Novedad para Cisco Business: Glosario de equipos y redes básicas

Objetivo

El objetivo de este documento es familiarizar a los principiantes con los equipos Cisco Business (Small Business) y algunos términos generales que debe conocer. Los temas incluyen Hardware Available (Hardware disponible), Términos comerciales de Cisco, Términos generales de la red, Herramientas de Cisco, Los fundamentos del intercambio de datos, Los fundamentos de una conexión a Internet y las redes y Cómo encajan juntas.

Introducción

¿Está empezando a configurar su red con equipos de Cisco? Puede ser abrumador entrar en todo el nuevo mundo de configuración y mantenimiento de una red. Este artículo está aquí para ayudarle a familiarizarse con algunos de los aspectos básicos. Cuanto más sepa, menos intimidante será.

Hardware disponible para Cisco Business

Router

Los routers conectan varias redes juntas, así como rutean los datos donde deben ir. También conectan ordenadores de esas redes a Internet. Los routers permiten que todos los ordenadores conectados en red compartan una única conexión a Internet, lo que ahorra dinero.

Un router actúa como dispatcher. Analiza los datos que se envían a través de una red, elige la mejor ruta para que los datos viajen y los envía en su camino.

Los routers conectan su empresa con el mundo, protegen la información de las amenazas de seguridad e incluso pueden decidir qué ordenadores tienen prioridad sobre otros.

Además de estas funciones básicas de red, los routers incorporan funciones adicionales para facilitar o aumentar la seguridad de las redes. Según sus necesidades, por ejemplo, puede elegir un router con un firewall, una red privada virtual (VPN) o un sistema de comunicaciones con protocolo de Internet (IP).

Los routers empresariales de Cisco más recientes incluyen las series RV160, RV260, RV340 y RV345.

Switch

Los switches son la base de la mayoría de las redes empresariales. Un switch actúa como controlador, conectando ordenadores, impresoras y servidores a una red de un edificio o un campus.

Los switches permiten que los dispositivos de la red se comuniquen entre sí, así como con otras redes, lo que crea una red de recursos compartidos. Mediante el uso compartido de la información y la asignación de recursos, los switches ahorran dinero y aumentan la productividad.

Hay dos tipos básicos de switches entre los que elegir como parte de sus conceptos básicos de red: administrado y no administrado.

> Un switch no administrado funciona de forma inmediata pero no se puede configurar. Los equipos de red doméstica suelen ofrecer switches no gestionados.
> Se puede configurar un switch administrado. Puede supervisar y ajustar un switch administrado de forma local o remota, lo que le proporciona un mayor control del tráfico de red y del acceso.

Para obtener más información sobre los switches, consulte el Glosario de Términos de Switches.

Los switches más recientes incluyen las series CBS110, CBS220, CBS250 y CBS350 del switch empresarial de Cisco.

Si desea conocer las diferencias entre los switches CBS, consulte

Punto de acceso inalámbrico

Un punto de acceso inalámbrico permite a los dispositivos conectarse a la red inalámbrica sin cables. Una red inalámbrica facilita la conexión de nuevos dispositivos y proporciona una asistencia flexible a los trabajadores móviles.

Un punto de acceso actúa como amplificador de la red. Mientras que un router proporciona el ancho de banda, un punto de acceso amplía ese ancho de banda para

que la red admita muchos dispositivos, y esos dispositivos pueden acceder a la red desde lejos.

Sin embargo, un punto de acceso no se limita simplemente a ampliar la red Wi-Fi. También puede proporcionar datos útiles sobre los dispositivos de la red, proporcionar seguridad proactiva y servir a muchos otros fines prácticos.

Los puntos de acceso inalámbricos más recientes, Cisco Business Wireless, incluyen los modelos AC140, AC145 y AC240, que permiten una red de malla inalámbrica. Si no está familiarizado con las redes inalámbricas de malla, puede leer más en Bienvenido a Cisco Business Wireless Mesh Networking o Preguntas frecuentes (FAQ) para una Cisco Business Wireless Network.

Si desea conocer algunos términos comunes con los puntos de acceso inalámbricos, consulte el Glosario de términos WAP.

Teléfono multiplataforma

Los teléfonos MPP proporcionan comunicación de voz sobre IP (VoIP) mediante el protocolo de inicio de sesión (SIP). Esto elimina la necesidad de las líneas telefónicas tradicionales, lo que hace que los teléfonos sean más portátiles dentro de la empresa. Con VoIP, un teléfono utiliza una infraestructura de red existente y una conexión a Internet en lugar de costosas líneas T1. Esto permite administrar más llamadas con menos 'líneas'. Otras opciones beneficiosas incluyen poner llamadas en espera, aparcar llamadas, transferir llamadas, etc. Algunos modelos permiten la comunicación de vídeo además de VoIP.

Los teléfonos MPP están diseñados para que se asemejen a un teléfono normal y se utilizan únicamente con ese fin, pero básicamente son un ordenador y forman parte de la red. Los teléfonos MPP requieren el servicio de un proveedor de servicios de telefonía por Internet (ITSP) o de un servidor de control de llamadas de IP Private Branch Exchange (PBX). WebEx Calling, Ring Central y Verizon son ejemplos de un ITSP. Algunos ejemplos de servicios PBX IP que funcionan con teléfonos Cisco MPP incluyen las plataformas Asterisk, Centile y Metaswitch. Muchas funciones de estos teléfonos se programan específicamente a través de proveedores externos (como FreePBX), por lo que los procesos (aparcamiento, acceso al buzón de voz, etc.) pueden variar.

Los teléfonos Cisco Business MPP más recientes incluyen las series 6800, 7800 y 8800.

A la que se hace referencia habitualmente en el negocio de Cisco

Guía de administración y guía de inicio rápido

Estos son dos recursos diferentes que se pueden buscar para obtener información

muy detallada sobre su producto y sus características. Al realizar una búsqueda en un sitio o en la Web con el número de modelo, puede agregar uno u otro para ver estas guías más largas.

Configuración predeterminada

Los dispositivos vienen con la configuración predeterminada preseleccionada. A menudo, son las configuraciones más comunes que un administrador elegiría. Puede cambiar los parámetros para adaptarlos a sus necesidades.

