Cisco 비즈니스의 새로운 기능: 장비 및 기본 네트워크 용어집

목표

이 문서의 목적은 Cisco Business(Small Business) 장비와 여러분이 알아야 할 일반적인 용어를 숙지하는 초급자를 확보하는 것입니다. 사용 가능한 하드웨어, Cisco 비즈니스 약관, 일반 네트워킹 약관, Cisco 툴, 데이터 교환의 기본 사항, 인터넷 연결의 기본 사항, 네트워크 및 이러한 기능이 어떻게 연결되는지 등의 주제를 다룹니다.

소개

Cisco 장비를 사용하여 네트워크를 막 설정하려고 하십니까? 네트워크 설정 및 유지 관리의 새로운 세계에 진입하는 것은 부담스러울 수 있습니다. 이 기사는 여러분이 몇 가지 기본 사항을 익히도록 돕기 위해 여기 있습니다. 여러분이 더 많이 알수록, 그것은 덜 위협적일 것입니다!

Cisco 비즈니스에서 하드웨어 사용 가능

라우터

라우터는 여러 네트워크를 함께 연결하고, 이동해야 하는 위치에 데이터를 라우팅합니다. 그들은 또한 네트워크에 있는 컴퓨터들을 인터넷에 연결합니다. 라우터를 사용하면 모든 네트워크 컴퓨터가 단일 인터넷 연결을 공유하여 비용을 절감할 수 있습니다.

라우터는 디스패처 역할을 합니다. 네트워크를 통해 전송되는 데이터를 분석하고, 데이터를 이동할 최적의 경로를 선택하고, 이동하는 동안 전송합니다.

라우터는 비즈니스를 전 세계에 연결하고, 보안 위협으로부터 정보를 보호하며, 어떤 컴퓨터가 다른 컴퓨터보다 우선순위가 높은지 결정할 수 있습니다.

라우터에는 이러한 기본적인 네트워킹 기능 외에도 네트워킹을 보다 쉽고 안전하게 만들 수 있는 추가 기능이 제공됩니다. 예를 들어 사용자의 필요에 따라 방화벽, VPN(Virtual Private Network) 또는 IP(Internet Protocol) 통신 시스템이 있는 라우터를 선택할 수 있습니다.

가장 최근에 개발된 Cisco Business 라우터에는 RV160, RV260, RV340 및 RV345 시리즈가 포함됩니다.

스위치

스위치는 대부분의 비즈니스 네트워크의 기반입니다. 스위치는 컨트롤러 역할을 하여 컴퓨터, 프린터 및 서버를 건물 또는 캠퍼스의 네트워크에 연결합니다.

스위치를 사용하면 네트워크의 디바이스가 서로 통신하고 다른 네트워크와 통신하여 공유 리소스 네트워크를 생성할 수 있습니다. 정보 공유 및 리소스 할당을 통해 스위치를 사용하면 비용을 절감하고 생산성을 높일 수 있습니다.

네트워킹 기본 사항의 일환으로 선택할 수 있는 두 가지 기본 스위치 유형이 있습니다. 관리 및 비관리.

> 관리되지 않는 스위치는 기본적으로 작동하지만 구성할 수 없습니다. 홈 네트워킹 장비는 일반적으로 관리되지 않는 스위치를 제공합니다.
> 관리되는 스위치를 구성할 수 있습니다. 매니지드 스위치를 로컬 또는 원격으로 모니터링하고 조정할 수 있으므로 네트워크 트래픽 및 액세스에 대한 제어력이 향상됩니다.

스위치에 대한 자세한 내용은 스위치 용어 **용어집을 참조하십시오**.

가장 최근에 개발된 스위치로는 Cisco Business Switch CBS110, CBS220, CBS250, CBS350 시리즈가 있습니다.

CBS 스위치 간의 차이점을 알고 싶다면

무선 액세스 포인트

무선 액세스 포인트를 사용하면 장치가 케이블 없이 무선 네트워크에 연결할 수 있습니다. 무선 네트워크를 사용하면 새로운 장치를 손쉽게 온라인으로 연결하고 모바일 근로자에게 유연한 지원을 제공할 수 있습니다.

액세스 포인트는 네트워크의 증폭기 역할을 합니다. 라우터가 대역폭을 제공하지만, 액세스 포인트는 네트워크가 많은 장치를 지원할 수 있도록 해당 대역폭을 확장하며, 이러한 디바이스는 멀리 떨어진 곳에서 네트워크에 액세스할 수 있습니다.

그러나 액세스 포인트는 단순히 Wi-Fi를 확장하는 것 이상을 수행합니다. 또한 네트워크의 디바이스에 대한 유용한 데이터를 제공하고, 사전 보안을 제공하며, 기타 여러 가지 실질적인 목적을 지원할 수 있습니다.

가장 최근에 개발된 무선 액세스 포인트인 Cisco Business Wireless에는 무선 메시 네트워크를 지원하는 AC140, AC145 및 AC240이 포함됩니다. 메시 무선 네트워크에 익숙하

지 않은 경우 Welcome to Cisco Business Wireless Mesh Networking 또는 Cisco Business Wireless Network에 대한 FAQ(자주 묻는 질문)에서 자세히 알아보십시오.

Wireless Access Point에서 자주 사용하는 용어를 알아보려면 WAP 용어를 확인하십시오.

다중 플랫폼 전화

MPP 전화기는 SIP(Session Initiation Protocol)를 사용하여 VoIP(Voice over IP) 통신을 제공합니다. 따라서 기존 전화 회선이 필요하지 않게 되므로 회사 내에서 휴대 전화를 더 많이 사용할 수 있습니다. VoIP를 사용하면 값비싼 T1 회선 대신 기존 네트워크 인프라 및 인터넷 연결을 사용합니다. 따라서 더 적은 수의 '회선'으로 더 많은 통화를 관리할 수 있습니다. 기타 유용한 옵션으로는 통화 보류, 주차 통화, 통화 호전환 등이 있습니다. 일부 모델은 VoIP 외에도 비디오 통신을 허용합니다.

MPP 전화기는 일반 전화기처럼 보이도록 제작되었으며 그 용도로만 사용되지만, 기본적으로 컴퓨터이며 네트워크의 일부입니다. MPP 전화에는 ITSP(Internet Telephony Service Provider) 또는 PBX(IP Private Branch Exchange) 통화 제어 서버의 서비스가 필요합니다. WebEx Calling, Ring Central 및 Verizon은 ITSP의 예입니다. Cisco MPP 전화와 함께 작동하는 IP PBX 서비스의 일부 예로는 별표, Centile 및 Metaswitch 플랫폼이 있습니다. 이러한 전화기의 많은 기능은 특히 서드파티 제공업체(예: FreePBX)를 통해 프로그래밍되므로 프로세스(주차 공간, 음성 메일 액세스 등)가 달라질 수 있습니다.

가장 최근에 개발된 Cisco Business MPP 전화에는 6800, 7800 및 8800 시리즈가 포함됩니다.

Cisco Business에서 일반적으로 참조

관리 설명서 및 빠른 시작 설명서

이러한 리소스는 제품 및 해당 기능에 대한 매우 자세한 정보를 얻기 위해 검색할 수 있는 두 가지 리소스입니다. 모델 번호를 사용하여 사이트나 웹 검색을 수행할 때 하나 또는 다른 하나를 추가하여 이러한 긴 안내선을 볼 수 있습니다.

