Imagine Cup Junior

Cybersecurity

Module 6

Microsoft

Table of Contents

Disclaimer:

Microsoft and our partners created the Imagine Cup Junior guides and lesson materials and intended them to be for guidance only to support with the Imagine Cup Junior Challenge. For the latest on Microsoft Cybersecurity, please visit https://www.microsoft.com/en-us/security/.

Learning objectives

This module gives students an overview of information security and help them understand how it provides the foundation for secure internet usage. Students should understand the basics of how the internet works and apply the discussed security concepts to help secure their daily online lives.

IMPORTANT: Throughout this document, we demonstrate how to use specific processes and keyboard shortcuts. It's important to note that the processes and shortcuts we discuss might be different depending on the operating system you're using.

Introduction

After completing this module, students should be able to understand or explain:

- Information about security topics, terms, and concepts.
- How a computer works.
- Virtual machines (VMs) and cloud computing.
- Internet basics and how to use built-in Windows tools to review your network settings.
- Internet protocol and the OSI model.
- Several technical terms and their associated acronyms, including among others:
    - Transmission Control Protocol/Internet Protocol (TCP/IP)
    - IP
    - TCP
    - User Datagram Protocol (UDP)
    - Media Access Control (MAC)
    - Address Resolution Protocol (ARP)
    - network address translation (NAT)
    - Internet Control Message Protocol (ICMP)
    - Domain Name System (DNS).
- Understand security and the privacy issues associated with web browsing.
- Distinct types of malware.
- Typical cyberattacks, such as social engineering, drive-by downloads, lateral movement, zero day, and others.
- The importance of data and ways to protect it by applying the Confidentiality, Integrity, and Availability (CIA) model of information protection to prioritize critical security resources.
- Basic cryptographic principles, processes, procedures, and applications.

Topic	Learning objective *At this topic's conclusion, students should be able to:*	Key points for topic core content	Activity details
Understanding technology **Media resources needed:** • Screenshots • Exercises	Understand how a computer works. ---------------- Understand internet protocol and the OSI model. ---------------- Understand virtual machines (VMs) and cloud computing. ---------------- Understand internet basics and utilize built-in Windows tools to review your network settings. ---------------- Map a network using advanced TCP/IP services, TCP, UDP, MAC, ARP, NAT,	Typical computer hardware purposes. ---------------------- Overview of the internet model compared to OSI model. ---------------------- How virtualization led to cloud computing. ---------------------- The basic internet services, focused on Wi-Fi. ---------------------- Top seven IP scanner tools. Top 7 IP Scanner Tools for Network Mapping and IP enumeration (securitytrails.com)	To determine the specifications for your device, you should enter **Settings** in the **Search** bar in Windows, select **System**, and then select **About** it. The system's **Device specifications** for this PC will display. ------------------------ Short quiz on the models. ------------------------ Create a VM on their local computer that's running Windows 10. Use labs for trainings - Azure Lab Services | Microsoft Docs ---------------------- Windows PowerShell & classic commands: **Get-NetIPAddress : ipconfig** **Test-NetConnection -TraceRoute : tracert** **Test-NetConnection : ping**

Topic	**Learning objective** *At this topic's conclusion, students should be able to:*	Key points for topic core content	Activity details
	ICMP, DNS, and other services.		**Test-NetConnection -Port : telnet** ------------------------ - Define the terms and the services. - Use the tools and services to map a network.
Analysing data risks. Applying security concepts to help mitigate popular attack vectors. Media resources needed: - Screenshots - Exercises	Understand security and the privacy issues associated with web browsing and passwords. ---------------- Understand distinct types of malware and phishing attacks ---------------- Explain typical attacks, such as social engineering, drive-by downloads, lateral movement, zero day, and other attacks.	Browser security practices. ---------------------- Discuss some well know attack types. Focus on prevention A guide to malware for entrepreneurs (microsoft.com) ---------------------- Attack vectors and their importance; a discussion about current common attack vectors. What is an Attack Vector? 16 Common Attack Vectors in 2021 | UpGuard	Discuss common browser security practices and password safety, such as don't reuse passwords. Use an InPrivate browser window. Examine and enable Windows Credential Manager. Microsoft Edge password strength and reuse warning. Protect your online accounts using Password Monitor (microsoft.com) ------------------------ Enable multifactor authentication. Microsoft account

Topic	Learning objective *At this topic's conclusion, students should be able to:*	Key points for topic core content	Activity details
			security info & verification codes Discuss virtual private network (VPN) usage. Discuss using a password manager.
Securing data	Understand the importance of data and ways to help protect it by applying the Confidentiality, Integrity, and Availability (CIA) triad model to prioritize critical security resources. ---------------- Comprehend basic cryptographic principles, processes, procedures, and applications.	The CIA triad forms the core foundation for the development of security systems and policies for organizations. The CIA triad plays a crucial role in helping keep your data safe and secure against growing cyberthreats. Similar content to Course 40551-A: Microsoft Security Workshop: Enterprise Security Fundamentals - Learn | Microsoft Docs ---------------------- Encryption mitigation to help prevent the risk of unauthorized data disclosure.	Short quiz on module content. ----------------------- Turn on device encryption Turn on device encryption (microsoft.com)

Topic	Learning objective *At this topic's conclusion, students should be able to:*	Key points for topic core content	Activity details
		Discuss Microsoft data-at-rest and data-in-transit encryption solutions.	

Understand the technology

Given that we don't know what you'll be building for your project, we'll provide general information about the protocol and services you'll need to support and help secure your projects. Let's start with some basic computer components.

Understand how a computer works

Notes for the educator

To activate learning and engage the students in the topic, ask them to add to a list of all computing devices or devices that contain computer technology that they're used or interacted with since they woke up this morning. After you've recorded their ideas, ask them "What basic differences are there between the computing devices you observe in this list? Can you categorize them into two basic types?"

The goal is that students can identify the wide variety of computing devices with which they interact and recognize differences between general processing computers (such as their laptop or calculator) and embedded computers (such as those in automobiles or smart phones).

What is a computer architecture?

A computer's architecture defines its functionality, and compatibility, and computer architecture isn't static or uniform across all devices. The design and construction of a device's architecture supports specific tasks. For example, a cell phone's architecture is significantly different from the architecture that supports self-driving cars.

We have all used computers, even if we don't recognize that we have. At a high level, they're divided into *general-processing* and *embedded* computers. You can program general-processing computers to perform a variety of tasks, while embedded computers traditionally have a fix programming purpose. Some examples of embedded computers are cell phones, video-game consoles, and digital watches. Examples of general-processing computers include laptops, mainframes, supercomputers, and cloud-compute services.

The two categories of computers serve different purposes, but they share many similar components. They all have at least one processor, and memory and input/output functionality so they can process, retrieve, and store data. Any device with a digital "heartbeat" is a computer.

However, the various hardware components come in all shapes, sizes, and capacities, each with a specific role in a computer system's function. Let's now discuss the major common computer components and their functions.

Central processing unit

Notes for the educator

If your students have limited knowledge about computer architecture and how computers function, consider playing the following video for them to ensure everyone has the basic information about CPUs and other computer components: *Inside Your Computer* at https://www.youtube.com/watch?v=AkFi90lZmXA.

To reinforce what the students will be learning in the next several sections of these materials, either play the following video for them or assign it as independent work: *See how a CPU works* at https://www.youtube.com/watch?v=cNN_tTXABUA.

The central processing unit (CPU) is the main computer component that processes all of its data. A CPU is defined by the manufacture's *instruction set*. The instruction set provides commands in the machine language of the specific CPU to tell it what it is supposed to do. The CPU, in a sequential process, executes each instruction that's fed to it. This process is the *machine cycle*, and it repeats for each instruction.

Intel and AMD CPUs run the x86 instruction set. The Intel instruction set has been extended over time to support 16-bit, 32-but, and 64-bit computers. The x86 instructions set consists of over 1,500 defined instructions, while the Intel instruction set defines a complex instruction set computing (CISC).

The Advanced RISC Machines (ARM) processor is classified as a reduced instruction set computing (RISC). The initial ARM instruction set had 50 defined instructions. However, its instruction set also has been extended over time. RISC processors typically execute an instruction with fewer clock cycles. Because of the larger instruction set of CISC processors, they require more transistors than a RISC processor. Fewer transistors mean lower energy requirements. Risk architectures have become incredibly popular in low power and portable devices such as smart TVs, smart watches, phones, tablets, and similar. Because of this, ARM processors and other architectures that are based on RISC now comprise more than 90 percent of all processors in use today. For a good video overview, refer to SLR2 Types of processor | CISC vs RISC.

All CPUs have some variation of the following components:

- *Control unit,* which retries the instructions and data to and from the storage unit, which the CPU is processing.
- *Arithmetic logic unit* (ALU), which performs all computations within the CPU. Most ALUs perform integer operations faster than floating point operations.

> **Note** *Floating point numbers* are numbers that contain floating decimal points. For example, the numbers 5.5, 0.001, and -2,345.6789 are floating point numbers. Numbers that don't have decimal places are called *integers*. Computers recognize real numbers that contain fractions as floating point numbers." For more information, refer to Floating Point Definition (techterms.com).

- *Input unit,* which connects the computer to the outside environment. An example is a keyboard.
- *Output unit*, which connects the computer's internal processing to the outside environment. An example is a monitor or phone screen.
- *Storage unit*, which holds the data and instructions. We'll delve into storage in subsequent sections.

CPU clock speed

As previously mentioned, the machine cycle is the main activity of the CPU. It consists of a four-step process that includes:

1. **Fetch** the instruction from memory.
2. **Decode** the instruction into commands**.**
3. **Execute** the commands**.**
4. **Store** the results back into memory**.**

It a CPU can perform more cycles per second, it can process data or instructions faster. A CPU's clock speed is measured in hertz (unit of frequency equal to one cycle per second). Most modern CPUs perform in the gigahertz (GHz) range. So, a CPU with a 2.9 GHz rating can perform 2,900,000,000 clock cycles per second.

Notes for the educator

Summarize the four-step machine cycle. Demonstrate the process by asking students to respond to written directions to solve simple mathematical problems. To reinforce the process, use the following video: *The Fetch-Execute Cycle: What's Your Computer Actually Doing? at https://www.youtube.com/watch?v=Z5JC9Ve1sfI.*

CPU cores

A CPU core is a CPU processor. Initially, computers had one or more physical CPUs in their systems. However, with technological advancements, manufacturers now can place more than one CPU within a single physical chip. A single CPU can perform one task at a time. Multi-core CPUs can process commands simultaneously based on the number of cores. For example, a four-core CPU can process four sets of commands at once.

Possible task

1. Use Task Manager on a Windows operating system (OS) to observe how many cores or logical processors your PC has. On Windows 10, select Ctrl+Shift+Esc to open Task Manager, and then select the **Performance** tab.
   For more information, Find out how many cores your processor has.
2. Download and install CPU-Z from CPUID. CPU-Z is freeware that gathers information on your system's main devices, including:
   - Processor name and number, codename, process, package, and cache levels.
   - Mainboard and chipset.
   - Memory type, size, timings, and module specifications (SPD).
   - Real-time measurements of each core's internal frequency, and memory frequency.

Motherboard or logic board

A system's motherboard is like your central nervous system. It's basically a large circuit board that fits into the computer. All of the computer's components plug into this board, including the CPU. The motherboard has sockets for the CPU, memory, expansion slots or bus slots, and pathways for data and instructions to flow into and out of all the system's connected components. Motherboards come with several input/output interfaces on its input/output panel. A universal serial bus (USB) port is the most common interface on a computer motherboard. Motherboards will typically have several USB ports because there are so many different peripherals that utilize the USB interface, such as a mouse, keyboard, headphones, and similar. In addition to connectivity, the USB port also supplies electrical power to the USB ports.

Additionally, there can be a RJ-45 wired Ethernet connector and/or a wireless network connector.

What motherboard does my computer have?

In Windows 10, in the search box, enter **System Information**. On the **System Information** window that opens, select **System Summary**, and the motherboard manufacturer should be listed in the **Value** column for the **System Manufacturer** row.

Notes for the educator

For more information about motherboards, review the *Motherboards Explained* video at https://www.youtube.com/watch?v=b2pd3Y6aBag&t=8s.

Computer memory

Computer memory is classified by speed of access and cost. The closer the memory is to the CPU, the faster it can receive input or can output the data or instructions that are stored in it. This memory is also the most expensive for the manufacture to use and usually limited in size and in the amount added to a computer.

