

Nieuw aan Cisco Business: Apparatuur en basisnetwerkwoordenlijst

Doel

Het doel van dit document is om beginners vertrouwd te maken met Cisco Business (Small Business)-apparatuur en bepaalde algemene termen die u dient te kennen. De onderwerpen omvatten beschikbare hardware, de Termen van Cisco Business, de Algemene Voorwaarden van de Netwerk, de Gereedschappen van Cisco, de Basisbeginselen van het Uitwisselen van Gegevens, de Grondbeginselen van een Verbinding van Internet, en netwerken en hoe zij bij elkaar passen.

Inleiding

Start u net het instellen van uw netwerk met Cisco-apparatuur? Het kan overweldigend zijn om de hele nieuwe wereld te betreden van het opzetten en onderhouden van een netwerk. Dit artikel is bedoeld om u vertrouwd te maken met een aantal grondbeginselen. Hoe meer je weet, hoe minder intimiderend het zal zijn!

- [Beschikbaar via Cisco Business](#)
 - [router](#)
 - [Switch](#)
 - [Draadloos access point](#)
 - [Multiplatform Phone](#)
- [Populair verwezen in Cisco Business](#)
 - [Systeemgids en Snel starten](#)
 - [Standaardinstellingen](#)
 - [Standaard gebruikersnaam en wachtwoord](#)
 - [Standaard IP-adressen](#)
 - [Op fabrieksstandaard terugzetten](#)
 - [Web User Interface \(UI\)](#)
 - [Wizard Instellen](#)
 - [Cisco eigen](#)
 - [Modellen in een serie](#)
 - [Firmware](#)
 - [Upgradefirmware](#)
- [Algemene netwerkvoorwaarden](#)
 - [Interface](#)
 - [Knooppunt](#)
 - [Host](#)
 - [Computer-programma](#)
 - [Toepassing](#)
 - [Best Practice](#)
 - [Topologie](#)
 - [Configureren](#)

- [MAC-adres](#)
- [Open source](#)
- [Zip-bestand](#)
- [Opdracht Line Interface \(CLI\)](#)
- [Virtuele machine](#)
- [Cisco-tools die u kunt gebruiken](#)
 - [Cisco Business Dashboard \(CBD\)](#)
 - [Hulpprogramma voor netwerkdetectie van FindIT](#)
 - [AnyConnect \(RV34x Series routers/VPN's\)](#)
- [De basisbeginselen van het uitwisselen van gegevens](#)
 - [Packet](#)
 - [Latentie](#)
 - [Redundantie](#)
 - [Protocols](#)
 - [Server](#)
 - [QoS-kwaliteit \(Quality of Service\)](#)
- [De basisbeginselen van een internetverbinding](#)
 - [Internet Service Provider \(ISP\)](#)
 - [Web browser](#)
 - [Unified Resource Locator \(URL\)](#)
 - [Standaard gateway](#)
 - [Firewall](#)
 - [Toegangscontrolelijsten \(ACL's\)](#)
 - [Bandbreedte](#)
 - [Ethernet-kabel](#)
- [Netwerken en hoe ze met elkaar passen](#)
 - [Local Area Network \(LAN\)](#)
 - [Wide Area Network \(WAN\)](#)
 - [Netwerkadresomzetting \(NAT\)](#)
 - [Statische NAT](#)
 - [CGNAT](#)
 - [VLAN](#)
 - [Subnetwerk](#)
 - [SSID](#)
 - [Virtual Private Networks \(VPN's\)](#)

Beschikbaar via Cisco Business

router

Routers verbinden meerdere netwerken samen zowel als routegegevens waar deze nodig zijn. Ze verbinden computers op die netwerken ook aan het internet. Routers stellen alle netwerkcomputers in staat om één internetverbinding te delen, waardoor geld wordt bespaard.

Een router werkt als een verzender. Ze analyseert gegevens die over een netwerk worden verzonden, kiest de beste route voor data om te reizen, en stuurt ze onderweg.

Routers verbinden uw zaken met de wereld, beschermen informatie tegen veiligheidsbedreigingen en kunnen zelfs beslissen welke computers prioriteit boven anderen ontvangen.

Buiten die basisnetwerkfuncties, komen routers met extra functies om netwerken makkelijker of veiliger te maken. Afhankelijk van uw behoeften, bijvoorbeeld, kunt u een router met een firewall, een virtueel privé netwerk (VPN) of een Internet Protocol (IP) communicatiesysteem kiezen.

De meest recent ontwikkelde Cisco Business-routers omvatten de RV160, RV260, RV340 en RV345-serie.

Switch

Switches vormen het fundament van de meeste bedrijfsnetwerken. Een switch werkt als een controller voor de aansluiting van computers, printers en servers op een netwerk in een gebouw of op een campus.

Switches staan apparaten op uw netwerk toe om met elkaar, zowel als met andere netwerken te communiceren, die een netwerk van gedeelde middelen creëren. Door het delen van informatie en het toewijzen van middelen, sparen switches geld en verhogen ze de productiviteit.

Er zijn twee basistypen switches om uit te kiezen als deel van uw netwerk basisgegevens: beheerd en onbeheerd.

Een switch zonder beheer werkt uit het vakje, maar kan niet worden ingesteld. Thuisnetwerkapparatuur biedt doorgaans onbeheerde switches.

Een beheerde switch kan worden geconfigureerd. U kunt een beheerde switch lokaal of op afstand bewaken en aanpassen, waardoor u meer controle over netwerkverkeer en toegang krijgt.

Zie voor meer informatie over switches de [Switches Lijst van termen](#).

De meest recent ontwikkelde switches omvatten de Cisco Business Switch CBS110, CBS220, CBS250 en CBS350-serie.

Als u de verschillen tussen de CBS-switches wilt leren, controleert u

Draadloos access point

Een draadloos access point stelt apparaten in staat zonder kabels aan te sluiten op het draadloze netwerk. Een draadloos netwerk maakt het makkelijk om nieuwe apparaten online te brengen en biedt flexibele ondersteuning aan mobiele arbeiders.

Een access point fungeert als een versterker voor uw netwerk. Terwijl een router de bandbreedte verstrekt, breidt een toegangspunt die bandbreedte uit zodat het netwerk veel apparaten kan steunen, en die apparaten kunnen het netwerk van verder weg

toegang hebben.

Maar een toegangspunt breidt Wi-Fi niet alleen uit. Het kan ook nuttige gegevens over de apparaten op het netwerk geven, pro-actieve veiligheid verstrekken en vele andere praktische doeleinden dienen.

De meest recent ontwikkelde draadloze access points, Cisco Business Wireless, omvatten AC140, AC145 en AC240 die voor een draadloos netwerk zijn voorzien. Als u niet bekend bent met draadloze netwerken, kunt u meer lezen in [Welcome to Cisco Business Wireless mesh](#) of [Frequent Asked Notes \(FAQ\) voor een Cisco Business Wireless Network](#).

Als u bepaalde termen wilt leren die normaal zijn voor draadloze access points, raadpleegt u het [WAP Glossary of Terms](#).

