CISM®

DOMAIN 2

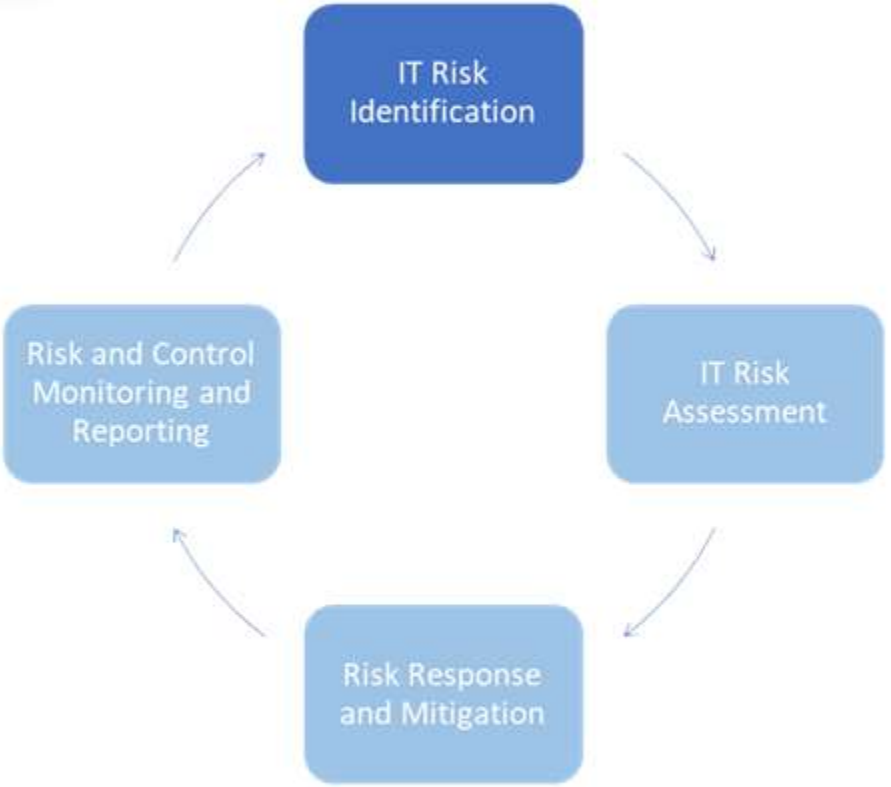
Welcome to the second CISM Domain.

- 30% of the exam questions on the certification are from this domain.
- As the name indicates, how do we manage our risk?
- What can we do to reduce the risk to an acceptable level?
- We identify all of our assets, and do qualitative and quantitative risk analysis.
- We cover the COBIT5, ISO27001/2, NIST 800-37, and NIST 800-53.
- System and software vulnerabilities.
- Networking, networking devices, IP, NAT, PAT, …
- Physical security.
- Redundancy, RAID, backups.

Risk Management - Identification:

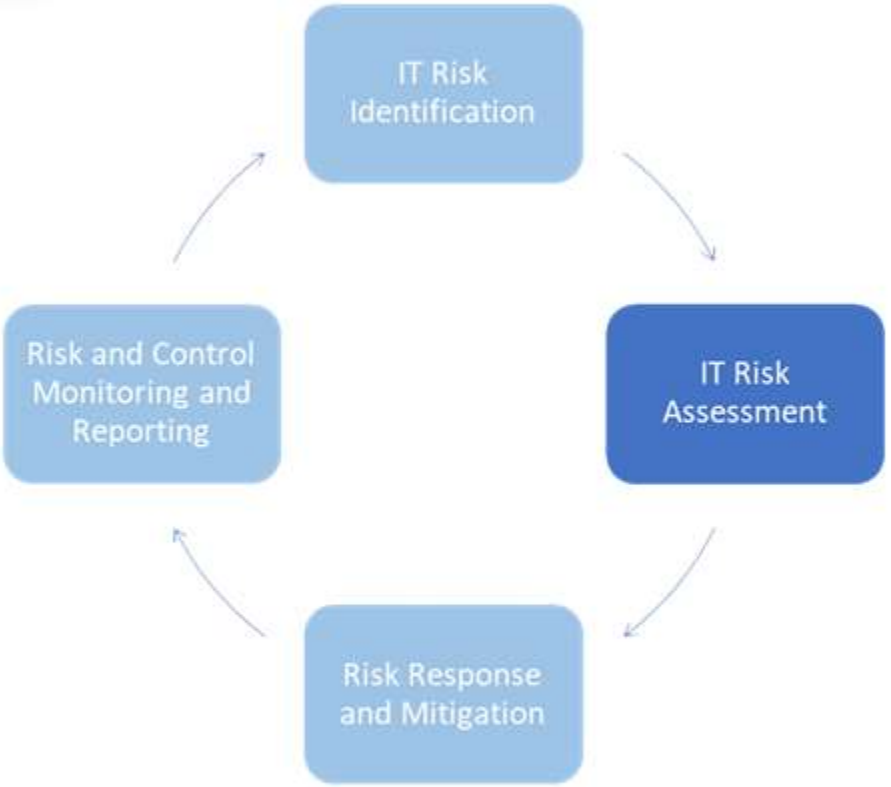
- Risk = Threat * Vulnerability
- The Risk Management lifecycle is iterative.

- 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 Management - Assessment:

- **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 anti-virus, …
  - **Risk** = Threat x Vulnerability.
  - **Impact** - Can at times be added to give a more full picture. Risk = Threat x Vulnerability x Impact (How bad is it?).
  - **Total Risk** = Threat x Vulnerability x Asset Value.
  - **Residual Risk** = Total Risk – Countermeasures.

Risk Management - Assessment:

- **Qualitative Risk Analysis with the Risk Analysis Matrix.**
- 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.
- 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".

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

Risk registers:

- 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.

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

Risk Management - Assessment:

- **Quantitative Risk Analysis** – We want exactly enough security for our needs.
  - This is where we put a number on that.
  - 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 Value 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 cost 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.

Risk Management - Assessment:

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)

Risk Management - Assessment:

Quantitative Risk Analysis

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.

Risk Management - Assessment:

- **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 up 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.

Risk Management - Assessment:

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).

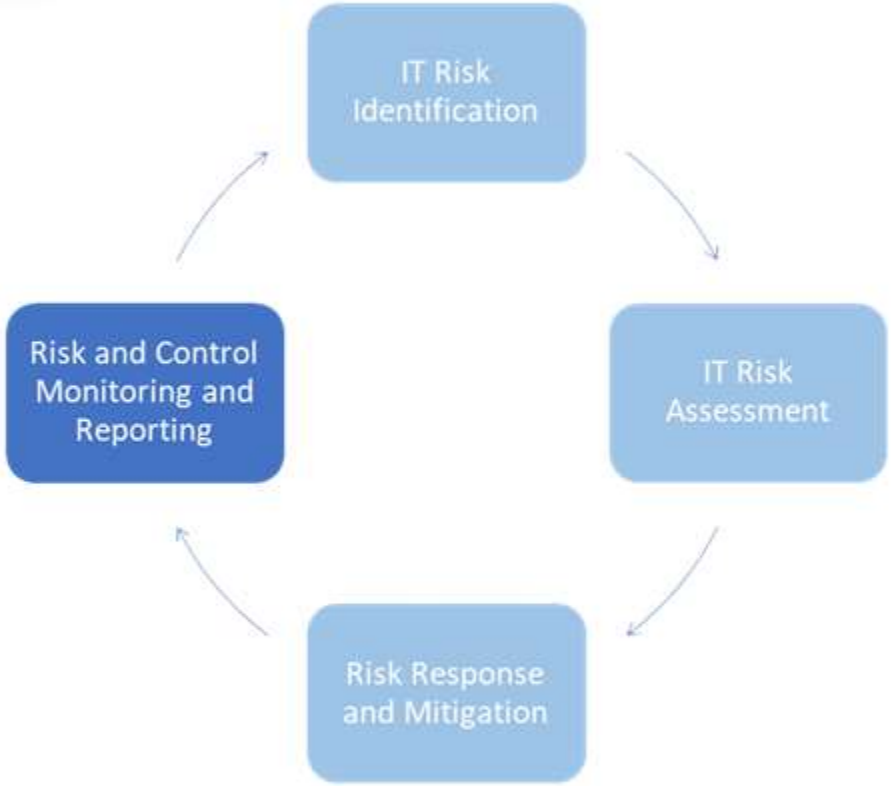
ThorTeaches.com

Risk Management:

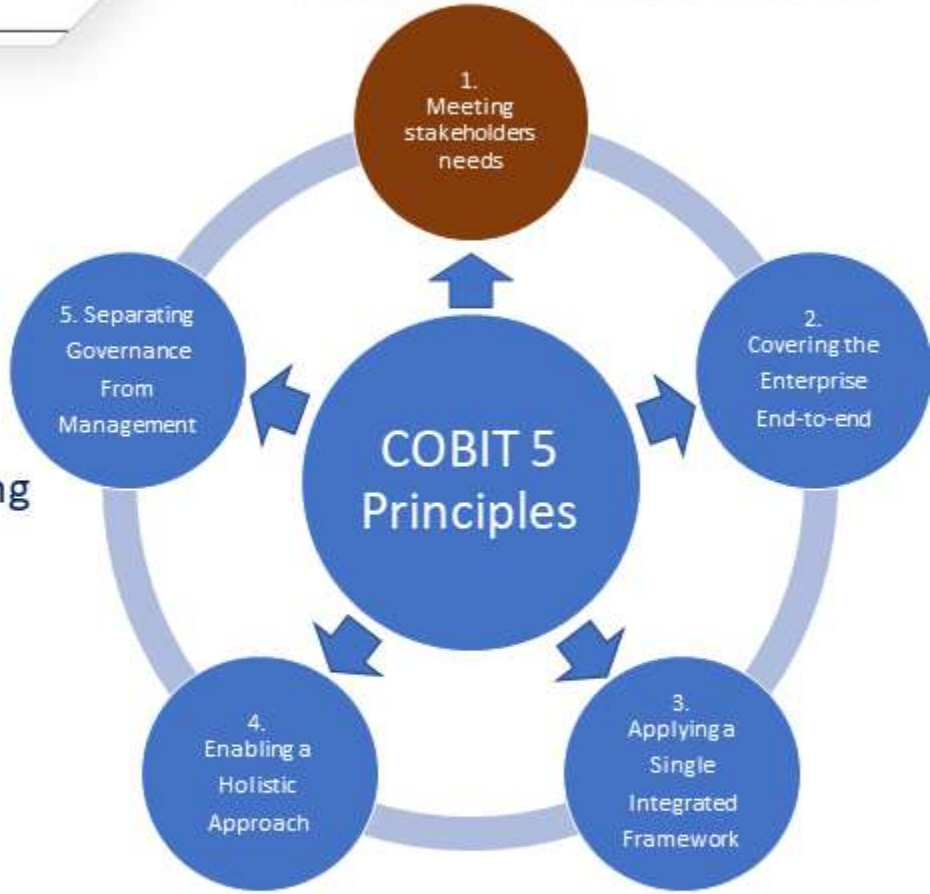
- **Risk response and mitigation.**
  - Risk mitigation, transference, acceptance or avoidance.
  - We act on senior managements choices, which they made based on our recommendations from the assessment phase.
  - Do we stop issuing laptops, or do we add full-disk encryption and remote wipe capabilities?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

Risk Management:

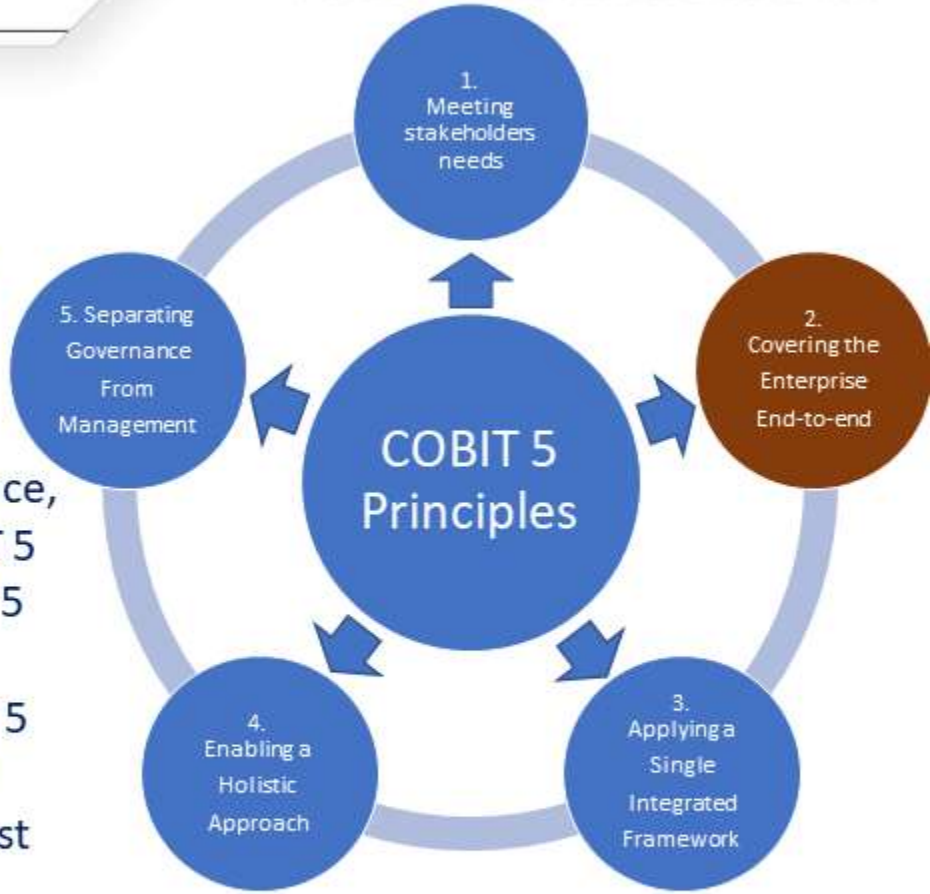
- **Risk and Control Monitoring and Reporting.**
  - The process is ongoing, we have to keep monitoring both the risk and the controls we implemented.
  - This is where we would use the KRIs (Key Risk Indicators).
  - We would also use KPIs (Key Performance Indicators).
  - You are the translating link, 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.



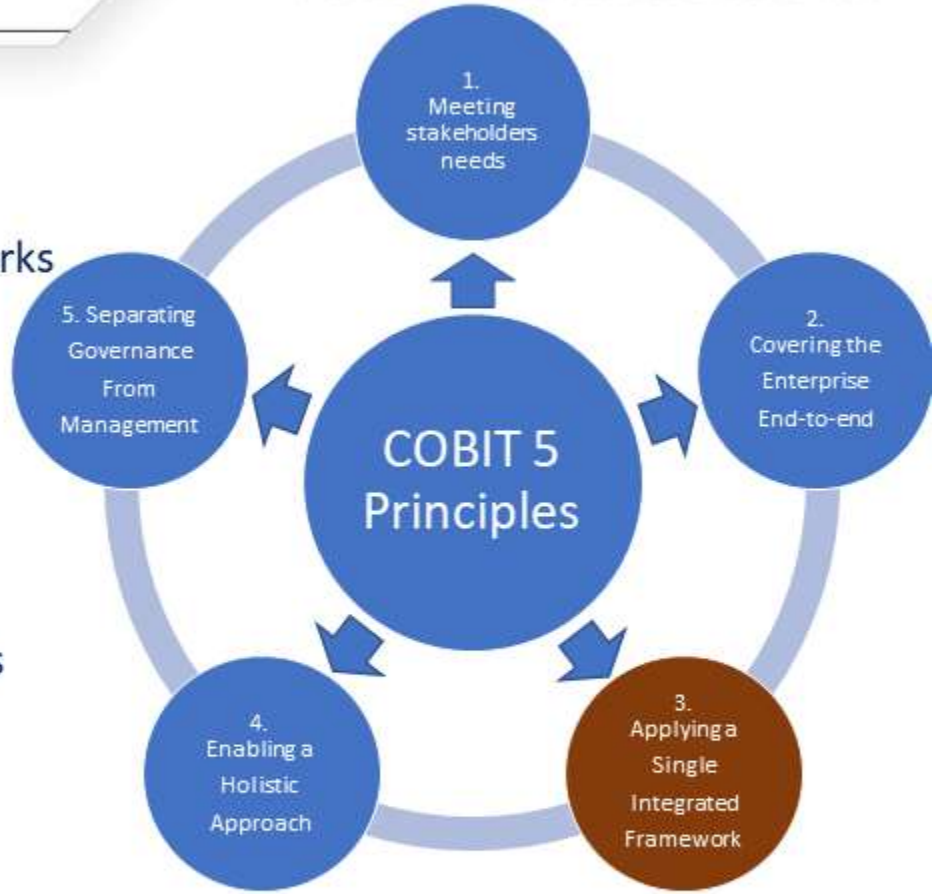
- **COBIT 5:**
  - **Principle 1: Meeting Stakeholder Needs**
    - Enterprises have many stakeholders, and 'creating value' means different—and sometimes conflicting—things to each of them.
    - Governance is about negotiating and deciding amongst different stakeholders' value interests.
    - The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.
    - For each decision, the following can and should be asked:
      - Who receives the benefits?
      - Who bears the risk?
      - What resources are required?
    - Stakeholder needs have to be transformed into an enterprise's practical strategy.



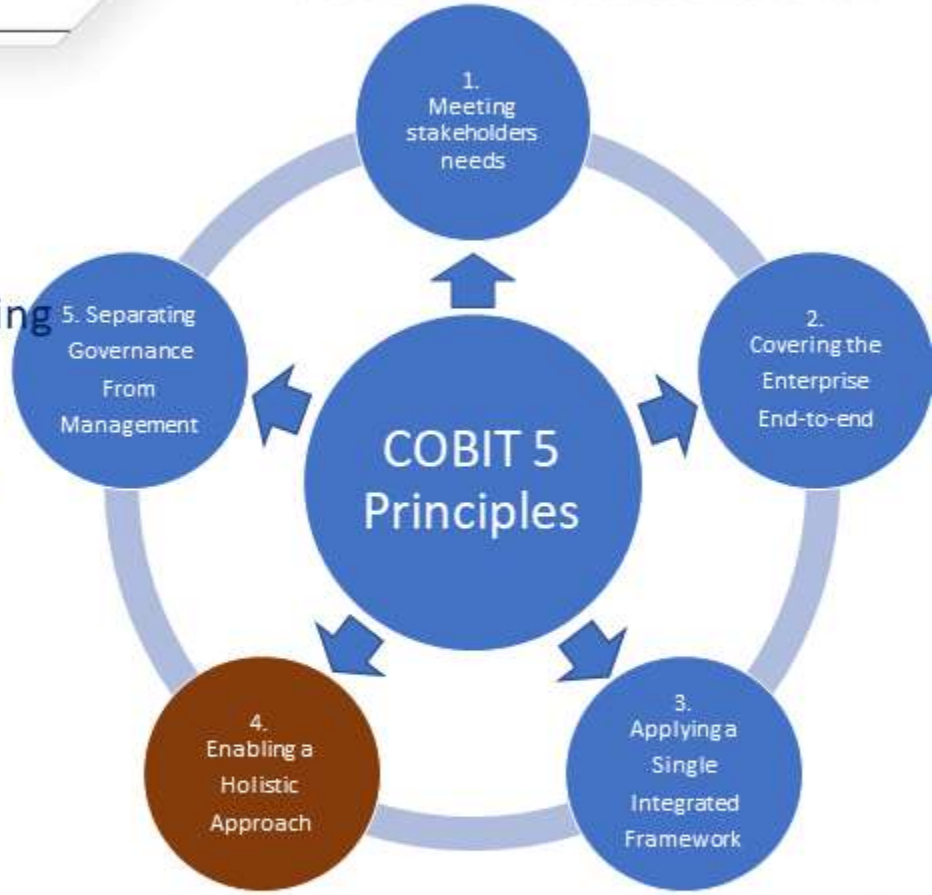
- **COBIT 5:**
  - **Principle 2: Covering the enterprise end-to-end.**
    - COBIT 5 addresses the governance and management of information and related technology from an enterprise wide, end-to-end perspective.
    - This means that COBIT 5:
      - Integrates governance of enterprise IT into enterprise governance, i.e., the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on governance.
      - Covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.



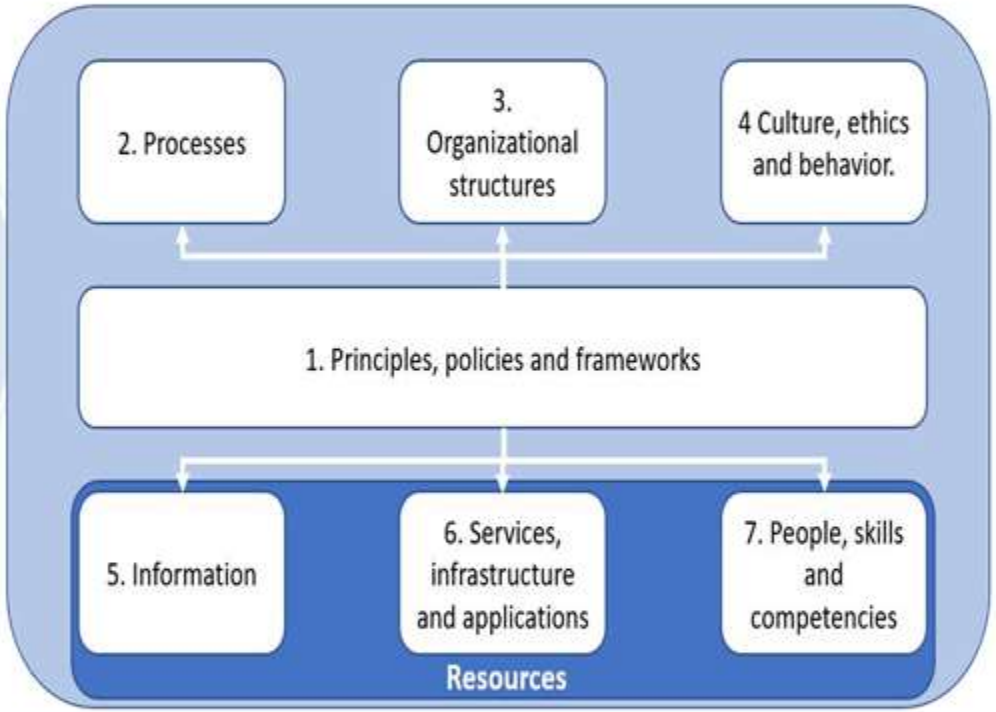
- **COBIT 5:**
  - **Principle 3: Applying a Single, Integrated Framework**
    - COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:
      - Enterprise: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
      - IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI
    - This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
    - ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references.



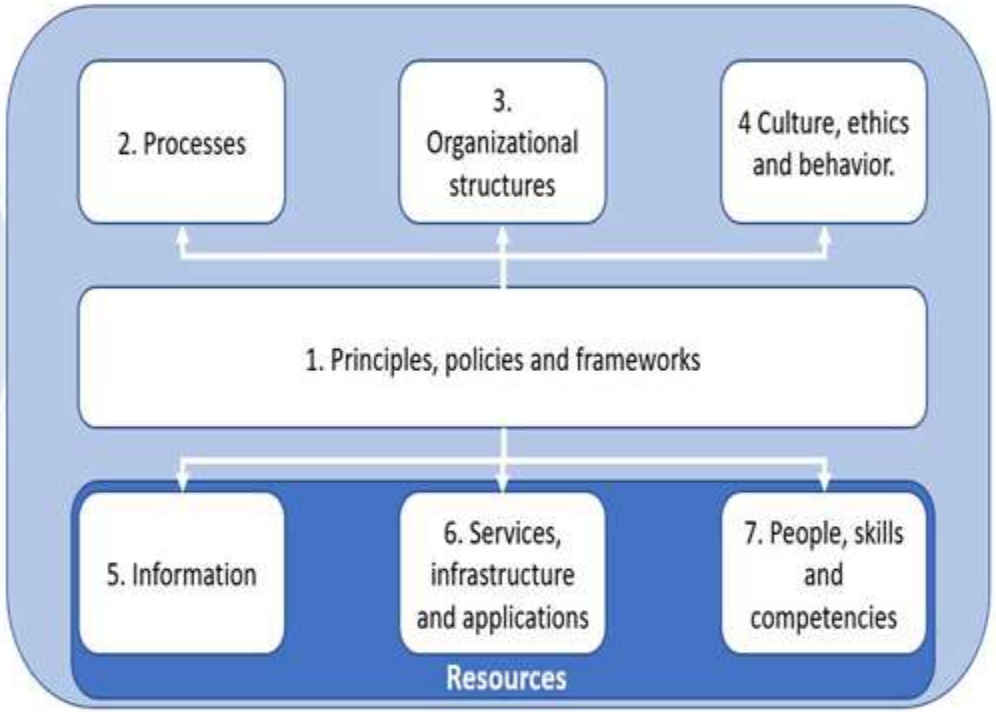
- **COBIT 5:**
  - **Principle 4: Enabling a Holistic Approach**
    - COBIT 5 enablers are:
    - Factors that, individually and collectively, influence whether something will work—in the case of COBIT, governance and management over enterprise IT
    - Driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve
    - Described by the COBIT 5 framework in seven categories.