A computer's standard memory components include:

1. *Register:* The memory component closest to the CPU is called the Register. The register is built into the CPU. They store instructions, calculations in process, I/O for various devices, and data.
2. *Cache:* The cache is also very close to the CPU and cache memory can be deployed in what is known as *cache levels*. L1 is closes to the CPU and the fastest of the cache levels, following by L2, L3, and so on. The cache acts as a buffer for data or instructions flowing into the CPU, modulating flow into the CPU to ensure no cycles are wasted.
3. *Main Memory:* Also known as random access memory (RAM), this is where the data and instructions that the CPU is processing are stored when the computer is operating. The memory is called random access because any area of the memory can be accessed directly and not sequentially. This type of memory is known as *Primary Storage*.

The memory types we've discussed are *volatile memory*, which means that when the computer's power is turned off, the contents of the memory cells are erased.

Another type of computer memory is *firmware*, which means that the software is stored permanently in a special type of memory and initializes the many hardware subsystems to the correct operating state. A process called the *bootloader* is in the firmware, and it loads into memory as the computer starts up and loads the OS into memory.

Graphics processing unit (GPU)

Most CPUs are slower when calculating floating point numbers versus integer numbers, as discussed in the preceding ALU section. Graphics are intense floating point number calculations. That's why separate graphics cards have been designed to perform floating point calculations fast and with high accuracy. PC gamers, digital artists, and 3-D graphics all benefit from these GPUs.

Currently, NVIDA is a leading manufacturer of high-end graphic processing cards.

Network interface card

Without network access our systems functionality is severely limited, and a network interface card (NIC) provides network connectivity. Networks are classified by size and purpose, such as a Personal Area Network (PAN), local area network (LAN), wide area network (WAN), and a metropolitan area network (MAN). However, they're all accessed through the same network interface.

The NIC is integrated into a computer system offering wired or wireless (Wi-Fi) network access.

Wi-Fi (Wireless Fidelity) networks are based on using radio waves to send signals between devices. The radio waves are measured in hertz (refer to previous discussion about CPU clock speed). Wi-Fi standard frequency speeds are defined to be 2.4Ghz and 5Ghz. These waves are very similar to the frequency found in your microwave! Your microwave uses 2.450Ghz to heat up food and your router uses 2.412 GHz to 2.472 GHz to transmit your data over Wi-Fi. These microwaves have non-ionizing radiation, which mean they don't cause cancer.

When you use your laptop or cell phone, and it's using Wi-Fi, all of your internet traffic is converted into binary data that's sent to your device's wireless chip. Your wireless chip converts the binary data into a radio frequency, and your router receives the signal and converts it back to binary data and then merges it into the traffic from your device.

Your wired NIC works performs the same steps except for the conversion from radio waves to binary data. The data entering and leaving the wired NIC is all binary. The encryption between the wireless router to your wireless device is normally encrypted using Wi-Fi Protected Access 2 (WPA2). Unless the initial traffic from your cell phone or laptop was encrypted, such as coming from a VPN or Hypertext Transfer Protocol Secure (https), once it leaves the NIC, it'll be in binary but no longer encrypted.

Storage

Storage devices have evolved from the early 1950s from a megabyte (MB) capacity (millions of bytes) to gigabytes (GB) capacity (1,024 megabytes) to terabytes (TB), which support 1,024 gigabytes in capacity. To convert from one unit to another, just know that for every level you go up, you multiply by 1,024.

Your computer's information is stored on your hard drive, where the OS and all of your files are stored. This type of storage is known as *Secondary Storage* because it's slower and cheaper than primary memory. It's used for permanent data storage.

There are currently two popular types of local disk technology in wide use today: magnetic and solid-state disks.

Hard or magnetic disk drives

- Contain a series of spinning rigid magnetic disks or platters rotating at high speeds:
  - Platters are coated with a magnetic material such as iron oxide.
  - An industry nickname was "Spinning rust!"

  - Read and write mechanical arms move over the spinning platters. The whole device is hermetically sealed, and the head floats on a thin film of air.
  - Magnetic disks have motors that drive the disk causing noise and heat.
- Some popular external magnetic drives include:
  - IDE (Integrated Drive Electronics)
  - SCSI (Small Computer System Interface)
  - SAS (Serial Attached SCSI)
  - NAS (Network attached storage)

Solid-state disks

Solid-state drives (SSDs) have no moving parts. They're made from *flash* memory. Flash memory will retain the data stored on it without constant power being supplied. Types of SSDs are based on their shape, size, and capacity, and the 2.5-inchnch SSD is the most common type used today.

Flash memory is like RAM memory except for one notable exception. When you turn off a computer's power, the data on an SSD persists. Since there aren't any moving parts, these drives are quieter and run cooler than hard disk drives (HDD). However, there's a tradeoff for these benefits in both cost and size constraints. Traditional hard drives are significantly less expensive than SSDs. Currently a 1 TB HDD might be about $50.00, while the same size SSD might be $200.00.

- Some popular uses for SSDs include:
  - USB thumb drives.
  - SD cards.
  - M.2, which are small form-factor SSD drives.
  - SATA-based SSDs.
  - CompactFlash (CF).

Notes for the educator

For an interesting history lesson of how data storage has evolved over time, refer to *The History of Computer Storage* video at https://www.youtube.com/watch?v=-KRLWGaIunA. Summarize the information with a discussion of what daily activities wouldn't be possible without electronic data storage.

Plug and play versus device drivers

Notes for the educator

Engage the students with a brief discussion about what they already know about drivers. Here are some questions you could ask:

- What do you know about device drivers?

- What experiences have you had with drivers?

It’s possible that some students have little experiences with device drivers. A portion of the following video (0:00:00 – 0:03:10) explains drivers with examples that students will likely identify with: *Software Drivers* at https://www.youtube.com/watch?v=t-aRlwLI-b0.

Device drivers

Before we discuss plug and play functionality, we must define what a device driver is. A device driver is what enables a computer’s OS to communicate with a hardware device. Every computer uses many drivers to control the hardware and devices that are installed or connect to it, such as monitors or a webcam. Without appropriate drivers installed, those devices wouldn’t be able to share data with the computer and wouldn’t function properly or not at all.

Why is that the case? If there was only one webcam in existence that plugs into a USB port for your computer, you would be able to plug it in with no device drivers needed, and it would work.

The issue is that there are hundreds of different webcams with distinctive features, and they all work differently. The signal that turns on HD in one camera, might turn on 4k in another camera. For everything to work correctly, software builders must rewrite their software with specialized signaling for your webcam along with every supported webcam. The driver acts a translator between your webcam and the program or app that wants to use the webcam. In technical terms, the driver acts as an *abstraction layer*, which allows the application developer to interact with a computer's hardware in one standardized language, and then the driver manages the communication.

Device drivers must be maintained for multiple operating systems, such as Linux and Windows 10. Each OS has its own universal language that a driver must translate, which means that there are openings for a driver for specific hardware to have a bug or two in translation.

On Windows 10, Drive Manager manages device drivers.

Possible task or demonstration: Inspect Windows 10 Drive Manager

There are multiple ways to open Drive Manager on Windows 10. The easiest way is to select Win+X. A panel of administrative programs and tasks appears, and you can select **Drive Manager**. For this discussion, we’re using a webcam that will be listed under **Cameras.** Select the greater-than (>) symbol and the installed camera should be listed. Windows doesn’t always categorize hardware the way you think it should. Therefore, if you don’t observe your device in the list, open other categories to determine if it’s listed under them. Right-click on the new device name to activate the context menu. In this instance, it’d be **USB Camera**. You should observe a list of actions you can perform to check out the driver. Select **Properties** to determine whether the Windows OS indicates the camera is working properly. You can update the USB Camera device driver, disable the device, uninstall the device, and check to determine whether the device's hardware has been modified (maybe because of an automatic firmware update).

The ease with which you can add new devices to your computer, as the preceding paragraph describes, is the result of technology that Microsoft and Intel developed known as Plug and Play, beginning with the Windows 95 OS.

Plug and Play

Plug and Play (PnP) was a standard introduced in the early 90s to help allocate computer resources more effectively. Before PnP, you had to rely on Dual Inline Package (DIP) switches, manual software configuration, and even hard soldering to configure a new device. Plug and Play is a set of operating-system standards that enable hardware connectivity through automatic device detection and configuration. When first introduced, it was often called *Plug and Pray*. Over time, industry standardization and integrated identification codes for devices were defined and implemented. For PnP to function correctly, a system must have three-way compatibility between the OS, the BIOS, and the Plug and Play component.

The Windows Driver Kit (WDK) was developed as part of PnP documentation, and it focuses on the system software support for PnP and how drivers use that support to implement PnP.

IP installation

IP-based installation or *Universal Plug and Play (UPnP)* is a set of protocols and technologies that allows devices to automatically discover and connect to each other using the TCP/IP, HTTP, or Dynamic Host Configuration Protocol (DHCP).

The UPnP architecture is more than just an extension of the plug and play model. It supports a zero-configuration approach and automatic discovery for a range of devices from many vendors. When a UPnP device is attached to the network, it can obtain an IP address and broadcast its services when queried. UPnP supports wired Ethernet, Bluetooth, and Wi-Fi.

How UPnP works

UPnP allows a device to automatically announce its presence and functionality to all other systems and devices on a network.

There are two main components of UPnP standard:

1. Control Point interface, which enables applications to discover and control UPnP devices.

2. Device Host interface, which allows manufactures to create a device description that can be registered with the UPnP Device Host, which manages discovery, description, control, and events portions of UPnP-based device functionality. This interface enables device manufactures to implement functionality of UPnP certified devices.

One of the most common uses of UPnP is accessing a network printer. Without UPnP, you would have to manually configure access to the printer. This can be a time-consuming process in which unexpected issues often arise. With UPnP, all you have to do is plug a UPnP-compatible printer into an open Ethernet port on the router or assign it a Wi-Fi address, and UPnP takes care of the rest.

Possible tasks or demonstration: Exercise enabling UPnP in Windows 10

1. Open the **Setting App** by selecting **Win+I**.
2. Select **Network and Internet**, and then select **Network and Sharing Center**.
3. In the left pane of the **Network and Sharing Center** panel, select **Change advanced sharing setting**s.
4. In the **Network Discovery** section, select the option for **Turn on network discovery**, and then select **Save changes**.

UPnP: security risks and a summary

UPnP assumes that devices on a network are trusted. If a printer or other device has been hacked and malware has been deployed on it, that malware can spread across the network.

Manufacturers will continue to make products that leverage UPnP.

Web-based configuration

Web-based configuration occurs when a user accesses a device's html interface to configure it. You do this by using a web browser. The most common example is configuration of your home router or access point.

Possible task or demonstration: Access your router's configuration page

On Windows

1. In the search box, enter **command prompt**. A Windows command window will appear.
2. In the window, enter **ipconfig**, and then select Enter.
3. Locate the line that starts with "Default Gateway" and note the address. Usually, it'll be 192.168.1.1 or 192.168.2.1.

4. This address is your router configuration webpage. The Uniform Resource Locator (URL) to use to access your router configuration webpage would be http://192.168.1.1.

On Linux

1. Open a terminal window.
2. In the window, enter **ifconfig**, and then select Enter.
3. Follow steps 3 and 4 from the preceding Windows OS directions.

Cloud or non-local storage

Cloud storage is storage provided through a public cloud provider like Microsoft OneDrive, Google Drive, Dropbox, and similar. Our device connects to storage over our network and to the internet.

There are points to consider regarding cloud storage, including:

- If you're using cloud storage for work, is it approved? If not, it's called *Shadow IT*.
- Depending on where you are, data sovereignty can be an issue. Data sovereignty is the idea that data might be subject to the laws of more than one country/region.
- Redundant internet connections should be available.
- Encryption must occur for data transfers and data at rest. Ensure a vendor can't read what you store.
- Automatic synchronization must occur.

Final thoughts on architecture

As we end this lesson on computer architecture, consider the term "Moore's Law," which helps define the concept of computer architecture.

