STP 문제 및 관련 설계 고려 사항 트러블슈팅

목차

관리 VLAN에서 트래픽을 차단하고 전체 네트워크에 걸쳐 단일 VLAN을 보유하지 않음
관련 정보

소개

이 문서에서는 Catalyst OS/Cisco IOS® Software를 실행하는 Cisco Catalyst 스위치 브리징에 대한 안전한 네트워크 구현 권장 사항에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 STP(Spanning Tree Protocol)가 실패할 수 있는 몇 가지 일반적인 이유와 문제의 원인을 식별하기 위해 찾아볼 수 있는 정보에 대해 설명합니다. 또한 스패닝 트리 관련 문제를 최소화하고 쉽게 문제를 해결할 수 있는 설계 유형을 보여줍니다.

이 문서에서는 STP의 기본 작업에 대해서는 다루지 않습니다. STP의 작동 방식을 알아보려면 다음 문서를 참조하십시오.

- Catalyst 스위치에서 STP(Spanning Tree Protocol) 이해 및 구성

이 문서에서는 IEEE 802.1w에 정의된 RSTP(Rapid STP)에 대해서는 다루지 않습니다. 또한 이 문서에서는 IEEE 802.1s에 정의된 MST(Multiple Spanning Tree) 프로토콜에 대해서는 다루지 않습니다. RSTP 및 MST에 대한 자세한 내용은 다음 문서를 참조하십시오.

- 다중 스패닝 트리 프로토콜 이해(802.1s)
- 빠른 스패닝 트리 프로토콜의 이해(802.1w)

Cisco IOS Software를 실행하는 Catalyst 스위치에 대한 자세한 STP 문제 해결 문서는 Cisco Integrated IOS(Native Mode)를 실행하는 Catalyst 스위치에서 STP 문제 해결 문서를 참조하십시오.

스패닝 트리 프로토콜 오류

STA(Spanning-Tree Algorithm)의 주요 기능은 브리지 네트워크에서 중복 링크가 생성하는 루프를 잘라내는 것입니다. STP는 OSI(Open System Interconnection) 모델의 레이어 2에서 작동합니다. STP는 브리지 간에 교환하는 BPDU(bridge protocol data unit)를 통해 트래픽을 전달하거나 차단하는 포트를 선택합니다. 이 프로토콜은 특정 경우에 실패 할 수 있으며, 네트워크 설계에 따라 결과가

매우 어려울 수 있는 상황을 해결 합니다. 이 특정 영역에서는 문제가 발생하기 전에 문제 해결 프로세스에서 가장 중요한 부분을 수행합니다.

STA에서의 장애는 일반적으로 브리징 루프(bridging loop)를 초래한다. 스패닝 트리 문제로 Cisco Technical Support에 문의하는 대부분의 고객은 버그를 의심하지만, 버그가 원인인 경우는 거의 없습니다. 소프트웨어에 문제가 있더라도 STP 환경의 브리징 루프는 여전히 트래픽을 차단할 수 있는 포트에서 나오지만 대신 트래픽을 전달합니다.

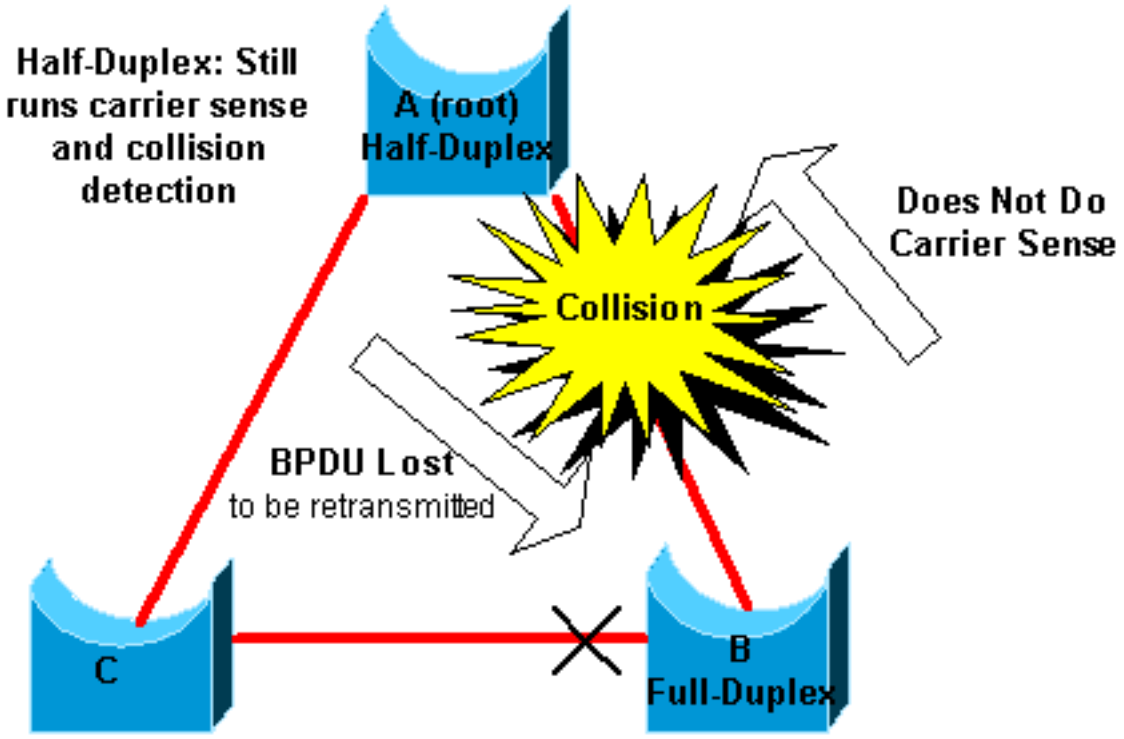
스패닝 트리 컨버전스

스패닝 트리가 처음에 수렴하는 방식을 설명하는 예를 보려면 스패닝 트리 비디오를 참조하십시오. 또한 이 예에서는 BPDU가 너무 많이 손실되어 STA 오류가 발생하여 차단된 포트가 전달 모드로 전환되는 이유를 설명합니다.

이 문서의 나머지 부분은 STA가 실패하게 할 수 있는 다양한 상황을 열거한다. 이러한 장애의 대부분은 BPDU의 대규모 손실과 관련이 있습니다. 이러한 손실로 인해 차단된 포트가 전달 모드로 전환됩니다.

듀플렉스 불일치

포인트-투-포인트 링크에서 듀플렉스 불일치는 매우 일반적인 컨피그레이션 오류입니다. 링크의 한 쪽에서 듀플렉스 모드를 수동으로 Full(전체)로 설정하고 다른 쪽은 자동 협상 모드로 두면 링크가 반이중으로 끝납니다. (이중 모드가 Full로 설정된 포트는 더 이상 협상하지 않습니다.)



