Cisco IOS 소프트웨어를 실행하는 Catalyst 6500/6000 Series 및 Catalyst 4500/4000 Series 스위치의 모범 사례

목차

소개

이 문서에서는 Supervisor Engine에서 Cisco IOS® Software를 실행하는 Catalyst 6500/6000 및 4500/4000 Series 스위치에 대한 모범 사례를 제공합니다.

Catalyst 6500/6000 및 Catalyst 4500/4000 시리즈 스위치는 Supervisor Engine에서 실행되는 다음 두 가지 운영 체제 중 하나를 지원합니다.

- Catalyst OS(CatOS)
- Cisco IOS 소프트웨어

CatOS에서는 다음과 같은 라우터 부속 카드 또는 모듈에서 Cisco IOS 소프트웨어를 실행할 수 있습니다.

- Catalyst 6500/6000의 MSFC(Multilayer Switch Feature Card)
- Catalyst 4500/4000의 4232 Layer 3(L3) 모듈

이 모드에서는 컨피그레이션을 위한 두 개의 명령줄이 있습니다.

- 스위칭을 위한 CatOS 명령줄
- 라우팅을 위한 Cisco IOS Software 명령행

CatOS는 Supervisor Engine에서 실행되는 시스템 소프트웨어입니다.라우팅 모듈에서 실행되는 Cisco IOS 소프트웨어는 CatOS 시스템 소프트웨어가 필요한 옵션입니다.

Cisco IOS Software의 경우 컨피그레이션을 위한 명령줄이 하나만 있습니다.이 모드에서는 CatOS의 기능이 Cisco IOS Software에 통합되었습니다.이러한 통합으로 스위칭 및 라우팅 컨피그레이션을 모두 하나의 명령줄로 구성할 수 있습니다.이 모드에서는 Cisco IOS 소프트웨어가 시스템 소프트웨어이며 CatOS를 대체합니다.

CatOS 및 Cisco IOS Software 운영 체제는 모두 중요 네트워크에 구축됩니다.라우터 부속 카드 및 모듈용 Cisco IOS Software 옵션이 포함된 CatOS는 다음 스위치 시리즈에서 지원됩니다.

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Cisco IOS 시스템 소프트웨어는 다음 스위치 시리즈에서 지원됩니다.

- Catalyst 6500/6000
- Catalyst 4500/4000

CatOS 구성 및 관리를 실행하는 Catalyst 4500/4000, 5500/5000 및 6500/6000 Series 스위치에 대한 모범 사례 문서에서 Cisco IOS 시스템 소프트웨어에 대한 정보를 참조하십시오.

Cisco IOS 시스템 소프트웨어는 사용자에게 다음과 같은 몇 가지 이점을 제공합니다.

- 단일 사용자 인터페이스
- 통합 네트워크 관리 플랫폼
- 향상된 QoS 기능
- 분산 스위칭 지원

이 문서에서는 모듈형 구성 지침을 제공합니다.따라서 각 섹션을 독립적으로 읽고 단계별 접근 방식을 변경할 수 있습니다.이 문서에서는 기본적으로 Cisco IOS Software 사용자 인터페이스에 대해 이해하고 있다고 가정합니다.이 문서에서는 전체 캠퍼스 네트워크 설계를 다루지 않습니다.

시작하기 전에

배경

이 문서에서 제공하는 솔루션은 복잡한 네트워크 및 많은 대규모 고객과 함께 일하는 Cisco 엔지니어의 오랜 현장 경험을 나타냅니다.따라서 이 문서에서는 네트워크를 성공적으로 만드는 실제 구성을 강조합니다.이 문서에서는 다음과 같은 솔루션을 제공합니다.

- 가장 광범위한 현장 노출, 그리고 그에 따라 가장 낮은 위험이 있는 솔루션
- 확실한 결과를 얻을 수 있는 유연성을 제공하는 간단한 솔루션
- 관리가 용이하고 네트워크 운영 팀이 구성하는 솔루션
- 고가용성 및 고안정성을 촉진하는 솔루션

참조

Cisco.com에는 Catalyst 6500/6000 및 Catalyst 4500/4000 제품 라인에 대한 많은 참조 사이트가 있습니다.이 단원이 나열하는 참조는 이 문서에서 설명하는 항목에 대한 추가 세부 정보를 제공합니다.

이 문서에서 다루는 항목에 대한 자세한 내용은 LAN 스위칭 기술 지원을 참조하십시오.지원 페이지에서는 제품 설명서와 트러블슈팅 및 구성 문서를 제공합니다.

이 문서에서는 퍼블릭 온라인 자료에 대한 참조를 제공하여 더 자세히 읽을 수 있습니다.그러나 다른 훌륭한 기본 및 교육 자료는 다음과 같습니다.

- Cisco ISP Essentials
- Cisco Catalyst 6500 Series 스위치를 위한 Cisco Catalyst 및 Cisco IOS 운영 체제 비교
- Cisco LAN 스위칭(CCIE Professional Development Series)
- Cisco 멀티레이어 스위치 네트워크 구축
- 성능 및 결합 관리
- 안전:엔터프라이즈 네트워크를 위한 보안 청사진
- Cisco 필드 설명서:Catalyst 스위치 구성

기본 구성

이 섹션에서는 대부분의 Catalyst 네트워크를 사용할 때 구축되는 기능에 대해 설명합니다.

Catalyst 컨트롤 플레인 프로토콜

이 섹션에서는 정상적인 작동 상태에서 스위치 간에 실행되는 프로토콜을 소개합니다.프로토콜에 대한 기본적인 이해는 각 섹션을 다룰 때 유용합니다.

수퍼바이저 엔진 트래픽

Catalyst 네트워크에서 활성화된 대부분의 기능을 사용하려면 두 개 이상의 스위치가 필요합니다.따라서 keepalive 메시지, 컨피그레이션 매개변수 및 관리 변경의 통제된 교환이 있어야 합니다.이러한 프로토콜이 CDP(Cisco Discovery Protocol)와 같은 Cisco 독점 프로토콜이든, IEEE 802.1D(STP[Spanning Tree Protocol])와 같은 표준 기반 프로토콜이든, Catalyst 시리즈에 프로토콜을 구현할 때 모두 특정 요소가 공통으로 존재합니다.

기본 프레임 포워딩에서 사용자 데이터 프레임은 최종 시스템에서 시작됩니다.데이터 프레임의 SA(소스 주소) 및 DA(대상 주소)는 L2(Layer 2) 스위치 도메인 전체에서 변경되지 않습니다.각 스위치의 CAM(Content-Addressable Memory) 조회 테이블은 SA 학습 프로세스로 채워집니다.테이블에는 수신된 각 프레임을 전달하는 이그레스 포트가 표시됩니다.대상을 알 수 없거나 프레임을 브로드캐스트 또는 멀티캐스트 주소로 보낼 경우 주소 학습 프로세스가 완료되지 않습니다.프로세스가 완료되지 않으면 프레임이 해당 VLAN의 모든 포트로 전달(플러드)됩니다.또한 스위치에서는 시스템을 통해 전환할 프레임과 스위치 CPU 자체에 전달할 프레임을 인식해야 합니다.스위치 CPU는 NMP(Network Management Processor)라고도 합니다.

CAM 테이블의 특수 항목은 Catalyst 컨트롤 플레인을 만드는 데 사용됩니다.이러한 특수 항목을 시스템 엔트리라고 합니다.컨트롤 플레인은 내부 스위치 포트의 NMP로 트래픽을 수신하고 전달합니다.따라서 잘 알려진 목적지 MAC 주소가 있는 프로토콜을 사용하면 컨트롤 플레인 트래픽이 데이터 트래픽에서 분리될 수 있습니다.

Cisco는 이 섹션의 표에 나와 있는 것처럼 이더넷 MAC 및 프로토콜 주소의 예약된 범위를 보유하고 있습니다.이 문서에서는 각 예약된 주소에 대해 자세히 설명하지만, 이 표에서는 편의를 위해 다음과 같은 요약을 제공합니다.

기능	SNAP[1] HDLC[2] 프로토콜 유형	대상 멀티캐스트 MAC
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
VLAN 브리지	0x010c	01-00-0c-cd-ce
UDLD[5]	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
STP 업링크 Fast	0x200a	01-00-0c-cd-cd-cd
IEEE 스패닝 트리 802.1D	해당 사항 없음—DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	해당 없음	01-00-0c-00-00-00
VTP[10]	0x2003	01-00-0c-cc-cc-cc
IEEE 일시중지 802.3x	해당 사항 없음—DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] SNAP = 하위 네트워크 액세스 프로토콜

[2] HDLC = 고급 데이터 링크 컨트롤

[3] PAgP = 포트 어그리게이션 프로토콜

[4] PVST+ = VLAN 스패닝 트리+ 및 RPVST+당 = Rapid PVST+

5 UDLD = UniDirectional Link Detection(단방향 링크 탐지).

[6] DTP = 동적 트렁킹 프로토콜

[7] DSAP = 대상 서비스 액세스 포인트

[8] SSAP = 소스 서비스 액세스 포인트

[9] ISL = 스위치 간 링크

[10] VTP = VLAN 트렁크 프로토콜

대부분의 Cisco 제어 프로토콜은 IEEE 802.3 SNAP 캡슐화를 사용합니다. 여기에는 LLC(Logical Link Control) 0xAAAA03 및 OUI(Organizational Unique Identifier) 0x0000C가 포함됩니다.LAN 분석기 추적에서 이를 확인할 수 있습니다.

이러한 프로토콜은 포인트 투 포인트 연결을 가정합니다.멀티캐스트 목적지 주소를 신중하게 사용하면 두 개의 Catalyst 스위치가 비 Cisco 스위치를 통해 투명하게 통신할 수 있습니다.프레임을 이해하고 가로채지 못하는 디바이스는 단순히 프레임을 플러딩합니다.그러나 멀티벤더 환경을 통한 point-to-multipoint 연결은 일관되지 않은 동작으로 이어질 수 있습니다.일반적으로 멀티벤더 환경을 통해 지점 간 연결을 방지합니다.이러한 프로토콜은 레이어 3 라우터에서 종료되며 스위치 도메인 내에서만 작동합니다.이러한 프로토콜은 인그레스(ingress) ASIC(application-specific integrated circuit) 처리 및 스케줄링을 통해 사용자 데이터보다 우선 순위를 지정합니다.

이제 SA로 넘어갑니다.스위치 프로토콜은 사용 가능한 주소의 은행에서 가져온 MAC 주소를 사용합니다.섀시의 EPROM은 사용 가능한 주소의 은행을 제공합니다.STP BPDU(Bridge Protocol Data Unit) 또는 ISL 프레임과 같은 트래픽 소싱을 위해 각 모듈에서 사용할 수 있는 주소 범위를 표시하려면 show module 명령을 실행합니다.다음은 샘플 명령 출력입니다.

```
>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
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1은 Catalyst 네트워크에서 특별한 의미를 갖습니다.

트렁킹 시 Catalyst Supervisor Engine은 항상 기본 VLAN, VLAN 1을 사용하여 여러 제어 및 관리 프로토콜에 태그를 지정합니다.이러한 프로토콜에는 CDP, VTP 및 PAgP가 포함됩니다.내부 sc0 인터페이스를 포함하는 모든 스위치 포트는 기본적으로 VLAN 1의 멤버로 구성됩니다. 모든 트렁크는 기본적으로 VLAN 1을 전달합니다.

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

- 관리 VLAN은 sc0이 CatOS 및 로우엔드 스위치에 상주하는 곳입니다.이 VLAN을 변경할 수 있습니다.CatOS와 Cisco IOS 스위치를 모두 상호 운용할 때 이 점을 염두에 두십시오.
- 네이티브 VLAN은 트렁킹 중이 아닐 때 포트가 반환하는 VLAN입니다.또한 네이티브 VLAN은 IEEE 802.1Q 트렁크에서 태그되지 않은 VLAN입니다.

네트워크를 조정하고 VLAN 1의 포트 동작을 변경하는 데에는 다음과 같은 몇 가지 이유가 있습니

다.

- 다른 VLAN과 마찬가지로 VLAN 1의 지름이 안정성에 위험할 정도로 커지면, 특히 STP의 관점에서 VLAN을 다시 정리해야 합니다.자세한 내용은 스위치 관리 인터페이스 및 네이티브 VLAN 섹션을 참조하십시오.
- 문제 해결을 간소화하고 사용 가능한 CPU 주기를 최대화하려면 VLAN 1의 컨트롤 플레인 데이터를 사용자 데이터와 별도로 유지해야 합니다.STP 없이 멀티레이어 캠퍼스 네트워크를 설계할 때 VLAN 1에서 레이어 2 루프를 방지합니다.레이어 2 루프를 방지하려면 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 사용해도 여전히 전송되는 컨트롤 플레인 트래픽에는 영향을 미치지 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 않습니다.이는 네이티브 VLAN 컨피그레이션과 상관없이 해당됩니다.Cisco PVST+ BPDU는 다른 모든 VLAN에 대해 전송 및 태그가 지정됩니다.자세한 내용은 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 루트 불일치 상태로 경계 포트의 MST 브리지 배치를 방지하려면 MST 브리지가 루트가 되어야 합니다.자세한 내용은 다중 스패닝 트리 프로토콜(802.1s) 이해를 참조하십시오.

표준 기능

이 섹션에서는 모든 환경에 공통된 기본 스위칭 기능에 대해 중점적으로 설명합니다.고객 네트워크의 모든 Cisco IOS Software Catalyst 스위칭 디바이스에서 이 기능을 구성합니다.

VLAN 트렁크 프로토콜

목적

VLAN 관리 도메인이라고도 하는 VTP 도메인은 동일한 VTP 도메인 이름을 공유하는 트렁크를 통해 하나 이상의 상호 연결된 스위치로 구성됩니다.VTP는 사용자가 하나 이상의 스위치에서 중앙에서 VLAN 컨피그레이션을 변경할 수 있도록 설계되었습니다.VTP는 (네트워크) VTP 도메인의 다른 모든 스위치에 변경 사항을 자동으로 전달합니다.스위치를 하나의 VTP 도메인에만 포함하도록 구성할 수 있습니다.VLAN을 생성하기 전에 네트워크에서 사용할 VTP 모드를 결정합니다.

운영 개요

VTP는 레이어 2 메시징 프로토콜입니다.VTP는 VLAN 컨피그레이션 일관성을 유지하기 위해 네트워크 전체에서 VLAN의 추가, 삭제 및 이름 변경을 관리합니다.VTP는 구성 및 컨피그레이션 불일치

를 최소화하여 여러 문제를 일으킬 수 있습니다.이러한 문제에는 중복 VLAN 이름, 잘못된 VLAN 유형 사양, 보안 위반이 포함됩니다.

기본적으로 스위치는 VTP 서버 모드이며 관리 대상이 아닌 도메인 상태입니다.이러한 기본 설정은 스위치가 트렁크 링크를 통해 도메인에 대한 알림을 수신하거나 관리 도메인을 구성할 때 변경됩니다.

VTP 프로토콜은 잘 알려진 이더넷 대상 멀티캐스트 MAC(01-00-0c-cc-cc-cc-cc) 및 SNAP HDLC 프로토콜 유형 0x2003을 사용하여 스위치 간에 통신합니다. 다른 내장 프로토콜과 마찬가지로 VTP는 LLC 0xAAAA03 및 OUI 0x0000c0x0003을 포함하는 IEEE 800202.3 PACENCAPSULATION0을 사용합니다. ...을 클릭합니다.LAN 분석기 추적에서 이를 확인할 수 있습니다.VTP는 트렁크가 아닌 포트에서 작동하지 않습니다.따라서 DTP가 트렁크를 가동할 때까지 메시지를 보낼 수 없습니다.즉, VTP는 ISL 또는 802.1Q의 페이로드입니다.

메시지 유형은 다음과 같습니다.

- 300초마다 요약 광고
- 변경이 있을 경우 서브세트 광고 및 광고 요청
- VTP 정리를 사용할 때 조인

VTP 컨피그레이션 개정 번호는 서버에서 모든 변경 사항이 포함된 1씩 증가하며, 해당 테이블은 도메인 전체에 전파됩니다.

VLAN을 삭제할 때 VLAN의 멤버였던 포트는 상태로 들어갑니다.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.

다음 VTP 모드 중 하나에서 작동하도록 대부분의 Catalyst 스위치를 구성할 수 있습니다.

- 서버 - VTP 서버 모드에서 다음을 수행할 수 있습니다.VLAN 생성VLAN 수정VLAN 삭제전체 VTP 도메인에 대해 VTP 버전 및 VTP 정리와 같은 다른 구성 매개 변수를 지정합니다.VTP 서버는 VLAN 컨피그레이션을 동일한 VTP 도메인의 다른 스위치에 알립니다.또한 VTP 서버는 트렁크 링크를 통해 수신되는 광고를 기준으로 VLAN 컨피그레이션을 다른 스위치와 동기화합니다.VTP 서버가 기본 모드입니다.
- 클라이언트 - VTP 클라이언트는 VTP 서버와 동일한 방식으로 작동합니다.그러나 VTP 클라이언트에서는 VLAN을 생성, 변경 또는 삭제할 수 없습니다.또한 VLAN 정보가 NVRAM에 기록되지 않으므로 재부팅 후 클라이언트가 VLAN을 기억하지 못합니다.
- 투명 - VTP 투명 스위치는 VTP에 참여하지 않습니다.VTP 투명 스위치는 VLAN 컨피그레이션을 광고하지 않으며 수신된 광고를 기준으로 VLAN 컨피그레이션을 동기화하지 않습니다.그러나 VTP 버전 2에서는 투명 스위치가 트렁크 인터페이스를 통해 수신하는 VTP 광고를 전달합니다.

기능	서버	클라이언트	투명	꺼짐[1]
소스 VTP 메시지	예	예	아니요	—
VTP 메시지 수신	예	예	아니요	—
VLAN 생성	예	아니요	예(로컬에서만 중요함)	—

VLAN 기억	예	아니요	예(로컬에서만 중요함)	—

[1] Cisco IOS Software에는 모드를 사용하여 VTP를 비활성화하는 옵션이 없습니다.

이 표는 초기 컨피그레이션의 요약입니다.

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

VTP 투명 모드에서는 VTP 업데이트가 무시됩니다.잘 알려진 VTP 멀티캐스트 MAC 주소는 일반적으로 제어 프레임을 가져와서 Supervisor Engine에 전달하는 데 사용되는 시스템 CAM에서 제거됩니다.프로토콜은 멀티캐스트 주소를 사용하므로 투명 모드 또는 다른 벤더 스위치의 스위치는 단순히 프레임을 도메인의 다른 Cisco 스위치로 플러딩합니다.

VTP 버전 2(VTPv2)에는 이 목록에서 설명하는 기능 유연성이 포함됩니다.그러나 VTPv2는 VTP 버전 1(VTPv1)과 상호 운용되지 않습니다.

- 토큰 링 지원
- 인식할 수 없는 VTP 정보 지원 - 이제 스위치가 구문 분석할 수 없는 값을 전파합니다.
- 버전 종속 투명 모드 - 투명 모드가 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 스위치 구성으로 모든 스위치를 활성화할 수 있습니다.

자세한 내용은 VTP(VLAN Trunk Protocol) 이해를 참조하십시오.

Cisco IOS 소프트웨어의 VTP 작업

CatOS의 컨피그레이션 변경 사항은 변경 후 즉시 NVRAM에 기록됩니다.이와 달리 Cisco IOS Software는 copy run start 명령을 실행하지 않는 한 컨피그레이션 변경 사항을 NVRAM에 저장하지 않습니다.VTP 클라이언트 및 서버 시스템은 사용자 개입 없이 다른 VTP 서버의 VTP 업데이트를 NVRAM에 즉시 저장해야 합니다.VTP 업데이트 요구 사항은 기본 CatOS 작업에 의해 충족되지만 Cisco IOS 소프트웨어 업데이트 모델에는 대체 업데이트 작업이 필요합니다.

이러한 변경을 위해 VTP 클라이언트 및 서버에 대한 VTP 업데이트를 즉시 저장하는 방법으로 Catalyst 6500용 Cisco IOS Software에 VLAN 데이터베이스가 도입되었습니다.일부 소프트웨어 버전에서 이 VLAN 데이터베이스는 NVRAM에서 vlan.dat 파일이라는 별도의 파일 형식입니다.VLAN 데이터베이스의 백업이 필요한지 확인하려면 소프트웨어 버전을 확인하십시오.show vtp status 명령을 실행하면 VTP 클라이언트 또는 VTP 서버의 vlan.dat 파일에 저장된 VTP/VLAN 정보를 볼 수 **있습니다**.

이 시스템에서 copy run start 명령을 실행할 때 전체 VTP/VLAN 컨피그레이션이 NVRAM의 시작 컨피그레이션 파일에 저장되지 않습니다.이는 VTP로 투명하게 실행되는 시스템에는 적용되지 않습니다.VTP 투명 시스템은 copy run **start** 명령을 실행할 때 NVRAM의 시작 구성 파일에 전체 VTP/VLAN 컨피그레이션을 저장합니다.

Cisco IOS Software 릴리스 12.1(11b)E 이전 버전의 Cisco IOS Software에서는 VLAN 데이터베이스 모드를 통해서만 VTP 및 VLAN을 구성할 수 있습니다.VLAN 데이터베이스 모드는 전역 컨피그레이션 모드와 별도의 모드입니다.이러한 컨피그레이션 요구 사항의 이유는 VTP 모드 서버 또는 VTP 모드 클라이언트에서 디바이스를 구성할 때 VTP 인접 디바이스가 VTP 광고를 통해 동적으로 VLAN 데이터베이스를 업데이트할 수 있기 때문입니다.이러한 업데이트가 자동으로 컨피그레이션에 전파되지 않도록 합니다.따라서 VLAN 데이터베이스와 VTP 정보는 주 컨피그레이션에 저장되지 않지만 vlan.dat라는 이름의 파일에 NVRAM에 저장됩니다.

다음 예에서는 VLAN 데이터베이스 모드에서 이더넷 VLAN을 생성하는 방법을 보여 줍니다.

```
Switch#vlan database
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
```

Cisco IOS Software 릴리스 12.1(11b)E 이상에서는 VLAN 데이터베이스 모드 또는 전역 컨피그레이션 모드를 통해 VTP 및 VLAN을 구성할 수 있습니다.VTP 모드 서버 또는 VTP 모드 투명 모드에서 VLAN의 컨피그레이션은 NVRAM의 vlan.dat 파일을 계속 업데이트합니다.그러나 이러한 명령은 컨피그레이션에 저장되지 않습니다.따라서 실행 중인 컨피그레이션에 명령이 표시되지 않습니다.

자세한 내용은 *Configuring VLANs(VLAN 구성)* 문서의 Global Configuration Mode(전역 컨피그레이션 모드의 VLAN 컨피그레이션)를 참조하십시오.

다음 예에서는 글로벌 컨피그레이션 모드에서 이더넷 VLAN을 생성하는 방법과 컨피그레이션을 확인하는 방법을 보여줍니다.

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

참고: VLAN 컨피그레이션은 비휘발성 메모리에 저장되는 vlan.dat 파일에 저장됩니다.컨피그레이션의 전체 백업을 수행하려면 컨피그레이션과 함께 백업에 vlan.dat 파일을 포함합니다.그런 다음 전체 스위치 또는 Supervisor Engine 모듈을 교체해야 하는 경우 네트워크 관리자가 전체 컨피그레이션을 복원하려면 다음 두 파일을 모두 업로드해야 합니다.

- vlan.dat 파일
- 구성 파일

VTP 및 확장 VLAN

확장 시스템 ID 기능은 확장 범위 VLAN 식별을 활성화하는 데 사용됩니다.확장 시스템 ID가 활성화

된 경우 VLAN 스패닝 트리에 사용되는 MAC 주소 풀을 비활성화하고 스위치를 식별하는 단일 MAC 주소를 남겨둡니다.Catalyst IOS Software 릴리스 12.1(11b)EX 및 12.1(13)E는 IEEE 802.1Q 표준에 따라 4096 VLAN을 지원하기 위해 Catalyst 600/6500에 대한 확장 시스템 ID 지원을 소개합니다.이 기능은 Cisco IOS Software Release12.1(12c)EW for Catalyst 4000/4500 스위치에 도입되었습니다.이러한 VLAN은 여러 범위로 구성되어 있으며 각각 다르게 사용할 수 있습니다.이러한 VLAN 중 일부는 VTP를 사용할 때 네트워크의 다른 스위치로 전파됩니다.확장 범위 VLAN은 전파되지 않으므로 각 네트워크 디바이스에서 확장 범위 VLAN을 수동으로 구성해야 합니다.이 확장 시스템 ID 기능은 Catalyst OS의 MAC 주소 감소 기능과 동일합니다.

이 표에서는 VLAN 범위에 대해 설명합니다.

VLAN	범위	사용	VTP에서 전파됩니까?
0, 4095	예약됨	시스템 전용입니다.이러한 VLAN을 보거나 사용할 수 없습니다.	—
1	보통	Cisco 기본값.이 VLAN은 사용할 수 있지만 삭제할 수는 없습니다.	예
2–1001	보통	이더넷 VLAN의 경우이러한 VLAN을 생성, 사용 및 삭제할 수 있습니다.	예
1002–1005	보통	Cisco는 FDDI 및 토큰 링에 대한 기본값을 설정합니다.VLAN 1002-1005는 삭제할 수 없습니다.	예
1006–4094	예약됨	이더넷 VLAN에만 해당.	아니요

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

1024 MAC 주소가 있는 Catalyst 스위치는 기본적으로 확장 시스템 ID를 활성화하지 않습니다.MAC 주소는 순차적으로 할당됩니다. VLAN 1에 할당된 범위의 첫 번째 MAC 주소, VLAN 2에 할당된 범위의 두 번째 MAC 주소 등이 여기에 할당됩니다.이를 통해 스위치는 1024개의 VLAN을 지원할 수 있으며 각 VLAN은 고유한 브리지 식별자를 사용합니다.

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 주소가 64개인 섀시는 기본적으로 확장 시스템 ID를 활성화하며 이 기능을 비활성화할 수 없습니다.

자세한 내용은 *STP* 및 IEEE 802.1s MST 구성의 브리지 *ID 이해* 섹션을 참조하십시오.

MAC 주소가 1024개인 Catalyst 시리즈 스위치의 경우 확장 시스템 ID를 활성화하면 스위치에서 필요한 MAC 주소 수를 늘리지 않고 PVST+ 또는 16개의 MISTP 인스턴스에서 실행되는 4096개의 VLAN을 지원할 수 있습니다.Extended System ID는 STP에 필요한 MAC 주소 수를 VLAN 또는 MISTP 인스턴스당 1개에서 스위치당 1개로 줄입니다.

이 그림에는 확장 시스템 ID가 활성화되지 않은 경우의 브리지 식별자가 나와 있습니다.브리지 식별자는 2바이트 브리지 우선 순위 및 6바이트 MAC 주소로 구성됩니다.

확장 시스템 ID는 BPDU(Bridge Protocol Data Units)의 STP(Spanning Tree Protocol) 브리지 식별자 부분을 수정합니다. 원래 2바이트 우선순위 필드는 2개의 필드로 분할됩니다.4비트 브리지 우선순위 필드 및 VLAN 번호 매기기를 0-4095로 허용하는 12비트 시스템 ID 확장.

확장 시스템 ID가 확장 범위 VLAN을 활용하기 위해 Catalyst 스위치에서 활성화된 경우 동일한 STP 도메인 내의 모든 스위치에서 활성화해야 합니다.이는 모든 스위치에서 STP 루트 계산을 일관되게 유지하기 위해 필요합니다.확장 시스템 ID가 활성화되면 루트 브리지 우선순위는 4096과 VLAN ID의 배수가 됩니다.확장 시스템 ID가 없는 스위치는 브리지 ID를 더 세분화하여 선택하므로 실수로 루트를 클레임할 수 있습니다.

동일한 STP 도메인 내에서 일관된 확장 시스템 ID 컨피그레이션을 유지하는 것이 좋지만, STP 도메인에 64개의 MAC 주소가 있는 새 섀시를 도입할 때 모든 네트워크 장치에 확장 시스템 ID를 적용하는 것은 실용적이지 않습니다.그러나 확장 시스템 ID가 없는 시스템은 스패닝 트리 우선 순위가 더 높은 스패닝 트리 우선 순위를 사용하여 두 시스템을 구성하는 경우 이를 이해하는 것이 중요합니다.확장 시스템 ID 컨피그레이션을 활성화하려면 다음 명령을 실행합니다.

스패닝 트리 확장 시스템 ID

내부 VLAN은 VLAN 1006부터 오름차순으로 할당됩니다.사용자 VLAN과 내부 VLAN 간의 충돌을 방지하려면 가능한 한 사용자 VLAN을 VLAN 4094와 가깝게 할당하는 것이 좋습니다.내부적으로 할당된 VLAN을 표시하려면 스위치**에서 show vlan 내부 사용량**을 실행합니다.

```
Switch#show vlan internal usage

VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

네이티브 IOS에서 내부 VLAN이 내림차순으로 할당되도록 **vlan 내부 할당 정책**을 내림차순으로 구성할 수 있습니다.CatOS 소프트웨어에 해당하는 CLI는 공식적으로 지원되지 않습니다.

vlan 내부 할당 정책 내림차순

Cisco 구성 권장 사항

Catalyst 6500/6000이 VTP 서버 모드에 있을 때 VLAN을 생성할 수 있으며, VTP 도메인 이름 없이도 가능합니다.Cisco IOS 시스템 소프트웨어를 실행하는 Catalyst 6500/6000 스위치에서 VLAN을 구성하기 전에 먼저 VTP 도메인 이름을 구성합니다.이 순서대로 구성하면 CatOS를 실행하는 다른 Catalyst 스위치와의 일관성이 유지됩니다.

VTP 클라이언트/서버 모드 또는 VTP 모드를 사용할지 여부에 대한 구체적인 권장 사항은 없습니다.일부 고객은 이 섹션에서 언급하는 몇 가지 고려 사항에도 불구하고 VTP 클라이언트/서버 모드를 손쉽게 관리할 수 있는 방법을 선호합니다.이중화를 위해 각 도메인에 2개의 서버 모드 스위치(일반적으로 2개의 디스트리뷰션 레이어 스위치)를 두는 것이 좋습니다.도메인의 나머지 스위치를 클라이언트 모드로 설정합니다.VTPv2를 사용하여 클라이언트/서버 모드를 구현할 때 동일한 VTP 도메인에서 항상 더 높은 개정 번호가 허용된다는 점을 기억하십시오.VTP 클라이언트 또는 서버 모드에서 구성된 스위치가 VTP 도메인에 도입되고 있는 VTP 서버보다 더 높은 수정 번호가 있는 경우 VTP 도메인 내의 VLAN 데이터베이스를 덮어씁니다.컨피그레이션 변경이 의도치 않게 변경되고 VLAN이 삭제되는 경우 이 덮어쓰면 네트워크에서 심각한 중단이 발생할 수 있습니다.클라이언트 또는 서버 스위치에 항상 서버의 구성 수정 버전 번호보다 낮은 구성 수정 번호가 있는지 확인하려면 클라이언트 VTP 도메인 이름을 표준 이름이 아닌 다른 이름으로 변경한 다음 다시 표준으로 돌아갑니다.이 작업은 클라이언트의 컨피그레이션 개정을 0으로 설정합니다.

네트워크에서 쉽게 변경할 수 있는 VTP 기능에 대한 장단점이 있습니다.많은 기업에서 신중한 접근 방식을 선호하며 다음과 같은 이유로 VTP 모드를 사용합니다.

- 스위치나 트렁크 포트에서 VLAN을 수정해야 하는 요구 사항은 한 번에 하나의 스위치로 간주해야 하므로 이러한 관행은 변경 제어가 효율적입니다.
- VTP 투명 모드는 VLAN의 실수로 삭제와 같은 관리자 오류의 위험을 제한합니다.이러한 오류

는 전체 도메인에 영향을 미칠 수 있습니다.
- 트렁크에서 VLAN에 포트가 없는 스위치로 VLAN을 정리할 수 있습니다.이로 인해 프레임 플러딩이 발생하여 대역폭 효율성이 향상됩니다.수동 정리 시 스패닝 트리 지름이 감소합니다.자세한 내용은 Dynamic Trunking Protocol 섹션을 참조하십시오.스위치당 VLAN 컨피그레이션도 이러한 방식을 권장합니다.
- 전체 도메인 VLAN 컨피그레이션을 덮어쓰는 더 높은 VTP 개정 번호를 사용하여 새 스위치의 네트워크에 도입될 위험은 없습니다.
- Cisco IOS Software VTP 투명 모드는 CiscoWorks2000의 일부인 Campus Manager 3.2에서 지원됩니다. VTP 도메인에 하나 이상의 서버가 있어야 하는 이전 제한 사항이 제거되었습니다.

VTP 명령	설명
vtp 도메인 *이름*	CDP는 도메인 간의 케이블 연결을 방지하기 위해 이름을 확인합니다.도메인 이름은 대/소문자를 구분합니다.
vtp 모드 {서버 | 클라이언트 | 투명}	VTP는 세 가지 모드 중 하나로 작동합니다.
vlan *vlan_number*	이렇게 하면 제공된 ID가 있는 VLAN이 생성됩니다.
switchport trunk allowed vlan_*range*	이 명령은 트렁크가 필요한 경우 VLAN을 전달할 수 있도록 하는 interface 명령입니다.기본값은 모든 VLAN입니다.
switchport trunk pruning vlan_*range*	이 명령은 VLAN이 없는 디스트리뷰션 레이어에서 액세스 레이어로의 트렁크와 같은 수동 정리로 STP 지름을 제한하는 인터페이스 명령입니다.기본적으로 모든 VLAN은 prune-eligible입니다.

기타 옵션

VTPv2는 클라이언트/서버 모드를 사용하는 토큰 링 환경의 요구 사항입니다.

이 문서의 Cisco Configuration Recommendation 섹션에서는 불필요한 프레임 플러딩을 줄이기 위해 VLAN을 제거함으로써 얻을 수 있는 이점을 설명합니다.vtp **pruning** 명령은 VLAN을 자동으로 삭제하여 필요 없는 프레임의 비효율적인 플러딩을 중지합니다.

참고: 수동 VLAN 정리와 달리 자동 정리는 스패닝 트리 지름을 제한하지 않습니다.

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 허용합니다.그러나 GVRP는 이 문서의 범위를 벗어납니다.

참고: Cisco IOS Software에는 VTP off 모드 기능이 없으며, VTPv1 및 VTPv2만 정리가 포함된 것을 지원합니다.

고속 이더넷 자동 협상

목적

자동 협상은 IEEE 802.3u FE(Fast Ethernet) 표준의 선택적 기능입니다.자동 협상을 사용하면 디바이스에서 링크를 통해 속도 및 듀플렉스 기능에 대한 정보를 자동으로 교환할 수 있습니다.자동 협상은 레이어 1(L1)에서 작동합니다. 이 기능은 임시 사용자 또는 디바이스가 네트워크에 연결되는 영역에 할당된 포트를 대상으로 합니다.액세스 레이어 스위치 및 허브를 예로 들 수 있습니다.

운영 개요

Autonegotiation에서는 10BASE-T 디바이스에 대해 수정된 버전의 링크 무결성 테스트를 사용하여 속도를 협상하고 다른 자동 협상 매개변수를 교환합니다.원래 10BASE-T 링크 무결성 테스트는 NLP(Normal Link Pulse)라고 합니다. 10/100Mbps 자동 협상에 대한 링크 무결성 테스트의 수정된 버전을 FLP(Fast Link Pulse)라고 합니다. 10BASE-T 디바이스는 링크 무결성 테스트의 일부로 16(+/-8) 밀리초마다 버스트 펄스를 예상합니다.10/100Mbps 자동 협상을 위한 FLP는 16(+/-8) ms마다 이러한 버스트를 전송하며 62.5(+/-7) 마이크로초마다 추가 펄스를 보냅니다.버스트 시퀀스 내의 펄스는 링크 파트너 간의 호환성 교환에 사용되는 코드 단어를 생성합니다.

10BASE-T에서는 스테이션마다 링크 펄스가 전송됩니다.이것은 16밀리초마다 전송되는 단일 펄스입니다.또한 10BASE-T 디바이스는 링크가 유휴 상태일 때 16ms마다 링크 펄스를 전송합니다.이러한 링크 펄스는 하트비트 또는 NLP라고도 합니다.

100BASE-T 디바이스는 FLP를 전송합니다.이 맥박은 한 맥박이 아니라 파열로 보내진다.버스트는 2ms 이내에 완료되며 16ms마다 다시 반복됩니다.초기화 시 디바이스는 속도, 이중 및 흐름 제어 협상을 위해 링크 파트너에게 16비트 FLP 메시지를 전송합니다.이 16비트 메시지는 파트너가 메시지를 승인할 때까지 반복적으로 전송됩니다.

참고: IEEE 802.3u 사양에 따라 100Mbps 전이중 및 다른 링크 파트너와 함께 전이중 방식의 협상을 수동으로 구성할 수 없습니다.100Mbps 전이중 및 자동 협상을 위해 다른 링크 파트너를 구성하려고 하면 이중 불일치가 발생합니다.한 링크 파트너가 자동 협상을 수행하고 다른 링크 파트너의 자동 협상 매개변수를 볼 수 없기 때문에 이중 불일치가 발생합니다.첫 번째 링크 파트너는 기본적으로 반이중으로 설정됩니다.

모든 Catalyst 6500 이더넷 스위칭 모듈은 10/100Mbps 및 반이중 또는 전이중(full duplex)을 지원합니다.다른 Catalyst 스위치에서 이 기능을 확인하려면 **show interface capabilities** 명령을 실행합니다.

10/100Mbps 이더넷 링크의 가장 일반적인 원인 중 하나는 링크의 한 포트가 반이중으로 작동하는 반면 다른 포트는 전이중으로 작동하면 발생합니다.이러한 상황은 링크에서 하나 또는 두 포트를 모두 재설정하고 자동 협상 프로세스에서 두 링크 파트너에 대해 동일한 컨피그레이션을 수행하지 못할 때 종종 발생합니다.이러한 상황은 링크의 한 면을 재구성하고 다른 면을 재구성하는 것을 잊었을 때도 발생합니다.다음과 같은 경우 성능 관련 지원 전화를 걸 필요가 없습니다.

- 모든 비일시적 디바이스에 필요한 동작에 대해 포트 컨피그레이션이 필요한 정책 생성
- 적절한 변경 제어 조치로 정책 시행

성능 문제의 일반적인 증상은 스위치에서 FCS(Frame Check Sequence), CRC(Cyclic Redundancy Check), 정렬 또는 실행 카운터를 증가시킵니다.

반이중 모드에서는 수신 한 쌍과 송신 전선 한 쌍이 있습니다.두 전선을 동시에 사용할 수 없습니다.수신 쪽에 패킷이 있는 경우 디바이스는 전송할 수 없습니다.

전이중 모드에서는 수신 및 전송 와이어와 동일한 쌍이 있습니다.그러나 Carrier Sense 및 Collision Detect 기능이 비활성화되었으므로 두 기능을 동시에 사용할 수 있습니다.디바이스는 동시에 전송 및 수신할 수 있습니다.

