# Resources:

[CompTia A+ practice exams and quizzes](https://www.examcompass.com/comptia-a-plus-certification-exam-220-1001-cpu-quiz)

<https://www.professormesser.com/>

W3 comptia

Comptia reddit

Test king

passcomptia.com

# Basics:

Dress code: polo shirt, khakis and dark shoes

Don’t use anything without permission

Abstain from learning passwords (have them put in the password for you)

do not yell at or accuse clients

**Expectations and follow-up:**

provide updates if fixes take longer than expected

provide repair options if applicable

document your repair progress: describe the problem, the time and day you started, hours you worked and list of replaced parts

follow-up later to confirm satisfaction

**Electrostatic discharge (ESD):**

if you open up the computer you have to worry about this... ESD wrist strap and mat

put electrical components in anti-static bag

Always disconnect power before repairing a computing device

Follow disposal requirements for environmentally harmful objects

lift with your back

check for hot components before working on them

**Computer has 3 major components:**

* Hardware
* Operating System
* Applications (software)

**The computing process:**

* Input
* Processing
* Output

**You need to know the specific path to tech tools on each OS**

Windows 7:

* Start > Control Panel (Classic or Category view by selecting large or small icons)
* Start > All Programs > Accessories > System Tools
* Start > type “cmd” in the search box or in run program

Windows 8:

* Click the down arrow on the lower right of the Start screen and scroll all the way to the right in the list of Apps. In the “Windows System” category click Control Panel
* Right-click the start button > select control panel
* In the Start screen, click the down arrow to open the Apps list. Scroll to the right to see the “Administrative Tools” category
* Right-click the start button > select control panel > Administrative tools
* Start > type “cmd” in the search box or in run program
* Right click start button and select Command Prompt

Windows 10:

* start > type “control panel” in search
* Press the Windows logo key and select “Settings”

MacOS

* Click the Apple icon and select “System Preferences”
* With the Finder in focus, Click “Go” > “Utilities”

Linux

* Access the terminal Start > type “cmd” in the search box or in run program with CTRL-ALT-T

# CPUs:

**External Data Bus** provides a channel for the flow of data and commands between the CPU and RAM. The CPU uses registers for temporary storage of internal commands and data

**Registers:** EAX, EBX, ECX, EDX for 32 bit and RAX, RBX, RCX, RDX for 64 bit

EDB went from 32 to 64 bits (the basis for 32 and 64 bit processing)

x86 processors are 32 bit, x64 bit processors are 64 bit

x86-64 are still 64 bit because 64 bit processors can run 32 bit software

Arithmetic Logic Unit (ALU)

Clock wire (CLK), a single charge is a clock cycle. Clock speed is the max number of cycles for the CPU**.** Hz: 1 cycle, MHz: 1 million cycles, GHz, 1 billion cycles (per second)

**System Crystal** determines the speed. A quartz oscillator similar to the one in a wristwatch

Real processor speed is the CPU clock but the actual speed is determined by a variety of factors including, clock speed, CPU architecture, bus speed, bus width, L1/L2 cache sizes, operating system capabilities

bit, byte (8 bits), word (16 bits), double word (32 bits), paragraph/quad word (64 bits)

**MCC (Memory Controller Chip)** sends bits from RAM to CPU

**The Address Bus** connects the CPU to the MCC. The number of wires determines the maximum amount of RAM a CPU can handle. These wires are set exponentially…

1 kilobyte: 1024

1 megabyte: 1,048,576

1 gigabyte: 1,073,741,824

1 terabyte: 1,099,511,627,776

Thermal Design Power: the amount of heat a CPU generates

**Static ram (SRAM) is very fast temporary memory storage on a CPU (faster than DRAM)**

level 1 cache: smallest and fastest, first check

level 2 cache: mid point between speed and size, secondary data

level 3 cache: slowest and largest, shared among cores

32 bit vs 64 bit CPUs: 2 to the power of 32 or 64

**64 bit CPUs enable you to use more than 4gb of ram**

All modern CPUs can run both 32 bit and 64 bit

**RISC:** reduced instruction set computer. A CPU design based on an instruction set that tries to improve speed by utilizing relatively few simple instructions

**CPU Extensions:** Virtualization support & **Integrated GPU,** allows certain CPU models to take over tasks normally executed by a dedicated graphics controller

Virtualization allows you to run other OSs within a single hardware platform

Modern CPUs have integrated graphics but a dedicated graphics card increases performance

**GPUs: graphics processing unit**

Modern video cards contain their own BIOS

**VRAM** is a special-purpose memory type used by graphics controllers

Most processors can use a process called **multithreading** or **hyper-threading (HTT)** to split a core into numerous virtual cores, which are called threads. Hyperthreading was developed by Intel for x86 CPUs. It does not double speed, increases only by 15% to 30%

**Multicore** is a type of CPU architecture in which a single physical CPU contains more than one execution core on a single die or chip. Each core has its own cache and the entire core might have a shared cache

**Overclocking** is a way to increase the performance of a device (e.g. a CPU, GPU, RAM, or motherboard) by running it at a higher speed than the rate tested and approved by the device manufacturer

modern CPU sockets are ZIF (zero insertion force) to prevent damage to fragile chips

If you snap off a pin you’ve pretty much wiped out the CPU

Intel and AMD products are not compatible. AMD tends to be a bit less expensive and Intel tends to be top of the line

**Intel:** LGA: land grid array. Pins are on the motherboard

**AMD:** PGA: pin grade array. Pins are on the CPU

**How to install a CPU:**

1. place the CPU on the motherboard
2. add thermal paste
3. place the heat sink
4. place the fan
5. plug in the fan to the motherboard

**passive cooling:** a heat sink with no fan

**active cooling (active heat sink):** a heat sink with a fan

**liquid cooling:** coolant is circulated through a computer, used on high-end systems for gaming and graphics-heavy machines

If the system shuts down after a few seconds or doesn’t turn on at all and you’ve checked that the computer has power, it’s probably a heating issue. Too much or not enough thermal paste, or the fan is not connected to the motherboard

Fan specifications: standard sizes are 80mm, 120mm, 200mm, variable speeds and noise levels. A heat sink dissipates heat through thermal conduction

# Memory:

Ram is volatile storage. The data is lost when the computer is turned off

The capacitors on the memory need constant electricity to run

In order for a program to run, it needs to be loaded to RAM first

DRAM: slower and less expensive than SRAM (asynchronous)

SRAM: synchronized to the system clock, used for CPU cache memory

SIMM: single inline memory module (discontinued). Transfers 32 bits per clock cycle

DIMM: dual inline memory module. Transfers 64 bits per clock cycle. 2 notches, 184 pins

**SDRAM types:** DDR input/output speed and latency increases with each generation

**SODIMM** and **micro-DIMM** for laptops

**DDR**: 1 notch, 184 pins

**DDR2**: 1 notch, 240 pins (200 pin SODIMM), 4 words per clock cycle,

**DDR3**: 1 notch, 240 pins (204 pin SODIMM), 8 words per clock cycle,

**DDR4**: 1 notch, 288 pins (260 pin SODIMM), 8 words per clock cycle

**maximum data transfer rate is 8x the frontside bus speed**

**clock speed is half the frontside bus speed**

* The number in front of DDRX refers to the frontside bus speed
* The number in front of PCX refers to the maximum data transfer rate

DDR2-400, 400Mhz FSB == PC2-3200, 3200 MB/s == 200MHz clock speed

Which of the following is the industry name used for DDR2-1066 modules?: (\*8) PC2-8500

What is the peak transfer rate of a DDR2-533 module?: (\*8) 4266 MB/s

The different DDR types are not compatible

Make sure your motherboard can handle the amount of ram you want to install

Avoid mixing ram sizes and speeds, it can cause stability issues

Single sided and double sided ram, must have a motherboard that supports it

ECC and parity ram: these types of ram can only be used on particular motherboards

This type of ram is on big server systems, it checks for and corrects errors automatically

A motherboard with color-coded memory slots provides support for **multi-channel memory architecture… Dual channel mode, triple channel** and **quad channel**

In order to take advantage of the performance benefits offered by the multi-channel memory architecture, RAM has to be of the same type, speed and capacity.

Windows Memory Diagnostic Tool and Memtest86+ (open source software) used to check bad memory

NMIs (non maskable interrupts) can sometimes be RAM problems, but not necessarily

* Blue screen of death
* Spinning pinwheel of death on MacOS

**Which type of memory allows for permanent data storage?: DVD-RAM**

# BIOS:

**BIOS** (basic input/output system) is programming stored on a physical chip that is used to talk to the different pieces of hardware. Stored on the motherboard in the form of nonvolatile memory called **ROM** (read-only memory). Software used to start your computer.

Modern systems use **UEFI** (Unified Extendable Firmware Interface). Features include:

* mouse support
* GUI
* DRM support
* secure boot
* network access

UEFI also allows you to boot from large (>2.2 TB drives) GUID partition table (GPT) disks. Also supports FAT and removable media. Includes a pre-boot environment: This is not an operating system, it has its own shell, drivers and applications. Browse the internet, backup a storage drive, remote diagnostics, even without an OS

**Windows stores device drivers in the registry**

**research the windows registry**

When you need to update BIOS/UEFI, you have to **flash the ROM (aka firmware updates)**

**firmware upgrades:** ROMs on older systems, flash memory on newer systems

Upgrades are rare and unnecessary unless you need to improve performance or fix bugs

Identify BIOS version through msinfo32. Interrupting the process during installation might brick your device.

**BIOS options:** press a “secret” button. Windows 8 and Windows 10 have a fast boot option that require disabling in order to access BIOS

* Set boot order, drive settings
* RAM - view and configure memory settings
* enable or disable optical drive
* monitor computer hardware, temperature, voltage information
* enable secure boot: digitally signs known-good software. Software won’t run without the proper signature
* BIOS password / User password needed to start the OS
* set an administrator/supervisor password that restricts BIOS changes
* chassis intrusion detection/notification
* Full disk encryption: Microsoft Bitlocker that BIOS integrates with Trusted Platform Module (TPM)
* LoJack (track a PC’s location if stolen, install a keylogger, remotely shut down). Remains on the system even if the OS is reinstalled
* activate virtualization support

Hardware and hardware cards sometimes come with **option ROM** that loads BIOS

**in modern PCs, BIOS contents are stored in flash memory and EEPROM**

**CMOS** (complementary metal-oxide semiconductor) is a small bit of nonvolatile memory (system ROM chip) that stores BIOS/UEFI settings, which can be adjusted using the system setup utility. It also handles the system’s RTC (real time clock). You can restore this to default settings by doing a **CMOS clear.** You have to tinker with the motherboard to do this, it’s a CLRTC jumper or a battery that you need to take out, on older systems.

If you lose CMOS settings, here are some common errors to troubleshoot:

* CMOS configuration mismatch
* CMOS date/time not set
* BIOS time and settings reset
* no boot device available
* CMOS battery state low

**POST** (power on self test): also stored on system ROM, performs preliminary hardware checks when the computer turns on and communicates results through **Beep Codes** and text messages

**POST card:** something to snap onto your computer to diagnose problems with a dead computer

When you turn on the computer it goes through a **boot sequence**:

1. power good
2. CPU
3. POST
4. **bootstrap loader (BIOS)/boot manager (UEFI)**
5. operating system

The **motherboard** is the main component of the computer (circuit board)

**Motherboard connectors:**

* CPU socket
* memory slots
* bus slots (various components that add capabilities)
* storage device cable connectors (SATA, PATA)
* front panel connectors (pwr button, reset button, LEDs, etc)
* USB connectors
* modern motherboards also contain an **M.2 SLOT** for an M.2 SSD

**Chipset** determines the processor and ram required. Chipsets were consolidated into these two types:

1. Older motherboards contain **Northbridge** and **Southbridge** chipsets.
   1. Northbridge managed communications between CPU, PCI express bus and memory
   2. Southbridge managed standard PCI slots, SATA connectors, USB hubs, etc.
2. Newer motherboards have a **PCH (Platform Controller Hub)** chip. Functions of the Northbridge chip have been integrated into the CPU.

**Form Factors:** Standard measurements for case, motherboard and power supply

AT was the old form factor and **ATX** form factor is the standard now

The main power connector used in modern ATX motherboards is a 24-pin connector

**Standard ATX** (12” / 9.6“), good for servers

**micro ATX (uATX)** (9.6” / 9.6“), good for desktops that don’t need extra expansion slots

**ITX** and **Mini-ITX** motherboards are low power and good for single purpose computing like streaming media. They are also screw compatible which allows them to fit in any traditional ATX or uATX case

A computer bus provides **Expansion Slots:** the expansion bus gets its own clock

PCI: shorter slots are 32 bit. Longer slots are 64 bit, Parallel communication speeds:

133 MB/s (32 bit @ 33MHz)

266 MB/s (32 bit @ 66MHz or 64-bit @ 33MHz)

533 MB/s (64 bit @ 66MHz)

PCIe (PCI express): Replaced PCI, PCI-x and AGP (accelerated graphics port). Serial communication. Slower devices don’t slow down everyone, unidirectional serial “lanes”. x1, x2, 4, x8, x16, x32 lanes of unidirectional (serial) communication

v1.x: 250 MB/s

v2.x: 500 MB/s

v3.x: ~ 1 GB/s

v4.x: 2 GB/s

v5.0: ~4 GB/s

mini-PCIe: laptop version of PCI, low power and lies flat

**Riser Card** adds more PCI slots and changes the directions of the slots

Expansion cards include: video cards (GPU) that usually come with fans, audio cards, network cards (NIC), multi-port Ethernet card, USB expansion card, storage cards (M.2), eSata card, check motherboard documentation before buying and installing cards.