최악의 시나리오는 BPDU를 전송하는 브리지의 경우 포트에서 듀플렉스 모드가 반이중으로 설정되지만 링크의 다른 끝에 있는 피어 포트의 경우 듀플렉스 모드가 전이중으로 설정된 경우입니다. 이전 예에서, 브리지 A와 B 사이의 링크 상의 듀플렉스 불일치는 브리징 루프로 쉽게 이어질 수 있다. 브리지 B는 전이중화를 위한 컨피그레이션을 가지고 있으므로 링크 액세스 전에 캐리어 감지를 수행하지 않습니다. 브리지 A가 링크를 이미 사용하고 있는 경우에도 브리지 B에서 프레임을 보내기 시작합니다. 이 상황은 A에 대한 문제입니다. 브리지 A는 충돌을 감지하고 브리지가 프레임의 다른 전송을 시도하기 전에 백오프 알고리즘을 실행합니다. B에서 A로의 트래픽이 충분할 경우, BPDU를 포함한 A가 전송하는 모든 패킷은 지연 또는 충돌을 겪으며 결국 삭제됩니다. STP 관점에

서, 브리지 B는 더 이상 A로부터 BPDU를 수신하지 않으므로, 브리지 B는 루트 브리지를 손실했습니다. 그러면 B가 브리지 C에 연결된 포트의 차단을 해제하여 루프가 생성됩니다.

이중 불일치가 발생할 때마다 CatOS 및 Cisco IOS 소프트웨어를 실행하는 Catalyst 스위치의 스위치 콘솔에 다음과 같은 오류 메시지가 표시됩니다.

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS Software

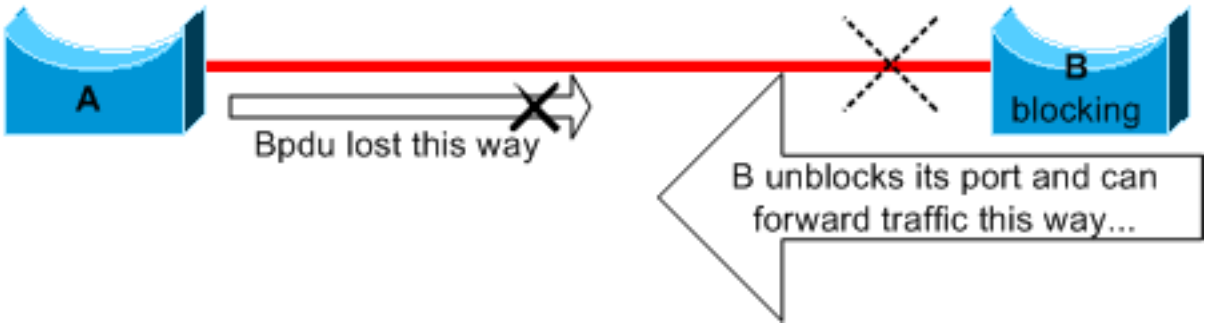
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

듀플렉스 설정을 확인하고 듀플렉스 컨피그레이션이 일치하지 않는 경우 컨피그레이션을 적절하게 설정합니다.

듀플렉스 불일치 문제를 해결하는 방법에 대한 자세한 내용은 이더넷 10/100/1000Mb 하프/풀 듀플렉스 자동 협상 구성 및 문제 해결 문서를 참조하십시오.

단방향 링크

단방향 링크는 브리징 루프의 일반적인 원인입니다. 파이버 링크에서 감지 없이 오류가 발생하면 종종 단방향 링크가 발생합니다. 또 다른 원인은 트렌시버에 문제가 있습니다. 링크가 끊임 없이 유지되고 단방향 통신을 제공할 수 있는 모든 것은 STP와 관련하여 매우 위험합니다. 이 예에서는 다음을 설명합니다.



여기서 A와 B의 연결이 단방향이라고 가정하자. 링크는 A에서 B로 트래픽을 전송하는 동안 A에서 B로 트래픽을 삭제합니다. 링크가 단방향이 되기 전에 브리지 B가 차단되었다고 가정합니다. 그러나 포트는 우선순위가 더 높은 브리지에서 BPDU를 수신하는 경우에만 차단할 수 있습니다. 이 경우 A에서 오는 모든 BPDU가 손실되므로 브리지 B는 결국 A로 향하는 포트를 포워딩 상태로 전환하고 트래픽을 전달합니다. 이렇게 하면 루프가 생성됩니다. 시작할 때 이 오류가 발생하면 STP가 올바르게 통합되지 않습니다. 이중 불일치의 경우 재부팅하면 일시적으로 도움이 되지만, 이 경우 브리지의 재부팅은 전혀 영향을 주지 않습니다.

포워딩 루프를 생성하기 전에 단방향 링크를 탐지하기 위해 Cisco는 UDLD(UniDirectional Link Detection) 프로토콜을 설계하고 구현했습니다. 이 기능은 레이어 2에서 부적절한 케이블링 또는 단방향 링크를 감지하고 일부 포트를 비활성화하여 결과 루프를 자동으로 끊을 수 있습니다. 브리지 환경에서 가능한 경우 UDLD를 실행합니다.

UDLD 사용에 대한 자세한 내용은 Understanding and Configuring the Unidirectional Link Detection Protocol Feature 문서를 참조하십시오.

패킷 손상

패킷 손상으로 인해 같은 종류의 오류가 발생할 수도 있습니다. 링크에 높은 물리적 오류 비율이 있는 경우 특정 수의 연속 BPDU가 손실될 수 있습니다. 이러한 손실로 인해 차단 포트가 전달 상태로 전환될 수 있습니다. STP 기본 매개변수는 매우 보수적이므로 이 경우가 자주 표시되지 않습니다. 차단 포트는 전달로 전환하기 전에 50초 동안 BPDU를 누락해야 합니다. 단일 BPDU의 성공적인 전송은 루프를 끊습니다. 이 경우는 STP 매개변수를 부주의하게 조정하는 경우에 흔히 발생합니다. 조정의 예로는 최대 연령 감소가 있습니다.

듀플렉스 불일치, 잘못된 케이블 또는 잘못된 케이블 길이로 인해 패킷이 손상될 수 있습니다. CatOS 및 Cisco IOS Software 오류 카운터 출력에 대한 설명은 스위치 포트 및 인터페이스 문제 해결 문서를 참조하십시오.

