Name : Anele Sibiya
Student no. : 2024030412
Group : 3

**Networks 2A assignment**

**Content**

Question 1

1.1 Networking Frames are small packages of data that are transmitted over a network at the data link layer. (layer 3), which facilitates the connection of devices on the same network (such as Ethernet or Wi-Fi PCs). They ensure that data is supplied consistently and in the correct order. The 3 types of Network frames are :

1. Ethernet Frames
   Local area network (LAN s) are heavily based on ethernet frames. it starts with what is referred to as a preamble, a pattern initiated to let the device know what is being transmitted so that the sender and receiver are both on the same page. Each frame also includes the station and source MAC addresses, which are the unique hardware addresses of the sending and receiving devices on the network. type/ length, the type/length field comes next, the type/length field defines the protocol in use the use (these would be an IPv4 or IPv6) or amount of data payload in the datagram. the actual data being transmitted is kept in the payload, which holds the important information the sender wants to share. At the end of the frame is the frame check sequence (FCS) an error-detection feature that ensures data integrity during transmission

2. Wi-fi Frames
   Wi-Fi frames are crucial for wireless communication because they offer flexible frameworks ascending different kinds of data. A frame control field at the start of each frame indicates its kind and function such as the era control or management frames. In a shared wireless medium the duration or ID field is essential for preventing collisions and guaranteeing effective channel utilization. Up to four address Fields are allowed in Wi-Fi frames these fields control communication between the sender the recipient and any device acting as middlemen, such as excess points a sequence control field is Incorporated to keep things organized and monitor broken packets. The payload, which contains the data to be sent is the central components of the fame Wi-Fi flames and with an FCS, just like infinite frames do, can guaranteeing everything transmission

3. PPP Frames
   point to point connections as those made with dial-up modems or VPNs PPP frames are frequently utilized. The unique best sequence 0x7E, which designates the star and finish of the frame is used to encapsulate each frame at the beginning and conclusion the address and control fields are usually set to 0xFF and 0x03, respectively, since PPP only uses a single point or points link and does not need complicated addressing. The type of data payload being carried such as IPv4 or IPv6 packets, is identified by the protocol field the payload which comprises the actual data in television for transmission, is the frames primary content. At the end of the frame and FCS is included to verify the integrity of data and detect any transmission errors

1.2 The code of contemporary networking is TCP/IP or transmission control protocol/internet protocol, which permits data transmission and communication across networks, including the internet its layered

architecture which device communication into four separate layers - application, transport, internet and network interface - is one of its fundamental ideas. Every layer has a distinct purpose, guaranteeing modular, scalable, and methodical data transfer. end-to-end communication, which enables direct device interaction and guarantees that the transferred data is consistent and reaches the intended recipient is another essential element.

The internet protocol IP enables rooting and addressing, two essential TCP/IP functions. For identification and routing purposes, each device in a network is given a unique IP address. This makes it possible for data packets to travel across civil networks in yet find the best route to their destination. Additionally, ccp/ip places a strong emphasis on error management and dependability comma which are overseen by the transmission control protocol TCP. By using techniques including Returns missions, acknowledgments comma and error checking procedures, TCP guarantees data integrity, resulting in reliable and strong communication.

Because of it's interopility comma the protocol may function across a wide variety of networks and technological platforms, facilitating smooth system to system communication. Furthermore at scalability accommodate networks of all sizes, from modest local configurations to expensive international infrastructures such as the internet. Email services, file transfers, and online browsing are just a few of the many uses for TCP/IP full stop by supporting encrypted tunneling protocols, it also makes so cute connections possible, like those found in virtual private networks. TCP/IP is essential for effective, dependable, and worldwide networking because of this combination of ideas.