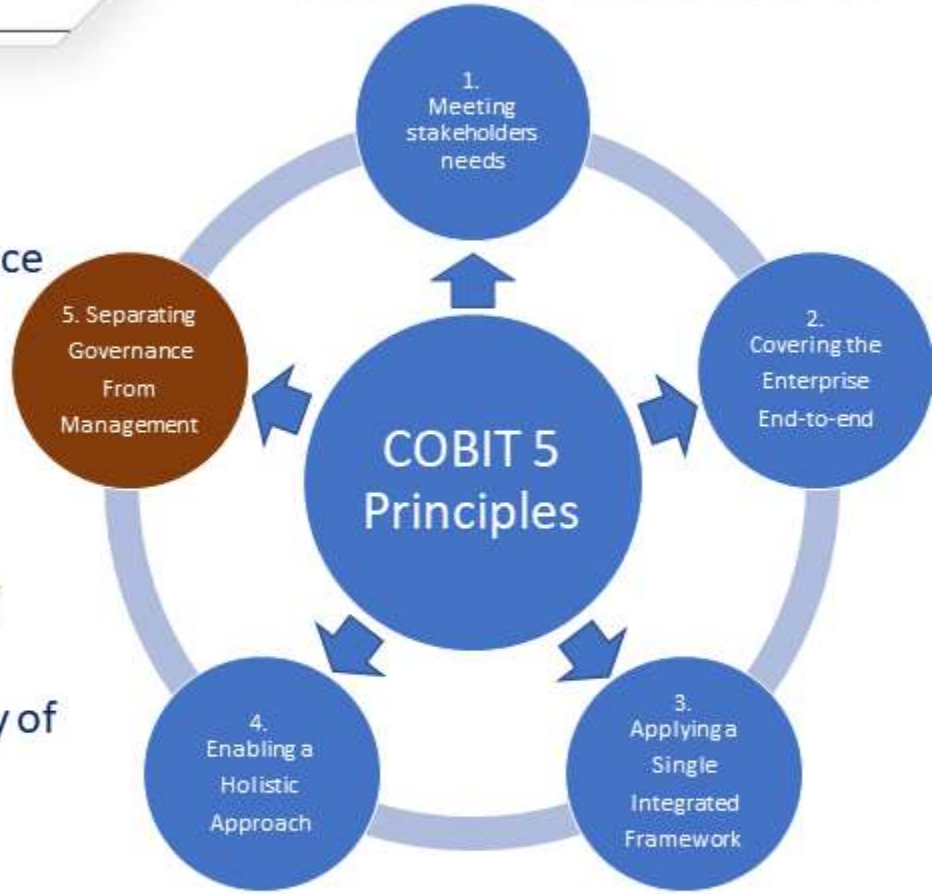
- **COBIT 5:**
  - **Principle 4: Enabling a Holistic Approach**
    1. **Principles, policies and frameworks:** Are the vehicles to translate the desired behavior into practical guidance for day-to-day management
    2. **Processes:** Describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals
    3. **Organizational structures:** Are the key decision-making entities in an organization
    4. **Culture, ethics and behavior:** Of individuals and of the organization; very often underestimated as a success factor in governance and management activities



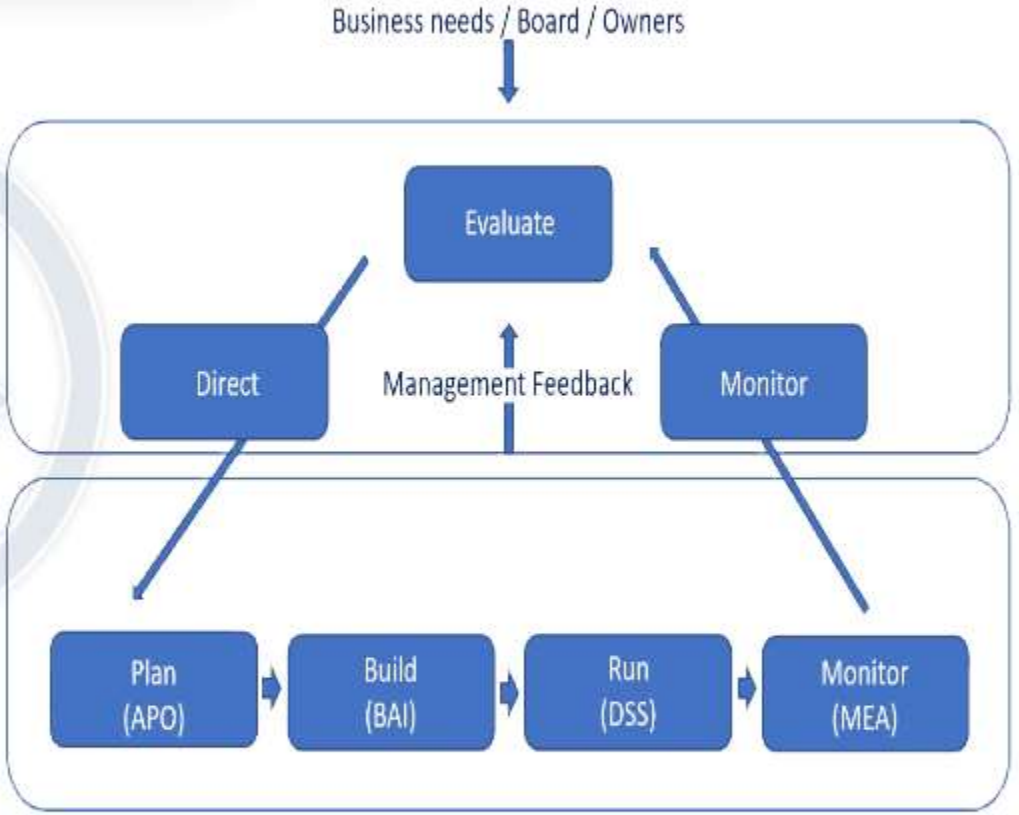
- **COBIT 5:**
  - **Principle 4: Enabling a Holistic Approach**
    5. **Information:** Is pervasive throughout any organization, it deals with all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
    6. **Services, infrastructure and applications:** Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services
    7. **People, skills and competencies:** Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions



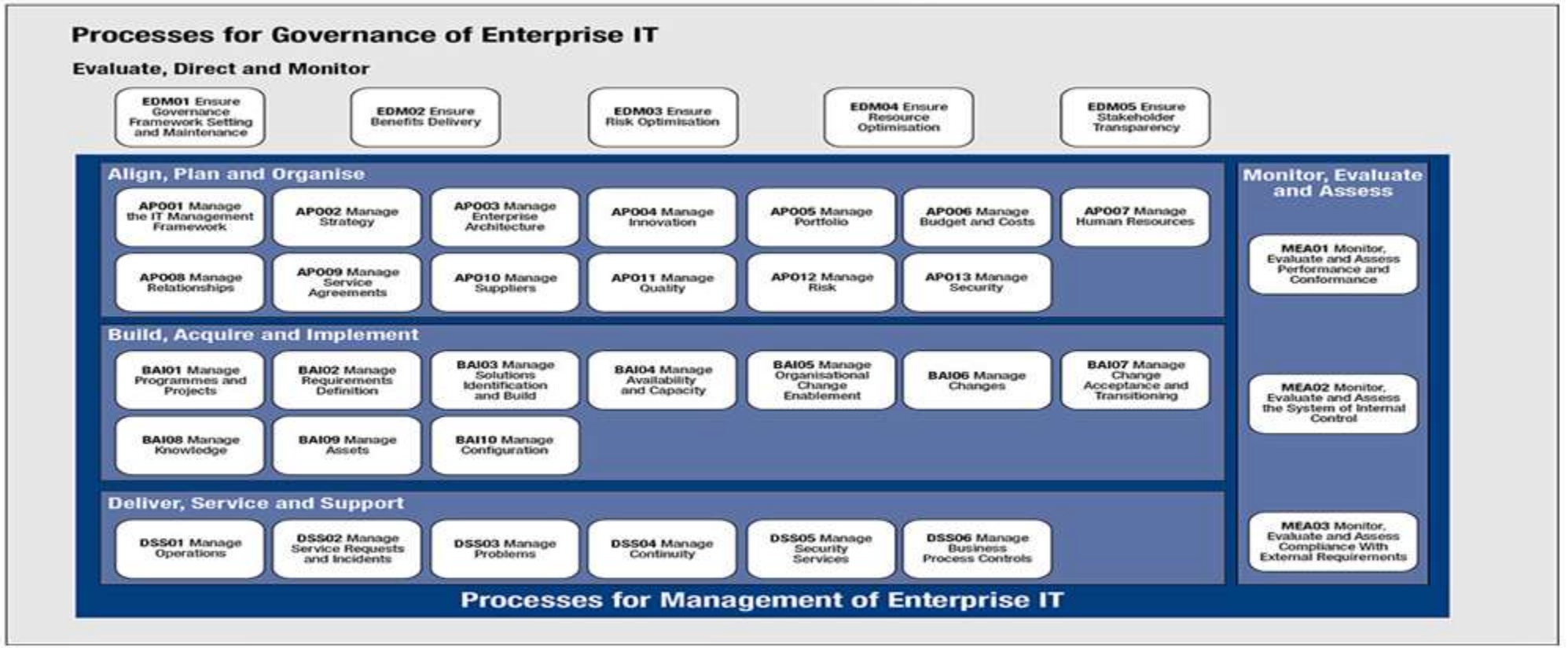
- **COBIT 5:**
  - **Principle 5: Separating Governance from Management**
    - The COBIT 5 framework makes a clear distinction between governance and management.
    - These two disciplines:
      - Encompass different types of activities.
      - Require different organizational structures
      - Serve different purposes
    - **Governance**: In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.
    - **Management**: In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.



- **COBIT 5:**
  - **Principle 5: Separating Governance from Management**
    - **Governance** ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.
    - **Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.



- **COBIT 5:**



Risk Analysis:

- **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.

Risk Analysis:

Types of attackers:

- **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.

Risk Analysis:

Types of attackers:

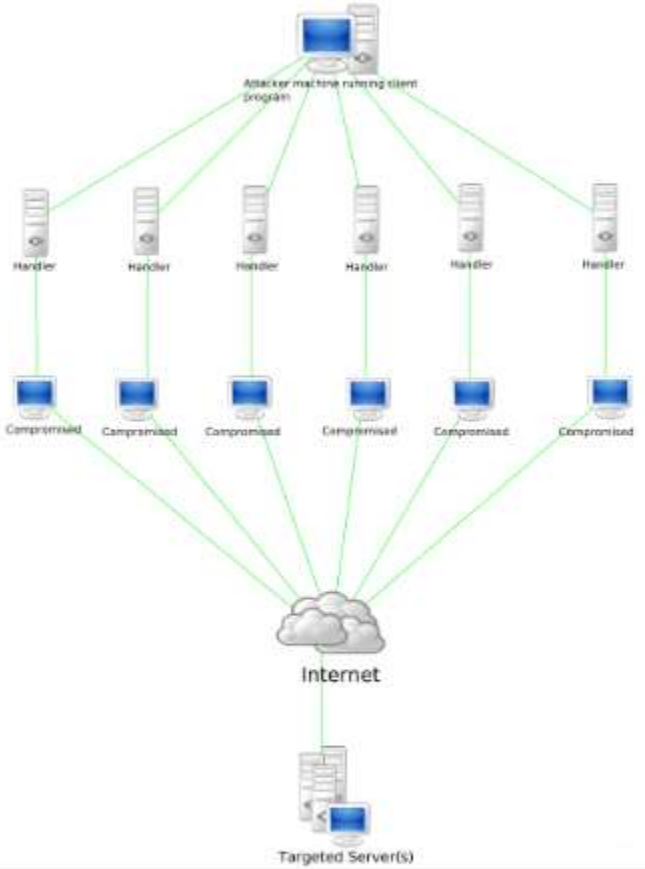
- **Hacktivism/Hacktivist (hacker activist):** Hacking for political or socially motivated purposes.
  - Often aimed at ensuring free speech, human rights, freedom of information movement.
  - Famous attacks: Anonymous – DDOS attack on Visa, Mastercard, PayPal to protest the arrest of Julian Assange (WikiLeaks). Google/Twitter/SayNow worked together to provide communication for the Egyptian people when the government orchestrated an internet blackout during the 2011 protests.
- **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), …

ThorTeaches.com

Risk Analysis:

Types of attackers:

- **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 can 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.



Risk Analysis:

Types of attackers:

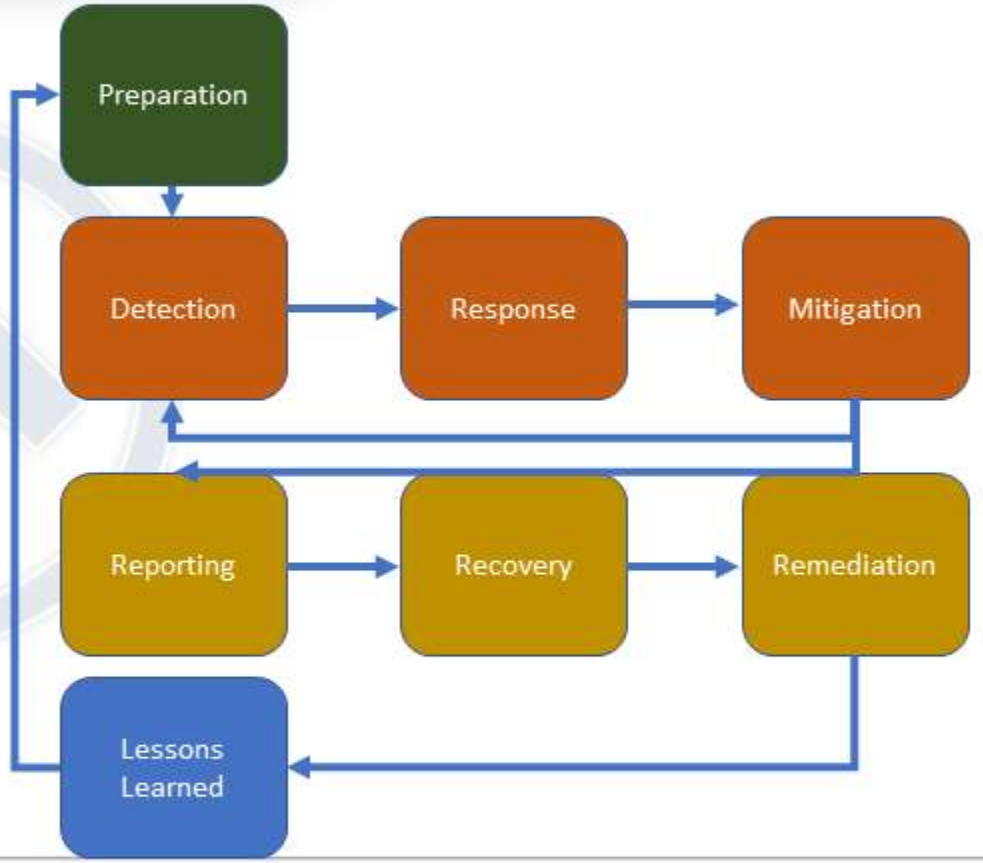
- **Phishing, spear phishing and whale phishing** (Fisher spelled in hacker speak with Ph not F).
  - **Phishing** (Social engineering email attack):
    - Click to win, Send information to get your inheritance …
    - Sent to hundreds of thousands of people; if just 0.02% follow the instructions they have 200 victims.
      - A public treasurer in Michigan sent $1.2m to Nigeria ($1.1m of taxpayer funds and $72,000 of his own).
  - **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.

- **Administrative Security:**
  - **Incident management:**
    - Involves the monitoring and detection of security events on our systems, and how we react in those events.
    - It is an administrative function of managing and protecting computer assets, networks and information systems.
    - The primary purpose is to have a well understood and predictable response to events and computer intrusions.
    - We have very clear processes and responses, and our teams are trained in them and know what to when an event occurs.
    - Incidents are very stressful situations, it is important staff knows exactly what to do, that they have received ongoing training and understand the procedures.
    - **Incidences and events can generally be categorized in 3 classes:**
      - **Natural:** Hurricanes, floods, earthquakes, blizzards, anything that is caused by nature.
      - **Human**: Done intentionally or unintentionally by humans, these are by far the most common.
      - **Environmental**: This is not nature, but the environments we work in, the power grid, the internet connections, hardware failures, software flaws, …

- **Administrative Security:**
  - **Incident management:** 
    - **Event:**
      - An observable change in state, this is neither negative nor positive, it is just something has changed.
      - A system powered on, traffic from one segment to another, an application started.
    - **Alert:**
      - Triggers warnings if certain event happens.
      - This can be traffic utilization above 75% or memory usage at 90% or more for more than 2 minutes.
    - **Incident:**
      - Multiple adverse events happening on our systems or network, often caused by people.
    - **Problem:**
      - Incidence with an unknown cause, we would follow similar steps to incidence response.
      - More time would be spent on root cause analysis, we need to know what happened so we can prevent it from happening again, this could be a total internet outage or server crash.

- **Administrative Security:**
  - **Incident management:**
    - **Inconvenience (non-disasters)**:
      - Non-disruptive failures, hard disk failure, 1 server in a cluster is down, ..
    - **Emergency (Crisis)**:
      - Urgent, event with the potential for loss of life or property.
    - **Disaster:**
      - Our entire facility is unusable for 24 hours or longer.
      - If we are geographically diverse and redundant we can mitigate this a lot.
      - Yes, a snowstorm can be a disaster.
    - **Catastrophe**:
      - Our facility is destroyed.

- **Administrative Security:**
  - **Incident management:**
  - The current exam lists a 7-step lifecycle, but does not include the first step in most incident handling methodologies preparation.
    1. **Preparation.**
    2. **Detection** (Identification).
    3. **Response** (Containment).
    4. **Mitigation** (Eradication).
    5. **Reporting.**
    6. **Recovery.**
    7. **Remediation.**
    8. **Lessons Learned** (Post-incident Activity, Post Mortem, or Reporting).



- **Administrative Security:**
  - **Incident management:**
    - **Preparation**:
      - This is all the steps we take to prepare for incidences.
      - We write the policies, procedures, we train our staff, we procure the detection soft/hardware, we give our incidence response team the tools they need to respond to an incident.
      - The more we train our team, the better they will handle the response, the faster we recover, the better we preserve the crime scene (if there is one), the less impactful an incident will be.
    - **Detection**
      - Events are analyzed to determine if they might be a security incident.
      - If we do not have strong detective capabilities in and around our systems, we will most likely not realize we have a problem until long after it has happened.
      - The earlier we detect the events, the earlier we can respond, IDS's can help us detect, where IPS's can help us detect and prevent further compromise.

- **Administrative Security:**
  - **Incident management:**
    - **Detection**
      - The IDS's and IPS's can help us detect and prevent on a single network segment, we also need something that can corollate all the information from the entire network.
    - **Response**
      - The response phase is when the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.
      - This can be taking a system off the network, isolating traffic, powering off the system, or however our plan dictates to isolate the system to minimize both the scope and severity of the incident.
      - Knowing how to respond, when to follow the policies and procedures to the letter and when not to, is why we have senior staff handle the responses.
      - We make bit level copies of the systems, as close as possible to the time of incidence to ensure they are a true representation of the incident.

- **Administrative Security:**
  - **Incident management:**
    - **Response:**
      - IT Security is there to help the business, it may not be the choice of senior management to disrupt business to contain or analyze, it is ultimately a decision that is made by them.
      - We stop it from spreading, but that is it, we contain the event.
    - **Mitigation:**
      - We understand the cause of the incident so that the system can be reliably cleaned and restored to operational status later in the recovery phase.
      - Organizations often remove the most obvious sign of intrusion on a system or systems, but miss backdoors and other malware installed in the attack.
      - The obvious sign is often left to be found, where the actual payload is hidden. if that is detected or assumed, we often just rebuild the system from scratch and restore application files from a known good backup, but not system files.

- **Administrative Security:**
  - **Incident management:**
    - **Mitigation (continued):**
      - To ensure the backup is good, we need to do root cause analysis, we need a timeline for the intrusion, when did it start?
      - If it is from a known vulnerability we patch. If it's a newly discovered vulnerability we mitigate it before exposing the newly built system to the outside again.
      - If anything else can be learned about the attack, we can add that to our posture.
      - Once eradication is complete, we start the recovery phase.
    - **Reporting:**
      - We report throughout the process beginning with the detection, and we start reporting immediately when we detect malicious activity.
      - The reporting has 2 focus areas: technical and non-technical.

- **Administrative Security:**
  - **Incident management:**
    - **Reporting (continued):**
      - The incident handling teams report the technical details of the incident as they start the incident handling process, but they also notify management of serious incidents.
      - The procedures and policies will outline when which level of management needs to be informed and involved, it is commonly forgotten until later and can be a RPE (Resume Producing Event).
      - Management will also involve other departments if needed, this could be legal, PR or whomever has been identified in the policies or procedures.
    - **Recovery:**
      - We carefully restore the system or systems to operational status.
      - When the system is ready for reinsertion is determined by the business unit responsible for the system.
      - We closely monitor the rebuilt or cleaned system carefully, it is possible the attackers left backdoors or we did not remove all the infected sectors.

- **Administrative Security:**
  - **Incident management:**
    - **Recovery:**
      - Often the system(s) are reinserted off peak hours to minimize the effect of the system(s) still being infected, or they can be introduced in a controlled sandbox environment to see if the infection persists.
    - **Remediation:**
      - The remediation happens during the mitigation phase, where vulnerabilities on the impacted system or systems are mitigated.
      - Remediation continues after mitigation and becomes broader, this can be patching all systems with the same vulnerability or change how the organization authenticates.

- **Administrative Security:**
  - **Incident management:**
    - **Lessons Learned:** 
      - This phase is often overlooked, we removed the problem, we have implemented new controls and safeguards.
      - We can learn a lot from lessons learned, not just about the specific incidence, but how well we handle them, what worked, what didn't.
      - How can we as an organization grow and become better next time we have another incidence? While we may have fixed this one vulnerability there are potentially 100's of new ones we know nothing about yet.
      - At the end of lessons learned we produce a report to senior management, with our findings, we can only make suggestions, they are ultimately in charge (and liable).
      - Often after major incidents organizations shift to a top-down approach and will listen more to IT Security.
      - The outcome and changes of the Lessons Learned will then feed into our preparation.

- **Administrative Security:**
  - **Incident management:**
    - **Root-cause analysis:**
      - We attempt to determine the underlying weakness or vulnerability that allowed the incident to happen.
      - If we do not do the root-cause analysis we will most likely face the same problem again.
      - We need to fix the vulnerability on the system(s) that were effected, but also on any system in the organization that has that particular vulnerability or set of vulnerabilities.
      - We could have a weak password policy and weak encryption, that could be the root cause of a system compromise, we then would implement countermeasures to remove the vulnerability.
      - If we do nothing and just fix the problem, the root of the issue still persists, that is what we need to fix.

- **NIST 800-53 Rev. 4:**
  - Security and Privacy Controls for Federal Information Systems and Organizations.
    - Tier 1: Organization.
    - Tier 2: Mission / Business Processes.
    - Tier 3: Information Systems.

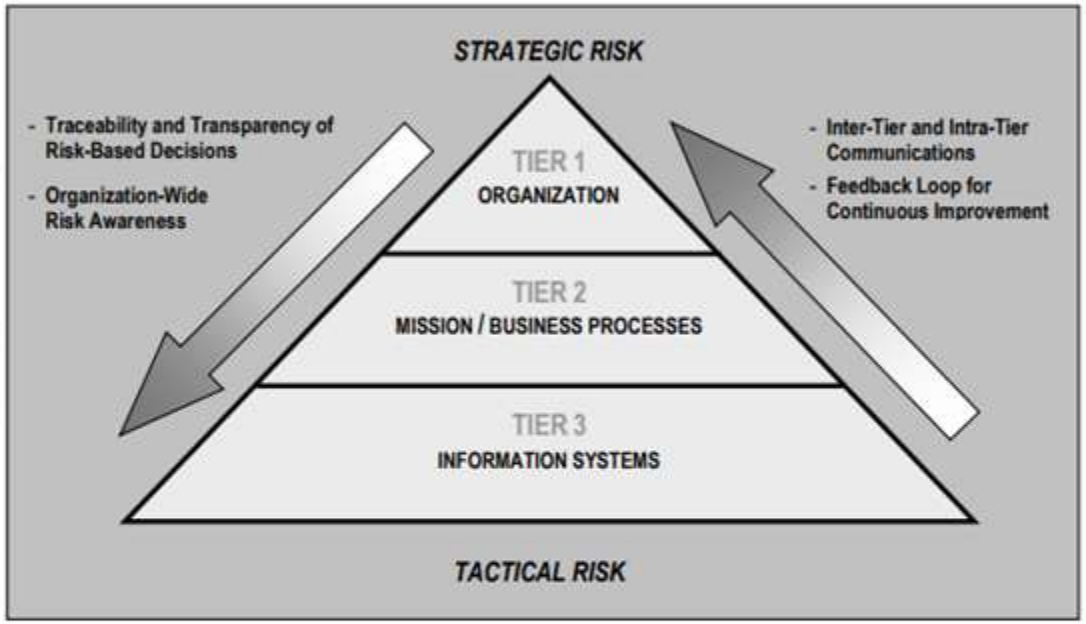


FIGURE 1: THREE-TIERED RISK MANAGEMENT APPROACH

- **NIST 800-53 Rev. 4:**
  - Security and Privacy Controls for Federal Information Systems and Organizations.
    - Tier 1: Organization.
    - Tier 2: Mission / Business Processes.
    - **Tier 3: Information Systems.**
      - Step 2: Select Security Controls.

