#### **Lesson Objectives**

* Recognize and define key network-related terminology
* Describe the concepts of the CIA Triad

#### **What Network Security Terminology Should You Know?**

Rather than torture you with slides here, I will provide a list of key terms below that you should know as we get started. We’ll go over a lot of these in the videos that follow, and I'll continue to provide new terms in each lesson.

Except otherwise noted, most of these definitions are from the [NIST Computer Security Resource Center](https://csrc.nist.gov/glossary). NIST is the National Institute of Standards and Technology, and many standards we rely upon in cybersecurity (and computing in general) were created by NIST.

In addition to the list of terms that you'll find in each lesson, a full glossary for this course is also available in the Resources tab of the course.

Key terms to know for this lesson include:

* Authentication - Verifying a user is who they say they are
* Authorization - Validating that an identity being claimed by the user is known to the system and verifying what that user should have access to.
* Availability - *This is part of the CIA Triad that we will talk about in the video below.* Availability means ensuring timely and reliable access to and use of information.
* Bit - A binary digit having a value of 0 or 1.
* Byte - A group of eight bits that is treated either as a single entity or as an array of 8 individual bits.
* Confidentiality - Another part of the CIA Triad, confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
* Identification - asserting an identity and having it confirmed
* Integrity - The last part of the CIA Triad, integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
* Defense-in-Depth - An information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. *Note: We will talk more about this concept in later lessons, but it’s good to start thinking about it now. A lot of what we are talking about here is how to defend our networks at every level. In the early days of network security, network administrators only concerned themselves with protecting the network at the perimeter or outward-facing edge of the network. As information security has evolved, it has become clear that we need to protect networks from the inside out, at each connection level in order to truly defend them.*
* Network - A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. *(Jenn's simpler definition: Two or more computers that are connected and share information and resources.)*
* Non-Repudiation - Not being able to deny you did something. In the context of network communications, non-repudiation refers to the proof of who the sender of a message was. In this way, the sender cannot deny that they sent it.
* Software - Computer programs and associated data that can be dynamically written and modified during execution.
* Threat Actor - An individual or a group posing a threat.

#### **Lesson Objectives**

* Describe what a network is
* Define some key concepts related to networks
* Describe the OSI Model

#### **Parts of a Network**

Before we jump into the video below, I want to describe some of the components you'll find in a basic network so you have a picture in your mind going forward. As we noted in the last lesson, a network is basically two or more computers that are linked together and share a common set of resources, files, and services. You likely have a home network, where you possibly have one or more desktops or laptops or phones or tablets connected to it. In fact, these days, you may even have a smart TV, doorbell, thermostat, or personal assistant device connected to that network as well. In order to connect your home network to the internet, you have a router, which is a device that connects networks and routes traffic between them.

