Novidade para os negócios da Cisco: Glossário de equipamentos e redes básicas

Objetivo

O objetivo deste documento é familiarizar os principiantes com o equipamento Cisco Business (Small Business) e alguns termos gerais que você deve saber. Os tópicos incluem hardware disponível, termos comerciais da Cisco, termos gerais de rede, ferramentas da Cisco, os fundamentos da troca de dados, os fundamentos de uma conexão com a Internet e redes e como eles se encaixam.

Introduction

Você está apenas começando a configurar sua rede com o equipamento da Cisco? Pode ser esmagador entrar no novo mundo da configuração e manutenção de uma rede. Este artigo está aqui para ajudá-lo a familiarizar-se com alguns dos conceitos básicos. Quanto mais você sabe, menos intimidante será!

    - Fonte aberta
    - Arquivo Zip
    - Interface da linha de comando (CLI)
    - Máquina virtual
- Ferramentas da Cisco que você pode usar
    - Cisco Business Dashboard (CBD)
    - Utilitário FindIT Network Discovery
    - AnyConnect (RV34x Series Routers/ VPNs)
- Conceitos básicos da troca de dados
    - Pacote
    - Latência
    - Redundância
    - Protocolos
    - Servidor
    - Quality of Service (QoS)
- Conceitos básicos de uma conexão com a Internet
    - Provedor de serviços de Internet (ISP)
    - Navegador da Web
    - Uniform Resource Locator (URL)
    - Gateway padrão
    - Firewall
    - Listas de controle de acesso (ACLs)
    - Largura de banda
    - Cabo Ethernet
- Redes e como elas se encaixam
    - Rede local (LAN)
    - Rede de longa distância (WAN)
    - Tradução de Endereço de Rede (NAT)
    - NAT Estático
    - CGNAT
    - VLAN
    - Sub-rede
    - SSID
    - VPNs (Virtual private networks, redes virtuais privadas)

Hardware disponível na Cisco Business

Router

Os roteadores conectam várias redes, bem como roteam dados para onde precisam. Eles também conectam computadores nessas redes à Internet. Os roteadores permitem que todos os computadores em rede compartilhem uma única conexão com a Internet, o que economiza dinheiro.

Um roteador atua como um despachante. Ele analisa os dados sendo enviados através de uma rede, escolhe a melhor rota para os dados trafegarem e os envia em seu caminho.

Os roteadores conectam sua empresa ao mundo, protegem as informações contra ameaças à segurança e podem até mesmo decidir quais computadores recebem prioridade sobre outros.

Além dessas funções básicas de rede, os roteadores vêm com recursos adicionais para tornar a rede mais fácil ou mais segura. Dependendo de suas necessidades, por exemplo, você pode escolher um roteador com um firewall, uma rede virtual privada (VPN) ou um sistema de comunicação IP (Internet Protocol).

Os roteadores Cisco Business desenvolvidos mais recentemente incluem as séries RV160, RV260, RV340 e RV345.

Switch

Os switches são a base da maioria das redes empresariais. Um switch atua como controlador, conectando computadores, impressoras e servidores a uma rede em um prédio ou campus.

Os switches permitem que os dispositivos na sua rede se comuniquem entre si, bem como com outras redes, criando uma rede de recursos compartilhados. Por meio do compartilhamento de informações e da alocação de recursos, os switches economizam dinheiro e aumentam a produtividade.

Há dois tipos básicos de switches para escolher como parte dos fundamentos de sua rede: gerenciado e não gerenciado.

> Um switch não gerenciado funciona fora da caixa, mas não pode ser configurado. O equipamento de rede residencial geralmente oferece switches não gerenciados.
> Um switch gerenciado pode ser configurado. Você pode monitorar e ajustar um switch gerenciado local ou remotamente, proporcionando maior controle sobre o tráfego e o acesso à rede.

Para obter mais detalhes sobre switches, consulte Glossário de Termos dos Switches.

Os switches desenvolvidos mais recentemente incluem o Cisco Business Switch CBS110, CBS220, CBS250 e CBS350 Series.

Se quiser saber as diferenças entre os switches CBS, confira

Ponto de acesso Wireless

Um ponto de acesso sem fio permite que os dispositivos se conectem à rede sem fio sem cabos. Uma rede sem fio facilita a colocação de novos dispositivos on-line e oferece suporte flexível para funcionários móveis.

Um ponto de acesso atua como um amplificador para sua rede. Embora um roteador forneça a largura de banda, um ponto de acesso estende essa largura de banda para que a rede possa suportar muitos dispositivos, e esses dispositivos podem acessar a

rede a partir de uma distância maior.

Mas um ponto de acesso faz mais do que simplesmente estender o Wi-Fi. Ele também pode fornecer dados úteis sobre os dispositivos na rede, fornecer segurança proativa e atender a muitos outros propósitos práticos.

Os access points sem fio mais recentes, Cisco Business Wireless, incluem o AC140, AC145 e AC240, que permitem uma rede em malha sem fio. Se você não está familiarizado com redes sem fio em malha, você pode ler mais em Welcome to Cisco Business Wireless Mesh Networking ou Frequently Asked Questions (FAQ) for a Cisco Business Wireless Network.

Se quiser saber alguns termos comuns aos Pontos de acesso sem fio, consulte o Glossário de Termos WAP.

Telefone multiplataforma

Os telefones MPP fornecem comunicação de Voz sobre IP (VoIP) usando o Session Initiation Protocol (SIP). Isso elimina a necessidade de linhas telefônicas tradicionais, tornando os telefones mais portáteis dentro da empresa. Com o VoIP, um telefone usa uma infraestrutura de rede existente e uma conexão com a Internet em vez de linhas T1 dispendiosas. Isso permite gerenciar mais chamadas com menos "linhas". Outras opções benéficas incluem colocar chamadas em espera, estacionar chamadas, transferir chamadas e muito mais. Alguns modelos permitem a comunicação por vídeo além do VoIP.

Os telefones MPP são criados para parecerem um telefone comum e são usados somente para esse fim, mas essencialmente, eles são um computador e fazem parte da sua rede. Os telefones MPP exigem um serviço de um provedor de serviços de telefonia pela Internet (ITSP) ou de um servidor de controle de chamadas IP Private Branch Exchange (PBX). WebEx Calling, Ring Central e Verizon são exemplos de um ITSP. Alguns exemplos de serviços IP PBX que funcionam com telefones Cisco MPP incluem plataformas Asterisk, Centile e Metaswitch. Muitos recursos nesses telefones são programados especificamente por provedores terceirizados (como o FreePBX), de modo que os processos (estacionamento, acesso ao correio de voz, etc.) podem variar.