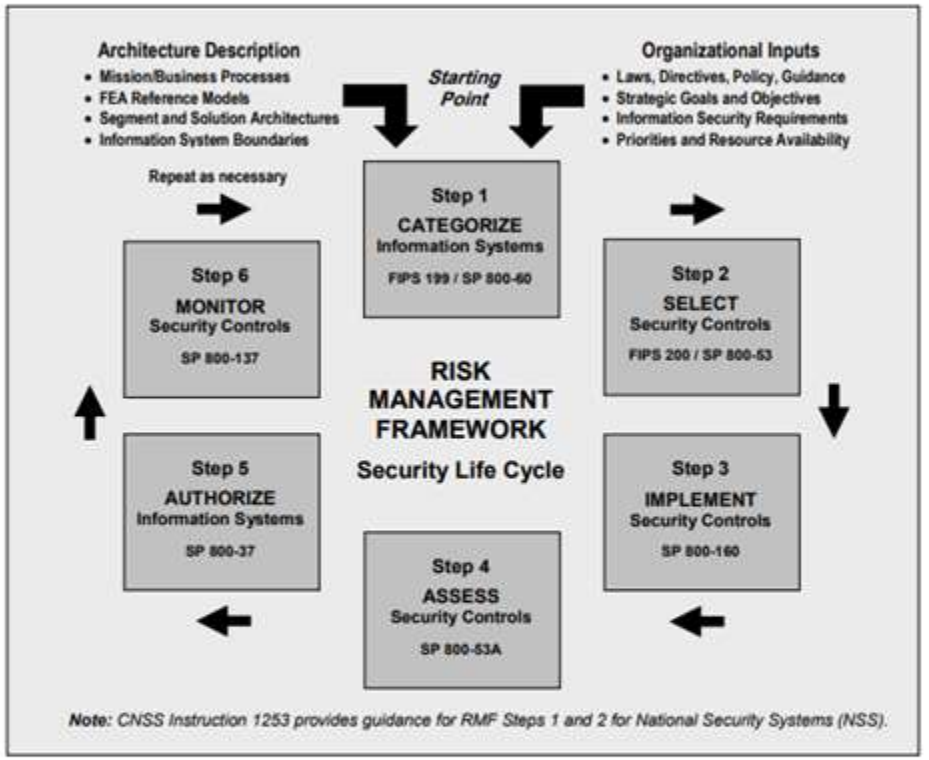


FIGURE 2: RISK MANAGEMENT FRAMEWORK

- **NIST 800-37 Rev. 1 and 2:**
  - Revision 1: Date Published: February 2010 (Updated 6/5/2014).
  - Revision 2: Date Published: December 2018.
  - The last exam revision was done prior to 800-37 R2 being published.

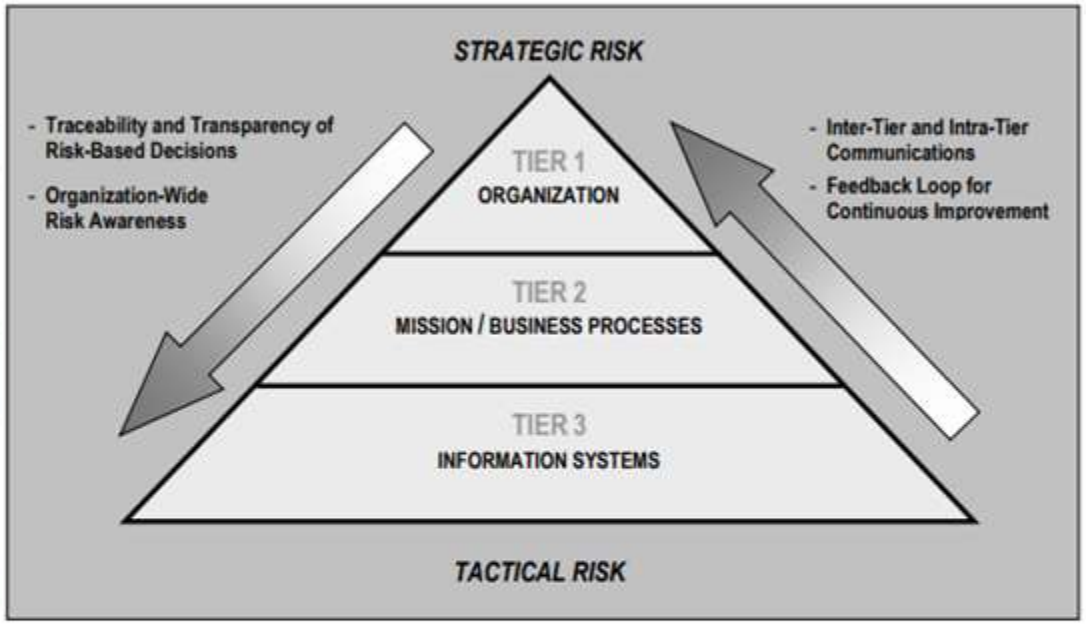


FIGURE 1: THREE-TIERED RISK MANAGEMENT APPROACH

- **NIST 800-37 Rev. 1 and 2:**

There are seven major objectives for this update:

1. To provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization;
2. To institutionalize critical risk management preparatory activities at all risk management levels to facilitate a more effective, efficient, and cost-effective execution of the RMF;
3. To demonstrate how the NIST Cybersecurity Framework [NIST CSF] can be aligned with the RMF and implemented using established NIST risk management processes;
4. To integrate privacy risk management processes into the RMF to better support the privacy protection needs for which privacy programs are responsible;
5. To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes in NIST Special Publication 800-160, Volume 1 [SP 800-160 v1], with the relevant tasks in the RMF;
6. To integrate security-related, supply chain risk management (SCRM) concepts into the RMF to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and
7. To allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in NIST Special Publication 800-53, Revision 5.

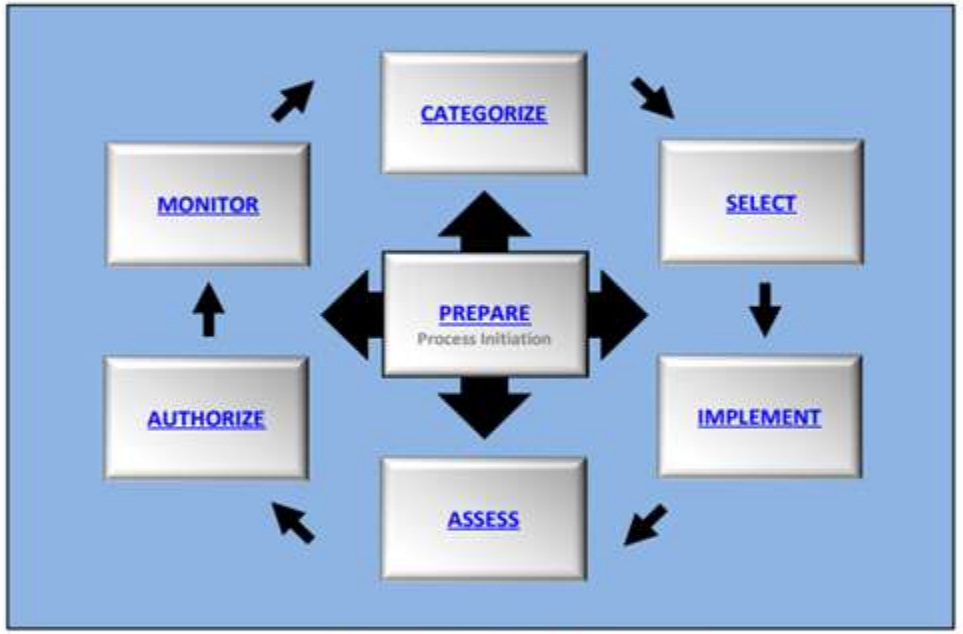


FIGURE 2: RISK MANAGEMENT FRAMEWORK

- **NIST Cyber Security Framework Rev. 1.1**

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

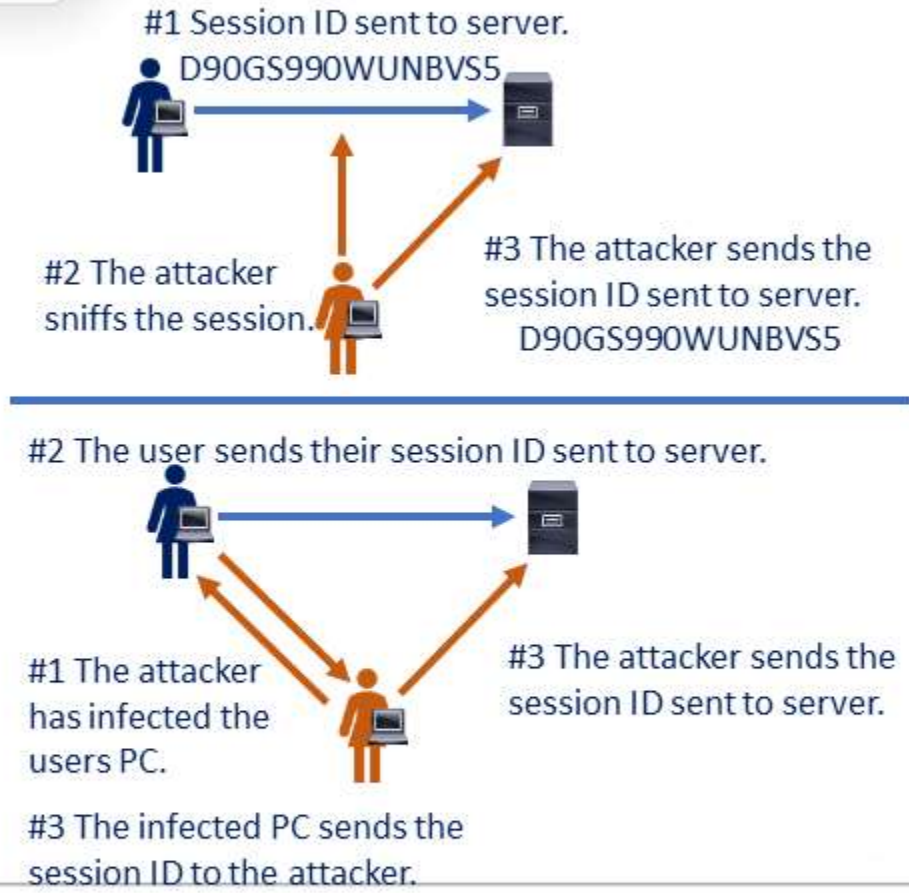
- **ISO/IEC 27001 and 27002**
  - Most organizations have many different of information security controls, if we do not have an information security management system (ISMS), our controls are often disorganized and only cover some of our organization.
  - ISO/IEC 27001 is a management system that is used to bring information security under management control and gives **specific** requirements. It is the framework, and we can get certified against ISO27001.
  - ISO/IEC 27002 provides **best practice** recommendations on information security controls for use by those responsible for initiating, implementing or maintaining ISMS. Much more in detail, how we implement our ISMS.

- **Software vulnerabilities and Attacks**
  - **OWASP** (Open Web Application Security Project):
    - Top 10 of the most common web security issues, from the 2017 candidate list.
      - **A1 Injection.**
      - **A2 Broken Authentication and Session Management.**
      - **A3 Cross-Site Scripting** (XSS).
      - **A4 Broken Access Control.**
      - **A5 Security Misconfiguration.**
      - **A6 Sensitive Data Exposure.**
      - **A7 Insufficient Detection and Response** (NEW still being worked on).
      - **A8 Cross-Site Request Forgery** (CSRF).
      - **A9 Using Components with Known Vulnerabilities.**
      - **A10 Underprotected APIs** (Application Programming Interfaces) (NEW still being worked on).

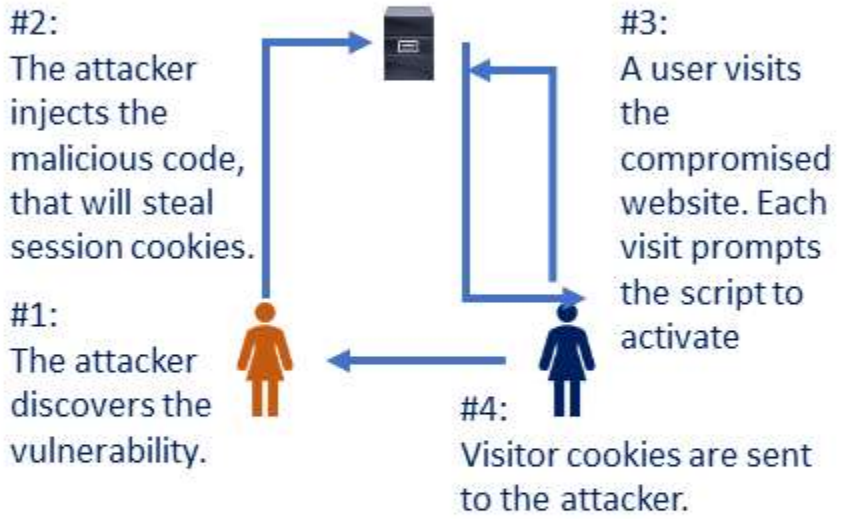
- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A1 Injection.**
      - Can be any code injected into user forms, often seen is SQL/LDAP.
      - Attackers can do this because our software does not use:
        - Strong enough input validation and data type limitations input fields.
        - Input length limitations.
      - 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, ...
      - **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).

ThorTeaches.com

- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A2 Broken Authentication and Session Management.**
      - Sessions do not expire or take too long to expire.
      - Session ID's are predictable. 001, 002, 003, 004, …
      - Tokens, Session ID's, Passwords, … are kept in plaintext.



- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A3 Cross-Site Scripting (XSS).**
      - Attackers inject client-side scripts into web pages viewed by other users.
      - Vulnerability may be used by attackers to bypass access controls such as the same-origin policy.
      - To prevent XSS we can use proper input validation and data typing.
      - Set our server to, redirect invalid requests, detect a simultaneous login from two different IP addresses and invalidate the sessions, require users to enter their passwords again before changing their registration information and set cookie with HttpOnly flag to prevent access from JavaScript.



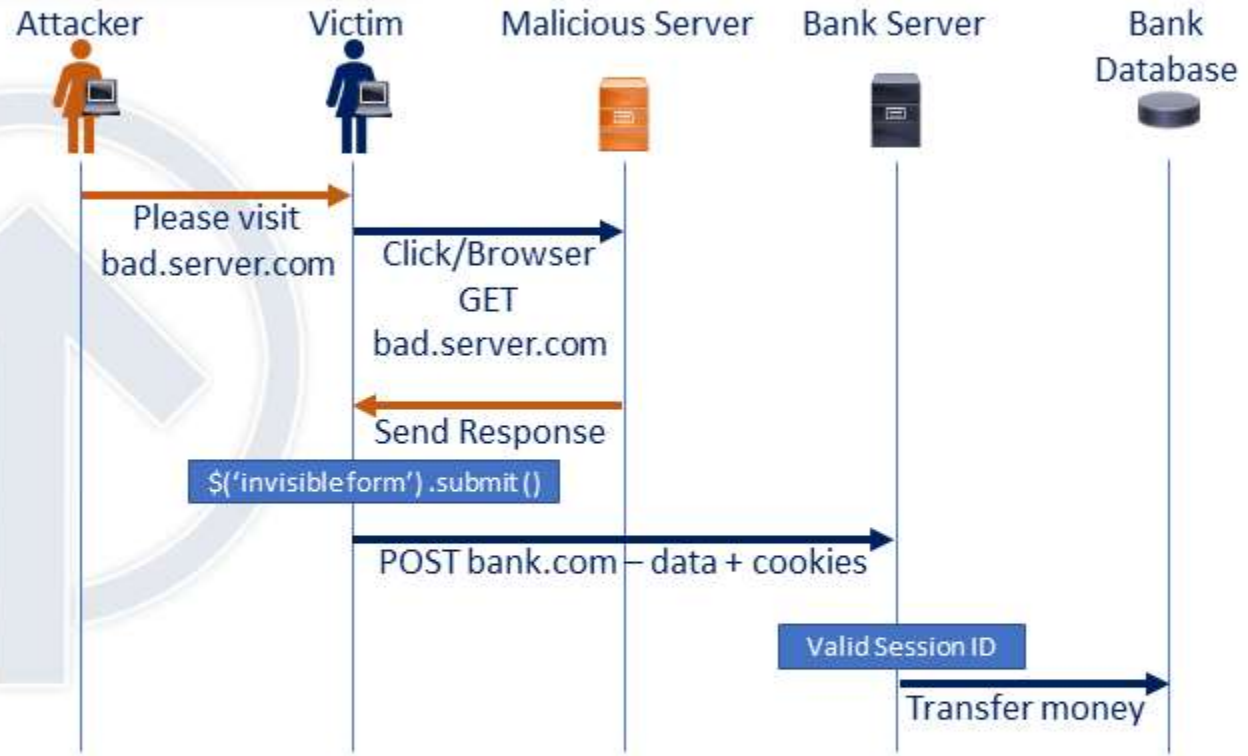
- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A4 Broken Access Control.**
      - Not implemented consistently across an entire application.
      - It might be done correctly in one location, but incorrectly in another.
      - We need a centralized access control mechanism, and we write the tricky logic once and reuse it everywhere.
      - This is important both for writing 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 web site.
      - Inconsistent access control rules are often inserted in various locations all over the code, making it near impossible to manage.
      - One particularly 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.

- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A5 Security Misconfiguration.**
      - Databases configured wrong.
      - Not removing out of the box default access and settings.
      - Keeping default usernames and passwords.
      - OS, Webserver, DBMS, applications, … not patched and up to date.
      - Unnecessary features are enabled or installed, this could be open ports, services, pages, accounts, privileges, ...

- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A6 Sensitive Data Exposure.**
      - Sites being http, not https.
      - Data at rest, backups and in transit are not encrypted (stored/transmitted in plain text).
      - Phishing.
      - Using older weak deprecated encryption.
      - Not monitoring if data is being exfiltrated.

- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A7 Insufficient Detection and Response (NEW).**
      - Not detecting we have been compromised, due to lack of controls, detection applications
      - Not performing our due diligence and due care on our applications, systems, and our response to compromise.
      - Not responding in a proper way to compromise, not informing anyone, informing too late or just ignoring the incident (at best plugging the leak).
      - We need to not just protect against this attack, but future similar attacks, patch software and applications, close ports.

- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A8 Cross-Site Request Forgery (CSRF).**
      - Stolen session ID's or tokens.
      - Often phishing.
      - Passwords/Username saved in cookies.
      - Saved site passwords, not logging off when done, using the same browser for sensitive and non-sensitive information.
      - Current browsers do mitigate some of this, they should use unique session specific tokens (random or pseudo random), and validate session tokens are not replayed.



- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - **A9 Using Components with Known Vulnerabilities.**
      - Developers using deprecated code or objects that are known to be unsecure, but they use them because they are used to it or the library they use has the objects in it.
    - **A10 Underprotected APIs (NEW).**
      - Badly coded API's.
      - Not using in depth API code reviews and auditing.
      - Not using SSL/TLS.
      - Forgotten and abandoned API's, that still have access to backend systems.

- **Software vulnerabilities and Attacks**
  - **OWASP:**
    - 2013 OWASP top 10 vulnerabilities, no longer on the 2017 list, but still something you should know for the exam and you future security job.
    - **2013 A4 Insecure direct object reference.**
      - Users can access resources they shouldn't, by guessing the URL or path, often if it is logical.
      - If you have access to a report name ending in financials_may2017.pdf on your organization's network, you can try guessing other file names you should not have access to financials_August.pdf or financials_2017.pdf
      - Mitigated by proper access control, using non-sequential names or monitoring file usage.
    - **2013 A10 Unvalidated Redirects and forwarding.**
      - Not confirming URL's forward and redirect us to the right page.
      - Mitigated with user awareness and spider our site to see if it generates any redirects (HTTP response codes 300-307, typically 302.

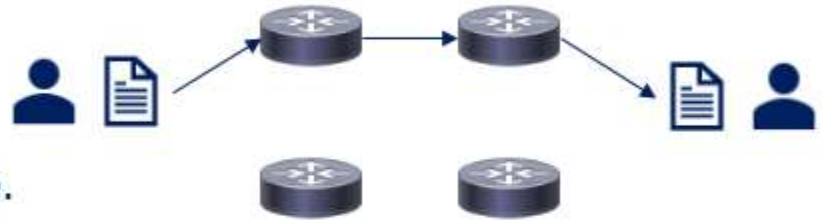
- **Assessment and test strategies.**
  - **Vulnerability scanning/testing:**
    - A vulnerability scanner tool is used to scan a network or system for a list of predefined vulnerabilities such as system misconfiguration, outdated software, or a lack of patching.
    - It is very important to understand the output from a vulnerability scan, they can be 100's of pages for some systems, and how do the vulnerabilities map to Threats and Risks (Risk = Threat x Vulnerability).
    - When we understand the true Risk, we can then plan our mitigation.
    - Common vulnerability scanners could be Nessus or OpenVAS, both list vulnerabilities in Critical, High, Medium, Low, and Informational.

- **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.

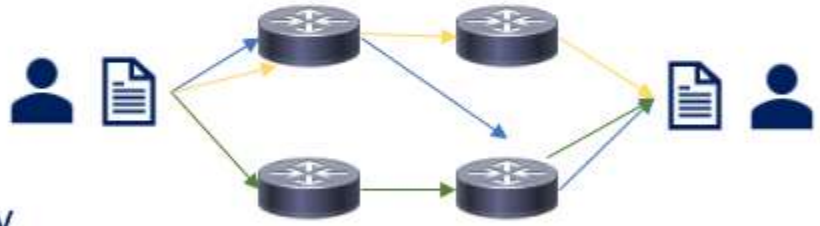
    - The **Internet** is a global collection of peered WAN networks, it really is a patchwork of ISP's.
    - An **Intranet** is an organization's privately owned network, most larger organizations have them.
    - An **Extranet** is a connection between private Intranets, often connecting business partners' Intranets.

- **Network basics and definitions:**
  - **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.

Circuit switching network

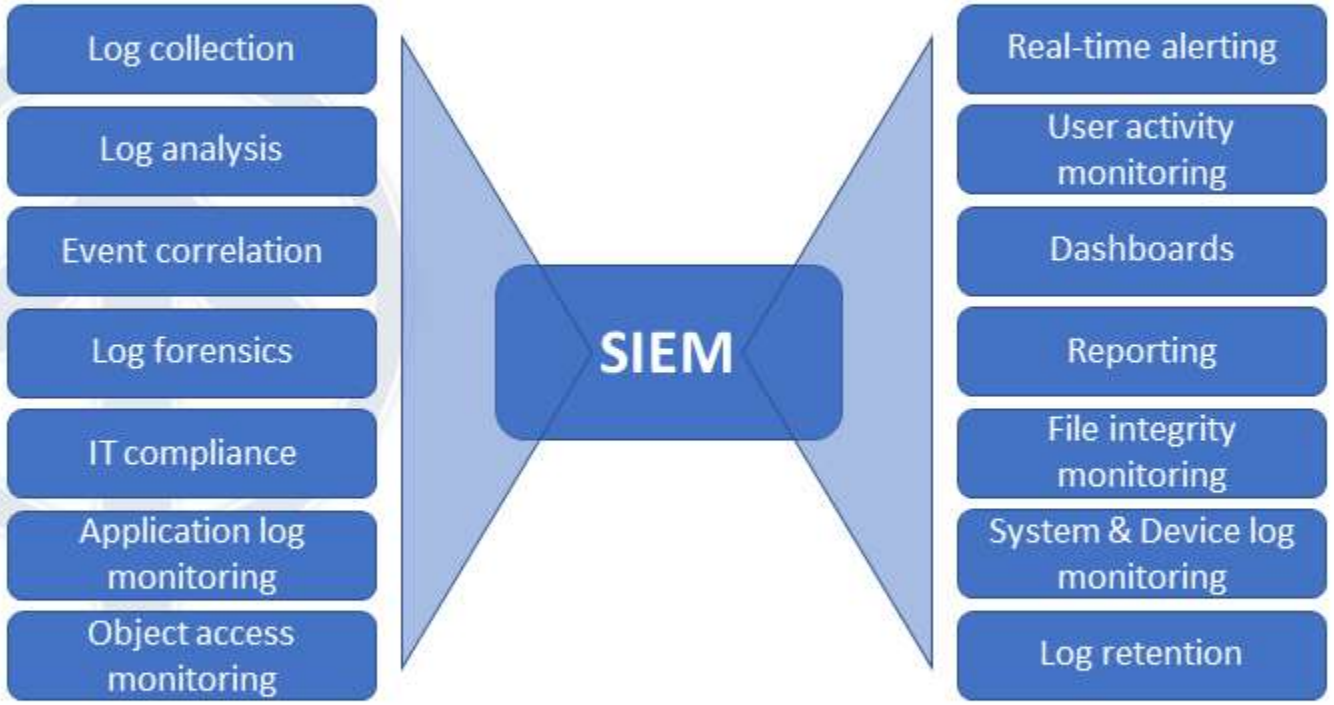


Packet switching network

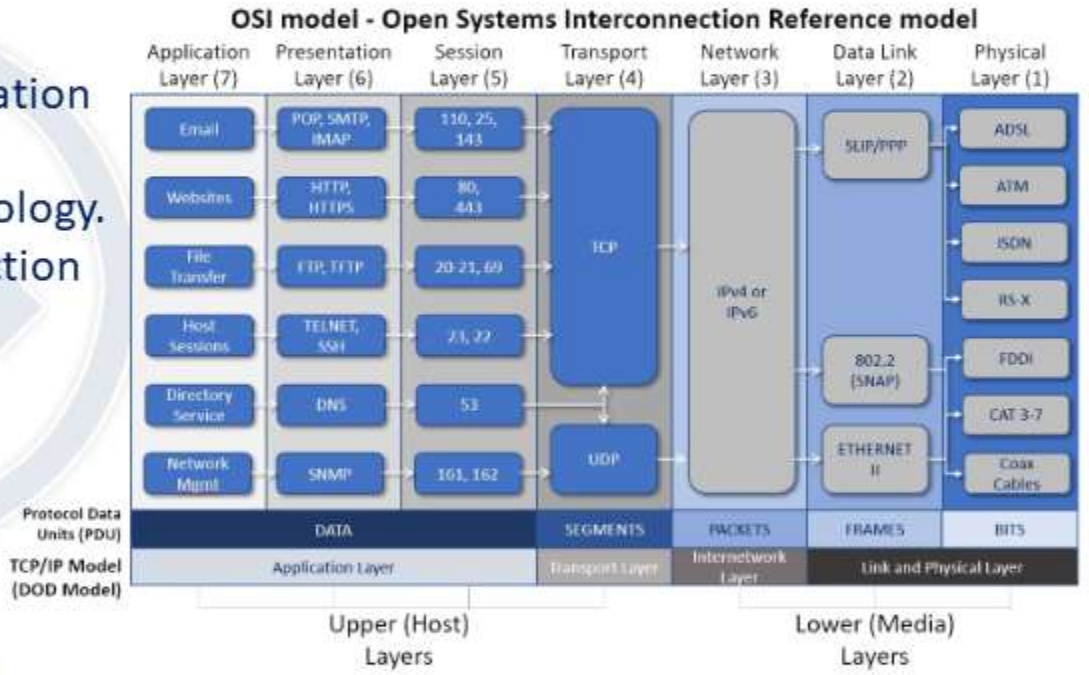


- **Network basics and definitions:**
  - **PAN** (Personal Area Network) - A personal area network is a computer network used for communication among computer and other information technological devices close to one person (PCs, printers, scanners, consoles …).
    - Can include wired (USB and FireWire) 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.