**Installing expansion cards requires four steps:**

1. Knowledge that the card works with your motherboard/OS
2. Installation without damaging the card (make sure the card is properly seated and screwed in)
3. device drivers: install the device then insert installation media if not detected automatically
4. verification: verify the new card is working properly

get images of these different types

**Troubleshooting expansion cards:** in Device Manager, a black ! On a triangle indicates a device is missing, Windows does not recognize the device, or there’s a device driver problem. The device may still work. A black downward-pointing arrow on a white field indicates a disabled device. Manually turned off or damaged. The ! Symbol is the most common error. Double-check device connections. Right click and select “update driver”.

**Computer Power Supply:** uses DC voltage. most power sources supply AC voltage

Power supplies convert 115V AC or 220V AC into DC power: 3.3V, 5.5V and 12V

Power supply tests are used to confirm voltage

**amp and volt:**

ampere (amp, A) - the rate of electron flow past a point… the diameter of the hose

voltage (volt, V) - electrical “pressure” pushing the electrons… how open the faucet is

**Wattage** is the main difference between power supplies… measured in A \* V = W

**Sizing a power supply:** calculate the watts required for all components. online calculators

A good rule of thumb is to get a PSU that runs at 50% capacity

**Current:**

US/Canada - 110 to 120 volts of AC (VAC), 60 Hz

Europe - 220-240 VAC, 50 Hz

since voltage varies by country, power supplies switch between 110-115V / 220-230V

sometimes it is a switch you have to flip or the power supply might do it automatically

if the PSU doesn’t turn on, it could be a voltage problem

be careful not to provide too much voltage to a machine built for lower voltage, it could fry all your electronics!

**24-pin motherboard power:** provides +3.3V, +/-5V, +/-12V

20 pin connector was the original ATX standard, 24 pin was added for PCI Express power

you can connect a 24 pin connector to a 20 pin motherboard. Some PSUs are 20+4pin

**Power supply output:** positive and negative voltage, voltage is a difference in potential. the electrical ground is a common reference point

different voltages for different components:

+12V: PCIe adapters, hard drive motors, cooling fans, most modern components

+5V: some motherboard components, many components are now using +3.3V

+3.3V: M.2 slots, RAM slots, motherboard logic circuits

-12V: older machines use this for integrated LAN, older serial ports and some PCI cards

-5V: modern power supplies probably won’t have this, but used for ISA adapter cards

# custom computer systems:

audio/video editing workstation such as graphics workstations, computer aided design (CAD), computer aided manufacturing (CAM): They need an SSD drive, specialized audio card, high-end video card, and RAM maxed out

virtualization workstation: every OS needs its own memory, max ram and CPU cores

gaming PCs: specialized GPU, high definition sound card, high-end cooling, SSD drive

network attached storage device: NAS (access from everywhere). Used for media streaming and file sharing. Gigabit NIC and a RAID array

**standard thick client:** apps run on the local PC, must meet hardware requirements

**thin client:** apps run on a remote server, Virtualization Desktop Infrastructure (VDI). minimal hardware requirements, but big network requirements

# Storage:

HDDs (hard disk drives) are ATA drives

Non volatile magnetic storage. Random access, can access any part of the drive

Lots of moving parts: spinning platters, moving actuator arm, mechanical components limit access speed but are easy to break. Spins at a rate measured in revolutions per minute

Rotational speed (RPM) Average rotational latency

15,000 2ms

10,000 3ms

7,200 4.16ms

5,400 5.55ms

USB flash drives use flash memory: EEPROM (electrically erasable programmable read-only memory). Non-volatile memory and no power required to retain data. Limited number of writes. Compact flash (CF), Secure Digital (SD), miniSD and micro SD, xD-Picture card

mSATA (micro sata), used for laptops and mounted directly on motherboards

**Desktop HDD form factor size is 3.5”**

**SSD: solid state drives, non-volatile memory. Most common form factor is 2.5”**

SSD host interfaces include:

It’s more like RAM than magnetic storage, it uses flash memory

Sata/AHCI and PCIe/NVMe are the interfaces and protocols used by SSDs

When buying an M.2 drive, read the box to confirm if it needs SATA or NVMe

NVMe: logical device interface designed to access storage devices attached via PCIe

NVMe drive uses an M.2 interface. This is a smaller storage device that is as fast or faster than SATA with no SATA power cables. PCI express bus connection: 4 GB/s throughput or faster. Different connector types, need to be compatible with the slot key/spacer.

B key: PCIe x2, M key: PCIe x4, B & M key: some drives support both

An M.2 key is a notch on the pin contact surface of an M.2 expansion card which prevents insertion into an incompatible socket. The M.2 key IDs include 12 available letters from A to M. These letters correspond to the locations of notched pins on the card's contact surface and designate which interface the card is compatible with. M.2 expansion cards that are used for solid-state storage applications have key IDs of B and M. The B-keyed M.2 SSD cards use 2 PCIe lanes (lower read/write speed), while M-keyed M.2 SSDs use 4 PCIe lanes (higher read/write speed). M.2 SSDs with 2 notches on the card's pin contact surface (B + M) increase the card's compatibility as they can be installed in either of the two types of expansion slots on the motherboard.

**SSHDs** are a mixture of ATA and SSD that combine high capacity and performance with lower price. AKA hybrid drives. SSD caches the slower spinning hard drive data, increases speed without the cost of an SSD-only drive. Same form factor as a normal hard drive or SSD (3.5”)

A Disk Defragmenter is a software tool used to rearrange data on magnetic drives in order to improve system performance. Defragmentation results in faster read/write operations of a magnetic hard drive's read/write heads because defragmentation consolidates data into the smallest contiguous regions. This means that the heads can access data sequentially without seeking data fragments in different areas of a disk.

**AHCI: advanced host controller interface,** must be turned on so that it recognizes different drives. before installing an OS, make sure AHCI is turned on to use newer SATA feature

Logical Block addressing: LBA, takes discrete information stored in blocks on your hard drive and offers them up to RAM as necessary

**The file system sits between the storage device and the OS**

**RAID: Redundant Array of Independent Disks**

Raid 0: striping, files are split between two or more physical drives (high performance, no redundancy)

Raid 1: mirroring, files are duplicated. Uses double the disk space but provides redundancy

Raid 5: Striping with parity, 3+ drives, more efficient use of disk space with redundancy

Raid 1+0 AKA raid 10: Nested RAID, 4+ drives. Provides performance of RAID 0 with redundancy

Hot swappable drives: add and remove while the system is running

Examples include, SATA drives, eSATA drives and USB drives

Drive chassis of two or more drives. Easy to repair. Combine with RAID for 100% uptime

Software RAID: the OS takes care of RAID configurations

Hardware RAID: hard drive controller invisible to OS. designed for speed and more expensive

The new RAID array will appear as a single drive

LPs are legacy data storage, then we got optical discs

small bumps with a laser beam, microscopic binary storage

Burners don’t create bumps, they darken photosensitive dye to write to discs.

research different CD/DVD types

DVD-R, DVD+R, DVD-RW, DVD-R-DL

CDFS: compact disc file system

CD-ROM: 700 MB, 80 minutes of uncompressed audio

DVDs have region codes

DVD-ROM: 4.7 GB single layer, 8.5 GB dual layer

Blu-ray disc: 25 GB single layer, 50 GB dual layer

mini Blu-ray disc: 7.8gb single layer, 15.6gb dual-layer

Blurays require UDF format

Blu ray discs include HDCP, a content control system designed to prevent piracy

Blu-ray formats: bd-video, bd-rom, bd-r and bd-re

BD-R: blu-ray disc recordable. This storage media can be read, but not written to

BD-RE: blu-ray disc erasable

mini Blu-ray disc

**USB:**

usb 1.0: 1.5 mbps & 12 mbps

usb 2.0: 4.8 mbps

usb 3.0: 5 gbps

usb-a points to the pc (downstream), usb-b points away from the pc (upstream)

usb 3.0 b connector

memorize the various types of usb connections

**flash media:** flash drives, compact media (CM), smart media card (SMC), secure digital (SD), miniSD, microSD

# Laptops:

**Fn key** on laptops overcomes keyboard size restrictions and adds additional functionality

Also serves secondary functions like toggling between LCD / external monitor / both

**LCD switch:** when you plug into a monitor and close the laptop, you may still use the laptop

**Wireless control:** airplane mode, secure areas. Look for a status switch

May include 802.11, Bluetooth and cellular

**Volume** **settings**: often includes a mute option. Maybe a physical dial or a button

**Brightness** backlight

Media options: play, stop, rewind, etc.

Some laptops include GPS

Laptops use various internal hard drives: SSHDs, SSDs and Magnetic Disks

Most common magnetic **hard drive form factor size for laptops** is 2.5”

**SSD form factor sizes for laptops** are 2.5” and 1.8”

A laptop **smart card reader** provides access control

Optical drives (CD and DVD rom) are not as common on laptops due to size restrictions

In Laptops, CPUs are designed for mobility, power management, smaller size and less heat. CPUs are replaceable but not upgradeable. Lots more integrated features like memory and video controllers

**Laptop Wireless Card**

802.11 wireless connection (wifi)

WWAN (cellular)

WPAN (bluetooth) is usually about 10 meters… high speed communication… Bluetooth security feature: PIN Code

set device to discoverable mode, select discovered device and enter or confirm PIN

**Laptops have multiple antennas (eg. WiFi, aux, Bluetooth) and they wrap around the top of the screen**

Not all laptops come with CPU integrated graphics, but most GPUs are not upgradeable on laptops

**laptop webcam:** for video capture, usually includes both audio and video

**microphones** on laptops are usually low quality, only good for video calls

Laptops have **external AC adapters** instead of power supplies. These may be auto-switching or fixed input of 110 volts or 220 volts. Converts AC to DC. Laptops have DC jacks

Laptops carry **lithium-ion batteries**

the **touchpad** functions as a pointing device on laptops

**OLED** on laptops is thinner and lighter than LED but not quite ready for laptops. More costly and power-hungry than LCD?

**LCD** is the most common display technology. These are backlit. Some laptops have inverters that convert DC to AC. If the screen isn’t working, verify backlight. Look closely and use a flashlight. May need to replace the LCD inverter or display

Newer laptop models may include rotating or increasingly mobile screens

**Digitizer** is used on laptops and touchpads as alternatives to keyboards, although some devices are hybrids of a touchscreen and a laptop

Older laptops use **CCFL** – Cold Cathode Fluorescent Lamp. Higher voltage and power needed and added thickness to display

**Integrated GPU is the most difficult hardware component to replace on a laptop**

A **laptop inverter** has two functions: supplies voltage to backlights in older LCD panels and converts DC power into AC power

**docking stations** usually offer additional ports and capabilities compared to port replicators. External mouse and keyboard, desktop adapter cards, avoid cable issues

protection against **laptop theft** includes: Laptop locks and cable locks

# Mobile Devices:

Portable devices combining the capabilities of mobile phones and handheld PCs are commonly called smartphones

Tablets are mobile devices. Single-screen touch computers. Larger than 7” diagonally. Usually great for media and application support. Specialized applications, productivity, games, utility

Smart phones: 3.5 – 6” diagonally. Mobile applications and other apps. Mobile communication

technologies that enable mobile device connectivity: IR, Bluetooth and NFC

Wearable tech: an extension of your phone on your body, fitness monitors

Virtual reality: input from the read world interacts with the virtual world

Used for gaming, industrial design, art, enhanced video and image viewing

Augmented reality is a virtual augmentation of the physical world

E-readers are specialized devices for book reading / document access. Black and white screen that performs well in direct light. Exceptionally long battery life. Network access: WiFi/Cellular

GPS are also mobile devices

**Mobile Device accessories:**

Wired: connects to 3.5 mm TRRS (tip-ring-ring-sleeve) connector… analog audio jack

Wireless: bluetooth headsets used for hands-free audio

Gamepads can be used on mobile devices (bluetooth)

microSD storage functionality on android

mobile phones can be used as wifi hotspots or physically tethered to computers to provide internet access

phones have baseband radio processors. Has its own firmware and memory

WWAN is a WAN technology that uses cell towers to provide wireless signal coverage for mobile devices

**Phone updates:**

Phones are radios. baseband radio processor is a network interface for your radio, this isn’t WiFi or Bluetoooth. Has its own firmware and memory, proprietary. Real-time operating system. Firmware can be updated over the air (OTA), invisible to the end user.