따라서 반이중-전이중 연결은 작동하지만 반이중 측에는 많은 수의 충돌이 발생하여 성능이 저하됩니다.전이중으로 구성된 디바이스가 데이터를 수신하는 동시에 전송할 수 있기 때문에 충돌이 발생합니다.

이 목록의 문서는 자동 협상에 대해 자세히 설명합니다.이 문서에서는 자동 협상 작동 방식을 설명하고 다양한 구성 옵션에 대해 설명합니다.

- 이더넷 10/100/1000Mb 하프/풀 듀플렉스 자동 협상 구성 및 트러블슈팅
- Cisco Catalyst Switch와 NIC의 호환성 문제 트러블슈팅

자동 협상에 대한 일반적인 오해는 100Mbps 전이중 및 자동 전이중 협상을 다른 링크 파트너와 함께 수동으로 링크 파트너를 구성할 수 있다는 것입니다.실제로 이를 시도하면 듀플렉스 불일치가 발생합니다.따라서 하나의 링크 파트너가 autonegotiate를 수행하고, 다른 링크 파트너의 자동 협상 매개변수를 볼 수 없으며, 기본적으로 반이중으로 설정되어 있기 때문입니다.

대부분의 Catalyst 이더넷 모듈은 10/100Mbps 및 반이중/전이중 지원그러나 **show interface mod/*port* capabilities** 명령을 실행하면 이를 확인할 수 있습니다.

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.

far end fault는 한 스테이션에서 감지할 수 있는 링크의 오류이며 다른 스테이션은 감지할 수 없습니다.연결이 끊긴 송신 배선이 그 예입니다.이 예에서 전송 스테이션은 여전히 유효한 데이터를 수신하며 링크 무결성 모니터를 통해 링크가 정상임을 탐지합니다.그러나 전송 스테이션은 다른 스테이션에서 전송을 받지 않음을 감지할 수 없습니다.이러한 원격 결함을 탐지하는 100BASE-FX 스테이션은 인접 디바이스에 원격 결함을 알리기 위해 특수 비트 패턴을 전송하기 위해 전송된 IDLE 스트림을 수정할 수 있습니다.특수 비트 패턴을 FFI-IDLE 패턴이라고 합니다.FFI-IDLE 패턴은 이후에 원격 포트의 종료를 트리거합니다(errDisable). 결함 보호에 대한 자세한 내용은 이 문서의 단방향 링크 탐지 섹션을 참조하십시오.

이러한 모듈/하드웨어 지원 FFI:

- Catalyst 6500/6000 및 4500/4000:모든 100BASE-FX 모듈 및 GE 모듈

Cisco 인프라 포트 권장 사항

10/100Mbps 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(Network Interface Card) 또는 벤더 스위치가 정확하게 일치하지 않으면 문제가 발생할 수 있습니다.또한 10/100Mbps 자동 협상을 위한 IEEE 802.3u 사양에 설명되어 있지 않은 공급업체별 고급 기능은 하드웨어 비호환성 및 기타 문제를 야기할 수 있습니다.이러한 고급 기능 유형에는 자동 극성과 케이블 무결성이 포함됩니다.이 문서에서는 다음 예를 제공합니다.

- 필드 경고:CAT4K/6K에 연결하는 Intel Pro/1000T NIC의 성능 문제

경우에 따라 호스트, 포트 속도 및 듀플렉스를 설정해야 합니다.일반적으로 다음과 같은 기본 문제 해결 단계를 완료합니다.

- 자동 협상이 링크의 양쪽에서 구성되었는지 또는 양쪽 모두에서 하드 코딩이 구성되었는지 확인합니다.
- 릴리스 노트에서 일반적인 주의 사항을 확인합니다.
- 실행하는 NIC 드라이버 또는 운영 체제의 버전을 확인합니다.최신 드라이버 또는 패치가 필요한 경우가 많습니다.

일반적으로, 먼저 모든 유형의 링크 파트너에 대해 자동 협상을 사용합니다.랩톱과 같은 임시 장치에 대한 자동 협상 컨피그레이션의 구성에는 분명한 이점이 있습니다.자동 협상은 다른 디바이스에서도 잘 작동합니다. 예를 들면 다음과 같습니다.

- 서버 및 고정 워크스테이션과 같은 일시적이지 않은 장치 사용
- 스위치에서 스위치로
- 스위치에서 라우터로

그러나 이 섹션에서 언급하는 몇 가지 이유로 협상 문제가 발생할 수 있습니다.이러한 경우 기본적인 문제 해결 단계는 이더넷 10/100/1000Mb 반이중/전이중 자동 협상 구성 및 문제 해결을 참조하십시오.

자동 협상 비활성화:

- 스위치 및 라우터와 같은 네트워크 인프라 디바이스를 지원하는 포트
- 서버 및 프린터와 같은 기타 비일시적인 엔드 시스템

이러한 포트의 속도 및 듀플렉스 설정을 항상 하드 코딩하십시오.

일반적으로 100Mbps 전이중인 속도 및 듀플렉스를 위해 이러한 10/100Mbps 링크 구성을 수동으로 구성합니다.

- 스위치 간
- 서버 간 전환
- 스위치-라우터

10/100Mbps 이더넷 포트에서 포트 속도가 자동으로 설정되면 속도와 양방향은 모두 자동 협상을 수행합니다.포트를 auto로 설정하려면 이 interface 명령을 실행합니다.

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

속도 및 듀플렉스를 구성하려면 다음 interface 명령을 실행합니다.

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Cisco 액세스 포트 권장 사항

최종 사용자, 모바일 작업자 및 임시 호스트는 이러한 호스트의 관리를 최소화하기 위해 자동 협상이 필요합니다.Catalyst 스위치에서도 자동 협상을 수행할 수 있습니다.최신 NIC 드라이버가 필요한 경우가 많습니다.

포트의 속도 자동 협상을 활성화하려면 다음 전역 명령을 실행합니다.

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

참고: 10/100Mbps 이더넷 포트에서 포트 속도를 auto로 설정하면 속도와 듀플렉스가 모두 자동 협상됩니다.자동 협상 포트의 이중 모드는 변경할 수 없습니다.

NIC 또는 공급업체 스위치가 IEEE 사양 802.3u와 정확히 일치하지 않을 경우 문제가 발생할 수 있습니다.또한 10/100Mbps 자동 협상을 위한 IEEE 802.3u 사양에 설명되어 있지 않은 공급업체별 고급 기능은 하드웨어 비호환성 및 기타 문제를 야기할 수 있습니다.이러한 고급 기능에는 자동 극성과 케이블 무결성이 포함됩니다.

기타 옵션

스위치 간에 자동 협상이 비활성화되면 특정 문제에 대해 레이어 1 결함 표시도 손실될 수 있습니다.레이어 2 프로토콜을 사용하여 적극적인 UDLD와 같은 장애 감지 기능을 보완합니다.

자동 협상이 활성화된 경우에도 자동 협상은 이러한 상황을 탐지하지 않습니다.

- 포트가 중단되고 수신 또는 전송되지 않음
- 선의 한 쪽이 위로 올라갔지만 다른 쪽은 내려갔습니다
- 파이버 케이블이 연결되지 않음

이러한 문제는 물리적 레이어에 없기 때문에 자동 협상이 탐지되지 않습니다.이 문제는 STP 루프 또는 트래픽 블랙홀로 이어질 수 있습니다.

UDLD가 양쪽 끝에 구성된 경우 UDLD는 이러한 모든 사례를 탐지하고 링크의 두 포트를 모두 errdisable할 수 있습니다.이러한 방식으로 UDLD는 STP 루프와 트래픽 블랙홀을 방지합니다.

기가비트 이더넷 자동 협상

목적

기가비트 이더넷(GE)에는 10/100Mbps 이더넷(IEEE 802.3z)에 사용되는 절차보다 더 광범위한 자동 협상 절차가 있습니다. GE 포트를 사용하면 자동 협상을 사용하여 다음을 교환할 수 있습니다.

- 플로우 제어 매개변수
- 원격 장애 정보
- 이중 정보**참고:** Catalyst 시리즈 GE 포트는 전이중 모드만 지원합니다.

IEEE 802.3z는 IEEE 802.3:2000 사양으로 대체되었습니다.자세한 내용은 Local and Metropolitan Area Networks + Draft(LAN/MAN 802s) Standards Subscription 을 참조하십시오.

운영 개요

10/100Mbps FE의 자동 협상과는 달리 GE 자동 협상은 포트 속도 협상을 포함하지 않습니다.또한 autonegotiation을 비활성화하려면 set **port speed** 명령을 실행할 수 없습니다.GE 포트 협상은 기본적으로 활성화되며, GE 링크의 양쪽 끝에 있는 포트는 동일한 설정을 가져야 합니다.링크의 각 끝에 있는 포트가 비일관성 있게 설정되어 있으면 링크가 나타나지 않습니다. 즉, 교환된 매개변수가 다릅니다.

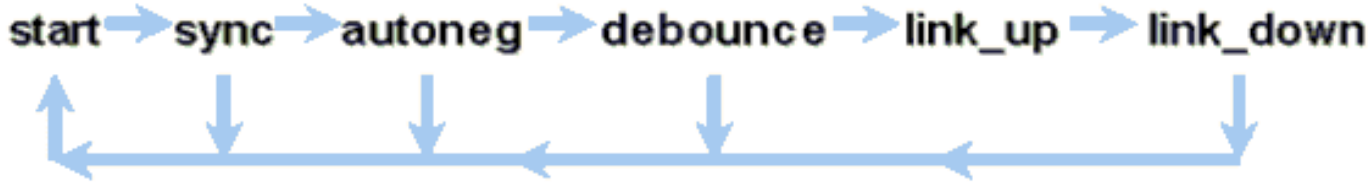
예를 들어, A와 B라는 두 개의 디바이스가 있다고 가정합니다. 각 디바이스는 자동 협상을 활성화하거나 비활성화할 수 있습니다.가능한 컨피그레이션 및 해당 링크 상태가 있는 테이블입니다.

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 동기화 실패 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 협상을 비활성화하면 autonegotiation 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: 그러나 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.**sync-restart-delay** 명령은 autonegotiation이 enable로 설정된 경우에만 적용됩니다.

Cisco 인프라 포트 권장 사항

자동 협상 구성은 10/100Mbps 환경보다 GE 환경에서 훨씬 더 중요합니다.다음 상황에서는 자동 협상을 비활성화만 합니다.

- 협상을 지원할 수 없는 디바이스에 연결되는 스위치 포트에서
- 상호 운용성 문제로 인해 연결 문제가 발생하는 경우

모든 스위치 간 링크 및 일반적으로 모든 GE 디바이스에서 기가비트 협상을 활성화합니다.기가비트 인터페이스의 기본값은 자동 협상입니다.여전히 autonegotiation이 활성화되도록 하려면 다음

명령을 실행합니다.

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

한 가지 알려진 예외는 플로우 제어 및 자동 협상을 추가한 릴리스인 Cisco IOS Software Release 12.0(10)S 이전의 Cisco IOS Software를 실행하는 GSR(Gigabit Switch Router)에 연결하는 경우입니다.이 경우 두 기능을 끕니다.이러한 기능을 끄지 않으면 스위치 포트가 연결되지 않은 것을 보고하고 GSR이 오류를 보고합니다.다음은 샘플 인터페이스 명령 시퀀스입니다.

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

Cisco 액세스 포트 권장 사항

FLP는 벤더에 따라 다를 수 있으므로 사례별로 서버 간 연결을 확인해야 합니다.Cisco 고객은 Sun, HP 및 IBM 서버에서 기가비트 협상을 하는 데 몇 가지 문제가 있었습니다.NIC 공급업체가 특별히 달리 명시하지 않는 한 모든 디바이스에서 기가비트 자동 협상을 사용하도록 합니다.

기타 옵션

흐름 제어는 802.3x 사양의 선택적 부분입니다.흐름 제어를 사용하는 경우 협상해야 합니다.디바이스는 PAUSE 프레임(잘 알려진 MAC 01-80-C2-00-00-00 0F)을 전송 및/또는 응답할 수 있거나 그럴 수 없습니다. 또한 디바이스는 원엔드 네이버의 흐름 제어 요청에 동의할 수 없습니다.입력 버퍼가 가득 찬 포트는 링크 파트너에게 PAUSE 프레임을 전송합니다.링크 파트너는 전송을 중지하고 링크 파트너 출력 버퍼에 추가 프레임을 보관합니다.이 기능은 정상 상태 초과 등록 문제를 해결하지 않습니다.그러나 이 기능은 부스트 전반에 걸쳐 파트너 출력 버퍼의 일부분의 일부만으로도 입력 버퍼를 효과적으로 증가시킵니다.

PAUSE 기능은 단기 일시적인 트래픽 오버로드로 인해 발생하는 버퍼 오버플로 조건 때문에 디바이스(스위치, 라우터 또는 엔드 스테이션)에서 수신한 프레임을 불필요한 폐기하지 않도록 설계되었습니다.트래픽 오버로드 중인 디바이스는 디바이스가 PAUSE 프레임을 전송할 때 내부 버퍼 오버플로를 방지합니다.PAUSE 프레임에는 파트너가 더 많은 데이터 프레임을 전송하기 전에 전이중 파트너가 대기하는 시간을 나타내는 매개 변수가 포함되어 있습니다.PAUSE 프레임을 수신하는 파트너는 지정된 기간 동안 데이터를 보내지 않습니다.이 타이머가 만료되면 스테이션에서 다시 데이터 프레임을 전송하기 시작합니다.

PAUSE를 실행하는 스테이션은 0시간의 매개 변수를 포함하는 다른 PAUSE 프레임을 실행할 수 있습니다.이 작업은 일시 중지 기간의 나머지 기간을 취소합니다.따라서 새로 받은 PAUSE 프레임은 현재 진행 중인 PAUSE 작업을 재정의합니다.또한 PAUSE 프레임을 실행하는 스테이션은 PAUSE 기간을 연장할 수 있습니다.스테이션은 첫 번째 PAUSE 기간이 만료되기 전에 0이 아닌 시간 매개 변수가 포함된 다른 PAUSE 프레임을 실행합니다.

이 PAUSE 작업은 속도 기반 흐름 제어가 아닙니다.이 작업은 트래픽의 디바이스, 즉 PAUSE 프레임을 전송한 디바이스, 버퍼 혼잡을 줄일 수 있는 간단한 시작 중지 메커니즘입니다.

이 기능을 가장 잘 사용하는 방법은 액세스 포트와 엔드 호스트 간의 링크입니다. 여기서 호스트 출력 버퍼는 가상 메모리만큼 커질 수 있습니다.스위치 간 사용은 이점이 제한적입니다.

스위치 포트에서 이 명령을 제어하려면 다음 interface 명령을 실행합니다.

```
flowcontrol {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 및 WS-X4306)은 차단 기능이 없으므로 일시 중지 프레임을 전송하지 않습니다.

동적 트렁킹 프로토콜

목적

디바이스 간에 VLAN을 확장하기 위해 트렁크는 원래 이더넷 프레임을 일시적으로 식별하고 표시(링크 로컬)합니다.이 작업을 수행하면 단일 링크를 통해 프레임을 멀티플렉싱할 수 있습니다.또한 스위치 간에 별도의 VLAN 브로드캐스트 및 보안 도메인이 유지되도록 합니다.CAM 테이블은 스위치 내에서 프레임을 VLAN에 매핑합니다.

운영 개요

DTP는 2세대 DISL(Dynamic ISL)입니다.DISL만 지원되는 ISL입니다.DTP는 ISL 및 802.1Q를 모두 지원합니다.이러한 지원을 통해 트렁크의 양쪽 끝에 있는 스위치가 서로 다른 트렁킹 프레임 매개변수에 동의하게 됩니다.이러한 매개변수는 다음과 같습니다.

- 구성된 캡슐화 유형
- 네이티브 VLAN
- 하드웨어 기능

또한 DTP 지원은 비 트렁크 포트로 태그된 프레임이 플러딩되는 것을 방지하는 데 도움이 되며, 이는 잠재적으로 심각한 보안 위험입니다.DTP는 포트와 인접 디바이스가 일관된 상태를 유지하도록 보장하므로 이러한 홍수를 방지합니다.

트렁킹 모드

DTP는 스위치 포트와 인접 디바이스 간에 컨피그레이션 매개변수를 협상하는 레이어 2 프로토콜입니다.DTP는 다른 잘 알려진 멀티캐스트 MAC 주소 01-00-0c-cc-cc-cc 및 SNAP 프로토콜 유형 0x2004를 사용합니다. 이 표에서는 가능한 각 DTP 협상 모드의 기능에 대해 설명합니다.

모드	함수	전송된 DTP 프레임	최종 상태(로컬 포트)
(CatO	포트가 링크를 트렁크로 변환할 수 있도록 합니다.인접 포	예, 주기적	

S의 모드 Auto 와 동일)	트가 on 또는 모드로 설정된 경우 포트는 트렁크 포트 됩니다.		
(CatOS에서 ON 모드와 동일)	포트를 영구 모드로 설정하고 링크를 트렁크로 변환하기 위해 협상합니다.인접 포트가 변경에 동의하지 않더라도 포트는 트렁크 포트가 됩니다.	예, 주기적	Trunking, 조건 없이
	포트를 영구 모드로 설정하지만 포트가 DTP 프레임을 생성하는 것을 허용하지 않습니다.트렁크 링크를 설정하려면 인접 포트를 트렁크 포트로 수동으로 구성해야 합니다.이는 DTP를 지원하지 않는 디바이스에 유용합니다.	아니요	Trunking, 조건 없이
(CatOS 비교 가능한 명령은)	포트가 링크를 트렁크 링크로 변환하려고 적극적으로 시도합니다.인접 포트가 on, 또는 모드 설정된 경우 포트는 트렁크 포트가 됩니다.	예, 주기적	원격 모드가 있거나 또는 경우에만 트렁킹 상태로 .
	포트를 영구 모드로 설정하고 링크를 비트렁크 링크로 변환하도록 협상합니다.인접 포트가 변경에 동의하지 않더라도 포트는 트렁크가 아닌 포트가 됩니다.	아니요, 안정된 상태이지만, 변경 후 원격 엔드 탐지를 가속화하기 위해 알림이 .	

참고: ISL 및 802.1Q 캡슐화 유형을 설정하거나 협상할 수 있습니다.

기본 컨피그레이션에서 DTP는 링크에서 다음 특성을 가정합니다.

- 포인트 투 포인트 연결 및 Cisco 디바이스는 포인트 투 포인트만 있는 802.1Q 트렁크 포트를 지원합니다.
- DTP 협상 과정에서 포트는 STP에 참여하지 않습니다.포트 유형이 다음 세 가지 유형 중 하나가 된 후에만 포트가 STP에 추가됩니다.액세스ISL802.1qPAgP는 포트가 STP에 참여하기 전에 실행해야 하는 다음 프로세스입니다.PAgP는 EtherChannel 자동화에 사용됩니다.
- VLAN 1은 항상 트렁크 포트에 있습니다.포트가 ISL 모드에서 트렁킹되는 경우 DTP 패킷은 VLAN 1에서 전송됩니다. 포트가 ISL 모드에서 트렁킹되지 않는 경우 DTP 패킷은 네이티브 VLAN에서 전송됩니다(802.1Q 트렁킹 또는 트렁킹 없음 포트의 경우).
- DTP 패킷은 VTP 도메인 이름과 트렁크 컨피그레이션 및 관리 상태를 전송합니다.협상된 트렁크가 작동하려면 VTP 도메인 이름이 일치해야 합니다.이러한 패킷은 협상 내내 1초마다 전송

되고 협상 후 30초마다 전송됩니다. 또는 모드의 포트가 5분(분) 내에 DTP 패킷을 탐지하지 못하면 포트가 비트렁크로 설정됩니다.

주의: 모드 , 및 포트가 종료되는 상태를 명시적으로 지정한다는 것을 이해해야 합니다.구성이 잘못되면 한 쪽이 트렁킹을 하고 다른 쪽은 트렁킹을 하지 않는 위험/일관성 없는 상태가 될 수 있습니다.

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.

캡슐화 유형

ISL 운영 개요

ISL은 Cisco 전용 트렁킹 프로토콜(VLAN 태깅 체계)입니다.ISL은 오랫동안 사용되고 있습니다.반면 802.1Q는 훨씬 최신 버전이지만 802.1Q는 IEEE 표준입니다.

ISL은 원래 프레임을 2 레벨 태깅 구성으로 완전히 캡슐화합니다.이러한 방식으로 ISL은 터널링 프로토콜이며 추가적인 이점으로 이더넷 이외의 프레임을 전달합니다.ISL은 표준 이더넷 프레임에 26바이트 헤더와 4바이트 FCS를 추가합니다.트렁크로 구성된 포트는 더 큰 이더넷 프레임을 기대하고 처리합니다.ISL은 1024개의 VLAN을 지원합니다.

프레임 형식 - ISL 태그가 음영처리됩니다.

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

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

802.1Q 운영 개요

IEEE 802.1Q 표준은 이더넷에만 해당되지만, 표준은 캡슐화 유형보다 훨씬 더 많은 것을 지정합니

다.802.1Q에는 다른 GARP(Generic Attribute Registration Protocols), 스패닝 트리 개선 사항 및 802.1p QoS 태깅이 포함됩니다.자세한 내용은 IEEE Standards Online 을 참조하십시오.

802.1Q 프레임 형식은 원래 이더넷 SA 및 DA를 유지합니다.그러나 이제 스위치는 호스트가 QoS 시그널링을 위해 802.1p 사용자 우선 순위를 express로 표시하기 위해 태깅을 사용할 수 있는 액세스 포트에서도 대형 소형 프레임을 수신해야 합니다.태그는 4바이트입니다.802.1Q 이더넷 v2 프레임은 1522바이트이며, 이는 IEEE 802.3ac 작업 그룹 성과입니다.또한 802.1Q는 4096 VLAN의 번호 지정 공간을 지원합니다.

전송 및 수신된 모든 데이터 프레임은 네이티브 VLAN에 있는 데이터 프레임을 제외하고 802.1Q 태그가 지정됩니다.이 경우 인그레스 스위치 포트 컨피그레이션을 기반으로 하는 암시적 태그가 있습니다.네이티브 VLAN의 프레임은 항상 태그가 지정되지 않은 상태로 전송되며 일반적으로 태그가 지정되지 않은 상태로 수신됩니다.그러나 이러한 프레임은 태깅될 수도 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- VLAN 상호 운용성
- 802.1q 캡슐화를 사용하는 Catalyst 4500/4000, 5500/5000 및 6500/6000 Series 스위치 간 트렁킹(Cisco CatOS 시스템 소프트웨어 사용)

802.1Q/802.1p 프레임 형식

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Cisco 구성 권장 사항

Cisco의 주요 설계 원칙은 일관성이 가능한 네트워크에서 일관성을 유지하기 위해 노력하는 것입니다.모든 최신 Catalyst 제품은 802.1Q를 지원하며, 일부 Catalyst 4500/4000 및 Catalyst 6500 시리즈의 이전 모듈과 같이 802.1Q만 지원합니다.따라서 모든 새로운 구현은 이 IEEE 802.1Q 표준 및 이전 네트워크를 따라야 하며 ISL에서 점진적으로 마이그레이션해야 합니다.

특정 포트에서 802.1Q 트렁킹을 활성화하려면 이 interface 명령을 실행합니다.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

IEEE 표준은 공급업체 상호 운용성을 허용합니다.새로운 호스트 802.1p 지원 NIC 및 장치를 사용할 수 있게 됨에 따라 모든 Cisco 환경에서 공급업체 상호 운용성이 유리합니다.ISL과 802.1Q 구현은 모두 견고하지만, IEEE 표준은 궁극적으로 현장 노출 및 네트워크 분석 지원을 포함한 타사 지원 기능이 더 뛰어납니다.또한 802.1Q 표준은 ISL보다 캡슐화 오버헤드가 낮다는 점도 약간 고려해야 합니다.

완전성을 위해 네이티브 VLAN에 대한 암시적 태깅은 보안 고려 사항을 생성합니다.라우터 없이 한 VLAN, VLAN X에서 다른 VLAN, VLAN Y로 프레임을 전송할 수 있습니다.소스 포트(VLAN X)가 동일한 스위치에 있는 802.1Q 트렁크의 네이티브 VLAN과 동일한 VLAN에 있는 경우 라우터 없이 전송이 발생할 수 있습니다.해결 방법은 트렁크의 네이티브 VLAN에 더미 VLAN을 사용하는 것입니다.

특정 포트에서 802.1Q 트렁킹을 위한 VLAN을 네이티브(기본값)로 설정하려면 다음 interface 명령을 실행합니다.

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

모든 최신 하드웨어는 802.1Q를 지원하므로 모든 새로운 구현이 IEEE 802.1Q 표준을 따르고 ISL에서 이전 네트워크를 점진적으로 마이그레이션합니다.최근까지 많은 Catalyst 4500/4000 모듈은 ISL을 지원하지 않았습니다.따라서 802.1Q는 이더넷 트렁킹에 대한 유일한 옵션입니다.show interface capabilities 명령의 출력 또는 CatOS의 **show port capabilities** 명령을 참조하십시오.트렁킹 지원에는 적절한 하드웨어가 필요하므로 802.1Q를 지원하지 않는 모듈은 802.1Q를 지원할 수 없습니다.소프트웨어 업그레이드는 802.1Q를 지원하지 않습니다.Catalyst 6500/6000 및 Catalyst 4500/4000 스위치의 대부분의 새로운 하드웨어는 ISL 및 802.1Q를 모두 지원합니다.

트렁크에서 VLAN 1이 지워진 경우 스위치 관리 인터페이스 및 네이티브 VLAN 섹션에 설명되어 있지만 사용자 데이터는 전송되거나 수신되지 않지만 NMP는 VLAN 1에서 제어 프로토콜을 계속 전달합니다. 제어 프로토콜의 예로는 CDP 및 VTP가 있습니다.

또한 VLAN 1 섹션에 대해 설명하면 트렁킹 시 항상 VLAN 1에서 CDP, VTP 및 PAgP 패킷이 전송됩니다.dot1q(802.1Q) 캡슐화를 사용하면 스위치 네이티브 VLAN이 변경되면 이러한 제어 프레임에는 VLAN 1로 태그가 지정됩니다.dot1q를 라우터로 트렁킹하고 스위치에서 네이티브 VLAN이 변경된 경우, 태그가 지정된 CDP 프레임을 수신하고 라우터에서 CDP 네이버 가시성을 제공하려면 VLAN 1의 하위 인터페이스가 필요합니다.

참고: 네이티브 VLAN의 암시적 태깅으로 인해 발생하는 dot1q의 잠재적인 보안 고려 사항이 있습니다.라우터 없이 한 VLAN에서 다른 VLAN으로 프레임을 전송할 수 있습니다.자세한 내용은 침입 탐지 FAQ 를 참조하십시오.해결 방법은 최종 사용자 액세스에 사용되지 않는 트렁크의 네이티브 VLAN에 VLAN ID를 사용하는 것입니다.이를 위해 대부분의 Cisco 고객은 VLAN 1을 트렁크에 기본 VLAN으로 남겨 두고 액세스 포트를 VLAN 1 이외의 VLAN에 할당하기만 하면 됩니다.

Cisco는 양쪽 끝에 으로 명시적 트렁크 모드 컨피그레이션을 권장합니다.이 모드는 기본 모드입니다.이 모드에서는 네트워크 운영자가 syslog 및 명령줄 상태 메시지를 신뢰하여 포트가 및 트렁킹 속할 수 있습니다.이 모드는 on 모드와 다릅니다. 이는 인접 디바이스가 잘못 구성되었더라도 포트를 표시할 수 있습니다.또한 모드 트렁크는 링크의 한 쪽이 트렁크가 될 수 없거나 상태를 삭제할 수 없는 상황에서 안정성을 제공합니다.

DTP를 사용하여 스위치 간에 캡슐화 유형을 협상하고 양쪽 모두 지원하는 경우 기본적으로 ISL이 승자로 선택되어 있는 경우 dot1q[1]을 지정하려면 이 interface 명령을 실행해야 합니다.

```
switchport trunk encapsulation dot1q
```

[1] WS-X6548-GE-TX 및 WS-X6148-GE-TX가 포함된 특정 모듈은 ISL 트렁킹을 지원하지 않습니다 .이러한 모듈에서는 명령 switchport trunk encapsulation *dot1q*를 허용하지 않습니다.

참고: 포트에서 트렁크를 비활성화하려면 switchport **mode access** 명령을 실행합니다.이렇게 비활성화하면 호스트 포트가 가동될 때 낭비되는 협상 시간을 없앨 수 있습니다.