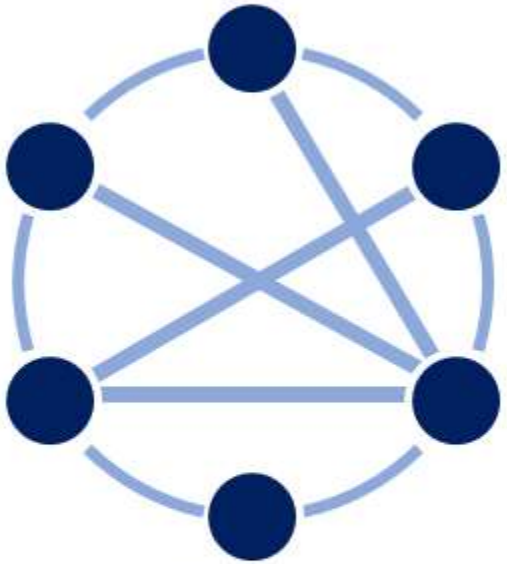
- **Preventive and Detective Controls:**
  - **Intrusion events and masking:**
    - **SIEM** (Security information and event management), often pronounced SEM or SIM.
      - Provides a holistic view of our organization's events and incidents.
      - Gathers from all our systems and looks at everything
      - Centralizes the storage and interpretation of logs, traffic and allows near real-time automated identification, analysis and recovery of security events.



- **Definitions:**
  - **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 All people seem to need data processing.
        - 1-7 Please do not throw sausage pizza away.
    - 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.



- **Definitions:**
  - **The OSI model:**
    - **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.



Partial Mesh topology

- **Definitions:**
  - **The OSI model:**
    - **Layer 2: Data Link Layer:**
      - Transports data between 2 nodes connected to 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.

- **Definitions:**
  - **The OSI model:**
    - **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 …

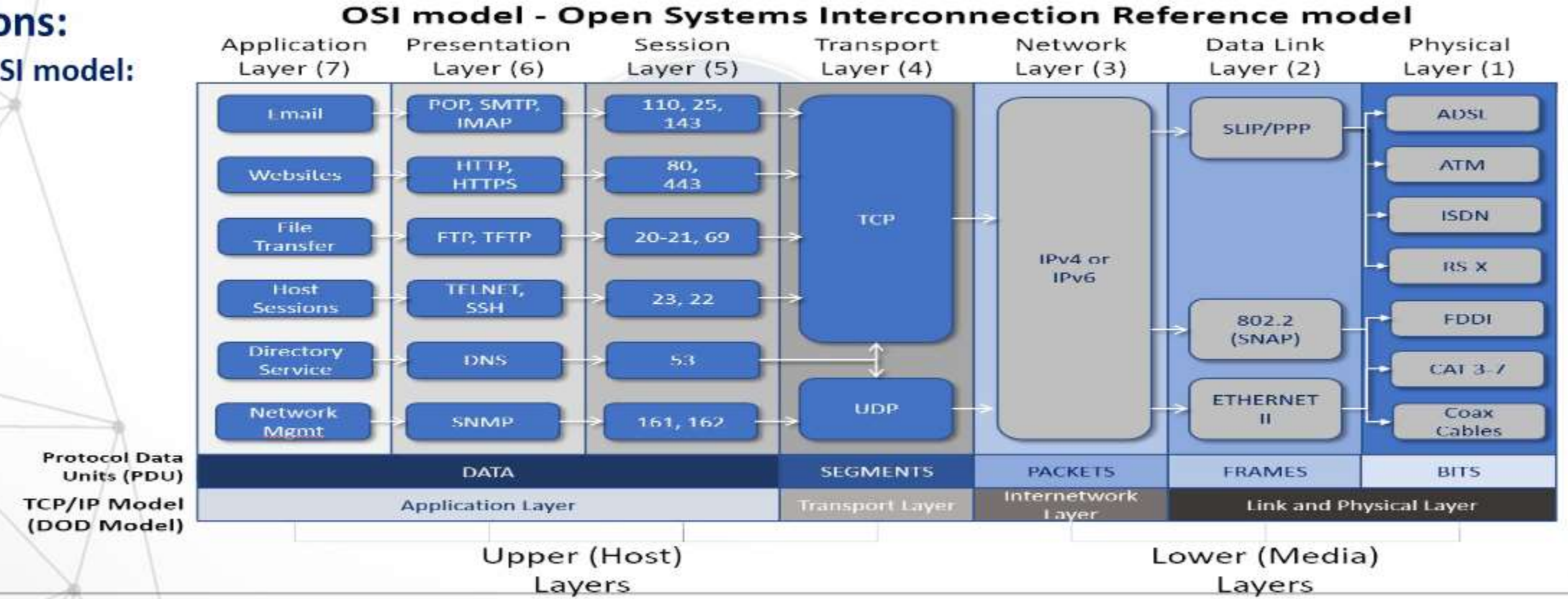
      - If the exam asks which layer a protocol with "I" is and you do not remember answer layer 3.
        - IP, IGMP, IGRP, IPSEC, IKE, ISAKMP, … are all layer 3, all except IMAP which is layer 7.

- **Definitions:**
  - **The OSI model:**
    - **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 orientated, 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.

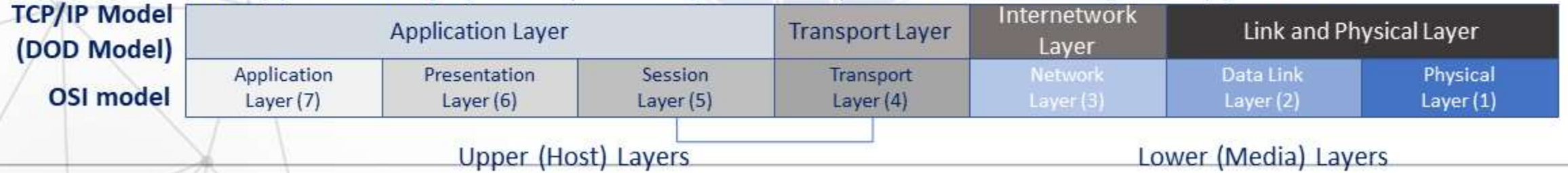
- **Definitions:**
  - **The OSI model:**
    - **Layer 4: Transport Layer:**
      - **TCP** Flags (9 bits 1-bit flags) (Control bits).
      - **NS**: ECN-nonce concealment protection.
      - **CWR** (Congestion Window Reduced) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in 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.

- **Definitions:**
  - **The OSI model:**
    - **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.

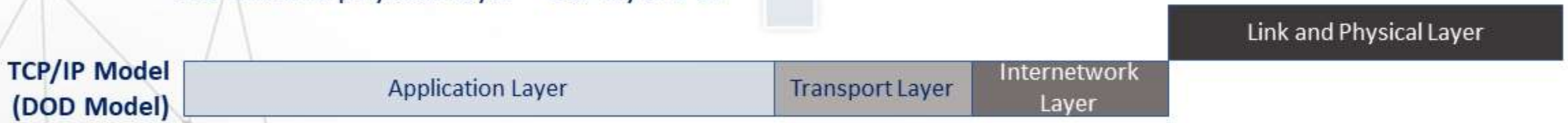
- **Definitions:**
  - **The OSI model:**



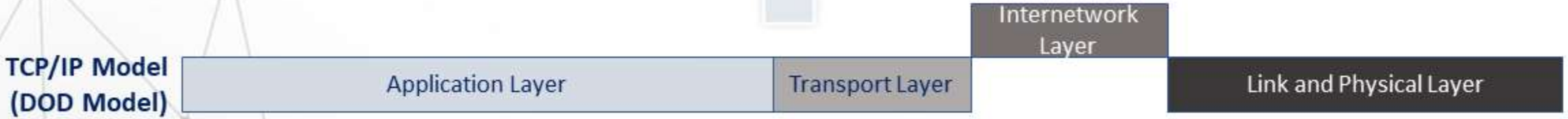
- **Definitions:**
  - **The TCP/IP Model** (Internet protocol suite):
    - A conceptual model that provides end-to-end data communication.
    - Specifying how data should be packetized, addressed, transmitted, routed and received.
    - It has four layers which are used to sort all related protocols 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.



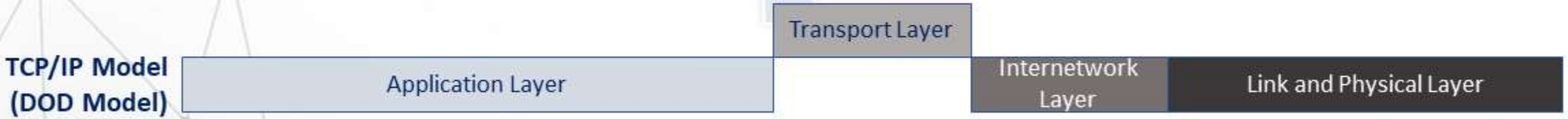
- **Definitions:**
  - **The TCP/IP Model:**
    - **The link and physical layer** has the networking scope of the local network connection to which a host is attached.
      - Used to move packets between the Internet layer interfaces of two different hosts on the same network.
      - The process of 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 transmit 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.



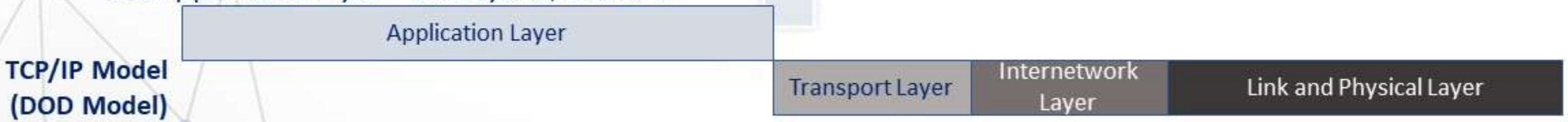
- **Definitions:**
  - **The TCP/IP Model:**
    - **Internet/Internetwork layer** is responsible for sending packets across potentially multiple networks.
      - Requires sending data from the source network to the destination network (routing)
      - The Internet Protocol performs two basic functions:
      - **Host addressing and identification:** This is done with a hierarchical IP addresses.
      - **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.



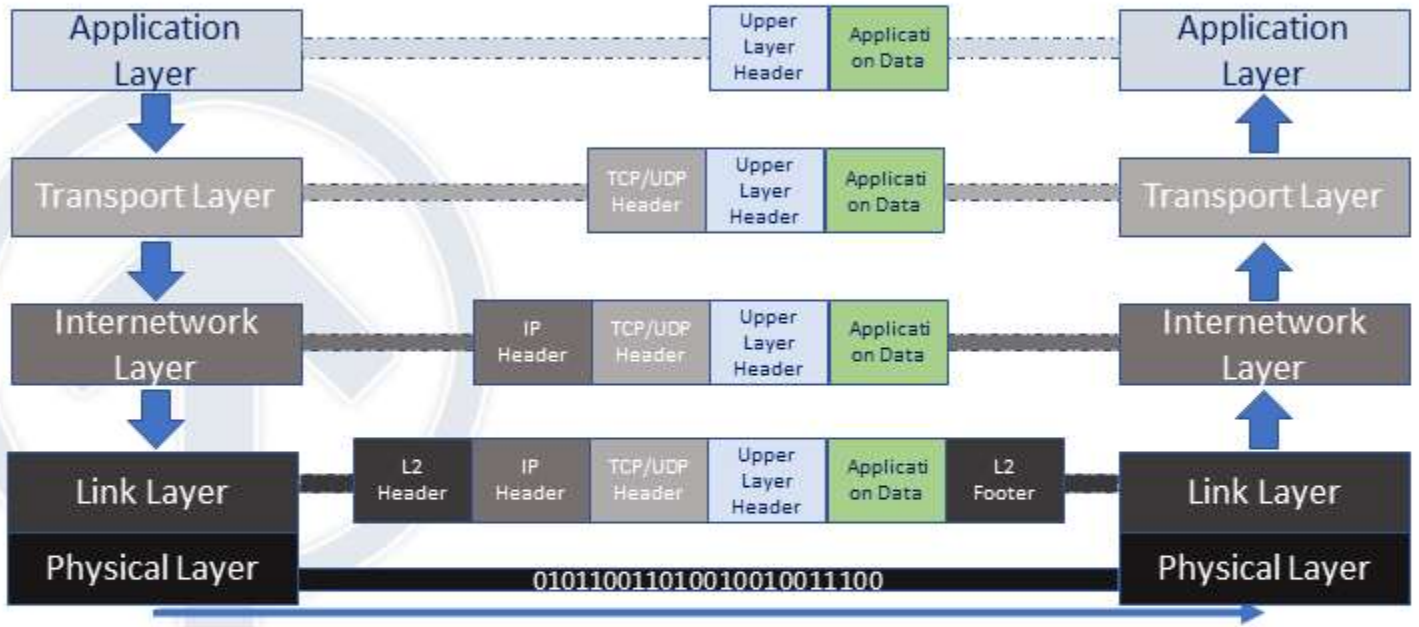
- **Definitions:**
  - **The TCP/IP Model:**
    - **The transport layer** establishes basic data channels that applications use for task-specific data exchange.
      - Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation,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



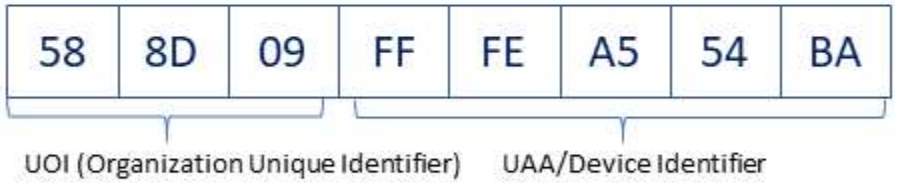
- **Definitions:**
  - **The TCP/IP Model:**
    - **The application layer** includes the protocols used by applications for providing user services or exchanging application data over the network (HTTP, FTP, SMTP, DHCP, IMAP).
    - Data coded according to application layer protocols are encapsulated 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.



- **Definitions:**
  - **The TCP/IP Model:**
    - 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 48bits (original design).
    - The first 24 are the manufacturer identifier.
    - The last 24 are unique and identify the host.
  - EUI-64 Mac Addresses use 24bit 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 64bit MAC's by adding FF:FE to the device identifier.



- **Protocols:**
  - **IPv4:**
    - 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 is currently over 8 billion mobile devices on the internet.
      - 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.

- **Protocols:**
  - **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.

- **Protocols:**
  - **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).

- **Protocols:**
  - **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.
    - **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.

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
```

- **Protocols:**
  - **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.

- **Protocols:**
  - **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 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.

- **Protocols:**
  - **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**.

172 .16 .254 . 1

10101100.00010000.11111110.00000001

1 byte = 8 bits

4 bytes = 32 bit (4x8)

Value of bit	128	64	32	16	8	4	2	1
	1	0	1	0	1	1	0	0
	128	0	32	0	8	4	0	0

172-128= 44-32= 12-8= 4-4= 0

If all bits are 0 = 0

If all bits are 1 = 255

- **Protocols:**
  - **IPv4:**
    - **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
172.16.0.0	172.31.255.255	1048576
192.168.0.0	192.168.255.255	65536

Other notable IP spaces:

127.0.0.0/8	Loopback IP's
169.254.0.0/16	Link-Local
255.255.255.255	Broadcast

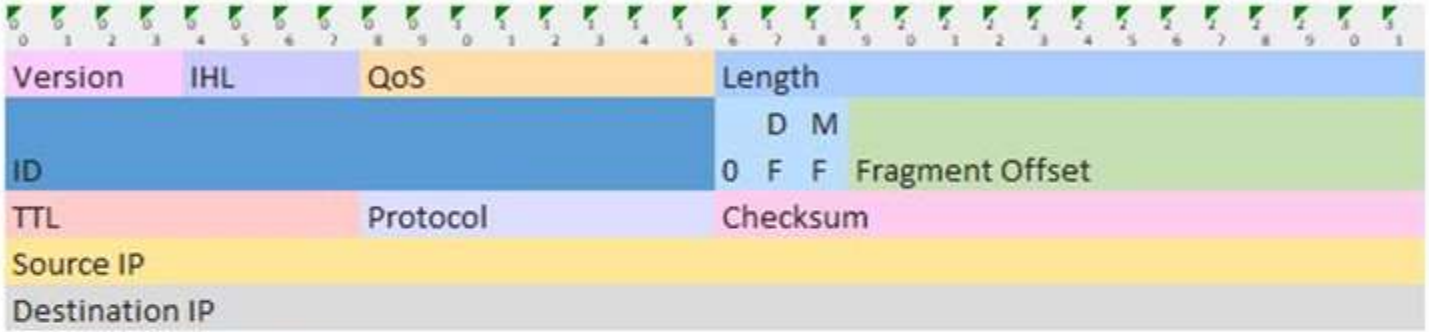
- **Protocols:**
  - **IPv4:**
    - As a band-aid solution to extend the depletion of IPv4 Addresses NAT and PAT were added:
    - **NAT** (Network Address Translation)
      - **Static NAT** Translates 1-1, we need 1 Public IP per Private IP we use, not practical and not sustainable.
      - **Pool 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 IP's.

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

- **Protocols:**
  - **IPv4:**
    - **Classful IP Networks** were used early on the internet for public address. 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 segment, 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 indicates how many IP's 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.

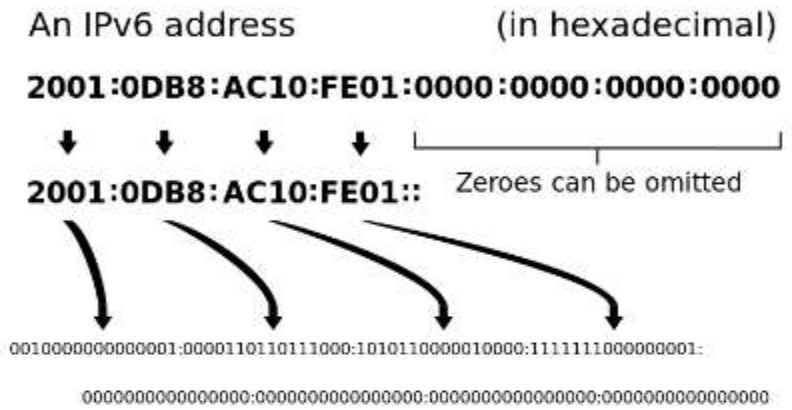
Address	Mask	How many
a.b.c.d / 32	255.255.255.255	1
a.b.c.d / 31	255.255.255.254	2
a.b.c.d / 30	255.255.255.252	4
a.b.c.d / 29	255.255.255.248	8
a.b.c.d / 28	255.255.255.240	16
a.b.c.d / 27	255.255.255.224	32
a.b.c.d / 26	255.255.255.192	64
a.b.c.d / 25	255.255.255.128	128
a.b.c.0 / 24	255.255.255.0	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

- **Protocols:**
  - **IPv4:**
    - 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.

- **Protocols:**
  - **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 extend 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::



- **Protocols:**
  - **IPv6:**
    - 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**

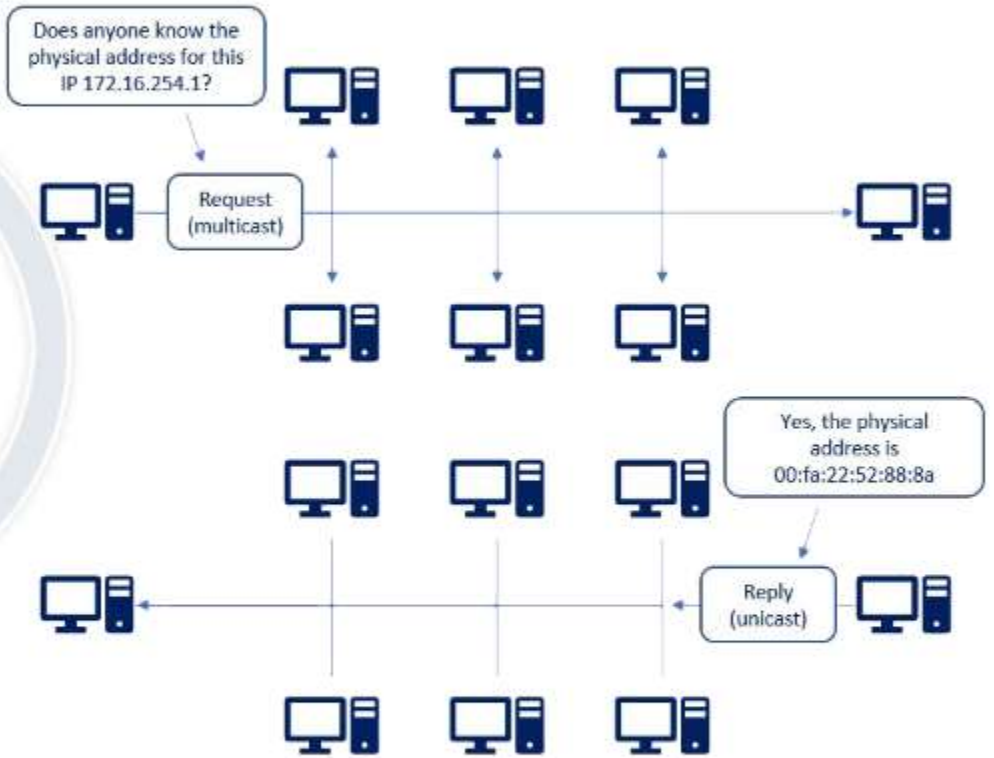
IPv6 address assigned on MAC Address

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							

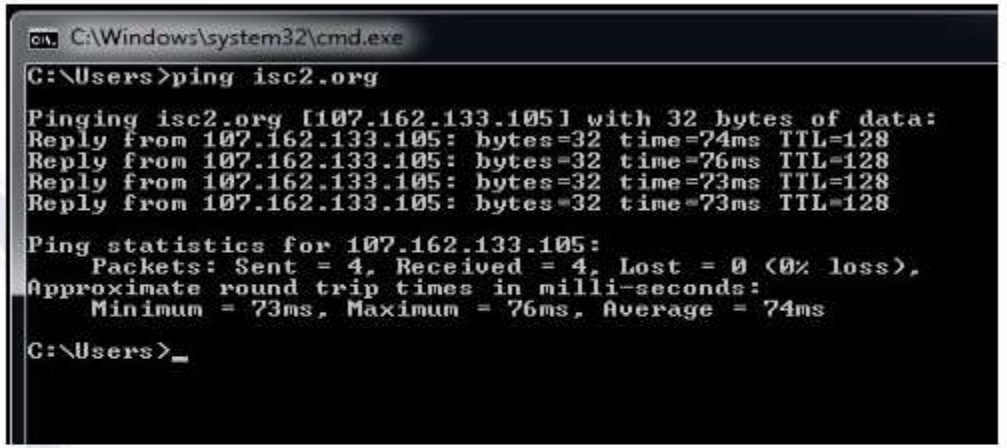
- **Protocols:**
  - **IPv6:**
    - IP Headers contain:
      - Version: IP version 6 (4 bits)
      - Traffic Class/Priority (8bits).
      - Flow Label/QoS management (20 bits).
      - Payload length in bytes(16 bits).
      - Next Header (8 bits).
      - Time To Live (TTL)/Hop Limit (8 bits).
      - 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.

- **Protocols:**
  - **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 IP's.



- **Protocols:**
  - **ICMP** (Internet Control Message Protocol):
    - Used to help 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.

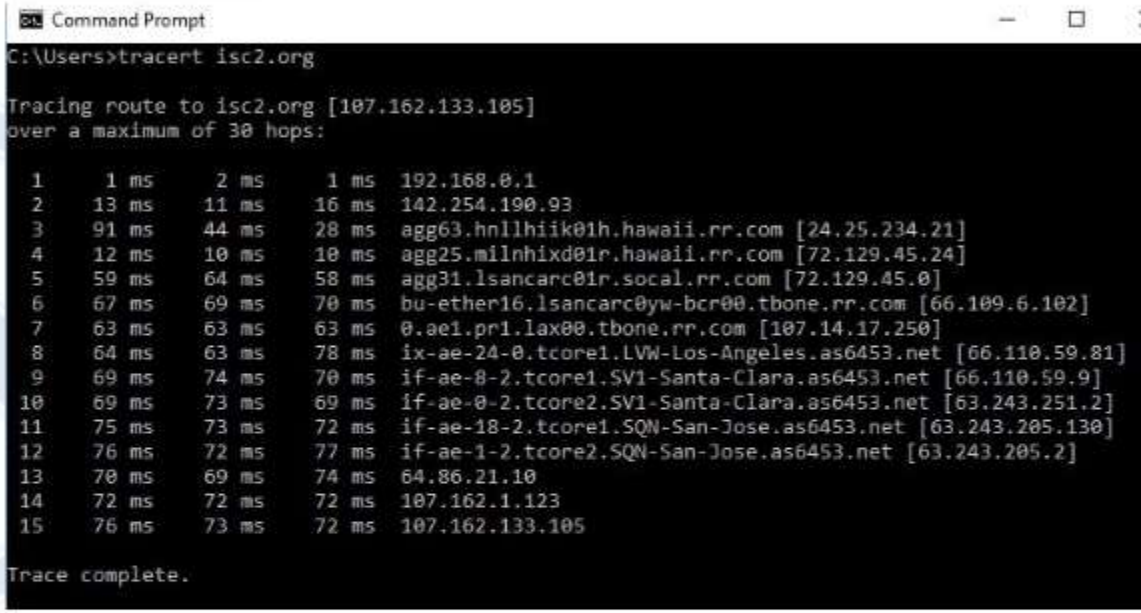


I ping isc2.org (can be name or IP if you know it).
The name is translated into the IP.
I get 4 replies from the IP, 32bytes (IPv4 ping size)
It took 73-76ms (milliseconds 1/1000th of a second)