PRL (preferred roaming list). CDMA networks (verizon, sprint) allows your phone to connect to the right tower. Can be updated over the air (OTA). PRL is a database on a mobile device containing bands, sub-bands and service provider IDs allowing the device to establish aconnection with the right cell phone tower

PRI (product release instructions): radio settings, ID numbers, network codes, country code, etc. Also updated OTA. PRI can be used as a reference during a mobile device update process

**IMEI.** International Mobile Station Equipment Identity. Identifies a physical mobile device. Every phone has a different IMEI and can be used to allow or disallow access.

**IMSI.** International Mobile Subscriber Identity. Identifies the user of a mobile network and is provisioned by the SIM card. Swap the SIM to move between phones.

Micro-USB and Mini-USB is used to plug in mobile devices

USB-C is a 24-pin double sided connector used for both hosts and devices

This connector acts as USB 3.1 and 2.0, and also includes analog audio option

USB-Micro B can be used on an Android device for mobile device synchronization

Lightning connector for iPhones offer higher power output and can be inserted either way

**Proprietary mobile interfaces:** there were lots of different cables for early mobile phones but the EU changed things, adding common cables for all data-enabled mobile phones sold in the EU

**NFC (near field communication):** small amounts of data transferred between phones, such as payment data, transportation, in-person information exchange or even bootstrap for other wireless such as bluetooth pairing. It also allows the phone to function as an access token or identity “card”. *Short range with encryption support.* Uses RFID.

**IR (infrared):** Your phone/wristwatch functions as a TV remote

**Post Office Protocol 3 (POP3):** used for Email retrieval. Downloads and optionally deletes from server. Legacy protocol but still used by some clients.

**Internet Message Access Protocol (IMAP4):** provides access to mail on a central server, mail is usually stored on the server and supports folders/server-side searching. Used for retrieving email messages from a mail server

**Simple Mail Transfer Protocol (SMTP):** allows you to send mail from a device to a mail server or between servers. Usually must send from a local or trusted device. Authentication is also required but may use different credentials from incoming mail. Not used to retrieve messages, only to send

Integrated message encryption with **S/MIME (Secure/Multipurpose Internet Mail Extensions)**

**Commercial email providers:**

Gmail: google email, splits inbox into tabs, IMAP4, POP3

Exchange Online (hosted email): Microsoft enterprise email with IMAP4 and POP3 support

iCloud Mail: Apple Mail, IMAP4 support only

Yahoo Mail: IMAP4 and POP3 support

**Phablets:** are a cross between a mobile device and a portable computer

Examples of universal connection types that enable mobile device synchronization:

* IEEE 802.11
* IEEE 802.3
* USB-C
* Cellular
* Bluetooth

# Printers:

**Printer:** color and B&W output. paper documents and photos

All-in-one - AIO: printer, scanner, copier, fax

connectivity: usb, ethernet, 802.11 wireless, bluetooth/infrared

duplex: printing on both sides of paper

collate: print pages in order. non-collated: 1,1,1,2,2,2,3,3,3,4,4,4

orientation: portrait vs landscape

quality: resolution, color, grayscale, color-saving mode

wired device sharing: USB type B is most common for older printers

parallel: centronics on the printer, DB-25 on the computer

wireless device sharing, bluetooth printer,

wireless printer (infrastructure mode)... many devices using an access point

802.11 Ad hoc mode, no access point, direct link between wireless devices

integrated print server: print directly to the printer, jobs queued and managed on printer

cloud printing: print to the cloud, useful for mobile devices, the cloud sends jobs to printer

You can share a printer from an OS. Common on Windows devices. Commonly uses udp/137, udp/138, tcp/139 and SMB/CIFS

printer drivers are specific to a printer model, 32bit or 64bit

Bonjour discovers Apple devices on the LAN. part of macOS but can be added to Windows

AirPrint: print from iOS devices to compatible printers

**printer data privacy:** user authentication, everyone can print, set rights and permissions to printing vs. managing the printer

**Print and scan caching**: click print, local system creates a file of the output, printing is done from a spoof file. Spoof file is deleted when done, but not always. Some printers can hack these spoof files to see what you’ve printed. Another security measure is regular clearing of printer’s cache memory

Printing speed is measured in PPM (pages per minute)

**printer wired connection types:** USB, Serial, Ethernet

**printer wireless connection types:** 802.11x, bluetooth

**legacy parallel printer ports:** LPT, DB-25

**remote printing network protocols:** LPD/LPR, IPP (SMB/CIFS also enables printing)

**Laser printer:** very high quality, fast printing speeds. requires on-printer memory

*Duplexing assembly*: printers usually print on one side, not two sides simultaneously, but some laser printers can turn the page around to print both sides.

**Steps to laser printing:**

1. Processing: build the entire page in memory
2. Charging: prepare the drum with a negative electrostatic charge. *Corona wire* on older printers and *primary charging roller* on newer printers
3. Exposing: laser writes the image, neutralizing negative charge on the print area
4. Developing: add negatively-charged toner to the *imaging drum*
5. Transferring: move the toner from the drum to the paper
6. Fusing: uses heat and pressure to melt the toner onto the paper
7. Cleaning: wipe off excess toner to prepare for the next print job

imaging drum holds a representation of output image drawn on its surface by laser

transfer belt (roller) picks up all the color layers of an image from imaging drums onto paper

fuser assembly applies heat and pressure to bond toner to paper

**Laser printer maintenance kit:** standard maintenance kits are a set of printer replacement parts. Replacement feed rollers, new fuser unit, etc. When to perform maintenance? check the printer page counter. power down and replace components, fuser units are HOT. reset the page counter when done

**laser printer calibration:** different toner cartridges print with different densities. Some dark, some light. Laser printer calibration adjusts the density. Can be automated or a manual process. Every printer is different, check the printer manual.

**laser printer cleaning:** check manufacturer recommendations. Water or IPA (alcohol). Outside, damp cloth. Inside, wipe dust away. Don’t use a normal vacuum cleaner or compressed air, clean rollers with IPA. Use toner vacuum, magnetic cleaning brush and isopropyl alcohol to clean laser printers

replacing the toner cartridge: low doesn’t mean empty, look for messages

The toner can also contain the Organic Photoconductor (OPC) Drum. This drum is sensitive to light, keep it in the bag. Don’t forget to remove packing strips from the new drum

**separation pad and pickup roller** prevent multiple sheets of paper from being fed at the same time

**Inkjet (ink-dispersion) printer:** relatively inexpensive technology. Quiet, high-resolution. printer ink eventually fades over time and cogs easily. Ink cartridges place drops of ink onto a page, pulled from a set of cartridges. CMYK cartridges. Print head: some consumer printers integrate the print head onto the ink cartridge. Change the cartridge, get a new print head. *Feed rollers* pick up and feed paper through the printer. Also supports duplex printing

Carriage and belt: ink cartridges are moved over the paper. Carriage may include its own print head. Belt moves the carriage back and forth.

Inkjet printer calibration: aligns the nozzles to the paper. Lines should be crisp, colors should align

ink cartridges are the most expensive part to replace in an inkjet printer (proprietary)

**Inkjet printer maintenance:** cleaning print heads. Small droplets of ink and small holes in a print head. Clogged heads is a big issue. Many printers automatically clean every day. Output has streaks or sections of missing color. Cleaning process can be started manually, only takes a few minutes. Clearing jams: remove tray paper and any loose paper. Use firm pressure to remove paper from the path, do not rip. Open the printer and check for any scraps of paper.

**Thermal printer:** uses thermal paper, turns black when heated. No ink! Very quiet. Paper is sensitive to light and heat. Usually used to print receipts. Feed assembly, pull paper through the printer, relatively small paper path. Full-length heating element, no moving print head. Different thermal printers are using different sizes. Used as a PoS terminal component

**Thermal printer maintenance:** paper replacement, relatively inexpensive. the replacement process is easy. Cleaning the heating element: Liquid cleaner, isopropyl alcohol (IPA). Get a cleaning pen, check the manufacturer's recommendations. Swab gently, usually small areas. use a cleaning card, which cleans the head and paper pathways. Removing debris: blow air out the printer and wipe it out with a damp cloth. Avoid using a vacuum unless it’s designed for computers… resists static buildup/discharge

**Impact / dot-matrix printers**: Tractor feed: paper pulled through with holes on the sides of the paper, instead of using friction. Continuous paper feed, perforation between pages. Impact printers do not need calibration. This is the only kind of printer that can print multipart forms. Uses an inked ribbon to print. Print head with a small matrix of pins. Presses against a ribbon to make a mark on paper. Low cost per page. Noisy. Niche uses, car rental, airports.

Dot-matrix print head: moves back and forth, pins hit ribbon and paper

**Virtual printers:** files are saved in a special file type, must use the command line to copy the file to the printer. file formats include: PDF, XPS, graphic image

**3D printers:** prints in 3 dimensions. additive manufacturing, melt plastic filament in layers to create the object. used for rapid prototyping…

**scanner:** connected via USB or 802.11 wireless

Different form factors: all-in-one or flatbed

May include an ADF: automatic document feeder

# Networking:

Learn the OSI model

figure out what layers certain network devices /protocols operate on

Where does the term IP come from? (internet protocol)

The internet is made up of Packets of TCP and UDP with application data inside them

Multiplexing: use many different applications at the same time

the difference between TCP and UDP

TCP: connection-oriented. A formal connection with set-up and close. “Reliable” delivery. Recovery from errors and can manage out-of-order messages. Flow control, the receiver can manage how much data is sent. Everytime a packet is sent, the receiving node sends back an acknowledgment of package receipt

UDP: connection-less, no formal open or close to the connection. “Unreliable” delivery. No error recovery and no acknowledgment, no reordering of data, no flow control. Sender determines the amount of data transmitted

IPv4 sockets

sent packets contain server IP address, protocol, server application port number

received packets contain client IP address, protocol, client port number

difference between ephemeral and non-ephemeral ports

Non-ephemeral ports – permanent port numbers

Ports 0 – 1023

usually on a server or service

Ephemeral ports – temporary

ports 1025 – 65535

determine in real time by the client

TCP and UDP ports can be any number between 0 and 65535

Most servers/services use non-ephemeral port numbers.

Port numbers are for communication, not security

Service port numbers need to be “well known”

TCP port numbers aren’t the same as UDP port numbers: eg. TCP 80 and UDP 80 are not the same thing

FTP: transfers files between systems. tcp/20 (active mode data) – tcp/21 (control)

TFTP is used to transfer files through a LAN (on UDP)

authenticates with a username and password. Some systems use a generic/anonymous login

full-featured functionality: list, add, delete, etc.

Telnet – telecommunication network – tcp/23

Provides username & password authentication

Enables remote login and command execution

Transmits data in an unencrypted form

SSH – secure shell: encrypted communication link – tcp/22

SMTP – tcp/25

POP3 – tcp/110

IMAP4 - tcp/143

DNS – Domain name system. Converts names to IP addresses udp/53

HTTP – tcp/80

HTTPS – tcp/443

RDP (remote desktop protocol) - tcp/3389

**HTTPS:** network protocol that secures web traffic via SSL/TLS encryption

difference between SMB/CIFS and NetBIOS

**SMB (Server Message Block) – Protocol used by Windows. File sharing/printer sharing**

Also called CIFS (common internet file system)

Using NetBIOS over TCP/IP: used when a WINS server tries to resolve a host name into an IP address on Windows based LAN. The function of the NetBT protocol is to allow NetBIOS services to be used over TCP/IP networks.

udp/137 – NetBIOS name services (nbname)

udp/138 – NetBIOS datagram service (nbdatagram)

tcp/139 – NetBIOS session service (nbsession)

Modern Windows devices don’t need NetBIOS, they just use tcp/445

AFP (Apple Filing Protocol): tcp/548

Works with SLP (Service Location Protocol): tcp & udp/427

also offers full-featured functionality: copy, move, delete files

SLP permits automated discovery of networked services on Local Area Networks (LANs)

research DNS and DHCP

DHCP (Dynamic Host Configuration Protocol). Automated configuration of IP address, subnet mask and other options. udp/67, udp/68

Requires a DHCP server: server, appliance, integrated into a SOHO router, etc

Dynamic/pooled. IP addresses are assigned in real-time from a pool. Each system is given a lease and must renew at set intervals

DHCP reservation: addresses are assigned by MAC address in the DHCP server. Quickly manage addresses from one location

LDAP (lightweight directory access protocol). Store and retrieve information in a network directory, commonly used with Microsoft Active Directory - tcp/389

what is the difference between snmp and snmp trap?