Nombre de usuario y contraseña predeterminados

En equipos Cisco Business anteriores, el valor predeterminado era *admin* tanto para el nombre de usuario como para la contraseña. Ahora, la mayoría tiene un valor predeterminado de *cisco* tanto para el nombre de usuario como para la contraseña. En los teléfonos de voz sobre IP (VoIP), debe iniciar sesión como *administrador* para cambiar muchas de las configuraciones. Se recomienda encarecidamente cambiar la contraseña para que sea más compleja por motivos de seguridad.

Direcciones IP predeterminadas

La mayoría de los equipos de Cisco incluyen direcciones IP predeterminadas para routers, switches y puntos de acceso inalámbricos. Si no puede recordar la dirección IP y no tiene una configuración especial, puede utilizar un clip abierto para pulsar el botón de reinicio del dispositivo durante al menos 10 segundos. Se restablecerán los parámetros predeterminados. Si el switch o WAP no está conectado a un router con DHCP activado y está conectado directamente al switch o WAP con el ordenador, estas son las direcciones IP predeterminadas.

La dirección IP predeterminada de un router Cisco Business es 192.168.1.1.
La dirección IP predeterminada para un switch Cisco Business es 192.168.1.254.
La dirección IP predeterminada para un punto de acceso inalámbrico (AP) Small Business es 192.168.1.245. No hay ninguna dirección IP predeterminada para los nuevos puntos de acceso inalámbricos de malla.

Restablecer a los valores por defecto de fábrica

Es posible que llegue el momento en el que desee restablecer los parámetros predeterminados de fábrica del router, el conmutador o el punto de acceso inalámbrico de Cisco Business y comenzar desde el principio. Esto resulta útil cuando se mueve el equipo de una red a otra o como último recurso cuando no se puede resolver un problema de configuración. Al restablecer los parámetros predeterminados de fábrica, perderá todas las configuraciones.

Puede realizar copias de seguridad de las configuraciones para que pueda restaurarlas después de un restablecimiento de fábrica. Haga clic en los siguientes enlaces para obtener más información:

- Reiniciar o restaurar los parámetros predeterminados de fábrica del router serie RV34x a través de la utilidad basada en Web
- Copia de seguridad y restauración o intercambio de firmware en un switch
- Descargar, realizar copias de seguridad, copiar y eliminar archivos de configuración en un punto de acceso inalámbrico
- Administrar los archivos de configuración en el punto de acceso WAP125 o WAP581

Si no realiza una copia de seguridad de la configuración, deberá volver a configurar el dispositivo desde el principio para asegurarse de que dispone de los detalles de la conexión. La mayoría de los modelos cuentan con un artículo en el que se detallan los pasos que se deben seguir para realizar un reinicio, pero la forma más sencilla de hacerlo es utilizar un clip abierto y pulsar el botón de reinicio del dispositivo durante al menos 10 segundos. Esto no se aplica a los teléfonos MPP, así que desprotéjase Restablecer un teléfono IP de Cisco para obtener más información.

Interfaz de usuario web (UI)

Todos los equipos de Cisco Business incluyen una interfaz de usuario web, excepto los switches no gestionados serie 100.

Este tipo de interfaz, que se muestra en la pantalla, muestra opciones para la selección. No necesita saber ningún comando para navegar por estas pantallas. La interfaz de usuario web también se denomina a veces interfaz gráfica de usuario (GUI), interfaz basada en web, guía basada en web, utilidad basada en web o utilidad de configuración web.

Una de las formas más sencillas de cambiar la configuración de un dispositivo es a través de la interfaz de usuario web. La interfaz de usuario Web proporciona al administrador una herramienta que contiene todas las características posibles que se pueden cambiar para modificar el rendimiento de un dispositivo.

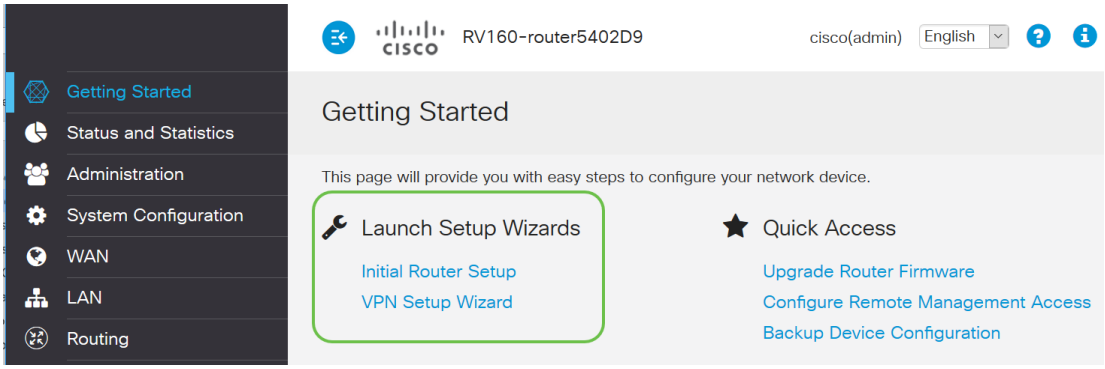
Después de iniciar sesión en un dispositivo Cisco, verá una pantalla de interfaz de usuario web que incluye un panel de navegación en el lado izquierdo. Contiene una lista de las funciones de nivel superior del dispositivo. El panel de navegación también se denomina a veces árbol de navegación, barra de navegación o mapa de navegación.

Los colores de esta página pueden variar, así como las funciones de nivel superior, según el equipo y la versión del firmware.

Asistente de configuración

Se trata de una pantalla interactiva por la que navegará cuando inicie sesión en un dispositivo Cisco Small Business por primera vez y, posiblemente, después. Puede ser una forma estupenda de ponerle en marcha su red. Hay varias configuraciones predeterminadas preseleccionadas que se pueden cambiar. Algunos dispositivos incluyen más de un asistente de configuración. En este ejemplo se muestran dos asistentes de configuración, *Configuración inicial del router* y *Asistente de*

configuración de VPN.



Es de propiedad exclusiva de Cisco.