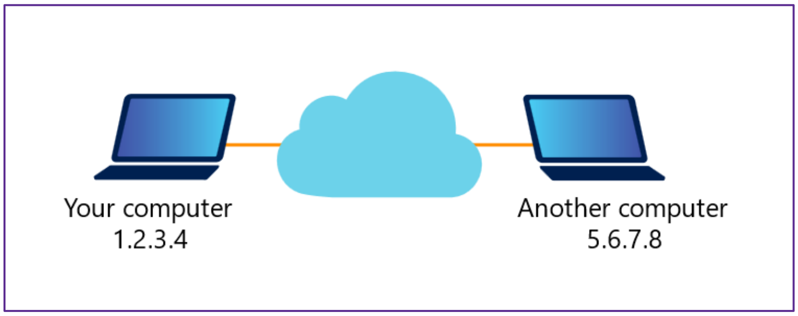
"Moore's Law is a computing term which originated around 1970 by Gordon E. Moore, co-founder and chairman emeritus of Intel Corporation. The simplified version of this law states that processor speeds, or overall processing power for computers, will double every two years." This theory still holds true today: Moore's Law.

Notes for the educator

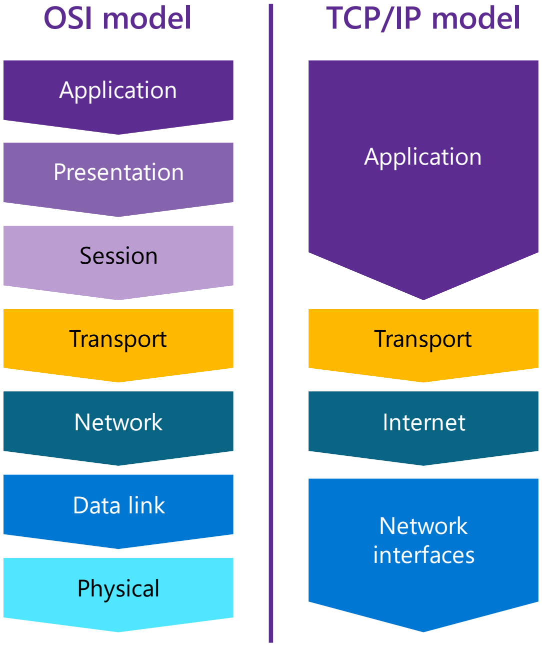
Conduct a class discussion about the types of cloud storage that students use for their schoolwork, recreation, photos, and other data-storage needs. Ask them to consider any problems they have with technology and how they think it could be better.

Understand Internet Protocol and the OSI model

Basics of network communications



Networking protocols are developed in layers, which are responsible for specific network communications and the protocols supported in it. For example, there is the academic Open Systems Interconnection (OSI Model) and the implemented model that combines two protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The *International Standards Organization (ISO)* adopted the OSI model in 1984. The OSI model has seven layers, while the TCP/IP model has four, which the following image depicts:



The TCP/IP protocols define the standards on which the internet was built. The OSI model is the “Reference Model” for guidelines about how messages are transmitted between network points.

Industry experts estimate that in 2020, there were 50 billion nodes connected to the internet.

To understand how to secure a network, we need to understand the basics of computer networking. The more one understands how TCP/IP network’s function, the easier it is to apply that knowledge to security.

Overview of the TCP/IP model

Note for the educator

Introduce the TCP/IP model with this video, *TCP/IP Protocol: The 4 Layer Model* at https://www.youtube.com/watch?v=KEWe-5Bk3Q0.

The TCP/IP model, as mentioned, is built from layers. The combined layers form what is known as the Internet Protocol Suite *(IPS)*. The four layers are:

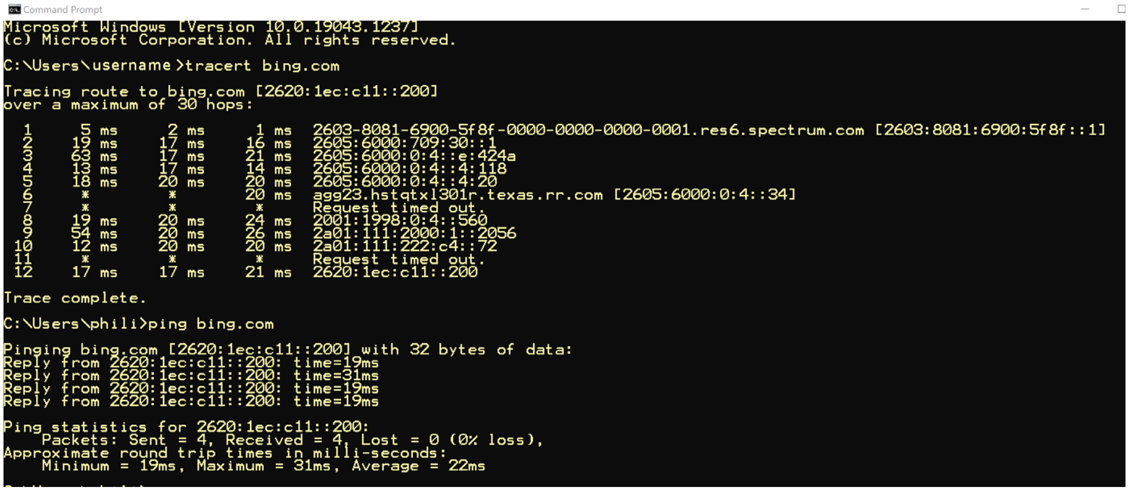
1. *Link-layer*, which is sometimes also called the data-link layer. It’s the lowest of the layers and details how the physical devices transfer information between nodes, the computer's operating systems, device drivers, and the node's network card. Example protocols at this level include Ethernet and Point-to-Point Protocol (PPP).
2. *Network layer*, which is sometimes called the internet layer. It manages movement or routing of packets around the network. This level contains where the IP layer. The protocol used could be version 4 (IPv4) or version 6 (IPv6).
3. *Transport layer*, which provides for the correct flow of packets between hosts and clients. This layer supports multiple services by assigning each service a different number known as a *port*. TCP is the supported protocol supported at this level for network transport and it’s a reliable protocol. A vastly different protocol, *User Datagram Protocol (UDP),* is lightweight but not always reliable.
4. *Application layer,* which is comprised of a variety of applications. Examples of applications include are HTTPS, which is used to transfer the content of webpages securely; Simple Mail Transport Protocol (SMTP), which transfers emails; Remote Desktop Protocol (RDP) for remote signing in to a system; and Short Messaging Service (SMS) for text messaging.

There is also the physical layer underneath the link layer. However, it’s not typically depicted in diagrams.

Notes for the educator

The terminology and technical details of how data moves through the internet is complex. Use an "unplugged" activity to provide the students with a kinetic or physical experience that depicts the process, either before delivering the following content or at the end as a review activity: *The Internet* at https://studio.code.org/s/coursef-2021/lessons/19.

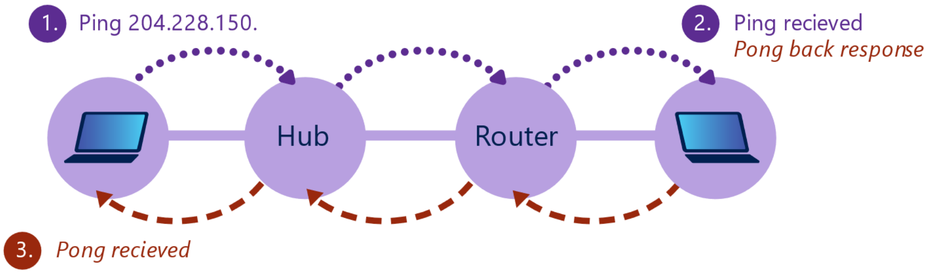
A way to demonstrate the movement of internet packets movement is by demonstrating the **ping** command, the tracetrt (Windows) commend, or traceroute (Linux). The following screen capture depicts all:



```
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\username >tracert bing.com

Tracing route to bing.com [2620:1ec:c11::200]
over a maximum of 30 hops:

  1     5 ms     2 ms     1 ms  2603-8081-6900-5f8f-0000-0000-0000-0001.res6.spectrum.com [2603:8081:6900:5f8f::1]
  2    19 ms    17 ms    16 ms  2605:6000:709:30::1
  3    63 ms    17 ms    21 ms  2605:6000:0:4::e:424a
  4    13 ms    17 ms    14 ms  2605:6000:0:4::4:118
  5    18 ms    20 ms    20 ms  2605:6000:0:4::4:20
  6     *        *       20 ms  agg23.hstqtx1301r.texas.rr.com [2605:6000:0:4::34]
  7     *        *        *     Request timed out.
  8    19 ms    20 ms    24 ms  2001:1998:0:4::560
  9    54 ms    20 ms    26 ms  2a01:111:2000:1::2056
 10    12 ms    20 ms    20 ms  2a01:111:222:c4::72
 11     *        *        *     Request timed out.
 12    17 ms    17 ms    21 ms  2620:1ec:c11::200

Trace complete.

C:\Users\phili>ping bing.com

Pinging bing.com [2620:1ec:c11::200] with 32 bytes of data:
Reply from 2620:1ec:c11::200: time=19ms
Reply from 2620:1ec:c11::200: time=31ms
Reply from 2620:1ec:c11::200: time=19ms
Reply from 2620:1ec:c11::200: time=19ms

Ping statistics for 2620:1ec:c11::200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 31ms, Average = 22ms
```

For an animated video of traceroute, refer to https://youtu.be/vUnCXVuH16Y.

The ping program depicted in the preceding screen capture sends an ICMP protocol data unit (PDU) to Bing.com. The ICMP PDU is part of IP datagram. The source and destination IP address is in the datagram header. The computer that initiated the ping records the time it sends and the time it received a ICMP reply. The pinged computer will respond with a reply, as the following image depicts, with the time expired to receive the reply is displayed (if it does receive a reply):



Basics of packet transmission

Notes for the educator

Preview the process of sending data through a network with the video, *Data Flow on the Internet*, at https://www.youtube.com/watch?v=hDHJxndSups.

The internet is a global packet-switching network loosely connected by the TCP/IP protocol. So, what's a network packet and what does it mean when it switches?

When data zooms across the internet, it's sent in a *packet* that contains the data destination's IP address and the packet source's IP address. This process enables routing of the data block to the correct destination and specifies where returned data should be sent. The packet is built as it passes through the TCP/IP protocol stack. The packet then travels from the application layer to the link layer, and information is added to the packet. Each layer adds a header and other data. The addition of information to the packet is called *data encapsulation*. When the packet reaches its destination, the reverse action takes place. Data added at each layer is removed until the packet reaches the application layer. This process is called *decapsulation*.

Example: How does IPS support sending text messages?

Most smartphones use a variant of SMS that supports multimedia, group messaging, and Wi-Fi. Apple's IMessage on an iPhone is an example of an enhanced SMS.

You enter a message to someone using a service at the *application layer* on your phone. The application is iMessage. This layer formats the message into the initial packet that is delivered to the transport layer using either TCP or UDP. In this case, iMessage uses TCP and then the following process occurs:

- The *transport layer* transfers the message, adding information to the original message for the TCP header source, destination port numbers, and additional fields. It then sends the packet to the network layer.
- This new layer, the *network layer*, adds additional information needed for either IPv4 or IPv6, and the modified packet is now called an *IP datagram*, and it's sent to the data-link layer.
- At the *data-link layer*, an additional transformation of the original packet occurs.
- If the systems being accessed are on a local network (same broadcast domain), the MAC address is used. If the systems are on different networks and routing is needed, then the IP address is used.
- The *IP datagram* gets a new header that includes the source and destination IP addresses. The encapsulated IP datagram is now called Ethernet frame or just "frame."

Note: We will review the MAC address in another section.

- Finally, the frame is pushed to the physical layer, converted to bits, and streamed onto the network for transmission to the receiving destination.

Notes for the educator

Assign students a task to send a short email message to a classmate. In the email, they should describe the process of how a message travels to the recipient using terms related to layers, packets, and other associated terms. Alternatively, they could draw the path a message takes and label the steps.

Quiz:

- Queston 1: What's the difference between data-packet encapsulation and data-packet decapsulation?
- When is a MAC address used and when are IP addresses used?

Understand internet basics and use built-in Windows tools to observe your network settings.

The World Wide Web (WWW) is a service built on the internet protocol, and it enables computers to share and exchange data quickly and reliably. The data has grown to encompass documents, videos, and digital data. The WWW is a client-server model. Computers that request data are clients. The computer that sends the data, meaning the computer that *serves* the data, is the server.

A client can be a machine or a program. When we say a client's machine, we're referring to any end-user device that's accessing the web. For example, your laptop or desktop computer are clients. Likewise, smartphones, tablets, and similar devices are all client machines.