The differences between TCP and IP are :

| **TCP** | **IP** |
|---|---|
| connection based | connectionless |
| reliable data delivery | No reliability guarantee |
| breaks data into packets, assigns sequence numbers, and manages acknowledgments | treats each data packet independently without ensuring integrity |
| requests retransmission of lost or corrupted packets | does not engage in recovery actions |
| preferred for applications requiring assured and orderly data transfer (viz emails, file transfers, and web browsing) | suitable for scenarios prioritizing speed over reliability, such as video streaming and online gaming |

1.3. Assigning IP address: every equipment in the businesses network, including service, routers and clients devices, will be given a distinct IP address. Data packet identification in network routing are made easier by this IP addresses for stop the business may utilize public IP addresses for servers that are visible to the outside world and private IP addresses for its internal network

2. Data transport with TCP: TCP would provide dependable clients-server communication. It ensures that data packets are sent without loss or corruption and in the correct order. To ensure dates integrity, TCP would manage error checking, acknowledgments, and retransmissions of lost packets when users interact with the web services

3. Routing via IP: data packets are rooted from the client to the server based on the internet protocol IP, and vice versa. In this entails navigating routers, which effectively forward communications using IP addresses. IP routing guarantees that request from users in various geographic areas are rooted to the closest server if the business is International.

4. Application-layer protocol: http/https (Hypertext transfer protocol) is commonly used by web services to facilitate communication between servers and browsers. These protocols function at the TCP/IP model's application layer, depending on TCP at the transport layer to provide dependable with content delivery.

5. DNS Configuration: the business would set up a domain name system DNS to associate the IP addresses of the web service within tuning readable domain memes common such as www.com company name.com uses no longer have to know numerical IP addresses, making access easier.

6. Firewalls and Security measures: to save god the businesses web services, firewalls and other security measures are crucial. Synthesis information is safeguarded during transmission things to TCP/IPs capability for secure communication via protocols like TLS (transport layer security), which encrypts data.

7. Load balancers : the business could utilize low balances to split up incoming client request among several servers in order to increase scalability. This reduces server overloads and delays while guaranteeing effectively source use. Does procedure is made easier by TCP/IP, which smoothly manages sessions and routes connections.

8. Testing and Optimization : to guarantee performance and dependability, extensive testing of TCP/IP communication would be parts of the network configuration. Any possible problems can be found and fixed with the use of tools like packet analyzers common trace routers, and ping.

These actions will help the business builds a strong TCP IP foundation for its web services, guarantee secure comma scalable, and effective client-server communication.

Question 2.

2.1 Subnetting is the process of splitting a large network into smaller networks known as subnets. Subnets give every device group a dedicated area for communication, which eventually facilitates the smooth operation of the network as it improves the network's speed. Because each subnet can be monitored and managed independently, this also improves security and facilitate network management.

Ways subnetting would improve network performance for a company:

4. **Improve Network Performance and Speed**
   Since every device has a point of entry into the network, information sent out by a single broadcast packet reaches every device connected to that network. However, a high number of entry points might have a detrimental affect on the performance of your network as a whole as well as internetwork switching devices. Another issue is, a network's capacity may be strained to the point of collapsed by broadcast packets ability to spam every device connected to the network, including those unrelated to the task it hand. However subnetting makes it possible to guarantee that data stays within the broadcast domain or subnetted network, allowing additional subnets to operate as officially and quickly as possible. Additionally, subnetting separate the broadcast domains of your network, giving you more control over traffic flow and improving network performance.

5. **Reduce Network Congestion**
   Subnetting lessens congestion by ensuring the traffic intended for a device within a subnet remains in that subnet. You may lessen the burden of your network and improve traffic routing by placing subnets strategically. However, broadcast traffic and other information that doesn't require routing are not transferred to other subnets when a router is used to transfer traffic between subnets. Network congestion is lessened as a result of each subnet's speed increasing due to a decrease in traffic within it.

6. **Improved Security**
   by segmenting the network, you can more easily detect threads common block points of entry, and targets you replies by dividing your network into subnet and controlling the traffic flow with ACL's, QoS, o4 route-maps. By configuring ACLs on the routers and switches, you may also use routers to divide your network into subnets. Devices within a subnet can't access the entire network as a result full stop another choice is to restrict wireless clients access to resources common making sure that important data isn't readily available in far-off places.

7. **Easier Scalability**
   Submitting enhances scalability by enabling a network to expand in a needs, orderly, and effective manner. Subnetting separates the network into smaller segments, each of which is able to manage its own traffic, as opposed to packing more devices into a single comic expensive network. This keeps

performance high even as more users and devices are added by preventing network overload and lowering broadcast traffic. By resolving address ranges for upcoming departments, locations, or projects, subnetting also enables it teams to plan forward, enabling expansion without requiring a full network rebuilt. Whether the Firm expends to additional floors opens new offices, or at new teams, it is simple to construct and administer you subnets on its own. Additionally, because submits are segregated, certain network components can be upgraded or altered without affecting the system as a whole. All things Considered commerce submitting guarantee that a business's network will continue to be quick, well-structured, safe and simple to administer as it grows.

