New to Cisco Business: Equipment and Basic Network Glossary

Objective

The objective of this document is to get beginners familiar with Cisco Business equipment and some general terms you should know. Topics include Hardware Available, Cisco Business Terms, General Networking Terms, Cisco Tools, The Basics of Exchanging Data, The Basics of an Internet Connection, and Networks and How They Fit Together.

Introduction

Are you just beginning to set up your network with Cisco equipment? It can be overwhelming to enter the whole new world of setting up and maintaining a network. This article is here to help get you familiar with some of the basics. The more you know, the less intimidating it will be!

Hardware Available from Cisco Business

Router

Routers connect multiple networks together as well as route data where it needs to go. They also connect computers on those networks to the Internet. Routers enable all networked computers to share a single Internet connection, which saves money.

A router acts as a dispatcher. It analyzes data being sent across a network, chooses the best route for data to travel, and sends it on its way.

Routers connect your business to the world, protect information from security threats, and can even decide which computers receive priority over others.

Beyond those basic networking functions, routers come with additional features to make networking easier or more secure. Depending on your needs, for example, you can choose a router with a firewall, a virtual private network (VPN), or an Internet Protocol (IP) communications system.

The most recently developed Cisco Business routers include the RV160, RV260, RV340, and RV345 series.

Switch

Switches are the foundation of most business networks. A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.

Switches allow devices on your network to communicate with each other, as well as with other networks, creating a network of shared resources. Through information sharing and resource allocation, switches save money and increase productivity.

There are two basic types of switches to choose from as part of your networking basics: managed and unmanaged.

> An unmanaged switch works out of the box but can't be configured. Home-networking equipment typically offers unmanaged switches.
> A managed switch can be configured. You can monitor and adjust a managed switch locally or remotely, giving you greater control over network traffic and access.

For more details on switches, check out **Switches Glossary of Terms**.

The most recently developed switches include the Cisco Business Switch CBS250 and CBS350 series.

Wireless Access Point

A wireless access point allows devices to connect to the wireless network without cables. A wireless network makes it easy to bring new devices online and provides flexible support to mobile workers.

An access point acts as an amplifier for your network. While a router provides the bandwidth, an access point extends that bandwidth so that the network can support many devices, and those devices can access the network from farther away.

But an access point does more than simply extend Wi-Fi. It can also give useful data about the devices on the network, provide proactive security, and serve many other practical purposes.

The most recently developed Wireless Access Points, Cisco Business Wireless, include the AC140, AC145, and AC240 which allow for a wireless mesh network. If you are unfamiliar with mesh wireless networks, you can read more in **Welcome to Cisco Business Wireless Mesh Networking** or **Frequently Asked Questions (FAQ) for a**

[Cisco Business Wireless Network](#).

If you would like to learn some terms that are common with Wireless Access Points, check out the **WAP Glossary of Terms**.

Multiplatform Phone

MPP phones provide Voice over IP (VoIP) communication using Session Initiation Protocol (SIP). This eliminates the need for traditional phone lines, making phones more portable within the company. With VoIP, a phone uses an existing network infrastructure and internet connection instead of costly T1 lines. This gives the ability to manage more calls with fewer 'lines'. Other beneficial options include placing calls on hold, parking calls, transferring calls, and more. Some models allow video communication in addition to VoIP.

MPP phones are built to look like a regular phone and are used only for that purpose, but essentially, they are a computer and are part of your network. MPP phones require either service from an Internet Telephony Service Provider (ITSP) or an IP Private Branch Exchange (PBX) call control server. **WebEx Calling**, **Ring Central**, and **Verizon** are examples of an ITSP. Some examples of IP PBX services that work with Cisco MPP phones include **Asterisk**, **Centile**, and **Metaswitch** platforms. Many features on these phones are programmed specifically through third-party providers (such as FreePBX), so processes (car park, accessing voicemail, etc.) can vary.

The most recently developed Cisco Business MPP phones include the 6800, 7800, and 8800 series.

Commonly Referenced in Cisco Business

Administration Guide and Quick Start Guide

These are two different resources to search through to get very detailed information about your product and its features. When you do a site or web search with your model number, you can add one or the other to view these longer guides.

Default Settings

Devices come with preselected, default settings. They are often the most common settings that an administrator would choose. You can change the settings to fit your needs.

Default Username and Password

In older Cisco Business equipment, the default was *admin* for both username and password. Now, most have a default of *cisco* for both username and password. On Voice over IP (VoIP) phones, you need to log in as *admin* to change many of the configurations. It is highly recommended that you change the password to be more complex for security purposes.

Default IP Addresses

Most Cisco equipment comes with default IP addresses for routers, switches, and wireless access points. If you can't remember the IP address and you don't have a special configuration, you can use an open paperclip to press the reset button on your device for at least 10 seconds. This will reset to default settings. If your switch or WAP is not connected to a router with DHCP enabled, and you are connected directly to the switch or WAP with your computer, these are the default IP addresses.

