シスコビジネスの新機能：機器および基本的なネットワーク用語集

目的

このドキュメントの目的は、初心者にCisco Business(Small Business)機器と一般的な用語について理解してもらうことです。トピックには、ハードウェアの利用、シスコのビジネス用語、一般的なネットワーク用語、シスコツール、データ交換の基本、インターネット接続の基本、ネットワークの組み合わせ方法などがあります。

概要

シスコの機器を使用してネットワークのセットアップを開始したばかりですか。ネットワークのセットアップと維持という新しい世界に入り込むのは圧倒的な可能性があります。この記事は、基本について理解するために役立ちます。知れば知るほど怖くなくなる！

シスコビジネスが提供するハードウェア

ルータ

ルータは、複数のネットワークを接続し、必要な場所にルートデータを接続します。また、これらのネットワーク上のコンピュータをインターネットに接続します。ルータを使用すると、ネットワークに接続されたすべてのコンピュータが1つのインターネット接続を共有できるため、コストを節約できます。

ルータはディスパッチャとして機能します。ネットワークを介して送信されるデータを分析し、データを転送するための最適なルートを選択して、その途中で送信します。

ルータは、ビジネスを世界に接続し、セキュリティの脅威から情報を保護し、他のコ

ンピュータよりも優先されるコンピュータを決定することもできます。

これらの基本的なネットワーキング機能に加えて、ルータにはネットワーキングをより簡単または安全にするために追加の機能が搭載されています。必要に応じて、ファイアウォール、バーチャルプライベートネットワーク(VPN)、またはインターネットプロトコル(IP)通信システムを備えたルータを選択できます。

最近開発されたCisco Businessルータには、RV160、RV260、RV340、およびRV345シリーズがあります。

最大 300 のアクセス ポイント グループ

スイッチは、ほとんどのビジネスネットワークの基盤です。スイッチは、コントローラとして機能し、コンピュータ、プリンタ、およびサーバをビルまたはキャンパス内のネットワークに接続します。

スイッチを使用すると、ネットワーク上のデバイスが互いに通信し、他のネットワークと通信して、共有リソースのネットワークを作成できます。情報共有とリソース割り当てを通じて、スイッチはコストを削減し、生産性を向上させます。

ネットワークの基本の一部として選択するスイッチには、2つの基本的なタイプがあります。マネージドおよびアンマネージド

> 管理対象外のスイッチは、すぐに動作しますが、設定はできません。ホームネットワーク機器は通常、アンマネージドスイッチを提供します。
> マネージドスイッチを設定できます。管理スイッチをローカルまたはリモートで監視および調整できるため、ネットワークトラフィックとアクセスをより詳細に制御できます。

スイッチの詳細については、「スイッチ用語集」を参照してください。

最近開発されたスイッチには、Cisco Business Switch CBS110、CBS220、CBS250、およびCBS350シリーズがあります。

CBSスイッチの違いを確認するには、次を参照してください

無線アクセス ポイント

ワイヤレスアクセスポイントを使用すると、デバイスをケーブルなしでワイヤレスネットワークに接続できます。ワイヤレスネットワークにより、新しいデバイスをオンラインで簡単に入手でき、モバイルワーカーに柔軟なサポートを提供できます。

アクセスポイントは、ネットワークのアンプとして機能します。ルータが帯域幅を提供している間、アクセスポイントはその帯域幅を拡張して、ネットワークが多数のデバイスをサポートできるようにし、それらのデバイスは遠くからネットワークにアクセスできるようにします。

しかし、アクセスポイントは単にWi-Fiを拡張するだけではありません。また、ネット

ワーク上のデバイスに関する有用なデータを提供し、予防的なセキュリティを提供し、その他の多くの実用的な目的を提供することもできます。

最近開発されたワイヤレスアクセスポイントであるCisco Business Wirelessには、ワイヤレスメッシュネットワークを可能にするAC140、AC145、およびAC240が含まれています。メッシュワイヤレスネットワークに詳しくない場合は、「Welcome to Cisco Business Wireless Mesh Networking」または「Cisco Business Wireless Networkに関するよくある質問(FAQ)」を参照してください。

ワイヤレスアクセスポイントに共通する用語を学びたい場合は、WAP用語集を参照してください。

マルチプラットフォーム電話

MPP電話機は、Session Initiation Protocol(SIP)を使用してVoice over IP(VoIP)通信を提供します。 これにより、従来の電話回線が不要になり、社内での電話機の携帯性が向上します。VoIPを使用すると、電話機はコストのかかるT1回線ではなく、既存のネットワークインフラストラクチャとインターネット接続を使用します。これにより、より少ない「回線」でより多くのコールを管理できます。 その他の有益なオプションには、コールの保留、コールの保留、コールの転送などがあります。一部のモデルでは、VoIPに加えてビデオ通信が可能です。

MPP電話は通常の電話のように設計されており、その目的のためだけに使用されますが、基本的にはコンピュータであり、ネットワークの一部です。MPP電話機には、インターネットテレフォニーサービスプロバイダー(ITSP)またはIP構内交換機(PBX)コール制御サーバからのサービスが必要です。WebEx Calling、Ring Central、VerizonはITSPの例です。Cisco MPP電話機で動作するIP PBXサービスの例には、アステリスク、Centile、およびMetaswitchプラットが含まれます。これらの電話機の多くの機能は、サードパーティのプロバイダー（FreePBXなど）を通じて特別にプログラムされているため、プロセス（駐車場、ボイスメールへのアクセスなど）は異なります。

最近開発されたCisco Business MPP電話機には、6800、7800、および8800シリーズがあります。

シスコビジネスで一般的に参照される

アドミニストレーションガイドとクイックスタートガイド

これらの2つの異なるリソースを検索して、製品とその機能に関する非常に詳細な情報を取得します。モデル番号を使用してサイトまたはWeb検索を行う場合は、どちらかのガイドを追加して、これらの長いガイドを表示できます。

デフォルト設定

デバイスには、あらかじめ選択されたデフォルト設定が用意されています。これらは、管理者が選択する最も一般的な設定です。必要に応じて設定を変更できます。

デフォルトのユーザ名とパスワード

以前のCisco Business機器では、デフォルトはユーザ名とパスワードの*両方*に対してadminでした。これで、ほとんどの場合、ユーザ名とパスワードの*両方*には*cisco*がデフォルトになっています。Voice over IP(VoIP)電話で、多くの設定を変更するには*admin*として*ログイン*する必要があります。セキュリティ上の理由から、パスワードをより複雑に変更することを強くお勧めします。