Os telefones Cisco Business MPP mais recentemente desenvolvidos incluem as séries 6800, 7800 e 8800.

Comumente referenciado nos negócios da Cisco

Guia de administração e Guia de início rápido

Esses são dois recursos diferentes a serem pesquisados para obter informações detalhadas sobre seu produto e seus recursos. Ao fazer uma pesquisa no site ou na Web com o número do modelo, você pode adicionar um ou outro para exibir esses guias mais longos.

Configurações padrão

Os dispositivos vêm com configurações padrão pré-selecionadas. Frequentemente, elas são as configurações mais comuns que um administrador escolheria. Você pode alterar as configurações de acordo com suas necessidades.

Nome de usuário e senha padrão

Em equipamentos comerciais antigos da Cisco, o padrão era *admin* para nome de usuário e senha. Agora, a maioria tem um padrão de *cisco* para nome de usuário e senha. Em telefones de Voz sobre IP (VoIP), você precisa fazer login como *administrador* para alterar muitas das configurações. É altamente recomendável alterar a senha para torná-la mais complexa para fins de segurança.

Endereços IP padrão

A maioria dos equipamentos Cisco vem com endereços IP padrão para roteadores, switches e pontos de acesso sem fio. Se você não consegue se lembrar do endereço IP e não tem uma configuração especial, você pode usar um clipe de papel aberto para pressionar o botão de reinicialização no dispositivo por pelo menos 10 segundos. Isso redefinirá as configurações padrão. Se seu switch ou WAP não estiver conectado a um roteador com DHCP ativado e você estiver conectado diretamente ao switch ou WAP com seu computador, esses são os endereços IP padrão.

O endereço IP padrão de um roteador Cisco Business é 192.168.1.1.
O endereço IP padrão de um switch Cisco Business é 192.168.1.254.
O endereço IP padrão para um ponto de acesso sem fio (AP) para pequenas empresas é 192.168.1.245. Não há endereço IP padrão para os novos pontos de acesso sem fio de malha.

Redefinir para o padrão de fábrica

Pode chegar a hora em que você deseja redefinir o roteador, switch ou ponto de acesso sem fio da Cisco Business de volta para as configurações padrão de fábrica e começar do zero. Isso é útil quando você move o equipamento de uma rede para outra ou como último recurso quando não é possível resolver um problema de configuração. Quando você redefine as configurações padrão de fábrica, todas as configurações são perdidas.

Você pode fazer backup das configurações para restaurá-las após uma redefinição de fábrica. Clique nos links a seguir para obter mais informações:

- Reinicialize ou restaure as configurações padrão de fábrica do RV34x Series Router através do utilitário baseado na Web
- Backup e restauração ou troca de firmware em um switch
- Fazer download, fazer backup, copiar e excluir arquivos de configuração em um ponto de acesso sem fio

- Gerenciar os arquivos de configuração no ponto de acesso WAP125 ou WAP581

Se você não fizer o backup da configuração, precisará configurar o dispositivo novamente do zero para garantir que tenha os detalhes da conexão. A maioria dos modelos tem um artigo detalhando as etapas a serem seguidas para uma redefinição, mas a maneira mais simples de fazer isso é usar um clipe de papel aberto e pressionar o botão de reinicialização no dispositivo por pelo menos 10 segundos. Isso não se aplica aos telefones MPP, portanto, marque a opção Reset a Cisco IP Phone para obter mais informações.

Interface de usuário da Web (IU)

Cada equipamento Cisco Business vem com uma interface de usuário da Web, exceto os switches não gerenciados da série 100.

Esse tipo de interface, o que você vê na tela, mostra opções para seleção. Você não precisa conhecer nenhum comando para navegar por essas telas. A IU da Web também é às vezes chamada de Interface Gráfica do Usuário (GUI), interface baseada na Web, orientação baseada na Web, utilitário baseado na Web ou um utilitário de configuração da Web.

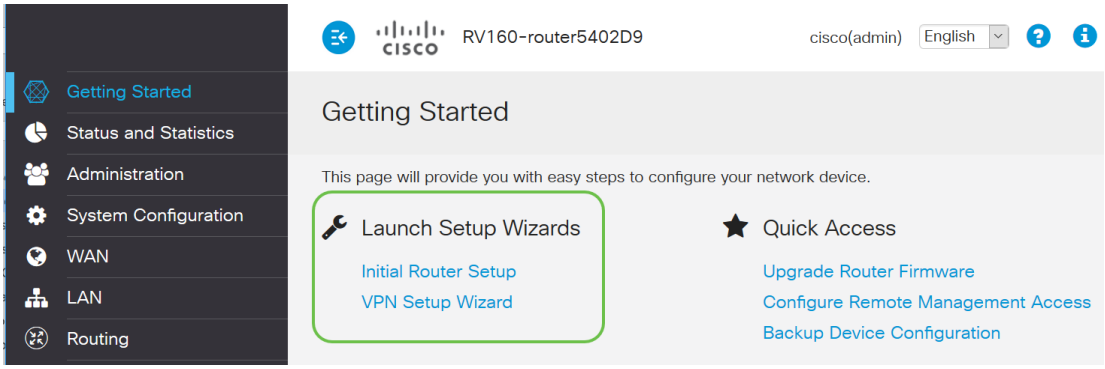
Uma das maneiras mais fáceis de alterar a configuração de um dispositivo é através da interface de usuário da Web. A interface de usuário da Web oferece ao administrador uma ferramenta que contém todos os recursos possíveis que podem ser alterados para modificar o desempenho de um dispositivo.

Depois de fazer login em um dispositivo Cisco, você verá uma tela da interface do usuário da Web que inclui um painel de navegação no lado esquerdo. Ele contém uma lista dos recursos de nível superior do dispositivo. O painel de navegação também é chamado às vezes de árvore de navegação, barra de navegação ou mapa de navegação.

As cores desta página podem variar, bem como os recursos de nível superior, dependendo do equipamento e da versão do firmware.

