Cisco 비즈니스 라우터를 위한 VLAN 모범 사례 및 보안 팁

목표

이 문서의 목적은 Cisco Business 장비에서 VLAN을 구성할 때 모범 사례 및 보안 팁을 수행하기 위한 개념과 단계를 설명하는 것입니다.

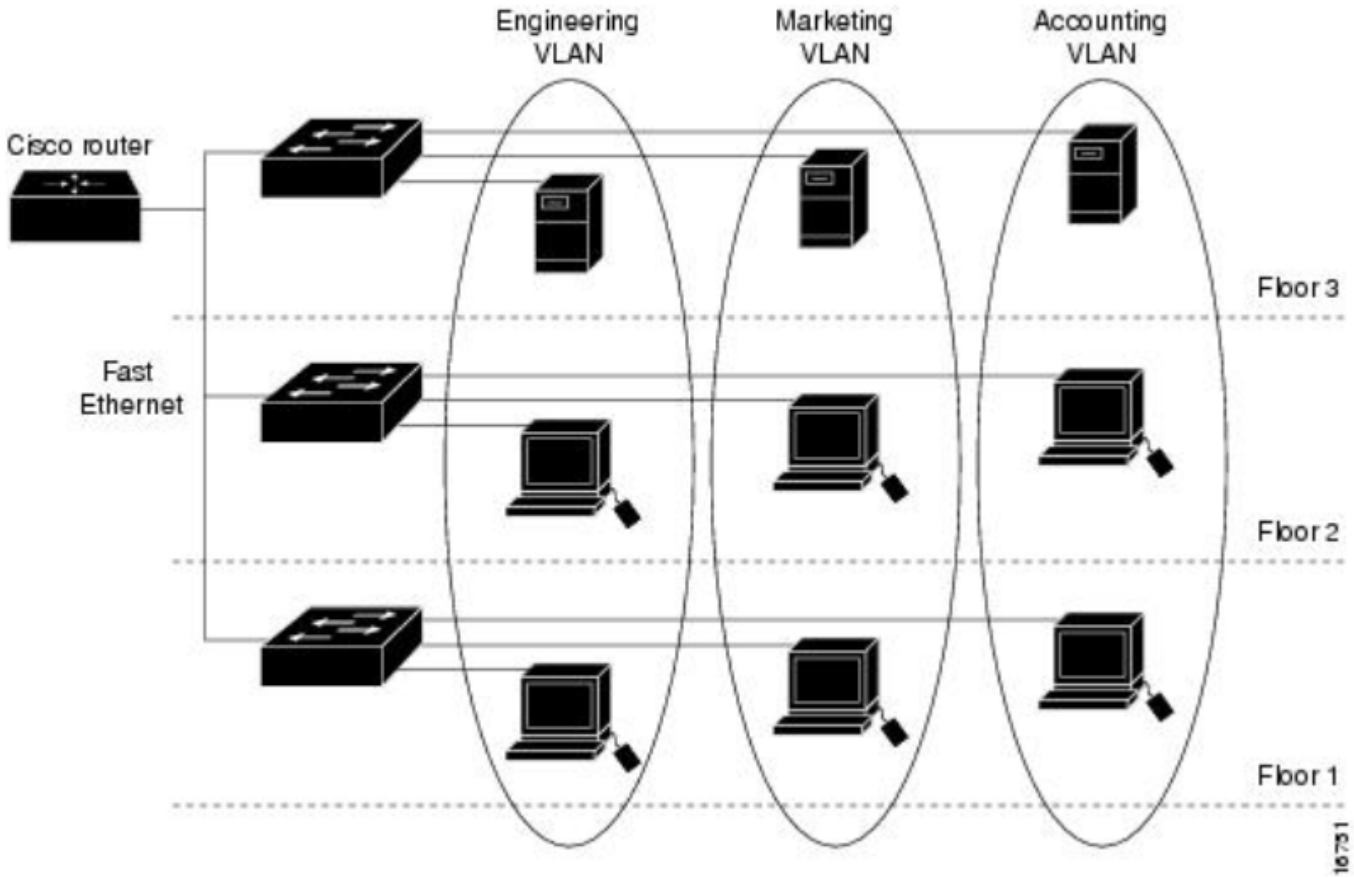
목차

소개

보안을 유지하면서 비즈니스 네트워크의 효율성을 높이고 싶으십니까? 이를 위한 방법 중 하나는 VLAN(Virtual Local Area Network)을 올바르게 설정하는 것입니다.

