Competency Based Learning Material (CBLM)

IT Support Services

Level-4

Module: Performing Advanced Networking

Code: CBLM-OU-ICT-ITSS-03-L4-V1

National Skills Development Authority
Prime Minister's Office
Government of the People's Republic of Bangladesh

Copyright

National Skills Development Authority
Prime Minister's Office
Level: 10-11, Biniyog Bhaban,
E-6 / B, Agargaon, Sher-E-Bangla Nagar Dhaka-1207, Bangladesh.
Email: ec@nsda.gov.bd
Website: www.nsda.gov.bd.
National Skills Portal: http:\\skillsportal.gov.bd

This Competency Based Learning Materials (CBLM) on "Performing Advanced Networking" under the IT support services, Level-4" qualification is developed based on the national competency standard approved by National Skills Development Authority (NSDA)

This document is to be used as a key reference point by the competency-based learning materials developers, teachers/trainers/assessors as a base on which to build instructional activities.

National Skills Development Authority (NSDA) is the owner of this document. Other interested parties must obtain written permission from NSDA for reproduction of information in any manner, in whole or in part, of this Competency Standard, in English or other language.

It serves as the document for providing training consistent with the requirements of industry in order to meet the qualification of individuals who graduated through the established standard via competency-based assessment for a relevant job.

This document has been developed by NSDA with the assistance of related specialist/trainer /related employee

Public and private institutions may use the information contained in this CBLM for activities benefitting Bangladesh.

Approved by _____ th Authority meeting held on .....

How To Use This Competency Based Learning Material (CBLM)

The module, "Performing Advanced Networking" contains training materials and activities for you to complete. These activities may be completed as part of structured classroom activities or you may be required you to work at your own pace. These activities will ask you to complete associated learning and practice activities in order to gain knowledge and skills you need to achieve the learning outcomes.

1. Review the **Learning Activity** page to understand the sequence of learning activities you will undergo. This page will serve as your road map towards the achievement of competence.

2. Read the **Information Sheets.** This will give you an understanding of the jobs or tasks you are going to learn how to do. Once you have finished reading the **Information Sheets** complete the questions in the **Self-Check.**

3. **Self-**Checks are found after each **Information Sheet**. **Self-Checks** are designed to help you know how you are progressing. If you are unable to answer the questions in the **Self-Check** you will need to re-read the relevant **Information Sheet**. Once you have completed all the questions check your answers by reading the relevant **Answer Keys** found at the end of this module.

4. Next move on to the **Job Sheets. Job Sheets** provide detailed information about *how to do the job* you are being trained in. Some **Job Sheets** will also have a series of **Activity Sheets**. These sheets have been designed to introduce you to the job step by step. This is where you will apply the new knowledge you gained by reading the Information Sheets. This is your opportunity to practice the job. You may need to practice the job or activity several times before you become competent.

5. Specification **sheets**, specifying the details of the job to be performed will be provided where appropriate.

6. A review of competency is provided on the last page to help remind if all the required assessment criteria have been met. This record is for your own information and guidance and is not an official record of competency

When working though this Module always be aware of your safety and the safety of others in the training room. Should you require assistance or clarification please consult your trainer or facilitator.

When you have satisfactorily completed all the Jobs and/or Activities outlined in this module, an assessment event will be scheduled to assess if you have achieved competency in the specified learning outcomes. You will then be ready to move onto the next Unit of Competency or Module

Table of Contents

Module Content

Unit of Competency	**Perform Advanced Networking**
Unit Code	**OU-ICT-ITSS-03-L4-V1**
Module Title	**Performing Advanced Networking**
Module Descriptor	This module covers the knowledge, skills and attitude required to perform advanced networking. It includes the task of planning for an advanced network, performing subnetting, configuring advance network services and protocol, configuring routing, testing newly created network and maintaining record of maintenance.
Nominal Hours	100 Hours
Lerning Outcome	After completing the practice of the module, the trainees will be able to perform the following jobs: 1. Plan for an advanced network 2. Perform subnetting 3. Configure advance network services and protocol 4. Configure routing 5. Test newly created network 6. Maintain record of maintenance

Assessment Criteria:

1. Organizational requirements to create advanced network are collected
2. Required tools, equipment's and component, are identified and listed
3. Materials and consumables are identified listed
4. Network design plan is approved by authorize person
5. Subnetting is interpreted
6. Range of IP address is identified and selected
7. Subnet mask is identified and selected
8. Subnetting is performed
9. According to the approved network design plan network is established
10. Network simulation tools are installed
11. Required Network services are identified
12. IP addresses is determined
13. VLAN is configured as per design plan
14. Dynamic Trunk protocol is applied if required
15. Spanning Tree protocol is identified and configured
16. Services of network is identified and configured
17. IP routing is interpreted
18. Routing protocol is interpreted

19. Types of routing is interpreted
20. Terms of routing is interpreted
21. Routing services is configured
22. Bandwidth management is performed as per requirement
23. Network performance is monitored using monitoring tools
24. Congestion of the network is observed
25. Reachability to the internet (if available) is tested
26. Network maintenance plan is completed.
27. Network maintenance plan is approved by the appropriate person or from the organization
28. Approved network maintenance plan is documented
29. Support plan for the network is documented
30. User manual for the network is prepared.

Learning Outcome-1: Plan for an Advanced Network

Assessment Criteria	1. Organizational requirements to create advanced network are collected 2. Required tools, equipment's and components are identified and listed 3. Materials and consumables are identified listed 4. Network design plan is approved by authorize person
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker 9. Internet Facilities
Contents	1. Procedure to collect organizational requirements to create advance networking 2. Network tools, equipment's, and component Internet ▪ Crimping tools ▪ UTP cable ▪ Cable tester ▪ Rj-45 connector ▪ Switch ▪ Router ▪ ONU/ Media converter 3. Materials and consumables 4. Procedure to prepare advance network design plan
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-1: Plan for an Advanced Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Plan for an advanced network"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Plan for an advanced network"	1. Read Information sheet 1: Plan for an advanced network 2. Answer Self-check 1: Plan for an advanced network 3. Check your answer with Answer key 1: Plan for an advanced network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	4. Job/Task Sheet and Specification Sheet Task Sheet 1.1: Prepare a plan for an advanced network Specification Sheet 1.1: Prepare a plan for an advanced network Task Sheet 1.2: Prepare a plan for an advanced network

fInformation Sheet-1: Plan For an Advanced Network

Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

1.1 Procedure to collect organizational requirements to create advance networking
1.2 Advanced network tools, equipment's, and component Internet
- Crimping tools
- UTP cable
- Cable tester
- Rj-45 connector
- Switch
- Router
- ONU/ Media converter

1.3 Materials and consumables
1.4 Procedure to prepare advance network design plan

2.1 Procedure to collect organizational requirements to create advance networking

Collecting organizational requirements to create an advanced networking solution involves several key steps to ensure that the solution aligns with the organization's goals, objectives, and technical needs. Here's a procedure to guide you through the process:

1. **Identify Stakeholders:**
   - Determine the key stakeholders who will be involved in the networking project, including executives, IT managers, network administrators, and end-users.
2. **Conduct Initial Meetings:**
   - Schedule meetings with stakeholders to discuss the organization's goals, objectives, and challenges related to networking.
   - Gather insights into the current network infrastructure, including strengths, weaknesses, and areas for improvement.
3. **Assess Business Needs:**
   - Identify the business drivers and requirements that will influence the design of the advanced networking solution.
   - Determine the organization's growth plans, scalability requirements, compliance needs, and budget constraints.
4. **Define Technical Requirements:**

- Work with IT teams to define the technical requirements for the advanced networking solution, considering factors such as bandwidth requirements, security needs, reliability, and performance.

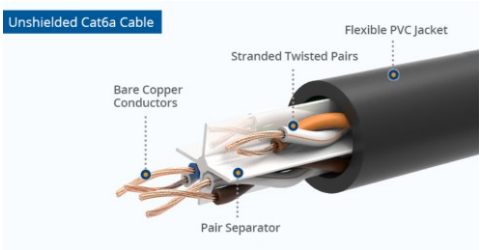
5. **Perform Network Audit:**
   - Conduct a thorough audit of the existing network infrastructure to assess its capabilities and limitations.
   - Identify areas of congestion, bottlenecks, security vulnerabilities, and outdated equipment that need to be addressed.
6. **Gather User Input:**
   - Solicit feedback from end-users and departmental managers to understand their specific networking needs and pain points.
   - Identify any specialized applications or services that require specific network configurations or optimizations.
7. **Research Best Practices and Technologies:**
   - Research industry best practices, emerging trends, and advanced networking technologies that can address the organization's requirements and objectives.
   - Consider technologies such as software-defined networking (SDN), virtualization, cloud networking, and network automation.
8. **Evaluate Vendor Solutions:**
   - Research and evaluate vendor solutions and products that align with the organization's requirements and technical specifications.
   - Consider factors such as product features, scalability, interoperability, support services, and total cost of ownership (TCO).
9. **Create Requirements Documentation:**
   - Document the organizational requirements, business objectives, and technical specifications for the advanced networking solution.
   - Create a comprehensive requirements document that serves as a roadmap for the design, implementation, and evaluation of the solution.
10. **Review and Validate Requirements:**
    - Review the requirements documentation with stakeholders to ensure alignment with business goals and technical needs.
    - Validate the requirements against industry standards, best practices, and feasibility considerations.
11. **Obtain Approval and Funding:**
    - Present the requirements documentation to executive management for approval and funding.

- Secure buy-in from decision-makers and allocate resources for the implementation of the advanced networking solution.

12. Iterate and Refine:

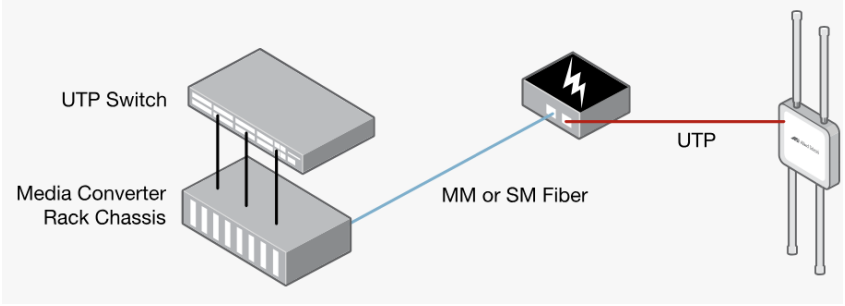
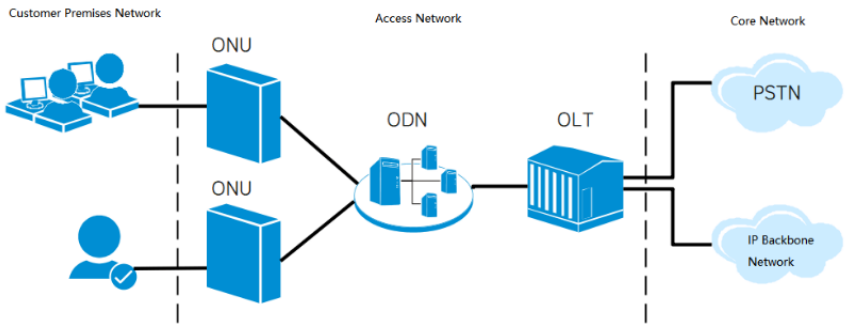
- Continuously iterate and refine the requirements based on feedback, changes in business priorities, and emerging technologies.
- Collaborate with stakeholders throughout the process to ensure that the advanced networking solution meets the organization's evolving needs.

2.2 Network tools and equipment's:

Tools and equipment's Name	Description	Image
Crimping tool	A crimping tool is a handy device that allows you to create secure connections between wires and connectors. It works by deforming the connector onto the wire, ensuring a strong bond. With a crimping tool, you can easily join electrical wires, network cables, coaxial cables, and more.	
UTP cable	UTP cable is a type of copper cable widely used for networking purposes. UTP cables consist of pairs of insulated wires that are twisted together to reduce interference and crosstalk.	
Cable tester	Network cable testers are designed to test the connectivity of the cables. They can check if a properly wired connection is available from one end of the cable to the other. Some advanced models can even measure the cable length, identify open circuits, short circuits, or reversed connections.	

2.3 Component for Networking

Tools and equipment's Name	Description	Image
RJ-45 connector	The eight-pin RJ45 connector is a standardised interface which often connects a computer to a Local Area Network (LAN). This type of connector was originally developed for telephone communications but is now used in a range of applications. The abbreviation, RJ45, stands for Registered Jack-45.	
Switch	A network switch allows two or more IT devices to communicate with one another. In addition to connecting to end devices like PCs and printers, switches may be connected to other switches, routers, and firewalls, all of which can provide connectivity to additional devices.	
Router	A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.	
Media converter	A media converter is a networking device that connects two different media, like Ethernet copper and Ethernet fiber. Typically, they connect devices that are beyond 100 meters from the nearest available switch.	

<table>
<tr><td></td><td colspan="2"> 
</td></tr>
<tr><td rowspan="2">Optical Network Unit (ONU)</td><td>ONU refers to optical network unit. It is the optical terminal device in the fiber access network, which provides users with multiple service interfaces. The network side of ONU is the optical interface. As for the user side, it's the electrical interface.</td><td> 
</td></tr>
<tr><td colspan="2"> 
</td></tr>
</table>

2.4 Materials and consumables for Networking

The bellow items are essential for building and maintaining network infrastructure.

Materials:

- Networking Devices (Routers, Switches, Access Points)
- Networking Cables (Ethernet, Fiber Optic, Coaxial)
- Networking Equipment Enclosures (Patch Panels, Cable Management)
- Networking Tools (Cable Testers, Crimping Tools)
- Networking Hardware (NICs, PoE Injectors, Transceivers)

Consumables:

- Networking Connectors (RJ45, LC, SC, ST)
- Patch Cables (Ethernet, Fiber Optic, Coaxial)
- Cable Management Supplies (Cable Ties, Labels)
- Networking Consumables (Adapters, Power Cables)
- Cleaning Supplies (Fiber Optic Cleaning Kits, Contact Cleaner)

2.5 Procedure to prepare advance network design plan

Preparing an advanced network design plan involves several steps to ensure that the network meets the organization's requirements and objectives. Here's a procedure to guide you through the process:

1. **Define Project Scope and Objectives:**

   Identify the scope of the network design project, including the goals, objectives, and desired outcomes.

   Determine the specific requirements and constraints that will shape the design, such as budget, timeline, and technical considerations.

2. **Gather Requirements:**

   Conduct stakeholder interviews and workshops to gather requirements from key stakeholders, including executives, IT managers, and end-users.

   Document functional and technical requirements, considering factors such as bandwidth, scalability, security, and performance.

3. **Conduct Network Assessment:**

   Perform a thorough assessment of the existing network infrastructure to understand its capabilities, limitations, and areas for improvement.

   Identify bottlenecks, security vulnerabilities, and other issues that need to be addressed in the new design.

4. **Develop Network Architecture:**

   Design a network architecture that aligns with the organization's requirements and objectives.

   Define the overall network topology, including the placement of routers, switches, access points, and other networking devices.

   Consider redundancy, scalability, and fault tolerance in the design to ensure high availability and reliability.

5. **Select Technologies and Solutions:**

   Research and evaluate advanced networking technologies and solutions that can meet the requirements of the network architecture.

   Consider factors such as performance, scalability, interoperability, security, and ease of management when selecting technologies.

6. **Design Security Framework:**

   Develop a comprehensive security framework to protect the network infrastructure from cyber threats and attacks.

   Implement security controls such as firewalls, intrusion detection and prevention systems (IDPS), access control lists (ACLs), and encryption.

7. **Plan for Network Management and Monitoring:**

   Define network management and monitoring processes to ensure the ongoing operation, performance, and security of the network.

   Implement network management tools and solutions for configuration management, performance monitoring, and troubleshooting.

8. **Create Implementation Plan:**

   Develop a detailed implementation plan that outlines the steps, tasks, and timeline for deploying the network design.

   Assign responsibilities to team members and stakeholders, and establish communication channels for coordination and updates.

9. **Test and Validate:**

   Conduct thorough testing and validation of the network design before deployment.

   Perform network performance testing, security assessments, and interoperability testing to identify and address any issues or concerns.

10. **Deploy and Monitor:** - Deploy the network design according to the implementation plan, ensuring minimal disruption to operations. - Monitor the network closely during the deployment phase and post-deployment to identify and address any issues or performance bottlenecks.

11. **Provide Training and Documentation:** - Provide training to network administrators, IT staff, and end-users on how to use and manage the new network infrastructure. - Develop comprehensive documentation, including network diagrams, configuration guides, and troubleshooting procedures.

12. **Review and Iterate:** - Review the performance and effectiveness of the network design regularly. - Gather feedback from stakeholders and end-users, and iterate on the design as needed to optimize performance and address evolving requirements.

Self-Check-1: Plan for an Advanced Network

1. What is the purpose of network cable testers?

Answer

2. What additional functionalities can advance network cable testers offer?
Answer

3. What is the primary function of an eight-pin RJ45 connector?
Answer

4. Question: What does the abbreviation "RJ45" stand for?

Answer

5. What types of devices can a network switch connect to?
Answer

6. What is the main purpose of connecting switches to other switches, routers, and firewalls?
Answer

7. What are the primary functions of a router?
Answer

8. What types of networks or subnetworks does a router typically connect?

Answer

9. What is the purpose of a media converter?
Answer

10. What scenario might require the use of a media converter?
Answer

Answer Key-1: Plan for an Advanced Network

1. **What is the purpose of network cable testers?**

   Answer: Network cable testers are used to test the connectivity of cables and ensure that a properly wired connection is available from one end of the cable to the other.

2. **What additional functionalities can advance network cable testers offer?**
   Answer: Advanced network cable testers can measure cable length and identify issues such as open circuits, short circuits, or reversed connections.

3. **What is the primary function of an eight-pin RJ45 connector?**
   Answer: The primary function of an eight-pin RJ45 connector is to provide a standardized interface for connecting devices, often used to connect computers to a Local Area Network (LAN).

4. **Question: What does the abbreviation "RJ45" stand for?**
   Answer: The abbreviation "RJ45" stands for Registered Jack-45.

5. **What types of devices can a network switch connect to?**
   Answer: A network switch can connect to end devices like PCs and printers, as well as other switches, routers, and firewalls.

6. **What is the main purpose of connecting switches to other switches, routers, and firewalls?**
   Answer: The main purpose is to provide connectivity to additional devices and manage traffic between different networks or subnetworks.

7. **What are the primary functions of a router?**
   Answer: The primary functions of a router are managing traffic between packet-switched networks by forwarding data packets to their intended IP addresses and allowing multiple devices to use the same Internet connection.

8. **What types of networks or subnetworks does a router typically connect? Answer 2: A** router typically connects two or more packet-switched networks or subnetworks.

9. **What is the purpose of a media converter?**
   Answer: The purpose of a media converter is to connect two different media types, such as Ethernet copper and Ethernet fiber.

10. **What scenario might require the use of a media converter?**
    Answer: Media converters are typically used to connect devices that are beyond 100 meters from the nearest available switch, where traditional Ethernet cables are not feasible.

Task Sheet-1.1: Prepare a Plan for an Advanced Network

Performance Objective: At the end of this task, the trainee should be able to Plan for an advanced network.

Working steps:

Step 1: Introduction

- Briefly introduce the topic of interpreting the functions of a SOHO network.
- Highlight the importance of understanding the core functions of SOHO networks for effective network design and management.

Step 2: Define Project Scope and Objectives:

- Identify the scope of the network design project, including goals, objectives, and desired outcomes.
- Document specific requirements, constraints, and considerations that will shape the design.

Step 3: Gather Requirements:

- Conduct stakeholder interviews and workshops to gather requirements from key stakeholders.
- Document functional and technical requirements, including bandwidth, scalability, security, and performance.

Step 4: Conduct Network Assessment:

- Perform a thorough assessment of the existing network infrastructure to understand capabilities, limitations, and areas for improvement.
- Identify bottlenecks, security vulnerabilities, and other issues to be addressed in the new design.

Step 5: Develop Network Architecture:

- Design a network architecture aligned with organizational requirements and objectives.
- Define network topology, including placement of routers, switches, access points, and other devices.
- Consider redundancy, scalability, and fault tolerance to ensure high availability and reliability.

Step 6: Select Technologies and Solutions:

- Research and evaluate advanced networking technologies and solutions.
- Consider factors such as performance, scalability, interoperability, security, and management ease.

Step 7: Design Security Framework:

- Develop a comprehensive security framework to protect the network infrastructure.
- Implement security controls such as firewalls, intrusion detection, access control, and encryption.

Step 8: Plan for Network Management and Monitoring:

- Define network management and monitoring processes to ensure ongoing operation, performance, and security.
- Implement tools and solutions for configuration management, performance monitoring, and troubleshooting.

Step 9: Create Implementation Plan:

- Develop a detailed implementation plan outlining steps, tasks, and timeline for deployment.
- Assign responsibilities and establish communication channels for coordination and updates.

Step 10: Test and Validate:

- Conduct thorough testing and validation of the network design before deployment.
- Perform network performance testing, security assessments, and interoperability testing.

Step 11: Deploy and Monitor:

- Deploy the network design according to the implementation plan, minimizing disruption.
- Monitor the network closely during deployment and post-deployment to address issues.

Step 12: Provide Training and Documentation:

- Provide training to network administrators, IT staff, and end-users on network usage and management.
- Develop comprehensive documentation, including diagrams, guides, and procedures.

Step 13: Review and Iterate:

- Review network performance regularly and gather feedback from stakeholders.
- Iterate on the design to optimize performance and address evolving requirements.

Specification Sheet-1.1: Plan for an Advanced Network

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1	Network assessment tools (e.g., Wireshark, SolarWinds Network Performance Monitor)	No.	1
2	Design software (e.g., Cisco Packet Tracer, Microsoft Visio)	No.	1
3	Security assessment tools (e.g., Nessus, Nmap)	Set	1
4	Network management and monitoring tools (e.g., Nagios, PRTG Network Monitor)	No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Networking hardware (routers, switches, access points, firewalls)	No.	1
2	Servers and storage devices (for network services and data storage)	No.	1
3	Network testing equipment (cable testers, network analyzers)	No.	1
4	Power distribution units (PDUs) and uninterruptible power supplies (UPS)	No.	1
5	Workstations and laptops for network administrators and designers	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	Network cables (Ethernet, fiber optic)	Meter	10
2	Mounting hardware (racks, cabinets, shelves)	Set	1
3	Patch panels and cable management accessories	No.	10
4	Power cords and adapters	No.	10
5	Labels and markers for equipment and cables	No.	20

Learning Outcome-2: Perform Subnetting

Assessment Criteria	1. Subnetting is interpreted. 2. Range of IP address is identified and selected. 3. Subnet mask is identified and selected. 4. Subnetting is performed. 5. According to the approved network design plan network is established.
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker • Internet Facilities 9. Whiteboard and Marker
Contents	1. Subnetting 2. Subnetting technique 3. Range of IP address ▪ Class A ▪ Class B ▪ Class C 4. Subnet mask 5. Subnetting implementation process
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience 2: Perform subnetting

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Perform subnetting"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Perform subnetting"	2. Read Information sheet 2: "Perform subnetting" 3. Answer Self-check 2: Perform subnetting 4. Check your answer with Answer key 2: "Perform subnetting"
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Task Sheet 2.1: Perform subnetting for 192.168.0.0/30 Specification Sheet 2.1: Perform subnetting for 192.168.0.0/30 Task Sheet 2.2: Perform subnetting 192.168.0.0/31 Specification Sheet 2.1: Perform subnetting for 192.168.0.0/30

Information Sheet 1: Perform subnetting

Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents

2.1 Subnetting
2.2 Subnetting technique
2.3 Range of IP address
- Class A
- Class B
- Class C

2.4 Subnet mask
2.5 Subnetting implementation process

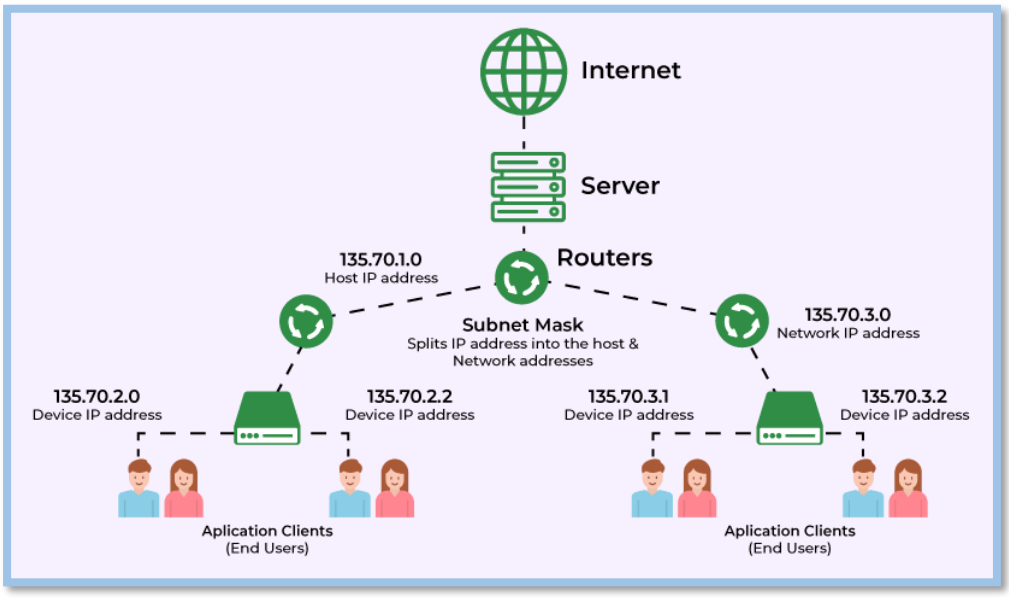
2.1 Subnetting:

Subnetting is the task of sub dividing the networks by increasing network bits and reducing host bits. On the others hands, Subnetting is done by borrowing bits from the host part and add them the network part.

11111111.11111111.11111111. 00000000

Network bits Host bit

11111111.11111111.11111111. 10000000 Borrowed bits from host



2.2 Subnetting technique:

Rule 1:

a. If the host bits in a given IP address are all set to '0' this is the network or subnet address.
b. If the host bits in a given IP address are all set to '1' this is the broadcast address (all hosts in the subnet/network are destination).

Rule 2: The formula used to calculate the number of available subnets given the specific length of network mask.

Number of Subnets = 2^N (where N = Borrowed network bits)

Rule 3: The formula used to calculate the number of available hosts given the specific length of network mask.

Number of Host = 2^H-2 (where H = Host bits)

Rule 4: The formula used to calculate the number of available block size given the specific length of network mask.

Number of Block Size = 2^H (where H = Host bits)

2.3 IP Address:

IP address is stand for internet protocol which is a unique 32-bit binary number assigned to a host and used for all communication with the host. For example:

32 – bit binary number 10000001 00110100 000000110 00000000
Equivalent dotted decimal 129.52.6.0

Range of IP Address:

- **Class A** - 0.0.0.0 - 127.255.255.255
- **Class B** - 128.0.0.0 - 191.255.255.255
- **Class C** - 192.0.0.0 - 223.255.255.255
- Class D - 224.0.0.0 - 239.255.255.255
- Class E - 240.0.0.0 - 255.255.255.255

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

2.4 Subnet mask:

A subnet mask is a 32-bit value that specifies the boundary between the network prefix and suffix. 1 bit represent the network portion and 0 bits represent the host portion.

Dotted decimal IP	192.168.0.0/25	
Subnet Mask	255.255.255.128	
Equivalent dotted binary	11111111.11111111.11111111.	10000000
	Network bits	Host bit

2.5 subnetting implementation process:

subnetting implementation of this IP address- 192.168.0.0/25

Dotted decimal IP	192.168.0.0	
Subnet Mask	255.255.255.128	
Equivalent dotted binary	11111111.11111111.11111111.	10000000
	Network bits	Host bit

Here, Host bits (H) = 7, Borrowed network bits (N) =1

i. Number of subnet = $2^{N} = 2^{1} = 2$
ii. Number of Host = $2^{H}-2 = 2^{7}-2 = 126$
iii. Number of block size = $2^{H} = 2^{7} = 128$ or (256 -128=128)
iv. Valid IP range:

Subnet Id	First Valid host	Last Valid host	Broadcast Address
192.168.0.0	192.168.0.1	192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129	192.168.0.254	192.168.0.255

2.6 Tools are commonly used for performing subnetting calculations

Tools such as subnet calculators, online subnetting calculators, and network simulation software are commonly used for performing subnetting calculations and planning network configurations.

Self-Check-2: Perform Subnetting

1. **What is subnetting?**

   Answer:

2. **What is range of IP address in different class?**

   Answer

3. **What is Subnet mask:**

   Answer

Answer Key-2: Perform Subnetting

1. What is subnetting?

Answer: Subnetting is the task of sub dividing the nerworks by increasing network bits and reducing host bits. On the others hands, Subnetting is done by borrowing bits from the host part and add them the network part.

11111111.11111111.11111111. 00000000
Network bits Host bit
11111111.11111111.11111111. 10000000 Borrowed bits from host part

2. What is range of IP address in different class?
Answer: Range of IP Address

- **Class A** - 0.0.0.0 - 127.255.255.255
- **Class B** - 128.0.0.0 - 191.255.255.255
- **Class C** - 192.0.0.0 - 223.255.255.255
- Class D - 224.0.0.0 - 239.255.255.255
- Class E - 240.0.0.0 - 255.255.255.255

3. What is Subnet mask:
Answer: A subnet mask is a 32-bit value that specifies the boundrary between the network prefix and suffix. 1 bit represent the network portion and 0 bits represent the host portion.

Dotted decimal IP	192.168.0.0/25	
Subnet Mask	255.255.255.128	
Equivalent dotted binary	11111111.11111111.11111111.	10000000
	Network bits	Host bit

4. Why is subnetting used?
Answer: Subnetting allows for efficient use of IP addresses, improves network performance by reducing broadcast traffic, and enhances network security by segmenting traffic.

5. How is subnetting accomplished?
Answer: Subnetting involves borrowing bits from the host portion of an IP address to create subnet addresses, which results in a network with multiple smaller subnets.

6. What are the benefits of subnetting?
Subnetting helps in optimizing network resources, simplifying network management, enhancing security by isolating network segments, and facilitating efficient routing.

7. What tools are commonly used for performing subnetting calculations?
Answer: Tools such as subnet calculators, online subnetting calculators, and network simulation software are commonly used for performing subnetting calculations and planning network configurations.

Job Sheet-2.1: Perform Subnetting for 192.168.0.0/30

Performance Objective: At the end of this task, the trainee should be able to Perform subnetting.

Working Procedure: Subnet the IP address 192.168.0.0/30 so that you can make usable subnets and the maximum number of addresses can be used. Hence steps the following-

Step 1: Determine the block size, subnets, and number of hosts required for your network. For block size, subnets, and number of hosts, the given IP address needs to be converted into a binary number then the network bits and host bits need to be identified.

Dotted decimal IP	192.168.0.0/30	
Subnet Mask	255.255.255.252	
Equivalent dotted binary	11111111.11111111.11111111.111111	00
	Network bits	Host bit

Step 2: You have to use all the formulas for calculating block sizes, subnets, and the number of hosts-

Here, Host bits (H) =2, Borrowed network bits (N) =6

i. Number of subnets = $2^N = 2^6 = 64$
ii. Number of Host = $2^H-2 = 2^2-2 = 2$
iii. Number of block size = $2^H = 2^2 = 4$ or (256-252=4)

Step 3: Finally, for valid first & last subnet IP addresses, you must be make a table.