SNMP – Simple Network Management Protocol. used in network management systems to monitor network-attached devices. Gather statistics from network devices:

An SNMP management station receives SNMP notifications on (queries udp/161)

An SNMP Agent receives requests on (traps udp/162)

v1 – The original. Structure tables, unencrypted

v2 – data type enhancements, bulk transfers, also unencrypted

v3 – message integrity / authentication / encryption

**Network Interface Card (NIC):** Every device on the network has a NIC. Specific to network type. Multiple NICs needed for multiple network types. Single port, multiport, copper, fiber. A computer component designed to enable network access

**Repeater**: Used to boost copper or fiber connections, convert one network media to another (e.g. copper to fiber) and also used to extend network reach. A **hub** is a multiport repeater. Traffic going in one port is repeated to every other port. Half-duplex. One device sends data at a time. Becomes less efficient as network speeds increase. Max speed of 10 megabits / 100 megabits per second (and even these are rare)

**bridge:** a switch with two to four ports. Typically capable of connecting fewer network segments than switch (fewer physical ports), older and less effective type of network device in comparison to network switch. Connects different physical networks and different topologies. Gets around physical network size limitations/collisions. Distributes traffic based on MAC address. A modern bridge is a **wireless access point**, it bridges wired ethernet to wireless. Forwarding decisions are made in software

the features of a network bridge:

typically capable of connecting fewer network segments than switch (fewer physical ports)

Older and less effective type of network device in comparison to network switch

the difference between routers, switches, hubs, repeaters and bridges

**Switches** are modern, multiport bridges. Typically capable of connecting more network segments than a bridge (more physical ports), newer and more effective type of network device in comparison to network bridge. Forwarding decisions made in hardware: Application-specific integrated circuit (ASIC). Forwards traffic based on data link address. Many ports and features. Injectors are used to provide Power over Ethernet (PoE).

A type of technology that enables sending data over wiring used for transmission of electrical power is known as: Ethernet over Power (EOP) AKA Power-line communication (PLC)

IEEE standard 1901. 500 megabits per second. Standard includes links to the premis, intra-building networking, vehicles, smart energy devices and more. Improves network performance by dividing a given network segment into separate collision domains

Multilayer switch includes routing functionality (AKA layer three switches). **Unamanaged Switches** are plug and play, fixed configuration (no VLANs). Very little integration with other devices. Less expensive. Switches improve network performance by dividing a given network segment into separate collision domains.

A network switch with configuration features that can be modified via a user interface is a managed switch.

**managed switches:** VLAN support. Interconnect with other switches via 802.1Q. Traffic prioritization, redundancy support via Spanning Tree Protocol (STP). External management via Simple Network Management Protocol (SNMP). Troubleshooting is done through port mirroring to capture packets. This type of network switch has configuration features that can be modified via a user interface

**Routers:** make forwarding decisions based on IP address. Often connects diverse network types: LAN, WAN, copper, fiber. A device designed to filter and transfer IP packets between dissimilar types of computer networks

Wireless Access Point (WAP/AP): an infrastructure device designed for connecting

wireless/wired client devices to a network

characteristic traits of a network switch:

Forwarding decisions made in hardware (ASIC)

Typically capable of connecting more network segments than bridge (more physical ports)

Sometimes referred to as multiport bridge

Newer and more effective type of network device in comparison to network bridge

Injectors are a dedicated device designed to supply power to PoE equipment

**Wireless LAN controllers**:centralized management of WAPs. Management functions: deploy new access points, performance and security monitoring, configure and deploy changes to all sites, report on access point use. Usually a proprietary system (like Cisco). The wireless controller is paired with access points. Can also be cloud-based, manage the console from anywhere

**Firewalls:** filters traffic by port number. OSI layer 4 (TCP/UDP). Modern firewalls can filter based on application. Can also be used to encrypt traffic into/out of the network to protect your traffic between sites. Firewalls can also proxy traffic. Most firewalls can be layer 3 devices (routers)

**research the difference between a cable modem and DSL modem**

**characteristics of DSL modems**

Dedicated bandwidth

Twisted-pair copper cabling

Telephone lines

**characteristics of cable modems**

Cabling that carries TV signals

Coaxial cabling

Shared bandwidth

**characteristics of fiber optic network cabling**

Immunity to electromagnetic interference

More suitable for carrying digital information than copper cabling

Used for network backbone cabling

typical maximum segment length for a copper twisted-pair Ethernet cable: 100 meters

**Cable modem:** broadband transmission across multiple frequencies (different traffic types). Data on the “cable” network: DOCSIS (data over cable service interface specification). High-speed networking: 4 Mbits/s through 250 Mbits/s and gigabit speeds too (though less common). Multiple services, such as data, voice and video. Transmission across multiple frequencies. Different traffic types. Network connections implemented with the use of a cable modem take advantage of: cabling that carries TV signals, coaxial cabling, shared bandwidth

**DSL modem:** ADSL (Asymmetric digital subscriber line). Uses telephone lines instead of cable. Download speed is faster than upload speed. ~10,000 foot limitation from the central office (CO). 52 Mbit/s downstream / 16 Mbit/s upstream are common. Faster speeds may be possible if closer to CO. Dedicated bandwidth and twisted-pair copper cabling.

**Dialup:** legacy network connection with voice telephone lines. Analog lines with limited frequency response. 56 kbit/s and up to 320 kbit/s with compression. Slow throughput so difficult to scale

**Fiber:** fiber optics is high speed networking. Converged services, voice/video/data. Enhanced features such as HD channels, 1Gbit/s internet access, 1 terabyte of cloud storage and 2 terabytes of DVR

**Satellite networking:** non-terrestrial networking used for remote sites. 50 Mbit/s down and 3 Mbit/s up. High latency, 250 ms up and 250 ms down. High frequencies – 2 GHz, line of sight/rain fade

**ISDN (Integrated Services Digital Network):**

BRI - basic rate interface (2B+D): two 64 kbit/s bearer (B) channels and on 16 kbit/s signaling (D) channel. PRI – primary rate interface delivered over a T1 (23B + D) or E1 (30B + D + alarm channel)… commonly used as connectivity from PSTN to large phone systems (PBX)

**Cable infrastructure:** Wires get run through the floor, ceiling or walls and into **patch panels…** A simple device consisting of multiple connector blocks and ports used for cable management. These are combinations of punch-down blocks and RJ-45 connectors. Runs from desks are made once and moving people across networks is as simple as unplugging the cable from one panel and connecting it to another

**SOHO router:** all in one device. Modem, router, switch, wireless AP, firewall, etc.

Routing and switching: routing to the outside world via WAN/DSL port. Switching local devices with one VLAN and several ports to plug ethernet cables into (eg LAN1, LAN2, LAN3, LAN4 etc)

Not much to configure, routes and switches by default

Access point settings: enable / disable frequencies: 2.4 GHz and/or 5GHz. Configure an SSID and a security mode (WPA2 preferable) with a pre-shared key or enterprise and set channel to one that is not currently in use to avoid causing interference with other networks in the area

WAN interface: automatically assigned via DHCP from the ISP, may require authentication

LAN interface: internal IP address and subnet mask of the router with DHCP and DNS

NIC configuration: wired, may not have many options. Ports configured for auto speed and duplex. Speed: 10/100/1000. Duplex, half/full. Wireless, enable/disable, SSID, password.

End-user device configuration: automatic, auto speed and duplex, DHCP addressing. Or static, need to configure IP address, subnet mask, default gateway and DNS servers

Network connections implemented with the use of a cable modem take advantage of: cabling that carries TV signals, shared bandwidth and coaxial cabling

**Configuring a SOHO firewall:** SOHO firewall prevents external devices from directly accessing the internal network. DMZ (demilitarized zone) are the midpoint between your internal network and the outside world. DMZ ports can be configured to allow unrestricted access. This is almost always a bad idea, consider creating more specific port forwarding rules or perhaps don’t allow access

**NAT (network address translation):** IPv4 is exhausted, only supports up to 4.29 billion addresses but there are over 20 billion devices connected. NAT serves (in part) to address this discrepancy. This is used to translate one address into another. You can set an IP address that is not in use on your local network and when that device wants to communicate to the outside world, it will be translated into your default gateway

**Configuring NAT:** For SOHO devices, this is automatic. Source NAT, aka PAT (Port address translation). All internal devices are translated to a single external address.

**Port forwarding:** 24x7 access to a service hosted internally (web server, gaming server, security system, etc). External IP/port number maps to an internal ip/port (does not have to be the same port number). Also called destination NAT or Static NAT: destination address is translated from a public IP to a private IP (does not expire or timeout)

**UpnP (universal plug and play):** allows network devices to automatically configure and find other network devices: zero-configuration. Applications on the internal network can open inbound ports using UpnP. No approval needed, used for many peer-to-peer (P2P) applications. Security issues, disable by default, only enabled if application requires it.

**Whitelist / blacklist:** content filtering, IP address ranges or a combination

Whitelist is more restrictive, nothing passes unless approved

blacklist: nothing on the “bad list” allowed. Specific URLs, domains, ip addresses

**MAC filtering:** MAC is the “hardware address”. A way to control what devices communicate through the router. Easy to find working MAC addresses through wireless LAN analysis (packet sniffer) and spoof them (fake a MAC address) to gain access so not a good security tactic

**Wireless channels and encryption:** configure for the highest encryption possible. WPA2-AES. WPA is less secure and WEP is not an appropriate option. Check your devices, some devices don’t allow additional encryption. Use an open frequency (channel), some access points will automatically find good frequencies. WPA/WPA2 Enterprise mode is suitable for large corporate networks but requires a RADIUS authentication server

Disabling SSID broadcast makes a WLAN harder to discover

Wi-Fi Protected Setup (WPS) simplifies network connectivity but is insecure

Which of the following is the best method to secure a small network lacking an authentication server? What is WPA2-PSK vs WPA2 Enterprise?

the characteristic features of a WPA/WPA2 Enterprise mode

Suitable for large corporate networks

Requires RADIUS authentication server

**Managing QoS (quality of service):** some routers have this option. Change traffic priority by application, port, or MAC address.

**IoT configuration:** home automation, mostly wireless, security is an issue

devices: thermostat, light switches, security cameras, door locks, voice-enabled smart speakers/digital assistants. Almost all of these devices communicate outbound, no special port mapping/NAT configuration required

**as a Service cloud computing options:**

IaaS: infrastructure, AKA hardware. eg web hosting provider. Instead of buying hardware and software you rent computing resources from suppliers who own and maintain all the necessary equipment and software

SaaS: software. no local installation, why manage your own email or payroll? central management of data and apps. eg, google mail. Offers remote access to applications based on a monthly or annual subscription fee

NaaS: network

PaaS: platform. middle point between infrastructure and software. no servers, no software, no maintenance team. Someone handles the platform, you handle development. Series of building blocks, developing an app from what’s available on the platform. eg, sales force.

DaaS: data

**cloud deployment models:**

private, your own virtual local data center

public, available to everyone over the internet

hybrid, a mix of public and private

community, several organizations share resources

**shared resources:**

internal cloud, no resources are shared. build your own cloud, pay for everything up front, no ongoing costs except part replacement and electricity

external cloud: share resources, underlying infrastructure owned by third party, cost may be metered or up front

**metered and non-metered cloud service:** cost per upload, storage space, download, pay for what you use. Or upfront cost with unlimited access

**cloud computing characteristics:**

Rapid elasticity: scale up and scale down as needed. seamless to everyone. Resources are automatically allocated in response to demand

on-demand self service: adding software, networks, servers, storage is a challenge outside the cloud. allows consumers to control the volume and type of computing resources used

Resource pooling: all of the computing power in one place. one large resource instead of many small resources. Grouping together computing resources and making them available for shared access for multiple consumers

measured service: costs and utilization are very closely tracked, resource planning and granular chargebacks

**Measured Service:** a billing model that enables a cloud provider to track the amount of computing resources that consumers are accessing and/or consuming.

**Metered Service:** a billing model in which gaining access to resources does not require payment of a flat fee. This type of billing model allows consumers to be charged variable rates depending on the exact amount of resources used.

**cloud services:**

Email is a challenge to maintain. expensive hardware and storage, trained support team, ongoing backup and maintenance. You can use cloud-based email hosting. flat cost per user per month. A personal option may have no direct cost. looks and feels the same for the user. examples include Microsoft office 365 and Google mail

cloud file storage services: access, share and exit from anywhere. easy to collaborate. synchronization app, store files on a local drive and the app syncs to the cloud. Syncs files to other devices. examples include: dropbox, google drive, one drive

virtual application streaming: on-demand apps, no local install, globally distributed.

The components are downloaded as needed and user data is stored in the cloud. easy to update. the application is in one place. some data is cached, only update the changes

cloud hosted virtual desktops: a virtual desktop infrastructure (VDI) in the cloud. access from almost any OS. Virtual NIC: all communication on the desktop is local to the virtual desktop. no sensitive information sent from the local device

Virtualization: one computer, many OS. separate OS, independent CPU, memory, network, etc. host-based virtualization: your normal desktop plus others. standalone server that hosts virtual machines: enterprise-level. This has been around since 1967.

Intel VT-x: Intel hardware enhancements for virtualization

AMD-V: AMD hardware enhancements for virtualization

what is the difference between Hyper-V and VT-x

The hypervisor: virtual machine manager, manages the virtual platform and guest OSs

may require a CPU that supports virtualization.

**Emulation vs virtualization:**

virtualization is a native OS identical to a non-virtual system. Performing native OS process

emulation is one device running processes designed for a completely different architecture. one device is pretending to be another. original code is used. code is interpreted from running on the current hardware. This is commonly slower than running natively, emulation is not as easy to do as virtualization.

**Hypervisor security:** Vm escaping, malware recognizes it is on a virtual machine, compromises the hypervisor and jumps from one guest OS to another. Many hosted services are virtual environments, malware on one customer’s server can gather information from another.

