Neu bei Cisco Business: Geräte- und grundlegende Netzwerkglossare

Ziel

Dieses Dokument soll Anfängern die Cisco Small Business-Geräte und einige allgemeine Begriffe näher bringen. Zu den Themen gehören verfügbare Hardware, Cisco Geschäftsbedingungen, allgemeine Netzwerkbegriffe, Cisco Tools, Grundlagen des Datenaustauschs, Grundlagen einer Internetverbindung und Netzwerke sowie deren Zusammenspiel.

Einleitung

Möchten Sie Ihr Netzwerk gerade mit Cisco Geräten einrichten? Es kann überwältigend sein, in die neue Welt der Einrichtung und Wartung eines Netzwerks einzutreten. Dieser Artikel soll Ihnen helfen, einige der Grundlagen kennen zu lernen. Je mehr Sie wissen, desto weniger einschüchternd wird es sein!

Hardware von Cisco

Router

Router verbinden mehrere Netzwerke miteinander und leiten Daten dorthin weiter, wo sie benötigt werden. Sie verbinden auch Computer in diesen Netzwerken mit dem Internet. Router ermöglichen es allen vernetzten Computern, eine einzige Internetverbindung zu nutzen, was Geld spart.

Ein Router fungiert als Dispatcher. Es analysiert Daten, die über ein Netzwerk gesendet werden, wählt die beste Route für Daten aus, die übertragen werden soll, und sendet sie auf dem Weg.

Router verbinden Ihr Unternehmen mit der Welt, schützen Informationen vor Sicherheitsbedrohungen und können sogar entscheiden, welche Computer Vorrang vor anderen erhalten.

Neben diesen grundlegenden Netzwerkfunktionen bieten Router zusätzliche Funktionen, die das Netzwerk einfacher oder sicherer machen. Je nach Ihren Anforderungen können Sie beispielsweise einen Router mit Firewall, einem Virtual Private Network (VPN) oder einem Internet Protocol (IP)-Kommunikationssystem auswählen.

Zu den neuesten Cisco Business-Routern gehören die Serien RV160, RV260, RV340 und RV345.

Switch

Switches bilden die Grundlage der meisten Unternehmensnetzwerke. Ein Switch fungiert als Controller, der Computer, Drucker und Server mit einem Netzwerk in einem Gebäude oder auf einem Campus verbindet.

Mit Switches können Geräte im Netzwerk miteinander und mit anderen Netzwerken kommunizieren, wodurch ein Netzwerk aus gemeinsam genutzten Ressourcen entsteht. Durch den Austausch von Informationen und die Ressourcenzuweisung sparen Switches Kosten und steigern die Produktivität.

Sie können zwischen zwei grundlegenden Switches wählen: verwaltet und nicht verwaltet.

> Ein Unmanaged Switch ist sofort einsatzbereit, kann aber nicht konfiguriert werden. Heimnetzwerkgeräte bieten in der Regel unverwaltete Switches an.
> Ein verwalteter Switch kann konfiguriert werden. Sie können einen Managed Switch lokal oder remote überwachen und anpassen, wodurch Sie eine bessere Kontrolle über Netzwerkverkehr und -zugriff erhalten.

Weitere Informationen zu Switches finden Sie im Begriffserläuterungen für Switches.

Zu den neuesten Switches gehören die Cisco Business Switches der Serien CBS 110, CBS 220, CBS 250 und CBS 350.

Wenn Sie mehr über die Unterschiede zwischen den CBS-Switches erfahren möchten, sehen Sie sich die folgenden Seiten an:

Wireless Access Point

Mit einem Wireless Access Point können Geräte ohne Kabel eine Verbindung zum Wireless-Netzwerk herstellen. Ein Wireless-Netzwerk vereinfacht die Online-Bereitstellung neuer Geräte und bietet flexible Unterstützung für mobile Mitarbeiter.

Ein Access Point fungiert als Verstärker für Ihr Netzwerk. Während ein Router die

Bandbreite bereitstellt, erweitert ein Access Point diese Bandbreite, sodass das Netzwerk viele Geräte unterstützen kann und diese Geräte von weiter entfernt auf das Netzwerk zugreifen können.

Ein Access Point kann jedoch mehr leisten, als nur Wi-Fi zu erweitern. Darüber hinaus können nützliche Daten zu den Geräten im Netzwerk bereitgestellt, proaktive Sicherheit gewährleistet und andere praktische Zwecke genutzt werden.

Zu den neuesten Wireless Access Points, Cisco Business Wireless, gehören die Modelle AC140, AC145 und AC240, die ein Wireless Mesh-Netzwerk ermöglichen. Wenn Sie mit vermaschten Wireless-Netzwerken nicht vertraut sind, finden Sie weitere Informationen in Welcome to Cisco Business Wireless Mesh Networking oder Frequently Asked Questions (FAQ) for a Cisco Business Wireless Network.

Wenn Sie einige Begriffe erfahren möchten, die in Wireless Access Points üblich sind, lesen Sie das WAP-Glossar der Begriffe.

Multiplattform-Telefon

MPP-Telefone ermöglichen die VoIP-Kommunikation (Voice over IP) über das Session Initiation Protocol (SIP). Dadurch entfällt die Notwendigkeit herkömmlicher Telefonleitungen, wodurch Telefone innerhalb des Unternehmens leichter tragbar werden. Bei VoIP verwendet ein Telefon eine vorhandene Netzwerkinfrastruktur und eine Internetverbindung anstelle kostspieliger T1-Leitungen. So können mehr Anrufe mit weniger Leitungen verwaltet werden. Weitere nützliche Optionen sind Halten von Anrufen, Parken von Anrufen, Weiterleiten von Anrufen und vieles mehr. Einige Modelle ermöglichen zusätzlich zu VoIP auch die Videokommunikation.

MPP-Telefone sind so konzipiert, dass sie wie ein normales Telefon aussehen und nur zu diesem Zweck verwendet werden. Sie sind jedoch im Wesentlichen ein Computer und Teil Ihres Netzwerks. MPP-Telefone benötigen entweder einen Service von einem Internettelefonie-Service-Provider (ITSP) oder einem IP Private Branch Exchange (PBX)-Anrufsteuerungsserver. WebEx Anrufe, Ring Central und Verizon sind Beispiele für einen ITSP. Beispiele für IP-PBX-Dienste, die mit Cisco MPP-Telefonen verwendet werden, sind Asterisk, Centile und Metaswitch-Plattformen. Viele Funktionen auf diesen Telefonen werden speziell von Drittanbietern programmiert (z. B. FreePBX), sodass die Prozesse (Parken, Zugriff auf Voicemail usw.) variieren können.

Zu den neuesten Cisco Business MPP-Telefonen zählen die Serien 6800, 7800 und 8800.

Häufig referenziert in Cisco Business

Administrationshandbuch und Schnellstartanleitung

Diese beiden Ressourcen können Sie durchsuchen, um detaillierte Informationen zu Ihrem Produkt und den Funktionen zu erhalten. Wenn Sie eine Website oder eine Websuche mit Ihrer Modellnummer durchführen, können Sie eine oder andere

hinzufügen, um diese längeren Leitfäden anzuzeigen.

Standardeinstellungen

Geräte werden mit vordefinierten Standardeinstellungen ausgeliefert. Sie sind häufig die gebräuchlichsten Einstellungen, die ein Administrator auswählen würde. Sie können die Einstellungen an Ihre Bedürfnisse anpassen.

