CatOS 구성 및 관리를 실행하는 Catalyst 4500/4000, 5500/5000 및 6500/6000 Series 스위치에 대한 모범 사례

목차

관련 정보

소개

이 문서에서는 네트워크에서 Cisco Catalyst Series 스위치 구현, 특히 Catalyst 4500/4000, 5500/5000 및 6500/6000 플랫폼의 구현에 대해 설명합니다.컨피그레이션 및 명령은 Catalyst OS(CatOS) General Deployment Software 6.4(3) 이상을 실행 중임을 전제로 설명합니다.일부 설계 고려 사항이 제시되었지만 이 문서에서는 전체 캠퍼스 설계에 대해 다루지 않습니다.

사전 요구 사항

요구 사항

이 문서에서는 Catalyst 6500 Series Command Reference, 7.6에 대해 잘 알고 있다고 가정합니다.

이 문서의 모든 부분에서 공용 온라인 자료에 대한 참조 자료가 제공되지만, 다른 기본 및 교육 자료는 다음과 같습니다.

- Cisco ISP Essentials - 모든 ISP가 고려해야 하는 필수 IOS 기능
- Cisco 네트워크 모니터링 및 이벤트 상관관계 지침
- 기가비트 캠퍼스 네트워크 설계—원칙 및 아키텍처
- Cisco SAFE:엔터프라이즈 네트워크를 위한 보안 청사진

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

이러한 솔루션은 Cisco 엔지니어가 많은 대규모 고객 및 복잡한 네트워크와 함께 수년 간 일한 현장 경험을 나타냅니다.따라서 이 문서에서는 네트워크를 성공적으로 만드는 실제 구성을 강조합니다.본 백서에서는 다음과 같은 솔루션을 제공합니다.

- 가장 광범위한 현장 노출, 그리고 가장 낮은 위험을 통계적으로 지닌 솔루션.
- 단순한 솔루션으로서 확실한 결과를 얻기 위해 일부 유연성을 거래합니다.
- 네트워크 운영 팀에서 쉽게 관리하고 구성할 수 있는 솔루션
- 고가용성 및 고안정성을 촉진하는 솔루션

이 문서는 다음 4개의 섹션으로 구분됩니다.

- 기본 컨피그레이션 - STP(Spanning Tree Protocol) 및 트렁킹 등 대부분의 네트워크에서 사용되는 기능입니다.
- 관리 컨피그레이션 — SNMP(Simple Network Management Protocol), RMON(Remote Monitoring), Syslog, CDP(Cisco Discovery Protocol), NTP(Network Time Protocol)를 사용한

시스템 및 이벤트 모니터링과 함께 설계 고려 사항
- 보안 컨피그레이션 - 비밀번호, 포트 보안, 물리적 보안 및 TACACS+를 사용한 인증
- 구성 체크리스트 - 제안된 구성 템플릿의 요약

기본 구성

이 섹션에서는 Catalyst 네트워크의 대부분과 함께 구축된 기능에 대해 설명합니다.

Catalyst 컨트롤 플레인 프로토콜

이 섹션에서는 정상적인 작동 상태에서 스위치 간에 실행되는 프로토콜을 소개합니다.이러한 프로토콜에 대한 기본적인 이해는 각 섹션을 해결하는 데 유용합니다.

수퍼바이저 트래픽

Catalyst 네트워크에서 활성화된 대부분의 기능을 사용하려면 두 개 이상의 스위치가 작동해야 하므로 keepalive 메시지, 구성 매개변수 및 관리 변경을 제어하여 교환해야 합니다.이러한 프로토콜이 CDP와 같은 Cisco 독점 프로토콜이든 IEEE 802.1d(STP)와 같은 표준 기반이든 Catalyst 시리즈에서 구현할 때 공통되는 특정 요소가 있습니다.

기본 프레임 포워딩에서 사용자 데이터 프레임은 엔드 시스템에서 시작되며, L2(Layer 2) 스위치 도메인 전체에서 해당 소스 주소와 목적지 주소는 변경되지 않습니다.각 스위치 수퍼바이저 엔진의 CAM(Content Addressable Memory) 조회 테이블은 소스 주소 학습 프로세스에 의해 채워지며, 수신된 각 프레임을 전달해야 하는 이그레스 포트를 나타냅니다.주소 학습 프로세스가 불완전한 경우(대상을 알 수 없거나 프레임이 브로드캐스트 또는 멀티캐스트 주소로 전송됨), 해당 VLAN의 모든 포트가 포워딩(플러드)됩니다.

또한 스위치는 시스템을 통해 전환될 프레임을 인식해야 하며 스위치 CPU 자체에 전달되어야 합니다(NMP[Network Management Processor] 라고도 함).

Catalyst 컨트롤 플레인은 내부 스위치 포트의 NMP에 트래픽을 수신하고 직접 전송하기 위해 **시스템 항목**이라는 CAM 테이블의 특수 항목을 사용하여 생성됩니다.따라서 잘 알려진 목적지 MAC 주소의 프로토콜을 사용하여 컨트롤 플레인 트래픽을 데이터 트래픽과 분리할 수 있습니다.다음과 **같이 스위치에서 show** CAM system **명령**을 실행하여 이를 확인합니다.

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  ---------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

Cisco는 예약된 범위의 이더넷 MAC 및 프로토콜 주소를 보유하고 있습니다(예:).각 내용은 이 문서의 뒷부분에서 다룹니다.그러나 이 표에는 편의상 요약이 나와 있습니다.

기능	SNAP HDLC 프로토콜 유형	대상 멀티캐스트 MAC

PAgP(Port Aggregation Protocol)	0x0104	01-00-0c-cc-cc-cc
스패닝 트리 PVSTP+	0x010b	01-00-0c-cc-cc-cd
VLAN 브리지	0x010c	01-00-0c-cd-ce
UDLD(Unidirectional Link Detection)	0x0111	01-00-0c-cc-cc-cc
Cisco 검색 프로토콜	0x2000	01-00-0c-cc-cc-cc
동적 트렁킹(DTP)	0x2004	01-00-0c-cc-cc-cc
STP 빠른 업링크	0x200a	01-00-0c-cd-cd-cd
IEEE 스패닝 트리 802.1d	해당 사항 없음 - DSAP 42 SSAP 42	01-80-c2-00-00-00
ISL(Inter Switch Link)	해당 없음	01-00-0c-00-00-00
VTP(VLAN Trunking)	0x2003	01-00-0c-cc-cc-cc
IEEE 일시 중지, 802.3x	해당 사항 없음 - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

대부분의 Cisco 제어 프로토콜은 LAN Analyzer 추적에서 볼 수 있는 LLC **0xAAAA03, OUI 0x0000C를** 포함하여 IEEE 802.3 SNAP 캡슐화를 사용합니다.이러한 프로토콜의 다른 일반적인 속성은 다음과 같습니다.

- 이러한 프로토콜은 포인트 투 포인트 연결을 가정합니다.멀티캐스트 목적지 주소를 신중하게 사용하면 프레임을 이해하고 가로채지 못하는 디바이스가 비 Cisco 스위치를 통해 투명하게 통신할 수 있으므로 두 개의 Catalyst가 이를 통해 통신할 수 있습니다.그러나 멀티벤더 환경을 통한 point-to-multipoint 연결은 일관되지 않은 동작으로 이어질 수 있으며 일반적으로 방지되어야 합니다.
- 이러한 프로토콜은 L3(Layer 3) 라우터에서 종료됩니다.스위치 도메인 내에서만 작동합니다.
- 이러한 프로토콜은 인그레스(ingress) ASIC(application-specific integrated circuit) 처리 및 스케줄링을 통해 사용자 데이터보다 우선 순위를 지정합니다.

제어 프로토콜 목적지 주소가 도입된 후에는 완전성을 위해 소스 주소도 설명해야 합니다.스위치 프로토콜은 섀시의 EPROM에서 제공하는 사용 가능한 주소의 은행에서 가져온 MAC 주소를 사용합니다.STP BPDU(**Bridge Protocol Data Unit**) 또는 ISL 프레임과 같은 트래픽을 소싱할 때 각 모듈에서 사용 가능한 주소 범위를 표시하려면 show module 명령을 실행합니다.

```
>show module

...
Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
```

```
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

VLAN 1은 Catalyst 네트워크에서 특별한 의미를 갖습니다.

Catalyst Supervisor Engine은 항상 기본 VLAN 1을 사용하여 CDP, VTP 및 PAgP와 같은 트렁킹 시 여러 제어 및 관리 프로토콜에 태그를 지정합니다.내부 sc0 인터페이스를 포함한 모든 포트는 기본적으로 VLAN 1의 멤버로 구성됩니다. 모든 트렁크는 기본적으로 VLAN 1을 전달하며 5.4 이전 버전의 CatOS 소프트웨어 버전에서는 VLAN 1의 사용자 데이터를 차단할 수 없습니다.

이러한 정의는 Catalyst 네트워킹에서 잘 사용되는 용어를 명확하게 하기 위해 필요합니다.

- 관리 VLAN은 sc0이 상주하는 곳입니다.이 VLAN을 변경할 수 있습니다.
- 네이티브 VLAN은 트렁킹을 수행하지 않을 때 포트가 반환하는 VLAN으로 정의되며 802.1Q 트렁크에서 태그가 지정되지 않은 VLAN입니다.기본적으로 VLAN 1은 기본 VLAN입니다.
- 네이티브 VLAN을 변경하려면 **set vlan**-*id mod/port* 명령을 실행합니다.**참고:** VLAN을 트렁크의 기본 VLAN으로 설정하기 전에 생성합니다.

다음은 네트워크를 조정하고 VLAN 1의 포트 동작을 변경하는 몇 가지 좋은 이유입니다.

- 다른 VLAN과 마찬가지로 VLAN 1의 지름이 안정성에 대한 위험(특히 STP 관점에서)이 될 만큼 커지면 다시 정리해야 합니다.자세한 내용은 이 문서의 대역 내 관리 섹션에서 설명합니다.
- 문제 해결을 간소화하고 사용 가능한 CPU 주기를 최대화하려면 VLAN 1의 컨트롤 플레인 데이터를 사용자 데이터와 분리해야 합니다.
- VLAN 1의 L2 루프는 STP 없이 멀티레이어 캠퍼스 네트워크를 설계할 때 방지되어야 하며, 여러 VLAN과 IP 서브넷이 있을 경우 액세스 레이어에 트렁킹이 계속 필요합니다.이렇게 하려면 트렁크 포트에서 VLAN 1을 수동으로 지웁니다.

요약하면 트렁크에 대한 다음 정보를 참고하십시오.

- **CDP, VTP 및 PAgP** 업데이트는 항상 VLAN 1 태그가 있는 트렁크에서 전달됩니다.이는 VLAN 1이 트렁크에서 지워지고 네이티브 VLAN이 아닌 경우에도 마찬가지입니다.사용자 데이터에 대해 VLAN 1을 지우면 VLAN 1을 사용하여 여전히 전송되는 컨트롤 플레인 트래픽에는 영향을 주지 않습니다.
- ISL 트렁크에서 DTP 패킷은 VLAN1에서 전송됩니다. 이는 VLAN 1이 트렁크에서 지워지고 더 이상 네이티브 VLAN이 아닌 경우에도 마찬가지입니다.802.1Q 트렁크에서 DTP 패킷은 네이티브 VLAN에서 전송됩니다.이는 기본 VLAN이 트렁크에서 지워진 경우에도 마찬가지입니다.
- PVST+에서 **802.1Q IEEE BPDU는** VLAN 1이 트렁크에서 지워지지 않는 한 다른 벤더와의 상호 운용성을 위해 공통 스패닝 트리 VLAN 1에 태그 처리되지 않은 상태로 전달됩니다.이는 네이티브 VLAN 컨피그레이션과 상관없이 해당됩니다.**Cisco PVST+ BPDU는** 다른 모든 VLAN에 대해 전송 및 태그가 지정됩니다.자세한 내용은 이 문서의 스패닝 트리 프로토콜 섹션을 참조하십시오.
- 802.1s MST(Multiple Spanning Tree) BPDU는 항상 ISL 및 802.1Q 트렁크의 VLAN 1에서 전송됩니다.이는 트렁크에서 VLAN 1이 지워진 경우에도 적용됩니다.
- MST 브리지 및 PVST+ 브리지 간 트렁크에서 VLAN 1을 지우거나 비활성화하지 마십시오.그러나 VLAN 1이 비활성화된 경우 모든 VLAN이 MST 브리지의 경계 포트를 루트 불일치 상태로 설정하지 않도록 하려면 MST 브리지가 루트가 되어야 합니다.자세한 내용은 다중 스패닝 트리 프로토콜(802.1s) 이해를 참조하십시오.

권장 사항

VLAN을 해당 VLAN에 연결된 클라이언트나 호스트가 없는 **up/up** 상태로 유지하려면 해당 VLAN에 연결된 물리적 디바이스가 하나 이상 있어야 합니다.그렇지 않으면 VLAN의 **up/down** 상태가 있습니다.현재, 해당 VLAN에 대한 스위치에 활성 포트가 없을 때 VLAN 인터페이스를 작동/가동하는 명령이 없습니다.

디바이스를 연결하지 않으려면 해당 VLAN에 대한 임의의 포트에 루프백 플러그를 연결합니다.대신 동일한 스위치에서 해당 VLAN의 두 포트를 연결하는 크로스오버 케이블을 사용해 보십시오.이 방법은 포트를 강제로 올려놓습니다.자세한 내용은 T1/56K 라인에 대한 루프백 테스트의 루프백 플러그 플러그 섹션을 참조하십시오.

네트워크가 통신 사업자에게 멀티홈(multihomed)되면 네트워크는 두 통신 사업자 간의 트랜짓 네트워크 역할을 합니다.패킷에서 수신된 VLAN 번호를 변환하거나 변경해야 하는 경우 한 통신 사업자로부터 다른 통신 사업자로 전달될 때 QinQ 기능을 사용하여 VLAN 번호를 변환하는 것이 좋습니다.

VLAN 트렁킹 프로토콜

VLAN을 생성하기 전에 네트워크에서 사용할 VTP 모드를 결정합니다.VTP는 하나 이상의 스위치에서 VLAN 컨피그레이션 변경을 중앙에서 수행할 수 있도록 합니다.이러한 변경 사항은 도메인의 다른 모든 스위치로 자동으로 전파됩니다.

운영 개요

VTP는 VLAN 컨피그레이션 일관성을 유지하는 L2 메시징 프로토콜입니다.VTP는 네트워크 전체에서 VLAN의 추가, 삭제 및 이름 변경을 관리합니다.VTP는 중복 VLAN 이름, 잘못된 VLAN 유형 사양, 보안 위반 등 여러 문제를 일으킬 수 있는 잘못된 컨피그레이션 및 컨피그레이션 불일치를 최소화합니다.VLAN 데이터베이스는 이진 파일이며 구성 파일과 별도로 VTP 서버의 NVRAM에 저장됩니다.

VTP 프로토콜은 이더넷 대상 멀티캐스트 MAC 주소(**01-00-0c-cc-cc-cc-cc**)를 사용하여 스위치 간에 통신합니다. SNAP HDLC 프로토콜 유형 Ox2003입니다. VTP는 ISL 또는 802.1Q의 페이로드이므로 DTP가 온라인 트렁크를 가져올 때까지 메시지를 전송할 수 없습니다.

메시지 유형에는 5분마다 요약 광고, 변경 사항이 있는 경우 하위 집합 광고 및 요청 광고, VTP 정리가 활성화된 경우 조인 등이 포함됩니다.VTP 컨피그레이션 수정 번호는 서버에서 변경 사항이 있을 때마다 하나씩 증가하며, 그런 다음 새 테이블을 도메인 전체에 전파합니다.

VLAN이 삭제되면 해당 VLAN의 멤버였던 포트는 비활성 상태가 됩니다.마찬가지로 클라이언트 모드의 스위치가 부팅 시 VTP VLAN 테이블을 수신할 수 없는 경우(VTP 서버 또는 다른 VTP 클라이언트에서) 기본 VLAN 1을 제외한 VLAN의 모든 포트가 비활성화됩니다.

이 표에서는 다양한 VTP 모드에 대한 기능 비교 요약을 제공합니다.

기능	서버	클라이언트	투명	꺼짐[1]
소스 VTP 메시지	예	예	아니요	아니요
VTP 메시지 수신	예	예	아니요	아니요
VTP	예	예	예	아니요

메시지 전달				
VLAN 생성	예	아니요	예(로컬에서만 중요함)	예(로컬에서만 중요함)
VLAN 기억	예	아니요	예(로컬에서만 중요함)	예(로컬에서만 중요함)

VTP 모드에서는 VTP 업데이트가 무시됩니다. VTP 멀티캐스트 MAC 주소는 일반적으로 제어 프레임을 선택하고 수퍼바이저 엔진에 전달하는 데 사용되는 시스템 CAM에서 제거됩니다. 프로토콜이 멀티캐스트 주소를 사용하므로 투명 모드(또는 다른 벤더 스위치)의 스위치는 도메인의 다른 Cisco 스위치로 프레임을 플러딩하기만 합니다.

[1] CatOS 소프트웨어 릴리스 7.1에는 모드를 사용하여 VTP를 비활성화하는 옵션이 도입되었습니다.VTP 모드에서는 스위치가 VTP 모드와 매우 유사한 방식으로 동작하지만, off 모드는 VTP 업데이트 전달을 억제한다는 점을 제외합니다.

이 표에서는 초기 컨피그레이션에 대한 요약을 제공합니다.

기능	기본값
VTP 도메인 이름	Null
VTP 모드	서버
VTP 버전	버전 1이 활성화되었습니다.
VTP 비밀번호	없음
VTP 정리	비활성화됨

VTP 버전 2(VTPv2)에는 이러한 기능 유연성이 포함됩니다.그러나 VTP 버전 1(VTPv1)과 상호 운용되지 않습니다.

- 토큰 링 지원
- 인식할 수 없는 VTP 정보 지원;스위치는 구문 분석할 수 없는 값을 전파합니다.
- 버전 종속 투명 모드; 모드는 더 이상 도메인 이름을 확인하지 않습니다.이렇게 하면 투명 도메인 전체에서 둘 이상의 도메인을 지원할 수 있습니다.
- 버전 번호 전파;모든 스위치에서 VTPv2를 사용할 수 있는 경우 단일 스위치의 컨피그레이션을 통해 모두 활성화할 수 있습니다.

자세한 내용은 VTP(VLAN 트렁크 프로토콜) 이해 및 구성을 참조하십시오.

VTP 버전 3

CatOS 소프트웨어 릴리스 8.1에는 VTP 버전 3(VTPv3)에 대한 지원이 도입되었습니다.VTPv3는 기존 버전에 대한 향상된 기능을 제공합니다.이러한 향상된 기능을 통해 다음을 수행할 수 있습니다.

- 확장 VLAN 지원
- 프라이빗 VLAN 생성 및 광고 지원
- VLAN 인스턴스 및 MST 매핑 전파 인스턴스 지원(CatOS 릴리스 8.3에서 지원됨)
- 서버 인증 향상
- "잘못된" 데이터베이스를 VTP 도메인에 실수로 삽입하지 않도록 보호
- VTPv1 및 VTPv2와의 상호 작용
- 포트별로 구성할 수 있는 기능

VTPv3 구현과 이전 버전의 주요 차이점 중 하나는 VTP 기본 서버의 도입입니다.도메인이 분할되지 않은 경우 VTPv3 도메인에는 기본 서버가 하나만 있어야 합니다.VTP 도메인으로 전파하려면 VTP 도메인에 대한 변경 사항을 VTP 주 서버에서 실행해야 합니다.보조 서버라고도 하는 VTPv3 도메인 내에 여러 서버가 있을 수 있습니다.스위치가 서버로 구성되면 기본적으로 스위치가 보조 서버가 됩니다.보조 서버는 도메인의 컨피그레이션을 저장할 수 있지만 컨피그레이션을 수정할 수는 없습니다.보조 서버는 스위치에서 성공적으로 인계를 수행하여 기본 서버가 될 수 있습니다.

VTPv3를 실행하는 스위치는 현재 기본 서버보다 버전 번호가 더 높은 VTP 데이터베이스만 허용합니다.이 프로세스는 스위치가 항상 동일한 도메인의 인접 디바이스로부터 우수한 구성을 허용하는 VTPv1 및 VTPv2와 크게 다릅니다.VTPv3의 이 변경 사항은 보호를 제공합니다.VTP 수정 번호가 더 높은 네트워크에 새로 도입된 스위치는 전체 도메인의 VLAN 컨피그레이션을 덮어쓸 수 없습니다.

VTPv3에서는 VTP에서 비밀번호를 처리하는 방법도 개선되었습니다.비밀번호를 "숨김"으로 구성하기 위해 숨겨진 비밀번호 컨피그레이션 옵션을 사용하는 경우 다음 항목이 발생합니다.

- 비밀번호는 컨피그레이션의 일반 텍스트로 표시되지 않습니다.비밀번호의 16진수 형식이 컨피그레이션에 저장됩니다.
- 스위치를 기본 서버로 구성하려고 하면 비밀번호를 입력하라는 프롬프트가 표시됩니다.비밀번호가 비밀번호와 일치하면 스위치가 기본 서버가 되어 도메인을 구성할 수 있습니다.

참고: 기본 서버는 인스턴스에 대한 VTP 컨피그레이션을 수정해야 할 경우에만 필요합니다.보조 서버는 재로드 시 컨피그레이션의 지속성을 보장하므로 VTP 도메인은 활성 주 서버 없이 작동할 수 있습니다.다음과 같은 이유로 주 서버 상태가 종료됩니다.

- 스위치 다시 로드
- 액티브 수퍼바이저와 이중화 수퍼바이저 엔진 간의 고가용성 전환
- 다른 서버에서 인계
- 모드 컨피그레이션의 변경
- VTP 도메인 컨피그레이션 변경 사항(예: 변경 사항):버전도메인 이름도메인 암호

또한 VTPv3에서는 스위치가 여러 VTP 인스턴스에 참여할 수 있습니다.이 경우 VTP 모드는 서로 다른 VTP 인스턴스에 특정하므로 동일한 스위치가 한 인스턴스의 VTP 서버와 다른 인스턴스의 클라이언트가 될 수 있습니다.예를 들어, 스위치는 VLAN 인스턴스에 대한 모드에서 스위치가 구성된 동안 MST 인스턴스에 대해 모드에서 작동할 수 있습니다.

VTPv1 및 VTPv2와의 상호 작용에서 모든 VTP 버전의 기본 동작은 이전 버전의 VTP가 새 버전 업데이트를 삭제하기만 한다는 것입니다.VTPv1 및 VTPv2 스위치가 모드에 있지 않으면 모든 VTPv3 업데이트가 삭제됩니다.반면, VTPv3 스위치가 트렁크에서 레거시 VTPv1 또는 VTPv2 프레임을 수신한 후 스위치는 데이터베이스 업데이트의 축소된 버전을 VTPv1 및 VTPv2 스위치로 전달합니다.그러나 VTPv1 및 VTPv2 스위치의 업데이트가 VTPv3 스위치에서 수락되지 않는다는 점에서 이 정보 교환은 단방향입니다.트렁크 연결에서 VTPv3 스위치는 트렁크 포트에서 VTPv2 및 VTPv3 인접 디바이스의 존재를 충족하기 위해 확장 다운된 업데이트와 모든 기능을 갖춘 VTPv3 업데이트를 계속 전송합니다.

확장 VLAN에 VTPv3 지원을 제공하기 위해 VTP가 VLAN당 70바이트를 할당하는 VLAN 데이터베이스의 형식이 변경됩니다.변경 사항을 사용하면 기존 프로토콜에 대해 수정되지 않은 필드를 전달하는 대신 기본값이 아닌 값만 코딩할 수 있습니다.이러한 변경으로 인해 4K VLAN 지원은 결과 VLAN 데이터베이스의 크기입니다.

권장 사항

VTP / 모드 또는 VTP 모드를 사용할지에 대한 구체적인 권장 사항은 없습니다.일부 고객은 나중에

에 몇 가지 고려 사항을 언급했지만 VTP / 모드를 손쉽게 관리할 수 있는 것을 선호합니다.리던던시를 위해 각 도메인에 2개의 모드 스위치를 두는 것이 좋습니다(일반적으로 2개의 디스트리뷰션 레이어 스위치).도메인의 나머지 스위치는 모드로 설정되어야 합니다.VTPv2를 사용하여 / 모드를 구현할 때 동일한 VTP 도메인에서 더 높은 수정 번호가 항상 허용된다는 점에 유의하십시오.VTP 또는 모드에 구성된 스위치가 VTP 도메인에 도입되고 기존 VTP 서버보다 높은 수정 번호가 있는 경우 이 옵션은 VTP 도메인 내의 VLAN 데이터베이스를 덮어씁니다.컨피그레이션 변경이 의도치 않게 변경되고 VLAN이 삭제되면 덮어쓰면 네트워크에서 심각한 중단이 발생할 수 있습니다. 또는 스위치에 항상 서버의 구성 수정 번호가 낮도록 하려면 클라이언트 VTP 도메인 이름을 표준 이름 이외의 이름으로 변경합니다.그런 다음 표준으로 돌아갑니다.이 작업은 클라이언트의 컨피그레이션 개정을 0으로 설정합니다.

네트워크에서 쉽게 변경할 수 있는 VTP 기능에 대한 장단점이 있습니다.많은 기업은 다음과 같은 이유로 VTP 모드에 대해 신중한 접근 방식을 선호합니다.

- 스위치나 트렁크 포트에서 VLAN을 수정하려면 한 번에 하나의 스위치로 간주해야 하므로, 올바른 변경 제어 방식을 권장합니다.
- 또한 실수로 VLAN을 삭제하는 등 전체 도메인에 영향을 미치는 관리자 오류의 위험을 제한합니다.
- VTP 수정 번호가 더 높은 새 스위치가 네트워크에 도입되면 전체 도메인 VLAN 컨피그레이션을 덮어쓸 위험이 없습니다.
- VLAN을 실행 중인 트렁크에서 해당 VLAN에 포트가 없는 스위치로 정리하도록 권장합니다.따라서 프레임 플러딩이 대역폭 효율성이 향상됩니다.수동 정리는 스패닝 트리 지름을 줄이므로 유용합니다(이 문서의 DTP 섹션 참조). 포트 채널 트렁크에서 사용되지 않는 VLAN을 정리하기 전에 IP 전화에 연결된 모든 포트가 음성 VLAN을 사용하는 액세스 포트로 구성되어 있는지 확인하십시오.
- CatOS 6.x 및 CatOS 7.x의 확장 VLAN 범위(숫자 1025~4094)는 이 방법으로만 구성할 수 있습니다.자세한 내용은 이 문서의 Extended VLAN and MAC Address Reduction 섹션을 참조하십시오.
- VTP 모드는 Cisco Works 2000의 일부인 Campus Manager 3.1에서 지원됩니다.VTP 도메인에서 하나 이상의 서버가 필요한 이전 제한이 제거되었습니다.

샘플 VTP 명령	**설명**
vtp 도메인 ***이름*** **암호** ***x 설정***	CDP는 도메인 간 케이블 연결을 확인하기 위해 이름을 확인합니다.간단한 비밀번호는 의도하지 않은 변경에 대한 예방책입니다.붙여 넣을 경우 대/소문자를 구분하는 이름이나 공백을 주의하십시오.
vtp 모드 투명 설정	
vlan ***vlan 번호*** **이름** ***설정***	VLAN에 포트가 있는 스위치당.
트렁크 ***mod/port*** **vlan** ***범위 설정***	트렁크가 필요한 경우 VLAN을 전달할 수 있습니다. 기본값은 모든 VLAN입니다.

트렁크 *mod/port vlan 범위 지우기*	VLAN이 없는 디스트리뷰션 레이어에서 액세스 레이어로의 트렁크와 같이 수동 정리로 STP 지름을 제한합니다.

참고: set 명령으로 VLAN을 **지정하면** VLAN만 추가되고 VLAN은 지워지지 않습니다.예를 들어 set trunk x/y 1-10 명령은 허용된 목록을 VLAN 1-10으로 설정하지 않습니다. **clear trunk x/y 11-1005 명령을 실행하여** 원하는 결과를 얻습니다.

토큰 링 스위칭이 이 문서의 범위를 벗어나도 VTP 모드는 TR-ISL 네트워크에 권장되지 않습니다 .토큰 링 스위칭의 기반은 전체 도메인이 단일 분산 다중 포트 브리지를 형성하므로 모든 스위치에는 동일한 VLAN 정보가 있어야 합니다.

기타 옵션

VTPv2는 / 모드가 권장되는 토큰 링 환경의 요구 사항입니다.

VTPv3는 보다 엄격한 인증 및 컨피그레이션 수정 제어를 구현하는 기능을 제공합니다.VTPv3는 기본적으로 VTPv1/VTPv2 모드에서 제공하는 것과 같이 동일한 수준의 기능을 제공하지만 더 향상된 보안을 제공합니다.또한 VTPv3는 레거시 VTP 버전과 부분적으로 호환됩니다.

이 문서에서는 불필요한 프레임 플러딩을 줄이기 위해 VLAN을 정리하여 얻을 수 있는 이점을 설명합니다.set vtp pruning enable 명령은 VLAN을 자동으로 정리하므로 불필요한 프레임의 비효율적인 플러딩을 중지합니다.수동 VLAN 제거와 달리 자동 제거는 스패닝 트리 지름을 제한하지 않습니다.

CatOS 5.1에서 Catalyst 스위치는 1000보다 큰 802.1Q VLAN 번호를 ISL VLAN 번호에 매핑할 수 있습니다.CatOS 6.x에서 Catalyst 6500/6000 스위치는 IEEE 802.1Q 표준에 따라 4096 VLAN을 지원합니다.이러한 VLAN은 다음 3가지 범위로 구성되어 있으며, 그중 일부만 VTP를 사용하여 네트워크의 다른 스위치에 전파됩니다.

- 일반 범위 VLAN:1–1001
- 확장 범위 VLAN:1025-4094(VTPv3에서만 전파 가능)
- 예약된 범위 VLAN:0,1002—1024, 4095

IEEE는 VTP와 유사한 결과를 달성하기 위해 표준 기반 아키텍처를 생성했습니다.802.1Q GARP(Generic Attribute Registration Protocol)의 멤버인 GVRP(Generic VLAN Registration Protocol)는 벤더 간의 VLAN 관리 상호운용성을 허용하지만 이 문서의 범위를 벗어납니다.

참고: CatOS 7.x에서는 과 매우 유사한 모드인 VTP를 `off` 모드 설정하는 옵션을 .그러나 스위치는 VTP 프레임을 전달하지 않습니다.이 기능은 관리 제어 이외의 스위치로 트렁킹할 때 일부 설계에서 유용할 수 있습니다.

확장된 VLAN 및 MAC 주소 감소

MAC 주소 감소 기능은 확장 범위 VLAN 식별을 활성화합니다.MAC 주소 감소를 활성화하면 VLAN 스패닝 트리에 사용되는 MAC 주소 풀이 비활성화되고 단일 MAC 주소가 유지됩니다.이 MAC 주소는 스위치를 식별합니다.CatOS 소프트웨어 릴리스 6.1(1)에는 IEEE 802.1Q 표준에 따라 4096 VLAN을 지원하도록 Catalyst 6500/6000 및 Catalyst 4500/400 스위치에 대한 MAC 주소 감소 지원이 도입되었습니다.

작업 개요

스위치 프로토콜은 섀시의 EPROM이 PVST+에서 실행되는 VLAN에 대한 브리지 식별자의 일부로 제공하는 사용 가능한 주소의 은행에서 가져온 MAC 주소를 사용합니다.Catalyst 6500/6000 및 Catalyst 4500/4000 스위치는 섀시 유형에 따라 1024 또는 64개의 MAC 주소를 지원합니다.

1024 MAC 주소가 있는 Catalyst 스위치는 기본적으로 MAC 주소 감소를 활성화하지 않습니다 .MAC 주소는 순차적으로 할당됩니다.범위의 첫 번째 MAC 주소는 VLAN 1에 할당됩니다. 범위의 두 번째 MAC 주소는 VLAN 2에 할당됩니다.그러면 스위치에서 고유한 브리지 식별자를 사용하여 각 VLAN에서 1024개의 VLAN을 지원할 수 있습니다.

섀시 유형	**섀시 주소**
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E,WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR6606-OSR 09-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7606, CISCO06606, NAT60006606, WS CISCO7613	641

[1] MAC 주소는 64개의 MAC 주소가 있는 스위치에 대해 기본적으로 활성화되어 있으며 이 기능을 비활성화할 수 없습니다.

MAC 주소가 1024개인 Catalyst 시리즈 스위치의 경우, MAC 주소 감소를 활성화하면 스위치에 필요한 MAC 주소 수를 늘리지 않고 PVST+ 또는 16개의 MISTP(Multiple Instance STP) 인스턴스에서 실행되는 4096개의 VLAN을 지원할 수 있습니다.MAC 주소 감소는 STP에 필요한 MAC 주소 수를 VLAN 또는 MISTP 인스턴스당 1개에서 스위치당 1개로 줄입니다.

이 그림은 브리지 식별자 MAC 주소 감소가 활성화되지 않았음을 보여줍니다.브리지 식별자는 2바이트 브리지 우선 순위 및 6바이트 MAC 주소로 구성됩니다.

MAC 주소 감소는 BPDU의 STP 브리지 식별자 부분을 수정합니다.원래 2바이트 우선 순위 필드는 두 개의 필드로 분할됩니다.이렇게 분할하면 4비트 브리지 우선 순위 필드와 12비트 시스템 ID 확장이 발생하여 VLAN 번호 매기기를 0~4095로 설정할 수 있습니다.

확장 범위 VLAN을 활용하기 위해 Catalyst 스위치에서 MAC 주소 감소를 활성화한 경우 동일한 STP 도메인 내의 모든 스위치에서 MAC 주소 감소를 활성화합니다.모든 스위치에서 STP 루트 계산을 일관되게 유지하려면 이 단계가 필요합니다.MAC 주소 감소를 활성화하면 루트 브리지 우선순위는 4096과 VLAN ID의 배수가 됩니다.MAC 주소 감소가 없는 스위치는 브리지 ID를 선택할 때 더 세분화되어 있기 때문에 실수로 루트가 될 수 있습니다.

구성 지침

확장 VLAN 범위를 구성할 때는 특정 지침을 따라야 합니다.스위치는 내부 목적을 위해 확장 범위에서 VLAN 블록을 할당할 수 있습니다.예를 들어, 스위치는 라우티드 포트 또는 Flex WAN 모듈에 대한 VLAN을 할당할 수 있습니다.VLAN 블록의 할당은 항상 VLAN 1006에서 시작되어 증가합니다.Flex WAN 모듈에 필요한 범위 내에 VLAN이 있는 경우 VLAN이 사용자 VLAN 영역에서 할당되지 않으므로 필요한 모든 VLAN이 할당되지 않습니다.사용자가 할당한 VLAN과 **내부 VLAN을 모두 표시하려면 스위치에서 show vlan 명령 또는 show vlan summary 명령**을 실행합니다.

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

또한 확장 범위 VLAN을 사용하기 전에 기존 802.1Q-to-ISL 매핑을 삭제해야 합니다.또한 VTPv3 이전 버전에서는 VTP 모드를 사용하여 각 스위치에서 확장 VLAN을 정적으로 구성해야 합니다.자세한 내용은 *VLAN 구성의 확장 범위 VLAN 컨피그레이션 지침* 섹션을 참조하십시오.

참고: 소프트웨어 릴리스 8.1(1) 이전의 소프트웨어에서는 확장 범위 VLAN에 대한 VLAN 이름을 구성할 수 없습니다.이 기능은 모든 VTP 버전 또는 모드와 독립적입니다.

권장 사항

동일한 STP 도메인 내에서 일관된 MAC 주소 감소 컨피그레이션을 유지하려고 합니다.그러나 MAC 주소가 64개인 새 섀시가 STP 도메인에 도입되면 모든 네트워크 디바이스에 MAC 주소 감소의 시행이 비현실적일 수 있습니다.MAC 주소가 64개인 스위치에는 MAC 주소 감소가 기본적으로 활성화되어 있으며 이 기능을 비활성화할 수 없습니다.두 시스템이 동일한 스패닝 트리 우선 순위로 구성된 경우 MAC 주소 감소 없이 시스템의 스패닝 트리 우선 순위가 더 높습니다.MAC 주소 감소를 활성화하거나 비활성화하려면 다음 명령을 실행합니다.