Subnet Id	First Valid host	Last Valid host	Broadcast Address
192.168.0.0	192.168.0.1	192.168.0.2	192.168.0.3
192.168.0.4	192.168.0.5	192.168.0.6	192.168.0.7
192.168.0.8	---	---	---

Block Size= 4 Increase for every subnet until 256

Specification Sheet-2.1: Perform Subnetting For 192.168.0.0/30

Tools:

1. Subnet Calculator
2. IP Addressing Charts
3. Command Line Interface (CLI)
4. Subnetting Practice Tools

Materials:

1. Pen and Paper
2. Whiteboard or Flipchart
3. Textbooks or Study Guides
4. Network Simulation Software

Job Sheet-2.2: Perform Subnetting 192.168.0.0/31

Working Procedure: Subnet the IP address 192.168.0.0/31 so that you can make usable subnets and the maximum number of addresses can be used. Hence steps the following-

Step 1: Determine the block size, subnets, and number of hosts required for your network. For block size, subnets, and number of hosts, the given IP address needs to be converted into a binary number then the network bits and host bits need to be identified.

Dotted decimal IP	192.168.0.0/31	
Subnet Mask	255.255.255.254	
Equivalent dotted binary	11111111.11111111.11111111.1111111	0
	Network bits	Host bit

Step 2: You have to use all the formulas for calculating block sizes, subnets, and the number of hosts-

Here, Host bits (H) =1, Borrowed network bits (N) =7

i. Number of subnets = $2^N = 2^7 = 128$
ii. Number of Host = $2^H - 2 = 2^1 - 2 = 0$
iii. Number of block size = $2^H = 2^1 = 2$ or (256-252=4)

Step 3: In this case, IP address 192.168.0.0/31 can not be subnetting because this IP address host size is 0. So, we can be subnetting any IP address class when its maximum CIDR value is 30 otherwise we can't.

Specification Sheet-2.2: Perform Subnetting 192.168.0.0/31

Tools:

5. Subnet Calculator
6. IP Addressing Charts
7. Command Line Interface (CLI)
8. Subnetting Practice Tools

Materials:

5. Pen and Paper
6. Whiteboard or Flipchart
7. Textbooks or Study Guides
8. Network Simulation Software

Learning Outcome-3: Configure Advance Network Services and Protocol

Assessment Criteria	1. Network simulation tools are installed 2. Required Network services are identified 3. IP addresses is determined 4. Vlan is configured as per design plan 5. Dynamic Trunk protocol is applied if required 6. Spanning Tree protocol is identified and configured 7. Services of network is identified and configured
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker • Internet Facilities 9. Whiteboard and Marker
Contents	1 VLAN 2 Dynamic Trunk protocol 3 Spanning Tree protocol 4 Network simulation tools ▪ Packet Tracer ▪ GNS3 5 Configuration services of network ▪ DHCP ▪ DNS ▪ NTP ▪ VPN
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-3: Configure Advance Network Services and Protocol

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
4. Trainee will ask the instructor about the learning materials	6. Instructor will provide the learning materials "Configure advance network services and protocol"
5. Read the Information sheet and complete the Self Checks & Check answer sheets on "Configure advance network services and protocol"	7. Read Information sheet 1: Configure advance network services and protocol 8. Answer Self-check 3: Configure advance network services and protocol 9. Check your answer with Answer key 3: Configure advance network services and protocol
6. Read the Job/Task Sheet and Specification Sheet and perform job/Task	10. Job/Task Sheet and Specification Sheet Job Sheet 3.1: Install network simulation tools Specification Sheet 3.1 Install network simulation tools Task Sheet 3.2: Configure VLAN and apply dynamic Trunk protocol Specification Sheet 3.2: Configure VLAN and apply dynamic Trunk protocol

Information Sheet-3: Configure Advance Network Services and Protocol

Learning Objective:

After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

3.1 VLAN
3.2 Dynamic Trunk protocol
3.3 Spanning Tree protocol
3.4 Network simulation tools
- Packet Tracer
- GNS3

3.5 Configuration services of network
- DHCP
- DNS
- NTP
- VPN

3.1 VLAN

VLAN stands for “Virtual Local Area Network”. It's a method of segmenting a physical network into multiple logical networks. In traditional LANs, all devices connected to the same network can communicate directly with each other. However, VLANs allow you to create separate logical networks within the same physical infrastructure. In a word, VLANs provide a powerful way to organize and secure network traffic in complex environments.

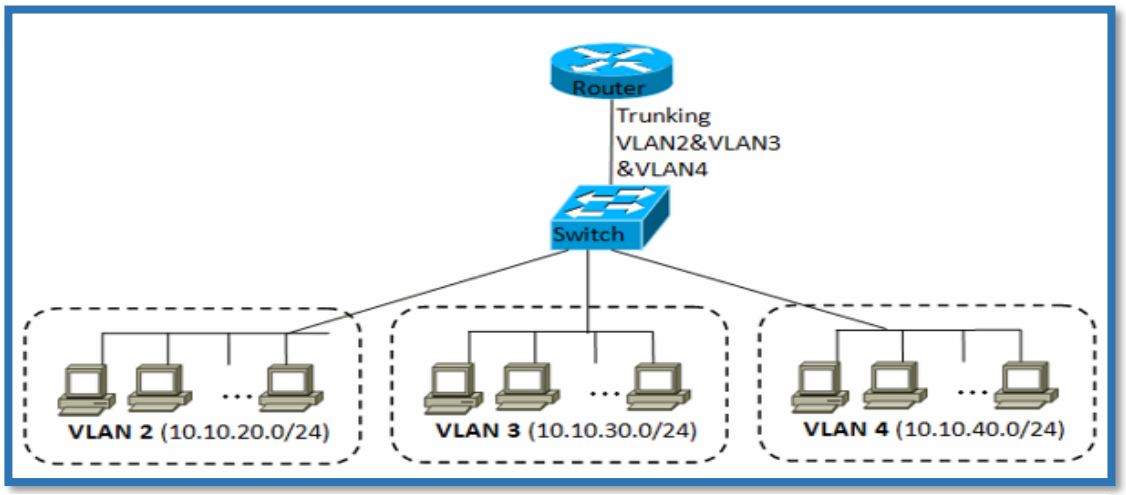


Figure: VLAN (Virtual Local Area Network).

3.2 Dynamic Trunk protocol

"Dynamic Trunking Protocol" (DTP) is a Cisco proprietary protocol used to negotiate trunking between two switches, allowing them to establish a trunk link between them without manual configuration dynamically. On the other hand, DTP can simplify network configuration, it's also important to understand its operation and configure switch ports appropriately to avoid unintended trunking or security vulnerabilities. Additionally, as DTP is a Cisco proprietary protocol, it may not be interoperable with devices from other vendors that use different trunk negotiation mechanisms.

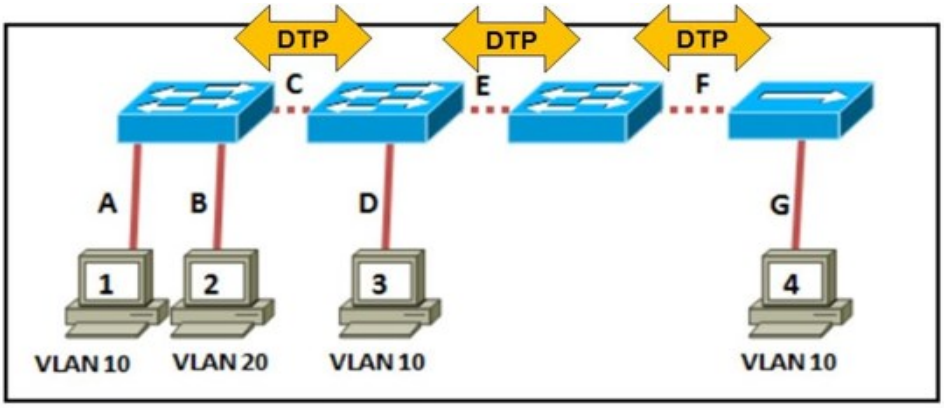


Figure 1: DTP (Dynamic Trunk Protocol)

3.3 Spanning Tree protocol

"Spanning Tree Protocol" (STP) is a network protocol that ensures a loop-free network infrastructure, particularly in Ethernet networks where redundancy is implemented to ensure high availability.

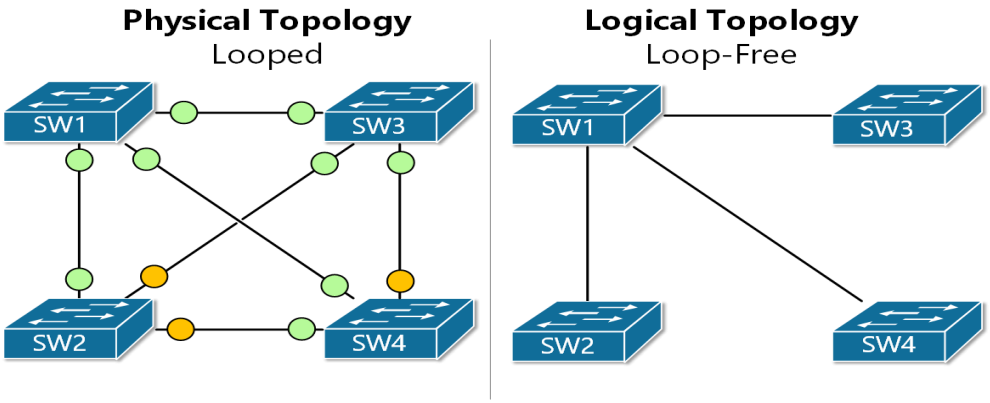


Figure 2: STP (Spanning Tree Protocol)

3.4 Network simulation tools

Packet Tracer: Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It's primarily used for teaching and learning about networking concepts and practices virtually. Packet Tracer provides a simulated environment where users can design, configure, and troubleshoot network setups without the need for physical networking hardware. In a word, Packet Tracer is a valuable tool for networking students, professionals,

and instructors alike, providing a safe and convenient environment to explore and experiment with networking concepts and technologies.

Figure: CISCO Packet Tracer

GNS3:

GNS3, short for "Graphical Network Simulator-3", is an open-source network emulator that allows users to simulate complex networks in a virtual environment. Like Packet Tracer, which is more focused on beginners and educational settings, GNS3 is geared towards professionals and advanced users who require more advanced networking features and flexibility.

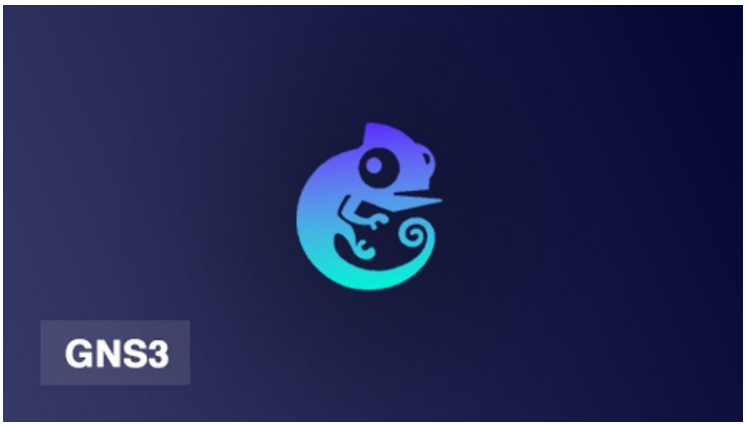


Figure: GNS3 (Graphical Network Simulator-3) Tool

3.5 Configuration services of network

DHCP:

DHCP stands for "Dynamic Host Configuration Protocol". It's a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. DHCP simplifies the process of configuring network devices by dynamically allocating IP addresses rather than requiring manual configuration. It ensures efficient use of IP addresses and reduces the likelihood of conflicts caused by duplicate addresses. DHCP is widely used in both wired and wireless networks, including home networks, corporate networks, and Internet Service Provider (ISP) networks.

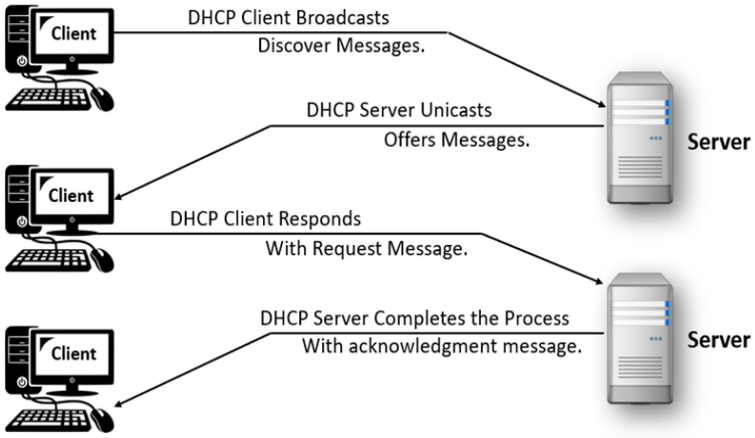


Figure: DHCP (Dynamic Host Configuration Protocol) Process

DNS:

DNS stands for Domain Name System. It is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network. DNS translates domain names, which are easy-to-remember human-readable names (like "example.com"), into IP addresses, which are numerical identifiers used by computers to communicate over a network.

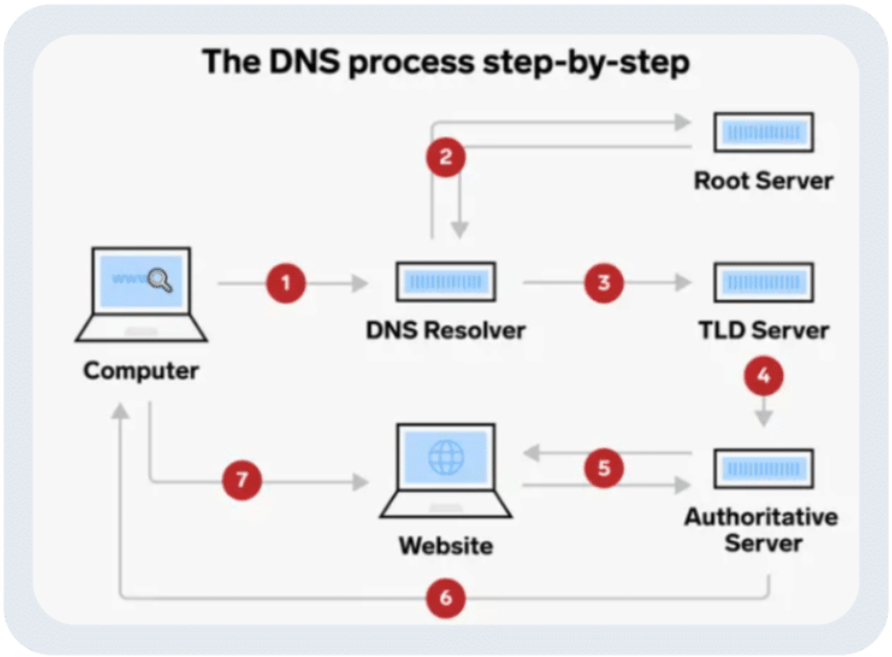
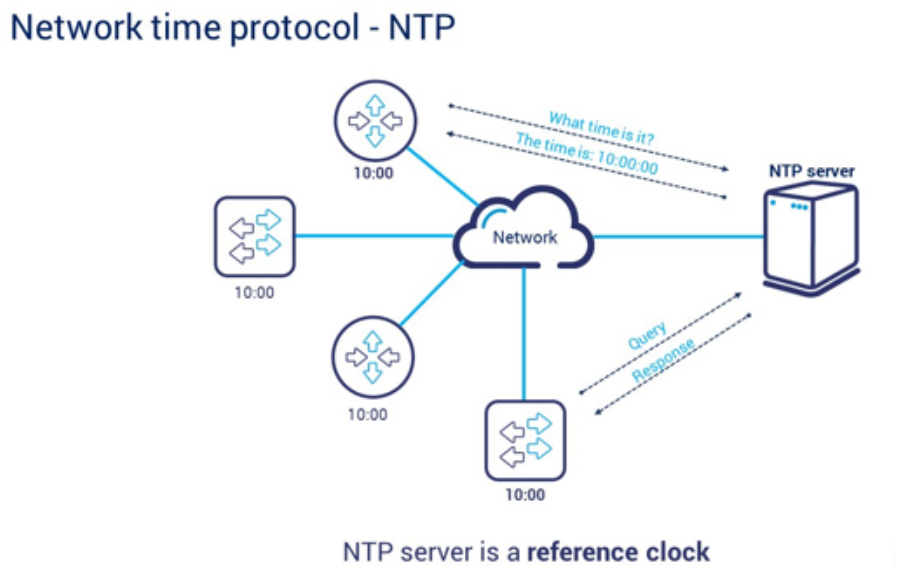


Figure: DNS (Domain Name System)

NTP:

NTP stands for “Network Time Protocol”. It's a networking protocol used to synchronize the time of computers and other networked devices to a reference time source. NTP is essential for maintaining accurate timekeeping across a network, which is crucial for various operations, including logging events, coordinating transactions, and ensuring the security of cryptographic protocols.



VPN:

VPN stands for Virtual Private Network. It's a technology that creates a secure and encrypted connection over a less secure network, such as the internet. VPNs provide privacy, anonymity, and security to users by encrypting their internet traffic and routing it through a remote server.

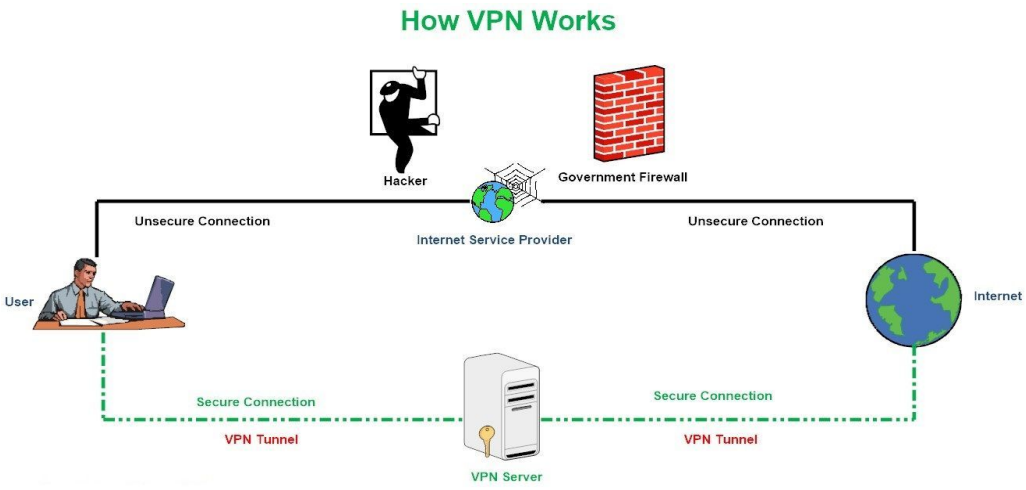


Figure: VPN (Virtual Private Network)

Self-Check 3: Configure Advance Network Services and Protocol

1. What is VLAN?

   Answer

2. What is the purpose of Dynamic Trunking Protocol (DTP)?

   Answer

3. Why is it important to configure switch ports appropriately for DTP?

   Answer

4. What does Spanning Tree Protocol (STP) ensure in a network infrastructure?

   Answer

5. In what type of networks is STP commonly implemented?

   Answer

6. What does DHCP stand for and what is its function?

   Answer

7. How does DHCP simplify network configuration?

   Answer

8. What does DNS stand for and what is its purpose?

   Answer

9. Why is DNS considered hierarchical and decentralized?

   Answer

10. What is NTP used for in networking?

    Answer

11. Why is accurate timekeeping important in networking?

    Answer

12. What does VPN stand for and what does it provide?

    Answer

13. What technology does VPN use to ensure secure connections?

    Answer

Answer Key-3: Configure Advance Network Services and Protocol

1. **What is VLAN?**

   Answer: VLAN stands for "Virtual Local Area Network". It's a method of segmenting a physical network into multiple logical networks. In traditional LANs, all devices connected to the same network can communicate directly with each other. However, VLANs allow you to create separate logical networks within the same physical infrastructure. In a word, VLANs provide a powerful way to organize and secure network traffic in complex environments.

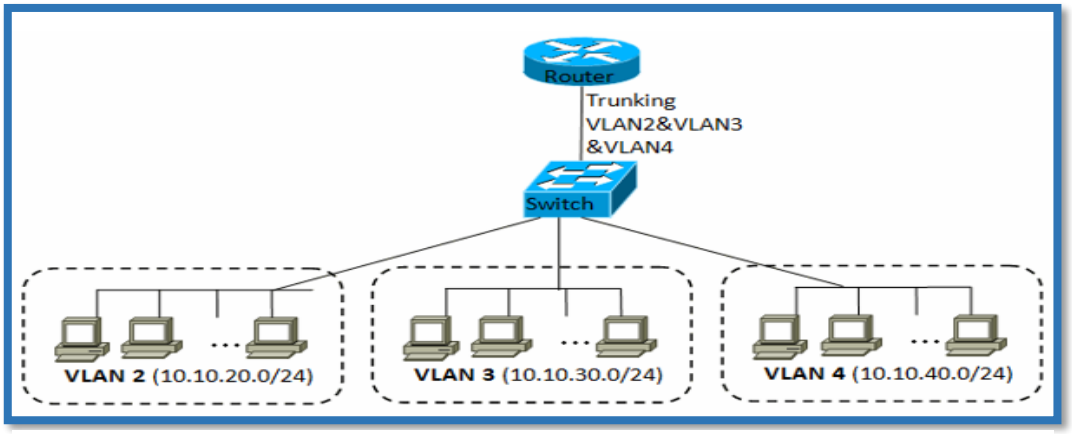


Figure: VLAN (Virtual Local Area Network).

2. **What is the purpose of Dynamic Trunking Protocol (DTP)?**
   Answer: DTP is used to negotiate trunking between switches dynamically, establishing trunk links without manual configuration.

3. **Why is it important to configure switch ports appropriately for DTP?**
   Answer: Configuring switch ports appropriately helps avoid unintended trunking or security vulnerabilities that may arise from DTP operation.

4. **What does Spanning Tree Protocol (STP) ensure in a network infrastructure?**
   Answer: STP ensures a loop-free network infrastructure, particularly in Ethernet networks with redundancy to ensure high availability.

5. **In what type of networks is STP commonly implemented?**
   Answer: STP is commonly implemented in Ethernet networks where redundancy is used to prevent network loops.

6. **What does DHCP stand for and what is its function?**
   Answer: DHCP stands for Dynamic Host Configuration Protocol. It automatically assigns IP addresses and network configuration parameters to devices on a network.

7. **How does DHCP simplify network configuration?**
   Answer: DHCP simplifies network configuration by dynamically allocating IP addresses, reducing the need for manual configuration and the likelihood of address conflicts.

8. **What does DNS stand for and what is its purpose?**

Answer: DNS stands for Domain Name System. It translates domain names into IP addresses, facilitating communication between devices on the Internet or a private network.

9. **Why is DNS considered hierarchical and decentralized?**
   Answer: DNS is hierarchical because it organizes domain names into a tree-like structure, and decentralized because it distributes authority and control over domain names among multiple DNS servers.

10. **What is NTP used for in networking?**
    Answer: NTP is used to synchronize the time of computers and other networked devices to a reference time source, ensuring accurate timekeeping across a network.

11. **Why is accurate timekeeping important in networking?**
    Answer: Accurate timekeeping is crucial for various network operations, including event logging, transaction coordination, and security protocols such as encryption.

12. **What does VPN stand for and what does it provide?**
    Answer: VPN stands for Virtual Private Network. It provides privacy, anonymity, and security by creating a secure and encrypted connection over a less secure network, such as the internet.

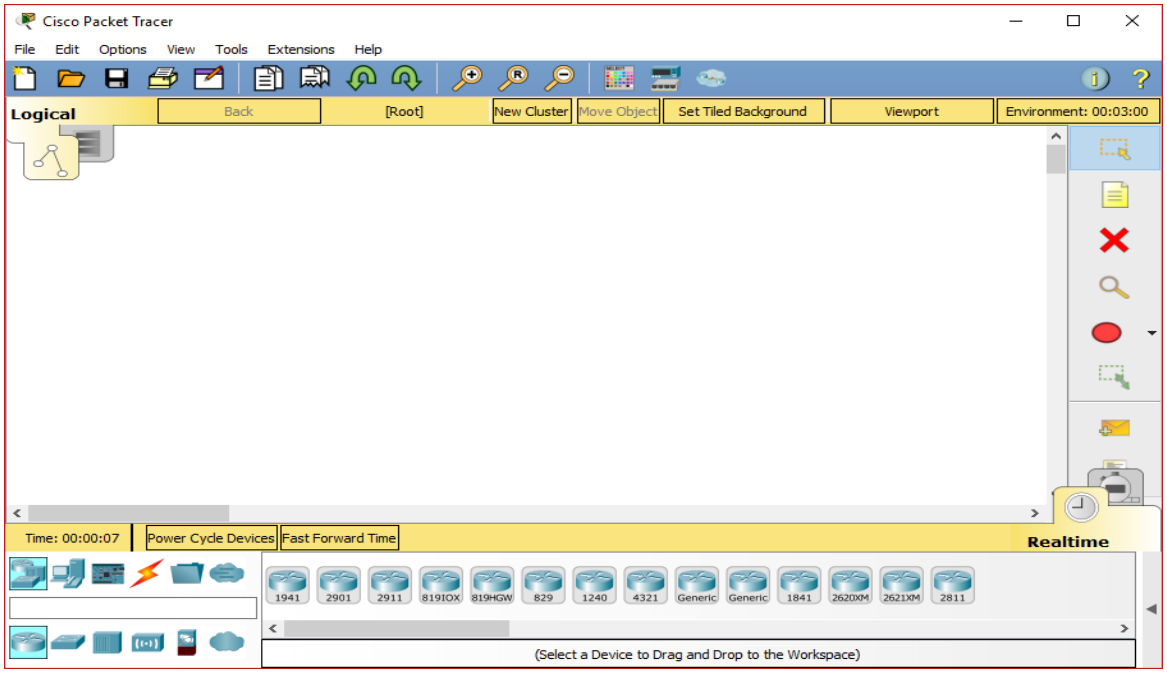
13. **What technology does VPN use to ensure secure connections?**
    Answer: VPNs use encryption to secure internet traffic and routing it through a remote server, ensuring privacy and security for users.

Job Sheet-3.1: Install Network Simulation Tools

Performance Objective: At the end of this task, the trainee should be able to Install network simulation tools

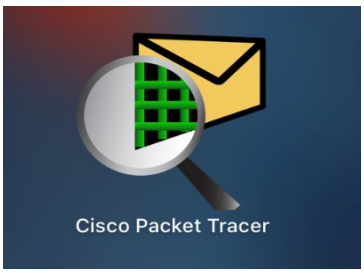
Working Procedure:

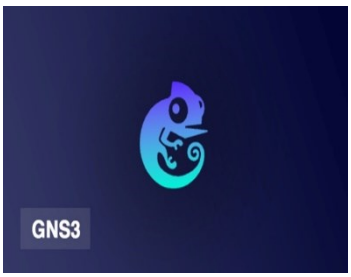
Installing network simulation tools involves several steps, including downloading the software, installing it on your computer, and configuring it to simulate network environments. Here's a general procedure for installing network simulation tools:



Step 1: Research and Choose a Network Simulation Tool:

- Research Consider factors such as supported features, compatibility with your operating system, ease of use, and community support.
- Cisco Packet Tracer or GNS3





Step 2: Download the Software:

- Visit the official website of the network simulation tool you've chosen.
- Locate the download section or page and select the appropriate version for your operating system (e.g., Windows, macOS, Linux).

Step 3: Verify System Requirements:

- Check the system requirements provided by the software vendor to ensure that your computer meets the minimum hardware and software requirements for installation.
- Make sure your computer has sufficient CPU, RAM, and disk space to run the simulation tool effectively.

Step 4: Run the Installer:

- Once the download is complete, locate the downloaded installation file on your computer.
- Double-click the installation file to run the installer and initiate the installation process.

Step 5: Follow Installation Wizard:

- Follow the prompts in the installation wizard to complete the installation process.
- Read and accept the end-user license agreement (EULA), if prompted.
- Choose the installation directory and any additional options or components you want to install.

Step 6: Wait for Installation to Complete:

- Allow the installation process to complete. This may take several minutes depending on the size of the software and the speed of your computer.

Step 7: Launch the Application:

- Once the installation is complete, launch the network simulation tool from the Start menu (Windows), Applications folder (macOS), or command line (Linux).
- Follow any initial setup or configuration steps provided by the software to configure the simulation environment.

Step 8: Explore and Familiarize Yourself:

- Take some time to explore the features and functionality of the network simulation tool.
- Familiarize yourself with the user interface, simulation options, and available network components (e.g., routers, switches, hosts).

Step 9: Optional: Install Updates or Plugins:

- Check for updates or plugins for the network simulation tool and install them if necessary.
- Updates may include bug fixes, performance improvements, and new features.

Step 10: Start Simulating Networks:

- Begin using the network simulation tool to create, configure, and simulate network environments.
- Experiment with different network topologies, protocols, and configurations to simulate real-world scenarios and test network designs.

Specification Sheet-3.1: Install Network Simulation Tools

Tools for Network Simulation Installation:

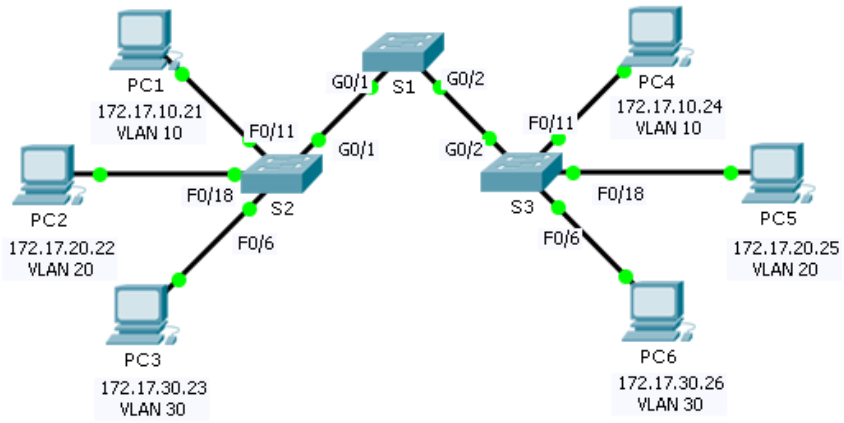
1. Network Simulation Software
2. Virtualization Software
3. Operating System
4. Network Devices
5. Internet Connection

Materials for Network Simulation Installation:

1. Computer Hardware
2. Installation Media
3. Documentation and Guides
4. License Keys
5. Updates and Patches

Task Sheet-3.2: Configure VLAN and Apply Dynamic Trunk Protocol

Topology



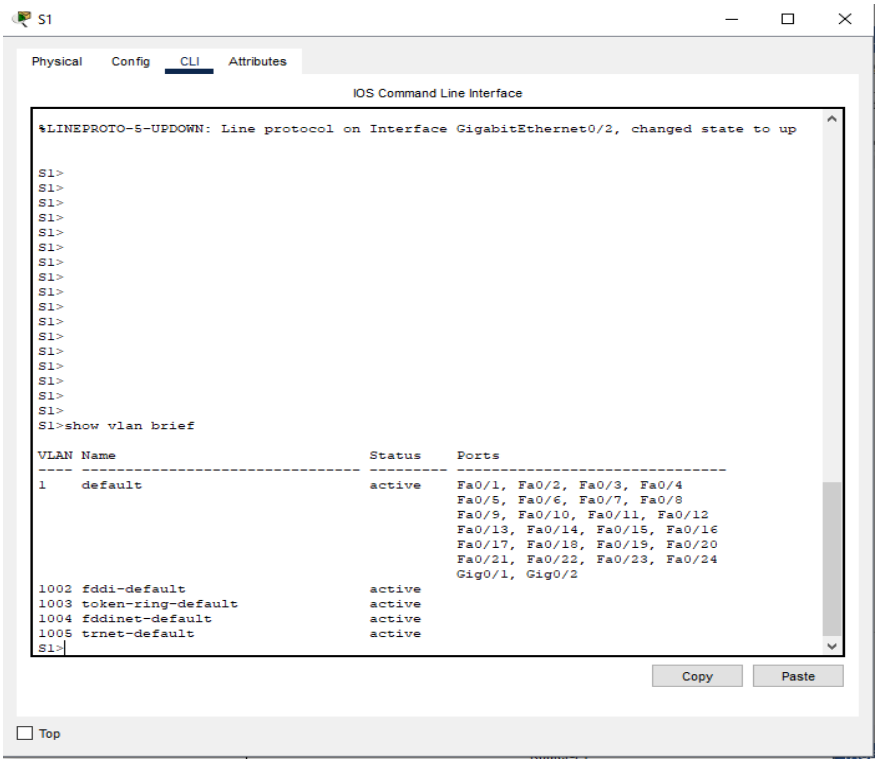
Addressing Table

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Step 1: View the default VLAN configuration

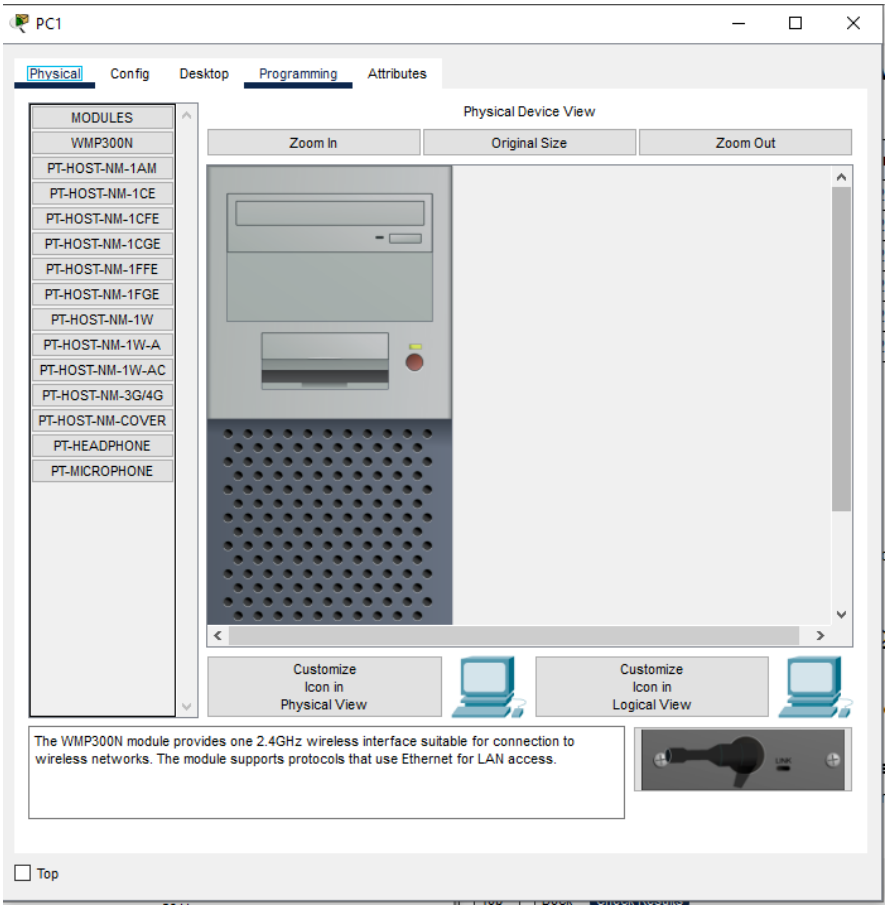
1.1: Display the current VLANS.