Additionally, a client program allows users to make requests through the WWW. A web browser is an example. A user can request a webpage through the browser. Other browser-based accessed services are email, productivity tools such as Office 365, Zoom, Microsoft Teams meeting services, and access to cloud storage. These programs are clients. Whether a machine or a program, they all make requests through the web:

- A server is on the receiving end of these requests. A server is a computer hardware or software that supports functionality for other devices or software, called clients. In this client-server architecture, a single server is designed to serve multiple clients at the same time. There are several types of servers, each one performing a specific task. For example, a web server such as Apache, manages HTTP requests, while a database server that's running a database management system (DBMS) such as SQL Server replies to SQL commands.
- A server in the client-server architecture can serve hundreds or thousands of clients. It's always listening for requests and as soon as it receives one, it responds with a message.

In summary, on the web, the client-server model is the architecture that splits computer operations into two parts: the client computers that request services, and the computers that "serve" them (the servers). The client-server model works through the request-response cycle.

The client-server model with a SQL Server example

We know that every device that connects to the internet must have a valid IP address. As discussed, servers can support multiple clients and run several programs. If a server runs a web server and email services, how can the server distinguish between the different requests? This is accomplished using *ports*, which enable servers to run various programs on a computer.

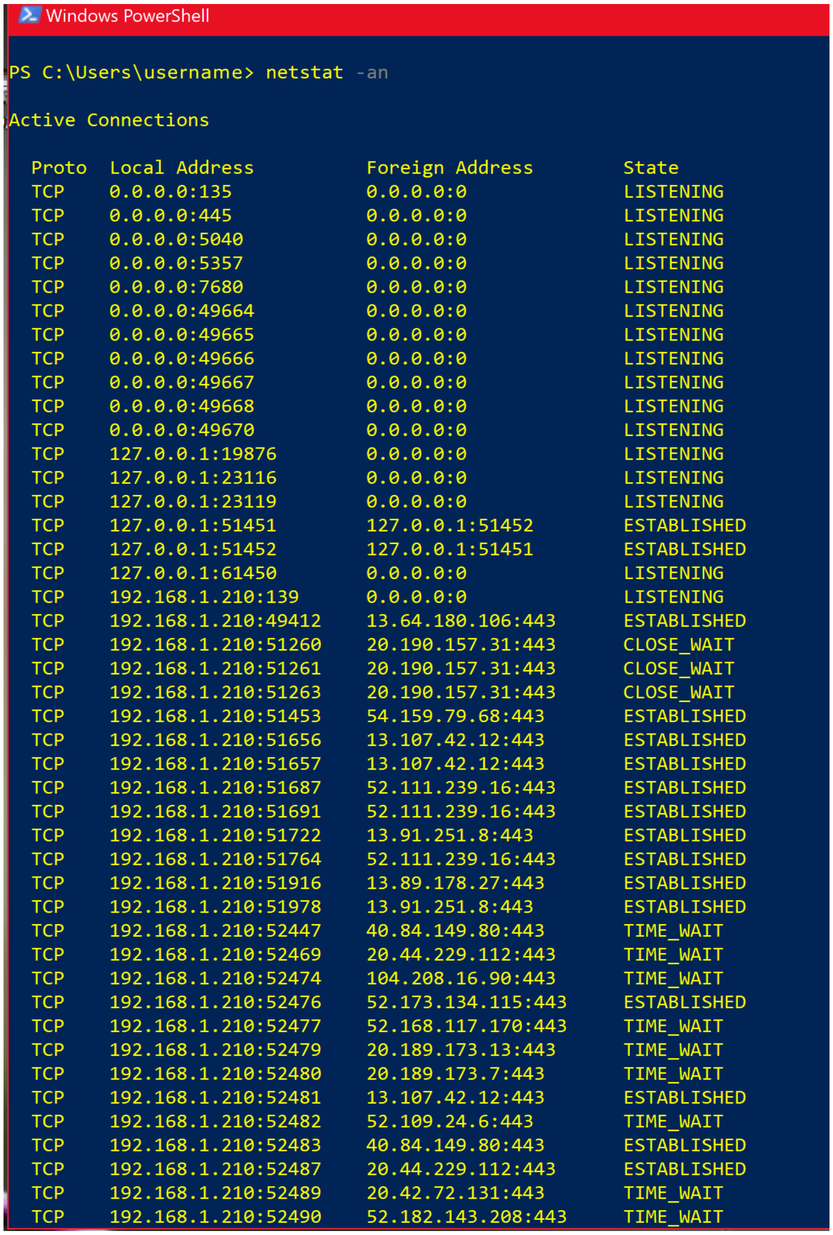
An analogy is an apartment building. The building has one street address, like the computer's unique IP address. Additionally, each apartment has a unique apartment number, like the port address. The *Internet Assigned Numbers Authority (IANA)* allocates the port number for standard services. For example, port 80 is the standard port for an HTTP request and 443 is the standard port for an HTTPS request.

- The connection between two computers over TCP/IP is a *socket*, and each side of the communication will have a socket. Both the server and the client have a library of prewritten and tested code that developers can use to build applications.
- **Definition**: "**A socket is the combination of IP address plus port."** [*Steve's Internet Guide*]
- Port 1433 is the default port for a standard SQL Server connection. The connection would be the servers **IP address:1433**. The SQL Server engine can listen on multiple ports on the same IP address. You use the SQL Server Configuration Manager to configure ports, entering them separated by commas in the format 1433,1500,1501. This field is limited to 2,047 characters.

Possible tasks or demonstration

To observe what ports are open and have a process listening on a port, run the *netstat* command, which is the same on Windows and Linux.

For example, the following code sample depicts how you'd run **netstat** with the **-an** option:



```
PS C:\Users\username> netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:19876        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:23116        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:23119        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:51451        127.0.0.1:51452        ESTABLISHED
  TCP    127.0.0.1:51452        127.0.0.1:51451        ESTABLISHED
  TCP    127.0.0.1:61450        0.0.0.0:0              LISTENING
  TCP    192.168.1.210:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.210:49412    13.64.180.106:443      ESTABLISHED
  TCP    192.168.1.210:51260    20.190.157.31:443      CLOSE_WAIT
  TCP    192.168.1.210:51261    20.190.157.31:443      CLOSE_WAIT
  TCP    192.168.1.210:51263    20.190.157.31:443      CLOSE_WAIT
  TCP    192.168.1.210:51453    54.159.79.68:443       ESTABLISHED
  TCP    192.168.1.210:51656    13.107.42.12:443       ESTABLISHED
  TCP    192.168.1.210:51657    13.107.42.12:443       ESTABLISHED
  TCP    192.168.1.210:51687    52.111.239.16:443      ESTABLISHED
  TCP    192.168.1.210:51691    52.111.239.16:443      ESTABLISHED
  TCP    192.168.1.210:51722    13.91.251.8:443        ESTABLISHED
  TCP    192.168.1.210:51764    52.111.239.16:443      ESTABLISHED
  TCP    192.168.1.210:51916    13.89.178.27:443       ESTABLISHED
  TCP    192.168.1.210:51978    13.91.251.8:443        ESTABLISHED
  TCP    192.168.1.210:52447    40.84.149.80:443       TIME_WAIT
  TCP    192.168.1.210:52469    20.44.229.112:443      TIME_WAIT
  TCP    192.168.1.210:52474    104.208.16.90:443      TIME_WAIT
  TCP    192.168.1.210:52476    52.173.134.115:443     ESTABLISHED
  TCP    192.168.1.210:52477    52.168.117.170:443     TIME_WAIT
  TCP    192.168.1.210:52479    20.189.173.13:443      TIME_WAIT
  TCP    192.168.1.210:52480    20.189.173.7:443       TIME_WAIT
  TCP    192.168.1.210:52481    13.107.42.12:443       ESTABLISHED
  TCP    192.168.1.210:52482    52.109.24.6:443        TIME_WAIT
  TCP    192.168.1.210:52483    40.84.149.80:443       ESTABLISHED
  TCP    192.168.1.210:52487    20.44.229.112:443      ESTABLISHED
  TCP    192.168.1.210:52489    20.42.72.131:443       TIME_WAIT
  TCP    192.168.1.210:52490    52.182.143.208:443     TIME_WAIT
```

What does the output mean? Here's an explanation:

- The number that follows the IP address is the port number. Example: 192.168.1.210:**50387**   20.189.173.14:**443** ESTABLISHED.
    - This is my browser connection to IP address 20.189.173.14 using 443 or HTTPS.
    - In lines that indicate **ESTABLISHED**, this refers to the connection being made successfully between the client and the server.
- In lines that indicate **LISTENING**, a listener (a process waiting for a connection) is waiting for a message:

    - Every outbound TCP connection causes a **LISTENING** entry on the same port.
- If a listing indicates 0.0.0.0 in the **Local Address** column:
    - This means that the port is listening on all "network interfaces" such as your computer, network card, or Wi-Fi.
- If a listing indicates 127.0.0.1 in the **Local Address** column:
    - This means that the port is *only* listening for connections from your PC, not from the internet or network.
- If a listing displays your online IP in the **Local Address** column:
    - This indicates that the port is *only* listening for connections from the internet.
- If a listing displays your local network IP in the **Local Address** column:
    - This indicates that the port is *only* listening for connections from the local network.

Access to server-based applications provides vendor-specific or standards-based network services that manage data communication between a remote application and a server. These network services run on top of the network protocol like TCP/IP.

Domain Name Service

DNS is a distributed hierarchical database that converts a node name to an IP address on the network or an IP address to a node name.

DNS is the service that enables users to enter a domain name into a browser instead of memorizing IP addresses.

DNS is distributed because every company, university, military branch, ISP, and organization with access to the internet maintains its own DNS database. The process of translating a node name to an IP address is called *resolving*. The systems that support DNS run a program, typically a free one named BIND 9, that the Internet Systems Consortium (ISC) supports. Also, Microsoft has a popular DNS server that's bundled with the Windows Server OS.

DNS is a client-server type of service, where each DNS server only maintains its portion of the DNS. For example, a host can query a DNS server for the IP address of a host's domain name. If the DNS server has that information in its database, it'll return the IP address. If the initial DNS server accessed doesn't have that information, it'll query other DNS servers. This process is known as a *recursive query*. The DNS default port is 53.

It's inefficient to always query a domain name server, or *authoritative server*, that's run by the organization that maintains it. That's why other DNS servers and clients keep a name cache for the names and IP addresses that have successfully resolved. If the DNS requested can be satisfied from the cache, there's no need to send out a DNS query to another DNS system. Each cache entry has a limited time in the cache, known as the Time-to-Live timer.

Without a DNS service, we would have to maintain a list of network addresses and hostnames on each system.

URL-to-IP transmission

A Uniform Resource Locator (URL) is something that you're probably familiar with, even if you don't realize it. Part of a specific URL is a domain name, such as amazon.com or microsoft.com. The end of the URL, the .com or .org, is called a top-level domain (TLD). We can think of the TLD as the main categories that sort every internet website and help route requests through a particular group of servers to get us to the correct website.

A request goes to a DNS server when you enter a URL in a browser. The DNS server resolves the URL's IP and sends it to the browser, which then requests the applicable website forwards the page associated with the URL.

LAN vs. WAN

A local area network (LAN) is different from a wide area network (WAN). A LAN is a small, geographically located area, such as a home, a school, or an office. Most LANs are networked with Wi-Fi.

WANs are geographically dispersed. An example would be a city, state, or county network, or the largest WAN of them all, the internet. You can interconnect LANs by using a WAN. An example is Azure WAN, which connects corporate LANs through the Azure high-speed backbone. A backbone is a high-bandwidth link used to carry traffic between networks or over physically large distances.