```
set spantree macreduction enable | disable
```

내부 VLAN의 할당은 오름차순이며 VLAN 1006에서 시작됩니다.사용자 VLAN과 내부 VLAN 간의 충돌을 방지하기 위해 가능한 한 VLAN 4094에 가까운 사용자 VLAN을 할당합니다.Cisco IOS® 시스템 소프트웨어를 실행하는 Catalyst 6500 스위치를 사용하면 내부 VLAN 할당을 내림차순으로 구성할 수 있습니다.CatOS 소프트웨어에 해당하는 CLI(Command-Line Interface)는 공식적으로 지원되지 않습니다.

자동 협상

이더넷/고속 이더넷

Autonegotiation은 IEEE FE(Fast Ethernet) 표준(802.3u)의 선택적 기능으로, **속도** 및 **이중** 기능에 대한 링크를 통해 디바이스에서 자동으로 정보를 교환할 수 있도록 합니다.Autonegotiation은 L1(Layer 1)에서 작동하며 PC와 같은 **임시 사용자**가 네트워크에 연결되는 액세스 레이어 포트를 대상으로 합니다.

운영 개요

10/100Mbps 이더넷 링크의 성능 문제의 가장 일반적인 원인은 링크의 한 포트가 반이중으로 작동하는 반면 다른 포트가 전이중 상태일 때 발생합니다.이는 링크의 하나 또는 두 포트가 모두 재설정되고 자동 협상 프로세스로 인해 두 링크 파트너가 동일한 컨피그레이션을 갖지 못할 때 종종 발생합니다.또한 관리자가 링크의 한 면을 재구성하고 다른 면을 재구성하는 것을 잊어버릴 때도 발생합니다.이러한 현상은 일반적으로 스위치에서 FCS(Frame Check Sequence), CRC(Cyclic Redundancy Check), 정렬 또는 런트 카운터를 증가시킵니다.

자동 협상은 이 문서에서 자세히 설명합니다.이러한 문서에는 자동 협상 작동 방식 및 구성 옵션에 대한 설명이 포함되어 있습니다.

- 이더넷 10/100Mb 반이중/전이중 자동 협상 구성 및 문제 해결
- Cisco Catalyst Switch와 NIC의 호환성 문제 트러블슈팅

자동 협상에 대한 일반적인 오해는 100Mbps 전이중 및 전이중 자동 협상을 다른 링크 파트너와 함께 수동으로 링크 파트너를 구성할 수 있다는 것입니다.실제로 이를 시도하면 듀플렉스 불일치가 발생합니다.이는 한 링크 파트너 자동 협상, 다른 링크 파트너의 자동 협상 매개변수 없음, 반이중 기본값 설정 등의 결과입니다.

대부분의 Catalyst 이더넷 모듈은 10/100Mbps 및 절반/전이중(half/full-duplex)을 지원하지만 **show port capabilities *mod/port*** 명령은 이를 확인합니다.

FFI

FFI(Far End Fault Indication)는 100BASE-FX(파이버) 및 기가비트 인터페이스를 보호하며, 자동 협상을 통해 물리적 레이어/신호 관련 결함에 대해 100BASE-TX(구리)를 보호합니다.

원거리 **엔드** 결함은 연결이 끊긴 TX-wire와 같이 한 스테이션에서 탐지할 수 있는 링크에서 발생한 오류입니다.이 예에서 전송 스테이션은 여전히 유효한 데이터를 수신하고 링크 무결성 모니터를 통해 링크가 정상임을 감지할 수 있습니다.다른 스테이션에서 전송이 수신되고 있지 않음을 탐지하지 못합니다.이러한 원격 결함을 탐지하는 100BASE-FX 스테이션은 인접 디바이스에 원격 결함을 알리기 위해 전송된 IDLE 스트림을 수정하여 특수 비트 패턴(FFI IDLE 패턴이라고도 함)을 전송할 수

있습니다.FFI-IDLE 패턴은 이후에 원격 포트의 종료를 트리거합니다(errdisable). 결함 보호에 대한 자세한 내용은 이 문서의 UDLD 섹션을 참조하십시오.

FFI는 이 하드웨어와 다음 모듈에서 지원됩니다.

- Catalyst 5500/5000:WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 및 WS-U5539
- Catalyst 6500/6000 및 4500/4000:모든 100BASE-FX 모듈 및 GE 모듈

권장 사항

10/100 링크에 대한 자동 협상을 구성할지, 하드 코드 속도와 듀플렉스에 대해 구성할지 여부는 궁극적으로 Catalyst 스위치 포트에 연결한 링크 파트너 또는 엔드 디바이스의 유형에 따라 달라집니다.엔드 디바이스와 Catalyst 스위치 간의 자동 협상이 일반적으로 잘 작동하며, Catalyst 스위치는 IEEE 802.3u 사양을 준수합니다.그러나 NIC 또는 벤더 스위치가 정확하게 일치하지 않을 경우 문제가 발생할 수 있습니다.10/100Mbps 자동 협상을 위한 IEEE 802.3u 사양에 설명되어 있지 않은 자동 극성 또는 케이블 무결성과 같은 공급업체별 고급 기능의 결과로 하드웨어 비호환성 및 기타 문제가 발생할 수도 있습니다.필드 알림을 참조하십시오.CAT4K/6K에 연결하는 Intel Pro/1000T NIC의 성능 문제의 예를 들면 다음과 같습니다.

호스트, 포트 속도 및 듀플렉스를 설정해야 하는 상황이 있을 것으로 예상합니다.일반적으로 다음과 같은 기본 문제 해결 단계를 수행합니다.

- 자동 협상이 링크의 양쪽에 구성되거나 하드 코딩이 양쪽에 구성되었는지 확인합니다.
- 일반적인 주의 사항은 CatOS 릴리스 노트를 참조하십시오.
- 최신 드라이버 또는 패치가 필요한 경우가 많으므로 실행 중인 NIC 드라이버 또는 운영 체제의 버전을 확인합니다.

일반적으로 어떤 유형의 링크 파트너에 대해서도 먼저 자동 협상을 사용해 보십시오.랩톱과 같은 임시 장치에 대한 자동 협상을 구성하면 상당한 이점이 있습니다.또한 서버 및 고정 워크스테이션과 같은 일시적이지 않은 장치나 스위치 간 및 스위치 간 라우터와 같은 장치에서도 자동 협상이 잘 작동하는 것이 좋습니다.언급된 이유 중 일부로는 협상 문제가 발생할 수 있습니다.이러한 경우 제공된 TAC 링크에 설명된 기본 문제 해결 단계를 수행합니다.

10/100Mbps 이더넷 포트에서 포트 속도가 으로 설정된 경우 속도와 양방향은 모두 자동 협상을 수행합니다.포트를 auto로 설정하려면 이 명령을 실행합니다.

```
set port speed port range auto
!--- This is the default.
```

포트를 하드 코딩하는 경우 다음 컨피그레이션 명령을 실행합니다.

```
set port speed port range 10 | 100 set port duplex port range full | half
```

CatOS 8.3 이상에서 Cisco는 선택적 auto-10-100 키워드를 도입했습니다.10/100/1000 Mbps의 속도를 지원하지만 1000Mbps에 대한 자동 협상이 바람직하지 않은 포트에서 auto-10-100 키워드를 사용합니다.auto-10-100 키워드를 사용하면 속도가 auto로 설정된 10/100Mbps 포트와 동일한 방식으로 포트가 작동합니다.속도와 양방향은 10/100Mbps 포트에만 협상되며 1000Mbps 속도는 협상에 참여하지 않습니다.

```
set port speed port_range auto-10-100
```

기타 옵션

스위치 간에 자동 협상이 사용되지 않을 경우 특정 문제에 대해 L1 장애 표시도 손실될 수 있습니다 .L2 프로토콜을 사용하여 적극적인 UDLD와 같은 장애 탐지를 강화하는 것이 좋습니다.

기가비트 이더넷

기가비트 이더넷(GE)에는 10/100Mbps 이더넷에 비해 더 광범위하고 흐름 제어 매개변수, 원격 결함 정보 및 이중 정보를 교환하는 데 사용되는 자동 협상 절차(IEEE 802.3z)가 있습니다(Catalyst 시리즈 GE 포트만 전이중 모드만 지원함).

참고: 802.3z는 IEEE 802.3:2000 사양으로 대체되었습니다.LAN/MAN 표준 서브스크립션의 IEEE 표준 참조:자세한 내용 을 위한 아카이브

운영 개요

GE 포트 협상은 기본적으로 활성화되며, GE 링크의 양쪽 끝에 있는 포트는 동일한 설정을 가져야 합니다.FE와 달리, 자동 협상 설정이 링크의 각 끝에서 포트에 다른 경우 GE 링크가 나타나지 않습니다.그러나 autonegotiation-disabled 포트를 연결하는 데 필요한 유일한 조건은 원거리의 유효한 기가비트 신호입니다.이 동작은 원거리의 자동 협상 컨피그레이션과 무관합니다.예를 들어, A와 B라는 두 개의 디바이스가 있다고 가정합니다. 각 디바이스는 자동 협상을 활성화하거나 비활성화할 수 있습니다.이 표는 가능한 컨피그레이션 및 각 링크 상태의 목록입니다.

협상	**B 사용**	**B 사용 안 함**
사용	양쪽에	A , B
사용 안 함	A 위, B	양쪽에

GE에서는 예약된 링크 코드 단어의 특수 시퀀스를 사용하여 링크 시작 시 동기화 및 자동 협상(활성화된 경우)이 수행됩니다.

참고: 유효한 단어 사전이 있으며 GE에서 가능한 모든 단어가 유효한 것은 아닙니다.

GE 연결의 수명은 다음과 같은 특성을 가질 수 있습니다.

동기화가 끊기면 MAC에서 링크가 다운된 것을 탐지합니다.동기화 상실은 자동 협상이 활성화되었는지 아니면 비활성화되었는지에 따라 적용됩니다.동기화는 세 개의 잘못된 단어를 연속해서 수신하는 등 장애가 발생한 특정 상황에서 손실됩니다.이 상태가 10ms 동안 지속되면 "sync fail" 조건이 설정되고 링크가 `link_down` 상태로 변경됩니다.동기화가 손실된 후 재동기화하려면 3개의 연속된 유효한 ID가 필요합니다.수신(Rx) 신호 손실과 같은 기타 치명적인 이벤트로 인해 링크 다운 이벤트가 발생합니다.

자동 협상은 연결 프로세스의 일부입니다.링크가 작동하면 자동 협상이 종료됩니다.그러나 스위치는 여전히 링크의 상태를 모니터링합니다.포트에서 자동 협상이 비활성화된 경우 "autoneg" 단계는 더 이상 옵션이 아닙니다.

GE 구리 사양(1000BASE-T)은 다음 페이지 교환을 통한 자동 협상을 지원합니다.Next Page Exchange에서는 구리 포트에서 10/100/1000Mbps 속도를 위한 자동 협상을 지원합니다.

참고: GE 파이버 사양은 듀플렉스, 흐름 제어 및 원격 장애 감지 협상을 위한 규정만 만듭니다.GE 파이버 포트는 포트 속도를 협상하지 않습니다.자동 협상에 대한 자세한 내용은 IEEE 802.3-2002 사양의 28 및 37절을 참조하십시오.

동기화 재시작 지연은 총 자동 협상 시간을 제어하는 소프트웨어 기능입니다.이 시간 내에 자동 협상이 성공하지 못하면, 교착 상태가 발생할 경우 펌웨어가 자동 협상을 다시 시작합니다.set port sync-restart-delay 명령은 autonegotiation이 enable로 설정된 경우에만 .

권장 사항

10/100 환경보다 GE 환경에서 자동 협상을 활성화하는 것이 훨씬 중요합니다.실제로, 협상을 지원할 수 없거나 상호 운용성 문제로 인해 연결 문제가 발생하는 경우 스위치 포트에 연결하는 스위치 포트에서만 자동 협상을 비활성화해야 합니다.Cisco는 모든 스위치 간 링크 및 일반적으로 모든 GE 디바이스에서 기가비트 협상을 활성화하도록 권장합니다(기본값).자동 협상을 활성화하려면 다음 명령을 실행합니다.

```
set port negotiation port range enable
!--- This is the default.
```

한 가지 알려진 예외는 릴리스 12.0(10)S 이전에 Cisco IOS Software를 실행하는 GSR(Gigabit Switch Router)에 연결되어 플로우 제어 및 자동 협상을 추가한 릴리스가 있는 경우입니다.이 경우, 이러한 두 기능을 끄거나 스위치 포트 보고서가 GSR에서 오류를 보고합니다.다음은 샘플 명령 시퀀스입니다.

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port negotiation port range disable
```

Switch-to-Server 연결은 사례별로 확인해야 합니다.Cisco 고객은 Sun, HP 및 IBM 서버에서 Gigabit 협상 과정에서 문제가 발생했습니다.

기타 옵션

흐름 제어는 802.3x 사양의 선택적 부분이며, 사용되는 경우 협상해야 합니다.디바이스는 PAUSE 프레임에 전송 및/또는 응답할 수 있거나 그럴 수 없습니다(**잘 알려진 MAC 01-80-C2-00-00-00F**). 또한 원엔드 네이버의 흐름 제어 요청에 동의할 수 없습니다.입력 버퍼가 가득 찬 포트는 링크 파트너에게 PAUSE 프레임을 전송하여 전송을 중지하고 링크 파트너 출력 버퍼에 추가 프레임을 저장합니다.이렇게 하면 장애 시에도 안정적인 초과 서브스크립션 문제가 해결되지는 않지만, 버스트 중에 파트너 출력 버퍼의 일부만으로도 입력 버퍼가 크게 증가합니다.

이 기능은 호스트 출력 버퍼가 가상 메모리만큼 커질 수 있는 액세스 포트와 엔드 호스트 간의 링크에서 가장 잘 사용됩니다.스위치 간 사용은 이점이 제한적입니다.

스위치 포트에서 이 명령을 제어하려면 다음 명령을 실행합니다.

```
set port flowcontrol mod/port receive | send off |on | desired
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

참고: 모든 Catalyst 모듈은 협상 시 PAUSE 프레임에 응답합니다.일부 모듈(예: WS-X5410, WS-X4306)은 차단을 사용하지 않으므로 협상하더라도 PAUSE 프레임을 보내지 않습니다.

동적 트렁킹 프로토콜

캡슐화 유형

트렁크는 원래 이더넷 프레임을 일시적으로 식별하고 태깅(링크-로컬)하여 디바이스 간에 VLAN을 확장하므로 단일 링크를 통해 멀티플렉싱할 수 있습니다.또한 스위치 간에 별도의 VLAN 브로드캐스트 및 보안 도메인이 유지되도록 합니다.CAM 테이블은 스위치 내에서 프레임-VLAN 매핑을 유지합니다.

트렁킹은 ATM LANE, FDDI 802.10 및 이더넷을 포함하여 여러 유형의 L2 미디어에서 지원되지만, 여기에 두 가지 미디어만 표시됩니다.

ISL 운영 개요

Cisco의 독자적인 식별 또는 태깅 구성인 ISL은 오랫동안 사용되어 왔습니다.802.1Q IEEE 표준도 사용할 수 있습니다.

ISL은 2-레벨 태깅 체계에 원래 프레임을 완전히 캡슐화함으로써 터널링 프로토콜이며 비-이더넷 프레임을 전송하는 추가적인 이점을 제공합니다.표준 이더넷 프레임에 26바이트 헤더와 4바이트 FCS를 추가합니다. 더 큰 이더넷 프레임은 트렁크로 구성된 포트에 의해 처리되고 예상됩니다 .ISL은 1024개의 VLAN을 지원합니다.

ISL 프레임 형식

40비트	4비트	4비트	48비트	16비트	24비트	24비트	15비트	비트	16비트	16비트	가변 길이	32비트
대상주소	유형	사용자	SA	길이	스냅 LLC	HSA	VLAN	BPDU	인덱스	예약	캡슐화된 프레	FCS

											임	
01-00-0c-00-00					AAAA03	0000C						

자세한 내용은 InterSwitch 링크 및 IEEE 802.1Q 프레임 형식을 참조하십시오.

802.1Q 운영 개요

IEEE 802.1Q 표준은 스패닝 트리 개선 사항, GARP(이 문서의 VTP 섹션 참조) 및 802.1p QoS(Quality of Service) 태깅 등 캡슐화 유형보다 훨씬 많은 것을 지정합니다.

802.1Q 프레임 형식은 원래 이더넷 소스 주소 및 대상 주소를 보존하지만, 이제는 호스트가 QoS 신호 처리를 위해 802.1p 사용자 우선순위를 표시하기 위해 태깅을 사용할 수 있는 액세스 포트에서도 태깅을 사용할 수 있는 거대 프레임이 수신될 것을 스위치에서 예상해야 합니다.태그는 4바이트이므로 802.1Q 이더넷 v2 프레임은 1522바이트이며 IEEE 802.3ac 작업 그룹 성과입니다 .802.1Q는 4096 VLAN의 번호 지정 공간도 지원합니다.

전송 및 수신된 모든 데이터 프레임은 네이티브 VLAN에 있는 프레임을 제외하고 802.1Q 태그됩니다(인그레스 스위치 포트 컨피그레이션을 기반으로 하는 암시적 태그가 있음). 네이티브 VLAN의 프레임은 항상 태그가 지정되지 않고 일반적으로 태그가 지정되지 않은 상태로 전송됩니다.그러나 태깅을 받을 수도 있습니다.

자세한 내용은 IEEE 802.10을 통한 VLAN 표준화 및 IEEE 802 를 참조하십시오.

802.1Q/801.1p 프레임 형식

		태그 헤더						
		TPID	**TCI**					
48비트	48비트	**16비트**	**3비트**	**1비트**	**12비트**	16비트	가변 길이	32비트
DA	SA	**TPID**	**우선순위**	**CFI**	**VLAN ID**	길이/유형	PAD를 사용한 데이터	FCS
		0x8100	**0 - 7**	**0-1**	**0-4095**			

권장 사항

모든 최신 하드웨어는 802.1Q를 지원합니다(일부 하드웨어는 Catalyst 4500/4000 시리즈 및 CSS 11000과 같은 802.1Q만 지원). Cisco는 새로운 모든 구현이 IEEE 802.1Q 표준 및 이전 네트워크를 단계적으로 ISL에서 마이그레이션할 것을 권장합니다.

IEEE 표준은 공급업체 상호 운용성을 허용합니다.이는 새로운 호스트 802.1p 지원 NIC 및 디바이스를 사용할 수 있게 되면서 모든 Cisco 환경에서 유리합니다.ISL과 802.1Q 구현이 모두 완성되었지만, IEEE 표준은 궁극적으로 현장 노출 및 네트워크 분석기 지원과 같은 타사 지원 기능이 더욱 강화될 것입니다.802.1Q의 캡슐화 오버헤드가 ISL에 비해 낮다는 점은 802.1Q에 비해 약간 낮은

수준입니다.

DTP를 사용하는 스위치 간에 캡슐화 유형이 협상되므로, 양쪽 모두 지원하는 경우 기본적으로 ISL이 승자로 선택되어 있으므로 dot1q를 지정하려면 이 명령을 실행해야 합니다.

```
set trunk mod/port mode dot1q
```

VLAN 1이 트렁크에서 지워진 경우(이 문서의 대역 내 관리 섹션에서 설명한 대로 사용자 데이터는 전송되거나 수신되지 않지만) NMP는 VLAN 1의 CDP 및 VTP와 같은 제어 프로토콜을 계속 전달합니다.

또한 이 문서의 VLAN 1 섹션에서 설명한 대로 트렁킹 시 VLAN 1에서 CDP, VTP 및 PAgP 패킷이 항상 전송됩니다.dot1q 캡슐화를 사용할 때 스위치의 네이티브 VLAN이 변경되면 이러한 제어 프레임에는 VLAN 1로 태그가 지정됩니다.라우터로 dot1q 트렁킹이 활성화되고 스위치에서 네이티브 VLAN이 변경되면 VLAN 1의 하위 인터페이스가 태그 있는 CDP 프레임을 수신하고 라우터에서 CDP 네이버 가시성을 제공해야 합니다.

참고: 네이티브 VLAN의 암시적 태깅으로 인해 dot1q가 발생할 수 있는 보안 고려 사항은 라우터가 없는 VLAN에서 다른 VLAN으로 프레임을 보낼 수 있기 때문입니다.VLAN 구현에 취약성이 있습니까? 를 참조하십시오. 자세한 내용을 확인하십시오.해결 방법은 최종 사용자 액세스에 사용되지 않는 트렁크의 네이티브 VLAN에 VLAN ID를 사용하는 것입니다.대부분의 Cisco 고객은 VLAN 1을 트렁크에 기본 VLAN으로 남겨 두고 액세스 포트를 VLAN 1이 아닌 VLAN에 할당하여 이를 간단하게 달성할 수 있습니다.

트렁킹 모드

DTP는 2세대 DISL(Dynamic ISL)이며, 구성된 캡슐화 유형, 네이티브 VLAN, 하드웨어 기능 등 ISL 또는 802.1Q 프레임을 전송하는 데 관련된 여러 매개 변수가 트렁크의 양쪽 끝에 있는 스위치에 의해 합의되도록 하기 위해 존재합니다.또한 포트와 인접 디바이스가 일관된 상태를 유지하도록 하여 잠재적으로 심각한 보안 위험 요소인 태그 있는 프레임이 플러딩되는 비 트렁크 포트로부터 보호합니다.

운영 개요

DTP는 스위치 포트와 인접 디바이스 간에 컨피그레이션 매개변수를 협상하는 L2 프로토콜입니다.또 다른 멀티캐스트 MAC 주소(**01-00-0c-cc-cc-cc-cc**)와 SNAP 프로토콜 유형 0x2004를 사용합니다. 이 표는 구성 모드에 대한 요약입니다.

모드	함수	전송된 DTP 프레임	최종 상태(로컬 포트)
( )	포트가 링크를 트렁크로 변환할 수 있도록 합니다.인접 포트가 on 또는 모드로 설정된 경우 포트는 트렁크 포트 됩니다.	네, 주기적이에요	트렁킹
	포트를 영구 트렁킹 모드로 설정하고 링크를 트렁크로 변환하기	네, 주기적이에요	**조건 없이**

	위해 협상합니다.인접 포트가 변경에 동의하지 않더라도 포트는 트렁크 포트가 됩니다.		트렁킹.
	포트를 영구 트렁킹 모드로 전환하지만 포트가 DTP 프레임을 생성하지 못하도록 합니다.트렁크 링크를 설정하려면 인접 포트를 트렁크 포트로 수동으로 구성해야 합니다.이는 DTP를 지원하지 않는 디바이스에 유용합니다.	아니요	**조건 없이** 트렁킹.
	포트가 링크를 트렁크 링크로 변환하려고 적극적으로 시도합니다.인접 포트가 on, 또는 모드 설정된 경우 포트는 트렁크 포트가 됩니다.	네, 주기적이에요	원격 모드가 , 또는 는 경우에만 트렁킹 상태로 .
	포트를 영구 비트렁킹 모드로 설정하고 링크를 비트렁크 링크로 변환하도록 협상합니다.인접 포트가 변경에 동의하지 않더라도 포트는 트렁크가 아닌 포트가 됩니다.	아니요(켜져 있음), 그러나 전송 시 변경 후 원격 엔드 탐지를 가속화하기 위해 알림 .	비트렁킹

다음은 프로토콜의 몇 가지 주요 특징입니다.

- DTP는 Point-to-Point 연결을 가정하고, Cisco 디바이스는 Point-to-Point인 802.1Q 트렁크 포트만 지원합니다.
- DTP 협상 중에 포트는 STP에 참여하지 않습니다.포트가 세 가지 DTP 유형(액세스, ISL 또는 802.1Q) 중 하나가 된 후에만 포트가 STP에 추가됩니다.그렇지 않으면 PAgP가 구성된 경우 포트가 STP에 참여하기 전에 다음 프로세스를 실행합니다.
- 포트가 ISL 모드에서 트렁킹 중인 경우 DTP 패킷은 VLAN 1에서 전송되고, 그렇지 않은 경우(802.1Q 트렁킹 또는 트렁킹 없음 포트의 경우) 네이티브 VLAN에서 전송됩니다.
- 권장 모드에서 DTP 패킷은 **VTP 도메인 이름**(협상된 트렁크가 작동하려면 일치해야 함)과 트렁크 컨피그레이션 및 **관리자 상태**를 전송합니다.
- 협상 중에는 1초마다, 그 후 30초마다 메시지가 전송됩니다.
- 포트가 종료되 상태 on, `nonegotiate` 및 `off`로 명시적으로 지정하는지 알아야 합니다.구성이 잘못되면 한 쪽이 트렁킹을 하고 다른 쪽은 트렁킹을 하지 않는 위험/일관성 없는 상태가 될 수 있습니다.
- on, `auto` 또 모드 포트는 주기적으로 DTP 프레임을 전송합니다. 또는 모드의 포트에 5분 내에 DTP 패킷이 표시되지 않으면 비 트렁크로 설정됩니다.

ISL에 대한 자세한 내용은 Catalyst 5500/5000 및 6500/6000 제품군 스위치에서 ISL 트렁킹 구성을 참조하십시오.자세한 802.1Q에 대한 자세한 내용은 Cisco CatOS 시스템 소프트웨어를 사용한 802.1Q 캡슐화를 사용하는 Catalyst 4500/4000, 5500/500 및 6500/6000 Series 스위치 간 트렁킹을 참조하십시오.

권장 사항

Cisco는 양쪽 끝에 트렁크 컨피그레이션을 권장합니다.이 모드에서는 네트워크 운영자가 syslog 및 명령줄 상태 메시지를 신뢰하여 포트가 작동 및 트렁킹(on 모드와 달리, 네이버가 잘못 구성되었더라도 포트가 표시되도록 할 수 있습니다.또한 모드 트렁크는 링크의 한 쪽이 트렁크 상태가 되거나 트렁크 상태가 될 수 없는 상황에서 안정성을 제공합니다. 모드를 설정하려면 다음 명령을 실행합니다.

```
set trunk mod/port desirable ISL | dot1q
```

참고: 트렁크가 아닌 모든 포트에서 끄도록 트렁크를 설정합니다.따라서 호스트 포트를 가동할 때 낭비되는 협상 시간을 줄일 수 있습니다.이 명령은 set port host **명령**을 사용할 **때도 실행됩니다.**자세한 내용은 STP 섹션을 참조하십시오.포트 범위에서 트렁크를 비활성화하려면 다음 명령을 실행합니다.

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

기타 옵션

또 다른 일반적인 고객 컨피그레이션은 디스트리뷰션 레이어에서만 모드를 사용하고 액세스 레이어에서는 가장 간단한 기본 컨피그레이션(모드)을 사용합니다.

Catalyst 2900XL, Cisco IOS 라우터 또는 기타 공급업체 디바이스와 같은 일부 스위치는 현재 DTP를 통한 트렁크 협상을 지원하지 않습니다.Catalyst 4500/4000, 5500/5000 및 6500/6000 스위치에서 비협상 모드를 사용하여 이러한 디바이스로 포트를 무조건 트렁킹하도록 설정할 수 있으며, 이는 캠퍼스 전체에서 공통된 설정을 표준화하는 데 도움이 됩니다.또한 "전체" 링크 초기화 시간을 줄이기 위해 모드를 구현할 수 있습니다.

참고: 채널 모드 및 STP 컨피그레이션과 같은 계수도 초기화 시간에 영향을 줄 수 있습니다.

비협상 모드를 설정하려면 다음 명령 실행합니다.

```
set trunk mod/port nonegotiate ISL | dot1q
```

브리징을 때 **on** 모드에서 수신한 일부 DTP 프레임이 트렁크 포트로 다시 들어올 수 있으므로 Cisco는 Cisco IOS 라우터와의 연결이 있을 때 논협상**을** 권장합니다.DTP 프레임을 수신하면 스위치 포트가 불필요하게 재협상(또는 트렁크를 다운 및 위로)을 시도합니다.nonegotiate가 활성화된 경우 스위치는 DTP 프레임을 전송하지 않습니다.

스패닝 트리 프로토콜

기본 고려 사항

STP(Spanning Tree Protocol)는 이중화된 스위치드 및 브리지 네트워크에서 루프 프리 L2 환경을

유지합니다.STP가 없으면 프레임 루프 및/또는 무한대로 곱하기 때문에 브로드캐스트 도메인의 모든 디바이스가 높은 트래픽으로 인해 지속적으로 중단되므로 네트워크가 용융됩니다.

일부 측면에서 STP는 처음에는 느린 소프트웨어 기반 브리지 사양(IEEE 802.1d)을 위해 개발된 성숙한 프로토콜이지만, 많은 VLAN, 도메인에 있는 많은 스위치, 멀티 벤더 지원 및 새로운 IEEE 개선 사항을 갖춘 대규모 스위치드 네트워크에서 잘 구현하기가 복잡할 수 있습니다.

향후 참조를 위해 CatOS 6.x는 MISTP, 루프 가드, 루트 가드, BPDU 도착 시간 기울이기 감지 같은 새로운 STP 개발을 계속 수행합니다.또한 IEEE 802.1s 공유 스패닝 트리 및 IEEE 802.1w 빠른 컨버전스 스패닝 트리 등 CatOS 7.x에서 표준화된 프로토콜을 사용할 수 있습니다.

운영 개요

VLAN당 루트 브리지 선택은 가장 낮은 루트 BID(Bridge Identifier)로 스위치에 의해 결정됩니다. BID는 스위치 MAC 주소와 결합된 브리지 우선 순위입니다.

처음에는 각 스위치의 BID와 해당 스위치에 도달하는 경로 비용이 포함된 BPDU가 모든 스위치에서 전송됩니다.이렇게 하면 루트 브리지 및 루트에 대한 가장 저렴한 경로를 확인할 수 있습니다.루트에서 BPDU에 전달되는 추가 컨피그레이션 매개변수는 전체 네트워크에서 일관된 타이머를 사용하도록 로컬에서 구성된 매개변수를 재정의합니다.

그런 다음 토폴로지는 다음 단계를 통해 통합됩니다.

1. 전체 스패닝 트리 도메인에 대해 단일 루트 브리지가 선택됩니다.
2. 루트 브리지를 향하는 루트 포트 하나가 루트 브리지가 아닌 모든 브리지에서 선택됩니다.
3. 모든 세그먼트에서 BPDU 전달을 위해 지정된 포트가 선택됩니다.
4. 지정되지 않은 포트가 차단됩니다.

자세한 내용은 스패닝 트리 구성을 참조하십시오.

기본 타이머 기본값(초)	이름	함수
2		BPDU 전송을 제어합니다.
15	(FWD DELAY)	포트가 수신 및 학습 상태에 얼마나 오래 소요되는지 제어하고 토폴로지 변경 프로세스에 영향을 줍니다(다음 섹션 참조).
20		대체 경로를 찾기 전에 스위치가 현재 토폴로지를 유지하는 시간을 제어합니다.Maxage 초 후에는 BPDU가 오래된 것으로 간주되고 스위치가 차단 포트 풀에서 새 루트 포트를 찾습니다.차단된 포트를 사용할 수 없는 경우 지정된 포트의 루트 자체가 됩니다.

포트 상태	의미	다음 상태에 대한 기본 타이밍
	관리적으로 다운되었습니다.	해당 없음

	BPDU 수신 및 사용자 데이터 중지	BPDU의 수신 모니터링Maxage 만료에 20초 정도 기다리거나 직접/로컬 링크 오류가 감지되면 즉시 변경합니다.
	BPDU를 보내거나 수신하여 차단이 필요한지 여부를 확인합니다.	FWDDELAY 타이머(대기 15초)
	토폴로지/CAM 테이블을 빌드하고 있습니다.	FWDDELAY 타이머(대기 15초)
	데이터 전송/수신	
	총 기본 토폴로지 변경:	**20 + 2(15) = 최대 만료 대기 시 50초, 직접 연결 실패 시 30초**

STP의 두 가지 유형의 BPDU는 구성 BPDU와 TCN(Topology Change Notification) BPDU입니다.

구성 BPDU 흐름

컨피그레이션 BPDU는 루트 브리지의 모든 포트에서 hello-interval(hello-interval)마다 소싱되며 이후 모든 리프 스위치로 플로우되어 스패닝 트리의 상태를 유지합니다.안정된 상태의 BPDU 흐름은 단방향입니다.루트 포트 및 차단 포트는 컨피그레이션 BPDU만 수신하고, 지정된 포트는 컨피그레이션 BPDU만 전송합니다.

루트에서 스위치에서 수신하는 모든 BPDU에 대해 Catalyst central NMP에서 새 BPDU를 처리하여 루트 정보를 포함하는 상태로 전송합니다.즉, 루트 브리지가 손실되거나 루트 브리지에 대한 모든 경로가 손실되면 BPDU의 수신은 중지됩니다(최대 타이머가 다시 선택되기 시작할 때까지).

TCN BPDU 흐름

TCN BPDU는 리프 스위치에서 소싱되고 스패닝 트리에서 토폴로지 변경이 감지되면 루트 브리지로 이동합니다.루트 포트는 TCN만 전송하고 지정된 포트는 TCN만 수신합니다.

TCN BPDU는 루트 리지를 향해 이동하며 각 단계에서 인식되므로 신뢰할 수 있는 메커니즘입니다.루트 브리지에 도착하면 루트 브리지는 최대 기간 `+ fwddelay` **시간**에 대해 설정된 TCN 플래그로 구성 BPDU를 소싱하여 변경 사항이 발생했음을 전체 도메인**에** 알립니다(기본값 35초). 이렇게 하면 모든 스위치가 기본 CAM 에이징 시간을 5분(기본값)에서 fwddelay로 지정된 간격**(기본값** 15초)으로 변경합니다. 자세한 내용은 스패닝 트리 프로토콜 토폴로지 변경 이해를 참조하십시오.

스패닝 트리 모드

VLAN과 스패닝 트리의 상관관계를 분석할 수 있는 방법에는 세 가지가 있습니다.

- 모든 VLAN을 위한 단일 스패닝 트리 또는 IEEE 802.1Q와 같은 모노 스패닝 트리 프로토콜
- VLAN당 스패닝 트리 또는 Cisco PVST와 같은 공유 스패닝 트리
- VLAN 집합당 스패닝 트리 또는 Cisco MISTP 및 IEEE 802.1s와 같은 다중 스패닝 트리

모든 VLAN에 대한 모노 스패닝 트리는 하나의 활성 토폴로지만 허용하므로 로드 밸런싱이 없습니다.모든 VLAN에 대해 STP가 차단된 포트 블록이며 데이터를 전송하지 않습니다.

VLAN당 하나의 스패닝 트리를 통해 로드 밸런싱을 허용하지만 VLAN 수가 증가함에 따라 더 많은

BPDU CPU 처리가 필요합니다.CatOS 릴리스 노트는 스위치당 스패닝 트리에서 권장하는 논리적 포트 수에 대한 지침을 제공합니다.예를 들어 Catalyst 6500/6000 Supervisor Engine 1 공식은 다음과 같습니다.

포트 수 + (트렁크 수 * 트렁크의 VLAN 수) < 4000

Cisco MISTP와 새로운 802.1s 표준은 두 개의 활성 STP 인스턴스/토폴로지만 정의하고 모든 VLAN을 이 두 트리 중 하나에 매핑하는 것을 허용합니다.이 기술을 통해 STP는 로드 밸런싱이 활성화되는 동안 수천 개의 VLAN으로 확장할 수 있습니다.

BPDU 형식

IEEE 802.1Q 표준을 지원하기 위해 IEEE 802.1Q 모노 스패닝 트리 리전 간의 터널링 지원을 추가하여 기존 Cisco STP 구현이 PVST+로 확장되었습니다.따라서 PVST+는 IEEE 802.1Q MST 및 Cisco PVST 프로토콜 모두와 호환되며 추가 명령이나 구성이 필요하지 않습니다.또한 PVST+는 스위치 간에 포트 트렁킹 및 VLAN ID의 컨피그레이션 불일치가 발생하지 않도록 확인 메커니즘을 추가합니다.

다음은 PVST+ 프로토콜의 몇 가지 주요 작동 기능입니다.

- PVST+는 802.1Q 트렁크를 통해 CST(Common Spanning Tree)를 통해 802.1Q 모노 스패닝 트리와 상호 운용됩니다.CST는 항상 VLAN 1에 있으므로 다른 벤더와 상호 운용되도록 트렁크에서 이 VLAN을 활성화해야 합니다.CST BPDU는 IEEE Standard Bridge-Group(MAC Address 01-80-c2-00-00-00, DSAP 42, SSAP 42)으로 전송되며 항상 태그가 지정되지 않습니다. 설명을 완성하기 위해 병렬 BPDU 집합도 VLAN 1의 Cisco 공유 스패닝 트리 MAC 주소로 전송됩니다.
- PVST+는 802.1Q VLAN 영역 전반에 멀티캐스트 데이터로 PVST BPDU를 터널링합니다.Cisco 공유 스패닝 트리 BPDU는 트렁크의 각 VLAN에 대해 MAC 주소 01-00-0c-cc-cc-cd(SNAP HDLC 프로토콜 유형 0x010b)로 전송됩니다.BPDU는 네이티브 VLAN에서 태그가 지정되지 않으며 다른 모든 VLAN에 대해 태그가 지정됩니다.
- PVST+는 포트 및 VLAN 불일치를 확인합니다.PVST+는 전달 루프를 방지하기 위해 일관되지 않은 BPDU를 수신하는 포트를 차단합니다.또한 syslog 메시지를 통해 컨피그레이션 불일치에 대해 사용자에게 알립니다.
- PVST+는 ISL 트렁크에서 PVST를 실행하는 기존 Cisco 스위치와 역호환됩니다.ISL 캡슐화된 BPDU는 여전히 IEEE MAC 주소를 사용하여 전송되거나 수신됩니다.즉, 각 BPDU 유형은 링크-로컬입니다.번역 문제가 없습니다.

권장 사항

모든 Catalyst 스위치에는 기본적으로 STP가 활성화되어 있습니다.이는 L2 루프를 포함하지 않는 설계를 선택하더라도 STP가 차단된 포트를 능동적으로 유지 관리하는 의미에서 활성화되지 않도록 하는 것이 좋습니다.