```
Pinging google.com [2607:f8b0:4007:80a::200e] with 32 bytes of data:
Reply from 2607:f8b0:4007:80a::200e: time=56ms
Reply from 2607:f8b0:4007:80a::200e: time=56ms
```

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

- **Protocols:**
  - **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).



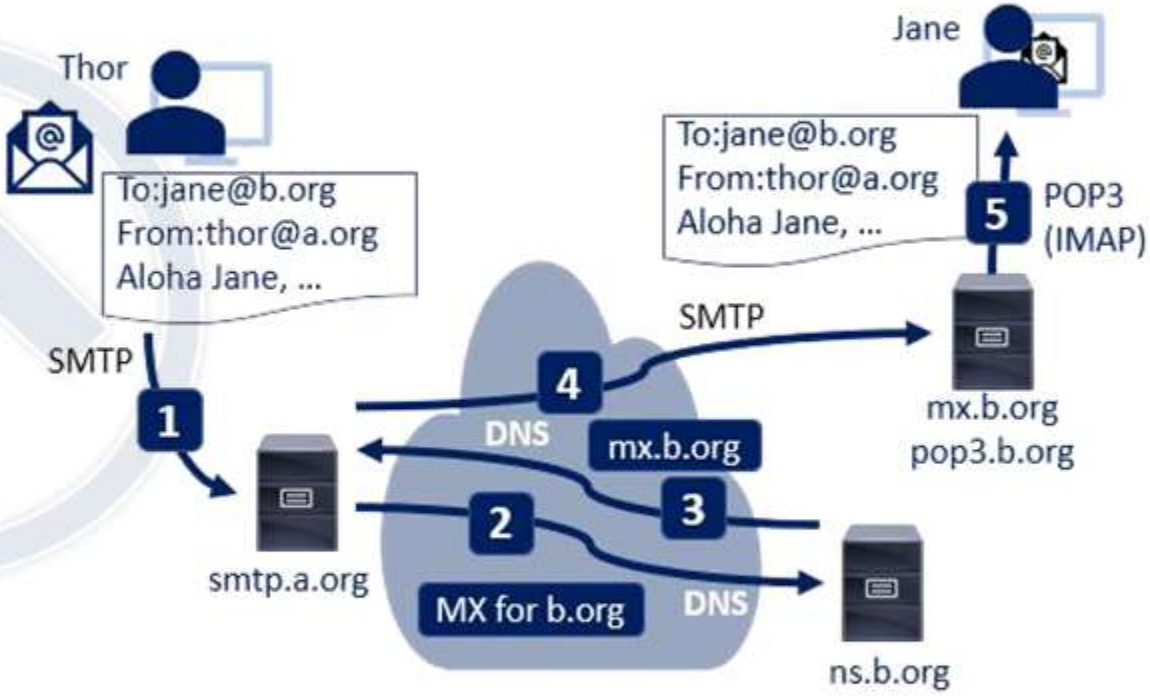
Traceroute to isc2.org (tracert on windows command line):
My local network > ISP > A few Hawaii hops > a few LA hops > 2x Santa Clara > 2x San Jose > Most likely ISC2 Firewall >
and finally the actual webserver.

- **Protocols:**
  - **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 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.

- **Protocols:**
  - **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 unsecure 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.

- **Protocols:**
  - **Email Protocols:**

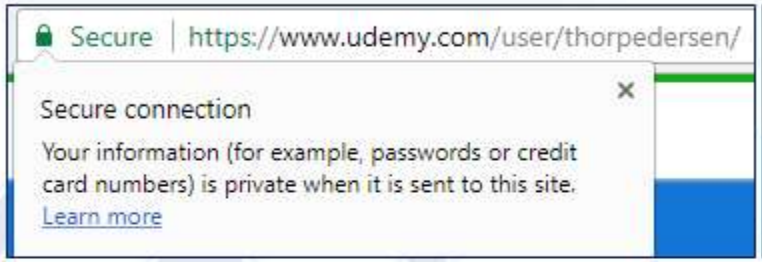
1. The MUA (Mail User Agent) formats the message and using SMTP sends the message to the MSA (Mail Submission Agent).
2. The MSA determines the destination address provided in the SMTP protocol, in this case jane@b.org. The MSA resolves the fully qualified domain name of the mail server in the DNS.
3. 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, a 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).



- **Protocols:**
  - **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 natively has no authentication. .
    - **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 a digital signature for DNS.

- **Protocols:**
  - **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.

- **Protocols:**
  - **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.



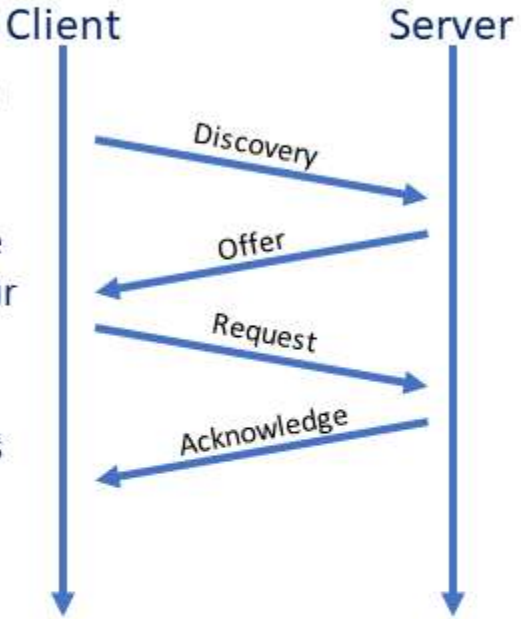
HTTPS: Connection (notice the Secure)

HTTP: Connection.

HTML: The basic building block of webpages.

- **Protocols:**
  - **BOOTP** (Bootstrap Protocol):
    - Used for diskless workstations, used to determines 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 uses UDP Port 67 for the BOOTP/DHCP Server and UDP Port 68 for the Client.

- Your device sends a DHCP discovery.
- The "server" (in the modem), offers your device an address.
- The device requests the address.
- The server acknowledges the address being assigned to the device.

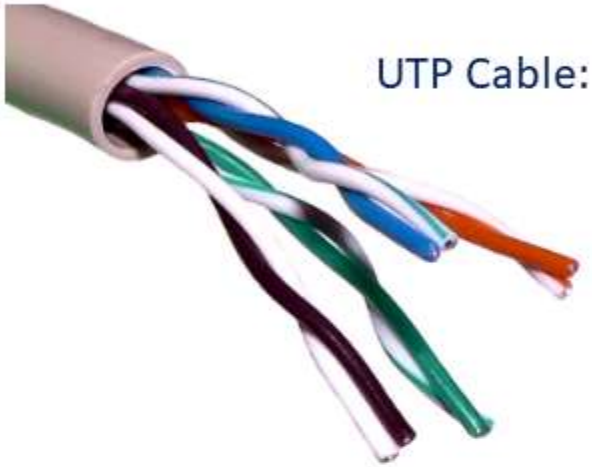


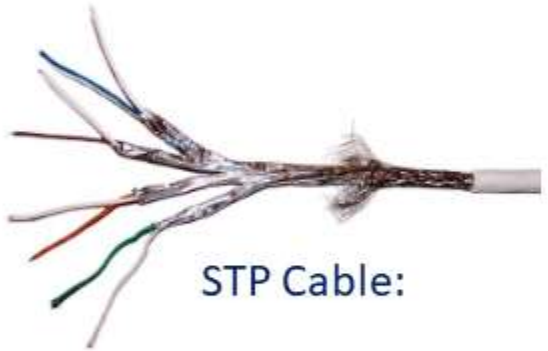
- **Cables:**
  - **Networking Cables:**
    - When it comes to networking cables, most people think RJ45 Copper Ethernet cables, many more types are used though.
    - Networking cables all come with pro's and con's, some are cheap, some more secure, some faster, ...
    - They can also pose different 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 speed you get.

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

- **Cables:**
  - **Twisted Pair Cables:**
    - **UTP** (Unshielded Twisted Pair):
    - Pairs of twisted pairs of cable.
      - Twisting them makes them less susceptible of 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 (more tight).
    - **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.

UTP Cable:





STP Cable:

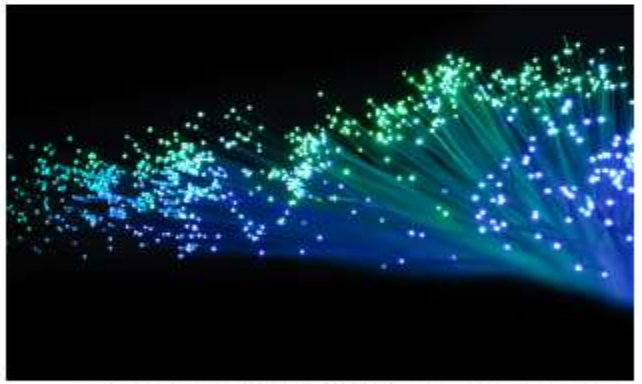
- **Cables:**
  - **Coax** (Coaxial) Cables:
    - Most commonly used for cable TV and Internet services.
    - Coax Cables have built in layers:
      - **Copper core** in the middle.
      - A **plastic insulator** around the middle core.
      - A **copper braid/shield** around the insulator.
   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

COAX Cables:

ThorTeaches.com

- **Cables:**
  - **Fiber Optic Cables** Use light to carry data (vs. electricity for copper cables)**:**
    - **Pro's:** Speed 1 Petabit per second, 35miles/50 km over a single fiber.
      - Distance 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.
    - **Con's:** 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.

- **Cables:**
  - 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

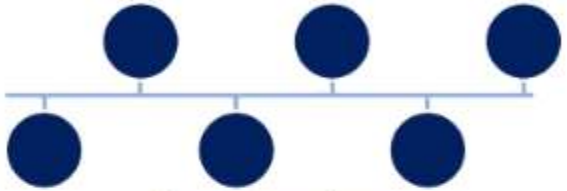
- **LAN Technologies and Protocols:**
  - Network topology describes the layout and topologies of interconnections between devices and network segments.
  - **Ethernet** and **Wi-Fi** are the two most common transmission technologies in use for local area networks.
  - At the data link layer and physical layer, a wide variety of LAN topologies have been used, including ring, bus, mesh and star.
  - At the higher layers, NetBEUI, IPX/SPX, 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, tablet 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.

- **LAN Technologies and Protocols:**
  - **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 anther work station 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.

- **LAN Technologies and Protocols:**
  - **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 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.

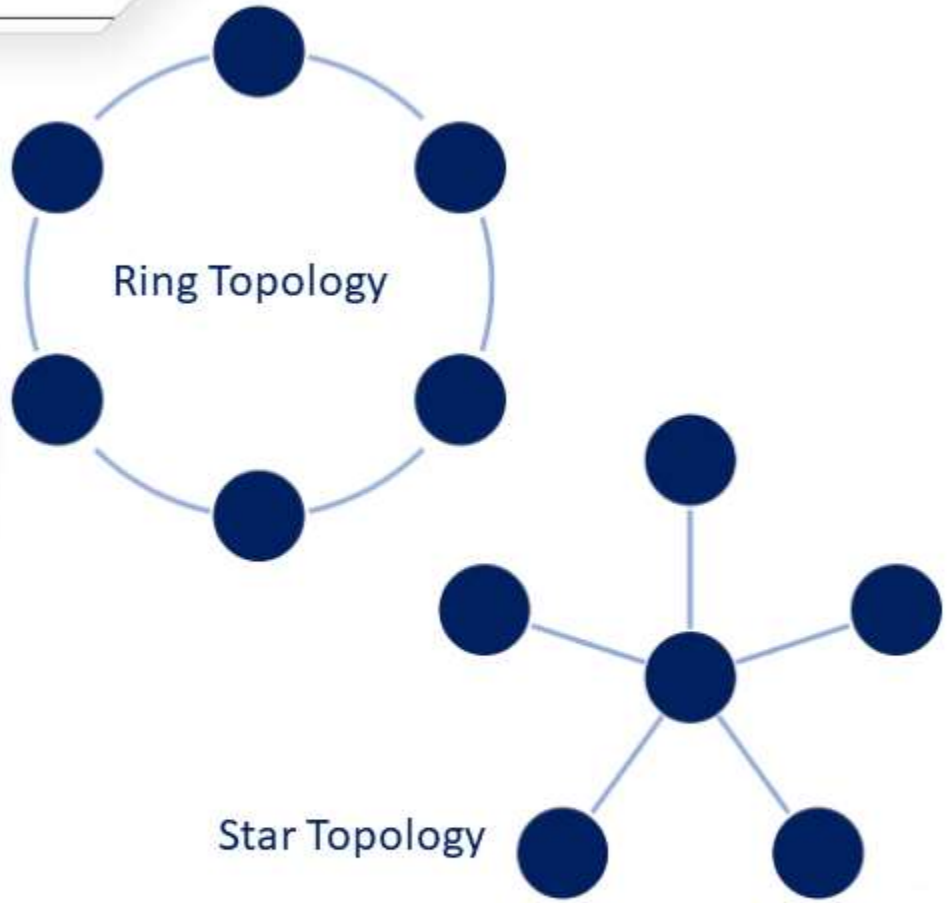


Bus Topology

Tree Topology

ThorTeaches.com

- **Physical LAN Topologies:**
  - **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.

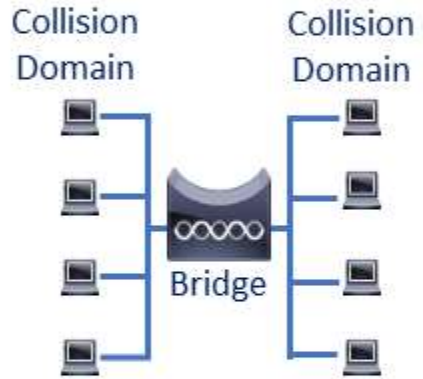


- **Physical LAN Topologies:**
  - **Mesh**:
    - Nodes are connected to each other in either a partial mesh or a full mesh.
    - **Partial Mesh**:
      - Nodes are directly connected to some other nodes.
    - **Full Mesh**:
      - All nodes are directly connected to all other nodes.
    - More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

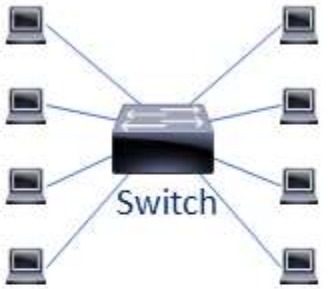
Full Mesh Topology

Partial Mesh Topology

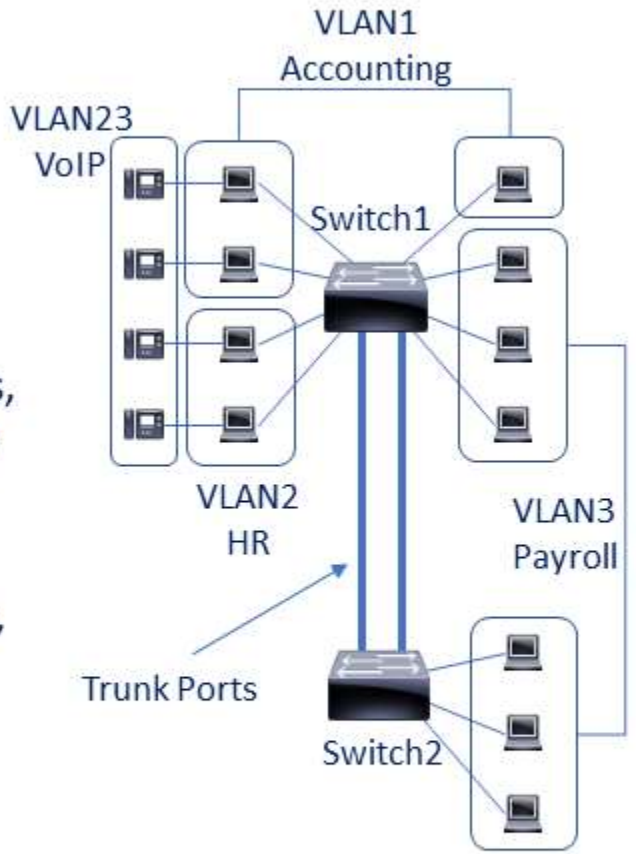
- **Secure Network Devices and Protocols:**
  - We have different network devices through the OSI and TCP/IP models and many have protocols specific to that device.
  - **Layer 1 devices:**
    - **Repeaters** receive a signal and retransmit it.
      - They are used to extend transmissions so that the 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, sends traffic across the 2 domains, but traffic from one domain is not seen on the other unless sent there.



- **Secure Network Devices and Protocols:**
  - **Layer 2 devices:**
    - **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 VLAN's.
        - 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.



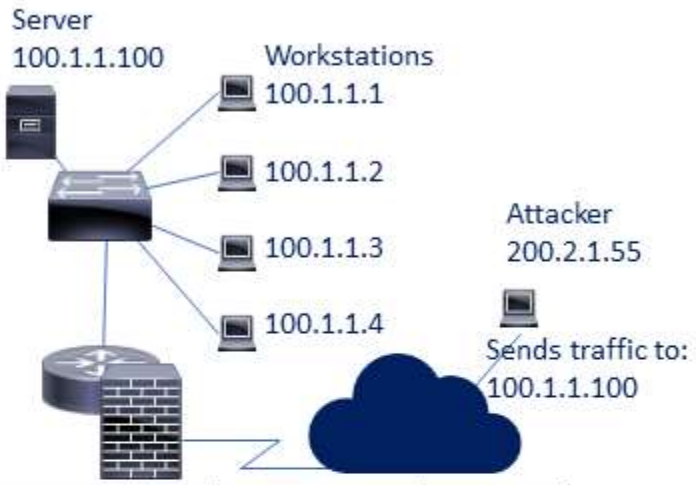
- **Secure Network Devices and Protocols:**
  - **Layer 2 Protocols:**
  - **VLAN** (Virtual LAN) is a broadcast domain that is partitioned and isolated at layer 2.
    - Specific ports on a switch are assigned to a certain VLAN.
    - The Payroll VLAN is in 2 different buildings and spans multiple switches.
    - 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 VLAN's across them.
    - VLAN's share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.



- **Secure Network Devices and Protocols:**
  - **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 IP's and ports.
      - Connecting our LAN's 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.

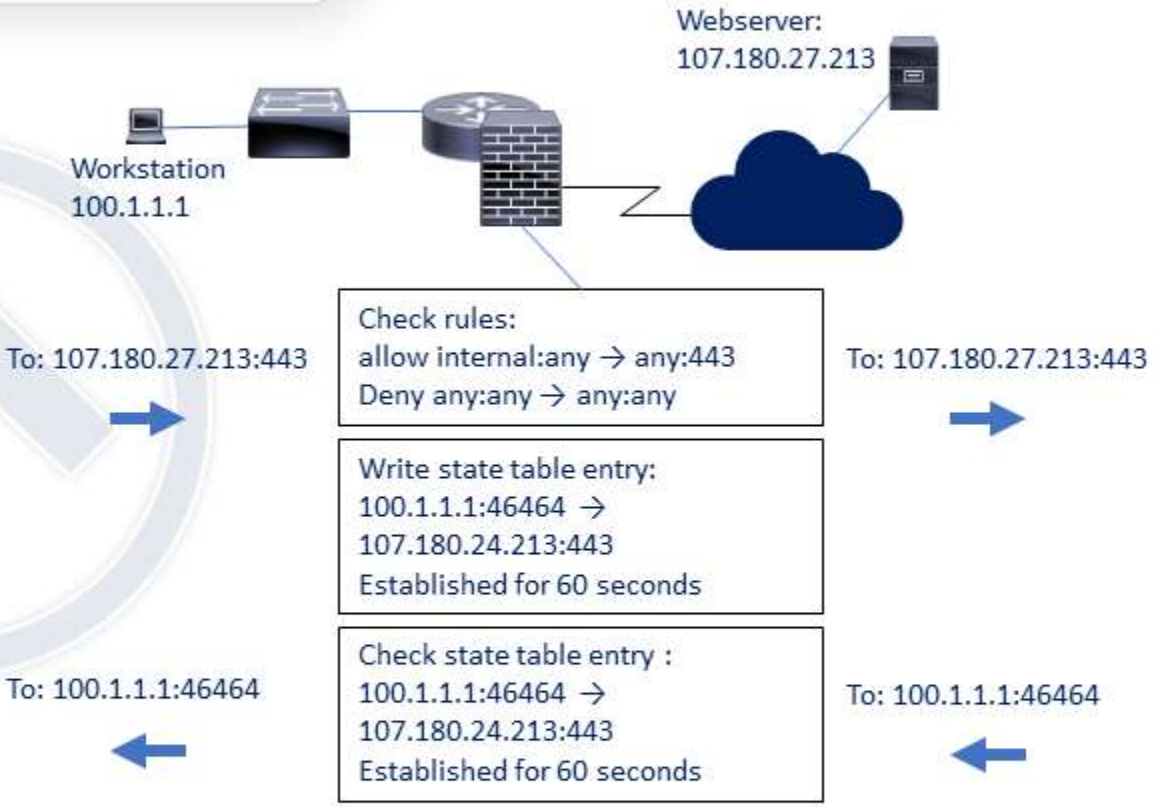
- **Secure Network Devices and Protocols:**
  - **Layer 3 devices:**
    - **Routers** have two operation planes:
      - **Control plane:**
        - A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection.
        - 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.

- **Secure Network Devices and Protocols:**
  - **Firewalls:** A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, like the Internet.
    - **First generation: 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 IP's are whitelisted in the first rule.

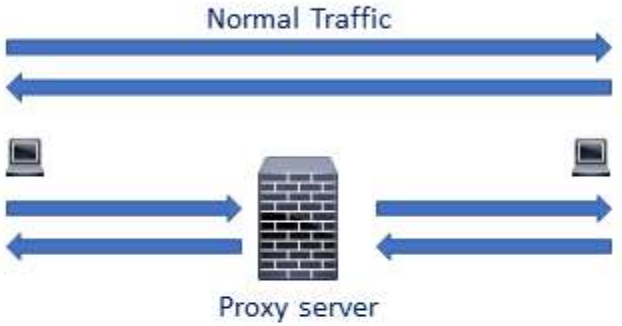


Source	Destination	Action
100.1.1.0/24	100.1.1.0/24	Permit
100.1.1.0/24	Any	Permit
Any	100.1.1.100	Deny
Any	Any	Deny

- **Secure Network Devices and Protocols:**
  - **Firewalls:**
    - **Second generation: 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.



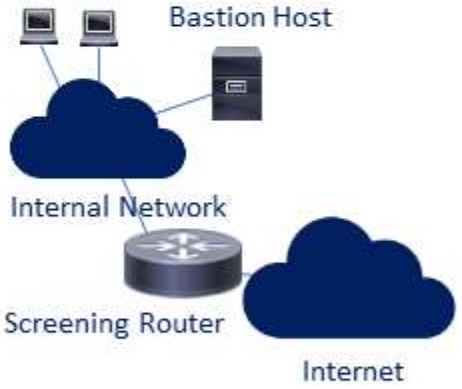
- **Secure Network Devices and Protocols:**
  - **Firewalls:**
    - **A proxy server** can act as a firewall by responding to input packets in the manner of an application, while blocking other packets.
    - A proxy server is a gateway from one network to another for a specific network application,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



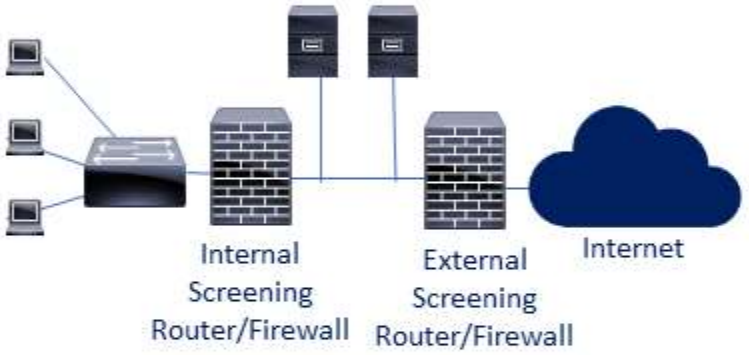
- **Secure Network Devices and Protocols:**
  - **Firewalls:**
    - **Third generation: Application layer firewalls**, OSI Layer 7.
      - The key benefit of application layer firewalls is that they can understand certain applications and protocols.
      - They see the entire packet, the packet isn't 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 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.

- **Secure Network Devices and Protocols:**
  - **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 pre modern firewalls.

- **Secure Network Devices and Protocols:**
  - **Firewalls design:**
    - **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.



- **Secure Network Devices and Protocols:**
  - **Firewalls design:**
    - **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.
      - 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.



Screened Subnet using Dual Firewall DMZ

- **Secure Network Devices and Protocols:**
  - **Firewalls design:**
    - **DMZ's:**
      - Normal DMZ's use 2 firewalls in a screened subnet, but they can also be three-legged DMZ's 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.
    - 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.

3-legged DMZ

Firewall pair

- **Preventive and Detective Controls:**
  - **IDS's and IPS's.**
    - We use both IDS's (Intrusion Detection Systems) and IPS's (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 (Behavioral) based**, 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.

- **Preventive and Detective Controls:**
  - **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 noticed.
  - **IPS** (Intrusion Prevention System):
    - Similar to IDS, but they also take action to 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.

- **Preventive and Detective Controls:**
  - **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, IP's, 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 doesn't have to be the entire system we monitor.
    - If we do chose 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.

- **Preventive and Detective Controls:**
  - **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 (Behavioral) based:**
    - 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.

- **Preventive and Detective Controls:**
  - **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.

- **Preventive and Detective Controls:**
  - **Intrusion events and masking:**
    - **Alerts on IDS's/IPS's 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.

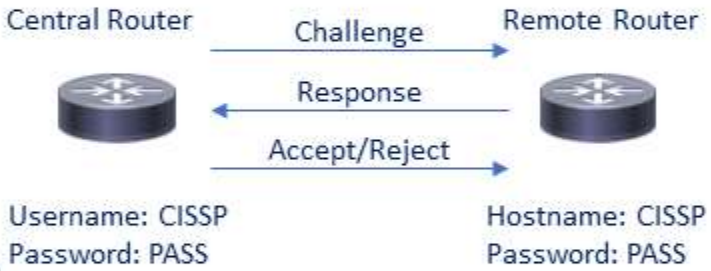
      - We rarely talk about the "true" states since things are happening like they are supposed to, we are interested in when it doesn't and we prevent authorized traffic or allow malicious traffic.

- **Asset Management:**
  - **0-day vulnerabilities:**
    - Vulnerabilities not generally known or discovered, the first time an attack is seen is considered day 0, hence the name.
    - From when a vulnerability is discovered it is now only a short timespan before patches or signatures are released on major software.
    - With millions of lines of code in a lot of software and the 1% errors we talked about there will always be new attack surfaces and vulnerabilities to discover. The only real defense against the 0 day exploits is defense in depth and when discovered immediate patching as soon as it is available and we have tested it in our test environments. Most signatures in IDS/IPS and anti virus auto update as soon as new signatures are available.
    - **0-day vulnerability:** The vulnerability that has not been widely discovered and published.
    - **0-day exploit:** Code that uses the 0-day vulnerability.

- **Asset Management:**
  - **0-day vulnerabilities:**
    - The Stuxnet worm that targeted Iran's nuclear centrifuges used 4 unique 0 day exploits (previously unheard of).
    - It was developed over 5+ years and estimated to have cost 100's of millions of dollars.
    - **Stuxnet has three modules:**
      - A **worm** that executes all routines related to the main payload of the attack;
      - A **link** file that automatically executes the propagated copies of the worm.
      - A **rootkit** responsible for hiding all malicious files and processes, preventing detection of Stuxnet.
    - It is introduced to the target environment by an infected USB flash drive.
    - The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC, If both are not present, Stuxnet becomes dormant inside the computer, it will still replicate the worm.
    - If both are present, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

- **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 client/user by sending 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.

- **Secure Communications:**
  - **Authentication protocols:**
  - **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.



- **Secure Communications:**
  - **Authentication protocols:**
    - **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.

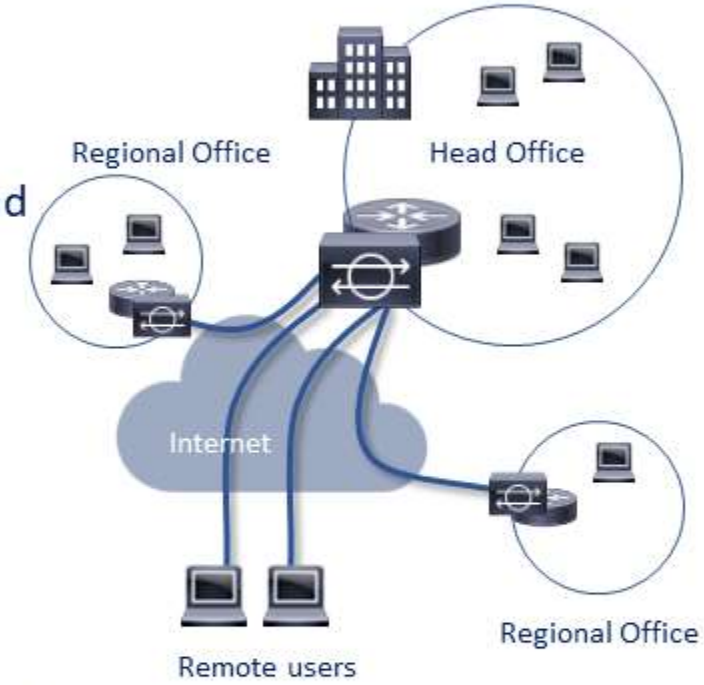
      - The **authenticator** is a network device, a switch or wireless AP.
      - The **AS** (Authentication sever) is typically a host running software supporting the RADIUS and EAP protocols.
      - In some cases, the authentication server software may be running on the authenticator hardware.
      - 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.

- **Secure Communications:**
  - **Authentication protocols:**
    - **PEAP** (Protected EAP):
      - A protocol that encapsulates EAP within a 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.

- **Secure Communications:**
  - **Authentication protocols:**
    - **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.

- **Secure Communications:**
  - **Authentication 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.

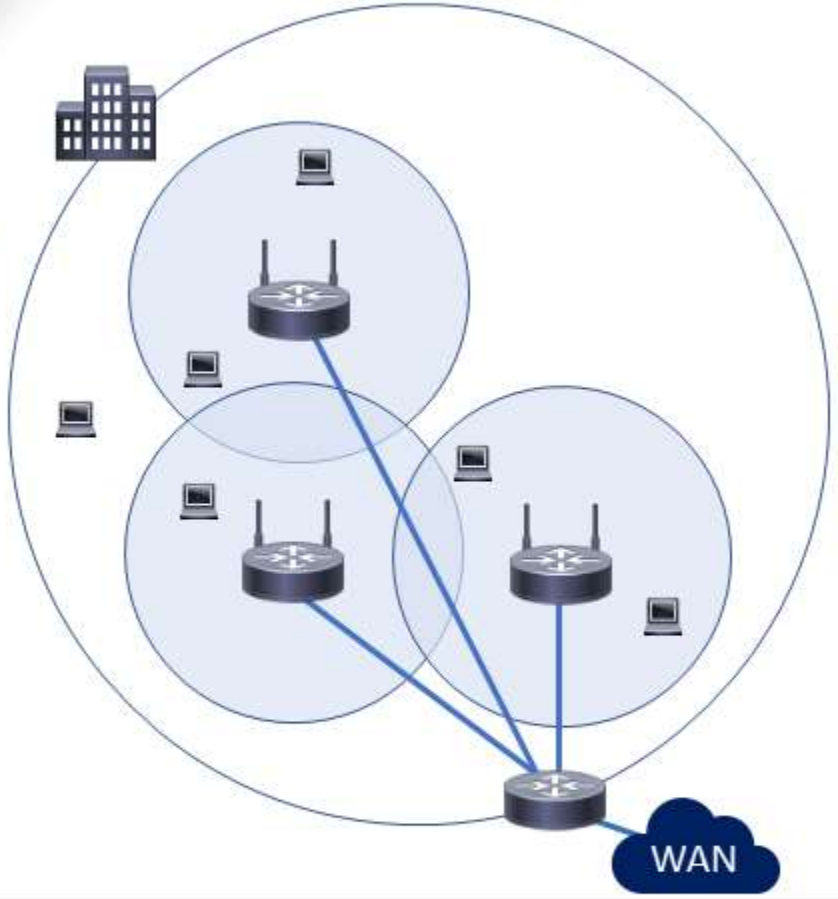
- **Secure Communications:**
  - **Authentication protocols:**
    - **VPN** (Virtual Private Network):
      - Extends a private network across a public network, and users can send and receive data across shared or public networks as if they were on the private network.
      - VPNs may allow employees 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.



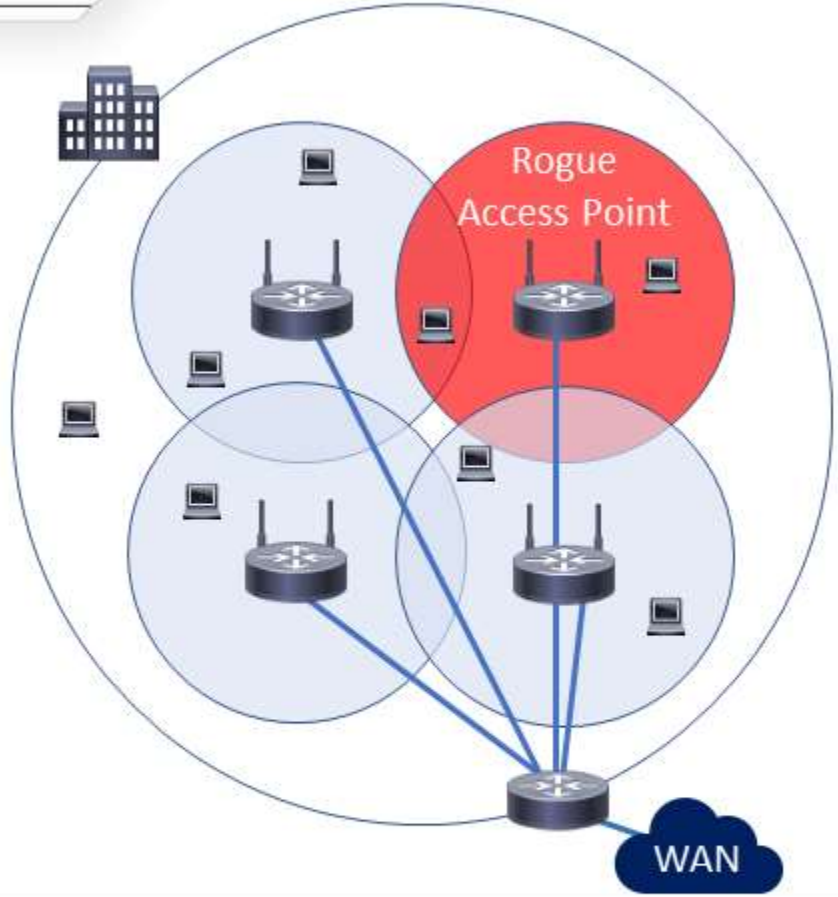
- **Secure Communications:**
  - **Authentication protocols:**
    - **PPTP** (Point-to-Point Tunneling Protocol):
      - Obsolete method for implementing virtual private networks, because of many known security issues.
      - PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets.
      - 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 AP's (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.

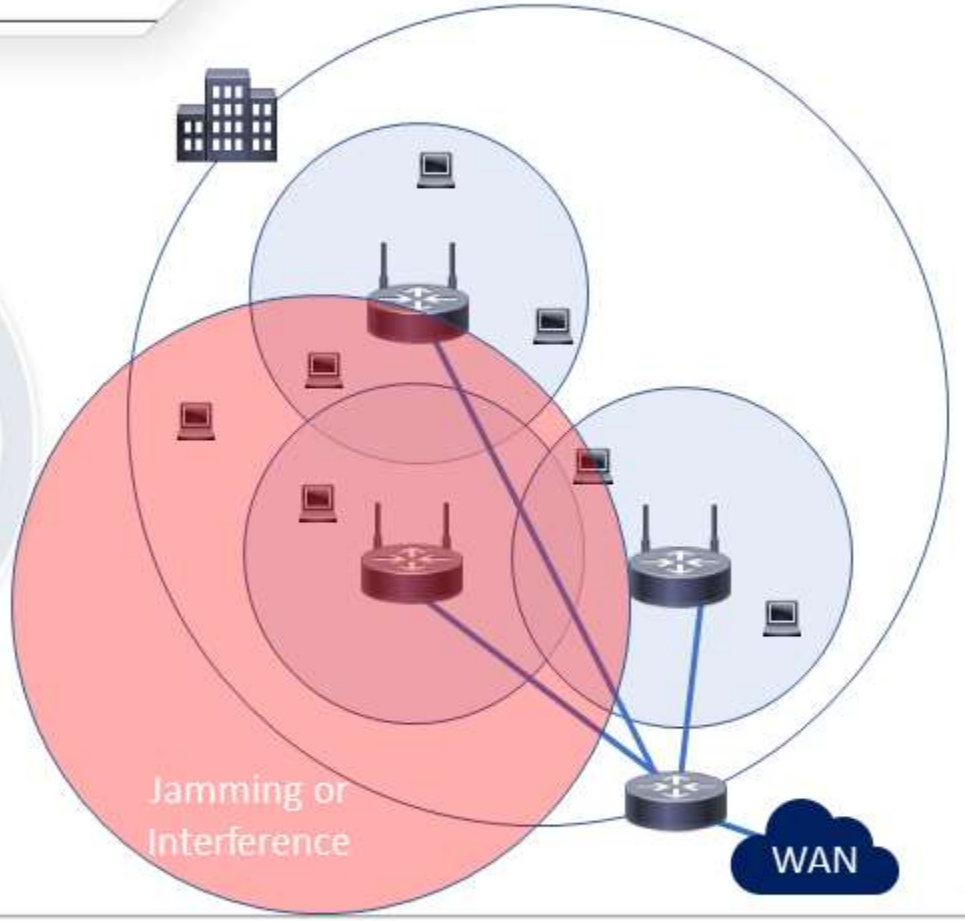
  - Wi-Fi makes us more mobile and our connection more seamless, but it is easier to compromise than cabled internet connection.



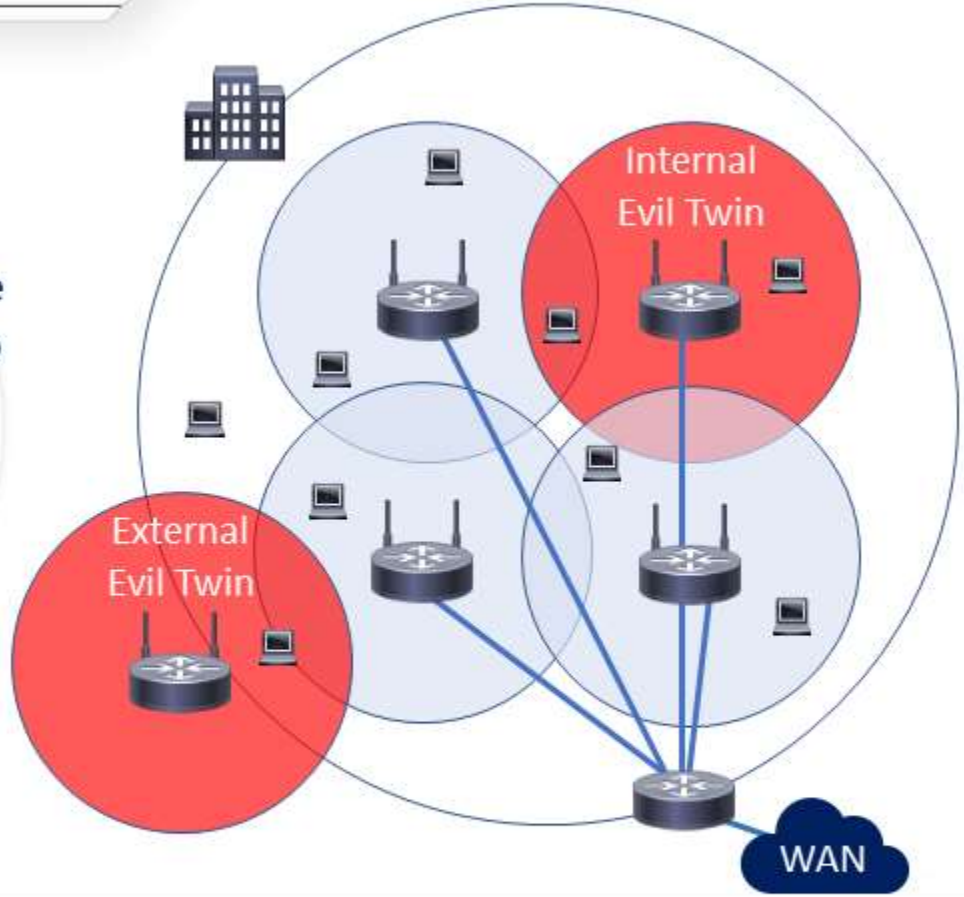
- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **Wi-Fi attacks:**
    - **Rogue access points:**
      - An unauthorized access point that has been added to our network without our knowledge.
      - This can be malicious by an attacker or just an employee wanting Wi-Fi somewhere with bad 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.



- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **Wi-Fi attacks:**
    - **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.



- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **Wi-Fi attacks:**
    - **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.

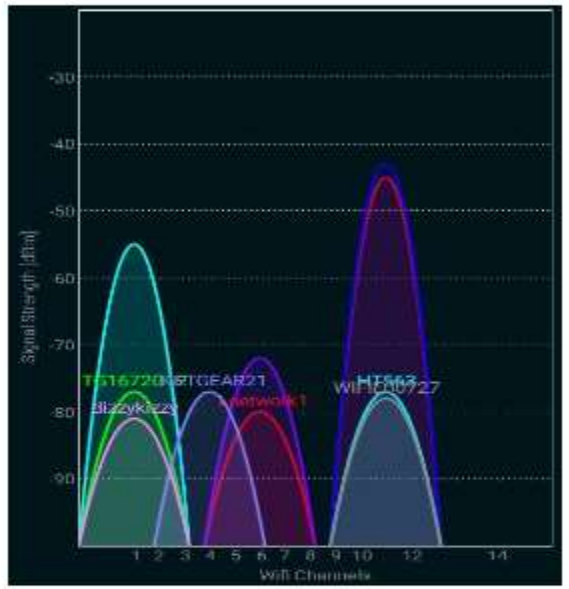


- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **802.11 standards:**
    - The 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing WLAN computer communication in the 2.4, 3.7 and 5 GHz frequency bands.
    - There are more 802.11 protocols but for the exam know these.

802.11 network PHY standards

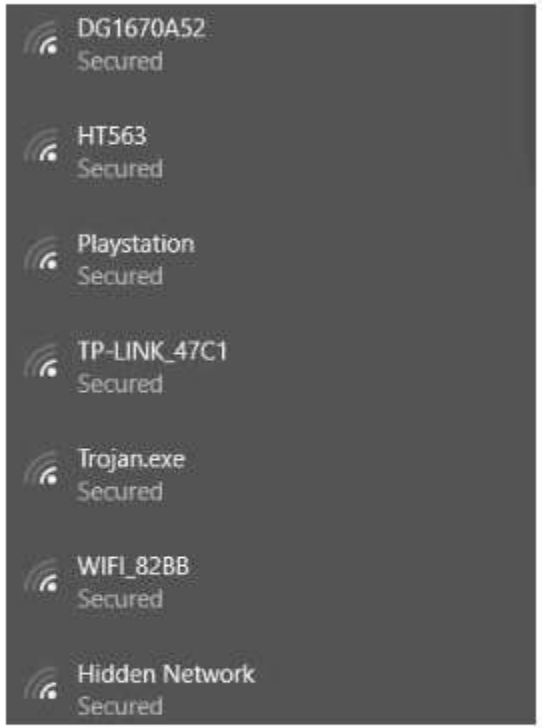
802.11 protocol	Release date:	Frequency (GHz)	Bandwidth (MHz)	Stream Data Rate (Mbit/s)	Approximate Range (Indoors):	Approximate Range (Outdoors):
802.11-1997	6/1/1997	2.4	22	1, 2	20 m (66 ft)	100 m (330 ft)
a	9/1/1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	35 m (115 ft)	120 m (390 ft)
		3.7				5,000 m (16,000 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	Up to 72.2	70 m (230 ft)	250 m (820 ft)
			40	Up to 150		
ac	12/1/2013	5	20	Up to 96.3	35 m (115 ft)	
			40	Up to 200		
			80	Up to 433.3		
			160	Up to 866.7		

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **802.11 standards:**
    - 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.