Multiplatform Phone

MPP-telefoons bieden Voice-over-IP (VoIP) communicatie met Session Initiation Protocol (SIP). Dit heft de behoefte aan traditionele telefoonlijnen op en maakt telefoons draagbaarder binnen het bedrijf. Met VoIP gebruikt een telefoon een bestaande netwerkinfrastructuur en internetverbinding in plaats van dure T1-lijnen. Dit geeft de mogelijkheid om meer oproepen met minder "lijnen" te beheren. Andere voordelige opties zijn het aanzetten van telefoontjes op de plaats, parkeergesprekken, het overdragen van gesprekken en meer. Sommige modellen staan videocommunicatie naast VoIP toe.

MPP-telefoons zijn gebouwd om er als een gewone telefoon uit te zien en worden alleen voor dat doel gebruikt, maar in wezen zijn ze een computer en maken ze deel uit van je netwerk. MPP-telefoons vereisen ofwel de service van een Internet Telephony Service Provider (ITSP) of een IP Private Branch Exchange (PBX)-gespreksserver. [Webex Calling](#), [Ring Central](#) en [Verizon](#) zijn voorbeelden van een ITSP. Enkele voorbeelden van IP PBX-services die met Cisco MPP-telefoons werken zijn onder andere [Asterisk](#)-, [Centile](#)- en [Metaswitch](#)-platforms. Veel functies op deze telefoons worden specifiek geprogrammeerd via derde providers (zoals FreePBX), dus processen (autopark, toegang tot voicemail, enzovoort) kunnen variëren.

De meest recent ontwikkelde Cisco Business MPP-telefoons bevatten de 6800, 7800 en 8800 Series.

Populair verwezen in Cisco Business

Systeemgids en Snel starten

Dit zijn twee verschillende resources om informatie te verkrijgen over uw product en de functies ervan. Wanneer u een website of webzoekactie met uw modelnummer doet, kunt u het ene of het andere toevoegen om deze langere gidsen te bekijken.

Standaardinstellingen

Apparaten worden geleverd met vooraf ingestelde standaardinstellingen. Ze zijn vaak de meest gebruikelijke instellingen die een beheerder zou kiezen. U kunt de instellingen aan uw behoeften aanpassen.

Standaard gebruikersnaam en wachtwoord

Bij oudere Cisco Business-apparatuur was de standaardinstelling *admin* voor zowel gebruikersnaam als wachtwoord. De meeste hebben nu een standaard *cisco* voor zowel gebruikersnaam als wachtwoord. Op Voice-over-IP (VoIP) telefoons moet u inloggen als *beheerder* om veel van de configuraties te wijzigen. Het wordt ten zeerste aanbevolen, het wachtwoord te wijzigen om het voor beveiligingsdoeleinden gecompliceerder te maken.

Standaard IP-adressen

De meeste apparaten van Cisco komen met de standaard IP adressen voor routers, switches, en draadloze access points. Als u het IP-adres niet kunt onthouden en u geen speciale configuratie hebt, kunt u een open papierklem gebruiken om ten minste 10 seconden op de resetknop op uw apparaat te drukken. Hiermee worden de standaardinstellingen hersteld. Als uw switch of WAP niet met DHCP is verbonden met een router die DHCP is ingeschakeld en u rechtstreeks met de switch of WAP met uw computer bent verbonden, zijn dit de standaardadressen van IP.

Het standaard IP-adres van een Cisco Business-router is 192.168.1.1.

Het standaard IP-adres voor een Cisco Business switch is 192.168.1.254.

Het standaard IP-adres voor een Wireless Access Point (AP) voor kleine bedrijven is 192.168.1.245. Er is geen standaard IP-adres voor de nieuwe draadloze access points.

Op fabrieksstandaard terugzetten

Er kan een moment komen waarop u uw Cisco Business-router, switch of draadloos access point wilt herstellen naar fabrieksstandaardinstellingen en van nul wilt beginnen. Dit komt handig voor als u de apparatuur van het ene netwerk naar het andere verplaatst, of in laatste instantie wanneer u geen configuratieprobleem kunt oplossen. Wanneer u de standaardinstellingen van de fabriek opnieuw instelt, verliest u alle configuraties.

U kunt back-upconfiguraties maken zodat u deze kunt herstellen nadat u een fabrieksreset hebt uitgevoerd. Klik op de volgende koppelingen voor meer informatie:

- [Herstart of herstel de standaardinstellingen van de RV34x Series router met behulp van het webgebaseerde hulpprogramma](#)
- [Firmware maken voor back-up en herstel of vervanging op een Switch](#)
- [Configuratiebestanden op een draadloos access point downloaden, downloaden, kopiëren en verwijderen](#)

- [De configuratiebestanden in WAP125 of WAP581 access point beheren](#)

Als u geen back-up maakt van de configuratie, dient u het apparaat opnieuw vanaf het begin in te stellen, zodat u over de verbidingsgegevens beschikt. De meeste modellen hebben een artikel waarin de stappen voor een reset worden beschreven, maar de eenvoudigste manier om dit te doen is door een open paperclip te gebruiken en de reset knop op uw apparaat minstens 10 seconden ingedrukt te houden. Dit is niet van toepassing op de MPP-telefoons, dus controleer [of u een Cisco IP-telefoon opnieuw instelt](#) voor meer informatie.

Web User Interface (UI)

Elk stuk van Cisco Business apparatuur komt met een Web UI, behalve de 100 reeksen onbeheerde switches.

Dit type interface, wat u op het scherm ziet, geeft opties voor selectie weer. U hoeft geen opdrachten te kennen om door deze schermen te navigeren. Web UI wordt ook soms ook genoemd als een Graphical User Interface (GUI), een web-gebaseerde interface, een web-Based guidance, een op internet gebaseerd gebruik of een web configuratie voorziening.

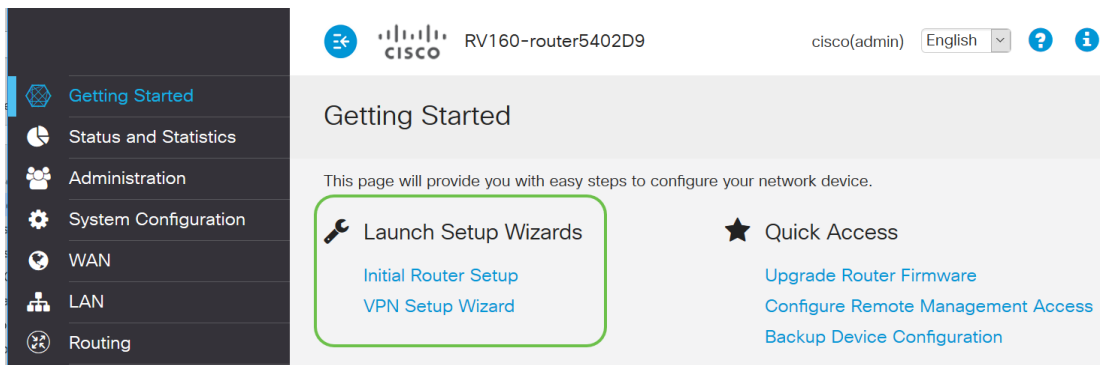
Een van de makkelijkste manieren om de configuratie van een apparaat te veranderen is door het Web UI. Web UI geeft de beheerder een gereedschap dat alle mogelijke eigenschappen bevat die kunnen worden gewijzigd om de prestaties van een apparaat aan te passen.