Standard-Benutzername und -Kennwort

Bei älteren Cisco Business-Geräten war der Standardwert *admin* für Benutzername und Kennwort. Jetzt haben die meisten einen Standardwert von *cisco* für Benutzername und Kennwort. Auf VoIP-Telefonen müssen Sie sich als *Administrator* anmelden, um viele Konfigurationen zu ändern. Es wird dringend empfohlen, das Kennwort aus Sicherheitsgründen zu ändern, um es zu vereinfachen.

Standard-IP-Adressen

Die meisten Cisco Geräte sind mit Standard-IP-Adressen für Router, Switches und Wireless Access Points ausgestattet. Wenn Sie sich die IP-Adresse nicht merken können und keine spezielle Konfiguration haben, können Sie eine offene Büroklammer verwenden, um die Reset-Taste auf Ihrem Gerät für mindestens 10 Sekunden zu drücken. Dadurch werden die Standardeinstellungen zurückgesetzt. Wenn Ihr Switch oder WAP nicht mit einem Router mit aktiviertem DHCP verbunden ist und Sie direkt mit dem Switch oder WAP mit Ihrem Computer verbunden sind, sind dies die Standard-IP-Adressen.

Die Standard-IP-Adresse eines Cisco Business-Routers ist 192.168.1.1.
Die Standard-IP-Adresse für einen Cisco Business Switch ist 192.168.1.254.
Die Standard-IP-Adresse für einen Small Business Wireless Access Point (AP) lautet 192.168.1.245. Es gibt keine Standard-IP-Adresse für die neuen Mesh Wireless Access Points.

Auf Werkseinstellungen zurücksetzen

Es kann vorkommen, dass Sie Ihren Cisco Business Router, Switch oder Wireless Access Point auf die werkseitigen Standardeinstellungen zurücksetzen und von Grund auf neu starten möchten. Dies ist praktisch, wenn Sie die Geräte von einem Netzwerk in ein anderes verschieben oder wenn Sie ein Konfigurationsproblem nicht lösen können. Beim Zurücksetzen auf die Werkseinstellungen gehen alle Konfigurationen verloren.

Sie können Konfigurationen sichern, sodass Sie sie nach einem Zurücksetzen auf die Werkseinstellungen wiederherstellen können. Klicken Sie auf die folgenden Links, um weitere Informationen zu erhalten:

- Starten oder Wiederherstellen der werkseitigen Standardeinstellungen des Routers der Serie RV34x mithilfe des webbasierten Dienstprogramms

- Sichern und Wiederherstellen oder Austauschen der Firmware auf einem Switch
- Herunterladen, Sichern, Kopieren und Löschen von Konfigurationsdateien auf einem Wireless Access Point
- Verwalten der Konfigurationsdateien auf dem WAP125 oder WAP581 Access Point

Wenn Sie die Konfiguration nicht sichern, müssen Sie das Gerät von Grund auf neu einrichten. Achten Sie also darauf, dass Sie über die Verbindungsdetails verfügen. In den meisten Modellen gibt es einen Artikel, in dem die Schritte zum Zurücksetzen beschrieben werden. Am einfachsten ist es jedoch, eine offene Büroklammer zu verwenden und die Reset-Taste mindestens 10 Sekunden lang auf dem Gerät zu drücken. Dies gilt nicht für die MPP-Telefone. Weitere Informationen finden Sie unter Zurücksetzen eines Cisco IP-Telefons.

Webbenutzerschnittstelle (UI)

Alle Cisco Business-Geräte werden mit einer Web-Benutzeroberfläche geliefert, mit Ausnahme der Unmanaged Switches der Serie 100.

Diese Art von Benutzeroberfläche, die auf Ihrem Bildschirm angezeigt wird, zeigt Optionen zur Auswahl an. Sie müssen keine Befehle kennen, um durch diese Bildschirme zu navigieren. Die Webbenutzeroberfläche wird auch als grafische Benutzeroberfläche (Graphical User Interface, GUI), webbasierte Benutzeroberfläche, webbasierte Anleitung, webbasiertes Dienstprogramm oder webbasiertes Konfigurationsprogramm bezeichnet.

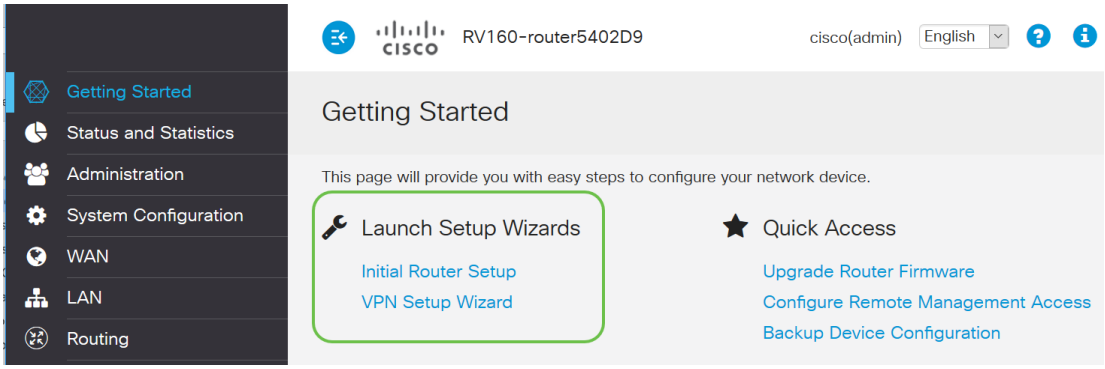
Eine der einfachsten Möglichkeiten, die Konfiguration eines Geräts zu ändern, ist die Webbenutzeroberfläche. Die Webbenutzeroberfläche stellt dem Administrator ein Tool zur Verfügung, das alle möglichen Features enthält, die geändert werden können, um die Leistung eines Geräts zu ändern.

Nachdem Sie sich bei einem Cisco Gerät angemeldet haben, wird ein Bildschirm für die Webbenutzeroberfläche mit einem Navigationsbereich links unten angezeigt. Sie enthält eine Liste der wichtigsten Funktionen des Geräts. Der Navigationsbereich wird manchmal auch als Navigationsbaum, Navigationsleiste oder Navigationskarte bezeichnet.

Die Farben dieser Seite und die Funktionen der obersten Ebene können je nach Gerät und Firmware-Version variieren.

Einrichtungsassistent

Dieser interaktive Bildschirm wird angezeigt, wenn Sie sich zum ersten Mal und möglicherweise danach bei einem Cisco Small Business-Gerät anmelden. So können Sie sich optimal auf Ihr Netzwerk konzentrieren. Es gibt mehrere vorgewählte Standardeinstellungen, die geändert werden können. Einige Geräte werden mit mehr als einem Installationsassistenten ausgeliefert. Dieses Beispiel zeigt zwei Setup-Assistenten, die *Ersteinrichtung des Routers* und den *VPN-Einrichtungsassistenten*.



Urheberrechtlich geschützt von Cisco

Speziell entwickelt und im Besitz von Cisco. Das Cisco Discovery Protocol (CDP) ist beispielsweise proprietär von Cisco. In der Regel können proprietäre Protokolle von Cisco nur auf Geräten von Cisco verwendet werden.

