의 다른 쪽 끝을 네트워크 관리 장치 또는 터미널 제어 장치에 연결하십시오.

인터페이스 케이블 연결

주의 사항

광 사용 시 인터페이스에서 단일 모드 또는 멀티 모드 사용여부를 확인하십시오.

연결 시 커넥터가 구부러지지 않게 연결하십시오.

연결 절차

이더넷 케이블의 RJ45 끝을 장치의 이더넷 인터페이스에 연결한 다음 이더넷 케이블의 다른 쪽 끝을 네트워크 관리자 장치 또는 터미널 제어 장치에 연결하십시오.
시리얼 케이블의 RJ45 끝을 장치의 시리얼 인터페이스에 연결한 다음 이더넷 케이블의 다른 쪽 끝을 네트워크 관리자 장치 또는 터미널 제어 장치에 연결하십시오.
단일 모드 또는 멀티 모드 광선로를 해당 인터페이스에 삽입하십시오.

케이블 정리

확인사항

전원 선과 케이블은 순서대로 깔끔하게 묶어야 합니다.

광 케이블을 정리할 때 광 커넥터를 구부러지지 않도록 하십시오.

광 케이블과 UTP 케이블을 너무 단단하게 묶어 선로 수명을 단축시키거나 전송 능력을 약화시키지 마십시오.

포장 절차

튀어 나온 광 선로 및 UTP 부분을 포장하여 장비 양면에 편리하게 연결하십시오.

양면에서 광섬유와 케이블을 와이어 슬롯에 고정하십시오.

전원 라인을 포장 할 때는 바닥에 단단히 정리하고 라인을 유지하십시오.

설치 후 확인

랙 확인

외부 전원 공급 장치가 캐비닛의 배전반과 일치하는지 확인.

스위치를 설치 한 후 도어를 닫을 수 있는지 확인하십시오.

넘어지지 않도록 고정되어 있는지 확인하십시오.

스위치가 제대로 설치되고 고정되어 있고 모든 케이블이 고정되어 있는지 확인하십시오.

케이블 연결 확인

광 케이블과 UTP가 포트와 일치하는지 확인하십시오.

케이블이 올바르게 연결되어 있는지 확인하십시오.

전원공급장치 점검

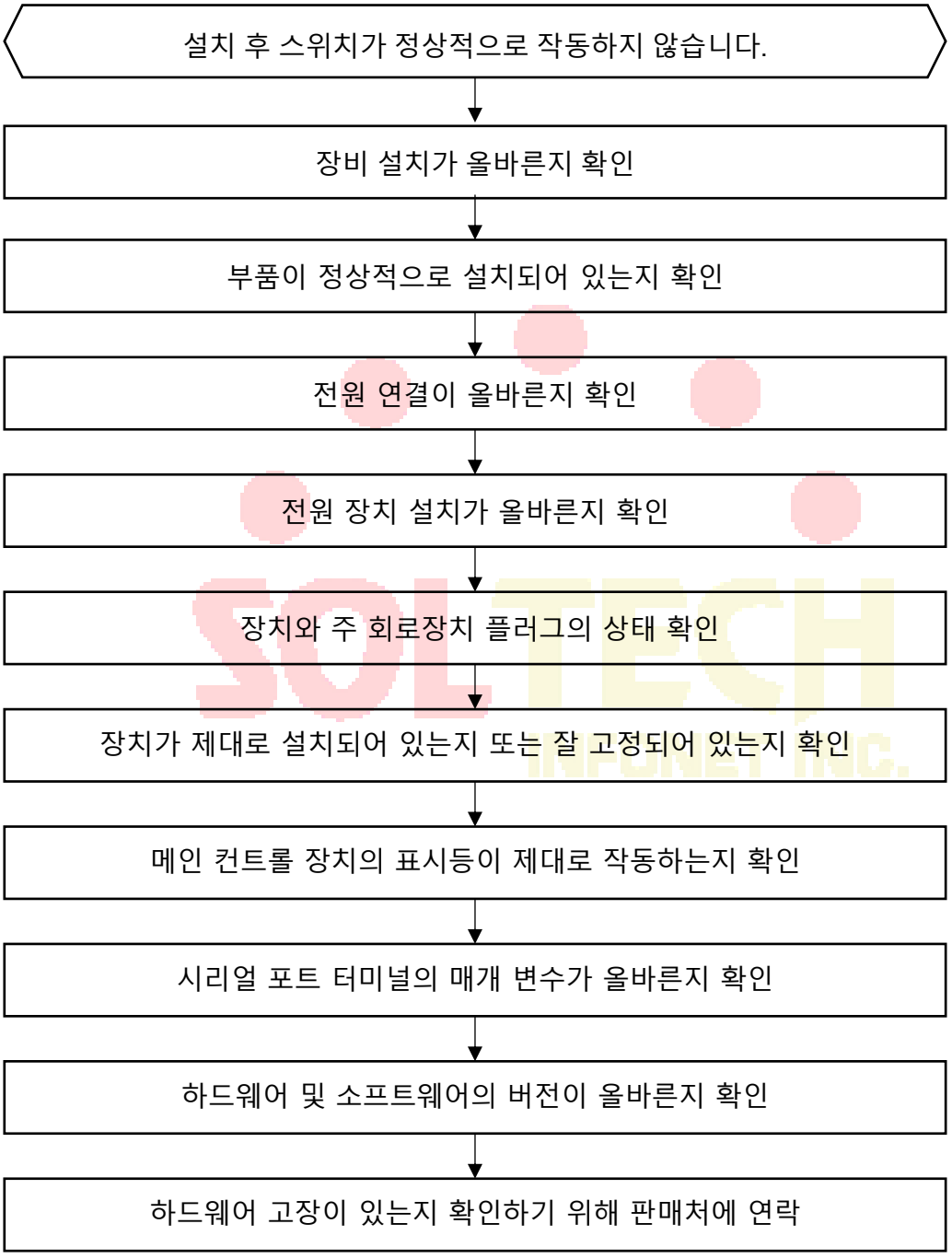
전원 선이 제대로 연결 되어있고 보안 요구 사항을 준수하는지 확인.

전원 공급 장치 장치가 템플릿에 있는 두 개의 볼트를 통해 단단히 조여 졌는지 확인하십시오.

전원 공급 장치의 스위치를 열고 전원 장치가 정상적으로 작동하는지 확인하십시오.

일반적인 설치 문제 해결

설치 중 문제 해결을위한 일반 절차



하드웨어 설치시 문제 해결

전원 공급 장치의 문제 해결

문제 1: AC 전원 장치에 전원을 공급할 수 없습니다.

【 문제 확인】

각 장치의 PWR 표시등이 켜져 있지 않습니다. 전원 장치의 녹색 표시등이 꺼져 있습니다. 팬이 작동하지 않습니다.

【 문제 해결 방법 】

먼저 전원 공급 장치의 모든 스위치를 OFF 상태로 변경합니다. 둘째, 전원 선이 올바르게 연결되어 있는지 확인하십시오. 필요한 경우 전원 공급 장치의 플러그를 뽑아 전원 시스템의 플러그인이 정상인지 확인하십시오.

장치 설치 문제

문제 1: 장치에 전원이 공급 된 후 LED 표시가 비정상입니다.

【 문제 확인 】

SYS 표시기는 항상 꺼져 있습니다. 네트워크 케이블이나 광선로를 삽입하지 않아도 장치의 LINK 표시등은 항상 켜져 있습니다.

【 문제 해결 방법 】

제품의 전원을 껏다가 다시 켜 봅니다. 약 2 분이상 후에도 LED 가 정상이 아니거나, 통신이 되지 않으면 제조업체에 기술지원을 요청하거나 AS 입고하여 수리하십시오.

트러블 슈팅

부트롬 접속

부트롬 접속을 하기 위하여 다음 절차를 수행한다.

장비의 콘솔 포트에 콘솔케이블을 연결하고 컴퓨터에 터미널 에뮬레이션 프로그램을 실행한다. (콘솔 포트 구성 속도: 9600, 데이터비트:8, 정지비트:1, 패리티: 없음)

장비의 전원을 켠다.

전원을 켜고 수 초 이내에 Ctrl + P 버튼을 수 차례 입력하여 bootrom 모드로 진입한다.

```
System Bootstrap, Version 0.4.3, Serial No:20016002957

Copyright (c) by Shanghai Baud Data Communication Co., Ltd.

Current time: 1970-1-1 0:00:00

SDRAM Fast Test.....PASS!

Flash Fast Test.....PASS!

 RTC Test.....  (Ctrl + P 수 차례 입력)
```

패스워드 복원

제품 시스템은 패스워드 복원 기능을 제공하지 않는다. 따라서 관리자는 패드워드를 별도로 기록하고 관리하여야 한다.

- 참고: TFTP/FTP를 통하여 startup-config 파일을 백업하면 계정 및 비밀정보를 제외한 구성 정보를 복원 시에 사용 또는 참고 할 수 있다.
- 참고: more startup-config 명령을 사용하면, 구동에 사용되는 구성 파일을 표시가능하며, 필요 부분을 복사하여 구성 시 참고 할 수 있다.

설정 초기화

구성값 및 각종 키 값을 초기화 하여 설정초기화 상태로 하기 위하여 다음 절차를 수행한다.

시스템에 관리자 계정으로 로그인 후 아래 명령을 수행 한다.

명령어	설명
default-config	Admin모드에서 실행하여 구성 및 각종 키 값을 설정 초기화 한다. (사용 권장)

아래 명령들은 startup-config 파일만을 삭제한다.

명령어	설명
default-config	Admin모드에서 구성파일을 삭제한다.

시스템을 재시작 한다.

명령어	설명
reboot	시스템을 재시작 한다.

OS 업데이트/복구/재설치

시스템에 관리자 계정으로 로그인 한다.

시스템에 콘솔 및 LAN 선을 연결하고 PC에 접속 가능한 IP를 구성한다.

명령어	설명
ip address A.B.C.D mask	장비의 IP주소를 구성 한다.

PC에 TFTP/FTP 서버를 실행하고 펌웨어가 저장된 디렉터리와 계정을 지정한다.

아래 명령으로 펌웨어를 플래시 메모리로 복사한다.

명령어	설명
copy tftp: flash:	펌웨어 파일을 플래시로 복사 한다. (부트롬모드 및 운영 중에 사용)
copy ftp: flash:	펌웨어 파일을 플래시로 복사 한다. (펌웨어 부팅 후 운영 중에 사용)

펌웨어 플래시에 저장되는 파일명 규칙은 아래와 같다.

플래시 저장 파일명	설명
Switch.bin	장치용 펌웨어 파일

제품 구성

제품의 구성품 목록은 아래와 같습니다.

이 름	내 용
본체	제품 본체
전원코드	AC 전원 연결용
마운팅 키트	19 인치 랙용
콘솔 케이블	Mini USB - DB9 (RS232 방식)

제품 설명서

제품 설명서는 전자문서 형태로 솔텍 홈페이지에서 다운로드 가능 합니다.

명령 줄에서 형식 규약

구문	의미
Bold	명령 행에서 키워드를 나타냅니다. 변경되지 않고 그대로 입력해야합니다. 명령 줄에서 굵게 표시 됩니다.
{italic}	명령 행에서 매개 변수를 나타내며 실제 값으로 대체해야합니다. 중괄호 안에 기울임 꼴로 표시 됩니다.
< italic>	명령 행에서 매개 변수를 나타내며 실제 값으로 대체해야합니다. 괄호 안에 기울임 꼴로 표시 됩니다.
[ ]	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 아무 것도 선택할 수도 없다는 의미입니다.
&<1-n>	"&"기호 앞에있는 매개 변수를 n 번 입력 할 수 있음을 나타냅니다.
#	"#"기호로 시작하는 줄이 설명 줄임을 나타냅니다.

구성 준비

이 장에서는 처음 스위치를 구성 할 경우 다음과 같은 준비작업을 설명한다.:

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

스위치의 포트 번호

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

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 매겨집니다.

시작 전 점검 사항

스위치를 켜고 구성하기 전에 다음 사항을 확인 하십시오:

하드웨어 설치설명서에 따라 스위치 하드웨어를 구성합니다.

최초 접속은 콘솔 포트와 PC 를 연결합니다. (콘솔 포트 구성 속도: 9600, 데이터비트:8, 정지비트:1, 패리티: 없음)

PC 터미널 에뮬레이션 프로그램을 구성합니다.

IP 네트워크 프로토콜에 따라 IP 주소, 사용자 계정 및 비밀번호에 대한 계획을 세웁니다.

도움말 얻기

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

- 현재 명령에서 사용가능한 모든 명령을 나열하려면 물음표를 입력하십시오.
  Switch> ?
- 알고있는 문자를 입력하고 물음표(공백없이)를 입력 하여 현재 알려진 문자로 시작하는 명령어 목록을 얻을 수 있습니다.
  Switch> s?
- 명령어를 입력 한 다음 공백과 물음표를 입력 하여 명령 매개변수 목록을 가져옵니다.
  Switch> show ?

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

명령어 모드

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

모드	**명령어**	**프롬프트 형식**	**종료 방법**
부트 모드	전원을 켠 후, "Ctrl+p"를 입력.	monitor#	Quit 실행
사용자 모드	로그인	Switch>	**exit** 나 **quit**를 실행.
관리 모드	사용자모드에서 **enter** 또는 **enable**을 입력.	Switch#	Exit 나 quit를 실행.
구성 모드	관리자모드에서 "config" 명령어를 입력 하십시오	Switch_config#	**Exit** 나 **quit** or **Ctrl-z** 로 관리자모드 실행.
포트 구성 모드	구성모드에서 interface 명령어를 입력 하십시요.	Switch_config_g 1/1#	**Exit** 나 **quit** or **Ctrl-z** 로 관리자모드 실행.

제한된 명령의 하위 명령어는 각 명령 모드에서 사용할 수 있습니다. 명령어를 입력 하는데 문제가 있으면 인터페이스 형식을 확인하고 물음표(?)를 입력 하여 사용 가능한 명령어 목록을 찾으십시오. 잘못된 명령 모드 이거나 잘못된 구문을 사용 중일 수 있습니다. 다음 예시에서 시스템 프롬프트 변경, 명령모드 변경을 나타냅니다.

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface g 1/1
Switch_config_g1/1# quit
Switch_config# quit
Switch#
```

명령어 취소

명령어를 취소하거나 기본 구성으로 돌아가려면 키워드를 추가 하십시오. 명령어 앞에는 'no'를 추가합니다.. 예를 들어

```
Switch_config# no ip telnet enable
```

구성 저장

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

```
Switch# write
```

기본 구성

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

버전 정보 확인

Switch#show version
Soltech Co., Ltd. Internetwork Operating System Software
SFC5200A Series Software, Version 2.2.0F Build 106319, RELEASE SOFTWARE
Copyright 2019
Compiled: 2022-11-22 13:50:43 by SYS, Image text-base: 0x80010000
ROM: System Bootstrap, Version 0.2.0,hardware version:A
Serial num:20070002314, ID num:20070002314
System image file is "Switch.bin"
Soltech SFC5200AT RISC
524288K bytes of memory,32768K bytes of flash
Base ethernet MAC Address: 00:21:6d:59:f5:84
PCB version:D
snmp info:
  vend_ID:11618 product_ID:455 system_ID:1.3.6.1.4.1.11618.301.2.455
Switch uptime is 0:00:03:06, The current time: 2000-1-1 0:3:47
 Reboot history information:
  No. 1: System is rebooted by power-on
  No. 2: System is rebooted by command at 2000-1-1 0:4:43, uptime 0:00:04:02

계정 관리

로컬 계정 구성

최초 로그인

최초 장비에 접속을 할 경우 비밀번호 관련하여 변경할 수 있는 기능을 제공하며, 최초 장비 기본 구성은 Console 만 접속 가능하다. 최초 접속 시에 해당하며 비밀번호는 9 자리 이상의 영문 대문자, 숫자, 특수문자 조합으로 구성하여야 한다.

명령어	내용
Username: admin Password:	초기 계정(admin) 및 비밀번호(admin)로 로그인한다. (비밀번호 화면 표시 안됨.)
Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.

관리자 비밀번호 변경

관리자 계정의 비밀번호를 변경하려면 아래 표에 명령 및 절차를 따른다.

명령어	내용
Username <username> password 0	계정의 비밀번호를 변경을 시작한다. 0 : 비밀번호 암호화 2 : SHA256 으로 암호화
Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.
no username <username>	생성되어있는 사용자 계정을 삭제

- 관리자/사용자 비밀번호는 암호화 되어 저장 된다.

계정 비밀번호 규칙 구성

관리자 및사용자 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:

구분	제품의 비밀번호 규칙	비고
준수 사항	비밀번호의 최소길이. 9 자리 이상의 길이 권고.	필수
	숫자, 대문자(영문), 소문자(영문), 특수문자 조합 가능. 각 1 개 이상 포함 권고.	필수
금지 항목	사용자 계정(ID)과 동일한 비밀번호 구성 금지	필수
	동일한 문자.숫자 연속적으로 반복사용 금지(3 번이상 반복금지)	필수
	키장치의 연속된 문자 또는 숫자의 3 글자 이상 순차적 나열 금지(qwe, asd, abc, 123 등)	필수
	직전 사용된 비밀번호 재사용 금지	필수
	비밀번호의 유효기간 구성(일, 시간, 분, 초 단위 가능)	선택

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 필수요소를 입력한다.
non-user	사용자 계정과 동일한 비밀번호 구성 금지
non-repeat	동일한 문자.숫자 연속적으로 반복사용 금지(3 번이상 반복금지)

non-seqlisting	키장치의 연속된 문자 또는 숫자의 순차적 나열 금지(qwe, asd, abc, 123 등)
non-history	직전 사용된 비밀번호 재사용 금지
validity <1d2h3m4s>	비밀번호의 유효기간(일,시간,분,초 단위)
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

- 비밀번호 규칙의 구성 및 적용할 것을 권고한다.

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 0	<username>은 사용할 사용자/관리자 명으로 입력 , 적용하여 비밀번호 구성. 정의된 pass-group <name>의 규칙 적용.
Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.

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

명령어	내용
username <username> pass-group <name> password 0	<username>은 사용할 사용자/관리자 명으로 입력, pass-group <name>의 규칙을 이 계정에만 적용하여 비밀번호 구성
Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.

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 적용한다.
enable level <1-15> password 0	운영모드 변경용 비밀번호와 권한(level 15 최상위)을 입력한다. 0 : 비밀번호 암호화 2 : SHA256 으로 암호화
Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.

- 운영모드 변경 비밀번호는 암호화 되어 안전하게 저장 된다.

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 0	RADIUS 키 입력 모드 0 : 비밀번호 암호화 2 : SHA256 으로 암호화
Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.

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 0	TACACS 키 입력 모드 0 : 비밀번호 암호화 2 : SHA256 으로 암호화

Please input password: Please input the password AGAIN:	새로운 비밀번호를 입력 및 재입력 프롬프트에 각각 입력한다.

시스템 관리 구성

파일 관리 구성

파일 시스템 관리

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

파일 시스템 명령어

모든 명령어는 굵은 글씨체 이며 기타는 매개변수 입니다.

꺾쇠 괄호"[ ]"의 내용은 선택 사항입니다.

명령어	설명
Format	파일 시스템을 포맷하고 모든 데이터를 삭제합니다.
dir [filename]	1 파일 및 디렉터리 이름을 표시 합니다. "[]"기호 안의 파일 이름은 여려 문자로 시작하는 파일을 표시하는 것을 의미 합니다. 파일은 다음 형식으로 표시 됩니다. 색인번호 파일이름 <파일> 길이 구성된 시간
delete filename	2 파일을 삭제합니다. 파일이 존재하지 않으면 시스템에서 표현합니다.
md dirname	3 디렉터리를 만듭니다.
rd dirname	4 디렉터리를 삭제 합니다. 디렉터리가 존재하지 않으면 시스템에서 표현합니다.

more <filename>	5	파일의 내용을 표시합니다. 파일 내용을 한 페이지로 표시 할 수 없는 경우 페이지 별로 표시 됩니다.
cd	6	현재 파일 시스템의 경로를 변경합니다.
pwd	7	현재 경로를 표시합니다.

부트롬 모니터 진입하기

시스템 전원을 켜거나 운영 중 reboot 명령으로 재시작 직후에 아래 메시지가 나올 때, 로컬 콘솔에서 <Control + P> 키를 입력하여 모니터 모드로 진입할 수 있다.

System Bootstrap, Version 0.4.6, Serial No:20042015660

Soltech2020

Soltech SFC5200AT

Current time: 1970-1-1 0:00:00

SDRAM Fast Test.....PASS!

Flash Fast Test.....PASS!

RTC Test.....PASS!

 # Control + P 수 차례 입력

시스템 부트 파일 구성

monitor#boot flash <*local_filename*>

이 명령에 지정한 파일명으로 플래시에서 시스템을 부팅 하는 명령 입니다. 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 입력해야 합니다.

예제

monitor#boot flash switch.bin

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	이더넷의 IP 주소
net_mask	이더넷의 마스크

예제

monitor#ip address 192.168.20.1 255.255.255.0

기본 경로 구성

monitor#ip route default <*ip_addr*>

이 명령은 기본 경로를 구성하여 사용합니다. 기본 경로는 하나만 구성 할 수 있습니다.

매개변수 설명

매개변수	설명
ip_addr	게이트웨이의 IP주소

예제

monitor#ip route default 192.168.20.1

Ping을 이용하여 네트워크 연결 상태 시험

monitor#ping <*ip_address*>

이 명령어는 네트워크 연결을 확인하기 위함입니다

매개변수 설명

매개변수	설명
ip_address	IP 주소 도착지

예제

monitor#ping 192.168.20.100

PING 192.168.20.100: 56 data bytes

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

64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms

----192.168.20.100 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

소프트웨어 업데이트

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

TFTP 를 이용하여 부트롬 업데이트 하기

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

매개변수 설명

매개변수	설명
A.B.C.D	TFTP 서버의 IP 주소 입니다. 지정된 IP주소가 없으면 복사명령이 실행된 후, 서버의 IP주소를 입력하라는 메세지가 나타납니다.
Source file name	TFTP 서버에 있는 받을 파일의 이름을 입력합니다.
Destination file name	로컬 플래시에 저장할 파일의 이름을 입력합니다.

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 표시 합니다.

매개변수 설명

매개변수	설명
A.B.C.D	TFTP 서버의 IP 주소 입니다.

	지정된 IP주소가 없으면 복사명령이 실행된 후 IP주소를 입력하라는 메세지가 나타납니다.
Source file name	TFTP 서버에 있는 받을 파일의 이름을 입력합니다.
Destination file name	로컬 플래시에 저장할 파일의 이름을 입력합니다.

예제

다음 예제는 TFTP 서버에서 읽은 파일이 스위치에 저장되는 파일명은 **switch.bin** 으로 저장하는 것을 보여줍니다.

monitor#copy tftp: flash:

Prompt: Source file name[]? SFC5200A_2.2.0C_99115.bin

Prompt: Remote-server ip address[]? 192.168.20.100

Prompt: Destination file name[main.bin]? Switch.bin

please wait ...

###

(중간생략)

###

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 업로드하여 구성을 복원 할 경우 사용할 수 있습니다.

TFTP 를 이용

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

매개변수 설명

매개변수	설명
A.B.C.D	TFTP 서버의 IP 주소 입니다. 지정된 IP 주소가 없으면 복사명령이 실행된 후 IP 주소를 입력하라는 메세지가 나타납니다.
Source file name	TFTP 서버에 있는 받을 파일의 이름을 입력합니다.
Destination file name	로컬 플래시에 저장할 파일의 이름을 입력합니다.

시스템 재시작 하기

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

monitor# boot flash Switch.bin

System Bootstrap, Version 0.4.6, Serial No:20042015660

Soltech2020

Soltech SFC5200AT

Current time: 1970-1-1 0:00:00

SDRAM Fast Test.....PASS!

Flash Fast Test.....PASS!

RTC Test.....PASS!

Loading Switch.bin.....

Start Decompress Switch.bin

```
################################################################################

################################################################################

####################
```

Decompress 6764426 byte. Please wait system up...

old idle is 86cc99a0,new idle is 30

System startup OK

load 51900 symbol OK

root stack_mngt_get_enable = 0

Switch console 0 is now available

Press RETURN to get started

Jan 1 00:00:01 AAA(Authentication,Authorization,Accounting) daemon is running

Jan 1 00:00:01 Stacking daemon is running

Jan 1 00:00:01 User default logouted on console 0

init phase 2

Jan 1 00:00:21 Switch chip daemon is running

Jan 1 00:00:21 %STATICMEM-6-REFILL:Static memory region refilled at 807578f0

Jan 1 00:00:21 Layer 2 daemon is running

Jan 1 00:00:21 vlan daemon is running

Jan 1 00:00:21 link aggregator daemon is running

Jan 1 00:00:21 802.1x daemon is running

Jan 1 00:00:21 Spanning tree daemon is running

Jan 1 00:00:21 General attribute registeration protocol daemon is running

Jan 1 00:00:21 GARP vlan registeration protocol daemon is running

Jan 1 00:00:21 Unicast reverse path checking daemon is running

Jan 1 00:00:21 Link Layer Discovery Protocol daemon is running

Jan 1 00:00:21 Link Layer Discovery Protocol daemon is running

Jan 1 00:00:21 Multi-EAPS daemon is running

Jan 1 00:00:21 Multi-EAPS daemon is running

Jan 1 00:00:21 Backup link daemon is running

Jan 1 00:00:21 OAM daemon is running

Jan 1 00:00:21 Connectivity Fault Management daemon is running

Jan 1 00:00:21 EAPS daemon is running

Jan 1 00:00:21 Loopback detecting daemon is running

Jan 1 00:00:21 Internet Protocol version 4 daemon is running

Jan 1 00:00:21 Internet Protocol version 6 daemon is running

Jan 1 00:00:21 Neighbour discover daemon is running

Jan 1 00:00:21 Dynamic host configuration protocol daemon is running

Jan 1 00:00:21 %MEM-6-EXT_REGION_CREATE 80440860: Create extend region for region 1 rank 4, 52448 blocks 27273596 bytes

Jan 1 00:00:21 IGMP snooping daemon is running

Jan 1 00:00:21 MLD snooping daemon is running

Jan 1 00:00:21 %SFLOW-6-INIT: Max sample rate is 32767

Jan 1 00:00:21 Sflow daemon is running

Jan 1 00:00:21 Telnet daemon is running

Jan 1 00:00:21 Radius daemon is running

Jan 1 00:00:21 Tacacs daemon is running

Jan 1 00:00:21 Routing daemon is running

Jan 1 00:00:21 Routing(for IPv6) daemon is running

Jan 1 00:00:21 IP access-list daemon is running

Jan 1 00:00:21 SNMP daemon is running

Loading startup-config ... Creating VLAN(s),please wait...

OK!

Wait for LS processing...OK!

(중략)

SUCCESS:8684 bytes loaded, 297 commands are successful executed.

Jan 1 00:00:28 QoS daemon is running

Jan 1 00:00:28 %PARTMEM-4-REFILL:Partion 0x5ff4f1f8 refilled

Jan 1 00:00:28 OSPFv6 daemon is running

Jan 1 00:00:28 OSPF daemon is running

Jan 1 00:00:28 EIGRP daemon is running

Jan 1 00:00:28 Rip daemon is running

Jan 1 00:00:28 BGP daemon is running

Jan 1 00:00:28 IGMP daemon is running

Jan 1 00:00:28 Multicast-routing daemon is running

Jan 1 00:00:28 PIM Dense Mode daemon is running

Jan 1 00:00:28 PIM Sparse Mode daemon is running

Jan 1 00:00:28 IS-IS daemon is running

Jan 1 00:00:28 VRRP daemon is running

Jan 1 00:00:28 %MPLS-6-LABELMGR: Max label value is 4096

Jan 1 00:00:28 NTP daemon is running

Jan 1 00:00:28 Rmon daemon is running

Jan 1 00:00:28 TFTPD:init error

Jan 1 00:00:28 Tftp daemon is running

Jan 1 00:00:28 Starting hardware self test

Jan 1 00:00:30 Flash memory test success

Jan 1 00:00:31 Memory test success

Jan 1 00:00:32 Temperature is normal

Jan 1 00:00:32 Fan status is normal

Jan 1 00:00:32 PSU status is normal

Jan 1 00:00:32 CPU load is normal

Jan 1 00:00:32 Memory usage is normal

Jan 1 00:00:32 interface status is normal

Jan 1 00:00:32 Starting process self test

Jan 1 00:00:32 Timing daemon is running

Jan 1 00:00:32 Switch chip daemon is running

Jan 1 00:00:32 Layer 2 daemon is running

Jan 1 00:00:32 vlan daemon is running

Jan 1 00:00:32 link aggregator daemon is running

Jan 1 00:00:32 802.1x daemon is running

Jan 1 00:00:32 Spanning tree daemon is running

Jan 1 00:00:33 General attribute registeration protocol daemon is running

Jan 1 00:00:33 GARP vlan registeration protocol daemon is running

Jan 1 00:00:33 Unicast reverse path checking daemon is running

Jan 1 00:00:33 Link Layer Discovery Protocol daemon is running

Jan 1 00:00:33 Connectivity Fault Management daemon is running

Jan 1 00:00:33 OAM daemon is running

Jan 1 00:00:33 EAPS daemon is running

Jan 1 00:00:33 Multi-EAPS daemon is running

Jan 1 00:00:33 Backup link daemon is running

Jan 1 00:00:33 Loopback detecting daemon is running

Jan 1 00:00:33 Internet Protocol version 4 daemon is running

Jan 1 00:00:33 Netflow daemon is running

Jan 1 00:00:34 Sflow daemon is running

Jan 1 00:00:34 Internet Protocol version 6 daemon is running

Jan 1 00:00:34 Neighbour discover daemon is running

Jan 1 00:00:34 Dynamic host configuration protocol daemon is running

Jan 1 00:00:34 IGMP snooping daemon is running

Jan 1 00:00:34 MLD snooping daemon is running

Jan 1 00:00:34 Syslog daemon is running

Jan 1 00:00:34 AAA(Authentication,Authorization,Accounting) daemon is running

Jan 1 00:00:34 Telnet daemon is running

Jan 1 00:00:35 Radius daemon is running

Jan 1 00:00:35 Tacacs daemon is running

Jan 1 00:00:35 Routing daemon is running

Jan 1 00:00:35 Routing(for IPv6) daemon is running

Jan 1 00:00:35 RipNG daemon is running

Jan 1 00:00:35 OSPFv6 daemon is running

Jan 1 00:00:35 IP access-list daemon is running

Jan 1 00:00:35 SNMP daemon is running

Jan 1 00:00:35 Inter-Card Communicating daemon is running

Jan 1 00:00:35 Card system daemon is running

Jan 1 00:00:35 QoS daemon is running

Jan 1 00:00:35 OSPF daemon is running

Jan 1 00:00:35 BEIGRP daemon is running

Jan 1 00:00:35 Rip daemon is running

Jan 1 00:00:35 BGP daemon is running

Jan 1 00:00:35 BFD daemon is running

Jan 1 00:00:36 IGMP daemon is running

Jan 1 00:00:36 Multicast-routing daemon is running

Jan 1 00:00:36 PIM Dense Mode daemon is running

Jan 1 00:00:36 PIM Sparse Mode daemon is running

Jan 1 00:00:36 IS-IS daemon is running

Jan 1 00:00:36 VRRP daemon is running

Jan 1 00:00:36 NTP daemon is running

Jan 1 00:00:36 Rmon daemon is running

Jan 1 00:00:36 Tftp daemon is running

Jan 1 00:00:36 File synchronizing daemon is running

Jan 1 00:00:36 Stacking daemon is running

Jan 1 00:00:36 Starting Integrity check

Jan 1 00:00:36 Timing integrity-check success

Jan 1 00:00:36 Switch chip integrity-check success

Jan 1 00:00:36 Layer 2 integrity-check success

Jan 1 00:00:36 vlan integrity-check success

Jan 1 00:00:36 link aggregator integrity-check success

Jan 1 00:00:36 802.1x integrity-check success

Jan 1 00:00:36 Spanning tree integrity-check success

Jan 1 00:00:36 General attribute registeration protocol integrity-check success

Jan 1 00:00:36 GARP vlan registeration protocol integrity-check success

Jan 1 00:00:36 Unicast reverse path checking integrity-check success

Jan 1 00:00:37 Link Layer Discovery Protocol integrity-check success

Jan 1 00:00:37 Connectivity Fault Management integrity-check success

Jan 1 00:00:37 OAM integrity-check success

Jan 1 00:00:37 EAPS integrity-check success

Jan 1 00:00:37 Multi-EAPS integrity-check success

Jan 1 00:00:37 Backup link integrity-check success

Jan 1 00:00:37 Loopback detecting integrity-check success

Jan 1 00:00:37 Internet Protocol version 4 integrity-check success

Jan 1 00:00:37 Netflow integrity-check success

Jan 1 00:00:37 Sflow integrity-check success

Jan 1 00:00:37 Internet Protocol version 6 integrity-check success

Jan 1 00:00:37 Neighbour discover integrity-check success

Jan 1 00:00:37 Dynamic host configuration protocol integrity-check success

Jan 1 00:00:37 IGMP snooping integrity-check success

Jan 1 00:00:37 MLD snooping integrity-check success

Jan 1 00:00:38 %LINE-5-UPDOWN: Line on Interface VLANs 1,3,5, changed state to up

Jan 1 00:00:38 SNMP server started on port 161.

Jan 1 00:00:38 Syslog integrity-check success

Jan 1 00:00:38 AAA(Authentication,Authorization,Accounting) integrity-check success

Jan 1 00:00:38 Telnet integrity-check success

Jan 1 00:00:38 Radius integrity-check success

Jan 1 00:00:38 Tacacs integrity-check success

Jan 1 00:00:38 Routing integrity-check success

Jan 1 00:00:38 Routing(for IPv6) integrity-check success

Jan 1 00:00:38 RipNG integrity-check success

Jan 1 00:00:38 OSPFv6 integrity-check success

Jan 1 00:00:38 IP access-list integrity-check success

Jan 1 00:00:38 SNMP integrity-check success

Jan 1 00:00:38 Inter-Card Communicating integrity-check success

Jan 1 00:00:38 Card system integrity-check success

Jan 1 00:00:38 QoS integrity-check success

Jan 1 00:00:38 OSPF integrity-check success

Jan 1 00:00:38 BEIGRP integrity-check success

Jan 1 00:00:39 Rip integrity-check success

Jan 1 00:00:39 BGP integrity-check success

Jan 1 00:00:39 BFD integrity-check success

Jan 1 00:00:39 IGMP integrity-check success

Jan 1 00:00:39 Multicast-routing integrity-check success

Jan 1 00:00:39 PIM Dense Mode integrity-check success

Jan 1 00:00:39 PIM Sparse Mode integrity-check success

Jan 1 00:00:39 IS-IS integrity-check success

Jan 1 00:00:39 VRRP integrity-check success

Jan 1 00:00:39 NTP integrity-check success

Jan 1 00:00:39 Rmon integrity-check success

Jan 1 00:00:39 Tftp integrity-check success

Jan 1 00:00:39 File synchronizing integrity-check success

Jan 1 00:00:39 Stacking integrity-check success

Jan 1 00:00:39 Switch system started –

User Access Verification

Username: admin

Password:

Welcome to Soltech SFC5200AT Ethernet Switch

Switch>

Switch>enable

Switch#Jan 1 00:02:44 User admin enter privilege mode from console 0, level = 15

Switch#

FTP를 사용하여 소프트웨어 및 구성 업데이트

- FTP서버에서 스위치로 파일을 다운로드

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

copy ftp: **flash**: *{<64-10240> | A.B.C.D | -w | type <1 | 2> | <active | passive> | ncheck size>}*

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

매개변수 설명

매개변수	설명
A.B.C.D	FTP 서버의 IP 주소 지정된 IP 주소가 없으면, **"Copy"** 명령을 실행 한 후 IP 주소를 입력하라는 메시지가 나타납니다.
ftp user name	FTP 서버의 사용자 이름 **"Copy"** 명령을 실행 한 후 사용자 이름을 입력하라는 메시지가 나타납니다.
ftp user password	FTP 서버의 비밀번호 **"Copy"** 명령을 실행 한 후 암호를 입력하라는 메세지가 나타납니다.
<64-10240>	데이터 블록 크기 값. 선택 사항. (기본값 512)
-w	파일을 받고 해시값 검사없이 파일을 플래시에 쓰기한다. 설정파일 복사에 사용. 선택사항.
<active | passive>	FTP 연결 모드를 활성 모드(active)와 수동 모드(passive) 중에서 선택한다. 선택사항.
Type <1 | 2>	데이터 전송 모드 구성합니다.(1: ascii, 2: binary)

ncheckсize	서버에 파일 크기를 확인하지 않는다. 선택사항.

- 스위치의 파일 시스템에서 FTP 서버로 파일을 업로드

스위치의 파일 시스템에서 FTP 서버로 파일을 업로드 하십시오.

copy flash: ftp: *{<64-10240> | 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 표시하며 그에 따라 입력 합니다.

매개변수 설명

매개변수	설명
A.B.C.D	FTP 서버의 IP 주소 지정된 IP 주소가 없으면, **"Copy"** 명령을 실행 한 후 IP 주소를 입력하라는 메시지가 나타납니다.
ftp user name	FTP 서버의 사용자 이름 **"Copy"** 명령을 실행 한 후 사용자 이름을 입력하라는 메시지가 나타납니다.
ftp user password	FTP 서버의 비밀번호 **"Copy"** 명령을 실행 한 후 암호를 입력하라는 메세지가 나타납니다.
<64-10240>	데이터 블록 크기 값. 선택 사항. (기본값 512)
-w	파일을 받고 해시값 검사없이 파일을 플래시에 쓰기한다. 선택사항.
<active | passive>	FTP 연결 모드를 활성 모드(active)와 수동 모드(passive) 중에서 선택한다. 선택사항.
Type <1 | 2>	데이터 전송 모드 구성합니다.(1: ascii, 2: binary)
ncheckсize	서버에 파일 크기를 확인하지 않는다. 선택사항.

예제

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

config#copy ftp: flash:

Prompt: ftp user name[anonymous]? login-nam

Prompt: ftp user password[anonymous]? login-password

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

참조:

FTP 서버가 작동하지 않을 때 대기 시간이 길어집니다. 이 문제는 TCP 시간 종료시간(기본 75S)으로 인해 발생하면 TCP 연결 시간을 수정하기 위에 "ip tcp synwait-time" 글로벌 모드에서 명령을 구성 합니다.
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.

VTY 구성 안내

시스템은 **"line"** 명령어를 사용하여 터미널 매개변수를 구성 합니다.

이 명령을 통해 터미널에 화면에 표시되는 구성을 구성 할 수 있습니다.

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

Line console (선택 – 기본 aaa 사용자 계정 사용)

명령어	설명
config	구성 모드로 진입
line console 0	라인 콘솔 모드로 전환
pass-group <group-name>	비밀번호 규칙 그룹을 적용하는 구성
password 0	비밀번호 입력
Please input password: Please input the password AGAIN:	사용할 비밀번호 입력 및 확인까지 2 회 입력. (인증 피드백 보호기능 제공)
no password	콘솔에 생성되어있는 비밀번호를 삭제
no pass-group	콘솔에 적용된 비밀번호 규칙 그룹을 해제

Line VTY (선택 – 기본 aaa 사용자 계정 사용)

명령어	설명
config	구성 모드로 진입

line vty <0-31> <0-31>	라인 콘솔 모드로 전환
pass-group <group-name>	비밀번호 규칙 그룹을 적용하는 구성
password 0	비밀번호 입력
Please input password: Please input the password AGAIN:	사용할 비밀번호 입력 및 확인까지 2 회 입력. (인증 피드백 보호기능 제공)
no password	콘솔에 생성되어있는 비밀번호를 삭제
no pass-group	콘솔에 적용된 비밀번호 규칙 그룹을 해제

Show line 을 실행하여 VTY 구성을 확인합니다.

네트워크 관리 구성

SNMP 구성

개요

SNMP 시스템에는 다음과 같이 나눌 수 있습니다.

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

SNMP 는 응용프로그램 계층에서 작동하는 프로토콜 입니다. SNMP 관리 측과 에이전트 간에 패킷 형식을 제공 합니다.

SNMP 관리적인 측면으로 네트워크 관리 시스템(CiscoWorks 와 같은 NMS)의 일부가 될 수 있습니다. Agent 및 MIB 은 시스템에 저장 됩니다. 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 베이스 입니다. 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 계층 상태(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 수신 되었다고 확신 할 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 도달 할 수 있습니다 "inform request"은 보다 신뢰성이 높기 때문에 시스템 및 네트워크의 더 많은 자원을 소비 합니다. 트랩은 전송 될 때 폐기 됩니다. 에코가 수신되거나 요청시간이 초과 될 때까지 "inform request"를 메모리에 저장해야 합니다. 또한 Trap 은 한번만 전송되고 "inform request"는 여러 번 재전송 될 수 있습니다. 재전송 "inform request"는 네트워크 통신에 추가가 되므로 더 많은 부하를 유발 합니다. 또한 트랩은 한번만 전송되고 "inform request"은 여러 번 재전송 될 수 있습니다. 따라서 트랩 및 알림 요청은 안정성과 리소스 간에 균형을 유지 합니다. SNMP

관리시스템에서 모든 알림를 대량 수신해야 하는 경우 "inform request"을 사용할 수 있습니다.

네트워크의 통신량을 우선시 하고 모든 통지를 받을 필요가 없으면 Trap 을 사용할 수 있습니다.

이 스위치는 트랩을 지원하지만 "inform request"에 대한 확장도 제공 합니다.

SNMP 버전

다음과 같은 SNMP 버전을 스위치 시스템은 지원합니다.:

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

SNMPv1 은 그룹 기반 보안 형식을 사용하고. IP 주소 접근 제어 및 암호를 사용하여 에이전트 MIB 에 접근 할 수있는 관리 측 그룹을 정의합니다.

SNMPv3 은 네트워크를 통한 패킷 인증 및 암호화의 조합을 통해 장치에 대한 보안 접근을 제공합니다.

SNMPv3 에서 제공되는 보안 기능은 다음과 같습니다.

•메시지 무결성— 패킷이 전송 중에 변조되지 않았는지를 확인 합니다.

•인증—메시지가 유효한 소스 주소 인지 확인 합니다.

•암호화— 패킷의 내용이 혼합되면 승인되지 않은 출처에 패킷을 볼 수 없습니다.

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 처리 할 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 통신 할 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..

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(incloud / excloud)을 제어하는 것입니다. 다음 명령을 사용하여 구성을 구성하십시요.

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

	Include : 액세스 허용

SNMP 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 제한 할 수 있습니다.

SNMP Community 에 대한 접근 제어 구성 또는 수정

SNMP community 의 문자열을 사용하여 관리시스템과 장비사이의 관계를 정의 할 수 있습니다. Community 문자열은 관리시스템이 장비에 로그인 할 수 있게 하는 암호와 유사합니다.

Community 문자열과 관련하여 하나 이상의 속성을 지정할 수 있습니다:

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

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

시스템 관리자의 호출 방법 및 시스템의 위치 설명 구성

SysContact 와 SysLocation 은 시스템 그룹에서의 관리 변수는 MIB 이며 각각의 장비의 ID 값과 위치를 정의 합니다. 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 문자열을 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 구성 할 수 있습니다. 글로벌 모드에서 다음 명령어를 사용 할 수 있습니다.

명령어	기능
snmp-server packetsize *byte-count*	2 데이터 패킷의 최대 길이를 구성합니다.

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 } }}*community-string* [*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 실행 됩니다. 모든 유형의 Trap 이 활성화 됩니다.

"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 활성화 해야 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 통과 할 수 없습니다.

명령어	기능
snmp-server user <name> <group> **v3 priv** <aes128 | aes256 | aes256-c> **auth** <sha | sha256> **<priv_passwd> <auth_passwd>**	SNMP v3 사용자 이름, 그룹, 암호화, 인증 방식 구성 (구성 후, 9 암호문 형태로 표시) priv_passwd: 암호화 비밀번호 입력(9 ~32글자) auth_passwd: 사용자 인증 비밀번호 입력(9~32글자)

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)

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 입력 할 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 80000523015a000003

snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 9 e7a86399065c56fa8645cc14e33f29f2d ac965c3d73fd879fb424419cac7a3ff

snmp-server user set-user setter v3 auth sha 9 2e556b053bf1903cf40643b2687dbdba5 2aa1ce594605fd77247f3322f88b48f

snmp-server user test admin_g v3 priv aes256 auth sha256 9 65c03eaf2ea90e0cdb8cf 68572b690fcec03713d31f1e566738db3e2dbe0fdae d3ec854a04c12dacc1ca380d999afe8d0054 e02370c8069000c8efd3ea112227

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 찾아 볼 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 암호화 합니다.

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

RMON 구성

RMON 구성 작업

RMON 구성 작업:

- 스위치에 대한 RMON 경보 기능
- 스위치에 대한 RMON 이벤트 기능
- 스위치에 대한 RMON 통계 기능
- 스위치에 대한 RMON 기록 기능
- 스위치 RMON 구성 표시

스위치에 대한 RMON 경보 기능

Command line 또는 SNMP NMS 를 통해 rMON 경보 기능을 구성 할 수 있습니다.

SNMP NMS 를 통해 구성하는 경우 스위치의 SNMP 를 구성해야 합니다.

경보 기능이 구성된 후 장치는 시스템의 일부 통계 값을 모니터 할 수 있습니다.

다음 표는 rMON 알람 기능을 구성하는 방법을 보여줍니다

명령어	기능
configure	전역 모드로 들어갑니다.
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*] [**repeat**]	RMON 알람 항목을 추가하십시오. **Index** 는 경보 항목의 색인입니다. 유효 범위는 1~65535 입니다. **Variable** 은 모니터링 되는 MIB 의 객체입니다. 시스템에서 유효한 MIB 객체여야 하며, Integer, Counter, Gauge 또는 Time Ticks 유형의 Objects 만 탐지 할 수 있습니다. **Interval** 은 샘플링을 위한 시간단위입니다. 단위는 초 단위이며 유효 값은 1 에서 2147483647 사이 입니다. **Absolute** 는 MIB 객체으 값을 직접 모니터링 하는 데 사용됩니다. 델타는 두 샘플링 사이에서 MIB 오브젝트의 값 변경을 모니터 하는데 사용됩니다. **Value** 는 경보가 생성될 때 임계 값입니다. 이벤트 번호는 임계 값에 도달했을 때 생성되는 이벤트의 index 값입니다. 이벤트 번호는 선택사항 입니다. **Owner string 은** 알람에 대한 정보를 설명합니다.
exit	관리자 모드로 되돌아갑니다.
write	구성을 저장합니다.

rMON 경보 항목이 구성된 후 장치는 지정된 OID 값을 가져옵니다.

획득된 값은 alarm 유형(알파 또는 델타)에 따라 이전 값과 비교됩니다.

획득된 값이 이전 값보다 크고 상승 임계 값으로 지정된 임계 값을 초과하는 경우 이벤트 번호가 index 번호인 이벤트. (이벤트 번호가 0 이거나 이벤트 번호가 index 번호가 될때 이벤트가 발생하지 않음)

변수가 지정된 OID 를 얻을 수 없으면 이 행의 알람 항목 상대가 무효로 구성됩니다. 동일한 색인으로 경보 항목을 구성하기 위해 rmon alarm 을 여러 번 실행하면 마지막 구성만 효과적입니다. 아무런 rmon alarm 의 index 도 실행하지 않아 인덱스가 동일한 알람 항목을 취소 할 수 있습니다.

스위치에 대한 RMON 이벤트 기능

다음 표에는 RMON 이벤트를 구성하는 단계가 나와있습니다:

단계	명령어	설명
1.	**configure**	글로벌 모드로 들어갑니다.
2.	**rmon event index** [**description** *string*] [**log**] [**owner** *string*] [**trap** community] [**ifctrl** interface]	RMON 이벤트 항목을 추가하십시오. **Index** 는 이벤트 항목 색인이며 유효 범위는 1~65535 입니다. **Description** 은 이벤트에 대한 정보를 의미합니다. **Log** 는 이벤트가 발생될 때의 로그 테이블에 정보를 추가하는 것을 의미 합니다. Trap 은 이벤트가 발생될 때 Trap 메시지의 생성됨 의미 합니다. **Community** 는 Community 이름입니다. **Owner string 은** 알람에 대한 정보를 설명합니다.
3.	**exit**	관리자 모드로 되돌아갑니다.
4.	**write**	구성을 저장합니다.

rMON 이벤트가 구성된 후에는 rMON 경보가 발생할 때 rMON 이벤트 항목의 도메인 eventLastTimeSent 를 SysUpTime 으로 구성해야 합니다.

Log 속성이 rMON 이벤트로 구성되면 메시지가 로그 테이블에 추가 됩니다. Trap 속성이 rMON 이벤트로 구성되면 트랩 메시지가 커뮤니티 이름으로 전송됩니다. rMON 이벤트를 여러 번 실행하여 동일한 index 로 이벤트 항목을 구성하면 마지막 구성만 적용됩니다. rMON 이벤트 index 를 실행하여 index 가 동일한 이벤트 항목을 취소할 수 있습니다

스위치의 RMON 통계 구성

rMON 통계 그룹은 장치의 모든 포트에 대한 통계 정보를 모니터 하는데 사용됩니다.

rMON 통계를 구성하는 단계는 다음과 같습니다

단계	명령어	설명
1.	**configure**	3 전역 모드로 들어갑니다.
2.	**interface iftype ifid**	4 포트 모드로 들어갑니다. iftype은 모듈 유형을 의미 합니다.

		5	Ifid는 포트의 ID를 의미합니다.
3.	**rmon collection stat index** [**owner** *string*]	6	포트에서 통계 기능을 활성화 합니다. **index**는 통계의 색인을 의미합니다. **owner string**은 통계에 대한 정보를 설명하는 것입니다.
4.	**exit**	7	전역 모드로 돌아 갑니다.
5.	**exit**	8	관리자 모드로 돌아 갑니다.
6.	**write**	9	구성을 저장합니다.

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

스위치의 RMON 기록 구성

rMON 기록 그룹은 장치의 포트에서 다른 시간 섹션의 통계 정보를 수집하는데 사용됩니다.

rMON 통계 기능은 다음과 같이 구성됩니다

단계	명령어	설명
1.	configure	글로벌 모드로 들어갑니다.
2.	interface iftype ifid	포트 모드로 들어갑니다. iftype 은 모듈 유형을 의미 합니다. Ifid 는 포트의 ID 를 의미합니다.
3.	rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	포트에서 통계 기능을 활성화 합니다. **index** 는 항목의 색인을 의미합니다. 이력 항목으로 수집된 모든 데이터 중에서 최신 버킷 번호 항목을 저장해야 합니다. 이러한 통계 값을 얻기 위해 이더넷의 기록 항목을 찾아 볼 수 있습니다. 기본값은 50 개 입니다. 두 번째는 격일로 통계 데이터를 확보하는 간격을 의미합니다. 기본 값은 1800 초 입니다. **owner string** 은 통계에 대한 정보를 설명하는 것입니다.
4.	exit	글로벌 모드로 돌아 갑니다.
5.	exit	관리자 모드로 돌아 갑니다.
6.	write	구성을 저장합니다.

RMON 기록 항목이 추가되면 장치는 지정된 포트에서 2 초마다 통계 값을 가져옵니다.

통계 값은 정보 항목으로 이력 항목에 추가 됩니다. rMON 수집, 기록, 색인을 여러 번 실행하여

동일한 색인으로 기록 항목을 구성하면 마지막에 구성 넣은 값만 적용 됩니다.

rMON 기록 index 를 실행하여 index 가 동일한 기록 항목을 취소할 수 있습니다.

참조:

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

스위치의 RMON 구성 표시

show 명령어를 실행하여 스위치의 rMON 구성을 보여줍니다.

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

SSH

개요

SSH 서버

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

클라이언트

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

기능

SSH 서버 및 SSH 클라이언트는 버전 2.0 을 지원합니다.

구성 작업

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. (선택)

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	미리 정의한 ACL을 적용합니다.

인증 시간 초과 값 구성

클라이언트와 서버간에 연결이 구성된 후 구성된 시간 내에 인증을 승인 할 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

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 시간을 구성 하십시오:

명령어	설명
ip sshd auth-retries <0-65535>	Configures the maximum times for retrying authentication.

SSH 서버 활성화

SSH 서버는 기본적으로 비활성화 되어 있습니다. SSH 서버가 활성화 되면 장치는 rsa 암호를 쌍으로 생성 한 다음 클라이언트의 연결 요청을 수신합니다. 과정은 1~2 분 정도 소요 됩니다.

글로벌 구성 모드에서 다음 명령어를 실행하여 SSH 서버를 활성화 합니다.

명령어	설명
ip sshd enable	SSH 서버를 사용 합니다. 암호는 2048bit 로 생성 됩니다.

SSH 버전 구성

SSH 버전을 구성 합니다.

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

SSH 키 저장

SSH 활성화후 생성된 키를 플래시 메모리에 저장하기 위해 다음 명령어를 실행 합니다.

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

SFTP 활성화

SSH 활성화후 SFTP 를 활성화 하기 위해 다음 명령어를 실행 합니다.

명령어	설명
ip sshd sftp	SFTP 를 플래시 메모리에 파일로 저장합니다.

SSH 동시 접속 세션 제한

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

SSH 접속자 확인

명령어	설명
show ssh	ssh 접속자 정보를 표시한다. 접속 IP, TCP 포트정보
show tcp brief	TCP 접속 세션 정보를 표시한다.

SSH 서버 구성 예제

다음 구성에서는 IP 주소가 192.168.20.40 인 host 만 SSH 서버에 접속 할 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
```

SSH 클라이언트 기능 사용

SSH 클라이언트 기능을 사용하려면 아래 명령을 참조 하십시오.

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.

Telnet 구성

Telnet 서비스 구성

명령어	설명
ip telnet enable	Telnet 를 사용할 수 있도록 활성화
ip telnet sour-interface vlan *<interface-id>*	Telnet 접속을 허용할 인터페이스를 지정
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

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. 접속 횟수 제한 : 3~10 회 재 접속 대기 시간 : 30~86400 초.
no ip telnet attack-defense	접속횟수 및 재접속 대기시간 구성 삭제

Telnet 동시 접속 세션 제한

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

관리자 접근제어 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 ACL을 Telnet

	서비스에 적용합니다.

Telnet 접속자 확인

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

인증(AAA) 구성

AAA 개요

액세스 제어는 네트워크 및 서비스에 대한 액세스를 제어하는 방법입니다. 인증, 권한 부여 및 계정 (AAA) 네트워크 보안 서비스는 라우터 또는 액세스 서버에 대한 액세스 제어를 구성하는 기본 프레임 워크를 제공합니다.

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. 명명 된 인증 방법 목록을 정의한 다음 해당 목록을 다양한 인터페이스에 적용하여 AAA 인증을 구성합니다. 메소드 목록은 수행 할 인증 유형 및 수행 할 인증 순서를 정의합니다. 정의 된 인증 메소드가 수행되기 전에 특정 인터페이스에 적용되어야합니다. 예외는 기본 메소드 목록 ("default"라는 이름)입니다. 기본 메소드 목록은 다른 메소드 목록이 정의되지 않은 경우 모든 인터페이스에 자동으로 적용됩니다. 정의 된 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 포함 된 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, 실행 된 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 추적 할 수 있습니다. AAA 계정이 활성화되면 네트워크 접근 서버는 계정 활동의 형태로 사용자 활동을 RADIUS 또는 TACACS + 보안 서버 (구현 한 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 명명 된 계정 방법 목록을 정의한 다음 다양한 인터페이스에 적용하여 AAA 계정을 구성합니다. AAA 를 사용하여 계정을 구성하는 방법에 대한 자세한 내용은 "계정 구성"장을 참조하십시오.

AAA 사용 이점

AAA의 이점:

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

AAA 원리

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

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 실패 할 경우를 대비하여 인증을 위한 백업 시스템을 보장 할 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 소모 될 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 응답 함) 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.

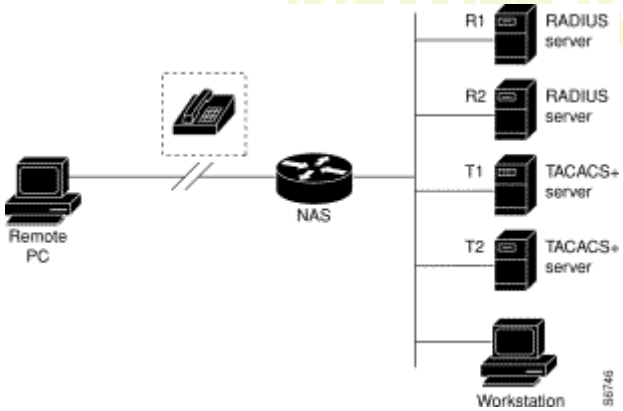


그림 0-1 전형적인 AAA 네트워크 구성

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 거부 될 때까지 또는 세션이 종료 될 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 포함 된 기준을 충족하지 못했음을 의미합니다. 인증은 FAIL 응답으로 끝납니다. ERROR 는 보안 서버가 인증 쿼리에 응답하지 않았 음을 의미합니다. 이 때문에 인증이 시도되지 않았습니다. ERROR 가 탐지 된 경우에만 AAA 는 인증 방법 목록에 정의 된 다음 인증 방법을 선택합니다..

AAA 구성 과정

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

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.

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

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.

AAA 을 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.

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

명령어	내용
aaa authentication login {**default** | *list-name*} *method1* [*method2*...]	전역 AAA를 활성화합니다.
line [**console** | **vty**] *line-number* [*ending-line-number*]	인증 목록을 적용 할 회선에 대한 회선 구성 모드를 시작합니다.
login authentication {**default** | *list-name*}	인증 목록을 한 줄 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 추가 하십시오.

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.

권한 단계 별 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	내용
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 입력 된 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.

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 실패 할 때 표시 될 메시지 배너를 구성 할 수 있습니다.

로그인 배너 구성하기

사용자가 로그인 할 때마다 표시 될 배너를 구성하려면 (로그인 용 기본 메시지 대체) 전역 구성 모드에서 다음 명령을 사용하십시오. :

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

로그인 실패 배너 구성하기

사용자가 로그인에 실패 할 때마다 표시되는 메시지를 구성하려면 (로그인 실패에 대한 기본 메시지 대체) 전역 구성 모드에서 다음 명령을 사용하십시오: :

명령어	내용
aaa authentication fail-message *delimiter text-string delimiter*	사용자가 로그인에 실패 할 때 표시 할 메시지를 작성합니다.

설명

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

AAA 사용자 이름 인증

사용자에게 사용자 이름을 입력하라는 메시지가 표시 될 때 표시되는 텍스트를 변경하려면 전역 구성 모드에서 aaa authentication username-prompt 명령을 사용하십시오. 기본 사용자 이름 프롬프트 텍스트로 돌아가려면이 명령의 no 형식을 사용하십시오.

aaa authentication username-prompt 명령은 원격 TACACS + 서버가 제공하는 대화 상자를 변경하지 않습니다. 전역구성모드에서 구성하려면 다음 명령을 사용하십시오. :

명령어	내용
aaa authentication username-prompt *text-string*	String of text that will be displayed when the user is prompted to enter an username.

AAA 사용자 비밀번호 인증

사용자에게 암호를 묻는 메시지가 표시 될 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	내용
aaa authentication password-prompt *text-string*	사용자가 암호를 입력하라는 메시지가 표시 될 때 표시 할 문자열입니다.

사용자이름 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 암호화 된 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*

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**

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 인증 한 경우 PPP 인증이 수행되지 않습니다.
- aaa authorization network radius-network radius 명령 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.

AAA 권한 구성 작업 목록

- AAA 를 사용하여 EXEC 권한 구성

AAA 권한 구성 작업

AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오. :

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

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

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

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 반환 할 수 있습니다.

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

명령어	내용
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	전역 권한 부여 목록을 구성합니다.
line [**console** | **vty**] *line-number* [*ending-line-number*]	인증 방법 목록을 적용 할 라인에 대한 구성 모드를 시작합니다.
login authorization {**default** | *list-name*}	권한을 행 이나 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 실패 할 경우 백업 시스템을 보장 할 수 있습니다. 시스템은 나열된 첫 번째 방법을 사용하여 특정 네트워크 서비스에 대해 사용자에게 권한을 부여합니다. 해당 메소드가 응답하지 않으면 시스템은 메소드 목록에 나열된 다음 메소드를 선택합니다. 이 프로세스는 나열된 권한 부여 메소드와의 성공적인 통신이있을 때까지 또는 정의 된 모든 메소드가 모두 소진 될 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. :

키워드	설명
group *WORD*	권한 부여를 위해 지정된 서버 그룹을 사용합니다.
group radius	Radius권한을 사용합니다
local	권한 부여에 로컬 DB를 사용합니다.
if-authenticated	사용자가 인증 된 경우 요청 된 기능에 접근이 가능합니다.
none	권한 부여를 수행하지 않습니다.

AAA 권한 예제

EXEC 로컬 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 수행 할 수 있습니다.
- 사용자 이름은 exec4, 로그인 암호는 abc, 사용자의 최대 링크는 10 입니다.

AAA 계정 구성 작업 목록

- AAA 사용 계정 연결 구성
- AAA 네트워크 계정 구성

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..

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	내용
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. 키워드 키워드는 Accounting 프로세스 중에 채택 된 실제 방법을 지정합니다..

다음 표는 현재 지원되는 연결 계정 방법을 나열합니다. :

키워드	설명
group *WORD*	계정에 대하여 명명 된 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 요청 된 프로세스가 시작될 때 "시작"계정 알림을 보내고 프로세스가 끝날 때 "중지"계정 알림을 보냅니다.

AAA 을 이용한 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	내용
aaa accounting network {**default** | *list-*	네트워크 전역 계정 활성화

name} {**start-stop** | **stop-only** | **none**} **group** *groupname*	

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

다음 표는 현재 지원되는 네트워크 계정 방법을 나열합니다.

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

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	내용
aaa accounting update [**newinfo**] [**periodic** *number*]	AAA 계정 업데이트 활성화

새 정보 키워드를 사용하면 보고 할 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 전송 될 때까지 해당 사용자에 대해 기록 된 모든 계정 정보가 들어 있습니다.

newinfo 및 periodic 키워드를 모두 사용하는 경우 보고 할 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.

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**

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.

개요

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 포함 된 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 제어 할 수 있습니다. 예를 들어 사용자가 로그인하면 RADIUS 는이 사용자를 IP 주소 10.2.3.4 를 사용하여 PPP 를 실행할 수있는 권한으로 식별하고 정의 된 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 사용 된 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.

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 포함 된 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

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.
- 정의 된 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

RADIUS 구성 작업

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 지정해야합니다.

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

명령어	내용
radius-server host *ip-address* [**auth-port** *port-number*][**acct-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	내용
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.

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	내용
radius-server vsa send [authentication]	네트워크 액세스 서버가 RADIUS IETF 속성 26에 정의 된대로 VSA를 인식하고 사용할

	수 있습니다.

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 입력해야합니다. 자세한 내용은 "인증 구성"장을 참조하십시오.

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.

특정 RADIUS 계정

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

RADIUS 구성 예제

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.

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.

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 적용 할 수 있는 통신 정보가 포함됩니다.

지원되는 인터페이스 유형

인터페이스 유형에 대한 자세한 내용은 다음 표를 참조하십시오.

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

지원되는 두 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

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 단축 된 인터페이스 형식으로 구성됩니다. 이 인터페이스를 번호로 사용하십시오. 번호는 설치 (exworks) 또는 인터페이스 카드가 시스템에 추가 될 때 지정됩니다. 이 인터페이스를 표시 하려면 **show interface** 명령을 실행하십시오 . 장치가 지원하는 각 인터페이스는 다음과 같이 자체 상태를 제공합니다.

```
스위치 # show interface
GigaEthernet1/1 is down, line protocol is down
Hardware is Fast Ethernet, Address is 0009.7cf7.7dc1
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
 Auto-duplex, Auto-speed
```

input flow-control is off, output flow-control is off

ARP type: ARPA, ARP Timeout 04:00:00

Last input never, output 17:52:52, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

1 packets input, 64 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 0 multicast, 0 pause input

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”.

.

노트 :

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

(1) 인터페이스 구성 모드에서 인터페이스 구성 명령을 구성 할 수 있습니다. 다양한 명령은 인터페이스에서 실행될 프로토콜 및 응용 프로그램을

정의합니다. 이 명령은 사용자가 인터페이스 구성 모드를 종료하거나 다른 인터페이스로 전환 할 때까지 유지됩니다.

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

인터페이스 구성

인터페이스 공통 속성 구성

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

설명 추가

관련 인터페이스에 대한 설명을 추가하면 인터페이스에 첨부 된 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.

인터페이스 설명 추가와 관련된 예제는 다음 섹션 '인터페이스 설명 예'를 참조하십시오.

대역폭 구성

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

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

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

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.

인터페이스 모니터링 및 유지 보수

다음 작업은 인터페이스를 모니터하고 유지 보수 할 수 있습니다.

인터페이스 상태 점검

인터페이스 초기화 및 삭제

인터페이스 다운 및 활성화

인터페이스 상태 확인

우리의 스위치는 소프트웨어 및 하드웨어의 버전 번호, 인터페이스 상태 등 인터페이스 정보와 관련된 몇 가지 명령을 표시 할 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.

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.

인터페이스 종료 및 활성화

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 전송 될 수 있습니다.

인터페이스 구성 모드에서 인터페이스를 종료하거나 활성화하려면 다음 명령을 사용하십시오.

명령	기술
shutdown	인터페이스를 종료합니다.
no shutdown	인터페이스를 사용합니다.

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

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

널 (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 기능 할 수 있습니다.

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

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

널 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

루프백 인터페이스 구성

루프백 인터페이스는 물류 인터페이스입니다. 외부 인터페이스가 종료 된 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 처리 될 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.

집계 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

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.

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 소유 할 수 없습니다.

명령 줄을 통해 Super VLAN 인터페이스를 구성 할 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. **index** 는 Super VLAN 인터페이스의 색인입니다. 유효 값의 범위는 1 에서 32 사이입니다. 슈퍼 VLAN 인터페이스를 삭제할 수 **없습니다** .
[no] subvlan [*setstr*] **[add** *addstr***] [remove** *remstr***]**	슈퍼 VLAN 에서 SubVLAN 을 구성 합니다. 추가 된 하위 VLAN 은 관리 인터페이스를 소유 할 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. **setstr** 은 Sub VLAN 목록을 구성하는 것을 의미합니다. 예를 들어 List 2,4-6 은 VLAN 2, 4, 5 및 6 을 나타냅니다. **add** 는 원래의 SubVLAN 목록에 VLAN 목록을 **추가** 하는 것을 의미합니다. **addstr** 은 위와 같은 형식의 문자열을 의미합니다. **제거** 는 원래의 SubVLAN 목록에서 VLAN 목록을 삭제 **하는** 것을 의미합니다. remstr 는 위와 같은 형식의 목록의 문자열입니다. SuperVLAN 에서 모든 SubVLAN 을 삭제할 수 없습니다.

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

인터페이스 구성 예

공용 속성의 인터페이스 구성

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
```

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
```

인터페이스 범위 구성

인터페이스 범위 구성

인터페이스 범위의 이해

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

Note :

인터페이스 범위 모드로 들어가면 모드에 포함된 인터페이스가 구성 되어야 합니다.

인터페이스 범위 모드로 들어가기

'interface range' 모드로 들어가기 위해 다음 명령어를 실행 하십시오.

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

구성 예제

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

Switch_config# interface range giga1 – 3 , 6 , 8 , 10 – 12

Switch_config_if_range#

물리적인 인터페이스 특성 구성

인터페이스 구성하기

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

이더넷 인터페이스 구성

전역모드에서 다음 명령을 실행하여 이더넷 인터페이스 구성 상태로 들어갑니다.

명령어	설명
interface gigaethernet [*slot/port*]	Gigaethernet 인터페이스에 접속합니다.
interface gigaethernet [*slot/port*]	Gigaethernet 인터페이스에 접속합니다.

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

속도 구성

이더넷 속도는 자동협상 또는 인터페이스에서 구성을 하여 구현 할 수 있습니다

명령어	실행
Speed {**10**|**100**|**1000**|**auto**}	이더넷 인터페이스에 10M, 100M, 1000M 혹은 Auto-negotiation의 옵션을 이용하여 Rate값을 구성 합니다
No speed	Rate옵션을 삭제합니다. 기본구성 auto-negotiation으로 돌아갑니다.

메모:

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 협상 할 수 없습니다. 기본 구성에서는 기가비트 인터페이스의 자동 협상을 활성화 할 수 있지만 100Mbps 인터페이스의 자동협상은 비활성화 입니다.

인터페이스에 흐름제어 구성하기

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

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

인터페이스 구성

인터페이스 구성하기

스위치는 10~10,000Mbps 이더넷 인터페이스를 지원합니다. 자세한 구성은 다음 내용을 참조하십시오. 구성 중 첫 번째 단계는 필수 사항이며 나머지는 선택 사항입니다.

포트 흐름 제어 구성

구성을 통해 들어오고 나가는 포트의 유량을 제어 할 수 있습니다.

미리 지정된 모드에서 다음 명령을 실행하여 포트의 유속을 제한하십시오.

각 대역은 기본적으로 128 kbps 입니다.

명령어	설명
configure	전역 구성모드를 시작합니다.
interface g0/0	구성 할 포트를 입력합니다.
[no] switchport rate-limit *band* { ingress|egress}	매개변수 대역은 제한 될 유량을 나타냅니다. 매개변수 유입/유출은 각각 수신/송신 포트에서 기능이 작동 함을 의미합니다.
exit	전역 구성 모드를 종료합니다.

포트에 Storm-control 기능 구성

스위치의 포트는 연속 비정상적인 유니 캐스트 (MAC 주소 검색 실패), 멀티 캐스트 또는 브로드 캐스트 메시지에 의한 공격을 수신 할 수 있습니다. 이 경우 공격 한 포트 또는 전체 스위치가 고장날 수 있습니다. 따라서 포트의 스톰 제어 메커니즘이 생성됩니다.

명령어	설명

storm-control {**broadcast** | **multicast** | **unicast**} **threshold count**	브로드 캐스트 / 멀티 캐스트 / 유니 캐스트 메시지에 대한 스톰 제어를 수행합니다.
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**	기능을 취소합니다.

보안 포트 구성

개요

보안 포트의 액세스 기능을 제어하여 구성에 따라 포트를 특정 범위에서 실행할 수 있습니다. 포트의 보안 MAC 주소 수를 구성하여 포트의 보안 기능을 활성화 한 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.

보안 포트의 구성 작업

- 보안 포트모드로 구성합니다
- 보안 포트의 정적 MAC 주소를 구성합니다

보안 포트 구성하기

보안포트 구성하는 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 수신 될 수 있습니다. 리 젝트 모드 인 경우 소스 주소가 로컬 MAC 주소와 다른 흐름 만 포트에서 수신 할 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 통신 할 수 있습니다. 거부 모드에서는 소스 주소가 로컬 MAC 주소와 다른 흐름을 포트에서 수신 할 수 있습니다.

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

명령어	설명
configure	전역 구성 모드를 시작합니다.
interface g0/1	구성할 포트를 입력합니다.
[no] switchport port-security static mac-address *mac-addr*	보안 포트의 정적 MAC 주소를 추가하거나 삭제합니다. mac-addr은 구성된 MAC 주소입니다.
exit	전역 구성모드로 돌아갑니다
exit	EXEC 모드로 돌아갑니다
write	구성을 저장합니다.

포트미러링 구성하기

포트미러링 작업 목록 구성

- 포트 미러링 구성하기
- 포트미러링 정보 표시

포트미러링 구성 작업

포트 미러링 구성

포트 미러링을 구성하면 스위치의 한 포트를 사용하여 포트 그룹의 트래픽을 관찰 할 수 있습니다.

포트 미러링을 구성하려면 권한 모드로 들어가 다음 단계를 수행하십시오.

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

포트미러링 정보 표시

show 를 실행하여 포트 미러링의 구성 정보를 표시합니다.

명령어	설명

show mirror [session *session_number]*	미러링포트의 구성정보를 표시합니다. **session-number :** 미러링포트의 수를 나타냅니다.

MAC 주소 속성 구성

MAC 주소 구성 작업 목록

정적 Mac 주소 구성

Mac 주소 에이징 시간 구성

VLAN 공유 MAC 주소 구성

Mac 주소 표 표시

동적 Mac 주소 지우기

MAC 주소 구성 작업

정적 Mac 주소 구성

정적 MAC 주소 항목은 스위치에 의해 사용되지 않고 수동으로 만 삭제할 수있는 MAC 주소 항목입니다.

명령	설명
config	전역 구성 모드를 시작합니다.
[no] mac address-table static *mac-addr* **vlan***vlan-id* **interface** *interface-id*	정적 MAC 주소 항목을 추가 / 삭제합니다. Mac-addr 은 MAC 주소를 나타냅니다. Vlan-id 는 VLAN 번호를 나타냅니다. 유효한 값은 1 ~ 4094 입니다. Interface-id 는 인터페이스 이름을 나타냅니다.
exit	EXEC 모드로 돌아갑니다.
write	구성을 저장합니다.

MAC 주소 에이징 시간 구성

지정된 에이징 시간 동안 동적 MAC 주소가 사용되지 않으면 스위치는 MAC 주소를 MAC 주소 테이블에서 삭제합니다. 스위치 MAC 주소의 에이징 시간은 필요에 따라 구성 할 수 있습니다. 기본 에이징 시간은 300 초입니다.

다음과 같이 권한 모드에서 MAC 주소의 에이징 시간을 구성 합니다.

명령	설명
config	글로벌 구성 모드로 들어갑니다.
mac address-table aging-time [0 | 10-1000000]	MAC 주소의 에이징 시간을 구성합니다. 0 은 MAC 주소가 없음을 나타냅니다. 유효한 값은 초 단위로 10 에서 1000000 입니다.
exit	관리 모드로 돌아갑니다.
write	구성을 저장합니다.

MAC 주소 표 표시

운영 프로세스에서 디버깅 및 관리가 필요하기 때문에 스위치 MAC 주소 테이블의 내용을 알고 싶습니다. 스위치 MAC 주소 테이블의 내용을 표시하려면 show 명령을 사용하십시오.

명령	설명
show mac address-table {**dynamic** [**interface**interface-id | **vlan** vlan-id] | **static**}	MAC 주소 테이블의 내용을 표시합니다. Dynamic 은 동적으로 획득하는 MAC 주소를 나타냅니다. Vlan-id 는 VLAN 번호를 나타냅니다. 유효한 값은 1 에서 4094 사이입니다. Interface-id 는 인터페이스 이름을 나타냅니다. Static 은 정적 MAC 주소 테이블을 나타냅니다.

동적 MAC 주소 지우기

다음 명령을 사용하여 권한 모드에서 동적 MAC 주소를 삭제하십시오.

명령	설명
clear mac address-table dynamic [address*mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*]	동적 MAC 주소 항목을 삭제합니다. 동적은 동적으로 획득하는 MAC 주소를 나타냅니다. Mac-addr 은 MAC 주소입니다. Interface-id 는 인터페이스 이름을 나타냅니다. Vlan-id 는 VLAN 번호를 나타냅니다. 유효한 값은 1 에서 4094 사이입니다.

MAC 목록 구성

MAC 목록 구성 작업

MAC 목록 생성

MAC 목록을 포트에 적용하려면 먼저 MAC 목록을 만들어야합니다. MAC 목록이 성공적으로 생성되면 MAC 목록 구성 모드로 로그인 한 다음 MAC 액세스 목록의 항목을 구성 할 수 있습니다.

권한 모드에서 MAC 목록을 추가 및 삭제하려면 다음 작업을 수행하십시오.

운영...	설명
configure	글로벌 구성 모드로 로그인하십시오.
[**no**] **mac access-list** *name*	MAC 목록을 추가하거나 삭제하십시오. **name** 은 MAC 목록의 이름을 의미합니다.

MAC 목록의 항목 구성

당신은 사용 **허가** 또는 **거부** 구성 명령을 **허가** 또는 **거부** MAC 리스트의 항목을. 여러 개의 **허용** 또는 **거부** 항목을 MAC 목록에 구성 할 수 있습니다.

MAC 목록에 구성된 여러 항목의 마스크는 동일해야합니다. 그렇지 않으면 구성이 유효하지 않을 수 있습니다 (다음 예 참조). 동일한 항목은 동일한 MAC 주소에서 한 번만 구성 할 수 있습니다.

MAC 목록 구성 모드에서 다음 작업을 수행하여 MAC 목록의 항목을 구성 합니다.

운영...	설명
[no] {deny | permit} {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*}**[**ethertype**]**	MAC 목록의 항목을 추가 / 삭제합니다. 명령을 다시 실행하여 MAC 목록의 여러 항목을 추가하거나 삭제할 수 있습니다. MAC 주소가 호환 될 수있는 **모든** 수단;

	src-mac-addr 은 소스 MAC 주소를 의미합니다. **dst-mac-addr** 은 대상 MAC 주소를 의미합니다. **ethertype** 은 일치하는 이더넷 패킷 유형을 의미합니다.
exit	MAC 목록 구성 모드에서 로그 아웃하고 글로벌 구성 모드로 다시 들어갑니다.
exit	관리 모드로 다시 들어갑니다.
write	구성을 저장하십시오.

MAC 목록 구성 예

Switch_config#mac acce 1

Switch-config-macl#permit host 1.1.1 any

Switch-config-macl#permit host 2.2.2 any

The above configuration is to compare the source MAC address, so the mask is the same. The configuration is successful.

Switch_config#mac acce 1

Switch-config-macl#permit host 1.1.1 any

Switch-config-macl#permit any host 1.1.2

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

위의 구성에서 첫 번째 줄은 원본 MAC 주소를 비교하는 것이고 두 번째 줄은 대상 MAC 주소를 비교하는 것입니다. 따라서 마스크가 다릅니다. 구성이 실패합니다.

MAC 목록 적용

생성 된 MAC 목록은 모든 물리적 포트에 적용 할 수 있습니다. 하나의 MAC 목록 만 포트에 적용 할 수 있습니다. 동일한 MAC 목록을 여러 포트에 적용 할 수 있습니다.

권한 모드로 들어가서 다음 작업을 수행하여 MAC 목록을 구성 합니다.

운영...	설명

configure	전역 구성 모드로 들어갑니다.
interface g0/1	구성 할 포트에 로그인하십시오.
[**no**] **mac access-group** *name*	생성 된 MAC 목록을 포트에 적용하거나 포트에서 적용된 MAC 목록을 삭제하십시오. **name** 은 MAC 목록의 이름을 의미합니다.
exit	글로벌 구성 모드로 다시 들어갑니다.
exit	관리 모드로 다시 들어갑니다.
write	구성을 저장하십시오.

802.1x 구성

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

802.1x 구성 작업

802.1x 포트 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 수행 할 수 있습니다. 인증 방법은 포트에서 기본값으로 지정됩니다. 필수 인증 비 승인은 어떤 종류의 메소드가 적용 되더라도 포트 인증이 통과되지 않음을 의미합니다. 사용자는 포트를 통해 데이터 액세스 제어를 수행 할 수 없습니다.

802.1x 인증 시작은 포트가 802.1x 인증 프로토콜을 실행 함을 의미합니다. 802.1x 인증은 포트에 액세스하는 사용자에게 적용됩니다. 인증을 통과 한 사용자 만 포트를 통해 데이터 액세스 제어를 수행 할 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 활성화 합니다.