기본 설정

디바이스는 미리 선택된 기본 설정으로 제공됩니다. 관리자가 가장 일반적으로 선택하는 설정입니다. 필요에 맞게 설정을 변경할 수 있습니다.

기본 사용자 이름 및 비밀번호

이전 Cisco Business 장비에서 기본값은 사용자 이름과 비밀번호 모두에 대한 *admin*이었습니다. 이제 대부분의 경우 사용자 이름과 비밀번호 모두에 *cisco*의 기본값이 있습니다. VoIP(Voice over IP) 전화에서 많은 컨피그레이션을 변경하려면 *관리자*로 로그인해야 합니다. 보안을 위해 비밀번호를 더 복잡하게 변경하는 것이 좋습니다.

기본 IP 주소

대부분의 Cisco 장비는 라우터, 스위치 및 무선 액세스 포인트에 대한 기본 IP 주소를 제공합니다. IP 주소를 기억할 수 없고 특별한 컨피그레이션이 없는 경우 열린 페이퍼클립을 사용하여 디바이스에서 재설정 버튼을 최소 10초 동안 누를 수 있습니다. 이렇게 하면 기본 설정으로 재설정됩니다. 스위치 또는 WAP가 DHCP가 활성화된 라우터에 연결되어 있지 않고 컴퓨터를 사용하여 스위치 또는 WAP에 직접 연결되어 있는 경우 이러한 IP 주소가 기본 IP 주소입니다.

Cisco Business 라우터의 기본 IP 주소는 192.168.1.1입니다.
Cisco Business 스위치의 기본 IP 주소는 192.168.1.254입니다.
Small Business 무선 액세스 포인트(AP)의 기본 IP 주소는 192.168.1.245입니다. 새 메시 무선 액세스 포인트에 대한 기본 IP 주소는 없습니다.

공장 기본값으로 재설정

Cisco Business 라우터, 스위치 또는 Wireless Access Point를 공장 기본 설정으로 재설정하고 처음부터 다시 시작하려는 경우가 있습니다. 이 기능은 장비를 한 네트워크에서 다른 네트워크로 이동하거나 구성 문제를 해결할 수 없는 마지막 수단으로 이동하는 데 유용합니다. 공장 기본 설정으로 재설정하면 모든 컨피그레이션이 손실됩니다.

공장 재설정 후 복원할 수 있도록 컨피그레이션을 백업할 수 있습니다. 자세한 내용을 보려면 다음 링크를 클릭하십시오.

- 웹 기반 유틸리티를 통해 RV34x Series 라우터의 공장 기본 설정 재부팅 또는 복원
- 스위치에서 펌웨어 백업 및 복원 또는 교체
- 무선 액세스 포인트에서 구성 파일 다운로드, 백업, 복사 및 삭제
- WAP125 또는 WAP581 액세스 포인트에서 구성 파일 관리

컨피그레이션을 백업하지 않을 경우 처음부터 다시 디바이스를 설정해야 연결 세부 정보가 있는지 확인합니다. 대부분의 모델에는 재설정을 위해 수행해야 하는 단계를 자세히 설명하는 문서가 있지만 가장 간단한 방법은 열린 페이퍼 클립을 사용하고 디바이스에서 재설정 버튼을 10초 이상 누르는 것입니다. MPP 전화에는 적용되지 않으므로 자세한 내용은 Reset a Cisco IP Phone(Cisco IP Phone 재설정)을 참조하십시오.

웹 사용자 인터페이스(UI)

Cisco Business 장비의 모든 부분에는 웹 UI가 제공됩니다. 단, 100 시리즈 비관리형 스위치를 제외합니다.

이 유형의 인터페이스, 화면에 표시되는 것은 선택 옵션을 보여줍니다. 이러한 화면을 탐색하기 위해 어떤 명령도 알 필요가 없습니다. 웹 UI는 GUI(Graphical User Interface), 웹 기반 인터페이스, 웹 기반 지침, 웹 기반 유틸리티 또는 웹 구성 유틸리티라고도 합니다.

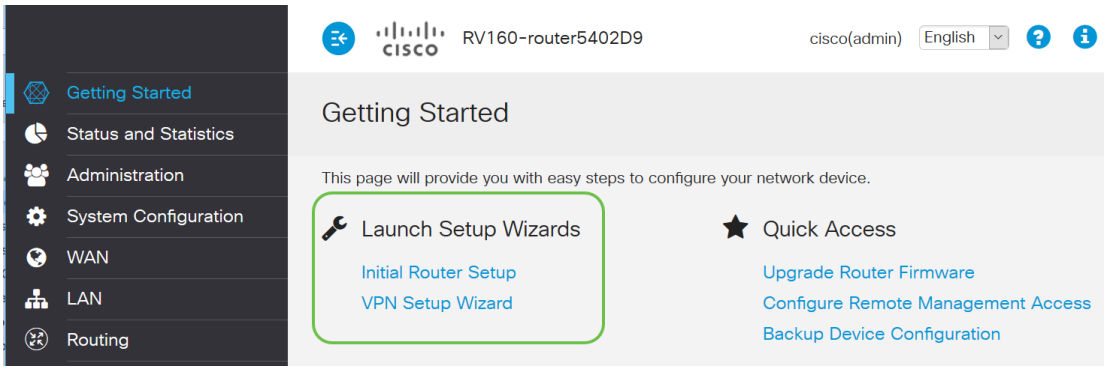
디바이스의 컨피그레이션을 변경하는 가장 쉬운 방법 중 하나는 웹 UI를 사용하는 것입니다. 웹 UI는 디바이스의 성능을 수정하도록 변경할 수 있는 모든 기능을 포함하는 툴을 관리자에게 제공합니다.

Cisco 디바이스에 로그인하면 왼쪽의 탐색 창이 포함된 웹 UI 화면이 표시됩니다. 여기에는 디바이스의 최상위 기능 목록이 포함됩니다. 탐색 창을 탐색 트리, 탐색 모음 또는 탐색 맵이라고도 합니다.

이 페이지의 색상은 장비 및 펌웨어 버전에 따라 최상위 기능은 물론 다양할 수 있습니다.

설치 마법사

이 인터랙티브 화면에서는 Cisco Small Business 디바이스에 처음 로그인할 때, 그리고 그 이후에 탐색할 수 있습니다. 네트워크를 가동할 수 있는 좋은 방법이 될 수 있습니다. 변경할 수 있는 몇 가지 기본 설정이 미리 선택되어 있습니다. 일부 장치에는 둘 이상의 설치 마법사가 제공됩니다. 이 예에서는 두 개의 설정 마법사, *초기 라우터 설정* 및 *VPN 설정 마법사*를 보여줍니다.



Cisco 독점

특히 Cisco가 개발 및 소유하고 있습니다. 예를 들어, Cisco CDP(Discovery Protocol)는 Cisco 독점 제품입니다. 일반적으로 Cisco 전용 프로토콜은 Cisco 디바이스에서만 사용할 수 있습니다.