Assistente de configuração

Esta é uma tela interativa na qual você navegará quando fizer login em um dispositivo Cisco Small Business pela primeira vez, e possivelmente depois disso. Pode ser uma excelente maneira de colocar você em operação na sua rede. Há várias configurações padrão pré-selecionadas que podem ser alteradas. Alguns dispositivos vêm com mais de um Assistente de configuração. Este exemplo mostra dois Assistentes de Configuração, *Configuração Inicial do Roteador* e *Assistente de Configuração de VPN*.



Propriedade da Cisco

Desenvolvido e de propriedade específica da Cisco. Por exemplo, o Cisco Discovery Protocol (CDP) é proprietário da Cisco. Geralmente, os protocolos proprietários da Cisco só podem ser usados em dispositivos da Cisco.

Modelos em uma série

A Cisco oferece aos proprietários de pequenas empresas vários modelos diferentes para atender às necessidades de sua empresa. Frequentemente, um modelo será oferecido com diferentes recursos, número de portas, Power over Ethernet ou mesmo sem fio. Se houver vários modelos em uma série, a Cisco colocará um x no lugar do número ou letra que varia entre os modelos, mas as informações se aplicam a todos nessa série. Por exemplo, os roteadores RV340 e RV345 são referidos na série RV34x. Se um dispositivo tem um P no final, ele oferece Power over Ethernet. Se o nome de um dispositivo termina em W, ele oferece recursos sem fio. Em geral, quanto maior o número do modelo, maiores as capacidades do dispositivo. Para ver detalhes sobre isso, confira os seguintes artigos:

- Toque de decodificador de produto - Roteador
- Decodificador de ID de produto - Switch
- Toque de decodificador de produto - WAP
- Decodificador de modelo sem fio comercial da Cisco (Mesh Wireless)

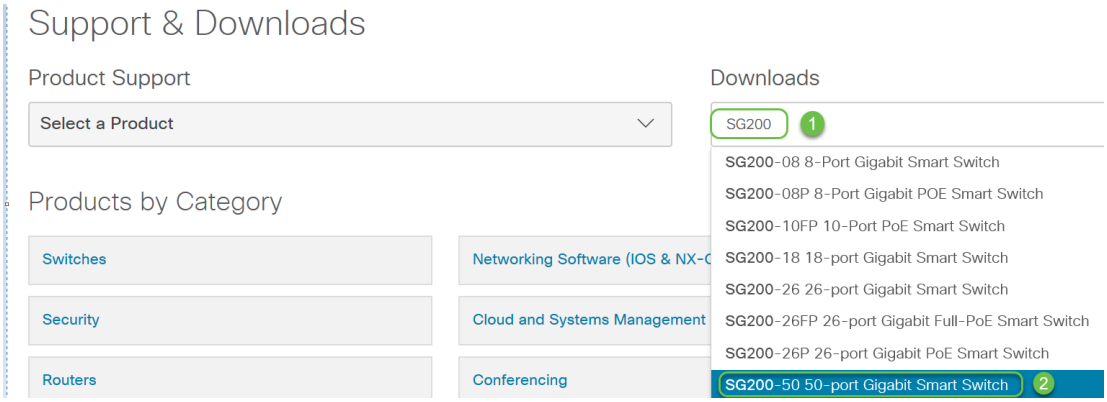
Firmware

Também conhecido como imagem. O programa que controla as operações e a funcionalidade do dispositivo.

Atualizar firmware

A atualização do firmware é essencial para um desempenho ideal em cada dispositivo. É muito importante instalar atualizações quando elas são lançadas. Quando a Cisco lança uma atualização de firmware, eles geralmente contêm melhorias, como novos recursos ou corrigem um bug que pode causar uma vulnerabilidade de segurança ou um problema de desempenho.

Vá para Suporte da Cisco e digite o nome do dispositivo que precisa de uma atualização em *Downloads*. Um menu suspenso deve ser exibido. Role para baixo e escolha o modelo específico que você possui.



Dica: ao examinar várias versões do firmware da Cisco, cada uma segue um formato x.x.x.x. que são considerados quatro octetos. Quando há uma atualização menor, o quarto octeto é alterado. O terceiro octeto muda quando é uma alteração maior. O segundo octeto significa uma grande mudança. O primeiro octeto muda se for uma revisão completa.

Se desejar orientação, clique neste link para baixar e atualizar o firmware em qualquer dispositivo.

Este artigo tem algumas ideias de solução de problemas no caso de você estar tendo problemas com uma atualização de switch: Atualizar firmware em um switch 200/300 Series.

Termos gerais de rede

Depois de ter seu equipamento, você deve se familiarizar com alguns termos comuns em redes.

Interface

Uma interface é geralmente esse espaço entre um sistema e outro. Qualquer coisa que possa se comunicar com o seu computador, incluindo portas. Uma interface de rede geralmente recebe um endereço IP local. Uma interface de usuário permite que o usuário interaja com o sistema operacional.

Nó

Um termo geral para descrever qualquer dispositivo que faz uma conexão ou interação dentro de uma rede, ou que pode enviar, receber e armazenar informações, comunicar-se com a Internet e ter um endereço IP.

Host

Um host é um dispositivo que é um endpoint para comunicações em uma rede, o host pode fornecer dados ou um serviço (como DNS) para outros nós. Dependendo da topologia, um switch ou um roteador pode ser um host. Todos os hosts também são nós. Os exemplos incluem um computador, um servidor ou uma impressora.

Programa de computador

Um programa de computador contém instruções que podem ser executadas em um computador.

Aplicativo

O software aplicativo é um programa que ajuda a executar tarefas. Frequentemente, eles são chamados de intercambiáveis por serem semelhantes, mas nem todos os programas são aplicativos.

Prática recomendada

O método recomendado para configurar algo e executar sua rede.

Topologia

A forma física como o equipamento está conectado. Um mapa da rede.

Configurar

Isso se refere à forma como as coisas são configuradas. Você pode deixar as configurações padrão, aquelas que vêm pré-configuradas quando compra equipamentos ou pode configurar para suas necessidades específicas. As configurações padrão são as configurações básicas, geralmente recomendadas. Quando você faz logon no dispositivo, pode haver um Assistente para configuração que pode orientá-lo sobre o que fazer.

Endereço MAC

Identificador exclusivo para cada dispositivo. Está localizado no dispositivo físico e pode ser detectado com Bonjour, LLDP ou CDP. Um switch controla os endereços MAC nos dispositivos à medida que interage com eles e cria uma tabela de endereços MAC. Isso ajuda o switch a saber onde rotear pacotes de informações.