Modelle einer Serie

Cisco bietet kleinen und mittleren Unternehmen eine Vielzahl von Modellen, die auf die Bedürfnisse ihres Unternehmens zugeschnitten sind. Oft wird ein Modell mit verschiedenen Funktionen, einer Anzahl von Ports, Power over Ethernet oder sogar Wireless angeboten. Wenn eine Serie mehrere Modelle enthält, setzt Cisco ein x anstelle der Zahl oder des Buchstabens ein, die von Modell zu Modell variiert. Die Informationen gelten jedoch für alle Modelle dieser Serie. Beispielsweise werden die Router RV340 und RV345 in der Serie RV34x genannt. Wenn ein Gerät über einen PoE-Anschluss verfügt, wird PoE (Power over Ethernet) angeboten. Wenn ein Gerätename in W endet, bietet er Wireless-Funktionen. Im Allgemeinen gilt: Je höher die Anzahl der Modelle, desto höher sind die Funktionen des Geräts. Einzelheiten hierzu finden Sie in den folgenden Artikeln:

- Produkt-Decoder-Ring - Router
- Produkt-ID-Decoder - Switch
- Product Decoder Ring - WAP
- Cisco Business Wireless Model Decoder (Mesh Wireless)

Firmware

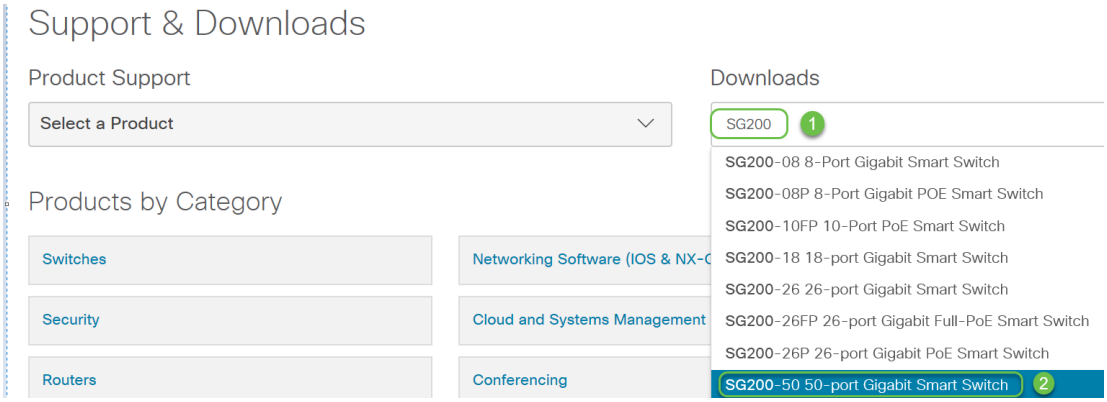
Wird auch als Bild bezeichnet. Das Programm, das die Vorgänge und Funktionen des Geräts steuert.

Firmware aktualisieren

Die Aktualisierung der Firmware ist für eine optimale Leistung auf jedem Gerät unerlässlich. Es ist sehr wichtig, Upgrades zu installieren, wenn sie veröffentlicht werden. Wenn Cisco ein Firmware-Upgrade veröffentlicht, enthält dies häufig Verbesserungen wie neue Funktionen oder die Behebung eines Fehlers, der eine Sicherheitslücke oder ein Leistungsproblem verursachen kann.

Rufen Sie den Cisco Support auf, und geben Sie unter *Downloads* den Namen des Geräts ein, das aktualisiert werden muss. Es sollte ein Dropdown-Menü angezeigt

werden. Blättern Sie nach unten, und wählen Sie das gewünschte Modell aus.



Tipp: Wenn Sie sich verschiedene Versionen der Cisco Firmware anschauen, folgt jeweils das Format x.x.x.x. die als vier Oktette gelten. Wenn eine kleine Aktualisierung vorliegt, ändert sich das vierte Oktett. Das dritte Oktett ändert sich, wenn es sich um eine größere Änderung handelt. Das zweite Oktett bedeutet eine große Veränderung. Das erste Oktett ändert sich, wenn es sich um eine vollständige Überarbeitung handelt.

Wenn Sie Hilfe benötigen, klicken Sie auf diesen Link, um Firmware auf jedem Gerät herunterzuladen und zu aktualisieren.

Dieser Artikel enthält einige Vorschläge zur Fehlerbehebung, falls Sie Probleme mit einem Switch-Upgrade haben: Firmware-Upgrade auf einem Switch der Serien 200 und 300.

Allgemeine Netzwerkbedingungen

Sobald Sie Ihre Geräte haben, sollten Sie sich mit einigen gebräuchlichen Begriffe im Netzwerkbereich vertraut machen.

Schnittstelle

Eine Schnittstelle ist normalerweise der Bereich zwischen einem System und einem anderen. Alles, was mit Ihrem Computer kommunizieren kann, einschließlich Ports. Eine Netzwerkschnittstelle wird in der Regel einer lokalen IP-Adresse zugewiesen. Über eine Benutzeroberfläche kann der Benutzer mit dem Betriebssystem interagieren.

Knoten

Ein allgemeiner Begriff, der jedes Gerät beschreibt, das eine Verbindung oder Interaktion innerhalb eines Netzwerks herstellt, Informationen sendet, empfängt und speichert, mit dem Internet kommuniziert und über eine IP-Adresse verfügt.

Host

Ein Host ist ein Gerät, das ein Endpunkt für die Kommunikation in einem Netzwerk ist. Der Host kann anderen Knoten Daten oder einen Dienst (z. B. DNS) bereitstellen. Je

nach Topologie kann ein Switch oder Router ein Host sein. Alle Hosts sind auch Knoten. Beispiele hierfür sind Computer, Server oder Drucker.

Computerprogramm

Ein Computerprogramm enthält Anweisungen, die auf einem Computer ausgeführt werden können.

Anwendung

Anwendungssoftware ist ein Programm, das Sie bei der Ausführung von Aufgaben unterstützt. Sie werden häufig als austauschbar bezeichnet, da sie ähnlich sind, aber nicht alle Programme sind Anwendungen.

Best Practices

Die empfohlene Methode für die Einrichtung und den Betrieb Ihres Netzwerks.

Topologie

Die physische Art der Verbindung Ihrer Geräte. Eine Netzwerkkarte.

Konfigurieren

Dies bezieht sich auf die Einrichtung der Dinge. Sie können die Standardeinstellungen beibehalten, die vorkonfiguriert werden, wenn Sie Geräte kaufen, oder Sie können sie für Ihre speziellen Anforderungen konfigurieren. Standardeinstellungen sind die grundlegenden, häufig empfohlenen Konfigurationen. Wenn Sie sich bei Ihrem Gerät anmelden, wird möglicherweise ein Setup-Assistent angezeigt, der Sie durch die erforderlichen Schritte führt.

MAC-Adresse

Eindeutige ID für jedes Gerät. befindet sich auf dem physischen Gerät und kann mit Bonjour, LLDP oder CDP erkannt werden. Ein Switch überwacht die MAC-Adressen auf Geräten, wenn er mit diesen interagiert, und erstellt eine MAC-Adresstabelle. Dadurch kann der Switch wissen, wohin Datenpakete weitergeleitet werden sollen.