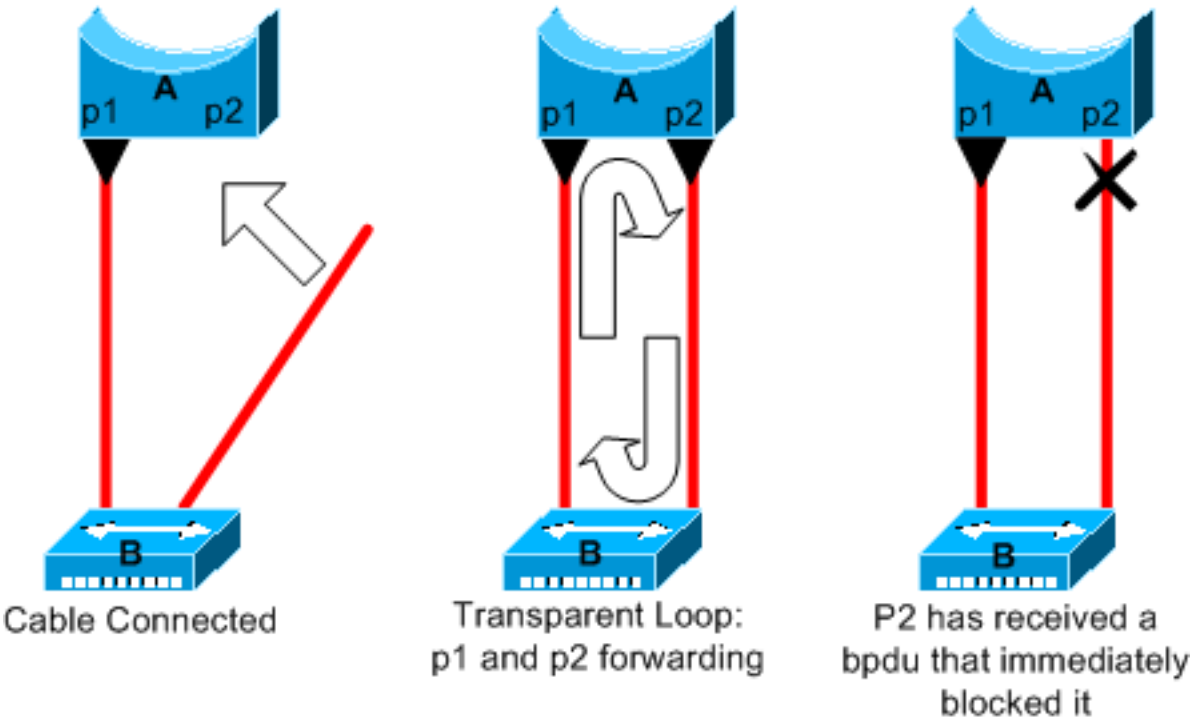
리소스 오류

STP는 특화된 ASIC(Application-Specific Integrated Circuits)로 대부분의 스위칭 기능을 하드웨어에서 수행하는 고급 스위치에서도 소프트웨어로 구현됩니다. 어떤 이유로든 브리지의 CPU 사용률이 초과될 경우 BPDU 전송에 리소스가 부족할 수 있습니다. STA는 일반적으로 프로세서 집약적이지 않으며 다른 프로세스들에 비해 우선순위를 갖는다. 이 문서의 리소스 오류 찾기 섹션에서는 특정 플랫폼에서 처리할 수 있는 STP 인스턴스 수에 대한 몇 가지 지침을 제공합니다.

PortFast 구성 오류

PortFast는 일반적으로 호스트에 연결되는 포트 또는 인터페이스에 대해서만 활성화하는 기능입니다. 링크가 이 포트에 도달하면 브리지는 STA의 첫 번째 스테이지를 건너뛰고 직접 전달 모드로 전환합니다.

> **주의**: 다른 스위치, 허브 또는 라우터에 연결되는 스위치 포트 또는 인터페이스에는 PortFast 기능을 사용하지 마십시오. 그렇지 않으면 네트워크 루프를 생성할 수 있습니다.



이 예에서 디바이스 A는 포트 p1이 이미 포워딩되어 있는 브리지입니다. 포트 p2에는 PortFast 컨피그레이션이 있습니다. 디바이스 B는 허브입니다. 두 번째 케이블을 A에 연결하는 즉시 포트 p2가 전달 모드로 전환되고 p1과 p2 사이에 루프가 생성됩니다. 이 루프는 p1 또는 p2가 이 두 포트 중 하나를 차단 모드로 설정하는 BPDU를 수신하는 즉시 중단됩니다. 그러나 이러한 일시적인 루프에는 문제가 있습니다. 루프 트래픽이 매우 많은 경우 브리지는 루프를 중지하는 BPDU를 성공적으로 전송하는 데 문제가 있을 수 있습니다. 이러한 문제로 인해 통합이 상당히 지연되거나 극단적인 경우 네트워크가 중단될 수 있습니다.

CatOS 및 Cisco IOS 소프트웨어를 실행하는 스위치에서 PortFast를 올바르게 사용하는 방법에 대한 자세한 내용은 PortFast 및 기타 명령을 사용하여 워크스테이션 시작 연결 지연을 수정하는 문서를 참조하십시오.

PortFast 컨피그레이션에서도 포트 또는 인터페이스는 STP에 계속 참여합니다. 현재 활성 루트 브리지보다 낮은 브리지 우선 순위를 가진 스위치가 PortFast로 구성된 포트 또는 인터페이스에 연결되는 경우 루트 브리지로 선택할 수 있습니다. 이러한 루트 브리지 변경은 활성 STP 토폴로지에 악영향을 줄 수 있으며 네트워크를 최적화하지 못할 수 있습니다. 이러한 상황을 방지하기 위해 CatOS 및 Cisco IOS Software를 실행하는 대부분의 Catalyst 스위치에는 BPDU Guard라는 이름의 기능이 있습니다. BPDU 가드는 포트 또는 인터페이스에서 BPDU를 수신하는 경우 PortFast 구성 포트 또는 인터페이스를 비활성화합니다.

CatOS 및 Cisco IOS 소프트웨어를 실행하는 스위치에서 BPDU 가드 기능을 사용하는 방법에 대한 자세한 내용은 Spanning Tree Portfast BPDU Guard Enhancement 문서를 참조하십시오.

어색한 STP 매개변수 조정 및 지름 문제

max-age 파라미터 및 전달 지연에 대한 적극적인 값은 매우 불안정한 STP 토폴로지를 초래할 수 있다. 그러한 경우, 일부 BPDU의 손실로 인해 루프가 나타날 수 있다. 잘 알려지지 않은 또 다른 이슈는 브리지 네트워크의 직경과 관련이 있다. STP 타이머의 보존적 기본값은 최대 네트워크 지름을 7로 지정합니다. 이 최대 네트워크 직경은 네트워크의 서로 브리지에서 얼마나 멀리 떨어져 있을 수 있는지를 제한합니다. 이 경우 두 개의 서로 다른 브리지는 서로 7홉 이상 떨어져 있을 수 없습니다. 이러한 제한의 일부는 BPDU가 전달하는 기간 필드에서 비롯됩니다.

BPDU가 루트 브리지에서 트리의 나뭇잎을 향해 전파되면 BPDU가 브리지를 통과할 때마다 에이

지 필드가 증가합니다. 결국, 기간 필드가 최대 기간을 초과할 경우 브리지는 BPDU를 폐기합니다. 루트가 네트워크의 일부 브리지에서 너무 멀리 떨어져 있으면 이 문제가 발생할 수 있습니다. 이 문제는 스패닝 트리의 컨버전스에 영향을 미칩니다.

STP 타이머를 기본값에서 변경할 계획인 경우 각별히 주의하십시오. 이런 식으로 더 빠른 재통합을 시도하면 위험이 있다. STP 타이머 변경은 네트워크의 직경과 STP의 안정성에 영향을 미칩니다. 브리지 우선순위를 변경하여 루트 브리지를 선택하고 포트 비용 또는 우선순위 매개변수를 변경하여 이중화 및 로드 밸런싱을 제어할 수 있습니다.

Cisco Catalyst 소프트웨어는 가장 중요한 STP 매개변수를 세부적으로 조정하는 매크로를 제공합니다.

- 이 **set spantree root [secondary]** macro 명령은 브리지 우선순위를 낮춰 루트(또는 대체 루트)가 됩니다. 이 명령에 사용할 수 있는 추가 옵션은 네트워크의 지름을 지정하여 STP 타이머를 조정하는 것입니다. 타이머 튜닝이 올바르게 수행되더라도 통합 시간이 크게 개선되지 않으며 네트워크에 몇 가지 불안정한 위험이 발생합니다. 또한, 이러한 종류의 조정은 디바이스가 네트워크에 추가될 때마다 업데이트되어야 합니다. 네트워크 엔지니어에게 친숙한 보존적 기본값을 유지합니다.
- 이 **set spantree uplinkfast** CatOS 또는 **spanning-tree uplinkfast** cisco IOS Software에 대한 명령은 스위치 우선 순위를 높이므로 스위치가 루트가 될 수 없습니다. 이 명령은 업링크 오류가 발생할 경우 STP 통합 시간을 늘립니다. 일부 코어 스위치에 대한 이중 연결이 있는 분산 스위치에서 이 명령을 사용합니다. Cisco UplinkFast 기능 이해 및 구성 문서를 참조하십시오.
- 이 **set spantree backbonefast enable** CatOS 또는 **spanning-tree backbonefast** cisco IOS Software에 대한 명령을 사용하면 간접 링크 장애 시 스위치의 STP 컨버전스 시간을 늘릴 수 있습니다. BackboneFast는 Cisco의 독점 기능입니다. Catalyst 스위치의 백본 Fast 이해 및 구성 문서를 참조하십시오.

