Welcome to CISM Domain 2: Information Security Risk Management

- As the name indicates, in Domain 2 we look at how do we manage our risk?
- What can we do to reduce that risk to an acceptable level?
- 20% of the exam questions on the certification are from this domain.

- We identify all our assets, identify the risks, then we assess the risks with qualitative and quantitative risk analysis, we respond to the risk, mitigation, and then we monitor controls.
- We talk about attackers, and he attacks in OWASP top 10 (2021).
- We will cover how we secure our communication, software, and systems, by securing our networking, networking devices.
- We will discuss many networking basics like IP, NAT, PAT, protocols, hardware, and software, wireless and much more from networking.
- Finally, we will talk about what cloud computing is and what is our responsibility to secure and IOT.

- This should be what you are tested on for Domain 2 until the next planned CISM curriculum change in 2027.

Risk Management – Identification

Risk = Threat * Vulnerability

- **The Risk Management lifecycle is iterative.**
- Identify our Risk Management team.
- What is in and what is out of scope?
- Which methods are we using?
- Which tools are we using?
- What are the acceptable risk levels, which type of risk appetite do we have in our enterprise?
- Identify our assets:
    - Tangible: Physical hardware, buildings, anything you can touch.
    - Intangible: Data, trade secrets, reputation, …

Risk Management – Assessment

Risk Assessment

- Quantitative and Qualitative Risk Analysis.
- Uncertainty analysis.
- Everything is done on a cost-benefit analysis.
- Risk Mitigation/Risk Transference/Risk Acceptance/Risk Avoidance.
- Risk Rejection is **NEVER** acceptable.
- We assess the current countermeasures.
    - Are they good enough?
    - Do we need to improve on them?
    - Do we need to implement entirely new countermeasures?

Risk Analysis

Qualitative vs. Quantitative Risk Analysis

For any Risk analysis we need to identify our assets. What are we protecting?

- **Qualitative Risk Analysis** – How likely is it to happen and how bad is it if it happens? This is a vague guess or a feeling, and relatively quick to do. Most often done to know where to focus the Quantitative Risk Analysis.
- **Quantitative Risk Analysis** – What will it actually cost us in $? This is fact-based analysis, Total $ value of asset, math is involved.
- **Threat** – A potentially harmful incident (Tsunami, Earthquake, Virus, …)
- **Vulnerability** – A weakness that can allow the Threat to do harm. Having a data center in the tsunami flood area, not earthquake resistant, not applying patches and antivirus, …
- **Risk** = ***Threat x Vulnerability***.
- **Impact** - Can at times be added to give a fuller picture. Risk = Threat x Vulnerability x Impact (How bad is it?).
- **Total Risk** = ***Threat x Vulnerability x Asset Value.***
- **Residual Risk** = ***Total Risk – Countermeasures.***

Qualitative Risk Analysis with the Risk Analysis Matrix

Let's pick an asset, A laptop.

- How likely is one to get stolen or left somewhere?
  I would think possible or likely.
- How bad is it if it happens?
  That really depends on a couple of things:
    - Is it encrypted?
    - Does it contain classified or PII/PHI content?
- Let's say it is likely and a minor issue, that puts the loss the high-risk category.

Likelihood \ Consequences	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Possible	L	M	H	H	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

Where the L, M, H, E is for your organization can be different from this.
L = Low, M = Medium, H = High, E = Extreme Risk

It is normal to move high and extreme on to quantitative risk analysis. If mitigation is implemented, we can maybe move the risk level to "Low" or "Medium".

Risk Registers

Category	Name	Risk #	Probability	Impact	Mitigation	Contingency	Risk Score after Mitigation	Action By	Action When

- A risk category to group similar risks.
- The risk breakdown structure identification number
- A brief description or name of the risk to make the risk easy to discuss.
- The impact (or consequence) if event actually occurs rated on an integer scale.
- The probability or likelihood of its occurrence rated on an integer scale.
- The Risk Score (or Risk Rating) is the multiplication of Probability and Impact and is often used to rank the risks.
- Common mitigation steps (e.g., within IT projects) are Identify, Analyze, Plan Response, Monitor and Control.

Quantitative Risk Analysis

This is where we put a number on our assets and risks.

- We find the asset's value: How much of it is compromised, how much one incident will cost, how often the incident occurs and how much that is per year.
  - Asset Value **(AV)** – How much is the asset worth?
  - Exposure factor **(EF)** – Percentage of Asset lost?
  - Single Loss Expectancy **(SLE)** = **(AV x EF)** – What does it cost if it happens once?
  - Annual Rate of Occurrence **(ARO)** – How often will this happen each year?
  - Annualized Loss Expectancy **(ALE)** – This is what it costs per year if we do nothing.
- Total Cost of Ownership **(TCO)** – The mitigation cost: upfront + ongoing cost (Normally Operational)

Let's look at a few examples.

Quantitative Risk Analysis
Laptop – Theft/Loss (unencrypted)

	Value
Asset Value (AV)	$10,000
Exposure factor (EF)	100%
Single Loss Expectancy (SLE) – (AV x EF)	$10,000
Annual Rate of Occurrence (ARO)	25
Annualized Loss Expectancy (ALE)	$250,000

The Laptop ($1,000) + PII ($9,000) per loss (AV)
It is a 100% loss, it is gone (EF)
Loss per laptop is $10,000 (AV) x 100% EF) = (SLE)
The organization loses 25 Laptops Per Year (ARO)
The annualized loss is $250,000 (ALE)

Data Center – Flooding

	Value
Asset Value (AV)	$10,000,000
Exposure factor (EF)	15%
Single Loss Expectancy (SLE) – (AV x EF)	$1,500,000
Annual Rate of Occurrence (ARO)	0.25
Annualized Loss Expectancy (ALE)	$375,000

The Data Center is valued at $10,000,000 (AV)
If a flooding happens, 15% of the DC is compromised (EF)
Loss per Flooding is $10,000,000 (AV) x 15% EF) = (SLE)
The flooding happens every 4 years = 0.25 (ARO)
The annualized loss is $375,000 (ALE)

For the example let's use a 4-year tech refresh cycle.

- Full disk encryption software and support = $75,000 initial and $5,000 per year.
- Remote wipe capabilities for the laptop = $20,000 initial and $4,000 per year.
- Staff for encryption and help desk = $25,000 per year

Doing nothing costs us $1,000,000 per tech refresh cycle ($250,000 per year).
Implementing full disk encryption and remote wipe will cost $231,000 per tech refresh cycle ($57,750 per year)

The laptop hardware is a 100% loss, regardless. What we are mitigating is the 25 x $9,000 = $225,000 by spending $57,750.

This is our ROI (Return on Investment): TCO ($57,750) < ALE ($250,000). This makes fiscal sense, we should implement.

Types of Risk Responses:

- **Accept the Risk** – We know the risk is there, but the mitigation is more costly than the cost of the risk (Low risks). We ensure we have a paper trail, and this was a calculated decision.
- **Mitigate the Risk (Reduction)** – The laptop encryption/wipe is an example – acceptable level (Leftover risk = Residual).
- **Transfer the Risk** – The insurance risk approach – We could get flooding insurance for the data center, the flooding will still happen, we will still lose 15% of the infrastructure, but we are insured for cost.
- **Risk Avoidance** – We don't issue employees laptops (if possible), or we build the data center in an area that doesn't flood. (Most often done before launching new projects – this could be the data center build).
- **Risk Rejection** – You know the risk is there, but you are ignoring it. This is **never** acceptable. (You are liable).
- **Secondary Risk** – Mitigating one risk may open another risk.

This is area very testable, learn the formula, the risk responses to differentiate Qualitative and Quantitative Risk.

Qualitative = Think "quality." This concept is semi-vague, e.g., "pretty good quality. "
Quantitative = Think "quantity." How many; a specific number.

NIST 800-30

NIST 800-30 - United States National Institute of Standards and Technology Special Publication

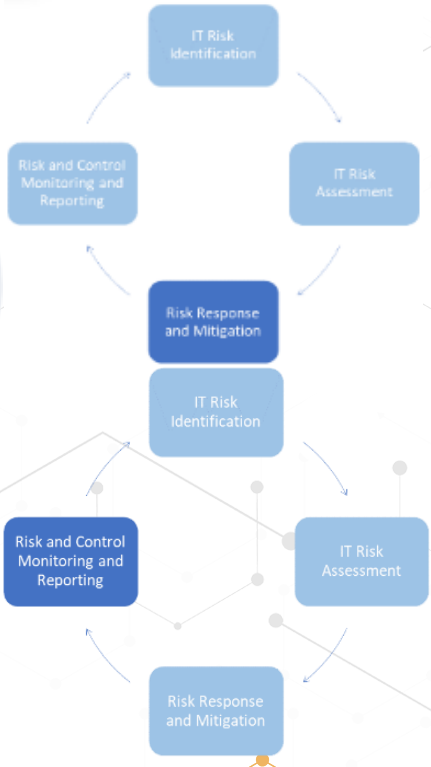
- A 9-step process for Risk Management.
    1. System Characterization (Risk Management scope, boundaries, system, and data sensitivity).
    2. Threat Identification (What are the threats to our systems?).
    3. Vulnerability Identification (What are the vulnerabilities of our systems?).
    4. Control Analysis (Analysis of the current and planned safeguards, controls, and mitigations).
    5. Likelihood Determination (Qualitative – How likely is it to happen)?
    6. Impact Analysis (Qualitative – How bad is it if it happens? Loss of CIA).

7. Risk Determination (Look at 5-6 and determine Risk and Associate Risk Levels).
8. Control Recommendations (What can we do to Mitigate, Transfer, … the risk).
9. Results Documentation (Documentation with all the facts and recommendations).

Risk Management

Risk Response and Mitigation

- Risk mitigation, transference, acceptance, or avoidance.
- We act on senior managements choices, which they made based on our recommendations from the assessment phase.
- Do we stop issuing laptops, or do we add full-disk encryption and remote wipe capabilities?
- We update the risk register, with the mitigations, the risk responses we chose and see if the new risk level is acceptable.



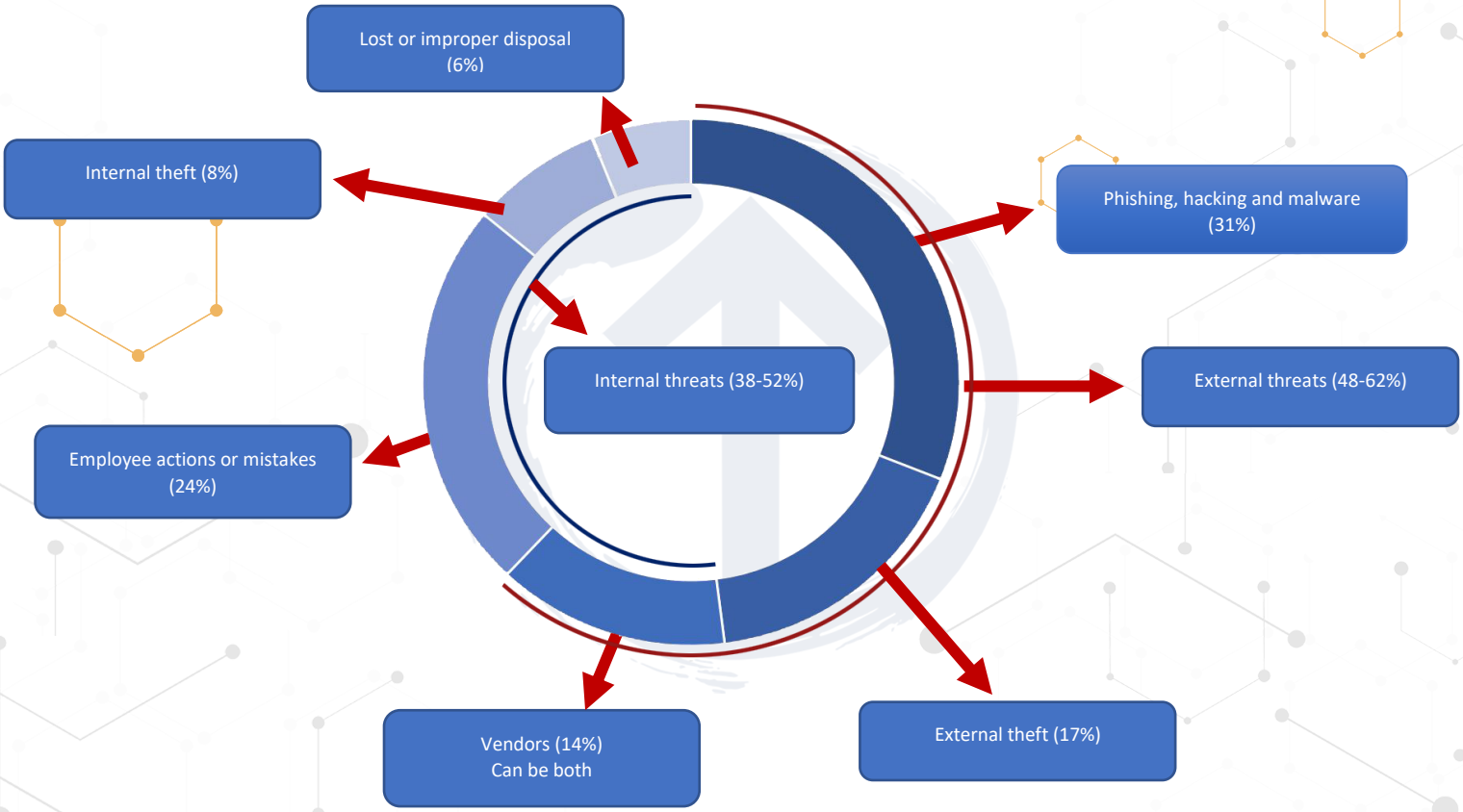
Risk and Control Monitoring and Reporting

- The process is ongoing, we have to keep monitoring both the risk and the controls we implemented.
- This is where we would use the KRIs (Key Risk Indicators).
- We would also use KPIs (Key Performance Indicators).
- You are the translating link; you have to be able to explain IT and IT
- Security to Senior Management in terms they can understand.
- It is normal to do the Risk Management lifecycle on an annual basis and do out-of-cycle Risk Management on critical items.

Types of Attackers

- **Hackers:**
  - **Now:** Anyone trying to get access to or disrupt any leg of the CIA Triad (Confidentiality, Integrity, Availability).
  - **Original use:** Someone using something in a way not intended.
  - **White Hat hackers:** Professional pen testers trying to find flaws so we can fix it (Ethical hackers).
  - **Black Hat hackers:** Malicious hackers, trying to find flaws to exploit them (Crackers – they crack the code).

- **Gray/Grey Hat hackers:** They are somewhere between the white and black hats, they go looking for vulnerable code, systems, or products. They often just publicize the vulnerability (which can lead to black hats using it before a patch is developed). Gray hats sometimes also approach the company with the vulnerability and ask them to fix it and if nothing happens, they publish.
- **Script Kiddies:** They have little or no coding knowledge, but many sophisticated hacking tools are available and easy to use. They pose a very real threat. They are just as dangerous as skilled hackers; they often have no clue what they are doing.

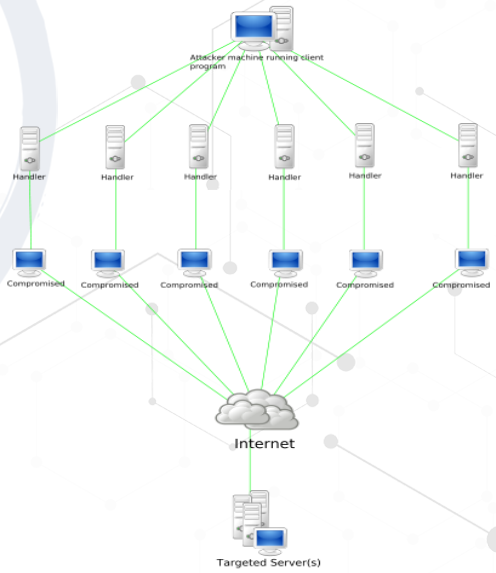


- **Outsiders:**
  - Unauthorized individuals - Trying to gain access; they launch the majority of attacks but are often mitigated if the organization has good Defense in Depth.
  - Interception, malicious code (e.g., virus, logic bomb, trojan horse), sale of personal information, system bugs, system intrusion, system sabotage or unauthorized system access.
  - 48-62% of risks are from outsiders.
- **Insiders:**

- Authorized individuals - Not necessarily to the compromised system, who intentionally or unintentionally compromise the system or data.
- This could be Assault on an employee, blackmail, browsing of proprietary information, computer abuse, fraud and theft, information bribery, input of falsified or corrupted data.
- 38-52% of risks are from insiders, another reason good Authentication and Authorization controls are needed.

- **Hacktivism/Hacktivist (hacker activist):**
  - Hacking for political or socially motivated purposes.
  - Often aimed at ensuring free speech, human rights, freedom of information movement.

- **Governments:**
  - State sponsored hacking is common; often you see the attacks happening between the hours of 9 and 5 in that time zone; this is a day job.
  - Approximately 120 countries have been developing ways to use the internet as a weapon to target financial markets, government computer systems and utilities.
  - Famous attacks: US elections (Russia), Sony websites (N. Korea), Stuxnet (US/Israel), US Office of Personnel Management (China), …
- **Bots and botnets** (short for robot):
  - **Bots** are a system with malware controlled by a botnet.
  - The system is compromised by an attack or the user installing a remote access Trojan (game or application with a hidden payload).
  - They often use IRC, HTTP or HTTPS.
  - Some are dormant until activated.
  - Others are actively sending data from the system (Credit card/bank information for instance).
  - Active bots can also be used to send spam emails.
- **Botnets** is a C&C (Command and Control) network, controlled by people (bot-herders).
  - There can often be 1,000's or even 100,000's of bots in a botnet.



- **Phishing, spear phishing and whale phishing** (Fishing spelled in hacker speak with Ph not F).
  - **Phishing** (Social engineering email attack):
    - Click to win, send information to get your inheritance, …
    - Sent to hundreds of thousands of people; if just 0.02% follow the instructions they have 200 victims.
  - **Spear Phishing:** Targeted phishing, not just random spam, but targeted at specific individuals.
    - Sent with knowledge about the target (person or company); familiarity increases success.
  - **Whale Phishing (Whaling):** Spear phishing targeted at senior leadership of an organization.

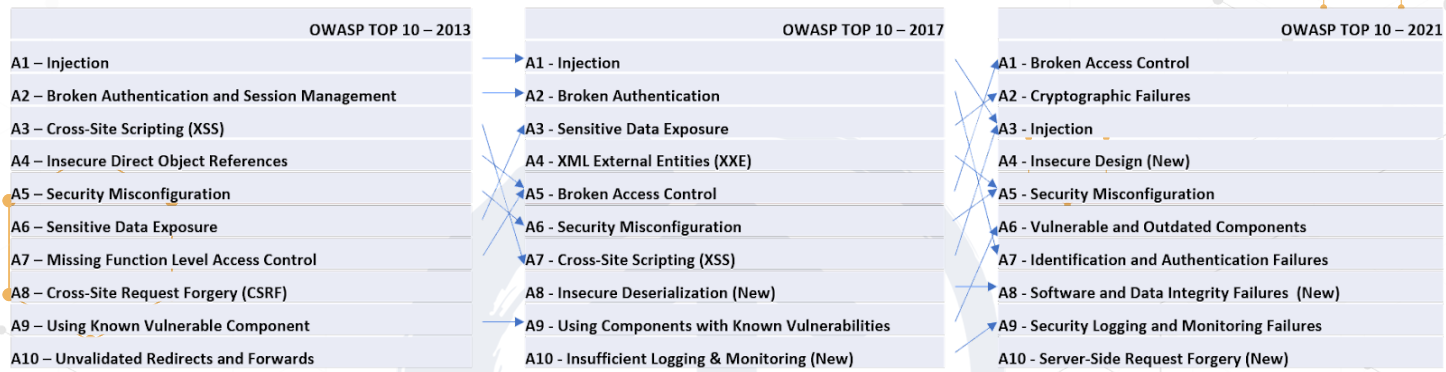
- This could be: “Your company is being sued if you don’t fill out the attached documents (with trojan in them) and return them to us within 2 weeks”.

