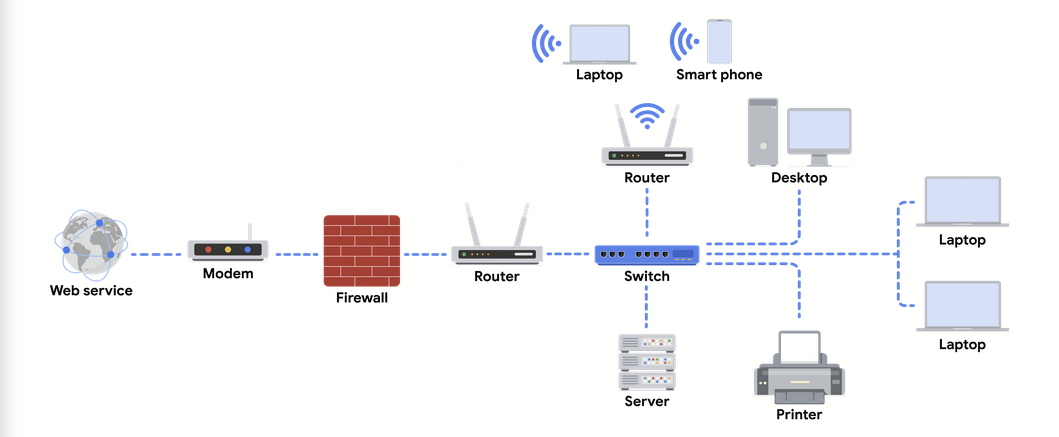
Week 1

Network: A group of connected devices

(LAN: local area network. Think devices like printers, smartphones, and computers in a home. The network can then connect with the internet)

(WAN: wide area network. Think of the internet and the wide web)

To communicate, devices need to be connected to a network. They use IP addresses to communicate with the correct devices.



Network diagram, starting from webservice and going to various devices

Personal devices

-Computers, phones. Have IP address/MAC address as ID in a network. Devices send/receive data packets

Firewalls

-Network security (hardware or software) that monitors activity in the network, and restricts certain devices from connecting to the network, or devices in the network connecting to external places. Rules are varied for each firewall. Serves as a barrier between secured internal network and dangerous/unknown external environment

Servers

-Servers provide a service for devices on a network. Clients send requests to the server for data or tasks.

Hubs and Switches

-Used for local networks to direct network traffic. Hubs communicate incoming traffic to all devices on the network, while switches direct data packets to reach specific devices on the same network. It has a table of MAC addresses to refer to devices on the network. The switch uses the MAC address to send traffic to the right devices.

Routers

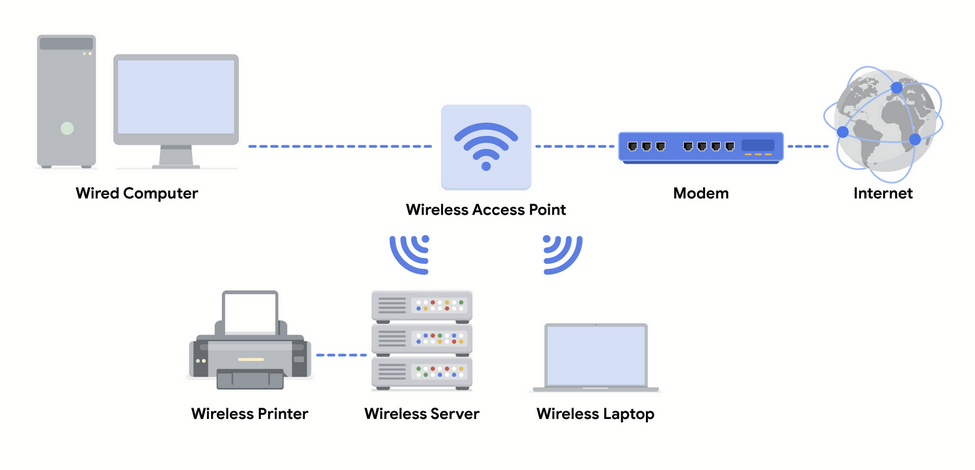
-Connects networks with direct traffic. The IP address of the destination is in the data packet. Routers pass it to different routers after reading the IP header, until it reaches the destination router. Routers can have firewalls.

Modems

-Internet connectivity by telephone cables, coaxial wires. Translates digital signals, and then sends them to the router to send messages to devices on the network.

Wireless access points

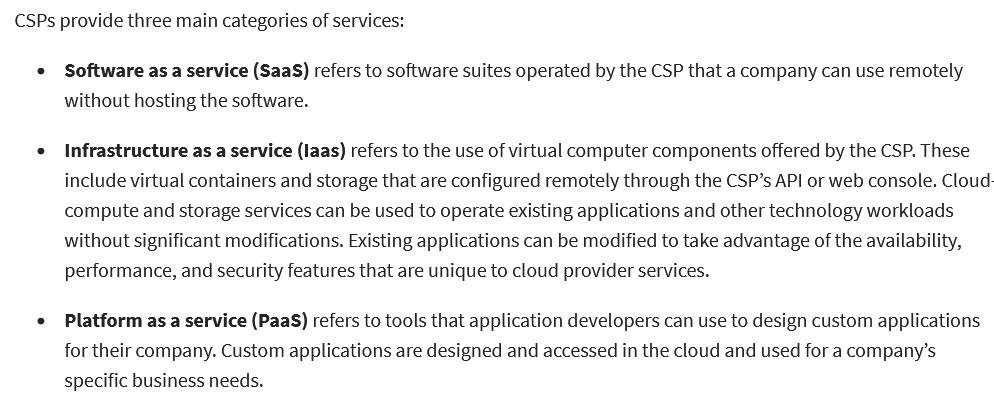
-Send data through radio waves. Wireless access points and connected devices (must have a wireless adapter) send data as radio waves to routers and switches in order to send data to the final destination.

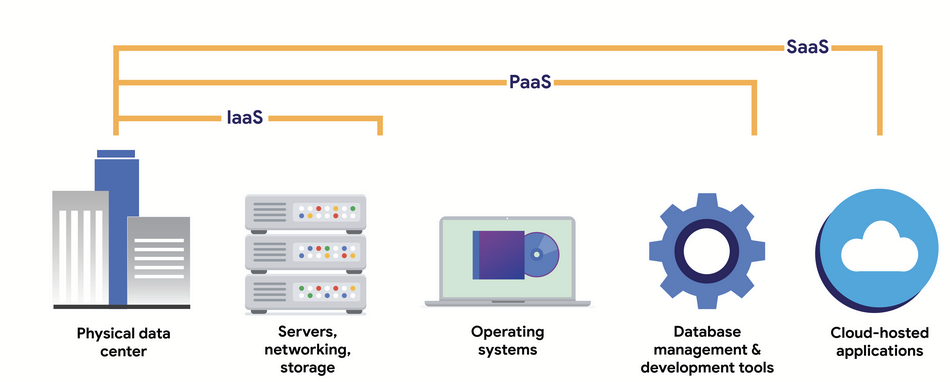


Cloud/software networks

-Cloud computing: remote servers, apps, network services hosted on internet

-CSP: virtual computers. has data centers that can store millions of servers. Companies pay for storage or other services





SDN (software defined networks): virtual network devices (firewalls, routers, etc.). Most physical network devices can now run software.