The default IP address of a Cisco Business router is 192.168.1.1.
The default IP address for a Cisco Business switch is 192.168.1.254.
The default IP address for a Small Business wireless Access Point (AP) is 192.168.1.245. There is no default IP address for the new mesh wireless access points.

Reset to Factory Default

There may come a time when you want to reset your Cisco Business router, switch, or Wireless Access Point back to factory default settings and start from scratch. This comes in handy when you move the equipment from one network to another, or as a last resort when you can't solve a configuration problem. When you reset to factory default settings you lose all configurations.

You can backup configurations so that you can restore them after a factory reset. Click on the following links for more information:

- **Reboot or Restore the Factory Default Settings of the RV34x Series Router through the Web-based Utility**
- **Backup and Restore or Swap Firmware on a Switch**
- **Download, Backup, Copy, and Delete Configuration Files on a Wireless Access Point**
- **Manage the Configuration Files on the WAP125 or WAP581 Access Point**

If you do not back up the configuration, you will need to set up the device again from scratch so make sure you have the connection details. Most models have an article detailing the steps to follow for a reset, but the simplest way to do this is to use an open paperclip and press the reset button on your device for at least 10 seconds. This does not apply to the MPP phones, so check out **Reset a Cisco IP Phone** for more information.

Web User Interface (UI)

Every piece of Cisco Business equipment comes with a Web UI, except for the 100 series unmanaged switches.

This type of interface, what you see on your screen, shows options for selection. You do not need to know any commands to navigate through these screens. The Web UI is also sometimes referred to as a Graphical User Interface (GUI), web-based interface, web-based guidance, web-based utility, or a web configuration utility.

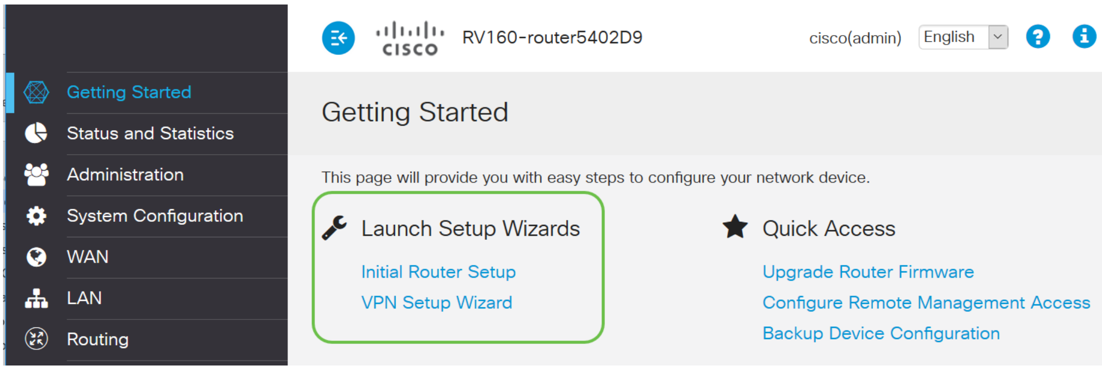
One of the easiest ways to change the configuration of a device is through the Web UI. The Web UI gives the administrator a tool that contains all of the possible features that can be changed to modify the performance of a device.

After you log into a Cisco device, you will see a Web UI screen that includes a navigation pane down the left side. It contains a list of the top-level features of the device. The navigation pane is also sometimes referred to as a navigation tree, navigation bar, or a navigation map.

The colors of this page may vary, as well as the top-level features, depending on the equipment and firmware version.

Setup Wizard

This is an interactive screen that you will navigate when you log in to a Cisco Small Business device for the first time, and possibly after that. It can be a great way to get you up and running on your network. There are several default settings preselected that can be changed. Some devices come with more than one Setup Wizard. This example shows two Setup Wizards, *Initial Router Setup*, and *VPN Setup Wizard*.



Cisco Proprietary

Specifically developed and owned by Cisco. For example, Cisco Discovery Protocol (CDP) is Cisco Proprietary. Usually, Cisco proprietary protocols can only be used on Cisco devices.