시리즈의 모델

Cisco는 소규모 비즈니스 소유자에게 회사의 요구 사항에 맞는 다양한 모델을 제공합니다. 모델에는 다양한 기능, 포트 수, PoE(Power over Ethernet) 또는 무선 기능이 제공됩니다. 시리즈에 모델이 여러 개 있는 경우 Cisco는 모델 간에 다른 번호 또는 문자 대신 x를 입력하지만 해당 시리즈의 모든 모델에 정보가 적용됩니다. 예를 들어 RV340 및 RV345 라우터는 RV34x 시리즈에서 참조됩니다. 끝에 IP가 있으면 POE(Power over Ethernet)를 제공합니다. 디바이스 이름이 W로 끝나는 경우 무선 기능을 제공합니다. 일반적으로 모델의 수가 많을수록 디바이스의 기능이 더 높습니다. 자세한 내용을 보려면 다음 문서를 확인하십시오.

- 제품 디코더 링 - 라우터
- 제품 ID 디코더 - 스위치
- 제품 디코더 링 - WAP
- Cisco Business Wireless Model Decoder(Mesh Wireless)

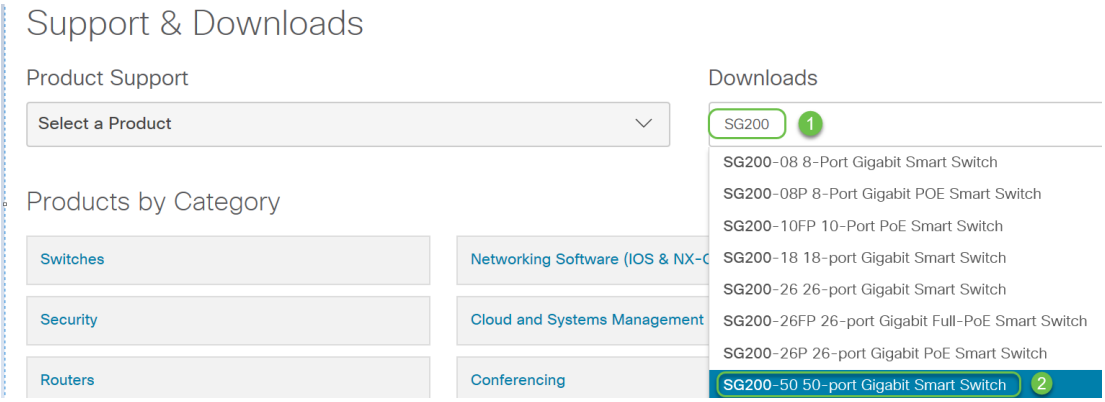
펌웨어

이미지라고도 합니다. 디바이스의 작업 및 기능을 제어하는 프로그램입니다.

펌웨어 업그레이드

펌웨어 업그레이드는 모든 디바이스에서 최적의 성능을 발휘하기 위해 필수적입니다. 업그레이드가 릴리스될 때 반드시 설치해야 합니다. Cisco에서 펌웨어 업그레이드를 릴리스할 때, 보안 취약성 또는 성능 문제를 일으킬 수 있는 새로운 기능 또는 버그 수정과 같은 개선 사항이 포함되어 있는 경우가 많습니다.

Cisco Support(시스코 지원)로 이동하여 Downloads(다운로드)에서 업그레이드가 필요한 디바이스의 이름을 *입력합니다*. 드롭다운 메뉴가 나타납니다. 아래로 스크롤하여 소유한 특정 모델을 선택합니다.



팁: 다양한 버전의 Cisco 펌웨어를 살펴볼 때 각각 x.x.x.x 형식을 따릅니다. 4개의 8진수로 간주됩니다. 사소한 업데이트가 있는 경우 네 번째 8진수가 변경됩니다. 세 번째 8진수는 더 큰 변화일 때 바뀝니다. 두 번째 8진수는 큰 변화를 의미합니다. 전면 재검토라면 첫 8진보는 달라진다.

지침을 원하는 경우 이 링크를 클릭하여 Download and Upgrade Firmware on any Device를 선택합니다.

이 문서에는 스위치 업그레이드에 문제가 있을 경우에 대비하여 몇 가지 트러블슈팅 아이디어가 있습니다. 200/300 Series 스위치에서 펌웨어 업그레이드.

일반 네트워킹 용어

장비가 있으면 네트워킹의 몇 가지 일반적인 용어를 숙지해야 합니다.

인터페이스

인터페이스는 일반적으로 한 시스템과 다른 시스템 사이의 공간입니다. 포트를 포함하여 컴퓨터와 통신할 수 있는 모든 것. 일반적으로 네트워크 인터페이스에는 로컬 IP 주소가 할당됩니다. 사용자 인터페이스를 사용하면 운영 체제와 상호 작용할 수 있습니다.

노드

네트워크 내에서 연결 또는 상호 작용을 수행하거나 정보를 전송, 수신 및 저장하며, 인

터넷과 통신하고, IP 주소를 가진 모든 장치를 설명하는 일반적인 용어입니다.

호스트

호스트는 네트워크에서 통신을 위한 엔드포인트인 디바이스이며, 호스트는 다른 노드에 데이터 또는 서비스(DNS와 유사)를 제공할 수 있습니다. 토폴로지에 따라 스위치 또는 라우터가 호스트가 될 수 있습니다. 모든 호스트도 노드입니다. 예를 들면 컴퓨터, 서버 또는 프린터가 있습니다.

컴퓨터 프로그램

컴퓨터 프로그램은 컴퓨터에서 실행할 수 있는 지침을 전달합니다.

애플리케이션

애플리케이션 소프트웨어는 작업을 수행하는 데 도움이 되는 프로그램입니다. 이러한 프로그램은 유사하기 때문에 상호 교환으로 언급되는 경우가 많으나, 모든 프로그램이 애플리케이션인 것은 아닙니다.

모범 사례

네트워크를 설정하고 실행하는 데 권장되는 방법입니다.

토폴로지

장비가 연결된 물리적 방식입니다. 네트워크의 맵입니다.

구성

이는 설정 방법을 의미합니다. 기본 설정, 장비를 구매할 때 미리 구성된 설정 또는 특정 요구 사항에 맞게 구성할 수 있습니다. 기본 설정은 기본, 자주 권장되는 컨피그레이션입니다. 디바이스에 로그온하면 작업 과정을 안내하는 설정 마법사가 있을 수 있습니다.

MAC 주소

각 디바이스의 고유 식별자입니다. 물리적 디바이스에 있으며 Bonjour, LLDP 또는 CDP에서 탐지할 수 있습니다. 스위치는 장치와 상호 작용할 때 MAC 주소를 추적하여 MAC 주소 테이블을 생성합니다. 이를 통해 스위치는 정보 패킷을 라우팅할 위치를 파악할 수 있습니다.

