Mariam Adegbindin

1133249

**Networking and IT**

**1.5 Introduction to IP**

* An IP (Internet protocol) is used to move information from point A to point B, basically it transports information. It serves as the truck that the information is loaded on.
* It uses ethernet networks, cable networks, DSL networks amongst others to carrying out the process of moving information. The networks serve as the road to transport the information.
* Data is kept in boxes inside the IP, which is a lot like how personal information is kept in boxes inside a moving van. There are several levels of information in these boxes. The main system is IP, and then there is TCP or UDP data.
* Port numbers are important for moving data, but they are not a security tool. Changing port numbers can make it harder to reach services, but it doesn't automatically make them safer.
* Knowing how to use IP names and port numbers together makes it easier to send different kinds of data to the right services on devices. This mix makes it possible for different types of data (HTTP, VoIP, email) to get where they need to go.

**1.6 DHCP Overview (important for web traffic and web site communication)**

* In the beginning of TCP/IP, IP addresses, subnet masks, and other settings had to be set up by hand, which made it impossible for big networks to use. In 1993, BOOTP assigned IP addresses automatically, but it didn't complete setup. When DHCP came out in 1997, it made it possible for IP numbers to be automatically configured and leased.
* There are four steps in the DHCP process: Discovery, Offer, Request, and Acknowledgement. A device, like Sam's, sends a DHCP Discover message as a spread to look for an open IP address when it joins to the network. In response, the DHCP server sends a DHCP Offer message with an open IP address.
* As part of the DHCP process, Broadcasts are important for DHCP, but they can't go across subnets in big networks because of routers. By sending DHCP messages from local subnets to DHCP servers in other places, DHCP Relay or IP Helper can fix this problem. Users with this feature can get IP numbers from central DHCP servers on devices connected to different subnets.

**2.1 Networking Devices**

* A hub communicates data from one port to all other connections, acting as a basic Ethernet device and also known as a multi-port repeater. As OSI Layer 1 devices, hubs don't have the intelligence to make smart decisions about how to forward data. In a half-duplex system, they can either send or receive data, but not at the same time. This makes the network less efficient as traffic grows.
* At OSI Layer 3, routers use IP numbers to decide how to forward packets and join different IP subnets and types of networks, such as LAN to WAN or copper to fibre. Wireless Access Points (WAPs) are like links between wired Ethernet networks and 802.11 wireless networks. They decide which packets to send based on their MAC IDs and work at OSI Layer 2.
* As a more current option to hubs, switches work like bridges but decide which connections to forward based on MAC addresses in hardware (ASIC). At OSI Layer 2, switches can handle many ports and offer extra features like Power over Ethernet (PoE). Some switches can do both routing and switching. These are called Multilayer Switches, and they blend router and switch functions into one device.
* Repeaters make new signals and send them over copper or fibre links. This makes network lengths longer without having to decide which signals to send next. In OSI Layer 1, converters do similar things but over different types of media, like fibre to wire, and often over long distances. They allow different media to join and work with different structures.

**3.2 Plans and Procedures**

* In the field of information technology (IT), things are always changing. Devices like computers, firewalls, routers, and switches need to be upgraded, their configurations changed, and their software updated. Making changes is hard because they might affect network uptime and general availability. This shows how important it is to have an organised process for managing changes.
* Data safety and the right way to get rid of old tools are essential. Organisations must safely get rid of assets that hold private data while also following the law.
* Documented Standard Operating Procedures (SOPs) tell staff what to do when a device fails, there is downtime, there are issues with the building, or data needs to be deleted. They also help staff understand the rules and keep things consistent.
* When you hire third-party service providers, you need to make written deals that spell out what you expect from them. Service Level Agreements (SLAs) are contracts between customers and service providers that spell out the minimum service terms, such as uptime standards and reaction times.
* NDAs protect confidential talks and information shared with other parties. Trade secrets, private business operations, and sensitive data are protected by NDAs, which frequently include penalties for exposure.

**4.2 Social Engineering**

* Phishing is a typical cyberattack in which attackers send emails or texts pushing users to visit bogus websites or enter key credentials. Check the URLs in such mails and avoid clicking links to prevent being victimised. Phishing sites have content, visuals, or page authenticity issues, such as a different logo.
* Tailgating and piggybacking allow unauthorised workplace access. Tailgating occurs when an authorised person leaves a door open for an unauthorised person. To piggyback, an authorised individual lets someone without credentials in. Despite politeness, it's important to enforce rigorous access controls and allow only authorised people in.
* Shoulder surfing—viewing sensitive information on others' screens—is dangerous in offices and public settings like cafés and airports. Being mindful of surroundings, setting privacy filters on screens to minimise view to the person in front, and avoiding windows and corridors helps prevent it.
* Office buildings need visitor regulations, badges, or scanners to maintain security. Access control vestibules and airlocks allow just one person at a time. You must ask about unidentified people in the building.

**5.3 Software Tools**

* Wireless network monitoring needs software that catches airborne packets. Traffic from these instruments during analysis should not overload local receivers. Since many network drivers only show Ethernet data, wireless information may require additional hardware.
* Wireshark, a popular protocol analyser, displays Ethernet-level or application traffic in real time. Most operating systems can install it. I used this in my cybersecurity class, and it works well.
* These tools provide network traffic, signal strength, channel characteristics, and application communication. They can record and analyse network data for troubleshooting or discovering unknown activity.
* NetFlow gathers and delivers network data from probes or devices linked to network taps to track traffic patterns. NetFlow reports provide top traffic sources, conversation summaries, and application traffic.
* Basic tools like TFTP servers help transfer firmware or software files for device upgrades, while terminal emulators like SSH clients offer encrypted remote access to devices for configuration and file transfer. Different operating systems have these tools.