**VM Sprawl** is used to describe a situation in which a large number of deployed virtual machines lack proper administrative controls. Prevented by usage audits and asset documentation. Generating new VMs has become really easy. You are unsure which VMs are related to which applications and it becomes extremely difficult to deprovision. You need a formal process and detailed documentation with information on every object.

**VM escape** refers to the process of breaking out of the boundaries of a guest operating system installation to access the primary hypervisor controlling all the virtual machines on the host machine . Prevented by sandboxing and patch management

guest operating system security: every guest is self-contained, like a real computer. used traditional security controls. host-based firewall. anti-virus, anti spyware. Watch out for rogue VMs. Third party VMs provided by 3rd parties can be dangerous.

Network requirements: most client-side virtual machine managers have their own virtual (internal) networks. shared network address, the virtual machine shares the same IP address as the physical host. uses a private IP address internal. Uses NAT to convert to the physical host IP. bridged network address: the VM is a device on the physical network. With private addressing, the VM does not communicate outside the virtual network

what’s the difference between IEEE 802.3 and IEEE 802.11

explore all the different wireless standards (graphs and flash cards)

IEEE 802.11 provides the basis for implementing most modern WLANs

**Wireless standards (802.11)**: managed by the IEEE LAN/MAN standards committee (IEEE 802) provides the basis for implementing most modern WLANs

Many updates over time, check with IEEE for the latest. Wi-Fi trademark, the Wi-Fi alliance handles interoperability testing

* 802.11a: released October 1999. Operates in the 5 GHz range or other frequencies with special licensing. 54 megabits per second (Mbit/s). Smaller range than 802.11b. Higher frequency is absorbed by objects in the way. Many rules-of-thumb calculate 1/3rd the range of 802.11b or 802.11g. Not commonly seen today
* 802.11b: released October 1999. Operates in the 2.4 GHz range. 11 Mbits/s. Better range than 802.11a, less absorption problems. More frequency conflict, baby monitors, cordless phones, microwave ovens, bluetooth. Sacrifices speed for range
* 802.11g: an “upgrade” to 802.11b. released June 2003. Operates in the 2.4 GHz range. 54 Mbits/s. Same as 802.11a (but a little less throughput). Backwards compatible with 802.11b but has the same frequency problems
* 802.11n: released October 2009. Operates in 2.4 / 5 GHz at 40 MHz channel widths. 600 Mbits/s, 40 MHz mode and 4 antennas. Increase in speed due to MIMO (multiple-input multiple-output). Multiple transmit and receive antennas. Backwards compatible with everything except 802.11ac
* 802.11ac: released January 2014. Operates in the 5 GHz band. Less crowded, more frequencies (up to 160 MHz channel bandwidth). Increased channel bonding, larger bandwidth usage. Denser signaling modulation, faster data transfers. Eight MU-MIMO streams. Twice as many streams as 802.11n… nearly 7 Gbits/s

802.11 technologies: frequency is 2.4 GHz or 5 GHz, sometimes both.

Channels are groups of frequencies, numbered by the IEEE. Non-overlapping channels would be necessary. Bandwidth: amount of frequency in use, 20 MHz, 40 MHz, 80 MHz, 160 MHz

**802.11 channel bandwidths:**

802.11a – 20 MHz

802.11b – 22 MHz

802.11g - 20 MHz

802.11n – 20 MHz or 40 MHz (two contiguous 20 MHz bonded channels)

2.4 GHz, a 40 MHz channel uses much of the available bandwidth. Channel bonding refers to a technique that allows for combining adjacent channels to increase the amount of available bandwidth

802.11ac, 40 MHz for 802.11n stations – 80 MHz required for 802.11ac stations – 160 MHz optional (contiguous channels or non-contiguous bonded). 802.11ac has multiple channel bandwidth options

**Which of the following channel options would allow three Wireless Access Points (WAPs) to be set up on non-overlapping channels? (1, 6 and 11). Research this**

**RFID** (radio frequency identification): access badges, inventory/assembly line tracking, pet-animal identification, anything that needs to be tracked. Very small chips. Use radar technology, radio energy transmitted to the tag, RF power the tag and ID is transmitted back, bidirectional communication and some tag formats can be active/powered

**zigbee:** IoT networking, open standard – IEEE 802.15.4 PAN. Alternative to WiFi and Bluetooth, longer distances than bluetooth, less power consumption than WiFi. Mesh network of all zigbee devices in your home. Uses the ISM (industrial, scientific and medical) band. 900 MHz and 2.4 GHz frequencies in the US

**Z-wave:** proprietary home automation networking. Also uses wireless mesh networking and the ISM band. No conflicts with 802.11

**cellular networks:** mobile devices are “cell” phones. Land is separated into cell and antenna covers a cell with certain frequencies. 2G networks are GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access). Offer poor data support: originally used circuit-switching and minor upgrades for some packet-switching.

3rd generation (3G) introduced in 1998: upgraded data connectivity over 2G… incremental 3G updates improved speeds, usually several Mbit/s. Bandwidth improvement allowed new functionality. GPS, Mobile television, video on demand, video conferencing

4G and LTE (Long Term Evolution): converged standard (GSM and CDMA providers). Based on GSM and EDGE (Enhanced Data Rates for GSM Evolution). Standard supports download rates of 150 Mbit/s and LTE Advanced (LTE-A) supports download rats of 300 Mbit/s

Moving to 5G: rollout in late 2018 and 2019, worldwide launches in 2020. Significant performance improvements at higher frequencies, not as significant at lower frequencies. Tech updates: additional frequencies and improved data transmission methods

**Line-of-sight services:** visual path between antennas, high frequencies. Common in metropolitan areas to cover many homes simultaneously. Also options for non-line-of-sight at lower frequencies. WiMAX networking (worldwide interoperability for microwave access)

**Web Server:** respond to browser requests. Using standard web browsing protocols: HTML5. Web pages are stored on the server, download to the browser, static pages built dynamically in real-time

**File Server:** centralized storage of documents, spreadsheets, videos, pictures and any other files**.** Standard system of file management: SMB or AFP. The front end hides the protocol

**Print Server:** connect a printer to the network. Provides printing services for all network devices. May be software in a computer that is then connected to the printer or may be built-in to the printer. Uses standard printing protocols: SMB, IPP (internet printing protocol), LPD (Line Printer Daemon)

**DHCP Server:** automatic IP address configuration. Very common service available on most home routers and enterprise DHCP will be redundant running on multiple servers

**DNS Server:** converts names to IP addresses and vice versa. The load is balanced across many different servers. Usually managed by the ISP or enterprise IT dept

**Proxy Server:** an intermediate server. Client makes a request to the proxy, the proxy performs the actual request, the proxy provides results back to the client. Useful features: access control, caching, URL filtering and content scanning

**Mail Server:** stores incoming mail and sends outgoing mail. Usually managed by ISP or enterprise IT dept.

**Authentication Server:** login authentication to resources, centralized management. Almost always an enterprise service, not required on a home network. Usually a set of redundant servers

**SIEM (Security Information and Event Management):** used by the security team for real-time log info. Usually includes advanced reporting features. Data correlation, link diverse data types and forensic analysis that gathers details after an event

**Syslog:** Standard for message logging. Diverse systems, consolidated log. Usually a central logging receiver, integrated into the SIEM. Requires lots of disk space. Uses WORM drive tech: Write Once Read Many. Protects important security logs

**IDS and IPS**: used for network intrusions. Exploits against operating systems, applications, etc. Buffer overflows, cross-site scripting, other vulnerabilities. **Detection vs. Prevention**

**All-in-one security appliance:** next-generation firewall, unified threat management (UTM) / web security gateway. URL filter / content inspection, malware inspection, spam filter, CSU/DSU, router/switch, IDS/IPS, bandwidth shaper

**Endpoint management server:** manage all devices from one console. Software installations, driver installations, software updates, security patches, remote troubleshooting. Requires an agent on the device. Server sends the commands. Agent executes the commands.

**Legacy systems:** old systems

**Embedded systems:** purpose-built device, not usual to have direct access to the operating system, alarm system, door security, timecard system

**IPv4 vs IPv6:**

IPv4 is the primary protocol but IPv6 is slowly appearing

IPv4 is 32 bits / 4 bytes

IPv6 is 128 bits / 16 bytes: first 64 bits is network prefix (/64) and second half is network address

Every device needs:

* unique IP address
* subnet mask: is used by the local device to determine what subnet it’s on.
* Default gateway: the router that allows you to communicate outside of the local subnet Has to be an IP address on the local subnet

**Assigning IP address:** configuration used to be manual until October 1993 – The bootstrap protocol

BOOTP didn’t handle Voice Over IP and didn’t renew ip address assignments

Dynamic Host Configuration Protocol (DHCP): 1997, provides automatic configuration

**Step 1: Discover**

DHCP redundancy provided by a Router with DHCP relay enabled (IP Helper). Client broadcasts to udp/67

**Step 2: Offer**

DHCP will examine the request and broadcast back an IP address via udp/68.

**Step 3: Request**

Client sends back request of that IP address via udp/67

**Step 4: acknowledge**

DHCP server sends back confirmation via udp/68

**Turning dynamic into static:** DHCP assigns from a pool of available addresses and may occasionally change. If you don’t want the IP address to change (server, printer or personal preference) you have to set it to static by disabling DHCP. Or, configure an IP reservation on the DHCP server

**Automatic Private IP Addressing (APIPA):** if you hop on the network but can’t communicate with DHCP, you will get a link-local address. No forwarding by routers, but allows you to communicate with devices on your local network. IETF has reserved 169.254.0.1 – 169.254.255.254 / First & last addresses are reserved. Automatically assigned, Address resolution protocol (ARP) to confirm the address isn’t currently in use

**IPv6 link-local address:** a non-routable local network address, only works on the local subnet**.** Required on every IPv6 enabled interface, sometimes multiple addresses per interface: fe80::/64**.** The last 64 bits are usually created with a modified EUI-64, based on MAC address

**Using IP addresses:**

**SSL VPN (Secure Sockets Layer VPN):** Uses common SSL/TLS protocol (tcp/443). Used to avoid running into firewall issues. No big VPN clients, usually remote access communication. Authenticates users, no requirement for digital certificates or shared passwords (IPSec). Can be run from a browser or from a VPN client. AKA **Client-to-Site VPNs**  or **remote access VPN.** Requires software on the user device, but can be used to login to the network from anywhere in the world

**LANs (Local area network):** A group of devices that share the same broadcast domain. Virtual LANs are used to logically separate domains. It allows you to divide networks on the same switch/router. Devices are not allowed to communicate across VLANs. Minimizes the number of switches needed

**WAN (wide area network):** connects LANs across a distance. WAN technologies include point-to-point serial, MPLS, etc. Terrestrial or non-terrestrial

**PAN (personal area network):** bluetooth, infrared (IR), NFC, automobile, wireless headset and health devices

**MAN (metropolitan area network):** network in your city. Larger than LAN, often smaller than WAN. Historically MAN-specific topologies but everyone’s moving to Metro Ethernet. Common to see government ownership, who “own” the right-of-way

**WMN (Wireless mesh network):** all devices connect together in a mesh / cloud. Devices self form: connect to each other automatically. They also self heal: react automatically to changes. Technologies include 802.11, Zigbee, Z-wave, etc

# Network tools

**cable crimpers:** “pinch” the connector to a wire. coaxial, twisted pair, fiber

electrician’s scissors / cable snips and a good wire stripper. Make sure you use the correct modular connectors (differences between wire types)

**Multimeter:** AC voltage to check wall outlet voltage / DC voltage to check PC power supply or CMOS battery power. Also used to check continuity: cable connectivity, fuse status, wire mapping

**Tone generator:** puts an analog sound on the wire. Inductive probe: doesn’t need to touch the copper, hear through a small speaker. Provides easy wire tracing even in complex environments. Connect the tone generator to the wire: modular jack, coax, punch down connectors

**Cable testers:** relatively simple continuity tests, can identify missing pins or crossed wires. Not usually used for frequency testing like crosstalk, signal loss, etc.

time domain reflectometer (TDR): used to find breaks in copper network cables

Optical Time-Domain Reflectometer (OTDR): is a type of specialized cable tester that locates faults and breaks in fiber-optic cabling

**Loobpack plugs:** used for testing physical ports or fooling applications that require an ethernet connection. Serial / RS 232 (9 pin or 25 pin). Separate plugs for ethernet, T1, fiber. These are not cross-over cables

**Punchdown tools:** “punch” a wire into a wiring block – 66 block / 110 block. Organization is key. Lots of wires require cable management. Document what wires are plugged into what connections. Maintain your twists as close as possible to the block, Category 6A cable

**WiFi analyzer:** wireless networks are incredibly easy to monitor. Everyone “hears” everything. Purpose-built hardware or mobile device add-on. Specializes in 802.11 analysis. Identify errors and interference, validate antenna location and installation

You can connect a SOHO multifunction device/printer with USB, Ethernet, or Serial, not bluetooth

# Network Connections:

watch review videos on: SSH, Telnet, RDP, SMTP, POP3, IMAP, SNMP, DNS, TCP/IP, DHCP, HTTP/HTTPS, NetBIOS/NetBT, SMB/CIFS, SLP, AFP, NAT, LDAP, NTP, TLS

**Copper network cables:** fundamental to network communications

The vast majority of wireless communication also uses cables

**copper cabling termination specifications:**

**Twisted pair copper cabling:** uses balanced pair operation. Two wires with equal and opposite signals: Transmit+, Transmit- / Receive+, Receive-

Twists keep a single wire constantly moving away from the interference. The opposite signals are compared on the other end. Pairs in the same cable have different twist rates

**network cabling standards:**

Electronic Industries Alliance (EIA). Alliance of trade associations, develops standards for the industry. Standards start with RS-# or EIA-#

Telecommunications Industry Association (TIA) Standards, market analysis, trade shows, government affairs, etc. ANSI/TIA/EIA-568 – Commercial building telecommunications cabling standard

International ISO/IEC 11801 cabling standards: defines classes of networking standards

**Copper cable categories:** rj-45 connector, Twisted-pair copper cabling

Category 3: 10BASE-T / 100 meters

Category 5: 100BASE-TX, 1000BASE-T / 100 meters

The common minimum requirement in modern Ethernet networks is Cat 5e

Category 5e (enhanced): 100BASE-TX, 1000BASE-T / 100 meters

Category 6: 10GBASE-T / 37 – 55 meters

Category 6a (augmented): 10GBASE-T / 100 meters

**plenum rated cable** is used in the drop ceiling of offices to avoid toxic fumes from spreading in the case of a fire emergency. The traditional cable jacket is polyvinyl chloride (PVC). Fire-rated cable jacket is fluorinated ethylene polymer (FEP) or a low-smoke polyvinyl chloride (PVC). Plenum-rated cable may not be as flexible. Research plenum and no plenum, which cable is used for which?