Desarrollado específicamente y propiedad de Cisco. Por ejemplo, Cisco Discovery Protocol (CDP) es propiedad de Cisco. Por lo general, los protocolos propiedad de Cisco solo se pueden utilizar en dispositivos Cisco.

Modelos de una serie

Cisco ofrece a los propietarios de pequeñas empresas muchos modelos diferentes para adaptarse a las necesidades de su empresa. A menudo, se ofrecerá un modelo con diferentes funciones, número de puertos, alimentación a través de Ethernet o incluso inalámbrica. Si hay varios modelos en una serie, Cisco pondrá una x en lugar del número o letra que varía entre los modelos, pero la información se aplica a todos en esa serie. Por ejemplo, los routers RV340 y RV345 se refieren a la serie RV34x. Si un dispositivo tiene una P al final, ofrece Power over Ethernet. Si el nombre de un dispositivo finaliza en W, ofrece funciones inalámbricas. En general, cuanto mayor sea el número del modelo, mayores serán las capacidades del dispositivo. Para ver detalles sobre esto, consulte los siguientes artículos:

- Timbre del descodificador del producto - Router
- Decodificador de ID de producto - Switch
- Timbre del descodificador del producto - WAP
- Decodificador del modelo inalámbrico Cisco Business (inalámbrico de malla)

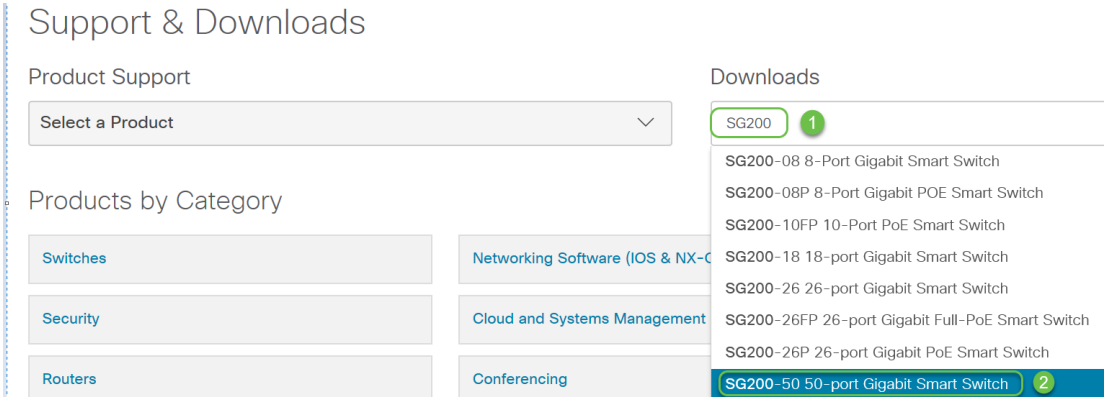
Firmware

También conocido como imagen. El programa que controla las operaciones y la funcionalidad del dispositivo.

Actualización del firmware

La actualización del firmware es esencial para lograr un rendimiento óptimo en todos los dispositivos. Es muy importante instalar actualizaciones cuando se lanzan. Cuando Cisco lanza una actualización de firmware, a menudo contienen mejoras como nuevas funciones o una corrección de errores que puede causar una vulnerabilidad de seguridad o un problema de rendimiento.

Vaya a Soporte de Cisco e ingrese el nombre del dispositivo que necesita una actualización en *Descargas*. Debe aparecer un menú desplegable. Desplácese hacia abajo y elija el modelo específico que posee.



Sugerencia: al examinar varias versiones del firmware de Cisco, cada una sigue un formato de x.x.x.x. que se consideran cuatro octetos. Cuando hay una actualización menor, cambia el cuarto octeto. El tercer octeto cambia cuando es un cambio mayor. El segundo octeto significa un cambio importante. El primer octeto cambia si es una revisión completa.

Si desea obtener orientación, haga clic en este enlace para Descargar y actualizar firmware en cualquier dispositivo.

Este artículo tiene algunas ideas de solución de problemas en caso de que tenga problemas con una actualización del switch: Upgrade Firmware en un Switch de la Serie 200/300.

Términos generales de las redes

Una vez que disponga de su equipo, debería familiarizarse con algunos términos comunes de las redes.

Interfaz

Una interfaz es generalmente ese espacio entre un sistema y otro. Cualquier cosa que pueda comunicarse con el ordenador, incluidos los puertos. A una interfaz de red generalmente se le asigna una dirección IP local. Una interfaz de usuario permite al usuario interactuar con el sistema operativo.

Nodo

Término general para describir cualquier dispositivo que realiza una conexión o interacción dentro de una red, o puede enviar, recibir y almacenar información, comunicarse con Internet y tener una dirección IP.

Host

Un host es un dispositivo que es un terminal para las comunicaciones en una red, el host puede proporcionar datos o un servicio (como DNS) a otros nodos. Según la topología, un switch o un router pueden ser un host. Todos los hosts también son nodos. Algunos ejemplos son un ordenador, un servidor o una impresora.

Programa informático

Un programa informático lleva instrucciones que se pueden ejecutar en un equipo.

Aplicación

El software de aplicaciones es un programa que le ayuda a realizar tareas. A menudo se hace referencia a ellos indistintamente, ya que son similares, pero no todos los programas son aplicaciones.

Práctica recomendada

El método recomendado para configurar y ejecutar la red.

Topología

La forma física en la que se conecta el equipo. Un mapa de la red.

Configurar

Esto se refiere a cómo se configuran las cosas. Puede dejar los parámetros predeterminados, los que vienen preconfigurados al comprar el equipo o puede configurarlos según sus necesidades específicas. Los valores predeterminados son las configuraciones básicas, a menudo recomendadas. Cuando inicie sesión en el dispositivo, es posible que el asistente de configuración le indique qué hacer.

Dirección MAC

Identificador único para cada dispositivo. Se encuentra en el dispositivo físico y se puede detectar con Bonjour, LLDP o CDP. Un switch realiza un seguimiento de las direcciones MAC en los dispositivos a medida que interactúa con ellos y crea una tabla de direcciones MAC. Esto ayuda al switch a saber dónde enrutar los paquetes de información.