- **Vishing (Voice Phishing):** Attacks over automated VOIP (Voice over IP) systems, bulk spam similar to phishing.
  - These are: “Your taxes are due”, “Your account is locked” or “Enter your PII to prevent this” types of calls.

Software Vulnerabilities and Attacks

OWASP (Open Web Application Security Project):

- Top 10 of the most common web security issues



https://owasp.org/www-project-top-ten/

- **A01:2021 - Broken Access Control:**
  - It is not implemented consistently across an entire application.
  - It can be done correctly in one location but incorrectly in another.
  - We need a centralized access control mechanism, and we write the tricky logic once and reuse it everywhere.
  - This is essential both for writing the code correctly and for making it easy to audit later.
  - Many access control schemes were not deliberately designed but have simply evolved along with the website.
  - Inconsistent access control rules are often inserted in various locations all over the code, making it near impossible to manage.
  - One especially dangerous type of access control vulnerability arises from web-accessible administrative interfaces, frequently used to allow site administrators to efficiently manage users, data, and content on their site.

  - **What can we do?**
    We can deny by default, limit user rights, use role-based access control, strong passwords, MFA, log/act on access control failures, proper user, and session management, ...

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

- **A02:2021 - Cryptographic Failures:**
  - Sites are HTTP rather than HTTPS.
  - Data is sent in cleartext.
  - Backups, data at rest and data in transit are not encrypted (stored/transmitted in plain text).
  - Using older, weaker, and deprecated encryption algorithms.
  - Using depreciated hash functions.
  - Not monitoring if data is being exfiltrated.
  - Improper use of initialization vectors.

  - **What can we do?**
    We ensure we do not use depreciated encryption, data is identified and protected properly, no clear-text, proper implementation of up-to-date encryption/protocols/keys, no caching for responses with sensitive data, only store sensitive data as long as required, …
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

- **A03:2021 – Injection:**
  - Can be any code injected into user forms. Often seen is SQL/NoSQL/OS command/LDAP.
  - Attackers can do this because our software does not use:
    - Strong enough input validation and data type limitations input fields.
    - Input length limitations.
  - **CGI (Common Gateway Interface):**
    - Standard protocol for web servers to execute programs running on a server that generates web pages dynamically. We use the interface to ensure only proper input makes it to the database.
      - The CGI separates the untrusted (user) from the trusted (database).

  - **What can we do?**
    - The fix is to do just that, we only allow users to input appropriate data into the fields, only letters in names, numbers in phone number, have dropdowns for country and state (if applicable), we limit how many characters people can use per cell, use secure APIs, ...
    - Separating the data from the web application logic.
    - Implement settings and/or restrictions to limit data exposure in case of successful injection attacks.
- https://owasp.org/Top10/A03_2021-Injection/

- **A04:2021 - Insecure Design:**
  - When we design our web applications, we need to design them securely.
  - This does not have to be design flaws, it can also be anything that is not secure, any weakness that an attacker could exploit.
  - Not to be confused insecure implementation.
    - We can have a securely designed app and still implement it insecurely.
    - However, we can't fix an insecure design with a flawless implementation.

- **What can we do?**
  - We have our software developers use secure design patterns and reference architectures to build applications.
  - Our organization should have libraries with references and patterns.
  - Before finalizing our application design, we use a red team to do threat modeling and penetration testing.

- https://owasp.org/Top10/A04_2021-Insecure_Design/

- **A05:2021 - Security Misconfiguration:**
  - Databases configured wrong.
  - Not removing out-of-the-box default access and settings.
  - Keeping default usernames and passwords.
  - VM, OS, webserver, DBMS, applications, are not patched and up to date.
  - Unnecessary features are enabled or installed. This could be open ports, services, pages, accounts, privileges, ...
  - With so much being cloud now, it is only natural that misconfiguration is more prevalent, so many more options admins can disable.

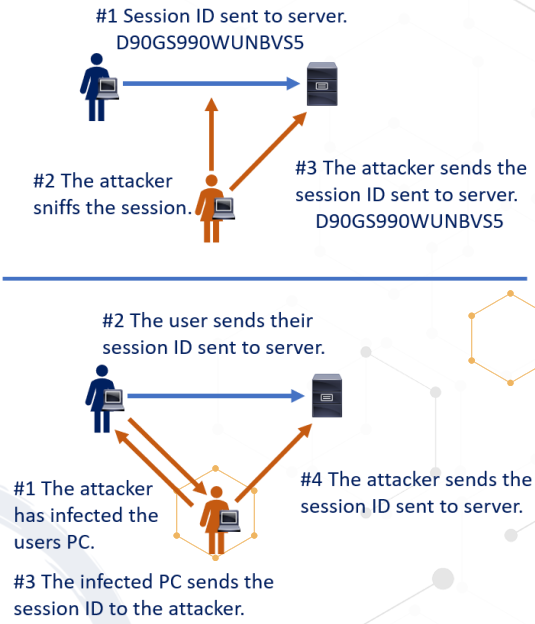
  - **What can we do?**
  - It is simple; server hardening, proper patching, do not disable security features unless we are completely clear on why and we have done proper risk analysis.
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

- **A06:2021 - Vulnerable and Outdated Components:**
  - Vulnerable components can be both client and server-side (OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, libraries,).
  - Developers use deprecated code or objects that are known to be unsecure.
    - Mostly happens because developers are used to the old code or the library, they could be uncertain about new code, or they are afraid to break anything.

  - **What can we do?**
  - Proper patch management, scan for vulnerabilities, make sure we don't use deprecated code, keep a continuous inventory of both server-side and client-side components and their dependencies, delete unused programs and features.
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

- **07:2021 - Identification and Authentication Failures:**
  - Sessions do not expire or take too long to expire.
  - Session IDs are predictable or part of the URL; 001, 002, 003, 004, …
  - Tokens, Session IDs, Passwords, are kept in plaintext or are poorly protected (poor encryption and hashing).
  - Weak/default passwords and knowledge-based password recovery.

  - **What can we do?**
  - MFA, sessions expire, non-predictable sessions, no plaintext anywhere, no session ID in URL, proper secure encryption, no default/weak passwords, log login failures, alert admins when detecting brute force, credential stuffing, and any other attacks.



- https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

- **A08:2021 - Software and Data Integrity Failures:**
  - When our applications use code, plugins, libraries, or modules from untrusted sources.
  - Insecure CI/CD pipelines or unverified updates.
  - Software with automatic updates without enough integrity checks.

  - **What can we do?**
  - Use digital signatures/hashes to verify the code/data is from the right source and is unaltered.
  - Make sure libraries and dependencies are using trusted repositories.
  - Deploy software supply chain tools to make sure components do not contain known vulnerabilities.
  - Ensure our CI/CD pipeline has proper segregation, configuration, and access control.
    - This should ensure the integrity of the code throughout the build and deploy processes.
- https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

- **A09:2021 - Security Logging and Monitoring Failures:**
  - When our intrusion monitoring and reporting system fail to catch and report signs of intrusion.
  - Result of poor configuration, low thresholds, or logs saved just locally.
  - Attacks go unnoticed if we do not act on appropriate logs or alerts.

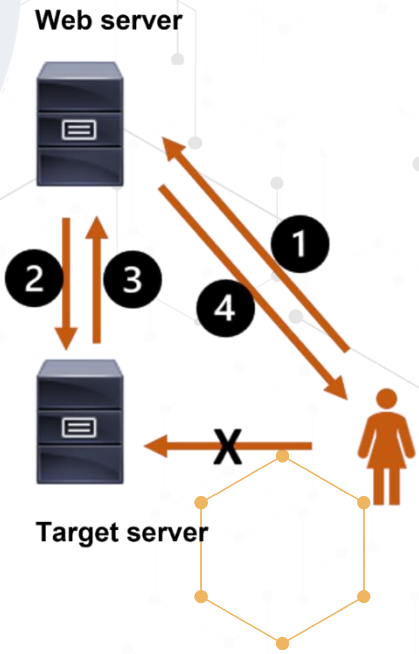
  - **What can we do?**

- Implement proper monitoring and logging, ensure we log/report all failed login attempts and server-side validations.
- Logs are generated in a format that our log management system can easily use, logs are kept long enough.
- Logs are kept secure and protected against injection or any other type of attack.
- Audit trails on high-value transactions.
- Have a proper incident response and recovery plan.

- https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures

- **A10:2021 - Server-Side Request Forgery:**
  - Web applications usually trigger requests between HTTP servers, to fetch remote resources, such as software updates, or to import metadata from a URL or another web application.
  - Usually benign, but if not implemented correctly, they can make a server vulnerable to SSRF.
  - Normally an attacker can't access an internal server because it would be blocked by the firewall. To get around that the attacker can exploit an SSRF vulnerability to launch their attack using a vulnerable web server.
  - The attacker changes a parameter value in the vulnerable web application to create or control requests from the vulnerable server.

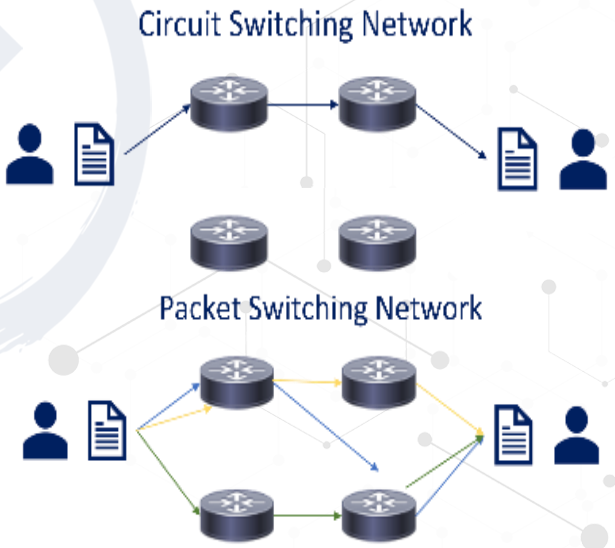
  - **What can we do?**
    - **Network layer:** Segment remote resource access functionality in separate networks. Enforce "deny by default" to block all non-essential intranet traffic.
    - **Application layer:** Sanitize and validate all client-supplied input data.
    - Enforce the URL schema, port, and destination with a positive allow list.
    - Do not send raw responses to clients. Disable HTTP redirections.



- https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

Network Basics and Definitions

- We use defense-in-depth on our internal network and when our data traverses the internet.
  - We do this by ensuring all our network devices, protocols and traffic are as secure as possible.
  - **Simplex** is a one-way communication (One system transmits, the other listen).
  - **Half-duplex** communication sends or receives at one time only (Only one system can transmit at a time).
  - **Full-duplex** communication sends and receives simultaneously. (Both systems can transmit/receive simultaneously).
  - **Baseband** networks have one channel and can only send one signal at a time.
    - Ethernet is baseband: "1000baseT" STP cable is a 1000-megabit, baseband, Shielded Twisted Pair cable.
  - **Broadband** networks have multiple channels and can send and receive multiple signals at a time.
  - The **Internet** is a global collection of peered WAN networks, it really is a patchwork of ISP's.
  - An **Intranet** is an organization's privately owned network, most larger organizations have them.
  - An **Extranet** is a connection between private Intranets, often connecting business partners' Intranets.
  - **Circuit switching -** Expensive, but always available, used less often.
  - A dedicated communications channel through the network.
  - The circuit guarantees the full bandwidth.
  - The circuit functions as if the nodes were physically connected by a cable.



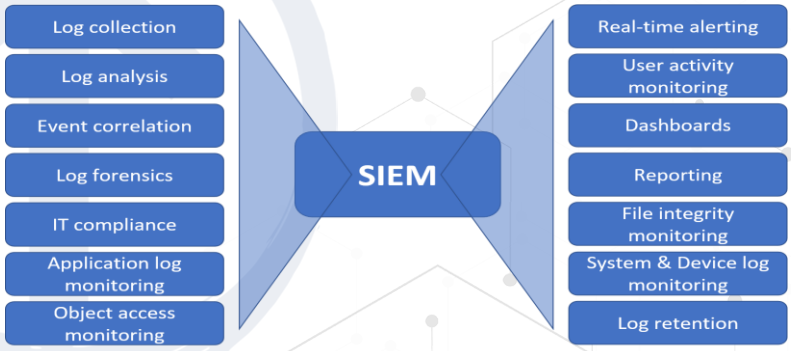
  - **Packet switching -** Cheap, but no capacity guarantee, very widely used today.
    - Data is sent in packets but take multiple different paths to the destination.
    - The packets are reassembled at the destination.
    - **QoS** (Quality of Service) gives specific traffic priority over other traffic.
      - Most commonly VOIP (Voice over IP), or other UDP traffic needing close to real time communication.
      - Other non-real time traffic is down prioritized, the 0.25 second delay won't be noticed.
  - **PAN** (Personal Area Network) - A personal area network is a computer network used for communication among computer and other information technological devices close to one person (PCs, printers, scanners, consoles …).
    - Can include wired (USB and FireWire) and wireless devices (Bluetooth and infrared).

- **LAN** (Local Area Network) - A network that connects computers and devices in a limited geographical area such as a home, school, office building, or campus.
  - Each computer or device on the network is a node; wired LANs are most likely based on Ethernet technology.
- **MAN** (Metropolitan Area Network) – A large computer network that usually spans a city or a large campus.
- **WAN** (Wide area network) - A computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. Combines many types of media such as telephone lines, cables, and air waves.
- **VPN** (Virtual private network) - A VPN network sends private data over an insecure network, most often the Internet.
  - Your data is sent across a public network but looks and feels private.
- **GAN** (Global area network) - A global area network, is a network used for supporting mobile users across a number of wireless LANs, satellite coverage areas, … the transition from one to the next can be seamless.

SIEM and SOAR Systems

SIEM (Security Information and Event Management)

- Often pronounced SEM or SIM.
- Provides a holistic view of our organization's events and incidents.
- Gathers from all our systems and looks at everything
- Centralizes the storage and interpretation of logs, traffic and allows near real-time automated identification, analysis, and recovery of security events.

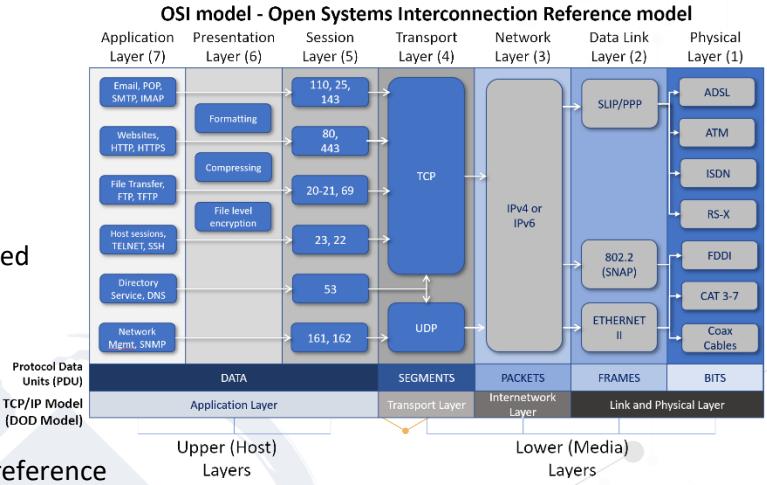


SOAR (Security Orchestration, Automation, and Response):

- A software solution that uses AI to allows us to respond to some security incidents automatically.
- SOAR vs. SIEM: Very similar, both detect/alert on security events, but using AI, SOAR will also react to some events.
  - SIEMs often generate more alerts than a SOC team can handle, SOAR can reduce that.
- SOAR combines all the comprehensive data we gather, has case management, standardization, workflows, and analytics, and it can integrate with many of our other solutions (Vulnerability Management (VM), IT Service Management (ITSM), Threat Intelligence, …).
- All this can help our organization implement a detailed defense-in-depth solution.

The OSI model (Open Systems Interconnect)

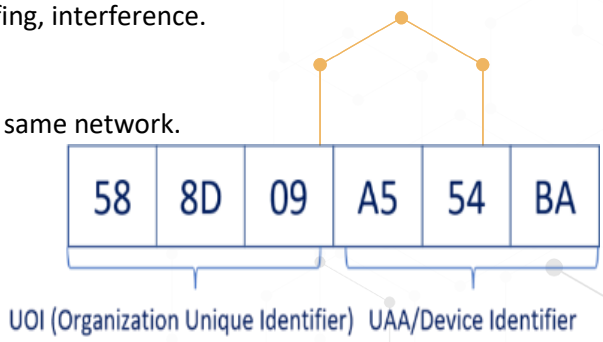
- A layered network model that standardizes the communication functions of a telecommunication or computing system regardless of their underlying internal structure and technology.
- The model partitions a communication system into abstraction layers, the model has 7 layers.
    1. Physical
    2. Data Link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application.
        - 7-1 **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing.
        - 1-7 **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way.



- Know the PDUs (Data, Segments, Packets, Frames, Bits).
- The model is less used now and used as a reference point.
- Know it for the exam, it is testable.

- **Layer 1 Physical Layer:**
    - Wires, Fiber, Radio waves, hub, part of NIC, connectors (wireless).
    - **Cable types:**
        - Copper TP (Twisted Pair) Least secure, eavesdropping, interference, easy tap into, but also cheap.
        - Fiber is more secure, not susceptible to eavesdropping, harder to use, can break, higher cost.
    - **Topologies:**
        - Bus, Star, Ring, Mesh partial/full.
    - **Threats:**
        - Data emanation, theft, eavesdropping, sniffing, interference.

- **Layer 2 Data Link Layer:**
    - Transports data between 2 nodes connected to the same network.
    - LLC – Logical Link Control – error detection.
    - MAC address (BIA) – a unique identifier on the network card.
        - Can be spoofed very easily, both for good and not so good reasons.
        - 48bit hexadecimal first 24 manufacturer identifier, last 24 unique.

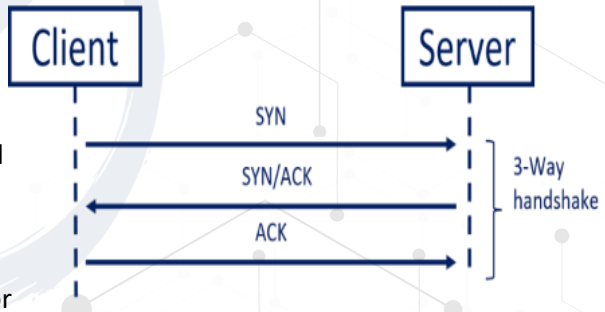


- 64bit hexadecimal first 24 manufacturer identifier, last 40 unique.
- **Threats** - MAC Spoofing, MAC Flooding.

- **ARP** (Address Resolution Protocol) Layer 2/3.
- **CSMA/CD** – Ethernet – minimized with switches vs. hubs.
- **CSMA/CA** – Wireless.
- **Token passing** – Similar to the talking stick, not really used anymore.

- **Layer 3 Network Layer:**
  - Expands to many different nodes (IP) – The Internet is IP based.
  - Isolates traffic into broadcast domains.
  - **Protocols:**
    - IP, ICMP, IPSEC, IGMP, IGRP, IKE, ISAKMP, IPX.
  - **Threats:**
    - Ping of Death, Ping Floods, Smurf – spoof source and directed broadcast, IP modifications, DHCP attacks, …
  - If the exam asks which layer a protocol with "I" is and you do not remember, answer layer 3.
    - IP, IGMP, IGRP, IPSEC, IKE, ISAKMP, … are all layer 3, all except IMAP which is layer 7.

