스위치 용어

목표

이 문서에는 Cisco Small Business 스위치를 설치, 구성 및 트러블슈팅하는 데 사용되는 용어 목록이 포함되어 있습니다.

적용 가능한 디바이스

- Sx200 시리즈
- Sx250 시리즈
- Sx300 시리즈
- Sx350 시리즈
- SG300X 시리즈
- Sx500 시리즈
- Sx550X 시리즈

용어 목록

- 802.1X 서플리컨트 — 서플리컨트는 802.1X IEEE 표준의 세 가지 역할 중 하나입니다. 802.1X는 OSI 모델의 레이어 2에서 보안을 제공하기 위해 개발되었습니다. 신청자, 인증자 및 인증 서버 구성 요소로 구성되어 있습니다. 신청자는 네트워크에 연결되어 해당 네트워크의 리소스에 액세스할 수 있는 클라이언트 또는 소프트웨어입니다. IP 주소를 얻고 특정 네트워크에 속하기 위해 자격 증명 또는 인증서를 제공해야 합니다. 신청자는 인증될 때까지 네트워크의 리소스에 액세스할 수 없습니다.
- ACL — ACL(Access Control List)은 보안 향상을 위해 사용되는 네트워크 트래픽 필터 및 상관관계가 있는 작업의 목록입니다. 사용자가 특정 리소스에 액세스하지 못하도록 차단하거나 허용합니다. ACL에는 네트워크 디바이스에 대한 액세스가 허용되거나 거부된 호스트가 포함됩니다. 라우터 또는 스위치는 액세스 목록 내의 지정된 기준에 따라 패킷을 전달할지 아니면 삭제할지를 결정하기 위해 각 패킷을 검사합니다. 액세스 목록 기준은 트래픽의 소스 주소, 트래픽의 목적지 주소, 상위 계층 프로토콜 또는 기타 정보일 수 있습니다.
- IGMP Snooping — IGMP(Internet Group Management Protocol)는 스위치에서 작동하는 프로토콜로서 멀티캐스트 트래픽에 대해 동적으로 학습할 수 있도록 합니다. IGMP 스누핑은 네

트워크 스위치가 호스트와 라우터 간의 IGMP 대화를 들을 수 있게 해주는 기능입니다. IGMP 스누핑은 그룹의 멀티캐스트 트래픽을 그룹에 가입한 포트로만 전달하도록 라우터에서 활성화되는 필터링 메커니즘을 수행합니다. 따라서 IGMP 스누핑을 사용하면 네트워크의 트래픽이 줄어들고 라우터 뒤에 있는 호스트의 성능이 향상될 수 있습니다. 멀티캐스트는 필요하지 않은 링크에서 필터링될 수 있다.

- IPv4 — IPv4는 네트워크에서 디바이스를 식별하는 데 사용되는 32비트 주소 지정 시스템입니다. 인터넷을 포함한 대부분의 컴퓨터 네트워크에서 사용되는 주소 지정 시스템입니다.

- IPv6 — IPv6는 네트워크에서 디바이스를 식별하는 데 사용되는 128비트 주소 지정 시스템입니다. IPv4의 후속 버전이자 컴퓨터 네트워크에 사용되는 가장 최신 버전의 주소 지정 시스템입니다. IPv6는 현재 전 세계에서 출시되고 있습니다. IPv6 주소는 16진수의 8개 필드로 표시되며, 각 필드에는 16비트가 포함됩니다. IPv6 주소는 두 부분으로 나뉘며, 각 부분은 64비트로 구성됩니다. 첫 번째 부분은 네트워크 주소이고 두 번째 부분은 호스트 주소입니다.

- Link Flap — Link Flap은 스위치의 물리적 인터페이스가 최소 10초 동안 1초에 3회 이상 계속해서 위아래로 진행되는 상황입니다. 일반적인 원인은 대개 불량, 지원되지 않음, 비표준 케이블 또는 SFP(Small Form-Factor Pluggable) 또는 기타 링크 동기화 문제와 관련이 있습니다. 링크 플래핑의 원인은 간헐적이거나 영구적일 수 있습니다.

- MAC 기반 ACL — MAC(Media Access Control) 기반 ACL(Access Control List)은 소스 MAC 주소의 목록입니다. 패킷이 무선 액세스 포인트에서 LAN(Local Area Network) 포트로 전송되거나 그 반대로 전송되는 경우 이 디바이스는 패킷의 소스 MAC 주소가 이 목록의 항목과 일치하는지 확인하고 프레임 내용에 대해 ACL 규칙을 확인합니다. 그런 다음 일치하는 결과를 사용하여 이 패킷을 허용하거나 거부합니다. 그러나 LAN-to-LAN 포트의 패킷은 검사하지 않습니다.