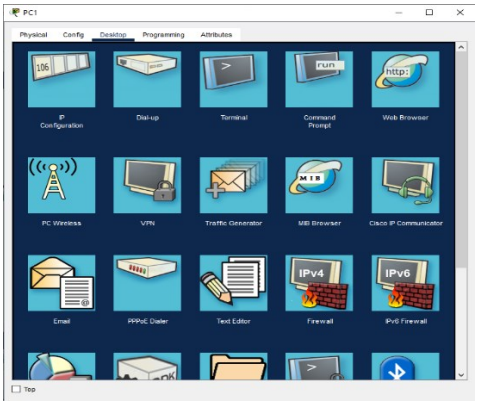
On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

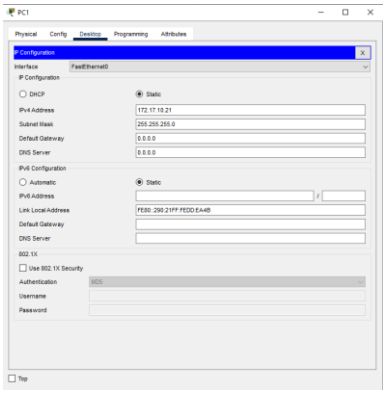


1.2: All PC configure & verify connectivity between PCs on the same network.

PC Configuration Steps:



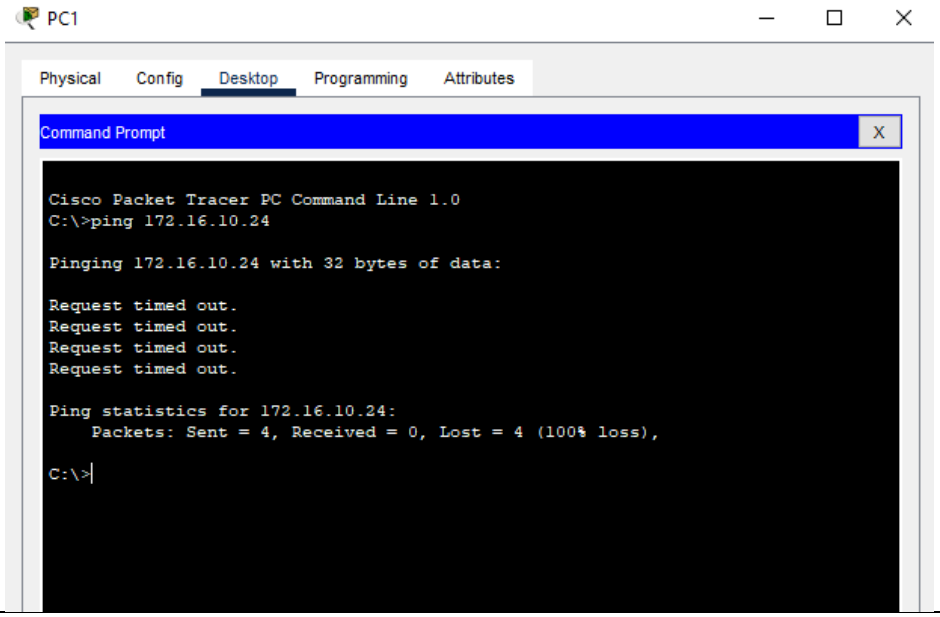




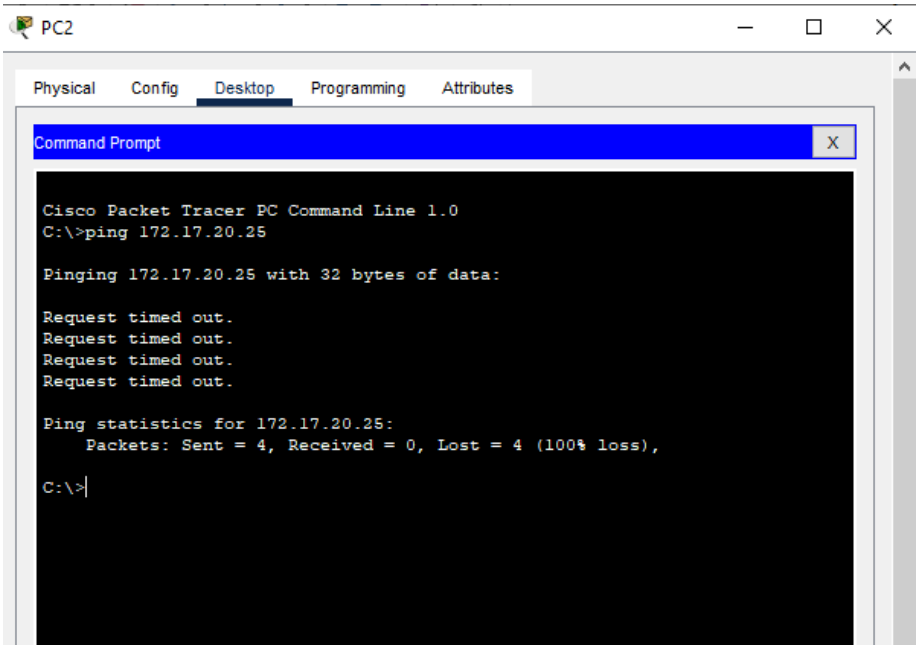
Using the same Steps, Configure PC2, PC3, PC4, PC5, and PC6.

Notice that each PC can ping the other PC that shares the same network.

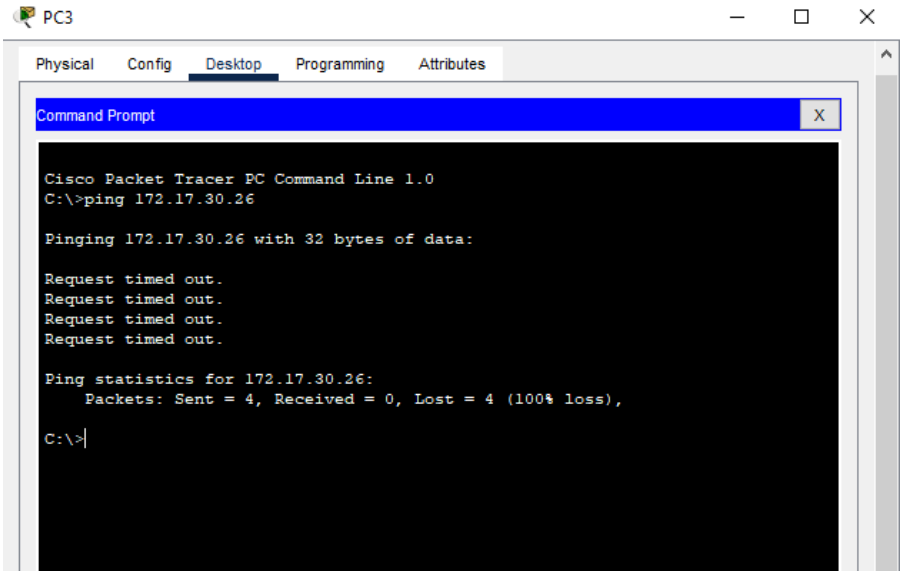
- PC1 can ping PC4



- PC2 can ping PC5



- PC3 can ping PC6



Pings to PCs in other networks fail.

What benefit will be configuring VLANs provide to the current configuration? The primary benefits of using VLANs are as follows: security, cost reduction, higher performance, broadcast storm mitigation, improved IT staff efficiency, and simpler project and application management.

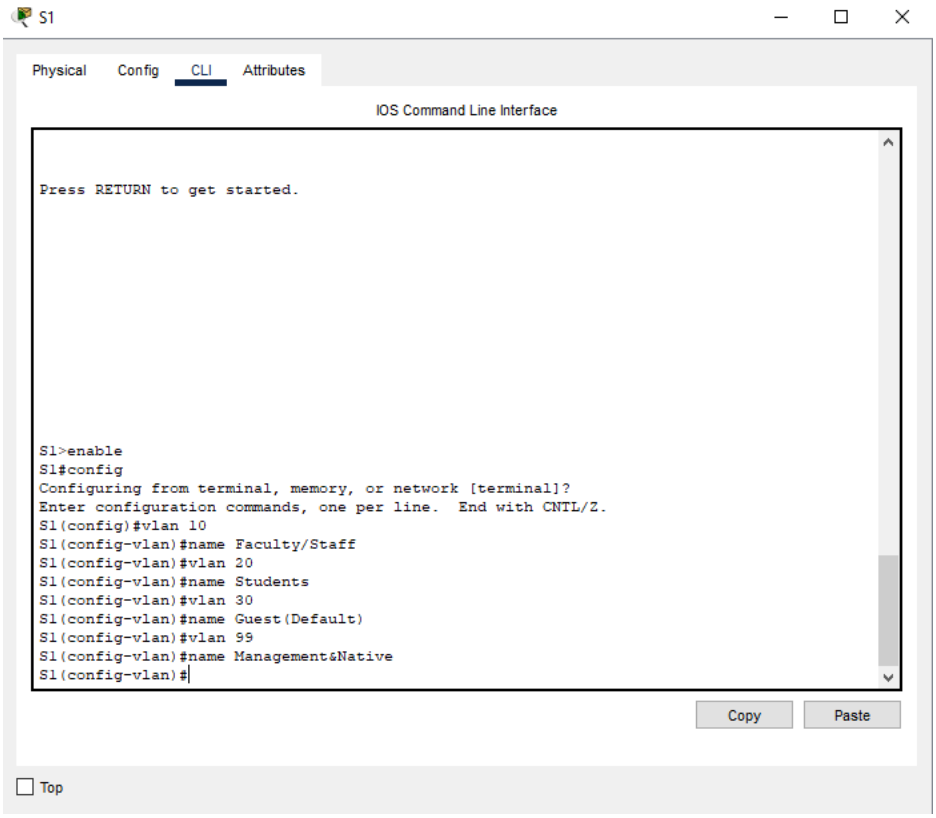
Step 2: Configure VLANs

2.1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native

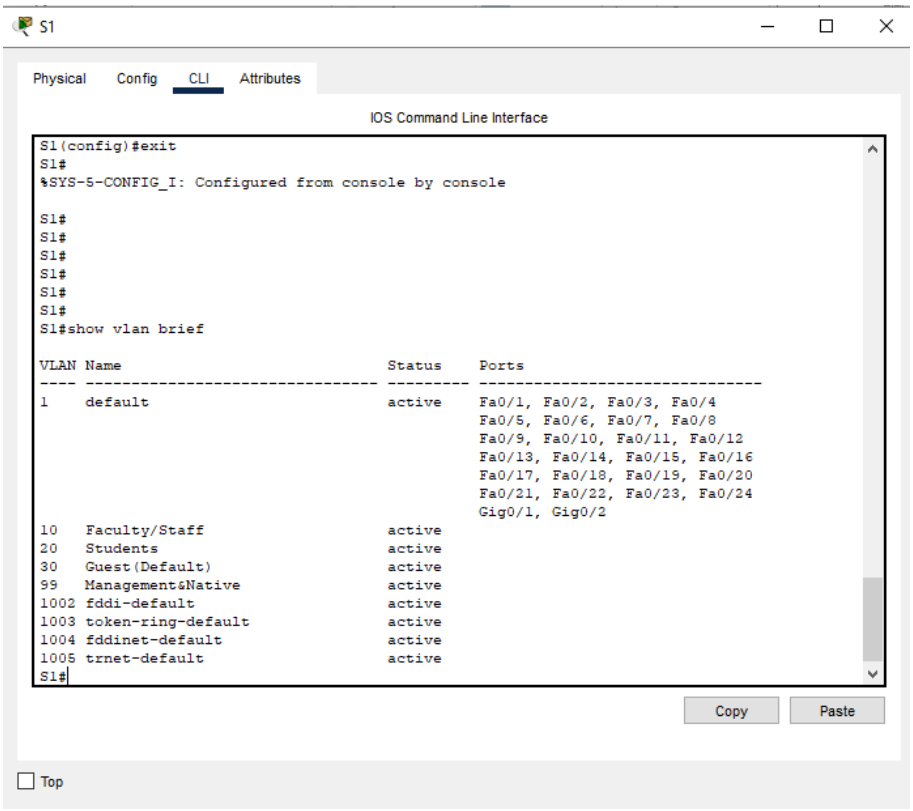
```
S1#(config)# vlan 10
S1#(config-vlan)# name Faculty/Staff
S1#(config-vlan)# vlan 20
S1#(config-vlan)# name Students
S1#(config-vlan)# vlan 30
S1#(config-vlan)# name Guest(Default)
S1#(config-vlan)# vlan 99
S1#(config-vlan)# name Management&Native
```



2.2: Verify the VLAN configuration.

Which command will only display the VLAN name, status, and associated ports on a switch?

S1# show vlan brief



2.3: Create the VLANs on S2 and S3.

Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

S3

Physical Config CLI Attributes

IOS Command Line Interface

```
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up


S3>enable
S3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#vlan 10
S3(config-vlan)#name Faculty/Staff
S3(config-vlan)#Vlan 20
S3(config-vlan)#name Students
S3(config-vlan)#Vlan 30
S3(config-vlan)#name Guest(Default)
S3(config-vlan)#vlan 99
S3(config-vlan)#name Management&Native
S3(config-vlan)#
```

Copy Paste

Top

S2

Physical Config CLI Attributes

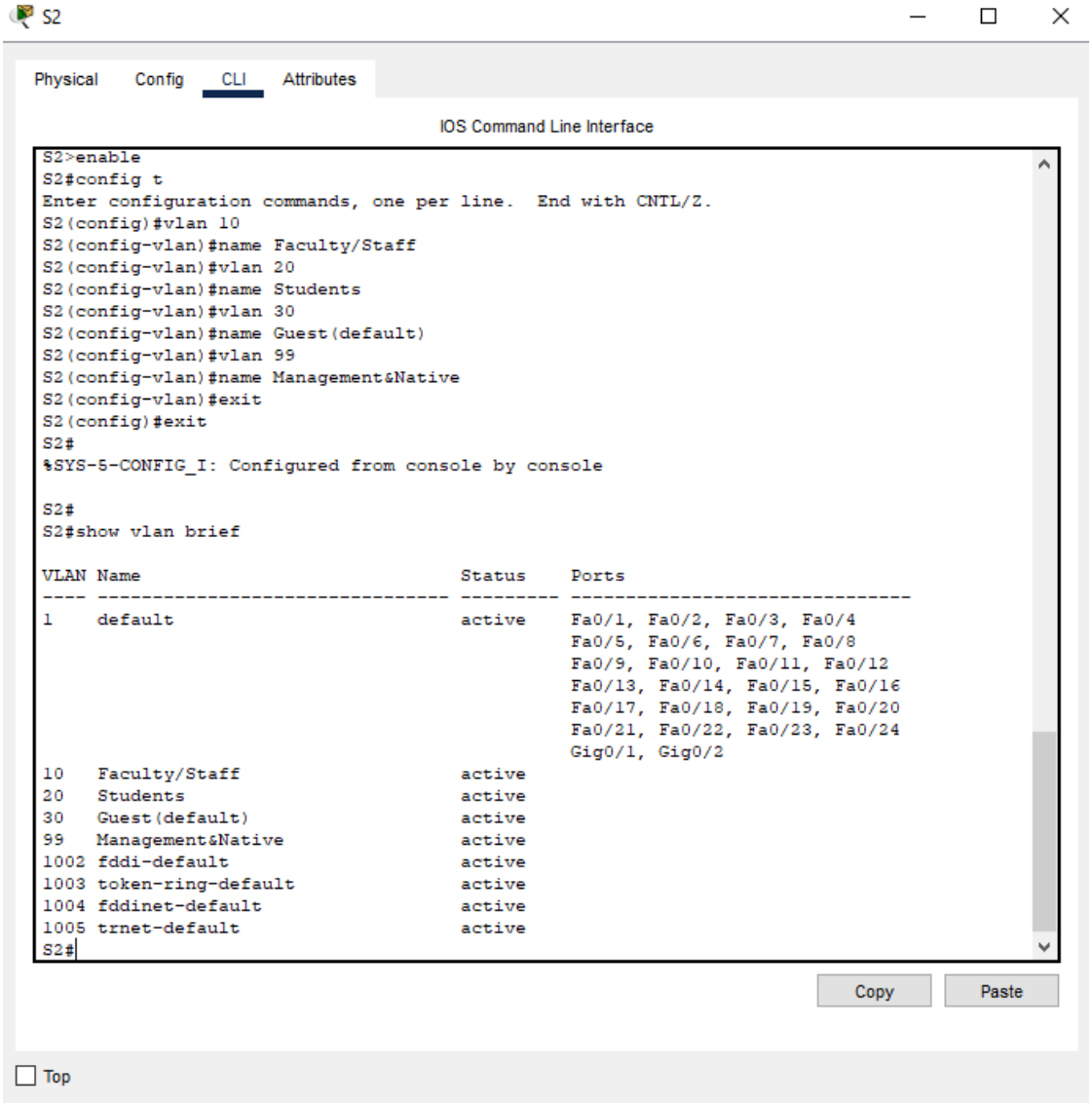
IOS Command Line Interface

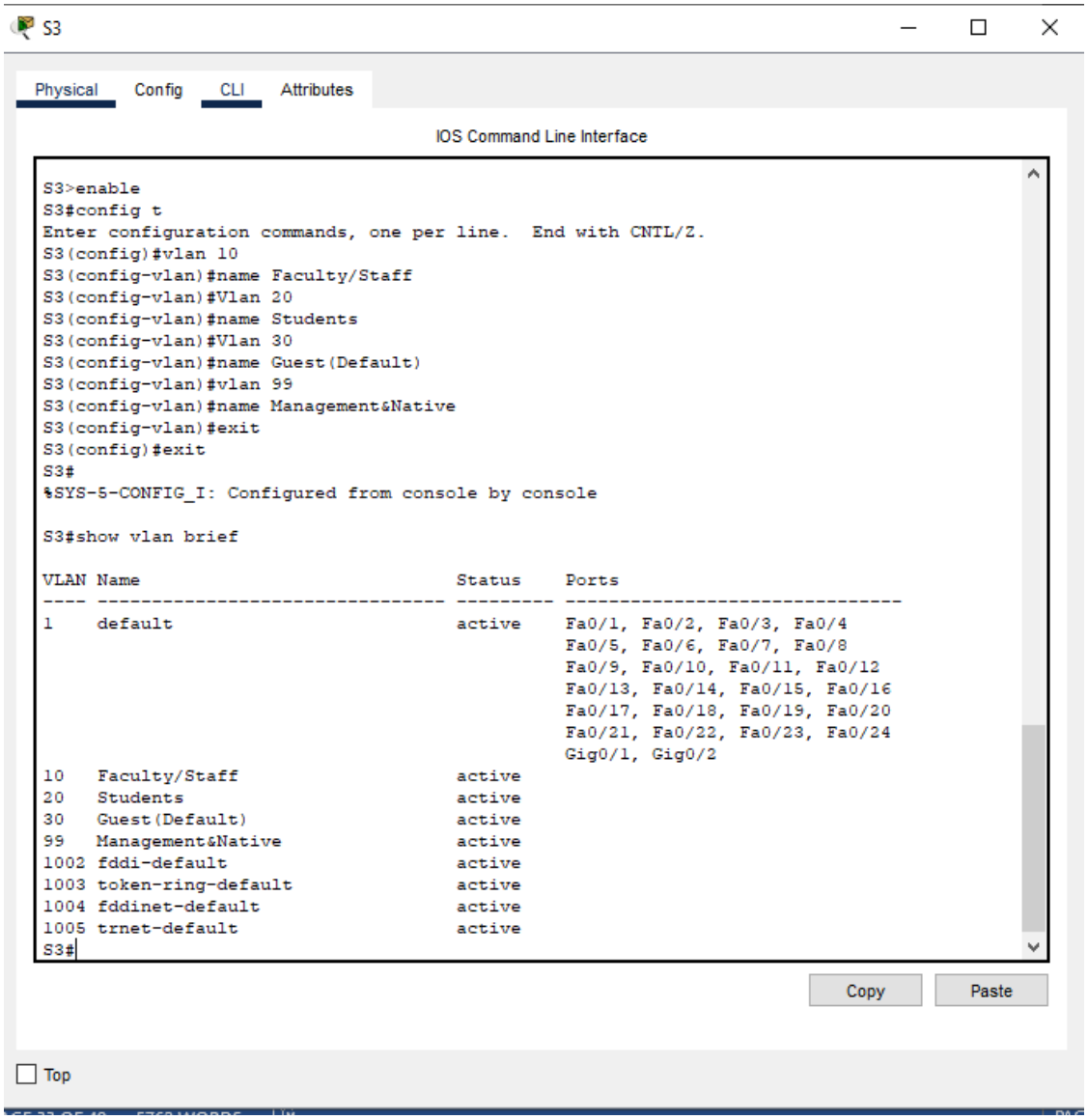
```
Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up


S2>
S2>enabel
Translating "enabel"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Faculty/Staff
S2(config-vlan)#vlan 20
S2(config-vlan)#name Students
S2(config-vlan)#vlan 30
S2(config-vlan)#name Guest(default)
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#
```

Copy Paste

Top

Job Sheet-3.2: Verify The VLAN Configuration.





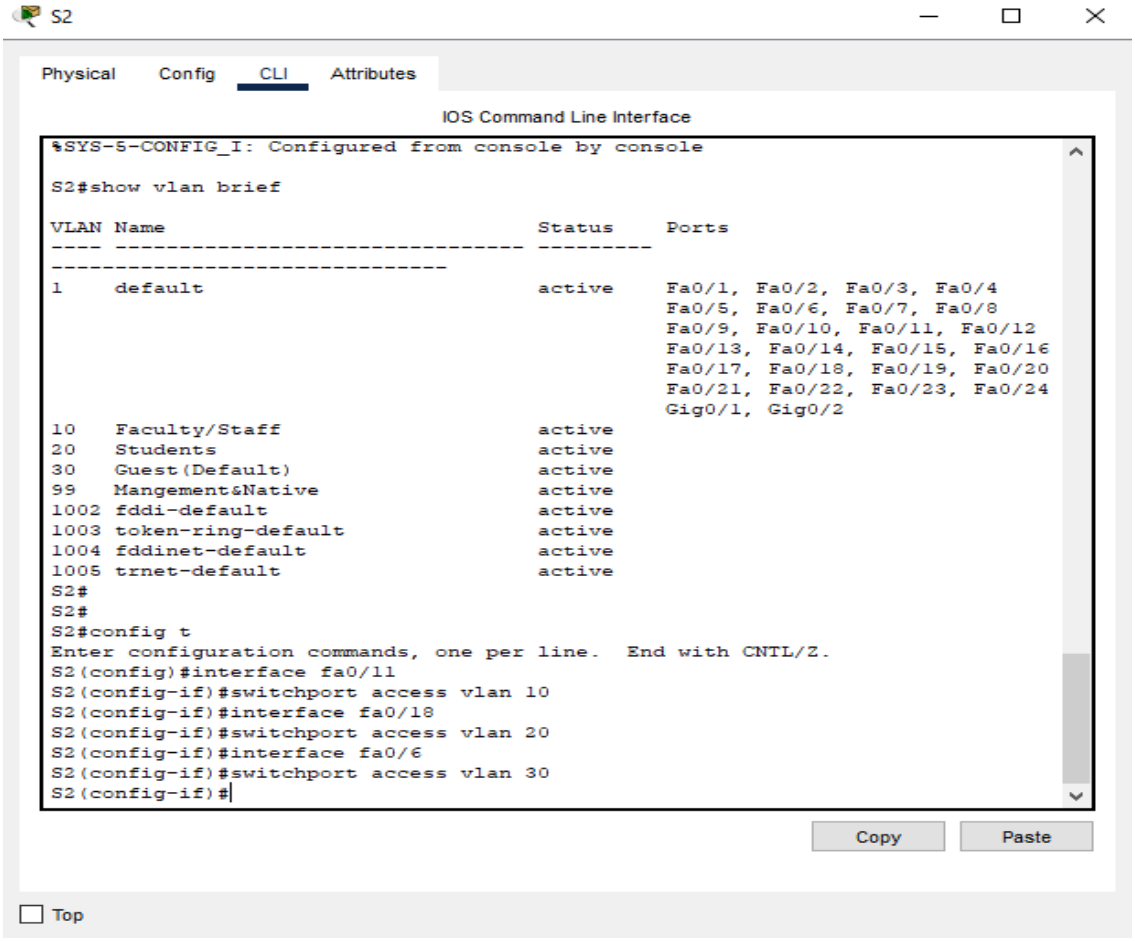
Step 3: Assign VLANs to ports

3.1: Assign VLANs to the active ports on S2.

Assign the VLANs to the following ports:

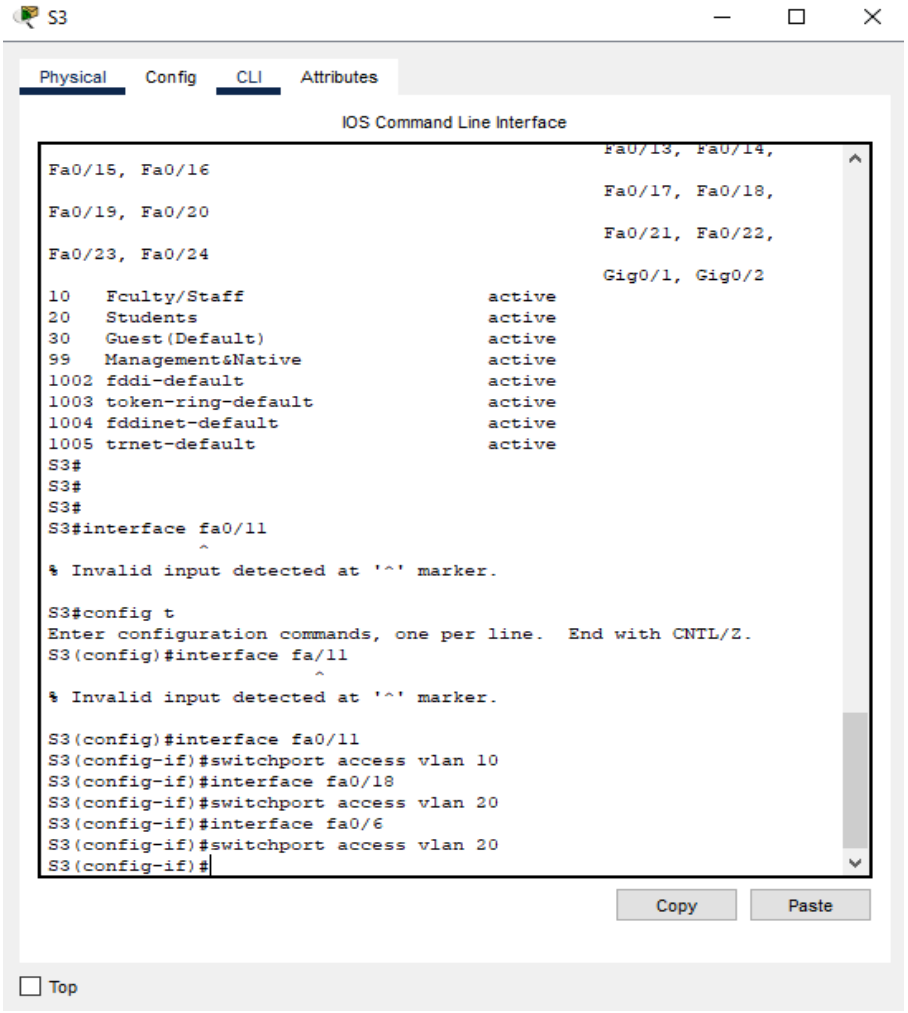
- VLAN 10: Fast Ethernet 0/11
- VLAN 20: Fast Ethernet 0/18
- VLAN 30: Fast Ethernet 0/6

```
S2(config)# interface fa0/11
S2(config-if)# switchport access vlan 10
S2(config-if)# interface fa0/18
S2(config-if)# switchport access vlan 20
S2(config-if)# interface fa0/6
S2(config-if)# switchport access vlan 30
```



3.2: Assign VLANs to the active ports on S3.

S3 uses the same VLAN access port assignments as S2.



3.3: Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully. Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, were the pings successful? Why? No, the pings failed because the ports between the switches are in VLAN 1 and PC1 and PC4 are in VLAN 10.

What could be done to resolve this issue? Configure the ports between the switches as trunk ports.

Step 4: Configure Trunks

4.1: Configure trunking on S1 and use VLAN 99 as the native VLAN.

a. Configure G0/1 and G0/2 interfaces on S1 for trunking.

```
S1(config)# interface range g0/1 - 2
S1(config-if)# switchport mode trunk
```

b. Configure VLAN 99 as the native VLAN for G0/1 and G0/2 interfaces on **S1**.