Nadat u in een Cisco-apparaat hebt gelogd, ziet u een Web UI-scherm dat aan de linkerkant een navigatiedeelvenster bevat. Het bevat een lijst van de bovenste functies van het apparaat. Het navigatiedeelvenster wordt ook soms aangeduid als een navigatieboom, navigatiebalk of een navigatiebalk.

De kleuren van deze pagina kunnen variëren, evenals de eigenschappen op het hoogste niveau, afhankelijk van het apparaat en de firmware versie.

Wizard Instellen

Dit is een interactief scherm dat u zult navigeren wanneer u voor het eerst inlogt op een Cisco Small Business-apparaat, en mogelijk daarna. Het kan een geweldige manier zijn om je op te zetten en te laten draaien op je netwerk. Er zijn verschillende standaardinstellingen die kunnen worden gewijzigd. Sommige apparaten voorzien van meer dan één setup-wizard. Dit voorbeeld toont twee de tovenaars van de opstelling, de *Eerste Toets van de router*, en de *Wizard van de VPN van de opstelling*.



Cisco eigen

Speciaal ontwikkeld en eigendom van Cisco. Cisco Discovery Protocol (CDP) is bijvoorbeeld eigen Cisco-software. Gewoonlijk kunnen de bedrijfseigen protocollen van Cisco alleen op Cisco apparaten worden gebruikt.

Modellen in een serie

Cisco biedt kleine bedrijfseigenaren veel verschillende modellen aan om in de behoeften van hun bedrijf te voorzien. Vaak wordt een model aangeboden met verschillende functies, aantal poorten, Power over Ethernet of zelfs draadloze verbindingen. Als er meerdere modellen in een serie zijn, zal Cisco een x in plaats van het nummer of de letter plaatsen die tussen modellen verschilt, maar de informatie is van toepassing op al in die serie. Bijvoorbeeld, de routers RV340 en RV345 worden bedoeld in de RV34x-serie. Als een apparaat aan het eind een P heeft biedt het Macht over Ethernet aan. Als een apparaatnaam eindigt in W biedt dit draadloze mogelijkheden. In het algemeen, hoe hoger het aantal van het model, hoe hoger de mogelijkheden van het apparaat. Bekijk de volgende artikelen voor meer informatie hierover:

- [Ring van productdecoder - router](#)
- [Product-ID-decoder - Switch](#)
- [Ring van productdecoder - WAP](#)
- [Cisco Business Wireless-model decoder](#) (mesh draadloos)

Firmware

Ook bekend als een afbeelding. Het programma dat de werking en functionaliteit van het apparaat controleert.

Upgradefirmware

Het verbeteren van firmware is essentieel voor optimale prestaties op elk apparaat. Het is zeer belangrijk om upgrades te installeren wanneer zij worden vrijgegeven. Wanneer Cisco een firmware-upgrade loslaat, bevatten ze vaak verbeteringen zoals nieuwe functies of repareren ze een bug die een security kwetsbaarheid of een prestatiekwestie kan veroorzaken.

Ga naar [Cisco Support](#) en voer de naam in van het apparaat dat een upgrade onder *Downloads* nodig heeft. Er moet een uitrolmenu verschijnen. Scrollt neer en kies het

specifieke model dat u bezit.

Support & Downloads

Product Support

Select a Product

Products by Category

Switches

Security

Routers

Networking Software (IOS & NX-C

Cloud and Systems Management

Conferencing

Downloads

SG200 1

SG200-08 8-Port Gigabit Smart Switch

SG200-08P 8-Port Gigabit POE Smart Switch

SG200-10FP 10-Port PoE Smart Switch

SG200-18 18-port Gigabit Smart Switch

SG200-26 26-port Gigabit Smart Switch

SG200-26FP 26-port Gigabit Full-PoE Smart Switch

SG200-26P 26-port Gigabit PoE Smart Switch

SG200-50 50-port Gigabit Smart Switch 2

Tip: wanneer u verschillende versies van Cisco firmware bekijkt, volgt elk een formaat van x.x.x.x. die als vier octetten worden beschouwd. Als er een kleine update is, verandert de vierde octet. De derde octet verandert als het een grotere verandering is. De tweede octet betekent een grote verandering. De eerste octet verandert als het een volledige revisie is.

Als u advies wilt, klik op deze link om [firmware op elk apparaat te downloaden en te upgraden](#).

Dit artikel bevat een aantal ideeën voor het oplossen van problemen voor het geval u problemen hebt met een upgrade van de switch: [upgrade Firmware op een Switch van 200/300 Series](#).

Algemene netwerkvoorwaarden

Zodra u uw apparatuur hebt, dient u bekend te worden met bepaalde algemene bepalingen in een netwerk.

Interface

Een interface is meestal die ruimte tussen het ene systeem en het andere. Alles dat kan communiceren met uw computer, inclusief poorten. Een netwerkinterface wordt over het algemeen toegewezen aan een lokaal IP-adres. Een gebruikersinterface maakt het mogelijk voor de gebruiker om met het besturingssysteem te communiceren.

Knooppunt

Een algemene term om elk apparaat te beschrijven dat een verbinding of interactie binnen een netwerk maakt, of informatie kan verzenden, ontvangen en opslaan, met het internet communiceren en een IP adres heeft.

Host

Een host is een apparaat dat een eindpunt voor communicatie op een netwerk is, kan de host gegevens of een service (zoals DNS) aan andere knooppunten leveren.

Afhankelijk van de topologie kan een switch of een router een host zijn. Alle hosts zijn ook knooppunten. Tot de voorbeelden behoren een computer, server of printer.

Computer-programma

Een computerprogramma bevat instructies die op een computer kunnen worden uitgevoerd.

Toepassing

Toepassingssoftware is een programma dat u helpt taken uit te voeren. Vaak worden ze door elkaar verwisselbaar genoemd, omdat ze vergelijkbaar zijn, maar niet alle programma's zijn toepassingen.

Best Practice

De aanbevolen methode voor het instellen van iets en het uitvoeren van uw netwerk.

Topologie

De fysieke manier waarop uw apparatuur is aangesloten. Een kaart van het netwerk.

Configureren

Dit heeft betrekking op de manier waarop de zaken worden opgezet. U kunt standaardinstellingen laten, de instellingen die vooraf worden ingesteld bij het aanschaffen van apparatuur, of u kunt configureren voor uw specifieke behoeften. Standaardinstellingen zijn de basisconfiguraties, vaak aanbevolen. Wanneer u op uw apparaat inlogt, kan er een Wizard Instellen zijn die u kan begeleiden wat u moet doen.