STP 타이머 및 이를 튜닝하는 규칙에 대한 자세한 내용은 스패닝 트리 프로토콜 타이머 이해 및 튜닝 문서를 참조하십시오.

소프트웨어 오류

서론에서 언급했듯이 STP는 Cisco 제품에 구현된 최초의 기능 중 하나입니다. 이 기능은 매우 안정적입니다. EtherChannel과 같은 최신 기능과의 상호작용만 수행하므로 이제 해결된 매우 특수한 경우 STP가 실패합니다. 여러 가지 서로 다른 요인들이 소프트웨어 버그를 일으킬 수 있고 여러 가지 서로 다른 영향을 미칠 수 있다. 버그로 인해 발생할 수 있는 문제를 적절하게 설명할 수 있는 방법은 없습니다. 소프트웨어 오류로 인해 발생하는 가장 위험한 상황은 일부 BPDU를 무시하거나 포워딩으로 포트 전환이 차단된 경우입니다.

장애 트러블슈팅

안타깝게도 STP 문제를 해결할 수 있는 체계적인 절차는 없습니다. 그러나 이 섹션에는 사용 가능한 몇 가지 작업이 요약되어 있습니다. 이 절의 대부분의 단계는 일반적으로 브리징 루프의 트러블슈팅에 적용됩니다. 더 일반적인 접근 방식을 사용하여 연결 손실로 이어지는 STP의 다른 장애를 식별할 수 있습니다. 예를 들어, 문제를 경험하는 트래픽에 걸리는 경로를 탐색할 수 있습니다.

> **참고**: 트러블슈팅을 위한 대부분의 단계는 브리지 네트워크의 서로 다른 디바이스에 대한 연결을 가정합니다. 이 연결은 콘솔 액세스 권한을 보유함을 의미합니다. 예를 들어 브리징 루프 중에는 텔넷 연결을 설정할 수 없습니다.

의 출력이 있는 경우 **show-tech support** 명령을 Cisco 디바이스에서 Cisco CLI Analyzer(등록된 고객만)를 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다.

네트워크 다이어그램 사용

브리징 루프를 트러블슈팅하기 전에 최소한 다음 항목을 알고 있어야 합니다.

- 브리지 네트워크의 토폴로지
- 루트 브리지의 위치
- 차단된 포트 및 이중화 링크의 위치

이러한 지식은 최소한 다음 두 가지 이유에서 필수적입니다.

- 네트워크에서 수정할 사항을 알기 위해서는 네트워크가 올바르게 작동할 때 네트워크가 어떻게 보이는지 알아야 합니다.
- 문제 해결을 위한 대부분의 단계는 **show** 명령을 사용하여 오류 상태를 확인합니다. 네트워크에 대한 지식을 바탕으로 주요 장치의 중요 포트에 집중할 수 있습니다.

브리징 루프 식별

방송 폭풍이 네트워크에 끔찍한 영향을 미칠 수 있다는 것이 예전에는 그랬다. 오늘날 하드웨어 수준에서 스위칭을 제공하는 고속 링크 및 디바이스에서 단일 호스트(예: 서버)가 브로드캐스트를 통해 네트워크를 중단시킬 가능성은 거의 없습니다. 브리징 루프를 식별하는 가장 좋은 방법은 포화된 링크에서 트래픽을 캡처하고 유사한 패킷이 여러 번 나타나는지 확인하는 것입니다. 그러나 현실적으로 특정 브리지 도메인의 모든 사용자에게 동시에 연결 문제가 발생하는 경우 브리징 루프를 의심할 수 있습니다.

디바이스의 포트 사용률을 확인하고 비정상적인 값을 찾습니다. 이 문서의 포트 사용률 확인 섹션을 참조하십시오.

CatOS를 실행하는 Catalyst 스위치에서 **show system** 명령을 실행합니다. 이 명령은 스위치 백플레인의 현재 사용량을 제공하고 피크 사용량 및 피크 사용 날짜도 지정합니다. 이례적인 최대 사용률은 이 디바이스에 브리징 루프가 있었는지 여부를 보여줍니다.

연결을 신속하게 복원하고 다음에 대한 준비를 하십시오.

루프를 중단하려면 포트 비활성화

브리징 루프는 브리지 네트워크에 매우 심각한 결과를 초래합니다. 일반적으로 관리자는 루프 원인을 찾을 시간이 없고 가능한 한 빨리 연결을 복원하는 것을 선호합니다. 이 경우 네트워크에서 이중화를 제공하는 모든 포트를 수동으로 비활성화하는 것이 쉬운 방법입니다. 가장 큰 영향을 받는 네트워크의 일부를 식별할 수 있는 경우 이 영역에서 포트 비활성화를 시작합니다. 또는 가능한 경우 처음에는 차단할 수 있는 포트를 비활성화합니다. 포트를 비활성화할 때마다 네트워크에서 연결을 복원했는지 확인합니다. 어떤 비활성화된 포트가 루프를 중지하는지 식별하여 이 포트가 있는 중복 경로도 식별합니다. 이 포트가 차단되고 있는 경우, 장애가 발생한 링크가 발견되었을 수 있습니다.

차단된 포트를 호스팅하는 디바이스에 STP 이벤트 기록

문제의 원인을 정확하게 식별할 수 없거나 문제가 일시적인 경우 장애를 겪는 네트워크의 브리지 및 스위치에서 STP 이벤트 로깅을 활성화합니다. 구성할 디바이스 수를 제한하려면, 최소한 차단된 포트를 호스팅하는 디바이스에서 이 로깅을 활성화하십시오. 차단된 포트의 전환은 루프를 생성합

니다.

- Cisco IOS Software - exec 명령 실행 **debug spanning-tree events** - STP 디버그 정보를 활성화합니다. general config mode 명령을 실행합니다 **logging buffered** 디바이스 버퍼에서 이 디버그 정보를 캡처합니다.
- CatOS - 더 **set logging level spantree 7 default** 이 명령은 STP와 관련된 이벤트의 기본 수준을 디버그 수준으로 높입니다. 스위치 버퍼에서 를 사용하여 최대 메시지 수를 기록해야 합니다. **set logging buffer 500** 명령을 실행합니다.

디버그 출력을 syslog 디바이스로 전송하려고 시도할 수도 있습니다. 브리징 루프가 발생할 경우 syslog 서버에 대한 연결을 유지하는 경우는 거의 없습니다.

포트 확인

먼저 조사해야 할 중요 포트는 차단 포트입니다. 이 섹션에서는 다른 포트에서 찾을 내용 목록을 제공하고, CatOS 및 Cisco IOS 소프트웨어를 실행하는 스위치에 대해 실행할 명령에 대한 빠른 설명을 제공합니다.

차단된 포트에서 BPDU를 수신하는지 확인

특히 차단된 포트 및 루트 포트에서 주기적으로 BPDU를 수신하는지 확인합니다. 몇 가지 문제로 인해 패킷 또는 BPDU를 수신하지 못하는 포트가 발생할 수 있습니다.

