Google IT Support Professional Training *(took 137hrs)*

Course #1: **Technical Support Fundamentals**

How much info/ what's the highest number you can make with a 2^x bit number? 2^8 = 8 bits

2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^{16}	2^{24}	2^{32}	2^{64}	2^{128}	2^{256}
4	8	16	32	64	128	256	65,536	16,777,216	4,294,967,296	18,446,744,073,709,551,616	340,282,366,920,938,463,463,374,607,431,768,211,456	1.158 x 10^77

Character Encoding is what translates binary into things humans can perceive. (ASCII, UTF-8 for text and even RGB for color)

- Hard Disk Drives are less expensive than Solid State Drives
- Computers use DC (Direct Current) voltage. If your outlet has a higher voltage than your device charges with, it'll explode.
- The "water pressure" of an electric cable is **Voltage** (wall outlets have voltage)
- The amount of electricity "coming out" is "Amperage" or "**Amps**"
- Watts are a combo of Volts and Amps, which means total electricity throughput. Watt is a a combo like how meters per second is a combo of distance and time (These combos are called "**vectors**" in math)
- Most desktops can work with a 500w power supply, but high performance shit like video editing or gaming may benefit from a higher wattage.
- Power standards for input voltages can vary from country to country. The most common voltage inputs are 110-120 VAC and 220-240 VAC. VAC stands for **volts of alternating current.**

If a computer needs	But the wall socket delivers	The result will be
220-240VAC	110-120VAC	not enough power for the computer to run properly
110-120VAC	220-240VAC	too much power, which will damage the computer's internal parts

- The computer's power supply plugs into an adapter on the computer's motherboard. The wiring for this connection uses color coded wires. Each wire color carries a different voltage of electricity to the motherboard or serves as a grounding wire. A standard ATX motherboard power adaptor has either 20-pins or 24-pins to connect these wires. The 20-pin design is an older technology. The 24-pin connector was developed to provide more power to support additional expansion cards, powerful CPUs, and more. The 24-pin connector has become the standard for today's personal computer power supplies and motherboards.

The power supply will have multiple connectors that plug into the motherboard, hard drives, and graphic cards. Each cable has a specific purpose and delivers the appropriate amount of electricity to the following parts:

Connections from a PC power supply (ATX 2)

1. Floppy disk drive (obsolete)
2. "Molex" universal (e.g. IDE hard drives, optical drives)
3. SATA drives
4. Graphics cards 8-pin, separable for 6-pin
5. Graphics cards 6-pin
6. Motherboard 8-pin
7. Motherboard P4 connector, can be combined to 8-pin mainboard connector 12V
8. ATX2 24-pin, divisible 20+4, and can therefore also be used for old 20-pin connections

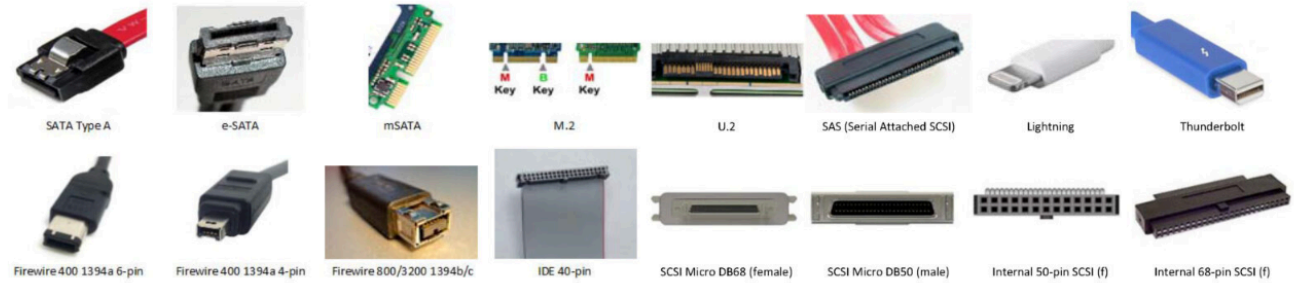
Key takeaways

When selecting a power supply for a computer, the following items should be taken into consideration:

1. Wall socket input voltage standard for the country where the computer will be used;
2. The number and power consumption needs of the computer's internal components;
3. The motherboard model and form factor engineering specifications and requirements.

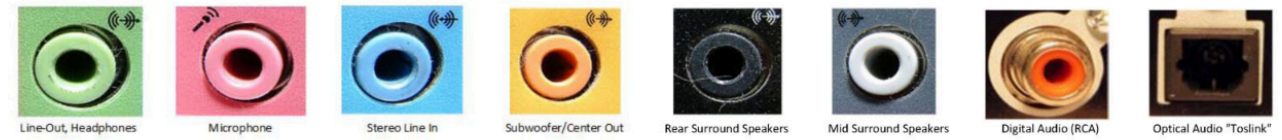
USB, Keyboard and Mouse

Storage / Disk

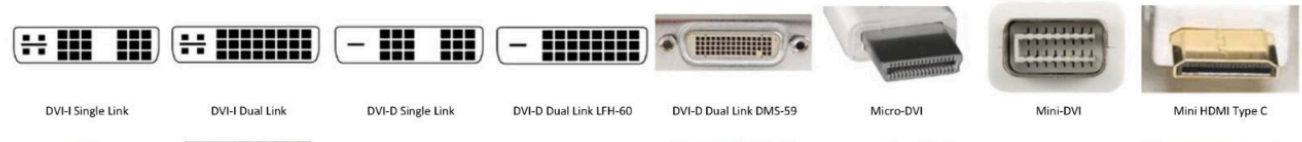


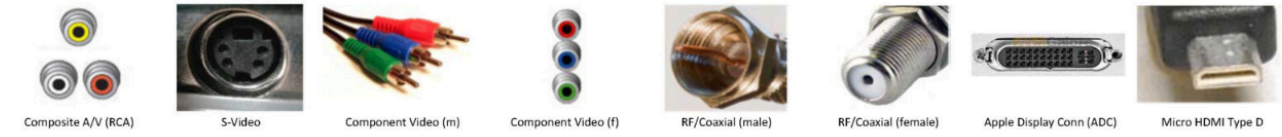
Network / Communications

Audio



Video





Power

- All **rechargeable batteries** have a lifespan measured in charge cycles.

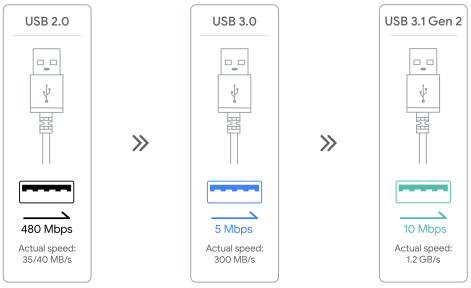
- to transfer 40 megabytes of data in a second, you need a transfer speed of 320 megabits per second. Thus, the formula for bytes-to-transfer in a second its (Bytes) times 8 = (Necessary megabits per second in order to transfer all the Bytes in one second)
- It's actually called the CMOS **battery** (a correction from the coursera vids)

Supplemental Reading on Connector Types

A computer has many physical ports or connectors. You can use these connectors to connect devices that add functionality to your computing, such as a keyboard, mouse, or monitor. These external devices are called peripherals. IT often works with and troubleshoots these peripherals, so it is helpful to understand the types of connectors. This reading will cover different types of connectors and their uses.

USB 2.0, 3.0 & 3.1

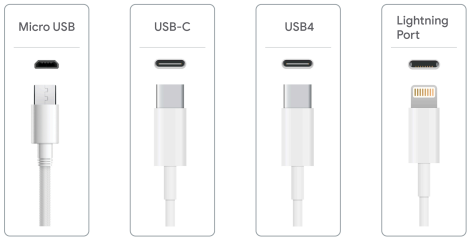
USB connectors transfer data and power to devices connected to a computer. USB connectors are the most popular connectors for all types of peripherals. There are three generations of USB type A connectors in use today: USB 2.0, 3.0, and 3.1. Here are the differences between the three generations:



- USB 2.0: Black port on the computer, 480 MBps transfer speed
- USB 3.0: Blue port on computer, 5 Gbps transfer speed
- USB 3.1: Teal port on the computer, 10 Gbps transfer speed

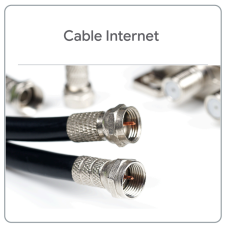
USB ports are backwards compatible, meaning a USB port can connect any of the three generations of USB type A connectors. The connected cable will determine the speed of data transfer. Connecting a USB 3 to a USB 2 port will result in 480 megabytes per second of speed.

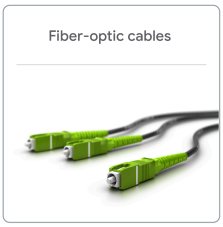
Micro USB, USB-C & Lightning Port



Micro USB, USB-C, USB4 (Thunderbolt), and Lightning Ports are smaller connectors that carry more power than older USB connectors and have faster data transfer speeds. These connectors are used for devices like smartphones, laptops, and tablets.

- **Micro USB** is a small USB port found on many non-Apple cellphones, tablets, and other portable devices.
- **USB-C** is the newest reversible connector with either end having the same build. USB-C cables replace traditional USB connectors since they can carry significantly more power and transfer data at 20 Gbps.
- **USB4** uses Thunderbolt 3 protocol and USB-C cables to transfer data at speeds of 40 Gbps and provide power as well.
- **Lightning Port** is a connector exclusive to Apple that is similar to USB-C. It is used for charging and connecting devices to computers, external monitors, cameras and other peripherals.





Communication Connectors

Different cable connectors are used to share information between devices and connect to the internet. IT professionals maintain network systems that use different types of communication connectors.

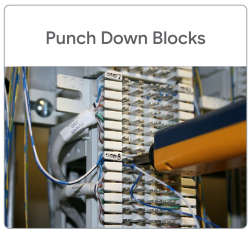
- **Plain Old Telephone Service (POTS)** refers to cables transmitting voice through twisted copper pair wires. Landline telephones, dial-up internet, and alarm systems use POTS. The RJ-11 (Register Jack 11) connector is used for POTS.
- **Digital Subscriber Line (DSL)** provides access to high-speed networks or the internet through telephone lines and a modem. The RJ-45 connects a computer to network elements and is mostly used with ethernet cables.
- **Cable Internet** uses a cable TV infrastructure and a modem to provide high-speed internet access to users. An F type connector is commonly used with cable modems..
- **Fiber-optic cables** contain strands of glass fibers inside an insulated casing that send data long-distance and allow for higher-bandwidth communication. The major internet providers use fiber-optic cables for high-speed internet service.

Device Connectors

IT professionals will encounter legacy devices that still use older connectors such as DB89 and Molex.

DB89 connectors are used for older peripherals like keyboards, mice, and joysticks. An IT professional may still encounter a DB89 connector for external tools a computer uses and should recognize the cable to connect to the appropriate port.

Molex connectors provide power to drives or devices inside the computer. Molex connectors are used for connecting a hard drive, disc drive (CD-ROM, DVD, Blu-ray), or a video card.



Punch Down Blocks

A punch down block is a terminal strip used to connect telephone or data lines. Punch down blocks are a quick and easy way to connect wiring. IT professionals use punch down blocks to change a wire or make a new connection for a telephone system or Local Area Network (LAN).

These are the most common cables and connectors. As technology advances, these cables and connectors will also change.

Key Takeaways

IT professionals need to be familiar with cables and connectors used to attach peripheral devices to computers.

- USB connectors are the most common connector type and they transfer data and power to devices connected to a computer.
- Communication connectors, such as RJ-45 and fiber optic cables, connect devices to the internet and one another.
- IT professionals may encounter legacy devices that use older connectors such as DB89 and Molex.
- Punch down blocks are terminal strips used to connect telephone or data lines.

When repairing mobile devices,

Protect against static discharge, use the right tools, keep parts organized and labeled, taking pictures along the way can help a lot too, follow vendor documentation, and test the device to make sure it still works.

Mobile Display Types

In this reading, you will learn about several types of displays used in modern mobile devices and monitors. As an IT Support professional, you may need to troubleshoot various types of displays. This might involve repairing damaged mobile device screens. You may even be responsible for selecting and ordering mobile devices for the employees of an organization. In your IT job role, you should have a basic understanding of the technology behind modern displays, as well as their common uses, positive features, and negative flaws. The top two technologies used in mobile system displays are Liquid Crystal Displays (LCD) and Light Emitting Diodes (LED).

Liquid Crystal Display (LCD)

LCDs use liquid crystal technology. Liquid crystals have the properties of both a liquid and a solid. The crystals can be aligned in a variety of patterns and manipulated with electricity. How the liquid crystals are arranged and manipulated inside display panels affects refresh rates, image quality, and display performance. LCDs require backlighting, often provided by LEDs. Displays that need backlighting are also called non-emissive or passive displays. The backlighting unit (BLU) requires extra space, which makes LCD panels thicker and less flexible than other displays. Polarizers on either side of the liquid crystal layer control the path of the backlight to ensure the light is aimed toward the user.

The following are common LCD display types used for mobile devices:

In-Plane Switching (IPS)

- **How it works:** In IPS displays, the liquid crystals are aligned horizontally to the screen. Electricity is passed between the ends of the crystals to control their behavior.
- **Uses:** IPS technology is used in touch screen displays and high-end monitors. They are often used for design, photography, video/film editing, animation, movies, and other media. They can also be used for games that rely on color accuracy and wide viewing angles, as opposed to speed.
- **Positives:** IPS displays provide vibrant colors, high quality graphics, and wide viewing areas. Additionally, they offer excellent color reproduction, accuracy, and contrast.
- **Negatives:** IPS displays are expensive. They have low refresh rates and slow response times. However, response times have been improving as the IPS technology evolves. IPS displays can be affected by “IPS Glow”, where the backlight is visible from side viewing angles.

Twisted Nematic (TN)

Twisted Nematic (TN) is the earliest LCD technology that is still in use today. The term nematic, which means “threadlike,” is used to describe the appearance of the molecules inside the liquid.

- **How it works:** In TN displays, the liquid crystals are twisted. When voltage is applied, the crystals will untwist to change the angle of the light they transmit.
- **Uses:** TN displays are appropriate for basic business use (e.g., email, document, and spreadsheet applications). They are also used for games that need rapid display response times.
- **Positives:** TN displays are low cost, easy to produce, have excellent refresh rates, response times, and resolutions. They are versatile and can be manufactured for any size and/or shape.
- **Negatives:** TN displays have narrow viewing angles, low image quality, color distortion, and poor color accuracy and contrast.

VA-Vertical Alignment

- **How it works:** In VA displays, the liquid crystal molecules are vertically aligned. They tilt when electricity passes through them.
- **Uses:** VA displays are intended for general purpose. Provides mid-range performance for graphic work, movies, and TV.
- **Positives:** VA displays offer great contrast, deep black shades, and fast response times. They are mid-range quality for refresh rates, image quality, viewing angle, and color reproduction.
- **Negatives:** On VA displays, motion blur and ghosting occurs with fast-motion visuals.

Organic Light Emitting Diodes (OLED)

OLEDs are diodes that emit light using organic (carbon-based) materials when electricity is passed through the diodes. Displays that are able to convert electricity into light are called emissive or active displays.

- **How it works:** The basic structure of an OLED display consists of an emissive layer placed between a cathode (which injects electrons) and an anode (which removes electrons). Electricity enters through the cathode layer, passes into the emissive layer and conductive layer to create light, then out through the anode layer.
- **Uses:** OLED display technology can be used in foldable smartphones, rollable TVs, as backlighting in LCD TVs, for gaming, and inside VR headsets.
- **Positives:** OLED displays deliver excellent picture quality, wide viewing angles, infinite contrast, fast response rate, and brilliant colors with true blacks. They are energy efficient, simpler to make, and much thinner than LCDs. OLED panels can be built to be flexible and even rollable.
- **Negatives**: OLED displays are sensitive to light and moisture. Blue LEDs degrade faster than other LED colors causing color distortion over time. They are also prone to image retention and burn-in.

Active Matrix Organic Light Emitting Diode (AMOLED)

Active Matrix Organic Light Emitting Diode (AMOLED) and Super AMOLED are recent technologies used in smartphone displays.

- **How it works:** AMOLED displays are a type of OLED panel that uses active matrix technology. Active-matrix displays have active capacitors arranged in a matrix with thin film transistors (TFTs). This technology enables the control of each individual pixel for rapid state changes, including changing brightness and color. AMOLEDs have touchscreen functions integrated into the screen.
- **Uses:** AMOLED and Super AMOLED panels are used in high-end mobile devices, flat screen monitors, curved screens, and touchscreens.
- **Positives:** AMOLED displays offer a high picture quality and fast response time. Color and brightness are consistent across the screen. Fast-moving images and motion are displayed clearly without blurring or ghosting. Super AMOLED panels can display a wider range of colors with enhanced contrast, which makes them easy to view in a wider variety of lighting conditions.
- **Negatives:** AMOLED displays have the same problems as OLED displays (listed above) plus AMOLED panels can be difficult and expensive to manufacture.

Inorganic mini-LEDs (mLEDs)

Inorganic mini-LEDs (mLEDs) are a next-generation, emissive display technology.

- **How it works:** Mini-LED displays work the same way that OLED displays work, but the individual LED size is much smaller at approximately 50-60 micrometers.
- **Uses:** Mini-LED displays are used for LCD backlighting in smartphones, public information displays, signage, electronics, vehicle displays, and more. Mini-LEDs are also the tech behind “Liquid Retina XDR” screens.
- **Positives:** Mini-LED displays offer ultra high luminance, superior HDR fineness, long lifetimes, thin panels, and are readable in sunlight. They are also less expensive than micro-LED displays.

- **Negatives:** Mini-LED displays, when used as LCD backlighting, are limited by the properties of LCD technology. Mini-LED displays for mobile devices are more expensive than OLED displays.

Inorganic micro-LEDs (µLEDs)

Micro-LEDs (µLEDs) are also emissive, next-generation displays.

- **How it works:** Micro-LED displays work the same way that OLED displays work, but the individual LED size is extremely small at 15 micrometers.
- **Uses:** Micro-LED displays can be used in smartphones, AR/VR headsets, wearables, public information displays, wall-sized TVs, vehicle displays, and more.
- **Positives:** Micro-LED displays offer superior performances across virtually all common display features, such as brightness, reaction speeds, power consumption, durability, color gamut, stability, viewing angles, HDR, contrast, refresh rates, transparency, seamless connectivity, and more. Micro-LED displays are readable in sunlight and have sensor integration capability.
- **Negatives:** Micro-LED displays are expensive to manufacture and are not yet ready for mass production.

Key takeaways

The two main technologies used in mobile displays are Liquid Crystal Display (LCD) and Organic Light Emitting Diodes (OLED). Each technology has its own benefits and drawbacks when used in mobile device displays, among other consumer goods.

- Common LCDs include:
  - In-Plane Switching (IPS) displays
  - Twisted Nematic (TN) displays
  - VA-Vertical Alignment displays
- Common and upcoming OLED displays include:
  - Active Matrix Organic Light Emitting Diode (AMOLED) displays
  - Inorganic mini-LEDs (mLEDs) displays
  - Inorganic micro-LEDs (µLEDs) displays

What is a cyclical redundancy check?

Ethernet is a data link level protocol
How the fuck do we prevent the electrical currents representing our 1s and 0s from crashing into each other? It's a li'l thing called CSMA/CD.

Boot Methods

While the most common way to boot a computer is to simply push the power button and allow the normal process to run, there are many other boot options. This reading covers the various methods you can use to boot a computer.

Internal method

You can create partitions on the computer's drive so that only one part of the drive runs the boot process. A common reason to partition your drive is to have two separate operating systems on your computer, such as both Windows and Linux. When you have two operating systems on your drive, you must choose which one will run the boot process. Having two possible systems to boot into is called dual booting.

While having two operating systems can be helpful for various reasons, it is especially helpful when one system is failing or unable to boot. If this happens, you can still boot the computer using the other system and troubleshoot from there.

External tools

External tools can be used to boot the computer. You can load the needed resources on an external tool to boot a system before any problems happen.

External bootable devices include:

- **USB drive**: You use a USB drive loaded with resources needed to boot the computer. This drive is inserted into a USB port and chosen at startup.
- **Optical Media:** You use a disk loaded with booting resources. This disk can be a DVD, CD, or Blu-ray disk and is loaded through the computer's optical drive.
- **Solid State Boot Drive:** You use a solid state drive to boot. Solid state drives do not use spinning discs or moving parts. This solid state drive can be installed in your computer or can be a smaller device such as a flash drive.
- **External hot-swappable drive**: You boot from an external hard drive that can be moved between computers without turning it off.
- **Network boot:** You boot the operating system directly from a local area network (LAN) without using a storage device. Your computer must be connected to a LAN for this option.
- **Internet-based boot:** You boot the computer from an internet source, as long as it is a secure source. Your computer must be connected to the internet for this option.

Window OS or Linux OS

In order to boot either Windows OS or Linux OS with an external tool, you'll need to enter BIOS at startup by pressing F2/F12/Del keys. From there you can change the boot order so that the first option is the external tool you want to use.

macOS

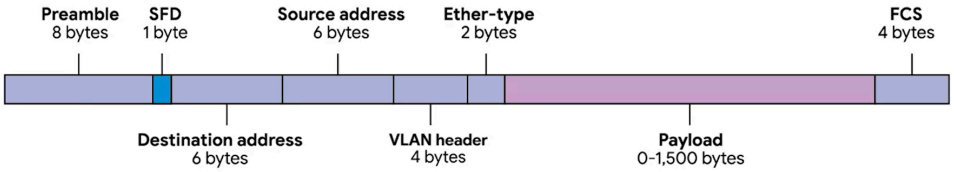
If booting macOS, press and hold the Option key at startup. This will open up the Startup Manager, which will scan your computer and identify bootable devices. Then you can choose the bootable device you want to use.

Key Takeaways

There are multiple ways to boot a computer.

- A computer can be partitioned into different operating systems and you can select which OS to use when booting.
- You can boot from an external tool. External tools include USB drives, optical media, solid state boot drives, external hot-swappable drives, network booting, and internet-based booting.
- Choosing a boot method on startup varies depending on which operating system you use.

Ethernet Frame Pictured RIght →



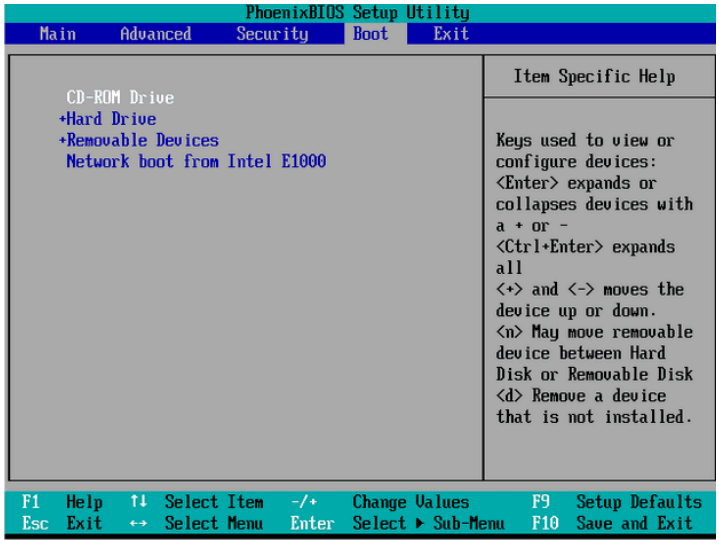
Boot Methods Best Practices

The most common way to boot a computer is to simply push the power button and allow the normal startup process to run. But what happens if the normal startup process becomes corrupted and the computer will not boot? Or maybe you would like to run a computer on a different operating system than the one specified by your normal boot process. For situations like these, you have several options for booting your operating system. This reading covers the various methods you can use to boot a computer.

The boot process

When your computer is powered on, the BIOS/UEFI (BIOS) runs a series of diagnostic tests to make sure that the computer is in proper working order. The BIOS is a low-level software that initializes a computer's hardware to make sure everything is good to go. A boot device is selected based on a boot order that is configured in the BIOS. Devices that are attached to your system, like hard drives, USB drives, and CD drives are checked in this configured boot order and the computer searches these devices for a small program called a “bootloader.” Once your computer finds a bootloader on a device, it executes this program. The bootloader program then initiates a process that loads the specific operating system setup that you want to use.

You can choose a computer’s boot method by telling the BIOS on which device to search for the bootloader. If you want to run an OS setup that’s stored on a USB drive, you can configure the boot order in your computer’s BIOS to search for a bootloader on a USB drive first.



Configuring boot options

Boot order is the order in which a computer chooses which boot files to use to startup. The boot order determines your boot method. To set the boot order for a computer, you need to enter the BIOS and configure the boot options.

To enter your computer’s BIOS on a Windows or Linux computer, power on the system and look for an on-screen message that says which function key you should press to enter setup. The function keys used for entering the BIOS vary between computer manufacturers and the version of BIOS. Some of the more common function key messages are "Press DEL to enter SETUP," "F2=SETUP," or "Press F12 to enter SETUP." If booting macOS, press and hold the Option key at startup. This will open up the Startup Manager, which will scan your computer and identify bootable devices. Then you can choose the bootable device you want to use.

If you press the specified function key during the Windows or Linux power up process (before the OS begins to load), you will open your BIOS program. A BIOS screen will look similar to this:

The BIOS screen will vary depending on your computer manufacturer and BIOS version, but all BIOS programs will feature a Boot Options menu. The Boot Options menu is where you can set your preferred boot method.

The boot options menu lists all the devices attached to your system where it may find a bootloader program. These include devices like internal hard drives, USB drives, CD drives, as well as other storage options, like network storage or cloud storage. In the BIOS boot options menu you can set the specific order you want to search these devices for the bootloader that will load your OS setup. The BIOS will run the first bootloader that it finds.

Boot method options

You may find the following boot methods listed in your BIOS boot options:

External options

- **USB drive:** You use a USB drive loaded with resources needed to boot the computer. This drive is inserted into a USB port and chosen at startup.
- **Optical Media:** You use an optical media disk loaded with booting resources. This disk can be a DVD, CD, or Blu-ray disk and is loaded through the computer's optical drive.

The USB drive and optical media methods are useful for recovering a computer with a corrupted OS. They can also be used to start up a computer with a different OS. For example, you might boot a Windows computer in a Linux environment by using a USB with Linux OS. You will need to prepare these media with a bootable OS in order to use them as a boot method (see resources linked below).

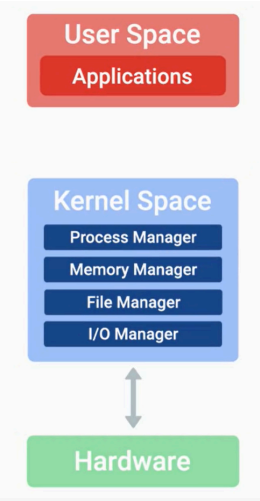
- **Solid State Boot Drive:** You can use a solid state drive to boot your computer. Solid state drives do not use spinning discs or moving parts. This solid state drive can be installed in the computer or can be a smaller device such as a flash drive.
- **External hot-swappable drive:** You may boot from an external hard drive that can be moved between computers without turning it off.
- **Network boot:** You can boot an operating system directly from a local area network (LAN) without using a storage device. Your computer must be connected to a LAN for this option. The network boot is used when the computer does not have an OS installed, among other things. To boot from a network, you will need to set up the Preboot Execution Environment (PXE) capability on the BIOS and have the network environment prepared for this type of request (see resources linked below).
- **Internet-based boot:** You boot the computer from an internet source, as long as it is a secure source. If you are in charge of a network and your server is down for any reason, you can use this boot method to remotely power on the server and restart network operations. Internet-based boot can be achieved in one of two ways:

1. Remote access. Remote Access Controller (IPMI or similar) has to be enabled on the BIOS and the computer needs to have a Remote access control device, such as IDRAC (see resources linked below).
2. Wake on LAN (WoL). This process requires the WoL option enabled on the BIOS (see resources linked below). The WoL instruction should come from a device in the network or use a WoL gateway, and the network card should have WoL capability.

Internal options

Disk partitions: You can create partitions on your computer's drive so that only one part of the drive runs the boot process. A common reason to partition your drive is to have two separate operating systems on your computer. For example, you could have Windows on one partition of your drive and Linux on the other. When you have two operating systems on your drive, you must choose which one will run the boot process. Having two possible systems to boot into is called dual booting.

While having two operating systems can be helpful for various reasons, it is especially helpful when one system is failing or unable to boot. If this happens, you can still boot the computer using the other system and troubleshoot from there.



Key Takeaways

There are multiple ways to boot a computer.

- A computer can be partitioned into different operating systems and you can select which OS to use when booting.
- You can boot from an external tool. External tools include USB drives, optical media, solid state boot drives, external hot-swappable drives, network booting, and internet-based booting.
- Choosing a boot method on startup varies depending on which operating system you use.

The hierarchy of an operating system pictured **left**. The Kernel Space is what the OS is handling in the background.

Windows 10 and 11 Feature Matrix

Windows 10 and 11 are two operating systems IT Professionals work with. This reading describes the differences between them and highlights features that are important to IT. Windows 11 was released more recently and has higher system requirements than Windows 10. Professionals will still work with Windows 10 often, as many companies still use it.

The primary difference between the two operating systems is aesthetic. Windows 11's design is more minimal, corners have been rounded, and colors are pastel. Another difference is in Windows 10, the start menu and taskbar are in the bottom left corner. In Windows 11, the start menu and taskbar are centered along the bottom.

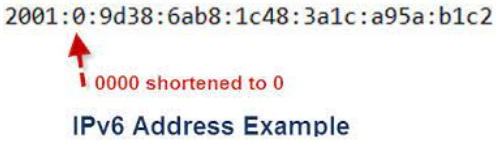
Features

- **Apps**: In Windows 10, apps can only be added from the Windows Store or installed manually. In Windows 11, Android apps can also be added natively.
- **Virtual desktop**: In Windows 10 it is possible to use Virtual Desktops, but it is unintuitive to set up. In Windows 11, the support for virtual desktops is more user-friendly making it easy to set up different desktops for work and personal use.
- **Teams**: In Windows 10, Teams is included in the operating system, but defaults to Skype for video conferencing. In Windows 11, Teams is featured prominently and incorporated into the taskbar and no longer defaults to Skype for video conferencing.
- **Widgets**: In Windows 10, there are desktop gadgets similar to widgets that can be added to the start menu. In Windows 11, widgets can be accessed from the taskbar directly.
- **Touch and pen**: Windows 11 has added more features for touch and pen use on supported devices, including vibration features for pens.
- **Random Access Memory (RAM) Support Limitations:** In Windows 10, the lowest RAM (Random Access Memory) requirements are 1GB for 32-bit versions and 2GB for 64-bit versions. In Windows 11, the base requirement is 4GB of RAM.

Services and settings

- **Domain access:** Joining a domain, a centrally administered group of computers, functions the same in Windows 10 and 11. A user can quickly join a domain from the "System Properties" window.
- **Workgroup access:** Joining a workgroup, a group of computers on the same Local Area Network (LAN) with shared access and responsibilities, also functions the same in Windows 10 and 11. A user can quickly join a workgroup from the "System Properties" window.
- **Group Policy Settings (Gpedit.msc)**: Editing Group Policies (with Gpedit.msc) locally or using Active Directory is largely unchanged. Note that Gpedit.msc is not available in Home licenses of Windows.
- **Remote Desktop Protocol:** The Remote Desktop tool, used for connecting to the desktop of a different computer over a network connection, is largely unchanged between Windows versions. Note that to use a Remote Desktop Server, the server machine needs to be running at least the Pro edition of Windows.
- **Bitlocker:** Bitlocker, a drive encryption tool included with Windows, is largely unchanged. Note that Bitlocker is only available for Pro and Enterprise licenses of Windows.

Key takeaways



IPv6 Address Example

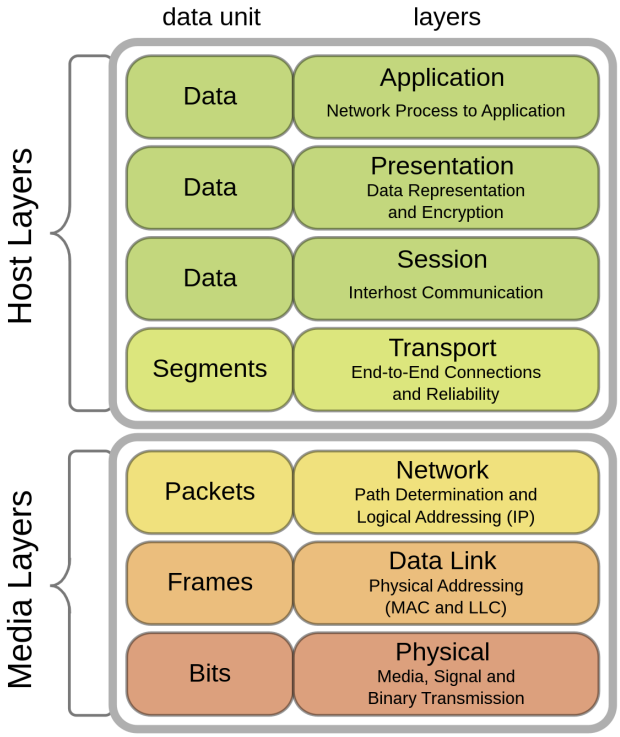
Operating systems like Windows 10 and Windows 11 are constantly changing and evolving. As an IT professional, you may be required to maintain two or more versions of an operating system at the same time. IT professionals need to stay on top of changes and new development to ensure they can support their users.

- Windows 10 and Windows 11 primary difference is aesthetic.
- Windows 11 updated and added new features to make it simpler to access or use apps services, and settings.

Chrome OS is based on Linux

BASH is the name of the shell (command line interface) for Linux. On windows it's Powershell/ Command Prompt. On Mac it's the Mac Terminal

If you're having a problem with network connectivity, you will need to work your way up the "network stack" (See the 7-layer pic below)



URL = Uniform Resource Locator

Common Scripting Solutions

In this reading, you will learn about a variety of scripting languages, their uses, and their risks. As an IT Support professional, you may need to automate routine tasks. For example, you might want to automate a backup of company data that runs every night. You might also need to automate high volume tasks, like changing security access settings on thousands of files. Scripting is a common tool used for automation. This tool can help IT Support staff save time and resources in a busy enterprise work environment.

Scripting languages

There are many scripting languages available to use for a variety of tasks in different operating system environments. Most scripts are written in command line environments.

Scripting languages for Windows environments:

- **PowerShell (.ps1)** - Windows PowerShell is among the most common command line scripting tools used in Windows environments. PowerShell is built on the .NET platform and employs many of the same elements that programming languages do. PowerShell scripts are used for building, testing, and deploying solutions, in addition to automating system management.
- **Batch scripts (.bat)** - Batch scripts, also called batch files, have been around since the early days of MS DOS and OS/2. Batch files can execute simple tasks, like calling a set of programs to run when a computer boots up. This type of script could be useful in setting up employees' workspaces when they power on their computers.
- **Visual Basic Script (.vbs)** - Visual Basic Script is an older scripting language. It has reached its end of life for Microsoft support and has been replaced by PowerShell scripts. However, as an IT professional, you may encounter .vbs scripts on some legacy systems.

Scripting languages for Linux and Unix environments:

- **Shell script (.sh)** - Shell scripting languages, like Bash, are used in Unix or Linux environments. The scripts are often used to manipulate files, including changing file security settings, creating, copying, editing, renaming and deleting files. They can also be used to execute programs, print, navigate the operating system, and much more. The scripts run in command-line interpreter (CLI) shells, such as the Bourne shell, Bourne Again SHell (Bash), C shell, and Korn (KSH) shell.

Programming languages that can be used for scripting:

- **JavaScript (.js)** - JavaScript the most used programming language in the world. It is a lightweight language that is used for scripting in web development, mobile and web apps, games, and more. It can also be used to develop software and automate web server functions.
- **Python (.py)** - Python is a user-friendly programming language that can perform advanced tasks and import modules from libraries specially designed for automation scripts.

Scripting uses - finding the right tool for the job

- **Basic automation:** Python is an excellent script for automation. It's one of the most commonly used, with many available automation libraries.
- **Restarting machines:** Many power users use PowerShell (.ps1) scripts to restart machines (Windows). For Linux machines, they can use .sh (shell) scripts.
- **Mapping network drives:** In the past, mapping network drives was accomplished with .bat or .vbs scripts. However, PowerShell scripts are most commonly used to map drives in Windows environments today. For Linux users, shell scripts can be used for this purpose.
- **Installing applications:** Batch files and shell scripts are often used for automated software installation.
- **Automated Backups:** Windows PowerShell and Linux/Unix shell scripts can automate backups.
- **Gathering of information and data:** Python is a popular choice for gathering data. Python has many available libraries to help with this task.
- **Initiating Updates:** Powershell and shell scripts can be used for initiating updates in Windows and Linux, respectively.

Security risks of using scripts

IT Support professionals need to be very careful when using scripts, especially with prewritten scripts copied or downloaded from the internet. Some of the security risks of using scripts could include:

- **Unintentionally introducing malware:** As an IT Support professional that is new to scripting, you may try to search the internet for assistance in writing scripts. In your search, you might find a script online for a task that you want to automate. It's tempting to save time and effort by downloading the script and deploying it in your network environment. However, this is dangerous because scripts authored by an unverified source could potentially contain malware. Malicious scripts could have the power to delete files, corrupt data and software, steal confidential information, disable systems, and even bring down an entire network. Malicious scripts can create security weaknesses for the purpose of creating entry points for cybercriminals to penetrate networks. Scripts could also introduce ransomware attacks, which often works by encrypting file systems and then selling the decryption keys for ransom.
- **Inadvertently changing system settings:** Scripts are powerful tools for changing system settings. Using the wrong script can cause the user to inadvertently configure harmful settings. For example, one minor typo in a shell script that sets file permission security in Linux could make confidential files accessible to the world.
- **Browser or system crashes due to mishandling of resources:** Mishandling resources can lead to program crashes in the browser or cause the entire computer to crash. For example, directing too much memory to the browser can overload the computer system.

Key takeaways

A basic knowledge of scripting is an important tool for IT professionals. You may need to improve workflow efficiency by automating basic functions with a scripting language. Some common scripting languages include:

- Windows environments: batch scripts (.bat), Powershell (.ps1), Visual Basic Script (.vbs)
- Linux/Unix environments: shell scripts (.sh)
- Most OS environments: javascript (.js), Python (.py)

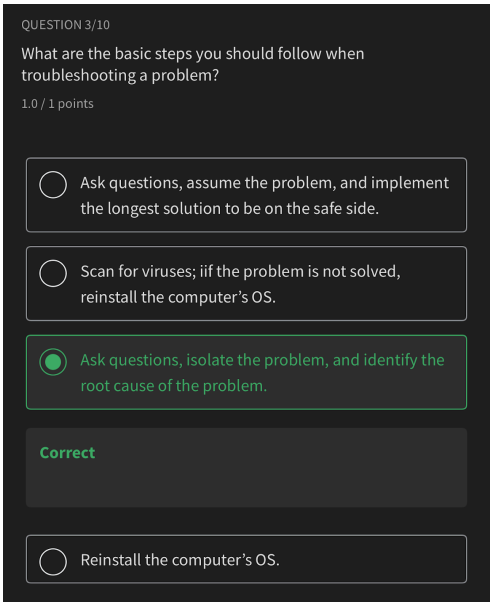
Scripts have multiple helpful uses, such as:

- Basic Automation
- Restarting Machines
- Remapping Network Drives
- Installing Applications
- Automating Backups
- Gathering of information/ data
- Initiating Updates

There are risks in using scripts, including:

- Unintentionally introducing malware
- Inadvertently changing system settings
- Browser or system crashes due to mishandling of resources

When troubleshooting or checking logs, be mindful that one error can cause “cascading errors” like a waterfall. So, go to the first error message you see, then try to fix THAT before going to the ones lower in the log.



When there's multiple options to address an issue, always start with the quickest one

Technical Interview Prep

No filler text. Stick to ***what’s relevant for the job***.

An **Elevator Pitch** is a short summary of who you are, and what kind of career you’re looking for.

Ex:

Hi! I’m Ellis, I’ve been working at X Company as an IT Support Specialist for the past two years. During those years, I’ve learned a lot about operating systems and networking and I’m looking to switch to a system administrator position, where I can focus on large scale deployments.

Hi! I’m Jamie, I’m in my senior year at Springfield University, studying Computer Science. I enjoy being able to help people and solve problems, so I’m looking forward to putting my tech skills into practice by working as an IT Support Specialist after I graduate.

My name is Rob Clifton, and I’m a Program Manager at Google. I manage all of our hiring efforts for our junior IT support roles. I’ve interviewed hundreds of candidates, and I help train our interviewers on how to find the best talent in the industry.

Technical Interview Tips:

1. **Having a strong problem-solving strategy is more important than having all the answers!**
2. Active Listening Skills:
    a. Make eye contact
    b. Nod to show understanding
    c. Ask follow-up questions
3. Remember to slow down

IT Best Practices:

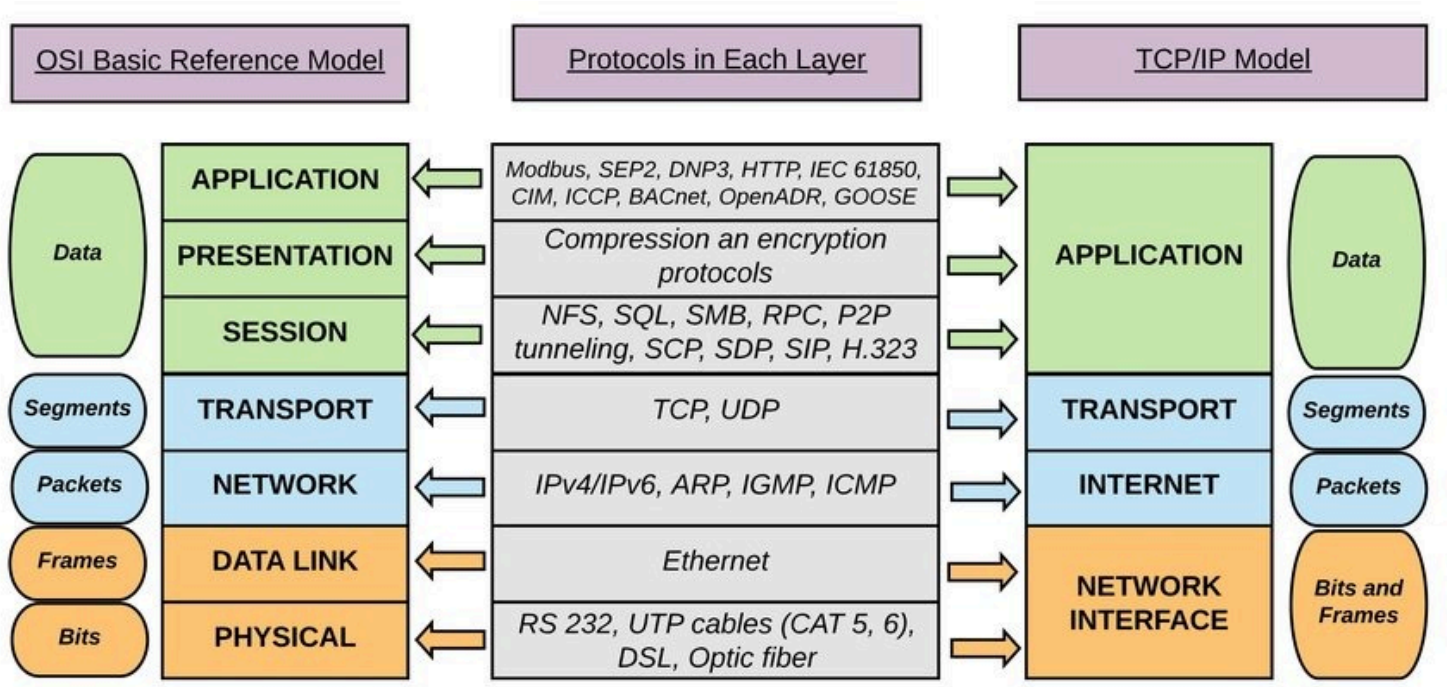
- Start with the quickest step first
- Follow the cookie crumbs (start where the problem occurred and work from there (like start at the first instance of an error message in a log)
- It’s important to prioritize right when managing the IT of a company.
    - Time-sensitive issues

Course #2: The Bits and Bytes of Computer Networking

An IP points only to a network, and a MAC Address points to a device/ host.
An IP Address is a 32-bit number, aka 4 octets, aka a number between 1 and 2^{32} (4,294,967,296)
BUT it ain't as simple as between 1 and 2^{32} because of IP classes. Class A is the biggest which can have an 8-bit network id (like a number between 1 and 256) and a host id of 24 bits.