Fonte aberta

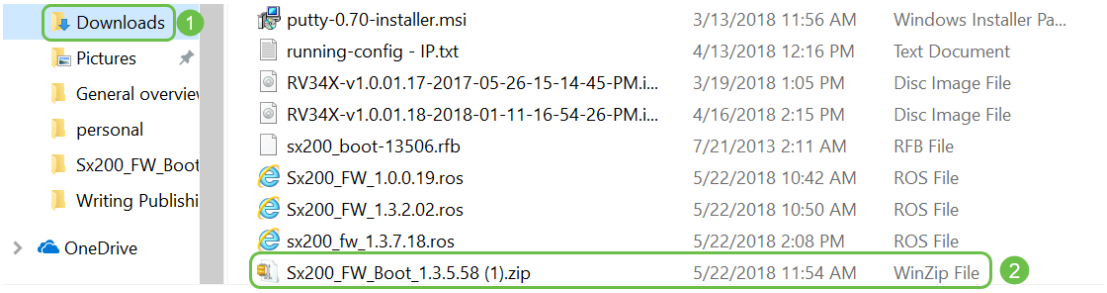
Um programa disponível gratuitamente para o público.

Arquivo Zip

Um grupo de arquivos compactados em um arquivo zip. Ele é usado quando você deseja transferir vários arquivos em uma única etapa. O receptor pode abrir o arquivo zip e acessar cada um separadamente. Um arquivo zip termina em *.zip*.

Se vir um arquivo em um formato que termina em *.zip*, você deve descompactar esse arquivo. Se você não tiver um programa unzip, será necessário baixar um. Há várias

opções gratuitas on-line. Depois de baixar um programa de descompactação, clique em **Downloads** e localize o arquivo *.zip* necessário para descompactar.



Clique com o botão direito do mouse no nome do arquivo zip; uma tela semelhante a esta será exibida. Passe o mouse sobre o software unzip e escolha **Extract Here (Extrair aqui)**. Neste exemplo, 7-Zip é usado.

Interface da linha de comando (CLI)

Interface de linha de comando (CLI): Às vezes conhecido como terminal. Isso é utilizado como outra opção para escolher configurações em dispositivos como roteadores e switches. Se você tiver experiência, essa pode ser uma maneira muito mais simples de configurar as coisas, já que você não precisaria navegar por várias telas da interface do usuário da Web. A queda disso é que você precisa conhecer os comandos e inseri-los perfeitamente. Como você está lendo um artigo para iniciantes, a CLI provavelmente não deve ser sua primeira escolha.

Máquina virtual

A maioria das máquinas tem mais recursos do que precisa. Um computador pode ser provisionado para manter tudo o que é necessário para executar mais de uma máquina. O problema com isso é que se uma parte ficar inativa ou precisar de uma reinicialização, todos eles seguirão.

Se você instalar o VMware ou Hyper-V, poderá carregar software, servidores Web, servidores de e-mail, FindIT e muito mais em um computador. Uma máquina virtual pode até usar um sistema operacional diferente. Eles são logicamente independentes um do outro. Cada um executa as funções de um dispositivo separado sem ser realmente um. Embora o hardware seja compartilhado, cada máquina virtual aloca uma parte do recurso físico para cada sistema operacional. Isso pode economizar dinheiro, energia e espaço.

Ferramentas da Cisco que você pode usar

Cisco Business Dashboard (CBD)

Esta é uma ferramenta da Cisco usada para monitorar e manter redes. O CBD pode ajudá-lo a identificar dispositivos Cisco em sua rede, bem como outros recursos de gerenciamento úteis.

Essa é uma ferramenta útil se você executar coisas em casa ou supervisionar mais de uma rede. O CBD pode ser executado em uma máquina virtual. Para obter mais informações sobre o CBD, consulte o Site de Suporte do Cisco Business Dashboard ou a Visão Geral do Cisco Business Dashboard.

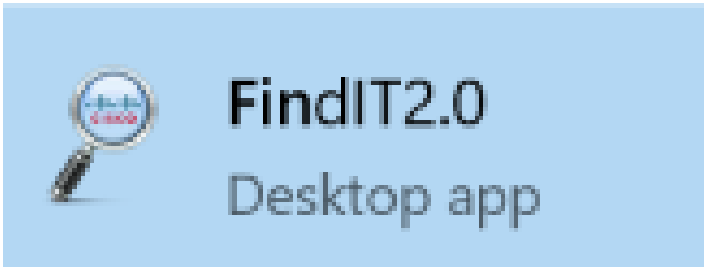
Utilitário FindIT Network Discovery

Essa ferramenta simples é muito básica, mas pode ajudá-lo a descobrir rapidamente os equipamentos da Cisco na sua rede. O Cisco FindIT descobre automaticamente todos os dispositivos Cisco Small Business suportados no mesmo segmento de rede local do seu PC.

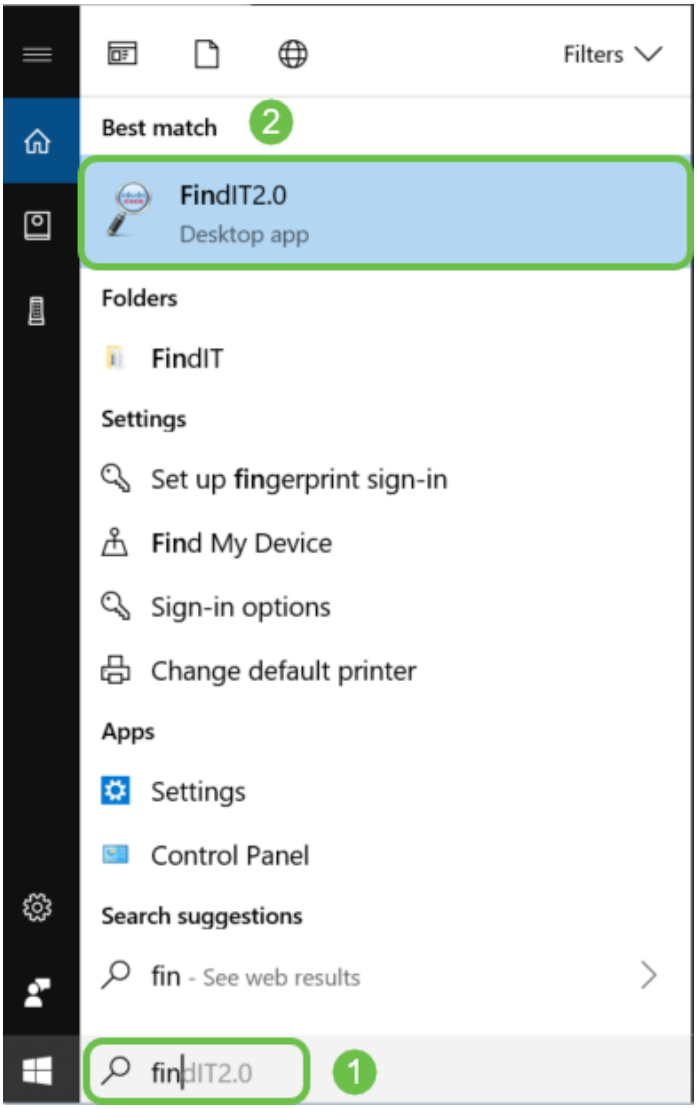
Clique para saber mais e baixar o Cisco Small Business FindIT Network Discovery Utility.