Models in a Series

Cisco offers small business owners many different models to fit the needs of their company. Often, a model will be offered with different features, number of ports, Power over Ethernet, or even wireless. If there are several models in a series, Cisco will put an x in place of the number or letter that varies between models, but the information applies to all in that series. For example, the routers RV340 and RV345 are referred to at the RV34x series. If a device has a P at the end it offers Power over Ethernet. If a device name ends in W it offers Wireless capabilities. In general, the higher the number of the model, the higher the capabilities of the device. To view details on this, check out the following articles:

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

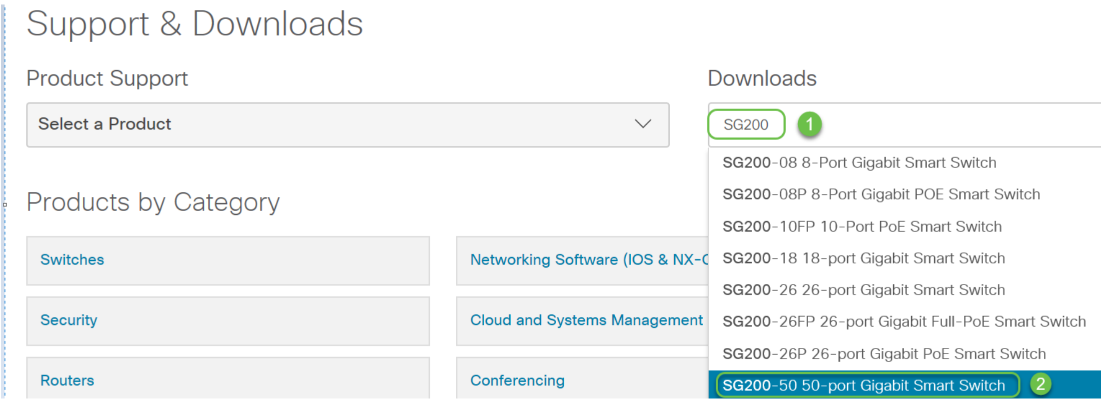
Firmware

Also known as an image. The program that controls the operations and functionality of the device.

Upgrade Firmware

Upgrading firmware is essential for optimum performance on every device. It is very important to install upgrades when they are released. When Cisco releases a firmware upgrade, they often contain improvements such as new features or fix a bug that can cause a security vulnerability or a performance issue.

Go to **Cisco Support**, and enter the name of the device that needs an upgrade under *Downloads*. A dropdown menu should appear. Scroll down and choose the specific model you own.



Tip: When looking through various versions of Cisco firmware, each follows a format of x.x.x.x. which are considered four octets. When there is a minor update, the fourth octet changes. The third octet changes when it is a bigger change. The second octet means a major change. The first octet changes if it is a complete overhaul.

If you want guidance, click on this link to **Download and Upgrade Firmware on any Device**.

This article has some troubleshooting ideas in case you are having issues with a switch upgrade: **Upgrade Firmware on a 200/300 Series Switch**.

General Networking Terms

Once you have your equipment, you should get familiar with some common terms in networking.

Interface

An interface is usually that space in between one system and another. Anything that can communicate with your computer, including ports. A network interface generally is assigned a local IP address. A user interface allows the user to interact with the operating system.

Node

A general term to describe any device that makes a connection or interaction within a network, or can send, receive, and store information, communicate with the Internet, and has an IP address.

Host

A host is a device that is an endpoint for communications on a network, the host can provide data or a service (Like DNS) to other nodes. Depending on the topology, a switch or a router can be a host. All hosts are also nodes. Examples include a computer, server, or printer.

Computer Program

A Computer Program carries instructions that can be run on a computer.

Application

Application software is a program that helps you perform tasks. They are often referred to interchangeably as they are similar, but not all programs are applications.

Best Practice

The recommended method for setting something up and running your network.

Topology

The physical way that your equipment is connected. A map of the network.

Configure

This refers to how things are set up. You can leave default settings, the ones that come preconfigured when you purchase equipment, or you can configure for your specific needs. Default settings are the basic, often recommended, configurations. When you log on to your device, there may be a Setup Wizard that can guide you through what to do.

MAC address

Unique identifier for each device. Is located on the physical device and can be detected with Bonjour, LLDP, or CDP. A switch keeps track of the MAC addresses on devices as it interacts with them and creates a MAC address table. This helps the switch know where to route packets of information.

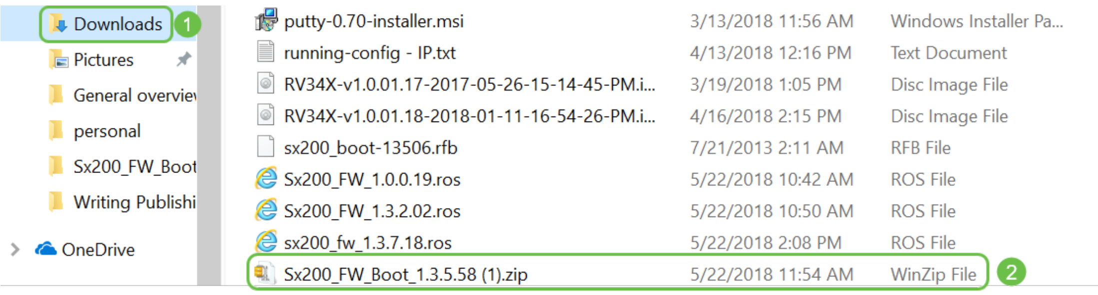
Open Source

A program that is available for free to the public.