Data packet: data with header, body, and footer that goes to devices within a network

Bandwidth: amount of data a device can receive

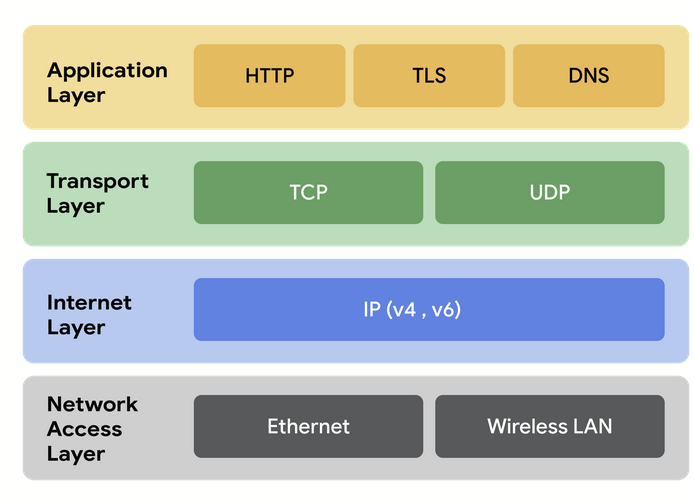
Speed: how fast data can travel to the device

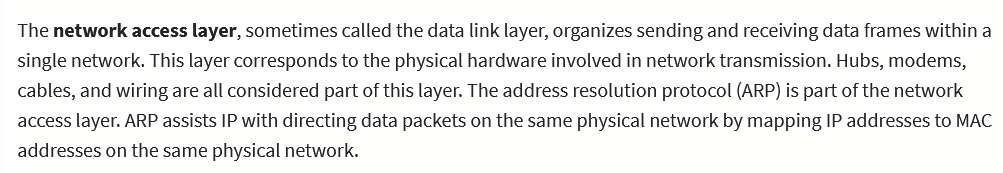
Packet sniffing: capturing, and inspecting data packets

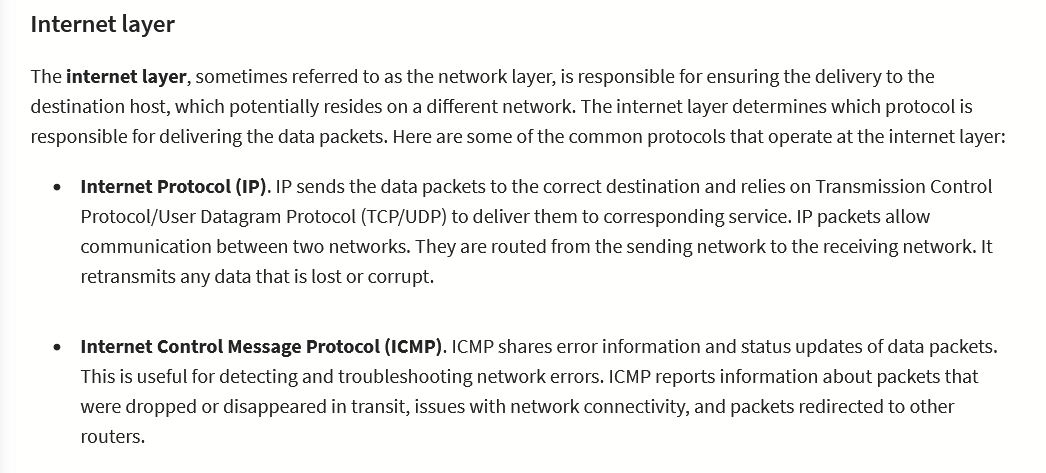
TCP(Transmission control protocol): allows devices to connect through the internet to stream data and communicate

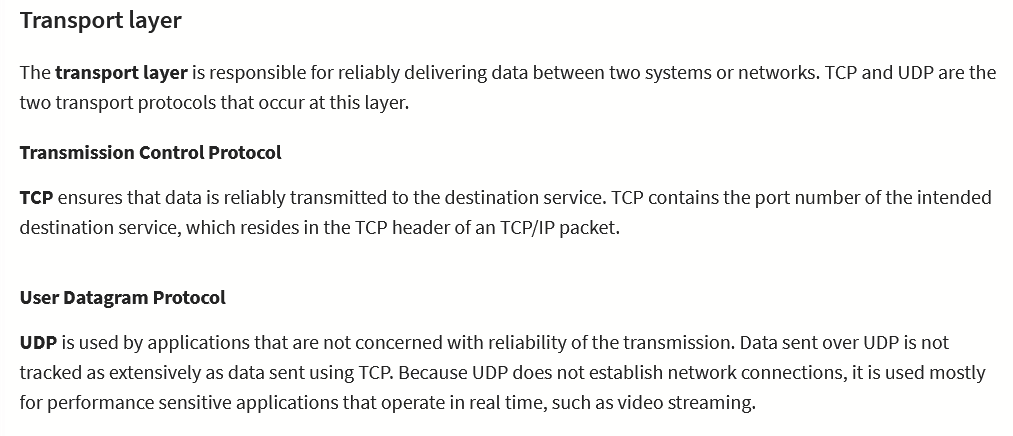
IP(Internet protocol): routing/addressing data packets as they travel between devices on a network

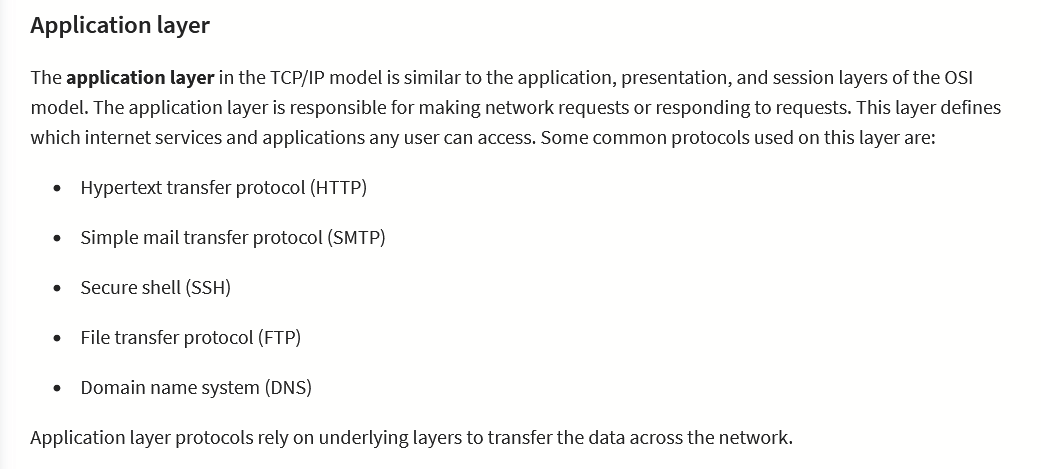
Port: software based location between devices on a network which organizes what to do with data packets received by a device. Devices know what to do with the ports (port 25 = email, port 20 = large files, etc.)