- Cisco IOS Software-In Cisco IOS Software 릴리스 12.0 이상, **show spanning-tree bridge-group #** 명령에는 BPDU 있습니다. 이 필드에는 각 인터페이스에 대해 수신된 BPDU 수가 표시됩니다. 디바이스에서 BPDU를 수신하는지 확인하기 위해 명령을 한 번 또는 두 번 더 실행합니다.의 출력에 BPDU 가 없는 경우 **show spanning-tree** 명령을 사용하여 STP 디버그를 **debug spanning-tree** 명령을 사용하여 BPDU 수신을 확인합니다.
- CatOS - 더 **show mac module/port** 명령은 특정 포트에서 수신하는 멀티캐스트 패킷의 수를 알려줍니다. 그러나 가장 간단한 명령은 **show spantree statistics module#/port# vlan#** 명령을 실행합니다. 이 명령은 특정 VLAN에서 특정 포트가 수신한 컨피그레이션 BPDU의 정확한 수를 표시합니다. 트렁킹의 경우 포트는 여러 VLAN에 속할 수 있습니다. 이 문서의 추가 CatOS 명령 섹션을 참조하십시오.

이중 불일치 확인

이중 불일치를 찾아보려면 포인트-투-포인트 링크의 각 측면을 확인해야 합니다.

- Cisco IOS Software-Issue **show interfaces [interface interface-number] status** 특정 포트의 속도 및 이중 상태를 확인하는 명령입니다.
- CatOS - 출력 첫 번째 행입니다. **show port module#/port#** 명령은 포트 컨피그레이션에 따라 속도와 양방향을 제공합니다.

포트 사용률 확인

트래픽 오버로드가 있는 인터페이스는 중요한 BPDU를 전송하지 못할 수 있습니다. 링크 오버로드는 브리징 루프가 있을 수도 있음을 나타냅니다.

- Cisco IOS Software-명령 사용 **show interfaces** - 인터페이스의 사용률을 확인합니다. 및 /과 같

은 여러 필드를 통해 이러한 결정을 . 에 대한 설명은 Troubleshooting Switch Port and Interface Problems 문서를 참조하십시오. **show interfaces** 명령 출력입니다.
- CatOS - 더 **show mac module#/port#** 명령은 포트가 수신하여 전송하는 패킷에 대한 통계를 표시합니다. 이 **show top** 이 명령은 30초 동안의 포트 사용률을 자동으로 평가하고 결과를 표시합니다. 이 명령은 결과 분류를 위한 다른 옵션을 사용할 수 있지만 대역폭 사용률에 따라 결과를 분류합니다. 또한 **show system** 명령이 특정 포트를 가리키지 않더라도 명령은 백플레인 사용률을 나타냅니다.

패킷 손상 확인

- Cisco IOS Software-Look for error increments in the `input errors` counter의 **show interfaces** 명령을 실행합니다. 오류 카운터에는 `runts, giants, no buffer, CRC, frame, overrun` 및 `ignored` 카운트가 .에 대한 설명은 Troubleshooting Switch Port and Interface Problems 문서를 참조하십시오. **show interfaces** command output.
- CatOS - 명령 **show port module#/port#** 에서는 Align-Err, FCS-Err, `Xmit-Err, Rcv-Err Undersize` 세부 정보를 . 이 **show counters module#/port#** 이 명령은 통계를 더 자세히 제공합니다.

추가 CatOS 명령

명령 **show spantree statistics module#/port# vlan#** 에서는 특정 포트에 대한 매우 정확한 정보를 제공합니다. 의심스러운 포트에 대해 이 명령을 실행하고 다음 필드에 특별히 주의하십시오.

- `Forward trans count` - 이 카운터는 포트가 학습에서 전달로 전환되는 횟수를 기억합니다. 안정적인 토폴로지에서 이 카운터는 항상 1을 표시합니다. 이 카운터는 포트가 작동 중지되고 올라감에 따라 0으로 재설정됩니다. 따라서 값이 1보다 크면 포트가 경험한 전환이 STP 재계산의 결과임을 나타냅니다. 이 전환은 직접 링크 장애로 인한 것이 아닙니다.
- `Max age expiry count`-이 카운터는 이 링크에서 최대 사용 기간이 만료된 횟수를 추적합니다. 기본적으로 BPDU를 예상하는 포트는 지정된 브리지가 손실된 것으로 간주하기 전에 최대 기간 동안 대기합니다. 최대 기간 기본값은 20초입니다. 이 이벤트가 발생할 때마다 카운터가 증가합니다. 값이 0이 아닌 경우 이 LAN에 지정된 브리지가 불안정하거나 BPDU 전송에 문제가 있음을 나타냅니다.

리소스 오류 검색

CPU 사용률이 높으면 STA를 실행하는 시스템에 위험할 수 있습니다. 이 방법을 사용하여 CPU 리소스가 디바이스에 적합한지 확인합니다.

- Cisco IOS Software - show processes **cpu 명령을** 실행합니다. CPU 사용률이 너무 높지 않은지 확인합니다. CatOS 또는 Cisco IOS 소프트웨어를 실행하는 Catalyst 4500/4000 Series 스위치의 경우 Catalyst 4500/4000, 2948G, 2980G 및 4912G 스위치의 CPU 사용률 문서를 참조하십시오.
- CatOS 발급 **show proc cpu** command to display CPU utilization information. Check that the CPU utilization is not too high.

수퍼바이저 엔진에서 처리할 수 있는 STP의 서로 다른 인스턴스 수에는 제한이 있습니다. 서로 다른 VLAN에 대한 STP의 모든 인스턴스에서 논리 포트의 총 수가 각 Supervisor Engine 유형 및 메모리 컨피그레이션에 대해 지원되는 최대 수를 초과하지 않는지 확인합니다.

명령 **show spantree summary** CatOS 또는 **show spanning-tree summary totals** 명령을 사용하여 Cisco IOS

Software를 실행합니다. 이 명령은 STP Active(STP 활성) 열에 VLAN당 논리적 포트 또는 표시합니다. 이 열의 아래쪽에 합계가 나타납니다. 총계는 서로 다른 VLAN에 대한 STP의 모든 인스턴스에서 모든 논리 포트의 합계를 나타냅니다. 이 수가 각 Supervisor Engine 유형에 지원되는 최대 수를 초과하지 않는지 확인합니다.

참고: 스위치의 논리 포트 합계를 계산하는 공식은 다음과 같습니다.

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Catalyst 스위치에 적용되는 STP의 제한 사항에 대한 요약은 다음 문서를 참조하십시오.

플랫폼	CatOS STP 제한	Cisco IOS Software STP 제한 사항
Catalyst 6500/6000 Supervisor Engine I 및 II	STP 문제 해결	
Catalyst 6500/6000 Supervisor Engine 720	STP 문제 해결	스패닝 트리 문제 해결
Catalyst 4500/4000	스패닝 트리	스패닝 트리 트러블슈팅
Catalyst 3750		STP 구성

불필요한 기능 사용 안 함

문제를 해결할 때 네트워크에서 현재 문제가 무엇인지 파악합니다. 가능한 한 많은 기능을 비활성화합니다. 비활성화는 네트워크 구조를 간소화하고 문제를 쉽게 식별할 수 있도록 도와줍니다. 예를 들어, EtherChanneling은 여러 개의 서로 다른 링크를 논리적으로 단일 링크로 번들링해야 하는 기능입니다. 문제 해결 프로세스 중에 이 기능을 비활성화하는 것은 타당합니다. 일반적으로 컨피그레이션을 최대한 단순하게 만들면 문제의 트러블슈팅 프로세스가 훨씬 쉬워집니다.