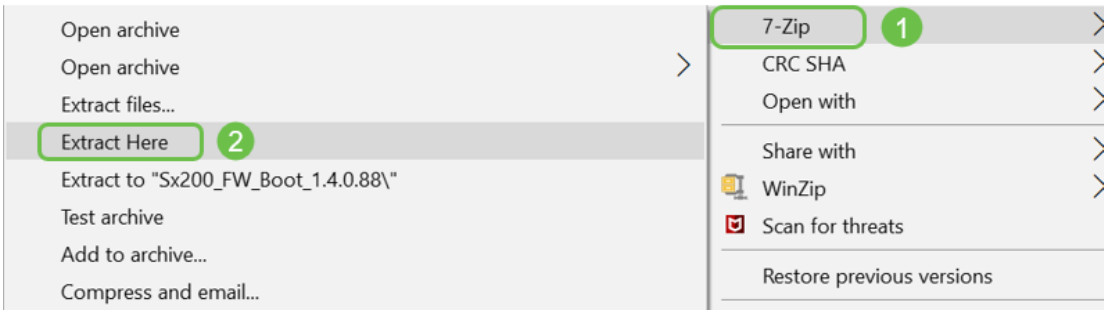
Zip File

A group of files compressed into one zip file. It is used when you want to transfer several files in one step. The receiver can open the zip file and access each one separately. A zip file ends in *.zip*.

If you see a file that is in a format ending in *.zip*, you must unzip that file. If you do not have an unzip program you will need to download one. There are several free options online. Once you have downloaded an unzip program, click **Downloads** and find the *.zip* file you need to unzip.



Right-click on the name of the zip file, a screen similar to this will appear. Hover over the unzip software, and choose **Extract Here**. In this example, 7-Zip is used.



Command Line Interface (CLI)

Command Line Interface (CLI): Sometimes referred to as terminal. This is utilized as another option for choosing configurations on devices such as routers and switches. If you are experienced, this can be a much simpler way to get things set up since you wouldn't have to navigate through various Web UI screens. The downfall of this is that you need to know the commands and enter them perfectly. Since you are reading an article for beginners, CLI probably shouldn't be your first choice.

Virtual Machine

Most machines have higher capabilities than they need. A computer can be provisioned to hold everything necessary to run more than one machine. The problem with this is that if one portion goes down or needs a reboot, they all follow.

If you install VMware or Hyper-V, you can load software, web servers, email servers, FindIT, and more on one computer. A virtual machine can even use a different operating system. They are logically independent of each other. Each performs the functions of a separate device without actually being one. Although the hardware is shared, each Virtual Machine allocates a part of the physical recourse for each operating system. This can save money, energy, and space.

Cisco Tools You Might Use

Cisco Business Dashboard (CBD)

This is a Cisco tool used to monitor and maintain networks. The CBD can help you identify Cisco devices in your network, as well as other helpful management features.

This is a beneficial tool if you run things from home or oversee more than one network. CBD can be run on a virtual machine. For more information on CBD, check out the **Cisco Business Dashboard Support Site** or **Cisco Business Dashboard Overview**.

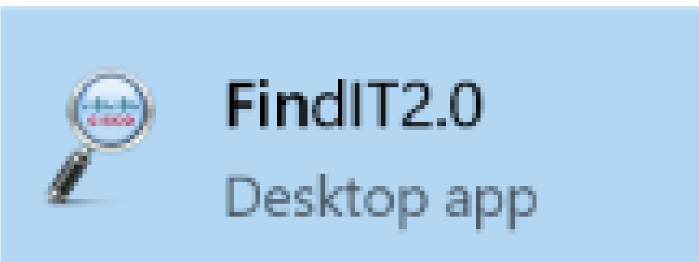
FindIT Network Discovery Utility

This simple tool is very basic but can help you to quickly discover Cisco gear on your network. Cisco FindIT automatically discovers all supported Cisco Small Business devices in the same local network segment as your PC.