VLAN은 지리적 분포에도 불구하고 동일한 LAN(Local Area Network)에 있는 것처럼 보이는 워크스테이션, 서버 및 네트워크 디바이스의 논리적 그룹입니다. 간단히 말해, 동일한 VLAN의 하드웨어는 장비 간의 트래픽을 분리하여 더욱 안전하게 보호할 수 있게 합니다.

예를 들어 엔지니어링, 마케팅, 회계 부서가 있을 수 있습니다. 각 부서에는 건물의 다른 층에 근무자가 있지만, 여전히 자신의 부서 내에서 정보에 액세스하고 정보를 전달해야 합니다. 문서 및 웹 서비스를 공유하는 데 필수적입니다.



네트워크를 안전하게 보호하려면 모범 사례를 적용하여 VLAN을 설정해야 합니다. VLAN을 설정할 때 다음 스마트 옵션을 선택합니다. 후회하지 않을 것입니다!

적용 가능한 장치

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

RV160 또는 RV260 Series 라우터는 최대 16개의 VLAN을, RV34x Series 라우터는 최대 32개의 VLAN을 전달할 수 있습니다. RV320은 최대 7개의 VLAN을 지원합니다. 라우터에서 전달할 수 있는 VLAN의 수를 알고 싶다면 Cisco 웹 사이트에서 해당 모델의 데이터 시트를 확인하십시오. 지원을 선택하고 모델 번호를 입력하거나 데이터 시트와 모델 번호를 검색하십시오.

신인을 위한 간단한 어휘

액세스 포트: 액세스 포트는 하나의 VLAN에 대해서만 트래픽을 전달합니다. 액세스 포트는 태그가 지정되지 않은 포트라고도 하는데, 해당 포트에 VLAN이 하나만 있으며 태그 없이 트래픽을 전달할 수 있기 때문입니다.

트렁크 포트: 둘 이상의 VLAN에 대한 트래픽을 전달하는 스위치의 포트. 트렁크 포트는 해당 포트에 둘 이상의 VLAN이 있고 하나의 VLAN을 제외한 모든 트래픽에 대해 태그를 지정해야 하므로 종종 태그 있는 포트라고 합니다.

네이티브 VLAN: 트렁크 포트에서 태그를 수신하지 않는 VLAN. 태그가 없는 트래픽은 네이티브 VLAN으로 전송됩니다. 따라서 트렁크의 양쪽 모두 동일한 네이티브 VLAN을 가지고 있는지 확인해야 합니다. 그렇지 않으면 트래픽이 올바른 위치로 이동하지 않습니다.