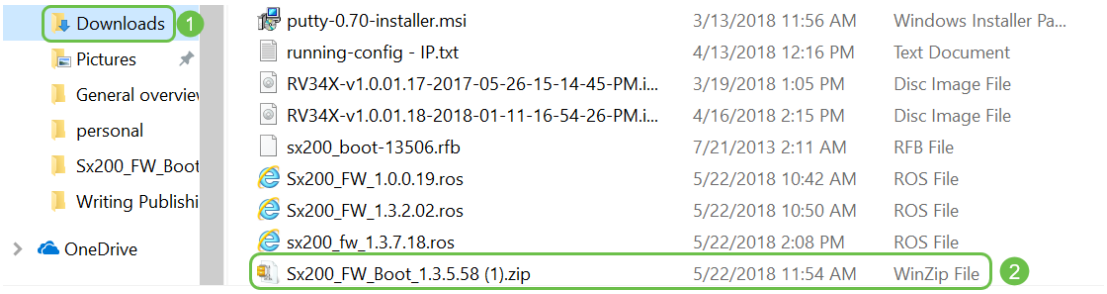
Open Source

Ein Programm, das der Öffentlichkeit kostenlos zur Verfügung steht.

Zip-Datei

Eine Gruppe von Dateien, die in einer ZIP-Datei komprimiert sind. Sie wird verwendet, wenn Sie mehrere Dateien in einem Schritt übertragen möchten. Der Empfänger kann die Zip-Datei öffnen und separat auf jede Datei zugreifen. Eine ZIP-Datei endet in *.zip*.

Wenn Sie eine Datei im Format *.zip* sehen, müssen Sie diese Datei entpacken. Wenn Sie kein Unzip-Programm haben, müssen Sie ein Programm herunterladen. Es gibt mehrere kostenlose Online-Optionen. Wenn Sie ein Entpackprogramm heruntergeladen haben, klicken Sie auf **Downloads** und suchen Sie die zu entpackende *.zip*-Datei.



Klicken Sie mit der rechten Maustaste auf den Namen der ZIP-Datei, ein ähnliches Fenster wird angezeigt. Bewegen Sie den Mauszeiger über die Entpacksoftware, und wählen Sie **Entpacken aus**. In diesem Beispiel wird 7-Zip verwendet.

Befehlszeilenschnittstelle (CLI)

Befehlszeilenschnittstelle (CLI): Manchmal auch als Terminal bezeichnet. Dies ist eine weitere Option zur Auswahl von Konfigurationen auf Geräten wie Routern und Switches. Wenn Sie Erfahrung haben, kann dies eine wesentlich einfachere Methode sein, Dinge einzurichten, da Sie nicht durch verschiedene Bildschirme der Webbenutzeroberfläche navigieren müssen. Der Nachteil ist, dass man die Befehle kennen und sie perfekt eingeben muss. Da Sie einen Artikel für Anfänger lesen, sollte CLI wahrscheinlich nicht die erste Wahl sein.

Virtuelles System

Die meisten Systeme verfügen über höhere Funktionen, als sie benötigen. Ein Computer kann so bereitgestellt werden, dass er alle notwendigen Komponenten enthält, um mehrere Computer auszuführen. Das Problem dabei ist, dass, wenn ein Teil ausfällt oder einen Neustart benötigt, alle dem folgen.

Wenn Sie VMware oder Hyper-V installieren, können Sie Software, Webserver, E-Mail-Server, FindIT und mehr auf einen Computer laden. Ein virtuelles System kann sogar ein anderes Betriebssystem verwenden. Sie sind logisch unabhängig voneinander. Jedes Gerät führt die Funktionen eines separaten Geräts aus, ohne dass es tatsächlich eines ist. Obwohl die Hardware gemeinsam genutzt wird, weist jedes virtuelle System einen Teil des physischen Zugriffs für jedes Betriebssystem zu. Dies kann Geld, Energie und Platz sparen.

Cisco Tools, die Sie verwenden können

Cisco Business Dashboard (CBD)

Dieses Tool von Cisco dient zur Überwachung und Wartung von Netzwerken. Das CBD unterstützt Sie bei der Identifizierung von Cisco Geräten in Ihrem Netzwerk sowie weiteren hilfreichen Verwaltungsfunktionen.

Dies ist ein nützliches Tool, wenn Sie Dinge von zu Hause aus ausführen oder mehr als ein Netzwerk überwachen. CBD kann auf einem virtuellen System ausgeführt werden. Weitere Informationen zu CBD finden Sie auf der Cisco Business Dashboard Support-Website oder im Cisco Business Dashboard Overview.

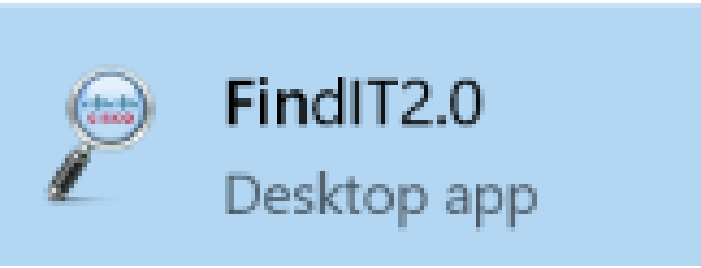
FindIT Network Discovery Utility

Dieses einfache Tool ist sehr einfach, hilft Ihnen jedoch, Cisco Geräte in Ihrem Netzwerk schnell zu erkennen. Cisco FindIT erkennt automatisch alle unterstützten Cisco Small Business-Geräte im gleichen lokalen Netzwerksegment wie Ihr PC.

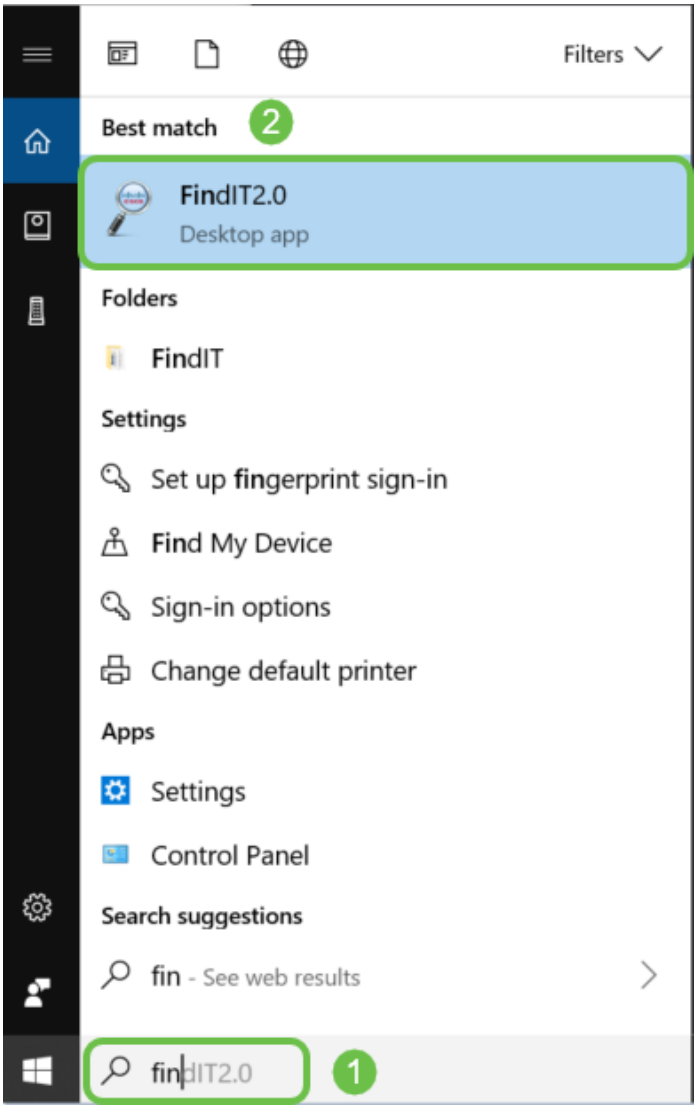
Klicken Sie hier, um mehr zu erfahren und das Cisco Small Business FindIT Network Discovery Utility herunterzuladen.