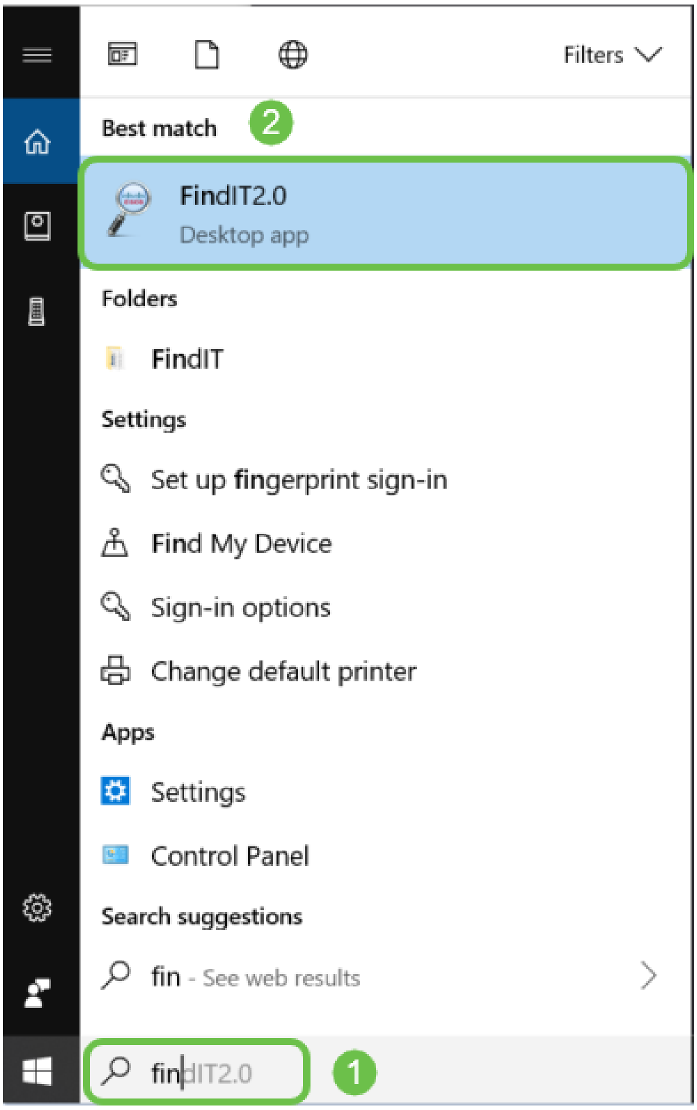
Click to learn more and to download the **Cisco Small Business FindIT Network Discovery Utility**.

Click this link to read an article on **How to Install and Set Up Cisco FindIT Network Discovery Utility**.

The Application looks like this for Windows 10.



Once it is downloaded you find it here in Windows 10.



AnyConnect (RV34x series routers/ VPNs)

This VPN is specifically used with the RV34x series routers (and enterprise/large company equipment). The Cisco AnyConnect Secure Mobility Client provides remote users with a secure VPN connection. It provides remote end-users with the benefits of a Cisco Secure Sockets Layer (SSL) VPN client and also supports applications and functions not available on a browser-based SSL VPN connection. Commonly used by remote workers, AnyConnect lets them connect to the corporate computer infrastructure as if they were physically at the office, even if they are not. This adds to the flexibility, mobility, and productivity of the workers. Client licenses are needed to use AnyConnect. Cisco AnyConnect is compatible with the following operating systems: Windows 7, 8, 8.1, and 10, Mac OS X 10.8 and later, and Linux Intel (x64).

Refer to the following articles for more guidance:

- **Install Cisco AnyConnect Secure Mobility Client on a Windows Computer**
- **Install Cisco AnyConnect Secure Mobility Client on a Mac Computer**

The Basics of Exchanging Data

Packet

In networking, information is sent in chunks, called packets. If there are connection issues, packets can get lost.

Latency

Delays in transferring packets.

Redundancy

In a network, redundancy is configured so that if part of the network has problems, the entire network doesn't fail. Consider it a backup plan if something happens to the main configuration.

Protocols

Two devices need to have some of the same settings to communicate. Think of it as a language. If one person only speaks German and the other one only speaks Spanish, they won't be able to communicate. Different protocols work together and there can be multiple protocols being transmitted within each other. Protocols have different purposes; some examples are listed and briefly described below.

Addressing Protocols

- **Session Initiation Protocol (SIP):** This is the main protocol for Voice over IP (VoIP), phones that communicate over the internet. Both sides of the network have to be set up using the same protocol to communicate so they would both need SIP to initiate communication over VoIP.
- **Dynamic Host Configuration Protocol (DHCP)** manages a pool of available IP addresses, assigning them to hosts as they join the network.
- **Address Resolution Protocol** (ARP): maps a dynamic IP address to a permanent physical MAC address in a LAN.
- **IPv4:** This is the most common version of IP used today. An IP address is written as 4 sets of numbers (also referred to as octets) separated by a period between each set. Each set can be a number between 0 and 255. An example of an IPv4 address is 8.8.8.8, which is the public DNS server at Google. There are more devices than unique IP addresses for IPv4, so it can be costly to purchase a permanent public IP address.
- **IPv6:** This latest version uses 8 sets of numbers with a colon between each set. It uses a hexadecimal numerical system, so there may be letters in the IP address. A company can have IPv4 and IPv6 addresses running concurrently.