```
set spantree enable all
!--- This is the default.
```

Cisco에서는 다음과 같은 이유로 STP를 사용하도록 설정하는 것이 좋습니다.

- 루프가 있는 경우(잘못된 패치, 잘못된 케이블 등으로 유발됨) STP는 멀티캐스트 및 브로드캐

스트 데이터로 인해 네트워크에 해로운 영향을 주지 않습니다.
- EtherChannel이 중단되는 것을 방지합니다.
- 대부분의 네트워크는 STP로 구성되어 있어 필드 노출 가능성이 극대화됩니다.노출이 더 많을수록 일반적으로 안정적인 코드와 같습니다.
- 이중 연결 NIC가 잘못 동작하지 않도록 보호(또는 서버에서 브리징이 활성화됨).
- 많은 프로토콜(예: PAgP, IGMP 스누핑, 트렁킹)의 소프트웨어는 STP와 밀접하게 관련되어 있습니다.STP 없이 실행하면 원치 않는 결과가 발생할 수 있습니다.

타이머를 변경하지 마십시오. 이 경우 안정성에 부정적인 영향을 줄 수 있습니다.구축된 대부분의 네트워크는 조정되지 않습니다.Hello-interval 및 Maxage와 같이 명령줄을 통해 액세스할 수 있는 단순 STP 타이머는 다른 가정 및 내장 타이머의 복잡한 집합으로 구성되어 있으므로 타이머를 조정하고 모든 결과를 고려하기가 어렵습니다.게다가, UDLD 보호를 손상시킬 위험이 있다.

사용자 트래픽을 관리 VLAN에서 분리하는 것이 좋습니다.특히 이전 Catalyst 스위치 프로세서의 경우 관리 VLAN을 사용자 데이터와 분리함으로써 STP 문제를 방지하는 것이 좋습니다.동작하지 않는 하나의 엔드 스테이션은 하나 이상의 BPDU를 놓칠 수 있는 브로드캐스트 패킷으로 수퍼바이저 엔진 프로세서를 사용할 수 있도록 해줍니다.그러나 CPU가 더 강력한 최신 스위치와 조절(throttling) 제어 기능이 있어 이러한 고려 사항이 해소됩니다.자세한 내용은 이 문서의 대역 내 관리 섹션을 참조하십시오.

이중화를 지나치게 설계하지 마십시오.이로 인해 문제 해결이 어려워질 수 있습니다. 너무 많은 차단 포트가 장기간 안정성에 부정적인 영향을 미칩니다.**총 SPT 지름을 7홉으로 유지합니다.**더 작은 스위치드 도메인, STP 삼각형, 결정론적 차단 포트(기가비트 캠퍼스 네트워크 설계 - 원리 및 아키텍처에 설명)를 사용하여 가능한 한 Cisco 멀티레이어 모델을 설계해 보십시오.

루트 기능 및 차단된 포트가 있는 위치에 영향을 미치고 이를 파악하여 토폴로지 다이어그램에 문서화합니다.차단된 포트는 STP 트러블슈팅을 시작하는 곳입니다. 이러한 포트가 차단을 차단에서 포워딩으로 변경된 것은 근본 원인 분석의 핵심 부분입니다.**분산 및 코어 레이어를 루트/보조 루트**의 **위치로 선택합니다.** 이는 네트워크에서 가장 안정적인 부분으로 간주되기 때문입니다.L2 데이터 포워딩 경로를 사용하는 최적의 L3 및 HSRP 오버레이를 확인합니다.이 명령은 브리지 우선순위를 구성하는 매크로입니다.root는 기본값(32768)보다 훨씬 낮게 설정되지만 루트 보조 집합은 기본값보다 상당히 낮습니다.

```
set spantree root secondary vlan range
```

참고: 이 매크로는 루트 우선 순위를 8192(기본값), 현재 루트 우선 순위 - 1(다른 루트 브리지를 아는 경우) 또는 현재 루트 우선 순위(MAC 주소가 낮은 경우 현재 루트로 설정)로 설정합니다.

트렁크 포트에서 불필요한 VLAN을 정리합니다(양방향 연습). 이렇게 하면 특정 VLAN이 필요하지 않은 네트워크의 일부에서 STP 및 NMP 처리 오버헤드의 지름이 제한됩니다.VTP 자동 정리는 트렁크에서 STP를 제거하지 않습니다.자세한 내용은 이 문서의 VTP 섹션을 참조하십시오.CatOS 5.4 이상을 사용하는 트렁크에서 기본 VLAN 1을 제거할 수도 있습니다.

자세한 내용은 스패닝 트리 프로토콜 문제 및 관련 설계 고려 사항을 참조하십시오.

기타 옵션

Cisco는 또 다른 STP를 VLAN-**bridge라고 합니다.**이 프로토콜은 대상 MAC 주소 **01-00-0c-cd-cd-ce** 및 프로토콜 유형 0x010c를 사용하여 작동합니다.

이 기능은 VLAN에서 실행되는 IEEE 스패닝 트리 인스턴스를 방해하지 않고 VLAN 간에 라우팅할

수 없거나 레거시 프로토콜을 연결해야 하는 경우에 가장 유용합니다.브리징되지 않은 트래픽에 대한 VLAN 인터페이스가 L2 트래픽에 대해 차단될 경우(그리고 IP VLAN과 동일한 STP에 참여하는 경우 이러한 현상이 쉽게 발생할 수 있음), 오버레이되는 L3 트래픽도 우연히 제거되어 원치 않는 부작용이 발생합니다.따라서 VLAN-bridge는 IP 트래픽에 영향을 주지 않고 조작할 수 있는 별도의 토폴로지를 제공하는 브리지 프로토콜 STP의 별도의 인스턴스입니다.

Cisco는 MSFC와 같은 Cisco 라우터의 VLAN 간에 브리징이 필요한 경우 VLAN 브리지를 실행하는 것이 좋습니다.

PortFast

PortFast는 액세스 포트에서 일반 스패닝 트리 작업을 우회하여 링크 초기화 후 연결하는 데 필요한 엔드포인트와 서비스 간의 연결 속도를 높이는 데 사용됩니다.IPX/SPX와 같은 일부 프로토콜에서는 GNS 문제를 방지하기 위해 링크 상태가 발생한 후 바로 포워딩 모드에서 액세스 포트를 확인하는 것이 중요합니다.

자세한 내용은 Portfast 및 기타 명령을 사용하여 워크스테이션 시작 연결 지연 문제 해결을 참조하십시오.

운영 개요

PortFast는 링크가 실행 중인 것으로 알려진 후 포트를 모드로 STP의 정상 및 상태를 건너뜁니다.이 기능이 활성화되지 않은 경우 STP는 포트를 모드로 이동할 준비가 될 때까지 모든 사용자 데이터를 삭제합니다.이 작업은 ForwardDelay 시간 최대 2배(기본적으로 총 30초)가 걸릴 수 있습니다.

또한 PortFast 모드에서는 포트 상태가 에서 포워딩 변경될 때마다 STP TCN이 생성되지 않습니다.TCN은 자체적으로 문제가 되지 않지만 TCN의 물결이 루트 브리지(일반적으로 PC를 켜는 아침에)에 도달하면 불필요하게 통합 시간을 연장할 수 있습니다.

STP PortFast는 멀티캐스트 CGMP 및 Catalyst 5500/5000 MLS 네트워크 모두에서 특히 중요합니다.이러한 환경의 TCN은 정적 CGMP CAM 테이블 엔트리를 오래된 상태로 만들어 다음 IGMP 보고서가 나올 때까지 멀티캐스트 패킷 손실이 발생하고 다시 구축해야 하는 MLS 캐시 엔트리를 플러시하여 캐시 크기에 따라 라우터 CPU가 급증할 수 있습니다.(Catalyst 6500/6000 MLS 구현 및 IGMP 스누핑에서 학습한 멀티캐스트 항목은 영향을 받지 않습니다.)

권장 사항

Cisco에서는 모든 활성 호스트 포트에 대해 STP PortFast를 활성화하고 스위치 스위치 링크 및 사용하지 않는 포트에 대해서는 비활성화하는 것이 좋습니다.

모든 호스트 포트에 대해 트렁킹 및 채널링을 비활성화해야 합니다.각 액세스 포트는 트렁킹 및 채널링에 기본적으로 활성화되어 있지만 호스트 포트의 설계에서는 스위치 네이버를 예상하지 않습니다.이러한 프로토콜이 협상하도록 남아 있는 경우, 포트 활성화의 후속 지연으로 인해 DHCP 요청과 같은 워크스테이션의 초기 패킷이 전달되지 않는 바람직하지 않은 상황이 발생할 수 있습니다.

CatOS 5.2에서는 매크로 명령을 도입하고, 액세스 포트에 대한 이 컨피그레이션을 구현하고 자동 협상 및 연결 성능을 크게 향상시키는 포트 호스트 *포트 범위*를 설정합니다.

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

참고: PortFast는 스패닝 트리가 해당 포트에서 전혀 실행되지 않음을 의미하지 않습니다.BPDU는 여전히 전송, 수신 및 처리됩니다.

기타 옵션

PortFast BPDU-guard는 비 트렁킹 포트를 해당 포트에서 BPDU가 수신될 때 `errdisable` 상태로 이동하여 루프를 방지하는 방법을 제공합니다.

호스트 포트를 스위치에 연결할 수 없으므로 PortFast에 대해 구성된 액세스 포트에서 BPDU 패킷을 수신해서는 안 됩니다.BPDU가 관찰되면 관리 작업이 필요한 유효하지 않거나 위험한 구성을 나타냅니다.BPDU-guard 기능이 활성화되면 스패닝 트리는 BPDU를 수신하는 PortFast 구성 인터페이스를 STP 상태로 설정하는 대신 종료합니다.

이 명령은 다음과 같이 포트별로 작동하지 않고 스위치 단위로 작동합니다.

```
set spantree portfast bpdu-guard enable
```

포트가 다운되면 네트워크 관리자는 SNMP 트랩 또는 syslog 메시지를 통해 알림을 받습니다 .errdisable 포트에 대한 자동 복구 시간을 구성할 수도 있습니다.자세한 내용은 이 문서의 UDLD 섹션을 참조하십시오.자세한 내용은 Spanning Tree Portfast BPDU Guard Enhancement를 참조하십시오.

참고: 트렁크 포트의 PortFast는 CatOS 7.x에서 도입되었으며 이전 릴리스의 트렁크 포트에는 영향을 미치지 않습니다.트렁크 포트의 PortFast는 L3 네트워크의 컨버전스 시간을 늘리도록 설계되었습니다.이 기능을 보완하기 위해 CatOS 7.x는 포트별로 PortFast BPDU-guard를 구성할 가능성도 도입했습니다.

Uplinkfast

UplinkFast는 네트워크 액세스 레이어에서 직접 링크 장애가 발생한 후 빠른 STP 컨버전스를 제공합니다.STP는 수정하지 않으며, 이 기능의 목적은 일반적인 30초 지연 시간이 아니라 특정 상황에서 컨버전스 시간을 3초 미만으로 단축하는 것입니다.자세한 내용은 Cisco 업링크 고속 기능 이해 및 구성을 참조하십시오.

운영 개요

액세스 레이어에서 Cisco 멀티레이어 설계 모델을 사용하여 포워딩 업링크가 손실되면 차단 업링크가 및 상태를 기다리지 않고 상태로 즉시 이동합니다.

업링크 그룹은 루트 포트 및 백업 루트 포트로 간주할 수 있는 VLAN당 포트 집합입니다.정상적인 조건에서 루트 포트는 루트에 대한 액세스에서 연결을 보장합니다.이 기본 루트 연결이 어떤 이유로든 실패하면 백업 루트 링크가 즉시 작동하므로 컨버전스 지연 시간이 30초 이상 발생하지 않습니다.

이렇게 하면 정상적인 STP 토폴로지 변경 처리 프로세스(및)를 효과적으로 우회하기 때문에 대체

경로를 통해 로컬 엔드포인트에 연결할 수 있는 도메인 스위치를 업데이트하려면 대체 토폴로지 수정 메커니즘이 필요합니다.UplinkFast를 실행하는 액세스 레이어 스위치는 또한 CAM의 각 MAC 주소에 대한 프레임을 멀티캐스트 MAC 주소(01-00-0c-cd-cd-cd, HDLC 프로토콜 0x200a)로 생성하여 도메인의 모든 스위치에서 새 토폴로지로 CAM 테이블을 업데이트합니다.

권장 사항

Cisco에서는 일반적으로 액세스 레이어에서 차단된 포트가 있는 스위치에 대해 UplinkFast를 활성화할 것을 권장합니다.백업 루트 링크에 대한 묵시적 토폴로지 지식이 없는 스위치에서는 사용하지 마십시오. 일반적으로 Cisco 멀티레이어 설계에서 디스트리뷰션 및 코어 스위치가 사용됩니다.운영 네트워크에 지장을 주지 않고 추가할 수 있습니다.UplinkFast를 활성화하려면 다음 명령을 실행합니다.

```
set spantree uplinkfast enable
```

또한 이 명령은 **브리지 우선 순위**를 높게 설정하여 이**가** 루트 브리지가 될 위험을 최소화하고 **포트 우선 순위**가 높은 값을 설정하여 기능을 해제하는 지정된 포트가 되도록 최소화합니다 .UplinkFast가 활성화된 스위치를 복원할 경우 이 기능은 비활성화되고 업링크 데이터베이스는 "clear uplink"로 지워지며 브리지 우선순위는 수동으로 복원됩니다.

참고: 프로토콜 필터링 기능이 활성화된 경우 UplinkFast 명령에 대한 **모든 프로토콜** 키워드가 필요합니다.프로토콜 필터링이 활성화된 경우 CAM은 프로토콜 유형과 MAC 및 VLAN 정보를 기록하므로 각 MAC 주소의 각 프로토콜에 대해 UplinkFast 프레임을 생성해야 합니다.rate 키워드는 업링크 토폴로지 업데이트 프레임의 초당 패킷을 나타냅니다.기본값은 권장 사항입니다.메커니즘이 기본적으로 RSTP에 포함되고 자동으로 활성화되므로 RSTP(Rapid STP) 또는 IEEE 802.1w를 사용하여 BackboneFast를 구성할 필요가 없습니다.

백본Fast

BackboneFast는 간접 링크 장애로부터 신속한 컨버전스를 제공합니다.STP에 기능이 추가됨에 따라 컨버전스 시간은 일반적으로 기본값인 50초에서 30초로 줄일 수 있습니다.

운영 개요

스위치의 루트 포트 또는 차단된 포트가 지정된 브리지에서 하위 BPDU를 수신하면 메커니즘이 시작됩니다.이 문제는 다운스트림 스위치가 루트에 대한 연결이 끊기고 새 루트를 선택하기 위해 자체 BPDU를 보내기 시작할 때 발생할 수 있습니다.하위 **BPDU**는 스위치를 루트 브리지 및 지정된 브리지로 식별합니다.

일반적인 스패닝 트리 규칙에서 수신 스위치는 구성된 최대 에이징 시간(기본적으로 20초)에 대해 하위 BPDU를 무시합니다.그러나 BackboneFast를 사용하면 스위치에서 하위 BPDU를 토폴로지가 변경될 수 있다는 신호로 보고 RLQ(Root Link Query) BPDU를 사용하여 루트 브리지에 대한 대체 경로가 있는지 확인하려고 시도합니다.이 프로토콜 추가를 통해 스위치에서 루트가 여전히 사용 가능한지 확인하고, 포트를 더 짧은 시간 내에 으로 이동하고, 하위 BPDU를 전송한 격리된 스위치에 루트가 여전히 존재함을 알립니다.

프로토콜 작업의 몇 가지 주요 내용은 다음과 같습니다.

- 스위치는 루트 포트만(즉, 루트 브리지 쪽으로) RLQ 패킷을 전송합니다.

- RLQ를 수신하는 스위치는 루트 스위치이거나 루트와의 연결이 끊어진 것을 아는 경우 응답할 수 있습니다.이러한 사실을 모르는 경우 쿼리를 루트 포트로 전달해야 합니다.
- 스위치에서 루트에 대한 연결이 끊어진 경우 이 쿼리에 대해 음수로 응답해야 합니다.
- 회신은 쿼리가 시작된 포트만 전송해야 합니다.
- 루트 스위치는 항상 이 쿼리에 긍정적인 회신을 사용하여 응답해야 합니다.
- 루트가 아닌 포트에서 응답이 수신되면 삭제됩니다.

따라서 최대 기간이 만료되지 않으므로 STP 통합 시간을 최대 20초 단축할 수 있습니다.

자세한 내용은 Catalyst 스위치에서 백본 빠른 구성 및 이해를 참조하십시오.

권장 사항

Cisco의 권장 사항은 STP를 실행하는 모든 스위치에서 BackboneFast를 활성화하는 것입니다.운영 네트워크에 지장을 주지 않고 추가할 수 있습니다.BackboneFast를 활성화하려면 다음 명령을 실행합니다.

```
set spantree backbonefast enable
```

참고: 이 전역 레벨 명령은 모든 스위치가 이해해야 하는 STP 프로토콜에 기능을 추가하므로 도메인의 모든 스위치에 구성해야 합니다.

기타 옵션

BackboneFast는 2900XL 및 3500에서 지원되지 않습니다.스위치 도메인에 Catalyst 4500/4000, 5500/5000 및 6500/6000 스위치 외에 이러한 스위치가 포함된 경우에는 이 스위치를 활성화하지 않아야 합니다.

메커니즘이 기본적으로 포함되고 RSTP에서 자동으로 활성화되므로 RSTP 또는 IEEE 802.1w를 사용하여 BackboneFast를 구성할 필요가 없습니다.

스패닝 트리 루프 가드

Loop Guard는 STP를 위한 Cisco 독점적 최적화 기능입니다.루프 가드는 L2 네트워크를 다음 루프에서 보호합니다.

- 장애가 발생한 네트워크 인터페이스
- 사용 중인 CPU
- BPDU의 정상적인 전달을 방해하는 모든 것

이중화 토폴로지의 차단 포트가 전달 상태로 잘못 전환될 경우 STP 루프가 발생합니다.이러한 전환은 일반적으로 물리적으로 이중화된 토폴로지(차단 포트가 아닐 수도 있음)의 포트 중 하나가 BPDU를 수신하지 않기 때문에 발생합니다.

루프 가드는 포인트 투 포인트 링크로 스위치가 연결된 스위치드 네트워크에서만 유용합니다.대부분의 최신 캠퍼스 및 데이터 센터 네트워크는 이러한 유형의 네트워크입니다.Point-to-Point 링크에서는 지정된 브리지가 하위 BPDU를 전송하거나 링크를 다운하지 않으면 사라질 수 없습니다.STP 루프 가드 기능은 Catalyst 4000 및 Catalyst 5000 플랫폼용 CatOS 버전 6.2(1) 및 Catalyst 6000 플랫폼의 버전 6.2(2)에 도입되었습니다.

루프 가드에 대한 자세한 내용은 Loop Guard 및 BPDU Skew Detection Features를 사용한 Spanning-Tree Protocol 개선 사항을 참조하십시오.

운영 개요

루프 가드는 루트 포트 또는 대체/백업 루트 포트가 BPDU를 수신하는지 확인합니다.포트에서 BPDU를 수신하지 못할 경우 루프 가드는 포트가 다시 BPDU를 수신하기 시작할 때까지 포트를 일관성 없는 상태(차단)로 전환합니다.일관성이 없는 상태의 포트는 BPDU를 전송하지 않습니다.이러한 포트에서 BPDU를 다시 수신하면 포트(및 링크)가 다시 사용 가능한 것으로 간주됩니다.루프 일관성 없는 상태가 포트에서 제거되고, STP는 해당 복구가 자동으로 수행되므로 포트 상태를 결정합니다.

루프 가드는 장애를 격리하고 스패닝 트리가 실패한 링크 또는 브리지 없이 안정적인 토폴로지로 통합되도록 합니다.루프 가드는 사용 중인 STP 버전의 속도를 가진 STP 루프를 방지합니다.STP 자체(802.1d 또는 802.1w) 또는 STP 타이머가 조정되는 시점에 종속되지 않습니다.이러한 이유로, STP를 사용하고 소프트웨어가 기능을 지원하는 토폴로지에서 UDLD와 함께 루프 가드를 구현합니다.

루프 가드가 일관성 없는 포트를 차단하면 이 메시지가 기록됩니다.

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state.
```

BPDU가 루프 불일치 STP 상태의 포트에서 수신되면 포트는 다른 STP 상태로 전환됩니다.수신된 BPDU에 따라 복구가 자동으로 수행되므로 별도의 작업이 필요하지 않습니다.복구 후 이 메시지가 기록됩니다.

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

다른 STP 기능과의 상호 작용

- **루트 가드**루트 가드는 포트를 항상 지정하도록 강제합니다.루프 가드는 포트가 루트 포트 또는 대체 포트인 경우에만 유효합니다.이러한 기능은 상호 배타적입니다.포트에서 루프 가드와 루트 가드를 동시에 활성화할 수 없습니다.
- **Uplinkfast**루프 가드는 UplinkFast와 호환됩니다.루프 가드가 루트 포트를 차단 상태로 설정하면 UplinkFast는 새 루트 포트를 포워딩 상태로 전환합니다.또한 UplinkFast는 루프 불일치 포트를 루트 포트로 선택하지 않습니다.
- **백본Fast**루프 가드는 BackboneFast와 호환됩니다.지정된 브리지에서 오는 하위 BPDU의 수신은 BackboneFast를 트리거합니다.이 링크에서 BPDU가 수신되므로 루프 가드가 활성화되지 않으므로 BackboneFast 및 루프 가드가 호환됩니다.
- **PortFast**PortFast는 연결 즉시 포트를 전달 지정 상태로 전환합니다.PortFast 지원 포트는 루트 또는 대체 포트일 수 없으므로 루프 가드 및 PortFast는 함께 사용할 수 없습니다.
- **PAgP**루프 가드는 STP에 알려진 포트를 사용합니다.따라서 루프 가드는 PAgP가 제공하는 논리적 포트의 추상화를 활용할 수 있습니다.그러나 채널을 구성하려면 채널에서 그룹화된 모든 물리적 포트에는 호환 가능한 컨피그레이션이 있어야 합니다.PAgP는 모든 물리적 포트에서 루프 가드의 균일한 컨피그레이션을 적용하여 채널을 구성합니다.**참고:** EtherChannel에서 루프 가드를 구성할 때 다음 사항이 주의 사항입니다.STP는 항상 BPDU를 전송하기 위해 채널의 첫 번째 운영 포트를 선택합니다.해당 링크가 단방향으로 되면 루프 가드는 채널 기능의 다른 링크가 제대로 작동하더라도 채널을 차단합니다.루프 가드에 의해 이미 차단된 포트가 채널을 형성하기 위해 함께 그룹화되면 STP는 해당 포트에 대한 모든 상태 정보를 잃게 됩니다.새 채널 포

트는 지정된 역할로 전달 상태를 얻을 수 있습니다.루프 가드에 의해 채널이 차단되고 채널이 끊기면 STP에서 모든 상태 정보를 잃게 됩니다.개별 물리적 포트는 채널을 형성하는 링크 중 하나 이상이 단방향인 경우에도 지정된 역할로 전달 상태를 얻을 수 있습니다.이 목록의 마지막 두 사례에서는 UDLD가 실패를 탐지할 때까지 루프가 발생할 가능성이 있습니다.그러나 루프 가드는 루프를 탐지할 수 없습니다.

루프 가드 및 UDLD 기능 비교

루프 가드 기능 및 UDLD 기능이 부분적으로 중첩됩니다.둘 다 단방향 링크로 인해 발생하는 STP 장애로부터 보호합니다.그러나 이 두 가지 기능은 문제에 대한 접근 방식과 기능에서도 다릅니다.특히 UDLD에서 감지할 수 없는 단방향 장애(예: BPDU를 전송하지 않는 CPU에 의한 장애)가 있습니다.또한 적극적인 STP 타이머와 RSTP 모드를 사용하면 UDLD에서 장애를 탐지하기 전에 루프가 발생할 수 있습니다.

루프 가드는 공유 링크 또는 링크 연결 이후 링크가 단방향인 상황에서 작동하지 않습니다.링크 시작 이후 링크가 단방향인 경우 포트는 BPDU를 수신하지 않으며 지정됩니다.이 동작은 정상일 수 있으므로 루프 가드가 이 특정 사례를 다루지 않습니다.UDLD는 이러한 시나리오에 대한 보호를 제공합니다.

최고 수준의 보호를 제공하려면 UDLD와 루프 가드를 모두 활성화합니다.루프 가드*와 UDLD 기능* 비교*에 대해 Loop Guard* 및 BPDU Skew Detection 기능을 사용하는 스패닝 트리 프로토콜 개선 사항의 Loop Guard vs. Unidirectional Link Detection 섹션을 참조하십시오.

권장 사항

물리적 루프가 있는 스위치 네트워크에서 루프 가드를 전역적으로 활성화하는 것이 좋습니다.Catalyst 소프트웨어 버전 7.1(1)에서는 모든 포트에서 loop guard를 전역적으로 활성화할 수 있습니다.이 기능은 모든 포인트 투 포인트 링크에서 활성화됩니다.링크의 듀플렉스 상태가 포인트-투-포인트 링크를 탐지합니다.듀플렉스가 꽉 차면 해당 링크는 포인트-투-포인트로 간주됩니다.전역 루프 가드를 활성화하려면 이 명령을 실행합니다.

```
set spantree global-default loopguard enable
```

기타 옵션

전역 루프 가드 컨피그레이션을 지원하지 않는 스위치의 경우 포트 채널 포트를 포함하는 모든 개별 포트에서 이 기능을 활성화합니다.지정된 포트에서 loop guard를 활성화할 경우 아무런 이점이 없지만, 이러한 지원은 문제가 아닙니다.또한 유효한 스패닝 트리 재컨버전스는 실제로 지정된 포트를 루트 포트로 전환할 수 있으므로 이 포트에서 이 기능이 유용합니다.루프 가드를 활성화하려면 다음 명령을 실행합니다.

```
set spantree guard loop mod/port
```

루프 프리(loop-free) 토폴로지가 있는 네트워크는 루프가 실수로 발생하는 경우에도 루프 가드의 이점을 계속 누릴 수 있습니다.그러나 이러한 유형의 토폴로지에서 루프 가드를 활성화하면 네트워크 격리 문제가 발생할 수 있습니다.루프 프리(loop-free) 토폴로지를 구축하고 네트워크 격리 문제를 방지하려면 이러한 명령을 실행하여 loop guard를 전역적으로 또는 개별적으로 비활성화합니다

.공유 링크에서 루프 가드를 활성화하지 마십시오.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  또는
- ```
  set spantree guard none mod/port
  !--- This is the default port configuration.
  ```

스패닝 트리 루트 가드

루트 가드 기능은 네트워크에서 루트 브리지 배치를 적용하는 방법을 제공합니다.루트 가드는 루트 가드가 활성화된 포트가 지정된 포트인지 확인합니다.일반적으로 루트 브리지 포트는 둘 이상의 루트 브리지 포트가 함께 연결되어 있지 않으면 모두 지정된 포트입니다.브리지가 루트 가드 지원 포트에서 우수한 STP BPDU를 수신하면 브리지는 이 포트를 루트 불일치 STP 상태로 이동합니다.이 근본 일관성 없는 상태는 사실상 수신 대기 상태와 같습니다.이 포트를 통해 전달되는 트래픽이 없습니다.이러한 방식으로 루트 가드는 루트 브리지의 위치를 적용합니다.루트 가드는 CatOS for Catalyst 29xx, 4500/4000, 5500/5000 및 6500/6000 소프트웨어 버전 6.1.1 이상에서 사용할 수 있습니다.

운영 개요

루트 가드는 STP 내장 메커니즘입니다.Root Guard에는 자체 타이머가 없으며 BPDU의 수신에만 의존합니다.루트 가드가 포트에 적용될 때 루트 가드는 포트가 루트 포트가 되는 것을 허용하지 않습니다.BPDU를 수신하면 지정된 포트가 루트 포트가 되는 스패닝 트리 컨버전스가 트리거되면 포트가 루트 일관성 없는 상태로 전환됩니다.이 syslog 메시지는 다음 작업을 보여줍니다.

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

포트가 우수한 BPDU를 전송하지 않게 되면 포트가 다시 차단되지 않습니다.STP를 통해 포트는 수신 상태에서 학습 상태로 전환되며 포워딩 상태로 전환됩니다.복구는 자동이며, 사람의 개입이 필요하지 않습니다.이 syslog 메시지는 다음 예를 제공합니다.

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

루트 가드는 포트를 강제로 지정하며, 루프 가드는 포트가 루트 포트 또는 대체 포트인 경우에만 유효합니다.따라서 두 기능은 상호 배타적입니다.포트에서 루프 가드와 루트 가드를 동시에 활성화할 수 없습니다.

자세한 내용은 스패닝 트리 프로토콜 루트 가드 향상을 참조하십시오.

권장 사항

Cisco에서는 직접 관리 제어하지 않는 네트워크 디바이스에 연결하는 포트에서 루트 가드 기능을 활성화할 것을 권장합니다.루트 가드를 구성하려면 다음 명령을 실행합니다.

```
set spantree guard root mod/port
```

EtherChannel

EtherChannel 기술을 사용하면 여러 채널(Catalyst 6500/6000에서 최대 8개)을 단일 논리적 링크로 역멀티플렉싱할 수 있습니다.각 플랫폼은 다음 구현과 다르지만 공통 요구 사항을 이해하는 것이 중요합니다.

- 여러 채널을 통해 통계적으로 프레임을 다중화하는 알고리즘
- STP의 단일 인스턴스를 실행할 수 있도록 논리 포트 생성
- PAgP 또는 LACP(Link Aggregation Control Protocol)와 같은 채널 관리 프로토콜

프레임 멀티플렉싱

EtherChannel은 구성 요소 10/100 또는 기가비트 링크에 걸쳐 프레임을 효율적으로 멀티플렉싱하는 프레임 배포 알고리즘을 포함합니다.플랫폼당 알고리즘의 차이는 각 하드웨어 유형의 기능에서 프레임 헤더 정보를 추출하여 총판사를 결정할 수 있다는 점에서 발생합니다.

로드 분배 알고리즘은 두 채널 제어 프로토콜 모두에 대한 전역 옵션입니다.IEEE 표준에는 특정 배포 알고리즘이 필요하지 않으므로 PAgP 및 LACP는 프레임 배포 알고리즘을 사용합니다.그러나 디스트리뷰션 알고리즘은 프레임을 수신할 때 알고리즘이 지정된 대화의 일부이거나 프레임을 중복하는 프레임을 잘못 정렬하지 않도록 합니다.

참고: 다음 정보를 고려해야 합니다.

- Catalyst 6500/6000은 Catalyst 5500/5000보다 최신 스위칭 하드웨어를 갖추고 있으며, 단순한 MAC L2 정보보다 지능적인 멀티플렉싱 결정을 내리기 위해 유선 속도로 IP Layer 4(L4) 정보를 읽을 수 있습니다.
- Catalyst 5500/5000 기능은 모듈에 EBC(Ethernet Bundling Chip)가 존재하는 것에 따라 달라집니다.show port capabilities *mod/port* 명령은 각 포트에서 가능한 작업을 확인합니다.

나열된 각 플랫폼에 대한 프레임 분포 알고리즘을 자세히 보여 주는 이 표를 참조하십시오.

플랫폼	채널 로드 밸런싱 알고리즘
Catalyst 5500/5000 시리즈	필요한 모듈이 포함된 Catalyst 5500/5000을 사용하면 FEC[1]당 2~4개의 링크가 있어야 하지만 동일한 모듈에 있어야 합니다.소스 및 대상 MAC 주소 쌍은 프레임 전달을 위해 선택한 링크를 결정합니다.X-OR 작업은 소스 MAC 주소 및 대상 MAC 주소의 최소 중요 2비트에서 수행됩니다.이 작업을 수행하면 4개의 결과 중 하나가 생성됩니다.(0), (0 1), (10) 또는 (1). 이러한 각 값은 FEC 번들의 링크를 가리킵니다.2포트 Fast EtherChannel의 경우 X-OR 작업에는 단일 비트만 사용됩니다.소스/목적지 쌍의 한 주소가 일정인 경우 상황이 발생할 수 있습니다.예를 들어, 대상은 서버일 수도 있고, 심지어 라우터일 수도 있습니다.이 경우 소스 주소가 항상 다르기 때문에 통계 로드 밸런싱이 표시됩니다.
Catalyst 4500	Catalyst 4500/4000 EtherChannel은 각 프레임의 소스 및 목적지 MAC 주소의 하위 비트를 기반으로 채널(단일 모듈)의 링크에 프레임을 배포합니다

/4000 시리즈	.Catalyst 5500/5000과 비교했을 때, 알고리즘은 더 관련되어 있으며 MAC DA(바이트 3, 5, 6), SA(바이트 3, 5, 6), 인그레스 포트 및 VLAN ID의 이러한 필드에 대한 결정적 해시를 사용합니다.프레임 배포 방법을 구성할 수 없습니다.
Catalyst 6500/6000 시리즈	Supervisor Engine 하드웨어에 따라 두 가지 가능한 해싱 알고리즘이 있습니다.해시는 하드웨어에서 구현된 77도 다항식이며, 모든 경우 MAC 주소, IP 주소 또는 IP TCP/UDP[2] 포트 번호를 사용하여 알고리즘을 적용하여 3비트 값을 생성합니다.이 작업은 소스 주소와 대상 주소 모두에 대해 별도로 수행됩니다.그런 다음 XORd를 통해 패킷의 전달에 사용되는 채널의 포트를 결정하는 데 사용되는 또 다른 3비트 값을 생성합니다.Catalyst 6500/6000의 채널은 모든 모듈의 포트 간에 구성할 수 있으며 최대 8개의 포트일 수 있습니다.

[1] FEC = Fast EtherChannel

[2] UDP = 사용자 데이터그램 프로토콜

이 표는 다양한 Catalyst 6500/6000 Supervisor Engine 모델에서 지원되는 배포 방법과 기본 동작을 나타냅니다.