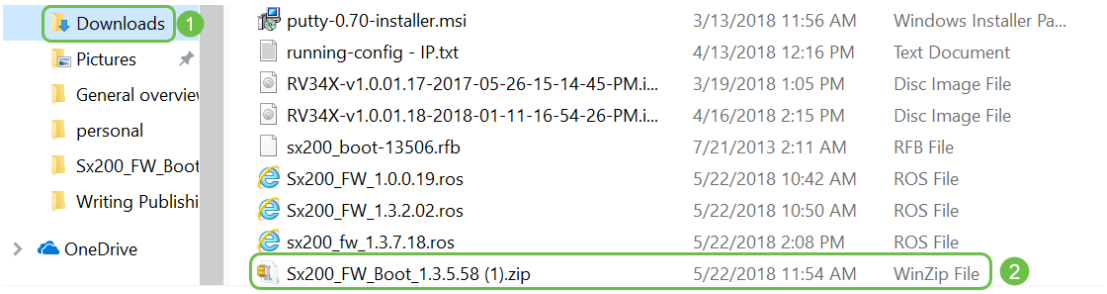
오픈 소스

일반에게 무료로 제공되는 프로그램.

Zip 파일

하나의 zip 파일로 압축된 파일 그룹입니다. 한 번에 여러 파일을 전송하려는 경우에 사용됩니다. 수신자는 zip 파일을 열고 각각의 파일에 개별적으로 액세스할 수 있습니다. zip 파일은 *.zip*으로 끝납니다.

*.zip*으로 끝나는 형식의 파일이 표시되는 경우 해당 파일의 압축을 풀어야 합니다. 압축 풀기 프로그램이 없으면 프로그램을 다운로드해야 합니다. 온라인에서는 몇 가지 무료 옵션이 있습니다. 압축 해제 프로그램을 다운로드했으면 **Downloads**(다운로드)를 클릭하고 압축을 풀어야 하는 *.zip* 파일을 찾습니다.



zip 파일의 이름을 마우스 오른쪽 버튼으로 클릭하면 이와 유사한 화면이 나타납니다. 압축 해제 소프트웨어 위에 마우스 커서를 올려 놓고 **Extract Here**를 선택합니다. 이 예에서는 7-Zip이 사용됩니다.

CLI(Command Line Interface)

CLI(Command Line Interface): 터미널이라고도 합니다. 이는 라우터 및 스위치와 같은 디바이스에서 구성을 선택하는 또 다른 옵션으로 사용됩니다. 다양한 웹 UI 화면을 탐색할 필요가 없으므로 설정을 간편하게 할 수 있습니다. 따라서 명령을 알고 완벽하게 입력해야 합니다. 초보자용 기사를 읽고 있으므로 CLI를 처음 선택하는 것은 아닐 것입니다.

가상 머신

대부분의 시스템은 필요한 기능보다 뛰어난 기능을 제공합니다. 컴퓨터를 프로비저닝하여 둘 이상의 시스템을 실행하는 데 필요한 모든 것을 보관할 수 있습니다. 문제는 한 부분이 중단되거나 재부팅이 필요할 경우 모두 따라온다는 것입니다.

VMware 또는 Hyper-V를 설치할 경우 한 컴퓨터에서 소프트웨어, 웹 서버, 이메일 서버, FindIT 등을 로드할 수 있습니다. 가상 머신은 다른 운영 체제를 사용할 수도 있습니다. 그들은 논리적으로 서로 독립되어 있다. 각각은 실제로 하나의 장치가 아닌 별도의 장치의 기능을 수행합니다. 하드웨어가 공유되지만 각 가상 머신은 각 운영 체제에 대해 물리적 상환의 일부를 할당합니다. 이렇게 하면 비용, 에너지 및 공간을 절약할 수 있습니다.

사용할 수 있는 Cisco 툴

Cisco Business Dashboard(CBD)

이는 네트워크를 모니터링하고 유지 관리하는 데 사용되는 Cisco 툴입니다. CBD는 네트워크의 Cisco 장치 및 기타 유용한 관리 기능을 식별하는 데 도움이 됩니다.

재택 근무 또는 둘 이상의 네트워크를 감독할 경우 이는 유용한 툴입니다. CBD는 가상 머신으로 운영됩니다. CBD에 대한 자세한 내용은 Cisco Business Dashboard Support Site 또는 Cisco Business Dashboard Overview를 참조하십시오.

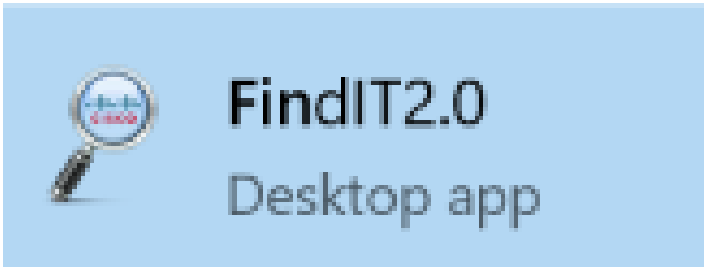
FindIT Network Discovery Utility

이 간단한 툴은 매우 기본적이지만 네트워크에서 Cisco 장비를 신속하게 검색할 수 있도록 지원합니다. Cisco FindIT는 PC와 동일한 로컬 네트워크 세그먼트에서 지원되는 모든 Cisco Small Business 장치를 자동으로 검색합니다.

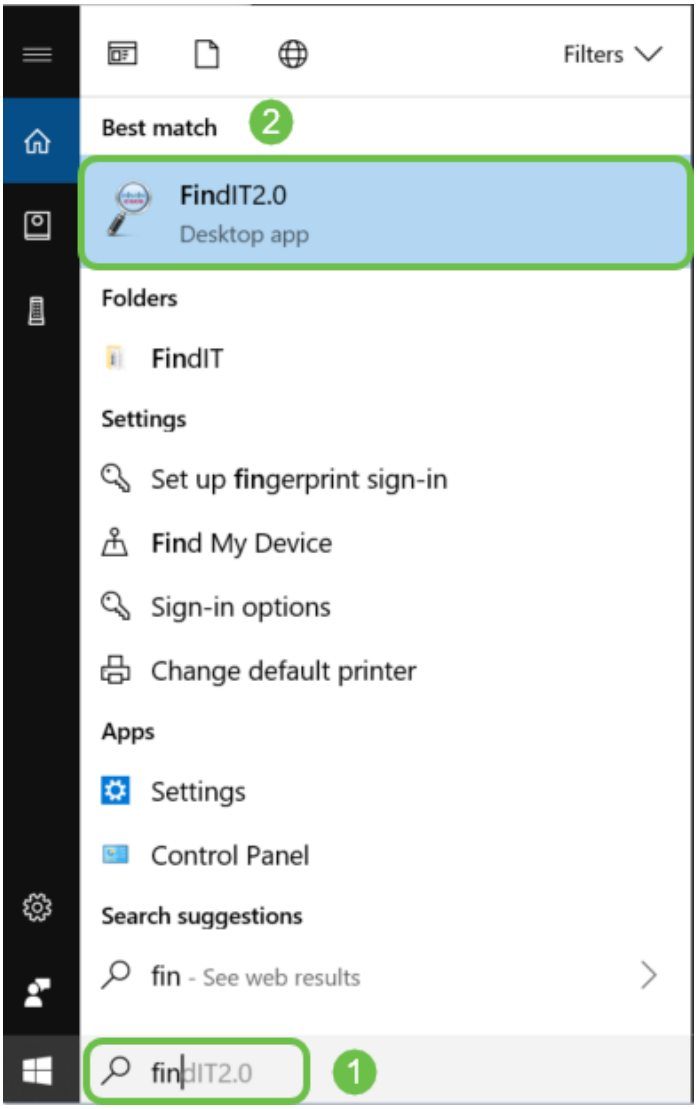
자세한 내용을 확인하고 Cisco Small Business FindIT Network Discovery Utility를 다운로드하려면 클릭하십시오.