    - 5 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 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.



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

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **802.11 wireless NIC's:**
    - **Operate in four different modes:**
      - **Managed/Client mode:**
        - 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.
      - **Master/infrastructure mode:**
        - The mode used by wireless access points.
        - A wireless card in master mode can only communicate with connected clients in managed mode.
        - Access point must have 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.



- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **802.11 wireless NIC's:**
    - **Operate in four different modes** (continued):
      - **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.

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **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.
    - SSID's 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 WLAN's, it is easy to sniff and spoof.

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **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 40bit 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 timestamp and have no replay protection, attackers can inject traffic by replaying previously sniffed WEP frames.

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **WPA** (Wi-Fi Protected Access): (2003)
    - Interim standard to address WEP issues. should not be used unless WPA2 is not feasible.
    - 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 preventing 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):
    - Current standard, should be used, 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).

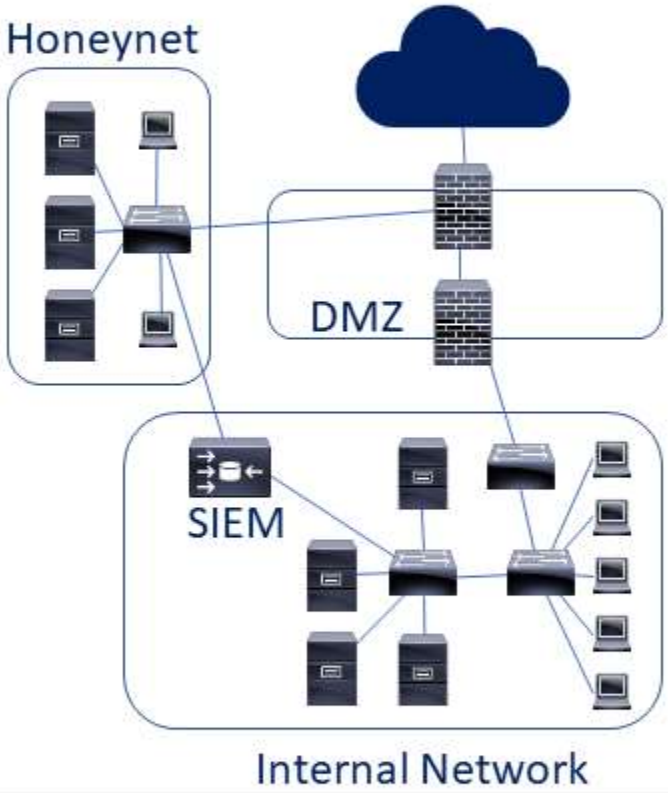
- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **Bluetooth:**
    - A wireless technology standard for exchanging data over short distances using 2.4 GHz from fixed and mobile devices, and building personal area networks (PANs).
    - Bluetooth has three classes of devices, while designed 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.

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **Bluetooth**
    - 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.

- **WLAN (Wireless LAN) Technologies and Protocols:**
  - **Bluetooth**
    - **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 OS's, newer smartphones constantly update their OS.
    - **Countermeasures:**
      - Enable Bluetooth only when you needed 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.

- **Preventive and Detective Controls:**
  - **Honey pots and Honey nets:**
    - **Honeynets:**
    - A network (real or simulated) of honeypots, can be a full server farm simulated with applications, OS's and fake data.
    - Best practice segments the honeynet from our actual network by a DMZ/firewall.
    - The SIEM collects the data from our internal systems as well as the honeynet.



- **Secure Communications:**
  - **IPSec:**
    - **SA** (Security Association): Simplex one-way communication, can be used to negotiate ESP or AH parameters.
      - If 2 systems use ESP to communicate they need 1 SA for each direction (2 total), if SA 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 ITSEC.
    - **IKE** (Internet Key Exchange):
      - IPsec can use different types of encryption (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

- **Secure Communications:**
  - **IPSec:**
    - 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 servers 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 (common), used for securing web traffic (less common).

- **Secure Communications:**
  - **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 commonly 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.

- **Secure Communications:**
  - **Callback** is a modem-based authentication system.
    - Was mostly used for securing dial-up connections.
    - The client computer calls the server computer.
    - After a greeting the client identifies itself, usually with a user name.
    - The server disconnects the call.
    - Depending on the user 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 pick their caller ID.

- **Secure Communications:**
  - **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 OS' (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 or support.me.

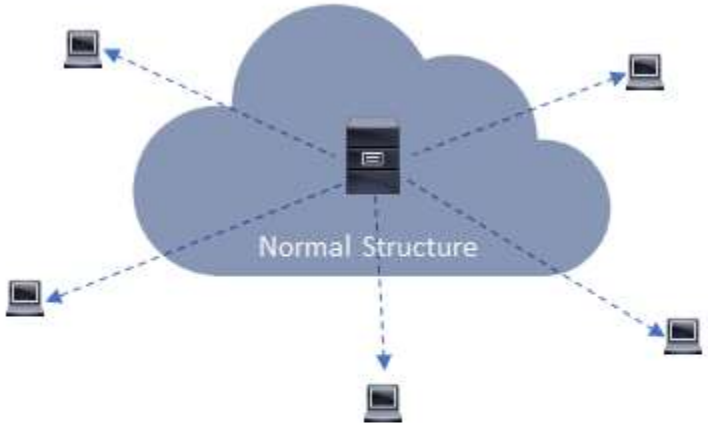
- **Secure Communications:**
  - **VDI** (Virtualized Desktop Infrastructure/Interface):
    - **Thin Clients:**
      - Diskless Workstation (Diskless node) has all the normal hardware/firmware except the disk, it has the lower level OS (the BIOS), which performs the POST and it then downloads the kernel 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, ...

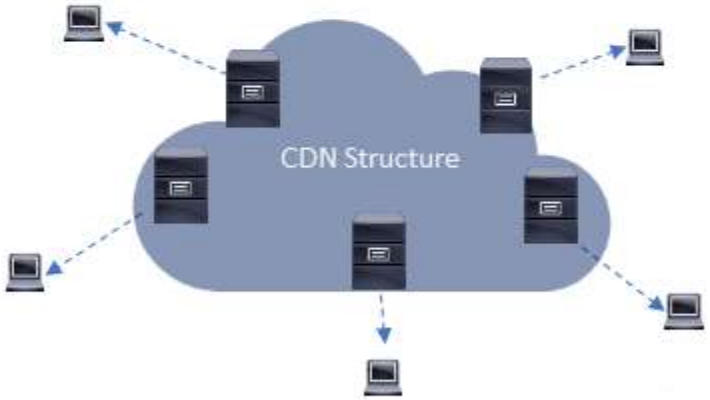
- **Secure Communications:**
  - **IM (Instant messaging):**
    - Short messages are typically sent between two parties (one-to-one) or many to many (group IM's).
    - Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are 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, Twitter, Google+, or WhatsApp.
    - Many IM applications and protocols are not designed with security in mind, they are designed for usability.
      - A 2014 report on the level of safety offered by instant messengers only 7 out of 39 instant messengers received a perfect score, and the most popular instant messengers scored 2 out of 7.
      - 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.

- **Secure Communications:**
  - **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, GoToMeeting, Google Hangouts, 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 IM's.
    - 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.

- **Secure Communications:**
  - **WAP** (Wireless Application Protocol):
    - Used for accessing information over a mobile wireless network.
    - A WAP browser is a web browser for mobile devices like mobile phones, it is a micro browser, does not have full browser functionality, but also uses less resources.
    - The browser accesses sites written in WML (Wireless Markup Language), based on XML.
    - Widely used in the early 2000's, but has mostly been replaced with newer standards and protocols.
    - Most mobile devices now fully support HTML, and WAP is not really needed anymore.

- **Secure Communications:**
  - **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 is 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 CDN's : 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.





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 don't know any better, didn't think about it or figured they wouldn't 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 Black/White list, Storage Segmentation, Remote Access Revocation, Configuration Pushes, Backups.
    - More controversial: Track the location of employees, monitor their data traffic and calls.

Mobile Security:

- 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?

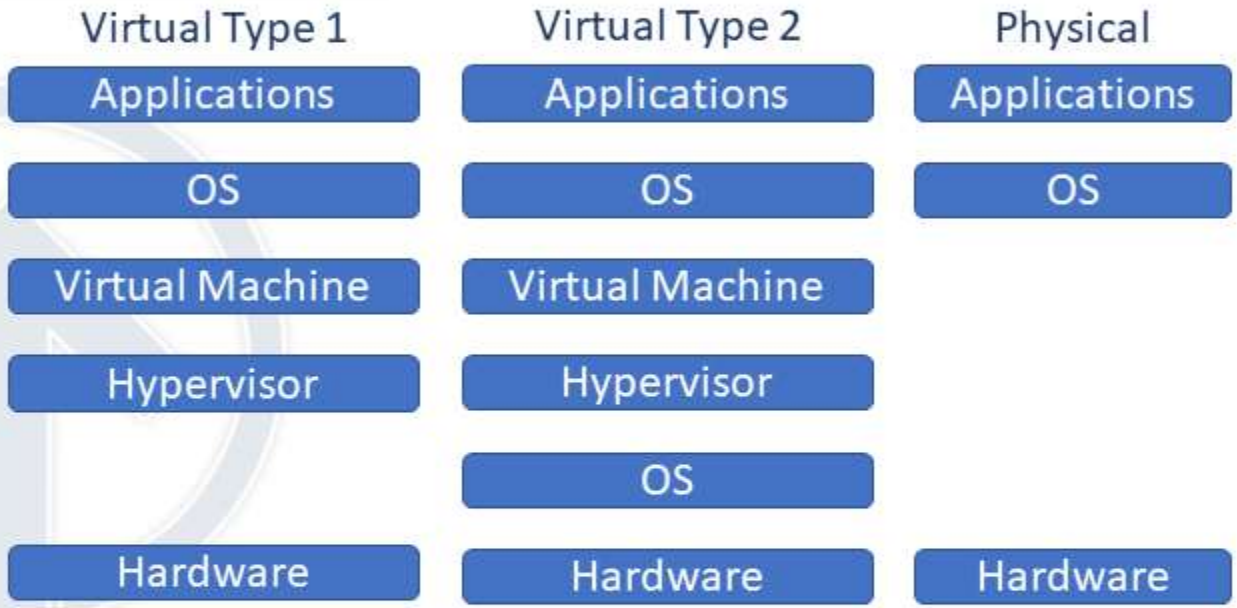
- **Preventive and Detective Controls:**
  - **Application whitelisting:**
    - We can whitelist the applications we want to allow to run on our environments, but it can also be compromised.
    - We would whitelist against a trusted digital certificate, a known hash or path and name, the latter is the least secure, an attacker can replace the file at the path with a malicious copy.
    - Building the trusted application whitelist takes a good deal of time, but is far superior to blacklisting, 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** 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 back up 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).

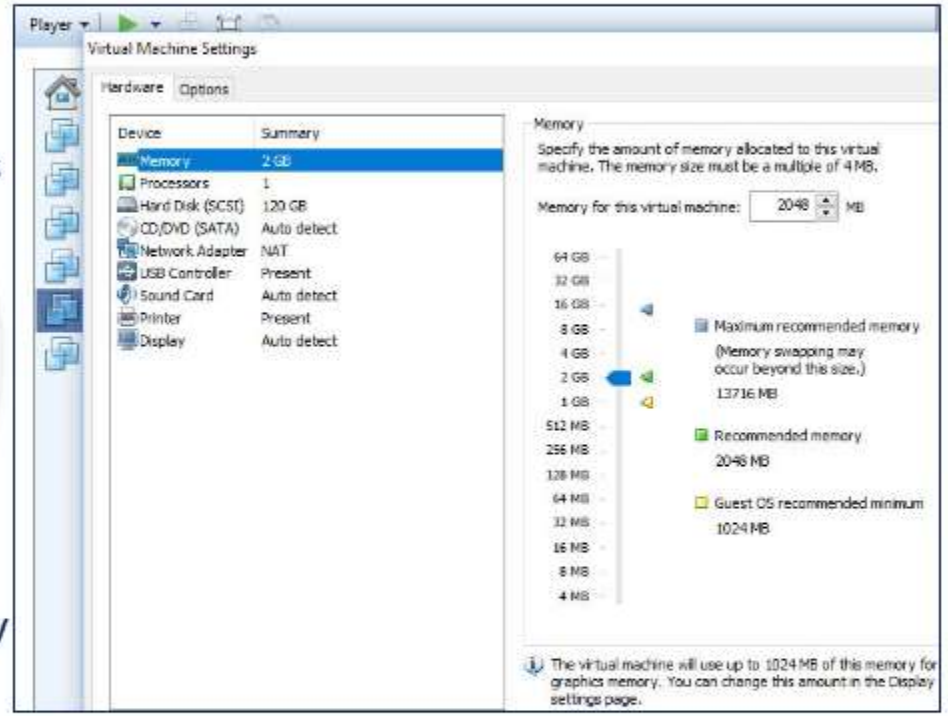
Virtualization and Distributed Computing:

- **Virtualization:**
  - **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 and Distributed Computing:

- **Virtualization:**
  - 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).

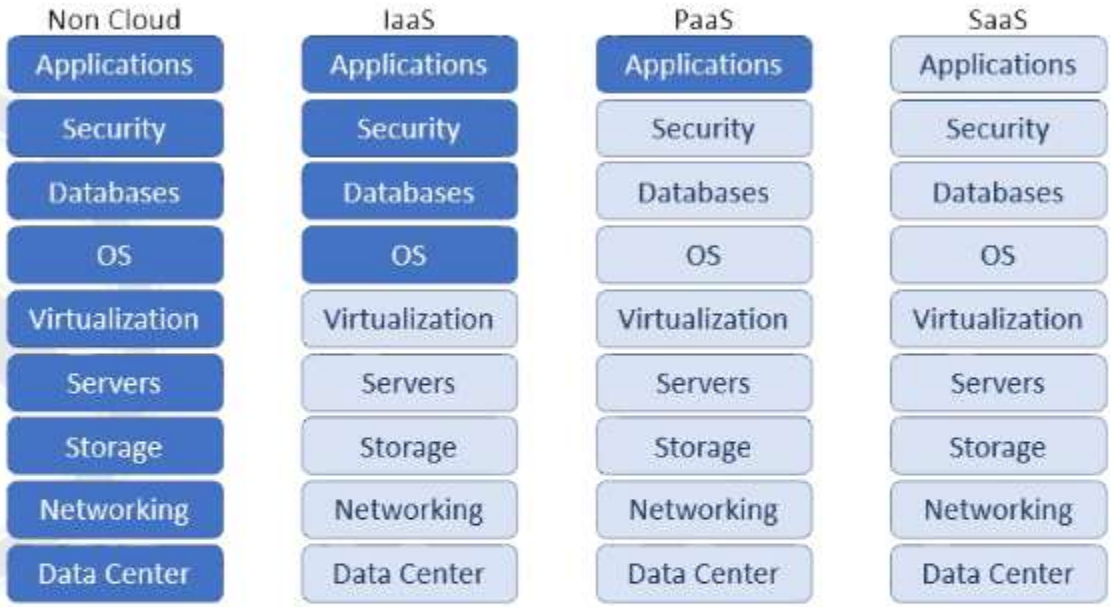


Virtualization and Distributed Computing:

- **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. It is cheaper to have someone larger or more specialized in that one area doing it for us.
  - Cloud Computing can be divided into 3 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.
  - 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.

Virtualization and Distributed Computing:

- **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.
    - **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).
    - **PaaS** - (Platform as a Service) The vendor provides pre-configured OSs, then the customer adds all programs and applications.



Virtualization and Distributed Computing:

- **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 uses 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 discernable impact.

Virtualization and Distributed Computing:

- **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.

Database Security

- **Polyinstantiation** (Alternative Facts) – Two (or more) instances of the same file depending on who accesses it.
  - The real information may be available to subjects with Top Secret clearance, but different information will be available to staff with Secret or lower clearance.
- **Aggregation** is a collection or gathering of data together for the purpose of statistical analysis. (You see the bigger picture rather than the individual pieces of data).
- **Inference** requires deducing from evidence and reasoning rather than from explicit statements.
- **Data mining** is the computing process of discovering patterns in large data sets.
  - It uses methods combining machine learning, statistics, and database systems.
- **Data Analytics** is looking at what normal operations look like, then allowing us to more proactively identify abuse from insider threats or compromised accounts.

We mitigate the attacks with **Defense in Depth** (again) – We secure the building, the entrances, the doors, the network, the servers, the OS, the DB, screen the employees, … We have solid policies, procedures, standards and guidelines.

- **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.

- **Software vulnerabilities and Attacks**
  - **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.

- **Software vulnerabilities and Attacks**
  - **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.
  - **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, Threats and Countermeasures.

- **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 kg.) 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 600ms 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).

System Vulnerabilities, Threats and Countermeasures.

- **Covert Channels**
  - **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 common are 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 *Great Expectations* (Charles Dickens, 1867 Edition - 4 pages at font size 11 , 1827 words, 7731 characters).
  - **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).

Original image

Altered image

System Vulnerabilities, Threats and Countermeasures.

- **Malware (Malicious Code)** - This is the catch-all name for any malicious software used to compromise systems or data.
  - **Viruses** - require some sort of human interaction and are often transmitted by USB sticks or other portable devices.
  - When the program is executed it replicates itself by inserting its own code into other programs.
    - **Macro** (document) viruses: Written in Macro Languages, embedded in other documents (Word, Outlook).
    - **Boot Sector** viruses: Infect the PC's boot sector or the Master Boot Record, ensuring they run every time the PC boots.
    - **Stealth** Viruses: Try to hide themselves from the OS and antivirus software.
    - **Polymorphic** Viruses: Change their signature to avoid the antivirus signature definitions. Well-written polymorphic viruses have no parts which remain identical between infections, making it very difficult to detect directly using antivirus signatures.
    - **Multipart** (Multipartite) Viruses: Spread across multiple vectors. They are often hard to get rid of because even if you clean the file infections, the virus may still be in the boot sector and vice-versa.

System Vulnerabilities, Threats and Countermeasures.

- **Malware (Malicious Code)**
  - **Worms** - spread through self propagation - they need no human interaction, they do both the payload damage and replicate through aggressive network use (also makes them easier to spot).
  - **Trojans** - malicious code embedded in a program that is normal. This can be games, attachments, website clicks, etc. …
  - **Rootkits** - Replace some of the OS/Kernel with a malicious payload. User rootkits work on Ring 3 and Kernel rootkits on Ring 0.
  - **Logic Bombs** - Malicious code that executes at a certain time or event - they are dormant until the event (IF/THEN).
    - IF Bob is not getting an annual bonus over $10,000, THEN execute malicious code.
    - IF date and time 5/15/18 00:02:12, THEN execute malicious code.
  - **Packers** – Programs to compress *.exe files, which can be used to hide malware in an executable, neutral technology.
  - **Antivirus Software** - tries to protect us against malware.
    - **Signature** based - looks for known malware signatures - MUST be updated constantly.
    - **Heuristic** (Behavioral) based - looks for abnormal behavior - can result in a lot of false positives.

System Vulnerabilities, Threats and Countermeasures.

- **Malware (Malicious Code)**
  - **Server (Service) Side Attacks:**
    - Attack directly from an attacker to a target.
    - Defense in Depth can mitigate some of these.
    - The term "Server" does not mean only servers, just that the attack is directly aimed at the end target. (They come to you).
  - **Client Side Attacks:**
    - The client initiates, then gets infected with malicious content usually from web browsers or instant messaging applications. (You go to them).
    - Since most firewalls protect inbound mostly client side attacks are often more successful.

Physical Security

- As part of physical security we also design **"Design-in-Depth"** into our plan.
  - **Preventative Controls:**
    - Prevents action from happening – Tall fences, locked doors, bollards.
  - **Detective Controls:**
    - Controls that detect an attack (before, during or after) – CCTV, alarms.
  - **Deterrent Controls:**
    - Controls that deter an attack – fences, security guards, dogs, lights, Beware of the Dog signs.
  - **Compensating Controls:**
    - Controls that compensate for other controls that are impossible or too costly to implement. We may not be able to move our datacenter or change the foundation, but we can add absorbers under the sub-floor, in the racks, …
  - **Administrative Controls:**
    - Controls that give us administrative framework – compliance, policies, procedures.

Physical Security

- **Perimeter defense:**
  - **Fences** (Deterrence, Preventative):
    - Smaller fences such as 3ft. (1m) can be a deterrence, while taller ones, such as 8ft. (2.4m) can be a prevention mechanism.
    - The idea of the fences is to ensure entrance/exits from the facility happen through only a few entry points (doors, gates, turnstiles).
  - **Gates** (Deterrence, Preventative):
    - Placed at control points at the perimeter.
    - Used with the fences to ensure access only happens through a few entry points.
    - **ATSM Standard:**
      - Class I Residential (your house) - Class II Commercial/General Access (parking garage).
      - Class III Industrial/Limited Access (loading dock for 18-wheeler trucks).
      - Class IV Restricted Access (airport or prison).

Physical Security

- **Perimeter defense:**
  - **Bollards** (Preventative):
    - Used to prevent cars or trucks from entering an area while allowing foot traffic to pass.
    - Often shops use planters or similar; it looks prettier, but achieves the same goal.
    - Most are static heavy duty objects, but some cylindrical versions can also be electronically raised or lowered to allow authorized traffic past a "no traffic" point. Some are permanent fixtures and can be removed with a key or other unlock function.
  - **Lights** (Detective and Deterrence):
    - Lights should be used to fully illuminate the entire area.
    - Lights can be static, motion activated (static) or automatic/manual Fresnel lights (search lights).
    - Measured in lumen - 1 lumen per square foot or lux - 1 lumen per square meter more commonly used.

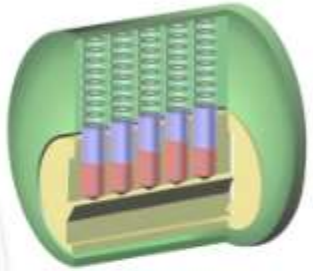
Physical Security

- **Perimeter defense:**
  - **CCTV** (Closed Circuit Television) (Detective, Deterrence) - used to monitor the facility's perimeter and inside it.
    - Normal cameras use normal light spectrum; proper lighting is essential.