802.1x 재 인증 구성

첫 번째 인증이 승인 된 후 클라이언트는 특정 시간마다 인증되어 클라이언트의 적법성을 보장합니다. 이 경우 재 인증 기능을 활성화 해야 합니다.

재 인증 기능이 활성화되면 802.1x 는 주기적으로 호스트에 인증 요청을 전송합니다.

다음 명령을 실행하여 재 인증 기능을 구성 할 수 있습니다.

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

802.1x 전송 빈도 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.

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 채택 될 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 실행 하여 기본값을 다시 시작 하지 않는 한 포트는 인증 유형을 사용합니다 .

Eap-tls 는 전자 인증서를 인증 영장으로 사용하고 Translation 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** }	갈라진 갈기 또는 먹기를 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.

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.

노트 :

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 guest-vlan 이 작동 할 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.

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.

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.

VLAN 구성

VLAN 개요

가상 LAN (VLAN)은 하나 이상의 LAN 에있는 논리적으로 네트워크화 된 장치 그룹을 말하며 실제로 동일한 와이어에 연결되어 있는 것처럼 통신 할 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.

VLAN 구성 작업 목록

VLAN 추가 / 삭제

스위치 포트 구성

VLAN 인터페이스 생성 / 삭제

VLAN 의 구성 및 상태 모니터링

VLAN 구성 작업

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 전달 될 수 있습니다. 각 VLAN 은 물류 네트워크입니다. 데이터가 다른 VLAN 에 도달하려면 라우터 또는 브리지에 의해 전달되어야 합니다.

다음 명령을 실행하여 VLAN 을 구성 합니다.

운영...	설명
vlan vlan-id	VLAN 구성 모드로 들어갑니다.
name str	vlan 구성 모드의 이름.
Exit	vlan 구성 모드를 종료하고 vlan 을 구성 합니다.

vlan vlan-range	동시에 여러 VLAN 을 구성 합니다.
no vlan vlan-id | vlan-range	하나 이상의 VLAN 을 삭제하십시오.

Vlan 은 VLAN 관리 프로토콜 GVRP 를 통해 동적 추가 및 삭제를 수행 할 수 있습니다.

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 프레임만 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 수신 된 vlan 태그가없는 모든 데이터는 vlan 의 데이터 패킷에 속합니다.

트렁크 모드는 포트를 여러 VLAN 으로 간주 할 수 있으며 전달할 패킷 종류와 포트에 전송 된 패킷에 태그가 있거나 태그가없는 패킷 수 및 포트가 속한 VLAN 목록을 구성 할 수 있습니다.

다음 명령을 실행하여 스위치 포트를 구성하십시오.

운영...	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 스위치는이 기능을 전역적으로 활성화 / 비활성화하는 기능 만 지원하며 다른 포트에 대해 다른 정책을 구성 할 수 없습니다.

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.

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

슈퍼 VLAN 인터페이스 구성

슈퍼 VLAN 기술은 다음과 같은 메커니즘을 제공합니다. 동일한 스위치를 실행하는 다른 VLAN 의 호스트를 동일한 IPv4 서브넷에 할당 할 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 소유 할 수 없습니다.

명령 줄을 통해 Super VLAN 인터페이스를 구성 할 수 있습니다. Super VLAN 인터페이스를 구성하는 절차는 다음과 같습니다 :

명령	기술
[no] interface supervlan *index*	인터페이스 구성 모드를 시작합니다. 지정된 수퍼 VLAN 인터페이스가 없으면 시스템에서 수퍼 VLAN 인터페이스를 만듭니다. **index** 는 슈퍼 VLAN 인터페이스의 색인입니다. 유효 값의 범위는 1 에서 32 사이입니다. **아니오** 는 슈퍼 VLAN 인터페이스를 삭제하는 것을 의미합니다.
[**no**] **subvlan** [*setstr*] [**add** *addstr*] [**remove** *remstr*]	Super VLAN 에서 SubVlan 을 구성합니다. 추가 된 하위 VLAN 은 관리 인터페이스를 소유 할 수 없습니다. 원래 상태에서는 Super VLAN 에 Sub VLAN 이 포함되지 않습니다. 매번 하나의 하위 명령 만 사용할 수 있습니다. **setstr** 은 Sub VLAN 목록을 구성하는 것을 의미합니다. 예를 들어 List 2,4-6 은 VLAN 2, 4, 5 및 6 을 나타냅니다. **add** 는 원래의 SubVLAN 목록에 VLAN 목록을 **추가** 하는 것을 의미합니다. **addstr** 은 위와 같은 형식의 문자열을 의미합니다. **제거** 는 원래의 SubVLAN 목록에서 VLAN 목록을 삭제 **하는** 것을 의미합니다. remstr 는 위와 같은 형식의 목록의 문자열입니다. SuperVLAN 에서 모든 SubVLAN 을 삭제할 수 **없습니다** . **어떤** 명령은 다른 하위 명령과 함께 사용되지 않습니다.

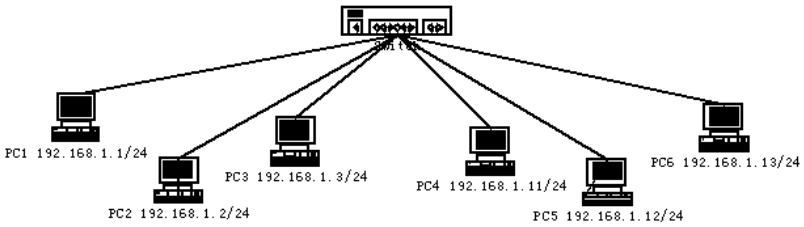
Super VLAN 인터페이스를 구성한 후 Super VLAN 인터페이스의 IP 주소를 구성 할 수 있습니다. Super VLAN 인터페이스는 다른 포트와 마찬가지로 구성 할 수있는 라우팅 포트이기도합니다.

VLAN 의 구성 및 상태 모니터링

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

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

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 관리 할 수 있습니다. 이렇게 하려면 포트 1 ~ 3 을 VLAN1 로, 포트 4 ~ 6 을 VLAN 으로 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
```

GVRP 구성

개요

GVRP (GARP VLAN 등록 프로토콜 GARP VLAN)는 802.1Q 트렁크 포트에서 IEEE 802.1Q 호환 VLAN 프루닝 및 동적 VLAN 생성을 제공하는 GARP (GARP VLAN 등록 프로토콜 GARP VLAN) 응용 프로그램입니다.

GVRP 를 사용하면 VLAN 구성 정보를 다른 GVRP 스위치와 교환하고 불필요한 브로드캐스트 및 알 수 없는 유니 캐스트 트래픽을 제거 할 수 있으며 802.1Q 트렁크 포트를 통해 연결된 스위치에서 VLAN 을 동적으로 만들고 관리 할 수 있습니다.

작업 목록 구성

GVRP 구성 작업 목록

GVRP 전역 활성화 / 비활성화

인터페이스에서 GVRP 활성화 / 비활성화

GVRP 모니터링 및 유지 보수

GVRP 구성 작업

전역 적으로 GVRP 활성화 / 비활성화

전역 구성 모드에서 다음 구성을 수행하십시오.

명령	기술
[no] gvrp	전역 적으로 GVRP 를 활성화 / 비활성화합니다.

기본적으로 사용하지 않도록 구성되어 있습니다.

인터페이스에서 GVRP 활성화 / 비활성화

인터페이스 구성 모드에서 다음 구성을 수행하십시오.

명령	기술
[no] gvrp	인터페이스 GVRP 를 활성화 / 비활성화합니다.

포트가 활성 GVRP 참가자가 되려면 먼저 GVRP 를 전역 적으로 활성화해야하며 포트는 802.1Q 트렁크 포트 여야합니다.

기본적으로 사용하도록 구성되어 있습니다.

GVRP 모니터링 및 유지 보수

EXEC 모드에서 다음 작업을 수행하십시오.

명령	기술
show gvrp statistics [**interface** port_list]	GVRP 통계를 표시합니다.
show gvrp status	GVRP 전역 상태 정보를 표시합니다.
[**no**] **debug gvrp** [**packet** | **event**]	GVRP 데이터 패킷 및 이벤트 디버그 스위치를 활성화 / 비활성화합니다. 콘크리트 스위치를 지정하지 않으면 모든 디버그 스위치가 활성화 / 비활성화됩니다.

GVRP 통계 표시 :

switch#show gvrp statistics interface Tthernet0/1

GVRP statistics on port Ethernet0/1

GVRP Status: Enabled

GVRP Failed Registrations: 0

GVRP Last Pdu Origin: 0000.0000.0000

GVRP Registration Type: Normal

Display GVRP global state information:

switch#show gvrp status

gvrp is enabled!

구성 예

네트워크 연결은 다음과 같습니다. 스위치 A 와 스위치 B 의 VLAN 구성 정보를 동일하게

만들려면 스위치 A 와 스위치 B 에서 GVRP 를 활성화 할 수 있습니다. 구성은 다음과 같습니다.

(1) 스위치 A 가 스위치 B 에 연결하는 인터페이스 8 을 트렁크로 구성합니다.

Switch_config_g0/8# switchport mode trunk

(1) 스위치 A 의 전역 GVRP 활성화 :

Switch_config # gvrp

(2) 스위치 A 의 인터페이스 8 의 GVRP 를 활성화합니다.

Switch_config_g0 / 8 # gvrp

(3) 스위치 A 에 VLAN 10, VLAN 20 및 VLAN 30 구성

Switch_config # vlan 10

Switch_config # VLAN 20

Switch_config # vlan 30

(4) 스위치 A 가 스위치 B 와 트렁크를 연결하는 인터페이스 9 를 구성합니다.

Switch_config_g0/9# switchport mode trunk

(5) 스위치 B 의 전역 GVRP 활성화 :

Switch_config # gvrp

(6) 스위치 B 의 인터페이스 9 의 GVRP 활성화

Switch_config_g0 / 9 # gvrp

(7) 스위치 B 에서 VLAN 40, Vlan 50 및 Vlan60 구성

Switch_config # vlan 40

Switch_config # vlan 50

Switch_config # vlan 60

구성이 완료되면 스위치 A 와 스위치 B 에 VLAN 구성 정보가 각각 표시됩니다 (즉, 두 스위치의 VLAN10, VLAN20, VLAN30, VLAN40, VLAN50 및 VLAN60).

사설 VLAN

사설 VLAN 개요

사설 VLAN 은 ISP 가 직면 한 VLAN 애플리케이션 문제를 해결했습니다. ISP 가 각 사용자에게 VLAN 을 제공하면 4094 VLAN 의 각 장치가 ISP 의 지원을받는 사용자를 제한합니다.

사설 VLAN 의 사설 VLAN 유형 및 포트 유형

사설 VLAN 은 VLAN 의 L2 브로드 캐스트 도메인을 여러 하위 도메인으로 세분화합니다. 각 하위 도메인은 사설 VLAN 쌍 (기본 VLAN 및 보조 VLAN)으로 구성됩니다. 하나의 사설 VLAN 도메인은 여러 개의 사설 VLAN 쌍을 가질 수 있으며 각 사설 VLAN 쌍은 하위 도메인을 나타냅니다. 사설 VLAN 도메인에는 기본 VLAN 이 하나만 있고 모든 사설 VLAN 쌍은 동일한 기본 VLAN 을 공유합니다. 각 하위 도메인의 보조 VLAN ID 는 서로 다릅니다.

하나의 기본 VLAN 유형 보유

기본 VLAN : 무차별 포트와 관련이 있으며 사설 VLAN 에는 기본 VLAN 이 하나만 존재합니다. 기본 VLAN 의 각 포트는 기본 VLAN 의 구성원입니다.

두 개의 보조 VLAN 유형 보유

격리 된 VLAN : 동일한 격리 VLAN 의 두 포트 사이에서 계층 2 통신을 수행 할 수 없습니다. 또한 사설 VLAN 에는 격리 된 VLAN 이 하나뿐입니다. 격리 된 VLAN 은 기본 VLAN 과 관련되어야 합니다.

커뮤니티 VLAN : 동일한 VLAN 의 두 포트간에 레이어 2 통신을 수행 할 수 있지만 다른 커뮤니티 VLAN 의 포트와 통신하지 않습니다. 하나의 사설 VLAN 에는 여러 개의

커뮤니티 VLAN 이 포함될 수 있습니다. 커뮤니티 VLAN 은 기본 VLAN 과 관련되어야 합니다.

사설 VLAN 포트에서의 포트 유형

다방면 포트 : 기본 VLAN 에 속합니다. 동일한 사설 VLAN 에있는 보조 VLAN 의 격리 된 포트 및 커뮤니티 포트를 포함하여 다른 모든 포트와 통신 할 수 있습니다.

격리 포트 : 격리 VLAN 의 호스트 포트입니다. 동일한 사설 VLAN 에서 격리 된 포트는 무차별 포트를 제외한 다른 포트에서 완전히 분리 된 L2 이므로 분리 된 포트에서 수신 된 플로우는 무차별 포트에만 전달 될 수 있습니다.

커뮤니티 포트 : 커뮤니티 VLAN 의 호스트 포트입니다. 사설 VLAN 에서 동일한 커뮤니티 VLAN 의 커뮤니티 포트는 서로 또는 무차별 포트를 통해 L2 통신을 수행 할 수 있지만 다른 VLAN 의 커뮤니티 포트 및 격리 된 VLAN 의 격리 포트는 사용할 수 없습니다.

VLAN TAG 의 필드 수정

이 기능은 VLAN 태그의 VLAN ID 및 우선 순위를 수정하고 사설 VLAN 의 송신 패킷이 태그를 전송하는지 여부를 결정합니다.

사설 VLAN 구성 작업 목록

사설 VLAN 구성

사설 VLAN 도메인의 연결 구성

사설 VLAN 의 L2 포트를 호스트 포트로 구성

사설 VLAN 의 L2 포트를 무차별 포트로 구성

사설 VLAN 의 송신 패킷 관련 필드 수정

사설 VLAN 의 구성 정보 표시

사설 VLAN 구성 작업

사설 VLAN 피어가 적용되는 조건은 다음과 같습니다.

1. 기본 VLAN 보유
2. 보조 VLAN 보유
3. 기본 VLAN 과 보조 VLAN 간에 연결이 있음
4. 기본 VLAN 에 무차별 포트가 있음

사설 VLAN 구성

VLAN 을 사설 VLAN 으로 구성하려면 다음 명령을 사용하십시오.

명령	설명
vlan *vlan-id*	VLAN 모드로 들어갑니다.
private-vlan {primary|community|isolated}	사설 VLAN 의 기능을 구성합니다.
no private-vlan {primary|community|isolated}	사설 VLAN 의 기능을 삭제합니다.
show vlan private-vlan	사설 VLAN 구성을 표시합니다.
exit	VLAN 구성 모드를 종료합니다.

사설 VLAN 도메인의 결합 구성

다음 명령을 실행하여 기본 VLAN 과 보조 VLAN 을 연결하십시오.

명령	설명
vlan *vlan-id*	기본 VLAN 구성 모드로 들어갑니다.
private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	연결된 보조 VLAN 을 구성합니다.

no private-vlan association	현재 기본 VLAN 과 모든 보조 VLAN 사이의 모든 연결을 지 웁니다.
exit	VLAN 구성 모드를 종료합니다.

사설 VLAN 의 L2 포트를 호스트 포트로 구성

다음 명령을 실행하여 사설 VLAN 의 L2 포트를 호스트 포트로 구성하십시오.

명령	설명
Interface *interface*	인터페이스 구성 모드를 시작합니다.
switchport mode private-vlan host	레이어 2 포트를 호스트의 포트 모드로 구성합니다.
no switchport mode	L2 포트의 사설 VLAN 모드 구성을 삭제합니다.
switchport private-vlan host-association *p_vid s_vid*	L2 호스트 포트를 사설 VLAN 과 연결합니다.
no switchport private-vlan host-association	L2 호스트 포트와 사설 VLAN 간의 연결을 삭제합니다.
exit	인터페이스 구성 모드를 종료합니다.

사설 VLAN 의 L2 포트를 무작위 포트로 구성

다음 명령을 실행하여 사설 VLAN 의 L2 포트를 무차별 포트로 구성하십시오.

명령	설명
Interface *interface*	인터페이스 구성 모드를 시작합니다.
switchport mode private-vlan promiscuous	레이어 2 포트를 무차별 포트 모드로 구성합니다.
no switchport mode	L2 포트의 사설 VLAN 모드 구성을 삭제합니다.
switchport private-vlan mapping *p_vid{svlist | add svlist |* **remove** *svlist}*	L2 무차별 포트를 사설 VLAN 과 연결합니다.
no switchport private-vlan mapping	L2 무차별 포트와 사설 VLAN 간의 연결을 삭제합니다.
exit	인터페이스 구성 모드를 종료합니다.

사설 VLAN 에서 응답 패킷 관련 필드 수정

다음 명령을 실행하여 사설 VLAN 의 송신 패킷 관련 필드를 수정하십시오.

명령	설명
Interface *interface*	인터페이스 구성 모드를 시작합니다.
switchport private-vlan tag-pvid *vlan-id*	출력 패킷의 태그에 VLAN ID 필드를 구성합니다.
switchport private-vlan tag-pri *pri*	출력 패킷의 태그에 우선 순위 필드를 구성합니다.
[no] switchport private-vlan untagged	출력 패킷에 태그가 있는지 여부를 구성합니다.
exit	인터페이스 구성 모드를 종료합니다.

사설 VLAN 의 구성 정보 표시

전역, 인터페이스 또는 VLAN 구성 모드에서 다음 명령을 실행하여 사설 VLAN 및 L2 포트의 사설 VLAN 구성 정보를 표시합니다.

명령	설명
show vlan private-vlan	사설 VLAN 구성을 표시합니다.
show vlan private-vlan interface *interface*	사설 VLAN 의 L2 포트 구성을 표시합니다.

STP 구성

STP 개요

표준 스패닝 트리 프로토콜 (STP)은 IEEE 802.1D 표준을 기반으로합니다. 스위치 스택은 나머지 네트워크에 대한 단일 스패닝 트리 노드로 나타나며 모든 스택 멤버는 동일한 브리지 ID 를 사용합니다. 달리 명시하지 않는 한 스위치라는 용어는 독립 실행 형 스위치 및 스위치 스택을 나타냅니다.

STP 는 스패닝 트리 알고리즘을 사용하여 중복 연결된 네트워크의 스위치 하나를 스패닝 트리의 루트로 선택합니다. 이 알고리즘은 활성 토폴로지의 포트 역할에 따라 각 포트에 역할을 할당하여 스위치 된 레이어 2 네트워크를 통해 최상의 루프없는 경로를 계산합니다.

STP 는 네트워크의 루프를 방지하면서 경로 중복성을 제공하는 레이어 2 링크 관리 프로토콜입니다. 레이어 2 이더넷 네트워크가 제대로 작동하려면 두 스테이션 사이에 하나의 활성 경로 만 존재할 수 있습니다. 엔드 스테이션 간의 여러 활성 경로로 인해 네트워크에서 루프가 발생합니다. 네트워크에 루프가 있으면 엔드 스테이션에서 중복 메시지를 수신 할 수 있습니다. 또한 스위치는 여러 Layer 2 인터페이스에서 엔드 스테이션 MAC 주소를 학습 할 수 있습니다. 이러한 조건은 불안정한 네트워크를 초래합니다. 스패닝 트리 작업은 엔드 스테이션에서 투명하므로 단일 LAN 세그먼트 또는 여러 세그먼트의 스위치 LAN 에 연결되어 있는지 여부를 감지 할 수 없습니다.

> STP 는 스패닝 트리 알고리즘을 사용하여 중복 연결된 네트워크의 스위치 하나를 스패닝 트리의 루트로 선택합니다. 이 알고리즘은 활성 토폴로지의 포트 역할에 따라 각 포트에 역할을 할당하여 스위치 된 레이어 2 네트워크를 통해 최상의 루프 없는 경로를 계산합니다.

표준 스패닝 트리 프로토콜 (STP)은 IEEE 802.1D 에 정의되어 있습니다. 이는 하나의 회전 트리에 여러 브리지로 구성된 LAN 토폴로지를 단순화하여 네트워크 루프가 발생하지 않도록 하고 네트워크의 안정적인 작동을 보장합니다.

STP 및 해당 프로토콜의 알고리즘은 랜덤 브리징 LAN 을 간단한 연결을 사용하는 활성 토폴로지로 구성합니다. 활성 토폴로지에서 일부 브리징 포트는 프레임을 전달할 수 있습니다. 일부 포트는 정체 상태에 있고 프레임을 전송할 수 없습니다. 폭주 상태에 있는 포트는 활성 토폴로지에서 종결 될 수 있습니다. 장치가 비효율적이거나 네트워크에 추가되거나 네트워크에서 제거되면 포트가 전송 상태로 변경 될 수 있습니다.

STP 토폴로지에서 브리지는 루트로 볼 수 있습니다. 모든 LAN 섹션에서 브리징 포트는 네트워크 섹션의 데이터를 루트로 전달합니다. 포트는 네트워크 섹션의 지정된 포트로 표시됩니다. 포트가 있는 브리지는 LAN 의 지정된 브리지로 간주됩니다. 루트는 루트가 연결하는 모든 네트워크 섹션의 지정된 브리지입니다. 각 브리지의 포트에서 루트에 가장 가까운 포트는 브리지의 루트 포트입니다. 루트 포트 및 지정된 포트 (사용 가능한 경우) 만 전송 상태입니다. 다른 유형의 포트는 종료되지 않지만 루트 포트 또는 지정된 포트가 아닙니다. 우리는 이들 포트를 대기 포트라고 부릅니다.

다음 매개 변수는 안정화 된 활성 토폴로지의 구조를 결정합니다.

(1) 각 브리지의 식별자

(2) 각 포트의 경로 비용

(3) 브리지의 각 포트에 대한 포트 식별자

최상위 우선 순위 (식별자 값이 가장 작은 브리지)가 루트로 선택됩니다. 각 브리지의 포트에는 루트 경로 비용 , 즉 루트에서 브리지까지의 모든 포트의 경로 비용 합계 중

최소 속성 이 있습니다. 각 네트워크 세그먼트의 지정된 포트는 네트워크 세그먼트에 연결되며 최소 경로 비용을 갖는 포트를 나타냅니다.

스위치의 두 포트가 루프의 일부인 경우 스패닝 트리 포트 우선 순위 및 경로 비용 구성은 어떤 포트가 전달 상태에 있고 어떤 포트가 차단 상태에 있는지를 제어합니다. 스패닝 트리 포트 우선 순위 값은 네트워크 토폴로지의 포트 위치와 트래픽을 전달하는 위치를 나타냅니다. 경로 비용 값은 미디어 속도를 나타냅니다.

우리의 스위치 표준은 스패닝 트리 프로토콜 802.1D STP 와 802.1w RSTP 의 두 가지 모드를 지원합니다. 스위치의 일부 모델은 VLAN 및 MSTP 스패닝 트리 프로토콜에 따라 STP 모드를 배포하는 것을 지원합니다. 자세한 내용은 2 장의 'STP 모드 및 모델 표'를 참조하십시오.

이 장에서는 스위치가 지원하는 표준 스패닝 트리 프로토콜을 구성하는 방법에 대해 설명합니다.

노트 :

이 문서에서는 802.1D STP 및 802.1w RSTP 를 SSTP 및 RSTP 로 약칭합니다. SSTP 는 단일 스패닝 트리를 의미합니다.

SSTP 구성 작업 목록

STP 모드 선택

STP 비활성화 / 활성화

스위치 우선 순위 구성

Hello 시간 구성

최대 사용 시간 구성

전달 지연 시간 구성

포트 우선 순위 구성

경로 비용 구성

자동 지정 포트 구성

STP 상태 모니터링

SSTP 구성 작업

STP 모드 선택

다음 명령을 실행하여 STP 모드를 구성하십시오.

명령	설명
spanning-tree mode {sstp | rstp}	STP 구성을 선택합니다.

STP 비활성화 / 활성화

스패닝 트리는 기본적으로 사용하도록 구성되어 있습니다. 네트워크 토폴로지에 루프가 없다고 확신하는 경우에만 스패닝 트리를 비활성화하십시오.

스패닝 트리를 비활성화하려면 다음 단계를 수행하십시오.

명령	설명
no spanning-tree	STP 를 비활성화합니다.

스패닝 트리를 활성화하려면 다음 명령을 사용하십시오.

명령	설명
spanning-tree	기본 모드 STP (SSTP)를 사용합니다.
spanning-tree mode {**sstp** | **rstp**}	특정 모드 STP 를 사용합니다.

스위치 우선 순위 구성

스위치 우선 순위를 구성하고 스택의 독립형 스위치 또는 스위치가 루트 스위치로 선택 될 가능성을 높일 수 있습니다.

스위치 우선 순위를 구성하려면 다음 단계를 따르십시오 .

명령	설명
spanning-tree sstp priority *value*	sstp 우선 순위 값을 수정합니다.
no spanning-tree sstp priority	sstp 우선 순위를 기본값 (32768)으로 되돌립니다.

Hello 시간 구성하기

사용자는 Hello 시간을 변경하여 루트 스위치가 전송 한 STP 데이터 단위 사이의 간격을 구성 할 수 있습니다.

다음 명령을 사용하여 SSTP 의 Hello Time 을 구성합니다 .

명령	설명
spanning-tree sstp hello-time *value*	sstp Hello 시간을 구성합니다.
no spanning-tree sstp hello-time	sstp Hello 시간을 기본값 (4s)으로 되돌립니다.

최대 사용 시간 구성

sstp max age 를 사용하여 재구성을 시도하기 전에 스패닝 트리 구성 메시지를 수신하지 않고 스위치가 대기하는 시간 (초)을 구성합니다.

최대 에이징 시간을 구성하려면 다음 단계를 수행하십시오 .

명령	설명
spanning-tree sstp max-age *value*	sstp 최대 사용 시간을 구성합니다.
no spanning-tree sstp max-age	최대 수명 시간을 기본값 (20 초)으로 되돌립니다.

전달 지연 시간 구성

sstp 전달 지연을 구성하여 스패닝 트리 학습 및 수신 상태에서 전달 상태로 변경하기 전에 인터페이스가 대기하는 시간 (초)을 결정합니다.

sstp 전달 지연을 구성하려면 다음 명령을 사용하십시오 .

명령	설명
spanning-tree sstp forward-time	sstp 전달 시간을 구성합니다.
no spanning-tree sstp forward-time	전달 시간을 기본값 (15 초)으로 되돌립니다.

포트 우선 순위 구성

루프가 발생하면 스패닝 트리는 포워딩 상태로 만들 인터페이스를 선택할 때 포트 우선 순위를 사용합니다. 선택된 우선 순위의 인터페이스에 더 높은 우선 순위 값 (더 낮은 숫자 값)을 할당하고 마지막으로 선택한 우선 순위 값 (더 높은 수치)을 할당 할 수 있습니다. 모든 인터페이스의 우선 순위 값이 같으면 스패닝 트리는 가장 낮은 인터페이스 번호를 가진 인터페이스를 전달 상태로 만들고 다른 인터페이스를 차단합니다.

다음 단계에 따라 인터페이스의 포트 우선 순위를 구성하십시오 .

명령	설명
spanning-tree port-priority *value*	인터페이스의 포트 우선 순위를 구성합니다.
spanning-tree sstp port-priority *value*	sstp 포트 우선 순위를 수정합니다.
no spanning-tree sstp port-priority	포트 우선 순위를 기본값 (128)으로 되돌립니다.

경로 비용 구성

다음 단계에 따라 인터페이스 비용을 구성하십시오 .

명령	설명
spanning-tree cost *value*	인터페이스 비용을 구성합니다.
spanning-tree sstp cost *value*	sstp 경로 비용을 수정합니다.
no spanning-tree sstp cost	경로 비용을 기본값으로 되돌립니다.

자동 지정 포트 구성

. 이 기능은 라인 카드가 BPDU 를 자동으로 지정된 포트로 자동 전송하여 MSU 의 부하를 줄입니다.

자동 지정 포트 기능은 STP 모드에서 효과적입니다.

명령	설명
spanning-tree designated-auto	자동으로 지정된 포트 기능을 사용합니다.
no spanning-tree designated-auto	자동으로 지정된 포트 기능을 비활성화합니다.

STP 상태 모니터링

STP 구성 및 상태를 모니터링하려면 관리 모드에서 다음 명령을 사용하십시오.

명령	설명
show spanning-tree	활성 인터페이스에 대해서만 스패닝 트리 정보를 표시합니다.
show spanning-tree detail	인터페이스 정보에 대한 자세한 요약을 표시합니다.
show spanning-tree interface	지정된 인터페이스에 대한 스패닝 트리 정보를 표시합니다.

PVST 구성

개요

SSTP 모드에서 전체 네트워크에는 하나의 STP 엔티티만 있습니다. STP 의 스위치 포트 상태는 모든 VLAN 에서 상태를 결정합니다. 네트워크에 여러 VLAN 이있는 경우 단일 STP 와 네트워크 토폴로지를 분리하면 네트워크의 일부에서 통신 정체가 발생할 수 있습니다.

스위치는 일정한 수의 VLAN 에서 독립적 인 STP 를 실행하여 포트가 다른 VLAN 에서 다른 상태를 유지하며 VLAN 간에로드 균형이 유지되도록 합니다.

스위치는 최대 30 개의 VLAN 에서 독립적 인 STP 를 실행할 수 있습니다. 다른 VLAN 토폴로지는 STP 에 의해 제어되지 않습니다.

VLAN STP 구성 작업

전역 구성 모드에서 다음 명령을 실행하여 VLAN 의 SSTP 특성을 구성합니다.

명령	설명
spanning-tree mode pvst	VLAN 기반 STP 배포 모드를 시작합니다.
spanning-tree vlan *vlan-list*	지정된 VLAN 에 대해 STP 사례를 배포합니다. vlan-list : VLAN 목록 스위치는 최대 30 개의 VLAN 에 대해 STP 사례를 분배합니다.
no spanning-tree vlan *vlan-list*	지정된 VLAN 에서 STP 사례를 삭제합니다.
spanning-tree vlan *vlan-list* **priority** *value*	지정된 VLAN 에서 STP 에 대한 우선 순위를 구성합니다.
no spanning-tree *vlan-list* **priority**	VLAN 의 STP 우선 순위를 기본 구성으로 다시 시작합니다.
spanning-tree vlan *vlan-list* **forward-time** *value*	지정된 VLAN 에 대한 전달 지연을 구성 합니다.
no spanning-tree vlan *vlan-list* **forward-time**	지정된 VLAN 의 기본 구성으로의 전달 지연을 재개 합니다.

spanning-tree vlan *vlan-list* **max-age** *value*	지정된 VLAN 의 최대 사용 기간을 구성합니다.
no spanning-tree vlan *vlan-list* **max-age**	지정된 VLAN 의 최대 사용 기간을 기본 구성으로 재개합니다.
spanning-tree vlan *vlan-list* **hello-time** *value*	지정된 VLAN 에 대해 HELLO-TIME 을 구성합니다.
no spanning-tree vlan *vlan-list* **hello-time**	지정된 VLAN 의 HELLO-TIME 을 기본 구성으로 다시 시작합니다.

포트 구성 모드에서 다음 명령을 실행하여 포트 속성을 구성 합니다.

명령	설명
spanning-tree vlan *vlan-list* **cost**	포트에 대해 지정된 VLAN 의 경로 비용을 구성합니다.
no spanning-tree vlan *vlan-list* **cost**	포트에 대해 지정된 VLAN 의 기본 경로 비용을 다시 시작합니다.
spanning-tree vlan *vlan-list* **port-priority**	VLAN 의 포트 우선 순위를 구성합니다.
no spanning-tree vlan *vlan-list* **port-priority**	VLAN 의 기본 포트 우선 순위를 다시 시작합니다.

모니터 또는 구성 모드에서 다음 명령을 실행하여 지정된 VLAN 의 STP 상태를 확인합니다.

명령	설명
show spanning-tree vlan *vlan-list*	VLAN 의 STP 상태를 확인하십시오.

RSTP 구성 작업 목록

스위치 RSTP 활성화/비활성화

스위치 우선 순위 구성

전달 지연 시간 구성

Hello 시간 구성하기

최대 age 구성

경로 비용 구성

포트 우선 순위 구성

RSTP 구성 작업

스위치 RSTP 활성화 / 비활성화

전역 구성 모드에서 다음 구성을 따르십시오.

명령	설명
spanning-tree mode rstp	RSTP 를 사용합니다.
no spanning-tree mode	STP 를 기본 모드 (SSTP)로 반환합니다.

스위치 우선 순위 구성

스위치 우선 순위를 구성하고 스택의 독립형 스위치 또는 스위치가 루트 스위치로 선택 될 가능성을 높일 수 있습니다.

스위치 우선 순위를 구성하려면 다음 단계를 따르십시오 .

전역 구성 모드에서 다음 구성을 따르십시오.

명령	설명
spanning-tree rstp priority *value*	rstp 우선 순위 값을 수정합니다.
no spanning-tree rstp priority	rstp 우선 순위를 기본값으로 되돌립니다.

참고 : 전체 스위치 네트워크에서 모든 브리지의 우선 순위가 동일한 값을 사용하면 가장 적은 MAC 주소를 가진 브리지가 루트 브리지로 선택됩니다. RSTP 프로토콜이 사용되는 상황에서 브리지 우선 순위 값이 수정되면 스패닝 트리를 다시 계산합니다.

브리지 우선 순위는 기본적으로 32768 로 구성됩니다.

전달 지연 시간 구성

링크 오류로 인해 네트워크가 스패닝 트리 구조를 다시 계산할 수 있습니다. 그러나 최신 구성 메시지는 전체 네트워크로 전달 될 수 없습니다. 새로 선택한 루트 포트와 지정된 포트가 즉시 데이터 전달을 시작하면 임시 경로 루프가 발생할 수 있습니다. 따라서 이 프로토콜은 일종의 국가 이주 메커니즘을 채택합니다. 루트 포트와 중간 포트가 데이터 전송을 시작하기 전에 중간 상태가 있고, 중간 상태가 전달 지연 시간을 지나면 전달 상태가 시작됩니다. 이 지연 시간은 새로 구성된 메시지가 전체 네트워크로 전달되도록 합니다. 브리지의 전달 지연 특성은 스위치 네트워크의 네트워크 직경과 관련됩니다. 일반적으로 네트워크 직경이 클수록 앞으로 지연 시간을 길게 구성해야 합니다.

전역 구성 모드에서 다음 구성을 따르십시오.

명령	설명
spanning-tree rstp forward-time *value*	전달 지연 구성
no spanning-tree rstp forward-time	전달 지연 시간을 기본값 (15 초)으로 되돌립니다.

참고 : 전달 지연 시간을 비교적 작은 값으로 구성하면 일시적인 경로가 더 길어질 수 있습니다. 전달 지연 시간을 비교적 큰 값으로 구성하면 시스템이 오랫동안 연결을 재개하지 못할 수 있습니다. 사용자가 기본값을 사용하는 것이 좋습니다.

브리지의 전달 지연 시간은 15 초입니다.

Hello 시간 구성하기

적절한 hello 시간 값을 사용하면 브릿지가 너무 많은 네트워크 리소스를 차지하지 않고도 네트워크의 링크 오류를 감지 할 수 있습니다.

전역 구성 모드에서 다음 구성을 따르십시오.

명령	설명
spanning-tree rstp hello-time *value*	Hello 시간 구성
no spanning-tree rstp hello-time	Hello 시간을 기본값으로 반환합니다.

참고 : 사용자는 기본값을 사용하는 것이 좋습니다.

기본 Hello 시간은 4 초입니다.

최대 age 구성

수명은 스위치가 재구성을 시도하기 전에 스패닝 트리 구성 메시지를 수신하지 않고 대기하는 시간 (초)입니다.

전역 구성 모드에서 다음 구성을 따르십시오 .

명령	설명
spanning-tree rstp max-age *value*	max-age 값을 구성합니다.
no spanning-tree rstp max-age	최대 수명 시간을 기본값 (20 초)으로 되돌립니다.

사용자가 기본값을 사용하는 것이 좋습니다. 참고 : 최대 수명을 비교적 작은 값으로 구성하면 스패닝 트리 계산이 상대적으로 빈번 해지며 시스템이 네트워크 블록을 링크 장애로 간주 할 수

있습니다. 최대 수명을 상대적으로 큰 값으로 구성하면 링크 상태가 시간에 눈에 띄지 않게됩니다.

브리지의 최대 수명은 기본적으로 20 초입니다.

경로 비용 구성

스패닝 트리 경로 비용 기본값은 인터페이스의 미디어 속도에서 파생됩니다. 루프가 발생하면 스패닝 트리는 전달 상태로 구성할 인터페이스를 선택할 때 비용을 사용합니다. 먼저 선택한 인터페이스에 낮은 비용 값을 할당하고 마지막으로 선택한 인터페이스에 높은 비용 값을 지정할 수 있습니다. 모든 인터페이스의 비용 값이 같으면 스패닝 트리는 가장 낮은 인터페이스 번호를 가진 인터페이스를 전달 상태로 만들고 다른 인터페이스를 차단합니다.

인터페이스 구성 모드에서 시작하여 다음 단계에 따라 인터페이스 비용을 구성합니다.

명령	설명
spanning-tree rstp cost *value*	인터페이스 비용을 구성합니다.
no spanning-tree rstp cost	경로 비용을 기본값으로 되돌립니다.

참고 : 이더넷 포트의 우선 순위를 수정하면 스패닝 트리가 다시 계산됩니다. 사용자는 기본값을 사용하고 RSTP 프로토콜이 현재 이더넷 인터페이스의 경로 비용을 계산하도록 할 것을 권장합니다.

포트 속도가 10Mbps 인 경우 이더넷 인터페이스의 경로 비용은 2000000 입니다.

포트 속도가 100Mbps 이면 이더넷 인터페이스의 경로 비용은 200000 입니다.

포트 우선 순위 구성

루프가 발생하면 스패닝 트리는 포워딩 상태로 만들 인터페이스를 선택할 때 포트 우선 순위를 사용합니다. 먼저 선택한 인터페이스에 높은 우선 순위 값 (낮은 수치 값)을 지정하고 마지막에 선택한 우선 순위 값 (높은 수치 값)을 지정할 수 있습니다. 모든 인터페이스의 우선 순위 값이 같으면 스패닝 트리는 가장 낮은 인터페이스 번호를 가진 인터페이스를 전달 상태로 만들고 다른 인터페이스를 차단합니다.

인터페이스 구성 모드에서 다음 구성을 따르십시오 .

명령	설명
spanning-tree rstp port-priority *value*	인터페이스의 포트 우선 순위를 구성합니다.
no spanning-tree rstp port-priority	포트 우선 순위를 기본값으로 되돌립니다.

참고 : 이더넷 인터페이스의 우선 순위를 수정하면 스패닝 트리가 다시 계산됩니다.

기본 이더넷 인터페이스 우선 순위는 128 입니다.

MTSP 구성

MSTP 개요

개요

MSTP (Multiple Spanning Tree Protocol)는 브리지 LAN 에서 간단한 완벽한 토폴로지를 만드는 데 사용됩니다. MSTP 는 이전 STP (Spanning Tree Protocol) 및 RSTP (Rapid Spanning Tree Protocol)와 호환 될 수 있습니다.

STP 와 RSTP 모두 단독 STP 토폴로지 만 만들 수 있습니다. 모든 VLAN 메시지는 유일한 STP 를 통해 전달됩니다. STP 는 너무 느리게 수렴하므로 RSTP 는 핸드 쉐이크 메커니즘을 통해 빠르고 안정적인 네트워크 토폴로지를 보장합니다.

MSTP 는 RSTP 의 신속한 핸드 셰이크 메커니즘을 상속합니다. 동시에 MST 는 다른 VLAN 을 다른 STP 에 배포하여 네트워크에 여러 토폴로지를 생성 할 수 있습니다. MSTP 에 의해 생성 된 네트워크에서 다른 VLAN 의 프레임을 다른 경로를 통해 전달할 수 있으므로 VLAN 데이터의 로드 균형을 실현할 수 있습니다.

VLAN 이 STP 를 배포하는 메커니즘과 달리 MSTP 는 여러 VLAN 을 하나의 STP 토폴로지에 분산시켜 많은 VLAN 을 지원하는 데 필요한 STP 를 효과적으로 줄입니다.

S2116, S2448, S3448 및 S6508 스위치는 MSTP 모드를 지원합니다. 자세한 내용은 장치 모델 및 관련 소프트웨어 버전 문서를 참조하십시오.

MST 도메인

MSTP 에서 VLAN 과 STP 간의 관계는 MSTP 구성 테이블을 통해 설명됩니다. MSTP 구성 테이블, 구성 이름 및 구성 편집 번호는 MST 구성 식별자를 구성합니다.

네트워크에서 동일한 MST 구성 식별자가 있는 상호 연결된 브리지는 동일한 MST 영역에서 고려됩니다. 동일한 MST 영역의 브리지는 항상 동일한 VLAN 구성을 가지므로 VLAN 프레임이 MST 영역에서 전송되도록 합니다.

IST, CST, CIST 및 MSTI

그림 2.1 은 3 개의 MST 영역과 802.1D STP 를 실행하는 스위치를 포함하는 MSTP 네트워크를 보여줍니다.

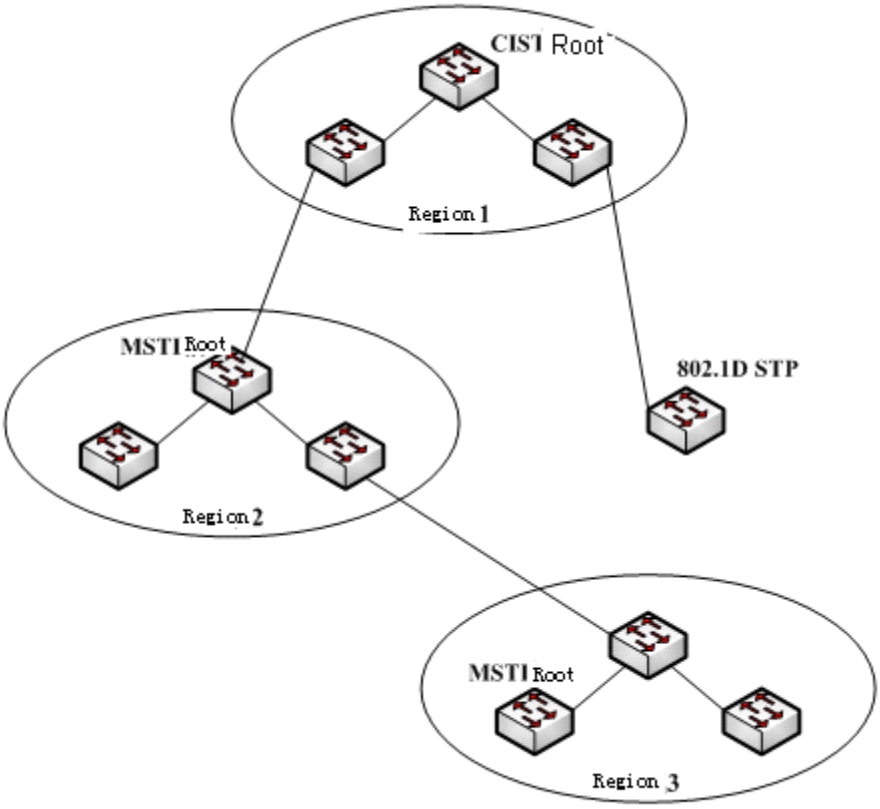


그림 2.1 MSTP 토폴로지

CIST

공통 및 내부 스패닝 트리 (CIST)는 모든 단일 스위치 및 상호 연결된 LAN 으로 구성된 스패닝 트리를 의미합니다. 이러한 스위치는 다른 MST 영역에 속할 수 있습니다. 전통적인 STP 또는 RSTP 를 실행하는 스위치 일 수 있습니다. MST 영역에서 STP 또는 RSTP 를 실행하는 스위치는 해당 지역에있는 것으로 간주됩니다.

네트워크 토폴로지가 안정된 후에 전체 CIST 가 CIST 루트 브리지를 선택합니다. 내부 CIST 루트 브리지는 각 영역에서 선택됩니다. 이 브리지는 영역의 핵심에서 CIST 루트까지의 최단 경로입니다.

CST

각 MST 영역을 단일 스위치로 보는 경우 CST (Common Spanning Tree)는 모든 "단일 스위치"를 연결하는 스패닝 트리입니다. 그림 2.1 에서 볼 수 있듯이 영역 1, 2 및 3 과 STP 스위치는 네트워크 CST 를 구성합니다.

IST

내부 스패닝 트리 (IST)는 MST 영역에있는 CIST 의 일부, 즉 IST 와 CST 가 CIST 를 구성하는 부분을 나타냅니다.

MSTI

MSTP 프로토콜을 통해 서로 다른 VLAN 을 다른 스패닝 트리에 분산시킬 수 있습니다. 그런 다음 여러 스패닝 트리 인스턴스가 생성됩니다. 일반적으로 No.0 스패닝 트리 인스턴스는 전체 네트워크로 확장 될 수있는 CIST 를 참조합니다. No.1 에서 시작하는 모든 스패닝 트리

인스턴스는 특정 영역에 있습니다. 각 스패닝 트리 인스턴스는 여러 VLAN 과 함께 분산 될 수 있습니다. 원래 상태에서는 모든 VLAN 이 CIST 에 분산되어 있습니다.

MST 영역의 MSTI 는 독립적입니다. 그들은 다른 스위치를 자신의 뿌리로 선택할 수 있습니다.

포트 역할

MSTP 의 포트는 RSTP 의 포트와 비슷한 다른 역할을 할 수 있습니다.

루트 포트

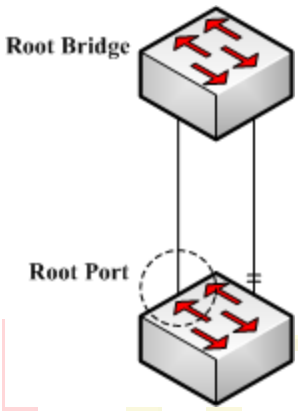


그림 2.2 루트 포트

루트 포트는 현재 스위치와 루트 브리지 사이의 경로를 나타내며 루트 경로 비용은 최소입니다.

대체 포트

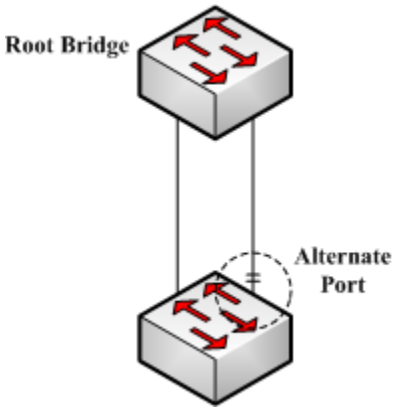


그림 2.3 대체 포트

대체 포트는 현재 스위치와 루트 브리지 사이의 백업 경로입니다. 루트 포트 연결이 유효하지 않으면 대체 포트는 작업 중단없이 새로운 루트 포트로 즉시 전환 할 수 있습니다.

지정 포트

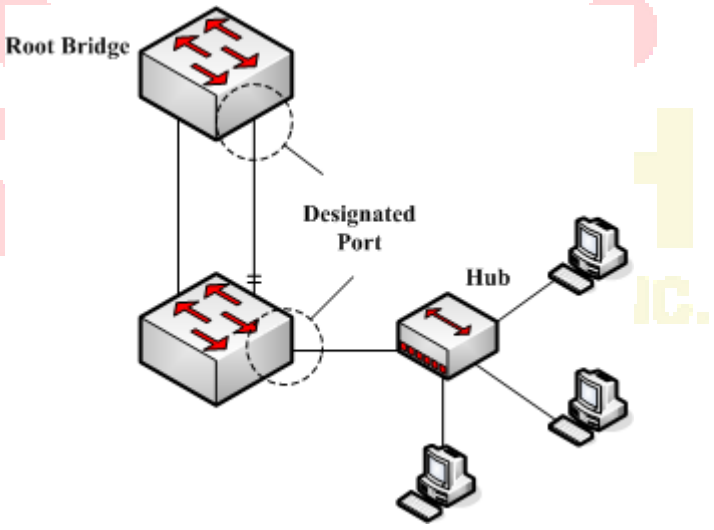


그림 2.4 지정된 포트

지정된 포트는 다음 지역의 스위치 또는 LAN 을 연결할 수 있습니다. 현재 LAN 과 루트 브리지 사이의 경로입니다.

백업 포트

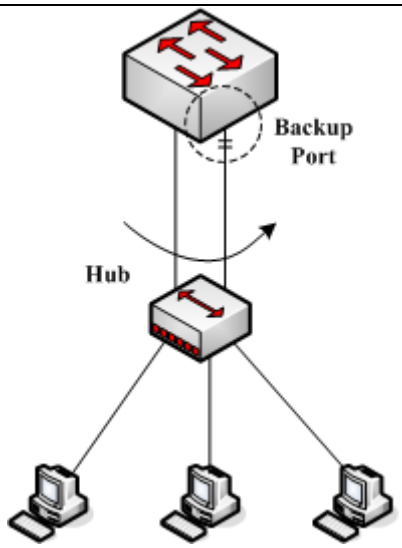


그림 2.5 백업 포트

2 개의 스위치 포트가 직접 연결되거나 둘 다 동일한 LAN 에 연결될 때 우선 순위가 낮은 포트가 백업 포트가되고 다른 포트는 지정된 포트가됩니다. 지정된 포트가 고장난 경우 백업 포트는 지정된 포트로 작동하여 작업을 계속합니다.

마스터 포트

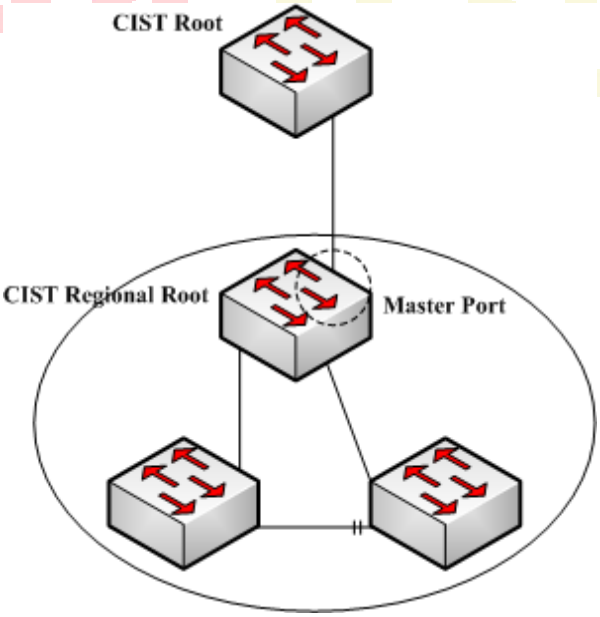


그림 2.6 마스터 포트

마스터 포트는 MST 영역과 CIST 루트 브리지 사이의 최단 경로입니다. 마스터 포트는 CIST 영역에서 루트 브리지의 루트 포트입니다.

경계 포트

CIST 의 경계 포트 개념은 각 MSTI 의 경계 포트와 약간 다릅니다. MSTI 에서 경계 포트의 역할은 스패닝 트리 인스턴스가 포트에서 확장되지 않는다는 것을 의미합니다.

에지 포트

RSTP 프로토콜 또는 MSTP 프로토콜에서 에지 포트는 네트워크 호스트에 직접 연결되는 포트를 의미합니다. 이 포트는 네트워크에서 루프를 유발하지 않고 직접 포워딩 상태로 들어갈 수 있습니다.

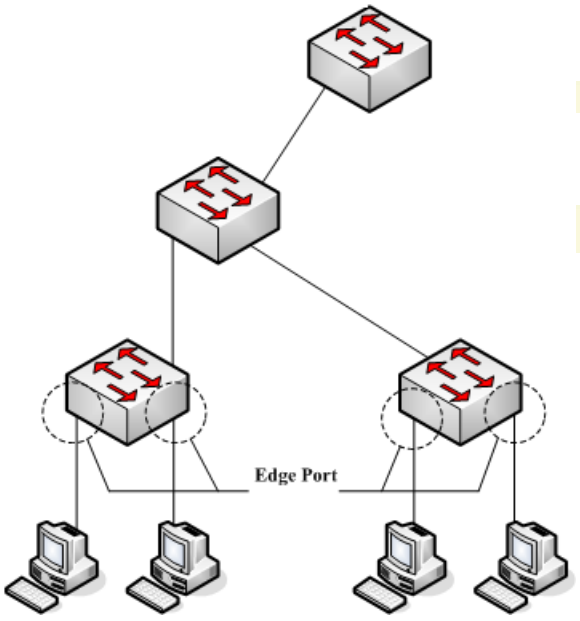


그림 2.7 에지 포트

원래 상태에서 MTSP 및 RSTP 는 모든 포트를 에지 포트로 사용하지 않으므로 네트워크 토폴로지를 신속하게 만들 수 있습니다. 이 경우 포트가 다른 스위치에서 BPDU 를 수신하면

포트가 에지 상태에서 정상 상태로 재개됩니다. 포트가 802.1D STP BPDU 를 수신하면 포트는 두 배의 전달 지연 시간을 기다린 다음 전달 상태로 들어갑니다.

MSTP BPDU

STP 및 RSTP 와 마찬가지로 MSTP 를 실행하는 스위치는 BPDU (Bridge Protocol Data Unit)를 통해 서로 통신 할 수 있습니다. CIST 및 MSTI 에 대한 모든 구성 정보는 BPDU 에서 전달할 수 있습니다. 표 2.1 과 표 2.2 는 MSTP 에서 사용하는 BPDU 의 구조를 나열합니다.

표 2.1 MSTP BPDU

분야 명	바이트 수
프로토콜 식별자	1 - 2
프로토콜 버전 식별자	3
BPDU 유형	4
CIST 플래그	5
CIST 루트 식별자	6 - 13
CIST 외부 루트 경로 비용	14 - 17
CIST 지역 루트 식별자	18 - 25
CIST 포트 식별자	26 - 27
메시지 시대	28 - 29
최대 age	30 - 31
안녕 시간	32 - 33
전달 지연	34 - 35
버전 1 길이	36
버전 3 길이	37 ~ 38
서식 선택기	39
구성 이름	40 - 71
개정	72 - 73
구성 다이제스트	74 - 89

CIST 내부 루트 경로 비용	90 - 93
CIST 브릿지 식별자	94 - 101
CIST 나머지 홉	102
MSTI 구성 메시지	103 ~

표 2.2 MST 구성 정보

분야 명	바이트 수
MSTI FLAGS	1
MSTI 지역 루트 식별자	2 - 9
MSTI 내부 루트 경로 비용	10 - 13
MSTI 브리지 우선 순위	14
MSTI 포트 우선 순위	15
MSTI 잔여 홉	16

안정된 상태

MSTP 스위치는 계산을 수행하고 수신 된 BPDU 에 따라 작업을 비교하고 마지막으로 다음을 보장합니다.

(1) 하나의 스위치가 전체 네트워크의 CIST 루트로 선택됩니다.

(2) 각 스위치 및 LAN 세그먼트는 CIST 루트에 대한 최소 비용 경로를 결정하여 완벽한 연결을 보장하고 루프를 방지 할 수 있습니다.

(3) 각 지역은 CIST 지역 루트로서 스위치를 가지고 있다. 스위치에는 CIST 루트에 대한 최소 비용 경로가 있습니다.

(4) 각 MSTI 는 스위치를 MSTI 지역 루트로 독립적으로 선택할 수 있습니다.

(5) 영역 및 LAN 세그먼트의 각 스위치는 MSTI 루트에 대한 최소 비용 경로를 결정할 수 있습니다.

(6) CIST 의 루트 포트는 CIST 지역 루트와 CIST 루트 사이의 최소 비용 경로를 제공합니다.

(7) CIST 의 지정 포트는 LAN 에 CIST 루트에 대한 최소 비용 경로를 제공했다.

(8) 대체 포트와 백업 포트는 스위치, 포트 또는 LAN 이 작동하지 않거나 제거 될 때 연결을 제공합니다.

(9) MSTI 루트 포트는 MSTI 지역 루트에 대한 최소 비용 경로를 제공합니다.

(10) MSTI 의 지정된 포트는 MSTI 지역 루트에 대한 최소 비용 경로를 제공합니다.

(11) 마스터 포트는 영역과 CIST 루트 간의 연결을 제공합니다. 이 영역에서 CIST 지역 루트의 CIST 루트 포트는 해당 지역의 모든 MSTI 의 마스터 포트로 작동합니다.

도약 횟수

STP 및 RSTP 와 달리 MSTP 프로토콜은 BPDU 구성 메시지에서 메시지 기간 및 최대 수명을 사용하여 네트워크 토폴로지를 계산하지 않습니다. MSTP 는 홉 수를 사용하여 네트워크 토폴로지를 계산합니다.

정보가 반복되는 것을 방지하기 위해 MSTP 는 전송 된 정보를 각 스패닝 트리의 홉 수 속성에 연결합니다. BPDU 에 대한 홉 수의 속성은 CIST 지역 루트 또는 MSTI 지역 루트에 의해 지정되고 각 수신 포트에서 감소합니다. 포트에서 홉 수가 0 이되면 정보가 삭제 된 다음 포트가 지정된 포트가 됩니다.

STP 호환성

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

참고 :

포트가 STP 호환 상태에 있으면 포트가 STP 메시지를 더 이상 수신하지 않더라도 포트는 자동으로 MSTP 상태로 재개되지 않습니다. 이 경우 **spanning-tree mstp migration-check** 를 실행 하여 포트가 학습 한 STP 메시지를 지우고 포트를 MSTP 상태로 되돌릴 수 있습니다.

RSTP 프로토콜을 실행하는 스위치는 MSTP 메시지를 식별하고 처리 할 수 있습니다. 따라서 MSTP 스위치는 RSTP 스위치와 작동 할 때 프로토콜 변환이 필요하지 않습니다.

MSTP 구성 작업 목록

기본 MSTP 구성

MSTP 활성화 및 비활성화

MSTP 영역 구성

네트워크 루트 구성

보조 루트 구성

브리지 우선 순위 구성

STP 의 시간 매개 변수 구성

네트워크 직경 구성

최대 홉 수 구성

포트 우선 순위 구성

포트의 경로 비용 구성

포트 연결 유형 구성

MST 호환 모드 활성화

MST 호환 모드 활성화

스위치가 지원하는 MSTP 프로토콜은 IEEE 802.1s 를 기반으로 합니다. 다른 MSTP, 특히 시스코 스위치가 지원하는 MSTP 와 호환되도록 MSTP 프로토콜은 MST 호환 모드에서 작동 할 수 있습니다. MSTP 호환 모드에서 실행중인 스위치는 다른 MSTP 의 메시지 구조를 식별하고 포함된 MST 지역 식별자를 확인하고 MST 영역을 구성할 수 있습니다.

MST 호환 모드 및 STP 호환 모드는 MSTP 프로토콜 변환 메커니즘을 기반으로 합니다. 스위치의 한 포트가 호환 모드에서 BPDU 를 수신하면 포트는 자동으로 모드로 변경되고 BPDU 를 호환 모드로 보냅니다. 포트를 표준 MST 모드로 다시 시작하려면 **spanning-tree mstp migration-check 를** 실행하면 됩니다.

전역 구성 모드에서 다음 명령을 실행하여 MST 호환 모드를 활성화하거나 비활성화합니다.

명령	설명
spanning-tree mstp mst-compatible	스위치에 대해 MST 호환 모드를 활성화합니다.
no spanning-tree mstp mst-compatible	스위치의 MST 호환 모드를 비활성화합니다.

노트 :

호환 모드의 주요 기능은 스위치 및 기타 MSTP 실행 스위치의 MST 영역을 만드는 것입니다. 실제 네트워킹에서는 스위치의 구성 이름과 편집 번호가 동일해야 합니다. 다른 MSTP 프로토콜을 실행하는 스위치를 CIST 루트에 구성하여 스위치가 메시지를 수신하여 호환 모드에 들어가는 지 확인하는 것이 좋습니다.

MST 호환 모드가 활성화되어 있지 않으면 스위치는 전체 BPDU 호환내용물을 해결하지 않고 내용물을 일반 RSTP BPDU 로 가져옵니다. 이 방법으로 스위치는 연결된 MST 호환 스위치와 같은 영역에 있을 수 없습니다.

호환 모드의 포트는 글로벌 구성 모드에서 호환 모드가 종료 된 경우에도 표준 MST BPDU 를 보내도록 자동으로 재개 할 수 없습니다. 이 경우 마이그레이션 검사를 실행하십시오.

프로토콜 변환 검사를 다시 시작하십시오.

MSTP 메시지를 확인하십시오.

MSTP 구성 작업

기본 MSTP 구성

속성	기본 구성
STP 모드	SSTP (PVST, RSTP 및 MSTP 가 시작되지 않음)
지역 이름	MAC 주소의 문자열
영역 편집 수준	0
MST 구성 목록	모든 VLAN 은 CIST (MST00)에 매핑됩니다.
스패닝 트리 우선 순위 (CIST 및 모든 MSTI)	32768
스패닝 트리 포트 우선 순위 (CIST 및 모든 MSTI)	128 자
스패닝 트리 포트 (CIST 및 모든 MSTI)의 경로 비용	1000Mbps : 20000 100Mbps : 200000 10Mbps : 2000000
안녕 시간	2 초
전달 지연	15 초
최대 노화 시간	20 초
최대 홉 수	20

MSTP 활성화 및 비활성화

STP 프로토콜은 기본적으로 PVST 또는 SSTP 모드에서 시작할 수 있습니다. 스패닝 트리가 필요하지 않을 때 실행을 중지 할 수 있습니다.

STP 를 MSTP 모드로 구성하려면 다음 명령을 실행하십시오.

명령	설명
spanning-tree	STP 를 기본 모드로 사용합니다.
spanning-tree mode mstp	MSTP 를 사용합니다.

STP 를 사용하지 않도록 구성하려면 다음 명령을 실행하십시오.

명령	설명
no spanning-tree	STP 를 비활성화합니다.

MST 영역 구성

스위치가 상주하는 MST 영역은 구성 이름, 편집 번호, VLAN 과 MSTI 간의 매핑 관계라는 세 가지 속성으로 결정됩니다. 영역 구성 명령을 통해 구성 할 수 있습니다. 세 가지 속성 중 하나를 변경하면 스위치가있는 영역이 변경됩니다. 원래 상태에서 MST 구성 이름은 스위치의 MAC 주소 문자열입니다. 편집 번호는 0 이고 모든 VLAN 은 CIST (MST00)에 매핑됩니다. 다른 스위치는 MAC 주소가 다르므로 MSTP 를 실행하는 스위치는 원래 상태의 다른 영역에 있습니다. spanning-tree mstp instance instance-id vlan vlan-list 를 실행하여 새 MSTI 를 만들고 지정된 VLAN 을 해당 VLAN 에 매핑 할 수 있습니다. MSTI 가 삭제되면 이러한 모든 VLAN 이 CIST 에 다시 매핑됩니다.

다음 명령을 실행하여 MST 영역 정보를 구성하십시오.

명령	설명
spanning-tree mstp name *string*	MST 구성 이름을 구성합니다.

	string 은 구성 이름의 **문자열을** 의미합니다. 최대 32 자까지 입력 할 수 있습니다. 기본값은 MAC 주소의 문자열입니다.
no spanning-tree mstp name	MST 구성 이름을 기본값으로 구성합니다.
spanning-tree mstp revision *value*	MST 편집 번호를 구성합니다. **value** 는 0 에서 65535 범위의 편집 번호를 나타냅니다. 기본값은 0 입니다.
no spanning-tree mstp revision	MST 편집 번호를 기본값으로 구성합니다.
spanning-tree mstp instance *instance-id* **vlan***vlan-list*	VLAN 을 MSTI 에 매핑합니다. **instance-id** 는 MSTI 를 의미하는 스패닝 트리의 인스턴스 번호를 나타냅니다. 1 부터 15 까지의 범위입니다. **vlan-list** 는 스패닝 트리에 매핑되는 VLAN 목록을 의미합니다. 1 에서 4094 범위입니다. **instance-id** 는 스패닝 트리 인스턴스를 나타내는 독립적인 값입니다. **vlan-list** 는 "1,2,3", "1-5"및 "1,2,5-10"과 같은 VLAN 그룹을 나타낼 수 있습니다.
no spanning-tree mstp instance *instance-id*	MSTI 의 VLAN 매핑을 취소하고 스패닝 트리 인스턴스를 비활성화합니다. instance-id 는 MSTI 를 의미하는 스패닝 트리의 인스턴스 번호를 나타냅니다. 1 부터 15 까지의 범위입니다.

다음 명령을 실행하여 MSTP 영역의 구성을 확인하십시오.

명령	설명
show spanning-tree mstp region	MSTP 영역의 구성을 표시합니다.

네트워크 루트 구성

MSTP 에서 각 스패닝 트리 인스턴스에는 우선 순위 값과 스위치의 MAC 주소가 포함된 브리지 ID 가 있습니다. 스패닝 트리 토폴로지를 구성하는 동안 상대적으로 작은 브리지 ID 를 가진 스위치가 네트워크 루트로 선택됩니다.

MSTP 는 구성을 통해 스위치를 네트워크 스위치로 구성할 수 있습니다. **spanning-tree mstp Spanning-tree mstp *instance-id* rootroot** 명령을 실행하여 스패닝 트리

인스턴스의 스위치 우선 순위 값을 기본 값에서 충분히 작은 값으로 수정하여 스위치가 스위치의 루트가되도록합니다. 스패닝 트리 인스턴스.

일반적으로 이전 명령이 실행 된 후 프로토콜은 현재 네트워크 루트의 브리지 ID 를 자동으로 확인한 다음 값 **24576** 이 현재 스위치가 스패닝 트리의 루트가되도록 보장 할 때 브리지 ID 의 우선 순위 필드를 **24576 으로** 구성합니다 .

네트워크 루트의 우선 순위 값이 **24576** 값보다 작 으면 MSTP 는 현재 브리지의 스패닝 트리 우선 순위를 루트의 우선 순위 값보다 4096 작은 값으로 자동 구성합니다. 숫자 **4096** 은 네트워크 우선 순위 값의 단계 길이입니다.

루트를 구성할 때 **직경** 부속 명령을 실행 하여 스패닝 트리 네트워크의 네트워크 지름을 지정할 수 있습니다 . 이 키워드는 스패닝 트리 인스턴스 ID 가 0 인 경우에만 유효합니다. 네트워크 직경이 구성된 후 MSTP 는 적절한 STP 시간 매개 변수를 자동으로 계산하여 네트워크 컨버전스의 안정성을 보장합니다. 시간 매개 변수에는 Hello 시간, 전달 지연 및 최대 수명이 포함됩니다. Hello-time 부속 명령을 사용하여 기본 구성을 대체 할 새로운 hello 시간을 구성할 수 있습니다.

스위치를 네트워크 루트로 구성하려면 다음 명령을 실행하십시오.

명령	설명
spanning-tree mstp *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	스위치를 지정된 스패닝 트리 인스턴스의 루트로 구성합니다. **instance-id** 는 0 - 15 범위의 스패닝 트리 인스턴스의 번호를 나타냅니다. **net-diameter** 는 선택적인 매개 변수 인 네트워크 **지름을** 나타냅니다. **instance-id** 가 0 일 때 효과적 입니다. 범위는 2 - 7 입니다. **seconds** 는 1 에서 10 까지의 hello 시간의 단위를 나타냅니다.
no spanning-tree mstp *instance-id* **root**	스패닝 트리에서 스위치의 루트 구성을 취소합니다.

	instance-id 는 0 에서 15 까지의 스패닝 트리 인스턴스의 번호를 의미합니다.

다음 명령을 실행하여 MSTP 메시지를 확인하십시오.

명령	설명
show spanning-tree mstp [**instance** *instance-id*]	MSTP 메시지를 확인합니다.

보조 루트 구성

네트워크 루트가 구성된 후에는 **spanning-tree mstp *instance-id* root secondary** 를 실행하여 하나 이상의 스위치를 보조 루트 또는 백업 루트로 구성할 수 있습니다. 특정 이유로 루트가 작동하지 않으면 2 차 루트가 네트워크 루트가됩니다.

기본 루트 구성과 달리 기본 루트 구성 명령이 실행 된 후 MSTP 는 스위치의 스패닝 트리 우선 순위를 **28672 로 구성** 합니다. 다른 스위치의 우선 순위 값이 기본값 **32768** 인 경우 현재 스위치는 2 차 루트가 될 수 있습니다.

보조 루트를 구성 할 때 부속 명령 인 **diameter** 및 **hello-time** 을 실행 하여 STP 시간 매개 변수를 업데이트 할 수 있습니다 . 2 차 루트가 1 차 루트가되어 작업을 시작하면이 모든 매개 변수가 작동하기 시작합니다.

스위치를 네트워크의 2 차 루트로 구성하려면 다음 명령을 실행하십시오.

명령	설명
spanning-tree mstp *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	스위치를 지정된 스패닝 트리 인스턴스의 보조 루트로 구성합니다. **instance-id** 는 0 - 15 범위의 스패닝 트리 인스턴스의 번호를 나타냅니다. **net-diameter** 는 선택적인 매개 변수 인 네트워크 **지름을** 나타냅니다. **instance-id** 가 0 일 때 효과적 입니다. 범위는 2 - 7 입니다.

	seconds 는 1 에서 10 까지의 hello 시간의 단위를 나타냅니다.
no spanning-tree mstp *instance-id* **root**	스패닝 트리에서 스위치의 루트 구성을 취소합니다. **instance-id** 는 0 에서 15 까지의 스패닝 트리 인스턴스의 번호를 의미합니다.

다음 명령을 실행하여 MSTP 메시지를 확인하십시오.

명령	설명
show spanning-tree mstp [**instance** *instance-id*]	MST 인스턴스에 대한 메시지를 확인합니다.

브리지 우선 순위 구성

경우에 따라 브리지 우선 순위를 구성하여 스위치를 네트워크 루트로 직접 구성할 수 있습니다. 하위 명령 **루트** 를 실행하지 않고 스위치를 네트워크 루트로 구성할 수 있음을 의미합니다 . 스위치의 우선 순위 값은 각 스패닝 트리 인스턴스에서 독립적입니다. 따라서 스위치의 우선 순위를 독립적으로 구성할 수 있습니다.

다음 명령을 실행하여 스패닝 트리의 우선 순위를 구성하십시오.

명령	설명
spanning-tree mstp *instance-id* **priority** *value*	스위치의 우선 순위를 구성합니다. instance-id 는 0 - 15 범위의 스패닝 트리 인스턴스의 번호를 나타냅니다. **값** 은 브리지의 우선 순위를 나타냅니다. 다음 값 중 하나일 수 있습니다. 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
no spanning-tree mstp *instance-id* **priority**	스위치의 브리지 우선 순위를 기본값으로 다시 시작합니다. **instance-id** 는 0 에서 15 까지의 스패닝 트리 인스턴스의 번호를 의미합니다.

STP 시간 매개 변수 구성

다음은 STP 시간 매개 변수입니다.

헬로우 시간 :

스위치가 네트워크 루트로 작동 할 때 지정된 포트로 구성 메시지를 보내는 간격입니다.

전달 지연 :

STP 모드에서 **차단** 상태에서 **학습** 상태로, **포워딩** 상태로 변경 될 때 포트가 필요로하는 시간 .

최대 age :

스패닝 트리에 대한 구성 정보의 최대 활성 기간.

네트워크 토폴로지의 충격을 줄이려면 시간 매개 변수에 대한 다음 요구 사항을 충족해야합니다.

2 x (fwd_delay - 1.0)> = max_age

max_age> = (hello_time + 1) x 2

명령	설명
spanning-tree mstp hello-time *seconds*	**Hello 시간** 매개 변수를 구성합니다 . 매개 변수 **초** 는 **Hello 시간** 의 단위이며 1 - 10 초입니다. 기본값은 2 초입니다.
no spanning-tree mstp hello-time	**Hello 시간** 을 기본값으로 다시 시작 합니다.
spanning-tree mstp forward-time *seconds*	**전달 지연** 매개 변수를 구성합니다 . 매개 변수 **초** 는 4 ~ 30 초 범위 의 **전달 지연** 단위입니다. 기본값은 15 초입니다.
no spanning-tree mstp forward-time	**전달 지연** 을 기본값으로 다시 시작 합니다.
spanning-tree mstp max-age *seconds*	**Max Age** 매개 변수를 구성합니다 . 매개 변수 **초** 는 6 ~ 40 초 범위 의 **최대 수명** 단위입니다. 기본값은 20 초입니다.
no spanning-tree mstp max-age	**Max Age** 를 기본값으로 다시 시작 합니다.

시간 매개 변수의 올바른 수정을 보장하는 루트 또는 네트워크 직경을 구성하여 STP 시간 매개 변수를 수정하는 것이 좋습니다.

새로 구성된 시간 매개 변수는 이전 수식의 요구 사항을 준수하지 않아도 유효합니다. 구성을 수행 할 때 콘솔의 알림에 주의하십시오.

네트워크 지름 구성

네트워크 직경은 네트워크의 규모를 나타내는 네트워크의 두 호스트 사이의 최대 스위치 수를 나타냅니다.

spanning-tree mstp diameter *net-diameter* 명령을 실행하여 MSTP 네트워크 직경을 구성할 수 있습니다 . 매개 변수 **net-diameter** 는 CIST 에만 유효합니다. 구성 후 3 개의 STP 시간 매개 변수가 자동으로 비교적 우수한 값으로 업데이트됩니다.

다음 명령을 실행하여 **net-diameter** 를 구성하십시오 .

명령	설명
spanning-tree mstp diameter *net-diameter*	구성 **그물 직경** . 매개 변수 **net-diameter 의** 범위는 2 에서 7 사이입니다. 기본값은 7 입니다.
no spanning-tree mstp diameter	다시 시작 **그물 직경** 기본값으로합니다.

매개 변수 **net-diameter** 는 스위치의 독립 구성으로 저장되지 않습니다. 네트워크 직경을 구성하여 수정 한 경우에만 시간 매개 변수를 저장할 수 있습니다.

최대 홉 카운트 구성하기

다음 명령을 실행하여 최대 홉 수를 구성하십시오.

명령	설명
spanning-tree mstp max-hops *hop-count*	최대 홉을 구성합니다. **hop-count 의** 범위는 1 - 40 입니다. 기본값은 20 입니다.

no spanning-tree mstp *hop-count*	최대 홉 수를 기본값으로 다시 시작합니다.

포트 우선 순위 구성

스위치의 두 포트간에 루프가 발생하면 우선 순위가 높은 포트는 **전달** 상태가되고 우선 순위가 낮은 포트는 차단됩니다. 모든 포트의 우선 순위가 같으면 더 작은 포트 번호를 가진 포트가 먼저 **전달** 상태가됩니다.

포트 구성 모드에서 다음 명령을 실행하여 STP 포트의 우선 순위를 구성합니다.

명령	설명
spanning-tree mstp *instance-id* **port-priority***priority*	STP 포트의 우선 순위를 구성합니다. **instance-id** 는 0 - 15 범위의 스패닝 트리 인스턴스 번호를 나타냅니다. **우선 순위** 는 포트 우선 **순위를** 나타냅니다. 다음 값 중 하나 일 수 있습니다. 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240
spanning-tree port-priority *value*	모든 스패닝 트리 인스턴스에서 포트 우선 순위를 구성합니다. **value** 는 포트 우선 순위를 나타냅니다. 다음 값 중 하나 일 수 있습니다. 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240
no spanning-tree mstp *instance-id* **port-priority**	포트 우선 순위를 기본값으로 다시 시작합니다.
no spanning-tree port-priority	모든 스패닝 트리 인스턴스에서 포트 우선 순위를 기본값으로 다시 시작합니다.

다음 명령을 실행하여 MSTP 포트에 대한 정보를 확인하십시오 .

명령	설명
show spanning-tree mstp interface *interface-id*	MSTP 포트 정보를 확인하십시오. interface-id 는 포트 이름을 나타냅니다 (예 : "F0 / 1"및 "FastEtnernet0 / 3").

포트의 경로 비용 구성

MSTP 에서 포트의 경로 비용의 기본값은 연결 속도를 기반으로 합니다. 두 스위치간에 루프가 발생하면 경로 비용이 적은 포트가 전달 상태가 됩니다. 경로 비용이 적을수록 포트의 비율이 높아집니다. 모든 포트의 경로 비용이 같으면 더 작은 포트 번호를 가진 포트가 먼저 전달 상태가 됩니다.

포트 구성 모드에서 다음 명령을 실행하여 포트의 경로 비용을 구성합니다.

명령	설명
spanning-tree mstp *instance-id* **cost** *cost*	포트의 경로 비용을 구성합니다. **instance-id** 는 0 - 15 범위의 스패닝 트리 인스턴스 번호를 나타냅니다. **비용** 은 포트의 경로 비용을 나타내며, 범위는 1 에서 200000000 입니다.
spanning-tree cost *value*	모든 스패닝 트리 인스턴스에서 포트의 경로 비용을 구성합니다. **값** 은 포트의 경로 비용을 나타내며, 범위는 1 에서 200000000 입니다.
no spanning-tree mstp *instance-id* **cost**	포트의 경로 비용을 기본값으로 다시 시작합니다.
no spanning-tree cost	모든 스패닝 트리 인스턴스에서 포트의 경로 비용을 기본값으로 다시 시작합니다.

MST 호환 모드 활성화

스위치가 지원하는 MSTP 프로토콜은 IEEE 802.1s 를 기반으로 합니다. 다른 MSTP, 특히 시스코 스위치가 지원하는 MSTP 와 호환되도록 MSTP 프로토콜은 MST 호환 모드에서 작동 할 수 있습니다. MSTP 호환 모드에서 실행중인 스위치는 다른 MSTP 의 메시지 구조를 식별하고 포함 된 MST 지역 식별자를 확인하고 MST 영역을 구성할 수 있습니다.

MST 호환 모드 및 STP 호환 모드는 MSTP 프로토콜 변환 메커니즘을 기반으로합니다. 스위치의 한 포트가 호환 모드에서 BPDU 를 수신하면 포트는 자동으로 모드로 변경되고 BPDU 를 호환 모드로 보냅니다. 포트를 표준 MST 모드로 다시 시작하려면 **spanning-tree mstp migration-check 를** 실행하면 됩니다.

전역 구성 모드에서 다음 명령을 실행하여 MST 호환 모드를 사용하거나 사용하지 않도록 구성합니다.

명령	설명
spanning-tree mstp mst-compatible	스위치의 MST 호환 모드를 활성화하십시오.
no spanning-tree mstp mst-compatible	스위치의 MST 호환 모드를 비활성화하십시오.

노트 :

호환 모드의 주요 기능은 스위치 및 기타 MSTP 실행 스위치의 MST 영역을 만드는 것입니다. 실제 네트워킹에서는 스위치의 구성 이름과 편집 번호가 동일해야합니다. 다른 MSTP 프로토콜을 실행하는 스위치를 CIST 루트에 구성하여 스위치가 메시지를 수신하여 호환 모드에 들어가는 지 확인하는 것이 좋습니다.

MST 호환 모드가 활성화되어 있지 않으면 스위치는 전체 BPDU 호환 컨텐트를 해결하지 않고 컨텐트를 일반 RSTP BPDU 로 가져옵니다. 이 방법으로 스위치는 연결된 MST 호환 스위치와 같은 영역에있을 수 없습니다.

호환 모드의 포트는 글로벌 구성 모드에서 호환 모드가 종료 된 경우에도 표준 MST BPDU 를 보내도록 자동으로 재개 할 수 없습니다. 이 경우 **마이그레이션 검사를** 실행 **하십시오** .

프로토콜 전환 확인 다시 시작

MSTP 를 사용하면 스위치가 프로토콜 변환 메커니즘을 통해 기존의 STP 스위치와 함께 작동 할 수 있습니다. 스위치의 한 포트가 STP 구성 메시지를 수신하면 포트는 STP 메시지 만 전송합니다. 동시에, STP 정보를 수신하는 포트는 경계 포트로 간주됩니다.

참고 :

포트가 STP 호환 상태에 있으면 포트가 STP 메시지를 더 이상 수신하지 않더라도 포트는 자동으로 MSTP 상태로 재개되지 않습니다. 이 경우 **spanning-tree mstp migration-check** 를 실행 하여 포트가 학습 한 STP 메시지를 지우고 포트를 MSTP 상태로 되돌릴 수 있습니다.

RSTP 프로토콜을 실행하는 스위치는 MSTP 메시지를 식별하고 처리 할 수 있습니다. 따라서 MSTP 스위치는 RSTP 스위치와 작동 할 때 프로토콜 변환이 필요하지 않습니다.

전역 구성 모드에서 다음 명령을 실행하여 스위치의 모든 포트에서 감지되는 모든 STP 정보를 지 웁니다.

명령	설명
spanning-tree mstp migration-check	스위치의 모든 포트에서 감지되는 모든 STP 정보를 지 웁니다.

포트 구성 모드에서 다음 명령을 실행하여 포트에서 감지 한 STP 정보를 지 웁니다.

명령	설명
spanning-tree mstp migration-check	포트가 감지 한 STP 정보를 지 웁니다.

MSTP 정보 확인

monitor 명령, 글로벌 구성 명령 또는 포트 구성 명령에서 다음 명령을 실행하여 MSTP 에 대한 모든 정보를 확인합니다.

명령	설명
show spanning-tree	MSTP 정보를 확인합니다.

	(SSTP, PVST, RSTP 및 MSTP 에 대한 정보를 확인할 수 있음)
show spanning-tree detail	MSTP 정보의 세부 사항을 확인합니다. (SSTP, PVST, RSTP 및 MSTP 에 대한 정보를 확인할 수 있음))
show spanning-tree interface *interface-id*	STP 인터페이스 정보를 확인합니다. (SSTP, PVST, RSTP 및 MSTP 에 대한 정보를 확인할 수 있음))
show spanning-tree mstp	모든 MST 인스턴스를 검사합니다.
show spanning-tree mstp region	MST 영역 구성을 확인합니다.
show spanning-tree mstp instance *instance-id*	MST 인스턴스에 대한 정보를 확인합니다.
show spanning-tree mstp detail	MST 정보를 확인합니다.
show spanning-tree mstp interface *interface-id*	MST 포트 구성을 확인합니다.
show spanning-tree mstp protocol-migration	포트의 프로토콜 변환 상태를 확인합니다.

STP 선택적 특성 구성

STP 선택적 특성 개요

스위치의 스패닝 트리 프로토콜 모듈은 일곱 가지 추가 기능 (소위 옵션 기능)을 지원합니다. 이러한 기능은 기본적으로 구성되지 않습니다. 선택적 특성을 향한 다양한 스패닝 트리 프로토콜 모드의 지원되는 조건은 다음과 같습니다.

선택적 특성	단일 STP	PVST	RSTP	MSTP
포트 패스트	예	예	아니오	아니오
BPDU 가드	예	예	예	예
BPDU 필터	예	예	아니오	아니오
업 링크 패스트	예	예	아니오	아니오
백본 Fast	예	예	아니오	아니오
루트 가드	예	예	예	예
루프 가드	예	예	예	예

Port Fast

Port Fast 는 청취 및 학습 상태를 우회하여 액세스 또는 트렁크 포트로 구성된 인터페이스를 차단 상태에서 전달 상태로 즉시 전환합니다. 단일 워크 스테이션이나 서버에 연결된 인터페이스에서 Port Fast 를 사용하여 스패닝 트리가 수렴되는 것을 기다리지 않고 해당 장치가 네트워크에 즉시 연결될 수 있습니다.

단일 워크 스테이션 또는 서버에 연결된 인터페이스는 브리지 프로토콜 데이터 단위 (BPDU)를 수신하지 않아야합니다. Port Fast 가 활성화 된 인터페이스는 스위치가 다시 시작될 때 정상적인 스패닝 트리 상태 변경주기를 거칩니다.

Port Fast 는 인터페이스가 스패닝 트리를 수렴 할 때까지 기다려야하는 시간을 최소화하기 때문에 엔드 스테이션에 연결된 인터페이스에서만 사용할 수 있습니다. 다른 스위치에 연결하는 인터페이스에서 Port Fast 를 활성화하면 스패닝 트리 루프가 생길 수 있습니다.

spanning-tree portfast 인터페이스 구성 또는 spanning-tree portfast default 전역 구성 명령을 사용하여 기능을 활성화 할 수 있습니다.

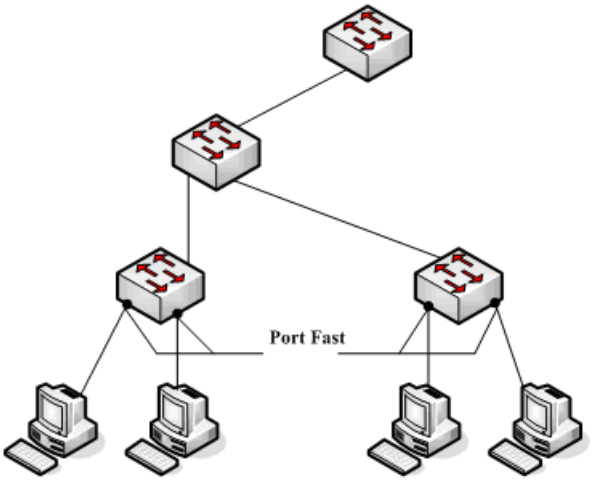


그림 1.1 Port Fast

조작법 :

신속한 컨버전스 스패닝 트리 프로토콜 인 RSTP 및 MSTP 의 경우 인터페이스를 즉시 전달 상태로 전환 할 수 있으므로 Port Fast 기능을 사용할 필요가 없습니다.

BPDU 감시

BPDU 보호 기능은 스위치에서 전역 적으로 활성화하거나 포트별로 활성화 할 수 있지만이 기능은 일부 차이점을 가지고 작동합니다.

전역 수준에서는 spanning-tree portfast bpduguard 기본 글로벌 구성 명령을 사용하여 PortFast 가 활성화 된 포트에서 BPDU 가드를 활성화합니다. 스패닝 트리는 BPDU 가 수신되면 포트 고속 작동 상태에 있는 포트를 종료합니다. 유효한 구성에서 PortFast 가 활성화 된 포트는 BPDU 를 수신하지 않습니다. portfast-enabled 포트에서 BPDU 수신은 장치의 연결과 같은 잘못된 구성을 의미하며 BPDU 보호 기능은 포트를 오류 비활성화 상태로 만듭니다. 이 경우 스위치는 위반이 발생한 전체 포트를 종료합니다.

포트가 종료되지 않도록 하려면 errdisable detect bpduguard shutdown VLAN 글로벌 구성 명령을 사용하여 위반이 발생한 포트에서 문제가 되는 VLAN 만 종료하십시오.

인터페이스 수준에서 포트 고속 기능을 활성화하지 않고 spanning-tree bpduguard enable 인터페이스 구성 명령 을 사용하여 모든 포트에서 BPDU 가드를 활성화 합니다. 포트가 BPDU 를 수신하면 오류 비활성화 상태가 됩니다.

BPDU 가드 기능은 수동으로 인터페이스를 다시 작동시켜야 하므로 유효하지 않은 구성에 대한 안전한 응답을 제공합니다. 액세스 포트가 스패닝 트리에 참여하는 것을 방지하려면 서비스 공급자 네트워크에서 BPDU 보호 기능을 사용하십시오.

BPDU 필터

BPDU 필터링 기능은 스위치에서 전역 적으로 활성화하거나 인터페이스별로 활성화 할 수 있지만 이 기능은 일부 차이점을 가지고 작동합니다.

SSTP / PVST 모드에서 BPDU 필터가 구성된 **포트 고속** 포트가 BPDU 를 수신하면 포트의 BPDU 필터 및 portfast 기능이 자동으로 비활성화되어 포트를 정상 포트로 다시 시작합니다. **전달** 상태로 들어가기 전에 포트는 **청취** 및 **학습** 상태여야 합니다 .

BPDU 필터 기능은 전역 구성 모드 또는 포트 구성 모드에서 구성 할 수 있습니다. 전역구성 모드에서 spanning-tree portfast bpdufilter 명령 **을** 실행하여 모든 포트에서 BPDU 를 보내지 않도록 차단합니다. 그러나 포트는 여전히 BPDU 를 수신하고 처리 할 수 있습니다.

업 링크 패스트

업 링크 패스트 기능을 사용하면 스위치와 루트 브리지 간의 연결이 끊어지면 새 루트 포트가 신속하게 전달 상태가 됩니다.

복잡한 네트워크에는 그림 1.2 와 같이 항상 여러 장치 계층이 있습니다. 스위치의 집계 레이어와 액세스 레이어는 모두 상위 레이어와 중복 연결됩니다. 이러한 중복 연결은 일반적으로 루프를 피하기 위해 STP 에 의해 차단됩니다.

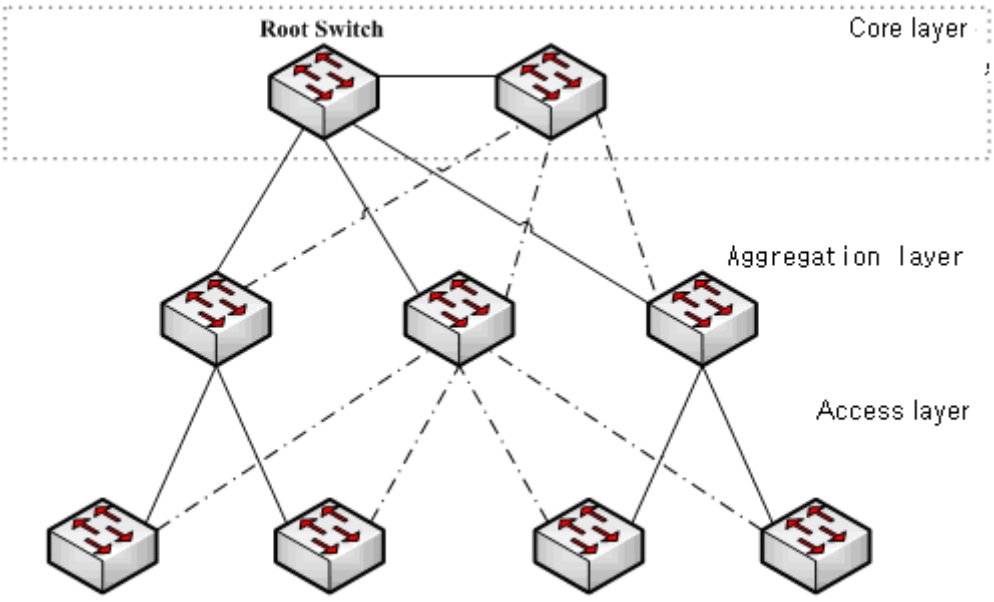


그림 1.2 스위칭 네트워크 토폴로지

스위치와 상위 계층 간의 연결이 끊긴 경우 (직접 링크 실패라고 함) STP 는 이중화 회선의 대체 포트를 루트 포트로 선택합니다. 전달 상태로 들어가기 전에 대체 포트는 청취 상태 및 학습 상태 여야합니다 . 전역 구성 모드에서 spanning-tree uplinkfast 명령을 실행 하여 Uplink Fast 기능을 구성 하면 새 루트 포트가 직접 포워딩 상태로 전환되어 스위치와 상위 계층 사이의 연결을 다시 시작할 수 있습니다.

그림 1.3 은 Uplink Fast 기능 의 작동 원리를 보여줍니다 . 스위치 B 를 연결하는 스위치 C 의 포트는 포트가 원래 상태 일 때 대기 포트입니다. 스위치 C 와 루트 스위치 A 사이의 연결이 끊어지면 이전 대체 포트가 새 루트 포트로 선택되고 즉시 전달이 시작됩니다.

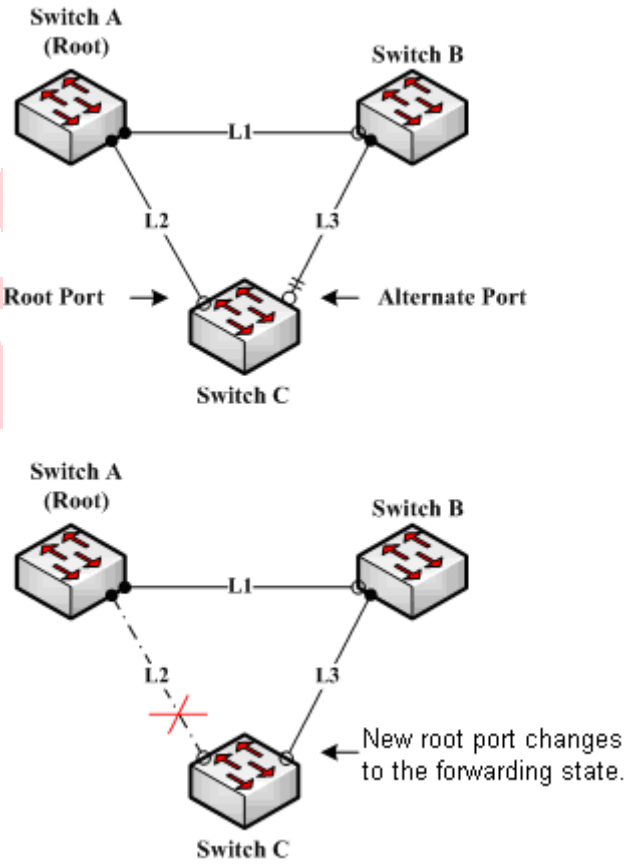


그림 1.3 Uplinkfast

노트 :

업 링크 fast 기능은 천천히 수렴 SSTP 및 PVST 로 조정합니다. RSTP 및 MSTP 모드에서 새 루트 포트는 Uplinkfast 기능 없이 신속하게 전달 상태가 됩니다.

BackboneFast

Backbonefast 은의 보충 업 링크 fast 기술. 링크 고속 그동안 기술을 용장 라인을 빠르게 지정된 스위치에 직접 접속이 끊어 경우 작동하게 백본 fast 기술은 상위 계층 네트워크의 간접 링크 네트워크 정전을 검출하고, 포트의 상태 변화를 밀어준다.

그림 1.3 에서 스위치 C 와 스위치 A 사이의 연결 L2 는 스위치 C 와 루트 스위치 A 간의 직접 링크라고 합니다. 연결이 끊어지면 Uplink Fast 기능으로 문제를 해결할 수 있습니다. 스위치 A 와 B 사이의 연결 L1 은 스위치 C 의 간접 링크로 불립니다. 연결 해제 된 간접 링크는 간접 장애로 불리며 간접 장애는 Backbone Fast 기능에 의해 처리됩니다 .

Backbone Fast 기능의 작동 원리는 그림 1.4 에 나와 있습니다.

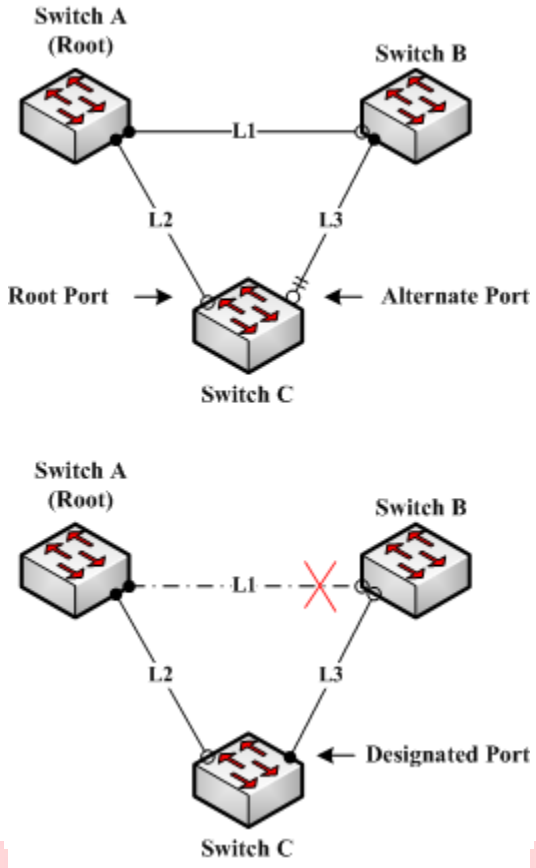


그림 1.4 백본 Fast

스위치 C 의 브리지 우선 순위가 스위치 B 의 우선 순위보다 높다고 가정합니다. L1 이 연결 해제되면 브리지 우선 순위가 루트 우선 순위로 사용되므로 스위치 B 가 BPDU 를 스위치 C 로 보내도록 선택됩니다. C 를 전환하기 위해 BPDU 에 포함 된 정보는 자체 정보가 포함되어 있지 않습니다. Backbone Fast 가 활성화되어 있지 않으면 스위치 C 와 스위치 B 사이의 포트는 브리지 정보를 기다리는 동안 시간이 경과 한 다음 지정된 포트가됩니다. 노화에는 일반적으로 몇 초가 걸립니다. **spanning-tree backbonefast** 명령을 실행하여 전역 구성 모드에서 기능을 구성한 후스위치 C 의 대체 포트가 우선 순위가 낮은 BPDU 를 수신하면 스위치 C 는 포트에서 간접 링크 및 루트 스위치에 연결할 수있는 연결이 끊어 졌다고 생각합니다. 그러면 스위치 C 는 에이징 정보를 기다리지 않고 포트를 지정된 포트로 즉시 업데이트합니다.

Backbone Fast 기능이 활성화 된 후 다른 포트에서 낮은 우선 순위의 BPDU 가 수신되면 스위치는 다른 동작을 수행합니다. 대체 포트가 메시지를 수신하면 포트는 지정된 포트로 업데이트됩니다. 루트 포트가 우선 순위가 낮은 메시지를 받고 다른 대기 포트가없는 경우 스위치는 루트 스위치가됩니다.

Backbone Fast 기능은 정보 수명의 시간을 생략합니다. 새로운 지정 포트는 여전히 상태 변경 순서 (수신 대기 상태, 학습 상태 및 최종 전달 상태)를 따라야합니다.

노트 :

Uplink Fast 와 유사하게 Backbone Fast 기능은 SSTP 및 PVST 모드에서 효과적입니다.

루트 가드

루트 가드 기능은 우선 순위가 높은 BPDU 를 수신하여 포트가 루트 포트로 변경되는 것을 방지합니다.

SP (서비스 공급자)의 Layer 2 네트워크에는 SP 가 소유하지 않은 스위치에 대한 많은 연결이 포함될 수 있습니다. 이러한 토폴로지에서 스패닝 트리는 그림 17-8 에서와 같이 루트 스위치로 고객 스위치를 선택하고 재구성 할 수 있습니다. 고객의 네트워크에있는 스위치에 연결된 SP 스위치 인터페이스에서 루트 가드를 활성화하면 이러한 상황을 피할 수 있습니다. 스패닝 트리 계산으로 인해 고객 네트워크의 인터페이스가 루트 포트로 선택되면 루트 가드가 인터페이스를 루트 불일치 (차단) 상태로 두어 고객의 스위치가 루트 스위치 또는 경로에 있지 않도록합니다 뿌리까지.

SP 네트워크 외부의 스위치가 루트 스위치가되면 인터페이스가 차단되고 (루트 불일치 상태) 스패닝 트리가 새 루트 스위치를 선택합니다. 고객의 스위치가 루트 스위치가 아니며 루트 경로에 있지 않습니다.

스위치가 여러 스패닝 트리 (MST) 모드에서 작동하는 경우 루트 가드는 인터페이스를 지정된 포트로 구성합니다. 루트 가드로 인해 경계 포트가 내부 스패닝 트리 (IST) 인스턴스에서 차단되는 경우 인터페이스는 모든 MST 인스턴스에서도 차단됩니다. 경계 포트는 지정된 스위치가 IEEE 802.1D 스위치이거나 다른 MST 영역 구성을 가진 스위치 인 LAN 에 연결하는 인터페이스입니다. 인터페이스에서 활성화 된 루트 가드는 인터페이스가 속한 모든 VLAN 에 적용됩니다. VLAN 은 그룹화되어 MST 인스턴스에 매핑 될 수 있습니다.

스패닝 트리 가드 루트 인터페이스 구성 명령을 사용하여이 기능을 활성화 할 수 있습니다.

참고 :

루트 가드 기능은 SSTP / PVST 및 RSTP / MSTP 에서 어떻게 든 다르게 작동합니다. SSTP / PVST 모드에서 루트 포트는 항상 루트 가드에 의해 차단됩니다. RSTP / MSTP 모드에서 상위 포트 BPDU 를 수신 할 때까지 루트 포트가 차단되지 않습니다. 이전에 루트 역할을 수행 한 포트는 차단되지 않습니다.

루프 가드

루프 가드를 사용하면 단방향 링크로 연결되는 장애로 인해 대체 포트 또는 루트 포트가 지정된 포트가되지 않도록 할 수 있습니다. 이 기능은 전체 스위치 네트워크에서 사용할 때 가장 효과적입니다. 루프 가드는 대체 및 루트 포트가 지정된 포트가되는 것을 방지하고 스패닝 트리는 루트 또는 대체 포트에서 BPDU 를 전송하지 않습니다.

spanning-tree loopguard 기본 글로벌 구성 명령을 사용하여이 기능을 활성화 할 수 있습니다.

스위치가 PVST + 또는 rapid-PVST + 모드에서 작동하는 경우 루프 보호는 대체 포트와 루트 포트가 지정된 포트가되는 것을 방지하며 스패닝 트리는 루트 또는 대체 포트에서 BPDU 를 전송하지 않습니다.

스위치가 MST 모드에서 작동하는 경우 모든 MST 인스턴스의 루프 가드가 인터페이스를 차단하는 경우에만 BPDU 가 비 경계 포트로 전송되지 않습니다. 경계 포트에서 루프 보호는 모든 MST 인스턴스의 인터페이스를 차단합니다.

참고 :

루프 가드 기능은 SSTP / PVST 및 RSTP / MSTP 에서 어떻게 든 다르게 작동합니다. SSTP / PVST 모드에서 지정된 포트는 항상 루프 가드에 의해 차단됩니다. RSTP / MSTP 모드에서는 BPDU 를 수신 할 수 없기 때문에 지정된 포트로 변경 될 때만 포트가 차단됩니다. 루프 가드는 하위 BPDU 수신으로 인해 지정된 역할과 함께 제공되는 포트를 차단하지 않습니다.

STP 선택적 특성 구성

STP 선택적 특성 구성 태스크

Port Fast 구성

BPDU Guard 구성

BPDU 필터 구성

Uplinkfast 구성

백본 Fast 구성

루트 가드 구성

루프 가드 구성

포트 고속 구성

PortFast 기능이 활성화 된 인터페이스는 표준 전달 지연을 기다리지 않고 직접 스패닝 트리 전달 상태로 이동합니다.

다음 명령을 사용하여 전역 구성 모드에서 portfast 기능을 구성합니다.

명령	설명
spanning-tree portfast default	전 세계적으로 포트 고속 기능을 지원합니다. 모든 인터페이스에 유효합니다.
no spanning-tree portfast default	전역 적으로 fast 포트 기능을 비활성화합니다. 인터페이스 구성에는 영향을 미치지 않습니다.

참고 :

portfast 기능은 호스트에 연결하는 인터페이스에만 적용됩니다. 포트 고속 기능이 전역으로 구성된 경우 BPDU Guard 또는 BPDU 필터를 동시에 구성해야 합니다.

인터페이스 구성 모드에서 portfast 기능을 구성하려면 다음 명령을 사용하십시오.

명령	설명
spanning-tree portfast	인터페이스에서 portfast 기능을 사용합니다.
no spanning-tree portfast	인터페이스의 portfast 기능을 비활성화합니다. 글로벌 구성에는 영향을 미치지 않습니다.

BPDU 보호 구성

portfast 사용 (포트가 고속 포트 작동) 상태 인 포트에서 BPDU 가드를 전역 적으로 활성화하면 스패닝 트리가 BPDU 를 수신하는 portfast 사용 포트를 종료합니다.

유효한 구성에서 PortFast 가 활성화 된 포트는 BPDU 를 수신하지 않습니다. portfast-enabled 포트에서 BPDU 수신은 권한이없는 장치의 연결과 같은 잘못된 구성을 의미하며 BPDU 보호

기능은 포트를 오류 비활성화 상태로 만듭니다. 이 경우 스위치는 위반이 발생한 전체 포트를 종료합니다.

포트가 종료되지 않도록 하려면 errdisable detect 원인 bpduguard shutdown vlan 전역 구성 명령을 사용하여 위반이 발생한 포트에서 문제가되는 VLAN 만 종료하십시오.

BPDU 보호 기능은 수동으로 포트를 다시 작동시켜야하므로 유효하지 않은 구성에 대한 안전한 응답을 제공합니다. 액세스 포트가 스패닝 트리에 참여하는 것을 방지하려면 서비스 공급자 네트워크에서 BPDU 보호 기능을 사용하십시오.

다음 단계에 따라 BPDU 보호 기능을 전역 적으로 활성화 하십시오 .

명령	설명
spanning-tree portfast bpduguard	전역 적으로 bpdu 보호 기능이 활성화됩니다. 모든 인터페이스에 유효합니다.
no spanning-tree portfast bpduguard	전역 적으로 bpdu 보호 기능이 비활성화됩니다.

조작법:

포트 고속 기능을 사용하면 브로드 캐스트가 폭주 할 수 있습니다. 보호를 위해 BPDU Guard 또는 BPDU 필터를 구성해야 합니다.

인터페이스 구성모드에서 BPDU 보호 기능을 활성화하려면 다음 단계를 수행하십시오.

명령	설명
spanning-tree bpduguard enable	인터페이스에서 bpdu 보호 기능을 사용합니다.
spanning-tree bpduguard disable	인터페이스에서 bpdu 보호 기능을 비활성화합니다. 글로벌 구성에는 영향을 미치지 않습니다.
no spanning-tree bpduguard	인터페이스에서 bpdu 보호 기능을 비활성화합니다. 글로벌 구성에는 영향을 미치지 않습니다.

BPDU 필터 구성

portfast 사용 가능 인터페이스에서 BPDU 필터링을 전역 적으로 활성화하면 포트 고속 작동 상태에 있는 인터페이스가 BPDU 를 보내거나 수신하지 못합니다. 스위치가 아웃 바운드 BPDU 를 필터링하기 전에 인터페이스가 링크업 될 경우 몇 개의 BPDU 를 보냅니다. 이러한 인터페이스에 연결된 호스트가 BPDU 를받지 못하도록 스위치에서 BPDU 필터링을 전역 적으로 활성화해야 합니다. portfast 사용 인터페이스에서 BPDU 를 수신하면 인터페이스는 portfast 작동 상태를 잃고 BPDU 필터링은 비활성화됩니다.

다음 단계에 따라 BPDU 필터 기능을 전역 적으로 활성화하십시오. :

명령	설명
spanning-tree portfast bpdufilter	전역 적으로 bpdu 필터 기능을 사용할 수 있습니다. 모든 인터페이스에 유효합니다.
no spanning-tree portfast bpdufilter	전역 적으로 bpdu 필터 기능이 비활성화됩니다.

조작법 :

포트 고속 기능을 사용하면 브로드 캐스트가 폭주 할 수 있습니다. 보호를 위해 BPDU Guard 또는 BPDU 필터를 구성해야 합니다.

인터페이스 구성 모드에서 BPDU 필터 기능을 활성화하려면 다음 단계를 수행하십시오 .

명령	설명
spanning-tree bpdufilter enable	인터페이스에서 bpdu 필터 기능을 사용합니다.
spanning-tree bpdufilter disable	bpdu 필터 기능을 사용하지 않습니다. 글로벌 구성에는 영향을 미치지 않습니다.
no spanning-tree bpdufilter	bpdu 필터 기능을 사용하지 않습니다. 글로벌 구성에는 영향을 미치지 않습니다.

업 링크 속도 구성

스위치의 연결이 끊어지면 스패닝 트리가 새 루트 포트를 선택하자 마자 대체 경로를 사용하기 시작합니다. spanning-tree uplinkfast 전역 구성 명령으로 UplinkFast 를 활성화하면 링크 또는

스위치가 실패하거나 스패닝 트리가 자동으로 재구성 될 때 새로운 루트 포트 선택을 가속화 할 수 있습니다. 루트 포트는 정상적인 스패닝 트리 절차 에서처럼 수신 및 학습 상태를 거치지 않고 즉시 전달 상태로 전환됩니다.

Uplinkfast 기능은 SSTP / PVST 모드에서만 유효합니다.

UplinkFast 를 전체적으로 활성화하려면 다음 단계를 수행하십시오. :

명령	설명
spanning-tree uplinkfast	업 링크 fast 기능을 사용합니다.
no spanning-tree uplinkfast	업 링크 fast 기능을 비활성화합니다.

백본 Fast 구성

BackboneFast 는 UplinkFast 기능에 대한 보완적인 기술로서 액세스 스위치에 직접 연결된 링크의 장애에 대응합니다. BackboneFast 는 스위치가 인터페이스에서 수신 한 프로토콜 정보를 저장하는 시간을 제어하는 최대 수명 타이머를 최적화합니다. 스위치가 다른 스위치의 지정된 포트에서 열악한 BPDU 를 수신하면 BPDU 는 다른 스위치가 루트에 대한 경로를 잃어 버렸을 수 있다는 신호이며 BackboneFast 는 루트에 대한 대체 경로를 찾습니다.

BackboneFast 는 SSTP / PVST 모드에서만 유효합니다.

BackboneFast 를 전역적으로 활성화하려면 다음 단계를 수행하십시오. :

명령	설명
spanning-tree backbonefast	Backbonefast 을 사용합니다.
no spanning-tree backbonefast	Backbonefast 을 비활성화합니다.

루트 가드 구성

인터페이스에서 활성화 된 루트 가드는 인터페이스가 속한 모든 VLAN 에 적용됩니다. UplinkFast 기능에서 인터페이스의 루트 가드를 사용하지 마십시오. UplinkFast 를 사용하면 실패한 경우

백업 포트가 차단 된 상태로 바뀝니다. 그러나 루트 가드도 활성화되어 있으면 UplinkFast 기능에서 사용하는 모든 백업 인터페이스가 루트가 일치하지 않는 상태 (차단됨)로 되어 전달 상태에 도달하지 못하게 됩니다.

루트 가드 기능은 SSTP / PVST 및 RSTP / MSTP 에서 어떻게 든 다르게 작동합니다. SSTP / PVST 모드에서 루트 포트는 항상 루트 가드에 의해 차단됩니다. RSTP / MSTP 모드에서 상위 포트 BPDU 를 수신 할 때까지 루트 포트가 차단되지 않습니다. 이전에 루트 역할을 수행 한 포트는 차단되지 않습니다.

인터페이스에서 루트 가드를 활성화하려면 다음 단계를 수행하십시오.:

명령	설명
spanning-tree guard root	인터페이스에서 루트 가드 기능을 활성화합니다.
no spanning-tree guard	인터페이스에서 루트 보호 및 루프 보호 기능을 비활성화합니다.
spanning-tree guard none	인터페이스에서 루트 보호 및 루프 보호 기능을 비활성화합니다.

루프 가드 구성

루프 가드를 사용하면 단방향 링크로 연결되는 장애로 인해 대체 포트 또는 루트 포트가 지정된 포트가 되지 않도록 할 수 있습니다. 이 기능은 전체 스위치 네트워크에서 구성 할 때 가장 효과적입니다. 루프 가드는 스패닝 트리에 의해 지점 간 (point-to-point)으로 간주되는 인터페이스에서만 작동합니다.

루프 가드 기능은 SSTP / PVST 에서 어떻게 든 다르게 작동합니다. SSTP / PVST 모드에서 지정된 포트는 항상 루프 가드에 의해 차단됩니다. RSTP / MSTP 에서 지정된 포트는 항상 루프 가드에 의해 차단됩니다. RSTP / MSTP 모드에서는 BPDU 를 수신 할 수 없기 때문에 지정된 포트로 변경

될 때만 포트가 차단됩니다. 하위 레벨의 BPDU 수신으로 인해 지정된 역할을 제공하는 포트는 루프 가드에 의해 차단되지 않습니다.

전역 구성 모드에서 루프 보호를 활성화하려면 다음 단계를 수행하십시오. :

명령	설명
spanning-tree loopguard default	전 세계적으로 루프 보호 기능을 사용할 수 있습니다. 모든 인터페이스에 유효합니다.
no spanning-tree loopguard default	루프 가드를 전역 적으로 비활성화합니다.

인터페이스 구성 모드에서 루프 가드를 활성화하려면 다음 단계를 수행하십시오. :

명령	설명
spanning-tree guard loop	인터페이스에서 루프 보호 기능을 활성화합니다.
no spanning-tree guard	인터페이스에서 루트 보호 및 루프 보호 기능을 비활성화합니다.
spanning-tree guard none	인터페이스에서 루트 가드 및 루프 가드를 비활성화합니다.

LACP

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 집합 된 물리적 포트에 분산됩니다.

포트 통합 구성 작업 목록

집합에 사용되는 논리 채널 구성

물리적 포트 집합

포트 집합 후 부하 균형 모드 선택

포트 집합의 구체적인 상태 모니터링

포트 집합 구성 작업 목록

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.

명령	설명
interface port-aggregator id	집합 된 논리 채널을 구성합니다.

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

집합 할 포트에 대한 선행 조건 :

포트의 링크를 올리고 포트를 전이중 모드로 협상해야 합니다.

모든 물리적 포트의 속도는 집합 프로세스 중에 동일해야합니다. 즉, 성공적으로 집합 된 물리적 포트가 하나있는 경우 두 번째 물리적 포트의 속도는 첫 번째 구성된 포트와 동일해야합니다. 또한 모든 물리적 포트의 VLAN 속성은 집합 된 포트와 동일해야합니다.

LACP 패킷은 다음 모드에서 포트간에 교환됩니다.

활성 - 포트를 활성 협상 상태로 전환합니다.이 상태에서 포트는 LACP 패킷을 보내 원격 포트와 협상을 시작합니다.

패시브 - 포트를 패시브 협상 상태로 전환합니다.이 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.

VALN 속성 : PVID, 트렁크 속성, VLAN 허용 범위 및 VLAN 비 태그 범위.

다음 명령을 사용하여 물리적 포트에서 집합을 수행하십시오.

명령	설명
aggregator-group *agg-id* **mode** { **lacp** | **static** }	물리적 포트의 집합 옵션을 구성합니다 .

포트 집합 후의 부하 균형 방법 선택

로드 공유 방법을 선택하여 모든 포트가 모든 물리적 포트를 모은 후에 데이터 트래픽을 공유 할 수 있도록 할 수 있습니다. 스위치는 최대 6 가지로드 밸런싱 정책을 제공 할 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.

명령	설명
aggregator-group load-balance	부하 분산 방법을 구성합니다.

노트 :

이 명령은 부하 분산 방법을 지원하지 않거나 하나의 방법 만 지원하는 스위치에서는 사용할 수 없습니다. 이 명령을 사용하는 스위치는 자체적으로 지원되는로드 균형 정책 만 선택합니다.

포트 집합의 구체적인 조건 모니터링

EXEC 모드에서 포트 집합 상태를 모니터링하려면 다음 명령을 사용하십시오.

명령	설명
show aggregator-group	포트 집합 상태를 표시합니다.

PDP

개요

PDP 는 네트워크 장비를 탐색하는 데 특히 사용됩니다. 즉 알려진 장치의 모든 이웃을 찾는 데 사용됩니다. PDP 를 통해 네트워크 관리 프로그램은 SNMP 를 사용하여 주변 장치에 쿼리하여 네트워크 토폴로지를 획득 할 수 있습니다.

우리 회사의 스위치는 인접 장치를 발견 할 수 있지만 SNMP 쿼리를 허용하지 않습니다. 따라서 스위치는 네트워크 끝에서만 실행되거나 완전한 네트워크 토폴로지를 얻을 수 없습니다.

PDP 는 모든 SNAP (예 : 이더넷)에 구성할 수 있습니다.

PDP 구성 작업

기본 PDP 구성

PDP 클럭 및 정보 저장 장치 구성

PDP 버전 구성하기

스위치에서 PDP 시작하기

포트에서 PDP 시작하기

PDP 모니터링 및 관리

기본 PDP 구성

기능	기본 구성
전역 구성 모드	이 기능은 기본적으로 활성화되어 있지 않습니다.
인터페이스 구성 모드	시작합니다.
PDP 클럭 (패킷 전송 주파수)	60 초

PDP 정보 저장 장치	180 초
PDP 버전	2

PDP 클록 및 정보 저장 장치 구성

PDP 패킷 전송 빈도 및 PDP 정보 저장 시간을 구성하려면 글로벌 구성 모드에서 다음 명령을 실행할 수 있습니다.

명령	**설명**
pdp timer *seconds*	PDP 패킷의 전송 빈도를 구성합니다.
pdp holdtime *seconds*	PDP 정보 저장 시간을 구성합니다.

PDP 버전 구성

PDP 버전을 구성하려면 글로벌 구성 모드에서 다음 명령을 실행하십시오.

명령	**설명**
pdp version {1|2}	PDP 버전을 구성합니다.

스위치에서 PDP 시작하기

PDP 를 사용하려면 전역 구성 모드에서 다음 명령을 실행하십시오.

명령	**설명**
pdp run	스위치에서 PDP 를 시작합니다.

포트에서 PDP 시작하기

기본적으로 포트에서 PDP 를 사용하려면 포트 구성 모드에서 다음 명령을 실행하십시오.

명령	**설명**
pdp enable	스위치의 포트에서 PDP 를 시작합니다.

PDP 모니터링 및 관리

PDP 를 모니터링하려면 EXEC 모드에서 다음 명령을 실행하십시오.

명령	**설명**
show pdp traffic	수신 및 전송 된 PDP 패킷의 수를 표시합니다.
show pdp neighbor [detail]	PDP 가 검색하는 이웃을 표시합니다.

PDP 구성 예

Example 1: Starting PDP

Switch_config# pdp run

Switch_config# int g0/1

Switch_config_g0/1#pdp enable

Example 2: Setting the PDP clock and information storage

Switch_config#pdp timer 30

Switch_config#pdp holdtime 90

Example 3: Setting the PDP version

Switch_config#pdp version 1

Example 4: Monitoring PDP

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 Fas0/1 169 Gig0/1 COMPANY, RISC R S

LLDP

LLDP 개요

802.1AB 의 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 구성 할 수 있습니다.

LLDP 는 관리 인력에게 정확한 네트워크 매핑, 트래픽 데이터 및 문제 감지 정보를 제공하는 유용한 관리 도구입니다.

LLDP 구성 작업 목록

- LLDP 활성화 또는 비활성화
- 대기시간구성
- 타이머구성하기
- 재시작구성
- 보낼 대상 tlv 구성
- 송수신모드구성

- 상대보기명령구성
- 삭제명령구성
- 디버깅명령구성

LLDP 구성 작업

LLDP 비활성화 / 활성화

LLDP 는 기본적으로 비활성화되어 있습니다. 실행하기 전에 LLDP 를 시작해야합니다.

LLDP 를 활성화하려면 전역 구성 모드에서 다음 명령을 실행하십시오.

명령	**설명**
lldp run	LLDP 를 실행합니다.

다음 명령을 실행하여 LLDP 를 비활성화하십시오.

명령	**설명**
no lldp run	LLDP 를 비활성화합니다.

유지 시간 구성

holdtime 수정을 통해 LLDP 메시지를 전송하는 시간 제한을 제어 할 수 있습니다 .

글로벌 구성 모드에서 다음 명령을 실행하여 LLDP 의 보류 시간 을 구성 합니다.

명령	**설명**
lldp holdtime *time*	LLDP 의 제한 시간을 구성합니다.
no lldp holdtime	시간 종료 시간을 기본값 인 120 초로 재개합니다.

타이머 구성

LLDP 의 타이머를 구성하여 메시지 전송을 위한 스위치 간격을 제어 할 수 있습니다.

LLDP 의 **타이머** 를 구성하려면 전역 구성 모드에서 다음 명령을 실행 하십시오 .

명령	**설명**
lldp timer *time*	LLDP 의 메시지 전송 간격을 구성합니다.
no lldp timer	기본 간격 즉, 30 초를 재개합니다.

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 구성 합니다.

명령	**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.

전송할 TLV 구성

LLDP 의 **tlv-select** 를 구성하여 보내야하는 TLV 를 선택할 수 있습니다 . 기본적으로 모든 TLV 가 전송됩니다.

LLDP 의 **tlv** 를 추가하거나 삭제하려면 전역 구성 모드에서 다음 명령을 실행하십시오 .

명령	**설명**
lldp tlv-select *tlv-type*	추가해야 할 Tlvs 또는 tlv 유형은 다음과 같습니다. 거시 환란 경영자 주소 포트 설명 포트 VLAN 시스템 기능 시스템 설명 시스템 이름
no lldp tlv-select *tlv-type*	삭제해야 할 Tlv 또는 tlv 유형은 다음과 같습니다. 거시 환란

	경영자 주소 포트 설명 포트 VLAN 시스템 기능 시스템 설명 시스템 이름

전송 또는 수신 모드 구성

LLDP 는 전송 전용, 수신 전용 및 전송 및 수신의 세 가지 모드로 작동 할 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.

명령	**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 불가능하게합니다.

표시 관련 명령 구성

Show 연관 명령을 실행하여 LLDP 모듈이 수신 한 이웃, 통계 또는 포트 상태에 대한 정보를 볼 수 있습니다.

EXEC 또는 전역 구성 모드에서 다음 명령을 실행합니다.

명령	**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 전송 된 통계 정보를 표시합니다.

삭제 명령 구성

EXEC 모드에서 다음 명령을 실행하여 수신 된 이웃 목록 및 모든 통계 정보를 삭제할 수 있습니다.

명령	**설명**
clear lldp counters	모든 통계 데이터를 삭제합니다.
clear lldp table	수신 된 모든 이웃 정보를 삭제합니다.

디버깅 명령 구성하기

LLDP 모듈을 쉽게 모니터링하려면 EXEC 모드에서 다음 명령을 실행하십시오.

명령	**설명**
debug lldp errors	LLDP 모듈에 대한 몇 가지 오류 정보를보고합니다.
debug lldp events	LLDP 모듈에 대한 몇 가지 특별 이벤트를보고합니다.
debug lldp packets	LLDP 모듈의 메시지 전송 이벤트를보고합니다.
debug lldp states	LLDP 포트의 상태에 대한 정보를보고합니다.

이더넷 자동보호절체(EAPS)

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 브로드캐스트스톰을 형성하는 것을 방지합니다. 링크가 끊어진 경우 프로토콜은 이전에 종료 된 링크를 즉시 다시 시작합니다. 이러한 방식으로, 링 네트워크들 사이의 노드들은 서로 통신 합니다.

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 재개 할 수 있습니다.

참고:

EAPS 는 스위치를 다수의 물리적 링의 노드로 구성하여 토폴로지를 구성 할 수 있도록 지원합니다.

EAPS 개념

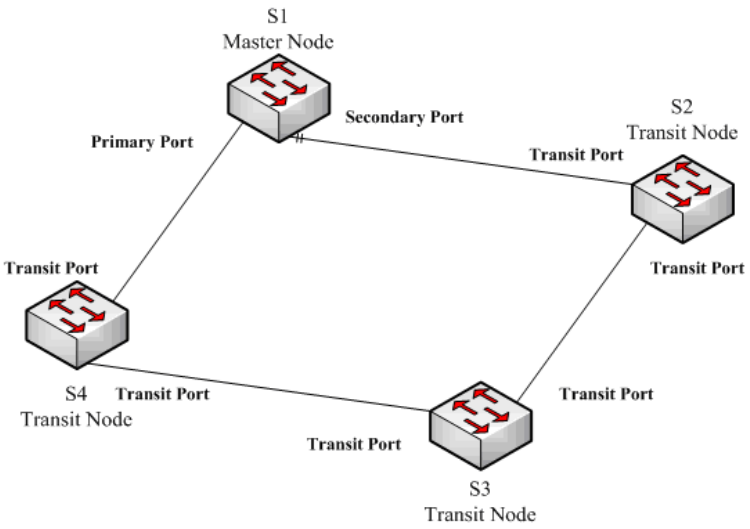


그림 1.1 EAPS 이더넷 링

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.

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 구성 할 수 있습니다. 마스터 노드는 기본 포트를 통해 링 감지 패킷을 전송합니다.

보조 포트 : 마스터 노드에서만 보조 포트를 구성 할 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 않도록합니다. 링 네트워크상의 링크가 인터럽트 된 후, 마스터 노드는 데이터 패킷을 포워딩하기 위해 제 2 포트를 열 것이다.

전송 포트 : 전송 포트는 전송 노드에서만 구성 할 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 구성 할 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.

참고:

스위치가 여러 개의 링에 속하도록 구성하려면 스위치가 다른 물리적 포트를 통해 다른 링을 연결해야 합니다.

제어 VLAN 및 데이터 VLAN

개인 제어 VLAN 은 마스터 노드와 중계 노드간에 사용되어 프로토콜 패킷을 전송합니다. 이 제어 VLAN 은 사용자 구성을 통해 지정되며 링의 포트는 사용자가 제어 VLAN 에 추가하므로 프로토콜 패킷이 정상적으로 전달 될 수 있습니다. 일반적으로 링 네트워크의 각 포트는 제어 VLAN 에서 전달 상태에 있고 링 네트워크에 속하지 않은 포트는 제어 VLAN 패킷을 전달할 수 없습니다.

노트 :

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.

노트 :

데이터 VLAN 은 일반 L2 / L3 통신에 사용될 수 있습니다. 예를 들어 데이터 VLAN 에 해당하는 VLAN 포트를 구성하고 동적 라우팅 프로토콜을 구성 할 수 있습니다.

MAC 주소의 에이징

이더넷 링 보호 프로토콜은 토폴로지가 변경 될 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 제어 할 수 있습니다.

완전한 링 네트워크의 상태

마스터 노드와 중계 노드는 현재 링 네트워크가 상태 기호 "COMPLETE"를 통해 완료되었는지 여부를 표시 할 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.

EAPS 패킷의 종류

EAPS 패킷은 표 1.1 에서와 같이 다음 유형으로 분류 할 수 있습니다.

표 1.1 EAPS 패킷 유형

패킷 유형	**비고**
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 중단 된 후 마스터 노드가 전송하고 패킷은 중계 노드의 MAC 주소 에이징 테이블을 표시합니다.
RING-UP-FLUSH-FDB	링 네트워크가 중단 된 후 마스터 노드가 전송하고 패킷은 중계 노드의 MAC 주소 에이징 테이블을 표시합니다.

패스트 이더넷 링 보호 메커니즘

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 (구성 할 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 에이징하도록보고합니다.

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.

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 수신 한 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.

이동 노드의 링크 재시작

중계 포트가 재개 된 후에는 데이터 VLAN 패킷을 즉시 전송하지 않고 사전 전달 상태가됩니다. 프리 포워딩 상태의 중계 포트는 제어 VLAN 에서 제어 패킷 만 전송 및 수신합니다.

링 네트워크에서 유효하지 않은 중계 포트가 하나 뿐이며 포트가 프리 포워딩 상태가되면 마스터 노드의 보조 포트는 기본 포트에서 HEALTH 패킷을 다시 수신 할 수 있습니다. 이 경우 마스터 노드는 보조 포트의 데이터 VLAN 을 다시 차단하고 에이징 주소 테이블의 알림을 외부로 전송합니다. 프리 포워딩 상태의 중계 포트가있는 노드가 에이징 주소 테이블의 알림을 수신하면 노드는 먼저 전달 포트에 대한 사전 전달 포트를 수정 한 다음 로컬 MAC 주소 테이블을 에이징합니다.

중계 모드가 마스터 노드에서 에이징 주소 테이블 알림을받지 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.

이더넷 자동보호절체(EAPS) 구성

기본 EAPS 구성

노트 :

빠른 이더넷 자동보호절체 프로토콜은 STP 와 함께 구성할 수 없습니다.

STP 가 비활성화 된 후에 링 노드가 BPDU 를 전달하지 **못하게** 하려면 **spanning-tree bpdu-terminal** 을 실행하는 것이 좋습니다 . 그러면 폭풍이 발생합니다.

다음 표를 참조하십시오 :

표 2.1 이더넷 링 보호 프로토콜 및 STP 의 기본 구성.

스패닝 트리 프로토콜	**spanning-tree mode rstp**
Ethernet Automatic Protection Switching	구성이 없습니다.

구성 전 요구 사항

MEAPS 를 구성하기 전에 다음 항목을주의 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 수정 된 후에는 Fail-time 을 적절히 수정해야합니다.

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 감지 할 수 있습니다 상태. 마스터 노드에 구성된 Hello-time 이 중계 노드의 Fre-Forward-Time 보다 길면 루프백이 쉽게 생성되고 브로드 캐스트 스톰이 트리거됩니다.

물리적 인터페이스, 고속 이더넷 인터페이스, 기가비트 이더넷 인터페이스 및 집계 인터페이스는 모두 링의 인터페이스로 구성 될 수 있습니다. 링크 집합, 802.1X 또는 포트 보안이 실제 인터페이스에 이미 구성된 경우 물리적 인터페이스를 더 이상 링 인터페이스로 구성할 수 없습니다.

MEAPS 구성 작업

마스터 노드 구성

중계 노드 구성

링 포트 구성

링 보호 프로토콜의 상태 탐색

고속 이더넷 링 보호 구성

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. id : 인스턴스 ID
Switch_config_ring#control-vlan *vlan-id*	제어 VLAN 을 구성합니다. 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 전송할주기를 구성합니다. 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. 값 : 3 초에서 30 초 사이의 시간 값이고 기본값은 3 초입니다.
Switch_config_ring#exit	현재 구성을 저장하고 노드 구성 모드를 종료합니다.

이동 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. id : 인스턴스 ID
Switch_config_ring#control-vlan *vlan-id*	제어 VLAN 을 구성합니다. 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. 값 : 3 초에서 30 초 사이의 시간 값이고 기본값은 3 초입니다.
Switch_config_ring#exit	현재 구성을 저장하고 노드 구성 모드를 종료합니다.

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. intf-name : 인터페이스 이름을 나타냅니다.
Switch_config_intf#ether-ring *id* **{primary-port | secondary-port | transit-port }**	이더넷 링의 포트 유형을 구성합니다. 이더넷 링의 노드 ID
Switch_config_intf#exit	인터페이스 구성 모드를 종료합니다.

참고:

ID 값과 관련 없는 명령어를 넣은 경우 이더넷 링의 구성포트가 취소될 수 있습니다.

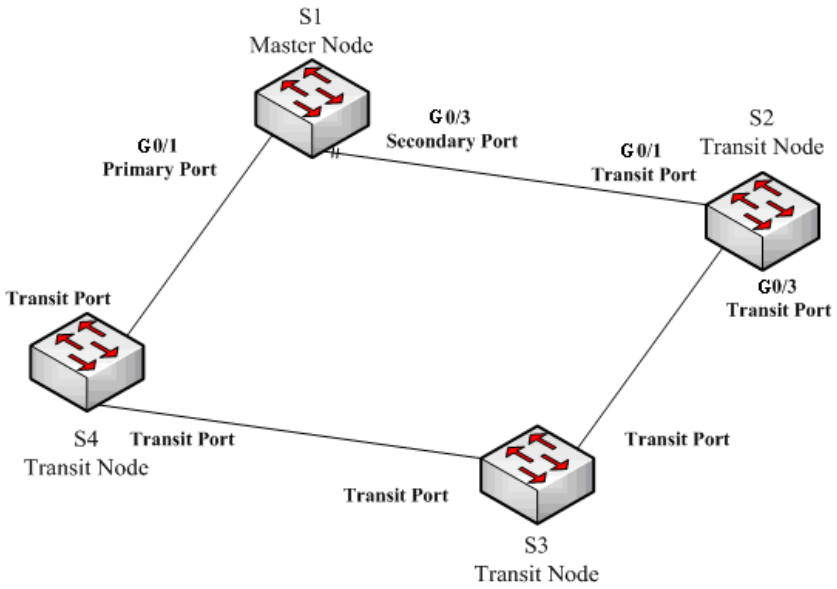
링 보호 프로토콜의 상태 탐색

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. 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.

MEAPS 구성

구성 예



MEAPS 구성

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
```