이 링크를 클릭하여 Cisco FindIT Network Discovery Utility 설치 및 설정 방법에 대한 기사를 읽습니다.

응용 프로그램은 Windows 10의 경우 다음과 같습니다.



다운로드가 완료되면 Windows 10에서 찾을 수 있습니다.



AnyConnect(RV34x series 라우터/VPN)

이 VPN은 RV34x 시리즈 라우터(및 엔터프라이즈/대규모 기업 장비)와 함께 사용됩니다. Cisco AnyConnect Secure Mobility Client는 원격 사용자에게 보안 VPN 연결을 제공합니다. 원격 최종 사용자에게 Cisco SSL(Secure Sockets Layer) VPN 클라이언트의 이점을 제공하며 브라우저 기반 SSL VPN 연결에서는 사용할 수 없는 애플리케이션 및 기능도 지원합니다. 원격 근무자가 일반적으로 사용하는 AnyConnect를 사용하면 마치 사무실에 물리적으로 있는 것처럼 회사 컴퓨터 인프라에 연결할 수 있습니다. 이를 통해 직원들의 유연성, 이동성 및 생산성이 향상됩니다. AnyConnect를 사용하려면 클라이언트 라이센스가 필요합니다. Cisco AnyConnect는 다음 운영 체제와 호환됩니다. Windows 7, 8, 8.1 및 10, Mac OS X 10.8 이상 및 Linux Intel(x64).

자세한 지침은 다음 문서를 참조하십시오.

- Windows 컴퓨터에 Cisco AnyConnect Secure Mobility Client 설치
- Mac 컴퓨터에 Cisco AnyConnect Secure Mobility Client 설치

데이터 교환의 기본 사항

패킷

네트워킹에서 정보는 패킷이라고 하는 청크로 전송됩니다. 연결 문제가 있으면 패킷이 손실될 수 있습니다.

레이턴시

패킷 전송 지연

이중화

네트워크에서 리던던시가 구성되어 네트워크의 일부에 문제가 있는 경우 전체 네트워크가 실패하지 않습니다. 기본 컨피그레이션에 문제가 발생할 경우 이를 백업 계획으로 간주합니다.

프로토콜

통신하려면 두 장치에 동일한 설정 중 일부가 있어야 합니다. 언어라고 생각해 한 사람이 독일어만 말하고 다른 사람은 스페인어만 말하면, 그들은 의사소통을 할 수 없을 것입니다. 서로 다른 프로토콜이 함께 작동하며 서로 간에 여러 프로토콜이 전송될 수 있습니다. 프로토콜의 용도는 다릅니다. 다음은 몇 가지 예시이며 아래에 간략하게 설명되어 있습니다.

주소 지정 프로토콜

- **SIP(Session Initiation Protocol):** 인터넷을 통해 통신하는 VoIP(Voice over IP)의 기본 프로토콜입니다. VoIP를 통한 통신을 시작하기 위해 둘 다 SIP가 필요하도록 동일한 프로토콜을 사용하여 통신해야 합니다.
- **DHCP(Dynamic Host Configuration Protocol)**는 사용 가능한 IP 주소의 풀을 관리하며, 네트워크에 연결될 때 호스트에 할당합니다.
- **ARP(Address Resolution Protocol)**: 동적 IP 주소를 LAN의 영구 물리적 MAC 주소에 매핑합니다.
- **IPv4:** 현재 사용되는 IP의 가장 일반적인 버전입니다. IP 주소는 4개의 숫자 집합(8진수)으로 작성되며 각 집합 간의 마침표로 구분됩니다. 각 집합은 0에서 255 사이의 숫자일 수 있습니다. IPv4 주소의 예는 Google의 공용 DNS 서버인 8.8.8.8입니다. IPv4의 고유 IP 주소보다 많은 디바이스가 있으므로 영구 공용 IP 주소를 구입하는 데 많은 비용이 들 수 있습니다.
- **IPv6:** 이 최신 버전은 각 집합 사이에 콜론이 있는 8개의 숫자 집합을 사용합니다. 16진수 숫자 시스템을 사용하므로 IP 주소에 문자가 있을 수 있습니다. 기업은 IPv4 및 IPv6 주소를 동시에 실행할 수 있습니다.

IPv6에 대해 얘기하므로 이 주소 지정 프로토콜에 대해 몇 가지 중요한 정보를 살펴보겠습니다.

IPv6 약어: 여러 세트의 모든 숫자가 0이면 행에 있는 콜론 2개가 해당 집합을 나타낼 수 있으며 이 약어는 한 번만 사용할 수 있습니다. 예를 들어 Google의 IPv6 IP 주소 중 하나는 2001:4860:4860::8888입니다. 일부 디바이스는 IPv6 주소의 8개 부분 모두에 대해 별도의 필드를 사용하며 IPv6 약어를 사용할 수 없습니다. 그러한 경우 2001:4860:4860:0:0:0:0:888을 입력합니다.

16진수: 10이 아닌 16을 사용하는 숫자 시스템입니다. 이것이 우리가 일상적인 수학에서 사용하는 것입니다. 0-9의 숫자는 동일하게 표시됩니다. 10-15는 A-F로 표시됩니다.

데이터 전송 프로토콜

- **TCP(Transmission Control Protocol) 및 UDP(User Datagram Protocol):** 데이터가 전송되는 두 가지 방법입니다. TCP는 데이터를 전송하기 전에 3방향 핸드셰이크라는 연결이 필요하므로 지연이 발생할 수 있습니다. 데이터(패킷)가 손실되면 다시 전송됩니다. UDP는 안정성이 낮지만 속도가 빠릅니다. 음성 및 비디오는 UDP를 사용하는 경우가 많습니다.
- **FTP(File Transfer Protocol):** 이 프로토콜은 클라이언트에서 서버로 파일을 전송하는 데 사용됩니다.
- **HTTP(Hypertext Transfer Protocol)와 HTTPS(Hypertext Transfer Protocol Secure):** 인터넷을 통한 데이터 통신을 위한 일반적인 기준입니다. 웹 사이트의 시작 부분에 http:// 및 *https://*으로 *작성되어* 있습니다. https://으로 시작하는 사이트는 더 안전하게 사용할 수 있습니다.
- **RIP(Routing Information Protocol):** 이 프로토콜은 오랫동안 사용되어 왔습니다. 세 가지 버전이 있으며 각 버전마다 보안 및 기능이 추가됩니다. 라우터는 서로 경로를 공유합니다. 이 라우터의 목표는 한 라우터에서 다음 라우터로 최대 "홉의 수를 설정하여 루프를 방지하는 것입니다. 더 효율적인 라우팅 프로토콜로는 EIGRP**(Enhanced Interior Gateway Routing Protocol)**, OSPF**(Open Shortest Path First)** 및 IS**-IS(Intermediate System to Intermediate System)가 있습니다**. 이 세 가지 스케일은 RIP보다 우수하지만 설정하기가 더 복잡할 수 있습니다.
- **SSH(Secure Shell):** 명령줄 트래픽에 대해 안전한 경로를 제공하는 보안 채널입니다. 원격 서버와 통신하는 데 사용되는 암호화된 프로토콜입니다. SSH를 중심으로 다양한 추가 기술이 구축됩니다.

