Prelude to Core 1 Notes

Per Scholas Notes, Archived

Chapters 1-10 contained within the “Document Tabs”

The “gaps” in some chapters are due to the original content source having multiple labs quizzes which cannot be replicated in these notes.

Chapters 1&2 are not well written, seek revision at a later date.
Chapters 5, 6 & 8 have subchapters that may need revision.

Below is the final list from study materials pre-certification test.

1. DomainKeys Identified Mail (DKIM) provides a cryptographic authentication mechanism. This can replace or supplement SPF. To configure DKIM, the organization uploads a public key as a TXT record in the DNS server. Sender Policy Framework (SPF) uses a DNS record published by an organization hosting an email service. The SPF record identifies the hosts authorized to send emails from that domain, and there must be only one per domain. SPF does not provide a cryptographic authentication mechanism like DKIM does, though. The Domain-Based Message Authentication, Reporting, and Conformance (DMARC) framework can ensure that SPF and DKIM are being utilized effectively. DMARC relies on DKIM for the cryptographic authentication mechanism, making it the incorrect option for this question. The simple mail transfer protocol (SMTP) is a communication protocol for electronic mail transmission that does not utilize cryptographic authentication mechanisms by default.
2. Nameserver (NS) records are used to list the authoritative DNS server for a particular domain. Mail Exchange (MX) records are used to provide the mail server that accepts email messages for a particular domain. Text (TXT) records are used to provide information about a resource such as a server, network, or service in human-readable form. They often contain domain verification and domain authentications for third-party tools that can send information on behalf of a domain name. Service (SRV) records are used to provide host and port information on services such as voice over IP (VoIP) and instant messaging (IM) applications. The DNS text (TXT) record lets a domain administrator enter text into the Domain Name Systems. The TXT record was originally intended as a place for human-readable notes. However, now it is also possible to put some machine-readable data into TXT records. TXT records are a key component of several different email authentication methods (SPF, DKIM, and DMARC) that help an email server determine if a message is from a trusted source. A DNS service (SRV) record specifies a host and port for specific services such as voice over IP (VoIP), instant messaging, and others. A Start of Authority (SOA) resource record indicates which Domain Name Server (DNS) is the best source of information for the specified domain. PTR records are used for the Reverse DNS (Domain Name System) lookup. Using the IP address, you can get the associated domain/hostname. An A record should exist for every PTR record.
3. The mATX (microATX) motherboard's form factor is 9.6" x 9.6" in size (24 cm x 24 cm). The mATX form factor is commonly used in smaller computer systems with a small form factor (SFF) case. An mATX motherboard is backward-compatible with the larger ATX motherboard since it contains the same mounting point locations as the full-size board. An ATX motherboard's form factor is 12" x 9.6" in size (305mm x 244mm). ITX is a series of form factors that began with the mini-ITX, but there is no specific size called ITX. The mITX (Mini-ITX) form factor is 6.7" x 6.7" in size (17 cm x 17cm). The mITX is commonly used in smaller computer systems with a small form factor (SFF) case. These motherboards are usually used in computers designed for passive cooling and a low power consumption architecture, such as a home theater PC system.
4. An intrusion detection system is a device or software application that monitors a network or system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator or collected centrally using a security information and event management system. Unlike an IPS, which can stop malicious activity or policy violations, an IDS can only log these issues and not stop them. An intrusion prevention system (IPS) conducts the same functions as an IDS but can also block or take actions against malicious events. An authentication, authorization, and accounting (AAA) server is a server used to identify (authenticate), approve (authorize), and keep track of (account for) users and their actions. AAA servers can also be classified based on the protocol they use, such as a RADIUS server or TACACS+ server. A proxy server is a server that acts as an intermediary between a client requesting a resource and the server that provides that resource. A proxy server can be used to filter content and websites from reaching a user.

5. A corona wire is a charged wire in a laser printer that draws the toner off the drum onto the paper. It must be cleaned when the toner cartridge is replaced. A dirty corona wire can cause a portion of the drum not to be charged properly and lead to a white streak appearing on the printed image. Some laser printers combine the toner and drum into a single replaceable item. The drum on a laser printer should be changed after printing 10,000 to 15,000 pages to prevent issues during printing
6. Slow data speeds can be caused by too much interference or a weak signal. Try changing the channel on Wi-Fi routers to less-used channels or boost the signal being transmitted, and the performance should increase. Alternatively, if the cellular signal is too low, you can install a signal booster or microcell in the home or office. Enabling MAC filtering would block devices attempting to connect to the Wi-Fi. Turning off the Wi-Fi and using their cellular data plan might be a valid workaround, but it does not solve the issue of the Wi-Fi not functioning properly at home. Upgrading the smartphone would not increase the speed of their home Wi-Fi, as their current smartphone already operates at faster speeds on other Wi-Fi networks.
7. IP addresses are either public, private, localhost, or APIPA addresses. Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems that enables a computer to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. When a host uses an APIPA address, it can communicate with other hosts on the same network using APIPA. Still, it cannot reach other networks or communicate with hosts who have managed to obtain a valid DHCP lease. Any address from 169.254.1.0 to 169.254.254.255 is considered an APIPA address. An APIPA address is also referred to as a link-local address. A private IP address is in the range of 10.x.x.x, 172.16-31.x.x, or 192.168.x.x. A localhost IP is 127.0.0.1. All others are considered public IP addresses.
8. Network address translation (NAT) is a network service provided by a router or proxy server to map private local addresses to one or more publicly accessible IP addresses. NAT can use static mappings but is commonly implemented as network port address translation (PAT) or NAT overloading, where a few public IP addresses are mapped to multiple LAN hosts using port allocations. The dynamic host control protocol (DHCP) is a protocol used to allocate IP addresses to a host when it joins a network. Universal plug-and-play (UPnP) is a protocol framework allowing network devices to autoconfigure services, such as allowing a game console to request appropriate settings from a firewall. A perimeter network (formerly called a Demilitarized Zone or DMZ) is a portion of a private network connected to the Internet and protected against intrusion. Certain services may need to be made publicly accessible from the Internet (such as a web, email, or Minecraft server), and they should be installed in the perimeter network instead of in your intranet. If communication is required between hosts on either side of a perimeter network, then a host within the perimeter network will act as a proxy to take the request.

PRL (Preferred Roaming List) A cell phone's priority-ordered list of other carrier networks and frequencies it should search for when it cannot find its home network.

PRI (Product Release Instruction) CDMA updates that modify a host of complex device settings.

Reset Jumper Lesson 1 or 2

Syslog (SNMP) used to store monitored logs

What chapter is ipconfig located?

DVI-D is for *Digital Only*
DVI-A is for Analog only. Very rare to find.
DVI-I is "Integrated" (Digital and Analog) which is ideal when dealing with VGA adapters.

Collate in Printers

For mobile phones, flickering is often caused by a failing backlight that needs to be replaced by a certified technician.

DB-9 connectors are designed to work with the EIA/TIA 232 serial interface standard, which determined the function of all nine pins as a standard so that multiple companies could design them into their products. DB-9 connectors were commonly used for serial peripheral devices like keyboards, mice, joysticks, and data connectivity. Today, the DB9 has mostly been replaced by more modern interfaces such as USB, PS/2, Firewire, etc. However, there are still many legacy devices that use the DB-9 interface for serial communication.

Network address translation (NAT) is a network service provided by a router or proxy server to map private local addresses to one or more publicly accessible IP addresses. NAT can use static mappings but is commonly implemented as network port address translation (PAT) or NAT overloading, where a few public IP addresses are mapped to multiple LAN hosts using port allocations. The dynamic host control protocol (DHCP) is a protocol used to allocate IP addresses to a host when it joins a network. Universal plug-and-play (UPnP) is a protocol framework allowing network devices to autoconfigure services, such as allowing a game console to request appropriate settings from a firewall. A perimeter network (formerly called a Demilitarized Zone or DMZ) is a portion of a private network connected to the Internet and protected against intrusion. Certain services may need to be made publicly accessible from the Internet (such as a web, email, or Minecraft server), and they should be installed in the perimeter network instead of in your intranet. If communication is required between hosts on either side of a perimeter network, then a host within the perimeter network will act as a proxy to take the request.

A riser card is a right-angle expansion card used to extend a slot for a card in a computer to make room to plug it in. They are most commonly used in low-profile, 1U and 2U rackmount chassis or embedded systems. Riser cards plug into their respective bus (they are available for PCI, PCI-X, AGP, AGP Pro, PCI Express, ISA, or other buses) and rotate the peripheral cards plugged into the riser card so that they are parallel with the motherboard. Riser cards are available in 1-slot passive risers up to 3-slot passive riser cards for 2U rackmounts. An AGP, SCSI, or PCIe x16 expansion card is a fixed size and shape that cannot be reduced to fit in a 1U server.

S.M.A.R.T. is an acronym for Self-Monitoring and Repair Tool. It is a feature in all modern magnetic hard drives (non-SSD drives) that monitors the hard drive to ensure it performs properly. S.M.A.R.T. can detect when the failure of a drive is imminent and can alert the user so that they can back up the drive before a complete failure occurs. If your hard drive produces a S.M.A.R.T. failure, you should immediately back up the drive. Once a backup has been completed, you can instead focus on repairing the drive using chkdsk.

Numlock: Most keyboards have a numeric side (numbers only) and an alphanumeric side (numbers, letters, and symbols). However, to minimize space usage, companies create some keyboards with the alphanumeric side only. This is quite common in laptops that insist on minimizing space for the sake of portability, as seen on mini-laptops and notebooks. Usually, the alphanumeric side is split into function keys (F1 to F12), followed by numeric keys (0-9), and then alphabetic keys (A-Z). To fix this, the fastest way to do this is to turn off NumLock using your laptop keyboard. If you hit the NumLock key, it will turn off. A light beside the key or on the laptop's top will go off to confirm that the NumLock is disabled.

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. If you are dealing with connecting two networks over a long distance (over a few hundred meters), you should use a fiber optic cable. Shielded and plenum copper cables can only cover a distance of approximately 100 meters in length. Coaxial cables can cover a maximum distance of 200 to 500 meters in length.

The transfer belt is the component in a color laser printer that combines the 4 colors before printing it to the paper in one pass. The transfer roller is the component in a laser printer that applies an electric charge to the paper to attract toner from the photoconductor during the imaging process. The pickup roller is the component in a laser printer that turns above a stack of paper to feed a sheet into the feed roller. The duplexing assembly is a component that enables a printer or scanner to use both sides of a page automatically.

3G cellular technology is made up of two different technologies: HSPA+ and EV-DO. HSPA+ (Evolved High-Speed Packet Access) is a 3G standard used for GSM cellular networks and can support up to a theoretical download speed of 168 Mbps and a theoretical upload speed of 34 Mbps. In the real world, though, HSPA+ normally reaches speeds around 20 Mbps. EV-DO (Evolution-Data Optimized) is a 3G standard used for CDMA cellular networks and can support up to 3.1 Mbps downloads. 4G cellular technology is made up of LTE and LTA-A. Long Term Evolution (LTE) is a packet data communications specification providing an upgrade path for both GSM and CDMA2000 cellular networks. LTE has a theoretical speed of 150 Mbps and a real-world speed of around 20 Mbps. LTE Advanced (LTE-A) has a theoretical speed of 300 Mbps and a real-world speed of around 40 Mbps. 5G cellular technology is made up of three different types: low-band, mid-band, and high-band mmWave technology. Low-band 5G reaches an average speed of 55 Mbps with a theoretical speed of 150 Mbps. Mid-band 5G reaches an average speed of 150 Mbps with a theoretical speed of 1.5 Gbps. High-band 5G reaches an average speed of 3 Gbps with a theoretical speed of up to 70 Gbps.

The best description of the purpose of containers in virtualization is that they provide a lightweight, consistent runtime environment because containers package applications with their dependencies, ensuring consistency across different environments while using fewer resources than traditional virtual machines. Containers share the host OS kernel rather than virtualizing hardware; they do not replace the need for a physical machine. The use of operating systems is still required since containers still rely on an OS, although they do not require a full guest OS. While containers can run directly on the host OS, hypervisors are still needed for full virtual machine environments.

Jitter is a network condition that occurs when a time delay in the sending of data packets over a network connection occurs. Jitter is a big problem for any real-time applications you may be supporting on your networks, like video conferences, voice-over IP, and virtual desktop infrastructure clients. Latency is the measure of time that it takes for data to reach its destination across a network. Usually, we measure network latency as the round-trip time from a workstation to the distant end and back. Throughput is an actual measure of how much data is successfully transferred from the source to a destination. Bandwidth is the maximum rate of data transfer across a given network. Now, bandwidth is more of a theoretical concept that measures how much data could be transferred from a source to a destination under ideal conditions. Therefore, we often measure throughput, instead of bandwidth, to monitor our network performance.

A proxy server acts as an intermediary between clients and the internet, providing security, content filtering, and improved performance by caching web content. Storing and retrieving email messages is performed by a mail server. Hosting websites for public access is provided by web servers. Synchronizing network time across devices is provided by a NTP (Network Time Protocol) server.

To troubleshoot the failed boot, you must reboot the computer and enter into recovery mode. In Windows 10, you will need to boot from the installation disc, select “Repair your computer,” and then enter the command-line interface (CLI). From the CLI, enter the command "bootrec /fixmbr" to repair the master boot record. Once completed, reboot the computer and allow it to load into Windows.

PS/2 Splitter, PS2 and SPDIF (Sony-Philips Digital Interface Format)

Tx port and Rx port and MTRJ (Mechanical Transfer Registered Jack)

- Transceiver and Receiver ports for Fiber cables, as they generally don’t do bi-directional signals on the same cable. These are plugged into a separate patch panel.

Zigbee & Z-Wave

- Used to control IoT devices. Zigbee is a standard connection between devices (open source). It’s faster and supports more devices at a shorter range, because it works on the 2.4GHz band. Z-Wave is proprietary and requires certification to use them.

Chapters 1 & 2

Group Discord Link: https://discord.gg/7n2x3Wa7

Members:
Toba
Dave (Team Leader)
Nyla
Diane

4.6.5 Troubleshooting Checklist'

Troubleshooting for a black screen: Black screen before logging into computer:

- Check for physical connections. Are video cables fully connected? Reconnect them and plug them back in. Try a different cable or try a different monitor.
- Is the power source on? Do you hear the fans and startup up but no display?
- Holding the power button to trigger a force reset.
- Try unplugging any unnecessary accessories like the keyboard and mouse
- If powering back on, check the UEFI/BIOS settings by holding F2 or DEL during startup

Black screen after logging in:

- Disabling startup applications by going into the task manager in the windows search bar.
- If there is a lack of loading applications and icons, go to task manager's explorer.exe and run a new task. (explorer.exe is responsible for loading your desktop and icons.)
- If connected to multiple monitors and screens, duplicate them.

Troubleshooting for a display that flickers or is distorted. What to consider: drivers, cables, and monitor settings.
Why is my computer flickering? Is it an application? Check the task manager. If everything except the task manager continues to flicker, it may be an unsupported application.
Flickering laptop screen:

- Boot in safe mode (turn on computer and continuously press F11)
- Loose cables
- Check display drivers. Are they fully updated?
- Is windows fully updated? Go to settings and updates and check if there are any available updates.

For desktops and monitors:

- Adjusting the refresh rate. Go to the desktop and right click your display. Go to display settings and advanced display settings. Display adapter settings and select the monitor tab to adjust the refresh rate.
- Check for loose connections
- Run windows built in troubleshooting. Go settings> update and security > troubleshoot display quality and select troubleshooter

Troubleshooting for a monitor that won't power on. Include steps to check power sources, hardware components, and external factors.

- Are there any lights? Any fans? If not then it is usually a power issue.
- Is the computer stuck at the loading or logo screen? No light up of the keyboard or caps key? Likely a problem with the startup.
- Fans spinning? Lights on? Likely a problem with the monitor.
- When did this occur? After you shut it down? Did you come back to a computer with no power?
- Hold the power button to see if the system resets.
- Ensure the cable is fully connected to the power source and laptop. Try different outlets and cables. Is the LED light on?

My troubleshooting process consists of identifying the problem. Asking clarifying questions to isolate what the issue is. For instance, if someone in the office was dealing with slow internet, I'd first ask them when they noticed the change in speed. I'd ask them if they notice anyone else in the office with slow internet. Establishing a theory. If the slow internet is affecting everyone in the office, the problem may be with the network.
Testing my theory. If it seems like a network issue, I might check the router or switch for errors, restart the device, or run diagnostics like a ping or traceroute. Establishing a plan of action. If it's isolated to one user, I'd verify their connection settings, test with a different device, or try using a wired connection instead of Wi-Fi. My process would consist of identifying the problem, establishing a theory of probable cause, testing my theory, establishing a plan of action, verifying my answer, and finally documenting my process for others and myself to refer to.

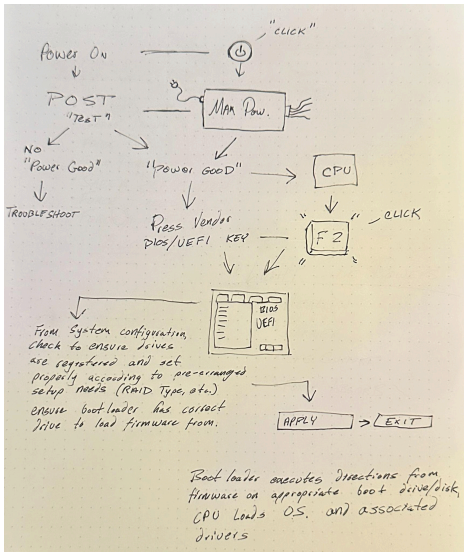
Notes from 132.4.6 - BIOS and UEFI

Additional Resources:

- 4.6.1: BIOS and UEFI
- 4.6.2: Troubleshooting Example: Video Issues
- 4.6.3: Exercise: Boot Process Walkthrough

During the initial boot process, upon completion of a successful POST, the CPU will be given power to initiate the installed firmware. It is at this moment that a user can prompt the CPU to initiate in BIOS/UEFI, which is a powerful directory of commands and processes that can be adjusted by the user for a number of reasons.

Initiating the system in BIOS/UEFI is the first step a user must take when they have built or changed the HDDs and/or SDDs, but also serves to tell the OS where to look for boot instructions. These instructions are vital to efficient and proper operation of system drives, and are important to understand in order to troubleshoot any problems in the initial boot process of an OS or troubleshooting an unknown device.



- 4.6.4: Exercise: Hard Drive Health Monitoring - Post Meeting
- 4.6.5: Exercise: Create a Troubleshooting Checklist - Post Meeting
- 4.6.6: Exercise: Power Supply Wattage Calculation Capstone - Post meeting

4.7 - Module QUIZ
4.8 - Checkpoint Review

Day 2: 7/29/2025

Homework: Read

All classes are recorded. Access to recordings are under “Cisco Webex”

1 Byte (Storage) = 8 bits (Speed)
1,000b = 1 kb
1,000kb = 1 Mb
1,000Mb = 1 Gb

Personal Notes from Reading: CertMaster Module 2.0: Installing Motherboards and Connectors

Front of PC: Optical Disc Drive | Unused Optical Disc Drive Bays | Front I/O Panel (Audio and USB) | Power Button | Temperature Display(rare) | Fan Vents for Airflow

Rear Panel of PC: Power Supply with Fan | Chassis Fan Airflow Cutout | Motherboard I/O Panel | Expansion Card Slots

Exposed card slots not covered with an adapter card or a blanking plate can cause the following:

- Dust entry, leading to overheating.
- Increased exposure to Electrostatic Discharge (ESD). (I/O Shield’s pins provide a safe path for ESD to ground via external metal parts/metal case)

- Increase exposure to Electromagnetic Interference (EMI). Typically the PC Case absorbs EMI, but gaps in the case reduce this protection.

Input/Output Ports:

- HDMI
- DVI
- SATA
- USB
- RJ-45 Network
- Audio Ports

EXTRA CONTENT: “Bus Interface” is a subsystem that allows communication between different components or devices within a system. It acts as a shared communication channel, enabling data transfer and control signals to be exchanged efficiently.

- Data Bus: Used for transferring data between components
- Address Bus: Used to specify the location in memory or the device that the data should be sent to or retrieved from.
- Control Bus: Carries control signals that manage the operations of the system, such as read/write commands, clock signals, and reset signals.
- System Bus: A combination of data, address, and control buses; provides a unified interface for all the components in a system to communicate with each other.

The Universal Serial Bus (USB) is the gold standard. Categorized into classes such as: Human interface (keyboards and mice), mass storage (disk drives), printers, and audio devices.A host controller manages a USB. A single controller can theoretically support up to 127 devices.

USB Connector types:

- Type A: Flat rectangular connector, inserted with the USB symbol facing up.
- Type B: Square connector with a beveled top for large devices like printers.
- Type B Mini: Smaller connector for smaller devices like early digital cameras. Rarely used now.
- Type B Micro: Flatter connector for smaller devices like smartphones and tablets.

USB 3 Connectors:

- NEW: Type A, Type B, Type B Micro.
- Usually a blue connector tab or housing.
- Type B and Type B Micro are INCOMPATIBLE.

USB 3.1 → USB-C connector

Cable Length to Speed:

- <3m/9’ for LowSpeed and SuperSpeeddevices
- <5m/15’ for FullSpeed and HighSpeed devices

Power: Basic USB ports can provide up to 4.5 watts. Power Deliver (PD) ports can supply up to 100 watts with suitable connectors and cables.

The evolution of the USB standard:

1. USB 1.0 (1996): Introduced with speeds of 1.5 Mbps (Low Speed) and 12 Mbps (Full Speed), using Type-A and Type-B connectors.
2. USB 1.1 (1998): Enhanced USB 1.0 with the same speeds but improved compatibility and reliability.
3. USB 2.0 (2000): Increased speed to 480 Mbps (High Speed) and introduced Mini-A/B and Micro-A/B connectors.
4. USB 3.0 (2008): Introduced SuperSpeed at 5 Gbps and new connectors like Micro-B, later rebranded as USB 3.1 Gen 1.
5. USB 3.1 (2013): Brought SuperSpeed+ at 10 Gbps and the versatile Type-C connector, rebranded as USB 3.1 Gen 2.
6. USB 3.2 (2017): Offered Gen 1 (5 Gbps), Gen 2 (10 Gbps), and Gen 2x2 (20 Gbps) speeds, using Type-A, Type-B, and Type-C connectors.
7. USB4 (2019): Achieved speeds up to 40 Gbps, unified with Thunderbolt 3, exclusively using the

	Speed Ratings		Connector Types
	Gen 1	Gen 2	
USB4	40Gbps		C
USB 2x2	20GBps		A, B, C
USB 3.2	5Gbps	10Gbps	A, B, C
USB 3.1	Rebranded as:	10Gbps	Introduced C, A, B
USB 3.0	5Gpbs		Micro-B, A, B
USB 2.0	480Mbps		Mini/Micro A&B
USB 1.1	1.5Mpbs	12Mbps	A, B
USB 1.0	1.5Mpbs	12Mbps	A, B

Type-C connector, and supported advanced features like multiple data and display protocols.

Display Technologies:
Liquid Crystal Displays:

- In-Plane Switching (IPS): Liquid crystals are aligned parallel to the screen for the light. Superior color accuracy and wide viewing angles, slower in response times compared to TN panels.
- Twisted Nematic (TN): Liquid crystals twist 90 degrees between the electrodes.Faster response times and higher refresh rates, poor color reproduction and limited viewing angles.
- Vertical Alignment (VA): Liquid Crystals are aligned vertically to the glass substrates and tilt when voltage is applied. Better color accuracy and viewing angles than TN, Slower response times than TN but better than IPS in some cases. Some color shifting when viewed from extreme angles.
- Organ Light-Emitting Diode (OLED): Each pixel emits light through organic compounds when an electric current is applied. Excellent color accuracy, contrast ratios, energy efficiency, and true blacks due to self-emissive pixels; potential for burn-in.
- Mini-LED: Thousands of tiny LEDs for backlighting, allowing for more precise control of brightness and contrast. Improved brightness, better contrast and black levels, enhanced color accuracy, and reduced halo effect, usually thin/light-weight designs; expensive, high power consumption than OLEDs, cannot achieve true black.

Display Components:

1. Touch Screens and Digitizers
2. Inverter: Crucial in older LCDs for converting DC power to AC for the backlight, not needed for modern displays.
3. Pixel Density: Higher density → Sharper images
4. Refresh Rates: Higher Rates → Smoother motions
5. Screen Resolutions:
    - SD (640x640)
    - HD (1920x1080)
    - Quad HD (2560x1440)
    - 4K (3840x2160)
    - 5K (5120x2880)
    - 8K (7680x4320)
6. Color Gamut: Refers to the range of colors a display can produce based on the RGB ccolor model.
    a. Wider Gamut → More Vibrant and accurate color.
    b. Common gamuts: sRGB, Adobe RGB, and DCI-P3 (The best)
    c. 24-bit color → 16.7 million colors
    d. 32-bit color → added Alpha channel for transparency

Video Cable Bandwidth:

- Determined by Resolution and Refresh Rate (Hertz[Hz] or frames per second[fps])

High-Definition Multimedia Interface (HDMI)

- Transmits HD Video and Audio through single cable.
- Available in different versions; Higher resolutions, increased refresh rates, and HDR.

DisplayPort

- Superior performance for high-resolution and Multi-display configurations.
- Preferred for Professional/Gaming setups
- Supports higher resolutions and refresh rates than HDMI
- Multi-Stream Transport (MST) allows multiple displays to connect through a single port.

- Transmits Audio
- Supports adaptive sync tech like AMD FreeSync and NVIDIA G-Sync
- Reduces screen tearing in gaming applications

Thunderbolt and Lightning

- Typically used on Apple products
- Thunderbolt 1 and 2 are compatible with DisplayPort, requiring an adaptor to connect physically.
- Thunderbolt 3 utilizes USB-C interface, supports up to 40 Gbps for short, high-quality cables.
- Thunderbolt 4 Supports up to 40 Gbps.
- Thunderbolt 5 is just better.

Lightning Connector: 2012 Apple cable primarily used for iPhone etc. Requires USB A or USB C adapter to connect to PC and others. No longer being employed on new models.

Serial Advanced Technology Attachment Interface (SATA)

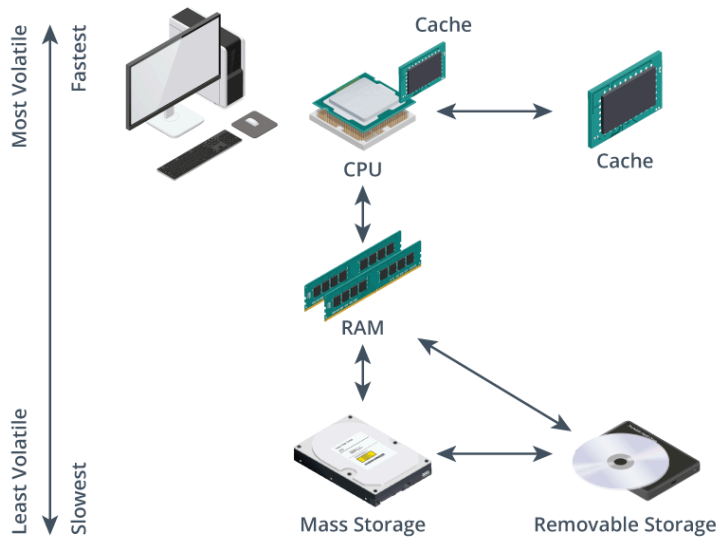
- Standard for connecting internal storage drives in desktop PCs
- 7-pin connector does not supply power
- 15-pin connector supplies power
- Original → 150MBps, Revision 2 → 300 MBps, Revision 3 → 600 MBps
- Revisions 3.1-3.5: SATA Universal Storage Module, SATA Express Specification
- DO NOT PLUG OR UNPLUG BEFORE POWERING OFF

Molex Power Connectors

- Used to connect legacy components to power
- Features wire insulation color codes for different voltage levels:
    - Red → 5 volt DC (VDC)
    - Yellow → 12 volt DC (VDC)
    - Black → Ground

eSATA

- External SATA for peripherals that connect outside the PC
- Not compatible with SATA
- eSATAp: Nonstandard powered port, works with USB and SATA
- DO NOT PLUG OR UNPLUG BEFORE POWERING OFF



Electrical Safety: Disconnect all power before opening devices. Hold power button to drain any remaining charge from internal components.