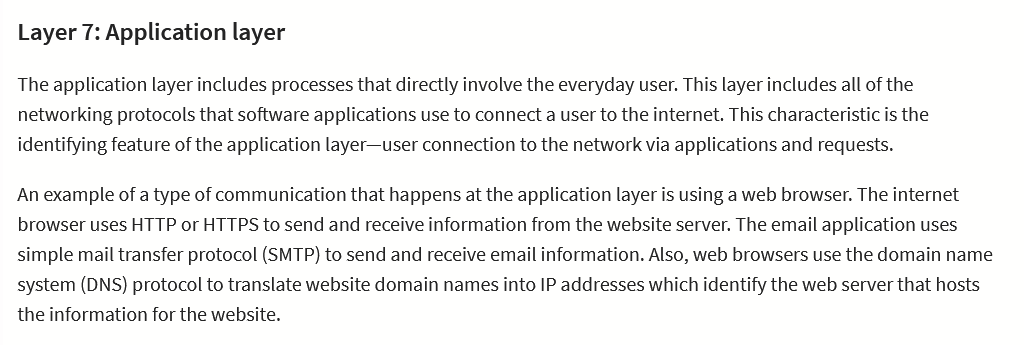


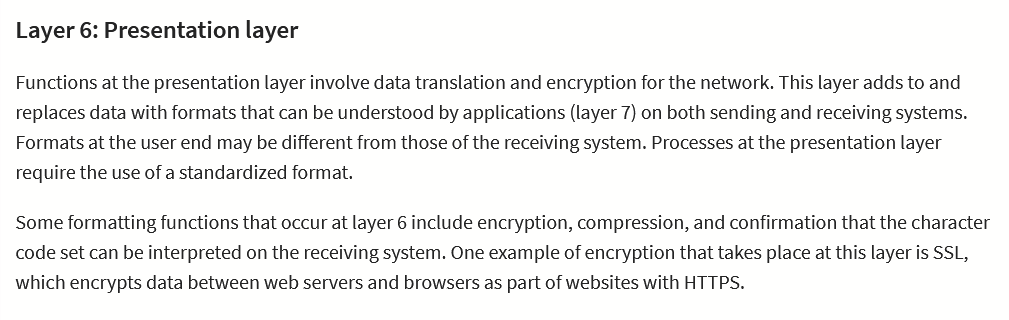


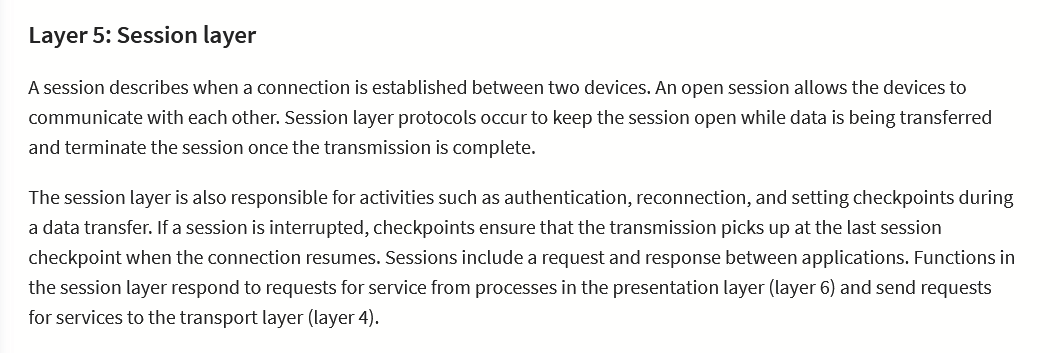


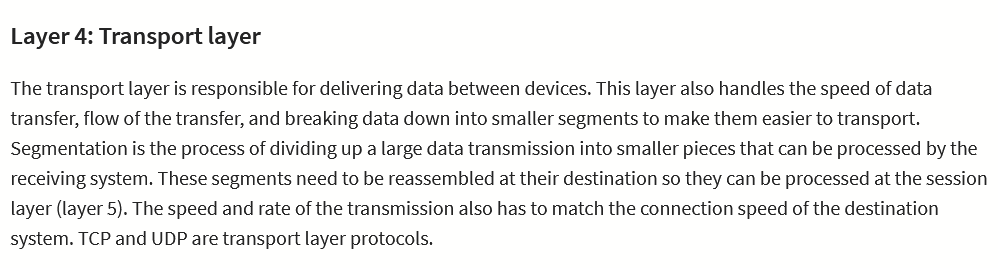


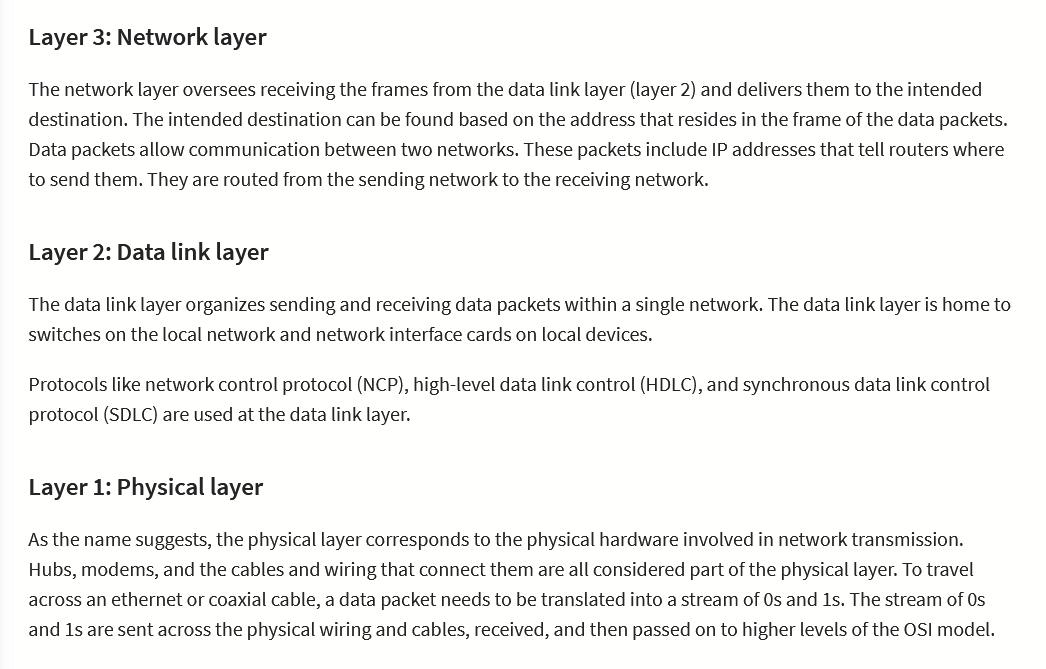
OSI (Open Systems Interconnections)