デフォルトIPアドレス

ほとんどのシスコ機器には、ルータ、スイッチ、およびワイヤレスアクセスポイントのデフォルトIPアドレスが付属しています。IPアドレスを覚えていなくて、特別な設定がない場合は、ペーパークリップを開いてデバイスのリセットボタンを少なくとも10秒間押すことができます。これにより、デフォルト設定にリセットされます。スイッチまたはWAPがDHCPが有効なルータに接続されておらず、スイッチまたはWAPにコンピュータで直接接続されている場合、これらはデフォルトのIPアドレスです。

Cisco Businessルータのデフォルト IPアドレスは192.168.1.1です。
Cisco Businessスイッチのデフォルト IPアドレスは192.168.1.254です。
Small Businessワイヤレスアクセスポイント(AP)のデフォルトIPアドレスは192.168.1.245です。新しいメッシュワイヤレスアクセスポイントのデフォルトIPアドレスはありません。

工場出荷時のデフォルトにリセット

Cisco Businessルータ、スイッチ、またはワイヤレスアクセスポイントを工場出荷時のデフォルト設定にリセットし、最初から設定し直す場合があります。これは、あるネットワークから別のネットワークに機器を移動する場合、または設定の問題を解決できない場合の最後の手段として役立ちます。工場出荷時設定にリセットすると、すべての設定が失われます。

出荷時のリセット後に復元できるように、設定をバックアップできます。詳細については、次のリンクをクリックしてください。

- Webベースユーティリティを使用したRV34xシリーズルータの工場出荷時のデフォルト設定のリブートまたは復元
- スイッチのバックアップと復元またはファームウェアの交換
- ワイヤレスアクセスポイントでのコンフィギュレーションファイルのダウンロード、バックアップ、コピー、および削除
- WAP125またはWAP581アクセスポイントのコンフィギュレーションファイルの管理

設定をバックアップしない場合は、デバイスを最初からセットアップし直して、接続の詳細を確認する必要があります。ほとんどのモデルには、リセットの手順を説明する記事が用意されていますが、最も簡単な方法は、開いたペーパークリップを使用して、デバイスのリセットボタンを少なくとも10秒間押すことです。これはMPP電話機には適用されないため、詳細についてはReset a Cisco IP Phoneを参照してください。

Webユーザインターフェイス(UI)

100シリーズのアンマネージドスイッチを除き、すべてのシスコビジネス機器にWeb UIが付属しています。

このタイプのインターフェイスは、画面に表示され、選択のオプションが表示されます。これらの画面をナビゲートするコマンドを知る必要はありません。Web UIは、グラフィカルユーザインターフェイス(GUI)、Webベースのインターフェイス、Webベースのガイダンス、Webベースのユーティリティ、またはWeb設定ユーティリティとも呼ばれます。

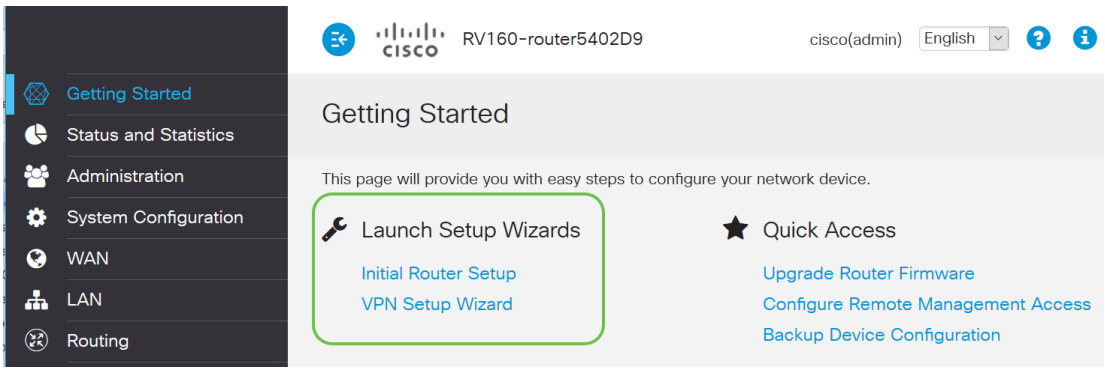
デバイスの設定を変更する最も簡単な方法の1つは、Web UIを使用することです。Web UIでは、デバイスのパフォーマンスを変更するために変更できるすべての機能を含むツールが管理者に提供されます。

シスコデバイスにログインすると、左側にナビゲーションペインが含まれたWeb UI画面が表示されます。デバイスのトップレベル機能のリストが含まれています。ナビゲーションペインは、ナビゲーションツリー、ナビゲーションバー、またはナビゲーションマップとも呼ばれます。

このページの色は、機器やファームウェアのバージョンによって、トップレベルの機能と同様に異なる場合があります。

セットアップウィザード

これは、Cisco Small Businessデバイスに初めてログインした後、その後に移動するインタラクティブ画面です。これは、ネットワーク上で起動して実行するための優れた方法です。変更可能なデフォルト設定が事前に選択されています。一部のデバイスには、複数のセットアップウィザードが付属しています。次の例は、2つのセットアップウィザード、初期ルータのセットアップ、および*VPNセットアップウィザードを示します。*



シスコ固有

シスコが特別に開発および所有している。たとえば、Cisco Discovery Protocol(CDP)はシスコ独自のものです。通常、シスコ独自のプロトコルはシスコデバイスでのみ使用できます。

シリーズのモデル

シスコは、小規模企業のオーナーに、自社のニーズに合わせて多くの異なるモデルを提供しています。多くの場合、モデルはさまざまな機能、ポート数、Power over Ethernet、またはワイヤレスで提供されます。シリーズに複数のモデルがある場合、シスコはモデルによって異なる番号または文字の代わりにxを配置しますが、この情報はそのシリーズのすべてのモデルに適用されます。たとえば、ルータRV340およびRV345はRV34xシリーズで参照されます。デバイスの端にPが付いている場合は、Power over Ethernet(PoE)を提供します。デバイス名がWで終わると、ワイヤレス機能が提供されます。一般に、モデルの数が多いほど、デバイスの機能が高くなります。詳細については、次の記事を参照してください。

