# Networking:

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

**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

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.

**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)

# 

**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

**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

**Network:**

BranchCache helps reduce repetitive traffic over a WWAN

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

An SOE is a standard operating environment, or a specific computer operating system and collection of software that an IT department defines as a standard build. SOEs help if you're managing a lot of computers and want to reduce complexity.

Wake on LAN is enabled through BIOS or Windows settings

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.