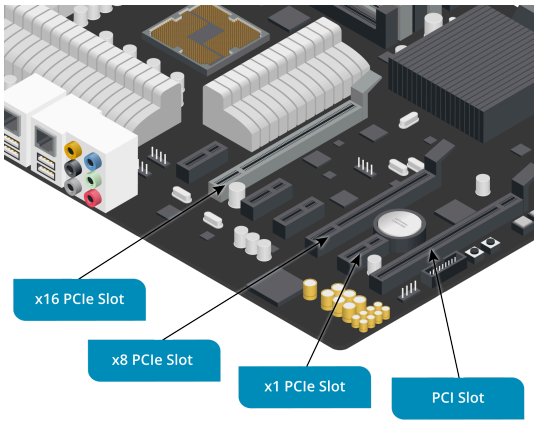
Central Processing Unit (CPU): Main processing function

Random Access Memory (RAM): nonpersistent memory storage for active processes

Dual Inline Memory Modules (DIMMs): RAM cards, inserted into motherboard slots

Graphics Processing Unit (GPU): Processes images

M.2 Interface: Type of Solid-State Drive (SSD) Comes in 42mm, 60mm, 80mm, 110mm. Supplies power over the bus.



Peripheral Component Interconnect Express Interface (PCI Express)

Each point-to-point connection is called a link, which can use one or more lanes. The raw transfer rate of each lane depends on the PCIe version and is measured in giga transfers per second (GT/s). Throughput in GB/s is the effective rate after accounting for encoding losses.

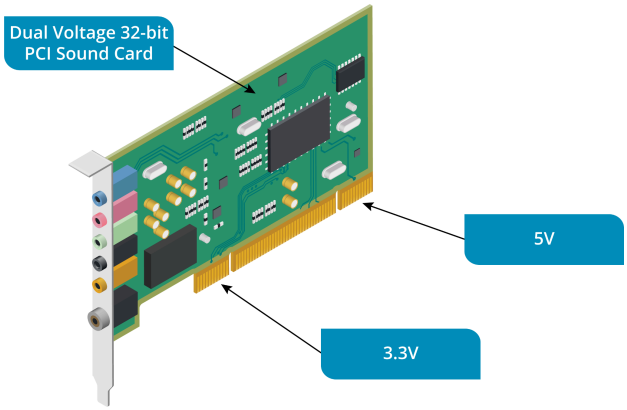
Version	GT/s	GB/s for x1	GB/s for x16
2	5	0.5	8
3	8	0.985	15.754
4	16	1.969	31.508
5	32	3.938	63.015
6	64	7.56	128

Adapter slots with more lanes are physically longer. Each PCIe adapter card supports a specific number of lanes, typically x1, x4, x8, or x16. Ideally, the card should be plugged into a port with the same number of lanes. However, if slots are limited, a card can fit into any port with an equal or greater number of lanes, known as up-plugging (e.g., an x8 card in an x8 or x16 slot). The card should work at x8 but may sometimes operate at x1. Down-plugging, fitting a longer card into a shorter slot, is possible if the card is not obstructed.

Note:
A slot may support fewer lanes than its physical size suggests, indicated by a label on the motherboard (e.g., an x16 slot supporting only x8 operation labeled as x16/x8 or x16 @ x8).

All PCIe versions are backward-compatible, meaning you can connect a PCIe version 2 adapter to a version 4 motherboard or a version 3 adapter to a version 2 motherboard, with the bus link operating at the speed of the lowest version component.

PCIe can supply up to 75W to a graphics card via a dedicated graphics adapter slot and up to 25W through other slots. An additional 75W can be supplied via a PCIe power connector.



Peripheral Component Interconnect Interface (PCI)

- Legacy bus
- Cannot fit into PCIe Slots

- Typically 32-bit, operating at 33.3 MHz, and transfers up to 133 MBps
- Different “keying” used for 5V, 3.3V and Dual-Voltage cards

Motherboard Form Factor

Advanced Technology eXtended Form Factor (ATX)

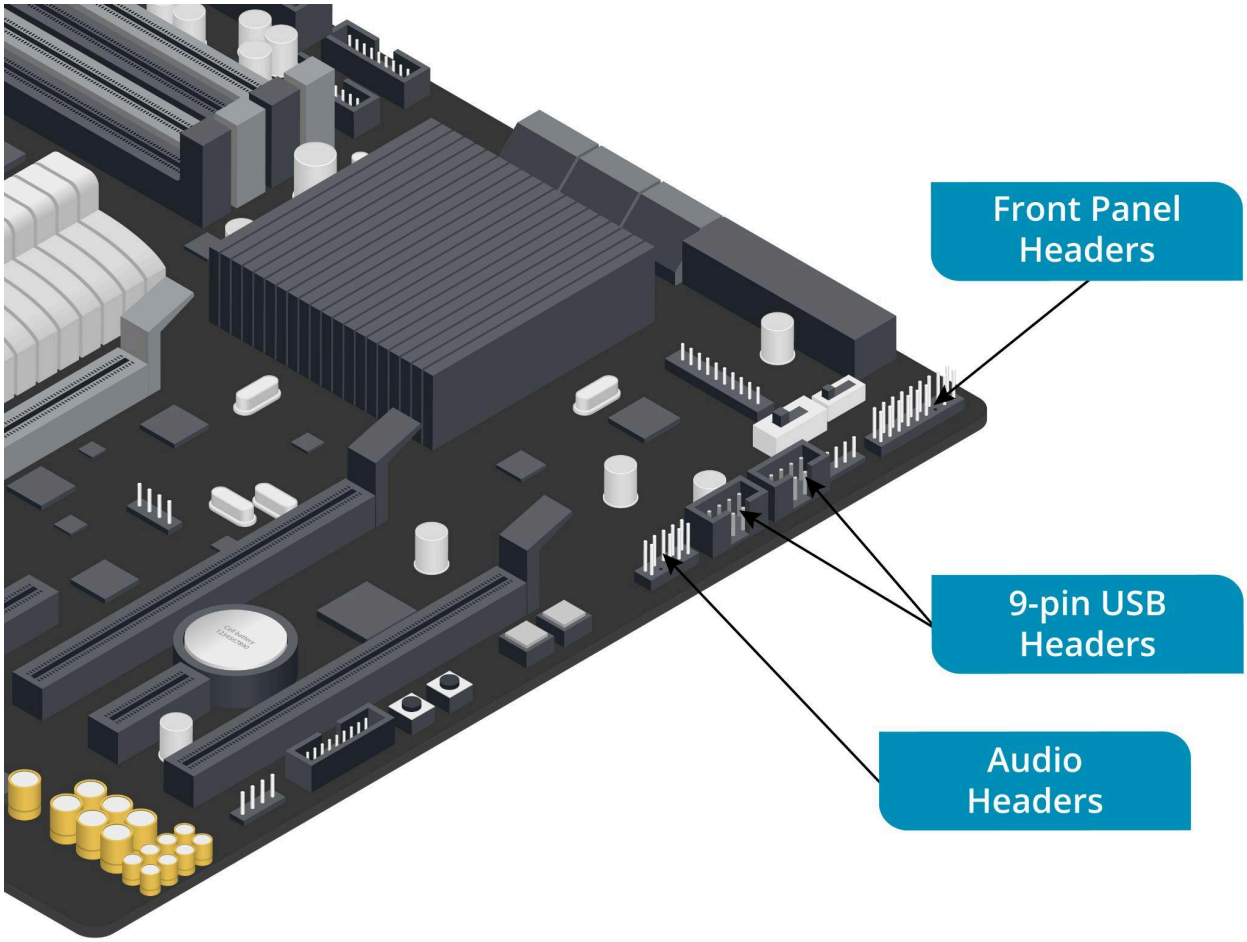
- Standard form factor for most desktop PC motherboards and cases
- 12” x 9.6” (244 x 244 mm) square board, MAX 4 expansion slots

Information Technology eXtended Form Factor

- Small Form Factor (SFF) PCs are popular for home use and mini servers
- Mini=ITX boards measure 6.7” x 6.7” (170x170mm)
- Can be mounted in ATX or small cases
- Smaller nano-, pico- and mobile-ITX form factors used for embedded systems and portables

Installing a motherboard

1. Review the Documentation
2. Install the I/O Shield
3. Insert Standoffs
4. Pre-Install the CPU and Memory
5. Align and Secure the Motherboard
6. Final Assembly
7. Cable Management



Headers: Connections on the motherboard that components on the panels connect to.

- Power button (soft power)
- Drive (HDD) activity lights
- Audio ports
- USB ports

**When disassembling the system, create a diagram or take photos to document th exposition and orientation of all header connectors, or refer to the motherboard documentation or the labels printed on the wires and headers.

– - End Day 2 - –

Day 1 - July 28, 2025

"The Troubleshooting Methodology"

- Identify the problem -> Establish and Test a theory -> Question the obvious -> Establish a New Theory or Escalate -> Implement a Plan of Action -> Verify and Document.

Simulation Scenario: Monitor Not Powering On
Scenario Title: "Black Screen at Onboarding"
Scenario Setup (Workplace Framing):
You're an IT Support Technician on the internal help desk team at "TechNova Solutions." It's Monday morning, and the HR team has just onboarded three new hires. One of the new employees, Jamie Chen, submitted a ticket because their monitor isn't turning on.
Ticket Description:
Submitted via helpdesk portal at 9:12 AM
"Hi IT,
My monitor isn't turning on. I've tried pressing the power button but nothing's happening. I need to get into onboarding materials ASAP. Can someone help?
Thanks,
Jamie C."
Your Task:
As the assigned IT Support Technician, your job is to diagnose and resolve the issue. You'll:
Review the ticket and plan next steps.
Communicate professionally with the user.
Investigate and troubleshoot the hardware issue.
Document your process and resolution.

- Check Power Cable, is power cord fully plugged in to the monitor? Is it loose towards the outlet?
- Try unplugging and replugging it in. If still no light or response, try a different plug
- Verify the new plug works, is the monitor turning on? If it is try turning iron and off again to verify that it works

Workplace Behaviors Practiced:

Communication & Documentation (writing updates, asking clarifying questions)
Task Ownership (responding to and resolving a user issue)
Professionalism (tone, timeliness, technical accuracy)
Problem Solving & Technical Reasoning (identifying root cause through structured steps)

Instructor Guidance: How to Plug In

Use this during a lab or as a scenario-based breakout.

Encourage learners to follow a basic ticketing workflow: intake → clarify → troubleshoot → resolve → document.

Observe how they collaborate, escalate, or request missing information.

Chapter 3

Notes from Chapter 3: Installing System Devices"

*NOTE: Much watch "Jason Dion Videos" in resources section at bottom of Announcement Rubric

3.1 - Power Supplies and Cooling

3.1.1 - Power Supply Units

The PSU receives ACV and converts to DCV, using regulators to ensure consistent output. It is crucial to correctly match the PSU wattage to the system's power requirements. Distribution of power is over output rails, wires providing current at a specific voltage. Voltage regulators adjust the supplied voltage to match the component's requirements.

North American outlets: 120 VAC (low-line)
UK outlets: 230 VAC (high-line)

- System Instability: Insufficient power can cause random shutdowns, reboots, or crashes, as the PSU struggles to supply adequate power to all components.
- Component Damage: Consistently running a PSU at or beyond its capacity can lead to overheating, potentially damaging the PSU and/or components

Output Rail (DCV)	Maximum Load (A)	Maximum Output (W)
+3.3	20	130
+5	20	130
+12	33	396
-12	0.8	9.6
+5 (Standby)	2.5	12.5

Energy Efficiency

PSU efficiency affects the performance and energy consumption, like a 300w PSU operating at 75% efficiency draws 400w from the outlet, with the excess 100w lost as heat. PSUs are often rated according to the 80 PLUS certification program.

- 80 PLUS Bronze: At least 82% efficiency at 20% load, 85% at 50% load, and 82% at 100% load
- 80 PLUS Silver: At least 85% at 20% load, 88% at 50% load, 85% at 100% load
- 80 PLUS Gold: At least 87% at 20% load, 90% at 50% load, and 87% at 100% load
- 80 PLUS Platinum: 90% at 20% load, 92% at 50% load, 94% at 50% load
- 80 PLUS Titanium: 90% at 10% load, 92% at 20% load, 94% at 50% load, 90% at 100% load
- Energy Star 80 PLUS at least 80% efficient at 20-100% load.

The mother board's port is called the P1 connector, or the 25-pin ATX power connector. It also includes Molex and SATA power, as well as 4/6/8/16-pin connectors for CPU and PCIe. The ATX PSU

2 types of heat sinks:

- Passive: Memory modules use passive heat sinks, also called heat spreaders, no fans.
- Active: Heat Sink with fins and thermal paste/pad to eliminate air gaps for efficiency.

Liquid Cooling: Used in high-end gaming PCs, high performance workstations, and those used in high ambient temperatures. Cools by pumping water around the chassis.

- Water loop/tubing and pump
- Water blocks and brackets: Attached to each device to remove heat by convection
- Radiators and fans: Positioned at air vents

3.1.3 - Wattage Rating

a. Power: The rate energy is generated/used in watts (w)
    i. Calculated as voltage multiplied by current (v x I)
b. Standard Desktop PSU ~400-500 W
c. PSU Efficiency is critical in system performance and energy consumption

d. 80 PLUS certification program signifies efficiency levels - 87%

3.1.4 - Power Supply Connectors

e. Each PSU has multiple power connectors
    i. Generally supplies 3.3 VDC, 5 VDC, and 12 VDC
f. PSU includes Molex and SATA power connectors, 4/6/8/16-pin for CPU, and PCIe

3.1.5 - 20-pin to 240pin Motherboard Adapter

g. Original ATX P1 connector is 20-pin
    i. Black wires for ground
    ii. Yellow for _12v
    iii. Red for +5v
    iv. Orange for _3.3V
h. Most systems use 24-pin P1, some with adaptor cable

3.1.6 - Modular Power Supplies

i. Has detachable power connector cables
j. Reduces clutter in chassis
k. Improves airflow and cooling

3.1.7 - Redundant Power Supplies

l. Crucial in continuous operations, such as data centers
m. Systems can have 2x PSUs to minimize downtime and prevent data loss
n. Less common in desktop PCs

3.1.10 - Fan Cooling Systems

3.1.11 - Heat Sinks and Thermal Paste

o. Heat Sink: Copper or Aluminum block with fins
p. Thermal paste/Pad: Used to attach the heat sink to CPU, effective heat transfer

3.1.12 - Fans

3.1.13 - Liquid Cooling Systems

q. Essential for gaming PCs and high-performance workstations
r. Pumps water around chassis
s. Quieter than fans
t. Components: Water loop/tubing, pump, water blocks and brackets, radiators and fans

3.2 - Storage Devices

Common Sizes: 5.25, 3.5, 2.5 inches. 5.25 common for DVD drives or smart card readers.

3.2.2 - Mass Storage Devices

a. Magnetic, optical, or solid-state technology
b. Non-Volatile storage (fixed disks) retain data when powered off

3.2.3 - Solid-State Drives

c. Uses Flash memory and offers better read performance than HDDs
d. Less prone to mechanical failure
e. Sometimes underperforms compared to HDDs
f. SATA: Can be packaged in a 2.5” caddy. Comes in mSATA form factor, can plug into combined data/power port on the motherboard. Backward compatible interface, but bottlenecked based on interface thresholds.
g. PCI Express: Utilizes Non-Volatile Memory Host Controller Interface Specification (NVMHCI) or non-volatile memory express (NVMe) interface. NVMe SSds can be installed in a PCIe slot as an expansion card or an M.2 slot.
h. M.2 SSDs are smaller, more suitable for laptops, but also for PCs. M.2 slots provide power over the bus.

i. Serial Attached SCSI Small Computer System Interface (SAS): High-performance, often used in enterprise environments. Faster data transfer rates and better reliability compared to SATA.

3.2.4 - Hard Disk Drives

j. Stores data on metal or glass platters coated with a magnetic substance
k. Platters have read/write head on both sides and spin at high speeds
l. Performance determined by disk's spindle-speed. High-performance drives spin at 10k-15k RPM (180MBps), average drives from 5,400-7,200 RPM (110MBps).
m. Higher latency due to read/write times. Average between 6ms - 3ms for moderate to high performance drives.

3.2.5 - Redundant Array of Independent Disks (RAID)

n. Use of RAID mitigates risk of data loss
o. Distributes data across multiple disks
p. Levels represent drive configurations
    i. With specific types of fault tolerance (numbered 0 to 6)
    ii. With nested solutions such as RAID 10 (RAID 1+ RAID 0)
    iii. Selecting an appropriate RAID level is crucial
        1. Factors: required fault tolerance, read/write performance, capacity, and cost

3.2.6 - RAID 0 and RAID 1

q. RAID 0 (striping without parity):
    i. Minimum 2 discs
    ii. Divides data into blocks and distributes across all disks. Makes data faster to retrieve. No backup of data.
r. RAID 1 (mirroring):
    i. Minimum 2 discs
    ii. Mirrored drive config using two disks; each write operation is duplicated on the second disk. Ideal for data backup.

3.2.7 - RAID 5 and RAID 10

s. RAID 5 (striping with distributed parity)
    i. 3 Discs Minimum
    ii. Distributed parity: error correction info is spread across all disks
    iii. If one disk fails, data is reconstructed from info on other disks
    iv. Hot-Swappable, safe with SATA
t. RAID 10 (stripe of mirrors)
    i. Combines RAID 0 (striped volume) and RAID 1 (mirrored arrays)
    ii. One disk in each mirror can fail without losing data

3.2.8 - Raid 6 (Striping with Double Parity)

u. 4 discs minimum
v. Spread two sets of parity info across all disks
w. Can tolerate simultaneous failure of two disks
x. Usable capacity is total capacity minus capacity of two disks for parity
y. More expensive than RAID 5

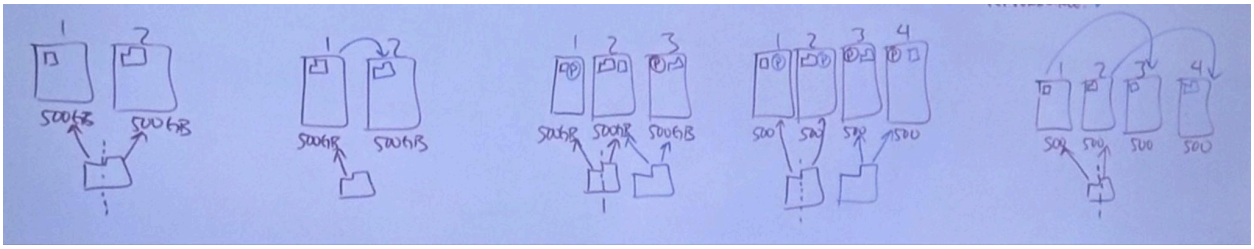
– – Continued – –

RAID Breakdown

Striping: Splitting the data between drives, increases performance
Parity: Instructions for split data on RAID, usually split onto all drives

	RAID 0	RAID 1	RAID 1+0	RAID 5	RAID 6	RAID 10 (Same as 1+0)
Min Discs:	2	2	4	3	4	4
Method	Striping	Mirroring	Striping + Mirror	Strip/Mirror	Striping + Parity	Striping + Parity
Redundancy	No	Yes	Yes	Yes	Yes	Yes
Fault Tolerance	No	Yes	2 Discs	1 Disc	2 Discs	2 Discs
Storage Loss	0	50%	50%	33%	50%	50%
Performance	Increase	Slower	Increase	Increase	Increase	Increase

RAID 0 is ideal for performance, like editing video.



3.2.10 - Removable Storage Drives

a. Can be moved between computers without opening case
b. Drive enclosures:
    - HDDs and SSDs can be removable storage by placing them into an enclosure.
    - Enclosure: data interface, power connector, and physical protection for disk.
c. Flash drives and memory cards
    - SSDs use flash memory, also known as USB, thumb, or pen drive

3.2.11 - Optical Drives

a. Use lasers to read data encoded on disc surface
b. Different formats: Basic recordable media, multisession recordable media, rewritable media
c. Consumer DVDs and Blu-rays often include digital rights management (DRM) and region coding, which restricts disc usage to players from the same region.

Each optical disc has different capacities/transfer rates:

- CD: Up to 700MB, at ~150KBps. Comes in CD-R (recordable) and CD-RW (rewritable)
- DVD: Up to 4.7GB (single-layer, single-sided) to 17GB (dual-layer, double-sided) at ~1.32MBps (9x CD Speed). Comes in DVD+R/RW and DVD-R/RW.
- Blu-ray: Up to 25GB per layer. Either BD-ROM (read-only) and BD-RE (rewritable).

3.3 - System Memory

3.3.1 - System RAM and Virtual Memory

a. Faster than SSD Flash and HDDs, but only works when power is provided
b. Address space has two main pathways:
    i. Data pathway - determines the amount of info transferred per clock cycle
    ii. Address pathway- determines the number of memory location the CPU can track

3.3.2 - RAM Types

c. Dynamic (DRAM): Stores data as electrical charges in bit cells made of capacitors
d. Synchronous DRAM (SDRAM): Synchronized to the system clock; ensures memory operations are timed with the CPUs instructions
e. Double Data Rate SDRAM (DDR SDRAM): transmits data on both rising and falling edges of the clock cycle
f. CAS latency (Column Access Strobe) refers to delay between the memory controller requesting data from the RAM and the moment it becomes available.

RAM Type	Data Rate	Transfer Rate	Maximum Size
DDR1	200-400 MT/s	1.6 - 3.2 GB/s	1GB
DDR2	400-1066 MT/s	3.2 - 8.5 GB/s	4GB
DDR3	800-2133 MT/s	6.4 - 17.066	16GB
DDR4	1600 - 3200 MT/s	12.8 - 25.6 GB/s	32GB
DDR5	4800 - 8K+	38.4 - 51.2+ GB/s	128GB or higher

3.3.3 - Memory Modules

g. Printed circuit board that hold a group of RAM devices as a single unit
h. Desktop memory is packaged as Dual Inline Memory Module (DIMM) and used in desktops
i. Small Outline DIMs (SODIMMs) are used in laptops and compact devices

3.3.5 - Multi-Channel System Memory

j. Single-channel memory has 1x 64-bit data bus, Dual-Channel doubles with 2x 64-bit pathways at 128 bits
k. Configuring dual-channel: slot arrangement, installation, and system setup
l. Mismatched modules and flex mode
m. Triple-channel and quadruple-channel memory

3.3.8 - Error Correction Code Ram (ECC RAM)

n. Used for high reliability, prevention of data corruption and crashes
o. Most ECC RAM is supplied as Registered DIMMs (RDIMMs), which include a register
p. Compatibility considerations:
    i. Motherboard and CPU support
    ii. DIMM type compatibility
    iii. Mixing ECC and Non-ECC

3.4 - CPUs

3.4.1 - CPU Architecture

a. When a software program runs, instructions are assembled using the CPU's instruction set, and loaded into memory
b. CPU then performs basic operations on each instruction, managed by the Control Unit
    i. Fetch: Control unit fetches instruction from system memory to the pipeline
    ii. Decode: Decode and either executes it or passes it to ALU (Arithmetic logic unit) or FPU (floating-point unit) for execution
    iii. Execute: The ALU or FPU execute the instruction
    iv. Write-back: The result is written back to a register, cache, or system memory
        1. A register is a temporary storage area within the CPU that operates at the same clock speed as the CPU

2. A cache is a small block of memory that operates at or near the speed of the CPU, depending on cache level (L1, L2, L3). A cache enhances performance by storing frequently used instructions and data, reducing the time needed to access this information.

3.4.2 - X86 CPU Architecture

c. CPU architecture determines performance and suitability for different applications
d. 2 Primary types:
    i. RISC: Reduced Instruction Set Computing, Uses small set of instructions for faster execution
    ii. CISC: Complex Instruction Set Computing, Uses a larger instruction set for complex operations
    iii. Key CPU Components: ALU, Control Unit, performance features, hyper-threading technology

3.4.3 - X64 CPU Architecture

e. Allows CPUs to handle 64-bit instructions, data paths, and memory
f. Can run both 32-bit and 64-bit software
g. Better performance, increased memory capacity, and support for advanced computing

3.4.4 - ARM (Advanced RISC Machine) CPU Architecture

h. Provide customized designs; typically uses a system-on-chip (SoC)
i. OS, drivers, and apps must be specifically compiled for ARM instruction set
j. Physical considerations
    i. Soldered directly on the motherboard; saves space and is lighter weight
    ii. Low power use and good heat management

3.4.5 - CPU Features

k. SImultaneous Multithreading (SMT)
    i. Allow multiple streams to be processed at the same time
    ii. Allow each physical core to act like two virtual cores
l. Symmetric Multiprocessing (SMP)
    i. Uses two or more physical CPUs in a system
m. Chip-level Multiprocessing (CMP)
    i. Places multiple cores on a single chip for better processing

3.4.6 - CPU Socket Types

n. Feature a Zero Insertion Force (ZIF) mechanism; allows CPU installation without pressure
o. Great care is needed when installing or removing a CPU
p. AMD socket types and features
    i. Uses Pin Grid Array (PGA) sockets with pins on the CPU fitting into the motherboard socket
    ii. AM4: Used for AMDs Ryzen processors, providing compatibility across multiple generations
    iii. TR4: Designed for Threadripper CPUs, catering to high-performance desktop applications
    iv. SP3: Used for AMD's EPYC server processors, which utilize LGA sockets for enhanced durability and performance.
q. Intel socket types and features
    i. Uses Land Grid Array (LGA) sockets, where pins are located on the motherboard socket, and the CPU has contact pads
    ii. LGA 1200 (10th and 11th gen core processors, compatible with Intel's Comet Lake and Rocket Lake CPUs)
    iii. LGA 1700 (12th gen Alder Lake SPUs
    iv. Turbo Boost tech: Dynamically increases the processor's clock speed to enhance performance during demanding tasks

3.4.7 - CPU Types and Motherboard Compatibility

r. Core configuration and performance impacts
    i. Single-core vs multi-core processing
    ii. Hyper-threading/Simultaneous Multithreading (SMT)
s. Practical scenarios of core configurations in action
    i. Gaming, virtualization, and workstations
t. Desktops
    i. Intel and AMD socket types
u. Workstations
    i. Business PC or network client; similar components as server-class computers
v. Servers
    i. Multisocket motherboards allow for installation of multiple CPU packages
w. Mobile devices
    i. ARM-based CPUs for superior energy efficiency

Chapter 4

Notes from Chapter 4: Troubleshooting PC Hardware

4.1 - Bios and UEFI

4.1.1 - BIOS and UEFI

Firmware: Special Program code stored in flash memory. Helps initialize components on the motherboard. Allows configuration of system settings.

- Accessed via one of the following key inputs when a vendor's logo appears at boot: Esc, Del, F1, F2, F10, F12.
- Allows the control of Controllers and Adapters, like USB ports

Basic Input/Output System (BIOS):

- Firmware, older version
- Navigation using Keyboard commands

Unified Extensible Firmware Interface (UEFI):

- Firmware, new version
- Supports 64-bit CPU operation, Compatible with 32-bit
- GUI with mouse support
- Networking at boot
- Better boot security

4.1.3 - Boot and Device Options

- Determines the order in which the system firmware searches devices for a boot manager
- Fixed Disk (HDD or SSD): For drives connected by SATA, recommended to connect the boot disk to the lowest-numbered port. In modern systems, SSDs using NVMe via m.2 or PCIe are often used as boot drives, faster than SATA SSDs
- Optical Drive (CD/DVD/Blu-ray): May need to set optical drive as the highest priority
- USB: Commonly used for OS installations and recovery utilities
- Network/PXE (Preboot Execution Environment): Boots via network adapter from a specified server

4.1.4 - USB Permissions

4.1.5 - Fan Considerations

Most cooling fans can be controlled through system settings

- Balanced: Standard setting
- Cool: Runs fans at high speeds for maximum cooling
- Quiet: Reduces fan speed, allowing for higher temps
- Fanless: Disables fans, relying on passive cooling
- Temperature Controlled
- Custom

Temperature Monitoring

- Manual Monitoring: Restart and enter BIOS/UEFI, look for an entry related to monitoring or sensors to view real-time readings
- Third-Party Applications: Monitoring through added sensors

4.1.6 - Boot Passwords and Secure Boot

Boot passwords require user authentication before the OS loads. Two main passwords below:

- Supervisor/Administrator/Setup/BIOS Password: Restricts access to the system's BIOS?UEFI setup program
- User/System Password: Locks the entire system until authentication is provided, preventing any actions until the firmware initializes the system

Secure Boot is a UEFI feature that protects against malware by ensuring only trusted, digitally signed bootloaders are used. The system firmware checks the operating system's bootloader against pre-loaded cryptographic keys to verify its integrity. Many modern systems require UEFI with Secure Boot enabled for security and compatibility with newer operating systems.