Código abierto

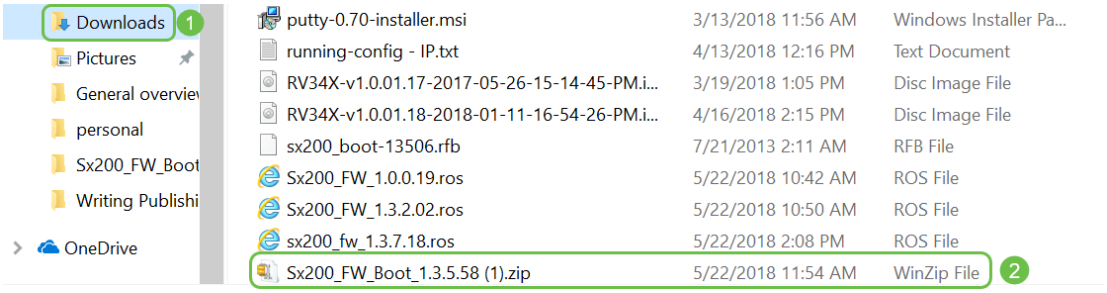
Un programa gratuito para el público.

Archivo Zip

Un grupo de archivos comprimidos en un archivo zip. Se utiliza cuando se desea transferir varios archivos en un solo paso. El receptor puede abrir el archivo zip y

acceder a cada uno por separado. Un archivo zip termina en *.zip*.

Si ve un archivo con un formato que termina en *.zip*, debe descomprimir ese archivo. Si no tiene un programa de descompresión, deberá descargar uno. Hay varias opciones gratuitas en línea. Una vez que haya descargado un programa unzip, haga clic en **Descargas** y busque el *.zip* archivo que necesita para descomprimir.



Haga clic con el botón derecho del ratón en el nombre del archivo zip; aparecerá una pantalla similar a esta. Pase el ratón sobre el software unzip y elija **Extraer aquí**. En este ejemplo, se utiliza 7-Zip.

Interfaz de Línea de Comandos (CLI)

Interfaz de línea de comandos (CLI): A veces se denomina terminal. Esto se utiliza como otra opción para elegir configuraciones en dispositivos como routers y switches. Si tiene experiencia, esta puede ser una forma mucho más sencilla de configurar las cosas, ya que no tendría que navegar por varias pantallas de la interfaz de usuario web. La caída de esto es que necesita conocer los comandos e ingresarlos perfectamente. Puesto que está leyendo un artículo para principiantes, es probable que CLI no deba ser la primera opción.

Máquina virtual

La mayoría de las máquinas cuentan con mayores capacidades de las que necesitan. Se puede aprovisionar un ordenador para que contenga todo lo necesario para ejecutar más de una máquina. El problema con esto es que si una parte se cae o necesita un reinicio, todos lo siguen.

Si instala VMware o Hyper-V, puede cargar software, servidores web, servidores de correo electrónico, FindIT y más en un ordenador. Una máquina virtual puede incluso utilizar un sistema operativo diferente. Son lógicamente independientes entre sí. Cada una de ellas realiza las funciones de un dispositivo independiente sin ser realmente uno. Aunque el hardware se comparte, cada máquina virtual asigna una parte del recurso físico para cada sistema operativo. Esto puede ahorrar dinero, energía y espacio.

Herramientas de Cisco que puede utilizar

Panel empresarial de Cisco (CBD)

Se trata de una herramienta de Cisco utilizada para supervisar y mantener las redes. El CBD puede ayudarle a identificar los dispositivos de Cisco en su red, así como otras útiles funciones de gestión.

Se trata de una herramienta útil si se ejecutan desde casa o se supervisa más de una red. CBD se puede ejecutar en una máquina virtual. Para obtener más información sobre el CBD, visite el sitio de soporte de Cisco Business Dashboard o Descripción general de Cisco Business Dashboard.

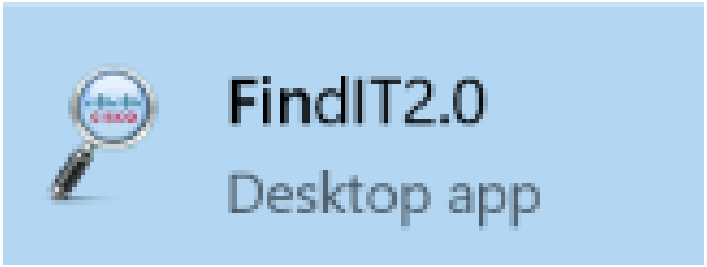
Utilidad de descubrimiento de red FindIT

Esta sencilla herramienta es muy básica, pero puede ayudarle a descubrir rápidamente los equipos de Cisco en su red. Cisco FindIT detecta automáticamente todos los dispositivos Cisco Small Business compatibles en el mismo segmento de red local que su PC.

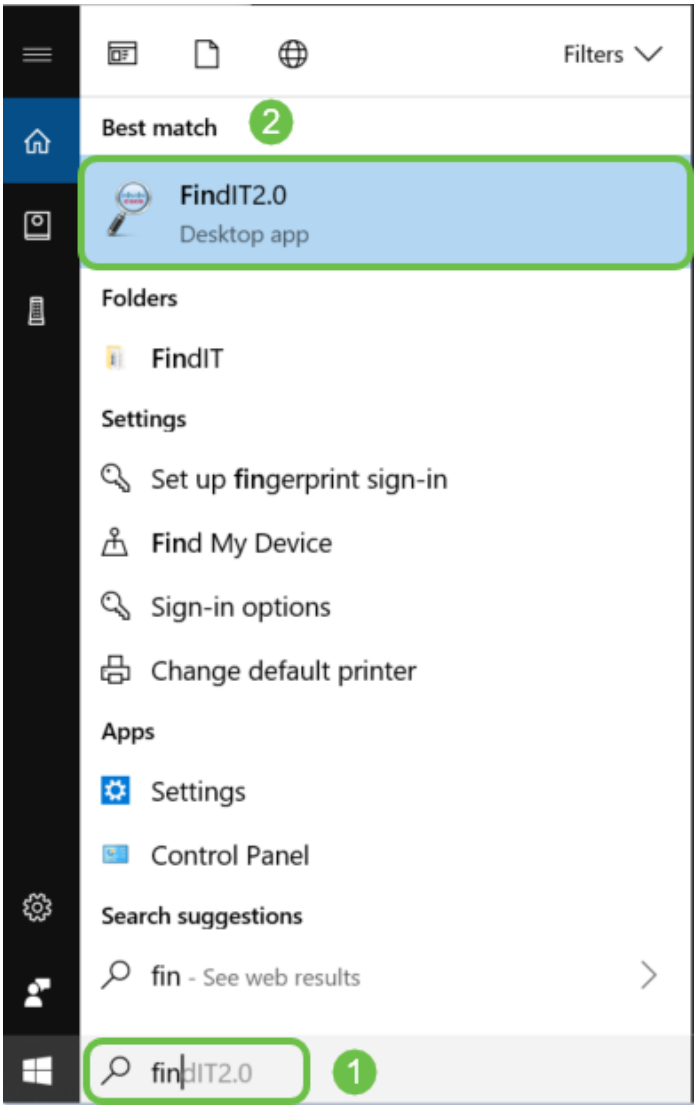
Haga clic para obtener más información y descargar la utilidad de descubrimiento de red de Cisco Small Business FindIT.