    - Infrared cameras pick up heat signatures and work similar in light and dark.
    - **Older cameras** are analog and use video tapes for storage (often VHS); quality is often bad, unclear.
    - **Modern cameras** are digital and use CCD (Charged Couple Discharge); also use a **DVR** (Digital Video Recorder) which stores on a local server or device, or an **NVR** (Network Video Recorder), which stores the video on a remote network location. This last option is preferable, as it is centralized and more secure.
    - Organizations may have retention requirements either from policies or legislation that requires a certain retention of their video (this could be bank ATM, data center or entry point footage).
    - Cameras can be either static or non-static (automatic or manual).
      - We have all seen the spy or heist movies where they avoid them by knowing the patterns and timers.
      - This risk can be mitigated with a randomizer or pseudo randomizer, we want to ensure full coverage.

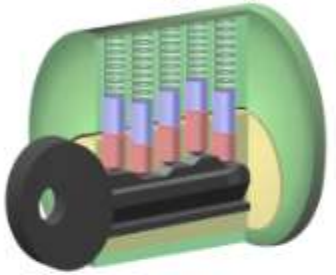
Physical Security

- **Perimeter defense:**
  - **Locks** (Preventative):
    - **Key locks:**
      - Requires a physical key to unlock; keys can be shared/copied.
      - **Key Bitting Code** (How far the key is bitten down for that section.) – Can be copied and replicated without the key from either the numbers or a photo of it.
      - **Pin Tumbler Lock** (or Yale lock) – A lock mechanism that uses pins of varying lengths to prevent the lock from opening without the correct key.

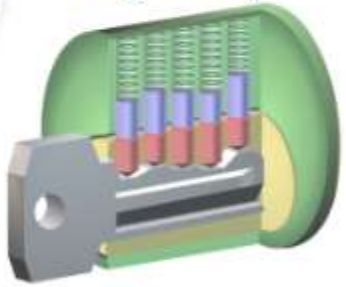
Locked Lock



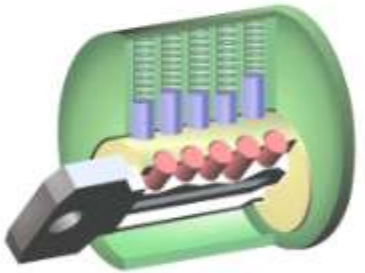
Wrong Key



Right Key

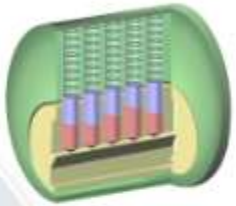


Lock opens



ThorTeaches.com

Physical Security



- **Perimeter defense:**
  - **Locks** (Preventative):
    - **Key Locks (continued):**
      - **Lock Picking** - with a lock pick sets or bumping, opening a lock without the key.
        - Any key lock can be picked or bumped; how long it takes depends on the quality of the lock.
        - Lock pick sets lift the pins in the tumbler, opening the lock.
      - **Lock Bumping** - Using a shaved-down key that matches the lock, the attacker "bumps" the key handle with a hammer or screwdriver which makes the pins jump, then the attacker quickly turns the key.

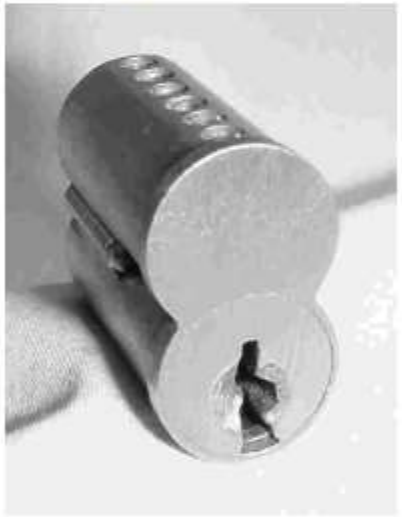
Lock picking

Bumping key

Physical Security

- **Perimeter defense:**
  - **Locks** (Preventative):
    - **Key Locks (continued):**
      - **Master Keys** open any lock in a given area or security zone.
        - Should be very closely guarded, both who has them and where they are kept at all times.
      - **Core Key** is used to remove a lock core in "interchangeable core locks."
        - An interchangeable core, or IC, is a compact keying mechanism in a specific figure-eight shape.
        - Relies upon a specialized "control" key for insertion and extraction of the core.
        - Should be kept secure and access should be very restricted.

Interchangeable core lock

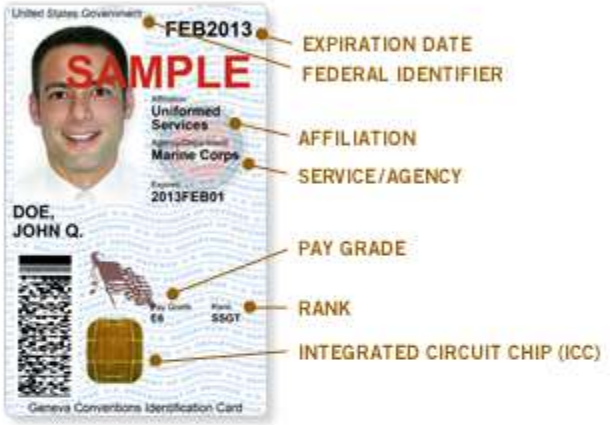


Physical Security

- **Perimeter defense:**
  - **Locks** (Preventative):
    - **Combination Locks:**
      - Not very secure and have limited accountability even with unique codes.
      - Should be used for low security areas.
      - Can be Dial type (think safe), Button or Keypad.
      - Very susceptible to brute force, shoulder surfing and are often configured with weak security (I know of a good deal of places where the code is the street number).
      - Over time the buttons used for the code will have more wear and tear
      - A 4-number PIN where 4 keys are used, the possible combinations are no longer 10,000, but 256; if 3 keys, then 81 options.

Physical Security

- **Perimeter Defense:**
  - **Smart Cards** (contact or contactless):
    - They contain a computer circuit, using ICC (Integrated Circuit Card).
    - **Contact Cards** - Inserted into a machine to be read.
      - This can be credit cards you insert into the chip reader or the DOD CAC (Common Access Card).
    - **Contactless Cards** - can be read by proximity.
      - Key fobs or credit cards where you just hold it close to a reader.
      - They use an RFID (Radio Frequency Identification) tag (transponder) which is then read by an RFID Transceiver.
  - **Magnetic Stripe Cards:**
    - Swiped through a reader, no circuit.
    - Very easy to duplicate.



Physical Security

- **Perimeter Defense (continued):**
  - **Tailgating/Piggybacking:**
    - Following someone authorized into an area you are not authorized to be in.
    - Often combined with Social Engineering.
    - It is easy to do if your reason for being there seems plausible.
    - Bring a lot of food, a cake and some balloons, have on clothes, ID badge and tools that a repairman would, the options are endless.
  - **Mantrap:**
    - A Mantrap is a room with 2 doors; door 1 must close completely before Door 2 can be opened.
    - Each door has a different authentication method (something you know, something you have, something you are).
    - They can at times use weight sensors - Bob weighs 220lbs (100kg), the weight measured by the pressure plate is 390lbs (177kg), someone is probably in the room with Bob. Door 2 won't open until Bob is confirmed alone in the Mantrap with a cart of old servers, normally done by the cameras in the trap.

Physical Security

- **Perimeter Defense (continued):**
  - **Turnstiles** (Preventative, Deterrence):
    - Also prevents tailgating, by only allowing 1 person to enter per Authentication (think like in US subway systems or amusement park entries, but for secure areas they are often floor to ceiling turnstiles with interlocking blades.

Both Mantraps and Turnstiles should be designed to allow safe evacuation in case of an emergency. (Remember that people are more important to protect than stuff.)

Physical Security

- **Perimeter Defense (continued):**
  - **Contraband Checks** (Preventative, Detective, Deterrent):
    - Often seen in airports, courthouses, intelligence offices or other higher security facilities.
    - Checking what you are bringing in or out of the building to ensure nothing dangerous gets in or anything confidential gets out.
    - With technology becoming much smaller, these are less effective when is comes to data theft; it is easy to hide a micro SD memory card, which can contain up to 256GB of data per card.

Physical Security

- **Perimeter Defense (continued):**
  - **Motion Detectors** (Detective, Deterrence):
    - Used to alert staff by triggering an alarm (silent or not).
    - Someone is here, did an authorized person pass the checkpoint?
      - IF yes, then log the event and do nothing else - IF no, then alert/alarm.
    - Basic ones are light-based - They require light, making them not very reliable.
    - **Ultrasound, Microwave, Infrared or Laser** (*pew-pew!!*)
      - Active sensors, they send energy (sound, wave or light).
      - If the sound takes less time to return or the pattern it receives back is altered, it means someone is somewhere they should not be.
      - Photoelectric motion sensors send a beam of light to a sensor; if broken the alarm sounds. These are the *pew-pew* lasers and sorry, no, they are not green or red and they are rarely visible.

Physical Security

- **Perimeter Defense (continued):**
  - **Perimeter Alarms:**
    - Door/window sensors – these are the thin strips around the edges of either, and also contact sensors.
      - If opened an alarm sounds; if broken, same effect.
      - Can be circumvented, but they are part of a layered defense.
    - Walls, windows, doors and any other openings should be considered equally strong.
    - Walls are inherently stronger; the rest need compensating measures implemented (locks, alarms, sensors).
    - Glass is normally easy to break, but can be bullet and/or explosion proof, or have a wire mesh in the middle.
    - Plexiglass can also be used, as it is stronger and does not shatter, but can be melted.
    - Door hinges should always be on the inside (or hidden in the door).
    - Just like the turnstiles and mantraps, doors (and in some cases windows) should be designed to allow safe exit from the building in case of an emergency. Often there is a "Panic Bar" that opens the door, but they are also connected to alarms that sound when opened (clearly labeled Emergency Only - Alarm WILL Sound).

Physical Security

- **Perimeter Defense (continued):**
  - **Walls, Floors, and Ceilings:**
    - In line with our layered defense strategy, the strong security encountered in getting to a data center does nothing if there is a crawl space that an attacker can use.
    - We need to secure all possible ways into our Data Center or other secure location.
    - Walls should be "slab to slab" (from the REAL floor to the REAL ceiling); if sub-flooring or sub-ceilings are used, then they should be contained within the slab to slab walls.
    - Walls, floors and ceilings should be made of materials (where it makes sense) that are secure enough for that location, e.g. don't have sheetrock around your Data Center because I can cut that with a knife.
    - Walls, floors and ceilings should have an appropriate fire rating.
      - So should your doors, but walls, floors and ceilings are more often overlooked.
      - This is to protect the Data Center from outside fire, but just as well the rest of the building from a Data Center fire.

Physical Security

- **Perimeter Defense (continued):**
  - **Guards** – (Deterrent, Detective, Preventative, Compensating)
    - Guards can serve many diverse purposes for an organization.
    - They can check credentials/ID Cards, monitor CCTV cameras, monitor environmental controls (HVAC), react to incidents, act as a deterrent and so much more.
    - **Professional Guards** - Professional training and/or schooling; armed.
    - **Amateur Guards** - No professional training or schooling ; armed.
    - **Pseudo Guard** - Unarmed guard.
    - Guards should have a very clear set of rules and regulations.
    - Social engineering attacks are common and should be prevented with training to raise awareness.

Physical Security

- **Perimeter Defense (continued):**
  - **Dogs** (Deterrent, Detective, Compensating):
    - Most often used in controlled, enclosed areas.
    - Liability can be an issue.
    - Dogs are trained to corner suspects and attack someone who's fleeing. People often panic when they encounter a dog and run.
    - Even if they're in a secure area the organization may still be liable for injuries.
    - Can also be internal authorized employees walking out the wrong door or trying to take a shortcut.
    - They panic and the dog attacks.

Physical Security

- **Perimeter Defense (continued):**
  - **Restricted Work Areas and Escorts.**
    - To track and funnel authorized visitors we can use visitor badges, visitor logs and escorts.
    - Non-electronic visitor badges are easy to make copies of and easy to fake.
    - Electronic can be just a cheap re-programmable magnetic strip (like for hotel rooms, easy to copy). Make sure they have a short window of use, or more secure individually printed ones for each visit, and only used once.
    - The return of all badges and physical sign-out should be enforced when the visitor leaves.
    - When a vendor is coming to repair, install or remove something in your facility, they need to be checked in and escorted from the entry point to where they are going to work by an employee, and the employee should stay with the vendor until the work is completed.
    - The vendor's employees should already have passed a security check when they were hired; the vendor is liable.
    - This sounds and is boring, but it is more likely to prevent the vendor from compromising your security than if they were free to roam the facility and the data center unsupervised.

Physical Security

- **Site Selection, Design and Configuration:**
  - Before building a new facility, it is very important to do proper research and planning.
  - Multiple factors need to be considered, but for the exam you need to think about the security ones.
  - **Site Selection:**
    - **Greenfield** - Not built on yet; undeveloped land.
    - **Topography** - the physical shape of the landscape - hills, valleys, trees, streams. Most often used at military sites where they can leverage (sometimes by altering) the topology for better security.
    - **Utilities** - How reliable is the power, the internet in the area?
    - **Crime** - How high are the crime rates in the area? How close are the police?

Physical Security

- **Site Selection, Design and Configuration:**
  - **Site Design:**
    - **Site Marking:**
      - Do not advertise your data center's (or other critical) locations.
      - The more non-descript and boring the building is, the less attention it gets (security through obscurity).
      - A determined attacker can obviously find the information, but the harder you make it, the less your chances of being compromised.
        - Example: Don't name your credit card processing server creditcard001.

Physical Security

- **Site Selection, Design and Configuration:**
  - Shared Tenancy and Neighbors
    - Sharing your building with someone else poses other security risks; the people working at or visiting those organizations are already past the perimeter.
    - Their bad security posture can be a risk to yours.
    - Attackers can set up base right next door, they can eavesdrop and attack on your wireless without causing much suspicion.
    - Think of the many movies with bank robberies or great heists where they go through a neighbor's wall, ceiling or floor.
    - These all have a basis in reality from real robbers who did just that.

Physical Security

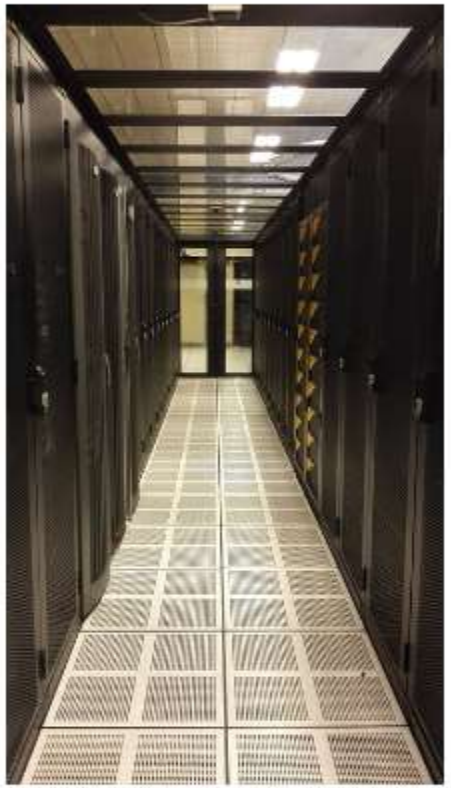
- **Site Selection, Design and Configuration:**
  - **Wiring Closets**
    - If shared, the other tenants have access to your network. You can lock it down, but it is still a big security concern. I have seen a place where one tenant had all their equipment bolted to the wall, but the wires were exposed; it would be easy to attach a sniffer to that.
  - **Demarc** - Point of Demarcation (POD) :
    - Where the ISP (Internet Service Provider) terminates their phone/internet lines and your network begins; most buildings only have one.
    - When shared, it is a security concern that other tenants have access. Can they access your equipment?
    - IPv4 is not inherently secure and ISP connections are not either. You must add the security on your end.
    - It is desired to have strong Access Control for the Demarc. If not possible, find another location. (IAAA)
    - For secure sites or sites that need high uptime it is common to have multiple Demarcs from multiple ISP's. How segmented and secure each Demarc is depends on your information security posture.

Physical Security

- **Site Selection, Design and Configuration:**
  - **Server Rooms and Data Centers:**
    - Many Data Centers were designed for our past requirements and not how much data we move today.
    - Pop-up server rooms are built when we outgrow our current Data Center and we bolt-on somewhere in the building that was NOT built for that purpose.
    - They often lack proper walls, floors, ceilings, flood prevention; bolted-on and not designed-in is less secure.
    - I have seen a bolt-on server room where there were showers and bathrooms just above it. What a fun day they would have if the floor/ceiling started leaking.
    - **Data Center Build or Expansion:**
      - How much HVAC (Heating, Ventilation and Air Conditioning) do we need for now/future use?
      - Which natural events do we need to factor in for where we are (e.g. hurricanes, floods, tornadoes)?
      - Do we have enough Power for current/future use; is the grid stable? Are blackouts or brownouts common? Brownout = drop in voltage (lights flicker). Blackout = power is interrupted completely.

Physical Security

- **Site Selection, Design and Configuration:**
  - **Server Rooms and Data Centers:**
    - **Data Center Build or Expansion** (continued):
      - **Power:**
        - What size generators do we need?
        - How large of a **UPS** (Uninterruptible Power Supply)? Huge battery bank also ensures consistent voltage.
      - **Fire Suppression:**
        - Dry pipe vs. wet pipe.
        - Halon/Chemical/FM200.
        - Fire extinguishers.



Environmental Controls

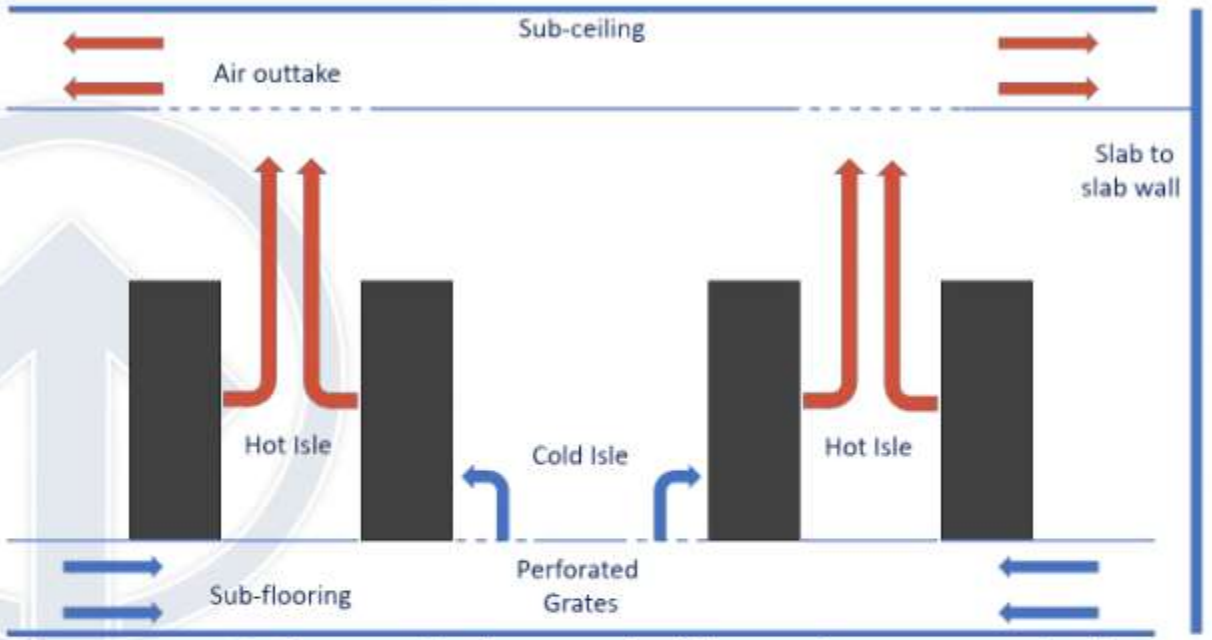
- **HCAC**
  - **Heat:**
    - Many data centers are kept too cold; the last decade's research has shown it is not needed.
    - Common temperature levels range from 68–77 °F (20–25 °C) - with an allowable range of 59–90 °F (15–32 °C).
    - Keeping a data center too cold wastes money and raises humidity.