Week 2

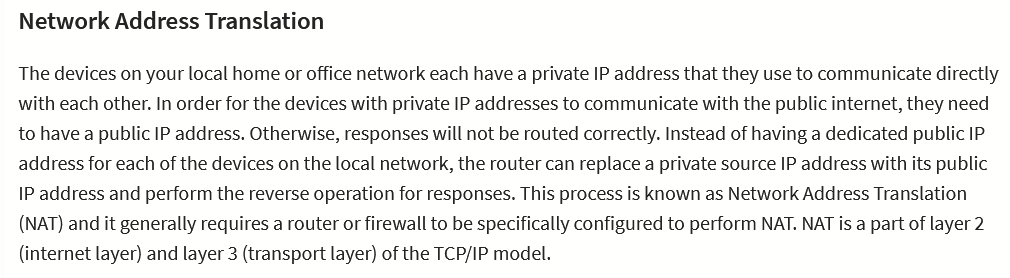
Network protocols: rules, structure of data, order of delivery. Instructions that come with the data packet: tell what to do with the data

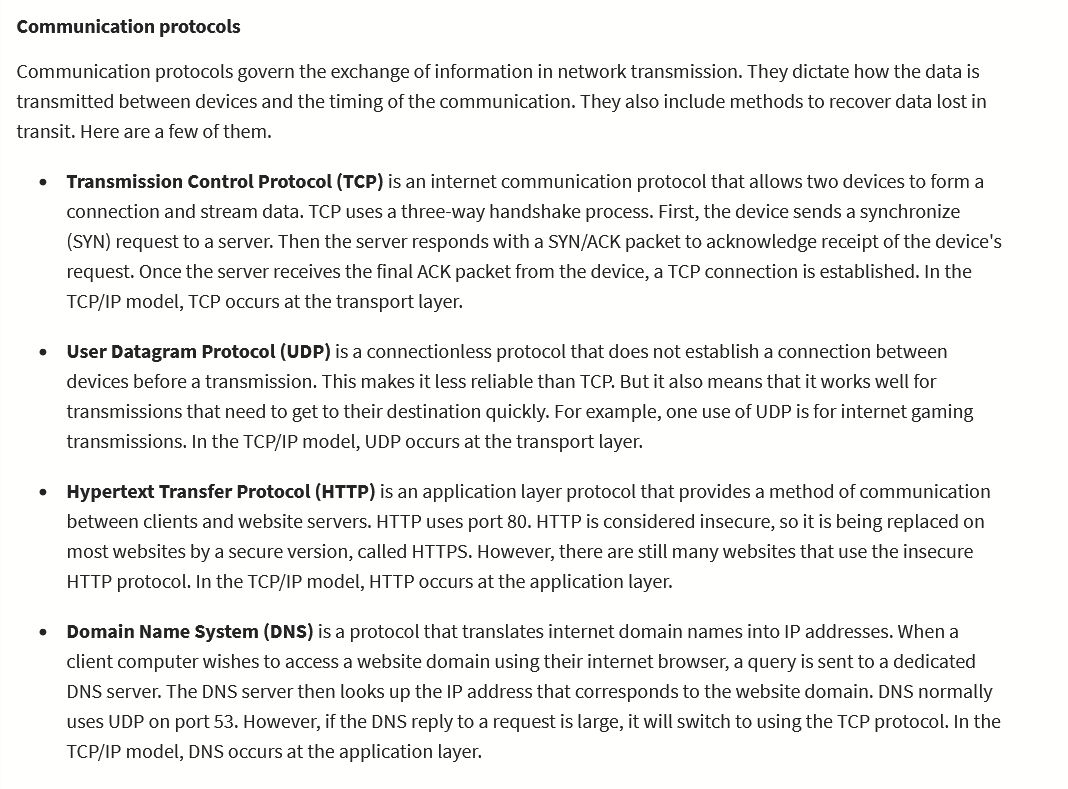
TCP(Transmission control protocol): allows devices to connect through the internet to stream data and communicate

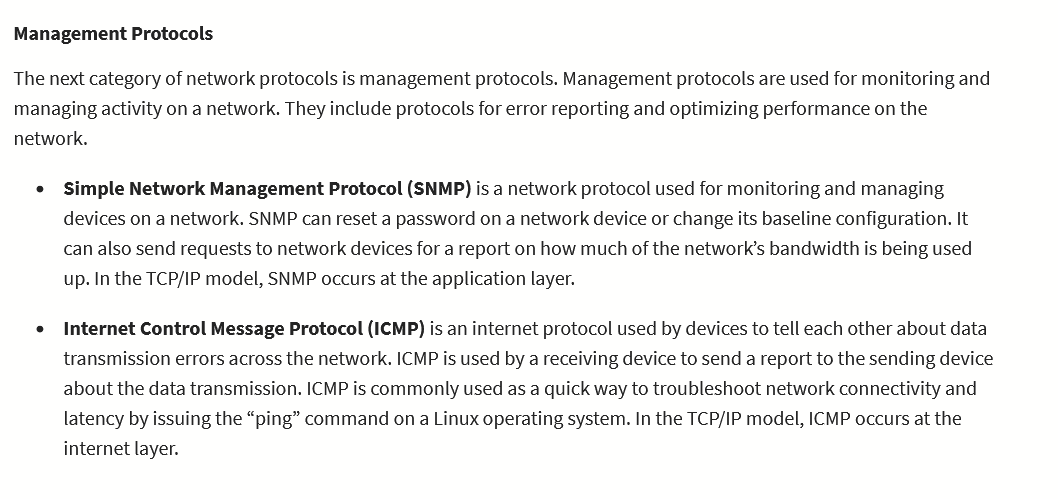
Address resolution protocol (ARP): uses MAC address to find next router or device on path

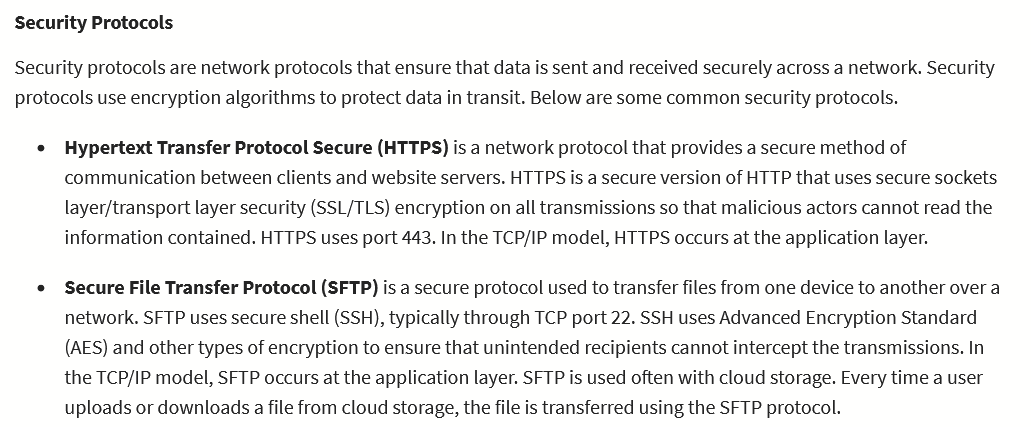
HyperText Transfer Protocol Secure: provides a secure method of communication between clients and web servers