- **Layer 4 Transport Layer:**
  - **SSL/TLS** Layer 4 to 7.
  - **UDP** (User Datagram Protocol):
    - Connectionless protocol, unreliable, VOIP, Live video, gaming, "real time''.
    - Timing is more important than delivery confirmation.
    - Sends message, doesn't care if it arrives or in which order.
    - **Attack**: **Fraggle attack** – works the same way as smurf but may be more successful since it uses UDP and not ICMP.



  - **TCP** (Transmission Control Protocol):
    - Reliable, Connection oriented, guaranteed delivery, 3-way handshake, slower/more overhead, data reassembled.
    - **Attacks: SYN floods** – half open TCP sessions, client sends 1,000's of SYN requests, but never the ACK.
  - **TCP** Flags (9 bits 1-bit flags) (Control bits).
    - **NS**: ECN-nonce concealment protection.
    - **CWR** (Congestion Window Reduced) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in a congestion control mechanism.
    - **ECE**: ECN-Echo has a dual role, depending on the value of the SYN flag.
    - **URG** (1 bit): indicates that the Urgent pointer field is significant.
    - **ACK** (1 bit): indicates that the Acknowledgment field is significant.

- **PSH** (1 bit): Push function. Asks to push the buffered data to the receiving application.
- **RST** (1 bit): Reset the connection.
- **SYN** (1 bit): Synchronize sequence numbers. Only the first packet sent from each end have this flag set.
- **FIN** (1 bit): Last package from sender.

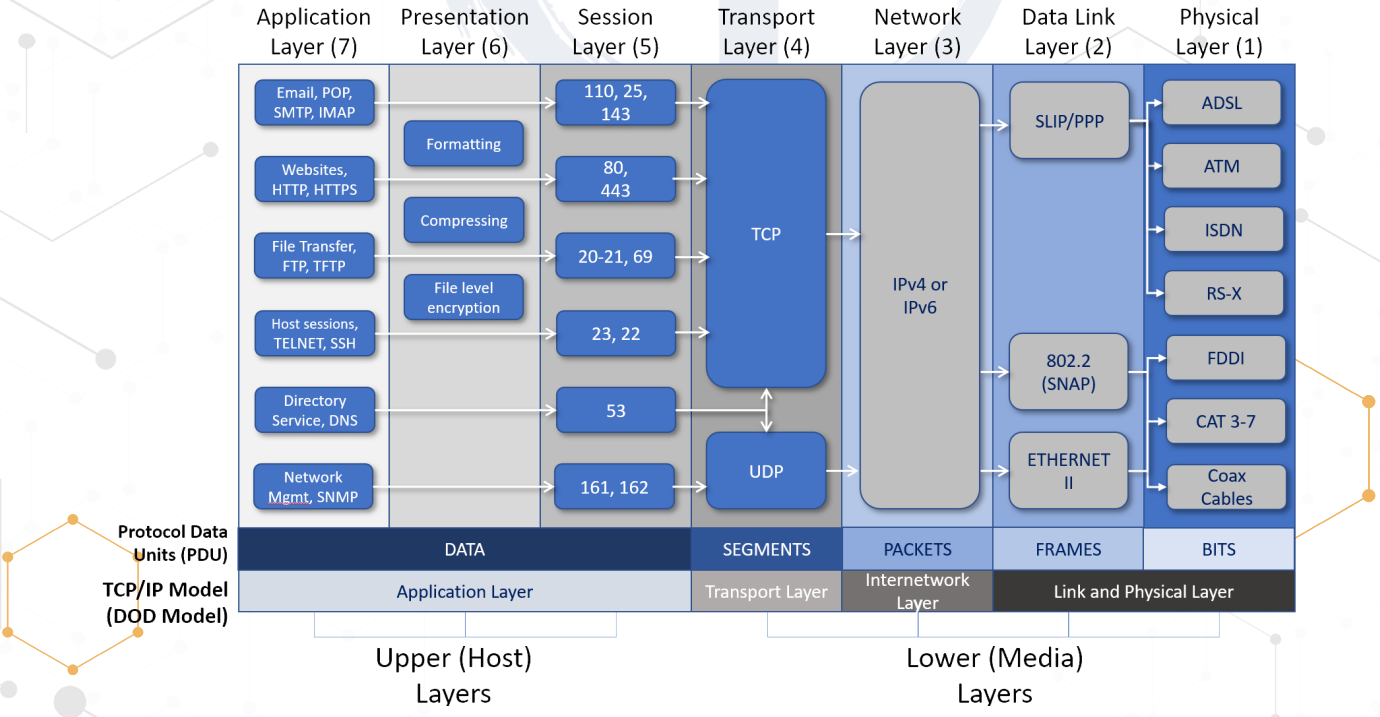
- **Layer 5 Session Layer:**
  - Establishes connection between 2 applications: Setup > Maintenance > Tear Down.

- **Layer 6 Presentation Layer:**
  - Only layer with no protocols.
  - Formatting, compressing, encryption (file level).

- **Layer 7 Application Layer:**
  - Presents data to user (applications/websites).
  - HTTP, HTTPS, FTP, SNMP, IMAP, POP and many more.
  - Non-Repudiation, certificates, application proxies, deep packet inspection, content inspection, AD integration.

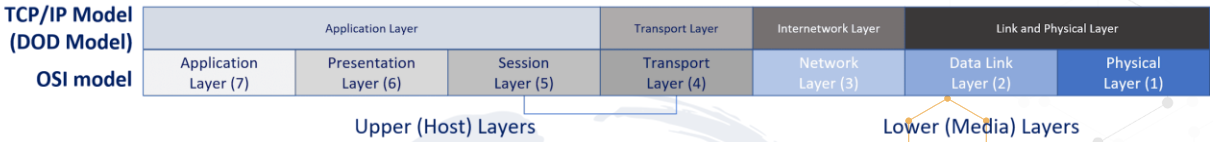
- The higher you go up the layers the slower it is, speed is traded for intelligence.
- **Threats to level 5-7:** Virus, worms, trojans, buffer overflow, application, or OS vulnerabilities.

OSI model - Open Systems Interconnection Reference model

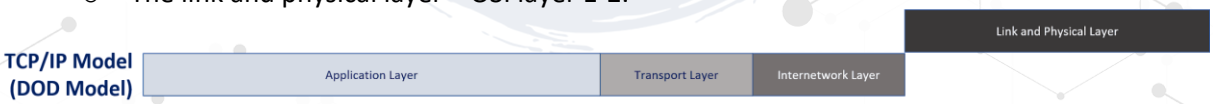


The TCP/IP Model (Internet Protocol Suite)

- A conceptual model that provides end-to-end data communication.
- Specifying how data should be packetized, addressed, transmitted, routed, and received.
- It has four layers which are used to sort all related protocols according to the scope of networking involved.
- From lowest to highest:
    - **The link layer,** containing communication methods for data that remains within a single network segment.
    - **The internet layer**, connecting independent networks, thus providing internetworking.
    - **The transport layer,** handling host-to-host communication. \
    - **The application layer,** which provides process-to-process data exchange for applications.

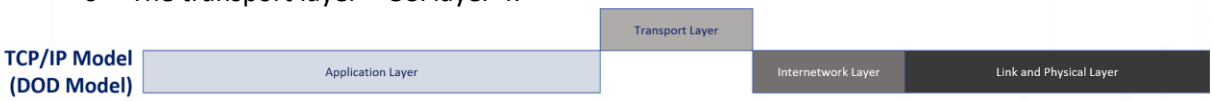


- **The link and physical layer** have the networking scope of the local network connection to which a host is attached.
    - Used to move packets between the Internet layer interfaces of two different hosts on the same network.
    - The process of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
    - These perform functions such as adding a packet header to prepare it for transmission, then transmits the frame over a physical medium.
    - The TCP/IP model includes specifications of translating the network addressing methods used in the Internet Protocol to link layer addresses, such as Media Access Control (MAC) addresses.
    - The link and physical layer = OSI layer 1-2.

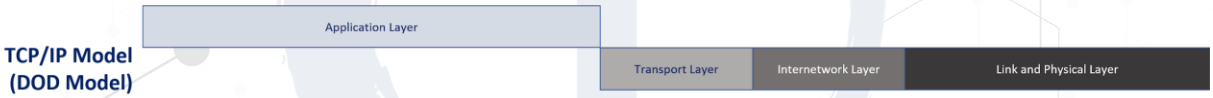


- **Internet/Internetwork layer** is responsible for sending packets across potentially multiple networks.
    - Requires sending data from the source network to the destination network (routing)
    - The Internet Protocol performs two basic functions:
        - **Host addressing and identification:** This is done with a hierarchical IP address.
        - **Packet routing:** Sending the packets of data (datagrams) from the source to the destination by forwarding them to the next network router closer to the final destination.
    - Internet/Internetwork layer = OSI layer 3.

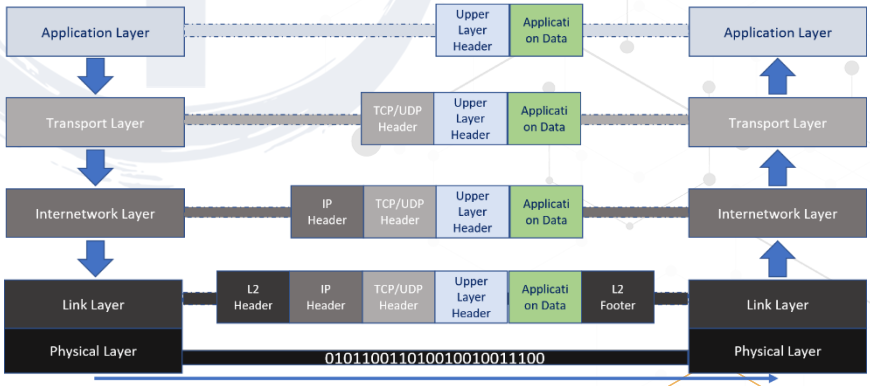
- **The transport layer** establishes basic data channels that applications use for task-specific data exchange.
    - Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers).
    - Data is sent connection-oriented (TCP) or connectionless (UDP).
    - The transport layer = OSI layer 4.



- **The application layer** includes the protocols used by applications for providing user services or exchanging application data over the network (HTTP, FTP, SMTP, DHCP, IMAP).
    - Data coded according to application layer protocols are encapsulated into transport layer protocol units, which then use lower layer protocols for data transfer.
    - The transport layer and the lower-level layers are unconcerned with the specifics of application layer protocols.
    - Routers and switches do not typically examine the encapsulated traffic, rather they just provide a conduit for it. However, some firewall and bandwidth throttling applications must interpret application data.
    - The TCP/IP reference model distinguishes between **user protocols** and **support protocols**.
    - The application layer = OSI layer 5, 6 and 7.



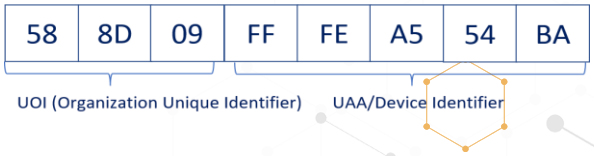
- Each layer of the model adds or removes encapsulation (encapsulation / de-capsulation).
- The higher we go the slower and smarter the stack is, just like the OSI model.



MAC Address (BIA)

- A unique identifier on the network card.
- Can be spoofed pretty easily, both for good and less good reasons.
- EUI/MAC-48 are 48-bits (original design).
  - The first 24 are the manufacturer identifier.
  - The last 24 are unique and identify the host.

- EUI-64 Mac Addresses use 24-bit for manufacturer, but 40 for unique ID.
  - The first 24 are the manufacturer identifier.
  - The last 40 are unique and identify the host.
- Both are widely used today and used by both IPv4 and IPv6.
  - For 48bit MAC's IPv6 modified it into 64-bit MAC's by adding FF:FE to the device identifier.



Protocols

- **IP Addresses:**
  - First deployed for production in the ARPANet in 1983, ARPANet later became the internet.
  - IP was developed in the 1970's for secure closed networks (DARPA - Defense Advanced Research Projects Agency). Security was not built in but was bolted on later.
  - IPv4 is a connectionless protocol for use on packet-switched networks.
  - It operates on a best effort delivery model, it does not guarantee delivery, it also does not assure proper sequencing or avoidance of duplicate delivery. We have added protocols on top of IP to ensure those.
  - IPv4 is the IT route's most Internet traffic today, but we are slowly moving towards IPv6.
    - The move towards IPv6 is mainly dictated by IPv4 Addresses being depleted years ago.
  - IPv4 has around 4.2 billion IP addresses and of those ~4 billion are usable internet addresses.
    - There are currently over 35 billion mobile devices on the internet, 75 billion is predicted by 2025.
    - All major cellphone carriers in the US use IPv6 for all cell phones.
    - **IPv4** has 4,294,967,296 addresses where **IPv6** has 340,282,366,920,938,463,463,374,607,431,768,211,456.
- **IP Addresses and Ports:**
  - When we send traffic, we use both the Source IP and Port as well as Destination IP and Port. This ensures we know where we are going, and when the traffic returns it knows where to return to.
  - The **IP addresses** can be seen as the number of an apartment building.
    - The **Port number** is your apartment number.
    - If you have 50 browser tabs open, each tab has its own port number(s).
  - **Well-known Ports:**
    - 0-1023 - Mostly used for protocols.
  - **Registered Ports:**
    - 1024 to 49151 - Mostly used for vendor specific applications.

- **Dynamic, Private or Ephemeral Ports:**
  - 49152–65535 - Can be used by anyone for anything.

- **Common Ports:**
  - 20 TCP FTP data transfer.
  - 21 TCP FTP control.
  - 22 TCP/UDP Secure Shell (SSH).
  - 23 TCP Telnet unencrypted text communications.
  - 25 TCP Simple Mail Transfer Protocol (SMTP) can also use port 2525.
  - 80 TCP/UDP Hypertext Transfer Protocol (HTTP) can also use port 8008 and 8080.
  - 110 TCP Post Office Protocol, version 3 (POP3).
  - 137 UDP NetBIOS Name Service, used for name registration and resolution.
  - 138 TCP/UDP NetBIOS Datagram Service.
  - 143 TCP Internet Message Access Protocol (IMAP).
  - 443 TCP Hypertext Transfer Protocol over TLS/SSL (HTTPS).
  - 3389 TCP/UDP Microsoft Terminal Server (RDP).

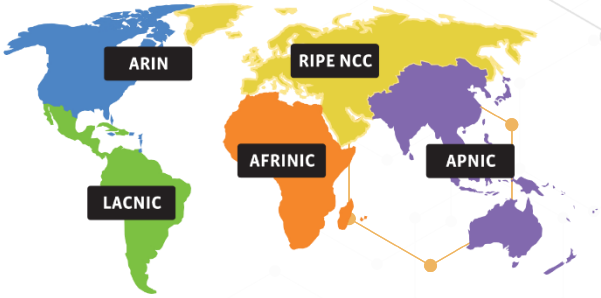
- **IP Addresses and Ports:**
  - **A Socket:**
  - 1 set of IP and Port.
  - UDP only uses 1 socket (connectionless), TCP uses 2 in a pair, 2 individual sockets making the pair.

Ports in use while browsing CISSP websites.

```
TCP    192.168.0.6:49691      195.122.177.218:https  ESTABLISHED
TCP    192.168.0.6:49814      157.55.56.154:40001    ESTABLISHED
TCP    192.168.0.6:49815      91.190.218.56:12350    ESTABLISHED
TCP    192.168.0.6:49995      195.122.177.218:https  ESTABLISHED
TCP    192.168.0.6:50490      vpn:https              ESTABLISHED
TCP    192.168.0.6:50674      ec2-52-4-144-94:https  ESTABLISHED
TCP    192.168.0.6:50678      ec2-54-242-92-62:5222  ESTABLISHED
TCP    192.168.0.6:50793      ec2-34-200-17-103:http  ESTABLISHED
TCP    192.168.0.6:51081      mail:https             ESTABLISHED
TCP    192.168.0.6:51082      mail:https             ESTABLISHED
TCP    192.168.0.6:51862      ec2-52-205-157-86:https  ESTABLISHED
TCP    192.168.0.6:52383      a2plcpnl0694:imaps     ESTABLISHED
TCP    192.168.0.6:52667      104.16.32.229:https    TIME_WAIT
TCP    192.168.0.6:52701      38.113.165.80:https    TIME_WAIT
TCP    192.168.0.6:52703      62.128.100.53:https    TIME_WAIT
TCP    192.168.0.6:52704      62.128.100.57:https    TIME_WAIT
```

- **Socket Pairs (TCP):**
  - 2 sets of IP and Port (Source and Destination).
  - My Pair for the top one is:
    - Source pair:192.168.0.6:49691
    - Destination pair: 195.122.177.218:https
    - Well-known ports are often translated, port 443 is https.

- **IPv4/IPv6 Address Space Management:**
  - **IANA** (Internet Assigned Numbers Authority) governs the IP's address allocation.
  - **IANA** is a department of **ICANN** (Internet Corporation for Assigned Names and Numbers).
  - The world is divided into **RIR** (Regional Internet Registry) regions and organizations in those areas delegate the address space they have control over.

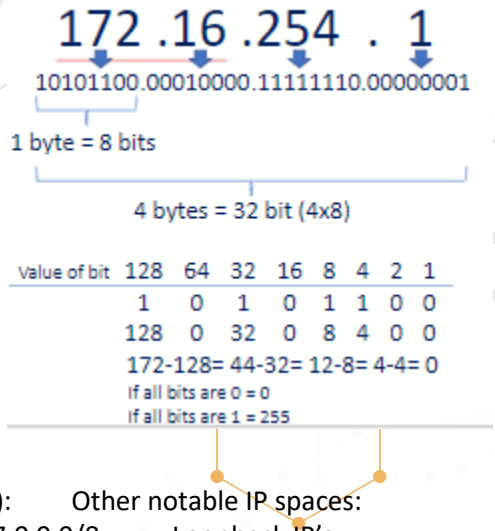


    - **AFRINIC** (African Network Information Center): Africa.
    - **ARIN** (American Registry for Internet Numbers): United States, Canada, several parts of the Caribbean region, and Antarctica.

- **APNIC** (Asia-Pacific Network Information Centre): Asia, Australia, New Zealand, and neighboring countries.
- **LACNIC** (Latin America and Caribbean Network Information Centre): Latin America and parts of the Caribbean region.
- **RIPE NCC** (Réseaux IP Européens Network Coordination Centre) Europe, Russia, Middle East, and Central Asia.

- **IP Address and Traffic Types:**
  - **Unicast, Multicast, and Broadcast Traffic:**
  - **Unicast** - one-to-one traffic (Client to Server): The traffic is from a client to a host or reversed.
    - To capture all unicast traffic on a network, we use promiscuous mode on specific clients' network cards (Network IDS'/IPS'), and the switch port they are attached to has to be configured as a Span-port.
  - **Multicast** -one-to-many (predefined): The traffic is sent to everyone in a predefined list.
  - **Broadcast** - one-to-all (on a LAN network): The traffic is sent to everyone.
    - **Limited L3 Broadcast:** Use the 255.255.255.255 broadcast IP address, routers do not pass (they drop it).
    - **Limited L2 broadcast:** Uses FF:FF:FF:FF:FF:FF broadcast MAC address, routers do not pass.
    - **Directed broadcast:** Sent to anyone logically connected to the same network.
    - A 192.168.19.12/24 will send to all hosts on that network, regardless of if it is physically behind the same router or not. Accounting could have a VLAN spanning 3 separate remote buildings, the broadcast would be sent to them all.