Haga clic en este enlace para leer un artículo sobre Cómo instalar y configurar Cisco FindIT Network Discovery Utility.

La aplicación se ve así en Windows 10.



Una vez descargado, puede encontrarlo aquí en Windows 10.



AnyConnect (RV34x Series Routers/VPN)

Esta VPN se utiliza específicamente con los routers de la serie RV34x (y con el equipo empresarial/de gran empresa). Cisco AnyConnect Secure Mobility Client proporciona a los usuarios remotos una conexión VPN segura. Proporciona a los usuarios finales remotos las ventajas de un cliente VPN de Cisco Secure Sockets Layer (SSL) y también admite aplicaciones y funciones que no están disponibles en una conexión VPN SSL basada en navegador. AnyConnect, que suelen utilizar los trabajadores remotos, les permite conectarse a la infraestructura informática corporativa como si estuvieran físicamente en la oficina, aunque no lo estén. Esto aumenta la flexibilidad, la movilidad y la productividad de los trabajadores. Se necesitan licencias de cliente para utilizar AnyConnect. Cisco AnyConnect es compatible con los siguientes sistemas operativos: Windows 7, 8, 8.1 y 10, Mac OS X 10.8 y posteriores, y Linux Intel (x64).

Consulte los siguientes artículos para obtener más información:

- Instalación de Cisco AnyConnect Secure Mobility Client en una computadora con Windows
- Instalación de Cisco AnyConnect Secure Mobility Client en una computadora Mac

Los fundamentos del intercambio de datos

Paquete

En la red, la información se envía en fragmentos, llamados paquetes. Si hay problemas de conexión, los paquetes pueden perderse.

Latencia

Retrasos en la transferencia de paquetes.

Redundancia

En una red, la redundancia se configura de modo que si parte de la red tiene problemas, no falle toda la red. Considere un plan de respaldo si algo le sucede a la configuración principal.

Protocolos

Dos dispositivos necesitan tener algunos de los mismos parámetros para comunicarse. Piensen en ello como un idioma. Si una persona solo habla alemán y la otra solo habla español, no podrá comunicarse. Diferentes protocolos funcionan juntos y puede haber varios protocolos siendo transmitidos entre sí. Los protocolos tienen propósitos diferentes; a continuación se enumeran algunos ejemplos y se describen brevemente.

Cómo abordar los protocolos

- **Protocolo de inicio de sesión (SIP):** Este es el protocolo principal para Voz sobre IP (VoIP), teléfonos que se comunican a través de Internet. Ambos lados de la red deben configurarse usando el mismo protocolo para comunicarse, por lo que ambos necesitarían SIP para iniciar la comunicación sobre VoIP.
- **El protocolo de configuración dinámica de host (DHCP)** administra un conjunto de direcciones IP disponibles, asignándolas a los hosts a medida que se unen a la red.
- **Protocolo de resolución de direcciones** (ARP): asigna una dirección IP dinámica a una dirección MAC física permanente en una LAN.
- **IPv4:** Esta es la versión más común de IP que se utiliza hoy en día. Una dirección IP se escribe como 4 conjuntos de números (también denominados octetos) separados por un punto entre cada conjunto. Cada conjunto puede ser un número entre 0 y 255. Un ejemplo de una dirección IPv4 es 8.8.8.8, que es el servidor DNS público de Google. Hay más dispositivos que direcciones IP únicas para IPv4, por lo que puede resultar costoso comprar una dirección IP pública permanente.
- **IPv6:** Esta última versión utiliza 8 conjuntos de números con dos puntos entre cada conjunto. Utiliza un sistema numérico hexadecimal, por lo que puede haber letras en la dirección IP. Una empresa puede tener direcciones IPv4 e IPv6 ejecutándose simultáneamente.

Dado que hablamos de IPv6, a continuación se proporcionan algunos detalles importantes sobre este protocolo de direccionamiento:

Abreviaturas de IPv6: Si todos los números de varios conjuntos son cero, dos puntos en una fila pueden representar esos conjuntos, esta abreviatura sólo se puede utilizar una vez. Por ejemplo, una de las direcciones IP IPv6 en Google es 2001:4860:4860::8888. Algunos dispositivos utilizan campos independientes para las ocho partes de las direcciones IPv6 y no pueden aceptar la abreviatura de IPv6. Si ese es el caso, introduciría 2001:4860:4860:0:0:0:0:8888.

Hexadecimal: Un sistema numérico que utiliza una base 16 en lugar de la base 10, que es lo que usamos en las matemáticas cotidianas. Los números 0-9 se representan igual. 10 a 15 están representados por las letras A a F.