하드웨어	설명	배포 방법
WS-F6020(L2 엔진)	초기 Supervisor Engine 1	L2 MAC:SA;DA;SA 및 DA
WS-F6020A(L2 엔진) WS-F6K-PFC(L3 엔진)	이후 Supervisor Engine 1 및 Supervisor Engine 1A/PFC1	L2 MAC:SA;DA;SA 및 DA L3 IP:SA;DA;SA 및 DA(기본값)
WS-F6K-PFC2	Supervisor Engine 2/PFC2(CatOS 6.x 필요)	L2 MAC:SA;DA;SA 및 DA L3 IP:SA;DA;SA & DA(기본값) L4 세션:S 포트;D 포트;S & D 포트(기본값)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Supervisor Engine 720/PFC3A(CatOS 8.1.x 필요) Supervisor Engine 720/Supervisor Engine 32/PFC3B(CatOS 8.4.x 필요) Supervisor Engine 720/PFC3BXL(CatOS 8.3.x 필요)	L2 MAC:SA;DA;SA 및 DA L3 IP:SA;DA;SA & DA(기본값) L4 세션:S 포트;D 포트;S & D 포트 IP-VLAN-L4 세션:SA 및 VLAN & S 포트;DA 및 VLAN 및 D 포트;SA & DA & VLAN & S 포트 및 D 포트

참고: L4 배포에서는 처음 조각화된 패킷이 L4 배포를 사용합니다.모든 후속 패킷은 L3 배포를 사용합니다.

다른 플랫폼에서 EtherChannel 지원에 대한 자세한 내용 및 구성 및 문제 해결 방법은 다음 문서에서 확인할 수 있습니다.

- Catalyst 스위치의 EtherChannel 로드 밸런싱 및 이중화 이해
- CatOS 시스템 소프트웨어를 실행하는 Catalyst 4500/4000, 5500/5000 및 6500/6000 스위치 간 EtherChannel 구성
- Catalyst 6500/6000과 Catalyst 4500/4000 간 LACP(802.3ad) 구성
- 레이어 3 및 레이어 2 EtherChannel 구성

권장 사항

Catalyst 6500/6000 Series 스위치는 기본적으로 IP 주소별로 로드 밸런싱을 수행합니다.이는 IP가 주요 프로토콜이라고 가정할 때 CatOS 5.5에서 권장됩니다.로드 밸런싱을 설정하려면 다음 명령을 실행합니다.

```
set port channel all distribution ip both
!--- This is the default.
```

L2 MAC 주소별 Catalyst 4500/4000 및 5500/5000 시리즈 프레임 분배는 대부분의 네트워크에서 허용됩니다.그러나 채널을 통해 통신하는 두 개의 기본 디바이스만 있는 경우(SMAC와 DMAC이 일정함) 모든 트래픽에 동일한 링크가 사용됩니다. 일반적으로 서버 백업 및 기타 대용량 파일 전송 또는 두 라우터 간의 전송 세그먼트에 대한 문제가 될 수 있습니다.

논리적 집계 포트(agport)는 SNMP에서 별도의 인스턴스로 관리할 수 있고 수집한 집계 처리량 통계로 관리할 수 있지만, Cisco에서는 프레임 분배 메커니즘의 작동 방식과 통계 로드 밸런싱이 달성되고 있는지 확인하기 위해 각 물리적 인터페이스를 별도로 관리하는 것이 좋습니다.

CatOS 6.x에서 새로운 명령인 **show channel traffic** 명령은 CatOS 5.x에서 **show counters mod/port 명령 또는 show mac *mod/port*** 명령을 사용하여 개별 포트 카운터를 확인하는 경우보다 쉽게 백분율 분포 통계를 표시할 수 있습니다.또 다른 새로운 명령인 CatOS 6.x에서 show channel hash 명령을 사용하면 배포 모드를 기준으로 특정 주소 및/또는 포트 번호에 대해 발신 포트로 선택할 포트를 확인할 수 있습니다.LACP 채널에 해당하는 명령은 **show lacp-channel traffic 명령** 및 **show lacp-channel hash** 명령입니다.

기타 옵션

Catalyst 4500/4000 또는 Catalyst 5500/5000 MAC 기반 알고리즘의 상대적 제한이 문제가 되고 올바른 통계 로드 밸런싱을 달성하지 못할 경우 수행할 수 있는 단계입니다.

- Catalyst 6500/6000 스위치의 포인트 구축
- 여러 FE 포트에서 하나의 GE 포트로 또는 여러 GE 포트에서 10GE 포트로 전환하여 채널을 변경하지 않고 대역폭을 늘립니다.
- 대규모 볼륨 플로우를 사용하는 엔드 스테이션의 주소 재설정
- 고대역폭 디바이스에 전용 링크/VLAN 프로비저닝

EtherChannel 구성 지침 및 제한 사항

EtherChannel은 호환 가능한 포트를 단일 논리 포트로 집계하기 전에 모든 물리적 포트에서 포트 속성을 확인합니다.구성 지침 및 제한은 서로 다른 스위치 플랫폼에 따라 다릅니다.번들링 문제를 방지하려면 지침을 따르십시오.예를 들어, QoS가 활성화된 경우 QoS 기능이 다른 Catalyst 6500/6000 시리즈 스위칭 모듈을 번들링할 때 EtherChannel이 형성되지 않습니다.Cisco IOS Software에서는 EtherChannel 번들링에서 no mls qos channel-consistency **port-channel interface 명령**과 함께 QoS 포트 특성 확인**을 비활성화할** 수 있습니다.CatOS에서는 QoS 포트 특성 검사를 비활성화하기 위한 동등한 명령을 사용할 수 없습니다.QoS 포트 기능을 표시하고 포트가 호환 가능한지 확인하기 위해 show **port capability *mod/port*** 명령을 실행할 수 있습니다.

구성 문제를 방지하려면 여러 플랫폼에 대해 다음 지침을 따르십시오.

- EtherChannel *구성*(Catalyst 6500/6000)의 EtherChannel 구성 지침 섹션
- Fast *EtherChannel 및 Gigabit EtherChannel*(Catalyst 4500/4000) 구성의 EtherChannel 구성 지침 및 제한 섹션
- Fast *EtherChannel 및 Gigabit EtherChannel*(Catalyst 5000) 구성의 EtherChannel 구성 지침 및 제한 사항 섹션

참고: Catalyst 4000에서 지원하는 최대 포트 채널 수는 126개입니다. 소프트웨어 릴리스 6.2(1) 이하에서는 6슬롯 및 9슬롯 Catalyst 6500 시리즈 스위치가 최대 128개의 EtherChannel을 지원합니다.소프트웨어 릴리스 6.2(2) 이상 릴리스에서 스패닝 트리 기능은 포트 ID를 처리합니다.따라서 지원되는 EtherChannel의 최대 수는 6슬롯 또는 9슬롯 섀시의 경우 126이고 13슬롯 섀시의 경우 63입니다.

포트 어그리게이션 프로토콜

PAgP는 링크 양쪽 끝에서 매개변수 일관성을 확인하고 링크 장애 또는 추가에 적응하는 데 채널을 지원하는 관리 프로토콜입니다.PAgP에 대한 다음 사항을 참고하십시오.

- PAgP는 채널의 모든 포트가 동일한 VLAN에 속하거나 트렁크 포트로 구성되어 있어야 합니다.(동적 VLAN은 포트를 다른 VLAN으로 강제로 변경할 수 있으므로 EtherChannel 참여에는 포함되지 않습니다.)
- 번들이 이미 있고 한 포트의 컨피그레이션이 수정되면(예: VLAN 변경 또는 트렁킹 모드) 번들의 모든 포트가 해당 컨피그레이션과 일치하도록 수정됩니다.
- PAgP는 다른 속도 또는 포트 듀플렉스에서 작동하는 포트를 그룹화하지 않습니다.번들이 있을 때 속도와 듀플렉스가 변경되면 PAgP는 번들의 모든 포트에 대해 포트 속도와 듀플렉스를 변경합니다.

운영 개요

PAgP 포트는 그룹화할 각 개별 물리적(또는 논리적) 포트를 제어합니다.PAgP 패킷은 CDP 패킷에 사용되는 동일한 멀티캐스트 그룹 MAC 주소, **01-00-0c-cc-cc-cc**를 사용하여 전송됩니다.프로토콜 값은 0x0104입니다. 프로토콜 작업의 요약입니다.

- 물리적 포트가 경우, PAgP 패킷은 탐지 중에 1초마다 전송되고 30초마다 정상 상태로 전송됩니다.
- 이 프로토콜은 물리적 포트가 다른 PAgP 지원 디바이스에 양방향 연결을 제공한다는 것을 증명하는 PAgP 패킷을 수신합니다.
- 데이터 패킷만 수신되지만 PAgP 패킷은 수신되지 않은 경우 포트가 비 PAgP 지원 디바이스에 연결된 것으로 간주됩니다.
- 물리적 포트 그룹에서 2개의 PAgP 패킷이 수신되는 즉시 집계된 포트를 형성하려고 시도합니

다.
- PAgP 패킷이 일정 기간 동안 중지되면 PAgP 상태가 .

일반 처리

프로토콜 동작을 쉽게 이해할 수 있도록 다음 개념을 정의해야 합니다.

- **Agport**—동일한 어그리게이션의 모든 물리적 포트로 구성된 논리적 포트로서, 고유한 SNMP ifIndex로 식별할 수 있습니다.따라서 보고서에는 작동하지 않는 포트가 포함되지 않습니다.
- **채널** - 구성 기준을 충족하는 어그리게이션따라서 비작동 포트를 포함할 수 있습니다(에이전트는 채널의 하위 집합임). STP 및 VTP를 포함하지만 CDP 및 DTP를 제외한 프로토콜은 에이전트를 통해 PAgP 위에서 실행됩니다.PAgP가 하나 이상의 물리적 포트에 에이전트를 연결할 때까지 이러한 프로토콜은 패킷을 보내거나 받을 수 없습니다.
- **Group Capability(그룹 기능)** - 각 물리적 포트 및 에이전트는 group-capability라는 컨피그레이션 매개변수를 보유합니다.물리적 포트는 동일한 그룹 기능이 있는 경우에만 다른 물리적 포트와 취합할 수 있습니다.
- **Aggregation Procedure**(어그리게이션 절차) - 물리적 포트가 `UpData` 또 `UpPAgP` 상태에 도달하면 적절한 에이전트에 연결됩니다.이러한 상태 중 하나를 다른 상태로 남겨두면 에이전트에서 분리됩니다.

상태 및 생성 프로시저의 정의는 다음 표에 나와 있습니다.

주/도	의미
	수신된 PAgP 패킷이 없습니다.PAgP 패킷이 전송됩니다.물리적 포트는 해당 에이전트에 연결된 유일한 포트입니다.비PAgP 패킷은 물리적 포트와 에이전트 간에 전달되고 전달됩니다.
	정확히 하나의 PAgP 패킷이 수신되어 정확히 하나의 네이버에 양방향 연결이 있음을 입증합니다.물리적 포트가 어떤 에이전트에도 연결되지 않았습니다.PAgP 패킷이 전송되고 수신될 수 있습니다.
PAgP	이 물리적 포트는 다른 물리적 포트와 연결되었을 수 있습니다.PAgP 패킷은 물리적 포트에서 전송 및 수신됩니다.비PAgP 패킷은 물리적 포트와 에이전트 간에 전달되고 전달됩니다.

두 연결의 양쪽 끝 모두 그룹화가 어떻게 될 것인지에 대해 동의해야 하며, 연결의 양쪽 끝에서 허용하는 포트에서 가장 큰 포트 그룹으로 정의되어야 합니다.

물리적 포트가 `UpPAgP` 상태에 도달하면 새 물리적 포트의 그룹 기능과 일치하고 BiDir 또는 UpPAgP 상태에 있는 멤버 물리적 포트가 있는 에이전트에 할당됩니다.(이러한 BiDir 포트는 동시에 `UpPAgP` 상태로 이동됩니다.) 구성 요소 물리적 포트 매개변수가 새로 준비된 물리적 포트와 호환되는 에이전트가 없는 경우, 관련 물리적 포트가 없는 적절한 매개변수가 있는 에이전트에 할당됩니다.

PAgP 시간 초과는 물리적 포트에서 알려진 마지막 네이버에서 발생할 수 있습니다.포트 시간 초과가 에이전트에서 제거됩니다.동시에 타이머가 시간 초과된 동일한 포트의 모든 물리적 포트가 제거됩니다.이렇게 하면 한 번에 하나의 물리적 포트가 아닌 다른 쪽 끝이 죽은 에이전트가 한 번에 모두 해체될 수 있습니다.

장애 시 동작

기존 채널의 링크에 장애가 발생하면(예: 포트 언플러그, GBIC(Gigabit Interface Converter) 제거 또는 파이버 파열), 에이전트가 업데이트되고 트래픽이 1초 내에 나머지 링크를 통해 해시됩니다.실패 후 다시 해시할 필요가 없는 트래픽(동일한 링크에서 계속 전송되는 트래픽)은 손실되지 않습니다 .실패한 링크를 복원하면 에이전트에 대한 또 다른 업데이트가 트리거되고 트래픽이 다시 해시됩니다.

참고: 전원이 꺼지거나 모듈이 제거되어 채널에서 링크가 실패하는 경우의 동작은 다를 수 있습니다.즉, 하나의 채널에 물리적 포트가 두 개 있어야 합니다.2포트 채널의 시스템에서 한 포트가 손실된 경우, 논리적 에이전트는 해제되고 원래 물리적 포트는 스패닝 트리를 기준으로 다시 초기화됩니다.즉, STP에서 포트를 다시 데이터에 사용할 수 있을 때까지 트래픽을 삭제할 수 있습니다.

Catalyst 6500/6000에서는 이 규칙에 예외가 있습니다. CatOS 6.3 이전 버전에서는 채널이 모듈 1 및 2의 포트로만 구성된 경우 모듈을 제거하는 동안 상담원이 않습니다.

이 두 가지 장애 모드의 차이점은 네트워크의 유지 관리를 계획할 때 중요합니다. STP TCN이 모듈의 온라인 제거 또는 삽입을 수행할 때 고려할 수 있기 때문입니다.앞서 언급한 대로, NMS와 함께 채널의 각 물리적 링크를 관리하는 것이 중요합니다. 에이전트는 장애를 통해 방해 받지 않을 수 있습니다.

Catalyst 6500/6000에서 원치 않는 토폴로지 변경을 완화하기 위한 권장 단계는 다음과 같습니다.

- 단일 포트를 모듈별로 사용하여 채널을 형성하는 경우 3개 이상의 모듈을 사용해야 합니다(3개 이상의 총 포트).
- 채널이 2개의 모듈에 걸쳐 있는 경우 각 모듈의 2개 포트를 사용해야 합니다(총 4개 포트).
- 두 카드에 2포트 채널이 필요한 경우 Supervisor Engine 포트만 사용합니다.
- 모듈 간에 분할된 채널에 대해 STP 재계산 없이 모듈 제거를 처리하는 CatOS 6.3으로 업그레이드합니다.

구성 옵션

EtherChannel은 다음 표에 요약된 대로 서로 다른 모드로 구성할 수 있습니다.

모드	구성 가능한 옵션
	PAgP가 작동하지 않습니다.네이버 포트의 구성 방식에 관계없이 포트가 채널링됩니다.인접 포트 모드가 켜져 있으면 채널이 형성됩니다.
	네이버가 구성된 방식과 상관없이 포트는 채널링되지 않습니다.
( )	어그리게이션이 PAgP 프로토콜을 제어하고 있습니다.포트를 패시브 상태로 배치하고 발신자가 모드에서 작동 중임을 나타내는 하나 이상의 PAgP 패킷이 수신될 때까지 인터페이스에서 PAgP 패킷이 전송되지 않습니다.

	어그리게이션이 PAgP 프로토콜을 제어하고 있습니다.포트를 활성 상태로 설정합니다. 그러면 포트가 PAgP 패킷을 전송하여 다른 포트와의 협상을 시작합니다.채널은 바람직한 또는 자동 모드에서 다른 포트 그룹으로 구성됩니다.
(Catalyst 5500/5000 파이버 FE 및 GE 포트의 기본값)	auto 또는 모드 키워드인터페이스에서 수신된 데이터 패킷이 없는 경우, 인터페이스는 에이전트에 연결되지 않으며 데이터에 사용할 수 없습니다.일부 링크 장애로 인해 채널이 분리됨에 따라 특정 Catalyst 5500/5000 하드웨어에 대해 이러한 양방향 검사가 제공되었습니다. 모드가 활성화되었으므로 복구 인접 포트 다시 돌아와서 채널을 불필요하게 분리할 수 없습니다.Catalyst 4500/4000 및 6500/6000 시리즈 하드웨어에서는 기본적으로 더 유연한 번들링 및 향상된 양방향 확인이 제공됩니다.
(모든 Catalyst 6500/6000 및 4500/4000 포트 및 5500/5000 구리 포트에서 기본값)	auto 또는 모드 키워드인터페이스에서 수신된 데이터 패킷이 없는 경우, 15초 시간 제한 기간이 지나면 인터페이스가 에이전트에 직접 연결되므로 데이터 전송에 사용할 수 있습니다. 모드에서는 파트너가 PAgP를 보내지 않는 분석기 또는 서버가 될 수 있는 경우 채널 작동을 허용합니다.

무음/ 설정은 단방향 트래픽을 발생시키는 상황에 포트가 반응하는 방식 또는 장애 조치를 수행하는 방법에 영향을 줍니다.포트에서 전송할 수 없는 경우(예: PHY[물리적 하위 레이어] 또는 손상된 파이버 또는 케이블 때문에), 이는 인접 포트가 작동 상태로 남아 있을 수 있습니다.파트너는 데이터를 계속 전송하지만 반환 트래픽을 수신할 수 없으므로 데이터가 손실됩니다.스패닝 트리 루프는 링크의 단방향 특성 때문에 형성될 수도 있습니다.

일부 파이버 포트는 수신 신호(FFI)가 손실되었을 때 포트를 비작동 상태로 만드는 데 필요한 기능을 제공합니다. 그러면 파트너 포트가 작동하지 않으며 링크의 양쪽 끝에 있는 포트가 효과적으로 다운됩니다.

BPDU와 같이 데이터를 전송하고 단방향 조건을 탐지할 수 없는 장치를 사용할 경우 수신 데이터가 있고 링크가 양방향으로 확인될 때까지 포트가 비작동 상태를 유지하도록 하기 위해 모드를 사용해야 합니다.PAgP가 단방향 링크를 탐지하는 데 걸리는 시간은 약 3.5 * 30초 = 105초이며, 여기서 30초는 두 연속 PAgP 메시지 사이의 시간입니다.단방향 링크에 대해 보다 빠른 탐지기로 UDLD를 사용하는 것이 좋습니다.

데이터를 전송하지 않는 디바이스를 사용할 경우 모드를 사용해야 합니다.이렇게 하면 수신된 데이터가 있는지 여부에 관계없이 포트가 연결되고 작동합니다.또한 L1 FFI 및 UDLD를 사용하는 새로운 플랫폼과 같이 단방향 조건의 존재를 탐지할 수 있는 포트에 대해서는 기본적으로 무음 모드가 사용됩니다.

확인

이 표는 직접 연결된 두 스위치(Switch-A 및 Switch-B) 간의 가능한 모든 PAgP 채널링 모드 시나리오를 요약하여 보여줍니다. 이러한 조합 중 일부는 STP가 채널링 측면에 있는 포트를 errdisable 상태 전환할 수 있습니다(즉, 일부 조합으로 인해 채널링 쪽에 있는 포트가 종료됨).

스위치-A 채널 모드	Switch-B 채널 모드	채널 상태
		(비 PAgP)
		(errdisable)
		(errdisable)
		(errdisable)
		(errdisable)
		(errdisable)
		PAgP
		(errdisable)
		PAgP
		PAgP

권장 사항

Cisco는 모든 스위치 간 채널 연결에서 PAgP를 활성화하여 모드를 사용하지 않도록 것 권장합니다.선호하는 방법은 링크 양쪽 끝에서 모드를 설정하는 것입니다.또 다른 권장 사항은 / 키워드를 기본적으로 유지하는 것입니다. 즉 Catalyst 6500/6000 및 4500/4000 스위치에서는 으로, Catalyst 5500/5000 파이버 포트에서는 무음으로 두는 것이 좋습니다.

이 문서에서 설명한 것처럼 다른 모든 포트에서 채널링 오프를 명시적으로 구성하면 데이터를 신속하게 전송할 수 있습니다.채널링에 사용되지 않는 포트에서 PAgP가 시간 초과될 때까지 최대 15초 동안 대기하는 것은 피해야 합니다. 특히, 데이터 전달을 허용하는 데 30초가 걸릴 수 있는 STP에 포트가 전달되기 때문에, DTP는 총 50초 동안 5초 정도 걸릴 수 있습니다.set **port host** 명령은 이 문서의 STP 섹션에서 자세히 설명합니다.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

이 명령은 채널**에 관리 그룹** 번호를 할당하며, show channel group **명령**과 함께 **표시됩니다**.동일한 어포트에 채널링 포트를 추가 및 제거하면 필요한 경우 관리 번호로 관리할 수 있습니다.

기타 옵션

액세스 레이어에서 최소 관리 모델이 있는 고객을 위한 또 다른 일반적인 컨피그레이션은 디스트리뷰션 및 코어 레이어에서 모드를 으로 설정하고 액세스 레이어 스위치를 기본 컨피그레이션으로 유지하는 것입니다.

PAgP를 지원하지 않는 장치로 채널링하는 경우 채널을 하드 코딩해야 .이는 서버, 로컬 디렉터, 콘텐츠 스위치, 라우터, 이전 소프트웨어가 설치된 스위치, Catalyst XL 스위치, Catalyst 8540과 같은 디바이스에 적용됩니다.다음 명령을 실행합니다.

```
set port channel port range mode on
```

CatOS 7.x에서 제공되는 새로운 802.3ad IEEE LACP 표준은 플랫폼 간 및 공급업체 상호 운용성의 이점을 제공하므로 장기적으로 PAgP를 대체할 가능성이 높습니다.

링크 집계 제어 프로토콜

LACP는 유사한 특성을 가진 포트가 인접 스위치와의 동적 협상을 통해 채널을 형성하도록 허용하는 프로토콜입니다.PAgP는 Cisco 스위치 및 라이센스 공급업체에서 릴리스하는 스위치에서만 실행할 수 있는 Cisco 전용 프로토콜입니다.그러나 IEEE 802.3ad에 정의된 LACP를 통해 Cisco 스위치에서는 802.3ad 사양을 따르는 디바이스로 이더넷 채널링을 관리할 수 있습니다.CatOS 7.x 소프트웨어 릴리스는 LACP 지원을 도입했습니다.

기능적 관점에서 LACP와 PAgP는 거의 차이가 없습니다.두 프로토콜 모두 각 채널에서 최대 8개의 포트를 지원하며, 번들이 형성되기 전에 동일한 포트 속성을 확인합니다.이러한 포트 속성은 다음과 같습니다.

- 속도
- 이중
- 네이티브 VLAN
- 트렁킹 유형

LACP와 PAgP의 현저한 차이점은 다음과 같습니다.

- LACP는 전이중 포트에서만 실행할 수 있으며 LACP는 반이중 포트를 지원하지 않습니다.
- LACP는 핫 스탠바이 포트를 지원합니다.LACP는 항상 하드웨어에서 허용하는 최대 개수(8개 포트)까지 채널에서 호환 가능한 최대 포트 수를 구성하려고 시도합니다. LACP에서 호환되는 모든 포트를 집계할 수 없는 경우, 채널에 능동적으로 포함할 수 없는 모든 포트는 핫 스탠바이 상태로 설정되며 사용된 포트 중 하나에 장애가 발생한 경우에만 사용됩니다.LACP가 모든 호환 포트를 집계할 수 없는 상황의 예는 원격 시스템에 더 제한적인 하드웨어 제한이 있는 경우입니다.

참고: CatOS에서 동일한 관리 키를 할당할 수 있는 최대 포트 수는 8개입니다.Cisco IOS Software에서 LACP는 EtherChannel에서 하드웨어에서 허용하는 최대 개수(8개 포트)까지 호환 가능한 최대 포트 수를 구성하려고 시도합니다. 8개의 포트를 핫 스탠바이 포트로 구성할 수 있습니다.

운영 개요

LACP는 번들링할 각 개별 물리적(또는 논리적) 포트를 제어합니다.LACP 패킷은 멀티캐스트 그룹 MAC 주소, **01-80-c2-00-00-02**를 사용하여 전송됩니다. 유형/필드 값은 0x01의 하위 유형으로 0x8809입니다. 프로토콜 작업의 요약은 다음과 같습니다.

- 프로토콜은 디바이스에 의존하여 어그리게이션 기능 및 상태 정보를 광고합니다.전송은 *각 "*집계 가능" 링크*에 대해* 정기적으로 전송됩니다.
- 물리적 포트가 작동 중인 경우, LACP 패킷은 탐지 중에 1초마다 전송되고 30초마다 정상 상태로 전송됩니다.
- "집계 가능" 링크의 파트너는 프로토콜 내에서 전송되는 정보를 듣고 어떤 조치를 취할 것인지 결정합니다.
- 호환 가능한 포트는 하드웨어에서 허용하는 최대 개수(8개 포트)까지 채널에서 구성됩니다.
- 이 집계는 링크 파트너 간의 최신 상태 정보를 적시에 정기적으로 교환하여 관리합니다.링크 장애 등의 이유로 컨피그레이션이 변경되면 프로토콜 파트너는 시간이 초과되어 시스템의 새 상태를 기준으로 적절한 조치를 취합니다.
- 주기적인 LACP LACPDU(Data Unit) 전송 외에도 상태 정보가 변경되면 프로토콜은 이벤트 중심 LACPDU를 파트너에게 전송합니다.프로토콜 파트너는 시스템의 새로운 상태에 따라 적절한 조치를 취합니다.

LACP 매개변수

LACP가 링크 집합이 동일한 시스템에 연결되는지 그리고 이러한 링크가 어그리게이션의 관점에서 호환되는지 확인하기 위해 이러한 매개변수를 설정하는 기능이 필요합니다.

- 링크 집계에 참여하는 각 시스템의 전역적으로 고유한 식별자LACP를 실행하는 각 시스템에는 자동으로 또는 관리자가 선택할 수 있는 우선 순위가 할당되어야 합니다.기본 시스템 우선순위는 32768입니다. 시스템 우선순위는 시스템 식별자를 구성하기 위해 시스템의 MAC 주소와 함께 주로 사용됩니다.
- 지정된 시스템에서 이해할 수 있듯이 각 포트 및 각 어그리게이터와 연결된 기능 집합을 식별하는 방법시스템의 각 포트에는 자동으로 또는 관리자가 우선 순위를 할당해야 합니다.기본값은 128입니다. 우선 순위는 포트 식별자를 구성하기 위해 포트 번호와 함께 사용됩니다.
- 링크 어그리게이션 그룹 및 관련 어그리게이터를 식별하는 방법다른 포트와 집계할 수 있는 기능은 엄격하게 0보다 큰 간단한 16비트 정수 매개 변수로 요약됩니다.이 매개 변수를 "key"라고 합니다. 각 키는 다음과 같은 여러 요인에 의해 결정됩니다.다음과 같은 포트 물리적 특성데이터 전송률이중성포인트 투 포인트 또는 공유 미디어네트워크 관리자가 설정하는 구성 제약 조건각 포트에 두 개의 키가 연결됩니다.관리 키 - 이 키를 사용하면 관리에서 키 값을 조작할 수 있습니다.사용자는 이 키를 선택할 수 있습니다.An operational key(운영 키) - 시스템에서 집계를 구성하기 위해 이 키를 사용합니다.사용자는 이 키를 선택하거나 직접 변경할 수 없습니다.동일한 운영 키 값을 공유하는 시스템의 포트 집합은 동일한 키 그룹의 멤버라고 합니다.

두 개의 시스템과 동일한 관리 키를 가진 포트 집합이 있는 경우 각 시스템은 포트를 집계하려고 시도합니다.각 시스템은 우선순위가 가장 높은 시스템에서 가장 높은 포트에서 시작합니다.이러한 동작은 각 시스템이 사용자 또는 시스템이 할당한 자체 우선 순위 및 LACP 패킷을 통해 검색된 파트너 우선 순위를 알고 있기 때문에 가능합니다.

장애 시 동작

LACP에 대한 실패 동작은 PAgP에 대한 동작과 동일합니다.기존 채널의 링크에 장애가 발생하면 에이전트가 업데이트되고 1초 이내에 나머지 링크를 통해 트래픽이 해시됩니다.다음과 같은 이유로 링크가 실패할 수 있습니다.

- 포트가 언플러그되었습니다.
- GBIC가 제거됩니다.
- 섬유질이 고장 났다

- 하드웨어 장애(인터페이스 또는 모듈)

실패 후 다시 해시할 필요가 없는 트래픽(동일한 링크에서 계속 전송되는 트래픽)은 손실되지 않습니다.실패한 링크를 복원하면 에이전트에 대한 또 다른 업데이트가 트리거되고 트래픽이 다시 해시됩니다.

구성 옵션

LACP EtherChannel은 다음 표에 요약되어 있으므로 서로 다른 모드로 구성할 수 있습니다.

모드	구성 가능한 옵션
	LACP 협상 없이 링크 집계를 구성해야 합니다.스위치는 LACP 패킷을 전송하거나 수신 LACP 패킷을 처리하지 않습니다.네이버 포트 모드가 있으면 채널이 형성됩니다.
	네이버가 구성된 방식과 상관없이 포트는 채널링되지 않습니다.
( )	이는 PAgP의 모드와 유사합니다.스위치는 채널을 시작하지 않지만 수신 LACP 패킷을 파악합니다.피어(상태)는 LACP 패킷을 전송하여 협상을 시작합니다.스위치는 패킷을 수신하고 응답하며, 궁극적으로는 피어와의 어그리게이션 채널을 형성합니다.
	이는 PAgP의 모드와 유사합니다.스위치는 aglink를 구성하기 위해 협상을 시작합니다.링크 집계는 LACP 또는 모드에서 다른 엔드가 실행되는 경우 형성됩니다.

확인(LACP 및 LACP)

이 섹션의 표에서는 두 개의 직접 연결된 스위치(Switch-A 및 Switch-B) 간에 가능한 모든 LACP 채널링 모드 시나리오를 요약하여 보여 줍니다. 이러한 조합 중 일부는 STP가 채널링 쪽에 포트를 errdisable 상태로 수 있습니다.즉, 일부 조합은 채널링 측면의 포트를 차단합니다.

스위치-A 채널 모드	Switch-B 채널 모드	스위치-A 채널 상태	스위치-B 채널 상태
		(비 LACP)	(비 LACP)
		(errdisable)	
		(errdisable)	
		(errdisable)	
		LACP	LACP
		LACP	LACP

확인(LACP 및 PAgP)

이 섹션의 표에서는 두 직접 연결된 스위치(Switch-A와 Switch-B) 간에 가능한 모든 LACP-to-PAgP 채널링 모드 시나리오를 요약하여 보여 줍니다. 이러한 조합 중 일부는 STP가 채널링 쪽에 포트를 errdisable 상태로 수 있습니다.즉, 일부 조합은 채널링 측면의 포트를 차단합니다.

스위치-A 채널 모드	Switch-B 채널 모드	스위치-A 채널 상태	스위치-B 채널 상태
		(비 LACP)	(비 PAgP)
		(errdisable)	
		(errdisable)	
		(errdisable)	
			(errdisable)
			(errdisable)
			(errdisable)

권장 사항

Cisco 스위치 간 채널 연결에서 PAgP를 활성화하는 것이 좋습니다.PAgP를 지원하지 않지만 LACP를 지원하는 디바이스에 채널을 연결할 경우 디바이스 양쪽 끝에서 LACP 컨피그레이션을 통해 LACP를 활성화합니다.디바이스 중 하나가 LACP 또는 PAgP를 지원하지 않는 경우 채널을 하드 코드해야 합니다.

- **set channelprotocol lacp** *module*

  CatOS를 실행하는 스위치에서 Catalyst 4500/4000 및 Catalyst 6500/6000의 모든 포트는 기본적으로 채널 프로토콜 PAgP를 사용하며, 따라서 LACP를 실행하지 않습니다.LACP를 사용하도록 포트를 구성하려면 모듈의 채널 프로토콜을 LACP로 설정해야 합니다.LACP와 PAgP는 CatOS를 실행하는 스위치에서 동일한 모듈에서 실행할 수 없습니다.

- **set port lacp-channel** *port_range admin-key*

  관리 **키**(관리 키) 매개변수는 LACP 패킷에서 교환됩니다.동일한 관리 키를 가진 포트 간에 채널만 형성됩니다.set port lacp-channel *port_range* admin-*key* 명령은 채널 및 관리자 키 번호를 할당합니다.show lacp-channel group 명령은 숫자를 표시합니다.set **port lacp-channel** ***port_range*** **admin-key** 명령은 포트 범위의 모든 포트에 동일한 관리 키를 할당합니다.특정 키가 구성되지 않은 경우 관리자 키가 무작위로 할당됩니다.그런 다음 필요한 경우 관리 키를 참조하여 동일한 에이전트에 채널링 포트를 추가하고 제거할 수 있습니다.

-

```
set port lacp-channel port_range mode active
```

set port lacp-channel *port_range* mode active 명령은 이전에 동일한 관리 키를 할당한 포트 집합에 대해 채널 모드를 active로 변경합니다.

또한 LACP는 LACP EtherChannel이 설정된 후 30초 간격 타이머(Slow_Periodic_Time)를 사용합니다.긴 시간 초과(3 x Slow_Periodic_Time)를 사용하여 수신된 LACPDU 정보를 무효화하기 전 시간(초)은 90입니다. 단방향 링크의 더 빠른 탐지기인 UDLD를 사용합니다.LACP 타이머를 조정할 수 없으며, 지금은 채널을 구성한 후 채널을 유지하기 위해 빠른 PDU 전송(초당)을 사용하도록 스위치를 구성할 수 없습니다.

기타 옵션

액세스 레이어에서 최소 관리 모델이 있는 경우, 일반적인 컨피그레이션은 디스트리뷰션 및 코어 레이어에서 모드를 으로 설정하는 것입니다.액세스 레이어 스위치를 기본 컨피그레이션으로 유지합니다.

단방향 링크 탐지

UDLD는 디바이스 간의 단방향 통신 인스턴스를 탐지하기 위해 개발된 Cisco만의 경량 프로토콜입니다.FFI와 같은 전송 미디어의 양방향 상태를 탐지하는 다른 방법이 있지만 L1 탐지 메커니즘이 충분하지 않은 특정 인스턴스가 있습니다.이러한 시나리오는 다음과 같은 상황을 야기할 수 있습니다.

- STP의 예측 불가능한 운영
- 패킷의 부정확하거나 과도한 폴러딩
- 트래픽의 블랙홀

UDLD 기능은 파이버 및 구리 이더넷 인터페이스에서 다음과 같은 결함 조건을 해결하기 위한 것입니다.

- 물리적 케이블 컨피그레이션을 모니터링하고 오류가 발생한 모든 포트를 errdisable로 .
- 단방향 링크로부터 보호합니다.단방향 링크가 탐지되면 미디어 또는 포트/인터페이스 오작동으로 인해 영향받는 포트가 errdisable로 종료되고 해당 syslog 메시지가 생성됩니다.
- 또한 UDLD aggressive 모드에서는 이전에 양방향으로 간주되었던 링크가 혼잡 중에 연결이 끊기지 않고 사용할 수 없게 되는지 확인합니다.UDLD는 링크 전체에서 지속적인 연결 테스트를 수행합니다.UDLD aggressive 모드의 기본 목적은 장애가 발생한 특정 상황에서 트래픽이 블랙홀딩되지 않도록 하는 것입니다.

일관된 상태 단방향 BPDU 플로우인 스패닝 트리는 이러한 장애로 인해 심각한 어려움을 겪었습니다.포트가 갑자기 BPDU를 전송할 수 없어 STP 상태가 에서 인접 디바이스의 으로 변경되는 방식을 쉽게 확인할 수 있습니다.포트가 계속 수신될 수 있으므로 이 변경 사항은 루프를 생성합니다.

운영 개요

UDLD는 LLC 레이어(대상 MAC 01-00-0c-cc-cc-cc, SNAP HDLC 프로토콜 유형 0x0111) 위에서 작동하는 L2 프로토콜입니다. FFI 및 자동 협상 L1 메커니즘과 함께 UDLD를 실행할 경우 링크의 물리적(L1) 및 논리적(L2) 무결성을 검증할 수 있습니다.

