Classwork Activity1: Adriana Coert 20240201

Chapter1

1. Define the following:
   1. Firewalls: Security devices or software that control network traffic based on rules, protecting internal networks from external threats.
   2. DMZ: A subnetwork that separates an internal network from untrusted external networks, adding a layer of security for publicly accessible services.
   3. VPN: A technology that creates a secure, encrypted connection over a less secure network, allowing secure remote access and protecting user privacy.
   4. Hostnames: Human-readable labels for devices on a network, used to identify them in electronic communication and translate to IP addresses via DNS.
   5. IP Addresses: Numerical labels for devices on a network, used to identify hosts and provide their location for data transmission, available in IPv4 and IPv6 formats.
   6. MAC Addresses: Unique hardware identifiers for network interface controllers, used to ensure data is delivered to the correct device on a local network.

1. Identify and give a scenario where the following Considerations for a business structure would be addressed:
   1. Budget: Determines the financial resources available for expansion, including capital expenditures (CapEx) and operational expenditures (OpEx).

Scenario- The company sets a budget of $500,000 for upgrading its IT infrastructure. This includes costs for new hardware, software licenses, and potential hiring of additional staff. The IT department must prioritize spending to ensure the most critical components are addressed first, such as upgrading servers and implementing new cybersecurity measures.

* 1. Skill set: Assess the existing skill sets within the team and identify any gaps that need to be filled through training or hiring.

Scenario- The IT manager finds that the team lacks cloud computing skills. The company decides to train employees in cloud technologies and hire a cloud architect to oversee the migration, ensuring effective management and support of the new infrastructure.

* 1. Existing infrastructure: Review the current IT infrastructure to determine what can be retained, what needs upgrading, and what should be replaced.

Scenario- An audit shows the network equipment is current, but the servers are outdated and can't meet growing demands. The company opts to replace the servers with scalable cloud solutions, while retaining the existing network infrastructure.

* 1. Hardware: Identify the hardware requirements for the expansion, including servers, computers, networking equipment, and peripherals.

Scenario- An audit finds the network equipment is current, but the servers are outdated and insufficient for increased demand. The company plans to replace the servers with scalable cloud solutions while retaining the existing network infrastructure.

* 1. Environment: Consider the physical environment where the IT infrastructure will be housed, including space, cooling, and power requirements.

Scenario- The company evaluates its current office space and determines that it is insufficient to accommodate the new data center. As a result, they decide to lease additional office space designed to support the cooling and power requirements of the new equipment.

* 1. The number of users: Estimate the number of users who will interact with the system and ensure that the infrastructure can support the load.

Scenario- The expansion will increase the number of employees from 100 to 200, requiring the IT department to ensure that the network and systems can handle the increased user load. This involves upgrading network bandwidth and implementing load-balancing solutions to maintain performance and reliability.

* 1. Security: Assess the security requirements to protect sensitive data and ensure compliance with industry regulations.

Scenario- With the expansion and increased customer data, the company implements enhanced security measures, including robust firewalls, intrusion detection systems, and data encryption. They also conduct a security audit to identify vulnerabilities and ensure compliance with data protection regulations like GDPR or CCPA.

1. Give examples of the following Network Models and explain how they work:
   1. peer-to-peer (P2P) networks: Example: BitTorrent. In P2P networks, each device acts as both a client and a server, sharing resources directly with other devices without a central server. This decentralized model allows for scalable resource sharing.
   2. Client-server networks: Example: Web Browsing. In client-server networks, clients request resources or services from a central server, which manages and provides these resources to multiple clients. This model centralizes data management and provides reliable service.
   3. Wired networks: Example: Ethernet. Wired networks use physical cables to connect devices, offering stable, high-speed, and reliable connections compared to wireless networks. Data is transmitted via electrical signals over the cables.