모범 사례 #1 - VLAN 포트 할당

포트 할당 기본 사항

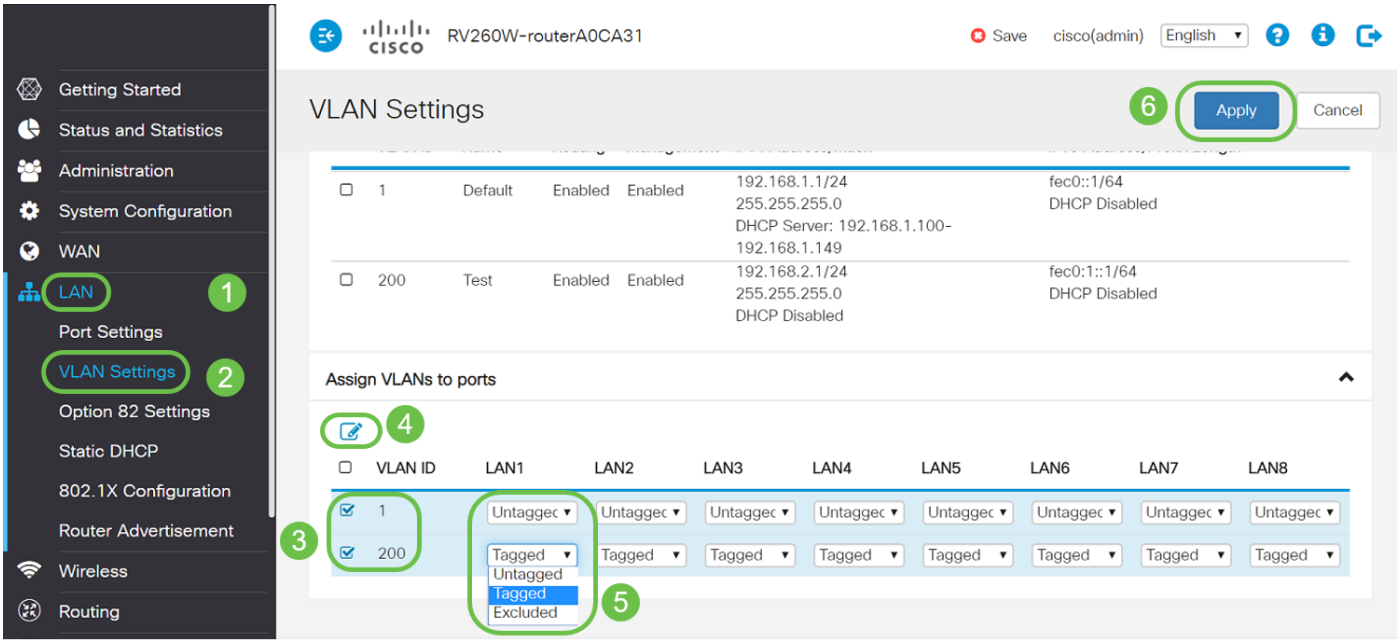
- 각 LAN 포트는 액세스 포트 또는 트렁크 포트로 설정할 수 있습니다.
- 트렁크에 원하지 않는 VLAN은 제외해야 합니다.
- VLAN은 둘 이상의 포트에 배치할 수 있습니다.

액세스 포트 구성

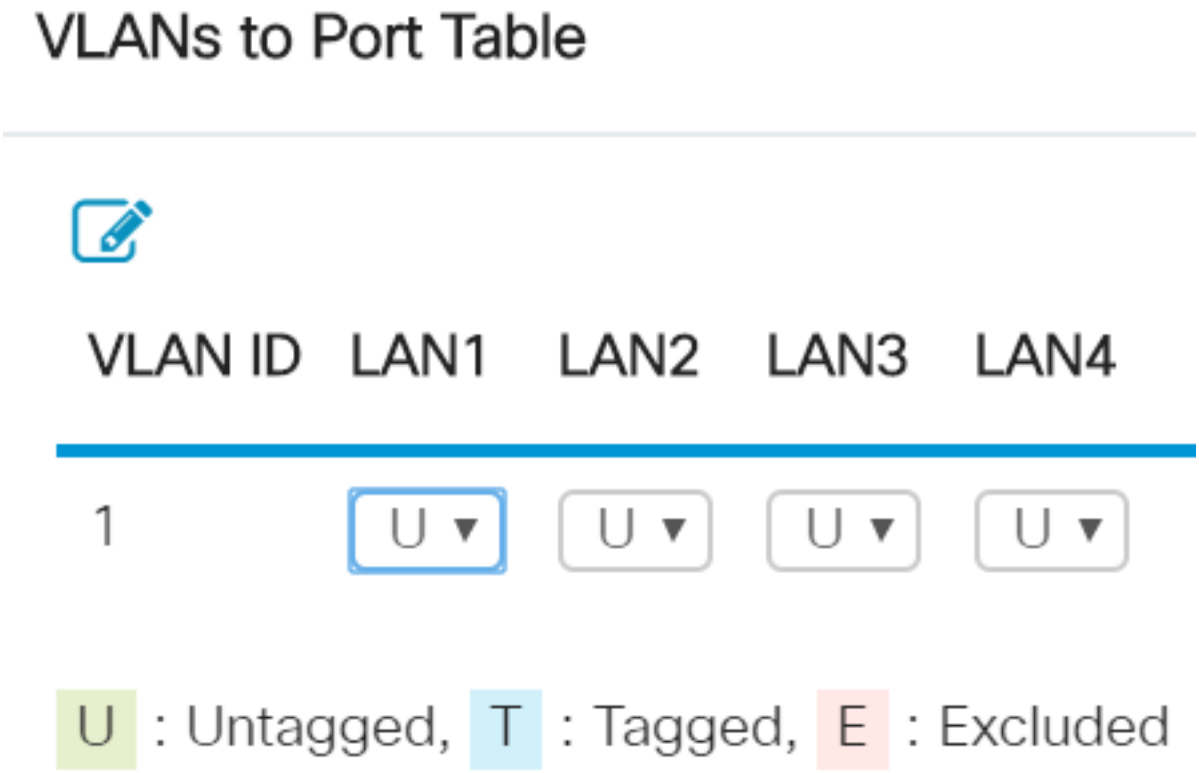
- LAN 포트에 할당된 VLAN 1개
- 이 포트에 할당된 VLAN은 Untagged(태그 없음)로 표시되어야 합니다.
- 다른 모든 VLAN은 해당 포트에 대해 *Excluded*(제외됨)로 표시되어야 합니다