The trunk port takes about a minute to become active due to Spanning Tree which you will learn in the subsequent chapters. Click Fast Forward Time to speed the process. After the ports become active, you will periodically receive the following

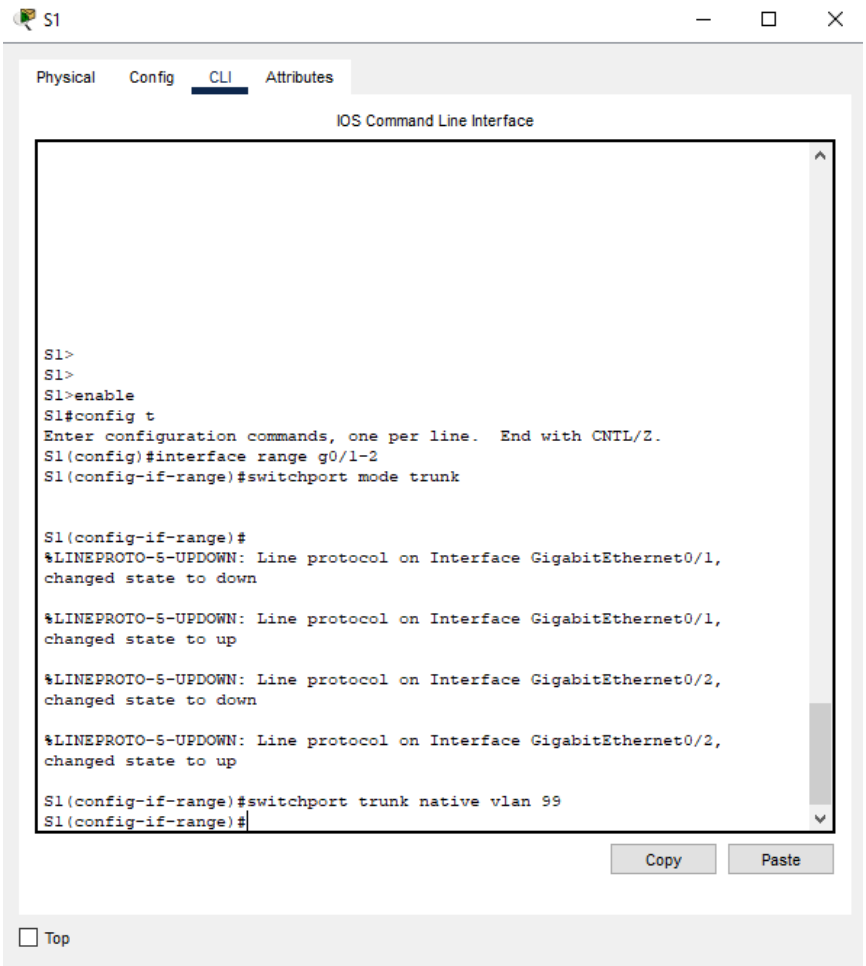
```
S1(config-if)# switchport trunk native vlan 99
```

syslog messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet0/2 (99), with S3 GigabitEthernet0/2 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet0/1 (99), with S2 GigabitEthernet0/1 (1).
```

You configured VLAN 99 as the native VLAN on S1. However, S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why? Pings are successful because trunking has been enabled on S1. Dynamic Trunking Protocol (DTP) has automatically negotiated the other side of the trunk links. In this case, S2 and S3 have now automatically configured the ports attached to S1 as trunking ports.



4.2: Verify trunking is enabled on S2 and S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.

Which active VLANs are allowed to cross the trunk? 1, 10, 20, 30, and 99.

4.3: Correct the native VLAN mismatch on S2 and S3.

1) Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.
2) Issue **show interface trunk** command to verify the correct native VLAN configuration.

4.4: Verify configurations on S2 and S3.

3) Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.
4) Use the **show vlan** command to display information regarding configured VLANs. Why port G0/1 on S2 is no longer assigned to VLAN 1? Port G0/1 is a trunk port and trunks ports are not displayed.

Specification Sheet-3.2: Configure VLAN and Apply Dynamic Trunk Protocol

Tools for Configuring VLAN and Applying DTP:

1. Network Switch
2. Command Line Interface (CLI)
3. Network Management Software
4. VLAN Configuration Templates
5. DTP Configuration Guide
6. Testing Tools

Materials for Configuring VLAN and Applying DTP:

1. Ethernet Cables
2. Console Cable
3. Network Diagram
4. Documentation
5. Labels

Learning Outcome-4: Configure Routing

Assessment Criteria	1. IP routing is interpreted 2. Routing protocol is interpreted 3. Types of routing is interpreted 4. Terms of routing is interpreted 5. Routing services is configured 6. Bandwidth management is performed as per requirement
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker • Internet Facilities 9. Whiteboard and Marker
Contents	1 IP routing 2 Types of routing ▪ Default routing ▪ Static routing ▪ Dynamic routing 3 Routing protocol ▪ AS ▪ EGP ▪ IGP ▪ OSPF ▪ RIP ▪ BGP ▪ EIGRP 4 Access control list (ACL) 5 Procedure to configure ACL 6 Routing services ▪ Static routing, ▪ Bridging ▪ PPPoE ▪ Pptp ▪ L2tp ▪ NAT 7 Procedure to manage Bandwidth

Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-4: Configure Routing

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Configure Routing"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Configure routing"	2. Read Information sheet 4: Configure routing 3. Answer Self-check 4: Configure routing 4. Check your answer with Answer key 4: Configure routing
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Job Sheet 4.1: Configure routing Specification Sheet 4.1: Configure routing

Information Sheet-4: Configure Routing

Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

4.1 IP routing
4.2 Types of routing
- Default routing
- Static routing
- Dynamic routing

4.3 Routing protocol
- AS
- EGP
- IGP
- OSPF
- RIP
- BGP
- EIGRP

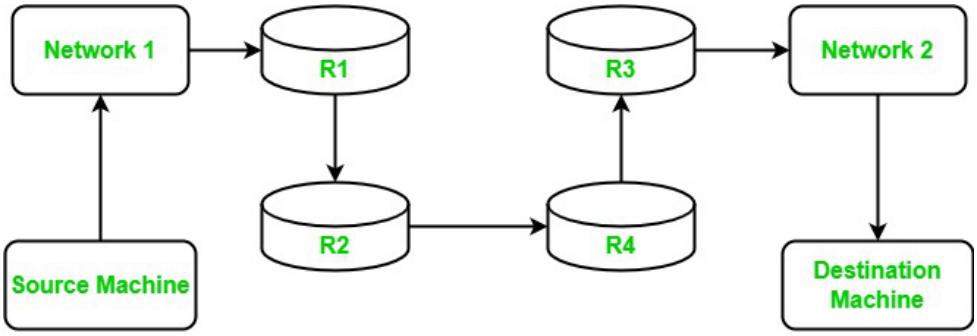
4.4 Access control list (ACL)
4.5 Procedure to configure ACL
4.6 Routing services
- Static routing,
- Bridging
- PPPoE
- Pptp
- L2tp
- NAT

4.7 Procedure to manage Bandwidth

4.1 IP routing

IP routing refers to the process of forwarding IP packets from one network to another. It is a fundamental function of routers in computer networks, enabling communication between devices on different networks. IP routing involves determining the best path for a packet to reach its destination based on the destination IP address and the information stored in the router's routing table.

Overall, IP routing is essential for enabling communication between devices on different networks and plays a crucial role in the functioning of the Internet and other large-scale computer networks.



IP Routing

4.2 Types of routing

- **Default routing**
  Default routing, as mentioned earlier, specifies a router's default next-hop gateway for packets with destinations outside of its locally connected networks. It is used when a router doesn't have a specific route for the destination IP address.

- **Static routing:**
  In static routing, network administrators manually configure routing tables on routers to determine the paths that packets should take to reach their destinations. Static routes do not change unless explicitly modified by administrators, making them simple to configure but less flexible in dynamic network environments.

- **Dynamic routing:**
  Dynamic routing protocols enable routers to automatically exchange routing information and dynamically update their routing tables based on network changes. Examples of dynamic routing protocols include:

  - **Distance Vector Protocols:** Protocols like Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP) use metrics like hop count to determine the best path to a destination.
  - **Link-State Protocols:** Protocols like Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) use information about network topology to calculate the shortest path to each destination.

4.3 Routing protocol

AS:

AS stands for Autonomous System. An Autonomous System is a collection of IP networks and routers under the control of one organization that presents a common routing policy to the Internet. ASes are fundamental units of routing on the Internet, and they play a crucial role in the operation of the Border Gateway Protocol (BGP), the primary routing protocol used for inter-domain routing on the Internet.

Overall, Autonomous Systems are integral to the structure and operation of the Internet, facilitating the exchange of routing information and enabling global connectivity between networks and users.

EGP:
EGP stands for Exterior Gateway Protocol. It is one of the earliest routing protocols used on the Internet for exchanging routing information between Autonomous Systems (ASes). EGP was defined in RFC 904 in 1984 and was initially used to route traffic between different networks on the early Internet.

IGP:
IGP stands for Interior Gateway Protocol. It's a type of routing protocol used to exchange routing information within an Autonomous System (AS). IGPs are responsible for determining the best paths to reach destinations within the same AS and are used for intra-domain routing.

Overall, Interior Gateway Protocols are essential for maintaining connectivity and efficient routing within Autonomous Systems, enabling devices to communicate and exchange data seamlessly within the same network.

OSPF:
OSPF stands for Open Shortest Path First. It is a link-state routing protocol used for intra-domain routing within Autonomous Systems (ASes). OSPF is widely used in enterprise networks, Internet Service Provider (ISP) networks, and large-scale deployments due to its scalability, flexibility, and support for complex network topologies.

Overall, OSPF is a robust and widely deployed routing protocol that provides efficient and scalable routing within Autonomous Systems, making it suitable for a wide range of network environments.

RIP:
RIP stands for Routing Information Protocol. It is one of the oldest distance vector routing protocols used for intra-domain routing within small to medium-sized networks. RIP is simple to configure and deploy, making it suitable for small networks, but it has limitations in scalability and convergence speed compared to more modern routing protocols like OSPF and EIGRP.
Overall, RIP is a simple and widely supported routing protocol suitable for small to medium-sized networks with relatively stable topologies. However, its limitations make it less suitable for large-scale deployments or networks with stringent performance and scalability requirements

BGP:
BGP stands for Border Gateway Protocol. It is the primary exterior gateway protocol used for inter-domain routing on the Internet. BGP is responsible for exchanging routing

information between Autonomous Systems (ASes) to determine the best paths for forwarding traffic across the Internet.

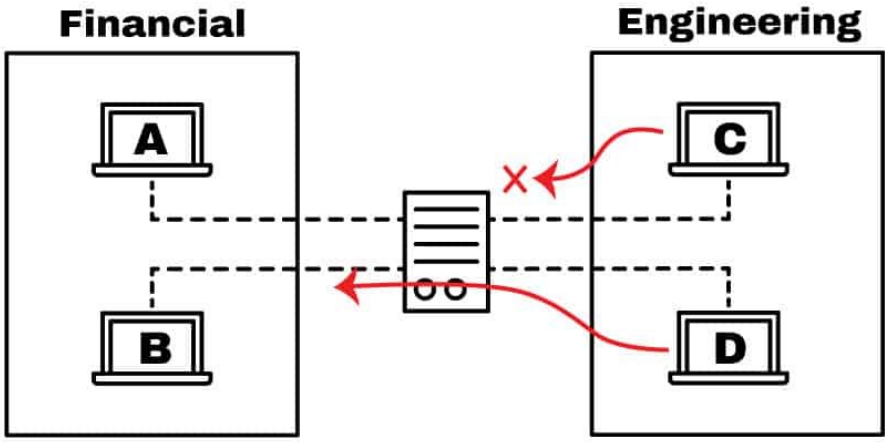
EIGRP:
EIGRP stands for Enhanced Interior Gateway Routing Protocol. It is a Cisco proprietary routing protocol used for intra-domain routing within Autonomous Systems (ASes). EIGRP combines features of both distance vector and link-state routing protocols, offering fast convergence, scalability, and support for complex network topologies.

Overall, EIGRP is a robust and efficient routing protocol suitable for enterprise networks, data center environments, and service provider networks. Its combination of fast convergence, scalability, and advanced features makes it a popular choice for Cisco-based network deployments.

4.4 Access control list (ACL)

An Access Control List (ACL) is a set of rules or conditions used to filter network traffic based on criteria such as source IP address, destination IP address, port numbers, protocol types, and other factors. ACLs are commonly used in network devices such as routers, switches, and firewalls to control the flow of traffic through the device, allowing or denying access to specific network resources or services.

Overall, Access Control Lists are essential tools for network administrators to enforce security policies, manage network traffic, and control access to network resources based on specific criteria. They play a crucial role in securing and optimizing network infrastructure in both enterprise and service provider environments.



4.5 Procedure to configure ACL

Configuring an Access Control List (ACL) involves defining rules that specify which types of traffic are allowed or denied based on criteria such as source and destination IP addresses, protocol types, and port numbers. Here's a general procedure to configure an ACL on a Cisco router:

i. Access the Device Configuration Mode:

- Log in to the router using SSH, Telnet, or a console connection.
- Enter privileged EXEC mode by typing '***enable'*** and providing the enable password if required.
- Access global configuration mode by typing ***'configure terminal'*** or ***'conf t'***.

ii. Create the ACL:

- Determine whether you need a standard or extended ACL based on your filtering requirements.
- For a standard ACL:

```
router(config)# access-list <acl-number> {permit|deny} <source>
```

- Replace ***<acl-number>*** with the ACL number (1-99) and ***<source>*** with the source IP address or subnet you want to filter.
- For an extended ACL:

```
router(config)# access-list<acl-number>{permit|deny}<protocol> <source>
```

Replace ***<protocol>*** with the protocol type (e.g., IP, TCP, UDP), ***<source>*** and ***<destination>*** with the source and destination IP addresses or subnets, and ***[operator] [port]*** with optional port-related parameters.

iii. Apply the ACL to an Interface:

- Navigate to the interface where you want to apply the ACL using the ***interface*** command followed by the interface name (e.g., ***interface GigabitEthernet0/0***).
- Specify the direction of traffic you want to filter (inbound or outbound) using the ***ip access-group <acl-number> {in|out}*** command.
- For example, to apply the ACL to inbound traffic on an interface, use:

```
router(config-if)# ip access-group <acl-number> in
```

iv. **Verify the ACL Configuration:**

- Use the '***show access-lists'*** command to display the configured ACLs and their entries.
- Verify that the ACL is applied to the correct interface and direction using the ***show running-config interface <interface>*** command.

v. Optional Steps:

- Repeat the above steps to create and apply additional ACLs as needed.
- Test the ACL configuration by sending traffic that matches the ACL criteria and verifying that it is permitted or denied as expected.
- Monitor network traffic and adjust the ACL configuration as necessary to meet changing requirements or address security concerns.

vi. **Save the Configuration:**

- Once you've verified that the ACL configuration is correct, save the configuration to the device's startup configuration to ensure that it persists across reboots.
- Use the write ***memory*** or ***copy running-config startup-config*** command to save the configuration changes.

4.6 Routing services

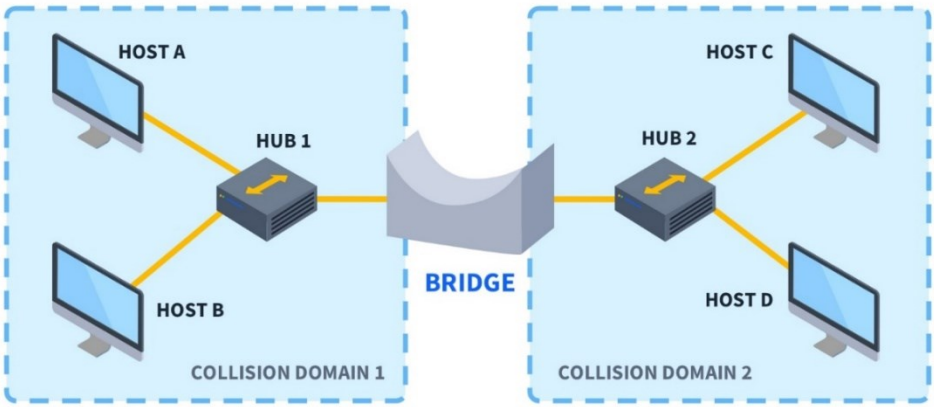
Static **routing:**

Static routing is a method of manually configuring the routing table of a network device, such as a router or a layer 3 switch, to specify the paths that packets should take to reach their destinations. Unlike dynamic routing protocols that automatically exchange routing information between routers, static routing requires network administrators to manually configure static routes on each router in the network.

Overall, static routing provides a simple and reliable method of forwarding packets in small or simple network environments where dynamic routing may not be necessary or practical. However, it has limitations in scalability and flexibility, making it less suitable for large-scale or dynamic network deployments.

Bridging:

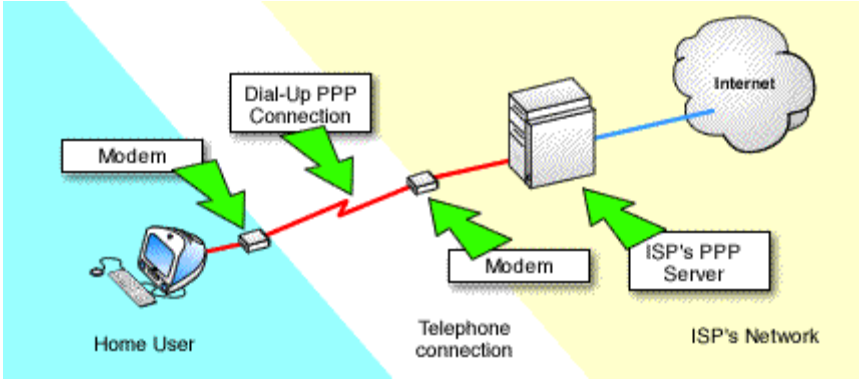
Bridging is a networking technique used to connect two or more separate network segments or LANs (Local Area Networks) together to form a single logical network. The device responsible for performing bridging is called a bridge. Bridges operate at the Data Link Layer (Layer 2) of the OSI (Open Systems Interconnection) model and are commonly used in Ethernet networks.



PPPoE:

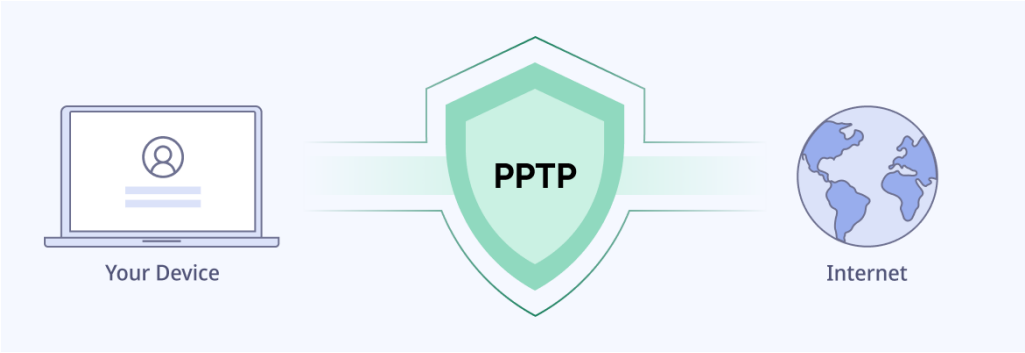
PPPoE stands for Point-to-Point Protocol over Ethernet. It is a networking protocol commonly used in broadband Internet connections to establish a point-to-point connection between a client device and an Internet Service Provider (ISP) using Ethernet as the

underlying transport medium. PPPoE encapsulates PPP frames within Ethernet frames, allowing the client device to connect to the ISP's network over a broadband connection, such as DSL or cable.



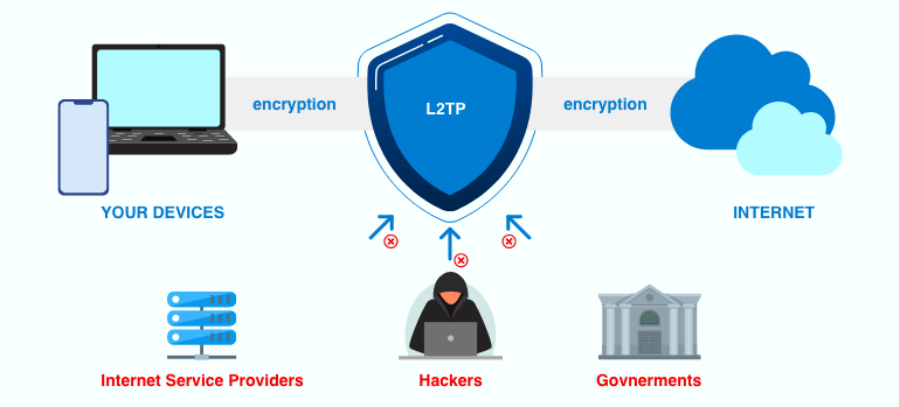
Pptp:

PPTP stands for Point-to-Point Tunneling Protocol. It is a networking protocol used to establish virtual private network (VPN) connections over the Internet or other public networks. PPTP encapsulates Point-to-Point Protocol (PPP) frames within IP packets, allowing remote users to securely access private networks or connect to the Internet through a VPN server.



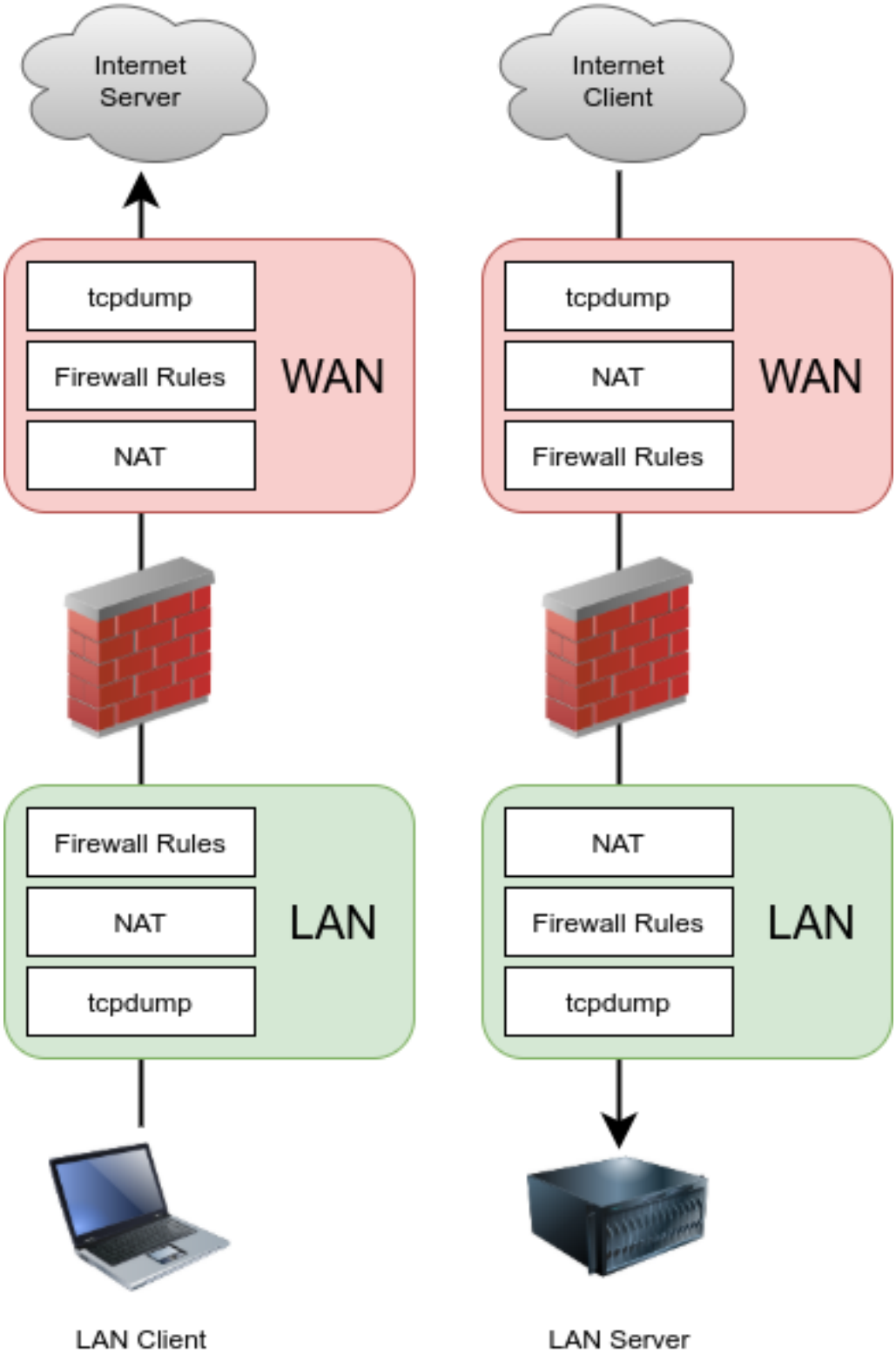
L2tp:

L2TP stands for Layer 2 Tunneling Protocol. It is a networking protocol used to establish virtual private network (VPN) connections over the Internet or other public networks. L2TP is commonly used in conjunction with IPsec (Internet Protocol Security) to provide encryption and authentication for VPN connections, creating a secure tunnel between a client device and a VPN server.



NAT:

NAT stands for Network Address Translation. It is a networking technique used to modify network address information in IP packet headers while they are in transit across a router or firewall. NAT is commonly used in IPv4 networks to allow multiple devices within a private network to share a single public IP address when accessing resources on the Internet.


Internet
Server
Internet
Client
tcpdump
Firewall Rules
NAT
WAN
tcpdump
NAT
Firewall Rules
WAN
Firewall Rules
NAT
tcpdump
LAN
NAT
Firewall Rules
tcpdump
LAN
LAN Client
LAN Server

4.7 Procedure to manage Bandwidth

Managing bandwidth involves controlling and optimizing the utilization of network resources to ensure that critical applications receive the necessary bandwidth while preventing congestion and ensuring fair access for all users. Here's a general procedure to manage bandwidth effectively:

i. **Understand Network Requirements:**

- Identify the critical applications, services, and users that require priority access to bandwidth.
- Determine the bandwidth requirements of each application or service, considering factors such as peak usage, latency sensitivity, and data transfer rates.

ii. Implement Quality of Service (QoS):

- Configure Quality of Service (QoS) policies on network devices, such as routers and switches, to prioritize traffic based on application requirements.
- Define QoS policies that classify and mark packets based on criteria such as application type, source/destination IP addresses, port numbers, and protocol.
- Assign different levels of priority (e.g., high, medium, low) to different types of traffic to ensure that critical applications receive sufficient bandwidth.

iii. Traffic Shaping and Policing:

- Implement traffic shaping and policing mechanisms to regulate the flow of traffic and prevent congestion.
- Use traffic shaping to control the rate of traffic transmission, smoothing out bursts of traffic and ensuring a consistent flow.
- Use traffic policing to enforce bandwidth limits and drop excess traffic that exceeds defined thresholds, preventing network congestion and ensuring fair access for all users.

iv. Optimize Network Performance:

- Monitor network traffic and performance using network monitoring tools and traffic analysis.
- Identify bandwidth-intensive applications, users, or devices that may be consuming excessive resources and impacting network performance.
- Implement optimization techniques such as caching, compression, and protocol optimization to reduce bandwidth usage and improve network efficiency.

v. Implement Bandwidth Management Policies:

- Define and enforce bandwidth management policies that specify acceptable use of network resources, including bandwidth allocation, usage limits, and acceptable use guidelines.
- Communicate bandwidth management policies to users and provide training or education on best practices for optimizing bandwidth usage and avoiding network congestion.

vi. Regular Monitoring and Adjustment:

- Continuously monitor network performance, bandwidth utilization, and QoS metrics to identify trends, anomalies, and areas for improvement.
- Adjust bandwidth management policies, QoS configurations, and traffic shaping parameters as needed based on changing network conditions, user requirements, and application priorities.

vii. Capacity Planning:

- Conduct regular capacity planning exercises to assess current and future bandwidth requirements based on projected growth, changes in network topology, and evolving business needs.
- Allocate sufficient resources and upgrade network infrastructure as necessary to accommodate increasing bandwidth demands and ensure optimal performance.

.

Self-Check Sheet-4: Configure Routing

1. What is IP routing?

Answer

2. What is ACL?

   Answer

3. Why is it important to configure switch ports appropriately for DTP?

   Answer

4. What does PPPoE stand for and what is its purpose?

   Answer

5. How does PPPoE work?

   Answer

6. What is the abbreviation PPTP and what does it enable?

   Answer

7. How does PPTP encapsulate data for secure transmission?

   Answer

8. What does L2TP stand for and how is it commonly used?

   Answer

9. What does L2TP create between a client device and a VPN server?

   Answer

10. What does NAT stand for and what is its purpose?

    Answer

Answer Key-4: Configure Routing

1. **What is IP routing?**

   Answer: IP routing refers to the process of forwarding IP packets from one network to another. It is a fundamental function of routers in computer networks, enabling communication between devices on different networks. IP routing involves determining the best path for a packet to reach its destination based on the destination IP address and the information stored in the router's routing table.

2. **What is ACL?**
   Answer: An Access Control List (ACL) is a set of rules or conditions used to filter network traffic based on criteria such as source IP address, destination IP address, port numbers, protocol types, and other factors. ACLs are commonly used in network devices such as routers, switches, and firewalls to control the flow of traffic through the device, allowing or denying access to specific network resources or services.

3. **Why is it important to configure switch ports appropriately for DTP?**
   Answer: Configuring switch ports appropriately helps avoid unintended trunking or security vulnerabilities that may arise from DTP operation.

4. **What does PPPoE stand for and what is its purpose?**
   Answer: PPPoE stands for Point-to-Point Protocol over Ethernet. It is used to establish a point-to-point connection between a client device and an ISP over broadband connections like DSL or cable.

5. **How does PPPoE work?**
   Answer: PPPoE encapsulates PPP frames within Ethernet frames, allowing the client device to connect to the ISP's network using Ethernet as the underlying transport medium.

6. **What is the abbreviation PPTP and what does it enable?**
   Answer: PPTP stands for Point-to-Point Tunneling Protocol. It enables the establishment of VPN connections over the Internet or public networks.

7. **How does PPTP encapsulate data for secure transmission?**
   Answer: PPTP encapsulates PPP frames within IP packets, allowing remote users to securely access private networks or connect to the Internet through a VPN server.

8. **What does L2TP stand for and how is it commonly used?**
   Answer: L2TP stands for Layer 2 Tunneling Protocol. It is commonly used in conjunction with IPsec to provide encryption and authentication for VPN connections.

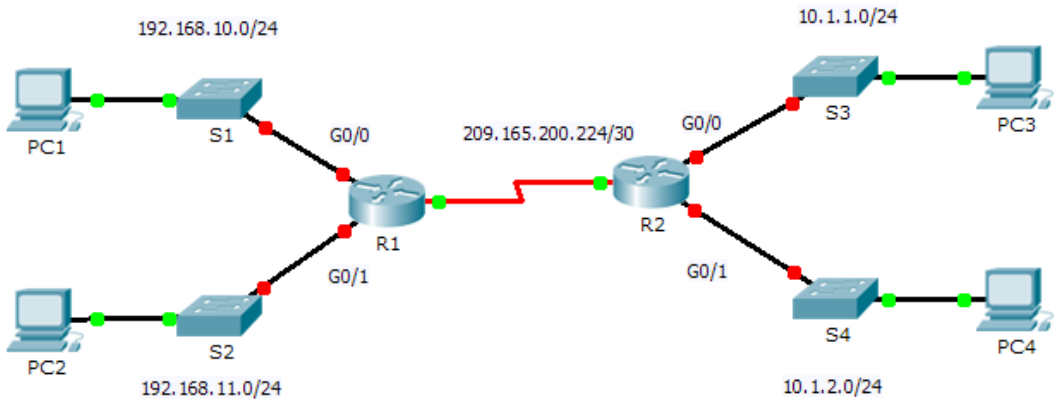
9. **What does L2TP create between a client device and a VPN server?**
   Answer: L2TP creates a secure tunnel between a client device and a VPN server, ensuring confidentiality and integrity of data transmitted over the VPN.

10. **What does NAT stand for and what is its purpose?**
    NAT stands for Network Address Translation. Its purpose is to modify network address information in IP packet headers while they are in transit across a router or firewall.

Job Sheet-4.1: Configure Routing

Working Procedure:

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	N/A
R2	G0/0	10.1.1.1	255.255.255.0	N/A
	G0/1	10.1.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Configuring routing involves setting up routing tables on network devices such as routers to determine the paths that packets take to reach their destinations. Follow this steps for configuring routing:

Step 1: Display Router Information

1.1: Display interface information on R1.

Note: Click a device and then click the CLI tab to access the command line directly. The console password is cisco. The privileged EXEC password is class.

a. Which command displays the statistics for all interfaces configured on a router? **show interfaces**
b. Which command displays the information about the Serial 0/0/0 interface only? **show interface serial 0/0/0**
c. c.Enter the command to display the statistics for the Serial 0/0/0 interface on R1 and answer the following questions:

   1) What is the IP address configured on **R1? 209.165.200.225/30**

   2) What is the bandwidth on the Serial 0/0/0 interface? **1544 kbits**

d. Enter the command to display the statistics for the GigabitEthernet 0/0 interface and answer the following questions:

   1) What is the IP address on R1? **There is no IP address configured on the GigabitEthernet 0/0 interface.**

   2) What is the MAC address of the GigabitEthernet 0/0 interface? **000d.bd6c.7d01**

   3) What is the bandwidth on the GigabitEthernet 0/0 interface? **1000000 kbits**

1.2: Display a summary list of the interfaces on R1.

a. Which command displays a brief summary of the current interfaces, statuses, and IP addresses assigned to them?

show ip interface brief

b. Enter the command on each router and answer the following questions:

   1) How many serial interfaces are there on R1 and R2? **Each router has 2 serial interfaces.**

   2) How many Ethernet interfaces are there on R1 and R2? **R1 has 6 Ethernet interfaces and R2 has 2 Ethernet interfaces.**

   3) Are all the Ethernet interfaces on R1 the same? If no, explain the difference(s). **No they are not. There are two Gigabit Ethernet interfaces and 4 Fast Ethernet interfaces. Gigabit Ethernet interfaces support speeds of up to 1,000,000,000 bits and Fast Ethernet interfaces support speeds of up to 1,000,000 bits.**

1.3: Display the routing table on R1.

a. What command displays the content of the routing table?

show ip route

b. Enter the command on R1 and answer the following questions:

1) How many connected routes are there (uses the C code)? 1

2) Which route is listed**? 209.165.200.224/30**

3) How does a router handle a packet destined for a network that is not listed in the routing table? **A router will only send packets to a network listed in the routing table. If a network is not listed, the packet will be dropped**.

Step 2: Configure Router Interfaces

2.1: Configure the GigabitEthernet 0/0 interface on R1.

a. Enter the following commands to address and activate the GigabitEthernet 0/0 interface on **R1**:

R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

b. It is good practice to configure a description for each interface to help document the network information. Configure an interface description indicating to which device it is connected.

R1(config-if)# description LAN connection to S1

c. **R1** should now be able to ping PC1.

R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

2.2: Configure the remaining Gigabit Ethernet Interfaces on R1 and R2.

a. Use the information in the Addressing Table to finish the interface configurations for R1 and R2. For each interface, do the following:

1) Enter the IP address and activate the interface.

2) Configure an appropriate description.

b. Verify interface configurations.

2.3: Back up the configurations to NVRAM.

Save the configuration files on both routers to NVRAM. What command did you use? **Copy run start**

Step 3: Verify the Configuration

3.1: Use verification commands to check your interface configurations.

a. Use the show ip interface brief command on both R1 and R2 to quickly verify that the interfaces are configured with the correct IP address and active.