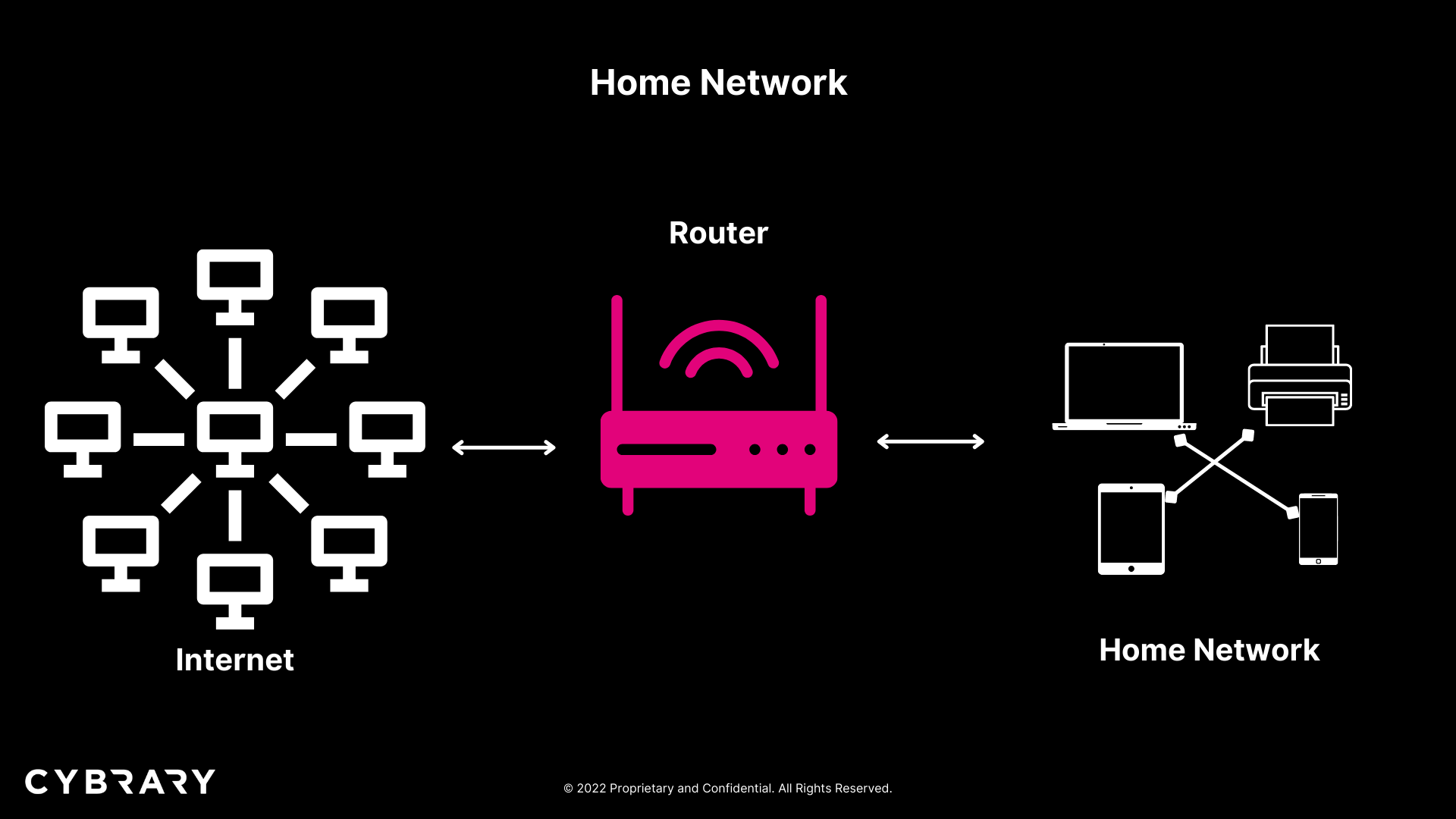


Image 2.1.1 - Home Network

Another device that you'll see in networks is called a switch or Ethernet switch. This is a device that connects nodes (computers) on the same network. So, unlike a router, a switch is only concerned about sending traffic between computers on the same network, rather than routing data between networks. You might encounter a switch at your office, where multiple computers on your LAN (Local Area Network) are connected via cables into a switch. You may not see the switch near your desk, as it may be located in a special room within your building, where network administrators can access it. A similar device is a hub. A hub also sends data between nodes on the same network, but the difference is that it broadcasts data to all nodes and is not smart enough to send only certain data to a certain node. Because switches can be used to send data to specific nodes, you may find that your office network only uses switches and does not have a hub.