4.1.8 - Trusted Platform Module (TPM)

A TPM is hardware that securely stores digital certificates, cryptographic keys, and hashed passwords. Each TPM chip has a unique, unchangeable endorsement key, establishing a root of trust.

During boot, the TPM compares hashes of key system data to ensure they haven't been tampered with.

- Superior security via cryptographic keys stored in tamper-resistant hardware
- The TPM's secure storage area can be used by disk encryption programs like Windows BitLocker to store their keys
- TPMs can be enabled, disabled, or reset via the system BIOS/UEFI, and managed from the OS

Hardware Security Module (HSM)

A removable USB thumb drive can be used to store cryptographic keys. Useful if the computer does not support TPM, as a recovery mechanism if the TPM is damaged, or if a disk needs to be moved to another computer. Typically "secure" by means of PIN, fingerprint, or password.

4.2 - Power and Disk Issues

4.2.1 - Troubleshoot Power Issues

Computer On: PSU Converts ACV → DCV. PSU tests 5V and 3.3V. Stable → Good Signal to PSU

To diagnose no power symptoms:

- Check if LEDs on front panel are lit, check fan noise

To isolate cause:

1. Check other equipment: Rule out a power circuit fault or blackout
2. Test the wall socket
3. Verify PSU connections
4. Try another power cable: Be sure to check with multimeter
5. Disconnect extra devices: If solved, not enough power from PSU, or device is faulty
6. Test the PSU: If safe, use a multimeter or power supply tester to check

If the problem persists, likely to be a faulty motherboard or power supply. If a faulty PSU, do not leave it on longer than necessary or unattended. Watch for external signs like smoke or fire, and turn off immediately if any unusual sights, smells, or noises.

4.2.3 - Troubleshoot POST Issues

Once the CPU has been given the "power good" signal, the system firmware performs "power-on self-test" (POST), a diagnostic program implemented in the system firmware that checks hardware components required to boot the computer.

If power is present but the computer doesn't start, shows a blank screen, and there are no beeps from the internal speaker, it is likely either a display issue or the POST procedure is not executing. Assuming the display is not the issue:

1. Ask what has changed
2. Check cabling and connections
3. Check for faulty interfaces and devices
4. Check the PSU
5. Check for a faulty CPU or system firmware

If POST runs but detects a problem, it generates an error message. If the fault prevents the computer from displaying anything on the screen, the error is often indicated by beep codes. The manufacturer's website should determine the meaning of the code.

Original IBM PC beep codes:

- 1 short beep: Normale POST
- 2 short beeps: POST error, -error code shown on screen
- No beep: Power supply, motherboard problem, or faulty onboard speaker
- Continuous beep: Problem with system memory modules or memory controller
- Repeating short beeps: Power supply fault or motherboard problem
- 1 long, 1 short beep: Motherboard problem
- 1 long, 2 or 3 short beeps: Video adapter error
- 3 long beeps: Keyboard issue

4.2.5 - Troubleshoot Boot Issues

After successful POST, the system searches for boot devices in the order specified in the boot sequence. If no bootable device is found, an error message is displayed, and the process halts.

If the system is booting from the wrong device, verify that removable drives do not have media interfering with the boot process, and ensure boot order is correct.

If a fixed disk is not detected:

- Power Check
- Data Connections
- UEFI/BIOS Settings
- m.2/NVMe Drives

4.2.7 - Troubleshoot Boot Sector Issues

If power and cable issues are ruled out, suspect a problem with the device’s boot sector and files. Corruption can occur due to disk faults, power failures, incorrect installation of multiple operating systems, or malware, preventing the disk from booting.

Boot Information Formatting: MBR and GPT

- Master Boot Record (MBR): Legacy scheme- Located in the first sector of the partitioned disk. Holds information about disk partitions and contains code pointing to the active boot sector. The boot sector (located immediately after the MBR or the first sector of each partition) describes the partition’s file system and contains code to boot the operating system. Includes Boot Configuration Data (BCD) for windows or boot managers like GRUB or LILO for Linux. Only one primary partition can be marked as active for booting.
    - Only works with 32-bit, max 4 partitions
- GUID Partition Table (GPT): Not limited to a single sector, provides more robust and flexible partitioning compared to MBR. Identifies partitions and OS boot loaders, with enhanced reliability.
    - Works on 64-bit, max 128 partitions

Damage to the MBR or GPT partition record can cause boot errors like “Boot device not found” “OS not found” or “Invalid drive specification”. If malware caused the issue, the best solution is to use your antivirus software’s boot disk option, which includes a scanner to detect malware and tools to repair the boot sector.

If a recovery disk is unavailable, use the repair options provided by the OS setup disk.

A blank screen during boot can indicate issues with the boot process or display connections.

1. Check display connections
2. Inspect boot errors
3. Malware solutions
4. Repair options

4.2.8 - Troubleshoot OS Errors and Crash Screens

If a boot device is found, the boot sector code is loaded into memory and takes over from the system firmware, loading the rest of the operating system files. Errors after this point are usually due to software or device driver issues rather than hardware problems. Common symptom: Blue Screen of Death (BSOD), which indicates issues such as system memory faults, hardware device or driver problems, or OS file corruption.

- Faulty or incompatible device drivers
- Corrupted system files
- Defective hardware components
- Overheating or power supply issues

To troubleshoot BSOD:

- Use a camera to scan the QR code
- The error is logged in the system log with “BugCheck” as the source. Use the first hex value (e.g. 0x0a) from the event description to search for more information online
- If you have a support contract, a memory dump is generated for further analysis

Troubleshoot Drive Availability

HDDs are more prone to mechanical failure either within the first few months or after several years of use (wear and tear). SSDs are generally more reliable but have a limited lifespan due to the wear on memory cells from repeated writes. Power loss during write operations can cause data corruption or hardware damage for both types of drives.

Common symptoms of a failing drive:

- Unusual noise (HDD)
- No LED status/activity
- Constant LED activity (Disk thrashing)
- Bootable device not found
- Missing drives in OS
- Read/Write failure
- Audible alarms
- BSOD

If you encounter any of these symptoms, it’s important to back up data immediately and replace the drive to prevent data loss.

4.2.9 - Troubleshoot Drive Reliability and Performance

If you suspect a drive is failing or experience performance issues, run advanced diagnostic tests. Most disk vendors provide utilities for testing drives as well as system diagnostics programs. Diagnostic tests can detect damage to the storage mechanisms and report statistics such as input/output operations per second (IOPS)

Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T.): Included on most fixed disks, can alert the OS if a failure is detected.

You can also use Windows utilities to query SMART and run manual tests. Some of the reasons read/write functions might be slow:

- Application load and general system resource issues
- File fragmentation on HDDs
- Limited remaining capacity
- Failing sectors (HDDs) or blocks (SSDs)

4.2.12 - Troubleshoot RAID Failure

There are 2 main scenarios for RAID failure:

1. Device Failure: If one of the devices in the array fails, the volume will be listed as “degraded,” but the data will still be accessible, and it should continue to function as a boot device if configured to do so.
2. Array Failure

Troubleshooting steps:

- Unavailable Volume or “array missing”: If the volume is not available, either more disks have failed than the array can tolerate, or the controller has failed. If the boot volume is affected, the OS will not start. Use the latest backup or file recovery solutions if too many disks have failed.
- Controller FailureIf the controller fails, data on the volume should be recoverable, though there may be file corruption if a write operation was interrupted. Install a new controller or import the disks into another system.
- Boot Process Issues: Use the RAID configuration utility to verify the status. If you cannot access the utility, the controller likely failed.

4.3 - System and DIsplay Issues

4.3.1 - Troubleshoot Component Issues

Diagnostic Steps:

1. Eliminate software issues: Ensure that software, disk/file corruption, and malware are not the causes
2. Identify patterns: e.g.: If errors occur after the PC has been running for a while, it could indicate a thermal issue.
3. Check power supply: Extended periods with very low power and damage components. Exceeding 12V will result in damage to sensitive components.
4. Suspect Hardware: Use diagnostic test programs provided by the vendor ,which are often run from the firmware setup utility rather than the OS
5. Observe Physical Symptoms

4.3.2 - Overheating

1. Temperature Sensors: Most systems have internal sensors accessible via driver or management software. Use vendor documentation to ensure the system operates within acceptable limits.
2. CPU Fan: Vital for keeping the processor cool for performance and longevity. A fan from an older CPU may not be suitable for an upgraded processor.
3. Heat Sink: Clean and replace old thermal paste if necessary to help lower the processor’s temperature.
4. Blanking Plates: Uncovered holes can disrupt airflow and reduce cooling effectiveness.
5. Environment: The colder the better.

**Thermal problems can also cause loose connectors, components to move in their sockets, or circuit board defects like hairline cracks to widen and break connections.

4.3.3 - Physical Damage

*Always inspect a computer closely for case damage; a small crack or dent may indicate a fall or knock that could have caused internal damage. If the motherboard shows physical damage, diagnostic software is essential to confirm the problem.

Motherboard issues are rare but possible. Be aware of the following:

- ESD, electrical spikes, or overheating: Can damage the motherboard’s soldered chips and components.
- Careless Insertion: Pins on integrated connectors can be damaged.
- Dirt and Chip Creep: Errors can be caused by dirty contacts or “chip creep”, where an adapter works loose from its socket over time due to temperature changes.
- Liquid Spills
- Schorch Marks and Capacitor Swelling: A “blown” component may leave scorch marks. Swollen or bulging capacitors, which regulate electricity flow, may indicate damage or manufacturing defects.

4.3.4 - Troubleshoot Performance Issues

1. Check for overheating: If temps are high, consider cleaning the computer and/or upgrading the cooling system.
2. Check for misconfigurations: Always ask “What has changed?” when diagnosing issues.
3. Verify the problem

4. Rule out software/configuration/networking issues: Rule out operating system and application issues before assuming hardware problems. Use built-in or third-party diagnostic tools to verify component performance.

4.3.5 - Troubleshoot Inaccurate System Date/Time

The real-time clock (RTC) tracks the date and time, powered by a coin-cell lithium battery (Usually CR2032) while the computer is off. An incorrect setting can disrupt network authentication and make scheduled tasks unreliable.

If the time in the system setup is incorrect, it may signal a failing RTC battery. This battery is often called the "CMOS battery" because older systems stored settings in CMOS (complementary metal-oxide semiconductor) RAM. Modern systems use NVRAM (non-volatile RAM) or flash memory for configuration data.

4.3.6 - Troubleshoot Missing Video Issues

1. Verify display device(s) are plugged in and turned on, and cycle the power.
2. Use the monitor's controls to adjust the image or select the correct input source.
3. Check cable and connectors between the video card and the monitor.
4. Verify the cable specification matches the application requirements.
5. Verify cable and port compatibility (such as HDMI 2.1 vs older versions)
6. If on a projector, verify the bulb hasn't burnt out. A completely failed bulb may produce a popping sound and show visible scorch marks or a broken filament. (Some projectors have sensors to detect and notify the user)
7. If on a projector, intermittent projector shutdown can be caused by overheating, check all fans and verify the ventilation system is clear of dust and debris, and all vents are unblocked.

4.3.7 - Troubleshoot Video Quality Issues

- Dim Image: Check the on-screen display (OSD) to adjust brightness and contrast. Take note of power-saving modes or features like adaptive brightness or eye-saving mode. If the image is barely visible, the backlight may have failed, and the display may need repair or replacement.
- Fuzzy image: Often due to a mismatch between the output resolution and the display's native resolution.
- Flashing screen: Check cables and connectors. Could also result from failing backlight components or internal circuitry. Other signs of failure include bands, lines, or bright spots.
- Dead pixels: Stuck (bright) or dead (black) pixels on flat-panel displays. Pixel cycling software or slightly tapping the screen with a soft object can fix Stuck pixels. Dead pixels cannot be repaired.
- Display burn-in: When a static image is displayed for so long it leaves a ghost image on the screen. OLED and plasma displays are more prone to this. A screen saver or displays auto-off function can help delay or prevent this.
- Incorrect color display: Utilize the Color Management applet in Control Panel along with a test card of color patterns and spectrophotometers to define and verify this profile.
- Color glitches, such as purple or green horizontal lines or unexpected color changes are often caused by a faulty or loose connector or low-quality cabling. If not the cabling, there may be a hardware fault in the monitor or graphics adapter.
    - Audio Issues: Verify that the correct audio output is selected in the OS and that volume settings are appropriate
    - Sizing Issues: If the image is stretched, compressed, or has black bars around the edges, adjust the display settings on your computer to match the monitor's native resolution and use the monitor's OSD to fit the image to the screen. Also, ensure correct video drivers are installed and updated.
    - Distorted Image: If the screen appears wavy or shows geometric warping, check for interference from nearby electronic devices, secure all cable connections, and ensure the display settings match the monitor's native resolution. For CRTs, adjust the pincushion settings and consider replacing the potentially faulty cable.

‼️ Chapter 5

Notes from Chapter 5: Comparing Local Networking Hardware

5.1 - Network Types

5.1.1 - LANs and WANs

Local Area Network (LAN)

- A group of computers connected by cabling and one or more network switches that are all installed at a single geographical location, usually within a mile of one another.
- Copper cabling is most common.
- Most are based on ethernet standards maintained by the Institute of Electrical and Electronics Engineers (IEEE).
- IEEE 802.3 standards are designed xBASE-Y, where x is the nominal data rate, and Y is the cable type, e.g.:
    - 100BASE-T refers to Fast Ethernet over copper twisted pair cabling, works at 100Mbps
    - 1000BASE-T refers to Gigabit ethernet over copper twisted pair cabling, works at 1Gbps (Mainstream standard for most LANs)
    - 10GBASE-T refers to a copper cabling standard working at 10Gbps

*Some LAN or special Ethernet networks will utilize fiber optic cabling, which pulses light to transmit data.

Wide Area Network (WAN)

- A network that spans multiple geographic locations.
- Often used to connect LANs to the internet.

Wireless LANs (WLAN)

- Uses radio and antenna for data transmission and reception
- IEEE 802.11 is common standard, known as WiFi

Metropolitan Area Networks (MAN)

- Generally a network provided by a company with multiple networks within the same metropolitan area

Personal Area Networks (PAN)

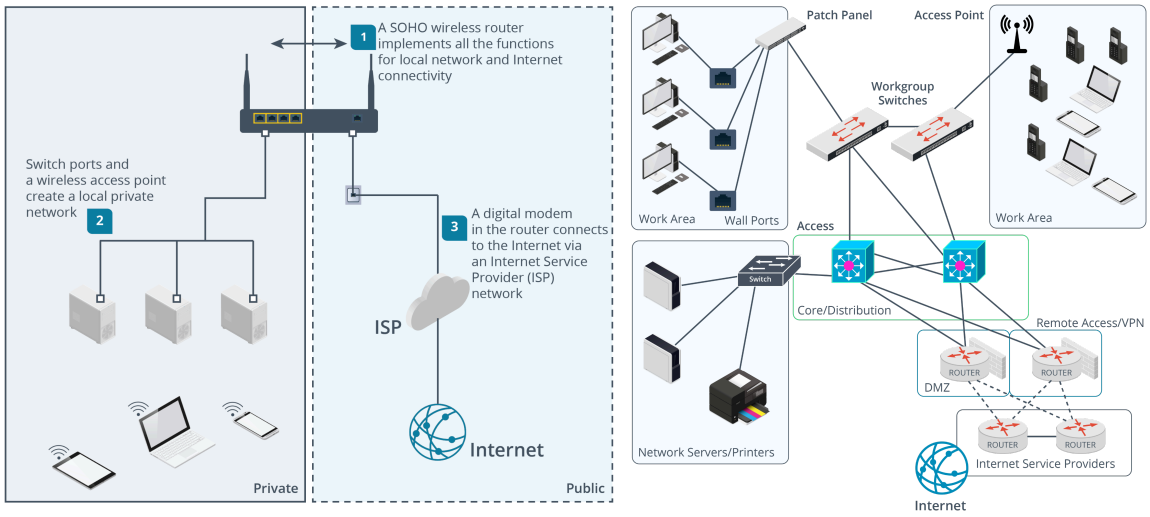
- Utilizing wireless connectivity to connect to devices at a range of a few meters

Storage Area Network (SAN)

- Specialized network dedicated to storage
- Dedicated Network - The SAN must be attached to a dedicated network that is independent of the LAN; keeps traffic consolidated.
- Block-Level Access - Data sent across the SAN is transferred in raw chunks of data with no file system structure called blocks. This allows for efficient data transfers and flexible storage management options.
- Consolidated Storage - Multiple types of storage, such as RAID arrays and tape drives; establishes a centralized storage resource for servers.
- High Speed - SANs will typically utilize high-speed connections such as Fibre Channel or Internet Small Computer System Interface (iSCSI) for data transfer.

5.1.2 - SOHO and Enterprise Networks

A small office/home office (SOHO) LAN is a small network possibly using a centralized server; often uses a single networking appliance to provide LAN and Internet connectivity. Often referred to as a "SOHO router" or "Internet router," or "broadband router." Only supports a small number of users.



5.1.3 - Datacenters

A datacenter is a whole site that is dedicated to provisioning server resources. A datacenter has dedicated networking, power, climate control, and physical access control features.

On an enterprise LAN, server computers are hosted in a separate area, the "server room".

5.2 - Networking Hardware

5.2.1 - Network Interface Cards

The physical connection to an internet cable is made using a transceiver port in a computer's Network Interface Card (NIC). Most PC motherboards have a built-in 1000BASE-T compatible adapter.

Multiple NIC adapter cards can be installed on a computer, which can be bonded to create a higher-speed link. E.g.: 4x Gigabit ports could be bonded to give a link speed of 4Gbps.

Media Access Control (MAC) - Each NIC port has a unique hardware/physical address, part of the data link protocol, where each frame of ethernet data identifies the source MAC address and destination MAC address in fields in a header.

A MAC address consists of 48 binary digits, making it six bytes in size. A MAC address is typically represented as 12 digits of hexadecimal. Hexadecimal is a numbering system often used to represent network addresses of different types. A hexadecimal digital can be one of 16 values: 0-9 and then A, B, C, D, E, F. Each hexadecimal digit represents half a byte (or four bits aka a nibble)

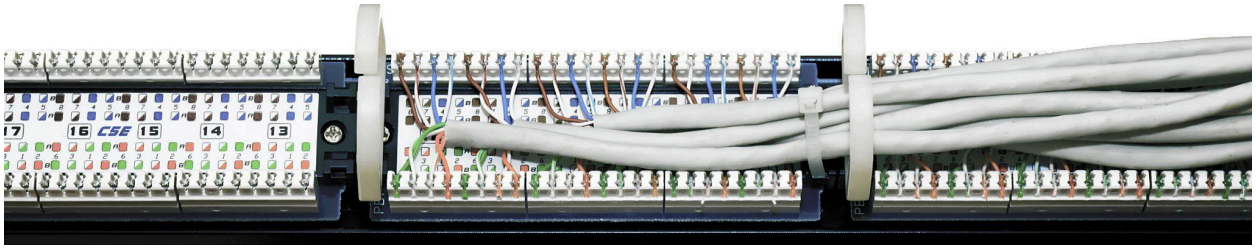
A MAC address is typically written out with a colon separating every two digits. They may occasionally use a hyphen or no separator. E.g.: 00:60:8C:12:3A:BC OR 00609C123ABC

A MAC address is broken into two distinct parts:

- The first 24 bits are known as the Organizationally Unique Identifier (OUI), which identifies the manufacturer of the NIC.
- The last 24 bits are known as the Network Interface Controller (NIC) Specific, which is unique to each NIC

When you convert the first two hex digits of a MAC address to binary, the two right-most bits act as flags. The very last bit shows individua11l (0) versus group/multicast (1). The bit just to its left shows universally administered (0, factory) versus locally administered (1, set by software).
https://www.youtube.com/watch?v=dR2nNOLV_1s

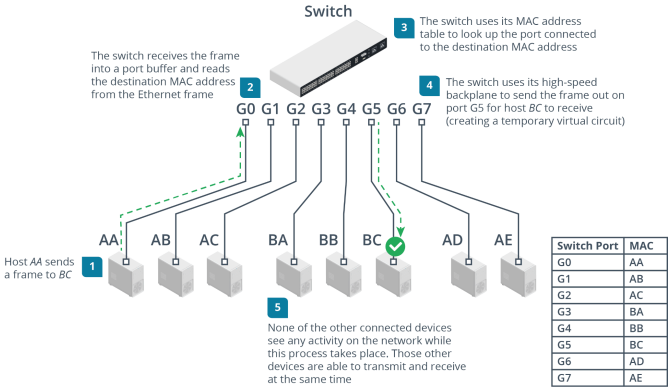
5.2.3 - Patch Panels



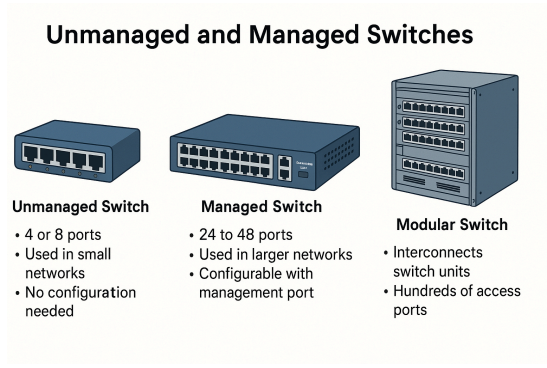
^IDCs (Insulation Displacement Connector) tied into punchdown blocks at the back of a patch panel. The reverse side has RJ45 ports.

A patch cord is used to connect a port on the patch panel to a port on an ethernet switch.

5.2.6 - Switches & 5.2.9 - Unmanaged and Managed Switches



Switch Port	MAC
G0	AA
G1	AB
G2	AC
G3	BA
G4	BB
G5	BC
G6	AD
G7	AE



^Used to connect multiple devices inside of a network together. The switch provisions one port for each device that needs to connect to the network. When a device is connected to the switch, it adds the device's MAC address to a table and keeps track of which port it connects to. The switch is able to intelligently forward frames to the ports that are a match for the destination MAC address.

- Each switch port is considered a separate collision domain, where the negative effects of collisions are eliminated.
- Unmanaged Switch: Doesn't require any configuration.Typically used in SOHO networks, and usually in 4-8 ports.
- Managed Switch: Designed for larger LANs, usually comes with 24 or 48 ports.

– – Continued – –

5.2.10 - Power Over Ethernet

PoE (Power over Ethernet) is when an ethernet line is capable of providing some power to a device, such as a camera, WAP, or voice over IP handset (VoIP)

- **802.3af** (Type 1 PoE or 2-pair PoE)
  - Allows up to 13W to a device, supplied as 350mA@48v. Maximum range 100m/300'
- **802.3at** (PoE+ or Type 2 PoE)
  - Allows up to 25W, at 600mA
- **802.3bt** (PoE++, Type 3 and Type 4 PoE, 4PPoE)
  - Allows up to 51W(Type 3) or 73W (Type 4).

Power over Ethernet (PoE) Basics

802.3bt	**Type 3 & 4**	**PoE++**	**51W or 73W**
802.3at	Type 2	**PoE+**	**25w**
802.3af	Type 1	PoE	13W

They are chronological: af, at, bt

Generally only provide nominal power under 100'

A POE injector, or Midspan, can add power if the switch doesn't

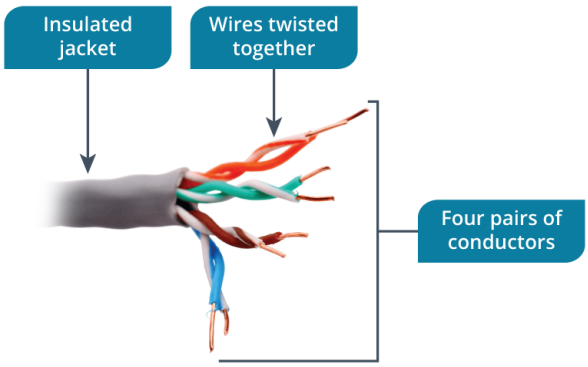
PoE Switch: Allows the governance of devices connected to the network

PoE Injector: Also called a "midspan", used to add PoE to a device when the switch doesn't support PoE. Cannot exceed 100m

5.3 - Network Cable Types

5.3.1 - Unshielded Twisted Pair (UTP)

Most popular type of network cable. Consists of conductor wire pairs. Each pair of insulated is twisted at a different rate from the other pairs, reduces interference. Signal loses strength over ranges, about 100m per segment



4x copper conductors which long

5.3.2 - Shielded Twisted Pair (STP)

Provides extra protection against interference; is usually a requirement in environments with high levels of external interference. Several types exist:

- Foiled Unshielded Twisted Pair (F/UTP) has a single foil shield around the all the wires. Also called Screened twisted pair (ScTP) or foiled twisted pair (FTP). "Decent protection" against EMI and crosstalk at "reasonable cost"
- Shielded Foiled Twisted Pair (S/FTP) has a braided outer screen and foil-shielded pairs. "Best protection" against EMI and crosstalk, expensive and less flexible. Also has a variant of foil outer shield (F/FTP)
- Unshielded with Foiled Twisted Pair (U/FTP) where each pair of wires has a foil shield around them. "Good protection" against EMI and crosstalk.

– – Continued – –

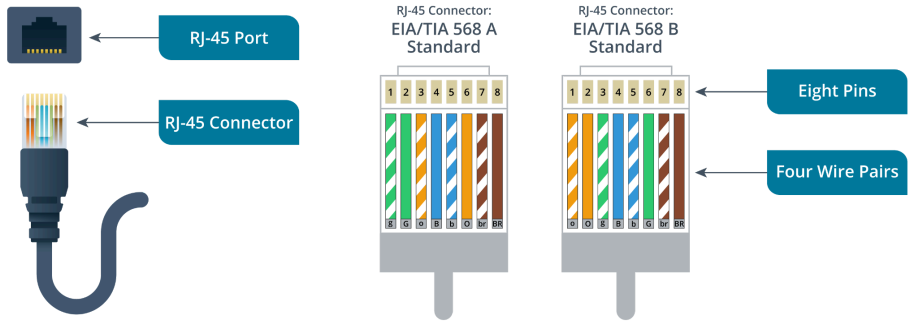
5.3.4 - Cat Standards

Cat specifications are defined in the TIA/EIA-568-C Commercial Building Telecommunications Cabling Standards.

Cat	Max Rate	Max Distance	IEEE Standard	
8	40Gbps	30m (100')	40GBASE-T	40G Ethernet
	25Gbps	30m (100')	25GBASE-T	25G Ethernet
7	100Gbps	15m (50')	100GBASE-T	100G Ethernet
	10Gbps	100m (328')	10GBASE-T	10G Ethernet
6A	10Gbps	100m (328')	10GBASE-T	10G Ethernet
6	10Gpbs	55m (180')	10GBASE-T	10G Ethernet
	1Gbps	100m (328')	1000BASE-T	Gigabit Ethernet
5e	1Gbps	100m (328')	1000BASE-T	Gigabit Ethernet
5	100Mbps	100m (328')	100BASE-TX	"Fast Internet
*CAT specifications are printed on the cable jacket along with the cable type				

*Cat specifications are printed on the cable jacket along with the cable type

5.3.5 - Copper Cabling Connectors



RJ45 Connectors are also referred to as “8P8C”, or eight-position / eight-contact.

The EIA/TIA-568 standard defines two methods for terminating twisted pair: T568A/T568B

In T568A, pin 1 is wired to green/white, pin 2 is wired to green, pin 3 is wired to orange/white, and pin 6 is wired to orange. (T stands for “Telecommunications”)

In T568B, the position of the green and orange pairs is swapped over, so that orange terminates to 1 and 2 and green to 3 and 6 (B standard is most common in USA)

5.3.7 - Copper Cabling Installation Tools

Cable Stripper and Snips, Punchdown Tool, Crimper

Copper Cabling Test Tools - Good testers incorporate the function of a toner probe, used to identify a cable within a bundle. A loopback plug can be used to test a NIC or switch port.

5.3.9 - Network Taps

Used to intercept the signals passing over a cable and send them to a packet or protocol analyzer, and come in either powered or unpowered.