MAC-adres

Uniek identificatienummer voor elk apparaat. Wordt gericht op het fysieke apparaat en kan worden gedetecteerd met Bonjour, LLDP of CDP. Een switch houdt de MAC adressen bij op apparaten terwijl het met hen interageert en maakt een MAC-adrestabel. Dit helpt de switch te weten waar ze pakketjes informatie moeten routeren.

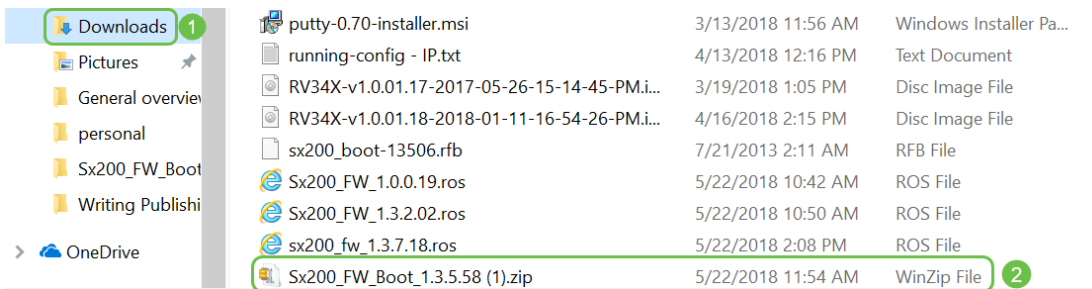
Open source

Een programma dat gratis toegankelijk is voor het publiek.

Zip-bestand

Een groep bestanden gecomprimeerd in één zip-bestand. Het wordt gebruikt wanneer u meerdere bestanden in één stap wilt overdragen. De ontvanger kan het zip-bestand openen en elk afzonderlijk openen. Een zip-bestand eindigt in *.zip*.

Als u een bestand ziet dat in een bestandsindeling eindigt in `.zip`, moet u dat bestand opheffen. Als u geen unzip-programma hebt, moet u er één downloaden. Online zijn er verschillende gratis opties. Nadat u een unzip-programma hebt gedownload, klikt u op **Downloads** en vervolgens vindt u het bestand `.zip` dat u moet opheffen.



Klik met de rechtermuisknop op de naam van het zip-bestand, er verschijnt een vergelijkbaar scherm. Draai de unzip software over en kies **Extract Here**. In dit voorbeeld wordt 7-Zip gebruikt.



Opdracht Line Interface (CLI)

Opdracht Line Interface (CLI): Soms wordt het terminaltype genoemd. Dit wordt gebruikt als een andere optie voor het kiezen van configuraties op apparaten zoals routers en switches. Als je ervaring hebt, kan dit een veel eenvoudigere manier zijn om dingen op te zetten omdat je niet door verschillende Web UI schermen hoeft te navigeren. De ondergang hiervan is dat je de opdrachten moet kennen en ze perfect moet invoeren. Omdat je een artikel voor beginners leest, zou CLI waarschijnlijk niet je eerste keuze moeten zijn.

Virtuele machine

De meeste machines hebben hogere mogelijkheden dan ze nodig hebben. U kunt een computer aanleveren om alles wat nodig is in de machine te houden om meerdere apparaten uit te voeren. Het probleem is dat als een deel omlaag gaat of opnieuw moet worden opgestart, ze allemaal volgen.

Als u VMware of Hyper-V installeert, kunt u software, web servers, e-mail servers, FindIT en meer op één computer laden. Een virtuele machine kan zelfs een ander besturingssysteem gebruiken. Ze zijn logisch onafhankelijk van elkaar. Elk voert de functies van een afzonderlijk apparaat uit zonder er een te zijn. Hoewel de hardware wordt gedeeld, wijst elke virtuele machine een deel van het fysieke beroep toe voor elk besturingssysteem. Dit kan geld, energie en ruimte besparen.

Cisco-tools die u kunt gebruiken

Cisco Business Dashboard (CBD)

Dit is een Cisco-gereedschap dat wordt gebruikt om netwerken te bewaken en onderhouden. CBD kan u helpen Cisco-apparaten in uw netwerk te identificeren, evenals andere behulpzame beheerfuncties.

Dit is een voordelig instrument als je dingen vanuit je huis runt of meerdere netwerken controleert. CBD kan op een virtuele machine worden uitgevoerd. Ga voor meer informatie over CBD naar de [Cisco Business Dashboard Support Site](#) of [Cisco Business Dashboard - Overzicht](#).

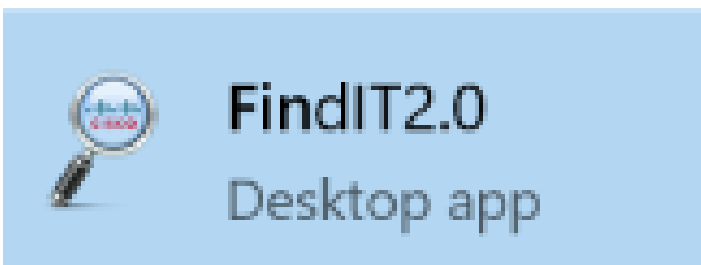
Hulpprogramma voor netwerkdetectie van FindIT

Dit eenvoudige gereedschap is zeer eenvoudig maar kan u helpen om snel de apparatuur van Cisco op uw netwerk te ontdekken. Cisco FindIT ontdekt automatisch alle ondersteunde Cisco Small Business-apparaten in hetzelfde lokale netwerksegment als uw pc.

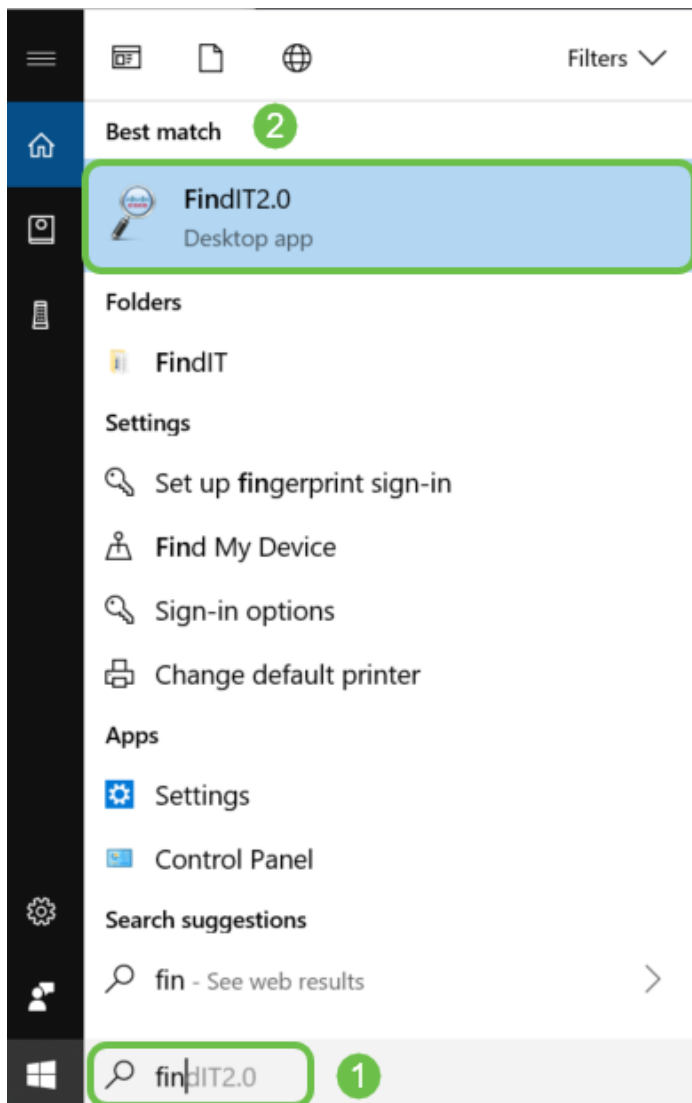
Klik op om meer te weten te komen en het [Cisco Small Business FindIT-netwerkdetectiehulpprogramma](#) te downloaden.