이러한 설정을 올바르게 설정하려면 **LAN > VLAN Settings**로 **이동합니다**. VLAN *ID*를 *선택하고* 수정 *아이콘* 을 **클릭합니다**. 나열된 VLAN의 LAN 인터페이스에 대한 드롭다운 메뉴를 선택하여 VLAN 태깅을 편집합니다. Apply를 **클릭합니다**.

자체 LAN 포트가 할당된 각 VLAN의 다음 예를 확인하십시오.



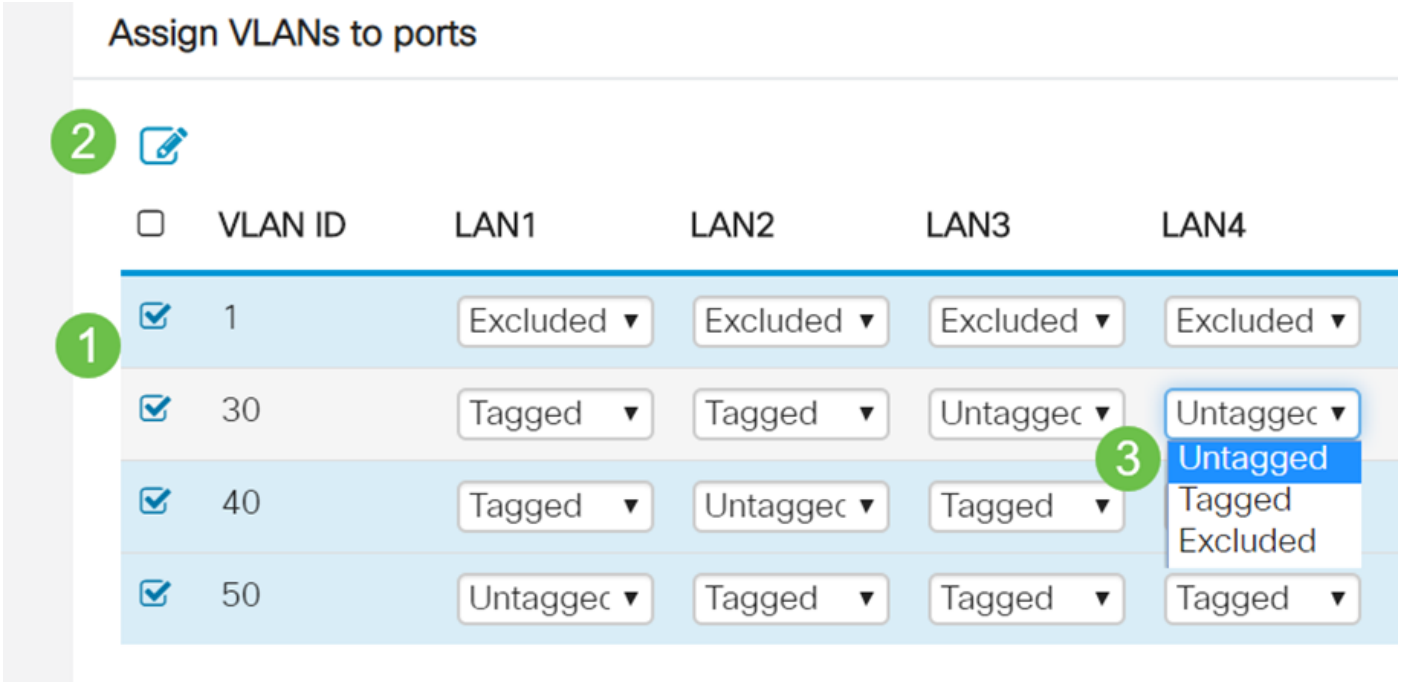
이 GUI 이미지는 RV260W 라우터에서 가져왔습니다. 옵션이 약간 다르게 나타날 수 있습니다. 예를 들어, RV34x 시리즈에서는 *Untagged*, *Excluded*, *Tagged* 레이블이 첫 글자로 축약됩니다. 이 과정은 여전히 똑같습니다.