```
Switch(config-if)#switchport host
```

기타 옵션

또 다른 일반적인 고객 컨피그레이션은 디스트리뷰션 레이어에서 모드 및 액세스 레이어에서 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.비협상 모드를 사용하여 조건 없이 이러한 디바이스로 트렁킹하도록 포트를 설정할 수 있습니다.이 모드는 캠퍼스 전체의 공통 설정을 표준화하는 데 도움이 됩니다.

Cisco IOS 라우터 연결할 때 비협상을 권장합니다.브리징 과정에서 스위치 포트 **모드 트렁크**로 구성된 포트에서 수신되는 일부 DTP 프레임은 트렁크 포트로 돌아갈 수 있습니다.DTP 프레임을 수신하면 스위치 포트가 불필요하게 재협상하려고 시도합니다.재협상하기 위해 스위치 포트가 트렁크를 후 합니다.nonegotiate가 활성화된 경우 스위치는 DTP 프레임을 전송하지 않습니다.

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

스패닝 트리 프로토콜

목적

스패닝 트리는 이중화 스위치 및 브리지 네트워크에서 루프 프리 레이어 2 환경을 유지합니다 .STP가 없으면 프레임 루프 및/또는 무한대로 곱합니다.트래픽이 높으면 브로드캐스트 도메인의 모든 디바이스가 중단되므로 네트워크 용해가 발생합니다.

어떤 면에서 STP는 느린 소프트웨어 기반 브리지 사양(IEEE 802.1D)을 위해 처음 개발된 초기 프로토콜입니다. 그러나 STP는 다음 기능을 갖춘 대규모 스위치드 네트워크에서 성공적으로 구현하기 위해 복잡할 수 있습니다.

- 많은 VLAN
- 도메인에 있는 많은 스위치
- 멀티벤더 지원
- 새로운 IEEE 개선 사항

Cisco IOS System Software는 새로운 STP 개발을 시작했습니다.802.1w Rapid STP 및 802.1s Multiple Spanning Tree 프로토콜을 포함하는 새로운 IEEE 표준은 신속한 통합, 로드 공유 및 컨트롤 플레인 확장을 제공합니다.또한 RootGuard, BPDU 필터링, Portfast BPDU 가드 및 Loopguard와 같은 STP 개선 기능을 통해 레이어 2 포워딩 루프를 추가로 보호합니다.

PVST+ 운영 개요

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

처음에 BPDU는 모든 스위치에서 전송되며 각 스위치의 BID와 해당 스위치에 도달하기 위한 경로 비용이 포함됩니다.이렇게 하면 루트 브리지 및 루트에 대한 가장 저렴한 경로를 결정할 수 있습니다.루트에서 BPDU에 전달되는 추가 컨피그레이션 매개변수는 전체 네트워크에서 일관된 타이머를 사용하도록 로컬로 구성된 매개변수를 재정의합니다.스위치가 루트에서 수신하는 모든 BPDU에 대해 Catalyst central NMP는 새 BPDU를 처리하고 루트 정보로 전송합니다.

그런 다음 토폴로지는 다음 단계를 통해 통합됩니다.

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

자세한 내용은 다음 문서를 참조하십시오.

- STP 및 IEEE 802.1s MST 구성
- 빠른 스패닝 트리 프로토콜의 이해(802.1w)

기본 타이머 기본값	이름	함수
2초	안녕하세요?	BPDU의 발신을 제어합니다.
15초	전달 지연(Fwddelay)	포트가 상태 및 상태에 소요하는 시간을 제어하고 토폴로지 변경 프로세스에 영향을 줍니다.
20초	최대	스위치가 대체 경로를 찾기 전에 현재 토폴로지를 유지하는 시간을 제어합니다.최대 에이징(maxage) 시간이 지나면 BPDU가 오래된 것으로 간주되고 스위치가 차단 포트 풀에서 새 루트 포트를 찾습니다.차단된 포트를 사용할 수 없는 경우, 스위치는 지정된

		포트의 루트 자체라고 주장합니다.

Cisco에서는 타이머를 변경하지 않는 것이 좋습니다. 타이머가 안정성에 부정적인 영향을 미칠 수 있기 때문입니다.구축된 대부분의 네트워크는 조정되지 않습니다.명령줄(예: hello-interval, maxage 등)을 통해 액세스할 수 있는 단순 STP 타이머는 다른 가정 및 내장 타이머의 복잡한 집합으로 구성됩니다.따라서 타이머를 조정하고 모든 결과를 고려하기는 어렵습니다.또한 UDLD 보호를 손상시킬 수 있습니다.자세한 내용은 UniDirectional Link Detection 섹션을 참조하십시오.

STP 타이머에 대한 참고 사항:

기본 STP 타이머 값은 7개의 스위치(루트에서 네트워크 에지까지 7개의 스위치 홉으로 전환)의 네트워크 지름을 고려하는 계산과 BPDU가 루트 브리지에서 네트워크의 에지 스위치로 이동하는 데 필요한 시간(7홉까지)을 기반으로 합니다.이 가정은 대부분의 네트워크에서 허용되는 타이머 값을 계산합니다.그러나 네트워크 토폴로지 변경 전반에 걸쳐 컨버전스 시간을 단축하기 위해 이러한 타이머를 보다 최적의 값으로 변경할 수 있습니다.

특정 VLAN에 대한 네트워크 지름을 사용하여 루트 브리지를 구성할 수 있으며 그에 따라 타이머 값이 계산됩니다.변경해야 하는 경우 VLAN의 루트 브리지에서 지름 및 선택적인 hello 시간 매개변수만 구성하는 것이 좋습니다.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

이 매크로는 지정된 VLAN의 스위치 루트를 만들고, 지정된 지름 및 hello 시간을 기준으로 새 타이머 값을 계산하고, 구성 BPDU의 이 정보를 토폴로지의 다른 모든 스위치에 전파합니다.

새 포트 상태 및 포트 역할 섹션에서는 802.1D STP에 대해 설명하고 802.1D STP와 RSTP(Rapid STP)를 비교하고 비교합니다. RSTP에 대한 자세한 내용은 802.1w(Rapid Spanning Tree Protocol) 이해를 참조하십시오.

새 포트 상태 및 포트 역할

802.1D는 다음과 같은 네 가지 포트 상태로 정의됩니다.

- 수신
- 학습
- 차단
- 전달

자세한 내용은 포트 상태 섹션의 표를 참조하십시오.포트의 상태는 활성 토폴로지(루트 포트, 지정 포트 등)에서 포트가 수행하는 역할처럼(트래픽을 차단하거나 포워딩하는지 여부) 혼합됩니다. 예를 들어, 운영 관점에서 볼 때, 차단 상태의 포트와 수신 대기 상태의 포트 간에는 차이가 없습니다.둘 다 프레임을 폐기하고 MAC 주소를 학습하지 않습니다.실제 차이점은 스패닝 트리가 포트에 할당하는 역할입니다.수신 대기 포트가 지정 또는 루트로 지정되고 전달 상태로 이동하는 중이라고 가정할 수 있습니다.그러나 포트가 포워딩 상태에 있으면 포트 상태가 루트 또는 지정인지 알 수 없습니다.이 상태 기반 용어 실패를 보여줍니다.RSTP는 포트의 역할과 상태를 분리하므로 RSTP는 이 오류를 해결합니다.

포트 상태

STP 802.1D의 포트 상태

포트 상태	의미	다음 상태에 대한 기본 시간
	관리적으로 다운되었습니다.	
	BPDU를 수신하고 사용자 데이터를 중지합니다.	BPDU의 수신 모니터링직접/로컬 링크 장애가 탐지되면 최대 기간 만료 또는 즉각적인 변경 대기 20초
	BPDU를 전송하거나 수신하여 차단이 필요한지 여부를 확인합니다.	15초 Fwddelay를 기다립니다.
	토폴로지/CAM 테이블을 작성합니다.	15초 Fwddelay를 기다립니다.
	데이터를 전송/수신합니다.	

기본 토폴로지 변경의 총 수는 다음과 같습니다.

- 20 + 2(15) = 50초(최대 만료 대기 중)
- 직접 링크 장애 시 30초

RSTP에 남아 있는 포트 상태는 세 가지 가능한 작동 상태에 해당합니다.802.1D 상태는 비활성화됨, 차단 및 수신 거부가 고유한 802.1w 폐기 상태로 병합되었습니다.

STP(802.1D) 포트 상태	RSTP(802.1w) 포트 상태	포트가 활성 토폴로지에 포함되어 있습니까?	포트 학습 MAC 주소입니까?
비활성화됨	취소	아니요	아니요
차단	취소	아니요	아니요
수신	취소	예	아니요
학습	학습	예	예
전달	전달	예	예

포트 역할

이제 역할은 지정된 포트에 할당된 변수입니다.루트 포트 및 지정된 포트 역할은 그대로 유지되지만 차단 포트 역할은 이제 백업 및 대체 포트 역할로 분할됩니다.STA(spanning tree algorithm)는 BPDU를 기반으로 포트의 역할을 결정합니다.BPDU에 대한 이 점을 기억하십시오.두 개의 BPDU를 비교하고 다른 BPDU보다 더 유용한지 결정할 수 있는 방법은 항상 있습니다.결정 기준은 BPDU에 저장되는 값과 BPDU가 수신되는 포트입니다.이 섹션의 나머지 부분에서는 포트 역할에 대한 매우 실용적인 접근 방식을 설명합니다.

루트 포트 역할

브리지에서 최상의 BPDU를 수신하는 포트는 루트 포트입니다.이는 경로 비용 측면에서 루트 브리지에 가장 가까운 포트입니다.STA는 전체 브리지 네트워크(VLAN당)에서 단일 루트 브리지를 선택

합니다. 루트 브리지는 다른 브리지가 전송할 수 있는 것보다 더 유용한 BPDU를 전송합니다.루트 브리지는 루트 포트가 없는 네트워크에서의 유일한 브리지입니다.다른 모든 브리지는 하나 이상의 포트에서 BPDU를 수신합니다.

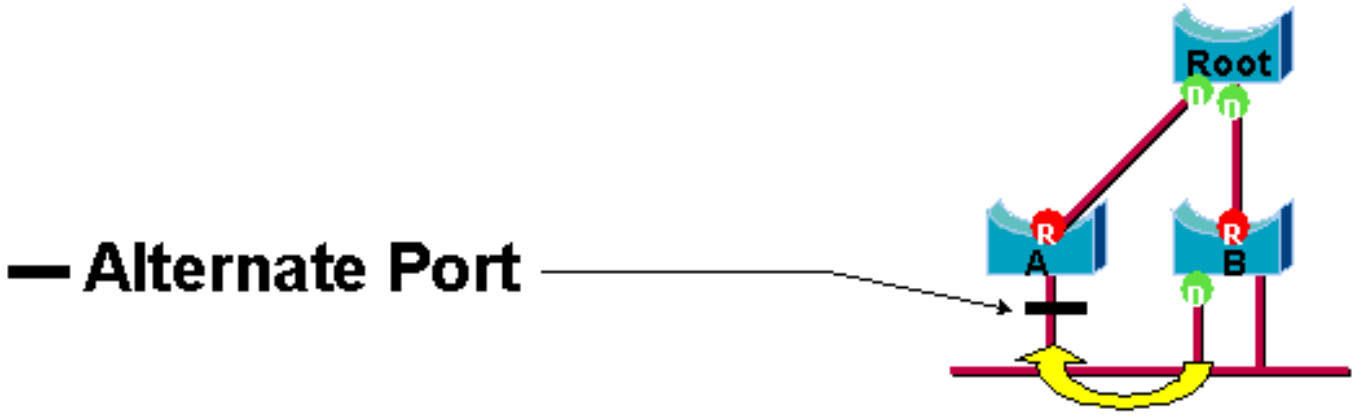
지정된 포트 역할

포트가 연결된 세그먼트에서 최상의 BPDU를 전송할 수 있는 포트는 지정됩니다.802.1D 브리지는 서로 다른 세그먼트(예: 이더넷 세그먼트)를 연결하여 브리지 도메인을 생성합니다.지정된 세그먼트에는 루트 브리지로 향하는 경로가 하나만 있을 수 있습니다.두 개의 경로가 있으면 네트워크에 브리징 루프가 있습니다.지정된 세그먼트에 연결된 모든 브리지는 다른 브리지의 BPDU를 수신하고 최상의 BPDU를 해당 세그먼트에 대해 지정된 브리지로 전송하는 브리지에 동의합니다.해당 브리지의 해당 포트가 지정됩니다.

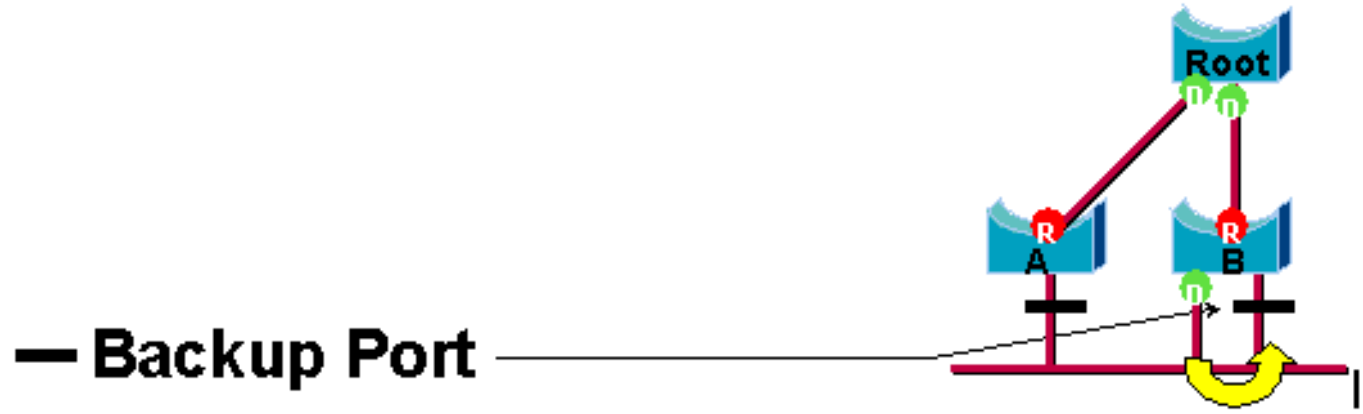
대체 및 백업 포트 역할

이 두 포트 역할은 802.1D의 차단 상태에 해당합니다.차단된 포트의 정의는 지정된 포트 또는 루트 포트가 아닌 포트입니다.차단된 포트는 세그먼트에서 전송하는 BPDU보다 더 유용한 BPDU를 수신합니다.포트는 차단 상태를 유지하기 위해 BPDU를 수신해야 합니다.RSTP에서는 이 목적을 위해 이러한 두 가지 역할을 도입합니다.

대체 포트는 다른 브리지에서 더 유용한 BPDU를 수신하여 차단된 포트입니다.다음 다이어그램은 다음과 같습니다.



백업 포트는 포트가 있는 동일한 브리지에서 더 유용한 BPDU를 수신하여 차단된 포트입니다.다음 다이어그램은 다음과 같습니다.



이러한 차이는 이미 802.1D 내에서 내부적으로 만들어졌습니다.이는 기본적으로 Cisco UplinkFast가 작동하는 방식입니다.이를 뒷받침하는 이유는 대체 포트가 루트 브리지에 대한 대체 경로를 제공한다는 것입니다.따라서 이 포트가 실패하면 루트 포트를 대체할 수 있습니다.물론 백업 포트는 동일한 세그먼트에 대한 중복 연결을 제공하여 루트 브리지에 대한 대체 연결을 보장 할 수는 없습니다.따라서 백업 포트는 업링크 그룹에서 제외되었습니다.

결과적으로 RSTP는 802.1D와 정확히 동일한 기준을 사용하여 스패닝 트리의 최종 토폴로지를 계산합니다.서로 다른 브리지 및 포트 우선 순위를 사용하는 방식은 변경되지 않습니다.이름 차단은 Cisco 구현에서 폐기 상태에 사용됩니다.CatOS 릴리스 7.1 이상 릴리스는 여전히 수신 및 학습 상태를 표시하며, 이는 IEEE 표준에서 요구하는 것보다 포트에 대한 더 많은 정보를 제공합니다.그러나 새로운 기능은 프로토콜이 포트에 대해 결정한 역할과 현재 상태에 차이가 있다는 것입니다.예를 들어, 이제는 포트를 지정하고 동시에 차단하는 것이 완벽하게 유효합니다.일반적으로 매우 짧은 시간 동안 발생하는 반면, 이 포트는 지정된 전달을 위한 일시적인 상태에 있음을 의미합니다.

VLAN과의 STP 상호 작용

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

- 모든 VLAN을 위한 단일 스패닝 트리 또는 IEEE 802.1D와 같은 CST(Common Spanning Tree Protocol)
- VLAN당 스패닝 트리 또는 Cisco PVST와 같은 공유 스패닝 트리
- VLAN 집합당 스패닝 트리 또는 MST(Multiple Spanning Tree)(예: IEEE 802.1s)

컨피그레이션 관점에서 VLAN과의 상호 작용과 관련된 이러한 세 가지 유형의 스패닝 트리 모드는 세 가지 모드 중 하나로 구성할 수 있습니다.

- **pvst** - VLAN별 스패닝 트리이 기능은 실제로 PVST+를 구현하지만 Cisco IOS Software에서는 PVST로만 표시됩니다.
- **rapid-pvst**—802.1D 표준의 발전은 컨버전스 시간을 향상시키고 UplinkFast 및 BackboneFast의 표준 기반(802.1w) 속성을 통합합니다.
- **mst** - VLAN 또는 MST 집합당 스패닝 트리의 802.1s 표준입니다.또한 802.1w의 고속 구성 요소가 표준 내에 통합되어 있습니다.

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

VLAN 또는 PVST+당 하나의 스패닝 트리를 사용하면 로드 밸런싱이 가능하지만 VLAN 수가 증가함에 따라 더 많은 BPDU CPU 처리가 필요합니다.

새로운 802.1s 표준(MST)을 사용하면 최대 16개의 활성 STP 인스턴스/토폴로지를 정의하고 모든 VLAN을 이러한 인스턴스에 매핑할 수 있습니다.일반적인 캠퍼스 환경에서는 두 개의 인스턴스만 정의해야 합니다.이 기술은 STP를 수천 개의 VLAN으로 확장하는 동시에 로드 밸런싱을 활성화합니다.

Rapid-PVST 및 사전 표준 MST에 대한 지원은 Cisco IOS Software 릴리스 12.1(11b)EX 및 12.1(13)E for Catalyst 6500에 도입되었습니다.Catalyst 4500과 Cisco IOS Software 릴리스 12.1(12c)EW 이상 릴리스는 사전 표준 MST를 지원합니다.Cisco IOS Software Release12.1(19)EW for Catalyst 4500 플랫폼에 빠른 PVST 지원이 추가되었습니다.표준 호환 MST는 Cisco IOS Software 릴리스 12.2(18)SXF for Catalyst 6500 및 Cisco IOS Software 릴리스 12.2(25)SG for Catalyst 4500 Series 스위치에서 지원됩니다.

자세한 내용은 고속 스패닝 트리 프로토콜(802.1w) 및 다중 스패닝 트리 프로토콜(802.1s) 이해를 참조하십시오.

스패닝 트리 논리적 포트

Catalyst 4500 및 6500 릴리스 노트는 스위치당 스패닝 트리의 논리적 포트 수에 대한 지침을 제공합니다.모든 논리적 포트의 합계는 스위치의 트렁크 수와 트렁크의 활성 VLAN 수와 스위치의 트렁킹 이외 인터페이스 수와 같습니다.논리적 인터페이스의 최대 수가 제한을 초과할 경우 Cisco IOS 소프트웨어가 시스템 로그 메시지를 생성합니다.권장 지침을 초과하지 않는 것이 좋습니다.

이 표에서는 지원되는 논리 포트의 수를 다양한 STP 모드 및 수퍼바이저 유형과 비교합니다.

수퍼바이저	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	6,000[1] 스위칭 모듈당 총 1,200개	스위칭 모듈당 총 6,000개 1,200개	스위칭 모듈당 총 3,000[2],25,000
Catalyst 6500 Supervisor 2	스위칭 모듈당 13,000[1] 총 1,800[2]개	스위칭 모듈당 총 10,000,800[2]개	스위칭 모듈당 총 50,000개 6,000[2개]
Catalyst 6500 Supervisor 720	스위칭 모듈당 총 13,000,800[2]개	스위칭 모듈당 총 10,000,800[2]개	스위칭 모듈당 총 50,003개 6,000[2개]
Catalyst 4500	총 1,500개	총 1,500개	총 25,000

Supervisor II +			
Catalyst 4500 Supervisor II plus-10GE	총 1,500개	총 1,500개	총 25,000
Catalyst 4500 Supervisor IV	총 3,000개	총 3,000개	총 50,000
Catalyst 4500 Supervisor V	총 3,000개	총 3,000개	총 50,000
Catalyst 4500 Supervisor V 10GE	총 3,000개	총 3,000개	총 80,000

[1] Cisco IOS Software Release 12.1(13)E 이전 PVST+에서 지원되는 최대 논리적 포트 수는 4,500입니다.

[2] 10Mbps, 10/100Mbps 및 100Mbps 스위칭 모듈은 모듈당 최대 1,200개의 논리적 인터페이스를 지원합니다.

[3] Cisco IOS Software Release 12.2(17b)SXA 이전에 MST에서 지원되는 최대 논리적 포트 수는 30,000개입니다.

권장 사항

하드웨어, 소프트웨어, 디바이스 수 및 VLAN 수와 같은 세부 정보 없이 스패닝 트리 모드 권장 사항을 제공하기가 어렵습니다.일반적으로 논리적 포트 수가 권장 지침을 초과하지 않는 경우 새 네트워크 구축에는 Rapid PVST 모드를 사용하는 것이 좋습니다.빠른 PVST 모드는 백본 고속 및 업링크 고속 같은 추가 컨피그레이션 없이 빠른 네트워크 컨버전스를 제공합니다.다음 명령을 실행하여 Rapid-PVST 모드에서 스패닝 트리를 설정합니다.

```
spanning-tree mode rapid-pvst
```

기타 옵션

레거시 하드웨어와 이전 소프트웨어가 혼합된 네트워크에서는 PVST+ 모드를 사용하는 것이 좋습니다.PVST+ 모드에서 스패닝 트리를 설정하려면 다음 명령을 실행합니다.

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

VLAN이 많은 VLAN을 사용하는 VLAN Everywhere 네트워크 설계에는 MST 모드가 권장됩니다.이 네트워크의 경우 논리적 포트의 합계가 PVST 및 Rapid-PVST에 대한 지침을 초과할 수 있습니다.MST 모드에서 스패닝 트리를 설정하려면 다음 명령을 실행합니다.

```
spanning-tree mode mst
```

BPDU 형식

IEEE 802.1Q 표준을 지원하기 위해 Cisco는 PVST+ 프로토콜을 제공하기 위해 존재하는 PVST 프로토콜을 확장했습니다.PVST+는 IEEE 802.1Q 모노 스패닝 트리 영역 전체에 대한 링크를 지원합니다.PVST+는 IEEE 802.1Q 모노 스패닝 트리 및 존재하는 Cisco PVST 프로토콜 모두와 호환됩니다.또한 PVST+는 스위치 간에 포트 트렁킹 및 VLAN ID의 컨피그레이션 불일치가 발생하지 않도록 확인 메커니즘을 추가합니다.PVST+는 새로운 CLI(Command-Line Interface) 명령 또는 컨피그레이션이 필요하지 않은 PVST와 플러그 앤 플레이 방식으로 호환됩니다.

다음은 PVST+ 프로토콜의 운영 이론에 대한 몇 가지 주요 내용입니다.

- PVST+는 802.1Q 모노 스패닝 트리와 상호 운용됩니다.PVST+는 802.1Q 트렁킹을 통해 공통 STP에서 802.1Q 호환 스위치와 상호 운용됩니다.기본 VLAN인 VLAN 1에는 기본적으로 공통 스패닝 트리가 있습니다.하나의 공통 스패닝 트리 BPDU가 802.1Q 링크를 통해 IEEE 표준 브리지 그룹 MAC 주소(01-80-c2-00-00-00, 프로토콜 유형 0x010c)로 전송되거나 수신됩니다.공통 스패닝 트리는 PVST 또는 모노 스패닝 트리 영역에서 루팅할 수 있습니다.
- PVST+는 802.1Q VLAN 영역 전체에서 PVST BPDU를 멀티캐스트 데이터로 터널링합니다.트렁크의 각 VLAN에 대해 Cisco SSTP(Shared STP) MAC 주소(01-00-0c-cc-cd)가 있는 BPDU가 전송되거나 수신됩니다.PVID(Port VLAN Identifier)와 동일한 VLAN의 경우 BPDU는 태그가 지정되지 않습니다.다른 모든 VLAN의 경우 BPDU에 태그가 지정됩니다.
- PVST+는 ISL 트렁킹을 통해 PVST의 기존 Cisco 스위치와 역호환됩니다.ISL 캡슐화된 BPDU는 이전 Cisco PVST와 동일한 ISL 트렁크를 통해 전송되거나 수신됩니다.
- PVST+는 포트 및 VLAN 불일치를 확인합니다.PVST+는 전달 루프가 발생하지 않도록 일관성 없는 BPDU를 수신하는 포트를 차단합니다.또한 PVST+는 syslog 메시지를 통해 불일치에 대해 사용자에게 알립니다.

참고: ISL 네트워크에서는 모든 BPDU가 IEEE MAC 주소를 사용하여 전송됩니다.

Cisco 구성 권장 사항

모든 Catalyst 스위치에는 기본적으로 STP가 활성화되어 있습니다.차단된 포트를 능동적으로 유지 관리하기 위해 레이어 2 루프가 포함되지 않은 설계와 STP가 활성화되지 않은 설계를 선택하더라도 다음과 같은 이유로 이 기능을 활성화한 상태로 둡니다.

- 루프가 있는 경우 STP는 멀티캐스트 및 브로드캐스트 데이터로 인해 더 악화될 수 있는 문제를 방지합니다.잘못된 패치, 잘못된 케이블 또는 다른 원인으로 인해 루프가 발생하는 경우가 많습니다.
- STP는 EtherChannel 분석을 차단합니다.
- 대부분의 네트워크는 STP로 구성되어 있으므로 최대 필드 노출을 가져옵니다.노출이 더 많을수록 일반적으로 더 안정적인 코드가 됩니다.
- STP는 이중 연결 NIC의 오작동을 방지합니다(또는 서버에서 브리징이 활성화됨).
- 많은 프로토콜이 코드의 STP와 밀접한 관련이 있습니다.예를 들면 다음과 같습니다 .PAgPIGMP(Internet Group Message Protocol) 스누핑트렁킹STP를 사용하지 않고 실행하면 바람직하지 않은 결과를 얻을 수 있습니다.
- 보고된 네트워크 중단 중에 Cisco 엔지니어는 STP의 비사용이 결함의 중심에 있다고 일반적으로 제안합니다.

모든 VLAN에서 스패닝 트리를 활성화하려면 다음 글로벌 명령을 실행합니다.

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

타이머를 변경하지 마십시오. 그러면 안정성에 부정적인 영향을 미칠 수 있습니다.구축된 대부분의

네트워크는 조정되지 않습니다.hello-interval 및 maxage와 같이 명령줄을 통해 액세스할 수 있는 단순 STP 타이머에는 다른 것으로 간주된 내장 타이머의 복잡한 집합이 있습니다.따라서 타이머를 조정하고 모든 결과를 고려한다면 어려움이 따를 수 있습니다.또한 UDLD 보호를 손상시킬 수 있습니다.

사용자 트래픽을 관리 VLAN에서 분리하는 것이 좋습니다.이는 Catalyst 6500/6000 Cisco IOS 스위치에는 적용되지 않습니다.그러나 별도의 관리 인터페이스를 가질 수 있고 Cisco IOS 스위치와 통합되어야 하는 소규모 Cisco IOS 스위치 및 CatOS 스위치에서 이러한 권장 사항을 준수해야 합니다.특히 이전 Catalyst 스위치 프로세서의 경우 STP에 문제가 발생하지 않도록 관리 VLAN을 사용자 데이터와 분리하십시오.잘못 동작하는 하나의 엔드 스테이션은 잠재적으로 Supervisor Engine 프로세서를 브로드캐스트 패킷으로 사용할 수 있도록 하여 프로세서가 하나 이상의 BPDU를 놓칠 수 있습니다.하지만 CPU 및 조절 제어 기능이 더욱 강력한 최신 스위치로 이러한 문제를 해결할 수 있습니다.자세한 내용은 이 문서의 Switch Management Interface and Native VLAN 섹션을 참조하십시오.

이중화를 오버설계하지 마십시오.이로 인해 너무 많은 차단 포트가 발생하여 장기 안정성에 부정적인 영향을 미칠 수 있습니다.총 STP 지름을 7홉으로 유지합니다.이 설계가 가능한 모든 곳에 Cisco 멀티레이어 모델을 설계해 보십시오.모델 기능은 다음과 같습니다.

- 더 작은 스위치드 도메인
- STP 삼각형
- 결정적 차단 포트

루트 기능 및 차단된 포트가 있는 위치에 영향을 미치고 파악합니다.토폴로지 다이어그램에 이 정보를 문서화합니다.스패닝 트리 토폴로지를 파악합니다. 이는 트러블슈팅을 위해 필수적입니다.차단된 포트는 STP 문제 해결이 시작되는 포트입니다.차단을 전달으로 변경하는 원인은 종종 근본 원인 분석의 핵심 부분입니다.이러한 레이어는 네트워크에서 가장 안정적인 부분으로 간주되므로 배포 및 코어 레이어를 루트/보조 루트의 위치로 선택합니다.레이어 2 데이터 포워딩 경로를 사용하는 최적의 레이어 3 및 HSRP(Hot Standby Router Protocol) 오버레이를 확인합니다.

이 명령은 브리지 우선순위를 구성하는 매크로입니다.루트는 기본(32,768)보다 훨씬 낮은 우선순위를 설정하고, 보조 는 기본값보다 상당히 낮은 우선순위를 설정합니다.

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

참고: 이 매크로는 루트 우선 순위를 다음 중 하나로 설정합니다.

- 기본적으로 8192
- 다른 루트 브리지가 알려진 경우 현재 루트 우선 순위 - 1
- MAC 주소가 현재 루트보다 낮은 경우 현재 루트 우선 순위

양방향 연습인 트렁크 포트에서 불필요한 VLAN을 정리합니다.이 작업은 특정 VLAN이 필요하지 않은 네트워크의 일부에서 STP 및 NMP 처리 오버헤드의 지름을 제한합니다.VTP 자동 정리는 트렁크에서 STP를 제거하지 않습니다.트렁크에서 기본 VLAN 1을 제거할 수도 있습니다.

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

기타 옵션

Cisco는 잘 알려진 대상 MAC 주소 **01-00-0c-cd-cd-ce** 및 프로토콜 유형 0x010c를 사용하여 작동하는 또 다른 STP 프로토콜(**VLAN-bridge**)을 제공합니다.

이 프로토콜은 이러한 VLAN에서 실행되는 IEEE 스패닝 트리 인스턴스와 간섭 없이 VLAN 간에 라우팅 불가 또는 레거시 프로토콜을 브리지해야 하는 경우 가장 유용합니다.비브리징 트래픽에 대한 VLAN 인터페이스가 레이어 2 트래픽에 대해 차단되면 레이어 3 트래픽에 대한 오버레이도 부주의하게 제거되므로 원치 않는 부작용이 발생합니다.이 레이어 2 차단은 브리지 없는 트래픽에 대한 VLAN 인터페이스가 IP VLAN과 동일한 STP에 참여하는 경우 쉽게 발생할 수 있습니다.VLAN-bridge는 브리징 프로토콜에 대해 별도의 STP 인스턴스입니다.이 프로토콜은 IP 트래픽에 영향을 주지 않고 조작할 수 있는 별도의 토폴로지를 제공합니다.

MSFC와 같은 Cisco 라우터의 VLAN 간에 브리징이 필요한 경우 VLAN-bridge 프로토콜을 실행합니다.

STP PortFast 기능

PortFast를 사용하여 액세스 포트에서 일반 스패닝 트리 작업을 우회할 수 있습니다.PortFast는 링크 초기화 후 엔드 스테이션이 연결해야 하는 서비스와 엔드 스테이션 간의 연결 속도를 높입니다.Microsoft DHCP 구현에서는 IP 주소를 요청 및 받으려면 링크 상태가 시작된 직후 모드에서 액세스 포트를 확인해야 합니다.IPX(Internetwork Packet Exchange)/SPX(Sequenced Packet Exchange)와 같은 일부 프로토콜은 GNS(Get Nearest Server) 문제를 방지하기 위해 링크 상태가 시작된 후 바로 모드에서 액세스 포트를 확인해야 합니다.

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

PortFast 운영 개요

PortFast는 STP 정상적인 , 및 상태를 건너뜁니다.이 기능은 링크가 으로 표시된 후 포트를 에서 모드로 직접 .이 기능이 활성화되지 않은 경우 STP는 포트를 모드로 이동할 준비가 될 때까지 모든 사용자 데이터를 삭제합니다.이 프로세스에는 기본적으로 30초인 최대 시간(2 x ForwardDelay)이 소요될 수 있습니다.

`Portfast` 모드에서는 포트 상태가 에서 으로 변경될 때마다 TCN(STP Topology Change Notification)을 생성할 수 없습니다.TCN은 정상입니다.그러나 루트 브리지에 도달하는 TCN의 물결이 불필요하게 통합 시간을 확장할 수 있습니다.사람들이 PC를 켜는 아침에 TCN의 물결이 종종 일어난다.

Cisco 액세스 포트 구성 권장 사항

활성화된 모든 호스트 포트에 대해 STP PortFast on으로 설정합니다.또한 사용하지 않는 스위치 스위치 링크 및 포트에 대해 STP PortFast를 off로 명시적으로 설정합니다.

액세스 포트에 대한 권장 컨피그레이션을 구현하려면 인터페이스 컨피그레이션 모드에서 switchport **host** macro 명령을 실행합니다.이 컨피그레이션은 자동 협상 및 연결 성능을 크게 향상시킵니다.

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

참고: PortFast는 스패닝 트리가 포트에서 전혀 실행되지 않음을 의미하지 않습니다.BPDU는 여전

히 전송, 수신 및 처리됩니다.스패닝 트리는 완전한 기능을 갖춘 LAN에 필수적입니다.루프 감지 및 차단 기능이 없으면 루프가 실수로 전체 LAN을 신속하게 다운할 수 있습니다.

또한 모든 호스트 포트에 대해 트렁킹 및 채널링을 비활성화합니다.각 액세스 포트는 트렁킹 및 채널링에 기본적으로 활성화되어 있지만 호스트 포트의 설계에서는 스위치 네이버를 예상하지 않습니다.이러한 프로토콜을 협상하기 위해 남겨둘 경우, 포트 활성화의 후속 지연은 바람직하지 않은 상황을 초래할 수 있습니다.DHCP 및 IPX 요청과 같은 워크스테이션의 초기 패킷은 전달되지 않습니다.

더 좋은 옵션은 다음 명령을 사용하여 전역 컨피그레이션 모드에서 기본적으로 PortFast를 구성하는 것입니다.

```
Switch(config)#spanning-tree portfast enable
```

그런 다음 하나의 VLAN에 허브 또는 스위치가 있는 액세스 포트에서 **interface** 명령을 사용하여 각 인터페이스에서 PortFast 기능을 비활성화합니다.

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

기타 옵션

PortFast BPDU 가드는 루프를 방지하는 방법을 제공합니다.BPDU 가드는 비트렁킹 포트를 해당 포트에서 BPDU를 수신할 때 `errDisable` 상태로 이동합니다.

정상적인 조건에서 PortFast에 대해 구성된 액세스 포트에서 BPDU 패킷을 수신하지 마십시오.들어오는 BPDU가 잘못된 컨피그레이션을 나타냅니다.가장 좋은 방법은 액세스 포트를 종료하는 것입니다.

Cisco IOS 시스템 소프트웨어는 UplinkFast에 대해 활성화된 모든 포트 `BPDU-ROOT-GUARD` 자동으로 활성화하는 유용한 전역 명령을 제공합니다.*항상* 이 명령을 사용합니다.이 명령은 포트별로 작동하지 않고 스위치별로 작동합니다.

BPDU`-ROOT-GUARD`를 활성화하려면 다음 전역 명령 .

```
Switch(config)#spanning-tree portfast bpduguard default
```

SNMP(Simple Network Management Protocol) 트랩 또는 syslog 메시지는 포트가 다운되면 네트워크 관리자에게 알립니다.errDisabled 포트에 대한 자동 복구 시간을 구성할 수도 .자세한 내용은 이 문서의 단방향 링크 탐지 섹션을 참조하십시오.

자세한 내용은 스패닝 트리 PortFast BPDU 가드 개선 사항을 참조하십시오.

참고: 트렁크 포트의 PortFast는 Cisco IOS Software 릴리스 12.1(11b)E에서 도입되었습니다.트렁크 포트의 PortFast는 레이어 3 네트워크의 컨버전스 시간을 늘리기 위해 설계되었습니다.이 기능을 사용할 때는 인터페이스를 기준으로 BPDU 가드 및 BPDU 필터를 비활성화해야 합니다.

Uplinkfast

목적

UplinkFast는 네트워크 액세스 레이어에서 직접 링크 장애가 발생한 후 빠른 STP 컨버전스를 제공합니다.UplinkFast는 STP를 수정하지 않고 작동합니다.이 목적은 일반적인 30초 지연 시간이 아니라 특정 상황에서 컨버전스 시간을 3초 미만으로 단축하는 것입니다.Cisco UplinkFast 기능 이해 및 구성을 참조하십시오.

운영 개요

액세스 레이어에서 Cisco 멀티레이어 설계 모델을 사용하면 포워딩 업링크가 손실된 경우 차단 업링크가 상태로 즉시 이동됩니다.이 기능은 및 상태를 기다리지 않습니다.

업링크 그룹은 루트 포트 및 백업 루트 포트로 간주할 수 있는 VLAN당 포트 집합입니다.정상적인 조건에서 루트 포트는 액세스로부터 루트로의 연결을 보장합니다.이 기본 루트 연결이 어떤 이유로든 실패하면 백업 루트 링크가 즉시 시작되며, 일반적인 컨버전스 지연 30초를 거치지 않아도 됩니다.

UplinkFast는 정상적인 STP 토폴로지 변경 처리 프로세스(및)를 효과적으로 우회하므로 대체 토폴로지 수정 메커니즘이 필요합니다.메커니즘은 대체 경로를 통해 로컬 엔드 스테이션에 연결할 수 있는 정보로 도메인의 스위치를 업데이트해야 합니다.따라서 UplinkFast를 실행하는 액세스 레이어 스위치는 CAM 테이블의 각 MAC 주소에 대한 프레임을 잘 알려진 멀티캐스트 MAC 주소(01-00-0c-cd-cd-cd-cd HDLC 프로토콜 0x200a)로 생성합니다. 이 프로세스는 도메인의 모든 스위치에 있는 CAM 테이블을 새 토폴로지로 업데이트합니다.

Cisco 권장 사항

802.1D 스패닝 트리를 실행하는 경우 차단된 포트가 있는 액세스 스위치에 대해 UplinkFast를 활성화하는 것이 좋습니다.Cisco 멀티레이어 설계에서 일반적으로 디스트리뷰션 및 코어 스위치를 사용하는 백업 루트 링크에 대한 묵시적 토폴로지 지식이 없는 스위치에서는 UplinkFast를 사용하지 마십시오.일반적으로 네트워크에서 두 가지 이상의 방법이 있는 스위치에서는 UplinkFast를 활성화하지 마십시오.스위치가 복잡한 액세스 환경에 있고 둘 이상의 링크 차단 및 링크 포워딩이 있는 경우 스위치에서 이 기능을 사용하지 않거나 고급 서비스 엔지니어에게 문의하십시오.

UplinkFast를 활성화하려면 다음 전역 명령을 실행합니다.

```
Switch(config)#spanning-tree uplinkfast
```

Cisco IOS Software의 이 명령은 모든 브리지 우선순위 값을 높은 값으로 자동으로 조정하지는 않습니다.대신, 이 명령은 수동으로 변경되지 않은 브리지 우선 순위를 가진 VLAN만 변경합니다.또한 CatOS와 달리 UplinkFast가 활성화된 스위치를 복원할 때 이 명령의 no 형식(spanning-tree uplinkfast **없음**)은 변경된 모든 값을 기본값으로 되돌립니다.따라서 이 명령을 사용할 때 원하는 결과가 달성되도록 하려면 브리지 우선 순위의 현재 상태를 전후에 확인해야 *합니다*.

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 프레임이 생성되어야 합니다.rate 키워드는 UplinkFast 토폴로지 업데이트 프레임의 초당 패킷을 나타냅니다.기본값은 권장 사항입니다.메커니즘이 기본적으로 포함되고 RSTP에서 자동으로 활성화되므로 RSTP를 사용하여 UplinkFast를 구성할 필요가 없습니다.

백본Fast

목적

BackboneFast는 간접 링크 장애로부터 신속한 컨버전스를 제공합니다.BackboneFast는 컨버전스 시간을 기본값인 50초에서 일반적으로 30초로 단축하며, 이러한 방식으로 STP에 기능을 추가합니다.이 기능은 802.1D를 실행할 때만 적용됩니다.Rapid PVST 또는 MST(빠른 구성 요소 포함)를 실행할 때는 기능을 구성하지 마십시오.

운영 개요

BackboneFast는 스위치의 루트 포트 또는 차단된 포트가 지정된 브리지에서 하위 BPDU를 수신할 때 시작됩니다.다운스트림 스위치가 루트에 대한 연결을 끊고 새 루트를 선택하기 위해 BPDU를 보내기 시작할 때 포트는 일반적으로 낮은 BPDU를 수신합니다.하위 BPDU는 스위치를 루트 브리지 및 지정된 브리지로 식별합니다.

일반적인 스패닝 트리 규칙에서 수신 스위치는 구성된 최대 시간 동안 하위 BPDU를 무시합니다.기본적으로 최대값은 20초입니다.그러나 BackboneFast를 사용하면 스위치에서 하위 BPDU를 토폴로지의 변경 가능성을 나타내는 신호로 간주합니다.이 스위치는 루트 브리지에 대한 대체 경로가 있는지 확인하기 위해 RLQ(Root Link Query) BPDU를 사용합니다.이 RLQ 프로토콜 추가를 사용하면 스위치가 루트가 여전히 사용 가능한지 확인할 수 있습니다.RLQ는 차단된 포트를 더 일찍 이동하고 하위 BPDU를 전송한 격리된 스위치에 루트가 여전히 존재함을 알립니다.

프로토콜 작업의 몇 가지 주요 내용은 다음과 같습니다.

- 스위치는 루트 포트에서만 RLQ 패킷을 전송합니다(즉, 패킷이 루트로 이동함).
- RLQ를 수신하는 스위치는 루트 스위치인 경우 또는 해당 스위치가 루트와의 연결이 끊어진 것을 알고 있는 경우 응답할 수 있습니다.스위치가 이러한 사실을 모를 경우 쿼리를 루트 포트로 전달해야 합니다.
- 스위치에서 루트에 대한 연결이 끊어진 경우 스위치는 이 쿼리에 대해 음수로 응답해야 합니다.
- 회신은 쿼리가 시작된 포트에서만 전송되어야 합니다.
- 루트 스위치는 항상 이 쿼리에 긍정적인 회신을 사용하여 응답해야 합니다.
- 루트가 아닌 포트에서 회신이 수신되면 회신을 취소합니다.

maxage가 만료될 필요가 없으므로 이 작업을 수행하면 STP 컨버전스 시간이 최대 20초까지 단축됩니다.자세한 내용은 Catalyst 스위치에서 백본 빠른 구성 및 이해를 참조하십시오.

Cisco 권장 사항

전체 스패닝 트리 도메인이 이 기능을 지원할 수 있는 경우에만 STP를 실행하는 모든 스위치에서 BackboneFast를 활성화합니다.프로덕션 네트워크에 지장을 주지 않고 기능을 추가할 수 있습니다.

BackboneFast를 활성화하려면 다음 전역 명령을 실행합니다.

```
Switch(config)#spanning-tree backbonefast
```

참고: 도메인의 모든 스위치에서 이 전역 레벨 명령을 구성해야 합니다.이 명령은 모든 스위치가 이해해야 하는 기능을 STP에 추가합니다.

기타 옵션

BackboneFast는 Catalyst 2900XL 및 3500XL 스위치에서 지원되지 않습니다.일반적으로 스위치 도메인에 Catalyst 4500/4000, 5500/5000 및 6500/6000 스위치 외에 이러한 스위치가 포함된 경우 BackboneFast를 활성화해야 합니다.엄격한 토폴로지에서 XL 스위치가 있는 환경에서

BackboneFast를 구현할 경우, XL 스위치가 마지막 라인 스위치이며 두 위치에서 코어에만 연결된 기능을 활성화할 수 있습니다.XL 스위치의 아키텍처가 데이지 체인 방식으로 되어 있는 경우에는 이 기능을 구현하지 마십시오.

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

스패닝 트리 루프 가드

Loop Guard는 STP를 위한 Cisco 독점적 최적화 기능입니다.루프 가드는 네트워크 인터페이스 오작동, 사용 중인 CPU 또는 BPDU의 정상적인 포워딩을 방해하는 것으로 인해 발생하는 루프에서 레이어 2 네트워크를 보호합니다.이중화 토폴로지의 차단 포트가 전달 상태로 잘못 전환될 경우 STP 루프가 생성됩니다.이는 일반적으로 물리적으로 이중화된 토폴로지의 포트 중 하나(반드시 차단 포트가 아님)가 BPDU 수신을 중지했기 때문입니다.

루프 가드는 스위치를 포인트-투-포인트 링크로 연결하는 스위치드 네트워크에서만 유용합니다. 대부분의 최신 캠퍼스 및 데이터 센터 네트워크에서도 마찬가지입니다.포인트 투 포인트 링크에서는 하위 BPDU를 보내거나 링크를 다운하지 않으면 지정된 브리지가 사라질 수 없습니다.STP 루프 가드 기능은 Catalyst 6500용 Catalyst Cisco IOS Software 릴리스 12.1(13)E 및 Catalyst 4500 스위치용 Cisco IOS Software 릴리스 12.1(9)EA1에서 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 BPDU를 다시 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 조건이 포트에서 제거되고 STP가 포트 상태를 결정합니다.이렇게 하면 복구가 자동으로 수행됩니다.

루프 가드는 장애를 격리하고 스패닝 트리가 실패한 링크 또는 브리지 없이 안정적인 토폴로지로 통합되도록 합니다.루프 가드는 사용 중인 STP 버전의 속도로 STP 루프를 방지합니다.STP 자체(802.1D 또는 802.1w) 또는 STP 타이머를 튜닝할 때 종속성이 없습니다.이러한 이유로 Cisco는 STP를 사용하는 토폴로지와 소프트웨어가 기능을 지원하는 위치에 UDLD와 함께 루프 가드를 구현하는 것이 좋습니다.

루프 가드가 일관성 없는 포트를 차단할 경우 이 메시지가 기록됩니다.

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

BPDU가 루프 불일치 STP 상태의 포트에서 수신되면 포트는 다른 STP 상태로 전환됩니다.수신한 BPDU에 따르면, 이는 복구가 자동으로 이루어지므로 개입할 필요가 없음을 의미합니다.복구 후 다음 메시지가 기록됩니다.

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

다른 STP 기능과의 상호 작용

루트 가드

루트 가드는 포트를 항상 지정하도록 강제합니다.루프 가드는 포트가 루트 포트 또는 대체 포트인 경우에만 유효하며, 이는 해당 기능이 상호 배타적임을 의미합니다.따라서 포트에서 루프 가드와 루트 가드를 동시에 활성화할 수 없습니다.

Uplinkfast

루프 가드는 UplinkFast와 호환됩니다.루프 가드가 루트 포트를 차단 상태로 설정하는 경우 UplinkFast는 포워딩 상태로 새 루트 포트를 설정합니다.또한 UplinkFast는 *루프 불일치 포트*를 루트 포트로 선택하지 않습니다.

백본Fast

루프 가드는 BackboneFast와 호환됩니다.BackboneFast는 지정된 브리지에서 오는 하위 BPDU의 수신에 의해 트리거됩니다.이 링크에서 BPDU가 수신되므로 루프 가드가 끼우지 않습니다.따라서 BackboneFast 및 루프 가드가 호환됩니다.

PortFast

PortFast는 연결 즉시 포트를 전달 지정 상태로 전환합니다.PortFast 지원 포트는 루트/대체 포트가 아니므로 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 형성하려면 채널에 그룹화된 모든 물리적 포트에는 호환 가능한 구성이 있어야 합니다.PAgP는 채널을 형성하기 위해 모든 물리적 포트에서 루프 가드의 균일한 컨피그레이션을 적용합니다.EtherChannel에서 루프 가드를 구성할 때 다음 주의 사항을 참고하십시오.

- STP는 항상 채널의 첫 번째 운영 포트를 선택하여 BPDU를 전송합니다.해당 링크가 단방향으로 되면 루프 가드는 채널 기능의 다른 링크가 제대로 작동하더라도 채널을 차단합니다.
- 루프 가드에 의해 이미 차단된 포트 집합이 채널을 형성하기 위해 함께 그룹화된 경우 STP는 해당 포트에 대한 모든 상태 정보를 잃게 되며 새 채널 포트는 지정된 역할로 포워딩 상태를 얻을 수 있습니다.
- 루프 가드에 의해 채널이 차단되고 채널이 끊기면 STP에서 모든 상태 정보를 잃게 됩니다.개별 물리적 포트는 지정된 역할로 전달 상태를 얻을 수 있습니다. 채널을 형성하는 링크 중 하나 이상이 단방향인 경우에도 마찬가지입니다.

이러한 마지막 두 경우 UDLD에서 오류를 탐지할 때까지 루프가 발생할 가능성이 있습니다.하지만 루프 가드는 이를 탐지할 수 없습니다.

루프 가드 및 UDLD 기능 비교

루프 가드 및 UDLD 기능은 부분적으로 중첩되며, 단방향 링크로 인해 발생하는 STP 장애로부터 둘 다 보호됩니다.이 두 가지 기능은 문제에 대한 접근 방식과 기능에서도 다릅니다.특히 UDLD에서 탐지할 수 없는 단방향 장애(예: BPDU를 보내지 않는 CPU에 의해 발생한 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 경우에는 작동하지 않습니다.링크 연결 이후 단방향인 링크의 경우 포트는 BPDU를 수신하지 않으며 지정됩니다.이는 정상적인 동작일 수 있으므로 루프 가드는 이 특정 사례를 다루지 않습니다.UDLD는 이러한 시나리오에 대한 보호를 제공합니다.

UDLD와 루프 가드 모두 지원되므로 최고 수준의 보호를 제공합니다.루프 가드와 UDLD 간의 기능 비교에 대한 자세한 내용은 다음을 참조하십시오.

- *Loop Guard 및 BPDU Skew Detection*(BPDU 스큐 탐지) 기능을 사용하여 스패닝 트리 프로토콜 개선 사항의 Loop Guard와 단방향 링크 탐지 섹션
- 이 문서의 UDLD 섹션

Cisco 권장 사항

물리적 루프가 있는 스위치 네트워크에서 루프 가드를 전역적으로 활성화하는 것이 좋습니다.모든 포트에서 루프 가드를 전역적으로 활성화할 수 있습니다.이 기능은 모든 포인트 투 포인트 링크에서 활성화됩니다.포인트-투-포인트 링크는 링크의 이중 상태로 탐지됩니다.듀플렉스가 꽉 차면 해당 링크는 포인트-투-포인트로 간주됩니다.