**Firewire:** be aware of connection types, cable length and speeds

Serial port: DB-9 connection

cisco routers use this port:

**Unshielded and shielded copper cable:** In Ethernet networks, installed with RJ-45

**UTP:** no additional shielding, most common twisted pair cabling

**STP:** additional shielding protects against interference. Shield each pair and/or the overall cable. Requires the cable to be grounded

Abbreviations: U = unshielded / S = braided shielding / F = foil shielding... TP

Braided shielding around the entire cable and foil around the pairs is S/FTP

Foil around the cable and no shielding around the pairs is F/UTP

**copper cabling termination specifications: T568A and T568B:** pin assignments from EIA/TIA-568-B standard. Eight conductor 100-ohm balanced twisted-pair cabling

T568A and T568B are different pin assignments for 8P8C connectors: assign the T568A pin-out to horizontal cabling. Many organizations traditionally use 568B, difficult to change mid-stream. You can’t terminate one side with 568A and the other side with 568B. It slows speeds and causes confusion

learn to match pin colors to the two termination standards

**coaxial cables (copper):** two or more forms share a common axis. RG-6 used in television/digital cable as well as high-speed internet over cable. RG-59 used as patch cables. Not designed for long distances. Also protects against EMI

A type of twisted-pair copper cable used for connecting workstations to network devices is known as: **patch cable** and **straight-through cable**

**Crossover cable** is used to establish a direct communication link between two PCs

**Optical fiber communication:** transmission by light, the visible spectrum. No RF signal so it is very difficult to monitor or tap. Signals slow to degrade, transmission over long distances. Immune to radio or electrical interference.

**Optical fiber cable** has coating, cladding and an optical fiber core. Multimode fiber divides into multiple lines of light, used for short-range communication: 2km for 110Mbit/s and 55 meters for 10Gbit/s. Inexpensive light source (LED). Single-mode fiber is used for long-range communication. Over 80km without additional processing. Expensive light source (laser beams)

# Connection types:

**Video connections:**

VGA (video graphics array), DB-15 connector (15 pins) AKA DE-15. Blue color and 2 screws

Analog signal: no digital. Image degrades after 5 – 10 meters

HDMI (high definition multimedia interface): video and audio stream. All digital, no analog. ~20 meter distance before losing too much signal. 19-pin (Type A) connector, proprietary connector. MiniHDMI, type C connector, designed for smaller devices

Display port: VESA standard (video electronics standards association). A royalty free standard. Data is sent in packetized form, like ethernet or PCI express. Compatible with HDMI and DVI (passive adapter).

DVI (digital visual interface): single and dual link. Single link: 3.7 Gbps (HDTV at 60 fps). Dual link: 7.4 Gbps (HDTV at 85 fps). DVI-A: analog signals, DVI-D: digital signals, DVI-I: integrated, digital and analog in the same connector

**Apple connections:**

Lightning cable: apple proprietary. 8-pin digital signals. Some advantages over Micro-USB. Higher power output for phones and tables, can be inserted either way, simpler design, more durable

All thunderbolt versions support the ability to daisy-chain up to 6 devices and has the capability to send PCIe/DisplayPort data and power over single cable

Thunderbolt. High-speed serial connector: data and power on the same cable, based on Mini DisplayPort (MDP) standard. DisplayPort can transmit both video and audio data

Thunderbolt v1: two channels, 10Gbit/s per channel for 20 Gbit/s total throughput. Thunderbolt v2: 20 Gbit/s aggregated channels

Thunderbolt v3: 40 Gbit/s aggregated throughput, USB-C connector, max 3 meters (copper) and 60 meters (optical)

**USB connections:**

USB (universal serial bus): simplifies connections. Printers, storage devices, keyboard, mouse, etc

USB 1.1/2.0 connectors: Standard-A plug: type A connectors can be attached to host devices and devices that supply power. Standard-B plug, Mini-B plug and micro-B plug. Type B connectors can be attached to devices that receive power and target devices

USB 1.1: low speed, 15 mbit/s, 3 meters. Full speed: 12 mbit/s, 5 meters

USB 2.0: high speed, 480 mbit/s, 5 meters

USB 3.0 connectors changed the standards a bit notice the difference between plugs

USB 3.0: SuperSpeed, 5 gbit/s, 3 meters. Standard does not specify a cable length

USB 3.1: released July 2013. SuperSpeed+, 10gbit/s – twice the rate of USB 3.0

USB 3.2: released September 2017, New SuperSpeed+ modes over USB-C. 10gbit/s and 20 gbit/s

USB 3.x Type-A provides full backward compatibility with earlier USB standards

USB-C: has a lot of different connectors. Replaces all other connectors. USB-C isn’t necessarily USB 3.1. The cable must support the function

**DB-9:** serial cable connector: D-subminiature or D-sub. Different sizes, A through E

Commonly used for RS-232: recommended standard 232, an industry standard since 1969

Serial communications standard: built for modern communication. printers, mice, networking

Commonly used as a configuration port: serial console interface. DE-9, DB-25

Also used for VGA cablesF

watch videos on hard drive connections

**Hard Drive connections:** SATA can only be used to connect one device. SATA (serial AT attachment): two cables, one plugs to motherboard the other plugs to power supply

SATA revision 1.0, SATA 1.5 gbit/s, 1 meter

SATA revision 2.0, SATA 3 gbit/s, 1 meter

SATA revision 3.0, SATA 6 gbit/s, 1 meter

SATA revision 3.2, SATA 16 gbit/s, 1 meter

The regular SATA connector is L shaped with one ear. ESATAis rectangular with two ears

The SATA interface specification defines data cable connector consisting of 7 pins

SATA and ESATA connectors. Molex connectors are 4 pin peripheral power, provides +12V a +5V

PATA drive cables (parallel AT attachment), Parallel ATA, ATA. Circa 1999 by Western Digital. Originally called integrated drive electronics (IDE). 2nd generation called EIDE Enhanced IDE). Promised faster speeds (from 16 Mb/s through 133 Mb/s). 39 PIN interface… cable consisting of 40 wires and a cable consisting of 80 wires. Molex connectors used to provide power. A PATA cable can connect a PC to two devices. Maximum cable length of 18 inches. PATA cabling uses 40-pin connectors

When installing two PATA drives on a single cable, each drive must be configured with a jumper to designate it as either a primary drive (a.k.a. "master") or a secondary drive (a.k.a. "slave"). The "cable select" jumper setting option automatically configures the drive as master or slave according to its position on a cable

SCSI standard (small computer systems interface): not really “small” any longer

Originally designed to string many peripherals together onto a single cable/controller. Up to 16 devices in a SCSI “chain”. Not just for hard drives… scanners, tape drives, CD-ROM drives. Many devices on a single bus. 8 on narrow bus, 16 on wide bus. Very intelligent interface functionality: much of the difficult configuration work is done between the SCSI devices. Industry longevity: well supported in the enterprise a standard drive for virtual systems.

SCSI ID and logical unit (LUN): Every SCSI device on a single bus is assigned a separate ID number. Logical units (LUNs) are defined within each SCSI ID. Separate drives in a storage array or virtual machine. The signal at the “end of a physical SCSI bus is terminated. LUN is a way to identify logical partitions on a SCSI hard drive.

1234567890+-

Serial attached SCSI (SAS) devices have no jumpers, terminators, or settings. Move from parallel to serial increases throughput similar to the move from PATA to SATA. Point to point connection (no daisy chains) and the control and management of SCSI but with the speed of a serial connection

**adapters and converters:**

DVI to HDMI: no loss of video quality and no signal conversion required

DVI to VGA: DVI-A includes analog signals. Only 640x480 resolution supported

USB to Ethernet: some laptops don’t have a wired Ethernet interface

**Network Connections:**

RJ11 and RJ45 are not copper cabling terminations, they are fiber optic

**RJ11:** 6 position, 2 conductor (6P2C0). RJ14 uses 6P4C for dual-line use. Telephone connector. Dial-up networking and twisted-pair copper cabling

**RJ45:** (8P8C) modular connector. Similar in shape to an RJ48C (8P4C), used with T1/WAN data lines**.** twisted pair copper cabling connector, used with Ethernet network cabling

**RS-232:** recommended standard 232, serial communications standard built for modems but commonly used as a configuration port serial console interface

**BNC:** bayonet neill-concelman. Coaxial cable connector for DS3 WAN links

**F-type:** used on cable television and cable modems, RG-6 or RG-59 cable with a threaded connector**.** coaxial cabling, copper cabling connector, used for analog video and CCTV installations

**barcode/QR code reader:** serial, USB or wireless connector. on your phone with apps

**Peripherals:**

microphone: analog - TRS (tip/ring/sleeve), digital - usb

speakers: analog output devices, TRS or speaker output, audio adapter

headset: desktop and mobile use, USB, TRS, wireless/bluetooth

digital projectors: not always LCD. Metal-halide lamp, very bright and very hot. brightness is measured in lumens. Always let bulbs cool off

KVM: keyboard, video and mouse. Use many computers with a single set of peripherals

magnetic reader / chip reader: Point of sale (POS) terminal, USB connected

VR headset: virtual reality. Motion tracking on X,Y,Z axis

touch pad: may be a standalone advice as well

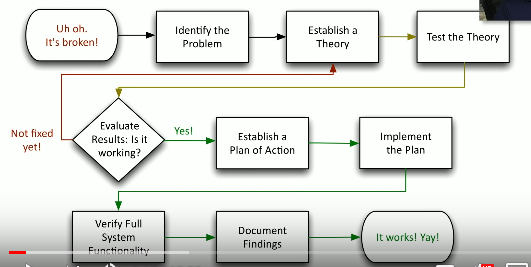
signature pad: small digitizer and stylus

gaming input: gamepad and joystick

webcam:

mouse: USB or adapter for PS/2

# Troubleshooting:



### The troubleshooting process: Change control is a formal process for managing change that avoids downtime, confusion and mistakes. Usually come in the form of corporate policy and procedures. Nothing changes without the process. You plan for a change, estimate risks associated, have a recovery plan, test before making a change and document everything to get approval

* **identify the problem:** Information gathering, get as many details as possible. Duplicate the issue, if possible. Identify symptoms: may be more than a single symptom. question users as much as possible. determine if anything has changed. approach multiple problems individually: break down problems into smaller pieces. backup everything: you’re going to make changes, always have a rollback plan. What else has changed? environmental / infrastructure changes? Clues: OS log files, application logsl
* **establish a theory:** the simplest explanation is the most likely but consider everything.. make a list of all possible causes ranked from easiest to most difficult. research the symptoms: internal knowledge base, google searches
* **Test the theory:** confirm the theory, determine next steps to solve the problem. theory didn’t work? re-establish a new theory or escalate, call an expert. If the theory doesn’t work, go back and establish a new theory. repeat as necessary
* **create a plan of action:** build the plan, correct the issue with minimum impact or do the work during non-production hours if they cause disruption. identify potential effects: every plan can go bad. Have a plan B and plan C
* **implement the solution:** fix the issue, implement during the change control window. Escalate as necessary, you may need 3rd party help
* **verify full system functionality:** Have the customer confirm the fix. Implement preventative measures to avoid issue in the future
* **document findings:** build a knowledge base of problems. What action did you take? What outcome did it have? consider a formal database, help desk case notes, searchable database