Klik op deze link om een artikel te lezen over [het installeren en instellen van het Cisco FindIT-hulpprogramma voor netwerkdetectie](#).

De toepassing ziet er zo uit voor Windows 10.



Nadat het is gedownload vindt u het hier in Windows 10.



AnyConnect (RV34x Series routers/VPN's)

Dit VPN wordt specifiek gebruikt met de RV34x-Series routers (en ondernemingen/grote bedrijfsapparatuur). De Cisco AnyConnect Secure Mobility Client biedt externe gebruikers een beveiligde VPN-verbinding. Het biedt externe eindgebruikers de voordelen van een Cisco Secure Socket Layer (SSL) VPN-client en ondersteunt ook toepassingen en functies die niet beschikbaar zijn op een browser-gebaseerde SSL VPN-verbinding. Deze kunnen worden aangesloten op de computer-infrastructuur van het bedrijf die wordt gebruikt door externe werkers. Deze kunnen worden aangesloten op de computer-infrastructuur van het bedrijf alsof ze fysiek aanwezig zijn, ook al is dat niet het geval. Dit draagt bij aan de flexibiliteit, mobiliteit en productiviteit van de werknemers. Clientlicenties zijn nodig om AnyConnect te gebruiken. Cisco AnyConnect is compatibel met de volgende besturingssystemen: Windows 7, 8, 8.1 en 10, Mac OS X 10.8 en later, en Linux Intel (x64).

Raadpleeg de volgende artikelen voor meer informatie:

- [Cisco AnyConnect Secure Mobility Client op een Windows-computer installeren](#)
- [Cisco AnyConnect Secure Mobility Client op een Mac Computer installeren](#)

De basisbeginselen van het uitwisselen van gegevens

Packet

In het voorzien van een netwerk, wordt de informatie verzonden in haakjes, genaamd pakketten. Als er verbindingsproblemen zijn, kunnen pakketten verloren gaan.

Latentie

Vertraging bij het verzenden van pakketten.

Redundantie

In een netwerk wordt redundantie zo ingesteld dat als een deel van het netwerk problemen heeft, het gehele netwerk niet faalt. Neem het een back-upplan als er iets gebeurt met de hoofdconfiguratie.

Protocols

Twee apparaten moeten een aantal van de zelfde te communiceren instellingen hebben. Zie het als een taal. Als de ene persoon maar Duits spreekt en de andere alleen Spaans, dan kunnen ze niet communiceren. Verschillende protocollen werken samen en er kunnen meerdere protocollen binnen elkaar worden verzonden. Protocollen hebben verschillende doelen; enkele voorbeelden worden hieronder opgesomd en kort beschreven .

Adressatieprotocollen

- **Session Initiation Protocol (SIP):** dit is het hoofdprotocol voor Voice-over-IP (VoIP), telefoons die via internet communiceren. Beide zijden van het netwerk moeten worden opgezet met behulp van hetzelfde protocol om te communiceren, zodat ze allebei SIP nodig hebben om de communicatie via VoIP te initiëren.
- **Dynamic Host Configuration Protocol (DHCP)** beheert een pool van beschikbare IP-adressen, en wijst deze toe aan hosts als zij zich bij het netwerk aansluiten.
- **Protocol voor adresoplossing (ARP):** Kaarten een dynamisch IP-adres aan een permanent fysiek MAC-adres in een LAN.
- **IPv4:** Dit is de meest gebruikelijke versie van IP die momenteel wordt gebruikt. Een IP-adres wordt geschreven als 4 series getallen (ook wel octetten genoemd), gescheiden door een periode tussen elke set. Elke set kan een getal tussen 0 en 255 zijn. Een voorbeeld van een IPv4-adres is 8.8.8.8, de openbare DNS-server bij Google. Er zijn meer apparaten dan unieke IP-adressen voor IPv4, zodat het duur kan zijn om een permanent openbaar IP-adres aan te schaffen.
- **IPv6:** In deze laatste versie worden 8 getallen gebruikt met een komma tussen elke set. Het gebruikt een hexadecimaal numeriek systeem, zodat er letters in het IP-adres kunnen staan. Een bedrijf kan IPv4- en IPv6-adressen tegelijkertijd laten draaien.

Aangezien we het hebben over IPv6, zijn er een paar belangrijke details te weten over dit adresseringsprotocol:

IPv6-afkortingen: Als alle getallen in verschillende sets nul zijn, kunnen twee kolonies op een rij deze sets vertegenwoordigen, kan deze afkorting slechts eenmaal worden gebruikt. Een van de IPv6-adressen bij Google is bijvoorbeeld 2001:4860:4860:888. Sommige apparaten gebruiken afzonderlijke velden voor alle acht delen van IPv6-adressen en kunnen de IPv6-afkorting niet accepteren. Als dat het geval is, zul je 2001:4860:4860:00:00:08:888.

Hexadecimaal: Een numeriek systeem met een basis 16 in plaats van basis 10, dat is wat we gebruiken in de dagelijkse wiskunde. De nummers 0-9 worden op dezelfde manier weergegeven. 10-15 worden vertegenwoordigd door de letters A-F.

Protocollen voor gegevensoverdracht

- **Transmission Control Protocol (TCP) en User Datagram Protocol (UDP):** Dit zijn twee manieren waarop gegevens worden getransporteerd. TCP vereist een verbinding, genaamd een handdruk van drie richtingen, alvorens gegevens te verzenden zodat soms een vertraging is. Als gegevens (pakketten) verloren gaan, zal het deze opnieuw verzenden. UDP is minder betrouwbaar, maar sneller. Vaak gebruiken spraak- en videobeelden UDP.
- **File Transfer Protocol (FTP):** Dit protocol wordt gebruikt om bestanden van een client naar een server over te brengen.
- **Hypertext Transfer Protocol (HTTP) vs. Hypertext Transfer Protocol Secure (HTTPS):** de algemene basis voor gegevenscommunicatie via het internet. Deze vinden u aan het begin van websites, geschreven als *http://* en *https://*. Plaatsen die beginnen met *https://* zijn veiliger om te gebruiken.
- **Routing Information Protocol (RIP):** Dit protocol bestaat al lange tijd. Er zijn drie versies, waarbij elke versie meer veiligheid en functionaliteit toevoegt. De routers delen routes met elkaar. Zijn doel is om loops te voorkomen door een maximum aantal "sprongen" van één router in het volgende te plaatsen. Andere, efficiëntere, protocollen voor routing omvatten **uitgebreid Interior Gateway Routing Protocol (IGMP)**, **Open Shortest Path First (OSPF)** en **Intermediate System to Intermediate System (IS-IS)**. Deze laatste drie schaal is beter dan RIP maar kan ingewikkelder worden opgezet.
- **Secure Shell (SSH):** een beveiligd kanaal dat een veilige route voor commando-lijnverkeer biedt. Het is een versleuteld protocol dat wordt gebruikt om met een externe server te communiceren. Veel extra technologieën zijn gebouwd rond SSH.