- 製品デコーダリング – ルータ
- 製品IDデコーダ – スイッチ
- 製品デコーダリング – WAP
- Cisco Business Wireless Model Decoder（メッシュワイヤレス）

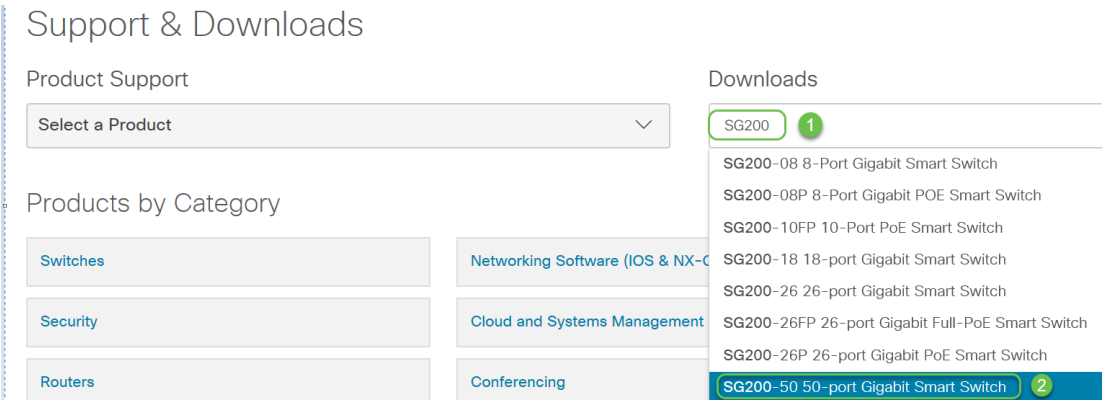
Firmware

イメージとも呼ばれます。デバイスの動作と機能を制御するプログラム。

Upgrade Firmware

すべてのデバイスで最適なパフォーマンスを得るには、ファームウェアのアップグレードが不可欠です。アップグレードをリリースするときにインストールすることが非常に重要です。シスコがファームウェアのアップグレードをリリースする際には、新しい機能や、セキュリティの脆弱性やパフォーマンスの問題を引き起こす可能性があるバグの修正などの改善が含まれることが多くなります。

シスコサポートに移動し、[Downloads]にアップグレードが必要なデバイスの名前を入力します。ドロップダウンメニューが表示されます。下にスクロールし、所有する特定のモデルを選択します。



ヒント：さまざまなバージョンのシスコのファームウェアを調べる際は、それぞれx.x.x.xの形式に従います。これは4オクテットと見なされますマイナーアップデートがあると、4番目のオクテットが変更されます。3番目のオクテットは、大きな変更になると変更されます。2番目のオクテットは大きな変化を意味します。最初のオクテットは、完全なオーバーホールの場合は変更されます。

ガイダンスが必要な場合は、このリンクをクリックして、任意のデバイスのファームウェアをダウンロードしてアップグレードしてください。

この記事では、スイッチのアップグレードで問題が発生した場合のトラブルシューティング方法をいくつか紹介しま[す。200/300シリーズスイッチのファームウェアのアップグレード](#)。

一般的なネットワーキング用語

機器を入手したら、ネットワーキングに関する一般的な用語について理解する必要があります。

インターフェイス

インターフェイスは、通常、あるシステムと別のシステムの間にあるスペースです。ポートを含め、コンピュータと通信できるあらゆるデバイス。通常、ネットワークインターフェイスにはローカルIPアドレスが割り当てられます。ユーザインターフェースは、ユーザがオペレーティングシステムと対話することを可能にする。

ノード

ネットワーク内で接続や対話を行うデバイス、または情報の送信、受信、保存、インターネットとの通信、およびIPアドレスを持つデバイスを表す一般的な用語。

ホスト

ホストは、ネットワーク上の通信のエンドポイントであるデバイスであり、ホストはデータまたはサービス（DNSなど）を他のノードに提供できます。トポロジに応じて、スイッチまたはルータをホストにすることができます。すべてのホストもノードです。たとえば、コンピュータ、サーバ、プリンタなどがあります。

コンピュータプログラム

コンピュータプログラムは、コンピュータ上で実行できる命令を運びます。

アプリケーション

アプリケーションソフトウェアは、タスクの実行に役立つプログラムです。これらは類似しているためによく同じ名前で呼ばれますが、すべてのプログラムがアプリケーションであるとは限りません。

ベスト プラクティス

ネットワークのセットアップと実行に推奨される方法。

トポロジ

機器が接続される物理的な方法。ネットワークのマップ。

設定

これは、設定の仕方を示します。機器を購入する際に事前設定されたデフォルト設定をそのまま使用することも、特定のニーズに合わせて設定することもできます。デフォルトの設定は、基本的な設定で、しばしば推奨されます。デバイスにログインすると、セットアップウィザードが表示され、操作をガイドできます。

MAC Address

各デバイスの固有識別子。物理デバイス上にあり、Bonjour、LLDP、またはCDPで検出できます。スイッチは、デバイスとの通信時にデバイスのMACアドレスを追跡し、MACアドレステーブルを作成します。これにより、スイッチは情報のパケットのルーティング先を知ることができます。

