**1a) Explain the following terms;**

**i)Subnet mask**

A subnet mask is a 32-bit number that divides an IP address into two parts which include the network portion and the host portion. It helps determine the network and which part identifies the device (host) on the network. For example in the IP address 192.168.1.10 a common subnet mask is 255.255.255.0

In binary this subnet mask is in form of zeros (0s) and ones (1s). The ones(1s) indicate the network part and the zeros(0s) indicate the host part.

**ii)Subnetting**

Is the process of dividing a larger network into smaller, more manageable sub-network (subnets). This technique allows for better organization, improved performance and enhanced security within a network by creating subnets, network administrators can;

Efficiently use the IP addresses by allocating them based on the needs of different departments or functions.

Reduce network congestion as broadcast traffic is limited to smaller subnets.

Enhance security by isolating different segments of a network.

Subnetting involves using different subnet masks to create subnets within a larger network.

**bi) Explain the various steps considered when subnetting.**

**Determine the Network Requirement**

Identify the need of subnetting in order to improve the performance, enhance security or manage IP address space.

Estimate the number of subsets in order to know the organization needs.

**Choose an IP addressing scheme**

Select the IP addressing class which decide if you’re using class A, B, or C address based on the size of the network.

**Determine subnet Mask.**

Calculate subnet Mask that is decide how many bits will be used for the subnet mask, this will determine the number of subnets and hosts per subnet.

**Calculate subnet Addresses**

Identify subnet Addresses involves using the subset mask to determine the range of addresses for each subnet

**Assign subsets and IP Addresses.**

Involves distributing subnets which allocate the subnets to different departments or geographical locations based on needs.

Also document the allocation of IPs which have been assigned to which subnet.

**Test and implement**

Configuration; configure routers and switches with the new subnet settings

Testing; verify connectivity between subnets and ensure the devices can communicate as expected

**Monitor and Adjust**

Monitor Network performance; keep an eye on network performance and usage

Adjust as needed due to growth and changing need of network.

**ii) State and explain the benefit of subnetting.**

**Improved Network Management**

Subnetting allows for better organization of IP addresses making it easier to manage large networks.

Isolation that is by isolating different segments of the network, it’s easier to monitor and control traffic.

**Enhanced security**

Access control; different subnets can have different security policies, allowing for more granular control over who can access sensitive data.

Reduced Broadcast Traffic subnetting limits the size of broadcast domain, reducing the risks of broad cast storms and making it harder for attackers to access all devices on the network.

**Easier Troubleshooting**

Localized issues; problems can be isolated to specific subnets making it easier to identify and resolve issues without impacting the entire network

**Improved performance**

Reduced congestion; smaller subnets reduce network congestion by limiting the number of devices that compete for bandwidth within a broadcast domain.

Faster Routing; Routers can make more efficient routing decisions with fewer subnetworks, teaching to improve overall network performance

**Facilitate Network design**

Scalability; subnetting provides a framework that makes it easier to expand the network as needed without disrupting existing services

**2a) What do you understand by the term Network Troubleshooting in Network problems?**

Network Troubleshooting refers to the systematic process of diagnosing and resolving issues within a computer network. It involves identifying the source of a problem, analyzing the symptoms and implementing solutions to restore normal network operation.

Troubleshooting facilitates in testing and verification that is testing tools using ping, traceroute and network analyzer to test connectivity and performance.

Troubleshooting facilitates in preventive measures such as helps regular maintenance that is implementing routine checks and updates to prevent issues before they arise.

**b) Explain the steps observed when Troubleshooting in Network problems.**

**Identify the problem**

Collect details about the issue which involves gathering information including the type of problem, affected devices and error messages

Clearly define the problem statement including the scope and impact of the issue.

**Gather the information and resources**

Network documentation; review network diagrams, configuration files and other relevant document.

Network monitoring tools; utilize tools like packet sniffers, network analyzers and system logs to gather data

**Isolate the problem**

Divide and conquer; breakdown the problem into smaller manageable parts.

Eliminate possibilities; systematically rule out potential causes starting with the most likely.

**Analyze Data and identify the Root cause**

Analyze logs and data that is examine network logs, system logs and other data to identify patterns and anomalies

Apply troubleshooting techniques such as packet analysis, network tracing and configuration reviews.

Consult experts and resources which involves seeking guidance from colleagues online forums or vendor documentation.

**Develop and Implement a solution**

This involves creating a plan based on the root cause, step- by-step plan to resolve the issue

Implement the solution by applying the planned changes which may involve configuration adjustments, software updates or hardware repairs.

Verify the solution by testing the solution to ensure the problem is resolved

**Document and Review**

Document the solution that record the steps taken for the solution to be implemented and any lessons learnt

Review and refine that is conduct a post incident reviews to identify areas for improvement and refine troubleshooting processing.

**Prevent Future Occurrences**

Implement preventive measures; apply changes to prevent similar issues from arising in the future.

Monitor and maintain; regularly monitor the network and perform maintenance tasks to ensure continued stability and performance.