Detectieprotocollen

- **Cisco Discovery Protocol (CDP):** ontdekt informatie over andere Cisco-apparatuur die rechtstreeks is aangesloten en slaat die informatie op. **Bonjour** and **Link Layer Discovery Protocol (LLDP)** voert dezelfde functies uit en kan ook informatie krijgen over niet-Cisco-apparaten. De meeste apparaten van kleine bedrijven gebruiken LLDP.
- **Layer Link Discovery Protocol (LLDP):** Maakt een apparaat in staat om zijn identificatie, configuratie, en mogelijkheden aan aangrenzende apparaten bekend te maken die dan de gegevens in een Management Information Base (MIB) opslaan. De informatie die tussen de burens wordt gedeeld, helpt de tijd te beperken die nodig is om een nieuw apparaat aan het LAN (Local Area Network) toe te voegen en biedt ook details die nodig zijn om veel configuratieproblemen op te lossen. LLDP kan worden gebruikt in

scenario's waar u moet werken tussen apparaten die niet voor eigen rekening van Cisco zijn en apparaten die voor eigen rekening van Cisco zijn. De switch geeft alle informatie over de huidige LLDP status van poorten en u kunt deze informatie gebruiken om aansluitingsproblemen binnen het netwerk op te lossen. Dit is een van de protocollen die door netwerkzoektoepassingen zoals FindIT Network Management worden gebruikt om apparaten in het netwerk te ontdekken.

Protocollen identificeren

- **Domain Name System (DNS):** Zodra er een Full Qualified Domain Name (FQDN) is toegewezen aan een IP-adres, wordt deze in een database gezet. Bijvoorbeeld, wanneer u *www.google.com* zoekt kunt u de website naam, en de gegevensbestand zoekacties naar het gebied binnendringen en u daar door hun IP adres krijgen. Uw **Internet Service Provider (ISP)** gebruikt hun DNS-server als standaard en is al geconfigureerd. U kunt dit echter handmatig wijzigen indien u bij het gebruik van internet een trage snelheid vindt.
- **Dynamische DNS:** wordt ook DDNS genoemd en werkt automatisch een server in de DNS bij met de actieve configuratie van de hostnamen, adressen of andere relevante informatie. Met andere woorden, DDNS kent een vaste domeinnaam aan een dynamisch WAN IP-adres toe. Hiermee bespaart u de kosten van het aanschaffen van een permanent IP-adres.
- **Internet Protocol (IP):** IP-adressen zijn unieke identificatoren die het verzenden en ontvangen van gegevens tussen hosts op internet mogelijk maken. Dit wordt bereikt via openbare internetadressen, waarvoor een aankoop bij een ISP vereist is.
- **Media Access Control (MAC-adres):** elk apparaat heeft een unieke identicator die erop is aangesloten. Dit verandert niet. Het is goed om uw MAC-adres te kennen wanneer u een netwerk maakt en problemen oplossen. Het bevindt zich gewoonlijk op het apparaat en bevat letters en cijfers. Switches houden MAC-adressen van apparaten bij en maken een MAC-adrestabel.

Protocollen voor probleemoplossing

- **Ping:** ping is een veel gebruikte methode om problemen op te lossen. Pingel stuurt CIP echo-berichten naar een IP-adres. Er wordt een bericht ontvangen in ruil. Een succesvolle reactie laat bidirectionele fysieke connectiviteit zien. Het is een manier om te zien of een netwerkgegevenspakket aan een adres zonder kwesties kan worden verdeeld.
- **Internet Control Message Protocol (ICMP):** Berichten over fouten en operationele informatie. Wanneer u een PING-test doet, wordt een ICMP-echo-bericht naar de bestemming gestuurd. Een succesvolle verbinding krijgt een reactie van dat apparaat.

Server

Een computer of een programma op een computer dat services levert aan andere computers. Een server kan virtueel zijn of zelfs een toepassing. Er kunnen meerdere servers zijn op één apparaat. De servers kunnen met elkaar delen. Ze kunnen gebruikt worden met Windows, Mac of Linux.

Webservers - formaat en huidige webpagina's voor webbrowsers

Bestandsservers - delen bestanden en mappen met gebruikers op een netwerk

E-mailservers - e-mails verzenden, ontvangen en opslaan

DNS-servers - vertaalt u gebruikersvriendelijke namen zoals www.cisco.com naar IP-adres 173.37.145.84, bijvoorbeeld

Instant Messaging Server-servers - controleert de stroom van Instant-berichten en beheert deze (Jabber, Skype)

QoS-kwaliteit (Quality of Service)

Deze instellingen zijn ingesteld om er zeker van te zijn dat voorrang wordt gegeven aan verkeer op een netwerk, meestal spraak of video, aangezien dit vaak het opmerkelijkst is wanneer er pakketvertraging (data) is.

De basisbeginselen van een internetverbinding

Internet Service Provider (ISP)

U hebt een ISP nodig om toegang te hebben tot het internet op uw netwerk. Er zijn veel opties om uit te kiezen voor verbindingssnelheden, evenals een verscheidenheid aan prijzen om aan de behoeften van uw bedrijf te voldoen. Naast toegang tot het internet biedt een ISP e-mail, webpagina's en meer.

Web browser

Een toepassing die op je apparaat komt. Er zijn andere die je kunt downloaden. Nadat het is gedownload kunt u het IP-adres of de website openen en invoeren waar u via het internet naar wilt gaan. Enkele voorbeelden van webbrowsers zijn:

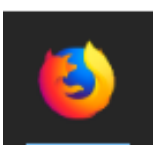
Microsoft Edge



Chroom



Firefox



en Safari.



Als je niet in staat bent om iets te openen of als je andere navigatieproblemen hebt, is het gemakkelijk om een andere webbrowser te openen en het opnieuw te proberen.

Unified Resource Locator (URL)

In een webbrowser typt u doorgaans de naam van een website die u wilt benaderen, dat is de URL, hun webadres. Elke URL moet uniek zijn. Een voorbeeld van een URL is <https://www.cisco.com>.

Standaard gateway

Dit is de router die door het lokale netwerkverkeer wordt gebruikt als stap naar de Internet Service Provider (ISP) en het internet. Met andere woorden, deze router verbindt u met andere apparaten buiten uw gebouw en over het internet.