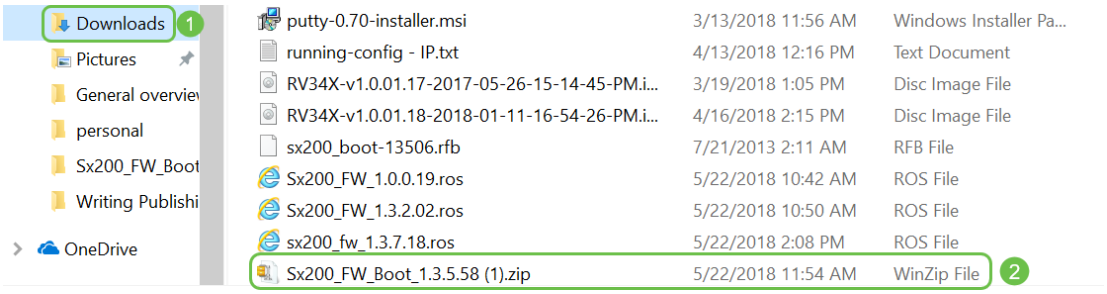
オープンソース

一般の人が無料で利用できるプログラム。

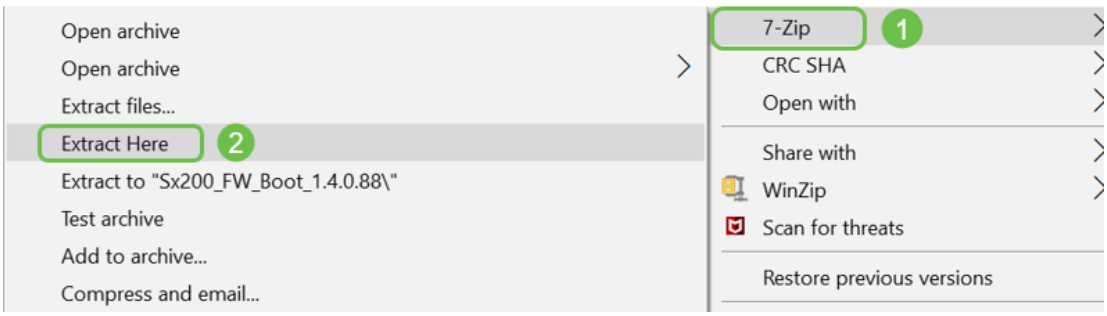
Zipファイル

1つのzipファイルに圧縮されたファイルのグループ。これは、複数のファイルを1つのステップで転送するときに使用されます。受信者はzipファイルを開き、それぞれに個別にアクセスできます。zipファイルの末尾は*.zip*です。

.zipで終わる形式のファイルが見つかった場合は、そのファイルを*解凍*する必要があります。解凍プログラムがない場合は、ダウンロードする必要があります。無料のオプションはオンラインでいくつかあります。解凍プログラムをダウンロードしたら、[ダウンロード]をクリックし、解凍する*必要がある*.zipファイルを探します。



zipファイルの名前を右クリックすると、次のような画面が表示されます。解凍ソフトウェアにカーソルを合わせ、[**Extract Here**]を**選択します**。この例では、7-Zipが使用されています。



コマンドライン インターフェイス (CLI)

コマンドラインインターフェイス(CLI):端末と呼ばれることもあります。これは、ルータやスイッチなどのデバイスの設定を選択する別のオプションとして使用されます。さまざまなWeb UI画面をナビゲートする必要がないため、この方法を使用すると、設定を簡単に行うことができます。この問題の解決は、コマンドを知り、完全に入力する必要があるということです。初心者向けの記事を読んでいるので、CLIが最初の選択肢ではないかもしれません。

仮想マシン

ほとんどのマシンは、必要よりも高い機能を備えています。コンピュータは、複数のマシンを実行するために必要なすべてを保持するようにプロビジョニングできます。この場合の問題は、一部がダウンしたり、リブートが必要になった場合は、すべて次のようになります。

VMwareまたはHyper-Vをインストールすると、ソフトウェア、Webサーバ、電子メールサーバ、FindITなどを1台のコンピュータにロードできます。仮想マシンは、別のオペレーティングシステムを使用することもできます。二人は論理的に独立している。各デバイスは、実際には1つではなく、個別のデバイスの機能を実行します。ハードウェアは共有されますが、各仮想マシンは物理リソースの一部を各オペレーティングシステムに割り当てます。これにより、コスト、エネルギー、スペースを節約できます。

使用できるシスコツール

Cisco Business Dashboard(CBD)

これは、ネットワークの監視と維持に使用されるシスコのツールです。CBDは、ネットワーク内のシスコデバイスの特定や、その他の便利な管理機能に役立ちます。

これは、複数のネットワークを自宅から実行したり、複数のネットワークを監視したりする場合に便利なツールです。CBDは仮想マシン上で実行できます。CBDの詳細については、Cisco Business Dashboard Support SiteまたはCisco Business Dashboard Overviewを参照してください。

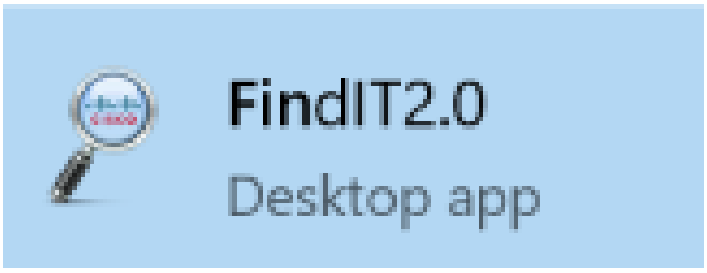
FindITネットワーク検出ユーティリティ

このシンプルなツールは非常に基本的ですが、ネットワーク上のシスコ製品を迅速に検出するのに役立ちます。Cisco FindITは、サポートされているすべてのCisco Small Businessデバイスを、PCと同じローカルネットワークセグメントで自動的に検出します。

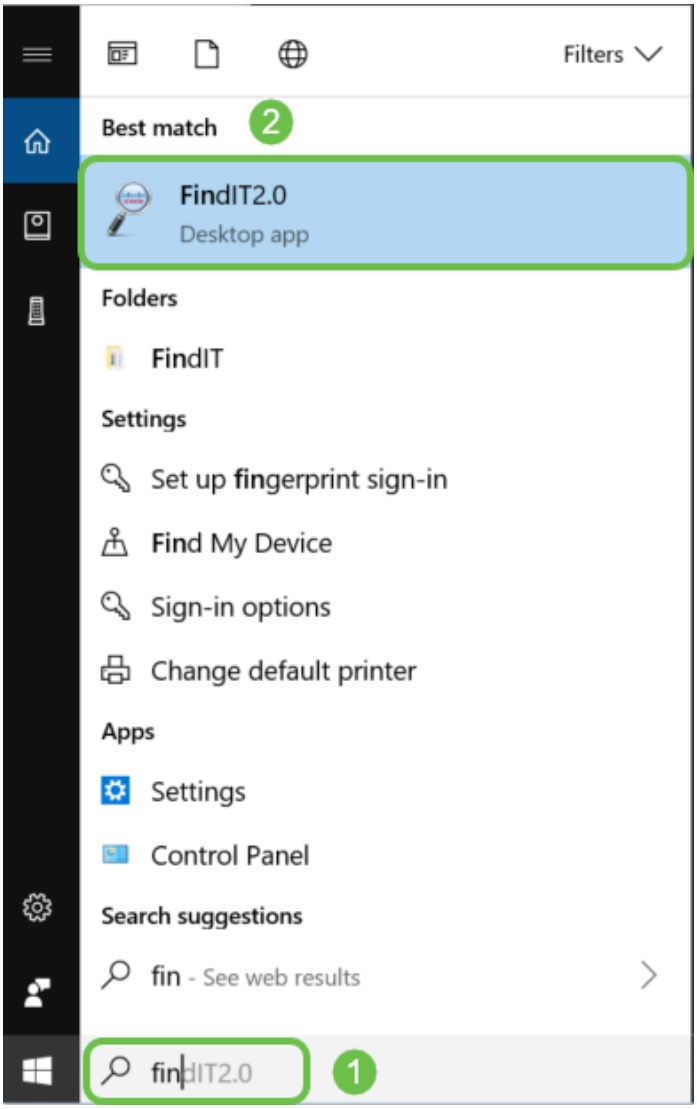
詳細については、をクリックしてください。また、Cisco Small Business FindIT Network Discovery Utilityをダウンロードしてください。