Since we are talking about IPv6, here are a few important details to know about this addressing protocol:

IPv6 abbreviations: If all the numbers in several sets are zero, two colons in a row can represent those sets, this abbreviation can only be used once. For example, one of the IPv6 IP addresses at Google is 2001:4860:4860::8888. Some devices use separate fields for all eight parts of IPv6 addresses and cannot accept the IPv6 abbreviation. If that is the case, you would enter 2001:4860:4860:0:0:0:0:8888.

Hexadecimal: A numerical system that uses a base 16 instead of base 10, which is what we use in everyday math. The numbers 0-9 are represented the same. 10-15 are represented by the letters A-F.

Data Transfer Protocols

- **Transmission Control Protocol (TCP) and User Datagram Protocol (UDP):** These are two ways that data is transported. TCP requires a connection, called a three-way handshake, before sending data so sometimes there is a delay. If data (packets) are lost, it will send them again. UDP is less reliable, but faster. Often, voice and video use UDP.
- **File Transfer Protocol (FTP):** This protocol is used to transfer files from a client to a server.
- **Hypertext Transfer Protocol (HTTP) vs. Hypertext Transfer Protocol Secure (HTTPS):** The general basis for data communication over the internet. You will find these at the beginning of websites, written as *http://* and *https://*. Sites that start with *https://* are more secure to use.
- **Routing Information Protocol (RIP):** This protocol has been around for a long time. There are three versions, with each version adding more security and functionality. Routers share routes with each other. Its goal is to prevent loops by setting a maximum number of "hops" from one router to the next. Other, more efficient, protocols for routing include **Enhanced Interior Gateway Routing Protocol (EIGRP)**, **Open Shortest Path First (OSPF)**, and **Intermediate System to Intermediate System (IS-IS)**. These last three scale better than RIP but may be more complicated to set up.
- **Secure Shell (SSH):** A secure channel that provides a safe route for Command Line traffic. It is an encrypted protocol used to communicate with a remote server. Many additional technologies are built around SSH.

Discovery Protocols

- **Cisco Discovery Protocol (CDP):** Discovers information about other Cisco equipment that is directly connected and saves that information. **Bonjour** and **Link Layer Discovery Protocol (LLDP)** perform the same functions and can get information about non-Cisco devices as well. Most small business devices use LLDP.
- **Layer Link Discovery Protocol (LLDP):** Enables a device to advertise its identification, configuration, and capabilities to neighboring devices that then store the data in a Management Information Base (MIB). The information shared among the neighbors helps reduce the time needed to add a new device to the Local Area Network (LAN) and also provides details necessary to troubleshoot many configuration problems. LLDP can be used in scenarios where you need to work between devices that are not Cisco proprietary and devices which are Cisco proprietary. The switch gives all the information about the current LLDP status of ports and you can use this information to fix connectivity problems within the network. This is one of the protocols used by network discovery applications such as FindIT Network Management to discover devices in the network.

Identifying Protocols

- **Domain Name System (DNS):** Once there is a Fully Qualified Domain Name (FQDN) assigned to an IP address, it is put into a database. For example, when you search *www.google.com* you can enter the website name, and the database searches for it and can get you there through their IP address. Your **Internet Service Provider (ISP)** uses their DNS server as a default and it has already been configured. However, you can manually change this if you are finding slow speeds when using the internet.
- **Dynamic DNS:** Also referred to as DDNS, automatically updates a server in the DNS with the active configuration of its hostnames, addresses, or any other pertinent information. In other words, DDNS assigns a fixed domain name to a dynamic WAN IP address. This saves the cost of purchasing a permanent IP address.
- **Internet Protocol (IP):** IP addresses are unique identifiers that enable the sending and receiving of data between hosts on the internet. This is achieved via public internet addresses, which require purchase from an ISP.
- **Media Access Control (MAC address):** Each device has a unique identifier connected to it. This does not change. It is good to know your MAC address when setting up a network and troubleshooting. It is usually located on the device and contains letters and numbers. Switches keep track of MAC addresses of devices and create a MAC address table.

Troubleshooting Protocols

- **Ping:** A ping is a common troubleshooting method. A ping sends ICMP echo messages to an IP address. A message is received in return. A successful response shows two-way physical connectivity. It is a way to see if a network data packet can be distributed to an address without issues.
- **Internet Control Message Protocol (ICMP):** Messages about errors and operational information. When you do a PING test, an ICMP echo message is sent out to the destination. A successful connection gets a response from that device.

Server

A computer or a program on a computer that provides services to other computers. A server can be virtual or even an application. There can be multiple servers on one device. Servers can share with each other. They can be used with Windows, Mac, or Linux.

Web Servers - format and present web pages for web browsers
File servers – share files and folders to users on a network
Email servers – send, receive, and store emails
DNS Servers – translate user-friendly names such as www.cisco.com into IP address 173.37.145.84 for example
Instant Messaging servers – control the flow of and manage Instant messages (Jabber, Skype)

Quality of Service (QoS)

These settings are configured to make sure priority is given to traffic on a network, usually voice or video, as this is often the most noticeable when there is packet (data) delay.