Klicken Sie auf diesen Link, um einen Artikel über die Installation und Einrichtung des Cisco FindIT Network Discovery Utility zu lesen.

Die Anwendung sieht für Windows 10 folgendermaßen aus.



Sobald es heruntergeladen ist, finden Sie es hier in Windows 10.



AnyConnect (Router der Serie RV34x/VPNs)

Dieses VPN wird speziell mit Routern der Serie RV34x (und Enterprise-/Large-Company-Geräten) verwendet. Der Cisco AnyConnect Secure Mobility Client stellt Remote-Benutzern eine sichere VPN-Verbindung zur Verfügung. Sie bietet Remote-Endbenutzern die Vorteile eines Cisco Secure Sockets Layer (SSL) VPN-Clients und unterstützt außerdem Anwendungen und Funktionen, die bei einer browserbasierten SSL VPN-Verbindung nicht verfügbar sind. AnyConnect wird häufig von Mitarbeitern an Remote-Standorten verwendet und ermöglicht ihnen die Verbindung mit der Computerinfrastruktur des Unternehmens, so als ob sie sich direkt im Büro aufhielten, selbst wenn dies nicht der Fall ist. Dies erhöht die Flexibilität, Mobilität und Produktivität der Mitarbeiter. Client-Lizenzen sind für die Verwendung von AnyConnect erforderlich. Cisco AnyConnect ist mit den folgenden Betriebssystemen kompatibel: Windows 7, 8, 8.1 und 10, Mac OS X 10.8 und höher und Linux Intel (x64).

Weitere Anleitungen finden Sie in den folgenden Artikeln:

- Installation des Cisco AnyConnect Secure Mobility Client auf einem Windows-Computer
- Installation des Cisco AnyConnect Secure Mobility Client auf einem Mac-Computer

Grundlagen des Datenaustauschs

Paket

Im Netzwerk werden Informationen in Textbausteinen, so genannten Paketen, gesendet. Bei Verbindungsproblemen können Pakete verloren gehen.

Latenz

Verzögerungen bei der Paketübertragung.

Redundanz

In einem Netzwerk wird Redundanz so konfiguriert, dass bei Problemen im Netzwerk das gesamte Netzwerk nicht ausfällt. Betrachten Sie es als Backup-Plan, wenn etwas mit der Hauptkonfiguration geschieht.

Protokolle

Für die Kommunikation zwischen zwei Geräten sind einige der gleichen Einstellungen erforderlich. Stellen Sie es sich als Sprache vor. Wenn eine Person nur Deutsch spricht und die andere nur Spanisch, kann sie nicht kommunizieren. Verschiedene Protokolle arbeiten zusammen, und es können mehrere Protokolle übertragen werden. Protokolle haben unterschiedliche Zwecke; einige Beispiele sind nachfolgend aufgeführt und kurz beschrieben.

Adressierungsprotokolle

- **Session Initiation Protocol (SIP):** Dies ist das Hauptprotokoll für VoIP (Voice over IP), Telefone, die über das Internet kommunizieren. Beide Seiten des Netzwerks müssen unter Verwendung desselben Protokolls eingerichtet werden, damit sie die Kommunikation über VoIP über SIP initiieren können.
- **Dynamic Host Configuration Protocol (DHCP)** verwaltet einen Pool verfügbarer IP-Adressen und weist diese Hosts zu, sobald sie dem Netzwerk beitreten.
- **Address Resolution Protocol** (ARP): Ordnet eine dynamische IP-Adresse einer permanenten physischen MAC-Adresse in einem LAN zu.
- **IPv4:** Dies ist die gängigste IP-Version, die heute verwendet wird. Eine IP-Adresse wird als 4 Zahlensätze (auch als Oktette bezeichnet) geschrieben, die durch einen Punkt zwischen den einzelnen Datensätzen getrennt sind. Jedes Set kann eine Zahl zwischen 0 und 255 sein. Ein Beispiel für eine IPv4-Adresse ist 8.8.8.8. Dies ist der öffentliche DNS-Server bei Google. Da es mehr Geräte als eindeutige IP-Adressen für IPv4 gibt, kann der Erwerb einer permanenten öffentlichen IP-Adresse teuer sein.
- **IPv6:** Diese neueste Version verwendet 8 Zahlensätze mit einem Doppelpunkt zwischen den einzelnen Datensätzen. Es verwendet ein hexadezimales numerisches System, sodass es Buchstaben in der IP-Adresse geben kann. Ein Unternehmen kann IPv4- und IPv6-Adressen gleichzeitig verwenden.

Da wir über IPv6 sprechen, sind hier einige wichtige Details zu diesem Adressierungsprotokoll enthalten:

IPv6-Abkürzungen: Wenn alle Zahlen in mehreren Sets 0 (null) sind, können zwei Doppelpunkte in einer Zeile diese Gruppen darstellen, kann diese Abkürzung nur einmal verwendet werden. Eine der IPv6-IP-Adressen bei Google ist beispielsweise 2001:4860:4860:888. Einige Geräte verwenden separate Felder für alle acht Teile von IPv6-Adressen und können die IPv6-Abkürzung nicht akzeptieren. In diesem Fall geben Sie 2001:4860:4860:0:0:0:0:888 ein.

Hexadezimal: Ein numerisches System, das eine Basis 16 anstelle von Basis 10 verwendet, was wir in alltäglicher Mathematik verwenden. Die Zahlen 0-9 sind identisch. 10-15 werden durch die Buchstaben A-F dargestellt.

Datenübertragungsprotokolle

- **Transmission Control Protocol (TCP) und User Datagram Protocol (UDP):** Dies sind zwei Arten der Datenübertragung. TCP erfordert eine Verbindung, die als Drei-Wege-Handshake bezeichnet wird, bevor Daten gesendet werden, sodass es manchmal zu einer Verzögerung kommt. Wenn Daten (Pakete) verloren gehen, werden sie erneut gesendet. UDP ist weniger zuverlässig, aber schneller. Sprach- und Videoanwendungen verwenden häufig UDP.
- **File Transfer Protocol (FTP):** Dieses Protokoll wird verwendet, um Dateien von einem Client auf einen Server zu übertragen.
- **Hypertext Transfer Protocol (HTTP) vs. Hypertext Transfer Protocol Secure (HTTPS):** Die allgemeine Basis für die Datenkommunikation über das Internet. Sie finden diese am Anfang der Websites, geschrieben als *http://* und *https://*. Sites, die mit *https://* beginnen, sind sicherer zu verwenden.
- **Routing Information Protocol (RIP):** Dieses Protokoll gibt es schon seit langem. Es gibt drei Versionen, wobei jede Version mehr Sicherheit und Funktionalität bietet. Router tauschen Routen untereinander aus. Das Ziel besteht darin, Schleifen zu vermeiden, indem eine maximale Anzahl von "Hops" zwischen den Routern festgelegt wird. Weitere, effizientere Protokolle für das Routing sind **EIGRP (Enhanced Interior Gateway Routing Protocol)**, **OSPF (Open Shortest Path First)** und IS-IS (Intermediate System to Intermediate System). Diese letzten drei Skalierungen sind besser als RIP, können aber komplizierter einzurichten sein.
- **Secure Shell (SSH):** Ein sicherer Kanal, der eine sichere Route für den Befehlszeilendatenverkehr bereitstellt. Es ist ein verschlüsseltes Protokoll, das für die Kommunikation mit einem Remote-Server verwendet wird. Viele zusätzliche Technologien basieren auf SSH.