このリンクをクリックすると、『How to Install and Set Up Cisco FindIT Network Discovery Utility』の記事が表示されます。

Windows 10の場合、アプリケーションは次のようになります。



ダウンロードしたら、Windows 10で見つけることができます。



AnyConnect（RV34xシリーズルータ/VPN）

このVPNは、特にRV34xシリーズルータ（およびエンタープライズ/大規模企業の機器）で使用されます。 Cisco AnyConnectセキュアモビリティクライアントは、リモートユーザにセキュアなVPN接続を提供します。リモートエンドユーザにCisco Secure Sockets Layer(SSL)VPNクライアントの利点を提供し、ブラウザベースのSSL VPN接続では使用できないアプリケーションや機能もサポートします。リモートワーカーが一般的に使用するAnyConnectを使用すると、オフィスにいなくても物理的にオフィスにいるかのように、企業のコンピュータインフラストラクチャに接続できます。これにより、従業員の柔軟性、モビリティ、生産性が向上します。AnyConnectを使用するには、クライアントライセンスが必要です。Cisco AnyConnectは、次のオペレーティングシステムと互換性があります。Windows 7、8、8.1、および10、Mac OS X

10.8以降、およびLinux Intel(x64)。

詳細については、次の記事を参照してください。

- Windows コンピュータへの Cisco AnyConnect セキュア モビリティ クライアントのインストール
- Mac コンピュータへの Cisco AnyConnect セキュア モビリティ クライアントのインストール

データ交換の基本

パケット

ネットワークでは、情報はパケットと呼ばれるチャンクで送信されます。接続の問題がある場合、パケットが失われる可能性があります。

遅延

パケット転送の遅延。

冗長性

ネットワークでは、ネットワークの一部に問題が発生しても、ネットワーク全体が失敗しないように冗長性が設定されます。メイン設定に何かが発生した場合は、バックアップ計画と考えてください。

プロトコル

2つのデバイスが通信するには、同じ設定の一部が必要です。それを言語として考えなさい。一人がドイツ語を話し、もう一人がスペイン語しか話さない場合、彼らはコミュニケーションを取ることができなかった。異なるプロトコルが連携して動作し、相互に複数のプロトコルを送信できます。プロトコルの目的は異なります。次に、いくつかの例と簡単に説明します。

アドレッシングプロトコル

- Session Initiation Protocol(SIP)：インターネット上で通信するVoice over IP(VoIP)電話のメインプロトコルです。ネットワークの両側で同じプロトコルを使用して通信を開始するように設定する必要があるため、両方ともVoIP経由で通信を開始するためにSIPが必要です。
- Dynamic Host Configuration Protocol (DHCP)は、使用可能なIPアドレスのプールを管理し、ネットワークに参加するホストに割り当てます。
- Address Resolution Protocol(ARP):は、ダイナミックIPアドレスをLAN内の永続的な物理MACアドレスにマッピングします。
- IPv4:これは、現在使用されているIPの最も一般的なバージョンです。IPアドレスは、4組の数字（オクテットとも呼ばれる）を各組の間でピリオドで区切って記述します。

各セットは0 ~ 255の数値にすることができます。IPv4アドレスの例は8.8.8.8で、これはGoogleのパブリックDNSサーバです。IPv4には一意のIPアドレスよりも多くのデバイスが存在するため、永続的なパブリックIPアドレスを購入するとコストがかかります。

- **IPv6：この最新バ**ージョンでは、8セットの番号を使用し、各セットの間にコロンを付けます。16進数法を使用するため、IPアドレスに文字が含まれる場合があります。企業は、IPv4アドレスとIPv6アドレスを同時に実行できます。

IPv6について説明しているため、このアドレッシングプロトコルについて知っておくべき重要な詳細情報を次に示します。

IPv6の省略形：複数のセットのすべての数字がゼロの場合、行内の2つのコロンがこれらのセットを表すことができます。この省略形は1回しか使用できません。たとえば、GoogleのIPv6 IPアドレスの1つは2001:4860:4860::8888です。デバイスによっては、IPv6アドレスの8つの部分すべてに個別のフィールドを使用し、IPv6省略形を受け入れることができません。その場合は、2001:4860:4860:0:0:0:0:8888と入力します。

16進数：10の代わりに16の底を使用する数値体系。これは私たちが日常的に行う計算で使用する方法です。0 ~ 9の数字は同じ数字で表されます。10 ~ 15は文字A ~ Fで表されます。