How many interfaces on R1 and R2 are configured with IP addresses and in the "up" and "up" state**? 3 on each router**

What part of the interface configuration is NOT displayed in the command output? **The subnet mask**

What commands can you use to verify this part of the configuration**? show run, show interfaces, show ip protocols**

b. Use **the show ip route** command on both **R1** and **R2** to view the current routing tables and answer the following questions:

1) How many connected routes (uses the C code) do you see on each router? 3

2) How many EIGRP routes (uses the D code) do you see on each router? 2

3) If the router knows all the routes in the network, then the number of connected routes and dynamically learned routes (EIGRP) should equal the total number of LANs and WANs. How many LANs and WANs are in the topology? 5

4) Does this number match the number of C and D routes shown in the routing table? yes

Note: If your answer is "no", then you are missing a required configuration. Review the steps in Part 2.

3.2: Test end-to-end connectivity across the network.

You should now be able to ping from any PC to any other PC on the network. In addition, you should be able to ping the active interfaces on the routers. For example, the following should tests should be successful:

- From the command line on PC1, ping PC4.
- From the command line on R2, ping PC2.

Note: For simplicity in this activity, the switches are not configured; you will not be able to ping them.

Specification Sheet-4.1: Configure Routing

Tools for Configuring Routing:

1. Router
2. Command Line Interface (CLI)
3. Network Management Software
4. Routing Protocol Software
5. Routing Configuration Templates
6. Testing Tools

Materials for Configuring Routing:

1. Ethernet Cables
2. Console Cable
3. Network Diagram
4. Documentation
5. Labels

Learning Outcome-5: Test Newly Created Network

Assessment Criteria	1. Network performance is monitored using monitoring tools 2. Congestion of the network is observed 3. Reachability to the internet (if available) is tested
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker • Internet Facilities 9. Whiteboard and Marker
Contents	1. Network performance monitoring tools ▪ Wireshark ▪ Cacti ▪ Manage engine ▪ PRTG ▪ MRTG ▪ Solarwinds ▪ Zabix Materials and consumables 2. Congestion of the network 3. Reachability to the internet
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-5: Test Newly Created Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Test newly created network"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Test newly created network"	2. Read Information sheet 1: Test newly created network 3. Answer Self-check 1: Test newly created network 4. Check your answer with Answer key 1: Test newly created network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Task Sheet 1.1: Install Network performance monitoring tools (Wireshark) Specification Sheet 1.1: Install Network performance monitoring tools (Wireshark) Task Sheet 5.2: Use NPMT Functions Specification Sheet 1.1: Use NPMT Functions

Information Sheet-5: Test Newly Created Network

Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

5.1 Network performance monitoring tools
- Wireshark
- Cacti
- Manage engine
- PRTG
- MRTG
- Solarwinds
- Zabix Materials and consumables

5.2 Congestion of the network
5.3 Reachability to the internet

5.1 Network performance monitoring tools

Network performance monitoring tools (NPMT) are software solutions which is the process of measuring and monitoring the quality of service of a network. NPMT are essential for network administrators and IT professionals to help gather network data, measure performance variables, and identify potential issues or risks that networks operate efficiently and reliably. Given below some NPMT tools or software's example:

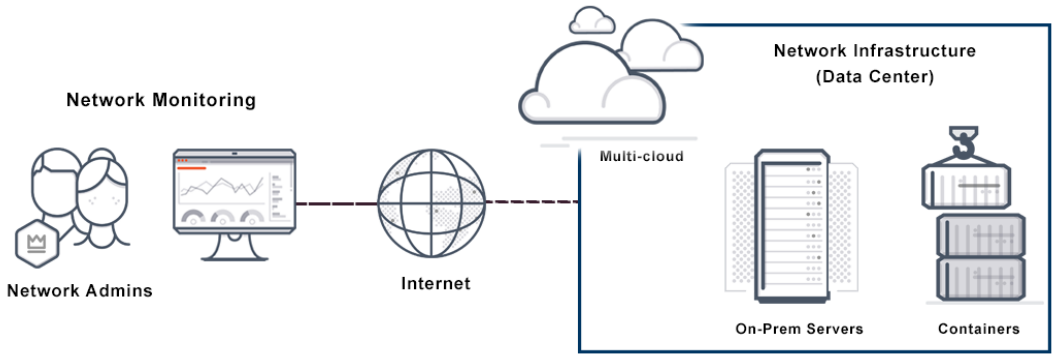


Figure: NPMT Working Process

Wireshark: Wireshark is a widely used, powerful open-source network protocol analyzer that can capture and display real-time details of network traffic. It is particularly used by network administrators, security professionals, developers, and enthusiasts for troubleshooting network issues, analyzing network protocols, and ensuring network security.

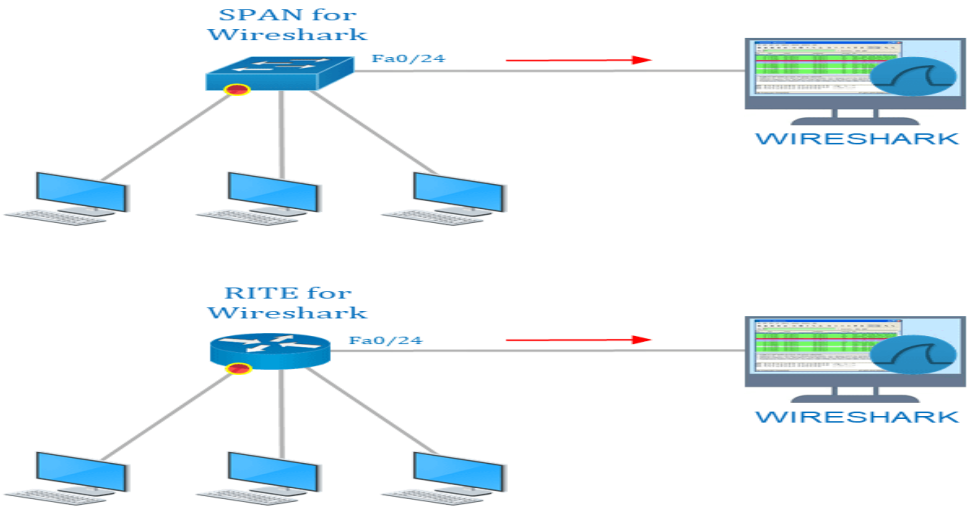


Figure: Wireshark

Cacti: Cacti is a versatile and scalable network monitoring tool (NPMT) which is an open-source, web-based network monitoring, performance, fault, and configuration management framework designed as a front-end application for the open-source, industry-standard data logging RRD (Round-robin database) tool. That provides valuable insights into network performance and helps maintain the stability and efficiency of network infrastructure.

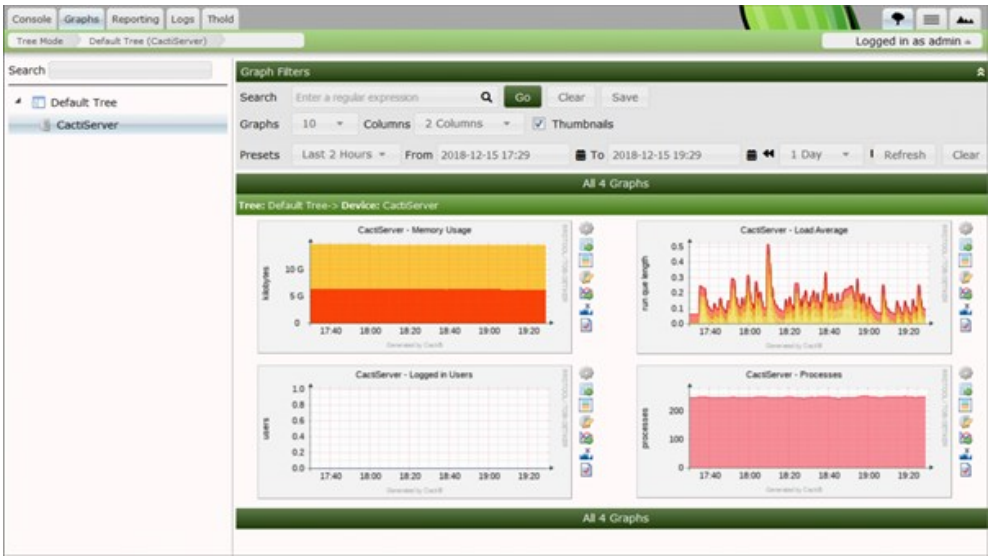


Figure: Cacti

Manage engine: ManageEngine is a suite of IT management software solutions developed by Zoho Corporation. It provides a comprehensive suite of IT management software designed to help organizations efficiently manage their IT infrastructure, improve operational efficiency, and enhance overall IT performance.

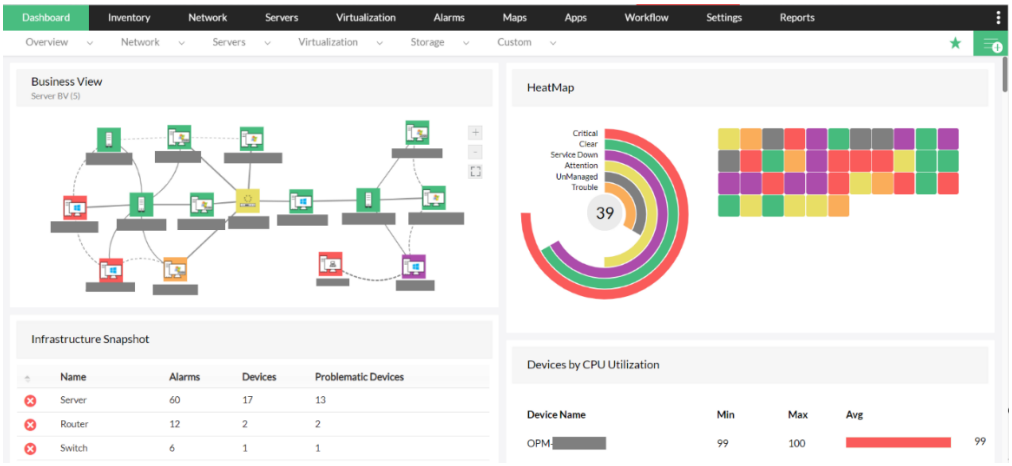
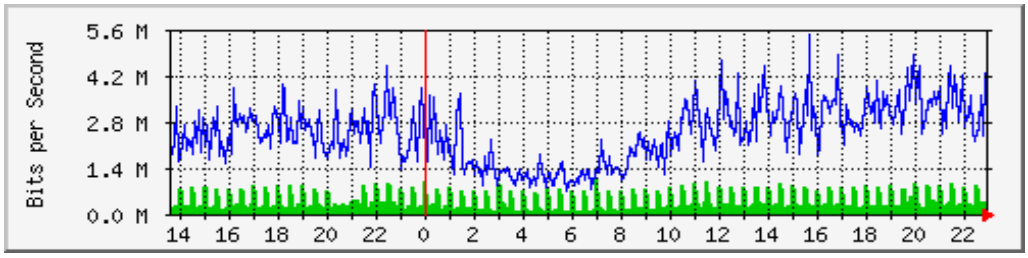


Figure: Manage Engine

PRTG: PRTG is a network monitoring software developed by Paessler AG. PRTG stands for "Paessler Router Traffic Grapher," reflecting its origins as a tool focused on monitoring router traffic. PRTG is network-monitoring software that can run on a Windows machine within your network and it can collect statistics from designated hosts such as routers, servers, switches and other important devices or applications.

Figure: PRTG

MRTG: MRTG stands for "Multi Router Traffic Grapher,". It is a network monitoring software developed by Paessler Tobias Oetiker.It is a free and open-source network monitoring tool primarily used to monitor the traffic load on network links. It is widely



used by network administrators and service providers to graphically display the traffic utilization of routers, switches, and other network devices over time.

Figure: MRTG

Solarwinds: SolarWinds Corporation is an American company (SolarWinds Inc.) that develops software for businesses to help manage their networks, systems, and information technology infrastructure. It provides comprehensive IT management software designed to help organizations monitor, manage, and secure their IT infrastructure effectively, improve operational efficiency, and ensure the reliability and performance of their IT systems and services.

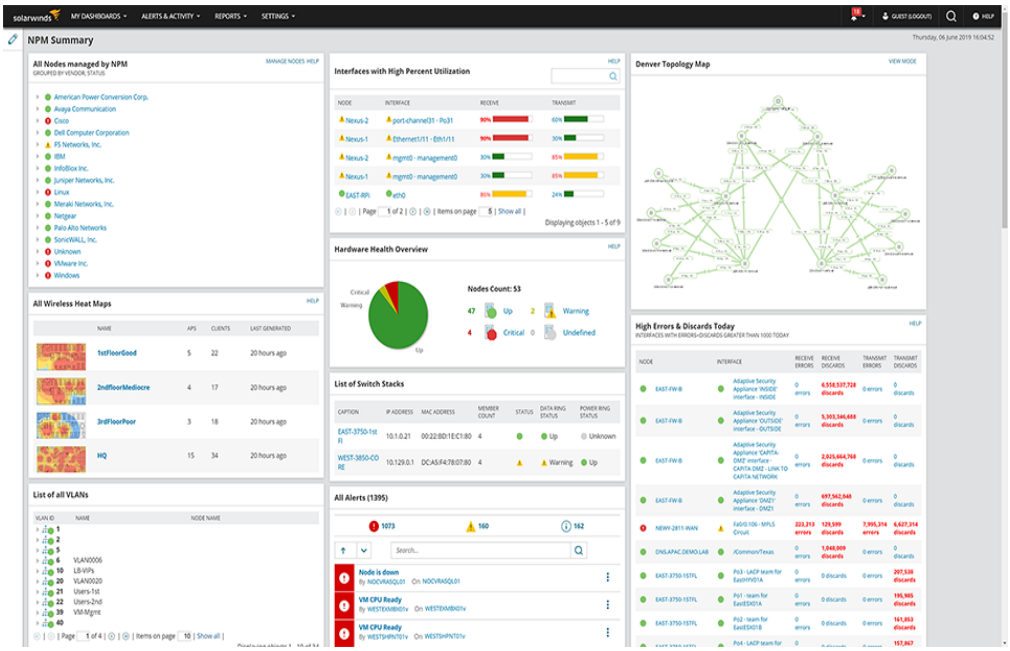
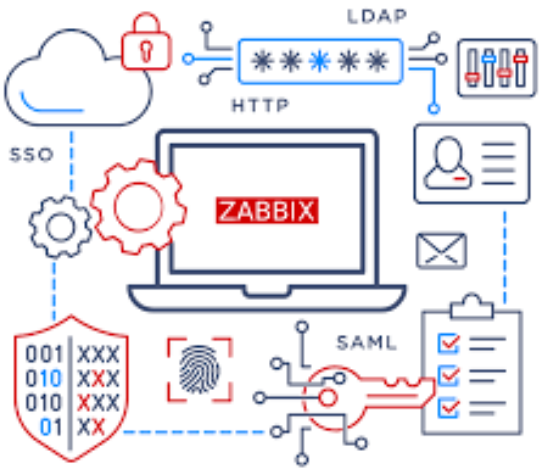


Figure: Solarwinds

Zabix Materials: Zabbix is an open-source network monitoring and management platform that provides monitoring of network services, servers, virtual machines, and other IT



assets. It offers a wide range of features for monitoring and alerting, making it a popular choice for organizations seeking a flexible and customizable monitoring solution.

Figure: Zabix Materials

5.2 Congestion of the network

Network congestion when network nodes and links are overloaded with traffic. This problem usually makes the end users' network slow. Congestion is often related to latency, throughput, and bandwidth. IT teams need to have a proper strategy to avoid, reduce, or temporarily eliminate network congestion. There are five ways to identify network congestion:

i. Bandwidth
ii. Latency
iii. Jitter
iv. Packet retransmission
v. Collisions

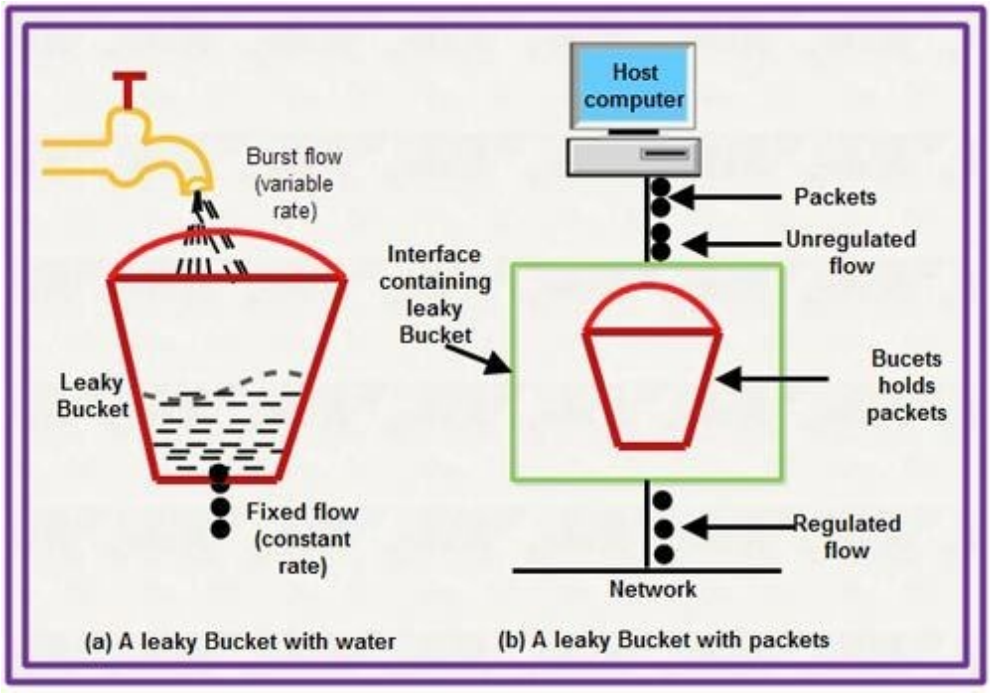


Figure: Congestion of the network

5.3 Reachability to the internet

Reachability to the internet refers to the ability of a device, network, or system to establish connections and exchange data with resources and services on the internet. It signifies whether a given entity can successfully send and receive data packets to and from destinations across the global network known as the internet.

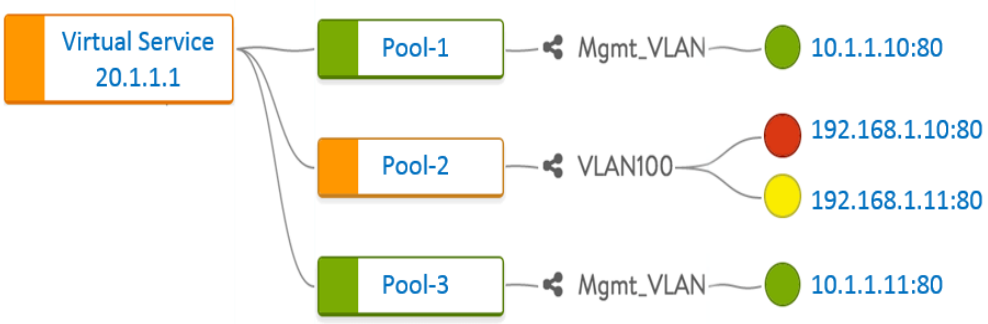


Figure: Reachability to the internet

Self-Check-5: Test Newly Created Network

1. List some network performance monitoring tools
   Answer

2. What does "reachability to the internet" entail?
   Answer

3. Why is reachability to the internet important?
   Answer

Answer Key-5: Test Newly Created Network

4. List some network performance monitoring tools
    - Answer: Wireshark
    - Cacti
    - Manage engine
    - PRTG
    - MRTG
    - Solarwinds
    - Zabix Materials
    - Congestion of the network
    - Reachability to the internet

5. **What does "reachability to the internet" entail?**
   Answer: "Reachability to the internet" signifies the capability of a device or network to connect with and exchange data with resources on the internet.

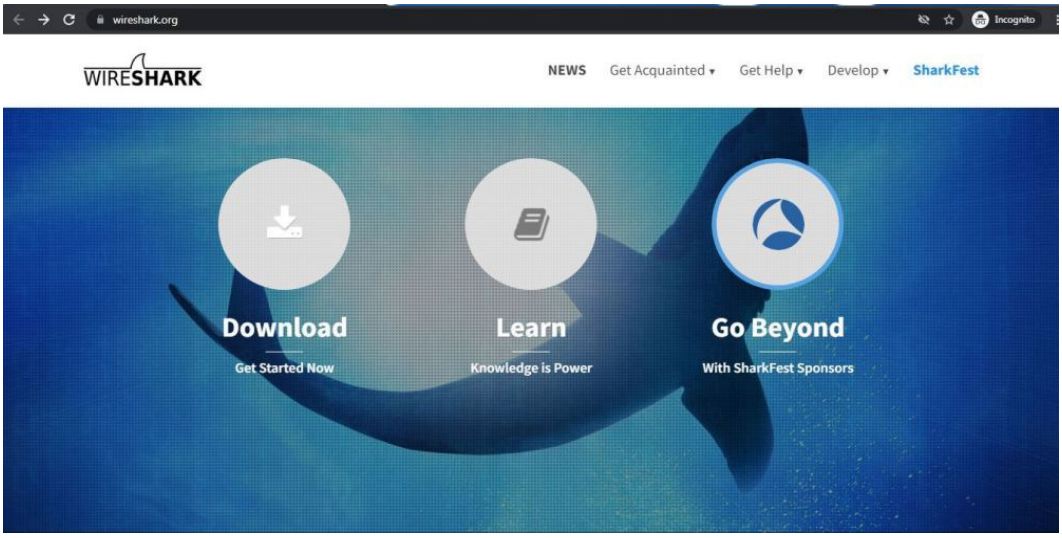
6. **Why is reachability to the internet important?**
   Answer: Reachability to the internet is crucial as it determines whether a device or network can successfully send and receive data packets to and from destinations across the global internet.

Job Sheet-5.1: Installing Network Performance Monitoring Tools (NPMT)

Working Procedure:

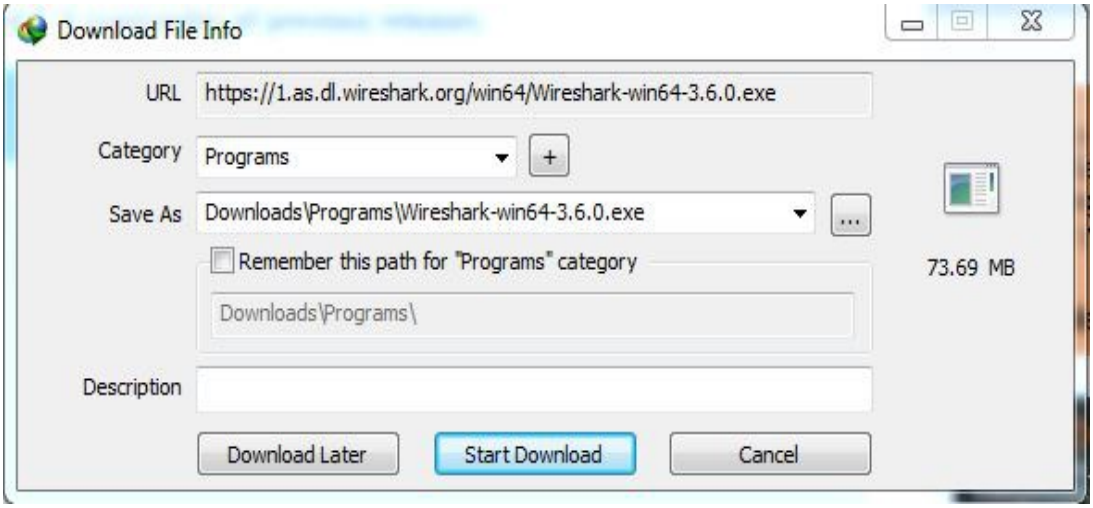
Installing network performance monitoring tools (NPMT) involves several steps, including downloading the software, installing it on your computer, and configuring it to simulate network environments. Here's a general procedure for installing NPM tools:

Step 1: Visit the official Wireshark website (https://www.wireshark.org) using any web browser**.**

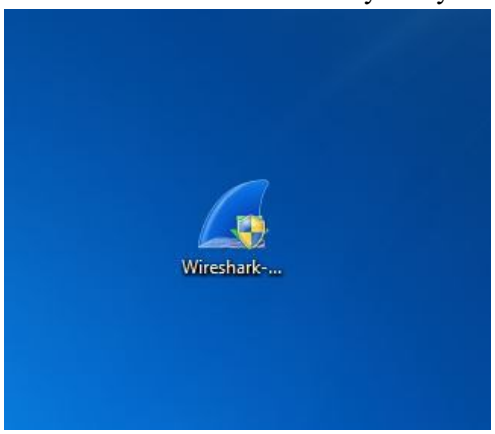


Step 2: Click on Download, a new webpage will open with different installers of Wireshark.

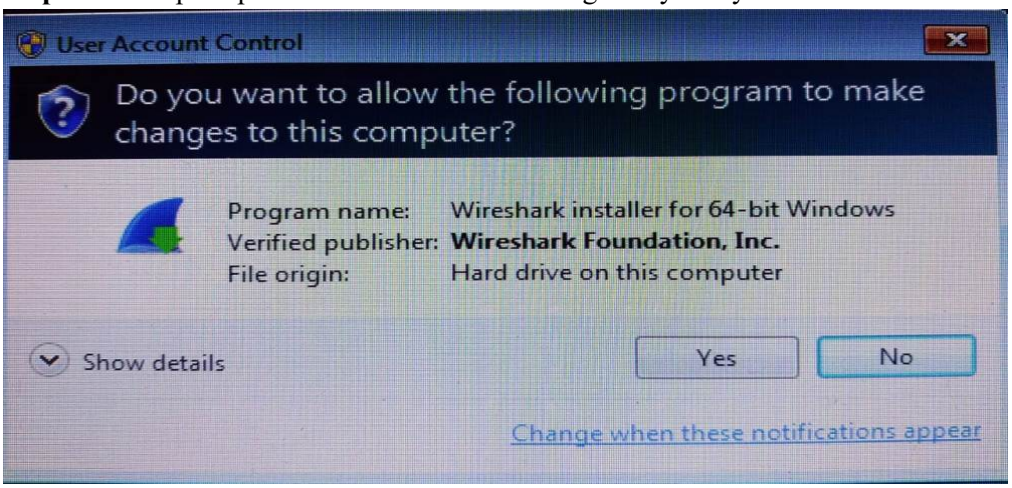
Step 3: Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.



Step 4: Now check for the executable file in downloads in your system and run it.

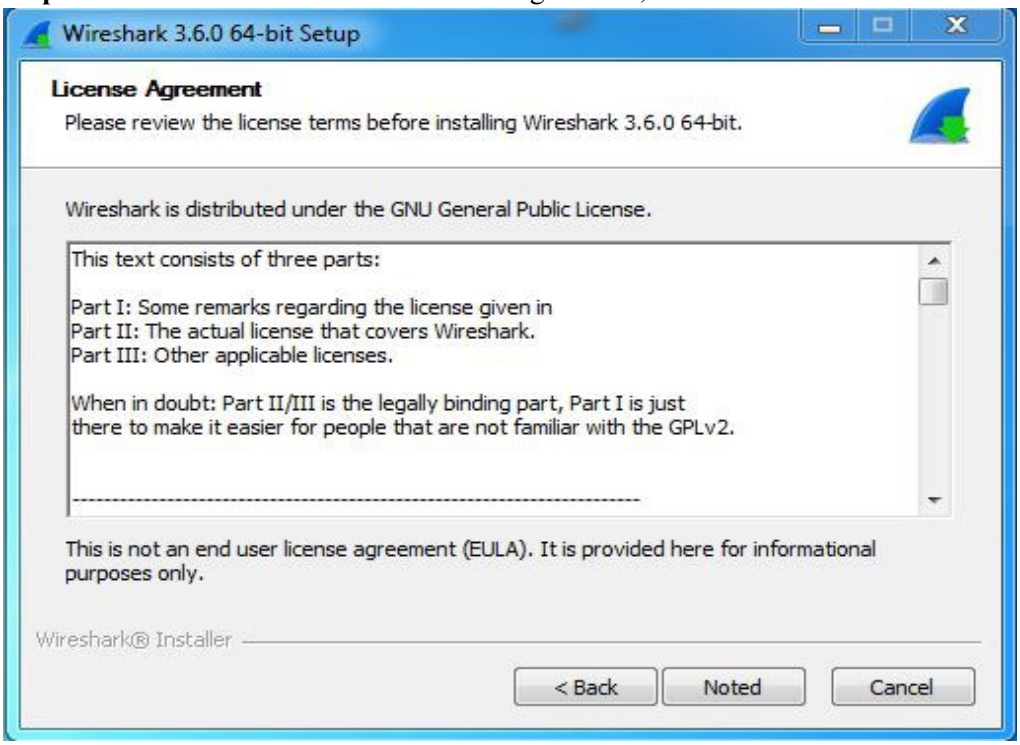


Step 5: It will prompt confirmation to make changes to your system. Click on Yes.

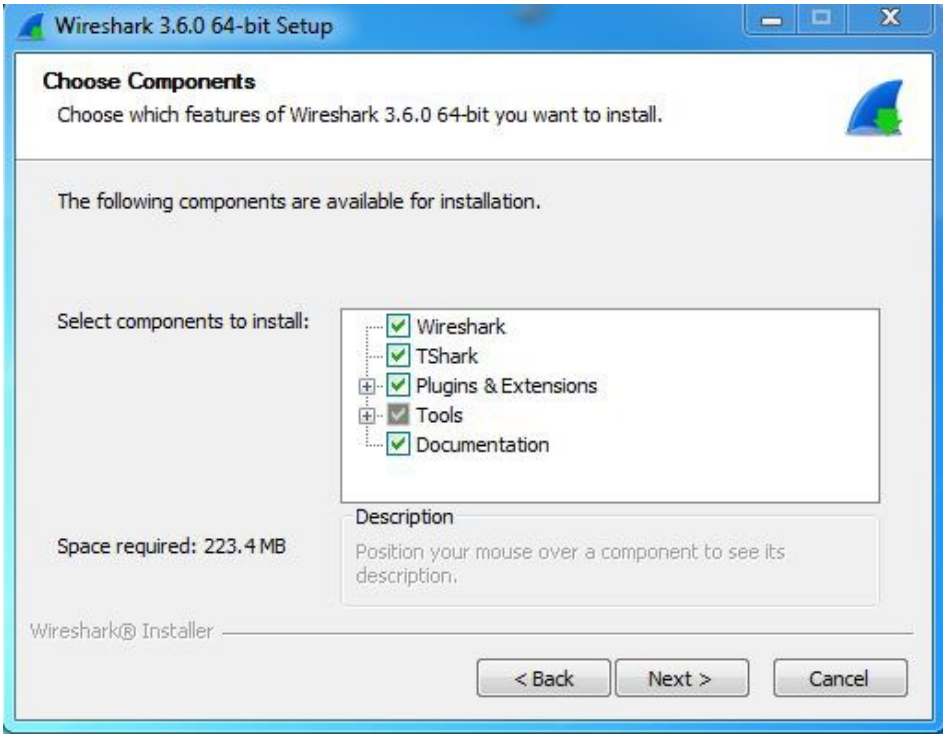


Step 6: Setup screen will appear, click on Next.

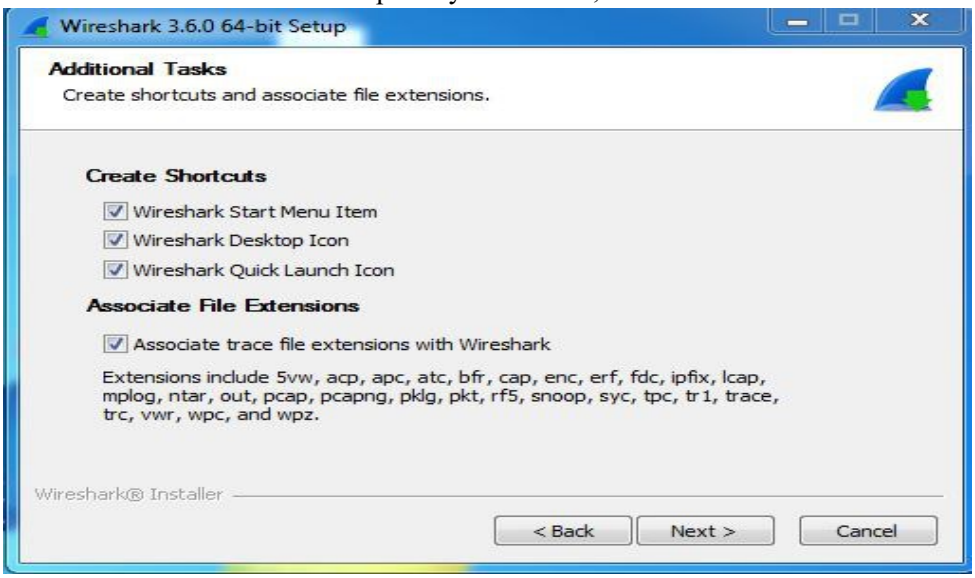
Step 7: The next screen will be of License Agreement, click on Noted.



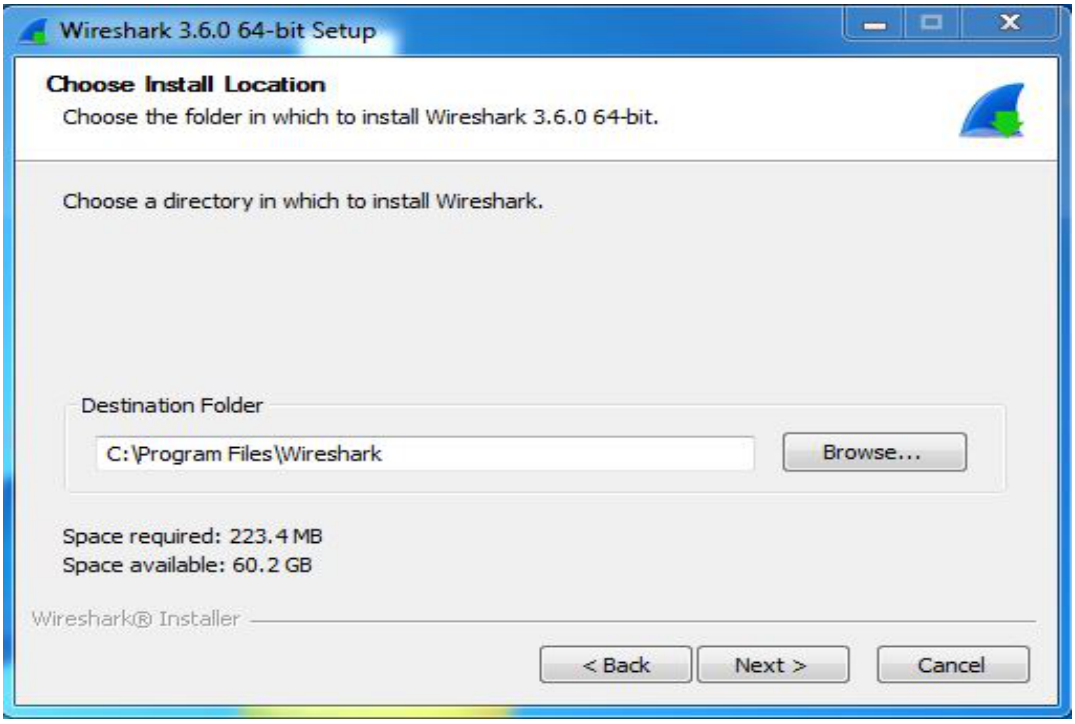
Step 8: This screen is for choosing components, all components are already marked so don't change anything Just click on the Next button.



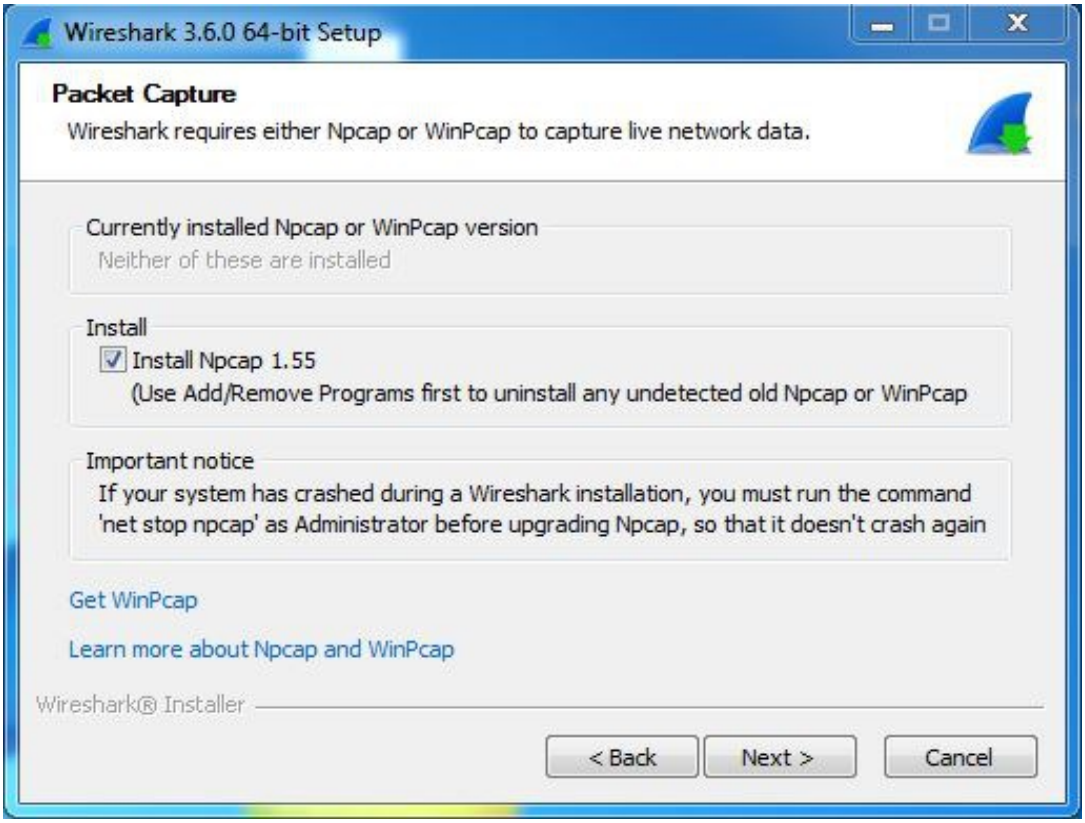
Step 9: This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.



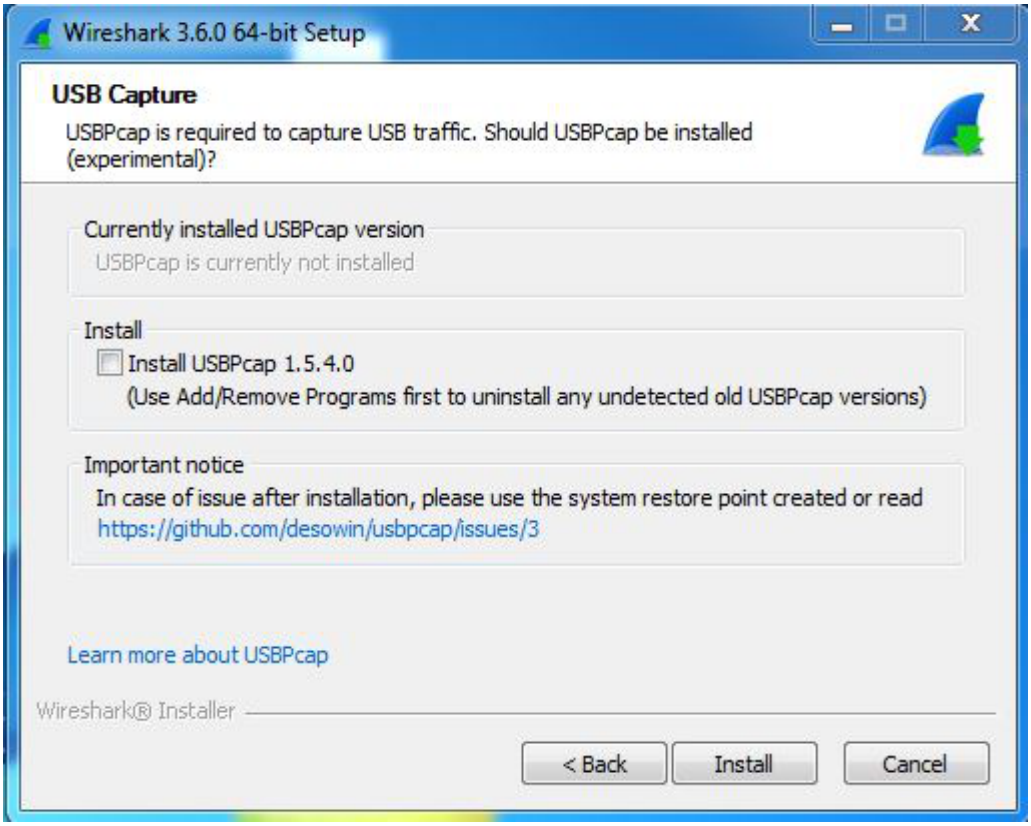
Step 10: The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed only a memory space of 223.4 MB.



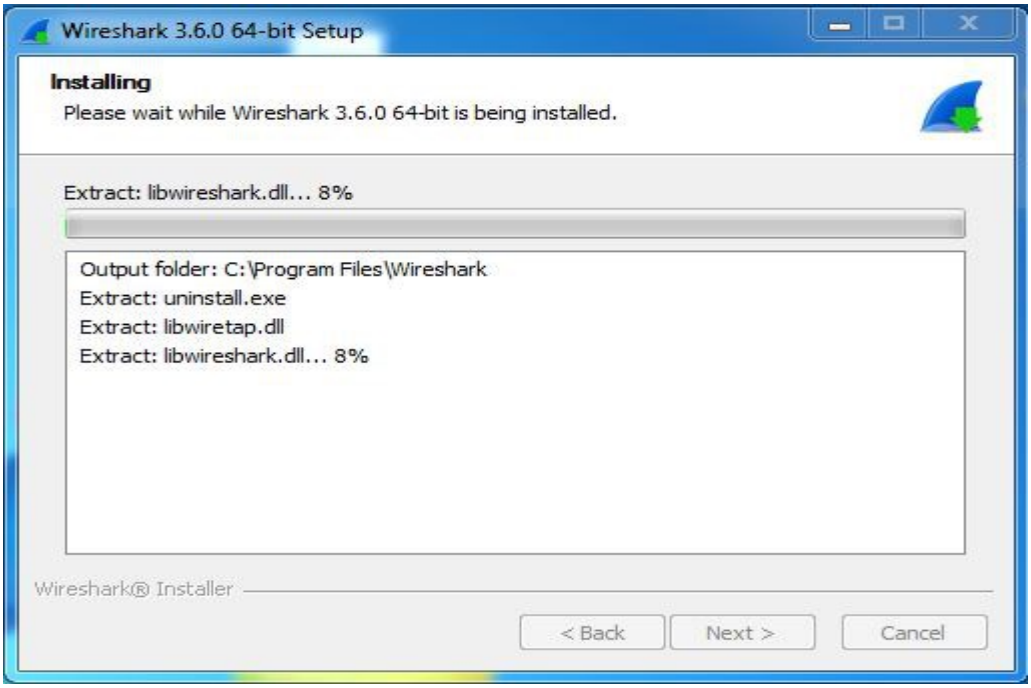
Step 11: Next screen has an option to install Npcap which is used with Wireshark to capture packets pcap means packet capture so the install option is already checked don't change anything and click the next button.



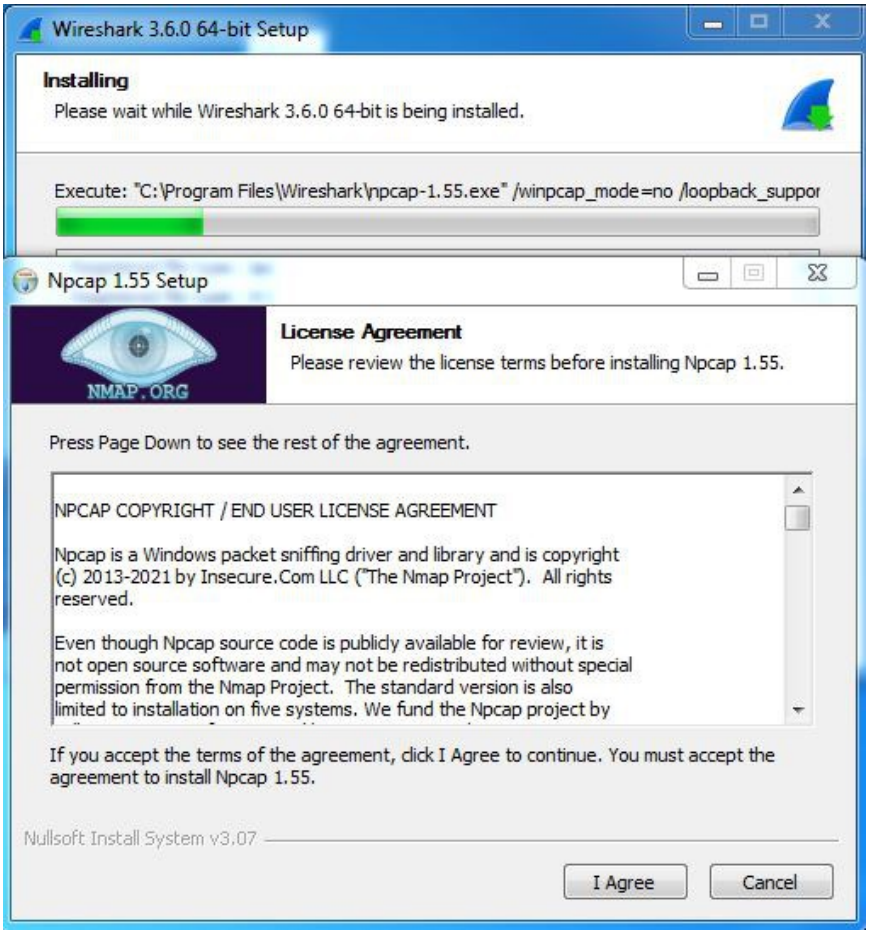
Step 12: Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.



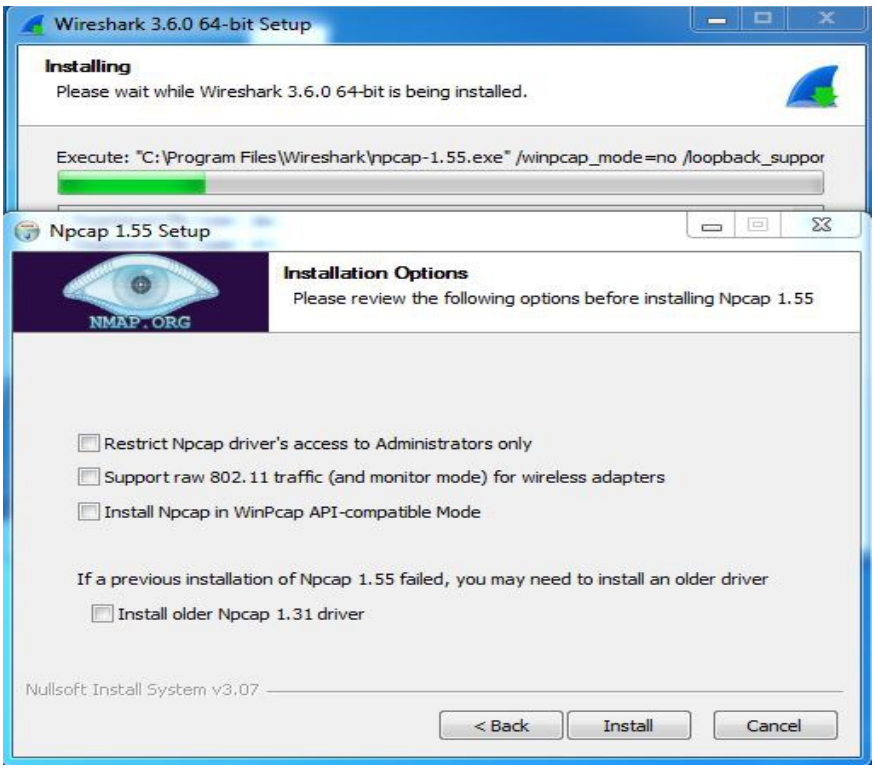
Step 13: After this installation process will start.



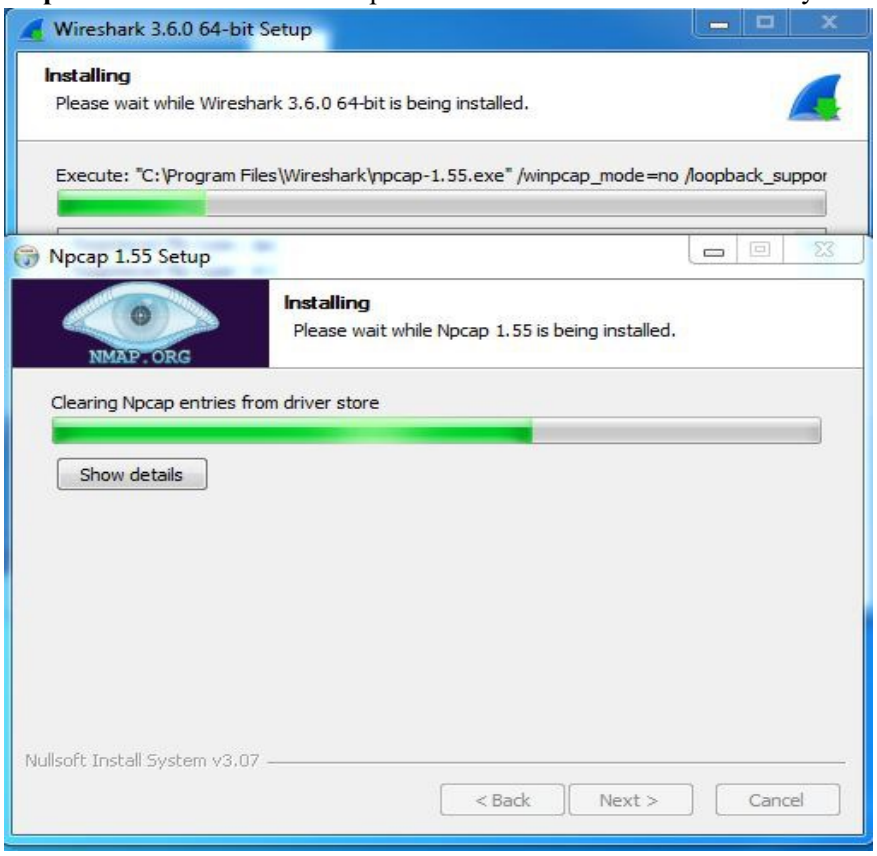
Step 14: This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the I Agree button.



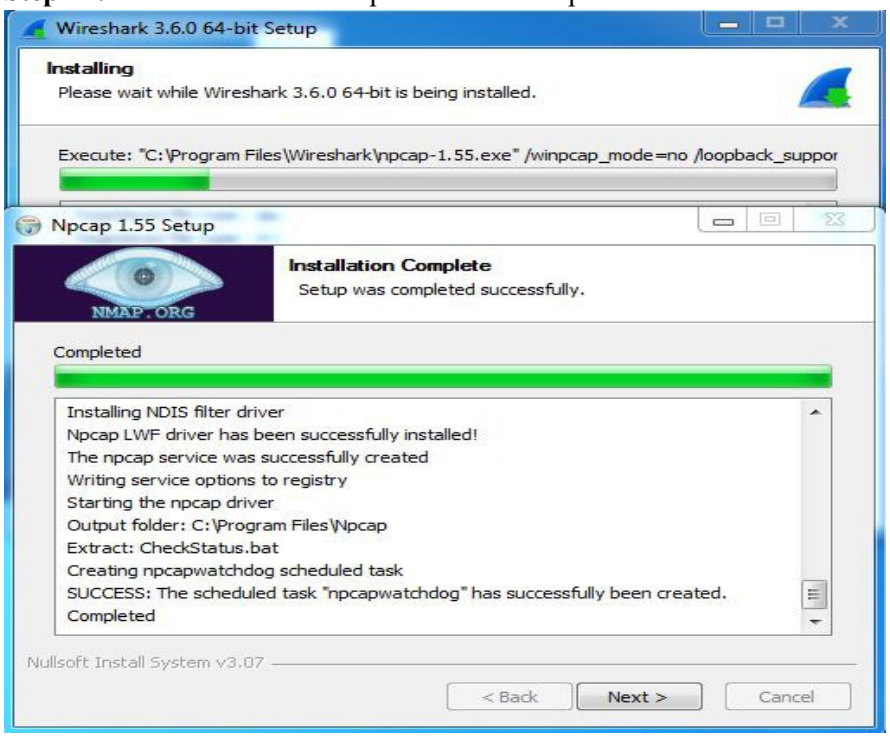
Step 15: Next screen is about different installing options of npcap, don't do anything click on Install.



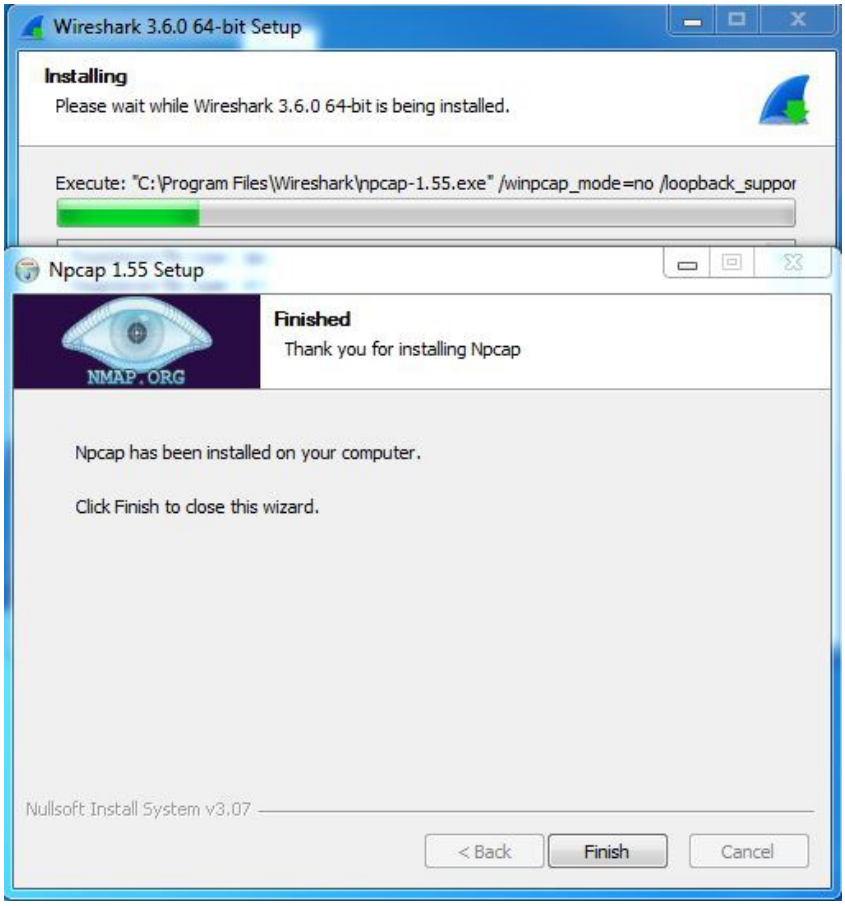
Step 16: After this installation process will start which will take only a minute.



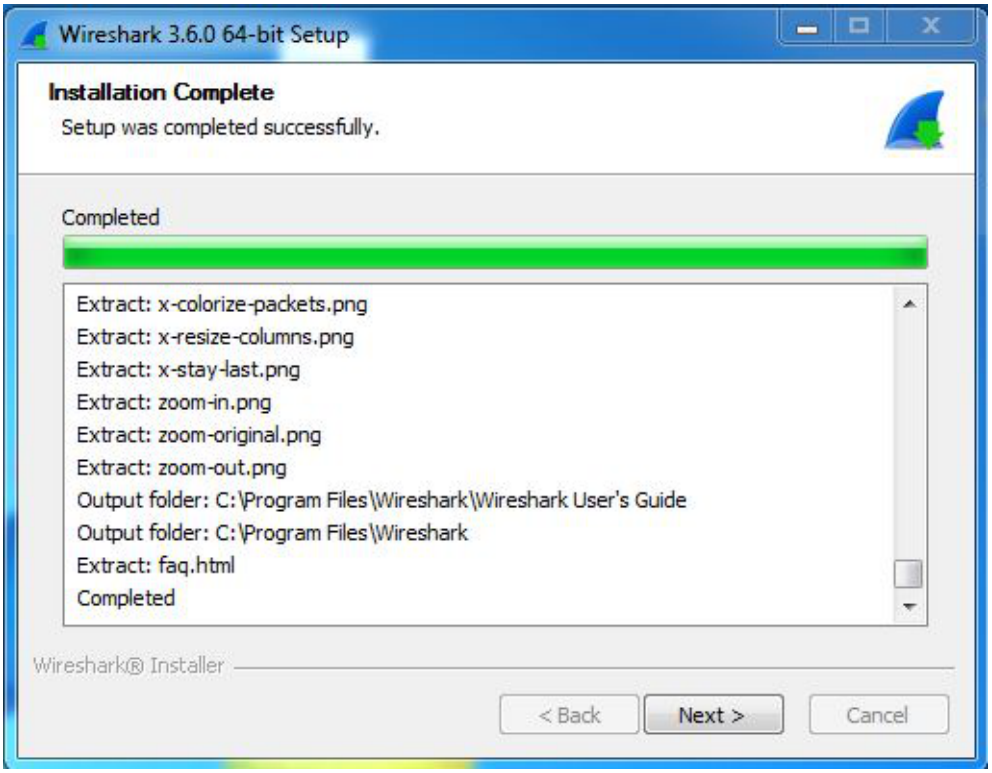
Step 17: After this installation process will complete click on the Next button.



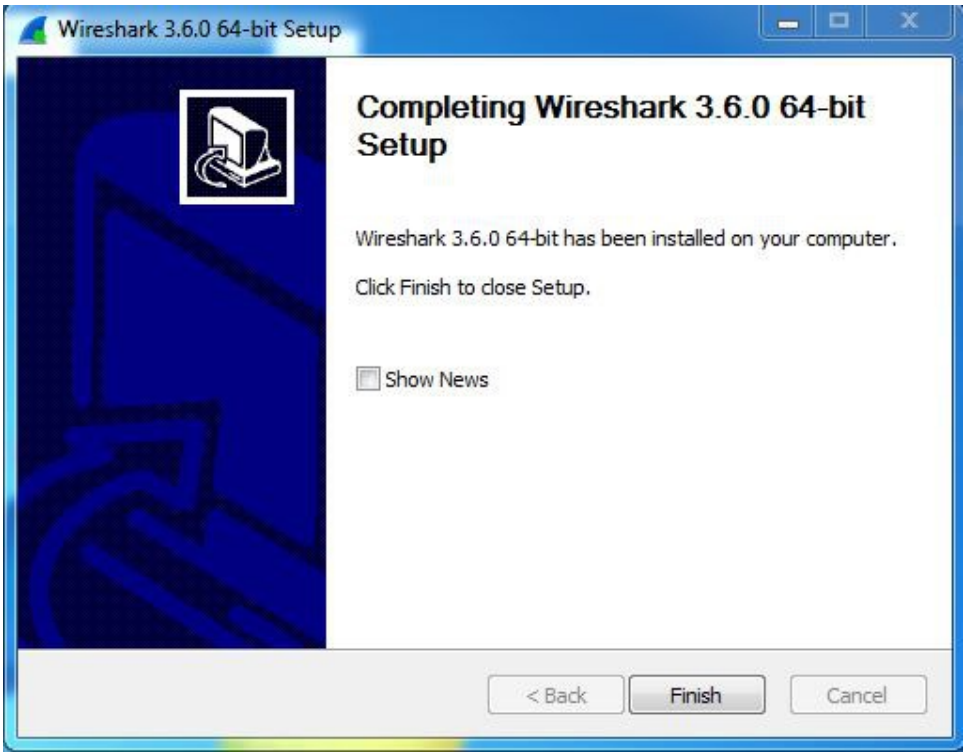
Step 18: Click on Finish after the installation process is complete.



Step 19: After this installation process of Wireshark will complete click on the Next button.

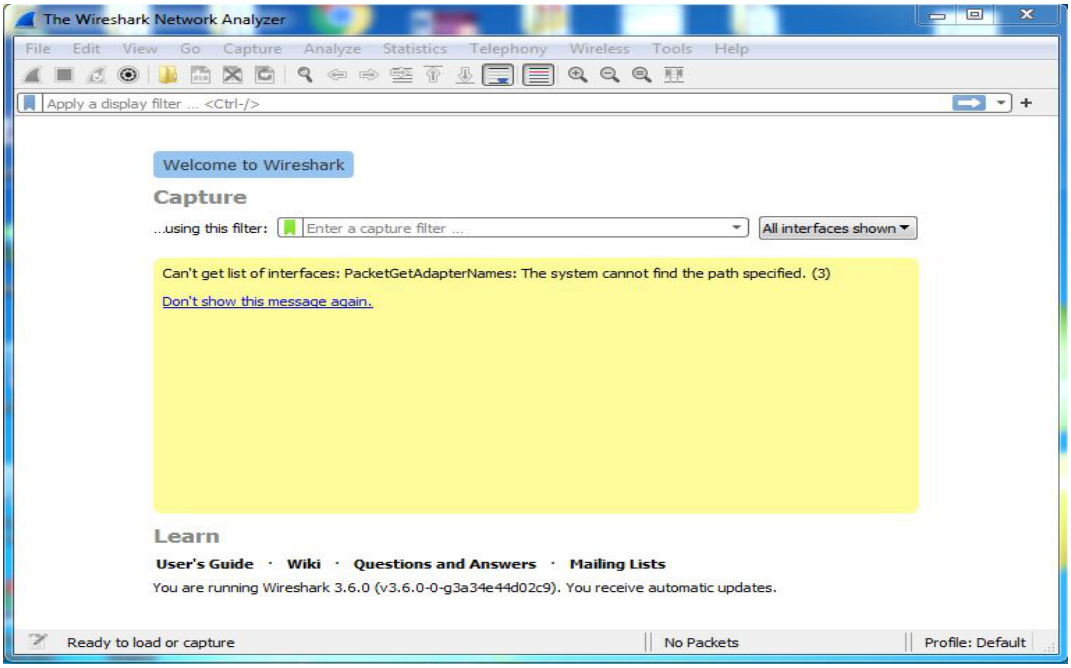


Step 20: Click on Finish after the installation process of Wireshark is complete.



Wireshark is successfully installed on the system and an icon is created on the desktop as shown below:

Now run the software and see the interface.



Congratulations!! At this point, you have successfully installed Wireshark on your windows system.

Specification Sheet-5.1: Install Network Performance Monitoring Tools (Wireshark)

Tools:

1. Computer or laptop: A device on which Wireshark will be installed.
2. Internet browser: To download the Wireshark installation files.
3. Administrative privileges: To install software on the device.

Materials:

1. Wireshark installation file: Downloaded from the official Wireshark website.
2. Storage space: Sufficient disk space to store the Wireshark installation files and captured network traffic.
3. Network connection: Required for downloading the installation files and for capturing live network traffic during analysis.

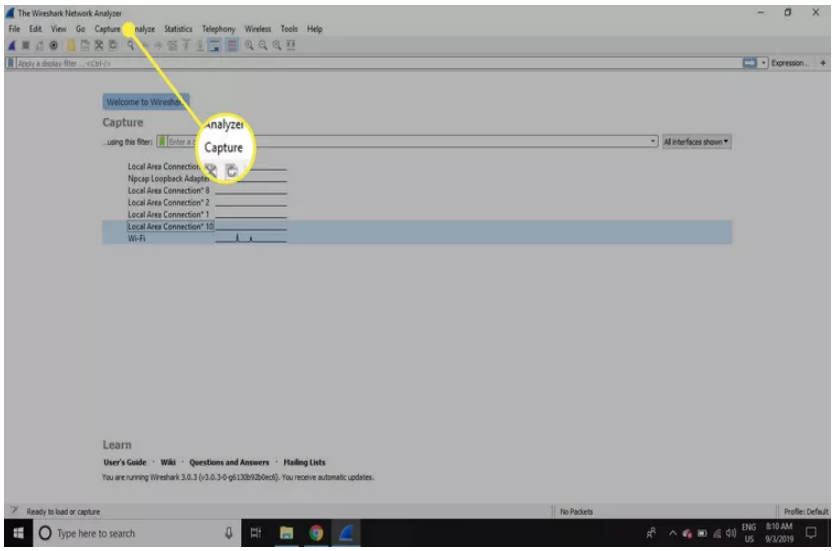
Task Sheet-5.2: Use NPMT Functions

Performance objective: At the end of the task trainee will be able to Use NPMT Functions.

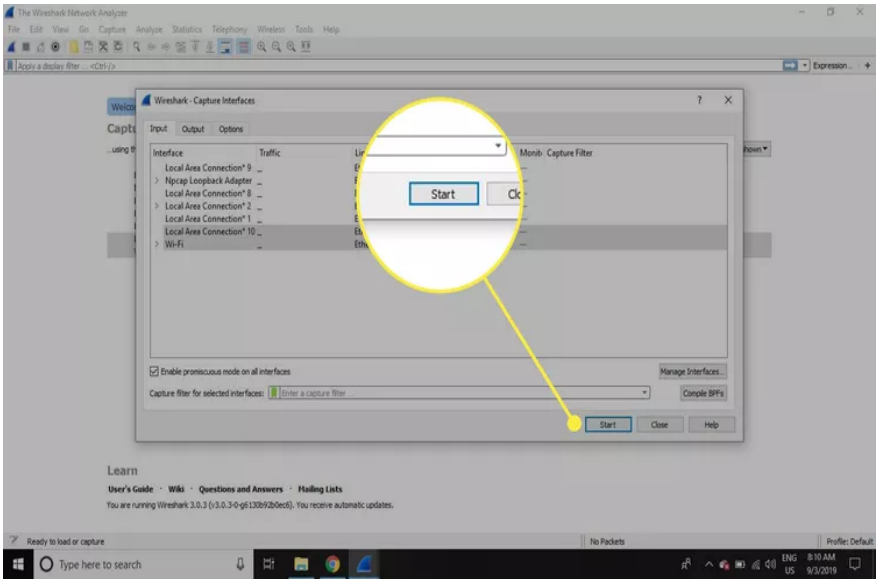
Work performance:

Capture Data Packets

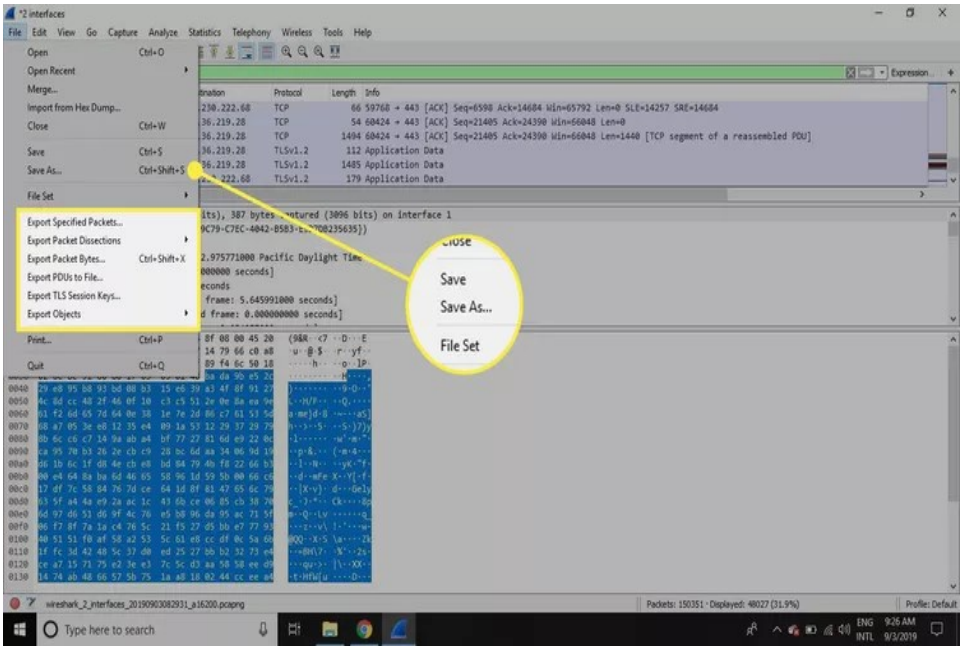
Step1: Select one or more of networks, go to the menu bar, then select Capture. (To select Multiple networks, hold the **Shift key** as you make your selection.)



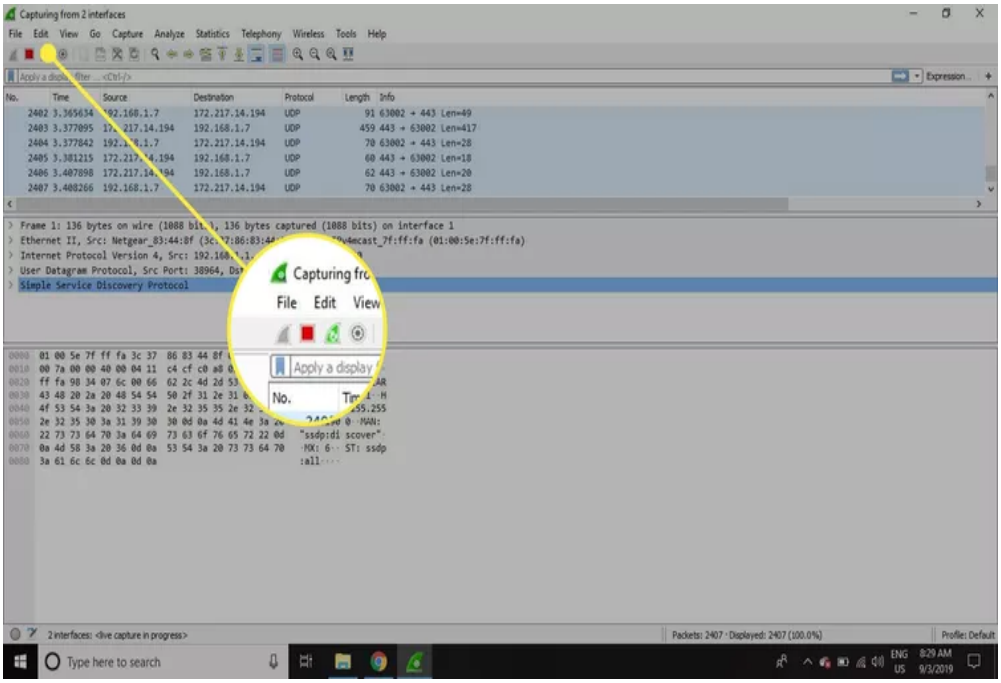
Step2: In the Wireshark Capture Interfaces window, select Start. (There are other ways to initiate packet capturing. Select the shark fin on the left side of the Wireshark toolbar, press **Ctrl+E**, or double-click the network.)



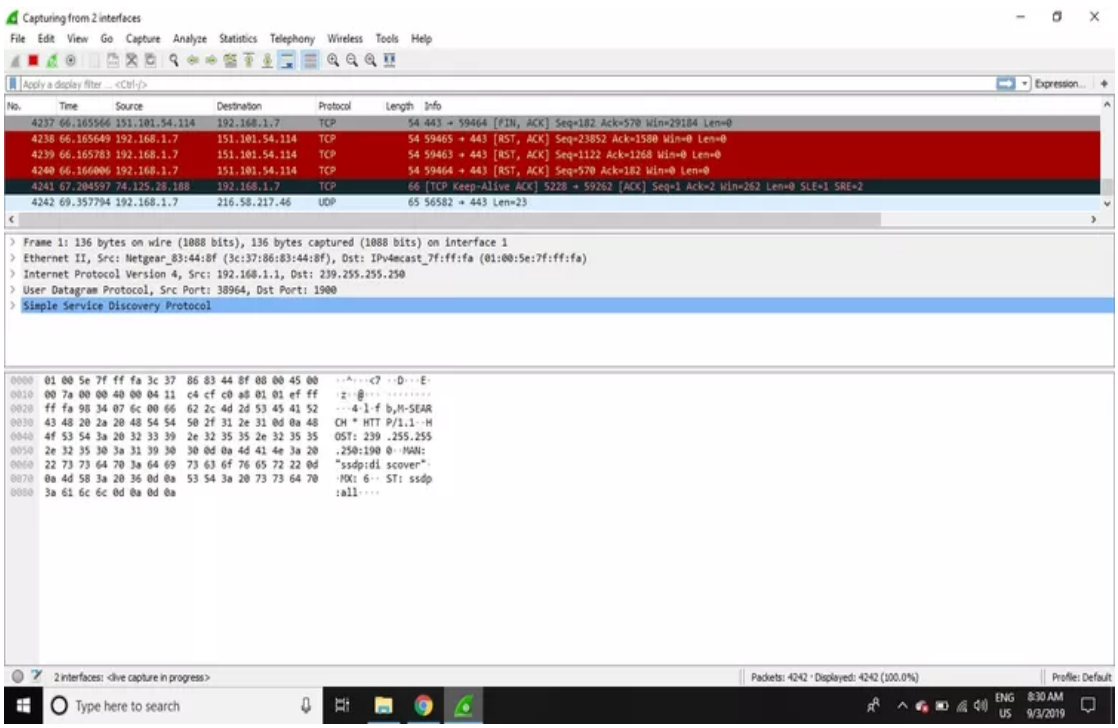
Step3: Select **File > Save** As or choose an Export option to record the capture.



Step4: To stop capturing, press **Ctrl+E**. Or, go to the Wireshark toolbar and select the red Stop button that's located next to the shark fin.



View and Analyze Packet Contents



Step 1: The packet list pane (the top section), located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points:

No: This field indicates which packets are part of the same conversation. It remains blank until you select a packet.

Time: The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture file was first created.

Source: This column contains the address (IP or other) where the packet originated.

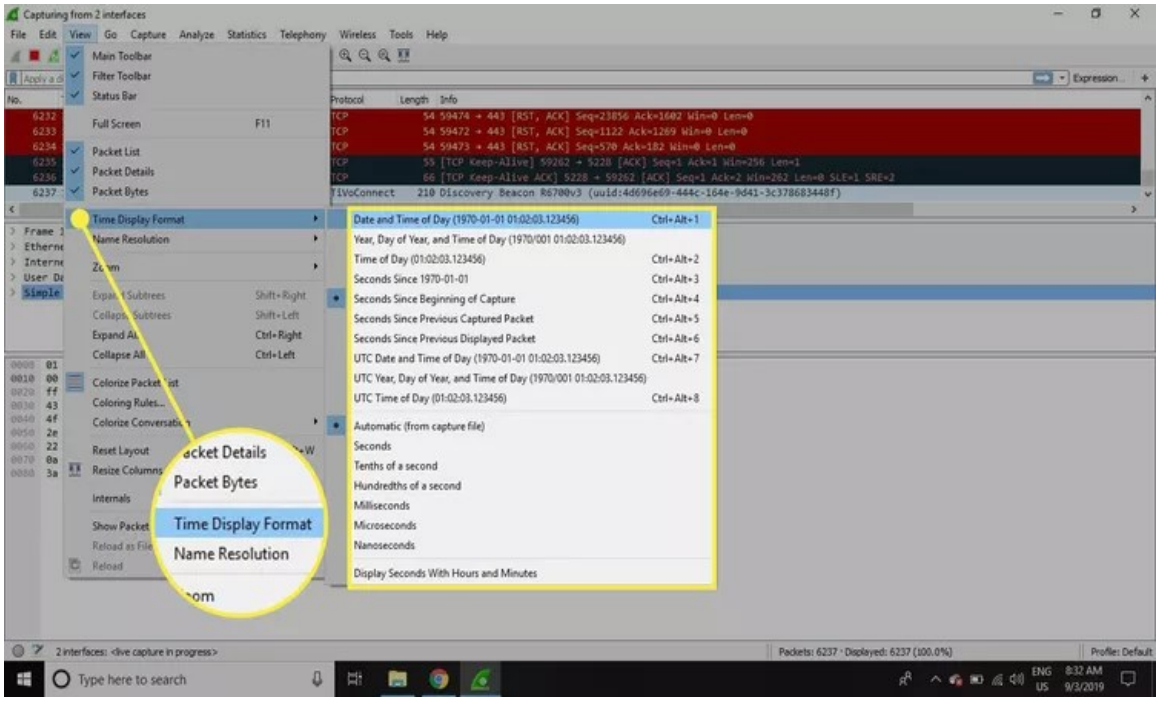
Destination: This column contains the address that the packet is being sent to.

Protocol: The packet's protocol name, such as TCP, can be found in this column.

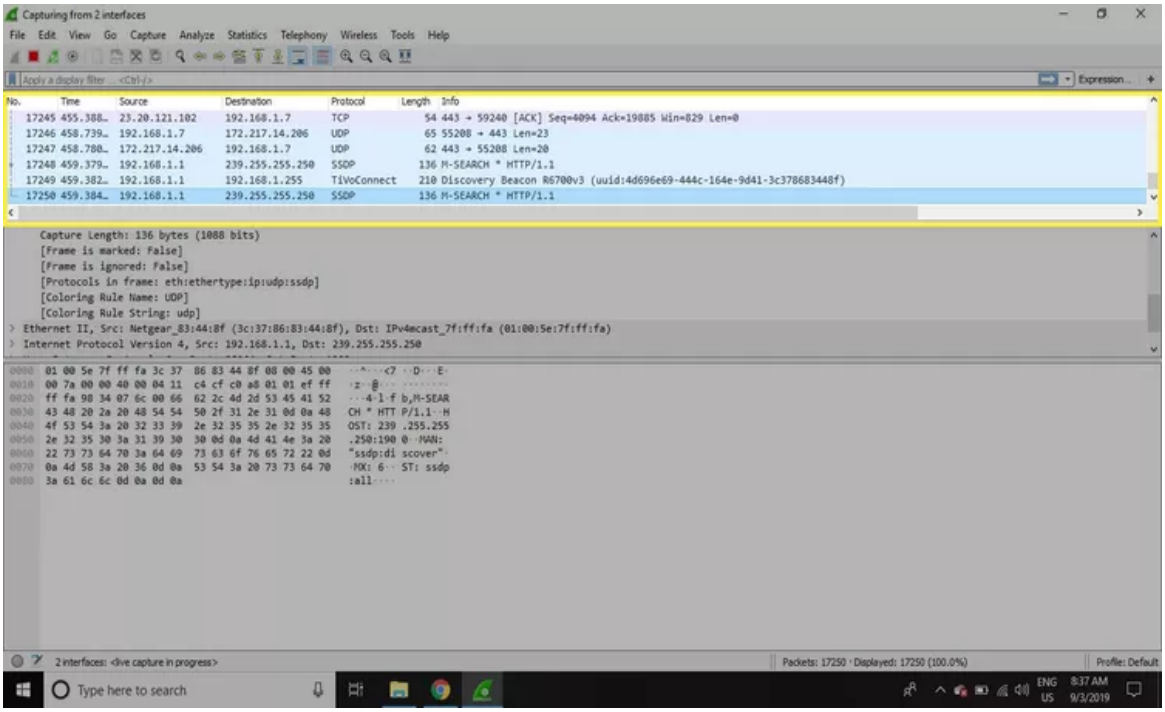
Length: The packet length, in bytes, is displayed in this column.

Info: Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.

To change the time format to something more useful (such as the actual time of day), select **View > Time Display Format**

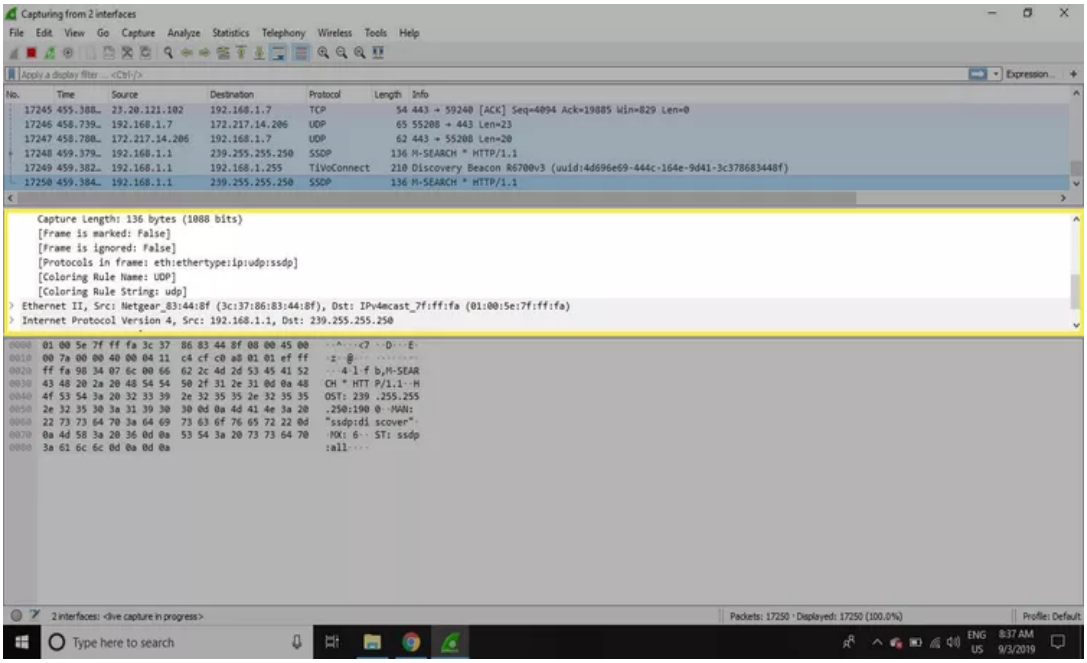