트렁크 포트 구성

- 둘 이상의 VLAN이 하나의 LAN 포트를 공유함
- VLAN 중 하나는 Untagged(태그 없음)로 *표시될 수 있습니다*.
- 트렁크 포트의 일부인 나머지 VLAN에는 Tagged(태그 지정)라는 레이블이 *있어야 합니다*.
- 트렁크 포트에 속하지 않는 VLAN은 해당 포트에 대해 Excluded(*제외됨*)로 표시되어야 합니다.

트렁크 포트에 있는 다양한 VLAN의 이 예를 살펴보십시오. 이를 올바르게 설정하려면 수정해야 *하는* VLAN ID를 선택합니다. *수정* 아이콘 을 **클릭합니다**. 위의 권장 사항에 따라 요구 사항에 따라 이를 변경합니다. 그런데 VLAN 1은 모든 LAN 포트에서 제외된다는 사실을 알고 있었나요? 이에 대해서는 기본 VLAN 1 모범 사례 섹션에서 설명합니다.



자주 묻는 질문(FAQ)

VLAN이 해당 포트의 유일한 VLAN인데 왜 태그가 지정되지 않았습니까?

액세스 포트에는 VLAN이 하나만 할당되어 있으므로, 프레임의 VLAN 태그 없이 포트의 발신 트래픽이 전송됩니다. 프레임이 스위치 포트(수신 트래픽)에 도달하면 스위치가 VLAN 태그를 추가합니다.

트렁크의 일부인 VLAN에 태그가 지정되는 이유는 무엇입니까?

이렇게 하면 통과하는 트래픽이 해당 포트의 잘못된 VLAN으로 전송되지 않습니다. VLAN이 해당 포트를 공유하고 있습니다. 주소에 추가된 아파트 번호와 비슷하게 메일을 공유 건물의 올바른 아파트로 보냅니다.

기본 VLAN의 일부인 경우 트래픽이 태그가 지정되지 않은 이유는 무엇입니까?

네이티브 VLAN은 하나 이상의 스위치에서 태그 없는 트래픽을 전달하는 방법입니다. 스위치는 태그가 지정된 포트에 도착하는 태그가 지정되지 않은 프레임을 네이티브 VLAN에 할당합니다. 네이티브 VLAN의 프레임이 트렁크(태그가 지정된) 포트를 떠나면 스위치에서 VLAN 태그를 제거합니다.

VLAN이 해당 포트에 없을 때 제외되는 이유는 무엇입니까?

그러면 사용자가 특별히 원하는 VLAN에 대해서만 해당 트렁크의 트래픽이 유지됩니다. 이는 모범 사례로 간주됩니다.

모범 사례 #2 - 기본 VLAN 1 및 미사용 포트

모든 포트는 기본 VLAN을 포함하여 하나 이상의 VLAN에 할당해야 합니다. Cisco Business 라우터는 기본적으로 모든 포트에 VLAN 1이 할당되어 제공됩니다.

관리 VLAN은 텔넷, SSH, SNMP, syslog 또는 Cisco FindIT를 사용하여 네트워크의 디바이스를 원격으로 관리, 제어 및 모니터링하는 데 사용되는 VLAN입니다. 기본적으로 이 역시 VLAN 1입니다. 관리 및 사용자 데이터 트래픽을 분리하는 것이 좋은 보안 방법입니다. 따라서 VLAN을 구성할 때는 관리 목적으로만 VLAN 1을 사용하는 것이 좋습니다.