Discovery-Protokolle

- **Cisco Discovery Protocol (CDP):** Erkennt Informationen über andere direkt verbundene Cisco Geräte und speichert diese Informationen. **Bonjour** und **Link Layer Discovery Protocol (LLDP)** führen dieselben Funktionen aus und können auch Informationen über Geräte von Drittanbietern abrufen. Die meisten Small Business-Geräte verwenden LLDP.
- **Layer Link Discovery Protocol (LLDP):** Ermöglicht es einem Gerät, seine Identifizierung, Konfiguration und Funktionen an benachbarte Geräte anzuzeigen, die die Daten dann in einer Management Information Base (MIB) speichern. Die Informationen, die von den

Nachbarn gemeinsam genutzt werden, reduzieren den Zeitaufwand für das Hinzufügen eines neuen Geräts zum Local Area Network (LAN) und liefern außerdem Details, die zur Behebung vieler Konfigurationsprobleme erforderlich sind. LLDP kann in Szenarien verwendet werden, in denen Sie zwischen Geräten arbeiten müssen, die nicht von Cisco stammen, und Geräten, die urheberrechtlich geschützt sind. Der Switch liefert alle Informationen zum aktuellen LLDP-Status der Ports. Sie können diese Informationen verwenden, um Verbindungsprobleme im Netzwerk zu beheben. Dies ist eines der Protokolle, die von Netzwerkerkennungsanwendungen wie FindIT Network Management zum Erkennen von Geräten im Netzwerk verwendet werden.

Identifizierung von Protokollen

- **Domain Name System (DNS):** Sobald einer IP-Adresse ein vollqualifizierter Domänenname (Fully Qualified Domain Name, FQDN) zugewiesen ist, wird dieser in eine Datenbank aufgenommen. Wenn Sie beispielsweise nach *www.google.com* suchen, können Sie den Namen der Website eingeben, die Datenbank sucht danach und kann Sie über die IP-Adresse dorthin bringen. Ihr **Internetdienstanbieter (ISP)** verwendet standardmäßig den DNS-Server, der bereits konfiguriert wurde. Sie können dies jedoch manuell ändern, wenn Sie bei der Nutzung des Internets eine langsame Geschwindigkeit feststellen.
- **Dynamischer DNS:** Auch als DDNS bezeichnet, aktualisiert automatisch einen Server im DNS mit der aktiven Konfiguration seiner Hostnamen, Adressen oder anderer relevanter Informationen. Mit anderen Worten weist DDNS einer dynamischen WAN-IP-Adresse einen festen Domänennamen zu. Dadurch werden die Kosten für den Erwerb einer permanenten IP-Adresse eingespart.
- **Internet Protocol (IP):** IP-Adressen sind eindeutige Kennungen, die das Senden und Empfangen von Daten zwischen Hosts im Internet ermöglichen. Dies erfolgt über öffentliche Internetadressen, die einen Kauf bei einem ISP erfordern.
- **Media Access Control (MAC-Adresse):** Jedes Gerät hat eine eindeutige ID, mit der es verbunden ist. Das ändert sich nicht. Es ist gut, Ihre MAC-Adresse zu kennen, wenn Sie ein Netzwerk einrichten und Fehler beheben. Sie befindet sich in der Regel auf dem Gerät und enthält Buchstaben und Zahlen. Switches überwachen MAC-Adressen von Geräten und erstellen eine MAC-Adresstabelle.

Fehlerbehebungsprotokolle

- **Ping:** Ein Ping ist eine gängige Fehlerbehebungsmethode. Ein Ping sendet ICMP-Echo-Nachrichten an eine IP-Adresse. Eine Nachricht wird als Gegenleistung empfangen. Eine erfolgreiche Antwort zeigt eine bidirektionale physische Verbindung. Es ist eine Möglichkeit zu sehen, ob ein Netzwerkdatenpaket problemlos an eine Adresse verteilt werden kann.
- **Internet Control Message Protocol (ICMP):** Meldungen über Fehler und betriebliche Informationen. Wenn Sie einen PING-Test durchführen, wird eine ICMP-Echo-Nachricht an das Ziel gesendet. Eine erfolgreiche Verbindung erhält eine Antwort von diesem Gerät.

Server

Ein Computer oder ein Programm auf einem Computer, der Dienste für andere Computer bereitstellt. Ein Server kann virtuell oder sogar eine Anwendung sein. Auf einem Gerät können mehrere Server vorhanden sein. Server können gemeinsam genutzt werden. Sie können mit Windows, Mac oder Linux verwendet werden.

Webserver - formatieren und präsentieren von Webseiten für Webbrowser
Dateiserver - Dateien und Ordner für Benutzer im Netzwerk freigeben
E-Mail-Server - Senden, Empfangen und Speichern von E-Mails
DNS-Server: Übersetzen benutzerfreundlicher Namen wie www.cisco.com in die IP-Adresse 173.37.145.84, z. B.
Instant Messaging-Server - Kontrolle und Verwaltung von Instant Messages (Jabber, Skype)

Quality of Service (QoS)

Diese Einstellungen werden so konfiguriert, dass der Datenverkehr in einem Netzwerk, in der Regel Sprache oder Video, priorisiert wird, da dies häufig die am stärksten wahrnehmbare Verzögerung bei Paketverzögerungen (Daten) ist.

Grundlagen einer Internetverbindung

Internetdienstanbieter (ISP)

Sie benötigen einen ISP, um auf das Internet in Ihrem Netzwerk zugreifen zu können. Es gibt viele Optionen für Verbindungsgeschwindigkeiten, sowie eine Vielzahl von Preisen, die den Anforderungen Ihres Unternehmens entsprechen. Neben dem Zugriff auf das Internet bietet ein ISP E-Mail, das Hosting von Webseiten und mehr an.

Webbrowser

Eine Anwendung, die auf Ihrem Gerät installiert ist. Es gibt andere, die Sie herunterladen können. Nach dem Download können Sie die IP-Adresse oder Website, zu der Sie über das Internet gehen möchten, öffnen und eingeben. Beispiele für Webbrowser:

Microsoft Edge

 ,

Chrome

 ,

Firefox

 ,

und Safari.

 .

Wenn Sie etwas nicht öffnen können oder andere Navigationsprobleme haben, können Sie einfach einen anderen Webbrowser öffnen und es erneut versuchen.

Uniform Resource Locator (URL)

In einem Webbrowser geben Sie in der Regel den Namen einer Website ein, auf die Sie zugreifen möchten, d. h. die URL, die Webadresse. Jede URL muss eindeutig sein. Ein Beispiel für eine URL ist https://www.cisco.com.

Standard-Gateway

Dies ist der Router, den der LAN-Datenverkehr als Ausgang zum Internet Service Provider (ISP) und zum Internet verwendet. Mit anderen Worten, dieser Router verbindet Sie mit anderen Geräten außerhalb Ihres Gebäudes und über das Internet.

Firewall

Eine Firewall ist ein Netzwerksicherheitsgerät, das eingehenden und ausgehenden Netzwerkverkehr überwacht und entscheidet, ob bestimmter Datenverkehr auf der Grundlage eines festgelegten Satzes von Sicherheitsregeln zugelassen oder blockiert wird, die Zugriffskontrolllisten (Access Control Lists, ACLs) genannt werden.