검색 프로토콜

- **Cisco CDP(Discovery Protocol):** 직접 연결된 다른 Cisco 장비에 대한 정보를 검색하고 해당 정보를 저장합니다. **Bonjour** 및 **LLDP(Link Layer Discovery Protocol)**는 동일한 기능을 수행하고 비 Cisco 장치에 대한 정보도 얻을 수 있습니다. 대부분의 소규모 비즈니스 디바이스는 LLDP를 사용합니다.
- **LLDP(Layer Link Discovery Protocol):** 디바이스가 식별, 구성 및 기능을 인접 디바이스에 광고한 다음 데이터를 MIB(Management Information Base)에 저장할 수 있도록 합니다. 인접 디바이스 간에 공유되는 정보는 LAN(Local Area Network)에 새 디바이스를 추가하는 데 필요한 시간을 단축하고 많은 컨피그레이션 문제를 해결하는 데 필요한 세부 정보를 제공합니다. LLDP는 Cisco 독점 제품이 아닌 장치와 Cisco 독점 장치가 아닌 장치 간에 작업해야 하는 경우에 사용할 수 있습니다. 이 스위치는 포트의 현재 LLDP 상태에 대한 모든 정보를 제공하며 이 정보를 사용하여 네트워크 내의 연결 문제를 해결할 수 있습니다. 이는 네트워크에서 디바이스를 검색하기 위해 FindIT Network Management와 같은 네트워크 검색 애플리케이션에서 사용하는 프로토콜 중 하나입니다.

프로토콜 식별

- **DNS(Domain Name System):** IP 주소에 FQDN(Fully Qualified Domain Name)이 할당되면 데이터베이스에 저장됩니다. 예를 들어, www.google.com을 검색하면 웹 사이트 이름을 입력할 수 있으며, 데이터베이스는 웹 사이트 이름을 검색하여 해당 IP 주소를 통해 해당 웹 사이트를 찾을 수 있습니다. **ISP(인터넷 서비스 공급자)는** DNS 서버를 기본값으로

사용하며 이미 구성되었습니다. 그러나 인터넷을 사용할 때 속도가 느린 경우 이를 수동으로 변경할 수 있습니다.

- **동적 DNS:** DDNS라고도 하며 호스트 이름, 주소 또는 기타 관련 정보의 활성 컨피그레이션으로 DNS의 서버를 자동으로 업데이트합니다. 즉, DDNS는 고정 도메인 이름을 동적 WAN IP 주소에 할당합니다. 이렇게 하면 영구 IP 주소 구매 비용이 절감됩니다.
- **IP(인터넷 프로토콜):** IP 주소는 인터넷에서 호스트 간에 데이터를 보내고 받을 수 있도록 하는 고유한 식별자입니다. 이는 ISP에서 구매해야 하는 공용 인터넷 주소를 통해 이루어집니다.
- **미디어 액세스 제어(MAC 주소):** 각 디바이스에는 고유한 식별자가 연결되어 있습니다. 이는 변경되지 않습니다. 네트워크 설정 및 문제 해결 시 MAC 주소를 아는 것이 좋습니다. 일반적으로 장치에 있으며 문자와 숫자를 포함합니다. 스위치는 디바이스의 MAC 주소를 추적하고 MAC 주소 테이블을 생성합니다.

문제 해결 프로토콜

- **Ping:** ping은 일반적인 문제 해결 방법입니다. ping은 IP 주소로 ICMP 에코 메시지를 전송합니다. 답례로 메시지가 수신됩니다. 응답에 성공하면 양방향 물리적 연결이 표시됩니다. 네트워크 데이터 패킷을 문제 없이 주소에 배포할 수 있는지 여부를 확인하는 방법입니다.
- **ICMP(Internet Control Message Protocol):** 오류 및 운영 정보에 대한 메시지입니다. PING 테스트를 수행하면 ICMP 에코 메시지가 대상으로 전송됩니다. 연결에 성공하면 해당 디바이스에서 응답이 전송됩니다.

서버

다른 컴퓨터에 서비스를 제공하는 컴퓨터의 컴퓨터 또는 프로그램. 서버는 가상 또는 애플리케이션일 수 있습니다. 하나의 디바이스에 여러 서버가 있을 수 있습니다. 서버는 서로 공유할 수 있습니다. Windows, Mac 또는 Linux에서 사용할 수 있습니다.

웹 서버 - 웹 브라우저의 웹 페이지 형식 및 표시
파일 서버 - 파일 및 폴더를 네트워크의 사용자에게 공유
이메일 서버 - 이메일 전송, 수신 및 저장
DNS 서버 - www.cisco.com과 같은 사용자 친화적인 이름을 IP 주소 173.37.145.84으로 변환합니다. 예:
인스턴트 메시징 서버 - 인스턴트 메시지의 흐름을 제어하고 관리(Jabber, Skype)

QoS(Quality of Service)

이러한 설정은 패킷(데이터) 지연이 있을 때 가장 잘 인식되기 때문에 일반적으로 음성 또는 비디오의 네트워크 트래픽에 우선 순위가 부여되도록 구성됩니다.

인터넷 연결의 기본 사항

인터넷 서비스 공급자(ISP)

네트워크에서 인터넷에 액세스하려면 ISP가 필요합니다. 연결 속도 및 비즈니스 요구 사항에 맞는 다양한 가격 중에서 선택할 수 있는 다양한 옵션이 있습니다. 인터넷 액세

스 외에도 ISP는 이메일, 웹 페이지 호스팅 등을 제공합니다.

웹 브라우저

디바이스에 제공되는 애플리케이션입니다. 다운로드할 수 있는 다른 항목이 있습니다. 다운로드가 완료되면 인터넷을 통해 이동할 IP 주소 또는 웹 사이트를 열고 입력할 수 있습니다. 웹 브라우저의 몇 가지 예는 다음과 같습니다.

Microsoft 에지

 ,

크롬

 ,

Firefox

 ,

Safari를 제공합니다.

 .

다른 항목을 열 수 없거나 다른 탐색 문제가 있는 경우 다른 웹 브라우저를 열고 다시 시도할 수 있습니다.

Uniform Resource Locator(URL)

웹 브라우저에서 일반적으로 액세스하려는 웹 사이트의 이름(URL, 웹 주소)을 입력합니다. 모든 URL은 고유해야 합니다. URL의 예는 https://www.cisco.com입니다.

기본 게이트웨이

로컬 영역 네트워크 트래픽이 ISP(인터넷 서비스 공급자)와 인터넷에 대한 이그레스(egress)로 사용하는 라우터입니다. 다시 말해, 이 라우터는 건물 외부 및 인터넷을 통해 다른 장치와 연결됩니다.

방화벽

방화벽은 수신 및 발신 네트워크 트래픽을 모니터링하고 ACL(Access Control Lists)이라는 정의된 보안 규칙 집합을 기반으로 특정 트래픽을 허용할지 아니면 차단할지를 결정하는 네트워크 보안 디바이스입니다.