Device addresses

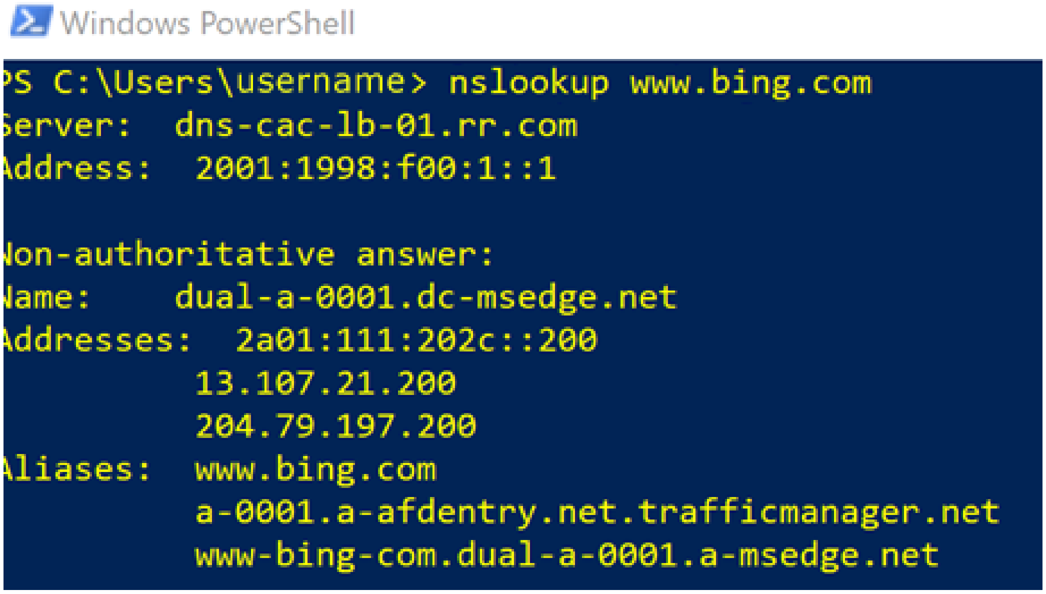
IP addresses

Every internet node has an individual IP address. If the address is an IPv6 address, it's a 128-bit number. An example fully qualified address is **FE80:0000:0000:0000:903A:1C1A:E802:11E4**.

If it's an IPv4 address, it's a 32-bit number written in dotted-decimal notation, as four decimal numbers. An example of IPv4 address is **192.168.10.100** or **11000000.10101000.00001010.01100100**.

Possible tasks or demonstration

If you use the **nslookup** command to review the Bing search engine's IP address, you'll observe the following:



```
PS C:\Users\username> nslookup www.bing.com
Server:  dns-cac-lb-01.rr.com
Address:  2001:1998:f00:1::1

Non-authoritative answer:
Name:    dual-a-0001.dc-msedge.net
Addresses:  2a01:111:202c::200
          13.107.21.200
          204.79.197.200
Aliases:  www.bing.com
          a-0001.a-afdentry.net.trafficmanager.net
          www-bing-com.dual-a-0001.a-msedge.net
```

Notice that the DNS reply is labeled **Non-authoritative answer**. What does that mean?

Notes for the educator

An interesting activity is to search for the IP address associated with a URL. Assign students to read about DNS Lookup at https://www.whatismyip.com/dns-lookup/. Lead a discussion of how DNS is similar to a phonebook.

MAC addresses

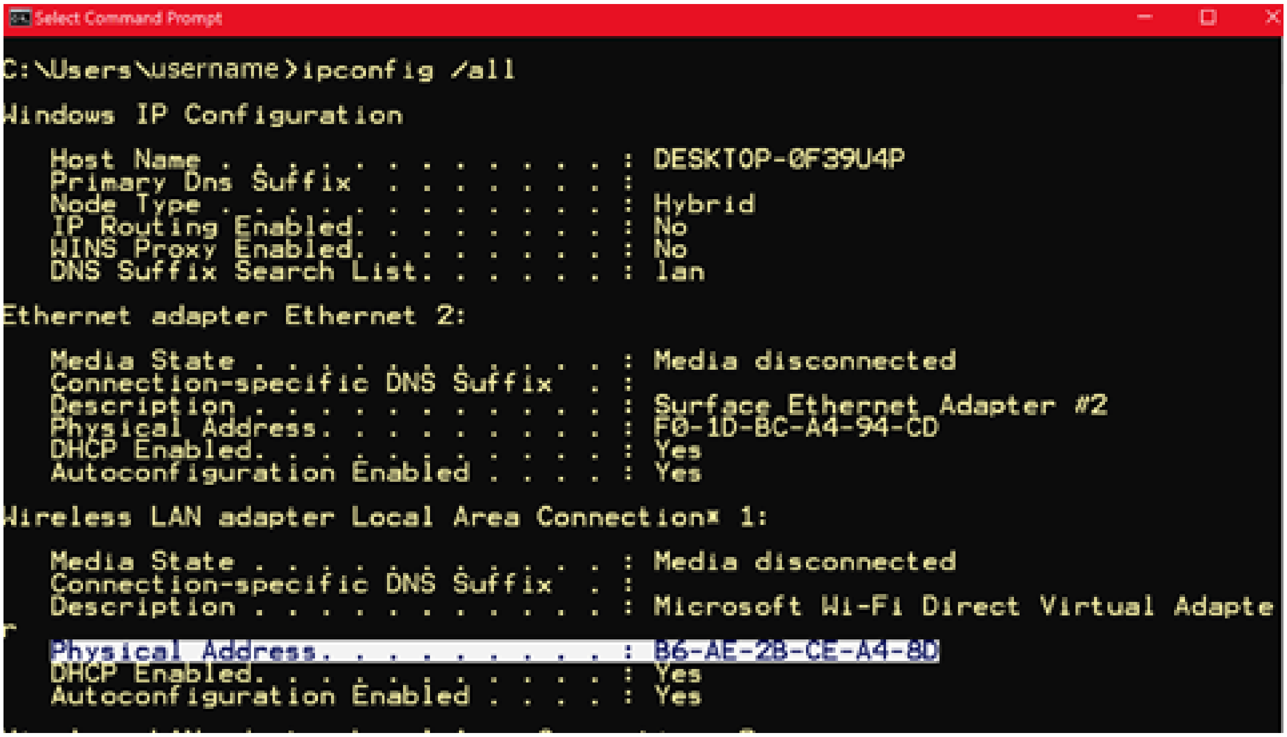
A *MAC* address is a hardware address that a manufacturer assigns to a NIC. The link layer uses a MAC address to identify a network interface. The MAC address helps to support the Plug and Play protocol, and it's globally unique and 48 bits long. The first 24 bits of the address are the vendor component and are unique to a vendor. The second group of 24 bits is the group identifiers. Each NIC that a manufacturer makes has a common vendor component that's followed by a different group identifier. A host that receives an IP address during its configuration will check if the received address is unique by broadcasting an ARP packet.

Possible tasks or demonstration

How to determine your MAC address on a Windows 10 device:

1. Open a command prompt.

2. Enter **ipconfig/all**, and then select Enter.
3. Review the returned information and find the **Wireless LAN** adapter section.
4. In the **Physical Address** row, you'll observe the MAC address, as the following graphic depicts:



```
C:\Users\username>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-0F39U4P
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : lan

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Surface Ethernet Adapter #2
   Physical Address. . . . . . . . . : F0-1D-BC-A4-94-CD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapte
r
   Physical Address. . . . . . . . . : B6-AE-2B-CE-A4-8D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Basic protocols

HTTP/S

Adding the */S* to HTTP means that TLS encryption is being added to the transferred data.

Note: TLS is the successor to Secure Sockets Layer (SSL).

POP3

Post Office Protocol (POP3) is the current mail-protocol release and is typically built into email clients. POP works by checking with an email server to determine if there's mail waiting. It'll then download that mail from the mail server to your device, using the mail client. This ensure the mail server isn't overloaded with messages. However, one issue that can arise is that if you access your mail from multiple devices, messages that have been previously downloaded might not be available. By default, the POP3 protocol works on two ports:

- Port 110, for sending unencrypted POP3 traffic.

- Port 995, for sending encrypted POP3 traffic.

IMAP

Your email client can use *Internet Mail Access Protocol (IMAP)* to access messages on an email server. There are critical differences between POP3 and IMAP, most notably how these protocols access and retrieve email. IMAP only downloads a copy of the message when you select it, and it doesn't automatically download attachments. This makes checking messages a lot quicker than when you're using POP. Additionally, the email remains on the mail server unless you delete it. Therefore, you can access email from different devices, such as a phone, computer, or watch. By default, the IMAP protocol works on two ports:

- Port 143, for sending unencrypted IMAP traffic.
- Port 993, for sending encrypted IMAP traffic.

SMTP

The SMTP has two main components, a *mail transfer agent (MTA)* and a *mail user agent (MAU)*. SMTP is the standard protocol for sending email across the internet, and it delivers email to a specific server. The server it's delivered to then decides what happens to it when it arrives.

By default, the SMTP protocol works on two ports:

- Port 25, for sending unencrypted SMTP traffic.
- Port 465, for sending encrypted SMTP traffic.

DoH

DNS over HTTPS (DoH) is a protocol that encrypts the contents of a DNS query. This prevents third parties from reading your DNS request. Many DNS providers support DoH.

Notes for the educator

Review basic protocols with the video, *Networking Protocols Explained | What Are TCP/IP, UDP, HTTP, SMTP, FTP*, at https://www.youtube.com/watch?v=g_kNTa9y6Is. Summarize with a discussion of the "rules" of each protocol.

Wireless networking

A wireless LAN (WLAN) requires no wires be installed to connect a client, which enables devices to roam for connection. You can configure the Institute *of Electrical and Electronics Engineers* (IEEE) 802.11 protocol WLAN to work in one of two modes: an *infrastructure* or an *ad-hoc* mode.

Infrastructure mode uses fixed access points (AP) that connect to a wired network. Each wireless networked device connects to the AP while in range. The AP acts as the device's gateway. Most people use this mode for their home WLANs. You can configure multiple access points to work together to extend coverage. This type of interconnectivity between access points is a *mesh network*.

Ad-hoc mode doesn't use access points for connections between devices. Instead, each networked device can communicate directly to other network devices that are within their transmission range.

The current 802.11 ac protocol has been renamed the new easy-to-remember Wi-Fi 5, which is easier to remember, and the IEEE 802.11ax to Wi-Fi 6. On the horizon is the IEEE 802.11be or Wi-Fi 7. The following table summarizes the Wi-Fi standard with its speed:

Standard	Speed
Wi-Fi 5	1300 megabits per second (Mbps)
Wi-Fi 6	10 gigabits per second (Gbps)
Wi-Fi 7	30 Gbps

Note: 1 Mbps can download one million bits of data per second, while 1 Gbps can download one billion bits of data per second. *Question: what would the downloads be in bytes per second?*

Speed limitations

A Wi-Fi network's maximum possible speed is defined for the IEEE version as the preceding table depicts. However, there are several factors that can affect the difference between the theoretical and actual speed. These factors include the overhead of network protocol, the process of encrypting and decrypting signals (refer to the next section), any physical obstruction that radio waves must pass through, and radio interference by other devices in the area, such as a microwave oven.

Additionally, as more wireless devices are added to the network, its bandwidth must be shared, which decreases performance. If you use a video-streaming service on the Wi-Fi network, it needs to be a sufficiently fast network. For example, the streaming service Netflix recommends people use a network of 5.0 Mbps for high-definition streaming and 25 Mbps for ultra-high-definition streaming.

Interference

The standard frequencies of wireless signals are 2.4 and 5.0 GHz. However, within these assigned frequencies of a wireless signal, there are *channels*. A straightforward way of mentally visualizing channels is to think of them as lanes on a highway. The number of channels per frequency is different based on what country/region you're in. In the United States, there are

11 channels per frequency. Communication between a wireless client and an access point takes place over a single channel. If two or more APs are within range of each other, signals on one channel can interfere with signals on another. You can minimize interference by setting the channels of the APs as differently as possible. For example, you have two APs that support 2.4 and 5.0 GHz frequencies each. To minimize interference, set one AP at 2.4 GHz and the other at 5.0 GHz.

Encryption versus unencrypted

Encryption uses a mathematical formula plus a secret key to scramble WLAN packets. The receiving device then uses a complementing formula to decrypt or unscramble the data. As a result, an attacker can capture the wireless signal packets. Still, without the secret encryption key, they can't read the contents without breaking the encryption.

WLAN security standards define how to implement authentication and encryption processes for device manufactures.

Note: The encryption services discussed in the following sections don't provide an end-to-end security solution. The traffic is only encrypted between a mobile computer and the nearest wireless access point (WAP). Once the traffic leaves the AP to the wired network, it is no longer encrypted.

What are service set identifiers?

- *Service Set Identifier (SSID):* A service set is a collection of names of WANs. An SSID has a maximum length text identifier of 32 bits for the wireless LAN. SSIDs are case-sensitive and defined in the IEEE 802.11 wireless standard. Given that multiple WLANs can coexist within range of each other, each WLAN must have a unique name. That name is the SSID. The WAP broadcasts the SSID, allowing a device that's searching for a Wi-Fi network to join to find it using human-readable names.
- *Basic Service Set Identifier (BSSID):* A BSSID is the same as a WAP's MAC when in *infrastructure mode*. The BSSID is included in the wireless packet to differentiate to which WAP the client is connected. A user is usually unaware of which basic service set (BSS) they're connected to.
- *Extended Service Set (ESS):* An ESS is when one or more interconnected basic service sets and their overlapping WLANs create a single BSS at the logical link layer (of the TCP/IP model), and then every device connects to one BSS.

Open wireless network

An open wireless network is typically found in a public place and is essentially free Wi-Fi. Most of us have connected to these available networks at some point, often while traveling. They're typically free to connect to. However, when accessing these open networks, you should heed to potential dangers of these open connections.

The problem with open wireless networks is that other people can use basic downloadable hacker tools to review your session's details. They often can observe your passwords, even to websites that are, in theory, encrypted. They also can create a wireless network that appears legitimate but is designed to have you sign in to it so they can potentially capture your banking details, personal information, and other passwords to secure sites. Thus, it can be dangerous to connect to an open wireless network.

Open wireless networks are a valuable service, so you might wonder how you can use them securely. You can use remote access over public Wi-Fi with a *VPN*. VPNs enable access to an organization's internal network from home or while traveling. VPNs use encryption protocols such as TLS or other protocols. Cloud-based VPNs for your own personnel use are an excellent service and inexpensive.

When you find yourself on an open Wi-Fi network, it's wise to follow a few rules, including:

- Use a VPN.
- Never access your bank or credit accounts, nor access financial information.
- Don't change or update passwords while connect to an open network.
- Avoid accessing your work email.

If you really need to access private information while you're mobile, you should use your phone, turn off Wi-Fi, and use your data plan.

What about DNS?

If you are concerned about privacy or are experiencing slow webpage response time, consider changing how you're accessing a DNS server by configuring your ISP to select it for you. When you receive your IP address from your ISP, you also receive their preferred DNS servers. Most DNS services requests are in clear text, meaning the ISP DNS can view and gather information about the sites you visit and how often. They collect this information from your URL requests. Have you noticed that ads start to show up with information about a particular item once you go to a specific website searching for a specific item? That's DNS at work. When you query your favorite search engine and select the URLs that are returned, DNS is used.

You ISP can sell this information to advertisers to enhance their profits. Changing your DNS will not stop an ISP from tracking you, but it'll be more difficult.

Possible tasks or demonstration

There are three well-known free and secure DNS services:

- Cloudflare: 1.1.1.1 and 1.0.0.1
- Cisco's OpenDNS: 208.67.222.222 and 208.67.220.220
- Google's Public DNS: 8.8.8.8 and 8.8.4.4

We recommend using Cloudflare or Google Public DNS because 1.1.1.1 or 8.8.8.8 are easy to remember.

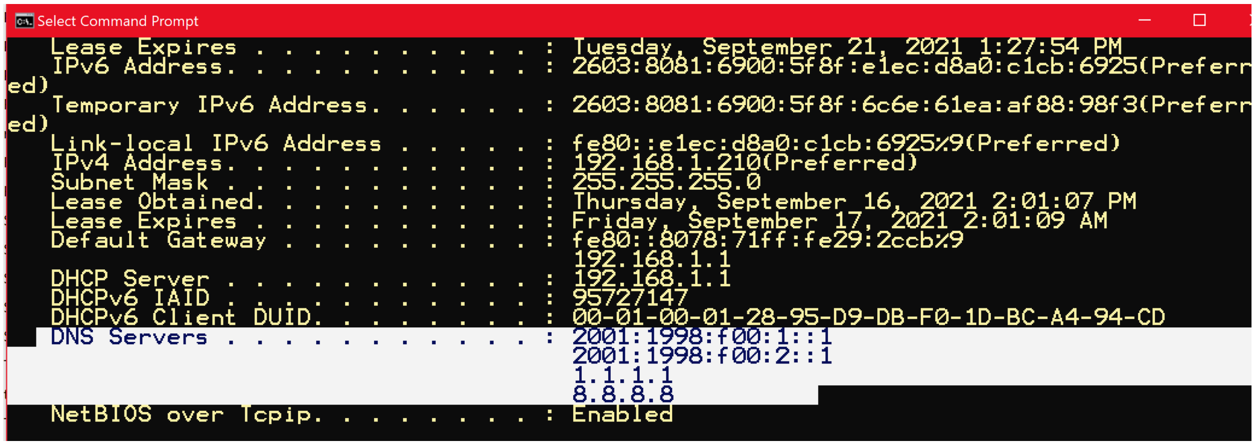
To select your DNS service, on a Windows 10 computer:

1. Select the **Start** button.
2. Select the **Settings** gear.
3. Select the **Network & Internet**.
4. Under the **Advanced network setting**, select **Change adapter options**. The Network Connections window opens, and you now should observe an icon for Wi-Fi and the name of the network you're connected to.
5. Right-click to activate the context menu on the Wi-Fi icon, and then from the displayed options, select **Properties**. The **Wi-Fi Properties** window opens.
6. Select **Internet Protocol Version 4 (TCP/IPv4)** in the **Wi-Fi Properties** section.
7. Select **Use the following DNS server address**, and then enter the **Preferred and Alternative DNS servers** from the previously suggested options.
8. Select **Ok**.

On your home router, you can also manually set your DNS server to one of the discussed servers. Changing the setting is vendor-specific, so you'll need to research online to discover how to change it for your specific router.

To review the results of the changes, open a command terminal and enter **ipconfig /all**.

Lots of information will return, and you should navigate to the row that starts with **DNS Servers**. In the following screen capture, you'll observe that there are four DNS servers listed. The first two are IPv6 addresses in hexadecimal and using ":". The other two are IPv4 and the ones you entered:



```
   Lease Expires . . . . . . . . . . : Tuesday, September 21, 2021 1:27:54 PM
   IPv6 Address. . . . . . . . . . . : 2603:8081:6900:5f8f:e1ec:d8a0:c1cb:6925(Preferr
ed)
   Temporary IPv6 Address. . . . . . : 2603:8081:6900:5f8f:6c6e:61ea:af88:98f3(Preferr
ed)
   Link-local IPv6 Address . . . . . : fe80::e1ec:d8a0:c1cb:6925%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.210(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, September 16, 2021 2:01:07 PM
   Lease Expires . . . . . . . . . . : Friday, September 17, 2021 2:01:09 AM
   Default Gateway . . . . . . . . . : fe80::8078:71ff:fe29:2ccb%9
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 95727147
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-95-D9-DB-F0-1D-BC-A4-94-CD
   DNS Servers . . . . . . . . . . . : 2001:1998:f00:1::1
                                       2001:1998:f00:2::1
                                       1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

You also might want to change your DNS settings on your iPhone or Android phone.

Wireless encryption for WAPs

The original 802.11 security standard for authentication and encryption was *Wired Equivalent Privacy (WEP***).** Cryptographers have shown that WEP is flawed and that its encryption is easy to break using freely available internet tools. The key issues with it include:

- The encryption key must be manually configured on each WAP. A dynamic key exchange without human intervention is the preferred method. In enterprises with large numbers of wireless clients, the keys weren't changed regularly.
- The keys that are installed are easy to break and are only 64 bits long, with 40 of those bits being the actual key.

We strongly recommend that you never use WEP to protect a wireless network.

WPA

WIFI Protected Access (WPA) was created by the Wi-Fi Alliance as a multivendor security standard. WPA improves security as compared to WEP, as it supports *dynamic key exchange* and has a *Message Integrity Check (MIC)* algorithm. MIC is a checksum on the wireless packet to ensure it hasn't been altered.

WPA2

The *WPA2* encryption service is based on *Advanced Encryption Standard (AES)* cryptography. AES provides better encryption than WPA because it has longer keys and more secure encryption algorithms. IEEE ratified this standard in 2005.

WPA3

Wi-Fi Protected Access version 3 (WPA3) is a new security model that was officially released in 2018 by the Wi-Fi Alliance. It has four enhancements that make it more secure than WPA2, including:

1. Robust protection for people that use weak passwords. It includes protection against dictionary attacks.
2. A simpler configuration process that's aimed at devices with limited displays, such as devices in the *Internet of Things (IoT)* category. For example, thermostats and smart door locks.
3. Individualized data encryption for open or public Wi-Fi issues. However, this could negatively affect VPN providers.
4. It will deliver stronger security for government and defense networks by following the *Commercial Security Algorithm (CNSA) Suite*. CNSA uses a 192-bit security protocol.

Note: If WPA2 or a new, more robust solution is not available on your device, you should consider upgrading your wireless equipment.

Security best practices

When configuring a WAP, you should:

- Update the SSID You shouldn't include personal information in the SSID since the SSID is being broadcast to all devices within range. Secure your access point with WPA2 encryption and a strong password.
- Change your default password: The default sign-on name and password for WAP are well known. You can use the Bing search engine to locate a specific WAP type and manufacturer, and then get the default administrator credentials. If you don't change your default password, you're leaving yourself open to a significant risk of getting *pwned*, which means your account security has been compromised).

Bluetooth

Bluetooth, similar to Wi-Fi, uses radio waves to send data between devices that are at short distances from each other. For example, Wi-Fi uses radio waves to transmit data between a router and a device. Bluetooth does it between devices. This means that if two devices have a Bluetooth option, they can send data to one another.

Radio waves are measured in Gigahertz. Both Bluetooth and Wi-Fi typically transmit at the 2.4 Gigahertz frequency or 2.4 billion waves per second. Even though Bluetooth works at the 2.4 Gigahertz frequency, it primarily works at shorter distances. This is because it uses a weaker signal of just 1 milliwatt of power. Bluetooth doesn't use as much power as Wi-Fi, but it can still connect to eight devices simultaneously. The Bluetooth transmitters in both a computer and any device can use 79 different frequencies, and a Bluetooth transmitter changes frequencies 1,600 times every second.

When trying to connect two Bluetooth devices, a dialogue takes place between them. They present their data to each other and decide whether they need to exchange information or if one of them needs to control the other. After this short digital dialogue ends and the two devices agree on their roles, they connect to form a network. A Bluetooth network of connected devices is called a *piconet*. Once their connection is established, they begin their frequency hopping to stay connected and avoid interference.

Each device has its own unique address programmed by the manufacturer, like a network card's MAC.

Security concerns

The way Bluetooth works raises a few security issues, similar to those raised when using Wi-Fi. Like all wireless networking configurations, there's always a legitimate concern of sending personal data over radio waves, where third parties can intercept it and potentially use it. When Bluetooth first came out, it was easy for someone to access data without permission. Bluetooth manufacturers are aware of the risks, though, so they continue to make devices that include more protection against security threats. New Bluetooth devices support the option of a trusted device that enables you to share data without permission. In contrast, others need permission to access your device. Making a device non-discoverable is the standard security setting used when moving to a location with other untrusted Bluetooth devices.

Bluetooth version 5 is the most current version available, and it has a range of 120 meters (about the height of the Statue of Liberty) and a faster connection capacity. It also has stable connections that can support data transmissions even in environments with significant interference. Additionally, its connectivity can help locate devices and manage connections between several devices simultaneously.

NFC

Near field communication (NFC) is a wireless data-transfer technology, like Bluetooth and Wi-Fi. NFC is effective to the distance of 4 inches, while Bluetooth can reach over 30 feet. NFC is the basis for contactless payments using Apple Pay or Samsung Pay.

Most people consider the short reach of NFC a significant security benefit, which is one reason NFC is popular as a secure alternative to credit cards. It doesn't use the pairing process that Bluetooth does. Instead, whenever two NFC devices are within the 4-inch range, a connection is made and prompts users. NFC can also transfer videos, contact information, and photos between two NFC-enabled devices.

Secure browsing and web-browser attacks

Whether on a desktop, laptop, or phone, browsers are a vital access tool for the internet. Security vulnerabilities in a browser can have a significant impact because of their pervasiveness. A browser's render engine is even built into your email application to review HTML-based email. Besides rendering webpages, browsers have taken on other jobs over time. Modern browsers work with the OS to:

- Cache and help resolve DNS addresses.
- Verify digital certificates.
- Encode requests in HTTPS.
- Store or share cookies that help websites track visitors.

These new browser features accelerated the growth and innovation of the "World Wide Web" and the hacking business that exploited security flaws. As a result, securing browser software is a priority for vendors and website owners.