Clique neste link para ler um artigo sobre Como instalar e configurar o Cisco FindIT Network Discovery Utility.

O aplicativo é semelhante ao Windows 10.



Quando o download for feito, você o encontrará aqui no Windows 10.



AnyConnect (RV34x Series Routers/ VPNs)

Essa VPN é usada especificamente com os roteadores da série RV34x (e equipamentos da empresa/grande empresa). O Cisco AnyConnect Secure Mobility Client fornece aos usuários remotos uma conexão VPN segura. Ele oferece aos usuários finais remotos os benefícios de um cliente VPN Cisco Secure Sockets Layer (SSL) e também suporta aplicativos e funções não disponíveis em uma conexão VPN SSL baseada em navegador. Geralmente usado por funcionários remotos, o AnyConnect permite que eles se conectem à infraestrutura corporativa de computadores como se estivessem fisicamente no escritório, mesmo que não estejam. Isso aumenta a flexibilidade, a mobilidade e a produtividade dos funcionários. As licenças do cliente são necessárias para usar o AnyConnect. O Cisco AnyConnect é compatível com os seguintes sistemas operacionais: Windows 7, 8, 8.1 e 10, Mac OS X 10.8 e posterior e Linux Intel (x64).

Consulte os seguintes artigos para obter mais orientação:

- Instalar o Cisco AnyConnect Secure Mobility Client em um computador com Windows
- Instalar o Cisco AnyConnect Secure Mobility Client em um computador Mac

Conceitos básicos da troca de dados

Pacote

Em redes, as informações são enviadas em blocos, chamados pacotes. Se houver problemas de conexão, os pacotes podem ser perdidos.

Latência

Atrasos na transferência de pacotes.

Redundância

Em uma rede, a redundância é configurada de modo que se parte da rede tiver problemas, toda a rede não falhará. Considere um plano de backup se algo acontecer com a configuração principal.

Protocolos

Dois dispositivos precisam ter algumas das mesmas configurações para se comunicar. Pense nisso como uma língua. Se uma pessoa só fala alemão e a outra só fala espanhol, ela não consegue se comunicar. Protocolos diferentes funcionam juntos e podem haver vários protocolos sendo transmitidos entre si. Os protocolos têm finalidades diferentes; alguns exemplos estão listados e descritos brevemente abaixo.

Protocolos de endereçamento

- **Session Initiation Protocol (SIP):** Este é o protocolo principal para Voz sobre IP (VoIP), telefones que se comunicam pela Internet. Os dois lados da rede precisam ser configurados usando o mesmo protocolo para se comunicar, de modo que ambos precisem do SIP para iniciar a comunicação via VoIP.
- O **Dynamic Host Configuration Protocol (DHCP)** gerencia um pool de endereços IP disponíveis, atribuindo-os aos hosts à medida que eles se juntam à rede.
- **Address Resolution Protocol** (ARP): mapeia um endereço IP dinâmico para um endereço MAC físico permanente em uma LAN.
- **IPv4:** Esta é a versão mais comum do IP usada atualmente. Um endereço IP é escrito como 4 conjuntos de números (também conhecidos como octetos) separados por um período entre cada conjunto. Cada conjunto pode ser um número entre 0 e 255. Um exemplo de endereço IPv4 é 8.8.8.8, que é o servidor DNS público no Google. Há mais dispositivos do que endereços IP exclusivos para IPv4, portanto, pode ser caro comprar um endereço IP público permanente.
- **IPv6:** Esta última versão usa 8 conjuntos de números com dois-pontos entre cada conjunto. Ele usa um sistema numérico hexadecimal, portanto, pode haver letras no endereço IP. Uma empresa pode ter endereços IPv4 e IPv6 em execução simultânea.

Como estamos falando sobre IPv6, aqui estão alguns detalhes importantes a serem conhecidos sobre esse protocolo de endereçamento:

Abreviações de IPv6: se todos os números em vários conjuntos forem zero, dois

pontos em uma linha podem representar esses conjuntos, essa abreviação só pode ser usada uma vez. Por exemplo, um dos endereços IP IPv6 no Google é 2001:4860:4860::8888. Alguns dispositivos usam campos separados para todas as oito partes dos endereços IPv6 e não podem aceitar a abreviação IPv6. Se for esse o caso, insira 2001:4860:4860:0:0:0:0:888.

Hexadecimal: Um sistema numérico que usa uma base 16 em vez da base 10, que é o que usamos na matemática do dia a dia. Os números de 0 a 9 são representados da mesma forma. 10-15 são representados pelas letras A-F.