- MLD Snooping — 멀티캐스트는 하나의 호스트에서 그룹의 선택된 호스트로 데이터 패킷을 전송하는 네트워크 레이어 기술입니다. 하위 레이어에서 스위치는 하나의 호스트만 수신을 원하는 경우에도 모든 포트에서 멀티캐스트 트래픽을 브로드캐스트합니다. MLD(Multicast Listener Discovery) 스누핑은 IPv6 멀티캐스트 트래픽을 원하는 호스트로만 전달하는 데 사용됩니다. 스위치에서 MLD 스누핑이 활성화되면 IPv6 라우터와 인터페이스에 연결된 멀티캐스트 호스트 간에 교환되는 MLD 메시지를 탐지합니다. 그런 다음 IPv6 멀티캐스트 트래픽을 제한하는 테이블을 유지 관리하고 이를 수신하고자 하는 포트에 동적으로 전달합니다.

- MSTP — MSTP(Multiple Spanning Tree Protocol)는 단일 물리적 네트워크에서 각 VLAN(Virtual LAN)에 대해 여러 스패닝 트리(인스턴스)를 생성하는 프로토콜입니다. 이렇게 하면 각 VLAN에 대해 구성된 루트 브리지 및 포워딩 토폴로지를 가질 수 있습니다. 이를 통해 네트워크 전체의 BPDU(Bridge Protocol Data Unit) 수가 감소하고 네트워크 디바이스의 CPU(Central Processing Unit)에 대한 스트레스가 감소합니다.

- 포트/VLAN 미러링 — 미러링은 네트워크 트래픽을 모니터링하는 데 사용되는 방법입니다. 포트 또는 VLAN 미러링을 사용하면 네트워크 디바이스의 포트(소스 포트)에서 수신 및 발신 패킷의 복사본이 패킷이 검토되는 다른 포트(대상 포트)로 전달됩니다. 이는 네트워크 관리자가 진단 도구로 사용합니다.

- 포트 보안 — 포트 보안을 구성하는 것도 네트워크 보안을 강화하는 한 가지 방법입니다. 특정 포트 또는 LAG(Link Aggregation Group)에서 구성할 수 있습니다. LAG는 개별 인터페이스를

단일 논리적 링크로 결합하여 최대 8개의 물리적 링크의 총 대역폭을 제공합니다. 지정된 포트/LAG에서 다른 사용자에 대한 액세스를 제한하거나 허용할 수 있습니다. 포트 보안은 동적으로 학습된 고정 MAC 주소와 함께 사용되어 포트의 인그레스 트래픽을 제한할 수도 있습니다.

- 프로토콜 기반 VLAN - 프로토콜 기반 그룹을 정의하고 포트에 바인딩할 수 있습니다. 따라서 프로토콜 그룹에서 시작되는 모든 패킷이 페이지의 구성된 VLAN에 할당됩니다. 프로토콜 기반 VLAN은 필요한 각 프로토콜에 대해 물리적 네트워크를 논리적 VLAN 그룹으로 나눕니다. 인바운드 패킷에서는 프레임이 확인되고 프로토콜 유형에 따라 VLAN 멤버십이 결정될 수 있습니다. 프로토콜 기반 그룹과 VLAN 매핑은 프로토콜 그룹을 단일 포트에 매핑하는 데 도움이 됩니다.

- QoS — QoS(Quality of Service)를 사용하면 다양한 애플리케이션, 사용자 또는 데이터 흐름에 대해 트래픽의 우선 순위를 지정할 수 있습니다. 또한 성능을 지정된 수준으로 보장하여 클라이언트의 서비스 품질에 영향을 주는 데 사용할 수 있습니다. QoS는 일반적으로 지터, 레이턴시, 패킷 손실의 영향을 받습니다.

- RADIUS 서버 — RADIUS(Remote Authentication Dial-In User Service)는 디바이스가 네트워크 서비스를 연결하고 사용하기 위한 인증 메커니즘입니다. 중앙 집중식 인증, 권한 부여 및 계정 관리 용도로 사용됩니다. RADIUS 서버는 입력한 로그인 자격 증명을 통해 사용자의 ID를 확인하여 네트워크에 대한 액세스를 제어합니다. 예를 들어, 대학 캠퍼스에는 공용 Wi-Fi 네트워크가 설치되어 있습니다. 암호를 가진 학생만 이러한 네트워크에 액세스할 수 있습니다. RADIUS 서버는 사용자가 입력한 비밀번호를 확인하고 액세스 권한을 적절하게 부여하거나 거부합니다.