### Troubleshooting common hardware problems:

unexpected shutdowns: no warning, black screen, may have details in your event viewer: heat-related issue:

* high CPU or graphics, gaming
* check all fans and heat sinks
* bios may show fan status and temperatures

Failing hardware: has anything changed recently? check device manager, run diagnostics

overheating: heat generation, CPUs, video adapters, memory

cooling systems: fans and airflow, heat sinks, clean and clear

verify with monitoring software: built into the bios or use HWMonitor

lockups: system completely stops. Usually not much in the event log

check for any activity. Hard drive, status lights, ctrl-alt-del

update drivers and software patches. Has this been done recently?

low resources: ram, storage

hardware diagnostics may be helpful

POST (power on self test)

tests major system components before booting the OS

* main systems (cpu, cmos, etc)
* video
* memory

failures are usually noted with beeps and/or codes. BIOS versions differ, check documentation

POST and boot: blank screen on boot

* listen for beeps
* bad video
* BIOS configuration issue

BIOS time and setting. maintained with the motherboard battery, replace the battery

attempts to boot to incorrect device: check boot order in BIOS configuration

confirm startup device has a valid os

continuous reboots: causes include overheating, hardware failures, corrupted or misconfigured OS installation. How far does the boot go before rebooting? BIOS only? OS splash screen?

bad driver configuration. F8 to boot from last known working configuration… safe mode

if system starts, disable automatic restarts in system properties

bad hardware: try removing or replacing devices

check connections and reseat

no power: at the source or from power supply? UPS?

get out your multimeter

fans may spin but no power to other devices. Where is your fan power connected?

no POST, bad motherboard?

case fans have lower voltage requirements

check the power supply output

loud noises: computers should hum, not grind. rattling indicates loose components

scraping might be a hard drive issue (HDD not SSD)

Loud clicking noises in hard drives are not good.

clicking is a fan or hard drive problem, maybe a problem with the PSU

a pop followed by smoke it might be a blown capacitor

intermittent device failure: bad installs. check and reseat, use all the screws

bad hardware, poor connection, heat and vibration

indicator lights: POST codes on the motherboard

power, link light, speed, activity

smoke and burning smell: electrical problems. always disconnect power

locate and replace damaged components

crash screen (BSOD): windows stop error

contains important information, also written to event log

useful when tracking down problems: sometimes more useful for manufacturer support

the spinning ball of death (pinwheel of death) on MacOS: macOS X spinning wait cursor

many possible reasons: application bug, bad hardware, slow paging to disk

log entries: windows event viewer, boot logs in system configuration: C:\Windows\ntbtlog.txt

Linux: individual application logs, /var/log

macOS X: utilities / console.app

error messages: the details of an error message can make or break a troubleshooting session

write down everything, take pictures or video and train your users to do the same

the error might not make sense, write it down anyway, the internet will tell you what it means

this way you spend your time troubleshooting the right things

**Troubleshooting hard drives:**

read/write failure: “cannot read from the source disk”

slow performance, constant LED activity, loud clicking noise

get a backup. check for loose or damaged cables. Check power supply and overheating

run hard drive diagnostics from the manufacturer on a known good computer to check if it’s an OS issue, an issue with the computer itself, or maybe the hard drive is bad

boot failure symptoms: drive not recognized, lights (or no lights), beeps, error messages

“OS not found”. troubleshooting: check your cables (physical problem?)

check boot sequence in BIOS

check for disabled storage interfaces

for a new installation, check hardware configuration. Data and power cables, try different SATA interfaces.

RAID not found: missing or faulty RAID controller

each RAID is different, don’t start pulling drives until you check the console

How many drives can be lost in each RAID array before data loss occurs?

crash screen: windows stop error and apple spinning wait cursor could be a hard drive issue

diagnostics needed for drive and motherboard

**SMART (Self-Monitoring, Analysis and Reporting Technology)**: Use third party utilities

avoid hardware failure, look for warning signs. enables monitoring a system for anticipated HDD failures. schedule disk checks, built in to most drive arrays

there are usually warning signs to replace a drive before data loss or user downtime

**troubleshooting video and display issues**

no video image: is it connected? check both power and signal cables

input selection on monitor: hdmi, dvi, vga, etc

image is dim: check brightness controls

swap the monitor and try it on another computer to check if monitor or PC is the issue

no video after windows loads: usa VGA mode (F8)

image quality problems: flickering, color patterns incorrect: check the cable pins

distorted image and geometry: check the OS refresh rate and resolution settings

native resolution is important on LCD displays, check or replace cable

disable hardware acceleration, troubleshoot with software drivers

image quality problems: oversized images and icons. resolution set too low. lower = larger

burn-in or ghosting: discoloration on the screen, some displays will pixel shift

LCDs have image sticking. remove by displaying a white screen for an extended period

pixel problems: stuck pixels (constantly bright), dead pixels (always black)

artifacts: unusual graphics - check adapter.

image persistence - turn off display

motion trails - disable advanced video features

BSOD and overheating: video drivers, monitor the internal temp

**troubleshooting laptops:**

no display or dim video: verify the backlight. look closely, it may be barely visible

no backlight, replace the inverters

confirm video with an external display: video good but LCD bad, replace the LCD display

flickering video: connector problem, bad video cable, bad video hardware

input issues: sticking keys, difficult to clean. keycaps are very delicate!

ghost cursor / pointer drift: mouse pad causes cursor to bounce around

modify the configuration to check for palm press

update your drivers

letters typing numbers: num lock indicator lights

wireless troubleshooting: multiple antennas, WiFi main and aux, bluetooth, antenna wires wrap around the laptop screen. Easy to accidentally disconnect during maintenance.

check the connectors: loose cables can cause intermittent wireless access

power issues: battery not charging. batteries lose capacity over time. laptop charging hardware may be faulty. try charging battery in an identical laptop

no power: check the external power adapter “brick” with multimeter

master laptop reset: hold power for 10 seconds or a set of keystrokes that provides hardware reset

external monitor issues: fn key that toggles between LCD / external monitor / both

power off the laptop, connect to the external display then turn back on. Laptop default may be set to display to plugged in screen first

**troubleshooting mobile devices:**

touchscreen not responsive: black screen or touchscreen not responding, Erasing all content/settings and restoring the device to factory defaults (factory reset/hard reset)

try reseating device battery, removing screen protector and cleaning the screen

app issues: apps not loading or slow performance. Stop the app and restart

update the app

unable to decrypt email:

built-in to corporate email systems is a private key that is distinct per user

install individual private keys on every mobile device using a mobile device manager (MDM)

short battery life: bad reception, disable unnecessary features. Check application battery usage in settings. Replace aging battery, batteries have a certain number of recharges

phone overheating: things that create heat in a phone include, charging and discharging battery, CPU usage, display light. Check app usage to learn about battery usage. Avoid direct sunlight

Frozen system: nothing works, no screen or button response. Soft resets. ongoing problems may require a factory reset

No sound from speakers: no sound from a particular app? check volume settings, both app and phone settings. Bad software or hardware? use headphones. Sound starts but then stops: dueling apps / keep apps in foreground. no speaker sound from any app? load latest software / factory reset

GPS not functioning: check settings to enable GPS.

configure location mode and what apps are allowed to use location services

Swollen battery: buildup of gas. designed to self-contain. Do NOT open the battery packet/container. Significant fire risk. Faulty battery, stop using immediately and dispose of properly.

**device disassembly best practices:** Many different pieces, intricately engineered and tight quarters. Very easy to take apart but putting back together is a lot harder.

Use manufacturer documentation as a reference

Magnetic mat/separate containers used for holding disassembled parts

Document and label cable and screw locations

Use appropriate hand tools: A good screwdriver, tweezer, and some specialized tools

get a big anti-static cloth, something soft to protect screens, easy to break parts

Laptops disassemble in sections: outer shell, keyboard, video connector, etc.

Step by step process to duplicate in reverse to put back together.

Refer to manufacturer resources for step by step repair guides

the internet provides the rest: online written guides and YouTube videos.

specialized sites can help: ifixit.com

**Troubleshooting printers:** print or scan a test page built into Windows, not the app.

use diagnostic tools, web-based utilities built into the printer. A vendor app or generic app to manage printer

streaks and blurs: lean print heads

blank pages. Low toner or ink

final print: color prints in the wrong color. Low ink on one cartridge

**Laser printer troubleshooting:**

long vertical streaks on the page indicate damage to the imaging drum (NOT clogged print head nozzles)

ghost images on output pages indicates a problem with the cleaning stage

toner falling off a printed copy or output smudges indicate a problem with the fuser assembly

garbled characters means old printer drivers

**depleted toner:** causes faded printouts and blank pages

paper jam: careful when removing, don’t rip the paper or damage the internal components

paper not feeding: check the tray, pickup rollers, part of a laser printer maintenance kit

network issues: powered on? user intervention required. wired cabling / wireless settings

access denied: security tab, print, manage this printer, manage documents

bad output: garbled characters on paper. bad printer driver, wrong model

incorrect page description language: (PCL or PostScript)

bad application: check with a test page outside the app

OS issues: unable to install printer: drivers are important OS updates. user must have permission to install, check the printer driver (23 bit VS 64 bit)

backed up print queue: printer server not working, print spooler crash, restart the spooler, change recovery options

error messages: on the printer display, modern printers have large LCDs

lower memory error: laser printers build the entire page in memory. complex images and graphics consume more memory

no output: check the printer. getting power? check for display messages. run a test print from the printer. Check the connectivity. print a test page from a computer. check direct connections. try across the network. tests the OS, network, drivers and spooler

check other applications. print from a different program?

multiple failed jobs in logs: corrupted print jobs. Print spooler will crash. most spooler configurations will automatically restart. Problems are logged: windows event viewer, windows-printservice. one job may be causing the issues. monitor the queue for details

**network troubleshooting:**

no network connectivity: do you have a link light, is it plugged in?

ping loopback: 127.0.0.1. Is the protocol stack working?

intermittent connectivity

ping local IP address to check local configuration, adapter and link signals

ping default gateway, connectivity on the local network

ping devices on router’s other side (google: 8.8.8.8)

automatic private IP addressing (APIPA): a link-local address, no router forwarding

IETF has allocated: 169.254.1.0 - 169.254.254.255

169.254.0.0/24 and 169.254.255.0/24

automatically assigned, uses ARP to confirm the address isn’t currently in use

check your ip address. Is it an APIPA address?

local resources unavailable: shares, server unavailable or share permissions modified. Computer relies on DNS to find the server

printers: device sharing printer (or printer is unavailable), printer permissions modified

email: service is associated with a specific server. maybe a cluster of servers. problem may be related to server or network path

limited or no connectivity: windows alert in the system tray. limited or no connectivity, no internet access, check the local IP address. An APIPA address will only be local. If DHCP address is obtained, perform ping tests, local gateway, remote IP address

intermittent connectivity: check the system tray. A broken LAN icon is a loss of signal. Check for a cable problem. Might have a bad NIC. Problems with switch or wireless access point. Bad interfaces, router rebooting

IP conflicts: DHCP helps, but static addresses can conflict

windows will identify a duplicate and prevent a conflict

two identical IP addresses will conflict, intermittent connectivity

reboot or reset the NIC and start over from the beginning (restart DHCP process)

Slow transfer speeds: router or infrastructure congestion, overloaded network or devices

speed and duplex incompatibility. hardware issues with the adapter, check cabling

it may also be caused by malware

low RF wireless signal: interference form a third party device, signal strength. Transmitting signal, transmitting antenna, receiving antenna, ETC. incorrect channel? usually automatic, look for manual tuning. Bounce and latency. Multipath interference; flat surfaces

incorrect access point placement: locate close to the users

wireless interference: predictable. Fluorescent lights, microwave ovens, cordless telephones, high-power sources. Unpredictable: multi-tenant building. measurements, signal strength, performance monitor

SSID not found: network name doesn’t appear: other networks are there. Too far away?

wireless router configured to disable SSID broadcast. you can still manually connect

Resume entry after you pass the A+:

“Install, configure, optimize, troubleshoot, repair, upgrade and perform preventative maintenance on PCs, digital devices and operating systems.”  
Install and configure PC system unit components and peripheral devices

Install, configure and troubleshoot display and multimedia devices, storage devices and internal system components

Maintain and troubleshoot Microsoft Windows

Configure and troubleshoot network connections

Manage users, workstations, and shared resources

Implement client virtualization

Implement physical security

Secure workstations and data

Troubleshoot workstation security issues

Support and troubleshoot laptops, mobile devices and print devices

DISM windows command

SFC windows command

Safe mode in win 7 and 8 with F8

Safe mode in win 10 with shift+click restart, or Msconfig or settings

Tasklist

Taskkill /IM <process name>

Taskkill /PID <task process ID> /t

Gpupdate

The difference between copy, xcopy and robocopy

Xcopy copies file permissions

Services.msc or net start/stop command

Memory diagnostics

Component services

Odbc data sources

Component services

Chkdsk /f and /r

"**End-of-life**" ("**EOL**") is a term used with respect to a product supplied to customers, indicating that the product is at the end of its useful life (from the vendor's point of view), and a vendor stops marketing, selling, or rework sustaining it. (Windows XP is EOL)

**Physical Address Extension (PAE)** enables 32 bit OS to utilize more than 4GB of memory

PAE only allows you to use up to 64gb of memory, not the 16 exabytes in 64 bit architecture

**Windows 8 and later requires CPUs to be capable of PAE**

The processor must be running in Physical Address Extension (PAE) mode to use the **NX bit** processor feature. The NX bit is a form of memory protection that provides additional security.