UDLD에는 FFI 및 자동 협상이 수행할 수 없는 기능 및 보호, 즉 인접 정보의 탐지 및 캐싱, 잘못 연결된 포트를 종료하고, 지점 간(미디어 변환기 또는 허브를 이동하는 링크)에서 논리적 인터페이스/포트 악성코드 또는 결함을 탐지하는 기능이 있습니다.

UDLD는 두 가지 기본 메커니즘을 사용합니다.네이버에 대해 학습하고 로컬 캐시에 정보를 최신 상태로 유지하고, 새 네이버를 탐지하거나 네이버가 캐시 재동기화를 요청할 때마다 UDLD 프로브/에코(hello) 메시지 세트를 전송합니다.

UDLD는 UDLD가 활성화된 모든 포트에서 프로브 메시지를 지속적으로 전송합니다.특정 "트리거" UDLD 메시지가 포트에서 수신될 때마다 탐지 단계 및 검증 프로세스가 시작됩니다.이 프로세스가 끝날 때 모든 유효한 조건이 충족되면 포트 상태가 변경되지 않습니다.조건을 충족하려면 포트가 양방향이어야 하고 올바르게 연결되어야 합니다.그렇지 않으면 포트가 `errdisable`이고 syslog 메시지가 표시됩니다.syslog 메시지는 다음 메시지와 유사합니다.

- `UDLD-3-: [dec]/[dec]  .`
- `UDLD-4-ONEDWAYPATH: [dec]/[dec]  [chars] [dec]/[dec]() .`

UDLD 이벤트를 포함한 기능별 시스템 메시지 전체 목록은 메시지 및 복구 절차(Catalyst 시리즈 스위치, 7.6)를 참조하십시오.

링크가 설정되고 양방향으로 분류되면 UDLD는 기본 간격인 15초에 프로브/에코 메시지를 계속 광고합니다.이 테이블은 show udld port 명령의 출력에 보고된 유효한 UDLD 링크 상태를 나타냅니다.

포트 상태	설명
확인되지 않음	탐지가 진행 중이거나 인접한 UDLD 엔터티가 비활성화되었거나 전송이 차단되었습니다.
해당 없음	UDLD가 비활성화되었습니다.
셧다운	단방향 링크가 탐지되었으며 포트가 비활성화되었습니다.
양방향	양방향 링크가 감지되었습니다.

- **Neighbor Cache Maintenance** - UDLD 는 UDLD 인접 디바이스 캐시의 무결성을 유지하기 위해 모든 활성 인터페이스에서 hello 프로브/에코 패킷을 정기적으로 전송합니다.hello 메시지가 수신될 때마다 보류 시간으로 정의된 최대 기간 동안 해당 메시지는 캐시되고 메모리에 보관됩니다.보류 시간이 만료되면 각 캐시 항목이 오래됩니다.보류 기간 내에 새 hello 메시지가 수신되면 새 hello 메시지가 이전 항목을 대체하고 해당 time-to-live 타이머가 재설정됩니다.
- UDLD 캐시의 무결성을 유지하기 위해 UDLD 지원 인터페이스가 비활성화되거나 디바이스가 재설정될 때마다 컨피그레이션 변경의 영향을 받는 인터페이스에 대한 기존 캐시 엔트리가 모두 지워지고 UDLD는 해당 네이버에 해당 캐시 엔트리를 플러시하도록 알리는 하나 이상의 메시지를 전송합니다.
- **Echo Detection Mechanism** - 에코 메커니즘은 탐지 알고리즘의 기반을 형성합니다.UDLD 디바이스는 새 네이버에 대해 학습하거나 동기화되지 않은 네이버에서 재동기화 요청을 수신할 때마다 연결 측에서 탐지 윈도우를 시작/재시작하고 에코 메시지의 버스트를 응답으로 보냅니다.이 동작은 모든 네이버에서 동일해야 하므로 에코 발신자는 회신으로 다시 수신해야 합니다.탐지 창이 종료되고 유효한 응답 메시지가 수신되지 않은 경우 링크는 단방향으로 간주되며 링크 재설정 또는 포트 종료 프로세스를 트리거할 수 있습니다.

통합 시간

STP 루프를 방지하기 위해 CatOS 5.4(3)는 차단된 포트가 전달 상태로 전환되기 전에 단방향 링크를 종료하기 위해 UDLD 기본 메시지 간격을 60초에서 15초로 줄였습니다.

참고: 메시지 간격 값은 연결 또는 탐지 단계 후에 인접 디바이스가 UDLD 프로브를 전송하는 속도

를 결정합니다.가능한 경우 일관된 컨피그레이션이 바람직하지만 메시지 간격이 링크의 양쪽 끝에서 일치할 필요는 없습니다.UDLD 인접 디바이스가 설정되면 구성된 메시지 간격이 전송되고 해당 피어에 대한 시간 초과 간격이 (3 * message_interval)으로 계산됩니다. 따라서 피어 관계는 연속된 세 개의 hello(또는 프로브)가 누락된 후 시간 초과됩니다.메시지 간격이 서로 다르기 때문에 이 시간 초과 값은 양쪽에서 다릅니다.

UDLD에서 단방향 오류를 탐지하는 데 필요한 대략적인 시간은 약(2.5 * message_interval + 4초) 또는 기본 메시지 간격을 15초로 사용하는 약 41초입니다.이는 STP가 다시 통합되는 데 일반적으로 필요한 50초 미만입니다.NMP CPU에 예비 주기가 몇 개 있고 사용률 수준을 신중하게 모니터링하는 경우 메시지 간격(짝수)을 최소 7초로 줄일 수 있습니다.이 메시지 간격은 탐지 속도를 크게 높이는 데 도움이 됩니다.

따라서 UDLD에는 기본 스패닝 트리 타이머에 대한 의존 관계가 있습니다.UDLD보다 빠르게 통합되도록 STP를 튜닝하는 경우 CatOS 6.2 루프 가드 기능과 같은 대체 메커니즘을 고려합니다.또한 RSTP는 토폴로지에 따라 달라지는 컨버전스 특성을 밀리초 단위로 가지므로 RSTP(IEEE 802.1w)를 구현할 때 대체 메커니즘을 고려하십시오.이러한 경우 가장 강력한 보호를 제공하는 UDLD와 함께 루프 가드를 사용합니다.루프 가드는 사용 중인 STP 버전의 속도로 STP 루프를 방지하며, UDLD는 개별 EtherChannel 링크에서 단방향 연결을 탐지하거나 BPDU가 끊어진 방향을 따라 이동하지 않는 경우를 탐지합니다.

참고: UDLD는 (2 * FwdDelay + Maxage)보다 긴 시간 동안 BPDU를 전송하지 않는 CPU로 인해 발생하는 장애와 같은 모든 STP 장애 상황을 탐지하지 않습니다. 이러한 이유로 Cisco에서는 STP를 사용하는 토폴로지에서 루프 가드(CatOS 6.2에서 도입됨)와 함께 UDLD를 구현하는 것이 좋습니다.

주의: 구성할 수 없는 60초 기본 메시지 간격을 사용하는 UDLD의 이전 릴리스를 주의하십시오.이러한 릴리스는 스패닝 트리 루프 조건에 취약합니다.

UDLD 적극적인 모드

양방향 연결의 지속적인 테스트가 필요한 (소수의) 사례를 구체적으로 해결하기 위해 적극적인 UDLD가 생성되었습니다.따라서 적극적인 모드 기능은 다음과 같은 상황에서 위험한 단방향 링크 상태에 대한 보호 기능을 강화합니다.

- UDLD PDU의 손실이 대칭이고 둘 다 시간 초과가 종료되면 어떤 포트도 errdisable되지 않습니다.
- 링크의 한 쪽에 포트가 고정되어 있습니다(전송 [Tx] 및 Rx 모두).
- 링크의 다른 쪽이 다운된 동안 링크의 한 쪽이 작동 상태로 유지됩니다.
- Autonegotiation 또는 다른 L1 장애 감지 메커니즘이 비활성화됩니다.
- L1 FFI 메커니즘에 대한 의존도를 줄이는 것이 바람직합니다.
- 포인트-투-포인트 FE/GE 링크에서 단방향 링크 장애에 대한 보호를 극대화해야 합니다.특히, 두 인접 디바이스 간의 실패가 허용되지 않는 경우, UDLD-aggressive 프로브는 "하트비트"로 간주될 수 있으며, 이 프로브는 링크의 상태를 보장합니다.

적극적인 UDLD 구현의 가장 일반적인 사례는 자동 협상 또는 다른 L1 결함 탐지 메커니즘이 비활성화되거나 사용할 수 없을 때 번들 구성원에 대한 연결 확인을 수행하는 것입니다.PAgP/LACP가 활성화된 경우에도 매우 낮은 hello 타이머를 정상 상태에서 사용하지 않으므로 EtherChannel 연결에서는 특히 그렇습니다.이 경우 적극적인 UDLD는 가능한 스패닝 트리 루프를 방지하는 추가적인 이점을 제공합니다.

UDLD 프로브 패킷의 대칭적인 손실과 관련된 상황은 규정하기가 더 어렵습니다.일반 UDLD는 링크가 양방향 상태에 도달한 후에도 단방향 링크 조건을 확인합니다.UDLD의 목적은 STP 루프를 발

생시키는 L2 문제를 탐지하는 것이며, BPDU는 한 방향으로만 일정한 상태로 흐르기 때문에 이러한 문제는 일반적으로 단방향입니다.따라서 자동 협상 및 루프 가드(STP에 의존하는 네트워크의 경우)와 함께 일반 UDLD를 사용하는 것은 거의 항상 충분합니다.그러나 UDLD 적극적인 모드는 양쪽 방향에서 혼잡이 균등하게 영향을 받는 상황에서 유용하며, 이 경우 양방향의 UDLD 프로브가 손실됩니다.예를 들어 링크의 각 끝에서 CPU 사용률이 상승하면 UDLD 프로브가 손실될 수 있습니다.양방향 연결 손실의 다른 예로는 다음 디바이스 중 하나의 fault가 있습니다.

- DWDM(Dense Wavelength Division Multiplexing) 트랜스폰더
- 미디어 변환기
- 허브
- 다른 L1 장치**참고:** fault는 자동 협상을 통해 감지할 수 없습니다.

Aggressive UDLD 오류는 이러한 장애 상황에서 포트를 비활성화합니다.포인트 투 포인트가 아닌 링크에서 UDLD 적극적인 모드를 활성화할 때 그 결과를 신중하게 고려하십시오.미디어 변환기, 허브 또는 유사 디바이스와의 링크는 포인트투포인트가 아닙니다.중간 디바이스는 UDLD 패킷의 전달을 방지하고 링크를 불필요하게 종료할 수 있습니다.

포트의 모든 네이버가 종료되면 UDLD aggressive 모드(활성화된 경우)는 동기화되지 않은 네이버와 재동기화하기 위해 링크 시퀀스를 재시작합니다.이러한 노력은 광고 또는 탐지 단계에서 수행됩니다.빠른 메시지 전달(8회 재시도 실패) 후에도 링크가 여전히 "undetermined"로 간주되면 포트는 errdisable 상태 전환됩니다.

참고: 일부 스위치는 적극적인 UDLD를 지원하지 않습니다.현재 Catalyst 2900XL 및 Catalyst 3500XL은 메시지 간격을 60초로 하드 코딩했습니다.이 간격은 잠재적인 STP 루프를 보호하는 데 충분히 빠른 것으로 간주되지 않습니다(기본 STP 매개변수 사용).

라우티드 링크의 UDLD

이 논의에서 라우티드 링크는 두 가지 연결 유형 중 하나입니다.

- 두 라우터 노드 간 포인트 투 포인트이 링크는 30비트 서브넷 마스크로 구성됩니다.
- 여러 포트가 있지만 라우팅된 연결만 지원하는 VLAN예를 들면 스플릿 L2 코어 토폴로지입니다.

각 IGRP(Interior Gateway Routing Protocol)는 네이버 관계 및 경로 컨버전스를 처리하는 방식과 관련하여 고유한 특성을 가집니다.이 섹션에서 다루는 특성은 현재 사용되는 보다 일반적인 라우팅 프로토콜 중 두 가지, 즉 OSPF(Open Shortest Path First) 프로토콜과 EIGRP(Enhanced IGRP)를 비교할 때 관련됩니다.

첫째, 모든 포인트 투 포인트 라우티드 네트워크에서 L1 또는 L2 장애가 발생하면 L3 연결이 거의 즉시 해제됩니다.해당 VLAN의 유일한 스위치 포트는 L1/L2 장애 시 연결되지 않은 상태로 전환되므로 MSFC 자동 상태 기능은 약 2초 내에 L2 및 L3 포트 상태를 동기화합니다.이 동기화를 수행하면 L3 VLAN 인터페이스가 up/down 상태가 됩니다(라인 프로토콜이 다운됨).

기본 타이머 값을 가정합니다.OSPF는 10초마다 hello 메시지를 전송하며, Dead 간격은 40초(4 * hello)입니다. 이러한 타이머는 OSPF 포인트-투-포인트 및 브로드캐스트 네트워크에 일관됩니다.OSPF는 인접성을 형성하기 위해 양방향 통신이 필요하므로 최악의 경우 장애 조치 시간은 40초입니다.이 장애 조치는 L1/L2 장애가 포인트 투 포인트 연결에서 순수 오류가 아닌 경우에도 해당되며, 이 경우 L3 프로토콜이 처리해야 하는 반작동 시나리오가 발생합니다.UDLD의 탐지 시간은 만료되는 OSPF 데드 타이머의 시간(약 40초)과 매우 유사하므로 OSPF L3 포인트-투-포인트 링크에서 UDLD 일반 모드를 구성할 경우 이점이 제한됩니다.

대부분의 경우 EIGRP는 OSPF보다 빠르게 통합됩니다.그러나 인접 디바이스에서 라우팅 정보를

교환하려면 양방향 통신이 필요하지 않습니다.매우 특정한 반 운영 실패 시나리오에서 EIGRP는 일부 다른 이벤트가 해당 인접 디바이스의 경로를 "활성"으로 만들 때까지 지속되는 트래픽의 블랙홀링에 취약합니다.UDLD 일반 모드에서는 이 섹션에서 설명하는 상황을 완화할 수 있습니다.UDLD 일반 모드는 단방향 링크 장애를 감지하고 오류가 발생하면 포트를 비활성화합니다.

라우팅 프로토콜을 사용하는 L3 라우팅 연결의 경우 UDLD 표준은 초기 링크 활성화 시 문제를 계속 보호합니다.이러한 문제에는 잘못된 케이블링 또는 하드웨어 결함이 있습니다.또한 UDLD aggressive 모드는 L3 라우팅 연결에서 다음과 같은 이점을 제공합니다.

- 불필요한 블랙홀 트래픽 방지**참고:** 경우에 따라 최소 타이머가 필요합니다.
- 플래핑 링크를 errdisable 상태로 .
- L3 EtherChannel 컨피그레이션에서 발생하는 루프를 차단합니다.

UDLD의 기본 동작

UDLD는 전역적으로 비활성화되며 기본적으로 파이버 포트에서 준비도 상태로 활성화됩니다 .UDLD는 스위치 간에 필요한 인프라 프로토콜이므로 구리 포트에서는 기본적으로 UDLD가 비활성화됩니다.구리 포트는 호스트 액세스에 사용되는 경향이 있습니다.

참고: 인접 디바이스가 양방향 상태를 달성하려면 먼저 UDLD를 전역 및 인터페이스 레벨에서 활성화해야 합니다.CatOS 5.4(3) 이상에서 기본 메시지 간격은 15초이며 7~90초 사이로 구성할 수 있습니다.

Errdisable 복구는 기본적으로 전역적으로 비활성화되어 있습니다.전역적으로 활성화된 후 포트가 errdisable 상태로 전환되면 선택한 시간 간격 후에 포트가 자동으로 다시 활성화됩니다.기본 시간은 300초이며, 이는 전역 타이머이며 스위치의 모든 포트에 대해 유지됩니다.해당 포트에 대한 errdisable 시간 제한을 비활성화하도록 설정한 경우 포트 재활성화를 수동으로 방지할 수 .set port errdisable-timeout *mod/port* disable 명령을 실행합니다.

참고: 이 명령의 사용은 소프트웨어 버전에 따라 다릅니다.

대역 외 네트워크 관리 기능이 없는 UDLD 적극적인 모드를 구현할 경우, 특히 액세스 레이어에서 또는 오류 비활성화 상황이 발생할 경우 네트워크에서 격리될 수 있는 모든 디바이스에서 errdisable 시간 초과 기능을 사용하는 것이 좋습니다.

`errdisable` 상태에 있는 포트의 시간 제한 기간을 구성하는 방법에 대한 자세한 내용은 이더넷, 고속 이더넷, 기가비트 이더넷 및 10기가비트 이더넷 스위칭 구성 참조하십시오.

권장 사항

정상 모드 UDLD는 대부분의 경우 적절한 기능 및 프로토콜과 함께 제대로 사용할 경우 충분합니다 .이러한 기능/프로토콜은 다음과 같습니다.

- FFI
- 자동 협상
- 루프 가드

UDLD를 구축할 때 양방향 연결(적극적인 모드)에 대한 지속적인 테스트가 필요한지 고려하십시오 .일반적으로 자동 협상이 활성화된 경우 자동 협상이 L1에서 결함 탐지를 보정하므로 적극적인 모드가 필요하지 않습니다.

Cisco에서는 UDLD 메시지 간격이 15초 기본값으로 설정된 Cisco 스위치 간의 모든 포인트-투-포인

트 FE/GE 링크에서 UDLD 일반 모드를 활성화하는 것이 좋습니다.이 컨피그레이션에서는 기본 802.1d 스패닝 트리 타이머를 가정합니다.또한 UDLD를 이중화 및 컨버전스에 STP를 사용하는 네트워크의 루프 가드와 함께 사용합니다.이 권장 사항은 토폴로지에 STP 차단 상태에 하나 이상의 포트가 있는 네트워크에 적용됩니다.

UDLD를 활성화하려면 다음 명령을 실행합니다.

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set
udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

단방향 링크 증상으로 인해 오류가 비활성화된 포트를 수동으로 활성화해야 합니다.**set port enable** 명령을 실행합니다.

자세한 내용은 UDLD(Unidirectional Link Detection Protocol) 기능 이해 및 구성을 참조하십시오.

기타 옵션

단방향 링크에서 발생하는 증상에 대한 보호를 극대화하려면 적극적인 모드 UDLD를 구성합니다.

```
set udld aggressive-mode enable port_range
```

또한 UDLD 메시지 간격 값을 각 끝에서 7~90초(지원되는 경우) 사이로 조정하여 컨버전스를 빠르게 수행할 수 있습니다.

```
set udld interval time
```

errdisable 상황이 발생할 경우 네트워크에서 격리될 수 있는 모든 디바이스에서 errdisable timeout 기능을 사용하는 것이 좋습니다.이러한 상황은 일반적으로 액세스 레이어와 OOB(Out of Band) 네트워크 관리 기능이 없는 UDLD 적극적인 모드를 구현할 때 적용됩니다.

포트가 errdisable 상태로 경우 포트는 기본적으로 다운 상태로 유지됩니다.시간 제한 간격 후 포트를 다시 활성화하는 이 명령을 실행할 수 있습니다.

참고: 시간 제한 간격은 기본적으로 300초입니다.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

파트너 디바이스가 엔드 호스트나 라우터와 같이 UDLD를 지원하지 않는 경우 프로토콜을 실행하지 마십시오.다음 명령을 실행합니다.

```
set udld disable port_range
```

UDLD 테스트 및 모니터링

UDLD는 결함이 있는 GBIC과 같은 실습에서 완전히 결함이 있는/단방향 구성 요소가 없으면 테스트하기가 쉽지 않습니다.이 프로토콜은 일반적으로 실습에 사용되는 시나리오보다 덜 일반적인 오류 시나리오를 탐지하도록 설계되었습니다.예를 들어, 간단한 테스트를 수행하고 원하는 `errdisable` 상태를 확인하기 위해 파이버 선을 하나의 플러그를 뽑으면 L1 자동 협상을 해제해야 합니다.그렇지 않으면 물리적 포트가 다운되어 UDLD 메시지 통신이 재설정됩니다.원격 끝은 UDLD 정상으로 확인되지 않은 상태로 이동합니다.UDLD aggressive 모드를 사용하는 경우 원격 끝이 errdisable 상태 이동합니다.

UDLD에 대한 네이버 PDU 손실을 시뮬레이션하는 추가 테스트 방법이 있습니다.UDLD/CDP 하드웨어 주소를 차단하지만 다른 주소가 전달되도록 하려면 MAC 레이어 필터를 사용합니다.

UDLD를 모니터링하려면 다음 명령을 실행합니다.

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds


>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1      enabled       disabled         bidirectional
```

또한 `enable` 모드에서 CDP가 수행하는 방식으로 UDLD 캐시 내용을 확인하기 위해 숨겨진 show udld neighbor **명령**을 실행할 수 있습니다.프로토콜별 이상 징조가 있는지 확인하기 위해 UDLD 캐시와 CDP 캐시를 비교하는 것이 자주 유용합니다.CDP도 영향을 받을 때마다 모든 PDU/BPDU가 영향을 받습니다.따라서 STP도 선택합니다.예를 들어, 최근 루트 ID 변경 또는 루트/지정 포트 배치 변경 사항을 확인합니다.

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

또한 Cisco UDLD SNMP MIB 변수를 사용하여 UDLD 상태 및 컨피그레이션 일관성을 모니터링할 수 있습니다.

점보 프레임

기본 MTU(Maximum Transmission Unit) 프레임 크기는 모든 이더넷 포트에 대해 1518바이트이며, 여기에는 GE 및 10GE가 포함됩니다.점보 프레임 기능을 사용하면 인터페이스에서 표준 이더넷 프레임 크기보다 큰 프레임을 전환할 수 있습니다.이 기능은 서버 간 성능을 최적화하고 원래 프레임의 크기를 늘리는 MPLS(Multi-Protocol Label Switching), 802.1Q 터널링 및 L2TPv3(Tunneling Protocol Version 3)과 같은 애플리케이션을 지원하기 위해 유용합니다.

운영 개요

IEEE 802.3 표준 사양은 일반 프레임의 경우 1518바이트의 이더넷 프레임 크기를, 캡슐화된 프레임 802.1Q의 경우 1522바이트를 정의합니다.캡슐화된 802.1Q 프레임을 "거대 아기"라고도 합니다.일반적으로 패킷이 특정 이더넷 연결에 대해 지정된 이더넷 최대 길이를 초과할 경우 패킷은 큰 프레임으로 분류됩니다.대형 패킷은 점보 프레임이라고도 합니다.

특정 프레임의 MTU 크기가 1518바이트를 초과할 수 있는 데에는 여러 가지 이유가 있습니다.다음은 몇 가지 예입니다.

- 공급업체별 요구 사항 - 애플리케이션 및 특정 NIC는 표준 1500바이트 외부에 있는 MTU 크기를 지정할 수 있습니다.이러한 MTU 크기를 지정하는 경향 때문에 이더넷 프레임의 크기가 증가하면 평균 처리량이 증가할 수 있다는 것을 입증한 연구 조사 때문입니다.
- 트렁킹 - 스위치나 다른 네트워크 디바이스 간에 VLAN ID 정보를 전달하기 위해 트렁킹을 사용하여 표준 이더넷 프레임을 보강했습니다.오늘날 가장 일반적인 두 가지 트렁킹 형태는 Cisco 전용 ISL 캡슐화와 IEEE 802.1Q입니다.
- MPLS - 인터페이스에서 MPLS가 활성화된 후 패킷의 프레임 크기를 늘릴 수 있습니다.이러한 확장은 MPLS 태그 패킷에 대한 레이블 스택의 레이블 수에 따라 달라집니다.레이블의 총 크기는 4바이트입니다.레이블 스택의 총 크기는 *n* x 4바이트입니다.레이블 스택이 형성되면 프레임이 MTU를 초과할 수 있습니다.
- 802.1Q 터널링 - 802.1Q 터널링 패킷에는 802.1Q 태그 2개가 포함되어 있으며, 이 중 한 번에 하나의 태그만 하드웨어에 표시됩니다.따라서 내부 태그는 MTU 값(페이로드 크기)에 4바이트를 추가합니다.
- UTI(Universal Transport Interface)/L2TPv3 - UTI/L2TPv3은 IP 네트워크를 통해 전달할 L2 데이터를 캡슐화합니다.캡슐화는 원래 프레임 크기를 최대 50바이트까지 늘릴 수 있습니다.새 프레임에는 새 IP 헤더(20바이트), L2TPv3 헤더(12바이트) 및 새 L2 헤더가 포함됩니다.L2TPv3 페이로드는 L2 헤더를 포함하는 전체 L2 프레임으로 구성됩니다.

다양한 Catalyst 스위치를 통해 다양한 프레임 크기를 지원할 수 있는 능력은 하드웨어와 소프트웨어를 포함한 여러 요소에 따라 달라집니다.특정 모듈은 다른 모듈보다 더 큰 프레임 크기를 지원할 수 있으며, 동일한 플랫폼 내에서도 마찬가지입니다.

- Catalyst 5500/5000 스위치는 CatOS 6.1 릴리스의 점보 프레임을 지원합니다.포트에서 점보 프레임 기능을 활성화하면 MTU 크기가 9216바이트로 증가합니다.10/100Mbps UTP(Unshielded Twisted Pair) 기반 라인 카드의 경우 지원되는 최대 프레임 크기는 8092바이트에 불과합니다.이 제한은 ASIC 제한입니다.일반적으로 점보 프레임 크기 기능의 활성화에는 제한이 없습니다.트렁킹/비트렁킹 및 채널링/비채널링에서 이 기능을 사용할 수 있습니다.
- Catalyst 4000 스위치(Supervisor Engine 1 [WS-X4012] 및 Supervisor Engine 2 [WS-X4013])는 ASIC 제한 때문에 점보 프레임을 지원하지 않습니다.그러나 802.1Q 트렁킹은 예외입니다.
- Catalyst 6500 시리즈 플랫폼은 CatOS 릴리스 6.1(1) 이상에서 점보 프레임 크기를 지원할 수 있습니다.그러나 이 지원은 사용하는 라인 카드의 유형에 따라 달라집니다.일반적으로 점보 프레임 크기 기능의 활성화에는 제한이 없습니다.트렁킹/비트렁킹 및 채널링/비채널링에서 이 기능을 사용할 수 있습니다.개별 포트에서 점보 프레임 지원이 활성화된 후 기본 MTU 크기는 9216바이트입니다.기본 MTU는 CatOS를 사용하여 구성할 수 없습니다.그러나 Cisco IOS Software 릴리스 12.1(13)E는 **기본 MTU를 재정의하기 위해** **system jumbomtu** **명령**을 도입했습니다.

자세한 내용은 Catalyst 스위치의 Jumbo/Giant Frame Support 구성 예를 참조하십시오.

이 표에서는 Catalyst 6500/6000 시리즈 스위치의 서로 다른 라인 카드에서 지원되는 MTU 크기에 대해 설명합니다.

참고: MTU 크기 또는 패킷 크기는 이더넷 페이로드만 참조합니다.

라인 카드	MTU 크기
기본값	9216바이트
WS-X6248-RJ-45, WS-X6248A-RJ-45 WS-X6248-TEL, WS-X6248A-TEL WS-X6348-RJ-45(V), WS-X6446 RJ-21(V) 8개	8092바이트(PHY 칩에 의해 제한됨)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9100바이트(@ 100Mbps) 9216바이트(@ 10Mbps)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP	9216바이트
WS-X6324-100FX-MM, -SM, WS-X6024-10FL-MT	9216바이트
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-WS-45X X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, WS-X6316-GE-TX, WS-X6416-GBIC WS-X6516-GBIC Supervisor Engine 1, 2, 32 및 720의 ws-X6516A-GBIC, WS-X6816-GBIC 업링크	9216바이트
WS-X6516-GE-TX	8092바이트(@ 100Mbps) 9216바이트(@ 10 또는 1000Mbps)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-WS-TX, WS-TX-X6548-GE-45AF	1500바이트(점보 프레임은 지원되지 않음)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx Series	9216바이트
OSM ATM(OC12c)	9180바이트
OSM CHOC3, CHOC12, CHOC48, CT3	9216바이트(OCx 및 DS3) 7673바이트(T1/E1)
Flex WAN	7673바이

	트(CT3 T1/DS0) 9216바이트(OC3c POS) 7673바이트(T1)
CSM(WS-X6066-SLB-APC)	9216바이트(CSM 3.1(5) 및 3.2(1) 기준)
OSM POS OC3c, OC12c, OC48c;OSM DPT OC48c, OSM GE WAN	9216바이트

레이어 3 점보 프레임 지원

Supervisor Engine 및 MSFC에서 실행되는 Cisco IOS Software에서 실행되는 CatOS를 사용하는 경우, Catalyst 6500/6000 스위치는 PFC/MSFC2, PFC2/MSFC2 이상의 하드웨어를 사용하여 Cisco IOS® Software Release 12.1(2)E 이상에서 L3 점보 프레임 지원을 제공합니다.인그레스(ingress) 및 이그레스(egress) VLAN이 점보 프레임에 대해 구성된 경우 모든 패킷은 PFC가 유선 속도로 하드웨어를 스위칭합니다.인그레스 VLAN이 점보 프레임에 대해 구성되어 있고 이그레스 VLAN이 구성되지 않은 경우 두 가지 시나리오가 있습니다.

- DF(Don't Fragment) 비트 설정(경로 MTU 검색용)이 설정된 엔드 호스트에서 보내는 점보 프레임 - 패킷이 삭제되고 ICMP(Internet Control Message Protocol)에 연결할 수 없는 경우 메시지 코드 DF 있는 엔드 호스트로 .
- DF 비트가 설정되지 않은 엔드 호스트가 전송하는 점보 프레임 - 패킷은 MSFC2/MSFC3에 펀딩되어 소프트웨어에서 조각화되고 전환됩니다.

이 표에는 다양한 플랫폼에 대한 L3 점보 지원이 요약되어 있습니다.

L3 스위치 또는 모듈	최대 L3 MTU 크기
Catalyst 2948G-L3/4908G-L3 Series	점보 프레임은 지원되지 않습니다.
Catalyst 5000 RSM[1]/RSFC[2]	점보 프레임은 지원되지 않습니다.
Catalyst 6500 MSFC1	점보 프레임은 지원되지 않습니다.
Catalyst 6500 MSFC2 이상	Cisco IOS Software 릴리스 12.1(2)E:9216바이트

[1] RSM = Route Switch Module

[2] RSFC = Route Switch 기능 카드

네트워크 성능 고려 사항

TCP over WAN(인터넷)의 성능이 광범위하게 연구되었습니다.이 수식은 TCP 처리량이 다음 기준에 따라 상한값을 갖는 방법을 설명합니다.

- MTU 길이에서 TCP/IP 헤더의 길이를 뺀 MSS(Maximum Segment Size)
- 왕복 시간(RTT)
- 패킷 손실

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

이 공식에 따르면 실현 가능한 최대 TCP 처리량은 MSS에 직접 비례합니다.지속적인 RTT 및 패킷 손실을 통해 패킷 크기를 두 배로 늘리면 TCP 처리량을 두 배로 늘릴 수 있습니다.마찬가지로, 1518바이트 프레임 대신 점보 프레임을 사용할 경우 6배 증가한 크기가 이더넷 연결의 TCP 처리량이 6배 증가할 수 있습니다.

두 번째로, 서버 팜의 성능 요구 사항이 지속적으로 증가함에 따라 NFS(Network File System) UDP 데이터그램으로 데이터 속도를 높일 수 있는 보다 효율적인 방법이 필요합니다.NFS는 UNIX 기반 서버 간에 파일을 전송하는 가장 널리 구축된 데이터 스토리지 메커니즘으로, 8,400바이트 규모의 데이터그램을 제공합니다.이더넷의 확장 9KB MTU를 고려했을 때 단일 점보 프레임은 8KB 애플리케이션 데이터그램(예: NFS)과 패킷 헤더 오버헤드를 전달할 수 있을 만큼 큽니다.이 기능은 부수적으로 호스트에서 NFS 블록을 별도의 UDP 데이터그램으로 분할하기 위해 더 이상 필요하지 않으므로 DMA(Direct Memory Access) 전송을 더 효율적으로 수행할 수 있습니다.

권장 사항

점보 프레임을 지원하려는 경우 모든 스위치 모듈(L2) 및 인터페이스(L3)가 점보 프레임을 지원하는 네트워크 영역으로 점보 프레임 사용을 제한합니다.이 컨피그레이션은 경로의 어느 위치에서나 단편화를 방지합니다.패스에서 지원되는 프레임 길이보다 큰 점보 프레임을 구성하면 단편화가 필요하므로 이 기능을 사용하여 얻을 수 있는 모든 이점이 없어집니다.이 점보 프레임 섹션의 표에서 볼 수 있듯이 지원되는 최대 패킷 크기에 따라 다양한 플랫폼과 라인 카드가 달라질 수 있습니다.

호스트 디바이스가 상주하는 전체 L2 VLAN에 대해 네트워크 하드웨어에서 지원하는 최소 공통 분모인 MTU 크기의 점보 프레임 인식 호스트 디바이스를 구성합니다.점보 프레임을 지원하는 모듈에 대한 점보 프레임 지원을 활성화하려면 다음 명령을 실행합니다.

```
set port jumbo mod/port enable
```

또한 L3 경계 전체에서 점보 프레임을 지원하려는 경우 해당 모든 VLAN 인터페이스에서 사용 가능한 최대 MTU 값인 9216바이트를 구성합니다.VLAN 인터페이스 아래에서 mtu 명령을 실행합니다.