```
Switch(config)#spanning-tree loopguard default
```

기타 옵션

전역 루프 가드 컨피그레이션을 지원하지 않는 스위치의 경우 포트 채널 포트를 포함하는 모든 개별 포트에서 이 기능을 활성화하는 것이 좋습니다.지정된 포트에서 루프 가드를 활성화하면 이점이 없지만 활성화와 관련된 문제는 고려하지 마십시오.또한 유효한 스패닝 트리 재컨버전스는 실제로 지정된 포트를 루트 포트로 전환할 수 있으므로 이 포트에서 이 기능이 유용합니다.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

루프 프리(loop-free) 토폴로지가 있는 네트워크는 루프가 실수로 발생하는 경우에도 루프 가드의 이점을 계속 누릴 수 있습니다.그러나 이러한 유형의 토폴로지에서 루프 가드 기능을 사용하면 네트워크 격리 문제가 발생할 수 있습니다.루프 프리(loop-free) 토폴로지를 구축하고 네트워크 격리 문제를 피하려면 전역 또는 개별적으로 루프 가드를 비활성화할 수 있습니다.공유 링크에서 루프 가드를 활성화하지 마십시오.

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

또는

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface 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.이렇게 하면 루트 가드가 루트 브리지의 위치를 적용합니다.루트 가드는 매우 초기 Cisco IOS Software 릴리스 12.1E 이상에서 사용할 수 있습니다.

운영 개요

루트 가드는 STP 내장 메커니즘입니다.Root Guard에는 자체 타이머가 없으며 BPDU의 수신에만 의존합니다.루트 가드가 포트에 적용될 때 이 포트가 루트 포트가 될 가능성을 거부합니다.BPDU를 수신하면 지정된 포트가 루트 포트가 되는 스패닝 트리 컨버전스가 트리거되면 포트는 루트 일관성 없는 상태가 됩니다.이 syslog 메시지는 다음을 보여줍니다.

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

포트가 우수한 BPDU를 전송하지 않게 되면 포트가 다시 차단되지 않습니다.STP를 통해 포트는 수신 상태에서 학습 상태로 전환되며 포워딩 상태로 전환됩니다.이 syslog 메시지는 전환을 보여줍니다.

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

복구는 자동으로 수행됩니다.사람의 개입이 필요 없다.

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

자세한 내용은 스패닝 트리 프로토콜 루트 가드 향상을 참조하십시오.

Cisco 권장 사항

Cisco에서는 직접 관리 제어하지 않는 네트워크 디바이스에 연결하는 포트에서 루트 가드 기능을 활성화할 것을 권장합니다.루트 가드를 구성하려면 인터페이스 컨피그레이션 모드에 있을 때 다음 명령을 사용합니다.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

목적

EtherChannel은 구성 요소 10/100Mbps 또는 기가비트 링크 전체에서 프레임을 효율적으로 멀티플렉싱하는 프레임 배포 알고리즘을 포함합니다.프레임 배포 알고리즘을 사용하면 여러 채널을 단일 논리적 링크로 역멀티플렉싱할 수 있습니다.각 플랫폼이 구현의 다음 플랫폼과 다르지만 다음과 같은 공통 속성을 이해해야 합니다.

- 여러 채널을 통해 통계적으로 프레임을 다중화하는 알고리즘이 있어야 합니다.Catalyst 스위치에서는 하드웨어와 관련된 것입니다.예를 들면 다음과 같습니다.Catalyst 5500/5000s—모듈에 EBC(Ethernet Bundling Chip)가 있거나 없는 경우Catalyst 6500/6000s—프레임으로 더 자세히 읽고 IP 주소로 멀티플렉스 변환할 수 있는 알고리즘
- 논리적 채널이 생성되어 STP의 단일 인스턴스를 실행하거나 단일 라우팅 피어링을 사용할 수 있습니다. 이는 레이어 2 또는 레이어 3 EtherChannel에 따라 달라집니다.
- 링크 끝에서 매개변수 일관성을 확인하고 링크 장애 또는 추가에서 번들링 복구를 관리하는 데 도움이 되는 관리 프로토콜이 있습니다.이 프로토콜은 PAgP 또는 LACP(Link Aggregation Control Protocol)일 수 있습니다.

운영 개요

EtherChannel은 구성 요소 10/100Mbps, 기가비트 또는 10기가비트 링크 전체에서 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 프레임이 수신될 때 해당 대화의 일부이거나 프레임을 복제하는 과정에서 프레임 순서가 잘못 지정되지 않도록 합니다.

다음 표에서는 나열된 각 플랫폼에 대한 프레임 분포 알고리즘을 자세히 설명합니다.

플랫폼	채널 로드 밸런싱 알고리즘
Catalyst 3750 시리즈	MAC 주소 또는 IP 주소를 사용하는 Cisco IOS Software 로드 밸런싱 알고리즘을 실행하는 Catalyst 3750과 메시지 소스 또는 메시지 대상 또는 둘 다를 실행합니다.
Catalyst 4500 시리즈	MAC 주소, IP 주소 또는 L4(Layer 4) 포트 번호를 사용하는 Cisco IOS Software 로드 밸런싱 알고리즘을 실행하는 Catalyst 4500과 메시지 소스 또는 메시지 목적지 또는 둘 다를 실행합니다.
Catalyst 6500/6000 시리즈	Supervisor Engine 하드웨어에 따라 사용할 수 있는 두 가지 해싱 알고리즘이 있습니다.해시는 하드웨어에서 구현되는 17도 다항식입니다.모든 경우 해시는 MAC, IP 주소 또는 IP TCP/UDP 포트 번호를 사용하며 3비트 값을 생성하기 위해 알고리즘을 적용합니다.이 프로세스는 SA와 DA에 모두 개별적으로 수행됩니다.그런 다음 XOR 작업을 결과에 사용하여 다른 3비트 값을 생성합니다.이 값은 패킷을 전달하는 데 사용되는 채널의 포트를 결정합니다.Catalyst 6500/6000의 채널은 모든 모듈의 포트 간에 구성할 수 있으며 최대 8개의 포트까지 구성할 수 있습니다.

이 표는 다양한 Catalyst 6500/6000 Supervisor Engine 모델에서 지원되는 배포 방법을 나타냅니다.이 표에서는 기본 동작도 보여 줍니다.

하드웨어	설명	배포 방법
WS-F6020A(레이어 2 엔진) WS-F6K-PFC(레이어 3 엔진)	이후 Supervisor Engine I 및 Supervisor Engine IA Supervisor Engine IA/Policy Feature Card 1(PFC1)	레이어 2 MAC:SA;DA;SA 및 DA 레이어 3 IP:SA;DA;SA 및 DA(기본값)

WS-F6K-PFC 2	Supervisor Engine II/PFC2	레이어 2 MAC:SA;DA;SA 및 DA 레이어 3 IP:SA;DA;SA 및 DA(기본값) 레이어 4 세션:S 포트;D 포트;S 및 D 포트
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	레이어 2 MAC:SA;DA;SA 및 DA 레이어 3 IP:SA;DA;SA 및 DA(기본값) 레이어 4 세션:S 포트;D 포트;S 및 D 포트

참고: 레이어 4 디스트리뷰션을 사용하면 첫 번째 프래그먼트된 패킷은 레이어 4 디스트리뷰션을 사용합니다.이후의 모든 패킷은 레이어 3 디스트리뷰션을 사용합니다.

참고: 다른 플랫폼에서 EtherChannel 지원에 대한 자세한 내용과 EtherChannel 구성 및 문제 해결 방법을 알아보려면 다음 문서를 참조하십시오.

- Catalyst 스위치의 EtherChannel 로드 밸런싱 및 이중화 이해
- 레이어 3 및 레이어 2 EtherChannel 구성(Catalyst 6500 Series Cisco IOS Software 컨피그레이션 가이드, 12.2SX)
- 레이어 3 및 레이어 2 EtherChannel 구성(Catalyst 6500 Series Cisco IOS Software 컨피그레이션 가이드, 12.1E)
- EtherChannel 구성(Catalyst 4500 Series Switch Cisco IOS Software 구성 가이드, 12.2(31)SG)
- EtherChannel 구성(Catalyst 3750 스위치 소프트웨어 구성 가이드, 12.2(25)참조)
- CatOS 시스템 소프트웨어를 실행하는 Catalyst 4500/4000, 5500/5000 및 6500/6000 스위치 간 EtherChannel 구성

Cisco 권장 사항

Catalyst 3750, Catalyst 4500 및 Catalyst 6500/6000 시리즈 스위치는 기본적으로 소스 및 대상 IP 주소를 모두 해싱하여 로드 밸런싱을 수행합니다.이는 IP가 주요 프로토콜이라는 가정하에 권장됩니다.로드 밸런싱을 설정하려면 다음 명령을 실행합니다.

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

기타 옵션

트래픽 흐름에 따라, 대부분의 트래픽이 동일한 소스 및 대상 IP 주소 사이에 있는 경우 로드 밸런싱을 개선하기 위해 레이어 4 분배를 활용할 수 있습니다.레이어 4 디스트리뷰션이 구성된 경우 해싱에는 레이어 4 소스 및 목적지 포트만 포함됩니다.레이어 3 IP 주소를 해싱 알고리즘에 결합하지 않습니다.로드 밸런싱을 설정하려면 다음 명령을 실행합니다.

```
port-channel load-balance src-dst-port
```

참고: Catalyst 3750 시리즈 스위치에서는 레이어 4 디스트리뷰션을 구성할 수 없습니다.

프레임 배포 정책을 확인하려면 **show etherchannel load-balance** 명령을 실행합니다.

하드웨어 플랫폼에 따라 CLI 명령을 사용하여 EtherChannel의 어떤 인터페이스에서 특정 트래픽 흐름을 전달할지 결정할 수 있으며, 이때 프레임 배포 정책이 기본으로 사용됩니다.

Catalyst 6500 스위치의 경우 **원격 로그인 스위치** 명령을 실행하여 SP(Switch Processor) 콘솔에 원격으로 로그인합니다.그런 다음 **test etherchannel load-balance interface** ***port-channel number*** **{ip | l4포트 | mac} [***source_ip_add*** | *source_mac_add* | *source_l4_port***] [***dest_ip_add* | *dest_mac_add* | *dest_l4_port***]** 명령

Catalyst 3750 스위치의 경우 **test etherchannel load-balance interface** ***port-channel number*** **{ip | mac} [***source_ip_add*** | *source_mac_add***] [***dest_ip_add* | *dest_mac_add***]** 명령

Catalyst 4500의 경우 해당 명령을 아직 사용할 수 없습니다.

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 방지하기 위해 이러한 지침 및 제한을 완료합니다.예를 들어, QoS가 활성화된 경우 QoS 기능이 다른 Catalyst 6500/6000 시리즈 스위칭 모듈을 번들링할 때 EtherChannel이 형성되지 않습니다 .Cisco IOS Software를 실행하는 Catalyst 6500 스위치의 경우 EtherChannel 번들링에서 no mls qos channel-consistency port-channel interface 명령과 함께 QoS 포트 특성 확인**을 비활성화할** 수 있습니다.show **interface capability** ***mod/port* 명령은 *QoS* 포트 기능을** 표시하고 포트가 호환 가능한지 확인합니다.

컨피그레이션 문제를 방지하려면 여러 플랫폼에 대한 다음 지침을 참조하십시오.

- 레이어 3 및 레이어 2 EtherChannel 구성(Catalyst 6500 Series Cisco IOS Software 컨피그레이션 가이드, 12.2SX)
- 레이어 3 및 레이어 2 EtherChannel 구성(Catalyst 6500 Series Cisco IOS Software 컨피그레이션 가이드, 12.1E)
- EtherChannel 구성(Catalyst 4500 Series Switch Cisco IOS Software 구성 가이드, 12.2(31)SG)
- EtherChannel 구성(Catalyst 3750 스위치 소프트웨어 구성 가이드, 12.2(25)참조)

지원되는 최대 EtherChannel 수는 하드웨어 플랫폼 및 소프트웨어 릴리스에 따라 달라집니다 .Cisco IOS Software Release 12.2(18)SXE 이상을 실행하는 Catalyst 6500 스위치는 최대 128개의 포트 채널 인터페이스를 지원합니다.Cisco IOS Software Release 12.2(18)SXE 이전의 소프트웨어 릴리스는 최대 64개의 포트 채널 인터페이스를 지원합니다.구성 가능한 그룹 번호는 소프트웨어 릴리스에 관계없이 1~256입니다.Catalyst 4500 시리즈 스위치는 최대 64개의 EtherChannel을 지원합니다.Catalyst 3750 스위치의 경우 스위치 스택에 48개 이상의 EtherChannel을 구성하지 않는 것이 좋습니다.

스패닝 트리 포트 비용 계산

EtherChannel의 스패닝 트리 포트 비용 계산을 이해해야 합니다.짧은 방법 또는 긴 방법으로 EtherChannel의 스패닝 트리 포트 비용을 계산할 수 있습니다.기본적으로 포트 비용은 짧은 모드에

서 계산됩니다.

다음 표에서는 대역폭을 기준으로 레이어 2 EtherChannel의 스패닝 트리 포트 비용을 보여 줍니다.

대역폭	이전 STP 값	새 긴 STP 값
10Mbps	100	2,000,000
100Mbps	19	200,000
1Gbps	4	20,000
N X 1Gbps	3	6660
10Gbps	2	2,000
100Gbps	해당 없음	200
1Tbps	해당 없음	20
10Tbps	해당 없음	2

참고: CatOS에서 EtherChannel의 스패닝 트리 포트 비용은 포트 채널 멤버 링크 장애 후에도 동일하게 유지됩니다.Cisco IOS Software에서는 새로운 가용 대역폭을 반영하기 위해 EtherChannel의 포트 비용이 즉시 업데이트됩니다.원하는 동작이 불필요한 스패닝 트리 토폴로지 변경을 방지하기 위한 것이면 spanning-**tree cost** ***cost*** **명령**을 사용하여 스패닝 트리 포트 비용을 정적으로 구성할 수 있습니다.

PAgP(Port Aggregation Protocol)

목적

PAgP는 링크 양쪽 끝에서 매개변수 일관성을 확인하는 관리 프로토콜입니다.PAgP는 링크 장애 또는 추가에 대한 적응도 지원합니다.다음은 PAgP의 특성입니다.

- PAgP는 채널의 모든 포트가 동일한 VLAN에 속하거나 트렁크 포트로 구성되어 있어야 합니다.동적 VLAN은 포트를 다른 VLAN으로 강제로 변경할 수 있으므로 동적 VLAN은 EtherChannel 참여에 포함되지 않습니다.
- 번들이 이미 존재하고 포트 컨피그레이션이 수정되면 번들의 모든 포트가 해당 컨피그레이션과 일치하도록 수정됩니다.이러한 변경의 예로 VLAN의 변경 또는 모드 변경이 있습니다.
- 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.CDP 패킷에 사용되는 동일한 멀티캐스트 그룹 MAC 주소가 PAgP 패킷을 전송하기 위해 사용됩니다.MAC 주소는 01-00-0c-cc-cc-cc입니다.그러나 프로토콜 값은 0x0104입니다. 프로토콜 작업의 요약입니다.

- 물리적 포트가 작동 중인 경우, PAgP 패킷은 탐지 중에 1초마다, 그리고 30초마다 정상 상태로 전송됩니다.
- 데이터 패킷이 수신되었지만 PAgP 패킷이 수신되지 않은 경우 포트가 PAgP를 지원하지 않는 디바이스에 연결된 것으로 간주됩니다.
- 물리적 포트가 다른 PAgP 지원 디바이스에 대한 양방향 연결을 가지고 있음을 증명하는 PAgP 패킷을 수신합니다.

- 물리적 포트 그룹에서 이러한 패킷 2개가 수신되는 즉시 집계된 포트를 구성하려고 시도합니다.
- PAgP 패킷이 일정 기간 동안 중지되면 PAgP 상태가 해제됩니다.

일반 처리

이러한 개념은 프로토콜의 동작을 보여주는 데 도움이 됩니다.

- Agport — 동일한 어그리게이션의 모든 물리적 포트로 구성되며 자체 SNMP ifIndex로 식별할 수 있는 논리적 포트입니다.에이전트에 작동하지 않는 포트가 없습니다.
- Channel(채널) - 구성 기준을 충족하는 어그리게이션.채널은 비작동 포트를 포함할 수 있으며 상위 에이전트 집합입니다.STP 및 VTP를 포함하지만 CDP 및 DTP는 제외하는 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-capability라고 하는 컨피그레이션 매개변수를 .물리적 포트는 동일한 을 가진 다른 물리적 포트와 집계할 수 있으며, 이러한 물리적 포트에서만 집계될 수 있습니다.
- Aggregation 절차 - 물리적 포트가 UpData 또 UpPAgP 상태에 도달하면 해당 포트가 적절한 에이전트에 연결됩니다.포트가 해당 상태 중 하나를 다른 상태로 전환하면 포트가 에이전트에서 분리됩니다.

이 표에서는 상태에 대한 자세한 내용을 제공합니다.

주/도	의미
	수신된 PAgP 패킷이 없습니다.PAgP 패킷이 전송됩니다.물리적 포트는 에이전트에 연결된 유일한 포트입니다.비PAgP 패킷은 물리적 포트와 에이전트 간에 전달되거나 전송됩니다.
	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 전달되거나 전송됩니다.

두 연결의 양쪽 끝이 그룹화에 동의해야 합니다.그룹화는 연결 허용의 양쪽 끝을 모두 포함하는 포트에서 가장 큰 포트 그룹으로 정의됩니다.

물리적 포트가 UpPAgP 상태에 도달하면 포트는 새 물리적 포트의 과 일치하고 BiDir 상태 또는 UpPAgP 상태에 있는 물리적 포트가 있는 할당됩니다.이러한 BiDir 포트는 UpPAgP 상태로 동시에 이동합니다.새로 준비된 물리적 포트와 호환되는 구성 가능한 물리적 포트 매개변수가 있는 에이전트가 없는 경우 해당 포트는 연결된 물리적 포트가 없는 적합한 매개변수를 가진 에이전트에 할당됩니다.

PAgP 시간 제한은 물리적 포트에서 알려진 마지막 네이버에서 발생할 수 있습니다.시간 초과된 포트는 에이전트에서 제거됩니다.동시에 시간 초과된 타이머가 있는 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

존재하는 채널의 링크에 장애가 발생하면 에이전트가 업데이트되고 손실 없이 유지되는 링크를 통해 트래픽이 해시됩니다.이러한 오류의 예는 다음과 같습니다.

- 포트가 언플러그되었습니다.
- GBIC(Gigabit Interface Converter)가 제거되었습니다.
- 파이버가 고장 났다

참고: 채널의 링크에 장애가 발생하면 모듈의 전원이 꺼지거나 모듈이 제거될 수 있습니다.즉, 채널에는 2개의 물리적 포트가 필요합니다.2포트 채널의 시스템에서 한 포트가 손실된 경우, 논리적 에이전트는 해제되고 원래 물리적 포트는 스패닝 트리를 기준으로 다시 초기화됩니다.STP를 통해 포트를 다시 데이터에 사용할 수 있을 때까지 트래픽을 삭제할 수 있습니다.

네트워크 유지 관리를 계획할 때 두 가지 장애 모드의 이러한 차이는 중요합니다.STP 토폴로지가 변경될 수 있으며, 이 경우 모듈을 온라인 제거 또는 삽입할 때 고려해야 합니다.에이전트가 장애를 통해 방해 받지 않을 수 있으므로 NMS(Network Management System)로 채널의 각 물리적 링크를 관리해야 합니다.

Catalyst 6500/6000에서 원치 않는 토폴로지 변경을 완화하기 위해 다음 권장 사항 중 하나를 완료합니다.

- 채널을 형성하기 위해 모듈당 단일 포트를 사용하는 경우 3개 이상의 모듈(총 3개)을 사용합니다.
- 채널이 2개의 모듈에 걸쳐 있는 경우 각 모듈에 2개의 포트를 사용합니다(총 4개).
- 2개의 카드에 2포트 채널이 필요한 경우 Supervisor Engine 포트만 사용합니다.

구성 옵션

다음 표에 요약되어 있듯이 서로 다른 모드에서 EtherChannel을 구성할 수 있습니다.

모드	구성 가능한 옵션
	PAgP가 작동 중이 아닙니다.네이버 포트의 구성 방식에 상관없이 포트 채널네이버 포트 모드가 있으면 채널이 형성됩니다.
	어그리게이션이 PAgP의 제어하에 있습니다.포트는 수동 협상 상태로 배치됩니다.발신자가 모드에서 작동함을 나타내는 하나 이상의 PAgP 패킷이 수신될 때까지 인터페이스에서 PAgP 패킷이 전송되지 않습니다.
	어그리게이션이 PAgP의 제어하에 있습니다.포트는 활성 협상 상태로 전환되며, 이 경우 포트는 PAgP 패킷 전송을 통해 다른 포트와의 협상을 시작합니다.채널은 또는 모드에서 다른 포트 그룹으로 구성됩니다.
Catalyst 5500/5000 파이버 FE 및 GE 포	auto 또는 모드 키워드인터페이스에서 수신된 데이터 패킷이 없는 경우, 인터페이스는 에이전트에 연결되지 않으며 데이터에 사용할 수 없습니다.일부 링크 장애로 인해 채널이 분리되기 때문에 특정 Catalyst 5500/5000 하드웨어에 대해 이러한 양방향 검사가 제공되었습니다. 모드를 활성화하면 복구 네이버 포트가 다시 돌아와서 채널을 불필요하게 분리할 수 없습니다.Catalyst

트의 기본값입니다.	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 기본값입니다.	auto 또는 모드 키워드인터페이스에서 수신된 데이터 패킷이 없는 경우, 15초 시간 제한 기간이 지나면 인터페이스가 에이전트에 단독으로 연결됩니다.따라서 인터페이스를 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 방법에 영향을 줍니다.물리적 인터페이스 장애 또는 파이버 또는 케이블 끊김 때문에 포트를 전송할 수 없는 경우, 인접 포트는 작동 상태를 유지할 수 있습니다.파트너는 계속해서 데이터를 전송합니다.그러나 반환 트래픽을 수신할 수 없으므로 데이터가 손실됩니다.스패닝 트리 루프는 링크의 단방향 특성 때문에 형성될 수도 있습니다.

일부 파이버 포트에는 포트가 수신 신호(FFI)를 잃을 때 포트를 비작동 상태로 만드는 기능이 필요합니다. 이 작업을 수행하면 파트너 포트가 작동하지 않으며 링크 양쪽 끝에 있는 포트가 효과적으로 다운됩니다.

데이터(BPDU)를 전송하는 디바이스를 사용하고 단방향 조건을 탐지할 수 없는 경우 수신 데이터가 있고 링크가 양방향으로 확인될 때까지 포트가 비작동 상태를 유지하도록 하려면 모드를 사용합니다.단방향 링크를 탐지하는 데 PAgP가 걸리는 시간은 약 3.5 * 30초 = 105초입니다.30초는 두 개의 연속된 PAgP 메시지 사이의 시간입니다.단방향 링크의 보다 빠른 탐지기인 UDLD를 사용합니다.

데이터를 전송하지 않는 디바이스를 사용할 경우 모드를 사용합니다. 모드를 사용하면 수신된 데이터가 있는지 여부에 관계없이 포트가 연결되고 작동하게 됩니다.또한 단방향 조건의 존재를 감지할 수 있는 포트에 대해 모드가 기본적으로 사용됩니다.이러한 포트의 예는 레이어 1 FFI 및 UDLD를 사용하는 새로운 플랫폼입니다.

인터페이스에서 채널링을 해제하려면 **no channel-group** *number* 명령을 **실행합니다**.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

확인

이 섹션의 표에서는 직접 연결된 두 스위치, 스위치 A와 스위치 B 사이의 가능한 모든 PAgP 채널링 모드 시나리오에 대한 요약을 제공합니다.이러한 조합 중 일부는 STP가 채널링 측면에 있는 포트를 errDisable 상태로 설정할 수 있습니다. 즉, 이러한 조합은 채널링 측면의 포트를 차단합니다 .EtherChannel 컨피그레이션 오류 가드 기능은 기본적으로 활성화되어 있습니다.

채널 모드 전환	스위치 B 채널 모드	채널 상태 전환	스위치 B 채널 상태

켜짐	켜짐	채널(비 PAgP)	채널(비 PAgP)
켜짐	구성되지 않음	채널 아님 (errDisable)	채널 아님
켜짐	자동	채널 아님 (errDisable)	채널 아님
켜짐	권장	채널 아님 (errDisable)	채널 아님
구성되지 않음	켜짐	채널 아님	채널 아님 (errDisable)
구성되지 않음	구성되지 않음	채널 아님	채널 아님
구성되지 않음	자동	채널 아님	채널 아님
구성되지 않음	권장	채널 아님	채널 아님
자동	켜짐	채널 아님	채널 아님 (errDisable)
자동	구성되지 않음	채널 아님	채널 아님
자동	자동	채널 아님	채널 아님
자동	권장	PAgP 채널	PAgP 채널
권장	켜짐	채널 아님	채널 아님
권장	구성되지 않음	채널 아님	채널 아님
권장	자동	PAgP 채널	PAgP 채널
권장	권장	PAgP 채널	PAgP 채널

L2 채널에 대한 Cisco 구성 권장 사항

PAgP를 활성화하고 모든 EtherChannel 링크 설정을 사용합니다.자세한 내용은 다음 출력을 참조하십시오.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

다음과 같이 컨피그레이션을 확인합니다.

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

EtherChannel 구성 오류 방지

EtherChannel을 잘못 구성하고 스패닝 트리 루프를 생성할 수 있습니다.이러한 컨피그레이션이 잘못되면 스위치 프로세스가 마비될 수 있습니다.Cisco IOS 시스템 소프트웨어에는 이 문제를 방지하

기 위해 **스패닝 트리 etherchannel guard** misconfig 기능이 포함되어 있습니다.

Cisco IOS Software를 시스템 소프트웨어로 실행하는 모든 Catalyst 스위치에서 이 컨피그레이션 명령을 실행합니다.

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

기타 옵션

PAgP를 지원하지 않지만 LACP를 지원하는 두 디바이스를 채널링하는 경우, 디바이스 양쪽 끝에서 LACP 컨피그레이션을 활성화하여 LACP를 활성화하는 것이 좋습니다.자세한 내용은 이 문서의 LACP(Link Aggregation Control Protocol) 섹션을 참조하십시오.

PAgP 또는 LACP를 지원하지 않는 장치로 채널링하는 경우 채널을 하드 코드해야 합니다.이 요구 사항은 다음 예제 장치에 적용됩니다.

- 서버
- 로컬 디렉터
- 콘텐츠 스위치
- 라우터
- 이전 소프트웨어가 포함된 스위치
- Catalyst 2900XL/3500XL 스위치
- Catalyst 8540s

다음 명령을 실행합니다.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#channel-group number mode on
```

LACP(Link Aggregation Control Protocol)

LACP는 유사한 특성을 가진 포트가 인접 스위치와의 동적 협상을 통해 채널을 형성하도록 허용하는 프로토콜입니다.PAgP는 Cisco 스위치 및 라이센스 공급업체가 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.

LACP는 다음 플랫폼 및 버전에서 지원됩니다.

- Catalyst 6500/6000 Series with Cisco IOS Software 릴리스 12.1(11b)EX 이상
- Catalyst 4500 Series with Cisco IOS Software 릴리스 12.1(13)EW 이상
- Catalyst 3750 series with Cisco IOS Software 릴리스 12.1(14)EA1 이상

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

- 속도
- 이중
- 네이티브 VLAN 및 트렁킹 유형

LACP와 PAgP의 현저한 차이점은 다음과 같습니다.

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

참고: Catalyst 4500 시리즈 스위치의 경우 동일한 관리 키를 할당할 수 있는 최대 포트 수는 8개입니다.Cisco IOS Software를 실행하는 Catalyst 6500 및 3750 스위치의 경우 LACP는 EtherChannel에서 최대 호환 포트 수를 구성하려고 시도합니다. 이는 하드웨어에서 허용하는 최대 포트(8개)입니다. 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 요약입니다.

- 프로토콜은 디바이스에 의존하여 어그리게이션 기능 및 상태 정보를 광고합니다.각 집계 가능한 링크에 대해 정기적으로 전송이 전송됩니다.
- 물리적 포트가 작동 중인 경우, LACP 패킷은 탐지 중에 1초마다 전송되고 30초마다 정상 상태로 전송됩니다.
- 집계 가능한 링크의 파트너는 프로토콜 내에서 전송되는 정보를 수신하고 어떤 조치 또는 조치를 취할 것인지 결정합니다.
- 호환 가능한 포트는 하드웨어에서 허용하는 최대(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 상태에 따라 적절한 작업을 수행합니다.
- 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 집계의 관점에서 호환되는지 확인하기 위해 다음을 설정할 수 있어야 합니다.

- 링크 어그리게이션에 참여하는 각 시스템에 대한 전역 고유 식별자입니다.LACP를 실행하는 각 시스템에는 자동으로(기본 우선 순위 32768) 또는 관리자가 선택할 수 있는 우선 순위가 할당되어야 합니다.시스템 우선 순위는 시스템 식별자를 구성하기 위해 시스템의 MAC 주소와 함께 주로 사용됩니다.
- 지정된 시스템에서 이해하는 대로 각 포트 및 각 어그리게이터와 연결된 기능 집합을 식별하는 방법입니다.시스템의 각 포트에는 자동으로(기본 우선 순위가 128인 경우) 또는 관리자가 우선 순위를 할당해야 합니다.우선 순위는 포트 번호를 형성하기 위해 포트 번호와 함께 사용됩니다.
- 링크 어그리게이션 그룹 및 관련 어그리게이터를 식별하는 방법입니다.다른 포트와 집계할 수 있는 기능은 키라고 하는 0보다 엄격하게 큰 간단한 16비트 정수 매개 변수로 요약됩니다.각 키는 다음과 같은 다양한 요소를 기반으로 결정됩니다.데이터 속도, 이중성, 포인트-투-포인트 또는 공유 미디어를 포함하는 포트 물리적 특성네트워크 관리자가 설정한 구성 제약 조건각 포트에 두 개의 키가 연결됩니다.관리 키운영 키관리 키를 사용하면 관리별로 키 값을 조작할 수 있으므로 사용자가 이 키를 선택할 수 있습니다.시스템에서 운영 키를 사용하여 집계를 구성합니다.사용자는 이 키를 직접 선택하거나 변경할 수 없습니다.동일한 운영 키 값을 공유하는 특정

시스템의 포트 집합은 동일한 키 그룹의 멤버라고 합니다.
따라서 두 개의 시스템과 동일한 관리 키를 가진 포트 집합이 주어진 경우 각 시스템은 우선순위가 가장 높은 포트에서 시작하여 포트를 집계하려고 시도합니다.이러한 동작은 각 시스템이 다음 우선순위를 알고 있기 때문에 가능합니다.

- 사용자 또는 소프트웨어가 할당된 자체 우선 순위
- LACP 패킷을 통해 발견된 파트너 우선순위

장애 시 동작

LACP의 실패 동작은 PAgP의 실패 동작과 동일합니다.기존 채널의 링크에 장애가 발생한 경우(예: 포트가 분리되었거나 GBIC가 제거되었거나 파이버가 손상된 경우), 에이전트가 업데이트되고 트래픽이 1초 이내에 나머지 링크를 통해 해시됩니다.장애 후 재검색이 필요하지 않은 트래픽(동일한 링크에서 계속 전송되는 트래픽)은 손실되지 않습니다.실패한 링크를 복원하면 에이전트에 대한 다른 업데이트가 트리거되고 트래픽이 다시 해시됩니다.

구성 옵션

다음 표에 요약되어 있듯이, LACP EtherChannel을 다른 모드로 구성할 수 있습니다.

모드	구성 가능한 옵션
켜짐	LACP 협상 없이 링크 집계를 구성해야 합니다.스위치는 LACP 패킷을 전송하거나 수신 LACP 패킷을 처리하지 않습니다.인접 포트 모드가 켜져 있으면 채널이 형성됩니다.
꺼짐 또는 구성되지 않음	네이버가 구성된 방식과 상관없이 포트는 채널링되지 않습니다.
수동(기본값)	이는 PAgP의 **자동** 모드와 유사합니다.스위치는 채널을 시작하지 않지만 수신 LACP 패킷을 파악합니다.피어(활성 상태)는 스위치가 수신하고 스위치가 응답하는 협상(LACP 패킷을 전송하여)을 시작하며, 결국 피어와 어그리게이션 채널을 형성합니다.
활성	이는 PAgP의 **바람직한** 모드와 유사합니다.스위치가 총괄 링크를 형성하기 위한 협상을 시작합니다.링크 집계는 LACP 액티브 또는 패시브 모드에서 다른 엔드가 실행되는 경우 형성됩니다.

LACP는 LACP EtherChannel이 설정된 후 30초 간격 타이머(Slow_Periodic_Time)를 사용합니다.긴 시간 초과(Slow_Periodic_Time의 3배)를 사용할 때 수신된 LACPDU 정보가 무효화되기 전의 시간(초)은 90입니다. 단방향 링크의 보다 빠른 탐지기로 UDLD를 권장합니다.LACP 타이머를 조정할 수 없으며, 이 시점에서는 채널이 형성된 후 채널을 유지하기 위해 빠른 PDU(Protocol Data Unit) 전송을 사용하도록 스위치를 구성할 수 없습니다.

확인

이 섹션의 표에서는 두 개의 직접 연결된 스위치(스위치 A와 스위치 B) 간에 가능한 모든 LACP 채널링 모드 시나리오를 요약하여 설명합니다. 이러한 조합 중 일부는 EtherChannel 가드가 채널링 측면에 있는 포트를 errdisable 상태로 설정할 수 있습니다.EtherChannel 컨피그레이션 오류 가드

기능은 기본적으로 활성화되어 있습니다.

채널 모드 전환	스위치 B 채널 모드	채널 상태 전환	스위치 B 채널 상태
켜짐	켜짐	채널(비 LACP)	채널(비 LACP)
켜짐	꺼짐	채널 아님(errDisable)	채널 아님
켜짐	수동	채널 아님(errDisable)	채널 아님
켜짐	활성	채널 아님(errDisable)	채널 아님
꺼짐	꺼짐	채널 아님	채널 아님
꺼짐	수동	채널 아님	채널 아님
꺼짐	활성	채널 아님	채널 아님
수동	수동	채널 아님	채널 아님
수동	활성	LACP 채널	LACP 채널
활성	활성	LACP 채널	LACP 채널

Cisco 권장 사항

Cisco 스위치 간 채널 연결에서 PAgP를 활성화하는 것이 좋습니다.PAgP를 지원하지 않지만 LACP를 지원하는 두 디바이스를 채널링하는 경우, 디바이스 양쪽 끝에서 LACP 컨피그레이션을 활성화하여 LACP를 활성화하는 것이 좋습니다.

CatOS를 실행하는 스위치에서 Catalyst 4500/4000 및 Catalyst 6500/6000의 모든 포트는 기본적으로 PAgP 채널 프로토콜을 사용합니다.LACP를 사용하도록 포트를 구성하려면 모듈의 채널 프로토콜을 LACP로 설정해야 합니다.LACP와 PAgP는 CatOS를 실행하는 스위치에서 동일한 모듈에서 실행할 수 없습니다.이 제한은 Cisco IOS 소프트웨어를 실행하는 스위치에는 적용되지 않습니다 .Cisco IOS Software를 실행하는 스위치는 동일한 모듈에서 PAgP 및 LACP를 지원할 수 있습니다 .LACP 채널 모드를 활성으로 설정하고 관리 키 번호를 할당하려면 다음 명령을 실행합니다.

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

show etherchannel **summary** 명령은 다음 정보를 포함하는 채널 그룹당 한 줄 요약을 표시합니다.

- 그룹 번호
- 포트 채널 번호
- 포트의 상태
- 채널의 일부인 포트

show etherchannel **port-channel** 명령은 모든 채널 그룹에 대한 자세한 포트 채널 정보를 표시합니다.출력에는 다음 정보가 포함됩니다.

- 채널의 상태
- 사용되는 프로토콜
- 포트가 번들로 제공된 이후 시간

각 포트의 세부사항이 별도로 표시된 상태에서 특정 채널 그룹에 대한 자세한 정보를 표시하려면 **show etherchannel** *channel_number* **detail** 명령을 사용합니다.명령 출력에는 파트너 세부사항 및 포트 채널 세부사항이 포함됩니다.자세한 내용은 Catalyst 6500/6000과 Catalyst 4500/4000 사이에서 LACP(802.3ad) 구성을 참조하십시오.

기타 옵션

PAgP 또는 LACP를 지원하지 않는 채널 디바이스를 사용하는 경우 채널을 하드 코드해야 합니다 .이 요구 사항은 다음 장치에 적용됩니다.

- 서버
- 로컬 디렉터
- 콘텐츠 스위치
- 라우터
- 이전 소프트웨어가 설치된 스위치
- Catalyst 2900XL/3500XL 스위치
- Catalyst 8540s

다음 명령을 실행합니다.

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

단방향 링크 탐지

목적

UDLD는 디바이스 간의 단방향 통신 인스턴스를 탐지하기 위해 개발된 Cisco만의 경량 프로토콜입니다.FFI와 같은 전송 미디어의 양방향 상태를 탐지하는 다른 방법이 있습니다.그러나 레이어 1 탐지 메커니즘으로는 충분하지 않은 인스턴스가 있습니다.이러한 시나리오는 다음과 같은 결과를 가져올 수 있습니다.

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

UDLD 기능은 파이버 및 구리 이더넷 인터페이스의 이러한 결함 조건을 해결합니다.