TCP/IP Five-Layer Network Protocol

Transmission Control Protocol/ Internet Protocol



- Copper & Fiber are the two main materials for network cables.
- Cables

The physical layer consists of devices and means of transmitting **bits** across computer networks.

UTP, STP, and FTP Ethernet cables

Twisted pair Ethernet cable uses four pairs of color-coded copper wires. Each colored pair, one solid and one striped, are twisted together. There are multiple types of twisted pair Ethernet cables available on the market. These types fall into three main categories:

- **Unshielded twisted pair (UTP)** - The most common and least expensive type of Ethernet cable found in business and home networks. UTP cables offer very basic protection against EMI, RFI, and crosstalk interference.
- **Shielded twisted pair (STP)** - Used in environments where electromagnetic interference (EMI), radio frequency interference (RFI), and crosstalk with nearby cables have been identified as a problem for network communications. An STP cable uses a braided aluminum and/or copper shielding to encase the four twisted pairs underneath the outer jacket.
- **Foiled twisted pair (FTP)** - Also used in environments where EMI, RFI, and crosstalk are a problem. An FTP cable uses a thin foil shield that wraps around the bundle of twisted pair wires underneath the outer jacket.

Straight-through cable

Straight-through cables are also known as patch cables. They are the primary type of Ethernet cable used in computer networks. Straight-through cables normally connect computers and routers to hubs and Ethernet switches. Ethernet cable can also connect servers to Ethernet switches.

Straight-through cables can be identified by comparing both ends of the cable with one another. The cable is a straight-through cable if the color and stripe order of the twisted pairs are in the same position on both ends of the cable. For example, in the image of the straight-through cable above, the orange-striped wire appears in pin position 1 at both ends of the cable. This one-to-one pattern is continued for each color in pin positions 2-8. Ethernet cables that use 100Base-T standards (common for home networks) do not use the blue and brown cables. Networks using gigabit Ethernet have the option to use the blue and brown cables for Power over Ethernet (PoE).

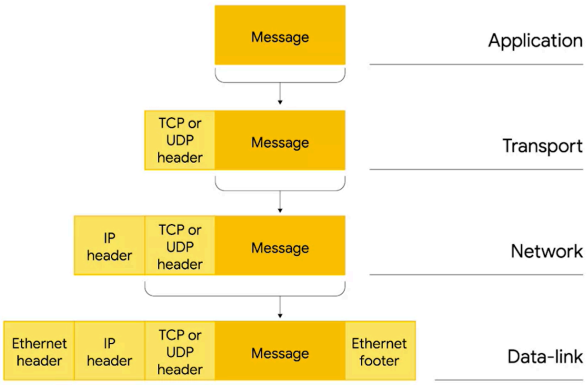
Straight-through cable key:

- Computers and routers use:
- Pins 1 & 2 - Orange wires for sending data
- Pins 3 & 6 - Green wires for receiving data
- Hubs and switches use:
    - Pins 1 & 2 - Green wires for sending data
    - Pins 3 & 6 - Orange wires for receiving data

- Crossover cables are used to connect two computing devices directly to one another. As an IT Support specialist, you might use a short crossover cable to connect an IT administrator laptop directly to an Enterprise machine (e.g., server, switch, router, hub, etc.). This type of connection is normally used to update, repair, and perform other administrative tasks on the Enterprise machine.

Cabling Tools:

- You can use a crimper to connect wires
- Wifi Analyzer measures wifi power and stability
- Use a toner probe to “find ethernet and internet connectors”
- Use a punch down tool to “connect wires to panels and jacks”
- The loopback plug “tests ports”
- You can use a network tap to copy traffic information that can be used to monitor devices.
- A cable stripper removes the protective coating from wires
- You can use a cable tester to measure integrity for standards compliance.

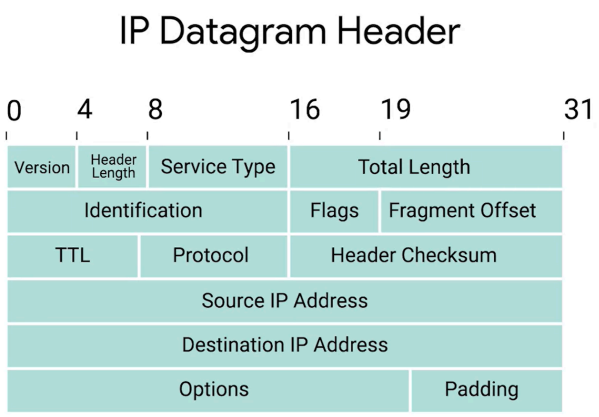


Encapsulation:

An Ethernet frame, is usually limited in size to 1,518 bytes

Address classes give us a way to break the total global IP space into discrete networks.

An IP address has 4 octets (1.2.3.4). No number should ever exceed 255 because an octet in binary is 2^8 and thus can't count past 255 (including 0).



Let's explore what you can discover by running a real IP address through an IP Lookup website like [this one](#).

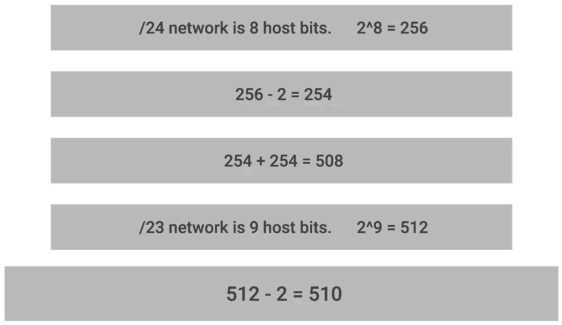
There are a handful of practical reasons people use IP Lookup, even with its limitations:

- Law enforcement and fraud investigators use online tools to see what ISP is hosting a spammer.
- Blacklist databases use it to find spammers or other violators and block their access to email servers.
- Retailers often use IP Lookup to make sure someone charging thousands of dollars is at the mailing address linked to the card...and not actually overseas with a stolen credit account.
- You can use it to verify that someone who tells you in an email that they're across town isn't really in an abandoned warehouse in another country.

A Subnet ID is how to break a big network into chunks. Instead of your IP being made up of a network and host ID, it's a network, subnet, then host ID.
A subnet mask is a bunch of 1s that define what to ignore when identifying a host address. The 0s in a subnet mask distinguish the bits reserved for a host address. Picture below:

Subnet masks and IP address

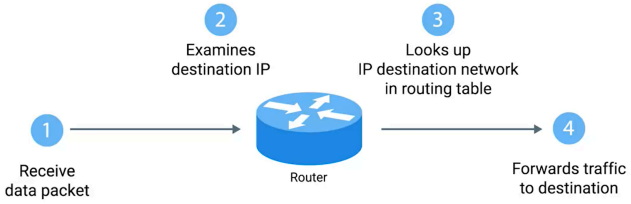
Class		Mask short name	Max Hosts
A	255.0.0.0 11111111.00000000.00000000.00000000	/8	16,777,214
B	255.255.0.0 11111111.11111111.00000000.00000000	/16	65,534
C	255.255.255.0 11111111.11111111.11111111.00000000	/24	254
	255.255.240.0 11111111.11111111.11110000.00000000	/20	4,094
	255.255.255.224 11111111.11111111.11111111.11100000	/27	30
	255.255.255.252 11111111.11111111.11111111.11111100	/30	2



Classless Inter-Domain Routing (CIDR) (Above right)

This figure talks about how many hosts you can get with different CIDR configurations. Whereas the Address Classes for IPs could only give you a network of 254, 65 thousand or 16 million hosts, CIDR allows networks to simply remove a 1 from the subnet mask to allow for twice as many potential hosts.
Note that there are almost always 2 hosts that are meant to be unused when designing a network. So instead of building the max 256 hosts on a class C network, you'd realistically only be able to have 254.

Basic routing:



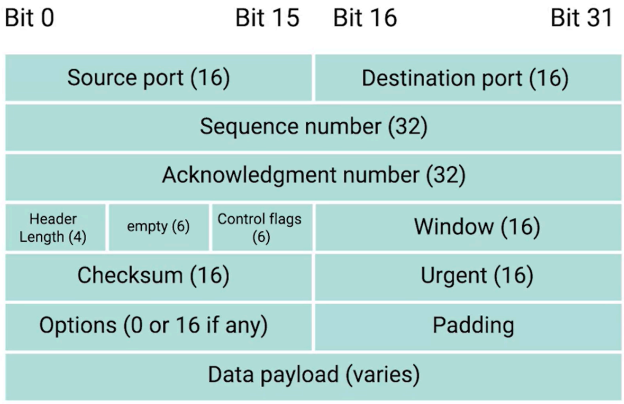
ARP = Address Resolution Protocol

Basic Routing Tables have 4 columns

https://www.coursera.org/learn/computer-networking/lecture/BVuUA/routing-tables
(Definitions here ^^^)

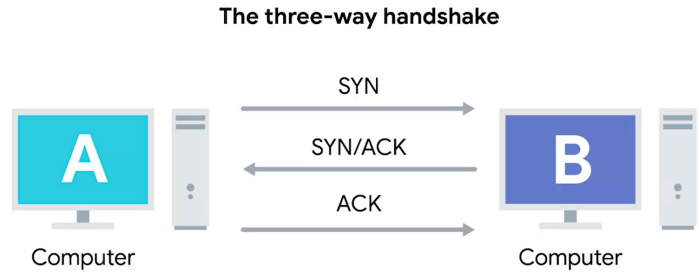
Destination Network	Next Hop	Total Hops	Interface

Dissection of a TCP Segment (below)

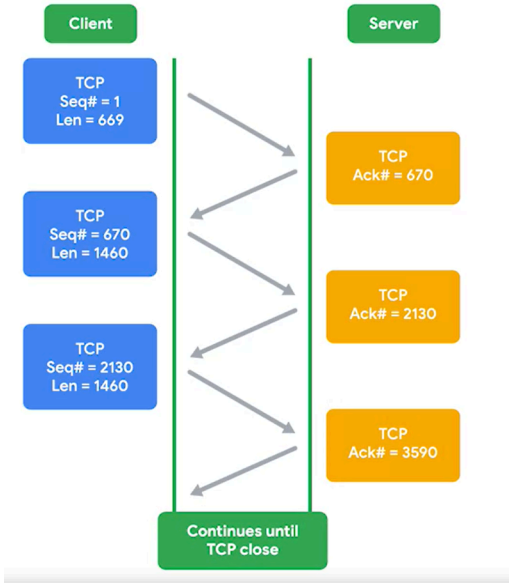


20 Bytes

The SYN and ACK are **control flags** that establish a

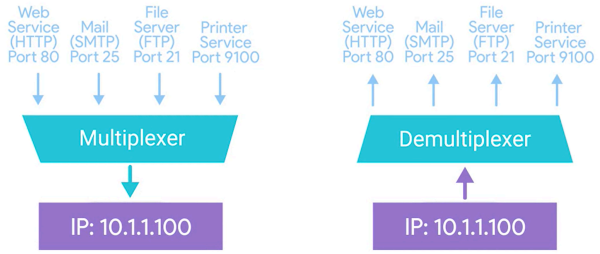


connection before data transfer. (Above)



← In TCP the server is constantly acknowledging that it's about to receive some data.

The four-way handshake is how computers close the connection, though it technically is possible to continue transfer in simplex form if one computer sends a FIN flag that isn't reciprocated.



Non-routable IP Addresses:

- 10.0. 0.0/8 (Range: 10.0. 0.0 – 10.255. 255.255) – Available IPs: 16,777,214.
- 172.16. 0.0/12 (Range: 172.16. 0.0 – 172.31. 255.255) – Available IPs: 1,048,574.
- 192.168. 0.0/16 (Range: 192.168. 0.0 – 192.168. 255.255) – Available IPs: 65,534.

Socket States

Client-side	Both-sides	Server-side

		LISTEN
SYN_SENT		SYN_RECEIVED
	ESTABLISHED	
	FIN_WAIT	
	CLOSE_WAIT	
	CLOSED	

System Ports versus Ephemeral Ports

Network services are run by listening to specific ports for incoming data requests. A port is a 16-bit number used to direct traffic to a service running on a networked computer. A "service" (or "server") is a program waiting to be asked for data. A "client" is another program that requests this data from the other end of a network connection. This reading explains how the Transmission Control Protocol (TCP) uses ports and sockets to establish a network connection and deliver data between services and clients.

System Ports stay the same (ports 1-1023) and identify a specific thing.

Ephemeral Ports are temporary. (ports 49152 through 65535) They can change numbers, turn on and off, etc.

The ones in between those ports are **User Ports**

TCP ports and sockets

Ports are used in the Transport Layer of the TCP/IP Five-Layer Network Model. At this layer, the TCP is used to establish a network connection and deliver data. A TCP "segment" is the code that specifies ports used to establish a network connection. It does this on the service side of the connection by telling a specific service to listen for data requests coming into a specific port. Once a TPC segment tells a service to listen for requests through a port, that listening port becomes a "socket." In other words, a socket is an active port used by a service. Once a socket is activated, a client can send and receive data through it.

Three categories of ports

Since a 16-bit number identifies ports, there can be 65,535 of them. Given the number of ports available, they have been divided into three categories by the Internet Assigned Numbers Authority (IANA): System Ports, User Ports, and Ephemeral Ports.

- **System Ports** are identified as ports 1 through 1023. System ports are reserved for common applications like FTP (port 21) and Telnet over TLS/SSL (port 992). Many still are not assigned. Note: Modern operating systems do not use system ports for outbound traffic.
- **User Ports** are identified as ports 1024 through 49151. Vendors register user ports for their specific server applications. The IANA has officially registered some but not all of them.
- **Ephemeral Ports (Dynamic or Private Ports)** are identified as ports 49152 through 65535. Ephemeral ports are used as temporary ports for private transfers. Only clients use ephemeral ports.

Not all operating systems follow the port recommendations of the IANA, but the IANA registry of assigned port numbers is the most reliable for determining how a specific port is being used. You can access the IANA Service Name and Transport Protocol Port Number Registry here or check out this helpful list of commonly used ports.

How TCP is used to ensure data integrity

The TCP segment that specifies which ports are connected for a network data transfer also carries other information about the data being transferred (along with the requested data). Specifically, the TCP protocol sends acknowledgments between the service and client to show that sent data was received. Then, it uses checksum verification to confirm that the received data matches what was sent.

Port security

Ports allow services to send data to your computer but can also send malware into a client program. Malicious actors might also use port scanning to search for open and unsecure ports or to find weak points in your network security. To protect your network, you should use a firewall to secure your ports and only open sockets as needed.

Key takeaways

Network services are run by listening to specific ports for incoming data requests.

- Ports are represented by a single 16-bit number (65535 different port ids)
- Ports are split up by the IANA (Internet Assigned Numbers Authority) into three categories: System Ports (ports 1-1023), User Ports (ports 1024-49151), and Ephemeral (Dynamic) Ports (ports 59152-65535).
- A socket is a port that a TCP segment has activated to listen for data requests.
- Ports allow services to send data to your computer but can also send malware into a client program. It's important to secure your ports.

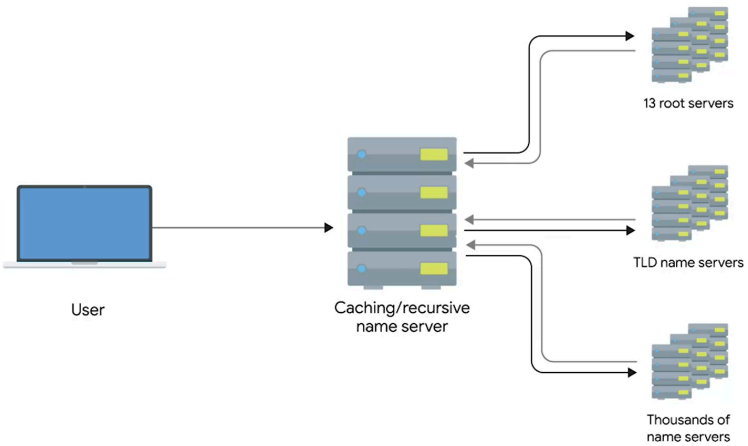
The most common Web Servers are Microsoft IIS, Apache, and nginx.

While there are bajillions of different applications that can operate on the “Application Layer,” different applications need to use their respective standardized protocol (like HTML for web browsers & servers) if they want to interact with other instances of the application.

the IP address, subnet mask, and gateway for a host must be specifically configured, a DNS server, is the fourth and final part of the standard modern network configuration. These are almost always the four things that must be configured for a host to operate on a network in an expected way.

There are five primary types of DNS servers:

1: Caching name servers
2: Recursive name servers
3: Root name servers
4: TLD name servers
5: Authoritative name servers



Port Forwarding seems like an amazing security measure to completely masquerade the IP of something like a web server which would automatically receive all traffic with a destination port of 80 or 443.

Non-routable Address space is space that will NEVER get traffic from the internet. Therefore, if your router has NAT set up, you can use one single IP address for all your internet traffic and then let up to thousands of hosts within your network to use non-routable address space with no problem! A very clever way to take advantage of the remaining of the 4.2 billion possible IPv4 addresses

USENET was invented by Duke Graduate Students to transmit info across phone lines for computers.

Broadband Protocols

Broadband communications require a set of instructions, rules, and communication to various network layer protocols to support operation. Point to Point Protocol (PPP) for broadband communications is a set of instructions used to transmit data between two directly connected devices. This reading will cover the definitions, structures, and details of Point to Point Protocol (PPP) and Point to Point Protocol over Ethernet (PPPoE).

Point to Point Protocol (PPP)

Point to Protocol (PPP) is a byte-oriented protocol broadly used for high-traffic data transmissions. PPP functions at the data link layer, which transmits data between two devices on the same network. PPP is designed to link devices, so the endpoints do not need to be the same vendor to work.

Configuring PPP

When configuring PPP for the devices on your network, you have the following options:

- **Multilink** connection provides a method for spreading traffic across multiple distinct PPP connections.
- **Compression** increases throughput by reducing the amount of data in the frame.
- **Authentication** occurs when connected devices exchange authentication messages using one of two methods:
    - **Password Authentication Protocol (PAP)** is a password authentication option that is hard to obtain plaintext from if passwords are compromised.
    - **Challenge Handshake Authentication Protocol (CHAP)** is a three-way handshake authentication that periodically confirms the identity of the clients.
- **Error detection** includes Frame Check Sequence (FCS) and looped link detection.
    - **Frame Check Sequence (FCS)** is a number included in the frame calculated over the Address, Control, Protocol, Information, and Padding fields used to determine if there has been data loss during transmission.
    - **Looped link detection** in PPP detects looped links using magic numbers. A magic number is generated randomly at each end of the connection, so when a looped message is received, the device checks the magic number against its own. If the line is looped, the number will match the sender's magic number, and the frame is discarded.

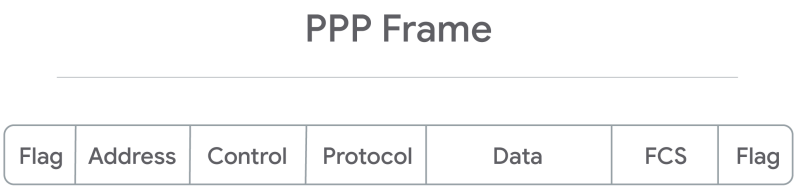
Sub-protocols for PPP

In addition, two sub-protocols for PPP occur on the network layer when the network decides what physical path the information will take. These protocols use the configuration options you set for the endpoints.

- **Network Control Protocol (NCP)** will be used to negotiate optional configuration parameters and facilities for the network layer. There is an NCP for each higher layer protocol used by the PPP.
- **Link Control Protocol (LCP)** initiates and terminates connections automatically for hosts. It automatically configures the interfaces at each end like magic numbers and selecting for optional authentication.

Data is sent using PPP in a frame. A frame is a collection of data sent to a receiving point.

PPP uses the following frame format:



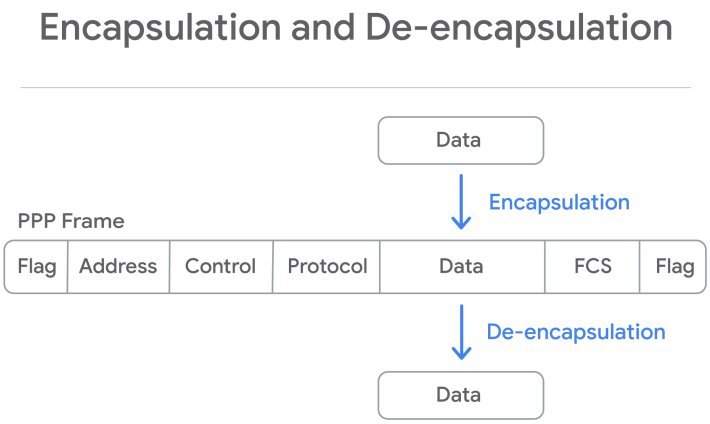
- **Flag** is a single byte and lets the receiver know this is the beginning of the frame. Depending on the encapsulation, there may or may not be a start flag or an end flag.
- **Address** is a single byte, and it contains the broadcast address.
- **Control** is a single byte required for various purposes but also allows a connectionless data link.
- **Protocol** varies from one to three bytes which identify the network protocol of the datagram.
- **Data** is where the information you need to transmit is stored and has a limit of 1500 bytes per frame.
- **Frame check sequence (FCS)** is 2 or 4 bytes and is used to verify data is intact upon receipt at the endpoint.

When the data is packaged in a frame, it undergoes encapsulation.

Encapsulation

Encapsulation is the process by which each layer takes data from the previous layer and adds headers and trailers for the next layer to interpret.

These frames are sent to the other endpoint where the process is reversed, which is called De-encapsulation.



PPP can get expensive and hard to manage due to all the direct cables and links required. In this case, you may want to switch to a multi-access Ethernet solution. Point to Point Protocol over Ethernet is a protocol made to bridge the gap between directly connected endpoints and other devices.

Point to Point Protocol over Ethernet (PPPoE)

Point to Point protocol over Ethernet (PPPoE) is a way of encapsulating PPP frames inside an ethernet frame. PPPoE is a solution for tunneling packets over the DSL connection service provider's IP network and from there to the rest of the Internet. Like PPP, PPPoE provides authentication, encryption, and compression, though it primarily uses Password Authentication Protocol (PAP) for authentication.

A common use case is PPPoE using DSL services where a PPPoE modem-router connects to the DSL service or when a PPPoE DSL modem is connected to a PPPoE-only router using an Ethernet cable.

PPP is strictly point-to-point, so frames can only go to the intended destination. PPPoE requires a new step because ethernet connections are multi-access enabled (every node connects to another). This requires an additional step called the discovery stage. The discovery stage establishes a session ID to identify the hardware address. This stage ensures data gets routed to the correct place.

PPPoE is an encapsulation of PPP inside an ethernet frame. PPPoE retains the same architecture, configuration options, and frame data as PPP but with one extra layer of ethernet encapsulation.

Key takeaways

Broadband internet requires several protocols to make sure different connected devices can communicate with each other.

- Point to Point Protocol (PPP) encapsulates data, so any PPP configured devices can communicate without issue.
- Point to Point over Ethernet (PPPoE) is an extra layer of encapsulation for standard PPP frames, to enable data to be sent over ethernet connections.

Wan Protocols V2

In this reading, you will continue learning about the various components of Wide Area Networks (WANs). WAN configurations are important for IT Support professionals to understand when working with the geographically dispersed networks of large organizations. WANs can be connected through the Internet with connections provided by Internet Service Providers (ISPs) in each locale. Regional WANs can also be formed by connecting multiple Local Area Network (LAN) sites using equipment and cables leased from a regional ISP. Security for WANs across the public Internet can be configured through Virtual Private Networks (VPNs).

Physical versus software-based WANs

- **WAN router:** Hardware devices that act as intermediate systems to route data amongst the LAN member groups of a WAN (also called WAN endpoints) using a private connection. WAN routers may also be called border routers or edge routers. These routers facilitate an organization's access to a carrier network. WAN routers have a digital modem interface for the WAN, which works at the OSI link layer, and an Ethernet interface for the LAN.
- **Software-Defined WAN (SD-WAN):** Software developed to address the unique needs of cloud-based WAN environments. SD-WANs can be used alone or in conjunction with a traditional WAN. SD-WANs simplify how WANs are implemented, managed, and maintained. An organization's overall cost to operate a cloud-based SD-WAN is significantly less than the overall cost of equipping and maintaining a traditional WAN. One of the ways that SD-WANs help reduce operational costs is by replacing the need for expensive lines leased from an ISP by linking regional LANs together to build a WAN.

WAN optimization

There are multiple techniques available to optimize network traffic and data storage on a WAN:

- **Compression:** Reducing file sizes to improve network traffic efficiency. There are many compression algorithms available for text, image, video, etc. The sender and the receiver will need apps that offer the same compression/decompression algorithm to encode and decode the compressed files.
- **Deduplication:** Prevents files from being stored multiple times within a network to avoid wasting expensive hard drive space. One copy of the file is kept in a central location. All other "copies" are actually file pointers to the single copy of the file. This saves valuable hard drive space, makes performing data backups more efficient, and reduces the amount of time needed to recover from data loss disasters.
- **Protocol Optimization:** Improves the efficiency of networking protocols for applications that need higher bandwidth and low latency.
- **Local Caching:** Storing local copies of network and internet files on a user's computer to reduce the need to resend the same information across the network every time the file is accessed. Some WAN optimization products can cache shared files at one physical LAN location when groups of employees at the location tend to request the same set of files frequently. **Traffic Shaping:** Optimizing network performance by controlling the flow of network traffic. Three techniques are commonly used in traffic shaping:
    - **bandwidth throttling -** controlling network traffic volume during peak use times
    - **rate limiting** - capping maximum data rates/speeds
    - **use of complex algorithms** - classifying and prioritizing data to give preference to more important traffic (e.g., an organization might want to prioritize private LAN-to-LAN traffic within the organization's WAN and give a lower priority to employees accessing the public Internet).

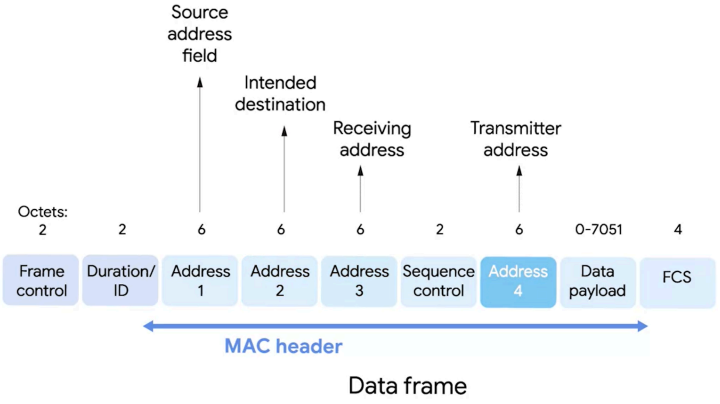
WAN Protocols

WAN Internet Protocols are used in conjunction with WAN routers to perform the task of distinguishing between a private LAN and the related public WAN. Several WAN protocols have been developed over the decades for this task, as well as other purposes, including:

- **Packet switching:** A method of data transmission. In packet switching, messages are broken into multiple packets. Each packet contains a header that includes information on how to reassemble the packets, as well as the intended destination of the packets. As a measure to prevent data corruption, the packets are triplicated. The triplicated packets are sent separately over optimal routes through the

internet. Then, once the packets reach their destination, they are reassembled. The triplicate copies are compared with one another to detect and correct any data corruption that occurred during transmission (at least two of the three copies should match). If the data cannot be reassembled and/or data corruption is evident in all three copies, the destination will make a request to the origin to resend the packet.

- **Frame relay:** Also a method of data transmission. Frame relay is an older technology originally designed for use on Integrated Services Digital Network (ISDN) lines. However, the technology is now used in other network interfaces. Frame relays are used to transmit data between endpoints of a WAN through a packet switching method that works at the OSI data link and physical layers. A fast data communications network, called a Frame Relay Network, is used to transport data packets in frames. The reliability of Frame Relay Networks minimizes the need for error checking. The frames include routing address information for the destination.
    - Permanent Virtual Circuits (PVCs) - Used for long-term data connections. Stays open even when data is not being transmitted.
    - Switched Virtual Circuits (SVCs) - Used in temporary session connections for sporadic communications.
- **Asynchronous Transfer Mode (ATM):** ATM is an older technology that encodes data using asynchronous time-division multiplexing. The encoded data is packaged into small, fixed-sized cells. ATM can send the cells over a long distance, which makes it useful for WAN communications. ATMs uses routers as end-points between ATM networks and other networks. ATM technology has been replaced for the most part by Internet Protocol (IP) technologies.
- **High Level Data Control (HLDC):** An encapsulation or data link protocol that delivers data frames through a network. The frames include multiple fields that can hold information about start and end flags, controls, Frame Check Sequence (FCS), and protocol used. HLDC was developed to use multiple protocols to replace Synchronous Data Link Control (SLDC), which used only one protocol. HDLC includes error correction, flow control, and data transmission through polling. HDLC has three modes to define the relationship between two devices, or nodes, during communications:



    - Normal Response Mode (NRM) - Primary node must give permission to the secondary node to transmit.
    - Asynchronous Response Mode (ARM) - Primary node allows the secondary node to initiate communication.
    - Asynchronous Balanced Mode (ABM) - Both nodes can act as either the primary or secondary nodes. They can each initiate communications without permission.
- **Packet over Synchronous Optical Network (SONET) or Synchronous Digital Hierarchy (SDH):** A communication protocol used for WAN transport. The SONET or SDH communication protocols define how point-to-point links communicate over fiber optics cables.
- **Multiprotocol Label Switching (MPLS):** A technique for optimizing network routing. MPLS replaces inefficient table lookups for long network addresses with short path labels. These labels direct data from node to node.

Data frame for a WLAN frame Pictured Above

Wi-Fi 6

Wi-Fi 6, formerly known as 802.11ax, is one of the largest leaps in Wi-Fi technology since its introduction. This reading will introduce you to the benefits and technology used in Wi-Fi 6.

Benefits of Wi-Fi 6

The Wi-Fi 6 network protocol is faster and more efficient for networks with a larger number of connected devices.

Key benefits of Wi-Fi 6 technology include:

- **Higher data rates:** Band splitting or increased client group sizes allow for uploading and downloading greater amounts of data.
- **Increased band capacity:** Band utilization increased from 80mHz to 160mHz, creating a faster connection from the router to connected devices.
- **Better performance**: The input/output streams are doubled from the 4 by 4 allowed by Wi-Fi 5, to 8 by 8 in Wi-Fi 6, allowing more clients to be grouped.
- **Improved power efficiency**: Devices only connect to the network when sending or receiving data, increasing battery life.

Capabilities of Wi-Fi 6

Wi-Fi 6 technology improves functionality and connectivity.

- **Channel sharing** for better efficiency and shortens the time it takes to send data once a user gives the send command.
- **Target Wake Time (TWT)** improves the network speed and increases battery life by allowing battery-powered devices to sleep when not in use.
- **Multi-user MIMO (Multiple Input, Multiple Output)** wireless technology allows more data to be transferred simultaneously. This ability increases capacity and efficiency in high bandwidth applications like voice calls or video streaming.
- **160 MHz channel utilization** gives more space for transmitting data and increases bandwidth capability.
- **1024 Quadrature amplitude modulation** combines two signals into a single channel, so more data is encoded.
- **Orthogonal Frequency Division Multiple Access (OFDMA)** allows for bandwidth splitting, which is assigned dynamically by the access point to separate devices.
- **Transmit beamforming** is a technique that sends signals that allow for more efficient higher data rates by targeting each connected device.

Wi-Fi 6E extends Wi-Fi 6 into 6 GHz

Wi-Fi 6E is an additional certification for Wi-Fi 6 that has all of the features of Wi-Fi 6 but adds a third 6 GHz band. Wi-Fi 6E has more channels to use to broadcast, including 14 more 80MHz channels and seven more 160MHz channels. The additional channels allow networks with Wi-Fi 6E for better performance even when streaming high-definition video or using virtual reality devices.

Key takeaways

- Wi-Fi technology will continue to change as the needs of companies and users change. Wi-Fi 6 improves the quality of networks with faster speeds and energy-saving technology.
- Wi-Fi 6 uses technologies like channel sharing, Target Wake Time, Multi-user MIMO, channel utilization, amplitude modulation, OFDMA, and transmit beamforming to increase the quality of a Wi-Fi network.
- Wi-Fi 6E is an additional certification of Wi-Fi 6 that has even faster speeds and stronger performance.

Resource for more information

For more information about Wi-Fi 6, read this article by the Wi-Fi Alliance: Wi-Fi CERTIFIED 6.

Alphabet Soup: Wi-Fi Standards

As an IT Support specialist, you may be responsible for supporting wireless technologies. In this reading, you will learn about the 802.11 Wireless-Fidelity (Wi-Fi) standards, including the alphabet-coded updates: a, b, g, n, ac, ad, af, ah, ax, ay, and az. You will also learn about the differences between the 2.4 gigahertz (GHz) and 5 GHz Wi-Fi frequencies.

You may already be familiar with selecting from the 2.4 GHz and 5 GHz frequency options on your home Wi-Fi router. Perhaps you also noticed the 802.11 specifications on the packaging for your Wi-Fi router when you purchased it. Have you wondered what these numbers and letters mean?

Wi-Fi 2.4 GHz and 5 GHz frequencies

There are multiple wireless technologies available today that use various frequencies ranging from radio to microwave bands. These wireless technologies include Wi-Fi, Z-Wave, ZigBee, Thread, Bluetooth, and Near Field Communication (NFC). Radio and microwave frequency bands each have specific ranges that are divided into channels. Wi-Fi uses the 2.4 GHz and 5 GHz microwave radio frequency band ranges for sending and receiving data. Some Wi-Fi routers use multiple channels within each range to avoid signal interference and to load-balance network traffic. Wi-Fi is commonly used for wireless local area networks (WLANs).

The following is a comparison of the performance characteristics between the 2.4 GHz and 5 GHz frequency bands:

2.4 GHz

- Advantages:
  - Has the longest signal range from 150 feet (45 meters) indoors to 300 feet (92 meters) outdoors.
  - Can pass through walls and other solid objects.
- Disadvantages:
  - The long signal range also increases the chances of Wi-Fi traffic being intercepted by cybercriminals.
  - Includes a limited number of channels. Can range from 11 to 14 channels, depending on regulations in the country of use.
  - Can experience network traffic congestion and interference with other Wi-Fi networks and wireless technologies, such as BlueTooth, that overlap the 2.4 GHz frequency bands.
  - Microwave ovens also work in the 2.4 GHz frequency band and can cause Wi-Fi interference.
  - Under specific conditions, the maximum achievable data rate is 600 Mbps.

5 GHz

- Advantages:
  - Includes significantly more channels than 2.4 GHz.
  - Experiences fewer interference problems and less wireless network traffic congestion than 2.4 GHz.
  - Can achieve over 2 Gbps data transfer speeds under specific conditions.
- Disadvantages:
  - The wireless range is limited to 50 feet (12 meters) indoors and 100 feet (30 meters) outdoors.
  - Does not penetrate walls and other solid objects as well as 2.4 GHz.

IEEE 802.11 standards

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) ratified the first 802.11 standard for wireless fidelity (later branded as Wi-Fi). The standard was first published for use by computer device manufacturers to use as a common protocol for wireless communications. The IEEE has amended the 802.11 specifications multiple times over the years with updates and additional enhancements to 802.11 Wi-Fi. The IEEE names each new amendment with one or two letters appended to 802.11 (e.g., 802.11n or 802.11ax). The IEEE plans to continue updating the 802.11 specifications until a new technology replaces Wi-Fi.

The majority of wireless networks use the IEEE 802.11 standards for Wi-Fi. Wi-Fi networks include client devices (e.g., laptops, tablets, smartphones, IoT devices, etc.) that are configured to connect to wireless access points. This configuration is referred to as “infrastructure mode”. Access points can serve both wireless and wired network traffic. For wired traffic, the access point works as a bridge between wireless devices and a wired network. The access point connects to an Ethernet switch through a wired Ethernet cable.

The various amended 802.11 specifications use the same fundamental data link protocol. However, some characteristics may vary at the OSI physical layer, including:

- signal ranges
- modulation techniques

- transmission bit rates
- frequency bands
- channels

Note that countries around the world may impose different regulations on channel usage, power limitations, and Wi-Fi ranges. A technology called dynamic frequency selection (DFS) is also required to prevent 5 GHz Wi-Fi signals from interfering with local radar and satellite communications.

A comparison of the frequencies, maximum data rates, and maximum signal ranges for each 802.11 update over the years is detailed below:

Year Ratified	IEEE 802.11 Standard	Marketing Name	Frequency	Maximum Range Indoors - Outdoors	Maximum Data Rate
1997	-	Wi-Fi 0	2.4 GHz	20-100 meters	2 Mbps
1999	a	Wi-Fi 2	5 GHz	35-120 meters	54 Mbps
1999	b	Wi-Fi 1	2.4 GHz	40-140 meters	11 Mbps
2003	g	Wi-Fi 3	2.4 GHz	40-140 meters	54 Mbps
2009	n	Wi-Fi 4	2.4 & 5 GHz	70-250 meters	600 Mbps
2015	ac wave 2	Wi-Fi 5	5 GHz	80-120 meters	6.9 Gbps
2019	ax	Wi-Fi 6	2.4 & 5 GHz	50-300 meters	10 Gbps
2021	ax	Wi-Fi 6e	6 GHz	Varies	10 Gbps
2024	be	Wi-Fi 7	6 GHz	TBD	46 Gbps

IEEE 802.11 major updates list:

- **802.11a (1999) - Wi-Fi 2**
  - Designed for 5 GHz frequency band only
  - Offered a maximum data rate of 54 Mbps
  - Offered a maximum signal range of 400 feet (120 m)
  - Defined 23 non-overlapping channels at 20 MHz wide
- **802.11b (1999) - Wi-Fi 1**
  - Designed for 2.4 GHz frequency band only
  - Offered a maximum data rate of 11 Mbps
  - Offered a maximum signal range of 450 feet (140 m)
  - Defined 14 overlapping channels (frequent cause of interference)
- **802.11g (2003) update to 802.11b - Wi-Fi 3**
  - Improved 2.4 GHz frequency band only
  - Increased the maximum data rate to 54 Mbps
- **802.11n (2009) bandwidth increase - Wi-Fi 4**
  - Improved both 2.4 GHz and 5 GHz frequency bands
  - Access points could offer “dual-band” support with each band implemented by a separate radio.
  - Increased bandwidth and reliability with “multiple input multiple output" (MIMO) technology.
  - Allowed “channel bonding” for 5 GHz (two adjacent channels could be combined).
  - Increased the maximum data rate to 72 Mbps per stream and 150 Mbps per stream for bonded channels. With specific configurations, the maximum data rate could be as high as 600 Mbps.
  - Increased maximum signal range of 825 feet (250 m)
- **802.11ac (2014) and Wave 2 (2015) bandwidth increases - Wi-Fi 5**
  - Improved the 5 GHz frequency band only, though access points could still offer dual band support for older 2.4 GHz specifications.
  - Access points could offer triband support (one 2.4 GHz and two 5 GHz radios).
  - Supported wider bonded channels at 80 and 160 MHz.
  - Allowed up to eight streams with each 80 MHz channel.
  - Increased maximum data rates to 1 Gbps and could be as high as 2.2 Gbps for specific configurations. Wave 2 increased the maximum data rate to 6.9 Gbps.
  - Increased sent data transmissions to up to 4 clients at the same time. This was achieved by allowing access points to use multiple antennas through downlink multiuser MIMO (DL MU-MIMO) technology.
- **802.11ax (2019) bandwidth increases - Wi-Fi 6**
  - Improved data stream rates to 600 Mbps per 80 MHz channel, with combined data rates of over 1 Gbps for the 2.4 GHz frequency and 4.8 Gbps for the 5 GHz frequency.
  - Increased sent data transmissions to up to 8 clients at the same time with downlink MU-MIMO.
  - Added support for full-duplex MU-MIMO to receive uplink data from multiple client devices.
  - Added support for “orthogonal frequency division multiple access” (OFDMA), which works with MU-MIMO to sustain high data rates during periods of high client device traffic.
  - Requires all client devices to use WPA3 security protocols.
- **Wi-Fi 6e (2020) bandwidth increases**
  - Added support for a new 6 GHz frequency band, which has a combined maximum data rate speed of 10 Gbps (shared by multiple devices).
  - Added new channels to reduce interference.
  - Improved frequency space for 80 and 160 MHz channels.

For more information about Wi-Fi standards, please visit:

- Official IEEE 802.11 Working Group Project Timelines - An IEEE published table detailing each update to the 802.11 standards.

IoT Data Transfer Protocols

In this reading, you will learn how Internet of Things (IoT) devices send and receive data across networks. As an IT Support specialist, you may need to support data collection from IoT devices. For example, you may work for a company that uses an array of IoT sensors in a manufacturing setting to help with the remote monitoring and proactive maintenance of industrial machines. You may need to manage the software applications and data transfer protocols that support automated and human interaction with the IoT devices and the data they collect.

Data protocol models used with IoT

There are two common data protocol models to illustrate how low-power IoT devices share data:

- **Request/Response model:** Often used in distributed systems where the communication flow between servers and clients consists of requests and responses for data. Examples include HTTP and CoAP (described in the “IoT data protocols at the application layer” section below)
- **Publish/Subscribe model:** A framework for message exchanges between publishers (hosts) and subscribers (clients) that are routed through a broker. Subscribers can sign up to a channel to receive notices through the broker when the publisher releases new messages. Examples: MQTT and AMQP (described in the “IoT data protocols at the application layer” section below).