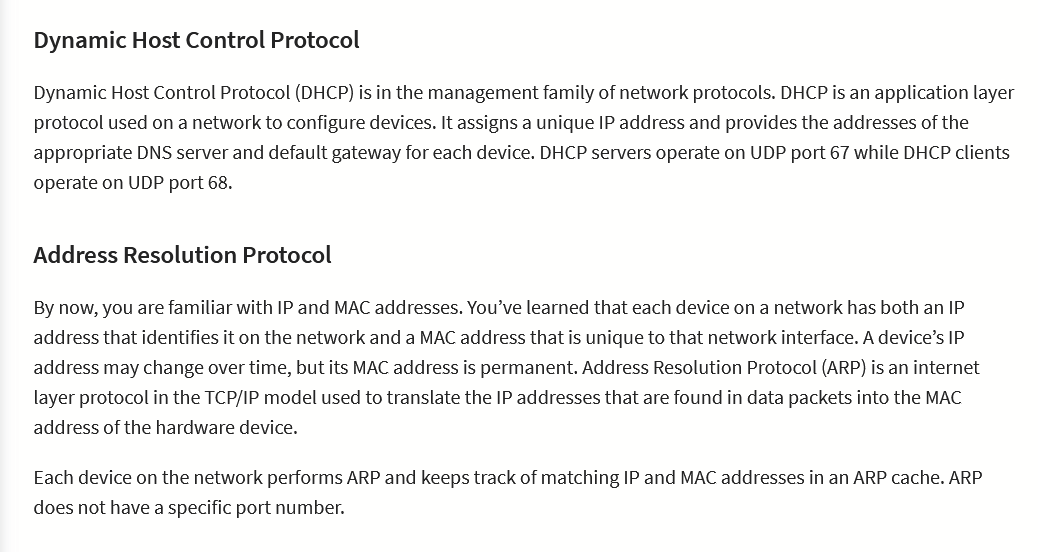
Domain Name Systems (DNS): translates internet domain names to IP addresses