When a packet is selected in the top pane, you may notice one or more symbols appear in the No. column. Open or closed brackets and a straight horizontal line indicate whether a packet or group of packets are part of the same back-and-forth conversation on the network. A broken horizontal line signifies that a packet is not part of the conversation.



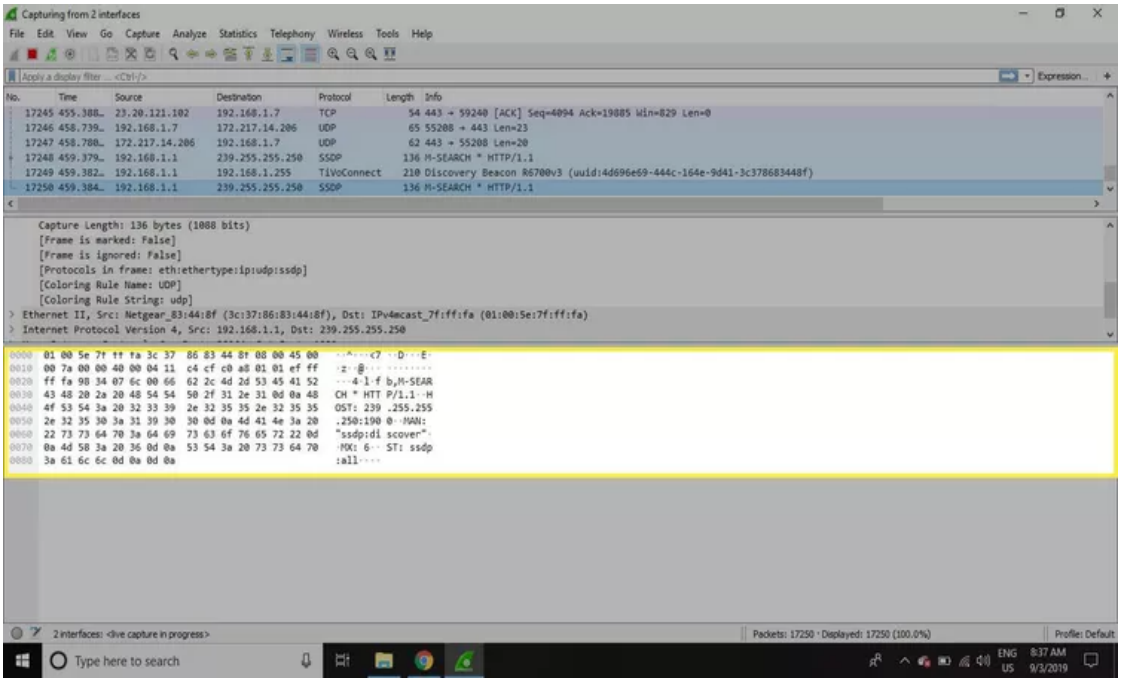
Step 2: The packet details pane (the middle section), found in the middle, presents the protocols and

Protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.

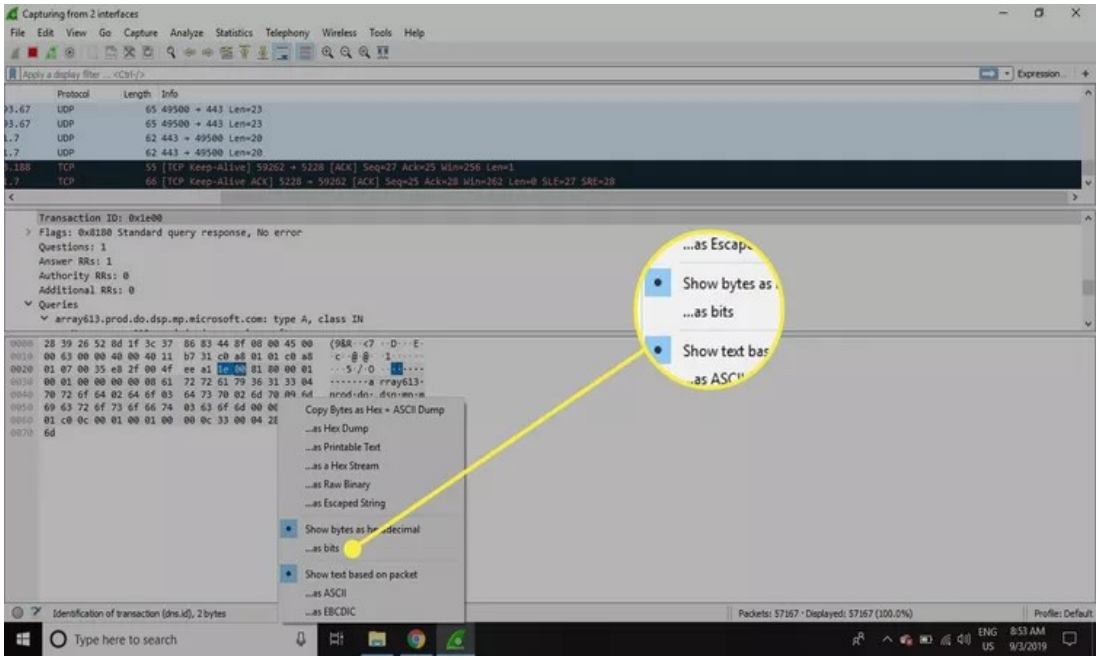


Step 3: The packet bytes pane (the bottom section) at the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.

Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that cannot be printed are represented by a period.



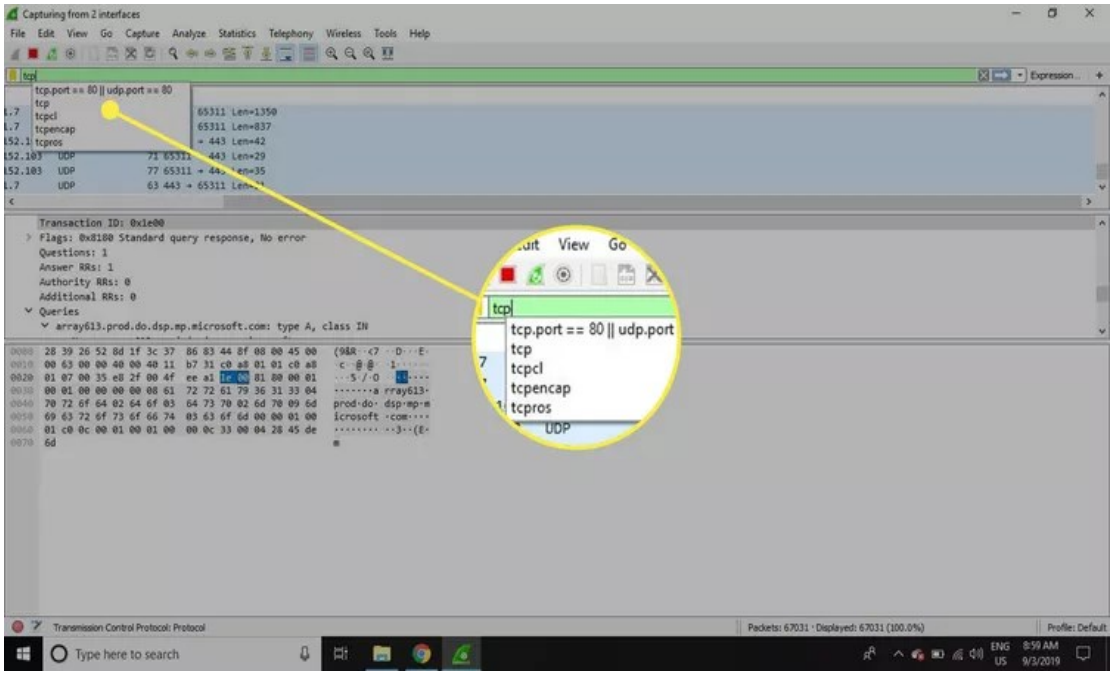
To display this data in bit format as opposed to hexadecimal, right-click anywhere within the pane and select as bits.



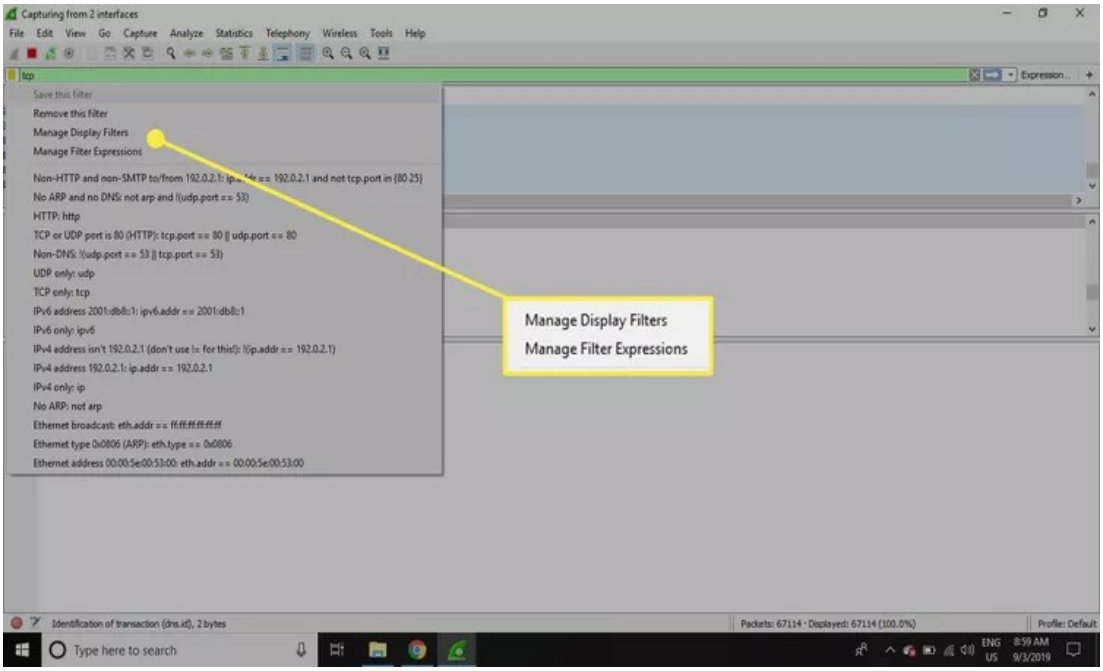
Task 3: Using Filters

Step 1: Wireshark provides a large number of predefined filters by default. To use one of these existing filters, enter its name in the Apply a display filter entry field located below the Wireshark toolbar or in the Enter a capture filter field located in the center of the welcome screen.

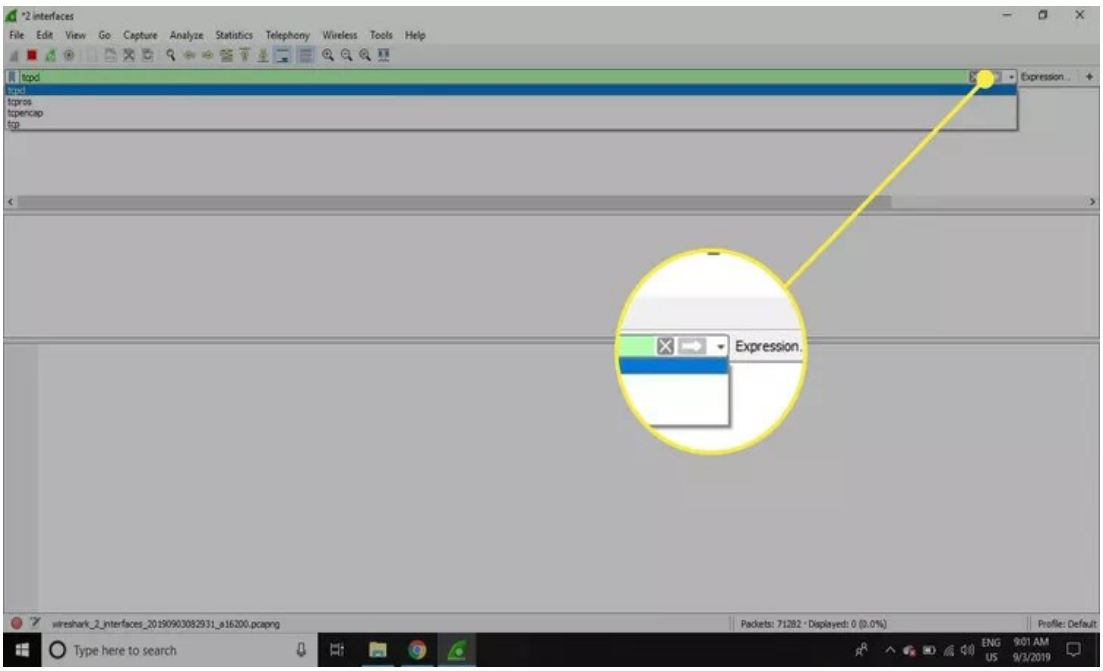
For example, if you want to display TCP packets, type tcp. The Wireshark autocomplete feature shows suggested names as you begin typing, making it easier to find the correct moniker for the filter you're seeking.



Step 2: Another way to choose a filter is to select the bookmark on the left side of the entry field. Choose Manage Filter Expressions or Manage Display Filters to add, remove, or edit filters.

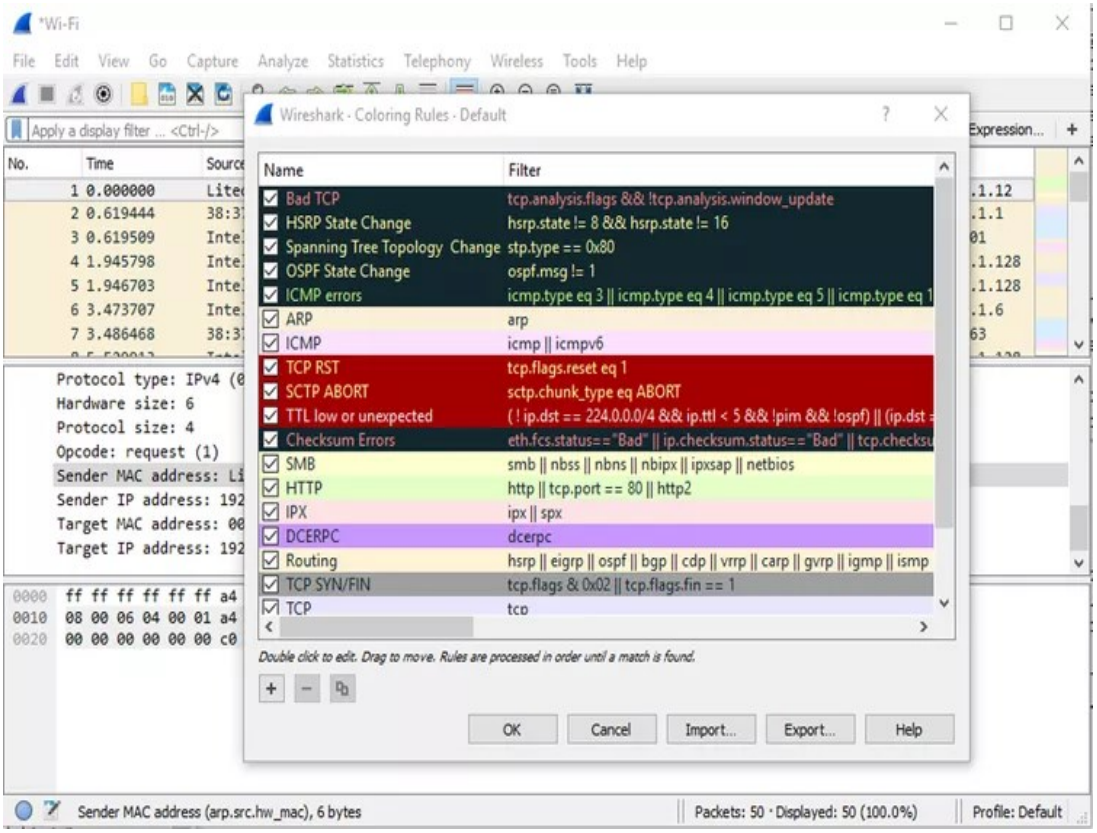


Step 3: You can also access previously used filters by selecting the down arrow on the right side of the entry field to display a history drop-down list.

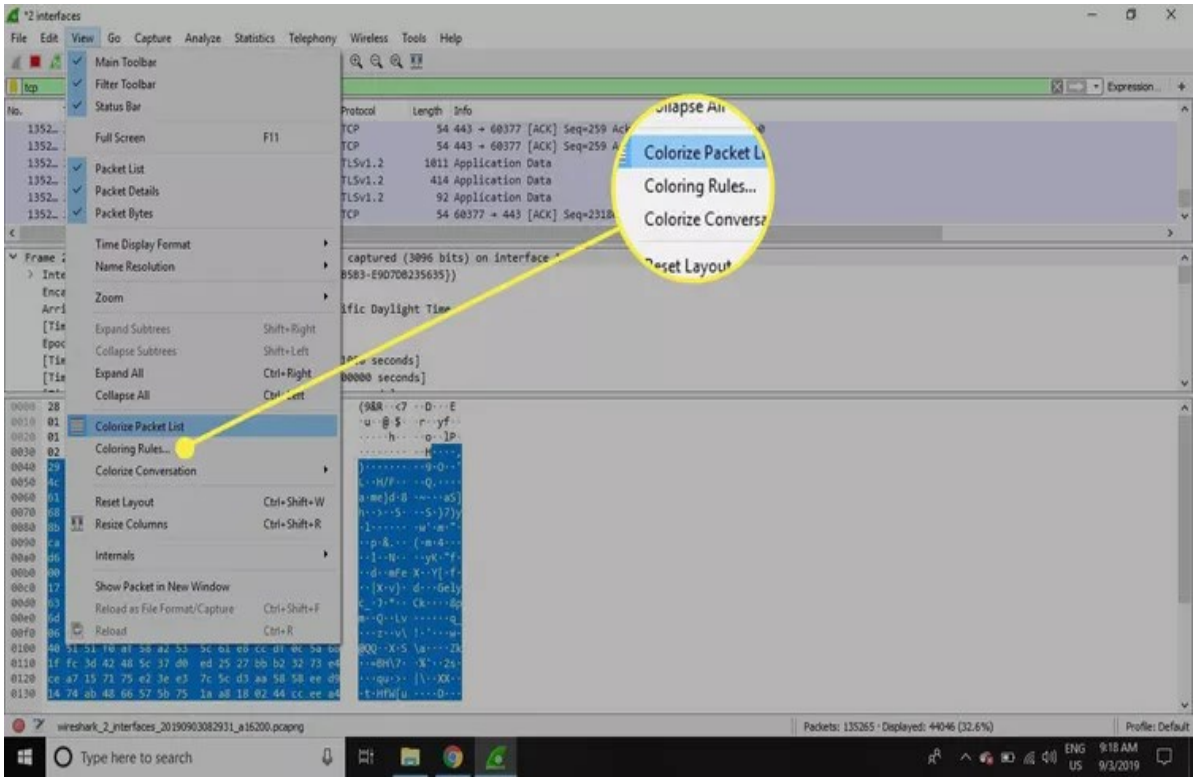


Task 4: Using Color Rules

Step 1: While Wireshark's capture and display filters limit which packets are recorded or shown on the screen, its colorization function takes things a step further: It can distinguish between different packets types based on their individual hue. This quickly locates certain packets within a saved set by their row color in the packet list pane.

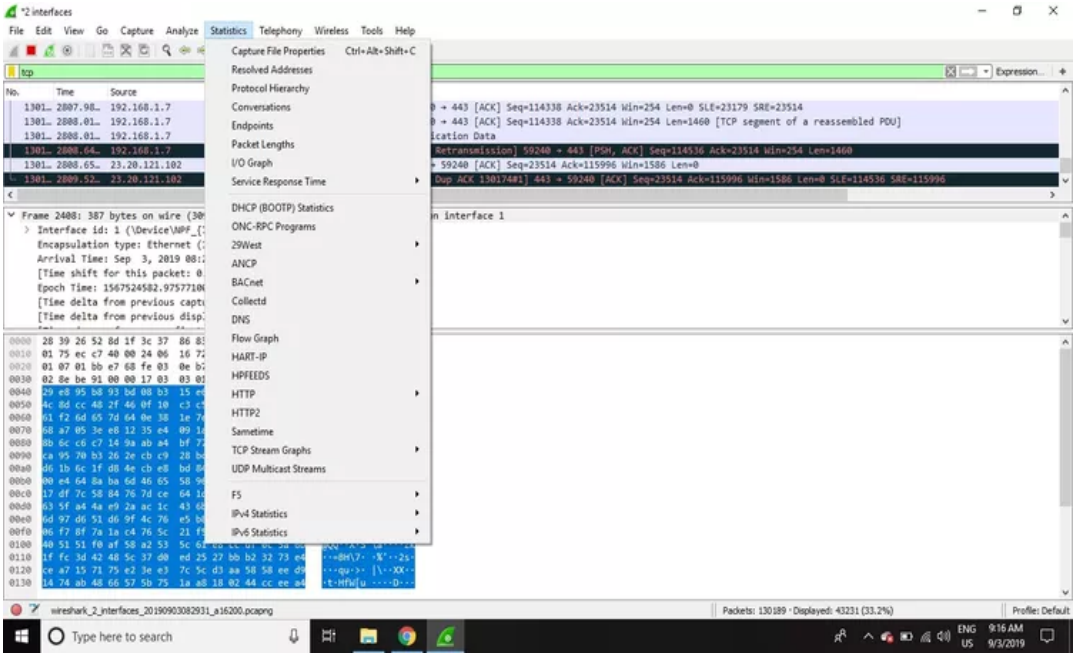


Step 2: Select **View** > **Colorize Packet List** to toggle packet colorization on and off.



Task 5: Using Statistics Rule

Step 1: Other useful metrics are available through the **Statistics** drop-down menu. These include size and timing information about the capture file, along with dozens of charts and graphs ranging in topic from packet conversation breakdowns to load distribution of HTTP requests.



Specification Sheet-5.2: Use NPMT Functions

Tools and materials for using NPMT functions include:

- NPMT software
- Computer/server
- Network devices
- Network cables
- Network diagrams
- Monitoring probes/agents
- Documentation
- Training materials

Learning Outcome-6: Maintain Record of Maintenance

Assessment Criteria	1. Organizational requirements to create advanced network are collected. 2. Required tools, equipment's and component, are identified and listed. 3. Materials and consumables are identified listed. 4. Network design plan is approved by authorize person.
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop 5. Multimedia Projector 6. Paper, Pen, Pencil and Eraser 7. Internet Facilities 8. Whiteboard and Marker • Internet Facilities 9. Whiteboard and Marker
Contents	1. Network maintenance plan 2. Implementation process of network maintenance plan 3. Documentation process of network maintenance plan 4. Process to documented the support plan 5. Process to prepare user manual
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-6: Maintain Record of Maintenance

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Maintain record of maintenance"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Document Approved Network Maintenance Plan"	2. Read Information sheet 6: Maintain record of maintenance 3. Answer Self-check 6: Document Approved Network Maintenance Plan 4. Check your answer with Answer key 6: "Document Approved Network Maintenance Plan"
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Job Sheet 6.1: "Document Approved Network Maintenance Plan" Specification Sheet 6.1: "Document Approved Network Maintenance Plan" Task Sheet 6.2: "Prepare User manual for the network" Specification Sheet 6.2: "Prepare User manual for the network"

Information Sheet-6: Maintain Record Of Maintenance

Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

1. Network maintenance plan
2. Implementation process of network maintenance plan
3. Documentation process of network maintenance plan
4. Process to documented the support plan
5. Process to prepare user manual

6.1 Network maintenance plan

A network maintenance plan outlines the procedures, schedules, and practices for ensuring the optimal performance, reliability, and security of a computer network. It encompasses a range of activities aimed at identifying and addressing potential issues, implementing updates and patches, monitoring network performance, and responding to security threats.

A proper network maintenance plan involves tasks such as:
Hardware and Software Installation
Network maintenance plans involve hardware and software installation to make sure that the devices and the programs you have are ready to be used.

The key components of a network maintenance plan typically include:

Regular Backups: Scheduled backups of critical network data and configurations to prevent data loss in case of hardware failure or security breaches.
Firmware and Software Updates: Regular installation of updates and patches for network devices and software applications to address security vulnerabilities and improve performance.
Security Audits and Assessments: Periodic evaluations of the network infrastructure to identify vulnerabilities, misconfigurations, and potential security threats.
Performance Monitoring: Continuous monitoring of network performance, bandwidth utilization, and traffic patterns to identify issues and optimize network efficiency.
Incident Response Plan: Procedures for detecting, analyzing, and responding to security incidents and network outages in a timely and effective manner.
User Training and Awareness: Training programs to educate network users about security best practices, data protection measures, and acceptable use policies.
Documentation and Documentation Management: Comprehensive documentation of network configurations, topology diagrams, security policies, and maintenance procedures.
Change Management Process: Formal procedures for tracking and authorizing changes to the network infrastructure, configurations, and policies.
A well-designed network maintenance plan helps organizations minimize downtime, reduce security risks, and ensure the smooth operation of their network infrastructure. It is essential for maintaining the integrity and availability of critical business resources and data.

6.2 Implementation process of network maintenance plan

The implementation process of a network maintenance plan involves several key steps to ensure that maintenance activities are carried out effectively and efficiently. Here's a general outline of the implementation process:

1. **Assessment and Planning:**
   - Review the current network infrastructure, configurations, and maintenance practices.
   - Identify areas for improvement and prioritize maintenance tasks based on criticality and impact.
   - Develop a detailed implementation plan that outlines the sequence of activities, responsibilities, and timelines.
2. **Development and Documentation:**
   - Develop detailed procedures and documentation for each maintenance activity outlined in the plan.
   - Create templates for backup schedules, firmware update schedules, incident response procedures, and other maintenance tasks.
   - Document network configurations, topology diagrams, security policies, and change management procedures.
3. **Training and Awareness:**
   - Conduct training sessions for network administrators, IT staff, and end-users on the maintenance plan and procedures.
   - Raise awareness about the importance of network maintenance and security among all stakeholders.
   - Provide training materials and resources to support ongoing education and awareness efforts.
4. **Implementation and Testing:**
   - Begin implementing the maintenance plan according to the established schedules and procedures.
   - Test backup and recovery procedures, firmware updates, and incident response protocols to ensure effectiveness.
   - Monitor network performance and security during implementation to identify any issues or concerns.
5. **Monitoring and Optimization:**
   - Continuously monitor network performance, security, and compliance with maintenance procedures.
   - Optimize maintenance schedules and procedures based on feedback, emerging threats, and changes in network requirements.
   - Regularly review and revise the maintenance plan to accommodate changes in technology, business requirements, and security threats.
6. **Review and Revision:**
   - Conduct post-implementation reviews and assessments to evaluate the effectiveness of maintenance procedures.
   - Identify areas for improvement and update the maintenance plan accordingly.
   - Communicate changes to stakeholders and provide ongoing support and training as needed

6.3 Documentation process of network maintenance plan

The documentation process for a network maintenance plan is essential for ensuring that maintenance activities are clearly defined, documented, and communicated to all stakeholders. Here's a step-by-step guide to the documentation process:

1. **Document Network Infrastructure:**

- Create detailed documentation of the network infrastructure, including hardware devices, software applications, and network topology.
- Include information such as device models, serial numbers, IP addresses, and physical locations.

2. **Define Maintenance Procedures:**
   - Develop step-by-step procedures for each maintenance activity outlined in the maintenance plan.
   - Clearly define the purpose, scope, and objectives of each maintenance task.
   - Specify the sequence of steps to be followed, including any prerequisites or dependencies.
3. **Create Maintenance Checklists:**
   - Develop checklists or task lists for routine maintenance activities, such as backups, updates, and security audits.
   - Include checkboxes or fields for documenting completion status, timestamps, and any issues encountered during the maintenance process.
4. **Outline Backup and Recovery Procedures:**
   - Document backup and recovery procedures for critical network data, configurations, and settings.
   - Specify backup schedules, retention policies, and storage locations for backup files.
   - Include instructions for testing backup and recovery procedures to ensure their effectiveness.
5. **Record Incident Response Protocols:**
   - Define incident response procedures for detecting, analyzing, and responding to security incidents and network outages.
   - Document escalation paths, communication channels, and roles and responsibilities of personnel involved in incident response.
   - Include templates for incident reports and post-incident reviews to facilitate documentation and analysis.
6. **Document Change Management Processes:**
   - Establish formal change management processes for tracking and authorizing changes to the network infrastructure, configurations, and policies.
   - Document change request forms, approval workflows, and implementation procedures.
   - Record change logs and maintain a change history to track modifications and updates to the network environment.
7. **Maintain Version Control:**
   - Implement version control mechanisms to track revisions and updates to the maintenance plan documentation.
   - Use version numbering or revision tracking tools to ensure that stakeholders are working with the most current and accurate documentation.
8. **Review and Update Documentation Regularly:**
   - Conduct regular reviews of the maintenance plan documentation to ensure accuracy, completeness, and relevance.
   - Update documentation as needed to reflect changes in technology, business requirements, and security threats.
   - Communicate updates to stakeholders and provide training and support as needed.

6.4 Process to documented the support plan

Documenting a support plan is crucial for ensuring that support activities are clearly defined, organized, and communicated to all stakeholders involved in maintaining the network infrastructure. Here's a step-by-step process to document a support plan:

1. **Identify Support Objectives:**
   - Define the objectives and goals of the support plan, such as ensuring network availability, addressing user issues promptly, and minimizing downtime.
2. **Outline Support Services:**
   - Identify the scope of support services to be provided, including help desk support, troubleshooting assistance, incident response, and ongoing maintenance.
3. **Define Support Levels:**
   - Establish different support levels based on the severity and complexity of issues, such as tiered support levels ranging from basic user support to advanced technical support.
4. **Document Support Procedures:**
   - Develop detailed procedures for each support activity, including how to log and prioritize support requests, troubleshoot common issues, and escalate unresolved problems.
5. **Create Support Documentation:**
   - Generate support documentation, including knowledge base articles, troubleshooting guides, and FAQs, to assist support staff in resolving issues efficiently.
6. **Establish Communication Channels:**
   - Define communication channels for reporting and tracking support requests, such as email, phone, ticketing systems, or online portals.
   - Specify response times and service level agreements (SLAs) for addressing support requests based on their priority and severity.
7. **Assign Responsibilities:**
   - Assign roles and responsibilities to support team members, including help desk technicians, network administrators, and subject matter experts.
   - Clearly define the duties and expectations for each role, including availability, response times, and escalation procedures.
8. **Provide Training and Resources:**
   - Offer training and resources to support staff to ensure they are equipped with the knowledge and skills needed to fulfill their roles effectively.
   - Provide access to support documentation, training materials, and ongoing professional development opportunities.
9. **Establish Monitoring and Reporting Mechanisms:**
   - Implement monitoring tools and systems to track support performance metrics, such as response times, resolution rates, and customer satisfaction scores.