```
interface vlan vlan# mtu 9216
```

이 컨피그레이션을 통해 모듈에서 지원되는 L2 점보 프레임 MTU는 트래픽이 통과하는 L3 인터페이스에 대해 구성된 값보다 항상 작거나 같습니다.이렇게 하면 트래픽이 L3 인터페이스를 통해 VLAN에서 라우팅될 때 프래그먼트화가 방지됩니다.

관리 구성

Catalyst 네트워크를 제어, 프로비저닝 및 트러블슈팅하는 데 도움이 되는 고려 사항에 대해서는 이 섹션에서 설명합니다.

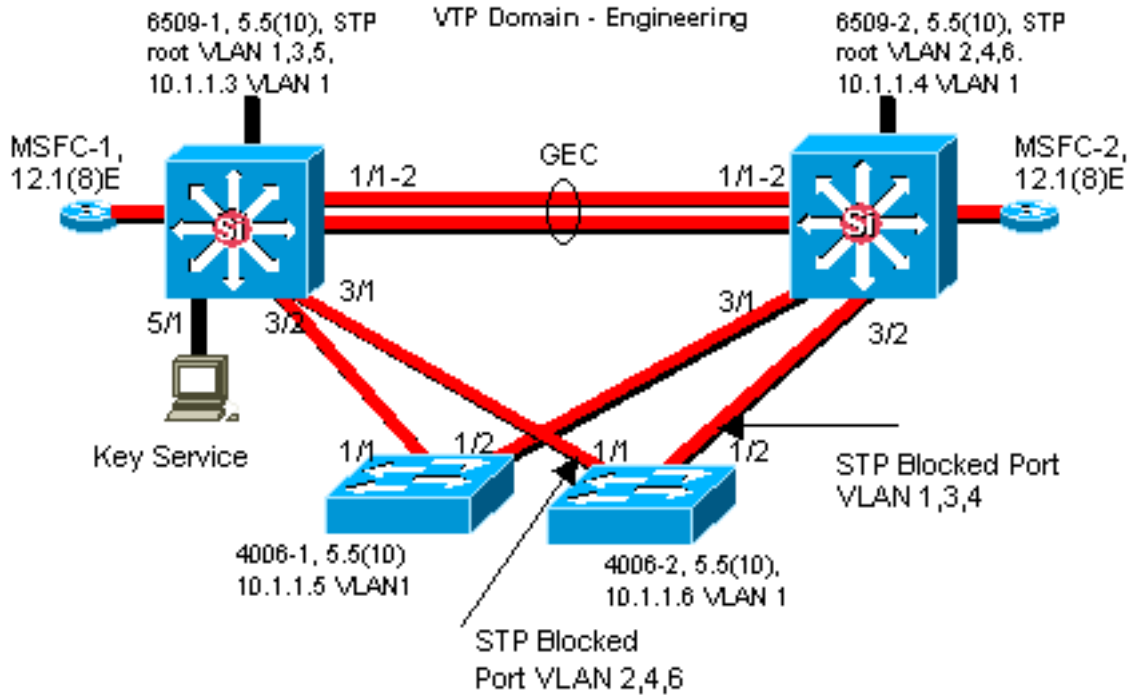
네트워크 다이어그램

네트워크 다이어그램 지우기는 네트워크 운영의 기본 요소입니다.문제 해결 과정에서 중요한 역할을 하게 되며, 가동 중단 시 공급업체 및 파트너에게 정보를 에스컬레이션할 때 가장 중요한 수단으로 활용됩니다.준비, 준비 상태, 접근성을 과소평가해서는 안 됩니다.

권장 사항

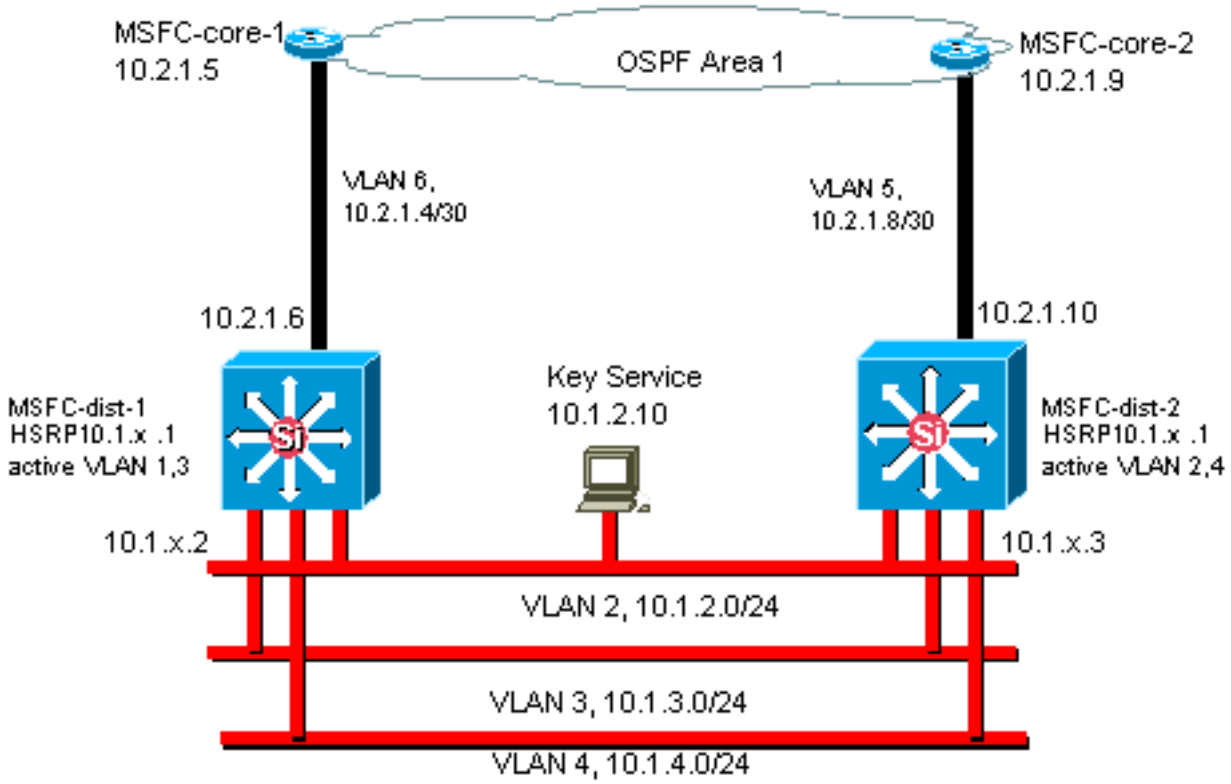
다음 세 가지 다이어그램을 만드는 것이 좋습니다.

- **전체 다이어그램**—대규모 네트워크에서도 엔드 투 엔드 물리적 및 논리적 연결을 보여주는 다이어그램이 중요합니다.계층적 설계를 구현하여 각 레이어를 개별적으로 문서화하는 기업은 일반적일 수 있습니다.그러나 계획 및 문제 해결 과정에서 도메인이 어떻게 연결되는지 잘 알고 있는 경우가 많습니다.
- **Physical Diagram**(물리적 다이어그램) - 모든 스위치 및 라우터 하드웨어 및 케이블을 표시합니다.VLAN별 트렁크, 링크, 속도, 채널 그룹, 포트 번호, 슬롯, 섀시 유형, 소프트웨어, VTP 도메인, 루트 브리지, 백업 루트 브리지 우선 순위, MAC 주소 및 차단된 포트에 레이블이 지정되어야 합니다.Catalyst 6500/6000 MSFC와 같은 내부 디바이스를 트렁크를 통해 연결된 스틱의 라우터로 표시하는 것이 더 분명합니다



.

- **Logical Diagram(논리적 다이어그램)** - L3 기능(라우터는 개체로, VLAN은 이더넷 세그먼트로)만 표시합니다.IP 주소, 서브넷, 보조 주소 지정, HSRP 활성 및 대기, 액세스 코어 디스트리뷰션 레이어 및 라우팅 정보에 레이블이 지정되어야 합니다



.

대역 내 관리

컨피그레이션에 따라 스위치 인밴드(내부) 관리 인터페이스(sc0)가 다음 데이터를 처리해야 할 수 있습니다.

- SNMP, 텔넷, SSH(Secure Shell Protocol) 및 syslog와 같은 스위치 관리 프로토콜
- 브로드캐스트 및 멀티캐스트와 같은 사용자 데이터
- STP BPDU, VTP, DTP, CDP 등의 스위치 제어 프로토콜

Cisco 멀티레이어 설계에서는 스위치드 도메인을 포괄하고 모든 sc0 인터페이스를 포함하는 관리 VLAN을 구성하는 것이 일반적입니다.따라서 관리 트래픽과 사용자 트래픽을 분리하여 스위치 관리 인터페이스의 보안을 강화할 수 있습니다.이 섹션에서는 기본 VLAN 1을 사용하고 사용자 트래픽과 동일한 VLAN에서 스위치로 관리 트래픽을 실행하는 경우의 중요성과 잠재적 문제에 대해 설명합니다.

운영 개요

사용자 데이터에 대한 VLAN 1의 사용에 대한 주요 문제는 일반적으로 엔드스테이션에서 생성되는 많은 멀티캐스트 및 브로드캐스트 트래픽에 의해 수퍼바이저 엔진 NMP가 중단될 필요가 없다는 것입니다.기존의 Catalyst 5500/5000 하드웨어인 Supervisor Engine I 및 Supervisor Engine II는 특히 이 트래픽을 처리하기 위한 리소스가 제한적입니다. 이 원칙은 모든 Supervisor Engine에 적용됩니다.Supervisor Engine CPU, 버퍼 또는 백플레인에 대한 대역 내 채널이 불필요한 트래픽의 청취를 완전히 수행할 경우 제어 프레임을 놓칠 수 있습니다.최악의 경우 스패닝 트리 루프 또는 EtherChannel 장애로 이어질 수 있습니다.

Catalyst에서 **show interface** 및 **show ip stats** 명령이 실행된 경우 유니캐스트 트래픽에 대한 브로드캐스트 비율 및 비IP 트래픽에 대한 비율(관리 VLAN에서 일반적으로 보이지 않음)을 나타낼 수 있습니다.

이전 Catalyst 5500/5000 하드웨어의 상태 확인은 **show inband**의 출력을 검사하는 것입니다. 라우

터의 버퍼 드롭과 유사한 리소스 오류(RsccErrors)에 대한| biga(**숨김 명령**)입니다.이러한 리소스 오류가 계속 증가하면 관리 VLAN의 상당한 양의 브로드캐스트 트래픽 때문에 시스템 패킷을 수신하는 데 메모리를 사용할 수 없습니다.단일 리소스 오류는 Supervisor Engine이 BPDU와 같은 패킷을 처리할 수 없음을 의미할 수 있습니다. 스패닝 트리 같은 프로토콜은 누락된 BPDU를 다시 전송하지 않으므로 문제가 빠르게 발생할 수 있습니다.

권장 사항

이 문서의 Cat Control 섹션에서 강조 표시된 대로 VLAN 1은 대부분의 컨트롤 플레인 트래픽을 태그 지정하고 처리하는 특수 VLAN입니다.VLAN 1은 기본적으로 모든 트렁크에서 활성화됩니다.더 큰 캠퍼스 네트워크를 사용하는 경우 VLAN 1 STP **도메인**의 지름에 대해 주의해야 합니다.네트워크의 한 부분이 불안정하면 VLAN 1에 영향을 미칠 수 있으므로 컨트롤 플레인 안정성과 다른 모든 VLAN에 대한 STP 안정성에 영향을 줄 수 있습니다.CatOS 5.4 이상에서는 다음 명령을 사용하여 VLAN 1을 사용자 데이터를 전송하고 STP를 실행하는 것을 제한할 수 있었습니다.

```
clear trunk mod/port vlan 1
```

이렇게 해도 네트워크 분석기와 같이 VLAN 1에서 스위치로 전송되는 제어 패킷은 중지되지 않습니다.그러나 데이터가 전달되지 않으며 STP가 이 링크를 통해 실행되지 않습니다.따라서 이 기술을 사용하여 VLAN 1을 더 작은 장애 도메인으로 분할할 수 있습니다.

참고: 현재 3500 및 2900XL에서 VLAN 1 트렁크를 지울 수 없습니다.

사용자 VLAN을 비교적 작은 스위치 도메인으로 제한하기 위해 캠퍼스 설계를 고려했지만 그에 따라 작은 장애/L3 경계로 제한하더라도, 일부 고객은 관리 VLAN을 다르게 취급하고 단일 관리 서브넷으로 전체 네트워크를 보호하려고 합니다.중앙 NMS 애플리케이션이 관리하는 디바이스에 L2가 인접해야 하며, 이것이 검증된 보안 인수여야 하는 기술적 이유는 없습니다.Cisco에서는 관리 VLAN의 지름을 사용자 VLAN과 동일한 라우티드 도메인 구조로 제한하고 네트워크 관리 보안을 강화하기 위해 대역 외 관리 및/또는 CatOS 6.x SSH 지원을 고려하는 것이 좋습니다.

기타 옵션

그러나 일부 토폴로지에서는 이러한 Cisco 권장 사항에 대한 설계 고려 사항이 있습니다.예를 들어, 바람직한 공통 Cisco 멀티레이어 설계는 활성 스패닝 트리 사용을 방지하는 것입니다.이를 위해서는 각 IP 서브넷/VLAN을 단일 액세스 레이어 스위치 또는 스위치 클러스터로 제한해야 합니다.이러한 설계에서는 액세스 레이어까지 트렁킹을 구성할 수 없습니다.

L2 액세스와 L3 디스트리뷰션 레이어 간에 이를 전달하기 위해 별도의 관리 VLAN을 생성하고 트렁킹을 활성화할지 여부에 대한 질문에 대한 쉬운 답은 없습니다.다음은 Cisco 엔지니어와 함께 설계 검토를 위한 두 가지 옵션입니다.

- **옵션 1:**디스트리뷰션 레이어에서 각 액세스 레이어 스위치까지 2개 또는 3개의 고유한 VLAN을 트렁크합니다.이를 통해 데이터 VLAN, 음성 VLAN 및 관리 VLAN을 사용할 수 있으며 STP가 비활성 상태라는 이점이 있습니다.(트렁크에서 VLAN 1이 지워지면 추가 컨피그레이션 단계가 있습니다.) 이 솔루션에는 장애 복구 중에 라우팅된 트래픽이 일시적으로 블랙홀링되지 않도록 하기 위해 고려해야 할 설계 지점이 있습니다.트렁크의 경우 STP PortFast(CatOS 7.x 이상) 또는 STP 포워딩과의 VLAN 자동 상태 동기화(CatOS 5.5[9] 이후).
- **옵션 2:**데이터 및 관리를 위한 단일 VLAN을 사용할 수 있습니다.더 강력한 CPU 및 컨트롤 플레인 속도 제한 제어 같은 최신 스위치 하드웨어와 멀티레이어 설계에서 권장하는 비교적 작은

브로드캐스트 도메인을 포함하는 설계로 인해 많은 고객이 sc0 인터페이스를 사용자 데이터와 분리시키는 것은 이전보다 문제가 되지 않습니다.최종 결정은 해당 VLAN에 대한 브로드캐스트 트래픽 프로필 검토 및 Cisco 엔지니어와 스위치 하드웨어 기능에 대한 논의와 함께 하는 것이 가장 좋습니다.관리 VLAN에 해당 액세스 레이어 스위치의 모든 사용자가 포함되어 있는 경우, 이 문서의 Security Configuration 섹션에서 설명한 대로 IP 입력 필터를 사용하여 사용자의 스위치를 보호하는 것이 좋습니다.

대역 외 관리

앞의 단원의 주장을 한 단계 더 자세히 살펴보면, 트래픽 제어 또는 컨트롤 플레인 이벤트가 발생하더라도 항상 원격으로 장치에 연결할 수 있도록 운영 네트워크에 별도의 관리 인프라를 구축함으로써 네트워크 관리를 더욱 높은 수준으로 수행할 수 있습니다.이 두 가지 방법은 일반적으로 다음과 같습니다.

- 전용 LAN을 통한 대역 외 관리
- 터미널 서버를 통한 대역 외 관리

운영 개요

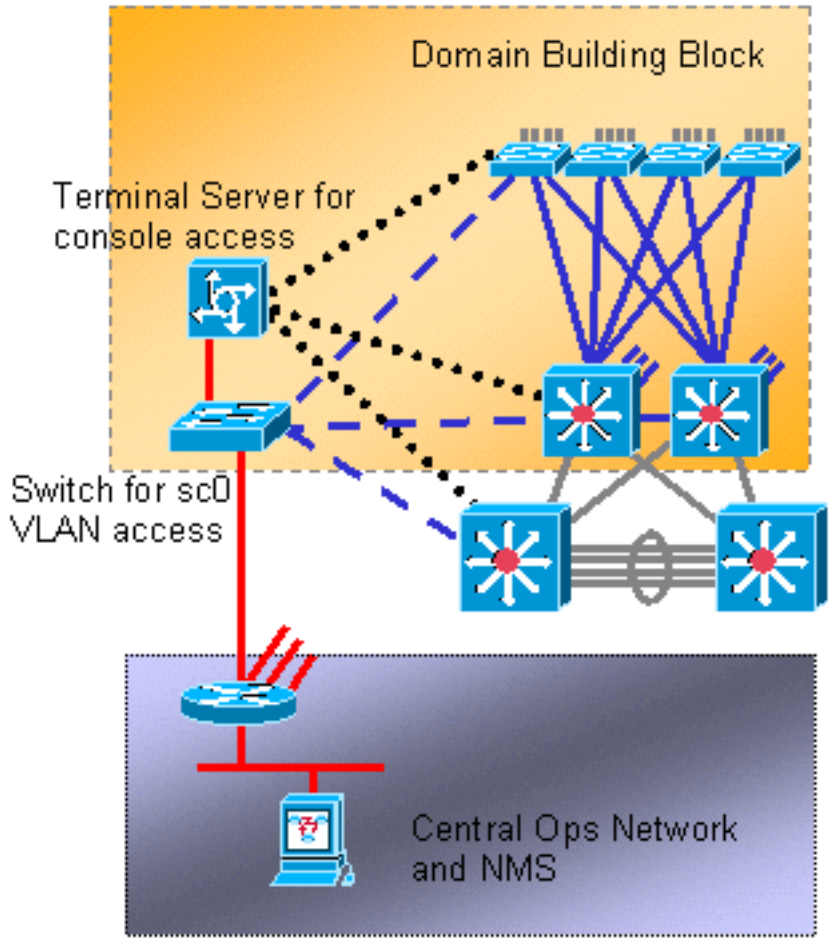
네트워크의 모든 라우터와 스위치에는 관리 VLAN에서 대역외 이더넷 관리 인터페이스가 제공됩니다.각 디바이스의 이더넷 포트 하나가 관리 VLAN에 구성되고 프로덕션 네트워크 외부의 sc0 인터페이스를 통해 별도의 스위치드 관리 네트워크에 케이블로 연결됩니다.Catalyst 4500/4000 스위치에는 Supervisor Engine에 스위치 포트가 아닌 대역 외 관리에만 사용되는 특수한 me1 인터페이스가 있습니다.

또한 RJ-45-직렬 케이블을 사용하는 Cisco 2600 또는 3600을 구성하여 레이아웃의 모든 라우터 및 스위치의 콘솔 포트에 액세스할 수 있습니다.또한 터미널 서버는 모든 디바이스의 보조 포트에 있는 모뎀과 같은 백업 시나리오를 구성할 필요가 없습니다.네트워크 연결 실패 시 다른 장치에 전화 접속 서비스를 제공하도록 터미널 서버의 보조 포트에 단일 모뎀을 구성할 수 있습니다.

권장 사항

이러한 방식으로 모든 스위치와 라우터에 대한 2개의 대역외 경로가 수많은 대역 내 경로 외에 추가로 가능하므로 가용성이 높은 네트워크 관리가 가능합니다.아웃오브밴드(Out-of-Band)의 책임:

- 아웃오브밴드(out-of-band) 방식으로 관리 트래픽을 사용자 데이터와 분리합니다.
- OOB(Out-of-Band)에는 별도의 서브넷, VLAN 및 스위치에 관리 IP 주소가 있어 보안을 강화합니다.
- 아웃오브밴드(Out-of-Band)는 네트워크 장애 시 관리 데이터 전달을 더욱 확실하게 보장합니다.
- 대역 외(out-of-band)에는 관리 VLAN에 활성 스패닝 트리가 없습니다.이중화는 중요하지 않습니다.



시스템 테스트

부팅 진단

시스템 부팅 중에, 결함이 있는 하드웨어가 네트워크에 지장을 주지 않도록 안정적이고 운영 플랫폼을 사용할 수 있도록 하기 위해 여러 프로세스가 수행됩니다.Catalyst 부트 진단은 POST(Power-On Self Test)와 온라인 진단 간에 분할됩니다.

운영 개요

플랫폼 및 하드웨어 컨피그레이션에 따라 부팅 시, 그리고 카드를 섀시로 핫 스왑 시 다른 진단 프로그램이 수행됩니다.진단 수준이 높을수록 더 많은 수의 문제가 발견되지만 부팅 주기가 길어집니다.다음 3가지 수준의 POST 진단 기능을 선택할 수 있습니다(모든 테스트는 DRAM, RAM, 캐시 현재 상태 및 크기를 확인하고 초기화함).

운영 개요			
우회	해당 없음	3	CatOS 5.5 이전 버전을 사용하는 4500/4000 시리즈에서는 사용할 수 없습니다.
최소	첫 번째 MB의 DRAM에서만 패턴 쓰기 테스트입니다.	30	5500/5000 및 6500/6000 시리즈의 기본값4500/4000 시리즈에서는 사용할 수 없습니다.
완료	모든 메모리에 대한 패턴 쓰기 테스트입니다.	60	4500/4000 시리즈의 기본값.

온라인 진단

이러한 테스트는 스위치에서 내부적으로 패킷 경로를 확인합니다.따라서 온라인 진단은 단순히 포트 테스트가 아닌 시스템 차원의 테스트라는 점에 유의해야 합니다.Catalyst 5500/5000 및 6500/6000 스위치에서는 먼저 대기 Supervisor Engine에서, 그리고 다시 기본 Supervisor Engine에서 테스트를 수행합니다.진단 프로그램의 길이는 시스템 컨피그레이션(슬롯, 모듈, 포트 수)에 따라 달라집니다. 테스트에는 세 가지 범주가 있습니다.

- 루프백 테스트 - Supervisor Engine NMP의 패킷이 각 포트로 전송되고 NMP로 반환되고 오류를 검사합니다.
- 번들링 테스트 - 최대 8개의 포트로 구성된 채널이 생성되고 에이전트에게 루프백 테스트를 수행하여 특정 링크에 대한 해싱을 확인합니다(자세한 내용은 이 문서의 EtherChannel 섹션 참조).
- EARL(Enhanced Address Recognition Logic) 테스트 - 중앙 수퍼바이저 엔진 및 인라인 이더넷 모듈 L3 재작성 엔진이 모두 테스트됩니다.각 모듈의 스위칭 하드웨어를 통해 NMP에서 샘플 패킷을 전송하기 전에(각 프로토콜 캡슐화 유형에 대해) 하드웨어 포워딩 항목과 라우티드 포트가 생성되어 NMP로 돌아갑니다.이는 Catalyst 6500/6000 PFC 모듈 이상용입니다.

전체 온라인 진단을 수행하는 데 약 2분이 걸릴 수 있습니다.최소 진단은 Supervisor Engine 이외의 모듈에서 번들 또는 재작성 테스트를 수행하지 않으며 약 90초가 걸릴 수 있습니다.

메모리 테스트 중에 작성된 패턴과 비교하여 다시 읽은 패턴에서 차이가 발견되면 포트 상태가 으로 변경됩니다.이러한 테스트의 결과는 **show test** 명령이 실행된 후 검사할 모듈 번호가 오는 경우 확인할 수 있습니다.

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ----------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ----------------- . . . .
```

권장 사항

Cisco는 모든 스위치를 완벽한 진단을 사용하여 장애 탐지를 극대화하고 정상적인 운영 중에 중단을 방지하도록 권장합니다.

참고: 이 변경 사항은 다음에 장치를 부팅할 때까지 적용되지 않습니다.전체 진단을 설정하려면 다음 명령을 실행합니다.

```
set test diaglevel complete
```

기타 옵션

경우에 따라 전체 진단을 실행하기 위해 기다리는 것보다 빠른 부팅 시간을 사용하는 것이 좋습니다.시스템을 구축하는 데 다른 요인과 시간이 포함되지만, 전반적으로 POST 및 온라인 진단은 3분의 1을 더 적시에 추가합니다.Catalyst 6509가 장착된 완전히 채워진 단일 Supervisor Engine 9슬롯 섀시를 사용하여 테스트한 경우, 전체 진단 기능으로 약 380초, 최소 진단 기능으로 약 300초, 진단 우회로 단 250초만 부팅했습니다.우회를 구성하려면 다음 명령을 실행합니다.

```
set test diaglevel bypass
```

참고: Catalyst 4500/4000은 최소 진단을 위해 구성된 것을 받아들이지만, 이 경우 전체 테스트가 계속 진행됩니다.이 플랫폼에서는 향후 최소 모드를 지원할 수 있습니다.

런타임 진단

시스템이 작동하면 스위치 Supervisor Engine은 다른 모듈에 대해 다양한 모니터링을 수행합니다.관리 메시지(대역외 관리 버스를 통해 실행되는 SCP[Serial Control Protocol])를 통해 모듈에 연결할 수 없는 경우 수퍼바이저 엔진은 카드를 재시작하거나 필요에 따라 다른 작업을 수행합니다.

운영 개요

수퍼바이저 엔진은 자동으로 다양한 모니터링을 수행합니다.컨피그레이션이 필요하지 않습니다.Catalyst 5500/5000 및 6500/6000의 경우 스위치의 다음 구성 요소가 모니터링됩니다.

- 감시장치를 통한 NMP
- 향상된 EARL 칩 오류
- Supervisor Engine에서 후면판까지 인밴드 채널
- Keepalive over-of-band 채널(Catalyst 6500/6000)을 통한 모듈
- Active Supervisor Engine은 대기 Supervisor Engine에서 상태를 모니터링합니다(Catalyst 6500/6000).

시스템 및 하드웨어 오류 감지

운영 개요

CatOS 6.2 이상에서는 중요한 시스템 및 하드웨어 수준 구성 요소를 모니터링하기 위해 추가 기능이 추가되었습니다.다음 세 가지 하드웨어 구성 요소가 지원됩니다.

- 인밴드
- 포트 카운터
- 메모리

기능이 활성화되고 오류 조건이 감지되면 스위치에서 syslog 메시지를 생성합니다.이 메시지는 심각한 성능 저하가 발생하기 전에 문제가 있음을 관리자에게 알립니다.CatOS 버전 6.4(16), 7.6(12), 8.4(2) 이상에서 세 구성 요소 모두의 기본 모드가 비활성화에서 활성화로 변경되었습니다.

인밴드

인밴드(inband) 오류가 탐지되면 syslog 메시지는 심각한 성능 저하가 발생하기 전에 문제가 있음을 알려줍니다.이 오류는 인밴드 오류 발생 유형을 표시합니다.예를 들면 다음과 같습니다.

- 인밴드 고정
- 리소스 오류
- 부팅 중 인밴드 실패

인밴드 ping 오류가 감지되면 이 기능은 인밴드 연결, CPU 및 스위치의 백플레인 로드 시 현재 Tx 및 Rx 속도의 스냅샷과 함께 추가 syslog 메시지를 보고합니다.이 메시지를 사용하면 인밴드가 고정되었는지(Tx/Rx 없음) 또는 오버로드(과도한 Tx/Rx) 여부를 올바르게 확인할 수 있습니다. 이 추가 정보를 통해 인밴드 ping 실패의 원인을 확인할 수 있습니다.

포트 카운터

이 기능을 활성화하면 포트 카운터를 디버깅하는 프로세스가 생성되고 시작됩니다.포트 카운터는 정기적으로 일부 내부 포트 오류 카운터를 모니터링합니다.라인 카드의 아키텍처, 특히 모듈의 ASIC에 따라 기능 쿼리에 대한 카운터가 결정됩니다.그런 다음 Cisco 기술 지원 또는 개발 엔지니어링에서 이 정보를 사용하여 문제를 해결할 수 있습니다.이 기능은 링크 파트너 연결과 직접 연결된 FCS, CRC, 정렬 및 런트와 같은 오류 카운터를 폴링하지 않습니다.이 기능을 통합하려면 이 문서의 EtherChannel/Link 오류 처리 섹션을 참조하십시오.

폴링은 30분마다 실행되며 선택한 오류 카운터의 백그라운드에서 실행됩니다.동일한 포트에서 두 개의 후속 폴링 사이에 카운트가 증가하면 syslog 메시지가 인시던트를 보고하고 모듈/포트 및 오류 카운터 세부 정보를 제공합니다.

포트 카운터 옵션은 Catalyst 4500/4000 플랫폼에서 지원되지 않습니다.

메모리

이 기능을 활성화하면 DRAM 손상 조건의 백그라운드 모니터링 및 탐지가 수행됩니다.이러한 메모리 손상 조건은 다음과 같습니다.

- 할당
- 여유 공간
- 범위를 벗어남
- 잘못된 맞춤

권장 사항

인밴드, 포트 카운터 및 메모리를 포함한 모든 오류 감지 기능을 활성화합니다. 여기서 이 기능은 지원됩니다.이러한 기능을 활성화하면 Catalyst 스위치 플랫폼에 대한 사전 대응적 시스템 및 하드웨어 경고 진단 기능이 향상됩니다.세 가지 오류 탐지 기능을 모두 활성화하려면 다음 명령을 실행합니다.

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

오류 탐지가 활성화되었는지 확인하려면 다음 명령을 실행합니다.

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

EtherChannel/링크 오류 처리

운영 개요

CatOS 8.4 이상에서는 EtherChannel의 한 포트에서 동일한 EtherChannel의 다른 포트로 트래픽을 자동으로 페일오버하는 기능을 제공하기 위해 새로운 기능이 도입되었습니다.채널의 포트 중 하나가 지정된 간격 동안 구성 가능한 오류 임계값을 초과할 경우 포트 장애 조치가 발생합니다.포트 페일오버는 EtherChannel에 운영 포트가 남아 있는 경우에만 발생합니다.장애가 발생한 포트가 EtherChannel의 마지막 포트인 경우 포트는 상태로 들어가지 않습니다.이 포트는 수신된 오류 유형에 관계없이 트래픽을 계속 전달합니다.단일 비채널링 포트는 상태로 이동하지 않습니다.이러한 포트는 지정된 간격 동안 오류 임계값 초과되면 errdisable 상태로 전환됩니다.

이 기능은 errordetection **포트 카운터**를 **설정할** 때만 **유효합니다**.모니터링할 링크 오류는 3개의 카운터를 기반으로 합니다.

- 오류 발생
- RxCRCs(CRCAlignErrors)
- TxCRC

오류 카운터 수를 표시하려면 스위치**에서** show counters **명령**을 실행합니다.예:

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

이 테이블은 가능한 컨피그레이션 매개변수 및 각 기본 컨피그레이션의 목록입니다.

매개변수	기본값
글로벌	비활성화됨
RxCRC용 포트 모니터	비활성화됨
InErrors용 포트 모니터	비활성화됨
TxCRC용 포트 모니터	비활성화됨
작업	포트 장애 조치
간격	30초
샘플링 수	3회 연속
낮은 임계값	1000
높은 임계값	1001

이 기능이 활성화되고 포트의 오류 수가 지정된 샘플링 수 기간 내에 구성 가능한 임계값의 높은 값에 도달하면 구성 가능한 작업은 오류 비활성화 또는 포트 장애 조치입니다.error disable 작업은 포트를 errdisable 상태 전환합니다.포트 장애 조치 작업을 구성할 경우 포트 채널 상태가 고려됩니다.포트가 채널에 있지만 해당 포트가 채널의 마지막 작동 포트가 아닌 경우에만 포트가 비활성화됩니다.또한 구성된 작업이 포트 장애 조치이고 포트가 단일 포트 또는 비입력 포트인 경우 포트 오류 수가 임계값의 높은 값에 도달할 때 포트가 errdisable 상태가 됩니다.

간격은 포트 오류 카운터를 읽는 데 사용되는 타이머 상수입니다.링크 오류 간격의 기본값은 30초입니다.허용되는 범위는 30~1800초입니다.

예기치 않은 일회성 이벤트로 인해 포트가 실수로 잘못 비활성화될 위험이 있습니다.이러한 위험을 최소화하기 위해, 이 연속 샘플링 횟수를 통해 조건이 지속되는 경우에만 포트에 대한 작업이 수행됩니다.기본 샘플링 값은 3이고 허용되는 범위는 1~255입니다.

임계값은 링크 오류 간격을 기준으로 확인할 절대 숫자입니다.기본 링크 오류 하한 임계값은 1000이고 허용되는 범위는 1~65,535입니다. 기본 링크 오류 상한 임계값은 1001입니다.샘플링 시간의 연속 수가 낮은 임계값에 도달하면 syslog가 전송됩니다.연속 샘플링 시간이 높은 임계값에 도달하면 syslog가 전송되고 오류 비활성화 또는 포트 장애 조치 작업이 트리거됩니다.

참고: 채널의 모든 포트에 대해 동일한 포트 오류 감지 컨피그레이션을 사용합니다.자세한 내용은 Catalyst 6500 Series 소프트웨어 구성 가이드의 다음 절을 참조하십시오.

- Checking *Status and Connectivity의 Configuring EtherChannel/Link Error* Handling 섹션
- 이더넷, 고속 이더넷, 기가비트 이더넷 및 10기가비트 이더넷 스위칭 구성의 포트 오류 감지 구성 섹션

권장 사항

이 기능은 데이터를 기록 및 비교하기 위해 SCP 메시지를 사용하므로 활성 포트 수가 많을수록 CPU 사용량이 많을 수 있습니다.임계값 간격이 매우 작은 값으로 설정된 경우 이 시나리오에서는 CPU 사용량이 더 많습니다.중요 링크로 지정된 포트에 대해 재량에 따라 이 기능을 활성화하고 민감한 애플리케이션에 대해 트래픽을 전달합니다.링크 오류 감지를 전역적으로 활성화하려면 이 명령을 실행합니다.

```
set errordetection link-errors enable
```

또한 기본 임계값, 간격 및 샘플링 매개변수로 시작합니다.기본 작업인 포트 장애 조치를 사용합니다.

개별 포트에 전역 링크 오류 매개변수를 적용하려면 다음 명령을 실행합니다.

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

링크 오류 컨피그레이션을 확인하기 위해 다음 명령을 실행할 수 있습니다.

```
show errordetection

show port errordetection {mod | mod/port}
```

Catalyst 6500/6000 패킷 버퍼 진단

CatOS 버전 6.4(7), 7.6(5) 및 8.2(1)에서는 Catalyst 6500/6000 패킷 버퍼 진단 기능이 도입되었습니다.기본적으로 활성화된 패킷 버퍼 진단은 일시적인 SRAM(Static RAM) 장애로 인해 발생하는 패킷 버퍼 오류를 탐지합니다.탐지는 다음과 같은 48포트 10/100Mbps 라인 모듈에서 이루어집니다.

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

장애 상태가 발생하면 48개의 10/100Mbps 포트 중 12개는 계속 연결되어 있으며 랜덤 연결 문제가 발생할 수 있습니다.이 상태에서 복구하는 유일한 방법은 라인 모듈의 전원을 껐다가 켜는 것입니다.

운영 개요

패킷 버퍼 진단은 패킷 버퍼의 특정 섹션에 저장된 데이터를 확인하여 일시적인 SRAM 장애로 인해 손상되었는지 확인합니다.프로세스가 작성한 것과 다른 내용을 읽으면 구성 가능한 두 가지 복구 옵션을 수행합니다.

1. 기본 작업은 버퍼 장애의 영향을 받는 라인 카드 포트를 error disable하는 것입니다.
2. 두 번째 옵션은 라인 카드의 전원을 껐다가 켜는 것입니다.

2개의 syslog 메시지가 추가되었습니다.이 메시지는 패킷 버퍼 오류로 인해 포트의 오류 비활성화 또는 모듈의 전력 주기에 대한 경고를 제공합니다.

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

8.3 및 8.4 이전의 CatOS 버전에서는 라인 카드 전원 주기 시간이 30~40초입니다.CatOS 버전 8.3 및 8.4에 Rapid Boot 기능이 도입되었습니다. 이 기능은 부팅 시간을 최소화하기 위해 초기 부팅 프로세스 중에 설치된 라인 카드에 펌웨어를 자동으로 다운로드합니다.Rapid Boot 기능은 전원 사이클 시간을 약 10초로 단축합니다.

권장 사항

Cisco에서는 errdisable의 기본 옵션을 *권장합니다*.이 작업은 운영 시간 동안 네트워크 서비스에 미치는 영향이 가장 적습니다.가능한 경우 오류 비활성화 포트의 영향을 받는 연결을 사용 가능한 다른 스위치 포트로 이동하여 서비스를 복원합니다.유지 보수 기간 동안 라인 카드의 수동 전원 주기를 예약합니다.손상된 패킷 버퍼 조건에서 완전히 복구하려면 reset module *mod* 명령을 실행합니다.

참고: 모듈을 재설정한 후 오류가 계속 발생하면 모듈을 다시 장착해 보십시오.

errdisable 옵션을 활성화하려면 다음 명령을 *실행합니다*.

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

기타 옵션

SRAM 오류가 발생한 모든 포트를 완전히 복구하려면 라인 카드의 전원 주기가 필요하므로 대체 복구 작업은 전원 주기 옵션을 구성하는 것입니다.이 옵션은 30초에서 40초 사이의 네트워크 서비스 중단을 허용할 수 있는 경우에 유용합니다.이 시간은 라인 모듈의 전원을 완전히 껐다가 다시 신속 부팅 기능 없이 작동시키는 데 필요한 시간입니다.Rapid Boot(빠른 부팅) 기능을 사용하면 전원 주기 옵션을 사용하여 네트워크 서비스 중단 시간을 10초로 줄일 수 있습니다.전원 주기 옵션을 활성화하려면 다음 명령을 실행합니다.

```
set errordetection packet-buffer power-cycle
```

패킷 버퍼 진단

이 테스트는 Catalyst 5500/5000 스위치에만 적용됩니다.이 테스트는 사용자 포트와 스위치 백플레인 간에 10/100Mbps 연결을 제공하는 특정 하드웨어를 사용하는 이더넷 모듈을 사용하는 Catalyst 5500/5000 스위치에서 장애가 발생한 하드웨어를 찾기 위해 설계되었습니다.트렁크 프레임에 대한 CRC 검사를 수행할 수 없으므로, 런타임 중에 포트 패킷 버퍼에 결함이 발생하면 패킷이 손상되어 CRC 오류가 발생할 수 있습니다.안타깝게도 이로 인해 불량 프레임이 Catalyst 5500/5000 ISL 네트워크에 더 많이 전파될 수 있으며, 이로 인해 최악의 경우 발생 시 컨트롤 플레인 중단 및 브로드캐스트 스톰이 발생할 수 있습니다.