- A passive test access point (TAP) is a box with ports for incoming and outgoing network cabling and an inductor or optical splitter that physically copies the signal from the cabling to a monitor port.
- An active tap is a powered device that performs signal regeneration.

5.3.10 - Copper Cabling Installation Considerations

- Plenum Cable: Fire-retardant cabling used in Plenum spaces, required by building code. Must not emit large amounts of smoke when burned, be self-extinguishing, and meet other strict fire-safety standards
- Direct Burial: Weathering and extreme conditions must be considered, as well as rodents chewing the lines.

5.3.11 - Optical Cabling

Consists of an ultra-fine core of glass to convey the light pulses. The core is surrounded by glass or plastic cladding, which guides the light pulses along the core. The cladding has a protective coating called the “buffer”. 2 main categories include:

- Single-mode fiber (SMF): Small core designed to carry a long wavelength infrared signal in the 1,310 to 1,550 nm range) which is generated by a laser diode. Supports up to 10Gbbps or better and can run great distances.
- Multimode fiber (MMF): Large core designed to carry a shorter wavelength infrared light in the 850 to 1,300 nm range. Less expensive, not as good. Doesn’t support high signaling speeds or long distances, is more suitable for LANs than WANs

Fiber optic connectors come in 3 common form factors and can be interchanged based on needs:

- Straight-tip connector (ST): Bayonet-style connector that uses a push-and-twist locking mechanism, used mostly on older multi-mode networks
- Subscriber connector (SC) has a push/pull design that allows for simpler insertion and removal. Simplex and duplex version, it can be used for single- or multi-mode
- Lucent connector (LC) Small form connector with a tabbed push/pull design, similar to SC, but smaller.

5.3.13 - Coaxial Cabling

Copper cabling that also carries electrical signals. The core signal conductor is enclosed by plastic insulation (dielectric) and a second wire mesh conductor serves both as shielding from EMI and as a ground.

Used mostly for CCTV installations and as a patch cable for Cable Access TV (CATV) and broadband cable modem.

5.4 - Wireless Networking Types

5.4.1 - Access Points

An access point can establish a wireless-only network, but it can also work as a bridge to forward communications between the wireless stations and a wired network, also referred to as a “Distribution system” (DS).

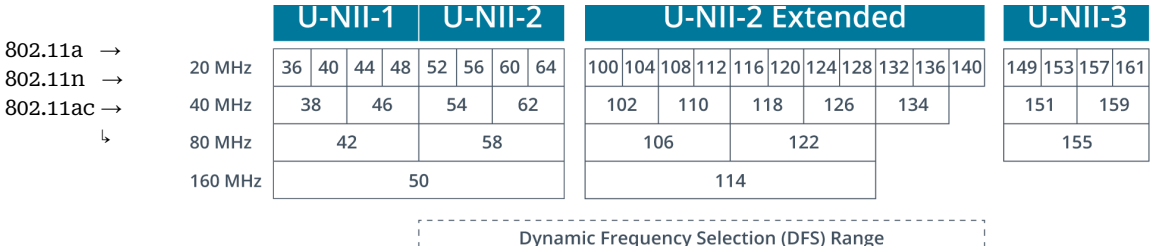
Most Wi-Fi networks are configured in what is technically referred to as “Infrastructure mode”, where each client device or station is configured to connect to the network via an access point. In 902.11 documentation, this is referred to as an infrastructure “Basic Service Set” (BSS).

5.4.2 - Frequency Bands

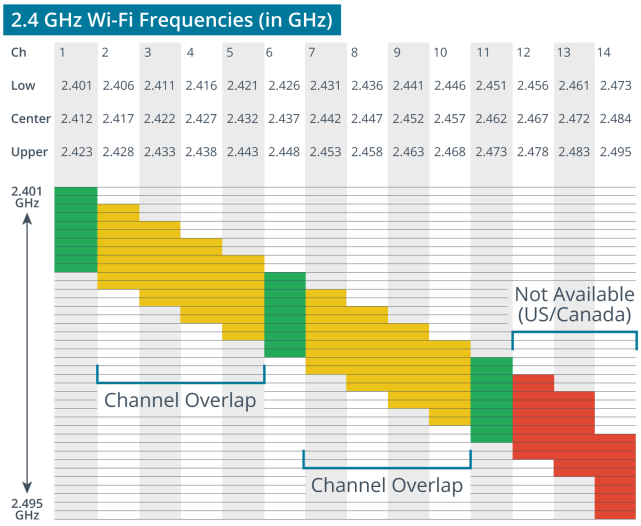
Remember this order: a/b/g/n/ag/ax/be

Each wireless frequency band is split into a series of smaller ranges referred to as a channel. Width and size of each channel is determined by the frequency band and access point configuration.

- 2.4GHz: Standard that is good at propagating through solid surfaces, increased risk of interference. Used by inferior IEEE802.11b. Max range 45m/150’ and 11Mbps. Has 3x non-overlapping channels (1, 6, 11)
- 5GHz: Not great at long ranges, but supports higher data rates at shorter ranges. Used exclusively by WiFi (IEEE 802.11a). Max range 30m/100’ and 54Mbps. 23 non-overlapping channels. Dynamic Frequency Selection (DFS) reduces potential interference when using a group of channels.
- 6GHz: Newest standard, less effective at penetrating solid surfaces, but faster than the older bands. Most stable and reliable connection. Max range 15m/50’



Unlicensed National Information Infrastructure (U-NII) sub-bands form the 20 MHz channels used in the 5 GHz frequency band. Each sub-band is 5 MHz wide, so the Wi-Fi channels are spaced in intervals of four to allow 20 MHz bandwidth. Channels within the DFS range will be disabled if the access point detects radar signals. 802.11n 40 MHz bonded channel options in the 5 GHz band. The center channel number is used to identify each bonded channel



The 2.4 GHz band is subdivided into up to 14 channels, spaced at 5 MHz intervals from 2,412 MHz up to 2,484 MHz. Because the spacing between each channel is only 5 MHz and 802.11b uses channels that are 22 MHz wide, 802.11b channels overlap quite considerably. This means that interference is going to occur unless you use one of the three non-overlapping channels (1, 6, and 11). Also, in the Americas, regulations permit the use of channels 1–11 only, while in Europe, channels 1–13 are permitted, and in Japan, all 14 channels are permitted.

5.4.3 - IEEE 802.11a

Remember this order: a/b/g/n/ag/ax/be

Wi-Fi 1 (802.11a) utilizing the 5GHz band only, achieves a maximum 54Mbps. Established dynamic frequency selection to prevent signals from interfering with nearby radar and satellite installations.

5.4.4 - IEEE 802.11b/g

Wi-Fi 2 (802.11b) utilizes the 2.4GHz band only, achieves a maximum of 11Mbps

Wi-Fi 3 (802.11g) utilizes the 2.4GHz band while achieving 54Mbps and making it backward compatible. Uses Orthogonal Frequency-Division Multiplexing (OFDM) which increases data rates on smaller channels (20MHz)

The IEEE 802.11g standard offered a relatively straightforward upgrade path from 802.11b. 802.11g uses the same encoding mechanism and 54 Mbps rate as 802.11a but in the 2.4 GHz band used by 802.11b. This made it straightforward for vendors to design 802.11g devices that could offer backward support for legacy 802.11b clients.

One key difference between 802.11b and 802.11g is the channel width. 802.11b uses a 22 MHz channel width, whereas 802.11g uses a 20 MHz channel width. This is due to the modulation technique that each standard uses. Modulation is the process or technique used to modify a radio wave so it can carry data.

5.4.5 - IEEE 802.11n

WiFi 4 (802.11n) utilizes the 2.4GHz and 5GHz bands, through channel bonding. Multiple input multiple output (MIMO) increased reliability and bandwidth by multiplexing signal streams from 2-3 separate antennas. 802.11n access points are marketed using Nxxx designations, where xxx is the nominal bandwidth: e.g.- N600 2x2 access point can allocate a bonded channel of two streams for a data rate of 300Mbps, or 600Mbps when dual banding.

5.4.7 - Wi-Fi 5 and Wi-Fi 6

Wi-Fi 5 (802.11ac), designed to only work on the 5GHz band. Allows up to 8 streams, but most often only supports 4x4 streams. Single stream over 80MHz channel has a nominal rate of 433Mbps, and allows wider 80 and 160MHz through channel bonding, which raises the concern for interference. Multiuser MIMO is a Wi-Fi- 5 introduction that allows the access point to use its multiple antennas to send data to up to four clients simultaneously. Potential for 6.9Gbps

Wi-Fi 6 (802.11ax) works over both 2.4GHz and 5GHz bands while introducing support for a new 6GHz band, which makes it easier to use 80 and 160, and allows for up to 8 clients and support for uplink MU-MIMO. It also improved “orthogonal frequency division multiple access (OFDMA)”, an improvement in sustaining high data rates. Can achieve 9.6Gbps

5.4.8 - Wi-Fi 7

Wi-Fi 7 (802.11be) operates in 2.4GHz, 5GHz, and 6GHz bands, utilizing channels that are 320MHz wide, and speeds up to 46Gbps. Also adds support for Multi-Link Operation (MLO) to reduce latency by connecting and sending data over multiple bands. Multi-Resource Units (MRUs) where each channel in the 6GHz range is broken down into smaller channels of different sizes based on the needs of the network.

5.4.9 - Wireless LAN Installation Considerations

– – null – –

5.4.10 - Wi-Fi Analyzers

Service Set Identifier (SSID) or “network name” that is configured on an access point. Up to 32 bytes in length, utilizing ASCII letters and digits plus the hyphen and underscore characters.

Utilizing a Wi-Fi Analyzer, one can determine the best channel layout and troubleshoot wireless network performance as well as measure the signal strengths of different networks.

- Wireless signal strength is measured in decibel units, and is represented as a ratio of a measurement to 1 milliwatt (mW), where 1mW is equal to 0dBm. dBm values closer to zero represent better performance.
    - A -30dBm is 0.001mW; a -60dBm is 0.000001mW

    - A value around -65dBm is good, anything over -85dBm is likely to suffer packet loss or be dropped.
- Signal-to-noise ratio: the comparative strength of the data signal to the background noise, values closer to zero are less welcome.
    - If a signal is -65dBm and noise is -90dBm, the SNR is 25dB.
    - If a signal is -80dBm and noise is -90dBm, the SNR is 15dB, worse than before.

5.4.11 - Long-Range Fixed Wireless

Solutions save on cable by utilizing wireless bridges between two networks.

- Point-to-point line-of-sight fixed wireless uses ground-based high-gain(strongly directional) microwave antennas. Can transmit up to 30 miles away when unobstructed.
- Licensed frequency in US regulated by FCC
- Unlicensed frequency uses “public frequency bands”, such as 900MHz, 2.4GHz and 5GHz. Power output is limited by regulatory requirements
- Effective isotropic radiated power (EIRP) is the sum of transmit power and gain, expressed in dBm.

5.4.12 - Bluetooth, RFID, and NFC

Bluetooth

- The earliest version supports a maximum range of 10m/30’, weak signal, supports up to 3Mbps.
- Version 3 & 4 support up to 24Mbps with the ability to share an 802.11 radio link for large files.
- Version 4 introduced Bluetooth Low Energy (BLE), designed for small battery-powered devices that transmit small amounts of data infrequently, and is not backward compatible with “classic” bluetooth.
- Version 5 offers a range of 240m/800’, 4x the range of version 4, with twice the speed and 8 times the messaging capacity, as well as an improvement over power consumption.

Radio Frequency Identification (RFID) is a means of identifying and tracking objects using specilay encoded tags.

- Can be unpowered, a passive device that responds with information when scanned
- Can be powered, with a device range of 100m/300’

Near Field Communications are peer-to-peer versions of RFID. Usually works up to 2”/6cm at data rates of 106, 212, and 424Kbps. Mostly used for contactless payment readers, security ID tags, and shop labels for stock control.

!! Chapter 6

Notes from Chapter 6: Configuring Network Addressing and Internet Connections

6.1 - Internet Connection Types

6.1.1 - Internet Connection Types and Modems

Public-Switched-Telephone-Network (PSTN)

- Fiber optic core, with some lines still composed of copper, “plain-old-telephone-system,” “Local loop,” or “last mile”.

6.1.2 - Digital-subscriber-line (DSL)

Uses higher frequencies available in these copper telephone lines as a communications channel. The use of advanced modulation and echo canceling techniques enables high-bandwidth, full-duplex transmissions.

- **Asymmetrical DSL (ADSL)** provides fast downlink, but slow uplink.
    - ADSL2+ offers downlink rates of 24Mbps and unlink rates of 1.4-3.3Mbps
- **Symmetric versions of DSL** offer the same, but are generally used by businesses and branch offices.
- A DSL modem is used to connect, often like a vendor’s specific device or a standalone.
- A filter, or splitter, must be installed on each phone socket to separate voice and data. Modern sockets often have it built in.

6.1.4 - Cable Access TV (CATV)

Often described as a **hybrid fiber coax (HFC)** as it combines a fiber optic core network with copper coaxial cable links to the customer’s equipment. Also described as “broadband cable” or “cable”.

- Data over cable service interface specification (DOCSIS) supports downlink speeds up to 42.88Mbps (North America) or 55.62Mbps (Europe), and uplinks up to 30.72Mbps.
- DOCSIS version 4 allows the use of multiplexed channels; 10Gbps downlink and 6Gbps uplink.

6.1.5 - Fiber to the Curb and Fiber to the Premises

Fiber to the Curb (FTTC) A method where an ISP provides fiber-optic cables as close to a customer’s front door as possible, and then utilizes the client’s telephone system to bridge the gap.

- Utilizes very high-speed DSL (VDSL) to bridge the internet
- Over 300m/1,000’ an asymmetric link supports 52Mbps downstream and 16Mbps upstream
- A symmetric link supports 26Mbps in both directions
- VDSL2-Vplus specifies a very short range (250m/820’) rate of 300Mbps download and 100Mbps upload

Fiber to the Premises (FTTP) and Optical Network Terminals

- FTTP Internet connection means the ISP’s fiber-optic cable is run all the way to the customer’s building, connecting to an NID (Network Interface Device).
- Implemented as a passive optical network (PON) where a single fiber cable is run from an optical line terminal (OLT) to a splitter.
- An optical network terminal (ONT) directs each subscriber’s traffic by converting the optical signal to an electrical one.

6.1.7 - Fixed Wireless Internet Access

Geostationary Orbital Satellite Internet Access

- Satellite-based microwave radio systems that provide massive areas of coverage.
- Transfer rates vary, 2-6Mbps up and 30Mbps down is typical
- Increased latency. E.g., where a DSL file involves 10-20ms round trip time (RTT), over satellite could take 600-800ms RTT delay.
- Interface involves ISP installing a very small aperture terminal (VSAT) satellite dish antenna and setting the proper alignment, South for North America.

Low Earth Orbital Satellite Internet Access (LEO)

- An array of satellites, LEO setups provide better bandwidth (5-220Mbps) and have lower latency (25-60ms RTT).

- Dish technology uses “phased array” to connect to different satellites as they pass overhead, as mechanical realignment is often required.
- New models feature a flat panel antenna that doesn’t require a motor.

Wireless Internet Service Providers (WISP) utilize ground-based, long-range, fixed-access wireless technology.
- May use Wi-Fi type networking or proprietary equipment and licensed or unlicensed frequency bands.
- Low latency, but struggles with obstructed line of sight between antennas.
- Risks of interference

6.1.8 - Cellular Radio Internet Connections

3G - Cellular radio that makes a connection to the closest base station. The area served by a base station is called a “cell”.
- Cells have an effective range up to 5 miles, though signal struggles through building materials.
- 3G cellular radio typically works in the 850 and 1,900MHz frequency bands (America) and the 900 and 1,800MHz bands everywhere else.
- Global system for mobile communication-based phones (GSM) subscribers utilize a removable subscriber identity module (SIM) card to unlock a handset with their provider.
- Code division multiple access (CDMA) handsets are directly managed by the provider, no SIM card.
- G, E, and 1x represent minimal service levels, with connections speeds of 50-400Kbps
- 3G → Universal Mobile Telecommunications Service (UMTS) on GSM handsets or Evolution-Data Optimized (EV-DO) on CDMA networks, up to 3Mbps.
- H/H+ → High Speed Packet Access (HSPA) provides improved data rates on GSM networks, can reach up to 42Mbps

4G - Long Term Evolution (LTE) is a series of converged 4G standards supported by both GSM and CDMA network providers. REQUIRES SIM card issued by network provider. Typically operates between 600 and 2500MHz frequency bands in the Americas, and 700 and 2600MHz everywhere else.

5G - Utilizes different spectrum bands, from low (6GHz) to medium/high (20-60GHz).
- Low bands have greater range and penetrating power
- High bands, referred to as millimeter wave (mmWave), require close range (a few hundred feet) and cannot penetrate walls or windows.
- 5G involves many small antennas to form an array, uses multipath and beamforming to overcome the propagation limitations of the spectrum; referred to as massive multiple input multiple output (mMIMO).

6.1.9 - Routers

– – null – –

6.1.10 - Firewalls

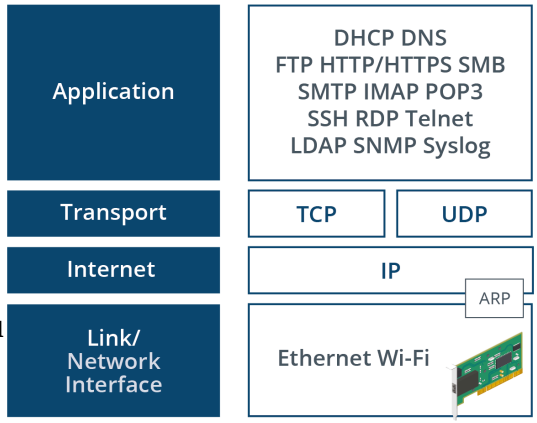
Technology used to filter allowed and denied hosts and protocols on a network.
- Access Control List (ACL) a network’s configured rules.
    - Each entry lists source and/or destination network addresses and protocol types, and whether to allow or block traffic that matches the rule.
- Most routers can implement some level of firewall functionality.

6.2 TCP/IP Concepts

6.2.1-5 - TCP/IP (and the 3 Network Interface Layers)

Transmission Control Protocol/Internet Protocol
*Establishes a 3-way handshake and ensures reliable data delivery

The items in the blue column are the top layer, or "protocols"; the items adjacent are the lower layers.



Application: Allows user-facing software to communicate over the network by providing a direct interface for users to interact with the network via services like email etc.

DHCP for network setup, **DNS** for domain resolution, **HTTP** for web.

Transport: Ensures reliable communication by managing the flow of data between applications on different devices and providing error-checking mechanisms.

TCP guarantees connection-oriented forwarding of packets.

- Can identify and recover from lost or out-of-order packets

UDP (User Datagram Protocol) provides unreliable connectionless forwarding

- Faster because it doesn't vet connections.
- Ideal for time-sensitive applications, such as speech or video

Internet: Responsible for addressing and routing data packets between devices on different networks. Uses the IP to uniquely identify senders and recipients.

IP addressing, handled by the **Address Resolution Protocol (ARP)**
Allows a host to query which MAC address associated with IP address

Data Link: Deals with the physical connection. Includes devices such as switches, bridges, and NICs, and focuses on converting data into signals suitable for transmission. Local communications only.

Network Interface: Responsible for putting frames onto the physical network.

6.2.6- - IPv4 Addressing

Check out this AMAZING VIDEO!! https://www.youtube.com/watch?v=5WfiTHiU4x8&t=102s

1. An IPv4 address is 32 bits long, can be arranged into four groups of eight bits (one byte) known as "octets."
2. To make IP addresses easier to use, they are used in dotted decimal notation, which requires each octet to be converted to a decimal value, each separated using a period. Called "Dotted Decimal Notation"

11000000		10101000		00000000		00000001
192	.	168	.	0	.	1

3. IPv4 addresses can have any value between 0.0.0.0 and 255.255.255.255, with some few exceptions, and provide 2 pieces of information encoded in the same value
   a. The network number (network ID) is common to all hosts on the same IP network.
   b. The host number (host ID) identifies a host within a particular IP network.

6.2.9 - IPv4 Forwarding

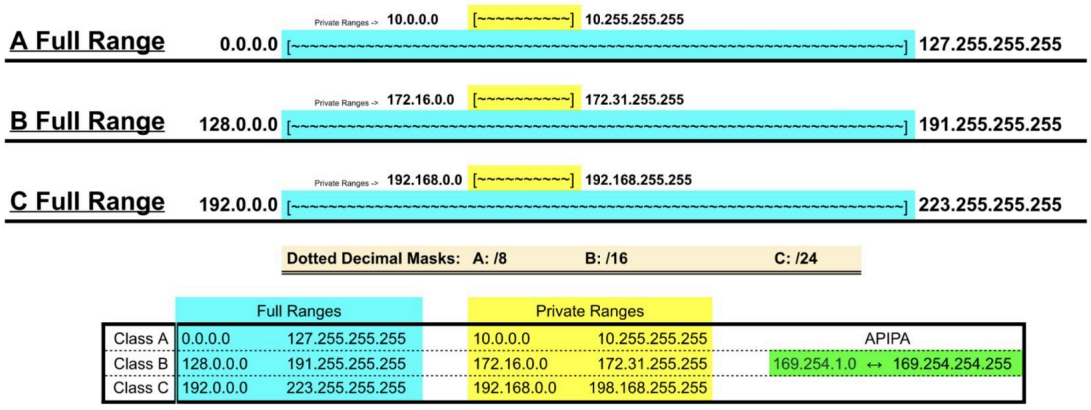
– – null – –

6.2.10 - Public and Private Addressing

Private Address Ranges

The IPv4 address scheme defines certain ranges as reserved for private addressing, often called “RFC 1918”. Hosts with IP addresses from these ranges are not allowed to route traffic over the public internet. Use of the addresses is confined to private LANs.

- 10.0.0.0 to 10.255.255.255 (Class A private address range). Entire Range: 0.0.0.0 → 127.255.255.255
- 172.16.0.0 to 172.31.255.255 (Class B private address range). Entire Range: 128.0.0.0 → 191.255.255.255
- 192.168.0.0 to 192.168.255.255 (Class C private address range). Entire Range: 192.0.0.0 → 223.255.255.255



	Full Ranges		Private Ranges		
Class A	0.0.0.0	127.255.255.255	10.0.0.0	10.255.255.255	APIPA
Class B	128.0.0.0	191.255.255.255	172.16.0.0	172.31.255.255	169.254.1.0 ↔ 169.254.254.255
Class C	192.0.0.0	223.255.255.255	192.168.0.0	198.168.255.255	

- 32-bit
- Dotted Decimal Mask: Class A: /8 Class B: /16 Class C: /24

Internet access can be facilitated for hosts using a private addressing scheme in two ways:

- Through a router configured with a single or block of valid public address, use the network address translation (NAT) to convert between private and public addresses.
- Through a proxy server that fulfills requests for internet resources on behalf of clients.

IPv6 Notation

- No Submasks!
- 8 octets, 4 on the left are Network ID, 4 on the right are Host ID. 64-bit:64-bit (128-bit)
- 0 in front of octet digits is removable; an entire octet of 0s can be removed. A single 0 must placehold host ID octet.
- Double Colons can be used once, to remove a double-octet of 0s. For a second set of 0s, reduce to a single 0 per octet.
    - 2001:0db8:0000:0000:0abc:0000:def0:1234
    - 2001:db8::abc:0:def0:1234

6.2.11 - IPv4 Host Address Configuration

– – null – –

6.2.12 - Static vs Dynamic host configuration Protocol (DHCP)

- Static addresses are typically assigned to systems with dedicated functionality, like router interfaces.
- DHCP is a service that will assign IP, subnet mask, default gateway and DNS server address.
- Microsoft’s Automatic Private IP Addressing (ipconfA) works as a failover mechanism when IP configuration fails.

6.2.15 IPv6 Addressing

Global and Link-Local addressing

- In hex notation, a global address starts with a 2 or 3

- Link-local addresses are used on the local segment to communicate with neighbor hosts. In hex notation, link-local addresses start with fe80:

6.3 - Network Communications

6.3.1 - Protocols and Ports

A Connection-oriented protocol is used by TCP to mitigate lack of reliability over IP through the following functions:

- Establishes a connection between the sender and the recipient using a three-way handshake sequence of SYN, SYN/ACK, and ACK packets.
- Assigns each packet a sequence number so that it can be tracked.
- Allows the receiver to acknowledge (ACK) that a packet has been received.
- Allows the receiver to send a negative acknowledgement (NACK) to force retransmission of a missing or damaged packet.
- Allows the graceful termination of a session using a FIN handshake.
- Main drawback is that this connection information requires multiple header fields.

6.3.2 - Transmission Control Protocol

TCP is used when the application protocol cannot tolerate missing or damaged information. The following application protocols must use TCP:

- Hyper Text Transfer protocol Secure (HTTPS): This protocol is used to deliver web pages and other resources. The secure version uses encryption to authenticate the server and protect the information that is being transmitted. A single missing packet would cause this process to fail completely.
- Secure Shell (SSH): This protocol is used to access the common-line interface of a computer from across the network. It uses encryption to authenticate the server and user and protect the information that is being transmitted. This process would also fail if a data packet is not received.

6.3.4 - User Datagram Protocol

A User Datagram Protocol (UDP) is a connectionless, non-guaranteed method of communication with no sequencing or acknowledgments. There is no guarantee regarding the delivery of messages or the sequence in which packets are received.

- Ideal for voice or video. Delivery is fast.
- If necessary, the application layer can be used to control delivery reliability.
- Dynamic Host Configuration Protocol (DHCP): Used by clients to request IP configuration information from a server. It uses broadcast transmissions, which are not supported by TCP, so it must use UDP. A simple protocol where a process can be restarted repeatedly until timing out.
- Trivial File Transfer Protocol (TFTP): Typically used by network devices to obtain a configuration file. The application protocol uses its own acknowledgment messaging, so it does not require TCP.

6.3.6 - Well-Known Ports

Server port numbers are assigned by the **Internet Assigned Numbers Authority (IANA)**. Here are some common ones:

Port#	TCP/UDP	Protocol	Purpose
20	TCP	File Transfer Protocol (FTP)—Data connection	Make files available for download across a network (data connection port)
21	TCP	File Transfer Protocol (FTP)—Control connection	Make files available for download across a network (control connection port)
22	TCP	Secure Shell (SSH)	Make a secure connection to the command-line interface of a server
23	TCP	Telnet	Make an unsecure connection to the command-line interface of a server
25	TCP	Simple Mail Transfer Protocol (SMTP)	Transfer email messages across a network
53	TCP/UDP	Domain Name System (DNS)	Facilitate identification of hosts by name alongside IP addressing
67	UDP	Dynamic Host Configuration Protocol (DHCP) Server	Provision an IP address configuration to clients
68	UDP	DHCP Client	Request a dynamic IP address configuration from a server
80	TCP	HyperText Transfer Protocol (HTTP)	Provision unsecure websites and web services
110	TCP	Post Office Protocol (POP)	Retrieve email messages from a server mailbox
137-139	UDP/TCP	NetBIOS over TCP/IP	Support networking features of legacy Windows versions
143	TCP	Internet Mail Access Protocol (IMAP)	Read and manage mail messages on a server mailbox
389	TCP	Lightweight Directory Access Protocol (LDAP)	Query information about network users and resources
443	TCP	HTTP Secure (HTTPS)	Provision secure websites and services
445	TCP	Server Message Block (SMB)	Implement Windows-compatible file and printer sharing services on a local network (also sometimes referred to as Common Internet File System [CIFS])
3389	TCP	Remote Desktop Protocol (RDP)	Make a secure connection to the graphical desktop of a computer

Email Ports

SMTP	25, 587
Simple Mail Transfer Protocol	
POP3	110, 995
Post Office Protocol v.3	
IMAP	143, 993
Internet Message Access Protocol	

File Transfer Ports

FTP	20, 21
File Transfer Protocol	
SMB	445
Server Messenger Block	
NetBIOS	137-139
Network Basic Input/Output System	

Remote Connections

RDP	3389
Remote Desktop Protocol	
SSH	22
Secure Shell	
Telnet	23
Don't use this unless necessary	

Networking Ports

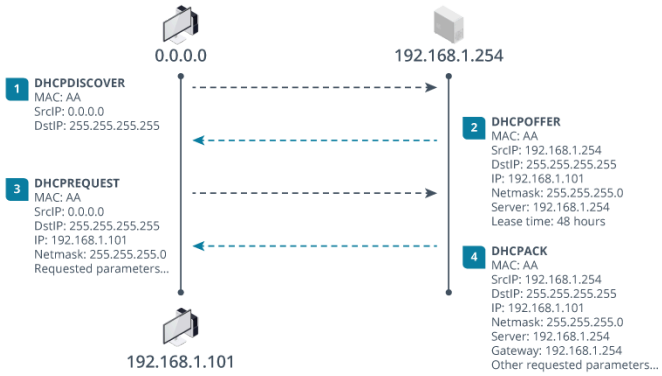
DHCP	67, 68
Dynamic Host Configuration Protocol	
DNS	53
Domain Name System	
LDAP	389
Lightweight Directory Access Protocol	
SNMP	161, 162
Simple Network Management Protocol	
HTTP	80
Hyper Text Transfer Protocol	
HTTPS	443 (TLS)
Hyper Text Transfer Protocol Secure	
NTP	123
Network Time Protocol	

6.4 - Network Configuration Concepts

6.4.1 - Dynamic Host Configuration Protocol (DHCP) Functions

DHCP Scope is the range of IP addresses that a DHCP server can offer to client hosts in a particular subnet. The scope should exclude any addresses that have been configured statically.