Intel: **XD bit (*execute disable*)**, AMD: **Enhanced Virus Protection** (**EVP**)

**SSE2** refers to a solution (a complimentary instruction set) that extends the capabilities of a CPU. All processors that support NX also support SSE2

SSE data transfers use XMM register

File attributes:

Read Only

Archive

System

Hidden

Windows extended attributes

Index

Compression

encryption

Attrib windows command

Relative path vs direct path

Partitioning schemes:

MBR for PC BIOS-based systems

GPT for UEFI-based systems

MBR:

Four primary partitions, 3 primary and 1 extended

One marked active

2tb partition size limit

All primaries contain data

Boot sectors become populated on active partitions called system partitions

Boot partition is where the operating system resides

GPT:

Newer partitioning

Allows for 128 partitions

Backwards compatible with BIOS-based systems

Boot code redundancy

No 2TB partition size limit

List disk

An asterisk means its GPT, no asterisk means its MBR

The theoretical memory limits in 16, 32 and 64 bit machines are as follows:

16 bit = 65, 536 bytes (64 Kilobytes)

32 bit = 4, 294, 967, 295 bytes (4 Gigabytes)

64 bit = 18, 446, 744, 073, 709, 551, 616 (16 Exabytes)

x86 is 32bit architecture

NTFS and ACL

What does the USMT tool do?: Migrates user setting and files from one OS to another

You use a class B fire extinguisher to put out electrical fires

What are the different classes of fire extinguishers?

**Steps to remove any malware:**

1. Identify and research malware symptoms
2. Quarantine infected systems
3. Disable system restore (Windows)
4. Remediate the infected system
5. Update (or install) anti-malware software
6. Scan and use removal techniques (safe mode, pre-installation environment)
7. Schedule scans and run updates
8. Enable system restore and create a restore point (Windows)
9. Educate the end user

You use the bcdedit.exe utility to edit, modify and update the boot configuration data (BCD) file, which contains boot settings for a computer. You could also change the boot order by using the MSCONFIG tool

If you want your computer to boot faster and access more RAM at startup, disable application startup.

Wearing leather soled shoes will help transfer electricity. Some rubber soled trues protect against ESD if the soles are made up of conductive rubber that scatters static electricity

What is Windows 8 RT?

All versions of Windows after Windows 8 support MUI (multilingual user interface)

So does Windows 7 Ultimate

MSDS, OSHA and EPA guidelines

Single-Sign-On (SSO) ensures that users are able to log in to multiple system using the same login credentials

Windows 7 allows you to boot the computer into Windows XP mode on a computer that supports virtualization.

Attributes of a person that can be used to grant biometric access:  
Fingerprints, face, signature, iris, retina, hand geometry, voice

Windows 7 can be upgraded to Windows 8 basic or pro

The task scheduler tool can be used to periodically create a Restore Point

Spotlight in mac: command + spacebar

What is the dock (mac)

Redhat, fedora, centos: yum update

Most of the other distros follow debian model: apt (apt-get) update

Apt dist-upgrade

DD command

Automated System Recovery is not an option listed in the Advanced Boot Options menu

If you get the following error the registry is corrupt:

Windows 8.1 could not start because the following file is missing or corrupt: \WINDOWS\SYSTEM32\CONFIG\SYSTEM

You are putting your registry file in jeopardy when you shut down your computer improperly

BranchCache helps reduce repetitive traffic over a WWAN

R sync

Mac OS X troubleshooting:

Physical security

Entry access control roster.

Man traps

Security guards

Access cards with RFID chips

Magnet locks unlock when power goes out

Desk mount (laptop lock)

Smart cards, CAT cards

Software token and hardware tokens

RSA secure ID key fob

Like the google or blizz authenticator

User security vs data security

User authentication and authorization

Password policies

Something you know, something you are, something you have authentication

Examples of something you have authentication:

Door locks, server locks and hardware tokens

MDM mobile device management

Data loss prevention (DLP)

Principle of least privilege

Access control lists

When a policy change is made in active directory, the policy is applied at logon

What are active directory policies?

What is folder redirection?

What is a logical domain (security boundary)?

FAT32 doesn’t allow ACL and permissions

Perfmon and resmon

Effective access lists lets you find troubleshoot file and folder access issues

When you have conflicting permissions on a user or a file, the most restrictive permission will always win out

If you have BIOS, you need two NTFS partitions

If you have UEFI, you need one FAT32 and an NTFS partition

A virus relies on other applications to execute and infect the system

EFS vs bitlocker

Bitlocker can be used in non TPM mode, but lowers security

It will use a USB key instead of a set of bits on the motherboard

Microsoft azure: microsoft intune, device compliance

Radius and TACACS servers. Radius does not provide accounting (what did the user do when he logged in) but is just as good as TACACS at authentication and authorization

When you’re infected with a virus, disable system restore.

**BranchCache:** allows computers at a local branch office to cache data from a file or web server on a WAN (wide area network)

**The difference between EFS and Bitlocker/TPM:** EFS allows you to encrypt certain sectors of the hard drive while TPM can be used to encrypt the entire hard drive. Windows home versions do not have TPM, TPM is needed to use Bitlocker.

**MSTSC shell command:** Creates connections to Remote Desktop Session Host servers or other remote computers, edits an existing Remote Desktop Connection (.rdp) configuration file, and migrates legacy connection files that were created with Client Connection Manager to new .rdp connection files.

**.vbs files** are virtual basic scripts. Most scripting is done through powershell now. .vbs scripts are also used in Microsoft Excel

**SSE2** (**Streaming SIMD Extensions 2**) is one of the Intel SIMD (Single Instruction, Multiple Data) processor supplementary instruction sets first introduced by Intel with the initial version of the Pentium 4 in 2000. It extends the earlier SSE instruction set, and is intended to fully replace MMX.

**MSI files** are used for installation, storage, and removal of programs in Windows

**MMC** is the windows GUI shell for administrative and even some non-administrative snap-ins

**Certmgr.msc** is an MMC snap-in

Short for Resource Monitor, **Resmon** is a feature introduced with Windows Vista that enables users to view real-time resource information about software and hardware on their computer. It shows things like memory, disk, CPU and network performance, as well as which software handles and file modules are working

**PERFMON** is a Caché utility that controls the MONITOR facility. The MONITOR facility provides performance data for the Caché system by collecting counts of events at the system level and sorting the metrics by process, routine, global, and network nodes.

**Chkdsk:** verifies the file system integrity of a volume and fixes logical file system errors

**Disk Clean-up:** is a computer maintenance utility included in Microsoft Windows designed to free up disk space on a computer's hard drive. The utility first searches and analyzes the hard drive for files that are no longer of any use, and then removes the unnecessary files...The

**Windows Event Viewer** shows a log of application and system messages, including errors, information messages, and warnings. It’s a useful tool for troubleshooting all kinds of different Windows problems.

**CDFS (compact disk file system)** is a file system for read-only and write-once CD-ROMs.

**Universal Disk Format:** has been most widely used for DVDs and newer optical disc formats, supplanting ISO 9660/CDFS

**FAT32** has a 4hb max file size and a 32gb max hard drive size

**NTFS:** most popular windows file system. Insanely huge file size limits so in practice, no maximum file size. Also allows file permissions and encryption. Windows must be installed on an NTFS formatted partition. NTFS is read only in MacOS and older linux distros.

**exFAT:** designed as an upgrade from FAT, used mostly in memory cards (SD). has wider non-windows support

**ext2, ext3, ext4:** extended file system developer for linux

**HFS, HFS+, APFS:** apple file system

You use a different file system depending on your OS:

* NTFS for Windows
* HFS+/APFS for MacOS
* ext4 for linux

Use FAT32 on removable media below 32 gbs and exFAT on anything bigger

You can use as many disks as you want with a striped volume

A mirrored volume uses a maximum of 2 disks

You need to enable wake on LAN. where would you go to do this?

Firewalls are port security?

Certificates

Press F8 on boot in Windows 7 to enable System Recovery

The NTLDR was replaced by the boot.ini file

Mutual or two-way authentication checks the identity of both ends of the connection

What is OEM software?

BCD

Bootmgr

Boot.ini was replaced by the BCD, which holds configuration data about which operating systems are installed. MSCONFIG is used to edit the BCD file.

If the screen on a CRT monitor is broken, you cannot reclaim any materials from it. If the CRT is intact, you can reclaim lead, mercury and phosphorus from it. You can reclaim metal from circuit boards and computer cases, you can also reclaim data from a hard drive, even if the data has been erased.

Grep Linux

Chmod linux

Ps linux

Apt-get linux

Learn all the hidden folders in Windows

Arp poisoning (spoofing)

SOE (standard operating environment)

What does increasing/decreasing the size of pagefile.sys do?

What does increasing/decreasing the size of win386.swp do?

WIN386.SWP

PAGEFILE.SYS

Winload.exe

bootmgr

hiberfil.sys

SmartScreen filter on Microsoft Edge

Material Safety Data Sheet (MSDS)

Wake on LAN is enabled through BIOS

The default permission position in a safe network should be implicit deny

You should return empty toner cartridges to the manufacturer for recycling

You can change your local password by pressing ctrl+alt+del and select Change a Password

Rainbow attack

Sfc utility

Which of the following authentication methods separates authentication and authorization into two different processes? TACACS?

Defrag /v

Gpupdate

Gpresult

You need to view the content of a Windows 10 update, what command line tool would you use?

Expand? Extract?

What does the $ stand for in Windows?

Regulated data and the privacy of electronic information in europe?

GPDR, PII, PCI, PHI

Is there a difference between flashing the bios and updating the EEPROM chip?

The difference between an implicit deny and an explicit deny /allow?

Active directory logical security concepts:

Folder redirection, login script, domain membership, organizational unit

What do you need to implement bitlocker to go on windows 7? What is bitlocker to go? It’s a technology in Windows 7 that allow you to encrypt the contents of USB flash drives.

REGSVR32 is used to register and unregister dll and Active X files in the registry.

A corrupt registry is solved by restoring the registry from a backup

Missing .exe files can be solved by application re-installation.

The boot.ini file was used in Windows xp, replaced by?...

The snap function to display two side-by-side applications can be done in Windows 7 and later

The difference between the services and startup tabs in msconfig

You cannot create a homegroup if the computer is already part of a domain

In order to return a Windows computer to its original setting, use the Factory recovery partition

Tools tab in hard drive properties, does not have format

What is a rainbow attack?

The factors that generate and promote the transmission of ESD are moving machines, moving people, improper grounding and humidity below 40%

How can you tell a shared folder is an administrative share?

Share permissions do not include read, write, modify and full control. They only include read, change and full control.

Homegroup only works on Windows 7, 8 and 8.1

Homegroup was removed in Windows 10

Windows commands you need to know for the exam:

Dir

Cd

Md

Ren

Rd

Deltree

Del

Tasklist

Taskkill

Shutdown

Sfc

bootrec

A user has a Windows 7 computer with 512 mb of ram and two hard drives, anmed drive C and D. The paging file is located on drive C. The user complains that his computer does not perform well after running for a couple hours. What should you tell the user to do? Move the paging file to drive D. **What does this mean?**

PowerShell Core 6.0 can be used on Windows 8 and later

A computer that is constantly being shut down improperly may negatively affect dll files

What are dll files?

What are BCD files?

The system restore feature is closely tied to the Volume Shadow Copy Service (VSS) in Win 7 and above. The feature is also disabled if VSS is disabled. VSS provides a mechanism for creating consistent point-in-time copies of data, known as shadow copies. System Restore allows you to use a restore point to return a system to a certain point in time.

If you want to increase the transmission area of a wireless access point increase the power level setting.

The only reason you would use WPA over WPA2 is with older wireless clients that do not support WPA2.

A trojan horse is malicious software that relies on other applications to execute and infect the system.

Confidentiality, integrity and availability, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC **triad** (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

You need to create a hard drive image on a Linux computer. Which command should you use?

Mv

Ls

Dd

Cp

What is the minimum free disk space needed to run defragmentation?

What three conditions affect the external vulnerabilities of wireless networks?

Access point power, antenna selection, antenna placement

As an IT technician, you should only report issues to your supervisor. If you find inappropriate material on a company owned computer and no specific acceptable use policy exists, inform your supervisor.

You need to take these security considerations into account then installing and configuring applications on Windows desktops: impact to device, user privileges, turning Windows features on or off.

The post-implementation impact a proposed change would have on the company workforce is covered in the “Documented business processes” section of the change request form.

“BOOTMGR is missing” is fixed by using an installation DVD and selecting “Automatic Repair” in the Advanced options menu.

The best way to decrease the amount of time it takes for Windows to startup and to increase the amount of available RAM on startup is to disable application startup.

Geotracking is not a security measure for mobile devices.