Firewalls sind seit Jahrzehnten die erste Verteidigungslinie im Bereich der Netzwerksicherheit. Sie stellen eine Barriere zwischen gesicherten und kontrollierten internen Netzwerken dar, die vertrauenswürdig und nicht vertrauenswürdig außerhalb von Netzwerken wie dem Internet sind.

Eine Firewall kann Hardware, Software oder beides sein.

Weitere Informationen finden Sie unter Konfigurieren der grundlegenden Firewall-Einstellungen auf dem Router der Serie RV34x.

Zugriffskontrolllisten (ACLs)

Listet auf, die das Senden von Datenverkehr an und von bestimmten Benutzern blockieren oder zulassen. Zugriffsregeln können so konfiguriert werden, dass sie jederzeit gültig sind oder auf einem definierten Zeitplan basieren. Eine Zugriffsregel wird anhand verschiedener Kriterien konfiguriert, um den Zugriff auf das Netzwerk zu ermöglichen oder zu verweigern. Die Zugriffsregel wird basierend auf dem Zeitpunkt geplant, zu dem die Zugriffsregeln auf den Router angewendet werden müssen. Diese werden unter Sicherheits- oder Firewall-Einstellungen eingerichtet. Ein Unternehmen möchte beispielsweise Mitarbeiter daran hindern, während der Geschäftszeiten Live-Sportveranstaltungen zu streamen oder eine Verbindung zu Facebook herzustellen.

Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraums von einem Punkt an einen anderen gesendet werden kann. Wenn Sie eine Internetverbindung mit einer größeren Bandbreite haben, kann das Netzwerk Daten viel schneller übertragen als eine Internetverbindung mit einer geringeren Bandbreite. Video-Streaming benötigt viel mehr Bandbreite als das Senden von Dateien. Wenn Sie feststellen, dass beim Zugriff auf eine Webseite eine Verzögerung auftritt oder das Video-Streaming verzögert wird, müssen Sie möglicherweise die Bandbreite in Ihrem Netzwerk erhöhen.

Ethernet-Kabel

Die meisten Geräte in einem Netzwerk haben Ethernet-Ports. Ethernet-Kabel sind das, was sie für eine kabelgebundene Verbindung anschließen. Beide Enden des RJ45-Kabels sind identisch und sehen aus wie die alten Telefonbuchsen. Sie können verwendet werden, um Geräte anzuschließen und eine Verbindung zum Internet herzustellen. Die Kabel verbinden Geräte für den Internetzugriff und die Dateifreigabe. Einige Computer benötigen einen Ethernet-Adapter, da sie möglicherweise keinen Ethernet-Port bereitstellen.

Netzwerke und deren Zusammenspiel

Local Area Network (LAN)

Ein Netzwerk, das so groß wie mehrere Gebäude oder so klein wie ein Zuhause sein kann. Alle mit dem LAN verbundenen Personen befinden sich am selben physischen Standort und sind mit demselben Router verbunden.

In einem lokalen Netzwerk wird jedem Gerät eine eigene eindeutige interne IP-Adresse zugewiesen. Sie folgen einem Muster 10.x.x.x, 172.16.x.x - 172.31.x.x oder 192.168.x.x. Diese Adressen sind nur innerhalb eines Netzwerks, zwischen Geräten sichtbar und gelten als privat. Es gibt Millionen von Standorten, die möglicherweise denselben Pool interner IP-Adressen wie Ihr Unternehmen haben. Es spielt keine Rolle, sie werden nur in ihrem eigenen privaten Netzwerk verwendet, sodass es keinen Konflikt gibt. Damit die Geräte im Netzwerk miteinander kommunizieren können, sollten sie alle das gleiche Muster verwenden wie die anderen Geräte, sich im gleichen Subnetz befinden und eindeutig sein. Diese Adressen sollten in diesem Muster niemals als öffentliche IP-Adresse angezeigt werden, da sie nur privaten LAN-Adressen

vorbehalten sind.

Alle diese Geräte senden Daten über ein Standard-Gateway (einen Router), um ins Internet zu gelangen. Wenn das Standard-Gateway die Informationen erhält, muss es eine Network Address Translation (NAT) durchführen und die IP-Adresse ändern, da alle Vorgänge im Internet eine eindeutige IP-Adresse erfordern.

Wide Area Network (WAN)

Ein Wide Area Network (WAN) ist ein Netzwerk, das sich teilweise global ausbreitet. Viele LANs können eine Verbindung zu einem einzelnen WAN herstellen.

Nur WAN-Adressen können im Internet miteinander kommunizieren. Jede WAN-Adresse muss eindeutig sein. Damit Geräte im Netzwerk Informationen über das Internet senden und empfangen können, müssen Sie über einen Router am Netzwerk-Edge verfügen (ein Standard-Gateway), der NAT durchführen kann.

Klicken Sie auf den Link Konfigurieren von Zugriffsregeln auf einem Router der Serie RV34x.

Network Address Translation (NAT)

Ein Router empfängt eine WAN-Adresse über einen Internet Service Provider (ISP). Der Router verfügt über eine NAT-Funktion, die den Datenverkehr aus dem Netzwerk nimmt, die private Adresse in die öffentliche WAN-Adresse übersetzt und sie über das Internet sendet. Beim Empfang von Datenverkehr umgekehrt. Dies wurde eingerichtet, weil nicht genügend permanente IPv4-Adressen für alle Geräte auf der Welt verfügbar sind.

NAT bietet zusätzliche Sicherheit, da das gesamte interne Netzwerk hinter dieser eindeutigen öffentlichen IP-Adresse verborgen bleibt. Interne IP-Adressen bleiben oft gleich, aber wenn sie für eine Weile getrennt, konfiguriert oder auf die Werkseinstellungen zurückgesetzt werden, ist dies möglicherweise nicht der Fall.

Statisches NAT

Sie können die interne IP-Adresse so konfigurieren, dass sie gleich bleibt, indem Sie das statische Dynamic Host Configuration Protocol (DHCP) auf dem Router konfigurieren. Öffentliche IP-Adressen werden nicht garantiert gleich bleiben, es sei denn, Sie bezahlen für eine statische öffentliche IP-Adresse über Ihren ISP. Viele Unternehmen zahlen für diesen Service, sodass ihre Mitarbeiter und Kunden eine zuverlässigere Verbindung zu ihren Servern (Web, Mail, VPN usw.) haben, diese jedoch möglicherweise teuer sind.

Statische NAT ordnet eine Eins-zu-Eins-Übersetzung der privaten IP-Adressen den öffentlichen IP-Adressen zu. Es wird eine feste Übersetzung von privaten Adressen in die öffentlichen Adressen erstellt. Dies bedeutet, dass Sie dieselbe Anzahl öffentlicher Adressen als private Adressen benötigen. Dies ist nützlich, wenn ein Gerät von

außerhalb des Netzwerks zugänglich sein muss.

Klicken Sie auf RV160 und RV260, um den Text Konfigurieren von NAT und statischer NAT zu lesen.

CGNAT

Carrier Grade NAT ist ein ähnliches Protokoll, mit dem mehrere Clients dieselbe IP-Adresse verwenden können.

VLAN

Mit einem Virtual Local Area Network (VLAN) können Sie ein Local Area Network (LAN) logisch in verschiedene Broadcast-Domänen segmentieren. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden. Eine Übertragung kann dann auf ein spezifisches VLAN beschränkt werden. Nur die Benutzer, die zu einem VLAN gehören, können auf die Daten in diesem VLAN zugreifen und sie ändern. Mithilfe von VLANs kann auch die Leistung verbessert werden, da Broadcasts und Multicasts seltener an unnötige Ziele gesendet werden müssen.