- 물리적 케이블 컨피그레이션 모니터링 - `errDisabled`로 잘못 연결된 포트가 있으면 종료됩니다.
- 단방향 링크로부터 보호 - 미디어 또는 포트/인터페이스 오작동으로 인해 발생하는 단방향 링크를 탐지하면 영향을 받는 포트가 errDisabled로 .해당하는 syslog 메시지가 생성됩니다.
- 또한 UDLD aggressive 모드는 이전에 양방향 링크로 간주된 링크가 혼잡 때문에 사용할 수 없게 될 경우 연결이 끊어지지 않는지 확인합니다.UDLD aggressive 모드는 링크 전체에서 지속적인 연결 테스트를 수행합니다.UDLD aggressive 모드의 기본 목적은 정상 모드 UDLD로 처리되지 않는 특정 실패 조건에서 트래픽의 블랙홀링을 방지하는 것입니다.

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

스패닝 트리에는 고정 상태의 단방향 BPDU 흐름이 있으며 이 섹션에 나열되는 장애가 있을 수 있습니다.포트가 갑자기 BPDU를 전송하지 못해 STP 상태가 에서 인접 디바이스의 으로 변경될 수 있습니다.그러나 포트가 여전히 수신 가능하므로 루프가 여전히 존재합니다.

운영 개요

UDLD는 LLC 레이어(대상 MAC 01-00-0c-cc-cc-cc, SNAP HDLC 프로토콜 유형 0x0111) 위에서 작동하는 레이어 2 프로토콜입니다. FFI 및 자동 협상 레이어 1 메커니즘과 함께 UDLD를 실행할 때

링크의 물리적(L1) 및 논리적(L2) 무결성을 검증할 수 있습니다.

UDLD에는 FFI 및 자동 협상이 수행할 수 없는 기능 및 보호에 대한 규정이 있습니다.이러한 기능은 다음과 같습니다.

- 네이버 정보의 탐지 및 캐시
- 잘못 연결된 포트의 종료
- 포인트투포인트가 아닌 링크에서 논리적 인터페이스/포트 악성코드 또는 결함 탐지**참고:** 링크가 포인트투포인트가 아닌 경우 미디어 변환기 또는 허브를 통과합니다.

UDLD는 이 두 가지 기본 메커니즘을 사용합니다.

1. UDLD는 네이버에 대해 학습하고 정보를 로컬 캐시에 최신 상태로 유지합니다.
2. UDLD는 새 네이버를 탐지할 때 또는 네이버가 캐시의 재동기화를 요청할 때마다 UDLD 프로브/에코(hello) 메시지 세트를 전송합니다.

UDLD는 모든 포트에서 프로브/에코 메시지를 지속적으로 전송합니다.포트에서 해당 UDLD 메시지를 수신하면 탐지 단계 및 검증 프로세스가 트리거됩니다.모든 유효한 조건이 충족되면 포트가 활성화됩니다.포트가 양방향이고 올바르게 연결된 경우 조건이 충족됩니다.조건이 충족되지 않으면 포트가 errDisabled로 설정되며 이 syslog 메시지가 트리거됩니다.

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

UDLD 이벤트를 포함하는 기능별 시스템 메시지의 전체 목록은 UDLD 메시지(Cisco IOS 시스템 메시지, 2/2 볼륨)를 참조하십시오.

링크 및 해당 분류를 양방향(bidirectional)으로 설정한 후 UDLD는 기본 간격인 15초에 프로브/에코 메시지를 계속 광고합니다.

이 표에서는 포트 상태에 대한 정보를 제공합니다.

포트 상태	설명
확인되지 않음	탐지 진행 중/인접한 UDLD가 비활성화되었습니다.
해당 없음	UDLD가 비활성화되었습니다.
셧다운	단방향 링크가 탐지되었으며 포트가 비활성화되었습니다.
양방향	양방향 링크가 감지되었습니다.

네이버 캐시 유지 관리

UDLD는 UDLD 네이버 캐시의 무결성을 유지하기 위해 모든 액티브 인터페이스에서 hello 프로브/에코 패킷을 정기적으로 전송합니다.hello 메시지가 수신될 때 메시지는 캐시에 저장되고 최대 기간 동안 메모리에 보관되며, 이는 보류 시간으로 정의됩니다.보류 시간이 만료되면 각 캐시 항목이 오래됩니다.보류 기간 내에 새 hello 메시지가 수신되면 새 hello 메시지가 이전 항목을 대체하고 해당 TTL(time-to-live) 타이머가 재설정됩니다.

UDLD 지원 인터페이스가 비활성화되거나 디바이스가 재설정될 때마다 컨피그레이션 변경이 영향을 미치는 인터페이스의 모든 기존 캐시 엔트리가 지워집니다.이 클리어런스는 UDLD 캐시의 무결성을 유지합니다.UDLD는 해당 캐시 엔트리를 플러시할 필요성을 각 인접 디바이스에 알리기 위해 하나 이상의 메시지를 전송합니다.

에코 탐지 메커니즘

에코 메커니즘은 탐지 알고리즘의 기반을 형성합니다.UDLD 디바이스가 새 네이버에 대해 알게 되거나 동기화되지 않은 네이버에서 재동기화 요청을 수신할 때마다 해당 디바이스는 연결 측에서 탐지 창을 시작하거나 다시 시작하고 에코 메시지의 버스트를 응답으로 보냅니다.이 동작은 모든 네이버에서 동일해야 하므로 에코 발신자는 반송 메시지를 다시 수신해야 합니다.유효한 응답 메시지를 수신하지 않고 탐지 창이 종료되면 링크는 단방향으로 간주됩니다.이 시점부터 링크 재설정 또는 포트 종료 프로세스를 트리거할 수 있습니다.디바이스에서 검사하는 기타 드문 이상 조건은 다음과 같습니다.

- 동일한 포트의 Rx 커넥터에 Tx(Looed-back transmit) 파이버
- 공유 미디어 인터커넥트의 경우 불일치(예: 허브 또는 유사 디바이스)

통합 시간

STP 루프를 방지하기 위해 Cisco IOS Software Release 12.1 이상에서는 UDLD 기본 메시지 간격을 60초에서 15초로 줄였습니다.802.1D 스패닝 트리의 이전에 차단된 포트가 전달 상태로 전환되기 전에 단방향 링크를 종료하기 위해 이 간격이 변경되었습니다.메시지 간격 값은 인접 디바이스가 linkup 또는 탐지 단계 후에 UDLD 프로브를 전송하는 속도를 결정합니다.가능한 경우 일관된 컨피그레이션이 바람직하지만 메시지 간격이 링크의 양쪽 끝에서 일치할 필요는 없습니다.UDLD 인접 디바이스가 설정되면 구성된 메시지 간격이 네이버로 전송되고 해당 피어에 대한 시간 초과 간격이 다음과 같이 계산됩니다.

```
3 * (message interval)
```

따라서 피어 관계는 연속적인 3개의 hello(또는 프로브)가 누락된 후 시간 초과됩니다.메시지 간격은 양쪽에서 다르기 때문에 이 시간 제한 값은 양쪽에서 서로 다르며 한 쪽에서 오류를 더 빠르게 인식합니다.

UDLD에서 이전에 안정적인 링크의 단방향 장애를 탐지하는 데 필요한 대략적인 시간은 대략 다음과 같습니다.

```
2.5 * (message interval) + 4 seconds
```

기본 메시지 간격이 15초인 약 41초입니다.이 시간은 STP가 다시 통합되는 데 일반적으로 필요한 50초보다 훨씬 짧습니다.NMP CPU에 예비 주기가 몇 개 있고 사용자가 사용률 수준(권장 사항)을 주의 깊게 모니터링하면 메시지 간격(짝수)을 최소 7초로 줄일 수 있습니다.또한 이 메시지 간격 감소를 통해 탐지 속도가 크게 향상됩니다.

참고: Cisco IOS Software 릴리스 12.2(25)SEC의 최소 시간은 1초입니다.

따라서 UDLD에는 기본 스패닝 트리 타이머에 대한 의존 관계가 있습니다.STP가 UDLD보다 빠르게 통합되도록 튜닝된 경우 STP 루프 가드 기능과 같은 대체 메커니즘을 고려합니다.RSTP(802.1w)를 구현할 때 토폴로지에 따라 RSTP에 컨버전스 특성이 ms로 있으므로 이 경우 대체 메커니즘을 고려하십시오.이러한 경우 UDLD와 함께 루프 가드를 사용하여 가장 강력한 보호를 제공합니다.루프 가드는 사용 중인 STP 버전의 속도로 STP 루프를 방지합니다.또한 UDLD는 개별 EtherChannel 링크에서 단방향 연결을 탐지하거나 BPDU가 끊어진 방향을 따라 이동하지 않는 경

우를 처리합니다.

참고: UDLD는 STP와 독립적입니다.UDLD는 (2 * Fwddelay + maxage)보다 긴 시간 동안 BPDU를 전송하지 않는 CPU로 인해 발생하는 장애와 같이 모든 STP 장애 상황을 탐지하지 않습니다. 따라서 Cisco에서는 STP를 사용하는 토폴로지에서 루프 가드와 함께 UDLD를 구현하는 것이 좋습니다.

주의: 구성할 수 없는 60초 기본 메시지 간격을 사용하는 2900XL/3500XL 스위치의 이전 릴리스의 UDLD를 주의하십시오.스패닝 트리 루프 상태에 취약합니다.

UDLD 적극적인 모드

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

- UDLD PDU의 손실이 대칭이고 둘 다 시간 초과로 끝나는 경우이 경우, 어떤 포트도 errdisable되지 않습니다.
- 링크의 한 쪽에 포트가 고정되어 있습니다(Tx 및 Rx 모두).
- 링크의 다른 쪽이 다운된 동안 링크의 한 쪽이 작동 상태로 유지됩니다.
- Autonegotiation 또는 다른 Layer 1 결함 탐지 메커니즘이 비활성화됩니다.
- 레이어 1 FFI 메커니즘에 대한 의존도를 줄이는 것이 바람직합니다.
- 포인트-투-포인트 FE/GE 링크에서 단방향 링크 장애에 대한 최대 보호 기능이 필요합니다.특히, 두 인접 디바이스 간의 실패가 허용되지 않는 경우, UDLD-aggressive 프로브는 하트비트로 간주될 수 있으며, 이 프로브는 링크의 상태를 보장합니다.

UDLD 적극적인 구현의 가장 일반적인 사례는 자동 협상 또는 다른 레이어 1 결함 탐지 메커니즘이 비활성화되거나 사용할 수 없을 때 번들 멤버에 대해 연결 확인을 수행하는 것입니다.PAgP 및 LACP가 활성화된 경우에도 Hello 타이머가 매우 낮은 상태에서는 사용하지 않으므로 EtherChannel 연결에서 특히 유용합니다.이 경우 UDLD는 스패닝 트리 루프를 방지하는 추가적인 이점을 제공합니다.

UDLD 정상 모드에서는 링크가 양방향 상태에 도달한 후에도 단방향 링크 조건을 확인합니다 .UDLD는 STP 루프를 발생시키는 레이어 2 문제를 탐지하기 위한 것으로, 이러한 문제는 일반적으로 단방향입니다(BPDU는 한 방향에서만 일정한 상태로 흐르기 때문입니다). 따라서 자동 협상 및 루프 가드(STP에 의존하는 네트워크의 경우)와 함께 UDLD 수직을 사용하는 것은 거의 항상 충분합니다.UDLD 적극적인 모드가 활성화되면, 알림 또는 탐지 단계에서 포트의 모든 네이버가 에이징된 후, UDLD 적극적인 모드는 동기화되지 않은 네이버와 재동기화하기 위해 링크 시퀀스를 재시작합니다.빠른 메시지 전달(8회 재시도 실패) 후에도 링크가 확인되지 않은 것으로 간주될 경우 포트는 errdisable 상태로 전환됩니다.

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

UDLD 링크 자동 복구

Errdisable 복구는 기본적으로 전역적으로 비활성화되어 있습니다.전역적으로 활성화된 후 포트가 errdisable 상태로 전환되면 선택한 시간 간격이 지나면 자동으로 다시 활성화됩니다.기본 시간은 300초이며, 이는 전역 타이머이며 스위치의 모든 포트에 대해 유지됩니다.소프트웨어 릴리스에 따라 UDLD에 대한 errdisable timeout 복구 메커니즘을 사용하여 해당 포트에 대한 errdisable 시간 제한을 비활성화하도록 설정한 경우 포트 재활성화를 수동으로 방지할 수 있습니다.

```
Switch(config)#errdisable recovery cause udld
```

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 상태의 포트에 대한 시간 제한 기간을 구성하는 방법에 대한 자세한 내용은 errdisable recovery(Catalyst 6500 Series Cisco IOS Command Reference, 12.1E)를 참조하십시오.

액세스 스위치가 캠퍼스 환경에 배포되고 두 업링크를 다시 활성화하기 위해 각 스위치를 수동으로 방문할 경우 액세스 레이어의 UDLD에 오류 비활성화 복구가 특히 중요할 수 있습니다.

일반적으로 코어에 여러 진입점이 있고 코어에 자동 복구가 반복적인 문제로 이어질 수 있으므로 Cisco는 네트워크 코어에서 errdisable 복구를 권장하지 않습니다.따라서 UDLD가 포트를 비활성화하는 경우 코어에서 포트를 수동으로 다시 활성화해야 합니다.

라우티드 링크의 UDLD

이 논의에서 라우티드 링크는 다음 두 연결 유형 중 하나입니다.

- 두 라우터 노드 간 포인트 투 포인트(30비트 서브넷 마스크로 구성)
- 여러 포트가 있지만 스플릿 레이어 2 코어 토폴로지와 같이 라우팅된 연결만 지원하는 VLAN

각 IGRP(Interior Gateway Routing Protocol)는 네이버 관계 및 경로 컨버전스를 처리하는 방식과 관련하여 고유한 특성을 가집니다.이 섹션에서는 이 논의와 관련된 특징에 대해 설명하며, 이는 오늘날 사용되는 보다 일반적인 라우팅 프로토콜 중 두 가지, 즉 OSPF(Open Shortest Path First) 프로토콜과 EIGRP(Enhanced IGRP)를 비교합니다.

참고: 포인트 투 포인트 라우티드 네트워크에서 레이어 1 또는 레이어 2 오류가 발생하면 레이어 3 연결이 거의 즉시 해제됩니다.해당 VLAN의 유일한 스위치 포트는 레이어 1/레이어 2 장애 시 연결되지 않은 상태로 전환되므로 인터페이스 자동 상태 기능은 약 2초 내에 레이어 2 및 레이어 3 포트 상태를 동기화하고 레이어 3 VLAN 인터페이스를 작동/중단 상태(라인 프로토콜은 작동 중지 중)로 배치합니다.

기본 타이머 값을 가정할 경우 OSPF는 10초마다 hello 메시지를 전송하고 40초(4 * hello)의 데드 간격을 가집니다. 이러한 타이머는 OSPF 포인트-투-포인트 및 브로드캐스트 네트워크에 일관됩니다.OSPF는 인접성을 형성하기 위해 양방향 통신이 필요하므로, 최악의 경우 장애 조치 시간은 40초입니다.이는 Point-to-Point 연결에서 레이어 1/Layer 2 장애가 순수하지 않고 레이어 3 프로토콜이 처리해야 하는 반올림 시나리오를 남겨두는 경우에도 마찬가지입니다.UDLD의 탐지 시간은 OSPF 데드 타이머가 만료되는 탐지 시간(약 40초)과 매우 유사하기 때문에 OSPF Layer 3 포인트-투-포인트 링크에서 UDLD 일반 모드를 구성할 경우 이점이 제한됩니다.

대부분의 경우 EIGRP는 OSPF보다 빠르게 통합됩니다.그러나 인접 디바이스에서 라우팅 정보를 교환하기 위해서는 양방향 통신이 필요하지 않다는 점에 유의해야 합니다.매우 특정한 반구화된 장애 시나리오에서 EIGRP는 일부 다른 이벤트가 해당 인접 디바이스를 통해 경로를 활성화할 때까지 지속되는 트래픽의 블랙홀링에 취약합니다.UDLD 일반 모드는 단방향 링크 장애를 탐지하고 오류가 발생하면 포트가 비활성화되므로 이러한 상황을 완화시킬 수 있습니다.

라우팅 프로토콜을 사용하는 레이어 3 라우티드 연결의 경우 UDLD Normal은 초기 링크 활성화 시 발생하는 오류(예: 케이블링 오류 또는 하드웨어 오류)로부터 보호합니다.또한 UDLD 적극적인 모드는 레이어 3 라우팅 연결에서 다음과 같은 이점을 제공합니다.

- 트래픽의 불필요한 블랙홀 방지(경우에 따라 최소 타이머가 필요함)
- 플래핑 링크를 errdisable 상태로 설정합니다.
- 레이어 3 EtherChannel 컨피그레이션에서 발생하는 루프를 차단합니다.

UDLD의 기본 동작

UDLD는 전역적으로 비활성화되며 기본적으로 파이버 포트에서 준비도 상태로 활성화됩니다 .UDLD는 스위치 간에 필요한 인프라 프로토콜이므로, UDLD는 호스트 액세스에 사용되는 구리 포트에서 기본적으로 비활성화되어 있습니다.인접 디바이스가 양방향 상태를 달성하려면 먼저 UDLD를 전역적으로 그리고 인터페이스 레벨에서 활성화해야 합니다.기본 메시지 간격은 15초입니다.그러나 경우에 따라 기본 메시지 간격은 7초로 표시될 수 있습니다.자세한 내용은 Cisco 버그 ID CSCea70679 (등록된 고객만 해당)를 참조하십시오.기본 메시지 간격은 7초에서 90초 사이로 구성할 수 있으며 UDLD aggressive 모드는 비활성화됩니다.Cisco IOS Software 릴리스 12.2(25)SEC는 이 최소 타이머를 1초로 더 줄입니다.

Cisco 구성 권장 사항

대부분의 경우 Cisco 스위치 간 모든 포인트-투-포인트 FE/GE 링크에서 UDLD 일반 모드를 활성화하고 기본 802.1D 스패닝 트리 타이머를 사용할 때 UDLD 메시지 간격을 15초로 설정하는 것이 좋습니다.또한 리던던시 및 컨버전스를 위해 네트워크가 STP를 사용하는 경우(즉, 토폴로지에 STP 차단 상태가 하나 이상 있는 경우), 적절한 기능 및 프로토콜과 함께 UDLD를 사용합니다.이러한 기능에는 FFI, 자동 협상, 루프 가드 등이 포함됩니다.자동 협상이 활성화된 경우, 자동 협상이 레이어 1에서 결함 탐지를 보완하므로 적극적인 모드가 필요하지 않습니다.

UDLD를 활성화하려면 다음 두 명령 옵션 중 하나를 실행합니다.

참고: 구문은 여러 플랫폼/버전에서 변경되었습니다.

- ```
  udld enable
  !--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
  udld port
  ```

  또는

- ```
  udld enable
  !--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
  by individual port command.
  ```

단방향 링크 증상으로 인해 종료된 포트를 수동으로 활성화해야 합니다.다음 방법 중 하나를 사용합니다.

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

errdisable **recovery cause udld** 및 errdisable **recovery interval** ***interval*** **전역 컨피그레이션 명령을 사용하여 UDLD error-disabled 상태에서 자동으로 복구할 수 있습니다.**

스위치에 대한 물리적 액세스가 어려운 경우, 복구 타이머가 20분 이상인 네트워크의 액세스 레이어에서만 errdisable 복구 메커니즘을 사용하는 것이 좋습니다.가장 좋은 상황은 포트가 다시 온라

인 상태가 되어 네트워크 불안정을 일으키기 전에 네트워크 안정화와 문제 해결 시간을 허용하는 것입니다.

Cisco에서는 네트워크 코어에서 복구 메커니즘을 사용하지 *않는* 것이 좋습니다. 이로 인해 장애가 발생한 링크가 백업될 때마다 컨버전스 이벤트와 관련된 불안정성이 발생할 수 있기 때문입니다.코어 네트워크의 이중화된 설계에서는 장애가 발생한 링크에 대한 백업 경로를 제공하고 UDLD 장애 원인을 조사하는 데 시간을 허용합니다.

STP 루프 가드 없이 UDLD 사용

루프 프리(loop-free) STP 토폴로지(포트 차단 없음)가 있는 레이어 3 포인트-투-포인트 또는 레이어 2 링크의 경우 Cisco 스위치 간 포인트-투-포인트 FE/GE 링크에서 적극적인 UDLD를 활성화하는 것이 좋습니다.이 경우 메시지 간격이 7초로 설정되고 802.1D STP는 기본 타이머를 사용합니다.

EtherChannel의 UDLD

STP 루프 가드의 구축 또는 구축 여부에 관계없이, 원하는 채널 모드와 함께 모든 EtherChannel 컨피그레이션에 대해 UDLD 적극적인 모드를 사용하는 것이 좋습니다.EtherChannel 컨피그레이션에서 스패닝 트리 BPDU와 PAgP 제어 트래픽을 전달하는 채널 링크의 장애가 발생하면 채널 링크가 번들되지 않으면 채널 파트너 간에 즉시 루프가 발생할 수 있습니다.UDLD aggressive 모드는 장애가 발생한 포트를 종료합니다.그런 다음 PAgP(자동/권장 채널 모드)는 새 제어 링크를 협상하고 채널에서 장애가 발생한 링크를 효과적으로 제거할 수 있습니다.

802.1w 스패닝 트리가 포함된 UDLD

새 스패닝 트리 버전을 사용할 때 루프를 방지하려면 UDLD 일반 모드 및 STP 루프 가드와 802.1w와 같은 RSTP를 사용합니다.UDLD는 링크 업 단계 중에 단방향 링크로부터 보호 기능을 제공할 수 있으며, STP 루프 가드는 UDLD가 링크를 양방향으로 설정한 *후* 링크가 단방향으로 되는 경우 STP 루프를 방지할 수 있습니다.UDLD를 기본 802.1w 타이머보다 작게 구성할 수 없으므로 중복 토폴로지에서 루프를 완전히 방지하려면 STP 루프 가드가 필요합니다.

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

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, 원하는 `errdisable` 상태를 확인하기 위해 파이버 한 가닥의 연결을 끊는 것과 같은 간단한 테스트를 수행할 경우 먼저 레이어 1 자동 협상을 해제해야 합니다.그렇지 않으면 물리적 포트가 UDLD 메시지 통신이 재설정됩니다.원격 끝은 UDLD 일반 모드 않은 상태로 이동하고 UDLD 적극적인 모드를 사용하는 경우에만 errdisable 상태로 이동합니다.

추가 테스트 방법은 UDLD에 대한 네이버 PDU 손실을 시뮬레이션합니다.UDLD/CDP 하드웨어 주소를 차단하는 동시에 다른 주소를 전달할 수 있도록 MAC 레이어 필터를 사용하는 방법이 있습니다.포트가 SPAN(Switched Port Analyzer) 대상으로 구성된 경우 일부 스위치는 UDLD 프레임을 전송하지 않으며, 이는 응답하지 않는 UDLD 인접 디바이스를 시뮬레이션합니다.

UDLD를 모니터링하려면 다음 명령을 사용합니다.

```
show udld gigabitethernet1/1
```

```
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

또한 Cisco IOS Software Release 12.2(18)SXD 이상 스위치의 활성화 모드에서 UDLD 캐시 내용(CDP와 같은 방식)을 확인하기 위해 **show udld neighbor** 명령을 실행할 수 있습니다. 프로토콜별 이상 징조가 있는지 확인하기 위해 UDLD 캐시를 CDP 캐시와 비교하는 것이 매우 유용합니다 .CDP도 영향을 받을 때마다 일반적으로 모든 BPDU/PDU에 영향을 줍니다.따라서 STP도 확인합니다.예를 들어, 최근 루트 ID 변경 또는 루트/지정 포트 배치 변경 사항을 확인합니다.

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

멀티레이어 스위칭

개요

Cisco IOS 시스템 소프트웨어에서 MLS(Multilayer Switching)는 Catalyst 6500/6000 시리즈에서 지원되며 내부에서만 지원됩니다.즉, 라우터가 스위치에 설치되어야 합니다.최신 Catalyst 6500/6000 Supervisor Engine은 라우팅 테이블이 각 카드에 다운로드되는 MLS CEF를 지원합니다.여기에는 DFC(Distributed Forwarding Card)가 포함된 추가 하드웨어가 필요합니다.라우터 카드에서 Cisco IOS Software를 사용하도록 선택한 경우에도 CatOS 소프트웨어에서 DFC가 지원되지 않습니다 .DFC는 Cisco IOS 시스템 소프트웨어에서만 지원됩니다.

Catalyst 스위치에서 NetFlow 통계를 활성화하는 데 사용되는 MLS 캐시는 Supervisor Engine I 카드와 레거시 Catalyst 스위치가 레이어 3 스위칭을 활성화하기 위해 사용하는 플로우 기반 캐시입니다.MLS는 MSFC 또는 MSFC2가 있는 Supervisor Engine 1(또는 Supervisor Engine 1A)에서 기본적으로 활성화됩니다. 기본 MLS 기능에는 추가 MLS 구성이 필요하지 않습니다.다음 세 가지 모드 중 하나로 MLS 캐시를 구성할 수 있습니다.

- 대상
- 소스 대상
- 소스 대상 포트

흐름 마스크는 스위치의 MLS 모드를 결정하는 데 사용됩니다.이러한 데이터는 이후에 Supervisor Engine IA 프로비저닝 Catalyst 스위치에서 레이어 3 플로우를 활성화하는 데 사용됩니다 .Supervisor Engine II 블레이드는 패킷을 전환하기 위해 MLS 캐시를 사용하지 않습니다. 이 카드는 훨씬 더 확장성이 뛰어난 하드웨어 CEF 지원 기술이기 때문입니다.MLS 캐시는 NetFlow 통계 내보내기만 활성화하려면 Supervisor Engine II 카드에서 유지됩니다.따라서 Supervisor Engine II는 필요한 경우 스위치에 부정적인 영향 없이 전체 플로우에 대해 활성화할 수 있습니다.

구성

MLS 에이징 시간은 모든 MLS 캐시 항목에 적용됩니다.에이징 타임 값은 대상 모드 에이징에 직접 적용됩니다.MLS 에이징 시간 값을 2로 나누어 소스-대상 모드 에이징 시간을 파생합니다.전체 플로우 에이징 시간을 찾으려면 MLS 에이징 타임 값을 8로 나눕니다.기본 MLS 에이징 타임 값은 256초입니다.

8초 단위로 32~4092초 범위에서 정상 에이징 시간을 구성할 수 있습니다.8초의 배수가 아닌 에이

징 타임 값은 가장 가까운 8초의 배수로 조정됩니다.예를 들어, 65 값은 64로 조정되고 127 값은 128로 조정됩니다.

다른 이벤트로 인해 MLS 항목이 삭제될 수 있습니다.이러한 이벤트는 다음과 같습니다.

- 라우팅 변경
- 링크 상태의 변경예를 들어 PFC 링크는 다운되었습니다.

MLS 캐시 크기를 32,000개 항목 미만으로 유지하려면 mls aging 명령을 실행한 후 다음 매개변수를 **활성화합니다.**

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

구성

제거된 일반적인 캐시 항목은 DNS(Domain Name Server) 또는 TFTP 서버와의 플로우에 대한 엔트리이며, 엔트리를 생성한 후에는 다시 사용할 수 없습니다.이러한 항목을 탐지하고 제어하면 다른 데이터 트래픽에 대한 MLS 캐시의 공간이 절약됩니다.

MLS 빠른 에이징 시간을 활성화해야 하는 경우 초기 값을 128초로 설정합니다.MLS 캐시 크기가 32,000개 항목을 계속 초과하는 경우 캐시 크기가 32,000개 미만으로 유지될 때까지 설정을 줄입니다. 캐시가 32,000개 항목을 계속 증가시키면 일반 MLS 에이징 시간을 줄입니다.

Cisco 권장 MLS 구성

NetFlow 내보내기가 필요하지 않은 경우 MLS를 기본값인 대상으로만 유지합니다.NetFlow가 필요한 경우 Supervisor Engine II 시스템에서만 MLS 전체 흐름을 활성화합니다.

MLS 흐름 대상을 활성화하려면 다음 명령을 실행합니다.

```
Switch(config)#mls flow ip destination
```

접보 프레임

최대 전송 단위

MTU(Maximum Transmission Unit)는 인터페이스에서 패킷을 조각화하지 않고 보내거나 받을 수 있는 최대 데이터그램 또는 패킷 크기(바이트)입니다.

IEEE 802.3 표준에 따라 최대 이더넷 프레임 크기는 다음과 같습니다.

- 일반 프레임용 **1518바이트**(1500바이트 + 18바이트의 이더넷 헤더 및 CRC 트레일러 추가)
- 802.1Q 캡슐화된 프레임(1518바이트 + 태그 4바이트)

베이비 자이언츠:Baby Giants 기능을 사용하면 스위치에서 IEEE 이더넷 MTU보다 약간 큰 패킷을 전달하여 프레임을 과도하게 선언하고 폐기할 수 있습니다.

점보:프레임 크기는 IEEE 표준의 일부가 아니므로 프레임 크기의 정의는 공급업체에 따라 다릅니다.점보 프레임은 표준 이더넷 프레임 크기(1518바이트, 레이어 2 헤더 및 프레임 검사 시퀀스[FCS] 포함)보다 큰 프레임입니다.

개별 포트에서 점보 프레임 지원이 활성화된 후 기본 MTU 크기는 9216바이트입니다.

1518바이트보다 큰 패킷을 예상하는 경우

스위치드 네트워크를 통해 트래픽을 전송하려면 전송된 트래픽 MTU가 스위치 플랫폼에서 지원되는 트래픽을 초과하지 않아야 합니다.특정 프레임의 MTU 크기를 잘라낼 수 있는 이유는 다양합니다.

- **공급업체별 요구 사항**—애플리케이션 및 특정 NIC는 표준 1500바이트 외부에 있는 MTU 크기를 지정할 수 있습니다.이러한 변화는 이더넷 프레임의 크기가 증가하면 평균 처리량이 증가할 수 있다는 연구 결과 때문입니다.
- **트렁킹** - 스위치나 다른 네트워크 디바이스 간에 VLAN ID 정보를 전달하기 위해 트렁킹을 사용하여 표준 이더넷 프레임을 보강했습니다.오늘날 가장 일반적인 두 가지 트렁킹 형식은 다음과 같습니다.Cisco 전용 ISL 캡슐화802.1q
- **MPLS(Multiprotocol Label Switching)** - 인터페이스에서 MPLS를 활성화하면 MPLS는 패킷의 프레임 크기를 늘릴 수 있습니다. 이는 MPLS 태그 패킷의 레이블 스택에 있는 레이블 수에 따라 달라집니다.레이블의 총 크기는 4바이트입니다.레이블 스택의 총 크기는 다음과 같습니다.
  ```
  n * 4 bytes
  ```
  레이블 스택이 형성되면 프레임이 MTU를 초과할 수 있습니다.
- **802.1Q 터널링**—802.1Q 터널링 패킷에는 802.1Q 태그 2개가 포함되며, 이 중 한 개만 일반적으로 하드웨어에 표시됩니다.따라서 내부 태그는 MTU 값(페이로드 크기)에 4바이트를 추가합니다.
- **UTI(Universal Transport Interface)/Layer 2 Tunneling Protocol Version 3(Layer 2TPv3)** - UTI/Layer 2TPv3은 IP 네트워크를 통해 전달할 레이어 2 데이터를 캡슐화합니다.UTI/Layer 2TPv3는 원래 프레임 크기를 최대 50바이트까지 늘릴 수 있습니다.새 프레임에는 새 IP 헤더(20바이트), 레이어 2TPv3 헤더(12바이트) 및 새 레이어 2 헤더가 포함됩니다.레이어 2TPv3 페이로드는 레이어 2 헤더를 포함하는 전체 레이어 2 프레임으로 구성됩니다.

목적

고속(1Gbps 및 10Gbps) 하드웨어 기반 스위칭은 점보 프레임을 최적 상태가 아닌 처리량 문제를 해결하기 위한 매우 구체적인 솔루션으로 만들었습니다.점보 프레임 크기에 대한 공식적인 표준은 없지만, 필드에서 자주 사용되는 꽤 일반적인 값은 9216바이트(9KB)입니다.

네트워크 효율성 고려 사항

페이로드 크기를 오버헤드 값과 페이로드 크기의 합계로 나누는 경우 패킷 전달의 네트워크 효율성을 계산할 수 있습니다.

점보 프레임으로 네트워킹 효율성이 약간 증가하고 94.9%(1500바이트)에서 99.1%(9216바이트)로 이동하는 경우에도 네트워크 디바이스 및 최종 호스트의 처리 오버헤드(CPU 사용률)가 패킷 크기

에 비례하여 감소합니다.따라서 고성능 LAN 및 WAN 네트워킹 기술이 훨씬 큰 프레임 크기를 선호하는 경향이 있습니다.

성능 향상은 긴 데이터 전송이 수행되는 경우에만 가능합니다.애플리케이션의 예는 다음과 같습니다.

- 서버 백투백 통신(예: NFS[Network File System] 트랜잭션)
- 서버 클러스터링
- 고속 데이터 백업
- 고속 수퍼컴퓨터 상호 연결
- 그래픽 애플리케이션 데이터 전송

네트워크 성능 고려 사항

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

- MTU 길이에서 TCP/IP 헤더의 길이를 뺀 최대 세그먼트 크기(MSS)
- 왕복 시간(RTT)
- 패킷 손실

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

이 공식에 따르면, 달성 가능한 최대 TCP 처리량은 MSS에 직접 비례합니다.즉, RTT와 패킷 손실이 일정하므로 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.

운영 개요

IEEE 802.3 표준 사양은 최대 이더넷 프레임 크기 **1518**을 정의합니다.길이가 1519에서 1522바이트 사이인 802.1Q 캡슐화된 프레임은 IEEE Std 802.3ac-1998 추록을 통해 이후 단계에서 802.3 사양에 추가되었습니다.그들은 종종 문학에서 **거대 아기**로 언급된다.

일반적으로 패킷은 특정 이더넷 연결에 대해 지정된 이더넷 최대 길이를 초과할 때 **큰 프레임**으로 분류됩니다.대형 패킷은 **점보 프레임이라고도 합니다**.

점보 프레임에 대한 혼동의 주요 요점은 다음과 같습니다.서로 다른 인터페이스는 서로 다른 최대 패킷 크기를 지원하며, 경우에 따라 큰 패킷을 약간 다른 방식으로 처리합니다.

Catalyst 6500 시리즈

이 표에서는 Catalyst 6500 플랫폼의 다른 카드가 현재 지원하는 MTU 크기를 요약하려고 합니다.

라인 카드	MTU 크기
기본값	9216바이트
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X8644644 RJ45V, WS-X6348-RJ-21 및 WX-X6348-RJ21V	8092바이트 (PHY 칩에 의해 제한됨)

WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF 및 WS-X6148-21AF	9100바이트 (100Mbps) 9216바이트 (10Mbps)
WS-X6516-GE-TX	8092바이트 (100Mbps) 9216바이트(10 또는 1000Mbps)
WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX 및 WS-X6548-GE-45AF	1500바이트
OSM ATM(OC12c)	9180바이트
OSM CHOC3, CHOC12, CHOC48 및 CT3	9216바이트 (OCx 및 DS3) 7673바이트 (T1/E1)
FlexWAN	7673바이트 (CT3 T1/DS0) 9216바이트 (OC3c POS) 7673바이트(T1)
WS-X6148-GE-TX 및 WS-X6548-GE-TX	지원 없음

자세한 내용은 이더넷, 고속 이더넷, 기가비트 이더넷 및 10기가비트 이더넷 스위칭 구성을 참조하십시오.

Catalyst 6500/6000 Cisco IOS Software에서 레이어 2 및 레이어 3 점보 지원

레이어 2 및 레이어 3 물리적 인터페이스로 구성된 모든 GE 포트에는 PFC/MSFC1, PFC/MSFC2 및 PFC2/MSFC2를 사용하는 레이어 2 및 레이어 3 점보 지원이 있습니다.은(는) 이러한 포트가 트렁킹 또는 채널링 중인지에 관계없이 존재합니다.이 기능은 Cisco IOS Software 릴리스 12.1.1E 이상에서 사용할 수 있습니다.

- 모든 점보 지원 물리적 포트의 MTU 크기가 함께 연결되어 있습니다.그 중 하나를 변경하면 모두 변경됩니다.점보 프레임 MTU 크기는 항상 활성화한 후에 유지합니다.
- 컨피그레이션 중에 점보 활성화와 동일한 VLAN의 모든 포트를 활성화하거나 점보 활성화가 활성화된 포트를 모두 활성화하지 마십시오.
- SVI(Switched Virtual Interface)(VLAN 인터페이스) MTU 크기는 물리적 포트 MTU와 별도로 설정됩니다.물리적 포트 MTU가 변경되어도 SVI MTU 크기는 변경되지 않습니다.또한 SVI MTU의 변경 사항은 물리적 포트 MTU에 영향을 주지 않습니다.
- FE 인터페이스에서 레이어 2 및 레이어 3 점보 프레임 지원은 Cisco IOS Software Release 12.1(8a) EX01에서 시작되었습니다. mtu **1500** 명령은 FE에서 점보를 비활성화하고 mtu **9216** 명령은 FE에서 점보를 활성화합니다.Cisco 버그 ID CSCdv90450 (등록된 고객만 해당)을 참조하십시오.
- VLAN 인터페이스의 레이어 3 점보 프레임은 다음에서만 지원됩니다.PFC/MSFC2(Cisco IOS Software 릴리스 12.1(7a)E 이상)PFC2/MSFC2(Cisco IOS Software 릴리스 12.1(8a)E4 이상)
- MSFC1에서는 프래그먼트화를 원하는 대로 처리할 수 없으므로 PFC/MSFC1과 함께 VLAN 인터페이스(SVI)에 점보 프레임을 사용하지 않는 것이 좋습니다.

- 동일한 VLAN(Layer 2 점보) 내의 패킷에 대해서는 프래그먼트화가 지원되지 않습니다.
- VLAN/서브넷 간 프래그먼트화가 필요한 패킷(레이어 3 점보)은 프래그먼트화를 위해 소프트웨어로 전송됩니다.

Catalyst 6500/6000 Cisco IOS 소프트웨어의 점보 프레임 지원 이해

점보 프레임은 기본 이더넷 프레임 크기보다 큰 프레임입니다.점보 프레임 지원을 활성화하려면 포트 또는 VLAN 인터페이스에서 기본값보다 큰 MTU 크기를 구성하고 Cisco IOS Software 릴리스 12.1(13)E 이상을 사용하여 전역 LAN 포트 MTU 크기를 구성합니다.

Cisco IOS Software에서 연결 및 라우팅된 트래픽 크기 확인

라인 카드	인그레스	이그레스
10, 10/100, 100 Mbps 포트	MTU 크기 검사가 완료되었습니다.점보 프레임 지원은 인그레스 트래픽 크기를 인그레스 10, 10/100 및 100Mbps 이더넷 및 기본이 아닌 MTU 크기가 구성된 10GE LAN 포트의 전역 LAN 포트 MTU 크기와 비교합니다.포트가 너무 큰 트래픽을 삭제합니다.	MTU 크기 검사가 완료되지 않았습니다.기본이 아닌 MTU 크기로 구성된 포트는 64바이트보다 큰 패킷을 포함하는 전송 프레임을 전송합니다.기본이 아닌 MTU 크기가 구성된 경우 10, 10/100 및 100Mbps 이더넷 LAN 포트는 큰 이그레스 프레임을 확인하지 않습니다.
GE 포트	MTU 크기 검사가 완료되지 않았습니다.기본이 아닌 MTU 크기로 구성된 포트는 64바이트보다 큰 패킷이 포함된 프레임을 수락하고 크기가 큰 인그레스 프레임을 확인하지 않습니다.	MTU 크기 검사가 완료되었습니다.점보 프레임 지원은 이그레스(egress) GE의 전역 이그레스(egress) LAN 포트 MTU 크기와 기본이 아닌 MTU 크기가 구성된 10GE LAN 포트를 비교합니다.포트가 너무 큰 트래픽을 삭제합니다.
10GE 포트	MTU 크기 검사가 완료되었습니다.포트가 너무 큰 트래픽을 삭제합니다.	MTU 크기 검사가 완료되었습니다.포트가 너무 큰 트래픽을 삭제합니다.
SVI	MTU 크기 검사가 완료되지 않았습니다.SVI는 인그레스 측의 프레임 크기를 확인하지 않습니다.	MTU 크기 검사가 완료되었습니다.SVI의 이그레스 측에서 MTU 크기를 확인합니다.
	PFC	
모든 라	라우팅해야 하는 트래픽의 경우, PFC의 점보 프레임 지원은 트래픽 크기를 구성된 MTU 크기와 비교하고, 트래픽을 수용하기에 충분한 크기의 MTU 크기로	

우팅된 트래픽	구성된 인터페이스 간의 점보 트래픽을 위한 레이어 3 스위칭을 제공합니다.충분한 MTU 크기로 구성되지 않은 인터페이스 간: • DF(Don't Fragment) 비트가 설정되지 않은 경우 PFC는 소프트웨어에서 프래그먼트되고 라우팅되기 위해 트래픽을 MSFC로 전송합니다. • DF 비트가 설정된 경우 PFC는 트래픽을 삭제합니다.

Cisco 권장 사항

제대로 구현된 경우 점보 프레임은 이더넷 연결의 TCP 처리량이 6배 향상될 수 있으며, 프래그먼트화 오버헤드가 감소하고 엔드 디바이스의 CPU 오버헤드가 줄어듭니다.

이 사이에 지정된 MTU 크기를 처리할 수 없는 장치가 없는지 확인해야 합니다.이 디바이스가 패킷을 프래그먼트하고 포워딩하는 경우 전체 프로세스가 무효화됩니다.이로 인해 패킷의 프래그먼트화 및 리어셈블을 위해 이 디바이스에 오버헤드가 추가될 수 있습니다.

이러한 경우 IP 경로 MTU 검색을 통해 발신자는 각 경로를 따라 트래픽을 전송하는 데 적합한 최소 공통 패킷 길이를 찾을 수 있습니다.또는 네트워크에서 지원되는 모든 디바이스 중 최소 MTU 크기의 점보 프레임 인식 호스트 디바이스를 구성할 수 있습니다.

MTU 크기를 지원할 수 있는지 확인하려면 각 디바이스를 신중하게 확인해야 합니다.이 섹션의 MTU 크기 지원 테이블을 참조하십시오.

점보 프레임 지원은 다음 유형의 인터페이스에서 활성화할 수 있습니다.

- 포트 채널 인터페이스
- SVI
- 물리적 인터페이스(레이어 2/레이어 3)

포트 채널이나 포트 채널에 참여하는 물리적 인터페이스에서 점보 프레임을 활성화할 수 있습니다.모든 물리적 인터페이스의 MTU가 동일한지 확인해야 합니다.그렇지 않으면 일시 중단된 인터페이스가 발생할 수 있습니다.모든 멤버 포트의 MTU가 변경되므로 포트 채널 인터페이스의 MTU를 변경해야 합니다.

참고: 멤버 포트가 차단 포트이므로 멤버 포트의 MTU를 새 값으로 변경할 수 없는 경우 포트 채널이 일시 중단됩니다.

SVI에서 점보 프레임 지원을 구성하기 전에 VLAN의 모든 물리적 인터페이스가 점보 프레임에 대해 구성되었는지 항상 확인합니다.패킷의 MTU는 SVI의 인그레스 측에서 확인되지 않습니다.그러나 SVI의 이그레스 쪽에서 확인됩니다.패킷 MTU가 이그레스 SVI MTU보다 클 경우, 패킷은 소프트웨어에 의해 조각화되어(DF 비트가 설정되지 않은 경우) 성능이 저하됩니다.소프트웨어 단편화는 레이어 3 스위칭에만 발생합니다.패킷이 더 작은 MTU로 레이어 3 포트 또는 SVI로 전달되면 소프트웨어 단편화가 발생합니다.

SVI의 MTU는 항상 VLAN의 모든 스위치 포트 중에서 가장 작은 MTU보다 작아야 합니다.

Catalyst 4500 시리즈

점보 프레임은 Catalyst 4500 라인 카드의 비차단 포트에서 주로 지원됩니다.이러한 비차단 GE 포트는 Supervisor Engine 스위칭 패브릭에 직접 연결되어 있으며 점보 프레임을 지원합니다.

- 수퍼바이저 엔진WS-X4515, WS-X4516 - Supervisor Engine IV 또는 V의 업링크 GBIC 포트 2개WS-X4516-10GE—10GE 업링크 2개 및 1GE SFP(Small Form Factor Pluggable) 업링크 4개WS-X4013+—1GE 업링크 2개WS-X4013+10GE—10GE 업링크 2개 및 1GE SFP 업링크 4개WS-X4013+TS—1-GE 포트 20개
- 라인 카드WS-X4306-GB—6포트 1000BASE-X(GBIC) GE 모듈WS-X4506-GB-T—6포트 10/100/1000Mbps 및 6포트 SFPWS-X4302-GB—2포트 1000BASE-X(GBIC) GE 모듈WS-X4232-GB-RJ 모듈의 18포트 서버 스위칭 GE 모듈(WS-X4418-GB) 및 GBIC 포트 중 처음 2개
- 고정 구성 스위치WS-C4948—모두 48개의 1GE 포트WS-C4948-10GE - 모든 1-GE 포트 48개와 10-GE 포트 2개

이러한 비차단 GE 포트를 사용하여 9KB 점보 프레임 또는 하드웨어 브로드캐스트 억제(Supervisor Engine IV만 해당)를 지원할 수 있습니다. 다른 모든 라인 카드는 아기 거대한 프레임을 지원합니다.MPLS의 브리징 또는 Q의 패스스루(최대 페이로드 1552바이트)에 아기 거스를 사용할 수 있습니다.

참고: 프레임 크기는 ISL/802.1Q 태그로 증가합니다.

Supervisor Engines IV 및 V를 사용하는 다른 Cisco IOS 기능에는 대형 아기 프레임 및 점보 프레임이 투명하게 표시됩니다.

Cisco IOS Software 보안 기능

기본 보안 기능

한때 캠퍼스 설계에서는 보안이 간과되는 경우가 많았습니다.하지만 보안은 이제 모든 엔터프라이즈 네트워크의 필수 요소입니다.일반적으로 클라이언트는 Cisco의 어떤 툴과 기술을 적용할 수 있는지를 정의하는 데 도움이 되는 보안 정책을 이미 수립했습니다.

기본 암호 보호

대부분의 Cisco IOS 소프트웨어 디바이스는 두 가지 비밀번호 레벨로 구성됩니다.첫 번째 레벨은 vty 액세스라고도 하는 디바이스에 대한 텔넷 액세스를 위한 것입니다.vty 액세스가 부여되면 활성화 모드 또는 특별 권한 exec 모드에 대한 액세스 권한이 필요합니다.

스위치의 활성화 모드 보호

enable 비밀번호는 사용자가 디바이스에 대한 완전한 액세스를 얻을 수 있도록 합니다.enable 비밀번호를 신뢰할 수 있는 사람에게만 지정합니다.