Protocolos de transferencia de datos

- **Protocolo de control de transmisión (TCP) y protocolo de datagramas de usuario (UDP):** Éstas son dos maneras de transportar los datos. TCP requiere una conexión, denominada entrada en contacto en tres direcciones, antes de enviar los datos, por lo que a veces se produce un retraso. Si se pierden datos (paquetes), los enviará de nuevo. UDP es menos fiable, pero más rápido. A menudo, la voz y el vídeo utilizan UDP.
- **Protocolo de transferencia de archivos (FTP):** Este protocolo se utiliza para transferir archivos de un cliente a un servidor.
- **Protocolo de transferencia de hipertexto (HTTP) frente a protocolo de transferencia de hipertexto (HTTPS) seguro:** la base general para la comunicación de datos a través de Internet. Las encontrará al principio de los sitios web, escritos como *http://* y *https://*. Los sitios que comienzan con *https://* son más seguros de usar.
- **Protocolo de información de routing (RIP):** Este protocolo existe desde hace mucho tiempo. Hay tres versiones, cada una de las cuales añade más seguridad y funcionalidad. Los routers comparten rutas entre sí. Su objetivo es evitar loops estableciendo un número máximo de "saltos" de un router a otro. Otros protocolos más eficientes para el routing son el **protocolo de routing de gateway interior mejorado (EIGRP)**, el **protocolo de ruta más corta primero (OSPF)** y el **sistema intermedio a sistema intermedio (IS-IS)**. Estas últimas tres escalas mejor que RIP, pero pueden ser más complicadas de configurar.
- **Secure Shell (SSH):** canal seguro que proporciona una ruta segura para el tráfico de la línea de comandos. Se trata de un protocolo cifrado que se utiliza para comunicarse con un servidor remoto. Muchas tecnologías adicionales se basan en SSH.

Protocolos de detección

- **Cisco Discovery Protocol (CDP):** Detecta información sobre otros equipos de Cisco que están conectados directamente y guarda esa información. **Bonjour** y **Link Layer Discovery Protocol (LLDP)** realizan las mismas funciones y pueden obtener información sobre dispositivos que no son de Cisco también. La mayoría de los dispositivos de pequeñas empresas utilizan LLDP.
- **Protocolo de descubrimiento de enlaces de capa (LLDP):** Permite a un dispositivo anunciar su identificación, configuración y capacidades a los dispositivos vecinos que después almacenan los datos en una base de información de administración (MIB). La información compartida entre los vecinos ayuda a reducir el tiempo necesario para

agregar un nuevo dispositivo a la red de área local (LAN) y también proporciona los detalles necesarios para solucionar muchos problemas de configuración. LLDP se puede utilizar en situaciones en las que necesite trabajar entre dispositivos que no son propiedad de Cisco y dispositivos que son propiedad de Cisco. El switch proporciona toda la información sobre el estado LLDP actual de los puertos y puede utilizar esta información para solucionar los problemas de conectividad dentro de la red. Se trata de uno de los protocolos que utilizan las aplicaciones de detección de redes, como FindIT Network Management, para detectar dispositivos en la red.

Identificación de protocolos

- **Sistema de nombres de dominio (DNS):** Una vez que hay un nombre de dominio completo (FQDN) asignado a una dirección IP, se coloca en una base de datos. Por ejemplo, cuando busca *www.google.com* puede ingresar el nombre del sitio web, y la base de datos lo busca y puede llegar allí a través de su dirección IP. El **Proveedor de servicios de Internet (ISP)** utiliza su servidor DNS como valor predeterminado y ya se ha configurado. Sin embargo, puede cambiar esto manualmente si encuentra velocidades lentas al utilizar Internet.
- **DNS dinámico:** También denominado DDNS, actualiza automáticamente un servidor en el DNS con la configuración activa de sus nombres de host, direcciones o cualquier otra información pertinente. En otras palabras, DDNS asigna un nombre de dominio fijo a una dirección IP WAN dinámica. Esto ahorra el coste de adquirir una dirección IP permanente.
- **Protocolo de Internet (IP):** Las direcciones IP son identificadores únicos que permiten el envío y recepción de datos entre hosts en Internet. Esto se logra a través de direcciones públicas de Internet, que requieren la compra de un ISP.
- **Control de acceso a medios (dirección MAC):** Cada dispositivo tiene un identificador único conectado a él. Esto no cambia. Es bueno saber la dirección MAC al configurar una red y solucionar problemas. Normalmente se encuentra en el dispositivo y contiene letras y números. Los switches realizan un seguimiento de las direcciones MAC de los dispositivos y crean una tabla de direcciones MAC.

Resolución de problemas de protocolos

- **Ping:** Un ping es un método común de resolución de problemas. Un ping envía mensajes de eco ICMP a una dirección IP. Se recibe un mensaje a cambio. Una respuesta exitosa muestra conectividad física bidireccional. Es una manera de ver si un paquete de datos de red puede ser distribuido a una dirección sin problemas.
- **Protocolo de mensajes de control de Internet (ICMP):** mensajes sobre errores e información operativa. Cuando realiza una prueba PING, se envía un mensaje de eco ICMP al destino. Una conexión correcta obtiene una respuesta de ese dispositivo.

Servidor

Equipo o programa de un equipo que proporciona servicios a otros equipos. Un servidor puede ser virtual o incluso una aplicación. Puede haber varios servidores en un dispositivo. Los servidores pueden compartirse entre sí. Se pueden utilizar con Windows, Mac o Linux.

Servidores Web: formato y presentación de páginas Web para exploradores Web
Servidores de archivos - Comparta archivos y carpetas a los usuarios en una red
Servidores de correo electrónico - enviar, recibir y almacenar correos electrónicos
Servidores DNS - Traduzca nombres fáciles de usar como www.cisco.com a la dirección IP 173.37.145.84 por ejemplo
Servidores de mensajería instantánea - controla el flujo y gestiona mensajes instantáneos (Jabber, Skype)

Quality of Service (QoS)

Estos parámetros se configuran para asegurarse de que se da prioridad al tráfico en una red, normalmente de voz o vídeo, ya que suele ser el más visible cuando hay un retraso de paquete (datos).

Los fundamentos de una conexión a Internet

Proveedor de servicios de Internet (ISP)

Necesita un ISP para acceder a Internet en la red. Hay muchas opciones entre las que elegir para velocidades de conexión, así como una variedad de precios que se adaptan a las necesidades de su empresa. Además del acceso a Internet, un ISP ofrece correo electrónico, alojamiento de páginas web y mucho más.

Explorador web

Aplicación que se incluye en el dispositivo. Hay otros que puede descargar. Una vez descargado, puede abrir e introducir la dirección IP o el sitio web al que desea ir a través de Internet. Algunos ejemplos de exploradores web son:

Microsoft Edge

 ,

Cromado

 ,

Firefox

 ,

y Safari.