DHCP Leases: A host is configured to use DHCP by specifying in its TCP/IP configuration that it should automatically obtain an IP address. When a DHCP client initializes, it broadcasts a DHCPDISCOVER packet to find a DHCP server. All communications are sent using UDP, with the server listening on port 67 and the client on port 68



DHCP server responds to the client with a DHCPOFFER packet, containing the address and other configuration information, like default gateway and DNS server addresses.
The client may choose to accept the offer using DHCPREQUEST
packet.

The next server response should be with a DHCPACK packet.
The client broadcasts an ARP message to check that the address is unused. If yes: Uses the address and option. If no: declines the address and requests a new one.

DORA!!!

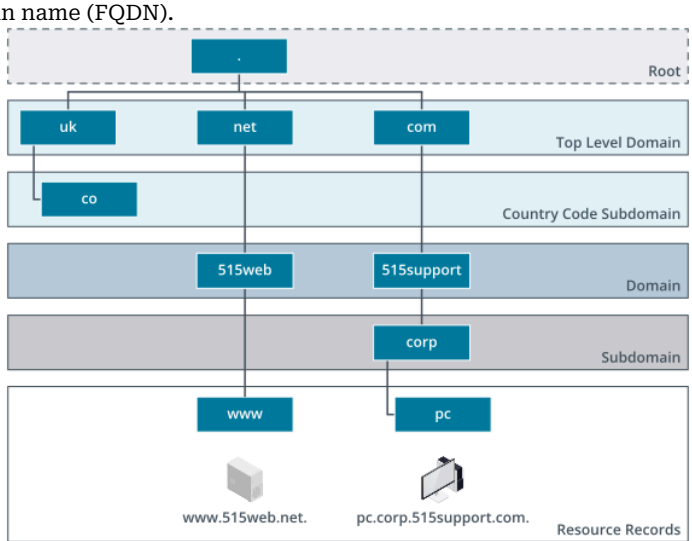
IP addresses are leased by the server for a limited period only. A client can attempt to renew or rebind the DHCP Lease before it expires. If the lease cannot be renewed, the client must release the IP address and start the discovery process again.

DHCP Reservations: Alternative to static addressing, the DHCP server is configured with a list of the MAC addresses of hosts that should receive the same IP address each time they join the network. When it is contacted by a host with one of the listed MAC addresses, it issues a lease for the reserved IP address to the system.

6.4.2 - Domain Name System (DNS)

A global hierarchy of distributed name server databases that contain information about each domain and the hosts within those domains. A "friendly" host name is also typically assigned to each host, which is configured when the OS is installed. Operated by ICANN (icann.org), also manages the generic TLDs. Country codes are generally managed by an organization appointed by the relevant government. *It must be unique on the local network

- To avoid the possibility of duplicate host names on the internet, the host name can be combined with a domain name and suffix; called a fully-qualified domain name (FQDN).
- FQDNs are assigned and managed using DNS



fully-qualified domain name (FQDN) Example below:

```
          domain suffix
      ___|___
      |      |
nut.widget.example
↓     |      |
host name    |
       |     ↓
```

↓ top-level domain
domain name ↱

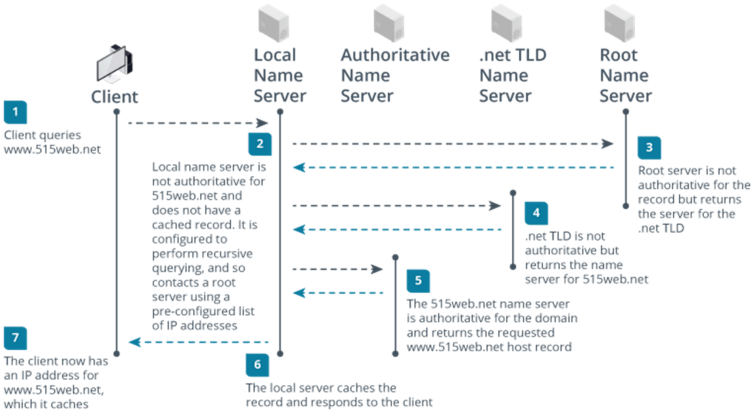
Check: pc.corp.515support.com.

DNS Hierarchy: At the top of a DNS hierarchy is the root, which is represented by the null label (.)

- 13 root-level servers (A to M).
  - Below the root are TLDs
    - Generic TLDS: .com, .org, .net, .info, .biz
    - Sponsored TLDs: .gov, .edu
    - Country Code: .uk, .ca, .de

6.4.3 - DNS Queries

Resolves a host name or FQDN to an IP address, a "stub resolver" checks its local cache for the mapping. If no mapping is found, it forwards the query to its local DNS server. *The client communicates with a DNS server over port 53. The resolution process takes place as demonstrated in the diagram here ⟶



6.4.3 - DNS Record Types

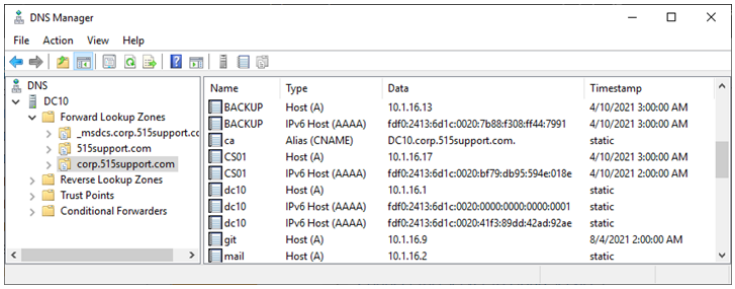
At least one DNS server needs to be configured to act as an authoritative store of information about each domain. The DNS server responsible for managing a zone will contain numerous resource records, which in turn, allow the name server to resolve queries for names and services hosted in the domain into IP addresses. These resources can be generated and updated manually (statically), or they can be generated dynamically from information received from client and server computers on the network.

An address (A) record is used to resolve a host name to an IPv4 address. AAAA records resolves a host name to an IPv6 address

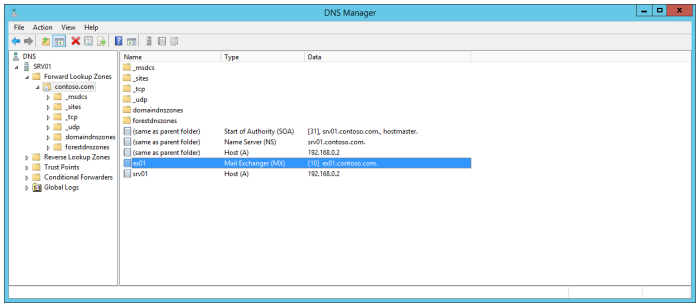
6.4.5 - DNS Spam Management Records

CNAME Records: A canonical name record is used to link one domain name to another. Example:

1. Company A acquires Company B
2. Instead of maintaining two websites, Company A makes a CNAME record entry
   a. Links www.companyA.com to www.companyB.com
3. Users who visit www.companyB.com will be redirected to www.companyA.com



Mail Exchanger (MX) Resource Records: Used to identify an email server for the domain so that other servers can send messages to it. In a typical network, multiple servers are installed to provide redundancy, and each one will be represented by an MX-record. Each MX record is given a preference value, with the lowest numbered entry preferred. The host name identified in an MX record must have an associated A or AAAA record.



DNS MX Record in Microsoft DNS Manager

6.4.5 - DNS Spam Management Records

A TXT-record is used to store any free-form text that may be needed to support other network services. A single domain name may have many TXT records, but they are most commonly used to verify email services and block the transmission of spoofed and unwanted messages, referred to as spam.

Sender Policy Framework (SPF) uses a TXT resource record published via DNS by an organization/s hosting email service. The SPF record identifies the hosts authorized to send email from that domain. An SPF can also indicate what to do with mail from servers not on the list, such as rejecting them (-all), flagging them (~all) or accepting them (+all).

DomainKeys Identified Mail (DKIM) utilizes cryptography to validate the source server for a given email message. This can replace or supplement SPF.

- To configure DKIM, the organization uploads a public encryption key as a TXT record in the DNS server
- Organizations receiving messages can use this key to verify that a message derives from an authentic server

Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
A framework that ensures that SPF and DKIM are being utilized effectively.

- A DMARC policy is published as a DNS TXT record.
- A DMARC can use SPF or DKIM or both.
- DMARC specifies a more robust policy mechanism for senders to specify how DMARC authentication failures should be treated (flag, quarantine, or reject) PLUS mechanisms for recipients to report DMARC authentication failures to the sender

6.4.6 - Virtual LANs

All hosts connected to the same unmanaged switch are said to be in the same broadcast domain. Placing hundreds or thousands of hosts in the same broadcast domain reduces performance. To mitigate this, the ports can be divided into groups using a feature of managed switches called VLAN. This method increases both performance and sometimes security too. *The VLAN with ID 1 is referred to as the “default VLAN”; unless configured differently, all ports on a managed switch default to being in VLAN 1

The simplest means of assigning a node to a VLAN is by configuring the port interface on the switch with a VLAN ID in the range of 2 to 4094. For example:

- Switch ports 5 - 8 could be configured as a VLAN with ID 100
- Switch ports 9-12 could be assigned to VLAN 200
- Host A connected to port 2 would be in VLAN 100
- Host B connected to port 12 would be in VLAN 200

Cumulus VX switch output showing
switch ports swp 5-8 configured in VLAN 100 and ports 9-12 in VLAN 200 ↴

```
interface swp5
  bridge-access 100

interface swp6
  bridge-access 100

interface swp7
  bridge-access 100

interface swp8
  bridge-access 100

interface swp9
  bridge-access 200

interface swp10
  bridge-access 200

interface swp11
  bridge-access 200

interface swp12
  bridge-access 200

interface bridge
  bridge-ports swp5 swp6 swp7 swp8 swp9 swp10 swp11 swp12
  bridge-vids 10 100 200
  bridge-vlan-aware yes
```

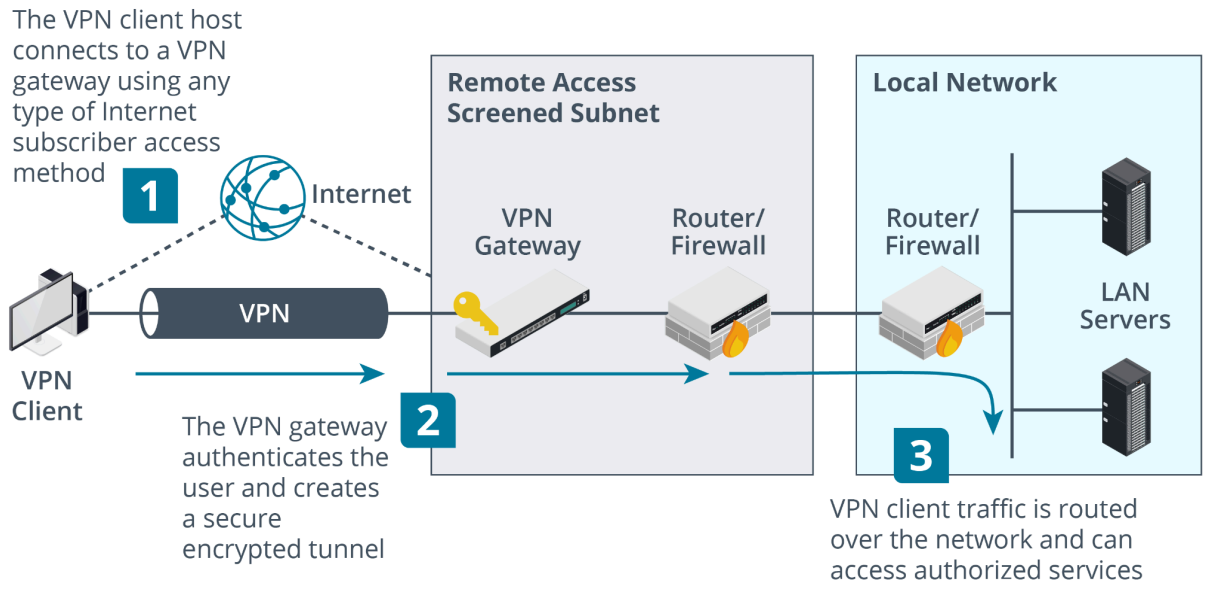
- When hosts are placed in separate VLANs, they can no longer communicate with one another directly, regardless of switch placement.
- Each VLAN must also be configured with its own subnet address and IP address range as well.
- Communications between VLANs must go through an IP router.
- Each VLAN must also be provisioned with its own DHCP and DNS services.
- Each VLAN can represent a separate zone.
- Traffic passing between VLANs can easily be filtered and monitored to ensure it meets security policies.

- VLANs are also used to separate nodes based on traffic type, such as isolating devices used for voice traffic so that they may be prioritized over data.

6.4.7 - Virtual Private Networks (VPN)

VPNs enable hosts to connect to the LAN without being physically installed at the site. Rather than attach to a switch or AP, the host connects to the local network via a remote access server that accepts connections from the internet.

A secure VPN configures a protected tunnel through the internet using special connection protocols and encryption technology. Once the connection has been established, the remote computer becomes part of the local network, albeit restricted to the bandwidth available over the physical connection.



Chapter 7

Notes from Chapter 7: Supporting Network Services

7.1 - Networked Host Services

7.1.1 - File/Print Services

File Share is known as the process where resources, such as printers and/or disc drives, are shared over a network; the machine hosting the disk or printer is the "server".

- A file server can be implemented using TCP/IP protocols, such as File Transfer Protocol (FTP).

Server Messenger Block (SMB): an application protocol underpinning file and printer sharing on Windows networks.

- Usually runs directly over TCP/445 port.
- Sometimes referred to as Common Internet Files System (CIFS).
- SMB3 is the current version.
- SMB1 is disabled by default on current Windows versions.

Network Basic Input/Output System (NetBIOS)

- Window's original version of TCP/IP
- Obsolete, and should be disabled on most networks due to high security risks
- Only used for file sharing with Windows version earlier than Windows 2000
- Utilizes UDP/TCP 137/138/139

File Transfer Protocol (FTP): Allows a client to upload and download files from a network server.

- Often used to upload files to websites.
- Utilizes TCP/21 to establish and maintain a connection
- Utilizes TCP/20 to transfer data in "active" mode or a server-assigned port in "passive" mode.

7.1.2 - Database Servers

Provides a method to store large amounts of structured and unstructured data.

- Relational databases link different data points together based on their relationships to each other.
    - Uses Structured Query Language (SQL) to interact with the database, storing data in rows and columns.
    - Examples include Oracle, MySQL, and MariaDB
- Non-relational databases store data in a flexible manner using graphs, documents, or key-value pairs.
    - Best used for large amounts of data.
    - Examples include MongoDB, CouchDB, and Amazon SimpleDB

7.1.3 - Web Servers

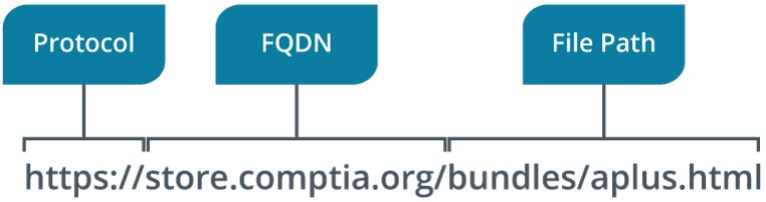
Provide client access via HTTP or its secure version, HTTPS.

- Utilizes TCP/80 by default (HTTP)
- Sends a request for resource (GET)
- The server either returns the requested data or responds with an error code.
- Usually used to serve HTML web pages.
- Features mechanism where a user can submit data from the client to the server (POST)

Uniform Resource Locators (URL)

- A URL contains all the information necessary to identify and access an item:
    - The protocol describes the access method or service type being used.
    - The host location is usually represented by a FQDN, which is not case-sensitive.
    - The host location can also be an IP address; an IPv6 address must be enclosed in square brackets.
    - The file path specifies the directory and file name location of the resource (if required).
    - The file path may or may not be case-sensitive, depending on how the server is configures.

Web Server Deployment



- Typically, an organization will lease a web server or space on a server from an ISP
- Larger organizations with Internet-connected datacenters may host websites themselves.
- Private networks using web technologies known as “intranets” if they permit only local access.
- “Extranets” if they permit remote access.

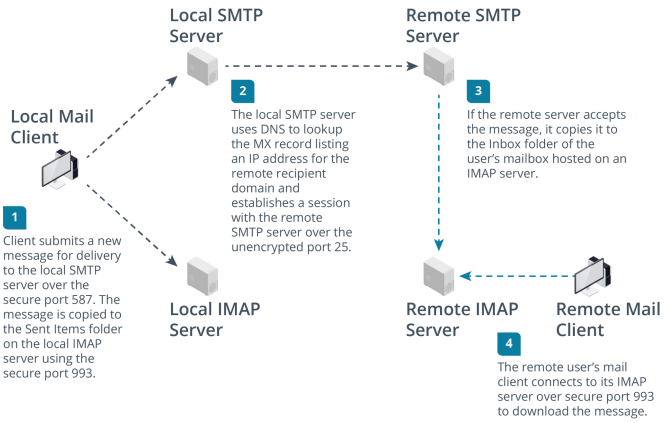
7.1.4 - Hypertext Transfer Protocol Secure (HTTPS)

- Secure Socket Layer (SSL) developed by Netscape in the 1990s to mitigate HTTP security issues.
- Transport Layer Security (TSL) developed from SSL and ratified as a standard by the IETF (Internet Engineering Task Force).
- HTTPS uses TLS, and utilizes TCP/443 (by default).
- TLS can also be used to secure other TCP application protocols, such as FTP, POP3/IMAP, SMTOP and LDAP.
- Digital certificates are issued by a trusted certificate authority (CA)
    - Uses public/private encryption key pair:
    - Private key is kept a secret known only to the server
    - Public key is given to clients via the digital certificate.
- A secure session uses URL starting with “https://” and has a padlock icon in the address bar.

7.1.5 - Mail Servers

Electronic mail enables a person to compose a message and send it to another user on their own network (intranet) or anywhere in the world via the internet.

- Mail transfer and mailbox access protocols are the two main mail servers.



Internet email addresses follow the mailto URL scheme. An internet email address comprises two parts:

- Username (local part)
- Domain name, separated by @ symbol
    - Domain name may refer to a company or an ISP
- TCP/25 used for message relay between SMTP servers, known as message transfer agents (MTAs).
- TCP/587 used by mail clients, called message submission agents (MSAs) to submit messages for delivery by an SMTP server.
    - TCP/587 servers should use encryption and authentication to protect the service.

SMTP specifies how email is delivered from one mail domain to another. The SMTP servers for the domain are registered in DNS using Mail Exchange (MX) and host (A/AAAA) records.

– – Continued – –

7.1.6 - Mailbox Servers

can by separate machines or a separate process running on the same computer. A mailbox access protocol allows the user's client email software to retrieve messages from the mailbox.

Post Office Protocol 3 (POP3) is an early example of a mailbox access protocol. Current version is 3.

- Utilizes TCP/110 to establish an unsecure connection
- Utilizes TCP/995 to establish a secure connection
- When the user is authenticated, the contents of the mailbox are downloaded for processing on the local PC.
- In POP3, messages are typically deleted from the mailbox server when they are downloaded
    - Some clients have the option to leave messages on the server.

Internet Message Access Protocol (IMAP)

- IMAP is a mail retrieval protocol.
- Supports permanent connections to a server and connects multiple clients to the same mailbox simultaneously.
- Allows a client to manage the mailbox on the server and to create multiple mailboxes.
- Utilizes TCP/143 for insecure connection.
- Utilizes TCP/993 (default IMAPS[IMAP-Secure])\

7.1.8 - Directory and Authentication Servers

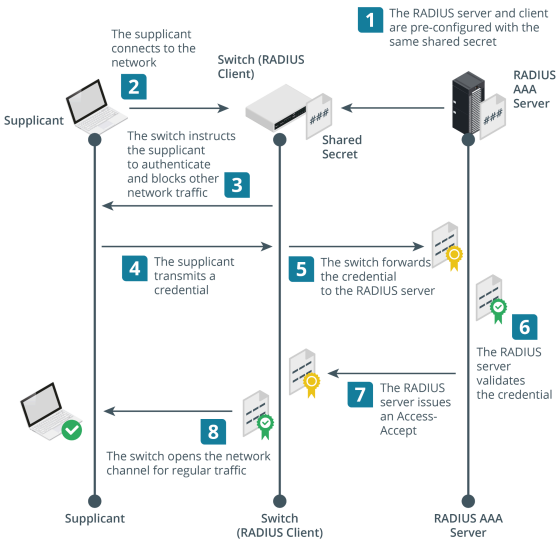
Single Sign-on (SSO): Utilizing a centralized database of user accounts, a user can authenticate once to access the network and gain authorization for all the compatible application servers running on it.

A directory is a type of database, where an object is like a record and things that you know about the object (attributes) are like fields.

- Most directories are based on the X.500 standard.
- The Lightweight Directory Access Protocol (LDAP) is a TCP/IP protocol used to query and update an X.500 directory.
    - Utilizes TCP/UDP port 389 (default)
    - Utilizes TCP/636 for TLS secure version: LDAPS

Authentication, Authorization, and Accounting (AAA): Consolidates authentication services across multiple access devices.

- Supplicant - The device requesting access, such as the user's PC or laptop.
- Network Access Server (NAS) or network access point (NAP) - Network access appliances, such as switches, access points, and VPN gateways; referred to as "AAA clients" or "authenticators"
- AAA server - The authentication server, positioned within the local network.



With AAA, the network access appliances do not have to store any authentication credentials.

- Often implemented using protocol Remote Authentication Dial In user Service (RADIUS)
    - TCP/UDP 1812/1812
    - Commonly used to authenticate users to a network
- Or as Terminal Access Controller Access Control System Plus (TACAS+)
    - TCP/49
    - Commonly used to authenticate devices such as routers and switches

7.1.9 - Remote Terminal Access Servers

These allow a host to accept connections to its command shell or graphical desktop from across the network.

- A teletype (TTY) device is the terminal or endpoint for communication between the computer and the user.
    - It handles text input and output between the user and the shell, or command environment.
- The shell performs the actual processing.
- A terminal emulator is any kind of software that replicates this TTY input/output function
    - A terminal emulator application might support connections to multiple types of shells.
    - Allows you to connect to the shell of a different host over the network.

Secure Shell (SSH) is the principal means of obtaining secure remote access to UNIX and Linux servers, and to most types of network appliances (switches, routers, and firewalls).

- Offers encrypted terminal emulation.
- Can be used for SFTP and to achieve many other network configurations.
- Most widely used: OpenSSH (openssh.com)
- Listens on TCP/22 by default.

Telnet: Both a protocol and a terminal emulation software tool that transmits shell commands and output between a client and the remote host.

- While the interface can be password protected, the password and other communications are not encrypted
    - Vulnerable to packet sniffing and replay.
- Listens on TCP/23 by default.
- Recommended that only secure access methods like SSH be used to configure switches and routers now.

Remote Desktop Protocol (RDP): Microsoft's protocol for operating remote GUI connections to a Windows machine.

- Utilizes TCP/3389
- Available for other OSs, like Linux, MacOS, iOS, and Android.
- Check out open-source RDP server products, such as xrdp (xrdp.org)

7.1.10 - Time Servers

Network Time Protocol (NTP) allows networked systems to sync their clocks to a common source.

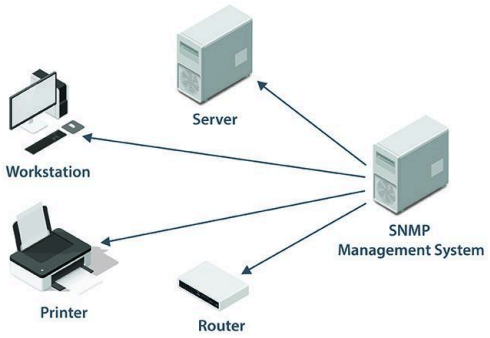
- Ensures network log entries have accurate time stamps for events.
- Some communication protocols rely on an accurate clock to control the transmission of data across the network.
- The *MOST ACCURATE* clock source would be an atomic clock, considered Stratum-0.
    - NTP servers that sync their clocks to this source would be Stratum-1 level of accuracy
    - NTP servers that sync their clocks to a Stratum-1 are considered Stratum-2 degree of accuracy
- NTP servers operate on UDP/123
- Network Time Security (NTS) was approved in 2020 and uses TLS encryption
    - Utilizes TCP/4460

– – Continued – –

7.1.11 - Network Monitoring Servers

Simple Network Management Protocol (SNMP): a framework for management and monitoring network devices.

- Utilizes UDP/162
- Has 3 versions, v1 and v2 have security issues
- Consists of 3 components:
    - Network management system
    - Managed devices
    - Agents



Agent: A process running on a switch, router, server, or other SNMP-compatible network device.

- Maintains a database called a management information base (MIB) that holds statistics relating to the activity of the device.
- Capable of initiating a trap operation where it informs the network management system of a notable event (like a port failure)

Network management system: Monitors all agents by polling them at regular intervals for information from their MIBs and displays the information for review. It also displays any trap operations as alerts for the network administrator to assess and act upon as necessary.

Syslog: A log collector that aggregates event messages from numerous devices to a single storage location; can be configured to run one or more status and alerting dashboards.

- Ef facto standard for logging events from distributed systems
- Comprises a PRI code, a header containing a timestamp and host name, and a message part.
    - PRI code is calculated from the facility and the severity level
    - The message part contains a tag showing the source process plus content
- Listens on port UDP/514

7.2 - Internet and Embedded Appliances

7.2.1 Proxy Servers

On a SOHO network, devices on the LAN access the internet via the ROUTER using a type of network address translation (NAT), either port-based or overloaded NAT.

- Port-based NAT translates between the private IP address used on the LAN and the publicly addressable IP configured on the router/s WAN interface.
- Overloaded NAT, also known as PAT, is where a single IP address is shared amongst several nodes, and they are differentiated by the port number for each connection.

Proxy Servers:

- A proxy can perform a security function by acting as a content filter to block access to sites deemed inappropriate
- It can apply rules to access requests, such as restricting overall time limits or imposing time-of-day restrictions.
- Manages and filters outgoing access requests
- Can be configured to cache content to improve performance and reduce bandwidth consumption.
- Does not just translate IP addresses
    1. It takes a whole HTTP request from a client, checks it, and then forwards it to the destination server on the internet.
    2. When the reply comes back, it checks it and then shuttles it back to the LAN computer
- Can be used for other types of traffic too, such as email.

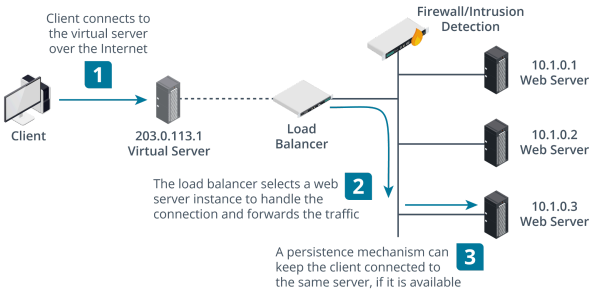
7.2.3 - Spam Gateways and Unified Threat Management

Networks connected to the internet need to be protected against malicious threats by various types of security scanners. These services can be implemented as software running on PC servers, but enterprise networks are more likely to use purpose-built internet security appliances.