データ転送プロトコル

- Transmission Control Protocol(TCP)とUser Datagram Protocol（UDP；**ユーザデータグラムプロトコル**）：これらは、データを転送する2つの方法です。TCPは、データを送信する前に、3ウェイハンドシェイクと呼ばれる接続を必要とするため、遅延が生じることがあります。データ（パケット）が失われた場合は、再送信されます。UDPの信頼性は低いが、高速である。多くの場合、音声とビデオはUDPを使用します。
- **ファイル転送プロトコル(FTP)：このプロトコル**は、クライアントからサーバーにファイルを転送するために使用されます。
- Hypertext Transfer Protocol(HTTP)とHypertext Transfer Protocol Secure(HTTPS)：**インターネットを介したデータ通信**の一般的な基盤。これらはWebサイトの冒頭にhttp://とhttps://と書いてあります。*https://*で始まるサイトの方が*安全*に使用できます。
- Routing Information Protocol (RIP)：**このプロト**コルは長い間使用されてきました。3つのバージョンがあり、各バージョンのセキュリティと機能が強化されています。ルータはルートを共有します。その目的は、1台のルータから次のルータまでの最大「ホップ」数を設定して、ループを防止することです。その他の、より効率的なルーティングのプロトコルには、Enhanced Interior Gateway Routing Protocol(EIGRP)、Open Shortest Path First(OSPF)、**およ**びIntermediate System to Intermediate System(IS-IS)**があります**。 この最後の3つのスケールはRIPよりも優れていますが、セットアップがより複雑になる可能性があります。
- **セキュアシェル(SSH)：コ**マンド回線トラフィックに安全なルートを提供するセキュアチャネル。これは、リモートサーバーとの通信に使用される暗号化されたプロトコルです。SSHを中心に多くの追加テクノロジーが構築されています。

検出プロトコル

- Cisco Discovery Protocol(CDP)：**直接接続されている他のシスコ機器に関する情報を検**

出し、その情報を保存します。BonjourとLink Layer Discovery Protocol(LLDP)は同じ機能を実行し、シスコ以外ののデバイスに情報をを取得します。ほとんどの小規模企業向けデバイスはLLDPを使用します。

- Layer Link Discovery Protocol(LLDP):デバイスがネイバーデバイスにID、設定、および機能をアドバタイズし、その後データを管理情報ベース(MIB)に保存できるようにします。 ネイバー間で共有される情報は、新しいデバイスをローカルエリアネットワーク(LAN)に追加するのに必要な時間を短縮し、多くの設定問題のトラブルシューティングに必要な詳細を提供します。LLDPは、シスコ独自ではないデバイスとシスコ独自のデバイスの間で作業する必要があるシナリオで使用できます。スイッチは、ポートの現在のLLDPステータスに関するすべての情報を提供します。この情報を使用して、ネットワーク内の接続の問題を修正できます。これは、ネットワーク内のデバイスを検出するためにFindIT Network Managementなどのネットワーク検出アプリケーションで使用されるプロトコルの1つです。

プロトコルの特定

- ドメインネームシステム(DNS):IPアドレスに完全修飾ドメイン名(FQDN)が割り当てられると、データベースに格納されます。たとえば、*www.google.com*を検索する場合は、Webサイト名を入力でき、データベースはこれを検索し、IPアドレスを通じてそこにアクセスできます。インターネットサービスプロバイダー(ISP)は、DNSサーバをデフォルトとして使用し、すでに設定済みです。ただし、インターネットの使用時に速度が遅いと思われる場合は、手動で変更できます。
- ダイナミックDNS:DDNSとも呼ばれ、ホスト名、アドレス、またはその他の関連情報のアクティブな設定でDNS内のサーバを自動的に更新します。つまり、DDNSは固定ドメイン名をダイナミックWAN IPアドレスに割り当てます。これにより、固定IPアドレスの購入コストが節約されます。
- インターネットプロトコル(IP):IPアドレスは、インターネット上のホスト間でデータの送受信を可能にする一意の識別子です。これは、ISPからの購入が必要なパブリックインターネットアドレスを介して実現されます。
- メディアアクセス制御（MACアドレス）：各デバイスに一意の識別子が接続されています。これは変更されません。ネットワークのセットアップとトラブルシューティングを行う際には、MACアドレスを知っておくことをお勧めします。通常はデバイス上にあり、文字と数字が含まれています。スイッチは、デバイスのMACアドレスを追跡し、MACアドレステーブルを作成します。

トラブルシューティングプロトコル

- ping:pingは一般的なトラブルシューティング方法です。pingは、ICMPエコーメッセージをIPアドレスに送信します。メッセージが返されて受信されます。正常な応答は、双方向物理接続を示します。これは、ネットワークデータパケットが問題なくアドレスに分散できるかどうかを確認する方法です。
- インターネット制御メッセージプロトコル(ICMP)：エラーおよび操作情報に関するメッセージ。pingテストを実行すると、ICMPエコーメッセージが宛先に送信されます。接続に成功すると、そのデバイスから応答が返されます。

サーバ

他のコンピュータにサービスを提供するコンピュータまたはコンピュータ上のプログ

ラム。サーバは仮想でも、アプリケーションでも構いません。1つのデバイスに複数のサーバを配置できます。サーバは互いに共有できます。Windows、Mac、またはLinuxで使用できます。

Webサーバ- WebブラウザのWebページのフォーマットと表示
ファイルサーバ：ネットワーク上のユーザにファイルとフォルダを共有します
電子メールサーバ – 電子メールの送信、受信、保存
DNSサーバ：例えば、www.cisco.comのようなユーザーフレンドリーな名前をIPアドレス173.37.145.84に変換します
インスタントメッセージングサーバ：インスタントメッセージ(Jabber、Skype)のフローを制御および管理します

Quality of Service（QoS）

これらの設定は、パケット（データ）の遅延が最も顕著になる場合が多いため、ネットワーク（通常は音声またはビデオ）上のトラフィックに優先順位が与えられるように設定されています。

インターネット接続の基礎

インターネットサービスプロバイダー(ISP)

ネットワーク上のインターネットにアクセスするには、ISPが必要です。接続速度に応じて選択できるオプションが数多くあり、ビジネスニーズに合わせて様々な価格を選択できます。インターネットへのアクセスに加えて、ISPは電子メール、Webページホスティングなどを提供しています。

Web ブラウザ

デバイスに付属するアプリケーション。他にもダウンロードできる機能があります。ダウンロードしたら、インターネット経由でアクセスするIPアドレスまたはWebサイトを開いて入力できます。Webブラウザの例は次のとおりです。

Microsoft Edge


、

クロム


、

Firefox


、

とSafariです


.