```
Switch(config)#enable secret password
```

비밀번호가 다음 규칙을 따라야 합니다.

- 비밀번호는 1~25자의 대문자 및 소문자 영숫자를 포함해야 합니다.
- 비밀번호는 첫 번째 문자로 숫자를 가질 수 없습니다.
- 선행 공백을 사용할 수 있지만 무시됩니다.중간 및 후행 공백을 인식합니다.
- 비밀번호 확인은 대/소문자를 구분합니다.예를 들어, 비밀번호 Secret은 비밀번호 비밀번호와 다릅니다.

참고: enable **secret** 명령은 단방향 암호화 MD5(Message Digest 5) 해싱 기능을 사용합니다.show

running-**config** 명령을 실행하면 이 암호화된 비밀번호를 볼 수 있습니다.enable **password** 명령을 사용하는 것도 enable 비밀번호를 설정하는 또 다른 방법입니다.그러나 enable **password** 명령과 함께 사용되는 암호화 알고리즘은 약하며 비밀번호를 얻기 위해 쉽게 되돌릴 수 있습니다.따라서 enable password 명령을 사용하지 마십시오.더 나은 보안을 위해 enable **secret** 명령을 사용합니다 .자세한 내용은 Cisco IOS Password Encryption Facts를 참조하십시오.

스위치에 대한 보안 텔넷/VTY 액세스

기본적으로 Cisco IOS Software는 5개의 활성 텔넷 세션을 지원합니다.이러한 세션을 vty 0~4라고 합니다. 이러한 행에 액세스할 수 있도록 설정할 수 있습니다.그러나 로그인을 활성화하려면 이러한 행에 대한 비밀번호를 설정해야 합니다.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

login 명령은 텔넷 액세스를 위해 이러한 행을 구성합니다.password 명령은 비밀번호를 구성합니다 .비밀번호가 다음 규칙을 따라야 합니다.

- 첫 번째 문자는 숫자일 수 없습니다.
- 문자열은 최대 80자의 영숫자 문자를 포함할 수 있습니다.문자는 공백을 포함합니다.
- number-space-character 형식으로 비밀번호를 지정할 수 없습니다.숫자 뒤의 공백은 문제를 유발합니다.예를 들어 hello 21은 올바른 암호이지만 21hello는 올바른 암호가 아닙니다.
- 비밀번호 확인은 대/소문자를 구분합니다.예를 들어, 비밀번호 Secret은 비밀번호 비밀번호와 다릅니다.

참고: 이 vty 라인 컨피그레이션에서는 비밀번호를 일반 텍스트로 저장합니다.누군가가 **show running-config** 명령을 실행하면 이 비밀번호가 표시됩니다.이러한 상황을 방지하려면 **service password-encryption** 명령을 사용합니다.이 명령은 비밀번호를 느슨하게 암호화합니다.이 명령은 vty 회선 비밀번호 및 enable password 명령으로 구성된 enable 비밀번호만 암호화합니다.enable secret 명령으로 구성된 enable 비밀번호**는** 강력한 암호화를 사용합니다.enable **secret** 명령을 사용한 컨피그레이션이 권장되는 방법입니다.

참고: 보안 관리의 유연성을 높이려면 모든 Cisco IOS Software 디바이스에서 AAA(Authentication, Authorization, and Accounting) 보안 모델을 구현해야 합니다.AAA는 로컬, RADIUS 및 TACACS+ 데이터베이스를 사용할 수 있습니다.자세한 내용은 TACACS+ 인증 컨피그레이션 섹션을 참조하십시오.

AAA 보안 서비스

AAA 운영 개요

액세스 제어는 스위치에 액세스할 수 있는 권한이 있는 사용자와 이러한 사용자가 사용할 수 있는 서비스를 제어합니다.AAA 네트워크 보안 서비스는 스위치에 액세스 제어를 설정하는 기본 프레임워크를 제공합니다.

다음 섹션에서는 AAA의 다양한 측면에 대해 자세히 설명합니다.

- Authentication(인증) - 이 프로세스는 최종 사용자 또는 디바이스의 클레임된 ID를 검증합니다 .먼저 사용자를 인증하는 데 사용할 수 있는 다양한 방법을 지정합니다.이러한 방법은 수행할 인증 유형(예: TACACS+ 또는 RADIUS)을 정의합니다. 이러한 인증 방법을 시도할 시퀀스도 정

의됩니다.그런 다음 적절한 인터페이스에 메서드가 적용되어 인증이 활성화됩니다.
- 권한 부여 - 이 프로세스는 사용자, 사용자 그룹, 시스템 또는 프로세스에 대한 액세스 권한을 부여합니다.AAA 프로세스는 작업 단위로 일회성 권한 부여 또는 권한 부여를 수행할 수 있습니다.이 프로세스는 사용자가 수행할 권한이 있는 AAA 서버에서 특성을 정의합니다.사용자가 서비스 시작을 시도할 때마다 스위치는 AAA 서버를 쿼리하고 사용자 권한 부여를 요청합니다.AAA 서버가 승인하면 사용자에게 권한이 부여됩니다.AAA 서버가 승인하지 않으면 사용자는 해당 서비스를 실행할 수 있는 권한을 받지 못합니다.일부 사용자가 특정 명령만 실행할 수 있도록 지정하려면 이 프로세스를 사용할 수 있습니다.
- Accounting(계정 관리) - 이 프로세스를 통해 사용자가 액세스하는 서비스 및 사용자가 사용하는 네트워크 리소스의 양을 추적할 수 있습니다.어카운팅이 활성화되면 스위치는 어카운팅 레코드 형태로 AAA 서버에 사용자 활동을 보고합니다.보고된 사용자 활동의 예로는 세션 시간, 시작 및 중지 시간이 있습니다.그런 다음 이 활동에 대한 분석을 관리 또는 청구 용도로 수행할 수 있습니다.

AAA가 액세스 제어를 위한 기본 권장 방법이지만, Cisco IOS Software는 AAA 범위를 벗어나는 간단한 액세스 제어를 위한 추가 기능을 제공합니다.다음과 같은 추가 기능을 제공합니다.

- 로컬 사용자 이름 인증
- 회선 암호 인증
- 비밀번호 인증 사용

그러나 이러한 기능은 AAA와 동일한 수준의 액세스 제어를 제공하지 않습니다.

AAA를 더 잘 이해하려면 다음 문서를 참조하십시오.

- AAA(Authentication, Authorization, and Accounting)
- 액세스 서버에서 기본 AAA 구성
- TACACS+ 및 RADIUS 비교

이러한 문서에는 스위치를 언급할 필요는 없습니다.그러나 문서에 설명된 AAA 개념은 스위치에 적용할 수 있습니다.

TACACS+

목적

기본적으로 비권한 및 특권 모드 비밀번호는 전역적입니다.이러한 비밀번호는 콘솔 포트에서 또는 네트워크 전체의 텔넷 세션을 통해 스위치 또는 라우터에 액세스하는 모든 사용자에게 적용됩니다.네트워크 디바이스에서 이러한 비밀번호를 구현하려면 시간이 많이 걸리고 중앙 집중화되지 않습니다.또한 컨피그레이션 오류가 발생할 수 있는 ACL(Access Control List)을 사용하여 액세스 제한을 구현하기가 어려울 수 있습니다.이러한 문제를 해결하려면 중앙 서버에서 사용자 이름, 비밀번호 및 액세스 정책을 구성할 때 중앙 집중식 접근 방식을 사용합니다.이 서버는 Cisco ACS(Secure Access Control Server) 또는 타사 서버일 수 있습니다.디바이스는 AAA 기능에 이러한 중앙 집중식 데이터베이스를 사용하도록 구성됩니다.이 경우 디바이스는 Cisco IOS Software 스위치입니다.디바이스와 중앙 서버 간에 사용되는 프로토콜은 다음과 같습니다.

- TACACS+
- RADIUS
- Kerberos

TACACS+는 Cisco 네트워크의 일반적인 구축이며 이 섹션의 주안점입니다.TACACS+는 다음 기능을 제공합니다.

- Authentication(인증) - 사용자를 식별하고 확인하는 프로세스입니다.사용자를 인증하기 위해 여러 방법을 사용할 수 있습니다.그러나 가장 일반적인 방법에는 사용자 이름과 비밀번호의 조합이 포함됩니다.
- Authorization(권한 부여) - 사용자가 명령을 실행하려고 시도할 때 스위치는 TACACS+ 서버와 함께 검사하여 사용자에게 해당 명령을 사용할 수 있는 권한이 부여되었는지 확인할 수 있습니다.
- Accounting(계정 관리) - 사용자가 디바이스에서 수행한 작업 또는 작업을 기록합니다.

TACACS+와 RADIUS의 비교는 TACACS+ 및 RADIUS 비교를 참조하십시오.

운영 개요

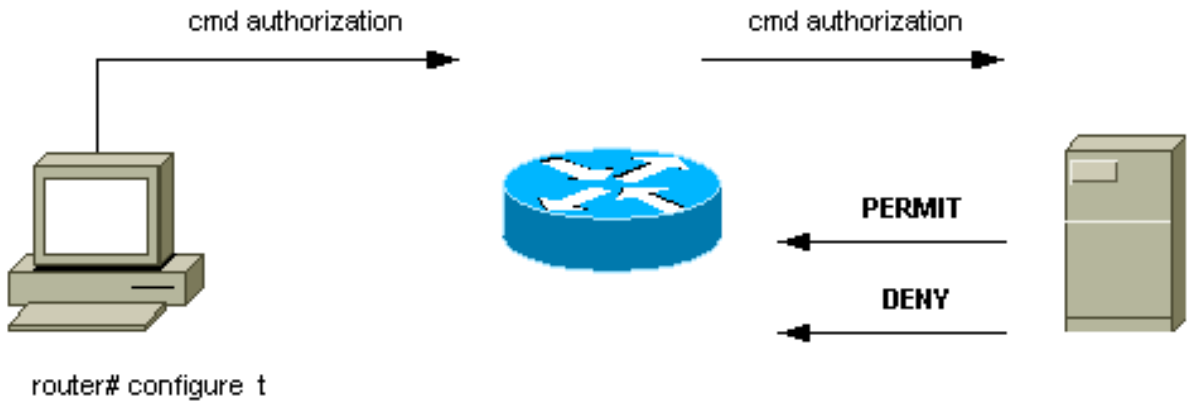
TACACS+ 프로토콜은 사용자 이름 및 비밀번호를 중앙 서버로 전달합니다.이 정보는 MD5 단방향 해싱을 사용하여 네트워크를 통해 암호화됩니다.자세한 내용은 RFC 1321 을 참조하십시오 .TACACS+는 TCP 포트 49를 전송 프로토콜로 사용하며, 이는 UDP에 비해 다음과 같은 이점을 제공합니다.

참고: RADIUS는 UDP를 사용합니다.

- 연결 지향 전송
- 백엔드 인증 메커니즘의 로드와 상관없이 요청이 수신되었음을 별도의 확인(TCP 승인[ACK])
- 서버 충돌 즉시 표시(RST[Reset] packets)

세션 중에 추가 권한 확인이 필요한 경우 스위치는 TACACS+를 사용하여 사용자에게 특정 명령을 사용할 수 있는 권한이 있는지 확인합니다.이 단계에서는 스위치에서 실행할 수 있는 명령을 더 효과적으로 제어하고 인증 메커니즘과 분리를 제공합니다.명령 어카운팅을 사용하면 특정 사용자가 특정 네트워크 디바이스에 연결된 동안 특정 사용자가 실행한 명령을 감사할 수 있습니다.

이 다이어그램은 관련된 권한 부여 프로세스를 보여줍니다.



사용자가 간단한 ASCII 로그인 시도에서 TACACS+를 사용하여 네트워크 디바이스에 인증하는 경우 이 프로세스는 일반적으로 다음과 같이 수행됩니다.

- 연결이 설정되면 스위치는 사용자 이름 프롬프트를 가져오기 위해 TACACS+ 데몬에 연결합니다.그러면 스위치에 사용자 프롬프트가 표시됩니다.사용자가 사용자 이름을 입력하면 스위치가 TACACS+ 데몬에 연결하여 비밀번호 프롬프트를 가져옵니다.이 스위치는 TACACS+ 데몬으로 전송되는 비밀번호를 입력하는 사용자의 비밀번호 프롬프트를 표시합니다.

- 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.사용자에게 추가 액세스가 거부되거나 로그인 시퀀스를 다시 시도하라는 메시지가 표시됩니다.결과는 TACACS+ 데몬에 따라 달라집니다.ERROR - 인증 중에 오류가 발생했습니다.이 오류는 디먼에 있거나 디먼과 스위치 간의 네트워크 연결에 있을 수 있습니다.ERROR 응답이 수신되면 일반적으로 네트워크 디바이스는 대체 방법을 사용하여 사용자를 인증하려고 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 연결합니다.TACACS+ 데몬은 ACCEPT 또 REJECT 권한 부여 응답 반환합니다.ACCEPT 응답이 반환되면 응답에는 해당 사용자의 EXEC 또는 NETWORK 세션을 지시하는 데 사용되는 속성 형식의 데이터가 포함됩니다.사용자가 액세스할 수 있는 명령을 결정합니다.

기본 AAA 컨피그레이션 단계

AAA의 구성은 기본 프로세스를 이해하고 나면 비교적 간단합니다.AAA를 사용하여 Cisco 라우터 또는 액세스 서버에서 보안을 구성하려면 다음 단계를 수행합니다.

1. AAA를 활성화하려면 aaa **new-model** 전역 컨피그레이션 명령을 실행합니다.
   ```
   Switch(config)#aaa new-model
   ```

   팁: AAA 명령을 구성하기 전에 컨피그레이션을 저장합니다.모든 AAA 컨피그레이션을 완료하고 컨피그레이션이 올바르게 작동하는지 확인한 후에만 컨피그레이션을 다시 저장합니다.그런 다음 필요한 경우 예기치 않은 잠금에서 복구하기 위해 스위치를 다시 로드할 수 있습니다(컨피그레이션을 저장하기 전에).
2. 별도의 보안 서버를 사용하려는 경우 RADIUS, TACACS+ 또는 Kerberos와 같은 보안 프로토콜 매개변수를 구성합니다.
3. **aaa authentication** 명령을 사용하여 인증 방법 목록을 정의합니다.
4. 특정 인터페이스 또는 행에 메서드 목록을 적용하려면 **login authentication** 명령을 사용합니다 .
5. 권한 부여를 구성하려면 선택적인 **aaa authorization** 명령을 실행합니다.
6. 어카운팅을 구성하려면 선택적 **aaa accounting** 명령을 실행합니다.
7. 스위치에서 인증 및 권한 부여 요청을 처리하도록 AAA 외부 서버를 구성합니다.**참고:** 자세한 내용은 AAA 서버 설명서를 참조하십시오.

TACACS+ 인증 컨피그레이션

TACACS+ 인증을 구성하려면 다음 단계를 수행합니다.

1. 스위치에서 **AAA를** 활성화하려면 전역 컨피그레이션 모드에서 aaa new-model 명령을 실행합니다.
2. TACACS+ 서버 및 관련 키를 정의합니다.이 키는 TACACS+ 서버와 스위치 간 트래픽을 암호화하는 데 사용됩니다.tacacs**-server host 1.1.1.1 key mysecretkey** 명령에서 TACACS+ 서버는 IP 주소 1.1.1.1에 있으며 암호화 키는 mysecretkey입니다.스위치가 TACACS+ 서버에 도달할 수 있는지 확인하려면 스위치에서 ICMP(Internet Control Message Protocol) ping을 시작합니다.

3. 메서드 목록을 정의합니다.메서드 목록은 다양한 서비스를 시도하기 위한 인증 메커니즘의 순서를 정의합니다.다음과 같은 다양한 서비스가 가능합니다.사용로그인(vty/텔넷 액세스용)**참고:** vty/텔넷 액세스에 대한 자세한 내용은 이 문서의 기본 보안 기능 섹션을 참조하십시오 .Console이 예에서는 **로그인만** 고려합니다.인터페이스/라인에 메서드 목록을 적용해야 합니다.

```
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
Switch(config)#line vty 0 4
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

이 컨피그레이션에서는 **aaa authentication login** 명령이 made-up 목록 이름 METHOD-LIST-LOGIN을 사용하고 메서드 행을 사용하기 전에 tacacs+ 메서드를 사용합니다.사용자는 첫 번째 방법으로 TACACS+ 서버를 사용하여 인증됩니다.TACACS+ 서버가 ERROR 메시지에 응답하지 않거나 전송하는 경우, 라인에 구성된 비밀번호가 두 번째 방법으로 사용됩니다.그러나 TACACS+ 서버가 사용자를 거부하고 REJECT 메시지로 응답할 경우 AAA는 트랜잭션을 성공한 것으로 간주하며 두 번째 방법을 사용하지 않습니다.**참고:** 목록(METHOD-LIST-LOGIN)을 vty 라인에 적용할 때까지 컨피그레이션이 완료되지 않습니다.예와 같이 라인 컨피그레이션 모드에서 **login authentication METHOD-LIST-LOGIN** 명령을 실행합니다.**참고:** 이 예에서는 TACACS+ 서버를 사용할 수 없는 경우에 대한 백도어를 생성합니다.보안 관리자는 백도어 구현을 허용할 수도 있고 허용할 수도 없습니다.이러한 백도어를 구현하는 결정이 사이트의 보안 정책을 준수하는지 확인하십시오.

RADIUS 인증 컨피그레이션

RADIUS 컨피그레이션은 TACACS+ 컨피그레이션과 거의 동일합니다.컨피그레이션에서 TACACS에 대해 RADIUS라는 단어를 대체하기만 하면 됩니다.다음은 COM 포트 액세스를 위한 샘플 RADIUS 컨피그레이션입니다.

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

로그인 배너

무단 액세스 시 수행되는 작업을 구체적으로 설명하는 적절한 디바이스 배너를 생성합니다.사이트 이름 또는 네트워크 정보를 권한이 없는 사용자에게 알리지 마십시오.배너에서는 장치가 손상되고 가해자가 붙잡혔을 경우에 상환청구가 가능합니다.로그인 배너를 생성하려면 다음 명령을 실행합니다.

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

물리적 보안

디바이스에 물리적으로 액세스하기 위해서는 적절한 권한이 있어야 합니다.통제된(잠긴) 공간에 장비를 보관합니다.네트워크가 작동 중이고 악의적인 변조 또는 환경 요인에 영향을 받지 않도록 하

려면 모든 장비에 다음이 있는지 확인하십시오.

- 가능한 경우 예비 전원을 사용하는 적절한 UPS(무정전 전원 공급 장치)
- 온도 제어(에어컨)

악의적인 의도가 물리적 액세스를 위반할 경우 비밀번호 복구 또는 기타 수단을 통해 중단되는 경우가 훨씬 더 많습니다.

관리 구성

네트워크 다이어그램

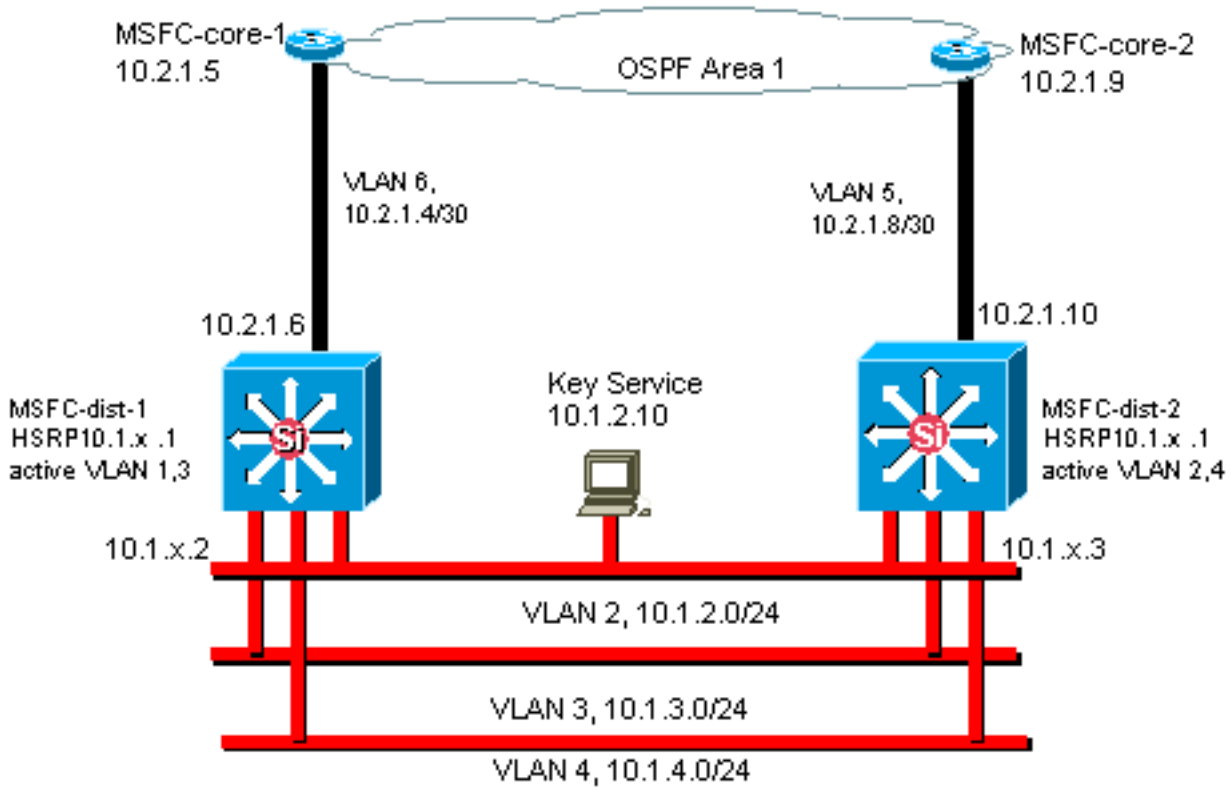
목적

네트워크 다이어그램 지우기는 네트워크 운영의 기본 요소입니다.이 다이어그램은 문제 해결 과정에서 중요한 요소가 되며, 가동 중단 시 공급업체 및 파트너에게 정보를 에스컬레이션하는 과정에서 가장 중요한 수단이 됩니다.네트워크 다이어그램에서 제공하는 준비, 준비도 및 접근성을 과소평가하지 마십시오.

권장 사항

다음 세 가지 유형의 다이어그램이 필요합니다.

- **전체 다이어그램**—대규모 네트워크에서도 엔드 투 엔드 물리적 또는 논리적 연결을 보여주는 다이어그램이 중요합니다.계층적 설계 문서를 각 레이어를 개별적으로 구현한 기업이 많습니다.계획을 세우고 문제를 해결할 때 도메인이 어떻게 연결되는지 잘 알고 있어야 합니다.
- **물리적 다이어그램**—이 다이어그램은 모든 스위치 및 라우터 하드웨어 및 케이블을 보여줍니다.다이어그램에서 다음 각 측면에 레이블을 지정해야 합니다.트렁크링크속도채널 그룹포트 번호슬롯섀시 유형소프트웨어VTP 도메인루트 브리지백업 루트 브리지 우선 순위MAC 주소 VLAN당 차단된 포트명확성을 위해 Catalyst 6500/6000 MSFC 라우터와 같은 내부 장치를 트렁크를 통해 연결된 스틱의 라우터로 표시합니다.
- **논리 다이어그램** — 이 다이어그램은 레이어 3 기능만 보여 줍니다. 즉, 라우터를 개체로 표시하고 VLAN을 이더넷 세그먼트로 표시합니다.다이어그램에서 다음 측면에 레이블을 지정해야 합니다.IP 주소서브넷보조 주소 지정HSRP 활성 및 대기코어 디스트리뷰션 레이어 액세스라우팅 정보



스위치 관리 인터페이스 및 네이티브 VLAN

목적

이 섹션에서는 기본 VLAN 1의 사용 의의와 잠재적인 문제에 대해 설명합니다. 또한 6500/6000 시리즈 스위치의 사용자 트래픽과 동일한 VLAN에서 스위치에 대한 관리 트래픽을 실행할 때 발생할 수 있는 문제를 다룹니다.

Supervisor Engines 및 Catalyst 6500/6000 시리즈용 MSFC의 프로세서는 여러 제어 및 관리 프로토콜에 VLAN 1을 사용합니다.예를 들면 다음과 같습니다.

- 스위치 제어 프로토콜:STP BPDUVTPDTPCDP
- 관리 프로토콜:SNMPTelnetSSH(Secure Shell Protocol)Syslog

이러한 방식으로 VLAN을 사용하면 이를 네이티브 VLAN이라고 합니다.기본 스위치 컨피그레이션은 VLAN 1을 Catalyst 트렁크 포트의 기본 네이티브 VLAN으로 설정합니다.VLAN 1을 기본 VLAN으로 유지할 수 있습니다.그러나 네트워크에서 Cisco IOS 시스템 소프트웨어를 실행하는 모든 스위치는 기본적으로 VLAN 1의 포트에 액세스하기 위해 레이어 2 스위치 포트로 구성된 모든 인터페이스를 설정합니다.네트워크 어딘가에 있는 스위치는 사용자 트래픽에 VLAN 1을 사용하여 VLAN을 사용합니다.

VLAN 1의 사용에 대한 주요 문제는 일반적으로 수퍼바이저 엔진 NMP가 엔드 스테이션에서 생성하는 브로드캐스트 및 멀티캐스트 트래픽의 많은 부분에 의해 중단될 필요가 없다는 것입니다.특히 멀티캐스트 애플리케이션은 서버와 클라이언트 간에 많은 데이터를 전송하는 경향이 있습니다 .Supervisor Engine에서 이 데이터를 볼 필요가 없습니다.수퍼바이저 엔진이 불필요한 트래픽을 수신 대기할 때 수퍼바이저 엔진의 리소스 또는 버퍼가 완전히 차지하는 경우, 수퍼바이저 엔진에서 스패닝 트리 루프 또는 EtherChannel 오류를 일으킬 수 있는 관리 패킷을 볼 수 없습니다(최악의 경우).

show **interfaces** *interface_type* **slot/***port* **counters** 명령 및 show ip traffic **명령은 다음과 같은 몇 가지 표시를 제공합니다.**

- 유니캐스트 트래픽에 대한 브로드캐스트 비율
- IP와 비 IP 트래픽의 비율(일반적으로 관리 VLAN에서 보이지 않음)

VLAN 1 태그는 대부분의 컨트롤 플레인 트래픽을 처리합니다.VLAN 1은 기본적으로 모든 트렁크에서 활성화됩니다.더 큰 캠퍼스 네트워크를 사용할 경우 VLAN 1 STP 도메인의 지름을 주의해야 합니다.네트워크의 한 부분이 불안정하면 VLAN 1에 영향을 줄 수 있으며 다른 모든 VLAN에 대한 컨트롤 플레인 안정성 및 STP 안정성에 영향을 줄 수 있습니다.인터페이스에서 사용자 데이터의 VLAN 1 전송 및 STP의 작업을 제한할 수 있습니다.트렁크 인터페이스에서 VLAN을 구성하지 마십시오.

이 컨피그레이션에서는 네트워크 분석기와 마찬가지로 VLAN 1에서 스위치로 제어 패킷의 전송을 중지하지 않습니다.그러나 어떤 데이터도 전달되지 않으며 STP는 이 링크를 통해 실행되지 않습니다.따라서 이 기술을 사용하여 VLAN 1을 더 작은 장애 도메인으로 분할할 수 있습니다.

참고: 트렁크에서 Catalyst 2900XL/3500XL로 VLAN 1을 지울 수 없습니다.

사용자 VLAN을 상대적으로 작은 스위치 도메인과 그에 상응하는 소규모 장애/레이어 3 경계로 제한하려는 경우에도 일부 고객은 관리 VLAN을 다르게 취급하려고 합니다.이러한 고객은 단일 관리 서브넷으로 전체 네트워크를 보호하려고 합니다.중앙 NMS 애플리케이션이 애플리케이션이 관리하는 디바이스에 인접한 레이어 2 또는 검증된 보안 인수여야 하는 기술적 이유는 없습니다.관리 VLAN의 지름을 사용자 VLAN과 동일한 라우티드 도메인 구조로 제한합니다.네트워크 관리 보안을 강화하기 위한 방법으로 대역 외 관리 및/또는 SSH 지원을 고려하십시오.

기타 옵션

일부 토폴로지에서는 이러한 Cisco 권장 사항에 대한 설계 고려 사항이 있습니다.예를 들어, 바람직한 공통 Cisco 멀티레이어 설계는 활성 스패닝 트리 사용을 방지하는 것입니다.이러한 방식으로 설계에서는 단일 액세스 레이어 스위치(또는 스위치 클러스터)에 각 IP 서브넷/VLAN의 제약 조건을 요청합니다. 이러한 설계에서는 액세스 레이어까지 트렁킹을 구성할 수 없습니다.

레이어 2 액세스와 레이어 3 디스트리뷰션 레이어 간에 이를 전달하기 위해 별도의 관리 VLAN을 생성하고 트렁킹을 활성화합니까?이 문제에 대한 쉬운 답은 없다.Cisco 엔지니어와 함께 설계 검토를 위한 다음 두 가지 옵션을 고려하십시오.

- **옵션 1** — 디스트리뷰션 레이어에서 각 액세스 레이어 스위치까지 2~3개의 고유한 VLAN을 트렁크합니다.이 컨피그레이션에서는 데이터 VLAN, 음성 VLAN 및 관리 VLAN을 사용할 수 있으며 STP가 비활성 상태라는 이점이 있습니다.트렁크에서 VLAN 1을 지우려면 추가 컨피그레이션 단계가 필요합니다.이 솔루션에는 장애 복구 중에 라우팅된 트래픽을 일시적으로 블랙홀링하지 않도록 하기 위해 고려해야 할 설계점도 있습니다.트렁크(향후) 또는 STP 포워딩과의 VLAN 자동 상태 동기화에 STP PortFast를 사용합니다.
- **옵션 2**—데이터 및 관리를 위한 단일 VLAN을 허용할 수 있습니다.sc0 인터페이스를 사용자 데이터와 분리하려는 경우, 최신 스위치 하드웨어로 인해 이 시나리오가 이전보다 더 작은 문제가 됩니다.최신 하드웨어는 다음과 같은 기능을 제공합니다.더욱 강력한 CPU 및 컨트롤 플레인 속도 제한 제어멀티레이어 설계에서 지원하는 비교적 작은 브로드캐스트 도메인이 포함된 설계최종 결정을 내리려면 VLAN에 대한 브로드캐스트 트래픽 프로필을 검토하고 Cisco 엔지니어와 스위치 하드웨어 기능에 대해 논의하십시오.관리 VLAN에 해당 액세스 레이어 스위치의 모든 사용자가 포함된 경우 Cisco IOS Software Security Features 섹션에 따라 IP 입력 필터를 사용하여 사용자로부터 스위치를 보호합니다.

Cisco 관리 인터페이스 및 기본 VLAN 권장 사항

관리 인터페이스

Cisco IOS 시스템 소프트웨어는 인터페이스를 레이어 3 인터페이스로 구성하거나 VLAN의 레이어 2 스위치 포트로 구성할 수 있는 옵션을 제공합니다.Cisco IOS Software에서 switchport 명령을 사용할 경우 기본적으로 모든 스위치 포트는 VLAN 1의 액세스 포트입니다.따라서 별도로 구성하지 않는 한 사용자 데이터도 VLAN 1에서 기본적으로 존재할 수 있습니다.

관리 VLAN을 VLAN 1 이외의 VLAN으로 설정합니다. 모든 사용자 데이터를 관리 VLAN에서 제외합니다.대신 각 스위치에서 루프백0 인터페이스를 관리 인터페이스로 구성합니다.