MEAPS

MEAPS 개요

EAPS 는 이더넷 링의 링크 레이어에 특별히 적용되는 프로토콜입니다. 이더넷 링이 완료되면 데이터 루프백에서 브로드캐스트 스톰이 발생하지 않도록 해야 합니다. 그러나 이더넷 링의 링크가 끊어지면 링에 있는 다른 노드의 통신을 재개하기 위해 백업 링크를 빠르게 활성화해야 합니다. 스위치의 역할은 구성을 통해 사용자가 지정합니다.

EAPS 는 단일 링 구조 만 지원하며 MEAPS 는 EAPS 를 기반으로 확장되므로 단일 링뿐만 아니라 레벨 2 다중 링 구조도 지원할 수 있습니다. 이후의 구조는 빠른 스위칭을 위해 이더넷 링을 통해 집계 장비로 구성된 중간의 집계 레이어와 액세스 장비로 연결된 외부 액세스 레이어로 구성됩니다. 서로 다른 레벨의 링이 접촉 또는 교차 모드를 통해 연결됩니다.

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 채택합니다. 따라서 링 네트워크에서 링 보호 프로토콜의 수렴은 STP 보다 우수합니다. 사운드 네트워크에서 링 보호 프로토콜은 50ms 이내에 네트워크 통신을 재개 할 수 있습니다.

MEAPS 의 기본 개념

도메인

도메인은 이더넷 루프백 보호 프로토콜의 보호 범위를 지정하며 정수로 구성된 ID 로 표시됩니다. 동일한 보호 데이터를 지원하고 동일한 제어 VLAN 을 가진 스위치 그룹은 서로 연결된 후에 도메인을 형성 할 수 있습니다. 하나의 도메인은 하나의 링 또는 서로 교차하는 다중 링을 포함 할 수 있습니다. 다음 그림을 참조하십시오.

하나의 MEAPS 도메인에는 MEAPS 링, 제어 VLAN, 마스터 노드, 중계 노드, 에지 노드 및 보조 에지 노드가 있습니다.

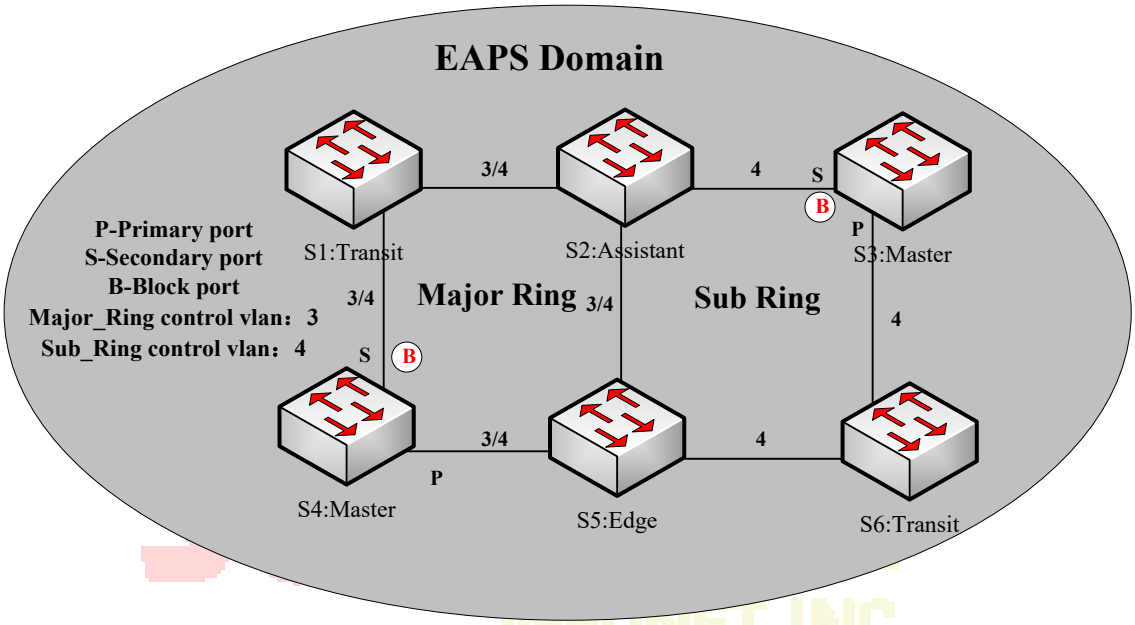


그림 1 간단한 MEAPS 모델

링

하나의 링은 물리적으로 링 이더넷 토폴로지에 해당하며, 이는 서로 링으로 연결된 스위치 그룹입니다. 하나의 MEAPS 도메인은 하나의 MEAPS 링 또는 서로 교차하는 다중 링을 포함 할 수 있습니다.

상위 링

도메인에 여러 개의 링이 포함되어 있는 경우 상위 링으로 하나의 링을 선택해야합니다. 상위 링의 각 노드의 기본 및 보조 포트는 주 제어 VLAN 과 하위 제어 VLAN 에 동시에 추가되어야 합니다. 다음 그림을 참조하십시오.

하위 링

도메인에 많은 링이 포함되어 있으면 상위 링을 제외한 포함 된 링을 하위 링이라고 합니다. 서브 링의 각 노드의 기본 및 보조 포트는 하위 제어 VLAN 에 추가되어야 합니다. 다음 그림을 참조하십시오.

제어 VLAN

제어 VLAN 은 데이터 VLAN 에 대한 개념이고 MEAPS 에서는 제어 VLAN 이 MEAPS 패킷을 전송하는 데 사용됩니다. 각 MEAPS 에는 주 제어 VLAN 과 보조 제어 VLAN 이라는 두 가지 제어 VLAN 이 있습니다.

상위 링 또는 하위 링을 구성 할 때 주 제어 VLAN 을 지정해야 합니다. 구성하는 동안 기본 제어 VLAN 을 지정하고 기본 제어 VLAN 의 ID 보다 1 이 큰 ID 인 VLAN 을 하위 제어 VLAN 으로 사용하면 됩니다. 상위 링은 기본 제어 VLAN 및 하위 제어 VLAN 에 동시에 추가되며 하위 링은 하위 제어 VLAN 에만 추가됩니다. 그림 1 의 각 포트 옆에 있는 3 번과 4 번을보십시오.

상위 링 프로토콜 패킷은 주 제어 VLAN 에서 전송되는 반면 하위 링 프로토콜 패킷은 보조 제어 VLAN 에서 전송됩니다. 상위 링의 하위 제어 VLAN 은 상위 링의 데이터

VLAN 입니다. 이더넷 링에 액세스하는 스위치의 포트는 제어 VLAN 에 속하며 이더넷 링에 액세스하는 포트만 제어 VLAN 에 추가 할 수 있습니다.

메모:

메이저 링의 MEAPS 포트는 주 제어 VLAN 과 하위 제어 VLAN 에 속해야 합니다. 하위 링의 MEAPS 포트는 하위 제어 VLAN 에만 속합니다. 상위 링은 서브 링의 논리적 노드로 간주되며 서브 링의 패킷은 메이저 링을 통해 투명하게 전송된다. 상위 링의 패킷은 상위 링에서만 전송됩니다.

데이터 VLAN

데이터 VLAN 은 데이터 패킷을 전송하는 데 사용됩니다. 데이터 VLAN 에는 MEAPS 포트와 비 MEAPS 포트가 포함될 수 있습니다. 각 도메인은 하나 이상의 데이터 VLAN 을 보호합니다. 도메인의 링 보호 프로토콜에 의해 계산 된 토폴로지는이 도메인의 데이터 VLAN 에만 유효합니다.

데이터 VLAN 이 생성되는지 여부는 MEAPS 포트가 MEAPS 모듈에 의해 제어되고 비 MEAPS 포트가 STP 모듈에 의해 제어되는 링 상태 시스템의 작업에 영향을 주지 않습니다.

메모:

MSTP 모듈과 유사한 처리 방법을 사용할 수 있습니다. 즉, 기본 STP 인스턴스의 포트 상태는 포트의 VLAN 구성과 상관없이 포트의 링크 상태에 따라 결정됩니다.

마스터 노드

마스터 노드는 정책 작성 및 링 제어 기능을 수행합니다. 각 링은 하나의 마스터 노드 만 소유해야 합니다. 마스터 노드는 링의 토폴로지가 완료되었는지, 루프백을 제거하는지, 다른 스위치를 제어하여 토폴로지 정보를 업데이트할지 여부를 알기 위해 적극적인 태도를 취합니다. 다음 그림을 참조하십시오. 여기서 S3 은 서브 링의 마스터 노드이고 S4 는 메이저 링의 마스터 노드입니다.

이동 노드

마스터 노드를 제외한 이더넷의 모든 스위치를 중계 노드라고 부를 수 있습니다. 중계 노드는 링의 로컬 포트 상태 만 확인하고 마스터 노드에 잘못된 링크를 알립니다. S1, S2, S5 및 S6 이 모두 중계 노드 인 다음 그림을 참조하십시오.

가장자리 노드와 보조 노드

서브 링과 메이저 링이 교차 할 때 두 개의 교차점이 있습니다. 두 개의 교차점이 하나의 에지 노드라고 하고 두 번째 스위치는 다른 노드의 보조 노드라고 합니다. 두 노드는 모두 서브 링의 노드입니다. 에지 노드 또는 보조 노드로 구성 될 스위치가 구성을 구분할 수 있는 경우 특별한 요구 사항은 없습니다. 그러나 그 중 하나는 에지 노드로 구성하고 다른 하나는 보조 노드로 구성되어야 합니다. 에지 노드 또는 보조 노드는 스위치가 서브 링을 담당하는 역할이지만 스위치는 상위 링에 있을 때 중계 노드 또는 마스터 노드 역할을 합니다. S2 가 보조 노드이고 S5 가 에지 노드 인 다음 그림을 참조하십시오.

기본 포트 및 보조 포트

마스터 노드가 이더넷 링에 액세스하는 두 개의 포트를 기본 포트 및 보조 포트라고 합니다. 두 포트의 역할은 클라이언트가 결정합니다.

기본 포트는 가동 중일 때 전달 상태에 있습니다. 이 기능은 마스터 노드에서 데이터 VLAN 의 패킷을 전달하고 제어 패킷을 수신하여 제어 VLAN 에 전달합니다. 마스터 노드는 루프백 탐지 패킷을 기본 포트에서 제어 VLAN 으로 전송합니다. 기본 포트의 링크가 유효하지 않은 상태에서 다시 시작되면 마스터 노드는 주소 에이징 알림을 제어 VLAN 에 즉시 보내고 기본 포트에서 루프백 탐지 패킷을 전송하기 시작합니다.

보조 포트는 작동 중일 때 전달 또는 차단 상태에 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.

메모:

포트는 노드의 기본 포트 또는 보조 포트로 구성할 수 있으며 기본 포트 및 보조 포트로 구성할 수 없습니다.

전송 포트 포트

중계 노드가 이더넷 링에 액세스하는 두 개의 포트는 모두 중계 포트입니다. 사용자는 구성을 통해 두 포트의 역할을 결정할 수 있습니다.

중계 포트가 작동 중일 때 전달 또는 프리 포워딩 상태입니다. 중계 포트는 제어 VLAN 에서 제어 패킷을 수신하고 이 패킷을 제어 VLAN 의 다른 포트로 전달합니다. 전송 포트가 유효하지 않은 상태에서 다시 시작되면 먼저 전달 전 상태가 되고 제어 패킷 만 수신 및 전달하고 데이터 VLAN 을 차단합니다. 중계 노드가 에이징 주소 테이블의 알림을 받으면 전달 상태가 됩니다.

메모:

포트는 노드의 기본 포트 또는 중계 포트로 구성할 수 있으며 재구성 할 수 없습니다.

일반적인 포트와 가장자리 포트

에지 노드와 보조 노드는 서브 링과 메이저 링이 교차하는 장소입니다. 이더넷에 액세스하는 두 개의 포트에 대해 하나는 공용 포트이며, 이는 보조 링과 상위 링의 공용 포트입니다. 다른 하나는 서브 링의 에지 포트입니다. 두 포트의 역할은 구성을 통해 사용자가 결정합니다.

공통 포트는 주 링 포트에 있으므로 주 링 포트의 상태에 따라 상태가 결정됩니다. 공용 포트 자체에는 아무 조작이나 알림도 없습니다. 공통 포트를 연결하는 링크가 변경되면 공통 포트가 있는 하위 링 노드는 통보되지 않습니다. 공통 포트의 존재는 링의 완전성을 보장합니다.

에지 노드의 에지 포트는 작동 중일 때 전달 또는 프리 포워드 상태에 있습니다. 기본 특성은 하나의 기능을 제외하고 전송 포트 포트의 특성과 일치합니다. 예외적 인 기능은 에지 포트가 올라가고 해당 메인 링 포트가 올라간 경우 메인 링 포트에서 에지 - 헬로 패킷을 전송하여 메이저 링의 완전성을 감지한다는 것입니다.

보조 노드의 에지 포트는 작동 중일 때 전달, 사전 전달 또는 EdgePreforwarding 상태에 있습니다. 중계 포트의 동일한 특성 외에도 하나 이상의 상태 인 EdgePreforwarding 상태가 있습니다. 에지 포트가 포워딩 상태이고 에지 포트가 대응하는 메인 링 포트가 에지 - Hello 패킷을 수신하지 않은 경우, 에지 포트의 상태는 EdgePreforwarding 상태로 변경되고, 제어를 수신하고 포워드한다. 패킷을 차단하고 해당 메인 링 포트가 Edge hello 패킷을 다시 수신 할 때까지 데이터 VLAN 을 차단합니다.

에지 노드와 보조 노드의 에지 포트는 상위 링의 완전성을 감지하는 데 도움이됩니다. 자세한 내용은 다음 장의 상위 링에 있는 하위 링 프로토콜 패킷의 채널 상태 검사 메커니즘을 참조하십시오.

메모:

각 포트는 노드의 유일한 에지 포트로 구성할 수 있으며 다시 구성 할 수 없습니다. 공용 포트는 상위 링의 포트에서만 지원 될 수 있으며 해당 주 링 포트가 없는 포트에는 구성 할 수 없습니다.

FLUSH MAC FDB

이더넷 링 보호 프로토콜은 토폴로지가 변경 될 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 제어 할 수 있습니다.

링의 완성 상태

마스터 노드와 중계 노드는 현재 링 네트워크가 상태 기호 "COMPLETE"를 통해 완료되었는지 여부를 표시 할 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 참이 될 수 있습니다.

링 네트워크의 상태 기호는 사용자가 현재 네트워크의 토폴로지 상태를 판단하는 데 도움이 됩니다.

EAPS 패킷의 종류

EAPS 패킷은 표 1.1 에서와 같이 다음 유형으로 분류 할 수 있습니다.

표 1.1 EAPS 패킷 유형

패킷 유형	비고
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 중단 된 후 마스터 노드가 전송하고 패킷은 중계 노드의 MAC 주소 에이징 테이블을 표시합니다.
RING-UP-FLUSH-FDB	링 네트워크가 중단 된 후 마스터 노드가 전송하고 패킷은 중계 노드의 MAC 주소 에이징 테이블을 표시합니다.
EDGE-HELLO	이는 에지 노드가 대응하는 메인 링 포트에 의해 전송 된 에지 노드의 에지 포트에 의해 결정되고, 메이저 링이 완료되었는지를 검출한다.

이더넷 보호 절체 메커니즘

폴링 메커니즘

기본 포트는 HEALTH 패킷을 제어 VLAN 으로 전송합니다. 정상적인 경우, HEALTH 패킷은 링의 다른 모든 노드를 통과하여 마침내 마스터 노드의 2 차 포트에 도착합니다.

보조 포트는 기본 조건의 모든 데이터 VLAN 을 차단합니다. HEALTH 패킷을 계속 수신하면 보조 포트는 데이터 VLAN 을 차단하고 루프를 차단합니다. 보조 포트가 특정 시간의 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 에이징하도록 보고합니다.

다음 그림 같이 S4 는 주기적으로 HELLO 패킷을 전송합니다. 루프백에 문제가 없으면 HELLO 패킷이 마스터 노드의 보조 포트에 도착하고 보조 포트가 속한 데이터 VLAN 의 데이터 전달을 차단하여 루프백이 일어나지 않도록 합니다.

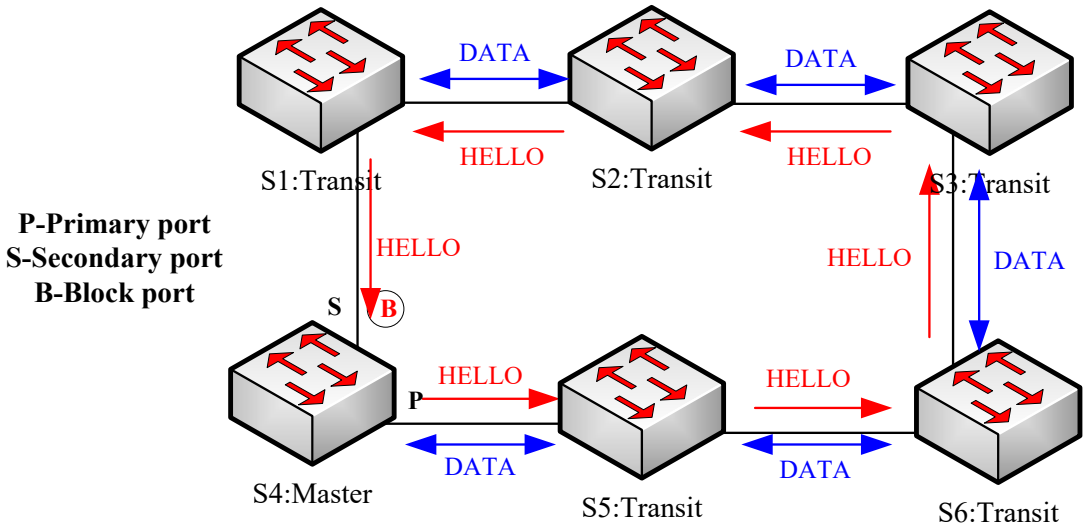


그림 3 폴링

메모:

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.

중계 노드의 무효 링크 통지

링크 상태 알림은 링 토폴로지를 변경하기위한 폴링 메커니즘보다 빠른 메커니즘입니다.

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 수신 한 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. 다음 그림과 같이 노드 S3 과 노드 S6 사이의 링크에 문제가 발생합니다. 노드 S3 과 노드 S6 이 링크에서 이미 문제가 발생했음을 감지하면 문제가 발생한 링크가 해당 포트를 차단하고 다른 포트에서 링크 다운 패킷을 각각 전송합니다. 마스터 노드가 LINK-DOWN 패킷을 수신하면 루프백에서 장애가 발생했다고 판정하고 장애 시간을 더 이상 기다리지 않기로 결정합니다.

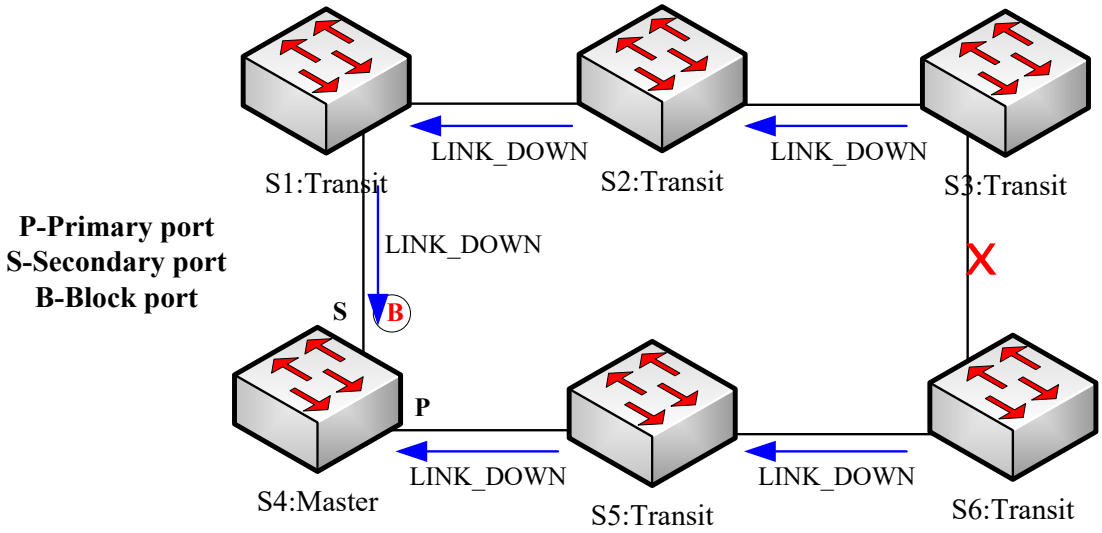


그림 4 링크 상태 변경 알림

중계 포트가 재개 된 후에는 데이터 VLAN 패킷을 즉시 전송하지 않고 사전 전달 상태가됩니다. 프리 포워딩 상태의 중계 포트는 제어 VLAN 에서 제어 패킷 만 전송 및 수신합니다.

링 네트워크에서 유효하지 않은 중계 포트가 하나 뿐이며 포트가 프리 포워딩 상태가되면 마스터 노드의 보조 포트는 기본 포트에서 HEALTH 패킷을 다시 수신 할 수 있습니다. 이 경우 마스터 노드는 보조 포트의 데이터 VLAN 을 다시 차단하고 에이징 주소 테이블의 알림을 외부로 전송합니다. 프리 포워딩 상태의 중계 포트가있는 노드가 에이징 주소 테이블의 알림을 수신하면 노드는 먼저 전달 포트에 대한 사전 전달 포트를 수정 한 다음 로컬 MAC 주소 테이블을 에이징합니다.

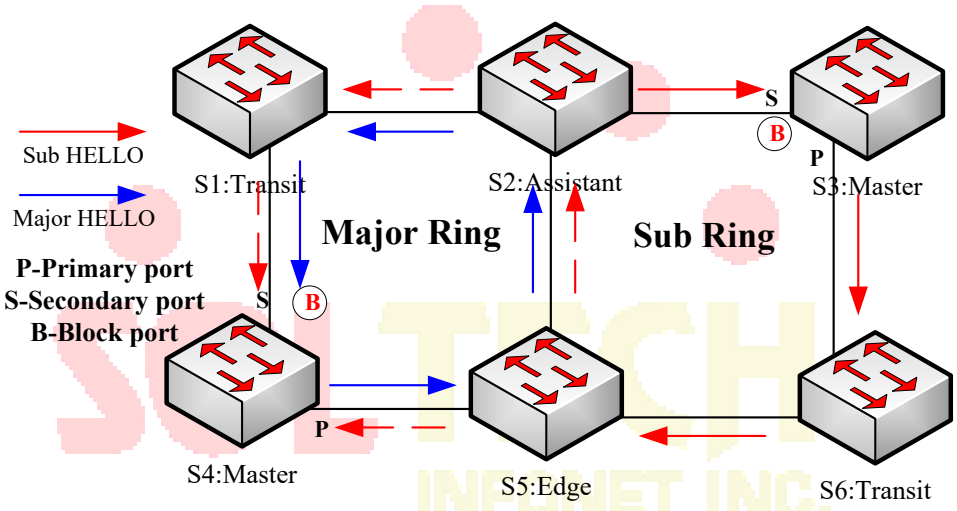
중계 모드가 마스터 노드에서 에이징 주소 테이블 알림을받지 못하면 마스터 노드를 연결하는 링크가 이미 유효하지 않으며 전송 노드가 자동으로 전달 전 포트를 전달 중으로 구성합니다.

메모:

사전 전달 시간 노드를 통해 관련 명령을 구성하여 전송 포트가 사전 전달 상태를 유지할 시간을 수정할 수 있습니다.

주 링상의 서브 링 프로토콜 패킷의 채널 상태 점검 메커니즘

상위 링의 포트는 상위 링의 제어 VLAN 과 하위 링의 제어 VLAN 에 동시에 추가됩니다. 따라서, 서브 링의 프로토콜 패킷은 메이저 링에 의해 제공되는 채널을 통해 엣지 노드 및 보조 노드의 에지 포트 사이에서 방송되어야한다. 이 경우 전체 링은 다음 그림과 같이 서브 링의 노드와 유사합니다 (가상 중계 노드와 유사 함).



메이저 링과 서브 링의 교차점

메이저 링의 링크에 문제가 발생하고, 에지 노드와 보조 노드 사이의 서브 링 프로토콜 패킷의 채널이 인터럽트되면, 서브 링의 마스터 노드는 마스터 노드 자신의 HELLO 패킷을 수신할 수 없다 전송합니다. 이 경우 실패 시간이 초과되고 하위 링의 마스터 노드가 실패 상태로 변경되고 보조 포트가 열립니다.

위에서 언급 한 프로세스는 일반 네트워크에 대한 효과적인 보호를 제공하여 브로드 캐스트 루프백 방지뿐만 아니라 백업 링크의 해당 기능을 보장합니다. 이중 원점 네트워킹 모드는 다음 그림과 같이 실제 네트워킹에서 항상 사용됩니다. 듀얼 호밍 네트워킹의 두 개의 서브 링인 서브

링 I 및 서브 링 II 는 에지 노드와 보조 노드를 통해 상호 연결되며 큰 링을 형성합니다. 주 링에 문제가 발생하면 모든 하위 링의 마스터 노드의 보조 포트가 열리고 큰 링에 브로드 캐스트 루프(화살표로 표시)가 형성됩니다.