Protocolos de transferência de dados

- **Transmission Control Protocol (TCP) e User Datagram Protocol (UDP):** esses são dois modos de transporte dos dados. O TCP exige uma conexão, chamada handshake triplo, antes de enviar dados, de modo que às vezes há um atraso. Se os dados (pacotes) forem perdidos, eles serão enviados novamente. O UDP é menos confiável, mas mais rápido. Frequentemente, voz e vídeo usam UDP.
- **Protocolo FTP:** este protocolo é usado para transferir arquivos de um cliente para um servidor.
- **Protocolo de Transferência de Hipertexto (HTTP - Hypertext Transfer Protocol Secure) vs. Protocolo de Transferência de Hipertexto Seguro (HTTPS - Hypertext Transfer Protocol Secure):** a base geral para a comunicação de dados pela Internet. Você encontrará essas informações no início dos sites, escritos como *http://* e *https://*. Os sites que começam com *https://* são mais seguros de usar.
- **Routing Information Protocol (RIP):** esse protocolo existe há muito tempo. Há três versões, com cada versão adicionando mais segurança e funcionalidade. Os roteadores compartilham rotas entre si. Seu objetivo é evitar loops definindo um número máximo de "saltos" de um roteador para o próximo. Outros protocolos de roteamento mais eficientes incluem **EIGRP (Enhanced Interior Gateway Routing Protocol)**, **OSPF (Open Shortest Path First)** e **IS-IS (Intermediate System to Intermediate System)**. Essas últimas três escalas são melhores que o RIP, mas podem ser mais complicadas de configurar.
- **Shell Seguro (SSH):** um canal seguro que fornece uma rota segura para o tráfego da Linha de Comando. É um protocolo criptografado usado para se comunicar com um servidor remoto. Muitas tecnologias adicionais são construídas em torno do SSH.

Protocolos de descoberta

- **Cisco Discovery Protocol (CDP):** descobre informações sobre outros equipamentos Cisco conectados diretamente e salva essas informações. **O Bonjour** e o **Link Layer Discovery Protocol (LLDP)** executam as mesmas funções e podem obter informações sobre dispositivos que não são da Cisco também. A maioria dos dispositivos para pequenas empresas usa o LLDP.
- **Protocolo LLDP (Layer Link Discovery Protocol):** Permite que um dispositivo anuncie sua identificação, configuração e recursos aos dispositivos vizinhos que armazenam os dados em uma Base de Informações de Gerenciamento (MIB). As informações compartilhadas entre os vizinhos ajudam a reduzir o tempo necessário para adicionar um novo dispositivo à rede local (LAN) e também fornecem detalhes necessários para

solucionar muitos problemas de configuração. O LLDP pode ser usado em cenários onde você precisa trabalhar entre dispositivos que não são proprietários da Cisco e dispositivos que são proprietários da Cisco. O switch fornece todas as informações sobre o status atual de LLDP das portas e você pode usar essas informações para corrigir problemas de conectividade na rede. Esse é um dos protocolos usados por aplicativos de descoberta de rede, como o FindIT Network Management, para descobrir dispositivos na rede.

Identificação de protocolos

- **Sistema de Nome de Domínio (DNS):** Quando houver um Nome de Domínio Totalmente Qualificado (FQDN) atribuído a um endereço IP, ele será colocado em um banco de dados. Por exemplo, quando você pesquisa em *www.google.com* você pode digitar o nome do site, e o banco de dados o procura e pode levá-lo através do endereço IP. O **ISP (Provedor de Internet)** usa seu servidor DNS como padrão e já foi configurado. No entanto, você pode alterar manualmente isso se encontrar velocidades lentas ao usar a Internet.
- **DNS dinâmico:** também conhecido como DDNS, atualiza automaticamente um servidor no DNS com a configuração ativa de seus nomes de host, endereços ou qualquer outra informação pertinente. Em outras palavras, o DDNS atribui um nome de domínio fixo a um endereço IP de WAN dinâmico. Isso economiza o custo de compra de um endereço IP permanente.
- **Internet Protocol (IP):** os endereços IP são identificadores exclusivos que permitem o envio e o recebimento de dados entre hosts na Internet. Isso é obtido por meio de endereços de Internet públicos, que exigem a compra de um ISP.
- **Controle de acesso ao meio (endereço MAC):** cada dispositivo tem um identificador exclusivo conectado a ele. Isso não muda. É bom saber seu endereço MAC ao configurar uma rede e solucionar problemas. Geralmente, ele está localizado no dispositivo e contém letras e números. Os switches controlam os endereços MAC dos dispositivos e criam uma tabela de endereços MAC.

Troubleshooting de Protocolos

- **Ping:** Um ping é um método comum de solução de problemas. Um ping envia mensagens de eco ICMP a um endereço IP. Uma mensagem é recebida em retorno. Uma resposta bem-sucedida mostra a conectividade física bidirecional. É uma forma de ver se um pacote de dados de rede pode ser distribuído para um endereço sem problemas.
- **Internet Control Message Protocol (ICMP):** mensagens sobre erros e informações operacionais. Quando você faz um teste de PING, uma mensagem de eco ICMP é enviada para o destino. Uma conexão bem-sucedida recebe uma resposta desse dispositivo.

Servidor

Um computador ou programa em um computador que fornece serviços para outros computadores. Um servidor pode ser virtual ou até mesmo um aplicativo. Pode haver vários servidores em um dispositivo. Os servidores podem compartilhar entre si. Eles

podem ser usados com Windows, Mac ou Linux.

Servidores Web - formatar e apresentar páginas Web para navegadores Web
Servidores de arquivos - compartilhar arquivos e pastas com usuários em uma rede
Servidores de e-mail - enviar, receber e armazenar e-mails
Servidores DNS - converta nomes amigáveis como www.cisco.com para o endereço IP 173.37.145.84, por exemplo
Servidores de mensagens instantâneas - controlar o fluxo e o gerenciamento de mensagens instantâneas (Jabber, Skype)

Quality of Service (QoS)

Essas configurações são configuradas para garantir que seja dada prioridade ao tráfego em uma rede, geralmente voz ou vídeo, pois isso é frequentemente o mais visível quando há atraso de pacote (dados).

Conceitos básicos de uma conexão com a Internet

Provedor de serviços de Internet (ISP)

Você precisa de um ISP para acessar a Internet em sua rede. Há muitas opções a escolher para velocidades de conexão, bem como uma variedade de preços para atender às necessidades da sua empresa. Além do acesso à Internet, um ISP oferece e-mail, hospedagem de página da Web e muito mais.

Navegador da Web

Um aplicativo que vem em seu dispositivo. Há outros que você pode baixar. Depois de fazer o download, você pode abrir e digitar o endereço IP ou o site para o qual deseja acessar pela Internet. Alguns exemplos de navegadores da Web incluem:

Microsoft Edge

 ,

Crome

 ,

Firefox

 ,

e Safari.

 .

Se você não conseguir abrir algo ou se estiver tendo outros problemas de navegação, é fácil tentar abrir um navegador da Web diferente e tentar novamente.