The Basics of an Internet Connection

Internet Service Provider (ISP)

You need an ISP to access the Internet on your network. There are many options to choose from for connection speeds, as well as a variety of prices to fit the needs of your business. Besides access to the Internet, an ISP offers email, web page hosting, and more.

Web Browser

An application that comes on your device. There are others that you can download. Once it is downloaded you can open and enter the IP address or website you want to go to over the internet. Some examples of web browsers include:

Microsoft Edge

,

Chrome

,

Firefox

,

and Safari.

.

If you are unable to open something or you are having other navigation issues, an easy thing to try would be to open a different web browser and try again.

Uniform Resource Locator (URL)

In a web browser, you typically type the name of a website you want to access, that is the URL, their web address. Every URL must be unique. An example of a URL is **https://www.cisco.com**.

Default Gateway

This is the router that local area network traffic uses as an egress out to the Internet Service Provider (ISP) and the internet. In other words, this router connects you with other devices outside of your building and across the internet.

Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules, called Access Control Lists (ACLs).

Firewalls have been the first line of defense in network security for decades. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

For more details, check out **Configure Basic Firewall Settings on the RV34x Series Router**.

Access Control Lists (ACLs)

Lists that block or allow traffic from being sent to and from certain users. Access Rules can be configured to be in effect all the time or based on a defined schedule. An access rule is configured based on various criteria in order to allow or deny access to the network. The access rule is scheduled based on the time when the access rules need to be applied to the router. These are set up under security or firewall settings. For example, a business may want to block employees from streaming live sports or connecting to Facebook during business hours.

Bandwidth

The amount of data that can be sent from one point to another in a certain period of time. If you have an internet connection with a larger bandwidth, the network can move data much faster than an internet connection with lower bandwidth. Streaming video takes much more bandwidth than sending files. If you are finding that there is a lag when accessing a web page, or delays in streaming video, you may need to raise the bandwidth in your network.

Ethernet Cable

Most devices in a network have Ethernet ports. Ethernet cables are what plug into them for a wired connection. Both ends of the RJ45 cable are the same and look like the old phone jacks. They can be used to connect devices and to connect to the internet. The cables connect devices for Internet access and file sharing. Some computers require an Ethernet adapter, as they may not provide an Ethernet port.

Networks and How They Fit Together

Local Area Network (LAN)

A network that might be as big as several buildings or as small as a home. Everyone connected to the LAN is in the same physical location and is connected to the same router.

In a local network, each device is assigned its own unique internal IP address. They follow a 10.x.x.x, 172.16.x.x - 172.31.x.x, or 192.168.x.x pattern. These addresses are only visible inside a network, between devices, and are considered private. There are millions of locations that might have the same pool of internal IP addresses as your business. It doesn't matter, they are only used within their own private network so there is no conflict. In order for the devices in the network to communicate with each other, they should all follow the same pattern as the other devices, be on the same subnet, and be unique. You should never see any of these addresses in this pattern as a public IP address, as they are reserved for private LAN addresses only.

All of these devices send data through a default gateway (a router) to get out to the internet. When the default gateway receives the information, it needs to do Network Address Translation (NAT), and change the IP address since anything going out across the internet needs a unique IP address.

Wide Area Network (WAN)

A Wide Area Network (WAN) is a network that is spread out, sometimes globally. Many LANs can connect to a single WAN.

Only WAN addresses can talk to each other across the internet. Each WAN address has to be unique. In order for devices inside a network to be able to send and receive information over the internet, you must have a router at the edge of your network (a default gateway) that can conduct NAT.

Click to read **Configure Access Rules on an RV34x Series Router**.

Network Address Translation (NAT)

A router receives a WAN address through an Internet Service Provider (ISP). The router comes with NAT capability that takes traffic leaving the network, translates the private address to the public WAN address, and sends it out across the internet. It does the reverse when receiving traffic. This was set up because there are not enough permanent IPv4 addresses available for all of the devices in the world.

The benefit of NAT is that it provides additional security by effectively hiding the entire internal network behind that one unique public IP address. Internal IP addresses often stay the same, but if unplugged for a while, configured a certain way, or reset to factory default, it may not.

Static NAT

You can configure the internal IP address to stay the same by configuring static Dynamic Host Configuration Protocol (DHCP) on the router. Public IP addresses are not guaranteed to stay the same either unless you pay to have a static public IP address through your ISP. Many companies pay for this service so their employees and customers have a more reliable connection to their servers (web, mail, VPN, etc.) but it can be expensive.

Static NAT maps a one-to-one translation of the private IP addresses to the public IP addresses. It creates a fixed translation of private addresses to the public addresses. This means that you would need an equal amount of public addresses as private addresses. This is useful when a device needs to be accessible from outside the network.