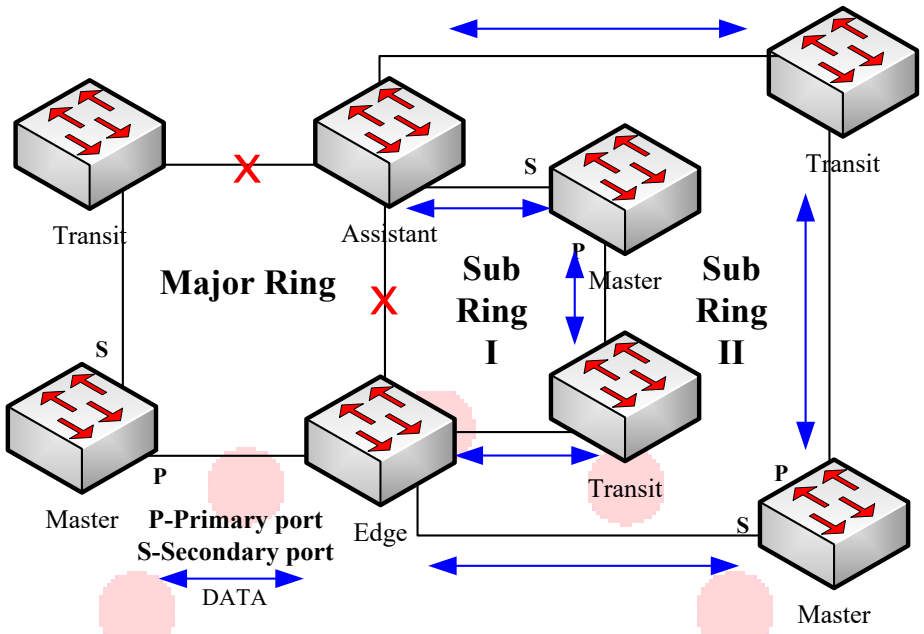
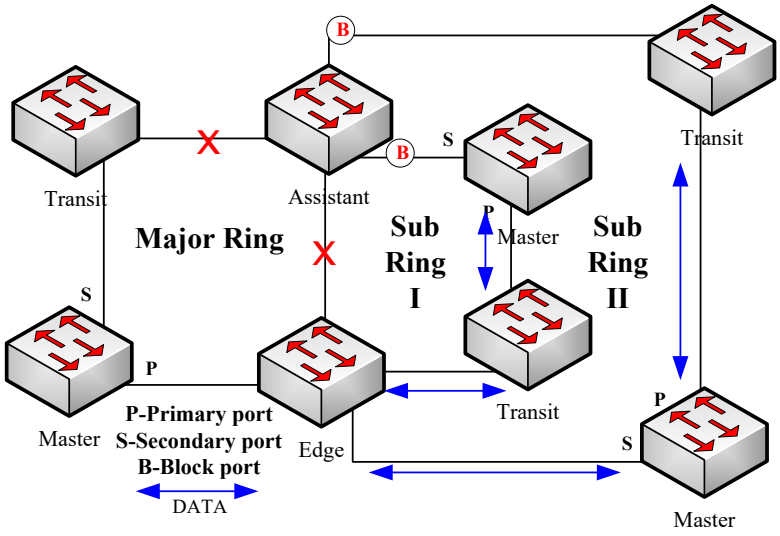


그림 6 듀얼 호밍 네트워킹 모드로 트리거 된 브로드 캐스트 스톰

상위 링에서 서브 링 프로토콜 패킷의 채널 상태 점검 메커니즘이 도입되어 듀얼 원점 복귀 링에 대한 문제점을 해결합니다. 이 메커니즘은 에지 노드와 보조 노드 사이의 상위 링에서 채널 링크의 상태를 모니터링하기위한 것으로, 에지 노드와 보조 노드의 도움이 필요합니다. 이 메커니즘의 목적은 서브 링의 마스터 노드의 보조 포트가 열리기 전에 에지 노드의 에지 포트를 차단하여 데이터 루프가 발생하지 않도록하는 것입니다. 보조 노드는이 메커니즘의 수신기 및 결정자 인 반면 에지 노드는 메커니즘의 트리거입니다. 에지 노드로부터의 통지 메시지가 수신 될 수 없으면, 에지 노드는이 통지 메시지가 다시 수신 될 때까지 즉시 블로킹 상태가 될 것이다. 메커니즘의 결과,



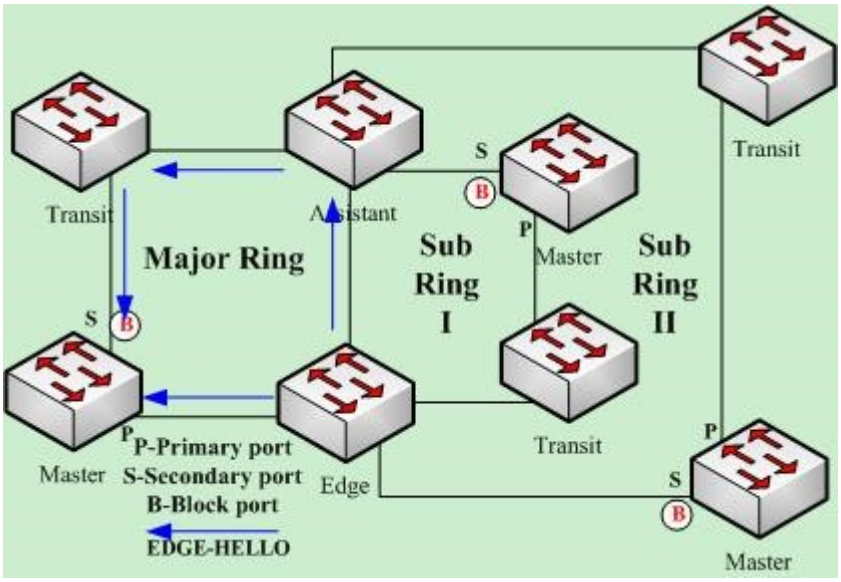
채널 상태 점검 메커니즘의 결과

그러나 보조 링의 마스터 노드의 보조 포트가 열리기 전에 보조 노드의 에지 포트가 차단되어야한다는 점에 특히주의해야합니다. 그렇지 않으면 브로드 캐스트 스톰이 발생합니다.

이 메커니즘의 전체 절차는 다음과 같이 설명됩니다.

1. 에지 노드와 보조 노드 사이의 상위 링에서 채널 상태를 확인합니다.

서브 링의 에지 노드는 메이저 링의 2 개의 포트를 통해 메이저 링으로 Edge-Hello 패킷을 주기적으로 전송하며, 이들 패킷은 메이저 링상의 모든 노드를 순차적으로 통과하고, 마지막으로 보조 노드에 도달한다 다음 그림. 보조 노드가 규정 된 시간 내에 에지 - 헬로 패킷을 수신 할 수 있으면,이 패킷의 채널이 정상임을 나타냅니다. 그렇지 않은 경우 채널이 인터럽트되었음을 나타냅니다. 에지 - 헬로 패킷은 서브 링의 제어 패킷이지만, 메이저 링상의 포트에 의해 송수신되고 처리를 위해 서브 링으로 전송된다.



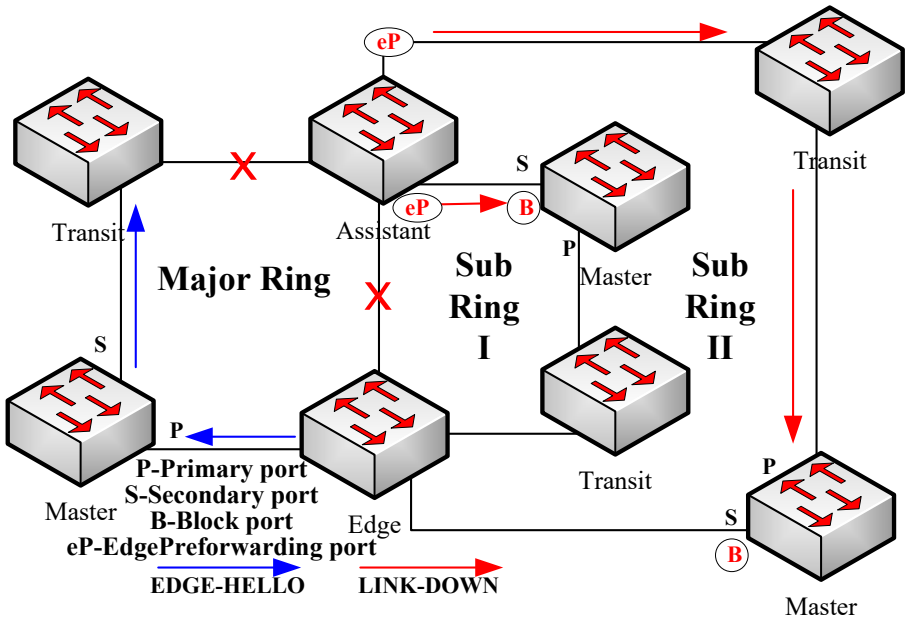
8. 에지 링과 보조 노드 사이의 상위 링에서 채널 상태를 확인합니다.

2. 에지 노드는 채널 중단시 에지 포트를 차단합니다.

보조 노드가 Edge Fail Time 동안 Edge-hello 패킷을 수신 할 수없는 경우 보조자는 Edge-hello 패킷 인 Sub-Ring 프로토콜 패킷의 채널이 방해 받고 에지 포트의 상태를 Edge-Preforwarding 상태로 변경합니다 즉각적으로 데이터 패킷의 전달을 차단하지만 (여전히 제어 패킷을 수신하고 전달 함), 마스터 노드가 마스터 노드에 대한 링크 패킷을 즉시 전송하여 보조 포트를 열어서 해당 노드의 모든 노드 사이의 통신 중단을 방지합니다.

메모:

에지 포트가 먼저 에지 프리 포워드 상태로 변경되고 마스터 노드가 보조 포트를 열도록 보장하기 위해 에지 노드가 에지 hello 패킷, Edge Hello Time 을 전송하는주기가 마스터 노드가 Hello 패킷, Hello Time 을 전송하는주기보다 작다. 마찬가지로 보조 노드의 Edge Fail Time 은 Fail Time 보다 작아야합니다. 동시에 Fail Time 은 일반적으로 Hello Time 의 세 배이고 Edge Fail Time 은 Edge Hello Time 의 세 배입니다.



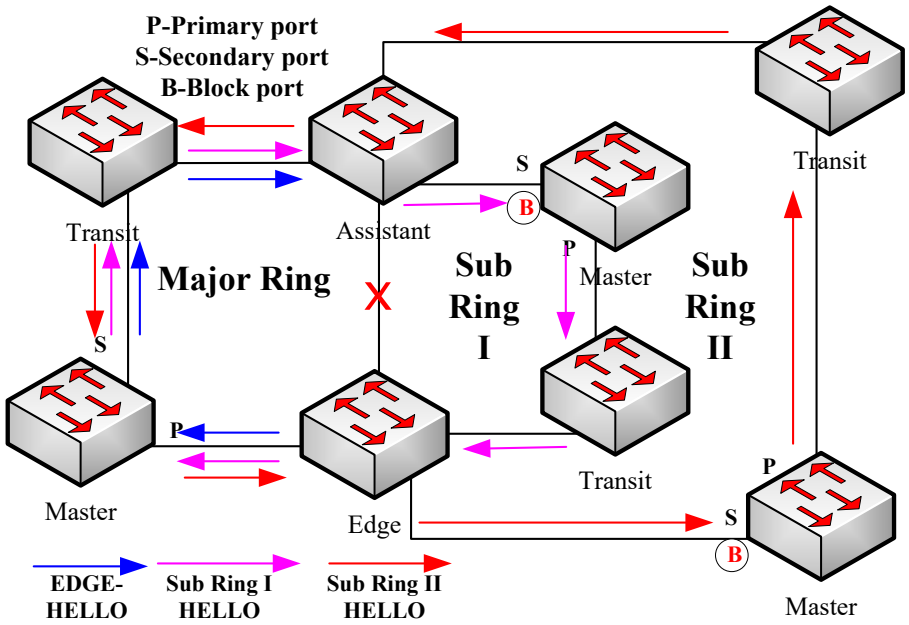
9. 에지 노드는 채널 중단시 에지 포트를 차단합니다.

3. 채널 복구

메이저 링의 링크와 에지 노드와 보조 노드 간의 통신이 재개 될 때, 서브 링 프로토콜 패킷의 채널은 정상 기능으로 재개된다. 이 경우, 서브 링의 마스터 노드는 마스터 노드 자신이 송신 한 Hello 패킷을 다시 수신하고, Complete 상태로 전환하여 2 차 포트를 차단하고 RING-UP-FLUSH-FDB 패킷을 송신한다 링에. 동시에 보조 노드의 에지 포트 상태가 Edge-Preforwarding 에서 Forwarding 으로 바뀌어 링의 모든 노드간에 원활한 통신이 보장됩니다. 다음 그림은 채널이 다시 시작된 후 링에서의 통신이 재개되는 것을 보여줍니다.

노트 :

에지 노드가 차단 된 에지 포트를 열기 전에 브로드캐스트 스톰이 발생하지 않도록 서브 링의 마스터 노드의 보조 포트를 차단해야 합니다.



10. 채널 복구

MEAPS 구성

구성 전 요구 사항

MEAPS 를 구성하기 전에 다음 항목을 주의 깊게 읽으십시오.

링 보호 프로토콜의 중요한 기능 중 하나는, 브로드 캐스트 폭풍을 중지 그래서 링 링크가 다시 연결하기 전에 모든 링 노드가 구성되어 있는지 확인하십시오 것입니다. 구성이 완료되지 않은 경우 링 네트워크가 연결되면 브로드 캐스트 스톰이 쉽게 발생할 수 있습니다.

STP 의 호환성을 실현하기 위해 링 보호 프로토콜을 구성 합니다. 사용자는 "스패닝 트리 없음", SSTP, RSTP 및 MSTP 를 구성할 수 있습니다.

- 링 노드의 인스턴스가 구성되면 현재 링 노드가 삭제 된 다음 재구성되지 않는 한 사용자는 노드의 기본 정보 (시간 매개 변수 제외)를 변경할 수 없습니다.

show 를 실행 하여 구성된 노드를 찾아보고 해당 노드의 상태가 **init** 인 경우 노드의 구성이 완료되지 않았으므로 노드를 시작할 수 없음을 나타냅니다. 이 경우 기본 정보를 변경하거나 추가하여 노드 구성을 완료해야합니다.

링 보호 프로토콜은 다중 링 네트워크를 구성하기위한 스위치를 지원합니다.

링 네트워크의 제어 VLAN 을 구성해도 해당 체계 VLAN 이 자동으로 구성되지 않습니다. 글로벌 VLAN 구성 명령을 통해 체계적으로 VLAN 을 수동으로 구성해야 합니다.

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 수정 된 후에는 Fail-time 을 적절히 수정해야합니다.

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 감지 할 수 있습니다 상태. 마스터 노드에 구성된 Hello-time 이 중계 노드의 Fre-Forward-Time 보다 길면 루프백이 쉽게 생성되고 브로드 캐스트 스톰이 트리거됩니다.

사용자는 Edge Hello Time 및 Edge Fail Time 을 구성할 수 없으며 기본값은 Hello Time 및 Fail Time 에 의해 결정됩니다. 각각의 값은 Hello Time 및 Fail Time 의 1/3 입니다.

물리적 인터페이스, 고속 이더넷 인터페이스, 기가비트 이더넷 인터페이스 및 집계 인터페이스는 모두 링의 인터페이스로 구성 될 수 있습니다. 링크 집합, 802.1X 또는 포트 보안이 실제 인터페이스에 이미 구성된 경우 물리적 인터페이스를 더 이상 링 인터페이스로 구성할 수 없습니다.

이 프로토콜은 원래의 EAPS 와 비슷하지만 링의 토폴로지는 확장 성과 유연성이 뛰어납니다. 따라서 MEAPS 및 EAPS 는 부분적으로 호환 가능하며 교차 구성은 MEAPS 링 및 EAPS 링에서 수행 될 수 있습니다. 그러나 MEAPS 및 EAPS 를 지원하도록 동일한 물리적 포트를 동시에 구성할 수는 없습니다.

MEAPS 구성 작업

마스터 노드 구성

중계 노드 구성

에지 노드 및 보조 노드 구성

링 포트 구성

링 보호 프로토콜의 상태 탐색

MEAPS 구성

마스터 노드 구성

다음 단계에 따라 스위치를 링 네트워크의 마스터 노드로 구성하십시오.

명령	**설명**
Switch#**config**	스위치 구성 모드로 들어갑니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 구성하고 노드 구성 모드로 들어갑니다. *id1* : 노드의 인스턴스 ID *id2* : 도메인의 인스턴스 ID (0 인 경우 생략)
Switch_config_ring1#**master-node**	노드 유형을 마스터 노드로 구성합니다.
Switch_config_ring1#**major-ring[sub-ring]**	노드 레벨을 주 상/하위 링 노드 중 하나로 구성합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	의무 단계입니다. 제어 VLAN 을 구성하고 VLAN "id"및 VLAN "id-1"을 구성합니다. *vlan-id* : 제어 VLAN 의 ID
Switch_config_ring1#**hello-time** *value*	이 단계는 선택 사항입니다. 마스터 노드가 HEALTH 패킷을 전송할주기를 구성합니다. *값* : 1 - 10 초 범위의 시간 값이고 기본값은 3 초입니다.
Switch_config_ring1#**fail-time** *value*	이 단계는 선택 사항입니다. 보조 포트가 HEALTH 패킷을 기다리는 시간을 구성합니다. *값* : 3 - 30 초 범위의 시간 값이고 기본값은 9 초입니다.
Switch_config_ring1#**exit**	현재 구성을 저장하고 노드 구성 모드를 종료합니다.

메모:

mether 링 아이디 도메인 ID2 의 명령은 노드 구성 및 링의 노드의 포트 구성을 삭제하는 데 사용됩니다.

메모:

구성 중에는 상위 링과 하위 링이 동일한 제어 VLAN, 즉 상위 링의 제어 VLAN 을 갖도록 구성해야 합니다. 이 구성이 성공적으로 구성되면 메이저 링의 제어 VLAN 과 서브 링의 제어 VLAN 이 메이저 링에 생성되고 동시에 서브 링 제어 VLAN 이 서브 링에 생성되고, 링 제어 VLAN 은 서브 링에서 금지됩니다.

이동 노드 구성

다음 단계에 따라 스위치를 링 네트워크의 중계 노드로 구성합니다.

명령	설명
Switch# config	스위치 구성 모드로 들어갑니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 구성하고 노드 구성 모드로 들어갑니다. *id1* : 노드의 인스턴스 ID *id2* : 도메인의 인스턴스 ID (0 인 경우 생략)
Switch_config_ring1# **transit -node**	의무 단계입니다. 노드 유형을 중계 노드로 구성합니다.
Switch_config_ring1#**major-ring[sub-ring]**	의무 단계입니다. 노드의 레벨을 주 노드 또는 하위 링 노드 중 하나로 구성합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	의무 단계입니다. 제어 VLAN 을 구성하고 VLAN "id"및 VLAN "id-1"을 구성합니다. *vlan-id* : 제어 VLAN 의 ID
Switch_config_ring1#**pre-forward-time** *value*	이 단계는 선택 사항입니다. 전송 포트에서 사전 전달 상태를 유지하는 시간을 구성합니다. *값* : 3 - 30 초 범위의 시간 값이고 기본값은 9 초입니다.
Switch_config_ring#exit	현재 구성을 저장하고 노드 구성 모드를 종료합니다.

Switch_config#	

.

에지 노드 및 보조 노드 구성

다음 단계에 따라 스위치를 링 네트워크의 마스터 노드로 구성하십시오.

명령	**설명**
Switch# **config**	스위치 구성 모드로 들어갑니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 구성하고 노드 구성 모드로 들어갑니다. *id1* : 노드의 인스턴스 ID *id2* : 도메인의 인스턴스 ID (0 인 경우 생략)
Switch_config_ring1#**edge-node[assistant-node]**	의무 단계입니다. 노드 유형을 가장자리 노드로 구성합니다.
Switch_config_ring1#**sub-ring**	이 단계는 생략 할 수 있습니다. 에지 노드는 서브 링 노드 여야합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	의무 단계입니다. 제어 VLAN 을 구성하고 VLAN "id"및 VLAN "id-1"을 구성합니다. *vlan-id* : 제어 VLAN 의 ID
Switch_config_ring1#**pre-forward-time** *value*	이 단계는 선택 사항입니다. 에지 포트의 프리 포워딩 상태를 유지하는 시간을 구성합니다. *값* : 3 - 30 초 범위의 시간 값이고 기본값은 9 초입니다.
Switch_config_ring1#**exit**	현재 구성을 저장하고 노드 구성 모드를 종료합니다.
Switch_config#	

단일 서브 링 네트워킹 모드 구성

다음 단계에 따라 스위치를 링 네트워크의 마스터 노드로 구성하십시오.

명령	**설명**
Switch# **config**	스위치 구성 모드로 들어갑니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 구성하고 노드 구성 모드로 들어갑니다. *id1* : 노드의 인스턴스 ID *id2* : 도메인의 인스턴스 ID (0 인 경우 생략)

Switch_config_ring1#**edge-node[assistant-node]**	의무 단계입니다. 노드 유형을 가장자리 노드로 구성합니다.
Switch_config_ring1#**sub-ring**	이 단계는 생략 할 수 있습니다. 에지 노드는 서브 링 노드 여야합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	의무 단계입니다. 제어 VLAN 을 구성하고 VLAN "id"및 VLAN "id-1"을 구성합니다. *vlan-id* : 제어 VLAN 의 ID
Switch _config_ring2#**single-subring-mode**	의무 단계입니다. 이 명령을 사용하지 않아도 링 구성을 완료 할 수 있지만 시스템이 단일 링 네트워킹 모드로 들어갈 수 없습니다. 단일 서브 링 네트워킹 모드에서, 서브 링 프로토콜 패킷의 채널 상태는 체크되지 않으며, 이중 제휴 네트워크는 링 내에 존재해서는 안된다. 이 명령은 에지 노드와 보조 노드에서만 적용됩니다.
Switch_config_ring1#**pre-forward-time** *value*	이 단계는 선택 사항입니다. 에지 포트의 프리 포워딩 상태를 유지하는 시간을 구성합니다. *값* : 3 - 30 초 범위의 시간 값이고 기본값은 9 초입니다.
Switch_config_ring1#**exit**	현재 구성을 저장하고 노드 구성 모드를 종료합니다.
Switch_config#	

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.
Switch_config_intf#mether-ring *id1* **domain** *id2* **primary-port [secondary-port | transit-port | common-port | edge-port]**	이더넷 링의 포트 유형을 구성합니다. *id1* : 노드의 인스턴스 ID *id2* : 도메인의 인스턴스 ID (0 인 경우 생략)
Switch_config_intf#exit	인터페이스 구성 모드를 종료합니다.

메모:

이 명령은 mether-ring id1 도메인이 없습니다. id2 primary-port **[secondary-port | transit-port | common-port | edge-port]** , 링의 포트의 구성을 취소 할 수 있습니다.

링 보호 프로토콜의 상태 탐색

다음 명령을 실행하여 링 보호 프로토콜의 상태를 찾습니다.

명령	설명
show mether-ring	링 보호 프로토콜 및 링의 포트에 대한 요약 정보를 검색합니다.
show mether-ring *id1* **domain** *id2*	지정된 링 보호 프로토콜 및 링의 포트에 대한 요약 정보를 검색합니다. *id1* : 노드의 인스턴스 ID *id2* : 도메인의 인스턴스 ID (0 인 경우 생략)
show mether-ring *id1* **domain** *id2* **detail**	지정된 링 보호 프로토콜 및 이더넷 링 포트에 대한 자세한 정보를 찾습니다.
show mether-ring *id1* **domain** *id2* **interface** *intf-name*	지정된 링 포트 또는 지정된 공용 포트의 상태를 탐색합니다.

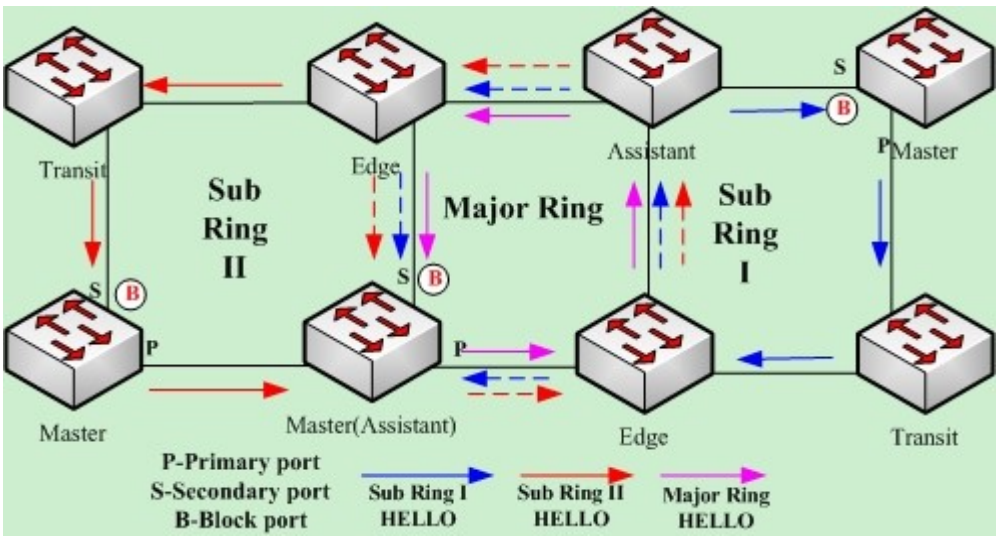
MEAPS 구성 예제

MEAPS 의 작업 절차

MEAPS 는 단일 링 또는 evel-2 다중 링 구조를 지원하는 세 가지 보호 메커니즘을 채택합니다. 다음 섹션에서는 완료 상태에서 링크 다운 상태로, 복구 후 마지막으로 전체 상태로 MEAPS 실행 및 MEAPS 토폴로지 변경에 대한 일반적인 예를 보여줍니다.

완전한 상태

단 하나의 링을 위해 권유되는 링의 완전한 상태는 폴링 메커니즘에 의해 모니터링되고 유지된다. 완료 상태에서 전체 링의 모든 링크는 UP 상태에 있으며 마스터 노드의 상태에서 표현식을 찾습니다. 브로드 캐스트 스톰이 발생하는 것을 방지하기 위해 마스터 노드는 보조 포트를 차단합니다. 동시에 마스터 노드는 기본 포트에서 Hello 패킷을 주기적으로 전송합니다. 이 hello 패킷은 순차적으로 중계 노드를 통과하고 마지막으로 보조 포트에서 마스터 노드로 돌아갑니다. 완성 된 상태의 링은 다음 그림과 같습니다. 메이저 링과 서브 링은 모두 완전한 상태입니다. 상위 링의 헬로우 패킷은 상위 링에서만 방송되며,

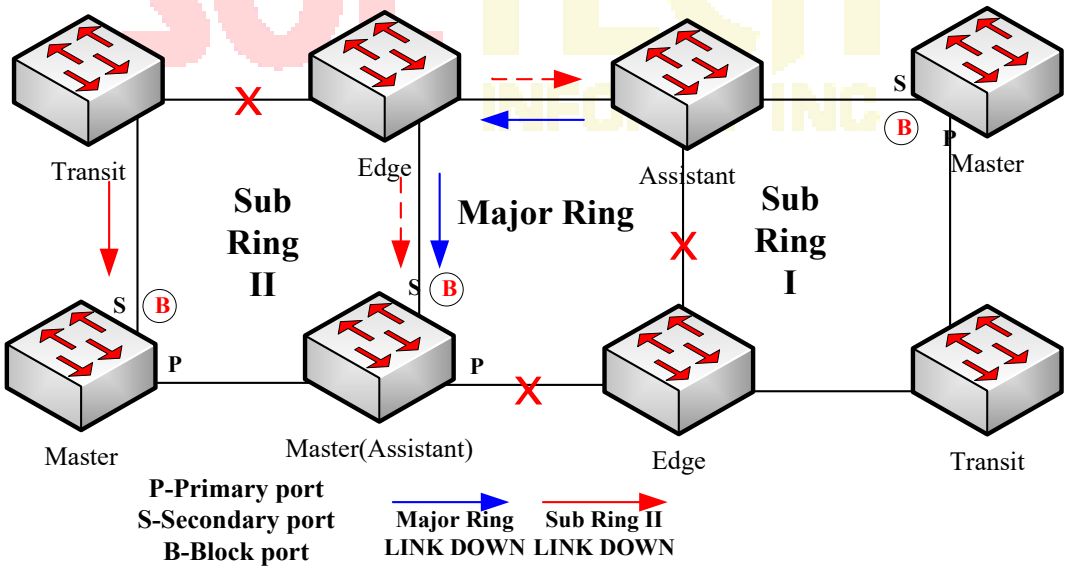


완료 상태

링크 다운

링의 링크 다운 상태는 폴링 메커니즘, 링크 상태 변경 통지 및 서브 링 프로토콜 패킷의 채널 상태 검사 메커니즘에 의해 결정된다. 물론 링의 링크 다운 상태는 하나의 링에 대해서만 지지됩니다. 링의 일부 링크가 링크 다운 상태에 있으면 링이 경쟁 상태에서 문제가 발생한 상태, 즉 링크 다운 상태로 바뀝니다.

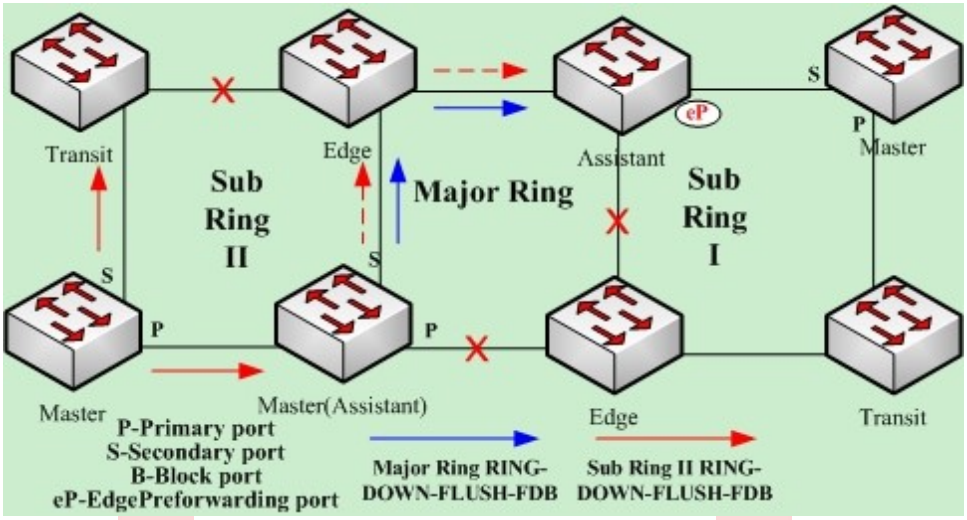
링크에서 링크 다운이 발생하면 폴링 메커니즘과 링크 상태 변경 알림 메커니즘이 모두 작동합니다. 링크 다운이 발생하는 중계 노드는 링크 다운 패킷을 다른 쪽의 업 포트를 통해 마스터 노드로 전송합니다. 동시에 폴링 메커니즘은 실패 시간을 통해 링의 상태를 즉시 모니터링하고 변경합니다. 서브 링 프로토콜 채널에 문제가 발생하면 상위 링에서 서브 링 프로토콜 패킷의 채널 상태 점검 메커니즘에 의해 문제가 처리됩니다. 다음 그림에서 볼 수 있듯이, 메이저 링의 링크 및 공통 링크의 장애 통지 메시지는 메이저 링에서만 전송되고 마침내 마스터 노드로 전송됩니다.



문제를 전송하고 마스터 노드에 알리는 링

마스터 노드가 링크 다운 패킷을 수신 한 후에는 상태가 실패 상태로 변경되고 동시에 보조 포트가 열리고 FDB 테이블이 새로 고쳐지고 RING-DOWN-FLUSH-FDB 패킷이 모든 노드에

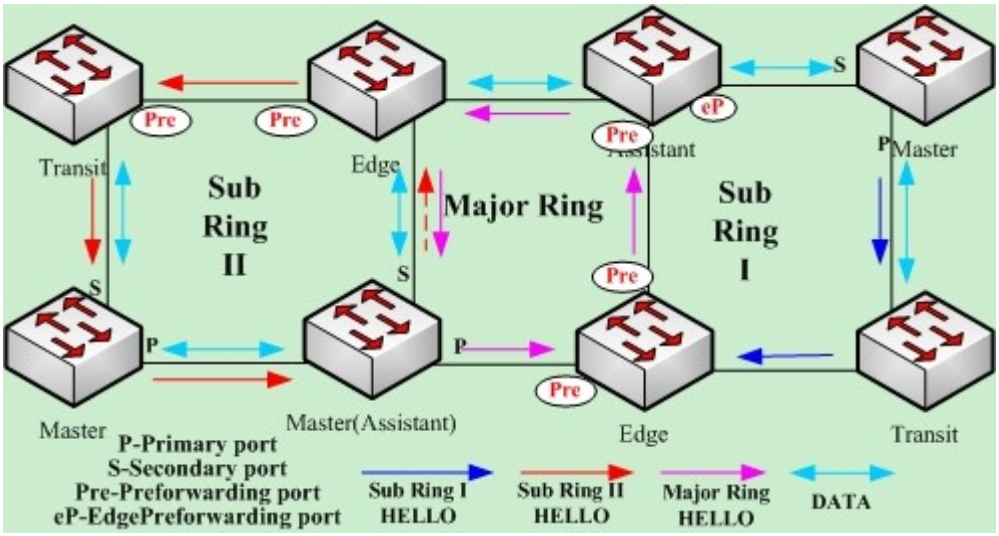
알리기 위해 두 개의 포트에서 전송할 수 있습니다. 다음 그림과 같이 상위 링의 마스터 노드는 새로 고치는 FDB 의 상위 링에있는 중계 노드에 알립니다. 서브 링 1 은 채널에 문제가있어 보조 노드의 에지 포트가 차단됩니다. 서브 링 2 의 마스터 노드는 서브 링상의 중계 노드들에게 FDB 를 리프레시하도록 통지하고,이어서 투명 링 전송이 메이저 링상에서 수행 될 것이다.



링 문제 해결 및 FDB 갱신

복구

중계 노드의 포트가 복구되면 중계 노드는 해당 사전 전송 상태로 전환됩니다. 중계 노드의 포트가 복구 될 때의 처리 절차는 다음 그림과 같습니다. 상위 링의 링크가 복구되며 상위 링의 링크를 연결하는 중계 노드는 Preforwarding 상태로 변경되고 데이터 패킷은 차단되지만 제어 패킷의 Hello 패킷은 통과 할 수 있습니다. 유사하게, 서브 링 (2)상의 중계 노드는 또한 프리 포워딩 상태로 변화한다; 재전송 된 중계 노드가 장조의 제어 패킷 만 통과시키고 하위 링 1 의 헬기 패킷은 단지 제 1 링의 헬기 패킷이 단지 제 1 링 노드의 데이터 패킷과 동일하다는 사실 때문에 서브 링 1 상의 헬로 패킷이 에지 노드에 도달 할 때, 상위 링, 안녕 패킷을 전달할 수 없습니다.



링의 링크 복구 및 중계 노드에서 프리 포워딩으로의 이동

중계 포트는 제어 패킷을 사전 전달 상태로 전송할 수 있으므로 마스터 노드의 보조 포트는 기본 포트에서 hello 패킷을 수신 할 수 있습니다. 따라서, 마스터 노드는 자신의 상태를 완료로 전환하고, 보조 포트를 차단하고 기본 포트에서 링 업 - 흐름 -FDB 패킷을 전송합니다. 중계 노드가 RING-UP-FLUSH-FDB 패킷을 수신 한 후 중계 노드는 다시 Link-Up 상태로 전환하고 차단된 포트를 열고 FDB 테이블을 새로 고칩니다. 링 복구 절차는 다음 그림과 같습니다. 메이저 링의 마스터 노드는 완전한 상태로 변경되고, 보조 포트를 차단하고, 메이저 링의 모든 중계 노드로 링 업 (RING-UP-FLUSH-FDB) 패킷을 전송하고,이 중계 노드를 링크 업 상태로 다시 이동시킵니다 차단 된 포트를 열고 FDB 테이블을 새로 고침합니다. 비슷하게, 중계 노드 및 서브 링 (2)상의 마스터 노드는 또한 대응하는 변화를 취한다; 서브 링 프로토콜 패킷의 채널 1 에서의 서브 링으로 인해, 마스터 노드의 제 2 포트는 제 1 포트로부터 헬로 패킷을 수신 할 수 있고, 마스터 노드는 자신의 상태를 완료 상태로 되돌리고, 제 2 포트를 차단하고, RING-UP-FLUSH-FDB 패킷을 송신하고 보조 노드를 에지 포트로 개방시키고 서브 링 (1)은 그 완전한 상태로 재개한다.

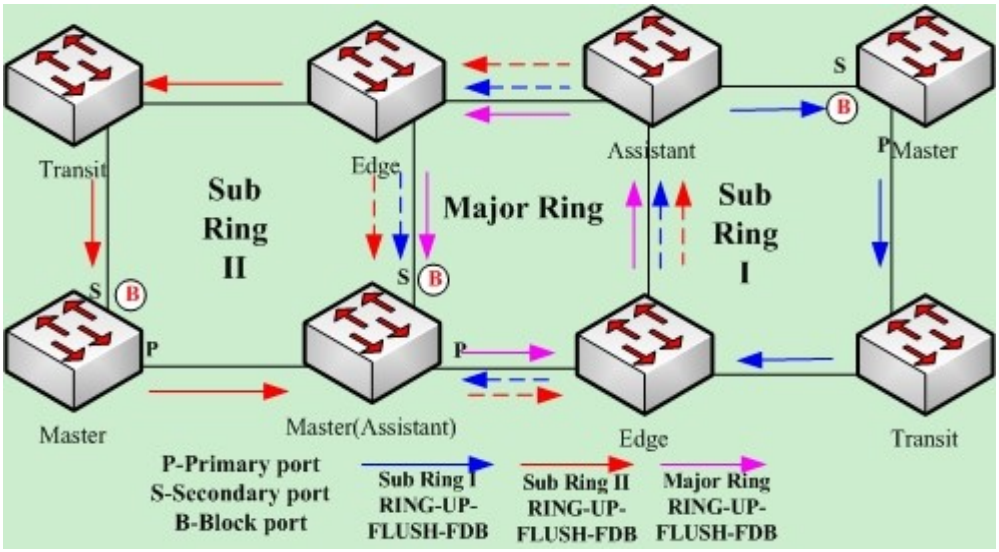
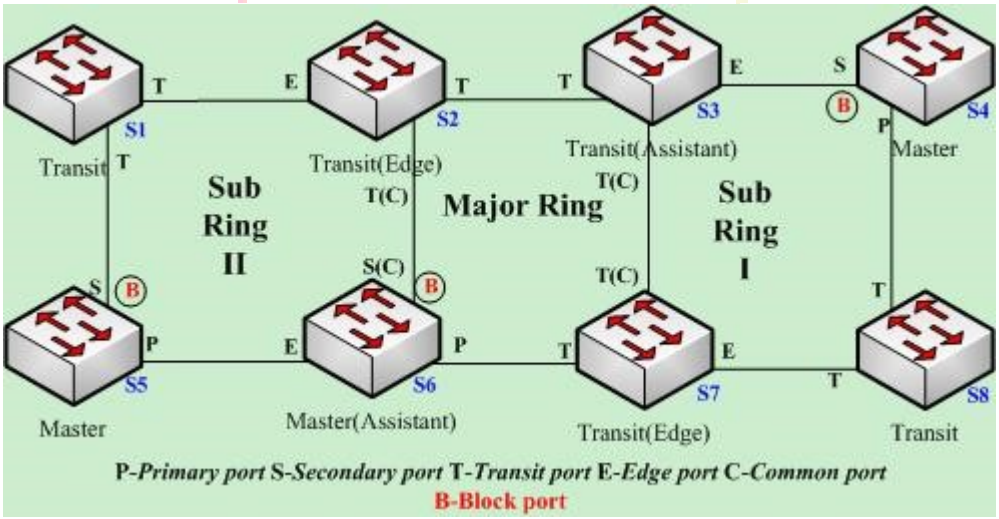


그림 15 링 복구

물론 Preforwarding 상태의 중계 노드가 RING-UP-FLUSH-FDB 패킷을받지 못하고 Fail Time 도 초과하면 중계 노드는 차단 된 중계 포트를 열고 데이터 통신을 다시 시작합니다.

MEAPS 구성

구성 예



MEAPS 구성

그림 1.1 에서와 같이 마스터 노드 S1 과 중계 노드 S2 는 다음과 같이 구성됩니다. 다른 노드의 구성은 S2 의 구성과 동일합니다.

스위치 S1 구성 :

다음 명령은 하위 링 중계 노드 인 노드 2 를 구성하는 데 사용됩니다.

Configuring switch S1:

다음 명령은 하위 링 중계 노드 인 노드 2 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#transit-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring2#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring2#quit

다음 명령은 노드 2 의 중계 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 2 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

Configuring switch S2:

다음 명령은 상위 링 중계 노드 인 노드 1 을 구성하는 데 사용됩니다.

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring1#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring1#quit

다음 명령은 노드 1 의 전송 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

다음 명령은 하위 링 에지 노드 인 노드 2 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#edge-node

Switch_config_ring2#sub-ring *(this can be omitted)*

Switch_config_ring2#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring2#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring2#quit

다음 명령은 노드 2 의 공통 포트 및 에지 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 2 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S3:

다음 명령은 상위 링 중계 노드 인 노드 1 을 구성하는 데 사용됩니다.

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring1#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring1#quit

다음 명령은 노드 1 의 전송 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

다음 명령은 하위 링 보조 노드 인 노드 4 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#assistant-node

Switch_config_ring4#sub-ring *(it can be omitted)*

Switch_config_ring4#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring4#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring4#quit

다음 명령은 노드 2 의 공통 포트 및 에지 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 4 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S4:

다음 명령은 서브 링 마스터 노드 인 노드 4 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#master-node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring4#hello-time 4

Switch_config_ring4#fail-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring4#quit

다음 명령은 노드 4 의 기본 포트와 보조 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 4 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

Configuring switch S5:

다음 명령은 서브 링 마스터 노드 인 노드 2 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#master-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring2#hello-time 4

Switch_config_ring2#fail-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring2#quit

다음 명령은 노드 2 의 기본 포트 및 보조 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 2 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

Configuring switch S6:

다음 명령은 메이저 링 마스터 노드 인 노드 1 을 구성하는 데 사용됩니다.

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#master-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring1#hello-time 4

Switch_config_ring1#fail-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring1#quit

다음 명령은 노드 1 의 전송 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

다음 명령은 하위 링 보조 노드 노드 2 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#assistant-node

Switch_config_ring2#sub-ring *(This can be omitted)*

Switch_config_ring2#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring2#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring2#quit

다음 명령은 노드 2 의 공통 포트 및 에지 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 2 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S7:

다음 명령은 상위 링 중계 노드 인 노드 1 을 구성하는 데 사용됩니다.

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring1#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring1#quit

다음 명령은 노드 1 의 전송 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

다음 명령은 하위 링 에지 노드 인 노드 4 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#edge-node

Switch_config_ring4#sub-ring *(This can be omitted)*

Switch_config_ring4#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring4#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring4#quit

다음 명령은 노드 4 의 공통 포트 및 에지 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 4 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S8:

다음 명령은 하위 링 중계 노드 인 노드 4 를 구성하는 데 사용됩니다.

Switch_config#mether-ring 4 domain 1

Switch_config_ring4# transit -node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

다음 명령은 시간 관련 매개 변수를 구성하는 데 사용됩니다.

Switch_config_ring4#pre-forward-time 12

노드 구성 모드를 종료합니다.

Switch_config_ring4#quit

다음 명령은 노드 4 의 중계 포트를 구성하는 데 사용됩니다.

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 4 domain 1 transit -port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 transit -port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

MEAPS 상태 설명

- 완성되지 않은 기본 정보 구성 : 링의 역할, 링의 등급 및 제어 VLAN이 구성되지 않았습니다. 한 가지 예외적 인 경우는 노드의 역할이 에지 노드 또는 보조 노드로 구성된 경우 기본 링의 등급이 하위 링입니다.

- 기본 정보의 모순 : 노드의 역할은 에지 노드 또는 보조 노드 인 경우, 기본 링의 등급은 하위 링입니다 링의 등급이 메이저 링이면 프롬프트 정보가 나타납니다.

- 대응하는 메이저 링 노드가없는 서브 링 : 노드의 역할이 에지 노드 또는 보조 노드 인 경우이 노드는 메이저 링 노드에서 수행됩니다. 하위 링 에지 노드 또는 하위 링 보조 노드를 강제로 생성 할 해당 주 링 노드가없는 경우 프롬프트 정보가 나타납니다 (이 경우 MEAPS 상태를 탐색하려면 show 명령을 사용할 수 있으며, 기본 정보는 완전하지만 상태는 init 입니다. 이는 링 노드의 구성이 완료되지 않았 음을 나타냄).

- 제어 VLAN 구성 중 발생하는 충돌 : 노드에 의해 구성된 제어 VLAN이 다른 구성된 노드와 충돌하면 프롬프트 정보가 나타납니다 (이 경우 MEASS 상태를 탐색하려면 show 명령을 사용할 수 있으며, 기본 정보는 완전하지만 상태는 init 입니다. 이는 링 노드의 구성이 완료되지 않았음을 나타냄).

- 메이저 - 링 노드에 대응하는 서브 링 노드가 구성되면, 서브 링 노드의 ID는 메이저 링 노드의 ID보다 커야한다. 서브 링 노드의 ID가 메이저 링 노드의 ID보다 작은 경우, 서브 링 노드는 생성 될 수없고 관련된 프롬프트 정보가 튀어 나옵니다.

DHCP Snooping

개요

VLAN 에서 DHCP 스누핑이 활성화 된 경우 VLAN 의 모든 신뢰할 수 없는 물리적 포트에서 수신 된 DHCP 패킷이 합법적으로 검사됩니다. VLAN 의 신뢰할 수 없는 물리적 포트에서 수신 된 DHCP 응답 패킷은 삭제되어 가짜 또는 잘못 구성된 DHCP 서버가 주소 분배 서비스를 제공하지 못하게 합니다. 신뢰할 수 없는 포트의 DHCP 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.

DHCP trust 인터페이스 구성

인터페이스가 DHCP trusting 인터페이스로 구성된 경우이 인터페이스에서 수신 한 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 수없는 인터페이스에 대한 인터페이스를 다시 시작합니다.

인터페이스는 기본적으로 신뢰할 수 없는 인터페이스입니다.

VLAN 에서 DAI 활성화

VLAN 의 모든 물리적 포트에서 동적 ARP 모니터링이 수행되면이 패킷의 소스 MAC 주소와 소스 IP 주소가 구성된 MAC-IP 바인딩 관계와 일치하지 않으면 수신 된 ARP 패킷이 거부됩니다. 인터페이스의 바인딩 관계는 DHCP 에 의해 동적으로 바인딩되거나 수동으로 구성 될 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.

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.

VLAN 에서 소스 IP 주소 모니터링 활성화

VLAN 에서 소스 IP 주소 모니터링이 활성화 된 후에는 소스 MAC 주소와 소스 IP 주소가 구성된 MAC-IP 바인딩 관계와 일치하지 않으면 VLAN 의 모든 물리적 포트에서 수신 된 IP 패킷이 거부됩니다. 인터페이스의 바인딩 관계는 DHCP 에 의해 동적으로 바인딩되거나 수동으로 구성 될 수 있습니다. 물리적 인터페이스의 IP 주소에 MAC 주소가 바인딩되어 있지 않으면 스위치는 물리적 인터페이스에서 수신 한 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.

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.

수동으로 인터페이스 바인딩 구성

호스트가 DHCP 를 통해 주소를 얻지 못하면 스위치의 인터페이스에 바인딩 항목을 추가하여 호스트가 네트워크에 액세스 할 수있게 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 .

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 생성 된 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

00-e0-0f-26-23-89   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

00-e0-0f-32-1c-59   192.2.2.1       infinite      MANUAL        1       Gigaethernet0/2
00-e0-0f-26-23-89   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, dilD: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface Gigaethernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 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
```

IGMP-Snooping

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 수있게하는 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.

노트 :

igmp-Snooping 은 질의 메시지를 받고 igmp 의 메시지를 보고 위의 기능을 실현하기 때문에 igmp-Snooping 은 멀티캐스트 라우터에서 작동 할 때만 제대로 작동 할 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

등록 된 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

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 생성 된 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.

참고 : 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.

VLAN 의 정적 멀티 캐스트 주소 추가 / 삭제

IGMP 를 지원하지 않는 호스트는 정적 멀티 캐스트 주소를 구성하여 해당 멀티 캐스트 메시지를 수신 할 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.

VLAN 의 즉시 종료기능

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 구성 합니다 .
no ip igmp-Snooping vlan *vlan_id* **immediate-leave**	VLAN 의 즉각적인 종료를 기본값으로 구성합니다.

VLAN 의 즉시 종료 특성은 기본적으로 비활성화되어 있습니다.

등록 된 대상 주소없이 멀티 캐스트 메시지를 필터링하는 기능 구성

멀티 캐스트 메시지 대상을 찾을 수 없으면 (DHL, 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 dlf-drop vlan *vlan_id*	대상을 찾을 수없는 멀티 캐스트 메시지를 삭제합니다.
no ip igmp-Snooping dlf-drop vlan *vlan_id*	오류 구성을 다시 시작합니다 (앞에서부터).

노트 :

1) 모든 VLAN 에 대해 속성이 구성됩니다.

2) 스위치가 유형의 메시지를 처리하는 기본 방법은 정방향입니다 (이 유형의 메시지는 VLAN 에서 브로드 캐스팅됩니다).

IGMP-Snooping 의 구성 Router-age 타이머

Router-age 는 IGMP 의 지망생이 존재하는지 여부를 모니터링하는 데 사용됩니다. IGMP 질의는 질의 메시지 를 보내 멀티 캐스트 주소를 유지 합니다. IGMP-Snooping 은 IGMP-inquier 와 호스트간의 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 .

노트 :

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.

IGMP-Snooping 응답 시간 타이머 구성

응답 시간 타이머는 IGMP 의 지망생이 전송 한 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.

노트 :

타이머 값은 너무 작을 수 없습니다. 그러면 멀티 캐스트 통신이 불안정 해집니다.

IGMP-Snooping 의 응답 시간 값은 10 초로 구성됩니다.

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 활성화 된 VLAN 에서 기능을 활성화 또는 비활성화 할 수 있습니다)

멀티 캐스트 라우터가 LAN 에 존재하지 않고 멀티 캐스트 플로우에 라우팅이 필요없는 경우 IGMP-Snooping 을 통해 스위치의 자동 쿼리 기능을 활성화 할 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 메시지 의 소스 IP 주소입니다 .

IGMP Snooping-querier 기능은 기본 비활성화되어 있습니다. 가짜 **쿼리** 메시지 의 원본 IP 주소는 기본적으로 10.0.0.200 입니다.

노트 :

만약 쿼리어 기능이 활성화되고 기능이 적용되지 않으면 멀티케스트 라우터가 vlan 에 존재하며 이기능은 자동적으로 멀티케스트 타임아웃때 활성화됩니다.

IGMP-Snooping 모니터링 및 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(G0/2)
```

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 G0/2
   1 0.0.0.0         239.255.255.250 IGMP G0/2
```

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      Rserved statistics option
    err_packets:0       Number of incorrect packets
```

IGMP-Snooping 의 메시지 타이머 디버그 :

```
switch#debug ip igmp-Snooping packet
```

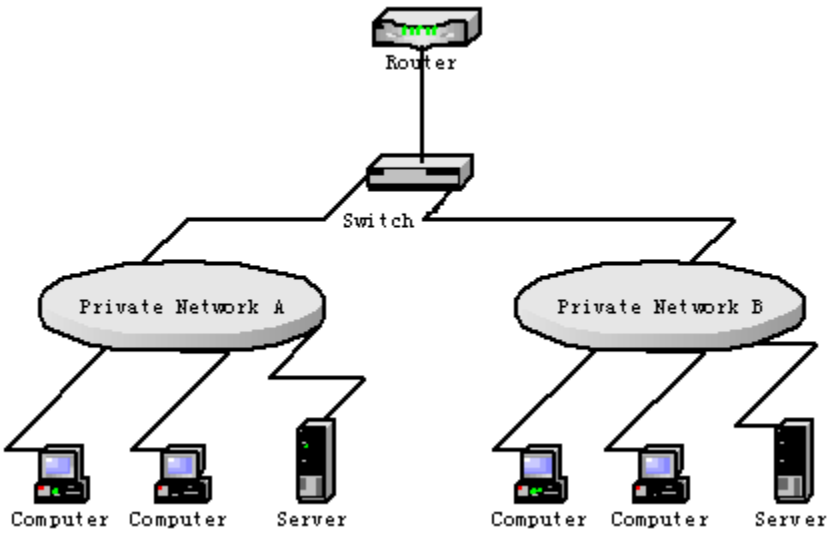
```
rx: s_ip:90.0.0.3, d_ip:224.0.8.9  Source and destination IP addresses where packets are received
        type:16(V2-Report), max resp:00, group address:224.0.8.9  Type and content of packet
rx: s_ip:90.0.0.90, d_ip:224.0.0.1
        type:11(Query), max resp:64, group address:0.0.0.0
rx: s_ip:90.0.0.3, 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
```

IGMP-Snooping 의 메시지 타이머 디버그 :

```
switch#debug ip igmp-Snooping timer
tm: vlan 1 igmp router age expiry at port 2(G0/2)
tm: multicast item 0.0.0.0->224.0.8.9(0100.5e00.0809) response time expiry at port G0/4  Inquerying the response timer expiry
```

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

IGMP 프록시 구성

IGMP 프록시 구성 작업

IGMP 프록시는 멀티 캐스트 사용자가 있는 VLAN 이 다른 VLAN 의 멀티 캐스트 소스를 수신하도록 허용합니다. IGMP 프록시는 다른 멀티 캐스트 라우팅 프로토콜없이 독립적으로 계층 2 에서 실행됩니다. IGMP 프록시는 프록시 된 VLAN 의 IGMP 패킷에 의해 프록시 VLAN 으로 전송되고 이러한 IGMP 패킷에 따라 에이전트 VLAN 의 멀티 캐스트 사용자의 하드웨어 포워드 테이블을 유지합니다. IGMP 프록시는 서로 다른 VLAN 을 프록시 VLAN 과 프록시 VLAN 의 두 가지로 나눕니다. 업스트림 멀티 캐스트 VLAN 은 프록시 VLAN 으로 구성할 수 있지만 다운 스트림 멀티 캐스트 VLAN 은 프록시 VLAN 으로 구성할 수 있습니다.

IGMP 프록시는 IGMP 스누핑을 기반으로 하지만 두 개는 응용 프로그램에서 독립적입니다. IGMP 스누핑은 IGMP 프록시가 활성화되거나 비활성화 될 때 영향을받지 않지만 IGMP 스누핑은 IGMP 스누핑이 활성화 된 경우에만 실행될 수 있습니다.

다음 조건이 충족되지 않으면 IGMP 프록시를 사용할 수 없습니다.

1. L3 스위치
2. 동시에 IP 멀티 캐스트 라우팅을 사용하지 않도록합니다.
3. vlan 이 다운 스트림 vlan 및 업스트림 vlan 으로 작동하는 것을 방지합니다.

IGMP-Proxy 활성화 / 비활성화

VLAN 에이전트 관계 추가 / 삭제

정적 멀티 캐스트 소스 항목 추가 / 삭제

IGMP-Proxy 모니터링 및 유지 관리

IGMP 프록시의 예 구성

IGMP 프록시 활성화 / 비활성화

전역 구성 모드에서 다음 명령을 실행하십시오.

명령	**설명**
ip igmp-proxy enable	IGMP 프록시를 사용합니다.
no ip igmp-proxy enable	기본 구성을 다시 시작합니다.

참고 : IP 멀티 캐스트 라우팅을 활성화 한 후에는 IGMP 프록시를 활성화 할 수 없습니다. 이전에 활성화 된 IGMP 프록시는 IP 멀티 캐스트 라우팅이 활성화 된 경우 자동으로 종료됩니다. ip multicast-routing 을 종료해도 IGMP 프록시가 자동으로 활성화되지 않습니다.

VLAN 에이전트 관계 추가 / 삭제

전역 구성 모드에서 다음 명령을 실행하십시오.

명령	**설명**
ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	vlan (cvlan_map)을 관리하기 위해 에이전트 VLAN (avlan_map)을 추가합니다.
no ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	에이전트 관계를 삭제합니다.

노트 :

1 . vlan 이 avlan_map 에 의해 지정되기 전에 표시된 VLAN 을 구성 할 수 없습니다. 또한 에이전트 VLAN 은 cvlan_map 전에 구성 할 수 없습니다.

2. 표시된 VLAN 과 에이전트 VLAN 은 IGMP-Snooping 의 제어를 받아 들여야합니다.

IGMP 프록시 모니터링 및 유지 보수

EXEC 모드에서 다음 명령을 실행하십시오.

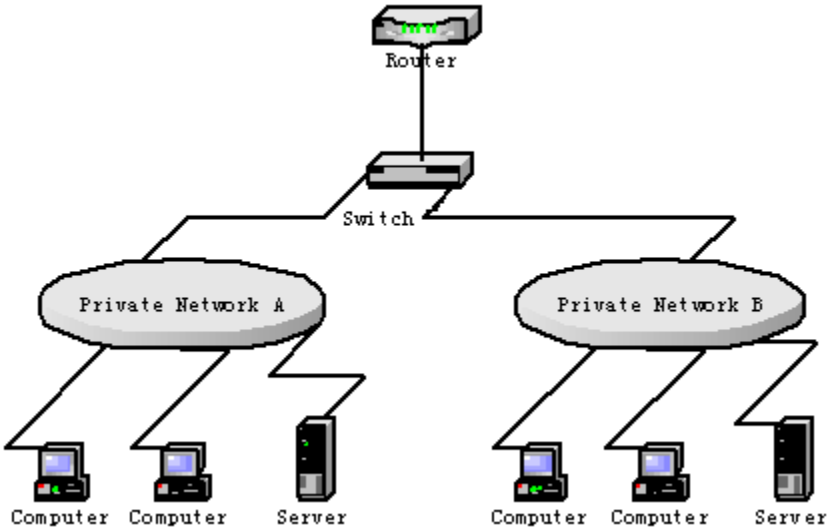
명령	**설명**
show ip igmp-proxy	IGMP 프록시에 대한 정보를 표시합니다.
show ip igmp-proxy mcache *[delete | nonsync | sync| static]*	IGMP 프록시의 전달 캐시를 표시합니다. delete : 하드웨어 캐시가 삭제되었지만 소프트웨어 캐시가 시간 초과되지 않는 항목을 표시합니다. nonsync : 처리되었지만 아직 하드웨어 캐시에 동기화되지 않은 항목을 표시합니다. 동기화 : 이미 하드웨어 캐시에있는 항목을 표시합니다. 여과 조건이 지정되지 않으면 모든 항목이 표시됩니다. static : 정적 멀티 캐스트 캐시 항목 만 표시합니다.
[**no**] **debug ip igmp-proxy** *[error / event / packet]*	IGMP 프록시 디버그 스위치를 활성화 또는 비활성화합니다.

다음 예에서는 IGMP 프록시의 전달 캐시를 표시하는 방법을 보여줍니다.

```
Switch# show ip igmp-proxy mcache
Codes: '+' synchronization, '-' deleted, 'S' static
       '^' unsynchronization

Item 1: Group 225.1.1.2
   +(192.168.213.163, 2, G3/24)
    VLAN 3,4
```

IGMP 프록시 구성 예

네트워크 토폴로지는 그림 1 에 나와 있습니다.



스위치 구성 :

(1) IGMP 스누핑 및 IGMP 프록시를 활성화합니다.

Switch_config # ip igmp-snooping

Switch_config # ip igmp-proxy enable

(2) VLAN 2 를 표시된 VLAN 3 의 에이전트 VLAN 으로 추가합니다.

Switch_config # ip igmp-proxy agent-vlan 2 client - VLAN map 3

MLD-Snooping

IPv6 Multicast 개요

MLD 스누핑의 임무는 VLAN 에 IPv6 그룹 주소의 전달 관계를 유지하고 멀티 캐스트 그룹의 변경과 동기화하여 멀티 캐스트 그룹의 토폴로지에 따라 데이터를 전달할 수있게하는 것입니다. 이 기능에는 MLD 스누핑 패킷 모니터링, 그룹 주소와 VLAN 간의 테이블 유지, MLD 스누핑 호스트와 MLD 스누핑 라우터의 동일성 유지 및 플러딩 문제 해결이 포함됩니다.

L2 장치가 MLD 스누핑을 실행하지 못하면 멀티 캐스트 데이터는 두 번째 계층에서 브로드 캐스팅됩니다. L2 장치가 MLD 스누핑을 실행하면 알려진 멀티 캐스트 그룹의 멀티 캐스트 데이터는 두 번째 계층에서 브로드 캐스트되지 않고 지정된 수신기로 보내지고 알 수없는 멀티 캐스트 데이터는 삭제됩니다.

메모:

MLD-snooping 은 MLD-Snooping 의 Query 또는 Report 패킷을 모니터링하여 위에서 언급 한 문제를 해결하므로 MLD 스누핑은 멀티 캐스트 라우터가있는 경우에만 정상적으로 작동 할 수 있습니다

MLD-Snooping Multicast 구성 목록

- 활성화/비활성화 MLD-Snooping
- 활성화/비활성화 멀티 캐스트 그룹의 하드웨어 전달 요청
- 추가/삭제 VLAN 의 정적 멀티 캐스트 주소
- MLD-Snooping 의 라우터 수명 시간 구성
- MLD-Snooping 응답 시간 타이머 구성
- 정적 멀티 캐스트 라우터의 포트 구성
- 즉각 종료 기능 구성하기
- MLD-Snooping 모니터링 및 유지 관리

MLD-Snooping Multicast 활성화 / 비활성화

전역 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld snooping	MLD-snooping 멀티 캐스트를 활성화합니다.
no ipv6 mld snooping	MLD 스누핑을 비활성화합니다.

메모:

MLD-Snooping 이 활성화되고 멀티 캐스트 패킷을 찾지 못하면 대상 주소가 등록되지 않은 멀티 캐스트 패킷이 삭제됩니다.

멀티 캐스트 그룹의 하드웨어 전달 요청 활성화 / 비활성화

global configuration mode 에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld-snooping solicitation	멀티 캐스트 그룹의 하드웨어 포워드를 가능하게합니다.
no ipv6 mld-snooping solicitation	멀티 캐스트 그룹의 하드웨어 포워드를 비활성화합니다.

VLAN 의 정적 멀티 캐스트 주소 추가 / 취소

global configuration mode 에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf*	VLAN의 정적 멀티 캐스트 주소를 추가합니다.
no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf*	VLAN의 정적 멀티 캐스트 주소를 제거합니다.

MLD-Snooping 의 라우터 수명 시간 구성

Global configuration mode 에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld-snooping timer router-age *timer_value*	MLD-Snooping 의 라우터 수명을 구성합니다.
no ipv6 mld-snooping timer router-age	MLD-Snooping 의 기본 라우터 수명을 재개합니다.

메모:

이 타이머의 구성은 MLD-Snooping 의 쿼리 기간 구성을 참조해야하며 쿼리 기간보다 커야합니다.
라우터 수명 타이머를 쿼리 기간의 세 배가되도록 구성하는 것이 좋습니다.
MLD 스누핑의 기본 라우터 수명은 260 초입니다..

MLD-Snooping 응답 시간 타이머 구성

Global configuration mode 에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld-snooping timer response-time *timer_value*	MLD-Snooping 의 응답 시간을 구성합니다.

no ipv6 mld-snooping timer response-time	MLD-Snooping 의 기본 응답 시간을 재개합니다.

메모:

타이머의 값을 너무 작게 구성할 수 없거나 멀티 캐스트 통신이 불안정 할 수 있습니다.
MLD 스누핑의 기본 응답 시간은 15 초입니다.

정적 멀티 캐스트 라우터의 포트 구성

Global configuration mode 에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld-snooping vlan *WORD* **mrouter** interface *inft_name*	Vlan **word** 를 MLD 스누핑의 고정 멀티캐스트 라우터 포트에 구성합니다.
no ipv6 mld-snooping vlan *WORD* **mrouter** interface *inft_name*	Vlan **word** 를 MLD 스누핑의 고정 멀티테스트 라우터 포트에 구성을 취소 합니다.

즉각 종료 활성화 / 비활성화

Global configuration mode 에서 다음 명령을 실행하십시오.

명령어	설명
ipv6 mld-snooping vlan *WORD* **immediate-leave**	즉시 휴가 기능을 사용합니다
no ipv6 mld-snooping vlan *WORD* **immediate-leave**	기본 구성을 다시 시작합니다

MLD 스누핑 멀티 캐스트 모니터링 및 유지 보수

EXEC 모드에서 다음 명령을 실행하십시오.:

명령어	설명
show ipv6 mld-snooping	MLD-Snooping 의 구성을 표시합니다.
show ipv6 mld-snooping timer	MLD-Snooping 의 시계를 표시합니다.
show ipv6 mld -snooping groups	MLD-Snooping 의 멀티 캐스트 그룹을 표시합니다.
show ipv6 mld-snooping statistics	MLD-Snooping 의 통계 정보를 표시합니다.
show ipv6 mld-snooping vlan *WORD*	VLAN 에 MLD-Snooping 의 구성을 표시합니다.

show ipv6 mld-snooping mac	MLD 스누핑에 의해 기록 된 멀티 캐스트 MAC 주소를 표시합니다.

MLD-Snooping 정보가 아래와 같이 표시됩니다.

```
#show ipv6 mld-snooping

Global MLD snooping configuration:
Globally enable       : Enabled
Querier               : Enabled
Querier address       : FE80::3FF:FEFE:FD00:1
Router age            : 260 s
Response time         : 10 s
Handle Solicitation   : Disabled

Vlan 1:
    Running
    Routers: SWITCH(querier);
```

MLD-Snooping 의 멀티 캐스트 그룹이 표시됩니다.

```
#show ipv6 mld--snooping groups

Vlan Group            Type Port(s)
---- --------------- ---- -------------------------------------
   1 FF02::1:FF32:1B9B MLD  G2/23
   1 FF02::1:FF00:2   MLD  G2/23
   1 FF02::1:FF00:12 MLD  G2/23
   1 FF02::1:FF13:647D MLD  G2/23
   2 FF02::1:FF00:2   MLD  G2/22
   2 FF02::1:FF61:9901 MLD  G2/22
```

MLD-Snooping 의 타이머가 표시됩니다.

```
#show ipv6 mld-snooping timers

vlan 1 Querier on port 0 : 251
#
```

Querier on port 0: 251 meaning the router age timer times out.

vlan 2 multicast address 3333.0000.0005 response time : This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

MLD 스누핑 통계 정보는 다음과 같습니다.

```
#show ipv6 mld-snooping statistics
 vlan 1
    v1_packets:0         quantity of v1 packets
    v2_packets:6         quantity of v2 packets
    v3_packets:0         quantity of v3 packets
    general_query_packets:5     Quantity of general query packets
    special_query_packets:0     Quantity of special query packets
    listener_packets:6       Quantity of Report packets
      done_packets:0     Quantity of Leave packets
      err_packets:0      Quantity of error packets
```

MLD-Snooping 프록시가 아래에 표시됩니다.

```
 #show ipv6 mld-snooping mac
Vlan Mac               Ref Flags
---- --------------- ---- ------
   1 3333:0000:0001     1    2
   2 3333:ff61:9901     1    0
        FF02::1:FF61:9901
   1 3333:0000:0002     1    2
   1 3333:ff00:0002     1    0
        FF02::1:FF00:2
   1 3333:ff00:0012     1    0
        FF02::1:FF00:12
   1 3333:ff13:647d     1    0
        FF02::1:FF13:647D
   1 3333:ff32:1b9b     1    0
        FF02::1:FF32:1B9B
   2 3333:ff00:0002     1    0
        FF02::1:FF00:2
   1 3333:ff00:0001     1    2
   1 3333:ff8e:7000     1    2
```

OAM 구성

OAM 개요

IEEE 802.3ah 의 EFM OAM 은 단일 링크에서 지점 간 링크 문제 / 성능 감지 기능을 제공합니다. 그러나 EFM OAM 을 EVC 에 적용 할 수 없으므로 터미널 간 이더넷 모니터링을 실현할 수 없습니다. OAM PDU 는 다른 인터페이스로 전달 될 수 없습니다. IEEE 802.3ah 에 의해 규제되는 이더넷 OAM 은 상대적으로 느린 프로토콜입니다. 최대 전송 속도는 초당 10 프레임이고 최소 전송 속도는 초당 1 프레임입니다..

OAM 프로토콜의 속성

- 이더넷 OAM 장치 및 OAM 속성 지원
  이더넷 OAM 연결 프로세스는 OAM 엔티티가 원격 장치의 OAM 엔티티를 찾고 안정된 세션이 구성 될 때 발견 단계로 호출됩니다. 단계 동안 연결된 이더넷 OAM 엔티티는 정보 OAM PDU 와 상호 작용하여 OAM 모드, 이더넷 OAM 구성 정보 및 로컬 노드 지원 이더넷 OAM 용량을 서로보고합니다. 두 터미널의 이더넷 OAM 에서 루프백 구성, 단방향 링크 감지 구성 및 링크 이벤트 구성이 전달 된 경우 이더넷 OAM 프로토콜이 링크 계층에서 작동하기 시작합니다.
- 링크 모니터링
  이더넷 OAM 은 이벤트 알림 OAM PDU 를 통해 링크 모니터링을 수행합니다. 링크에 문제가 있고 로컬 링크가 문제를 모니터링하면 로컬 링크는 정상 링크 이벤트를보고하기 위해 이벤트 알림 OAM PDU 를 피어 이더넷 OAM 으로 전송합니다. 관리자는 링크 모니터링을 통해 네트워크 상태를 동적으로 알 수 있습니다. 일반 링크 이벤트의 정의는 표 1 에 나와 있습니다.

표 1 정상 링크 이벤트의 정의

정상 링크 이벤트	정의
Period event of error signal	신호 번호 N 을 마침표로 지정합니다. N 개의 신호가 수신되면 오류 신호 수가 정의 된 임계 값을 초과합니다.
Error frame event	단위 시간 동안 오류 프레임 수가 정의 된 임계 값을 초과합니다.
Period event of error frame	프레임 번호 N 을 마침표로 지정합니다. N 프레임을 수신하면 오류 프레임 수가 정의 된 임계 값을 초과합니다.
Second frame of error frame	오류 프레임의 초 수가 지정된 M 초에 정의 된 임계 값을 초과하도록 지정합니다.

- 원격 문제 표시
  이더넷의 문제, 특히 물리적 네트워크 통신이 계속되는 동안 네트워크 성능이 느려지는 경우를 확인하는 것은 어렵습니다. OAM PDU 는 이더넷 OAM 엔티티가 문제 정보를 피어에 전송할 수 있도록 플래그 도메인을 정의합니다. 플래그는 다음과 같은 긴급한 링크 이벤트를 나타낼 수 있습니다.:

- Link Fault : 물리 계층은 로컬 DTE 의 수신 방향이 효과가 없음을 감지합니다. 문제가 발생하면 물리 계층의 일부 장치가 단방향 작업을 지원하고 원격 OAM 에서 문제 알림을 허용합니다.
- Dying Gasp : 복구 할 수없는 로컬 오류 (예 : OAM 종료)가 발생하면 인터페이스가 오류 비활성 상태가 된 다음 종료됩니다.
- 중요 이벤트 : 불확실한 중대한 이벤트가 발생합니다 (중요한 이벤트는 제조업체가 지정합니다).

정보 OAM PDU 는 이더넷 OAM 연결 중에 지속적으로 전송됩니다.Local OAM entity 는 Local 중요 링크 이벤트를 정보 OAM PDU 를 통해 원격 OAM entity 에 보고 할 수있다. 따라서 관리자는 동적으로 링크의 상태를 알 수 있으며 해당 오류를 처리 할 수 있습니다.

- 원격 루프백

  OAM 은 옵션 인 링크 계층 레벨 루프백 모드를 제공하며 비 OAM-PDU 루프백을 통해 오류 위치 및 링크 성능 테스트를 수행합니다. 원격 루프백은 OAM 연결이 생성 된 후에 만 실현됩니다. OAM 연결이 생성 된 후, 활성 모드의 OAM 엔티티는 원격 루프백 명령을 트리거하고 피어 엔티티는 명령에 응답합니다. 원격 터미널이 루프백 모드에 있으면 OAM PDU 패킷 및 일시 중지 패킷을 제외한 모든 패킷이 이전 경로를 통해 다시 전송됩니다. 오류 위치 및 링크 성능 테스트를 수행 할 수 있습니다. 원격 DTE 가 원격 루프백 모드에 있으면 로컬 또는 원격 통계 데이터를 쿼리하고 무작위로 비교할 수 있습니다. 쿼리 동작은 루프백 프레임이 원격 DTE 로 전송되기 전에, 언제 또는 후에 수행 될 수있다. 정기 루프백 검사는 네트워크 오류를 즉시 감지 할 수 있지만 세그먼트 루프백 검사는 이러한 네트워크 오류를 찾은 다음 이러한 오류를 제거하는 데 도움이됩니다..

- 모든 MIB 변수의 라운드 쿼리는 30 장에설명되어있습니다. (802.3)

OAM 모드

장치는 두 가지 모드, 즉 활성 모드와 수동 모드를 통해 OAM 연결을 수행 할 수 있습니다. 다른 모드의 장치 용량은 표 2 에서 비교됩니다. 수동 모드의 OAM entity 는 피어 OAM entity 의 연결 요청을 기다려야하는 반면, 활성 모드의 OAM entity 만 연결 프로세스를 트리거 할 수 있습니다. 원격 OAM 발견 프로세스가 완료된 후, 원격 entity 가 활성 모드 인 경우 활성 모드의 로컬 entity 는 모든 OAM PDU 패킷을 전송할 수 있지만 원격 entity 가 수동 모드 인 경우 활성 모드의 로컬 entity 작동은 제한됩니다. 활성 모드의 장치가 수동 원격 entity 가 전송 한 원격 루프백 명령과 변수 요청에 반응하지 않기 때문입니다..

표 2 액티브 및 패시브 모드의 장치 용량 비교

Capacity	Active Mode	Passive Mode
이더넷 OAM 검색 프로세스 초기화	Yes	No
OAM 검색 초기화 프로세스에 응답	Yes	Yes
정보 OAM PDU 패킷 전송	Yes	Yes
이벤트 통지 OAM PDU 패킷 전송 허용	Yes	Yes
가변 요청 OAM PDU 패킷 전송 허용	Yes	No

가변 응답 OAM PDU 패킷 전송 허용	Yes	Yes
Loopback Control OAM PDU 패킷 전송 허용	Yes	No
루프백 제어 OAM PDU 에 대한 응답	Yes , 피어 터미널은 활성 모드 여야합니다.	Yes
지정된 OAM PDU 전송 허용	Yes	Yes

이더넷 OAM 연결이 구성된 후 두 터미널에있는 OAM entities 는 Information OAM PDU 패킷을 전송하여 연결을 유지합니다. 피어 OAM entity 로부터의 정보 OAM PDU 패킷이 5 초 내에 수신되지 않으면, 연결 시간 초과 및 새로운 OAM 연결이 구성 될 필요가있다.

OAM 패킷의 구성 요소

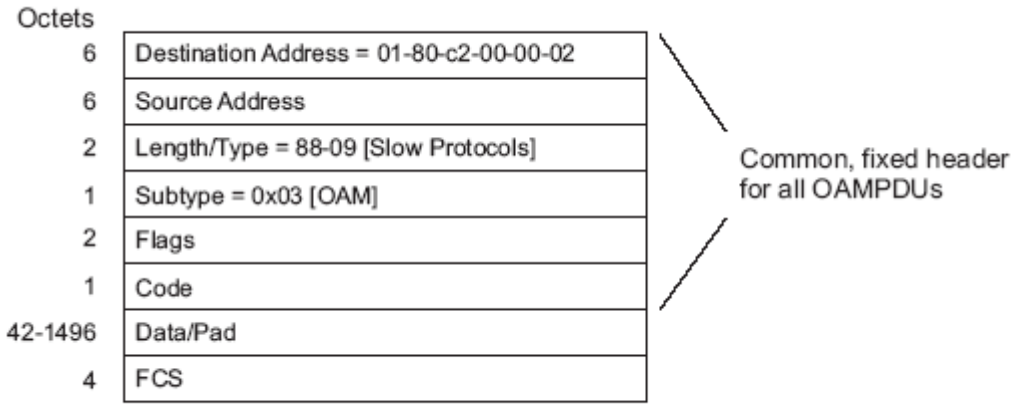


Figure 57–9—OAMPDU frame structure

그림 1 OAM 패킷의 구성 요소

OAM 패킷의 필드의 의미는 다음과 같습니다:

- 목적지 주소 : 이더넷 OAM 패킷의 목적지 MAC 주소를 의미합니다.
- 원본 주소 : 이더넷 OAM 패킷의 원본 MAC 주소
  이것은 송신기 터미널 포트의 MAC 주소이며 또한 유니 캐스트 MAC 주소입니다.MAC address.
- 길이 / 유형 : 항상 유형 인코딩을 채택합니다. 이더넷 OAM 패킷의 프로토콜 유형은 0x8809 입니다.
- 서브 타입 : 이더넷 OAM 패킷을위한 프로토콜의 서브 타입은 0x03 이다.
- Flags : Ethernet OAM 엔티티의 상태가 표시되는 도메인
- 코드 : OAMPDU 패킷의 유형이 표시된 도메인
- 데이터 / 패드 : OAMPDU 데이터 및 패드 값을 포함하는 도메인
- FCS : 프레임의 체크섬

표 3 CODE 도메인 유형

CODE	OAMPDU
00	정보
01	이벤트 알림
02	변수 요청
03	가변 응답
04	루프백 제어
05-FD	제한된
FE	조직 별
FF	제한된

정보 OAM PDU 패킷은 OAM 엔티티의 상태에 관한 정보를 원격 OAM 엔티티로 전송하여 OAM 연결을 유지하는 데 사용됩니다.

이벤트 알림 OAMPDU 패킷은 링크를 모니터링하고 로컬 OAM 엔티티와 원격 OAM 엔티티 간의 링크에서 발생한 문제를보고하는 데 사용됩니다.

루프백 제어 OAMPDU 패킷은 주로 원격 장치의 OAM 루프백 상태를 포함하여 원격 루프백을 제어하는 데 사용됩니다. 패킷에는 루프백 기능을 활성화 또는 비활성화하는 정보가 들어 있습니다. 포함 된 정보에 따라 원격 루프백을 열거 나 종료 할 수 있습니다.

OAM 구성 작업 목록

- 인터페이스에서 OAM 활성화
- 원격 OAM 루프백 활성화
- OAM 링크 모니터링 구성
- 원격 OAM 엔터티로부터 장애 통지 구성
- OAM 프로토콜에 대한 정보 표시

OAM 구성 작업

3.1.1 인터페이스에서 OAM 활성화

OAM 을 사용하려면 다음 명령을 실행:

순서	명령어	설명
1단계	**config**	글로벌 구성 모드로 들어갑니다..
2단계	**interface** intf-type intf-id	인터페이스 구성 모드를 시작합니다.
3단계	**ethernet oam**	인터페이스에서 이더넷 OAM 을 활성화합니다.
4단계	**ethernet oam** [**max-rate** oampdus | **min-rate** seconds | **mode** {**active** | **passive**} | **timeout** seconds]	선택적 OAM 매개 변수 구성: ● max-rate 매개 변수는 초당 전송되는 OAMPDU의 최대 수를 구성하는 데 사용됩니다. 범위는 1 - 10이며 기본값은 10입니다.

		• 최소 속도 매개 변수는 OAMPDU의 최소 전송 속도를 구성하는 데 사용됩니다. 그 단위는 초입니다. 범위는 1 - 10이며 기본값은 1입니다. • 모드 {활성 | passive} 매개 변수는 OAM의 모드를 구성하는 데 사용됩니다. OAM 연결은 적어도 하나의 인터페이스가 활성 모드에있는 경우에만 두 인터페이스간에 구성 될 수 있습니다 • timeout 매개 변수는 OAM 연결의 시간 초과 시간을 구성하는 데 사용됩니다. 범위는 1 - 30 초이며 기본값은 1 초입니다.

No Ethernet oam 시 기능 비활성화 됩니다. .

원격 OAM 루프백은 집계 인터페이스에 속한 실제 인터페이스에서 활성화 할 수 없습니다.

원격 OAM 루프백 활성화

인터페이스에서 원격 루프백을 활성화하는 절차는 다음 표에 나와 있습니다.