방화벽은 수십 년 동안 네트워크 보안 분야의 1차 방어선이었습니다. 보안과 제어된 내부 네트워크 간의 장벽을 설정하며, 이는 인터넷과 같은 외부 네트워크의 신뢰와 신뢰할 수 없습니다.

방화벽은 하드웨어, 소프트웨어 또는 둘 다일 수 있습니다.

자세한 내용은 RV34x Series Router의 Configure Basic Firewall Settings(기본 방화벽 설정 구성)를 참조하십시오.

Access control lists (ACLs)

특정 사용자에게 트래픽을 보내거나 받는 것을 차단하거나 허용하는 목록을 표시합니다. 액세스 규칙은 항상 적용되도록 구성하거나 정의된 일정에 따라 구성할 수 있습니다. 액세스 규칙은 네트워크에 대한 액세스를 허용하거나 거부하기 위해 다양한 기준에 따라 구성됩니다. 액세스 규칙은 액세스 규칙을 라우터에 적용해야 하는 시간을 기반으로 예약됩니다. 보안 또는 방화벽 설정에서 설정합니다. 예를 들어, 비즈니스는 업무 시간 중에 직원들이 라이브 스포츠 스트리밍을 하거나 Facebook에 연결하는 것을 차단할 수 있습니다.

대역폭

특정 기간 동안 한 지점에서 다른 지점으로 전송할 수 있는 데이터의 양입니다. 인터넷 연결이 더 큰 대역폭과 연결되어 있으면 네트워크가 더 낮은 대역폭과 인터넷 연결보다 훨씬 빠르게 데이터를 이동할 수 있습니다. 스트리밍 비디오는 파일을 전송하는 것보다 훨씬 많은 대역폭을 사용합니다. 웹 페이지에 액세스할 때 지연이 있거나 비디오 스트리밍이 지연되는 경우 네트워크의 대역폭을 늘려야 할 수 있습니다.

이더넷 케이블

네트워크의 대부분의 디바이스에는 이더넷 포트가 있습니다. 이더넷 케이블은 유선 연결을 위해 연결되는 케이블입니다. RJ45 케이블의 양쪽 끝은 동일하며 기존 전화 잭과 같습니다. 장치를 연결하고 인터넷에 연결하는 데 사용할 수 있습니다. 이 케이블은 인터넷 액세스 및 파일 공유를 위해 장치를 연결합니다. 일부 컴퓨터는 이더넷 포트를 제공하지 않을 수 있으므로 이더넷 어댑터가 필요합니다.

네트워크 및 그 구성 방식

LAN(Local Area Network)

몇 개의 건물이나 가정처럼 작은 네트워크입니다. LAN에 연결된 모든 사용자가 동일한 물리적 위치에 있으며 동일한 라우터에 연결됩니다.

로컬 네트워크에서는 각 디바이스에 고유한 내부 IP 주소가 할당됩니다. 10.x.x.x, 172.16.x.x - 172.31.x.x 또는 192.168.x.x 패턴을 따릅니다. 이러한 주소는 네트워크 내부에서만, 디바이스 간에만 표시되며, 비공개로 간주됩니다. 비즈니스와 동일한 내부 IP 주소 풀을 가질 수 있는 위치는 수백만 개에 달합니다. 상관없습니다. 자체 프라이빗 네트워크 내에서만 사용되므로 충돌이 없습니다. 네트워크의 디바이스가 서로 통신하려면, 모든 디바이스가 다른 디바이스와 동일한 패턴을 따르고 동일한 서브넷에 있어야 하며 고유해야 합니다. 이 패턴에서 이러한 주소는 사설 LAN 주소에만 예약되므로 공용 IP 주소로 표시해서는 안 됩니다.

이러한 모든 디바이스는 기본 게이트웨이(라우터)를 통해 데이터를 전송하여 인터넷으로 이동합니다. 기본 게이트웨이가 정보를 수신하면 NAT(Network Address Translation)를 수행하고, 인터넷을 통해 전송되는 모든 항목에 고유한 IP 주소가 필요하므로 IP 주소를 변경해야 합니다.

WAN(Wide Area Network)

WAN(Wide Area Network)은 전 세계적으로 분산되는 네트워크입니다. 많은 LAN이 단일 WAN에 연결할 수 있습니다.

WAN 주소만 인터넷을 통해 서로 통신할 수 있습니다. 각 WAN 주소는 고유해야 합니다. 네트워크 내부의 디바이스에서 인터넷을 통해 정보를 보내고 받으려면 NAT를 수행할 수 있는 라우터(기본 게이트웨이)가 네트워크 에지에 있어야 합니다.

RV34x Series Router에서 Configure Access Rules(액세스 규칙 구성)를 읽으려면 클릭합니다.

NAT(Network Address Translation)

라우터는 ISP(인터넷 서비스 공급자)를 통해 WAN 주소를 수신합니다. 라우터는 네트워크에서 나가는 트래픽을 가져오는 NAT 기능과 함께 제공되며, 사설 주소를 공용 WAN 주소로 변환하고 인터넷을 통해 전송합니다. 트래픽을 수신할 때 역순으로 수행합니다. 이 설정은 전 세계 모든 장치에 사용할 수 있는 영구 IPv4 주소가 충분하지 않기 때문에 설정되었습니다.

NAT의 장점은 하나의 고유한 공용 IP 주소 뒤에 전체 내부 네트워크를 효과적으로 숨겨 추가적인 보안을 제공한다는 것입니다. 내부 IP 주소는 항상 동일하게 유지되지만, 플러그를 뽑았거나, 특정 방법으로 구성하거나, 공장 기본값으로 재설정할 경우 그렇지 않을 수 있습니다.

고정 NAT

라우터에서 고정 DHCP(Dynamic Host Configuration Protocol)를 구성하여 내부 IP 주소를 동일하게 유지할 수 있습니다. ISP를 통해 고정 공용 IP 주소를 보유하도록 비용을 지불하지 않는 한 공용 IP 주소는 동일하게 유지되지 않습니다. 많은 기업이 이 서비스에 비용을 지불하므로 직원과 고객이 서버(웹, 메일, VPN 등)에 보다 안정적인 연결을 제공하지만 비용이 많이 들 수 있습니다.

고정 NAT는 프라이빗 IP 주소의 일대일 변환을 공용 IP 주소에 매핑합니다. 공용 주소에

대한 전용 주소의 고정 변환을 생성합니다. 즉, 동일한 양의 공용 주소가 전용 주소로 필요합니다. 이는 네트워크 외부에서 디바이스에 액세스해야 하는 경우에 유용합니다.

RV160 및 RV260에서 Configuring NAT and Static NAT를 읽으려면 클릭합니다.

CGNAT

Carrier Grade NAT는 여러 클라이언트가 동일한 IP 주소를 사용할 수 있도록 하는 유사한 프로토콜입니다.