- **IPv4 (Internet Protocol version 4) Addresses:**
  - IPv4 addresses are made up of 4 octets (dotted-decimal notation) and broken further down in a 32bit integer binary.
  - We use IP addresses to make it readable to normal people, it is easier to read 4 sets of numbers than a 32 bits string of 0's and 1's.
  - Similarly, websites are really just IP addresses translated with DNS, which is then translated into binary.
  - It is easier to remember **google.com**, than it is to remember **66.102.12.231** or **2607:f8b0:4007:80b::200e**.
  - **Public IP Addresses** (Internet routable addresses):
    - Used to communicate over the internet between hosts.
  - **Private Addresses** (RFC 1918 – Not routable on the internet):



10.0.0.0	10.255.255.255	16777216	127.0.0.0/8	Loopback IP's
172.16.0.0	172.31.255.255	1048576	169.254.0.0/16	Link-Local
192.168.0.0	192.168.255.255	65536	255.255.255.255	Broadcast

Other notable IP spaces:

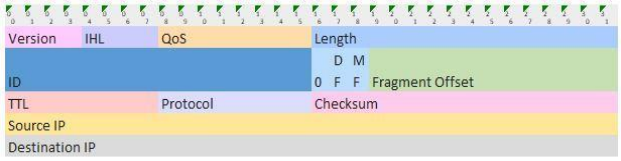
- As a Band-Aid solution to extend the depletion of IPv4 Addresses NAT and PAT were added:
- **NAT (Network Address Translation):**
  - **Static NAT** Translates 1-1, we need 1 Public IP per Private IP we use, not practical and not sustainable.
  - **Pool NAT:** Also, still 1-1, but a pool was available to all clients not assigned to specific clients.
- **PAT** (Port Address Translation):
  - PAT was introduced to solve that issue; it uses IP AND Port number.
  - Also called One-to-Many or NAT Overload since it translates one public IP to many private IPs.

NAT TYPE	
Static	172.16.254.1 → 55.45.125.16
Pool	172.16.254.1 → 55.45.125.16 172.16.254.2 → 55.45.125.17 172.16.254.5 → 55.45.125.18 172.16.254.51 → 55.45.125.19
PAT	172.16.254.1 172.16.254.2 172.16.254.5 172.16.254.51 172.16.254.58 172.16.254.59 → 55.45.125.16

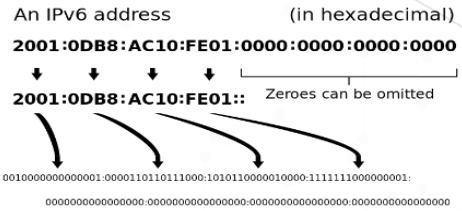
- **Classful IP Networks** were used early on the internet for public addresses. Networks were VERY large, some with 16 million+ IP's. Very inefficient use of IP addresses.
- **CIDR** (Classless Inter-Domain Routing) (also called slash notation):
  - We used CIDR to break our addresses into smaller logical segments, this saves addresses, we can make suitable sized IP ranges for our subnets, and it is easier to add security to our subnets if they are logically segmented.
  - This would be the CIDR notation for our earlier IP address: 172.16.254.1/24.
  - This was done to the /24, which indicates how many IPs are in that subnet, from that we know the broadcast and the range of host addresses.
  - Our /24 address would have 256 addresses, 255 are usable for hosts.
  - Earlier the first (0) and last (255) in a /24 could not be used, but now with newer technology and protocol use only 255 is not usable, since it is the broadcast address.

Address	Mask	How many
a.b.c.d / 32	255.255.255.255	1
a.b.c.d / 31	255.255.255.254	2
a.b.c.d / 30	255.255.255.252	4
a.b.c.d / 29	255.255.255.248	8
a.b.c.d / 28	255.255.255.240	16
a.b.c.d / 27	255.255.255.224	32
a.b.c.d / 26	255.255.255.192	64
a.b.c.d / 25	255.255.255.128	128
*a.b.c.*0 / 24	255.255.255.0	256
*a.b.c.*0 / 23	255.255.254.0	512
*a.b.c.*0 / 22	255.255.252.0	1,024
*a.b.c.*0 / 21	255.255.248.0	2,048
*a.b.c.*0 / 20	255.255.240.0	4,096
*a.b.c.*0 / 19	255.255.224.0	8,192
*a.b.c.*0 / 18	255.255.192.0	16,384
*a.b.c.*0 / 17	255.255.128.0	32,768
*a.b.*0.0 / 16	255.255.0.0	65,536
*a.b.*0.0 / 15	255.254.0.0	131,072
*a.b.*0.0 / 14	255.252.0.0	262,144
*a.b.*0.0 / 13	255.248.0.0	524,288
*a.b.*0.0 / 12	255.240.0.0	1,048,576
*a.b.*0.0 / 11	255.224.0.0	2,097,152
*a.b.*0.0 / 10	255.192.0.0	4,194,304
*a.b.*0.0 / 9	255.128.0.0	8,388,608
*a.*0.0.0 / 8	255.0.0.0	16,777,216
*a.*0.0.0 / 7	254.0.0.0	33,554,432
*a.*0.0.0 / 6	252.0.0.0	67,108,864
*a.*0.0.0 / 5	248.0.0.0	134,217,728
*a.*0.0.0 / 4	240.0.0.0	268,435,456
*a.*0.0.0 / 3	224.0.0.0	536,870,912
*a.*0.0.0 / 2	192.0.0.0	1,073,741,824
*a.*0.0.0 / 1	128.0.0.0	2,147,483,648
0.0.0.0 / 0	0.0.0.0	4,294,967,296

- **IP Headers contain:**
  - Version: IP version 4.
  - IHL: Length of the IP header.
  - QoS (Quality of Service).
  - Identification, Flags, Offset: used for IP fragmentation.
  - TTL (Time To Live): to prevent routing loops.
  - Protocol: Protocol number for TCP, UDP, ...
  - Source and Destination IP addresses.
  - Optional: Options and padding.
  - MTU (Maximum Transmission Unit) - normally 1500 bytes in Ethernet usage.
    - If a packet exceeds that size, a router along the path may fragment into smaller packets.

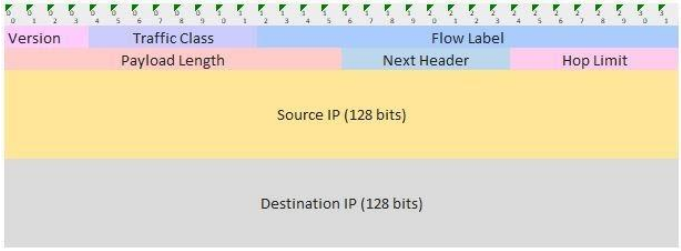


- **IPv6**
  - IPv6 is 128bit in hexadecimal numbers (uses 0-9 and a-f).
  - 8 groups of 4 hexadecimals, making addresses look like this:
    - fd01:fe91:aa32:342d:74bb:234c:ce19:123b
  - The IPv6 address space is huge compared to IPv4. 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses.
    - 34 with 37 0's total or 79 with 27 0's as many addresses as IPv4.
    - Every square foot on the planet can have 65000 IP addresses.
  - IPSec is built in, not bolted on like with IPv4.
  - Mostly switched behind the scenes today, many organizations do not have Dual Stack equipment in place.
  - Used by major US ISPs for cell phones (and to some extent the connection to your modem).
  - To make the address more manageable 1 set of 0's can be shortened with:: above you see the last 16 0's being shortened to 2001:0DB8:AC10:FE01::
  - Our MAC address is **00:fa:22:52:88:8a**
  - It is a EUI-48 address we add "fffe" (for EUI-64) **00:fa:22:ff:fe:52:88:8a**
  - Set the U/L bit **20:fa:22:ff:fe:52:88:8a**
    - (The use of the universal/local bit in the Modified EUI-64 format identifier is to allow development of future technology that can take advantage of interface identifiers with universal scope).
  - Add our network prefix (2001:0000:0000:00b8) **2001:0000:0000:00b8:20fa:22ff:fe52:888a**
    - Remove largest group of 0's **2001::b8:20fa:22ff:fe52:888a**
    - Link Local address (only for local) **fe80::b8:20fa:22ff:fe52:888a**
  - **IP Headers contain:**
    - Version: IP version 6 (4 bits)
    - Traffic Class/Priority (8bits).
    - Flow Label/QoS management (20 bits).
    - Payload length in bytes (16 bits).
    - Next Header (8 bits).
    - Time To Live (TTL)/Hop Limit (8 bits).
    - Source IP address (128 bits).
    - Destination IP address (128 bits).
    - MTU (Maximum Transmission Unit) - normally 1500 bytes in Ethernet usage.
      - If a packet exceeds that size, a router along the path may fragment into smaller packets.

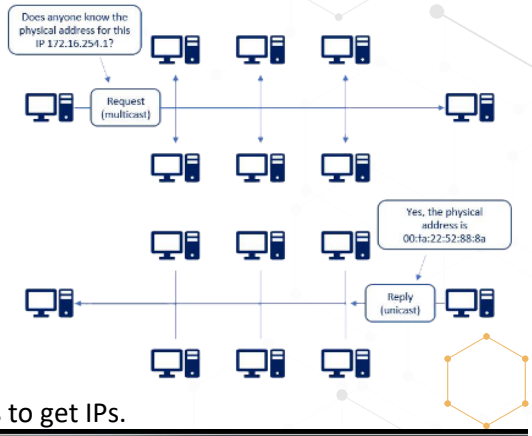


IPv6 address assigned on MAC Address

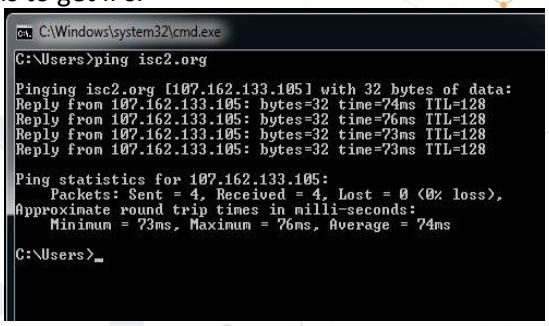
MAC Address		00	fa	22	52	88	8a
Added "fffe" if 48bit	00	fa	22	ff	fe	52	88	8a
Set Universal/local bit	20	fa	22	ff	fe	52	88	8a
Add prefix and :	2001:0000:0000:00b8:20fa:22ff:fe52:888a							
Remove leading 0's	2001::b8:20fa:22ff:fe52:888a							
A link-local address is also assigned	fe80::b8:20fa:22ff:fe52:888a							



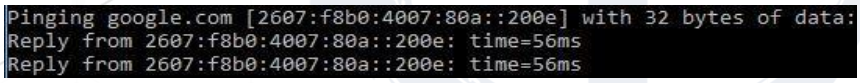
- **ARP (Address Resolution Protocol):**
  - Translates MAC Addresses into IP Addresses.
    - OSI Data/Network Layer or Network/Internet Layer.
  - ARP is a simple and trusting protocol, anyone can respond to an ARP request.
  - **ARP (cache) Poisoning:** An attacker sends fake responses to ARP requests, often done repeatedly for critical ARP entries (Default Gateway).
    - A countermeasure can be hardcoding ARP entries.
  - **RARP (Reverse ARP)** is used by diskless workstations to get IPs.



- **ICMP (Internet Control Message Protocol):**
  - Used to help with IP, for Ping (Echo request/reply) and TTL Exceeds in Traceroute.
  - Often used for troubleshooting.
  - An ICMP Echo Request is sent to the IP, which then sends an ICMP reply back (or not).
  - Originally used (and still) to see if a host is up or down.
  - Today if we get an Echo reply we know the host is up, but no reply does not mean it is down.
  - Firewalls and routers can block ICMP replies.

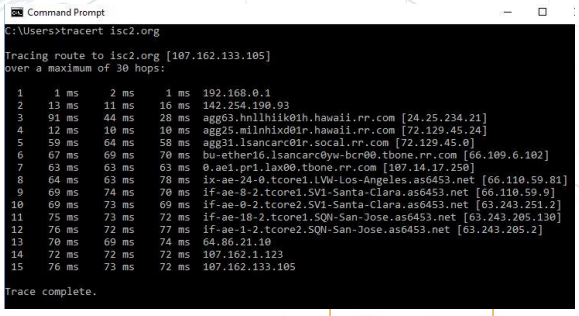


I ping isc2.org (can be name or IP if you know it).
The name is translated into the IP.
I get 4 replies from the IP, 32bytes (IPv4 ping size).
It took 73-76ms (milliseconds 1/1000th of a second)



IPv6 pings are slightly different, since they use the IPv6 headers, but the payload size is the same.

- **Traceroute:**
  - Uses ICMP to trace a network route.
  - Traceroute uses the TTL value in somewhat reverse.
  - We send a message with TTL 1.
    - The first router decrements the TTL to 0 and sends an ICMP Time Exceed message back, First Hop is now identified.
  - We send message 2 with TTL 2, 2nd router does the same, it is identified.
  - We do that over and over till the destination is reached (maximum 30 hops).



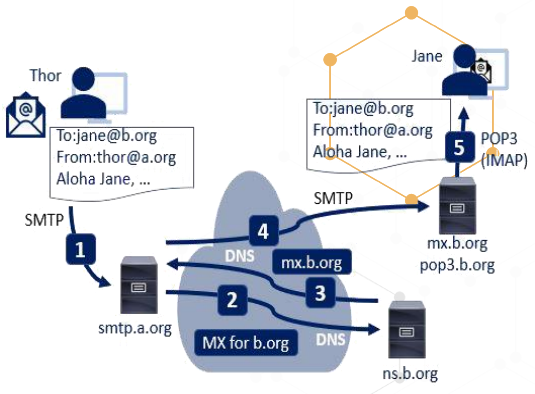
Traceroute to isc2.org (tracert on windows command line):
My local network > ISP > A few Hawaii hops > a few LA hops > 2x Santa Clara > 2x San Jose > Most likely ISC2 Firewall > and finally the actual webserver.

- **Telnet:**
  - Remote access over a network.
  - Uses TCP port 23, all data is plaintext including usernames and passwords, should not be used.
  - Attackers with network access can easily sniff credentials and alter data and take control of telnet sessions.

- **SSH (Secure Shell):**
  - Designed to replace or add security to unsecure protocols such as Telnet, FTP, HTTP...
  - V1 had vulnerabilities long ago, and v2 has as well recently.
  - Provides a 'secure' connection over an unsecured network (the internet).
  - The Snowden leak in 2013 showed the NSA can 'sometimes' decrypt SSL and get access to the data.
  - On July 6th, 2017, WikiLeaks confirmed the CIA (ONLY this one time it is the Central Intelligence Agency) has developed a tool to crack the SSH protocol.
    - BothanSpy is an implant that targets the SSH client program Xshell on the Microsoft Windows platform.
    - Gyrfalcon is an implant that targets the OpenSSH client on Linux platforms centos, debian, rhel, suse, ubuntu.

- **FTP** (File Transfer Protocol): Transfers files to and from servers.
  - No confidentiality or Integrity checks.
  - Should also not be used since the vast majority of what we transport is over insecure networks.
  - Uses TCP Port 21 for the control collection - commands are sent here.
  - Uses TCP Port 20 for the data collection - the actual data is sent here.
- **SFTP (SSH /Secure File Transfer Protocol)**: Uses SSH to add security to FTP.
- **FTPS (FTP Secure)**: Uses TLS and SSL to add security to FTP.
- **TFTP (Trivial FTP):**
  - Uses UDP Port 69.
  - No authentication or directory structure, files are written and read from one directory /tftpboot.
  - Used for "Bootstrapping" - Downloading an OS over the network for diskless workstations.
  - Used for saving router configuration.

- **Email Protocols:**
  1. The MUA (Mail User Agent) formats the message and using SMTP sends the message to the MSA (Mail Submission Agent).
  2. The MSA determines the destination address provided in the SMTP protocol, in this case jane@b.org. The MSA resolves the fully qualified domain name of the mail server in the DNS.
  3. The DNS server for the domain b.org (ns.b.org) responds with any MX (Mail eXchange) records



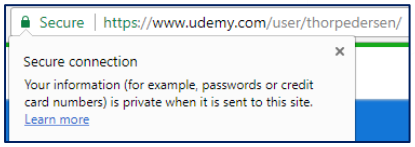
listing for that domain, in this case mx.b.org, an MTA (Message Transfer Agent) server run by the recipient's ISP.
4. smtp.a.org sends the message to mx.b.org using SMTP. This server may need to forward the message to other MTAs before the message reaches the final MDA.
5. The MDA delivers it to the mailbox of user Jane.
6. Jane's MUA picks up the message using either the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP).

- **DNS (Domain Name System):**
  - Translates server names into IP Addresses, uses TCP and UDP Port 53
  - Google.com can get translated into 66.102.12.231 or 2607:f8b0:4007:80b::200e depending on requester's IP.
  - Uses gethostbyname() and gethostbyaddress()
  - **Authoritative name servers** - The authority for a given name space.
  - **Recursive name server** - Tries to resolve names it does not already know.
  - **Cache name server** - Keeps previously resolved names in a temporary cache.
  - DNS uses UDP for most requests and has no authentication natively.
  - **DNS Poisoning** is similar to ARP poisoning, an attacker sends a fake address/name combo to another DNS server when asked and the server keeps it in its DNS records until it expires.

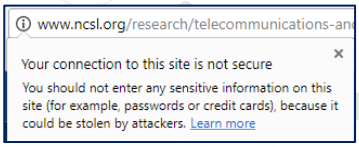
- **DNSSEC** (DNS Security Extensions):
  - Provides Authentication and Integrity using PKI Encryption.
  - Does **not** provide Confidentiality - Think of it as a digital signature for DNS.

- **SNMP (Simple Network Management Protocol):**
  - Mostly used to monitor devices on our network (routers, switches, servers, HVAC, UPS ...).
  - An SNMP client agent is enabled or installed on the client.
  - The device can report port up/down, traffic utilization, temperature, memory use, HDD allocation, ...
  - **SNMPv1** and SNMPv2 sends data in cleartext.
  - **SNMPv2** is still widely used but should be avoided.
    - An attacker on the network can sniff the traffic, often the default community strings are used "public'' and "private".
    - If an attacker gains access to the private (write) string they can re-configure the device, shut it or interfaces down ...
  - **SNMPv3** uses encryption to provide CIA (Confidentiality, Integrity, and Availability).
    - This should be the standard across any organization.

- **HTTP** and **HTTPS** - Transport HTML data.
  - **HTTP** (Hypertext Transfer Protocol):
    - Uses TCP port 80 (8008 and 8080), unencrypted website data sent across the internet.
  - **HTTPS** (HTTP Secure):
    - Uses TCP Port 443 (8443), encrypted data sent over the internet.
  - **HTML** (Hypertext Markup Language):
    - The actual language webpages are written in.
    - Not to be confused with HTTP/HTTPS.



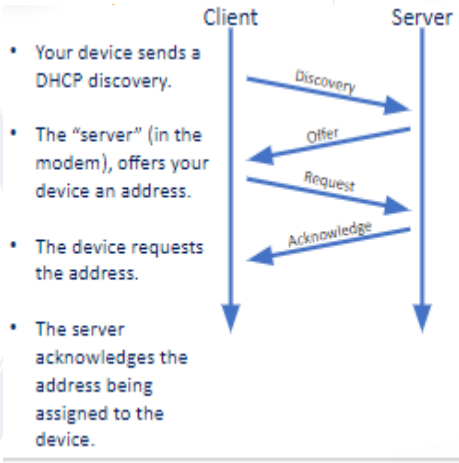
HTTPS: Connection (notice the Secure)



HTTP: Connection.