관리를 위해 Cisco 스위치와 원격으로 통신하려면 관리 VLAN에 IP 주소가 구성되어 있어야 합니다. 다른 VLAN의 사용자는 관리 VLAN으로 라우팅되지 않는 한 스위치에 대한 원격 액세스 세션을 설정할 수 없어 추가 보안 레이어를 제공합니다. 또한 원격 관리를 위해 암호화된 SSH 세션만 허용하도록 스위치를 구성해야 합니다. 이 주제에 대한 토론을 읽으려면 Cisco 커뮤니티 웹 사이트에서 다음 링크를 클릭하십시오.

- 관리 VLAN 논의 #1
- 관리 VLAN 논의 #2

자주 묻는 질문(FAQ)

네트워크를 가상으로 분할하는 데 기본 VLAN 1이 권장되지 않는 이유는 무엇입니까?

주요 이유는 적대적 행위자들이 VLAN 1이 기본값이며 자주 사용된다는 것을 알기 때문입니다. 이를 사용하여 "VLAN 호핑"을 통해 다른 VLAN에 액세스할 수 있습니다. 이름에서 알 수 있듯이, 적대적 액터는 트렁크 포트 및 기타 VLAN에 액세스할 수 있는 VLAN 1로 가장하여 스푸핑된 트래픽을 전송할 수 있습니다.

사용하지 않는 포트를 기본 VLAN 1에 할당할 수 있습니까?

네트워크를 안전하게 보호하려면 그렇게 하지 마십시오. 이러한 모든 포트를 기본 VLAN 1 이외의 VLAN과 연결되도록 구성하는 것이 좋습니다.

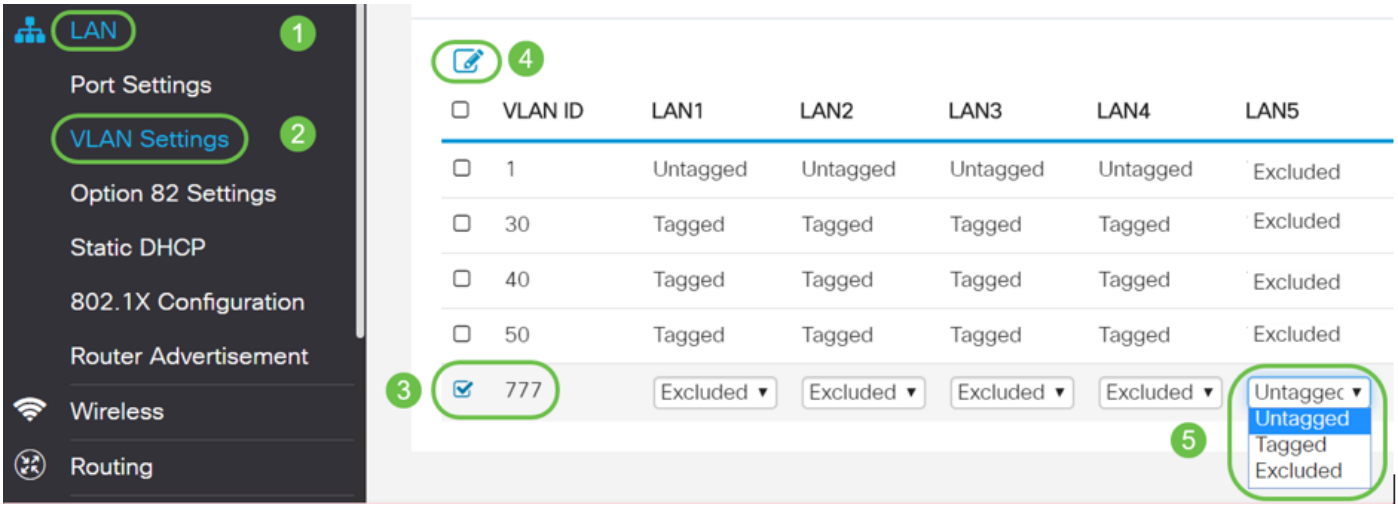
사용하지 않는 포트에 프로덕션 VLAN을 할당하지 않습니다. 어떻게 해야 합니까?

이 문서의 다음 섹션에 있는 지침에 따라 "데드 엔드" VLAN을 생성하는 것이 좋습니다.