Click to read **Configuring NAT and Static NAT on the RV160 and RV260**.

CGNAT

Carrier Grade NAT is a similar protocol that allows multiple clients to utilize the same IP address.

VLAN

A Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network (LAN) into different broadcast domains. In scenarios where sensitive data may be broadcast on a network, VLANs can be created to enhance security by designating a broadcast to a specific VLAN. Only users that belong to a VLAN are able to access and manipulate the data on that VLAN. VLANs can also be used to enhance performance by reducing the need to send broadcasts and multicasts to unnecessary destinations.

A VLAN is mainly used to form groups among the hosts regardless of where the hosts are physically located. Thus, a VLAN improves security with the help of group formation among the hosts. When a VLAN is created, it has no effect until that VLAN is attached to at least one port either manually or dynamically. One of the most common reasons to set up a VLAN is to set up a separate VLAN for voice, and a separate VLAN for data. This directs the packets for both types of data despite using the same network.

For more information, you should read **VLAN Best Practices and Security Tips for Cisco Business Routers**.

Subnetwork

Often called Subnets, Subnetworks are independent networks inside of an IP network.

SSID

The Service Set Identifier (SSID) is a unique identifier that wireless clients can connect to or share among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters. This is also called Wireless Network Name.

Virtual Private Networks (VPNs)

Technology has evolved, and business is often conducted outside of the office. Devices are more mobile, and employees often work from home or as they travel. This can cause some security vulnerabilities. A Virtual Private Network (VPN) is a great way to connect remote workers on a network in a secure way. A VPN allows a remote host to act as if it were located on the same local network.

A VPN is set up to provide secure data transmission. There are different options for setting up a VPN and the way the data is encrypted. VPNs use Secure Sockets Layer (SSL), Point to Point Tunneling Protocol (PPTP), and Layer Two Tunneling Protocol.

A VPN connection allows users to access, send, and receive data to and from a private network by means of going through a public or shared network such as the Internet but still ensuring a secure connection to an underlying network infrastructure to protect the private network and its resources.

A VPN tunnel establishes a private network that can send data securely using encryption and authentication. Corporate offices mostly use a VPN connection since it is both useful and necessary to allow their employees to have access to their private network even if they are outside the office.

A VPN connection can be set up between the router and an endpoint after the router has been configured for an Internet connection. The VPN client is entirely dependent on the settings of the VPN router to be able to establish a connection.

A VPN supports site-to-site VPN for a gateway-to-gateway tunnel. For example, a user can configure a VPN tunnel at a branch-site to connect to the router at a corporate site, so that the branch site can securely access the corporate network. In a site-to-site VPN connection, anyone can initiate communication. This configuration has a constant encrypted connection.

IPsec VPN also supports client-to-server VPN for a host-to-gateway tunnel. The client to server VPN is useful when connecting from Laptop/PC from home to a corporate network through the VPN server. In this case, only the client can initiate the connection.

Click to read **Cisco Business VPN Overview and Best Practices**.

Certificates

A secure step in setting up a VPN is obtaining a Certificate from a Certificate Authority (CA). This is used for authentication. Certificates are purchased from any number of third-party sites. It is an official way to prove that your site is secure. Essentially, the CA is a trusted source that verifies that you are a legitimate business and can be trusted. For a VPN you only need a lower-level certificate at a minimal cost. You get checked out by the CA, and once they verify your information, they will issue the certificate to you. This certificate can be downloaded as a file on your computer. You can then go into your router (or VPN server) and upload it there.

Clients usually don't need a Certificate to use a VPN; it is just for verification through the router. An exception to this is OpenVPN, which requires a client certificate.

Many small businesses choose to use a password or a pre-shared key in place of a certificate for simplicity. This is less secure but can be set up at no cost.

Some articles on this topic that you might enjoy:

- **Certificate (Import/Export/Generate CSR) on the RV160 and RV260 Series Router**
- **Replace the Default Self-Signed Certificate with a 3rd Party SSL Certificate on the RV34x Series Router**
- **Manage Certificates on the RV34x Series Router**

Pre-shared Key (PSK)

This is a shared password, decided, and shared before the configuration of a VPN and can be used as an alternate for using a certificate. A PSK can be whatever you want it to be, it just has to match at the site and with the client when they set up as a client on their computer. Keep in mind, depending on the device, there may be forbidden symbols that you cannot use.

Key Lifetime

How often the system changes the key. This setting also needs to be the same as the remote router.

Conclusion

There you have it, you now have many of the basics to get you on your way.

If you want to keep learning more, check these links out!

Best Practices for Setting Static IP Addresses **Cisco Business VPN Overview and Best Practices** **VLAN Best Practices and Security Tips for Cisco Business Routers** **Internet Backup - Windows Internet Backup - Mac How to Log into a Switch**