참고: OSPF Protocol을 사용하는 경우 OSPF 라우터 ID도 됩니다.

루프백 인터페이스에 32비트 서브넷 마스크가 있는지 확인하고 루프백 인터페이스를 스위치에서 순수 레이어 3 인터페이스로 구성합니다.예:

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

네이티브 VLAN

네이티브 VLAN을 라우터에서 활성화되지 않은 명백한 더미 VLAN으로 구성합니다.Cisco는 과거에 VLAN 999를 권장했지만, 그 선택은 전적으로 임의적입니다.

특정 포트에서 802.1Q 트렁킹을 위한 네이티브(기본값)로 VLAN을 설정하려면 다음 interface 명령을 실행합니다.

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

추가 트렁킹 컨피그레이션 권장 사항은 이 문서의 Dynamic Trunking Protocol 섹션을 참조하십시오.

대역 외 관리

목적

운영 네트워크를 중심으로 별도의 관리 인프라를 구축하면 네트워크 관리를 더욱 높은 수준으로 유지할 수 있습니다.이 설정을 사용하면 제어되는 트래픽 또는 발생하는 컨트롤 플레인 이벤트에도 불구하고 원격으로 디바이스에 연결할 수 있습니다.이 두 가지 방법은 일반적으로 다음과 같습니다.

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

운영 개요

관리 VLAN에서 대역외 이더넷 관리 인터페이스를 통해 네트워크의 모든 라우터 및 스위치를 제공

할 수 있습니다.관리 VLAN의 각 디바이스에서 이더넷 포트 하나를 구성하고 프로덕션 네트워크 외부에 별도의 스위치드 관리 네트워크에 연결합니다.

참고: Catalyst 4500/4000 스위치에는 Supervisor Engine에 스위치 포트가 아닌 대역 외 관리에만 사용되는 특수한 me1 인터페이스가 있습니다.

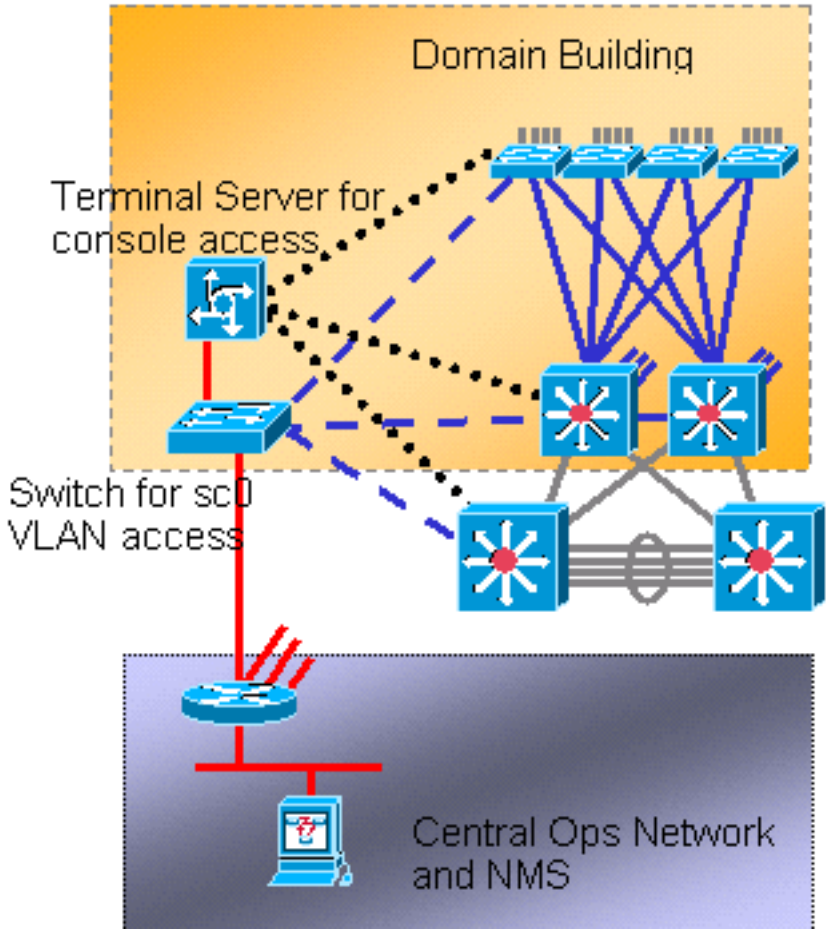
또한 RJ-45 직렬 케이블을 사용하여 Cisco 2600 또는 3600 라우터를 구성하여 레이아웃의 모든 라우터 및 스위치의 콘솔 포트에 액세스하면 터미널 서버 연결을 구현할 수 있습니다.또한 터미널 서버를 사용하면 모든 디바이스의 보조 포트에 있는 모뎀과 같은 백업 시나리오를 구성할 필요가 없습니다.터미널 서버의 보조 포트에서 단일 모뎀을 구성할 수 있습니다.이 컨피그레이션은 네트워크 연결 실패 시 다른 디바이스에 전화 접속 서비스를 제공합니다.자세한 내용은 Catalyst 스위치의 콘솔 포트에 모뎀 연결 을 참조하십시오.

권장 사항

이러한 방식으로 모든 스위치와 라우터에 대한 2개의 대역외 경로가 가능하며 다수의 대역 내 경로가 가능합니다.이러한 방식으로 고가용성 네트워크 관리가 가능합니다.이점은 다음과 같습니다.

- 이러한 배열은 관리 트래픽과 사용자 데이터를 구분합니다.
- 관리 IP 주소는 보안을 위해 별도의 서브넷, VLAN 및 스위치에 있습니다.
- 네트워크 장애 시 관리 데이터 전달에 대한 보증 수준이 높아집니다.
- 관리 VLAN에 활성 스패닝 트리가 없습니다.여기서 이중화는 중요하지 않습니다.

이 다이어그램은 대역 외 관리를 보여줍니다.



시스템 로깅

목적

Syslog 메시지는 Cisco에 한정되며 표준화된 SNMP보다 더 응답적이고 정확한 정보를 제공할 수 있습니다.예를 들어 Cisco RME(Resource Manager Essentials) 및 NATKit(Network Analysis Toolkit)와 같은 관리 플랫폼은 인벤토리 및 컨피그레이션 변경 사항을 수집하기 위해 syslog 정보를 효과적으로 사용합니다.

Cisco Syslog 구성 권장 사항

시스템 로깅은 일반적으로 사용되는 운영 방식입니다.UNIX syslog는 다음과 같은 라우터의 정보/이벤트를 캡처 및 분석할 수 있습니다.

- 인터페이스 상태
- 보안 알림
- 환경 조건
- CPU 프로세스 호그
- 기타 이벤트

Cisco IOS Software는 UNIX syslog 서버에 UNIX 로깅을 수행할 수 있습니다.Cisco UNIX syslog 형식은 4.3 BSD(Berkeley Standard Distribution) UNIX와 호환됩니다.다음 Cisco IOS 소프트웨어 로그 설정을 사용합니다.

- **no logging console**—기본적으로 모든 시스템 메시지가 시스템 콘솔로 전송됩니다.콘솔 로깅은 Cisco IOS Software에서 우선 순위가 높은 작업입니다.이 함수는 시스템 오류 전에 시스템 운영자에게 오류 메시지를 제공하도록 기본적으로 설계되었습니다.디바이스가 터미널에서 응답을 기다리는 동안 라우터/스위치가 중단될 수 있는 상황을 방지하려면 모든 디바이스 컨피그레이션에서 콘솔 로깅을 비활성화합니다.그러나 콘솔 메시지는 문제 격리 중에 유용할 수 있습니다.이러한 경우 콘솔 로깅을 활성화합니다.원하는 수준의 메시지 로깅을 얻으려면 logging **console level** 명령을 실행합니다.로깅 레벨은 0~7입니다.
- **no logging monitor**—이 명령은 시스템 콘솔 이외의 터미널 회선에 대한 로깅을 비활성화합니다.모니터 로깅이 필요할 수 있습니다(로깅 **모니터 디버깅** 또는 다른 명령 옵션 사용). 이 경우 활동에 필요한 특정 로깅 수준에서 모니터 로깅을 활성화합니다.로깅 레벨에 대한 자세한 내용은 이 목록의 **no logging console** 항목을 참조하십시오.
- **logging buffered 16384** - **logging buffered** 명령**을** 내부 로그 버퍼에 시스템 메시지를 기록하기 위해 추가해야 합니다.로깅 버퍼가 순환입니다.로깅 버퍼가 채워지면 이전 엔트리를 새 엔트리에 덮어씁니다.로깅 버퍼의 크기는 사용자가 구성할 수 있으며 바이트 단위로 지정됩니다.시스템 버퍼의 크기는 플랫폼에 따라 다릅니다.16384는 대부분의 경우 적절한 로깅을 제공하는 좋은 기본값입니다.
- **logging trap notifications**—이 명령은 지정된 syslog 서버에 알림 레벨(5) 메시징을 제공합니다.모든 디바이스(콘솔, 모니터, 버퍼 및 트랩)의 기본 로깅 레벨은 디버깅(레벨 7)입니다. 트랩 로깅 수준을 7로 유지하면 네트워크 상태에 거의 또는 전혀 영향을 미치지 않는 많은 외부 메시지가 생성됩니다.트랩의 기본 로깅 레벨을 5로 설정합니다.
- **logging facility local7**—이 명령은 UNIX syslogging의 기본 로깅 기능/수준을 설정합니다.동일한 기능/수준에 대해 이러한 메시지를 수신하는 syslog 서버를 구성합니다.
- **logging host**—이 명령은 UNIX 로깅 서버의 IP 주소를 설정합니다.
- **logging source-interface loopback 0** - 이 명령은 syslog 메시지에 대한 기본 IP SA를 설정합니다.메시지를 더 쉽게 보낸 호스트를 식별하기 위해 로깅 SA를 하드 코딩합니다.
- **service timestamp debug datetime localtime show-timezone msec** - 기본적으로 로그 메시지는 타임스탬프가 지정되지 않습니다.이 명령을 사용하여 로그 메시지의 타임스탬프를 활성화하고

시스템 디버그 메시지의 타임스탬프를 구성할 수 있습니다.타임스탬프는 로깅된 이벤트의 상대적 타이밍을 제공하며 실시간 디버깅을 향상시킵니다.이 정보는 고객이 기술 지원 담당자에게 디버깅 출력을 보내 지원을 받을 때 특히 유용합니다.시스템 디버그 메시지의 타임스탬프를 활성화하려면 글로벌 컨피그레이션 모드에서 명령을 사용합니다.디버깅이 활성화된 경우에만 명령이 적용됩니다.

참고: 또한 모든 인프라 기가비트 인터페이스에서 링크 상태 및 번들 상태에 대한 로깅을 활성화합니다.

Cisco IOS Software는 syslog 서버로 향하는 모든 시스템 메시지에 대해 기능 및 로그 레벨을 설정하는 단일 메커니즘을 제공합니다.로깅 트랩 수준을 알림(수준 5)으로 설정합니다. 트랩 메시지 레벨을 알림으로 설정하면 syslog 서버로 전달되는 정보 메시지의 수를 최소화할 수 있습니다.이 설정은 네트워크의 syslog 트래픽 양을 크게 줄이고 syslog 서버 리소스에 대한 영향을 줄일 수 있습니다.

syslog 메시징을 활성화하기 위해 Cisco IOS Software를 실행하는 각 라우터 및 스위치에 다음 명령을 추가합니다.

- 전역 syslog 컨피그레이션 명령:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- 인터페이스 syslog 컨피그레이션 명령:

```
logging event link-status
logging event bundle-status
```

SNMP

목적

SNMP를 사용하여 네트워크 디바이스 MIB에 저장된 통계, 카운터 및 테이블을 검색할 수 있습니다.HP OpenView와 같은 NMS는 이 정보를 사용하여 다음을 수행할 수 있습니다.

- 실시간 알림 생성
- 가용성 측정
- 용량 계획 정보 생성
- 구성 및 문제 해결 확인 수행 도움말

SNMP 관리 인터페이스 작업

SNMP는 SNMP 관리자와 에이전트 간 통신을 위한 메시지 형식을 제공하는 애플리케이션 레이어 프로토콜입니다.SNMP는 표준화된 프레임워크와 네트워크에서 디바이스를 모니터링하고 관리할 수 있는 공통 언어를 제공합니다.

SNMP 프레임워크는 다음 세 부분으로 구성됩니다.

- SNMP 관리자
- SNMP 에이전트
- MIB

SNMP 관리자는 네트워크 호스트의 활동을 제어하고 모니터링하기 위해 SNMP를 사용하는 시스템입니다.가장 일반적인 관리 시스템을 NMS라고 합니다.네트워크 관리에 사용되는 전용 디바이스 또는 그러한 디바이스에서 사용되는 애플리케이션에 NMS라는 용어를 적용할 수 있습니다.다양한 네트워크 관리 애플리케이션을 SNMP와 함께 사용할 수 있습니다.이러한 애플리케이션의 범위는 간단한 CLI 애플리케이션부터 CiscoWorks 제품 라인과 같은 기능이 풍부한 GUI에 이르기까지 다양합니다.

SNMP 에이전트는 관리되는 디바이스 내의 소프트웨어 구성 요소로, 디바이스에 대한 데이터를 유지 관리하고, 필요한 경우 시스템 관리를 위해 이러한 데이터를 보고합니다.에이전트 및 MIB는 라우팅 디바이스(라우터, 액세스 서버 또는 스위치)에 상주합니다. Cisco 라우팅 디바이스에서 SNMP 에이전트를 활성화하려면 관리자와 에이전트 간의 관계를 정의해야 합니다.

MIB는 네트워크 관리 정보를 위한 가상 정보 스토리지 영역입니다.MIB는 관리되는 개체의 컬렉션으로 구성됩니다.MIB 내에는 MIB 모듈에 정의된 관련 객체 모음이 있습니다.MIB 모듈은 SNMP MIB 모듈 언어로 작성되며, STD 58, RFC 2578 , RFC 2579 , RFC 2580 정의됨.

참고: 개별 MIB 모듈은 MIB라고도 합니다.예를 들어 인터페이스 그룹 MIB(IF-MIB)는 시스템의 MIB 내의 MIB 모듈입니다.

SNMP 에이전트에는 MIB 변수가 포함되어 있습니다. SNMP 관리자가 get 또는 set 작업을 통해 요청하거나 변경할 수 있는 값입니다.관리자는 상담원으로부터 값을 받거나 해당 상담원에 값을 저장할 수 있습니다.에이전트는 MIB에서 데이터를 수집합니다. MIB는 디바이스 매개변수 및 네트워크 데이터에 대한 정보를 위한 저장소입니다.또한 에이전트는 관리자 요청에 응답하여 데이터를 가져오거나 설정할 수도 있습니다.

관리자는 MIB 값을 가져오고 설정하기 위해 에이전트 요청을 보낼 수 있습니다.에이전트는 이러한 요청에 응답할 수 있습니다.이러한 상호 작용과 상관없이 에이전트는 관리자에게 원치 않는 알림(트랩 또는 알림)을 전송하여 네트워크 조건을 관리자에게 알릴 수 있습니다.일부 보안 메커니즘을 통해 NMS는 MIB에서 `get` 및 요청으로 정보를 검색할 수 있으며 매개변수를 변경하기 위해 set 명령을 실행할 수 있습니다.또한 실시간 알림을 위해 NMS에 대한 트랩 메시지를 생성하도록 네트워크 디바이스를 설정할 수 있습니다.IP UDP 포트 161 및 162는 트랩에 사용됩니다.

SNMP 알림 운영 개요

SNMP의 주요 기능은 SNMP 에이전트에서 알림을 생성하는 기능입니다.이러한 알림은 SNMP 관리자에서 요청을 보낼 필요가 없습니다.요청되지 않은(비동기) 알림은 트랩으로 생성되거나 알림 요청으로 생성될 수 있습니다.Traps는 SNMP 관리자에게 네트워크의 조건을 알리는 메시지입니다.알림 요청(알림)은 SNMP 관리자의 수신 확인 요청을 포함하는 트랩입니다.알림은 다음과 같은 중요한 이벤트를 나타낼 수 있습니다.

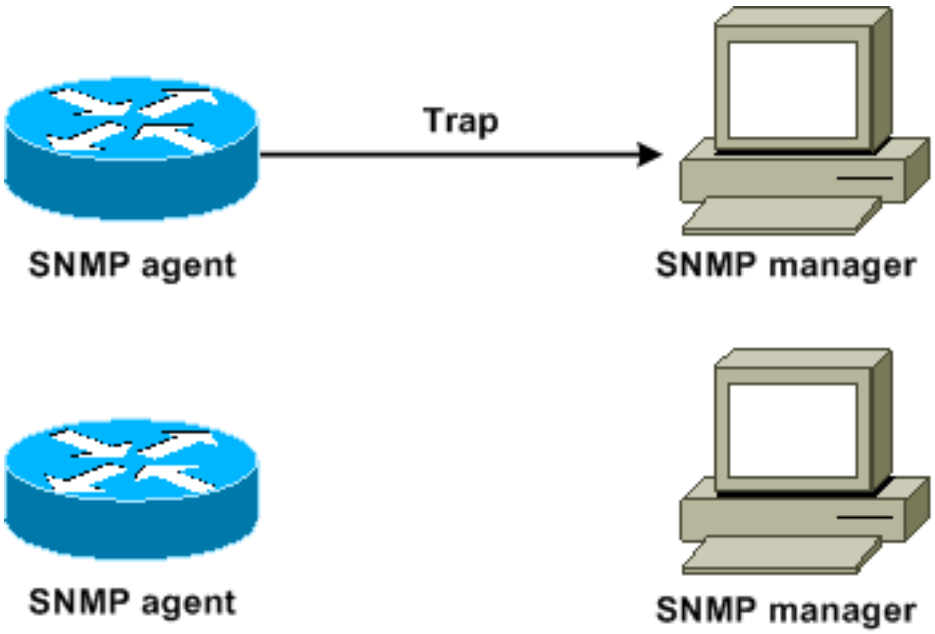
- 잘못된 사용자 인증
- 재시작
- 연결 닫기
- 인접 라우터와의 연결 끊김
- 기타 이벤트

수신자가 트랩을 수신할 때 수신자가 승인을 보내지 않으므로 트랩은 알려진 것보다 신뢰성이 낮습

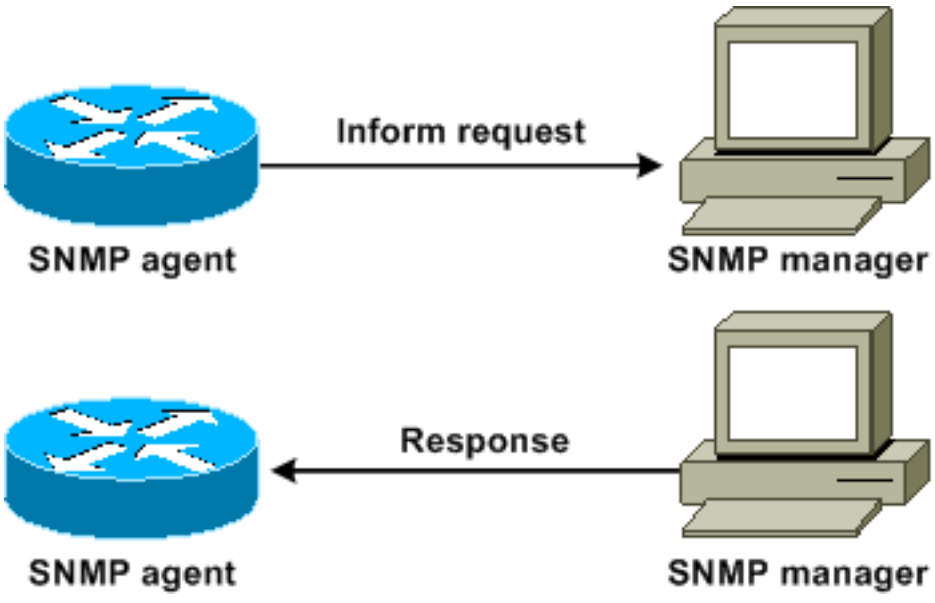
니다.발신자가 트랩이 수신되었는지 확인할 수 없습니다.알림 요청을 수신하는 SNMP 관리자는 SNMP PDU(Response Protocol Data Unit)를 사용하여 메시지를 승인합니다. 관리자가 알림 요청을 받지 않으면 관리자가 응답을 보내지 않습니다.발신자가 응답을 받지 못한 경우 발신자는 알림 요청을 다시 보낼 수 있습니다.Inform(알림)은 의도한 대상에 도달할 가능성이 높습니다.

그러나 알림이 라우터와 네트워크에서 더 많은 리소스를 소비하기 때문에 트랩을 선호하는 경우가 많습니다.트랩은 전송되자마자 삭제됩니다.그러나 알림 요청은 응답을 받거나 요청이 시간 초과될 때까지 메모리에 보관해야 합니다.또한 트랩은 한 번만 전송되며 알림을 여러 번 재시도할 수 있습니다.재시도는 트래픽을 증가시키고 네트워크 오버헤드를 높입니다.따라서 트랩 및 알림 요청은 안정성과 리소스 간에 절충을 제공합니다.SNMP 관리자가 모든 알림을 수신해야 하는 경우 알림 요청을 사용합니다.그러나 네트워크 또는 라우터의 메모리 트래픽에 대한 우려가 있고 모든 알림을 받을 필요가 없는 경우 트랩을 사용합니다.

다음 다이어그램은 트랩과 알림 요청의 차이점을 보여줍니다.

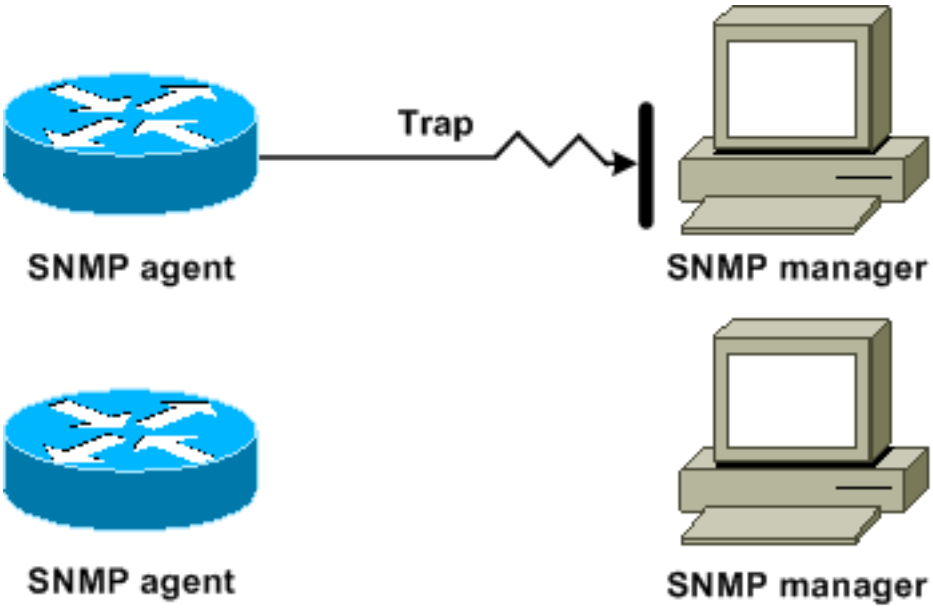


이 다이어그램은 에이전트 라우터가 SNMP 관리자에게 트랩을 성공적으로 전송하는 방법을 보여줍니다.관리자는 트랩을 수신하지만 상담원에게 승인을 보내지 않습니다.에이전트는 트랩이 대상에 도달했음을 알 수 없습니다.

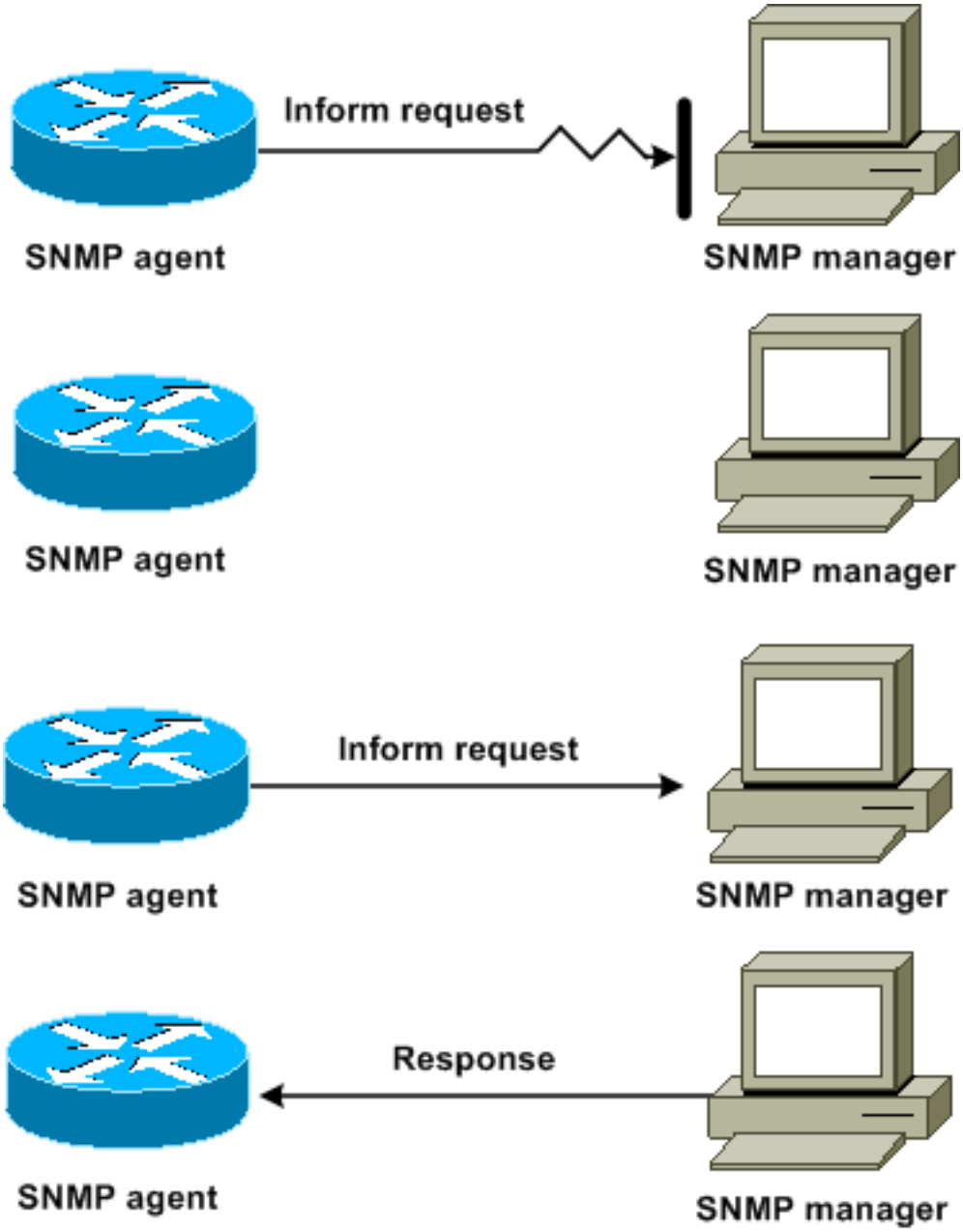


이 다이어그램은 에이전트 라우터가 관리자에게 알림 요청을 성공적으로 전송하는 방법을 보여줍

니다.관리자는 알림 요청을 받으면 상담원에게 응답을 보냅니다.이렇게 하면 상담원은 알림 요청이 대상에 도달했음을 알게 됩니다.이 예에서는 트래픽이 2배 많습니다.그러나 에이전트는 관리자가 알림을 받았음을 알고 있습니다.



이 다이어그램에서 에이전트는 관리자에게 트랩을 전송하지만 트랩은 관리자에 연결되지 않습니다.에이전트는 트랩이 대상에 도달하지 않았음을 알 수 없으므로 트랩이 다시 전송되지 않습니다.관리자는 트랩을 수신하지 않습니다.



이 다이어그램에서 에이전트는 관리자에게 알림 요청을 전송하지만 알림 요청이 관리자에게 전달되지 않습니다.관리자가 알림 요청을 받지 못했으므로 응답이 없습니다.일정 기간이 지나면 상담원은 알림 요청을 재전송합니다.두 번째로 관리자는 알림 요청을 수신하고 응답으로 응답합니다.이 예에서는 트래픽이 더 많습니다.그러나 알림이 SNMP 관리자에게 전달됩니다.

Cisco MIB 및 RFC 참조

RFC 문서는 일반적으로 MIB 모듈을 정의합니다.RFC 문서는 국제 표준 기관인 IETF(Internet Engineering Task Force)에 제출됩니다.개인 또는 그룹이 ISOC(Internet Society) 및 인터넷 커뮤니티 전체에서 RFC를 고려합니다.IETF의 표준 프로세스 및 활동에 대해 알아보려면 인터넷 소사이어티 홈 페이지를 참조하십시오.Cisco 문서에서 참조하는 모든 RFC, 인터넷 초안(I-D) 및 STD의 전체 텍스트를 읽으려면 IETF 홈 페이지를 참조하십시오.

Cisco의 SNMP 구현에서는 다음을 사용합니다.

- RFC 1213에서 설명하는 MIB II 변수 정의
- RFC 1215에서 설명하는 SNMP 트랩 정의

Cisco는 모든 시스템에 고유한 프라이빗 MIB 확장을 제공합니다.Cisco 엔터프라이즈 MIB는 설명

서에 다른 설명이 없는 한 관련 RFC에서 설명하는 지침을 따릅니다.Cisco MIB 홈 페이지의 각 Cisco 플랫폼에서 지원되는 MIB 모듈 정의 파일 및 MIB 목록을 찾을 수 있습니다.

SNMP 버전

Cisco IOS Software는 다음 버전의 SNMP를 지원합니다.

- SNMPv1—RFC 1157이 정의하는 전체 인터넷 표준.RFC 1157 은 RFC 1067 및 RFC 1098로 게시된 이전 버전을 대체합니다 .보안은 커뮤니티 문자열을 기반으로 합니다.
- SNMPv2c—SNMPv2c는 SNMPv2를 위한 커뮤니티 문자열 기반 관리 프레임워크입니다. SNMPv2c(c는 커뮤니티를 나타냅니다)는 RFC 1901 , RFC 1905 , RFC 1906 을 정의하는 실험적 인터넷 프로토콜입니다.SNMPv2c는 SNMPv2p(SNMPv2 Classic)의 프로토콜 작업 및 데이터 유형의 업데이트입니다.SNMPv2c는 SNMPv1의 커뮤니티 기반 보안 모델을 사용합니다.
- SNMPv3—SNMPv3은 RFC 2273 , RFC 2274 , RFC 2275 정의하는 상호 운용 가능한 표준 기반 프로토콜입니다.SNMPv3는 네트워크를 통한 인증 및 패킷 암호화 조합으로 디바이스에 대한 보안 액세스를 제공합니다.SNMPv3에서 제공하는 보안 기능은 다음과 같습니다.Message integrity(메시지 무결성) - 패킷이 전송 중에 손상되지 않았는지 확인합니다.Authentication(인증) - 메시지가 유효한 소스의 메시지인지 확인합니다.Encryption(암호화) - 패킷의 내용을 스크램블링하여 권한이 없는 소스에 의한 검색을 방지합니다.

SNMPv1 및 SNMPv2c 모두 커뮤니티 기반 보안 형식을 사용합니다.IP 주소 ACL 및 비밀번호는 에이전트 MIB에 액세스할 수 있는 관리자 커뮤니티를 정의합니다.

SNMPv2c 지원에는 대량 검색 메커니즘과 관리 스테이션에 대한 보다 자세한 오류 메시지 보고가 포함됩니다.벌크 검색 메커니즘은 테이블 및 많은 양의 정보를 읽어들일 수 있도록 지원하므로 필요한 라운드 트립 수를 최소화할 수 있습니다.SNMPv2c의 향상된 오류 처리 지원에는 다양한 종류의 오류 조건을 구분하는 확장된 오류 코드가 포함됩니다.이러한 조건은 SNMPv1의 단일 오류 코드를 통해 보고됩니다. 오류 반환 코드는 이제 오류 유형을 보고합니다.

SNMPv3는 보안 모델과 보안 수준을 모두 제공합니다.보안 모델은 사용자 및 사용자가 상주하는 그룹에 대해 설정된 인증 전략입니다.보안 레벨은 보안 모델 내에서 허용되는 보안 레벨입니다.보안 모델과 보안 수준의 조합은 SNMP 패킷을 처리할 때 사용할 보안 메커니즘을 결정합니다.

일반 SNMP 컨피그레이션

SNMP 관리를 활성화하려면 모든 고객 스위치에서 다음 명령을 실행합니다.

- SNMP ACL에 대한 명령:

```
Switch(config)#access-list 98 permit ip_address
!--- This is the SNMP device ACL.
```

- 전역 SNMP 명령:

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

SNMP 트랩 권장 사항

SNMP는 네트워크 관리의 기반이며 모든 네트워크에서 사용 및 사용 가능합니다.

SNMP 에이전트는 여러 관리자와 통신할 수 있습니다.따라서 SNMPv1을 사용하는 한 관리 스테이션 및 SNMPv2를 사용하는 다른 관리 스테이션과의 통신을 지원하도록 소프트웨어를 구성할 수 있습니다. NMS 플랫폼에서 SNMPv3 네트워크 장치 지원이 다소 지연되므로 대부분의 고객 및 NMS는 여전히 SNMPv1 및 SNMPv2c를 사용합니다.

사용 중인 모든 기능에 대해 SNMP 트랩을 활성화합니다.원하는 경우 다른 기능을 비활성화할 수 있습니다.트랩을 활성화한 후 **test snmp** 명령을 실행하고 NMS에서 오류에 대한 적절한 처리를 설정할 수 있습니다.이러한 처리의 예로는 호출기 알림 또는 팝업이 있습니다.

모든 트랩은 기본적으로 비활성화되어 있습니다.다음 예와 같이 코어 스위치의 모든 트랩을 활성화합니다.

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

또한 라우터 및 스위치에 대한 인프라 링크, 주요 서버 포트 등 주요 포트에 대한 포트 트랩을 활성화합니다.호스트 포트와 같은 다른 포트에는 지원 기능이 필요하지 않습니다.포트를 구성하고 링크 작동/중단 알림을 활성화하려면 다음 명령을 실행합니다.

```
Switch(config-if)#snmp trap link-status
```

다음으로, 트랩을 수신할 디바이스를 지정하고 트랩에서 적절하게 동작합니다.이제 각 트랩 대상을 SNMPv1, SNMPv2 또는 SNMPv3 수신자로 구성할 수 있습니다.SNMPv3 디바이스의 경우 UDP 트랩 대신 신뢰할 수 있는 알림을 전송할 수 있습니다.컨피그레이션은 다음과 같습니다.

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

SNMP 폴링 권장 사항

이러한 MIB가 캠퍼스 네트워크에서 폴링되거나 모니터링되는 주요 MIB인지 확인합니다.

참고: 이 권장 사항은 Cisco Network Management Consulting 그룹의 것입니다.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Network Time Protocol(네트워크 타이밍 프로토콜)

목적

NTP(Network Time Protocol), RFC 1305 는 분산 시간 서버 및 클라이언트 집합 간에 시간 유지를 동기화합니다.NTP는 시스템 로그 생성 시 및 다른 시간별 이벤트가 발생할 때 이벤트의 상관관계를 설정할 수 있습니다.

운영 개요

RFC 958 문서화된 NTP가 먼저 있습니다.그러나 NTP는 RFC 1119 (NTP 버전 2)를 통해 발전했습니다.RFC 1305 는 이제 NTP를 정의합니다. NTP는 세 번째 버전입니다.

NTP는 컴퓨터 클라이언트 또는 서버의 시간을 다른 서버 또는 참조 시간 소스(예: 라디오, 위성 수신기 또는 모뎀)와 동기화합니다.NTP는 동기화된 기본 서버를 기준으로 LAN의 ms 및 WAN의 최대 수십 ms 내에 있는 클라이언트 정확성을 제공합니다.예를 들어 NTP를 사용하여 GPS(Global Positioning Service) 수신기를 통해 UTC(Coordinated Universal Time)를 조정할 수 있습니다.

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.

NTP는 UDP를 통해 실행되며, IP를 통해 실행됩니다.모든 NTP 통신에서는 UTC를 사용합니다. 이 시간은 Greenwich Mean Time과 동일합니다.

현재 NTP 버전 3(NTPv3) 및 NTP 버전 4(NTPv4) 구현을 사용할 수 있습니다.현재 사용 중인 최신 소프트웨어 릴리스는 NTPv4이지만 공식 인터넷 표준은 여전히 NTPv3입니다. 또한 일부 운영 체제 공급업체는 프로토콜의 구현을 사용자 정의합니다.

NTP 보호

또한 NTP 구현에서는 시간을 정확하게 확인할 수 없는 시스템에 대한 동기화를 피하려고 시도합니다.NTP는 다음 두 가지 방법으로 이를 수행합니다.

- NTP는 자체적으로 동기화되지 않은 시스템과 동기화하지 않습니다.
- NTP는 여러 시스템에서 보고하는 시간을 항상 비교하며, 시간이 다른 컴퓨터와 크게 다른 시스템과 동기화하지 않습니다. 이 시스템은 계층이 낮은 경우에도 마찬가지입니다.

연결

NTP를 실행하는 시스템 간 통신(연결)은 일반적으로 정적으로 구성됩니다.각 시스템에는 연관을 형성해야 하는 모든 시스템의 IP 주소가 지정됩니다.정확한 시간 제한은 각 머신 쌍 간에 NTP 메시지를 교환하고 연결을 통해 가능합니다.그러나 LAN 환경에서는 IP 브로드캐스트 메시지를 사용하도록 NTP를 구성할 수 있습니다.이 방법을 사용하면 브로드캐스트 메시지를 보내거나 받도록 시스템을 구성할 수 있지만, 정보 흐름은 단방향 전용이므로 시간 보기의 정확성이 다소 줄어듭니다.

네트워크가 인터넷과 격리된 경우 Cisco NTP 구현에서는 다른 방법을 사용하여 시간을 실제로 결정한 경우 NTP 사용과 동기화되는 것처럼 작동하도록 시스템을 구성할 수 있습니다.다른 시스템은 NTP를 사용하여 해당 시스템과 동기화합니다.

NTP 연결은 다음 중 하나일 수 있습니다.

- 피어 연결즉, 이 시스템은 다른 시스템과 동기화하거나 다른 시스템에서 동기화하도록 허용할 수 있습니다.
- 서버 연결즉, 이 시스템만 다른 시스템과 동기화됩니다.다른 시스템이 이 시스템과 동기화되지 않습니다.

다른 시스템과 NTP 연결을 구성하려면 글로벌 컨피그레이션 모드에서 다음 명령 중 하나를 사용합니다.

명령	목적
ntp 피어 *ip-address* [normal-sync] [version *number*] [key *key-id*] [source *interface*] [prefer]	다른 시스템과의 피어 연결을 구성합니다.
ntp server *ip-address* [version *number*] [key *key-id*] [source *interface*] [prefer]	다른 시스템과 서버 연결 구성

참고: 연결의 한쪽 끝만 구성해야 합니다.다른 시스템은 자동으로 연결을 설정합니다.