유용한 명령

Cisco IOS Software 명령

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

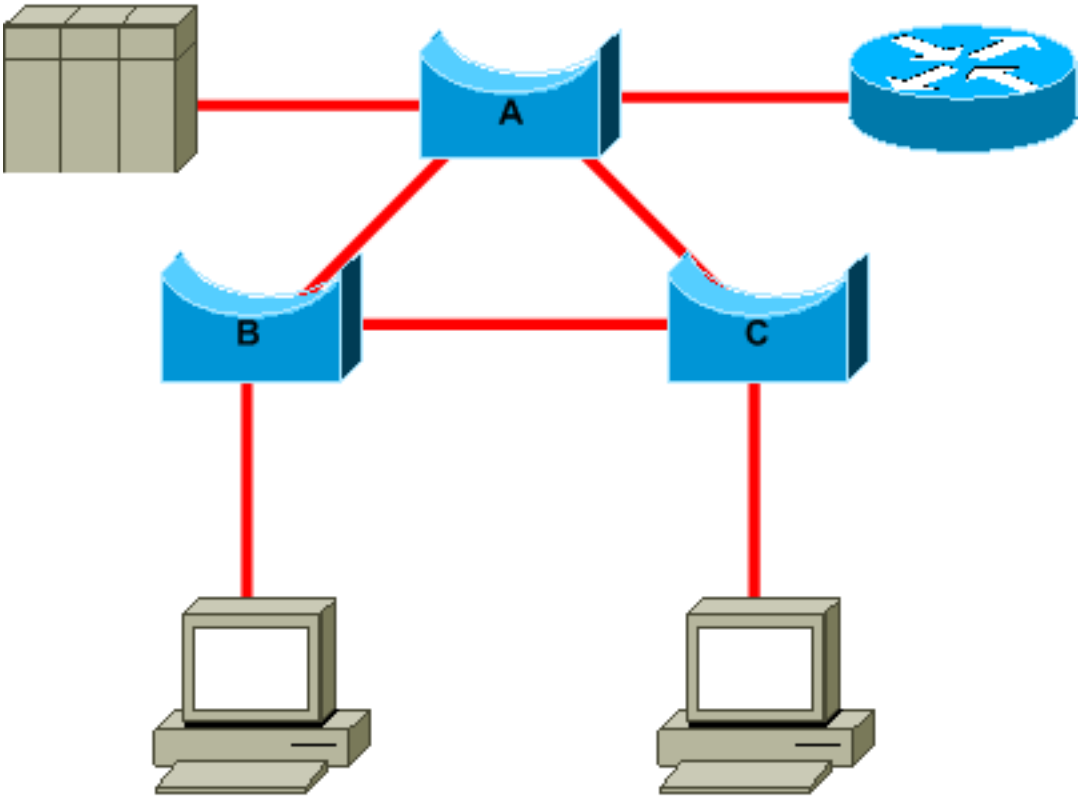
CatOS 명령

- **show port**
- **show mac**
- **show spantree**
- **show spantree statistics**
- **show spantree blockedports**
- **show spantree summary**
- **show top**
- **show proc cpu**
- **show system**
- **show counters**
- **set spantree root [secondary]**
- **set spantree uplinkfast**
- **set logging level**
- **set logging buffered**

문제 방지를 위한 설계 STP

루트가 어디에 있는지 파악

문제 해결 시 루트의 위치에 대한 정보를 사용할 수 없는 경우가 많습니다. 어떤 브리지가 루트인지 결정하려면 STP를 남겨두지 마십시오. 각 VLAN에 대해 일반적으로 어떤 스위치가 루트로 가장 적합한지 식별할 수 있습니다. 이는 네트워크의 설계에 따라 달라집니다. 일반적으로 네트워크 중간에 있는 강력한 브리지를 선택합니다. 루트 브리지를 서버 및 라우터에 직접 연결하여 네트워크의 중심에 배치할 경우 일반적으로 클라이언트에서 서버 및 라우터까지의 평균 거리를 줄일 수 있습니다.



이 다이어그램에는 다음이 나와 있습니다.

- 브리지 B가 루트이면 브리지 A 또는 브리지 C에서 링크 A와 C가 차단됩니다. 이 경우 스위치 B에 연결하는 호스트는 두 홉으로 서버와 라우터에 액세스할 수 있습니다. 브리지 C에 연결되는 호스트는 세 번의 홉으로 서버와 라우터에 액세스할 수 있습니다. 평균 거리는 2.5홉입니다.
- 브리지 A가 루트이면 B와 C에 연결하는 두 호스트 모두에 대해 라우터와 서버에 두 홉으로 연결할 수 있습니다. 이제 평균 거리는 두 홉입니다.

이 간단한 예제의 논리는 좀 더 복잡한 토폴로지로 넘어갑니다.

> **참고**: 각 VLAN에 대해 루트 브리지 및 백업 루트 브리지를 하드 코딩하여 STP 우선순위 매개변수 값을 줄입니다. 또는 set spantree root 매크로를 사용할 수 있습니다.

이중화가 어디에 있는지 파악

이중화 링크의 구성을 계획합니다. STP의 플러그 앤 플레이 기능은 잊으십시오. STP 비용 매개변수를 튜닝하여 어떤 포트가 차단되는지 결정합니다. 계층 구조 설계와 루트 브리지가 좋은 위치에 있는 경우 일반적으로 이 튜닝이 필요하지 않습니다.

참고: 각 VLAN에 대해 안정적인 네트워크에서 어떤 포트를 차단할 수 있는지 파악합니다. 차단된 포트가 루프를 끊는 네트워크의 각 물리적 루프를 명확하게 보여 주는 네트워크 다이어그램을 준비하십시오.