  - **Pressure:**
    - Keeping positive pressure keeps outside contaminants out.
  - **Humidity:**
    - Humidity should be kept between 40 and 60% rH (Relative Humidity).
    - Low humidity will cause static electricity and high humidity will corrode metals (electronics).

Vendor Data Center temperature recommendations:

Vendor	Low (C°/F°)	High (C°/F°)	Optimal
Cisco	18/64.4	27/80.6	-
Google	-	-	26.7/80
Dell	24+/Upper 70 F°	26+/Lower 80 F°	
HP	18/64.4	27/80.6	
IBM	18/64.4	27/80.6	
Oracle	21/70	23/74	22/72

Environmental Controls

- **HCAC (continued):**
  - **Drains:**
    - Many data centers use subflooring where water and contaminants (mostly dust) can gather. If an HVAC unit malfunctions, it can leak water.
    - It is important to have sensors in the subfloor for both water and dust, and to regularly vacuum the space.



Servers, switches and other rackable equipment are built with air intake and exhaust facing the hot and cold aisles. Servers have intake in the back and exhaust in the front and switches are often reserved.

Environmental Controls

- **Static Electricity:**
  - Can be mitigated by proper humidity control, grounding all circuits, using antistatic wrist straps and work surfaces.
  - All personnel working with internal computer equipment (motherboards, insert cards, memory sticks, hard disks) should ground themselves before working with the hardware.

Antistatic shoes.
Not the prettiest thing I ever saw, but effective!

Antistatic wrist strap.

Environmental Controls

- **Heat, Flame, and Particle/Smoke Detectors:**
  - All used for detecting fires or potential fires, they are connected to warning lights, sirens and suppression systems.
  - **Heat Detectors:**
    - Configured to trigger when a certain threshold is exceeded (Rise of 10° F in < 5 minutes or rising above 90° F).
  - **Smoke Detectors:** (Ionization or Photoelectric):
    - **Ionization** detectors have a small radioactive source which creates a small electric charge.
    - **Photoelectric** uses LED (Light Emitting Diode) and a photoelectric sensor that produces a small charge while receiving light.
    - Both trigger when smoke or any higher particle density interrupts the radioactivity or light.
  - **Flame Detectors:**
    - Flame detectors detect infrared or ultraviolet light emitted by fire.
    - They require line of sight to detect the flame.

Environmental Controls

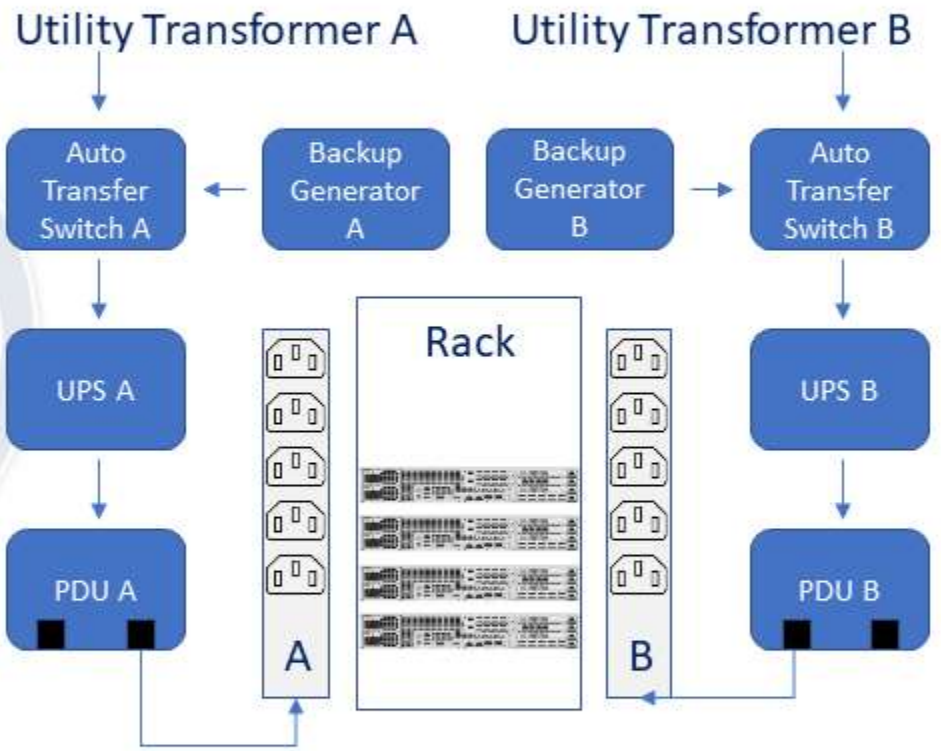
- **Electricity** - It is important to have clean, reliable power for our servers, disk arrays, network equipment.
  - Loss of power can effect our availability and the Integrity of our data.
    - Nothing can be accessed and power fluctuations can damage hardware and corrupt data.
  - **Power Fluctuation** Terms:
    - **Blackout** - Long loss of power.
    - **Fault** - Short loss of power.
    - **Brownout** - Long low voltage.
    - **Sag** - Short low voltage.
    - **Surge** - Long high voltage.
    - **Spike** - Short high voltage.

Data Center Batteries for UPS'

Data Center PDU's

Environmental Controls

- **Electricity:**
  - **Surge Protectors, UPSs** and Generators are used to get clean power.
    - **Surge Protectors** - Protect equipment from high voltage.
    - **UPSs** (Uninterruptible Power Supplies):
      - Ensure constant clean power to the systems.
      - Have large battery banks that take over in the event of a power outage; they also act as surge protectors.
    - **Generator:**
      - Fueled generators are programmed to manually or automatically (preferred) kick in during a power outage event.
      - Will run as long as they have fuel, must be maintained.
    - **PDU** (Power Distribution Unit) can be in rack or not.



Environmental Controls

- **Electricity:**
  - **EMI (Electromagnetic Interference)**
    - Disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction.
    - In our world this includes circuits, power cables, network cables, ...
    - Often this is an issue with network cables that are not shielded properly or run too closely to power cables. Magnetism from one cable "crosses" over to a neighbor cable (crosstalk).
    - This can impact the **Integrity** (data corruption), **Confidentiality** (data sniffed), and **Availability** (data unavailable).
    - Crosstalk is avoided with proper cable management, and by using STP (Shielded Twisted Pair) cables, not UTP (Unshielded Twisted Pair) cables.
    - Power cables should never be run close to copper data cables.
    - Fiber optic cables are used when it makes sense (not susceptible to EMI or sniffing, since they are glass).
    - On the exam, if asked for the cheapest secure cables, fiber > copper; while not as cheap they are way more secure.

- **Continuity of Operations:**
  - **Fault tolerance:**
    - To ensure our internal SLA's and provide as high availability as possible we use as high degree of redundancy and resiliency as makes sense to that particular system and data set.
    - **Backups:**
      - One of the first things that comes to mind when talking about fault tolerance is backups of our data, while it is very important it is often like log reviews an afterthought and treated with "Set it and forget it" mentality.
      - For backups we use Full, Incremental, Differential and Copy backups, and how we use them is determined on what we need from our backups.
      - How much data we can stand to lose and how fast we want the backup and restore process to be.
      - In our backup solution we make backup policies of what to back up, what to exclude, how long to keep the data of the Full, Incremental and Differential backups.
      - All these values are assigned dependent on what we back up, and normal organizations would have different backup policies and apply those to the appropriate data.

- **Continuity of Operations:**
  - **Backups:**
    - This could be Full 3, 6, 12, 36, 84 months and infinity, the retention is often mandated by our policies and the regulations in our field of business.
    - It is preferable to run backups outside of business hours, but if the backup solution is a little older it can be required to run around the clock, in that case we put the smaller and less important backups in the daytime and the important larger ones after hours.
    - We often want to exclude parts of the system we are backing up, this could be the OS, the trashcan, certain program folders, ... we just backup what is important and rarely everything.
    - If a system is compromised and the issue is a rootkit, the rootkit would persist on the backup if we did a full mirror restore, by eliminating some of the system data we not only backup a lot less data, we also may avoid the infection we are trying to remedy.
    - For very important data we may do hourly incrementals or use another form of data loss prevention (covered later in this chapter).

- **Continuity of Operations:**
  - **Backups:**
    - **Full backup:**
      - This backs everything up, the entire database (most often), or the system.
      - A full backup clears all archive bits.
      - Dependent on the size of the data we may do infrequent full backups, with large datasets it can take many hours for a full backup.

Full Backup:
Everything in the backup policy is backed up

- **Continuity of Operations:**
  - **Backups:**
    - **Incremental backups:**
      - Backs up everything that has changed since the last backup.
      - Clears the archive bits.
      - Incrementals are often fast to do, they only backup what has changed since the last incremental or full.
      - The downside to them is if we do a monthly full backup and daily incrementals, we have to get a full restore and could have to use up to 30 tapes, this would take a lot longer than with 1 Full and 1 Differential.

Incremental Backup:
Anything changed since the last backup is backed up.
The archive bit is cleared.

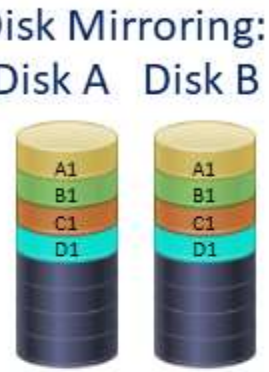
- **Continuity of Operations:**
  - **Backups:**
    - **Differential backup:**
      - Backs up everything since the last Full backup.
      - Does not clear the archive bit.
      - Faster to restore since we just need 2 tapes for a full restore, the full and the differential.
      - Backups take longer tjan the incrementals, we are backing everything since the last full.
      - Never use both incremental and differential on the same data, it is fine on the same backup solution, different data has different needs.

Differential Backup:
Anything changed since the last Full backup is backed up.
The archive bit is not cleared.

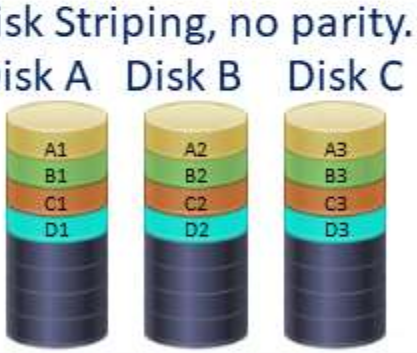
- **Continuity of Operations:**
  - **Backups:**
    - **Copy backup:**
      - This is a full backup with one important difference, it does not clear the archive bit.
      - Often used before we do system updates, patches and similar upgrades.
      - We do not want to mess up the backup cycle, but we want to be able to revert to a previous good copy if something goes wrong.
    - **Archive bit:**
      - For Windows the NTFS has an archive bit on file, it is a flag that indicates if the file was changed since the last Full or Incremental backup.

- **Continuity of Operations:**
  - On our systems we build in fault tolerance to give them as high as possible uptime, we do this with redundant hardware and systems, one of the practices we use is RAID.
  - **RAID** (Redundant Array of Independent/Inexpensive Disks):
    - Comes in 2 basic forms, disk mirroring and disk striping.
    - **Disk mirroring:**
      - Writing the same data across multiple hard disks, this is slower, the RAID controller has to write all data twice.
      - Uses at least 2 times as many disks for the same data storage, needs at least 2 disks.
    - **Disk striping:**
      - Writing the data simultaneously across multiple disks providing higher write speed.
      - Uses at least 2 disks, and in it self does not provide redundancy.
      - We use parity with striping for the redundancy, often by XOR, if we use parity for redundancy we need at least 3 disks.

Disk Mirroring:



Disk Striping, no parity.



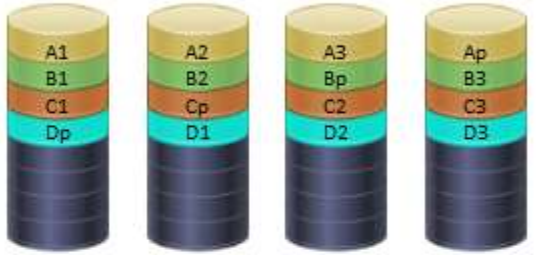
- **Continuity of Operations:**
  - **RAID** (Redundant Array of Independent/Inexpensive Disks):
    - There are many different types of RAID, for the exam I would know the above terms and how RAID 0, 1 and 5 works.
    - **RAID 0:**
    - Striping with no mirroring or parity, no fault tolerance, only provides faster read write speed, requires at least 2 disks
    - **RAID 1:**
    - Mirror set, 2 disks with identical data, and write function is written to both disks simultaneously.

RAID 0

RAID 1

- **Continuity of Operations:**
  - **RAID** (Redundant Array of Independent/Inexpensive Disks):
    - **RAID 5:**
      - Block level striping with distributed parity, requires at least 3 disks.
      - Combined speed with redundancy.
  - RAID will help with data loss when we have a single disk failure if we use a fault tolerant RAID type, if more than one disk fails before the first is replaced and rebuilt, we would need to restore from our tapes.
  - Most servers have the same disks with the same manufacturer date, they will hit their MTBF (Mean time between failures) around the same time.
  - Larger data centers often have SLA's with the hard disk/server vendor, which also includes MTTR (Mean time to repair).
  - This could be within 4 or 8 hours the vendor has to be onsite with a replacement disk.

RAID 5



- **Continuity of Operations:**
  - **System redundancy:**
    - On top of the RAID and the backups we also try to provide system redundancy as well as redundant parts on the systems.
    - The most common system failures are from pieces with moving parts, this could be disks, fans or PSU (power supplies).
    - Most servers have redundant power supplies, extra fans, redundant NIC's.
    - The NIC and PSU serve a dual purpose, both for internal redundancy and external. If a UPS fails, the server is still operational with just the 1 PSU getting power.
    - Redundant disk controllers are also reasonably common, we design and buy the system to match the redundancy we need for that application.

Redundant PSU's in s server

- **Continuity of Operations:**
  - **System redundancy:**
    - Often we have spare hardware on hand in the event of a failure, this could include hard disks, PSU's, fans, memory, NICs.
    - Many systems are built for some hardware to be hot-swappable, most commonly HDD's, PSU's and fans.
    - If the application or system is important we often also have multiple systems in a cluster.
    - Multiple servers often with a virtual IP, seen as a single server to users.
    - Clustering is designed for fault tolerance, often combined with load balancing, but not innately.
    - Clustering can be active/active, this is load balancing, with 2 servers both servers would actively process traffic.
    - Active/passive: There is a designated primary active server and a secondary passive server, they are connected and the passive sends a keep-alive or heartbeat every 1-3 seconds, are you alive, are you alive ...
    - AS long as the active server responds the passive does nothing, if the active does not respond for (normally) 3 keepalives the passive assumes the primary is dead and assumes the primary role.
    - In well designed environments the servers are geographically dispersed.

- **Continuity of Operations:**
  - **System redundancy:**
    - We can also use other complementary backup strategies to give ourselves more real time resilience, and faster recovery.
    - **Database shadowing:**
      - Exact real time copy of the database or files to another location.
      - It can be another disk in the same server, but best practice dictates another geographical location, often on a different media.
    - **Electronic vaulting** (e-vaulting):
      - Using a remote backup service, backups are sent off-site electronically at a certain interval or when files change.
    - **Remote journaling:**
      - Sends transaction log files to a remote location, not the files themselves. The transactions can be rebuilt from the logs if we lose the original files.

Physical Security

- **Media Storage and Locations:**
  - Where and how you store your offline data/media and (preferably) offsite is dictated by internal policies, procedures and compliance requirements.
  - All storage media should be encrypted (Data at Rest).
  - Media (often tape) should be stored at an offsite facility designed for just that.
  - The facility should be climate controlled (temperature,humidity) less strict than a data center, standards still apply.
    - Tape will deteriorate at a certain temperature just like disks will corrode at a certain humidity.
    - The storage facility should be secure, licensed and bonded (both for transport and storage).
    - Lost data is just as lost, but they are liable.
  - Under an employee's bed is NOT an OK place to store backups.
  - Multiple incidents have happened when this was done, and break-ins relieved the employees of the tapes, which in many cases were NOT encrypted. Welcome to $10,000, $100,000 or $1,000,000 fines/lawsuits or loss of revenue from the bad publicity hit. (Data at Rest should always be encrypted).

Physical Security

- **Asset Tracking:**
  - Keeping an accurate inventory of all our assets is important; we can't protect what we don't know we have.
  - We covered this a little in our risk analysis section, but other than identifying the assets, we also should have it as part of our technology refresh cycle to record the Asset Serial Number, Model Number and often an internal Asset ID.
- **Hardware Hardening:**
  - On our servers - we harden the server.
    - Apply all patches, block ports not needed, delete default users, … most places are good about this.
  - Workstations are often overlooked.
- **Disabling the USB Ports**, CD drives and any other port that can introduce malware to our network.
  - Physically: Disabled on motherboard or port itself blocked, easy to bypass - not very secure.
  - Logically: Locked in Windows services or through AD (Active Directory) is not easy to bypass (if done right) - more secure.

Virtualization and Distributed Computing:

- **The Internet of Things** (IoT) – This is one of the new things added to the 2015 CISSP update.
  - 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.

What we covered in Domain 2

- 30% of the exam questions on the certification are from this domain.
- As the name indicates, how do we manage our risk?
- What can we do to reduce the risk to an acceptable level?
- We identify all of our assets, and do qualitative and quantitative risk analysis.
- We cover the COBIT5, ISO27001/2, NIST 800-37, and NIST 800-53.
- System and software vulnerabilities.
- Networking, networking devices, IP, NAT, PAT, …
- Physical security.
- Redundancy, RAID, backups.