HTML: The basic building block of webpages.

- **BOOTP (Bootstrap Protocol):**
  - Used for diskless workstations, used to determine OS (Downloaded with tftp) and IP Address.
  - Most system BIOS' support BOOTP, they can then load the OS without a disk.
- **DHCP (Dynamic Host Configuration Protocol):**
  - The common protocol we use to assign IP's. Controlled by a DHCP Server for your environment.
  - You most likely already use it on your home network, this is how when you connect a cable or connect wireless you are online right away.
- Both BOOTP and DHCP use UDP Port 67 for the BOOTP/DHCP Server and UDP Port 68 for the Client.

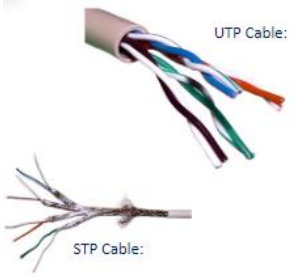


Cables

- **Networking Cables:**
  - When it comes to networking cables, most people think of RJ45 Copper Ethernet cables; many more types are used though.
  - Networking cables all come with pro's and con's, some are cheap, some more secure, some faster, ...
  - They can also pose different security vulnerabilities depending on the cable type and the environment.
  - **EMI (Electromagnetic Interference):**
    - Magnetism that can disrupt data availability and integrity.
  - **Crosstalk** is the signal crossing from one cable to another, this can be a confidentiality issue.
  - **Attenuation** is the signal getting weaker the farther it travels.
    - Copper lines have attenuation, with DSL the farther you are from the DSLAM (Digital Subscriber Line Access Multiplexer) the lower the speed you get.


Putting a data center in a basement is a bad idea, in this case drowned DSLAM's

- **Twisted Pair Cables:**
  - **UTP (Unshielded Twisted Pair):**
  - Pairs of twisted pairs of cable.
    - Twisting them makes them less susceptible to EMI.
    - 1 cable sends and 1 receives data.
    - The tighter the cables are twisted the less susceptible to EMI. For example, CAT3 pairs (less tight) are more susceptible to EMI than CAT6 (tighter).

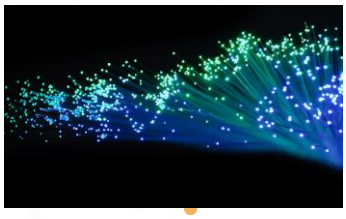


  - **STP (Shielded Twisted Pair):**
    - Has extra metal mesh shielding around each pair of cables, making them less susceptible to EMI, but also making the cables thicker, stiffer, and more expensive.

- **Coax (Coaxial) Cables:**
  - Most commonly used for cable TV and Internet services.
  - Coax Cables have built in layers:
    - **Copper core** in the middle.
    - A **plastic insulator** around the middle core.
    - A **copper braid/shield** around the insulator.
    - A **plastic outer layer**.
  - The braid/shield makes it less susceptible to EMI, and the thicker core can provide higher speeds.

- **Fiber Optic Cables** Use light to carry data (vs. electricity for copper cables)**:**
  - **Pros:** Speed 1 Petabit per second, 35miles/50 km over a single fiber.
    - It has no attenuation like copper; a single uninterrupted cable can be 150 miles+ (240km+) long.
    - Not susceptible to EMI.
    - More secure than copper since it can't be sniffed as easily as copper.
  - **Cons:** Price, more difficult to use, you can break the glass in the cable if you are not careful.
  - **Single-Mode fiber** - A Single strand of fiber carries a single mode of light (down the center), used for long distance cables (Often used in IP-Backbones).
  - **Multi-Mode fiber** - Uses multiple modes (light colors) to carry multiple data streams simultaneously, this is done with WDM (Wavelength Division Multiplexing).

Single-Mode fiber.



Light through fiber strands.

- All cable measurements are in metric (m/km).
- Only 3 countries in the world do not use metric (Burma, Liberia, and the United States).
    - **1Kbps** - Kilobits per second
        - 1,000 bps (10^3)
    - **1Mbps** - Megabit per second
        - 1,000,000 bps (10^6)
    - **1Gbps** - Gigabit per second
        - 1,000,000,000 bps (10^9)
    - **1Tbps** - Terabit per second
        - 1,000,000,000,000 bps (10^{12})
    - **1Pbps** - Petabit per second
        - 1,000,000,000,000,000 bps (10^{15})

UTP Categories – Copper Ethernet Cables				
CAT1	Up to 1Mbps		Twisted Pair	Old phone cable
CAT2	Up to 1Mbps		Twisted Pair	Token Ring network
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE T
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring network
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, Fast Ethernet, Token Ring
CAT5e	Up to 1Gbps	100m	Twisted Pair	Ethernet, Fast Ethernet, Gigabit Ethernet
CAT6/6a	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet, 10G Ethernet (55m)
CAT7	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet, 10G Ethernet (100m)
Multi-mode Fiber Ethernet Cables				
FDDI	160 / 500 MHz			1Gbps 220m, 10Gbps 26m
OM1	200 / 500 MHz			1Gbps 275m, 10Gbps 33m
OM2	500 / 500 MHz			1Gbps 550m, 10Gbps 82m
OM3	1500 / 2000 MHz			1Gbps 550m, 10Gbps 300m, 40/100Gbps 100m
OM4	3500 / 4700 MHz			1Gbps 550m, 10Gbps 400m, 40/100Gbps 150m
All fiber				100BASE-FX 2000m, 1000BASE-SE-LX 550m
Single-mode Fiber Cables				
				1 Pbps 50 km, 69.1Tbps 240 km

LAN Technologies and Protocols

- Network topology describes the layout and topologies of interconnections between devices and network segments.
- **Ethernet** and **Wi-Fi** are the two most common transmission technologies in use for local area networks.
- At the data link layer and physical layer, a wide variety of LAN topologies have been used, including ring, bus, mesh, and star.
- At the higher layers, NetBEUI, IPX/SPX, and AppleTalk used to be common, but TCP/IP is now the de facto standard.
- **Fiber-optic** is commonly used between switches to servers and for backbone data transfers; rarely used for desktops.
- **Ethernet** is baseband and uses copper TP, coax, and fiber cables.
    - Ethernet was also not built for how we use networks today, so we bolt on functionality we want.
- **Wireless** technologies are often built into Smartphones, tablets, and laptops.
    - In a wireless LAN, users can move unrestricted in the coverage area; the transfer from one wireless access point to another is often completely seamless.
- **CSMA (Carrier Sense Multiple Access):**
    - Clients on a network check to see if the shared line is in use, if not they will send their data.
    - Clients listen to see if the line is idle: If idle, they send; if in use, they wait a random amount of time (milliseconds).
- **CSMA/CD (CSMA/Collision Detection):**
    - Used for systems that can send and receive at the same time like Ethernet.
    - If 2 clients listen at the same time and see the line is clear they can both transmit at the same time causing collisions, CD is added to help with that scenario.
    - Clients listen to see if the line is idle: If idle, they send; if in use, they wait a random amount of time (milliseconds).
        - While transmitting, they monitor the network.
        - If more input is received than sent, another workstation is also transmitting.
            - They send a Jam signal to tell the other nodes to stop sending.

- Wait for a random amount of time before starting to retransmit.

- **CSMA CA (CSMA/Collision Avoidance):**
  - Used for systems that can either send or receive like wireless.
  - They check if the line is idle: If idle, they send; if in use, they wait a random amount of time (milliseconds).
    - Slightly different than CD, on Ethernet networks clients are normally aware of other clients, on wireless that is not always the case.
    - If there is a lot of congestion, the client can send a RTS (Request To Send), and if the host (the wireless access point) replies with a CTS (Clear To Send), similar to a token, the client will transmit.
    - This goes some way to alleviating the problem of hidden nodes, in a wireless network, the Access Point only issues a Clear to Send to one node at a time.

Legacy Lan Systems

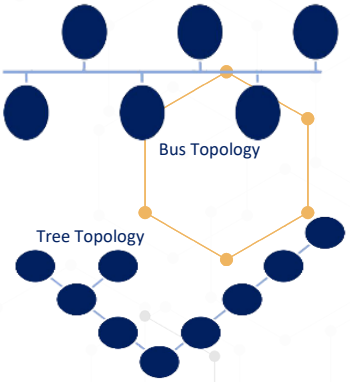
- **ARCNET (Attached Resource Computer Network):**
  - Used network tokens for traffic, no collisions.
  - Used a Star topology.
  - 2.5Mbps.

- **Token Ring**:
  - Used network tokens for traffic, no collisions.
  - Used a Ring topology.
  - 16Mbps.

- **FDDI (Fiber Distributed Data Interface):**
  - Used token-bus for traffic, no collisions.
  - Used a Ring topology.
  - Used fiber and not copper so not susceptible to EMI.
  - 100Mbps.

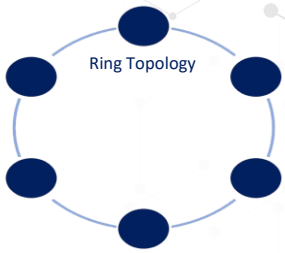
Physical LAN Topologies:

- **Bus:**
  - All nodes are connected in a line, each node inspects traffic and passes it along.
  - Not very stable, a single break in the cable will break the signal to all nodes past that point, including communication between nodes way past the break.
  - Faulty NIC's (Network Interface Card) can also break the chain.



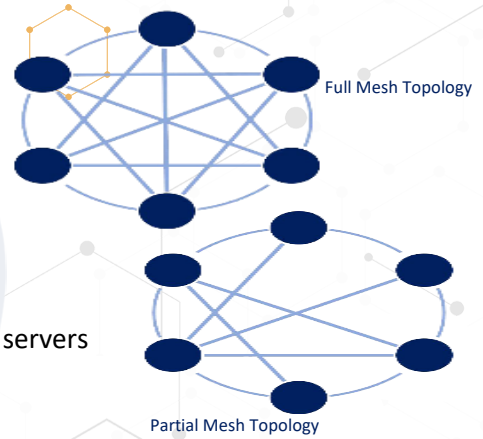
- **Tree** (Hierarchical):
  - The base of the Tree topology controls the traffic, this was often the mainframe.

- **Ring**:
  - All nodes are connected in a ring.



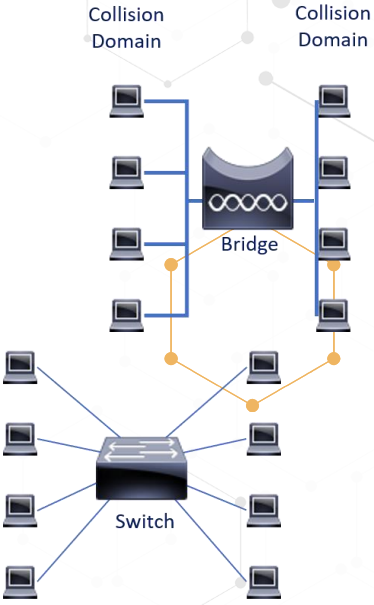
- **Star**:
  - All nodes are connected to a central device.
  - This is what we normally use for ethernet, our nodes are connected to a switch.
  - Provides better fault tolerance, a break in a cable or a faulty NIC will only effect that one node.
  - If we use a switch, no token passing, or collision detection is needed since each node is on its own segment.
  - If we use hubs, collisions will still occur, but I hope none are around anymore, not just how slow they are, but more how unsecure they are now.

- **Mesh**:
  - Nodes are connected to each other in either a partial mesh or a full mesh.
  - **Partial Mesh**:
    - Nodes are directly connected to some other nodes.
  - **Full Mesh**:
    - All nodes are directly connected to all other nodes.
  - More redundant but requires a lot more cables and NIC's.
  - Often used in HA (High Availability) environments, with cluster servers for keepalives.

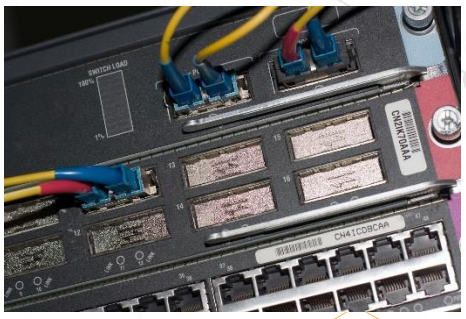


Secure Network Devices and Protocols

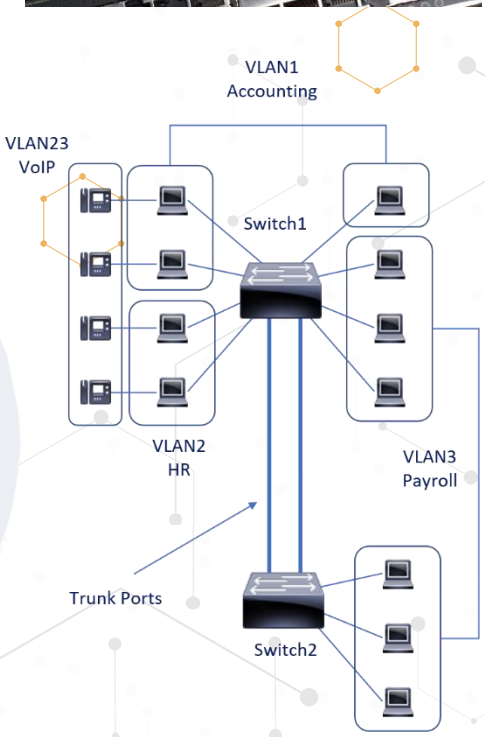
- We have different network devices through the OSI and TCP/IP models and many have protocols specific to that device.
- **Layer 1 devices:**
  - **Repeaters** receive a signal and retransmit it.
    - They are used to extend transmissions so that the signal can cover longer distances.
  - **Hubs** are repeaters with more than 2 ports.
    - All traffic is sent out all ports, no Confidentiality or Integrity, half-duplex and not secure at all.
- **Layer 2 devices:**
  - **Bridges** are 2 port switches used to separate collision domains, which send traffic across the 2 domains, but traffic from one domain is not seen on the other unless sent there.
  - **Switches** are bridges with more than 2 ports.
    - Each port is its own collision domain, fixing some of the issues with collisions.
    - Can range from 4 to 500+ ports.
    - Use MAC addresses to direct traffic.



- Good switch security includes:
  - Shutting unused ports down.
  - Put ports in specific VLANs.
  - Using the MAC Sticky command to only allow that MAC to use the port, either with a warning or shut command if another MAC accesses the port.
  - Use VLAN pruning for Trunk ports.



- **Layer 2 Protocols:**
  - **VLAN (Virtual LAN)** is a broadcast domain that is partitioned and isolated at layer 2.
    - Specific ports on a switch are assigned to a certain VLAN.
    - The Payroll VLAN is in 2 different buildings and spans multiple switches.
    - VLANs uses tags within network packets and tag handling in networking systems, replicating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks.
    - It allows networks and devices that must be kept separate to share the same physical devices without interacting, for simplicity, security, traffic management, and/or cost reduction.
    - **VLAN Trunks** - Ports connecting two switches to span VLANs across them.
    - VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.



- **Virtual eXtensible Local Area Network (VXLAN):**
  - Made and widely used for cloud computing with organizations that have mass tenants. (Think AWS, Google or similar).
  - Solves the issue with only having 4094 maximum VLANs.

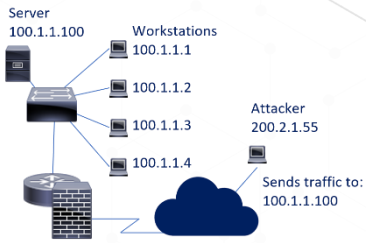
VLAN	VXLAN
Maximum 4094 VLANs, 12-bit VLAN ID.	Maximum 16 million VLANs, 24-bit VLAN ID.
Less flexible and not very suitable for cloud multi-tenant environment.	Very flexible and very suitable for cloud multi-tenant environment.
Uses VLAN tagging on L2 frame for encapsulation to extend VLAN across switches.	Uses MAC-in-UDP encapsulation to extend L2 segments across locations.
VLAN is any L2 partitioned and isolated broadcast domain on our network.	VXLAN is an encapsulation protocol that runs an overlay network on existing L3 infrastructure.

- **Layer 3 devices:**
  - **Routers:**
    - Normally have a few ports vs. a lot on switches.
    - For our organizations they are in the data centers.
    - In your home they are often combined with a switch, and wireless in one box.
    - Forwards traffic based on source and destination IPs and ports.

    - Connecting our LANs to the WAN.
    - Routers send traffic to the most specific route in their routing table.
    - **Static route,** a preconfigured route, always sends traffic there for a certain subnet.
    - **Default gateway** sends all non-local traffic to an ISP for instance.
    - **Dynamic route** is learned from another routing via a routing protocol (OSPF, EIGRP, BGP, IS-IS).
    - **Metric** is used to determine the best route to a destination.
  - **Routers** have two operation planes:
    - **Control plane:**
      - A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection.
      - It uses internal pre-configured static routes, or by learning routes using a dynamic routing protocol.
      - Static and dynamic routes are stored in the **RIB** (Routing Information Base).
      - The control-plane logic then strips non-essential directives from the RIB and builds a **FIB** (Forwarding Information Base) to be used by the forwarding-plane.
    - **Forwarding plane:**
      - The router forwards data packets between incoming and outgoing interface connections.
      - It routes them to the correct network type using information that the packet header contains.
      - It uses data recorded in the routing table control plane.

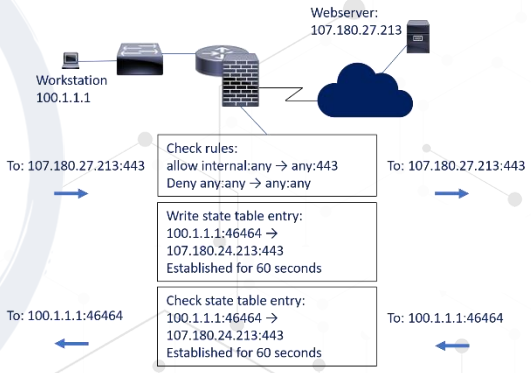
Firewalls

- **Firewalls:** A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, like the Internet.
  - **Packet filtering firewalls**, OSI Layer 1-3.
    - Packet filters act by inspecting the "packets" which are transferred between clients.
    - If a packet does not match the packet filter's set of filtering rules, the packet filter will drop the packet or reject it and send error responses to the source.
    - Any packet that matches one of the Permits is allowed to pass.
    - Rules are checked in order; the attacker's traffic is dropped on the 3rd filter rule. Drop anything trying to access 100.1.1.100.
    - The internal machines can access the server since their IPs are whitelisted in the first rule.

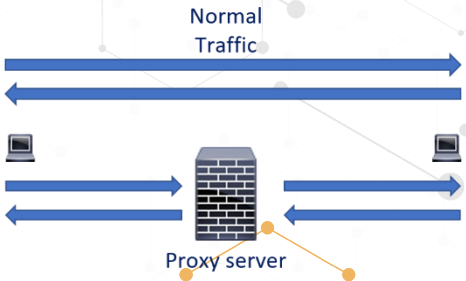


Source	Destination	Action
100.1.1.0/24	100.1.1.0/24	Permit
100.1.1.0/24	Any	Permit
Any	100.1.1.100	Deny
Any	Any	Deny

  - **Stateful filtering firewalls**, OSI Layer 1-4.
    - Records all connections passing through and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection.
    - Static rules are still used; these rules can now contain connection state as one of their criteria.
    - Some DOS attacks bombard the firewall with thousands of fake connection packets trying to overwhelm the firewall by filling its connection state memory.



  - **A proxy server** can act as a firewall by responding to input packets in the manner of an application, while blocking other packets.
  - A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.