순서	**명령어**	**설명**
1단계	**config**	글로벌 구성 모드로 들어갑니다..
2단계	**interface** intf-type intf-id	인터페이스 구성 모드로 들어갑니다..
3단계	**ethernet oam remote-loopback {supported | timeout** seconds**}**	원격 OAM 에서 선택적 루프백 매개 변수를 구성합니다 • 지원되는 매개 변수는 인터페이스가 이더넷 OAM의 원격 루프백을 지원할 수있게하는 데 사용됩니다. 원격 루프백은 기본적으로 지원되지 않습니다. • timeout 매개 변수는 원격 루프백의 시간 초과 시간을 구성하는 데 사용됩니다. 범위는 1 - 10이며 기본값은 2입니다..
4단계	**exit**	인터페이스 구성 모드를 종료합니다..
5단계	**exit**	global 구성 모드를 종료합니다..
6단계	**ethernet oam remote-loopback {start | stop} interface** intf-type intf-id	인터페이스에서 원격 루프백을 활성화하거나 비활성화합니다.

원격 OAM 루프백은 집계 인터페이스에 속한 실제 인터페이스에서 활성화 할 수 없습니다.

OAM 링크 모니터링 구성

OAM 링크 모니터링의 낮은 임계 값 및 높은 임계 값을 구성 할 수 있습니다.
인터페이스에서 OAM 링크 모니터링을 구성하는 절차는 다음 표에 나와 있습니다:

순서	**명령어**	**설명**
1단계	**config**	글로벌 구성 모드로 들어갑니다.
2단계	**interface** intf-type intf-id	인터페이스 구성 모드를 시작합니다
3단계	**ethernet oam link-monitor**	인터페이스에서 링크 모니터링을 활성화합니다. 링크 모니터링은 기본적으로 지원됩니다..
4단계	**ethernet oam link-monitor symbol-period {threshold {high** { symbols **|none} | low** {symbols}} **| window** symbols}	오류 링크 이벤트를 트리거하는 오류 신호의주기적인 이벤트의 상한 및 하한 임계 값을 구성합니다.. 임계 값 상위 매개 변수는 상위 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1 ~ 65535 이며 기본값은 none 입니다.. 임계 값 상위 매개 변수는 낮은 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0 ~ 65535 이며 기본값은 1 입니다 window 매개 변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 창 크기의 단위는 100M 신호의 번호입니다. 창 크기는 1000M 이더넷 인터페이스에서 10에서 600 사이이며이 경우 기본값은 10이며 창 크기는 100M 이더넷 인터페이스에서 1에서 60 사이이며이 경우 기본값은 1입니다..
5단계	**ethernet oam link-monitor frame {threshold {high** { symbols **|none} | low** {symbols}} **| window** symbols}	오류 프레임의 링크 이벤트를 트리거하는 오류 프레임 이벤트의 상한 및 하한 임계 값을 구성합니다. 임계 값 상위 매개 변수는 상위 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1 ~ 65535 이며 기본값은 none 입니다. 임계 값 상위 매개 변수는 낮은 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0 ~ 65535 이며 기본값은 1 입니다.

		window 매개 변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 그 단위는 초입니다. 범위는 1 - 60 이며 기본값은 1 입니다.
6단계	**ethernet oam link-monitor frame-period {threshold {high** { symbols **|none} | low** {symbols}} **| window** symbols}	오류 프레임 기간의 링크 이벤트를 트리거하는 오류 프레임의 기간 이벤트의 상한 및 하한 임계 값을 구성합니다. 임계 값 상위 매개 변수는 상위 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1 ~ 65535 이며 기본값은 none 입니다. 임계 값 상위 매개 변수는 낮은 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0 ~ 65535 이며 기본값은 1 입니다. window 매개 변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 창 크기의 단위는 14881 프레임의 수입니다. 창 크기는 1000M 이더넷 인터페이스에서 100과 6000 사이의 범위이며이 경우 기본값은 100입니다. 창 크기는 100M 이더넷 인터페이스에서 10에서 600 사이이며이 경우 기본값은 10입니다.
7 단계	**ethernet oam link-monitor frame-seconds {threshold {high** { symbols **|none} | low** {symbols}} **| window** symbols}	오류 프레임의 두 번째 이벤트의 상위 및 하위 임계 값을 구성합니다.이 임계 값은 오류 프레임의 초의 링크 이벤트를 트리거합니다. 임계 값 상위 매개 변수는 상위 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1 - 900 이며 기본값은 none 입니다. 임계 값 낮음 매개 변수는 낮은 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0 에서 900 사이이며 기본값은 1 입니다. window 매개 변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 그 단위는 초입니다. 범위는 10 에서 900 사이이며 기본값은 60 입니다.
8 단계	**ethernet oam link-monitor receive-crc {threshold {high** { symbols **|none} | low** {symbols}} **| window** symbols}	CRC 체크섬 오류의 링크 이벤트를 트리거하는 오류 CRC 프레임 이벤트의 상한 및 하한 임계 값을 구성합니다.

		임계 값 상위 매개 변수는 상위 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1 ~ 65535 이며 기본값은 none 입니다. 임계 값 상위 매개 변수는 낮은 임계 값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0 ~ 65535 이며 기본값은 1 입니다. window 매개 변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 그 단위는 초입니다. 범위는 1 - 180 이며 기본값은 10 입니다.
9단계	**ethernet oam link-monitor**	로컬 링크 모니터링을 사용합니다. 링크 모니터링 기능이 지원되면 로컬 링크 모니터링이 자동으로 활성화됩니다.

원격 OAM 엔티티에서 문제점 통지 구성

인터페이스에서 오류 비활성화 조치를 구성 할 수 있습니다. 다음과 같은 경우 로컬 인터페이스는 errdisabled 상태가됩니다.

1. 로컬 인터페이스에서 정상 링크 이벤트의 상위 임계 값을 초과했습니다.

2. 로컬 인터페이스를 연결하는 원격 인터페이스는 errdisabled 상태가됩니다.

3. 로컬 인터페이스를 연결하는 원격 인터페이스의 OAM 기능은 관리자가 종료합니다. 다음 표에는 인터페이스에서 원격 OAM 문제 표시를 구성하는 절차가 나와 있습니다.:

순서	**명령어**	**설명**
1단계	**config**	글로벌 구성 모드로 들어갑니다..
2단계	**interface** intf-type intf-id	인터페이스 구성 모드를 시작합니다..
3단계	**ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface**	인터페이스에서 원격 OAM 문제의 트리거 동작을 구성합니다. critical-event 매개 변수는 지정되지 않은 치명적인 이벤트가 발생할 때 인터페이스가 errdisable 상태로 들어가도록하는 데 사용됩니다. dying-gasp 매개 변수는 로컬 인터페이스에서 일반 링크 이벤트의 상위 임계 값이 초과되거나 로컬 인터페이스를 연결하는 원격 인터페이스가 errdisabled 상태가되거나 또는 로컬 인터페이스를

		연결하는 원격 인터페이스의 OAM 기능은 관리자가 종료합니다. link-fault 매개 변수는 수신기가 신호 손실을 감지했을 때 errdisable 상태로 들어가도록 인터페이스를 활성화하는 데 사용됩니다.

스위치는 LINK FAULT 패킷 및 중요 이벤트 패킷을 생성 할 수 없습니다. 그러나 이러한 패킷은 원격 터미널에서 수신 된 경우 처리됩니다. 스위치는 Dying Gasp 패킷을 송수신 할 수 있습니다. 로컬 포트가 errdisable 상태로 들어가거나 관리자에 의해 닫히거나 로컬 포트의 OAM 기능이 관리자에 의해 닫히면 Dying Gasp 패킷은 로컬 포트를 연결하는 원격 터미널로 전송됩니다.

OAM 프로토콜에 대한 정보 표시

표 4 OAM 프로토콜에 대한 정보 표시

명령어	설명
show ethernet oam discovery interface [intf-type intf-id]	모든 인터페이스 또는 지정된 인터페이스에서 OAM 검색 정보를 표시합니다..
show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id]	모든 인터페이스 또는 지정된 인터페이스에 대한 OAM 통계 정보를 표시합니다. ● pdu 매개 변수는 OAM 패킷의 코드 도메인 값에 따라 OAM 패킷을 분류하고 계산하는 데 사용됩니다. ● link-monitor 매개 변수는 일반적인 링크 이벤트의 자세한 통계 정보를 표시하는 데 사용됩니다. ● remote-failure 매개 변수는 원격 문제에 대한 자세한 통계 정보를 표시합니다.
show ethernet oam configuration interface [intf-type intf-id]	모든 인터페이스 또는 지정된 인터페이스에 대한 OAM 구성 정보를 표시합니다.
show ethernet oam runtime interface [intf-type intf-id]	모든 인터페이스 또는 지정된 인터페이스에 대한 OAM 실행 정보를 표시합니다..

구성 예

네트워크 환경 요구 사항

사용자 액세스 측면에서 제품 수신 오류 프레임에 대한 정보를 캡처하기 위해 두 개의 제품 스위치가 연결되는 인터페이스에서 OAM 프로토콜을 구성해야합니다..

네트워크 토폴로지

Switch A Switch B

그림 2 네트워크 토폴로지

구성 절차

Configuring 제품 switch A:

Switch_config_g0/1#ethernet oam

Switch_config_g0/1#ethernet oam mode passive

Switch_config_g0/1#ethernet oam link-monitor frame threshold low 10

Switch_config_g0/1#ethernet oam link-monitor frame window 30

Switch_config_g0/1#show ethernet oam configuration int g0/1

GigaEthernet0/1

General

Admin state : enabled

Mode : passive

PDU max rate : 10 packets/second

PDU min rate : 1 seconds/packet

Link timeout : 1 seconds

High threshold action: no action

Remote Failure

Link fault action : no action

Dying gasp action : no action

Critical event action: no action

Remote Loopback

Is supported : not supported

Loopback timeout : 2

Link Monitoring

Negotiation : supported

Status : on

Errored Symbol Period Event

Window : 10 * 100M symbols

Low threshold : 1 error symbol(s)

High threshold : none

Errored Frame Event

Window : 30 seconds

Low threshold : 10 error frame(s)

High threshold : none

Errored Frame Period Event

Window : 100 * 14881 frames

Low threshold : 1 error frame(s)

High threshold : none

Errored Frame Seconds Summary Event

Window : 60 seconds

Low threshold : 1 error second(s)

High threshold : none

Errored CRC Frames Event

Window : 1 seconds

Low threshold : 10 error frame(s)

High threshold : none

Configuring 제품 switch B:

Switch_config_g0/1#ethernet oam

Switch_config_g0/1#show ethernet oam statistics link-monitor int g0/1

GigaEthernet0/1

Local Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:
No errored frame seconds summary event happened yet.

Errored CRC Frames Event:
No errored CRC frame event happened yet.

Remote Link Events:

Errored Symbol Period Event:
No errored symbol period event happened yet.

Errored Frame Event:
No errored frame event happened yet.

Errored Frame Period Event:
No errored frame period event happened yet.

Errored Frame Seconds Summary Event:
No errored frame seconds summary event happened yet.
Errored CRC Frames Event:
No errored CRC frame event happened yet.

CFM 구성

CFM 구성 작업 목록

- 유지 관리 도메인 추가
- Maintenance Association 추가
- MIP 추가 (Maintenance Domain Intermediate Point)
- MEP 추가(Maintenance association End Point)
- CFM 추가

CFM 유지 관리 작업 목록

- 루프백 기능 사용
- 링크 추적 기능 사용

CFM 구성

유지 보수 도메인 추가

구성 모드 : Global

명령어	설명
ethernet cfm md mdnf string <char_string> [**level** <0-7> | **creation** <MHF_creation_type> | **sit** <sender_id_type> | **ip** <IP_address>]	이름이 char_string 인 유지 보수 도메인을 추가합니다. 메모: 【1】 유지 관리 도메인을 추가 한 후 시스템이 유지 관리 도메인 구성 모드로 들어갑니다.

유지보수 협력 추가

구성 모드 : maintenance domain

명령어	설명
ma manf string <char_string> **ci** {100ms | 1s | 10s | 1min | 10min} **meps** <mepids> [**vlan** <1-4094> | **creation** <MHF_creation_type> | **sit**	이름이 char_string 인 유지 보수 연결을 추가합니다.

<sender_id_type> | **ip** <IP_address>]	

MDIP 추가 (Maintenance Domain Intermediate Point)

구성 모드 : physical interface

명령어	설명
ethernet cfm mip add level *<0-7>* [vlan *<1-4094>*]	지정된 VLAN 및 계층 적 MIP를 지정된 물리적 인터페이스에 추가합니다.

MEP 추가 (Maintenance association End Point)

구성 모드 : physical interface

명령어	설명
ethernet cfm mep add mdnf string *<char_string>* **manf string** *<char_string>* **mepid** *<1-8191>* [**direction** *{up | down}* **| ip** *<ip_address>*]	지정된 유지 관리 도메인과 MEP를 지정된 물리적 인터페이스에 추가합니다..**ethernet cfm mep add mdnf string** *<char_string>* **manf string** *<char_string>* **mepid** *<1-8191>* **rmpid** *<1-8191>* [**direction** *{up | down}* **| ip** *<ip_address>*]

CFM 시작

구성 모드 : Global

명령어	설명
ethernet cfm *{enable}*	CFM 시작.

CFM 유지 관리

루프백 기능 사용

구성 모드 : EXEC

명령어	설명
ethernet cfm loopback mdnf string <char_string> **manf string** <char_string> **mepid** <1-8191> **mac**	지정된 MEP를 사용하여 루프백을 수행합니다.

<AA:BB:CC:DD:EE:FF> **number** <1-64>	

링크 추적 기능 사용

구성 모드 : EXEC

명령어	설명
ethernet cfm linktrace mdnf string <char_string> **manf string** <char_string> **mepid** <1-8191> **mac** <AA:BB:CC:DD:EE:FF> [**ttl** {1-255} | **fdb-only** {yes}]	지정된 MEP를 사용하여 루프백을 수행합니다.

구성 예

이름이 customer 이고 계층이 5 인 유지 관리 도메인을 추가하고 vlan1 에 대한 고객 1 유지 관리 연결을 구성하고 유지 관리 연결의 CCM 전송 간격을 1 초로 구성한 다음 MEPID 가 2009 인 MEP 를 실제 포트 1 에 추가합니다.

Switch_config#ethernet cfm md mdnf string mdn customer level 5

Switch_config_cfm#ma manf string man customer1 vlan 1 ci 1s meps 1-2,2009

Switch_config_cfm#interface g0/1

Switch_config_g0/1#ethernet cfm mep add mdnf string mdn customer manf string man customer1 mepid 2009 direction DOWN

Switch_config_g0/1#exit

Switch_config#ethernet cfm enable

MACFF 구성

구성 작업

MACFF 는 스위치 내 동일한 VLAN 의 다운 링크 포트를 상호 액세스 패킷 교환과 분리하여 DHCP 서버를 통해 클라이언트의 기본 게이트웨이에 할당 한 다음 다운 링크 포트에 할당 할 수 있도록합니다. MACFF 는 다운 링크 포트간에 ARP 패킷을 캡처함으로써 다운 링크 포트가 ARP 를 학습하는 것을 방지 할 수 있습니다. MACFF 는 게이트웨이의 MAC 주소에 응답하여 모든 다운 링크 포트 간의 모든 상호 액세스 패킷이 게이트웨이를 통과하도록합니다.
Note: MACFF 는 DHCPR 스누핑을 지원해야하므로 MACFF 를 활성화하기 전에 DHCPR 스누핑이 정상적으로 작동하는지 확인해야합니다. 게이트웨이의 ICMP 리디렉션은 기본적으로 닫힙니다.
VLAN 관리 주소는 MACFF 사용 스위치로 구성되어야합니다..

- MACFF 활성화 또는 비활성화
- VLAN 에서 MACFF 사용
- VLAN 에서 MACFF 의 기본 AR 구성
- VLAN 에서 MACFF 의 다른 AR 구성
- 물리적 포트를 지정하여 MACFF 를 종료합니다.

MVC 활성화 / 비활성화

Global 모드에서 다음 명령을 실행하십시오..

명령어	설명
macff enable	MACFF 를 사용합니다.
no macff enable	기본 구성을 다시 시작합니다.

이 명령은 전역 구성 모드에서 MACFF 를 활성화하는 데 사용됩니다.이 명령을 실행하면 모든 ARP 패킷이 스위치로 수신됩니다.
Note: 이 명령을 구성하기 전에 DHCP-Snooping 이 활성화되어 있는지 확인해야합니다. 이 명령을 실행하기 전에 클라이언트가 스위치의 주소를 얻으면 스위치는 해당 바인딩 관계를 추가 할 수 없습니다.

VLAN 에서 MACFF 사용

VLAN 에서 MACFF 가 활성화되면 VLAN 의 모든 DHCP 스누핑 신뢰할 수없는 물리적 포트에서 수신 된 DHCP 패킷이 합법적으로 검사됩니다.
대상 IP 주소가 ARP 패킷을 수신하는 실제 포트가있는 DHCP 클라이언트의 IP 주소 인 경우 이러한 ARP 패킷은 삭제됩니다. ARP 응답 패킷 인 경우이 패킷도 삭제됩니다.
Note: MACFF 가 활성화 된 VLAN 은 관리 주소를 가지도록 구성해야합니다. DHCP 스누핑은이 VLAN 에서도 활성화되어야합니다..
Global 모드에서 다음 명령을 실행하십시오..

명령어	설명
macff vlan *vlan_id* **enable**	VLAN에서 MACFF를 활성화합니다.
no macff vlan *vlan_id* **enable**	VLAN의 MACFF를 비활성화합니다.

VLAN 에서 MACFF 의 기본 AR 구성

클라이언트에서 주소를 수동으로 구성하면 스위치는 MACFF 가 지정된 기본 게이트웨이로 기본 AR 을 자동으로 활성화합니다. 하나의 기본 AR 만 있습니다..
Global 모드에서 다음 명령을 실행하십시오..

명령어	설명
macff vlan *vlan_id* **default-ar** *A.B.C.D*	VLAN 에 MACFF 의 기본 AR 을 구성합니다.
no macff vlan *vlan_id* default-ar *A.B.C.D*	VLAN 에있는 MACFF 의 기본 AR 을 삭제합니다.

Note: 이 명령을 구성하기 전에 스위치에 클라이언트 바인딩 테이블을 추가하기 위해 **ip source binding xx-xx-xx-xx-xx-xx A.B.C.D interface name** 을 실행할 수 있습니다. 이렇게하지 않으면 MACFF 는 수동으로 구성된 클라이언트를 잘못된 클라이언트로 간주하고 MACFF 는이 클라이언트를 제공하지 않습니다.VLAN 에서 MACFF 의 다른 AR 구성
MACFF 의 다른 AR 이 구성된 후 MACFF 는 DHCP 클라이언트가 DHCP 서버가 할당 한 기본 게이트웨이를 통해 패킷을 전달하지 않고 이러한 AR 에 직접 액세스 할 수있게합니다.
이 기능은 클라이언트의 네트워크 세그먼트에있는 일부 서버 또는 다른 서비스 주소에 적용될 수 있습니다.
Global 모드에서 다음 명령을 실행하십시오..

명령어	설명
macff vlan *vlan_id* **other_ar** *A.B.C.D*	VLAN 에 MACFF 의 다른 AR 을 구성합니다.
no macff vlan *vlan_id* **other_ar** *A.B.C.D*	VLAN 에있는 MACFF 의 다른 AR 을 삭제합니다.

MACFF 디버깅

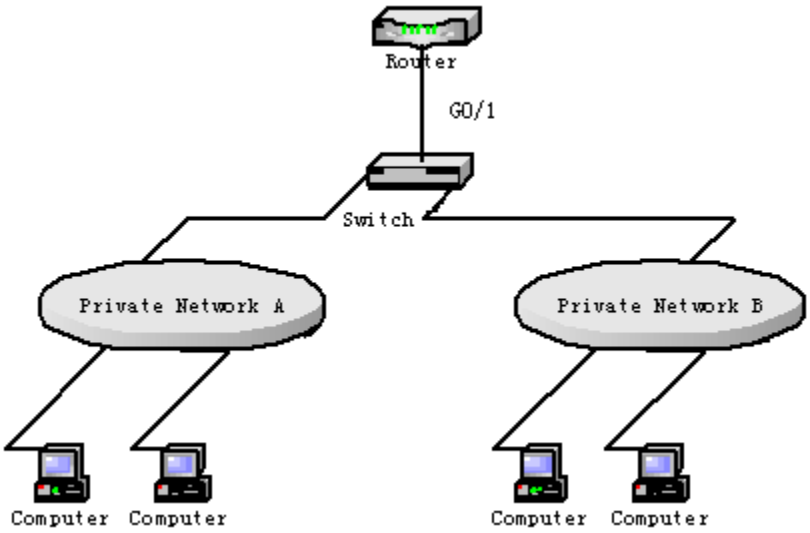
EXEC 모드에서 다음 명령을 실행하십시오..

명령어	설명

debug macff	Macff 디버깅 활성화합니다.
no debug macff	Macff 디버깅 비활성화합니다.

MACFF 구성 예

그림 1 에 네트워크 구성도를보고



네트워크 구성:

개인 네트워크 A 를 연결하는 VLAN 1 에서 MACFF 를 활성화합니다. DHCP 서버가 할당한 기본 게이트웨이는 192.168.2.1 입니다..

Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

Switch_config#macff enable

Switch_config#macff vlan 1 enable

사설망 B 를 연결하는 VLAN2 에서 MACFF 를 활성화합니다. DHCP 서버에서 할당 한 기본 게이트웨이는 192.168.2.2 입니다 (필요한 경우 기본 게이트웨이는 192.168.2.1 일 수도 있음).

Switch_config#arp 192.168.2.2 00:e0:0f:ea:74:ee vlan 2

Switch_config#ip dhcp-relay snooping vlan 2

Switch_config#macff vlan 2 enable

DHCP 서버, 기본 게이트웨이 및 기타 AR을 각각 연결하는 포트를 각각 신뢰할 수있게 구성합니다..

Switch_config_g0/1#dhcp snooping trust

VLAN 1 의 다운 링크 호스트 A 가 IP 및 기본 게이트웨이를 수동으로 구성한 경우 IP 주소는 192.168.2.102 이고 MAC 주소는 6c-62-6d-59-18-b7 입니다. 기본 게이트웨이 192.168.2.1 을 사용하면 MACFF 를 적용 할 수 있습니다.

(클라이언트가 수동으로 구성되어 있지 않으면이 단계가 수행되지 않습니다.)

Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1

Switch_config#ip source binding 6c-62-6d-59-18-b7 192.168.2.102 interface GigaEthernet0/1

Switch_config_g0/1#macff vlan 1 default-ar 192.168.2.1

MACFF 를 사용하는 VLAN 의 물리적 포트를 지정하여 MACFF 를 종료합니다..

Switch_config_g0/1#macff disable

클라이언트의 동일한 네트워크 세그먼트에있는 다른 AR 을 구성합니다. MACFF 는 클라이언트가 게이트웨이의 도움없이 직접 액세스를 수행 할 수있게합니다. (다른 AP 를 신뢰할 수있는 포트로 구성해야하는 포트)

Switch_config_g0/1#macff disable

2 계층 프로토콜 터널 구성하기

개요

2 계층 프로토콜 터널은 스위치의 양면 사이에 사용자가 스위치의 관련
2 계층 소프트웨어 모듈에 의해 영향을 받지 않고 자신의 네트워크에 지정된 2 계층 프로토콜을 전송 할 수 있습니다.

2 계층 프로토콜 터널 계층 구성하기

스위치 인터페이스에서 명령어를 사용하여 계층 2 프로토콜의 터널 기능을 구성 합니다.
구성 단계는 다음과 같습니다.

명령어	설명
configure	전역 구성 모드를 시작합니다.
interface *<intf_name>*	스위치의 인터페이스 구성모드를 시작합니다.
[**no**] **l2protocol-tunnel** *[stp]*	현재 stp 프로토콜의 터널기능을 스위치가 지원하며 2 계층을 사용합니다.
[CTRL] + Z	EXEC 모드로 나갑니다.
write	구성을 저장합니다.

2 계층 프로토콜 터널 구성 예제

A1 / A2 /는 코어 네트워크에 속하며, C1 / C2 는 두 곳에서 분산 된 스위치입니다. 고객은 자사의 네트워크 중 두 가지를 하나로 결합하고자 합니다.
 즉, 핵심 네트워크는 고객을 위한 명백한 전송 채널입니다. 사용자가 STP 의 명백한 전송을 실현하려면 각 스위치에서 다음 구성을 수행해야합니다.

1) 스위치A1의 g0/2, g0/1 과 g0/2이 모이고, 스위치A2 g0/1 와 g0/2가 트렁크 모드로 구성됩니다.

2) STP 프로토콜의 터널기능과 A2의 g0/2와 A1의 0/1이 접근하도록 구성되어 있습니다.

루프백 탐지 구성

루프백 탐지 개요

네트워크의 루프백은 브로드 캐스트, 멀티 캐스트 또는 유니 캐스트 패킷의 반복 전송을 유발하여 네트워크 리소스를 낭비하고 네트워크 고장을 일으킬 수 있습니다. 전술 한 트러블을 피하기 위해서는, 루프백 발생시에 네트워크 접속 및 구성을 사용자에게 신속하게 통지하고, 문제가있는 포트를 제어하는 검출 메커니즘을 제공 할 필요가있다. 루프백 탐지는이 포트에서 탐지 패킷을 전송하고이 패킷을이 포트에서 계속 수신 할 수 있는지 여부를 검사하여 테스트 대상 장치의 포트에서 루프백이 발생하는지 여부를 확인할 수 있습니다. 장치는 해당 포트에 루프백이 있음을 발견하면 관리자가 즉시 네트워크 문제를 감지 할 수 있도록 네트워크 관리 시스템에 즉시 경보를 전송할 수 있습니다. 따라서, 네트워크 단절의 장시간이 방지 될 수있다. 또한 루프백 탐지는 포트를 제어 할 수 있습니다. 실제 요구 사항에 따라 포트 차단, 포트 MAC 학습 금지 또는 오류 비활성화를 선택하여 해당 포트를 제어하고 루프백의 네트워크 영향을 최소화 할 수 있습니다.

스위치는 다음과 같은 측면에서 루프백 감지를 지원합니다.:

- 포트에서 루프백 탐지를 지원하도록 지원
- 루프백 탐지 패킷의 대상 MAC 주소 구성 지원
- 최대 10 개의 지정된 포트에 대한 루프백 감지를 지원합니다.
- 루프백 탐지 패킷의 전송 간격 및 제어 포트의 복구 시간 구성 지원
- 포트 블록, 포트 MAC- 학습 금지 및 오류 비활성화를 포함한 제어 포트 지원
- 루프백이 기본적으로 포트에 존재하는지 여부를 구성하는 지원

루프백 탐지 패킷의 형식

필드	길이/Byte	값
DMAC	6	0x0180C2B0000A (구성 가능한 기본값)
SMAC	6	MAC address of the switch
TPID	2	0x8100, VLAN tag type
TCI	2	Specific value of the VLAN tag, priority, VLAN ID
TYPE	2	Protocol type, 0 에서 9001 까지
CODE	2	Protocol sub-type, 루프백 감지를 나타내며 0x0001 입니다.
VERSION	2	0x0000 (최근 지정 값)
Length	2	0x0008, 루프백 탐지 패킷의 헤더 길이
RESERVE	2	필드 지정 값
SYSMAC	6	스위치의 MAC 주소
SEQUENCE	4	패킷이 전송되기 전에 시스템에 의해 임의로 생성되는 패킷의 시퀀스 ID
DiID	4	Port ID, 85 시리즈의 글로벌 포트 ID
End	2	0x0000, 끝 문자

루프백 검색 구성 작업

- 전역으로 루프백 검색 구성
- 포트 루프백 탐지 구성
- 지정된 VLAN 방향으로 루프백 검색을 수행하도록 포트 구성
- 포트에서 루프백 감지 간격 구성
- 제어하에 포트 구성하기
- 기본적으로 루프백을 포트에 구성
- 전역 루프백 검색 구성 표시
- 루프백 감지 포트에 대한 정보 표시

루프백 탐지 구성

전역으로 루프백 검색 구성

루프백 탐지를 전역 적으로 활성화 또는 비활성화한다는 것은 모든 물리적 포트에서 루프백 탐지를 활성화 또는 비활성화하는 것을 의미합니다. 글로벌 구성은 스위치와 같습니다. 이 스위치를 열 때만 포트의 루프백 탐지를 활성화 할 수 있습니다.

명령어	설명
[no] loopback-detection	루프백 탐지를 구성/해제합니다.

포트 루프 검사 구성

지정된 포트에서 루프백 탐지를 활성화 또는 비활성화하려면 먼저 루프백 탐지를 활성화해야합니다.

명령어	설명
[no] loopback-detection enable	포트 루프백 탐지를 구성합니다.

지정된 VLAN 에서 루프백 검색을 수행하도록 포트 구성

지정된 VLAN 에서 루프백 탐지를 구성하면 포트는 지정된 VLAN 태그가있는 여러 탐지 패킷을 정기적으로 전송해야하며 포트는 지정된 VLAN 태그로 최대 10 개의 탐지 패킷을 전송할 수 있습니다.

주목할 점은 포트가 지정된 VLAN 에 존재해야한다는 것입니다. 그렇지 않으면 구성이 아무런 영향을 미치지 않습니다. VLAN2 에서 VLAN8 까지 루프백 감지가 발생하면 포트는 트렁크 모드로 구성되고 트렁크 VLAN 허용은 VLAN 5-8 이며, 스위치로 전송 된 태그 2-4 가있는 패킷은이 포트를 통과 할 수 없으므로 구성이 적용되지 않습니다.

명령어	설명
[no] loopback-detection vlan-control *vlanlist*	지정된 VLAN 에서 루프백 감지를 수행하도록 포트를 구성합니다.

루프백 감지 간격 구성 (패킷 전송 간격, 제어되는 포트 복구 시간)

명령어	설명
[no] loopback-detection hello-time *time*	포트 루프백 탐지 패킷의 전송 간격을 구성합니다.

네트워크는 항상 변경 가능하기 때문에 루프백 탐지는 지속적인 프로세스입니다. 포트는 정기적 인 시간에 루프백 탐지 패킷을 전송합니다. 이 정규 시간은 루프백 탐지 패킷의 전송 간격으로 불린다. 시스템의 기본 전송 간격은 3 초입니다..

명령어	설명
[no] loopback-detection recovery-time *time*	포트 루프백 탐지 패킷의 전송 간격을 구성합니다.

위의 명령은 루프백이 사라지면 포트의 자동 복구 시간을 구성하는 데 사용됩니다. 기본 구성에서 포트가 이미 전송 된 루프백 탐지 패킷을 10 초 이내에 수신하지 못하면 루프백이 사라지는 것으로 간주됩니다. 복구 시간은 패킷 전송 시간의 3 배가되도록 구성하는 것이 좋습니다. 전송 시간이 매우 작은 값으로 구성되면 복구 시간을 전송 시간보다 적어도 10 초 더 길게 구성하는 것이 좋습니다.

포트 제어 구성

명령어	설명
[no] loopback-detection control {block|learning|shutdown}	포트 제어를 구성합니다.

포트가 네트워크에 루프백이 있음을 감지하면 포트 제어를 구성하여이 포트를 관리 할 수 있습니다. 포트의 제어 상태는 block, nolearn, shutdown 또는 trap 일 수 있습니다. 제어 상태가 구성되고 포트에 루프백이 존재하면 트랩 경보 메시지가 전송됩니다. 기본적으로 구성되지 않습니다..

루프백 탐지가 전역 적으로 활성화되면 루프백 탐지 패킷이 루프백 탐지가 활성화 된 포트에서 전송되어이 포트에서 다시 수신되며 포트는 다음 네 가지 제어 작업을 수행 할 수 있습니다.

BLOCK : 루프백이 발견되면이 포트는 다른 포트와 분리됩니다. 따라서이 포트에 들어오는 패킷은 다른 포트로 전달 될 수 없습니다. 포트는 프로토콜 다운 상태이며 MAC 주소 테이블 목록의 수명이 만료됩니다..

Nolearn : 포트가 MAC 주소를 알지 못하게하는 것을 의미합니다. 루프백이 감지되면 포트는 더 이상 MAC 주소 학습을 수행하지 않으며 동시에이 포트의 MAC 주소 테이블은 오래되었습니다.

shutdown : 포트를 닫는 것을 의미합니다. 루프백이 감지되면 트랩 메시지가 전송되고 포트의 MAC 주소 테이블이 오래된다는 점을 제외하고는 포트가 자동으로 닫히고 err-disable-recover 시간까지 패킷을 더 이상 전달할 수 없습니다.

Trap : 포트가 알람 만보고 함을 의미합니다. 루프백이 감지되면 포트는 아무런 조치없이 경보 만보고하고 MAC 주소 표를 오래 사용합니다.

포트가 블록 상태에 있으면 수신 패킷을 전달할 수 없으며 동시에 루프백 탐지 패킷을 연속적으로 전송합니다. 루프백이 사라지면 포트가 자동으로 복구됩니다. 기본 구성에서 포트가 이미 전송 된 루프백 탐지 패킷을 10 초 내에 수신하지 않은 경우 루프백이 사라지는 것으로 간주됩니다.

Block 상태에서는 포트 프로토콜이 작동하지 않습니다. 종료 상태에서 포트의 링크는 직접 작동 중지됩니다.

루프백 탐지 패킷의 대상 MAC 주소 구성

명령어	설명
[no] loopback-detection dest-mac *Mac-address*	루프백 탐지 패킷의 대상 MAC 주소를 구성합니다.

루프백 감지 패킷의 기본 대상 MAC 주소는 01-80-C2-00-00-0a 입니다. 다른 목적지 MAC 을 구성 한 경우 루프백 탐지 패킷의 목적지 MAC 주소로 사용됩니다.

기본적으로 루프백이 포트에 존재하도록 구성

명령어	설명
[no] loopback-detection existence	루프백이 기본적으로 포트에 존재하도록 구성합니다.

포트가 가동되고 포트 루프백 감지가 적용되면 위의 명령을 사용하여이 포트에 루프백이 있는지 여부를 구성합니다. 포트가 종료 상태 인 경우이 포트는 루프백을 구성하는 데 적합하지 않습니다. 이는 종료 상태의 포트가 패킷을 전달할 수 없기 때문입니다. 기본 구성은 루프백이 포트에 존재하지 않는다는 것입니다..

전역 루프백 검색 구성 표시

명령어	설명
show loopback-detection	루프백 검색 구성을 표시합니다.

이 명령은 global 구성, 각 포트에 루프백이 있는지 여부 및 일부 포트의 구성을 포함하여 전역 루프백 검색 구성에 대한 정보를 표시하는 데 사용됩니다.

포트 루프백 감지 구성 표시

명령어	설명
show loopback-detection interface *intf*	포트 루프백 검색 구성을 표시합니다.

이 명령은 주로 포트 타이머 및 전송 및 수신 된 패킷에 대한 정보를 포함하여 포트 루프백 검색을 표시하는 데 사용됩니다.

구성 예

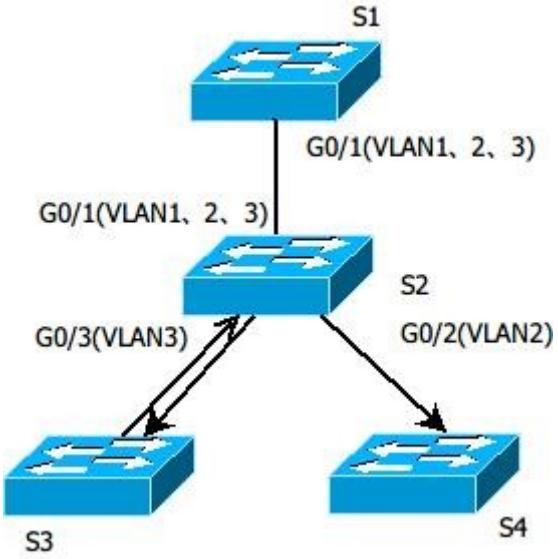


그림 1.1 루프백 감지 구성

그림 1.1 에서 볼 수 있듯이 S1 의 포트는 지정된 VLAN 1, 2 및 3 에 대한 루프백 감지를 수행합니다. 모든 스위치의 해당 구성은 아래에 나와 있습니다:

Switch S1:

Configuration of interface GigaEthernet0/1:

switchport trunk vlan-untagged 1-3

switchport mode trunk

loopback-detection enable

loopback-detection control block

loopback-detection vlan-control 1-5

Global Configuration

loopback-detection

vlan 1-3

Switch S2:
Configuration of interface GigaEthernet0/1:
switchport mode trunk
Configuration of interface GigaEthernet0/2:
switchport mode trunk
Configuration of interface GigaEthernet0/3:
switchport mode trunk
Global Configuration
vlan1-3

Switch S3:
Configuration of interface GigaEthernet0/1:
switchport pvid 3

S3 가 연결되는 네트워크에 루프백이 있고 루프백이있는 인터페이스의 PVID 가 3 인 경우 패킷은 S1 의 인터페이스 g0 / 1 에 전송되고 S1 은 루프백을 찾은 후 인터페이스 g0 / 1 을 차단합니다.

QoS 구성

QoS 개념

스위치는 일반적으로 최선의 노력을 다하는 서빙 모드에 있습니다. 이 모드에서 스위치는 모든 플로우를 동등하게 처리하고 모든 플로우를 전달하도록 최선을 다합니다. 이 경우, 모든 플로우는 정체가 발생하면 동일한 기회가 삭제됩니다. 실제 네트워크 조건에서 다른 흐름은 다른 중요성을 갖습니다. 스위치의 QoS 기능은 흐름의 중요성에 따라 다른 흐름에 다른 서비스를 제공하여 더 중요한 흐름을 보다 신중히 제공합니다.

현재 네트워크는 흐름의 중요성을 구별하는 두 가지 방법을 제공합니다.

- 802.1Q 프레임의 태그를 기준으로 중요성을 구별합니다. 태그에는 2 바이트가 있습니다. 가장 높은 바이트의 세 비트는 우선 순위 수준을 나타냅니다. 8 개의 우선 순위 레벨 0과 7이 각각 가장 낮은 우선 순위와 가장 높은 우선 순위 레벨을 나타냅니다.
- IP 메시지의 IP 헤더에서 DSCP 필드를 기반으로 중요성을 구별합니다. DSCP 필드는 IP 헤더의 TOS 도메인에서 6 비트를 차지합니다.

실제 네트워크 어플리케이션에서 발신 스위치는 중요도에 따라 다른 우선 순위를 다른 플로우에 분배합니다. 다른 스위치는 흐름에 포함 된 우선 순위 정보에 따라 다른 서비스를 제공합니다. peer-to-peer (P2P) QoS 서비스가 실현됩니다.

또한 네트워크를 구성하여 특정 메시지로 전환 할 수 있습니다. 동작은 하나의 홉으로 불리는 동작으로 수행됩니다.

스위치의 QoS 기능은 네트워크 대역폭을 효과적으로 만들어 성능을 향상시킵니다.

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. 베스트에 포트 서비스 모델에서 스위치의 QoS 기능은 "선착순" 주문을 준수합니다.

Differentiated 서비스

차별화 된 서비스의 경우 서비스가 특수한 경우 각 패킷에 해당 QoS 레이블을 지정해야 합니다. 지정 된 다른 모드로 구체화 될 수 있습니다 .IP 패킷의 IP 주소. 스위치는 QoS 규칙을 사용하여 서비스를 분류하고 지능형 대기열을 수행합니다. 스위치의 QoS 기능은 엄격한 우선 순위, 가중 라운드 로빈 (WRR) 및 "선착순 우선" (FCFS)를 통해 차별화 된 서비스를 전송할 수 있습니다.

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 WWW 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.

QoS 구성 업무

일반적으로 스위치는 모든 메시지를 전달하기 위해 최선을 다합니다. 정체가 발생하면 모든 메시지가 삭제 될 수 있습니다. 실제로, 다른 메시지는 다른 중요성을 가지고 있습니다. 중요한 메시지는 더 나은 서비스와 함께 제공 되어야 합니다. QoS 기능은 서로 다른 서비스를 제공하기 위해 서로 다른 우선 순위를 갖는 다른 메시지를 제공합니다. 따라서 네트워크 성능이 향상되어 효과적으로 사용합니다.

이번 장에서는 스위치의 기능을 구성하는 방법을 설명합니다.

- 전역 CoS 우선 순위 대기열 구성
- CoS 우선 순위 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 일치 된 데이터 흐름 구성
- QoS 정책 매핑의 일치 된 데이터 흐름에 대한 작업 구성
- 포트에 QoS 정책 적용
- QoS 정책 매핑 테이블 표시
- 포트 유량 제한 구성

QoS 작업 구성하기

전역 우선순위 Queue 구성하기

QoS 우선 순위 큐를 구성하는 것은 IEEE802.1p 에 정의 된 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.

명령어	설명
Configure	전역 구성모드로 들어갑니다.
[no] cos map *quid cos1..cosn* (0-7)	COS 우선순위 큐를 구성합니다. **quid** 는 COS 우선순위의 ID 입니다 **cos1..cosn** 는 IEEE802.1p 에 정의 된 cos 값입니다.
Exit	관리 모드로 돌아갑니다.
Write	구성을 저장합니다.

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 (Sheer Priority): 완벽한 우선 순위 일정. 우선 순위가 낮은 대기열의 패킷은 우선 순위가 높은 대기열이 비어있는 경우에만 전달됩니다. 우선 순위가 높은 대기열에 패킷이 있으면 이 패킷이 먼저 전송됩니다.
- WRR (Weighted Round Robin): 각 큐에 가능한 한 많이 할당하는 것입니다.

권한 모드에서 다음 작업을 수행하여 CoS 우선 순위 대기열의 일정을 구성합니다

명령어	설명
configure	전역 구성 모드를 시작하십시오.
[**no**] **scheduler policy** { **sp** | **wrr** | **wfq**| **fcfs** }	QoS 우선 순위 대기열에 대한 일정 정책을 구성합니다
Exit	관리 모드로 돌아갑니다.
Write	구성을 저장합니다.

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 : 전송 된 시간에 세그먼트를 사용하여 점유 대역폭을 나타냅니다.

일련의 스위치는 패킷 수만 지원합니다. 패킷 수는 기본 스케줄 표준입니다.
따라서 표준 스케줄 정책을 선택하라는 명령은 없습니다.

포트의 기본 CoS 값 구성

포트가 레이블이 없는 프레임을 수신하면 스위치는 기본 COS 우선 순위를
레이블에 추가하려고 합니다. 기본 CoS 값 구성은 레이블이 없는 프레임의 기본값입니다.

특정 모드에서 다음 포트의 기본 CoS 값 조작을 수행하십시오.

명령어	설명
Configure	전역 구성 모드를 시작하십시오
interface g0/1	구성 할 포트에 로그인합니다
[**no**] **cos default** *cos* **(0~7)**	레이블이 없는 프레임의 CoS 값을 구성하고 CoS 는 cos 값을 나타냅니다. 기본 값으로 cos (0~7) 구성이 가능합니다.
Exit	전역 구성 모드로 돌아갑니다
Exit	관리 모드로 돌아갑니다
Write	구성을 저장합니다

Qos 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 있어야합니다.

QoS 매핑 정책을 만들려면 권한 모드에서 다음 작업을 수행하십시오.

명령어	설명
Configure	전역 구성 모드를 시작합니다.
[no]policy-map *name*	QoS 정책 테이블 구성 모드를 시작합니다. name 은 정책테이블의 이름을 나타냅니다.
description *description-text*	QoS 의 정책을 설명을 구성합니다. **description-text** 는 설명입니다
[**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 일치된 데이터 흐름을 구성합니다 access-list-name 는 일치하는 IP Access list 의 이름입니다. **dscp-value** 이란 IP 메시지에 다른 서비스를 의미합니다. **mac-list-name** Mac 주소 리스트의 일치하는 주소 목록 이름이다.. **vlan-id** vlan 과 일치하는 ID 이다 **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. **max-band** 데이터흐름에 의해 최대 대역폭이 발생합니다, **cos-value** 일치된 서비스 등급을 cos-value 으로 구성하는 것을 의미합니다. **dscp-value** 는 흐름의 맞춘 **dscp 필드 dscp-value**. 값을 매칭시킵니다. **interface-id** 지향성에 맞춘 흐름의 종료를 나타냅니다. **Drop** 드롭 메시지를 삭제합니다.. **Stat** 통계 정보를 나타냅니다 **monitor** 패킷을 미러링 포트로 전송을
Exit	전역 구성모드로 돌아갑니다
Exit	관리모드로 돌아갑니다.

QoS 정책 매핑 구성

설명

권한 모드에서 다음 작업을 수행하여 QoS 정책 매핑에 대한 설명을 구성합니다.

명령어	설명
Configure	전역 구성 모드로 들어갑니다.
[**no**]**policy-map** *name*	QoS 정책 목록 구성 모드를 입력합니다.. **name** 정책 이름을 나타냅니다.
description description-text	Qos 정책 설명을 구성합니다 **description-text** 는 정책을 설명하는 텍스트입니다.
Exit	글로벌 구성 모드로 돌아갑니다
Exit	관리 모드로 돌아갑니다.

QoS 매핑 정책의 일치하는 데이터 흐름 구성하기

QoS 데이터 흐름의 분류 규칙은 요구 사항에 따라 구성한 필터링 규칙입니다.
다음 작업을 일치하는 정책 데이터 흐름을 구성 합니다.

명령어	설명

configure	전역 구성 모드로 들어갑니다.
[**no**]**policy-map** *name*	QoS 정책 목록에 구성을 합니다. **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 일치 하는 데이터흐름을 구성합니다. **access-list-name** 일치하는 IP ac-list 이름입니다. **dscp-value** stands for the **diffserv** field in the IP message. **mac-list-name** 는 일치하는 MAC ac-list 이름입니다. **vlan-id** Vlan 아이디를 나타냅니다. **cos** 일치하는 서비스 등급 값입니다.
Exit	전역 구성 모드로 돌아갑니다
Exit	관리 모드로 돌아갑니다

QoS 매핑 정책의 일치하는 데이터 흐름을 일치하는 구성하기

데이터 흐름의 작용을 정의한다는 것은 대역 폭 제한, 메시지 삭제, 도메인 업데이트 등 필터링 규칙을 데이터 흐름에 따라 작업을 수행한다는 것을 의미합니다.
다음 작업을 수행하여 일치하는 데이터 흐름에 대한 작업을 구성 합니다.

명령어	설명
configure	전역 구성 모드를 사용합니다.
[**no**]**policy-map** *name*	Qos 정책 구성 모드를 실행합니다. **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. **max-band**: 최대값을 나타냅니다. **cos-value** 흐름의 서비스 등급 필드를 cos-value 로 구성하는 것을 의미합니다. **dscp-value** 일치하는 흐름의 dscp 필드를 VSE-값으로 구성하는 방법입니다. **vlanid-value** 일치된 흐름의 VLANID 필드를 vlanid-value 로 구성하는 것을 의미합니다. **interface-id** 방향성 일치 항목 흐름의 종료를 나타냅니다. **drop** 드롭 된 메시지를 나타냅니다 **Stat-packet, Stat-byte** 스위치에 의해 수집된 통계 정보를 패킷 또는 바이트 단위로 나타냅니다. **monitor** 패킷을 미러링 포트에 전송하는것을 의미합니다
Exit	전역 구성 모드로 돌아갑니다.
Exit	관리모드로 돌아갑니다.

포트에 QoS 정책을 적용하기

QOS 정책을 포트에 적용 할 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.:

명령어	설명
Configure	전역 구성 모드를 시작합니다
interface g0/1	구성 할 포트에 로그인합니다.
[**no**] **qos policy** *name* { **ingress**|**egress**}	포트에 QoS 정책을 적용합니다. **name** QoS 정책을 적용합니다. **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.

QoS 매핑 정책 테이블 표시

show QoS strategy 매핑 테이블을 실행할 수 있습니다.

QoS 정책 매핑 테이블을 표시하려면 권한 모드에서 다음 작업을 수행하십시오.

명령어	설명
show policy-map [*policy-map-name*]	모든 또는 지정된 QoS 정책 매핑 테이블을 표시합니다. **policy-map-name** 매핑 테이블의 이름을 나타냅니다.

QoS 구성 예제

포트에 QoS 정책 예제 적용하기

포트에서 메시지의 COS 값을 2 로 변경하는 정책을 구성합니다. 그렇지 않으면 다른 정책을 적용해야 합니다. 모든 데이터 흐름을 통과 할 수 없습니다.

```
ip access-list extended ipacl
permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255 policy-map
any
classify any
policy-map pmap
classify ip access-group ipacl
action cos 2
interface GigaEthernet0/2
        qos policy pmap ingress
```

DoS 공격 방지 구성

DoS 공격 개요

DoS 공격의 개념

DoS 공격은 서비스 거부 공격이라고도합니다. 일반적인 DoS 공격에는 네트워크 대역폭 공격과 연결 공격이 포함됩니다. DoS 공격은 해커가 자주 발생시키는 네트워크 공격 모드입니다. 궁극적 인 목적은 합법적 인 사용자에게 일반적인 네트워크 서비스를 제공하지 않으려 고 네트워크를 무너 뜨리는 것입니다.

DoS 공격 방지는 Pingflood, SYNflood, Landattack, Teardrop 및 불법 플래그가 포함 된 TCP 와 같은 공격을 막기위한 많은 공격 예방 방법을 제공하는 스위치가 필요합니다. 스위치가 공격 받고있을 때 어떤 공격 유형인지 판단해야하며이 공격 패킷을 특수하게 처리해야합니다 (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 수있는 IP 조각의 패킷 헤더에 포함 된 정보를 사용하여 공격을 실현합니다. IP 조각에는 원래 패킷의 어느 부분이 포함되어 있는지를 나타내는 정보가 포함되어 있으며 일부 TCP / IP 스택은 겹치는 오프셋이 포함 된 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 트리거합니다..

Land Attack

공격자는 특수 SYN 메시지를 만듭니다 (발신 주소와 수신 주소는 동일한 서비스 주소임). SYN 메시지는 서버가 SYN-ACK 메시지를 서버 자체로 전송하도록하므로이 주소는 또한 ACK 메시지를 보내고 null 링크를 생성합니다. 이러한 각 종류의 링크는 제한 시간까지 유지되므로 서버가 고장납니다. Landattack 은 IPland 와 MACland 로 분류 할 수 있습니다..

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 표시

DoS 공격 방지 구성 작업

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 방지 할 수 있지만 DoS ICMP 하위 기능은 Ping of Death 를 방지 할 수 있습니다. 실제 요구 사항에 따라 해당 하위 기능을 구성할 수 있습니다.
EXEC 모드에서 DoS 공격 방지 기능 구성.

명령어	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 all을 구성합니다.. ICMP 패킷을 방지하도록 ICMP 를 구성합니다. ICMP 값은 ICMP 패킷의 최대 길이를 의미합니다. 출발지 IP 가 목적지 IP 와 동일한 IP 패킷을 방지하도록 ip 를 구성합니다. ipv4 첫 번째 플래그를 구성하여 IP 패킷의 첫 번째 조각을 확인합니다. 원본 포트 ID 가 대상 포트 ID 인 TCP / UDP 패킷을 방지하도록 l4port 를 구성합니다..

	불법 TCP 플래그를 포함하는 TCP 패킷을 방지하도록 tcpflags 를 구성합니다.. 최소 TCP 헤더가 tcpfrag-value 인 TCP 패킷을 방지하도록 tcpfrag 를 구성합니다..
exit	EXEC 모드로 돌아갑니다..
write	구성을 저장합니다..

모든 DoS 공격 방지 구성 표시

show 명령을 통해 Dos 공격 방지 구성을 표시 할 수 있습니다.
EXEC 모드에서 다음 명령을 실행하여 구성된 DoS 공격 방지 기능을 표시하십시오..

명령어	설명
show dos	DOS 공격 방지 구성을 표시합니다..

DoS 공격 방지 구성 예

다음 예는 잘못된 플래그가있는 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
```

공격 예방 구성

개요

스위치는 네트워크 대역폭의 유용성을 보장하기 위해 트래픽이 사용되는 것을 방지하는 기능을 제공합니다. 현재의 공격 모드에 비추어 우리 호스트는 일정 기간 동안 ARP, IGMP 또는 IP 메시지를 많이 보내고 이러한 호스트에 서비스를 제공하지 않습니다. 이 기능은 악의적 인 메시지가 많은 네트워크 대역폭을 차지하는 것을 막을 수 있습니다. 따라서 네트워크가 정체 될 수 없습니다.

공격 예방 구성 작업

임계 값을 초과하는 지정된 간격으로 호스트에서 보낸 IGMP, ARP 또는 IP 메시지의 수는 호스트가 네트워크를 공격한다고 생각합니다.
공격 방지 유형 (ARP, IGMP 또는 IP), 공격 방지 포트 및 공격 탐지 매개 변수를 선택할 수 있습니다. 다음과 같은 구성 작업이 있습니다.

- 공격 방지 유형 구성
- 공격 탐지 매개 변수 구성

공격 예방 구성

공격 탐지 매개변수 구성하기

명령어	설명
filter period *time*	공격 탐지 기간을 초단위로 구성합니다.
filter threshold *value*	공격 탐지 임계 값을 value 로 구성합니다. 매개 변수 값은 임계 값에서의 메시지 수를 나타냅니다.
filter block-time *time*	공격 소스의 서비스 중단 시간을 구성합니다. 단위는 초입니다.

공격 방지 유형 구성

명령어	설명
filter igmp	igmp 공격을 탐지합니다.
fileter ip source-ip	IP 주소를 기반으로 공격을 감지합니다.
interface f x/y	인터페이스 y 에 슬롯 x 에 들어갑니다..
filter arp	Arp 공격을 탐지합니다

ARP 공격은 호스트의 MAC 주소와 소스 포트를 공격 소스로 사용합니다. IGMP 공격과 IP 공격은 호스트의 IP 주소와 소스 포트를 공격 소스로 사용합니다. IGMP 공격 방지와 IP 공격 방지는 함께 시작할 수 없습니다.

공격 예방 기능 시작하기

공격 예방을 위한 모든 매개 변수가 끝나면 공격 방지 기능을 시작할 수 있습니다. 공격 방지 기능이 시작됩니다.

명령	설명
filter enable	공격 방지 기능을 시작합니다.

공격 방지 기능을 비활성화하고 모든 공격 소스로 차단을 제거하려면
no filter enable 명령을 사용하십시오.

공격 예방 상태 점검

공격 방지가 시작되면 다음 명령을 실행하여 공격 방지 상태를 확인할 수 있습니다:

명령	설명
show filter	공격 예방 상태 점검.

공격 방지 구성 예

포트 1/2 에서 IGMP 공격 방지 및 ARP 공격 방지를 사용하려면 공격 소스로 15 초 내에 1200 개 이상의 메시지를 보내고 공격 소스에 대한 네트워크 서비스를 차단하는 호스트를 고려하십시오.

filter period 15

filter threshold 1200

filter block-time 600

interface g0/2

filter arp

exit

filter enable

IP 주소 구성

IP 개요

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

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

IP 라우팅 프로토콜

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

IP 동적 라우팅 프로토콜을 구성하려면 먼저 관련 프로세스를 구성해야 합니다.
관련 네트워크 포트를 동적 라우팅 프로세스와 상호 작용하도록 만든 다음
포트에서 시작될 라우팅 프로세스를 지정합니다. 이를 위해 구성 명령 문서의 구성 단계를 점검 할 수 있습니다.

라우팅 프로토콜을 선택한다.

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

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

IGRP

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

라우팅 스위치가 지원하는 IGRP 는 다음과 같습니다.

- RIP
- OSPF
- BEIGRP
- EGRP

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

IP 작업 목록 구성

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

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

다음은 IP 주소 구성 작업 목록입니다.

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

IP 주소 구성

네트워크 인터페이스 IP 주소 구성

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

형태	**주소와 범위**	**상태**
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	지정 유효 지정

B	128.0.0.0 to 191.254.0.0 191.255.0.0	유효 지정
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	지정 유효 지정
D	224.0.0.0 to 239.255.255.255	Multicast 주소
E	240.0.0.0 to 255.255.255.254 255.255.255.255	예약 주소 Broadcast 주소

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

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

마스크는 네트워크를 나타내고 IP 주소의 일부입니다.

노트 : 우리의 스위치는 네트워크 문자 순서에 따라 가장 높은 바이트에서 연속적으로 구성된 마스크 만 지원합니다.

네트워크 인터페이스 다중 IP 주소구성

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

- 네트워크 세그먼트에 IP 주소가 충분하지 않은 경우

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

있습니다. 구성된 종속 IP 주소를 통해 네트워크의 라우팅 스위치는 동일한 실제 네트워크를 연결하는 여러 서브넷을 인식 할 수 있습니다.

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

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

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

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

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

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

주소 구성 해결법

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

- 주소 해결법 만들기

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

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

우리의 시스템은 두가지 유형의 주소 해결법을 ARP 와 Proxy ARP 적용한다. ARP 와 Proxy ARP 는 RFC(860)과 RFC(1027)에 각각 정의되어 있습니다. ARP 는 IP 주소를 미디어 매체나 MAC 주소에 매핑하는데 사용하고 IP 주소로 ARP 는 해당하는 MAC 주소를 찾습니다. MAC

주소를 알고 있으면 IP 주소와 MAC 주소 간의 매핑 관계가 빠른 액세스를 위해 ARP 캐시에 저장됩니다. 그러면 IP 메시지는 링크계층의 메시지에 패키징 되어 마지막으로 네트워크로 전송됩니다.

- Static ARP 캐시 정의

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

ARP 항목을 영구적으로 존재하지 않으려면 ARP 항목의 활성 기간을 구성할 수 있습니다.

인터페이스 구성모드에서 명령어를 실행합니다

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

명령어 show interface 는 지정 인터페이스의 ARPM timeout 을 나타냅니다.

명령어 show arp 는 ARP 캐시의 내용을 확인합니다

명령어 Clear arp 는 모든 항목의 arp 캐시를 지웁니다.

- Proxy ARP 활성화

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

프록시 ARP 를 활성화하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip proxy-arp	Proxy-ARP 를 인터페이스에서 활성화

- 자유로운 ARP 기능 구성

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

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

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

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

- IP주소에 Host 이름을 매핑

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

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

명령어	설명
ip host *name address*	IP 주소에 호스트이름을 고정시킨다.

라우팅 프로세스 구성

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

Broadcast 메시지 처리 구성

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

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

- 지정된 Broadcast에서 물리적인 Broadcast로 허용된 변환

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

인터페이스 구성모드에서 지정된 Broadcast 의 전달을 활성화하세요

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

- UDP Broadcast 메시지 전달

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

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

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

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

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

전체 구성 모드에서 다음 명령을 실행하여 전달할 프로토콜을 지정하십시오.

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

IP 주소 지정 및 유지

네트워크를 탐지하고 유지 관리하려면 다음 작업을 수행하십시오.

캐시와 기록 과 데이터베이스 지우기

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

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

명령어	설명
clear arp-cache	IP 와 ARP 의 캐시를 제거합니다.

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

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

관리자 모드에서 다음 명령을 실행하십시오.:

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

IP 주소화 예제

다음은 Interface VLAN 11 에 IP 주소가 구성되는 경우를 나타냅니다.

interface vlan 11

Ip address 202.96.2.3 255.255.255.0

DHCP 구성

개요

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

- 자동 분배

  DHCP 서버는 영구 IP 주소를 클라이언트에 자동으로 배포합니다..

- 동적 배포

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

- 수동 배포

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

DHCP 적용

DHCP 에는 여러 종류의 응용프로그램이 있는데, 다음과 같은 경우 사용가능 합니다. DHCP 클라이언트를 구성하여 IP 주소, 네트워크 세그먼트 및 관련 소스 (관련 게이트웨이 등)를 이더넷 인터페이스에 배포 할 수 있습니다. DHCP 에 액세스 할 수 있는 스위치가 여러 호스트를 연결하면 스위치는 DHCP 릴레이를 통해 DHCP 서버에서 IP 주소를 가져온 다음 호스트에 주소를 배포 할 수 있습니다.

DHCP 이점

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

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

DHCP 용어

DHCP 는 서버와 클라이언트 기반으로 하며 각각은 실행 조건이 존재합니다.

- DHCP-서버

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

- DHCP-클라이언트

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

- 임대 시간 - 분배 이후 IP 주소의 유효 기간.

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

DHCP 클라이언트 구성

DHCP 클라이언트 구성 업무

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

IP 주소 배정

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

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

DHCP서버에 주소를 지정

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

명령어	설명
ip dhcp-server *ip-address*	DHCP 서버의 IP 주소를 지정합니다.

이 명령어는 IP 주소 입력을 위해 선택적인 작업입니다.

DHCP 매개변수 구성

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

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

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

DHCP 모니터링

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

명령어	설명
show dhcp server	라우팅 스위치가 아는 DHCP 서버정보를 표시합니다.

관리모드에서 명령어를 실행하여 라우팅 스위치에 사용중인 IP 주소를 확인합니다..

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

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

DHCP 클라이언트 구성 예시

IP 주소를 받는 경우

The following example shows Ethernet1/1 obtains an IP address through DHCP를 통해IP주소를 이더넷 1/1 에서 얻게 되어 나타납니다.

interface vlan 11

ip address dhcp

DHCP 서버 구성

DHCP 서버 구성 내용

DHCP 서버 사용

DHCP 서버 비활성화

ICMP 감지 매개 변수 구성

데이터베이스 저장 영역 매개 변수 구성

DHCP 서버의 주소 풀 구성

DHCP 서버의 주소 풀에 대한 매개 변수 구성

DHCP 서버 모니터링

DHCP 서버 정보 지우기

DHCP 서버 구성

DHCP 서버 사용

DHCP 서버를 활성화하고 IP 주소와 같은 매개 변수를 배포하려면
DHCP 클라이언트가 전역 구성 모드에서 다음 명령을 실행합니다 (DHCP 서버는 연속적인 작업도

지원합니다. 일반 DHCP 서버가 배포 할 수 없는 주소의 경우에는 ip helper-address 가 구성된 포트는 DHCP 요청을 전달하는 것입니다).

명령어	설명
ip dhcpd enable	DHCP 서버 사용

DHCP 서버 비활성화

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

명령어	설명
no ip dhcpd enable	DHCP 서버 비활성화

ICMP 감지 매개 변수 구성

서버가 전송 될 때 보낼 ICMP 메시지의 매개 변수를 조정할 수 있습니다
주소 검색을 수행합니다. 전역 구성 모드에서 다음 명령을 실행하십시오.
보낼 ICMP 메시지 수를 구성하려면 다음을 수행하십시오.

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

전역 구성모드에서 명령을 실행하여 ICMP 메시지 응답시간 초과시간을 구성합니다.

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

데이터베이스 저장 영역 매개 변수 구성

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

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

DHCP 서버의 주소 풀 구성

전역 구성 모드에서 다음을 실행하여 DHCP 에 주소풀을 추가합니다.

명령어	설명

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

DHCP 서버의 주소 풀에 대한 매개 변수 구성

주소 풀 구성모드에서 명령어로 주소 풀의 망 주소를 구성합니다.

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

자동 분류에 사용되는 주소 범위를 구성하는 경우 다음 명령을 실행하세요.

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

다음 명령어는 클라이언트에 배포되는 기본경로를 구성합니다.

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

다음 명령어는 클라이언트에 배포되는 DNS 서버 주소를 구성합니다.

명령어	설명
dns-server *ip-addr ...*	DNS 서버 주소를 구성합니다.

다음 명령어는 클라이언트에 배포되는 도메인을 구성합니다.

명령어	설명
domain-name *name*	Client 에 분배되는 도메인을 구성합니다.

다음 명령어는 클라이언트에 배포되는 주소 임대시간을 구성합니다.

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

다음 명령어는 클라이언트에서 배포되는 Netbios 서버주소를 구성합니다.

명령어	설명
netbios-name-server *ip-addr...*	Client 에 부류된 Netbios 서버를 구성합니다

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

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

DHCP 서버 모니터링

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

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

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

명령어	설명
show ip dhcpd statistic	DHCP 서버에 통계정보를 삭제합니다

DHCP 서버 정보 지우기

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

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

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

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

DHCP 서버 구성 예시

다음 예시문에 ICMP 탐지 패킷의 시간에 초과 시간은 200ms 로 구성됩니다. 주소 풀 pool 1 이 구성되고 DHCP 서버가 사용됩니다.

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

IP 서비스 구성

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

IP 서비스 구성하기

IP 서비스를 선택적으로 구성하는 방법은 다음과 같습니다.:

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

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

IP 연결 관리하기

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

다른 IP 연결 조건에 따라 다음과 같은 작업을 수행하십시오.

ICMP 연결 해제 메시지 보내기

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

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

명령어	설명
ip unreachables	ICMP 연결 해제 메시지를 전송하려면 이 기능을 사용하도록 구성합니다.

ICMP 경로 수정 메시지 보내기

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

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

이 기능은 기본적으로 사용하도록 구성되어 있습니다. HSRP(Hot Standby Routing Protocol) =상시 대기 라우터 프로토콜이 인터페이스에 구성된 경우 자동으로 비활성화됩니다. 하지만 이기능은 자동으로 실행되지 않으며 프로토콜이 취소 된 경우에도 자동으로 활성화되지 않습니다.

이 기능을 사용하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오.:

명령어	설명
ip redirects	ICMP 방향 수정 메시지 전송 허용

ICMP mask 응답 메시지 전송

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

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

명령어	설명
ip mask-reply	ICMP mask 응답메시지를 보냅니다.

지원경로 MTU 탐지

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

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

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

MTU IP 구성

Maximum Transmission Unit (MTU)는 IP 메시지로 전송이 가능한 최대 길이를 말합니다. IP 메시지 길이가 MTU 를 초과하는 경우는 라우팅 스위치에서 분할합니다. 인터페이스의 MTU 값을 변경하면 IP MTU 값에 영향을줍니다. IP MTU 가 MTU 와 같으면 IP MTU 는 자동으로 MTU 가 변경 될 때 새로운 MTU 와 동일하게 조정됩니다. 그러나 IP MTU 의 변경은 MTU 에 영향을 미치지 않습니다. IP MTU 는 현재 인터페이스에 구성된 MTU 보다 클 수 없습니다. 동일한 물리적 미디어를 연결하는 모든 장치가 동일한 MTU 프로토콜을 가져야하는 경우에만 정상적인 통신을 생성 할 수 있습니다.

특정 인터페이스에서 IP MTU 를 구성하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
ip mtu *bytes*	인터페이스의 IP MTU 를 구성하십시오.

IP 소스 경로 인증

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

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

명령어	**설명**
ip source-route	IP 소스 라우트 권한 부여

IP 의 빠른 교섭 허용

IP 빠른 교섭은 캐시를 사용하여 IP 메시지를 전달합니다. 스위치가 특정 대상으로 메시지를 전달하기 전에 시스템은 라우팅 테이블을 확인한 다음 경로에 따라 메시지를 전달합니다. 선택한 경로는 시스템 소프트웨어의 라우팅 캐시에 저장됩니다. 후자의 메시지가 동일한 호스트로 보내지면 스위치는 라우팅 캐시에 저장된 경로에 따라 후자의 메시지를 전달합니다. 메시지가 전달 될 때마다 해당 라우트 항목의 적중 횟수 값이 1 씩 증가합니다. 적중 횟수가 구성 값과 같으면 소프트웨어 라우팅 캐시가 하드웨어 라우팅 캐시에 저장됩니다. 동일한 호스트에 대한 다음 메시지는 하드웨어에 의해 직접 전달됩니다. 일정 시간 동안 캐시를 사용하지 않으면 캐시가 삭제됩니다. 소프트웨어 / 하드웨어 캐시 항목이 상한 값에 도달하면 새 대상 호스트는 더 이상 캐시에 저장되지 않습니다. 빠른 교섭을 허용하거나 금지하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오:

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

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

명령어	설명

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

같은 인터페이스에서 빠른 IP 교섭 지원

스위치가 수신 인터페이스를 송신 인터페이스와 동일하게함으로써 빠른 IP 교섭을 지원할 수 있습니다. 일반적으로 라우터의 리다이렉션 기능과 충돌하기 때문에이 기능을 사용하지 않는 것이 좋습니다.

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

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

매개 변수 구성 성능

TCP 연결 대기 시간 구성

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

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

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

TCP windows의 크기 구성하기

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

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

IP 네트워크 유지 및 탐지

캐시와 데이터베이스 목록을 제거합니다.

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

잘못된 데이터를 지우려면 다음 명령을 실행하십시오.

명령어	설명
clear tcp statistics	TCP 통계 데이터를 지웁니다.

TCP 연결 해제

TCP 연결을 끊으려면 다음 명령을 실행하십시오.

명령어	설명
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	지정된 TCP 연결을 지웁니다. TCB 는 TCP 제어 블록을 나타냅니다.

시스템 및 네트워크에 대한 통계 데이터 표시

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

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

명령어	설명
show ip access-lists *name*	모든 엑세스 목록의 내용을 표시합니다
show ip cache [prefix mask] [type number]	IP 메시지교환 된 캐시를 표시합니다.
show ip sockets	스위치에 소켓 정보를 표시합니다.
show ip traffic	IP 프로토콜에 대한 통계 데이터를 표시합니다
show tcp	모든 TCP 연결 상태에 대한 정보를 표시합니다.
show tcp brief	TCP 에 대한 정보를 간략히 나타냅니다.
show tcp statistics	TCP 통계 데이터를 표시합니다.
show tcp tcb [TCP control block address]	지정 TCP 연결상태 정보를 표시합니다.

디버깅 정보 표시.

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

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

명령어	설명
debug arp	ARP 에 대한 상호작용 정보를 표시합니다
debug ip icmp	ICMP 에 대한 상호작용 정보를 표시합니다.
debug ip raw	수신/발신 된 IP 메시지에 대한 정보를 표시합니다.
debug ip packet	IP 에 대한 상호 작용 정보를 표시합니다.
debug ip tcp	TCP 에 대한 상호 작용 정보를 표시합니다.
debug ip udp	UDP 에 대한 상호 작용 정보를 표시합니다.

Access List 구성하기

IP 메시지 필터링

필터링 메시지는 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 방법은 특정 사용자 또는 장치를 통해 네트워크 전송 및 네트워크 사용을 제한 할 수 있습니다. 교차 지정 인터페이스를 통해 패킷을 유효하거나 무효로 만들기 위해 라우팅 스위치는 Access-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 을 사용하는 방법에 대해 설명합니다.

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

다음 항목에 따라 Access-list 를 사용하십시오.

(1) Access list 의 이름과 조건을 지정하여 작성합니다.

(2) Access list 를 인터페이스에 적용합니다.

표준 및 확장 가능 IP 액세스 목록 만들기

문자열을 사용하여 IP 액세스 목록을 만듭니다.

참고:

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

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

명령어	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.

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

명령어	설명
ip access-list extended *name*	확장 Access-List 이름을 정의합니다.
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos**	하나 이상의 허용 및 거부 조건을 지정하고 패킷 승인여부를 결정합니다. 서비스약관(TOS)는 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 추가 할 수 없습니다. 그러나 액세스 허용 목록에서 항목을 삭제하려면 허용 안 함과 거부 안 함을 실행할 수 있습니다.

참고:

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 3.2.3 "인터페이스에 Access-List 적용" 장을 참조하십시오

인터페이스에 Access-list 적용

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

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip access-group *name* **{in | out}**	Access 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 확인해야합니다. 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 도달 할 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 도달 할 수 없는 메시지를 반환합니다.

지정된 Access-list 이 없으면 모든 패킷이 통과 할 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 구성 될 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

물리적인 포트를 기반으로 IP Access-list 구성

IP 메시지 필터링

필터링 메시지는 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 이 방법은 특정 사용자 또는 장치를 통해 네트워크 전송 및 네트워크 사용을 제한 할 수 있습니다. 교차로 지정

인터페이스를 통해 패킷을 유효하거나 무효로 만들기 위해 라우팅 스위치는 Access-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 ROS 소프트웨어는 규정에 따라 Access-List 에서 주소를 하나씩 테스트합니다. 첫 번째 일치는 ROS 가 주소를 수락 또는 거절하는지 여부를 결정합니다. 첫 번째 경기가 끝나면 ROS 소프트웨어가 경기 규칙을 종료합니다. 따라서 조건의 순서가 중요합니다. 규정이 일치하지 않으면 주소가 거부됩니다.

Access list 의 사용은 다음과 같은 단계가 있습니다.

(1) access list의 이름과 조건을 지정하여 작성합니다.

(2) 인터페이스에 Access-list를 저장합니다.

표준 및 확장IP Access List 생성

문자열을 사용하여 IP access list 를 만듭니다.

참고:

표준 Access-list 과 확장 Access-list 에는 동일한 이름을 사용할 수 없습니다.

전역 구성 모드에서 다음 명령을 실행하여 표준 Access-list 을 만듭니다.

명령어	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.

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

명령어	설명
ip access-list extended *name*	Access-list 에 이름을 적용합니다.
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos**	하나이상의 허가/거부 지정하며 조건 이전 구성은 패킷의 승인여부를 결정합니다. 서비스약관(TOS)는 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 추가 할 수 없습니다. 그러나 액세스 허용 목록에서 항목을 삭제하려면 허용 안 함과 거부 안 함을 실행할 수 있습니다.

참고:
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.

인터페이스에 Access-List 적용

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

인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	**설명**
ip access-group *name*	Access 그룹의이름을 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 확인해야합니다. 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 도달 할 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 도달 할 수 없는 메시지를 반환합니다.

지정된 액세스 목록이 없으면 모든 패킷이 통과 할 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 실패 할 수 있다. 이 경우 한쪽에서 포트 범위를 지정 하는 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 g0/10

ip access-group aaa

-

IP 액세스 제어 목록 적용

IP Access Control List 적용

포트에 ACL 적용

ACL 이 구성된 후에는 하나 이상의 슬롯 또는 전역 적으로 적용될 수 있습니다.
global 또는 포트 구성 모드에서 다음 명령을 실행하십시오.:

명령어	설명
config	글로벌 구성 모드로 들어갑니다..
interface g0/1	구성 할 포트 입력.
[**no**] {**ip** | **ipv6**} **access-group** *name* [**<cr>** | **egress** | [**stat-packet** | **stat-byte**]]	구성된 IP / IPv6 액세스 목록을 인터페이스에 적용하거나 인터페이스에서 취소합니다.. Egress 는 ACL 이 아웃 바운드 방향으로 적용됨을 의미합니다..
exit	글로벌 구성 모드로 돌아갑니다..
exit	EXEC 모드로 돌아갑니다.
write	구성을 저장합니다.

RIP 구성하기

개 요

이 섹션에서는 RIP 명령을 구성하는 방법을 설명합니다. RIP 명령에 대한 자세한 내용은 "네트워크 프로토콜 명령 참조"의 "RIP 명령"을 참조하십시오.

라우팅 정보 프로토콜 (RIP)은 아직 일반적으로 사용되는 내부 게이트웨이 프로토콜 (IGP)이며 주로 같은 유형의 소규모 네트워크에 적용됩니다. RIP 는 RFC 1058 에 나오는 고전적인 거리 벡터 라우팅 프로토콜입니다.
RIP 는 UDP 패킷의 Broadcast 를 사용하여 라우팅 정보를 교환합니다. 라우팅 스위치에서 라우팅 정보의 업데이트는 30 초마다 수행됩니다. 스위치가 180 초 내에 인접 스위치의 업데이트 정보를 받지 못하면 스위치는 인접 스위치의 라우팅 테이블에 있는 경로를 "사용할 수 없음"으로 표시합니다. 업데이트 정보가 다음 120 초 내에 여전히 수신되지 않으면 스위치는 라우팅 테이블에서 경로를 삭제합니다.

RIP 는 홉의 개수를 사용하여 여러 경로의 가중치의 균형을 조정합니다. 홉 수는 패킷이 정보 소스 및 정보 싱크에서 가져 오는 스위치 수입니다. 직접 연결된 네트워크의 라우팅 가중치는 0 입니다. 도달 할 수 없는 네트워크의 라우팅 가중치는 16 입니다. RIP 를 사용하는 라우팅 가중치의 범위가 작기 때문에 대규모 네트워크에는 적합하지 않습니다.
스위치에 기본 경로가 있는 경우 RIP 는 네트워크에 대한 경로를 선언합니다 0.0.0.0. 사실 네트워크 0.0.0.0 은 존재하지 않습니다. 기본 경로를 구현하기 위해 RIP 에만 사용됩니다

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

RIPv2 는 일반 텍스트, MD5 인증, 라우팅 요약, CIDR 및 VLSM 을 지원합니다.

RIP 작업 목록 구성

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

- RIP을 시작합니다.
- RIP 경로가 단일 프로그램 broadcast를 업데이트하도록 허용한다

- 라우팅 가중치에 Offset 적용
- 타이머 조정하기
- RIP 버전 번호 지정하기
- RIP 인증 활성화
- 라우팅 요약 금지하기
- 소스주소의 인증 금지하기
- 최대 경로 수 구성
- Split-Horizon 활성화 또는 금지
- RIP 모니터링 및 유지보수

RIP 구성작업

RIP 시작하기

스위치 구성모드에서 다음 명령어를 실행하여 RIP 를 활성화합니다.

명령어	설명
router rip <Process ID>	RIP 라우팅 프로세스를 활성화합니다.
Interface vlan <Vlan ID> **ip rip** <Process ID> **enable**	RIP 라우팅 프로세스를 인터페이스 vlan 에 넣어 사용합니다.

단일 프로그램 broadcast를 업데이트 하도록 RIP라우팅을 허용하기

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

라우팅 정보 교환을 사용하려면 스위치 구성 모드에서 다음 명령을 실행하십시오.

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

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

라우팅 가중치에 Offset 적용

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

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

타이머 조정하기

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

명령어	설명
timers holddown *value*	라우팅 테이블에서 경로가 삭제되는 데 필요한 시간을 나타냅니다.
timers expire *value*	이는 경로가 비효율적으로 선언되기 위해 필요한 간격을 의미합니다.
timers update *value*	라우팅 업데이트 정보의 전송빈도를 의미합니다.
timers trigger *value*	라우팅 트리거 정보의 전송빈도를 의미힙니다.
timers peer *value*	peer 값의 전송 시간 종료를 의미합니다.

RIP 버전 번호 지정하기

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

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

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

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

인터페이스 내에 다음 명령을 실행하십시오.

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

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

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

RIP 인증 활성화

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

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

참고:

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

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

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

인터페이스 구성 모드에서 다음 명령을 실행하여 RIP 의 MD5 인증을 구성합니다.

명령어	설명
ip rip authentication md5	MD5 인증을 사용하여 구성합니다.
ip rip md-key [*key-ID*] **md5 <0,7>**[*key*]	MD5 인증의 PIN 및 ID 를 구성합니다

라우팅 요약 제한

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

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

명령어	설명
no auto-summary	자동 경로요약 기능을 비활성화합니다.

소스 ip 주소의 인증 금지

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

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

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

최대 경로의 수 구성

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

명령어	설명
maximum-nexthop *number*	로컬 RIP 경로의 최대 수를 구성합니다.
no maximum-nexthop	기본 최대 경로의 수를 재개합니다.

Split-Horizon 활성화 와 비활성화

일반적으로 Broadcast IP 네트워크에 연결하고 원거리 벡터 라우팅 프로토콜을 채택하는 스위치는 라우팅 경로의 가능성을 줄이기 위해 Split-Horizon 을 채택합니다. Split-Horizon 의 라우팅 루프에 대한 정보는 라우팅 정보를 수신하는 인터페이스로 자기자신을 선언합니다. 이러한 방식으로, 특히 루프가 끊어 질 때 여러 라우팅 스위치 간의 통신이 향상됩니다. 그러나 Broadcast 가 없는 네트워크만큼 좋지는 않습니다. 이 시점에서 Split-Horizon 을 금지 할 수 있습니다.

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

다음 명령을 실행하여 Split-Horizon 을 활성화하거나 비활성화 하세요

명령어	설명
ip rip split-horizon	Split-Horizon 를 활성화합니다
no ip rip split-horizon	Split-Horizon 를 활성화하지 않습니다.

기본적으로 수평 분할은 지점 간 인터페이스에서 활성화됩니다. 그만큼
point-to-multiple 인터페이스는 금지되어 있습니다.
적의 세부 사항은 "split-horizon 예제"섹션을 참조하십시오.

Note:

정상적인 경우 프로그램이 상태를 변경해야 한다는 확신이 없는 경우 기본 구성을 변경하지 마십시오. Split-Horizon 이 패킷 교환망을 연결하는 직렬 포트에서 금지되어있는 경우 Split-Horizon 을 금지해야 합니다.
네트워크의 상대적 다중 프로그램 그룹의 스위치에서.

Rip를 유지보수 및 모니터링하기

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

모든 라우팅 통계 정보를 표시하려면 관리모드에서 다음명령을 실행하십시오:

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

라우팅 프로토콜 정보를 추적하려면 관리 모드에서 다음 명령을 실행하십시오.:

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

BEIGRP 구성하기

개요

BEIGRP 에서 사용되는 기술은 거리 벡터 프로토콜과 유사합니다.

- 라우터는 라우터가 제공 한 정보에 따라 라우팅을 결정합니다.
- 라우터는 직접 연결하는 Neighbor에게 라우팅 정보를 제공합니다.
- 라우터는 직접 연결하는 Neighbor에게 라우팅 정보를 제공합니다.
  그러나 BEIGRP는 거리 벡터 프로토콜 보다 더 은 장점을 가지고 있습니다.
- BEIGRP는 목적지에 접근 할 수없고 교체 가능한 경로가 없을 때 Neighbor을 질의 할 수있다. 따라서 BEIGRP의 수렴 속도는 최상의 링크 상태 프로토콜이다.

BEIGRP 의 확산 된 업데이트 알고리즘 (DUAL)은 BEIGRP 가 다른 전통적인 거리 벡터 프로토콜보다 우수한 핵심적인 이유입니다. 항상 활성 상태이며 목적지에 액세스 할 수 없고 교체 가능한 경로가 없는 경우 인접 라우터에 질의합니다. 따라서 BEIGRP 의 수집 속도가 빠릅니다.

BEIGRP 는 EIGRP 요구 사항을 기반으로 설계된 특수 전송 프로토콜입니다. BEIGRP 는 IP 프로토콜에서 생성됩니다. BEIGRP 는 다음 요구 사항을 만족시킨다

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

BEIGRP 구성 업무 목록

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

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

BEIGRP 구성 작업

BEIGRP 활성화하기

BEIGRP 프로세스를 작성하려면 다음을 수행하십시오.

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

위의 구성이 완료되면 BEIGRP 는 네트워크 세그먼트의 모든 인터페이스에서 실행되기 시작합니다. BEIGRP 는 hello 메시지를 통해 새로운 Neighbor 을 찾고 업데이트 정보를 통해 원래의 경로와 상호 작용합니다.

대역폭 점유율 구성하기

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

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

BEIGRP 복합 거리에 대한 규정 계수

어떤 경우에는 BEIGRP 복합 거리의 계수가 최종적으로 라우팅 정책에 영향을 미칠 필요가 있다. BEIGRP 가 사용하는 기본 계수는 대부분의 네트워크 조건에 적합하지만 일부 특수한 경우에는 규제해야 합니다. 규제로 인해 전체 네트워크가 크게 변경 될 수 있습니다. 이 규정을 수행 할 때 주의하십시오.

경로 구성모드에서 다음명령을 실행하십시오.

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

Offset을 통한 복합 거리 조정하기

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

명령어	설명
offset{type number | *} {**in** | **out**}	Offset 테이블을 적용합니다.

자동 요약 기능 비활성화

BEIGRP 의 자동 수집은 다른 동적 라우팅 프로토콜과 다릅니다.
다음 규정을 준수합니다.

- BEIGRP 프로세스의 여러 네트워크가 정의되면 네트워크의 하나 이상의 서브넷이 BEIGRP 토폴로지 테이블에 있으면 네트워크의 요약 경로가 생성됩니다.
- 생성 된 요약 경로는 모든 서브넷의 최소 거리를 갖는 Null0 인터페이스를 지향합니다. 요약 경로는 기본 IP 라우팅 테이블에도 추가됩니다. 관여 거리는 5 (구성 할 수 없음)입니다.
- 업데이트 정보가 다른 주 IP 네트워크의 Neighbor 노드로 전송되면 룰 1과 룰 2의 요약 라우트 서브넷이 취소됩니다. 요약 경로만 전송됩니다.
- BEIGRP 절차에서 정의 된 망에 속하지 않는 서브넷은 수집되지 않습니다.

일부 네트워크 환경에서는 각 세부 경로를 Neighbor 에게 알릴 수 있습니다. 이 경우 다음 명령을 실행해야 합니다.

명령어	설명
no auto-summary	자동 요약 경로를 실행하지 않습니다.

전송 경로 구성하기

BEIGRP 가 다른 유형의 경로를 전달할 때, 다음 규정을 준수합니다.

- 현재 경로가 정적 또는 직접 연결되어 있는 경우, 명령 default-metric을 구성 할 필요가 없으며 다른 복합 거리 매개 변수 (대역폭, 지연, 신뢰성, 유효로드 및 MTU)를 현재 포트에서 직접 가져올 수 있습니다.
- 현재 경로가 다른 BEIGRP 프로세스의 경로 인 경우 default-metric 명령을 구성할 필요가 없으며 BEIGRP 프로세스에서 복합 매개 변수 매개 변수를 직접 가져올 수 있습니다.
- default-metric 명령은 rip 및 ospf와 같은 다른 프로토콜의 라우트가 전송 될 때 구성되어야합니다. 경로 전달의 적절한 거리는 구성 값에 의해 결정됩니다. 명령이 구성되어 있지 않으면 경로 전달이 작동하지 않습니다.

BEIGRP 와 RIP 가 동시에 실행되는 스위치에서 BEIGRP Neighbor 라우터가 로컬 스위치의 RIP 프로토콜에 대해 학습 한 경로를 알리려면 다음 명령을 실행합니다.

명령어	설명
default-metric bandwidth delay reliability loading mtu	경로 전달의 기본 백터 거리를 구성합니다.
redistribute *protocol* [**route-map** *name*]	경로를 BEIGRP 프로토콜로 전달합니다.

다른 BEIGRP 매개변수 구성하기

다른 네트워크 조건에 BEIGRP 를 효율적으로 만들려면 다음을 수정해야합니다.

- BEIGRP가 hello 메시지와 Neighbor 시간 초과를 보낼 간격을 수정하십시오.
- Split-Horizon 비활성화

BEIGRP가 Hello메시지와 인접과의 Timeout 일 경우 보내기 위한 간격을 생성합니다.
올바른 BEIGRP 작업을 수행하기 위해 BEIGRP hello 프로토콜에 필요한 다음과 같은 정보가 나열됩니다.

- 새로운 접근 가능한 Neighbor을 발견 할 수 있으며 Neighbor 검출은 구성없는 자동 프로세스입니다.
- Neighbor 구성을 인증하고 호환 모드로 구성된 Neighbor 간의 통신만 허용합니다.

- Neighbor의 유용성을 지속적으로 모니터링하고 Neighbor들 실종을 감지합니다.

라우터는 BEIGRP 가 실행되는 인터페이스에서 hello 멀티프로그램 Broadcast 패킷을 보냅니다. 각 BEIGRP 지원 라우터는 이러한 멀티프로그램 Broadcast 패킷을 수신합니다. 따라서 모든 Neighbor 을 찾을 수 있습니다.

Hello 프로토콜은 두 개의 타이머를 사용하여 Neighbor 의 소멸을 감지합니다. hello 간격은 라우터의 인터페이스에서 BEIGRP hello 메시지의 전송 빈도를 지정합니다. hold timer 는 라우터가 지정된 Neighbor 으로부터 데이터를 수신 할 수 없을 때 Neighbor 이 죽었다 고 선언 할 시간을 지정합니다. Neighbor 라우터로부터 어떤 종류의 BEIGRP 패킷이 수신 된 후에는 홀드 타이머의 값을 리셋 해야 합니다.

다른 네트워크 유형 과 대역폭은 hello Timer 의 다른 기본값을 채택합니다.

네트워크 유형	상태	**Hello Timer (초)**	**Hold Timer (초)**
LAN 인터페이스	Any	5	15

Hello 프로토콜에서 타이머의 다른 기본값으로 동일한 IP 서브넷을 연결하는 BEIGRP Neighbor 라우터가 다른 hello 타이머 와 Hold 타이머를 사용 할 수 있습니다. 에러가 발생하지 않도록 하려면 각 라우터의 hello 패킷에 hold 타이머를 지정해야 합니다. 각 BEIGRP 라우터는 Neighbor 라우터의 hello 패킷에 지정된 hold 타이머를 사용하여 Neighbor 라우터가 시간 초과되는지 여부를 판단합니다. 이러한 방식으로 하나의 WAN 토폴로지에서 서로 다른 Neighbor 의 장애 감지 타이머가 나타납니다. 특별한 경우 타이머의 기본값은 실제 요구 사항을 충족시킬 수 없습니다.

hello 메시지를 보낼 간격을 수정하려면 다음 명령을 실행하십시오.

명령어	설명
ip beigrp hello-interval *seconds*	인터페이스에 Hello-interval 메시지를 보내는 간격을 수정합니다

Neighbor 의 시간 초과 타이머를 수정하려면 다음 명령을 실행하십시오.

명령어	설명
ip beigrp hold-time *seconds*	Neighbor 의 시간에 초과시간을 정합니다

Split-Horizon 비활성화

Split-Horizon 기능이 일반적으로 적용됩니다. 수신 된 라우팅 정보가 동일한 인터페이스에서 Broadcast 되지 않게 경로에 반복현상을 방지합니다. 어떤 경우에는 Split-Horizon 함수가 좋지 않을 경우 다음 명령을 실행하여 Split-Horizon 함수를 비활성화 할 수 있습니다.

명령어	설명
no ip beigrp split-horizon	Split-Horizon 기능을 비활성화 합니다.

BEIGRP 모니터링과 유지보수하기

다음 명령어를 실행하여 neighbor 의 관계를 정리 할 수 있습니다.

명령어	설명
clear ip beigrp neighbors [*interface*]	Neighbor 의 관계를 정리합니다.

모든 BEIGRP 통계 정보를 표시하려면 다음 명령을 실행하십시오:

명령어	설명
show ip beigrp interfaces [*interface*] *[as-number]*	인터페이스에 대한 정보를 표시합니다.
show ip beigrp neighbors [*as-number* | *interface*]	인접 항목에 대한 정보를 표시합니다.
show ip beigrp topology [*as-number* | all-link | summary | active]	토폴로지 테이블에 대한 정보를 표시합니다

OSPF 구성

개 요

이 장에서는 OSPF 를 구성하는 방법에 대해 설명합니다. OSPF 명령에 대한 자세한 내용은 OSPF 명령에 대한 상대 섹션을 참조하십시오.

OSPF 는 IETF 의 OSPF 팀에서 개발한 IGP 라우팅 프로토콜입니다. IP 네트워크 용으로 설계된 OSPF 는 IP 서브넷 및 외부 라우팅 정보 식별자, 메시지 인증 및 IP 멀티 캐스트를 지원합니다.

우리 스위치의 OSPF 기능은 OSPF V2 (RFC2328 참조)의 요구 사항을 준수합니다. 다음 표에는 실제의 주요 기능이 나와 있습니다.

중요 특징	설명
Stub domain	남은 도메인을 지원합니다.
Rout forwarding	모든 라우팅 프로토콜에 의해 학습 된 경로는 다른 라우팅 프로토콜 도메인으로 전달 될 수 있습니다. 즉, OSPF 는 자동 도메인에서 RIP 가 학습 한 경로를 입력 할 수 있습니다. 그 경로 또한 OSPF 는 RIP 로 내보낼 수 있음을 알게 됩니다.
Authentication	도메인의 인접한 스위치 중 텍스트 및 MD5 인증이 지원됩니다.
Routing interface parameters	구성 가능한 인터페이스 매개 변수에는 출력 비용, 재전송 간격, 인터페이스 출력 지연, 스위치의 우선 순위, 스위치의 종료를 판단하는 간격, hello 패킷의 간격 및 인증 PIN 이 포함됩니다.
Virtual link	가상의 링크를 지원합니다
NSSA area	RFC 1587 참조 하십시오
OSPF in the on-demand circuit	RFC 1793 참조 하십시오.

OSPF 구성 작업 목록

OSPF 는 전체 도메인에서 스위치, ABR 및 ASBR 간에 라우팅 데이터 교환이 필요합니다. 구성을 단순화하기 위해 인증없이 기본 구성으로 실행되도록 할 수 있습니다. 그러나 특정

매개 변수를 수정하는 경우 수정 된 매개 변수가 모든 스위치에서 동일해야 합니다. OSPF 를 구성하려면 다음 작업을 완료해야 합니다. OSPF 를 활성화하는 작업은 필수이며 다른 구성은 선택 사항입니다.

- OSPF의 매개변수 인터페이스 구성하기
- 서로 다른 물리적 네트워크에서 OSPF 구성
- OSPF Area 매개변수 구성
- OSPF의 NSSA 도메인 구성
- OSPF Area에서 경로 요약 구성
- 전달된 경로 요약 구성
- 기본 경로 생성
- Loopback 인터페이스에서 경로 ID 선택
- OSPF의 관리 범위 구성
- 경로 계산을 위한 타이머 구성
- OSPF 모니터링 및 유지 보수

경로 구성의 경우 IP 라우팅 프로토콜 구성에 대한 관련 내용을 참조하십시오.

OSPF 작업 구성하기

OSPF 시작하기

다른 라우팅 프로토콜과 마찬가지로 OSPF 를 활성화하기 전에 OSPF 라우팅 프로세스를 만들어야 합니다. 라우팅 프로세스를 생성 할 때 처리와 관련된 IP 주소
범위와 관련 도메인 ID 를 배포 해야 합니다.

전역 구성 모드에서 다음 명령을 실행하여 OSPF 를 시작합니다.

명령어	설명
router ospf *process-id*	OSPF 라우팅 프로토콜을 활성화와 스위치 구성 모드를 시작합니다.

network *address mask* **area** *area-id*	OSPF 및 관련 인터페이스 도메인 ID 의 실행중인 인터페이스를 구성합니다.

OSPF 인터페이스 매개변수 구성하기

요구 사항에 따라 인터페이스의 OSPF 변수를 수정할 수 있습니다. 변수를 수정할 때 연결된 네트워크의 모든 스위치에서 매개 변수가 동일한 지 확인하십시오.

인터페이스 구성에서 다음 명령을 실행하여 인터페이스 매개 변수를 구성하십시오.

명령어	설명
ip ospf cost *cost*	OSPF 인터페이스에서 전송 패킷의 값을 구성합니다.
ip ospf retransmit-interval *seconds*	동일한 OSPF 인터페이스에서 neighbor 사이의 LSA 재전송 시간 (초)을 구성합니다.
ip ospf transmit-delay *seconds*	OSPF 인터페이스에서 LSA 를 보낼 시간을 구성합니다 (단위: 초).
ip ospf priority *number*	라우팅 스위치가 OSPF 에서 DR 이 되도록 되도록 우선 순위 번호를 구성합니다.
ip ospf hello-interval *seconds*	OSPF 인터페이스에서 hello 패킷을 보내는 간격을 구성합니다.
ip ospf dead-interval *seconds*	Dead-interval 을 구성합니다. 소정의 간격에서, neighbor 들로부터 hello 패킷이 수신되지 않으면, 인접 스위치는 shutdown 상태로 간주합니다.
ip ospf authentication *message-digest*	네트워크 세그먼트에서 인접 라우터의 인증 암호를 나타냅니다. OSPF 인증 암호가 채택됩니다.
ip ospf message-digest-key *keyid* md5 *key*	MD5 인증을 사용하려면 OSPF 가 필요합니다
ip ospf passive	포트에서 hello 메시지의 상태를 구성합니다.

서로 다른 물리적 네트워크에서 OSPF 구성

OSPF 는 네트워크의 물리적 미디어를 다음과 같은 클래스로 나눕니다.

- Broadcast 네트워크 (Ethernet, Token Ring, FDDI)
- Non-broadcast 와 다중 접속 네트워크(SMDS, Frame Relay, X.25)
- Point-to-point 네트워크(HDLC, PPP)

X.25 및 Frame-relay 네트워크는 선택적 broadcast 기능을 제공합니다. map 명령을 통해 broadcast 네트워크에서 실행되도록 OSPF 를 구성합니다.. map 명령에 대한 자세한 내용은 WAN 명령어 참조안에 map 명령에 대한 설명을 참조하십시오

OSPF 네트워크 유형 구성

네트워크가 속한 물리적 미디어 유형에 상관없이 네트워크를 Broadcast 네트워크 또는 non-Broadcast 및 다중 접근성 네트워크로 구성 할 수 있습니다. 이 기능을 사용하면 네트워크를 유연하게 구성 할 수 있습니다. Broadcast 네트워크를 non-Broadcast 및 멀티 액세스 네트워크로 구성 할 수 있습니다. Broadcast 네트워크에 X.25, 프레임 릴레이 및 SMDS 와 같은 non-Broadcast 네트워크를 구성 할 수도 있습니다. 이 기능은 neighbor 의 구성을 용이하게 합니다. 자세한 내용은 non-Broadcast 네트워크의 OSPF 구성에 대한 내용을 참조하십시오.

Broadcast 네트워크 또는 non-Broadcast 네트워크에 non-Broadcast 및 멀티 액세스 네트워크를 구성하는 것은 두 개의 랜덤 스위치 간에 가상 링크가 존재한다고 가정하거나 네트워크가 그물형 네트워크라고 가정하는 것입니다. 이전 구성은
비용이 너무 많이 들기 때문에 비현실적입니다. 부분 Broadcast 및 다중 액세스 네트워크를 부분적으로 그물형 된 네트워크로 구성 할 수 있습니다. 비용을 절약하기 위해 non-Broadcast 및 멀티 액세스 네트워크를 지점 간 네트워크로 구성 할 수 있습니다. 분리 된 스위치는 가상 링크를 통해 라우팅 정보를 서로 교환 할 수 있습니다.
OSPF 지점을 다른 지점에 연결하는 인터페이스는 지점 간 (point-to-multipoint) 네트워크 인터페이스로 정의됩니다. 그것은 많은 호스트 경로를 만듭니다. 비교
Non-broadcast 및 멀티 액세스 네트워크 또는 지점 간 네트워크의 경우 OSPF point-to-multipoint 네트워크에는 다음과 같은 이점이 있습니다.

- point-to-multipoint network는 쉽게 구성 할 수 있습니다.
- Point-to multipoint network는 전체 메시 네트워크의 토폴로지가 필요하지 않으므로 비용이 적다
- 더 신뢰할 수 있습니다. 가상 링크가 실패하더라도 연결은 계속 작동 할 수 있습니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 OSPF 네트워크 유형을 구성합니다.

인터페이스 구성 모드에서 명령을 실행하여 OSPF 네트워크의 유형을 구성하십시오

명령어	설명
ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] }}	OSPF 의 형태의 네트워크로 구성한다.

Broadcast network 는 하나의 스위치의 네트워크이다.

매개변수 지역 구성하기

구성 가능한 Area 매개 변수에는 인증, 스텁 Area 및 기본 라우팅 요약 값이 포함됩니다. 인증은 암호 보호를 기반으로 합니다. 스텁 Area 은 외부 경로가 전송되지 않는 Area 입니다. ABR 은 기본값을 생성합니다.

스터브 Area 에 들어가기 한 외부 경로. 자동 Area 외부의 외부 네트워크에 스텁 Area 을 연결할 수 있습니다. OSPF 스텁이 지원하는 기능을 사용하려면 스텁 Area 에서 기본 경로를 사용해야합니다. 스텁 Area 에 들어가기 위해 LSA 를 추가로 줄이려면 ABR 에서 옵션 없음을 선택해야합니다.
스위치 매개 변수를 구성하려면 스위치 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
area *area-id* **authentication simple**	OSPF Area 의 인증을 활성화합니다.
area *area-id* **authentication message-digest**	MD5 인증을 인증 OSPF 로 지정합니다.
area *area-id* **stub** [no-summary]	Stub Area 을 정의합니다.
area *area-id* **default-cost** *cost*	스텁 Area 의 기본 경로 값을 구성합니다.

OSPF Area에서의 라우팅 요약 구성

이 기능을 사용하면 ABR 은 다른 지역으로 요약 경로를 Broadcast 할 수 있습니다. OSPF 에서 ABR 은 모든 네트워크를 다른 Area 으로 Broadcast 합니다. 일부 방법에 따라 네트워크 번호가 순차적으로 분배되는 경우 ABR 을 구성하여 요약 경로를 다른 Area 에 broadcasting 요약 경로는 특정 범위의 모든 네트워크를 포괄 할 수 있습니다.

스위치 구성 모드에서 다음 명령을 실행하여 주소 범위를 구성하십시오.

명령어	설명
area *area-id* **range** *address mask*	요약 Area 의 주소 범위를 구성합니다.

전달 된 라우팅 요약 구성

경로가 다른 Area 에서 OSPF Area 으로 분배 될 때, 각 경로는 외부 LSA 방법으로 고유하게 Broadcast 됩니다. 그러나 특정 주소 Area 을 포함 할 수 있는 경로를 Broadcast 하도록 스위치를 구성 할 수 있습니다. 이 방법은 OSPF 연결 상태 데이터베이스의 크기를 줄입니다.

스위치 구성 모드에서 다음 명령을 실행하여 요약 경로를 구성하십시오.

명령어	설명
summary-address *prefix mask* [not advertise]	분산 경로를 다루는 주소와 마스크를 설명합니다. 하나요약 라우트는

기본 경로 생성

ASBR 에서는 OSPF 경로 Area 에 들어가기 위해 기본 경로를 생성해야 합니다.

OSPF Area 에 경로를 배포하도록 스위치를 구성하면 경로가 자동으로 ASBR 이 됩니다. 그러나 기본 ASBR 은 기본 경로를 생성하지 않아 OSPF 라우팅 Area 에 들어갑니다.

ASBR 이 기본 경로를 생성하도록 스위치 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
default-information originate [always]	목표 ASBR 기본 경로를 생성하도록 합니다.

Loopback 인터페이스를 통한 경로 ID선택

OSPF 는 인터페이스에 구성된 최대의 값을 IP 주소를 스위치 ID 로 사용합니다. IP 주소를 연결하는 인터페이스가 다운 상태로 변경되거나 IP 주소가 취소 된 경우 OSPF 프로세스는 새 스위치 ID 를 다시 계산하고 모든 인터페이스에서 라우팅 정보를 다시 보냅니다. 인터페이스가 IP 주소로 구성되면 스위치는 IP 주소를 ID 로 사용합니다. Loopback 인터페이스는 절대로 다운 상태가 되지 않습니다. 따라서 라우팅 테이블은 안정적입니다. 스위치는 우선적으로 Loopback 인터페이스를 스위치 ID 로 사용합니다. 또한 스위치 ID 로 최대 IP 주소를 선택합니다. Loopback 인터페이스가 없으면 스위치의 큰 값의 IP 주소가 스위치 ID 로 간주됩니다. 특수 인터페이스를 사용하려고 OSPF 를 지정하는 건 불가능합니다.

글로벌 루프 모드에서 다음 명령을 실행하여 IP Loopback 인터페이스를 구성하십시오.

명령어	설명
interface loopback 0	Loopback 인터페이스를 생성하고 인터페이스 구성 모드를 시작합니다.
ip address *ip-address mask*	인터페이스의 IP 주소를 분배합니다.

OSPF 관리 공간 구성

관리 공간은 단일 스위치 또는 스위치 그룹과 같은 라우팅 소스정보의 신용 수준을 나타냅니다. 일반적으로 관리 공간은 0 에서 255 사이의 정수입니다. 숫자가

클수록 신용도가 낮아집니다. 만약 관리 공간이 255 인 경우 라우팅 소스 정보가 신뢰 되지 않거나 생략되어야 합니다.

OSPF 는 세 가지 종류의 서로 다른 관리 공간 (Area 간 및 내-외부)를 사용합니다. 한 지역의 경로를 intra-area 경로라고 부릅니다. 다른 지역으로 가는 경로를 inter-area 경로라고 부릅니다. 다른 라우팅 프로토콜 Area 에서 분산 된 경로를 external-area 경로라고 합니다. 각 경로의 유형 기본값은 110 입니다.

스위치 구성 모드에서 다음 명령을 실행하여 OSPF 의 거리 값을 구성 합니다.

명령어	설명
distance ospf [intra-area *dist1*] [inter-area *dist2*] [external *dist3*]	Area 내 경로, Area 간 경로 및 외부 경로의 관리 거리 값을 수정합니다.

경로 계산을 위한 타이머구성

OSPF 가 토폴로지 변경 정보를 수신하고 계산이 시작될 때까지 지연 시킬 수 있습니다. 연속적으로 SPF 를 계산하는 간격을 구성 할 수도 있습니다. 스위치 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
timers delay-timer *delaytime*	라우팅 계산의 지연시간을 구성합니다.
timers hold-timer *holdtime*	라우팅 계산의 최소 간격을 구성합니다.

OSPF 모니터링 및 유지보수하기

네트워크 통계정보에는 IP 라우팅 테이블, 캐시 및 데이터베이스의 내용이 포함됩니다. 모든 정보는 네트워크 리소스 사용을 판단하고 네트워크 문제를 해결하며 네트워크 노드의 연결 가능성을 확인하고 패킷이 네트워크를 통과하는 경로를 찾는데 도와줍니다.

모든 라우팅 통계 정보를 표시하려면 다음 명령을 실행하십시오.

명령어	설명
Show ip ospf [*process-id*]	OSPF 프로세스의 정보를 표시합니다.

Show ip ospf [*process-id*] **database** **show ip ospf** [*process-id*] **database [router]** [*link-state-id*] **show ip ospf** [*process-id*] **database [router] [self-originate]** **show ip ospf** [*process-id*] **database [router] [adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database [network]** [*link-state-id*] **show ip ospf** [*process-id*] **database [summary]** [*link-state-id*] **show ip ospf** [*process-id*] **database [asbr-summary]** [*link-state-id*]	OSPF 데이터베이스에 대한 상대적 정보를 표시합니다.
show ip ospf border-routers	ABR 과 ASBR 간의 라우팅 테이블에 내부 항목을 표시합니다.
show ip ospf interface	OSPF 인터페이스에 대한 정보를 표시합니다.
show ip ospf neighbor	인터페이스에 따라 OSPF 의 neighbor 에 대한 정보를 표시합니다.
debug ip ospf adj	OSPF 인접 구축 절차를 모니터링합니다.
debug ip ospf events	OSPF 인터페이스 및 인접 이벤트를 모니터합니다.
debug ip ospf flood	OSPF 데이터베이스의 초과를 모니터합니다.
debug ip ospf lsa-generation	OSPF 의 LSA 생성을 모니터링합니다.
debug ip ospf packet	OSPF 메시지를 모니터합니다.
debug ip ospf retransmission	OSPF 의 메시지 재전송을 모니터합니다.
debug ip ospf spf **debug ip ospf spf intra** **debug ip ospf spf inter** **debug ip ospf spf external**	OSPF 의 SPF 계산 경로를 모니터링합니다.
debug ip ospf tree	OSPF 의 SPF 트리 구성을 모니터링합니다.

OSPF 및 VLSM 구성 예제

OSPF 및 고정 경로는 VLSM 을 지원합니다. VLSM 을 통해 서로 다른 인터페이스의 다른 마스크에서 동일한 네트워크 번호를 사용할 수 있습니다. 따라서 IP 주소가 저장되고 주소 공간이 효과적으로 활용됩니다. 다음 예에서는 30 자리 서브넷

마스크가 사용됩니다. 2 자리 주소 공간은 직렬 포트의 호스트 주소 용으로 예약되어 있습니다. 두 개의 호스트 주소로 충분합니다.