- Firewalls allow or block traffic based on a network access control list specifying source and destination IP addresses and application ports.
- Intrusion detection systems (IDS) are programmed with scripts that can identify known malicious traffic patterns. An IDS can raise an alert when a match is made. An intrusion prevention system (IPS) can additionally take some action to block the source of the malicious packets.
- Antivirus/anti-malware solutions scan files being transferred over the network to detect any matches for known malware signatures in binary data.
- Spam gateways use SPF, DKIM, and DMARC to verify the authenticity of mail servers and are configured with filters that can identify spoofed, misleading, malicious, or otherwise unwanted messages. The spam gateway is installed as a network server to filter out these messages before it is delivered to the user's inbox.
- Content filters are used to block outgoing access to unauthorized websites and services.
- Data leak/loss prevention (DLP) systems scan outgoing traffic for information that is marked as confidential or personal. The DLP system can verify whether the transfer is authorized and block it if it is not.

A Unified threat management (UTM) appliance is one that enforces a variety of security policies and controls, combining the work of multiple security functions.

7.2.4 - Load Balancers



- Deployed to distribute client requests across server nodes in a farm or pool.
- Used when multiple servers are providing the same function.
    - Web servers, email servers, web conferencing, and streaming media servers.
- Placed in front of the server network and distributes requests from the client network or internet to the application servers.
- The service address is advertised to clients as a virtual server.

7.2.5 - Legacy Systems

- A system that is no longer directly supported by its vendor.
- A product that is no longer supported is referred to as end-of-life (EOL).
- It is important to isolate them as far as possible from the rest of the network and to ensure that any network channels linking them are carefully protected and monitored.

7.2.6 - Embedded Systems

An embedded system is an electronic device that is designed to perform a specific, dedicated function.

- Examples: a microcontroller in an intravenous drip-rate meter; industrial control system managing a water treatment plant.
- Typically designed for a closed system.

Workflow and Process Automation Systems

An industrial control system (ICS) provides mechanisms for workflow and process automation.

- Comprises plant devices and equipment with embedded programmable logic controllers (PLCs).
- An embedded system network is usually referred to as an operational technology network to distinguish it from an IT network.
- Output and configuration of a PLC is performed by a human-machine-interface (HMI).
    - HMI interface could be a local control panel or software on a computing host.
- PLCs are connected within a control loop, and the whole process automation system can be governed by a control server.

- A data historian stores a database of all the information generated by the control loop.

Supervisory Control and Data Acquisition (SCADA)
A SCADA system takes the place of a control server in large-scale, multiple site ICSs.
- Typically uses WAN to connect the SCADA server to field devices.

7.2.7 - Internet of Things Devices
A term used to describe the global network of wearable technology, home appliances, home control systems, vehicles, and other items that have been equipped with sensors, software, and network connectivity.
- Hub/Control System - IoT devices usually require a communications hub to facilitate wireless networking.
    - There must also be a control system; IoTs are "headless"
    - Often implemented as a smart speaker operated by voice control or use of a smartphone/PC app for configuration.
- Smart Device - IoT endpoints implement the function, such as a smart lightbulb, refrigerator, thermostat/heating control, or doorbell/video entry phone that you can operate and monitor remotely.
    - Potentially vulnerable to malicious code.
    - Most use Linux or Android kernel.
    - Integrated peripherals, such as cameras or microphones, could be compromised to facilitate surveillance.

7.3 - Troubleshoot Networks

7.3.1 - Troubleshoot Wired Connectivity
A client-wired connectivity issue means that either the network adapter does not establish a network link at all (no connectivity) or the connection is unstable or intermittent. Assuming that you can establish that the problem affects a single host only, you need to isolate the precise location of the physical issue.

Troubleshoot Cable and Network Adapter issues.
A typical ethernet link for an office workstation includes the following components:
- NIC port on the host
- RJ45 terminated patch cord between the host and a wall port
- Structured cable between the wall port and a patch panel, terminated to insulation displacement connector (IDC) blocks (the permanent link).
- RJ45 terminated patch cord between the patch panel port and a switch port
- Network transceiver in the switch port.

1. In resolving a no or intermittent connectivity issue, check that the patch cords are properly terminated and connected to the network ports.
    a. If you suspect a fault, substitute the patch cord with a known good cable, and test.
2. If not the patch cord, test the transceivers. Use a loopback tool to test for a bad port.
3. If no loopback tool is available, substitute known working hosts (ideally swap ports at the switch).
    a. Kind of a dangerous security threat move.
4. If none of the above, use a cable tester to verify the structured cabling.
    a. An advanced type of cable tester is called a "certifier" and can report detailed information about the cable performance and interference.
5. If no issue still, verify the ethernet speed/duplex configuration on the switch interface and NIC.
    a. Usually set to auto-negotiate
    b. Try updating the NIC's device driver software

Intermittent connectivity might manifest as port flapping, which means that the NIC or switch interface transitions continually between up and down states. This is often caused by bad cabling, external interference, or a faulty NIC at the host end. You can use the switch configuration interface to report how long a port remains in the up state.

7.3.2 - Troubleshoot Network Speed Issues

1. If a user reports slow speed, establish exactly what network activity they are performing (web browsing, file transfer, authentication, etc..)
    a. Establish that there is a link speed problem by checking the nominal link speed and using a utility to measure transfer rate independent of specific apps or network services.
2. If you can isolate the speed issue to a single cable segment, the cabling could be affected by interference.
    a. External interference is typically caused by nearby power lines, fluorescent lighting, motors, and generators.
    b. Poorly installed cabling and connector termination can cause “crosstalk”
    c. If you have access to a network tap, the analyzer software is likely to report high numbers of damaged frames.
    d. You can also view error rates from the switch interface configuration utility.
    e. You may also need to use shielded cables to reduce interference.
3. If the cabling is not the issue, there could be a problem with the network adapter driver.
    a. Install an update if available
    b. Check whether the issue affects other hosts using the same NIC and driver version.
4. Consider the possibility that the computer could be infected with malware or have faulty software installed.
    a. Consider removing the host from the network for scanning.
    b. If you can install a different host to the same network port and that solves the issue, identify what is different about the original host.
5. Establish the scope of the problem: are network speeds an issue for a single user, for all users connected to the same switch, or for all users connecting to the internet?
    a. There may be congestion at the switch or router or some other network-wide problem

7.3.4 - Troubleshoot Wireless Issues

When troubleshooting wireless networks, you need to consider problems with the physical media, such as interference and configuration issues.

If you experience intermittent wireless connectivity, slow transfer speeds, or inability to establish a connection, then first try to move the devices closer together. If that didn’t fix it, check that the security and authentication parameters are correctly configured on both devices. (Authentication failures usually result from entering the incorrect network password or selecting the wrong security standard.

Troubleshooting Wireless Configuration Issues

- If a user is looking for a network name that is not shown in the list of available wireless networks (SSID not found), the user could be out of range or the SSID name broadcast might be suppressed.
    - In the latter scenario, the connection to the network name must be configured manually on the client.
- If an access point is not operating in compatibility mode, it will not be able to communicate with devices that only support older standards.
    - When an older device joins the network, the performance of the whole network can be affected.
    - To support 802.11b clients, an 802.11n/ac/ax are more compatible in terms of negotiating collision and avoidance.
    - Not all clients supporting 802.11n have dual-band radios, if the 5GHz band isn’t working, check whether its radio is 2.4GHz-capable only.

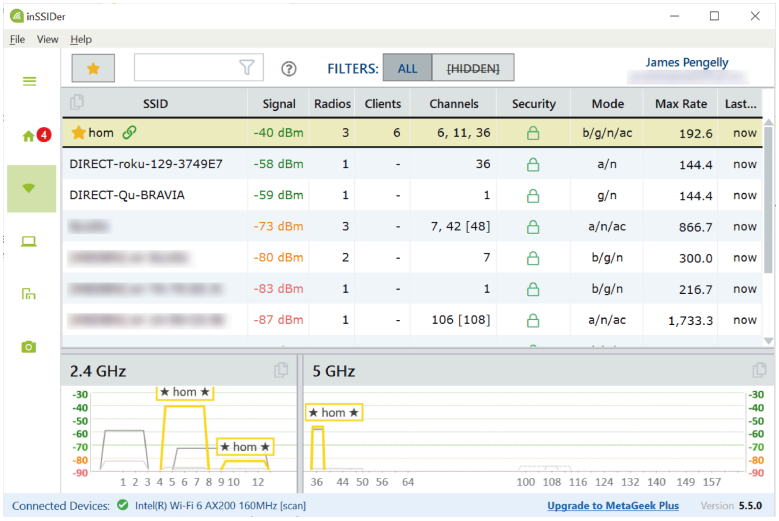
Received Signal Strength Indicator (RSSI)

- A wireless adapter will reduce the connection speed if the received signal strength indicator is not at a minimum required level. The RSSI is an index level calculated from the signal strength level.
    - Example: an 802.11n might be capable of 144Mbps, but if the signal is weak, it might reduce to a 54Mbps or 11Mbps rate to make the connection more reliable.
    - If the RSSI is too low, the adapter will drop the connection entirely and try to use a different network.

- If there are two weak networks, the adapter might “flap” between them.

Troubleshooting Wireless Signal Issues

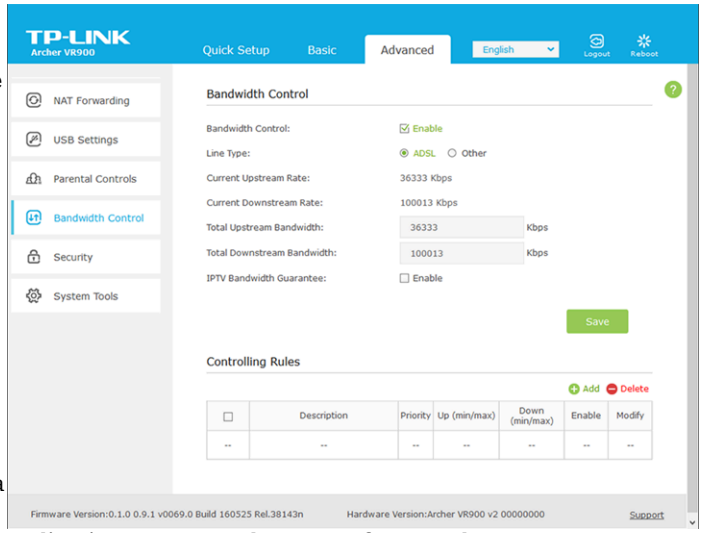
- If a device is within the supported range, but the signal is weak, or you can only get an intermittent connection, there is likely interference from another radio source broadcasting at the same frequency.
  - Try adjusting the channel that the devices use.
  - Another possibility is interference from a powerful electromagnetic source such as a motor or microwave oven.
  - The signal may be obstructed by building materials, try angling or repositioning the device or antenna to try to get better reception.



A Wi-Fi analyzer software is deigned to identify the signal strength of nearby network on each channel. It shows signal strength, measured in dBm, and expressed as a negative value, where values close to zero represent a stronger signal. The analyzer will show how many networks are utilizing each channel. Setting the network to use a less congested channel can improve performance.

7.3.5 - Troubleshoot VoIP Issues

- When using “real time” network protocols (voice and video), watch for poor VoIP service quality issues
  - Dropouts, echo, or other glitches in the call.
- Problems with the timing and sequence of packet delivery are defined as latency and jitter:
  - Latency is the time it takes for a signal to reach the recipient, measured in milliseconds (ms)
    - VoIP can support a maximum one-way latency of about 150ms. RTT is the time taken for a host to receive a response to a probe.
  - Jitter is the amount of variation in delay over time and is measured by sampling the elapsed time between packets arriving.
    - VoIP can use buffering to tolerate jitter of up to around 30ms without a severe impact on call quality.
    - Often caused by network congestion affecting packet processing on routers and switches.



- Quality of service (QoS) mechanism ensures that switches, access points, and routers are all configured to identify VoIP data and prioritize it over bursty data.
- On a SOHO network, you may be able to configure a QoS or bandwidth control feature on the router/modem to prioritize the port used by a VoIP application over any other type of protocol.
- You should be able to use the management interface to report connection latency and possibly jitter.

    - Use a speed test site to measure latency and bandwidth. If latency is persistently higher than an agreed services level, contact your ISP to resolve the issue.

7.3.6 - Troubleshoot Limited Connectivity

In Windows, a limited connectivity message specifically means that the host can establish a physical connection to the network, but has not received a lease for an IP configuration from the DHCP server. The host will be configured with an address in the automatic private IP addressing (APIPA) 169.254.x.y range. In Linux, the APIPA may set the IP address to unknown (0.0.0.0) or just leave the IP unconfigured.

- Establish the scope of the issue:
    - If the issue affects multiple users, the problem is likely to be the DHCP server itself.
    - The DHCP server could be offline, could have run out of available leases, or forwarding between the server and clients could be improperly configured.
- Check the configuration of patch cords:
    - Verify that the wall port is connected to an appropriate port on a switch via the patch panel.
- Check the VLAN configuration - If the switch port is not configured with the correct VLAN ID, it can have the same effect as connecting the host to the wrong switch port.

Windows may also report that a network adapter has no internet access, which means that the adapter has obtained an IP configuration, but cannot reach the Microsoft test site to download a test file. This error indicates that there is an issue with either internet access at the gateway router or name resolution.

- On a SOHO network, access the router management interface and verify the internet connection via a status update page.
    - If the link is down, contact your ISP

!! Chapter 8

Notes from Chapter 8: Summarizing Virtualization and Cloud Concepts

8.1 - Client-Side Virtualization

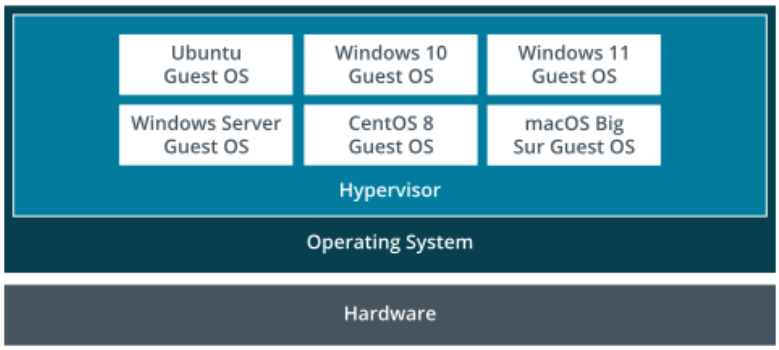
8.1.1 - Hypervisors

Software that enables virtualization; manages virtual machines (VMs), also known as guest OSs.

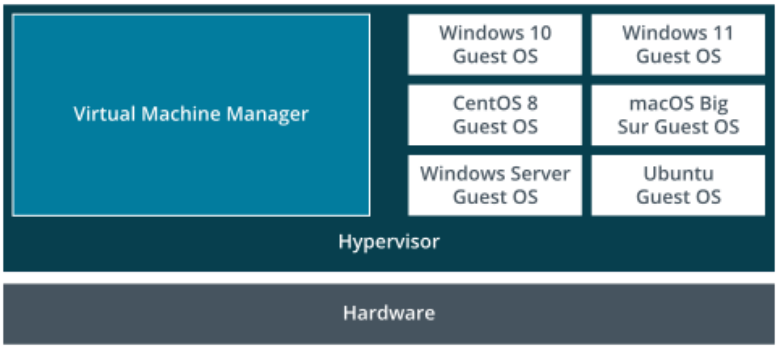
Virtualization: The ability to run multiple OSs simultaneously on one system

Two main types of hypervisors:

- Type 2 (Host-based hypervisors): Installed on top of an existing host OS. Examples include:
  - VMware Workstation, Oracle Virtual Box, and Parallels Workstation
  - Requires enough resources to run both the host OS and Guest OS



- Type 1 (Bare Metal Hypervisors): These are installed directly onto the hardware, bypassing a host OS. Examples:
  - VMware ESXi Server, Microsoft's Hyper-V, and Citrix's XEN Server
  - Needs only system requirements of the hypervisor and guest OSs



8.1.2 - Uses for Virtualization

Client-Side Virtualization: Refers to solutions designed to run on standard desktops or workstations, where each user interacts directly with the virtualization host.

- Sandboxing: Creates an isolated environment, or sandbox, to analyze malware. Containing malware within the guest OS prevents it from infecting the researcher's computer or network.
- Supporting legacy software and OSs: If host computers are upgraded, older software may not be compatible with the new OS. The old OS can be installed as a VM, allowing access to legacy software.
- Cross-platform virtualization: Test software applications under different OSs and resource constraints.

- Training: Set up lab environments for students to practice using a live OS and software without affecting the production environment. Changes to the VM can be discarded after the lab, restoring the original environment.

Server-Side Virtualization: Involves deploying a server role as a VM. Typically a hardware server may only utilize about 10% of its resources. With virtualizing, one can run 8-9 additional server instances on the same hardware without compromising performance.

Desktop Virtualization

Virtual Desktop Infrastructure (VDI) uses VMs to provision corporate desktops, replacing traditional desktop computers with low-spec thin clients. A thin client is a computer that uses a centralized server for most of its resources, instead of a drive.

When a thin client starts, it boots minimal OS, allowing the user to log on to a VM stored on the company server or cloud infrastructure. The user connects to the VM using a remote desktop protocol, such as Microsoft Remote Desktop or Citrix ICA (Independent Computing Architecture). The thin client locates the correct VM image and uses an appropriate authentication mechanism, which may involve a 1:1 mapping based on machine name or IP address or be managed by a connection broker.

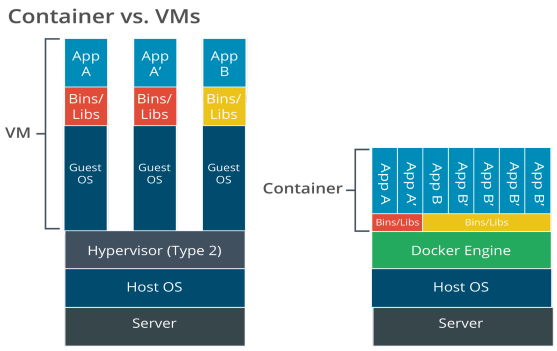
- All application processing and data storage occurs on the server.
- The VM server hosting the virtual desktop can be on-premises or in the cloud.
- Centralizing data simplifies backups, and desktop VMs are easier to support, troubleshoot, and secure.

Application Virtualization: Allows clients to access or stream applications from a server, ensuring they always run the latest version without local installation.

- Most solutions are based on Citrix Virtual Apps, while Microsoft offers App-V within its Windows Server Range, and VMware provides ThinApp.

Container Virtualization: Eliminates the need for a hypervisor by isolating resources at the OS level.

- Containers run processes through the host OS kernel, with each container allocated CPU and memory.
- Containers must run the same OS kernel (No Windows in a Linux container)
- Containers often encapsulate specific application processes, making them light-weight compared to VMs
- The most highly used VM is Docker.
- Containerization is also widely being used to implement corporate workspaces on mobile devices.



8.1.4 - Virtualization Resource Requirements

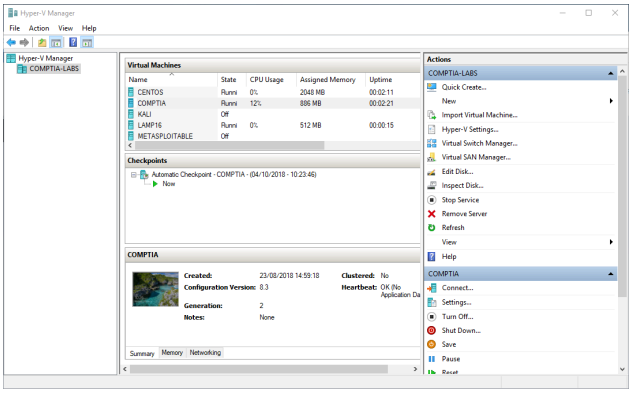
CPU and Virtualization Extensions
CPU vendors have developed special instruction sets to enhance virtualization performance

- Intel's "VT-x" (Virtualization Technology)
- AMD's "AMD-V"

Most virtualization products benefit from "Second Level Address Translations" (SLAT)

- Improves virtual memory performance when multiple VMs are installed
- Intel's SLAT implementation is "Extended Page Table" (EPT)
- AMD's is "Rapid Virtualization Indexing" (RVI)

Most virtualization software requires a CPU with virtualization support enabled.



- When choosing a computer for virtualization, ensure the CPU supports:
    - Intel VT-x or AMD-V and SLAT
    - Verify in BIOS settings.

System Memory
Each guest OS requires additional system memory.

- Each virtualization workstation must have at least 8GB of RAM
    - This is the bare minimum for the host and a single Windows 11 guest OS.

Microsoft Hyper-V hypervisor software ↗

Mass Storage
Each guest OS requires significant disk space, with VM's "hard disk" stored as an image file on the host.

- Most hypervisors use dynamically expanding disk images that grow as more data is added to the guest OS
- Snapshots, which capture the VM's disk state at a specific point in time, increases storage demands
    - Useful for rolling back changes during testing or system mods

Networking
A hypervisor can create a virtual network allowing communication between VMs, the host, and other hosts.
Enterprise virtualization platforms also support configuring virtual switches and routers.
Virtualization Security Requirements

8.1.5 - Virtualization Security Requirements

Guest OS Security
Each guest OS requires regular patching and protection against malware.

- To mitigate performance issues, many environments use a template image that is patched, tested and then deployed to production.
- Modern virtualization-aware security solutions allow security to be managed at the hypervisor or host level, reducing the performance drain on individual VMs.
- Security management should include strict controls over VM template development, ensuring they are free from unnecessary services, malware, or unauthorized code.
    - Major risks of rogue devs: Inserting backdoors or malicious code, such as "logic bombs"

Virtual machine sprawl happens during an uncontrolled deployment of unauthorized VMs (rogue VMs), complicating security and resource management.

Host Security
In virtualization, the host is a single point of failure for multiple guest OS instances. Methods to mitigate this risk:

- Enabling Automatic restart of VMs on another host
- Power redundancy, such as using uninterruptible power supplies (UPS) or backup generators.

Hypervisor Security
Virtual machine escaping, where malware on a guest OS can access other guest VMs or the host.

- Always keep the hypervisor patched with updates for critical vulnerabilities.

Cloud Characteristics
They distinguish cloud provisioning from on-premises or hosted client/server network architecture.

From the consumer's perspective:

- Cloud Computing provides on-demand resources over a network, typically the internet.
    - Server instances, file storage, databases, or applications
- Users don't manage the underlying infrastructure and pay only for what they use.
    - Known as metered utilization.
    - This includes charges for ingress (data entering the cloud) and egress (data leaving the cloud).

From the provider's perspective:

- Cloud infrastructure operates like any large-scale datacenter, using virtualization to allocate resources efficiently.

    - High Availability: Minimal downtime, with services like “Five Nines” (99.999%) availability, equating to only 5 minutes 15 seconds of annual downtime.
    - Salability: Costs involved in supplying the service to more users are linear.
        - Example: If #users x 2, then costs to maintain the same level of service = x2
        - Scalability can be achieved by adding nodes (horizontal/scaling out) or by adding resources to each node (vertical/scaling up).
    - Rapid Elasticity: The ability to handle real-time demand changes without loss of services or performance Systems can also reduce costs when demand is low.
- Cloud providers meet these requirements through automatic provisioning and de-provisioning of resources via pooling shared resources and virtualization
    - Shared resource pooling means datacenter hardware is not dedicated to a single customer.
    - Allows providers to manage resources like CPU, memory, disk, or network through software.

8.2 - Cloud Concepts

8.2.1 - Cloud Characteristics

– – null – –

8.2.3 - Common Cloud Deployment Models

Cloud deployment models can be categorized based on ownership and access arrangements.

- Public (Multitenancy): Offered over the internet by a cloud service provider (CSP)
    - Often includes subscription or pay-as-you-go options, sometimes free lower-tier services.
    - As a shared resource, it carries performance and security risks.
    - Multicloud architectures involve using services from multiple CSPs.
- Private: Cloud infrastructure exclusively owned and managed by an organization.
    - Typically managed by a dedicated business unit, while other units use it.
    - Offers greater control over privacy and security.
    - Ideal for banking and governmental services requiring strict access control.
- Community: Several organizations share the costs of a hosted private or fully private cloud in order to pool resources for common concerns, such as standardization and security policies.
- Hybrid: Combines public, private, and/or community cloud elements.
    - Example: A hybrid deployment might use a public cloud for some functions while keeping sensitive data and applications on-premises.
    - Example: A travel organization might use a private cloud for most of the year but switch to a public cloud during peak times.

8.2.5 - Common Cloud Service Models

A cloud service model is differentiated by the level of complexity and preconfiguration provided, in addition to the deployment model. The most common models are infrastructure, software, platform, and desktop.

Infrastructure as a Service (IaaS) allows organizations to provision and manage IT resources like virtual servers, storage, networking, and load balancers from a cloud provider, without needing to purchase and maintain physical hardware.

- Can be deployed quickly and scaled as needed
- Popular IaaS platforms:
    - Amazon Elastic Compute Cloud (aws.amazon.com/ec2)
    - Microsoft Azure Virtual Machines (azure.microsoft.com/services/virtual-machines)
    - OpenStack (openstack.org)

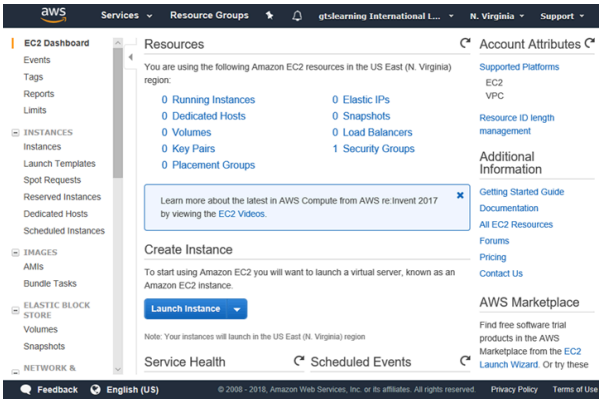
Software as a Service (SaaS) delivers software applications over the internet on a subscription or pay-as-you-go basis, eliminating the need for businesses to purchase and install software locally.

- Devs can provision, test, and deploy applications quickly using cloud infrastructure without installing them on client machines.
- SaaS can be used with single tenancy implementation or with multi-tenancy implementation.
- Popular SaaS platforms:
    - Microsoft 365 (support.office.com)

    - Salesforce (salesforce.com)
    - Google Workspace (workspace.google.com)

Platform as a Service (PaaS) provides a development environment that includes infrastructure like servers and storage (similar to IaaS) but also offers tools for building, testing, and deploying applications.

- Does not come with a pre-built application, devs are responsible for creating, securing, and managing the software they deploy on the platform
- The provider ensures the platform's availability and infrastructure integrity.
- Examples of PaaS platforms:
    - Oracle Cloud (cloud.oracle.com/paas)
    - Microsoft Azure SQL Database (azure.microsoft.com/services/sql-database)
    - Google App Engine (cloud.google.com/appengine)



Dashboard for Amazon Web Services Elastic Compute Cloud (EC2)

IaaS/PaaS ➥

Desktop as a Service (DaaS) is a cloud computing solution that delivers virtual desktops to end-users over the internet, allowing them to access their desktop environment and applications from any device, anywhere.
Cloud File Storage

8.2.7 - Cloud File Storage

Cloud storage is a type of Software as a Service (SaaS) that allows users to store and sync files across multiple devices.

- File synchronization is offered by Microsoft OneDrive, Dropbox, Apple iCloud, and Google Drive.
- Allows multiple users to collaborate on the same document, with features like change tracking and commenting.
- Content delivery networks (CDNs) are often used to store files closer to where they will be downloaded, speeding up access times.
- Often cost tiers based on factors like replication speed and geographical distribution.

Chapter 9

Notes from Chapter 9: Supporting Mobile Devices

9.1 - Mobile Devices and Peripherals

9.1.1 - Mobile Device Accessories

Input Devices

- Touchpad: Usually refers to the embedded panel on a laptop that is used for pointer control. Most support multitouch and gestures.
- Trackpad: Can be used to mean the same thing as touchpad, but is often used to mean a larger-format device attached as a peripheral.
- Drawing Pad: A large-format touch device attached as a peripheral. Also called graphics tablets as they are most widely used for sketching and painting in a digital art application
- Track point: A pressure-sensitive little nub that is embedded into the keyboard on some laptops.