.

Si no puede abrir algo o tiene otros problemas de navegación, lo más sencillo sería abrir un navegador web diferente e intentarlo de nuevo.

Localizador uniforme de recursos (URL)

En un explorador Web, normalmente escribe el nombre de un sitio Web al que desea acceder, es decir, la dirección URL y su dirección Web. Cada URL debe ser única. Un ejemplo de URL es https://www.cisco.com.

Gateway predeterminado

Este es el router que el tráfico de red de área local utiliza como salida al proveedor de servicios de Internet (ISP) y a Internet. En otras palabras, este router le conecta con otros dispositivos fuera del edificio y a través de Internet.

Firewall

Un firewall es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si se permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad, denominado Listas de control de acceso (ACL).

Los firewalls han sido la primera línea de defensa de la seguridad de la red durante décadas. Establecen una barrera entre las redes internas seguras y controladas que pueden ser de confianza y las redes externas no fiables, como Internet.

Un firewall puede ser hardware, software o ambos.

Para obtener más detalles, consulte Configuración de los parámetros básicos del firewall en el router serie RV34x.

Listas de Control de Acceso (ACLs)

Listas que bloquean o permiten el envío del tráfico hacia y desde determinados usuarios. Las reglas de acceso se pueden configurar para que estén en vigor todo el tiempo o en función de una programación definida. Una regla de acceso se configura en función de varios criterios para permitir o denegar el acceso a la red. La regla de acceso se programa en función del momento en que se deben aplicar las reglas de acceso al router. Estos se configuran en seguridad o en configuración de firewall. Por ejemplo, una empresa puede querer impedir que los empleados transmitan deportes en directo o se conecten a Facebook durante el horario laboral.

Ancho de banda

Cantidad de datos que se pueden enviar de un punto a otro en un período determinado. Si tiene una conexión a Internet con un ancho de banda mayor, la red puede mover los datos mucho más rápido que una conexión a Internet con un ancho de banda inferior. La transmisión de vídeo requiere mucho más ancho de banda que el envío de archivos. Si descubre que hay un retraso en el acceso a una página web o retrasos en la transmisión de vídeo, es posible que deba aumentar el ancho de banda de la red.

Cable Ethernet

La mayoría de los dispositivos de una red tienen puertos Ethernet. Los cables Ethernet son lo que se conecta a ellos para una conexión por cable. Ambos extremos del cable RJ45 son iguales y se parecen a las tomas telefónicas antiguas. Se pueden utilizar para conectar dispositivos y conectarse a Internet. Los cables conectan los dispositivos para el acceso a Internet y el uso compartido de archivos. Algunos ordenadores requieren un adaptador Ethernet, ya que es posible que no proporcionen un puerto Ethernet.

Redes y cómo encajan

Red de área local (LAN)

Una red que puede ser tan grande como varios edificios o tan pequeña como una casa. Todas las personas conectadas a la LAN se encuentran en la misma ubicación física y están conectadas al mismo router.

En una red local, a cada dispositivo se le asigna su propia dirección IP interna única. Siguen un patrón 10.x.x.x, 172.16.x.x - 172.31.x.x, o 192.168.x.x. Estas direcciones sólo son visibles dentro de una red, entre dispositivos, y se consideran privadas. Hay millones de ubicaciones que pueden tener el mismo conjunto de direcciones IP internas que su empresa. No importa, solo se usan dentro de su propia red privada, por lo que no hay conflicto. Para que los dispositivos en la red se comuniquen entre sí, deben seguir el mismo patrón que los otros dispositivos, estar en la misma subred y ser únicos. Nunca debería ver ninguna de estas direcciones en este patrón como una dirección IP pública, ya que están reservadas sólo para direcciones LAN privadas.

Todos estos dispositivos envían datos a través de una gateway predeterminada (un router) para conectarse a Internet. Cuando el gateway predeterminado recibe la información, necesita hacer Traducción de direcciones de red (NAT) y cambiar la dirección IP, ya que todo lo que sale por Internet necesita una dirección IP única.

Red de área extensa (WAN)

Una red de área extensa (WAN) es una red que se distribuye, a veces de forma global. Muchas LAN se pueden conectar a una sola WAN.

Sólo las direcciones WAN pueden comunicarse entre sí a través de Internet. Cada dirección WAN debe ser única. Para que los dispositivos dentro de una red puedan enviar y recibir información a través de Internet, debe tener un router en el borde de la red (un gateway predeterminado) que pueda realizar NAT.

Haga clic para leer Configure Access Rules on an RV34x Series Router.

traducción de Dirección de Red (NAT)

Un router recibe una dirección WAN a través de un proveedor de servicios de Internet (ISP). El router viene con la función NAT que toma el tráfico que sale de la red, traduce la dirección privada a la dirección WAN pública y la envía a través de Internet. Hace lo contrario al recibir tráfico. Esto se configuró porque no hay suficientes direcciones IPv4 permanentes disponibles para todos los dispositivos del mundo.

La ventaja de NAT es que proporciona seguridad adicional al ocultar de forma eficaz toda la red interna detrás de esa única dirección IP pública única. Las direcciones IP internas a menudo permanecen iguales, pero si se desconectan durante un tiempo, se configura de cierta manera o se restablecen a los valores predeterminados de fábrica, es posible que no lo sea.

NAT estática

Puede configurar la dirección IP interna para que permanezca igual mediante la configuración del protocolo de configuración dinámica de host (DHCP) estático en el router. No se garantiza que las direcciones IP públicas permanezcan iguales a menos que pague por tener una dirección IP pública estática a través del ISP. Muchas empresas pagan por este servicio, por lo que sus empleados y clientes disponen de una conexión más fiable a sus servidores (web, correo, VPN, etc.), pero puede resultar caro.

La NAT estática asigna una traducción uno a uno de las direcciones IP privadas a las direcciones IP públicas. Crea una traducción fija de direcciones privadas a las direcciones públicas. Esto significa que necesitaría una cantidad equivalente de direcciones públicas como direcciones privadas. Esto es útil cuando un dispositivo necesita ser accesible desde fuera de la red.