Firewall

Een firewall is een apparaat voor netwerkbeveiliging dat inkomend en uitgaand netwerkverkeer controleert en beslist of hij specifiek verkeer toestaat of blokkeert op basis van een gedefinieerde reeks beveiligingsregels, genaamd Access Control Lists (ACL's).

Firewalls zijn al tientallen jaren de eerste verdedigingslinie in de netwerkbeveiliging. Ze creëren een barrière tussen beveiligde en gecontroleerde interne netwerken die vertrouwd en onbetrouwbaar kunnen worden buiten netwerken, zoals het internet.

Een firewall kan hardware, software of beide zijn.

Voor meer informatie, controleer of [de Firewall-instellingen configureren op de RV34x Series router](#).

Toegangscontrolelijsten (ACL's)

Lijsten die verkeer van en naar bepaalde gebruikers blokkeren of toestaan. Toegangsregels kunnen zo worden ingesteld dat ze de hele tijd of op basis van een vastgesteld schema van kracht zijn. Een toegangsregel is op basis van verschillende criteria ingesteld om toegang tot het netwerk toe te staan of te weigeren. De toegangsregel is gepland op basis van het tijdstip waarop de toegangsregels op de router moeten worden toegepast. Deze worden ingesteld onder beveiligingsinstellingen of firewalls. Een bedrijf wil bijvoorbeeld werknemers ervan weerhouden om live sporten te streamen of tijdens de kantooruren verbinding te maken met Facebook.

Bandbreedte

De hoeveelheid gegevens die in een bepaalde periode van het ene punt naar het andere kan worden verzonden. Als u een internetverbinding hebt met een grotere bandbreedte, kan het netwerk gegevens veel sneller verplaatsen dan een internetverbinding met een lagere bandbreedte. Streamingvideo neemt veel meer bandbreedte in dan het verzenden van bestanden. Als u ontdekt dat er een vertraging is wanneer u tot een webpagina toegang heeft, of vertraging in het streamen van video, kunt u de bandbreedte in uw netwerk moeten verhogen.

Ethernet-kabel

De meeste apparaten in een netwerk hebben Ethernet poorten. Ethernet-kabels zijn de stekkers die erin zitten voor een bekabelde verbinding. Beide uiteinden van de RJ45-kabel zijn gelijk en lijken op de oude telefoonaansluitingen. Ze kunnen worden gebruikt om apparaten aan te sluiten en verbinding te maken met internet. De kabels verbinden apparaten voor de toegang tot internet en het delen van bestanden. Sommige computers hebben een Ethernet-adapter nodig, omdat zij mogelijk geen Ethernet-poort bieden.

Netwerken en hoe ze met elkaar passen

Local Area Network (LAN)

Een netwerk dat zo groot kan zijn als meerdere gebouwen of zo klein als een huis. Iedereen die is aangesloten op het LAN heeft dezelfde fysieke locatie en is verbonden met dezelfde router.

In een lokaal netwerk wordt elk apparaat zijn eigen unieke interne IP-adres toegewezen. Ze volgen een patroon van 10.x.x, 172.16.x.x - 172.31.x.x of 192.168.x.x. Deze adressen zijn alleen zichtbaar binnen een netwerk, tussen apparaten, en worden als privé beschouwd. Er zijn miljoenen locaties die dezelfde pool van interne IP-adressen hebben als uw bedrijf. Het maakt niet uit, ze worden alleen gebruikt binnen hun eigen privénetwerk, dus er is geen conflict. Omdat de apparaten in het netwerk met elkaar moeten communiceren, zouden zij allen het zelfde patroon moeten volgen als de andere apparaten, op zelfde net moeten zijn, en uniek zijn. U zou nooit een van deze adressen in dit patroon als een openbaar IP-adres moeten zien, aangezien ze alleen voor privé LAN-adressen zijn gereserveerd.

Al deze apparaten verzenden gegevens via een standaardgateway (een router) om op internet te komen. Wanneer de standaardgateway de informatie ontvangt, moet hij Netwerkadresomzetting (NAT) uitvoeren en het IP-adres wijzigen omdat alles dat via het internet wordt gedaan een uniek IP-adres nodig heeft.

Wide Area Network (WAN)

Een Wide Area Network (WAN) is een netwerk dat wordt verspreid, soms wereldwijd. Veel LAN's kunnen worden aangesloten op één WAN.

Alleen WAN-adressen kunnen via het internet met elkaar praten. Elk WAN-adres moet uniek zijn. Om apparaten in een netwerk op het internet informatie te kunnen verzenden en ontvangen moet u een router aan de rand van uw netwerk (een standaardgateway) hebben die NAT kan uitvoeren.

Klik om te lezen [Configureer de toegangsregels in een RV34x Series router](#).

Netwerkadresomzetting (NAT)

Een router ontvangt een WAN-adres via een Internet Service Provider (ISP). De router komt met NAT-mogelijkheid die verkeer verlaat vanuit het netwerk, het privéadres vertaalt naar het openbare WAN-adres en het via het internet stuurt. Het doet het omgekeerde wanneer je verkeer ontvangt. Dit werd ingesteld omdat er niet genoeg permanente IPv4 adressen beschikbaar zijn voor alle apparaten in de wereld.

Het voordeel van NAT is dat het extra beveiliging biedt door het gehele interne netwerk effectief te verbergen achter dat ene unieke openbare IP-adres. De interne IP-adressen blijven vaak hetzelfde, maar als ze een tijdje niet op de stekker zijn aangesloten, op een bepaalde manier zijn geconfigureerd of als ze naar een fabrieksstandaard worden hersteld, is dat mogelijk niet het geval.

Statische NAT

U kunt het interne IP-adres configureren om hetzelfde te blijven, door het statische DHCP-configuratieschema (Dynamic Host Configuration Protocol) op de router te configureren. Openbare IP-adressen blijven evenmin hetzelfde, tenzij u betaalt om een statisch openbaar IP-adres door uw ISP te hebben. Veel bedrijven betalen voor deze service, zodat hun werknemers en klanten een betrouwbaarder verbinding hebben met hun servers (web, mail, VPN, enzovoort), maar deze kan duur zijn.

Statische NAT-kaarten een één-op-één vertaling van de privé IP-adressen aan de openbare IP-adressen toe. Het creëert een vaste vertaling van privéadressen naar de openbare adressen. Dit betekent dat je een gelijk aantal openbare adressen nodig hebt als privéadressen. Dit is handig wanneer een apparaat van buiten het netwerk toegankelijk moet zijn.

Klik op de [knoppen RV160 en RV260 om NAT en Static NAT te](#) lezen.

CGNAT

Carrier Grade NAT is een vergelijkbaar protocol dat meerdere klanten toestaat om hetzelfde IP-adres te gebruiken.