Ein VLAN wird hauptsächlich verwendet, um Gruppen zwischen den Hosts zu bilden, unabhängig davon, wo sich die Hosts befinden. So verbessert ein VLAN mithilfe der Gruppenerstellung zwischen den Hosts die Sicherheit. Wenn ein VLAN erstellt wird, hat dies keine Auswirkungen, bis dieses VLAN mindestens einem Port manuell oder dynamisch zugewiesen wird. Einer der häufigsten Gründe für die Einrichtung eines VLAN besteht darin, ein separates VLAN für Sprache und ein separates VLAN für Daten einzurichten. Dadurch werden die Pakete für beide Datentypen weitergeleitet, obwohl dasselbe Netzwerk verwendet wird.

Weitere Informationen finden Sie in den VLAN Best Practices und Security Tips für Cisco Business Router.

Subnetz

Subnetze werden häufig als Subnetze bezeichnet und sind unabhängige Netzwerke innerhalb eines IP-Netzwerks.

SSID

Der Service Set Identifier (SSID) ist eine eindeutige ID, mit der Wireless-Clients eine Verbindung zu allen Geräten in einem Wireless-Netzwerk herstellen oder diese gemeinsam nutzen können. Es wird zwischen Groß- und Kleinschreibung unterschieden und darf 32 alphanumerische Zeichen nicht überschreiten. Dies wird auch als Wireless-Netzwerkname bezeichnet.

Virtual Private Networks (VPNs)

Technologien haben sich weiterentwickelt, und Geschäfte werden häufig außerhalb des Büros abgewickelt. Geräte sind mobiler, und Mitarbeiter arbeiten häufig von zu Hause oder unterwegs. Dies kann einige Sicherheitslücken verursachen. Ein Virtual Private Network (VPN) ist eine hervorragende Methode, um externe Mitarbeiter sicher mit einem Netzwerk zu verbinden. Mit einem VPN kann ein Remote-Host so agieren, als ob er sich im selben lokalen Netzwerk befinde.

Ein VPN ist für die sichere Datenübertragung eingerichtet. Es gibt verschiedene Optionen für die Einrichtung eines VPN und die Verschlüsselung der Daten. VPNs verwenden Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP) und Layer Two Tunneling Protocol.

Eine VPN-Verbindung ermöglicht es Benutzern, über ein öffentliches oder gemeinsam genutztes Netzwerk (z. B. das Internet) auf Daten zuzugreifen, sie zu senden und von einem privaten Netzwerk zu empfangen. Gleichzeitig wird jedoch eine sichere Verbindung zu einer zugrunde liegenden Netzwerkinfrastruktur sichergestellt, um das private Netzwerk und seine Ressourcen zu schützen.

Ein VPN-Tunnel richtet ein privates Netzwerk ein, das Daten sicher mit Verschlüsselung und Authentifizierung senden kann. Firmenbüros verwenden in der Regel eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, den Mitarbeitern den Zugriff auf ihr privates Netzwerk zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

Nachdem der Router für eine Internetverbindung konfiguriert wurde, kann zwischen dem Router und einem Endpunkt eine VPN-Verbindung eingerichtet werden. Der VPN-Client ist vollständig von den Einstellungen des VPN-Routers abhängig, um eine Verbindung herstellen zu können.

Ein VPN unterstützt Site-to-Site-VPN für einen Gateway-to-Gateway-Tunnel. Ein Benutzer kann beispielsweise einen VPN-Tunnel in einer Zweigstelle so konfigurieren, dass er sich mit dem Router an einem Unternehmensstandort verbindet, sodass die Zweigstelle sicher auf das Unternehmensnetzwerk zugreifen kann. In einer Site-to-Site-VPN-Verbindung kann jeder die Kommunikation initiieren. Diese Konfiguration verfügt über eine konstante verschlüsselte Verbindung.

IPsec VPN unterstützt auch Client-to-Server-VPN für einen Host-to-Gateway-Tunnel. Das VPN zwischen Client und Server ist nützlich, wenn von Laptop/PC aus eine Verbindung mit einem Unternehmensnetzwerk über den VPN-Server hergestellt wird. In diesem Fall kann nur der Client die Verbindung initiieren.

Klicken Sie hier, um die Übersicht und Best Practices zu Cisco Business VPN zu lesen.

Zertifikate

Ein sicherer Schritt bei der Einrichtung eines VPN ist der Erhalt eines Zertifikats einer Zertifizierungsstelle (Certificate Authority, CA). Diese wird für die Authentifizierung verwendet. Zertifikate werden von einer beliebigen Anzahl von Websites Dritter

erworben. Es ist eine offizielle Methode, zu beweisen, dass Ihre Website sicher ist. Im Wesentlichen ist die CA eine vertrauenswürdige Quelle, die sicherstellt, dass Sie ein legitimes Unternehmen sind und vertrauenswürdig sind. Für ein VPN benötigen Sie nur ein Zertifikat der unteren Ebene zu einem minimalen Preis. Sie werden von der Zertifizierungsstelle ausgecheckt, und sobald diese Ihre Informationen überprüft hat, wird Ihnen das Zertifikat ausgestellt. Dieses Zertifikat kann als Datei auf Ihren Computer heruntergeladen werden. Sie können dann zu Ihrem Router (oder VPN-Server) gehen und ihn dort hochladen.

Clients benötigen normalerweise kein Zertifikat für die Verwendung eines VPN. sondern nur zur Überprüfung durch den Router. Eine Ausnahme hiervon ist OpenVPN, das ein Clientzertifikat erfordert.

Viele kleine und mittlere Unternehmen verwenden aus Gründen der Einfachheit ein Kennwort oder einen vorinstallierten Schlüssel anstelle eines Zertifikats. Dies ist weniger sicher, kann aber kostenlos eingerichtet werden.

Einige Artikel zu diesem Thema könnten Ihnen nützlich sein:

- Zertifikat (Import/Export/CSR erstellen) für Router der Serien RV160 und RV260
- Ersetzen Sie das Standard-selbstsignierte Zertifikat durch ein SSL-Zertifikat eines Drittanbieters auf dem Router der Serie RV34x.
- Verwalten von Zertifikaten auf dem Router der Serie RV34x

Vorinstallierter Schlüssel (PSK)

Dies ist ein gemeinsam genutztes Kennwort, das vor der Konfiguration eines VPNs festgelegt und freigegeben wurde und als Alternative zur Verwendung eines Zertifikats verwendet werden kann. Ein PSK kann das sein, was Sie möchten. Er muss nur am Standort und mit dem Client übereinstimmen, wenn er als Client auf dem Computer eingerichtet ist. Beachten Sie, dass es je nach Gerät verbotene Symbole geben kann, die Sie nicht verwenden können.

Wichtige Lebensdauer

Legt fest, wie oft das System den Schlüssel ändert. Diese Einstellung muss auch mit dem Remote-Router identisch sein.

Schlussfolgerung

Da haben Sie es, jetzt haben Sie viele der Grundlagen, um Sie auf dem Weg zu bringen.

Wenn Sie mehr erfahren möchten, sehen Sie sich diese Links an!

Best Practices für die Einrichtung statischer IP-Adressen Cisco Business VPN - Überblick und Best Practices VLAN Best Practices und Security Tips für Cisco Business Router Internet-Backup

- Windows Internet-Backup - Mac So melden Sie sich bei einem Switch an