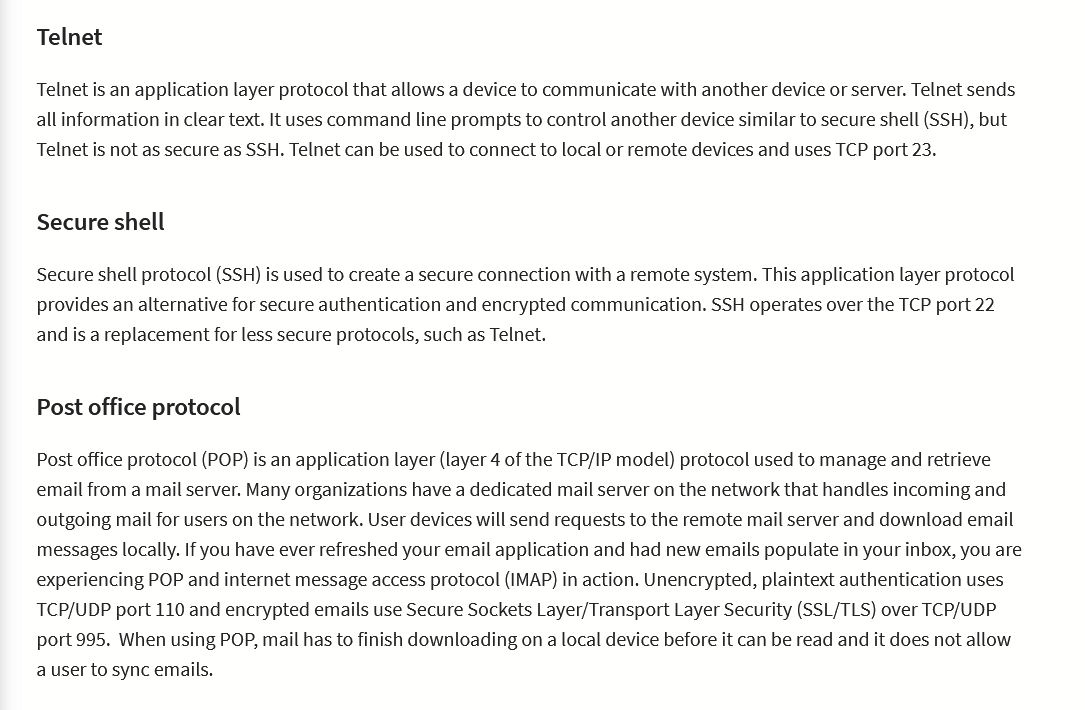


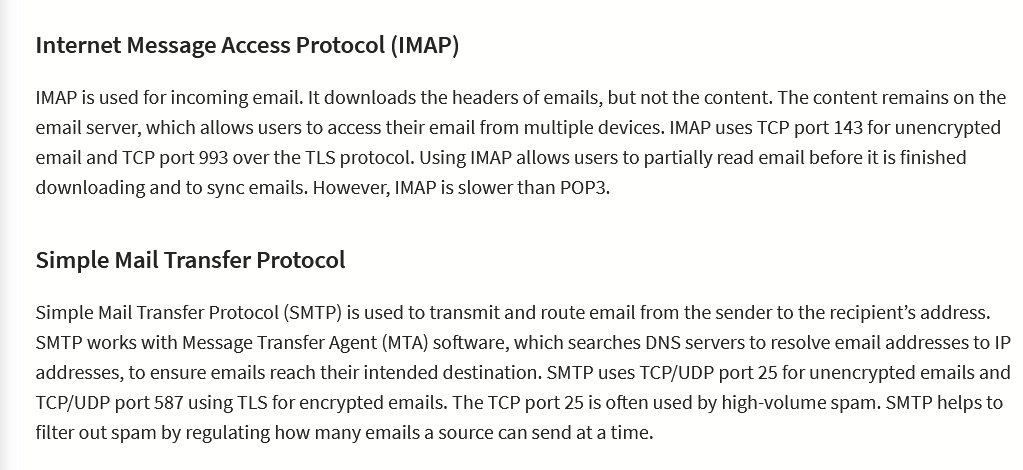




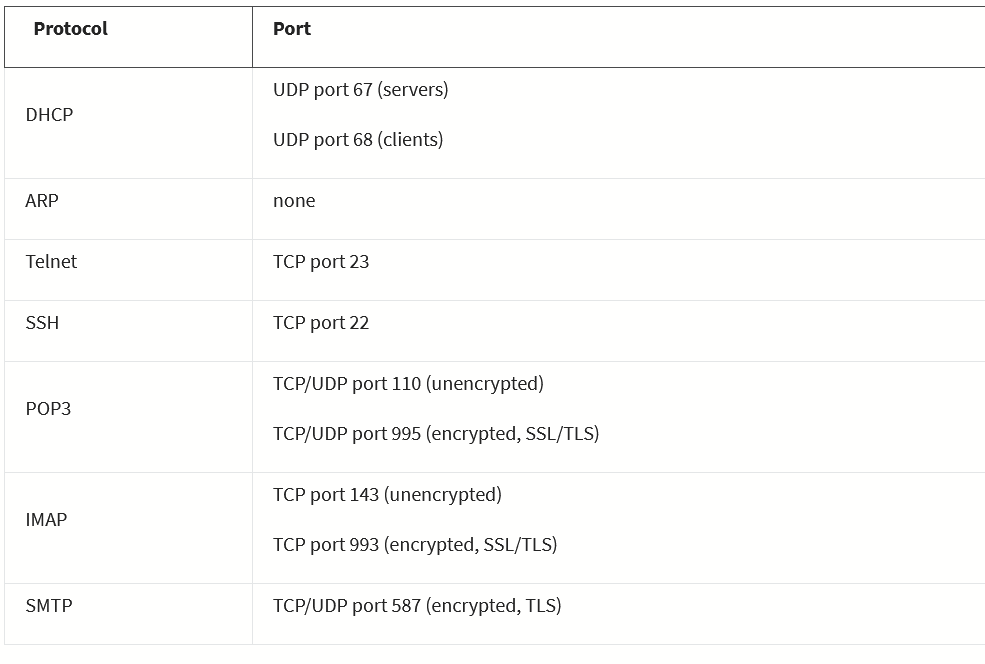








Port: what should be done with the data once it reaches its destination

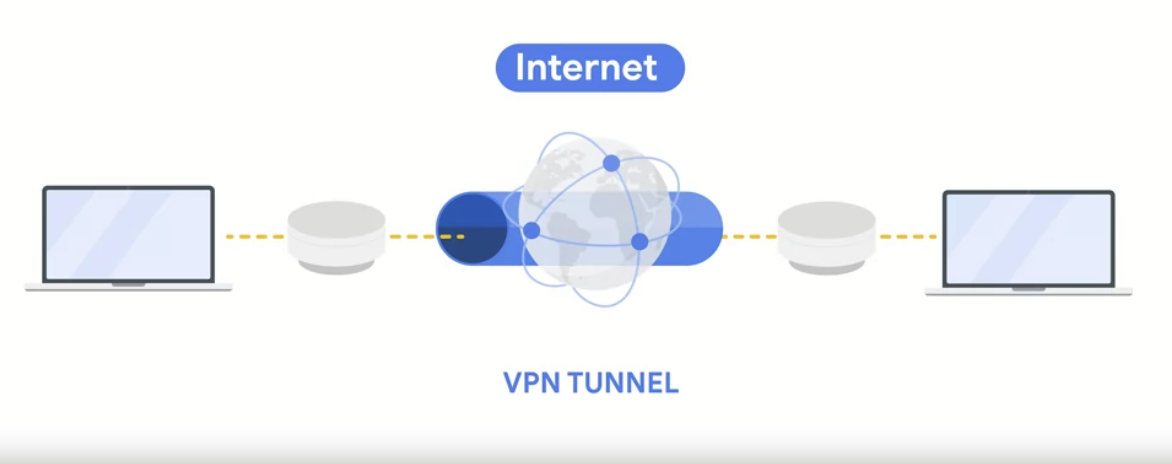


Firewalls: filter network traffic. Hardware, software, or cloud.

Port filtering: only allows data for certain ports

Stateful firewall: analyzes/stores past traffic in order to improve security

Stateless firewall: doesn’t store data, only acts on pre-programmed instructions

VPNs: change public IP, and hides physical address. Encrypts data, encapsulates (wraps data in other data packets). Encapsulation results in outer data packets which the destination can read. Also uses an unhackable VPN tunnel between device and VPN server

Security zones: segment of network that protects the internal network from the internet

Network segmentation: divides network into segments

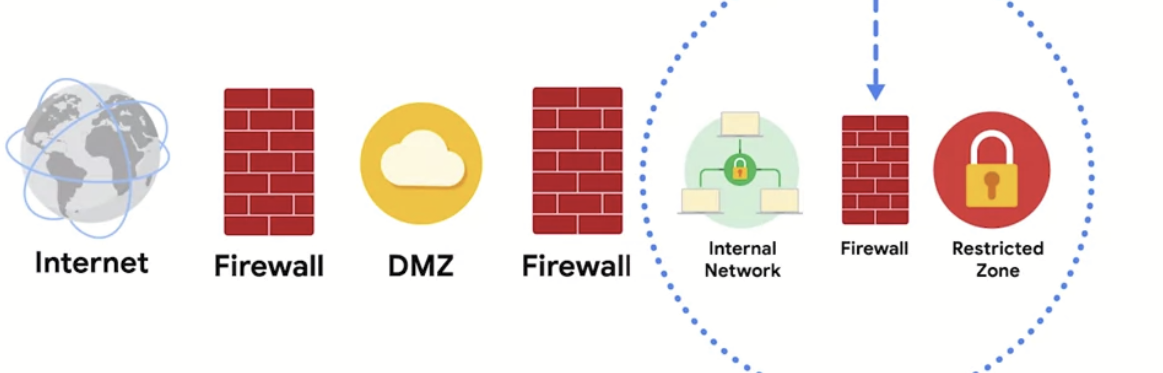
Uncontrolled zone: any network outside org’s control

Controlled zone: zone that protects from uncontrolled zone

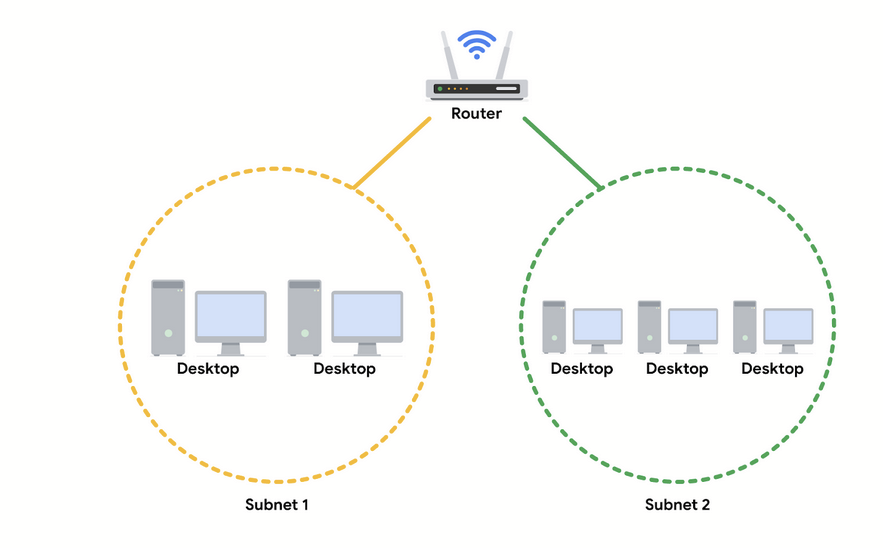
Demilitarized zone (DMZ): zone that can access the internet easily: proxy servers, DNS servers, web servers