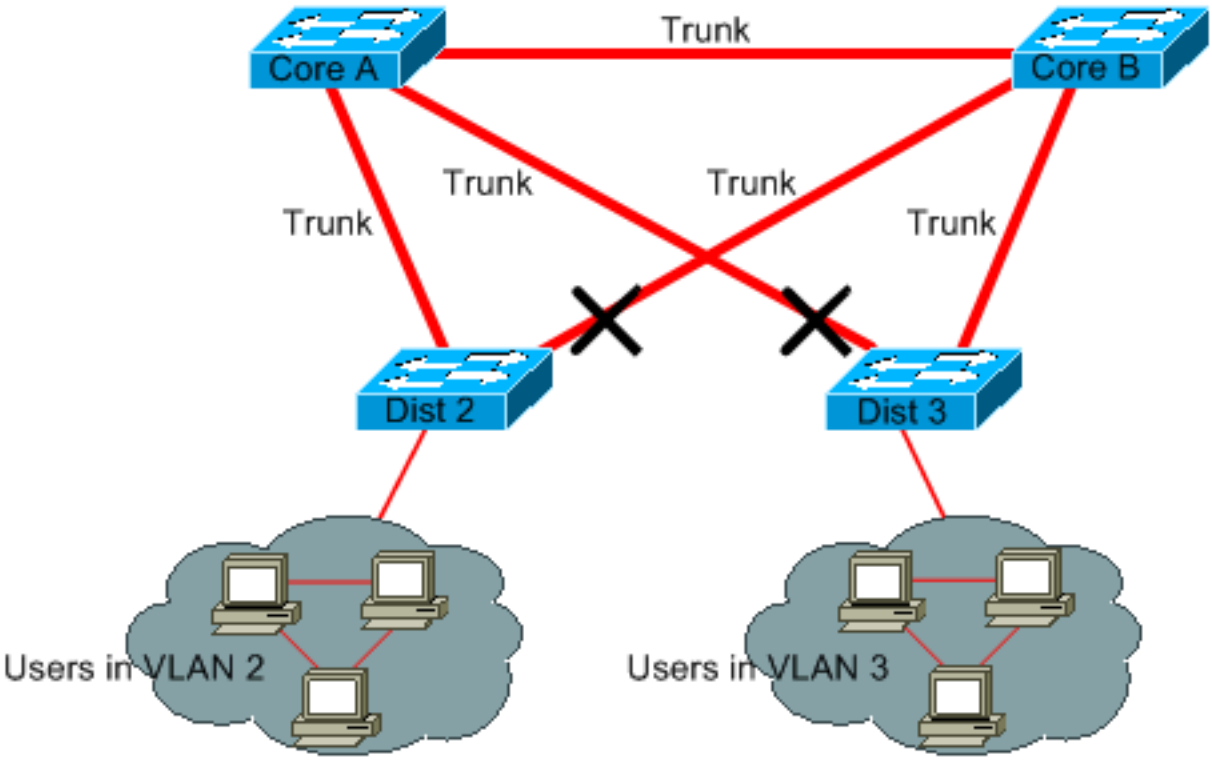
이중화 링크의 위치를 알고 있으면 우발적인 브리징 루프 및 원인을 파악할 수 있습니다. 또한 차단된 포트의 위치를 알면 오류 위치를 확인할 수 있습니다.

차단된 포트 수 최소화

STP가 수행하는 유일한 중요한 작업은 포트 차단입니다. 실수로 포워딩로 전환되는 단일 차단 포트가 네트워크의 상당 부분을 녹일 수 있습니다. STP 사용에 내재된 위험을 제한하는 좋은 방법은 차단된 포트의 수를 최대한 줄이는 것입니다.

사용하지 않는 VLAN 정리

브리지 네트워크의 두 노드 간에 둘 이상의 이중화 링크가 필요하지 않습니다. 그러나 이러한 컨피그레이션은 일반적입니다.



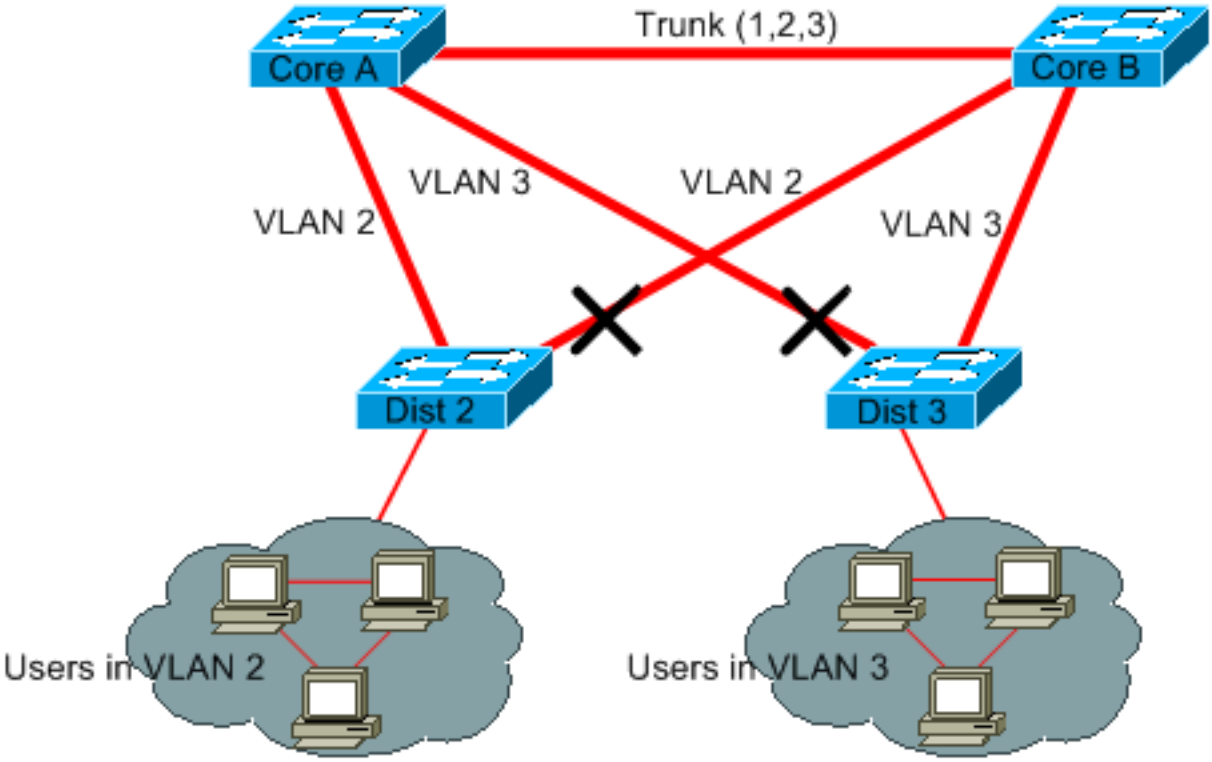
디스트리뷰션 스위치는 2개의 코어 스위치에 이중 연결됩니다. 디스트리뷰션 스위치에 연결하는 사용자는 네트워크에서 사용 가능한 VLAN의 하위 집합에만 있습니다. 이 예에서 Dist 2에 연결하는 사용자는 모두 VLAN 2에 있으며, Dist 3은 VLAN 3의 사용자만 연결합니다. 기본적으로 트렁크는 VTP(VLAN Trunk Protocol) 도메인에 정의된 모든 VLAN을 전송합니다. Dist 2만 VLAN 3에 대한 불필요한 브로드캐스트 및 멀티캐스트 트래픽을 수신하지만 VLAN 3에 대한 포트 중 하나를 차단하고 있습니다. 그 결과, 코어 A와 코어 B 간에 3개의 이중화 경로가 생성됩니다. 이러한 이중화로 인해 포트가 더 많이 차단되고 루프가 발생할 가능성이 높아집니다.

참고: 트렁크에서 필요하지 않은 VLAN은 정리합니다.

VTP 프루닝이 도움이 될 수 있지만, 이러한 플러그 앤 플레이 기능은 네트워크의 코어에서 필요하

지 않습니다.

이 예에서는 액세스 VLAN만 디스트리뷰션 스위치를 코어에 연결하는 데 사용됩니다.