최신 Catalyst 5500/5000 모듈 및 기타 플랫폼에서는 하드웨어 오류 검사 기능이 내장되어 있으며 패킷 버퍼 테스트가 필요하지 않으므로 구성할 수 있는 옵션이 없습니다.

패킷 버퍼 진단이 필요한 회선 모듈은 WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X514, WS-X55115입니다. 201, WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X55509, WS-U5351, WS-3555535 및 WS-U5535가 있습니다.

운영 개요

이 진단에서는 패킷 버퍼의 특정 섹션에 저장된 데이터가 하드웨어 오류로 인해 실수로 손상되지 않았는지 확인합니다.프로세스가 쓴 것과 다른 내용을 다시 읽는 경우 해당 포트가 데이터를 손상시킬 수 있으므로 모드에서 포트를 종료합니다.필요한 오류 임계값이 없습니다.모듈이 재설정되거나 교체될 때까지 실패한 포트를 다시 활성화할 수 없습니다.

패킷 버퍼 테스트에는 두 가지 모드가 있습니다.예약 및 온디맨드.테스트가 시작되면 테스트의 예상 길이(가장 가까운 분으로 반올림됨)와 테스트가 시작되었다는 사실을 나타내기 위해 syslog 메시지가 생성됩니다.테스트의 정확한 길이는 포트 유형, 버퍼 크기 및 테스트 실행 유형에 따라 달라집니다.

온디맨드 테스트는 몇 분 내에 완료하기 위해 적극적입니다.이러한 테스트는 패킷 메모리에 능동적으로 간섭하기 때문에 테스트하기 전에 포트를 관리 목적으로 종료해야 합니다.포트를 종료하려면 다음 명령을 실행합니다.

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
```

```
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

예약된 테스트는 온디맨드 테스트보다 훨씬 덜 공격적이며 백그라운드에서 실행됩니다.테스트는 여러 모듈에서 동시에 수행되지만 모듈당 하나의 포트에서 동시에 수행됩니다.이 테스트는 사용자 패킷 버퍼 데이터를 복원하기 전에 패킷 버퍼 메모리의 작은 섹션을 보존, 쓰기 및 읽므로 오류가 발생하지 않습니다.그러나 테스트는 버퍼 메모리에 쓰기 때문에 수신 패킷을 몇 밀리초 동안 차단하며 사용 중인 링크에서 일부 손실을 초래합니다.기본적으로 패킷 손실을 최소화하기 위해 각 버퍼 쓰기 테스트 사이에 8초의 일시 중지가 있지만 이는 패킷 버퍼 테스트가 필요한 모듈로 가득 찬 시스템이 테스트를 완료하는 데 24시간 이상이 걸릴 수 있음을 의미합니다.이 예약된 테스트는 매주 일요일 03:30에 CatOS 5.4 이상에서 실행되도록 기본적으로 활성화되며, 이 명령을 사용하여 테스트 상태를 확인할 수 있습니다.

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

권장 사항

모듈에서 문제를 발견함으로써 패킷 손실 위험을 해결할 수 있으므로 Catalyst 5500/5000 시스템에 대해 패킷 버퍼 테스트 예약 기능을 사용하는 것이 좋습니다.

그런 다음 표준화된 주간 시간을 네트워크 전체에서 스케줄링하여 고객이 필요에 따라 결함 포트 또는 RMA 모듈에서 링크를 변경할 수 있도록 해야 합니다.이 테스트로 인해 일부 패킷 손실이 발생할 수 있으므로, 네트워크 로드에 따라 일요일 오전 3:30의 기본값과 같이 더 조용한 네트워크 시간으로 예약해야 합니다.테스트 시간을 설정하려면 다음 명령을 실행합니다.

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

CatOS를 5.4 이상으로 처음 업그레이드할 때와 같이 활성화하면 이전에 숨겨진 메모리/하드웨어 문제가 노출되고 결과적으로 포트가 자동으로 종료될 가능성이 있습니다.다음 메시지가 표시됩니다.

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

기타 옵션

매주 포트당 낮은 수준의 패킷 손실을 감수하는 것이 허용되지 않는 경우, 예약된 중단 중에 온디맨드 기능을 사용하는 것이 좋습니다.이 기능을 범위별로 수동으로 시작하려면(먼저 포트를 관리적으로 비활성화해야 하지만) 다음 명령을 실행합니다.

```
test packetbuffer port range
```

시스템 로깅

Syslog 메시지는 Cisco 고유의 메시지이며 사전 예방적 장애 관리의 핵심 부분입니다.표준화된 SNMP를 통해 가능한 것보다 더 광범위한 네트워크 및 프로토콜 조건이 syslog를 사용하여 보고됩

니다.Cisco RME(Resource Manager Essentials) 및 NATkit(Network Analysis Toolkit)와 같은 관리 플랫폼은 다음 작업을 수행하기 때문에 syslog 정보를 효과적으로 사용합니다.

- 심각도, 메시지, 디바이스 등을 기준으로 분석 제공
- 분석을 위해 들어오는 메시지의 필터링 사용
- 호출기 등의 경고 또는 인벤토리 및 구성 변경 사항의 온디맨드 수집

권장 사항

중요한 중점 사항은 로깅 정보가 syslog 서버로 전송(set logging server severity *value* ***명령*** 사용)하는 것과는 달리, 로컬 로깅 정보를 스위치 버퍼에 보관해야 하는 수준입니다. 일부 조직에서는 중앙 집중식으로 높은 수준의 정보를 로깅하는 반면, 다른 조직에서는 스위치 자체로 이동하여 이벤트에 대한 자세한 로그를 확인하거나 문제 해결 중에만 더 높은 수준의 syslog 캡처를 활성화합니다.

디버깅은 CatOS 플랫폼과 Cisco IOS Software의 경우 다르지만, 기본적으로 로깅된 내용을 변경하지 않고 **set logging session enable을 사용하여 세션별로** 자세한 시스템 로깅을 활성화할 수 있습니다.

일반적으로 Cisco는 이러한 기능이 추적해야 할 주요 안정성 기능이므로 spantree 및 시스템 syslog 기능을 최대 6수준으로 가져오도록 권장합니다.또한 멀티캐스트 환경에서는 라우터 포트가 삭제될 경우 syslog 메시지가 생성되도록 멀티캐스트 기능의 로깅 레벨을 최대 4로 설정하는 것이 좋습니다.그러나 CatOS 5.5(5) 이전에는 IGMP 조인과 이면에 대해 syslog 메시지가 기록될 수 있으므로 모니터링하기에 너무 소음이 많습니다.마지막으로, IP 입력 목록을 사용하는 경우 무단 로그인 시도를 캡처하려면 최소 로깅 레벨 4를 사용하는 것이 좋습니다.다음 옵션을 설정하려면 다음 명령을 실행합니다.

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

메시지 볼륨이 높으면 느린 터미널 또는 기존 터미널이 아닌 터미널로부터 응답을 기다리는 동안 스위치가 매달려 있는 위험을 방지하려면 콘솔 메시지를 끕니다.콘솔 로깅은 CatOS에서 우선 순위가 높으며, 주로 트러블슈팅 또는 스위치 충돌 시나리오에서 로컬로 최종 메시지를 캡처하는 데 사용됩니다.

이 표에서는 Catalyst 6500/6000에 대한 개별 로깅 기능, 기본 레벨 및 권장 변경 사항을 제공합니다. 각 플랫폼에는 지원되는 기능에 따라 약간 다른 기능이 있습니다.

시설	기본 수준	권장 작업
acl	5	그냥 내버려둬
cdp	4	그냥 내버려둬
경찰	3	그냥 내버려둬
dtp	8	그냥 내버려둬
백작	2	그냥 내버려둬

etc[1]	5	그냥 내버려둬
파일	2	그냥 내버려둬
gvrp	2	그냥 내버려둬
IP	2	**IP 입력 목록이 사용되는 경우 4로 변경합니다**.
커널	2	그냥 내버려둬
1d	3	그냥 내버려둬
캐스트	2	**멀티캐스트가 사용되는 경우 4로 변경합니다(CatOS 5.5[5] 이상)**.
관리	5	그냥 내버려둬
mls	5	그냥 내버려둬
페이지	5	그냥 내버려둬
프로토콜	2	그냥 내버려둬
정리	2	그냥 내버려둬
프라이빗	3	그냥 내버려둬
qos	3	그냥 내버려둬
반경	2	그냥 내버려둬
rsvp	3	그냥 내버려둬
보안	2	그냥 내버려둬
snmp	2	그냥 내버려둬
스팬트리	2	**6으로 변경합니다**.
sys	5	**6으로 변경합니다**.
tac	2	그냥 내버려둬
tcp	2	그냥 내버려둬
텔넷	2	그냥 내버려둬
Tftp	2	그냥 내버려둬
UDLD	4	그냥 내버려둬
VMPS	2	그냥 내버려둬
VTP	2	그냥 내버려둬

[1] CatOS 7.x 이상에서는 LACP 지원을 반영하기 위해 etc 시설 코드가 pagp 기능 코드를 대체합니다.

참고: 현재 Catalyst 스위치는 컨피그레이션 모드를 종료한 후에만 메시지를 트리거하는 Cisco IOS Software와 달리 실행된 각 **세트** 또는 **clear** 명령에 대해 컨피그레이션 변경 syslog 레벨-6 메시지를 기록합니다.이 트리거 시 컨피그레이션을 실시간으로 백업하기 위해 RME가 필요한 경우 이러한 메시지도 RME syslog 서버로 전송해야 합니다.대부분의 고객은 Catalyst 스위치에 대한 주기적인 컨피그레이션 백업만으로도 충분하며, 기본 서버 로깅 심각도를 변경할 필요가 없습니다.

NMS 알림을 조정하는 경우 시스템 메시지 가이드를 참조하십시오.

Simple Network Management Protocol

SNMP는 네트워크 MIB(Device Management Information Base)에 저장된 통계, 카운터 및 테이블을 검색하는 데 사용됩니다. 수집된 정보는 NMS(예: HP Openview)에서 실시간 경고를 생성하고 가용

성을 측정하며 용량 계획 정보를 생성하며 구성 및 문제 해결 확인을 수행하는 데 도움이 되도록 사용할 수 있습니다.

운영 개요

일부 보안 메커니즘을 통해 네트워크 관리 스테이션은 SNMP 프로토콜 get 및 get 다음 요청을 사용하여 MIB의 정보를 검색하고 set 명령을 사용하여 매개변수를 변경할 수 **있습니다**.또한 실시간 알림을 위해 NMS에 대한 트랩 메시지를 생성하도록 네트워크 디바이스를 구성할 수 있습니다.SNMP 폴링은 IP UDP 포트 161을 사용하며 SNMP 트랩은 포트 162를 사용합니다.

Cisco는 다음 버전의 SNMP를 지원합니다.

- SNMPv1:RFC 1157 Internet Standard, 일반 텍스트 커뮤니티 문자열 보안 사용IP 주소 액세스 제어 목록 및 비밀번호는 에이전트 MIB에 액세스할 수 있는 관리자 커뮤니티를 정의합니다.
- SNMPv2C:SNMPv2의 조합, RFC 1902~1907에 정의된 초안 인터넷 표준, SNMPv2의 커뮤니티 기반 관리 프레임워크인 SNMPv2C, RFC 1901에 정의된 실험적 초안.테이블 및 많은 양의 정보를 검색하고 필요한 왕복 수를 최소화하며 오류 처리를 개선하는 대량 검색 메커니즘이 있습니다.
- SNMPv3:RFC 2570 제안 초안은 네트워크를 통한 패킷의 인증 및 암호화 조합을 통해 디바이스에 대한 보안 액세스를 제공합니다.SNMPv3에서 제공되는 보안 기능은 다음과 같습니다.메시지 무결성:패킷이 전송 중에 손상되지 않았는지 확인인증:메시지가 유효한 소스의 메시지인지 확인합니다.암호화:패킷의 내용을 스크램블하여 권한이 없는 소스에서 쉽게 볼 수 없게 합니다.

이 표에서는 보안 모델의 조합을 식별합니다.

모델 레벨	인증	암호화	결과
v1	noAuthNoPriv, 커뮤니티 문자열	아니요	인증에 커뮤니티 문자열 일치를 사용합니다.
v2c	noAuthNoPriv, 커뮤니티 문자열	아니요	인증에 커뮤니티 문자열 일치를 사용합니다.
v3	noAuthNoPriv, 사용자 이름	아니요	인증에 사용자 이름 일치를 사용합니다.
v3	authNoPriv, MD5 또는 SHA	NP	HMAC-MD5 또는 HMAC-SHA 알고리즘을 기반으로 인증을 제공합니다.
v3	authPriv, MD5 또는	DES	HMAC-MD5 또는 HMAC-SHA 알고리즘을 기반으로 인증을 제공합니다.CBC-DES(DES-56) 표준을 기반으로 하는 인

	SHA		증 외에 DES 56비트 암호화를 제공합니다.

참고: SNMPv3 개체에 대해 다음 정보를 기억하십시오.

- 각 사용자는 그룹에 속합니다.
- 그룹은 사용자 집합에 대한 액세스 정책을 정의합니다.
- 액세스 정책은 읽기, 쓰기 및 생성을 위해 액세스할 수 있는 SNMP 객체를 정의합니다.
- 그룹은 사용자가 받을 수 있는 알림 목록을 결정합니다.
- 그룹은 사용자의 보안 모델과 보안 수준도 정의합니다.

SNMP 트랩 권장 사항

SNMP는 모든 네트워크 관리의 기반이며 모든 네트워크에서 사용 및 사용 가능합니다.스위치의 SNMP 에이전트는 관리 스테이션에서 지원하는 SNMP 버전을 사용하도록 설정해야 합니다.에이전트는 여러 관리자와 통신할 수 있으므로 SNMPv1 프로토콜을 사용하는 한 관리 스테이션 및 SNMPv2 프로토콜을 사용하는 다른 관리 스테이션과의 통신을 지원하도록 소프트웨어를 구성할 수 있습니다.

대부분의 NMS 스테이션은 현재 이 구성에서 SNMPv2C를 사용합니다.

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

사용 중인 모든 기능에 대해 SNMP 트랩을 활성화할 것을 권장합니다(필요한 경우 사용하지 않는 기능을 비활성화할 수 있음). 트랩이 활성화되면 NMS에 **test snmp 명령** 및 오류(예: 호출기 알림 또는 팝업)에 대해 설정된 적절한 처리를 사용하여 트랩을 테스트할 수 있습니다.

모든 트랩은 기본적으로 비활성화되며, 다음과 같이 개별적으로 또는 **모든** 매개변수를 사용하여 컨피그레이션에 추가해야 합니다.

```
set snmp trap enable all
set snmp trap server address read-only community string
```

CatOS 5.5에서 사용 가능한 트랩은 다음과 같습니다.

트랩	설명
인증	인증
다리	브리지
섀시	섀시
구성	구성
엔티티	엔티티
ippermit	IP 허용
모듈	모듈
반복	리피터

stpx	스패닝 트리 확장
syslog	Syslog 알림
vmps	VLAN 구성원 정책 서버
vtp	VLAN 트렁크 프로토콜

참고: syslog 트랩은 스위치에서 생성된 모든 syslog 메시지를 NMS에 SNMP 트랩으로 전송합니다 .Cisco Works 2000 RME와 같은 분석기에서 syslog 알림을 이미 수행하고 있는 경우 이 정보를 두 번 수신하는 것이 반드시 유용하지 않을 수도 있습니다.

Cisco IOS Software와 달리, 스위치에는 수백 개의 활성 인터페이스가 있을 수 있으므로 포트 레벨 SNMP 트랩은 기본적으로 비활성화되어 있습니다.따라서 라우터, 스위치 및 주 서버에 대한 인프라 링크와 같은 주요 포트에는 포트 레벨 SNMP 트랩이 활성화되어 있는 것이 좋습니다.사용자 호스트 포트와 같은 다른 포트는 필요하지 않으므로 네트워크 관리를 간소화할 수 있습니다.

```
set port trap port range enable
!--- Enable on key ports only.
```

SNMP 폴링 권장 사항

구체적인 요구 사항에 대해 자세히 알아보려면 네트워크 관리 검토를 권장합니다.그러나 대규모 네트워크 관리를 위한 몇 가지 기본적인 Cisco 철학은 다음과 같습니다.

- 간단한 일을 하고 잘 하세요.
- 과도한 데이터 폴링, 수집, 툴, 수동 분석 등으로 인한 직원 과부하 감소
- NMS로 HP Openview, Cisco RMEs as a configuration, syslog, inventory, software manager, Microsoft Excel as a NMS data analyzer, CGI와 같은 몇 가지 툴을 사용하여 네트워크를 관리할 수 있습니다.
- 고위 관리 및 분석가와 같은 사용자는 웹에 보고서를 게시하면 특별한 요청이 많은 운영 직원에게 부담을 주지 않고 정보를 제공할 수 있습니다.
- 네트워크에서 무엇이 잘 작동하는지 확인하고 그대로 둡니다.작동하지 않는 것에 집중하십시오.

NMS 구현의 첫 번째 단계는 네트워크 하드웨어의 베이스라인이어야 합니다.라우터의 간단한 CPU, 메모리 및 버퍼 활용도와 스위치의 NMP CPU, 메모리 및 백플레인 활용률에서 디바이스 및 프로토콜 상태에 대해 많은 것을 유추할 수 있습니다.하드웨어 베이스라인이 L2 및 L3 트래픽 로드, 피크 및 평균 베이스라인이 완전히 의미가 있게 된 후에만 해당됩니다.기준선은 일반적으로 회사의 비즈니스 주기에 따라 일일, 주별, 분기별 추세를 파악하기 위해 몇 개월에 걸쳐 수립됩니다.

많은 네트워크에서 오버폴링으로 인해 NMS 성능 및 용량 문제가 발생합니다.따라서 베이스라인이 설정되면 디바이스에서 경보 및 이벤트 RMON 임계값을 설정하여 비정상적인 변경 사항에 대해 NMS에 알림을 보내고 폴링을 제거하는 것이 좋습니다.이를 통해 네트워크는 지속적으로 폴링하는 대신 정상적인 것이 아닐 때 운영자에게 모든 것이 정상인지 확인할 수 있습니다.임계값은 최대값과 백분율 또는 평균에서 표준 편차 등 다양한 규칙에 따라 설정할 수 있으며 이 문서의 범위를 벗어납니다.

NMS 구현의 두 번째 단계는 SNMP를 사용하여 네트워크의 특정 영역을 더 자세히 폴링하는 것입니다.여기에는 의심스러운 영역, 변경 전 영역 또는 정상적으로 작동하는 것으로 특징지어지는 영역이 포함됩니다.NMS 시스템을 검색 표시등으로 사용하여 네트워크를 자세히 스캔하고 핫 스팟을 조명합니다(전체 네트워크를 켜지 마십시오).

Cisco Network Management Consulting 그룹은 캠퍼스 네트워크에서 이러한 주요 결함 MIB를 분석

또는 모니터링하도록 제안합니다.폴링할 성능 MIB에 대한 자세한 내용은 Cisco Network Monitoring and Event Correlation Guidelines를 참조하십시오(예:).

개체 이름	개체 설명	OID	폴링 간격	임계값
MIB-II				
sysUp시간	시스템 가동 시간(1/100초)	1.3.6.1.2.1.1.3	5분	< 30000

개체 이름	개체 설명	OID	폴링 간격	임계값
CISCO-PROCESS-MIB				
cpmCPUTotal5min	최근 5분 동안의 전체 CPU 사용 중 비율	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10분	초기 계획

개체 이름	개체 설명	OID	폴링 간격	임계값
CISCO-STACK-MIB				
sysEnable섀시Traps	이 MIB의 chassisAlarmOn 및 chassisAlarmOff 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.24	24시간	1
sysEnableModule트랩	이 MIB의 moduleUp 및 moduleDown 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.25	24시간	1
sysEnableBridge트랩	BRIDGE-MIB(RFC 1493)의 newRoot 및 topologyChange 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.26	24시간	1
sys활성화리피터 트랩	REPEATER-MIB(RFC1516)의 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.29	24시간	1

sysEnableIpPermitTraps	이 MIB의 IP 허용 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.31	24시간	1
sysEnableVmpsTraps	CISCO-VLAN-MEMBERSHIP-MIB에 정의된 vmVmpsChange 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.33	24시간	1
sysEnableConfig트랩	이 MIB의 sysConfigChange 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.35	24시간	1
sysEnableStpxTrap	CISCO-STP-EXTENSIONS-MIB의 stpxUn불일치Update 트랩을 생성해야 하는지 여부를 나타냅니다.	1.3.6.1.4.1.9.5.1.1.40	24시간	1
섀시Ps1상태	전원 공급 장치 1의 상태.	1.3.6.1.4.1.9.5.1.2.4	10분	2
섀시Ps1테스트 결과	전원 공급 장치 1의 상태에 대한 자세한 정보.	1.3.6.1.4.1.9.5.1.2.5	필요에 따라	
섀시Ps2상태	전원 공급 장치 2 상태.	1.3.6.1.4.1.9.5.1.2.7	10분	2
섀시Ps2테스트 결과	전원 공급 장치 상태에 대한 자세한 정보 2	1.3.6.1.4.1.9.5.1.2.8	필요에 따라	
섀시 FanStatus	섀시 팬의 상태입니다.	1.3.6.1.4.1.9.5.1.2.9	10분	2
섀시 FanTestResult	섀시 팬 상태에 대한 자세한 정보.	1.3.6.1.4.1.9.5.1.2.10	필요에 따라	
섀시 MinorAlarm	섀시 Minor Alarm 상태.	1.3.6.1.4.1.9.5.1.2.11	10분	1
섀시 MajorAlarm	섀시 주요 경보 상태	1.3.6.1.4.1.9.5.1.2.12	10분	1
섀시 TempAlarm	섀시 온도 경보 상태.	1.3.6.1.4.1.9.5.1.2.13	10분	1
모듈 상태	모듈의 작동 상태입	1.3.6.1.4.1.9.	30	2

	니다.	5.1.3.1.1.10	분	
모듈 테스트 결과	모듈 조건에 대한 자세한 정보.	1.3.6.1.4.1.9.5.7.3.1.1.11	필요에 따라	
모듈 StandbyStatus	이중화 모듈의 상태입니다.	1.3.6.1.4.1.9.5.7.3.1.1.21	30분	= 1 또는 4

개체 이름	개체 설명	OID	폴링 간격	임계값
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	엔티티에서 토폴로지 변경을 마지막으로 탐지한 이후 경과한 시간(1/100초).	1.3.6.1.2.1.17.2.3	5분	< 30000
dot1dStpTop변경 사항	관리 엔터티가 마지막으로 다시 설정되거나 초기화된 이후 이 브리지에서 탐지된 총 토폴로지 변경 수입니다.	1.3.6.1.2.1.17.2.4	필요에 따라	
dot1dStpPortState [1]	스패닝 트리 프로토콜의 애플리케이션에 의해 정의된 포트의 현재 상태.반환 값은 다음 중 하나일 수 있습니다 `.disabled(1), blocking(2), listening(3), learning(4), forwarding(5)` 또는 `broken(6).`	1.3.6.1.2.1.17.2.15.1.3	필요에 따라	

개체 이름	개체 설명	OID	폴링 간격	임계값
CISCO-MEMORY-POOL-MIB				
ciscoMemoryPool사용됨	관리되는 디바이스의 애플리케이션에	1.3.6.1.4.1.9.9.48.1.1.1.5	30	초기

	서 현재 사용 중인 메모리 풀의 바이트 수를 나타냅니다.		분	계획
cisco메모리 풀사용 가능	관리되는 디바이스에서 현재 사용되지 않는 메모리 풀의 바이트 수를 나타냅니다. **참고:** ciscoMemoryPoolUsed 및 ciscoMemoryPoolFree의 합계는 풀의 총 메모리 양입니다.	1.3.6.1.4.1.9.9.48.1.1.1.6	30분	초기 계획
cisco메모리 풀사용 가능	관리되는 디바이스에서 현재 사용되지 않는 메모리 풀에서 가장 많은 연속 바이트 수를 나타냅니다.	1.3.6.1.4.1.9.9.48.1.1.1.7	30분	초기 계획

Cisco MIB 지원에 대한 자세한 내용은 Cisco Network Management Toolkit - MIB를 참조하십시오.

참고: 일부 표준 MIB에서는 특정 SNMP 엔티티에 MIB의 인스턴스가 하나만 있다고 가정합니다.따라서 표준 MIB에는 사용자가 MIB의 특정 인스턴스에 직접 액세스할 수 있는 인덱스가 없습니다.이러한 경우 표준 MIB의 각 인스턴스에 액세스하기 위해 커뮤니티 문자열 인덱싱이 제공됩니다.구문은 [community string]@[instance number]입니다. 여기서 instance는 일반적으로 VLAN 번호입니다.

기타 옵션

SNMPv3의 보안 측면은 SNMPv2를 적시에 추월할 것으로 예상됨을 의미합니다.Cisco는 고객이 NMS 전략의 일환으로 이 새로운 프로토콜을 준비할 것을 권장합니다.그 이점은 변조 또는 손상을 두려워하지 않고 SNMP 디바이스에서 데이터를 안전하게 수집할 수 있다는 것입니다.스위치 컨피그레이션을 변경하는 SNMP **set** 명령 패킷과 같은 기밀 정보를 암호화하여 해당 콘텐츠가 네트워크에 노출되지 않도록 할 수 있습니다.또한 서로 다른 사용자 그룹마다 다른 권한을 가질 수 있습니다.

참고: SNMPv3의 컨피그레이션은 SNMPv2 명령줄과 크게 다르며 Supervisor Engine의 CPU 로드가 증가할 것으로 예상됩니다.

원격 모니터링

RMON은 기록 기준 결정 및 임계값 분석 수행과 같은 네트워크 관리자가 해당 정보의 일반적인 사용 또는 적용을 준비하기 위해 네트워크 디바이스 자체에서 MIB 데이터를 사전 처리할 수 있도록 허용합니다.

RMON 처리 결과는 RFC 1757에 정의된 대로 NMS의 후속 수집을 위해 RMON MIB에 저장됩니다 .

운영 개요

Catalyst 스위치는 4개의 기본 RMON-1 그룹으로 구성된 각 포트의 하드웨어에서 mini-RMON을 지원합니다.통계(그룹 1), 기록(그룹 2), 경보(그룹 3) 및 이벤트(그룹 9)

RMON-1의 가장 강력한 부분은 **경보 및 이벤트** 그룹에서 제공하는 **임계값 메커니즘**입니다.앞서 설명한 대로 RMON 임계값 컨피그레이션을 통해 이상 조건이 발생할 경우 스위치에서 SNMP 트랩을 전송할 수 있습니다.키 포트가 식별되면 SNMP를 사용하여 카운터 또는 RMON 기록 그룹을 폴링하고 해당 포트에 대한 정상 트래픽 활동을 기록하는 베이스라인을 생성할 수 있습니다.다음으로, 기준선에서 정의된 차이가 있을 때 RMON 상승 및 하락 임계값을 설정하고 경보를 구성할 수 있습니다.

임계값 구성은 경보 및 이벤트 테이블에서 매개변수 행을 성공적으로 생성하는 것이 번거롭기 때문에 RMON 관리 패키지를 사용하여 수행하는 것이 좋습니다.Cisco Works 2000의 일부인 Cisco Traffic Director와 같은 상용 RMON NMS 패키지는 RMON 임계값 설정을 훨씬 간소화하는 GUI를 통합합니다.

EtherStats 그룹은 기준상의 목적으로 L2 트래픽 통계의 유용한 범위를 제공합니다.이 테이블의 객체를 사용하여 유니캐스트, 멀티캐스트, 브로드캐스트 트래픽과 다양한 L2 오류에 대한 통계를 얻을 수 있습니다.스위치의 RMON 에이전트는 이러한 샘플링된 값을 기록 그룹에 저장하도록 구성할 수도 있습니다.이 메커니즘을 사용하면 샘플 속도를 줄이지 않고 폴링 양을 줄일 수 있습니다.RMON 기록은 상당한 폴링 오버헤드 없이 정확한 베이스라인을 제공할 수 있습니다.그러나 기록을 수집할수록 스위치 리소스가 더 많이 사용됩니다.

스위치는 RMON-1의 기본 그룹을 4개만 제공하지만 나머지 RMON-1 및 RMON-2를 잊지 않는 것이 중요합니다. 모든 그룹은 UsrHistory(그룹 18) 및 ProbeConfig(그룹 19)를 포함하여 RFC 2021에 정의됩니다.외부 RMON SwitchProbe 또는 내부 NAM(Network Analysis Module)에 트래픽을 복사할 수 있는 SPAN 포트 또는 VLAN ACL 리디렉션 기능을 사용하는 스위치에서 L3 이상의 정보를 검색할 수 있습니다.

NAM은 모든 RMON 그룹을 지원하며 MLS가 활성화될 때 Catalyst에서 내보낸 Netflow 데이터를 포함하여 **애플리케이션 레이어 데이터**를 검토할 수 있습니다.MLS를 실행하면 라우터가 흐름의 모든 패킷을 전환하지 않으므로 Netflow 데이터 내보내기 및 인터페이스 카운터가 아닌 Netflow 데이터 내보내기만 신뢰할 수 있는 VLAN 어카운팅을 제공합니다.

SPAN 포트와 스위치 프로브를 사용하여 특정 포트, 트렁크 또는 VLAN에 대한 패킷 스트림을 캡처하고 RMON 관리 패키지로 디코딩할 패킷을 업로드할 수 있습니다.SPAN 포트는 CISCO-STACK-MIB의 SPAN 그룹을 통해 SNMP 제어 가능하므로 이 프로세스를 쉽게 자동화할 수 있습니다.Traffic Director는 이동 에이전트 기능을 사용하여 이러한 기능을 사용합니다.

전체 VLAN을 스패닝할 때 유의해야 할 사항이 있습니다.1Gbps 프로브를 사용하는 경우에도 하나의 VLAN 또는 1Gbps 전이중 포트에서 전체 패킷 스트림이 SPAN 포트의 대역폭을 초과할 수 있습니다.SPAN 포트가 계속 전체 대역폭에서 실행되는 경우 데이터가 손실될 가능성이 있습니다.자세한 내용은 Catalyst SPAN(Switched Port Analyzer) 기능 구성을 참조하십시오.

권장 사항

Cisco에서는 SNMP 폴링만 사용하는 것보다 더 지능적인 방법으로 네트워크 관리를 지원하기 위해 RMON 임계값 및 알림을 구축하는 것이 좋습니다.이렇게 하면 네트워크 관리 트래픽 오버헤드가 줄어들고 베이스라인에서 변경된 사항이 있을 때 네트워크에서 지능적으로 알림을 보낼 수 있습니다.RMON은 Traffic Director와 같은 외부 에이전트에 의해 제어되어야 합니다.CLI는 지원되지 않습니다.RMON을 활성화하려면 다음 명령을 실행합니다.

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

스위치의 주요 기능은 대형 다중 포트 RMON 프로브 역할을 하지 않고 프레임을 전달하는 것입니다.따라서 여러 조건에 대해 여러 포트에 대한 기록 및 임계값을 설정할 때 리소스가 소비되고 있다는 점에 유의하십시오.RMON을 확장하는 경우 NAM 모듈을 고려하십시오.또한 중요한 포트 규칙을 기억하십시오.계획 단계에서 중요한 것으로 식별된 포트에 대한 폴링 및 임계값만 설정합니다.

메모리 요구 사항

RMON 메모리 사용량은 통계, 기록, 경보 및 이벤트와 관련된 모든 스위치 플랫폼에서 일정합니다.RMON은 버킷을 사용하여 RMON 에이전트(이 경우 스위치)에 내역과 통계를 저장합니다. 버킷 크기는 RMON 프로브(Switch Probe) 또는 RMON 애플리케이션(Traffic Director)에 정의된 다음 스위치로 전송하여 설정합니다.일반적으로 메모리 제한은 32MB 미만의 DRAM을 사용하는 이전 Supervisor Engines에서만 고려됩니다.다음 지침을 참조하십시오.

- 미니-RMON(RMON의 4개 그룹)을 지원하기 위해 NMP 이미지에 약 45만 개의 코드 공간이 추가됩니다.통계, 기록, 경보 및 이벤트) RMON에 대한 동적 메모리 요구 사항은 런타임 컨피그레이션에 따라 달라지므로각 mini-RMON 그룹에 대한 런타임 RMON 메모리 사용량 정보는 여기에서 설명합니다.Ethernet Statistics group(이더넷 통계 그룹) - 각 스위치드 이더넷/FE 인터페이스에 800바이트를 사용합니다.History group(기록 그룹) - 이더넷 인터페이스의 경우, 50개의 버킷으로 구성된 각 기록 제어 항목은 약 3.6KB 메모리 공간과 각 추가 버킷에 56바이트를 사용합니다.Alarms and Events groups(경보 및 이벤트 그룹) - 구성된 각 경보 및 해당 이벤트 항목에 대해 2.6KB를 사용합니다.
- RMON 관련 컨피그레이션을 저장하려면 전체 NVRAM 크기가 256K 이상이고 총 NVRAM 크기가 128K인 경우 10K의 NVRAM이 공간의 20K NVRAM을 사용합니다.

Network Time Protocol(네트워크 타이밍 프로토콜)

NTP, RFC 1305 는 분산된 시간 서버 및 클라이언트 집합 간에 시간 유지를 동기화하며, 시스템 로그가 생성되거나 기타 시간 관련 이벤트가 발생할 때 이벤트를 상관관계를 설정할 수 있도록 합니다.

NTP는 일반적으로 LAN에서 밀리초 이내, WAN에서는 최대 몇 십 밀리초 이내에 클라이언트 시간을 UTC(Coordinated Universal Time)에 동기화된 기본 서버와 비교하여 정확하게 제공합니다. 일반적인 NTP 구성은 높은 정확성과 신뢰성을 얻기 위해 여러 개의 이중화 서버와 다양한 네트워크 경로를 사용합니다.일부 컨피그레이션에는 우발적이거나 악의적인 프로토콜 공격을 방지하기 위한 암호화 인증이 포함됩니다.

운영 개요

NTP는 RFC 958 에서 처음 문서화되었지만 RFC 1119(NTP 버전 2)를 통해 진화했으며 현재 RFC 1305에 정의된 세 번째 버전에 있습니다 .UDP 포트 123을 통해 실행됩니다. 모든 NTP 통신에서는 UTC를 사용합니다. UTC는 그리니치 표준시(Greenwich Mean Time)와 동일합니다.

공용 시간 서버 액세스

NTP 서브넷에는 현재 라디오, 위성 또는 모뎀에 의해 UTC에 직접 동기화된 50개 이상의 공용 주 서버가 포함됩니다.일반적으로 클라이언트 워크스테이션 및 비교적 적은 수의 클라이언트가 있는 서버는 주 서버와 동기화되지 않습니다.100,000개 이상의 클라이언트 및 서버에 대한 동기화를 제

공하는 1 주 서버에 약 100개의 공용 보조 서버가 동기화되어 있습니다.현재 목록은 정기적으로 업데이트되는 List of Public NTP Servers(공용 NTP 서버 목록) 페이지에서 유지 관리됩니다.일반에서도 일반적으로 사용할 수 없는 수많은 사설 기본 및 보조 서버가 있습니다.공용 NTP 서버의 목록 및 사용 방법에 대한 자세한 내용은 University of Delaware Time Synchronization Server 웹 사이트를 참조하십시오.

이러한 공용 인터넷 NTP 서버를 사용할 수 있는지 또는 시간이 정확한지 보장할 수 없으므로 다른 옵션을 고려하는 것이 좋습니다.여기에는 여러 라우터에 직접 연결된 다양한 독립형 GPS(Global Positioning Service) 디바이스를 사용할 수 있습니다.

또 다른 가능한 옵션은 Stratum 1 마스터로 구성된 다양한 라우터를 사용하는 것이지만 권장되지는 않습니다.