Haga clic para leer Configuración de NAT y NAT estática en RV160 y RV260.

CGNAT

La NAT de nivel de operador es un protocolo similar que permite que varios clientes utilicen la misma dirección IP.

VLAN

Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En los escenarios donde los datos

confidenciales se pueden difundir en una red, se pueden crear VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Sólo los usuarios que pertenecen a una VLAN pueden acceder y manipular los datos en esa VLAN. Las VLAN también se pueden utilizar para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusión a destinos innecesarios.

Una VLAN se utiliza principalmente para formar grupos entre los hosts independientemente de dónde se encuentren físicamente los hosts. Por lo tanto, una VLAN mejora la seguridad con la ayuda de la formación de grupos entre los hosts. Cuando se crea una VLAN, no tiene efecto hasta que esa VLAN se conecta al menos a un puerto, ya sea manual o dinámicamente. Una de las razones más comunes para configurar una VLAN es configurar una VLAN separada para voz y una VLAN separada para datos. Esto dirige los paquetes para ambos tipos de datos a pesar de usar la misma red.

Para obtener más información, debe leer Prácticas recomendadas de VLAN y Consejos de Seguridad para Cisco Business Routers.

Subred

A menudo llamadas subredes, las subredes son redes independientes dentro de una red IP.

SSID

El identificador de conjunto de servicios (SSID) es un identificador único al que los clientes inalámbricos pueden conectarse o compartir entre todos los dispositivos de una red inalámbrica. Distingue entre mayúsculas y minúsculas y no debe superar los 32 caracteres alfanuméricos. También se denomina Wireless Network Name (Nombre de red inalámbrica).

Redes privadas virtuales (VPN)

La tecnología ha evolucionado y, a menudo, los negocios se llevan a cabo fuera de la oficina. Los dispositivos son más móviles y los empleados suelen trabajar desde casa o mientras viajan. Esto puede causar algunas vulnerabilidades de seguridad. Una red privada virtual (VPN) es una forma excepcional de conectar a los trabajadores remotos en una red de forma segura. Una VPN permite que un host remoto actúe como si estuviera ubicado en la misma red local.

Se ha configurado una VPN para proporcionar transmisión de datos segura. Existen diferentes opciones para configurar una VPN y la forma en que se cifran los datos. Las VPN utilizan Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP) y Layer Two Tunneling Protocol.

Una conexión VPN permite a los usuarios acceder, enviar y recibir datos de una red privada a través de una red pública o compartida, como Internet, pero garantiza una conexión segura a una infraestructura de red subyacente para proteger la red privada

y sus recursos.

Un túnel VPN establece una red privada que puede enviar datos de forma segura mediante cifrado y autenticación. Las oficinas corporativas utilizan principalmente una conexión VPN, ya que es útil y necesario permitir que sus empleados tengan acceso a su red privada aunque se encuentren fuera de la oficina.

Se puede configurar una conexión VPN entre el router y un terminal después de que el router se haya configurado para una conexión a Internet. El cliente VPN depende completamente de la configuración del router VPN para poder establecer una conexión.

Una VPN admite VPN de sitio a sitio para un túnel de gateway a gateway. Por ejemplo, un usuario puede configurar un túnel VPN en una sucursal para conectarse al router en un sitio corporativo, de modo que la sucursal pueda acceder de forma segura a la red corporativa. En una conexión VPN de sitio a sitio, cualquiera puede iniciar la comunicación. Esta configuración tiene una conexión cifrada constante.

VPN IPsec también admite VPN de cliente a servidor para un túnel de host a gateway. La VPN de cliente a servidor es útil cuando se conecta desde un portátil/PC desde casa a una red corporativa a través del servidor VPN. En este caso, sólo el cliente puede iniciar la conexión.

Haga clic para leer Descripción general y prácticas recomendadas de Cisco Business VPN.

Certificados

Un paso seguro en la configuración de una VPN es obtener un certificado de una Autoridad de Certificación (CA). Esto se utiliza para la autenticación. Los certificados se adquieren en cualquier número de sitios de terceros. Es una manera oficial de probar que su sitio es seguro. Básicamente, la CA es una fuente de confianza que verifica que usted es una empresa legítima y de confianza. Para una VPN sólo necesita un certificado de nivel inferior a un costo mínimo. La CA le desprotege y, una vez que verifiquen su información, le emitirán el certificado. Este certificado se puede descargar como un archivo en su equipo. A continuación, puede ir al router (o al servidor VPN) y cargarlo allí.

Los clientes normalmente no necesitan un certificado para utilizar una VPN; es sólo para verificación a través del router. Una excepción a esto es OpenVPN, que requiere un certificado de cliente.

Muchas pequeñas empresas prefieren utilizar una contraseña o una clave previamente compartida en lugar de un certificado para simplificar. Esto es menos seguro, pero se puede configurar sin coste alguno.

Algunos artículos sobre este tema que puede disfrutar:

- Certificado (Importar/Exportar/Generar CSR) en el router serie RV160 y RV260
- Reemplace el certificado firmado automáticamente predeterminado por un certificado SSL de terceros en el router serie RV34x
- Gestión de certificados en el router serie RV34x

Clave precompartida (PSK)

Se trata de una contraseña compartida, decidida y compartida antes de la configuración de una VPN y puede utilizarse como alternativa para utilizar un certificado. Un PSK puede ser lo que quieras que sea, sólo tiene que coincidir en el sitio y con el cliente cuando se configuran como cliente en su equipo. Tenga en cuenta que, en función del dispositivo, puede haber símbolos prohibidos que no pueda utilizar.

Vida útil de la clave

Frecuencia con la que el sistema cambia la clave. Este ajuste también debe ser el mismo que el router remoto.

Conclusión

Ahí lo tienen, ahora tienen muchos de los fundamentos para que se encaminen.

Si desea seguir aprendiendo más, consulte estos enlaces.

Prácticas recomendadas para configurar direcciones IP estáticas Descripción general y prácticas recomendadas de Cisco Business VPN Prácticas recomendadas de VLAN y consejos de seguridad para routers empresariales de Cisco Copia de seguridad de Internet - Windows Copia de seguridad de Internet - Mac Cómo iniciar sesión en un switch