모범 사례 #3 - 미사용 포트에 대한 "데드 엔드" VLAN 생성

1단계. **LAN > VLAN Settings(VLAN 설정)로 이동합니다**.

VLAN에 대한 임의의 숫자를 선택합니다. 이 VLAN에는 DHCP, Inter-VLAN 라우팅 또는 디바이스 관리가 활성화되어 있지 않아야 합니다. 이렇게 하면 다른 VLAN의 보안을 강화할 수 있습니다. 사용되지 않는 LAN 포트를 이 VLAN에 배치합니다. 아래 예에서 VLAN *7770*이 생성되어 *LAN5*에 할당되었습니다. 이 작업은 사용되지 않은 모든 LAN 포트에서 수행해야 합니다.



다른 VLAN은 이 LAN 포트에서 제외됩니다.

2단계. **Apply**(*적용*) 버튼을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

모범 사례 #4 - VLAN의 IP 전화

음성 트래픽에는 엄격한 QoS(Quality of Service) 요구 사항이 있습니다. 동일한 VLAN에 컴퓨터와 IP 전화가 있는 회사의 경우, 각 디바이스는 다른 디바이스를 고려하지 않고 가용 대역폭을 사용하려고 시도합니다. 이러한 충돌을 방지하려면 IP 텔레포니 음성 트래픽과 데이터 트래픽에 별도의 VLAN을 사용하는 것이 좋습니다. 이 구성에 대한 자세한 내용은 다음 문서 및 비디오를 참조하십시오.

- Cisco 기술 상담: Cisco Small Business 제품을 사용한 음성 VLAN 설정 및 구성(비디오)
- SG500 Series 스위치에서 QoS를 사용하는 자동 음성 VLAN 구성
- 200/300 Series 매니지드 스위치의 음성 VLAN 컨피그레이션
- Cisco 기술 상담: SG350 및 SG550 Series 스위치에서 자동 음성 VLAN 구성(비디오)

모범 사례 #5 - VLAN 간 라우팅

VLAN은 트래픽을 분리할 수 있도록 설정되지만 간혹 VLAN이 있어야 서로 간에 라우팅할 수 있습니다. 이는 VLAN 간 라우팅이며 일반적으로 권장되지 않습니다. 회사에 필요한 경우 가능한 한 안전하게 설정하십시오. VLAN 간 라우팅을 사용할 경우 ACL(Access Control List)을 사용하여 기밀 정보가 포함된 서버로 트래픽을 제한해야 합니다.

ACL은 패킷 필터링을 수행하여 네트워크를 통한 패킷 이동을 제어합니다. 패킷 필터링은 네트워크에 대한 트래픽 액세스를 제한하고, 네트워크에 대한 사용자 및 디바이스 액세스를 제한하며, 트래픽이 네트워크에서 나가는 것을 방지함으로써 보안을 제공합니다. IP 액세스 목록은 스푸핑 및 서비스 거부 공격의 가능성을 줄이고, 방화벽을 통한 동적 임시 사용자 액세스를 허용합니다.

- 대상 ACL 제한이 있는 RV34x 라우터의 VLAN 간 라우팅
- Cisco 기술 상담: SG250 Series 스위치에서 VLAN 간 라우팅 구성(비디오)
- Cisco 기술 상담: RV180 및 RV180W의 VLAN 간 컨피그레이션(비디오)
- RV34x VLAN 간 액세스 제한(CSCvo92300 버그 수정)

결론

이제 보안 VLAN을 설정하기 위한 몇 가지 모범 사례를 알 수 있습니다. 네트워크에 대한 VLAN을 구성할 때 이러한 팁을 기억하십시오. 아래 목록에는 단계별 지침이 포함된 일부 문서가 나와 있습니다. 이를 통해 비즈니스에 꼭 맞는 생산적이고 효율적인 네트워크로 계속 나아갈 수 있습니다.

- RV160 및 RV260에서 VLAN 설정 구성
- RV34x Series 라우터에서 VLAN(Virtual Local Area Network) 설정 구성
- RV320 및 RV325 VPN 라우터에서 VLAN 멤버십 구성
- RV Series 라우터에서 VLAN(Virtual Local Area Network) 멤버십 구성
- CLI를 통해 Sx350 또는 SG350X 스위치에서 VLAN 인터페이스 IPv4 주소 구성

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.