8. **Logical Structure**
   By making the network more structured, manageable, and troubleshootable, subnetting enhances network administration. Administrators can allocate various device groups to distinct regions, such as department, buildings, of functions, by splitting a big network into smaller, logical subnets. Because problems can frequently be localized to a particular subnet rather than examining the entire network, this topology enables faster issue discovery. Because each subnet can have its own set of rules and controls, also makes jobs like maintaining IP addresses, applying security policies, and monitoring traffic easier. It makes it possible to use resources like bandwidth and firewall rules more effectively and makes network expansions, upgrades, and modifications less complicated. All things considered, subnetting offers network managers more flexibility common clarity, and control, resulting in a more secure and reliable network environment.

2.2.

1. **Network Topology**

How devices and nodes are connected is determined by network topology. A thorough understanding of this aids in creating routing solutions that complement the organizational structure of the business, whether that be a decentralized mesh that directly connects departments or a centralized setup with a single hub. Effective data flow and seamless communication are guaranteed by a well designed topology and improved overall performance.

2. **Addressing scheme**

Using private IP ranges to prevent conflicts, designing a structured IP addressing strategy using subnets and address summarization puts departments into logical groups. This simplifies routing, facilitating the rapid detection and isolation of problems or IP conflicts between departments, keeps tables smaller and facilitating the seamless integration of future extensions.

3. **Scalability**

Network expansion, such as the inclusion of additional departments or increase in traffic, should be anticipated or managed by routing solutions without requiring significant redesigns. Because they automatically adjust to changes, This involves making plans for future expansions of departments, users, or distant locations without resulting in performance problems or overloading routing tables, dynamic routing protocols like OSPF (open shortest path first) and BGP (border gateway protocol) .etc are perfect for bigger networks. Long-term viability is ensured and expensive upgrades are avoided by designing with scalability in mind.

4. **Bandwidth Management**

Using quality of services (QoS) rules, efficient bandwidth management prioritizes the important data, such as final transactions or real-time communication by enabling dynamic bandwidth allocation, QoS enables administrators to avoid bottlenecks and guarantee equitable distribution among departments. This also reduces packet loss and latency by streamlining the network. Methods like route summarization and load balancing over several networks make sure data moves between departments in the quickest and most efficient way possible.

5. **Security Measures**

In interdepartmental routing, security is crucial as it limits which departments or devices can communicate, you can safeguard each department's network. Access controls can be enforced by routers to limit communication between HR and finance for example. VLANs enable traffic separation, while encryption reduces vulnerabilities by guaranteeing that interdepartmental data is private and cannot be altered. You can also employ firewalls and route filtering to stop unauthorized access and if required , to impose department isolation.

2.3 Many TCP/IP tools are frequently used in business to  diagnose network problems. These common ones are:

1. **Ping**

Ping is a straightforward yet crucial tool for determining whether units and a network are connected. It helps network managers find problems like whether a server or printer is reachable on the network and packet loss or latency by issuing ICMP echo queries two a particular IP address or host name and waiting for a response. This utility ensures dependable communication across systems and is especially helpful and resolving situations they want device cannot access another.

2. **Traceroute**

Another useful tool for tracking the precise route data takes from the source to get to the destination is Traceroute. It assists and identifying delays or malfunctions in certain routers on network signals by

providing information about each hop along the route and recording the time spent on each hop, including IP addresses. This is especially useful for locating packet delays or drops in the network, and detecting bottlenecks.

3. **Netstat**

Lastly, Netstat offers comprehensive information about a device's listening ports and all active network connections. Administrators can keep an eye on network traffic, sport anonymous activity, and resolve connection problems by viewing statistics for the TCP and UDP protocols. Because of this, Netstat is a vital tool for preserving network security and performance inside an organization.

Question 3.

3.1 Differences between wired and wireless networks :

9. **Speed and Reliability**
   Wired networks are generally faster and more reliable than wired ones. This is due to the fact that connected networks transfer data via actual wires, which can offer a more reliable connection with lower interference. conversely, wireless networks use radio waves to transfer data, and these waves can be impacted by several elements like distance, obstructions, and device interference.