- RSTP — RSTP(Rapid Spanning Tree Protocol)는 STP의 향상된 기능입니다. RSTP는 토폴로지 변경 후 더 빠른 스패닝 트리 컨버전스를 제공합니다. STP는 토폴로지 변경에 응답하는 데 30~50초가 걸릴 수 있으며, RSTP는 구성된 hello 시간의 3배 이내에 응답합니다. RSTP는 STP와 역호환됩니다.

- SNMP — SNMP(Simple Network Management Protocol)는 네트워크 디바이스에 대한 정보를 저장하고 공유하기 위한 네트워크 표준입니다. SNMP는 네트워크 관리, 문제 해결 및 유지보수를 용이하게 합니다.

- STP(Spanning Tree Protocol)는 LAN(Local Area Network)에서 사용되는 네트워크 프로토콜입니다. STP의 목적은 LAN에 루프 프리(loop-free) 토폴로지를 보장하는 것입니다. STP는 두 네트워크 디바이스 간에 하나의 활성 경로만 있음을 보장하는 알고리즘을 통해 루프를 제거합니다. STP는 트래픽이 네트워크 내에서 가능한 최단 경로를 사용하는지 확인합니다. 또한 STP는 활성 경로에 장애가 발생할 경우 중복 경로를 백업 경로로 자동으로 다시 활성화할 수 있습니다.

- SSL 서버 — SSL(Secure Sockets Layer)은 주로 인터넷의 보안 관리에 사용되는 프로토콜입니다. HTTP와 TCP 레이어 사이에 있는 프로그램 레이어를 사용합니다. 인증을 위해 SSL은 공개 키에 디지털 서명되고 바인딩된 인증서를 사용하여 개인 키 소유자를 식별합니다. 이 인증은 연결 시 도움이 됩니다. SSL을 사용하여 인증서는 ITU-T 표준 X.509에 설명된 형식으로 인증 프로세스 동안 블록 단위로 교환됩니다. 그런 다음 외부 기관인 인증 기관에서 X.509 인증서를 발급하며, 이 인증서는 디지털 서명됩니다.

- Syslog 어그리게이션 — Syslog 서비스는 단순히 메시지를 수락하고, 이를 파일에 저장하거나 간단한 컨피그레이션 파일에 따라 인쇄합니다. Syslog Aggregation(Syslog 어그리게이션)은 동일한 유형의 여러 syslog 메시지가 인스턴스가 발생할 때마다 화면에 나타나지 않음을 의미합니다. 로깅 집계를 활성화하면 특정 기간 동안 수신할 시스템 메시지를 필터링할 수 있습니다. 이 기능은 동일한 유형의 몇 가지 syslog 메시지를 수집하므로 메시지가 발생할 때 나타나지 않고 지정된 간격에 나타납니다.

- TACACS+ — TACACS+(Terminal Access Controller Access Control System)는 사용자 이름과 비밀번호를 통해 인증 및 권한 부여를 제공함으로써 향상된 보안을 구현하는 데 사용되는 Cisco 전용 프로토콜입니다. TACACS+ 서버를 구성하려면 사용자에게 스위치의 모든 컨피그레이션 기능에 대한 액세스 권한을 제공하는 권한 15 액세스 권한이 있어야 합니다. 일부 스위치는 TACACS+ 클라이언트 역할을 할 수 있으며, 여기서 연결된 모든 사용자는 올바르게 구성된 TACACS+ 서버를 통해 네트워크에서 인증되고 권한을 부여받을 수 있습니다. TACACS+는 IPv4만 지원합니다.

- TFTP 서버 — TFTP(Trivial File Transfer Protocol) 서버는 LAN의 디바이스 간에 컨피그레이션 및 부팅 파일을 자동으로 전송하는 데 사용되는 서버입니다. 프로토콜은 간단하여 메모리 사용량이 적지만, 이러한 단순성으로 인해 프로토콜이 쉽게 손상될 수도 있습니다. 이러한 이유로, TFTP는 인터넷과 함께 거의 사용되지 않는다.

- VLAN — VLAN(Virtual Local Area Network)은 사용자의 물리적 위치와 상관없이 기능, 영역 또는 애플리케이션별로 논리적으로 분할된 스위치드 네트워크입니다. VLAN은 네트워크의 어느 곳에나 위치할 수 있지만 동일한 물리적 세그먼트에 있는 것처럼 통신할 수 있는 호스트 또는 포트 그룹입니다. VLAN을 사용하면 물리적 연결을 변경하지 않고 디바이스를 새 VLAN으로 이동할 수 있으므로 네트워크 관리가 간소화됩니다.

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.