```
interface vlan 10
                ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernets
interface vlan 11
                ip address 131.107.254.1 255.255.255.252
! 2 bits of address space reserved for serial lines
! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
                network 131.107.0.0 255.255.0.0 area 0.0.0.0
```

OSPF 경로와 경로 분배의 구성 예

OSPF 는 내부 스위치, ABR(Area Bounder Router) 및 ASBR(Autonomous System Border Router) 간에 정보를 교환해야 합니다. 최소 구성에서 OSPF 기반 스위치는 기본 매개 변수 구성으로 작동할 수 있습니다. 인증을 요구하지 않습니다.

다음은 세 가지 구성 예입니다.

첫 번째 예는 기본적인 OSPF 명령을 보여줍니다.

두 번째 예는 자동 라우팅 스위치, ABR 및 ASBR 을 자동 시스템에 구성하는 방법을 보여줍니다.

세 번째 예는 모든 종류의 OSPF 도구를 사용하는 방법을 보여줍니다.

기본 OSPF 구성 예

다음 예에서는 간단한 OSPF 를 구성하는 방법을 보여줍니다. 라우팅 프로세스 활성화 번호 90 과 이더넷 인터페이스 0 을 Area 0.0.0.0 에 연결하십시오. 한편 RIP 를 OSPF 로 보내거나 OSPF 를 RIP 로 보냅니다.

```
interface vlan 10
ip address 130.130.1.1 255.255.255.0
ip ospf cost 1
interface vlan 10
```

```
ip address 130.130.1.1 255.255.255.0
router ospf 90
network 130.130.0 .0 255.255.0.0 area 0
redistribute rip
router rip
network 130.130.0.0
redistribute ospf 90
```

내부 라우팅 스위치, ABR 및 ASBR 의 기본 구성 예제

다음 예제에서는 네 개의 IP 주소 범위에 네 개의 Area ID 가 배포됩니다. 라우팅 프로세스 (109)가 활성화된다. 네 개의 area 는 area10.9.50.0, area 0, area 2 및 area 3 입니다. Area 10.9.50.0, 2 및 3 의 마스크는 주소 범위로 지정됩니다.
Area 0 에는 모든 네트워크가 포함됩니다.

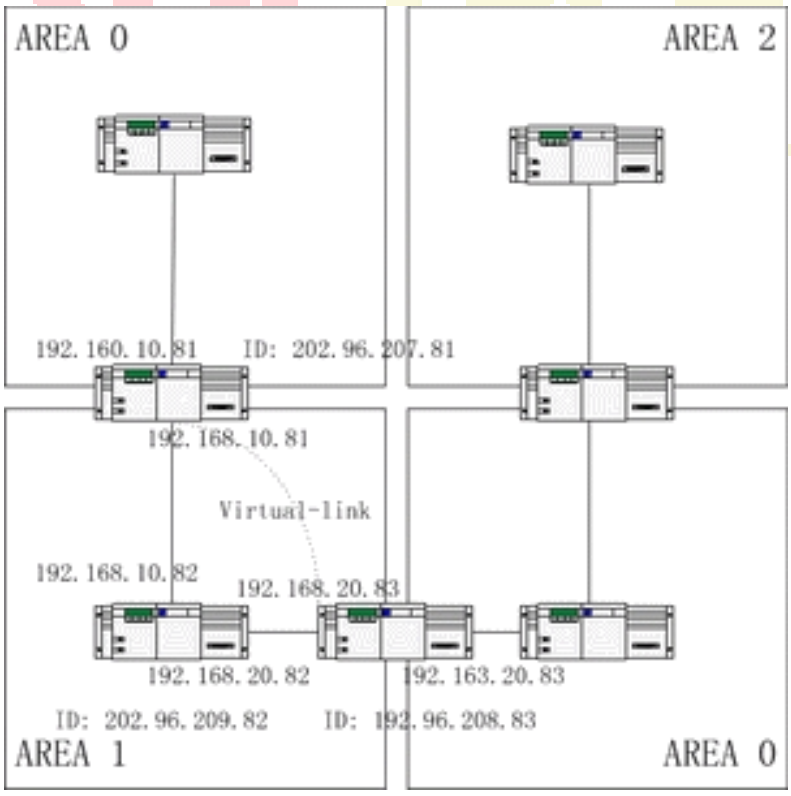
```
router ospf 109
        network 131.108.20.0 255.255.255.0 area 10.9.50.0
        network 131.108.0.0 255.255.0.0 area 2
        network 131.109.10.0 255.255.255.0 area 3
        network 0.0.0.0 0.0.0.0 area 0
! Interface vlan10 is in area 10.9.50.0:
interface vlan 10
        ip address 131.108.20.5 255.255.255.0
! Interface vlan11 is in area 2:
interface vlan 11
        ip address 131.108.1.5 255.255.255.0
! Interface vlan12 is in area 2:
interface vlan 12
        ip address 131.108.2.5 255.255.255.0
! Interface vlan13 is in area 3:
interface vlan 13
        ip address 131.109.10.5 255.255.255.0
! Interface vlan14 is in area 0:
interface vlan 14
        ip address 131.109.1.1 255.255.255.0
! Interface vlan 100 is in area 0:
interface vlan 100
        ip address 10.1.0.1 255.255.0.0
```

네트워크 Area 구성 명령의 기능은 순서가 있으므로 명령 순서가 중요합니다.
스위치는 순서에 따라 IP 주소 / 마스크의 짝을 일치시킵니다. 자세한 내용은 OSPF 명령 섹션을 참조하십시오.
첫 번째 네트워크 Area 을 확인하십시오. Area ID 10.9.50.0 에 대해 구성된 인터페이스 서브넷 131.108.20.0 은 131.108.20.0 입니다. 이더넷 인터페이스는 0 으로 구성됩니다. 따라서 인터페이스는 10.9.50.0 Area 에 있습니다.
두 번째 Area 에서는 다른 인터페이스를 분석하기 위해 이전 프로세스가 채택되면 인터페이스가 1 로 일치합니다. 따라서 인터페이스 1 은 Area 2 를 연결합니다.

다른 네트워크 Area 을 계속 일치시킵니다. 마지막 네트워크 Area 명령은 예외이며, 이는 나머지 모든 인터페이스가 네트워크 Area 0 에 연결된다는 것을 의미합니다.

내부스위치에서의 ABR 과 ASBR 의 복잡한 구성

다음 예는 단일 OSPF 자동 시스템에 여러 스위치를 구성하는 방법을 보여줍니다. 다음 그림은 구성 예에 대한 네트워크 토폴로지를 보여줍니다.



위의 그림에 따라 스위치를 구성하십시오.

RTA :

```
interface loopback 0
                ip address 202.96.207.81 255.255.255.0
!
interface vlan 10
                ip address 192.168.10.81 255.255.255.0
```

!

interface vlan 10

ip address 192.160.10.81 255.255.255.0

!

router ospf 192

network 192.168.10.0 255.255.255.0 area 1

network 192.160.10.0 255.255.255.0 area 0

!

RTB :

interface loopback 0

ip address 202.96.209.82 255.255.255.252

!

interface vlan 10

ip address 192.168.10.82 255.255.255.0

!

interface vlan 11

ip address 192.160.20.82 255.255.255.0

!

router ospf 192

network 192.168.20.0 255.255.255.0 area 1

network 192.168.10.0 255.255.255.0 area 1

!

RTC :

interface loopback 0

ip address 202.96.208.83 255.255.255.252

!

interface vlan 10

ip address 192.163.20.83 255.255.255.0

!

interface vlan 11

ip address 192.160.20.83 255.255.255.0

!

router ospf 192

network 192.168.20.0 255.255.255.0 area 1

network 192.163.20.0 255.255.255.0 area 0

!

ABR에 복잡한 OSPF 구성하기

다음은 ABR 구성 작업에 대한 설명입니다.

- 기본 OSPF 구성하기
- 경로 분배하기

다음은 기본 구성 작업입니다.

(1) 이더넷 0 ~3 에 대한 주소 범위 구성

(2) 모든 인터페이스에서 OSPF 활성화

(3) 각 Area 및 네트워크의 인증 비밀번호 구성

(4) 링크 상태 값 및 기타 인터페이스 매개 변수 구성

참고:
하나의 영역 명령을 각각 사용하여 인증 매개 변수와 스텝 영역을 구성하세요
하나의 명령을 사용하여 이러한 매개변수를 구성할 수 있습니다 .

- 백본 영역 구성(Area 0).

배포와 관련된 구성 작업은 다음과 같습니다.

- IGRP 경로와 RIP 경로를 배포하여 OSPF 매개 변수 구성
  (매트릭, 매트릭 유형, 태그 및 서브넷 포함)을 입력합니다.
- IGRP 경로와 OSPF 경로를 RIP에 배포하십시오. .

다음은 OSPF 의 구성의 예시입니다.

```
interface vlan 10
  ip address 192.168.20.81 255.255.255.0
  ip ospf password GHGHGHG
  ip ospf cost 10
!
```

```
interface vlan 11
  ip address 192.168.30.81 255.255.255.0
  ip ospf password ijklmnop
  ip ospf cost 20
  ip ospf retransmit-interval 10
  ip ospf transmit-delay 2
```

```
   ip ospf priority 4
!
interface vlan 12
   ip address 192.168.40.81 255.255.255.0
   ip ospf password abcdefgh
   ip ospf cost 10
!
interface vlan 13
   ip address 192.168.0.81 255.255.255.0
   ip ospf password ijklmnop
   ip ospf cost 20
   ip ospf dead-interval 80
!
router ospf 192
   network 192.168.0.0 255.255.255.0 area 0
   network 192.168.20.0 255.255.255.0 area 192.168.20.0
   network 192.168.30.0 255.255.255.0 area 192.168.30.0
   network 192.168.40.0 255.255.255.0 area 192.168.40.0
   area 0 authentication simple
   area 192.168.20.0 stub
   area 192.168.20.0 authentication simple
   area 192.168.20.0 default-cost 20
   area 192.168.20.0 authentication simple
   area 192.168.20.0 range 36.0.0.0 255.0.0.0
   area 192.168.30.0 range 192.42.110.0 255.255.255.0
   area 0 range 130.0.0.0 255.0.0.0
   area 0 range 141.0.0.0 255.0.0.0
   redistribute rip
```

RIP 은 네트워크 192.168.30.0. 주소

```
router rip
   network 192.168.30.0
   redistribute ospf 192
 !
```

BGP 구성하기

이 장에서는 경계 게이트웨이 프로토콜 (BGP)을 구성에 대해 설명합니다.
BGP 명령에 대한 자세한 내용은 "BGP 명령" 섹션을 참조하십시오. BGP 는 RFC1163, 1267 및 1771 에 정의된 Exterior Gateway Protocol (EGP)입니다. BGP 를 사용하면 자치 시스템(AS) 간에 라우팅 선택 방법을 만들 수 있습니다. 라우팅 선택 방법을 사용하면 루프없이 자동 관리 시스템 간에 라우팅 선택 정보를 자동으로 교환 할 수 있습니다.

개요

BGP 개요

BGP 에서 각 경로는 네트워크 번호, 경로가 통과하는 자동 관리 시스템 목록 (as-path) 및 기타 속성 목록을 포함합니다. 우리의 스위치 소프트웨어는 BGP 4 버전을 지원합니다. BGP 는 RFC1771 에 정의되어 있습니다. BGP 의 기본 기능은 네트워크를 교환하는 것입니다.

AS 라우팅 테이블에 대한 정보를 포함하여 다른 BGP 시스템과 연결 가능한 정보. AS 라우팅 테이블에 대한 정보는 AS 연결 그림을 구성하고 AS 연결 그림을 통해 AS 레벨 라우팅 정책을 적용하는 데 사용될 수 있습니다. BGP 버전 4 는 CIDR 을 지원합니다. CIDR 은 요약 경로를 만들어 라우팅 테이블의 크기를 줄입니다. 따라서 수퍼 네트워크가 생성됩니다. CIDR 은 BGP 네트워크 클래스의 개념을 취소하고 IP 고정-Broadcast 를 지원합니다. CIDR 은 OSPF, IGRP 및 RIP2 를 통해 전송합니다.

EGP 는 향상된 제어 기능으로 IGP 와 다릅니다. BGP 는 경로를 제어하기위한 여러 가지 선택적 방법을 제공합니다.

- 인접한 라우터들의 Access-list를 사용하여 유동경로의 의하여 고정경로를 필터링합니다.
- 로컬 환경구성 및 용량 MED 같은 BGP라우트들의 속성을 경로를 구성하여 수정하십시오.
- ospf 및 rip과 같은 동적 IGRP와 상호 작용하려면 distribute 명령을 사용하여 경로를 재분배합니다. 따라서 BGP 라우팅 정보가 자동 생성됩니다. BGP 경로는 수동으로 네트워크 및 집합을 구성하여 생성 할 수도 있습니다. BGP경로 생성시 route-map을 사용하여 경로의 속성을 구성합니다.
- 시스템에서 BGP 경로의 우선 순위를 조정하여 BGP 경로의 관리 범위를 distance 명령어를 사용하여 구성하십시오.

BGP 경로 선택

BGP 의 진행 절차는 경로 속성 비교에 기반합니다. 동일한 네트워크에 도달하는 경로가 여러 개인 경우 BGP 는 최적의 경로를 선택합니다. 최적 경로를 선택하는 BGP 절차는 다음과 같습니다.

- 다음 홉에 도달 할 수 없는 경우, 최적 경로가 고려하게 됩니다.
- 경로가 내부 경로이고 동기화가 활성화 된 경우, 경로가 IGP에 없을 때 최적의 경로는 고려되지 않습니다.
- 최대 무게의 경로가 우선적으로 선택됩니다..
- 모든 경로의 가중치가 동일하면 우선 순위가 가장 높은 경로가 우선적으로 선택됩니다.
- 모든 경로가 동일한 로컬 우선순위를 가지면 로컬에 의해 생성 된 경로가 우선적으로 생성 된 것으로 선택됩니다. 예를 들어 라우터가 네트워크 명령 또는 집계 명령을 실행하거나 IGP 경로가 전달 될 때 경로가 생성 될 수 있습니다.
- 로컬 우선 순위가 같거나 로컬 라우터에 의해 라우트가 생성되지 않으면 가장 짧은 AS 경로를 가진 라우트가 먼저 선택됩니다.
- AS 경로가 동일하면 Origin 속성 값이 가장 작은 경로 (IGP <EGP <INCOMPLETE)가 먼저 선택됩니다.
- Origin 속성 값이 같으면 MED 값이 가장 작은 경로가 먼저 선택됩니다. bgp always-compare-med가 활성화되어 있지 않으면 MED 값 비교는 동일한 인접 AS의 경로에 대한 것입니다.
- 모든 경로의 MED 값이 같으면 EBGP가 먼저 선택됩니다. 자율 시스템의 모든 경로는 IBGP로 사용됩니다.

각 경로 동일한 연결 속성을 갖는 경우 가장 작은 router-id 를 가진 경로가 먼저 선택됩니다..

BGP 작업 구성

BGP 기본 특성 구성

BGP 구성 작업은 기본 작업과 고급 작업의 두 그룹으로 분류 할 수 있습니다. 기본 작업의 처음 두 항목은 BGP 구성에 필수 항목입니다. 기본 작업 및 고급 작업의 다른 항목은 선택 사항입니다.

BGP 경로선택 활성화하기

글로벌 구성 모드에서 다음 명령을 실행하여 BGP 경로 선택을 활성화합니다.

명령어	설명
router bgp *autonomous-system*	라우터 구성 모드에서 BGP 라우팅 프로세스를 활성화합니다.
network *network-number/masklen [route-map*	네트워크를 로컬 자치 시스템으로 표시하고 BGP 테이블에 추가합니다.

참고:

1) EGP의 경우 라우터 구성 네트워크의 명령어 사용하여 IP 네트워크를 구성 할 때 어떤 네트워크가 알림을 받을 수 있는지 제어 할 수 있습니다. 그것은 IGP와 반대입니다. 예를 들어, RIP 프로토콜은 네트워크 명령을 사용하여 업데이트가 전송되는 위치를 결정합니다.

2) network 명령을 사용하여 IGP 경로를 BGP 라우팅 테이블에 추가 할 수 있습니다. 구성된 RAM 과 같은 라우터 리소스가 사용 가능한 네트워크 명령의 상한을 결정합니다. 추가 선택 사항으로 redistribute 명령을 실행할 수도 있습니다.

BGP Neighbor 구성

외부와 라우팅 정보를 교환하려면 BGP 네이버를 구성해야 합니다.

BGP 는 IBGP 와 EBGP 의 두 neighbor 을 지원합니다. 내부 Neighbor 은 같은 AS 에 있습니다. 외부 Neighbor 은 다른 AS 가 있습니다. 일반적으로 외부 Neighbor 은 밀접하게 인접 해 있으며 서브넷을 공유합니다. 내부 Neighbor 는 같은 AS 의 어느 곳에 나 있습니다.

라우터 명령을 사용하여 BGP neighbors 를 구성합니다.

명령어	설명
neighbor {*ip-address* } **remote-as** *number*	BGP neighbor 를 설계합니다.

자세한 사항은 "BGP Neighbor 구성 예제"를 참조하시기 바랍니다.

BGP 정렬 재구성 구성

일반적으로 BGP neighbor 라우터는 연결이 생성 될 때만 모든 경로를 교환합니다. 그런 다음 변경된 경로 만 나중에 교환합니다. 구성된 라우팅 정책이 변경된 경우 변경된 라우팅 정책을 수신 된 경로에 적용하기 전에 BGP 세션을 지워야 합니다. 그러나 BGP 세션을 지우면 고속 캐시를 비활성화하고 네트워크 실행을 손상시킬 수 있습니다. BGP 세션을 지우지 않고 정책을 구성하고 활성화하는 데 도움이 되기 때문에 Soft 재구성 기능을 채택하는 것이 좋습니다. 현재,

새로운 Soft 재구성 기능은 각각의 neighbor 에 적용될 수 있다. 새로운 소프트 재구성은 neighbor 에 의해 생성 된 수신 업데이트에 적용되며 수신 소프트 재구성이라고 합니다. 새로운 소프트 재구성을 사용하여 출력되는 업데이트를 neighbor 로 전송하는 경우 이를 출력 소프트 재구성 이라고 합니다. 입력 소프트 재구성을 실행 한 후 새 입력 정책이 유효한지 확인합니다. 출력 소프트 재구성을 실행 한 후에는 새 로컬 출력 정책이 BGP 세션을 재구성하지 않고 유효성을 검사합니다.

BGP 세션을 리셋 하지 않고 입력 된 업데이트를 생성하기 위해 로컬 BGP 세션의 라우터는 수정없이 수신 된 들어오는 업데이트를 복원해야 합니다. 입력 된 업데이트가 현재 들어오는 정책에 의해 수신되거나 거부되는지 여부는 고려 대상이 아닙니다. 이 경우 메모리가 많이 사용됩니다. 발신 재구성에는 추가 메모리 비용이 없으므로 항상 유효합니다. BGP 의 다른 쪽에서 나가는 소프트 재구성을 트리거 할 수 있습니다

세션을 사용하여 새 로컬 들어오는 정책의 유효성을 검사합니다. 들어오는 소프트 재구성을 허용하려면 수신 된 모든 라우팅 업데이트를 복원하도록 BGP 를 구성해야 합니다. 발신 소프트 재구성에는 사전 구성이 필요하지 않습니다.

BGP SOFT 재구성을 구성하려면 다음 명령을 실행하십시오.

명령어	설명
Neighbor { ip-address } soft-reconfiguration [inbound]	BGP soft 를 재구성하여 구성합니다.

BGP 연결

두 개의 라우터가 BGP Neighbor 로 정의되면 BGP 연결을 만들고 경로 선택 정보를 교환합니다. BGP 라우팅 정책이 나중에 수정되거나 다른 구성이 변경되면 BGP 연결을 재구성하여 변경된 구성의 유효성을 검사해야 합니다. 다음 명령 중 하나를 실행하여 BGP 연결을 재구성하십시오

명령어	설명
clear ip bgp *	Resets 모든 BGP 연결을 재구성합니다.
clear ip bgp *address*	특정 BGP 연결을 재구성합니다.

BGP 와 IGPs 간의 동기화 구성

AS 가 자신의 AS 를 통해 세 번째 AS 에서 정보를 보내는 경우, AS 의 내부 라우팅 상태는 AS 가 다른 AS 에 broadcasting 하는 라우팅 정보와 일치 해야합니다. 예를 들어, AS 의 모든 라우터가 IGP 를 통해 경로를 학습하기 전에 AS 는 BGP 에서 일부 라우터가 라우팅 할 수 없는 라우팅 정보를 수신 할 수 있습니다. BGP 와 IGP 사이의 동기화는 AS 내의 모든 IGP 라우터가 라우팅 정보를 알아낼 때까지 BGP 가 라우팅 정보를 Broadcast 안 한다는 것입니다. 동기화는 기본적으로 활성화됩니다.

어떤 경우에는 BGP 와 IGP 간의 동기화를 수행 할 필요가 없습니다. 다른 AS 가 AS 를 통해 데이터를 전송하도록 허용되지 않거나 AS 의 모든 라우터가 BGP 를 실행하는 경우 동기화가 취소됩니다. 동기화가 취소 된 후 IGP 는 몇 개의 경로를 수행 할 수 있으며 BGP 는 더 빨리 집계됩니다.

동기화를 취소하려면 다음 명령을 실행하십시오.

명령어	설명
no synchronization	BGP 와 IGP 사이에 동기화를 취소한다.

동기화를 취소 할 때 BGP 세션을 지우려면 "clear ip bgp" 명령을 실행해야 합니다.
자세한 내용은 " Neighbor 기반 BGP 경로 필터링 예제" 섹션을 참조하십시오.
일반적으로 하나 또는 두 개의 경로 만 IGP 로 전달되고 IGRP 의 외부 경로가
되거나 BGP 세션 스폰서가 기본 AS 경로를 생성합니다. BGP 에서 IGP 로 경로가 전달되면 EBGP 를 통해
얻은 경로 만 전달할 수 있습니다. 대부분의 경우 IGP 는 BGP 에 재 배포되지 않습니다. AS 에있는
네트워크는 라우터 구성 네트워크 명령어를 실행하여 나열됩니다. 따라서 네트워크가 Broadcast 됩니다. 이
방법으로 나열된 네트워크를 로컬 네트워크라고 합니다. BGP 는 IGP 의 origin 속성을 가집니다. 직접 연결된
경로, 고정 경로 또는 IGP 에서 학습 한 경로와 같은 이러한 경로는 주 IP 라우팅 테이블에 있어야
유효합니다. BGP 라우팅 과정에서 주 IP 라우팅 테이블은 주기적으로 스캔 되어 로컬 네트워크가
존재하는지 여부를 탐지하고 이후에 BGP 라우팅 테이블이 업데이트됩니다. BGP 가 경로를 포워드 할 때
주의하십시오. IGP 의 경로는 BGP 를 통해 다른 라우터에 전달 될 수 있습니다. BGP 는 잠재적으로 정보를
IGP 로 보내고 IGP 는 정보를 다시 BGP 로 보냅니다.

BGP 경로 크기 구성

BGP 경로 크기는 경로 선택 프로세스를 제어하기 위해 BGP 경로에 부여되는
번호입니다. 무게는 라우터에 대해 로컬입니다. 가중치 범위는 0 에서 65535 입니다. 로컬 BGP 경로의 기본
크기는 32768 입니다. Neighbor 에서 얻은 경로 크기는
0 입니다. 관리자는 경로 크기를 수정하여 라우팅 정책을 수행 할 수 있습니다.

경로 중량을 구성하려면 다음 명령을 실행하십시오.

명령어	설명
neighbor {*ip-address* } **weight** *weight*	**모든 라우터의 크기 값을 지정합니다.**

라우트 맵을 통한 경로의 크기를 구성가능 합니다.

Neighbor 기반의 BGP 라우팅 필터링 구성

라우터 소프트웨어는 다음과 같은 방법으로 지정된 Neighbor 의 BGP 라우트를 필터링합니다

ip as path-와 **neighbor filter-list**과 함께 **aspath** 목록 필터를 사용합니다**.**

명령어	설명
ip as-path access-list *aspaths-list-name* {**permit	deny**} *as-regular-expression*	BGP 관련 Access-table 정의합니다.

router bgp *autonomous-system*	라우터 구성 모드를 시작합니다
neighbor {*ip-address* } **filter-list** *aspath-list-name* {**in | out** }	BGP 필터를 구성합니다.

ip access-list 및 **neighbor distribute-list** 을 사용하여 액세스 목록을 사용합니다.

명령어	설명
ip access-list standard *access-list-name*	Defines an access list.
router bgp *autonomous-system*	Enters the router configuration mode.
neighbor {*ip-address* } **distribute-list** *access-list-name* {**in | out** }	Establishes a BGP filter.

(5) 접두사 목록을 **ip prefix-list** 및 **neighbor prefix-list**와 함께 사용하십시오.

명령어	설명
ip prefix-list *prefixs-list-name /sequence number* **{ permit |deny }** A.B.C.D/n **ge** x **le** y	prefix list 를 정의합니다..
router bgp *autonomous-system*	라우터 BGP 구성모드로 들어갑니다
neighbor {*ip-address* } **prefix-list**	BGP filter 를 만듭니다..
prefix-list-name {**in | out**}	고정 리스트 이름의 입출력을 구성합니다.

route-map 및 neighbor route-map 명령을 사용하여 route mapping을 사용합니다.

라우트 맵핑은 라우팅 속성을 필터링하고 변경할 수 있습니다.

자세한 내용은 "네이버 기반 BGP 경로 필터링 예제" 섹션을 참조하십시오.

포트기반 BGP 라우트 필터링 구성하기

Access-list 이나 prefix-list 를 사용하여 포트 기반 BGP 라우트 필터링을 구성 할 수 있습니다. 경로의 네트워크 번호 또는 게이트웨이 주소를 필터링 할 수 있습니다. Access-list 를 사용하도록 Access-list 옵션을 지정하거나 prefix-list 을 사용하여 경로의 네트워크 번호를 필터링하려면 prefix-list 옵션을 지정할 수 있습니다. 또한 게이트웨이 옵션을 지정하여 Access-list 를 사용하여 경로의 Nexthop 속성을 필터링 할 수 있습니다. access-list 옵션과 prefix-list 옵션은 함께 사용할 수 없습니다. 별표 (*)를 지정하여 모든 포트의 경로를 필터링 할 수 있습니다.

다음 명령을 실행하여 포트 기반 BGP 라우트 필터링을 구성하십시오

명령어	설명
filter interface { **in | out** }[**access-list** access-list-name] [**prefix-list** prefix-list-name][**gateway**	포트 기반 BGP 라우트 필터링을 구성합니다.

자세한 내용은 "포트 기반 BGP 라우트 필터링 예제" 섹션을 참조하십시오.

BGP-Updated Next Hop 진행중 취소하기

Neighbor 라우터의 BGP 업데이트에 대한 다음 홉 처리를 취소 할 수 있습니다. 구성은 프레임 릴레이 또는 X.25 와 같은 non-broadcast 네트워크에서 유용합니다. 프레임 릴레이 또는 X.25 에서 BGP 출력 라우터는

동일한 IP 서브넷의 다른 모든 neighbor 라우터에 직접 액세스 할 수 없습니다. 다음 방법은 다음 홉 처리를 취소 할 수 있습니다.

- BGP연결을 사용하는 로컬 IP주소는 출력경로의 다음 홉 주소를 사용합니다..
- 라우팅 맵을 사용하여 나가는 경로 또는 들어오는 경로의 다음 홉주소를 하십시오.

다음 홉 처리를 취소하려면 다음 명령을 실행하십시오.

명령어	설명
neighbor {*ip-address*} **next-hop-self**	BGP neighbor 가 업데이트 될 때 다음 홉 처리를 취소합니다.

이전 명령이 사용되면 현재 라우터는 라우트의 다음 홉으로 인식하도록 스스로 알립니다. 따라서 다른 BGP 이웃 라우터는 패킷을 현재 라우터로 보냅니다. 현재 Broadcast 라우터에서 지정된 이웃 라우터로의 경로이기 때문에 non-broadcast 네트워크에서 유용합니다. 그러나 불필요한 여분의 홉 (hop)이 발생하기 때문에
broadcast 네트워크에서는 사용빈도가 낮습니다.

상위 BGP 특징 구성

Route map 을 통한 Route Update 필터링 및 수정

경로 맵은 각 이웃에서 경로 업데이트를 필터링하고 매개 변수의 속성을 수정하는 데 사용할 수 있습니다. 경로 맵은 들어오는 업데이트와 나가는 업데이트에 모두 적용 할 수 있습니다. 경로 업데이트를 보내거나 받을 때 경로 맵을 통과 한 경로 만 처리됩니다. 라우트 맵은 들어오는 업데이트와 나가는 업데이트가 AS 경로, 커뮤니티 및 네트워크 번호를 기반으로 한다는 것을 지원합니다. aspath 명령은 AS 일치에 사용되어야 합니다. 커뮤니티 일치에는 커뮤니티 목록 명령어가 필요합니다. 네트워크 옵션 맞추기 위해서는 ip access-list 명령이 필요합니다

다음 명령을 실행하여 경로 맵을 통해 경로 업데이트를 필터링하고 수정하십시오.

명령어	설명
neighbor {*ip-address*} **route-map** *route-map-name* **{in | out}**	들어오는 경로 나 나가는 경로에 경로 맵을 적용합니다.

집계 주소

비 유형 필드 간 라우트는 라우팅 테이블을 최소화하기 위해 집계 라우트 (및 수퍼 네트워크)를 작성할 수 있습니다. 집계 경로를 BGP 에 재분배하거나 다음 표에 설명 된 집계 속성을 사용하여 구성 할 수 있습니다. BGP 테이블에 적어도 하나 이상의 자세한 레코드가 있으면 BGP 테이블에 집계 주소를 추가하십시오.

다음 명령 중 하나 이상을 사용하여 라우팅 테이블에 집계 주소를 만듭니다.

명령어	설명
Aggregate-address net/len	라우팅 테이블에 집계 주소를 만듭니다.
aggregate-address net/len **summary-only**	요약주소만 Broadcast 합니다.
aggregate-address net/len **attribute-map** map-name	라우트 맵을 통해 지정된 집계 주소를 생성합니다.

"BGP 경로 집계 예" 섹션을 참조하십시오.

BGP 커뮤니티 구성하기

BGP 가 지원하는 라우팅 정책은 BGP 라우팅 정보에 대해 다음 세 가지 값 중 하나를 기반으로 합니다.

- 네트워크 망 경로 번호
- **AS_PATH** 속성의 값
- COMMUNITY 속성의 값

라우트는 COMMUNITY 속성을 통해 커뮤니티로 분류 될 수 있으며 커뮤니티 기반 라우팅 정책은 라우트에 적용될 수 있습니다.

0 -라우팅 정보 제어의 구성이 간단 해진다.

1 -커뮤니티는 동일한 속성을 갖는 라우트 그룹입니다. 각 경로는 여러 커뮤니티에 속할 수 있습니다. AS 관리자는 경로가 속한 커뮤니티를 결정할 수 있습니다.

2 -COMMUNITY 속성은 선택적이고 전송 가능하며 전역 적이며 범위는 다음과 같습니다.

3 -0 ~ 4,294,967,200 인터넷에서 미리 정의 된 유명한 커뮤니티는 다음 표에 나열되어 있습니다

명령어	설명
no-export	자율 시스템의 EBGP 피어를 포함하여 EBGP 피어에 대한 경로를 Broadcast 하지 않습니다.
no-advertise	모든 Peer 에게 경로를 Broadcast 하지 않습니다.
local-as	자치시스템 외부로 경로를 Broadcast 하지 않습니다

BGP 세션 스폰서는 라우트를 생성, 수신 또는 전달할 때 라우트 커뮤니티 속성을 구성, 추가 또는 수정할 수 있습니다. 라우트가 집계 된 후, 집계에는 모든 원래 라우트의 COMMUNITY 속성이 포함됩니다.

COMMUNITY 속성은 기본적으로 인접 항목에 전송되지 않습니다. 다음을 실행하십시오.

명령을 사용하여 COMMUNITY 속성을 지정된 neighbor 으로 보냅니다.

명령어	설명
neighbor {*ip-address* } **send-community**	지정된 Neighbor 에 COMMUNITY 특성을 보냅니다.

커뮤니티 속성을 구성하려면 다음 조작을 수행하십시오.

명령어	설명
route-map *map-name sequence-number*	경로 맵을 구성합니다
router bgp *autonomous-system*	라우터 구성 모드를 시작합니다.
neighbor {*ip-address* } **route-map** *access-list-name* {**in | out** }	경로 맵을 적용합니다.

다음 작업을 수행하여 커뮤니티 속성 기반 라우팅 정보 필터링을 구성합니다.

명령어	설명
ip community-list standard | expended *community-list-name* {**permit | deny**}	커뮤니티 목록을 정의합니다.
route-map *map-name sequence-number* **{deny | permit}**	경로 맵을 구성합니다.
router bgp *autonomous-system*	라우터 구성모드를 시작합니다.
neighbor {*ip-address* } **route-map** *route-map-name* {**in | out** }	경로 맵을 적용합니다.

"BGP 커뮤니티 속성을 통한 라우트 맵 예제" 섹션을 참조하십시오.

A S A (Autonomous System Alliance) 자치 연합 시스템 구성하기

IBGP 연결을 줄이는 방법은 하나의 AS 를 여러 개의 하위 AS 로 나누고 이를 자치 연합시스템으로 분류하는 것입니다. 외부에 관해서는, 동맹은 AS 처럼 보인다. 동맹 내부에 관해서는, 각각의 하위 AS 는 완전 접속되어 있으며 동일한 연합관계에 있는 다른 하위 AS 를 연결합니다. EBGP 세션이 다른 하위 AS 의 Peer 에 존재하더라도 IBGP peer 와 마찬가지로 경로 선택 정보를 교환합니다. 즉, 다음 홉, MED 및 로컬 우선 순위 정보를 저장합니다.
BGP 자치 연합 시스템을 구성하려면 동맹 식별자를 지정해야 합니다. 연합식별자는 AS 번호입니다. 외부에 관해서는, AS 는 동맹 식별자를 AS 번호로 취하는 단일 AS 처럼 보입니다.

다음 명령을 실행해 자치 연합 시스템의 식별자를 구성합니다.

명령어	설명
bgp confederation identifier *autonomous-system*	자치 연합 시스템의 식별자를 구성합니다.

다음 명령을 실행해 자치 연합 시스템에 속한 자치 시스템 번호를 지정합니다

명령어	설명
bgp confederation peers autonomous-system [autonomous-system ...]	자치 연합 시스템에 속한 AS 를 지정합니다.

"BGP 연합 자치 시스템 예제" 섹션을 참조하십시오.

Route Reflector 구성하기

IBGP 연결을 줄이는 또 다른 방법은 reflector 를 구성하는 것입니다.
Route reflector 의 피어는 클라이언트 peer 와 AS 의 다른 라우터 (비-클라이언트 피어)의 두 그룹으로 나뉩니다. Route reflector 는 두 그룹 사이의 경로를 반영합니다. Route reflector 및 클라이언트 피어는 클러스터로 구성됩니다. 비-클라이언트 피어는 완전히 연결되어야 합니다. 클라이언트 피어는 완전히 연결될 필요는 없습니다. 클러스터의 클라이언트는 다른 클러스터의 IBGP 세션 스폰서와 통신하지 않습니다.

Route reflector 가 라우팅 정보를 수신하면 다음 작업을 수행합니다.

- 외부 BGP 세션 스폰서의 경로를 모든 클라이언트와 비-클라이언트 피어로 Broadcast 합니다.
- 비 클라이언트 경로에서 모든 클라이언트로 경로를 Broadcast 합니다.
- 클라이언트에서 모든 클라이언트 피어 및 클라이언트 peer로 경로를 broadcast 합니다. 클라이언트 피어는 완전히 연결될 필요는 없습니다.

다음 명령을 실행하여 로컬 라우터를 Reflector 로 구성하고 이웃 라우터를 클라이언트로 지정하십시오.

명령어	설명
neighbor *ip-address* **route-reflector-client**	로컬 라우터를 route-reflector 로 구성하고 neighbor 클라이언트로 지정합니다.

하나의 AS 에는 다중 경로 reflector 가 있습니다. 경로 reflector 는 IBGP 세션 스폰서를 처리 할 때 다른 **route-reflector** 를 처리합니다. 일반적으로 동일한 클러스터의 클라이언트에는 하나의 **route-reflector** 만 있습니다. 클러스터는 **route-reflector** 의 라우터 ID 로 식별됩니다. 이중화를 추가하고 단일 노드의 장애를 피하려면 하나의 클러스터에 여러 개의 **route-reflector** 가 있을 수 있습니다. 이 경우 클러스터의 모든 경로 reflector 를 4 비트 클러스터 ID 로 구성해야 경로 reflector 가 동일한 클러스터의 다른 경로 reflector 의 업데이트 정보를 식별 할 수 있습니다. 동일한 클러스터의 모든 **route-reflector** 는 완전히 연결되어 있고 동일한 클라이언트 피어 및 비 클라이언트 peer 를 가지고 있어야합니다.

route-reflector 가 클러스터에 있으면 다음 명령을 실행하여 ID 를 구성하십시오.

명령어	설명
bgp cluster-id *cluster-id*	cluster ID 를 구성합니다..

"BGP Route Reflector 구성 예제"섹션을 참조하십시오.

6. peers 종료하기

BGP neighbors 에 shutdown 명령어를 실행합니다.

명령어	설명
neighbor {ip-address } **shutdown**	BGP neighbor 에 shutdown 을 실행합니다..

Run the following command to activate the neighbor:

명령어	설명
no neighbor {ip-address } **shutdown**	BGP neighbor.활성화합니다.

멀티-홉 외부의 피어 구성하기

외부 피어는 기본적으로 직접 연결된 망에 있어야합니다.
다음 명령을 실행하여 멀티 홉 외부 피어를 구성합니다.

명령어	설명
neighbor {ip-address } **ebgp-multihop** ttl	BGP 의 neighbor 를 멀티 홉 외부 peer 로 구성합니다.

BGP 관리 경로 구성하기

관리 거리는 라우팅 프로토콜의 우선 순위를 측정하는 단위입니다. BGP 는 외부 거리, 내부 거리 및 로컬 거리 등 3 가지 종류의 관리 거리를 사용합니다. 외부 BGP 에서 학습 한 경로는 외부 거리를 보여줍니다.

내부 BGP 에서 학습 한 경로는 내부 거리를 보여줍니다. 로컬 경로에는 로컬 거리가 표시됩니다. BGP 경로 관리 거리를 구성하려면 다음 명령을 실행하십시오.

명령어	설명
distance bgp external-distance internal-distance local-distance	BGP route 관리 거리를 구성합니다..

BGP 경로의 관리 거리를 수정하는 것은 위험합니다. 외부 거리는 모든 동적라우팅 프로토콜의 거리보다 짧아야 합니다. 내부 거리는 모든 동적 라우팅 프로토콜의 거리보다 길어야 합니다.

BGP timer 수정하기

BGP keepalive 및 hold-time timer 를 수정하려면 다음 명령을 실행하십시오.

명령어	설명

neighbor *[ip-address	peer-group name]* **timers** *keepalive holdtime*	설계된 피어 또는 피어 그룹의 keepalive 및 holdtime 타이머를 구성합니다 (단위 : 초).

no neighbor timer 명령을 실행하여 BGP neighbor 또는 피어 그룹의 타이머를 기본값으로 다시 시작합니다.

다른 AS 의 경로 MED 비교

MED 는 여러 경로 중에서 최적의 경로를 선택해야 할 때 고려되는 매개 변수입니다. 비교적 작은 MED 값을 가진 경로가 먼저 고려됩니다.

기본적으로 최상의 경로가 선택 될 때 MED 비교는 동일한 AS 의 경로 중에서 만 수행됩니다. 경로 선택에 상관없이 MED 를 비교할 수 있도록 구성 할 수 있습니다.

다른 AS 의 경로 간 MED 비교를 수행하려면 다음 명령을 실행하십시오.

명령어	설명
bgp always-compare-med	AS 의 경로 간 MED 비교를 수행합니다.

BGP 모니터링과 유지보수하기

관리자는 BGP 의 라우팅 테이블이나 다른 데이터베이스의 내용을 찾아보고 삭제할 수 있습니다. 세부 통계 정보의 값을 표시 할 수 있습니다.

BGP 라우팅 테이블 및 데이터베이스 지우기

관리 모드에서 다음 명령을 실행하여 고속 캐시, 테이블 또는 BGP 데이터베이스 지우기 관련 작업을 수행합니다.

명령어	설명
clear ip bgp *	모든 BGP 연결을 재구성합니다.
clear ip bgp *as-number*	지정된 자율 시스템의 BGP 연결을 재구성합니다.
clear ip bgp *address*	지정된 이웃의 BGP 연결을 재구성합니다.
clear ip bgp *address* **soft**	지정된 이웃의 들어오는 또는 나가는 데이터베이스를 지웁니다.
clear ip bgp *aggregates*	경로 집계 중에 생성 된 경로를 지웁니다.

clear ip bgp *networks*	네트워크 명령에 의해 생성 된 경로를 지웁니다.
clear ip bgp peer-group *name*	Peer 의 그룹이름을 지웁니다.
clear ip bgp *redistribute*	프로세서 전달중 생성 된 경로를 지웁니다.

라우팅 테이블 및 시스템 통계 정보 표시

BGP 라우팅 테이블 및 데이터베이스와 같은 자세한 통계 정보를 나타낼 수 있습니다. 이러한 통계 정보는 네트워크 리소스를 완전히 사용하고 네트워크 문제를 해결하는 데 도움이 됩니다.

다른 통계 정보를 표시하려면 다음 명령을 실행하십시오.

명령어	설명
show ip bgp	시스템에 BGP route table 을 보여줍니다..
show ip bgp prefix	접두부 일치하는 목록과 일치하는 경로를 표시합니다.
show ip bgp community	커뮤니티 속성에 대한 통계 정보를 표시합니다.
show ip bgp regexp *regular-expression*	정규 표현식과 일치하는 경로를 표시합니다.
show ip bgp *network*	지정된 BGP 경로를 표시합니다.
show ip bgp neighbors *address*	지정된 이웃의 TCP 연결 및 BGP 연결에 대한 자세한 정보를 표시합니다.
show ip bgp neighbors *[address]* [received-routes | routes | advertised-routes]	특정한 BGP neighbor 로부터 배운 경로를 표시합니다.
show ip bgp paths	모든 BGP 경로 정보를 데이터베이스에 표시합니다.
show ip bgp summary	모든 BGP 연결 상태를 표시합니다.

BGP 정보 추적하기

오류를 찾아서 문제를 해결하려면 BGP 연결 추적, BGP 정보를 추적하여 경로 수신 및 경로 전달을 관찰해야 합니다. 다음 작업을 수행하십시오.

Command	설명
debug ip bgp *	일반적인 BGP 정보를 추적합니다
debug ip bgp all	모든 BGP 정보를 추적합니다
debug ip bgp fsm	BGP 기계 상태를 추적합니다
debug ip bgp keepalive	BGP Keepalive 메시지를 추적합니다
debug ip bgp open	BGP open 메시지를 추적합니다
debug ip bgp update	BGP 업데이트 메시지를 추적합니다.

BGP 구성 예제

BGP route-map 예제

다음 예에서는 route-map 을 사용하여 들어오는 경로의 속성을 이웃 라우터에서 수정하는 방법을 보여줍니다. 인접 라우터 140.222.1.1 에서 수신 한 모든 경로의 가중치를 구성하고 ASPATH 액세스 목록 aaa 를 200 으로 일치시킵니다. 로컬 우선 순위를 250 으로 구성합니다. 경로가 거부되면 다른 경로가 거부됩니다.

```
router bgp 100
!
        neighbor 140.222.1.1 route-map fix-weight in
        neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight permit 10
        match as-path aaa
        set local-preference 250
        set weight 200
!
ip as-path access-list aaa permit ^690$
ip as-path access-list aaa permit ^1800
```

다음 예에서 경로 맵 freddy 의 첫 번째 항목은 자치 시스템 690 에서 시작하는 모든 경로의 MED 속성을 127 로 구성합니다. 두 번째 항목은 이전 조건을 만족하지 않는 경로를 인접 라우터 1.1.1.1 로 전송합니다.

```
router bgp 100
        neighbor 1.1.1.1 route-map freddy out
!
ip as-path access-list abc permit ^690_
ip as-path access-list xyz permit .*
!
route-map freddy permit 10
        match as-path abc
        set metric 127
!
route-map freddy permit 20
match as-path xyz
```

다음은 route-map 을 통해 전달해서 생성 된 경로를 수정하는 방법을 보여줍니다.

```
router bgp 100
        redistribute rip route-map rip2bgp
!
        route-map rip2bgp
        match ip address rip
        set local-preference 25
        set metric 127
```

```
        set weight 30000
        set next-hop 192.92.68.24
        set origin igp
!
ip access-list standard rip
        permit 131.108.0.0 255.255.0.0
        permit 160.89.0.0 255.255.0.0
        permit 198.112.0.0 255.255.128.0
```

BGP neighbor 구성 예

다음 예에서 BGP 라우터는 AS109 에 속합니다. AS109 는 두 개의 네트워크를 구축합니다. 라우터에는 외부 이웃 (다른 AS 에 있음), 내부 이웃 (동일한 AS 번호로) 및 외부 이웃 등 3 개의 이웃이 있습니다.

```
router bgp 109
        network 131.108.0.0
        network 192.31.7.0
        neighbor 131.108.200.1 remote-as 167
        neighbor 131.108.234.2 remote-as 109
        neighbor 150.136.64.19 remote-as 99
```

neighbor-기반 BGP 경로필터의 예

다음은 neighbor 기반 BGP 경로 필터링의 예입니다. as-path 의 액세스 목록 test1 을 통과하는 라우트는 가중치 100 을 얻습니다. as-path 의 액세스 목록 test2 를 통해 도달하는 라우트만 이웃 193.1.12.10 으로 전송 될 수 있습니다.
마찬가지로 액세스 목록 test3 을 통과하는 경로는 이웃 라우터 193.1.12.10 에서 허용 할 수 있습니다.

```
router bgp 200
        neighbor 193.1.12.10 remote-as 100
        neighbor 193.1.12.10 filter-list test2 out
        neighbor 193.1.12.10 filter-list test3 in
ip as-path access-list test1 permit _109_
ip as-path access-list test2 permit _200$
ip as-path access-list test2 permit ^100$
ip as-path access-list test3 deny _690$
ip as-path access-list test3 permit .*
```

포 트 -based BGP 의 route 필터 예

다음 예에서는 포트 e1 / 0 의 경로가 액세스를 통해 필터링 됨을 보여줍니다.

```
router bgp 122
        filter vlan10 in access-list acl
```

다음 예에서는 액세스 목록 filter-network 및 액세스 목록 filter-gateway 를 사용하여 포트 번호 e1 / 0 에서 경로를 동시에 필터링하여 네트워크 번호와 게이트웨이 주소를 각각 필터링하는 방법을 보여줍니다.

```
router bgp 100
        filter vlan100 in access-list filter-network gateway filter-gateway
```

다음 예는 prefix list filter-prefix 와 prefix list filter-gateway 를 사용하여 네트워크 번호와 게이트웨이 주소를 각각 필터링하여 포트에서 동시에 경로를 필터링하는 방법을 보여줍니다.

```
router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway
```

prefix-list 기반 경로 필터 구성 예

다음 예는 기본 경로 0.0.0.0 /0 가 거부되었음을 보여 줍니다.

```
ip prefix-list abc deny 0.0.0.0/0
```

다음 예는 prefix- 35.0.0.0/8 과 일치하는 경로가 허용됨을 보여줍니다.

```
ip prefix-list abc permit 35.0.0.0/8
```

다음 예제에서는 / 8 에서 / 24 사이의 길이를 가진 prefix 만 BGP 프로세스에서 허용됩니다.

```
router bgp
        network 101.20.20.0
        filter * in prefix max24
!
        ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

다음 예에서 라우터는 모든 경로를 필터링하고 prefix 길이가 8~ 24 사이 인 경로 만 허용합니다.

```
router bgp 12
        filter * in prefix-list max24
 !
```

ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24

다음 예는 prefix 길이가 24 이하인 경로가 망 192/8 에서 허용됨을 보여줍니다.

ip prefix-list abc permit 192.0.0.0/8 le 24

다음 예는 prefix 길이가 25 를 초과하는 경로가 망 192/8 에서 허용됨을 보여줍니다.

ip prefix-list abc deny 192.0.0.0/8 ge 25

다음 예는 prefix 길이가 8 보다 크고 24 보다 작은 경로가 허용됨을 보여줍니다.

ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24

다음 예는 접두사 길이가 25 를 초과하는 경로가 거부되었음을 보여줍니다.

ip prefix-list abc deny 0.0.0.0/0 ge 25

다음 예는 네트워크 10/8 의 모든 경로가 거부되었음을 보여줍니다.
A 클래스 네트워크 10.0.0.0/8 의 마스크가 32 비트보다 작거나 같으면
모든 경로가 거부됩니다.

ip prefix-list abc deny 10.0.0.0/8 le 32

다음 예에서는 네트워크 204.70.1 / 24 의 마스크 길이가 25 를 초과하므로 모든 경로가 거부되었음을 보여줍니다.

ip prefix-list abc deny 204.70.1.0/24 ge 25

다음 예는 모든 경로가 허용됨을 보여줍니다.:

ip prefix-list abc permit any

BGP 집합 경로 예

다음 예는 경로 전달 또는 조건부 경로 집계 기능을 통해 BGP 에서 집계 경로를 생성하는 방법을 보여줍니다.

다음 예는 명령어 **redistribute static 는 통합경로** 193. * . * . * 으로 전송하는데 사용됩니다.

```
ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
        redistribute static
```

라우팅 테이블의 하나 이상의 경로가 지정된 범위에 속하면 다음 구성에 따라 BGP 라우팅 테이블에 집계 경로가 만들어집니다. 집계 경로는 사용자 AS 의 것으로 간주되며 표시 정보에서 손실 될 수 있는 atomic 속성을 가집니다.

```
router bgp 100
aggregate 193.0.0.0/8
```

다음 예는 집계 경로 193. *. *. *을 만드는 방법과 Broadcast 에서 모든 Neighbor 라우터에 대한 자세한 경로를 제한하는 방법을 보여줍니다.

```
router bgp 100
aggregate 193.0.0.0/8 summary-only
```

BGP 경로 reflector 구성 예

다음은 경로 reflector 구성의 예입니다. RTA, RTB, RTC 및 RTE 는 동일한 자치 시스템 AS 200 에 속합니다. RTA 는 경로 reflector 역할을 하지만 RTB 및 RTC 는 경로 reflector 기능을 담당합니다. RTE 는 일반적인 IBGP 이웃입니다. RTD 는 AS100 에 속하며 RTA 와의 EBGP 연결을 구성합니다. 구성은 다음과 같습니다.

RTA 구성:

```
interface vlan110
ip address 2.0.0.1 255.0.0.0
!
interface vlan111
ip address 3.0.0.1 255.0.0.0
!
interface vlan112
ip address 4.0.0.1 255.0.0.0
!
interface vlan113
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200    /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200    /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200    /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100    /*RTD EBGP*/
network 11.0.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

RTB 구성 :

```
interface vlan110
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200    /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

RTC 구성 :

```
interface vlan110
 ip address 2.0.0.2 255.0.0.0
 !
 router bgp 200
 neighbor 2.0.0.1 remote-as 200    /*RTA IBGP*/
 network 12.0.0.0/8
 !
 ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

RTD 구성:

```
interface vlan110
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200    /*RTA EBGP*/
network 14.0.0.0/8
 !
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

RTE 구성:

```
interface vlan110
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200    /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12
```

BGP 자율 결합 시스템의 예

다음 그림은 자치 결합 시스템 구성을 보여줍니다. RTA, RTB 및 RTC 는 IBGP 연결을 만듭니다. RTA, RTB 및 RTC 는 사설 자치 시스템 65010 에 속합니다. RTE 는 사설 자치 시스템 65020 에 속합니다. RTE 및 RTA 는 자치 결합 시스템 에서 EBGP 연결을 구성합니다.
AS65010 및 AS65020 은 자치 결합 시스템을 구성합니다. 자치 결합 시스템 의 번호는 AS 200 입니다. RTD 는 AS100 에 속합니다. RTA 를 통해 RTD 와 AS200
간에 EBGP 연결이 구성됩니다.