1. What Is a network HUB- A network hub is a basic device that connects multiple devices in a LAN by broadcasting data to all connected devices. It operates at the physical layer of the OSI model, lacks intelligence to route or filter data, and can lead to network congestion and collisions. Hubs are simple and cost-effective but are often replaced by switches in modern networks for better performance.
2. What is a network bridge- A network bridge connects and filters traffic between multiple network segments, making them function as a single network. Operating at the data link layer, it uses MAC addresses to forward or filter data and reduces network congestion by dividing traffic into smaller segments.
3. What is a network Switch- A network switch connects multiple devices in a LAN and directs data traffic efficiently by using MAC addresses to send data only to the intended recipient. Operating at the data link layer, switches manage multiple collision domains and support full-duplex communication for improved network performance.
4. What is Internet Service Providers (ISPs)- Internet Service Providers (ISPs) are companies that offer internet access to individuals and businesses through various connection types like broadband, wireless, and satellite. They provide different service plans and maintain the necessary infrastructure for internet connectivity, often offering additional services such as email and web hosting.
5. Explain VLAN- A Virtual Local Area Network (VLAN) segments a physical network into multiple logical networks, improving traffic management and security. VLANs allow devices to communicate as if they were on the same physical network, regardless of their actual location, by tagging data packets with VLAN IDs. This setup enhances network performance and isolates traffic, with inter-VLAN communication managed by routers or Layer 3 switches.
6. What is the difference between Circuit Switching and Packet Switching- Circuit Switching provides a dedicated, continuous connection for a session, ensuring consistent quality but with less efficient use of resources. Packet Switching breaks data into packets that are routed independently, offering efficient resource use and scalability but with variable performance.
7. What are some Understanding carrier standards, elaborate their functions- Carrier standards like GSM, CDMA, LTE, 5G, DOCSIS, and Ethernet ensure compatibility and performance across telecommunications by providing essential services such as 2G voice and text, multi-user frequency access, high-speed data, ultra-fast connectivity, and reliable wired LAN connections.

1. Explain the following:
   1. Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)- A protocol for wireless networks that helps avoid data collisions by having devices check if the channel is clear before transmitting.
   2. Radio waves- Electromagnetic waves used for wireless communication, transmitting data through the air.
   3. Frequency- The number of wave cycles per second, determining the communication channel and bandwidth.
   4. Modulation- The process of varying a carrier signal to encode data for transmission.
   5. Encryption- Converting data into a secure format to prevent unauthorized access.
   6. MAC filtering- A security feature that controls network access based on the MAC addresses of devices.

1. Visually present the structure of these types of Network Topologies
   1. Logical topologies versus physical topologies- refers to how data flows within a network and how devices interact with each other whereas physical topology refers to the actual physical layout of network devices and cables.
   2. Bus topology- [Device1]---[Device2]---[Device3]---[Device4]---[Device5]

All devices are connected to a single central cable (the bus). Data is sent to all devices, but only the intended recipient processes it

* 1. Ring topology- [Device1]

/ \

[Device2]---[Device3]

\ /

[Device4]

Devices are connected circularly. Data travels in one direction around the ring, passing through each device until it reaches its destination.

* 1. Star topology- [Device1]

|

[Switch]

|

[Device2]

|

[Device3]

|

[Device4]

All devices are connected to a central hub or switch. Data is sent from one device to the central hub, which then forwards it to the intended recipient.

* 1. Mesh topology- [Device1]---[Device2]

/ | \ / |

/ | \ / |

[Device3]---[Device4]---[Device5]

\ | / \ |

\ | / \ |

[Device6]---[Device7]

Every device is connected to every other device. This provides high redundancy and reliability but requires more cables

* 1. Hybrid topology- [Star1]---[Switch]---[Star2]

/ \ | / \

[DeviceA] [DeviceB] [DeviceC] [DeviceD]

A combination of two or more different topologies. For example, combining star and bus topologies, where multiple star networks are connected via a bus.