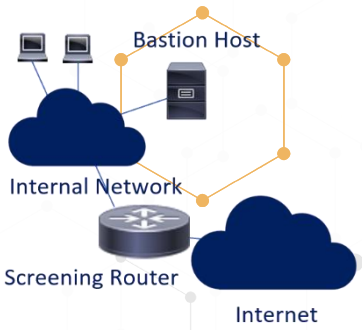
  - **Application layer firewalls**, OSI Layer 7.
    - The key benefit of application layer firewalls is that they can understand certain applications and protocols.
    - They see the entire packet, the packet isn't decrypted until layer 6, any other firewall can only inspect the packet, but not the payload.
    - They can detect if an unwanted application or service is attempting to bypass the firewall using a protocol on an allowed port or detect if a protocol is being used in any malicious way.

- **Network firewalls** filter traffic between two or more networks, either software appliances running on general purpose hardware, or hardware-based firewall.
- **Host-based firewalls** provide a layer of software security on one host that controls network traffic in and out of that single machine.
- **Next-generation firewall (NGFW)**
  - NGFW combines traditional firewall technologies with deep packet inspection (DPI) and network security systems (IDS/IPS, malware filtering and antivirus).
  - Packet inspection in traditional firewalls only looks at the protocol header of the packet DPI also looks at the actual data the packet is carrying.
  - Next-generation firewalls tries to include more layers of the OSI model, improving filtering of network traffic that is dependent on the packet contents.
  - DPI firewalls track the progress of web browsing sessions and can tell if a packet payload, when assembled with other packets in an HTTP server reply, is actually a legitimate HTML-formatted response.

- **Firewalls Design:**
  - **A bastion host** is a special purpose host designed and configured to withstand attacks.
    - Normally hosts a single application, all other services are removed or limited to reduce the threat to the host.
    - It is hardened in this manner because of its location and purpose, which is either on the outside of a firewall or in a DMZ (demilitarized zone) and usually involves access from untrusted networks or computers.

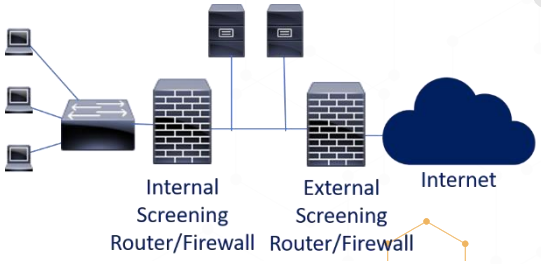
  - A **dual-homed host** has two network interfaces, one connected to a trusted network, and the other connected to an untrusted network (Internet).
    - The dual-homed host doesn't route.
    - Any user wanting to access the trusted network from the outside, needs to log into the dual-homed host and then access the trusted network from there.
    - No longer really used, mostly used premodern firewalls.

  - **Screened host architecture**:
    - An older flat network design using one router to filter external traffic to and from a bastion host via ACLs.
    - The bastion host can reach other internal resources, but the router's ACL denies direct internal/external connectivity.
    - The difference between dual-homed host and screened host design is screened host uses a screening router, which filters Internet traffic to other internal systems.
    - Screened host network design does not use defense-in-depth: a failure of the bastion host puts the entire trusted network at risk.



- Screened subnet architecture evolved as a result, using network defense in depth by using DMZs.

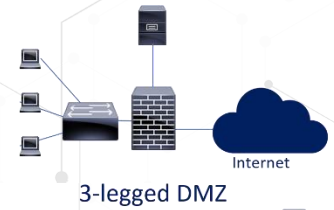
- **Screened Subnet Architecture:**
  - A screened subnet firewall is a variation of the dual-homed and screened host firewall.
  - It can be used to separate components of the firewall onto separate systems, achieving greater throughput and flexibility, although at some cost to simplicity.



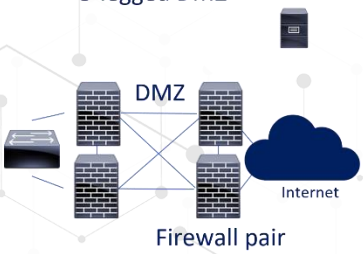
Screened Subnet using Dual Firewall DMZ

  - As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.
  - A screened subnet firewall is often used to establish a **DMZ** (demilitarized zone).
  - Good design uses 2 different brands of firewalls, to avoid both having the same vulnerabilities.

- **DMZs:**
  - Normal DMZs use 2 firewalls in a screened subnet, but they can also be three-legged DMZs which only use 1 firewall.
  - Physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, like the Internet.
  - It adds an additional layer of security to our organization's LAN, an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.



3-legged DMZ



Firewall pair

  - Firewalls are designed to fail closed, if they crash, get flooded with traffic or are shut down, they block all traffic.
  - To get some redundancy we often use firewall pairs, and have the firewall in a mesh topology, this way one firewall failure will just shift the traffic paths.

Preventive and Detective Controls

- **IDSs and IPSs.**
  - We use both IDSs (Intrusion Detection Systems) and IPSs (Intrusion Prevention Systems) on our network to capture and alert or block traffic seen as malicious.
  - They can be categorized into 2 types and with 2 different approaches toward identifying malicious traffic.
    - **Network-based**, placed on a network segment (a switch port in promiscuous mode).
    - **Host-based**, on a client, normally a server or workstation.
    - **Signature (Pattern) matching**, similar to anti-virus, it matches traffic against a long list of known malicious traffic patterns.

        - **Heuristic-based (Behavioral)**, uses a normal traffic pattern baseline to monitor for abnormal traffic.
    - Just like firewalls, routers, servers, switches, and everything else in our environment they just see part of the larger picture, for full picture views and data correlation we use a **SIEM** (Security Information and Event Management) system or even better a **SOAR** (Security Orchestration, Automation, and Response) system.

- **IDS (Intrusion Detection System):**
    - They are passive, they monitor, but they take no action other than sending out alerts.
    - Events trigger alerts: Emails/text message to administrators or an alert on a monitoring tool, but if not monitored right this can take hours before being noticed.

- **IPS (Intrusion Prevention System):**
    - Similar to IDS, but they also take action against malicious traffic, what they do with the traffic is determined by configuration.
    - Events trigger an action, drop/redirect traffic, often combined with the trigger monitoring/administrator warnings, emails, or text messages.

- **IDS/IPS:**
    - Part of our layered defense.
    - Basically, they are packet sniffers with analysis engines.

- **Network-based**, placed on a network segment (a switch port in promiscuous mode).
    - Looks at a segment of our network, normally a switch, but can aggregate multiple switches.
    - Inspects Host/destination ports, IPs, protocols, content of traffic, but can obviously not look in encrypted traffic.
    - Can protect against DDOS, Port scans, brute force attacks, policy violations …
    - Deployed on one switch, port and NIC must be promiscuous, and port must be a span port.

- **Host-based**, on a client, normally a server or workstation.
    - We only look at a single system.
    - Who is using the system, the resource usage, traffic, ...
    - It can be application specific; it does not have to be the entire system we monitor.
    - If we do choose to do traffic analysis it will impact the host by slowing it down.
    - Certain attacks can turn off HIDS/HIPS.
    - Can look at the actual data (it is decrypted at the end device), NIDS/NIPS can't look at encrypted packets.

- **Signature-based:**
    - Looks for known malware signatures.
    - Faster since they just check traffic against malicious signatures.
    - Easier to set up and manage, someone else does the signatures for us.

- They are completely vulnerable to 0-day attacks and have to be updated constantly to keep up with new vulnerability patterns.

- **Heuristic-based (Behavioral):**
  - Looks for abnormal behavior - can produce a lot of false positives.
  - We build a baseline of what normal network traffic looks like and all traffic is matched to that baseline.
  - Traffic not matching the baseline is handled depending on settings, they can take a lot of tweaking.
  - Can detect 'out of the ordinary' activity, not just attacks.
  - Takes much more work and skills.

- **Hybrid based** systems combining both are more used now and check for both signatures and abnormalities.
- **Intrusion Events and Masking:**
  - IDS/IPS obviously then prompt attackers to develop attacks that try to avoid detection.
    - **Fragmentation:** Sending fragmented packets, the attack can avoid the detection system's ability to detect the attack signature.
    - **Avoiding Defaults:** The TCP port utilized by a protocol does not always provide an indication to the protocol which is being transported. Attackers can send malware over an unexpected port.
    - **Low-Bandwidth Coordinated Attacks:** A number of attackers (or agents) allocate different ports or hosts to different attackers making it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.
    - **Address spoofing/proxying:** attackers can use poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server then it makes it very difficult for IDS to detect the origin of the attack.
    - **Pattern Change Evasion:** The attacker changes the data used slightly, which may avoid detection.

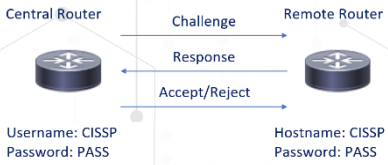
  - **Alerts on IDSs/IPSs can, like biometrics, be one of 4 categories:**
    - **True Positive:** An attack is happening, and the system detects it and acts.
    - **True Negative:** Normal traffic on the network and the system detects it and does nothing.
    - **False Positive:** Normal traffic and the system detects it and acts.
    - **False Negative:** An attack is happening; the system does not detect it and does nothing.

	TRUE	FALSE
POSITIVE	True-Positive Rule matched Attack	False-Positive Rule matched No attack
NEGATIVE	True-Negative No rule matched No attack	False-Negative No rule matched Attack

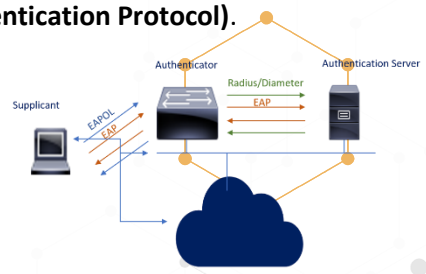
  - We rarely talk about the “true” states since things are happening like they are supposed to, we are interested in when it does not, and we prevent authorized traffic or allow malicious traffic.

Secure Communications

- Securing our data-in-motion is one of the most difficult tasks we have.
- The internet and IPv4 was never built to be secure and just like anywhere else we need to find the right balance of Confidentiality, Integrity, and Availability.
- **Authentication Protocols:**
  - Communications or cryptographic protocols designed to transfer authentication data between two entities.
  - They authenticate to the connecting entity (often a server) as well as authenticate themselves (often a server or desktop) by declaring the type of information needed for authentication as well as syntax.
  - It is the most important layer of protection needed for secure communication between networks.
  - **PAP (Password Authentication Protocol):**
    - Authentication is initialized by the client/user by sending a packet with credentials (username and password) at the beginning of the connection.
    - One of the oldest authentication protocols, no longer secure. The credentials are being transmitted over the network in plain text making it vulnerable to simple attacks like Eavesdropping and man-in-the-middle attacks.
  - **CHAP (Challenge-Handshake Authentication Protocol):**



    - Provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value.
    - Requires that both the client and server know the plaintext of a shared secret like a password, it is never sent over the network.
    - Providing better security compared to PAP, which is vulnerable for both these reasons.
    - Used by PPP (Point to Point Protocol) servers to validate the remote clients.
    - CHAP periodically verifies the identity of the client by using a three-way handshake.
    - The CHAP server stores plaintext passwords of each client; an attacker gaining access to the server can steal all the client passwords stored on it.
  - **802.1X** defines the encapsulation of the **EAP (Extensible Authentication Protocol)**.



    - 802.1X authentication involves three parties: a supplicant, an authenticator, and an AS (authentication server).
    - The **supplicant** is a client device (normally a workstation) that wants to attach to the LAN/WLAN, normally software running on the client that provides credentials to the authenticator.
    - The **authenticator** is a network device, a switch or wireless AP.

- The **AS** (Authentication server) is typically a host running software supporting the RADIUS and EAP protocols.
- In some cases, the authentication server software may be running on the authenticator hardware.
- EAP is widely used, in 802.11 (Wi-Fi) the WPA and WPA2 standards it was adopted with 100+ EAP Types as the official authentication mechanism.

- **PEAP (Protected EAP):**
  - A protocol that encapsulates EAP within an encrypted and authenticated TLS (Transport Layer Security) tunnel.
  - Developed by Cisco Systems, Microsoft, and RSA Security.

- **EAP-MD5:**
  - Very weak forms of EAP. It offers client-to-server authentication only, where most others provide mutual authentication.
  - Vulnerable to man in the middle attacks and password attacks.

- **LEAP (Lightweight Extensible Authentication Protocol):**
  - Cisco distributed the protocol through the CCX (Cisco Certified Extensions) as part of getting 802.1X and dynamic WEP adoption into the industry in the absence of a standard.
  - No native support of LEAP in the Windows OS.

- **EAP-TLS (EAP-Transport Layer Security):**
  - Uses PKI, requiring both server and client-side certificates.
  - Establishes a secure TLS tunnel used for authentication.
  - This makes it very secure, but also complex and expensive.

- **EAP-TTLS (EAP Tunneled Transport Layer Security):**
  - Simpler than EAP-TLS by dropping the client-side certificate requirement, allowing other authentication methods for client-side authentication.
  - This makes it easier to deploy, but also less secure.

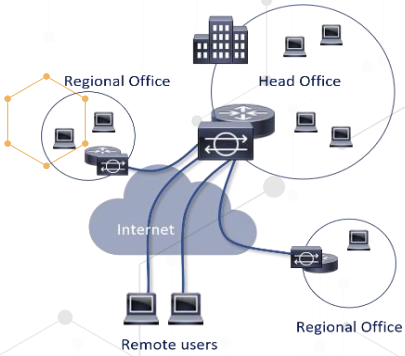
- **PANA (Protocol for Carrying Authentication for Network Access):**
  - Allows a device to authenticate itself with a network to be granted access.
  - EAP will be used for authentication protocol, key distribution, key agreement, and key derivation protocols.

- **SLIP (Serial Line Internet Protocol):**
  - An encapsulation of IP designed to work over serial ports and modem connections.
  - On PCs it has been replaced by PPP, which is better engineered, has more features, and does not require its IP address configuration to be set before it is established.

- On microcontrollers, SLIP is still the preferred way of encapsulating IP packets because of the very small overhead.

- **PPP (Point-to-Point Protocol):**
  - Used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, ...
  - PPP is also used over Internet access connections.
  - ISPs (Internet Service Providers) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol.

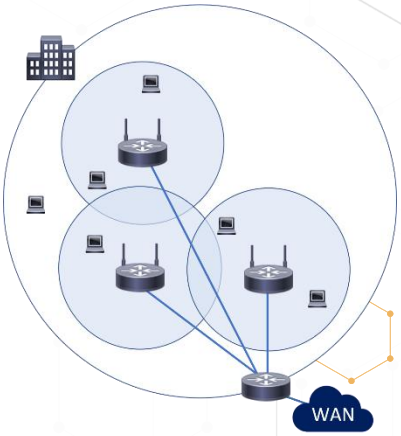
- **VPN (Virtual Private Network):**
  - Extends a private network across a public network, and users can send and receive data across shared or public networks as if they were on the private network.
  - VPNs may allow employees and satellite offices to securely access the organization's intranet.
  - They are used to securely connect.
  - Can also be used to get around geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location.
  - Created by establishing a virtual point-to-point connection using dedicated connections, virtual tunneling protocols, or traffic encryption.



- **PPTP (Point-to-Point Tunneling Protocol):**
  - Obsolete method for implementing virtual private networks because of many known security issues.
  - PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets.
  - No built-in encryption or authentication and PPP being tunneled to implement security.

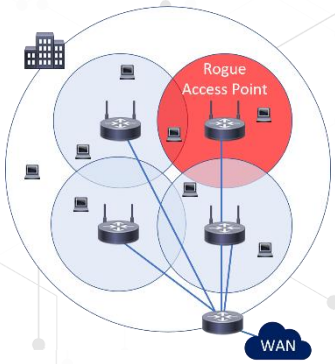
- **L2TP (Layer 2 Tunneling Protocol):**
  - Tunneling protocol used to support VPNs or as part of the delivery of services by ISPs.
  - No built-in encryption or confidentiality, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

WLAN (Wireless LAN) Technologies and Protocols

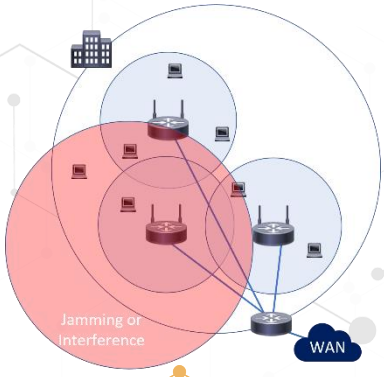


- A wireless computer network that links two or more devices using a wireless distribution method within a limited area (a home, a school, a coffee shop, or an office building).
- Gives users the ability to move around within a locally covered area and be connected to the network.
- Often multiple APs (Access Points) are set up throughout an office building to give seamless roaming coverage for the employees.
- WLAN normally also provides an Internet connection, but not always.
- Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.
- Wi-Fi makes us more mobile and our connection more seamless, but it is easier to compromise than cabled internet connection.

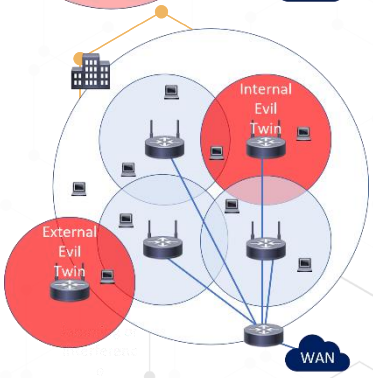
- **Wi-Fi Attacks:**
  - **Rogue Access Points:**
    - An unauthorized access point that has been added to our network without our knowledge.
    - This can be malicious by an attacker or just an employee wanting Wi-Fi somewhere with bad coverage.
    - Without our security posture they are a very big concern.
    - Can be somewhat mitigated with Port security on the switches, and by scanning for Rogue access points.
    - Can compromise confidentiality and integrity.



  - **Jamming/Interference:**
    - This can be a lot of traffic on the Wi-Fi frequencies or done by attackers to disrupt our network (DOS).
    - If interference is an issue we can change to other channels, if any less crowded channels are available, or to different frequencies if our equipment supports it.
    - The 2.4 GHz band is used by Bluetooth, microwaves, cordless phones, baby monitors, Wi-Fi, …
    - Can compromise integrity and availability.

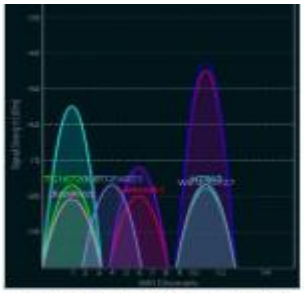


  - **Evil Twin:**
    - An evil twin is used when attackers are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network.
    - Can be done on your network or not, the attacker simply names their access point the same as ours, but with no security and user devices automatically connect to them.
    - Can compromise confidentiality and integrity.



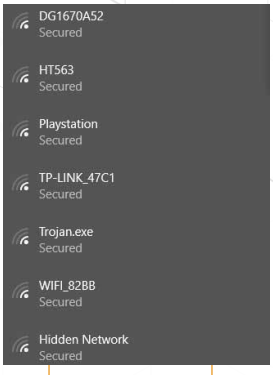
- **802.11 Standards:**
  - The 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing WLAN computer communication in the 2.4, 3.7, 5, and 6 GHz frequency bands.
  - There are more 802.11 protocols but for the exam know these.
  - The 2.4 GHz frequency can be very crowded, wireless, Bluetooth, microwaves, cordless phones, and baby monitors, ... use that frequency.
  - The 5 GHz frequency is normally less crowded and has less interference than 2.4 GHz.
  - Now with the 6 GHz being available, one of its largest selling points is a completely non-crowded frequency.
  - 5 and 6 GHz is a higher frequency with shorter waves, it does not penetrate walls, floors, and other obstructions as well as the longer 2.4 GHz waves.
  - It is easy to change the channel of your Wi-Fi to a less crowded one.
  - Some access points management software can dynamically change the channels on individual access points, to find better channels and provide less overlap.