RTA 구성:

```
interface vlan110
ip address 1.0.0.1 255.0.0.0
!
interface vlan111
ip address 2.0.0.1 255.0.0.0
!
interface vlan112
ip address 4.0.0.1 255.0.0.0
!
interface vlan113
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010   /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010   /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020   /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100     /*RTD EBGP*/
```

RTB 구성:

```
interface vlan110
ip address 1.0.0.2 255.0.0.0
!
interface vlan111
ip address 3.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.1 remote-as 65010   /*RTA IBGP*/
neighbor 3.0.0.2 remote-as 65010   /*RTC IBGP*/
```

RTC 구성:

```
interface vlan110
ip address 2.0.0.2 255.0.0.0
!
interface vlan111
ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 2.0.0.1 remote-as 65010   /*RTA IBGP*/
neighbor 3.0.0.1 remote-as 65010   /*RTB IBGP*/
```

RTD 구성:

```
interface vlan110
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200   /*RTA EBGP*/
```

RTE 구성:

```
interface vlan110
```

```
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010   /*RTA EBGP*/
```

9. route-map BGP community 특성의 예

다음의 예는 명령어 **route map set-community** 을 neighbor 의 나가는 경로 171.69.232.50 를 업데이트하는데 사용됩니다. 특정 커뮤니티 속성 값 no-export 는액세스 목록 aaa 의 경로를 통해 구성할 수 있습니다. 다른 경로는 정상적인 Broadcast 를 수행합니다.
특정커뮤니티 속성 값은 AS200 의 BGP 세션 스폰서가 자동으로 자율 시스템 외부로 경로를 Broadcasting 하는 것을 방지합니다.

```
router bgp 100
        neighbor 171.69.232.50 remote-as 200
        neighbor 171.69.232.50 send-community
        neighbor 171.69.232.50 route-map set-community out
!
        route-map set-community 10 permit
        match ip address aaa
        set community no-export
        !
        route-map set-community 20 permit
```

다음 예에서 route map set-community 명령어는 neighbor 171.69.232.90 의 출력 경로를 업데이트하는 데 사용됩니다. 현재 값을 커뮤니티 속성 값 200 으로 구성하십시오. 다른 경로는 정상 Broadcasting 를 수행합니다.

```
route-map bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
 match as-path test1
```

```
 set community-additive 200 200
!
route-map set-community 20 permit
 match as-path test2
!
ip aspath-list test1 permit 70$
ip aspath-list test2 permit .*
```

다음 예는 경로의 MED 및 로컬 우선 순위를 인접 라우터에서 구성합니다.

커뮤니티 속성 값에 따라 171.69.232.55. 커뮤니티 목록 com1 과 일치하는 모든 경로의 MED 를 8000 으로 구성합니다. 이 경로에는 커뮤니티 값이 "100 200 300"및 "900 901"인
경로가 포함될 수 있습니다. 이러한 경로에는 다른 속성 값이 있을 수 있습니다.

커뮤니티 목록 com2 를 보내는 경로의 로컬 우선 순위를 500 으로 구성합니다.

다른 경로의 로컬 우선 순위를 50 으로 구성하십시오. 따라서 이웃 171.69.232.55 의 나머지 모든 경로의 모든 로컬 우선 순위 값은 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
!
```

하드웨어 IP Subnet 경로

개요

하드웨어 IP Subnet 경로는 IP 의 빠른 교환과 유사합니다. 하드웨어 IP Subnet 경로가 활성화되지 않은 경우 IP 주소가 포함 된 전달 메시지 앞에 표시됩니다. 항목이 있으면 메시지가 하드웨어를 통해 전달됩니다. 해당 항목이 없으면 메시지가 CPU 로 전송 된 다음 소프트웨어를 통해 처리됩니다.
하드웨어 IP Subnet 경로 항목에는 대상 Subnet, 마스크, 다음 홉의 IP 주소, 인터페이스 등이 포함됩니다. 하드웨어 IP Subnet 경로가 활성화되면 IP 캐시가 실패한 후 시스템은 하드웨어 IP Subnet 경로 항목을 확인합니다. 일치 항목이 발견되면 메시지는 다음 홉 IP 주소와 일치 항목에 지정된 인터페이스를 통해 직접 전달됩니다. 하드웨어 IP Subnet 경로 항목이 없으면 처리를 위해 메시지가 CPU 로 전송됩니다.
하드웨어 IP Subnet 경로에는 자동 및 수동의 두 가지가 있습니다. 수동 모드에서는 하드웨어 IP Subnet 경로를 수동으로 구성합니다. 목적지 서브넷의 더 긴 마스크가 있는 라우팅 항목은 먼저 구성되어야 합니다. 자동 모드에서 시스템은 알려진 경로를 하드웨어 Subnet 경로에 자동으로 추가합니다. 하드웨어 Subnet 경로가 시작되면 모든 절차가 자동으로 수행됩니다.

하드웨어 IP Subnet 경로 구성하기

하드웨어 IP Subnet 경로 구성하려면 다음 단계를 수행하십시오.

단계	명령어	설명
1	[**no**] **ip exf**	하드웨어 IP 서브넷 라우팅을 활성화 또는 비활성화합니다.
2	[**no**] **ip exf down-up-threshold** *<Number>*	최대칩번호의 <Number>값의 미만일 때 exf 기능을 활성화합니다.
3	[**no**] **ip exf exclude-slot** *<SlotID>*	exf 기능의 SlotID 을 포함합니다.

하드웨어 IP Subnet 경로 구성의 상태 확인하기

명령어	설명
show ip route	현재 경로 구성상태를 보여줍니다.

IP-PBR 구성

IP-PBR 구성

IP-PBR 은 스위치 칩의 하드웨어를 통해 소프트웨어 PBR 기능을 구현합니다.

PBR 은 정책 기반 라우팅을 나타냅니다. PBR 을 사용하면 사용자는 라우팅을위한 라우팅 프로토콜이 아닌 특정 정책에 의존 할 수 있습니다. 소프트웨어 기반 PBR 은 다중 정책 및 규칙을 지원하고로드 밸런스를 지원합니다. 정책에 맞는 패킷에 대해 다음 홉의 IP 주소 또는 포트를 지정할 수 있습니다. PBR 은로드 밸런스를 지원하고 정책 지원 패킷에 여러 개의 다음 홉 IP 주소 또는 포트를 적용합니다..

경로 맵에 의해 지정된 다음 홉 출구 ARP 가 이미 학습 된 경우에만 IP-PBR 은이 출구가 유효하고 해당 규칙이 유효하다고 간주 할 수 있습니다. 패킷이 IP-PBR 정책을 만족하면 하드웨어는이 패킷을 규칙이 지정하는 다음 홉 (NAP) 홉으로 직접 전달합니다. 이 프로세스는 CPU 가 작동하지 않는 하드웨어에 의해 완료됩니다. IP-PBR 에 의해 포워딩 된 패킷은 가장 높은 우선 순위를 가지며 IP-PBR 규칙과 일치하지 않는 패킷들만이 CPU 로 포워딩됩니다.

현재 IP-PBR 은 IP ACL 정책과 다음 홉 IP 주소 정책을 지원합니다. 여러 개의 다음 홉이 구성되면 첫 번째 효과 다음 홉이 선택됩니다. IP-PBR 은 또한 스위치 칩에 의해 실현되는 등가 라우팅을 지원합니다. 하드웨어 동등 라우팅에는 추가 구성이 필요하지 않습니다..

IP-PBR 은 다음 정책 라우팅 명령을 지원합니다.:

- **route-map** *WORD*
- **match ip address** *WORD*
- **set ip next-hop** *X.X.X.X* [**load-balance**]

IP-PBR 은 라우터의 정책 라우팅과 조금 다릅니다. IP-PBR 은 유효한 다음 홉을 출구로 선택하고 유효한 다음 홉이 없으면 패킷을 버리고 라우터의 정책 라우팅은 효과적인 다음 홉을 선택하지만 패킷 손실은 다음 홉이 ARP 를 알지 못하면 발생합니다. 여러 시퀀스가 구성되면 IP-PBR 과 소프트웨어 정책 라우팅의 차이점 하나를 기록해야합니다. 소프트웨어 정책 라우팅은 우선 순위가 높은 시퀀스와 일치하는 IP 주소가 우선 순위가 낮은 시퀀스와 겹치는 지 여부와 이러한 라우팅이 유효한 지 여부와 관계없이 항상 높은 우선 순위 시퀀스 경로를 선택합니다. 반면 IP-PBR 은 높은 우선 순위 시퀀스 경로를 선택합니다. 우선 순위 순서 경로가 무효화됩니다.

IP-PBR 활성화/비활성화

Global 구성 모드에서 다음 명령을 실행하십시오..

명령어	설명
ip pbr	IP-PBR 기능활성화합니다. (기본적으로 비활성화 입니다)
no ip pbr	IP-PBR 비활성화합니다.

IP-PBR 은 기본적으로 비활성화 상태입니다..

구성 작업 목록

IP-PBR 을 구성하려면 다음을 수행하십시오.:

ACL 생성;

route map 생성;

port 에 route map 적용

ACL 을 만들려면 다음 명령을 실행하십시오.:

명령어	설명
ip access-list standard *net1*	ACL 구성 모드를 시작하고 ACL을 정의합니다..

route-map 을 만들려면 다음 명령을 실행하십시오..

명령어	설명
route-map *pbr*	route-map 구성 모드를 시작합니다.
match ip address *access-list*|prefix-list	Match-up 정책 구성.
set ip next-hop *A.B.C.D*	IP 패킷의 다음 홉 주소를 구성합니다..

IP 수신 포트에서 정책 라우팅을 적용하려면 다음 명령을 실행하십시오.:

명령어	설명
interface *interfacevlan_name*	인터페이스 구성 모드로 들어갑니다..
ip policy route-map *route-map_name*	포트에서 정책 라우팅을 적용합니다..

MVC 모니터링 및 유지 보수

EXEC 모드에서 다음 명령을 실행하십시오.:

명령어	설명
show ip pbr	RIP 구성에 대한 정보를 표시하는 데 사용됩니다..
show ip policy	IP-PBR이 적용되는 포트를 보여줍니다..
show ip pbr policy	IP-PBR 등가 라우팅에 대한 정보를 표시하는 데 사용됩니다..
debug ip pbr	IP-PBR의 디버깅 스위치를 활성화 또는 비활성화하는 데 사용됩니다..

IP-PBR 이 실행되지 않는 정보가 표시됩니다.

```
switch#show ip pbr

IP policy based route state: disabled

No pbr apply item
```

```
No equiv exf apply item
```

IP-PBR 실행과 관련된 모든 데이터는 다음과 같습니다:

```
switch#show ip pbr
IP policy based route state: enabled

No equiv exf apply item

VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
    90.0.0.3
```

IP-PBR 정책 라우팅 정보는 아래와 같습니다:

```
switch#show ip pbr policy
IP policy based route state: enabled

VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
    90.0.0.3
```

동일한 라우팅 정보가 아래에 나와 있습니다.:

```
switch#show ip pbr exf
IP policy based route state: enabled

Equiv EXF has 1 entry active.
------------------
Entry sequence 1, handle c1f95b0
  Dest ip: 1.1.0.0/16
    90.0.0.3
    192.168.213.161
```

IP-PBR 구성 예제

스위치 구성:

```
ip pbr
interface vlan1
ip address 10.1.1.3 255.255.255.0
ip policy route-map pbr
!
ip access-list standard ac1
permit 10.1.1.21 255.255.255.255
!
ip access-list standard ac2
permit 10.1.1.2 255.255.255.255
!
route-map pbr 10 permit
match ip address ac1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address ac2
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
```

구성 설명

스위치는 VLAN1 에서 수신 한 패킷에 대해 정책 라우팅을 적용합니다. 소스 IP 가 10.1.1.21 이고 다음 홉이 13.1.1.99 인 패킷에 대해 소스 IP 가 10.1.1.2 인 패킷에 대해 노선지도 pbr 20 에 적용; set ip next-hop 에는 load-balance 매개 변수가 있기 때문에 스위치 칩은 목적지 IP 주소에 따라 자동으로 13.1.1.99 또는 14.1.1.99 를 출구로 선택합니다..

Multi-VRF CE 개요

개요

가상 사설망 (VPN)은 여러 클라이언트 네트워크가 ISP 에서 제공하는 대역폭을 공유 할 수있는 안전한 방법을 제공합니다. 일반적으로 하나의 VPN 은 ISP 의 라우터에서 공용 라우팅 테이블을 공유하는 클라이언트 네트워크 팀으로 구성됩니다. 각 클라이언트 네트워크는 ISP 의 네트워크 장치 인터페이스에 연결되며 ISP 장치는 각 인터페이스를 VPN 라우팅 테이블과 연결합니다. 하나의 VPN 라우팅 테이블은 VRF (VPN 라우팅 / 전달 테이블)입니다.
VRF 는 일반적으로 MPLS VRF VPN 과 같은 PE (Provider Edge) 장치에 배포됩니다. PE 는 여러 VPN 을 지원하며 각 VPN 에는 IP 주소가 겹칠 수있는 독립적 인 IP 주소 공간이 있습니다. 다른 클라이언트의 VPN 은 PE 의 다른 인터페이스를 연결하는 반면 PE 는 패킷의 수신 포트에 따라 검사 할 라우팅 테이블을 구분합니다.
다중 VRF CE 는 여러 클라이언트 네트워크를 PE 에서 CE 로 연결하는 작업을 제거하는 것으로, CE 및 PE 를 연결하는 데 물리적 링크 만 있으면됩니다. 이 방법으로 PE 의 포트 리소스가 저장됩니다. 또한 CE 는 각 VPN 에 대한 VRF 라우팅 테이블을 유지 관리합니다. 클라이언트 네트워크의 패킷은 먼저 CE 에서 전달 된 다음 패킷이 ISP 네트워크를 통과 한 후 PE 로 전송됩니다.
MCE 역할을하는 스위치는 다른 포트를 통해 다른 클라이언트 네트워크를 연결 한 다음이 포트를 VPN 라우팅 테이블과 연결합니다. (당사 장비는 VLAN 포트의 VRF 구성 만 지원합니다).
MCE 기능은 대개 대규모 MPLS-VRF VPN 네트워크의 에지에 배치됩니다. Multi-VRF CE, MPLS 레이블 스위칭 및 MPLS 제어 계층의 기능의 세 가지 기능은 독립적입니다. 그림 1.1 은 MPLS-VRF VPN 네트워크를 보여줍니다.

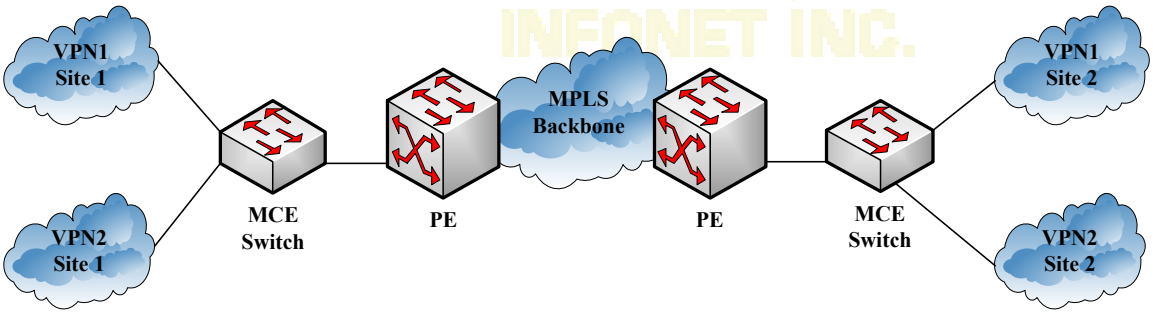


그림 1.1 MPLS-VRF VPN 네트워크의 MCE Switch

CE 와의 경로 구성

Multi-VRF CE 스위치는 여러 동적 라우팅 프로토콜을 통해 CE 와의 경로를 구성할 수 있습니다. CE 는 라우터 또는 이더넷 스위치가 될 수 있습니다. 지원되는 라우팅 프로토콜에는 OSPF, RIP 및 BEIGRP 가 포함됩니다. MCE 스위치는 정적 라우팅 구성도 지원합니다.

일반적으로 MCE 스위치는 다른 VPN 에 속한 CE 를 연결하기 위해 서로 다른 VLAN 포트가 필요합니다. VPN 을 연결하는 데 사용되는 VLAN 포트는 VRF 와 관련이 있어야합니다. CE 는 VRF 를 지원할 필요가 없습니다.

PE 와의 경로 구성

MCE 스위치 (MCE)는 하나 이상의 PE 를 연결할 수 있지만 MCE 와 연결된 PE 는 모두 VRF 를 구성해야합니다. MCE 는 CE 로부터 MCE 가 배운 경로를 PE 에 제공하고 PE 로부터 원격 클라이언트 네트워크의 경로를 학습합니다.
BGP, OSPF, RIP 및 BEIGRP 와 같은 동적 라우팅 프로토콜을 통해 MCE 와 PE 간에 VRF 라우트를 구성할 수 있습니다. 물론 VRF 경로는 정적으로 구성 될 수도 있습니다.
일반적으로 MCE 와 PE 는 서로 다른 자율 시스템에 속합니다. 따라서 EBGP 를 사용하여 MCE 와 PE 간에 VRF 라우트를 구성하는 방법이이 문서의 핵심입니다.

Multi-VRF CE 구성

기본 VRF 구성

기능	**기본 구성**
VRF	VRF는 기본적으로 비활성화 상태입니다. 모든 경로가 기본 라우팅 테이블에 추가됩니다.
VRF의 VPN 확장 성	Route-distinguisher기본 비활성화. (RD). 입력 / 출력 라우팅 대상이 없습니다. (RT).
최대 VRF 경로 수	10240
VRF port	N/A. VRF와 관련된 VLAN 포트는 없으며 포트 경로는 기본 라우팅 테이블에 추가됩니다.
IP Express Forwarding	하드웨어 IP 라우팅은 활성화 되어있지 않습니다.

MCE 구성 작업

- VRF 구성
- VPN 경로 구성
- PE 와 CE 사이의 BGP 경로 구성하기
- PE 와 CE 간의 VRF 연결 확인

MCE 구성

VRF 구성

하나 또는 다수의 VRF 를 구성하려면 다음 단계를 참조하십시오.

명령어	설명
Switch# **config**	스위치 구성 모드로 들어갑니다.
Switch_config# **ip vrf** *vrf-name*	VRF를 생성하고 VRF 구성 모드로 들어갑니다.. vrf-name: 최대 31 자의 VRF 이름
Switch_config_vrf# **rd** *route-distinguisher*	route-dstinguisher를 구성합니다. route-distinguisher: 경로 구별자를 의미합니다. 자율 도메인 ID와 nn 또는 IP와 nn로 구성됩니다..
Switch_config_vrf# **route-target** **{ export | import | both }** *route-target-extened-community*	입 / 출력 VRF 객체의 확장 된 VPN 속성을 만듭니다. route-target-extended-community: 자율 도메인 ID와 난수 또는 IP와 난수로 구성됩니다.
Switch_config_vrf# **interface** *intf-name*	인터페이스 구성 모드로 들어갑니다. intf-name: 인터페이스의 이름을 의미합니다.
Switch_config_intf# **ip vrf forwarding** *vrf-name*	VRF와 L3 인터페이스를 연결합니다. vfi-name: VRF의 이름을 의미합니다.
Switch_config_intf# **exit**	인터페이스 구성 모드를 종료합니다.
Switch_config# **ip exf**	ip 하드웨어 라우팅 사용.
Switch_config# **show ip vrf** **[brief | detail | interface] [** *vrf-name* **]**	VRF 정보를 확인합니다.
Switch_config#**no ip vrf** *vrf-name*	구성된 VRF 및 VRF와 L3 인터페이스 간의 관계를 삭제합니다. vfi-name: VRF의 이름을 의미합니다.
Switch_config_intf# **no ip vrf forwarding** **[** *vrf-name* **]**	L3 인터페이스와 VRF 간의 관계를 삭제합니다.

VPN 경로 구성

경로는 BGP, OSPF, RIP, BEIGRP 또는 고정 경로의 구성을 통해 MCE 와 고객 장치간에 구성 될 수 있습니다. 다음은 다른 경로 구성과 유사한 OSPF 구성을 예로 들어 설명합니다.

Note:
클라이언트 네트워크에 연결하기 위해 MCE 에 라우트가 구성되면 라우팅 프로토콜의 VRF 속성을 지정해야합니다. VRF 는 고객 장치에 구성 할 필요가 없습니다.

명령어	**설명**
Switch# **config**	스위치 구성 모드로 들어갑니다..
Switch_config# **router ospf** *process-id* **vrf** *vrf-name*	OSPF-VRF 경로를 시작하고 구성 모드로 들어갑니다.
Switch_config_ospf# **network** *network-number network-mask* **area** *area-id*	OSPF 네트워크, 마스크 및 영역 ID를 정의합니다.
Switch_config_ospf# **redistribute bgp** *ASN*	지정된 BGP 네트워크를 OSPF 네트워크로 전달합니다.
Switch_config_ospf# **exit**	OSPF 구성 모드를 종료합니다.
Switch_config# **show ip ospf**	OSPF 프로토콜에 대한 정보를 탐색합니다.
Switch_config# **no router ospf** *process-id*	OSPF-VRF 라우팅 구성을 삭제합니다.

VPN 경로 구성 PE 와 CE 사이의 BGP 경로 구성

다음 구성 명령을 참조하십시오.:

명령어	**설명**
Switch# **config**	스위치 구성 모드로 들어갑니다.
Switch_config# **router bgp** *autonomous-system-number*	자율 시스템 번호를 지정하여 BGP 프로토콜을 시작하고 BGP 구성 모드 진입.
Switch_config_bgp# **bgp log-neighbor-changes**	BGP 이웃 변경에 대한 기록을 시작합니다.
Switch_config_bgp# **address-family ipv4 vrf** *vrf-name*	VRF address-family의 구성 모드로 들어갑니다.
Switch_config_bgp_af# **redistribute ospf** *ospf-process-id*	OSPF 라우팅 정보를 BGP 네트워크로 전달.
Switch_config_bgp_af# **network** *network-number/prefix-length*	BGP에 의해 배포되는 네트워크 번호와 마스크 길이를 구성합니다..
Switch_config_bgp_af# **neighbor** *address* **remote-as** *ASN*	neighbor 의 BGP neighbor 와 AS번호를 구성합니다..

Switch_config_bgp_af# **exit-address-family**	address-family의 구성 모드 종료.
Switch_config_bgp# **exit**	BGP 구성 모드를 종료합니다.
Switch_config# **show ip bgp vpnv4** **[all | rd | vrf]**	BGP-VRF 라우팅 정보를 확인합니다.
Switch_config# **no router bgp** *ASN*	BGP 라우팅 구성을 삭제합니다.

PE 와 CE 간의 VRF 연결 확인

PE 및 CE 의 VRF 연결을 확인하려면 VRF 옵션과 함께 PING 명령을 사용하십시오.

명령어	**설명**
Switch# **ping –vrf** *vrf-name ip-address*	VRF의 주소로 PING 작업을 수행합니다.

MCE 구성 예제

그림 2.1 은 간단한 VRF 네트워크를 보여줍니다. S1 과 S2 는 모두 Multi-VRF CE 스위치입니다. S11, S12 및 S13 은 VPN1 에 속하며, S21 및 S22 는 VPN2 에 속하며 모두가 고객 장치입니다. OSPF 경로는 CE 와 고객 장치간에 구성되어야하며 BGP 경로는 CE 와 PE 사이에 구성되어야합니다.

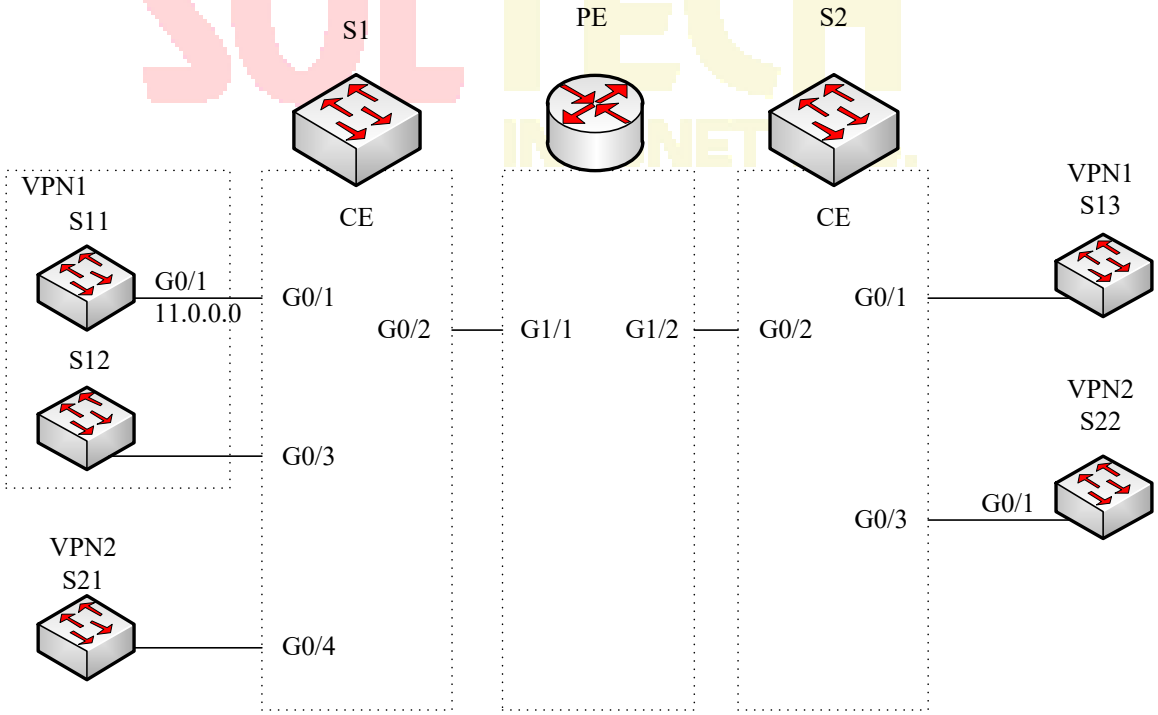


그림 2.1 MCE 구성 예제

S11 구성

CE 를 연결하는 물리적 인터페이스의 VLAN 속성 구성:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

IP 주소 및 VLAN 인터페이스를 구성합니다.

Switch_config# interface VLAN11

Switch_config_v11# ip address 11.0.0.2 255.0.0.0

Switch_config_v11# exit

CE 와 고객 장치 사이의 라우팅 프로토콜 구성:

Switch_config# router ospf 101

Switch_config_ospf_101# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_101# exit

MCE-S1 구성

Multiple-VRF CE 장치에서 VRF 를 구성합니다..

Switch#config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 100:1

Switch_config_vrf_vpn1# route-target export 100:1

Switch_config_vrf_vpn1# route-target import 100:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 100:2

Switch_config_vrf_vpn2# route-target export 100:2

Switch_config_vrf_vpn2# route-target import 100:2

Switch_config_vrf_vpn2# exit

루프백 포트와 물리적 포트를 구성하고 루프백 포트의 주소를 BGP 프로토콜의 라우터 ID 로 사용하십시오.

Switch_config# interface loopback 0

Switch_config_l0# ip address 101.0.0.1 255.255.255.255

Switch_config_l0# exit

S1 은 S11 을 F0 / 1 포트를 통해, S21 을 G0 / 4 포트를 통해, PE 를 G0 / 2 포트를 통해 연결합니다.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/4

Switch_config_g0/4# switchport pvid 15

Switch_config_g0/4# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

스위치의 L3 VLAN 포트를 구성하고 VRF 를 VLAN 포트에 바인딩하고 IP 주소를 구성합니다. S1 은 두 개의 논리적 포트 인 VLAN21 과 VLAN22 를 통해 PE 를 연결합니다. VLAN11 과 VLAN15 의 두 포트는 각각 VPN1 과 VPN2 를 연결합니다.

Switch_config# interface VLAN11

Switch_config_v11# ip vrf forwarding vpn1

Switch_config_v11# ip address 11.0.0.1 255.0.0.0

Switch_config_v11# exit

Switch_config# interface VLAN15

Switch_config_v15# ip vrf forwarding vpn2

Switch_config_v15# ip address 15.0.0.1 255.0.0.0

Switch_config_v15# exit

Switch_config# interface VLAN21

Switch_config_v21# ip vrf forwarding vpn1

Switch_config_v21# ip address 21.0.0.2 255.0.0.0

Switch_config_v21# exit

Switch_config# interface VLAN22

Switch_config_v22# ip vrf forwarding vpn2

Switch_config_v22# ip address 22.0.0.2 255.0.0.0

Switch_config_v22# exit

CE 와 고객 장치 사이의 OSPF 경로 구성.

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 100

Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 15.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 100

Switch_config_ospf_2#exit

PE 와 CE 사이의 EBGP 경로 구성.

Switch_config# router bgp 100

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 21.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 22.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

VLAN 생성.

Switch_config# vlan 1,11-12,21-22

스위치의 서브넷 경로 전달을 활성화합니다.

Switch_config# ip exf

PE 구성

VRF on PE 구성:

```
Switch#config
Switch_config# ip vrf vpn1
Switch_config_vrf_vpn1# rd 200:1
Switch_config_vrf_vpn1# route-target export 200:1
Switch_config_vrf_vpn1# route-target import 200:1
Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2
Switch_config_vrf_vpn2# rd 200:2
Switch_config_vrf_vpn2# route-target export 200:2
Switch_config_vrf_vpn2# route-target import 200:2
Switch_config_vrf_vpn2# exit
```

루프백 인터페이스를 라우터 식별자로 구성하십시오:

```
Switch_config# interface loopback 0
Switch_config_l0# ip address 102.0.0.1 255.255.255.255
Switch_config_l0# exit
```

PE 와 CE 를 연결하는 물리적 인터페이스 구성 : G1 / 1 과 G1 / 2 는 각각 S1 과 S2 를 연결합니다:

```
Switch_config# interface gigaEthernet 1/1
Switch_config_g1/1# switchport mode trunk
Switch_config_g1/1# interface gigaEthernet 1/2
Switch_config_g1/2# switchport mode trunk
Switch_config_g1/2# exit
```

S1 을 연결하는 PE 의 L3 VLAN 인터페이스를 구성합니다:

```
Switch_config# interface VLAN21
Switch_config_v21# ip vrf forwarding vpn1
Switch_config_v21# ip address 21.0.0.1 255.0.0.0
Switch_config_v21# exit

Switch_config# interface VLAN22
Switch_config_v22# ip vrf forwarding vpn2
Switch_config_v22# ip address 22.0.0.1 255.0.0.0
```

Switch_config_v22# exit

S2 를 연결하는 PE 의 L3 VLAN 인터페이스를 구성합니다:

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.1 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.1 255.0.0.0

Switch_config_v32# exit

EBGP of PE 구성:

Switch_config# router bgp 200

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# neighbor 21.0.0.2 remote-as 100

Switch_config_bgp_vpn1# neighbor 31.0.0.2 remote-as 300

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# neighbor 22.0.0.2 remote-as 100

Switch_config_bgp_vpn2# neighbor 32.0.0.2 remote-as 300

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

VLAN 을 구성하고 서브넷 라우팅 전달을 활성화합니다.

Switch_config# vlan 1,21-22,31-32

Switch_config# ip exf

MCE-S2 구성

VRF 구성:

Switch#config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 300:1

Switch_config_vrf_vpn1# route-target export 300:1

Switch_config_vrf_vpn1# route-target import 300:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 300:2

Switch_config_vrf_vpn2# route-target export 300:2

Switch_config_vrf_vpn2# route-target import 300:2

Switch_config_vrf_vpn2# exit

루프백 포트와 물리적 포트를 구성하고 루프백 포트의 주소를 BGP 프로토콜의 라우터 ID 로 사용하십시오.

Switch_config# interface loopback 0

Switch_config_l0# ip address 103.0.0.1 255.255.255.255

Switch_config_l0# exit

S2 는 F0 / 1 포트를 통해 S13 을 연결하고 G0 / 3 포트를 통해 S22 를 연결하고 G0 / 2 포트를 통해 PE 를 연결합니다.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 41

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# switchport pvid 46

Switch_config_g0/3# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

스위치의 L3 VLAN 포트를 구성하고 VRF 를 VLAN 포트에 바인딩하고 IP 주소를 구성합니다. S2 는 두 개의 논리 포트 인 VLAN31 과 VLAN32 를 통해 PE 를 연결합니다. 두 개의 포트 인 VLAN41 과 VLAN46 은 각각 VPN1 과 VPN2 를 연결합니다.

Switch_config# interface VLAN41

Switch_config_v41# ip vrf forwarding vpn1

Switch_config_v41# ip address 41.0.0.1 255.0.0.0

Switch_config_v41# exit

Switch_config# interface VLAN46

Switch_config_v46# ip vrf forwarding vpn2

Switch_config_v46# ip address 46.0.0.1 255.0.0.0

Switch_config_v46# exit

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.2 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.2 255.0.0.0

Switch_config_v32# exit

CE 와 고객 장치 사이의 OSPF 경로 구성.

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 41.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 300

Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 300

Switch_config_ospf_2# exit

PE 와 CE 사이의 EBGP 경로 구성.

Switch_config# router bgp 300

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 31.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 32.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

VLAN 생성.

Switch_config# vlan 1,31-32,41,46

스위치의 서브넷 경로 전달을 활성화합니다.

Switch_config# ip exf

S22 구성

CE 의 물리적 인터페이스의 VLAN 속성을 구성하고 인터페이스 g0/1 을 통해 S22 와 S2 를 연결하십시오:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 46

Switch_config_g0/1# exit

IP 주소 및 VLAN 인터페이스를 구성합니다.

Switch_config# interface VLAN46

Switch_config_v46# ip address 46.0.0.2 255.0.0.0

Switch_config_v46# exit

CE 와 고객 장치 사이의 라우팅 프로토콜 구성:

Switch_config# router ospf 103

Switch_config_ospf_103# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_103# exit

VRF 연결 테스트

S1 에서 PING 명령을 실행하여 S1 과 S11 사이의 VPN1 연결을 확인하십시오.:

Switch# ping -vrf vpn1 11.0.0.2

!!!!!

--- 11.0.0.2 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/0/0 ms

Testify the connectivity between S1 and PE:

Switch# ping -vrf vpn1 21.0.0.1

!!!!!

--- 21.0.0.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/0/0 ms

HSRP 프로토콜 구성

개요

HSRP 는 기본 게이트웨이 IP 주소로 구성된 IEEE 802 LAN 에서 IP 호스트에 대한 첫 번째 홉 중복을 제공하여 높은 네트워크 가용성을 제공하는 표준 방법입니다. HSRP 는 단일 라우터의 가용성에 의존하지 않고 IP 트래픽을 라우팅합니다. 이 인터페이스를 사용하면 일련의 라우터 인터페이스를 함께 사용하여 단일 가상 라우터 또는 기본 게이트웨이의 모양을 LAN 의 호스트에 제공 할 수 있습니다. HSRP 가 네트워크 또는 세그먼트 상에 구성 될 때 가상 라우터는 구성된 라우터 그룹간에 공유되는 가상 MAC (Media Access Control) 주소와 IP 주소를 제공합니다. HSRP 는 둘 이상의 HSRP 구성 라우터가 가상 라우터의 MAC 주소와 IP 네트워크 주소를 사용할 수있게합니다. 가상 라우터는 존재하지 않습니다. 서로 백업을 제공하도록 구성된 라우터의 공통 대상을 나타냅니다.
HSRP 는 지정된 활성 라우터에 장애가 발생하면이를 감지하고 선택된 대기 라우터는 상시 대기 그룹의 MAC 및 IP 주소를 제어합니다. 또한 새로운 대기 라우터가 선택됩니다. HSRP 를 실행하는 장비는 라우터 실패를 감지하고 활성 및 대기 라우터를 지정하기 위해 멀티 캐스트 UDP 기반 hello 패킷을 보내고받습니다. 인터페이스에서 HSRP 를 구성하면 ICMP (Internet Control Message Protocol) 리디렉션 메시지가 기본적으로 해당 인터페이스에 대해 비활성화됩니다.
HSRP 는 토큰 링 , 토큰 버스, FDDI 및 ATM LAN 네트워크 를 지원하지 않고 이더넷 / 패스트 이더넷 / VLAN 네트워크에서 구성 할 수 있습니다 .

HSRP 프로토콜 구성 작업 목록

HSRP 프로토콜 활성화
HSRP 그룹 등록 정보 구성

HSRP 프로토콜 구성 작업

HSRP 프로토콜 사용

인터페이스 HSRP 프로토콜을 활성화하려면 , 당신은 인터페이스 구성 모델에서 아래 명령을 구성해야 합니다

명령	설명
standby [*group-number*] **ip** [*ip-address/mask*][**secondary**]]	hsrp 프로토콜 활성화.

HSRP 그룹 등록 정보 구성

HSRP 그룹 속성을 구성하려면 , 당신은 하나의 인터페이스 구성 모델의 아래에서 더 명령 목록을 구성해야합니다 :

명령	설명
standby [*group-number*] **timers** hellotime *holdtime*	HSRP 타이머 매개 변수를 구성하십시오.
standby [*group-number*] **mac-address** *mac-address*	HSRP 그룹 가상 MAC 주소를 구성하십시오.
standby [*group-number*] **priority** *priority*	hsrp 우선 순위 구성를 구성합니다. (활성 / 대기 라우터에서 투표) (기본값 100)
standby [*group-number*] **preempt** [**delay***delay*]	hsrp 선점을 구성 합니다. 로컬 라우터의 우선 순위가 활성 라우터보다 큰 경우 로컬 라우터는 활성 라우터를 교체해야합니다. 구성 hsrp preempt 지연 timer.Local 라우터 선점 지연 타이머 후 활성 라우터를 교체해야합니다.
standby [*group-number*] **track** *type number* [*interface-priority*]	hsrp 그룹 추적 인터페이스 목록을 구성합니다. 추적 인터페이스가 실패하면 HSRP 우선 순위 값이 감소합니다.
standby [*group-number*] **authentication** *string*	hsrp 패킷 유효성 검사를 인증하기 위해 HSRP 그룹 인증 문자열을 구성합니다.
standby [*group-number*] **timers** *number*	Hello timer 에 전송주기를 구성합니다.

아래 명령을 사용하여 구성 및 상태 정보를 확인합니다.

명령	설명
show interface vlan <1-4094>	HSRP 구성정보를 확인합니다.
show standby [**interface** *interface-number*]**brief** | **detail]**	HSRP 상태 정보를 확인합니다. 옵션을 추가하여 정보를 확인합니다.

HSRP 구성의 예

다음은 일반적인 HSRP 구성 예제입니다. 네트워크 세그먼트 171.16.6.0/24 의 호스트는 L3SW#1 과 L3SW#2 를 통해 서버 1 과 서버 2 에 액세스합니다. L3SW#1 과 L3SW#2 는 HSRP 구성을 통해 단말들에 기본 게이트웨이 이중화(Hot-standby)를 제공 합니다.

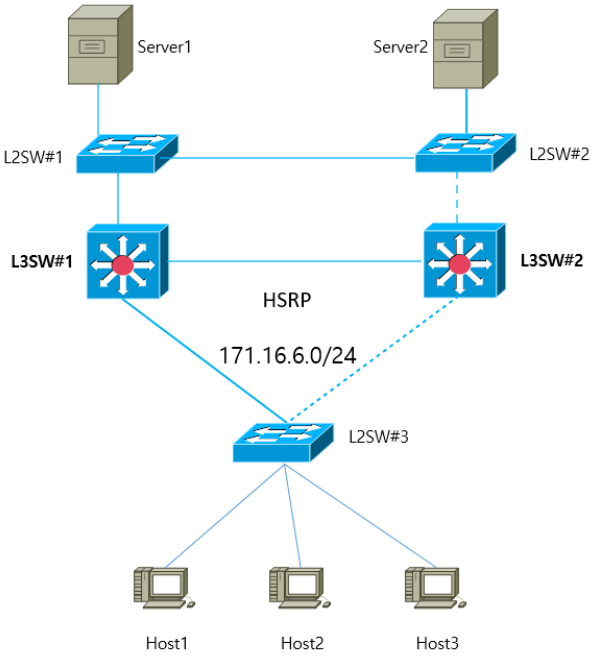


그림 2 - 1 HSRP 구성

L3SW#1 HSRP 구성
Interface vlan 1
ip address 171.16.6.5 255.255.255.0
standby 1 preempt
standby 1 ip 171.16.6.100 255.255.255.0

L3SW#2 HSRP 구성
Interface vlan 1
ip address 171.16.6.6 255.255.255.0
standby 1 priority 95
standby 1 ip 171.16.6.100 255.255.255.0

두 대의 L3 스위치는 가상 IP 가 171.16.6.100 인 HSRP 그룹을 구성합니다.
L3SW#1 의 기본 우선순위의 값은 100 이지만 L3SW#1 의 우선순위의 값은 95 입니다. 따라서, 우선순위가 높은 L3SW#1 이 활성화되어 게이트웨이로 동작하고, L3SW#2 는 대기 상태가 됩니다.

L3SW#1 가 문제가 생겨 다운되면 대기상태였던 L3SW#2 가 활성화 되어 게이트웨이로 동작합니다.

VRRP 구성

VRRP 개요

VRRP (Virtual Router Redundant Protocol)는 여러 라우터를 라우터 백업 그룹으로 사용하여 네트워크 사용자에게 가상 게이트웨이 라우터를 제공 할 수 있습니다. 라우터 감지 프로토콜이 지원되지 않는 경우 사용자에게 유용합니다. 선택한 라우터를 다시 설치하거나 고장 나면 새 NMS 라우터로 자동 전환 할 수 없기 때문입니다.
VRRP 는 가상 MAC 주소와 VRRP 실행 라우터 그룹이 공유하는 가상 IP 를 제공합니다. VRRP 는이 라우터 그룹에서 메인 라우터로 서버까지 라우터를 선택합니다. 주 라우터는 대상 주소가 백업 그룹의 가상 MAC 주소 인 패킷을 수신하고 전달합니다. VRRP 가 주 라우터의 무효를 감지하면 VRRP 라우터는 하나를 새로운 주 라우터로 선택하여 백업 그룹의 MAC 및 IP 를 얻습니다.
VRRP 실행 메인 라우터는 Sock Raw 멀티 캐스트를 기반으로 Advertise 패킷을 전송하고 대기 라우터는 이러한 패킷을 수신합니다. 대기 라우터는 Timer out 메커니즘과 Preempt 메커니즘을 통해 기본 라우터 역할을 할 수 있습니다. 라우터를 완전히 사용하려면 인터페이스에 여러 개의 대기 대기 그룹을 구성 할 수 있습니다.
현재 VRRP 는 이더넷 / 패스트 이더넷 / VLAN 프로토콜을 지원하지만 토큰 링과 토큰 버스를 지원하지 않습니다.
VRRP 는 RFC2338 에 정의 된 IETF VRRP 워킹 그룹에 의해 지정됩니다.

VRRP 적용 예

라인 백업

VRRP 를 통해 링크를 백업 할 수 있습니다.
예를 들어 회사 나 은행의 노드가 VRRP 그룹을 통해 외부 네트워크에 연결하려는 경우 하나의 라우터가 무효화되면 다른 라우터가 자동으로 작업을 인계합니다.

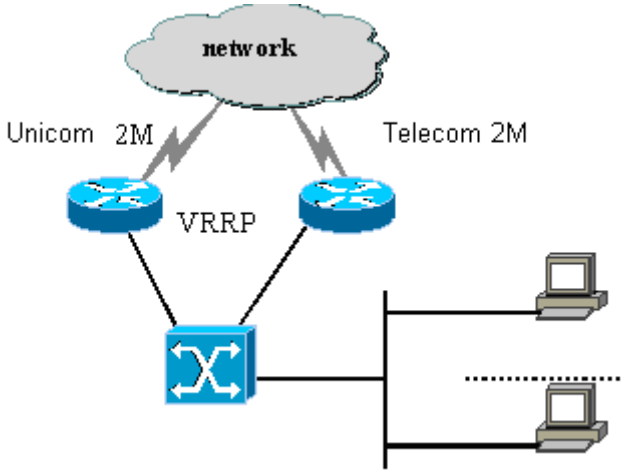


그림 3 - 1 VRRP 애플리케이션

VRRP 용어

VRRP	가상 라우터 중복 프로토콜
VIP	가상 IP
VMAC	가상 MAC 주소
VRRP Router	VRRP 를 실행하는 라우터
Virtual Router	네트워크의 다른 부분에서 가상 라우터로 볼 수있는 VRRP 그룹
IP Address Owner	VRRP VIP 에 대한 인터페이스의 실제 IP 를 구성하는 VRRP 라우터
Virtual Router Master	현재 VRRP 그룹의 데이터를 전달하는 활성 라우터
Primary IP Address	특정 규정에 따라 인터페이스의 주소 중에서 선택된 IP 주소. 일반적으로 첫 번째 IP 주소입니다.
Virtual Router Backup	마스터 라우터가 무효화 할 때 데이터 전달 라우터로 사용되도록 선택되는 대기 라우터

VRRP 구성 작업 목록

VRRP 활성화
VRRP 에 대한 시간 구성
VRRP 학습 모드 구성
VRRP 에 대한 설명 문자열 구성
VRRP 핫 백업에 대한 권한 구성
선점 모드 구성
다른 인터페이스를 추적 할 수있는 권한 구성
인증 문자열 구성
VRRP 모니터링 및 유지 보수

VRRP 구성 작업

VRRP 활성화

명령	설명
[**no**] **vrrp** *group-number* **ip** *[ip-address netmask* [**secondary**]]	VLAN 인터페이스 모드 VRRP 를 활성화하거나 비활성화합니다 .

VRRP 의 시간 구성

명령	설명
[**no**] **vrrp** *group-number* **timers advertise** *<1-255>*|<dsec *<5-360>*>	단위가 초 또는 0.1 초 단위(dsec)인 VRRP 의 시간을 구성합니다.

VRRP 학습 모드 구성

명령	설명
[**no**] **vrrp** *group-number* **timers learn**	VRRP 학습 모드를 구성합니다.

VRRP 의 Description 문자열 구성

명령	설명
[**no**] **vrrp** *group-number* **description** *TEXT*	VRRP 에 대한 설명 문자열을 구성합니다.

VRRP 핫 백업에 대한 권한 구성

명령	설명
[**no**] **vrrp** *group-number* **priority** *<1-255>*	기본 라우터 및 대기 라우터를 선택하기 위해 VRRP 라우터 에서 핫 대기 우선순위를 구성 합니다.(기본값 100)

선점 모드 구성

명령	설명
[**no**] **vrrp** *group-number* **preempt** [**delay** *<1-254>*]	선점 모드를 구성합니다.

다른 포트 추적을 위한 권한 구성

명령	설명
[**no**] **vrrp** *group-number* **track type** *number*[*interface-priority*]	다른 포트를 추적 할 수있는 권한을 구성하여 추적 포트의 상태 변경에 따라 VRRP 권한을 변경할 수 있습니다. 추적 포트가 무효화되면 VRRP 권한이 감소합니다. 추적 포트가 다시 시작되면 VRRP 권한이 증가합니다.

인증 문자열 구성

명령	설명
[**no**] **vrrp** *group-number* **authentication***string*	백업 프로토콜 패킷 교환시 동일한 그룹의 다른 라우터를 인증하는 데 사용되는 인증 문자열을 선택합니다.

VRRP 상태 확인 및 유지 보수

명령	설명
show vrrp [**interface** *interface-number*]**brief** | **detail]**	현재 VRRP 의 실행 상태를 표시합니다.
debug vrrp [**interface** *interface-numbergroup-number*] **all** | **packets** | **events** | **errors**	3 종류의 VRRP 이벤트를 디버그합니다.

VRRP 구성 예

다음 네트워크 토폴로지에서 동일한 네트워크의 두 서브넷은 각각 자신의 게이트웨이 (게이트웨이 A 와 게이트웨이 B)를 사용하여 인터넷에 액세스하지만 게이트웨이 A 와 게이트웨이 B 는 서로 대기합니다. 하나의 게이트웨이 (하나의 라우터)가 고장 나면 다른 하나는 두 서브넷에서 작동합니다.

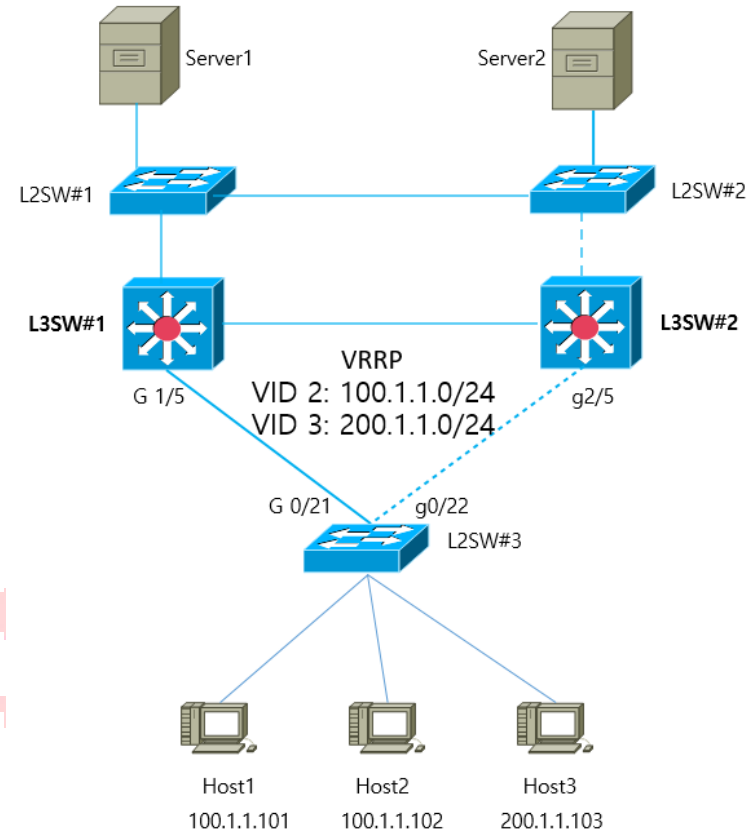


그림 3 - 2 단순 VRRP 애플리케이션 토폴로지

L3SW#1 VRRP 구성

```
vlan 2-3
interface gi 1/5
 switchport mode trunk
!
interface vlan 2
ip address 100.1.1.5 255.255.255.0
vrrp 3 associate 100.1.1.1 255.255.255.0
  vrrp 3 priority 120
  vrrp 3 description line1-master
  vrrp 3 authentication line1pwd
vrrp 3 preempt
  vrrp 3 timers advertise dsec 15
!
interface vlan 3
ip address 200.1.1.5 255.255.255.0
vrrp 6 associate 200.1.1.1 255.255.255.0
  vrrp 6 priority 110
  vrrp 6 description line2-backup
  vrrp 6 authentication line2pwd
vrrp 6 preempt
  vrrp 6 timers advertise dsec 15
```

L3SW#2 VRRP 구성

```
vlan 2-3
interface gi 2/5
switchport mode trunk
!
Interface vlan 2
ip address 100.1.1.6 255.255.255.0
vrrp 3 associate 100.1.1.1 255.255.255.0
  vrrp 3 priority 110
  vrrp 3 description line1-backup
  vrrp 3 authentication line1pwd
vrrp 3 preempt
  vrrp 3 timers advertise dsec 15
!
Interface vlan 3
ip address 200.1.1.6 255.255.255.0
vrrp 6 associate 200.1.1.1 255.255.255.0
  vrrp 6 priority 120
  vrrp 6 description line2-master
  vrrp 6 authentication line2pwd
vrrp 6 preempt
  vrrp 6 timers advertise dsec 15
```

L2SW#3 구성

```
vlan 2-3
interface Gigaethernet0/21
 switchport mode trunk
interface Gigaethernet0/22
 switchport mode trunk
!
interface Gigaethernet0/1
 switchport pvid 2
!
interface Gigaethernet0/2
 switchport pvid 2
interface Gigaethernet0/3
 switchport pvid 3
```

Multicast

이 장에서는 Multicast 라우팅 프로토콜을 구성하는 방법에 대해 설명합니다. Multicast 라우팅 명령에 내용은 "Multicast 라우팅 명령" 부분을 참조하십시오.
전통적인 IP 전송은 하나의 호스트 만 단일 호스트와 통신하거나 (unicast 통신) 모든 호스트와 통신 할 수 있습니다 (Broadcast 통신). Multicast 기술을 사용하면 한 호스트가 일부 호스트에 메시지를 보낼 수 있습니다. 이 호스트는 그룹 구성원이라고 합니다.
그룹 구성원에게 전송 된 메시지의 대상 주소는 D 클래스 주소 (224.0.0.0 ~ 239.255.255.255)입니다. Multicast 메시지는 UDP 와 같이 전송됩니다. TCP 처럼 신뢰할 수 있는 전송 및 오류 제어를 제공하지 않습니다. 발신자와 수신자는 Multicast 응용 프로그램을 구성합니다. 보낸 사람은 그룹에 가입하지 않고 Multicast 메시지를 보낼 수 있습니다. 그러나 수신자는 그룹의 메시지를 받기 전에 그룹에 가입해야 합니다. 그룹 구성원 간의 관계는 동적입니다. 호스트는 언제든지 그룹에 가입하거나 그룹에서 탈퇴 할 수 있습니다. 그룹 회원의 위치와 번호에는 제한이 없습니다. 필요한 경우 호스트는 여러 그룹의 구성원이 될 수 있습니다. 따라서 그룹의 상태와 그룹 구성원의 수는 시간에 따라 다릅니다.

IP Multicast 기술은 "일 대 다" 멀티미디어 응용 프로그램에 적합합니다.

Multicast 라우팅 인식

우리 라우터의 라우터 소프트웨어에서 Multicast 라우팅에 다음 사항이 포함됩니다.

- IGMP는 LAN에서 라우터와 호스트 간에 실행되며 그룹 구성원 관계를 추적하는 데 사용됩니다.
- OLNK는 간단한 토폴로지에서 사용되는 정적 Multicast 기술입니다. Multicast 포워딩을 실현하고 CPU와 대역폭을 효과적으로 절약합니다.
- PIM-DM, PIM-SM 및 DVMRP는 동적 Multicast 라우팅 프로토콜입니다. 라우터 간에 실행되며 Multicast 라우팅 테이블을 만들어 Multicast 전달을 실현합니다.

Multicast 구성 작업 목록

기본 Multicast 구성 작업 목록

- Multicast 라우팅 시작 (필수)
- TTL 임계 값 구성 (선택 사항)
- 고속 multicast 전달 취소 (선택 사항)
- 정적 multicast 경로 구성 (선택 사항)
- Multicast 경계 구성 (선택 사항)
- Multicast 도움 구성 (선택 사항)
- Stub Multicast 경로 구성 (선택 사항)
- Multicast 경로 모니터링과 유지 관리 (선택 사항)

IGMP 구성 작업 목록

- 현재 버전의 IGMP 수정
- IGMP 쿼리 간격 구성
- IGMP Querier 간격 구성
- IGMP의 최대 응답 시간 구성
- 마지막 IGMP 그룹 구성원의 쿼리 간격 구성
- 정적 IGMP 구성
- IGMP 즉시 제거 목록 구성

PIM-DM 구성 작업 목록

- 타이머 조절하기
- PIM-DM 버전 지정
- 상태 다과 구성하기
- 여과 목록 구성

- DR 우선 순위 구성
- 정보 (S, G) 삭제

PIM-SM 구성 작업 목록

- 정적 RP 구성
- 대기 BSR 구성
- 대기 RP 구성
- PIM-SM Multicast 라우팅 표시
- PIM-SM에서 학습한 Multicast 경로 지우기

DVMRP 구성 작업 목록

- 경로 요약 구성
- 포트의 필수적인 leaf-node 구성
- 경로 필터 구성
- DVMRP Unicast 경로 표시
- DVMRP multicast 경로 표시
- DVMRP에서 학습한 multicast경로 지우기

기본 Multicast 라우팅 구성

Multicast 라우팅 시작하기

라우터 소프트웨어가 Multicast 메시지를 전달할 수 있게 하려면 Multicast 라우팅을 시작해야합니다. 전역 구성 모드에서 다음을 실행하여 Multicast 메시지 전달을 시작합니다.

명령어	설명
ip multicast-routing	IP 라우팅 Multicast 시작하기

포트에서 Multicast 기능 구성하기

Multicast 라우팅 프로토콜이 포트에서 실행되면 IGMP 가 해당 포트에서 활성화됩니다. Multicast 라우팅 프로토콜에는 OLNK, PIM-DM, PIM-SM 및 DVMRP 가 포함됩니다.
하나의 Multicast 라우팅 프로토콜 만 동일한 포트에서 실행되도록 허용됩니다. 라우터가 여러 Multicast 도메인을 연결하면 다른 포트에서 다른 Multicast 프로토콜을 실행합니다.
라우터 소프트웨어가 Multicast 경계 라우터 (MBR)로 작동 할 수는 있지만. 가능하다면 여러 Multicast 라우팅 프로토콜을 동일한 라우터에서 동시에 실행하지 마십시오.
일부 Multicast 라우팅 프로토콜의 경우 심각한 영향을 받을 수 있습니다.
예를 들어, PIM-DM 과 BIDIR PIM-SM 이 동시에 실행되면 혼동이 발생합니다.

PIM-DM 시작하기

다음 실행하여 포트에서 PIM-DM 으로 multicast dense 기능을 활성화합니다.

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다
ip pim-dm	PIM-DM 이 실행중인 포트를 입력 한 다음 포트 구성 모드에서 PIM-DM Multicast 라우팅 프로세스를 활성화합니다.

PIM-SM 시작하기

PIM-DM 을 실행하고 PIM-DM Multicast 를 활성화하려면 다음 작업을 수행하십시오.

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다

ip pim-sm	PIM-SM 을 실행해야 하는 포트로 들어가고 포트 구성 모드에서 PIM-SM Multicast 라우팅 프로세스를 활성화합니다.

TTL 임계 값 구성

ip multicast ttl-threshold 명령을 실행하여 포트를 통과 할 수 있는 Multicast 메시지의 TTL 임계 값을 구성합니다. 기본 임계 값 1 을 사용하려면 no ip multicast ttl-threshold 명령을 실행하십시오.

명령어	설명
ip multicast ttl-threshold *ttl-value*	포트에 TTL 임계 값을 구성합니다.

예제

다음 예에서는 관리자가 포트에서 TTL 임계 값을 구성하는 방법을 보여줍니다.

```
interface vlan 1
ip multicast ttl-threshold 200
```

빠른 Multicast 전달기능을 취소하기

ip multicast mroute-cache 명령을 실행하여 포트에서 빠른 Multicast 전달 기능을 구성합니다. 빠른 Multicast 전달 기능을 취소하려면 no ip multicast mroute-cache 명령을 실행하십시오.

명령어	설명
ip mroute-cache	포트에 빠른 Multicast 전달을 실행합니다.

예제

다음 예는 관리자가 포트에서 고속 Multicast 전달 기능을 취소하는 방법을 보여 줍니다.

```
interface vlan1
no ip mroute-cache
```

경계 IP Multicast 구성하기

ip multicast boundary 명령을 실행하여 포트의 경계 Multicast 를 구성합니다. 구성된 경계를 취소하려면 no ip multicast boundary 명령을 실행하십시오. 두 번째 구성에서 사용 된 명령은 첫 번째 구성에서 사용 된 명령을 대체합니다.

명령어	설명
ip multicast boundary *access-list*	인터페이스에 경계 multicast 를 구성합니다.

예제

다음 예는 포트의 관리 경계를 구성하는 방법을 보여줍니다.

```
interface vlan 1
ip multicast boundary acl
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

IP Multicast 도움 구성하기

ip multicast helper-map 명령을 실행하여 Multicast 경로를 사용하여 Multicast 네트워크에서 두 개의 Broadcast 네트워크를 연결합니다.
명령을 취소하려면 no ip multicast helper-map 명령을 실행하십시오.

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다
ip multicast helper-map broadcast *group-address access-list*	ip multicast helper 명령을 구성하여 Broadcast 메시지를 Multicast 메시지로 변환합니다.
ip directed-broadcast	지향성 Broadcast 를 허용합니다.
ip forward-protocol udp [*port*]	메시지를 전달하도록 번호를 구성합니다.

Broadcast 네트워크의 목적지를 연결하는 마지막-홉 라우터에 다음을 수행하십시오.

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다
ip directed-broadcast	지향성 broadcast 를 허용합니다.
ip multicast helper-map *group-address broadcast-address access-list*	ip multicast helper 명령을 구성하여 multicast 메시지를 Broadcast 메시지로 변환합니다.
ip forward-protocol udp [port]	메시지를 전달하도록 포트번호를 구성합니다.

예제

다음 예는 ip multicast helper 명령을 구성하는 방법을 보여줍니다.

라우터 구성은 다음과 같습니다. 지향성 메시지를 처리하기 위해 첫 번째 홉 라우터의 e0 포트에 ip directed-broadcast 명령을 구성합니다. ip multicast helper-map Broadcast 230.0.0.1 구성

testacl1 을 사용하여 소스 주소 192.168.20.97/24 에서 대상 주소 230.0.0.1 의 Multicast 메시지로 전송 된 포트 번호 4000 의 UDP Broadcast 메시지를 변환 할 수 있습니다.

방향 메시지를 처리하기 위해 마지막 홉 라우터의 e1 포트에 ip directed-broadcast 명령을 구성합니다. ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2 를 구성하여 포트 번호가 4000 이고 소스 주소가 192.168.20.97/24 인 대상 주소 230.0.0.1 을 대상이 있는 Broadcast 메시지로 변환 할 수 있습니다 address 172.10.255.255.

소스 Broadcast 네트워크를 연결하는 첫 번째 홉 라우터에서 다음 작업을 수행하십시오. (라우터가 VLAN 포트에 구성되어 있음)

```
interface vlan 1
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim-dm
!
ip access-list extended testacl    permit udp 192.168.20.97 255.255.255.0 any ip
forward-protocol udp 4000
```

Broadcast 네트워크의 목적지를 연결하는 마지막-홉 라우터에 다음을 수행합니다..

```
interface vlan 1
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
!
ip access-list extended testacl2    permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

Stub Multicast 경로 구성하기

ip igmp helper-address 및 ip pim-dm neighbor-filter 명령을 실행하여 stub multicast 경로를 구성합니다.

stub 라우터와 호스트가 연결된 포트에서 다음 작업을 수행하십시오.

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다
ip igmp helper-address *destination-address*	IP igmp 명령을 구성합니다. 멀티케스트를 전달할 도움주소를 중앙라우터에 메시지보냅니다.

중앙 라우터와 stub 라우터가 연결된 포트에서 다음 작업을 수행합니다.

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다
ip pim neighbor-filter *access-list*	Stub 라우터에서 모든 PIM 메시지를 필터링합니다

예제

다음과 같이 라우터 A 와 B 를 구성합니다.

Stub 라우터 A 구성

ip multicast-routing

interface vlan 1

ip pim-dm

ip igmp helper-address 10.0.0.2

중심 라우터 B 구성

ip multicast-routing

ip pim-dm

ip pim-dm neighbor-filter stubfilter

ip access-list stubfilter

deny 10.0.0.1

Multicast 경로 모니터링 및 유지보수하기

Multicast 캐시와 라우팅 테이블 지우기

특정 캐시 또는 라우팅 테이블이 유효하지 않은 경우 해당 내용을 지워야합니다.
관리모드에서 다음을 실행하십시오.

명령어	설명
clear ip igmp group [*type interface*]	IGMP 캐시의 항목을 지 웁니다.
clear ip mroute *[pim-dm /sm group-address / source-address]*	Multicast 라우팅 테이블의 항목을 지 웁니다.

Multicast 라우팅 테이블 및 시스템 통계 정보 표시.

IP Multi 라우팅 테이블, 캐시 또는 데이터베이스에 대한 자세한 정보는 리소스 사용 방법을 판단하고 네트워크 문제를 해결하는 데 도움이 됩니다.

다음 명령을 실행하여 multicast 라우팅에 대한 통계 정보를 표시합니다.

명령어	설명
show ip igmp groups [*type number* | *group-address*] [detail]	IGMP-cache 에 멀티케스트 그룹을 표시합니다 .
show ip igmp interface [*type number*]	인터페이스에 IGMP 구성정보를 표시합니다.
show ip mroute mfc	멀티케스트 전달케시를 표시합니다.
show ip rpf [**ucast | pim-dm** | **pim-sm**] *source-address*	RPF 정보를 표시합니다.

IGMP 구성하기

개요

IGMP

IGMP (Internet Group Management Protocol)는 Multicast group 구성원을 관리하는 데 사용되는 프로토콜입니다. IGMP 는 호스트 측과 스위치 측을 포함하는 비대칭형 프로토콜입니다. 호스트 측에서 IGMP 프로토콜은 호스트, Multicast 그룹 구성원이
자신이 속한 Multicast 그룹을 보고하는 방법과 호스트가 스위치의 쿼리 메시지에 응답하는 방법을 규정합니다. 스위치 측면에서 IGMP 프로토콜은 IGMP 지원
스위치가 로컬 네트워크에 있는 호스트의 Multicast 그룹 구성원 ID 를 학습하는
방법과 호스트의 보고 메시지에 따라 저장된 Multicast 그룹 구성원 정보를
수정하는 방법을 규정합니다.

스위치가 IGMP 라우터 프로토콜을 지원하기 때문에 multicast 라우팅 프로토콜에 현재 네트워크의 multicast 그룹 구성원에 대한 정보가 제공 될 수 있으며 스위치는 Multicast 메시지를 전달할지 여부를 결정합니다. 즉, 스위치가 IP 메시지의 Multicast 프로세스를 지원할 수 있게 하려면 Multicast 라우팅 프로토콜과
IGMP 라우터 프로토콜을 지원하도록 스위치를 구성해야 합니다. 현재 AAA 스위치는 최신 버전인 IGMP 라우터 프로토콜과 버전 3 IGMP 를 지원합니다.

IGMP 에 대한 독립적 인 시작 명령이 없습니다. IGMP-Router 프로토콜의 기능은 Multicast 라우팅 프로토콜을 통해 시작됩니다.

OLNK

정확히 말하면 IGMP 의 유일한 링크 프로토콜 (OLNK)은 다른 프로토콜처럼 상호 작용 프로세스가 없기 때문에 Multicast 라우팅 프로토콜이 아닙니다. 그러나 일부 특수한 경우 OLNK 를 단순 토폴로지에서 실행하면 좋은 결과를 얻을 수 있습니다. 협상 프로세스가 없는 PIM-DM 프로토콜과 마찬가지로 OLNK 는 IGMP 그룹 구성원의 변경을 처리하고 토폴로지 변경에 따라 RPF 인터페이스를 즉시 조정할 수 있습니다. 이러한 방식으로 OLNK 는 Multicast 전달을 보장하고 Multicast 라우팅
프로토콜의 제어 메시지가 대역폭을 차지하는 것을 방지합니다.

IGMP 구성하기

IGMP 라우터의 속성을 구성하는 명령은 주로 IGMP 매개 변수를 조정하는 명령입니다. 다음은 이러한 명령을 설명합니다. 자세한 내용은 IGMP 명령과 관련된 설명 문서를 참조하십시오.

현재 IGMP 버전 변경

지금까지 IGMP 프로토콜에는 세 가지 정식 버전이 있습니다. 해당 RFC 는 RFC1112, RFC2236 및 RFC3376 입니다. IGMP V1 은 Multicast 그룹 구성원을
기록하는 기능만 지원합니다. IGMP V2 는 지정된 Multicast 그룹 구성원을
쿼리하고, IGMP 호스트가 Multicast 그룹을 떠날 때 유휴 메시지를 생성하고
그룹 구성원의 변경 지연을 단축 할 수 있습니다. IGMP V3 에는 소스 호스트 주소에 해당하는 Multicast 그룹 구성원 ID 를 업데이트하고 유지 관리하는 추가 기능이
있습니다. IGMP V3 의 IGMP 라우터 프로토콜은 IGMP V1 및 IGMP V2 의 호스트 측과 완벽하게 호환됩니다. AAA 의 스위치 소프트웨어는 3 개의 IGMP 버전의 IGMP 라우터 프로토콜을 지원합니다.
서로 다른 인터페이스에서 IGMP-Router 기능을 구성 할 수 있습니다 (서로 다른 인터페이스에 구성된 Multicast 라우팅 프로토콜이 IGMP 라우터 기능을 시작함). 그리고 다른 버전의 IGMP 를 다른 인터페이스에서 실행할 수 있습니다.

> Multicast 스위치는 동일한 네트워크를 연결하는 포트 중 하나에서만 IGMP 라우터 기능을 시작 할 수 있습니다.

다음 명령을 실행하여 포트에서 IGMP-Router 프로토콜의 버전을 변경합니다.

명령어	설명
ip igmp version *version_number*	포트에서 실행중인 IGMP 버전을 변경합니다.

IGMP 쿼리 간격 구성

현재 IGMP 라우터 프로토콜의 버전 번호가 무엇이든 관계없이 Multicast 스위치는 IGMP 라우터 기능이 시작된 포트에서 특정 시간마다 IGMP 일반 쿼리 메시지를 보낼 수 있습니다. 전송 주소는 224.0.0.1 입니다. Multicast 스위치의 목적은 IGMP 호스트에서 보고 메시지를 가져 와서
네트워크의 각 IGMP 호스트가 속한 Multicast 그룹을 파악하는 것입니다. 일반 쿼리 메시지를 보내는 간격을 IGMP 쿼리 간격이라고 합니다. IGMP Query Interval (IGMP 쿼리 간격) 매개 변수가 큰 값으로 구성된 경우 스위치는 현재 IGMP 호스트가 속한 Multicast 그룹에 대한 정보를

즉시 수신 할 수 없습니다. IGMP Query Interval (IGMP 쿼리 간격) 매개 변수가 작은 값으로 구성된 경우 현재 네트워크에서 IGMP 메시지의 흐름이 증가합니다.

다음 명령을 실행하여 포트에서 IGMP 쿼리 간격을 수정합니다.

명령어	설명
ip igmp query-interval *time*	현재 인터페이스에서 IGMP 쿼리 간격을 수정합니다 (단위 : 초).

IGMP 쿼리의 간격 구성하기

IGMP 라우터 프로토콜의 버전 2 및 버전 3 에 대해 IGMP 라우터 프로토콜을 실행하는 다른 스위치가 동일한 네트워크에 있으면 쿼리 프로그램을 선택해야합니다.

Querier 는 쿼리 메시지를 보낼 수 있는 스위치를 의미합니다 (사실 IGMP-Router 프로토콜이 활성화 된 스위치의 포트입니다). 보통은 하나의 네트워크에는 하나의 쿼리가 있습니다. 즉, 하나의 스위치만 IGMP 쿼리 메시지를 보냅니다. Multicast
라우팅 프로토콜은 IGMP-Router V1 에서 IGMP 쿼리 메시지를 보낼 스위치를 결정하기 때문에 IGMP-Router V1 에 대한 쿼리 작성자 선택이 없습니다.

IGMP-Router V2 및 IGMP-Router V3 에는 동일한 querier 선택 방법이 있습니다. 즉, 최소 IP 주소를 가진 스위치가 네트워크의 querier 입니다. querier 가 아닌 스위치는 querier 의 존재를 기록하기 위해 시계를 저장해야 합니다. 클록 시간이 초과되면 더 작은 IP 주소로 스위치에서 IGMP 쿼리 메시지를 수신 할 때까지 비 쿼리 스위치가 querier 로 변합니다.

IGMP-Router V2 경우 다음을 사용하여 다른 쿼리 간격을 구성 할 수 있습니다

명령어	설명
ip igmp querier-timeout *time*	다른 queriers 의 간격을 구성합니다 (단위 : 초).

IGMP-Router V1 의 경우 다른 쿼리의 간격은 쓸모가 없습니다. IGMP-Router V3 의 경우, 프로토콜 자체에 의해 결정되기 때문에 간격을 구성 할 수 없습니다.

최대 IGMP 응답 시간 구성

IGMP-Router V2 및 IGMP-Router V3 의 경우 전송 된 IGMP 일반 쿼리 메시지의 특수 데이터 필드는 IGMP 호스트의 최대 응답 시간을 조절합니다. 즉, IGMP 호스트는 규정 된 최대 응답 시간이 만료되기 전에 응답 메시지를 보내야 하며 이는 일반 쿼리 메시지가 수신되었음을 나타냅니다. 최대 응답 시간이 큰 값으로 구성된 경우 Multicast 그룹 구성원의 변경이

지연됩니다. 최대 응답 시간을 작은 값으로 구성하면 현재 네트워크에서 IGMP 메시지의 흐름이 증가합니다.

참고:

최대 IGMP 응답 시간은 IGMP 쿼리 간격보다 짧아야 합니다. 최대 응답 시간 값이 쿼리 간격보다 크면 시스템은 query-interval-1 에 대한 최대 응답 시간을 자동으로 구성합니다. IGMP-Router V2 및 IGMP-Router V3 의 경우 인터페이스 구성 모드에서

다음 명령을 실행합니다 최대 IGMP 응답 시간을 구성하려면 다음을 수행하십시오.

명령어	설명
ip igmp query-max-response-time *time*	최대 IGMP 응답 시간 (단위:초)을 구성합니다.

IGMP-Router V1 의 경우, 최대 IGMP 응답 시간은 프로토콜 자체에 의해 결정됩니다. 따라서 이전 명령은 IGMP-Router V1 에서는 쓸모가 없습니다.

마지막 그룹 구성원에 대한 IGMP 쿼리 간격 구성하기

IGMP-Router V2 및 IGMP-Router V3 의 경우 특정 Multicast 그룹에 대한 그룹 별 쿼리 메시지가 전송되면 마지막 그룹 구성원의 쿼리 간격이 호스트의 최대 응답 시간으로 사용됩니다. 즉, IGMP 호스트는 그룹 특정 쿼리 메시지가 수신되었음을 나타내는 마지막 그룹 구성원의 최대 응답 시간이 만료되기 전에 응답 메시지를 보내야합니다. IGMP 호스트가 쿼리 메시지에 응답 할 필요가 없다는 것을 발견하면 기존 간격 이후에 메시지에 응답하지 않습니다. 이 경우 Multicast 스위치는
저장된 Multicast 그룹 구성원 정보를 업데이트합니다. 마지막 그룹 구성원의 쿼리 간격이 큰 값으로 구성된 경우 Multicast 그룹 구성원의 변경이 지연됩니다. 마지막 그룹 구성원의 쿼리 간격이 작은 값으로 구성된 경우 현재 네트워크에서 IGMP 메시지의 흐름이 증가합니다.

IGMP-Router V2 및 IGMP-Router V3 의 경우 인터페이스 구성 모드에서 다음을 실행하여 마지막 그룹 구성원의 IGMP 쿼리 간격을 구성합니다.

명령어	설명
ip igmp last-member-query-interval *time*	마지막 그룹 구성원의 IGMP 쿼리 간격 (단위: 밀리 초)을 구성합니다.

앞의 명령은 IGMP-Router V1 에서는 유효하지 않습니다.

정적 IGMP 구성

IGMP-Router 프로토콜에 의해 규제되는 기능 외에도 스위치는 포트상의 정적 Multicast 그룹 구성을 지원합니다. IGMP 호스트의 경우 Multicast 그룹 구성원 관계가 다를 수 있습니다. IGMP

호스트가 Multicast 그룹 group1 에만 속하고, Multicast 메시지를 수신 시 Multicast 그룹 group1 에 Multicast 메시지를 보냅니다. 일정 시간이 지나면 Multicast 그룹 인 그룹 2 에 속할 수 있으며 Multicast 그룹 2 에 Multicast 메시지를 전송하여 Multicast 그룹 2 에 보냅니다. 다른 시간이 지나면 IGMP 호스트는 Multicast 그룹에 속하지 않을 수 있습니다. 따라서, Multicast 그룹 할당 정보는 다양하다.

위의 "동적 Multicast 그룹"과 달리 포트가 정적 Multicast 그룹에 속하도록 구성된 경우 Multicast 라우팅 프로토콜은 포트를 Multicast 그룹의 Multicast 메시지를 항상 수신하고 보내는 포트로 사용합니다. IGMP-Router V3 와 더 잘 호환되도록 정적 Multicast 그룹은 지정된 소스 주소에서 Multicast 메시지를 수신하도록 구성 할 수 있습니다. 즉, Multicast 메시지가 수신 될 때 소스 필터 기능이 추가됩니다.

인터페이스 구성 모드에서 다음 명령을 실행하여 포트에 대한 정적 Multicast 그룹을 구성합니다.

명령어	설명
ip igmp static-group { *| *group-address*} {**include** *source-address* | *<cr>* }	포트의 정적 Multicast 그룹 속성을 구성합니다.

IGMP 즉시-방출 목록 구성

스위치의 포트에서 IGMP V2 가 시작되고 포트가 연결된 네트워크에 IGMP 호스트가 하나만 있는 경우 IGMP 즉시-방출 목록을 구성하여 IGMP 호스트의 즉시-방출기능을 구현할 수 있습니다. IGMP V2 의 규정에 따르면 호스트가 특정 Multicast 그룹을 떠날 때 호스트는 모든 Multicast 스위치에 Leave 메시지를 보냅니다. Leave 메시지를 수신 한 후 Multicast 스위치는 그룹 별 메시지를 보내 호스트에서 Multicast 그룹과 주고받는 Multicast 메시지가 포트에 있는지 여부를 확인합니다. 즉시 방출 기능이 구성되어 있으면 IGMP 호스트와 Multicast 스위치 간에 메시지를 상호 작용할 필요가 없으므로 Multicast 그룹 구성원 ID 의 변경가능 합니다.

참고:

명령어는 전역 구성 모드와 인터페이스 구성 모드에서 모두 구성 할 수 있습니다. 전역 구성 모드에서 구성된 명령의 우선 순위는 인터페이스 구성 모드에서 구성된 명령의 우선 순위보다 높습니다. 전역 구성 모드에서 명령을 처음 구성하면
인터페이스 구성 모드에서 구성된 명령이 생략됩니다. 명령이 인터페이스 구성 모드에서 처음 구성되면 전역 구성 모드에서 구성된 명령은 인터페이스 구성 모드에 구성된 명령을 삭제합니다.

IGMP-Router V2 의 경우 인터페이스 구성 모드에서 다음 명령을 실행하여 IGMP 즉시-방출 목록을 구성합니다.

명령어	설명
ip igmp immediate-leave group-list *list-name*	IGMP 호스트에 대한 Multicast 그룹에서 즉시 나가는 기능을 구현하는 액세스 목록을 구성합니다.
ip access-list standard *list-name*	list-name 이라는 표준 IP Access-list 를 만듭니다.
permit *source-address*	표준 Access-list 구성 모드에서 즉석 탈퇴 기능을 구현하는 IGMP 호스트의 IP 주소를 구성합니다.

이전 명령은 IGMP-Router V1 및 IGMP-Router V3 에는 유효하지 않습니다.

IGMP 특성 구성 예

모든 구성은 Vlan 포트에서 IGMP 특성을 수행합니다.

IGMP 버전 변경의 예

상위 버전의 IGMP-라우터 프로토콜은 하위 버전의 IGMP 호스트와 호환되지만,
이전 버전의 IGMP-라우터 프로토콜과 호환되지 않는다. 따라서 현재 네트워크에 있는 이전 버전의 IGMP-라우터 프로토콜을 실행하는 스위치가 있는 경우 최신 버전의 IGMP-라우터 프로토콜을 초기 버전이 같은 IGMP-라우터 프로토콜로 변경해야 합니다.

관리자가 IGMP-라우터 V1 및 IGMP-라우터 V2 를 실행하는 스위치가 로컬 스위치가 연결된 네트워크에 있다는 것을 알고 있다고 가정하면, 관리자는 IGMP-라우터 프로토콜 버전의 V2 버전을 IGMP-라우터 2 에서 변경해야 합니다.