   - Generate regular reports to assess support performance, identify trends, and make data-driven improvements to support processes.
10. **Review and Update Regularly:**
    - Conduct regular reviews of the support plan to ensure it remains aligned with business objectives, technological advancements, and evolving support needs.
    - Update the support documentation and procedures as needed to reflect changes in technology, processes, or organizational requirements.

6.5 Process to prepare user manual

Preparing a user manual involves several steps to ensure that it effectively communicates important information about the product or system to its users. Here's a step-by-step process to prepare a user manual:

1. **Understand the Audience:**
   - Identify the target audience for the user manual, including their level of technical expertise, language proficiency, and specific needs or requirements.
2. **Define the Scope:**
   - Determine the scope of the user manual by outlining the features, functions, and capabilities of the product or system that will be covered.
3. **Gather Information:**
   - Collect relevant information about the product or system, including technical specifications, operating procedures, troubleshooting steps, and safety precautions.
4. **Organize Content:**
   - Structure the content of the user manual in a logical and easy-to-follow manner, using headings, subheadings, and bullet points to organize information into sections and subsections.
5. **Write Clear and Concise Instructions:**
   - Write clear, concise, and user-friendly instructions that are easy to understand and follow, avoiding technical jargon or complex terminology whenever possible.
   - Use simple language and provide step-by-step instructions with clear explanations and visual aids (e.g., diagrams, screenshots) to illustrate key concepts.
6. **Provide Context and Examples:**
   - Provide context for users by explaining the purpose and significance of the product or system, as well as its intended use cases and potential benefits.
   - Include real-world examples, case studies, and scenarios to help users understand how to apply the information in practical situations.
7. **Include Visuals and Multimedia:**
   - Enhance the user manual with visual elements such as diagrams, illustrations, screenshots, and videos to clarify concepts, demonstrate procedures, and provide visual cues.
   - Ensure that visual elements are relevant, high-quality, and effectively integrated into the text to complement the written instructions.
8. **Test and Review:**
   - Test the user manual with representative users to identify any ambiguities, inconsistencies, or usability issues.
   - Gather feedback from users and stakeholders to validate the clarity, completeness, and effectiveness of the user manual.
   - Revise and refine the user manual based on feedback and testing results to improve its usability and accessibility.
9. **Format and Design:**
   - Choose an appropriate format and layout for the user manual, considering factors such as readability, navigation, and accessibility.
   - Use consistent formatting, typography, and styling throughout the document to maintain visual coherence and professionalism.

10. **Publish and Distribute:**
    - Finalize the user manual by proofreading, formatting, and preparing it for publication.
    - Distribute the user manual through appropriate channels, such as print copies, digital downloads, or online documentation portals.
    - Provide ongoing support and updates to the user manual as needed to ensure its relevance and accuracy over time.

Self-Check-6: Maintain Record of Maintenance

1. Why is it important to identify the target audience for the user manual?

   Answer
2. What does determining the scope of the user manual involve?

   Answer
3. What kind of information should be collected for the user manual?

   Answer
4. How should the content of the user manual be structured?

   Answer
5. Why is it important to use simple language in the user manual?

   Answer
6. Question: Why should real-world examples be included in the user manual?

   Answer
7. How can visual elements enhance the user manual?

   Answer
8. What is the purpose of testing the user manual with representative users?

   Answer
9. Why is it important to use consistent formatting throughout the user manual?

   Answer
10. What channels can be used to distribute the user manual?

    Answer

Answer Key-6: Maintain Record of Maintenance

1. **Why is it important to identify the target audience for the user manual?**
   Answer: It helps tailor the content and language to their level of technical expertise and specific needs.

2. **What does determining the scope of the user manual involve?**
   Answer: Outlining the features, functions, and capabilities of the product or system that will be covered.

3. **What kind of information should be collected for the user manual?**
   Answer: Technical specifications, operating procedures, troubleshooting steps, and safety precautions.

4. **How should the content of the user manual be structured?**
   Answer: Using headings, subheadings, and bullet points to organize information into sections and subsections.

5. **Why is it important to use simple language in the user manual?**
   Answer: To ensure that instructions are easy to understand and follow, avoiding technical jargon or complex terminology.

6. **Question: Why should real-world examples be included in the user manual?**
   Answer: To help users understand how to apply the information in practical situations.

7. **How can visual elements enhance the user manual?**
   Answer: By clarifying concepts, demonstrating procedures, and providing visual cues.

8. **What is the purpose of testing the user manual with representative users?**
   Answer: To identify any ambiguities, inconsistencies, or usability issues and gather feedback for improvement.

9. **Why is it important to use consistent formatting throughout the user manual?**
   Answer: To maintain visual coherence and professionalism, enhancing readability and navigation.

10. **What channels can be used to distribute the user manual?**
    Answer: Print copies, digital downloads, or online documentation portals can be used for distribution.

Task Sheet-6.1: Document Approved Network Maintenance Plan

Performance Objective: At the end of the activity trainees will be able to Document Approved Network Maintenance Plan.

Working Steps:

1. Review Approved Maintenance Plan:
    - Review the approved network maintenance plan to understand the maintenance procedures, protocols, and policies outlined in the plan.
2. Document Maintenance Procedures:
    - Document detailed procedures for each maintenance activity, including backups, updates, security audits, incident response, and change management.
    - Ensure that each procedure is clearly defined, easy to follow, and includes all necessary steps and considerations.
3. Outline Backup and Recovery Procedures:
    - Outline backup and recovery procedures for critical network data, configurations, and settings.
    - Specify backup schedules, retention policies, and storage locations for backup files.
4. Record Security Protocols and Policies:
    - Record security protocols and policies for protecting the network infrastructure from cyber threats.
    - Document access controls, encryption standards, and incident response protocols.
5. Document Change Management Procedures:
    - Document change management procedures for tracking and authorizing changes to the network infrastructure.
    - Include change request forms, approval workflows, and implementation details.
6. Define Incident Response Protocols:
    - Define incident response protocols for detecting, analyzing, and responding to security incidents and network outages.

- Outline escalation paths, communication channels, and roles and responsibilities of personnel involved.

7. Establish Documentation Management Processes:
    - Establish documentation management processes for maintaining and updating the network maintenance documentation.
    - Implement version control, revision tracking, and document storage procedures.
8. Provide Training Materials:
    - Develop training materials and resources to support ongoing education and awareness efforts for network administrators, IT staff, and end-users.
    - Ensure that training materials are comprehensive, easy to understand, and accessible to all stakeholders.

Specification Sheet-6.1: Document Approved Network Maintenance Plan

Tools and Resources:

- Document editing software (e.g., Microsoft Word, Google Docs)
- Graphic design software (e.g., Adobe InDesign, Canva) for creating visuals and multimedia elements
- User feedback and testing tools for gathering feedback and assessing usability

Task Sheet-6.2: Prepare User Manual for The Network

Performance Objective: At the end of the activity trainee will be able to Prepare User manual for the network.

Working Steps:

1. Understand the Audience:
    - Identify the target audience for the user manual, including their level of technical expertise, language proficiency, and specific needs or requirements.
2. Define the Scope:
    - Determine the scope of the user manual by outlining the features, functions, and capabilities of the network infrastructure that will be covered.
3. Gather Information:
    - Collect relevant information about the network infrastructure, including technical specifications, operating procedures, troubleshooting steps, and safety precautions.
4. Organize Content:
    - Structure the content of the user manual in a logical and easy-to-follow manner, using headings, subheadings, and bullet points to organize information into sections and subsections.
5. Write Clear and Concise Instructions:
    - Write clear, concise, and user-friendly instructions that are easy to understand and follow, avoiding technical jargon or complex terminology whenever possible.
    - Provide step-by-step instructions with clear explanations and visual aids (e.g., diagrams, screenshots) to illustrate key concepts.
6. Provide Context and Examples:
    - Provide context for users by explaining the purpose and significance of the network infrastructure, as well as its intended use cases and potential benefits.
    - Include real-world examples, case studies, and scenarios to help users understand how to apply the information in practical situations.
7. Include Visuals and Multimedia:
    - Enhance the user manual with visual elements such as diagrams, illustrations, screenshots, and videos to clarify concepts, demonstrate procedures, and provide visual cues.
    - Ensure that visual elements are relevant, high-quality, and effectively integrated into the text to complement the written instructions.
8. Test and Review:

- Test the user manual with representative users to identify any ambiguities, inconsistencies, or usability issues.
- Gather feedback from users and stakeholders to validate the clarity, completeness, and effectiveness of the user manual.
- Revise and refine the user manual based on feedback and testing results to improve its usability and accessibility.

9. Format and Design:
    - Choose an appropriate format and layout for the user manual, considering factors such as readability, navigation, and accessibility.
    - Use consistent formatting, typography, and styling throughout the document to maintain visual coherence and professionalism.
10. Publish and Distribute:
    - Finalize the user manual by proofreading, formatting, and preparing it for publication.
    - Distribute the user manual through appropriate channels, such as print copies, digital downloads, or online documentation portals.
    - Provide ongoing support and updates to the user manual as needed to ensure its relevance and accuracy over time.

Specification Sheet-6.2: Prepare User manual for the network

Tools:

1. Word processing software (e.g., Microsoft Word, Google Docs)
2. Desktop publishing software (e.g., Adobe InDesign, Microsoft Publisher)
3. Graphics editing software (e.g., Adobe Photoshop, Canva)
4. Screen capture software (e.g., Snagit, Greenshot)
5. Project management tools (e.g., Asana, Trello) for collaboration and task management

Materials:

1. Computer or laptop
2. Printer and printer paper
3. Graphic design elements (icons, images, illustrations)
4. Internet access for research and online resources
5. User manuals of similar products for reference
6. Writing supplies (pens, notebooks) for note-taking and brainstorming sessions

Review of Competency

Below is yourself assessment rating for module "Performing Advanced Networking" of Information Technology.

Assessment of performance Criteria	Yes	No
Organizational requirements to create advanced network are collected		
Required tools, equipment's, and component, are identified, and listed		
Materials and consumables are identified listed		
Network design plan is approved by authorize person		
Subnetting is interpreted		
Range of IP address is identified and selected		
Subnet mask is identified and selected		
Subnetting is performed		
According to the approved network design plan network is established		
Network simulation tools are installed		
Required Network services are identified		
IP addresses is determined		
VLAN is configured as per design plan		
Dynamic Trunk protocol is applied if required		
Spanning Tree protocol is identified and configured		
Services of network is identified and configured		
IP routing is interpreted		
Routing protocol is interpreted		
Types of routing is interpreted		
Terms of routing is interpreted & Routing services is configured		
Bandwidth management is performed as per requirement		
Network performance is monitored using monitoring tools		
Congestion of the network is observed		
Reachability to the internet (if available) is tested		
Network maintenance plan is completed.		
Network maintenance plan is approved by the appropriate person or from the organization		
Approved network maintenance plan is documented		
Support plan for the network is documented		
User manual for the network is prepared		

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

Development of CBLM

The Competency based Learning Material (CBLM) of **‘‘Performing Advanced Networking’’ (Occupation: IT Support Service, Level-4)** for National Skills Certificate is developed by NSDA with the assistance of SIMEC System Ltd., ECF Consultancy & SIMEC Institute of Technology JV (Joint Venture Firm) in the month of July, 2024 under the contract number of package SD-9B dated 15th January 2024.

SL No.	Name & Address	Designation	Contact Number
1	Anisuzzaman Tuheen	Writer	01714-422225
2	Engr. Md. Zuwel Parves	Editor	01737-278906
3	Engr. Md. Zuwel Parves	Co-Ordinator	01737-278906
4	Md. Saif Uddin	Reviewer	01723-004419