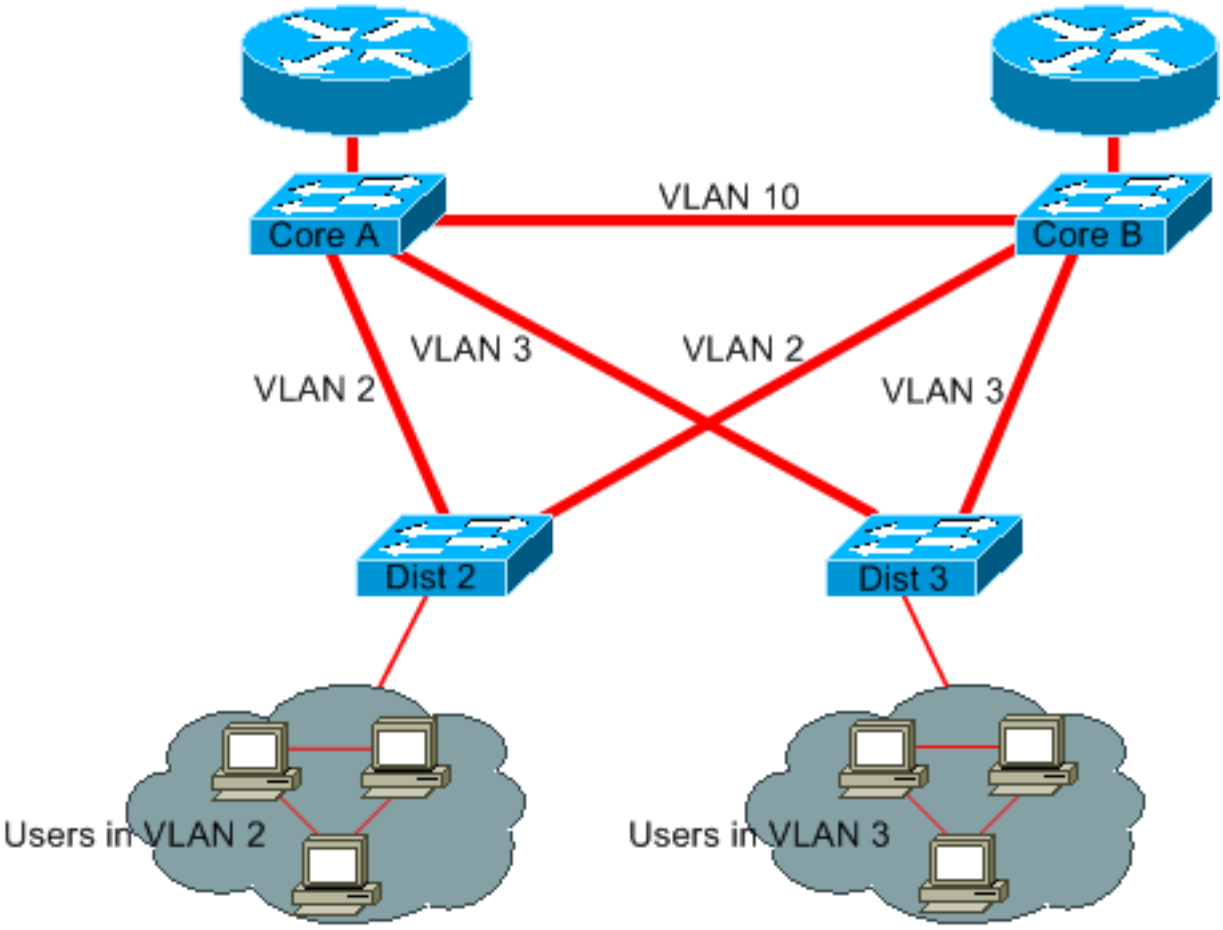
이 설계에서는 VLAN당 하나의 포트만 차단됩니다. 또한 이 설계에서는 Core A 또는 Core B를 종료하면 모든 이중 링크를 단 한 번에 제거할 수 있습니다.

레이어 3 스위칭 사용

레이어 3 스위칭은 대략 스위칭 속도로 라우팅하는 것을 의미합니다. 라우터는 두 가지 주요 기능을 수행합니다.

- 라우터는 전달 테이블을 구축합니다. 라우터는 일반적으로 라우팅 프로토콜을 통해 피어와 정보를 교환합니다.
- 라우터는 패킷을 수신하고 목적지 주소를 기반으로 올바른 인터페이스로 전달합니다.

하이엔드 Cisco 레이어 3 스위치는 이제 레이어 2 스위칭 기능과 동일한 속도로 이 두 번째 기능을 수행할 수 있습니다. 라우팅 홉을 도입하고 추가적인 네트워크 세그멘테이션을 생성하면 속도 제한이 없습니다. 이 다이어그램에서는 기본으로 사용하지 않는 VLAN 정리 섹션의 예를 사용합니다.



이제 코어 A와 코어 B는 일부 레이어 3 스위치입니다. VLAN 2와 VLAN 3은 더 이상 코어 A와 코어 B 간에 브리지되지 않으므로 STP 루프가 발생할 가능성이 없습니다.

- 레이어 3 라우팅 프로토콜에 의존하여 이중화가 여전히 존재합니다. 이 설계는 STP를 사용한 재통합보다 훨씬 빠른 재통합을 보장합니다.
- STP가 차단하는 단일 포트가 더 이상 없습니다. 따라서 브리징 루프에 대한 가능성이 없습니다 .
- 레이어 3 스위칭으로 VLAN을 남겨 두는 것은 VLAN 내에서 브리징만큼 빠릅니다.

이 디자인에는 단점이 하나 있습니다. 이러한 설계로의 마이그레이션은 일반적으로 주소 지정 체계의 재작업을 의미합니다.

불필요한 경우에도 STP 유지

네트워크에서 차단된 모든 포트를 제거했으며 물리적 이중화가 없는 경우에도 STP를 비활성화하지 마십시오. STP는 일반적으로 프로세서 집약적이지 않습니다. 패킷 스위칭은 대부분의 Cisco 스위치에서 CPU와 관련이 없습니다. 또한 각 링크에서 전송되는 몇 개의 BPDU는 가용 대역폭을 크게 줄이지 않습니다. 그러나 STP가 없는 브리지 네트워크는 운영자가 패치 패널에서 오류를 발생시키면 1초의 짧은 시간 내에 녹아 내려갈 수 있습니다. 일반적으로 브리지 네트워크에서 STP를 비활성화하는 것은 위험할 만한 가치가 없습니다.

관리 VLAN에서 트래픽을 차단하고 전체 네트워크에 걸쳐 단일 VLAN을 보유하지 않음

Cisco 스위치에는 일반적으로 관리 VLAN이라고 하는 VLAN에 바인딩되는 단일 IP 주소가 있습니다. 이 VLAN에서 스위치는 일반 IP 호스트처럼 작동합니다. 특히 모든 브로드캐스트 또는 멀티캐스트 패킷이 CPU에 전달됩니다. 관리 VLAN에서 브로드캐스트 또는 멀티캐스트 트래픽의 비율이 높

으면 CPU와 중요한 BPDU를 처리하는 CPU 기능에 부정적인 영향을 미칠 수 있습니다. 따라서 관리 VLAN에서 사용자 트래픽을 제거합니다.

최근까지 Cisco 구현에서는 트렁크에서 VLAN 1을 제거할 방법이 없었습니다. VLAN 1은 일반적으로 모든 스위치가 동일한 IP 서브넷에서 액세스할 수 있는 관리 VLAN의 역할을 합니다. 이 설정은 유용하지만 VLAN 1의 브리징 루프가 모든 트렁크에 영향을 미쳐 전체 네트워크가 중단될 수 있으므로 위험할 수 있습니다. 물론 어떤 VLAN을 사용하더라도 동일한 문제가 존재합니다. 고속 레이어 3 스위치를 사용하여 브리징 도메인을 분할해 보십시오.

CatOS 버전 5.4 및 Cisco IOS Software 릴리스 12.1(11b)E부터 트렁크에서 VLAN 1을 제거할 수 있습니다. VLAN 1은 여전히 존재하지만 트래픽을 차단하므로 루프 가능성을 방지합니다.

관련 정보

- 툴 및 리소스 - 기술 지원 및 문서
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.