802.11 network PHY standards						
802.11 protocol	Release date:	Frequency (GHz)	Bandwidth (MHz)	Stream Data Rate (Mbit/s)	Approximate Range (Indoors):	Approximate Range (Outdoors):
802.11-1997	6/1/1997	2.4	22	1, 2	20 m (66 ft)	100 m (330 ft)
a	9/1/1999	5 3.7	20	6, 9, 12, 18, 24, 36, 48, 54	35 m (115 ft)	120 m (390 ft) 5,000 m (16,000 ft)
b	9/1/1999	2.4	22	1, 2, 5.5, 11	35 m (115 ft)	140 m (460 ft)
g	6/1/2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	38 m (125 ft)	140 m (460 ft)
n	10/1/2009	2.4 and 5	20 40	Up to 72.2 Up to 150	70 m (230 ft)	250 m (820 ft)
ac	12/1/2013	5	20 40 80 160	Up to 346.8 Up to 800 Up to 1733.2 Up to 3466.8	35 m (115 ft)	
ax	2/9/2021	2.4, 5, 6	80+80	Up to 9608	30 m (98 ft)	120 m (390 ft)



Wireless access points seen with a wireless sniffer, even if you hide the SSID they can easily be found.

- **802.11 Wireless NICs:**
  - **Operate in four different modes:**
    - **Managed/Client mode:**
      - A wireless access point is required.
      - Clients connect to an access point in managed mode; once connected, clients communicate with the access point only, they can't directly communicate with other clients.
    - **Infrastructure mode:**
      - A wireless access point is required.
      - Client must use the same SSID (service set identifier) as the access point and if encryption is enabled, they must share the same keys or other authentication parameters.
    - **Ad-hoc mode** network:
      - The WNIC does not require an access point but can interface with all other wireless nodes directly.
      - All the nodes in an ad hoc network must have the same channel and SSID.



        - A computer connected to the Internet via a wired NIC may advertise an ad-hoc WLAN to allow internet sharing.
    - **Monitor mode** or **RFMON (Radio Frequency Monitor) mode:**
        - Enables a computer with a WNIC to monitor all traffic received from the wireless network.
        - Unlike promiscuous mode, which is also used for packet sniffing, monitor mode allows packets to be captured without having to associate with an access point or ad hoc network first.

- **SS (Service Set)** is a set consisting of all the devices associated with an organization's WLAN (Wireless Local Area Network).

- **SSID (Service Set Identifier)** is the name of the wireless access point you see when you connect.
    - Clients must know the SSID before joining that WLAN.
    - The SSID is a configuration parameter.
    - SSIDs are normally broadcasted, but we can disable the broadcast in the access point configuration.
    - It is a security measure we want to use, but it is easy to bypass.
    - We can also use MAC address filtering on our wireless access points, this is another limited security feature.
    - MAC addresses are sent in plaintext on 802.11 WLANs, it is easy to sniff and spoof.

- **WEP (Wired Equivalent Privacy)** protocol, early 802.11 wireless security (1997).
    - No longer secure, should not be used.
    - Attackers can break any WEP key in a few minutes.
    - It was designed to not conflict with the Wassenaar Arrangement's 40-bit limit on encryption and because of that, it was designed weaker than it should have been.
    - Many access points still have the WEP option today, but most are preconfigured with WPA2/PSK.
    - WEP uses 10 or 26 hexadecimal digits (40 or 104 bits).
    - It was years back used widely and was often the first security choice presented to users by router configuration tools.
    - WEP frames do not use timestamps and have no replay protection; attackers can inject traffic by replaying previously sniffed WEP frames.

- **WPA (Wi-Fi Protected Access):** (2003)
    - Interim standards to address WEP issues, should not be used.
    - Uses RC4 and TKIP (Temporal Key Integrity Protocol).
        - Neither are considered secure anymore.
        - TKIP uses a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and prevents the types of attacks that compromised WEP.
    - WPA has been designed specifically to work with wireless hardware produced prior to the introduction of the WPA protocol.

- **WPA2 (Wi-Fi Protected Access II),** also called RSN (Robust Security Network) (2004):
  - Most commonly used but a slow move towards WPA3; the most secure form of WPA2 is WPA2-PSK (Pre-Shared Key) using AES.
  - AES provides confidentiality and CCMP (Counter Mode CBC MAC Protocol), a Message Integrity Check (MIC), which provides integrity. It can be configured to use older less secure protocols (TKIP)

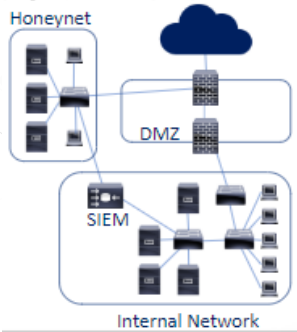
- **WPA3 (Wi-Fi Protected Access III) (2020)**
  - Current standard but transition from WPA2 is slow.
  - 192-bit key strength and WPA3 replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, uses AES-256 in GCM mode with SHA-384 as HMAC.
- **Bluetooth:**
  - A wireless technology standard for exchanging data over short distances using 2.4 GHz from fixed and mobile devices and building personal area networks (PANs).

  - Bluetooth has three classes of devices, while designed for short-distance networking, Class 1 can reach up to 100 meters.
  - Class 1: 100 meters, 2: 10 meters, 3: under 10 meters.
  - Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher.
  - The E0 stream cipher is used for encrypting packets, granting confidentiality, and is based on a shared cryptographic secret, namely a previously generated link key or master key.
  - Cryptanalysis of E0 has proven it to be weak, attacks show the true strength to be 38 bits or even less.
  - Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered on one or both devices.
  - Bluetooth security is to some extent security through obscurity, it assumes the 48-bit MAC address of the Bluetooth adapter is not known.
  - Even when disabled, Bluetooth devices may be discovered by guessing the MAC address.
  - The first 24 bits are the OUI, which can be easily guessed, the last 24 bits can be discovered with brute-force attacks.
  - **Attacks:**
    - **Bluejacking**: Sending unsolicited messages over Bluetooth, most often harmless but annoying.
    - **Bluesnarfing**: Unauthorized access of information from a Bluetooth device phones, desktops, laptops, ...
    - **Bluebugging**: The attacker gains total access and control of your device; it can happen when your device is left in the discoverable state.
    - Only possible on older phones with outdated OSs, newer smartphones constantly update their OS.
  - **Countermeasures:**
    - Enable Bluetooth only when you need it.

- Enable Bluetooth discovery only when necessary and disable discovery when your devices are paired.
- Do not enter link keys or PINs when unexpectedly prompted to do so.
- Remove paired devices when you do not use them.
- Regularly update firmware on all Bluetooth enabled devices.

Preventive and Detective Controls

- **Honey pots and Honey nets:**
  - **Honeypots:**
    - System looking like a real system, but with the sole purpose of attracting attackers.
    - They are used to learn about our vulnerabilities and how attackers would circumvent our security measures.
    - Used both internally and externally, internal honeypots can alert us to attackers and malware that made it past our security perimeter and external honeypots teach us about the attack vectors attackers' use.
    - External honeypots will get compromised on a regular basis, we analyze the attack and ensure our internal systems are protected against that type of attack.
    - Honeypots are rarely hardened completely; our actual data servers are always hardened completely.
    - Always talk to your legal department before deploying honeypots.
      - Remember the thin line between entrapment and enticement.
      - What are the legal/liability ramifications if an attacker launches a 3rd party attack from your honeypot/net?
      - Get very clear legal guidelines issued before deploying and get senior management's approval in writing.
  - **Honeynets:**
    - A network (real or simulated) of honeypots, can be a full server farm simulated with applications, OSs, and fake data.
    - Best practice segments the honeynet from our actual network by a DMZ/firewall.
    - The SIEM/SOAR systems collect the data from our internal systems as well as the honeynet.



Secure Communications:

- **IPSEC (Internet Protocol Security):**
  - **SA (Security Association):** Simplex one-way communication, can be used to negotiate ESP (Encapsulation Security Payload) or AH (Authentication Header) parameters.
    - If 2 systems use ESP to communicate, they need 1 SA for each direction (2 total); if AH and ESP, 4 total.
    - A unique 32bit SPI (Security Parameter Index) is used to identify each SA connection.
  - **ISAKMP (Internet Security and Key Management Protocol):**

        - Manages the SA creation process.
    - **Tunnel mode** encrypts and authenticates the entire package (including headers).
    - **Transport mode** only encrypts and authenticates the payload, used for systems that speak IPSEC.
    - **IKE (Internet Key Exchange):**
        - IPsec can use different types of encryptions (3DES or AES) and hashes (MD5, SHA1, SHA2, …).
        - IKE negotiates the algorithm selection process.
        - The 2 sides of an IPsec tunnel will normally use IKE to negotiate to the highest and fastest level of security, selecting AES over single DES for confidentiality if both sides support AES, for example.
    - IPSec can protect data flows between a pair of hosts (host-to-host), a pair of security gateways (network-to-network), and a security gateway and a host (network-to-host).
    - IPSec is an end-to-end security scheme operating in the Internet Layer of the TCP/IP model, only IPsec protects all application traffic over an IP network.
    - IPsec can automatically secure applications at the IP layer.

- **SSL** and **TLS** – Confidentiality and Authentication for web traffic.
    - Cryptographic protocols for web browsing, email, Internet faxing, instant messaging, and VOIP.
    - You download the server's digital certificate which includes the sites public key.
    - **SSL (Secure Socket Layer)** Currently on v3.0.
        - Mostly used for web traffic.
    - **TLS (Transport Layer Security)** More secure than SSL v3.0.
        - Used for internet chat and email client access and used for securing web traffic.

- **ISDN (Integrated Services Digital Network)** - OSI layer 1-3.
    - Used for digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
    - A circuit-switched telephone network system which also provides access to packet switched networks.
    - It offers circuit-switched connections (for either voice or data) and packet-switched connections (for data) in increments of 64 kilobit/s but could be higher with channel bonding.

- **DSL (Digital Subscriber Line)** is a family of technologies that are used to transmit digital data over telephone line.
    - Often used to describe ADSL (Asymmetric DSL), the most common DSL technology.
    - DSL service can be delivered side by side with wired telephone service on the same line, this is possible because DSL uses higher frequency bands for data.
    - At the customer Demarc, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL services.

- **Callback** is a modem-based authentication system.
    - mostly used for securing dial-up connections.

- The client computer calls the server computer.
- After a greeting the client identifies itself, usually with a username.
- The server disconnects the call.
- Depending on the user's name and a list of users' phone numbers, the server will then establish a second call back to the client computer.
- The client computer expecting this returned call will then answer and communications between the two computers will proceed normally.

- **Caller ID** does the same, but the user has to be calling from the right number.
  - It can easily be faked; many phones or phone companies allow the end user to pick their caller ID.

- **Remote Administration** is controlling a computer from a remote location, we do this through software.
  - A remote location may refer to a computer in the next room or to one across the world.
  - Any computer with an Internet connection can be remotely administered.

- **RDP (Remote Desktop Protocol) -** A Microsoft proprietary protocol.
  - The user uses RDP client software for this, and the other computer must run RDP server software.
  - Providing a user with a GUI (Graphical User Interface) by default, the server listens on TCP and UDP 3389.

- **VNC (Virtual Network Computing) -** Non-MS proprietary and can run on most OSs (Using screen scraping).
  - It was at first used for remote administration of computers but is also being used more and more now for Remote Desktop Protocol for multi-user environments and helpdesk RDP access.

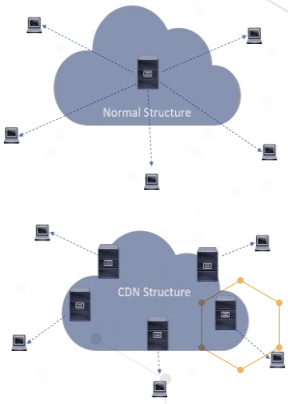
- Newer versions use HTTPS (TCP port 443) and has the GUI contained in a browser.
  - You install the software on the system you want to access and the one you want to access from, set up username/password and you can control that system from anywhere.
  - Commonly used include: Chrome Remote Desktop, LogMeIn, GoToMyPC, support.me, …

- **VDI (Virtualized Desktop Infrastructure/Interface):**
  - **Thin Clients:**
    - Diskless Workstation (Diskless node) has all the normal hardware/firmware except the disk, it has the lower-level OS (the BIOS) which performs the POST, and it then downloads the kernel and OS.
    - Thin Client Applications - We use a Web Browser to connect to the application on a server on port 80 (HTTP) or port 443 (HTTPS), the full application is housed and executed on the server vs. on your PC.
    - Often stripped of non-essentials like CD drives, most ports, ...

- **Zero Clients:**
  - Getting more popular for VDI because they are even slimmer and more cost-effective than thin clients.
  - These are client devices that require no configuration and have nothing stored on them.
  - They are sold by Dell, Fujitsu, HP, Pano Logic, ...

- **IM (Instant Messaging):**
  - Short messages are typically sent between two parties (one-to-one) or many to many (group IMs).
  - Some IM applications can use push technology to provide real-time text which transmits messages character by character as they are typed, others send when you hit enter.
  - More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, and video chat.
  - Commonly used chat protocols today include IRC, Jabber, Lync, and still used but very limited ICQ and AIM.
  - Today most IM'ing is done embedded in other applications like Facebook, LinkedIn, Twitter, or WhatsApp.
  - Many IM applications and protocols are not designed with security in mind, they are designed for usability.
    - A report on the level of safety offered by instant messengers, only 2 out of 18 instant IM apps they looked got "nothing of concern" on sending sensitive attachments and mining/selling customer data, the rest got "not recommended". The most popular messenger has 25 "not recommended" and only 6 "nothing of concern" when looking at privacy and security
    - IM connections are often sent in plain text, making them vulnerable to eavesdropping.
    - Software often requires the user to open UDP ports, increasing the threat posed by potential security vulnerabilities.
- **Web Conferencing:**
  - An umbrella term for different types of online collaborative services including webinars, webcasts, and peer-level web meetings.
  - Commonly used ones are WebEx, Zoom, GoToMeeting, Google Meet, TeamViewer, ...
  - Done over TCP/IP connections, services often use real-time point-to-point communications as well as multicast communications from one sender to many receivers.
  - It offers data streams of text-based messages, voice, and video chat to be shared simultaneously across geographically dispersed locations.
  - Applications where web conferencing is used: Meetings, training events, lectures, or presentations one-to-one or many-to-many like IMs.
  - The use of web conferencing should align with your organizations policies, some may, if not implemented right be a security vulnerability.
  - They can bypass some security by using SSL/TLS tunnels and acceptable products should be hardened.

- **CDN (Content Distribution Network):**
  - A geographically dispersed network of proxy servers and data centers.
  - The client is sent to the server node with the lowest latency in MS.
  - The client's webpages, software download, and video streaming are faster.
  - The provider saves on cost, sending traffic short distances vs. long distance and it provides redundancy and some DDOS protection.
  - The idea is to distribute service spatially relative to end-users to provide high availability and high performance.
  - Many different services can be provided over CDNs: video streaming, software downloads, web, and mobile content acceleration, licensed/managed CDN, transparent caching, and services to measure CDN performance, load balancing, multi-CDN switching and analytics, and cloud intelligence.



- **Third-party Connectivity:**
  - Medium size enterprises typically have 20 or more third-party providers. I believe the hospital where I worked in Hawaii had more than 200 third-party providers.
  - How do we ensure they are secure enough and conform to our policies and procedures?
  - Many never have direct contact with IT or IT-Security.
  - We must conduct a thorough risk assessment to ensure that whatever they provide does not jeopardize our security posture, or we must accept the risk.
  - We should have MOUs/MOAs and ISAs (Interconnection Security Agreement).
- **Network Access Control (NAC):**
  - Automatic detection and response to ensure our systems are in adherence with our security policies.
  - Can helps us with the prevention or reduction of 0-day and known attacks.
  - Along with ensuring that security policies are adhered to at all times.

Mobile Security:

- The more external devices we connect, the more complex policies, procedures, and standards we need.
- **Mobile devices** are really anything “mobile” – External hard disks, USB drives, CDs, laptops, cell phones, ...
- Most internal threats are **not** malicious people. They just do not know any better, did not think about it or figured they would not get found out.
- **Good security policies** should lock down USB ports, CD drives, network ports, wireless networks, disable autorun on media, use full disk encryption, have remote wipe capabilities, raise user awareness training on where (if anywhere) mobile devices are allowed. (Defense in Depth)
- **Cell phones** are the mobile devices most often lost – Current Android and iOS phones all have full disk encryption.
  - We can add a lot more features to our company cell phones to make them more secure.
  - Remote wipe, find my device, lock after x minutes, number of failed passwords, disable removable storage, …
  - We can also use a centralized management system: **MDM (Mobile Device Management)** controls a lot of settings.

        - App negative/positive list, Storage Segmentation, Remote Access Revocation, Configuration Pushes, Backups.
        - More controversial: Track the location of employees, monitor their data traffic and calls.
    - Laptops, Smartphones and Tablets are great productivity tools, but they (just like anything else) have to be secured properly or they are a liability.
        - BYOD (Bring Your Own Device) - There should be clear corporate policies/procedures/guidelines.
        - On/off boarding - How is the return of mobile devices handled and enforced?
        - It is much harder to standardize on BYOD. Is support staff ready for that many devices, OSs, applications?
        - Should we use MDM?
        - How do we handle patch and virus management?

Preventive and Detective Controls:

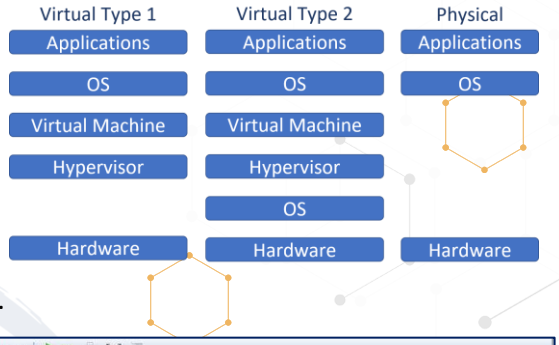
- **Application Positive listing:**
    - We can positive list the applications we want to allow to run on our environments, but it can also be compromised.
    - We would positive list against a trusted digital certificate, a known hash or path and name, the latter is the least secure, an attacker can replace the file at the path with a malicious copy.
    - Building the trusted application positive-list takes a good deal of time, but is far superior to negative-listing, there are 10,000's of application and we can never keep up with them.
- **Removable Media Controls:**
    - Good security policies would also have us lock down USB ports, CD drives, memory card ports and anything else where you can load malicious code onto our systems from external devices.
    - For servers we may rarely have to enable USB ports for firmware or other updates, we would enable the ports while we use them and lock them right away after, it is safer to be done centrally via group policies or similar.