VLAN

VLAN(Virtual Local Area Network)을 사용하면 LAN(Local Area Network)을 서로 다른 브로드캐스트 도메인으로 논리적으로 분할할 수 있습니다. 네트워크에서 민감한 데이터를 브로드캐스트할 수 있는 시나리오에서는 특정 VLAN에 브로드캐스트를 지정하여 보안을 강화하기 위해 VLAN을 생성할 수 있습니다. VLAN에 속하는 사용자만 해당 VLAN의 데이터에 액세스하고 조작할 수 있습니다. 또한 VLAN을 사용하여 불필요한 대상으로 브로드캐스트 및 멀티캐스트를 보낼 필요가 없으므로 성능을 높일 수 있습니다.

VLAN은 주로 호스트의 물리적 위치에 관계없이 호스트 간에 그룹을 구성하는 데 사용됩니다. 따라서 VLAN은 호스트 간의 그룹 구성을 통해 보안을 개선합니다. VLAN이 생성되면 해당 VLAN이 하나 이상의 포트에 수동 또는 동적으로 연결될 때까지 효과가 없습니다. VLAN을 설정하는 가장 일반적인 이유 중 하나는 음성에 대해 별도의 VLAN을 설정하고 데이터에 대해 별도의 VLAN을 설정하는 것입니다. 이렇게 하면 동일한 네트워크를 사용하더라도 두 데이터 유형 모두에 대해 패킷을 전달합니다.

자세한 내용은 Cisco Business Router용 VLAN 모범 사례 및 보안 팁을 참조하십시오.

하위 네트워크

서브넷, 하위 네트워크는 IP 네트워크 내부에 독립적인 네트워크입니다.

SSID

SSID(Service Set Identifier)는 무선 클라이언트가 무선 네트워크의 모든 장치에 연결하거나 공유할 수 있는 고유한 식별자입니다. 대/소문자를 구분하며 32자의 영숫자를 초과할 수 없습니다. 무선 네트워크 이름이라고도 합니다.

가상 사설망(VPN)

기술은 발전했고 사무실 밖에서도 종종 비즈니스를 수행합니다. 모바일 장치가 더 많아지고 직원들은 종종 집에서 또는 이동 중에 업무를 수행합니다. 이로 인해 일부 보안 취약성이 발생할 수 있습니다. VPN(Virtual Private Network)은 네트워크의 원격 작업자를 안전한 방법으로 연결하는 좋은 방법입니다. VPN을 사용하면 원격 호스트가 동일한 로컬 네트워크에 있는 것처럼 작동할 수 있습니다.

보안 데이터 전송을 제공하도록 VPN이 설정되었습니다. VPN을 설정하고 데이터를 암

호화하는 방법에는 여러 옵션이 있습니다. VPN은 SSL(Secure Sockets Layer), PPTP(Point to Point Tunneling Protocol) 및 Layer Two Tunneling Protocol을 사용합니다.

VPN 연결을 통해 사용자는 인터넷과 같은 공용 또는 공유 네트워크를 통해 사설 네트워크에 액세스하고 데이터를 보내고 받을 수 있지만 사설 네트워크와 해당 리소스를 보호하기 위해 기본 네트워크 인프라에 안전하게 연결할 수 있습니다.

VPN 터널은 암호화 및 인증을 사용하여 데이터를 안전하게 전송할 수 있는 사설 네트워크를 설정합니다. 회사 사무실은 직원들이 사무실 외부에 있더라도 개인 네트워크에 액세스할 수 있도록 하는 것이 유용하고 필요하기 때문에 VPN 연결을 주로 사용합니다.

라우터가 인터넷 연결을 위해 구성된 후 라우터와 엔드포인트 간에 VPN 연결을 설정할 수 있습니다. VPN 클라이언트는 연결을 설정할 수 있도록 VPN 라우터의 설정에 전적으로 의존합니다.

VPN은 게이트웨이 간 터널을 위해 사이트 간 VPN을 지원합니다. 예를 들어, 사용자가 지사 사이트에서 기업 사이트의 라우터에 연결하도록 지사 사이트의 VPN 터널을 구성하여 지사 사이트가 기업 네트워크에 안전하게 액세스할 수 있도록 할 수 있습니다. 사이트 간 VPN 연결에서는 누구나 통신을 시작할 수 있습니다. 이 컨피그레이션에는 지속적인 암호화 연결이 있습니다.

IPsec VPN은 호스트-게이트웨이 터널에 대해 클라이언트-서버 VPN도 지원합니다. 클라이언트-서버 VPN은 VPN 서버를 통해 랩톱/PC에서 기업 네트워크로 연결할 때 유용합니다. 이 경우 클라이언트만 연결을 시작할 수 있습니다.

Cisco Business VPN Overview and Best Practices(Cisco 비즈니스 VPN 개요 및 모범 사례)를 읽으려면 클릭하십시오.

인증서

VPN 설정의 보안 단계는 CA(Certificate Authority)에서 인증서를 가져오는 것입니다. 인증에 사용됩니다. 인증서는 다양한 서드파티 사이트에서 구매합니다. 이는 귀하의 사이트가 안전하다는 것을 증명하는 공식적인 방법입니다. 기본적으로 CA는 신뢰할 수 있는 소스이며, 사용자가 합법적인 비즈니스인지 확인하고 신뢰할 수 있는지 확인합니다. VPN의 경우 최소 비용으로 더 낮은 수준의 인증서만 있으면 됩니다. CA에서 체크 아웃한 후, 해당 정보가 확인되면 사용자에게 인증서를 발급합니다. 이 인증서는 컴퓨터에서 파일로 다운로드할 수 있습니다. 그런 다음 라우터(또는 VPN 서버)로 이동하여 업로드할 수 있습니다.

일반적으로 클라이언트는 VPN을 사용하기 위해 인증서가 필요하지 않습니다. 이는 라우터를 통한 확인을 위한 것입니다. 이에 대한 예외는 클라이언트 인증서가 필요한 OpenVPN입니다.

많은 중소기업에서는 간소화를 위해 인증서 대신 비밀번호 또는 사전 공유 키를 사용하도록 선택합니다. 이는 보안이 덜 되지만 무료로 설정할 수 있습니다.

이 주제에 대한 몇 가지 기사:

- RV160 및 RV260 Series 라우터의 인증서(CSR 가져오기/내보내기/생성)
- RV34x Series 라우터에서 기본 자체 서명 인증서를 타사 SSL 인증서로 교체
- RV34x Series 라우터의 인증서 관리

사전 공유 키(PSK)

이는 VPN 구성 전에 결정 및 공유되는 공유 비밀번호로, 인증서를 사용하기 위한 대체 비밀번호로 사용할 수 있습니다. PSK는 원하는 대로 구성할 수 있으며, PSK는 컴퓨터에서 클라이언트로 설정할 때 사이트 및 클라이언트와 일치해야 합니다. 디바이스에 따라 사용할 수 없는 기호가 있을 수 있습니다.

키 수명

시스템이 키를 변경하는 빈도. 이 설정은 원격 라우터와 동일해야 합니다.

결론

이제 여러분이 길을 떠날 수 있는 많은 기본을 가지고 있습니다.

더 많은 것을 배우고 싶다면, 이 링크를 확인하십시오!

고정 IP 주소 설정을 위한 모범 사례 Cisco Business VPN 개요 및 모범 사례 Cisco 비즈니스 라우터에 대한 VLAN 모범 사례 및 보안 팁 인터넷 백업 - Windows 인터넷 백업 - Mac 스위치에 로그인하는 방법