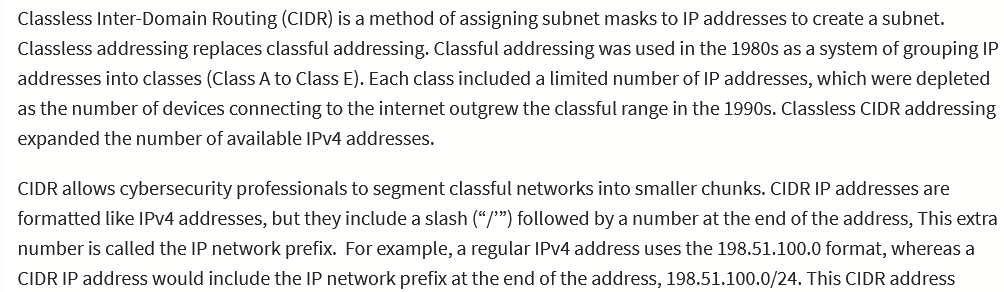
Internal network: private network that holds valuable organization assets to be protected

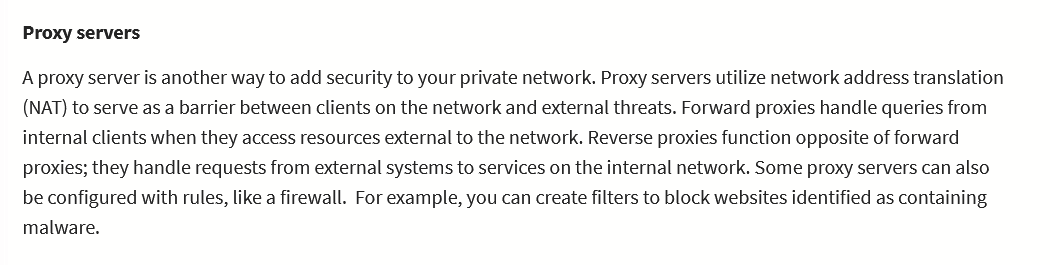
Restricted zone: highly confidential, only accessible by employees with permissions



Subnetting: dividing a larger network into smaller networks. Keeps issues isolated, improves efficiency (e.g. for switches)







Network interception: packet sniffing, or altering data packets

Backdoors: hidden entry/exit points. Steal info, malware, DoS attack (flooding network with traffic), and changing security settings

DDoS(distributed denial of service): using multiple devices/networks to flood operations with traffic

SYN attack: DoS attack where actor floods with SYN packets using a TCP connection

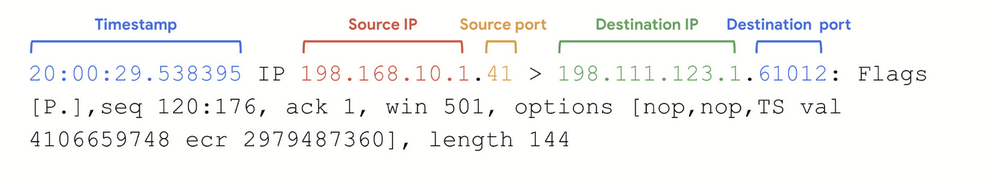
ICMP: Protocol used to tell other devices about data transmission errors

ICMP flood: Sending ICMP warnings in bulk to a network/server

Ping of death: sending one ICMP packet that is over 64kb to a system

Network protocol analyzer/packet sniffer: used to analyze packets in a network to detect suspicious activity

Tcpdump: light command line network protocol analyzer. Converts packet info to readable info for humans. unix/macos



Malicious packet sniffing: use vpn, https, secure wifi (not public ones)

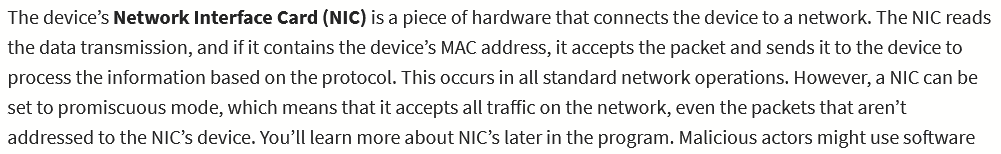
IP spoofing: used to change source IP address of data packet to gain control of the network

On path attack: intercepting/changing data being transported in an authorized connection

Replay attack: actor intercepts data packet and delays it/sends it again

Smurf attack: sniffs user IP address and floods their network with traffic

NIC



Week 4

Patch update: software/os update that addresses security vulnerabilities

Baseline configuration/image: documented specs that serve as a baseline for future patch updates/builds/releases

Password strength

Multi Factor Authentication

Brute force attacks: trial and error to gain access to private information

Simple: Threat actors guessing a combination

Dictionary attacks: Threat actors have a list of possible combinations (from breaches, or commonly used) which they use to gain access to private information

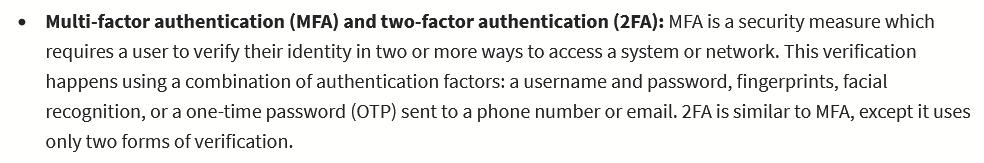
Assessing vulnerabilities

Virtual machines: Software computers. Can be used for testing/security operations at low risk: easy to wipe/reset. Also separate from real systems, easy to isolate damage due to malware. Risk that the malware can go past the VM to the real host.

Sandboxes: testing environment that can execute programs/code separate from network. They are commonly used for testing patches, identifying and addressing bugs, or detecting cybersecurity vulnerabilities. Can simulate attacks. Can be a physical device not connected to the network, or virtual machine. Attackers can write code to trick VMs and sandboxes.

Prevention techniques:

Hashing and salting: hashing turns information to a unique value which can not be uncoded. Salting adds random characters to hashed passwords.



* **CAPTCHA and reCAPTCHA:** CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It asks users to complete a simple test that proves they are human. This helps prevent software from trying to brute force a password. reCAPTCHA is a free CAPTCHA service from Google that helps protect websites from bots and malicious software.
* **Password policies:** Organizations use password policies to standardize good password practices throughout the business. Policies can include guidelines on how complex a password should be, how often users need to update passwords, and if there are limits to how many times a user can attempt to log in before their account is suspended.