```
ip igmp version 1
```

모든 것 IGMP쿼리 간격 구성 예

다음 예는 IGMP 쿼리 간격을 50 초로 수정하는 방법을 보여줍니다.

```
ip igmp query-interval 50
```

IGMP Querier 간격 구성 예

다음 예는 IGMP Querier 간격을 100 초로 수정하는 방법을 보여줍니다.

```
ip igmp querier-timeout 10
```

IGMP 최대 응답 시간 예제

다음 예는 최대 IGMP 응답 시간을 15 초로 수정하는 방법을 보여줍니다.

```
ip igmp query-max-response-time 15
```

마지막 그룹 구성원에 대한 IGMP 쿼리 간격 구성의 예

다음 예에서는 마지막 그룹 구성원의 IGMP 쿼리 간격을 2000ms 로 수정하는 방법을 보여줍니다.

ip igmp last-member-query-interval 2000

정적 IGMP 구성 예제

정적 Multicast 그룹의 구성 명령은 다른 매개 변수를 채택하여 정적 클래스의 다른 클래스를 정의 할 수 있습니다. 다음 예제는 다른 명령 매개 변수를 실행 한 결과를 보여줍니다.

ip igmp static-group *

이전 구성 명령은 모든 정적 Multicast 그룹을 구성합니다. Multicast 라우팅 프로토콜은 모든 IP multicast 메시지를 interface vlan 1 으로 전달하는 것입니다.

ip igmp static-group 224.1.1.7

이전 구성 명령은 interface vlan 1 에 정적 multicast 그룹 224.1.1.7 을 구성합니다. 즉, 인터페이스는 multicast 그룹 224.1.1.7 에 속합니다. Multicast 라우팅 프로토콜은 마침내 Multicast 그룹 224.1.1.7 로 전송 된 모든 IP Multicast 메시지를 interface vlan 1 으로 전달하는 것입니다.

interface vlan 1

ip igmp static-group 224.1.1.7 include 192.168.20.168

기존 명령 구성은 인터페이스 ethernet 0/0 에 정적 Multicast 그룹 224.1.1.7 을 구성하고 Multicast 그룹의 source-filter 를 192.168.20.168 로 정의합니다. 즉, 인터페이스는 Multicast 그룹 224.1.1.7 에 속하지만 192.168.20.168 의 IP Multicast 메시지 만 수신합니다. Multicast 라우팅 프로토콜은 192.168.20.168 에서 수신되고 마침내 Multicast 그룹 224.1.1.7 로 전송 된 IP Multicast 메시지를 인터페이스 이더넷 0/0 으로 전달하는 것입니다.
인터페이스 구성 모드에서 다음 명령을 실행하여 192.168.20.169 에서 마지막으로 Multicast 그룹 224.1.1.7 로 전송 된 IP Multicast 메시지를 수신합니다.

ip igmp static-group 224.1.1.7 include 192.168.20.169

기존 명령은 여러 소스 주소를 정의하기 위해 여러 번 실행될 수 있습니다.

참고:

Multicast 그룹에서 Multicast 그룹 정보는 특정 소스 주소와 모든 소스 주소에 대해 동시에 구성 할 수 없습니다. 이후 구성에서 사용되는 명령은 생략됩니다. 예를 들어 ip igmp static-group 224.1.1.7 명령을 실행 한 후 ip igmp static-group 224.1.1.7 include 192.168.20.168 명령을 실행하면 ip igmp 명령이 실행됩니다
정적 그룹 224.1.1.7 포함 192.168.20.168 은 생략 됩니다.

IGMP 즉시-방출 목록 구성 예시

다음 예에서는 immediate-leave 기능을 사용하여 interface Vlan 1 에서 일시 중지되도록 Access-list 를 구성하고 IGMP 호스트의 IP 주소 192.168.20.168 을
Access-list 에 추가하는 방법을 보여줍니다. 이 구성을 사용하면 IP 주소가 192.168.20.168 인 IGMP 호스트에서 즉석 탈퇴 기능을 사용할 수 있습니다.

```
interface vlan 1
ip igmp immediate-leave imme-leave
exit
ip access-list standard imme-leave
permit 192.168.20.168
```

PIM-DM 구성

PIM-DM 개요

Protocol Independent Multicast Dense Mode (PIM-DM)는 결합 모드의 Multicast 라우팅 프로토콜입니다. 기본적으로 Multicast 소스가 Multicast 데이터를 보내기 시작하면 도메인의 모든 네트워크 노드가 데이터를 수신합니다. 따라서 PIM-DM 은 Multicast 패킷을 Broadcast 전정 모드로 전달합니다. Multicast 소스가 데이터를 보내기 시작하면 스위치는 RPF 인터페이스를 제외한 모든 PIM 활성화 인터페이스로 Multicast 패킷을 전달합니다. 이러한 방식으로 PIM-DM 도메인의 모든 네트워크 노드는 이러한 Multicast 패킷을 수신 할 수 있습니다. Multicast 포워딩을 완료하기 위해 스위치는 그룹 G 와 소스 S 에 해당하는 Multicast 라우팅 항목 (S, G)을 생성해야 합니다. 라우팅 항목 (S, G)에는 Multicast 소스 주소, Multicast 그룹 주소, 발신 인터페이스 목록, 타이머 및 로고를 포함합니다.

특정 네트워크 세그먼트에 Multicast 그룹 구성원이 없으면 PIM-DM 은 pruning 정보를 보내고 네트워크 세그먼트를 연결하는 전달 인터페이스를 정리 한 다음 pruning 상태를 구성합니다. pruning 상태는 제한 시간 타이머에 해당합니다. 타이머가 시간 초과되면 pruning 상태가 다시 전달 상태가 되며 Multicast 데이터는 이 분기를 따라 전달 될 수 있습니다. 또한 pruning 상태에는 Multicast 소스 및 Multicast 그룹에 대한 정보가 들어 있습니다. pruning 영역에 Multicast 그룹 구성원이 나타나면 PIM-DM 은 상위 필드의 pruning 상태가 시간 초과되어 pruning
상태가 전달이 될 때까지 기다리지 않고 관여 메시지를 상위 필드로 변환합니다

소스 S 가 여전히 그룹 G 에 정보를 보내는 한, 첫 번째-홉 위치는 라우팅 항목 (S, G)의 새로 고침 정보를 주기적으로 원래 Broadcast 트리로 보내서 새로 고침을 마칩니다. PIM-DM 의 상태 새로 고침 방법은 다운 스트림 상태를 새로 고침 하여 Broadcast 트리의 pruning 이 시간 초과되지 않도록 합니다.

다중 액세스 네트워크에서 DR 선택에도 PIM-DM 은 다음과 같은 법을 도입합니다.

- 반복적으로 전달되는 Multicast 패킷을 방지하기 위해 고유의 전달자를 선택하는 주장 메커니즘을 사용합니다.
- add / prune 억제 메커니즘을 사용하여 중복 추가 / 정리 정보를 줄이십시오.
- 부적절한 가지 치기 작업을 거부하는 메커니즘을 치기를 거부합니다.

PIM-DM 도메인에서 PIM-DM을 주기적으로 실행하는 스위치는 Hello 정보를 주기적으로 보내 다음과 같은 목적을 달성합니다.:

- 인접하는 PIM 스위치를 찾습니다.
- 결정 리프 네트워크와 리프 스위치.
- Multi-access 네트워크에서 지정된 라우터(DR)를 선택합니다.

IGMP v1 과 호환되도록 PIM-DM 은 DR 선택을 합니다. 인터페이스의 모든 PIM 인접 라우터가 DR 우선 순위를 지원하면 우선 순위가 높은 인접 라우터가 DR 으로 선택됩니다. 우선 순위가 같으면 인터페이스 IP 값이 최대 인 인접 라우터가 DR 으로 선택됩니다. 우선 순위가 여러 라우터의 Hello 메시지에 표시되지 않으면 인터페이스가 가장 큰 IP 값을 가진 라우터가 DR 으로 선택됩니다.
스위치의 PIM-DM v2 는 CIDR, VLSM 및 IGMP v1-v3 을 지원합니다.

PIM-DM 구성하기

타이머 수정하기

라우팅 프로토콜은 Hello 메시지와 State-Refresh 제어 메시지의 전송 빈도를 판단하기 위해 여러 개의 타이머를 사용한다. Hello 메시지를 전송하는 간격은 인접 관계가 올바르게 생성 될 수 있는지 여부에 영향을 미칩니다.
스위치 구성 모드에서 다음 명령을 실행하여 타이머를 조절하십시오:

명령어	설명
ip pim-dm hello-interval	인터페이스 및 neighbor 으로부터 Hello 메세지를 송신하는 간격 (초 단위)을 구성합니다.
ip pim-dm state-refresh origination-interval	소스를 직접 연결하는 첫 번째-홉 스위치의 상태 새로 고침 메시지를 보내는 간격은 업스트림 포트의 구성에만 유효합니다. 다음 스위치의 경우 간격은 상태 새로 고침 메시지를 수신하고 처리하는 기간입니다.

상태 새로 고침 구성

PIM-DM 의 상태 새로 고침 제어 정보는 기본적으로 관리 모드에서 전달됩니다. 인터페이스 구성 모드의 구성 명령은 소스를 직접 연결하는 첫 번째 홉 스위치가 주기적으로 상태 새로 고침

메시지를 보낼 때 업스트림 포트의 구성에만 적용됩니다. 다음 스위치의 경우 간격은 상태 새로 고침 메시지를 처리 기간입니다.

명령어	설명
no ip pim-dm state-refresh disable	포트에서 상태 새로 고침 메시지를 보내고받을 수 있습니다.
ip pim-dm state-refresh origination-interval	포트에서 상태 새로 고침 메시지를 보내고받을 간격을 구성합니다.

필터 구성 목록

PIM-DM 은 기본적으로 필터링 목록을 구성하지 않습니다. 참조 된 필터링 목록은 인접 필터링 목록 및 Multicast 경계 필터링 목록을 포함합니다. 여과 목록은 인터페이스 구성 모드에서 구성해야 합니다.

네트워크 세그먼트의 스위치 또는 스위치가 PIM-DM 협상에 참가하는 것을 금지하려면 인접 필터링 목록을 구성해야 합니다. 일부 그룹이 로컬 영역을 통과하는 것을 금지하거나 허용하려면 Multicast 경계 필터링 목록을 구성해야 합니다.

명령어	설명
ip pim-dm neighor-filter	인접 필터링 목록을 구성합니다.
ip multicast boundary	Multicast 경계에서 필터링 목록 만듭니다.

DR 우선순위 구성하기

IGMP v1 과 호환성에는 DR 선택이 필요합니다. 기본적으로 DR 의 우선 순위는
1 로 구성됩니다. 인터페이스의 모든 PIM 인접 라우터가 DR 우선 순위를 지원하면 높은 우선 순위를 가진 인접 라우터가 DR 으로 선택됩니다. 우선 순위가 같으면
인터페이스 IP 값이 최대 인 인접 라우터가 DR 으로 선택됩니다. 우선 순위가 여러 라우터의 Hello 메시지에 표시되지 않으면 인터페이스가 가장 큰 IP 값을 가진
라우터가 DR 으로 선택됩니다.
인터페이스 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip pim-dm dr-priority	지정된 포트에서 로컬 DR 에 대한 우선 순위를 구성합니다.

항목 (S,G) 지우기

일반적으로 로컬 MRT 의	**설명**
clear ip mroute pim-dm {***** | *group* [*source*]}	로컬 MRT 에서 품목 (S, G)을 지웁니다. 작업은 라우팅 테이블의 항목 삭제하는 것입니다. 명령은 업스트림 포트에서 PIM-DM Multicast 라우팅 프로토콜에 의해 생성 된 (S, G) 항목 만 삭제하는 데 사용됩니다.

PIM-SM 구성하기

PIM-SM 개요

Protocol Independent Multicast Spare Mode (PIM-SM)는 스파 스 모드의 Multicast 라우팅 프로토콜입니다. PIM-SM 도메인에서 PIM-SM 을 실행하는 스위치는 주기적으로 Hello 정보를 전송하여 다음과 같은 목적을 달성합니다.

- 인접한 PIM-SM 스위치를 발견하십시오.
- 다중 액세스 네트워크에서 지정된 라우터 (DR)를 선택합니다.

다음 그림과 같이 DR 은 조인 / 정리 메시지를 Multicast 트리의 방향으로 직접 연결된 그룹 구성원을 연결하거나 직접 연결된 multicast 소스의 데이터를 muticast 분배 트리로 보냅니다.

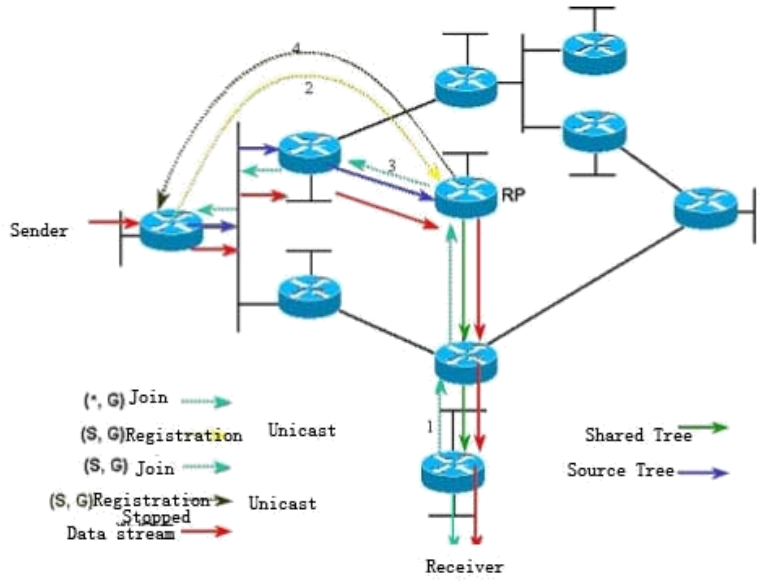


그림 5-1 PIM-SM 의 참여 방법

PIM-SM 은 Multicast 배포 트리를 만들어 Multicast 패킷을 전달합니다. Multicast 분포 트리는 공유 트리와 최단 경로 트리의 두 그룹으로 분류 할 수 있습니다. Shared Tree 는 그룹 G 의 RP 를 루트로 사용하고 Shortest Path Tree 는 Multicast
소스를 루트로 사용합니다. PIM-SM 은 표시된 join / prune 모드를 통해 Multicast
배포 트리를 만들고 유지 관리합니다. 그림 5-1 과 같이 DR 이 수신 측에서 Join 메시지를 수신하면 DR 은 그룹 B 의 RP 에 대한 각 홉에서 (*, G) - 가입 메시지
공유 트리에 가입시킵니다. 소스 호스트 Multicast 메시지를 그룹에 전송하면 소스 호스트의 패킷은 등록 메시지에 패키지화 되고 DR 에 의해 RP 에 Unicast 됩니다.

그런 다음 RP 는 소스 호스트의 패키지 되지 않은 패킷을 공유 트리를 따라 그룹 구성원에게 보냅니다. RP 는 소스의 최단 경로 트리에 참여하기 위해 (S, G) - 조인 메시지를 소스 방향으로 첫 번째 홉 스위치로 보냅니다. 이 방법으로 소스의 패킷은 패키징 되지 않고 최단 경로 트리를 따라 RP 로 전송됩니다. 첫 번째 Multicast 데이터가 도착하면 RP 는 등록 중지 메시지를 소스의 DR 에 보내고 DR 은 등록 패키지 프로세스를 중지합니다. 이후 소스의 Multicast 데이터는 더 이상 패키징 되지 않지만 소스의 최단 경로 세 개를 따라 RP 로 전송 된 다음 RP 가 공유 트리를 따라 각 그룹 멤버에게 전송합니다. Multicast 데이터가 필요하지 않은 경우 DR 은 Prune 메시지를 그룹 G 의 RP 를 향해 Multicast 하여 공유 트리를 제거합니다.

PIM-SM 은 RP 선택 방법도 인지합니다. 하나 이상의 후보 BSR 이 PIM-SM 도메인에서 구성됩니다. 특정 규정에 따라 후보 BSR 중에서 BSR 을 선택할 수 있습니다. 후보 RP 도 PIM-SM 도메인에서 구성됩니다. 이러한 후보 RP 는 RP 의 주소와 Multicast 그룹을 포함하는 패킷을 BSR 에 Uni-casting 합니다. BSR 은 일련의 후보 RP 및 대응하는 그룹 어드레스를 포함하는 부트스트랩 메시지를 규칙적으로 생성한다. 부트스트랩 메시지는 전체 도메인에서 홉 단위로 전송됩니다. 스위치는 부트스트랩 메시지를 수신하여 저장합니다. DR 이 직접 연결된 호스트와 그룹 구성원의 관계에 대한 보고서를 받은 후 DR 에 그룹의 라우팅 항목이 없으면 DR 은 해시 알고리즘을 통해 그룹 주소를 후보 RP 에 매핑합니다. 그런 다음 DR 은 Join / prune 메시지를 RP 쪽으로 호프별로 Multicast 합니다. 마지막으로, DR 은 등록 메시지에 Multicast 데이터를 패키징하고 이를 RP 에 Unicasting 합니다.

PIM-SM 구성하기

PIM-SM 시작하기

다음 명령을 실행하여 VLAN 인터페이스에서 PIM-SM 을 실행하여 sparse 모드에서 멀티 캐스트 기능을 활성화합니다.

명령어	설명
ip pim-sm	인터페이스 구성 모드에서 PIM-SM 멀티 캐스트 라우팅 프로세스를 인터페이스 활성화를 시작합니다.

BSR 구성하기

PIM-SM 도메인에서 경계 BSR 을 선언 할 수 있습니다.

VLAN 인터페이스 모드에서 다음 명령을 실행합니다.

명령어	설명
ip pim-sm bsr-border **no ip pim-sm bsr-border**	VLAN 인터페이스에 경계 BSR 을 선언한다.

PIM-SM Multicast 경로 표시

명령어	설명
show ip mroute pim-sm [*group-address*] [*source-address*] [**summary**]	다음 명령을 실행하여 PIM-SM 에서 학습 한 multicast 경로 정보를 확인합니다.

Multicast 라우트로 얻은 PIM-SM 지우기

다음 명령을 실행하여 PIM-SM 에서 학습 한 멀티 캐스트 경로를 지 웁니다.

명령어	설명
clear ip mroute pim-sm [* | group-address] [source-address]	PIN-SM 대한 정보에 대한 자세한 정보

구성 예제

PIM-SM 구성

예제 다음 예제는 두 개의 스위치가 PIM-SM 멀티 캐스트 경로를 학습하고 전달하는 방법을 보여줍니다.

스위치 A:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.166.100.142 255.255.255.0
ip pim-sm
ip rip 1 enable
!
interface vlan1
ip address 192.166.1.142 255.255.255.0
ip pim-sm
ip pim-sm dr-pri 100
ip rip 1 enable
!
interface vlan2
ip address 192.168.21.142 255.255.255.0
ip rip 1 enable
ip pim-sm
!
router rip 1
version 2
!
```

스위치 B:

```
!
ip multicast-routing
!
interface vlan1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
ip pim-sm dr-pri 200
!
interface vlan 2
```

ip address 192.168.21.144 255.255.255.0

ip pim-sm

!

BSR 구성 예(Vlan 포트에 구성하는 경우)

다음 예는 두 스위치의 BSR 구성을 보여줍니다..

스위치 A

!

ip multicast-routing

!

interface Loopback0

ip address 192.166.100.142 255.255.255.0

ip pim-sm

ip rip 1 enable

!

interface vlan1

ip address 192.166.1.142 255.255.255.0

ip pim-sm

!

interface vlan2

ip address 192.168.21.142 255.255.255.0

physical-layer speed 128000

ip pim-sm

ip rip 1 enable

!

router rip 1

!

스위치 B :

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.168.100.144 255.255.255.0
ip pim-sm
!
interface vlan1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
!
interface vlan2
ip address 192.168.21.144 255.255.255.0
ip pim-sm
```

IPv6 프로토콜 구성

IPv6 프로토콜 구성

라우터의 IPv6 주소 구성은 물리적 인터페이스가 아닌 VLAN 인터페이스에서만 적용됩니다.

IPv6 프로토콜은 기본 상태에서 사용할 수 없습니다. IPv6 프로토콜을 VLAN 인터페이스에서 사용해야하는 경우이 프로토콜은 먼저 VLAN 인터페이스 구성 모드에서 활성화해야합니다. IPv6 프로토콜을 사용하려면 사용자가 IPv6 주소를 구성해야합니다. VLAN 인터페이스에서 적어도 하나의 IPv6 주소가 구성되면 VLAN 인터페이스는 IPv6 패킷을 처리하고 다른 IPv6 장치와 통신할 수 있습니다.

IPv6 프로토콜을 사용하려면 사용자는 다음 작업을 완료해야합니다:

VLAN 인터페이스 구성 모드에서 적어도 하나의 IPv6 주소 구성하기

IPv6 활성화

IPv6 주소 구성

Pv6 주소는 IPv6 패킷을 보낼 수있는 대상 주소를 결정하는 데 사용됩니다. IPv6 주소에는 세 가지 종류가 있습니다.

종류	기본 형식	설명
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	2001 : 0 : 0 : 0 : 0DB8 : 800 : 200C : 417A 는 유니 캐스트 주소를 나타내고 64 는 이 주소의 접두사 길이를 나타냅니다..

Multicast address	FF01:0:0:0:0:0:0:101	모든 멀티 캐스트 주소는 FF 로 시작합니다..
Any address	2002:0:0:0:0DB8:800:200C:417A/64	이 주소의 형식은 유니 캐스트 주소의 형식과 동일합니다. 유니 캐스트 / 브로드 캐스트 / 멀티 캐스트 주소에 상관없이 서로 다른 VLAN 인터페이스가 동일한 주소를 갖도록 구성할 수 있습니다.

IPv6 주소에 대한 자세한 내용은 RFC 4291 을 참조하십시오.

IPv6 을 사용하려면 사용자가 VLAN 인터페이스 구성 모드에서 유니 캐스트 주소를

구성해야합니다. 구성된 유니 캐스트 주소는 다음 유형의 하나 또는 여러 주소 여야합니다:

IPv6 링크 로컬 주소

Global IPv6 주소

VLAN 인터페이스 구성 모드에서 IPv6 링크 - 로컬 주소를 구성하려면 다음 명령을

실행하십시오.

명령어	설명
ipv6 enable	링크 로컬 주소를 자동으로 구성합니다..
ipv6 address fe80::x link-local	링크 로컬 주소를 수동으로 구성합니다.

링크 로컬 주소는 fe80 으로 시작해야합니다. 접두어의 기본 길이는 64 비트입니다. 수동

구성에서 마지막 64 비트의 값만 지정할 수 있습니다.

VLAN 인터페이스에서 하나의 링크 로컬 주소 만 구성할 수 있습니다.

IPv6 가 링크 로컬 주소의 구성을 통해 활성화되면 IPv6 은 로컬 링크에서만 적용됩니다.

VLAN 인터페이스 모드에서 전역 IPv6 주소를 구성하려면 다음 명령을 실행하십시오.

명령어	설명
ipv6 address autoconfig	전역 주소를 자동으로 구성합니다.
ipv6 address [ipv6-address/prefix-length | prefix-name sub-bits/prefix-length] | [eui-64]	전체 주소 구성.

ipv6 address X:X:X:X::X/<0-128> anycast	유니/브로드/멀티캐스트 주소를 구성합니다.

전역 주소 구성을 통해 IPv6이 활성화되면, 상호 연결된 모든 IPv6 장비는 IPv6에 의해 처리 될 수 있습니다.

글로벌 주소를 구성하기 전에 링크 로컬 주소가 구성되어 있지 않으면, 시스템은 링크 로컬 주소를 자동으로 구성합니다.

IPv6 서비스 구성

IPv6 서비스 구성

IPv6 을 사용하도록 구성하면 IPv6 에서 제공하는 모든 서비스를 구성할 수 있습니다. 구성 가능한 IPv6 서비스는 아래와 같습니다:

IPv6 링크 관리

IPv6 링크 관리

IPv6 은 IPv6 링크를 제어하고 관리하기위한 일련의 서비스를 제공합니다. 이 일련의 서비스에는 다음이 포함됩니다.:

ICMPv6 패킷의 송신 주파수 구성

출발지 IPv6 경로 구성

IPv6 의 MTU 구성

IPv6 리디렉션 구성

IPv6 목적지 Unreachablity 구성

IPv6 ACL 구성

IPv6 Hop-Limit 구성

발신지 IPv6 경로 구성

IPv6 은 호스트가 IPv6 네트워크의 경로, 즉 소스 경로를 지정할 수있게합니다. 호스트는 IPv6 패킷의 라우팅 헤더를 사용하여 소스 경로를 구현할 수 있습니다. 라우터는 라우팅 헤더에 따라 패킷을 전달하거나 보안을 고려하여 이러한 종류의 패킷을 버릴 수 있습니다.

라우터는 기본적으로 소스 경로를 지원합니다. 원본 경로가 닫혀 있으면 사용자는 전역 구성 모드에서 다음 명령을 실행하여 원본 경로를 열 수 있습니다.

명령어	설명
ipv6 source-route	소스 IPv6 경로 허용.

IPv6 의 MTU 구성

모든 인터페이스에는 기본 IPv6 MTU 가 있습니다. IPv6 패킷의 길이가 MTU 를 초과하면 라우터는이 IPv6 패킷을 조각 낼 것입니다.

특정 인터페이스에서 IPv6 MTU 를 구성하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
ipv6 mtu *bytes*	인터페이스에 IPv6 MTU 를 구성합니다.

IPv6 리디렉션 구성

때때로 호스트가 선택한 경로가 최상의 경로가 아닙니다. 이 경우, 스위치가이 경로에서 패킷을 수신하면 스위치는 라우팅 테이블에 따라 패킷이 수신 된 인터페이스의 패킷을 전송하고 호스트와 동일한 네트워크 세그먼트에 속한 다른 라우터로 전달합니다. 이 상태에서 스위치는 스위치 자체를 통하지 않고 동일한 목적지 주소를 가진 패킷을 다른 라우터에 직접 전송한다는 것을 소스 호스트에 알립니다. 리디렉션 패킷은 원래 경로를 리디렉션 패킷에 포함 된보다 직접적인 경로로 바꾸도록 원본 호스트에 요구합니다. 많은 호스트의 운영

체제가 라우팅 테이블에 호스트 경로를 추가합니다. 그러나 스위치는 라우팅 프로토콜로부터 정보를 더 신뢰하므로 호스트 경로가이 정보에 따라 추가되지 않습니다.

IPv6 리디렉션은 기본적으로 열립니다. 그러나 인터페이스에 hot standby 라우터 프로토콜이 구성된 경우 IPv6 리디렉션은 자동으로 닫힙니다. hot standby 라우터 프로토콜이 취소되면이 기능은 자동으로 열리지 않습니다.

IPv6 리디렉션을 구성 하려면 다음 명령을 실행하십시오.:

명령어	설명
ipv6 redirects	IPv6 가 리디렉션 패킷을 전송할 수있게합니다.

IPv6 destination unreachablity 구성

대부분의 경우 시스템은 목적지에 도달 할 수없는 패킷을 자동으로 전송합니다. 사용자는이 기능을 닫을 수 있습니다. 이 기능이 닫히면 시스템은 ICMP 도달 할 수없는 패킷을 전송하지 않습니다.

이 기능을 사용하려면 다음 명령을 실행하십시오.:

명령어	설명
ipv6 unreachables	IPv6 가 목적지에 도달 할 수없는 패킷을 전송하도록 허용합니다.

IPv6 Hop-Limit 구성

사용자는 패킷에서 hop-limit 필드 값을 전송하도록 라우터를 지정할 수 있습니다 (전송 된 패킷을 제외). 이 라우터가 전송하는 모든 패킷, 상위 레벨 응용 프로그램이 hop-limit 값을

분명히 지정하지 않으면 hop-limit 의 구성 값을 사용하십시오. At the 동일한 시간에,이

라우터가 전송하는 RA 패킷에 hop-limit 필드의 값이 추가됩니다.

기본 hop-limit 값은 64 입니다.이 값을 변경하려면 인터페이스 구성 모드에서 다음 명령을

실행할 수 있습니다.

명령어	설명
ipv6 cur-hoplimit *value*	**패킷의 HOP-LIMIT 필드를 전송할 라우터를 지정합니다.**

ND 구성

ND 개요

노드 (호스트 및 라우터)는 ND (Neighbor Discovery Protocol)을 사용하여 결된 이웃의 링크 계층 주소를 확인하고 잘못된 캐시를 빠르게 삭제합니다. 또한 호스트는 이웃 라우터를 사용하여 패킷 전송 인접 라우터를 찾습니다. 추가적으로 노드는 ND 메커니즘을 사용하여 도달 가능한 또는 도달 할 수없는 이웃을 명확하게 추적하고 변경된 링크 계층 주소를 테스트합니다. 라우터 또는 라우터의 경로에 문제가 발생하면 호스트는 다른 라우터 또는 다른 경로를 찾는 중입니다..

IPv6 ND 는 IPv4 ARP, ICMP 라우터 검색 및 ICMP 리디렉션에 해당합니다.

ND 는 P2P, 멀티 캐스트, NBMA, 공유 미디어, 변경 가능한 MTU 및 비대칭 도달 기능과 같은 링크 유형을 지원합니다. ND 메커니즘은 다음과 같은 기능을합니다:

(1) To discover routers : 호스트가 연결된 링크에서 라우터를 찾는 방법.

(2) To discover prefixes: 호스트가 주소 그룹을 찾는 방법, 연결된 대상에서 어떤 대상이 온 링크인지 정의하는 방법.

(3) To discover parameters: 노드가 전송 인터페이스의 링크 관련 또는 네트워크 관련 매개 변수를 알 수있는 방법.

(4) To automatically set addresses: 노드가 인터페이스의 주소를 자동으로 구성하는 방법.

(5) Address solution: 목적지의 IP 가 주어질 때 노드가 링크 대상의 링크 계층 주소를 결정하는 방법.

(6) To determine the next hop: 목적지의 IP 주소를 인접 IP 에 매핑하는 알고리즘입니다. 다음 홉은 라우터 또는 대상이 될 수 있습니다.

(7) To test unreachable 도달 할 수없는 이웃을 결정하는 노드; 네이버가 라우터 인 경우 기본 라우터를 사용할 수 있습니다.

(8) To test repeated address: 사용되는 주소가 다른 노드에 의해 사용되지 않는지를 결정하는 노드.

(9) Redirect: 라우터가 최상의 다음 홉을 호스트에 알리는 방법.

주소 확인

주소 확인은 노드의 IP 를 통해 링크 계층 주소를 확인하는 절차입니다. ND 요청과 ND 알림을 통해 패킷 교환을 실현.

i. 정적 ND 캐시 구성

대부분의 경우 동적 주소 확인이 사용되며 정적 ND 캐시 구성은 필요하지 않습니다. 필요한 경우, 전역 모드에서 정적 ND 캐시를 구성할 수 있으며 시스템은이를 사용하여 IP 를 링크 계층 주소로 변환합니다. 다음 표는 정적 IP 대 링크 계층 주소 매핑을 구성하는 방법을 보여줍니다.

Global 모드에서 다음 명령을 실행하십시오.:

명령어	설명
ipv6 neighbor ipv6address **vlan** vlanid hardware-address	정적 ND 캐시를 구성하고 IPv6 주소를 링크 계층 주소로 변환합니다.

Nd 구성

ND 프로토콜은 주소 확인뿐만 아니라 인접 요청, 인접 광고, 라우터 요청, 라우터 광고 및 리디렉션과 같은 다른 기능에도 사용됩니다.

Global 모드에서 다음 명령을 실행하십시오.:

명령어	설명
ipv6 nd-redirect	Ipv6의 nd 프로토콜을 재전송합니다.
ipv6 nd-synchronize [**update-period** *synchronizing_period*] | [**response-immediately]** | [**request-immediately] | [deletion]**	nd 프로토콜의 동기화를 실행합니다.

RIPNG 구성

개요

차세대 라우팅 정보 프로토콜 RIPng 은 버전 6 의 RIP 입니다. 장비에서 RIPng 및 RIP 는 각각 버전 6 및 버전 4 의 라우팅 정보 학습 및 관리를 담당하는 두 개의 완전히 독립적 인 모듈입니다.

RIPng 은 내부 작업 메커니즘에서 RIP 와 동일합니다. RIPng 은 UDP 브로드 캐스트를 통해 라우팅 정보를 전환합니다. 라우터에서 라우팅 정보의 업데이트는 30 초마다 전송됩니다. 라우터가 180 초 내에 인접 라우터로부터 라우팅 업데이트를받지 못하면 라우터는 라우팅 테이블에서이 경로를 사용할 수 없음이라고 표시합니다. 그리고 120 초 후에이 라우터는 라우팅 테이블에서이 경로를 원격으로 제거합니다.

RIPng 은 소규모 네트워크에도 적용 할 수 있습니다. 다른 경로의 가중치를 측정하기 위해 홉 수를 사용합니다. 이 홉 수는 패킷이 신호 소스에서 다른 신호 소스로 통과 한 라우터의 수를 의미합니다. 직접 연결된 네트워크의 라우팅 가중치는 0 이고 도달 할 수없는 네트워크의 라우팅 가중치는 16 입니다.

RIPng 에서 사용하는 라우트 가중치가 작기 때문에 대규모 네트워크의 경우 적합하지 않습니다.

라우터에 기본 경로가있는 경우 RIPng 은 가짜 네트워크에 대한 경로를 0 :: 0/0 으로 선언합니다. 실제로 네트워크 0 :: 0/0 은 존재하지 않으며 RIPng 에서 기본 경로를 구현하는 데 사용됩니다. RIPng 이 기본 경로를 학습하거나 라우터가 기본 게이트웨이와 기본 가중치를 구성하면 라우터는 기본 네트워크를 선언합니다.

RIPng 은 라우트 업데이트를 인스턴스가 처리하는 인터페이스로 보냅니다. 인터페이스가 IPv6 인터페이스로 구성되지 않은 경우 RIPng 인스턴스로 덮어 쓰지 않습니다.

라우터의 RIPng 프로토콜은 여러 인스턴스를 지원합니다. 인터페이스에서 최대 4 개의 인스턴스를 구성할 수 있으며 하나의 인스턴스에서 최대 4 개의 인터페이스를 처리 할 수 있습니다.

RIPng 구성 작업 목록 구성

RIPng 을 구성하기 전에 다음 작업을 완료해야합니다. 이러한 작업 중에서 RIPng 을 활성화해야하지만 다른 작업에서는 실제 요구 사항에 따라 작업을 수행하도록 선택할 수 있습니다.

Unicast Routing Protocol 구성 허용

RIPng 활성화

RIPng 경로에 유니캐스팅 브로드캐스트 패킷 업데이트 허용

Routing Weight에 오프셋 적용

수신 또는 전송 된 경로 필터링

관리 범위 구성

타이머 조정

Unlocal Instance의 경로 재분배

수동으로 경로 요약

Maximum Number of Routes

Horizontal Fragmentation 활성화 또는 금지

RIPng 모니터링 및 유지 보수

RIPng 구성 작업

Unicast Routing Protocol 구성 허용

RIPng 을 구성하려면 먼저 다음 명령을 실행하여 유니 캐스트 경로의 스위치를 구성할 수 있어야합니다.

명령어	설명
Ipv6 unicast-routing	장치에 유니 캐스트 라우팅 프로토콜을 구성할 수 있습니다..

RIPng 활성화

RIPng 인스턴스를 활성화하려면 interface vlan 에서 다음 명령을 실행합니다:

명령어	설명
ipv6 rip *instance-name* **enable**	인터페이스에서 RIPng 사용 구성.

RIPng 인스턴스를 시작하려면 전역 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
router ripng *instance-name*	RIPng 인스턴스 및 해당 구성 모드로 들어갑니다.

Note: 사용자는 인터페이스에서 RIPng 인스턴스를 활성화 할 수 있습니다. RIPng 인스턴스가 없으면 RIPng 인스턴스가 생성됩니다. 시스템이 전역 구성 모드에서 RIPng 인스턴스에 직접 입력 할 수 있으며이 RIPng 인스턴스가없는 경우 RIPng 인스턴스가 생성됩니다. 사용자는 인터페이스에서 최대 4 개의 RIPng 인스턴스를 활성화 할 수 있으며 RIPng 인스턴스는 최대 4 개의 인터페이스를 커버 할 수 있습니다.

Unlocal Instance 의 경로 재분배

RIPng 은 로컬 인스턴스의 라우팅 정보 데이터베이스에 비 로컬 인스턴스의 라우팅 정보를 재배포 한 다음이 인스턴스의 라우팅 데이터베이스에있는 경로를 통해 다른 장치와의 라우팅 상호 작용을 수행합니다. 위의 목표를 달성하려면 RIPng 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
Redistribute *protocol [instance-name	process-id]*	고정 경로, 기타 ospfv6 프로세스 및 기타 RIPng 인스턴스를 재분배합니다..

RIPng 경로에 유니캐스팅 브로드캐스트 패킷 업데이트 허용

RIPng 은 일반적으로 멀티 캐스트 프로토콜입니다. RIPng 라우팅 업데이트가 비 브로드 캐스트 네트워크에 도달하도록하려면 라우팅 정보를 전환 할 수 있도록 라우터에서 구성해야합니다. 위의 목표를 달성하려면 RIPng 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
neighbor *ipv6-address*	이웃 라우터를 정의하고이 인접 라우터와 라우팅 정보를 전환합니다.

Routing Weight 에 오프셋 적용

오프셋 목록은 RIPng 에서 인식하는 수신 또는 발신 경로에 대한 오프셋을 추가하는 데 사용됩니다. 이 경우, routing weight 를 추가하기위한 로컬 메커니즘이 제공됩니다. 또한 액세스 목록이나 인터페이스를 사용하여 오프셋 목록을 제한 할 수도 있습니다. routing weight 를 추가하려면 RIPng 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
offset { [interface-type number]|* } {**in**|**out**} *access-list-name* offset *value*	routing weight에 오프셋을 추가합니다..

수신 또는 전송 된 경로 필터링

구성을 통해 RIPng 인스턴스는 해당 인터페이스에서 수신되거나 전송 된 라우트를 필터링 할 수 있으며 유연한 구성 정책을 유연하게 구현할 수 있습니다. RIPng 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
filter *interface-type interface-number* **{in | out}** access-list | gateway | prefix-list	수신 또는 전송 된 라우팅 정보를 필터링합니다.

관리 범위 구성

관리 범위를 구성하면 RIPng 인스턴스 경로의 신뢰성을 변경할 수 있습니다. 일반적으로 가치가 클수록 더 가치가 있습니다. 관리 범위를 구성하려면 RIPng 구성 모드에서 다음 명령을 실행하십시오.:

명령어	설명
distance *weight* [*X:X:X:X::X/*<0-128> [Acc-list_name]	RIPng 인스턴스 경로의 관리 거리를 구성합니다.

타이머 조정

라우팅 프로토콜은 라우팅 업데이트의 전송 빈도를 판단하는 데 몇 개의 타이머가 필요하며 라우트가 무효화되는 데 걸리는 시간이 필요합니다. 이러한 타이머를 조정하여 라우팅 프로토콜의 성능을 네트워크 상호 연결 요구 사항에보다 적합하게 만들 수 있습니다.

또한 라우팅 프로토콜을 조정하여 IPv6 알고리즘의 컨버전스 시간을 단축하고 중복 라우터를 신속하게 백업 할 수 있으므로 빠른 복구가 필요할 때 터미널 사용자가 최대한 중단 될 수 있습니다. 타이머를 조정하려면 RIPng 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
timers holddown *value*	경로가 라우팅 테이블에서 제거되는 데 걸리는 시간을 의미합니다.
timers garbage *value*	경로가 유효하지 않은 것으로 선언되는 데 걸리는 시간을 의미합니다.
timers update *value*	라우팅 업데이트의 전송 빈도를 의미하며 그 단위는 초입니다.

수동으로 경로 요약

RIPng 은 라우팅 정보를 수동으로 요약하여 이웃 라우터와 상호 작용하는 경로 수를 줄여야합니다. 라우팅 정보를 요약하려면 RIPng 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
aggregate-address *ipv6-prefix/prefixlen*	라우팅 정보를 요약합니다..

Horizontal Fragmentation 활성화 또는 금지

일반적으로 브로드 캐스트 IPv6 네트워크를 연결하고 거리 벡터 라우팅 프로토콜을 사용하는 라우터는 경로 단 루프의 가능성을 줄이기 위해 수평 단편화를 사용합니다. 수평 분할은이 라우팅 정보를 수신하는 인터페이스에 라우팅 정보가 선언되는 것을 차단합니다. 이러한 방식으로 여러 라우터 간의 통신을 최적화 할 수 있습니다 (특히 루프백이 끊어진 경우). 그러나이 솔루션은 un-broadcast 네트워크에 좋지 않습니다. 이 네트워크에서는 horizontal fragmentation 을 금지해야합니다.

horizontal fragmentation 을 활성화 또는 비활성화하려면 VLAN 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
Ipv6 rip split-horizon	수평 분할을 활성화합니다.
no ipv6 rip split-horizon	수평 분할을 금지.

기본적으로 수평 단편화는 해당 지점 간 인터페이스에서 활성화되고 해당 지점 간 인터페이스에서 금지됩니다.

메모:

일반적인 경우 응용 프로그램 상태가 변경된 후에 경로가 올바르게 선언 될 수 없다면 기본 상태를 변경하지 않는 것이 좋습니다. 패킷 교환망을 연결하는 직렬 인터페이스에서 수평 분할이 금지 된 경우 네트워크상의 모든 관련 멀티 캐스트 그룹의 라우터에서 수평 분할을 비활성화해야합니다.

RIPng 모니터링 및 유지 보수

RIPng 의 모니터링 및 유지 관리를 통해 RIPng 의 매개 변수, 네트워크 사용 정보 및 실제 통신 추적 정보를 포함하여 네트워크의 통계 정보를 얻을 수 있습니다. 이러한 종류의 정보는 사용자가 네트워크 리소스

사용을 판단하고 네트워크 문제를 해결하는 데 도움이 될 수 있습니다. 통계 정보에서 네트워크 노드의 도달 가능성을 알 수 있습니다.

모든 종류의 통계 정보를 표시하려면 EXEC 모드에서 다음 명령을 실행하십시오:

명령어	설명
show ipv6 rip *process-id* **summary**	RIPng 인스턴스에 대한 전체 라우팅 정보를 표시합니다..
show ipv6 rip *iprocess-id* **database**	RIPng 인스턴스의 모든 경로를 표시합니다.
show ipv6 rip *process-id* **interface**	RIPng 인스턴스가 포함하는 모든 인터페이스를 표시합니다.

라우팅 프로토콜에 대한 정보를 추적하려면 EXEC 모드에서 다음 명령을 실행하십시오:

명령어	설명
debug ipv6 rip database	라우팅 테이블에서 RIPng 인스턴스의 경로가 추가, 제거 또는 변경되었음을 추적합니다..
debug ipv6 rip event	RIPng 인스턴스 실행 및 RIPng 인스턴스 재분배 프로세스에서 발생하는 비정상을 추적합니다.
debug ipv6 rip send	RIPng 인스턴스가 패킷을 전송하는 프로세스를 추적합니다.
debug ipv6 rip recv	RIPng 인스턴스가 패킷을받는 프로세스를 추적합니다.
debug ipv6 rip msg	RIPng 인스턴스의 시작 종료로 이어지는 중요한 이벤트를 추적합니다.
debug ipv6 rip all	RIPng 인스턴스에 대한 모든 정보를 추적합니다.

RIPng 구성 예

RIPng 구성 예제:

장치 A 와 장치 B 를 직접 연결하고 다음과 같이 구성합니다:

장치 A:

```
interface VLAN2
 no ip address
 no ip directed-broadcast
 ipv6 address 4444::4444/64
 ipv6 enable
 ipv6 rip 2 enable
 ipv6 rip 2 split-horizon
!
router ripng 2
                redistribute static
 exit
!
```

장치 B:

```
interface vlan 2
 no ip address
 no ip directed-broadcast

                ipv6 address 4444::2222/64
 ipv6 enable
 ipv6 rip 1 enable
 ipv6 rip 1 split-horizon
!
router ripng 1
 redistribute static
 exit
!
```

이러한 방식으로 장치 A 와 장치 B 는 서로 정적 라우팅 정보를 학습합니다.

OSPFv3 구성

개요

OSPFv3 은 IPv6 네트워크를 위해 IETF 의 OSPF 워킹 그룹에 의해 개발 된 IGP 라우팅 프로토콜입니다.

OSPFv3 은 IPv6 서브넷, 외부 라우팅 정보의 표시 및 패킷의 인증을 지원합니다.

OSPFv3 와 OSPFv2 는 많은 공통점이 있습니다:

- Router-ID 와 area-ID 는 모두 32 비트입니다..
- 다음은 동일한 패킷 유형입니다 : Hello 패킷, DD 패킷, LSR 패킷, LSU 패킷 및 LSAck 패킷.
- 같은 이웃 탐색 메커니즘과 같은 이웃 생성 메커니즘을 가짐
- 동일한 LSA 확장 메커니즘과 동일한 LSA 에이징 메커니즘

OSPFv3 과 OSPFv2 의 주요 차이점은 아래와 같습니다:

- OSPFv3 는 링크 기반으로 실행되고 OSPFv2 는 네트워크 세그먼트를 기반으로 실행됩니다.
- OSPFv3 는 동일한 링크에서 여러 인스턴스를 실행할 수 있습니다.
- OSPFv3 은 라우터 ID 를 통해 인접 라우터에 레이블을 지정하고 OSPFv2 는 IP 를 통해 인접 라우터를 레이블링합니다.
- OSPFv3 는 7 가지 클래스의 LSA 를 정의합니다.

다음 표는 OSPFv3 기능 구현에 필요한 몇 가지 주요 기능을 보여줍니다..

주요 속성	설명
Stub domain	스텁 도메인 지원.
Route forwarding	모든 라우팅 프로토콜에 의해 학습되거나 생성 된 경로가 다른 라우팅 프로토콜의 도메인으로 전달 될 수 있음을 의미합니다. 자율 도메인에서 OSPFv3이 RIPng 학습 경로를 입력 할 수 있음을 의미합니다. OSPFv3에서 습득 한 경로는 RIPng으로 내보낼 수도 있습니다. 자치 도메인간에 OSPFv3은 BGP 학습 경로를 가져올 수 있습니다. BGP에 OSPFv3 경로를 내보낼 수도 있습니다.

Parameters of a routing interface	다음은 구성 가능한 인터페이스 매개 변수입니다. 출력 비용, 재전송 간격, 인터페이스의 전송 지연, 라우터의 우선 순위, hello interval 및 인증 키에 대한 라우터의 shutdown 판단 간격
Virtual link	가상 링크 지원.

OSPFv3 구성 작업 목록

OSPFv3 은 도메인 내 라우터, ABR 및 ASBR 간에 라우팅 데이터의 전환을 요구합니다. 구성을 단순화하기 위해 관련 구성을 만들어 인증없이 기본 매개 변수로 작동하도록 할 수 있습니다. 일부 매개 변수를 변경하려면 모든 라우터의 매개 변수가 동일 함을 보장해야합니다.

OSPFv3 을 구성하려면 다음 작업을 수행해야합니다. OSPFv3 을 활성화하는 작업이 필수 항목이 아니라는 점을 제외하면 다른 구성은 선택 사항입니다..

- OSPFv3 활성화
- OSPFv3 인터페이스의 매개 변수 구성
- 다른 네트워크에서 OSPFv3 구성
- OSPFv3 도메인의 매개 변수 구성
- OSPFv3 의 NSSA 도메인 구성
- OSPFv3 도메인에서 경로 요약 구성
- 경로 요약 구성
- 기본 경로 생성
- 루프백 인터페이스에서 경로 ID 선택하기
- OSPFv3 의 management distance 구성
- 라우팅 알고리즘 타이머 구성하기
- OSPFv3 모니터링 및 유지 보수

OSPFv3 구성 작업

OSPFv3 활성화

OSPFv3 을 활성화하기 전에 IPv6 패킷을 전달하는 기능을 활성화해야합니다.

전역 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
router ospfv3 *process-id*	OSPFv3을 활성화하고 라우터 구성 모드로 들어갑니다.
router-id *router-id*	OSPFv3이 실행되는 라우터의 라우터 ID를 구성합니다.

인터페이스 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
ipv6 ospf *process-id* **area** *area-id* **[instance** *instance-id***]**	인터페이스에서 OSPFv3을 사용하도록 구성합니다.

메모: 인터페이스에서 OSPFv3 을 활성화하기 전에 OSPFv3 프로세스가 아직 생성되지 않은 경우 OSPFv3 프로세스가 자동으로 생성됩니다.

OSPFv3 인터페이스의 매개 변수 구성

OSPFv3 실현 중에 인터페이스의 관련 OSPFv3 매개 변수는 실제 요구 사항에 따라 수정 될 수 있습니다. 모든 매개 변수를 변경할 필요가 없지만 일부 매개 변수가 연결된 네트워크의 모든 라우터에서 일관성을 유지하는지 확인해야합니다.

관련 구성을 수행하려면 인터페이스 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
ipv6 ospf cost *cost*	OSPFv3 인터페이스에서 전송되는 패킷의 비용을 구성합니다..
ipv6 ospf retransmit-interval *seconds*	이웃 사이의 LSA 재전송 간격을 구성합니다..

ipv6 ospf transmit-delay *seconds*	OSPFv3 인터페이스에서 LSA를 전송하기위한 지연 시간을 구성합니다..
ipv6 ospf priority *number*	라우터를 OSPFv3 DR 라우터의 우선 순위로 구성합니다..
ipv6 ospf hello-interval *seconds*	Hello 패킷을 전송할 OSPFv3 인터페이스의 간격을 구성합니다..
ipv6 ospf dead-interval *seconds*	OSPFv3 패킷이 인접 라우터로부터 수신되지 않은 경우 규제 된 간격으로이 인접 라우터가 종료 된 것으로 간주됨을 의미합니다.

다른 네트워크에서 OSPFv3 구성

OSPFv3 은 물리적 네트워크 미디어를 다음 세 가지 종류로 나눕니다:

- 브로드 캐스트 네트워크(Ethernet, Token Ring, FDDI)
- 논 브로드 캐스트 및 멀티 액세스 네트워크(SMDS, Frame Relay, X.25)
- Point-to-point 네트워크 (HDLC, PPP)

OSPF 네트워크 유형 구성

네트워크가 어떤 물리적 미디어 유형이든 상관없이 브로드 캐스트 네트워크, 논 브로드 캐스트 네트워크 또는 멀티 액세스 네트워크로 네트워크를 구성 할 수 있습니다. 따라서 네트워크를 유연하게 구성하고 네트워크를 논 브로드 캐스트 및 멀티 액세스 또는 X.25, 프레임 릴레이 또는 SMDS 네트워크와 같은 브로드 캐스트 네트워크로 구성할 수 있습니다. 또한 이웃의 구성이 단순화됩니다..

논 브로드 캐스트 및 멀티 액세스 네트워크를 구성하려면 두 개의 라우터마다 가상 링크가 있거나 full-mesh 네트워크가 있다고 가정해야합니다. 물론 가상이므로 네트워크를 다수 vs 하나의 네트워크로 구성합니다. 인접하지 않은 라우터 사이에서 라우팅 정보는 가상링크를 통해 전환 될 수 있습니다.

OSPFv3 point-to-multipoint 인터페이스는 호스트의 여러 경로를 구성할 수있는 multipoint-to-point 인터페이스로 구성할 수 있습니다: 논 브로드 캐스트 와 다중접근 네트워크 또는 점대점 네트워크는 다음과 같은 이점이 있습니다.

- point-to-multipoint 네트워크는 DR 을 생성하지 않고 구성하기 쉽습니다..
- 이러한 종류의 네트워크는 전체 메시 토폴로지를 필요로하지 않으므로 건설 비용이 상대적으로 낮습니다.
- 이러한 종류의 네트워크는보다 안정적입니다. 가상 링크가 실패하더라도 연결을 유지할 수 있습니다..

라우터의 네트워크 유형은 브로드 캐스트 유형입니다.

OSPFv3 도메인의 매개 변수 구성

구성 가능한 도메인 매개 변수에는 인증, 스텁 영역 지정 및 기본 요약 라우트에 대한 가중치 지정이 포함됩니다. 인증은 암호 보호를 기반으로합니다..

스텁 영역은 외부 경로를이 영역에 배포 할 수 없음을 의미합니다. 대신 ABR 은 스텁 영역에 들어가는 기본 외부 경로를 생성하여 스텁 영역이 자치 영역의 외부 네트워크와 통신 할 수있게합니다. OSPF 스텁에서 지원하는 속성을 사용하려면 스텁 영역에서 기본 경로를 사용해야합니다. 스텁 영역으로 전달되는 LSAs 를 추가로 줄이려면 ABR 에 대한 요약 기능을 금지 할 수 있습니다.

라우터 구성 모드에서 다음 명령을 실행하여 도메인 매개 변수를 구성하십시오:

명령어	설명
area *area-id* **stub** [no-summary]	스텁 영역을 정의합니다..
area *area-id* **default-cost** *cost*	스텁 영역의 기본 경로의 Cost를 구성합니다..

백본 영역이 아니고 백본 영역을 직접 또는 불연속 영역에 연결하지 않는 영역에 대해서는 OSPFv3 가상 링크를 사용하여 논리 연결을 구성할 수 있습니다. 가상 링크를 만들려면 가상 링크의 두 터미널에서 구성을 수행해야합니다. 하나의 터미널 만 구성되어 있으면 가상 링크가 작동하지 않습니다.

라우터 구성 모드에서 다음 명령을 실행하여 도메인 매개 변수를 구성하십시오:

명령어	설명
area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*]	가상 링크를 구성합니다.

OSPFv3 도메인에서 경로 요약 구성

이 기능을 사용하면 ABR 은 다른 지역으로 요약 경로를 브로드 캐스트 할 수 있습니다. OSPFv3 에서 ABR 은 각 네트워크를 다른 영역으로 브로드 캐스트합니다. 네트워크 ID 가 연속적으로 배포되면 요약 경로를 다른 영역에 브로드 캐스트하도록 ABR 을 구성할 수 있습니다. 요약 경로는 특정 범위의 모든 네트워크를 포괄 할 수 있습니다.

라우터 구성 모드에서 다음 명령을 실행하여 주소의 범위를 구성하십시오:

명령어	설명
area *area-id* **range** *ipv6-prefix /prefix-length* **[advertise | not-advertise]**	주소의 요약 경로 범위를 구성합니다.

경로 요약 구성

경로가 다른 라우팅 영역에서 OSPFv3 라우팅 영역으로 분산되면 각 경로가 외부 LSA 로 단독으로 브로드 캐스트됩니다. 그러나 라우터에서이 라우트가 주소 범위를 포함하도록 라우트를 구성할 수 있습니다. 이러한 방식으로 OSPFv3 연결 상태 데이터베이스의 크기를 줄일 수 있습니다.

라우터 구성 모드에서 다음 명령을 실행하여 요약 경로를 구성하십시오:

명령어	설명
summary-prefix *ipv6-prefix /prefix-length*	하나의 요약 경로 만 브로드 캐스트합니다.

기본 경로 생성

ASBR 은 OSPFv3 라우팅 영역에 들어가기 위해 기본 경로를 생성해야합니다. 그럴 때마다 라우터가 OSPFv3 라우팅 영역에 라우트를 배포 할 수 있도록 구성하고이 라우트는 자동으로 ASBR 이됩니다. 그러나 ASBR 은 기본적으로 OSPFv3 라우팅 영역에 들어가기 위해 기본 경로를 생성하지 않습니다.

루프백 인터페이스에서 경로 ID 선택하기

OSPFv3 은 라우터 ID 로 최대 IPv4 주소를 사용합니다. IPv4 주소를 연결하는 인터페이스가 다운되거나 IPv4 주소가 삭제되면 OSPF 프로세스는이 새 라우터의 ID 를 다시 계산하고 모든 인터페이스에서 라우팅 정보를 다시 전송합니다.

루프백 인터페이스에 IPv4 주소가 구성된 경우 라우터는 먼저 루프백의 IPv4 주소를 ID 로 사용합니다. 루프백 인터페이스가 절대로 다운되지 않으므로 라우팅 테이블이 크게 안정적입니다.

라우터는 먼저 ID 로 루프백 인터페이스를 선택하거나 모든 루프백 인터페이스에서 최대 IPv4 주소를 ID 로 선택할 수 있습니다. 루프백 인터페이스가 없으면 라우터의 IPv4 주소가 라우터 ID 로 사용됩니다. 특정 인터페이스를 사용하기 위해 OSPFv3 을 지정할 수 없습니다.

IP 루프백 인터페이스를 구성하려면 글로벌 구성 모드에서 다음 명령을 실행하십시오:

명령어	설명
interface loopback *num*	루프백 인터페이스를 생성하고 인터페이스 구성 모드를 시작합니다.
ip address *ip-address mask*	인터페이스에 IPv4 주소를 배포합니다.

OSPFv3 의 Management Distance 구성

Management Distance 는 라우팅 정보 소스의 신뢰 수준을 의미합니다. 일반적으로 Management Distance 는 0 에서 255 사이의 정수입니다. 값이 클수록 신뢰 수준은 낮아집니다. Management Distance 가 255 인 경우 라우팅 정보 소스는 신뢰할 수없고 생략됩니다..

OSPFv3 은 세 가지 종류의 Management Distance, 즉 도메인 간, 내부 도메인 및 외부를 사용합니다. 도메인의 경로를 내부 도메인 경로라고합니다. 다른 도메인에 대한 경로를 도메인 간 경로라고합니다. 다른 라우팅 프로토콜에서 전송 된 경로를 외부 경로라고합니다. 각 종류의 경로의 기본값은 110 입니다..

라우팅 알고리즘의 타이머 구성

토폴로지 변경 정보를 받고 SPF 를 계산할 때까지 지연을 구성할 수 있습니다. 두 개의 연속적인 SFP 알고리즘 사이의 간격을 구성할 수도 있습니다.

라우터 구성 모드에서 다음 명령을 실행하십시오.:

명령어	설명
timers delay *delaytime*	area에서 라우팅 알고리즘에 대한 지연 구성.
timers hold *holdtime*	영역에서 라우팅 알고리즘의 최소 간격을 구성합니다.

OSPFv3 모니터링 및 유지 관리

표시 할 수있는 네트워크 통계 정보에는 IP 라우팅 테이블의 내용, 캐싱 및 데이터베이스가 포함됩니다. 이러한 종류의 정보는 사용자가 네트워크 리소스 사용을 판단하고 네트워크 문제를 해결하는 데 도움이 될 수 있습니다.

다음 명령을 실행하여 모든 종류의 라우팅 통계 정보를 표시 할 수 있습니다:

명령어	설명

show ipv6 ospf [*process-id*]	OSPFv3 라우팅 프로세스에 대한 일반 정보를 표시합니다..
show ipv6 ospf [*process-id*] **database** **show ipv6 ospf** [*process-id*] **database [router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [network] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-prefix] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [external] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [link] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [intra-prefix] [adv-router** *router-id***]**	OSPFv3 데이터베이스에 대한 정보를 표시합니다.
show ipv6 ospf interface	OSPFv3 인터페이스에 대한 정보를 표시합니다.
show ipv6 ospf neighbor	OSPFv3 인접 항목에 대한 정보를 표시합니다.
show ipv6 ospf route	OSPFv3에 대한 라우팅 정보를 표시합니다.
show ipv6 ospf topology	OSPFv3 토폴로지를 표시합니다.
show ipv6 ospf virtual-links	OSPFv3의 가상 링크를 표시합니다.
debug ipv6 ospf	모든 OSPFv3 동작을 모니터링합니다.
debug ipv6 ospf events	OSPFv3 이벤트를 모니터합니다.
debug ipv6 ospf ifsm	OSPFv3 인터페이스의 상태 시스템을 모니터합니다.
debug ipv6 ospf lsa	OSPFv3 LSA에 대한 관련 동작을 모니터링합니다.
debug ipv6 ospf nfsm	OSPFv3 인접 장치의 상태 시스템을 모니터링합니다.
debug ipv6 ospf nsm	관리 모듈이 OSPFv3에 알리는 정보를 모니터합니다.
debug ipv6 ospf packet	OSPFv3 패킷을 모니터합니다.
debug ipv6 ospf route	OSPFv3에 대한 라우팅 정보를 모니터합니다.

OSPFv3 구성 예

OSPFv3 경로 학습 구성의 예

OSPFv3 은 많은 내부 라우터, ABR 및 ASBR 간에 정보를 전환해야합니다. 최소 구성에서 OSPFv3 기반 라우터는 모든 매개 변수가 기본값을 사용하고 인증이없는 경우에 작동합니다.

다음은 네 가지 구성 예제입니다.:

첫 번째 예는 기본 OSPFv3 구성에 대한 명령을 보여줍니다.

두 번째 예는 라우터에 여러 개의 OSPFv3 프로세스를 구성할 수 있음을 보여줍니다.

세 번째 예에서는 OSPFv3 을 사용하여 경로를 확인하는 방법을 보여줍니다.

네 번째 예는 OSPFv3 가상 링크를 구성하는 방법을 보여줍니다.

기본 OSPFv3 구성 예

다음 예는 간단한 OSPFv3 구성을 보여줍니다. 이 예에서는 프로세스 90 을 활성화하고 이더넷 인터페이스 0 을 영역 0.0.0.0 에 연결하고 RIPng 을 OSPFv3 에 배포하고 OSPFv3 을 RIPng 에 배포해야합니다.

```
ipv6 unicast-routing
!
interface vlan 10
ipv6 address 2001::1/64
ipv6 enable
ipv6 rip 1 enable
ipv6 rip 1 split-horizon

ipv6 ospf 90 area 0
ipv6 ospf cost 1
!
router ospfv3 90
router-id 1.1.1.1
```

```
redistribute rip 1
!
router ripng 100
redistribute ospf 90
```

Multiple OSPFv3 프로세스 구성

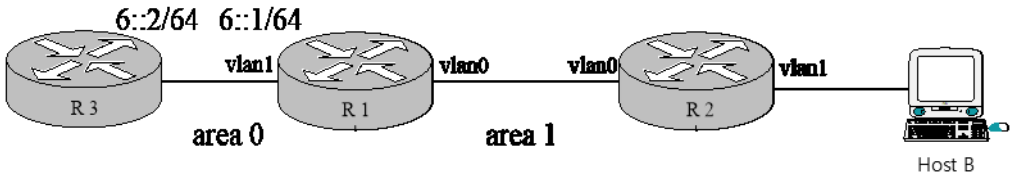
The following example shows that two OSPFv3 processes are created.

```
ipv6 unicast-routing
!
!
interface vlan 10
  ipv6 address 2001::1/64
  ipv6 enable

  ipv6 ospf 109 area 0 instance 1
  ipv6 ospf 110 area 0 instance 2
!
!
interface vlan 11
  ip address 2002::1/64
  ipv6 enable

 ipv6 ospf 109 area 1 instance 1
 ipv6 ospf 110 area 1 instance 2
!
!
router ospfv3 109
  router-id 1.1.1.1
  redistribute static
!
router ospfv3 110
  router-id 2.2.2.2
!
```

각 인터페이스는 여러 OSPFv3 프로세스에 속할 수 있지만 인터페이스가 여러 OSPFv3 프로세스에 속한 경우 각 OSPFv3 프로세스는 서로 다른 인스턴스에 해당해야합니다.

실 구성 예

다음 예는 단일 OSPFv3 자율 시스템에 여러 라우터를 구성하는 방법을 보여줍니다. 다음 그림은 구성 예에 대한 네트워크 토폴로지를 보여줍니다:



위에서 설명한 그림에 따라 라우터를 구성하십시오:

```
R1 :
interface vlan 10
   ipv6 enable

       ipv6 ospf 1 area 1
!
interface vlan 10
   ipv6 enable
       ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
  router-id 1.1.1.1
       redistribute static
!

R2 :
interface vlan 10
```

```
 ipv6 enable

    ipv6 ospf 1 area 1
!
!
router ospfv3 1
  router-id 2.2.2.2
!
```

Browsing the routing table of R2:

```
R2#show ipv6 route
O       6::/64[1]
        [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)
O       2001::/64[1]
        [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)
C       fe80::/10[1]
        is directly connected, L,Null0
C       fe80::/64[1]
        is directly connected, C, VLAN10
C       fe80::2e0:fff:fe26:a8/128[1]
        is directly connected, L, VLAN10
C       ff00::/8[1]
        is directly connected, L,Null0
```

위의 명령 문장에서 R2 가 경로 전달을 학습했다는 것을 알 수 있습니다.

Area 1 을 스텁 영역으로 구성:

```
R1 :
interface vlan 10
 ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
 ipv6 enable
```

```
        ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
  router-id 1.1.1.1
  area 1 stub
        redistribute static
!
```

R2 :

```
interface vlan 10
   ipv6 enable

        ipv6 ospf 1 area 1
!
!
router ospfv3 1
  router-id 2.2.2.2
  area 1 stub
!
```

R2 의 라우팅 테이블:

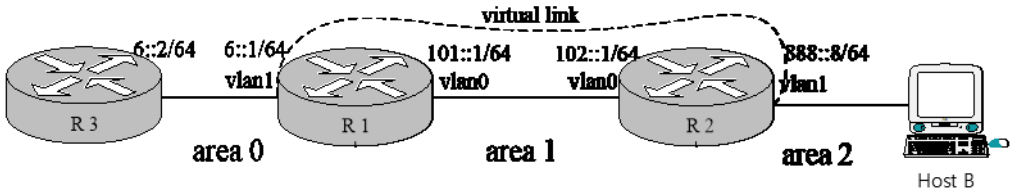
```
R2#show ipv6 route
O       ::/0[1]
        [110,11] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)
O       6::/64[1]
        [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)
C       fe80::/10[1]
        is directly connected, L,Null0
C       fe80::/64[1]
        is directly connected, C, VLAN10
C       fe80::2e0:fff:fe26:a8/128[1]
        is directly connected, L, VLAN10
C       ff00::/8[1]
```

is directly connected, L,Null0

스텁 영역의 ABR 이 기본 경로를 정상적으로 생성하고 ASE LSA 를 스텁 영역으로 가져 오지 않고이 영역의 다른 라우터에 알릴 수 있다고 판단 할 수 있습니다.

가상 링크 구성

다음 예제에서는 단일 자율 OSPFv3 시스템에서 가상 링크를 구성하는 방법을 보여줍니다. 다음 그림은 구성 예에 대한 네트워크 토폴로지를 보여줍니다:



그림에 따라 라우터를 구성하십시오.:

R1 :

```
interface vlan 10
        ipv6 address 101::1/64
    ipv6 enable

        ipv6 ospf 1 area 1
!
interface vlan 1
        ipv6 address 6::1/64
    ipv6 enable

        ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
  router-id 200.200.200.1
  area 1 virtual-link 200.200.200.2
```

```
  redistribute static
!

R2 :
interface vlan 10
        ipv6 address 101::2/64
    ipv6 enable

        ipv6 ospf 1 area 1
!
interface vlan 1
        ipv6 address 888::8/64
    ipv6 enable

        ipv6 ospf 1 area 2
!
!
router ospfv3 1
 router-id 200.200.200.2
 area 1 virtual-link 200.200.200.1
!

OSPFv3 네이버의 상태:
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
200.200.200.2      1   Full/DR         00:00:35    VLAN10       0
200.200.200.2      1   Full/ -         00:00:36    VLINK1       0

R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
200.200.200.1      1   Full/Backup     00:00:36    VLAN10       0
200.200.200.1      1   Full/ -         00:00:37    VLINK1       0
```

각 라우터의 라우팅 테이블:

R1#show ipv6 route

C 6::/64[1]

is directly connected, C,VLAN1

C 6::1/128[1]

is directly connected, L, VLAN1

C 101::/64[2]

is directly connected, C, VLAN10

C 101::1/128[2]

is directly connected, L, VLAN10

O 101::2/128[2]

[110,10] via fe80:4::2e0:fff:fe26:a8(on VLAN10)

O 888::/64[2]

[110,20] via fe80:4::2e0:fff:fe26:a8(on VLAN10)

S 2001::/64[1]

[1,0] via 6::2(on VLAN1)

C fe80::/10[2]

is directly connected, L,Null0

C fe80::/64[2]

is directly connected, C, VLAN10

C fe80::2e0:fff:fe26:2d98/128[2]

is directly connected, L, VLAN10

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:2d99/128[1]

is directly connected, L, VLAN1

C ff00::/8[2]

is directly connected, L,Null0

R2#show ipv6 route

O 6::/64[1]

[110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)

C 101::/64[1]

is directly connected, C, VLAN10

O 101::1/128[1]

[110,10] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)

C 101::2/128[1]

is directly connected, L, VLAN10

C 888::/64[1]

is directly connected, C, VLAN1

C 888::8/128[1]

is directly connected, L, VLAN1

O 2001::/64[1]

[110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN10)

C fe80::/10[1]

is directly connected, L,Null0

C fe80::/64[1]

is directly connected, C, VLAN10

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN10

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:a9/128[1]

is directly connected, L, VLAN1

C ff00::/8[1]

is directly connected, L,Null0

BFD 구성

개요

BFD (Bidirectional Forwarding Detection)는 링크 또는 IP 라우팅 포워딩 연결을 신속하게 탐지하고 모니터링하는 데 사용되는 모든 네트워크 균일 탐지 메커니즘 세트입니다. 기존 네트워크의 성능을 향상시키기 위해 인접 프로토콜 간 통신 장애를 빠르게 감지하여 대기 통신 채널을 신속하게 구축 할 수 있습니다.

BFD 는 두 시스템 간의 세션을 구성하여 두 시스템 간의 양방향 전달 경로를 모니터하고 상위 레벨 프로토콜을 제공 할 수 있습니다. 제공된 상위 레벨 프로토콜은 세션이 구성된 BFD 에 통보합니다. 세 핸드 쉐이크 메커니즘을 통해 세션이 구성된 후 탐지 시간 내에 피어로부터 BFD 제어 패킷을 수신하지 못하거나 허용 된 임계 값을 초과하는 손실 된 에코 패킷 수가 문제를 일으 킵니다. 그런 다음이 사례는 해당 처리를 위해 상위 프로토콜로보고됩니다.

BFD 구성 작업

Port BFD 활성화

Port BFD 는 기본적으로 활성화되지 않습니다.

Port BFD 가 활성화되면 동적 프로토콜을 통해 구성된 BFD 가 적용됩니다.

다음 명령어을 실행하여 BFD 를 활성화 하십시오:

명령어	설명
Interface vlan *vlan-id*	VLAN 구성 모드를 시작합니다
bfd enable <cr> | min_tx <tx_value> min_rx <rx_value> multiplier <m_value>]	BFD 포트를 활성화합니다.

BFD 세션이 구성되기 전에 BFD 제어 패킷은 1 초 이상의 간격으로 전송되어 트래픽을 줄입니다. 세션이 확립된 후, BFD 제어 패킷은 협상 된 간격으로 전송되어 신속한 검출을 실현한다. BFD 세션의 구성 동안, BFD 제어 패킷의 전송 간격 및 검출 시간은 또한 패킷 교환을 통해 결정된다. 효과적인 BFD 세션에서이 타이머는 세션 상태에 영향을주지 않고 언제든지 협상을 통해 수정할 수 있습니다. 서로 다른 BFD 세션 방향에서의 타이머 협상은 독립적으로 수행되며 양방향 타이머는 다를 수 있습니다. BFD 제어 패킷의 전송 간격은 로컬 min_tx_interval 과 피어 min_rx_interval 사이의 최대 값입니다. 즉, 비교적 느린 부분이 전송 빈도를 결정합니다.

탐지 시간은 피어 BFD 제어 패킷에서 피어 BFD 제어 패킷의 협상 된 전송 간격을 곱한 다중 탐지입니다. 로컬 엔드의 min_tx_interval 을 늘리면 로컬 엔드에서 BFD 제어 패킷의 실제 전송 간격은 피어의 F 필드로 재구성 된 패킷을 수신 할 때까지 수정할 수 없으므로 증가하기 전에 감지 시간이 피어에서 길어지도록합니다 국부적 인 끝에 BFD 통제 소포의 전송 간격의. 그렇지 않으면 피어의 검색 타이머가 시간 초과 될 수 있습니다.

로컬 엔드에서 min_rx_interval 이 감소하면 피어의 F 필드에 의해 재구성 된 패킷을 수신 할 때까지 로컬 탐지 시간을 수정할 수 없으므로 피어에서 BFD 제어 패킷의 전송 간격이 로컬 탐지가 감소하기 전에 감소 된 것을 보장합니다 시각. 그러나, min_tx_interval 이 감소되면, BFD 제어 패킷의 로컬 송신 간격은 즉시 감소 할 수있다. min_rx_interval 이 증가하면 로컬 탐지 시간이 즉시 증가합니다.

Port BFD 쿼리 모드 활성화

포트 BFD 쿼리 모드는 기본적으로 활성화되지 않습니다.

질의 모드에서는 각 시스템이 다른 시스템과의 연결을 확인하는 독립적 인 방법을 가지고 있다고 가정합니다. BFD 세션이 구성되면 특정 시스템에서 명시 적 연결 검사가 필요하지 않으면 시스템은 BFD 제어 패킷 전송을 중지합니다. 명시적인 연결 검사가 필요한 시스템에서 시스템은 짧은 시퀀스 BDF 제어

패킷을 전송하고 검사 기간에 응답 패킷을받지 못하면 세션이 중단되었다고 주장합니다. 점검 기간에 응답 패킷이 피어로부터 수신되면 이는 전달 경로가 정상이며 BFD 제어 패킷이 전송을 중지 함을 의미합니다.

다음 명령을 vlan 인터페이스에서 실행 시 쿼리모드로 실행합니다.

명령어	설명
bfd demand enable	BFD 쿼리 모드를 활성화합니다.

시스템은 BFD 쿼리 모드를 활성화 또는 비활성화하도록 지원합니다.

Port BFD 활성화 Echo

포트 BFD 에코는 기본적으로 활성화되지 않습니다.

BFD 에코가 활성화 된 후, BFD 에코를 지원하는 이웃이 올라가면, 제어 패킷은 느린 타이머에 의해 구성된 간격에 따라 전송됩니다. 연결 감지는 반향 패킷에 의해 완료되고 반향 패킷의 전송 간격은 min_echo_rx_interval 에 의해 구성된 시간입니다.

관련 구성을 수행하려면 다음 명령을 실행하십시오:

명령어	설명
bfd echo enable *<cr>|<number>*	BFD 에코 활성화.

이미 "업"된 이웃장비에 대한 에코 기능의 활성화 및 종료는 이웃의 상태에 영향을주지 않지만 제어 패킷의 전송 간격은 영향을받습니다.

BFD 포트 인증 사용

BFD 포트 인증은 기본적으로 활성화되지 않습니다.

인증 구성은 BFD 인접 장치가 가동되기 전에 즉각적인 효력을 발휘하며 BFD 감지 구성이 동일 할 때만 BFD 감지가 수행되는 링크의 두 터미널을 가동 할 수 있습니다. 그러나 BFD 네이버가 가동 된 후 인증 구성이 수정되면 두 단말기의 동일한 구성 또는 다른 구성이 BFD 네이버의 상태에 영향을 미치지 않습니다.

관련 구성을 수행하려면 다음 명령을 vlan 인터페이스에서 실행하십시오:

명령어	설명
bfd authentication-mode [md5 | meticulous md5 | simple] <key id> <key>	BFD 인증 기능을 사용합니다..

BFD 정보 확인

관련 구성을 수행하려면 다음 명령을 실행하십시오:

명령어	**설명**
show bfd interfaces *[details]*	BFD가 활성화 된 시스템의 포트를 표시합니다..
show bfd neighbors *[details]*	시스템에 BFD 이웃을 표시합니다..

BFD 구성 예

BFD 감지를위한 관련 프로토콜을 구성하고 BFD 구성 전에 해당 포트에서 BFD 기능을 활성화해야합니다.

다음 예는 BFD 가 양방향 감지 기능을 가진 BGP 를 제공하는 방법을 보여줍니다.

A 와 B 사이의 EBGP 관계를 구성하고 BFD 를 통해 링크를 확인하십시오..

A :

```
interface vlan1
 ip address 1.1.1.1 255.255.255.0
                    bfd enable
 no ip directed-broadcast
 !
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 1.1.1.2 remote-as 200
 neighbor 1.1.1.2 fall-over bfd
!
```

B :

```
interface vlan1
 ip address 1.1.1.2 255.255.255.0
                    bfd enable
 no ip directed-broadcast
 !
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 fall-over bfd
```

NTP 구성

개요

NTP (Network Time Protocol)는 현재 인터넷에서 시간 동기화를 실현하는 중요한 방법입니다.

NTP 는 클라이언트 - 서버 모드를 사용합니다. 서버는 GPS 신호를 수신하여 자체 시간을 얻거나 시간 기준으로 자체의 원자 시계를 취하고 서버가 제공하는 시간 서비스에 정기적으로 액세스하여 클라이언트가 정확한 시간 정보를 얻고 동기화 할 시계를 조정합니다 인터넷상의 시간. UDP 프로토콜과 포트 123 은 클라이언트와 서버 간의 통신에 사용됩니다..

NTP 구성 작업 목록

NTP 구성은 두 부분으로 나눌 수 있습니다. 하나는 NTP 서버로 사용할 로컬 스위치이고 다른 하나는 NTP 클라이언트로 사용할 로컬 스위치입니다..

로컬 스위치는 NTP 서버로 사용됩니다.:

- NTP 서버의 등급 구성
- NTP 서버 활성화

로컬 스위치는 NTP 클라이언트로 사용됩니다.:

- NTP 서버의 IP 주소 구성
- NTP 서버 탐색 간격 구성
- NTP 서버 비활성화

NTP 구성

NTP 서버의 등급 구성

구성 모드: 전역

명령어	설명
NTP master [Stratum]	NTP 서버의 등급을 구성합니다.

NTP 서버 활성화

구성 모드: 전역

명령어	표
NTP master	NTP 서버는 기본적으로 활성화되어 있습니다..

NTP 서버의 IP 주소 구성

구성 모드: 전역

명령어	설명
NTP server <A.B.C.D> [NTP-version]	NTP 서버의 IP 주소와 버전을 구성합니다..

NTP 서버 탐색 간격 구성

구성 모드: 전역

명령어	설명
NTP query-interval *<Seconds>*	NTP 클라이언트가 NTP 서버를 탐색하는 간격을 구성합니다.(2-3600초)

NTP 서버 비활성화

구성 모드: 전역

명령어	설명
no NTP master	NTP 서버를 정지 합니다.