VLAN

Met een Virtual Local Area Network (VLAN) kunt u een Local Area Network (LAN) logisch segmenteren in verschillende broadcastdomeinen. In scenario's waarbij gevoelige gegevens via een netwerk kunnen worden doorgegeven, kunnen VLAN's

worden opgezet om data beter te beveiligen door een broadcast aan een specifiek VLAN toe te wijzen. Alleen gebruikers die tot een VLAN behoren kunnen de data op dat VLAN benaderen en bewerken. VLAN's kunnen ook worden gebruikt om prestaties te verbeteren door de behoefte te verminderen om broadcast en multicast pakketten naar onnodige bestemmingen te verzenden.

Een VLAN wordt vooral gebruikt om groepen onder de hosts te vormen, ongeacht de plaats waar de hosts fysiek is gelegen. Zodoende verbetert een VLAN veiligheid met de hulp van groepsvorming onder de hosts. Wanneer een VLAN wordt gecreëerd, heeft het geen effect tot dat VLAN aan minstens één poort handmatig of dynamisch is verbonden. Eén van de meest gebruikelijke redenen om een VLAN op te zetten is het instellen van een afzonderlijk VLAN voor spraak, en een afzonderlijk VLAN voor gegevens. Dit leidt de pakketten voor beide types van gegevens ondanks het gebruiken van het zelfde netwerk.

Voor meer informatie, zou u [de Beste praktijken en de Tips van VLAN voor het Zaken van Cisco moeten](#) lezen.

Subnetwerk

Vaak genoemd Subnetwork, zijn subnetwerken onafhankelijke netwerken binnen een IP netwerk.

SSID

De Service Set Identifier (SSID) is een uniek identificatiemiddel dat draadloze klanten met alle apparaten in een draadloos netwerk kunnen verbinden of delen. Het is hoofdlettergevoelig en mag niet meer dan 32 alfanumerieke tekens bevatten. Dit wordt ook wel draadloze netwerknaam genoemd.

Virtual Private Networks (VPN's)

De technologie is geëvolueerd en er wordt vaak buiten het kantoor gehandeld. Apparaten zijn mobieler, en werknemers werken vaak vanuit hun eigen woning of tijdens het reizen. Dit kan enige veiligheidskwetsbaarheden veroorzaken. Een Virtual Private Network (VPN) is een goede manier om externe medewerkers op een veilig netwerk aan te sluiten. Een VPN kan een externe host gebruiken alsof deze zich op hetzelfde lokale netwerk bevindt.

Er wordt een VPN ingesteld om beveiligde gegevensoverdracht mogelijk te maken. Er zijn verschillende opties voor het instellen van een VPN en de manier waarop de gegevens worden versleuteld. VPN's gebruiken Secure Socket Layer (SSL), Point to Point Tunneling Protocol (PPTP) en Layer 2 Tunneling Protocol.

Een VPN-verbinding stelt gebruikers in staat om toegang te krijgen tot, gegevens te verzenden en te ontvangen van en naar een privaat netwerk door middel van een openbaar of gedeeld netwerk zoals het internet, maar toch een beveiligde verbinding met een onderliggende netwerkinfrastructuur te waarborgen om het particuliere

netwerk en de bijbehorende bronnen te beschermen.

Een VPN-tunnel stelt een privaat netwerk in dat gegevens veilig kan verzenden met behulp van encryptie en verificatie. Bedrijven gebruiken vooral een VPN-verbinding omdat die nodig en nuttig is om hun werknemers toegang te geven tot hun privénetwerk, zelfs als ze zich niet binnen het kantoor bevinden.

Een VPN-verbinding kan tussen de router en een eindpunt worden ingesteld nadat de router voor een internetverbinding is geconfigureerd. De VPN-client is volledig afhankelijk van de instellingen van de VPN-router om een verbinding op te zetten.

Een VPN ondersteunt site-to-site VPN voor een gateway-naar-gateway tunnel. Bijvoorbeeld, kan een gebruiker een VPN tunnel op een tak-plaats vormen om aan de router op een bedrijfsplaats te verbinden, zodat de kantorsite veilig tot het bedrijfsnetwerk kan toegang hebben. In een site-to-site VPN-verbinding kan iedereen de communicatie starten. Deze configuratie heeft een constante versleutelde verbinding.

IPsec VPN ondersteunt client-to-server VPN voor een host-to-gateway-tunnel. De client-naar-server-VPN is handig bij de verbinding van Laptop/PC van thuis naar een bedrijfsnetwerk via de VPN-server. In dit geval kan alleen de client de verbinding openen.

Klik om [Cisco Business VPN - Overzicht en beste praktijken](#) te lezen.

Certificaten

Een beveiligde stap in het opzetten van een VPN is het verkrijgen van een certificaatinstantie (CA). Dit wordt gebruikt voor authenticatie. Certificaten worden aangeschaft op elk aantal locaties van derden. Het is een officiële manier om te bewijzen dat je site veilig is. De CA is in wezen een vertrouwde bron die verifieert dat u een legitiem bedrijf bent en kan worden vertrouwd. Voor een VPN hebt u alleen een lagere certificering nodig tegen minimale kosten. U wordt uitgecheckt door de CA en zodra ze uw informatie hebben geverifieerd, geven ze het certificaat aan u af. Dit certificaat kan als bestand op uw computer worden gedownload. U kunt dan naar uw router (of VPN-server) gaan en het daar uploaden.

Clients hebben doorgaans geen certificaat nodig om een VPN te gebruiken; het is enkel voor verificatie door de router . Een uitzondering hierop is OpenVPN, waarvoor een client-certificaat vereist is.

Veel kleine bedrijven kiezen ervoor om een wachtwoord of een vooraf gedeelde sleutel te gebruiken in plaats van een certificaat voor eenvoud. Dit is minder veilig maar kan zonder kosten worden opgezet.

Sommige artikelen over dit onderwerp waar je van zou kunnen genieten:

- [Certificaat \(Importeren/Exporteren/Generate CSR\) op RV160 en RV260 Series router](#)
- [Vervang het standaard zelfgetekende certificaat met een SSL-certificaat van een derde partij op de RV34x Series router](#)
- [Certificaten beheren op RV34x Series router](#)

Vooraf gedeelde sleutel (PSK)

Dit is een gedeeld wachtwoord, dat wordt besloten en gedeeld vóór de configuratie van een VPN en dat kan worden gebruikt als alternatief voor het gebruik van een certificaat. Een PSK kan zijn wat je wilt, het moet gewoon passen op de site en met de klant wanneer ze op hun computer als klant zijn ingesteld. Houd in gedachten, afhankelijk van het apparaat, kunnen er verboden symbolen zijn die u niet kunt gebruiken.

Sleutellevensduur

Hoe vaak verandert het systeem de toets. Deze instelling moet ook hetzelfde zijn als de externe router.

Conclusie

Daar heb je het, je hebt nu veel basiselementen om je op weg te krijgen.

Als je meer wilt leren, kijk dan naar deze links!

[Beste praktijken voor het instellen van statische IP-adressen Cisco Business VPN - Overzicht en beste praktijken VLAN-beste praktijken en -beveiligingstips voor Cisco Business-routers](#) [Internet Backup - Windows Internet Backup - Mac Inloggen op een Switch](#)