Network hardening

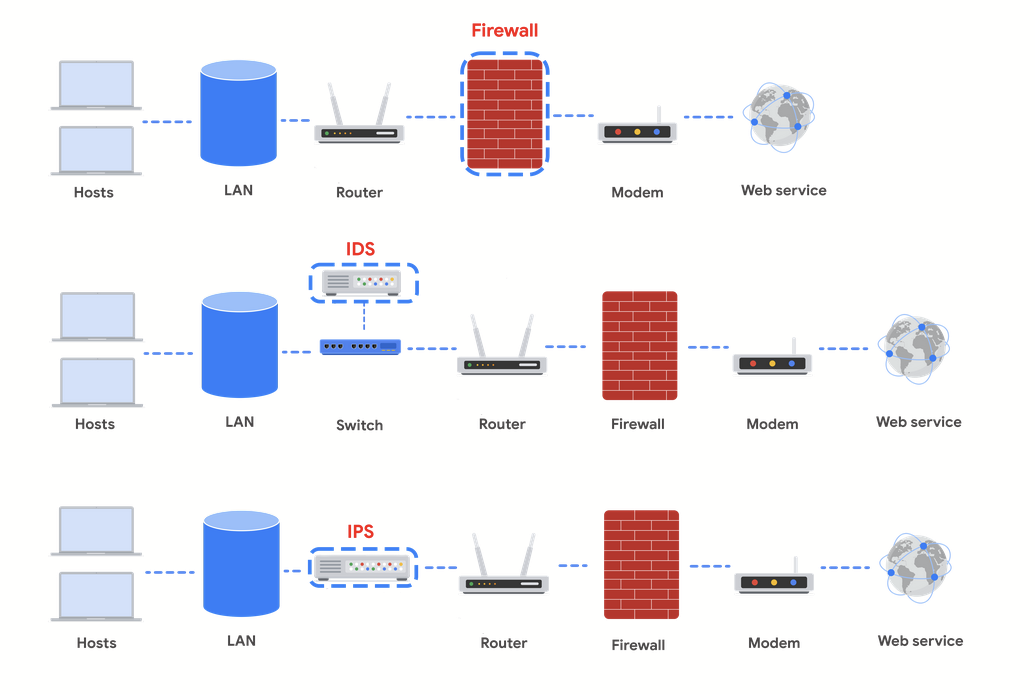
Processes: Network log analysis: examining network logs for points of interests (SIEM tools), updating firewall rules, patches, backups

One time:

Port filtering: firewall function that blocks certain ports to limit unwanted communications

Network segmentation

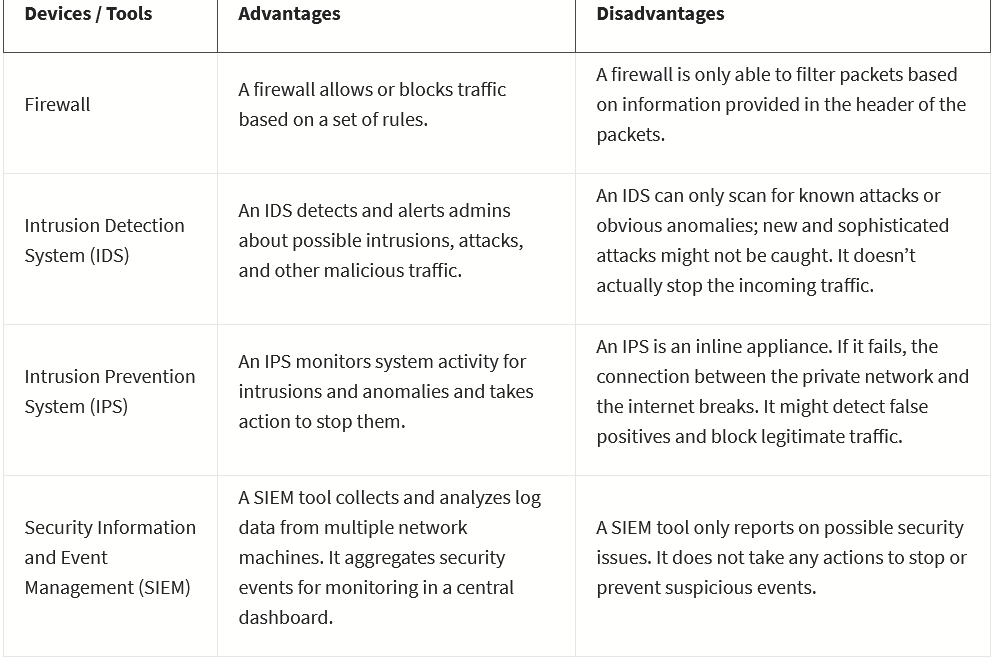
Encryption: data is encrypted using the latest encryption standards



IDS: packets sniffs and looks for signatures and patterns. Sends alerts to network admin if anomalies are found. Doesn’t stop intrusions itself, can’t detect new types of attacks. Placed after the firewall to prevent excess alerts.

IPS: same as IDS, but prevents suspected malicious data. If IPS breaks, network cant work properly (it’s inline). Can also stop legitimate traffic if it thinks that its malicious.

Full packet capture devices can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all of the data that is transmitted over your network. They also aid in investigating alerts created by an IDS.



Cloud hardening:

Cloud network: a collection of servers/computers that store data in a remote location. Can be accessed from the internet.   
Cloud provider mostly handles security of data.

Cloud baseline image: logs all data/server activity so that they can tell if intrusions/changes happened

Cloud segmentation: data/apps kept separate from each other on the cloud (done on the end of the client company)

**Identity access management (IAM)** is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can use different cloud resources. A common problem that organizations face when using the cloud is the loose configuration of cloud user roles. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations.

### **Configuration**

The number of available cloud services adds complexity to the network. Each service must be carefully configured to meet security and compliance requirements. This presents a particular challenge when organizations perform an initial migration into the cloud. When this change occurs on their network, they must ensure that every process moved into the cloud has been configured correctly. If network administrators and architects are not meticulous in correctly configuring the organization’s cloud services, they could leave the network open to compromise. Misconfigured cloud services are a common source of cloud security issues.

### **Attack surface**

Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost.

Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization’s overall attack surface. An increased attack surface must be compensated for with increased security measures.

Cloud networks that utilize many services introduce lots of entry points into an organization’s network. However, if the network is designed correctly, utilizing several services does not introduce more entry points into an organization’s network design. These entry points can be used to introduce malware onto the network and pose other security vulnerabilities. It is important to note that CSPs often defer to more secure options, and have undergone more scrutiny than a traditional on-premises network.

### **Zero-day attacks**

Zero-day attacks are an important security consideration for organizations using cloud or traditional on-premise network solutions. A **zero day** attack is an exploit that was previously unknown. CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does. CSPs have ways of patching hypervisors and migrating workloads to other virtual machines. These methods ensure the customers are not impacted by the attack. There are also several tools available for patching at the operating system level that organizations can use.

### **Visibility and tracking**

Network administrators have access to every data packet crossing the network with both on-premise and cloud networks. They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks.

This kind of visibility is also offered in the cloud through flow logs and tools, such as packet mirroring. CSPs take responsibility for security in the cloud, but they do not allow the organizations that use their infrastructure to monitor traffic on the CSP’s servers. Many CSPs offer strong security measures to protect their infrastructure. Still, this situation might be a concern for organizations that are accustomed to having full access to their network and operations. CSPs pay for third-party audits to verify how secure a cloud network is and identify potential vulnerabilities. The audits can help organizations identify whether any vulnerabilities originate from on-premise infrastructure and if there are any compliance lapses from their CSP.