공개 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.100개의 공용 보조 서버가 기본 서버에 동기화되어 있습니다.이러한 서버는 인터넷에 있는 총 100,000개 이상의 클라이언트 및 서버에 대한 동기화를 제공합니다.Public NTP Servers(공용 NTP 서버) 페이지는 현재 목록을 유지 관리하고 자주 업데이트됩니다.

또한 일반에게 일반적으로 제공되지 않는 수많은 프라이빗 기본 및 보조 서버가 있습니다.공용 NTP 서버 목록 및 사용 방법에 대한 자세한 내용은 Network Time Protocol Project (University of Delaware)를 참조하십시오.이러한 공용 인터넷 NTP 서버를 사용할 수 있고 정확한 시간을 생성할 수 있다는 보장이 없습니다.따라서 다른 옵션을 고려해야 합니다.예를 들어, 여러 라우터에 직접 연

결되는 다양한 독립형 GPS 디바이스를 사용합니다.

또 다른 옵션은 Stratum 1 마스터로 설정된 다양한 라우터를 사용하는 것입니다.그러나 이러한 라우터는 사용하지 않는 것이 좋습니다.

지층

NTP는 신뢰할 수 있는 시간 소스의 NTP 홉의 수를 설명하기 위해 계층을 사용합니다.계층 1 시간 서버에는 직접 연결된 라디오 또는 원자 시계가 있습니다.계층 2 시간 서버는 계층 1 시간 서버에서 시간을 수신하는 등NTP를 실행하는 시스템은 NTP를 통해 통신하도록 구성된 가장 낮은 계층 번호의 시스템을 시간 소스로 자동으로 선택합니다.이 전략은 NTP 스피커의 자체 구성 트리를 효과적으로 구성합니다.

NTP는 시간이 정확하지 않을 수 있는 디바이스에 대한 동기화를 방지합니다.자세한 내용은 *Network Time Protocol*의 NTP Safety 섹션을 참조하십시오.

서버 피어 관계

- 서버는 클라이언트 요청에 응답하지만 클라이언트 시간 소스의 날짜 정보를 통합하려고 시도하지 않습니다.
- 피어는 클라이언트 요청에 응답하고 더 나은 시간 소스를 위한 잠재적 후보로 클라이언트 요청을 사용하고 클럭 빈도를 안정화하려고 시도합니다.
- 진정한 피어가 되려면 연결의 양쪽이 피어 관계에 들어가야 합니다. 한 사용자가 피어 역할을 하고 다른 사용자가 서버 역할을 하는 상황이 아니라 피어 관계를 설정해야 합니다.신뢰할 수 있는 호스트만 피어로서 다른 호스트와 통신할 수 있도록 피어 교환 키를 갖도록 합니다.
- 서버에 대한 클라이언트 요청에서 서버는 클라이언트에 응답하고 클라이언트가 질문을 한 것을 잊어버립니다.
- 피어에 대한 클라이언트 요청에서 서버는 클라이언트에 응답합니다.서버는 클라이언트의 시간 유지 관리 작업 및 클라이언트가 실행하는 계층 서버를 추적하기 위해 클라이언트에 대한 상태 정보를 유지합니다.

NTP 서버는 문제 없이 수천 개의 클라이언트를 처리할 수 있습니다.그러나 NTP 서버가 몇 개 이상의 클라이언트(최대 몇 백 개)를 처리할 경우, 상태 정보를 유지할 수 있는 서버 기능에 메모리가 영향을 미칩니다.NTP 서버가 권장 수량보다 많은 양을 처리할 경우, 상자에 더 많은 CPU 리소스와 대역폭이 사용됩니다.

NTP 서버와의 통신 모드

서버와 통신하는 두 가지 별도의 모드입니다.

- 브로드캐스트 모드
- 클라이언트/서버 모드

브로드캐스트 모드에서는 클라이언트가 수신 대기합니다.클라이언트/서버 모드에서 클라이언트는 서버를 폴링합니다.속도 때문에 WAN 링크가 포함되지 않은 경우 NTP 브로드캐스트를 사용할 수 있습니다.WAN 링크를 통과하려면 클라이언트/서버 모드(폴링)를 사용합니다. 브로드캐스트 모드는 많은 클라이언트가 서버를 폴링해야 할 수 있는 LAN용으로 설계되었습니다.브로드캐스트 모드가 없을 경우 이러한 폴링은 네트워크에서 많은 수의 패킷을 생성할 수 있습니다.NTP 멀티캐스트는 아직 NTPv3에서 사용할 수 없지만 NTPv4에서 사용할 수 있습니다.

기본적으로 Cisco IOS Software는 NTPv3 사용과 통신하지만 이 소프트웨어는 이전 버전의 NTP와 역호환됩니다.

폴링

NTP 프로토콜을 사용하면 클라이언트가 언제든지 서버를 쿼리할 수 있습니다.

Cisco 상자에서 NTP를 처음 구성할 때 NTP는 NTP_MINPOLL(2^4=16초) 간격으로 8개의 쿼리를 신속하게 전송합니다.NTP_MAXPOLL은 2^14초(16,384초 또는 4시간, 33분, 4초)입니다. 이 기간은 NTP가 응답을 위해 다시 폴링하기 전 가장 긴 기간입니다.현재 Cisco는 사용자가 POLL 시간을 수동으로 수행하도록 허용하는 방법이 없습니다.

NTP 폴링 카운터가 2^6(64)초 또는 1분, 4초에서 시작됩니다.이 시간은 2개의 서버가 서로 동기화될 때 2의 제곱으로 증가하여 2^10까지 증가합니다. 서버 또는 피어 구성에 따라 64, 128, 256, 512 또는 1024초 중 하나의 간격으로 동기화 메시지가 전송될 것으로 예상할 수 있습니다.폴링 사이에 긴 시간은 현재 클럭이 위상 잠금 루프로 인해 안정화되면서 발생합니다.위상 잠금 루프를 통해 로컬 클럭 크리스탈을 최대 1024초(17분)까지 다듬습니다.

시간은 64초~1024초(64, 128, 256, 512 또는 1024초마다 1회)의 전력으로 달라집니다. 시간은 패킷을 보내고 수신하는 단계적 잠금 루프를 기반으로 합니다.시간에 지터가 많이 있으면 폴링이 더 자주 발생합니다.참조 시계가 정확하며 네트워크 연결이 일관적인 경우 폴링 시간은 각 폴링 사이에 1024초로 통합됩니다.

클라이언트와 서버 간의 연결이 변경되면 NTP 폴링 간격이 변경됩니다.더 나은 연결을 통해 폴링 간격이 더 깁니다.이 경우 더 나은 연결은 NTP 클라이언트가 마지막 8개 요청에 대해 8개의 응답을 수신했음을 의미합니다.그러면 폴링 간격이 두 배로 늘어납니다.응답이 한 개 누락되면 폴링 간격이 절반으로 감소합니다.폴링 간격은 64초부터 시작하여 최대 1024초로 이동합니다.최상의 경우 폴링 간격이 64초에서 1024초로 이동하는 데 필요한 시간은 2시간을 약간 넘습니다.

브로드캐스트

NTP 브로드캐스트는 전달되지 않습니다.ntp **브로드캐스트** 명령을 실행하면 라우터가 구성된 인터페이스에서 NTP 브로드캐스트를 시작합니다.

일반적으로 **ntp 브로드캐스트** 명령을 실행하여 클라이언트 엔드 스테이션 및 서버를 서비스하기 위해 LAN에 NTP 브로드캐스트를 전송해야 합니다.

시간 동기화

클라이언트와 서버의 동기화는 여러 패킷 교환으로 구성됩니다.각 교환은 요청/응답 쌍입니다.클라이언트가 요청을 보내면 클라이언트는 로컬 시간을 보낸 패킷에 저장합니다.서버가 패킷을 수신하면 현재 시간의 자체 추정치를 패킷에 저장하고 패킷이 반환됩니다.회신이 수신되면 수신자는 패킷의 출장 시간을 예측하기 위해 자체 수신 시간을 한 번 더 기록합니다.

이러한 시간 차이를 사용하여 서버에서 요청자에게 패킷을 전송하는 데 필요한 시간을 추정할 수 있습니다.그 왕복 시간은 현재 시간의 추정을 고려한다.왕복 시간이 짧을수록 현재 시간의 추정치가 더 정확합니다.

몇 개의 동의 패킷 교환이 이루어질 때까지 시간이 허용되지 않습니다.샘플의 품질을 추정하기 위해 몇 가지 필수 값을 멀티스테이지 필터에 넣습니다.일반적으로 NTP 클라이언트가 서버와 동기화하려면 약 5분이 필요합니다.흥미롭게도, 이것은 어떠한 지연도 전혀 없는 지역 참조 시계에서도 마찬가지입니다.

또한 네트워크 연결의 품질도 최종 정확성에 영향을 줍니다.지연이 각기 다른 느리고 예측할 수 없는 네트워크는 시간 동기화에 나쁜 영향을 미칩니다.

NTP를 동기화하려면 128ms 미만의 시간 차이가 필요합니다.인터넷의 일반적인 정확도는 네트워크 지연에 따라 달라질 수 있는 약 5ms~100ms입니다.

NTP 트래픽 레벨

NTP에서 사용하는 대역폭은 최소 수준입니다.피어가 교환하는 폴링 메시지 간의 간격은 일반적으로 17분(1024초)마다 메시지를 1개 이하로 되돌립니다. 신중하게 계획하면 WAN 링크를 통해 라우터 네트워크 내에서 이를 유지할 수 있습니다.NTP 클라이언트가 로컬 NTP 서버에 피어링하도록 하고, WAN을 통해 Stratum 2 서버인 중앙 사이트 코어 라우터에 피어링하지 않도록 합니다.

컨버지드 NTP 클라이언트는 서버당 평균 0.6bps를 사용합니다.

Cisco NTP 권장 사항

- Cisco는 정확성과 안정성을 높이기 위해 여러 시간 서버와 다양한 네트워크 경로를 사용하는 것이 좋습니다.일부 컨피그레이션에는 우발적이거나 악의적인 프로토콜 공격을 방지하기 위한 암호화 인증이 포함됩니다.
- RFC에 따라 NTP는 폴링하는 모든 서버가 신뢰할 수 있는지 확실하지 않더라도 유효한 시간을 내기 위해 여러 개의 다른 시간 서버를 폴링하고 복잡한 통계 분석을 사용할 수 있도록 설계되었습니다.NTP는 모든 클럭의 오류를 추정합니다.따라서 모든 NTP 서버는 현재 오류의 예상 값과 함께 시간을 반환합니다.여러 시간 서버를 사용하는 경우 NTP는 이러한 서버가 일정 시간 동안 동의하도록 합니다.
- Cisco의 NTP 구현은 계층 1 서비스를 지원하지 않습니다.라디오나 원자 시계는 연결할 수 없습니다.Cisco는 네트워크에 대한 시간 서비스를 IP 인터넷에서 사용 가능한 공용 NTP 서버에서 파생시키는 것이 좋습니다.
- 모든 클라이언트 스위치가 NTP 서버에 정기적으로 시간 요청을 전송하도록 합니다.신속한 동기화를 위해 클라이언트당 최대 10개의 서버/피어 주소를 구성할 수 있습니다.
- 프로토콜 오버헤드를 줄이기 위해 보조 서버는 NTP를 통해 나머지 로컬 네트워크 호스트에 시간을 분산합니다.신뢰성의 이익을 위해, 선택한 호스트에 기본 및/또는 보조 서버 또는 이들 간의 통신 경로에 장애가 발생할 경우 백업에 사용할 정확도가 낮지만 비용이 덜 드는 시계를 제공할 수 있습니다.
- **ntp update-calendar**—일반적으로 NTP는 시스템 클럭만 변경합니다.이 명령을 사용하면 NTP에서 달력의 날짜/시간 정보를 업데이트할 수 있습니다.업데이트는 NTP 시간이 동기화된 경우에만 수행됩니다.그렇지 않으면 달력은 자체 시간을 유지하고 NTP 시간 또는 시스템 클럭의 영향을 받지 않습니다.항상 하이엔드 라우터에서 사용합니다.
- **clock calendar-valid**—이 명령은 달력 정보가 유효하고 동기화되었음을 선언합니다.NTP 마스터에서 이 옵션을 사용합니다.이 구성이 구성되지 않은 경우, 달력이 있는 하이엔드 라우터는 NTP 마스터 회선이 있더라도 시간이 권한이 없다고 생각합니다.
- 15를 초과하는 계층 번호는 동기화되지 않은 것으로 간주됩니다.따라서 클럭이 동기화되지 않은 라우터에서 **show ntp status** 명령의 출력에서 stratum 16을 볼 수 있습니다.마스터가 퍼블릭 NTP 서버와 동기화되는 경우 NTP 마스터 라인의 계층 번호가 폴링하는 퍼블릭 서버의 최상위 계층 번호보다 1 또는 2개 높은지 확인합니다.
- 많은 고객이 Cisco IOS Software 플랫폼의 서버 모드에서 NTP를 구성했으며, 인터넷 또는 라디오 클럭의 여러 안정적인 피드에서 동기화되었습니다.스위치 수가 많은 스위치를 운영할 때 서버 모드의 더 간단한 대안은 스위치드 도메인의 관리 VLAN에서 브로드캐스트 모드에서 NTP를 활성화하는 것입니다.이 메커니즘을 통해 Catalyst는 단일 브로드캐스트 메시지에서 시계를 수신할 수 있습니다.그러나 정보 흐름이 단방향으로 이루어지기 때문에 시간 관리의 정확성은 다소 낮아집니다.

- 루프백 주소를 업데이트의 소스로 사용하면 일관성에도 도움이 될 수 있습니다.다음과 같은 두 가지 방법으로 보안 문제를 해결할 수 있습니다.Cisco에서 권장하는 서버 업데이트 제어인증별

NTP 전역 컨피그레이션 명령

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

NTP 상태 명령

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

라우터가 NTP 마스터 역할을 할 때 Cisco 라우터의 참조 클럭 주소입니다.라우터가 NTP 서버와 동기화되지 않은 경우 라우터는 이 주소를 참조 ID로 사용합니다.컨피그레이션 및 명령에 대한 자세한 내용은 Performing Basic System Management(기본 시스템 관리 수행)의 *Configuring NTP(NTP 구성) 섹션을* 참조하십시오.

Cisco 검색 프로토콜

목적

CDP는 모든 Cisco 라우터, 브리지, 액세스 서버 및 스위치에서 레이어 2(데이터 링크 계층)를 통해 실행됩니다.CDP를 사용하면 네트워크 관리 애플리케이션에서 이미 알려진 디바이스의 네이버인 Cisco 디바이스를 검색할 수 있습니다.특히 네트워크 관리 애플리케이션은 하위 계층 투명 프로토콜을 실행하는 인접 디바이스를 검색할 수 있습니다.네트워크 관리 애플리케이션은 CDP를 통해 인접 디바이스의 디바이스 유형 및 SNMP 에이전트 주소를 학습할 수 있습니다.이 기능을 사용하면 애플리케이션에서 SNMP 쿼리를 인접 디바이스로 전송할 수 있습니다.

CDP 기능과 연결된 show 명령을 사용하면 네트워크 엔지니어가 다음 정보를 확인할 수 있습니다.

- 인접한 다른 CDP 지원 디바이스의 모듈/포트 번호
- 인접 디바이스의 주소:MAC 주소IP 주소포트 채널 주소
- 인접 디바이스 소프트웨어 버전
- 인접 디바이스에 대한 정보:속도이중VTP 도메인네이티브 VLAN 설정

운영 개요 섹션에서는 CDP 버전 1(CDPv1)을 통한 CDP 버전 2(CDPv2)의 몇 가지 향상된 기능에 대해 설명합니다.

운영 개요

CDP는 SNAP을 지원하는 모든 LAN 및 WAN 미디어에서 실행됩니다.

각 CDP 구성 디바이스는 멀티캐스트 주소로 주기적인 메시지를 전송합니다.각 디바이스는 디바이스에서 SNMP 메시지를 수신할 수 있는 하나 이상의 주소를 알립니다.또한 광고에는 TTL(Time-to-Live) 또는 TTL(Hold Time) 정보도 포함됩니다.이 정보는 폐기 전에 수신 디바이스가 CDP 정보를 보유하는 시간을 나타냅니다.

CDP는 유형 코드 2000으로 SNAP 캡슐화를 사용합니다.이더넷, ATM 및 FDDI에서 목적지 멀티캐스트 주소 01-00-0c-cc-cc-cc가 사용됩니다.토큰 링에서 기능 주소 c000.0800.0000이 사용됩니다.CDP 프레임은 주기적으로 1분마다 전송됩니다.

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

이 표에서는 CDPv1에서 지원하는 매개변수를 제공합니다.

매개변수	유형	설명
1	장치 ID	디바이스 또는 하드웨어 일련 번호의 호스트 이름(ASCII)
2	주소	업데이트를 전송하는 인터페이스의 레이어 3 주소
3	포트 ID	CDP 업데이트가 전송되는 포트
4	기능	다음과 같은 방식으로 디바이스 기능 기능에 대해 설명합니다. • 라우터:0x01 • SR[1] 브리지:0x04 • 스위치:0x08(레이어 2 및/또는 레이어 3 스위칭 제공) • 호스트:0x10 • IGMP 조건부 필터링:0x20 • 브리지 또는 스위치는 비라우터 포트에서 IGMP 보고서 패킷을 전달하지 않습니다.
5	버전	소프트웨어 버전을 포함하는 문자열 **참고:** show **version** 명령 출력에 동일한 정보가 표시됩니다.
6	플랫폼	하드웨어 플랫폼(예: WS-C5000, WS-C6009 및 Cisco RSP[2])

[1] SR = source-route.

[2] RSP = Route Switch Processor.

CDPv2에서는 추가 유형, 길이, 값(TLV)이 도입되었습니다.CDPv2는 모든 TLV를 지원합니다.그러나 이 표는 스위치드 환경과 Catalyst 소프트웨어가 사용하는 환경에서 특히 유용할 수 있는 매개변수를 제공합니다.

스위치가 CDPv1을 실행하면 스위치가 CDPv2 프레임을 삭제합니다.스위치에서 CDPv2를 실행하고 인터페이스에서 CDPv1 프레임을 수신하면 CDPv2 프레임 외에도 해당 인터페이스에서 CDPv1 프레임을 전송하기 시작합니다.

매개변수	유형	설명
9	VTP 도메인	VTP 도메인(디바이스에 구성된 경우)
10	네이티브 VLAN	dot1q에서 포트가 트렁킹되지 않은 경우 포트가 있는 VLAN의 프레임은 태그가 지정되지 않은 상태로 유지됩니다.일반적으로 이를 네이티브 VLAN이라고 합니다.
11	전이중/반이중	이 TLV에는 전송 포트의 이중 설정이 포함되어 있습니다.
14	어플라이언스 VLAN-ID	별도의 VLAN ID(보조 VLAN)를 통해 VoIP 트래픽을 다른 트래픽과 차별화할 수 있습니다.
16	전력 소비량	연결된 디바이스에서 mW로 소비될 것으로 예상되는 최대 전력 양입니다.
17	MTU	CDP 프레임이 전송되는 인터페이스의 MTU.
18	확장된 트러스트	포트가 확장 트러스트 모드임을 나타냅니다.
19	신뢰할 수 없는 포트에 대한 COS	연결된 스위칭 장치의 신뢰할 수 없는 포트에서 수신된 모든 패킷을 표시하는 데 사용되는 CoS(Class of Service) 값입니다.
20	시스템 이름	디바이스의 정규화된 도메인 이름(알 수 없는 경우 0)입니다.
25	전원 요청	적절한 전력 수준을 협상하기 위해 전원 공급 장치에서 전송됨
26	전원 사용 가능	스위치에서 전송됨전원 공급 장치가 적절한 전원 설정을 협상하고 선택할 수 있도록 허용합니다.

CDPv2/PoE(Power over Ethernet)

Catalyst 6500/6000 및 4500/4000과 같은 일부 스위치는 UTP(Unshielded Twisted Pair) 케이블을 통해 전원 공급 장치에 전원을 공급할 수 있습니다.CDP(매개변수 16, 25, 26)를 통해 수신되는 정보는 스위치 전원 관리를 최적화하는 데 도움이 됩니다.

CDPv2/Cisco IP Phone 상호 작용

Cisco IP Phone은 외부 연결 10/100Mbps 이더넷 장치에 대한 연결을 제공합니다.이러한 연결은 IP 전화 내에서 내부 3포트 레이어 2 스위치를 통합하여 구현됩니다.내부 스위치 포트는 다음과 같습니다.

- P0(내부 IP 전화 장치)
- P1(외부 10/100Mbps 포트)
- P2(스위치에 연결되는 외부 10/100Mbps 포트)

dot1q 액세스 트렁크 포트를 구성하는 경우 스위치 포트의 개별 VLAN에서 음성 트래픽을 전송할 수 있습니다.이 추가 VLAN은 보조(CatOS) 또는 음성(Cisco IOS Software) VLAN이라고 합니다.따라서 IP 전화의 dot1q 태그 처리된 트래픽은 보조/음성 VLAN에서 전송할 수 있으며, 태그되지 않은 트래픽은 액세스 VLAN을 통해 전화의 외부 10/100Mbps 포트를 통해 전송할 수 있습니다.

Catalyst 스위치는 CDP를 통해 음성 VLAN ID를 IP 전화기에 알릴 수 있습니다(매개변수-14:어플라이언스 VLAN-ID TLV)입니다. 그 결과, IP Phone은 적절한 VLAN ID와 802.1p 우선 순위를 가진 모든 VoIP 관련 패킷에 태그를 지정합니다.이 CDP TLV는 어플라이언스 ID 매개변수를 통해 IP 전화가 연결되어 있는지 확인하는 데에도 사용됩니다.

이 개념은 QoS 정책을 개발할 때 악용될 수 있습니다.다음 세 가지 방법으로 Catalyst 스위치가 IP 전화와 상호 작용하도록 구성할 수 있습니다.

- 신뢰 장치 Cisco IP PhoneCDP를 통해 IP 전화가 탐지된 경우에만 조건부로 CoS를 신뢰합니다.CDP Parameter-14를 통해 IP 전화가 탐지될 때마다 포트 신뢰 상태가 Trust COS로 설정됩니다.IP 전화기가 탐지되지 않은 경우 포트는 Untrusted입니다.
- 확장된 트러스트이 스위치는 CDP(Parameter-18)를 통해 IP 전화기에 알림으로써 외부 10/100Mbps 디바이스 포트에서 수신되는 모든 프레임을 신뢰할 수 있습니다.
- 신뢰할 수 없는 포트에 대한 COS 재작성이 스위치는 CDP(Parameter-19)를 통해 IP 전화기에 알림하여 외부 10/100Mbps 디바이스 포트에서 수신되는 802.1p CoS 값을 재작성할 수 있습니다.**참고:** 기본적으로 IP 전화기에서 외부 10/100Mbps 포트에서 수신되는 모든 트래픽은 Untrusted입니다.

참고: 다음은 Cisco 이외의 IP Phone을 스위치에 연결하는 방법의 예입니다.

참고: 예를 들어

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Cisco 구성 권장 사항

CDP에서 제공하는 정보는 레이어 2 연결 문제를 해결할 때 매우 유용합니다.작업을 지원하는 모든 디바이스에서 CDP를 활성화합니다.다음 명령을 실행합니다.

- 스위치에서 CDP를 전역적으로 활성화하려면
  ```
  Switch(config)#cdp run
  ```

- 포트별로 CDP를 활성화하려면
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

구성 체크리스트

전역 명령

스위치 컨피그레이션 프로세스를 시작하려면 로그인, 활성화 및 전역 컨피그레이션 모드로 들어갑니다.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

일반 전역 명령(전사적)

이 Global Commands 섹션에는 고객 엔터프라이즈 네트워크의 모든 스위치에 적용할 전역 명령이 나열됩니다.

이 컨피그레이션에는 초기 컨피그레이션에 추가할 수 있는 권장 전역 명령이 포함되어 있습니다.텍스트를 복사하여 CLI에 붙여넣으려면 먼저 출력에서 값을 변경해야 합니다.전역 컨피그레이션을 적용하려면 다음 명령을 실행합니다.

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
```

```
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

각 스위치 섀시에 특정한 전역 명령

이 섹션의 전역 명령은 네트워크에 설치된 각 스위치 섀시에만 적용됩니다.

섀시별 컨피그레이션 변수

날짜와 시간을 설정하려면 다음 명령을 실행합니다.

```
Switch#clock set hh:mm:ss day month year
```

디바이스 호스트 이름을 설정하려면 다음 명령을 실행합니다.

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

```
Switch(config)#hostname Cat6500
```

관리를 위한 루프백 인터페이스를 구성하려면 다음 명령을 실행합니다.

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Supervisor Engine Cisco IOS Software 버전을 표시하려면 다음 명령을 실행합니다.

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

MSFC 부트 파일 수정 버전을 표시하려면 다음 명령을 실행합니다.

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

SNMP 서버 연락처 정보 및 위치를 지정하려면 다음 명령을 실행합니다.

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

기존 Supervisor Engine에서 새 Supervisor Engine으로 시작 컨피그레이션을 복사하려면 기존 Supervisor 인터페이스의 컨피그레이션과 같은 컨피그레이션이 손실될 수 있습니다.컨피그레이션 문제가 발생하는지 확인하기 위해 텍스트 파일에 컨피그레이션을 복사한 후 콘솔에 붙여넣는 것이 좋습니다.

인터페이스 명령

Cisco 기능 포트 유형

Cisco IOS Software의 스위치 포트를 인터페이스라고 합니다.Cisco IOS Software에는 두 가지 유형의 인터페이스 모드가 있습니다.

- 레이어 3 라우티드 인터페이스
- 레이어 2 스위치 인터페이스

인터페이스 기능은 포트를 구성한 방법을 나타냅니다.포트 컨피그레이션은 다음과 같을 수 있습니다.

- 라우티드 인터페이스
- SVI(Switched Virtual Interface)
- 액세스 포트
- 트렁크
- EtherChannel

- 이러한

인터페이스 유형은 포트 유형을 참조합니다.포트 유형은 다음 중 하나일 수 있습니다.

- FE
- GE
- 포트 채널

이 목록에서는 다양한 Cisco IOS 소프트웨어 인터페이스 기능에 대해 간략하게 설명합니다.

- Routed Physical Interface(라우팅된 물리적 인터페이스)(기본값) - 스위치의 각 인터페이스는 기본적으로 라우팅된 Layer 3 인터페이스이며, 이는 모든 Cisco 라우터와 유사합니다.라우티드 인터페이스는 고유한 IP 서브넷에 있어야 합니다.
- 액세스 스위치 포트 인터페이스 - 이 기능은 동일한 VLAN에 인터페이스를 배치하는 데 사용됩니다.포트는 라우티드 인터페이스에서 스위치드 인터페이스로 변환되어야 합니다.
- SVI - SVI는 VLAN 간 라우팅에 대한 액세스 스위치 포트를 포함하는 VLAN에 연결할 수 있습니다.서로 다른 VLAN의 액세스 스위치 포트 간에 경로나 브리지를 원하는 경우 SVI를 VLAN과 연결하도록 구성합니다.
- 트렁크 스위치 포트 인터페이스 - 이 기능은 여러 VLAN을 다른 디바이스로 전달하는 데 사용됩니다.포트는 라우티드 인터페이스에서 트렁크 스위치 포트로 변환해야 합니다.
- EtherChannel—EtherChannel은 이중화 및 로드 밸런싱을 위해 개별 포트를 단일 논리적 포트로 번들링하는 데 사용됩니다.

Cisco 기능 포트 유형 권장 사항

인터페이스에 적용할 매개변수를 결정하는 데 도움이 되도록 이 섹션의 정보를 사용합니다.

참고: 일부 인터페이스별 명령은 가능한 경우 통합됩니다.

자동 협상

다음 상황 중 하나에서 자동 협상을 사용하지 마십시오.

- 스위치 및 라우터와 같은 네트워크 인프라 디바이스를 지원하는 포트
- 서버 및 프린터와 같이 일시적이지 않은 다른 엔드 시스템의 경우

이러한 10/100Mbps 링크 컨피그레이션의 속도와 듀플렉스를 위해 수동으로 구성합니다.컨피그레이션은 일반적으로 100Mbps 전이중입니다.

- 100MB 링크 스위치 간
- 100MB 링크 스위치-서버
- 100MB 링크 스위치-라우터

다음과 같은 방법으로 이 설정을 구성할 수 있습니다.

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco는 최종 사용자를 위해 10/100Mbps 링크 구성을 권장합니다.모바일 근로자 및 임시 호스트는 다음과 같이 자동 협상이 필요합니다.

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

기가비트 인터페이스의 기본값은 .그러나 autonegotiation이 활성화되어 있는지 확인하기 위해 이러한 명령을 실행합니다.Cisco는 기가비트 협상을 활성화하는 것을 권장합니다.

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

스패닝 트리 루트

네트워크 설계를 고려하여 각 VLAN의 루트에 가장 적합한 스위치를 식별합니다.일반적으로 네트워크 중간에 강력한 스위치를 선택합니다.루트 브리지를 네트워크 중앙에 두고 루트 브리지를 서버와 라우터에 직접 연결합니다.이 설정은 일반적으로 클라이언트에서 서버와 라우터까지의 평균 거리를 줄입니다.자세한 내용은 스패닝 트리 프로토콜 문제 및 관련 설계 고려 사항을 참조하십시오.

스위치를 지정된 VLAN의 루트로 강제 지정하려면 다음 명령을 실행합니다.

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

스패닝 트리 포트Fast

PortFast는 엔드 스테이션이 스위치에 연결될 때 발생하는 초기 연결 지연 속도를 높이기 위해 액세스 포트에서 정상적인 스패닝 트리 작업을 우회합니다.PortFast에 대한 자세한 내용은 PortFast 및 기타 명령을 사용하여 워크스테이션 시작 연결 지연 문제 해결을 참조하십시오.

단일 호스트에 연결된 활성화된 모든 액세스 포트에 대해 STP PortFast를 on으로 설정합니다.예:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

케이블의 물리적 구성을 모니터링하려면 파이버 연결 인프라 포트 또는 구리 이더넷 케이블에서만 UDLD를 활성화합니다.UDLD를 활성화하려면 다음 명령을 실행합니다.

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

VLAN 컨피그레이션 정보

다음 명령으로 VLAN을 구성합니다.

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

각 VLAN에 대해 명령을 반복한 다음 종료합니다.다음 명령을 실행합니다.

```
Cat6500(config)#exit
```

모든 VLAN을 확인하려면 다음 명령을 실행합니다.

```
Cat6500#show vlan
```

라우팅된 SVI

interVLAN 라우팅에 대한 SVI를 구성합니다.다음 명령을 실행합니다.

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

라우티드 SVI가 포함된 각 인터페이스 함수에 대해 이 명령을 반복한 다음 종료합니다.다음 명령을 실행합니다.

```
Cat6500(config-if)#^Z
```

라우팅된 단일 물리적 인터페이스

기본 라우팅 레이어 3 인터페이스를 구성하려면 다음 명령을 실행합니다.

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

라우티드 물리적 인터페이스가 포함된 각 인터페이스 함수에 대해 이 명령을 반복한 다음 종료합니다.다음 명령을 실행합니다.

```
Cat6500(config-if)#^Z
```

라우티드 EtherChannel(L3)

레이어 3 인터페이스에서 EtherChannel을 구성하려면 이 섹션의 명령을 실행합니다.

다음과 같이 논리적 포트 채널 인터페이스를 구성합니다.

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

특정 채널을 형성하는 포트에 대해 이 섹션의 단계를 수행합니다.다음 예에서는 다음과 같이 나머지 정보를 포트 채널에 적용합니다.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

참고: EtherChannel을 구성한 후 포트 채널 인터페이스에 적용되는 컨피그레이션은 EtherChannel에 영향을 미칩니다.LAN 포트에 적용하는 컨피그레이션은 컨피그레이션을 적용하는 LAN 포트에만 영향을 줍니다.

Trunking을 지원하는 EtherChannel(L2)

다음과 같이 트렁킹을 위해 레이어 2 EtherChannel을 구성합니다.

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

특정 채널을 형성하는 포트에 대해서만 이 섹션의 단계를 수행합니다.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

참고: EtherChannel을 구성한 후 포트 채널 인터페이스에 적용되는 컨피그레이션은 EtherChannel에 영향을 미칩니다.LAN 포트에 적용하는 컨피그레이션은 컨피그레이션을 적용하는 LAN 포트에만 영향을 줍니다.

모든 EtherChannel 및 트렁크의 생성을 확인합니다.예:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

액세스 포트

인터페이스 기능이 단일 인터페이스로 구성된 액세스 포트인 경우 다음 명령을 실행합니다.

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

레이어 2 스위치 포트로 구성해야 하는 각 인터페이스에 대해 이 명령을 반복합니다.

스위치 포트를 엔드 스테이션에 연결하려면 다음 명령을 실행합니다.

```
Cat6500(config-if)#spanning-tree portfast
```

트렁크 포트(단일 물리적 인터페이스)

인터페이스 기능이 단일 인터페이스로 구성된 트렁크 포트인 경우 다음 명령을 실행합니다.

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

트렁크 포트로 구성해야 하는 각 인터페이스 기능에 대해 이 명령을 반복합니다.

비밀번호 정보

비밀번호 정보에 대해 다음 명령을 실행합니다.

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

구성 저장

컨피그레이션을 저장하려면 다음 명령을 실행합니다.

```
Cat6500#copy running-config startup-config
```

Cisco IOS Software 릴리스 12.1(13)E의 새로운 소프트웨어 기능

IP 전화 지원에 대한 자세한 내용은 Cisco IP Phone 지원 구성을 참조하십시오.

LAN 포트의 NBAR(Network-Based Application Recognition)에 대한 자세한 내용은 네트워크 기반

애플리케이션 인식 및 분산 네트워크 기반 애플리케이션 인식을 참조하십시오.

참고:

- LAN 포트용 NBAR는 MSFC2의 소프트웨어에서 지원됩니다.
- PFC2는 NBAR를 구성하는 LAN 포트의 입력 ACL에 대한 하드웨어 지원을 제공합니다.
- PFC QoS가 활성화되면 NBAR를 구성하는 LAN 포트를 통한 트래픽이 인그레스 및 이그레스 대기열을 통과하고 임계값을 삭제합니다.
- PFC QoS가 활성화된 경우 MSFC2는 이그레스 IP 우선 순위와 같은 CoS(egress class of service)를 설정합니다.
- 트래픽이 인그레스 대기열을 통과하면 NBAR를 구성하는 LAN 포트의 MSFC2의 소프트웨어에서 모든 트래픽이 처리됩니다.
- Distributed NBAR는 Cisco IOS Software 릴리스 12.1(6)E 이상과 함께 FlexWAN 인터페이스에서 사용할 수 있습니다.

NetFlow Data Export(NDE) 개선에는 다음이 포함됩니다.

- 대상 소스 인터페이스 및 전체 인터페이스 플로우 마스크
- PFC2의 NDE 버전 5
- 샘플링된 NetFlow
- NDE 레코드의 이러한 추가 필드를 채우는 옵션:다음 hop 라우터의 IP 주소인그레스 인터페이스 SNMP ifIndex이그레스 인터페이스 SNMP ifIndex소스 자동 시스템 번호

이러한 개선 사항에 대한 자세한 내용은 NDE 구성을 참조하십시오.

기타 기능 개선 사항은 다음과 같습니다.

- UDLD 구성
- VTP 구성
- WCCP를 사용하여 웹 캐시 서비스 구성

다음 명령은 새로운 명령입니다.

- **대기 지연 최소 다시 로드**
- **디바운스 연결**
- **vlan 내부 할당 정책 {오름차순 | 내림차순}**
- **시스템 점보투**
- **clear catalyst6000 트래픽 미터**

이 명령은 향상된 명령입니다.

- **show vlan internal usage**—이 명령은 WAN 인터페이스에서 사용하는 VLAN을 포함하도록 향상되었습니다.
- **show vlan id**—이 명령은 VLAN 범위의 항목을 지원하도록 향상되었습니다.
- **show l2protocol-tunnel** - 이 명령은 VLAN ID 항목을 지원하도록 향상되었습니다.

Cisco IOS Software 릴리스 12.1(13)E는 이전에 Cisco IOS Software 릴리스 12.1 EX 릴리스에서 지원되었던 이러한 소프트웨어 기능을 지원합니다.

- 서로 다른 DFC 기반 스위칭 모듈의 인터페이스를 포함하는 레이어 2 EtherChannel 구성Cisco 버그 ID CSCdt27074의 릴리스 12.1(13)E의 해결된 일반 주의 섹션 (등록된 고객만 해당)을 참조하십시오.
- RPR+(Route Processor Redundancy Plus) 이중화RPR 또는 RPR+ Supervisor Engine 이중화

구성을 참조하십시오.**참고:** Cisco IOS Software 릴리스 12.1(13)E 이상에서는 RPR 및 RPR+ 이중화 기능이 향상된 EHSA(High System Availability) 이중화를 대체합니다.
- 4,096개의 레이어 2 VLANVLAN 구성을 참조하십시오.**참고:** Cisco IOS Software 릴리스 12.1(13)E 이상 릴리스는 4,096 Layer 3 VLAN 인터페이스의 컨피그레이션을 지원합니다.수퍼바이저 엔진 II 또는 수퍼바이저 엔진 I를 사용하여 MSFC2에서 총 2,000개 이하의 레이어 3 VLAN 인터페이스와 레이어 3 포트를 구성합니다. MSFC에서 총 1,000개 이하의 레이어 3 VLAN 인터페이스와 레이어 3 포트를 구성합니다.
- IEEE 802.1Q 터널링IEEE 802.1Q 터널링 및 레이어 2 프로토콜 터널링 구성을 참조하십시오.
- IEEE 802.1Q 프로토콜 터널링IEEE 802.1Q 터널링 및 레이어 2 프로토콜 터널링 구성을 참조하십시오.
- IEEE 802.1s MST(Multiple Spanning Tree)STP 및 IEEE 802.1s MST 구성을 참조하십시오.
- IEEE 802.1w RSTP(Rapid STP)STP 및 IEEE 802.1s MST 구성을 참조하십시오.
- IEEE 802.3ad LACP레이어 3 및 레이어 2 EtherChannel 구성을 참조하십시오.
- PortFast BPDU 필터링STP 기능 구성을 참조하십시오.
- VACL(VLAN ACL)을 지원하는 레이어 3 VLAN 인터페이스 자동 생성네트워크 보안 구성을 참조하십시오.
- 모든 VLAN에서 임의의 레이어 2 이더넷 포트가 될 수 있는 VACL 캡처 포트네트워크 보안 구성을 참조하십시오.
- 개별 물리적 레이어 3 포트에서 구성 가능한 MTU 크기인터페이스 컨피그레이션 개요를 참조하십시오.
- 모든 SPAN 트래픽이 태그되도록 트렁크로 SPAN 대상 포트 구성로컬 및 원격 SPAN 구성을 참조하십시오.

관련 정보

- **툴 및 리소스 - Cisco Systems**
- **스위치 제품 지원**
- **LAN 스위칭 기술 지원**
- **기술 지원 및 문서 – Cisco Systems**