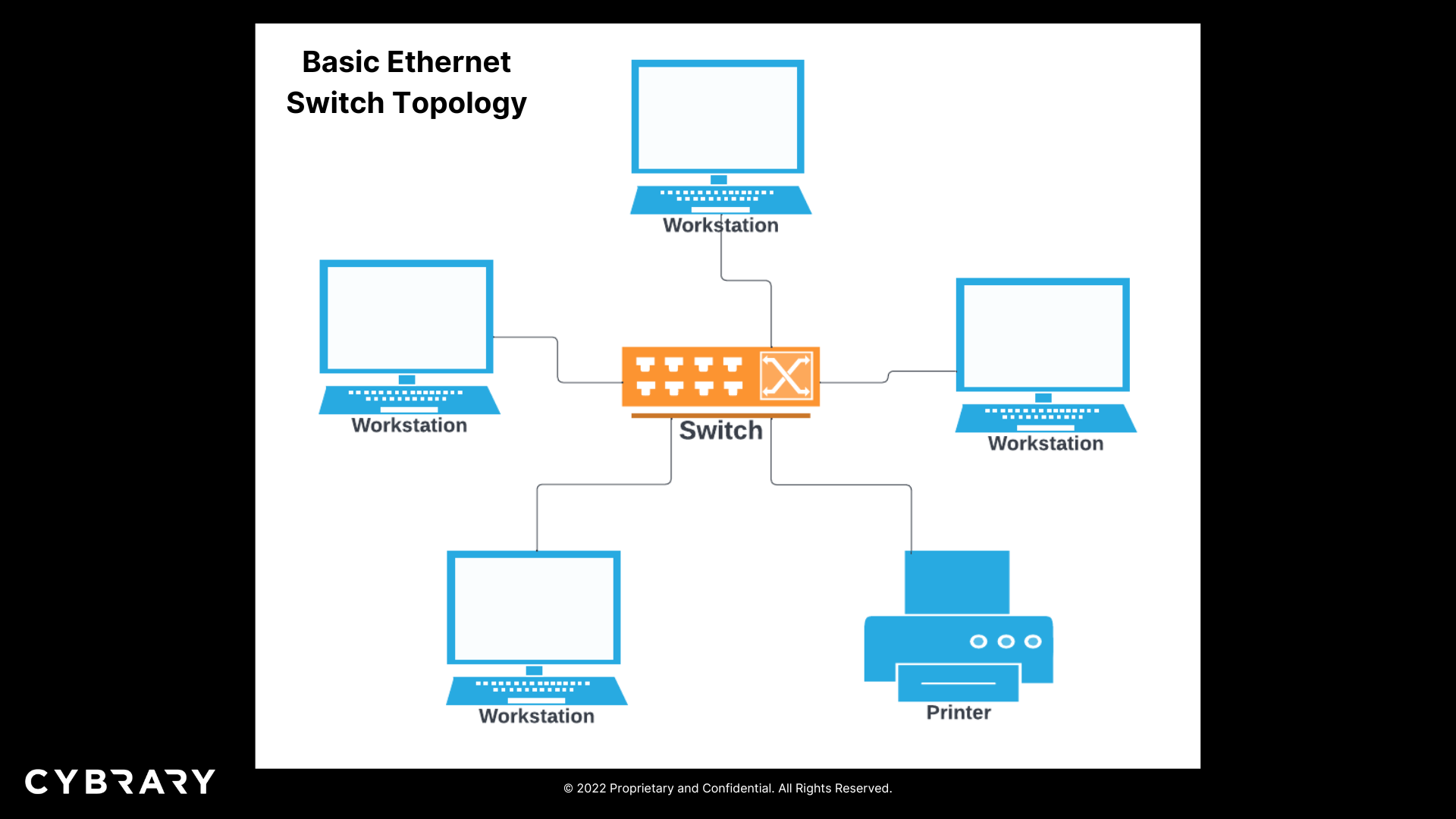


Image 2.2.2 - Ethernet Switch Topology

A few other items on a network that you need to know about are servers, firewalls, and endpoints. We'll start with endpoints, as we actually already mentioned them above. Endpoints are typically those things that end-users interact with, such as desktops, laptops, mobile phones, and so forth. That's sort of where the data ends as it goes out of a network, to a human, and back again. Then you have servers, these are simply computers that provide a particular service. Examples are web servers, email servers, print servers, and so forth. You can think of them as providing services that everyone needs (i.e., everyone needs to send email; everyone needs to print files, and so forth). And, then finally, firewalls are important devices in a network that filter traffic going between networks for the purposes of protecting the network. Typically, we think of the firewall as being something that protects us from bad things coming in from the internet, such as spam, viruses, and so forth.