10. **Installation and setup**
    Wired setups are more complex and time-consuming due to cabling, while wireless is easier. It can be a difficult undertaking to run cables throughout your house or workspace when using a Wired network, particularly if you have several devices that need to be linked. Conversely, establishing a wireless network is comparatively more convenient and easy. You can connect numerous devices to the network using a wireless router.

11. **Cost**
    Wired networks are typically more expensive initially due to hardware and potential installation costs, whereas wireless is often more cost-effective to start. In addition, if you need to engage a professional to set up the network for you, the cost of installation may also be higher. However, since all you need to get started is a wireless router, wireless networks are more affordable. To guarantee sufficient coverage across your house or workspace, you might need to spend more money on extra devices like access points or range extenders.

12. **Security**
    Wired networks are generally considered more secure as they require physical access, while wireless networks are more susceptible to hacking or illegal access, as wireless networks are more vulnerable

to interception over airwaves, although they can be secured with encryption like WPA3 and other techniques, like employing strong password and authentication improve security.

13. **Flexibility and Mobility**
    Wireless networks offer greater flexibility and mobility, ideal for mobile devices like laptops, tablets, and cellphones. Without being constrained by cables, a wireless network allows you to access the internet from any location within its coverage area, while wired networks require a physical cable connection, they are less adaptable and movable. If you have to move around while accessing the internet  this could be a restrictive.
14. **Scalability**
    Wired networks can be more scalable for adding devices since more devices may be added to the network with ease by connecting them via cables, because of this wired networks are perfect for big homes or companies where a lot of devices need to be connected. while wireless scalability can be challenging due to potential congestion and slower rates, although solutions like access points and range extenders exists.

A comparison of Wi-fi 5 and Wi-fi 6 standards :

| **Feature** | **Wi-fi 5 (802.11ac)** | **Wi-fi (802.11ax)** |
|---|---|---|
| Release Year | 2014 | 2020 |
| Frequency bands | 5 GHz only | 2.4 GHz and 5 GHz |
| Speed | Up to 6.9 Gbps | Up to 9.6 Gbps |
| Efficiency | Limited support for multiple devices | Handles more devices efficiently with OFDMA and improved MU-MIMO |
| Latency | Higher latency | Lower latency |
| Battery Life | Regular | Better power saving |
| Security | WPA2 | WPA3 |
| Network Congestion | Struggles with lots of devices | Designed for dense environments (viz smart homes, offices) |
| Compatability | Works with older Wi-fi devices | Backward compatible, but benefits best with Wi-fi 6 devices |

3.2.

**Security Implications:**

1. **Increased Attack Surface** - When employees connect remotely, the organization's network expands beyond the traditional office boundaries. This makes it harder to control and monitor all access points. Every remote connection—even just one laptop or mobile device—can open the door to cyber threats if it's not properly secured.

2. **Unsecured Networks -** People working from home or in public places often use Wi-Fi networks that aren't secure. If those connections aren't protected with encryption or a VPN, sensitive data can be intercepted by hackers—especially through attacks like "man-in-the-middle" that eavesdrop on your traffic.

3. **Device Security Risks -**When employees use personal or unmonitored devices to connect remotely, those devices might not have the right protections—like firewalls, antivirus software, or regular updates. That makes them easier targets for malware or hackers, which could put the whole company network at risk.

4. **Weak Authentication and Access Control -** If strong login security—like multi-factor authentication (MFA)—isn't in place, it becomes easier for attackers to guess passwords or steal login details. And if access permissions aren't set up properly, users might accidentally be given more access than they actually need, which increases the risk of a security breach.

5. **Data Leakage and Loss** - When employees work remotely, sensitive company data might be saved on personal devices or sent over unsecure channels. This makes it easier for information to be accidentally leaked or intentionally stolen—especially if there aren't strong protections or proper monitoring in place.

**Measures to mitigate risks**

1. **Wider Attack Surface** - As employees connect from home, coffee shops, or on the go, the organization's network is no longer confined to the office—it's everywhere. This expanded perimeter can be hard to keep track of, and every device or access point becomes a potential target for attackers. To reduce this risk, companies should adopt a Zero Trust approach, which means no device or user is automatically trusted. They should also limit access only to what's necessary for each person's role and regularly monitor remote connections to catch suspicious activity early.