Virtualization and Distributed Computing:

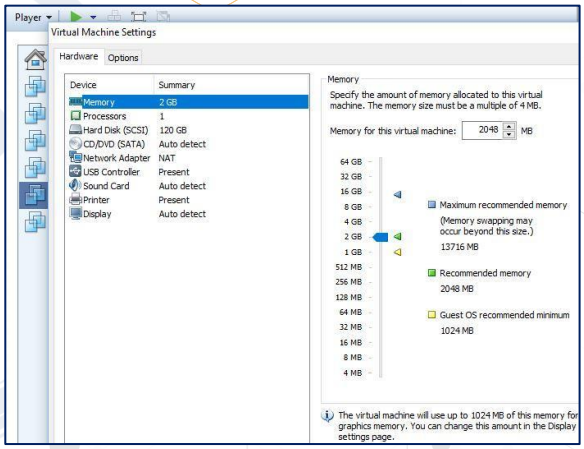
- **Virtualization**
    - **Virtualization** poses a whole new set of standards, best practices, and security concerns.
        - With Virtualization we have many servers (clients) on the same hardware platform (host).
        - Virtualization is software running under the OS and above the Hardware (Ring -1).
        - Traffic between the clients on the host doesn't have to traverse our network.
        - Common Virtualization software could be VMWare, Hyper-V, or Xen.
        - With Distributed Computing we use either multiple local or remote clients for our needs, most commonly cloud computing. How do we ensure the cloud Data Center meets our security posture, how do they segment their network?
    - **Virtualization holds a ton of benefits:**
        - Virtualized environments cost a lot less than all physical servers.

- It is much easier to stand up new servers (don't need to buy hardware, wait 2 weeks, rack it, run power/internet).
- You can easily backup servers with snapshots; server builds can be done with images.
- You can instantly reallocate resources.
- They have lower power and cooling costs, a much smaller rack footprint (50-100 servers in the space of 5-8).

- **Hypervisor** - Controls the access between the virtual guest/clients and the host hardware.
  - Type 1 hypervisor (Bare Metal) is a part of a Virtualization OS that runs on top of the host hardware (Think Data Center).
  - Type 2 hypervisor runs on top of a regular OS like Windows 10 - (Think your PC).



- Virtualization also poses new vulnerabilities because the technology is new-ish and very complex.
- Clients on the same host should be on the same network segment (Internal/DMZ). A host should never house both zones.
- Clients should be logically separated on the network like physical servers would be (HR, Accounting, IT VLANs).
- **VM Escape** (Virtualization escape) is when an attacker can jump from the host or a client to another client, this can be even more of a concern if you have different Trust Level Clients on the same host. They should ideally be on separate hosts.



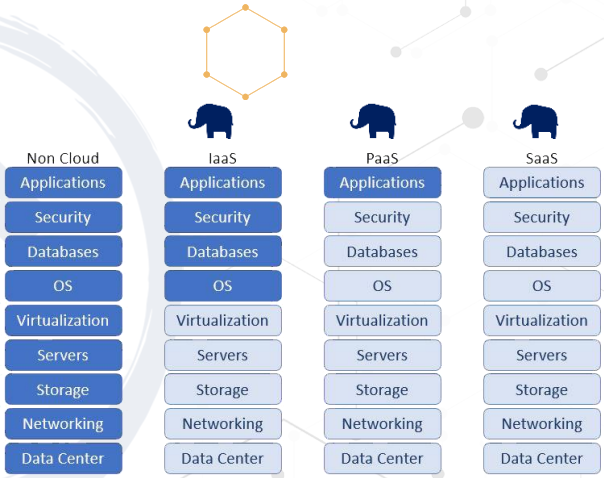
- **Hypervisor Security -** If an attacker can get access to the hypervisor, they may be able to gain access to the clients.
- **Resource Exhaustion -** Admins oversubscribe the CPU/Memory and do not realize more is needed (availability).

- **Cloud Computing** - (There is no 'Cloud' it is just another computer somewhere else).
  - When we use cloud computing we build or outsources some part of our IT Infrastructure, storage, applications.
  - This can be done for many good reasons, but most are cost related.
  - Cloud Computing can be divided into 4 main types:
    - **Private Cloud Computing** - Organizations build and run their own cloud infrastructure (or they pay someone to do it for them).
    - **Public Cloud Computing** - Shared tenancy – A company builds massive infrastructures and rents it out to anyone who wants it. (Amazon AWS, Microsoft, Google, IBM).

- **Hybrid Cloud Computing** – A mix of Private and Public Cloud Computing. An organization can choose to use Private Cloud for sensitive information and Public Cloud for non-sensitive data.
- **Community Cloud Computing –** Only for use by a specific community of consumers from organizations that have shared concerns. (Mission, policy, security requirements, and/or compliance considerations.)

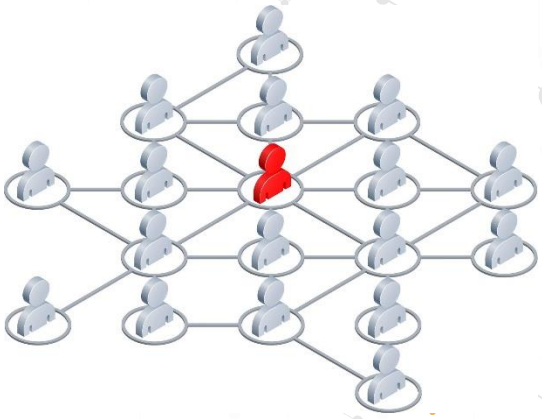
As with any other outsourcing make sure you have the right to audit, pen test (clearly agreed upon criteria), conduct vulnerability assessment, and check that the vendor is compliant with your industry and the standards you adhere to.

- **Cloud Computing Public Cloud Computing:**
  - Platforms are normally offered as:
    - **IaaS - (Infrastructure as a Service)** The vendor provides infrastructure up to the OS; the customer adds the OS and up.
    - **PaaS - (Platform as a Service)** The vendor provides pre-configured OSs, then the customer adds all programs and applications.
    - **SaaS - (Software as a Service)** The vendor provides the OS and applications/programs. Either the customer interacts with the software manually by entering data on the SaaS page, or data is automatically pushed from your other applications to the SaaS application (Gmail, Office 365, Dropbox, Payroll, …).



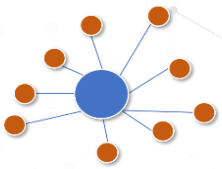
- **Grid Computing** – can make use of resources not currently in use from 100 or 100,000's of computers to perform very complex tasks.
  - Each node has a smaller subtask but leveraging the entire Grid can make it be very powerful and fast.
  - Often used in problems so complex that they need that many nodes to be solved.
  - BOINC (Berkeley Open Infrastructure for Network Computing) has over 4,000,000 machines enrolled, used for a wide variety of scientific research.
  - **Peer to Peer** (P2P) - Any system can be a client and/or a server.

- Most commonly used on torrent networks to share music, movies, programs, pictures and more (The majority without the copyright holder's consent).
- Older versions had centralized index servers making it easier to disrupt a sharing network, but the current versions use no centralized infrastructure.
- Each client is often also a server and has the index. Taking down 10,000 in a network of 100,000 will just result in a network of 90,000, with no other discernible impact.

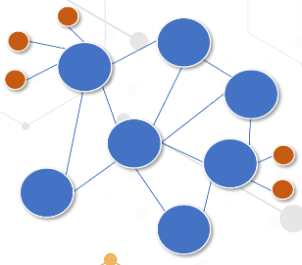


- **Thin Clients** (Boot sequence - BIOS > POST > TCP/IP > BOOTP or DHCP)
  - **Diskless Workstation** (Diskless node) has all the normal hardware/firmware except the disk, and the low-level OS (BIOS), which performs the POST. It then downloads the kernel and higher-level OS.
  - **Thin Client Applications** - We use a Web Browser to connect to the application on a server on port 80 (HTTP) or port 443 (HTTPS). The full application is housed and executed on the server vs. on your PC.

- **Distributed Systems:**
  - **Can also be referred to as:**
    - Distributed computing environment (DCE), concurrent computing, parallel computing, and distributed computing.
  - A collection of individual systems that work together to support a resource or provide a service.
  - Most end-users see the DCE as a single entity and not as multiple systems.
  - **Why do we use DCEs?**
    - They can give us horizontal scaling (size, geography, and administration), modular growth, fault tolerance, cost-effectiveness, low latency (users connect to the closest node).
  - **Where do we use DCEs?**
    - All over the place (The internet, websites, cell networks, research, P2P networks, blockchain, …).



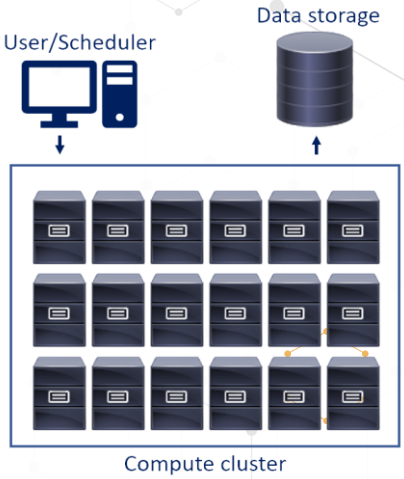
Centralized System



Distributed System

- **High-Performance Computing (HPC) Systems:**

- Most often aggregates of compute nodes in a system designed to solve complex calculations or manipulate data at very high speeds.
- HPCs have 3 components. Compute, network, and storage.
  - All 3 must have enough resources to not become a bottleneck.
- Most well-known versions are super computers.



- **Edge Computing Systems:**
  - The processing of data is done as close as possible to where it is needed, we do that by moving the data and compute resources.
  - This will optimize bandwidth use and lower latency.
  - CDN's are one of the most common types of edge computing.
  - 80%+ of large enterprises have already implemented or are in the process of implementing an edge computing strategy.

Software Vulnerabilities and Attacks

- **Buffer overflow (buffer overrun):**
  - An anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations, happen from improper coding when a programmer fails to perform bounds checking.
  - Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs.
  - Buffer overflows can often be triggered by malformed inputs, if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, if an anomalous transaction produces more data, it could cause it to write past the end of the buffer.
  - If this overwrites adjacent data or executable code, this may result in erratic program behavior, including memory access errors, incorrect results, and crashes.
  - By sending in data designed to cause a buffer overflow, it is possible to write into areas known to hold executable code and replace it with malicious code.
- **Race condition (race hazard):**
  - Two or more programs may collide in their attempts to modify or access a file.
  - This can be an attacker with access, altering files which can then result in data corruption or privilege escalation.
  - **TOCTOU** (time of check to time of use):
    - A software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check.
- **Privilege escalation:**
  - Exploiting a bug, design flaw or configuration oversight in an OS or application to gain access to resources that are normally protected from an application or user.
  - Attacker often use this to elevate the user account they have gained access to, in order to get administrator access.
  - The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

- **Backdoors:**
  - Often installed by attackers during an attack to allow them access to the systems after the initial attack is over, to exfiltrating data over time or to come back and compromise other systems.
  - Bypassing normal authentication or encryption in a computer system, a product, or an embedded device, ...
  - Backdoors are often used for securing remote access to a computer or obtaining access to plaintext in cryptographic systems.
- **Ethical Disclosure:**
  - What do you do when you discover a vulnerability? we covered some of this in the white, gray, black hat hacker section.
  - **Full disclosure:** Tell everyone, make it public, assuming attackers already know and are using it.
  - **Responsible/Partial disclosure:** Telling the vendor, they have time to develop a patch and then disclose it.
    - If they do nothing, we can revert to the full disclosure forcing them to act.
  - **No disclosure:** Attackers finding a vulnerability would try to exploit it and keep it secret as long as possible.

System Vulnerabilities and Attacks

- **Security Orchestration, Automation, and Response (SOAR):**
  - A software solution that uses AI to allows us to respond to some security incidents automatically.
  - SOAR vs. SIEM: Very similar, both detect and alert on security events, but using AI, SOAR will also react to some security events.
    - SIEMs often generate more alerts than a SOC team can handle, SOAR can help reduce the number of alerts and make workflows more manageable.
  - SOAR combines all the comprehensive data we gather, has case management, standardization, workflows, and analytics, and it can integrate with many of our other solutions (Vulnerability Management (VM), IT Service Management (ITSM), Threat Intelligence, …).
  - All this can help our organization implement a detailed defense-in-depth solution.

- **Operation and Maintenance:**
  - Once our finished software/project is handed off to operations, there will still be some maintenance tasks our organization needs to perform.
  - Our environment and the requirements for our applications are never static.
  - We need a solid support team in place to make sure the software functions as required, that any required changes are implemented using proper change management, and that all this is done with security in mind.

- **Integrated Development Environment (IDE):**
  - Applications that help in the development of other applications.
  - They are designed to contain all programming tasks in a single application, having a single central interface with all the tools the developer needs, including:

- **The Code editor:** For writing and editing source code, these editors are different from text editors, they are designed to either simplify or enhance the process of writing and editing the code.
- **Compiler:** The compilers change our source code, which is written in a human-readable language, into a form that computers can execute.
- **Debugger:** Debuggers are used during the testing phase and can help our developers debug their code.
- **Build automation tools:** Tools to help automate common dev tasks to save time.
- On top of this some IDEs may also include:
  - **Class browser:** Used to reference and study the properties of an object-oriented class hierarchy.
  - **Object browser:** Used to inspect objects present in a running application program.
  - **Class hierarchy diagram:** Helps devs to visualize the structures of object-oriented programming code.

- **Runtime:**
  - Runtime is the amount of time when a program is running. Starting when a program is executed/started and stopping with the program terminated/closed.
  - The term, runtime, is most often used in software development. Commonly used with "runtime error," an error that occurs while a program is running. This error is used to differentiate from other types of errors, like syntax errors and compilation errors, which happen before a program is run.

Emanations and Covert Channels

- **Emanations -** Often Electromagnetic Emanations.
  - Information that can be disseminated from the electrical changes from a system or a wire.
  - It is possible to log a user's keystrokes on a smart phone using the motion sensor.
  - It is unintentional information-bearing signals, which - if intercepted and analyzed - can lead to a compromise.
  - We can protect against Electromagnetic Emanations with heavy metals, but we would have 80 lbs. (40 kgs.) laptops.
- **Covert Channels** – Creates the capability to transfer information using channels not intended to do so.
  - **Covert Timing Channels:** Operations that affect the "real response time observed" by the receiver.
    - Most common is username/password - wrong username takes 100ms to confirm, wrong password takes 500ms to confirm, you get the "Wrong username or password" error, but an attacker can tell when they use a correct username because of the delay difference.
  - **Covert Storage Channels:** Hidden information through the modification of a stored object.
    - Certain file sizes have a certain meaning.
    - Attackers can add data in payload if outbound ICMP packets (Unless we need it, block outbound ICMP packets).
  - **Steganography** - Hiding a message within another media (invisible ink and the hidden clues in da Vinci's paintings).

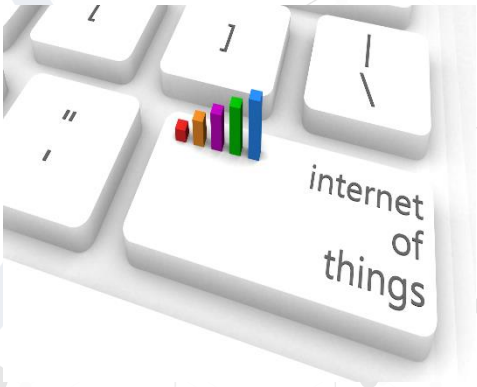
- The messages can be hidden in anything really, most commonly images and soundtracks.
- On images like this one, the program changes the shading of some of the pixels of the image. To the naked eye, it is not noticeable, but a lot of information can be hidden in the images this way.
- Hidden in the bottom image is the first chapter of G*reat Expectations* (Charles Dickens, 1867 Edition - 4 pages at font size 11, 1827 words, 7731 characters).

Original image

- **Digital Watermarks** encode data into a file.
  - The watermark may be hidden, using steganography, or visible watermarks.
  - Often used to fingerprint files (the file is identified as yours).

Altered image

The Internet of Things (IoT)



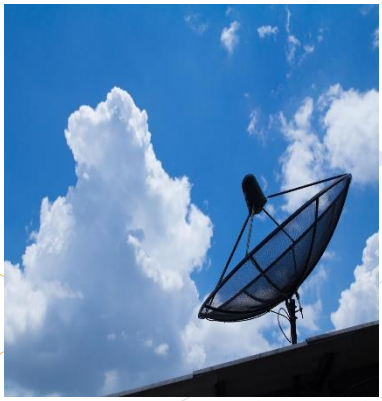
- It is really anything "Smart": Smart TVs, Thermostats, Lightbulbs, Cars, anything that connects to the internet in some way (that didn't before).
- They can be an easy way into your smart device, as most are never patched (many don't even have the option).
- Most devices have very basic security (if any). They use the default login/password, and they often use well-known ports, making them easy to target. We harden here, we patch, segment the network, lock ports, and change defaults.
- They are not only simple to hack but can also provide attackers an easy way onto your network. If you use it in your organization or at home, segment that part of the network off from everything else and lock it down.

WLAN (Wireless LAN) Technologies and Protocols

- **Li-Fi:**
  - Uses light to transmit data and position between devices.
  - Can send high-speed data using visible light, ultraviolet, and infrared spectrums.
  - Can be used in areas prone to EMI (Electromagnetic interference), such as aircraft cabins, hospitals, and nuclear power plants.
  - Speeds (currently) up to 100 Gbit.
  - Light can reflect off walls and still reach 70 Mbit without requiring a direct line of sight.
  - Pros: Not the same capacity as Wi-Fi (radio frequency exhaustion) and can be used in places where Wi-Fi is prohibited.
  - Cons: Short-range, not always reliable, and high cost of implementation.

- **Zigbee:**
  - Mesh wireless network with low power, low data rate, and close proximity.
  - Simple and less complex compared to other WPANs (Wireless Personal Area Networks) such as Bluetooth or Wi-Fi.
  - It has a range of 10 to 100 meters, but it requires line-of-sight. Data rates vary between 20 kbit/s (868 MHz band) and 250 kbit/s (2.4 GHz band).

- **Satellite:**
  - For many years, satellite internet was a relatively slow and expensive option.
  - You have a modem, as with any other internet connection, as well as a satellite dish (2-3 ft. or 60-90 cm).
  - Typical satellite connections have had a latency of 500 ms and speeds ranging from 10 to 50 Mbps.
  - Starlink is currently testing speeds ranging from 20-200 Mbps down to 15-50 Mbps up, with latencies ranging from 15-40 ms.



Cellular Networks

- Cellular networks/mobile networks are communication networks where the last leg is wireless.
- The network is divided into cells and distributed across areas, with each cell containing at least one fixed-location transceiver, if not more.
- These base stations provide network coverage to the cell, allowing it to transmit voice, data, and other types of content.
- To avoid interference and provide guaranteed service quality within each cell, a cell typically uses a different set of frequencies than neighboring cells.

- **3G:**
  - Bandwidth: 2 Mbps, latency: 100-500 ms, average speed 144 kbps.
- **4G:**
  - Bandwidth: 200 Mbps, latency: 20-30 ms, average speed 25 Mbps, 16km (10 miles).
- **5G:**
  - Bandwidth: 5-20 Gbps, latency: <10 ms, average speed 200-400 Mbps, 500m (1500 ft).
  - High frequency, short-range, and can be blocked by anything metal and even just solid objects.
  - A lot more 5G towers are needed to get coverage.

What we covered in Domain 2

- Congratulations on finishing Domain 2: Information Security Risk Management.
- 20% of the exam questions on the certification are from this domain.

- We identify all of our assets, identify the risks, then we assess the risks with qualitative and quantitative risk analysis, we respond to the risk, mitigation, and then we monitor controls.
- We talked about attackers, and he attacks in OWASP top 10 (2021).
- We covered how we secure our communication, software, and systems, by securing our networking, networking devices.
- Many networking basics like IP, NAT, PAT, protocols, hardware, and software, wireless and much more from networking.
- Finally, we talked about what cloud computing is and what is our responsibility to secure and IOT.

- This should be what you are tested on for Domain 2 until the next planned CISM curriculum change in 2027.

OSI model - Open Systems Interconnection Reference model