何かを開くことができない場合、または他のナビゲーションの問題が発生している場合は、簡単に別のWebブラウザを開いて再試行してください。

Uniform Resource Locator(URL)

Webブラウザでは、通常、アクセスするWebサイトの名前（URL、Webアドレス）を入力します。すべてのURLは一意である必要があります。URLの例はhttps://www.cisco.comです。

[Default Gateway]

これは、ローカルエリアネットワークトラフィックがインターネットサービスプロバイダー(ISP)およびインターネットへの出力として使用するルータです。つまり、このルータは、建物外やインターネット経由で他のデバイスと接続します。

Firewall

ファイアウォールは、着信および発信ネットワークトラフィックを監視し、アクセスコントロールリスト(ACL)と呼ばれる定義済みのセキュリティルールに基づいて特定のトラフィックを許可またはブロックするかどうかを決定するネットワークセキュリティデバイスです。

何十年にもわたって、ファイアウォールはネットワークセキュリティの最初の防衛線となっています。インターネットなどの外部ネットワークに対して信頼できる内部ネットワークと信頼できない外部ネットワークとの間に障壁を設けます。

ファイアウォールには、ハードウェア、ソフトウェア、またはその両方を使用できます。

詳細については、「RV34xシリーズルータの基本的なファイアウォール設定の構成」を参照してください。

Access Control List（ACL; アクセス コントロール リスト）

特定のユーザとの間で送受信されるトラフィックをブロックまたは許可するリスト。アクセスルールは、常に有効になるように、または定義されたスケジュールに基づいて設定できます。アクセスルールは、ネットワークへのアクセスを許可または拒否す

るためのさまざまな基準に基づいて設定されます。アクセスルールは、アクセスルールをルータに適用する必要がある時間に基づいてスケジュールされます。これらは、セキュリティまたはファイアウォール設定で設定されます。たとえば、ある企業が勤務時間中に従業員がライブスポーツをストリーミングしたり、Facebookに接続したりするのをブロックする場合があります。

帯域幅

あるポイントから別のポイントに一定時間内に送信できるデータの量。帯域幅の大きいインターネット接続の場合、ネットワークは帯域幅の小さいインターネット接続よりもはるかに高速にデータを移動できます。ストリーミングビデオは、ファイルの送信よりもはるかに多くの帯域幅を必要とします。Webページへのアクセス時に遅延が発生したり、ストリーミングビデオの遅延が発生したりする場合は、ネットワークの帯域幅を増やす必要があります。

イーサネット ケーブル

ネットワーク内のほとんどのデバイスにはイーサネットポートがあります。イーサネットケーブルは、有線接続用に接続するケーブルです。RJ45ケーブルの両端は同じで、古い電話ジャックのように見えます。デバイスの接続やインターネットへの接続に使用できます。ケーブルは、インターネットアクセスとファイル共有のためにデバイスを接続します。コンピュータによっては、イーサネットポートを備えていない場合があるため、イーサネットアダプタが必要になります。

ネットワークとネットワークの組み合わせ

ローカルエリア ネットワーク (LAN; Local Area Network)

複数の建物と同じ大きさまたは家庭と同じ小さなネットワーク。LANに接続されたすべてのユーザは、同じ物理的な場所にあり、同じルータに接続されています。

ローカルネットワークでは、各デバイスに固有の内部IPアドレスが割り当てられます。10.x.x.x、172.16.x.x ~ 172.31.x.x、または192.168.x.xパターンに従います。これらのアドレスは、ネットワーク内、デバイス間でのみ表示され、プライベートと見なされます。企業と同じ内部IPアドレスのプールを持つ可能性がある場所は数百万あります。これは問題ではありません。これらは独自のプライベートネットワーク内でのみ使用されるため、競合はありません。ネットワーク内のデバイスが互いに通信するためには、他のデバイスと同じパターンに従い、同じサブネット上にあり、一意である必要があります。これらのアドレスはプライベートLANアドレス専用に予約されているため、このパターンではパブリックIPアドレスとして表示されないはずです。

これらのデバイスはすべて、デフォルトゲートウェイ (ルータ) を介してデータを送信し、インターネットにアクセスします。デフォルトゲートウェイは、情報を受信すると、ネットワークアドレス変換(NAT)を実行し、インターネット経由で送信される何かが一意のIPアドレスを必要とするため、IPアドレスを変更する必要があります。

ワイドエリアネットワーク(WAN)

ワイドエリアネットワーク(WAN)は、時にはグローバルに広がるネットワークです。多くのLANは1つのWANに接続できます。

インターネット経由で相互に通信できるのはWANアドレスだけです。各WANアドレスは一意である必要があります。ネットワーク内のデバイスがインターネット経由で情報を送受信できるようにするには、ネットワークのエッジ（デフォルトゲートウェイ）にNATを実行できるルータが必要です。

RV34xシリーズルータのアクセスルールの設定をクリックして確認してください。

ネットワーク アドレス変換（NAT）

ルータは、インターネットサービスプロバイダー(ISP)経由でWANアドレスを受信します。 ルータにはNAT機能が備わっており、ネットワークから出るトラフィックを受け取り、プライベートアドレスをパブリックWANアドレスに変換し、インターネット経由で送信します。トラフィックを受信すると逆の処理を行います。これは、世界中のすべてのデバイスで使用可能な十分な固定IPv4アドレスがないために設定されました。

NATの利点は、内部ネットワーク全体を1つの一意のパブリックIPアドレスの背後に効果的に隠すことで、セキュリティを強化できることです。内部IPアドレスは頻繁に同じままですが、しばらく抜かれた場合、特定の方法で設定された場合、または工場出荷時のデフォルトにリセットされた場合は、そうでないことがあります。

スタティック NAT

ルータでスタティックDynamic Host Configuration Protocol(DHCP)を設定することで、内部IPアドレスを同じままに設定できます。パブリックIPアドレスは、ISP経由でスタティックなパブリックIPアドレスを取得する場合を除き、同じアドレスを維持することは保証されません。多くの企業がこのサービスに対して料金を支払うため、従業員や顧客はサーバ（Web、メール、VPNなど）への信頼性の高い接続を持っていますが、コストがかかることがあります。

スタティックNATは、プライベートIPアドレスの1対1変換をパブリックIPアドレスにマッピングします。プライベートアドレスからパブリックアドレスへの固定変換が作成されます。つまり、プライベートアドレスと同量のパブリックアドレスが必要になります。これは、デバイスがネットワークの外部からアクセスできる必要がある場合に便利です。