2. **Unsecured Networks** -Remote workers often rely on public or home Wi-Fi networks that aren't as secure as a company's internal systems. If someone connects over an unprotected network, sensitive data could be intercepted without them even knowing—especially if there's no encryption in place. One effective way to counter this is by requiring employees to use a VPN, which creates a secure tunnel for data. Training staff to avoid using public Wi-Fi and encouraging them to use personal hotspots or secured connections can also make a big difference.

3. **Device Security Risks** - Not everyone uses a company-issued laptop when working remotely—many rely on personal devices. These devices might lack key protections like antivirus software, firewalls,

or regular updates. That leaves them open to malware and cyberattacks, which can then spread to the company's systems. To manage this risk, companies should either provide secure, pre-configured devices or use Mobile Device Management (MDM) tools to ensure personal devices meet company security standards. Regular updates and security software should be non-negotiable.

4. **Weak Authentication and Access Control** - When logging in remotely, weak passwords and poor access controls can make it easy for attackers to break in using stolen or guessed credentials. If users are given more access than they actually need, the damage can be even worse. The best way to strengthen this is by enforcing Multi-Factor Authentication (MFA) for all remote access. It adds an extra layer of protection even if a password is compromised. Companies should also review user permissions regularly to ensure no one has access to information or systems they don't need.

5. **Data Leakage and Loss** - Working remotely often means data is accessed or stored on local devices, or sent through apps and tools that may not be secure. This creates a real risk of data being leaked—either accidentally or on purpose. To prevent this, sensitive information should always be encrypted, whether it's being stored or shared. It's also important to use Data Loss Prevention (DLP) tools that can detect and block risky behavior, like uploading confidential files to unauthorized platforms. Encouraging secure cloud storage rather than local saving helps reduce the chances of data loss.

3.3

| **Aspect** | **SD-WAN** | **MPLS** | **Traditional Leased Lines** |
|---|---|---|---|
| **Definition** | Uses Software Defined Networking principles. | Uses traditional WAN technology with dedicated circuits | Provides point-to-point dedicated communication with guaranteed bandwidth. |
| **Cost** | More cost-effective and cheaper than MPLS. | More costly than SD-WAN. | Extremely expensive due to exclusive use and maintenance costs. |
| **Control** | Controlled via software-defined networking. | Controlled through provider-managed networks. | Fully controlled by the organization, offering complete autonomy. |
| **Flexibility** | Offers high flexibility and support multiple connection types. | Provide limited flexibility and supports fewer connection types | Very rigid with minimal flexibility in terms of expansions. |
| **Performance** | Helps eliminate network congestion issues. | Can suffer from network congestion in certain scenarios. | Provides consistent, high-speed performance with no congestion. |

| | | | |
|---|---|---|---|
| **Implementation** | Easy to set up and deploy. | Hard to set up, requiring more time and expertise. | Complex and time-consuming to establish due to dedicated infrastructure. |
| **Security** | Provides more security features than MPLS. | Less secure than SD-WAN but still reliable. | Highly secure, as it offers dedicated communication without shared infrastructure |
| **Scalability** | Easily scalable, supports adding or removing connections dynamically. | Not easily scalable, requires dedicated circuits for new locations. | Difficult to scale, requiring separate leased lines for each site. |

**References**


1. Tanenbaum, A.S, & Wetherall, D.J (2011). Computer Networks. Pearson
2. Postel, J. (1981). Internet Protocol. https://tools.ietf.org/html/rfc791
3. Olifer, N, & Olifer, V (2006). Computer Networks: Principles, Technologies and Protocols for Network Design. Willey
4. Forouzan, B.A (2017) Computer Networking: A top-down approach. Pearson.
5. Stewart, J (2014). Routing Protocols and Concepts : CCNA exploration companion guide.
6. Kerosene, J.F, & Ross, K.W (2021). Computer Networking: A top-down approach. Pearson.
7. Simpson, W. (1994). The Point-to-point Protocol (PPP). https://tools.ietf.org/html/rfc1661
8. Cisco systems. (2021). Cisco Wirelss LAN design guide. Cisco Press.
9. Grag, V.K. (2010). Wireless communication & Networking. Morgan Kaufmann.
10. Goldsmith, A. (2005). Wireless communications. Cambridge University Press.