Browser and page rendering

Browsers are one of the most powerful tools for accessing the internet, and it's crucial to understand how they work. This understanding is especially needed for information technology (IT) and security professionals who build and help secure websites. They need to know how browsers transform the *Hypertext Markup Language (HTML)* that defines the transferred webpage into the interactive, visual images on the screen.

The software component within a browser that parses HTML and transforms it into text and images is the *rendering engine*. The Microsoft Edge rendering engine contains several million lines of code that interpret and generate HTML correctly. The browser's interpretation of the rendered page is stored in Edge's memory as a *Document Object Model (DOM)*. If any JavaScript is present, the browser loads and executes it.

Note: "The Document Object Model (DOM) connects webpages to scripts or programming languages by representing the structure of a document—such as the HTML." [https://developer.mozilla.org/docs/Web/API/Document_Object_Model]

The preceding process happens in fractions of a second and continues as additional pages are accessed. Each of these pages has a unique web address called a *URL*. A *hyperlink* connects webpages within a website or across the web.

Browsing in action

Given the components previously described, let's follow the steps you'd use to sign into Twitter:

1. You want to access Twitter, so you enter twitter.com in their browser's address bar.
2. The browser checks its DNS cache to resolve the domain (twitter.com) to an IP address. If it doesn't find it, it checks the operating system's DNS cache. If it doesn't find it, it queries the ISP DNS server. If still not found, the ISP resolves the domain at an authoritative DNS server.
3. The browser now receives the IP address of Twitter.com, and it initiates a TCP handshake with one of Twitter's servers.
4. The browser sends an HTTP *get* request to Twitter.com after the TCP session is established. Typically, the TCP request will be split into multiple packets and sent to a Twitter server, where it's reassembled.
5. The "conversation" now switches to using HTTPS to ensure secure communications. Next, the browser and the server initiate a TLS handshake, agree on an encryption cipher, and then exchange encryption keys.
6. The server returns an HTTP response of the Twitter front page using the secure channel, the browser displays it, and then additional *get* requests are sent.
7. The login form is submitted with your credentials, which generates a *post* request to the server.
8. The Twitter server validates your credentials, and then begins a session by sending a *Set-Cookie* header response.
9. The browser stores the cookie and sends it back with subsequent requests to Twitter.

After all these steps, you're able to access your Twitter account. If you're using an app, the preceding process is followed. The exception for the app is that, typically, it has stored your credentials, so you won't need to enter them. The website will also have different home pages for mobile-app access versus browser access.

Browsing securely

Help secure connections with websites

Step 5 just discussed uses HTTPS to secure communication between your browser and the website. Describing TLS is beyond the scope of this lesson, but you need to know that HTTP is the basis for how data is communicated across the WWW. The data transferred using HTTP is not encrypted and readable by someone intercepting your communications. Using HTTPS ensures communications between you and the website are encrypted. Most websites have switched to always using HTTPS, but some haven't yet. We recommend installing the HTTPS Everywhere [https://www.eff.org/https-everywhere] plug-in for your browser. It'll automatically request a site to switch from insecure HTTP to secure HTTPS.

Use private mode with browsers

All modern browsers offer a private-browsing mode. For example, in Edge, it's known as an *InPrivate Window*, and you can access it by selecting Ctrl+Shift+N. This mode provides a higher level of privacy than using a browser in regular mode, as your browsing history is deleted when you close all of the InPrivate windows. It'll also delete the logging of sites visited and temporary files or cookies stored on your computer. However, it won't hide your browsing history from your school, employer, or ISP.

Choose a search engine

You also can change a browser's default search engine to a more privacy-focused search engine that helps protect your privacy by not logging or sharing search results. "What you may not realize is 76 percent of websites now contain hidden Google trackers. While 24 percent have hidden Facebook trackers, according to the Princeton Web Transparency & Accountability Project.". If this is a concern, consider using one of these search engines discussed in this article. [https://vivaldi.com/blog/search-engines-that-don't-track/]

Ensure critical certificates checks occur

A secure browser monitors the status of website certificates. They are checked to determine if the certificate is from a valid domain and if it's expired. Valid website certificates help you determine whether a website is pretending to be the requested site. The public certificates come from a Certificate Authority (CA) like VeriSign, and the organization installs the certificates on their website. The client can verify the server identity by checking the certificate store.

Keep your browser updated

You should regularly update your browser and your OS. Security vulnerabilities are typically patched promptly, and vulnerabilities in the render engine and JavaScript engine, when patched, prevent malicious code from running.

Enable the Pop-Up blocker

Pop-ups are typically small advertising ads that “pop up” in your browser without warning or permission. They’re created by JavaScript code that’s embedded in the HTML webpage. You run the risk that malicious software downloads to your computer from pop-up ads if they contain malicious links. Therefore, we recommend that you turn on your browser's pop-up blocker.

Turn on a "Do Not Track" request

All major companies and corporations are collecting user's data. They track your movements across the internet. Modern browsers, both mobile and desktop versions, enable you to configure a "Do not track" setting. When you enable it, a request is sent to the website, internet ad companies, and other analytic companies, asking that they not track your internet movements. Technically, they should obey that request and not follow you. However, studies by privacy advocates discovered that most commercial sites ignore this request. It’s worth turning on for the organizations that do respect it. This likely will become regulated in the future.

Delete your browser cache and cookies

Since "Do Not Track" requests aren’t always honored, regularly clearing your browser cache and not accepting third-party cookies can help stop tracking behavior. You can also default to using your browser’s private mode (refer to preceding discussion), which will ensure an automatic cache deletion occurs when you close it.

Enable DNS over HTTPS

The following process enables DoH in Microsoft Edge:

1. Select the *three dots* in the upper-right corner of Edge, and then select the *Settings* (gear) option.
2. Select *Privacy, search, and services*.
3. Scroll to the *Security* section, and then locate the "*Use secure DNS to specify how to look up the network address for websites*" entry, and then select and turn it on.
4. If this option is grayed out, find out how to make the change at Microsoft Edge Browser Policy Documentation | Microsoft Docs.
5. You can also choose to change your DNS service to use a DoH provider like those previously discussed.

Threat landscape

Threat intelligence is the knowledge that you can use to prevent or mitigate cyberattacks. It helps you make informed decisions about your security by asking you to answer essential questions. Those questions include who's attacking you, their motivations and capabilities, and what indicators of compromise you can search for in your systems. The threat landscape is in constant motion. For example, organized criminals are moving from traditional criminal activities to cybercrime.

The following list includes the most common cybercrime attacks today:

- Intellectual property theft.
- Destruction of property and/or IT resources.
- Identity theft.
- Social-engineering attacks.
- Espionage.
- Surveillance of enemies or dissidents.
- Sowing confusion.

Nation-state attacks typically come from other countries/regions. It's difficult, or even impossible, to prove who ordered the attack. Using contracted hackers is common to lower the risk of political consequences. Cybercrime on a global and political scale is happening and, in many cases, helps to support an underground economy.

Overview of common attack exploits

Network attacks

A *denial-of-service* (DoS) attack comes in two forms. Both forms overload a system, server, or network with traffic. Regardless of whether the IP packets are legitimate or malformed, this traffic overload means normal functions can't occur.

The two variants are:

- *DoS*: This is an attack in which a computer sends many requests to a network service to overwhelm the target service.
- *Distributed denial of service (DDoS):* This is a DoS attack that uses multiple computers in several locations.

Social-engineering exploitation

Social-engineering impersonation refers to an unauthorized person who gains the trust of an authorized person. The goal is usually something nefarious. When their target is a company's employee, they often masquerade as upper management, technical support, or a trusted group member. Social engineering exploits the human element, which typically is the weakest link in security.

Email malware is a form of social engineering. Phishing and spear phishing are the most common social-engineering attacks. Messages are delivered to a user's inbox. They appear to be from a work colleague, friend, or reputable person or company. The email includes an attachment or a URL to select. We're all commonly warned not to select or open unknown attachments, but many people do.

In 2011, a security-infrastructure company was the victim of a sophisticated cyberattack using a phishing email. The email was reported to come from a recruiter. It included a spreadsheet to calculate what your salary should be. Four employees opened the spreadsheet. Inside the spreadsheet was a zero-day Flash Exploit that installed a backdoor for accessing their computers. When the attack was mitigated, it was estimated to have cost $66.3 million.

Malicious hackers can use minor updates made to social media to take aggressive action against individuals or companies. For example, updates on LinkedIn or likes and shared photos on social-media sites are all fodder for bad actors. Hackers use open-source AI to scan social-media posts and sites to harvest details about a person's activities. The AI tools can check millions of profiles and updates, searching for specific vulnerabilities to use in a future targeted attack. This data can then be used in a spear-phishing attack.

For example, you and your team members have returned from a group meeting. You post a photo with the caption: "Great to see everyone in person again! I brought treats from Fourth Coffee!" The hacker reads your "great to be back" post and sends an email to you, supposedly from Fourth Coffee. "Thanks for allowing us to be part of your return to the office celebration. Here is a link for a 15 percent discount on your next visit." But the link installs malware on your system. Unfortunately, hackers are using AI to improve their tools and techniques.

Another example is how social engineering was used to spread a phone attack. The attack was against a popular phone OS. It masqueraded as an operating-system update. When users downloaded the updated app, it prompted them for administrative credentials. The app then installed its malicious payload with administrative privileges. Since the app was downloaded from a third-party website, which should have been a warning sign. Apps should always be downloaded from the applicable app store.

Other social engineering attacks are:

- *Vishing:* Similar to phishing, these attacks use voicemail calls. With the advent of robocalling, it's an effective method of attack.
- *Baiting:* Also, like phishing, but the attacker offers a fake reward or prize.

- *Tailgating:* This type of attack, sometimes called "piggybacking," is where an unauthorized person follows an authorized person into a secure location.

Data breach

A 2021 investigation report details how more than 90 percent of companies that acknowledge they've been hacked were alerted to the hack from entities outside their organizations. A recent data breach involved *shadow IT*. Shadow IT is the use of hardware or software by a department or individual without the knowledge of the IT or security group within the organization. Some employees were using an unapproved off-site storage solution and received what appeared to be a valid email asking them to follow the link and change their passwords because a hack had compromised their user-account information. Some users responded that they thought they were changing their passwords. Instead, they gave their account information to hackers. With that information, the hackers were able to steal data from the cloud-storage vendor. They then used that account information to move into the company's networked computers. The term for unauthorized removal of data is *data exfiltration*.

The company's IT department eventually discovered the data loss and the compromise of their internal system. Employees were questioned about using the unauthorized cloud storage instead of Office365 and OneDrive. They said they used the cloud storage from home and just continued to use it.

Mitigation strategies

The following section details additional mitigation strategies and policies that can help keep you safe online.

Use multifactor authentication

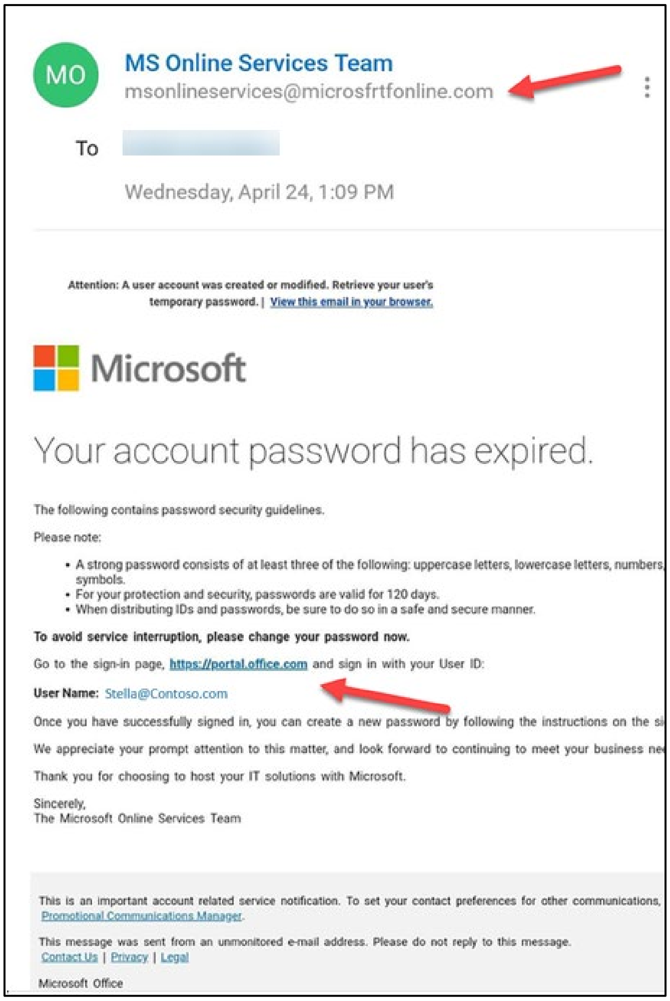
Multifactor authentication is the process of using two or more methods to verify identity. The methods include:

- Something you know (such as a PIN or a password).
- Something you have (such as a cell phone or token).
- Something you are (such as biometric physical characteristics, like a fingerprint).