Stylus

A touch pen that allows for more precise control, can be used for handwriting and drawing. The functionality is often referred to as natural input. Some come with removable and changeable nibs for use as different pen/brush types with digital art applications.

Microphone, Speakers, and Camera/Webcam

- Microphone: Used to record audio and for voice calling.
- Speakers: Produce audio output
- Digital Camera: Allows for video recording or web conferencing and can be used to take still pictures.
- External headset/earbud set: Can provide both speaker microphone and headphone speakers.
    - Wired headsets use either 3.5mm audio jack or a USB/Lightning connector.
    - Wireless headsets are connected via Bluetooth.

9.1.2 - Mobile Device Wired Connection Methods

Laptop Ports

Most laptops ship with standard wired ports for connectivity. They are typically in the following conventions:

- HDMI or DisplayPort/Thunderbolt.
    - Possibly VGA or DVI on older laptops
- USB Type A or C ports are common on modern laptops
- Microphone and/or Speaker jacks
- RJ45 for networking
- Memory Card Readers

Smartphone and Tablet Connectors

- Modern Android and Apple smartphones and tablets use USB-C for wired peripherals and charging.
- Older devices may use Micro-B USB and Mini-B connector form factors.
- Older Apple iPhone and iPad models use the proprietary Lightning connector.

9.1.3 - Port Replicators and Docking Stations

Port Replicator

- Attaches to a special connector on the back or underside of a laptop or connected via USB

Docking Station

- A sophisticated port replicator that may support add–in cards or drives via a media bay.

Smartphone and Tablet Docks

- Can connect the device to a monitor, external speakers, and keyboard/mouse input devices.

9.1.5 - Wi-Fi Networking

Enabling and Disabling Wi-Fi: Easy to find settings in device menus.

Airplane Mode: Disables some or all of the wireless features (cellular data, Wi-Fi, GPS, Bluetooth, and NFC). Some services may be selectively restored while still in airplane mode.

Wi-Fi Antenna Connector/Placement: Usually 2 wires that run the border of the device to the Wi-Fi chip.

9.1.7 - Cellular Data Networking

*Connecting to the internet via the device's cellular radio and the handset's network provider.

Cellular Networking Technologies

The evolution of cellular networking technologies:

- 3rd Gen (3G): First used in iPhones and Android smartphones. 7.2Mbps
- 4th Gen (4G): Introduced **Long-Term Evolution (LTE)**. 300Mbps
- 5th Gen (5G): 10Gbps

Subscriber Identity Module (SIM/eSIM)

- A SIM card allows the device to connect to the correct service to utilize functions such as call, texting, and using mobile data.
- May be used to store contact and a limited number of texts, but usually now stored in phone's memory and in cloud services.
- Can be switched to an alternative handset if needed.
- eSIM is embedded in the phone
    - Many devices that support eSIM allow for multiple eSIM profiles to be stored on a single device.
    - A single device could have multiple phone numbers or data plans.

Enabling and Disabling Cellular Data

Some devices allow usage warnings and caps and prevent selected apps from using cellular data connections. Some handsets support the use of two SIMs, and you can choose which one to use for data networking.

9.1.8 - Mobile Hotspots and Tethering

Tethering refers to connecting another device to a mobile device so that it can share its data connection. Can occur over USB, Bluetooth, or Wi-Fi connections.

Hotspot: Tethering over a Wi-Fi connection.

9.1.9 - Bluetooth Wireless Connections

Bluetooth connections can be configured in the settings.

Enable Pairing

1. The Bluetooth radio on each device must be put into discoverable or pairing mode.
2. Select the device from the Bluetooth settings menu to begin pairing.
3. Most pairing systems will generate a passkey or PIN.
4. Enter the PIN and your connection will be complete.
5. Test the pairing by using the device as intended.

9.1.10 - Near-Field Communication Wireless Connections

Allows short-range data transmission (~8") to activate a receiver chip in the contactless reader.

- Typically used to make payments with mobile devices via contactless PoS machines.
- On Android, NFC can be disabled via settings.
- Can also be used to configure other types of connections, such as pairing Bluetooth devices.

– – 9.2 Mobile Apps and Data – –

9.2.1 - Mobile Apps

Installable programs that extend the functionality of the mobile device they are installed on.

- Must be written and compiled for a particular mobile operating system.

iOS Apps: Apps distributed via Apple's app store. Often referred to as the ***walled garden model***, it is designed to prevent the spread of malware or code that could cause faults or crashes.

- Apps come in a variety of commercial models: Free to use, free with in-app purchases, or paid-for.
- Using Apple's **integrated development environment (IDE)**, 3rd-party devs can create apps using **Xcode**.
    - Xcode can only be installed and run on a computer using macOS.

Android Apps: The Java-based IDE, **Android Studio**, is available to devs on Linux, Windows, and macOS.

9.2.2 - Account Setup

- A user account is used to manage the apps installed on the device by representing the user on the app store.
    - iOS requires an Apple ID
    - Android requires either a Google Account or similar, such as a Samsung Account
- Most accounts require you to select a unique ID (email address) and to configure credentials (pattern lock, fingerprint, face ID, etc.)
    - Accounts can also be linked to a cellphone number or alternative email address for verification and recovery functions.
- The owner account can be used to access various services, such as an email account or cloud storage.
    - Allows app settings and data to be synchronized between multiple devices.
- Examples of account services:
    - Microsoft 365: A Microsoft digital identity is used to access cloud subscriptions for the Office productivity software suite and the OneDrive cloud storage service.
        - Uses @outlook.com domain by default, but can be registered with a 3rd-party address.
    - Google Workspace: A Google account (@gmail.com) grants free access to Google's Workspace productivity software and the free storage tier on Google Drive.
    - iCloud: An Apple ID (@icloud.com) grants free access to Apple's productivity software and the free storage tier on iCloud.

9.2.3 - Types of Data to Synchronize

Mobile device synchronization (sync) refers to copying data back and forth between different devices. There are many different types of information that users might synchronize and many issues to go along.

Contacts

- A record with fields for name, address, email address(es), phone numbers, notes, and so on.
    - One issue: matching fields or phone number formats when importing from one system to another
    - **vCard** represents one standard format.

Calendar

- A record with fields for appointment or task information, such as subject, date, location, and participants.
    - Most people have trouble managing them.
    - Calendar items can be exchanged between different services using the **iCalendar (ICS)** format.

Mail

- Most email systems store messages on the server.
    - Sync issues happen with deletions, sent items, and draft compositions.

Media Files and Documents

- The main issue comes down to storage, where one device may not have the storage to hold what another device does.
- Issues with file formats are common, not all devices can play or show all formats.

- Users editing a document on different devices may have trouble with version history unless the changes are saved directly to the copy stored in the cloud.

Apps
- Apps are usually available across all devices that the account holder signs in on, as long as they are on the same platform.
- Despite lack of cross-play support, many apps will share data seamlessly, such as social media ones.

Passwords
- Passwords are cached securely within the device file system and protected by the authentication and encryption mechanisms required to access the device via the lock screen.
- Cloud services allow cached passwords to be synchronized across devices.
- Password managers can also be used to store and sync passwords across multiple devices.

9.2.4 - Email Configuration Options

Commercial Provider Email Configuration
- Most commercial email providers allow the OS to *autodiscover* connection settings.
    - The mail service has published special DNS records that identify how an account for a domain should be configured.
- To connect to an autodiscover-enabled account, simply choose the mail provider and enter your email address and credentials.

Corporate and ISP email Configuration
Many institutions use Microsoft's Exchange mail server for corporate email.
- To manually configure an **Exchange ActiveSync (EAS)** account, you'll need to enter the email address and username and a host address as well as a password and the choice of whether to use **Transport Layer Security (TLS)**.

If you are connecting to an **internet service provider (ISP)** email host or **corporate mail gateway** that does not support autodiscovery of configuration settings, you can enter the server address manually by selecting "Other", then inputting the appropriate server address.
- Incoming mail server - The FQDN or IP address of the **Internet Mail Access Protocol (IMAP)** or **Post Office Protocol (POP3)** server.
    - Choose IMAP if you are viewing and accessing the mail from multiple devices.
    - POP3 will download the mail to the device, removing it from the server mailbox.
    - Exchange doesn't use either POP3 or IMAP, it uses EAS.
- Outgoing mail server - The address of the **Simple Mail Transfer Protocol (SMTP)** server.
- Enable or disable **Transport Layer Security (TLS)**.
    - TLS protects confidential information such as the account password and is necessary if you connect to mail over a public link (Wi-Fi "hotspot")
        - Can only be enabled if the mail provider supports it.
- Ports - The secure (TLS enabled) or insecure ports used for IMAP, POP3, and SMTP would normally be left to the default ports.
    - If the email provider uses custom port settings, you would need to obtain those and enter them in the manual configuration.

9.2.5 - Synchronization Methods

When synchronizing large amounts of data, you should account for different types of **data cap**.
- The account will have an overall storage limit
    - Most accounts are issued with 5GB of free tier storage, more can be "subscribed to".
- If synchronizing over a cellular data network, there are usually monthly data allowances and a rate for exceeding that allowance.
    - To avoid unwanted charges, configure the device to warn and/or cap cellular data transfers
    - Most apps can be configured to sync over Wi-Fi only

Synchronizing to PCs
If cloud services are not available, one can usually view an Android phone or tablet from Windows over a USB or Bluetooth, and use drag-and-drop for file transfer.

Synchronizing to Automobiles
Most new automobiles come with an in-vehicle entertainment and navigation system.

- The main part of this system is referred to as the head unit.
    - If supported, a smartphone can be used to "drive" the head unity so the navigation features from your smartphone will appear on the display.
        - The main technologies here are Apple CarPlay and Android Auto

9.2.6 - Enterprise Mobility Management (EMM)

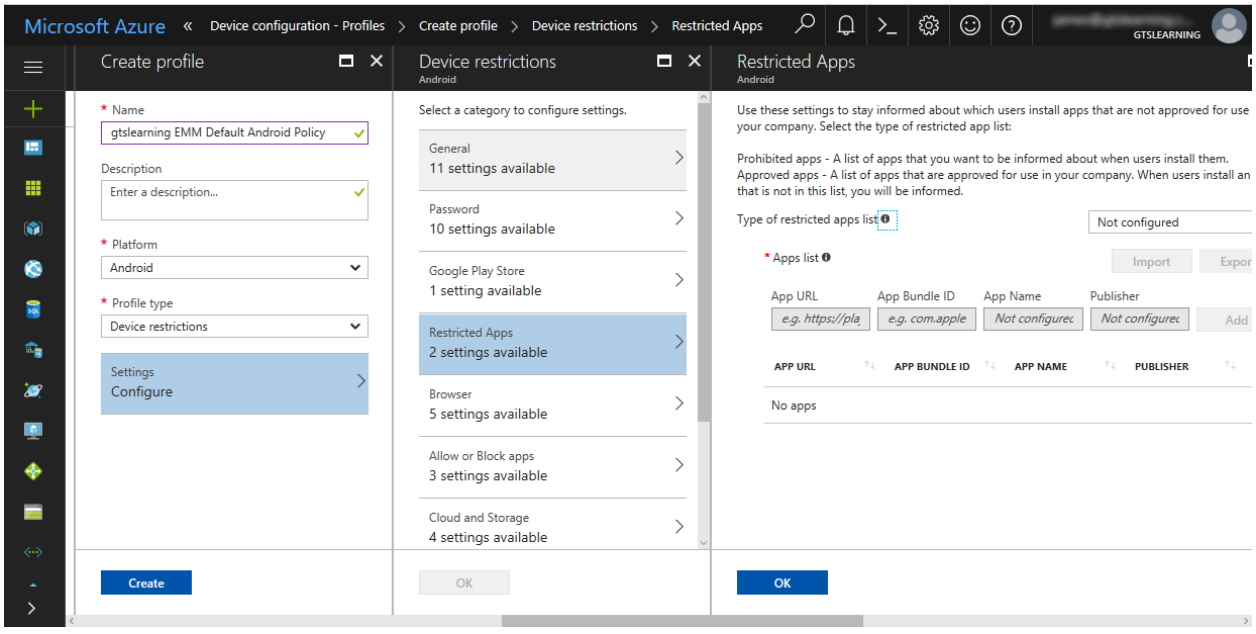
A class of management software designed to apply security policies to the use of mobile devices and apps in the enterprise. The challenge of identifying and managing all the devices attached to a network is often referred to as "visibility".

There are two main functions of an EMM product suite:

- **Mobile Device Management (MDM)** sets device configuration policies for authentication, policy enforcement, feature use (camera and microphone), and connectivity.
    - Can also allow device resets and remote wipes.
- **Mobile Application Management (MAM)** sets policies for apps that can process corporate data and prevent data transfer to personal apps. This solution configures an enterprise-managed container or workspace.
- Examples of EMM solution providers:
    - **Omnissa ONE, Microsoft Intune, Broadcom, Citrix Endpoint Management**.

BYOD - Bring your own device
COPE - Company owned "Personally Enabled"
COBO - Company Owned "Business Only"
CYOD - Choose Your Own Device

When a device is enrolled with the MAM software, it can be configured into an enterprise workspace mode in which only a certain number of authorized **corporate applications** can run. *Messages and attachments sent from the account might be subject to **Data Loss Prevention (DLP)** controls to prevent unauthorized forwarding of confidential or privacy-sensitive data.



Apple operates enterprise developer and distribution programs to allow private app distribution via **Apple Business Manager**.

Google's Play Store has a private channel option called **Managed Google Play**.
*Both of these options allow a MAM suite to push apps from the private channel to the device.

9.2.7 - Location Services

Geolocation is the use of network attributes to identify or estimate the physical position of a device. A mobile device operates a **location service** to determine its current position, using two systems:

- **Global Positioning System**: A means of determining the device's latitude and longitude based on information received from orbital satellites via a GPS sensor.
    - Not all mobile devices have GPS sensors
- **Indoor Positioning System**: Finds a device's location by triangulating its proximity to other radio sources.

Location services store highly personal data, it is only available to an app where the user has granted specific permission to use it.

*Some mobile devices are additionally fitted with a magnetometer sensor, which enables more accurate compass directions.

9.3 - Laptop Hardware

9.3.1 - Laptop Disassembly Processes

Hand Tools and Parts

- Small screws are easy to strip.
- Document every step, photograph screw locations.
- Tape screws from specific areas to the chassis to avoid losing them.
- Keep static-sensitive parts in antistatic packaging.
    - SSDs, memory modules, and adapter cards.

Form Factors and Plastics/Frames

- Obtain the manufacturer's service documentation before commencing any upgrade or replacement work.
- Only perform this work if a warranty option is not available.

9.3.2 - Battery Replacement

AC Adapters

- AC Adapters are normally universal or auto-switching
    - Can operate from any 110-240 VAC 50/60Hz supply
- Always check the label to confirm.

Battery Power

- Li-ion batteries are typically available in 6-, 9-, or 12-cell versions.
- Connector and form factor are typically specific to the laptop vendor and a range/model.
- Li-ion battery life is affected by being fully drained of charge.
- Li-ion battery life is affected by being held at 100% charge.
- Balanced power charging stops trickle charging at 80%.
- If storing a Li-ion battery, reduce the charge to 40% and stoe below 20°C/68°F.
- **Li-ion batteries generally last 2-3 years.**

9.3.3 - RAM and Adapter Replacement

Laptops have fewer **field-replaceable units (FRU)** than desktops.

Upgrading RAM Modules

- Laptop RAM comes in **Small Outline Dual In-Line Memory Modules (SODIMMs)**.
    - The slots are keyed to prevent incompatible modules from being installed.

Upgrading Adapter Cards

- When upgrading radio adapters, you need to re-connect the antenna wires used by the old adapter or install a new antenna kit.
    - The antenna connections can be fiddly to connect and are quite delicate.
- If installing an adapter with GSM or LTE cellular functionality, remember to insert the SIM card as well.

9.3.4 - Disk Upgrades and Replacement

In order to upgrade a fixed disk, there must be a plan for what to do with existing data:

- **Migration**, using backup software to create an image or clone of the old drive and store it on USB media.
    - The new drive must be the same size or larger than the old one for a backup to work.
        - Unless using a cloning tool that can shrink the source image.
    - As an alternative to using a 3rd USB drive to store the image, a disk enclosure allows you to connect an internal drive temporarily as an external drive. You can then migrate the image directly to the SSD before removing the old drive and installing the new one.
- **Replacement**, where only data is backed up from the old drive.
    - The new drive is then fitted to the laptop and an OS plus apps are installed.
    - User data can then be restored from backup.

Laptop HDDs are usually 2.5" form factor, though sometimes the 1.8" form factor is used.

- Laptop 2.5" HDDs are slower and have lower capacity than 3.5" desktop counterparts.
- A standard 2.5" drive has a z-height of 9.5mm; an ultraportable laptop may require 7mm(thin) or 5mm(ultrathin) drives.

Magnetic drives use ordinary SATA data and power connectors. *Drive bays measuring 1.8" might require the use of the micro SATA (uSATA) connector.

An SSD flash storage device can also use the SATA interface and connector form factors, but is more likely to use an adapter card interface:

- mSATA: An SSD might be housed on a card with a **Mini-SATA (mSATA)** interface.
    - Uses SATA bus, so max transfer speed is 6Gb/s.
    - May resemble PCIe cards, but are not compatible with the PCIe slots.
- M.2: An M.2 SSD usually interfaces with the PCI Express bus, allowing much higher bus speeds than SATA.
    - M.2 adapters can be different lengths (42mm, 60mm, 80mm, 110mm)
        - The most popular size is M.2 2280 (80mm).

9.3.5 - Keyboard and Security Component Replacement

Keyboard and Touchpad Replacement

- Each part connects to the motherboard via a data cable, typically a flat ribbon tape.
    - Each cable is held in place by a latch, release these before trying to remove them.
- When replacing an input device, use the OS/driver settings utility or app to configure it.
    - A keyboard needs to be set to the correct input region.
- Touchpads need to be configured to an appropriate sensitivity to be comfortable for the user.

Key Replacement

- Sometimes it is more economical to lift a single key for cleaning or replacement.
- The retainer clips can also be removed for cleaning.

Biometric Security Components

- Attached to the motherboard by a flat ribbon cable in the same way as the keyboard and touchpad.

Camera and Microphone

- The connections for the camera will run through the display assembly and connect to the motherboard.
- The microphone assembly is often connected right next to the camera assembly but will have separate connections.

Near-Field Scanner

- An NFC is primarily used to pair peripheral devices or to establish a connection to a smartphone.
- Connects to an antenna to operate.

9.4 - Troubleshoot Mobile Devices

9.4.1 - Power and Battery Issues

If you experience problems working from AC power:

1. Test the outlet with a "known good" device.
2. Check that the LED on the AC Adapter is green.
3. If no LED, check the fuse on the plug, and if available, try testing with a known good adapter.

Once you confirm the correct AC adapter is being utilized, if your device is powering up and you are experiencing power consumption issues, you may need to recalibrate your battery.

If a mobile device will not power on when disconnected from building power:

1. First check that the battery is seated properly in its compartment.
2. Check whether the battery contacts are dirty
    a. Clean with isopropyl alcohol (90% or higher).

If the battery is properly inserted and the mobile device does not switch on or only remains on for a few seconds, it is most likely completely discharged.

- Test this by using a known good battery. If the good battery doesn't work, then there is something wrong with the power circuitry on the motherboard.

Improper Charging Symptoms

An improper charging routine will reduce the usable life of a battery.

- Make use of power management features included with your device/OS to prolong battery life.

Swollen Battery Symptoms

If you notice any swelling from the battery compartment, discontinue use of the mobile device immediately. Signs of a swollen battery:

- The device wobbles when placed flat on a desk
- A deformed touchpad or keyboard.

A swollen battery indicates some sort of problem with the battery's charging circuit, which is supposed to prevent overcharging.

- If a device is exposed to liquid, this could also have damaged the battery.

Li-ion batteries are designed to swell to avoid bursting or exploding.

- A swollen battery is a fire hazard and could leak hazardous chemicals - do not allow these to come into contact with your skin or your eyes.
- If the battery cannot be released safely and easily from its compartment, contact the manufacturer for advice, as well as disposal instructions.
    - A swollen battery should not be discarded via standard recycling points unless the facility confirms it can accept batteries in a potentially hazardous state.
- Manufacturing defects in batteries and AC adapters often occur in batches, make sure you remain signed up to the vendor's alerting service so you are informed about product recalls or safety advisories.

9.4.2 - Hardware Failure Issues

Overheating Symptoms

- Laptop cooling (or chilling) pads can help reduce overheating by maximizing airflow.
- Dust trapped in vents acts as an insulator and can prevent proper cooling.
- High screen brightness and use of the flashlight function will rapidly increase heat.
- A mobile device will quickly overheat when exposed to direct sunlight.
- Devices have protective circuitry that will initiate a shutdown if the internal temperature is at the maximum safe limit.
- Approaching 40°C is getting too warm.

Liquid Damage Symptoms

- Waterproofing in mobile devices is rated on the **Ingress Protection (IP)** scale.
- A case or device will have two numbers, such as IP67.

    - The first (6) is a rating for repelling solids, with a 5 or 6 representing devices that are dust-protected and dust-proof, respectively.
    - The second value (7) is for liquids, with a 7 being protected from immersion in up to 1m/3' and 8 being protected from immersion beyond 1m.
    - If dust protection is unrated, the IP value will be IPX7 or IPX8.

If a mobile device is exposed to liquid damage, there may be visible signs of water damage under the screen. The screen might display graphics artifacts or not show an image. *Even if there is no visible sign, power off the device immediately if you suspect liquid damage.

- Dry as much excess liquid as possible.
- If you suspect internal components have been exposed, disassemble the device to fully dry.
    - Place the components in a bag of rice for expedited drying
- Once dry, clean the circuit boards and contacts and replace the battery.

Physically Damaged Port Symptoms

- If a port is damaged, the connector may be loose or may no longer fit. There may be no data =connection at all, or it might be intermittent. The device may fail to charge properly.
- Always remember to *hold the connector* (not the cable) and pull straight out.
    - DO NOT JIGGLE CONNECTORS TO REMOVE THEM.

9.4.4 - Screen and Calibration Issues

- If there is no image on the screen, check that the video card is good by using an external monitor.
- There should be a very dim image on the display if the graphics adapter is functioning, but th ebacklight has failed.

Broken Screen Issues

- Impacts on a hard surface from over 1m in height will usually result in cracking or shattering.
- If only the glass layer is damaged, the digitizer and display may remain usable, to some extent.
- A broken screen is likely to require warranty or professional services to repair it.

Digitizer Issues

Symptoms such as the touch screen not responding to input or the stylus not working can indicate a problem with the digitizer. If you can discount shock and liquid damage, try the following:

- Remember to ask, "What has changed?"
- Verify that the touchscreen and the user's fingers are clean and dry.
- If a screen protector is fitted, check that it is securely adhered to the surface and that there are no bubbles or lifts.
- Check that there is not a transitory software problem by restarting the device.
- Try using the device in a different location in case some source of electromagnetic interference (EMI) is affecting the operation of the digitizer.
- If the device has just been serviced, check that the right wires are still connected in the right places for the digitizer to function.

Cursor Drift/Touch Calibration Issues

- On a laptop, if touchpad sensitivity is too high, typing can cause vibrations that move the cursor.
    - Many laptops come with a Fn key to disable the touchpad.
- Sans hardware causes, unresponsive or inaccurate touch input can be an indication of:
    - Resources being inadequate (too many open apps)
    - Badly written apps that hog memory or other resources.
- Try a soft reset.
- If the problem persists
    - Try to identify whether the problem is linked to running a particular app.
    - Try freeing space by removing data or apps.
    - Windows devices and some versions of Android support re-calibration utilities.
    - If no cause, then likely in need of a warranty repair.

9.4.5 - Connectivity Issues

Wi-Fi and Bluetooth connectivity problems can generally be categorized as either relating to “physical” issues (interference), or to “software” configuration problems.

- Verify that the adapter is enabled. Check the status of function key toggles on a laptop, or use the notification shade toggles on a mobile device to check that airplane mode has not been enabled or that the specific radio is not disabled.
- If a laptop has been serviced recently and wireless functions have stopped working, check that the antenna connector has not been dislodged or wrongly connected.
- If a wireless peripheral such as a Bluetooth mouse or keyboard that has been working stops, it probably needs a new battery.
- If you experience problems restoring from hibernate or sleep mode, try cycling the power on the device or reconnecting it and checking for updated drivers for the wireless controller and the devices.

If you are experiencing intermittent connectivity issues:

- Try moving the two devices closer together.
- Try moving the devices from a side-to-side or up-and-down position to a different position or changing how the device is held.
    - Sometimes, certain hand positions around a cell phone’s antenna can stop the device from functioning as well as it should.
- Consider using a Wi-Fi analyzer to measure the signal strength in different locations to try to identify the source of interference.

A utility such as **Cell Tower Analyzer** or **GSM Signal monitor** can be used to analyze cellular radio signals. An app might combine both functions.

9.4.6 - Malware Issues

Whenever a device does not function as expected, you should assess whether it could be infected with malware.

- Malware or rogue apps are likely to try to collect data in the background. They can become unresponsive and might not shut down when closed. Such apps might cause excessive power drain and high resource utilization, potentially leading to overheating problems.
- This excessive background usage will also lead to degraded performance. This is a common sign of a malware infection.
- Another tell-tale sign of a hacked device is reaching the data transmission overlimit unexpectedly. Most devices have an option to monitor data usage and have limit triggers to notify the user if the limit has been reached. This protects from large data bills but should also prompt the user to check the amount of data used by each application to monitor their legitimacy.
- Malware may try to use the camera or microphone to record activity. Check that the camera LED is not activated.
- The user also may not be able to install new applications. Malware may block new applications sto prevent security software from being installed or the malware may use up so much free space tha there is not enough space left to install new applications.

Chapter 10

Notes from Chapter 10: Supporting Print Devices

10.1 - Printers and Multifunction Devices

10.1.1 - Printer Unboxing and Setup Location

- The most common printers for home and office use are inkjet and laser printers.
- Major print device vendors include HP, Epson, Canon, Xerox, Brother, OKI, Konica/Minolta, Lexmark, Ricoh, Samsung.

Selecting a Printer

- Speed: Measured in **pages per minute (ppm)**.
    - Monochrome text prints faster than color photos.
    - Recommended 40ppm for office environments.
- Resolution: Measured in **dots per inch (DPI)**.
    - Higher dpi means better quality.
- Paper Handling: Types and sizes of paper the printer can handle, including labels, envelopes, and card stock.
    - Consider paper tray capacity to avoid jams.
- Options: Additional features like an automatic duplex unit for double-sided printing and finishing units for folding, stapling, and hole punching.

Setup Location

- Power and Network: Ensure access to a power outlet and network data port.
    - Avoid trip hazards with cables.
- Environment: Place the printer on a stable, flat surface away from direct sunlight. Ensure good ventilation to disperse fumes and store consumables in a dry, temperature-controlled area.
- Accessibility: The printer should be easily accessible but not disruptive.

Unboxing

- Lifting: Use safe lifting techniques, and ensure the path is free from trip hazards.
- Packing Materials: Check for strips on removable components concealed by panels.
- Acclimation: Allow the printer to acclimate after unboxing. Leave it powered off for a few hours to prevent condensation issues if it has moved from a cold to a warm environment.

10.1.2 - Firmware Management in MFDs and Printers

Firmware in **multifunctional devices (MFDs)** and printers controls functions like printing, scanning, and network connectivity.

- Regular updates improve performance, fix bugs, and address security vulnerabilities.

Checking and Updating Firmware

To check the firmware version:

- Use the control panel under System Information.
- Access the device's web interface by entering its IP address in a browser.

To update firmware:

- Download and install updates via the control panel, web interface, or manufacturer tools like HP Web Jetadmin or Canon imageWARE.

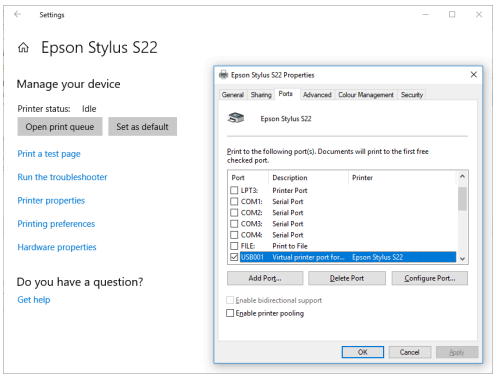
Resetting and Reflashing Firmware

Outdated or corrupted firmware can cause malfunctions. Learning to reset or reflash firmware is a key troubleshooting skill.