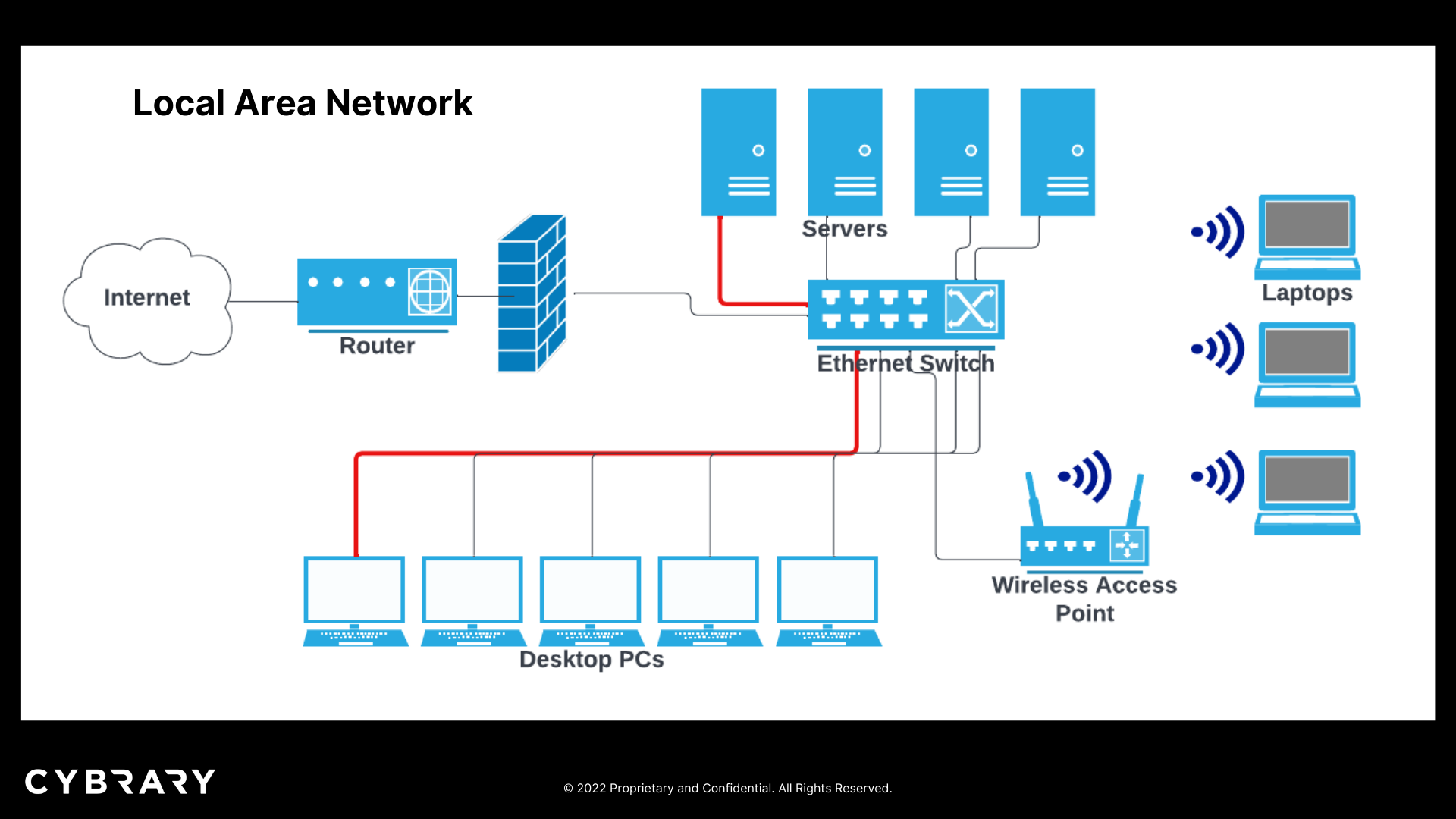


Image 2.2.3 - Basic Local Area Network Showing Servers and a Firewall

#### **A Quick Review of Network Device Terms**

To recap, here are the network terms covered above:

* Hub - According to [TechTarget](https://www.techtarget.com/searchnetworking/definition/hub), a network hub is "a node that broadcasts data to every computer or Ethernet-based device connected to it." *Remember that unlike a switch, a hub broadcasts to all nodes and cannot direct traffic to specific nodes.*
* Switch - A device that connects multiple nodes on the same network. *Remember that it is more sophisticated than a hub because it can direct traffic to only certain nodes instead of broadcasting to all nodes.*
* Router - A device that connects and routes traffic between networks
* Endpoint - Typically, an end-user device like a desktop, laptop, printer, mobile phone, etc.
* Server - A computer that is dedicated to providing a particular service, like a mail server or print server.
* Firewall - A device that filters traffic going between networks for the purposes of protecting the network

#### **A Little More about FTPS and SFTP**

First of all, be aware that some protocols deal with communication, some deal with management, and some deal with security. As such, they are often used in concert with each other. For example, a protocol that handles communication may be used along with a protocol that handles security. That is the case with the two secure versions of File Transfer Protocol (FTP): FTPS and SFTP. FTPS is where file transfer is being done with SSL (Secure Sockets Layer) encryption added to it. SFTP is where file transfer is being done with SSH (Secure Shell), which sort of provides a secure channel for the file transfer to take place. SSH itself is worth knowing more about, and I go into SSH a bit more below.

#### **What is a Shell?**

Since we talked about SSH, let's go into it a bit more and talk about a couple of other concepts that are sort of related and important for you to know in the context of cybersecurity.

* Shell - If SSH is a Secure Shell, what is a shell? A shell is a computer program that allows you to control a computer from a command-line interface (CLI). This is where you don't have a graphical user interface (with images and buttons and so forth), but just a command prompt, where you type in commands in order to control what's happening on the computer. I think of a shell as a sort of portal -- either to the control center of the computer I'm on or to a remote computer if I'm using SSH to connect remotely. As you move further in your cybersecurity journey, you will likely type commands from a CLI at some point, if you haven't already.
* SSH - As we've mentioned, SSH stands for Secure Shell. Per [Wikipedia](https://en.wikipedia.org/wiki/Secure_Shell), SSH is "a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution." It is also worth noting that SSH uses public key cryptography, and we will be talking about public keys in our lesson on encryption. In any case, I can't stress enough how important it is for you to know this protocol and the concept it represents. When a hacker wants to get access to a server on a network and control it, a major accomplishment would be for the hacker to obtain SSH credentials for that server. So, it's extremely important to protect those credentials, which should only be accessible to authorized administrators.
* Web Shell - A web shell, on the other hand, is a nefarious script that a hacker will use to access and control a web server remotely.

In the context of cybersecurity, you may hear the phrase, "get a shell," which typically refers to a hacker obtaining control over a server so as to carry out an attack.