Uniform Resource Locator (URL)

Em um navegador da Web, você normalmente digita o nome de um site que deseja acessar, ou seja, o URL, seu endereço da Web. Cada URL deve ser exclusiva. Um exemplo de URL é https://www.cisco.com.

Gateway padrão

Este é o roteador que o tráfego de rede local usa como saída para o provedor de serviços de Internet (ISP) e para a Internet. Em outras palavras, esse roteador conecta você com outros dispositivos fora do seu prédio e através da Internet.

Firewall

Um firewall é um dispositivo de segurança de rede que monitora o tráfego de rede de entrada e saída e decide se permite ou bloqueia o tráfego específico com base em um conjunto definido de regras de segurança, chamadas Access Control Lists (ACLs).

Os firewalls são a primeira linha de defesa na segurança de rede há décadas. Eles estabelecem uma barreira entre redes internas seguras e controladas que podem ser confiáveis e não confiáveis em redes externas, como a Internet.

Um firewall pode ser hardware, software ou ambos.

Para obter mais detalhes, confira Configuração básica do firewall no RV34x Series Router.

Listas de controle de acesso (ACLs)

Listas que bloqueiam ou permitem que o tráfego seja enviado de e para determinados usuários. As regras de acesso podem ser configuradas para serem aplicadas o tempo todo ou com base em uma programação definida. Uma regra de acesso é configurada com base em vários critérios para permitir ou negar acesso à rede. A regra de acesso é agendada com base no tempo em que as regras de acesso precisam ser aplicadas ao roteador. Eles são configurados em configurações de segurança ou firewall. Por exemplo, uma empresa pode querer impedir que os funcionários transmitam esportes ao vivo ou se conectem ao Facebook durante o horário comercial.

Largura de banda

A quantidade de dados que pode ser enviada de um ponto a outro em um determinado período. Se você tiver uma conexão com a Internet com uma largura de banda maior, a rede poderá mover dados muito mais rapidamente do que uma conexão com a Internet com uma largura de banda menor. O fluxo de vídeo exige muito mais largura de banda do que o envio de arquivos. Se estiver descobrindo que há um atraso no acesso a uma página da Web ou atrasos na transmissão de vídeo, talvez seja necessário aumentar a largura de banda na rede.

Cabo Ethernet

A maioria dos dispositivos em uma rede tem portas Ethernet. Os cabos Ethernet são o que os conecta a uma conexão com fio. As duas extremidades do cabo RJ45 são iguais e se parecem com as tomadas antigas do telefone. Eles podem ser usados para conectar dispositivos e para se conectar à Internet. Os cabos conectam dispositivos para acesso à Internet e compartilhamento de arquivos. Alguns computadores exigem um adaptador Ethernet, pois podem não fornecer uma porta Ethernet.

Redes e como elas se encaixam

Rede local (LAN)

Uma rede que pode ser tão grande quanto vários edifícios ou tão pequena quanto uma casa. Todos conectados à LAN estão no mesmo local físico e conectados ao mesmo roteador.

Em uma rede local, cada dispositivo recebe seu próprio endereço IP interno exclusivo. Eles seguem um padrão 10.x.x.x, 172.16.x.x - 172.31.x.x ou 192.168.x.x. Esses endereços são visíveis apenas dentro de uma rede, entre dispositivos e são considerados privados. Há milhões de locais que podem ter o mesmo pool de endereços IP internos que sua empresa. Não importa, eles são usados apenas em sua própria rede privada, então não há conflito. Para que os dispositivos na rede se comuniquem entre si, eles devem seguir o mesmo padrão dos outros dispositivos, estar na mesma sub-rede e ser exclusivos. Você nunca deve ver nenhum desses endereços neste padrão como um endereço IP público, pois eles são reservados apenas para endereços LAN privados.

Todos esses dispositivos enviam dados através de um gateway padrão (um roteador) para sair para a Internet. Quando o gateway padrão recebe as informações, ele precisa fazer a Network Address Translation (NAT) e alterar o endereço IP, já que qualquer coisa que saia pela Internet precisa de um endereço IP exclusivo.

Rede de longa distância (WAN)

Uma rede de longa distância (WAN) é uma rede que se espalha, às vezes globalmente. Muitas LANs podem se conectar a uma única WAN.

Somente endereços WAN podem se comunicar através da Internet. Cada endereço WAN deve ser exclusivo. Para que os dispositivos dentro de uma rede possam enviar e receber informações pela Internet, você deve ter um roteador na borda da rede (um gateway padrão) que possa conduzir NAT.

Clique para ler Configurar regras de acesso em um RV34x Series Router.

Tradução de Endereço de Rede (NAT)

Um roteador recebe um endereço WAN por meio de um ISP (Provedor de serviços de Internet). O roteador vem com o recurso NAT que leva o tráfego que sai da rede, converte o endereço privado para o endereço WAN público e o envia pela Internet. Ele faz o inverso ao receber tráfego. Isso foi configurado porque não há endereços IPv4 permanentes suficientes disponíveis para todos os dispositivos no mundo.

O benefício do NAT é que ele fornece segurança adicional ocultando efetivamente toda a rede interna por trás desse único endereço IP público. Os endereços IP internos geralmente permanecem os mesmos, mas se estiverem desconectados por algum tempo, configurados de uma certa maneira ou redefinidos para o padrão de fábrica, talvez não.

NAT Estático

Você pode configurar o endereço IP interno para permanecer o mesmo configurando o Dynamic Host Configuration Protocol (DHCP) estático no roteador. Os endereços IP públicos também não têm garantia de permanecer os mesmos, a menos que você pague para ter um endereço IP público estático através do ISP. Muitas empresas pagam por esse serviço para que seus funcionários e clientes tenham uma conexão mais confiável com seus servidores (web, correio, VPN, etc.), mas pode ser caro.

O NAT estático mapeia uma tradução um para um dos endereços IP privados para os endereços IP públicos. Cria uma tradução fixa de endereços privados para os endereços públicos. Isso significa que você precisaria de uma quantidade igual de endereços públicos como endereços privados. Isso é útil quando um dispositivo precisa ser acessível de fora da rede.

Clique para ler Configurando NAT e NAT estático no RV160 e RV260.

CGNAT

NAT de classe de operadora é um protocolo semelhante que permite que vários clientes utilizem o mesmo endereço IP.