The conditional access policy of a service enables the enforcement of multifactor authentication.

Defeat social-engineering attacks

Currently, the most successful method for protecting our security depends heavily on training individuals. The training needs to be interesting, engaging, current, and easy to access. Organizations can reinforce learning by using tools such as attack-simulation training in Microsoft Defender for Office 365. The attack-simulator training enables administrators to run benign cyberattack simulations in their organization to test security policies and practices. The following screen capture depicts a testing notice, from a fake Microsoft account (top red arrow), about “Unusual sign-in activity" that directs users to a malicious website (bottom red arrow):



MO

MS Online Services Team
msonlineservices@microsfrtfonline.com

To [redacted]

Wednesday, April 24, 1:09 PM

Attention: A user account was created or modified. Retrieve your user's temporary password. | View this email in your browser.

Microsoft

Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, symbols.
- For your protection and security, passwords are valid for 120 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page, https://portal.office.com and sign in with your User ID:

User Name: Stella@Contoso.com

Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business ne

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team

This is an important account related service notification. To set your contact preferences for other communications, Promotional Communications Manager.

This message was sent from an unmonitored e-mail address. Please do not reply to this message.
Contact Us | Privacy | Legal

Microsoft Office

Here are some additional best practices to help protect you and your company from hackers:

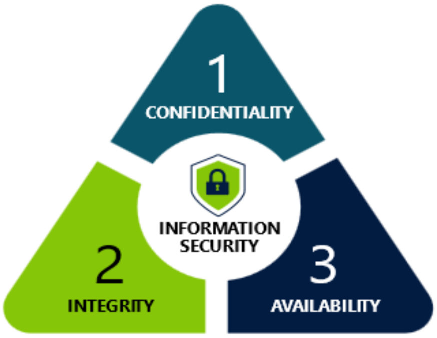
- Examine all of your network accessible settings and enable two-factor authentication. Two-factor authentication is the most common form of multifactor authentication.
- Avoid sharing your work email address.
- Know that most companies will never send an email to verify your credentials.
- Hover over links (but don't select them) to observe the actual URL underneath the words.
- Use cloud-based antivirus solutions such as Microsoft Windows Defender on a Windows 10 device. Windows Defender leverages Azure for faster analysis instead of waiting for traditional antivirus definitions to be delivered.
- Before you post to social media, think about the information that can be harvested from it.
- Don't select links in "call-to-action" messages that demand action, such as "do this now, or something terrible will happen!" Instead, open a web browser and access that company's website and your account. If it's authentic, that message will be there also.
- Keep your OS and its apps patched and updated.

Securing data

The current cybersecurity environment is enormous and impossible to outline in one document. There are, however, several aspects of that environment that you should be aware of, including:

- *Malware*, which is short for malicious software. "It's a catch-all term for any computer program or code that's created to cause harm to computer systems or networks." [A guide to malware for entrepreneurs. https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/a-guide-to-malware-for-entrepreneurs]
  - Malware can alter or delete files, extract sensitive data like passwords and or account numbers, and even send malicious emails or traffic on your behalf.
  - Malware is sometimes bundled with other free software that you or an employee might discover and download.
- *Social engineering* is another popular approach for attacking a business. For example, phishing emails are designed to trick users into selecting links that install malware. By employing urgency or spoofing a senior leader's email address, these messages convince employees to "act now" even if something doesn't seem correct about the communication.

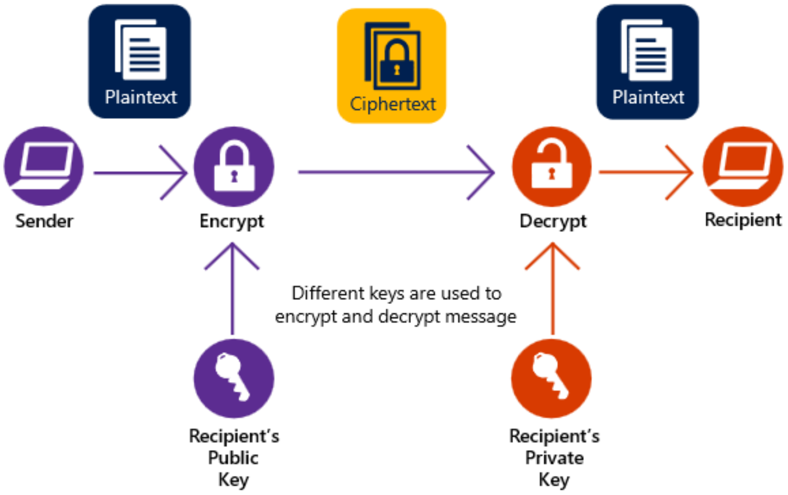
- *CIA Triad,* which include three important data-security principles that form the CIA (*Confidentiality*, *Integrity*, and *Availability***)** Triad. When an organization deploys security controls, they're often evaluated against these three principles, as follows:



  - Confidentiality: Ensure data is protected from unauthorized access?
  - Integrity: Ensure that data isn't altered by unauthorized users.
  - Availability: timely access to the data when needed.

You also can use encryption as another method to help secure data. This method uses a private key and a public key to form a *keypair*, and they mathematically relate to each other. Public key encryption is a form of asymmetric encryption, which often is used to encrypt data in transit. An example is when you're using TLS/HTTPS to secure web traffic.

The following illustration depicts sending an encrypted message by using public key encryption:



The process includes the following procedures:

- First, public, and private keys are generated.
- Public keys are exchanged or placed in a publicly accessible database.
- Each party keeps their private key secret.

Here's an example of this process, with User A sending an encrypted message to User B:

- User A encrypts the message using User B's public key and sends the message to User B.
- User A signed the message with User A's private key.
- User B uses User A's public key to decrypt the signature, confirming the message from User A.
- User B is the only one that can decrypt the message because it requires User B's private key.
- Public key encryption works with SSL/TLS protocol for end-to-end encryption connections.

Notes for the educator

Quiz:

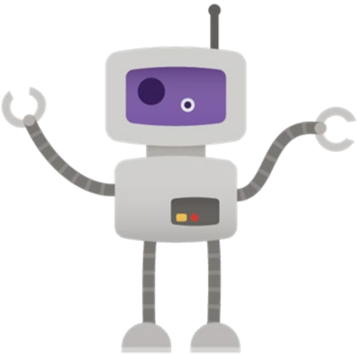
- Wired Equivalent Privacy (WEP) is a preferred encryption for wireless Wi-Fi networking. True or False.
- In the CIA Triad, Availability is the least important concept. Discuss.
- What is the difference between a computer worm and a computer virus?

Additional information

Check out Microsoft Learn for more information

Microsoft Learn provides students with self-paced, digital-learning resources through which they can build skills and foundational understanding of technology. With step-by-step tutorials, hands-on labs, and learning modules, students can advance their knowledge and prepare for industry-recognized certifications.

Check out this list of free courses that'll help further your students' learning from this course or to get certified on Azure



security Fundamentals!

Eligible educators and faculty members can access Microsoft's ready-to-teach curriculum and teaching materials aligned to industry-recognized Microsoft certifications, including Microsoft Azure, Azure Data, Azure AI, and Power Platform fundamentals. Each course covers Microsoft Certification exam objectives through lessons based on real-world scenarios and practice exercises. Supporting resources for the set of "Fundamentals" courseware include:

- Online training
- Microsoft Official Curriculum (MOC)
- Course datasheet
- Educator teaching guide.

Visit aka.ms/learnforedu to get started.

Reference Links

- Steves Internet Guide, TCP/IP Ports, and Sockets Explained at http://www.steves-internet-guide.com/tcpip-ports-sockets
- How do I interpret 'netstat -a' output at https://stackoverflow.com/questions/20882/how-do-i-interpret-netstat-a-output
- Microsoft data platform at https://www.microsoft.com/en-us/sql-server/
- Intel® 64 and IA-32 Architectures Software Developer Manuals at https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html
- Arm Instruction Set Architecture at https://developer.arm.com/architectures/instruction-sets
- OCR A' Level (H046-H446) CISC vs RISC at https://www.youtube.com/watch?v=PaeXsm5HGJs
- Floating Point at Floating Point Definition (techterms.com)

- Find out how many cores your processor has at https://support.microsoft.com/en-us/windows/find-out-how-many-cores-your-processor-has-3126ef99-0247-33b3-81fc-065e9fb0c35b
- CPU-Z System information software at CPU-Z | Softwares | CPUID
- Motherboards Explained at https://www.youtube.com/watch?v=b2pd3Y6aBag&t=8s
- High-Performance Computing at https://www.nvidia.com/en-us/high-performance-computing
- Windows Network Architecture and the OSI Model at https://docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model
- BIND 9 at https://www.isc.org/bind/
- Why you shouldn't use your ISP's default DNS server at https://www.howtogeek.com/664608/why-you-shouldnt-be-using-your-isps-default-dns-server/
- Introduction to cybersecurity at https://docs.microsoft.com/en-us/learn/modules/intro-to-cybersecurity/
- Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security at https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security
- A Guide to Malware for entrepreneurs at A guide to malware for entrepreneurs (microsoft.com)

Glossary

- **Adware**: Software that manipulates a browser into opening pop-ups ads or other ads that contain links that download malicious software.
- **Authentication**: The process that validates that the user is who they claim to be.
- **Botnet**: A collection of compromised internet devices under third-party control. Each device is known as a bot. A botnet distributes malware or performs other functions decided by the third party.
- **Computer worm**: Harmful software code that can replicate and search for new hosts to infect. Once it infects hosts, it destroys data and/or corrupt the system.
- **Computer virus**: This malware can replicate itself by modifying other computer applications. It's malicious software that interferes with a computer's operations.
- **Cryptography**: A field of mathematics that's used to protect data and communications with encryption. The unencrypted data is *plaintext,* and the encrypted information is a *cipher*. A cryptographic key is often a large number and is "seeded" into the encryption algorithm to scramble the data.
- **Cryptojacking**: Malware that uses CPU cycles to mine bitcoin.
- **Data breach**: A data breach is the inadvertent release of secure or confidential information to an untrusted environment.

- **Encryption:** This is the process of encoding data to keep contents secret.
- **Firewall**: The first line of defense between untrusted network-application traffic and your trusted device or your company's trusted network.
- **Keylogger**: A type of adware that tracks keystrokes, typically with the purpose of stealing passwords.
- **Kill chain**: Framework for a cyberattack. Typically, it consists of:
    - Reconnaissance of a target.
    - Determination of the best attack methods.
    - Delivery of the malware.
    - The exploitation of malware on the target.
    - Attacker gaining persistent access to the target.
    - The intruder starting the end goal of intrusion.
- **Malvertising:** Advertising that is served via a legitimate ad network and then delivers malware to users who engage with the ad.
- **Malware**: The malicious software that disrupts a computer's normal operations. Malware is classified as an *advanced persistent threat* (APT). After it's successfully deployed, it remains undetected until activated.
- **Phishing**: An attempt to trick someone into sharing personal information or sending money to them. The most common method is using email messages that appear legitimate.
- **Ransomware**: A form of malware that exploits a system's vulnerability to encrypt files and demand payment to unencrypt the files. Ransomware typically is introduced in email messages.
- **Rootkit**: A collection of software tools that gives an external user administrator-level control over a computer or system.
- **Spear phishing**: A phishing attack that targets specific organizations, businesses, or individuals.
- **Spyware**: Malware that installs itself on a computer to secretly collect and track data.
- **Trojan horse**: Named after the Greeks hollow horse that they used to gain entrance into the city of Troy and win the Trojan war, this is a form of malware software that appears to be something it isn't. It typically functions as a hacker's back door into an organization's system.
- **Zero-day vulnerability**: The term "zero day" is a security flaw in software, hardware, or firmware that's unknown to the party or parties responsible for patching or otherwise fixing the flaw. It typically refers to the vulnerability itself or an attack that has zero days between the time the vulnerability is discovered and the first attack.