RV160およびRV260でのNATおよびスタティックNATの設定を参照してください。

CGNAT

キャリアグレードNATは、複数のクライアントが同じIPアドレスを使用できるようにする同様のプロトコルです。

VLAN

仮想ローカルエリアネットワーク(VLAN)を使用すると、ローカルエリアネットワーク(LAN)を論理的に異なるブロードキャストドメインにセグメント化できます。機密データがネットワーク上でブロードキャストされるシナリオでは、特定のVLANにブロードキャストを指定することでセキュリティを強化するためにVLANを作成できます。VLANに属するユーザだけが、そのVLANのデータにアクセスして操作できます。また、VLANを使用して、ブロードキャストやマルチキャストを不要な宛先に送信する必要性を減らし、パフォーマンスを向上させることもできます。

VLANは主に、ホストが物理的に配置されている場所に関係なく、ホスト間でグループを形成するために使用されます。したがって、VLANはホスト間のグループ形成を助けてセキュリティを向上させる。VLANが作成されると、そのVLANが手動または動的に少なくとも1つのポートに接続されるまでは、VLANは影響を受けません。VLANを設定する最も一般的な理由の1つは、音声用に個別のVLANを設定し、データ用に個別のVLANを設定することです。これにより、同じネットワークを使用しているにもかかわらず、両方のタイプのデータのパケットが転送されます。

詳細については、『Cisco Business RoutersのVLANのベストプラクティスとセキュリティのヒント』を参照してください。

サブネットワーク

サブネットと呼ばれるサブネットワークは、IPネットワーク内の独立したネットワークです。

SSID

Service Set Identifier(SSID)は、無線クライアントが無線ネットワーク内のすべてのデバイスに接続または共有できる一意の識別子です。大文字と小文字を区別し、32文字以下の英数字を使用してください。これは、ワイヤレスネットワーク名とも呼ばれます。

バーチャル プライベート ネットワーク (VPN)

テクノロジーが進化し、オフィス外で業務が行われることが多くなっています。デバイスはモバイル性が高く、従業員は自宅や出張先で仕事をすることが多い。これにより、セキュリティの脆弱性が発生する可能性があります。バーチャルプライベートネットワーク(VPN)は、ネットワーク上のリモートワーカーを安全な方法で接続する優れた方法です。VPNを使用すると、リモートホストを同じローカルネットワーク上に配置されているかのように動作させることができます。

VPNは、セキュアなデータ伝送を提供するように設定されています。VPNの設定とデータの暗号化方法には、さまざまなオプションがあります。VPNは、Secure Sockets Layer(SSL)、Point to Point Tunneling Protocol(PPTP)、およびLayer Two Tunneling Protocolを使用します。

VPN接続を使用すると、ユーザはインターネットなどのパブリックまたは共有ネットワークを経由し、プライベートネットワークとそのリソースを保護するために、基盤となるネットワークインフラストラクチャへのセキュアな接続を確保することで、プ

ライベートネットワークとの間でデータの送受信を行うことができます。

VPNトンネルは、暗号化と認証を使用してデータを安全に送信できるプライベートネットワークを確立します。企業オフィスはVPN接続を主に使用します。これは、従業員がオフィスの外からでもプライベートネットワークにアクセスできるようにするために便利で必要な機能です。

ルータがインターネット接続用に設定された後、ルータとエンドポイントの間にVPN接続を設定できます。VPNクライアントは、接続を確立できるVPNルータの設定に完全に依存しています。

VPNは、ゲートウェイ間トンネルのサイト間VPNをサポートします。たとえば、ユーザは、企業サイトのルータに接続するようにブランチサイトでVPNトンネルを設定し、ブランチサイトが企業ネットワークに安全にアクセスできるようにします。サイト間VPN接続では、誰でも通信を開始できます。この設定には、暗号化された接続が常に存在します。

IPsec VPNは、ホストとゲートウェイ間のトンネルに対するクライアントとサーバ間のVPNもサポートします。クライアントからサーバへのVPNは、自宅からVPNサーバを介してラップトップ/PCから企業ネットワークに接続する場合に便利です。この場合、クライアントだけが接続を開始できます。

クリックして、『Cisco Business VPN Overview and Best Practices』を参照してください。

証明書

VPNのセットアップにおける安全な手順は、認証局(CA)から証明書を取得することです。 これは認証に使用されます。証明書は、任意の数のサードパーティサイトから購入します。これは、あなたのサイトが安全であることを証明する公式の方法です。基本的に、CAは正当なビジネスであり、信頼できることを検証する信頼できるソースです。VPNの場合、低レベルの証明書が必要なのは最小限のコストだけです。CAによってチェックアウトされ、情報を確認すると、証明書が発行されます。この証明書は、コンピュータ上のファイルとしてダウンロードできます。その後、ルータ（またはVPNサーバ）に移動し、そこにアップロードできます。

通常、クライアントはVPNを使用するために証明書を必要としません。ルータを介した確認のためだけに使用されます。ただし、OpenVPNではクライアント証明書が必要です。

多くの小規模企業では、簡単に証明書の代わりにパスワードまたは事前共有キーを使用することを選択しています。これは安全性が低いですが、無償で設定できます。

このトピックに関する記事には、次のようなものがあります。

- RV160およびRV260シリーズルータの証明書（CSRのインポート/エクスポート/生成）
- RV34xシリーズルータのデフォルトの自己署名証明書をサードパーティのSSL証明書に置き換える
- RV34xシリーズルータでの証明書の管理

事前共有キー（PSK）

これは、VPNの設定前に共有パスワードとして決定され、共有されており、証明書を使用する代わりに使用できます。PSKは何でも構いません。PSKはサイトとクライアントがコンピュータ上でクライアントとして設定するときに一致する必要があります。デバイスによっては、使用できない禁止シンボルが存在する場合があることに注意してください。

キーライフタイム

システムがキーを変更する頻度。この設定は、リモートルータと同じである必要があります。

結論

これで、あなたは多くの基本を持っています。

さらに学習を続けたい場合は、これらのリンクをチェックしてください。

スタティックIPアドレスを設定するためのベストプラクティス Cisco Business VPNの概要とベストプラクティス シスコビジネスルータのVLANのベストプラクティスとセキュリティヒント インターネットバックアップ – Windows インターネットバックアップ – Mac スイッチにログインする方法