VLAN

Uma rede local virtual (VLAN) permite segmentar logicamente uma rede de área local (LAN) em diferentes domínios de transmissão. Nos cenários em que dados confidenciais podem ser transmitidos em uma rede, as VLANs podem ser criadas para

aumentar a segurança, designando uma transmissão para uma VLAN específica. Somente usuários que pertencem a uma VLAN podem acessar e manipular os dados nessa VLAN. As VLANs também podem ser usadas para melhorar o desempenho, reduzindo a necessidade de enviar broadcasts e multicasts para destinos desnecessários.

Uma VLAN é usada principalmente para formar grupos entre os hosts, independentemente de onde os hosts estão fisicamente localizados. Assim, uma VLAN melhora a segurança com a ajuda da formação de grupos entre os hosts. Quando uma VLAN é criada, ela não tem efeito até que essa VLAN esteja conectada a pelo menos uma porta manual ou dinamicamente. Uma das razões mais comuns para configurar uma VLAN é configurar uma VLAN separada para voz e uma VLAN separada para dados. Isso direciona os pacotes para os dois tipos de dados, apesar de usar a mesma rede.

Para obter mais informações, leia as Melhores práticas de VLAN e as Dicas de segurança para os Cisco Business Routers.

Sub-rede

Frequentemente chamadas de Sub-redes, as sub-redes são redes independentes dentro de uma rede IP.

SSID

O SSID (Service Set Identifier) é um identificador exclusivo que os clientes sem fio podem se conectar ou compartilhar entre todos os dispositivos de uma rede sem fio. Ela diferencia maiúsculas de minúsculas e não deve exceder 32 caracteres alfanuméricos. Também é chamado de Nome da rede sem fio.

VPNs (Virtual private networks, redes virtuais privadas)

A tecnologia evoluiu e os negócios são frequentemente conduzidos fora do escritório. Os dispositivos são mais móveis e os funcionários frequentemente trabalham de casa ou enquanto viajam. Isso pode causar algumas vulnerabilidades de segurança. Uma VPN (Virtual Private Network) é uma excelente maneira de conectar trabalhadores remotos em uma rede de forma segura. Uma VPN permite que um host remoto atue como se estivesse localizado na mesma rede local.

Uma VPN é configurada para fornecer transmissão de dados segura. Há diferentes opções para configurar uma VPN e a maneira como os dados são criptografados. As VPNs usam SSL (Secure Sockets Layer), PPTP (Point to Point Tunneling Protocol) e protocolo de encapsulamento de camada dois.

Uma conexão VPN permite que os usuários acessem, enviem e recebam dados de uma rede privada, passando por uma rede pública ou compartilhada, como a Internet, mas ainda garantindo uma conexão segura a uma infraestrutura de rede subjacente para proteger a rede privada e seus recursos.

Um túnel VPN estabelece uma rede privada que pode enviar dados com segurança usando criptografia e autenticação. Os escritórios corporativos usam principalmente uma conexão VPN, pois ela é útil e necessária para permitir que seus funcionários tenham acesso à sua rede privada mesmo que estejam fora do escritório.

Uma conexão VPN pode ser configurada entre o roteador e um endpoint depois que o roteador tiver sido configurado para uma conexão de Internet. O cliente VPN depende inteiramente das configurações do roteador VPN para poder estabelecer uma conexão.

Uma VPN suporta VPN site a site para um túnel gateway a gateway. Por exemplo, um usuário pode configurar um túnel VPN em um local de filial para se conectar ao roteador em um local corporativo, de modo que o local da filial possa acessar com segurança a rede corporativa. Em uma conexão VPN site a site, qualquer pessoa pode iniciar a comunicação. Essa configuração tem uma conexão criptografada constante.

A VPN IPsec também suporta VPN cliente-servidor para um túnel host-para-gateway. A VPN do cliente para o servidor é útil ao conectar do laptop/PC de casa a uma rede corporativa através do servidor VPN. Nesse caso, somente o cliente pode iniciar a conexão.

Clique para ler Visão geral e práticas recomendadas do Cisco Business VPN.

Certificados

Uma etapa segura na configuração de uma VPN é obter um certificado de uma autoridade de certificação (CA). É usado para autenticação. Os certificados são adquiridos de qualquer número de sites de terceiros. É uma forma oficial de provar que seu site é seguro. Essencialmente, a AC é uma fonte confiável que verifica se você é uma empresa legítima e se pode ser confiável. Para uma VPN, você só precisa de um certificado de nível inferior a um custo mínimo. Você recebe check-out do CA e, depois que ele verificar suas informações, ele emitirá o certificado para você. Este certificado pode ser baixado como um arquivo em seu computador. Você pode então ir para o roteador (ou servidor VPN) e carregá-lo lá.

Os clientes geralmente não precisam de um certificado para usar uma VPN; é apenas para verificação através do roteador. Uma exceção a isso é o OpenVPN, que requer um certificado de cliente.

Muitas pequenas empresas optam por usar uma senha ou uma chave pré-compartilhada em vez de um certificado para simplificar. Isso é menos seguro, mas pode ser configurado sem nenhum custo.

Alguns artigos sobre este tópico que você pode gostar:

- Certificado (Import/Export/Generate CSR) no RV160 e RV260 Series Router

- Substitua o certificado autoassinado padrão por um certificado SSL de terceiros no roteador RV34x Series
- Gerenciar certificados no RV34x Series Router

Chave pré-compartilhada (PSK)

Esta é uma senha compartilhada, decidida e compartilhada antes da configuração de uma VPN e pode ser usada como alternativa para o uso de um certificado. Uma PSK pode ser o que você quer que seja, apenas tem que corresponder no local e com o cliente quando eles se configuram como um cliente em seu computador. Lembre-se, dependendo do dispositivo, pode haver símbolos proibidos que você não pode usar.

Vida útil principal

Com que frequência o sistema altera a chave. Essa configuração também precisa ser a mesma do roteador remoto.

Conclusão

Aí está, agora você tem muitos dos fundamentos para você ir embora.

Se você quiser continuar aprendendo mais, verifique estes links!

Práticas recomendadas para configurar endereços IP estáticos Visão geral e práticas recomendadas do Cisco Business VPN Melhores práticas de VLAN e Dicas de segurança para roteadores comerciais Cisco Backup da Internet - Windows Backup de Internet - Mac Como fazer login em um switch