IoT data protocols at the application layer

IoT devices can collect environmental data around their physical location (e.g., temperature), equipment data (e.g., maintenance status), and metered data (e.g., electricity usage). Data protocols are needed to transfer and format the data for use by applications that interface with either humans or automated systems. IoT devices can be configured to use various data transfer and formatting protocols at the OSI application/software layer of communication.

Most IoT devices can use at least one of the following data transfer protocols:

- **HyperText Transfer Protocol / Secure (HTTP/HTTPS):** HTTP and HTTPS are the most widely used information transfer protocols across the World Wide Web (WWW). The protocols define how information is formatted and transmitted. HTTP/HTTPS uses ASCII formatting, has a header size of 8 bytes, and is designed for transmitting documents. HTTP/HTTPS use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) for sending information across the internet. HTTP/HTTPS uses the request/response model. When a website address is entered into a browser, HTTP/HTTPS sends a request to the site’s web server, which then returns an HTTP/HTTPS formatted response to the browser. The protocols use ports 80 or 8080 and data security is provided on the HTTPS version of the protocol. HTTP is supported by Google Cloud IoT Core for device-to-cloud communication.
- **Machine-to-Machine (M2M) Communication Protocols:** A set of direct communication methods for low-power devices, machines, and systems. There are three primary architectural and protocol groups in M2M electronic communications:
    - **Representational State Transfer (REST):** An architectural style for communication amongst web accessible systems.
    - **Service-oriented Architectures (SOA):** An architecture for data exchanges in industrial automation systems.
    - **Message Oriented Protocols:** A protocol for asynchronous data transfers for distributed systems.
- **Message Queue Telemetry Transport (MQTT):** An IoT data-centric interaction protocol for M2M that uses a simple publish-subscribe model. MQTT supports Quality of Service (QoS), uses TCP for sending

information, and utilizes Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for security. MQTT using binary format and 2-byte header sizes for efficient messaging. MQTT is supported by Google Cloud IoT Core for device to cloud communication.

- **Constrained Application Protocol (CoAP):** A web transfer protocol for IoT constrained nodes and networks designed for M2M applications. CoAP is used for IoT applications like building automation and smart energy management. CoAP is very similar to HTTP: both are based on the REST model and both place resources on a server that is accessible to clients via a URL.
- **Advanced Message Queuing Protocol (AMQP):** An open standard for messaging amongst applications in different organizations and/or platforms. Its purpose is to remove vendor lock-in for app communication. In addition to interoperability, AMQP also offers reliability and security.
- **Extensible Messaging and Presence Protocol (XMPP):** A decentralized, open standard for chat, messaging, video and voice calls, collaboration tools, and more. Built upon Japper, XMPP offers a proven communication technology that is extensible, flexible, and diverse.
- **Data Distribution Service (DDS):** An API standard and middleware protocol from the Object Management Group. Middleware exists in the OSI applications layer, between software and the operating system. DDS uses the publish-subscribe communications model. DDS is also data-centric, provides low-latency data connectivity, and helps the devices in an IoT ecosystem share data more efficiently. DDS is reliable, scalable, and provides control of QoS parameters, including bandwidth and resource limits.

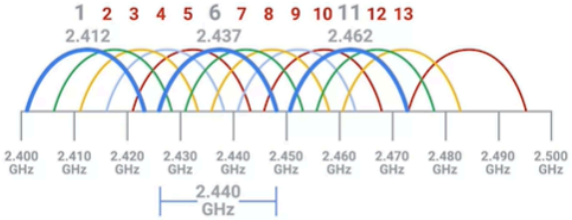


Illustration of Wireless Channels (left)

WPA3 Protocols & Encryption

Protocols and encryption are vital components in cybersecurity. Network security continues to evolve along with technological innovations and ever-increasing computing power. You have learned about WPA2 and how it improved the security of the Wi-Fi Protected Access (WPA) protocol. In this reading, you will explore WPA3, the third iteration of WPA wireless security. You will also learn about various internet connectivity technologies, as well as the basics of wireless and cellular networking.

WPA3 is built upon the WPA2 protocol and is intended to replace WPA2. The WPA3 protocol introduces new features and methods to repair the security weaknesses of WPA2. The benefits of this advancement in Wi-Fi security include:

- Simplified wireless security
- Stronger authentication
- Powerful encryption
- Stable business continuity
- Enhanced security methods
- Replacement for legacy protocols
- Protected Management Frames (PMF) requirement for enterprise networks

WPA3 offers two versions, a personal and an enterprise version.

WPA3-Personal

WPA3-Personal is intended for individual users and personal/home Wi-Fi networks. This protocol addresses common cybersecurity weaknesses that affect consumers' wireless devices. It also simplifies Wi-Fi security for users. The improvements to WPA3-Personal include:

- **Natural password selection:** Gives users the ability to set passwords that are easier for the user to remember.
- **Increased ease of use:** Users do not need to change the way they connect to Wi-Fi to benefit from WPA3's improved security.

- **Forward secrecy:** If a password is stolen, WPA3 can continue to protect data that is transmitted.
- **Simultaneous Authentication of Equals (SAE)**: WPA3-Personal improves upon the WPA2-Personal Pre-Shared Key (PSK) handshake protocol. SAE uses PSK to generate a Pairwise Master Key (PMK). The PMK uses password-based authentication and is shared between a Wi-Fi access point and a wireless device. The pair use a complex, multi-stage process for proving to one another that they each possess the PMK. This complex handshake makes it extremely difficult for cybercriminals to intercept packets in order to extract an identifiable authentication key. If the SAE transaction is successful, the wireless device will pass the authentication stage and gain access to the secured Wi-Fi network.

The SAE authentication also reduces the probability of successful dictionary and brute force attacks, in which cybercriminals try to crack short, weak, and commonly used passwords. Additionally, SAE corrects a weakness exploited by cybercriminals who could perform key reinstallation attacks (KRACKs) when in close proximity to a Wi-Fi user. This type of attack could decrypt data and expose passwords, credit card information, photos, chats, emails, and more.

WPA3-Enterprise

WPA3-Enterprise is intended for business networks with multiple users. This protocol addresses the WPA2-Enterprise weaknesses that cybercriminals have been able to exploit. In addition to the WPA3-Personal SAE improvements, the WPA3-Enterprise security improvements and options include:

- **Galois/Counter Mode Protocol (GCMP-256):** The Advanced Encryption Standard (AES) with GCMP-256-bit encryption replaces the WPA2 128-bit AES-Counter Mode Protocol (CCMP) Cipher Block Chaining Message Authentication Code (CBC-MAC). GCMP for data integrity. The GCMP-256-bit encryption strength takes significantly more computing power for cybercriminals to crack than 128-bit encryption. The average person would not have access to that level of computing power. GCMP-256-bit encryption provides a stronger security protocol and makes it harder for cybercriminals to perform Meddler-in-the-Middle attacks.
- **Opportunistic Wireless Encryption (OWE):** OWE improves upon the WPA2 wireless encryption standard of 802.1x Open Authentication and Extensible Authentication Protocol (EAP). In WPA2, EAP required additional support to help it encrypt and authenticate login credentials. In the WPA3 protocol, OWE replaces EAP with a solution that encrypts and authenticates all wireless traffic. It also replaces Wi-Fi passwords by assigning a unique key to each device that has permission to access the network. This technology repairs a weakness Wi-Fi users experience in open networks, which are often found in restaurants, coffee shops, hotels, airports, malls, and more.
- **Wi-Fi Device Provisioning Protocol (DPP):** DPP improves upon the WPA2 Wi-Fi Protected Setup (WPS) encryption technology between wireless devices and routers. WPA3's DPP uses QR codes or NFC tags to grant passwordless Wi-Fi access to wireless devices.
- **384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA):** HMAC creates hash code from a secret key. This hash code is sent with each message passed between a Wi-Fi access point and a user's device. The hash code from the origin of the message is compared to the hash code from the receiver of the message to determine if the hash codes match. A discrepancy between the two hashes would indicate that the message was compromised or corrupted during transmission.
- **Elliptic Curve Diffie-Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA):** In WPA3, key management and authentication use the ECDHE protocol and ECDSA encryption for faster performance. The protocol is supported by most browsers. This key management technology replaces the WPA2 4-way handshake.

Key takeaways

As the tech industry develops more powerful computers, cybercriminals will use them to crack older encryption standards. The need to create more complex encryption algorithms will always be present in order to stay ahead of the evolving tools used by cybercriminals.

For **WPA3-Personal**, some of the new features include:

- Natural password selection
- Increased ease of use
- Forward secrecy
- Simultaneous Authentication of Equals (SAE)

For **WPA3-Enterprise**, some of the new features include:

- Galois/Counter Mode Protocol (GCMP-256)
- Opportunistic Wireless Encryption (OWE)
- Wi-Fi Device Provisioning Protocol (DPP)
- 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)
- Elliptic Curve Diffie-Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA)

Wireless Network Protocols for IoT

In this reading, you will learn how Internet of Things (IoT) devices connect to wireless networks. As an IT Support specialist, you may need to support wireless IoT devices in a networked environment. For example, you may have a client who needs to install a smart, wireless security system for their home or office. The client might need assistance with connecting the security system to a private network for onsite monitoring and/or to the internet for remote monitoring. Understanding the properties of wireless IoT networks will help you select appropriate network protocols for various IoT applications.

IoT wireless network protocols at the physical layer

IoT devices can use both wired and wireless methods to connect to the Internet. For wireless connections, there are multiple network protocols that manufacturers configure IoT devices to use. Some of these network protocols support global internet connectivity, while others are intended for short-distance Personal Area Networks (PANs). Network protocols connect at the OSI physical layer.

Most IoT devices can use at least one of the following network protocols:

Wireless-Fidelity (Wi-Fi): Wi-Fi is the more familiar brand name for the IEEE 802.11 standard for wireless networks. Wi-Fi is the most common wireless protocol across the world, with billions of devices capable of using Wi-Fi, including many IoT devices. Wi-Fi is a great option when needing to integrate IoT devices into an existing IP network that is connected to the internet. Wi-Fi 6 can support up to 500 Mbps data transfer speeds, for fast performance with large amounts of data. IoT networks often include a hub or a control system that uses Wi-Fi to facilitate wireless networking.

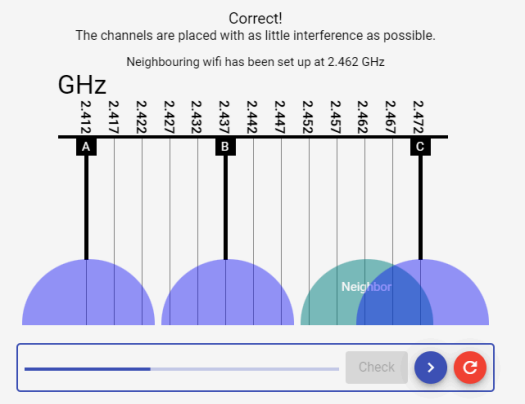
- As you have learned previously, Wi-Fi networks communicate on radio frequencies 2.4 GHz and 5 GHz. The 2.4 GHz frequency extends to 150 feet (45 meters) indoors and 300 feet (92 meters) outdoors. However, the 2.4 GHz frequency can experience congestion due to a limited number of channels. Plus, 2.4 GHz is more likely to experience interference from other nearby devices that use the same frequency, like microwaves. The 5 GHz frequency provides a stronger signal than 2.4 GHz and has more channels to handle more traffic. The 5 GHz drawback is that its range is limited to 50 feet (12 meters) indoors and 100 feet (30.6 meters) outdoors.
- **IEEE 802.15.4:** An inexpensive, low-power wireless access technology intended for IoT devices that operate on battery power. IEEE 802.15.4 uses the 2.4 GHz or lower radio band frequencies. IEEE 802.15.4 is normally used for low-rate wireless personal area networks (LR-WPANs) and uses a 128-bit encryption. Examples of IoT technologies that use IEEE 802.15.4 network connections include:
    - **ZigBee:** An LR-WPAN intended for smart home use. However, ZigBee has also been adopted globally for commercial IoT products. ZigBee includes a universal language that facilitates the interoperability of smart objects through a self-healing mesh network. ZigBee LR-WPAN networks can be accessed through Wi-Fi or Bluetooth.
- **Thread:** A low-latency wireless mesh networking protocol based on IPv6 addressing and existing open standards and technologies. These characteristics make thread networks compatible with a broad

spectrum of IoT ecosystems. Thread devices do not use proprietary gateways or translators, making them inexpensive and easier to implement and maintain than other wireless technologies. Thread is used by the Google Nest Hub Max.

- **Z-Wave:** An interoperable, wireless mesh protocol (described below) that is based on low powered radio frequency (RF) communications. The Z-Wave protocol uses an RF signal on the 908.2MHz frequency band and extends 330 feet. Z-Wave allows users to control and monitor IoT smart devices. Z-Wave is inexpensive, reliable, and simple to use. The Z-wave protocol supports a closed network for security purposes. Over 3300 types and models of home and business IoT devices are certified to use Z-Wave technology, with more than 100 million devices in use worldwide.
- **Wireless mesh network (WMN):** Mesh networks are used by many popular wireless IoT network protocols, like Zigbee and Z-Wave, for device communication. Wireless mesh networks use less power than other wireless connectivity options. Wireless mesh is a decentralized network of connected wireless access points (WAP), also called nodes. Each WAP node forwards data to the next node in the network until the data reaches its destination. This network design is "self-healing," meaning the network can recover on its own when a node fails. The other nodes will reroute data to exclude the failed node. Wireless mesh is a good option for high reliability and low power consumption, which is better for battery powered IoT devices. Wireless mesh networks can be configured to be full or partial mesh:
    - **Full mesh network:** Every node can communicate with all of the other nodes in the network.
    - **Partial mesh network:** Nodes can only communicate with nearby nodes.
- **Bluetooth:** Bluetooth is a widely used wireless network that operates at a 2.45 GHz frequency band and facilitates up to 3 Mbps connections among computing and IoT devices. Bluetooth has a range of up to 100 feet (30.6 meters) and can accommodate multiple paired connections. It is a good choice for creating a short distance wireless connection between Bluetooth enabled devices. Bluetooth is often used by computing devices to manage, configure, control, and/or collect small amounts of data from one or more close range IoT devices. For example, Bluetooth may be used to control smart home lighting or thermostat IoT devices from a smartphone.
- **Near-Field Communication (NFC):** NFC is a short-range, low data, wireless communication protocol that operates on the 13.56 MHz radio frequency. NFC technology requires a physical chip (or tag) to be embedded in the IoT device. NFC chips can be found in credit and debit cards, ID badges, passports, wallet apps on smartphones (like Google Pay), and more. A contactless NFC scanner, like a Point-of-Sale (PoS) device, is used to read the chip. This scanner communication connection often requires the IoT device to be within 2 inches (6 cm) of the scanner, but some NFC chips have an 8 inch (20 cm) range. This short-distance range helps to limit wireless network security threats. However, criminals can carry a portable NFC scanner into a crowded area to pick up NFC chip data from items like credit cards stored inside purses and wallets. To protect against this type of data theft, the cards should be placed inside special NFC/RFID sleeves that make the chips unreadable until they are removed from the sleeves. NFC technology may also be used in the pairing process for Bluetooth connections.
- **Long Range Wide Area Network (LoRaWan):** LoRaWan is an open source networking protocol designed to connect battery powered, wireless IoT devices to the Internet for widely dispersed networks.

Ways to investigate connection issues:

- Ping
- Traceroute
- Test-NetConnection / netcat



Supplemental Reading for IPv6 and IPv4 Harmony

IPv6 and IPv4 harmony

At the network layer of the TCP/IP Five-Layer Network Model, nodes connect through the internet protocol (IP) and the IP addresses that come along with it. The most common version of IP is version four (IPv4), but version six (IPv6) is rapidly seeing more widespread adoption.

This reading covers key differences between IPv6 and IPv4 and the methods that allow them to work together.

When IPv4 was first developed, a 32-bit number was chosen to represent the address for a node on a network. This means there can be around 4.2 billion individual IPv4 addresses. But this just isn't enough addresses for the number of Internet-connected devices we have in the world today. IPv6 was developed to provide plenty of addresses for all of our Internet connected devices. While IPv4 represents addresses with a 32-bit number, IPv6 represents addresses with 128 bits. This 128-bit update allows for a practically unlimited number of IPv6 addresses, 340 trillion trillion trillion addresses to be exact!

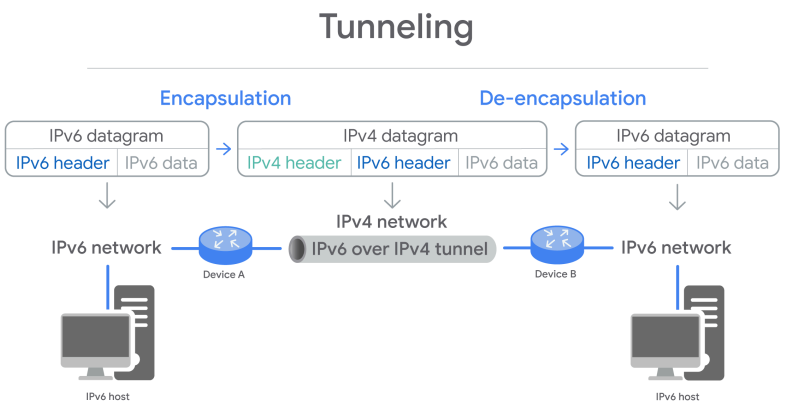
IPv4 and IPv6 require a different structure for each version's datagrams. This means the IPv4 and IPv6 networks speak different languages. For IPv6 data to travel over an IPv4 network, the IPv6 datagram has to be translated into something IPv4 can understand. Since it's not possible for the entire Internet and all connected networks to switch to IPv6 all at once, IPv6 tunneling protocols are used to allow IPv6 traffic to travel over the remaining IPv4 network.

Tunneling

Tunneling protocols allow users to carry IPv6 traffic across an IPv4 network. Tunnels are created using IPv6 servers on either end of a network connection. A tunnel server at one end takes incoming IPv6 traffic and encapsulates it within a traditional IPv4 datagram. Encapsulation is the process of transporting a data packet inside the payload of another packet.

IPv6 data that's encapsulated within an IPv4 datagram can then be delivered across the IPv4 network and received by another IPv6 tunnel server. The receiving server de-encapsulates the datagram and passes the IPv6 traffic further along the IPv6 network.

Three types of tunnels



Since IPv6 tunneling is still an evolving technology, there are several competing protocols used to establish IPv6 tunnels. Here are three commonly used tunnel protocols:

- **6in4/manual protocol** encapsulates IPv6 packets immediately inside an IPv4 packet, without using additional headers to configure the setup of the tunnel endpoints. Setup is configured manually instead. This makes performance predictable and easy to debug.
  Unfortunately, this protocol often will not function if the host uses network address translation (NAT) technology to map its IPv4 address. This makes the 6in4/manual protocol difficult to deploy.
- **Tunnel Setup Protocol (TSP)** specifies rules for negotiating the setup parameters between tunnel endpoints. This allows for a variety of tunnel encapsulation methods and wider deployment than is possible with the 6in4/manual protocol.
- **Anything in Anything (AYIYA)** protocol defines a method for encapsulating any protocol in any other protocol. AYIYA was developed for tunnel brokers, a service which provides a network tunnel. This protocol specifies the encapsulation, identification, checksum, security, and management operations that can be used once the tunnel is established. A key advantage of AYIYA is that it can provide a stable tunnel through an IPv4 NAT. It allows users behind a NAT or a dynamic address to maintain connectivity even when roaming between networks.

Each protocol has its pros and cons, depending on the nature of the communicating endpoints of the IPv6 connection.

Key takeaways

As IPv6 becomes more widely adopted, IPv6 traffic needs a way to travel over the IPv4 network.

- Tunneling protocols allow users to carry IPv6 traffic across an IPv4 network.
- Since IPv6 tunneling is still an evolving technology, there are several competing protocols used to establish IPv6 tunnels.
- Each protocol has its pros and cons, depending on the nature of the communicating endpoints of the IPv6 connection.

Course #3: **Operating Systems and You: Becoming a Power User**

Windows uses CLIs called "command line" and "Powershell"

Linux uses a "shell" the language of which is BASH

Windows Powershell Commands *[fun fact: cmd.exe commands are from DOS]*:

ls	List directories in current path
Get-Help [command] -Full	Description of each parameter of the command
ls -Force [directory]	List files not shown from normal ls. **Ex: Where the recycle bin is :D**
pwd	Print working directory (where you currently are)
cd [path]	Change directory
mkdir [name]	Make a directory
You can escape space characters with single quotes or a ` back tick before each special character	
history	Show previous commands
You can press the # key, type part of a recent command, then tab to cycle through items in your history	
clear	Wipe screen
cp [file path] [destination]	Copy (**Copy folder contents with -Recurse**)
mv [new name or file path] [destination]	Rename or move a file
rm	Skip recycle bin and remove a file
cat [file name]	Display whole contents of file
more [file name]	Display contents page-at-a-time
Enter key advances page by one line	
Space key advances to next page	
Q key quits the *more* command	
Can use -Head or -Tail parameters for just the first or last 10 lines of a file	
start notepad++ [file name]	Create and start editing a file in notepad++
sls **OR** Select-String [word] [file to search]	Search specific document for a word
echo	Alias for Write-Output command. Part of I/O operations
Can use > [file] to redirect output to start a word doc	
Can use >> [file] to redirect output to append something	
Use | pipe to direct a command as input to another command. (cat words.txt | Select-String blah)	
Use < to use something like a file's content as input instead of your keyboard strokes	
Get-LocalGroup	Show all groups on Local Machine
Get-LocalGroupMember [group]	Show users in a group
net user [username] [password]	Set password for a user
Could also put * instead of password then net will let you input the password without printing	
net user [username] /logonpasswordch:y	Make user change password on next log-on
net user [username] * /add	Create new user
net user [username] /del	Delete a user
icacls [directory]	See users with permissions to this directory
See descriptions for output with icacls /?	
icacls '[directory]' [user] [permissions]	

Icacls is a cmd.exe command, so use single quotes for some parameters when in powershell

icacls '[directory of interest]' /grant '[Group]:[Permissions]'	Grant permissions to a group for a dir
icacls '[directory of interest]' /remove '[Group]:[Permissions]'	Remove permissions of a group to a dir
Find-Package [package] -IncludeDependencies	See if a software package is available
Register-PackageSource -Name [name] -ProviderName [provider name] -Location [url]	Add new repository
Install-Package -Name [package name]	Install a software package
Compress-Archive	Create a zip
Get-Package -name [package name]	Verify that a software package is in place
Uninstall-Package -Name [package name]	Uninstall a software package.
Get-AdForest	Details about your Active Directory version.
Get-AdDomain	See details of your Active Directory version.

cmd.exe Exclusive

Diskpart	Video shows formatting a thumbdrive with Diskpart
mklink	Create a symbolic link for a file

*A symbolic link will not have link headers like a shortcut. Rather, a symbolic link is treated EXACTLY like the original file.

mklink /h	Create a hardlink

*Hardlinks attach to a file number, not a file name, so you can change the file name and the link is fine.

fsutil	See state of NTFS Self-Repair
taskkill	End a process with PID or other means.
sort	
select	Only display a certain type of output
net	Can use to share folders along the network

Windows doesn't use "root" or "sudo" but does use "UAC" or "User Access Control"
Help on Powershell and cmd.exe

Default source of packages in PowerShell is in the PowerShell Gallery. If your package isn't there, you can tell powershell where to find it like in a repository like Chocalatey.

Powershell Commands (Ex. ls)	cmd.exe Commands (Ex. dir)
Get-Help ls	dir /?

The **Computer Management** window is often used in the course to manage users, passwords, etc on a local machine.

Notepad++ is what Google course recommended for Windows Text Editor

The "Authenticated Users" group in windows

Hitting tab circulates through the directories in your active directory
-Verbose shows thought process of computer
-Force if you're an admin can skip confirmation questions and just immediately do the command.
-Filter will use a given pattern (like the * or other regex) to only give you certain results.

```
C:\Windows\system32>icacls "C:\Vacation Pictures" /grant Everyone:(OI)(CI)(R)
```

Add a user with permissions in cmd.exe

Add a user with permissions in PowerShell

Linux CLI Commands:

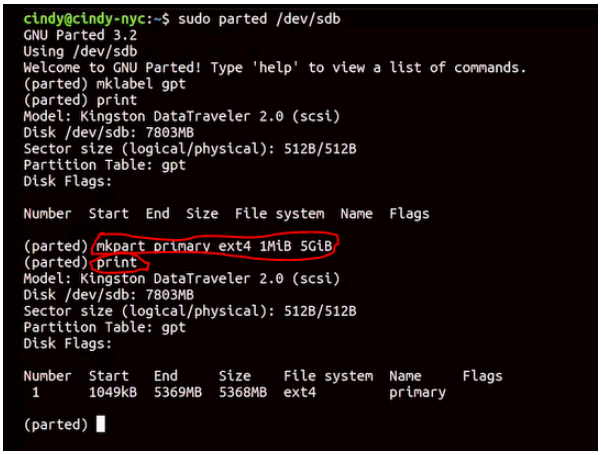
pwd	Print working directory
cd	Change directory
mkdir [name]	Make directory (escape characters with single quotes or \ back slashes)
history	Show recent commands
Ctrl+r is how you search your history	
cp [source] [destination]	Copy (use -r to include directory contents)
mv	Rename or move files
rm	Remove a file (use -r to delete directories)
cat [file name]	Show whole file contents
less [file name]	Has better functionality than “more” on windows
Lowercase g moves to start of text file	
Uppercase G moves to end of text file	
/word allows you to search for a specific word in the file	
head	Show first 10 lines in a file
tail	Show last 10 lines in a file
nano [file name]	One of the basic text editors in linux
grep [word] [file name]	Search a file for a given word
service [service name] [parameter]	Manage services on a linux machine
passwd [user]	Change user password
Passwords are scrambled and stored in /etc/shadow	
passwd -e [user]	Make user password expire so they gotta change
useradd [user]	Create new user
userdel [user]	Delete a user
chmod	Change file permissions
-s means run file with owner permissions	
-u or -g means if you’re adding/ removing permissions to a group or user	
+ or - to indicate if granting or removing a permission	
-t is the sticky bit which means allow a file to be written to by anyone, but only removable by the owner or root	
chown	Change owner of a file
dpkg -i [package name]	Install a debian package
dpkg -r [package name]	Remove a debian package
dpkg -l	List all debian packages installed
7z -e [file]	Extract an archive with 7zip
apt install [package name]	Install a package from repository in /etc/apt/sources.list directory
apt update	Update REPOSITORIES
apt upgrade	Update NEWER SOFTWARE as listed in repositories
uname -r	See system information (-r for kernel release version)

OpenLDAP Commands

ldapadd	Takes the input of an LDIF file and adds the context of the files
ldapmodify	Modifies an object
ldapdelete	Will remove the object that the LDIF file refers to
ldapsearch	Search entries in your directory database

parted -l	List the disks connected to the computer.
mkpart	Create a partition
mkfs	Format a disk
Ex: “sudo mkfs -t ext4 /dev/sdb1”	
mount	Mount a filesystem to a directory
umount	Unmount a filesystem

blkid	List UUIDs of connected storage devices
swapon	Create swap space
ln	Create soft or hard links to files
dh -u	Shows disk usage
df -h	Shows free space on machine (-h makes is human readable)
fsk (**don't run on mounted filestystems)**	Checks integrity of file system
Kill	Sent SIGTERM signal (end a process)
top	Show biggest resource hogs on machine
Quit with q key	
uptime	Give details like load averages on current machine session
ls -of	List open files and the processes using them.
scp	Securely copy a file over the network
logrotate	Rotate logs?
tail -f	Idk what she did but it was really cool to see the log update
dd	Copy disks to other drives
which	Find the PATH of a command



mkpart example (Left)

Users and groups in linux are usually listed in /etc/group or /etc/sudoers for example

The file that contains user information is **/etc/passwd**
Many "users" in that file are often programs that create an entry in order to run properly

"Root" is the first user made on a linux machine: a "superuser" of which there's usually only one.

Add -h after any command for help on it.

Hitting tab in Linux can show you all possible options at the same time w/ directories

700. The two zeros keep everyone, but the owner, from having any permissions at all, and the seven grants all available permissions to the owner (including execute). Keep in mind that because the file is owned by "root" you'll need to use **sudo**:

```
sudo chmod 700 important_document
```

The numerical equivalent of rwx is:

- 4 for read or r
- 2 for write or w
- 1 for execute or x

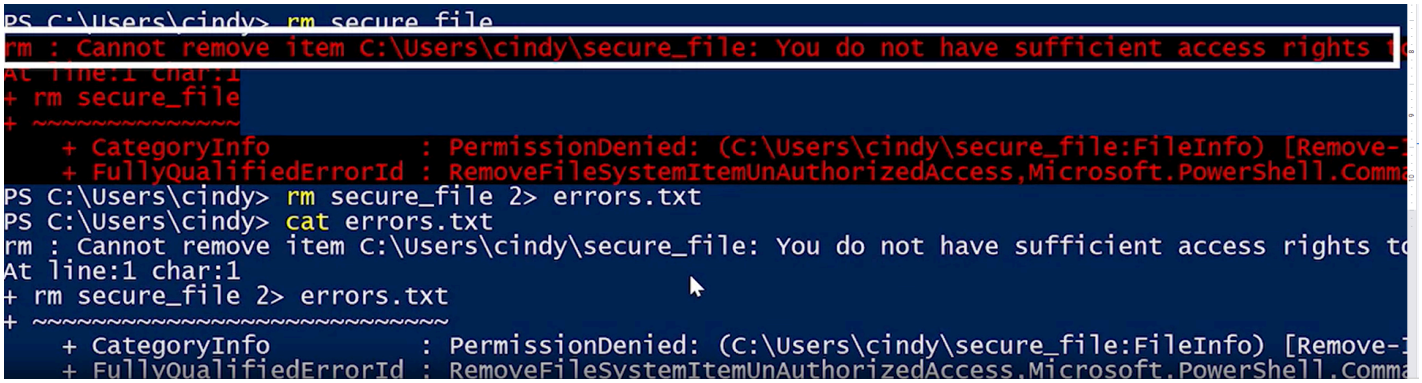
The ~ is a shortcut for your home directory in Windows and Linux

"Wildcards" are characters used to select files based on a certain pattern
Like copy all jpegs with "cp *.jpg"

Permissions can be represented as a sum. Like read(4) and write (2) permission = 6
An "s" in the permissions output means SetUID and lets you run file with permissions of the owner

Nano is one of the most basic (and user friendly) text editors in the linux shell.

```
1: stdout - the output
2: stderr - the error
```



Picture here is using rm secure_file **2>** blah blah blah to filter standard errors to a text file

Common Root Directory Subfolders

- Program Files (x86) - Most Windows program files.
- Users - The home directories of each user on the device.
- Windows - Where the Windows OS files are stored.

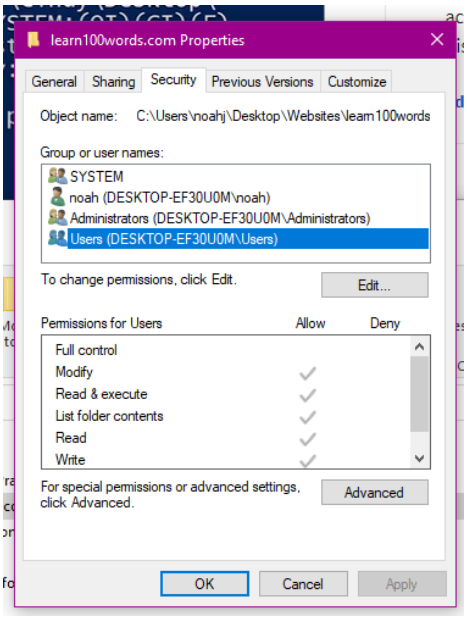
An “Absolute Path” is one that starts from the main directory.
A “Relative Path” is the path from your current directory.

$null is a PowerShell variable that literally represents nothing. It’s like “a black hole for the purposes of redirection”
/dev/null is the Linux equivalent of $null

Files and Permissions

In Windows, files and directory permissions are assigned using access control lists or **ACL**s. Specifically, we're going to work with discretionary access control lists or **DACLs**.

You can find permissions info in “Security Tab” of a directory on Windows GUI



Package & Software Management

“Installing and maintaining packages is something you'll do almost every day in an IT support role. So you should be familiar with how this works on the Windows and Linux OS.”

Microsoft install package (.msi)

Used to guide a program called the Windows Installer in the installation, maintenance, and removal of programs on the Windows operating system

Windows Software Packages

Developers have different ways to package software using software compiling tools. In Windows, software is usually packaged as a .exe (executable file). Windows software can be sourced from the Microsoft Store or downloaded directly and installed in several ways. This reading covers the most common methods software packages are installed on Windows OS.

Installation Package

Installation packages contain all the information the Windows Installer needs to install software on a computer. The packages include a .msi file (Microsoft install file) which contains an installation database, summary information, and data streams for each part of the installation. The .msi file may also include internal source files and external source files needed for the installation. Windows Installer uses the information contained in the .msi file to install, maintain, and remove programs on Windows.

Portable Executable

These .msi files are contained within a portable executable (PE), which is a format specific to Windows. The file type extension for a PE is .exe. Although these PEs commonly include instructions for the computer to run, such as the .msi files, they may also have images that the program may run or computer code.

Self-extracting Executable

While it is common to install software using the Windows Installer, it is helpful for you to know how to install software using the command line.

Self-extractor packages are executable files (.exe) that are run in the Windows interface by clicking on them or running from the command line. Software installed by an IT professional onto an end user's computer will likely use this format. Software installation package, update package, or hotfix package created with the Microsoft Self-Extractor, can be executed using the following command lines:

- **/extract:[path]**: Extracts the content of the package to the path folder. If a path isn't specified, then a Browse dialog box appears.
- **/log:[path to log file]**: Enables verbose logging (more detailed information recorded in the log file) for the update installation.
- **/lang:lcid**: Sets the user interface to the specified locale when multiple locales are available in the package.
- **/quiet**: Runs the package in silent mode.
- **/passive**: Runs the update without any interaction from the user.
- **/norestart**: Prevents prompting of the user when a restart of the computer is needed.
- **/forcerestart**: Forces a restart of the computer as soon as the update is finished.

You can always type **/?**, **/h**, or **/help** from the command line to view these options.

App Packager

The app packager used in the Windows Software Development Kit (SDK) and Microsoft Visual Studio includes a program called MakeAppx.exe. MakeAppx.exe is a tool that creates an app package from files on disk or extracts the files from an app package to disk. For Windows 8.1 and higher, this program can also create and extract app package bundles. This tool is primarily used by software developers.

Microsoft Store

The Microsoft Store, included in the Windows OS, is the primary source for apps, games, and videos in Windows. The Microsoft Store only contains apps and programs certified for compatibility and curated for content. Software installed through the Microsoft store is automatically updated by default. Some organizations may disable the Microsoft store on user computers to limit users' ability to install new applications without authorization.

While the Microsoft Store is a convenient and popular way to get programs on Windows, some software can also be downloaded directly from developers.

Key takeaways

Windows has many different ways to distribute, install, uninstall, and update programs and code on a computer. Depending on the organization, IT might use any of these installation options regularly.

- Installation packages contain all the information the Windows Installer needs to install software on a computer.
- While it is common to install software using the Windows Installer, it is helpful for you to know how to install software using the command line.
- The Windows Software Development Kit (SDK) and Microsoft Visual Studio include a program called MakeAppx.exe. MakeAppx.exe is a tool that creates an app package from files on disk or extracts the files from an app package to disk.
- Microsoft Store is a digital distribution storefront for apps, games, and other media.

Resources for more information

- Installation Package: https://docs.microsoft.com/en-us/windows/win32/msi/installation-package
- App packager (MakeAppx.exe): https://docs.microsoft.com/en-us/windows/win32/appxpkg/make-appx-package--makeappx-exe-
- Portable Executables: https://docs.microsoft.com/en-us/windows/win32/debug/pe-format
- Self-extractor: https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/command-switches-supported-by-self-extractor-package

Mobile App Distribution

You are likely familiar with using either the Apple App Store or Google Play store to download and install apps on your smartphone. As an IT Support professional, you may need to deploy mobile apps across large organizations. In this reading, you will learn more about how mobile apps are distributed both publicly and privately for iOS and Android.

How apps are distributed

Apple mobile apps

Apple's App Store provides apps to millions of mobile devices around the world, including the iPhone, iPad, and Apple Watch. Apple's App Store Connect allows developers and organizations to distribute both public and private apps, provided that the app passes an intensive review process to meet Apple's quality standards. App Store Connect also allows developers and organizations to set individualized prices for the apps, enter banking information to accept payments for apps or in-app purchases, schedule beta testing, and more. Apple recommends that developers use the Xcode integrated development environment (IDE) or Ad Hoc for developing iOS, iPadOS, and watchOS apps.

Apple's App Store

Apple's public App Store is a marketplace that reaches millions of Apple mobile device users across the world. The App Store offers developers unlimited bandwidth for hosting, handles payment processing, verifies users, etc. Developers must first register through the Apple Developer Program if they wish to distribute apps through the App Store. The Apple Developer Program offers resources, tools, and support for app development, including testing tools, beta software, analytics, etc. Apple has a long and detailed list of guidelines for all apps that developers and organizations must follow. The guidelines include rules for safety, third-party software development kits (SDKs), ad networks, trademarks and copyrights, and much more. Additionally, submitted apps cannot be copies of other developers' products, nor can they be designed to steal users' data. Though the Apple Store Connect review process is rigorous, the platform also provides an appeals process for rejected apps.

Custom Apple apps

Organizations may opt to create private customized apps to meet specific and unique organizational needs. These custom apps may be designed for the organization's students, employees, clients, partners, franchisees, etc. Organizations can choose to offer the apps for free, for a price, or through special redemption codes. They also have the option to automatically distribute and configure apps to large numbers of registered devices using Mobile Device Management (MDM).

Apple offers a couple of options for private and secure customized app distribution:

- **Apple School Manager** - For educational institutions, provides the option to distribute proprietary apps for internal use and to purchase other apps in large volumes, often with educator discounts. Common apps in Apple School Manager might include those for course registration or digital textbook access. Apple School Manager also offers educational institutions the ability to create accounts for students and staff, as well as to setup automatic device enrollment.
- **Apple Business Manager** - For businesses, offers similar features as the Apple School Manager including the distribution and purchase of private apps, as well as the automatic deployment of apps to the business' mobile devices. As an IT Support professional, you might want to volume purchase mobile virus protection and automatically deploy the app across your business' mobile devices. An organization can set private audience groups in App Store Connect. The audience groups will be able to see and download the organization's custom apps through the Apps and Books or Content sections of the Apple School and Apple Business Managers.

Outside official Apple distribution channels

Some developers and organizations might not want to use an Apple platform for app distribution. As an alternative, they have the option to distribute Apple "trusted developer" apps from websites or private file shares using their Apple Developer ID certificate and Apple's notarization process.

Android mobile apps

Google makes considerable investments into Android development, the Google Play platform, services, tools, and marketing to support developers and organizations who choose Google Play to deploy Android apps. Android Studio is the official Android integrated development environment (IDE) for developing Android apps. Android Studio is used to compile Android Package Kit (APK) files, and the Android App Bundle is used to publish apps to Google Play. The Android App Bundle enables Google Play to automatically generate the APK files for a variety of devices and provide app signing keys. This service is a significant time saver for developers and it ensures Google Play apps will work on most Android devices.

Google Play Store

Google Play revenue makes it possible for Google to offer the open Android operating system for free to device manufacturers in order to promote growth and innovation. This business model has driven Android adoption across 24,000+ device models with **billions** of Android mobile device users around the world. The Google Play store hosts 2 million apps and games with 140+ billion downloads per year, and growing. Google also keeps consumers safe with Google Play's built-in protections, which require developers to adhere to high safety standards.

To distribute an app publicly through the Google Play Store, a developer will:

1. Create a Google Play developer account.
2. Use the Google Play Console to Create App.
    a. Provide preliminary information about the app.
    b. Review and agree to the Developer Program Policies, Terms of Service, and documentation about export laws (where applicable).
3. Use the app's Dashboard for guidance through the app publishing process:
    a. Google Play Store listing

b. Pre-release management
c. Prepare a release
d. Testing
e. Submit app and declarations for review by Google
f. Promotion/pre-registration
g. Publish app (upon review approval)

Custom Android Apps
Large organizations, or Enterprise customers, can use “managed Google Play” as a distribution tool for deploying apps to employees. Enterprise customers operate their own Google Play store to host their apps publicly and/or privately. They can grant access to select users or user groups to view and download private apps. Google Play Custom App Publishing API is an Application Programming Interface from Google that enables developers and organizations to create and publish private custom apps. Apps that are published through Google Play Custom App Publishing API cannot be converted to public apps. The apps will remain private permanently. Google offers a streamlined verification process for private custom apps. These apps can be available to an organization for deployment in as little as 5 minutes after verification.

Google Play Custom App Publishing API can be used by:

- Enterprise mobility management providers (EMMs)
- Third-party app developers
- Organizations/developers that want their enterprise clients to be able to distribute private/custom apps from an EMM console, IDE, or other interface.

Enterprise customers can publish apps by:

1. Enabling the Google Play Custom App Publishing API.
2. Creating a service account.
3. Granting publishing permission to the service account on the organization’s Play Console developer account.

Using Google Play within an organization, IT Support administrators should:

1. Use their organization’s managed version of Google Play to select and approve apps.
2. Ensure all employee Android devices are set up to use the organization’s managed Google Play account.
3. Use the organization’s Enterprise Mobility Manager (EMM) to manage employee Android devices and deploy selected apps to employees’ Android devices.

For Android devices that are owned by employees (BYODs) and not registered with the organization’s EMM:

1. Consider Google’s recommendation to create a work profile on each device..
2. Show employees how to use their work profile to access the organization’s managed Google Play account.
3. Demonstrate that employees can then view and install any of the administrator selected and approved apps.

Outside official Google distribution channels
Google’s open platform policies includes allowing competitors to innovate in developing app stores. Some alternative app stores that distribute Android apps include:

- APKMirror
- Aurora Store
- Aptoide
- Amazon Appstore
- F-Droid
- Uptodown
- SlideMe
- APKPure
- Galaxy Store
- Yalp Store

Please see Fossbytes “10 Best Google Play Store Alternatives: Websites And Apps” for more information about each Android app store in the list above.

Resources for more information

- App Store Review Guidelines - Apple’s comprehensive list of guidelines developers must follow for designing and submitting apps to the Apple App Store.
- Distributing custom apps for business - Apple’s guide to publishing custom apps.
- About Android App Bundles - Android developer’s guide to using Android App Bundles to develop and publish apps on Google Play.
- Get started with custom app publishing - Google’s guide to publishing custom apps.

Mobile App Packages: App Updates

In this reading, you will learn about updating apps on mobile devices. IT Support professionals use this skill for the maintenance and troubleshooting of mobile devices. It is a best practice to keep apps updated for security purposes and to avoid any problems that affect outdated apps.

How to update apps

Android mobile apps

It is important to note that Android is an open operating system (OS). This means mobile device manufacturers and cellular service providers can modify the Android OS to enhance, control, or restrict elements of the OS. These modifications can include how system settings are accessed. If an Android device’s Storage settings cannot be located easily, it is best to consult the device manufacturer’s manual. Mobile device manuals can often be found online.

Instructions for most Android phones and tablets *(note that instructions may vary by OS version; Android 12 was used for these instructions)*:

Automatic updates

1. Open the **Google Play Store** app.
2. At the top right, tap the **profile icon**.
3. Select **Settings**.
4. Open the sub-menu for **Network preferences**.
5. Select an option:
    a. **App download preference** Over any network - to update apps using either Wi-Fi or mobile data (data usage charges may apply, depending on cellular plan).
    b. **Auto-update apps** Over Wi-Fi only - to update apps only when connected to Wi-Fi.

Troubleshooting note: If the user is not logged in to their Google account on the Android device, apps may not update automatically.

Manual updates

1. If automatic updates are toggled on, repeat steps 1 to 5 for the “Automatic updates” instructions listed above. However, for step 5, select **Don’t auto-update apps**.
2. Open the **Google Play Store** app.
3. At the top right, tap the **profile icon**.
4. Select **Manage apps & device**.
5. In the Update available section, select See details.
6. Select individual software to Update.

Apple mobile devices

Automatic updates

Apple's iPhones and iPads are configured by default to automatically update apps stored on these devices. However, as an IT Support specialist, you may encounter a variety of reasons why automatic updates were disabled for a device, but need to be enabled again. The instructions to turn on automatic updates for installed apps may vary by OS version. Please see Apple's website to view instructions for the specific OS version in use.

Manual updates

Some IT departments have policies to test all updates before allowing the updates to be applied across the organization's devices. In this case, you may need to configure the organization's Apple mobile devices to use manual updates for apps. Turning on manual updates will involve turning off automatic updates. This step enables notifications to display each time an update becomes available for an app installed on the device.

Instructions for app updates

The instructions for configuring automatic and manual updates for installed apps may vary by OS version. Please see the "Resources for more information" section below for links to Apple's Support website to obtain detailed instructions.

Resources for more information

For more information about updating apps on mobile devices, please visit:

- How to manually update apps on your Apple device - Instructions for configuring both manual updates and automatic updates for apps on Apple mobile devices.
- Manage software updates for Apple devices - Advanced administrative information for managing software updates for Apple mobile devices. Centered on devices enrolled in mobile device management (MDM) solutions.
- How to update the Play Store & apps on Android - Provides step-by-step instructions on multiple options for updating Android apps.

Mobile Device Storage Space

In this reading, you will learn how to check mobile devices for available storage space and how to free up storage when space is low. Storage space on mobile devices is often limited. It is a best practice to ensure that there is sufficient space on a mobile device before installing new apps or saving new files. As an IT Support Specialist, checking storage space is an important troubleshooting step. Like PCs, mobile devices can experience unusual errors when storage space runs low. Imagine a user is trying to install an app or save a file to a mobile device and an unexpected error occurs. If the error does not generate an informative error message, you will have to investigate the problem. The first troubleshooting step for an installation or saving problem should be to check if there is enough storage space for the new app or file.

Sometimes, limitations may be reached without the user intentionally adding programs or files to their device. Automatically generated temporary cache files, for instance, can fill up the last bit of storage space and cause unusual performance problems. Fortunately, unused or rarely used apps and files can be uninstalled or deleted to make space for new items. Users should also be encouraged to use cloud storage for photos, videos, and other important files, instead of storing the files locally on the mobile device. This not only saves storage space, but it also helps in protecting the files if the mobile device is lost, stolen, or broken.

Apple mobile devices

Both iOS and iPadOS automatically analyze how much space apps occupy in storage on iPhones and iPads. You can see how much storage is available through the device's Settings menu, on iTunes, or through a computer with a connection to the mobile device. Apple mobile devices can be configured to free up space automatically when they are low on storage space. The devices will select files that can be downloaded again if needed for removal. These files can include cache, local copies of files that are stored in the cloud, streamed videos and music, and temporary files. Apple devices should also generate an alert when storage space is almost full to give the user an opportunity to select specific apps and files for removal.

The following steps should be followed to check the storage space available on iPhones and iPads *(note that instructions may vary by OS version; iPadOS 15 was used for these instructions)*:

1. Navigate to **Settings > General > iPhone Storage** or **iPad Storage.**
2. The first item on the Storage screen should be a visual indicator of how much storage space has been used out of the total storage space available on the device. It might be color coded to delineate which types of items are occupying the used storage space, such as apps, messages, media, system data, etc.
3. Check the RECOMMENDATIONS section near the top of the screen (if available). This section might suggest automatically deleting messages that are over a year old or automatically uninstalling unused apps when space is running low. Be sure to investigate the suggested items for deletion to ensure that the items will not be missed before clicking **Enable**.
4. Review the next section, which lists the apps installed on the device. The file size and date last used will be listed for each app. If you open the detailed view for an app, you might see options like:
    a. **Offload the app** - Removes the app only, but keeps app data and documents.
    b. **Delete the app** - Removes the app, its data, and related documents.
5. Select the best option that suits the device user's needs.
6. Move any photos, videos, and other user-created files to iCloud storage and remove the copy stored on the device's storage space.

Android mobile devices

Android is an open operating system (OS), which allows manufacturers to change the OS configuration. These changes can include how system settings are accessed. For example, most versions of Android should have **Storage** listed immediately under **Settings**. However, Samsung Android phones have **Storage** settings listed under either **Device Maintenance** or **Device Care**. If an Android device's Storage settings cannot be located easily, it is best to consult the device manufacturer's manual. Mobile device manuals can often be found online.

Instructions for most Android phones and tablets *(note that instructions may vary by OS version; Android 12 was used for these instructions)*:

1. Navigate to **Settings > Storage**
2. The Storage screen may display a visual indicator illustrating how much storage space has been used out of the total storage space available on the device. Like Apple devices, the graphic might be color coded to indicate which types of `USER DATA` are occupying the used storage space, such as images, videos, audio, documents, apps, etc.
3. Click the `CLEAN UP` button under the graphic (if available).
4. A new window should open to show a list of items that Android has analyzed and `RECOMMENDED FOR CLEANUP.` Next to each item may be a button labeled `CLEAN UP`. Scroll down to the bottom of the list to find the `SPECIAL CLEANUPS` section.
    a. For some items, like **Junk Files**, clicking the `CLEAN UP` button will automatically remove the files.
    b. For other items, like **Images** or **Videos**, clicking the `CLEAN UP` button will give the user a checklist of specific items to select for removal. Be sure to investigate the suggested items for deletion to ensure that the items will not be missed by the user.

7-zip is an open source archiving tool

DLL Files and Windows Package Dependencies

In this reading, you will learn about dynamic link library (DLL) files. This information includes how Windows package dependencies can break and how Microsoft has remedied these DLL dependency problems using the .NET framework and other methods. You will also learn about the side-by-side assemblies and manifest files for Windows applications.

Dynamic link library (DLL)

Windows DLL files are vital to the core functions of the Windows operating system (OS). Some Windows-compatible applications also use DLL files to function. DLLs are made up of programming modules that contain reusable code. Multiple applications can use and reuse the same DLL files. For example, the Comdlg32 DLL file is used by many applications to provide Windows dialog box functions. The reusable feature helps Windows conserve disk space and use RAM more efficiently, which improves the operating speed of the OS and applications. The modular structure also makes updating a DLL file fast and simple, eliminating the need to update the entire library. DLL updates are installed once for use by any number of applications.

A few common DLLs used by Windows include:

- **.drv files** - Device drivers manage the operation of physical devices such as printers.
- **.ocx files** - Active X controls provide controls like the program object for selecting a date from a calendar.
- **.cpl files** - Control panel files manage each of the functions found in the Windows Control Panel.

An application can use DLLs to load parts of the app as modules. This means that if the application offers multiple functions, the app can selectively load only the modules that offer the functionality requested by the user. For example, if a user does not access the Print function within an application, then the printer driver DLL file does not need to be loaded into memory. This system requires less RAM to hold the application in working memory, which improves operating speeds.

DLL dependencies

A Windows package dependency is created when an application uses a DLL file. Although the Windows DLL system supports the sharing of DLL files by multiple applications, the applications' dependencies can be broken under certain circumstances.

DLL dependencies can be broken when:

- **Overwriting DLL dependencies** - It is possible for an application to overwrite the DLL dependency of another app, causing the other app to fail.
- **Deleting DLL files** - Some applications and malware may delete the DLLs needed by other applications installed on a system.
- **Applying upgrades or fixes to DLLs** - Can cause a problem called "DLL hell" where an application installs a new version of the shared DLL for a computer system. However, other applications that are dependent on the shared DLL have not yet been updated to be compatible with the new version of the DLL. This causes the other applications to fail when the end user tries to launch them.
- **Rolling-back to previous DLL versions** - A user may try to reinstall an older application that stopped working after a shared DLL file was upgraded by a newer app. However, the reinstallation of the app that uses the old DLL version can overwrite the new DLL file. This DLL version roll-back can cause the newer app with the shared DLL dependency to fail the next time it tries to run.

Microsoft has remedied these problems through the use of:

- **Windows File Protection -** The Windows OS controls the updates and deletions of system DLL files. Windows File Protection will allow only applications with valid digital signatures to update and delete DLL files.

- **Private DLLs** - Removes the sharing option from DLLs by creating a private version of the DLL and storing it in the application's root folder. Changes to the shared version of the DLL will not affect the application's private copy.
- **.NET Framework assembly versioning** - Resolves the "DLL hell" problem by allowing an application to add an updated version of a DLL file without removing the older version of the DLL file. This prevents the malfunction of applications that have dependencies on the older DLL file. The DLL versions can be found in the "C:\Windows\assembly" path and are placed in the Global Assembly Cache (GAC). The GAC contains the .NET "Strong Name Assembly" of each DLL file version. This "Strong Name Assembly" includes the:
    - **name of the assembly** - multiple DLL files can share the assembly name
    - **version number** - differentiates the version of DLLs
    - **culture** - country or region where the application is deployed, can be "neutral"
    - **public key token** - a unique 16-character key assigned to an assembly when it is built

Side-by-side assemblies

DLLs and dependencies can also be located in side-by-side assemblies. A side-by-side assembly is a public or private resource collection that is available to applications during run time. Side-by-side assemblies contain XML files called manifests. The manifests contain data similar to the configuration settings and other data that applications traditionally stored in the Windows registry. Instead of registering this data in the Windows registry, the applications store shared side-by-side assembly manifests in the WinSxS folder of the computer. Private manifests are stored inside the application's folder or they can be embedded in an application or assembly. The metadata of a manifest may include:

- **Names** - Manages file naming.
- **Resource collections** - Can include one or more DLLs, COM servers, Windows classes, interfaces, and/or type libraries.
- **Classes** - Included if versioning is used.
- **Dependencies** - Applications and assemblies can create dependencies to other side-by-side assemblies.

As an IT Support professional, this concept should be considered when troubleshooting application issues. If the application's configuration settings are not found in the Windows registry, they might be located in the manifest from the app's side-by-side assembly.

Linux Package Dependencies

In this reading, you will review how to install and manage Debian packages in Linux using the **dpkg** command. This skill may be helpful to IT Support professionals that work with Linux systems like Debian or Ubuntu.

The following is a list of terms used in this reading:

- **Debian:** One of many free Linux operating systems (OSes), used as the foundation for other OSes, like Ubuntu.
- **Linux packages:** A compressed software archive file that contains the files needed for a software application. These files can include binary executables, a software libraries, configuration files, package dependencies, command line utilities, and/or application(s) with a graphical user interface (GUI). A Linux package can also be an OS update. Linux OS installations normally come with thousands of packages. Common Linux package types include:
    - **.deb** - Debian packages
    - **.rpm** - Redhat packages
    - **.tgz** - TAR archive file
- **Linux repository:** Storage space on a remote server that hosts thousands of Linux packages. Repositories must be added to a Linux system in order for the system to search and download packages from the repository.

- **Stand alone package:** A package that does not require any dependencies. All files required to install and run the package on a Linux system are contained inside a single package.
- **Package dependency:** A package that other Linux packages depend upon to function properly. Often, packages do not include the dependencies required to install the software they contain. Instead, package manifests list the external dependencies needed by the package.
- **Package manager:** A tool on Linux systems used for installing, managing, and removing Linux packages. Package managers can also read package manifests to determine if any dependencies are needed. The package manager then finds and downloads the dependency packages before installing the packaged software. Several common Linux Package Managers include:
    - For Debian and Debian-based systems, like Ubuntu:
        - **dpkg** - Debian Package Manager
        - **APT** - Advanced Package Tool, uses dpkg commands
        - **aptitude** - user-friendly package manager
    - RedHat and RedHat-based systems, like CentOS:
        - **rpm** - RedHat Package Manager
        - **yum** - Yellowdog Updater Modified, comes with RedHat
        - **dnf** - Dandified Yum

The dpkg command

The Linux **dpkg** command is used to build, install, manage, and remove packages in Debian or Debian-based systems.

Syntax (Credit to Joseph Cardona for examples)

The following are a few common **dpkg** command action parameters, with syntax and uses:

To install a package: $ sudo dpkg - -install packagename

To update a package saved locally: $ sudo dpkg - -update-avail *packagename*

To remove a package: $ sudo dpkg - -remove *packagename*

To purge a package, which removes the package and all files belonging to the package: $ sudo dpkg - -purge *packagename*

To get a list of packages installed: *$ sudo dpkg - -list*

To get a list of all files belonging to or associated with a package: *$ sudo dpkg - -listfiles packagename*

To list the contents of a new package: $ sudo dpkg -contents *packagename*

When an action parameter is added to the **dpkg** command, one of the following two commands are run in the background:

- **dpkg-deb:** A back-end tool for manipulating .deb files. The dpkg-deb tool provides information about .deb files, and can pack and unpack their contents.
- **dpkg-query:** A back-end tool for querying .deb files for information.

Additional Debian package managers

There are several alternate methods for managing Debian packages. Some have command-line interfaces (CLI) while others have GUIs. The alternative options to **dpkg** include:

- **APT (Advanced Package Tool)** - A powerful package manager designed to be a front-end for the **dpkg** command. APT installs and updates dependencies required for proper .deb package installation.
- **Synaptic Package Manager** – A popular GTK (GNU Image Manipulation Program ToolKit) widget with a GUI. Provides an array of package management features.
- **Ubuntu Software Center** – A GTK GUI developed by Ubuntu and integrated into the Ubuntu OS.
- **aptitude** – A user-friendly front-end for APT, with a menu-driven console and a CLI.
- **KPackage** – A part of KDE (Kool Desktop Environment) used to install and load packages that do not contain binary content. Non-binary content includes graphics and scripted extensions.

Package Managers

“Apt” or “Advanced Package Tool” is the package manager for Ubuntu

Def see the google video notes on the website. Great information.

If you install a package but it’s still giving you problems, the program may be closed-sourced, so you can’t see exactly what it does, but you **can** see what steps it’s taking in the installation process with the **sys internals** tools from the Chocolatey repository. See “Process Monitoring”

If you're curious about the details of what goes into an MSI file or want to create a Windows installer package yourself, check out the orca.exe tool that Microsoft provides.

Software Managers

Devmgmt.msc is the file where device manager is held. If you can’t access the gui windows bar, you can search this.

The PnP or “Plug & Play” system is where you plug in a thingy, and Windows looks for the software it needs to get it ready. (See video of Windows:Devices and Drivers)

When a device is connected to a linux computer, a device file is created in /dev

In linux, when looking at permissions with ls -l, a b means block device file and c means character device file.

For example, the “null” device is character because it handles data character-by-character

/dev/sda or /dev/sdb or /dev/sdc are SD devices

Linux Devices and Drivers

In this reading, you will learn how devices and drivers are managed in Linux. Previously, you learned that in Linux, devices attached to the computer are recognized by the operating system as device files. Devices are located in the /dev directory in Linux. A few examples of devices you may find in the /dev directory include:

- **/dev/sda** - First SCSI drive
- **/dev/sr0** - First optical disk drive
- **/dev/usb** - USB device
- **/dev/usbhid** - USB mouse
- **/dev/usb/lp0** - USB printer
- **/dev/null** - discard

Some of the Linux device categories include:

- **Block devices:** Devices that can hold data, such as hard drives, USB drives, and filesystems.
- **Character devices:** Devices that input or output data one character at a time, such as keyboards, monitors, and printers.

- **Pipe devices:** Similar to character devices. However, pipe devices send output to a process running on the Linux machine instead of a monitor or printer.
- **Socket devices:** Similar to pipe devices. However, socket devices help multiple processes communicate with each other.

Installing a device in Linux

There are hundreds of versions of Linux available due to the fact that Linux is an open source operating system. The methods for installing devices on Linux can vary from version to version. The instructions in this section provide various options for installing a printer and its device drivers on a Red Hat 9 Linux system running the GNOME user interface.

Device autodetect with udev

Udev is a device manager that automatically creates and removes device files in Linux when the associated devices are connected and disconnected. Udev has a daemon running in Linux that listens for kernel messages about devices connecting and disconnecting to the machine.

Installation through a user interface - GNOME

There are multiple user interfaces available for Linux. These instructions are specifically for the GNOME user interface.

1. In the GNOME user interface, open the **Settings** menu.
2. On the left-side menu, select **Printers**.
3. Click the **Unlock** button in the top right corner to change the system settings. Note that your user account must have *superuser*, *sudo,* or *printadmin* privileges to unlock the system settings for printers.
4. A dialog box will open showing a list of available printers. If your network has a large number of printers, you can search for the printer by IP address or host name.
5. Select the printer you want to install on the local system and click **Add**.
6. The printer listing will appear in the **Settings** window for the **Printers.**
7. In the top right corner of the printer listing, click the **Printer Settings** icon and select **Printer Details** from the pop-up menu.
8. The details of the printer will open in a new window. You should have three options for installing the printer driver:
    a. **Search for Drivers:** The GNOME Control Center will automatically search for the driver in driver repositories using PackageKit.
    b. **Select from Database:** Manually select a driver from any databases installed on the Linux system.
    c. **Install PPD File:** Manually select from a list of postscript printer description (PPD) files, which may be used as printer drivers.

Installation through the command line

Red Hat Linux uses the Common Unix Printing System (CUPS) to manage printers from the command line. CUPS servers broadcast to clients for automatic printer installation on Linux machines. However, for network environments with multiple printers, it may be preferable to manually install specific printers through the command line.

- From the command-line, enter **$ lpadmin -p printername -m driverfilename.ppd**
    - **Lpadmin** is the printer administrator command.
    - The **-p printername** command adds or modifies the named printer.
    - The **-m driverfilename.ppd** command installs the postscript printer description (PPD) driver filename that you provide. The file should be stored in the **/usr/share/cups/model/** directory.
    - Enter **$ man lpadmin** to open the manual for the lpadmin command to find additional command line options.

How to check if a device is installed

There are a couple of methods for checking if a device is already installed on a Linux machine:

Through a user interface like GNOME

1. In the GNOME user interface, open the **Settings** menu.
2. Browse each device set on the left-side menu.
3. The attached devices of the selected device type will appear in the window pane on the right.

Through the command line

The most common way to check if a device is installed is to use the “ls” (lowercase L and S) command, which means “list”.

- **$ ls /dev** - Lists all devices in the /dev folder
- **$ lscpci** - Lists devices installed on the PCI bus
- **$ lsusb** - Lists devices installed on the USB bus
- **$ lsscsi** - Lists SCSI devices, such as hard drives
- **$ lpstat -p** - Lists all printers and whether they are enabled
- **$ dmesg** - Lists devices recognized by the kernel

Windows Update

The Windows operating system updates frequently, These updates often include important security patches. It is important \ to keep your Windows systems up to date with the most current changes. This reading covers the different types of Windows updates and how to install them.

The Windows OS includes the Windows Update Client service. This service runs in the background on your computer to help you download and install updates and patches for the operating system. It does this by checking in with the Windows Update servers at Microsoft and looking for updates that should be applied to your computer. If your Windows system is functioning properly, the Windows Update Client will alert you when there are updates to install.

Types of Windows updates

There are several types of updates that the Windows Update Client might find for your Windows system.

- **Critical updates** address critical bugs that are not security related. These are widely released fixes for a specific problem.
- **Definition updates** are widely released and frequent updates to a product's definition database. Definition databases are used to detect specific types of objects on your system, such as malicious code, phishing websites, or junk mail.
- **Driver updates**: Drivers are software that control the input and output of devices running on your system. This software may be updated when new versions of the driver become available for your devices or if you install a new device on your system.
- **Feature packs** add new product functionality to your system. This functionality is first distributed as an update to a product currently running on your system. It is usually included in the next full product release.
- **Security updates** are widely released patches for a security related vulnerability. Security vulnerabilities are rated by severity as being critical, important, moderate, or low.

a) **Critical** vulnerabilities pose an active threat. Patch *should be installed immediately*.

b) **Important** vulnerabilities pose a likely threat. Patch *should be installed as soon as possible*.

c) **Moderate** vulnerabilities pose a potential threat. Patch *should be installed soon*.

d) **Low** severity vulnerabilities are not an immediate threat, but a *patch is recommended*.

- **Service packs** collect all tested hotfixes, security updates, critical updates, and general updates together and distribute them as a set. A service pack also may contain new fixes or design changes requested by customers.
- **General updates** are widely released fixes for specific problems. They address noncritical bugs that are not security related.
- **Update rollups** collect a set of tested hotfixes and updates that target a specific area, such as a component or service. These fixes and updates are packaged together for easy deployment.
- **Security-only updates** collect all the new security updates from a given month for distribution through the Windows Server Update Services (see below). These updates are called “Security Only Quality Update” when you download them and will be rated as “Important.”
- **New OS**: A new version of the Windows operating system may also be deployed through the Windows Update Client. For example, Windows 10 and 11 were both delivered as updates to a previously installed OS.

Installing updates
The process for installing updates may be automatic, depending on which version of Windows you’re using

Automatic updates
Beginning with Windows 10, the Windows OS ships with automatic updates turned on. With automatic updates on, Windows Update Client will download and install available updates without prompting you. For older versions of Windows, you must configure Windows Update to update automatically.

Windows 10 and 11 no longer allow you to turn off automatic updates completely, but you can pause updates for up to 35 days. Once the pause period ends, you are required to perform an update before you can pause again.

Manual updates
You can manually prompt Windows to perform an update at any time by checking for updates with the Windows Update tool. Manually updating does vary based on the version of Windows used. For detailed instructions on how to do this, see the Windows Update: FAQ page.

To ensure top performance and security for your Windows system you should make sure it is always updated to the most recent changes.

Key takeaways
The Windows operating system updates frequently, so it is important that you know how to keep your Windows systems up to date with the most current changes.

- Windows operating systems include the Windows Update Client service to help you download and install updates and patches for the operating system.
- There are several types of updates that the Windows Update Client might find for your Windows system.
- The process for installing updates depends on which version of Windows you’re using.
- Regular updates ensure top performance and security for your Windows system.

Linux Update
Linux is a free, open-source operating system used on a wide variety of computing systems, such as embedded devices, mobile devices including its use in the Android operating system, personal computers, servers, mainframes, and supercomputers. The Linux kernel is the core interface between a device’s hardware and the rest of its processes. The kernel controls all the major functions of hardware running the Linux operating system. To keep the core operating system up to date with current security patches, new features, and bug patches, you

need to update the Linux kernel. This reading covers how the Linux kernel functions and how to update Ubuntu, the most common Linux distribution.

Linux kernel

The Linux kernel is the main component of a Linux operating system (OS). The kernel is software located in the memory that tells the central processing unit (CPU) what to do. The Linux kernel is like a personal assistant for the hardware that relays messages and requests from users to the hardware.

The kernel has four main jobs:

1. **Memory management** tracks how much memory is being used by what and where it is stored.
2. **Process management** determines which processes can use the central processing unit (CPU), when, and for how long.
3. **Device drivers** act as an interpreter between the hardware and processes.
4. **System calls and security** receives requests for service from the processes.

To ensure that Linux distribution is running the most current version of the operating system, you will need to update it regularly.

Updating Ubuntu Linux distribution

A Linux distribution is an operating system (OS) that includes the Linux kernel and usually a package management system. There are almost one thousand Linux distributions, and each distribution has a slightly different way of updating.

The Ubuntu distribution is one of the most popular since it is easy to use. There are two ways to update the Ubuntu distribution:

- **Update Manager** is a graphical user interface (GUI) that is nearly 100% automated. When updates are available, it will open on your desktop and prompt you to complete the updates. It checks for security updates daily and nonsecurity updates weekly. You can also choose to check for updates manually.
- **Apt** is the Ubuntu package management system that uses command line tools to update a Ubuntu distribution. Apt does not check for updates automatically, you must manually run it to check for updates. You can use the following commands to check for updates and upgrade:

1. `apt-get update` To update with apt, open the terminal and use the command `apt-get update`. This command prompts you to enter your password, then it updates the list of system packages.
2. `apt-get upgrade` Once the package list is up to date, use the command `apt-get upgrade` to actually download and install all updated versions for the packages in the list.

Key Takeaways

Linux is a free open-source operating system used on a wide variety of computing systems.

- The kernel is a part of the operating system of Linux and runs communications between the computer's hardware and its processes.
- Unbuntu is the most popular distribution because it is easy to use and update with the update manager or the command sudo apt-get upgrade.
- As improvements to the processes are released, Linux needs to be updated to ensure the kernel communicates the right information to the hardware about the process.

In the `Windows Powershell` terminal, enter the following commands to download and install VLC media player.

```
$VLC_URL = "https://get.videolan.org/vlc/last/win64/"
```

```
$GET_HTML = Invoke-WebRequest $VLC_URL
```

```
$FILE = $GET_HTML.Links | Select-Object
@{Label='href';Expression={@{$true=$_.href}
[$_.href.EndsWith('win64.exe')]}} | Select-Object -
ExpandProperty href
```

```
$URL = ($VLC_URL+$FILE)
```

```
$DOWNLOAD_DIR = "C:\users\qwiklabs\Downloads\"
```

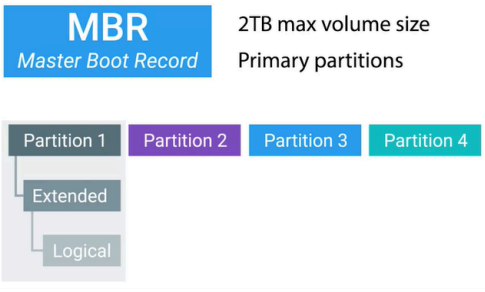
Resources for more information

Linux Foundation article. Ubuntu's guide here.

(Left) Install VLC w/ PowerShell?

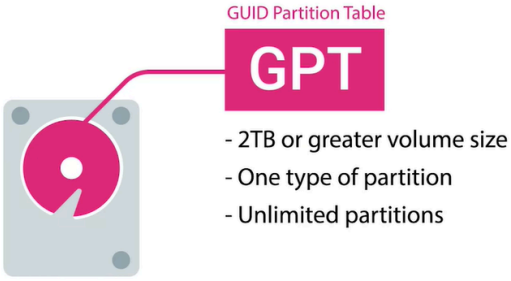
File Systems

Windows uses NTFS
Linux uses ext4
USBs with a NTFS file system can be read on Linux but ext4 isn't compatible with Windows.
Fat32 supports reading & writing to all 3 major operating systems.
Partition = Part of the disk you can manage. They act
Volume = a formatted partition.
Partition Table = Tells the OS how the disk is partitioned.
Master Boot Record (MBR) and GUID Partition Table (GPT) are most common Partition Table Schemes.



MBR is fading out.

UEFI Booting is dependent on GUID Partition Table



How to Format a Filesystem

Windows: In the Computer Management console under "Storage Tab" in "Disk Management"

Allocation Unit Size is the size of memory blocks. Big files will need bigger blocks, and more space will be saved with smaller files if you use smaller blocks.

Difference between quick format and full format is on a full format Windows will spend extra time scanning the integrity and checking for errors.

Disk Partitioning and Formatting in Windows

Disk partitioning enables more efficient management of hard disk space by breaking or "slicing" up the disk storage space into partitions. This breaking allows for each partition to be managed separately by reducing inefficient use of space. DiskPart is a disk partitioning utility on the Windows operating system which uses the command line to perform operations. This reading covers the component parts that make up a drive, common DiskPart commands, and how cluster size affects your usable drive space in the Windows OS.

DiskPart

The DiskPart command terminal helps you manage storage on your computer's drives. DiskPart utility can be used to manage partitions of hard disks including creating, deleting, merging, or expanding partitions and volumes. It can also be used to assign a file formatting system to a partition or volume.

There are three main divisions of storage that you will find on a drive: cluster, volume, and partition.

- **Cluster** (allocation unit size) is the minimum amount of space a file can take up in a volume or drive.
- **Volume** is a single accessible storage area with a single file system; this can be across a single disk or multiple.
- **Partition** is a logical division of a hard disk that can create unique spaces on a single drive. Generally used for allowing multiple operating systems.

To use DiskPart you will need to use specific commands to select and manage the parts of your drive you need to access. For a list of common DiskPart terminal commands visit this helpful guide.

The commands let you work with partitions and volumes but the base storage unit called cluster size is set when initiating the volume or partition.

Cluster Size

Cluster size is the smallest division of storage possible in a drive. Cluster size is important because a file will take up the entire size of the cluster regardless of how much space it actually requires in the cluster.

For example, if the cluster size is 4kb (the default size for many formats and sizes) and the file you're trying to store is 4.1kb, that file will take up 2 clusters. This means that the drive has effectively lost 3.9 kb of space for use on a single file.

When partitioning a disk, you should specify the cluster size based on your file sizes. If no cluster size is specified when you format a partition, a default is selected based on the size of the partition. Using defaults can result in loss of usable storage space.

It is important to remember when using DiskPart that the actions you take are permanent so be careful not to erase data accidentally.

Key Takeaways

DiskPart is a tool that lets you manage your storage from a command line interface and is useful for a multitude of actions including creating, deleting, merging, and repairing drives.

- The three main divisions of storage that you will find on a drive are cluster, volume, and partition.
- To use DiskPart you will need to use specific commands to select and manage the parts of your drive you need to access.
- Cluster size is the smallest division of storage possible in a drive. Cluster size is important because a file will take up the entire size of the cluster regardless of how much space it actually requires in the cluster.

Don’t forget to mount/ unmount external filesystems!

File systems gotta be mounted to a directory to work.

To make a device automatically mount a device you need to put the UUID into the /etc/fstab directory.

Use sudo blkid to list UUIDs of connected storage devices.

Mounting and Unmounting a File System in Linux

In this reading, you will learn how to mount and unmount file systems in Linux using the **fstab** table. IT Support professionals who work with Linux systems should know how to mount and unmount file systems both manually and automatically. This skill is often used when configuring Linux servers and other Linux systems to connect to network file systems.

File system table (fstab)

File System Table (**fstab**) is a Linux configuration table. It helps to simplify mounting and unmounting file systems in Linux. Mounting means to connect a physical storage device (hard drives, CD/DVD drives, network shares) to a location, also called a mount point, in a file system table. In the past, IT Support specialists for Linux systems had to manually mount hard drives and file systems using the **mount** command. The **fstab** configuration file made this administrative task more efficient by offering the option to automate the mounting of partitions or file systems during the boot process. Additionally, **fstab** allows for customized rules for mounting individual file systems.

The **fstab** configuration table consists of six columns containing the following parameters:

Column 1 - Device:

- The universally unique identifier (UUID) or the name of the device to be mounted (sda1, sda2, … sda#).

Column 2 - Mount point:

- Names the directory location for mounting the device.

Column 3 - File system type:

- Linux file systems, such as ext2, ext3, ext4, JFS, JFS2, VFAT, NTFS, ReiserFS, UDF, swap, and more.

Column 4 - Options:

- List of mounting options in use, delimited by commas. See the next section titled “Fstab options” below for more information.

Column 5 - Backup operation or dump:

- This is an outdated method for making device or partition backups and command dumps. It should not be used. In the past, this column contained a binary code that signified:
  - **0** = turns off backups
  - **1** = turns on backups

Column 6 - File system check (fsck) order or Pass:

- The order in which the mounted device should be checked by the **fsck** utility:
  - 0 = fsck should not run a check on the file system.
  - 1 = mounted device is the root file system and should be checked by the **fsck** command first.
  - 2 = mounted device is a disk partition, which should be checked by **fsck** command after the root file system.

Example of an **fstab** table:

<File System>	<Mount Point>	<Type>	<Options>	<Dump>	<Pass>
/dev/sda1	/	ext3	nouser	0	1
/dev/sda2	swap	swap	defaults	0	0
/dav/hda1	/mnt/shared	nfs	rw, noexec	0	2

Fstab options

In Column 4 of the **fstab** table, the available options include:

- **sync or async** - Sets reading and writing to the file system to occur synchronously or asynchronously.
- **auto** - Automatically mounts the file system when booting.
- **noauto** - Prevents the file system from mounting automatically when booting.
- **dev or nodev** - Allows or prohibits the use of the device driver to mount the device.
- **exec or noexec** - Allows or prevents file system binaries from executing.
- **ro** - Mount file system as read-only.
- **rw** - Mount file system for read-write operations.
- **user** - Allows any user to mount the file system, but restricts which user can unmount the file system.
- **users** - Any user can mount the file system plus any user can unmount file system.
- **nouser** - The root user is the only role that can mount the file system (default setting).
- **defaults** - Use default settings, which include **rw**, **suid**, **dev**, **exec**, **auto**, **nouser**, **async**.

For more options, consult the **man** page for the file system in use.

Editing the fstab table

As an IT Support professional, you may need to expand the hard drive space on a server. Imagine that you have installed a new hard drive and the Linux server does not seem to recognize the drive. In the background, Linux

has detected the new hardware, but it does not know how to display information about the drive. So, you will need to add an entry in the **fstab** table so that Linux will know how to mount it and display its entry within the file system. The following steps will guide you through this process:

1. Format the drive using the **fdisk** command. Select a Linux compatible file system, like ext4. If needed, you can also create a partition on the drive with the **fdisk** command.
2. Find which block devices the Linux system has assigned to the new drive. The block device is a storage device (hard drive, DVD drive, etc.) that is registered as a file in the **/dev** directory. The device file provides an interface between the system and the attached device for read-write processes. Use the **lsblk** command to find the list of block devices that are connected to the system.

Example output from the **lsblk** command:

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sda	8:0	0	512G	0	disk	
└ sda1	8:1	0	1G	0	part	/boot
sdb	8:16	0	1T	0	disk	
└ sdb1	8:17	0	128G	0	part	

The seven columns in the output from the **lsblk** command are as follows:

a. **NAME** - Device names of the blocks. In this example, the device names are the existing **sda** drive and **sda1** partition plus the new **sdb** hard drive and a newly formatted **sdb1** partition.

b. **MAJ:MIN** - Major and minor code numbers for the device:

1. The major number is the driver type used for device communication. A few examples include:
   - **1** = RAM
   - **3** = IDE hard drive
   - **8** = SCSI hard drive
   - **9** = RAID metadisk
2. The minor number is an ID number used by the device driver for the major number type.
   - The minor numbers for the first hard drive can range from 0 to 15.
     a. The **0** minor number value for **sda** represents the physical drive.
     b. The **1** minor number value for **sda1** represents the first partition on the **sda** drive.
   - The minor numbers for the second hard drive can range from 16 to 31.
     a. The **16** minor number value for **sdb** represents the physical drive.
     b. The **17** minor number value for **sdb1** represents the first partition on the **sdb** drive.
   - Minor numbers for a third hard drive would range from 32 to 47, and so on.

c. **RM** - Indicates if the device is:

1. **0** = not removable

2. **1** = removable

d. **SIZE** - The amount of storage available on the device.

e. **RO** - Indicates file permissions:

1. **0** = read-write
2. **1** = read-only

f. **TYPE** - Lists the type of device, such as:

1. **disk** = hard drive
2. **part** = disk partition

g. **MOUNTPOINT** - The location where the device is mounted. A blank entry in this column means it is not mounted.

3. Use an editor, like gedit, to open the **fstab** file:

Example fstab file:

Device	Mount Point	File System	Options	Dump	Pass
/dev/sda1	/	ext3	nouser	0	1

4. To add the new file system partition:

1. In the first column, add the new file system device name. In this example, the device name would be **/dev/sdb1**.
2. In the second column, indicate the mount point for the new partition. This should be a directory that would be easy to find and identify for users. For the sake of simplicity, the mount point for this example is **/mnt/mystorage**.
3. In the third column, enter the file system used on the new partition. In this example, the file system used for the new partition is **ext4**.
4. In the fourth column, enter any options you would like to use. The most common option is to select **default**.
5. In the fifth column, set the dump file to 0. Dump files are no longer configured in the **fstab** file, but the column still exists.
6. In the sixth column, the pass value should be **2** because it is not the root file system and it is a best practice to run a file system check on boot.

7. Your **fstab** table should now include the new partition:

<File System>	<Mount Point>	<Type>	<Options>	<Dump>	<Pass>
/dev/sda1	/	ext3	nouser	0	1
/dev/sdb1	/mnt/mystorage	ext4	default	0	2

8. Reboot the computer and check the **mystorage** directory for the new partition.

Windows Swap Space

Swap space is the space used as virtual memory for programs.
https://www.coursera.org/learn/os-power-user/lecture/58R7e/windows-swap

Windows Paging Files

In this reading, you will learn about Windows paging files and their primary functions. You will also learn how to set the appropriate Windows paging file size. As an IT Support specialist, you may want to add or maintain page files to improve system performance. A paging file is an optional tool that uses hard drive space to supplement a system's RAM capacity. The paging file offloads data from RAM that has not been used recently by the system. Paging files can also be used for system crash dumps or to extend the system commit charge when the computer is in peak usage. However, paging files may not be necessary in systems with a large amount of RAM.

Page file sizing

Determining the size needed for a paging file depends on each system's unique needs and uses. Variables that have an impact on page file sizes include:

- System crash dump requirements - A system crash dump is generated when a system crashes. A page file can be allocated to accept the Memory.dmp. Crash dumps have several size options that can be useful for various troubleshooting purposes. The page file needs to be large enough to accept the size of the selected crash dump. If the page file is not large enough, the system will not be able to generate the crash dump file. If the system is configured to manage page dumps, the system will automatically size the page files based on the crash dump settings. There are multiple crash dump options. Two common options include:
    - **Small memory dump:** This setting will save the minimum amount of info needed to troubleshoot a system crash. The paging file must have at least 2 MB of hard drive space allocated to it on the boot volume of the Windows system. It should also be configured to generate a new page file for each system crash to save a record of system problems. This history is stored in the Small Dump Directory which is located in the %SystemRoot%\Minidump file path.
        - To configure a small memory dump file, run the following command using the cmd utility:

Wmic recoveros set **DebugInfoType** = 3

- Alternatively, this option can be configured in the registry:

Set the **CrashDumpEnabled** DWORD value to 3

- To set a folder as the Small Dump Directory, use the following command line:

Wmic recoveros set **MiniDumpDirectory** = <folderpath>

- Alternatively, the directory option can be set in the registry:

Set the **MinidumpDir Expandable String Value** to <folderpath>

- **Complete memory dump:** The option records the contents of system memory when the computer stops unexpectedly. This option isn't available on computers that have 2 or more GB of RAM. If you select this option, you must have a paging file on the boot volume that is sufficient to hold all the physical RAM plus 1 MB. The file is stored as specified in %SystemRoot%\Memory.dmp by default. The extra megabyte is required for a complete memory dump file because Windows writes a header in addition to dumping the memory contents. The header contains a crash dump signature and specifies the values of some kernel variables. The header information doesn't require a full megabyte of space, but Windows sizes your paging file in increments of megabytes.
    - To configure a complete memory dump file, run the following command using the cmd utility:

wmic recoveros set **DebugInfoType** = 1

- Alternatively, a complete memory dump file can be configured in the registry:

Set the **CrashDumpEnabled** DWORD value to 1

- To set a memory dump file, use the following command line:

wmic recoveros set **DebugFilePath =** <folderpath>

- Alternatively, the memory dump file can be set in the registry:

Set the **DumpFile Expandable String Value** to <folderpath>

- To indicate that the system should not overwrite kernel memory dumps or other complete memory dumps, which may be valuable for troubleshooting system problems, use the command:

wmic recoveros set **OverwriteExistingDebugFile** = 0

- Alternatively, the overwrite setting can be turned off in the registry:
    - Set the **Overwrite** DWORD value to 0
- Peak usage or expected peak usage of the system commit charge - The system commit limit is the total of RAM plus the amount of disk space reserved for paging files. The system commit charge must be equal to or less than the system commit limit. If a page file is not in place, then the system commit limit is less than the system's RAM amount. The purpose of these measurements is to prevent the system from overpromising available memory. If this system commit limit is exceeded, Windows or the applications in use may stop functioning properly. So, it is a best practice to assess the amount of disk storage allocated to the page files periodically to ensure there is sufficient space for what the system needs during peak usage. It is fine to reserve 128 GB or more for the page files, if there is sufficient space on the hard drive to dedicate a reserve of this size. However, it might be a waste of available storage space if the system only needs a small fraction of the reserved disk space. If disk space is low, then consider adding more RAM, more hard drive storage, or offload non-system files to network or cloud storage.
- Space needed to offload data from RAM - Page files can serve to store modified pages that are not currently in use. This keeps the information easily accessible in case it is needed again by the system, without overburdening RAM storage. The modified pages to be stored on the hard drive are recorded in the **\Memory\Modified Page List Bytes** directory. If the page file is not large enough, some of the pages added to the Modified Page List Bytes might not be written to the page file. If this happens, the page file

either needs to be expanded or additional page filles should be added to the system. To assess if the page file is too small, the following conditions must be true:

- \Memory\Available MBytes indicates more physical memory is needed.
- A significant amount of memory exists in the modified page list.
- \Paging Files(*)% Usage (existing page files) are almost full.

Linux Swap Space

https://www.coursera.org/learn/os-power-user/lecture/WIEEL/linux-swap

Process Management

All processes have a parent. In linux, that process is **init** and its PID is 1

When Windows boots up or starts, the first non kernel and user mode that starts as the Session Manager Subsystem or smss.exe. The smss.exe process is in charge of setting some stuff up for the OS to work. It then kicks off the login process called windlogon.exe appropriately enough. Along with the client server runtime subsystem called csrss.exe, which handles running the Windows GUI and command-line console.

Use taskkill to kill a command
“Windows processes can operate independent of their parents. Linux has a parent-child relationship.”

Init starts the processes in linux needed for the rest of the computer.
Get WIndows PID from Task Manager under details or tasklist (cmd.exe) and Get-Process (PowerShell)
ps in Linux shell shows running processes

- R: running
- T: stopped
- S: interruptible sleep

← Linux process statuses

To view the files that correspond to processes, we can look into the /proc directory.

A signal is a way to tell a process that something's just happened.

One of the most common signals you'll come across is called SIGINT, which stands for signal interrupt.
The SIGINT signal is sent when you hit CTRL+C during a command in both Windows and Linux

Process Explorer is a utility Microsoft created to let IT support specialist, systems administrators and other users look at running processes.
Downloadable from the Microsoft Website

The kill command sends a SIGTERM
kill -KILL will send a SIGKILL and not give the process time to clean up. Just die

Send a SIGTSTP signal to suspend a service with kill -tstp or Ctrl+z
Kill -CONT will continue a suspended process.

Resource Management

Windows has a “Resource Monitor” that shows details on your machine

Resource Monitoring in Linux

Balancing resources keeps a computer system running smoothly. When processes are using too many resources, operating problems may occur. To avoid problems from the overuse of resources, you should monitor the usage of resources. Monitoring resources and adjusting the balance is important to keep computers running at their best. This reading will cover how to monitor resources in Linux using the load average metric and the common command.

Load in Linux

In Linux, a **`load`** is the set of processes that a central processing unit (CPU) is currently running or waiting to run. A load for a system that is idle with no processes running or waiting to run is classified as a 0. Every process running or waiting to run adds a value of 1 to the load. This means if you have 3 applications running and 2 on the waitlist, the load is 5. The higher the load, the more resources are being used, and the more the load should be monitored to keep the system running smoothly.

Load average in Linux

The load as a measurement doesn't provide much information as it constantly changes as processes run. To account for this, an average is used to measure the load on the system. The load average is calculated by finding the load over a given period of time. Linux uses three decimal values to show the load over time instead of the percent other systems use. An easy way to check the load average is to run the **`uptime`** command in the terminal. The following image depicts the load values returned from the **`uptime`** command.

```
root@ubuntu : ~# uptime
   12:28:35 up 2 days, 16:26 ,1 user, load average: 0.03, 0.03, 0.01
root@ubuntu : ~#
```

The command returns three load averages:

1. **Average CPU load for last minute,** which corresponds to 0.03. This is a very low value and means an average of 3% of the CPU was used over the last minute.
2. **Average CPU load for last 5 minutes** corresponds to the second value of 0.03. Again, this can be thought of as, on average, 3% of the CPU was being used over the past five minutes.
3. **Average CPU load for last 15 minutes** corresponds to 0.01, meaning on average, 1% of the CPU has been used over the last 15 minutes.

Top

```
top  -  23:01:54 up 3 min,      1 user,      load average: 1.21, 0.57, 0.22
Tasks: 221 total,  2 running, 219 sleeping,  0 stopped,   0 zombie
%Cpu ( s ) : 94.7 us, 4.7 sy,   0.0 id,   0.0 wa,   0.7 hi,   0.0 si,   0.0 st
Mib Mem :       3898.5 total,      1737.0 free,    1142.0 used,    1019.5 buff / cache
Mib Swap :      3898.0 total,      3898.0 free,       0.0 used,    2509.6 avail Mem
```

Another way you can monitor the load average in Linux is to use the **`top`** (table of processes) command in the terminal. The result of running the top command is an in-depth view of the resources being used on your system.

The first line displayed is the same as the load average output given using the uptime command It lists what percent of the CPU is running processes or has processes waiting. The second line shows the task output and describes the status of processes in the system. The five states in the task output represent:

1. **Total** shows the sum of the processes from any state.
2. **Running** shows the number of processes currently handling requests, executing normally, and having CPU access.
3. **Sleeping** shows the number of processes awaiting resources in their normal state.
4. **Stopped** shows the number of processes ending and releasing resources. The stopped processes send a termination message to the **parent process**. The process created by the kernel in Linux is known as the "Parent Process." All the processes derived from the parent process are termed as "Child Processes."
5. **Zombie** shows the number of processes waiting for its parent process to release resources. Zombie processes usually mean an application or service didn't exit gracefully. Having a few zombie processes is not a problem.

The top command gives detailed insight on usage for an IT individual to gauge the availability of resources on a system.

Key Takeaways

Computers need to balance the resources used with the resources that are free. Ensuring that the CPU is not overused means that a system will run with few issues.

- The load in Linux is calculated by adding 1 for each process that is running or waiting to run.
- Monitoring the average load of Linux allows an IT professional to identify which processes are running to determine what to end in order to balance the system. A balanced system runs with fewer problems than one that is using too high of a percent of resources.
- The load average uses three time lengths to determine the use of the CPU: one minute, five minutes and fifteen minutes.

The `top` command can give detailed information about the resource usage of tasks that are running or waiting to run.

Remote Connections in Windows

Connecting securely to remote machines is an important task for deploying services. Secure Shell (SSH) was developed in the 1990s to address this issue. This reading will cover what SSH is, the features it enables, and common SSH clients and their key features in Windows.

SSH

Secure Shell (SSH) is a network protocol that gives users a secure way to access a computer over an unsecured network. SSH enables secure remote access to SSH-enabled network systems or devices and automated processes. It also allows for secure remote access to transfer files, use commands and manage network infrastructure.

OpenSSH

OpenSSH is the open-source version of the Secure Shell (SSH) tools used by administrators of Linux and other non-Windows for cross-platform remote systems management. OpenSSH has been added to Windows (as of autumn 2018) and is included in Windows Server and Windows client.

Common SSH Clients

An SSH client is a program that establishes secure and authenticated SSH connections to SSH servers. The following common SSH clients are Windows compatible:

PuTTY is a terminal emulator and the inspiration for all subsequent remote access systems.

- **Features:** This tool offers Telnet, SSH, Rlogin (A remote login tool for use with UNIX-based machines on your network), and raw socket connections plus Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP) for file transfers between two hosts.
- **Protocols**: SCP, SSH, Telnet, rlogin, and raw socket connection.

SecureCRT is a remote access system available for macOS, Linux, iOS, and Windows.

- **Features:** It offers terminal emulation and file transfer through an SSH tunnel. It enables connections through many protocols and has usability features like tabbed sessions and customizable menus.
- **Protocols**: SSH1, SSH2, Telnet, and Telnet/SSL

SmarTTY is a free SSH client with a multi-tabbed interface to allow multiple simultaneous connections.

- **Features:** This tool includes SCP capabilities for file transfers. It also includes usability features like auto-completion, file panel, and package management.

- **Protocols**: SSH and SCP

mRemoteNG is a remote desktop system with a tabbed interface for multiple simultaneous connections.

- **Features:** The system enables connections with Remote Desktop Protocol (RDP), Telnet (two-way text communication via virtual terminal connections), Rlogin, Virtual Network Computing (VNC, a graphics-based desktop sharing system), and SSH.
- **Protocols**: RDP, VNC, SSH, Telnet, HTTP/HTTPS, rlogin, Raw Socket Connections, Powershell remoting

MobaXterm is a remote access system built for Unix and Linux, and Windows.

- **Features:** Features include an embedded X server (a graphical interface akin to windows), X11 forwarding (a way to run applications over a remote connection), and easy display exportation to let X11 applications know which screen to run on.
- **Protocols**: SSH, X11, RDP, VNC

Key Takeaways

Secure Shell(SSH) is a way to securely connect two remote machines over an unsecured network.

- You can use SSH to remotely control, transfer files from, and manage network resources for SSH-enabled clients.
- OpenSSH is an open-source version for cross-platform management.
- There are many common Window-compatible SSH clients with various features to fit any need, including PuTTY, SecureCRT, SmarTTY, mRemoteNG, and MobaXterm.

Resources

- Download PuTTY
- Download SecureCRT
- Download SmarTTY
- Download mRemoteNG
- Download MobaXterm

Putty is the GUI client for SCP transfers on Windows.
Shared Folders are also done using SCP.

Virtual Machines

Virtualization creates a simulated computer environment for running a complete operating system (OS). The simulated computer environment is called a virtual machine (VM). On a VM, you can run an OS as if it were running directly on your physical hardware. This reading explains how virtual machines work and introduces some tools for creating a VM.

How VMs work

Virtual machine software creates a virtualized environment that behaves like a separate computer system. The VM runs in a window on the operating system of your physical computer. The operating system that runs on your physical computer is called the “host” OS. Any operating systems running inside a VM are called “guests.” In the virtual environment, you can install your guest OS, and it will function like it’s running on a physical machine. Whenever you want to use the guest OS, open your VM software and run the guest OS in a window on your host desktop.

Using a virtual machine lets you experiment with different operating systems without having to uninstall or replace your host OS. For example, you can try a Linux OS as a VM on your Windows computer to see how the two OSs compare, or you can use a VM on your Linux system to run a Mac software package.

Another advantage of VMs is that they are isolated from the rest of your system. Software running inside a VM doesn’t affect the host OS or other VMs on your system. This isolation makes VMs a safe place to test software even when there is a risk of negative effects on a system.

A key advantage of VMs is significant reduction in hardware and electricity costs. You can run many VMs on a single host by dividing available hardware resources among each virtualized environment. Modern computer hardware offers a lot of computing power in a single device. But a typical OS will require only a fraction of the computing resources available in a computer. This means you won't have to run those systems on several physical computers that are only partially used.

VM software divides hardware resources among virtualized environments by designating a portion of resources as virtual resources. When you create a VM you may be asked to specify the amount of physical hard drive space you want to set apart for your VM to use. The VM software will create a virtual hard drive for your VM of the specified size. VM software may have you also specify the amount of RAM you want to allocate for your VM. After you create the VM, you can usually adjust resource allocations. If you want more drive space or RAM for your VM, you can adjust the settings in the VM software to allocate more of those resources.

VM software

Some common Virtual Machine software used to create VMs:

- **VirtualBox** runs on Windows, Linux, Macintosh, and Solaris hosts. VirtualBox supports various guest operating systems, including Windows, Linux, Solaris, OpenBSD, and macOS. VirtualBox is open-source software available for free on the VirtualBox download page.
- **Hyper-V** is Microsoft's virtualization platform. It is available as an integrated feature on the Windows operating system. Hyper-V supports Windows, Linux, and FreeBSD virtual machines. It does not support macOS. See Microsoft's Hyper-V for Windows documentation for information on how to access Hyper-V on recent versions of Windows.
- **VMware** desktop software runs on Windows, Linux, and macOS hosts. VMware Workstation Player is the VMware software that lets users run multiple operating systems on a single physical personal computer. It is freely available for non-commercial use on the VMware Workstation Download page.
- **Red Hat Virtualization (RHV)** is a business-oriented platform developed for virtualization in enterprise computing contexts. RHV supports a variety of guest systems. Red Hat charges an annual subscription fee for product access, updates, patches, and technical support. See Red Hat's RHV Datasheet for information on how to implement RHV on existing hardware infrastructures.

Key takeaways

Virtualization lets you create a simulated computer environment for running a complete operating system.

- Virtual machine (VM) software creates a virtualized environment that behaves like a separate computer system.
- Virtualization lets you experiment with different operating systems without having to uninstall or replace your host OS and provides a safe place to test software.
- VM software divides hardware resources among virtualized environments by allocating portions of available resources as virtual resources.
- A variety of Virtual Machine software are available for creating VMs.

More resources

For step-by-step instructions on how to create a virtual machine using VirtualBox, see the VirtualBox manual.

Logs

Windows stores logs in the **"Event Viewer"** (eventvwr.msc)

Linux logs are in /var/log (/var means variable, so things that change often go into /var)
/var/log/syslog should contain basically every event except off events.

If you're tryna find an error in a log, search "error"
If the issue's with a certain program, search or grep the program
REMEMBER WHEN WORKING WITH LOGS TO START WITH THE **FIRST** ERROR that cascaded the rest.

OS Deployment Methods

In this reading, you will learn about operating system (OS) deployment methods, including the use of disk cloning. A cloned disk is an identical copy of a hard drive. Cloning is often used when an Enterprise company purchases a large number of identical computers. The IT Support Administrators for the company are responsible for installing and configuring the computers to meet the needs of the company and its network. Disk cloning is used to save time on this type of deployment. IT Administrators will select one of the new computers to install and configure needed items, such as the OS, utilities, tools, network settings, software, drivers, firmware, and more. Then they make a clone of this first hard drive. The cloned disk is used to copy the entire disk image over to the remaining new computers so that the IT Admins do not need to repeat the same installation and configuration steps on each new computer. They may keep a copy of the original disk from this deployment to reimage the systems if a clean OS install is required (e.g., following a virus or malware infection, OS corruption, etc.).

Cloned disks have uses beyond deploying OSs. They can be used to test new software and configurations in a lab environment before applying the updates to similar production systems. Cloning can also be used for system migrations, data backups, disk archival, or to make a copy of a hard drive for investigative or auditing purposes.

Hard disk duplicator

Hard drive duplicators are machines that can make identical copies of hard drives. The original drive is inserted into the duplicator machine along with one or more blank hard drives as targets. Disk duplicators can have anywhere from a single target bay for limited disk cloning (example use: law enforcement investigations) up to 100+ target bays for industrial use (example use: computer manufacturing). If the target drives are not blank, the duplicator machine can wipe the drives. The target drives usually need to share the same characteristics (e.g., interface, form factor, transfer rate) of the original drive. The targets should also have the same or greater storage capacity than the original.

The hard drive duplicator may have an LCD interface built-in to the machine and/or a management software/HTML interface, the latter of which can be accessed over a networked or directly-connected computer or server. The duplicator interface can be used to initiate and manage disk cloning and/or disk wiping (reformatting). Most duplicators copy data sector-by-sector. The time to transfer data from the original to the target drives depends on multiple variables. The machine's user manual should be consulted to calculate duplication time.

Disk cloning software

Hard drives can also be cloned using software. This method allows the original and target to be different media from one another. For example, a hard drive can be cloned from an IDE drive to an SSD drive, a CD-ROM/DVD, removable USB drive, cloud-based systems, or other storage media, and vice versa. Software cloning supports full disk copies (including the OS, all settings, software, and data) or copies of selected partitions of the drive (useful for data-only or OS-only copies). Disk cloning software is often used by IT Administrators who need to deploy disk images across a network to target workstations or to cloud-based systems. Cloud platforms normally offer a virtual machine (VM) cloning tool as part of their services. VM cloning is the most efficient method for cloning servers and workstations. VM cloning takes a few seconds to deploy new systems.

A few examples of disk cloning software include:

- **NinjaOne Backup** - Cloud-based cloning, backup, and data recovery service designed for managed service providers (MSPs) and remote workplaces.
- **Acronis Cyber Protect Home Office** - Desktop and mobile device cloning software that works with Windows, Apple, and Android systems. Designed for end users. Supports backup, recovery, data migration, and disk replication. Includes an anti-malware service that can overcome ransomware attacks.
- **Barracuda Intronis Backup** - Cloud-based cloning and backup service on a SaaS platform. Designed for MSPs who support small to mid-sized businesses. Can integrate with professional services automation (PSA) and remote monitoring and management (RMM) packages.
- **ManageEngine OS Deployer** - Software for replications, migrations, standardizing system configurations, security, and more. Can create images of Windows, macOS, and Linux operating systems with all drivers, system configurations, and user profiles. These images can be saved to a locally stored library. The library is available to deploy OSs to new, migrated, or recovered systems as needed.

- **EaseUS Todo Backup** - Free Windows-compatible software for differential, incremental, and full backups, as well as disaster recovery. Supports copying from NAS, RAID, and USB drives.

Methods for deploying disk clones

The sections above have described disk clone deployment through copied hard drives, image libraries, network storage, and cloud-based deployments. There are some other options for cloned disk deployments:

Flash drive distribution

OSs can be distributed on flash drives. IT professionals can format flash drives to be bootable prior to copying a cloned disk image to the flash drive. Target systems should be set to boot from removable media in the BIOS. After inserting a flash drive containing the OS into an individual computer, restart the system and follow the prompts to install the OS. Microsoft offers this method as an option for Windows installations. Linux systems can also be booted and installed from flash drives.

The Linux dd command

The Linux/Unix dd command is a built-in utility for converting and copying files. On Linux/Unix-based OSs, most items are treated as files, including block (storage) devices. This characteristic makes it possible for the dd command to clone and wipe disks.

Key takeaways

Hard drives can be duplicated by:

- Hard disk duplicator machines
- Disk cloning software. Examples:
    - NinjaOne Backup
    - Acronis Cyber Protect Home Office
    - Barracuda Intronis Backup
    - ManageEngine OS Deployer
    - EaseUS Todo Backup

Operating systems can be deployed through:

- Cloned hard drives
- Hard drive image libraries
- Network storage
- Cloud-based deployments
- Flash drive distributions
- In Linux, using the dd command

More:

- How to clone a hard drive on Windows - Step-by-step guide with screenshots on how to clone a hard drive using the software Macrium Reflect Free.
- Best Hard Drive Duplicator/Cloner Docking Station for 2022 - Comparison guide to popular hard drive duplicator machines.
- OS deployment methods with Configuration Manager - Microsoft's guide to options for deploying Windows in a network environment.
- dd(1) - Linux manual page - The manual for the Linux dd command, which describes how to use the command and lists the available optional flags.

Windows Troubleshooting

In an IT support environment, it's common to come across issues that you can resolve using the log analysis tools. These tools can help with application crashes, a slow boot or startup, application hangs, or unexpected reboots. In this reading you will learn how to resolve application crashes through the Windows' graphical user interface (GUI) and your system log files.

Solving the problem

When you begin to troubleshoot an IT issue, you should begin by researching the root of the problem.You might ask yourself these questions:

- Is the problem unique to one computer or all computers on the network?
- Does the problem affect a single user or all users?
- Is the problem related to a particular application? Is that application up-to-date?

Information in your system and application logs can help you answer these questions.

Once you have figured out the problem, decide how you are going to fix it. You first attempt at fixing it might not be the right solution. This is okay and you are keeping the problem-solving process moving forward and helping to develop your technical troubleshooting skills.

After you have solved the issue and have figured out how to fix it, educate others on your team and in your company about what you discovered. Educating others about IT issues that are happening will help prevent them from happening again.

It's also important to document your solution to a problem. Many organizations have a structured documentation process in place for IT. This documentation is a place for you to record the issues you have encountered and the solutions you discovered. If they don't already have a documentation system, it is an opportunity to create a documentation system for your company and follow it. Documenting issues that arise, and solutions to those issues, will save the company and other IT support professionals time and resources in the future.

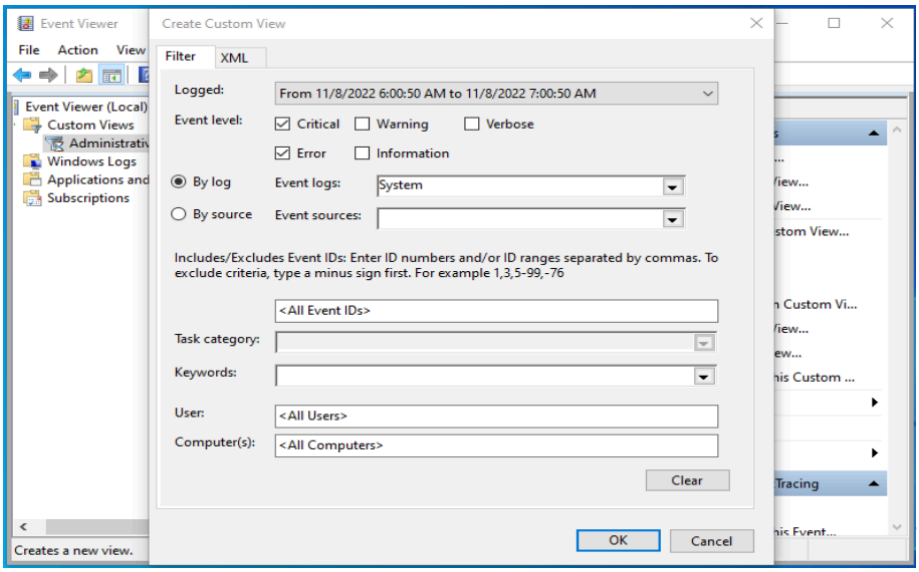
An example scenario

Consider this situation: One of the commonly-used software applications at your company continuously crashes around the same time every day. You use information in the Windows log files to investigate the issue and see events as they happen live. There are several types of logs you may analyze. A good way to start is by analyzing the system and application logs.

Accessing logs through the Windows GUI tool

In Windows you can access logs through the GUI using the Event Viewer tool. You can launch the Event Viewer through the Windows start menus or by typing eventvwr.msc from the run box. The Event Viewer records a lot of information about the system. With a custom view, you can create a filter that will look across all the event logs and focus the view on just the information you're interested in.

In the scenario above, you're interested in a crash event that happens around the same time every day. You may create a custom view to filter only events that happen around the time of your crash event. Select the "error" and "critical" checkboxes to limit the view to include crash events. You can also select specific logs to view. The system log is a good place to start. Name the new view and save it for future reference.



Interpreting the log file

Once you have accessed your logs and focused on those parts that contain information most relevant to your crash event, you can examine the logs to find the root cause of the issue. Since you're concerned with the crash of a specific application, you might scan the log file for the word "error" or the application name.

Check the timestamps of these error logs for crashes that happen around the time that you suspect your crashes are happening. These parts of your system logs are most likely to offer clues about what's causing your problem and how to fix it.

You may have to examine the logs a few times to collect the data you need. You may also have to try multiple different solutions before finding the right one. Then once you have, you can document it so others don't have to go through the same process again.

Key takeaways

Good problem solving skills will help expedite the troubleshooting process and increase productivity.

- When faced with a problem, analyze the situation to determine what steps to take.
- There are two key tools that can help you resolve application errors:

1. Access to logs through the Windows GUI

2. Log analysis

- After reaching your conclusions about a problem, communicate your findings.
- Document your solution to every problem.

Windows Troubleshooting Tools

In this reading, you will learn some basic steps for troubleshooting the Windows operating system (OS). This article focuses primarily on troubleshooting tools available in the desktop/laptop versions of Windows 10 and 11. However, many of these tools and solutions are available in other versions of Windows. Additionally, there are multiple methods for approaching and solving problems in Windows. This article is not an extensive resource of all possible troubleshooting tools and solutions.

Troubleshooting tools for Windows

Some of the troubleshooting tools provided by Windows include:

- **Windows Update:** One of the most important repair tools for Windows problems. Widespread and known Windows problems will often have a software resolution provided by Microsoft or Original Equipment Manufacturers (OEMs). Windows Update will find, download, and install the required and/or recommended software resolutions, which include operating system patches and updates, security updates and fixes, .NET framework updates, driver and firmware updates, etc.
- **Updates from the hardware manufacturer(s)**: Some OEM updates are not accessible through Windows Update. For these items, it is necessary to go to the OEM's website for updates, patches, drivers, and firmware for components such as computer hardware, peripherals, and third-party applications.
- **Optimize Drives with Disk Defragmenter:** When files on a hard drive are saved, deleted, or altered, fragmentation across storage blocks can occur. A file may become spread across the drive in non-contiguous storage blocks. This issue results in performance problems within the system as the hard drive spends additional seek time finding the scattered file fragments and piecing them back together. The Windows Disk Defragmenter can automatically relocate file fragments onto a continuous series of storage blocks in order to remedy these seek time delays.
- **Disk Cleanup:** Windows utility that simplifies removing temporary files including downloaded program files, thumbnail files, system files, and temporary internet files. Disk Cleanup also offers an option to compress the primary hard drive where the Windows OS resides.
- **CHKDSK command:** A command-line utility for Windows that scans hard drives to find and flag bad sectors. Flagged bad sectors will be removed from use and no data will be stored on them. The tool will attempt to recover any data found on the bad sector.
- **Disk Management tool:** A Windows system utility for performing advanced storage management tasks, including initializing a new drive, extending or shrinking a volume, and changing a drive letter.

- **Event Viewer:** Software tool for monitoring events and errors produced by the system, security, hardware, software, and more. The Event Viewer divides logs into four main categories:
    - Custom Views
    - Windows Logs
    - Applications and Services Logs
    - Subscriptions
- **Registry Editor (regedit):** The Registry Editor should only be used by advanced system administrators. It is possible to cause serious system and software problems if the wrong edits are made to the Registry.
- **System Configuration tool (msconfig):** Software tool for changing system settings, including the services and applications that can load on system startup.
- **Safe Mode (Windows 10 and 11):** There are multiple options for booting into safe mode. A couple of these options include:
    - **System Configuration tool** - Can be used to configure a clean boot in Safe Mode to help isolate the source of a system problem.
    - **Startup Settings** - Can be accessed through **System > Recovery** or through the sign-in screen.
- **System Troubleshoot tool (Windows 11):** The Windows Troubleshoot menu can be accessed from **Start > Settings > System > Troubleshoot**. The following options are available on the Troubleshoot menu:
    - **Recommended troubleshooter preferences** - Set preferences for Microsoft's recommendations for troubleshooting tools.
    - **Recommended troubleshooter history** - Easy access to troubleshooting tools used previously.
    - **Other troubleshooters** - This menu includes tools for troubleshooting internet connections, audio, printers, Windows Update, Bluetooth, camera, incoming connections, keyboard, network adapter, power, program compatibility, search & indexing, shared folders, video, Windows Store apps, privacy, and misc help.

Common problems in Windows

The following is a list of common problems encountered in Windows, along with common troubleshooting first steps:

- **Computer is running slowly:** There are many issues that could make a computer run slowly. Troubleshooting can involve multiple steps, many of which should be performed on a regular schedule to proactively prevent problems from happening. The first step should almost always be to reboot the computer. This step can fix a large percentage of problems reported by end users. If rebooting does not resolve the problem, check that there is sufficient processing power, disk space, and RAM to support the OS, hardware, software, and intended use of the computer. For example, video editing may require a relatively more powerful computer, a large amount of free hard drive space, and lots of RAM. Check system event logs for errors. Research any error codes found using the Microsoft knowledge base or an internet search to see if there is a known solution to the problem. Run an antivirus and anti-malware scan. Use Windows Update and OEM updates to ensure the system is up to date. Remove temporary and unneeded files and software. Check the software and services that load at startup for potential problem sources. Reboot the computer into Safe Mode to see if the computer performance improves. Unplug peripherals and turn off network connections to eliminate these as sources of the slow down. If the OS is Windows 11, use the System Troubleshoot tools found at **Start > Settings > System > Troubleshoot.**
- **Computer is frozen:** Power off the computer. Wait 30 seconds to drain residual power and clear any potentially corrupted data held by RAM. Boot up the computer again and check system event logs. If the system does not boot, go to the BIOS settings and boot into Safe Mode to gain access to the event logs. Research any error codes found. If the root cause cannot be determined, run the same checks as listed above for "Computer is running slowly".
- **Blue screen errors:** If the blue screen provides an error code or QR code, record this information in order to research the root cause of the issue and possible solutions. Power off the computer, wait 30 seconds, then boot the computer again. If the system does not boot, go into the BIOS settings to boot into Safe Mode. Obtain system event logs in the Windows Event Viewer and research any error codes found there. If the root cause cannot be determined through event codes within the logs, then run the same checks as listed above for "Computer is running slowly".

- **Hardware problems:** Check the hardware OEM's website for updates to drivers, firmware, and software management consoles. If this does not resolve the problem, check the system Device Manager to see if the device has been disabled or is not recognized. Additionally, check system event logs and research any error codes found. If the root cause cannot be determined, then run the same checks as listed above for "Computer is running slowly".
- **Software problems:** Go to the software manufacturer's website to check for software patches or updates. If the problem continues after updating the software, check the application event logs and research any error codes found. If the root cause cannot be determined, then run the same checks as listed above for "Computer is running slowly".
- **Application is frozen:** End application processes in Task Manager. Restart application. If the problem persists, reboot the computer and try to run the application again. If the issue is still not resolved, then follow the instructions listed above for software problems.
- **A peripheral is not working:** Check to ensure the peripheral is on and is receiving sufficient power, especially if the item is battery powered. Check cables to ensure they are attached securely. If the item is connected through USB, try a different USB port. If the device connects through Bluetooth, check to ensure that Bluetooth is active on both the computer and the peripheral. Reboot the computer to see if the system can reconnect to the device. Inexpensive, high-use peripheral devices experience high failure rates, especially keyboards and mice. Swap the peripheral for a working replacement to see if the problem was the peripheral itself, or perhaps an error in how the computer is detecting the peripheral. If the problem persists with the replacement peripheral, check the system Device Manager to see if the device has been disabled or is not recognized. Check the event logs for any errors. Visit the OEM's website to look for updates to drivers, firmware, and/or software management consoles, if available. Run a Windows Update as well.
- **Audio problems:** Check audio volume. Run the Windows audio troubleshooter. Check speaker cables, plugs, jacks, and/or headphones. Check sound settings. Update or repair audio drivers and sound card firmware. Check to ensure the active and default audio devices are the desired audio devices. Turn off audio enhancements. Stop and restart audio services in Task Manager. Restart the computer. Research if specific audio CODECs are needed for audio media. If audio is not working in a browser, ensure the browser has permission to use the system audio and/or microphone.

Resources

- Windows Server performance troubleshooting documentation - Microsoft list of articles on common Windows Server errors, troubleshooting, and solutions.
- How to scan and repair disks with Windows 10 Check Disk - Instructions for using the CHKDSK command.
- Overview of Disk Management - Lists uses for the Windows Disk Management system utility, along with links to step-by-step instructions for using the utility.
- How to use Event Viewer on Windows 10 - A walkthrough tour of Windows Event Viewer with screenshots and detailed explanations of each part of the tool.
- Registry - Microsoft article about the Windows Registry.
- How to use System Configuration tool on Windows 10 - Tutorial for using the Windows System Configuration tool.

Example Troubleshooting a problem in Windows

As an IT Support professional, you will likely run into problems caused by a full primary hard drive, where the OS is installed. An affected computer may display an error message stating there is insufficient space on the drive to save new files, apply an update, or install new software. In some cases, the computer might not provide an informative error message at all. Instead, the system may experience performance issues, hang, crash, or it might not even load the OS after booting. Note that it is a best practice to routinely perform maintenance and clean-up of computer hard drives to free storage space, improve system performance, and prevent the myriad of issues that can arise when the primary hard drive is full.

Imagine that you are an IT Support Specialist for an organization. An employee reports that their computer is running very slowly and keeps hanging. You know that Windows Update had been scheduled to run overnight to update all of the organization's systems with multiple patches, updates, and fixes. Although it is possible for

these changes to cause system problems, there is only one employee reporting a problem. So, it is more likely that the system did not have adequate storage space to install all of the updates on that employee's computer system. You suspect that the primary hard drive could be full. Your troubleshooting and repair steps might include:

1. **Check how much free storage space remains.** A quick and easy troubleshooting step for system performance issues is to check if the primary hard drive is full. In this scenario, you discover that the employee's hard drive has less than 5 GB of space left. Microsoft recommends giving Windows 10 at least 20 GB of free space for normal OS processes. You will need to find at least 15 GB of files to delete or move to another storage location.
2. **Delete temporary and unneeded files.** There are a few methods for cleaning out junk files from Windows. Two system maintenance tools for this purpose, found in several versions of Windows, include:
    a. **Storage Sense:** Use the Windows Storage Sense tool to delete unnecessary files like temporary files, offline cloud files, downloads, and those stored in the Recycle Bin. You can also configure Storage Sense to regularly and automatically clean the hard drive for proactive maintenance.
    b. **Disk Cleanup:** A simple alternative tool to Storage Sense. Disk Cleanup performs most of the same operations as Storage Sense, plus it offers a drive compression utility. Note: If you run Disk Cleanup on a drive, but the computer is still reporting "Low Disk Space", the Temp folder is most likely filling up with Microsoft Store .appx files. In this case, you will need to clear the cache for Microsoft Store.
3. **Reset Windows Update.** Since you know the employee's computer went through a Windows Update overnight and possibly did not complete this process fully, it may be wise to perform a Windows Update reset. The reset tool can check whether a system reboot is required to apply the updates, security settings were changed, update files are missing or corrupted, service registrations are missing or corrupt, and more.This utility can be found in the Windows system **Settings** menu, under **Troubleshoot > Other troubleshooters > Windows Update**.
4. **Move files off of the primary hard drive and onto** (one or more of the following)**:**
    a. **Internal or external storage device:** Install an additional hard drive or add an external storage device, like a USB drive or SD card, to hold user files.
    b. **Network storage:** Network storage space is often available in network environments in the form of Network Attached Storage (NAS) appliances or large Enterprise Storage Area Networks (SANs). In these environments, end users should have network drive space mapped to their workstations for file storage, instead of saving files to their local hard drives.
    c. **Cloud storage** (OneDrive, File Explorer, Google Drive, etc.)**:** Providing cloud storage space to end users is a lower cost alternative to network storage. However, this option is less secure than onsite NAS or SAN storage.

In Windows **System Storage**, under **Advanced storage settings**, set the new drive storage as the destination for "Where new content is saved."

1. **Set any cloud storage solutions to be online-only.** This will prevent cloud files from downloading an offline or cached version of the files to the hard drive.
2. **Uninstall apps that are not needed** (including Windows Store apps)**.** This is an effective way to free up large amounts of storage space.
3. **Run antivirus and antimalware software.** Some viruses and malware intentionally fill up hard drives with garbage data.
4. **Wipe hard drive and reinstall the OS.** If none of the suggestions listed above solve the problem with slow system performance and hanging, consider wiping the hard drive and reinstalling the OS. This is the best method for repairing failed system updates.

Resources

- Free up drive space in Windows - Microsoft article for Windows 10 and 11 that provides step-by-step instructions for freeing storage space on a hard drive.
- Low Disk Space error due to a full Temp folder - Steps to clear the cache for Microsoft Store and reset Windows Update for Windows 10 and 11.
- Manage drive space with Storage Sense - Instructions for configuring this Windows tool to automatically remove temporary files, downloads, offline cloud files, and empty the Recycle Bin.

- How to use Event Viewer on Windows 10 - A walkthrough tour of Windows Event Viewer with screenshots and detailed explanations of each part of the tool.
- How do I reset Windows Update components? - Steps for troubleshooting problems with Windows Update.

Course #4: **System Administration and IT Infrastructure Services**

Change Management

(When you change things using admin privileges)

IT change management is a standardized process for planning, communicating, and implementing technical changes to information systems. IT Support professionals are often responsible for installations, updates, upgrades, migrations, etc. to an organization's software, hardware, network security policy, data storage policy, cloud platforms, and more. IT Support staff are expected to make these changes while also minimizing disruptions to the organization's IT services. By following IT change management best practices, IT Support professionals can create robust plans for change rollouts that protect business continuity. The change management plan is often reviewed by change board approvals, management teams, and/or project stakeholders for risk assessment, feedback, and plan approvals or rejections.

IT change management plans

Each organization will have their own change management policies, processes, and procedures. However, there are several common items that should be included in change management plans as a best practice. When proposing a change, IT professionals may create documentation or use change request forms to detail the following elements:

- **Person/team responsible for the change:** Names at least one person as the responsible party for overseeing the change management plan.
- **Change priority:** States the urgency of the change. For example, critical security patches would have a high priority and need to be scheduled ASAP. Whereas, a software update that merely adds new features might be a very low priority and can be scheduled for a convenient future date.
- **Change description:** Gives an overview of the planned changes. The change description should also provide a list of the planned changes. For example, if the change involves updating firmware on several router models, the description should include which routers and models will be updated. Additionally, the plan should list the old firmware versions currently on the routers along with the new firmware versions to be applied during the update.
- **Purpose of the change:** Explains why the change is necessary. For IT Support professionals, the most common reasons for changes are operating system, software, driver, and firmware patches and updates, as well as hardware and peripheral upgrades. Installations, implementations, and redesigns of software and hardware systems are also common IT changes. IT Support professionals should regularly evaluate the need for improvements and changes to network security policies and procedures. Laws, regulations, and company policies may also require changes to how organizations store, transmit, and protect data.
- **Scope of the change:** Describes the extent of the changes. The documentation should include a list of all IT systems (hardware, software, etc.), locations, departments, individuals, vendors, partners, customers, and others the changes affect, whether directly or indirectly. Any changes to policies, processes, or procedures should also be recorded.
- **Date, time, and duration of the change:** Indicates when the change is scheduled to take place and the duration of the change rollout. If the change is expected to create service outages, the person or team responsible for managing the change should inform all affected staff about the outage before the systems are taken offline. IT changes are often implemented outside of normal business hours, when systems can be taken offline with minimal disruption. For organizations with traditional Monday through Friday, 8 a.m. to 5 p.m. business hours, changes are usually planned to begin in the early evening on a Friday, after end users have logged out for the weekend. The change implementation process should include plenty of contingency time before the next business day in order to test, troubleshoot, repair, and roll-back any changes that are not successful. When an unsuccessful change occurs, IT Support professionals may need to work through the night and into the next morning. Organizations and IT departments may opt to

hire a vendor to perform overnight system changes to adhere to company overtime policies and labor laws.

- **Change rollback or backout plan:** In case of primary plan failures, details a rollback plan to return the affected systems back to their original state before the changes were attempted. Additionally, a secondary or alternative plan may be included. This could be a plan to activate a failover system to replace any problemed systems until they are repaired. IT Support professionals should detail the steps involved in the rollback and/or alternative plans, including the original configuration settings and software, patch, driver, and/or firmware versions. Files needed to rollback updates and patches should be downloaded and stored in an accessible location to simplify rollbacks. Cloud-based virtual systems can be restored in seconds by simply using clones of saved previous VM states.
- **Technical evaluation:** Records the results of any testing performed on the proposed changes in a lab or sandboxed environment. The testing environment should be as similar to the target environment as possible. For example, the same operating system versions, hardware parts, drivers, firmware, etc. of the target system should be reflected in the lab/sandbox testing environment. Setting up a testing sandbox for cloud platforms should be as simple as cloning the virtual system(s) targeted for updates. The plans should also include metrics for evaluating if a change is successful or not.
- **Systems affected by the change:** Lists all IT resources (including hardware, software, networked, and cloud systems) that will experience direct or indirect changes as a result of the change rollout.
- **Anticipated impact of changes:** Describes how the planned changes are expected to impact the affected systems. For example, if the change involves adding new servers to a resource pool, the plan might describe that this increase in load capacity will result in system performance improvements and faster server response times.
- **Resources needed to implement the change:** Lists the human resources, budget, time, management oversight, subject matter expert (SME) consultations, training, equipment, hardware, software, parts, systems, tools, insurance policies, and any other resource needed to complete the planned changes.
- **Training for users impacted by the change:** Outlines any training needs to help users adapt to the changes. This might include classes on how to use new software applications, hands-on practice with new hardware, a company-wide announcement for security procedure changes, and more.
- **Risk level for change:** Describes how much risk is involved in making the proposed changes. Some changes are high risk and might cause catastrophic failures if the plan goes wrong. For example, an upgrade involving a single point of failure on a critical system could create a system-wide outage. In this case, it would be wise to implement a redundant failover system for that critical system before attempting any other changes.
- **Change instructions:** Details each step of the planned changes. This should be formatted as an instruction manual for the IT Support professionals to follow to ensure there is no guesswork involved in implementing the changes.

Change board approvals

Some large organizations may have a Change Advisory Board (CAB). The CAB is a board of directors appointed to oversee all implemented IT changes in the organization. The CAB can be the official governing body to approve or deny change management plans. They may advise on needed adjustments to the plan to meet business goals or to comply with regulatory compliance criteria. The CAB may also assist with mitigating risk brought about by proposed changes.

User acceptance

Including a user acceptance process for information system changes is a best practice in IT change management. IT change management plans can include a beta testing period similar to software development user acceptance testing. This plan might include several days of testing by a select group of users to ensure that the changes have been successful and that there are no hidden surprises caused by the changes. The change management team for the plan should develop user acceptance criteria forms for the beta testers to complete. The criteria normally includes common activities that all end users should be able to perform successfully in the new or changed environment. A period of time should be reserved for fixing any problems the beta testers find. When beta testing is successful and the changes have been accepted/approved by the users, the changes should become available to all appropriate end users.

Recording your actions

When you are going to make changes in a machine, it's very important to have a clear plan of what you are going to do and to store the actions that you actually took.

A common practice for system administrators that work with bug queues or ticketing systems is to include the commands executed and the output obtained in the corresponding bug or ticket. This is recommended if the commands that need to be executed are few and straightforward.

However, there are situations where you don't yet know which commands exactly you'll need to execute because there's some investigation that needs to happen. In cases like that, it can be helpful to use a command like script for Linux or Start-Transcript for Windows.

script

In the case of script, you can call it like this:

```
script session.log
```

This will write the contents of your session to the session.log file. When you want to stop recording, you can write **exit** or press Ctrl-D. The generated file will be in ANSI format which includes the colors that were displayed on screen. In order to read them, you can use commands like ansi2txt or ansi2html to convert it to plain text or HTML respectively.

Start-Transcript

In the case of Start-Transcript, you can call it like this:

```
Start-Transcript -Path C:\Transcript.txt
```

This will write the contents of the session to C:\Transcript.txt. When you want to stop recording you need to call **Stop-Transcript**. The file created is a plain text file where the commands executed and their outputs are stored.

Recording Graphical Sessions

Performing system administration actions through a Graphical user interface is less common (as it's harder to automate and to perform remotely), but it's still something that may happen sometimes.

If you are going to be performing an action that needs to be done graphically and you can document what you are doing, you can use a specialized tool like recordMyDesktop for Linux, or general video tools like OBS or VLC.

Reproduction Phase (Roadmapping a user-end error)

Three questions to answer:

1. What steps did you take to get to this point?
2. What's the bad result?
3. What's the expected result?

Next, document your findings & steps taken to reach the expected result.
Remember: *Always fix things in a test environment before touching user systems.*

Week 2: IT Infrastructure Services

Pictures left: Diagram of Infrastructure as a s Service if you don't want to personally maintain some physical networking components, and rather them be managed by a 3rd party cloud.
You can also use **NaaS** for companies that don't want to spend a lot of money on networking hardware, so they send their stuff off shore.
Software **SaaS** like Office 365 (instead of manually installing a word processor on every individual machine) is an example of Software as a Service
PaaS (Platform as a service) like Heroku, Windows Azure and Google App Engine provide almost everything except the data and application ready for you to deploy thing onto
DaaS is Directory as a Service like Windows Active Directory and OpenLDAP that provide the service of managing user and authentication.

Remote connections

Previously, you learned about the fundamentals of remote access. In this reading, you will learn about various methods and tools for connecting remotely. You will also learn about some of the security risks related to using remote connections.

Remote connections can be used by IT Support professionals to troubleshoot remote systems. Remote systems may include laptops, PCs, workstations, servers, data center machines, and other IT equipment that supports remote access. Additionally, remote connections can be used for file transfers and terminal emulations. IT Support professionals often use remote access software to save time by eliminating the need to travel to the computer system's location.

Remote access software can also be used for remote and flexible work arrangements, which have been increasing in popularity in recent years. Numerous organizations have developed remote, hybrid, and flexible work opportunities to give employees the option to work from home. Through these arrangements, employers and employees have discovered the benefits of remote work. Employees save time and money by avoiding the commute to work. Employees also report an improvement in their work-life balance. Employers can save on the costs of maintaining physical offices. Employers can opt to expand their hiring pool far beyond their physical locations by hiring talent in other cities, regions, states, or even countries.

Multiple surveys have revealed that up to 95% of employers and employees in the United States would like to keep remote, hybrid, and/or flexible work options permanently. Recently, Microsoft reported that 66% of employers around the world are adapting their workplaces to support hybrid work models (see the Resources section at the bottom of this reading for more information). Given this workplace transformation, organizations are likely to ask IT Support professionals to design, configure, manage, and/or troubleshoot remote connections for business networks.

Remote access software for IT management

Unlike RDP and VPN, there are some types of remote access software that are typically used only by IT management and other computer support professionals. These remote applications help IT Support teams manage and monitor large networks more efficiently.

- **Secure Shell or Secure Socket Shell (SSH):** SSH is a network protocol and suite of tools that can be used to establish a secure connection between a computer and a private network over the internet. SSH is included with Linux/Unix and Mac Server operating systems. SSH provides identity and access management protocols through robust password authentication and public key authentication. SSH also encrypts data transmissions over the internet. Sessions are established by using an SSH client application to connect to an SSH server. For security, SSH keys are used to provide single sign-on (SSO) services and to automate access to servers for running scripts, backups, and configuration tools. SSH is primarily used by IT Support professionals to remotely manage file transfers and terminal emulators on Linux/Unix systems. For example, IT Support staff can use the SSH network protocol tool to establish an encrypted tunnel from their computer to a remote server over a network. The SSH file transfer tool can then be used to transfer a file, like a firmware update package, to the remote server. Finally, the SSH terminal emulator can be used to issue command lines to install the firmware onto the remote server.

- **Remote Monitoring and Management (RMM):** RMM is used by IT Support professionals to remotely monitor and manage information systems. Implementing RMM involves installing an RMM agent on each endpoint within a network, including servers, workstations, and mobile devices. The agents then send periodic status reports about the health of each endpoint to IT Support staff. RMM tools also help IT Support professionals proactively maintain the network by facilitating the remote installation of security patches and updates. If a problem occurs on an endpoint, the RMM agent will create a ticket, classify the problem type and severity, and then forward the ticket to IT Support staff. RMM systems enable IT Support providers to improve efficiency in information systems management. IT Support providers can manage and even automate routine maintenance for multiple endpoints simultaneously through a unified RMM dashboard.

Remote access software

End user remote connections to business networks can be established using remote access software. IT professional can also use this software to manage business networks remotely. There are multiple options available for remote access software, each with their own benefits and disadvantages. The following list provides a few options for various uses, workforce sizes, and network environments:

- **Remote Desktop Protocol (RDP):** RDP is a remote protocol developed by Microsoft. It is compatible with most Windows and Mac operating systems. An RDP solution may work well for flexible or hybrid work environments where employees split their work schedule between being physically in the office and working remotely. With RDP, end users can remotely access the physical computers housed at their offices, in addition to the desktop, software, files, and network access available to those systems. IT Support professionals can also use RDP software to troubleshoot, repair, patch and update end user computers without needing to be in the same room as the PCs.

RDP works by encrypting and transmitting the user's desktop, data, keystrokes, and mouse movements over the internet. Users may notice delayed responses to their keystrokes and mouse activity during the transmission process. RDP creates a dedicated network channel and uses network port 3389 to transmit this information using the TCP/IP protocol standard. Unfortunately, using a single dedicated port creates a security weakness that cybercriminals can target for on-path attacks. Further, RDP does not enforce strong sign-in credentials, which leaves RDP systems vulnerable to stolen credential and brute force attacks.

- **Virtual Private Network (VPN):** VPNs are often described as private tunnels through the public internet. Organizations can use VPNs to create encrypted connections over the internet between remote computers or mobile devices and the organizations' networks. VPNs can be implemented as software running on networked servers or on network routers with VPN features enabled. When the employees remotely connect to their VPN, they are able to access their organization's network as though they were physically in the office, eliminating the need to travel to the office in person. VPNs work well for small to medium sized organizations, but may not be adequate for large enterprises. Additionally, VPNs might not be the right solution for organizations that need to provide restricted levels of network access to groups like contractors or vendors.

Third party tools

- **Integrated video conferencing, screen sharing, and desktop management apps:** Video conferencing apps like Google Meet, Zoom, Microsoft Teams, Skype, etc. are growing in popularity as remote work tools. Video conferencing allows two or more people to meet "face-to-face" in a virtual environment. Some video conferencing apps also offer screen sharing tools, remote desktop control, polling tools, text messaging, meeting transcripts, webinar management options, the ability to record meetings, and more. The growing popularity of these tools for remote work has also invited an increase in related security attacks. Fortunately, the major providers of video conferencing software continuously update and patch their applications in response to these attacks.
- **File sharing and transfer platforms:** Cloud storage platforms, like Google Drive, Microsoft OneDrive, and Dropbox, have largely replaced file transfer protocol (FTP) tools. File sharing through a cloud platform provides the benefits of asynchronous file transfers, file transfer and data encryption,

customizable security and authentication settings, and the ability to file share with multiple users simultaneously. File owners can share individual files, folders, or entire drives. However, cloud storage might not be an appropriate option for organizations affected by certain privacy laws, regulations, or other security concerns. These organizations can still use FTP applications based on SSH or HTTPS protocols for secure file transfers over the internet.

Resources for more information

- How to use Remote Desktop - Walkthrough from Microsoft on how to use Remote Desktop to connect to a remote Windows 10 or 11 computer from a device running Windows, Android, or iOS.
- The Next Great Disruption Is Hybrid Work—Are We Ready? - Microsoft's Work Trend Index report on global workplace trends regarding hybrid work environments.
- Remote Work Stats & Trends: Navigating Work From Home Jobs - Provides findings from multiple surveys about attitudes and growing prevalence of remote work.

PowerShell Managing Services

"On Windows, most service configuration is stored in the **Registry**"

Get-Service	Shows all services & their state
Get-Service [Service] | Format-List *	Checks the status of a service | Shows everything in a list
Stop-Service [Service]	
Start-Service	

Linux Shell Managing Services

"Configuration files for installed services are in the **/etc** directory."

service [command] [parameter]	Manage services
service [command] reload	Makes service re-read configuration file without stopping service
lftp [host name]	An ftp client program on linux

dnsmasq

A program that provides DNS, DHCP, TFTP and PXE services in a simple package

Configuring DNS w/ Dnsmasq (in linux)

See linked video for a DNS Server in action!

Once we've installed dnsmasq, it's immediately enabled with the most basic functionality. It provides a cache for DNS queries. This means that you can make DNS requests to it and will remember the answers, so your machine doesn't need to ask an external DNS server each time you make the query.

dig www.example.com @localhost	Is how to check what's in the DNS cache
sudo service dnsmasq stop	Stop the dnsmasq service
Sudo service dnsmasq -d -q	Launch dnsmasq in debug mode and print activity

Configuring DHCP w/ Dnsmasq (in linux)

ip address show [dhcp server hostname or ip]	Show the ip of
cat dhcp.conf	Show the config file of the dhcp server. **Def rewatch video good info like default gateway and dns configurations.**
Sudo dnsmasq -d -q -C dhcp.conf	
Sudo dhclient -i eth_cli -v	Using a common dhcp client to test

```
devan@instance-1:~$ ip address show eth_srv
4: eth_srv@eth_cli: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue sta
    link/ether d6:83:2a:1e:21:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 scope global eth_srv
       valid_lft forever preferred_lft forever
    inet6 fe80::b492:cbff:fe17:3e13/64 scope link
       valid_lft forever preferred_lft forever
devan@instance-1:~$ ip address show eth_cli
3: eth_cli@eth_srv: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue sta
    link/ether 36:07:e6:5d:c5:1f brd ff:ff:ff:ff:ff:ff
    inet6 fe80::3407:e6ff:fe5d:c51f/64 scope link
       valid_lft forever preferred_lft forever
devan@instance-1:~$ cat dhcp.conf
# This is the interface on which the DHCP server will be listening to.
interface=eth_srv
```

```
devan@instance-1:~$ sudo dhclient -i eth_cli -v
Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth_cli/36:07:e6:5d:c5:1f
Sending on   LPF/eth_cli/36:07:e6:5d:c5:1f
Sending on   Socket/fallback
Created duid \000\001\000\001#6D\2556\007\346]\305\037.
DHCPDISCOVER on eth_cli to 255.255.255.255 port 67 interval 3 (xid=0x18656b4f)
DHCPREQUEST of 192.168.1.80 on eth_cli to 255.255.255.255 port 67 (xid=0x4f6b65
18)
DHCPOFFER of 192.168.1.80 from 192.168.1.1
DHCPACK of 192.168.1.80 from 192.168.1.1
```

Dnsmasq can act as a dns and dhcp server, as demonstrated in these videos.

Popular Email Protocols:

- POP3
- IMAP
- SMTP

Spam Management and Mitigation

In this reading, you will learn about common spam mitigation strategies. Spam is defined as any unsolicited message or call that is sent to a large number of recipients. Spam is a prevalent security concern for organizations. Cybercriminals use spam to steal important information from victims. Excessive spam can slow down mail servers and even cause the servers to crash. IT Support professionals must know how to mitigate and manage spam problems.

Types of spam

There are several different types of spam. Some spam is mass marketing from legitimate businesses. Legitimate spam is simply a nuisance, especially when it is unsolicited. Other spam can be malicious and criminal.

- **Phishing emails** attempt to trick recipients into providing personal information, credit card numbers, login credentials, etc. One famous phishing racket is the Nigerian royalty scam that asks victims to help a member of a royal family to move a large amount of money out of Nigeria. The story includes an excuse for why the royal person cannot do this for themselves and needs the victim's assistance. The cybercriminal requests the victim's bank account information for the purpose of wire-transferring the fictional royal money to the victim's account. However, the cybercriminal drains all of the money from the victim's bank account instead.

Phishing emails can also include clickbait links, which offer the victims something enticing, such as celebrity gossip, tabloid scandals, lottery winnings, etc. Cybercriminals even use spam to lure in victims by appealing to people's vices. Once the recipient clicks on the emailed clickbait link, they become victim to a number of malicious attacks. The attacks can include exposure to malware, ransomware, viruses, keyloggers, trackers, information phishing, and more.

- **Text spam** is another method used by cybercriminals to send phishing scams. Text message spam is normally less elaborate than email spam. The texts often contain a brief clickbait message followed by a link.
- **Email spoofing** is a type of phishing where emails appear to be from reputable companies, like banks, well-known brand names, government agencies, charities, etc. The "From" address of spoofed emails is forged to look like it came from the reputable company. Additionally, spoofed emails often use stolen company logos, verbiage, and formatting to appear authentic. A couple of common email spoofing scams include:
    - Fake job opportunities - Cybercriminals send emails with fake job opportunities and ask victims to provide all of the personal information that is normally requested in a job application and background check. This data may include the victim's social security number, government-issued ID info (e.g., driver's license or passport), current and former addresses, current and former employers, etc. The goal of the cybercriminal is to obtain all of the information needed to steal the victim's identity.
    - Fake credit card charges - Cybercriminals send emails that appear to be purchase receipts or alerts stating a business will be charging a large amount of money to the victim's credit cards for items the victim never purchased. The goal is to get the victim to reply or call a fake customer service line listed in the email to dispute the charges. The cybercriminal, posing as a customer service representative, asks the victim for their personal and credit card information to look up the bogus charge and pretend to cancel the fake order. Then the cybercriminal will either use the stolen credit cards or sell the victim's credit card information on the black market.
- **Tech support scams** are used to trick people into creating a security weakness for cybercriminals to hijack their computers. The cybercriminals introduce themselves as technical support for Microsoft, Dell, or other well-known computer companies. They claim that the victim's computer has been sending the company alerts about some type of fictional computer problem. The cybercriminal will direct the victims to change system settings or even set up remote sessions for the cybercriminals to change the settings themselves. The changed system settings open a door for the cybercriminals to hijack the computers to steal information, install ransomware or malware, or even to use the victims' computers as a vehicle to commit other crimes.

- **Call spam or robocalls** mimic telemarketing-type calls to collect personal information, bank or credit card numbers, and other criminally useful data from victims. Robocalls are also used to test databases of phone numbers to determine which are legitimate numbers. The phone numbers that are answered by a live human are sold to telemarketers as customer leads or on the black market to cybercriminals, who use the numbers as lists of potential victims.

One of the largest spam call scams was based out of India where 700+ employees in a call center in India were arrested or detained for impersonating the United States Internal Revenue Service (IRS). This criminal organization targeted Americans with phone calls claiming that the victim owed back taxes to the IRS and must pay hundreds or even thousands of dollars immediately to avoid arrest. The criminal organization stole up to $150,000 USD per day using this extortion scam.

Spam mitigation and management solutions:

Fortunately, many cloud platforms offer services and tools to help minimize these types of attacks. The following security measures are offered by platforms like Google Workspace. Google Workspace Administration Help guides are listed with each item below. These guides provide more information, as well as the instructions for implementing these security measures in Google Workspace.

- **DomainKeys Identified Mail (DKIM):** Helps to protect victims against phishing, email spoofing, and other email spam by preventing sender address forgery. DKIM attaches a header that contains a cryptographic private key to each email sent. This key is used to verify the identity of the sender and to detect if the email message was manipulated while in transit across the internet. Receiving email servers will usually designate emails without legitimate DKIM keys as spam. For more information and instructions to implement DKIM in Google Workspace, please see the article: Help prevent spoofing and spam with DKIM
- **Sender Policy Framework (SPF):** Used to control which domains, email servers, and IP addresses can send emails for an organization. SPF is examined by the receiving email servers to verify that the domains, email servers, and IP addresses from incoming emails are from approved senders. For more information and instructions to implement SPF in Google Workspace, please see the article: Help prevent spoofing and spam with SPF
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** Defines how the receiver should treat email messages depending on the results of DKIM and SPF checking. For more information and instructions to implement DMARC in Google Workspace, please see the article: Help prevent spoofing and spam with DMARC

Resources for more information

- Stop Unwanted Robocalls and Texts - The United States Federal Communications Commission offers tips for stopping robocalls and phone scams.
- 10 tips on how to help reduce spam - Microsoft's tips on how to handle email spam. Some items suggested are specific to Microsoft Outlook.
- How to stop spam texts: 8 do's and don'ts - Norton's advice on preventing attacks from spam texts. Some of the methods listed for combating text spam are specific to the United States.

Web Server Security

Obviously you're gonna need HTTPS, but did you know the 2 protocols that make it so secure?

- TLS (Transport Layer Security Protocol)
- SSL (Secure Socket Layer Protocol)
    - Been deprecated in favor of TLS

You need to go to a Certificate Authority for a HTTPS certificate to install on your web server

Mobile Synchronization

Mobile devices present some challenges for IT professionals. Mobile devices are easily lost, damaged, or stolen. With mobile synchronization, an IT professional can easily restore all the data stored on a lost or damaged device to a new device. This reading covers mobile synchronization on devices for collaboration with productivity platforms.

Mobile synchronization as backup

Most mobile OS platforms have built-in ways to backup mobile data to the cloud. For detailed steps on how to back up an Andriod or iOS device click below:

- Back up or restore data on your Android device
- How to back up your iPhone, iPad, and iPod touch

These backup methods help preserve the data carried on a mobile device and exchange it with other devices. They preserve the key types of data that a user wants to have backed up:

- App data
- Call history
- Contacts
- Settings
- SMS messages
- Pictures and videos
- MMS messages

As a backup method, mobile synchronization allows an IT professional to move the user's data seamlessly to a new device.

Mobile synchronization for collaboration and productivity platforms

Mobile synchronization is essential to today's collaboration and productivity platforms, such as Microsoft 365 and Google Workspace. These are account-based platforms that allow the user to link familiar productivity software and apps to a particular user or company profile. This way one username and password connects the user to the files, photos, people, and content needed to sync across different instances of the software or app.

Sync Microsoft 365 to a mobile device

To sync Microsoft 365 to a mobile device, the user needs to have a Microsoft account. With a Microsoft account, a user can set up Office apps and email on an iOS or Android mobile device. This setup process typically involves installing and setting up the Outlook mobile app for email, and the Office mobile app for other Microsoft tools, like Word, Excel, and PowerPoint. The following link provides detailed guidance on how to set up these capabilities on a device:

1. Set up Office apps and email on an iOS or Android mobile device
2. Use apps provided by Microsoft to sync the account with your device (consult your app store to find apps developed by Microsoft).

Sync Google Workspace to a mobile device

To sync email, calendar, and contacts using Google Workspace on an iOS or Android mobile device:

1. Set up Google Workspace on a device
2. Use apps provided by Google to sync the account with your device (consult your app store to find apps developed by Google).

To ensure that users have the most up-to-date information it is important to synchronize mobile devices on a regular basis.

Key takeaways

Mobile synchronization allows for data to be recovered if a mobile device is lost or damaged. It also ensures users have the most up-to-date information on any platform they use.

- Mobile OS platforms have built-in ways to backup the data carried on your mobile device and exchange with other devices.
- Account-based platforms link familiar productivity software and apps to a particular user profile. One username and password syncs files, photos, people, and content across different instances of the software or app.

Linux open source printing server software is **CUPS**

Print Services

IT professionals are often responsible for adding and updating printer drivers and settings. This may occur when a printer is added to a network, moved to a new location, or there is a software update. Along with updating drivers and settings on printers, IT may also be responsible for adding network printers to employee computers. Correct printer configuration saves time, supplies, and effort. This reading covers printing languages, basic printer configuration settings, printer sharing, printer security, and network scan services.

Printing languages

When choosing a print driver or troubleshooting issues with one, it is important to know which printing language the printer and computer operating system are using. Printing languages describe images on a screen to a printing device, so the printed output matches what is on screen. Printing languages are also called page description languages. Two of the most common printing languages are Printer Control Language and PostScript.

Printing languages can be either device-dependent or device-independent. Device-dependent means both the printer and computer are responsible for creating parts of the printed data. Device-independent means that the computer is solely responsible for creating the printed data. It is helpful for IT to know if the printing languages used are device-dependent or independent as it can help them troubleshoot whether printing errors are occurring because of the driver on the computer or the printer's hardware.

Printer Control Language (PCL)

Printer Control Language (PCL) is a printing language created by Hewlett-Packard that is used by many printer brands and computer operating systems. PCL is printing device-dependent because both the printer and computer are responsible for creating parts of the printed data. Because PCL is device-dependent, the output may not be the same on every printing device.

PostScript (PS)

PostScript was created by Adobe and is a printing language used by many printer brands but most commonly used in Macintosh systems. Unlike PCL, PostScript does not use the printer to create data. PostScript is device-independent, and the output is the same on any printer. If an error arises when PostScript is used, then it is usually an error with the driver on the computer.

Basic printer configuration settings

Configuration settings tell a printer how to complete a print job including the size, type of paper, number of sides, and use of color. IT professionals help employees change and select the correct settings for their document. The following are basic configuration settings that can be adjusted using printer settings.

- **Orientation** is the direction in which a document is printed. The main options for most printers are portrait (vertical) and landscape (horizontal).

- **Print Quality** refers to the level of detail that both the paper and the print settings are set to. The higher the DPI (Dots Per Inch), the higher the resolution or quality of the print.
- **Tray settings** tell the printer which tray of paper to use for the print job. Different trays can hold different paper sizes and types. Telling the printer to select paper from the correct tray ensures that the document is printed as it was designed.
- **Duplex** allows for printing on both sides of the paper. Printers can print information on one side (simplex) or both sides of the paper. Many brochures, booklets, and packets are printed on both sides to save paper.

Sharing a printer on a network

Printers can be shared on a network allowing multiple computers to access one printer across the network instead of having to be wired to the computer directly. IT professionals maintain and set up networks that include shared printers. For more information on sharing printers on your network read the article in the reference section below.

Network scan services

Network scan services allow a printer with scanning capabilities to create a file of a scanned image and upload or send it to a location on the network or in the cloud, or attach the file to an email and send it. Employees often need IT support for ways to use this type of technology. The following network scan services can be used for fast file uploads or attachments.

- **Email** scan service allows a document to be scanned directly from the printer to email.
- **Server Message Block (SMB) protocol** allows a document to be a shared resource once scanned by the printer.
- **Cloud services** enable a document to be scanned from the printer and uploaded directly to the cloud.

Printer security

Printer security protects access and tracks the activity of a print device. Printer security aims to ensure that only authorized users can use a printer. Setting up and monitoring proper security permissions falls under the job of an IT professional.

Some basic measures for limiting access to printers and tracking print activity are:

- **User authentication** commonly requires a user to enter a username and password before completing the print job.
- **Badges** are usually a physical card a user must scan at the printer to complete the print job.
- **Secured prints** require a user to enter a user-created code at the printer to complete the print job.
- **Audit logs** track users that have accessed the printer, including the date and time of use.

Key takeaways

IT support professionals are often responsible for printer management. It is helpful to know about printing languages, printer configuration, networking, and security.

- Printer Control Language is device-dependent, while Postscript is device-independent.
- Some basic printer configuration settings are orientation, print quality, tray settings, and duplex.
- Having a printer on a network enables multiple users to share printers.
- Network scan services allow a printer with scanning capabilities to create a file of a scanned image and upload or send it to a location on the network, on the cloud, or email.
- Printers have security and tracking features such as user authentication, badges, secured print, and audit logs.

Resources for more information

For more information about software and driver downloads for specific brand devices, review the links below.

HP Customer Support - Software and Driver Downloads

Cannon Customer Support - Software and Driver Downloads

Xerox Customer Support - Software and Driver Downloads

Ricoh Customer Support - Software and Driver Downloads

HP - How to Update Printer Settings for the Highest Quality Printing

Microsoft Support - Share your network printer

Xerox - Scan a Document to an Email Address

HP Customer Support - Set up Scan to Network Folder

Dell - How to Configure Your PC or Server for SMB (Server Message Block) Scanning on Dell Laser Printers

Xerox - Scan to Cloud or Enable Remote Destination

Printers

Sometimes you just need to create a hard copy of something on a computer. You need to be able to pass it around, mark it up, or store something as a physical copy. This is where a printer comes in! Printers work in a lot of different ways. In each case, the printer uses some type of printing technology to apply an image to a printing substrate such as paper, plastic, cloth, or just about any sort of surface you can imagine!

Printer technologies

Over time, many types of printing technologies have been developed. Here are some of the most common types:

Inkjet printersuse arrays of very small nozzles to spray ink onto the printing substrate. These are very versatile printers that can print onto a lot of different surfaces.

- https://computer.howstuffworks.com/inkjet-printer.htm

Laser printersuse a laser to draw an image in static electricity on a **photosensitive drum**. The statically charged image on the drum attracts a powdered pigment called **toner**, which is transferred onto the paper and **fused** in place!

- **https://computer.howstuffworks.com/laser-printer.htm**

Impact printerswork sort of like a typewriter. A **dot-matrix printer**, for example, has an array of small pins that press against the paper through an inked ribbon. Dot-matrix printers used to be very common, but now are only used in special situations. One example of this is when you need to print on **carbon (or carbon-less) copy paper**.

Thermal printersapply heat to special **thermochromatic paper**. Thermochromatic paper changes color when it is heated, so thermal printers don't require any ink! Thermal printers are very commonly used as receipt printers.

3D printersdon't apply an image to a substrate. 3D printers slowly layer small amounts of material at a time to create 3-dimensional objects! There are a lot of types of 3D printing technologies, and you need not only drivers, but other special software to build the instructions for your specific 3D printer.

- **https://3dinsider.com/3d-printer-types/**

Viewing your printers

To see what printers are already installed in your operating system, navigate to the OS's printer settings. You can also add new printers, and manage existing printers from there.

- In Windows, you will go to one of two places, depending on the version of Windows that installed. You will go to either **Settings > Devices > Printers & Scanners**, or to **Control Panel > Printers and Devices**.
- In MacOS, navigate to **System Preferences > Printers & Scanners**.
- There are a lot of different utilities for configuring printer settings in Linux. Take a look at the documentation for your version of Linux to be sure. Just as an example, for one common distribution of Linux, Ubuntu, you will navigate to **Activities > Printers**.

Each printer in your OS has a **print queue**, or **print spool**. If you send multiple **print jobs** to a printer, those jobs will line up in the queue to be handled, one at a time. Print jobs can be reordered or canceled while they are in the print queue.

- **Windows - View the print queue**
- **MacOS - Use the Dock on your Mac to check on a printer or print job**
- **Ubuntu - Cancel, pause or release a print job**

Your operating system will have a **default printer.** If you only have one printer, then that will be the default printer. If you have multiple printers configured, then you can select one to be used, well, by default!

- **Windows - How to set a default printer in Windows 10**
- **MacOS - Change the default printer or a printer's name on your Mac**
- **Ubuntu - Set the default printer**

Installing a printer

Printers can be pretty complicated devices, with lots of settings. There are dozens of common printer brands and thousands of printer models. Your operating system has a printer service, and knows how to talk to many printers, but it might not know how to talk to your printer. Operating systems have generic printer **device drivers** that will work for many common styles of printers. Beyond this, major operating systems will also understand how to search catalogs of device drivers in order to find the correct driver for a given printer. If your operating system does not automatically locate a driver for the printer you are trying to install, then the best place to look is on the printer manufacturer's support website. Remember, device drivers are specific to your operating system, so be sure to use the correct drivers for your OS.

- Windows - How to install a printer in Windows 10
- MacOS - How to add a printer on your Mac
- Use your Mac to print to a printer connected to a Windows computer
- Ubuntu - Printing

One thing you may notice when you are looking at printer device drivers is that some printers can speak more than one **page description language**. The most common of these languages are **PostScript (PS)**, and **Printer Command Language (PCL)**. Some printers will work better with one language than another. Most of the time, whatever is default or recommended by the printer manufacturer is what you should go with. Sometimes, the applications that you are printing from will prefer one language over another. If your printer supports multiple

languages and it is failing to print certain documents, or failing to print from certain applications, you might try a different language.

Virtual Printers

What do you do if there is an important document that you want to save, but you don't need a paper copy? You can use a **virtual printer**. A virtual printer is a printer driver that looks like a real printer to the operating system, but instead of printing print jobs onto paper, it creates a file! Virtual printers have names like "**Print to PDF**", or "**Print to File**". You can use virtual printers to create documents like **PDFs**or **XPS** files, or just about any type of image file!

- Microsoft XPS Document Writer
- Save a document as a PDF on Mac
- Ubuntu - Print to file

Printer Sharing

What if you have a printer attached to your computer, and you want to share that printer with someone who is using a different computer? You can! You can **share** your printer! When you share your printer, you are making it available to other computers as a **shared printer**. With a shared printer, other computers will send print jobs across the network to the computer that is attached to the printer. Take a look at these instructions on how to share your printer, and connect to the shared printer:

- Windows - How to share your network printer
- MacOS - How to share your printer on Mac
- MacOS - How to add a printer on Mac

Network Printers

Some printers can be directly attached to the network without having to be shared by a computer's operating system. These are standalone **network printers**. You can add network printers to your computers in a very similar way as a shared printer:

- Windows - How to install a printer in Windows 10
- MacOS - How to add a printer on Mac
- Network printing from Ubuntu

Watch out! Some network printers contain hard drives or other storage that are used to hold jobs in a print queue. This storage can end up holding on to some pretty sensitive information! Make sure to control access to this storage. Destroy the storage or **securely** delete any data from this storage before servicing, selling, or disposing of a network printer!

Print Servers

What if you have just a few printers, and a several people who need to share those printers? You might need a print server! Print servers work similarly to a local printer share, but on a larger scale. They can accept many print jobs at once, and will **queue** or **spool** the print jobs so they can be processed one at a time by the printer(s).

- Print and Document Services Overview
- Ubuntu - CUPS Print Server

Nice Troubleshooting Printers Module

https://www.coursera.org/learn/system-administration-it-infrastructure-services/ungradedWidget/3NxgP/troubleshooting-printer-issues

Clean rollers and print heads with **denatured alcohol**

https://www.coursera.org/learn/system-administration-it-infrastructure-services/ungradedWidget/bZBGZ/common-printer-types

Platform Services

Include web servers and web sites that serve as a “platform” for a company.
Thing YOU build and deploy are also considered the “service” used by the company.

Apache is the most common web server software.

Common Database Platforms include:

- MySQL
- PostgresSQL

HTTP Status Codes are how we troubleshoot web server issues.

Load Balancers

A load balancer ensures that each VM receives a balanced number of queries.

In this reading, you will learn about load balancers and their importance in cloud computing. You will become familiar with load balancing components and the benefits of utilizing load balancers.

IT Support professionals who manage cloud environments and/or physical servers in enterprise networks will likely need to configure, manage, or troubleshoot load balancers. Load balancers monitor and route network traffic flowing to and from a pool of physical or virtual servers. Load balancers can be hardware (e.g., load balancing routers) or software (e.g., Citrix ADC Virtual Platform). Load balancers distribute the traffic evenly, or by customized rules, across multiple servers. This function maximizes server performance and prevents the flow of traffic from overwhelming any one server and its resources. Basic server resources normally include CPUs, RAM, and network bandwidth. Servers can also offer other resources, like applications, file servers, database services, and more.

Load balancers can also detect when a server has failed and can reroute and balance network traffic across the remaining servers. This important business continuity and reliability function is often referred to as high availability. Additionally, load balancers provide IT Support professionals with the ability to add and remove servers to the pool as needed.

Load balancing terminology

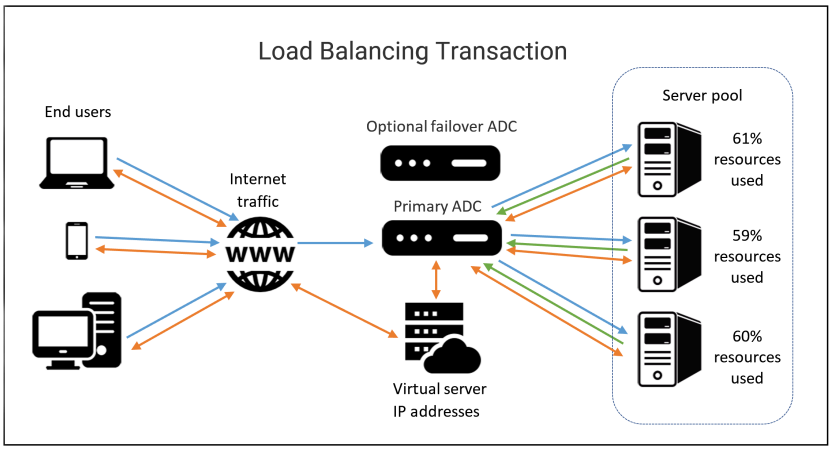
The following short glossary includes some common terminology for several concepts related to load balancers:

- **Client:** A computer or program that sends requests to a server. For example, a client could be a browser that requests a web page from a web server. It could also be a workstation requesting a file from a file server.
- **Host/node:** A physical or virtual server that receives network traffic from an Application Delivery Controller (ADC). The server is identified by its IP address. Whether the server is called a “host” or a “node” depends on the terminology used by the vendor of the load balancing solution.
- **Member:** A host/node that receives network traffic on a specified TCP port. The host/node is identified by its IP address plus the TCP port of the app that should receive network traffic.
- **Pool/cluster/farm:** A grouping of hosts/nodes or members that offer similar services, such as application or web services.
- **Application Delivery Controllers (ADC):** Physical appliances, virtual appliances, or software that provide load balancing services by managing traffic between clients and host/node or member pools. ADCs can also provide other important services such as security and encryption.

- **Path-based routing:** Routes network traffic based on URL paths.
- **Listener:** A software process that checks network traffic for client requests and forwards them to target groups.
- **Open Systems Interconnection (OSI) model:** Model that depicts the seven layers of computer data communications: 7-application, 6-presentation, 5-session, 4-transport, 3-network, 2-data, and 1-physical.
- **Front end:** In load balancing environments, the front end can include the ADC system and any virtual servers that act as proxies for client communications with the ADC system and the back end servers.
- **Back end:** In load balancing environments, the back end normally includes the pool/cluster/farm systems. The back end can also include disk storage systems.
- **Distributed applications:** Software stored on cloud platforms or physical servers that can run on multiple networked computers at the same time.
- **Containerization:** Isolated runtime environments that can deploy and run distributed applications through application virtualization. This method is faster and is more scalable than older load balancing solutions.
- **Availability Zones (AZs):** Regional data centers that host cloud platforms and are configured for high availability.
- **Elastic Load Balancer (ELB):** Enables the use of more than one Availability Zone.
- **SSL/TLS:** Network protocols for encrypted communication.

Example ADC process for load balancing

The following steps are an example of one possible load balancing configuration using an ADC solution:



1. **[Blue arrows]** The client sends a connection and an information request to the ADC service.
2. **[Blue arrows]** The ADC listener detects and accepts the connection. Then the ADC load balancing service analyzes the best host (or member) routing path for the client request. The ADC changes the destination IP to the address (and possibly the TCP port) of the selected host (or member).
3. **[Green arrows]** The host or member approves the client connection and routes a response to the client through the ADC.
4. **[Orange arrows]** The ADC changes the source IP (and TCP port, if applicable) to a virtual server IP (and port) before forwarding the response to the client. The clients will continue to use the IP address of the virtual server for further communications.

Load balancing types

- **Application Load Balancer:** Operates at the application layer (HTTP and HTTPS) of the OSI model. Application load balancers also scan traffic for HTTP errors and coding bugs, as well as guard applications against distributed denial-of-service (DDoS) attacks.
- **Network Load Balancer:** Operates at the transport layer (TCP/UDP) of the OSI model. Network load balancers can route millions of client requests per second and handle volatile workloads. Network load balancers also support static IP addressing and containerization, among other services.
- **Classic Load Balancer:** Can operate at either the application layer (HTTP/HTTPS) or the transport layer (TCP/SSL). Classic load balancers use fixed ports for communication.
- **Gateway Load Balancers:** Operates at the network layer (IP) of the OSI model. Gateway load balancers have listeners on all ports that scan every IP packet in the network traffic and route each request to the target pools, as defined by the listener configuration. A gateway load balancer is the only point of entry and exit for network traffic.

Load balancers in cloud environments

In cloud environments, load balancing across virtual servers is configured through the cloud platform. A few of the load balancing options offered by several top cloud platforms include:

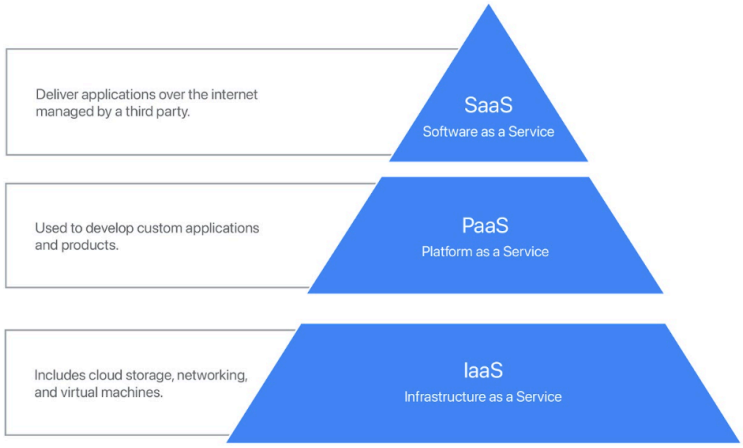
- **Google Cloud:** Google offers an array of options for load balancers, such as application and network level load balancing, software-defined load balancing, multi-region failover, and seamless autoscaling. Google Cloud also offers external, internal, global, and regional load balancing. For security measures, the load balancers are integrated with Google Cloud Armor, which protects against distributed denial-of-service (DDoS) attacks.
- **Amazon Web Services (AWS):** AWS offers three ELB solutions: an Application Load Balancer, a Gateway Load Balancer, and a Network Load Balancer. AWS ELBs provide security through user authentication, certificate management, and SSL/TLS decryption.
- **Microsoft Azure:** Operates at the transport layer of the OSI model. Azure load balancer is the only front end point for accepting client requests to route to the back end server pools. The backend pool may consist of Azure Virtual Machines (VMs) or instances running in Azure virtual machine scale sets. Azure offers public load balancers for internet traffic and private/internal load balancers for private virtual networks. Azure's Standard load balancer uses the zero trust security model.

Load balancers in physical environments

In physical environments, such as server rooms and data centers, load balancing can be configured across multiple servers with operating systems like VMware. Network traffic loads can also be configured for smaller environments across two servers in a physical active-active cluster. In active-active clusters, both servers actively handle network traffic simultaneously.

Common Cloud Models

The cloud is a part of everyday life in the modern internet world. It gives users a place to work, access, and store data from any system plugged into the cloud. Being able to work with the cloud is a vital skill in IT. This reading will cover common cloud services and four types of cloud computing.



Types of cloud services

Companies use cloud services to provide access to internal tools, develop software, store data, and more. The three primary cloud services are Software as a service, Platform as a service, and Infrastructure as a service. The Google Cloud Platform is a prime example of a system that employs all three types of cloud services.

Software as a Service (SaaS)

SaaS providers allow users to use their software with an internet browser or application instead of having to download software to a specific device. Users access information from any device through a login. The SaaS vendor stores all user data and files online instead of on the user's physical equipment. SaaS typically uses a subscription model for its services. Hacking is a concern when using this service since the full-service run in the cloud.

Platform as a Service (PaaS)

PaaS offers computer hardware and software in the cloud that allows users to develop and deploy applications or cloud based services. PaaS makes buying, developing, configuring, managing, and installing software and hardware unnecessary.

Infrastructure as a Service (IaaS)

IaaS provides an IT infrastructure to a company over the internet and on-demand. IaaS provide access to things like virtual machines, containers, networks, and storage. This service reduces the need to purchase expensive hardware. IaaS allows companies to centralize infrastructure for faster disaster recovery.

VPN as a Service (VPNaaS)

VPNaaS secure networks through a cloud-based connection between the employee and the organization's network. Using this approach eliminates the need for a physical VPN endpoint.

Function as a Service (FaaS)

FaaS is an event-based service that lets developers do the building, running, and managing functions directly in the cloud without needing to maintain a server. Event-based systems use an event, such as a website click, to trigger communication within a system.

Data as a Service (DaaS)

DaaS provides data access as a service to a business. It manages the data companies generate and uses APIs to deliver data from various sources on demand. DaaS allows companies to organize and access the data they need. DaaS monetize by providing access to data. By increasing accessibility to data, DaaS can lower the cost of data-driven decision making, remove personal bias in data collection, and innovation.

Blockchain as a Service (BaaS)

BaaS is a newer and increasingly mainstream cloud model that uses a non-centralized system. This model uses encrypted, connected blocks of information for higher security than standard cloud services. BaaS is used to store smart contracts and high-security documents. This model authenticates users without needing additional applications. SaaS services may adapt BaaS as a standard feature to address the risk of hacking.

Four types of cloud computing

Cloud computing is the delivery of computing services like the cloud services mentioned above. There are four main types of cloud computing:

1. **Public clouds**: cloud environments created from IT infrastructure owned by a provider such as Google Cloud or Amazon Web Services. Public clouds host the data of multiple companies. Be aware that public clouds do not provide absolute security for the information it stores.
2. **Private clouds:** serve a single business or organization. The cloud runs behind an internal firewall. Private clouds can be deployed and managed by a third-party vendor.
3. **Multiclouds**: involve using more than one cloud service from more than one vendor. These can be private or public.
4. **Hybrid clouds:** blend at least two public or private cloud services and connects them with internal networks, such as local area networks or VPNs.

Cloud services and cloud computing work together to meet the needs of companies and organizations.

Key Takeaways

Companies use the cloud for many tasks and services.

- The three primary cloud services are SaaS, PaaS, and IaaS.
- Additional cloud services include VPNaaS, FaaS, DaaS, and BaaS.
- Four main types of cloud computing are public clouds, private clouds, multiclouds, and hybrid clouds that deliver cloud services.

Resource for more information

For more information on the Google Cloud Platform and the services it offers, visit this website.

Managing Cloud Resources

If you are considering hosting some services in the Cloud, you'll need to learn what the different terms used to configure the services mean.

When deploying a service to the cloud, you will typically create a number of virtual machines that will be the servers in charge of hosting your service. In the usual case, you would start by creating a single machine that will run the service, creating the configuration associated with the machine, verifying that it works, and then turning this into a template that can be used for the creation of many machines as needed.

In order to do this, you'll make use of both **Autoscaling** and **Load Balancing**. Autoscaling means being able to automatically create new instances when the load increases and automatically turn them down when the load decreases. In order for this to be possible, you need to ensure that your instances can be completely configured automatically, and that there's no data being kept in the instances themselves (data can be stored in a database, or in separate drives).

Load Balancing means distributing the load among many servers. There's different approaches to doing load balancing, but the main concept is that there's a load balancing service that will route traffic to the servers in a way that they each get to serve a portion of users, without the users realizing that they are connecting to different machines. In other words, the users will access a single address (e.g. http://www.example.com), which can be served by different servers, in different parts of the world, without the users having to care about that.

Once you have your service set up to scale automatically and balance the load, you'll want to also setup **Monitoring** and **Alerting** for it. Monitoring means checking that the service is healthy, that it's responding to queries as expected and not generating unusual errors. Alerting means sending alerts when things don't happen as expected.

For a simple service, you might go with the monitoring that is already built in by the cloud provider, which will allow you to check that your instance is healthy, but is likely not going to go into much detail as to whether the content is being served correctly. If your service is more complex, you might want to invest more time into making it possible to monitor additional parameters of your service.

Depending on the specific service you are deploying, there might be more concepts that you need to understand before you can actually do it. We recommend reading the documentation offered by the cloud provider you have chosen to figure out what you need to do.

Here are some links with more information from some of the biggest cloud providers:

- https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/
- https://aws.amazon.com/getting-started/
- https://cloud.google.com/docs/overview/

Directory Services

Active Directory is the native Windows Directory service.

- GPOs (group policy objects) manage Windows machine configuration

Everything done in the Windows Active Directory GUI is actually just being translated into Powershell.

When a domain joined computer or user signs into the domain by contacting a domain controller, that domain controller gives the computer a list of group policies that it should apply. The computer then downloads those policies from a special folder called **Sisfall**.

OpenLDAP is the open-source equivalent of Windows Active Directory that works on all operating systems.

Controlled through command line or things like phpLDAP admin which allows a web-interfacet to interact with OpenLDAP

This is how the Google guy downloaded LDAP

Sudo apt-get install slapd ldap-utils

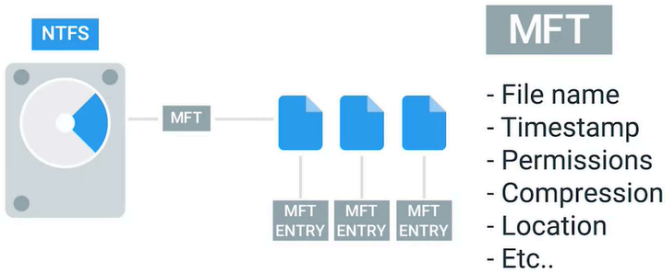
```
dn: uid=cindy,ou=Engineering,dc=example,dc=com
objectClass: inetOrgPerson
description: Cindy works in the Engineering department.
cn: Cindy
uid: cindy
```

Example LDIF file for a user on right.

SEE LINUX COMMANDS IN COURSE 3 FOR LDAP CLI COMMANDS

Windows Files

NTFS uses the MFT (Master File Table) to store and manage data.



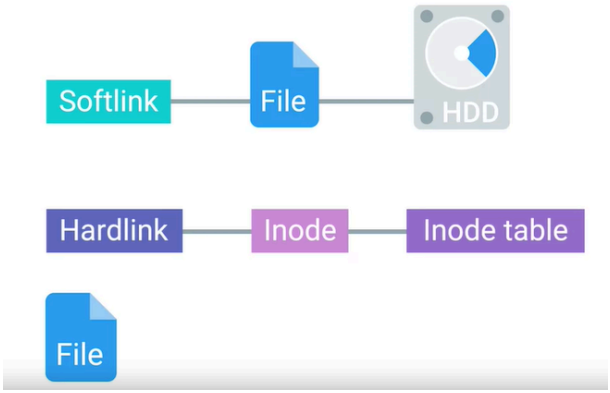
Linux Files

Instead of MFT like in Windows, Linux uses inodes. They store everything except a file's actual data and name. Inode tables sort files in linux.

Linux softlinks work like symbolic links

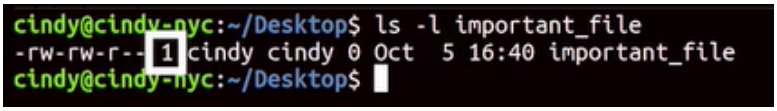
The number in an ls -l is how many hardlinks there are to a file. When this is 0, the file is completely removed from the computer.

Links are great for conserving space but still keeping files accessible.



How Windows Repairs Files

https://www.coursera.org/learn/os-power-user/lecture/aXBeM/windows-filesystem-repair



How Linux Repairs Files

https://www.coursera.org/learn/os-power-user/lecture/1d4Y4/linux-filesystem-repair

Linux File System Repair

In this reading, you will learn how to use the file system consistency check or **fsck** command to repair data corruption in file systems on Linux machines. As an IT Support specialist, you will most likely encounter instances of data corruption in onsite systems. It is critical for you to know how to recover corrupted data, file systems, and hard drives.

A computer file system is software that provides structure for storing the operating system (OS) and all other software installed on system hard drives. A hard drive must be formatted with a file system before the operating system can be installed. Since Linux is an open source OS, innovators have created nearly 100 file systems that support Linux OS installations. Several common file systems that are used for Linux systems include ext, ext2, ext3, ext4, JFS, XFS, ZFS, F2FS, and more.

Like all software, software-based computer file systems can experience corruption. File system corruption can impede the computer's ability to locate files stored on the hard drive, including important OS files. File locations are stored as i-nodes (index nodes) in Linux. Every file in a Linux system has its own i-node identifier. The i-node stores metadata about the storage block and fragment location(s) where each file is stored. The i-node metadata also holds information about the file type, size of the files, file permissions, links to the file, and more.

Symptoms of data corruption

Symptoms of data corruption can include:

- System suddenly shuts down
- Software program will not launch or it crashes when opening a corrupted file. May also give an error message saying:
    - “File format not recognized” *or*
    - “(file name) is not recognized”
- Corrupted files and folders may no longer appear in the file system.
- The operating system (OS) may report bad sectors when failing to execute commands.
- Damaged platter-based hard drives can make clicking sounds or unusual vibrations.

Causes of data corruption

Data corruption on system hard drives and file systems can be caused by:

- **Software errors** -
    - Software errors can be any software event that interferes with normal hard disk read/write operations.
    - Viruses and malware can be designed to intentionally cause corruption to data.
    - Antivirus software can damage files if the software experiences problems while scanning or repairing the files.
- **Hardware malfunctions** -
    - Larger files are more likely to experience corruption than smaller files. Large files occupy more disk space, making them statistically more likely to cross a bad sector on the hard drive.
    - Hard drives that contain platters are at risk of experiencing malfunctioning read/write heads. Damaged heads can corrupt multiple files and directories in a single read/write transaction. Hard drives with moving mechanical parts are more likely to experience failures from moving parts that wear out over time.
- **Electrical damage** - Can happen when a power failure occurs while the system is writing data to a hard drive.

Data corruption repair

The most critical first step, after data corruption has been identified or suspected, is to shut down the affected hard drive(s). The reason for this step is to stop the cause of the corruption from writing to the hard drives. The longer the corruption activity continues, the more difficult recovering the data becomes.

Precautions should be taken before powering up a corrupted hard drive to run repair tools. It is important to minimize any read/write operations on the disk other than those produced by data recovery tools. One method to prevent further damage could be to have a corrupted Linux system boot from an external device or network (PXE boot). An alternative method might be to attach the corrupted hard drive as an external hard drive to a healthy system running Linux. A hard drive adapter or drive docking station can be used to convert an internal drive into an external device.

Before connecting a corrupted drive to a healthy system, the **automount** service must be disabled. The **fsck** command will not repair corruption on a mounted file system. In fact, mounting a corrupted file system can cause the healthy Linux system to crash. Although the corrupted file system should not be mounted, the device file for the corrupted hard drive in the ***/*dev directory** must be readable for the **fsck** command to access the drive.

The fsck command

***Important Warning:** The **fsck** command should NOT be used:*

- *on a hard drive that was a member of a RAID array.*
- *on a mounted file system (must be unmounted).*

An important command line data recovery tool offered in the Linux operating system is the **fsck** command. It should be run anytime a Linux system malfunctions. The **fsck** command can check the file system and repair

some, but not all, inconsistencies found. In some cases, **fsck** may recommend deleting a corrupted file or directory. The default setting for the **fsck** command is to prompt the user to approve or deny the repair of any problems found. The user running the **fsck** command must have write permissions for the corrupted file or directory to be able to approve a repair. If the user does not choose to repair inconsistencies found, the file system will remain in a corrupted state.

The **fsck** command will check for inconsistencies and and prompt the user to make decisions on whether or **fsck** should repair for the following problems:

- Block count is not correct
- Blocks and/or fragments that are:
    - allocated to multiple files
    - illegally allocated
- Block and/or fragment numbers listed in i-node metadata that are:
    - overlapping
    - out of range
    - marked free in the disk map
    - corrupted
- Map inconsistencies on the disk or in the i-node.
- Directory:
    - contains references to a file but that number does not equal the number of links listed in the same file's i-node metadata.
    - sizes are not multiples of 512

The following checks are not run on compressed file systems.

- Directory checks:
    - Directories or files that cannot be located or read.
    - The i-node map has an i-node number marked as being free in the directory entry.
    - The i-node number in the metadata is out of range.
    - The . (current directory) or .. (parent directory) link is missing or does not point to itself.
- Fragments found in files larger than 32KB.
- Any fragments that are not listed as the last address of the file in an i-node metadata file.

How to use the fsck command

1. Enter **fsck** as a command line instruction. Syntax:

fsck [**-n**] [**-p**] [**-y**] [**-f**] [*FileSystem1name - FileSystem2name ...*]

- The **-n** flag - Sends a "**n**o" response to all **fsck** questions and does not allow **fsck** to write to the drive.
- The **-p** flag - **P**revents error messages for minor problems from displaying while automatically fixing those minor errors. Outside of recovering from data corruption, it is a best practice to run the **fsck -p** command regularly at startup as a preventative measure.
- The **-y** flag - Sends a "**y**es" response to all **fsck** questions to automatically attempt to repair all inconsistencies found. This flag should be reserved for severely corrupt file systems only.
- The **-f** flag - Runs a **f**ast check that excludes file systems that were successfully unmounted for shutdown before the system crashed.
- *FileSystem#name* - If you do not specify a file system, the **fsck** command checks all file systems in **/etc/filesystems,** where the **check** attribute is set to **true**.
- To see more advanced flags, use the **man fsck** command.

a. To have the **fsck** command check all of the default file systems and prompt the user on how to handle each inconsistency found, simply enter at a command line:

b. For ext, ext2, ext3, and ext4 file systems, the **e2fsck** command can be used:

c. To have the **fsck** command check specific file system(s) and automatically fix any inconsistencies found, enter:

2. The **fsck** command outputs an exit value, or code, when the tool terminates. The code is the sum of one or more of the following conditions:

- 0 = All scanned file systems have been restored to a functional state.
- 2 = **fsck** did not finish checks or repairs due to an interruption.
- 4 = File system has changed and the computer needs to be rebooted.
- 8 = **fsck** could not repair some or all file system damage.

How to run fsck on the next boot or reboot

In many Linux OS distributions, the **fsck** utility will automatically run at boot under certain circumstances, including:

- When a file system has been labeled as “dirty”, meaning that data scheduled to be written to the file system is different from what was actually written or not written to the disk. This could occur if the system shut down during a write operation.
- When a file system has been mounted multiple times (can be set to a specific value) without a file system check.

Configuring the **fsck** command to run automatically on boot and reboot differs depending on which brand and version of Linux is installed on the system. As a root or sudo user, use vi (visual instrument) to add the **fsck** command to the boot sequence.

1. In Debian and Ubuntu,
   a. Edit the **rcS** file.
   b. Add the following command to the **rcS** file:
2. In CentOS,
   a. Create or edit a file named autofsck.
   b. Add the following command to the autofsck file:

Edit & Create Group (GPO) Policies using GPMT

https://www.coursera.org/learn/system-administration-it-infrastructure-services/lecture/s8fRo/group-policy-creation-and-editing

Group Policy Troubleshooting

https://www.coursera.org/learn/system-administration-it-infrastructure-services/lecture/NKERN/group-policy-troubleshooting

Most commonly: a user cannot log in/ authenticate

The SRV records that we’re interested in are _ldap._tcp.dc._msdcs.DOMAIN.NAME, where DOMAIN.NAME is the DNS name of our domain.

Any networking issue that would prevent the computer from contacting the domain controller or its configured DNS servers, which is used to find the domain controller, **could be an issue.**

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Resolve-DNSName -Type SRV -Name _ldap._tcp.dc._msdcs.example.com

Name                                 Type   TTL   Section    NameTarget                Priority Weight Port
----                                 ----   ---   -------    ----------                -------- ------ ----
_ldap._tcp.dc._msdcs.example.com     SRV    600   Answer     dc1.example.com           0        100    389
_ldap._tcp.dc._msdcs.example.com     SRV    600   Answer     dc2.example.com           0        100    389

Name       : dc1.example.com
QueryType  : A
TTL        : 600
Section    : Additional
IP4Address : 10.128.0.3


Name       : dc2.example.com
QueryType  : A
TTL        : 600
Section    : Additional
IP4Address : 10.128.0.4
```

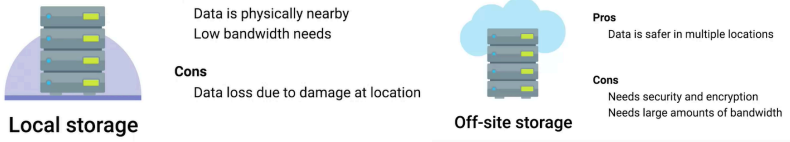
Resolving your domain controllers (left) if this doesn’t work, your DNS is bunked. See the SRV records I think that’s relevant to DNS

Mobile Device Management (MDM) Systems

https://www.coursera.org/learn/system-administration-it-infrastructure-services/lecture/iWEiS/mobile-device-management-mdm
Supplemental Reading:
https://www.coursera.org/learn/system-administration-it-infrastructure-services/supplement/LnGpY/supplemental-readings-for-mobile-device-management-mdm

Data Recovery

ALWAYS HAVE BACKUPS
When a catastrophe occurs, the priority must be to get back to normal business operations as soon as possible.
MUST have a disaster plan.



We create a **post-mortem** after an incident, a outage, or some event when something goes wrong, or at the end of a project to analyze ho it went.

rsync is the **linux** cli tool that works great with remote backups.

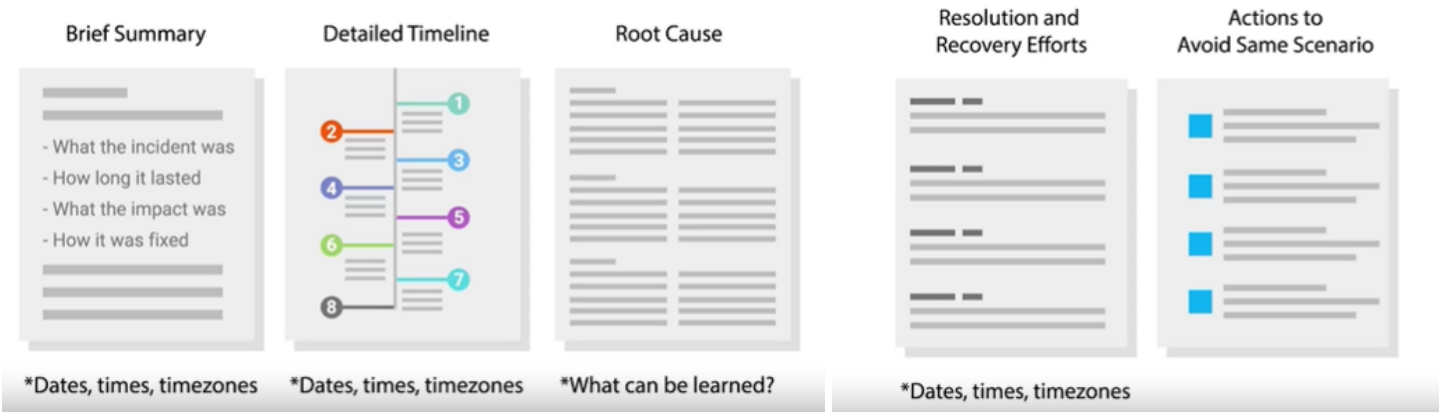
Restoration procedures

Should be documented and accessible so that anyone with the right access can restore operations when needed

Apple uses **Time Machine** for backups
Windows uses **"Backup and Restore"** for backups.

Sharing post-mortem's help remind people that making mistakes is normal, and we can learn from them

Writing a post-mortem:



Noice :)

Deploying Software/ Files to Different Groups

Came up in an interview role play:

- Active Directory can be used to determine what softwares (like msi files) should be installed on a machine. Those files can be stored on a shared drive.

Course #5: **IT Security: Defense against the Digital Dark Arts**

Starting Here from Week 2 (Go over Week 1 notes on Coursera)

Physical Privacy and Security Components

In this reading, you will learn more about physical privacy and security, including biometric and Near Field Communication authentication. You will also revisit the “confidentiality” aspect of the CIA Principle (Confidentiality, Integrity, Availability), which was introduced previously in this certificate program.

CIA Principle: Confidentiality

Preventing unauthorized access to an organization’s data and networks is imperative in protecting a company’s information systems. Regulations, standards, and laws may also require that certain information be kept confidential, like health records. Failing to ensure the confidentiality of specific types of data could result in damage to reputation, loss of customers, liability lawsuits, financial losses, penalty fines, criminal charges, and more. It is vital for IT Support specialists to take all measures possible to protect confidential information.

In a previous video, you learned about three types of authentication methods:

- **Something you know** - password or pin number
- **Something you have** - bank card, USB device, key fob, or OTP (one-time password)
- **Something you are** - biometric data, like a fingerprint, voice signature, facial recognition, or retinal scan

You will learn more about biometrics in this reading, along with two additional categories of authentication methods:

- **Somewhere you are** - geofencing, GPS, Indoor Positioning Systems (IPS)
- **Something you do** - gestures, swipe patterns, CAPTCHA, or patterns of behavior

Some authentication technologies inherently require two factors:

- **Somewhere you are + Something you have** - Near Field Communication (NFC) uses both proximity to an NFC scanner and a device like an NFC-enabled smartphone or an RFID chip on an employee ID or bank card.

Something you are: Biometrics

Biometric authentication occurs in two steps: enrollment and authentication. Enrollment happens when the user provides their biometric data for the first time through a hardware scanner. Specific features of that biometric data are extracted, encrypted, and stored, often in a database or on a personal mobile device. Authentication, as the second step, happens when a user presents their biometric data again to the scanner to gain access to the secured item. This new scan is compared against the original stored biometric data to authenticate the person’s identity.

Fingerprint scanning

In a previous video, you learned about fingerprint scanners as an authentication method for mobile devices. Fingerprint scanners use small capacitive cells that are engineered to detect fingerprint ridges. Dirt and moisture can interfere with the scanner’s ability to do its job. As an IT Support specialist, you may need to replace damaged fingerprint scanners on customer devices.

Facial recognition

Many smartphone models provide the hardware and software to use facial recognition as a biometric authentication method. This often requires two cameras. The first camera uses normal color photography. The second camera uses

infrared technology to measure depth and ensure your face is 3-dimensional. This prevents hackers from using photographs of the authorized users to unlock mobile devices.

Iris and Retinal scanning

Iris scanning is not a secure form of biometric authentication because a photograph of the user's iris can be used to gain access. In contrast, retinal scanning is one of the more secure forms of biometric authentication. It is exceedingly difficult to impersonate the retinal features of a person's eye. Our retinas have unique and complex patterns in how our blood vessels are arranged. These fingerprint-like patterns can be scanned by shining a beam of infrared light into the eye. Note that eye injuries and medical problems with the eyes can change retinal blood vessel patterns and cause users to be denied access to their devices. Although retinal scanning is secure, the technology can be expensive and difficult to implement.

Somewhere you are: Geolocation

The geographical location of a user can serve as one part of a multi-factor authentication policy or to deny access to users based on their locations. Geolocation services can use GPS, IP ranges, WiFi access points, cell phone towers, and/or Bluetooth beacons to estimate a mobile user's location.

Geofencing

Geofencing is used to authenticate users who are physically within a certain radius of a specific location. For example, if you order food using McDonald's smartphone app, the restaurant will not process your order until your smartphone is within a certain radius of the restaurant. You cannot send someone else to pick up your order either, as that person cannot authenticate without your smartphone being within the geofencing radius.

Global Positioning Systems (GPS)

Global Positioning Systems (GPS) use satellites orbiting Earth to map a device's longitude and latitude. The mobile device needs to be equipped with GPS sensors and have GPS services enabled to take advantage of GPS-based authentication technologies. GPS could be used to authenticate a device based on the physical location of the user. Insurance companies use GPS data to verify the authenticity of disaster claims filed through mobile apps.

Indoor Positioning Systems (IPS)

Indoor Positioning Systems (IPS) triangulate a device's location by using WiFi access points, cell phone towers, and/or Bluetooth beacons. Users must grant permission to apps to use this technology. IPS locations might be used to deny network access when the user has entered a restricted area.

Near-field communication (NFC) and scanners

You may have interacted with a near-field communication (NFC) scanner by using contactless payments with a credit card, bank card, or smartphone. NFC technology can also be used for authentication and access to physical buildings through school or employment ID cards.

NFC transmits on the same frequency as high frequency RFID (13.56 MHz) and has a short distance range of 10 centimeters. The short distance range provides some protection from hackers attempting to intercept the connection to obtain your credit card information. However, NFC is not fully secure. An innocuous looking NFC scanner sitting next to an NFC-enabled payment device could record all NFC transactions that occur within the 10 cm of the device in a "man in the middle" security breach.

Something you do: Gestures and Behaviors

You may already be familiar with using gestures like swipe patterns to unlock a smartphone. Another gesture-based authentication method is the Picture Password, which requires the user to touch specific, secret points on a photograph to unlock the device.

Patterns of people's behaviors can be used to authenticate identity. For example, an organization might keep track of computer system login and logout times of employees. These patterns could be monitored for any unusual changes in employee behavior, which may indicate that the "employee" is instead an imposter.

Turing tests are used to determine if an unknown entity is a human or a machine. You have probably responded to a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to authenticate that you are indeed a human and not a bot. This is accomplished by asking the user to identify items within a set of photographs. Photos are used for this test because images are more difficult for bots to identify than text.

Key takeaways

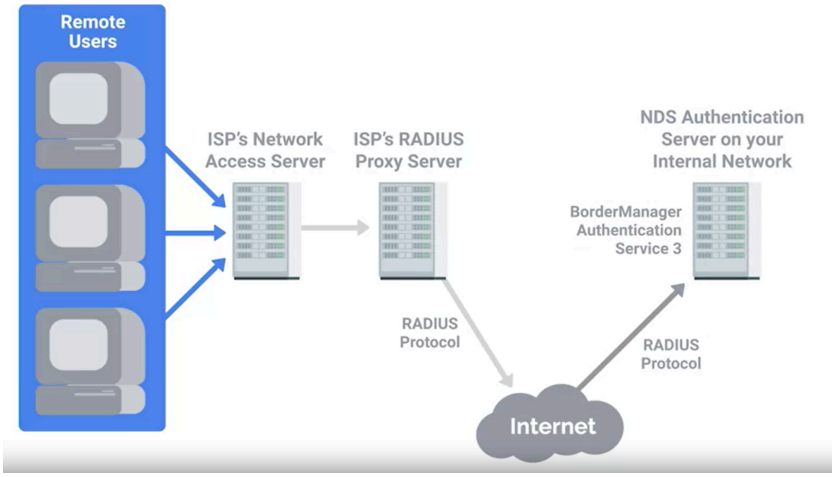
There are a variety of MFA protocols that can be implemented to protect the confidentiality, privacy, and security of data and networks. The 5 types of authentication can be categorized as:

1. Something you know - password or pin number
2. Something you have - bank card, USB device, key fob, or OTP (one-time password)
3. Something you are - biometric data, like a fingerprint, voice signature, facial recognition, or retinal scan
4. Somewhere you are - geolocation, geofencing, GPS, Indoor Positioning Systems (IPS), NFC scanning
5. Something you do - gestures, swipe patterns, CAPTCHA, or patterns of behavior

Resources for more information

For more information about methods of authentication to protect data, please visit:

- Geolocation—The Risk and Benefits of a Trending Technology - Discusses impacts, benefits, risks, risk mitigation, security, governance, and privacy concerns of geolocation technologies.
- Understanding The 5 Factors Of Multi-Factor Authentication - Overview of the 5 Factors: Something you know, Something you have, Something you are, Somewhere you are, and Something you do.
- Homeland Security Biometrics - History and use cases of biometrics for maximum security and identification of criminals in the United States Departments of Homeland Security, Defense, Justice, and Commerce, as well as the National Institute of Standards and Technology.
- A Review on Authentication Methods - Informative peer-reviewed journal article on authentication methods.
- Modern Authentication Methods: A Comprehensive Survey - Peer-reviewed journal article with expanded coverage of two-factor and multi-factor authentication topics. Provides comprehensive comparisons of advantages and disadvantages of each authentication method.
- What is the Difference Between NFC and RFID? - A comparison of NFC and RFID technologies.
- Fingerprint Reader Replacement Guide - Provides photos of internal fingerprint scanner hardware parts, as well as instructions on how to replace a fingerprint scanner on a laptop.



(Left) Radius Servers Authentication Process

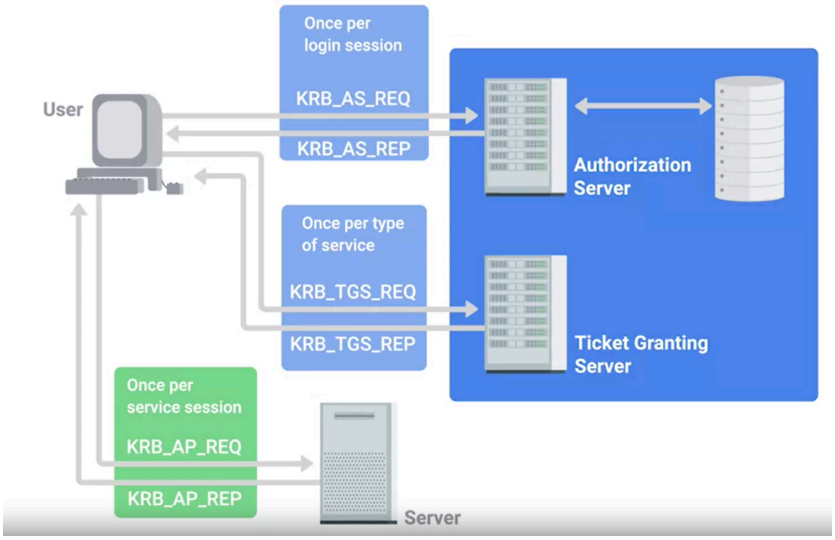
Kerberos (Big detailed stuff)

https://www.coursera.org/learn/it-security/lecture/0uTpl/kerberos

Single Sign-On

Example pictured in blue, yellow green below.

Authorization and Access Control



Pictured left is illustration of Authorization through a Kerberos example.
←

Mobile Security Methods

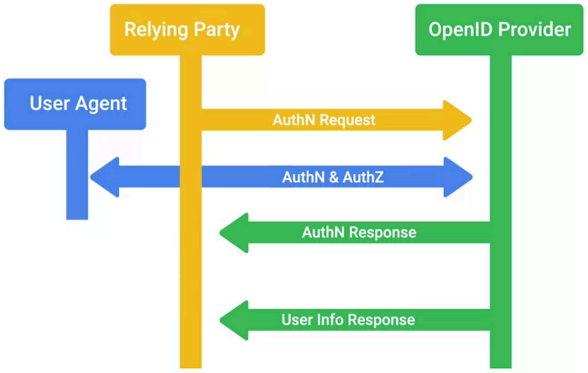
Laptop computers, tablets, smartphones, and other mobile devices allow people to remain productive from various locations, such as at home or while traveling. This increased flexibility raises various security concerns that IT departments need to address. This reading provides information about the current security measures used to protect mobile devices.

Common mobile security threats and challenges

Many of the security threats associated with mobile devices are the same as those of traditionally networked devices, such as hacking and malware. However, mobile devices face additional threats that other devices do not.

Here are some threats facing mobile device security:

1. **Phishing**: Phishing attacks can use SMS messaging, email accounts, messages via numerous social media applications, or malicious links in browsers to target your mobile devices.
2. **Malicious applications (malware)**: Malware can take the form of apps designed to collect and transmit personal and corporate information to third parties.
3. **Insecure Wi-Fi and "meddler in the middle" attacks**: An attacker places themself in the middle of two hosts that think they're communicating directly. The attacker may monitor the information from these hosts and potentially modify it in transit. Open or "free" Wi-Fi hotspots are especially susceptible to meddler in the middle and similar attacks.
4. **Poor update habits for devices and apps**: An example is failure to install security patches regularly deployed through software and firmware updates. Unpatched devices and applications often contain exploits and vulnerabilities that attackers may use to collect sensitive data.



You can imagine how all these issues could threaten confidentiality, integrity, or access (the CIA triad)—but confidentiality is of particular concern for mobile security.

Security measures used to protect mobile devices

There are several security measures in place to protect mobile devices from these security concerns.

Screen Locks

Screen locks are methods for preventing unauthorized access to a device. They can be particularly effective for diminishing risks associated with the loss or theft of the device. These measures include:

- **Facial recognition**: uses a device's camera to unlock the device once the user's face is recognized
- **PIN codes**: uses a sequence of four or more numbers to unlock the device
- **Fingerprint recognition**: matches a user's fingerprint with a saved image of the fingerprint to unlock the device
- **Pattern uses:** uses a pattern that users must trace to unlock the device

Remote wipes

Remote wipes are methods to remove data from a device remotely. Remote wiping is another way to diminish risks associated with the loss or theft of a device and include:

- **Locator applications**: apps that help users find lost devices
- **OS updates**: security patches regularly deployed through Operating System updates (as well as firmware and application updates)
- **Device encryption:** encryption techniques that protect the device from unauthorized access
- **Remote backup applications**: apps that allow administrators to remotely remove applications that compromise security
- **Failed login attempt restrictions**: stops access, either completely or for a set period of time, after too many failed attempts to log in
- **Antivirus/Antimalware**: software packages for mobile devices often offered by the same vendors as desktop Antivirus programs
- **Firewalls**: either devices or software that check incoming network traffic and keep out unwanted traffic

Policies and procedures

IT departments establish policies and procedures to ensure users don't make security mistakes. They typically include mobile-specific policies such as acceptable use guidelines, preferred mobile security practices, and security platforms or services.

Once IT staff and management collaborate to build a mobile security policy, there is still work to do. Organizations must find the best way to outline this policy and communicate it to users. A policy is only effective if users understand and adhere to it.

Key takeaways:

As your organization embraces the advantages of mobile devices and wireless networks, your IT security strategies must account for the specific risks, vulnerabilities, and threats associated with mobile computing by:

1. Monitoring for common mobile security concerns such as phishing, malicious applications, insecure Wi-Fi, and poor upgrade habits and applying the current methods for addressing them
2. Implementing security measures to protect mobile devices like screen lock and remote wipes
3. Providing clear mobile security policies and procedures and communicating them to users

Citations:

Top 4 mobile security threats and challenges for businesses

https://www.techtarget.com/searchmobilecomputing/tip/Top-4-mobile-security-threats-and-challenges-for-businesses

The ultimate guide to mobile device security in the workplace

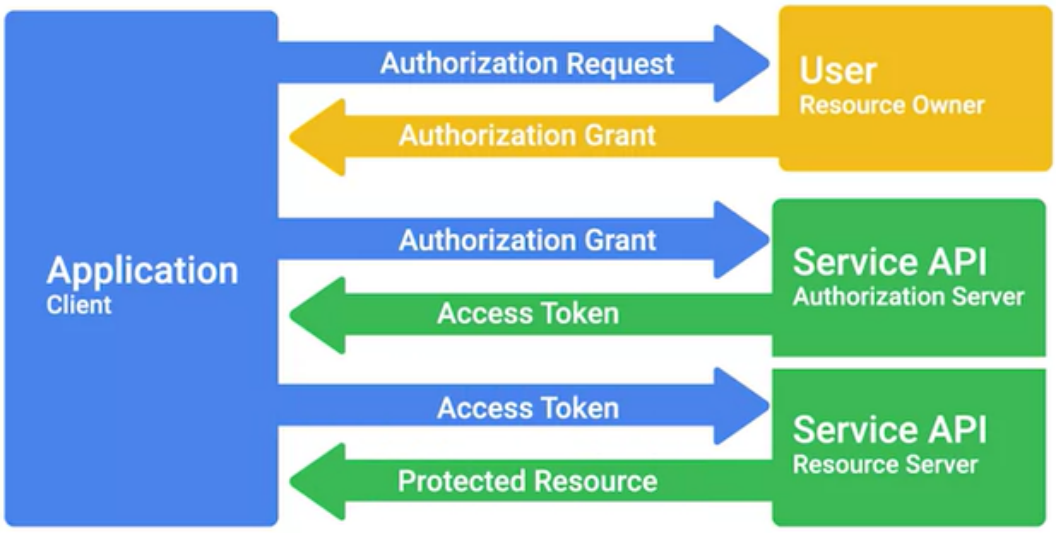
https://www.techtarget.com/searchmobilecomputing/The-ultimate-guide-to-mobile-device-security-in-the-workplace

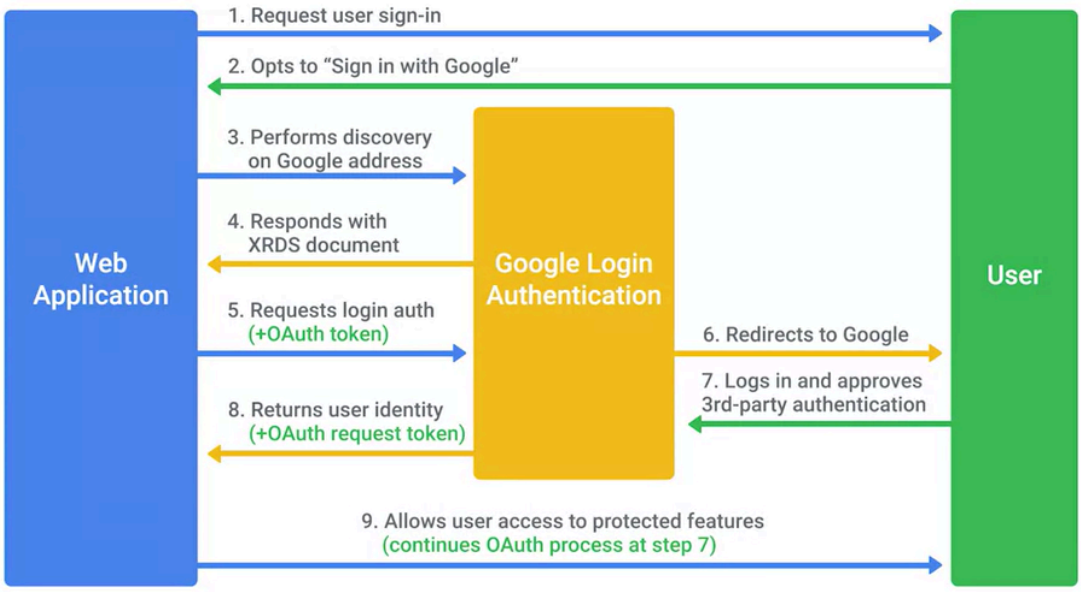
What Is the CIA Triad?

https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Understanding the significance of the three foundational information security principles: confidentiality, integrity, and availability.

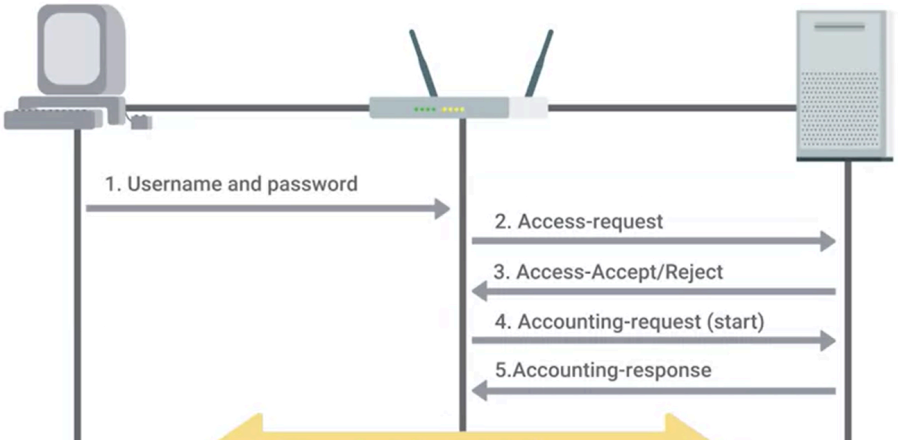
OAuth





Accounting

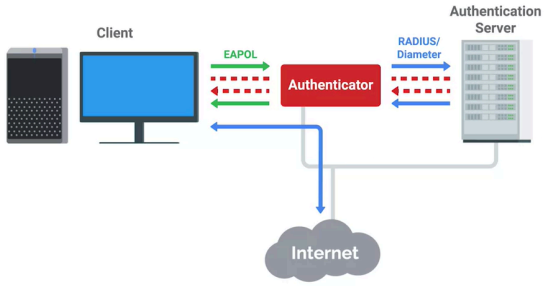
Radius Accounting Example Shown



Walkthrough of “One of the more secure wireless configurations”

From “Network Hardware Security” in Week 4

common and secure EAP methods. When a client wants to authenticate to a network using 802.1X, there are three parties involved. The client device is what we call the supplicant. It's sometimes also used to refer to the software running on the client machine that handles the authentication process for the user. The open source Linux utility, WPA supplicant is one of those. The supplicant communicates with the authenticator, which acts as a gatekeeper for the network. It requires clients to successfully authenticate to the network before they're allowed to communicate with the network. This is usually an enterprise switch or an access point in the case of wireless networks. It's important to call out that while the supplicant communicates with the authenticator, it's not actually the authenticator that makes the authentication decision. The authenticator acts like a go-between and forwards the authentication request to the authentication server. That's where the actual credential verification and authentication occurs. The authentication server is usually a radius server. EAP-TLS is an authentication type supported by EAP that uses TLS to provide mutual authentication of both the client and the authenticating server. This is considered one of the more secure configurations for wireless security. So it's definitely possible that you'll encounter this authentication type in your IT career. Like with



HTTPS is a combo of HTTP and SSL-TLS Cryptographic Protocols

IEEE 802.1X

When clients are trying to communicate on a local network, the devices must have a standard method of communication and authentication. The Institute of Electrical and Electronics Engineers (IEEE) created a standard called IEEE 802.1X. This standard specifies a common architecture, functional elements, and protocols that support authentication between the clients of ports attached to the same Local Area Network (LAN). This reading will cover what 802.1X is, basic components of authentication and how it works, and different kinds of authentication available for use under the standard.

IEEE 802.1X Protocol

IEEE 802 networks are deployed in locations that provide access to critical data, support mission critical applications, or charge for service. Port-based network access control regulates access to the network, guarding against attacks by unauthorized parties, network disruption, and data loss.

Authentication

The three main components in the authentication process are:

- **Supplicant** is the client making the request to access the LAN or wireless access point.
- **Authenticator** takes the packet from the supplicator and sends it to the authentication server until the session is authenticated. Any other information sent before authentication occurs is dropped.
- **Authentication server** provides a database of information required for authentication, and informs the authenticator to deny or permit access to the supplicant.

Authentication occurs when a client first connects to a network. The client sends a packet of information and the authenticator sends the packet to the authentication server. In some instances, the authenticator and authentication server may be integrated into a single point. The authentication server then verifies the identity or key against the information in its database. If the credentials are valid, the authentication succeeds. Then the server begins processing the connection request. If the credentials are not valid, the authentication fails. The authentication server sends an Access Reject message and the connection request is denied.

Authentication methods

When the request is sent to the authentication server there are a couple of methods for authentication. IEEE defines two different link-level authentication methods:

- **Shared key system** is a shared key or passphrase that is manually set on both the mobile device and the AP/router.
- **Open system** is when the authentication server has a list of authorized clients to check against when a client requests access. This list is usually in the form of MAC addresses but it varies by network.

Shared Key authentication methods

There are several shared key authentication methods that are commonly used:

- **Wired Equivalent Privacy (WEP)** is not recommended for a secure WLAN. The main security risk is hackers capturing the encrypted form of an authentication response frame, using widely available software applications, and using the information to crack WEP encryption.
- **Wi-Fi Protected Access (WPA)** complies with the wireless security standard and strongly increases the level of data protection and access control (authentication) for a wireless network. WPA enforces IEEE 802.1X authentication and key-exchange and only works with dynamic encryption keys.
- **Wi-Fi Protected Access 2 (WPA2)** is a security enhancement to WPA. Users must ensure the mobile device and AP/router are configured using the same WPA version and pre-shared key (PSK).
- **Association** allows the access point or router to record each mobile device so that data is properly delivered. This occurs after authentication is complete.

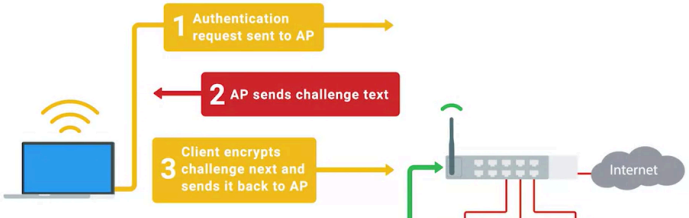
These authentication methods are standardized under the IEEE 802.1X protocol.

Key takeaways

IEEE 802.1x is a protocol developed to let clients connect to port based networks using modern authentication methods.

- There are three nodes in the authentication process: supplicant, authenticator, and authentication server.
- The authentication server uses either a shared key system or open access system to control who is able to connect to the network.
- Based on the criteria of the authentication server the supplicator will grant the authentication request and begin the connection process or it will be sent an Access Reject message and terminate the connection.

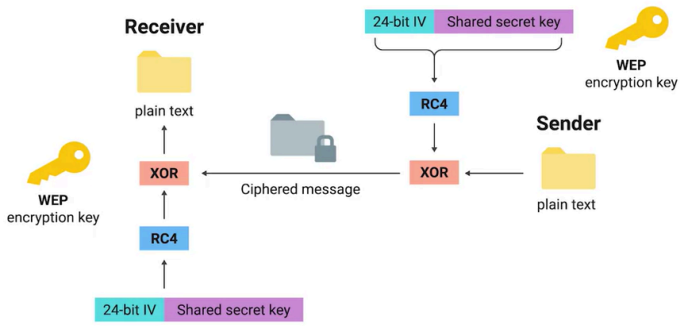
WEP



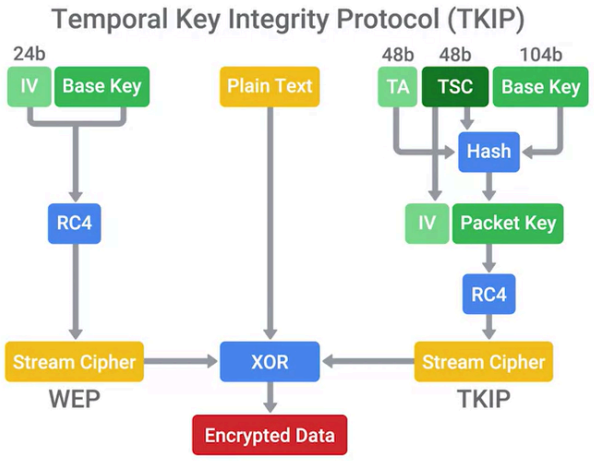
<u>← Open Mode (left)</u>

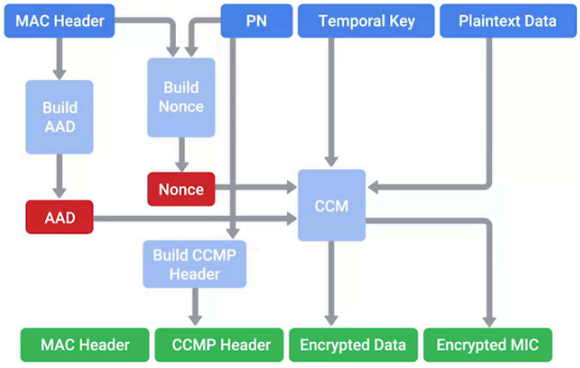
How WEP works basically (right) →

Alternatives to WEP (That were WEP hardware compatible)

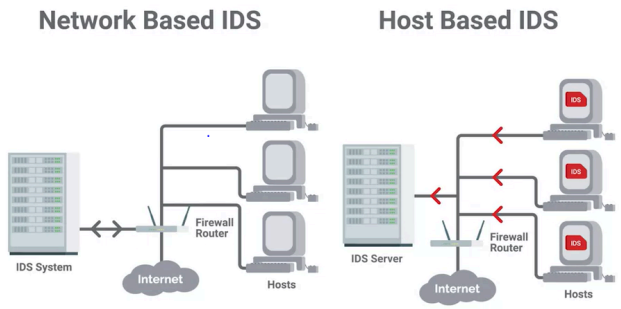


https://www.coursera.org/learn/it-security/lecture/ommXt/lets-get-rid-of-wep





Network Monitoring



Unified Threat Management (UTM)

Previously, you learned about several network security topics, including network hardening best practices, firewall essentials, and the foundations of IEEE 802.1X. In this reading, you will learn about a robust solution for network security, Unified Threat Management (UTM), along with its features, benefits, and risks.

UTM solutions stretch beyond the traditional firewall to include an array of network security tools with a single management interface. UTM simplifies the configuration and enforcement of security controls and policies, saving time and resources. Security event logs and reporting are also centralized and simplified to provide a holistic view of network security events.

UTM options and configurations

UTM solutions are available with a variety of options and configurations to meet the network security needs of an organization:

UTM hardware and software options:

- Stand-alone UTM network appliance
- Set of UTM networked appliances or devices
- UTM server software application(s)

Extent of UTM protection options:

- Single host
- Entire network

UTM security service and tool options can include:

- **Firewall:** Can be the first line of defense in catching phishing attacks, spam, viruses, malware, and other potential threats that attempt to access an organization's network. Firewalls can be hardware devices or software applications. Firewalls filter and inspect packets of data attempting to enter and exit a managed network. Rules can be configured to permit or prevent certain types of packets from entering the network.
- **Intrusion detection system (IDS):** Passively monitors packets of data and network traffic for unusual patterns that could indicate an attack. IDS devices can monitor entire networks (NIDS) or just a single host (HIDS). IDS identifies, logs, and alerts IT Support about suspicious traffic. However, IDS does not prevent an attack from occurring. This system gives IT Support professionals the opportunity to inspect flagged events to determine how to handle the threat on a case by case basis.
- **Intrusion prevention system (IPS):** Actively monitors packets and network traffic for potential malicious attacks. IPS systems can be configured to automatically block attacks or to allow manual interventions. IPS devices can monitor entire networks (NIPS) or just a single host (HIPS).
- **Antivirus software:** Uses a signature database to obtain the profiles of malicious files, such as spyware, Trojans, malware, worms, and more. The antivirus software monitors the organization's network and systems for these virus signatures. Once identified, the software will block, quarantine, or destroy them.
- **Anti-malware software:** Scans information streams for known malicious malware signatures and blocks threats. Additionally, anti-malware software can use heuristic analysis to detect novel malware threats by identifying key behaviors and characteristics. The software can also use sandboxing to isolate suspicious files.
- **Spam gateway:** Filters, identifies, and quarantines spam email. Spam gateways are network servers that use Domain Name Server (DNS) management tools to protect against spam.
- **Web and content filters:** Block user access to risky and malicious websites. When a user attempts to access an unauthorized or suspicious website using a browser, the UTM web filter can prevent the website from loading. The filter can also be customized to block certain types of websites or specific URLs, like social media or other websites that might be a distraction in the workplace.
- **Data leak/loss prevention (DLP):** Monitors outgoing network traffic for personal, sensitive, and confidential data. DLP includes a verification system to determine if the external data transfer is authorized or malicious, and can block unauthorized attempts.
- **Virtual Private Network (VPN):** Encrypts data and creates a private "tunnel" to safely transmit the data through a public network.

Stream-based vs. proxy-based UTM inspections

UTM solutions offers two methods for inspecting packets in UTM firewalls, IPS, IDS, and VPNs:

- **Stream-based inspection, also called flow-based inspection:** UTM devices inspects data samples from packets for malicious content and threats as the packets flow through the device in a stream of data. This process minimizes the duration of the security inspection, which keeps network data flowing at a faster rate than a proxy-based inspection.
- **Proxy-based inspection:** A UTM network appliance works as a proxy server for the flow of network traffic. The UTM appliance intercepts packets and uses them to reconstruct files. Then the UTM device will analyze the file for threats before allowing the file to continue on to its intended destination. Although this security screening process is more thorough than the stream-based inspection technique, proxy-based inspections are slower in the transmission of data.

Benefits of using UTM

UTM solutions can offer multiple benefits to an organization:

- **UTM can be cost-effective:** Reduces the time and resources needed to manage multiple stand-alone security tools. Purchasing a suite of integrated tools may also be less expensive than buying each tool separately.
- **UTM is flexible and adaptable:** Offers flexible solutions and options for security management. The security services and tools in a UTM can be implemented in any combination that is appropriate for each network environment.
- **UTM offers integrated and centralized management:** Consolidates multiple security tools into a central management console. This simplifies monitoring and addressing security threats, as well as streamlines the management of updates to the UTM components. The central management feature also helps IT Support staff identify and stop the full extent of an attack across an entire network.

Risks of using UTM

- **UTM can become a single point of failure in a network security attack:** If an attack disables an entire UTM solution, there would be no other backup security services or tools to stop that attack. One of the core principles of information systems management is to design and implement redundant, backup, and failover systems. When one element of an IT system is attacked or experiences a failure, there should always be a backup or parallel system to replace it.
- **UTM might be a waste of resources for small businesses:** Small businesses may not need a robust security solution like UTM. The time and money needed to purchase, implement, and manage a complex UTM system may not provide a significant return on security benefits for a smaller network. Cybercriminals are more likely to attack larger targets.

Key takeaways

- Unified Threat Management (UTM) systems offer multiple options in a comprehensive suite of network security tools. UTM solutions can be implemented as hardware and/or software and can protect either a single host or an entire network.
- UTM security services and tool options include firewalls, IDS, IPS, antivirus and anti-malware software, spam gateways, web and content filters, data leak/loss prevention, and VPN services.
- The benefits of using a UTM solution include having a cost-effective network security system that is flexible and adaptable with a management console that is integrated and centralized. The risks of using UTM include creating a single point of failure for a network security system and it might be an unnecessary use of resources for small businesses.

Home Network Security

Employees who work from home use home networks to access company files and programs. Using home networks creates security challenges for companies. Companies can provide employees guidance for protecting their home networks from attacks. This reading will cover common attacks on home networks and steps to make home networks more secure.

Common security vulnerabilities

Home networks have vulnerabilities to various types of attacks. The most common security attacks on home networks include:

- **Meddler in the middle attacks** allows a meddler to get between two communication devices or applications. The meddler then replies as the sender and receiver without either one knowing they are not communicating with the correct person, device, or application. These attacks allow the meddler to obtain login credentials and other sensitive information.

- **Data Theft** is when data within the network is stolen, copied, sent, or viewed by someone who should not have access.
- **Ransomware** uses malware to keep users from accessing important files on their network. Hackers grant access to the files after receiving a ransom payment.

Keeping home networks secure

To protect company data, employees working from home need to take steps to improve the security of their home networks. Home networks can have added protection without expensive equipment or software.

Employees can take steps to keep home networks more secure:

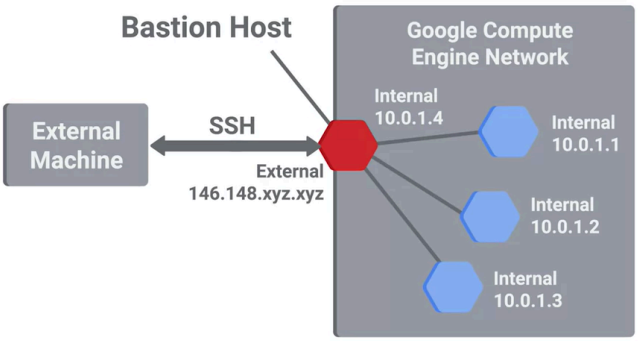
- **Change the default name and password** using the same password guidelines as your company.
- **Limit access to the home network** by not sharing access credentials outside of trusted individuals.
- **Create a guest network** that allows guests to connect to the internet but not your other devices.
- **Turn on WiFi network encryption** requiring a password before a device can access the internet.
- **Turn on the router's firewall** to prevent unwanted traffic from entering or leaving your wireless network without your knowledge. Regularly update your router firmware.
- **Update to the newest WiFi standard** which is the most secure standard for home WiFi.

Another security measure that a company can take is for employees to work over a virtual private network, or VPN. Using a VPN creates an encrypted, secure internet connection through which employees can access company data.

Key takeaways

Home network security is vital to protect a company's sensitive information when employees work from home.

- Data theft, ransomware, and meddler in the middle are common attacks on home networks.
- Employees working from home need to take steps to improve the security of their home networks.

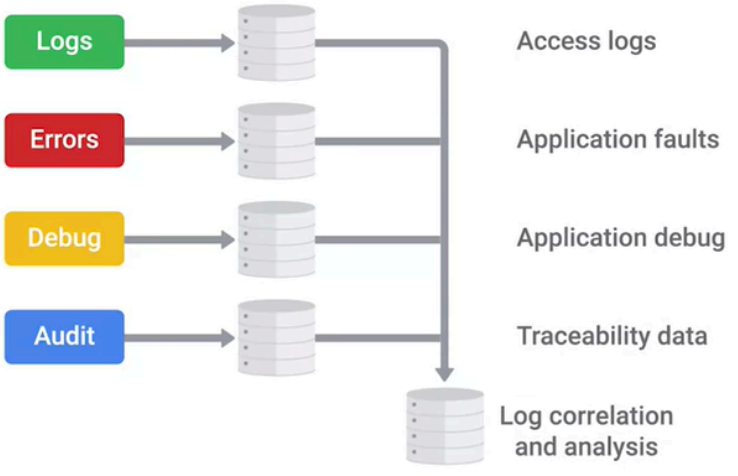


Host-Based Firewalls

Bastion Host (Right)

Logs, Analysis, Incident Investigation

See illustration (right)



Windows Defender Guide

]Microsoft 365 Defender

Previously, you learned about system hardening and critical elements in security architecture. In this reading, you will learn how Microsoft 365 Defender can be used within an organization for expanded security services and tools. You will also learn about User Account Control (UAC) and its importance in endpoint security.

Microsoft 365 Defender services

Preventing threats across an enterprise environment can be challenging for IT Support professionals. Microsoft 365 Defender can help to simplify this responsibility. Defender provides enterprise-wide security through an integrated suite of tools. It offers tools to prevent attacks, detect threats, investigate security breaches, and coordinate effective response strategies. The Defender portal also offers an action center for monitoring incidents and alerts, as well as for threat hunting and analytics.

Microsoft 365 Defender protection and services include:

- **Defender for Endpoint:** Protects network endpoints including servers, workstations, mobile devices, and IoT devices. Provides preventative safeguards, breach detections, automated analyses, and threat response services.
- **Defender Vulnerability Management:** Protects assets including, hardware, software, licenses, networks, and data. Provides asset inventory, vulnerability discovery, configuration assessment, risk-based prioritization, and remediation tools.
- **Defender for Office 365:** Protects Microsoft 365 (formerly Office 365), including Exchange, Outlook, files, and attachments. Guards against malicious threats entering from email messages, links (URLs), and collaboration tools.
- **Defender for Identity:** Protects user identities and credentials. Detects, identifies, and investigates advanced threats, compromised identities, and malicious actions performed using stolen user identities or by internal threats.
- **Azure Active Directory Identity Protection:** Protects cloud-based identities in Azure by automating detection and resolutions for identity risks.
- **Defender for Cloud Apps:** Protects cloud applications by providing deep visibility searches, robust data controls, and advanced threat protection.

Using Microsoft 365 Defender

As an IT Support professional in an organization, you might use Microsoft 365 Defender to monitor your enterprise's IT security. You can customize the Defender portal Home page by job roles. Various security cards can be selected to appear on the Home page for your role. For example, you might see cards for monitoring:

- **Identities:** Monitor user identities for suspicious or risky behaviors.
- **Data**: Track user activity that is risky to data security.
- **Devices**: See alerts, breach activity, and other threats on devices connected to the organization's network.
- **Apps**: Observe how cloud apps are being used in your organization.
- **Incidents:** Review attacks through compiled comprehensive incident data.
- **Alerts:** View alerts compiled from across the Microsoft 365 suite.
- **Advanced hunting:** Scan for suspicious files, malware, and risky activities.
- **Threat Analytics:** View information about current cybersecurity threats.
- **Secure score:** Get a calculated score for your security configuration and recommendations on how to improve your score.
- **Learning hub:** Easily access Microsoft 365 security tutorials and other learning materials.
- **Reports:** Obtain information to help you better protect your organization.

Microsoft 365 Defender aggregates and organizes this monitoring data to provide IT Support professionals details on where attacks began, which malicious tactics were used, the scope of the attacks, and other related incident information.

Microsoft 365 Defender in action

The following are examples of how a cyberattack might penetrate and infect an enterprise network. For each type of malicious attack, a potential Microsoft 365 Defender response follows, illustrating how the security suite could respond:

A phishing attempt enters through email: An employee in an organization receives an email from a business that appears to be legitimate, like a bank. The email might claim that there is a problem with the employee's account and that they must click on a given link to resolve the problem. However, the phishing email actually contains a link to a malicious website that a cybercriminal disguised to look like a real bank. If the employee clicks on the link to view the website, the site requests that the user enter their account credentials or other sensitive information. This information is then transmitted to the cybercriminal.

- **Microsoft Defender for Office 365** detects the emailed phishing scam by monitoring Exchange and Outlook. Both the employee and the IT Support team are alerted about this attempted phishing attack.

Malware enters through social media: An employee clicks on an enticing link posted on their favorite social media app. The link triggers an automatic download of a malware file to the employee's laptop.

- **Microsoft Defender for Endpoint** monitors the employee's laptop for suspicious malware signatures. Upon detecting the malware, Defender for Endpoint alerts the employee and the organization's IT Support team about the malware and discloses its endpoint location.

A cybercriminal intercepts an employee's work login credentials: An employee accesses their work account using their laptop and an open Wi-Fi access point in a busy coffee shop. A cybercriminal is in the same coffee shop to intercept and collect unprotected information flowing through the open Wi-Fi access point. The cybercriminal obtains the employee's user account credentials and uses them to hijack the employee's work account. The cybercriminal then begins a malicious attack on the employer's network.

- **Microsoft Defender for Identity** can detect the sudden change in activity on the employee's user account. Defender for Identity alerts the employee and the IT Support team about the compromised user identity.

A virus enters a cloud drive through a file upload: An employee unknowingly uploads an file that is infected with a virus to their work cloud storage drive. When the employee opens the file from the cloud drive, the virus is activated and begins changing the security settings on the other files in the employees cloud drive.

- **Microsoft Defender for Cloud Apps** detects the unusual pattern of activity and alerts the employee and IT Support team of the suspicious activity in the cloud account.

User Account Control (UAC)

User Account Control (UAC) allows IT administrators to create standard user accounts with limited access rights and privileges for end users. This configuration can prevent users from installing unauthorized programs, changing system settings, tampering with firewalls, and more. In order to perform these types of tasks, administrator credentials must be provided. For less restrictive controls, UAC provides the option to grant end users local administrative privileges for approved activities that require administrative privileges. For more restrictive controls, UAC can require global administrator credentials be entered for each and every administrative change the user attempts to make.

Resources for more information

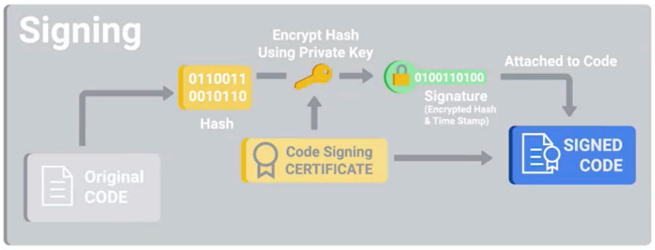
To learn more about Microsoft Defender through the Microsoft learning portal, please visit:

- Microsoft Learn: Introduction to Microsoft 365 Defender - Microsoft's self-paced course for Microsoft 365 Defender
- Protect your organization with Microsoft 365 Defender - An interactive guide to Microsoft 365 Defender and how it detects security risks, investigates attacks, and prevents harmful activities.
- Microsoft Defender for Endpoint - Gives an overview of product, services, architecture, and training opportunities.
- Microsoft Defender Vulnerability Management - Provides information about the services and tools available to find and fix vulnerabilities.

- Microsoft Defender for Office 365 - Lists included services and tools for various product levels, as well as the types of threats it protects against.
- Microsoft Defender for Identity - Offers product information, how-to guides, tutorials, and reference information.
- Microsoft Defender for Cloud Apps - Provides product overview, quickstart reference guide, tutorials, best practices, and additional resources.
- How User Account Control works - User Account Control (UAC) is a fundamental component of Microsoft's overall security vision. UAC helps mitigate the impact of malware.

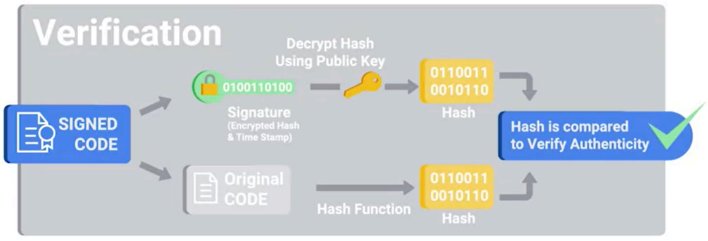
Anti-Malware Protection

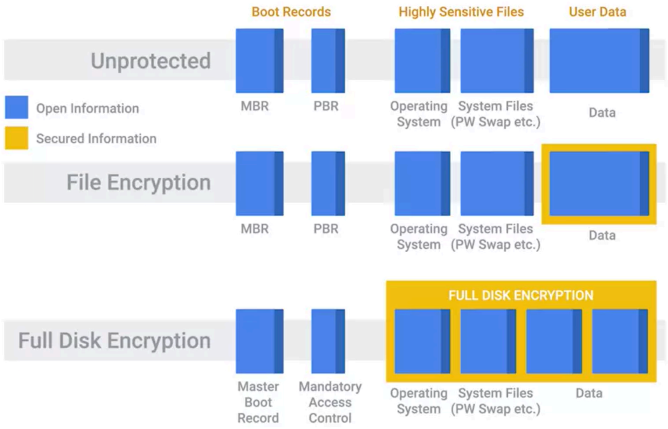
Binary Whitelisting (right)

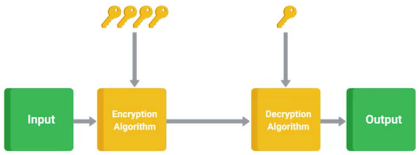


Disk Encryption

See below







Supplemental Reading on Disk Encryption Tools

https://www.coursera.org/learn/it-security/supplement/Gguk0/supplemental-reading-for-disk-encryption

Browser Hardening

In this reading, you will learn how to harden browsers for enhanced internet security. The methods presented include evaluating sources for trustworthiness, SSL certificates, password managers, and browser security best practices. Techniques for browser hardening are important components in enterprise-level IT security policies. These techniques can also be used to improve internet security for organizations of any size and for individual users.

Identifying trusted versus untrusted sources

Some cybercriminals monitor SEO search terms for popular software downloads. Then they create fake websites to pose as hosts for these popular downloads. They might even use advertising and stolen logos of trusted companies to make the sites appear to be legitimate businesses. However, the downloadable files available on the cybercriminals' websites are usually malicious software. Unaware of the deception, users download and install the malware. In some cases, the users don't even need to download a file. Savvy cybercriminals can design web pages that have the ability to infect users' devices simply upon visiting the sites.

To guard against threats like this, there are checks you can perform to evaluate websites:

- **Use antivirus and anti-malware software and browser extensions.** Run antivirus and anti-malware scans regularly and scan downloaded files. Ensure antivirus and anti-malware browser extensions are enabled when surfing the web.
- **Check for SSL certificates.** See the "Secure connections and sites" section below.
- **Ensure the URL displayed in the address bar shows the correct domain name.** For example, Google websites use the Google.com domain name.

- **Search for negative reviews of the website from trusted sources.** Be wary of websites that have few to no reviews. They may not have been active long enough to build a bad reputation. Cybercriminals will create new websites when they get too many negative reviews on their older sites.
- **Don't automatically trust website links provided by people or organizations you trust.** They may not be aware that they are passing along links to malicious websites and files.
- **Use hashing algorithms for downloaded files.** Compare the developer-provided hash value of the original file to the hash value of the downloaded copy to ensure the two values match.

Secure connections and sites

Secure Socket Layer (SSL) certificates are issued by trusted certificate authorities (CA), such as DigiCert. An SSL certificate indicates that any data submitted through a website will be encrypted. A website with a valid SSL certificate has been inspected and verified by the CA. You can find SSL certificates by performing the following steps:

1. Check the URL in the address bar. The URL should begin with the **https://** protocol. If you see **http://** without the "s", then the website is not secure.
2. Click on the closed padlock icon in the address bar to the left of the URL. An open lock indicates that the website is not secure.
3. A pop-up menu should open. Websites with SSL certificates will have a menu option labeled "Connection is secure." Click on this menu item.
4. A new pop-up menu will appear with a link to check the certificate information. The layout and wording of this pop-up will vary depending on which browser you are using. When you review the certificate, look for the following items:4
    a. **The name of the issuer** - Make sure it is a trusted certificate authority.
    b. **The domain it was issued to** - This name should match the website domain name.
    c. **The expiration date** - The certificate should not have passed its expiration date.

Note that cybercriminals can obtain SSL certificates too. So, this is not a guarantee that the site is safe. CAs also vary in how thorough they are in their inspections.

Password managers

Password managers are software programs that encrypt and retain passwords in secure cloud storage or locally on users' personal computing devices. There are a wide variety of activities users perform online that require unique and complex passwords, such as banking, managing health records, filing taxes, and more. It can be difficult for users to keep track of so many different logins and passwords. Fortunately, password managers can help.

- **Advantages of using a password manager:**
    - It provides only one password for a user to remember;
    - Can generate and store secure passwords that are difficult for cybercriminal tools to crack;
    - Is more secure than keeping passwords written down on paper or in an unencrypted file on a computer; and
    - Work across multiple devices and operating systems.
- **Disadvantages of using a password manager:**
    - It can expose all of the user's account credentials if a cybercriminal obtains the master password to the password manager;
    - Can be very difficult for a user to regain access to the password manager account if the master password is lost or forgotten;
    - Requires the user to learn a new method for logging in to their various accounts in order to retrieve passwords from the password manager software; and
    - Often requires a fee or subscription for password management services.

A few of the top brands for password manager applications include Bitwarden, Last Pass, and 1Password. Please see the Resource section at the end of this reading for more information.

Browser settings

Browser settings can be configured for additional safety measures. Some additional options for hardening browsers include:

1. Use pop-up blockers: Disable Web Browser Pop-up Blockers
2. Clear browsing data and cache: Clear your web browser's cache, cookies, and history
3. Use private-browsing mode: How to Turn on Incognito Mode in Your Browser
4. Sign-in/browser data synchronization:
    a. Turn sync on and off in Chrome
    b. Disable Firefox Sync
    c. Change and customize sync settings in Microsoft Edge
5. Use ad blockers: How to block ads

Key takeaways

You learned about multiple steps you can take to harden a browser and protect your online security:

- **Identify if sources can be trusted or not:**
    - Use antivirus and anti-malware software and browser extensions.
    - Check for SSL certificates.
    - Ensure the URL displayed in the address bar shows the correct domain name.
    - Search for negative reviews of the website from trusted sources.
    - Don't automatically trust website links provided by people or organizations you trust.
- **Use a password manager**
- **Configure your browser settings:**
    - Use pop-up blockers.
    - Clear browsing data and cache.
    - Use private-browsing mode.
    - Sign-in/browser data synchronization.
    - Use ad blockers.

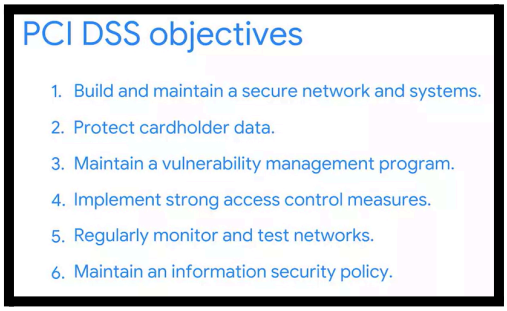
Resources for more information

To learn more about hardening bowsers for safer web surfing, please visit the following articles:

- Dubious downloads: How to check if a website and its files are malicious - Provides information on evaluating websites and downloads for the presence of malware.
- The Best Password Managers to Secure Your Digital Life - Compares and contrasts the top password managers on the market.
- Avoiding Social Engineering and Phishing Attacks - Tips for avoiding an array of internet scams.
- Blocking Unnecessary Advertising Web Content - From the United States National Security Agency Cybersecurity Information, notice about ad-blocking through network functions, at the host level, and other concerns.
- Securing Web Browsers and Defending Against Malvertising for Federal Agencies - From the United States Cybersecurity and Infrastructure Security Agency, guide for protecting computing systems from malvertising.
- Browser sync—what are the risks of turning it on? - Explains the security threats associated with having browsers set to synchronize account data across multiple devices.
- List of Participants - Microsoft Trusted Root Program - Microsoft's list of trusted Certificate Authorities and the common names of the issued certificates.

WEEK 6 BABAY!

Data Destruction



Data destruction is removing or destroying data stored on electronic devices so that an operating system or application cannot read it. Data destruction is required when a company no longer needs a device, when there are unused or multiple copies of data, or you are required to destroy specific data.

There are three categories of data destruction methods: recycling, physical destruction, and third-party destruction. This reading will introduce the data destruction methods and how to decide which method to use.

Recycling

Recycling includes methods that allow for device reuse after data destruction. This option is recommended if you hope to reuse devices internally, sell surplus equipment, or your devices are on loan and are due to be returned. Standard recycling methods include the following:

- **Erasing/wiping**: cleans all data off a device's hard drive by overwriting it. Erasing or wiping data can be done manually or with data-destruction software. This method is practical when you only have a few devices that need data destroyed, as it takes a long time. Note that it may take multiple passes to wipe highly sensitive data completely.
- **Low-level formatting:** erases all data written on the hard drive by replacing it with zeros. Low-level reformatting can be done using a tool such as HDDGURU on a PC or the Disk Utility function on a Mac.
- **Standard formatting:** erases the path to the data and not the data itself. Both PCs and Macs have internal tools that can perform a standard format, Disk Management on a PC or Disk Utility on a Mac. Note that standard formatting does not remove the data from the device, enabling data rediscovery using software.

Physical destruction

Physical destruction includes any method that physically destroys a device to make it difficult to retrieve data from it. You should only use physical destruction if you do not need to reuse the device. However, only completely destroying the device ensures the destruction of all data with physical methods. Physical destruction methods include the following:

- **Drilling** holes directly into the device wipes data out on the sections where there are holes. However, individuals can recover data from the areas that are still intact.
- **Shredding** includes the physical shredding of hard drives, memory cards, CDs, DVDs, and other electronic storage devices. Shredding reduces the potential for recovery. Shredding requires special equipment or outsourcing to another facility.
- **Degaussing** uses a high-powered magnet which destroys the data on the device. This method effectively destroys large data storage devices and renders the hard drive unusable. As electronic technology changes, this method may become obsolete
- **Incinerating** destroys data by burning the device. Most companies do not have an incinerator on-site. Devices need to be transported to a facility for incineration. Due to this, devices can be lost or stolen in transit.

In addition to effectively destroying data on electronic devices, it is essential to follow best practices for electronic device disposal.

Outsourcing

Outsourcing means using a third-party specializing in data destruction to complete the physical or recycling process. This option appeals to companies that do not have the staff or knowledge to complete the destruction themselves. Once a vendor has completed the task, they issue a certificate of destruction/recycling.

The certificate of destruction serves as a statement of completed destruction of data on electronics, hard drives, or other devices. The certificate includes the client's contact information, date of service, vendor company name, manifest, signature, method of destruction, and legal statement. However, exercise caution as the certificate

does not indicate a level of training, auditing, or any other verification that a vendor is knowledgeable about data destruction.

Key Takeaways

Data destruction makes data unreadable to an operating system or application. You should destroy data on devices no longer used by a company, unused or duplicated copies of data, or data that's required to destroy. Data destruction methods include:

- **Recycling:** erasing the data from a device for reuse
- **Physical destruction**: destroying the device itself to prevent access to data
- **Outsourcing**: using an external company specializing in data destruction to handle the process

Resource for further information

For more information about disposing of electronics, please visit Proper Disposal of Electronic Devices, a resource from CISA.

Incident Response

When you've had a data breach, you may need forensic analysis to analyze the attack. This analysis usually involves extensive evidence gathering. This reading covers some considerations for protecting the integrity of your forensic evidence and avoiding complications or issues related to how you handle evidence.

Regulated data

It's important to consider the type of data involved in an incident. Many types of data are subject to government regulations that require you to take extra care when handling it. Here are some examples you're likely to encounter as an IT support specialist.

1. **Protected Health Information:** This information is regulated by the Health Insurance Portability and Accountability Act (HIPAA). It is personally identifiable health information that relates to:

- Past, present, or future physical or mental health or condition of an individual
- Administration of health care to the individual by a covered provider (for example, a hospital or doctor)
- Past, present, or future payment for the provision of health care to the individual

2. **Credit Card or Payment Card Industry (PCI) Information:** This is information related to credit, debit, or other payment cards. PCI data is governed by the Payment Card Industry Data Security Standard (PCI DSS), a global information security standard designed to prevent fraud through increased control of credit card data.

3. **Personally Identifiable Information (PII):** PII is a category of sensitive information associated with a person. Examples include addresses, Social Security Numbers, or similar personal ID numbers.

4. **Federal Information Security Management Act (FISMA) compliance:** FISMA requires federal agencies and those providing services on their behalf to develop, document, and implement specific IT security programs and to store data on U.S. soil. For example, organizations like NASA, the National Institutes of Health, the Department of Veteran Affairs—and any contractors processing or storing data for them—need to comply with FISMA.

5. **Export Administration Regulations (EAR) compliance:** EAR is a set of U.S. government regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security (BIS). These regulations govern the export and re-export of commercial and dual-use goods, software, and technology. Dual-use goods

are items that can be used both for civilian and military applications. These goods are heavily regulated because they can be classified for civilian use and then transformed for military purposes.

Digital rights management (DRM)

Digital Rights Management (DRM) technologies can help ensure data regulations compliance. DRM technology comes in the form of either software or hardware solutions. Both options allow content creators to prevent deliberate piracy and unauthorized usage. DRM often involves using codes that prohibit content copying or limit the number of devices that can access a product. Content creators can also use DRM applications to restrict what users can do with their material. They can encrypt digital media so only someone with the decryption key can access it. This gives content creators and copyright holders a way to:

- **Restrict users** from editing, saving, sharing, printing, or taking screenshots of content or products
- **Set expiration dates** on media to prevent access beyond that date or limit the number of times users can access the media
- **Limit access** to specific devices, Internet Protocol (IP) addresses, or locations, such as limiting content to people in a specific country

Organizations can use these DRM capabilities to protect sensitive data. DRM enables organizations to track who has viewed files, control access, and manage how people use the files. It also prevents files from being altered, duplicated, saved, or printed. DRM can help organizations comply with data protection regulations.

End User Licensing Agreement (EULA)

End User Licensing Agreements (EULAs) are similar to DRM in specifying certain rights and restrictions that apply to the software. You often encounter EULA statements when installing a software package, accessing a website, sharing a file, or downloading content. A EULA is usually considered a legally binding agreement between the owner of a product (e.g., a software publisher) and the product's end-user. The EULA specifies the rights and restrictions that apply to the software, and it's usually presented to users during installation or setup of the software. You can't complete an installation (or access, share, or download data) until you agree to the terms written in the EULA statement.

Unlike DRM restrictions, EULAs are only valid if you agree to it (i.e., you check a box or click the 'I Agree' button). DRM restrictions don't require your agreement—or rely on you to keep that agreement. DRMs are built into the product they protect, making it easier for content creators to ensure users do not violate restrictions.

Chain of custody

"Chain of custody" refers to a process that tracks evidence movement through its collection, safeguarding, and analysis lifecycle. Maintaining the chain of custody makes it difficult for someone to argue that the evidence was tampered with or mishandled. Your chain of custody documentation should answer the following questions. Documentation for these questions must be maintained and filed in a secure location for current and future reference.

- Who collected the evidence? Evidence can include the afflicted or used devices, media, and associated peripherals.
- How was the evidence collected, and where was it located?
- Who seized and possessed the evidence?
- How was the evidence stored and protected in storage? The procedures involved in storing and protecting evidence are called evidence-custodian procedures.
- Who took the evidence out of storage and why? Ongoing documentation of the names of individuals who check out evidence and why must be kept.

When a data breach occurs, forensic analysis usually involves taking an image of the disk. This makes a virtual copy of the hard drive. The copy lets an investigator analyze the disk's contents without modifying or altering the

original files. An alteration compromises the integrity of the evidence. This kind of compromised integrity is what you want to avoid when performing forensic investigations.

Key takeaways:

Incident handling requires careful attention and documentation during an incident investigation's analysis and response phases.

- Be familiar with what types of regulated data may be on your systems and ensure proper procedures are in place to ensure your organization's compliance.
- DRM technologies can be beneficial for safeguarding business-critical documents or sensitive information and helping organizations comply with data protection regulations.
- When incident analysis involves the collection of forensic evidence, you must thoroughly document the chain of custody.

BYOD

In this reading, you will learn about a business practice called "bring your own device" (BYOD), as well as the security risks related to BYOD policies and how to mitigate these risks. Organizations can reduce IT costs by limiting the number of company-owned mobile devices issued to employees. Instead, businesses are passing on the costs of mobile devices and cellular services to employees by allowing employees to bring their own devices for business use.

Bring your own device (BYOD)

Traditionally, IT departments would provide mobile devices to employees for business use. This gave the IT staff control over the security of those devices. Today, an increasing number of companies permit employees to bring their own devices to work. This trend started with employees requesting permission to carry a single smartphone rather than carrying one phone for work and one for personal use. Organizations noticed the cost savings gained by allowing their employees to select their personal smartphones as the single device. By using smartphones with dual SIM card slots or phone apps like Google Voice, users can configure multiple phone lines on a single smartphone. However, BYODs can become dangerous security threats to companies' data and networks. IT departments do not have the same level of control over the security of BYOD devices as they would with company-owned devices.

BYOD Threats

Some of the potential threats BYODs pose to company networks, resources, and data include:

- **Loss or theft** could result in an organization's data being stolen or the lost device being used to gain unauthorized access to a company's network.
- **Data loss**, including:

1. **Data leakage** losses can happen when a computing device is lost or compromised; when an employee accidentally saves or sends confidential information to the wrong destination; when a disgruntled employee exposes data maliciously; or when viruses, malware, phishing attacks, etc. penetrate organizations' networks.
2. **Data portability** losses can occur when former employees take company data with them on their BYOD when they resign or are fired by the organization.

- **Security vulnerabilities** are any type of weakness in the security of a device or network that provides access for a threat to penetrate the system.
- **Meddler in the middle attacks (MITM)** occur when an attacker monitors the data transfers between two sources with the intent to copy and/or interfere with that information. One of the most common opportunities for an MITM attack arises when a mobile device accesses important information through a public Wi-Fi connection, such as at a hotel or restaurant.

- **Malware** is malicious software that can be used to steal, modify, or delete data. It can also be used to gain unauthorized access to a device or network.
- **Jailbreaking** happens when a manufacturer's protective restrictions are removed on a mobile device. Without these restrictions, a device becomes vulnerable to the risk of the user unknowingly installing malicious software.

Solutions

To mitigate these threats, organizations and their IT departments should design security policies for BYOD use inside company networks. Some preventative steps could include:

1. **Develop a bring your own device (BYOD) policy:** IT departments and organizations can create written policies that detail the minimum technology requirements for permitted BYODs, provide instructions for employees on how to properly secure their devices, and list the rules for safe data access and storage.
2. **Use Mobile Device Management (MDM) software:** MDM software can be used to enforce BYOD policy requirements for mobile devices to help secure company data and networks. IT departments can use MDM software to:
    a. Automatically install apps and updates, including antivirus and anti-malware software
    b. Configure secure connections to an organization's wireless networks
    c. Encrypt storage on devices
    d. Require a lock screen and password
    e. Remote wipe a mobile device that is lost or stolen
    f. Block the execution of certain apps
    g. Meet compliance standards
    h. Prevent data being shared or stored in unauthorized locations
    i. Manage devices remotely
3. **Use an Enterprise Mobile Management (EMM) system:** MDM policies are specific to mobile operating systems. In order to distribute MDM policies across Android, iOS, and other mobile operating systems, the BYODs can be enrolled through an Enterprise Mobility Management (EMM) system.
4. **Require the use of multi-factor authentication (MFA):** Users can be authenticated by presenting more than one method of identification. Some common identification factors include:
    a. **Something you know**: a password or pin number
    b. **Something you have:** a physical token, like an ATM or bank card, USB device, key fob, or OTP (one-time password)
    c. **Something you are**: biometric data, like a fingerprint, voice signature, facial recognition, or retina scan
    d. **Somewhere you are**: location-dependent access, like a Global Positioning System (GPS) location
    e. **Something you do**: gestures, like swipe patterns; Turing tests, like CAPTCHA; or normal patterns of behavior, like regular login and logout times
5. **Set an acceptable use policy (AUP):** Organizations could create policies that set a code of conduct for use of the companies' data, systems, network, and other resources.
6. **Use non-disclosure agreements (NDA):** Organizations can create legally binding contracts with employees to assert the confidentiality and security policies for the companies' data and intellectual property.
7. **Restrict data access**: IT departments should protect company data by limiting access to only those employees who need access to perform their jobs.
8. **Educate staff about data security:** Organizations can provide training manuals and seminars to inform employees about network security risks and to instruct on how to secure their BYODs.
9. **Back up device data:** IT departments need to create backup policies for all important data. This should include a schedule for frequency of backups, storage space for the back-up copies, how long back-ups should be stored, and disaster recovery plans.
10. **Data leakage prevention (DLP):** IT departments can implement DLP software solutions to help manage and protect confidential information.

Key takeaways

Organizations are taking advantage of the cost savings created by adopting “bring your own device” (BYOD) policies for employees. However, permitting employees to connect personal mobile devices to company networks introduces multiple security threats. There are a variety of security measures that IT departments can implement to protect organizations’ information systems:

- Develop BYOD policies
- Enforce BYOD policies with MDM software
- Distribute MDM settings to multiple OSes through EMM systems
- Require multi-factor authentication (MFA)
- Create acceptable use policies for company data and resources
- Require employees to sign NDAs
- Limit who can access data
- Train employees on data security
- Back up data regularly

Resources for more information

- BYOD (bring your own device) - Additional information on how BYOD works, why is it important, level of access options, risks, challenges, policy comparisons, best practices, how to implement a BYOD policy.
- BYOD policy: An in-depth guide from an IT leader - Compares BYOD advantages and disadvantages, what should be included in a BYOD policy, tips for reducing security risks, and more.
- What is MDM? - Introduces the purpose of MDM software, how it works, advantages of using MDM, use cases, and more.
- Enterprise Mobility Management (EMM) - Outlines the features, services, and benefits of EMM systems.

Authentication

Authentication will be handled centrally by an LDAP server and will incorporate One-Time Password generators as a 2nd factor for authentication.

External Website

The customer-facing website will be served via HTTPS, since it will be serving an e-commerce site permitting visitors to browse and purchase products, as well as create and log into accounts. This website would be publically accessible.

Internal Website

The internal employee website will also be served over HTTPS, as it will require authentication for employees to access. It will also only be accessible from the internal company network and only with an authenticated account.

Remote Access

Since engineers require remote access to internal websites, as well as remote command line access to workstations, a network-level VPN solution will be needed, like OpenVPN. To make internal website access easier, a reverse proxy is recommended, in addition to VPN. Both of these would rely on the LDAP server that was previously mentioned for authentication and authorization.

Firewall

A network-based firewall appliance would be required. It would include rules to permit traffic for various services, starting with an implicit deny rule, then selectively opening ports. Rules will also be needed to allow public access to the external website, and to permit traffic to the reverse proxy server and the VPN server.

Wireless

For wireless security, 802.1X with EAP-TLS should be used. This would require the use of client certificates, which can also be used to authenticate other services, like VPN, reverse proxy, and internal website authentication. 802.1X is more secure and more easily managed as the company grows, making it a better choice than WPA2.

VLANs

Incorporating VLANs into the network structure is recommended as a form of network segmentation; it will make controlling access to various services easier to manage. VLANs can be created for broad roles or functions for devices and services. An engineering VLAN can be used to place all engineering workstations and engineering services on. An Infrastructure VLAN can be used for all infrastructure devices, like wireless APs, network devices, and critical servers like authentication. A Sales VLAN can be used for non-engineering machines, and a Guest VLAN would be useful for other devices that don't fit the other VLAN assignments.

Laptop Security

As the company handles payment information and user data, privacy is a big concern. Laptops should have full disk encryption (FDE) as a requirement, to protect against unauthorized data access if a device is lost or stolen. Antivirus software is also strongly advised to avoid infections from common malware. To protect against more

uncommon attacks and unknown threats, binary whitelisting software is recommended, in addition to antivirus software.

Application Policy

To further enhance the security of client machines, an application policy should be in place to restrict the installation of third-party software to only applications that are related to work functions. Specifically, risky and legally questionable application categories should be explicitly banned. This would include things like pirated software, license key generators, and cracked software.

In addition to policies that restrict some forms of software, a policy should also be included to require the timely installation of software patches. “Timely” in this case will be defined as 30 days from the wide availability of the patch.

User Data Privacy Policy

As the company takes user privacy very seriously, some strong policies around accessing user data are a critical requirement. User data must only be accessed for specific work purposes, related to a particular task or project. Requests must be made for specific pieces of data, rather than overly broad, exploratory requests. Requests must be reviewed and approved before access is granted. Only after review and approval will an individual be granted access to the specific user data requested. Access requests to user data should also have an end date.

In addition to accessing user data, policies regarding the handling and storage of user data are also important to have defined. These will help prevent user data from being lost and falling into the wrong hands. User data should not be permitted on portable storage devices, like USB keys or external hard drives. If an exception is necessary, an encrypted portable hard drive should be used to transport user data. User data at rest should always be contained on encrypted media to protect it from unauthorized access.

Security Policy

To ensure that strong and secure passwords are used, the password policy below should be enforced:

- Password must have a minimum length of 8 characters
- Password must include a minimum of one special character or punctuation
- Password must be changed once every 12 months

In addition to these password requirements, a mandatory security training must be completed by every employee once every year. This should cover common security-related scenarios, like how to avoid falling victim to phishing attacks, good practices for keeping your laptop safe, and new threats that have emerged since the last time the course was taken.

Intrusion Detection or Prevention Systems

A Network Intrusion Detection System is recommended to watch network activity for signs of an attack or malware infection. This would allow for good monitoring capabilities without inconveniencing users of the network. A Network Intrusion Prevention System (NIPS) is recommended for the network where the servers containing user data are located; it contains much more valuable data, which is more likely to be targeted in an attack. In addition to Network Intrusion Prevention, Host-based Intrusion Detection (HIDS) software is also recommended to be installed on these servers to enhance monitoring of these important systems.

Bonus Week! JOB SEARCHING

GOOGLE IT SUPPORT PROFESSIONAL CERTIFICATE SKILLS LIST

- Basic computer architecture
- Operating systems (Windows, Linux)
- Remote connection and virtual machines
- Computer networking
- Software management
- Troubleshooting
- Customer service
- Routing concepts
- VPNs and proxies
- Permissioning
- Package and software management
- Process management
- Resource monitoring
- Systems administration
- Configuration
- Centralized management
- Implementing/managing directory services
- Data management and recovery
- IT security
- Cryptology/encryption
- Hashing
- Network security

Common Job Search Terms

- Technical Support Specialist
- IT Help Desk
- Help Desk
- IT Technician
- IT Support Specialist
- Computer User Specialist
- IT Helpdesk Technician
- Computer Support
- Technical Support
- IT Assistant