- Resetting: Use the control panel to navigate to settings or Maintenance, then select Reset or Restore Factory Defaults.
- Reflashing: Access the web interface, go to the Firmware Update or Maintenance section, upload the latest firmware file from the manufacturer's website, and follow the prompts.
    - Reflashing should only be done when necessary, as it could potentially cause issues if interrupted.

Best Practices
Always back up configurations before performing updates. Always test new firmware on a single device before deploying it across multiple devices to ensure compatibility and stability.

10.1.3 - Print Device Connectivity



USB Print Device Connectivity
When connected to a device through a USB, the computer should automatically detect the printer through **Plug and Play(PnP)**, and install the necessary driver.

Ethernet Print Device Connectivity
Most printers come with an Ethernet adapter and RJ45 port.

- Can obtain an IP address through DHCP or be manually configured.
- IP can be registered on a DNS server for easier client connections via a FQDN.
- For broader management, vendors usually provide web-based utilities, and many newer printers also offer mobile apps or cloud-based portals for remote configuration and monitoring.
    - When managing a computer over a browser, ensure the printer can communicate over the necessary TCP or UDP ports and verify that these ports are not blocked by firewalls or security software.

Wireless Print Device Connectivity
Wireless printers can utilize either Wi-Fi or Bluetooth. For Bluetooth connections, make the printer discoverable and add the device through the Bluetooth settings in Windows or macOS.

Wi-Fi connectivity can be established in two ways:

- Infrastructure Mode: Connect the printer to a Wi-Fi access point, making it available to clients on the network via an IP address or FQDN. Make sure the wireless adapter supports the same 802.11 standard as the access point.
- Wi-Fi Direct: Set up a software-implemented access point on the printer to allow direct connections from client devices.

Mobile printing features like Apple AirPrint, Mopria, and cloud-based solutions such as HP ePrint are now commonly used for wireless printing.

10.1.5 - Printer Drivers and Page Description Languages

Applications that support printing typically follow the **“what you see is what you get” (WYSIWYG)** principle, meaning the screen and print output are identical.

- Printer drivers serve as the interface between the print device and the operating system.
- For networked printers, each client must have a suitable driver installed.
    - 64-bit operating systems require 64-bit drivers
    - If an up-to-date driver is not available from Microsoft, download it form the printer vendor’s website, extract it to a folder on the PC, and use the “Have Disk” option in the Add Printer Wizard to install it.
- If a print driver isn’t detected/updated through Plug and Play (PnP), you may need to manually add it or choose a version that supports a specific **page description language (PDL)**. The steps are as follows:
    1. Download the driver from the printer vendor’s website.
    2. Open the “**Add Printer Wizard**” in your operating system.
    3. Choose the “**Have Disk**” option and navigate to the folder where the driver is extracted.
    4. Select the driver that matches the desired PDL (e.g., PCL, PostScript, or XPS).
    5. Complete the installation process.

A PDL converts print commands from software applications into a raster file, which is a dot-by-dot description of where the printer should place ink. PDLs generally support the following features:

- **Scalable Fonts**: Unlike bitmap fonts, which are fixed-size dot-by-dot images, scalable fonts are described by vectors and can be resized. All Windows printers support scalable **TrueType** or **OpenType** fonts.

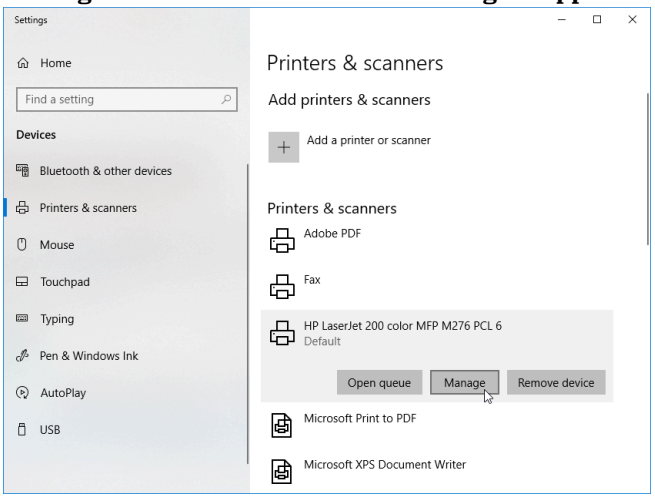
- **Vector Graphics**: Similar to scalable fonts, vector graphics describe how lines should be drawn, rather than providing a pixel-by-pixel description.
- **Color Printing**: PDLs support color models to ensure accurate translation between on-screen colors and print output. Printers use CMYK (cyan, magenta, yellow, black) color model, which differs from RGB (red, green, blue) model used by computer displays.
    - The “K” in CMYK is usually explained as standing for “key”, as in a key plate used to align the other plates in the sort of offset print press used for professional color printing in high volumes.

The choice of PDL is often driven by software compatibility.

- **Adobe PostScript** is device-independent and commonly used for professional desktop publishing and graphic design.
    - It ensures consistent output across different devices but may be slower than other PDLs.
- **HP’s Printer Control Language (PCL)** is more closely tied to specific printer models and may vary in output depending on the device, but is usually faster than PostScript.
- Many Windows printers default to using **Microsoft's XML Paper Specification (XPS)** PDL, which offers better integration with Microsoft applications and faster performance than PostScript in some cases.
    - It lacks the widespread compatibility of PCL and PostScript.
- In a setting where speed is critical, PCL is often preferred due to its faster processing.
- In a setting where quality is critical, PostScript is preferred for its superior consistency and precision.

10.1.6 - Printer Properties

Viewing the print queue and configuring preferences through the Printers and Scanners settings in app page ↴



In Windows, there are two main configuration dialogs for a local printer: **Printer Properties** and **Printing Preferences**

The **Printer Properties** dialog allows you to manage settings for the printer object and hardware, such as updating the driver, changing the port, sharing and permissions, installing a duplex unit or configuring a finisher unit.

- A **duplex unit** enables double-sided printing; it is a component that can be installed or configured through the **Properties** dialog.
- The **About** tab contains information about the driver and the printer vendor and may include links to support and troubleshooting resources.

10.1.7 - Printing Preferences

This dialog sets default print job options, such as paper type, orientation, and color or B/W printing.

Paper/Quality Tab: Lets you select the paper size and type and choose economy or draft mode to save ink or toner.

Color Tab allows you to switch between color and grayscale printing.

Finishing Tab lets you select output options such as whether to print on both sides of the paper (duplex), print multiple images per sheet, and/or print in portrait or landscape orientation.

10.1.8 - Printer Sharing

Printer interfaces determine how print devices connect to the network, while the sharing model describes how multiple clients access the printer. Some printers have integrated **print servers**, allowing direct network connections without a server computer.

A public printer has no access controls, allowing any guest to use it.

- Most guest printing today often includes some security measures like network segmentation, user authentication, or guest Wi-Fi networks.

Windows Print Server Configuration

As an alternative to direct-connect, any computer with an installed printer can share it with other clients.

- The print server can connect to the printer via USB or over the network, providing more administrative control over client access.
- Permissions can be set to allow only authenticated users to submit print jobs.\

The **Sharing** tab in the printer's **Properties** dialog allows configuration of sharing.

- Drivers for different operating systems can be made available so clients can download and install the appropriate driver when they connect to the print share.
- For **"Type 3"** drivers, add x86 (32-bit) and/or x64 (64-bit) Windows support.
- **"Type 2"** drivers require specific versions for each Windows release.
- Windows 10 added support for **"Type 4"** drivers, which aim to create a print class driver framework where a single driver works with multiple devices.

Shared Printer Connections

Ordinary users can connect to a network printer if they have the necessary permissions.

- In **File Explorer**, under **Network**, open the server hosting the printer, **right-click** the desired printer and select **connect**.

10.1.11 - Printer Security

User Authentication

To prevent unauthorized use of a network printer, user authentication ensures that only authorized accounts can submit print jobs.

In Windows, configure user or group permissions in the Sharing and Security tabs of the printer's **Properties** dialog.

- Local authentication stores valid usernames and passwords on the printer.
- Network authentication communicates with a directory server to verify users.

Secured Print and Badging

Secured Print holds a print job on the device until the user authenticates, reducing the risk of confidential information being intercepted from an output tray. This happens via:

- **PIN** entry
- **Badging**: The device has a smart card reader, and the user presents their ID badge to release the print job.

Secured print can be set as a default or configured per job.

Print jobs may be cached for a limited time and deleted if not printed.

- The device might need a memory card or storage to cache encrypted print jobs.

Audit Logs

A print share server or print device can **log** each job, creating an **audit** record of documents printed by specific users and devices. If the log is generated on the print device, tools like **syslog** can transmit logs to a centralized server.

10.1.13 - Scanner Configuration

Scanners in **multi-function devices (MFDs)** create digital files from physical flat objects like documents, receipts, or photos. **Optical character recognition (OCR)** software an convert scanned text into editable digital documents.

Scanner Types

- **Flatbed Scanner**: Shines a bright light on the object placed on a glass surface. Mirrors reflect the image onto a lens, which either splits it into RGB colors with a prism or focuses it onto imaging sensors with color filters.
    - This creates a bitmap file of the object.
- **Automatic Document Feeder (ADF)**: Passes paper over a fixed scan head, efficiently scanning multi=page documents.

Network Scan Services

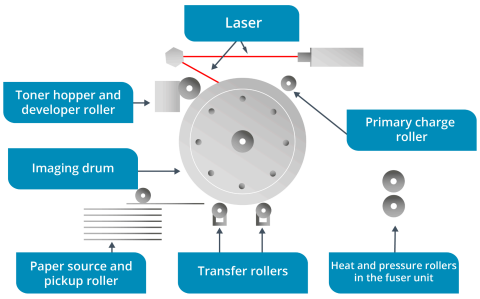
Network scan services direct scan output to specific media:

- Scan to email: The scan is sent as an email attachment. The MFD must be configured with the IP address of an SMTP server.
- **Server Message Block (SMB)**: The scan is saved to a shared network folder. The MFD must be configured with the path to a file server and shared folder, and users must have write permissions to share.
- Scan to cloud: The scan is uploaded to a cloud storage service. The MFD may offer these options or allow custom configurations via a template. Users authenticate to their cloud accounts through the scan dialogs.

10.2 - Print Device Maintenance

10.2.1 - Laser Printer Imaging Process

Laser printers are popular for office use due to their affordability, quiet operation, speed, and high-quality output. THey are available in both grayscale and color models. The laser printing process involves several stages:



Processing Stage: The OS driver encodes the page and sends it to the printer, where it's processed into a bitmap and stored in RAM.

Charging Stage: The **primary charge roller (PCR)** applies a uniform negative charge to the photosensitive imaging drum.

Exposing Stage: The photosensitive imaging drum loses charge when exposed to light. The laser fires light pulses for each raster dot, neutralizing the **PCR** charge and forming an electrostatic latent image on the drum.

Developing Stage: Toner is attracted to the neutralized areas on the drum, forming the image to be printed.

Transferring Stage: The paper is guided through the printer, receiving a positive charge to attract tinder from the drum.

Fusing Stage: The paper passes through the fuser, where heat and pressure bond the toner to the paper.

Cleaning Stage: The drum is cleaned of residual toner and charge, readying it for the next print cycle.

Duplex Printing and Paper Output Path: After the paper passes through the fuser, it is flipped and returned to the developer unit to print the second side of a duplexing assembly unit. If not, the paper is directed to the selected output bin via the exit rollers.

Color Laser Printers: Utilizes separate toner cartridges for each CMYK color.

10.2.2 - Laser Printer Maintenance

When performing any type of maintenance other than loading paper, unplug the printer from the power supply, open the panels, and allow all components to cool to room temperature.

Printers require more maintenance than most IT devices due to their mechanical parts and consumables.

- They create debris like paper dust and toner spills.
- Under heavy use, toner cartridges, fusers, and rollers need frequent replacement.
- Laser printers require regular maintenance and proper user training.

Loading Paper

- Use high-quality paper designed for your printer model and the required output type.
- Position the media guides at the edges of the paper stack.
    - Avoid adding unsupported media or overloading the tray
- Do not use creased, dirty, or damp paper
    - Store paper in a climate-controlled environment, free from excessive humidity, temperatures, or dust.

Replacing the Toner Cartridge

Keep a supply of the correct toner cartridges for your printer model. *Gently rocking the cartridge from front to back can extend its life. Color laser printers typically have four separate cartridges for different colors.
To replace a toner cartridge:

- Open the service panel and remove the old cartridge, placing it in a bag to prevent toner spills
- Take the new cartridge, remove the packing strips, and gently rock it from front to back to distribute the toner evenly.
- Insert the new cartridge, close the service panel, turn on the printer, and print a test.
    - The drum in the toner cartridge is light-sensitive, install the cartridge immediately!

Cleaning the Printer

Consult and follow the manufacturer's specific recommendations for cleaning and maintenance.

- Use a damp cloth to clean exterior surfaces (Ideally Isopropyl >90%)
- Wipe dust and toner away from the printer interior or exterior with a soft cloth, or use a toner-safe vacuum.
- If toner is spilled on skin or clothes, wash it off with cold water.
- Use 99% Isopropyl Alcohol and non-scratch, lint-free swabs to clean rollers and electronic contacts, taking care not to scratch the rollers.
- Replace the printer's dust and ozone filters regularly.
- *DO NOT USE COMPRESSED AIR TO CLEAN A LASER PRINTER.
    - It can disperse toner dust into the air, creating a health hazard.
    - Avoid using a domestic vacuum cleaner, as toner can damage the motor and pass through the dust collection bag.

Replacing the Maintenance Kit

A maintenance kit typically includes replacement feed rollers, a transfer roller, and a fuser unit.

- Remove the old fuser and rollers.
- Clean the printer.
- Install the new fuser and rollers, remove packing strips, and follow the instructions carefully.
    - Dispose of the fuser unit and old rollers through a recycling program to ensure environmental responsibility.

Calibrating a Printer

Calibration determines the appropriate print density or color balance for the printer.

- Most printers do this automatically.
- If print output is not expected, you can manually invoke the calibration routine from the printer's control panel or software driver.

10.2.3 - Inkjet Printer Imaging Process

Inkjet printers are often used for good-quality color output, such as photo printing.

- Typically inexpensive to purchase but costly to operate due to expensive ink cartridges and high-grade paper.
- Slower and noisier than laser printers.

Inkjet Printer Imaging Process

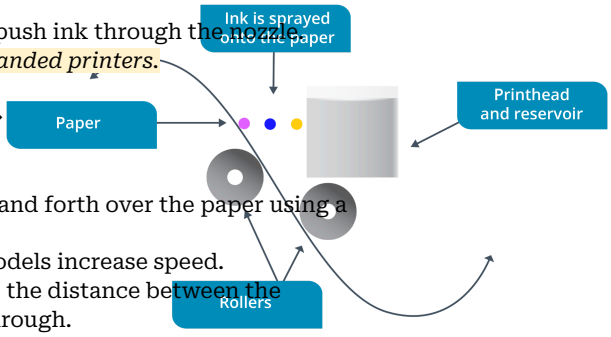
Inkjet printers create high-quality images by spraying tiny ink droplets onto paper, with optimal results on treated paper.

There are 2 main print head types:

1. Thermal Method (HP, Canon, Lexmark): Heats ink to form a bubble that bursts, spraying ink.
    a. Cost-effective, but have a shorter lifespan.
2. Piezoelectric Method (Epson): Uses a piezoelectric element to push ink through the nozzle.

Both technologies are licensed to other manufacturers, resulting in re-branded printers.

The inkjet printing process →



Carriage System

Inkjet printers build images line by line by moving the print head back and forth over the paper using a carriage system.

- Some printers apply ink only in one direction, bidirectional models increase speed.
- Some printers feature a platen gap adjustment, which controls the distance between the print head and the paper, allowing for thicker media to pass through.

10.2.4 - Inkjet Printer Maintenance

Paper Handling and Duplex Assembly

Printers are generally categorized into two types: Top loading/Bottom output or Bottom input/output.

- The paper pickup mechanism is similar to that of a laser printer. A load roller moves the top sheet while a separation roller prevents multiple sheets from entering.
- A sensor detects the paper once it is sufficiently advanced. The stepper motor thena advances the paper as the print head completes each pass until printing is finished.
- Eject rollers deliver the paper to the duplexing assembly (if installed and duplex printing is selected) or the output bin. Some inkjets with a curved paper path may have a “straight-through” rear panel for bulkier media.
    - Inkjets typically have smaller paper trays than laser printers, requiring more frequent restocking.
    - With inkjets, premium, less absorbent paper produces better results, but is really only for single-sided prints.

Replacing Inkjet Cartridges

- Inkjet print heads are often considered consumable items.
- Epson’s piezoelectric print heads are non-removable and designed to last as long as the printer.
- Cartridge reservoirs have sensors to detect ink levels.
- When driver software detects an empty cartridge, it will prompt you to replace it.

Other Inkjet Maintenance Operations

- Print head alignment: If output is skewed, use the print head alignment function from the printer’s property sheet to calibrate it. This is typically done after replacing an ink cartridge.
- Print head cleaning: A blocked or dirty nozzle will result in missing lines on the output. Use the printer’s cleaning cycle to resolve the issue. If this doesn’t work, consider using inkjet cleaning products available on the market
    - Accessible via the property sheet or control panel.
- Clearing paper jams: Paper jams can occur when paper is misfed or stuck inside the printer.
    - To clear, carefully open the printer’s access panel and gently remove the jammed paper, ensuring no torn pieces are left behind. Avoid using excessive force to prevent damaging the internal components.

10.2.5 - Thermal Printer Maintenance

Thermal printers use a heating element to create images on paper. The most common type you'll support is the direct thermal printer, used for high-volume barcode, label printing, and receipts.

- Typically support 200-300dpi resolution, with some capable of printing in one or two colors.

Direct Thermal Printer Imaging Process

Most direct thermal print devices require special thermal paper that contain chemicals designed to react and change color as it is heated by the heating element within the printer. In the feed assembly, a stepper motor turns a rubber-coated roller to friction-feed the paper through the print mechanism. Paper and labels come in fanfold or roll format.

Direct Thermal Printer Maintenance Tips

- Receipts are separate by tearing across serrated teeth, which can create paper dust and debris, use a vacuum or soft brush to remove any buildup.
- Label printers may accumulate sticky residue if labels are not loaded correctly and separate from the backing.
    - Use a swab of isopropyl alcohol to clean the print head and remove sticky residue.
    - Alternatively, use cleaning cards to safely clean the print head.

10.2.6 - Impact Printer Maintenance

Impact printers strike an inked ribbon against paper to create marks. A common type is the dot matrix printer, which uses a column of pins in the print head to strike the ribbon.

Multipart paper consists of multiple layers of paper with carbon or carbonless coating between them, allowing the printer to create duplicate or triplicate copies of a document in a single pass.

Impact Printer Paper

- **Plain Paper**: Held against the moving roller (platen) and pulled through by friction as the platen rotates. Some printers can add a cut sheet feeder to automate page feeding.
- **Carbon Paper (or impact paper)**: Used for making multiple copies in one pass. A sheet of carbon paper is placed between each plain paper sheet, transferring the print head's mark to all sheets.
- **Tractor-Fed Paper**: Features removable, perforated side strips with holes that fit over studded rollers at each end of the platen. This setup reduces skewing and slippage, making it ideal for multi=part stationary.
    - When loading, ensure the paper holes engage with the sprockets and the paper feeds cleanly.

Impact Printer Components

- Impact printers have replaceable ribbons.
    - Modern printers use cartridge ribbons that slot over or around the print head carriage, forming a continuous loop moving in one direction.
    - Older models used two-spool ribbons, requiring a sensor and reversing mechanism.
- When print quality deteriorates, replace the ribbon holder and contents as an integrated component.
    - Some printers use reusable cartridges.

10.3 - Troubleshoot Print Devices

10.3.1 - Printer Connectivity Issues

These can occur when the device cannot be located during installation or when the OS reports an installed device as offline or unavailable.

1. Basic Checks:
    a. Ensure the printer is switched on and online.
    b. Verify all components and cartridges are correctly installed, service panels are closed, and at least one tray is loaded with paper.
    c. Print a test page using the printer's control panel. If successful, the issue lies with the connection to the computer/network.
    d. Cycle the power on the printer. If this doesn't resolve the issue, consider performing a factory reset.
    e. Inspect the USB/Ethernet cable and connectors. Replace with a known good cable to test for cable or connector problems. If possible, try a different connection type.

2. Wireless Printer Connectivity:
    a. Ensure the printer is connected to the correct Wi-Fi network. Wireless printers may attempt to connect to different networks if multiple routers are in range.
    b. Check for interference from other wireless devices or obstacles like walls.
    c. Restart the router or access point, as the issue may lie in the network rather than the printer.
3. Firmware and Driver Updates:
    a. Update printer firmware and driver, as outdated software can cause connectivity issues, especially after an OS update. Modern printers often offer automatic firmware updates, but this feature may need to be manually enabled.
    b. Ensure the computer's OS is up-to-date and compatible with the printer's drivers.
4. Cloud Printing:
    a. If the printer is configured for cloud printing, verify it is correctly registered with the cloud service and that there are no account-related issues preventing access.

10.3.2 - Print Feed Issues

If there is connectivity with the print device but multiple jobs do not print, there is likely to be a mechanical problem with the printer.

Paper Jam Issues

To address a paper jam, gain proper access to the stuck page without using force to avoid further damage.

- Most sheets can be pulled free, but if a page is stuck in the fuser unit of a laser printer, use the release levers.
- Forcibly pulling paper through the fuser can damage the rollers and leave debris.
- Frequent jams often result from unsuitable media (paper or labels), creased or improperly loaded sheets, or faulty rollers.
    - If the jam occurs in the same place each time, perform preventive maintenance, such as cleaning or replacing parts.
- If jams occur within the drum assembly but before the image is fused, a faulty static eliminator may be the cause.
    - This part removes the high static charge from the paper as it leaves the transfer unit.
    - If it fails, the paper may stick to the drum or curl entering the fuser unit.

Paper Feed Issues

If paper is not feeding into the printer, or if a multipage misdeed occurs, follow these steps:

- Verify hat the paper size and weight are compatible with the print tray options and that it is loaded properly with the media guides set correctly.
- Ensure the paper is not creased, damp, or dirty.
    - It is generally a good idea to fan the edge of a paper stack to separate the sheets before loading the tray.
- If the media is not the issue, try changing the pickup rollers.
    - In a laser printer, these are part of the maintenance kit.

Grinding Noise Issues

In a laser printer, a grinding noise usually indicates a problem with the toner cartridge, fused, or gears/rollers.

- Identify the noise source, ensure all components are seated correctly, and check the paper path for jams and debris.
- If the issue persists, replace the printer cartridge, maintenance kit, or both.

In an inkjet printer, a grinding noise typically points to a fault in the carriage mechanism.

- Consult the vendor documentation for instructions on re-engaging the clutch mechanism with the gear that moves the cartridge.

10.3.3 - Print Quality Issues

If a print job results in smudged, faded, or marked output, the issue is likely due to printer hardware or media faults.

Laser Printer Print Defects

Common print defects in laser printers include:

- **Faded or faint prints**: Likely indicates the toner cartridge needs replacing unless a low-density (draft) option was selected.
- **Blank pages**: Usually an application or driver issue, or the toner cartridge packing seals were not removed. It could also indicate a damaged transfer roller (the image transfer stage fails).
- **White stripes**: Indicates poorly distributed toner (gently shake the cartridge) or a dirty/damaged transfer roller.
- **Black stripes or whole page black**: Suggest a dirty or damaged primary charge roller or a malfunctioning high-voltage power supply. Try a known good toner cartridge.
- **Speckling on output**: Loose toner may be contaminating the paper. Clean the printer interior with an approved toner vacuum.
- **Vertical or horizontal lines**: Repetitive marks often result from dirty feed rollers (note that there are rollers in the toner cartridge and fused unit too) or a damaged/dirty photosensitive drum.
- **Toner not fused to paper**: Smudging output indicates the fused needs replacing.
- **Double/echo images**: Indicates the photosensitive drum is not properly cleaned. Try printing different images; if the issue persists, replace the drum/toner cartridge.
- **Incorrect chroma display**: If prints display incorrect colors, ensure toner cartridges are installed in the correct slots and have sufficient toner. Misalignment of the transfer belt or cartridges can cause color casts or shadows. Reseat components, run the calibration utility, and print a test page.
- **Color missing**: Replace the cartridge. If the issue resists, clean the contacts between the printer and cartridge.

Inkjet Print Defects

- **Lines through printouts**: Indicate a dirty print head or blocked ink nozzle. Run a cleaning cycle to fix this.
- **Smearing, wavy, or blurry output**: Likely a media problem. Persistent marks suggest a dirty feed roller.
- **Print head jams**: The printer will display a status message or a flashing LED. Turn the printer off, unplug it, count to 10, then turn it back on.
- **Inconsistent color output**: Indicates a low ink reservoir or a completely blocked print head for ne of the colors.
- **No color printing**: Ensure color printing is selected.

Dot Matrix Print Defects

Lines in the output of a dot matrix printer indicate a stuck pin in the print head.

- The platen position, which adjusts the gap between the paper and the print head to accommodate different paper types, can also affect output.
    - An incorrect gap can cause faint printing if too wide or smudging if too narrow.

10.3.4 - Finishing Issues

A **finisher unit** on laser printers and MFDs can perform functions like stapling pages or punching holes for binders. Ensure printer settings are configured to select the finisher as an installed output option.

- **Incorrect page orientation**: Set the correct paper size and orientation for the print job to ensure proper finishing/binding. Users may find it tricky to paginate and select the correct output options, especially for booklet printing which applies staples to the middle of the sheet. The printing preferences dialog icon shows the binding edge. Test settings on a short document first.
- **Hole punch**: Exceeding the maximum number of sheets can cause jams. Send print jobs in batches within the permissible sheet count for the finisher unit. Note that the maximum sheet count may vary based on paper weight.
- **Staple jam**: An excessive number of sheets can cause staple jams, bending and sticking a staple within the punch mechanism. Remove the stable cartridge and release the catch to remove stuck staples.

10.3.5 - Print Job Issues

If there is no hardware or media issue, investigate the OS print queue and driver settings.

Print Monitors

In Windows, display and print functions are handled by the **Windows Presentation Foundation (WPF)** subsystem.

- A WPF print job is formatted using the **Page Description Language (PDL)** and spooled in the logical printer's spool folder within%SystemRoot%\System32\Spool\Printers\
- The print monitor transmits the print job to the printer and provides status information.
    - If a problem occurs, the printer sends a status message back to the print monitor, which displays a desktop notification.
- For networked printers, a redirect or service on the local computer passes the print job from the local spool file to the spoiler on the print server, which then transmits it to the printer.

Print Queue and Spooler Troubleshooting

- A backed-up print queue indicates multiple pending print jobs.
    - Can occur when printer is offline, out of paper, low on ink/toner, or due to an error processing a specific job.
- In Windows, access the printer through Windows **Settings** and open its print queue.
    - Try restarting the job by right-clicking the document name and selecting **Restart**.
    - If that doesn't work, delete the print job and try printing again.
    - If you cannot delete a job due to a backed-up or stalled queue, stop and restart the Print Spooler service.

Tray Not Recognized

An unrecognized paper tray can prevent jobs from printing or cause failures.

- Driver issues: Ensure the driver is configured to recognize all the installed trays. Check for driver updates from the printer manufacturer's website.
- Physical Connection: Ensure the tray is properly seated in the printer. Reseat the tray or ensure it's loaded with the correct paper.
- Printer Settings: Verify the correct tray is selected in both the printer settings and print driver settings. In multi-tray systems, jobs may fail if an unrecognized tray is assigned as the default.
- Restart: Power cycle the printer and computer to refresh settings.

Frozen Print Queue

- Stop and Restart the Print Spooler Service.
- Clear the Spooler Cache:
    - Stop the Print Spooler service.
    - Navigate to the spool folder (%SystemRoot%\System32\Spool\Printers\) and delete all files inside.
    - Restart the Print Spooler Service.
- Check for Corrupt Print Jobs: Sometimes a particular print job may be corrupt and cause the entire queue to freeze. Deleting the problematic job can restore functionality.

Garbled Print Issues

Oot