지층

각 NTP 서버는 서버가 있는 외부 시점과 얼마나 멀리 떨어져 있는지를 나타내는 계층을 채택합니다.계층 1 서버는 라디오 클럭과 같은 특정 종류의 외부 시간 소스에 액세스할 수 있습니다.Stratum 2 서버는 지정된 Stratum 1 서버 집합에서 시간 세부 정보를 얻으며, Stratum 3 서버는 Stratum 2 서버로부터 시간 세부 정보를 얻습니다.

서버 피어 관계

- 서버는 클라이언트 요청에 응답하지만 클라이언트 시간 소스의 날짜 정보를 통합하려고 시도하지 않습니다.
- 피어는 클라이언트 요청에 응답하지만 클라이언트 요청을 더 나은 시간 소스를 위한 잠재적 후보로 사용하고 클럭 빈도를 안정화하는 데 도움이 되도록 시도합니다.
- 진정한 피어가 되려면 연결의 양쪽이 한 사용자에게 피어, 다른 사용자는 서버를 갖는 대신 피어 관계에 들어가야 합니다.또한 신뢰할 수 있는 호스트만 피어로 서로 통신하도록 피어가 키를 교환하는 것이 좋습니다.
- 서버에 대한 클라이언트 요청에서 서버는 클라이언트에 응답하고 클라이언트가 질문을 한 적이 있음을 잊어버립니다.피어에 대한 클라이언트 요청에서 서버는 클라이언트에 응답하고 클라이언트에 대한 상태 정보를 보관하여 시간 유지 시 얼마나 잘 수행되고 있으며 어떤 계층 서버가 실행 중인지 추적합니다.**참고:** CatOS는 NTP 클라이언트로만 작동할 수 있습니다.

NTP 서버에서 수천 개의 클라이언트를 처리하는 것은 문제가 없습니다.그러나 수백 개의 피어를 처리하는 것은 메모리에 영향을 미치며, 상태 유지 관리에서 박스(box)의 CPU 리소스와 대역폭을 더 많이 소비합니다.

폴링

NTP 프로토콜을 사용하면 클라이언트가 원하는 시간에 언제든지 서버를 쿼리할 수 있습니다.실제로 NTP가 Cisco 디바이스에서 처음 구성된 경우 NTP_MINPOLL(24 = 16초) 간격으로 8개의 쿼리를 빠르게 전송합니다.NTP_MAXPOLL은 214초(16,384초 또는 4시간, 33분, 4초)이며, 이는 NTP가 응답을 위해 다시 폴링하는 데 걸리는 최대 시간입니다.현재 Cisco는 사용자가 POLL 시간을 수동으로 설정할 방법이 없습니다.

NTP 폴링 카운터는 2^6(64)초에서 시작하며 두 서버가 서로 동기화될 때 두 개의 제곱으로 2^{10}으로 증가합니다. 즉, 구성된 서버 또는 피어당 64, 128, 256, 512 또는 1024초의 간격으로 동기화 메시지가 전송될 것으로 예상할 수 있습니다.시간은 패킷을 보내고 받는 phase-locked-loop에 따라 2의 전원으로 64초에서 1024초 사이에 달라집니다.시간에 지터가 많으면 더 자주 폴링됩니다.참조 시계가 정확하며 네트워크 연결이 일관되면 폴링 시간이 각 폴링 사이에 1024초로 수렴되는 것을 볼

수 있습니다.

실제 환경에서는 클라이언트와 서버 간의 연결이 변경될 때 NTP 폴링 간격이 변경됩니다.연결이 좋아질수록 폴링 간격이 길어집니다. 즉 NTP 클라이언트가 마지막 8개 요청에 대해 8개의 응답을 수신했습니다(폴링 간격이 2배로 표시됨).단일 응답이 누락되면 폴링 간격이 절반으로 줄어듭니다 .폴링 간격은 64초부터 시작하여 최대 1024초로 이동합니다.최상의 경우 폴링 간격이 64초에서 1024초로 이동하는 데 2시간 이상이 걸립니다.

브로드캐스트

NTP 브로드캐스트는 전달되지 않습니다.ntp **broadcast** 명령을 사용하면 라우터가 구성된 인터페이스에서 NTP 브로드캐스트를 시작합니다.ntp broadcastclient 명령을 사용하면 라우터 또는 스위치가 구성된 인터페이스에서 NTP 브로드캐스트를 수신하게 됩니다.

NTP 트래픽 레벨

NTP에서 사용하는 대역폭은 최소 수준입니다. 피어 간에 교환되는 폴링 메시지 간의 간격은 일반적으로 17분(1024초)마다 메시지를 1개 이하로 되돌리기 때문입니다. 신중하게 계획하면 WAN 링크를 통해 라우터 네트워크 내에서 이를 유지 관리할 수 있습니다.NTP 클라이언트는 WAN을 통해 계층 2 서버가 될 중앙 사이트 코어 라우터로 전환하는 것이 아니라 로컬 NTP 서버로 피어링해야 합니다.

통합 NTP 클라이언트는 서버당 약 0.6비트/초를 사용합니다.

권장 사항

오늘날 많은 고객이 CatOS 플랫폼에서 클라이언트 모드로 NTP를 구성했으며, 인터넷 또는 라디오 클럭에서 여러 개의 신뢰할 수 있는 피드에서 동기화되었습니다.그러나 스위치 수가 많은 경우 서버 모드의 보다 간단한 방법은 스위치드 도메인의 관리 VLAN에서 브로드캐스트 클라이언트 모드에서 NTP를 활성화하는 것입니다.이 메커니즘을 사용하면 전체 Catalyst 도메인이 단일 브로드캐스트 메시지에서 시계를 수신할 수 있습니다.그러나 정보 흐름이 단방향으로 이루어지므로 시간 관리의 정확성은 다소 낮아집니다.

루프백 주소를 업데이트의 소스로 사용하는 것도 일관성에 도움이 될 수 있습니다.다음과 같은 두 가지 방법으로 보안 문제를 해결할 수 있습니다.

- 서버 업데이트 필터링
- 인증

이벤트의 시간 상관관계는 두 가지 경우 매우 중요합니다.문제 해결 및 보안 감사.시간 소스 및 데이터를 보호하기 위해 주의를 기울여야 하며, 키 이벤트가 의도적으로 또는 의도하지 않게 지워지지 않도록 암호화를 권장합니다.

Cisco에서는 다음 구성을 권장합니다.

Catalyst 구성
set ntp broadcastclient enable **set ntp authentication enable** **set ntp key** *key* *!--- This is a Message Digest 5 (MD5) hash.* **set ntp**

timezone

대체 Catalyst 구성
!--- This more traditional configuration creates !--- more configuration work and NTP peerings. **set ntp client enable** **set ntp server** *IP address of time server* **set timezone** *zone name* **set summertime** *date change details*

라우터 컨피그레이션
!--- This is a sample router configuration to distribute !--- NTP broadcast information to the Catalyst broadcast clients. **ntp source loopback0** **ntp server** *IP address of time server* **ntp update-calendar** **clock timezone** *zone name* **clock summer-time** *date change details* **ntp authentication key** *key* **ntp access-group** *access-list* *!--- To filter updates to allow only trusted sources of NTP information.* **Interface** *to campus/management VLAN containing switch sc0* **ntp broadcast**

Cisco 검색 프로토콜

CDP는 데이터 링크 레이어를 통해 인접 디바이스 간에 정보를 교환하며, 논리적 또는 IP 레이어 외부의 네트워크 토폴로지 및 물리적 컨피그레이션을 결정하는 데 매우 유용합니다.지원되는 디바이스는 주로 스위치, 라우터 및 IP 전화입니다.이 섹션에서는 버전 1에 대한 CDP 버전 2의 몇 가지 개선 사항을 설명합니다.

운영 개요

CDP는 유형 코드 2000으로 SNAP 캡슐화를 사용합니다.이더넷, ATM 및 FDDI에서 대상 멀티캐스트 주소 **01-00-0c-cc-cc-cc, HDLC 프로토콜 유형 0x2000이** 사용됩니다.토큰 링에서 기능 주소 c000.0800.0000이 사용됩니다.CDP 프레임은 기본적으로 매분마다 정기적으로 전송됩니다.

CDP 메시지에는 대상 디바이스가 모든 인접 디바이스에 대한 정보를 수집하고 저장할 수 있는 하나 이상의 하위 메시지가 포함되어 있습니다.

CDP 버전 1은 다음 매개변수를 지원합니다.

매개변수	유형	설명
1	장치 ID	ASCII의 디바이스 또는 하드웨어 일련 번호의 호스트 이름.
2	주	업데이트를 보낸 인터페이스의 L3 주소입니다.

	소	
3	포트 ID	CDP 업데이트가 전송된 포트입니다.
4	기능	디바이스의 기능 기능에 대해 설명합니다.라우터 :0x01TB 브리지:0x02 SR 브리지:0x04 스위치 :0x08(L2 및/또는 L3 스위칭 제공) 호스트:0x10 IGMP 조건부 필터링:0x20 브리지 또는 스위치는 비라우팅 포트에서 IGMP 보고서 패킷을 전달하지 않습니다.리피터:0x40
5	버전	소프트웨어 버전을 포함하는 문자열(**show version**과 동일).
6	플랫폼	하드웨어 플랫폼(예: WS-C5000, WS-C6009 또는 Cisco RSP).

CDP 버전 2에서는 추가 프로토콜 필드가 도입되었습니다.CDP 버전 2는 모든 필드를 지원하지만 나열된 항목은 스위치드 환경에서 특히 유용할 수 있으며 CatOS에서 사용됩니다.

참고: 스위치가 CDPv1을 실행하면 v2 프레임이 삭제됩니다.CDPv2를 실행하는 스위치가 인터페이스에서 CDPv1 프레임을 수신하면 CDPv2 프레임 외에도 해당 인터페이스에서 CDPv1 프레임을 전송하기 시작합니다.

매개변수	유형	설명
9	VTP 도메인	디바이스에 구성된 경우 VTP 도메인.
10	네이티브 VLAN	dot1q에서 이는 태그가 지정되지 않은 VLAN입니다.
11	전이중/반이중	이 필드에는 전송 포트의 듀플렉스 설정이 포함됩니다.

권장 사항

CDP는 기본적으로 활성화되어 있으며 인접 디바이스를 모니터링하고 문제 해결을 위해 필수적입니다.또한 네트워크 관리 애플리케이션에서 L2 토폴로지 맵을 구축하는 데 사용됩니다.CDP를 설정하려면 다음 명령을 실행합니다.

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

인터넷 연결 DMZ와 같이 높은 수준의 보안이 필요한 네트워크의 일부에서 다음과 같이 CDP를 해제해야 합니다.

```
set cdp disable port range
```

show cdp neighbors 명령은 로컬 CDP 테이블을 표시합니다.별표(*)로 표시된 항목은 VLAN 불일치

를 나타냅니다.#으로 표시된 항목은 이중 불일치를 나타냅니다.이는 문제 해결에 도움이 될 수 있습니다.

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ----------------- ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

기타 옵션

Catalyst 6500/6000과 같은 일부 스위치는 UTP 케이블을 통해 IP 전화에 전원을 공급할 수 있습니다.CDP를 통해 수신되는 정보는 스위치의 전력 관리를 지원합니다.

IP 전화기는 PC를 연결할 수 있고 두 장치가 모두 Catalyst의 동일한 포트에 연결되므로, 이 스위치는 VoIP 전화기를 별도의 VLAN인 보조형 VLAN에 넣을 수 있습니다.이를 통해 스위치는 VoIP 트래픽에 다른 QoS(Quality of Service)를 쉽게 적용할 수 있습니다.

또한 보조 VLAN이 수정될 경우(예: 특정 VLAN 또는 특정 태깅 방법을 강제로 사용하기 위해) 이 정보는 CDP를 통해 전화기로 전송됩니다.

매개변수	유형	설명
14	어플라이언스 ID	별도의 VLAN-id(보조 VLAN)로 VoIP 트래픽을 다른 트래픽과 차별화할 수 있습니다.
16	전력 소비량	VoIP 전화에서 소비하는 전력(밀리와트)

참고: Catalyst 2900 및 3500XL 스위치는 현재 CDPv2를 지원하지 않습니다.

보안 구성

이상적으로, 고객은 Cisco의 어떤 툴과 기술이 검증되었는지 정의할 수 있도록 보안 정책을 이미 수립했습니다.

참고: Cisco IOS Software 보안은 CatOS와 달리 Cisco ISP Essentials와 같은 여러 문서에서 다룹니다.

기본 보안 기능

비밀번호

사용자 수준 암호(로그인)를 구성합니다. 비밀번호는 CatOS 5.x 이상에서 대/소문자를 구분하며 공백을 포함하여 길이가 0~30자입니다.enable 비밀번호를 설정합니다.

```
set password password set enablepass password
```

모든 비밀번호는 최소 길이 표준(예: 최소 6자, 문자 및 숫자 조합, 대문자 및 소문자)을 충족해야 로그인할 수 있으며, 사용할 경우 비밀번호를 사용할 수 있습니다.이러한 비밀번호는 MD5 해싱 알고리즘을 사용하여 암호화됩니다.

비밀번호 보안 및 디바이스 액세스를 보다 유연하게 관리할 수 있도록 TACACS+ 서버를 사용하는 것이 좋습니다.자세한 내용은 이 문서의 TACACS+ 섹션을 참조하십시오.

보안 셸

SSH 암호화를 사용하여 텔넷 세션 및 스위치에 대한 기타 원격 연결에 보안을 제공합니다.SSH 암호화는 스위치에 대한 원격 로그인에 대해서만 지원됩니다.스위치에서 시작된 텔넷 세션은 암호화할 수 없습니다.SSH 버전 1은 CatOS 6.1에서 지원되고 버전 2는 CatOS 8.3에 추가되었습니다. SSH 버전 1은 DES(Data Encryption Standard) 및 3-DES(3-DES) 암호화 방법을 지원하며 SSH 버전 2는 3-DES 및 AES(Advanced Encryption Standard) 암호화 방법을 지원합니다.RADIUS 및 TACACS+ 인증과 함께 SSH 암호화를 사용할 수 있습니다.이 기능은 SSH(k9) 이미지에서 지원됩니다.자세한 내용은 CatOS를 실행하는 Catalyst 스위치에서 SSH를 구성하는 방법을 참조하십시오 .

```
set crypto key rsa 1024
```

버전 1 폴백을 비활성화하고 버전 2 연결을 승인하려면 다음 명령을 실행합니다.

```
set ssh mode v2
```

IP 허용 필터

텔넷 및 기타 프로토콜을 통해 관리 sc0 인터페이스에 대한 액세스를 보호하는 필터입니다.이는 관리에 사용되는 VLAN에 사용자도 포함되어 있는 경우 특히 중요합니다.IP 주소 및 포트 필터링을 활성화하려면 다음 명령을 실행합니다.

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

그러나 텔넷 액세스가 이 명령으로 제한된 경우, CatOS 디바이스에 대한 액세스는 소수의 신뢰할 수 있는 엔드스테이션을 통해서만 가능합니다.이 설정은 문제 해결에 방해가 될 수 있습니다.IP 주소를 스푸핑하고 필터링된 액세스를 속일 수 있으므로 이는 첫 번째 보호 레이어일 뿐입니다.

포트 보안

하나 또는 여러 개의 알려진 MAC 주소만 특정 포트에 데이터를 전달할 수 있도록 포트 보안을 활용

하는 것이 좋습니다(예: 변경 제어 없이 고정 엔드 스테이션이 새 스테이션으로 교환되는 것을 막기 위해). 이는 고정 MAC 주소를 사용하여 수행할 수 있습니다.

```
set port security mod/port enable MAC address
```

이는 제한된 MAC 주소를 동적으로 학습하여 가능합니다.

```
set port security port range enable
```

다음 옵션을 구성할 수 있습니다.

- set port security *mod/port* age *time value*—새 주소를 학습하기 전에 포트의 주소를 보호하는 기간을 지정합니다.유효한 시간(분)은 10~1440입니다.기본값은 no aging(에이징 없음)입니다.
- set port *securitymod/port* maximum *value* - 포트에서 보호할 최대 MAC 주소 수를 지정하는 키워드유효한 값은 1(기본값) - 1025입니다.
- set port security *mod/port violation shutdown*—위반이 발생하면 포트(기본값)를 종료하고 syslog 메시지(기본값)를 전송하고 트래픽을 삭제합니다.
- set port security *mod/port* shutdown *time value*(포트가 비활성화된 상태로 유지되는 기간).유효한 값은 10~1440분입니다.기본값은 영구적으로 종료됩니다.

CatOS 6.x 이상에서 Cisco는 802.1x 인증을 도입했습니다. 이 인증은 클라이언트가 중앙 서버에 인증한 후 포트에 데이터를 사용하도록 설정할 수 있습니다.이 기능은 Windows XP와 같은 플랫폼에 대한 지원 초기 단계에 있지만 많은 기업에서 전략적 방향으로 간주할 수 있습니다.Cisco IOS Software를 실행하는 스위치에서 포트 보안을 구성하는 방법에 대한 자세한 내용은 포트 보안 구성을 참조하십시오.

로그인 배너

적절한 디바이스 배너를 생성하여 권한 없는 액세스에 대한 조치를 구체적으로 명시합니다.권한이 없는 사용자에게 정보를 제공할 수 있는 사이트 이름 또는 네트워크 데이터를 광고하지 마십시오 .이러한 배너에서는 장치가 손상되고 가해자가 붙잡히는 경우에 대응할 수 있습니다.

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

물리적 보안

적절한 권한 부여 없이는 디바이스에 물리적으로 액세스할 수 없으므로 장비가 제어된(잠긴) 공간에 있어야 합니다.네트워크가 작동 중이고 환경 요소의 악의적 변동으로 영향을 받지 않도록 모든 장비에는 적절한 UPS(가능한 경우 이중화 소스 포함)와 온도 제어(에어컨)가 있어야 합니다. 악의적인 의도로 물리적 액세스가 침해된 경우, 비밀번호 복구 또는 기타 방법을 통해 중단되는 경우가 훨씬 더 많습니다.

터미널 액세스 컨트롤러 액세스 제어 시스템

기본적으로 비권한 및 특권 모드 비밀번호는 전역적이며 콘솔 포트에서 또는 네트워크 전체의 텔넷 세션을 통해 스위치 또는 라우터에 액세스하는 모든 사용자에게 적용됩니다.네트워크 디바이스에 구현하려면 시간이 많이 소요되고 중앙 집중화되지 않습니다.또한 구성 오류가 발생할 수 있는 액세스 목록을 사용하여 액세스 제한을 구현하기가 어렵습니다.

네트워크 디바이스에 대한 액세스 제어 및 보안을 지원하는 세 가지 보안 시스템을 사용할 수 있습니다.이러한 아키텍처는 클라이언트/서버 아키텍처를 사용하여 모든 보안 정보를 단일 중앙 데이터베이스에 저장합니다.이 세 가지 보안 시스템은 다음과 같습니다.

- TACACS+
- RADIUS
- Kerberos

TACACS+는 Cisco 네트워크의 일반적인 구축이며 이 장의 핵심입니다.다음과 같은 기능을 제공합니다.

- Authentication(인증) - 사용자에 대한 식별 및 확인 프로세스입니다.여러 방법을 사용하여 사용자를 인증할 수 있지만 가장 일반적인 방법에는 사용자 이름과 비밀번호의 조합이 포함됩니다.
- 사용자가 인증되면 다양한 명령 중 권한 부여가 가능합니다.
- Accounting(계정 관리) - 사용자가 디바이스에서 수행하고 있거나 수행한 작업을 기록합니다.

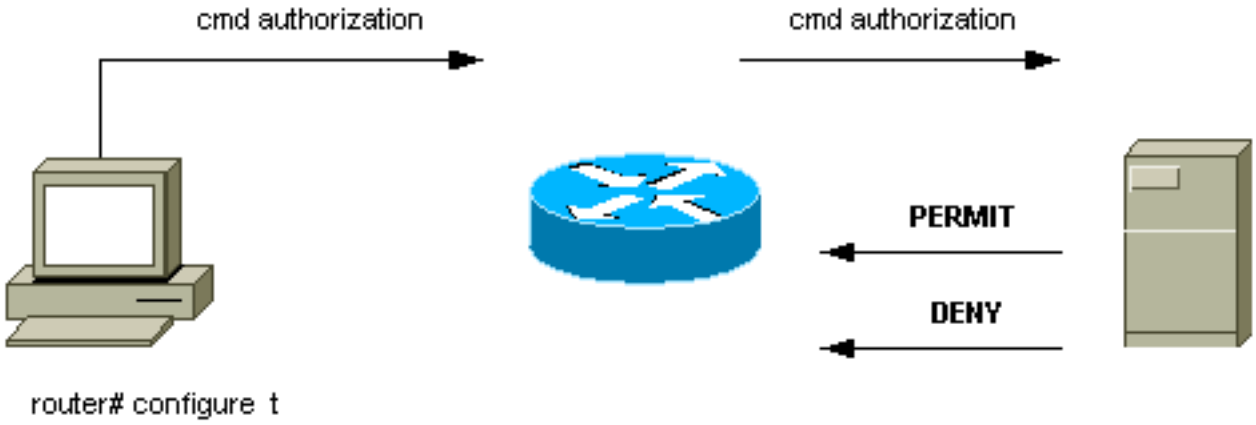
자세한 내용은 Cisco Catalyst 스위치에서 TACACS+, RADIUS 및 Kerberos 구성을 참조하십시오.

운영 개요

TACACS+ 프로토콜은 **MD5** 단방향 해싱(RFC 1321)을 사용하여 네트워크를 통해 암호화된 중앙 집중식 서버로 사용자 이름과 비밀번호를 전달합니다. TCP 포트 49를 전송 프로토콜로 사용합니다.UDP(RADIUS에서 사용)에 비해 다음과 같은 장점이 있습니다.

- 연결 지향 전송
- 백엔드 인증 메커니즘이 현재 로드된 방식과 상관없이 요청이 수신되었다는 별도의 확인(TCP ACK)
- 서버 충돌(RST 패킷)의 즉각적인 표시

세션 중에 추가 권한 확인이 필요한 경우 스위치는 TACACS+를 통해 사용자에게 특정 명령을 사용할 수 있는 권한이 부여되었는지 확인합니다.이렇게 하면 인증 메커니즘에서 연결을 해제하면서 스위치에서 실행할 수 있는 명령을 더 효과적으로 제어할 수 있습니다.명령 어카운팅을 사용하면 특정 네트워크 디바이스에 연결된 동안 특정 사용자가 실행한 명령을 감사할 수 있습니다.



사용자가 TACACS+를 사용하여 네트워크 디바이스에 인증하여 간단한 ASCII 로그인을 시도할 경우 이 프로세스는 일반적으로 다음과 같이 수행됩니다.

- 연결이 설정되면 스위치는 TACACS+ 데몬에 연결하여 사용자 이름 프롬프트를 가져온 다음 사용자에게 표시됩니다.사용자가 사용자 이름을 입력하면 스위치가 TACACS+ 데몬에 연결하여 비밀번호 프롬프트를 가져옵니다.이 스위치는 사용자에게 비밀번호 프롬프트를 표시합니다. 그러면 TACACS+ 데몬으로 전송되는 비밀번호를 입력합니다.
- 네트워크 디바이스는 결국 TACACS+ 디먼으로부터 다음 응답 중 하나를 수신합니다.ACCEPT - 사용자가 인증되고 서비스가 시작될 수 있습니다.네트워크 디바이스가 권한 부여가 필요하도록 구성된 경우 권한 부여가 지금 시작됩니다.REJECT - 사용자가 인증하지 못했습니다.사용자는 추가 액세스를 거부할 수 있으며 TACACS+ 데몬에 따라 로그인 시퀀스를 재시도하라는 메시지가 표시됩니다.ERROR - 인증 중에 오류가 발생했습니다.데몬 또는 데먼과 스위치 간의 네트워크 연결에서 이 값을 지정할 수 있습니다.ERROR 응답이 수신되면 일반적으로 네트워크 디바이스는 사용자를 인증하기 위해 대체 방법을 사용하려고 시도합니다.CONTINUE(계속) - 사용자에게 추가 인증 정보를 묻는 메시지가 표시됩니다.
- 사용자는 TACACS+ 권한 부여를 진행하기 전에 먼저 TACACS+ 인증을 성공적으로 완료해야 합니다.
- TACACS+ 권한 부여가 필요한 경우 TACACS+ 데몬에 다시 연결하여 ACCEPT 또는 REJECT 권한 부여 응답을 반환합니다.ACCEPT 응답이 반환되면 응답에는 해당 사용자에 대한 EXEC 또는 NETWORK 세션을 지시하고 사용자가 액세스할 수 있는 명령을 결정하는 데 사용되는 속성 형식의 데이터가 포함됩니다.

권장 사항

NT, Unix 또는 기타 타사 소프트웨어용 CiscoSecure ACS를 사용하여 손쉽게 구현할 수 있으므로 TACACS+를 사용하는 것이 좋습니다.TACACS+ 기능에는 명령 사용 및 시스템 사용에 대한 통계, MD5 암호화 알고리즘, 인증 및 권한 부여 프로세스에 대한 관리 제어를 제공하는 자세한 어카운팅이 포함됩니다.

이 예에서 로그인 및 활성화 모드는 인증을 위해 TACACS+ 서버를 사용하며 서버를 사용할 수 없는 경우 로컬 인증으로 돌아갈 수 있습니다.대부분의 네트워크에서 중요한 백도어입니다.TACACS+를 설정하려면 다음 명령을 실행합니다.

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

기타 옵션

TACACS+ 권한 부여를 사용하여 스위치에서 각 사용자 또는 사용자 그룹이 실행할 수 있는 명령을 제어할 수 있지만, 모든 고객이 이 영역에서 개별 요구 사항을 가지고 있기 때문에 권장하기 어렵습니다.자세한 내용은 인증, 권한 부여 및 계정 관리를 사용하여 스위치에 대한 액세스 제어를 참조하십시오.

마지막으로, 어카운팅 명령은 각 사용자가 입력 및 구성한 항목에 대한 감사 추적을 제공합니다.다음은 명령 끝에서 감사 정보를 수신하는 일반적인 방법을 사용하는 예입니다.

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

이 구성에는 다음과 같은 기능이 있습니다.

- connect 명령을 사용하면 텔넷과 같은 스위치에서 아웃바운드 연결 이벤트를 어카운팅할 수 있습니다.
- exec 명령을 사용하면 운영 직원과 같은 스위치의 로그인 세션을 어카운팅할 수 있습니다.
- system 명령은 다시 로드 또는 재설정과 같은 스위치에서 시스템 이벤트를 어카운팅할 수 있도록 합니다.
- commands 명령을 사용하면 **show** 및 configuration 명령에 대해 스위치에 입력된 내용을 확인할 수 있습니다.
- 서버에 대한 정기 *업데이트*는 사용자가 아직 로그인되어 있는지 여부를 기록하기 위해 1분마다 유용합니다.

구성 체크리스트

이 섹션에서는 보안 세부사항을 제외하고 권장 컨피그레이션에 대한 요약을 제공합니다.

모든 포트에 레이블을 지정하는 것이 매우 유용합니다.포트에 레이블을 지정하려면 다음 명령을 실행합니다.

```
set port description descriptive name
```

이 키를 나열된 명령 테이블과 함께 사용합니다.

키:
굵은 텍스트 - 권장 변경
일반 텍스트 - 기본, 권장 설정

전역 구성 명령

명령	**설명**
vtp 도메인 *이름 암호* 설정	새로운 스위치로부터 무단 VTP 업데이트를 차단합니다.
vtp 모드 투명 설정	이 문서에서 승격된 VTP 모드를 선택합니다.자세한 내용은 이 문서의 VLAN Trunking Protocol 섹션을 참조하십시오.
spantree enable all(spantree 모두 설정)	모든 VLAN에서 STP가 활성화되었는지 확인합니다.
spantree 루트 *vlan 설*	VLAN별로 루트(및 보조 루트) 브

정	리지를 배치하는 것이 좋습니다.
spantree backboneast 사용 설정	간접 장애로부터 신속한 STP 컨버전스를 활성화합니다(도메인의 모든 스위치가 이 기능을 지원하는 경우에만).
spantree uplinkfast enable 설정	직접 장애로부터 신속한 STP 컨버전스를 활성화합니다(액세스 레이어 스위치에만 해당).
spantree portpdu-guard 활성화	권한이 없는 스패닝 트리 확장이 있는 경우 포트를 자동으로 종료하도록 설정합니다.
udld 사용 설정	단방향 링크 탐지를 활성화합니다(포트 레벨 컨피그레이션도 필요).
테스트 진단 수준 설정 완료	부팅 시 전체 진단을 활성화합니다(Catalyst 4500/4000의 경우 기본값).
set test packetbuffer sun 3:30	포트 버퍼 오류 검사를 활성화합니다(Catalyst 5500/5000에만 적용).
로깅 버퍼 설정 500	최대 내부 syslog 버퍼를 유지합니다.
로깅 서버 *IP 주소 설정*	외부 시스템 메시지 로깅을 위한 대상 syslog 서버를 구성합니다.
로깅 서버 설정	외부 로깅 서버를 허용합니다.
로깅 타임스탬프 설정	로그에 있는 메시지의 타임스탬프를 활성화합니다.
로깅 레벨 spantree 6 기본값 설정	기본 STP syslog 레벨을 높입니다.
로깅 레벨 sys 6 기본값 설정	기본 시스템 syslog 레벨을 높입니다.
로깅 서버 심각도 4 설정	심각도가 높은 syslog의 내보내기만 허용합니다.
로깅 콘솔 비활성화	문제를 해결하지 않으면 콘솔을 비활성화합니다.
snmp 커뮤니티 읽기 전용 *문자열 설정*	원격 데이터 수집을 허용하도록 비밀번호를 구성합니다.
snmp 커뮤니티 읽기-쓰기 *문자열 설정*	원격 구성을 허용하도록 비밀번호를 구성합니다.
snmp community read-write-all *문자열 설정*	비밀번호를 포함한 원격 구성을 허용하도록 비밀번호를 구성합니다.
snmp 트랩 설정 all	오류 및 이벤트 알림을 위해 NMS 서버에 대한 SNMP 트랩을 활성화합니다.
snmp 트랩 *서버 주소 문자열 설정*	NMS 트랩 수신자의 주소를 구성합니다.
snmp rmon 설정	로컬 통계 수집을 위해 RMON을 활성화합니다.자세한 내용은 이

	문서의 원격 모니터링 섹션을 참조하십시오.
ntp broadcast client enable 설정	업스트림 라우터에서 정확한 시스템 클럭 수신 기능을 활성화합니다.
ntp 표준 시간대 *영역 이름 설정*	디바이스의 로컬 시간대를 설정합니다.
ntp 여름철 *날짜 변경 세부사항 설정*	표준 시간대로 적용 가능한 경우 여름철 구성
ntp 인증 설정	보안을 위해 암호화된 시간 정보를 구성합니다.
ntp 키 *키 설정*	암호화 키를 구성합니다.
cdp 활성화 설정	네이버 검색이 활성화되었는지 확인합니다(기본적으로 포트에서도 활성화됨).
tacacs 서버 *IP 주소* 기본 설정	AAA 서버의 주소를 구성합니다.
tacacs 서버 *IP 주소 설정*	가능한 경우 이중화 AAA 서버.
tacacs 시도 설정 3	AAA 사용자 계정에 대해 3개의 비밀번호 시도를 허용합니다.
tacacs 키 *키 설정*	AAA MD5 암호화 키를 설정합니다.
tacacs 시간 초과 설정 15	더 긴 서버 시간 초과 허용(5초가 기본값입니다).
인증 로그인 tacacs 활성화	로그인을 위해 AAA를 사용합니다.
인증 enable tacacs enable 설정	활성화 모드에 대한 인증에 AAA를 사용합니다.
인증 로그인 로컬 활성화 설정	기본값;사용할 수 있는 AAA 서버가 없는 경우 로컬 폴백을 허용합니다.
설정 인증 enable local enable	기본값;사용할 수 있는 AAA 서버가 없는 경우 로컬 폴백을 허용합니다.

호스트 포트 컨피그레이션 명령

명령	설명
포트 호스트 포트 범위 설정	불필요한 포트 처리를 제거합니다.이 매크로는 PortFast 활성화, 채널 끄기, 트렁크 오프를 지원합니다.
udld 비활성화 *포트 범위 설정*	불필요한 포트 처리를 제거합니다(기본적으로 구리 포트에서 비활성화됨).
포트 속도 *포트 범위* 자동 설정	최신 호스트 NIC 드라이버와 자동 협상을 사용합니다.

포트 트랩 *포트 범위 설정* 비활성화	일반 사용자를 위한 SNMP 트랩이 필요하지 않습니다.키 포트만 추적합니다.

서버 구성 명령

명령	설명
포트 호스트 *포트 범위 설정*	불필요한 포트 처리를 제거합니다.이 매크로는 PortFast 활성화, 채널 끄기, 트렁크 오프를 지원합니다.
udld 비활성화 *포트 범위 설정*	불필요한 포트 처리를 제거합니다(기본적으로 구리 포트에서 비활성화됨).
포트 속도 *포트 범위 설정 10 | 100*	일반적으로 고정/서버 포트를 구성합니다.그렇지 않으면 autonegotiation을 사용합니다.
포트 듀플렉스 *포트 범위 전체 설정 | 절반*	일반적으로 고정/서버 포트;그렇지 않으면 autonegotiation을 사용합니다.
포트 트랩 *포트 범위 설정* 활성화	키 서비스 포트는 NMS로 트랩을 보내야 합니다.

사용되지 않은 포트 컨피그레이션 명령

명령	설명
spantree portfast *포트 범위 비활성화* 설정	STP에 필요한 포트 처리 및 보호를 활성화합니다.
포트 비활성화 *포트 범위 설정*	사용하지 않는 포트를 비활성화합니다.
vlan *사용되지 않은 더미 VLAN 포트 범위 설정*	포트가 활성화된 경우 미사용 VLAN으로 무단 트래픽을 전송합니다.
트렁크 *포트 범위* 끄기 설정	관리될 때까지 트렁킹에서 포트를 비활성화합니다.
포트 채널 *포트 범위* 모드 설정 해제	관리될 때까지 채널링에서 포트를 비활성화합니다.

인프라 포트(스위치, 스위치 라우터)

명령	설명
udld enable *포트 범위 설정*	단방향 링크 탐지를 활성화합니다(구리 포트의 기본값은 아님).
udld aggressive-mode enable *포트 범위 설정*	적극적인 모드를 활성화합니다(이를 지원하는 디바이스의 경우).
포트 협상 *포트 범위 설정사용* 가능	링크 매개변수의 기본 GE 자동 협상을 허용합니다.

포트 트랩 *포트 범위 설정* 사용	이러한 키 포트에 대해 SNMP 트랩을 허용합니다.
트렁크 *포트 범위* 끄기 설정	트렁크를 사용하지 않는 경우 기능을 비활성화합니다.
set trunk *mod/port desired ISL | dot1q | 협상*	트렁크를 사용하는 경우 dot1q를 사용하는 것이 좋습니다.
트렁크 *mod/port vlan 범위 지우기*	필요 없는 트렁크에서 VLAN을 정리하여 STP 지름을 제한합니다.
포트 채널 *포트 범위* 모드 설정 해제	채널을 사용하지 않는 경우 기능을 비활성화합니다.
포트 채널 *포트 범위* 모드 권장 설정	채널을 사용하는 경우 PAgP가 활성화됩니다.
포트 채널 모든 배포 ip 모두 설정	채널을 사용하는 경우 L3 소스/대상 로드 밸런싱을 허용합니다(Catalyst 6500/6000에서 기본값).
set trunk *mod/port nonegotiate* ISL *설정 | dot1q*	라우터, Catalyst 2900XL, 3500 또는 기타 벤더로 트렁킹하는 경우 DTP를 비활성화합니다.
포트 협상 *모드/포트 비활성화 설정*	일부 이전 GE 디바이스에는 협상이 호환되지 않을 수 있습니다.

관련 정보

- Catalyst 4500/4000 Series 스위치의 일반적인 CatOS 오류 메시지
- Catalyst 5000/5500 Series 스위치의 일반적인 CatOS 오류 메시지
- Catalyst 6500/6000 Series 스위치의 일반적인 CatOS 오류 메시지
- 스위치 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems