RQF LEVEL 4

NITWN401

NETWORKING AND INTERNET TECHNOLOGIES

Wide Area Network

TRAINEE'S MANUAL

October, 2024

WIDE AREA NETWORK

KOICA Korea International Cooperation Agency

TQUM TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

Copies available from:

- *HQs: Rwanda TVET Board-RTB*
- *Web: www.rtb.gov.rw*
- **KIGALI-RWANDA**

Original published version: October 2024

ACKNOWLEDGEMENTS

The publisher would like to thank the following for their assistance in the elaboration of this training manual:

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate IV in Networking and Internet Technologies, specifically for the module **"NITWN401: Wide Area Network."**
We extend our gratitude to KOICA Rwanda for its contribution to the development of these training manuals and for its ongoing support of the TVET system in Rwanda
We extend our gratitude to the TQUM Project for its financial and technical support in the development of these training manuals.

We would also like to acknowledge the valuable contributions of all TVET trainers and industry practitioners in the development of this training manual.

The management of Rwanda TVET Board extends its appreciation to both its staff and the staff of the TQUM Project for their efforts in coordinating these activities.

This training manual was developed:

Under Rwanda TVET Board (RTB) guiding policies and directives

Under Financial and Technical support of

COORDINATION TEAM

RWAMASIRABO Aimable

MARIA Bernadette M. Ramos

MUTIJIMA Asher Emmanuel

Production Team

Authoring and Review

SINDIKUBWABO Telesphore

BYIRINGIRO Elie

NTIBIBUKA Eraste

Validation

KURADUSENGE Alphonse

KAREKEZI Gustave

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

NIYOMUGABO Silas

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe

SUA Lim

SAEM Lee

SOYEON Kim

WONYEONG Jeong

NDAYISABA Olivier

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

ACL: Access Control List

AM: Amplitude Modulation

AS: Autonomous System

ASK: Amplitude Shift Keying

BGP: Border Gateway Protocol

BNC: Bayonet Neill-Concelman

BPDU: Bridge Protocol Data Unit

BPSK: Binary Phase Shift Keying

CBT/A: Competency Based Training/ Assessment

CDM: Code Division Multiplexing

CLI: Command Line Interface

CSV: Comma-Separated Values

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DoS: Denial of Service

DSD-AM: Double Sideband Amplitude Modulation

EIGRP: Enhanced Interior Gateway Routing Protocol

FDM: Frequency Division Multiplexing

FM: Frequency Modulation

FSK: Frequency Shift Keying

FSO: Free Space Optical

HTTPs: HyperText Transfer Protocols.

HTML: Hypertext Markup Language

IGRP: Interior Gateway Routing Protocol

IP: Internet Protocol

IPS: Intrusion Prevention/Detection Systems

IPV4: Internet Protocol Version 4

IPV6: Internet Protocol Version 6

KOICA: Korea International Cooperation Agency

KPIs: Key Performance Indicators selection

LACP: Link Aggregation Control Protocol

LAN: Local Area Network

LED: Light Emitting Diode

MAC: Media Access Control

MAN: Metropolitan Area Network

MPLS: Multiprotocol Label Switching

NMS: Network Management System

NPM: Network Performance Monitor

OSPFv2: Open Shortest Path First version 2

OSPFv3: Open Shortest Path First version 3

PAgP: Port Aggregation Protocol

PC: Personal Computer

PDF: Portable Document Format

PM: Phase Modulation

PRTG: Paessler Router Traffic Grapher

PSK: Phase Shift Keying

PVST+: Per VLAN Spanning tree Plus

QAM: Quadrature Amplitude Modulation

QoS: Quality of Service

QPSK: Quadrature Phase Shift Keying

RIP: Routing Information Protocol

RIPv1: Routing Information Protocol Version 1

RJ-11: Registered Jack 11

RJ-45: Registered Jack 45

RSTP: Rapid Spanning tree Protocol

RTB: Rwanda TVET Board

SMS: Short Message Service

SNMP: Simple Network Management Protocol

SSB-AM: Single Sideband Amplitude Modulation

SSH: Secure Shell

TDM: Time Division Multiplexing

TQUM Project: TVET Quality Management Project

UPS: Uninterruptible Power Supply

VLANs: Virtual Local Area Networks

VLSM: Variable Length Subnet Mask

VoIP: Voice over Internet Protocol

VRRP: Virtual Router Redundancy Protocol

VPN: Virtual Private Network

VPNs: Virtual Private Networks

VSB-AM: Vestigial Sideband Amplitude Modulation

WAN: Wide Area Network

WAP: Wireless Access Point

WDM: wavelength Division Multiplexing

WMI: Windows Management Instrumentation

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Networking and Internet Technologies specifically for the module of **"Wide area Network."** Trainees enrolled in this module will engage in practical activities designed to develop and enhance their competencies. The development of this training manual followed the Competency-Based Training and Assessment (CBT/A) approach, offering ample practical opportunities that mirror real-life situations.

The trainee's manual is organized into Learning Outcomes, which is broken down into indicative content that includes both theoretical and practical activities. It provides detailed information on the key competencies required for each learning outcome, along with the objectives to be achieved.

As a trainee, you will start by addressing questions related to the activities, which are designed to foster critical thinking and guide you towards practical applications in the labor market. The manual also provides essential information, including learning hours, required materials, and key tasks to complete throughout the learning process.

All activities included in this training manual are designed to facilitate both individual and group work. After completing the activities, you will conduct a formative assessment, referred to as the end learning outcome assessment. Ensure that you thoroughly review the key readings and the 'Points to Remember' section.

MODULE CODE AND TITLE: NITWM401 WIDE AREA NETWORK

Learning Outcome 1: Install WAN Equipment.
Learning Outcome 2: Apply VLAN Configurations.
Learning Outcome 3: Apply Router Configurations.
Learning Outcome 4: Maintain WAN.

Indicative contents
1.1 Conduct Site Visit.
1.2 Identification of WAN Installation requirements.
1.3 Performing WAN Connections.
1.4 Apply Modulation & demodulation Techniques.
1.5 Apply Multiplexing & De-multiplexing Techniques.

Key Competencies for Learning Outcome 1: Install WAN Equipment

Knowledge	Skills	Attitudes
• Description of WAN site visit • Identification of tools, materials and equipment as used to install WAN. • Description of WAN installation requirements. • Description of WAN Technologies. • Description of WAN Connection Types. • Description of modulation and demodulation techniques. • Description of Multiplexing & De-multiplexing techniques.	• Conducting WAN site visit. • Selecting Tools, Materials and Equipment of WAN installation. • Connecting WAN connection types. • Applying modulation and demodulation techniques. • Applying Multiplexing & De-multiplexing techniques.	• Being adaptable on WAN site. • Having critical thinking about WAN site. • Being protected on WAN site. • Being a team player when installing WAN.

Duration: 20 hrs

Learning outcome 1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe properly WAN site visit and infrastructure as used in WAN installation.
2. Conduct effectively WAN site visit based on organization's infrastructure requirements.
3. Identify clearly tools, materials and equipment as used in WAN installation.
4. Select properly tools, materials and equipment based on WAN installation requirements.
5. Describe clearly WAN installation requirements as used in network.
6. Describe clearly WAN Connection Types as used in network.
7. Connect correctly WAN connection types based on WAN infrastructure equipment.
8. Describe clearly modulation and demodulation techniques as used in WAN.
9. Apply appropriately modulation and demodulation techniques based on WAN infrastructure equipment.
10. Describe clearly Multiplexing & De-multiplexing techniques as used in WAN.
11. Apply appropriately Multiplexing & De-multiplexing based on WAN infrastructure equipment.

Resources

Equipment	Tools	Materials
• Routers • Switches • Hubs • Repeaters • Gateways • Bridges • Modems • Rack Mount • Access Point	• Cable tester • Crimping tool • Wire cutter • Striping tool • Putty • Terra term • CISCO Packet tracer	• CAT5 • CAT6 or CAT6e • Fiber optic cables • Coaxial Cable • Console cable • BNC • RJ45 • RJ11

• Computer • Modems • Transmitters and Receivers • Multiplexers/Demultiplexers • Antennas		

Indicative content 1.1: Conduct Site Visit

Duration: 4 hrs

Theoretical Activity 1.1.1: Description of WAN Site Visit

Tasks:

1: Answer the following questions

i. What do you understand by the term WAN site visit?

ii. What is the primary purpose of WAN site visit?

iii. What is the element considered when you are doing WAN site assessment?

iv. What is the key element do you considered when evaluating WAN site infrastructure?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present your finding to the whole class.

4: Ask questions for clarification when necessary.

5: Read the Key readings 1.1.1 in trainee manuals.

Key readings 1.1.1.: Description of WAN Site Visit

A WAN site visit refers to an on-site evaluation or inspection of a location where a Wide Area Network (WAN) is being installed, maintained, or upgraded. The keys considerations while conducting site visit.

1. Preparation of Site Visits

1.1. Understand Purpose: Clearly define the reason for the visit, whether it's for assessment, research, inspection, training, or networking.

The primary purpose of a WAN (Wide Area Network) site visit is to assess and understand the specific requirements and challenges of a remote location or branch office. This information is crucial for designing and implementing an effective WAN solution that can connect the site to the main corporate network.

1.2. Define the objectives: Set specific goals for the visit, such as evaluating performance, gathering data, identifying hazards, or providing training.

- **Network assessment:** Evaluate the existing network infrastructure, including hardware, software, and connectivity options.
- **Site requirements analysis:** Gather information about the site's specific needs, such as bandwidth requirements, latency tolerance, and security considerations.
- **Identify challenges:** Pinpoint potential obstacles or limitations that could affect network performance or reliability.
- **Recommend solutions:** Propose tailored WAN solutions that address the site's unique needs and align with the overall business goals.
- **Plan implementation:** Develop a detailed implementation plan, including hardware procurement, network configuration, and testing procedures.
- **Build relationships:** Foster communication and collaboration with local IT staff to ensure a smooth transition and ongoing support.
- **Prepare a checklist:** Create a detailed list of items to be observed, assessed, or collected during the WAN site visit.

2. Site assessment

Site assessment refers to the process of evaluating a physical location to determine its suitability for network infrastructure deployment. This involves assessing various factors that can impact network performance, reliability, and security. The following elements are considered while doing WAN site assessment:

2.1. Surroundings: Evaluate the overall environment of the site, including cleanliness, organization, and accessibility.

2.2. Safety hazards: Identify potential safety risks, such as tripping hazards, electrical hazards, or chemical spills.

3. Infrastructure evaluation

When evaluating WAN site infrastructure, it's essential to assess various factors that impact network performance, reliability, and security. Here are some key elements to consider while evaluating WAN site infrastructure.

3.1. Physical Infrastructure or Existing infrastructure

- **Location:** Geographic location can influence factors like distance, latency, and potential natural disasters.

- **Building infrastructure:** Consider the building's structural integrity, power supply reliability, and environmental conditions (e.g., temperature, humidity).
- **Physical security:** Assess the site's physical security measures, such as access controls, surveillance, and vulnerability to threats like theft or vandalism.

3.2. Network Infrastructure or Cabling and network layout

- **Existing network equipment:** Evaluate the current network devices (routers, switches, firewalls) and their capabilities.
- **Connectivity options:** Assess available connectivity options, including broadband (DSL, cable, fiber), cellular (4G, 5G), or satellite.
- **Bandwidth requirements:** Determine the required bandwidth based on expected data traffic and applications.
- **Latency and jitter:** Consider the acceptable levels of latency (delay) and jitter (variation in delay) for critical applications.

4. Document findings

Document findings refer to the process of systematically recording and organizing information, observations, or results from a study, investigation, or research project.

- **Record observations:** Take detailed notes on your findings, including observations, measurements, and any issues encountered.
- **Collect evidence:** Gather supporting materials, such as photographs or samples, to document your findings.
- **Analyse data:** Analyse the collected information to identify trends, patterns, or areas for improvement.

Practical Activity 1.1.2: Conducting WAN Site Visit

Task:

1: Refer to the key reading 1.1.2 and perform the following task:

You are asked to go to the WAN site for gathering information about requirements needed for installing WAN.

2: Present steps for conducting WAN site visits.

3: Conduct WAN site visits.

4: Ask for clarification if any

5: For more clarifications, read the key readings 1.1.2

6: Perform the activity in the application of learning 1.1

Key readings 1.1.2.: Conducting WAN Site Visit

The key considerations while conducting site visits.

Step1: Preparation of Site Visits

- **Understand Purpose:** Clearly define the reason for the visit, whether it's for assessment, research, inspection, training, or networking.

  The primary purpose of a WAN (Wide Area Network) site visit is to assess and understand the specific requirements and challenges of a remote location or branch office. This information is crucial for designing and implementing an effective WAN solution that can connect the site to the main corporate network.

- **Define the objectives:** Set specific goals for the visit, such as evaluating performance, gathering data, identifying hazards, or providing training.

  Step2: Site assessment refers to the process of evaluating a physical location to determine its suitability for network infrastructure deployment. This involves assessing various factors that can impact network performance, reliability, and security.

  - **Surroundings**: Evaluate the overall environment of the site, including cleanliness, organization, and accessibility.
- **Safety hazards:** Identify potential safety risks, such as tripping hazards, electrical hazards, or chemical spills.

  Step3: Infrastructure evaluation

  When evaluating WAN site infrastructure, it's essential to assess various factors that impact network performance, reliability, and security. Here are some key elements to consider, the goal is to ensure the network infrastructure is capable of meeting current and future demands, identifying potential risks, and planning for upgrades or expansions.

Step4: Document findings refer to the process of systematically recording and organizing information, observations, or results from a study, investigation, or research project.

- **Record observations:** Take detailed notes on your findings, including observations, measurements, and any issues encountered.
- **Collect evidence:** Gather supporting materials, such as photographs or samples, to document your findings.
- **Analyse data:** Analyse the collected information to identify trends, patterns, or areas for improvement.

Step5: Prepare a report: Write a comprehensive report summarizing your findings, conclusions, and recommendations.

Points to Remember

- A WAN site visit refers to an on-site evaluation or inspection of a location where a Wide Area Network (WAN) is being installed, maintained, or upgraded.
- The following elements are considered while doing WAN site assessment such as Surroundings and safety hazards.
- Here are some key elements to consider while evaluating WAN site infrastructure such as existing infrastructure, Cabling and network layout.
  - Preparation of Site Visits.
  - Site assessment.
  - Infrastructure evaluation.
  - Document findings.
  - Prepare a report.

Application of learning 1.1.

You are part of the IT Technician at ABCD Bank, conduct a site visit at the new branch office to assess the requirements for establishing a Wide Area Network (WAN) between the headquarters and the branch.

Indicative content 1.2: Identification of WAN Installation requirements

Duration: 4 hrs

Theoretical Activity 1.2.1: Description of WAN installation requirements

Tasks:

1. Answer the following questions:
    i. What do you understand by the following terms?
        a) WAN
        b) LAN
        c) MAN
        d) VLAN
    ii. List and explain the types of WAN.
    iii. When evaluating WAN network infrastructure design, what are the elements to focus on?
    iv. Identify required tools, Materials and Equipment used when installing WAN.
2. Write answers on paper flipchart, blackboard or whiteboard.
3. Present your findings to the whole class.
4. Ask questions for clarification when necessary.
5. Read the Key readings 1.2.1 in trainee manuals.

Key readings 1.2.1.: Description of WAN installation requirements

2.1. Definitions of Key Terms

- **WAN (Wide Area Network)**

WAN Is a network that connects multiple computers and devices over a large geographic area, often spanning cities, states, or even countries. WANs are

typically used to connect branch offices, remote workers, and other geographically dispersed locations.

- **LAN (Local Area Network)**

  LAN Is a network that connects computers and devices within a limited geographic area, such as a single building or campus. LANs are used for sharing resources, communication, and collaboration within a local environment.

- **MAN (Metropolitan Area Network)**

  MAN Is a network that connects multiple LANs within a metropolitan area. MANs are typically used to connect businesses, educational institutions, and government agencies within a city or region.

- **VLAN (Virtual Local Area Network)**

  VLAN Is a logical division of a physical network into multiple virtual networks. VLANs allow administrators to segment a network into smaller, isolated segments based on factors such as department, function, or security requirements. This can improve network performance, security, and management.

2.2. Types of WAN

WANs (Wide Area Networks) are used to connect multiple remote locations over a large geographic area. Here are some common types of WANs:

2.2.1. Switched WAN

- ✓ **Description:** A switched WAN uses a network switch to connect multiple devices or networks together. It allows for flexible and scalable connections between different locations.
- ✓ **Common Technologies:** Ethernet, Frame Relay, ATM (Asynchronous Transfer Mode)

2.2.2. Point-to-Point WAN

- **Description:** A point-to-point WAN connects two specific locations directly, providing a dedicated connection between them.
- **Common Technologies:** Leased lines (dedicated circuits), DSL, cable modems

2.2.3. Cloud-Based WAN (SD-WAN)

- ✓ **Description:** An SD-WAN (Software-Defined WAN) leverages cloud-based technology to manage and control WAN connections. It offers enhanced flexibility, scalability, and centralized management.

Key Benefits:

- **Centralized Management:** SD-WANs can be managed from a central location, simplifying network administration.
- **Dynamic Routing:** SD-WANs can automatically adjust routing based on network conditions, ensuring optimal performance.
- **Application-Aware Routing:** SD-WANs can prioritize specific applications or traffic flows, improving performance for critical applications.
- **Hybrid Connectivity:** SD-WANs can support multiple WAN connections (e.g., MPLS, broadband, cellular) to provide redundancy and optimize costs.

3. Evaluation of Network Infrastructure Design

- Hardware Infrastructure

When evaluating the hardware infrastructure of a network design, consider the following key elements:

- ✓ **Devices:** Assess the types and capabilities of network devices, including routers, switches, firewalls, and wireless access points. Ensure they have sufficient capacity to handle current and future traffic loads.
- ✓ **Physical Infrastructure:** Evaluate the physical layout of the network, including cabling, racks, and power distribution. Ensure the infrastructure is organized, well-maintained, and can accommodate future growth.
- ✓ **Redundancy:** Assess the level of redundancy in the hardware infrastructure, such as dual power supplies, redundant links, and backup devices. This helps to improve reliability and minimize downtime in case of failures.

- **Environmental Factors:** Consider the environmental conditions where the hardware is located, including temperature, humidity, and power quality. Ensure the equipment is properly protected and can operate reliably in these conditions.
- Software Infrastructure

The software infrastructure of a network plays a critical role in its overall performance, security, and management. Key elements to consider include:

- ✓ **Operating Systems:** Evaluate the operating systems used on network devices. Ensure they are up-to-date and supported by the vendor.
- ✓ **Network Management Systems (NMS):** Assess the NMS software used to monitor, manage, and configure network devices. Ensure it is capable of providing real-time visibility into network performance and identifying potential issues.
- ✓ **Security Software:** Evaluate the security software deployed on network devices, including firewalls, intrusion detection systems (IDS), and antivirus software. Ensure it is up-to-date and effectively protects the network from threats.
- ✓ **Application Software:** Consider the specific applications that will be running on the network and ensure the software infrastructure can support them adequately.
- ✓ **Virtualization:** If virtualization is used, evaluate the virtualization platform and its capabilities.

Ensure it is compatible with the network hardware and can provide the necessary resources for virtual machines.

By carefully evaluating both the hardware and software infrastructure, organizations can ensure that their network design is well-equipped to meet their current and future needs, while providing a reliable, secure, and efficient platform for their operations.

4. **Material**

Materials may fall into a number of categories, including consumables, raw materials, and equipment (for temporary or permanent use).

- ✓ **CAT5 and CAT6 Cables**

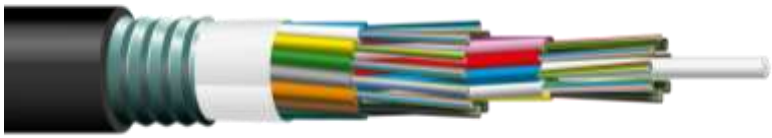
CAT5 (Category 5) and CAT6 (Category 6) are types of twisted-pair Ethernet cables. They are used to connect devices within a local area network (LAN) and provide high-speed data transmission.

CAT6 offers better performance and higher data transfer rates compared to CAT5.

- ✓ **Fiber Optic Cables**

Fiber optic cables use light signals to transmit data. They offer high-speed data transmission over long distances and are less susceptible to electromagnetic interference.

Fiber optics are commonly used in telecommunications and high-speed internet connections.



- ✓ **Coaxial Cables**

Coaxial cables are used for various applications, including cable television, internet, and other data transmission.

They consist of a central conductor, insulating material, a metallic shield, and an outer insulating layer.

- ✓ **BNC Connectors (Bayonet Neill–Concelman)**

BNC connectors are a type of coaxial connector used for connecting coaxial cables. They are often used in video surveillance systems and some networking equipment.

- ✓ **RJ45 Connector**

An RJ45 connector is the standard connector used for Ethernet cables and network connections. It is typically used in Ethernet networks for data transmission and is widely known as the connector for CAT5 and CAT6 cables.

- ✓ **RJ11 Connector:**

RJ11 connectors are commonly used for telephone lines and analog modems. They have fewer pins compared to RJ45 connectors and are typically used for voice communication.

- ✓ **Blank CDs/DVDs or USB Drives**: For creating bootable installation media or backup purposes.

- ✓ **Cleaning Supplies:** Microfiber cloths, isopropyl alcohol, or compressed air to clean components and surfaces.

- ✓ **Spare Screws and Fasteners:** In case any are lost or damaged during disassembly.

- ✓ **Static-free Work Surface or Mat:** Provides an ESD-safe area for working on components.

5. Tools

Lists of Networking Tools and Their Uses. Here are some lists of commonly used networking tools and their uses:

- ✓ **Cable Crimper**

A cable crimper, also called a wire crimper, is a hand-held tool used to join two or more wires together by crimping a metal connector onto the ends of the wires. It is mostly used to terminate Ethernet cables with RJ45 connectors.

Some cable crimpers also have a built-in wire stripper, which allows you to strip the insulation from the wire before crimping the connector onto the end.

- ✓ **Punch-Down Tool**

A punch-down tool is a networking tool used to punch wires into a connection block, keystone jack, or patch panel. It is commonly used in network cabling installations, particularly for terminating twisted-pair cables, such as Category 5e or Category 6 Ethernet cables.

- ✓ **Cable Stripper**

A cable stripper, also known as a wire stripper, is a hand-held networking tool used to remove the outer insulation layer from an electrical wire or cable without damaging the inner conductor. Apart from stripping insulators, it can also be used for cutting wires with its built-in blade.

- ✓ **Wire Cutter**

A wire cutter is a networking tool used to cut network cables to the required length. Wire cutters are designed with sharp blades that are able to cleanly cut

through the wire or cable without causing any damage to the conductor or insulation.

- ✓ **Multimeter**

A multimeter is a versatile networking tool that is used to measure a variety of electrical parameters such as voltage, current, and resistance. In networking, it is used for testing power supplies, i.e., to measure the voltage output of power supplies in networking equipment such as routers, switches, and access points.

It can also be used for testing continuity in network cables and to measure the resistance of network components such as resistors, which can help diagnose problems with the network.

- ✓ **Tone Generator**

A tone generator is a networking device used to identify and trace the path of a network cable. It works by sending a signal down the cable and producing a tone at the other end of the cable, which can be detected using a probe.

- ✓ **Cable Tester**

A cable tester is a networking tool used to test the continuity and functionality of network cables. It helps identify any miswires, opens, shorts, or crossed wires that can affect network performance.

- ✓ **Loopback Adapter**

A loopback adapter, also known as a loopback plug, is a small networking tool used to test the functionality of a network interface card (NIC) or other network device. It is essentially a short cable with a connector at each end, which is plugged into the network port of a device to create a loop back.

- ✓ **Time Domain Reflectometer (TDR)**

A Time Domain Reflectometer (TDR) is a hardware device used in networking to diagnose and pinpoint problems in copper cables such twisted pair, coaxial, and flat ribbon cables.

The TDR sends a signal through the cable and measures the time it takes for the signal to be reflected, allowing it to determine the distance to the fault in the cable.

- ✓ **Heat Gun for Shrink Tubing**

A heat gun is a handheld tool that is commonly used in various applications, including networking. In networking, heat guns are primarily used for heat-shrink tubing applications. Another advantage of a heat gun is for drying and curing adhesives, coatings, and other materials used in networking.

- ✓ **Screwdriver Set**

A screwdriver set is a collection of screwdrivers in various sizes and shapes that are used to loosen or tighten screws. It is an essential tool for anyone working with electronics, computers, or other devices that have screws. In networking, it is mostly used to open and repair network devices.

- ✓ **Cable Tie**

A cable tie, also known as a zip tie or tie-wrap, is a type of fastener used to secure and organize wires, cables, and other components in a network installation. It consists of a flexible nylon strap with teeth on one end and a ratchet-like mechanism on the other end.

Cable ties are commonly used in networking installations to keep cables and wires neatly organized and to prevent them from becoming tangled or damaged. They are also used in a variety of other industries and applications, such as in automotive and aerospace manufacturing, packaging, and home improvement projects.

- ✓ **Scissors**

Scissors can be a useful tool in networking for cutting cables and wires. They are commonly used in conjunction with wire strippers and cable cutters to trim and shape cables to the desired length.

Scissors with a serrated edge can help prevent the wires from slipping while cutting, and those with a pointed tip can be useful for precise cuts in tight spaces.

- ✓ **PuTTY**

PuTTY is a free and open-source terminal emulator, serial console, and network file transfer application. It is commonly used on Windows to establish secure SSH, Telnet, and serial connections to remote devices, such as servers, routers, and switches.

- ✓ **Tera Term**

Tera Term is another free and open-source terminal emulator program, primarily used for serial port communication and remote terminal access. It is often employed for configuring and managing network equipment, embedded systems, and more.

- ✓ **Cisco Packet Tracer**

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It's widely used for learning and practicing networking concepts, including configuring and simulating Cisco network devices. It's especially popular in educational settings and network training.

- ✓ **EdrawMax**

EdrawMax is a diagramming software that allows users to create various types of diagrams, charts, and visual representations, including flowcharts, network diagrams, org charts, and more. It's often used in business, education, and other fields to create professional-looking visuals for presentations and documentation.

6. Equipment

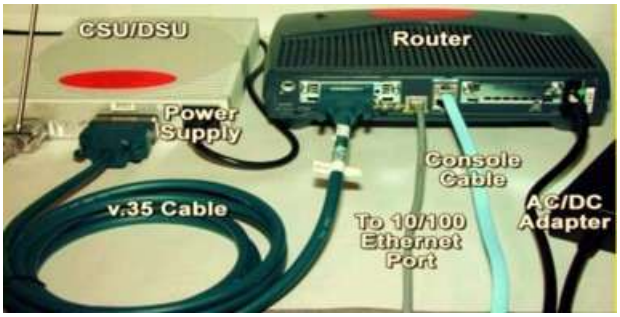
Hubs provide a centralized point at which cables may be attached to individual workstations. Hubs are classified into two types: active and passive. Devices on a twisted-pair network are connected by it. A hub just regenerates signals; it does not conduct any other functions.

- ✓ **Switches** link peripherals to host computers and enable several peripherals to share a small number of ports. Connects many devices that make up a twisted-pair network. A switch uses the MAC address included in each packet to forward data to its destination.

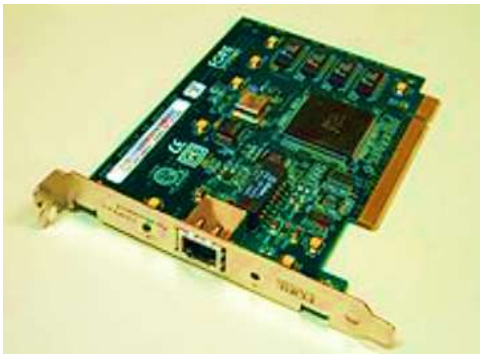
- **Routers** are devices that connect sub-networks or divide a large network into smaller networks based on the protocols they use. Facilitates the linking of several networks. A router decides where to send data based on the network address that is set up in software.
- **Repeaters** use regeneration and retiming to send signals clearly throughout all network segments.
- **Bridges** are used to link local and distant networks. Network administration is centralised. Separates networks to decrease network traffic. By reading the MAC address, a bridge permits or prohibits data from traveling across it.
- **Gateways** could link networks using incompatible communication protocols. Performs the translation from one data format to another. Gateways may be based on either hardware or software. Any device that transforms data types is referred to as a gateway.
- **Multiplexers** are devices that combine many different signal inputs into a single output.

- **Transceivers** transmit and receive signals and link nodes. They are sometimes referred to as medium access units (MAU). Transceiver Converts between different media types, such as UTP to fiber. A device that operates as both a transmitter and receiver of analogue or digital signals.

- **Firewalls** protect networks against illegal access. Provides secure data transfer across networks. Firewalls are an integral component of a network's security strategy and may be hardware or software based.
- **The CSU/DSU** is responsible for converting digital signals from the local area network (LAN) to the wide area network (WAN). CSU/DSU capability is sometimes integrated into other devices, such as a router with WAN connectivity.



- **Network cards** Allows systems to connect to the network. Network interfaces can be add-in cards, PCMCIA cards, or interfaces that are built into the computer.



- **ISDN terminal adapter** Connects devices to ISDN lines. ISDN is a digital WAN technology that is often used instead of modem links, which are slower. ISDN terminal adapters are needed to change the format of data so it can be sent over ISDN links.
- **AP** Provides wireless network devices with network functionality. A WAP is often used to connect to a wired network, connecting the wired and wireless parts of the network.
- **MODEM** provides serial communication capabilities across phone line. At the sending end, modems change the digital signal into an analogue one, and at the receiving end, they do the opposite'

Points to Remember

- WAN is a network that connects multiple computers and devices over a large geographic area, often spanning cities, states, or even countries.
- LAN is a network that connects computers and devices within a limited geographic area.
- MAN is a network that connects multiple LANs within a metropolitan area.
- VLAN is a logical division of a physical network into multiple virtual networks.
- While prepare the requirement tools materials and equipment do not forget the types of WAN like Switched WAN, point to point WAN, Cloud-Based WAN.
- While Identify requirements of WAN Installation remember to make Evaluation of Network Infrastructure Design

Application of learning 1.2.

XYZ Is a growing technology firm with two or more offices across different district, they need to set up a WAN to ensure seamless communication between their headquarters and branch

offices. So, as IT technician Identify the required various type of network will be used, and tools, materials and equipment, and evaluate network infrastructure design for a successful WAN installation.

Indicative content 1.3: Performing WAN Connections

Duration: 4 hrs

Theoretical Activity 1.3.1: Description of WAN technologies

Tasks:

While delivering this activity, pass through the following steps:

1: Answer the following questions:

i. What does it mean by the term WAN technology?
ii. Describe at least 4 WAN technologies you know?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 1.3.1 in trainee's manuals.

Key readings 1.3.1: Description of WAN Technologies

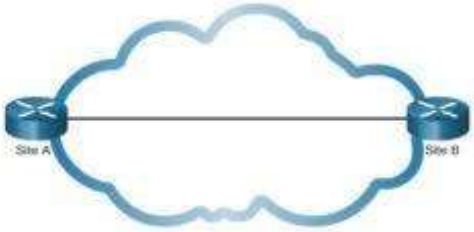
✔ **Description of WAN Technologies**

WAN (Wide Area Network) technology refers to the methods and systems used to connect multiple local area networks (LANs) over large geographical distances.

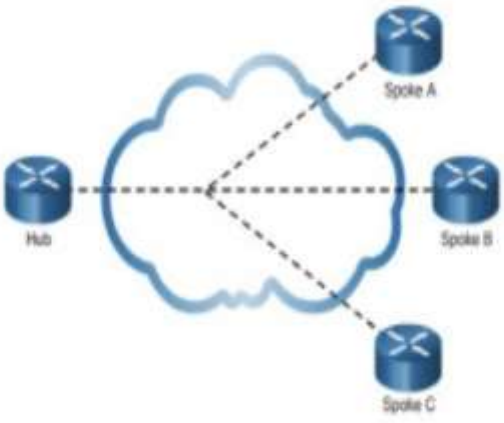
The Common WAN Technologies are:

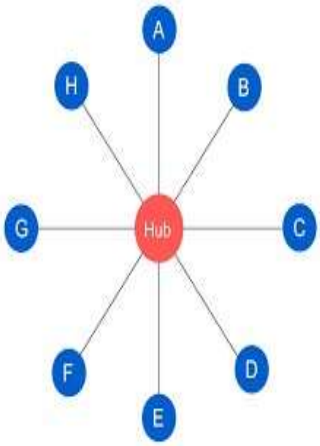
1. Point-to-Point Topology

In a point-to-point topology, two Site or networks are connected directly to each other. This creates a dedicated link between the two endpoints, which ensures reliable and high-speed communication.



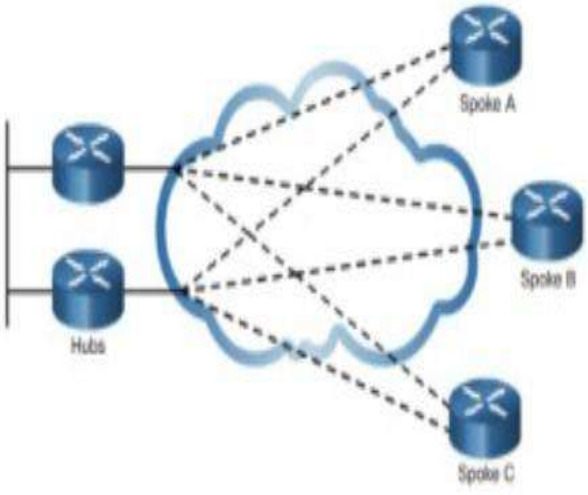
2. **Hub-and-Spoke**: This is a network architecture where multiple sites or branches are connected to a central location, known as the hub. All communication between the spokes must pass through the hub. It's a cost-effective solution for organizations with a central main office and multiple remote locations





3. **Full Mesh** In a full mesh topology, every node or site is connected to every other device. This provides redundancy and ensures multiple paths for data to travel. It's commonly used in critical applications where high availability and fault tolerance are crucial.

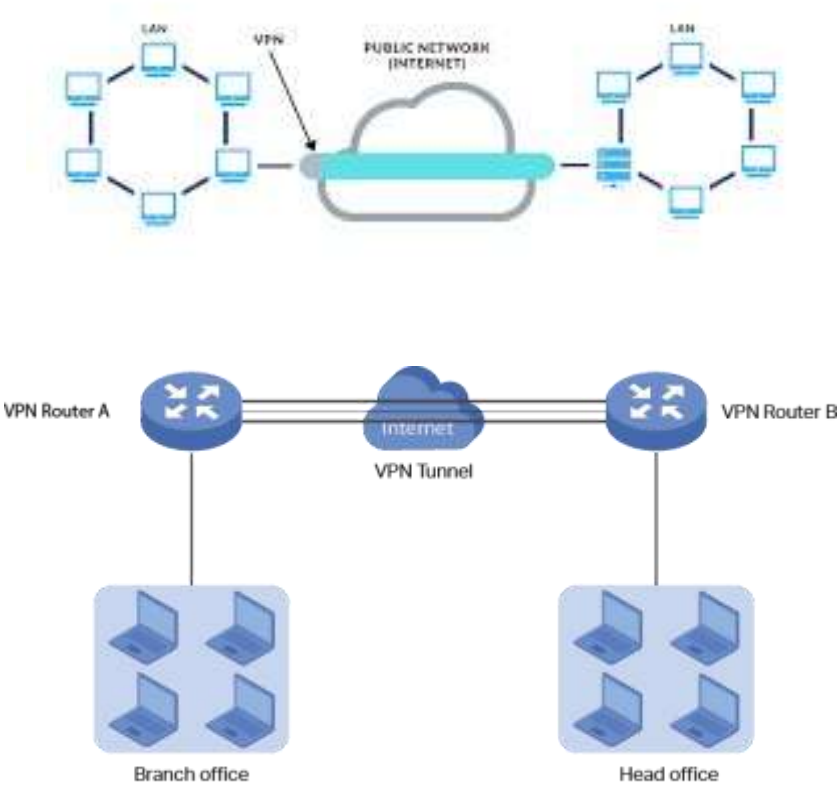
One of the disadvantages of hub-and-spoke topologies is that all communication has to go through the hub. With a full mesh topology using virtual circuits, any site can communicate directly with any other site. The disadvantage here is the large number of virtual circuits that need to be configured and maintained.



5. Virtual Private Network (VPN)

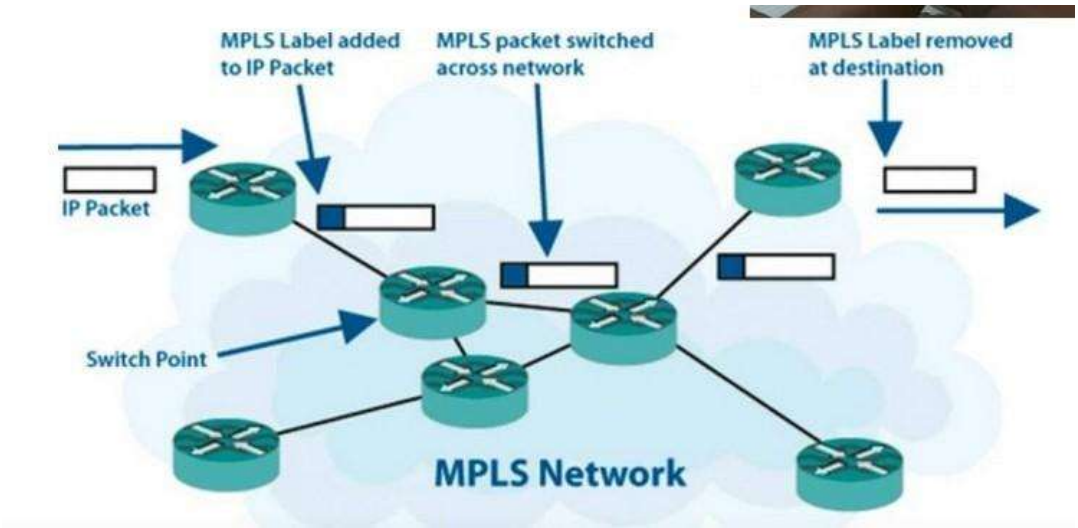
A VPN creates a secure, encrypted tunnel over a public network like the internet. It allows remote users or branch offices to securely connect to a private network, enabling them to access resources as if they were directly connected to the private network

It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.



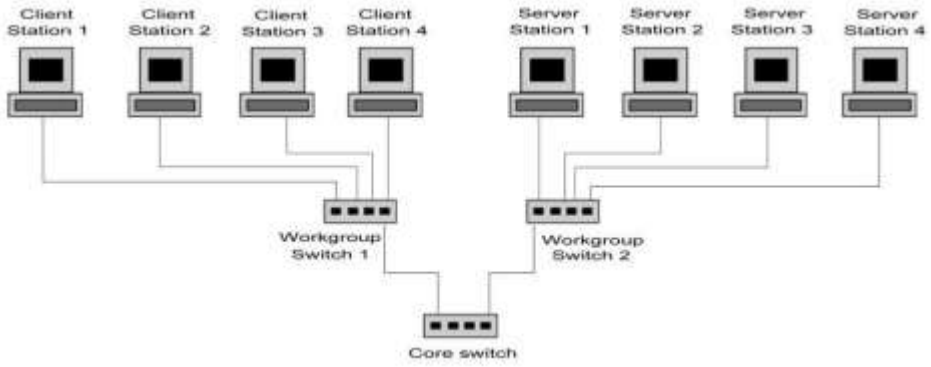
6. Multiprotocol Label Switching (MPLS):

MPLS is a technique used in high-performance telecommunications networks. It directs data from one network node to the next based on short path labels rather than long network addresses. This enhances network performance and allows for traffic engineering.



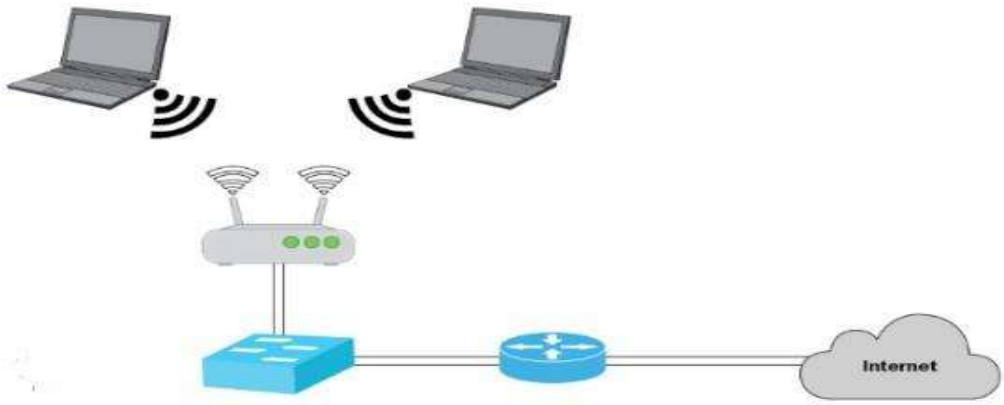
7. Ethernet

Ethernet is a standard for wired local area networks (LANs) and wide area networks (WANs). It uses a protocol that controls how data packets are placed on the network. Ethernet is widely used for connecting devices within a local area.



8. Wireless

Wireless WAN technologies utilize radio frequencies to connect devices and networks over the air. This can be through technologies like Wi-Fi or cellular networks. Wireless WANs are particularly useful in situations where wired connections are impractical.



9. Cloud-Based (SD-WAN)

SD-WAN (Software-Defined Wide Area Network) leverages cloud-based technology to centralize the control of WAN management. It allows for dynamic

path selection across multiple WAN links and can enhance performance, security, and management of a WAN.

- ✓ **Wired WAN connection technologies**

1.1. Leased line

A leased line is a dedicated, fixed-bandwidth, point-to-point data connection established between two locations. It provides a continuous and secure connection, typically over fiber optic cables. Leased lines are often used for critical applications that require consistent high-speed connectivity

1.2. T1/E1 Lines

T1 and E1 lines are digital telecommunications technologies that carry voice and data signals over copper or fiber optic lines. A T1 line provides a data rate of 1.544 Mbps, while an E1 line provides a data rate of 2.048 Mbps. These lines are commonly used for voice and data transmission in businesses**.**

1.3. T3/E3 Lines

T3 and E3 lines are high-speed digital transmission lines. T3 lines offer a data rate of 44.736 Mbps, while E3 lines provide 34.368 Mbps. They are typically used for connecting large networks or for high-volume data transfer requirements.

1.4. Metro Ethernet

Metro Ethernet is a technology that uses Ethernet as the access technology for connecting users to a wide area network. It provides high-speed, scalable, and cost-effective connectivity over metropolitan areas. Metro Ethernet is commonly used by businesses for connecting branch offices.

1.5. MPLS (Multiprotocol Label Switching)

MPLS is a technique used to speed up and shape network traffic flows. It directs data from one network node to the next based on short path labels, which

enhances network performance and allows for traffic engineering. MPLS is often used by enterprises to improve the efficiency and reliability of their WAN connections

These wired WAN connections offer various options for establishing reliable and high-speed communication between geographically dispersed locations. The choice of technology depends on factors such as bandwidth requirements, distance between locations, and budget considerations.

2. Wireless Connections technologies

2.1 **Wi-Fi/WLAN**

A WLAN connects local network nodes using radio technology rather than wired connections. Wi-Fi is a specific type of WLAN that conforms to the IEEE standard 802.11 and relies on access points (APs) to connect to clients and IoT devices using the 2.4 GHz, 5 GHz, and the 6 GHz band.

2.2 Cellular Networks

A cellular network or mobile network is a telecommunications network where the link to and from end nodes is wireless and the network is distributed over land areas called cells, each served by at least one fixed-location transceiver (typically three cell sites or base transceiver stations).

Popular examples for cellular networks are **GSM** (Global System for Mobile communication), **GPRS** (General Packet Radio Service), and **CDMA** (Code Division Multiple Access).

They have undergone significant development over time.

1G analog signal at the rate of 2.4kbps,

2G digital signal at the rate of 50kbps,

3G at the rate of 2mbps,

4G at the rate of 20 to 100mbps, and **5G** at the rate of 10gbps

2.3 Satellite

This is a communication system that provides links between various points on Earth. They are used for diverse purposes such as weather forecasting, television signal, amateur radio and internet communications and the Global

Positioning System. They are also used to look outward at the solar system for research and data gathering purposes.

3. Hybrid Connections

A hybrid connection is any connection that can use more than one type of connecting technology.

3.1 VPN

VPN stands for "**Virtual Private Network**" and describes the opportunity to establish a protected network connection when using public networks.

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online.

3.2 MPLS-VPN

This is a popular technique to build VPNs for customers over the MPLS provider network. It is a flexible method to transport and route several types of network traffic using an MPLS backbone. here are three types of MPLS VPNs deployed in networks today namely Virtual leased lines (VLL), virtual private LAN service (VPLS), and virtual private routed network (VPRN).

4. **Dial-up Connections**

4.1 Traditional Dial-up

Dial-**up** is a connection that is established using a modem. It is established when two or more communication devices use a public switched telephone network (PSTN) to connect to an Internet service provider (ISP). To make the dial-up connection, the modem must connect to an active phone line that is not in use.

Dial up has the following features:

- Dial up access offers speeds up to a maximum of only 56Kbs
- Dial up access is capable of providing internet access to only one PC/end-user, thereby charging extra for each additional PC/end user access.
- Dial up access is not a scalable service due to its bandwidth limitations of 56Kbps

Dial up access is faced with the sometimes-tedious process of dialing in for internet access.

4.2 ISDN (Integrated Services Digital Network)

Integrated Services Digital Network (ISDN) is a set of communications standards for the simultaneous digital transmission of voice, video, data, and other network services over the digitized lines of the public switched telephone network.

ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires.

ISDN lines can transmit uncompressed data at speeds up to 128 Kbps; with data compression, transmission speeds can jump to as much as 512 Kbps.

5. **Broadband Connections**

Broadband refers to various high-capacity transmission technologies that transmit data, voice, and video across long distances and at high speeds.

5.1 DSL (Digital Subscriber Line)

This is a type of internet connection that uses the voice frequency of telephone lines to send and receive internet data and traffic. DSL speeds vary from 256 Kbps to 100 Mbps.

5.2 Cable Internet

Cable internet is a type of broadband connection that uses cable television infrastructure to provide homes or buildings with Internet access. Functional cable internet requires a **Modem, Wi-Fi router, Coaxial cable, Switch, and Ethernet cable.** Speeds for cable internet can vary widely, anywhere up to 940 Mbps for downloading and up to 50 Mbps for uploading,

5.3 Fiber Optic

This is the technology used to transmit information as pulses of light through strands of fiber made of glass or plastic over long distances at speeds ranging from 100 Mbps up to 10 Gigabits per second (Gbps).

Theoretical Activity 1.3.2: Description of WAN connection types

Tasks:

1: Answer the following questions:

I. What is WAN connection?

II. Describe types of WAN connections

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 1.3.2 in trainee's manuals.

Key readings 1.3.2: Description of WAN Connection types.

A WAN (Wide Area Network) connection links multiple local area networks (LANs) across geographical locations, enabling data communication and resource sharing between remote sites. **1. Wired connection:** refers to a network connection where devices are linked using physical cables, such as Ethernet cables, to transmit data.

1.1. Leased line

A leased line is a dedicated, fixed-bandwidth, point-to-point data connection established between two locations. It provides a continuous and secure connection, typically over fiber optic cables. Leased lines are often used for critical applications that require consistent high-speed connectivity

1.2. T1/E1 Lines

T1 and E1 lines are digital telecommunications technologies that carry voice and data signals over copper or fiber optic lines. A T1 line provides a data rate of 1.544 Mbps, while an E1 line provides a data rate of 2.048 Mbps. These lines are commonly used for voice and data transmission in businesses**.**

1.3. T3/E3 Lines

T3 and E3 lines are high-speed digital transmission lines. T3 lines offer a data rate of 44.736 Mbps, while E3 lines provide 34.368 Mbps. They are typically used for connecting large networks or for high-volume data transfer requirements.

1.4. Metro Ethernet

Metro Ethernet is a technology that uses Ethernet as the access technology for connecting users to a wide area network. It provides high-speed, scalable, and cost-effective connectivity over metropolitan areas. Metro Ethernet is commonly used by businesses for connecting branch offices.

1.5. MPLS (Multiprotocol Label Switching)

MPLS is a technique used to speed up and shape network traffic flows. It directs data from one network node to the next based on short path labels, which enhances network performance and allows for traffic engineering. MPLS is often used by enterprises to improve the efficiency and reliability of their WAN connections

These wired WAN connections offer various options for establishing reliable and high-speed communication between geographically dispersed locations. The choice of technology depends on factors such as bandwidth requirements, distance between locations, and budget considerations.

2.Wireless Connections: refers to a network connection where devices communicate and transmit data without the need for physical cables, using radio waves or other wireless signals instead.

Wireless connections are commonly used in LANs (Local Area Networks) but also in WANs (Wide Area Networks) for long-distance data transmission.

2.1. Wi-Fi/WLAN

A WLAN connects local network nodes using radio technology rather than wired connections. Wi-Fi is a specific type of WLAN that conforms to the IEEE standard

802.11 and relies on access points (APs) to connect to clients and IoT devices using the 2.4 GHz, 5 GHz, and the 6 GHz band.

2.2. Cellular Networks

A cellular network or mobile network is a telecommunications network where the link to and from end nodes is wireless and the network is distributed over land areas called cells, each served by at least one fixed-location transceiver (typically three cell sites or base transceiver stations).

Popular examples for cellular networks are **GSM** (Global System for Mobile communication), **GPRS** (General Packet Radio Service), and **CDMA** (Code Division Multiple Access).

They have undergone significant development over time.

1G analog signal at the rate of 2.4kbps,

2G digital signal at the rate of 50kbps,

3G at the rate of 2mbps,

4G at the rate of 20 to 100mbps, and **5G** at the rate of 10gbps

2.3. Satellite

This is a communication system that provides links between various points on Earth. They are used for diverse purposes such as weather forecasting, television signal, amateur radio and internet communications and the Global Positioning System. They are also used to look outward at the solar system for research and data gathering purposes.

3. Hybrid Connections

A hybrid connection is any connection that can use more than one type of connecting technology.

3.1.VPN

VPN stands for "**Virtual Private Network**" and describes the opportunity to establish a protected network connection when using public networks.

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your

Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online.

3.2. MPLS-VPN

This is a popular technique to build VPNs for customers over the MPLS provider network. It is a flexible method to transport and route several types of network traffic using an MPLS backbone. Here are three types of MPLS VPNs deployed in networks today namely Virtual leased lines (VLL), virtual private LAN service (VPLS), and virtual private routed network (VPRN).

4. Dial-up Connections are a type of internet connection that uses a standard telephone line to connect to an Internet Service Provider (ISP).

4.1. Traditional Dial-up: is one of the earliest methods of connecting to the internet. It uses a standard analog telephone line to establish a connection to an Internet Service Provider (ISP).

4.2. ISDN (Integrated Services Digital Network): is a digital communication method that uses digital telephone lines to transmit both voice and data. It allows for multiple data and voice channels on a single line, providing faster data transmission than traditional dial-up.

5. Broadband Connections: refers to various high-capacity transmission technologies that transmit data, voice, and video across long distances and at high speeds.

5.1. DSL (Digital Subscriber Line)

This is a type of internet connection that uses the voice frequency of telephone lines to send and receive internet data and traffic. DSL speeds vary from 256 Kbps to 100 Mbps.

5.2. Cable Internet: is a type of broadband connection that uses cable television infrastructure to provide homes or buildings with Internet access.

Functional cable internet requires a Modem, Wi-Fi router, Coaxial cable, Switch, and Ethernet cable. Speeds for cable internet can vary widely, anywhere up to 940 Mbps for downloading and up to 50 Mbps for uploading.

5.3. Fiber Optic: This is the technology used to transmit information as pulses of light through strands of fiber made of glass or plastic over long distances at speeds ranging from 100 Mbps up to 10 Gigabits per second (Gbps).

Practical Activity 1.3.3: Connecting WAN connections.

Task:

1: Refer to the key reading 1.3.3 and perform the following task:

You are asked to go to your school WAN and establish hybrid connections that enable secure data exchange and network communication.

2: Present the steps of establishing hybrid connections

3: Connect hybrid connection.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 1.3.3.

6: Perform the activity in the application of learning 1.3.

Key readings 1.3.3: Connecting WAN connections.

To perform hybrid WAN connections using MPLS-VPN for secure data exchange and communication, here's a simplified operational plan:

1. Evaluate Network Readiness

- Ensure all routers and devices in the school's WAN support MPLS and VPN technologies.
- Confirm the availability of a reliable internet connection for the VPN component.

2. Configure MPLS

- Access MPLS-capable routers: Log into your edge and core routers.
- Enable MPLS: On each router, enable MPLS forwarding. For example, on a Cisco router, you can use the following commands:

```
router> enable
router# configure terminal
router(config)# mpls ip
router(config)# interface <interface>
router(config-if)# mpls ip
```

- Assign Labels: Set up MPLS label distribution protocol (LDP) to facilitate the labeling of packets for forwarding.

3.Set Up VPN

- VPN Gateway: Configure a VPN gateway on the network to enable secure access to remote locations. If using IPsec VPN, the basic steps include:

```
router(config)# crypto isakmp policy 1
router(config-isakmp)# encryption aes
router(config-isakmp)# hash sha256
router(config-isakmp)# authentication pre-share
router(config-isakmp)# group 5
```

- VPN Configuration for Remote Users: Provide VPN access credentials to remote users (e.g., staff or teachers) to connect securely via the VPN.

4. Establish Hybrid Connections

- Combine MPLS and VPN: Ensure that MPLS handles internal traffic within the WAN for high-priority, low-latency needs, while VPN secures remote access and internet-bound traffic.
- Configure the router interfaces to ensure proper routing between MPLS paths and VPN connections.

5. Implement Security

- Set up encryption and strong authentication protocols (e.g., IPsec with AES encryption).
- Use access control lists (ACLs) on routers to restrict access to only authorized VPN connections.

6. Test and Verify

- Test the VPN connection from a remote user location to ensure encrypted access.
- Test MPLS paths for low-latency communication across your WAN sites.
- Monitor network traffic using WAN monitoring tools to ensure performance is as expected.

Points to Remember

- The Common WAN Technologies are Point to point, Hub and Spoke, Full Mesh, Virtual Private Network (VPN), Multiprotocol Label Switching (MPLS), Ethernet, Wireless and Cloud Based (SD WAN).
- Types of WAN connections are: Wired Connections, Wireless Connections, Hybrid Connections, Dial-up Connections and Broadband Connections.
- While connecting WAN connections, consider the following steps:

✓ Evaluate Network Readiness.
✓ Configure MPLS.
✓ Set Up VPN.
✓ Establish Hybrid Connections.
✓ Implement Security.
✓ Test and verify.

Application of learning 1.3.

XYZ Media Ltd is a growing private company operating in Gasabo, Rubavu, and Nyagatare. To enhance communication and data sharing across these districts, they decide to establish a wide area network (WAN). As student you are tasked to implement various WAN technologies and connections to ensure a reliable and efficient network.

Indicative content 1.4: Apply Modulation & Demodulation Techniques

Duration: 4 hrs

Theoretical Activity 1.4.1: Description of modulation and demodulation techniques.

Task:

1. Answer the following questions:
   i. What do you understand by the following terms?
      a. Modulation
      b. Demodulation
      c. Digital Modulation
      d. Optical Modulation
   ii. Give and explain the types of Modulation?
   iii. Differentiate unguided and guided optical modulation?
2. Write your findings on paper flipchart, blackboard or whiteboard.
3. Present your findings to the whole class.
4. Ask for clarification where necessary.
5. Read the Key readings 1.4.1.

Key readings 1.4.1: Description of modulation and demodulation Techniques

Introduction:

Modulation: is the process of converting digital data (binary 0s and 1s) into analog signal that can be transmitted over communication channels like radio waves, telephone lines, or optical fibers.

Demodulation: is the process of extracting the original information-bearing signal from a modulated carrier wave. It's essentially the reverse of modulation.

Types of modulation

1. **Analog modulation** is a process where the properties of a continuous wave (called the carrier signal) are varied in proportion to a message signal, which is typically analog.

1.1. Amplitude Modulation (AM): The amplitude of the carrier signal is varied in proportion to the message signal.

1.1.1. Types of Amplitude Modulation (AM):

- ✓ **Double-Sideband (DSB-AM)**: Standard AM; both sidebands are transmitted.
- ✓ **Single-Sideband (SSB-AM)**: Only one sideband is transmitted to conserve bandwidth.
- ✓ **Vestigial Sideband (VSB-AM)**: A compromise between DSB and SSB where one sideband is fully transmitted, and the other is partially transmitted.

1.1.2. Applications of Amplitude Modulation (AM): AM radio broadcasting, aviation communication.

1.2. Frequency Modulation (FM): The frequency of the carrier wave is varied according to the amplitude of the message signal.

1.2.1. Applications: FM radio broadcasting, audio signals in television.

1.3. Phase Modulation (PM): The phase of the carrier wave is varied in accordance with the message signal.

1.3.1. Applications: Used in digital communication systems like Wi-Fi and satellite systems.

2. **Digital Modulation:** Digital modulation is a technique used in wide area networks (WANs) to transmit digital data over analog channels.

2.1. Amplitude Shift Keying (ASK): The amplitude of the carrier wave is changed according to the digital data being transmitted (on-off keying for binary data).

2.1.1. Applications: Low-speed communication systems like optical fiber communication.

2.2. Frequency Shift Keying (FSK): The frequency of the carrier wave is shifted between discrete values to represent binary data.

2.2.1. Applications: Wireless systems, low-frequency communication, like pager systems.

2.3. Phase Shift Keying (PSK): The phase of the carrier wave is changed to represent binary data.

2.3.1. Types of Phase Shift Keying (PSK):

✔ **Binary Phase Shift Keying (BPSK)**: Two phases are used to represent 0s and 1s.

✔ **Quadrature Phase Shift Keying (QPSK)**: Four phases are used, allowing two bits to be transmitted per symbol.

2.3.2. Applications: Satellite communications, Wi-Fi, Bluetooth.

3. Optical modulation: refers to the process of encoding information onto a light signal, typically for transmission over fiber optic cables.

Fiber optics use light (usually from lasers or LEDs) as the carrier of data, and the modulation of this light allows digital information to be transmitted over long distances at high speeds.

3.1. Unguided optical modulation refers to the process of modulating a light signal that is transmitted through free space rather than through a physical medium like an optical fiber. In this case, the light (usually from a laser or LED) travels through the air or vacuum to communicate information, often in wireless optical communication systems such as Free Space Optical (FSO) communication.

3.2. Guided optical modulation refers to the process of controlling or varying the properties of a guided light signal (such as amplitude, phase, or frequency) as it travels through an optical waveguide, such as an optical fibre. This modulation can encode information onto the light signal for communication or data transmission purposes.

Difference between Unguided optical modulation and guided optical modulation.

1. Unguided Optical Modulation:

- ✓ **Transmission medium:** Free space (air or vacuum).
- ✓ **Example:** Laser communication systems, where the laser beam is transmitted directly through the air to a receiver.

✔ **Advantages:**

- No physical infrastructure required.
- Potentially high data rates.
- Can cover long distances.

✔ **Disadvantages:**

- Susceptible to atmospheric conditions (e.g., fog, rain, turbulence).
- Security concerns (eavesdropping).
- Limited bandwidth compared to guided optical modulation.

2. Guided Optical Modulation

✔ **Transmission medium:** Optical fibers.

✔ **Example:** Fiber-optic communication systems, where light is transmitted through thin, flexible glass or plastic fibers.

✔ **Advantages:**

- High bandwidth, allowing for the transmission of large amounts of data.
- Low attenuation, resulting in minimal signal degradation over long distances.
- Immunity to electromagnetic interference.
- High security due to the confinement of light within the fiber.

✔ **Disadvantages:**

- Requires a physical infrastructure of optical fibers.
- Installation can be expensive.
- Potential for fiber breaks or damage.

Practical Activity 1.4.2: Applying Modulation and Demodulation Techniques

Task:

1: Refer to the key reading 1.4.2 and perform the following task:

You are asked to go to the WAN site, which is near to your school, and apply modulation and Demodulation techniques used to enable data transmission over long distances.

2: Presents the steps of apply modulation and Demodulation techniques.

3: Apply modulation and demodulation techniques in WAN.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 1.4.2.

6: Perform the activity in the application of learning 1.4.

Key readings 1.4.2: Applying Modulation and Demodulation Techniques

Steps to Perform Modulation and Demodulation:

1. **Install WAN Devices:**

- Ensure that the modems or routers capable of handling modulation and demodulation are installed at both ends of the WAN link (e.g., between different buildings or distant networks).
- Devices like DSL modems, satellite modems, or optical Fiber transceivers are commonly used for this purpose.

2. **Configure the Modem or Transceiver:**

- Access the configuration panel of the modem (typically through a web interface or command-line interface).
- Set up the modulation scheme (e.g., QAM, FSK, PSK) that is appropriate for the type of medium (fibre-optic, satellite, or copper cables).
- Select the transmission rate and bandwidth depending on your network's capabilities and requirements.

3. **Test the Connection:**

- Once configured, perform a test transmission of data from one location (e.g., sending files from Building A).
- Ensure the modem or transceiver modulates the digital data into analog signals and transmits it over the physical medium (fiber, copper, etc.).

4. **Receive and Demodulate:**

- At the receiving end (e.g., in Building B), the modem or transceiver will automatically demodulate the received analog signal back into digital data.
- You can verify the successful transmission by checking whether the file/data appears correctly at the destination server or device.

5. **Monitor for Errors:**

- Use WAN monitoring tools to check for signal degradation or transmission errors, adjusting the modulation settings if necessary to optimize performance.

Points to Remember

- Modulation is the process of converting digital data (binary 0s and 1s) into analog signals that can be transmitted over communication channels and Demodulation is the process of extracting the original information-bearing signal from a modulated carrier wave.
- Digital modulation is a technique used in wide area networks (WANs) to transmit digital data over analog channels and Optical modulation refers to the process of encoding information onto a light signal.
- When discussing modulation types, Key types of modulation include analog modulation such as Amplitude Modulation and Frequency Modulation, digital modulation such as Phase Shift Keying and Quadrature Amplitude Modulation, and optical modulation such as modulation of light waves using techniques like On-Off Keying and Pulse Position Modulation.
- Additionally, guided optical modulation uses optical fibers, whereas unguided optical
- Modulation involves free-space light transmission.
- You should consider the type of data and distance to determine the best modulation method.
- You should use suitable methods such as Amplitude Modulation (AM), Frequency Modulation (FM), or Phase Modulation (PM) based on the WAN's needs.
- Ensure the demodulation technique is compatible with the modulation process to accurately decode the transmitted signal.
- Verify that both the transmitting and receiving devices support the chosen modulation/demodulation techniques.
- You should monitor data integrity, signal strength, and transmission quality to detect any issues.

Application of learning 1.4.

Suppose that in your school needs to establish efficient and reliable data transmission over long distances, as an IT technician you are requested to apply modulation and demodulation techniques which will be suited in that place.

Indicative content 1.5: Apply Multiplexing & Demultiplexing

Duration: 4 hrs

Theoretical Activity 1.5.1: Description of Multiplexing and De-multiplexing Techniques.

Task:

1: Answer the following questions:

i. What do you understand by the following terms?

   a. Multiplexing

   b. De-Multiplexing

ii. What are the different types of multiplexing techniques used in WAN?

iii. List out the types of Time division multiplexing (TDM)

2: Write your findings on paper flipchart, blackboard or whiteboard.

3: Present your findings to the whole class.

4: Ask for clarification where necessary.

5: Read the Key readings 1.5.1.

Key readings 1.5.1: Description of Multiplexing and De-multiplexing Techniques

- **Introduction:**

Multiplexing and de-multiplexing are essential techniques used in Wide Area Networks

(WANs) to efficiently manage and transmit data across long distances.

Multiplexing: is the process of combining multiple signals or data streams into one signal for transmission over a shared medium.

This allows for more efficient use of the communication channel by transmitting several signals simultaneously.

De-multiplexing refers to the process of separating multiple data streams that were combined (multiplexed) into a single signal for transmission across the network.

1.1. Frequency Division Multiplexing (FDM): FDM assigns each signal a unique frequency band within a shared communication channel.

Multiple signals are transmitted at different frequencies simultaneously.

1.2. Time division multiplexing (TDM): In TDM, multiple signals are transmitted by allocating each signal a specific time slot.

This ensures that only one signal is transmitted at a time but rapidly switches between different signals so that it appears they are transmitted simultaneously.

1.2.1. How TDM (Time division multiplexing) Works:

- **Time Slots:** The communication channel is divided into fixed, repeating time intervals (slots). Each data stream is allocated a specific slot in the sequence.
- **Transmission:** The data streams take turns using the channel. During its designated time slot, a data stream can send its data.
- **High Speed Switching:** The transmission happens so quickly that the individual signals appear to be transmitted simultaneously, but they are being sent one after another.
- **Synchronization:** The receiver is synchronized with the transmitter to correctly interpret which time slot corresponds to which signal.

1.2.2. Types of TDM (Time division multiplexing):

- **Synchronous TDM:** Time slots are pre-assigned to specific data streams, whether or not the data is ready to be transmitted.

  It works best when the data sources have predictable traffic patterns.

  Example: Telephone networks traditionally used synchronous TDM to allocate time slots for voice communication.

- **Asynchronous TDM (or Statistical TDM):** Time slots are dynamically assigned based on demand. If a data stream has no data to send, its time slot is not used.

  This is more efficient as bandwidth is allocated only when data is ready.

  Example: Modern data networks often use statistical TDM for efficiency.

1.2.3. Wavelength division multiplexing (WDM): Used in Fiber optic communication,

WDM works similarly to FDM but transmits data using different wavelengths (or colors) of light through the same optical Fiber.

1.2.4. Code Division Multiplexing (CDM): CDM allows multiple signals to be transmitted over the same channel simultaneously by assigning unique codes to each signal, allowing the receiver to distinguish between them.

Practical Activity 1.5.2: Applying Multiplexing and De-Multiplexing Techniques

Task:

1: Refer to the key reading 1.5.2 and perform the following task::

Go to your school WAN and manage the WAN link between two branches of your school, Branch A and Branch B. network needs to transmit voice (VoIP), video conferencing, and file transfer data simultaneously over the same WAN link, configure multiplexing and de-multiplexing.

2: Present steps to perform modulation and demodulation.

3: Apply Multiplexing (TDM) and Frequency Division Multiplexing (FDM) in WAN.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 1.5.2.

6: Perform the activity in the application of learning 1.5.

Key readings 1.5.2: Applying Multiplexing and De-Multiplexing Techniques

- Steps to Configure and Manage Multiplexing and Demultiplexing for WAN Link (Branch A to Branch B)

1. **Assess Network Requirements**

- Identify the bandwidth needs for voice (VoIP), video conferencing, and file transfer.
- Ensure the WAN link can support the combined data traffic without congestion.

2. **Select the Right Multiplexing Technique**

- Choose **Time Division Multiplexing (TDM)** for fixed time slots for each data type.
- Alternatively, choose **Frequency Division Multiplexing (FDM)** if different frequencies can be allocated to each type of traffic.
- Ensure that your network equipment (routers, switches) supports the selected technique.

3. **Configure Multiplexing on the WAN Link**

- Access the network router or WAN device at Branch A.
- Set up the **Multiplexing Protocol** (TDM or FDM).
- Assign proper **bandwidth allocation** for each service (VoIP, video, and file transfer), ensuring higher priority for real-time services like VoIP and video conferencing.

4. **Apply Quality of Service (QoS) Policies**

- Implement **QoS rules** on the router to prioritize voice and video traffic, ensuring minimal latency for these services.
- Configure specific **port numbers** for each type of data to ensure that traffic is correctly classified and prioritized.

5. **Configure Demultiplexing at Branch B**

- Set up the router at Branch B to recognize and demultiplex incoming traffic based on the settings configured at Branch A.
- Ensure that the router separates the voice, video, and file transfer streams.

6. **Monitor WAN Link Performance**

- Use WAN monitoring tools to track **bandwidth usage**, latency, and packet loss for each data type.
- Set up alerts to detect performance issues, especially for real-time services like VoIP and video conferencing.

7. **Test the Configuration**

- Conduct tests for each service (VoIP, video conferencing, file transfer) to ensure proper transmission and demultiplexing.
- Adjust **QoS settings** if one type of traffic negatively impacts others.

8. **Optimize as Needed**

- Regularly analyze the performance of the WAN link and adjust multiplexing or QoS settings to optimize the efficiency of the data transmission.

Points to Remember

- Multiplexing is the process of combining multiple data streams into a single signal while de-multiplexing separates the combined signal back into its original data streams.
- In WAN, the main types of multiplexing techniques include Time Division Multiplexing (TDM), Frequency Division Multiplexing (FDM) and Wavelength Division Multiplexing (WDM).
- TDM further includes synchronous TDM and asynchronous TDM.
- While Applying Multiplexing and De-Multiplexing Techniques:

✓ Ensure the WAN link can handle voice (VoIP), video conferencing, and file transfer simultaneously.

✓ Use a suitable multiplexing technique (e.g., Time Division Multiplexing - TDM, or Frequency Division Multiplexing - FDM) to combine multiple data streams over a single WAN link.

✓ Prioritize traffic using Quality of Service (QoS) settings to ensure voice and video data (real-time) have priority over file transfer (non-real-time).

✓ Ensure the equipment at both branches is configured to properly separate the combined data streams into individual components (VoIP, video, and files.

✓ Monitor bandwidth to ensure the WAN link can handle the data volume without delays or interruptions.

✓ Regularly test the performance of the link for each data type, and optimize based on performance results.

Application of learning 1.4.

Your school needs to establish efficient and reliable data transmission over long distances. As an IT technician, you are requested to apply multiplexing and de-multiplexing techniques that will suit this purpose.

Learning outcome 1 end assessment

Theoretical assessment

Q1. Match the following Concept in the column A with their descriptions in the column B and write a letter to the number corresponding to the correct answer.

Answers	Column A	Column B
1……	1.Site assessment	**A.** Refer to the process of systematically recording and organizing information, observations, or results from a study, investigation, or research project.
2……	2. Define the objectives	**B.** Refers to the process of evaluating a physical location to determine its suitability for network infrastructure deployment. This involves assessing various factors that can impact network performance, reliability, and security.
3……	3.Document findings	**C.** Clearly define the reason for the visit, whether it's for assessment, research, inspection, training, or networking.
4……	4.Understand Purpose	**D.** Set specific goals for the visit, such as evaluating performance, gathering data, identifying hazards, or providing training.
5……	5.Prepare a report	**E.** Write a comprehensive report summarizing your findings, conclusions, and recommendations.
6……		**F.** Refer to the physical inspection and assessment of a location where a wide area network (WAN) is to be implemented or upgraded.

Q2. Match the Multiplexing Technique in column A with its Key Feature in column B of the with the in the column C, with its corresponding task:

Column A	Column B	Column C (Answers)
1.Frequency Division Multiplexing (FDM)	A. Uses unique codes for each signal	……
2.Time Division Multiplexing (TDM)	B. Multiple signals are transmitted at different frequencies	……
3.Wavelength Division Multiplexing (WDM)	C. Time slots are allocated based on demand	……

4. Code Division Multiplexing (CDM)	D. Transmits signals at different wavelengths of light	……
5. Statistical TDM	E. Divides the available bandwidth into time slots	……
	F. Dynamically assigned based on demand.	

Q3. Define the following terms:

i. WAN Site visits

ii. Site assessment

iii. WAN

iv. LAN

v. VLAN

Q4. Answer the following question using true if the statements below are correct or false if they are incorrect:

i. MAN Is a network that connects computers and devices within a limited geographic area, such as a single building or campus.

ii. LAN Is a network that connects multiple MANs within a metropolitan area. LANs are typically used to connect businesses, educational institutions, and government agencies within a city or region.

iii. WANs (Wide Area Networks) are used to connect multiple remote locations over a large geographic area.

iv. VLAN is a logical division of a physical network into multiple virtual networks.

v. An autonomous system is a collection of IP networks and routers under the control of a single organization that presents a common routing policy.

vi. In Frequency Division Multiplexing (FDM), multiple signals are transmitted simultaneously, each within its own frequency range, without time-sharing the transmission medium.

vii. Time Division Multiplexing (TDM) uses different wavelengths to transmit multiple data streams, like Wavelength Division Multiplexing (WDM).

viii. Amplitude Modulation (AM) alters the frequency of the carrier wave to encode information.

ix. In Frequency Shift Keying (FSK), digital data is transmitted by varying the frequency of the carrier signal between two discrete values.

Q5. Circle only the correct answer for the questions below:

A. The following tools are used for configuring router EXCEPT two (2) of them:

   i. Cable tester
   ii. CAT6 or CAT6e
   iii. Crimping tool
   iv. Coaxial Cables
   v. Only ii and iv is correct.

B. The following Materials are not used for configuring router EXCEPT two (2) of them:

   i. Fiber optic cables
   ii. Access Point
   iii. Coaxial Cables
   iv. Routers
   v. Switches

C. The following equipment are used for configuring router EXCEPT:

   i. Modems
   ii. Rack Mount
   iii. Wire cutter
   iv. Access Point
   v. Computer

D. Which of the following is a type of analog modulation technique?
   i. Amplitude Shift Keying (ASK)
   ii. Frequency Shift Keying (FSK)
   iii. Amplitude Modulation (AM)
   iv. Phase Shift Keying (PSK)

E. In Frequency Modulation (FM), the information signal is represented by variations in which characteristic of the carrier wave?
   i. Amplitude
   ii. Frequency
   iii. Phase
   iv. Wavelength

F. Amplitude Shift Keying (ASK) is a digital modulation technique where the information is encoded by varying the _____ of the carrier signal.
   i. Frequency
   ii. Amplitude
   iii. Phase
   iv. Bandwidth

G. Which of the following types of optical modulation is guided by a physical medium like fiber optic cables?
   i. Unguided
   ii. Guided
   iii. Free space
   iv. Line-of-sight

Q6 Fill in the Blanks using the appropriate words:

1. A T1 line offers a bandwidth of _____ Mbps**. (2.5, 1.544, 15).**
2. In a Hub and Spoke WAN technology, all data passes through a _____ before reaching its destination. **(Hub, router, switch)**
3. SD-WAN stands for _____. **(software defined WAN, software digital WAN)**
4. _____ is a technology used to route traffic based on labels instead of long network addresses**. (MPLS,SDWAN,VLAN)**

Practical assessment

You are an IT network engineer for XYZ Company that is expanding its operations. The company plans to set up a new Wide Area Network (WAN) to connect their headquarters to three branch offices in different cities. You have been tasked with conducting a site visit to assess the infrastructure, identify installation requirements, and set up a reliable WAN that supports data communication between the locations. During this project, you will apply key networking techniques, including modulation, demodulation, multiplexing, and demultiplexing, to ensure efficient and reliable data transmission.

References

Clark, R. (2020, May 25). *Efficient Demultiplexing in WAN Systems: Techniques and Applications.* San Francisco, CA.: Wide Area Network Digest.

Davis, P. (2020, October 5). *Demodulation Techniques for Efficient WAN Communication.* Los Angeles, CA.: Network Infrastructure Journal.

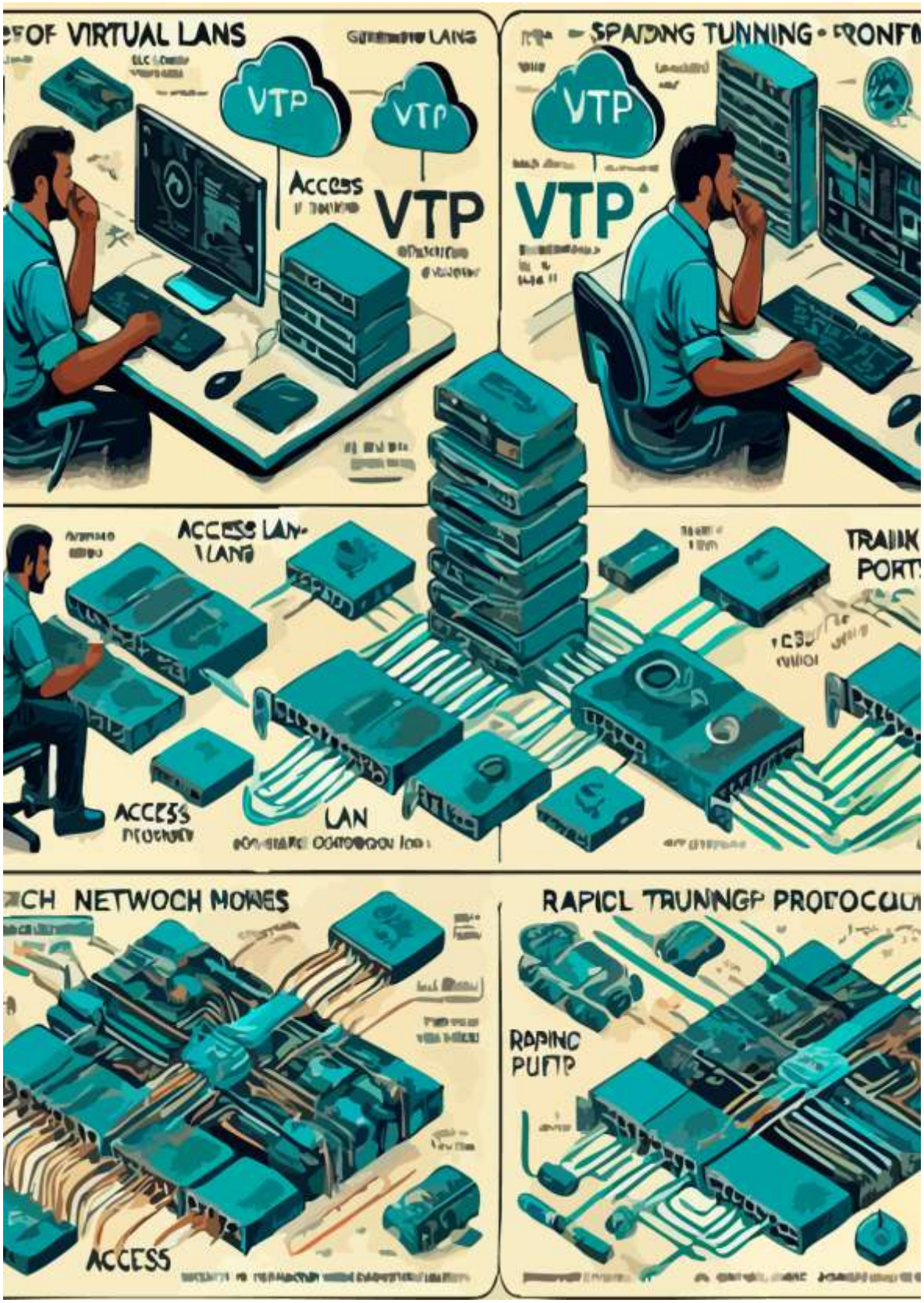
Smith, A. (2021, March 12). *Modulation Techniques in Wide Area Networks: An Overview.* Chicago, IL.: Global Communication Systems.

Taylor, M. (2021, July 18). *Multiplexing Methods for Optimizing WAN Performance.* New York, NY.: Telecommunications Today.

Difference between modulation and demodulation. (2025, January). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/difference-between-modulation-and-demodulation/

WAN and WAN technology. (2025, January). Retrieved from www.ipcisco.com: https://ipcisco.com/lesson/wan-and-wan-technologies/

www.scaler.in. (2025, January). Retrieved from Multiplexing and demultiplexing in computer networks: https://www.scaler.in/multiplexing-and-demultiplexing-in-computer-networks/


VIRTUAL LANS
VTP
VTP
Access
VTP
VTP
VTP
ACCESS LAN-
LAN
ACCESS
LAN
ACCESS

Indicative contents

2.1. Creation of VLANs.

2.2. Configuration of VTP.

3.3. Configuration of Switch port Interface.

2.4. Configure inter VLAN routing.

2.5. Configure Spanning Tree Protocol.

2.6. Apply Converge STP.

2.7. Configure PVST+, RSTP and rapid PVST+.

2.8. Apply Aggregation modes.

Key Competencies for Learning Outcome 2: Apply VLAN Configurations

Knowledge	Skills	Attitudes
• Description of VLAN. • Description of VTP. • Description of inter-VLAN routing. • Description of STP. • Description of PVST+, RSTP and rapid PVST+.	• Configuring VLANs. • Verifying VLANs configuration. • Configuring VTP. • Configuring Switch port interface. • Configuring inter-VLAN routing. • Verifying inter-VLAN Routing. • Configuring STP. • Applying converge STP. • Configuring PVST+, RSTP and rapid PVST+	• Being adaptable while configuring. • Having critical thinking while configuring. • Detail-Oriented when setting up inter-VLAN routing

	• Applying Aggregation modes.	

Duration: 30 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly VLAN as used in switched network.
2. Create properly VLANs based on organization's structure.
3. Describe clearly VTP as used in switched network.
4. Configure appropriately VTP based on created VLANs.
5. Configure properly Switchport interfaces based on modes.
6. Describe clearly Inter-VLAN routing as used in router or layer 3 switch.
7. Implement effectively Inter-VLAN based on different created VLANs.
8. Describe clearly STP as used in switched network.
9. Apply properly Spanning Tree Protocol (STP) based on IEEE 802.1Q standards.
10. Describe clearly PVST+, RSTP and rapid PVST+ as used in switched network.
11. Configure correctly PVST+, RSTP and rapid PVST+ based on switch.
12. Apply efficiently Aggregation modes based on IEEE 802.1Q standards.

Resources

Equipment	Tools	Materials
• Routers • Switches • Hubs • Repeaters • Gateways • Bridges • Modems • Uninterruptible Power Supply (Ups)	• Network Cable Testers • SolarWinds Network Performance Monitor (NPM) • Paessler PRTG • Network Monitor • Wireshark	• CAT5 • CAT6 • Fiber optic cables • Coaxial Cables • BNC • RJ45 • RJ11

Indicative content 2.1: Creation VLANs.

Duration: 5 hrs

Theoretical Activity 2.1.1: Description of VLAN.

Tasks:

1: Read carefully and answer the following questions:

i. What is VLAN?
ii. What are the primary benefits of implementing VLANs in a network?
iii. What is the range of VLAN IDs?
iv. What are the main characteristics of a VLAN?
v. What are the different types of VLANs?
vi. What are the different types of network traffic in VLAN environments?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 2 .1.1 in trainee manuals.

Key readings 2.1.1. Description of VLAN Concepts.

1. VLAN (Virtual Local Area Network) Overview

- **Definition**: A VLAN is a logical subdivision of a physical network, which allows devices in different physical locations to communicate as if they were on the same physical LAN. VLANs are created to improve network efficiency and security.
- **Purpose**: VLANs isolate network segments for performance and security, reducing the size of broadcast domains.

2. Benefits of VLANs

1. **Improved Security**: VLANs segment network traffic, reducing the risk of attacks by isolating sensitive data or devices.

2. **Enhanced Performance**: By reducing the size of broadcast domains, VLANs reduce unnecessary traffic and enhance network efficiency.
3. **Simplified Management**: VLANs allow for logical grouping of devices, making it easier to manage large, complex networks.
4. **Flexibility**: Devices can be grouped into the same VLAN regardless of physical location, offering flexibility in network design.

3. VLAN ID Range

The **VLAN ID Range** refers to the numerical identifiers used to distinguish different VLANs within a network. Each VLAN is assigned a unique VLAN ID, which helps the switch or router identify and separate traffic within the VLAN.

Two Main VLAN ID Ranges:

- **Normal Range VLANs (VLAN IDs 1-1005)**:

VLAN ID 1: Default VLAN for all switch ports. Cannot be deleted or renamed but can be used for normal traffic.

VLAN IDs 2-1001: Usable VLANs for normal purposes in small to medium-sized networks.

VLAN IDs 1002-1005: Reserved VLANs for legacy purposes (used for FDDI and Token Ring networks).

Stored in the **VLAN database** and persist through reboots.

1. **Extended Range VLANs (VLAN IDs 1006-4094)**:

Used in **larger networks** requiring a greater number of VLANs.

Not supported by all switches (depends on the switch model and software).

Stored in the device's **running configuration (NVRAM)**, not the VLAN database.

Often used in service provider environments and larger enterprises.

4. VLAN Characteristics

1. **Segmentation**: VLANs logically segment a physical network into smaller, separate broadcast domains.
2. **Broadcast Domain Control**: VLANs limit the scope of broadcast traffic to the devices within the same VLAN. Devices in one VLAN will not receive broadcast messages from another VLAN, reducing unnecessary traffic and improving performance.
3. **Inter-VLAN Communication**: Devices within the same VLAN can communicate directly. However, devices in different VLANs require a **Layer 3 device** (router or Layer 3 switch) for communication, a process known as **Inter-VLAN routing**.
4. **Improved Network Security**: VLANs isolate traffic between segments of the network. Unauthorized users cannot access devices or resources in other VLANs

unless explicitly allowed through routing or firewall configurations, enhancing security.

5. **Flexibility and Scalability**: VLANs are independent of physical network topology, meaning devices from different physical locations can be placed in the same VLAN. This allows for easier reconfiguration and network expansion without hardware changes.
6. **Quality of Service (QoS)**: VLANs can be prioritized for certain types of traffic (e.g., Voice VLANs for VoIP). This ensures **Quality of Service (QoS)**, giving priority to time-sensitive traffic like voice or video over regular data traffic.
7. **Simplified Network Management**: VLANs allow for logical grouping of devices, making network administration easier.

   Changes like adding or removing devices from a VLAN can be done through configuration without physically changing connections.
8. **Traffic Filtering**: Traffic between VLANs can be filtered using access control lists (ACLs) or firewalls, allowing administrators to control which devices or services can be accessed across VLANs.
9. **VLAN Tagging (802.1Q)**:

- When a device communicates across a network, VLAN information is tagged onto the Ethernet frame. This tagging process allows switches to identify the VLAN a packet belongs to, ensuring proper routing of the packet.

Types of VLANs
Main Types of VLANs

- ✓ **Data VLAN**:

Purpose: Carries user data traffic.

Example: VLANs for different departments like sales or engineering.

- ✓ **Voice VLAN**:

Purpose: Optimized for carrying voice traffic from IP phones, ensuring QoS.

Example: A VLAN specifically for VoIP communication.

- ✓ **Management VLAN**:

Purpose: Used for network management traffic (e.g., SNMP).

Example: A dedicated VLAN for network management tools.

- ✓ **Native VLAN**:

Purpose: Carries untagged traffic on a trunk port, used in trunking configurations.

Example: Typically configured as VLAN 1, but can be set to any VLAN.

- ✓ **Default VLAN**: The VLAN assigned to all switch ports by default, typically VLAN 1.

Purpose:

To carry untagged traffic on access ports.

To manage the switch and other devices connected to it.

Characteristics:

All ports are members of the default VLAN until reconfigured.

Typically used for management tasks and communication that does not involve VLAN tagging.

5. **Network traffic types**
   Network traffic types Refer to the different kinds of data transmitted over a network.

   Network traffic types is cotegorized into the following:

1. **Data**

- ✓ **Web Traffic:** HTTP/HTTPS traffic generated by web browsers accessing websites.
- ✓ **File Transfer Traffic:** FTP/SFTP traffic used for transferring files between computers.
- ✓ **Database Traffic:** Traffic generated by database servers and clients interacting with databases.
- ✓ **Email Traffic:** SMTP, POP3, and IMAP traffic related to sending and receiving emails.

2. **Voice Traffic**
   Voice-over-IP (VoIP): Voice conversations transmitted over the internet using protocols like SIP, H.323, and RTP.

3. **Video Traffic**

- ✓ **Streaming Video:** Real-time transmission of video content, such as from video streaming platforms like Netflix or YouTube.
- ✓ **Video Conferencing:** Traffic generated during video conferences using applications like Zoom or Microsoft Teams.

4. **Control Traffic**

- ✓ **Network Management:** Traffic used to manage and monitor network devices and services.

- ✓ **Routing Protocols:** Traffic exchanged between routers to determine the best path for packets.
- ✓ **Security Protocols:** Traffic related to network security, such as firewall rules, intrusion detection systems, and VPN connections.

5. Application-Specific Traffic

- ✓ **Gaming Traffic:** Traffic generated by online games.
- ✓ **IoT Traffic:** Traffic from Internet of Things devices.
- ✓ **Real-time Applications:** Traffic for applications requiring low latency, such as financial trading or remote surgery

6. **Controlling Broadcast Domains**

A **broadcast domain** is a logical division of a computer network where all devices can receive broadcast messages from each other. Controlling broadcast domains is important in networking because excessive broadcasts can lead to network congestion, reduced performance, and increased collision rates.

7.1 Methods to control broadcast domains:

1. **Routers**: Routers separate broadcast domains by design. Devices in different networks (subnets) do not share broadcast messages.
2. **VLANs (Virtual Local Area Networks)**: VLANs logically separate devices within the same physical network, creating isolated broadcast domains.

✓ **Network Without VLANs**

In a network without VLANs, all devices connected to the same switch or set of switches are part of the same broadcast domain. Broadcast traffic (such as ARP requests or DHCP discovery) is forwarded to all devices.

Challenges of Network Without VLANs

- Increased network traffic due to broadcasts.
- Lack of network segmentation.
- Difficulty in managing larger networks.
- Excessive Broadcast Traffic: This can lead to network congestion and performance degradation.
- Security Risks: Sensitive data can be easily intercepted by unauthorized devices.

✔ **Network With VLANs**

A **network with VLANs** allows you to divide a single physical network into multiple logical networks. Each VLAN is a separate broadcast domain, meaning that broadcast traffic in one VLAN will not reach devices in another VLAN.

Benefits:

- **Improved network performance**: Reduces unnecessary traffic by limiting broadcast traffic to specific VLANs.
- **Increased security**: Devices in different VLANs are isolated unless explicitly routed.
- **Simplified network management**: Easier to manage and organize large networks.
- **Cost-effectiveness**: No need for additional physical infrastructure; VLANs are configured in software.
- **Reduced Broadcast Traffic:** This improves network performance and reduces the risk of broadcast storms.

7. **Configuration of VLANs**

   Configuring VLANs is typically done on managed switches and involves the following steps:

1. **Identify VLAN Requirements:** Determine the number of VLANs needed and the devices that should belong to each VLAN.
2. **Create VLANs:** Configure VLANs on your network switches using the appropriate management interface (e.g., CLI, web interface).
3. **Assign Ports to VLANs:** Assign switch ports to the desired VLANs. This can be done using static port assignments or dynamic VLAN membership based on criteria like MAC addresses or IP addresses.
4. **Configure Trunking:** If VLANs need to span multiple switches, configure trunking between the switches to allow traffic from multiple VLANs to pass through.
5. **Verify VLAN Configuration:** Use appropriate tools (e.g., show commands on switches)

   To verify that VLANs are created correctly and ports are assigned to the intended VLANs.

8. **Verification of VLAN Configuration**

1. **Show VLAN Commands:** Use commands like show vlan or show interface to display information about VLANs and port assignments.
2. **Ping Tests:** Verify communication between devices in different VLANs to ensure proper isolation.
3. **Broadcast Storm Detection:** Monitor network traffic for signs of excessive broadcast activity, which could indicate a VLAN configuration issue.

Example VLAN Configuration (Cisco Switches):

```
Switch# configure terminal
Switch(config)# vlan 10  # Create VLAN with ID 10
Switch(config-vlan)# name Sales  # Name VLAN
Switch(config-vlan)# exit

Switch(config)# interface fastEthernet 0/1  # Select interface
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10  # Assign port to VLAN 10
Switch(config-if)# exit
```

For trunk port configuration:

```
Switch(config)# interface fastEthernet 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20  # Allow VLAN 10 and 20 on the trunk
Switch(config-if)# exit
```

Practical Activity 2.1.2: Configuring and verifying VLANs.

Tasks:

1: Refer to the key reading 2.1.2 and perform the following task:
You are asked to Configure VLANs, verify their setup, and ensure effective network segmentation.

2: Present the steps of configuring and Verifying VLANs.
3: Configure and verify VLNs.
4: Ask if any clarification.
5: For more clarifications, read the key readings 2.1.2.
6: Perform the activity in the application of learning 2.1.

Key readings 2.1.2. Configuring and verifying VLANs.

Configuring VLANs involves the following steps:

- **Create VLANs:** VLANs are created on a switch using commands (e.g., vlan <ID> in Cisco IOS). Assign a unique VLAN ID (1-4094). Use commands like vlan 10 (on Cisco).

```
Switch#configure terminal
Enter configuration commands
Switch(config)#vlan 10
```

- **Assign Ports to VLANs:** Each switch port is assigned to a specific VLAN. Devices connected to that port will become part of the assigned VLAN. Use commands like switchport access vlan 10 for access ports.

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

- **Configura Trunk Ports:** For inter-switch communication and passing VLAN traffic across multiple switches, trunk ports are configured. Trunking uses protocols like **802.1Q** to tag VLAN traffic. Use switchport mode trunk command to allow multiple VLANs over a single link.

```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Verification of VLAN Configuration

- **Show VLAN Information:** Use commands like **show vlan brief** (Cisco IOS) to display a summary of VLANs configured on the switch.

```
SW2#show vlan brief
```

- **Check VLAN Membership:** Verify which ports are assigned to which VLANs using **show vlan** or similar commands.
- **Trunk Port Status:** Use **show interfaces trunk** to verify that trunking is working correctly between switches to lists all trunk ports and the VLANs they carry.
- **Ping/Connectivity Tests:** Test network connectivity across VLANs to ensure proper configuration.

  Example: Creating VLAN 20 for "HR":

```
enable
configure terminal
vlan 20
name HR
interface FastEthernet 0/2
switchport mode access
switchport access vlan 20
interface FastEthernet 0/24
switchport mode trunk
switchport trunk allowed vlan 20
end
write memory
show vlan brief
```

Points to Remember

- Server, Client, and Transparent modes help manage VLAN information across switches.
- VLANs in separate broadcast domains need inter-VLAN routing (usually performed by a Layer 3 switch or a router) to communicate with each other.
- VLAN Tagging: 802.1Q standard is the most used protocol for VLAN tagging, which appends a VLAN tag to Ethernet frames as they traverse a trunk link.
- You should select a tool that aligns with your specific task needs.
- You should follow the manufacturer's instructions carefully.
- You should stay updated with tool updates and patches.
- You should monitor tool health regularly and provide user training for effective utilization.

Application of learning 2.1.

VLANs are used to divide a large network into smaller logical segments to improve network performance, security, and management, that why the Tech Solutions Inc. is expanding its network by implementing VLANs for different departments (HR, Sales, IT, and Guest access) so that the users in different department can operate independently without interfering with

one another and the users within the same VLAN can communicate. You are asked to configure and verify VLANs.

Indicative content 2.2: Configuration of VTP.

Duration: 5 hrs

Theoretical Activity 2.1.2: Explanation of VTP Theories

Tasks:

1. Read carefully and answer the following questions:
    i. What is VTP in a network?
    ii. What are the benefits of using VTP?
    iii. Name different VTP modes.
    iv. What is VTP pruning, and why is it important?
2. Write answers on paper flipchart, blackboard or whiteboard.
3. Present the finding to the whole class.
4. Ask questions for clarification if needed.
5. Read the Key readings 2.2.1 in trainee manuals.

Key readings 2.2.1 Explanation of VTP Theories

1. VTP definition

The **VLAN Trunking Protocol (VTP)** is a Cisco proprietary protocol that simplifies the management of VLANs across a network. VTP allows switches to synchronize their VLAN information by sharing VLAN configurations through VTP messages over trunk links.

2. VTP Benefits

Centralized VLAN management: VTP reduces the need to manually configure VLANs on each switch.

Consistency across the network: All switches in a VTP domain share the same VLAN configuration, preventing VLAN misconfiguration.

Automatic updates: VLAN changes on one switch are automatically propagated to other switches in the VTP domain.

Reduced configuration errors: VTP minimizes human errors by managing VLANs from a single switch.

Reduced Configuration Time: Eliminates the need to manually configure VLANs on each switch.

Improved Scalability: Easily manages large-scale networks with many switches.

Enhanced Fault Tolerance: Automatically propagates VLAN changes to other switches in the VTP domain.

3.VTP Components

✓ **VTP Domain**

A logical grouping of switches that share VLAN information, Switches in the same VTP domain must have the same VTP domain name, A VTP domain is a group of switches that share VLAN information. All switches in the same domain exchange VLAN information.

✔ **VTP Advertisement**

VTP messages that are periodically sent by switches to propagate VLAN information, VTP advertisements contain information about VLANs, VTP mode, VTP domain name, and revision number, VTP messages (advertisements) are exchanged between switches to synchronize VLAN information. Advertisements include VLAN changes or new VLANs and are propagated across the network.

There are three types of VTP advertisements:

- **Summary Advertisements**: Sent every 5 minutes to inform neighboring switches about the current VTP version and configuration revision number.
- **Subset Advertisements**: Sent when there is a change in the VLAN configuration (additions, deletions, or changes).
- **Request Advertisements**: Sent by switches when they are rebooted or if they want updated VLAN information.

✔ **VTP Modes**

Server mode

Is the default mode on Cisco switches, allows the creation, modification, and deletion of VLANs, Propagates VLAN information to other switches in the domain.

- **Client mode**

  The switch receives VLAN information from a server and updates its local database, Cannot create, modify, or delete VLANs, Synchronizes its VLAN database from VTP servers.

- **Transparent Mode:**

  Does not participate in VTP advertisements, VLAN changes made on a transparent switch are local and not propagated to other switches, Forwards VTP advertisements to other switches but doesn't process them, The switch does not participate in VTP but can still carry VTP messages.

✓ **VTP Pruning**

A mechanism that prevents unnecessary VLAN information from being propagated to switches that do not need it.

Pruning reduces network traffic and improves performance. VTP Pruning optimizes bandwidth by restricting the distribution of VLAN traffic only to switches that require it. Without pruning, VLAN traffic is broadcasted to all switches, even those that do not need the traffic.

Configuration Example:

Switch# configure terminal

Switch(config)# vtp pruning

Switch(config)# exit

Benefits of VTP Pruning:

- Reduces unnecessary VLAN traffic.
- Improves network performance by limiting traffic to only where it's needed.

✔ **VTP Operations**

- **VTP Version:** Determines the features supported by VTP.
  VTP has three main versions:

- **VTP Version 1**: Basic VTP functionality.

- **VTP Version 2**: Adds support for Token Ring VLANs and enhancements for VTP consistency checks.
- **VTP Version 3**: Provides additional security, support for private VLANs, and improved version control.

Configuration Example:

Switch# configure terminal

Switch(config)# vtp version 2

Switch(config)# exit

- **Revision numbers:** track VLAN changes. Each time a VLAN is created, modified, or deleted, the revision number increases. Switches use the highest configuration revision number to synchronize VLAN information. **Configuration Revisions:** A number assigned to each VTP configuration change.
- **VTP Domain Name**
- **Domain name** specifies the VTP domain to which the switch belongs.
- All switches in a VTP domain must share the same domain name to exchange VLAN information.

Configuration Example:

Switch# configure terminal

Switch(config)# vtp domain <domain-name>

Switch(config)# exit

- **VTP Operating Mode:** Determines the role of the switch in VTP.

Switch# configure terminal

Switch(config)# vtp mode server

Switch(config)# exit

- **VTP Pruning Mode:** Controls whether the switch prunes unnecessary VLAN information.
- **VTP Traps Generation:** Configures the switch to generate SNMP traps for VTP events

- **SNMP Traps** can be generated when VTP changes occur, notifying network administrators of changes to VLANs.

  Configuration Example:

  Switch# configure terminal

  Switch(config)# snmp-server enable traps vtp

  Switch(config)# exit

Practical Activity 2.2.2: Configuring VTP

Task:

1: Refer to the key reading 2.2.2 and perform the following task:
You are asked to go to the computer lab in your school and configure a VTP server switch and client's switches. Ensure optimal bandwidth usage enabling VTP pruning, Enable VTP version 2, add a new client switch to the domain, and verify that all switches are properly synchronized to manage VLANs centrally on the VTP server and propagate them to all client switches.

2: Present the steps of configure and verify VTP.
3: Trainer ask trainees to configure and verify VTP.
4: Trainees start doing the work.
5: Ask if any clarification.
6: Trainee read the Key readings 2.2.2 in the trainee manuals.

Key readings 2.2.2 Configuring VTP

1. Configure VTP Server and Client Switches

VTP server and client switches form the foundation of VLAN management in a network using VLAN Trunking Protocol (VTP). Configurations made on a VTP server propagate across all client switches in the same VTP domain.

- **VTP Server Switches:** These switches are responsible for creating, deleting, and modifying VLANs. They also propagate this information to other switches.

- **VTP Client Switches:** These switches receive VLAN information from VTP servers but cannot modify VLAN configurations.

2. Managing VLAN on VTP Server and Client

- **On VTP Server:** VLANs are created, deleted, and modified using commands like vlan <ID>. Once the changes are made on the server, they are automatically propagated to all VTP clients.
- **On VTP Client:** The VLAN configuration cannot be altered. VLANs on the client switch are inherited from the server and applied without modification.

3. Enabling VTP Version

By default, switches run VTP version 1. However, for enhanced features, version 2 or version 3 might be used. To enable a specific VTP version:

Switch(config)# vtp version <1 | 2 | 3>

4. Enabling VTP Pruning

VTP pruning limits VLAN broadcast traffic to trunk links that need it, thereby optimizing bandwidth usage. To enable pruning:

Switch(config)# vtp pruning

Pruning ensures that VLAN traffic is only forwarded over trunks that have devices in the specified VLAN.

5. Adding a VTP Client Switch to a VTP Domain

To add a client switch to an existing VTP domain:

- Set the **VTP mode** to client:
  Switch(config)# vtp mode client

  Assign the VTP domain name to match the existing VTP domain:

  Switch(config)# vtp domain <domain-name>

  Optionally, configure VTP password (if VTP authentication is in use):

  Switch(config)# vtp password <password>

  The client switch will receive VLAN information from the VTP server after this configuration.

6. Verify VTP Configurations

To ensure VTP is properly configured and operational, use the following commands:

Show VTP Status: Displays the current VTP configuration, including the domain name, version, mode, pruning status, and configuration revision number.

Switch# show vtp status

Show VTP Password: Displays the current VTP password, if configured.

Switch# show vtp password

7. Configuration of Switchport Interface

Access Mode

In access mode, the switchport is assigned to a single VLAN, typically for end devices like PCs or printers:

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan <VLAN-ID>

This ensures that the port is part of a specific VLAN.

Trunk Mode

In trunk mode, the switchport carries multiple VLANs, usually between switches or between switches and routers. Trunking uses tagging protocols like 802.1Q to differentiate VLAN traffic:

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

You can also restrict which VLANs can be passed through the trunk:

Switch(config-if)# switchport trunk allowed vlan <vlan-list>

8. Verifying Switchport Interfaces

To verify the switchport mode and its configuration, use the following commands:

Show Switchport: Displays detailed information about the switchport's mode (access/trunk), VLAN assignment, and operational status:

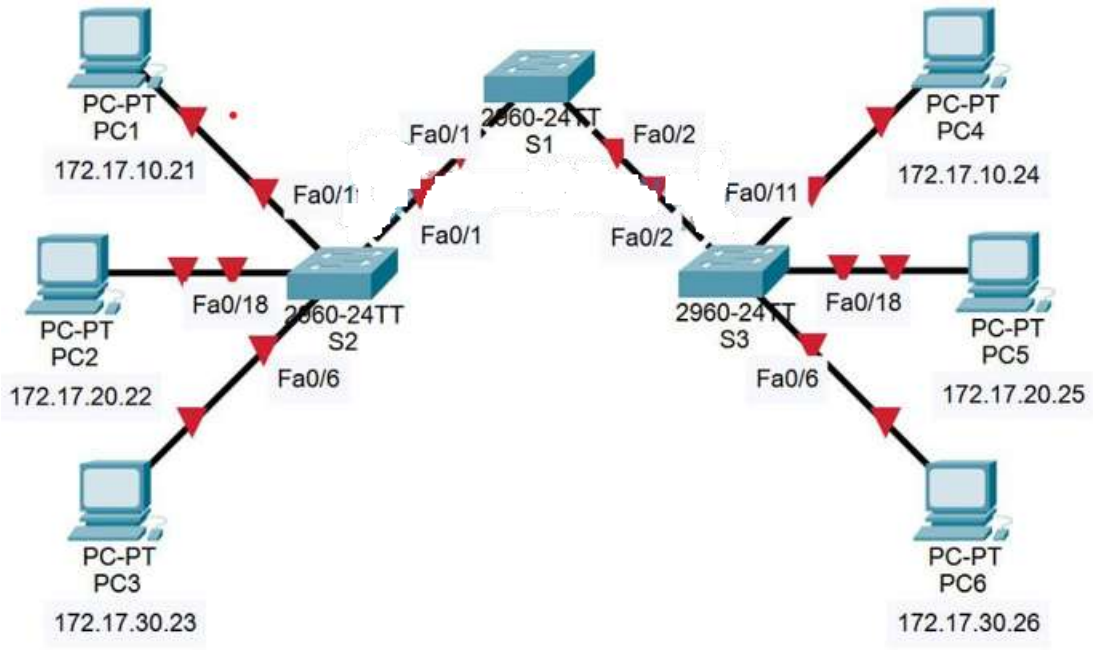
Switch# show interfaces switchport

Show VLAN Brief: Displays which VLANs are assigned to specific ports:

Switch# show vlan brief

Example;

In the diagram below, a trunk link is configured between switch S1, (VTP Server), S2, and S3 – VTP client.



Step 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname S1

S1(config)#enable secret class

S1(config)#no ip domain-lookup

S1(config)#line console 0

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#line vty 0 15

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#end

%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Step2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses and default gateways indicated in the addressing table.

Step 3: Configure VTP and Security on the Switches

- ✓ **Enable the access ports on S2 and S3.**
  Configure the user ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

S2(config)#interface fa0/6

S2(config-if)#switchport mode access

S2(config-if)#no shutdown

S2(config-if)#interface fa0/11

S2(config-if)#switchport mode access

S2(config-if)#no shutdown

S2(config-if)#interface fa0/18

S2(config-if)#switchport mode access

S2(config-if)#no shutdown

- ✓ **Check the current VTP settings on the three switches.**
  Use the **show vtp status** command to determine the VTP operating mode for all three switches.
  S1#**show vtp status**

  VTP Version : 2
  Configuration Revision : 0
  Maximum VLANs supported locally : 64
  Number of existing VLANs : 5
  VTP Operating Mode : Server
  VTP Domain Name :
  VTP Pruning Mode : Disabled
  VTP V2 Mode : Disabled
  VTP Traps Generation : Disabled
  MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
  Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
  Local updater ID is 0.0.0.0 (no valid interface found)

  S2#**show vtp status**

  VTP Version : 2
  Configuration Revision : 0
  Maximum VLANs supported locally : 64
  Number of existing VLANs : 5
  VTP Operating Mode : Server
  VTP Domain Name :
  VTP Pruning Mode : Disabled
  VTP V2 Mode : Disabled
  VTP Traps Generation : Disabled
  MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
  Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
  Local updater ID is 0.0.0.0 (no valid interface found)

S3#**show vtp status**

VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 64
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Step 3. Configure the operating mode, domain name, and VTP password on all three switches.

Set the VTP domain name to **Lab4** and the VTP password to **cisco** on all three switches. Configure S1 in server mode, S2 in client mode, and S3 in transparent mode.

S1(config)#vtp mode server

Device mode already VTP SERVER.

S1(config)#vtp domain Lab4

Changing VTP domain name from NULL to Lab4

S1(config)#vtp password cisco

Setting device VLAN database password to cisco

S1(config)#end

S2(config)#vtp mode client

Setting device to VTP CLIENT mode

S2(config)#vtp domain Lab4

Changing VTP domain name from NULL to Lab4

S2(config)#vtp password cisco

Setting device VLAN database password to cisco

S2(config)#end

S3(config)#vtp mode transparent

Setting device to VTP TRANSPARENT mode.

S3(config)#vtp domain Lab4

Changing VTP domain name from NULL to Lab4

S3(config)#vtp password cisco

Setting device VLAN database password to cisco

S3(config)#end

Step 4. Configure trunking and the native VLAN for the trunking ports on all three switches.

On all switches, configure trunking and the native VLAN for FastEthernet interfaces 0/1-5. Only commands for fa0/1 on each switch are shown below.

S1(config)#interface fa0/1

S1(config-if)#switchport mode trunk

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

S1(config-if)#no shutdown

S1(config-if)#interface fa0/2

S1(config-if)#switchport mode trunk

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

S1(config-if)#no shutdown

S1(config-if)#end

S2(config)#interface fa0/1

S2(config-if)#switchport mode trunk

S2(config-if)#switchport trunk native vlan 99

S2(config-if)#no shutdown

S2(config-if)#end

S3(config)#interface fa0/2

S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 99

S3(config-if)#no shutdown

S3(config-if)#end

Step 5. Configure port security on the S2 and S3 access layer switches.

Configure ports fa0/6, fa0/11, and fa0/18 so that they allow only a single host and learn the MAC address of the host dynamically.

S2(config)#interface fa0/6

S2(config-if)#switchport port-security

S2(config-if)#switchport port-security maximum 1

S2(config-if)#switchport port-security mac-address sticky

S2(config-if)#interface fa0/11

S2(config-if)#switchport port-security

S2(config-if)#switchport port-security maximum 1

S2(config-if)#switchport port-security mac-address sticky

S2(config-if)#interface fa0/18

S2(config-if)#switchport port-security

S2(config-if)#switchport port-security maximum 1

S2(config-if)#switchport port-security mac-address sticky

S2(config-if)#end

S3(config)#interface fa0/6

S3(config-if)#switchport port-security

S3(config-if)#switchport port-security maximum 1

S3(config-if)#switchport port-security mac-address sticky

S3(config-if)#interface fa0/11

S3(config-if)#switchport port-security

S3(config-if)#switchport port-security maximum 1

S3(config-if)#switchport port-security mac-address sticky

S3(config-if)#interface fa0/18

S3(config-if)#switchport port-security

S3(config-if)#switchport port-security maximum 1

S3(config-if)#switchport port-security mac-address sticky

S3(config-if)#end

Step 6. Configure VLANs on the VTP server.

There are four VLANS required in this lab:

- VLAN 99 (management)
- VLAN 10 (faculty/staff)
- VLAN 20 (students)
- VLAN 30 (guest)

Configure these on the VTP server.

S1(config)#vlan 99

S1(config-vlan)#name management

S1(config-vlan)#exit

S1(config)#vlan 10

S1(config-vlan)#name faculty/staff

S1(config-vlan)#exit

S1(config)#vlan 20

S1(config-vlan)#name students

S1(config-vlan)#exit

S1(config)#vlan 30

S1(config-vlan)#name guest

S1(config-vlan)#exit

Verify that the VLANs have been created on S1 with the show vlan brief command.

Step 7. Check if the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all the switches.
S2#show vlan brief

VLAN Name Status Ports

1 default activeFa0/1, Fa0/2, Fa0/4, Fa0/5

Fa0/6, Fa0/7, Fa0/8, Fa0/9

Fa0/10, Fa0/11, Fa0/12,Fa0/13

Fa0/14, Fa0/15, Fa0/16,Fa0/17

Fa0/18, Fa0/19, Fa0/20,Fa0/21

Fa0/22, Fa0/23, Fa0/24, Gi0/1

Gi0/2

10 faculty/staff active

20 students active

30 guest active

99 management active

S3#show vlan brief

VLAN Name Status Ports

1 default active Fa0/1, Fa0/3, Fa0/4, Fa0/5

Fa0/6, Fa0/7, Fa0/8, Fa0/9

Fa0/10, Fa0/11, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/18, Fa0/19, Fa0/20, Fa0/21

Fa0/22, Fa0/23, Fa0/24, Gig1/1

Gig1/2

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

Configure the management interface address on all three switches.

S1(config)#interface vlan 99

S1(config-if)#ip address 172.17.99.11 255.255.255.0

S1(config-if)#no shutdown

S2(config)#interface vlan 99

S2(config-if)#ip address 172.17.99.12 255.255.255.0

S2(config-if)#no shutdown

S3(config)#interface vlan 99

S3(config-if)#ip address 172.17.99.13 255.255.255.0

S3(config-if)#no shutdown

Step 11. Assign switch ports to VLANs.

S3(config)#interface fa0/6

S3(config-if-range)#switchport access vlan 30

S3(config-if-range)#interface fa0/11

S3(config-if-range)#switchport access vlan 10

S3(config-if-range)#interface fa0/18

S3(config-if-range)#switchport access vlan 20

S3(config-if-range)#end

S3#copy running-config startup-config

Destination filename [startup-config]? [enter]

Building configuration...

[OK]

S3#

Points to Remember

- VTP is used to manage and propagate VLAN information across multiple switches in a network.
- Functionality: VTP distributes and synchronizes VLAN configuration (like VLAN names, numbers, and associated information) across all connected switches in the same VTP domain.
- The VTM Modes are Server Mode, Client Mode and Transparent Mode.
- Common Use of VTP Simplifies large networks where VLANs are used on multiple switches, allowing changes to be made centrally and propagated automatically.
- Set the switch mode to VTP server.
- Enable VTP version 2.
- Configure VTP Domain.
- Enable VTP pruning to optimize bandwidth.
- Verify synchronization with the command.

Application of learning 2.2.

Imagine you are an IT network administrator tasked with configuring a VTP (VLAN Trunking Protocol) network for your company, the task comprises to configure a VTP server switch, client switches, add client switches to the domain, and ensure optimal bandwidth usage using VTP pruning. The goal is to manage VLANs centrally and ensure all switches in the network have the same VLAN information.

Indicative content 2.3: Configuration of Switch Port Interface.

Duration: 5 hrs

Practical Activity 2.3.1: Configuring Switch port interface.

Task:

1: Refer to the key reading 2.3.1 and perform the following task:
You are asked to go to the computer lab in your school and configure to create VLANs and assign interfaces, configure trunk and access ports, Verify the configuration, and Test connectivity between devices in different VLANs. The network should be segmented into two VLAN which are Marketing and Sales**.** Each department has its own VLAN for better network management and security. Marketing for workstations and sales for the server and printer.

2: Presents the steps of configure and verify Switch port interface.
3: configure and verify Switch port interface.
4: Trainees start doing the work.
5: Ask if any clarification
6: Trainee read the Key readings 2.3.1 in the trainee manuals.

Key readings 2.3.1: Configuring Switch port interface

1. Access Mode Configuration

Configuration Steps:

1. **Enter global configuration mode**.
2. **Select the interface you want to configure**.
3. **Set the interface to access mode**.
4. **Assign the VLAN**.

Example Configuration:

Switch# configure terminal

Switch(config)# interface FastEthernet0/1 # Select the interface

Switch(config-if)# switchport mode access # Set the port to access mode

Switch(config-if)# switchport access vlan <VLAN-ID> # Assign the VLAN ID

Switch(config-if)# exit

Switch(config)# exit

2. Trunk Mode Configuration

Configuration Steps:

1. Enter global configuration mode.
2. Select the interface you want to configure.
3. Set the interface to trunk mode.
4. Define the allowed VLANs (optional).

Example Configuration:

Switch# configure terminal

Switch(config)# interface FastEthernet0/2 # Select the interface

Switch(config-if)# switchport mode trunk # Set the port to trunk mode

Switch(config-if)# switchport trunk allowed vlan <VLAN-ID1>,<VLAN-ID2> # Specify allowed VLANs

Switch(config-if)# exit

Switch(config)# exit

3. Verifying Switch Port Interfaces

After configuring switch port interfaces, it's essential to verify that the configurations are correct and functioning as expected.

Verification Commands: Ensures proper configuration and operation of switch ports.

1. **Show Interface Status**: This command provides a summary of the interface status, including whether it's in access or trunk mode.

Switch# show interfaces status

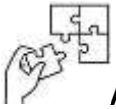
2. **show interfaces switchport**
   This command displays detailed information about the switch port configuration on a Cisco switch. It provides insights into how the interface is set up regarding VLANs and trunking.

3. **show running-config interface [interface ID]**
   This command displays the current configuration of a specific interface on a device. You would replace [interface ID] with the specific interface you want to inspect (e.g., FastEthernet0/1, GigabitEthernet1/0/1.

4. **Show Interfaces Trunk** This command specifically lists all trunk interfaces and their configurations. Switch# show interfaces trunk

Points to Remember

- Create VLANs for Marketing and Sales.
- Assign interfaces to VLANs.
- Configure trunk ports for VLAN communication.
- Test connectivity between VLANs using ping.



Application of learning 2.3.

You are a network administrator at a company called Tech Solutions. The company has two departments: Marketing and Sales. Each department has its own VLAN for better network management and security. The company is expanding and needs to configure its network switches to support this growth. Your tasks include configuring the switch ports for the two departments, establishing trunk links between switches, and verifying the configurations.

Indicative content 2.4: Configure Inter VLAN Routing.

Duration: 3 hrs

Theoretical Activity 2.4.1: Description of inter-VLAN routing

Task:

1: Read carefully and answer the following questions:

i. What is inter-VLAN routing?

ii. What is a router sub-interface?

iii. What is the advantage of using sub-interfaces on a router?

iv. What are the main types of inter-VLAN routing?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 2.4.1 in trainee manuals.

Key readings 2.4.1 Description of inter-VLAN routing

- **Introduction inter-VLAN routing**

Definition: Inter-VLAN routing is the process of forwarding traffic between different VLANs (Virtual Local Area Networks) using a router. It enables communication among devices in different VLANs.

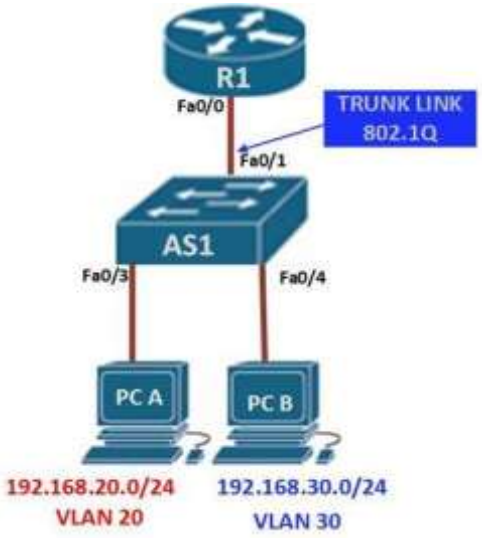
Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network.

Types of Inter-VLAN Routing

➢ **Router-on-stick inter-VLAN routing**

Router-on-a-stick, the router is connected to the switch using a single interface. The switchport connecting to the router is configured as a trunk link.

- ❖ The single interface on the router is then configured with multiple IP addresses that correspond to the VLANs on the switch.
- ❖ Router interface is divided into subinterfaces, each assigned to to a specific VLAN.
- ❖ Traffic between router and switch is tagged with VLAN IDs using 802.1Q.
- ❖ Require fewer physical router interfaces.



Router Sub-Interfaces

Definition: A sub-interface is a virtual interface created on a physical interface of a router.

Functionality: Each sub-interface can handle traffic for a different VLAN by encapsulating the traffic with the appropriate VLAN tags (IEEE 802.1Q).

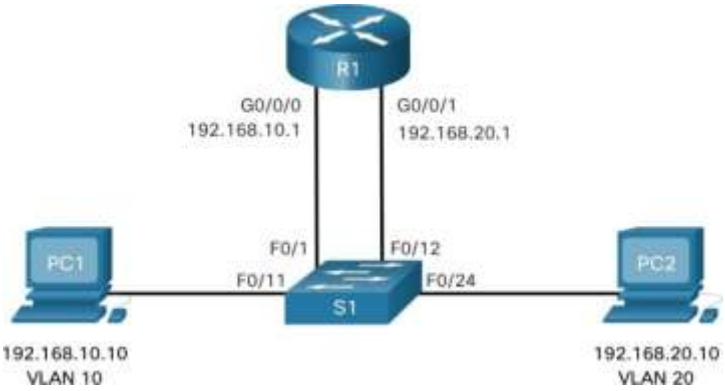
Router Interface vs. Sub-Interface Comparison

Feature	Router Interface	Sub-Interface
Physical vs Virtual	Physical interface	Virtual interface
VLAN Handling	One VLAN per interface	Multiple VLANs per interface
Resource Utilization	More ports required	Fewer physical interfaces needed
Complexity	Simpler configuration	More complex configuration

- **Traditional inter-VLAN routing**

Traditional inter-VLAN routing involves using separate physical interfaces on a router for each VLAN.

- With each VLAN having its own dedicated connection to the router.
- Each VLAN is connected to a separate router interface via individual cables.
- Doesn't rely on 802.1Q tagging since each VLAN has its own physical connection
- Require more router interfaces

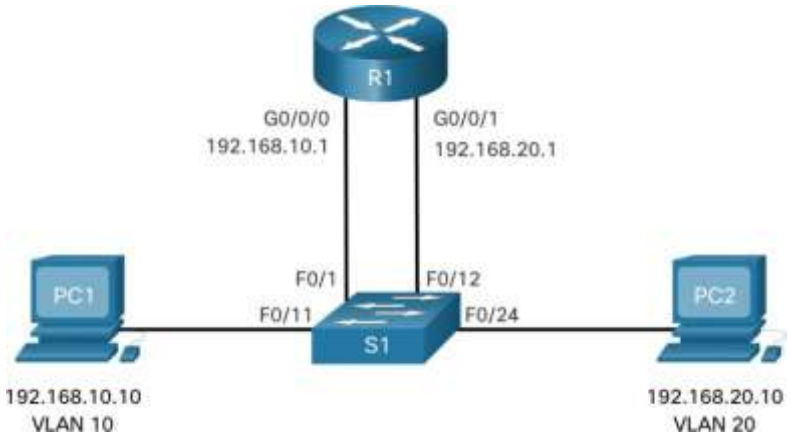


- **Router sub-interfaces**

A sub-interface is a virtual interface created by dividing one physical interface into multiple logical interfaces.

- A sub-interface in a Cisco Router uses the parent physical interface for sending and receiving data.
- A Sub-interface can be configured just like a physical interface.
- R1(config)#interface fastEthernet 0/0.?

- **Configure traditional inter VLAN Routing**



The IP addressing in use as shown in figure.

Fa0/1 port is assigned to VLAN 10 and is connected to the R1 G0/0/0 interface.

Fa0/11 port is assigned to VLAN 10 and is connected to PC1.

Fa0/12 port is assigned to VLAN 20 and is connected to the R1 G0/0/1 interface.

Fa0/24 port is assigned to VLAN 20 and is connected to PC2.

Configuration

Step 1: Create VLANs (VLANs 10 and 20) on the switch

Description	Command
Enter global configuration mode	Switch# conf t
Create VLAN 10	Switch(config)# vlan 10
Give a name to VLAN 10	Switch(config-vlan)# name Admin-dept
Create VLAN 20	Switch(config-vlan)# vlan 20
Give a name to VLAN 20	Switch(config-vlan)# name Finance-dept
Exit the VLAN config. Mode	Switch(config-vlan)# exit
Check if the VLANs were created	Switch # show vlan brief

Step 2: Assign the VLANs to switch port

Description	Command
Enter global configuration mode	Switch# conf t
Enter interface config. mode for fa0/2	Switch(config)# interface fa0/11
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 10 to interface fa0/2	Switch(config-if)#switchport access vlan 10

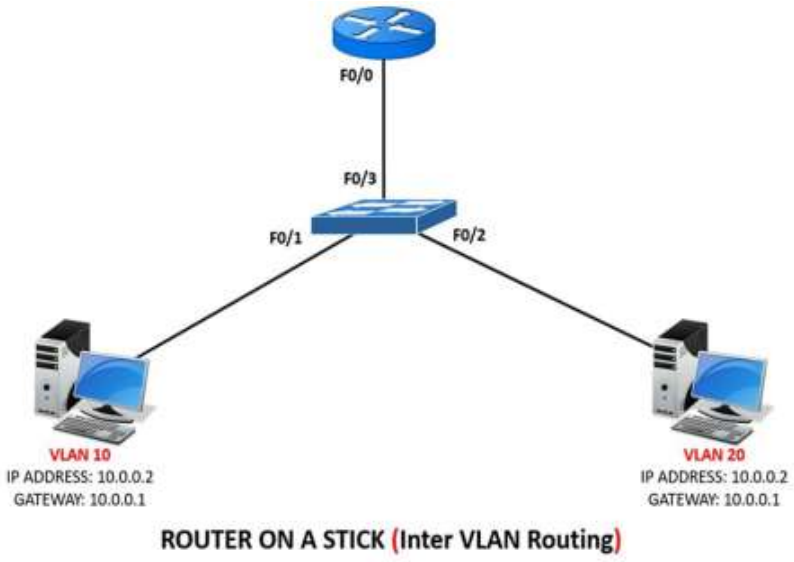
Enter interface configuration for fa0/3	Switch(config)# interface fa0/24
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 20 to interface fa0/3	Switch(config-if)#switchport access vlan 20
Exit the interface	Switch(config-if)# exit

Step 3: Configure the IP addresses on the router

Description	**Command**
Enter global configuration mode	Router# conf t
Enter interface config. mode for fa0/0	Router(config)# interface G0/0/0
Configure IP address and subnet mask	Router(config-if)#ip address 192.168.10.1 255.255.255.0
Activate the interface	Router(config-if)#no shutdown
Exit the interface	Router(config-if)#exit
Enter interface config. mode for fa0/1	Router(config)# interface G0/0/1
Configure IP address and subnet mask	Router(config-if)# ip address 192.168.20.1 255.255.255.0
Activate the interface	Router(config-if)#no shutdown
Exit the interface	Router(config-if)# exit

Save configuration	Router# copy running-config startup-config

- **Configure router-on-stick inter VLAN Routing**



Configuration:

Step 1: create VLANs

Switch>en **(enable privilege mode)**

Switch#conf t **(entering configuration mode)**

Switch(config)#vlan 10 **(Creating VLAN 10)**

Switch(config-vlan)#name production **(Assigning name to VLAN)**

Switch(config-vlan)#vlan 20 **(Creating VLAN 20)**

Switch(config-vlan)#name sales **(Assigning name to VLAN)**

Switch(config-vlan)#exit

Step 2: Assign port to VLANs and configure trunk

Switch(config)#int f0/1 **(Selecting port 1 of the switch)**

Switch(config-if)#switchport access vlan 10 **(Assigning port 1 to VLAN 10)**

Switch(config-if)#int f0/2 **(Selecting port 2 of the switch)**

Switch(config-if)#switchport access vlan 20 **(Assigning port 2 to VLAN 20)**

Switch(config-if)#int f0/3 **(Selecting port 3 of the switch)**

Switch(config-if)#switchport mode trunk **(Configuring port 3 as trunk)**

Switch(config-if)#exit

Switch(config)#do copy run start **(Save switch configuration)**

Switch(config)#

Step 3: Configure router on a stick by configuring sub interface.

Router>en **(enable privilege mode)**

Router#conf t **(entering configuration mode)**

Router(config)#int f0/0.1 **(Creating and selecting sub-interface port "f0/0.1" on f0/0)**

Router(config-subif)#encapsulation dot1q 10 **(Assigning the sub-interface port f0/0.1 to VLAN 10. Here, 10 is the VLAN number)**

Router(config-subif)#ip address 10.0.0.1 255.0.0.0 **(Assigning IP Address to the sub-interface port f0/0.1)**

Router(config-subif)#exit

Router(config)#int f0/0.2 **(Creating and selecting sub-interface port "f0/0.2" on f0/0)**

Router(config-subif)#encapsulation dot1q 20 **(Assigning the sub-interface port f0/0.2 to VLAN 20. Here, 20 is the VLAN number)**

Router(config-subif)#ip address 20.0.0.1 255.0.0.0 **(Assigning IP Address to the sub-interface port f0/0.2)**

Router(config-subif)#exit

Router(config)#exit

Router#

Router#conf t **(Entering configuration mode)**

Router(config)#int f0/0 **(Selecting f0/0 port)**

Router(config-if)#no shutdown **(Enabling the fast ethernet port f0/0)**

Router(config-if)#

- **Layer 3 switch inter-VLAN Routing (SVI)**

LAYER 3 SWITCHING It is referred to as a multilayer switch -- combines the duties of a switch and a router

Benefits of Layer 3 switch:

- Reduces broadcast domains, increasing network performance and efficiency.
- Multilayer topologies based upon inter-VLAN routing are much more scalable
- Allows for centralized security access control between each VLAN.
- Increases manageability.

Comparison to the Router

The major difference between the packet switching operation of a router and a Layer 3 switch is the physical implementation.

In general-purpose routers, packet switching takes place using microprocessor-based engines, whereas

- Layer 3 switch performs this using application specific integrated circuit (ASIC) hardware.

  Multilayer switches support configuring a VLAN as a logical routed interface, known as a **Switched Virtual Interface (SVI)**. The SVI is referenced by the VLAN number:

  Switch(config)# interface vlan 101

  Switch(config-if)# ip address 10.101.101.1 255.255.255.0

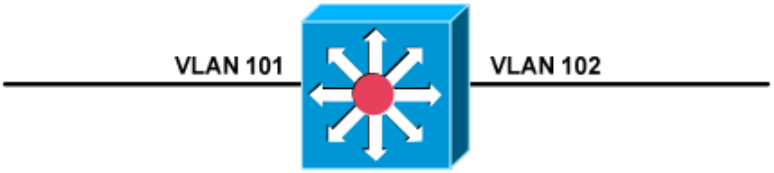
  Switch(config-if)# no shut

  SVIs are the most common method of configuring inter-VLAN routing.

  Note: The logical VLAN interface will not become online unless:

- The VLAN is created.
- At least one port is active in the VLAN.

➢ **Configuring Inter-VLAN Routing Using SVIs**



Configuring inter-VLAN routing using SVIs is very simple. First, the VLANs must be created:

SwitchA(config)# vlan 101

SwitchA(config-vlan)# name VLAN101

SwitchA(config)# vlan 102

SwitchA(config-vlan)# name VLAN102

Layer-3 forwarding must then be enabled globally on the multilayer switch:

SwitchA(config)# ip routing

Finally, each VLAN SVI must be assigned an IP address:

SwitchA(config)# interface vlan 101

SwitchA(config-if)# ip address 10.101.101.1 255.255.255.0

SwitchA(config-if)# no shut

SwitchA(config)# interface vlan 102

SwitchA(config-if)# ip address 10.102.102.1 255.255.255.0

SwitchA(config-if)# no shut

The IP address on each SVI represents the gateway for hosts on each VLAN. The two networks will be added to the routing table as directly connected routes.

Remember: an SVI requires at least one port to be active in the VLAN:

SwitchA(config)# interface gi1/14

SwitchA(config-if)# switchport mode access

SwitchA(config-if)# switchport access vlan 101

SwitchA(config-if)# no shut

SwitchA(config)# interface gi1/15

SwitchA(config-if)# switchport mode access

SwitchA(config-if)# switchport access vlan 102

SwitchA(config-if)# no shut

- **Verifying inter VLAN Routing**

Verifying and troubleshooting inter-VLAN routing issues In verifying inter-VLAN routing, the commands mostly used are:

Show run

Show ip interface brief

Show interface

Practical Activity 2.4.2: Configuring inter-VLAN routing

Task:

1: Refer to the key reading 2.4.2 and perform the following task:

You are asked go to the computer lab of your school to Configure and verify Inter-VLAN Routing using Router-on-a-Stick and a Layer 3 switch in a simulated network environment, ensure that devices in different VLANs can communicate effectively.

Network Requirements:

1. **VLANs:**
   - ✓ **VLAN 10**: Sales (IP range: 192.168.10.0/24)
   - ✓ **VLAN 20**: Marketing (IP range: 192.168.20.0/24)
2. **PC Assignments:**
   - ✓ **PC1 (Sales)**: IP: 192.168.10.2
   - ✓ **PC2 (Sales)**: IP: 192.168.10.3
   - ✓ **PC3 (Marketing)**: IP: 192.168.20.2
   - ✓ **PC4 (Marketing)**: IP: 192.168.20.3
3. **Devices:**
   - ✓ 1 Layer 3 Switch
   - ✓ 1 Router
   - ✓ 2 Access Switches
   - ✓ 4 PCs

2: Presents the steps to Configure and verify Inter-VLAN Routing

3: Configure and verify Inter-VLAN Routing

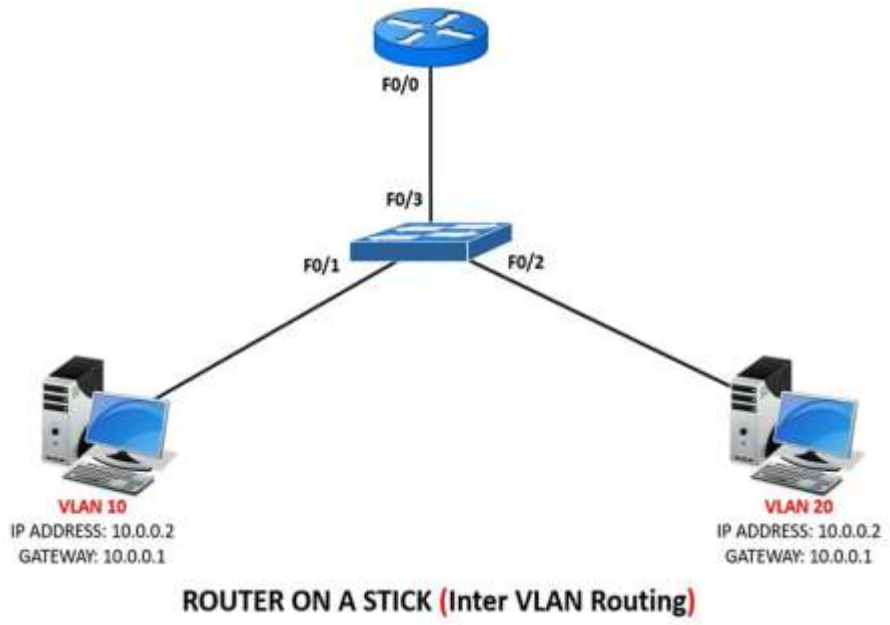
4: Ask if any clarification

5: For more clarifications, read the key readings 2.4.2

6: Perform the activity in the application of learning 2.4.

Key readings 2.4.2. Configure inter VLAN routing

- **Configure router-on-stick inter VLAN Routing**



ROUTER ON A STICK (Inter VLAN Routing)

Configuration:

Step 1: create VLANs

Switch>en **(enable privilege mode)**

Switch#conf t **(entering configuration mode)**

Switch(config)#vlan 10 **(Creating VLAN 10)**

Switch(config-vlan)#name production **(Assigning name to VLAN)**

Switch(config-vlan)#vlan 20 **(Creating VLAN 20)**

Switch(config-vlan)#name sales **(Assigning name to VLAN)**

Switch(config-vlan)#exit

Step 2: Assign port to VLANs and configure trunk

Switch(config)#int f0/1 **(Selecting port 1 of the switch)**

Switch(config-if)#switchport access vlan 10 **(Assigning port 1 to VLAN 10)**

Switch(config-if)#int f0/2 **(Selecting port 2 of the switch)**

Switch(config-if)#switchport access vlan 20 **(Assigning port 2 to VLAN 20)**

Switch(config-if)#int f0/3 **(Selecting port 3 of the switch)**

Switch(config-if)#switchport mode trunk **(Configuring port 3 as trunk)**

Switch(config-if)#exit

Switch(config)#do copy run start **(Save switch configuration)**

Switch(config)#

Step 3: Configure router on a stick by configuring sub interface.

Router>en **(enable privilege mode)**

Router#conf t **(entering configuration mode)**

Router(config)#int f0/0.1 **(Creating and selecting sub-interface port "f0/0.1" on f0/0)**

Router(config-subif)#encapsulation dot1q 10 **(Assigning the sub-interface port f0/0.1 to VLAN 10. Here, 10 is the VLAN number)**

Router(config-subif)#ip address 10.0.0.1 255.0.0.0 **(Assigning IP Address to the sub-interface port f0/0.1)**

Router(config-subif)#exit

Router(config)#int f0/0.2 **(Creating and selecting sub-interface port "f0/0.2" on f0/0)**

Router(config-subif)#encapsulation dot1q 20 **(Assigning the sub-interface port f0/0.2 to VLAN 20. Here, 20 is the VLAN number)**

Router(config-subif)#ip address 20.0.0.1 255.0.0.0 **(Assigning IP Address to the sub-interface port f0/0.2)**

Router(config-subif)#exit

Router(config)#exit

Router#

Router#conf t **(Entering configuration mode)**

Router(config)#int f0/0 **(Selecting f0/0 port)**

Router(config-if)#no shutdown **(Enabling the fast ethernet port f0/0)**

Router(config-if)#

Layer 3 switch inter-VLAN Routing (SVI)

LAYER 3 SWITCHING It is referred to as a multilayer switch -- combines the duties of a switch and a router

Benefits of Layer 3 switch:

- Reduces broadcast domains, increasing network performance and efficiency.
- Multilayer topologies based upon inter-VLAN routing are much more scalable

- Allows for centralized security access control between each VLAN.
- Increases manageability.

Comparison to the Router

The major difference between the packet switching operation of a router and a Layer 3 switch is the physical implementation.

- In general-purpose routers, packet switching takes place using microprocessor-based engines, whereas
- Layer 3 switch performs this using application specific integrated circuit (ASIC) hardware.

Multilayer switches support configuring a VLAN as a logical routed interface, known as a **Switched Virtual Interface (SVI)**. The SVI is referenced by the VLAN number:

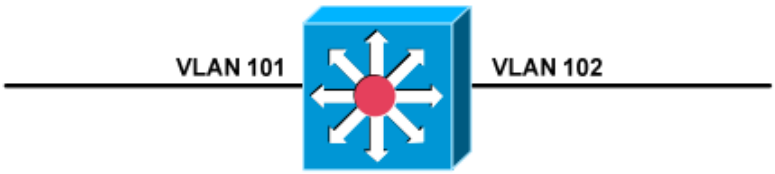
```
Switch(config)# interface vlan 101
Switch(config-if)# ip address 10.101.101.1 255.255.255.0
Switch(config-if)# no shut
```

SVIs are the most common method of configuring inter-VLAN routing.

Note: The logical VLAN interface will not become online unless:

- The VLAN is created.
- At least one port is active in the VLAN.

Configuring Inter-VLAN Routing Using SVIs



Configuring inter-VLAN routing using SVIs is very simple. First, the VLANs must be created:

SwitchA(config)# vlan 101

SwitchA(config-vlan)# name VLAN101

SwitchA(config)# vlan 102

SwitchA(config-vlan)# name VLAN102

Layer-3 forwarding must then be enabled globally on the multilayer switch:

SwitchA(config)# ip routing

Finally, each VLAN SVI must be assigned an IP address:

SwitchA(config)# interface vlan 101

SwitchA(config-if)# ip address 10.101.101.1 255.255.255.0

SwitchA(config-if)# no shut

SwitchA(config)# interface vlan 102

SwitchA(config-if)# ip address 10.102.102.1 255.255.255.0

SwitchA(config-if)# no shut

The IP address on each SVI represents the gateway for hosts on each VLAN. The two networks will be added to the routing table as directly connected routes.

Remember: an SVI requires at least one port to be active in the VLAN:

SwitchA(config)# interface gi1/14

SwitchA(config-if)# switchport mode access

SwitchA(config-if)# switchport access vlan 101

SwitchA(config-if)# no shut

SwitchA(config)# interface gi1/15

SwitchA(config-if)# switchport mode access

SwitchA(config-if)# switchport access vlan 102

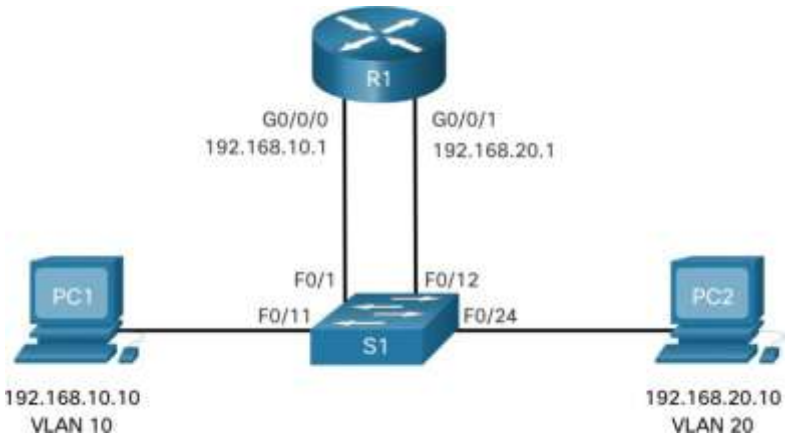
SwitchA(config-if)# no shut

Verifying inter VLAN Routing

Verifying and troubleshooting inter-VLAN routing issues In verifying inter-VLAN routing, the commands mostly used are:

- Show run
- Show ip interface brief
- Show interface

Configure traditional inter VLAN Routing



The IP addressing in use as shown in figure.

Fa0/1 port is assigned to VLAN 10 and is connected to the R1 G0/0/0 interface.

Fa0/11 port is assigned to VLAN 10 and is connected to PC1.

Fa0/12 port is assigned to VLAN 20 and is connected to the R1 G0/0/1 interface.

Fa0/24 port is assigned to VLAN 20 and is connected to PC2.

Configuration

Step 1: Create VLANs (VLANs 10 and 20) on the switch

Description	**Command**
Enter global configuration mode	Switch# conf t
Create VLAN 10	Switch(config)# vlan 10
Give a name to VLAN 10	Switch(config-vlan)# name Admin-dept
Create VLAN 20	Switch(config-vlan)# vlan 20
Give a name to VLAN 20	Switch(config-vlan)# name Finance-dept
Exit the VLAN config. mode	Switch(config-vlan)# exit
Check if the VLANs were created	Switch # show vlan brief

Step 2: Assign the VLANs to switch port

Description	**Command**
Enter global configuration mode	Switch# conf t

Enter interface config. mode for fa0/2	Switch(config)# interface fa0/11
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 10 to interface fa0/2	Switch(config-if)#switchport access vlan 10
Enter interface configuration for fa0/3	Switch(config)# interface fa0/24
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 20 to interface fa0/3	Switch(config-if)#switchport access vlan 20
Exit the interface	Switch(config-if)# exit

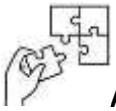
Step 3: Configure the IP addresses on the router

Description	**Command**
Enter global configuration mode	Router# conf t
Enter interface config. mode for fa0/0	Router(config)# interface G0/0/0
Configure IP address and subnet mask	Router(config-if)#ip address 192.168.10.1 255.255.255.0
Activate the interface	Router(config-if)#no shutdown
Exit the interface	Router(config-if)#exit

Enter interface config. mode for fa0/1	Router(config)# interface G0/0/1
Configure IP address and subnet mask	Router(config-if)# ip address 192.168.20.1 255.255.255.0
Activate the interface	Router(config-if)#no shutdown
Exit the interface	Router(config-if)# exit
Save configuration	Router# copy running-config startup-config

Points to Remember

- Inter-VLAN routing allows communication between devices in different VLANs.
- Types of Inter-VLAN Routing are Router-on-a-Stick Inter-VLAN Routing, Traditional Inter-VLAN Routing and Layer 3.
- A sub-interface is a virtual interface created on a router's physical interface.
- Configure VLANs on the Layer 3 switch.
- Set up sub-interfaces on the router for Router-on-a-Stick.
- Enable Inter-VLAN routing on the Layer 3 switch.
- Test communication between PCs in different VLANs.



Application of learning 2.4.

You are a network engineer at a corporate office that has recently implemented VLANs to enhance network performance and security. The office consists of two departments: Sales and Marketing, each requiring its own VLAN for segmented network traffic. The management needs to ensure that devices in different VLANs can communicate effectively. Configure and verify Inter-VLAN Routing using Router-on-a-Stick and a Layer 3 switch in a simulated network environment.

Network Requirements:

1. **VLANs:**
   - **VLAN 10**: Sales (IP range: 192.168.10.0/24)
   - **VLAN 20**: Marketing (IP range: 192.168.20.0/24)
2. **PC Assignments:**
   - **PC1 (Sales)**: IP: 192.168.10.2
   - **PC2 (Sales)**: IP: 192.168.10.3
   - **PC3 (Marketing)**: IP: 192.168.20.2
   - **PC4 (Marketing)**: IP: 192.168.20.3
3. **Devices:**
   - 1 Layer 3 Switch
   - 1 Router
   - 2 Access Switches
   - 4 PCs

Indicative content 2.5: Configure Spanning Tree Protocol.

Duration: 3 hrs

Theoretical Activity 2.5.1: Description of STP

Task:

1: Read carefully and answer the following questions:

i. What is Spanning Tree Protocol (STP)?

ii. What is BPDU?

iii. What is a Bridge ID, and how is it composed?

iv. How does the Spanning Tree Algorithm (STA) work?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 2.5.1 in trainee manuals.

Key readings 2.5.1: Description of STP

✔ **Introduction to STP**

Definition: Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for computer networks. It prevents broadcast storms and ensures that frames are not endlessly circulated in a network. Developed by: Dr. Radia Perlman in 1985, is **IEEE Standard**: 802.1D.

✔ **Redundancy**

Definition:

Redundancy in networking refers to the inclusion of extra components that are not strictly necessary for functioning but can take over in case of failure. The Purpose is to Enhances network reliability and availability by providing alternative paths for data.

Redundancy in networking refers to the inclusion of extra components that are not strictly necessary for functioning but can take over in case of failure. The Purpose is to Enhances network reliability and availability by providing alternative paths for data.

Benefits of Redundancy in STP:

Increased Network Reliability: Redundant paths ensure that the network can recover from failures without significant downtime.

Automatic Rerouting: If a primary path fails, STP quickly reconfigures the network to use the redundant path.

Efficient Use of Resources: STP allows multiple redundant links but only activates them when necessary, making efficient use of network resources.

- ✓ **Spanning Tree Algorithm (STA)**

Function: The algorithm determines the best path for data transmission while blocking redundant paths. The algorithm dynamically selects the best, most efficient paths for data traffic while blocking any redundant links that could create network loops.

How the Spanning Tree Algorithm Works:

1.Root Bridge Election:

The STA begins by selecting a Root Bridge, which is the switch with the lowest Bridge ID (a combination of the switch's priority and MAC address).

All path decisions are made relative to this Root Bridge.

The switch with the lowest priority value is preferred. If the priority values are the same, the switch with the lowest MAC address becomes the Root Bridge.

2.Selecting Root Ports:

Each non-root switch identifies a single Root Port. This is the port with the shortest path (lowest cost) to the Root Bridge.

The Root Port is the designated port through which the switch communicates with the Root Bridge.

3.Selecting Designated Ports:

For each segment (link between switches), one switch is designated as the Designated Bridge, and the port on that switch connected to the segment becomes the Designated Port.

The Designated Port is responsible for forwarding traffic to and from that segment.

4.Blocking Redundant Paths:

Any redundant paths (links that could create loops) are placed in a blocking state.

Ports in a blocking state do not forward traffic but are still part of the spanning tree, ready to be activated if the active link fails.

Only one active path is maintained between any two network segments to prevent loops.

5.Path Cost Calculation:

The STA assigns a cost to each path based on the bandwidth of the links. Lower cost paths are preferred.

The default cost for a link is inversely proportional to the bandwidth, so higher-speed links are preferred over lower-speed ones (e.g., Gigabit Ethernet paths are preferred over Fast Ethernet paths).

6.Convergence:

When the algorithm has finished, the network has converged into a loop-free tree structure.

If a link fails or topology changes, STP recalculates the tree, reactivating redundant links if necessary to restore connectivity.

- ✓ **STP BPDU (Bridge Protocol Data Unit)**

Definition: BPDUs are messages exchanged between switches to maintain the spanning tree

The BPDU (Bridge Protocol Data Unit) are frames/ messages that contain information about the spanning tree protocol.

A switch sends BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC.

The destination MAC address is 01:80:C2:00:00:00, which is a multicast address for the spanning-tree group.

Types of BPDUs:

- **Configuration BPDUs**: Used to establish and maintain the spanning tree.
- **Topology Change Notification (TCN) BPDUs**: Indicate changes in the network topology.

- ✓ **Bridge ID**

Definition: A unique identifier for each switch in an STP network.

The bridge ID consists of switch priority, extended system ID, and MAC address

The switch priority is a numerical value defined by IEEE 802.1D it is equal to 32,768 by default.

- **Purpose**: Helps in determining the Root Bridge and managing the topology.

✓ **Port Roles**

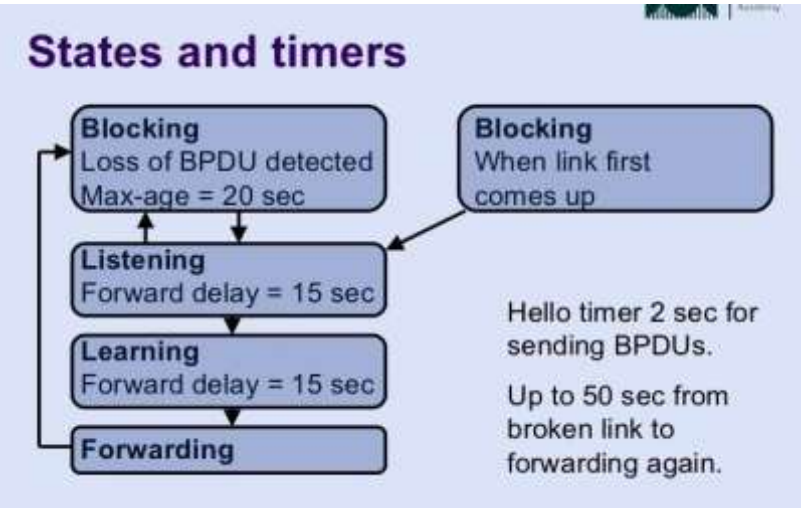
Definition :

In Spanning Tree Protocol (STP), a port role defines how a particular port on a switch participates in the spanning tree topology. These roles determine whether a port forwards traffic, stays in a blocked state to prevent network loops, or provides redundancy for failover. Each port is assigned a role based on its position in the network relative to the Root Bridge and the network's overall topology.

- **Root Port**: The port on a non-root switch with the lowest cost to the Root Bridge.
- **Designated Port**: The port that has the lowest cost to the Root Bridge on a network segment; it forwards traffic.
- **Blocked Port**: A port that does not participate in frame forwarding to prevent loops.

STP Port States and BPDU Timers

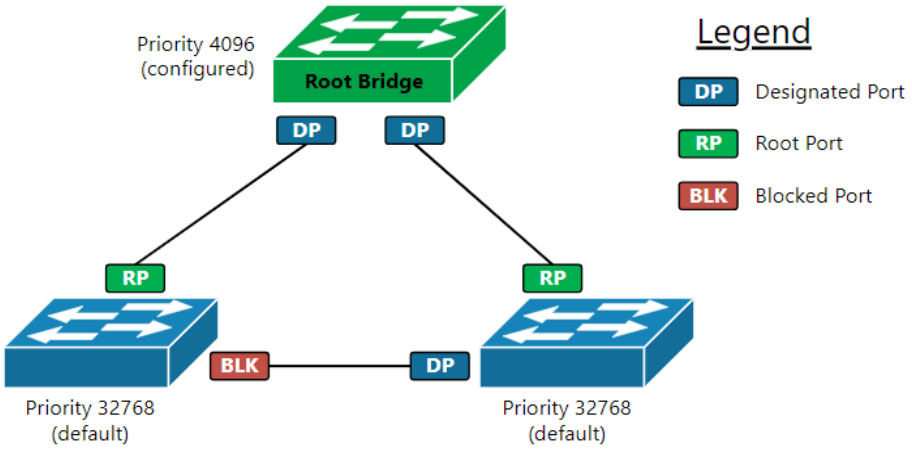
- **Port States:**
  - **Disabling:** port is turned off.
  - **Blocking**: Port does not forward frames or learn MAC addresses.
  - **Listening**: Port prepares to forward frames but does not send or receive frames.
  - **Learning**: Port learns MAC addresses but does not forward frames.
  - **Forwarding**: Port sends and receives frames and learns MAC addresses.
- **BPDU Timers**:
  - **Hello Time**: Time interval between BPDUs sent (default is 2 seconds).
  - **Max Age**: Time a BPDU is considered valid (default is 20 seconds).
  - **Forward Delay**: Time spent in Listening and Learning states (default is 15 seconds).



✓ **Configuration of STP Bridge IDs**

Steps:

1. **Access Switch Configuration**: Log into the switch.
2. **Set Bridge Priority**: Adjust the bridge priority to influence which switch becomes the Root Bridge.
3. **Verify Configuration**: Use commands (e.g., show spanning-tree) to check STP settings and ensure proper operation.



Set priority directly

SW1#spanning-tree vlan 1 priority 24576

Or indirectly

SW1#spanning-tree vlan 1 root primary

Sets value to 24576 or 4096 less than lowest priority detected.

SW1#spanning-tree vlan 1 root secondary

Sets value to 28672. This switch should becomes the root bridge if the primary root bridge fails.

Configure port priority

SW2(config-if)#spanning-tree port-priority 112

Priority values range from 0 - 240, in increments of 16.

The default port priority value is 128.

Practical Activity 2.5.2: Configuring STP

Task:

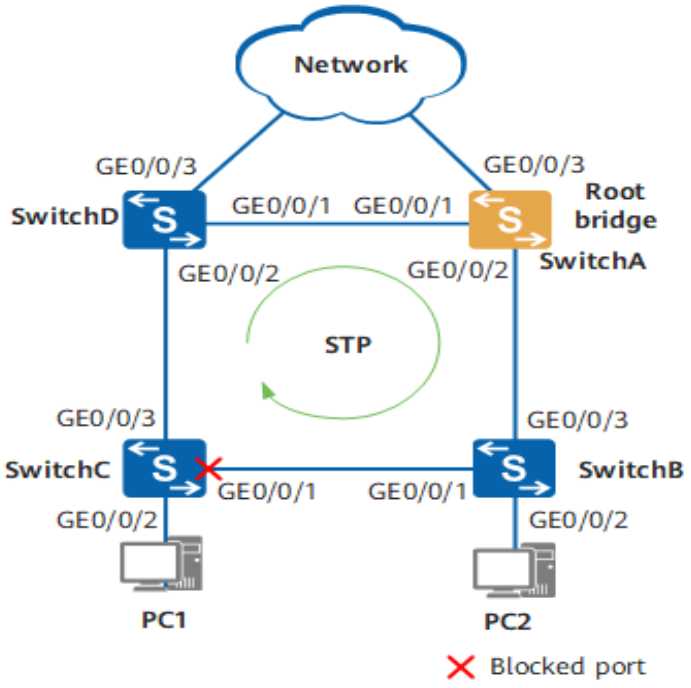
1: Refer to the key reading 2.5.2 and perform the following task:

You are asked to go to computer lab of your school and Configure STP to prevent loops in the network, Ensure Switch A becomes the Root Bridge, Set the correct bridge priorities for Switch B and Switch C. Configure port settings for optimal performance and redundancy.

2: Presents the steps to Configure STP to prevent loops in the network.
3: Configure STP to prevent loops in the network.
4: Ask if any clarification
5: For more clarifications, read the key readings 2.5.2.
6: Perform the activity in the application of learning 2.5.

Key readings 2.5.2 Configuring STP

Refers to the Figure below and follow the steps of how to configure STP



- Step-by-Step Configuration of STP
  - ✓ **Step 1: Access the Switch**

Connect to the switch via console, SSH, or Telnet.

Step 2: Enter Global Configuration Mode

Switch> enable

Switch# configure terminal

Step 3: Verify STP is Enabled

STP is generally enabled by default. Check its status with:

Switch# show spanning-tree

If STP is not enabled, you might need to check your switch model, as some newer models use RSTP by default.

Step 4: Configure STP Mode

To ensure you are using classic STP instead of PVST or RSTP:

Switch(config)# spanning-tree mode stp

This command enables classic STP (IEEE 802.1D).

Step 5: Set the Bridge Priority

The switch with the lowest Bridge ID becomes the Root Bridge. The Bridge ID consists of the priority and the MAC address. To set the priority, use:

Switch(config)# spanning-tree vlan <VLAN_ID> priority <PRIORITY_VALUE>

Example for VLAN 1:

Switch(config)# spanning-tree vlan 1 priority 4096

- Lower values have higher priority, so 4096 is preferred over the default 32768.

Step 6: Configure Interfaces

For each interface, you may want to ensure they are in the correct state. By default, all ports are in the blocking state until STP has determined their roles.

- Access interface configuration:
  Switch(config)# interface <INTERFACE_TYPE> <INTERFACE_NUMBER>

  Example:

  Switch(config)# interface fastethernet 0/1
- Enable the interface:
  Switch(config-if)# no shutdown
- Optionally, enable **PortFast** on access ports (ports connecting to end devices) to speed up the port state transitions:
  Switch(config-if)# spanning-tree portfast
- Repeat this for all access ports.

Step 7: Configure STP Timers (Optional)

You can adjust STP timers to optimize convergence times, but the default settings are typically sufficient.

- Set the **Hello Time** (default is 2 seconds):
  Switch(config)# spanning-tree hello-time 2
- Set the **Max Age** (default is 20 seconds):
  Switch(config)# spanning-tree max-age 20
- Set the **Forward Delay** (default is 15 seconds):

Switch(config)# spanning-tree forward-time 15

Step 8: Enable BPDU Guard (Optional)

To protect against loops caused by incorrect connections, enable **BPDU Guard** on access ports:

Switch(config-if)# spanning-tree bpduguard enable

Step 9: Save the Configuration

Once you have made all necessary configurations, save the settings to ensure they persist after a reboot:

Switch# write memory

or

Switch# copy running-config startup-config

Step 10: Verify STP Configuration

Check the STP configuration and port roles:

Switch# show spanning-tree

To see the detailed status for a specific VLAN:

Switch# show spanning-tree vlan <VLAN_ID>

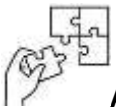
Key Commands and their descritpions:

Command	Description
show spanning-tree	View current STP status.
spanning-tree mode stp	Enable classic STP (IEEE 802.1D).
spanning-tree vlan <vlan_id> priority <value>	Set switch priority for VLAN.
interface <type> <number>	Access interface configuration.
spanning-tree portfast	Enable PortFast on access ports.

spanning-tree bpduguard enable	Enable BPDU Guard on access ports.
write memory or copy running-config startup-config	Save configuration changes.

Points to Remember

- STP prevents switching loops in redundant network designs by selectively blocking certain ports.
- STP uses the Spanning Tree Algorithm (STA) to build a loop-free topology.
- BPDUs are used to share information about the network topology between switches.
- STP Port Roles are Root Port (RP), Designated Port (DP) and Blocking/Non-Designated Port (NDP).
- Configure Switch A as the Root Bridge.
- Set bridge priorities for Switch B and Switch C.
- Configure port settings for optimal performance.
- Enable redundancy and loop prevention.



Application of learning 2.5.

As a network engineer at XYZ Corporation, you are tasked with optimizing network performance and redundancy for the Sales and Marketing departments by configuring VLANs on three switches. To prevent broadcast storms and loops, you will implement Spanning Tree Protocol (STP), ensuring Switch A becomes the Root Bridge, while setting appropriate bridge priorities for Switch B and Switch C. Additionally, you will configure Switch B as a backup to ensure optimal performance and redundancy, providing high availability and secure traffic management across the network.

Indicative content 2.6: Apply Converge STP.

Duration: 3 hrs

Practical Activity 2.6.1: Applying converge STP

Task:

1: Refer to the key reading 2.6.1 and perform the following task:
You are asked to go to computer lab of your school and applying Converged Spanning Tree Protocol (STP) in a network consisting of three switches: Switch A, Switch B, and Switch C. The network uses VLANs 10 (Sales) and 20 (Marketing). You are tasked to configure STP to elect the root bridge, root ports, designated ports, non-designated ports, and understand how STP responds to topology changes.

2: Presents the steps to configure STP to elect the Root Bridge, root ports, designated ports, and non-designated ports.
3: Configure STP to elect the Root Bridge, root ports, designated ports, and non-designated ports.
4: Ask if any clarification if any.
5: For more clarifications, read the key readings 2.6.1.
6: Perform the activity in the application of learning 2.6.

Key readings 2.6.1 Apply Converge STP

STP (Spanning Tree Protocol) Convergence Steps with Configuration

STP convergence ensures a loop-free topology in a network by electing a root bridge, designating specific ports, and recalculating paths when changes occur.

Step-by-step guide to STP convergence, along with configuration commands.

1. Elect the Root Bridge

- STP selects the switch with the lowest Bridge ID (combination of priority, SystemID and MAC address) as the Root Bridge. All switches exchange Bridge Protocol Data Units (BPDUs) to identify the Root Bridge.
- **Configuration**: Set the switch priority to make a specific switch the Root Bridge (lower priority means higher preference).

  Configuration: On the switch you want to be the Root Bridge (e.g., SW1):

Switch(config)# spanning-tree vlan <vlan_id> priority <priority_value>

For example:

Switch(config)# spanning-tree vlan 10 priority 4096

This sets the switch's priority to 4096 (lower than the default 32768).

2. Elect Root Ports on Non-Root Switches

- Each non-root switch selects a Root Port (RP), which is the port with the lowest cost path to the Root Bridge.
- **Default Configuration**: STP automatically selects the Root Port. However, you can influence path selection by adjusting interface costs.

  Optional Configuration (tuning path costs):

  Switch(config)# interface <interface_id>

  Switch(config-if)# spanning-tree cost <cost_value>

  For example, to set the cost of a GigabitEthernet port:

  Switch(config)# interface GigabitEthernet 0/1

  Switch(config-if)# spanning-tree cost 4

3. Elect Designated Ports

- For each network segment, the switch with the lowest path cost to the Root Bridge has its port elected as the Designated Port (DP). Non-Designated Ports (NDP) on other switches will be blocked to prevent loops.

  Configuration: Designated Ports are automatically selected based on path costs, but similar to Root Port election, you can influence it by changing the port cost or priority.

  To set the priority of a port:

  Switch(config)# interface <interface_id>

  Switch(config-if)# spanning-tree port-priority <priority_value>

  For example, to set the priority of an interface:

  Switch(config)# interface FastEthernet 0/2

  Switch(config-if)# spanning-tree port-priority 32

4. Handle Topology Changes

- If a topology change occurs (e.g., link failure or a new link), the switches detect the change, send Topology Change Notifications (TCNs), and recalculate the Root and Designated Ports.

Configuration: No specific configuration is needed for topology changes, but you can enable features like PortFast and BPDU Guard to speed up convergence for edge ports.

Enable PortFast for access ports:

Switch(config)# interface <interface_id>

Switch(config-if)# spanning-tree portfast

Enable BPDU Guard to protect the network from accidental loops on PortFast-enabled interfaces:

Switch(config)# interface <interface_id>

Switch(config-if)# spanning-tree bpduguard enable

Example Configuration:

For VLAN 10 on Switch SW1 (Root Bridge), Switch SW2 (Non-Root Switch), and Switch SW3:

SW1 (Root Bridge):

Switch(config)# spanning-tree vlan 10 priority 4096

Switch(config)# interface GigabitEthernet 0/1

Switch(config-if)# spanning-tree portfast

Switch(config)# interface GigabitEthernet 0/2

Switch(config-if)# spanning-tree portfast

SW2 (Non-Root Switch):

Switch(config)# interface GigabitEthernet 0/1

Switch(config-if)# spanning-tree cost 19

Switch(config)# interface GigabitEthernet 0/2

Switch(config-if)# spanning-tree port-priority 32

Switch(config)# interface GigabitEthernet 0/3

Switch(config-if)# spanning-tree bpduguard enable

SW3 (Non-Root Switch):

Switch(config)# interface GigabitEthernet 0/1

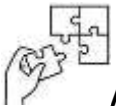
Switch(config-if)# spanning-tree cost 19

```
Switch(config)# interface GigabitEthernet 0/2

Switch(config-if)# spanning-tree bpduguard enable
```

Points to Remember

- Elect the Root Bridge.
- Configure Root Ports and Designated Ports.
- Set Non-Designated Ports.
- Explain STP Response to Topology Changes.



Application of learning 2.6.

As a network administrator managing a small enterprise LAN with four switches (SW1, SW2, SW3, and SW4) in a mesh topology, you need to implement the Spanning Tree Protocol (STP) to prevent loops and ensure efficient traffic flow. Ensure all switches agree on a single Root Bridge, which will serve as the reference point for path calculations. Each non-root switch must elect its Root Ports for the best path to the Root Bridge based on path cost. Additionally, elect a Designated Port for each network segment to forward traffic, while all other ports become Non-Designated Ports to block traffic and prevent loops.

Indicative content 2.7: Configure PVST+, RSTP and Rapid PVST+.

Duration: 3 hrs

Theoretical Activity 2.7.1: Description of PVST+, RSTP and rapid PVST+.

Task:

1. Read carefully and answer the following questions:
   i. What does PVST+ stand for?
   ii. What components make up the Bridge ID in PVST+?
   iii. What are the key characteristics of RSTP?
   iv. Name the three link types recognized by RSTP.
2. Write answers on paper flipchart, blackboard or whiteboard.
3. Present the finding to the whole class.
4. Ask questions for clarification if needed.
5. Read the Key readings 2.7.1 in trainee manuals.

Key readings 2.7.1 Description PVST+, RSTP and rapid PVST+

1. STP Variants

Spanning Tree Protocol (STP) is used to prevent loops in Ethernet networks by creating a loop-free topology. There are several variants of STP, including:

- **PVST+ (Per-VLAN Spanning Tree Plus)**: An enhancement of the original STP that allows for multiple spanning trees for each VLAN. This helps optimize traffic by enabling separate path calculations for each VLAN.
- **RSTP (Rapid Spanning Tree Protocol)**: An evolution of STP that significantly reduces the convergence time when a topology change occurs. RSTP can rapidly transition ports to a forwarding state.
- **Rapid PVST+**: Combines the benefits of PVST+ and RSTP, allowing for rapid convergence while maintaining per-VLAN spanning trees.

2. PVST+ Bridge ID

- **Bridge ID**: In PVST+, the Bridge ID is a unique identifier for each switch and is used during the election of the Root Bridge.
  - The Bridge ID consists of:
    - **Bridge Priority** (default is 32768; can be configured for influence during Root Bridge election)
    - **MAC Address** of the switch
  - The Bridge with the lowest Bridge ID becomes the Root Bridge.

3. Per-VLAN Spanning Tree (PVST+): runs a separate STP instance for each VLAN.

Advantages of PVST+

Load balancing: You can assign different root bridges for different VLANs.

Customized network control: You can adjust the spanning tree configuration on a per-VLAN basis.

Example: VLAN 10 might have SW1 as the Root Bridge, while VLAN 20 has SW2 as the Root Bridge.

- Primary and Secondary Root Bridges:
  - **Primary Root Bridge**: The main Root Bridge for a VLAN.
  - **Secondary Root Bridge**: A backup Root Bridge that is elected to take over in case the primary fails.
- **PVST+ Switch Priority**: Switch Priority: A configurable value used to influence the election of the root bridge. The lower the priority, the more likely the switch is to be elected as the root.

  Default switch priority is 32768, and it must be adjusted in increments of 4096.

  Setting a lower switch priority (e.g., 4096) makes a switch more likely to be elected as the Root Bridge.
- **Example:** For VLAN 10, you can configure SW1 with a priority of 4096 to ensure it becomes the Root Bridge for that VLAN.
  - **Use the following command to change the priority:**

  switch(config)# spanning-tree vlan <vlan_id> priority <priority_value>

4. Rapid Spanning Tree Protocol (IEEE 802.1w): improves upon traditional STP by achieving faster convergence and eliminating some of the delays in port transitions.

- RSTP Characteristics:
  - RSTP provides faster convergence compared to standard STP, with recovery times typically less than a second.
  - It uses the same BPDU format as STP but introduces new mechanisms to achieve rapid transitions.
  - Introduces new port roles (Alternate and Backup) for faster failover.
  - Ports can quickly move to forwarding or discarding states without waiting for timers like traditional STP.
  - **Port Roles:**
  - **Root Port:** Port with the best path to the Root Bridge.
  - **Designated Port:** Port that forwards traffic for a network segment.
  - **Alternate Port:** Provides an alternative path to the Root Bridge if the Current Root Port fails.
  - **Backup Port:** A backup to the Designated Port on the same segment.
- **RSTP Port States**:
  - **Discarding**: The port does not forward frames and does not learn MAC addresses.
  - **Learning**: The port learns MAC addresses but does not forward frames.
  - **Forwarding**: The port forwards frames and learns MAC addresses.

802.1D is defined in the following five different port states:

STP (802.1D) Port state	**RSTP (802.1W) Port state**	**Is port included in Active topology ?**	**Is port Learning MAC Address**
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes

Forwardin g	Forwardin g	Yes	Yes

5. RSTP BPDU: RSTP uses a faster BPDU mechanism. BPDUs are sent every 2 seconds and contain updated information about network topology.

- RSTP sends BPDUs (Bridge Protocol Data Units) every 2 seconds, which contain information about the network topology.
- The BPDU includes flags indicating the role of the port and the status of the link.
- Unlike traditional STP, where only the Root Bridge generates BPDUs, in RSTP, **every switch** generates BPDUs, improving the speed of network recovery.

6. Edge Ports:

- Edge Ports are ports that connect directly to end devices (e.g., computers, printers) rather than other switches.
- These ports can transition immediately to the forwarding state, bypassing the listening and learning states.
- Equivalent to Cisco's **PortFast** feature in traditional STP.

7. Link Types:

- RSTP recognizes three types of links:
  - **Point-to-Point**: Links between switches, allowing rapid convergence.
  - **Shared**: Older hubs or segments shared by multiple devices.

Practical Activity 2.7.2: Configuring PVST+, RSTP and rapid PVST+

1: Refer to the key reading 2.7.2 and perform the following task:
You are asked to go to school lab and Configure modes such as PVST+, PVST, and Rapid Spanning Tree Protocol to optimize traffic flow and reducing broadcast domains.

2: Presents the steps to configure PVST+, RSTP and rapid PVST+.
3: Trainer ask trainees to configure PVST+, RSTP and rapid PVST+
4: Ask if any clarification
5: For more clarifications, read the key readings 2.7.2.

6: Perform the activity in the application of learning 2.7.

Key readings 2.7.2 Configure PVST+, RSTP and rapid PVST+

1. Configure PVST+ (Per-VLAN Spanning Tree Plus)

- **Default Configuration**: PVST+ is enabled by default on Cisco switches. Each VLAN operates its own spanning tree.
- **Bridge Priority**: To influence Root Bridge election, adjust the switch priority using the command:

  Switch(config)# spanning-tree vlan [VLAN_ID] priority [PRIORITY_VALUE]

  - Priority value is configured in increments of 4096 (default is 32768).
  - Example: To set priority for VLAN 10:

    Switch(config)# spanning-tree vlan 10 priority 4096

- Verify Configuration:

  Switch# show spanning-tree

  Switch# show spanning-tree vlan 10

2. Configuring RSTP (Rapid Spanning Tree Protocol)

Step 1: Access the Switch CLI

- Connect to the switch as before.

Step 2: Enter Global Configuration Mode

Switch# configure terminal

Step 3: Enable RSTP

- Configure the switch to use Rapid PVST:

  Switch(config)# spanning-tree mode rapid-pvst

Step 4: Verify RSTP Configuration

- Check the RSTP status:

  Switch# show spanning-tree

3. Configuring Rapid PVST+

Step 1: Access the Switch CLI

- Connect to the switch.

Step 2: Enter Global Configuration Mode

Switch# configure terminal

Step 3: Enable Rapid PVST+ (if not already enabled)

Switch(config)# spanning-tree mode rapid-pvst

Step 4: Configure Edge Ports (Optional)

- Set a port to be an edge port (for direct connections to end devices):

Switch(config)# interface [INTERFACE_ID]

Switch(config-if)# spanning-tree portfast

Step 5: Adjust Port Cost (Optional)

- To manually set the path cost for a specific interface:

Switch(config)# interface [INTERFACE_ID]

Switch(config-if)# spanning-tree cost [COST_VALUE]

Points to Remember

- PVST+ runs a separate STP instance per VLAN, allowing for efficient traffic management and load balancing across VLANs.
- Bridge ID combines switch priority and MAC address; a lower priority increases the likelihood of being elected as the Root Bridge.
- Primary and Secondary Root Bridges ensure redundancy, with the secondary taking over in case of failure.
- Switch priority can be configured in PVST+ to influence which switch becomes the Root Bridge for a VLAN.
- RSTP provides faster convergence than STP by introducing new port roles (Alternate, Backup) and quicker transition to forwarding states.

- BPDUs in RSTP are sent by all switches every 2 seconds, enabling quicker detection of topology changes.
- Edge Ports (like PortFast in Cisco) skip STP transitions and go directly to forwarding, making RSTP efficient for end-user devices.
- Link types (point-to-point vs. shared) influence how quickly RSTP can converge on different network segments.
- Configure PVST+ for VLAN Support.
- Use PVST for Legacy Support.
- Implement Rapid Spanning Tree Protocol (RSTP).
- Verify Configuration and Traffic Optimization.

Application of learning 2.7.

In a corporate environment, the network infrastructure consists of multiple switches supporting various VLANs. The IT team has been experiencing issues with slow network convergence and occasional loops, causing disruptions in service. The team is tasked with configuring PVST+, RSTP, and Rapid PVST+ to enhance network stability, reduce downtime, and optimize traffic flow.

Indicative content 2.8: Configuring Aggregation Modes

Duration: 3 hrs

Practical Activity 2.8.1: Configuring Aggregation modes

Task

1: Refer to the key reading 2.8.1 and perform the following task:

You are asked to go to Configure link aggregation modes (PAgP, LACP, Static Link Aggregation) and implement VRRP to ensure continuous network availability in a simulated environment. Equipment:

2Cisco switches (Switch A and Switch B)

2 PCs (PC1 and PC2)

Console access to switches.

2: Presents the steps to Configure link aggregation modes.
3: Configure link aggregation modes.
4: Ask clarification if any.
5: Ask trainees to read key readings 2.8.1 in their manuals.

Key readings 2.8.1 Configuring Aggregation modes

1. Configure Port Aggregation Protocol (PAgP)

PAgP Overview:

- PAgP helps in dynamically establishing EtherChannel links between switches.
- It can operate in two modes: **Desirable** (actively attempts to form an EtherChannel) and **Auto** (passively waits for the other side to initiate).

Configuration Steps:

1. Enter interface configuration mode for the interfaces to be aggregated:

   Switch(config)# interface range GigabitEthernet 0/1 - 2

2. Configure PAgP to operate in desirable mode:

   Switch(config-if-range)# channel-group 1 mode desirable

3. Verify the configuration:

   Switch# show etherchannel summary

➢ **Configure Port Aggregation Protocol (PAgP)**

Port Aggregation Protocol or **PAgP** is an EtherChannel technology that is a Cisco proprietary protocol.

It is a form of logical aggregation of Cisco Ethernet switch ports, and it enables data/traffic load balancing.

PAgP EtherChannel can combine a maximum of 8 physical links into a single virtual link. We also have an IEEE open standard, Link Aggregation Control Protocol, LACP.

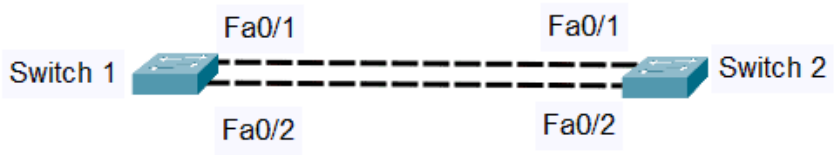
✔ **PAgP Initial Configuration Check**

Since PAgP is a Cisco proprietary protocol, we need to make sure that all of the interfaces have the same following configurations in our Cisco network devices:

1. Speed and Duplex
2. Operational State (all Access or all Trunking)
3. Access VLAN on access interfaces
4. Native VLAN and Allowed VLANs on trunk interfaces
5. STP interface settings

How to Configure Port Aggregation Protocol?

We'll use the network topology below for our example. We have two Cisco switches to be configured with PAgP.



Switch 1 Configuration:

```
Switch 1#conf t

Switch 1(config)#interface range fa0/1 - 2

Switch 1(config-if-range)#speed 100

Switch 1(config-if-range)#duplex full

Switch 1(config-if-range)#switchport mode trunk

Switch 1(config-if-range)#channel-group 1 mode desirable

Switch 1(config-if-range)#end
```

Switch 2 Configuration:

```
Switch 2#conf t

Switch 2(config)#interface range fa0/1 - 2

Switch 2(config-if-range)#speed 100

Switch 2(config-if-range)#duplex full

Switch 2(config-if-range)#switchport mode trunk

Switch 2(config-if-range)#channel-group 1 mode auto

Switch 2(config-if-range)#end
```

Switch logs showing Port-Channel1 comes up:

```
%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

Port Aggregation Protocol Verification

We can issue the **'show etherchannel <channel-group number> port-channel'** command to check if the Port-channel is active or not. We can verify which of the two protocols is used, PAgP or LACP, and the interfaces participating in the aggregation.

```
Switch1#show etherchannel 1 port-channel

Port-channels in the group:

Port-channel: Po1

Age of the Port-channel = 0d:00h:04m:07s

Logical slot/port   = 16/0 Number of ports = 2

GC= 0x00010001 HotStandBy port = nullPort state = Port-channel Ag-Inuse
Protocol =PAgP

Port security = Disabled

Ports in the Port-channel:

Index Load Port EC state No of bits

------+------+------+------------------+-----------

0  00  Fa0/1  Automatic-Sl      0

0  00   Fa0/2  Automatic-Sl   0

Time since last port bundled: 0d:00h:00m:26s Fa0/2
```

Next, **'show etherchannel summary'** will show us a quick overview of the EtherChannel status.

```
Switch 1#show etherchannel summary

Flags: D - down  P - bundled in port-channel

 I - stand-alone  s - suspended

H - Hot-standby (LACP only)
```

R - Layer3 S - Layer2

U - in use N - not in use, no aggregation

f - failed to allocate aggregator

M - not in use, minimum links not met

m - not in use, port not aggregated due to minimum links not met

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

A - formed by Auto LAG

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

------+-------------+-----------+---**1 Po1(SU) PAgP Fa0/1(P) Fa0/2(P)**

Lastly, we can issue the **'show interfaces fa0/1 etherchannel'** command. We can see both local and neighbor interface information, and also the Cisco PAgP mode used.

Switch 1#show interfaces fa0/1 etherchannel

2. Configure Link Aggregation Control Protocol (LACP)

LACP Overview:

- LACP allows multiple links to be bundled together and provides fault tolerance by enabling dynamic link aggregation.

Configuration Steps:

1. Enter interface configuration mode for the interfaces to be aggregated:

Switch(config)# interface range GigabitEthernet 0/3 - 4

2. Configure LACP:

   Switch(config-if-range)# channel-group 2 mode active

   - Use **passive** mode to wait for another device to initiate aggregation.

3. Verify the configuration:

   Switch# show etherchannel summary

- **Configure Link Aggregation Control Protocol (LACP)**

Link Aggregation Control Protocol or **LACP** in networking is an IEEE standard and a part of the IEEE 802.3ad specification that allows you to combine multiple physical links to form a single logical link and enable load balancing in our interfaces.

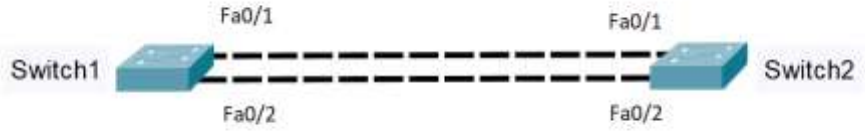
If a link fails, LACP will also fail over automatically.

We can configure LACP EtherChannel with a maximum of 16 multiple Ethernet links of the same type.

In a LAG or Link Aggregation Group, up to eight member links can be active, and the other eight links can be on standby.

EtherChannel LACP Configuration

Now, using our sample network topology below, let's configure LACP on our network switches' multiple links:



Switch 1 – Active Mode

```
Switch1#conf t

Switch1(config)#interface range fa0/1 - 2
```

```
Switch1(config-if-range)#speed 100

Switch1(config-if-range)#duplex full

Switch1(config-if-range)#switchport mode trunk

Switch1(config-if-range)#channel-group 1 mode active

Switch1(config-if-range)#end
```

Switch 2 – Passive Mode

```
Switch2#conf t

Switch2(config)#interface range fa0/1 - 2

Switch2(config-if-range)#speed 100

Switch2(config-if-range)#duplex full

Switch2(config-if-range)#switchport mode trunk

Switch2(config-if-range)#channel-group 1 mode passive

Switch2(config-if-range)#end
```

The logs on our switch show that Port-Channel1 came up, and the aggregated link is working:

```
*Sep 5 15:30:06.378: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up



*Sep 5 15:30:07.378: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

How to Verify LACP?

We can use the **'show etherchannel <channel-group number> port-channel'** command to verify link aggregation and our port channel status:

```
Switch1#show etherchannel 1 port-channel
```

```
Port-channels in the group:

Port-channel: Po1    (Primary Aggregator)

Age of the Port-channel   = 0d:00h:01m:05s

Logical slot/port = 16/0 Number of ports = 2

HotStandBy port = null

Port state = Port-channel Ag-Inuse

Protocol  = LACP

Port security = Disabled

Ports in the Port-channel:

Index Load Port EC state No of bits

------+------+------+------------------+-----------

0  00 Fa0/1  Active   0

0 00  Fa0/2    Active   0

Time since last port bundled: 0d:00h:00m:50s Fa0/2
```

3. Configure Static Link Aggregation / Manual EtherChannel

Static Link Aggregation Overview:

- In Static Link Aggregation, EtherChannel is configured manually without negotiation protocols.

Configuration Steps:

1. Enter interface configuration mode for the interfaces to be aggregated:

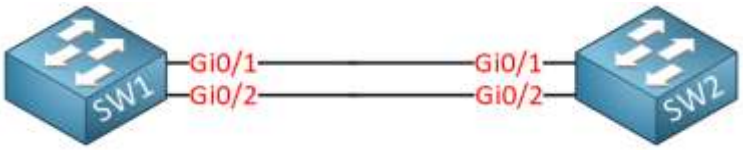
   Switch(config)# interface range GigabitEthernet 0/5 - 6
2. Manually configure EtherChannel:

   Switch(config-if-range)# channel-group 3 mode on
3. Verify the configuration:

   Switch# show etherchannel summary

- **Configure Static Link Aggregation / Manual Ether Channel**

Instead of PAgP or LACP, we can also manually enable the Etherchannel. I'll use the same topology to demonstrate this:



Here's the configuration:

SW1(config)#**interface range GigabitEthernet 0/1 - 2**

SW1(config-if-range)#**channel-group 1 mode on**

SW2(config)#**interface range GigabitEthernet 0/1 - 2**

SW2(config-if-range)#**channel-group 1 mode on**

That's all there is to it. Let's try our show commands. We'll start with an overview:

SW1#**show etherchannel summary**

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use N - not in use, no aggregation

f - failed to allocate aggregator

M - not in use, minimum links not met

m - not in use, port not aggregated due to minimum links not met

u - unsuitable for bundling

```
w - waiting to be aggregated

d - default port

A - formed by Auto LAG

Number of channel-groups in use: 1

Number of aggregators:          1

Group  Port-channel  Protocol    Ports

------+-------------+-----------+-----------------------------------------------1     Po1(SU)       -

Gi0/1(P)    Gi0/2(P)
```

In the output above, you can see we don't use any protocol. Let's take a closer look at the Port-channel interface:

```
SW1#show etherchannel 1 port-channel

Port-channels in the group:

Port-channel: Po1

Age of the Port-channel = 0d:00h:06m:54s

Logical slot/port = 16/0 Number of ports = 2

GC  = 0x00000000 HotStandBy port = null

Port state…….= Port-channel Ag-Inuse

Protocol ……=…… -

Port security       = Disabled

Load share deferral = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
```

```
------+------+------+-----------------+-----------

0….00…..Gi0/1…..On……. 0

0……00……Gi0/2…..On…..0

Time since last port bundled:    0d:00h:01m:21s    Gi0/2

Time since last port Un-bundled: 0d:00h:04m:05s    Gi0/2
```

And we can check one of the two physical interfaces and see the Etherchannel information:

```
SW1#show interfaces GigabitEthernet 0/1 etherchannel

Port state    = Up Mstr In-Bndl

Channel group = 1 Mode = On

Pseudo port-channel = Po1

Port index = 0 Load = 0x00 Protocol =-

Age of the port in the current state: 0d:00h:01m:41s
```

4. Configure Virtual Router Redundancy Protocol (VRRP)

VRRP Overview:

- VRRP allows multiple routers to work together to present a single virtual router (gateway) to clients, providing redundancy and high availability.

Configuration Steps:

1. Enter global configuration mode:

   Switch(config)#

2. Configure the VRRP group:

   Switch(config)# interface GigabitEthernet 0/0

   Switch(config-if)# vrrp 1 ip 192.168.1.1

3. Set the priority of the router (higher values have higher priority):

   Switch(config-if)# vrrp 1 priority 120

4. Enable preemption (optional):

   Switch(config-if)# vrrp 1 preempt

5. Verify the configuration:

   Switch# show vrrp

Virtual Router Redundancy Protocol (VRRP) is an open standard fault-tolerant protocol that provides redundancy and improves network reliability. It can also be used to create a virtual gateway.

There are two versions of VRRP:

1. **VRRPv2** – supports IPv4
2. **VRRPv3** – supports IPv4 and IPv6

✔ **HSRP vs. VRRP**

VRRP functions like HSRP but the following differences should be remembered:

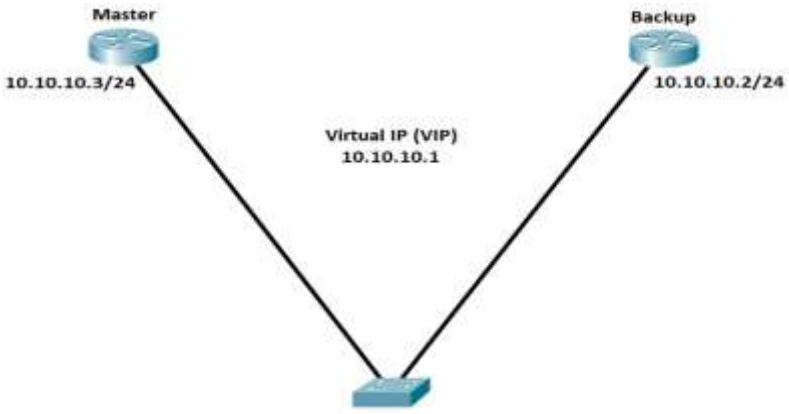
HSRP	**VRRP**
Proprietary	Open Standard
RFC 2281	RFC 3768
Cannot set physical IP as Virtual IP address (VIP)	Can use physical IP as Virtual IP (VIP) if needed
One Active Router, one Standby Router, all others are listening	One Master router, all other routers are Backup routers
Can track an interface for failover	Can track an interface for failover. It can also track the reachability of an IP

	address depending on the operating system and version.
Uses multicast IP address 224.0.0.2 for version 1 and 224.0.0.102 for version 2.	Uses multicast IP address 224.0.0.18
VIP gateway uses virtual MAC address 0000.0c07.acXX where XX is the group ID.	VIP gateway uses 0000.5e00.01xx, where XX is the group ID

Legacy Configuration

Now, let's discuss the virtual routers' configurations.

We have two ways of configuring VRRP routers, the legacy configuration, and the hierarchical configuration. We'll do the legacy first and use the topology below.



In configuring VRRPv2, we only need to define instance ID and VIP or virtual IP.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#interface GigabitEthernet 0/1

R1(config-if)#ip address 10.10.10.3 255.255.255.0

R1(config-if)#vrrp 10 ip 10.10.10.1

R1(config-if)#

*Mar 2 16:45:46.586: %VRRP-6-STATECHANGE: Gi0/1 Grp 10 state Init -> Backup

*Mar 2 16:45:50.195: %VRRP-6-STATECHANGE: Gi0/1 Grp 10 state Backup -> Master
```

```
R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#interface GigabitEthernet 0/0

R2(config-if)#

R2(config-if)#ip address 10.10.10.2 255.255.255.0

R2(config-if)#vrrp 10 ip 10.10.10.1

R2(config-if)#

*Mar 2 16:47:55.877: %VRRP-6-STATECHANGE: Gi0/0 Grp 10 state Init -> Backup

*Mar 2 16:47:55.882: %VRRP-6-STATECHANGE: Gi0/0 Grp 10 state Init -> Backup
```

For our verification, we can use the following show commands. Master router:

```
R1#sh vrrp

GigabitEthernet0/1 - Group 10
```

State is Master

Virtual IP address is 10.10.10.1

Virtual MAC address is 0000.5e00.010a

Advertisement interval is 1.000 sec

Preemption enabled

Priority is 100

Master Router is 10.10.10.3 (local), priority is 100

Master Down interval is 3.609 sec

R1#sh vrrp brief

Interface Grp Pri Time Own Pre State   Master addr   Group addr

Gi0/1 10 100 3609 Y Master 10.10.10.3 10.10.10.1

Backup router:

R2#sh vrrp

GigabitEthernet0/0 - Group 10

State is Backup

Virtual IP address is 10.10.10.1

Virtual MAC address is 0000.5e00.010a

Advertisement interval is 1.000 sec

Preemption enabled

Priority is 100

Master Router is 10.10.10.3, priority is 100

Master Advertisement interval is 1.000 sec

```
Master Down interval is 3.609 sec (expires in 3.331 sec)

R2#sh vrrp brief

Interface Grp Pri Time  Own Pre State   Master addr     Group addr

Gi0/0 10  100 3609 Y  Backup  10.10.10.3  10.10.10.1
```

Points to Remember

- Understand Link Aggregation Modes.
- Implement VRRP for Redundancy.
- Verify Configuration.
- Test Connectivity.

Application of learning 2.8.

You are a network administrator responsible for ensuring high availability, redundancy, and efficient traffic management in a small enterprise network. The network comprises two switches (SW1 and SW2) and two routers (R1 and R2) that act as gateways for the network. Your tasks include bundling multiple physical links into one logical link for better bandwidth and redundancy and ensuring gateway redundancy with VRRP, LACP, PAgP and Static EtherChannel.

Learning outcome 2 end assessment

Theoretical assessment

Q1. Circle the corresponding to the right answers:

What is the main purpose of VTP in a network?

A) To provide dynamic IP addressing
B) to manage and propagate VLAN information across switches
C) To control network traffic speed
D) To establish secure tunnels between network devices

What is a VLAN?

A) A protocol for routing network traffic
B) A virtual switch used to control IP addresses
C) A virtual network that segments traffic within a physical network
D) A device that manages network connections

What is the VLAN ID range for normal-range VLANs?

A) 1-100
B) 1-4094
C) 1006-4094
D) 1-1005

Which of the following is a valid network traffic type associated with VLANs?

A) Voice traffic
B) Control traffic
C) Broadcast traffic
D) All of the above

In a network without VLANs, what happens when a broadcast is sent?

A) The broadcast is limited to a single port
B) The broadcast is sent to all devices in the network
C) The broadcast is discarded
D) The broadcast is sent only to switches

Q2. Match the elements of the column A with the column B in the column C, to find out the right VLAN concept with its corresponding description:

Column A	**Column B**	**Column C (Answers)**
1. VLAN that carries control traffic (e.g., STP, CDP).	a. VLAN ID Range	
2. VLAN range used for VLANs 1-1005.	b. Voice VLAN	
3. VLAN range used for VLANs 1006-4094	c. Trunk VLAN	
4. VLAN type for carrying multiple VLAN traffic across switches	d. Normal Range VLANs	
5. VLAN used for separating voice traffic from data traffic.	e. Extended Range VLANs	
6. The default VLAN that carries untagged traffic on a trunk link.	f. Native VLAN	
	g. Update network configurations	

Q3. Read carefully and answers the following questions by using True or False:

a. A sub-interface in router-on-a-stick inter-VLAN routing is assigned the same VLAN ID as its physical interface.

b. In legacy inter-VLAN routing, VLANs communicate without the need for a router.

c. Switch port interfaces can be verified using the command show switch port.

d. Switch in VTP server mode can receive VLAN updates but cannot propagate them to other switches. Answer: (Server mode can propagate VLAN updates to other switches).

e. Redundancy in a network refers to having multiple paths to ensure continuous connectivity in case of a failure.

Practical assessment

A company named "Tech Innovators" has expanded its operations and needs a robust network infrastructure to support its growing workforce and operations. The company requires a VLAN-based design to segment traffic for different departments, ensure redundancy, and provide inter-departmental communication. The network should also incorporate link aggregation for increased bandwidth and redundancy, along with VRRP for gateway redundancy.

Objective: To configure a network that meets the requirements outlined below, students will complete a series of tasks integrating VLANs, VTP, inter-VLAN routing, STP, link aggregation, and VRRP.

Task 1: VLAN Creation and Configuration

Instructions:

1. **Create two VLANs on Switch A:** VLAN 10 (HR) and VLAN 20 (Sales).
    - VLAN 10 Name: HR
    - VLAN 20 Name: Sales
2. **Assign the following ports to the corresponding VLANs:**
    - Assign ports Fa0/1 - Fa0/5 to VLAN 10.
    - Assign ports Fa0/6 - Fa0/10 to VLAN 20.
3. **Verify VLAN creation and port assignments.**

Task 2: Configure VTP and Verify

1. **Configure Switch A as a VTP server:**
    - VTP domain: CorpNet
    - VTP mode: Server
2. **Configure Switch B as a VTP client:**
    - VTP domain: CorpNet
    - VTP mode: Client
3. **Verify that the VLANs configured on Switch A are propagated to Switch B.**

Task 3: Inter-VLAN Routing using Router-on-a-Stick

Instructions:

1. **Configure subinterfaces on the router (Router0):**

- Subinterface Fa0/0.10 for VLAN 10 with IP address 192.168.10.1/24.
- Subinterface Fa0/0.20 for VLAN 20 with IP address 192.168.20.1/24.
- Enable dot1q encapsulation for each subinterface.

2. **Configure hosts in VLAN 10 and VLAN 20 with the following IP addresses:**
   - VLAN 10 host: 192.168.10.10/24, Gateway: 192.168.10.1.
   - VLAN 20 host: 192.168.20.10/24, Gateway: 192.168.20.1.
3. **Verify communication between the two hosts using ping.**

Task 4: Configure and Verify STP (Spanning Tree Protocol)

Task 5: Configure VRRP for Router Redundancy

Instructions:

1. **Configure VRRP on Router0 and Router1:**
   - Assign a virtual IP address 192.168.10.254 for VRRP.
   - Router0 should be the VRRP master with priority 110.
   - Router1 should act as the VRRP backup with default priority.
2. **Verify that Router0 is the master and Router1 is the backup.**
3. **Simulate a failure on Router0 and verify that Router1 takes over as the master.**

END

References

Carter, J. (2021). *Comprehensive Guide to WAN Maintenance Reports.* San Francisco: NetworkTech Publishing.

Carter, O. (2020). *Evaluating Hardware Status for Network Performance.* Seattle: Network Engineering Press.

Clark, J. (2021). *Guide to Installing Network Monitoring Tools.* Los Angeles: Network Solutions Press.

Doe, J. (2020). *Effective Bandwidth Management. .* Miami: Tech Insights Publishing.

Evans, E. (2021). *Customizing Network Monitoring Dashboards. .* New York: IT Solutions Publishing.

G, B. (2003). *Hardware Maintenance in WAN.* Chicago: TechSolutions Publishing.

Johnson, E. (2022). *Troubleshoot network configurations and Update network configurations.* London:: Global Network Publishing.

Mitchell, L. (2022). *Elaborating a Maintenance Report for WAN.* New York: TechPress.

spanning tree protocol explained with examples. (n.d.). Retrieved from www.computernetworkingnotes.com: https://www.computernetworkingnotes.com/ccna-study-guide/stp-spanning-tree-protocol-explained-with-examples.html

Types of spanning tree protocol. (n.d.). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/types-of-spanning-tree-protocol-stp/

www.geeksforgeeks.org. (n.d.). Retrieved from Virtual LAN: https://www.geeksforgeeks.org/virtual-lan-vlan/


PERFOM
IP ADDERSING
PERFOM
IP ADDESSING
NAT
NAT
NAT
OSA
IPV4
IPV6
INTERNOR
TRANSLEATION
ENTANCED
SHORTTESTH
PATH FIRST

Indicative contents
3.1 Perform IP addressing.
3.2 Configuration of NAT.
3.3 Configure routing protocols.
3.4 Configuration of EIGRP IPV4 & IPV6
3.5 Configuration of OSPF IPV4 & IPV6
3.6 Configuration of router security

Key Competencies for Learning Outcome 3: Apply Router Configurations

Knowledge	Skills	Attitudes
• Description of IP addressing. • Description of Network Address Translation (NAT). • Description of routing protocols in a network. • Description of EIGRP IPv4 & IPv6. • Description of OSPF for IPv4&IPv6. • Description of router security.	• Calculating and troubleshooting VLSM. • Summarizing roote. • Configuring DHCP server. • Configuring Network Address Translation (NAT). • Configuring routing protocols. • Configuring EIGRP IPv4 & IPv6. • Verifying and troubleshooting Identifying and EIGRP issues. • Configuring OSPF for IPv4&IPv6. • Configuring access control list. • Configuring filtering devices.	• Being a proactive approach to addressing and troubleshooting . • Being Careful while configuring. • Having critical thinking while configuring. • Being Accountability for the configuration and management of routing protocols, understanding their impact on network performance and reliability.

	● Testing router security.	

Duration: 25 hrs

Learning outcome 3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly IP addressing as used in router configurations.
2. Calculate correctly VLSM based on WAN requirements.
3. Troubleshoot properly VLSM based on WAN requirements.
4. Configure properly DHCP server based on WAN requirements.
5. Describe clearly Network Address Translation (NAT) used in WAN.
6. Configure properly Network Address Translation (NAT) based on the design.
7. Describe clearly routing protocols as used in WAN.
8. Configure properly routing protocols based on the design.
9. Describe clearly EIGRP and OSPF IPv4 & IPv6 as used in WAN.
10. Configure properly EIGRP and OSPF IPv4 & IPv6 based on the Design.
11. Describe clearly security router used in WAN.
12. Configure and test properly WAN security tools based on organization's measures.

Resources

Equipment	Tools	Materials
• Routers • Switches • Hubs • Repeaters • Gateways • •Bridges • Modems • Rack Mount • Access Point • Computer	• Cable tester • Crimping tool • Wire cutter • Striping tool • Putty • Terra term • CISCO Packet tracer	• CAT5 • CAT6 or CAT6e • Fiber optic cables • Coaxial Cables • BNC • RJ45 • RJ11

• Multi-Layer Switch		

Indicative content 3.1: Perform IP Addressing

Duration: 4 hrs

Theoretical Activity 3.1.1: Description of IP addressing

Tasks:

1: Read carefully and answer the following questions:

i. What do you understand by the term IP address?

ii. Describe class full IP addressing.

iii. What is classless IP addressing?

iv. Describe IP address scheme.

v. What is VLSM?

vi. Describe classless interdomain routing?

2. Write answers on paper flipchart, blackboard or whiteboard.

3. Present the finding to the whole class.

4. Ask questions for clarification if needed.

5. Read the Key readings 3.1.1 in trainee manuals.

Key readings 3.1.1: Description of IP addressing.

Definition of key terms:

An IP address, or Internet Protocol address, is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main purposes: identifying the host or network interface and providing the location of the host in the network.

Classful IP addressing refers to the original method of dividing IP addresses into different classes based on predefined ranges. This system was used to allocate IP addresses before the introduction of Classless Inter-Domain Routing (CIDR), which offers more flexibility. Here's a detailed look at classful IP addressing:

1. Class full IP Addressing Overview

In classfull IP addressing, IP addresses are divided into five classes (A, B, C, D, and E) based on their leading bits and intended use. Each class has a specific range of addresses and a default subnet mask.

Class A

Address Range: 1.0.0.0 to 126.0.0.0

Default Subnet Mask: 255.0.0.0 (or /8)

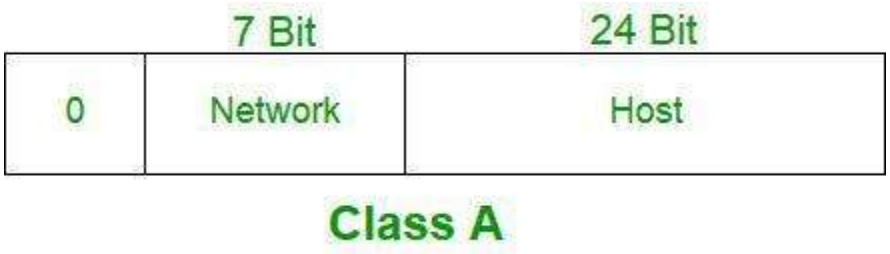
Number of Networks: 128 (including 0.0.0.0 and 127.0.0.0)

Number of Hosts per Network: Approximately 16 million

Leading Bits: 0 (binary)

Usage: Large networks, such as major corporations or ISPs.

Example Address: 10.0.0.1



Class A

Class B

Address Range: 128.0.0.0 to 191.255.0.0

Default Subnet Mask: 255.255.0.0 (or /16)

Number of Networks: 16,384

Number of Hosts per Network: Approximately 65,000

Leading Bits: 10 (binary)

Usage: Medium to large networks, such as universities or large businesses.

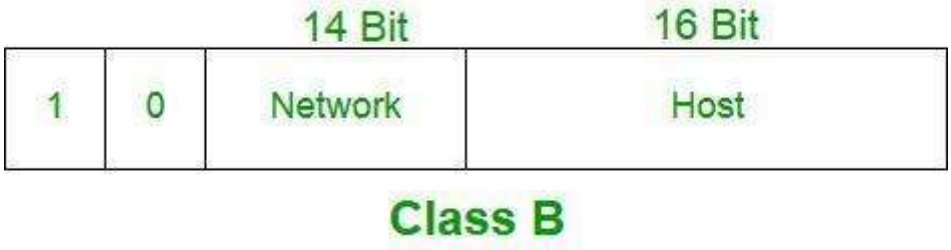
Example Address: 172.16.0.1

The 16 bits of host ID are used to determine the host in any network.

Class B has a total of:

2^14 = 16384 network address

2^16 – 2 = 65534 host address



Class B

Class C

Address Range: 192.0.0.0 to 223.255.255.0

Default Subnet Mask: 255.255.255.0 (or /24)

Number of Networks: 2,097,152

Number of Hosts per Network: 254

Leading Bits: 110 (binary)

Usage: Small networks, such as small businesses or home networks.

Example Address: 192.168.1.1

Class C has a total of:

2. 2^21 = 2097152 network address
3. 2^8 – 2 = 254 host address

IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.

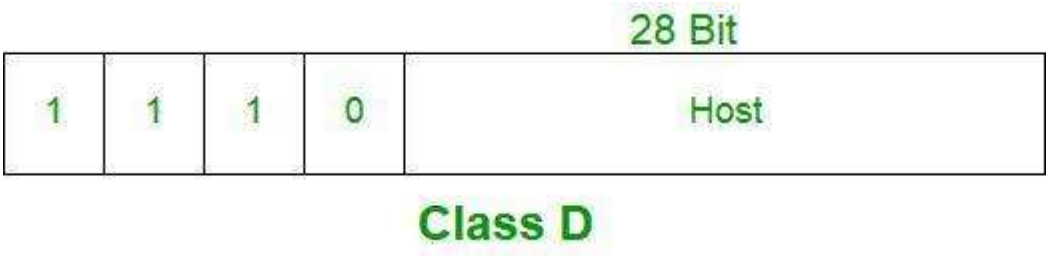
Class C

Class D (Multicast)

IP address belonging to class D is reserved for multi-casting.

The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask.



Class D

Address Range: 224.0.0.0 to 239.255.255.255

Default Subnet Mask: Not applicable

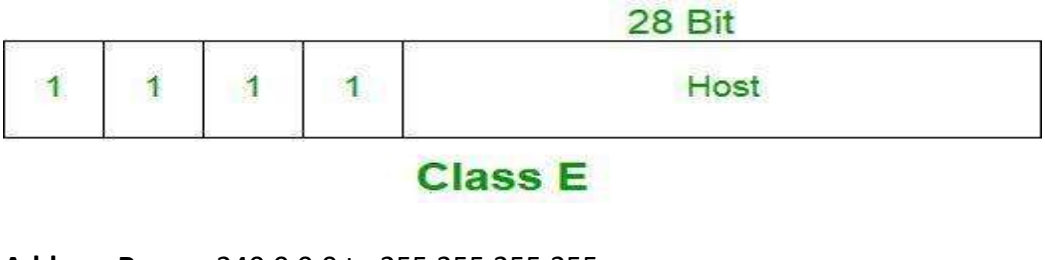
Usage: Used for multicast groups (sending data to multiple hosts).

Leading Bits: 1110 (binary)

Example Address: 224.0.0.1

Class E (Experimental)

IP addresses belonging to class E are reserved for experimental and research purposes. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Class E

Address Range: 240.0.0.0 to 255.255.255.255

Default Subnet Mask: Not applicable

Usage: Reserved for experimental purposes and future use.

Leading Bits: 1111 (binary)

Example Address: 250.0.0.1

Range of Special IP Addresses

127.0.0.0– 169.254.0.16 : Link-local addresses

127.0.0.0 – 127.255.255.255 : Loop-back addresses

0.0.0.0 – 0.0.0.8: used to communicate within the current network.

2. Classless Ip addressing

Classless IP addressing, also known as Classless Inter-Domain Routing (CIDR), is a method used to allocate IP addresses more flexibly and efficiently compared to the traditional classful addressing system. CIDR was introduced to overcome the limitations of classful addressing, such as inefficient IP address usage and the large size of routing tables.

Key Concepts of Classless IP Addressing (CIDR)

- **CIDR Notation**

Format: CIDR notation combines an IP address with a prefix length to indicate the subnet mask. It's written as IP_Address/Prefix_Length.

Example: 192.168.1.0/24

192.168.1.0 is the network address.

/24 denotes that the first 24 bits are used for the network portion.

- **Prefix Length**

The prefix length specifies how many bits of the IP address are used to identify the network, with the remaining bits used for host addresses.

Example: In 192.168.1.0/24, /24 means the first 24 bits are the network portion, leaving 8 bits for hosts.

- **Variable-Length Subnet Masking (VLSM)**

CIDR allows for subnetting with variable-length subnet masks, which means different subnets can have different sizes based on the number of addresses needed.

Example: A /24 subnet provides 256 IP addresses, while a /26 subnet provides 64 IP addresses.

- **Address Aggregation**

CIDR supports address aggregation (or supernetting), where multiple IP address ranges can be combined into a single, summarized route. This reduces the number of entries in routing tables.

Example: Instead of advertising 192.168.1.0/24 and 192.168.2.0/24 separately, a single route for 192.168.0.0/22 can be used to cover both ranges.

3.IP address scheme

An IP address scheme refers to the structured plan or method used to assign IP addresses within a network. It involves designing how IP addresses are distributed among devices, subnetworks, and network segments to ensure efficient communication, proper address management, and optimized network performance. Here's a detailed look at IP address schemes:

3.1. Components of an IP Address Scheme

- **IP Address Allocation**

Public IP Addresses: Assigned by Internet Service Providers (ISPs) and used to identify devices on the global internet. These addresses are routable across the internet.

Private IP Addresses: Used within private networks (e.g., home or corporate networks). These addresses are not routable on the public internet and are defined by specific ranges:

Class A Private Range: 10.0.0.0 to 10.255.255.255

Class B Private Range: 172.16.0.0 to 172.31.255.255

Class C Private Range: 192.168.0.0 to 192.168.255.255

- **Subnetting**

Subnet Mask: Defines which portion of an IP address identifies the network and which part identifies the host. For example, a /24 subnet mask means the first 24 bits are used for the network portion, leaving 8 bits for host addresses.

Subnetting involves dividing a larger network into smaller sub-networks to optimize address usage and improve network performance.

3.2. Address Allocation Method

Static IP Addressing: Addresses are manually assigned to devices. This method is used for servers, printers, and other devices that need a fixed IP address.

Dynamic IP Addressing: Addresses are assigned automatically from a pool of available addresses using DHCP (Dynamic Host Configuration Protocol). This method is commonly used for client devices like computers and smartphones.

Example IP Address Scheme

You have a small company with 3 departments and need to create a network with public and private IP addresses.

Public IP Address:

Public IP Range: Assigned by ISP (e.g., 203.0.113.0/24 for internet-facing services).

Private IP Addressing:

Network: 192.168.1.0/24

Subnet 1 (HR Department): 192.168.1.0/26 (64 addresses, 62 usable)

Subnet 2 (IT Department): 192.168.1.64/26 (64 addresses, 62 usable)

Subnet 3 (Sales Department): 192.168.1.128/26 (64 addresses, 62 usable)

4. Classless Inter-Domain Routing (CIDR)

4.1.Description of CIDR

Classless Inter-Domain Routing (CIDR) is a method used in IP networks to improve the flexibility and efficiency of IP address allocation and routing. Introduced in the 1990s, CIDR replaced the older class full network addressing system. Here's a detailed overview:

Key Concepts of CIDR:

- **IP Address and Subnet Notation:**
  - **CIDR Notation**: IP addresses are written with a suffix that specifies the network portion of the address. For example, 192.168.1.0/24:
    - 192.168.1.0 is the base IP address.
    - /24 denotes that the first 24 bits are used for the network address, leaving the remaining bits for host addresses.
  - This notation allows for more precise definition of network sizes compared to the old class-based system.
- **Flexible Subnetting:**
  - Unlike the old classful system, which had fixed subnet sizes (Class A, B, C), CIDR allows variable-length subnet masking (VLSM). This means networks can be divided into subnets of any size, accommodating more or fewer hosts as needed.

Practical Activity 3.1.2: Calculating and troubleshooting VLSM.

Task:

1: Refer to the key reading 3.1.2 and perform the following task:

Suppose that you have a network 192.168.1.0/24 and need the following subnets:1 subnet for 50 hosts, 1 subnet for 30 hosts and 2 subnets for 10 hosts each. Calculate and troubleshoot VLSM.

2: Present the steps to calculate and troubleshoot VLSM.

3: Calculate and troubleshoot VLSM.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.1.2.

6: Perform the activity in the application of learning 3.1.

Key readings 3.1.2: Calculating and troubleshooting VLSM.

1. Steps for Basic VLSM Calculation:

1. Calculate Subnet Masks:

For 50 hosts: Need 64 addresses (next power of 2), so /26 mask.

For 30 hosts: Need 32 addresses, so /27 mask.

For 10 hosts: Need 16 addresses, so /28 mask.

2. Allocate Subnets:

/26 Subnet: 192.168.1.0/26 (range: 192.168.1.1 - 192.168.1.62, broadcast: 192.168.1.63)

/27 Subnet: 192.168.1.64/27 (range: 192.168.1.65 - 192.168.1.94, broadcast: 192.168.1.95)

/28 Subnet: 192.168.1.96/28 (range: 192.168.1.97 - 192.168.1.110, broadcast: 192.168.1.111)

/28 Subnet: 192.168.1.112/28 (range: 192.168.1.113 - 192.168.1.126, broadcast: 192.168.1.127)

2.Troubleshooting VLSM:

Here are some common troubleshooting steps if you run into issues with VLSM:

- **Verify Subnet Calculations:**
  - Ensure subnet sizes match the number of required hosts.
  - Double-check subnet mask calculations and address allocations.
- **Check Overlapping Subnets:**

Confirm that subnets do not overlap. Each subnet should have a unique range of IP addresses.

- **Review IP Address Assignment:**

  Make sure all devices are assigned IP addresses within the correct subnet and that there are no address conflicts.

- **Verify Routing Configuration:**

  Ensure that routers have proper routes for each subnet. Update routing tables if necessary.

- **Check for Proper Mask Application:**

  Ensure that subnet masks are correctly applied to the interfaces. An incorrect mask can lead to network communication issues.

- **Test Connectivity:**

  Use tools like ping and traceroute to test connectivity between devices in different subnets. This can help identify issues with routing or address assignments.

Practical Activity 3.1.3: Summarizing route in Router.

Task:

1: Refer to the key reading 3.1.3 and perform the following task:

let's consider the following IP subnets:192.168.1.0/24, 192.168.2.0/24 ,192.168.3.0/24. You are asked to determine the IP address ranges you want to summarize.

2: Presents the steps to Summarizing route in Router.

3: Summarize network.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.1.3.

6: Perform the activity in the application of learning 3.1.

Key readings 3.1.3: Summarizing route in Router.

1. Route Summarization

Route summarization (or route aggregation) is a technique used to consolidate multiple IP address ranges into a single, larger route. This reduces the number of entries in a routing table and simplifies network management. Here's a step-by-step guide to determine route summarization, with an illustrative example.

Steps for Route Summarization

1. Identify the IP Address Ranges

Determine the IP address ranges you want to summarize. For example, let's consider the following IP subnets:

- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

2. Convert IP Addresses to Binary

Convert each subnet's network address into its binary form:

- 192.168.1.0/24 = 11000000.10101000.00000001.00000000
- 192.168.2.0/24 = 11000000.10101000.00000010.00000000
- 192.168.3.0/24 = 11000000.10101000.00000011.00000000

3. Find the Common Prefix

Compare the binary representations to find the longest common prefix. The prefix length is determined by counting the number of matching bits from the beginning:

- 11000000.10101000.00000001.00000000 (192.168.1.0)
- 11000000.10101000.00000010.00000000 (192.168.2.0)
- 11000000.10101000.00000011.00000000 (192.168.3.0)

The common prefix is 11000000.10101000.000000, which is 22 bits long.

4. Determine the Summary Address and Mask

The summary address is found by using the common prefix and setting all remaining bits to zero. The prefix length is determined from the common prefix:

- Common prefix length: 22 bits
- Summary address: 192.168.0.0 (binary: 11000000.10101000.00000000.00000000)
- CIDR notation: /22

5. Verify the Summarized Range

Check that the summary address range includes all original subnets:

- **Summary Range**: 192.168.0.0/22
  - Network address: 192.168.0.0
  - Broadcast address: 192.168.3.255
  - This range covers: 192.168.0.0 to 192.168.3.255

Summary Address Range Validates:

- Includes 192.168.1.0/24
- Includes 192.168.2.0/24
- Includes 192.168.3.0/24

Practical Activity 3.1.4: Configuring DHCP Server.

Task:

1: Refer to the key reading 3.1.4 and perform the following task:

You have a small office network with a DHCP server that needs to assign IP addresses to the computers. Configure DHCP Server to obtain an IP address automatically to the client computers.

2: Presents the steps to Configure DHCP Server.

3: Configure DHCP server and enabling host to get IP address automatically.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.1.4.

6: Perform the activity in the application of learning 3.1.

Key readings 3.1.4: Configuring DHCP Server.

Configuring a DHCP (Dynamic Host Configuration Protocol) server on a router allows the router to automatically assign IP addresses and other network configuration details to devices on the network. Here's a step-by-step guide to configuring a DHCP server on a router, using a common example of a Cisco router. The process may vary slightly depending on the router's make and model, but the general principles are similar.

Steps to Configure DHCP on a Cisco Router

Step1: Access the Router:

- Connect to the router via a console cable or telnet/SSH.
- Enter the router's enable mode by typing enable.
- Enter global configuration mode by typing configure terminal.

```
Router>enable
Router#configure terminal
```

Step2: Create a DHCP Pool:

- A DHCP pool defines the range of IP addresses that the router can assign to devices.
- Use the ip dhcp pool command to create a pool:
- ip dhcp pool POOL_NAME
- Replace POOL_NAME with a descriptive name for your DHCP pool.

```
Router(config)#ip dhcp pool Left_Network
```

Step3: Configure DHCP Pool Parameters:

Set the network address and netmask for the pool:

- network 192.168.1.0 255.255.255.0
- Set the default gateway address:
- default-router 192.168.1.1

Set the DNS server addresses:

- dns-server 192.168.1.2

Configure other options as needed, such as lease time, exclusion ranges, and option 82.

```
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.2
Router(dhcp-config)#option 150 ip 192.168.1.3
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#exit
```

Step4: Assign the DHCP Pool to an Interface:

Use the interface command to specify the interface that will act as the DHCP server:

- interface GigabitEthernet0/0

Enable DHCP on the interface and assign the DHCP pool:

- ip address dhcp ip dhcp pool POOL_NAME

Example Configuration

configure terminal

interface GigabitEthernet0/0

ip address dhcp

ip dhcp pool MY_POOL

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

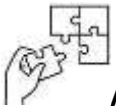
dns-server 8.8.8.8 8.8.4.4

exit

Points to Remember

- In classful IP addressing, IP addresses are divided into five classes (A, B, C, D, and E) based on their leading bits and intended use. Each class has a specific range of addresses and a default subnet mask.

- Classless Inter-Domain Routing (CIDR) is a method used to allocate IP addresses more flexibly and efficiently compared to the traditional classful addressing system.
- Calculate Subnet Masks.
- Allocate Subnets.
- Verify Subnet Calculations.
- Check Overlapping Subnets.
- Review IP Address Assignment.
- Verify Routing Configuration.
- Check for Proper Mask Application.
- Identify the IP Address Ranges.
- Convert IP Addresses to Binary.
- Find the Common Prefix.
- Determine the Summary Address and Mask.
- Access the Router.
- Create a DHCP Pool.
- Configure DHCP Pool Parameters.
- Assign the DHCP Pool to an Interface.



Application of learning 3.1.

Suppose that ABC School's network has a router, a switch, and several computers. The network administrator wants to automate the process of assigning IP addresses to devices on the network. Configure those automatically process of assign IP addresses to devices on this network.

Indicative content 3.2: Configuration of NAT

Duration: 4 hrs

Theoretical Activity 3.2.1: Description of Network Address Translation (NAT).

Tasks:

1: Read carefully and answer the following questions:

i. What do you understand about NAT?

ii. What is the purpose of NAT?

iii. List at least five advantages and disadvantages of NAT

iv. Describe the types of NAT.

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 3.2.1 in trainee manuals.

Key readings 3.2.1. Description of Network Address Translation (NAT).

NAT (Network Address Translation) is a technique used to translate private IP addresses to public IP addresses. This allows multiple devices on a private network (like a home or office network) to share a single public IP address, providing internet access to all devices without requiring a unique public IP address for each one.

How NAT works:

Step1: Private IP Addresses: Devices on a private network are assigned private IP addresses that are not routable on the public internet.

Step2: Public IP Address: A single public IP address is assigned to the network's router or firewall.

Step2: Translation: When a device on the private network wants to communicate with a device on the public internet, the router or firewall translates the private IP address of the device to the public IP address.

Step3: Packet Forwarding: The translated packet is then forwarded to the public internet.

Step4: Reverse Translation: When a response packet is received from the public internet, the router or firewall translates the public IP address back to the original private IP address and forwards the packet to the correct device on the private network.

3.2.1. NAT (Network Address Translation) serves several key purposes

- **Conserving Public IP Addresses**

  There is a limited pool of publicly routable IP addresses. NAT allows multiple devices on a private network (like a home or office network) to share a single public IP address, conserving the available public addresses.

- **Enhanced Security**

  By hiding the private IP addresses of devices on a network, NAT helps to protect them from unauthorized access and attacks. This is because attackers cannot directly target specific devices by knowing their public IP addresses.

- **Simplified Network Management**

  NAT reduces the need to manage and assign multiple public IP addresses to devices on a network. This simplifies network administration and reduces the administrative overhead.

- **Supporting Multiple Devices**

  NAT enables multiple devices on a network to connect to the internet simultaneously, using a single public IP address. This is essential for households and small businesses with multiple devices that need internet access.

- **Enabling Internet Access**

  NAT is often used by internet service providers (ISPs) to provide internet access to their customers. By using NAT, ISPs can efficiently allocate public IP addresses

to their customers and provide internet connectivity to a large number of devices.

3.2.2. Advantages and disadvantages

Advantages:

- **Conserves Public IP Addresses**

  NAT allows multiple devices on a private network to share a single public IP address, conserving the limited pool of available public IP addresses.

- **Enhanced Security**

  By hiding the private IP addresses of devices on a network, NAT helps to protect them from unauthorized access and attacks.

- **Simplified Network Management**

  NAT reduces the need to manage and assign multiple public IP addresses to devices on a network, simplifying network administration.

- **Supports Multiple Devices**

  NAT enables multiple devices on a network to connect to the internet simultaneously, using a single public IP address.

- **Enables Internet Access**

  NAT is often used by internet service providers (ISPs) to provide internet access to their customers, allowing them to efficiently allocate public IP addresses.

Disadvantages:

- **Reduced Traceability**

  NAT can make it more difficult to trace network traffic and identify the source of network issues. This can complicate troubleshooting efforts.

- **Potential for Interference**

NAT can sometimes interfere with certain applications or services that require direct communication between devices, such as peer-to-peer file sharing or VoIP.

- **Security Risks**

  While NAT can enhance security by hiding private IP addresses, it can also introduce new security risks, such as NAT traversal attacks.

- **Increased Network Complexity**

  NAT can add complexity to network configurations and management, especially in large or complex networks.

3.2.3. Types of NAT

- **Static NAT**

  Directly maps a public IP address to a private IP address on a one-to-one basis. This means that a specific public IP address is always associated with a particular private IP address.

  Ideal for servers that require a fixed public IP address, such as web servers, email servers, and FTP servers. It provides a predictable and consistent way for clients to connect to these services.

- **Dynamic NAT**

  Dynamically maps a public IP address to a private IP address on a one-to-one basis, but the mapping can change over time. This allows multiple devices on a private network to share a limited number of public IP addresses.

  Suitable for networks with a limited number of public IP addresses, such as home networks or small businesses. It efficiently manages the allocation of public IP addresses among devices.

- **Port Address Translation (PAT) or NAT Overload**

  Maps multiple private IP addresses to a single public IP address using different port numbers. This allows many devices on a private network to share a single public IP address, conserving public IP address space.

Commonly used in large networks, such as corporate networks or ISPs, where there is a limited supply of public IP addresses. It enables many devices to connect to the internet simultaneously using a single public IP address.

- **NAT64**

  Translates IPv6 addresses to IPv4 addresses, allowing IPv6-enabled devices to communicate with IPv4-only devices. This is a transitional solution to bridge the gap between the two IP address formats while IPv6 adoption is still ongoing.

  Useful for networks that need to support both IPv4 and IPv6 devices, such as large data centers or ISPs. It allows for seamless communication between devices using different IP address formats.

Practical Activity 3.2.2: Configuring NAT.

Task:

1: Refer to the key reading 3.2.2 and perform the following task:

You have a home network with several devices (computers, smartphones, smart TVs) that need to access the internet through a single public IP address provided by your ISP. Configuring NAT (Network Address Translation) allows multiple devices on a local network to share a single public IP address for accessing the internet.

2: Presents the steps to Configuring NAT (Network Address Translation).

3: Configure NAT.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.2.2.

6: Perform the activity in the application of learning 3.2.

Key readings 3.2.2: Configuring NAT.

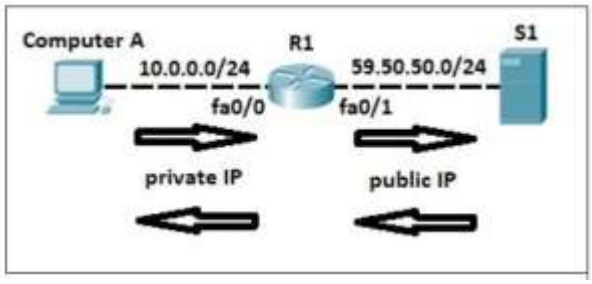
- **Static NAT**

With static NAT, routers or firewalls translate one private IP address to a single public IP address. Each private IP address is mapped to a single public IP address. Static NAT is not often used because it requires one public IP address for each private IP address.

To configure static NAT, three steps are required:

Step1. configure private/public IP address mapping by using the *ip nat inside source static PRIVATE_IP PUBLIC_IP* command.
Step2. configure the router's inside interface using the *ip nat inside* command
Step3. configure the router's outside interface using the *ip nat outside* command

Here is an example.



Computer A requests a web resource from S1. Computer A uses its private IP address when sending the request to router R1. Router R1 receives the request, changes the private IP address to the public one, and sends the request to S1. S1 responds to R1. R1 receives the response, looks it up in its NAT table, and changes the destination IP address to the private IP address of Computer A.

In the example above, we need to configure static NAT. To do that, the following commands are required on R1:

R1(config)#ip nat inside source static 10.0.0.2 59.50.50.1

R1(config)#interface fastEthernet 0/0

R1(config-if)#ip nat inside

R1(config-if)#interface fastEthernet 0/1

R1(config-if)#ip nat outside

Using the commands above, we have configured a static mapping between Computer A's private IP address of 10.0.0.2 and the router's R1 public IP address of 59.50.50.1. To check NAT, you can use the *show ip nat translations* command:

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 59.50.50.1:9 10.0.0.2:9 59.50.50.2:9 59.50.50.2:9

--- 59.50.50.1 10.0.0.2 --- ---

- **Dynamic NAT**

Unlike with static NAT, where you had to manually define a static mapping between a private and public address, **dynamic NAT** does the mapping of a local address to a global address happens dynamically. This means that the router dynamically picks an address from the global address pool that is not currently assigned. The dynamic entry stays in the NAT translations table as long as the

traffic is exchanged. The entry times out after a period of inactivity and the global IP address can be used for new translations.

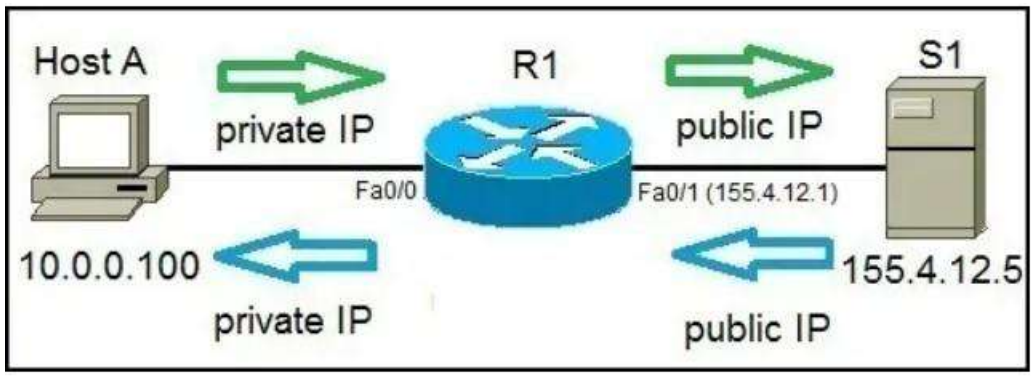
With dynamic NAT, you need to specify two sets of addresses on your Cisco router:

- the inside addresses that will be translated
- a pool of global addresses

To configure dynamic NAT, the following steps are required:

Step1: configure the router's inside interface using the *ip nat inside* command
Step2: configure the router's outside interface using the *ip nat outside* command
Step3: configure an ACL that has a list of the inside source addresses that will be translated
Step4: configure a pool of global IP addresses using the *ip nat pool NAME FIRST_IP_ADDRESS LAST_IP_ADDRESS netmask SUBNET_MASK* command
Step5: enable dynamic NAT with the *ip nat inside source list ACL_NUMBER pool NAME* global configuration command

Consider the following example:



Host A requests a web resource from a internet server S1. Host A uses its private IP address when sending the request to router R1. Router R1 receives the request, changes the private IP address to one of the available global addresses in the pool and sends the request to S1. S1 responds to R1. R1 receives the response, looks up in its NAT table and changes the destination IP address to the private IP address of Host A.

To configure dynamic NAT, the following commands are required on R1:

- **First we need to configure the router's inside and outside NAT interfaces:**

  R1(config)#int f0/0

  R1(config-if)#ip nat inside

  R1(config-if)#int f0/1

  R1(config-if)#ip nat outside

- **Next, we need to configure an ACL that will include a list of the inside source addresses that will be translated. In this example we want to translate all inside hosts on the 10.0.0.0/24 network:**

  R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255

- ✓ **We need to configure the pool of global (public) IP addresses available on the outside interface:**

  R1(config)#ip nat pool STUDY-CCNA_POOL 155.4.12.1 155.4.12.3 netmask 255.255.255.0

  The pool configured above consists of 3 addresses: 155.4.12.1, 155.4.12.2, and 155.4.12.3.

- ✓ **Lastly, we need to enable dynamic NAT:**

  R1(config)#ip nat inside source list 1 pool STUDY-CCNA_POOL

  The command above tells the router to translate all addresses specified in the *access list 1* to the pool of global addresses named *MY POOL*.

  You can list all NAT translations using the *show ip nat translations* command.

  Generate some traffic **from the PC to the server** first to test:

  C:\>ping 155.4.12.5

  Pinging 155.4.12.5 with 32 bytes of data:

  Reply from 155.4.12.5: bytes=32 time<1ms TTL=127

  Reply from 155.4.12.5: bytes=32 time=3ms TTL=127

  Reply from 155.4.12.5: bytes=32 time=1ms TTL=127

Reply from 155.4.12.5: bytes=32 time<1ms TTL=127

Ping statistics for 155.4.12.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 3ms, Average = 1ms

Then enter the show ip nat translations command quickly enough before the translation has timed out:

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 155.4.12.1:16 10.0.0.100:16 155.4.12.5:16 155.4.12.5:16

In the output above you can see that the translation has been made between the Host A's private IP address (*Inside local, 10.0.0.100*) to the first available public IP address from the pool (*Inside global, 155.4.12.1*) and it is connecting to the server on the outside (*Outside local and Outside global, 155.4.12.5*).

Points to Remember

- NAT (Network Address Translation) is a technique used to translate private IP addresses to public.
- NAT (Network Address Translation) serves several key purposes such as Conserving Public IP Addresses, Enhanced Security, Simplified Network Management, Supporting Multiple Devices, and Enabling Internet Access.
- Advantages of NAT like Conserves Public IP Addresses, Enhanced Security, Simplified Network Management, Supports Multiple Devices and Enables Internet Access
- Disadvantages of NAT like Increased Network Complexity, Security Risks, Potential for Interference and Reduced Traceability
- Types of NAT such as Static, Dynamic, Port Address Translation (PAT) or NAT Overload and NAT64.
- First, we need to configure the router's inside and outside NAT interfaces.
- We need to configure an ACL that will include a list of the inside source addresses that will be translated.
- We need to configure the pool of global (public) IP addresses available on the outside interface.

- we need to enable dynamic NAT.

Application of learning 3.2.

XYZ Company has several employees requires internet access and has a limited number of public IP addresses. The office network uses NAT to enable multiple computers and devices to access the internet through a single public IP address. NAT also helps in keeping the internal network secure by masking internal IP addresses and providing a basic layer of security against external threats.

Indicative content 3.3: Configure routing Protocols

Duration: 5 hrs

Theoretical Activity 3.3.1: Description of routing protocols in a network.

Tasks:

1: Read carefully and answer the following questions:

i. What is static route?
ii. What do you understand by default route?
iii. Describe dynamic routing protocol?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 3.3.1 in trainee manuals.

Key readings 3.3.1: Description of routing protocols in a network.

Before we delve into the configuration, it's essential to understand the different types of routing protocols:

- **Static Routing:** Manually configured routes. Best suited for small networks with predictable traffic patterns.
- **Default Routing:** A single route that directs all traffic not matching a specific route to a default gateway.
- **Dynamic Routing:** Automatically calculates and updates routes based on network

A dynamic routing protocol is a method used in networks to automatically discover and maintain the optimal paths for data transmission across routers.

Unlike static routing, where routes are manually configured, dynamic routing protocols adjust routes in real-time as network conditions change (e.g., link failures, congestion, or topology updates). conditions.

Types of Dynamic Routing Protocols:

1.Distance Vector Protocols:

Routers share routing table information with their neighbors.

Examples 1: RIP (Routing Information Protocol)

- **RIPv1 Operation:**

1. **Distance Vector Protocol:** RIPv1 is a distance vector routing protocol, meaning it uses hop count as it's metric. The maximum number of hops allowed is 15, with 16 considered unreachable.
2. **Periodic Updates:** RIPv1 routers send updates every 30 seconds to share routing information with neighboring routers.
3. **Broadcast Updates:** RIPv1 sends updates using broadcast addresses (e.g., 255.255.255.255), which can lead to inefficiencies.
4. **Classful Protocol:** RIPv1 does not support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR), meaning it can't recognize subnets or supernets.

- **RIPv1 Summarizations**

RIPv1 does not support manual route summarization, but it automatically summarizes routes at classful boundaries. To optimize the routing table, you can:

1. **Use Classful Networks**: Ensure that you use classful network addresses to take advantage of automatic summarization.
2. **Consider Route Filtering:** If necessary, filter certain routes to limit the information shared with neighbors, but this typically requires using other methods or protocols.

- **Processing RIP Update**

1. **Receive Update:** When a router receives a RIP update, it processes the update and adds any new routes to its routing table.
2. **Update Metric:** The router evaluates the hop count for each route and updates its metrics accordingly.
3. **Send Triggered Updates:** If the metric for a route changes significantly (e.g., a route becomes unreachable), the router may send a triggered update immediately rather than waiting for the next scheduled update.
4. **Hold-Down Timers:** If a route is marked as unreachable, the router enters a hold-down state to prevent fluctuations in routing information.
5. **Periodic Updates:** Every 30 seconds, the router sends out its routing table to

neighbors.

- ✓ **Interior Gateway Routing Protocol (IGRP)**

Interior Gateway Routing Protocol (IGRP) is a distance-vector routing protocol developed by Cisco. It is designed to manage routing within an autonomous system (AS) and was introduced to address some limitations of earlier protocols like RIP (Routing Information Protocol). Here's a deeper look at IGRP:

- ✓ **IGRP Operation**

1. Protocol Overview:

- **IGRP** is a distance-vector routing protocol developed by Cisco. It was designed to address some of the limitations of RIP (Routing Information Protocol).
- It uses a combination of metrics including bandwidth, delay, load, and reliability to determine the best path.

2. Metrics:

- IGRP calculates the best path based on a composite metric, which is derived from:
  - **Bandwidth:** The slowest bandwidth of the route.
  - **Delay:** The cumulative delay across the route.
  - **Load:** The current load on the route.
  - **Reliability:** The stability of the route.
- The metric is calculated as a weighted sum of these factors.

3. Update Mechanism:

- IGRP routers send routing updates every 90 seconds by default.
- Updates are sent to a multicast address (224.0.0.9) to reduce broadcast traffic.

4. Timers:

Update Timer: The interval at which routing updates are sent (90 seconds).

Invalid Timer: Time to consider a route invalid if no updates are received (270 seconds).

Hold-Down Timer: Time to wait before considering a route as potentially valid again after a route is deemed invalid (280 seconds).

Flush Timer: Time to remove the route from the routing table if it remains invalid (630 seconds).

- ✓ **Processing IGRP Updates**

Processing IGRP (Interior Gateway Routing Protocol) updates involves several steps to ensure that routing information is accurately exchanged and maintained across routers within an autonomous system. Here's a detailed look at how IGRP updates are processed:

Sending IGRP Updates

1. **Triggering Updates:**

IGRP routers send updates when there is a change in the network topology,

such as a new route being added or an existing route's metric changing. This is known as a triggered update.

2. **Periodic Updates:**

Regardless of network changes, IGRP routers also send periodic updates every 90 seconds by default. These updates contain the entire routing table and are sent to the multicast address 224.0.0.9.

3. **Update Packet Structure:**

- **Header:** Contains protocol information, including the command (request or response) and version number.
- **Route Entries:** Each entry includes:
  - **Destination Network:** The IP network being advertised.
  - **Metric:** The cost associated with reaching the destination, calculated using bandwidth, delay, load, and reliability.

Receiving IGRP Updates

1. **Receiving Process:**

- When a router receives an IGRP update, it performs several steps:

  - **Verify Packet:** Ensure the packet is correctly formatted and from a trusted source.
  - **Extract Routing Information:** Read the routing entries contained in the update.
  - **Update Routing Table:** Process each route entry to update the routing table.

2. **Route Comparison and Updates:**

- **Metric Comparison:** Compare the received metric with the existing metric for each route:
  - **Lower Metric:** If the new route's metric is lower than the current metric, the routing table is updated with the new route.

- **Higher Metric:** If the new route's metric is higher, it may not be updated.
- **Equal Metric:** If the metrics are equal, the route may be retained but not updated.

- **Route Addition:** If a route does not already exist in the table, it is added with the received metric.
- **Route Removal:** If a route is no longer advertised and its invalid timer expires, it is removed from the routing table.

3. **Timer Management:**

- **Invalid Timer:** If no updates are received for a route within the invalid timer period (270 seconds), the route is marked as invalid.
- **Hold-Down Timer:** During this period (280 seconds), the route is prevented from being immediately re-added to the routing table.
- **Flush Timer:** If the route remains invalid after the flush timer period (630 seconds), it is permanently removed from the routing table.

2. Link State Protocols: Routers have a complete view of the network's topology and calculate the best paths.

Examples include:

✓ **OSPF (Open Shortest Path First):** A more efficient and scalable protocol that uses Dijkstra's algorithm to determine the shortest path.

3.Hybrid Protocols: Combine features of both distance vector and link-state protocols. **Example:**

✓ **EIGRP (Enhanced Interior Gateway Routing Protocol):** Developed by Cisco, it optimizes path selection and convergence times while minimizing bandwidth usage.

Examples of widely used dynamic routing protocols include RIP, OSPF, EIGRP, and BGP (Border Gateway Protocol, typically used between ISPs or very large networks). These protocols are essential for large, dynamic environments where network topologies frequently change, such as in WANs.

Practical Activity 3.3.2: Configuring routing protocols

Task:

1: Refer to the key reading 3.3.2 and perform the following task:

You are asked to go to configure both static and dynamic routing protocols for managing how data packets travel across a network in a medium-sized enterprise with multiple interconnected networks, including two main offices in different cities and a remote branch office.

2: Presents the steps to Configure routing protocols.

3: Configure routing protocols.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.3.2.

6: Perform the activity in the application of learning 3.3.

Key readings 3.3.2: Configuring routing protocols

1.Static Routing Configuration

Step 1: Network Topology Design

- Identify all networks and subnets, including:

  - Main Office A
  - Main Office B
  - Remote Branch Office

Step 2: Access the Router

- Connect via console, SSH, or Telnet.
- Log in with appropriate credentials.

Step 3: Enter Configuration Mode

```
configure terminal
```

Step 4: Add Static Routes

- For each router at Main Office A and B, define static routes to other networks.
- Example:
  - **Main Office A:**

```
ip route 192.168.2.0 255.255.255.0 192.168.1.1  # To Main Office B
ip route 192.168.3.0 255.255.255.0 192.168.1.2  # To Remote Branch
```

  - **Main Office B**:

```
ip route 192.168.1.0 255.255.255.0 192.168.2.1  # To Main Offi
ip route 192.168.3.0 255.255.255.0 192.168.2.2  # To Remote Br
```

  - **Remote Branch Office**:

```
ip route 192.168.1.0 255.255.255.0 192.168.3.1  # To Main Of
ip route 192.168.2.0 255.255.255.0 192.168.3.2  # To Main Of
```

Step 5: Save Configuration:

```
write memory
```

2.Configuring Default Routing

Step 1: Determine the Default Route

- Typically points to the router that connects to the internet or a main network.

Step 2: Access the Router

- Log in to the router that will have the default route.

Step 3: Enter Configuration Mode

```
configure terminal
```

Step 4: Configure the Default Route

- Use the following command:

```
ip route 0.0.0.0 0.0.0.0 [next_hop_ip_address]
```

- **Example** for Main Office A:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1  # Points to ISP router
```

Step 5: Save Configuration:

```
write memory
```

3.Dynamic Routing Configuration

Step 1: Choose a Routing Protocol

- Select an appropriate dynamic routing protocol (e.g., OSPF, EIGRP). OSPF is widely used in enterprises.

Step 2: Access the Router

- Connect and log in as before.

Step 3: Enter Configuration Mode

```
configure terminal
```

Step 4: Configure OSPF

- For each router, enable OSPF and specify networks:

  - **Main Office A**:

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
```

  - **Main Office B**:

```
router ospf 1
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
```

  - **Remote Branch Office**:

```
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
```

Step 5: Save Configuration:

```
write memory
```

✓ **Routing Information Protocol version 1 (RIPv1)**

- **RIPv1 Configuration**

Step 1: Enter global configuration mode and then RIP configuration mode.

- Router(config)# router rip

Step 2: Use the **router rip** command to start RIP routing.

- Router(config-router)# version 1

Step 3: Define the networks that will participate in RIP routing using the network command.

- Router(config-router)# network <network_address>

Example configuration:

Router(config)# router rip

Router(config-router)# version 1

Router(config-router)# network 192.168.1.0

Router(config-router)# network 10.0.0.0

RIPv1 Verification.

Step1: viewing the routing table and verify the routes learned via RIP use the following command:

Router# show ip route rip.

RIP Database:

To see the routes stored in the RIP database use the following command:

Router# show ip rip database.

Neighbors:

To verify if RIP neighbors are correctly recognized use the following command:

Router# show ip rip neighbors.

Debugging Commands:

RIP Updates: To debug RIP updates and see RIP packet exchanges.

Router# debug ip rip

✓ **RIPv1 Troubleshooting**

➢ **Common Issues:**

- **Routing Loops:** Check if routing loops are present due to incorrect configurations or incorrect timers.

- **Connectivity Issues:** Verify if routers are physically connected and if interfaces are up.
- **Update Problems:** Ensure that routing updates are being sent and received. Check if there's a firewall or access list blocking RIP packets.

➢ **Troubleshooting Steps:**

Check Interface Status: Router# show ip interface brief

Verify RIP Configuration: Router# show running-config | include router rip

Check for Correct Updates: Router# debug ip rip

Check Routing Tables: Router# show ip route

➢ **Ensure Compatibility:**

Confirm that RIPv1 is used consistently across routers if there's a mix of RIPv1 and RIPv2 in the network.

✓ **IGRP Configuration**

1. Basic Configuration:

- Enter global configuration mode and then IGRP configuration mode.
- Define the IGRP autonomous system (AS) number.
- Specify the networks to be included in IGRP routing.

Router(config)# router igrp <AS_number>

Router(config-router)# network <network_address>

Example of configuration:

Router(config)# router igrp 10

Router(config-router)# network 192.168.1.0

Router(config-router)# network 10.0.0.0

2. Passive Interfaces:

To prevent IGRP updates from being sent out a specific interface, use the passive-interface command.

Example: Router(config-router)# passive-interface gig0/1

✓ **IGRP Summarizations**

1. Route Summarization:

- IGRP supports automatic route summarization on classful boundaries.
- To manually configure summarization, use the ip summary-address igrp command.

Example of Manual Summarization:

Router(config-router)# ip summary-address igrp 10 192.168.0.0 255.255.0.0

This command summarizes the 192.168.0.0 network into a single route with a subnet mask of 255.255.0.0.

IGRP Verification

1. Show Commands:

Routing Table: To view routes learned via IGR.: Router# show ip route igrp

IGRP Neighbors: To verify IGRP neighbor relationships: Router# show ip igrp neighbors

IGRP Database: To view the routes stored in the IGRP database: Router# show ip igrp database

2. Debugging Commands:

- **IGRP Updates:** To debug IGRP updates and packet exchanges

Router# debug ip igrp transactions

Router# debug ip igrp events

IGRP Troubleshooting

Step 1. Identify Common Issues:

- **Routing Loops:** These may occur if there are misconfigurations or network topology changes.
- **Update Issues:** Problems with updates can occur due to network connectivity issues or misconfigurations.
- **Neighbor Issues:** Verify if IGRP neighbors are correctly recognized.

Step 2. Troubleshooting issues:

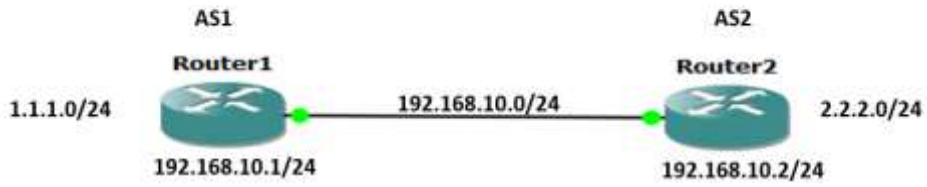
- **Check Interface Status:** Router# show ip interface brief
- **Verify IGRP Configuration:** Router# show running-config | include router igrp
- **Check for Correct Updates:** Router# debug ip igrp transactions

- **Verify Neighbor Relationships:** Router# show ip igrp neighbors
- **Check Routing Tables:** Router# show ip route

Note: Ensure that all routers in the IGRP AS have consistent configurations and are running the same IGRP version.

✓ **Configure BGP**

The network topology below will be used for configuring BGP. There are two BGP routers, Router1 and Router2, with 1.1.1.1 as loopback addresses for Router1 and 2.2.2.2 for Router2.



First, configure the physical and the loopback interfaces on both routers.

Router1(config)#interface Loopback 0

Router1(config-if)#ip address 1.1.1.1 255.255.255.0

Router1(config-if)#exit

Router1(config)#interface GigabitEthernet0/0

Router1(config-if)#ip address 192.168.10.1 255.255.255.0

Router2(config)#interface Loopback 0

Router2(config-if)#ip address 2.2.2.2 255.255.255.0

Router2(config-if)#exit

Router2(config)#interface GigabitEthernet0/0

Router2(config-if)#ip address 192.168.10.1 255.255.255.0

To configure BGP, initialize the BGP routing process using the command **'router bgp <as-number>'**. Optionally, a BGP router ID (RID) can be manually configured using the **'bgp router-id <router-id>'** command. If not, the RID dynamically uses the highest loopback address. If there's no active loopback interface, then the highest IP address will be used as the RID.

Next, specify the IP address and the AS number of the BGP neighbor using the **'neighbor <ip-address> remote-as <as-number>'** command under the BGP router configuration mode. MD5 authentication can also be enabled using the **'neighbor <ip-address> password <apassword>'** command.

```
Router1(config)#router bgp 1
Router1(config-router)#neighbor 192.168.10.2 remote-as 2
Router1(config-router)#neighbor 192.168.10.2 password STUDY-CCNP
Router2(config)#router bgp 2
Router2(config-router)#neighbor 192.168.10.1 remote-as 1
Router2(config-router)#neighbor 192.168.10.1 password STUDY-CCNP
```

Points to Remember

- Static Route Manually configured routes. Best suited for small networks with predictable traffic patterns.
- Default Routing: A single route that directs all traffic not matching a specific route to a default gateway.
- Types of Dynamic routing protocol are Distance Vector Protocols and Link State Protocols.

For Static Routing:

- Manual Configuration: Routes are manually configured by the network administrator.
- Predictability: Ensures fixed paths for data packets, useful for smaller, stable networks.
- Use Case: Suitable for simple routes between the two main offices and remote branch.

For Dynamic Routing:

- Automated Routing Decisions: Dynamic routing protocols automatically adjust routes based on network changes (failures, new links, etc.).
- Routing Protocols: Commonly used protocols include RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and EIGRP (Enhanced Interior Gateway Routing Protocol).

Default Routing:

- Simplified Routing for Unknown Networks: Directs all traffic for unknown destinations to a default route, usually towards a central router or gateway.

- Configuration: Commonly used in smaller branches or remote offices with a single exit point.

Application of learning 3.3.

ABC Retail Ltd is a growing retail chain with a head office in Kigali, two regional offices in Huye and Musanze, and several stores across various districts. Each office manages several local stores, and the entire network is connected via a WAN (Wide Area Network) to ensure centralized inventory management, sales reporting, and communication. After learning routing protocols, you are requested to configure static routing, dynamic routing, and default routing to ensure seamless communication and data packet travel between the head office, regional offices, and stores. choose appropriate routing protocols for different sections of the network based on size, reliability, and scalability.

Network Topology:

Head Office (Kigali): Network IP range 10.1.0.0/16

Regional Office 1 (Huye): Network IP range 10.2.0.0/16

Regional Office 2 (Musanze): Network IP range 10.3.0.0/16

Local Stores: Each store has a small LAN with unique subnets (e.g., 10.2.1.0/24 for Huye store 1, 10.3.1.0/24 for Musanze store 1).

WAN: Connections between the head office, regional offices, and stores are established through leased lines from an ISP.

Indicative content 3.4: Configuration of EIGRP IPV4 & IPV6

Duration: 4 hrs

Theoretical Activity 3.4.1: Description of EIGRP IPV4 & IPV6

Tasks:

1: Read carefully and answer the following questions:

i. Describe EIGRP network topology?

ii. What is EIGRP autonomous system numbers?

iii. Explain EIGRP router Id.

iv. What is passive interface?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 3.4.1 in trainee manuals.

Key readings 3.4.1: Description of EIGRP IPV4 & IPV6

✔ **EIGRP network topology**

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol that uses a distance vector routing algorithm and is designed to facilitate efficient routing within an autonomous system. Understanding EIGRP network topology involves several key concepts:

1. Basic Concepts

- **Neighbors**: Routers that are directly connected and can exchange EIGRP routing information.
- **AS (Autonomous System)**: A group of IP networks and routers under the control of one organization that presents a common routing policy.

2. Topology Representation

- **Topological Database (Topology Table)**: Each EIGRP router maintains a topology table that includes all known routes from neighbors. It uses this information to determine the best path to each destination.
- **Routing Table**: After calculating the best paths using the DUAL (Diffusing Update Algorithm), EIGRP installs routes in the routing table.

3. Metric Calculation

- EIGRP uses a composite metric based on:
- **Bandwidth**: The highest bandwidth of the path.
- **Delay**: The cumulative delay of the path.
- **Load**: Current traffic load on the link (optional).
- **Reliability**: The link's reliability (optional).

4. Topology Types

- **Flat Topology**: All routers are connected in a single tier with equal access.
- **Hierarchical Topology**: Routers are organized in a tiered structure, improving scalability and manageability.

5. EIGRP Operations

- **Hello Protocol**: EIGRP routers send hello packets to discover neighbors and maintain neighbor relationships.
- **Route Updates**: EIGRP uses partial updates, sending only changes rather than the entire routing table.

6. Route Redistribution

- EIGRP can redistribute routes from other routing protocols, which is useful in multi-protocol environments.

7.Configuration Considerations

- **Router Configuration**: EIGRP is configured on a router using the router eigrp [AS number] command.
- **Network Statements**: Define which interfaces will participate in EIGRP.

✔ **Autonomous System Numbers (ASNs)**

Autonomous System Numbers (ASNs) are unique identifiers assigned to each autonomous system (AS) in the Internet. An autonomous system is a collection of IP networks and routers under the control of a single organization that presents a common routing policy. ASNs are crucial for routing protocols like BGP (Border Gateway Protocol), enabling efficient routing between different ASes.

Types of ASNs

1. **Public ASNs**:

   Assigned by the Internet Assigned Numbers Authority (IANA) to organizations that need to connect to the Internet. Range: 1 to 65,535 (16-bit numbers). Some larger organizations may have multiple public ASNs.

2. **Private ASNs**:

   Used for internal routing within an organization's network and not advertised on the public Internet. Range: 64,512 to 65,535 (16-bit numbers) and also includes 4-byte private ASNs (10,000,000,000 to 10,000,000,000). Commonly used in enterprise environments.

✔ **Router EIGRP Commands**

✔ **EIGRP Router ID**

The **EIGRP Router ID** (RID) is a unique identifier assigned to each router participating in the EIGRP (Enhanced Interior Gateway Routing Protocol). This ID plays a critical role in ensuring that each router can be uniquely identified within an EIGRP network.

1. **Purpose**:

   The router ID is used to identify the source of routing updates and maintain neighbor relationships within the EIGRP topology.

2. **Format**:

   The router ID is represented as an IPv4 address (e.g., 1.1.1.1), but it does not need to be assigned to any interface on the router.

3. **Selection Process**: The router ID is chosen based on the following criteria:

   Manual Configuration: If explicitly configured, that ID will be used.

   router eigrp 100

   eigrp router-id 1.1.1.1

✔ **Passive interface**

In EIGRP (Enhanced Interior Gateway Routing Protocol), the **passive interface** command is used to control whether a specific interface sends EIGRP routing

updates or listens for them. Setting an interface to passive prevents EIGRP from sending hello packets on that interface while still allowing the router to receive routing updates from other routers.

1. **Purpose**:

   To limit EIGRP advertisements on certain interfaces, such as those connected to end devices or networks where routing updates are not necessary.

2. **Functionality**: When an interface is set as passive, the router will not send EIGRP hello packets or routing updates on that interface. However, it can still receive EIGRP updates from other routers on that interface.

   To configure an interface as passive in EIGRP, use the following command in the router configuration mode:

   router eigrp [AS number]

   passive-interface [interface]

   Examples

   router eigrp 100

   passive-interface GigabitEthernet0/1

Points to Remember

- EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol that uses a distance vector routing algorithm and is designed to facilitate efficient routing within an autonomous system.
- Hello Protocol: EIGRP routers send hello packets to discover neighbors and maintain neighbor relationships.
- Route Updates: EIGRP uses partial updates, sending only changes rather than the entire routing table.
- Autonomous System Numbers (ASNs) are unique identifiers assigned to each autonomous system (AS) in the Internet
- The EIGRP Router ID (RID) is a unique identifier assigned to each router participating in the EIGRP (Enhanced Interior Gateway Routing Protocol).
- In EIGRP (Enhanced Interior Gateway Routing Protocol), the passive interface command is used to control whether a specific interface sends EIGRP routing updates or listens for them.

- Verifying EIGRP (Enhanced Interior Gateway Routing Protocol) operation is crucial to ensure that routing is functioning correctly within your network.
- While configuring EIGRP remember to configure passive interface, Set EIGRP router ID, Set EIGRP metric and specify the network
- Ensure that you save your configuration from time to time.

Application of learning 3.4.

XYZ University has multiple buildings, including dormitories, classrooms, and administration offices. Network administrator use EIGRP to manage routing between the different routers installed in each building. If a router fails, EIGRP can instantly adjust, directing traffic through other buildings, which is critical for student access to online resources and administrative systems

Practical Activity 3.4.2: Configuring EIGRP IPV4 and IPV6

Task:

1: Refer to the key reading 3.4.2 and perform the following task:

A medium-sized corporation with multiple interconnected offices, including a headquarters, branch offices, Let's setup EIGRP on our branch router and our HQ router. And let's ensure that HQ has the ability to route to the 10.1.1.0/24 network and branch and send traffic over to 172.16.1.0/24. The network supports both IPv4 and IPv6 protocols.

2: Presents the steps to Configure EIGRP IPV4 & IPV6.

3: Configure EIGRP IPV4 & IPV6.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.4.2.

6: Perform the activity in the application of learning 3.4.

Key readings 3.4.2: Configuring EIGRP IPV4 and IPV6.

✔ **Router EIGRP Commands**

Here are some essential EIGRP commands for configuring EIGRP on Cisco routers:

Step1: Enable EIGRP: router eigrp [AS number]

Step2: Specify Networks: To include networks in EIGRP, use the network command. This command identifies which interfaces to include in the EIGRP process.

network [network address] [wildcard mask]

Step3: Set EIGRP Metrics (optional): You can manually configure the bandwidth, delay, load, or reliability if needed.

bandwidth [value]

delay [value]

Step4: Configure Passive Interfaces: To prevent EIGRP from sending updates on a specific interface:

passive-interface [interface]

Step5: Configure Passive Interfaces: (optional): To enable MD5 authentication for EIGRP:

key chain [name]

key [key number]

key-string [key string]

exit

interface [interface]

ip authentication mode eigrp [AS number] md5

ip authentication key-chain eigrp [AS number] [name]

Here's a basic example of configuring EIGRP on a router:

EIGRP configuration for IPv4

It's time for the exciting part of our Enhanced Interior Gateway Routing Protocol, or EIGRP, discussion, configuration. Let's setup EIGRP on our branch router and our HQ router. And let's ensure that HQ has the ability to route to the 10.1.1.0/24 network and branch, and send traffic over to 172.16.1.0/24.

Branch(config)#routereigrp 100
Branch(config-router)#network 10.0.0.0
Branch(config-router)#network 192.168.1.0

Branch(config-router)#passive-interface GigabitEthernet 0/0

HQ(config)#router eigrp 100
HQ(config-router)#network 172.16.1.0 0.0.0.255
HQ(config-router)#network 192.168.1.0 0.0.0.255

EIGRP for IPv6 configuration.

It's time for the exciting part of our Enhanced Interior Gateway Routing Protocol, or EIGRP, discussion, configuration. Let's setup EIGRP on our branch router and our HQ router. And let's ensure that HQ has the ability to route the **2001:DB8:D1A5:C900::1/64** network and branch , and send traffic over to **2001:DB8:D1A5:C900::2/64**.

Branch(config)#ipv6 unicast-routing

Branch(config)#ipv6 router eigrp 100

Branch(config-rtr)#no shutdown

Branch(config-rtr)#exit

Branch(config)#interface GigabitEthernet0/1

Branch(config-if)#ipv6 eigrp 100

HQ(config)#ipv6 unicast-routing
HQ(config)#ipv6 router eigrp 100
HQ(config-rtr)#no shutdown
HQ(config-rtr)#exit
HQ(config)#interface GigabitEthernet0/0
HQ(config-if)#ipv6 eigrp 100
HQ(config-if)#exit

HQ(config)#interface GigabitEthernet0/1
HQ(config-if)#ipv6 eigrp 100.

✔ **Verifying EIGRP (Enhanced Interior Gateway Routing Protocol)**

- This command displays information about the routers that are directly connected and participating in EIGRP: **HQ# show ip eigrp neighbors, Branch# show ip eigrp neighbors**
- This command shows the EIGRP topology table, which lists all the routes known to the EIGRP process: **HQ# show ip eigrp topology, Branch# show ip eigrp topology,**
- This command provides details about the routes that have been learned through EIGRP and installed in the routing table: **HQ# show ip route eigrp,**
- This command lists all the interfaces that are participating in EIGRP, along with their status (active or passive): **HQ# show ip eigrp interfaces**
- To display a summary of the EIGRP process and configuration: **HQ# show ip protocols**
- To see the metrics for routes learned via EIGRP: **HQ# show ip eigrp topology [network] [mask]**

✔ **Troubleshooting EIGRP (Enhanced Interior Gateway Routing Protocol)**

Troubleshooting EIGRP (Enhanced Interior Gateway Routing Protocol) issues involves several steps and techniques to identify and resolve problems. Here's a guide to help you troubleshoot common EIGRP issues:

Common EIGRP Issues

1. **Neighbor Relationships Not Established**

   Neighbors not listed in show ip eigrp neighbors.

   Example **: HQ#** show ip interface brief

2. **Incomplete or Missing Routes**

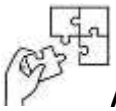
   Example: HQ# show ip eigrp topology.

3. **Flapping Neighbors**

   Example **: HQ#** debug eigrp neighbors

Points to Remember

- EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol that uses a distance vector routing algorithm and is designed to facilitate efficient routing within an autonomous system.
- Autonomous System Numbers (ASNs) are unique identifiers assigned to each autonomous system (AS) on the Internet.
- The EIGRP Router ID (RID) is a unique identifier assigned to each router participating in the EIGRP (Enhanced Interior Gateway Routing Protocol).
- In EIGRP (Enhanced Interior Gateway Routing Protocol), the passive interface command is used to control whether a specific interface sends EIGRP routing updates or listens for them.
- Enable EIGRP.
- Specify Networks.
- Set EIGRP Metrics.
- Configure Passive Interfaces.
- Configure Passive Interfaces.



Application of learning 3.4.

XYZ University has multiple buildings, including dormitories, classrooms, and administration offices. Network administrator use EIGRP to manage routing between the different routers installed in each building. If a router fails, EIGRP can instantly adjust, directing traffic through other buildings, which is critical for student access to online resources and administrative systems.

Indicative content 3.5: Configuration of OSPF for IPV4 & IPV6

Duration: 4 hrs

Practical Activity 3.5.1: Configuring OSPF V2 (single area OSPF).

Task:

1: Refer to the key reading 3.5.1 and perform the following task:

A large enterprise network with multiple interconnected offices, including a headquarters, regional branches, and a remote data center. The network requires a scalable and efficient routing protocol to handle both IPv4 and IPv6 traffic. You are asked to configure OSPF for IPv4 & IPv6. Based on this Network Information: Headquarters Network: 192.168.1.0/24, Branch Office Network: 192.168.2.0/24, Data Center Network: 192.168.3.0/24, WAN IP Range: 10.10.10.0/30 (HQ to Branch) and 10.10.20.0/30 (HQ to Data Center).

2: Presents the steps to Configure OSPF V2 single area..

3: Configure OSPF V2 single area.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.5.1.

6: Perform the activity in the application of learning 3.5.

Key readings 3.5.1: Configuring OSPF V2 (single area OSPF).

Step 1: Enable OSPF on Headquarters Router

1.Log in to the router at the headquarters (HQ).

2.Enter global configuration mode:

```
enable
configure terminal
```

3.Start the OSPF process and assign the process ID (for example, 1) :

```
router ospf 1
```

4.Configure the networks that will participate in OSPF, defining them to belong to Area 0 (the backbone area):

```
network 10.1.0.0 0.0.255.255 area 0
network <WAN IP Range> area 0
```

5.Exit OSPF configuration and save the changes:

```
end
write memory
```

Step 2: Enable OSPF on Regional Branch 1 Router

1.Log in to the router at Regional Branch 1.

2.Enter global configuration mode:

```
enable
configure terminal
```

3.Start the OSPF process and assign the process ID (for example, 1):

```
router ospf 1
```

4.Configure the networks that will participate in OSPF, defining them to belong to Area 0 (the backbone area):

```
network 10.2.0.0 0.0.255.255 area 0
network <WAN IP Range> area 0
```

5. Exit OSPF configuration and save the changes:

```
end
write memory
```

Step 3: Enable OSPF on Regional Branch 2 Router

1.Log in to the router at Regional Branch 1.

2.Enter global configuration mode:

```
enable
configure terminal
```

3.Start the OSPF process and assign the process ID (for example, 1):

```
router ospf 1
```

4.Configure the networks that will participate in OSPF, defining them to belong to Area 0 (the backbone area):

```
network 10.3.0.0 0.0.255.255 area 0
network <WAN IP Range> area 0
```

5. Exit OSPF configuration and save the changes:

Step 4: Enable OSPF on Remote Data Center Router

1.Log in to the router at Regional Branch 1.

2.Enter global configuration mode:

```
enable
configure terminal
```

3.Start the OSPF process and assign the process ID (for example, 1):

```
router ospf 1
```

4.Configure the networks that will participate in OSPF, defining them to belong to Area 0 (the backbone area):

```
network 10.4.0.0 0.0.255.255 area 0
network <WAN IP Range> area 0
```

5. Exit OSPF configuration and save the changes:

Practical Activity 3.5.2: Configuring OSPF V3 (Multi area OSPF).

Task:

1: Refer to the key reading 3.5.1 and perform the following task:

A large enterprise network with multiple interconnected offices, including a headquarters, regional branches, and a remote data center. The network requires a scalable and efficient routing protocol to handle both IPv4 and IPv6 traffic. You are asked to configure OSPF V2 single area Based on this Network Information: Headquarters Network: 2001:db8:1::/64, Branch Office Network: 2001:db8:2::/64, Data Center Network: 2001:db8:3::/64, WAN IP Range: 2001:db8:10::/126 (HQ to Branch) and 2001:db8:20::/126 (HQ to Data Center).

2: Presents the steps to configure OSPF V3 Multi area OSPF...

3: Configure OSPF V3 Multi area OSPF.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.5.2.

6: Perform the activity in the application of learning 3.5.

Key readings 3.5.2: Configuring OSPF V3 (single area OSPF).

Step 1: Enable OSPF on Headquarters Router

1.Log into the routers at the headquarters, branch office, and data center.

2.Enable IPv6 routing on each router:

```
enable
configure terminal
ipv6 unicast-routing
```

3. Enable OSPFv3 for IPv6 on all routers with OSPF process ID 1.

Step 2: OSPFv3 Configuration on Headquarters Router:

1.Enter OSPFv3 configuration mode:

```
ipv6 router ospf 1
```

2. Set the router ID (use an IPv4 address for simplicity):

```
router-id 1.1.1.1
```

3. Assign the networks to OSPF Area 0:

```
interface g0/0  (LAN interface)
ipv6 ospf 1 area 0
exit

interface g0/1 (WAN interface to Branch)
ipv6 ospf 1 area 0
exit

interface g0/2 (WAN interface to Data Center)
ipv6 ospf 1 area 0
exit
```

Step 3: OSPFv3 Configuration on Branch Office Router

1.Enter OSPFv3 configuration mode:

```
ipv6 router ospf 1
```

2.Set the router ID:

3. Assign the networks to OSPF Area 0:

```
interface g0/0 (LAN interface)
ipv6 ospf 1 area 0
exit

interface g0/1 (WAN interface to HQ)
ipv6 ospf 1 area 0
exit
```

Step 4: Step 3: OSPFv3 Configuration on Data Center Router

1. Enter OSPFv3 configuration mode:

```
ipv6 router ospf 1
```

2. Set the router ID:

```
router-id 3.3.3.3
```

3. Assign the networks to OSPF Area 0:

```
interface g0/0 (LAN interface)
ipv6 ospf 1 area 0
exit

interface g0/1 (WAN interface to HQ)
ipv6 ospf 1 area 0
exit
```

Points to Remember

- Log in to the router at Regional Branch 1.
- Enter global configuration mode.
- Start the OSPF process and assign the process ID (for example, 1).
- Configure the networks that will participate in OSPF, defining them to belong to Area 0 (the backbone area).
- Exit OSPF configuration and save the changes.

Application of learning 3.5.

XYZ Company has multiple branches across different cities. Each branch has its own local area network (LAN) and connects to a central data center. XYZ Company decides to use OSPF to efficiently manage routing within and between its branches and the data center. You task is to configure both OSPFv2&v3.

Indicative content 3.6: Configuration of Router Security

Duration: 4 hrs

Theoretical Activity 3.6.1: Description of router security.

Tasks:

1: Read carefully and answer the following questions:

i. What is ACL?

ii. Differentiate types of ACL

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 3.6.1 in trainee manuals.

Key readings 3.6.1: Description of router security.

An **Access Control List (ACL)** is a set of rules used to control network traffic and dictate who can access certain resources in a computer network. ACLs can be implemented on routers, switches, and firewalls to filter traffic based on predefined criteria. Here's a breakdown of their key features and functions:

1.Access Control List Types

1.1. Standard ACLs: Filter traffic based only on source IP addresses. These are simpler and typically used for basic access control.

1.2. Extended ACLs: Filter traffic based on both source and destination IP addresses, as well as protocols and port numbers. These provide more granular control.

2. Key Features of ACLs

- **Traffic Filtering**: ACLs can permit or deny traffic based on various attributes such as IP address, protocol type (TCP, UDP, and ICMP), port numbers, and other parameters.

- **Application**: ACLs can be applied to incoming and outgoing traffic on interfaces of routers and switches, controlling what traffic is allowed or denied.
- **Order of Processing**: ACL rules are processed in a sequential manner, from top to bottom. The first matching rule is applied, so the order of rules is crucial.
- **Default Behavior**: If no rules match, ACLs usually deny traffic by default,

  ensuring that unapproved traffic is blocked.

3.Benefits of Using ACLs

- **Enhanced Security:** By controlling which departments can access sensitive resources, the company reduces the risk of data breaches.
- **Traffic Management:** ACLs help manage network traffic, ensuring that guest users cannot disrupt internal operations.
- **Regulatory Compliance:** Limiting access to financial data helps the company comply with regulations such as GDPR or HIPAA.

Practical Activity 3.6.2: Configuring router security

Task:

1. Refer to the key reading 3.6.2 and perform the following task:

Implement security measures for an enterprise network with multiple interconnected networks (headquarters, branch offices, and a remote data center) to prevent unauthorized access and malicious activities.

2: Presents the steps to Configure and test router security.

3: Configure and test router security.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 3.6.2.

6: Perform the activity in the application of learning 3.6.

Key readings 3.6.2: Configuring router security.

1. Access List Configuration

Step 1: Create Access Control Lists (ACLs)

- Standard ACL (to permit or deny traffic based on source IP):

Example: Allow traffic from the headquarters (192.168.1.0/24) to the branch office (192.168.2.0/24).

```
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any
```

- Extended ACL (to permit or deny traffic based on source/destination IP and protocol):

Example: Deny HTTP access from the branch office to the internet.

```
access-list 100 deny tcp 192.168.2.0 0.0.0.255 any eq 80
access-list 100 permit ip any any
```

Step 2: Apply ACLs on Routers/Switches

Apply the ACL to the appropriate interface in the inbound or outbound direction.

```
interface g0/0
ip access-group 10 in
```

2. Configure Filtering Devices

a. Firewalls

Install and Configure Firewalls:

Use a dedicated firewall appliance or a software firewall.

Define rules to allow or block traffic based on the organizational policy.

Example rules:

Allow SSH (TCP 22) and HTTPS (TCP 443) traffic.

Block all other incoming traffic by default.

1. **Example Firewall Rule** (on a Cisco ASA):

```
access-list outside_access_in extended permit tcp any any eq 22
access-list outside_access_in extended permit tcp any any eq 443
access-list outside_access_in extended deny ip any any
```

b. Intrusion Prevention/Detection Systems (IPS/IDS)

1. **Deploy IPS/IDS**:
- Install an IPS/IDS appliance or use integrated solutions in firewalls.
- Configure policies to detect and prevent suspicious activities.
2. **Example Configuration** (on a Cisco IPS):

```
ip ips signature
```

3. **Set Alerting Mechanisms**:
- Configure alerts to notify administrators of detected threats.

c. Proxy Servers

1. **Implement Proxy Servers**:

- Use software like Squid or dedicated hardware proxies.

2. **Configure Filtering Policies**:

- Allow access to specific websites and block access to malicious sites.

3. **Example Configuration** (for Squid):

```
acl allowed_sites dstdomain .trustedwebsite.com
http_access allow allowed_sites
http_access deny all
```

d. Content Filtering Appliances

1. **Install Content Filtering Appliances**:

- Deploy appliances like Webroot or Cisco Umbrella.

2. **Configure Content Filtering Policies**:

- Restrict access to inappropriate content based on categories (e.g., gambling, adult content).

e. Load Balancers

1. **Deploy Load Balancers**:

- Use hardware load balancers like F5 or software solutions.

2. **Configure Security Features**:

- Implement SSL offloading and traffic inspection.

3. **Example Load Balancer Configuration** (F5):

```
create virtual myVirtual 10.10.10.10:80 {
    pool myPool
    profiles { http }
    ssl-profile mySSLProfile
}
```

3. Test Router Security

Step 1: Conduct Security Assessments

1. **Review Router Configurations**:
- Ensure strong passwords and updated firmware.
2. **Secure Routing Protocols**:
- Implement OSPF authentication if OSPF is used.

```
router ospf 1
area 0 authentication message-digest
```

Step 2: Perform Regular Security Audits

1. **Conduct Penetration Testing**:
- Schedule regular penetration tests to identify vulnerabilities.
- Use tools like Nmap or Nessus for vulnerability assessments.

Points to Remember

- An Access Control List (ACL) is a set of rules used to control network traffic and dictate who can access certain resources in a computer network.
- Types of access control list such as Standard ACLs: Filter traffic based only on source IP addresses and Extended ACLs: Filter traffic based on both source and destination IP addresses.
- Access List Configuration
- Configure Filtering Devices
- Test Router Security

Application of learning 3.6.

University of Tourism has a network with various departments, including HR, Finance, and IT. The University wants to ensure that sensitive information is protected and that only authorized users can access specific resource.

Learning outcome 3 end assessment

Theoretical assessment

1. Match the following IP addressing items with their solutions, write a letter to the number corresponding to the correct answer.

Answers	Column A	Column B
	1.An IP address scheme	**A.** is a method used in IP networks to improve the flexibility and efficiency of IP address allocation and routing.
	2.Variable Length Subnet Mask	**B**. allows the router to automatically assign IP addresses and other network configuration details to devices on the network.
	3.Classless Inter-Domain Routing (CIDR)	**C**. refers to the structured plan or method used to assign IP addresses within a network.
	4.Route summarization (or route aggregation)	**D**.is a technique used to consolidate multiple IP address ranges into a single, larger route.
	5.Configuring a DHCP server router	**E** . is a technique used in IP networking to efficiently allocate IP address space by allowing different subnets to have different subnet masks

2. Answer the following question using true or false

i. An autonomous system is a collection of IP networks and routers under the control of a single organization that presents a common routing policy.

ii. The router ID is used to identify the source of routing updates and maintain neighbor relationships within the EIGRP topology.

iii. Verifying EIGRP (Enhanced Interior Gateway Routing Protocol) operation is crucial to ensure that routing is functioning correctly within your network.

iv. Extended ACLs Filter traffic based only on source IP addresses. These are simpler and typically used for basic access control.

v. Standard ACLs Filter traffic based on both source and destination IP addresses, as well as protocols and port numbers. These provide more granular control.

3. Given the network address 192.168.10.0 using the subnet mask 255.255.255.192.**/ 5marks**

i. How many subnets?

ii. How many hosts per subnet?

iii. What are the valid subnets?

iv. What's the broadcast address for each subnet?

v. What are the valid hosts for each subnet?

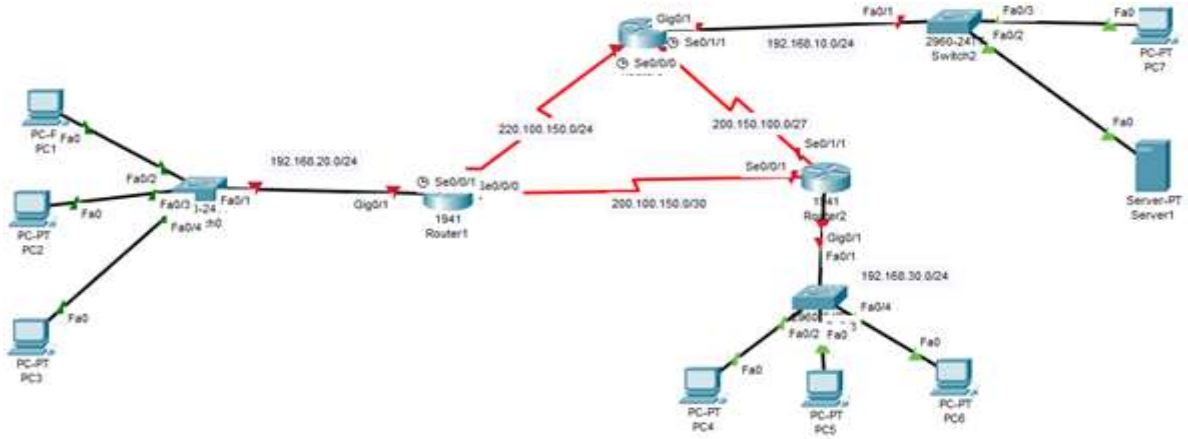
4. Given the IP address 172.74.34.168/29 for each row in table below, enter the values of that type of address

Type of address	**Enter last octet in binary**	**Enter last octet in decimal**	**Enter the full address in decimal**
Network			
Broadcast			
First usable host address			
last usable host address			

Practical assessment

ABCD Bank Headquarter located in Kigali city; it has two branches, one in Nyamagabe district and another on in Rubavu district. The employees from Nyamagabe branch no longer provide efficient services to the customers, but instead they are often busy doing unnecessary activities on the internet.

As Network technician; you are requested to make necessary configurations on appropriate router so that the users in Nyamagabe branch cannot communicate with the web server which is located at headquarter network as illustrated on the topology below. Make sure that other remaining users can access all the services. Use the given public and private IPs to accomplish the task expectedly. Use Static routing protocol for routing the packets..



Addressing Table

Device	Interface	IPV4 Address	Subnet Mask	Default Gateway
Router01	S0/0/0	220.150.50.1	255.255.255.0	N/A
	S0/1/1	200.150.100.1	255.255.255.224	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
Router02	S0/0/1	200.100.150.2	255.255.255.252	N/A
	S0/1/1	200.150.100.2	255.255.255.224	N/A
	G0/1	192.168.30.1	255.255.255.0	N/A
Router03	S0/0/0	220.150.50.2	255.255.255.0	N/A
	S0/0/1	200.100.150.1	255.255.255.252	N/A
	G0/1	192.168.20.1	255.255.255.0	N/A
PC-1	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC-2	NIC	192.168.20.11	255.255.255.0	192.168.20.1
PC-3	NIC	192.168.20.12	255.255.255.0	192.168.20.1
PC-4	NIC	192.168.30.10	255.255.255.0	192.168.30.1
PC-5	NIC	192.168.30.11	255.255.255.0	192.168.30.1
PC-6	NIC	192.168.30.12	255.255.255.0	192.168.30.1
PC-7	NIC	192.168.10.11	255.255.255.0	192.168.10.1
Server1	NIC	192.168.10.10	255.255.255.0	192.168.10.1

END

References

Baker, G. (2023). *Hardware Maintenance in WAN.* Chicago: TechSolutions Publishing.

Carter, J. (2021). *Comprehensive Guide to WAN Maintenance Reports.* San Francisco: NetworkTech Publishing.

Carter, O. (2020). *Evaluating Hardware Status for Network Performance.* Seattle: Network Engineering Press.

Clark, J. (2021). *Guide to Installing Network Monitoring Tools.* Los Angeles: Network Solutions Press.

Doe, J. (2020). *Effective Bandwidth Management.* Miami: Tech Insights Publishing.

Evans, E. (2021). *Customizing Network Monitoring Dashboards.* New York: IT Solutions Publishing.

Johnson, E. (2022). *Troubleshoot network configurations and Update network configurations.* London: Global Network Publishing.

Lee, D. (2020). *Monitoring Security Threats in WANs.* San Francisco: CyberTech Press.

Mitchell, L. (2022). *Elaborating a Maintenance Report for WAN.* New York : TechPress.

Thompson, D. (2021). *Assessing Hardware Connectivity in WAN.* Boston: Tech Systems Publishing.

Introduction to subnetting. (n.d.). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/introduction-to-subnetting/

IP address. (n.d.). Retrieved from www.javatpoint.com: https://www.javatpoint.com/ip-address

routing protocols. (n.d.). Retrieved from www.indeed.com: https://www.indeed.com/career-advice/career-development/routing-protocols

Routing protocols in computer network. (n.d.). Retrieved from www.javatpoint.com: https://www.javatpoint.com/routing-protocols-in-computer-networks


WAN
NETWORK
MAINTENANCE
MAINTENANCE
NETWORK

Indicative contents
4.1 Installation of WAN monitoring tools.
4.2 Performing hardware and software Preventive maintenance.
4.3 Performing Corrective maintenance.
4.4 Checking hardware and software functionalities.
4.5 Elaboration of maintenance report.

Key Competencies for Learning Outcome 4: Maintain WAN.

Knowledge	Skills	Attitudes
• Identification of WAN monitoring objectives. • Description of hardware and software preventive. maintenance in a Wide Area Network (WAN). • Description of corrective maintenance of WAN. • Explanation of maintenance reports in a Wide Area Network (WAN).	• Selecting WAN monitoring tools. • Installing and customizing WAN monitoring tools. • Applying WAN security monitoring. • Performing hardware and software preventive maintenance in a Wide Area Network (WAN). • Performing WAN corrective maintenance. • Checking hardware and software functionalities in a Wide Area Network (WAN).	• Being Analytical & Resourceful on WAN. • Being Careful attention to detail on WAN • Being protected on WAN. • Being Diligent & Preventive on WAN. • Being Clear Communicator & Organizer on WAN.

	● Elaborating maintenance reports in a Wide Area Network (WAN).	

Duration:25 hrs

Learning outcome 4 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify properly monitoring objectives as used in WAN.
2. Select correctly WAN monitoring tools based on environment.
3. Install properly suitable WAN monitoring tools according to WAN design.
4. Customize Properly suitable WAN monitoring tools according to WAN design.
5. Describe clearly WAN security monitoring as used in WAN.
6. Apply correctly WAN security monitoring based on oraganization's measures.
7. Describe clearly hardware and software preventive maintenance as used in WAN.
8. Perform correctly hardware and software Preventive maintenance based on identified WAN threats.
9. Check accurately hardware and software functionalities based on WAN infrastructure.
10. Describe correctly corrective maintenance as used in WAN.
11. Perform effectively corrective maintenance based on WAN vulnerabilities.
12. Describe clearly elements of maintenance report as used in WAN.
13. Elaborate Properly comprehensive maintenance report based on work done.

Resources

Equipment	Tools	Materials
• •Routers • •Switches • •Hubs • •Repeaters • •Gateways	• •Network Cable Testers • •SolarWinds Network Performance Monitor (NPM)	• •CAT5 • •CAT6 • •Fiber optic cables • •Coaxial Cables • •BNC

• Bridges • Modems • Uninterruptible Power Supply (Ups)	• Paessler PRTG Network Monitor • Wireshark	• RJ45 • RJ11

Indicative content 4.1: Installation of WAN Monitoring Tools

Duration: 7 hrs

Theoretical Activity 4.1.1: Description of WAN monitoring

Tasks:

1. Read carefully and answer the following questions:

   i. What do you understand by the term WAN Monitoring?
   ii. Identify the WAN Monitoring objectives?
   iii. What are WAN Monitoring Tools?

2. Write answers on paper, flipchart, blackboard or whiteboard.

3. Present the findings to the whole class.

4. Ask questions for clarification if needed.

5. Read the Key readings 4.1.1 in trainee manuals.

Key readings 4.1.1: Description of Installing WAN monitoring

1.Installation of WAN monitoring tools

Introduction: WAN monitoring refers to the continuous tracking and analysis of network performance across wide area networks (WAN). involves overseeing the health, performance, and security of a wide area network (WAN) to ensure it operates efficiently and reliably.

This process is crucial for identifying issues such as bottlenecks, outages, and security threats in real time.

1.1.Identify Monitoring Objectives

1.1.1.Bandwidth: refers to the maximum amount of data that can be transmitted over a network connection within a given period.

It indicates how much data can be transmitted over the WAN connection in a given period, usually measured in bits per second (bps), such as Mbps (megabits per second) or Gbps (gigabits per second).

1.1.2Latency: refers to the time it takes for data to travel from its source to its destination across the network. It is usually measured in milliseconds (ms) and is a critical factor in network performance.

Lower latency means faster communication between devices, while higher latency can cause delays and affect the responsiveness of network applications.

1.1.3.Packet Loss: refers to the failure of one or more data packets to reach their destination across the network.

Packets are small units of data transmitted over a network, and packet loss occurs when these packets are dropped or lost in transit.

It is typically measured as a percentage of packets lost compared to packets sent.

1.1.4.Security threats: refer to the risks and vulnerabilities that can compromise the security and integrity of the network and its monitoring systems. These threats can impact the ability to monitor, manage, and protect a WAN effectively.

- **Tools for WAN Monitoring Report Generation**

- **Network Management Systems (NMS):** SolarWinds Orion, Cisco Prime Infrastructure, IBM Tivoli Netcool.
- **Performance Monitoring Tools:** Nagios, Zabbix, PRTG Network Monitor.
- **Security Monitoring Tools:** McAfee Enterprise Security Manager, Symantec Endpoint Protection Cloud.
- **Data Visualization Tools:** Tableau, Grafana, Qlik Sense

Practical Activity 4.1.2: Installing and customizing WAN Monitoring tools.

Task:

1: Refer to the key reading 4.1.2 and perform the following task:

Go to the computer lab of your school and install the following suitable WAN monitoring tools: Placement of Monitoring Probes, SPAN (Switched Port Analyzer), Bandwidth Monitoring, Latency and Packet Loss Analysis, Verify Quality of Service on your assigned

computer and customizing according to Key Performance Indicators (KPIs) Selection, dashboard and User Access and Roles.

2: Presents the steps to Install and customize WAN monitoring tool.

3: Install and customize WAN monitoring tool on your computer

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.1.2.

6: Perform the activity in the application of learning 4.1.

Key readings 4.1.2: Installing and customizing WAN Monitoring tools.

1.2.Perform installation of suitable tools

1.2.1. Placement of Monitoring Probes

Step 1: Determine Strategic Locations for Monitoring Probes

- **Identify Critical Points:**
  - **Place probes at key network locations, such as:** Main router or gateway that handles internet traffic, Core switches connecting different segments of the network And Any firewalls or WAN connections.

Step 2: Install the Probes

- Install hardware probes or configure software-based probes on network devices.
- Ensure that the probes can access network traffic from multiple segments for comprehensive monitoring.

Step 3: Integrate Probes with Monitoring Tool

- Add the probes to the WAN monitoring tool's interface.
- Configure the probes to start collecting data from their respective segments, focusing on metrics like traffic volume and performance.

1.2.2.SPAN (Switched Port Analyzer) Configuration

Step 1: Identify the Switch

- Identify the switch where the target network traffic is flowing.

Step 2: Configure the SPAN Port

- Access the Switch Configuration (via SSH or direct interface).
- Configure the SPAN Session:

- **Command (Cisco switches example):**

```
Switch(config)# monitor session 1 source interface <source_interface>
Switch(config)# monitor session 1 destination interface <monitoring_interf
```

- Select the source interface (the port where the traffic you want to monitor is passing).
- Set the destination interface (where the monitoring tool or probe is connected).

Step 3: Verify SPAN Operation

- Ensure that the selected network traffic is mirrored to the monitoring interface.
- Use the WAN monitoring tool to confirm the reception of mirrored traffic.

1.2.3.Bandwidth Monitoring

Step 1: Set Up Bandwidth Monitoring

- Configure the WAN monitoring tool to track the bandwidth usage across key network devices (e.g., routers, switches).
- Define bandwidth thresholds (e.g., 80% utilization) to trigger alerts when bandwidth is overused.

Step 2: Monitor Real-Time Bandwidth Usage

- Access the monitoring dashboard and observe bandwidth usage in real-time.
- Check for any abnormal spikes that could indicate network congestion or performance issues.

Step 3: Generate Bandwidth Reports

- Customize reports to show bandwidth trends over different time periods (e.g., daily, weekly).
- Include key statistics like peak usage times and the most bandwidth-intensive applications or devices.

1.2.4. Latency and Packet Loss Analysis

Step 1: Configure Latency Monitoring

- In the WAN monitoring tool, set up latency monitoring for specific WAN links.
- Monitor round-trip time (RTT) between devices to detect delays.

Step 2: Packet Loss Monitoring

- Enable packet loss detection on important WAN links and network paths.
- Define thresholds (e.g., alert if packet loss exceeds 1%).

Step 3: Real-Time Monitoring

- Continuously observe latency and packet loss metrics in the tool's dashboard.
- Identify patterns or anomalies that may indicate network instability or hardware issues.

1.2.5.Quality of Service (QoS) Verification

Step 1: Enable QoS Monitoring

- If your network devices support QoS, enable QoS monitoring in the WAN monitoring tool.
- Ensure that QoS policies (e.g., prioritization of VoIP traffic) are implemented on the WAN devices.

Step 2: Monitor QoS Performance

- Track the performance of different traffic classes (e.g., voice, video, data) and verify that high-priority traffic is receiving appropriate bandwidth.
- Ensure that the QoS policy is being enforced across the WAN.

Step 3: Analyze QoS Reports

- Generate reports to verify the quality of different types of traffic, focusing on key metrics like jitter, latency, and packet delivery for critical services (e.g., voice and video).

1.3.Customisation of tools.

Customization of WAN Monitoring Tools

Step 1. Key Performance Indicators (KPIs) Selection:

- Choose essential KPIs such as bandwidth usage, latency, packet loss, jitter, network uptime, and security alerts.
- Set thresholds for alerts (e.g., 80% bandwidth usage, 100ms latency).
- Assign KPIs to critical network devices (routers, switches, gateways).

Step 2. Dashboard Customization:

- Arrange a user-friendly dashboard layout with real-time displays of key metrics.
- Add widgets for bandwidth graphs, latency heatmaps, uptime meters, and security alerts.
- Use color coding (green, yellow, red) for status and ensure the dashboard updates in real time.

Step 3. Customize User Access and Roles:

- Create roles such as Administrator, Network Engineer, Viewer, and Security Analyst.
- Define permissions: Admins have full access, engineers can adjust settings, and viewers can only monitor.
- Customize dashboards for different roles (e.g., IT team sees all KPIs, management gets a simplified view).

Theoretical Activity 4.1.3: Identification of WAN Security Monitoring

Tasks:

1. Read carefully and answer the following questions:

   i. What is WAN Security Monitoring?
   ii. What are the main WAN monitoring threats?

2. Write answers on paper, flipchart, blackboard or whiteboard.

3. Present the findings to the whole class.

4. Ask questions for clarification if needed.

5. Read the Key readings 4.1.3 in trainee manuals.

Key readings 4.1.3: Identification of WAN Security Monitoring.

1. Application of WAN security monitoring

- **WAN Security Monitoring:** WAN Security Monitoring involves using tools and practices to continuously observe and protect the wide area network (WAN) from potential threats and vulnerabilities.

  WAN security monitoring plays a crucial role in identifying and mitigating various cyber threats, including:

  1. Suspicious Traffic Patterns:

✔ **Definition:** are deviations from normal network behaviour that raise red flags. These patterns can range from unusual spikes in traffic volume to unexpected data transfers or unauthorized access attempts.

✔ **Detection: suspicious** traffic patterns involve using various tools and techniques to identify anomalies or deviations from normal network behaviour.

- **Mitigation:** suspicious traffic patterns involve taking proactive measures to neutralize potential threats once they are identified.

2.DDoS Attacks

- **Definition:** Distributed Denial of Service (DDoS) attacks overwhelm a network or server with excessive traffic, rendering it inaccessible.
- **Detection:** WAN security monitoring systems can detect DDoS attacks by identifying unusual spikes in traffic volume, abnormal source IP addresses, and unusual traffic patterns.
- **Mitigation:** By detecting DDoS attacks early, organizations can implement mitigation techniques such as rate limiting, traffic filtering, and leveraging DDoS protection services.

3.Brute Force Attacks

- **Definition:** Brute force attacks involve systematically trying different combinations of usernames and passwords to gain unauthorized access to a system.
- **Detection:** WAN security monitoring systems can detect brute force attempts by identifying repeated failed login attempts from the same IP address or unusual login patterns.
- **Mitigation:** Implementing strong password policies, enabling two-factor authentication, and using intrusion detection systems can help prevent brute force attacks.

4.Man-in-the-Middle Attacks

- **Definition:** Man-in-the-middle attacks involve intercepting communication between two parties to eavesdrop on or manipulate data.
- **Detection:** WAN security monitoring systems can detect man-in-the-middle attacks by identifying unusual traffic patterns, unexpected encryption errors, or discrepancies between the expected and observed data.
- **Mitigation:** Using encryption protocols (e.g., HTTPS, VPNs), verifying the authenticity of websites, and implementing intrusion detection systems can help prevent man-in-the-middle attacks.

Practical Activity 4.1.4: Performing WAN Security Monitoring.

Task:

1: Refer to the key reading 4.1.4 and perform the following task:

After installing WAN Monitoring tools, perform WAN security monitoring to identify suspicious traffic patterns, DDoS attacks, Brute force and Man in the middle.

2: Presents the steps to Perform WAN security monitoring.

3: Perform WAN security monitoring.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.1.4.

6: Perform the activity in the application of learning 4.1.

Key readings 4.1.4: Performing WAN Security Monitoring.

1.Detect Suspicious Traffic Patterns

1.1.Inspect for Unusual Spikes

Step 1: In your WAN monitoring dashboard, look for real-time reports on traffic volume.

- Track spikes in bandwidth usage, especially during off-peak hours or in areas where no activity is expected (e.g., at midnight).

Step 2: If you spot a spike, drill down into the specific IP addresses or devices generating that traffic.

- Check the destination and protocol used (e.g., large HTTP traffic spikes might suggest data exfiltration).

1.2.Monitor for Lateral Movement

Step 3: Enable internal traffic monitoring in your tool to watch for lateral movement.

- Lateral movement refers to compromised devices trying to spread across your internal network.

Step 4: Look for abnormal internal communication patterns, such as one device suddenly communicating with many others that it normally doesn't interact with.

2.DDoS Attack Detection

2.1.Identify Traffic Floods

Step 1: Set up the WAN monitoring tool to track total request volume targeting specific services (e.g., web servers). Watch for high-frequency traffic hitting one or a few network devices, which may suggest a DDoS attack.

Step 2: Check the packet types (e.g., SYN packets). A high volume of incomplete connection attempts (half-open SYN packets) can signal a SYN flood DDoS attack.

2.2.Check for Multiple IP Sources

Step 3: Use the tool's traffic analysis features to analyze the source IP addresses. A typical DDoS attack will come from many different, often spoofed, IP addresses. If you see a large number of unique IPs attempting to connect at once, this is a red flag.

Step 4: Use geolocation analysis to verify the source of traffic. If your organization operates locally but you're suddenly receiving large amounts of traffic from international IPs, this might indicate a DDoS attack.

Set Up Rate-Limiting

Step 5: Set up rate-limiting rules using your WAN monitoring tool to prevent overwhelming requests.

3.Brute Force Attack Detection

3.1.Monitor for Repeated Login Failures

Step 1: Configure your tool to monitor authentication logs. Most tools allow you to set up rules that track failed login attempts across the network.

Step 2: Set up alerts to trigger when multiple failed login attempts (e.g., more than 5 in a row) occur from the same IP address or different IPs attempting the same user account.

3.2.Analyze Login Patterns

Step 3: Analyze login logs for anomalies, such as:

- Access from unusual geographic locations.
- Login attempts outside normal working hours.

Step 4: Review any suspicious login trends. If an employee who typically logs in from New York is suddenly trying to log in from another country, this could indicate a compromise.

3.3.Limit Login Attempts

Step 5: Implement a lockout policy: If a specific IP or account exceeds a threshold of failed attempts (e.g., 3-5 attempts), lock the account temporarily or block the IP for a period of time.

Step 6: Set up your monitoring tool to send an instant alert when this happens so that immediate action can be taken.

4.Man-in-the-Middle (MitM) Attack Detection

4.1.Look for Abnormal Packet Alterations

Step 1: Enable deep packet inspection (DPI) in your WAN monitoring tool. DPI allows you to examine packet headers and payloads for unusual changes.

Step 2: Watch for signs of packet tampering, such as:

- Unexpected packet delays.
- Packets being retransmitted.
- Modifications to packet content (especially encrypted packets being decrypted).
- Example: If encrypted traffic between two nodes suddenly becomes unencrypted, it may indicate a MitM attack.

4.2.Check for Unusual Encryption Changes

Step 3: Set up monitoring for SSL/TLS encryption changes. If secure communication suddenly reverts to an insecure protocol (e.g., from HTTPS to HTTP), this could be a sign of an attacker downgrading encryption to intercept traffic.

Step 4: Configure alerts for SSL/TLS certificate changes: MitM attackers sometimes insert their own certificates to impersonate legitimate entities.

Practical Activity 4.1.5: Generating WAN monitoring report.

Task:

1: Refer to the key reading 4.1.5 and perform the following task:

After performing WAN security monitoring in your school generate a comprehensive WAN monitoring report for the past month.

2: Presents the steps to Generate WAN monitoring report..

3: Generate WAN monitoring report.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.1.5.

6: Perform the activity in the application of learning 4.1.

Key readings 4.1.5: Generating WAN monitoring report.

1. Executive Summary

This report provides an overview of the WAN monitoring activities conducted over the past month. It highlights significant findings regarding network performance, security incidents, and potential vulnerabilities, alongside recommended actions for enhancement.

2. Monitoring Overview

- Monitoring Tools Used: [List of WAN monitoring tools]
- Objectives:

- To ensure network integrity and availability.
- To identify potential security threats.
- To monitor traffic patterns and performance metrics.

3. Traffic Analysis

- Total Data Transmitted: [Total Data]
- Average Daily Bandwidth Usage: [Average Usage]
- Peak Traffic Periods:

- [Day/Time] with [Peak Data] transmitted.

- Off-Peak Usage: [Description]

3.1 Baseline Traffic Established

- Normal traffic patterns were established based on data collected over the first two weeks.
- Notable average usage during school hours (8 AM - 4 PM) was consistent, with minimal traffic during nights and weekends.

4. Security Incident Overview

4.1 Detected Suspicious Traffic Patterns

- Unusual Spikes:

- A spike of [Percentage]% in traffic was recorded on [Date], primarily from [Specific Source].
- Investigation revealed [Nature of Activity/Incident].

- Lateral Movement:

- Monitored internal communications indicated [Details of Any Abnormal Activity].

4.2 DDoS Attack Detection

- Incidents Detected:

- On [Date], a DDoS attack was attempted, characterized by [Details of Attack].
- Actions Taken: Traffic from identified sources was blocked, and rate-limiting rules were implemented.

4.3 Brute Force Attack Detection

- **Login Failures:**

- [Number] repeated login failures were recorded from [Source IP/Account].
- Accounts were temporarily locked after exceeding the threshold.

4.4 Man-in-the-Middle Attack Detection

Anomalies Detected:

- Signs of packet alteration were identified during [Timeframe].
- Prompt action was taken to verify the integrity of data transmissions.

5. Performance Metrics

- Average Latency: [Average Latency]
- Packet Loss: [Packet Loss Percentage]
- Network Availability: [Availability Percentage]

- Response Times for Security Alerts: [Average Response Time]

6. Recommendations

- **Immediate Actions:**

[Action 1: e.g., strengthen firewall settings, update security protocols, etc.]

[Action 2: e.g., implement multi-factor authentication for critical accounts.]

- **Long-term Improvements:**

- Regularly review and update baseline traffic patterns.
- Schedule training for staff on recognizing phishing attempts and secure practices.

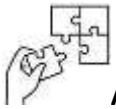
7. Conclusion

The WAN monitoring efforts over the past month have highlighted areas of success and concern. Continued vigilance is essential to maintain network security and performance. Implementing the recommended actions will enhance our defenses against potential threats and ensure optimal network performance for all users.

Points to Remember

- You should remember that WAN Monitoring refers to the continuous tracking and analysis of network performance across wide area networks (WAN).
- Placement of Monitoring Probes.
- SPAN (Switched Port Analyzer).
- Bandwidth Monitoring.
- Latency and Packet Loss Analysis.
- Verify Quality of Service Key Performance Indicators (KPIs) Selection.
- Customize dashboard.
- Customize User Access and Roles.
- WAN Security Monitoring involves using tools and practices to continuously observe and protect the wide area network (WAN) from potential threats and vulnerabilities.
- Identification of suspicious traffic patterns.
- DDoS attacks.
- Brute force.
- Man in the middle.

- Title and Date.
- Executive Summary
- Monitoring Tools
- Objectives
- Recommendations



Application of learning 4.1.

Suppose that your school needs to improve the network's performance and prevent future outages and you are asked to install WAN monitoring tools that will help them to monitor bandwidth usage, detect latency, and identify potential security threats in real-time.

Indicative content 4.2: Performing Hardware and Software Preventive Maintenance.

Duration: 5 hrs

Theoretical Activity 4.2.1: Description of hardware and software preventive maintenance.

Tasks:

1: Read carefully and answer the following questions:

I. Define the following terms as used in WAN:

   a. Preventive maintenance

   b. Firmware.

   c. Disaster recovery.

II. What is the difference between Backup and Disaster Recovery?

III. What are the main preventive measures that you can set in WAN?

2: Write answers on paper, flipchart, blackboard or whiteboard.

3: Present the findings to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 4.2.1 in trainee manuals.

Key readings 4.2.1. Description of hardware and software Preventive maintenance

Introduction:

Preventive maintenance: is a proactive approach to maintaining the reliability and performance of your Wide Area Network (WAN).

Hardware maintenance in a Wide Area Network (WAN): involves a range of activities designed to keep the physical components of the network operating efficiently and reliably.

Software maintenance in a Wide Area Network (WAN): involves ensuring that the network's software components operate efficiently and securely.

1.1. Setting of preventive measures

✔ **Setting preventive measures in a WAN (Wide Area Network):** involves implementing strategies and practices to minimize the risk of network failures and maintain smooth operation.

✔ **Here are some key preventive measures you might cover:**

- **Regular Monitoring:** Use network monitoring tools to continuously check the health and performance of the WAN. This helps in early detection of potential issues.
- **Performance Optimization:** Regularly analyze and optimize network performance to avoid bottlenecks and ensure efficient data flow.
- **Security Measures:** Implement robust security protocols, such as firewalls, intrusion detection/prevention systems, and encryption, to protect against cyber threats.
- **Redundancy and Failover:** Design the WAN with redundancy and failover capabilities to ensure continuity in case of a failure. This includes having backup connections and alternative routes.
- **Firmware and Software Updates:** Regularly update firmware and software on network devices to patch vulnerabilities and improve performance.
- **Capacity Planning:** Plan for future growth by analyzing traffic patterns and ensuring that the network can handle increased load without degradation.
- **Documentation:** Maintain comprehensive documentation of the network topology, configurations, and procedures to aid in troubleshooting and planning.
- **Training and Awareness:** Ensure that staff are trained in best practices for network management and aware of potential risks and preventive measures.
- **Regular Backups:** Regularly back up configurations and critical data to prevent loss in case of failure or disaster.
- **Compliance Checks:** Ensure that the network adheres to industry standards and regulatory requirements.

1.2. Regular Firmware and Software Updates

1.2.1. Firmware: is the low-level software programmed into a network device's hardware, such as routers, switches, and firewalls. It controls the device's operations at a fundamental level.

✔ **Purpose:** Updating firmware ensures that the device has the latest features, bug fixes, and security patches. It helps in fixing vulnerabilities and improving device performance.

✔ **Process:**

- **Check for Updates:** Regularly check the manufacturer's website or management interface for available firmware updates.
- **Backup Configuration:** Before applying updates, back up the device's current configuration to avoid data loss.
- **Install Update:** Follow the manufacturer's instructions to apply the firmware update. This usually involves uploading the new firmware file and rebooting the device.
- **Verify Operation:** After the update, verify that the device is functioning correctly and that there are no issues with connectivity or performance.

1.2.2. Software Updates: Software updates apply to the network management software, operating systems, and applications running on network devices and servers.

✔ **Purpose:** These updates provide new features, performance improvements, and security enhancements. They also fix bugs and vulnerabilities.

✔ **Process:**

- **Monitor for Updates:** Regularly check for updates from software vendors or use automated update tools if available.
- **Backup Systems:** Backup critical data and system configurations before applying updates.
- **Apply Updates:** Follow the vendor's instructions to apply the updates. This may involve downloading and installing new software versions or patches.
- **Test and Validate:** After updating, test the system to ensure that it is functioning as expected and that the update hasn't introduced any new issues.

1.3. Backup and Disaster Recovery

Backup and disaster recovery are critical components of a WAN (Wide Area Network) strategy to ensure continuity and minimize downtime in the event of a failure or disaster. Here's a detailed look at both:

1.3.1. Backup refers to the process of creating copies of data, configurations, and other critical information to protect against data loss due to hardware failure, corruption, or other issues.

1.3.2. Disaster Recovery is the process of restoring network operations and data access after a significant failure or disaster, such as hardware failure, cyberattack, or natural disaster.

Practical Activity 4.2.2: Performing hardware and software Preventive maintenance.

Task:

1: Refer to the key reading 4.2.2 and perform the following task:

Go to the computer lab in your school and perform hardware and software preventive maintenance of WAN.

2: Presents the steps to Perform hardware and software preventive maintenance.

3: Perform hardware and software preventive maintenance on WAN routers.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.2.2.

6: Perform the activity in the application of learning 4.2.

Key readings 4.2.2: Performing hardware and software preventive Maintenance

Go to the computer lab in your school and perform hardware preventive maintenance on the school WAN router:

1. **Power down the router:**

- ✔ Safely shut down the router by turning it off or unplugging it from the power source.
- ✔ Disconnect any backup power supply, such as an uninterruptible power supply (UPS), if applicable.

2. **Inspect the router's physical condition:**

- ✔ Check for dust: Look for any dust accumulation on the router's surface and vents.
- ✔ Check cables: Ensure all power and network cables are securely connected and show no signs of wear, such as fraying or discoloration.
- ✔ Examine LED indicators: Note any abnormalities (e.g., burnt-out or malfunctioning LEDs).

3. Clean the router:

- ✔ Use a soft, dry cloth to wipe the exterior.
- ✔ Clean air vents: Use compressed air to remove dust from the air vents to ensure proper ventilation and prevent overheating.
- ✔ Ensure the environment around the router is clean and free from clutter or obstruction.

4. Check the ventilation and temperature:

- ✔ Ensure the router is positioned in a well-ventilated area.
- ✔ Confirm the room's temperature is within the manufacturer's recommended range (typically between 0°C to 40°C).

5. Inspect internal components (if needed):

- ✔ If the router has accessible internal components (such as fans or power supplies), carefully open the casing (following the manufacturer's guidelines).
- ✔ Check internal fans for dust buildup and clean as needed.
- ✔ Verify that internal connections (e.g., modules, cards) are secure.

6. Reconnect power and restart:

- ✔ After completing the inspection and cleaning, reconnect the power and turn on the router.
- ✔ Monitor the router as it powers up, checking for normal operation of the LED indicators and any error messages.

i. Perform software preventive maintenance on the school WAN router:

1. Access the router's management interface:

- ✔ Open a web browser and type the router's IP address (e.g., 192.168.1.1) into the address bar.
- ✔ Log in to the router using the administrator credentials.

2. **Check for firmware updates:**

- ✔ Navigate to the Firmware/Software Update section of the interface.
- ✔ Check if a newer firmware version is available.
- ✔ Download and install the update if available (ensure you back up the configuration before updating).

3. **Back up the router configuration:**

- ✔ In the router's interface, locate the Backup/Restore section.
- ✔ Create a backup of the current router configuration and save it to an external storage device for future recovery.

4. **Review and clear logs:**

- ✔ Check the router's log files for any unusual activity, errors, or warnings.
- ✔ Clear old logs to free up space and improve router performance.

5. **Check routing table and network settings:**

- ✔ Review the current routing table to ensure no unnecessary or outdated routes are configured.
- ✔ Verify that WAN settings, DNS settings, and security configurations (e.g., firewall, VPN) are functioning correctly.

6. **Optimize performance settings:**

- ✔ Review bandwidth usage and adjust Quality of Service (QoS) settings if necessary to prioritize important traffic.
- ✔ Check for any unused or unnecessary features (e.g., DHCP servers, wireless services) that can be disabled to improve performance.

7. **Run diagnostics:**

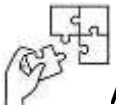
- ✔ Run diagnostic tools available in the router's interface to check network health, test connectivity, and identify any potential issues.

8. **Restart the router:**

✔ After completing the software maintenance, restart the router to apply any changes and ensure all settings are functioning properly.

Points to Remember

- Preventive maintenance is a proactive approach to maintaining the reliability and performance of your Wide Area Network (WAN).
- Firmware is the low-level software programmed into a network device's hardware, such as routers, switches, and firewalls.
- Disaster Recovery is the process of restoring network operations and data access after a significant failure or disaster, such as hardware failure, cyberattack, or natural disaster.
- The difference between Backup it's like copying data for restoration while Disaster Recovery it's like broader strategies for system recovery and continuity.
- The main preventive measures in WAN include Regular Firmware Updates, Monitoring Tools , Redundant Connections and Training Staff.
- Turn off or unplug the router, and disconnect any backup power supplies (e.g., UPS).
- Check for dust on the router and cables, ensuring all connections are secure. Clean the exterior and air vents using compressed air.
- Ensure the router is in a well-ventilated area with a room temperature within the manufacturer's recommended range (0°C to 40°C).
- Access the router's management interface, check for firmware updates, back up the configuration, and review log files for errors or unusual activity.
- Review routing tables and settings for efficiency, adjust QoS if necessary, run diagnostics, and restart the router to apply changes.



Application of learning 4.2.

Suppose that your school needs to enhance the reliability of its WAN and they plan to implement a preventive maintenance strategy and as technician you are asked to perform hardware and software preventive maintenance on your school WAN.

Indicative content 4.3: Performing Corrective Maintenance.

Duration: 5 hrs

Theoretical Activity 4.3.1: Description of corrective maintenance in WAN

Tasks:

1: Read carefully and answer the following questions:

i. What do you understand by the term corrective maintenance in WAN?

ii. What are the Types of Corrective Maintenance in WAN?

2: Write answers on paper, flipchart, blackboard or whiteboard.

3: Present the findings to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 4.3.1 in trainee manuals.

Key readings 4.3.1: Description of corrective maintenance in WAN.

1. Performing Corrective maintenance

Corrective maintenance in a WAN (Wide Area Network) involves actions taken to fix problems and restore network functionality after an issue has been identified.

1.1. Hardware Maintenance

Hardware maintenance involves the regular inspection, cleaning, and repair of physical network components to ensure optimal performance and reliability.

1.1.1. Identification of Common Problems and Their Causes

- ✔ **Device Failure:** Symptoms include complete loss of connectivity or specific device malfunctions.
- ✔ **Interface Issues:** Problems with network interfaces can result in intermittent connectivity.

- **Performance Degradation:** Devices may show degraded performance due to issues like high CPU usage or memory leaks.

1.1.2. Repair/Replace Damaged Devices

- **Diagnose Faulty Hardware:** Use diagnostic tools to identify which component is faulty. This might involve checking device logs, running hardware diagnostics, or using network testing tools.
- **Replace Defective Components:** Swap out damaged parts like faulty network cards, routers, or switches. Ensure that replacement components are compatible with the existing network setup.
- **Repair Devices:** If feasible, repair the damaged hardware. This could involve fixing or cleaning components, resetting devices to factory settings, or performing firmware upgrades.

1.2. Software Maintenance

Software maintenance in a WAN (Wide Area Network) refers to the activities involved in managing, updating, and troubleshooting software components that support and manage the network.

1.2.1. Troubleshoot Network Configurations

- **Identify Configuration Errors:** Use network management tools to detect misconfigurations or errors in the network setup.
- **Analyse Logs and Reports:** Review system and network logs to trace the source of configuration issues.
- **Verify Settings:** Ensure that all network settings, such as subnet masks, gateway addresses, and DNS configurations, are correctly configured and aligned with network design.

1.2.2. Update Network Configurations

- **Apply Configuration Changes:** Modify network configurations to resolve identified issues.
- **Validate Updates:** Test the updated configurations to ensure they have resolved the issues and that the network is functioning correctly.
- **Document Changes:** Record all changes made to the network configuration, including the reasons for the changes and their impact.

Practical Activity 4.3.2: Performing Corrective maintenance.

Task:

1: Refer to the key reading 4.3.2 and perform the following task:

You are asked to go to the computer lab of your school and perform corrective maintenance on the school's Wide Area Network (WAN).

2: Presents the steps to Perform corrective maintenance.

3: Perform corrective maintenance on school WAN.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.3.2.

6: Perform the activity in the application of learning 4.3

Key readings 4.3.2: Performing corrective maintenance

1. **Identify the Problem:**

1.1. Access the WAN monitoring tool:

- ✔ Go to the computer assigned for network monitoring in the computer lab.
- ✔ Open the WAN monitoring tool (e.g., SolarWinds, PRTG, or Nagios).

1.2. Check for alerts or warnings:

- ✔ Review the dashboard for any device issues such as high bandwidth usage, device failure, or abnormal latency.
- ✔ Look for alerts related to slow response times or disconnections.

1.3. Inspect specific network devices:

- ✔ Identify key devices that handle WAN traffic (routers, switches).
- ✔ Use the tool to monitor these devices and observe parameters such as bandwidth utilization, error rates, and packet loss.

1.4. Record findings:

✔ Document any significant issues (e.g., bandwidth spikes, high packet loss, or misconfigured devices).

2. Diagnose the Root Cause:

2.1. Test connectivity:

✔ Use Ping to test the connectivity of WAN devices (e.g., router or switch). For example, open the Command Prompt and type:

```css
ping [device IP address]
```

✔ Check for high latency or packet loss.

2.2. Run a traceroute:

✔ Perform a traceroute to identify where network slowdowns or disconnects occur.

```css
tracert [destination IP address]
```

✔ Identify any slow hops or devices causing delays.

2.3. Check network congestion:

✔ Check for excessive bandwidth usage in the WAN monitoring tool.

✔ Identify if certain applications, users, or devices are consuming more bandwidth than expected.

2.4. Check for hardware issues:

✔ Inspect routers and switches for overheating, faulty cables, or loose connections.

2.5. Check device configuration:

✔ Access the router or switch configuration interface (via web interface or SSH) and verify if configurations are correct.

✔ Look for misconfigured routing tables, incorrect IP addresses, or VLAN misconfigurations.

2.6. Record diagnostic findings:

✔ Document your findings from these diagnostic tools.

3. Apply Corrective Actions:

3.1. Resolve hardware issues:

✔ If any cables or devices are faulty or loosely connected, replace or secure them.

✔ If devices are overheating, ensure proper ventilation or clean dust buildup.

3.2. Resolve software and configuration issues:

✔ Reboot malfunctioning devices (routers, switches) if necessary.

✔ If bandwidth congestion is an issue, adjust Quality of Service (QoS) settings to prioritize critical traffic.

✔ If routing issues are detected, correct the routing tables or reconfigure network paths.

3.3. Replace faulty equipment:

✔ If hardware devices (e.g., a switch or router) are found to be faulty, replace them with backup equipment.

3.4. Document corrective actions:

✔ Record the corrective actions taken for each identified issue, such as replacing cables, adjusting QoS, or rebooting devices.

4. Verify the Fix:

4.1. Monitor the network:

✔ After applying corrective actions, monitor the WAN performance through the WAN monitoring tool.

✔ Look for improvement in network parameters like bandwidth usage, latency, and packet loss.

4.2. Test the network's performance:

✔ Use a client device to access shared resources (e.g., network files or applications).

✔ Check if response times have improved and disconnections no longer occur.

4.3. Run diagnostic tests again:

- ✔ Perform Ping and Traceroute tests again to confirm there are no more issues with high latency or disconnections.

4.4. Generate a report:

- ✔ Generate a report from the WAN monitoring tool summarizing the improvements in network performance.
- ✔ List any remaining issues that may still need attention.

Points to Remember

- Corrective Maintenance refers to the process of identifying, diagnosing, and fixing issues or faults that arise in a Wide Area Network (WAN).
- Types of Corrective Maintenance are hardware and software corrective maintenance.
- Assess the network issues by checking devices like routers, switches, and cables for any visible faults.
- Use network diagnostic tools to identify any software configuration issues or performance bottlenecks.
- Replace faulty hardware such as routers, switches, or damaged network cables.
- Reconfigure network settings to restore proper connectivity.
- After repairs, test the WAN to verify that all issues are resolved.

Application of learning 4.3.

Suppose that your school is experiencing intermittent connectivity issues affecting internet access for several classrooms and you asked to resolve this issue using the corrective maintenance.

Indicative content 4.4: Checking Hardware and Software Functionalities.

Duration: 5 hrs

Practical Activity 4.4.1: Checking hardware and software functionalities in WAN.

Task:

1: Refer to the key reading 4.4.1 and perform the following task:

Go to the computer lab of your school and check the hardware and software functionalities about your school WAN to ensure all components are working as expected.

2: Presents the steps to Check the hardware and software functionalities.

3: Check the hardware and software functionalities about your school WAN.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.4.1.

6: Perform the activity in the application of learning 4.4.

Key readings 4.4.1.Checking hardware and software functionalities

1. **Hardware Functionality Check:**

1.1. Inspect Physical Components:

- ✔ Routers and Switches: Ensure that the routers and switches are powered on, with all indicators (LEDs) showing normal operation (green or blue lights). Look for any red or amber lights, which could indicate hardware issues.
- ✔ Cabling: Check all network cables for secure connections and any visible wear or damage. Ensure there are no loose connections or broken cables.

1.2. Monitor Device Temperatures:

- ✔ Check for overheating by ensuring proper airflow around network devices. Use the WAN monitoring tool (if available) to read device temperatures or inspect built-in temperature sensors on routers/switches.

1.3. Test Power Supply:

- ✔ Verify that the power supply to each device is stable and working. If a device is connected to an Uninterruptible Power Supply (UPS), confirm that the UPS is functioning and providing backup power as needed.

2. Software Functionality Check:

2.1. Access the Router/Switch Interface:

- ✔ Log into the web-based or command-line interface (CLI) of the router and switches using their IP addresses.
- ✔ Check the firmware version. Ensure it's up-to-date, and if not, consider updating the firmware to fix bugs or security issues.

2.2. Verify Routing and Configuration:

- ✔ Check the current routing table to ensure there are no incorrect routes that could be causing network issues.
- ✔ Ensure that Quality of Service (QoS) settings are optimized for efficient traffic management, and any necessary VLANs (Virtual Local Area Networks) are properly configured.

2.3. Run Diagnostic Tools:

- ✔ Use Ping and Traceroute to test network connections between key WAN components. Confirm that there is no packet loss or unusual latency.
- ✔ Check the WAN monitoring tool for device performance metrics like bandwidth usage, latency, and error rates.

2.4. Review Logs and Alerts:

- ✔ Look through the system logs of routers and switches for any errors, warnings, or alerts that indicate hardware or software issues.
- ✔ Clear old logs and set up automatic alerts for future issues if not already configured.

Final Checks:

1. **Reboot Devices (if necessary):** If any software settings seem off or hardware behaves unusually, reboot the affected device.

2. **Monitor Network Health:** Use the WAN monitoring tool to check that all components are performing as expected, and that the WAN is functioning smoothly with no bottlenecks or errors.

Points to Remember

- Ensure routers and switches are powered on, with normal LED indicators (green or blue). Look for any red or amber lights that may indicate issues.
- Verify all network cables are secure and undamaged. Confirm stable power supply to devices and check that any connected UPS is functioning properly.
- Ensure proper airflow around devices and check for overheating using the WAN monitoring tool or built-in temperature sensors.
- Log into the device interfaces to check firmware versions and verify routing configurations and QoS settings for optimal performance.
- Use tools like Ping and Traceroute to test connections, check for packet loss, and review logs for any errors or warnings. Reboot devices if necessary and monitor overall network health with the WAN monitoring tool.

Application of learning 4.4.

Suppose that your school is experiencing intermittent network connectivity issues in its Wide Area Network (WAN) and you asked to perform both the hardware and software functionalities to identify and resolve any potential issues.

Indicative content 4.5: Elaboration of Maintenance Report.

Duration: 3 hrs

Theoretical Activity 4.5.1: Description of WAN Maintenance Report

Tasks:

1: Read carefully and answer the following questions:

i. What is Maintenance report as used in WAN?
ii. What is the main goal of a maintenance report used in WAN?
iii. What are the main elements of Maintenance report used in WAN?

2: Write answers on paper flipchart, blackboard or whiteboard.

3: Present the finding to the whole class.

4: Ask questions for clarification if needed.

5: Read the Key readings 4.5.1 in trainee manuals.

Key readings 4.5.1: Description of WAN Maintenance Report

1. Elaboration of maintenance report

1.1. Introduction to Maintenance report

1.1.1. **Definition: A Maintenance Report in a WAN (Wide Area Network) context** is a comprehensive document that records the activities performed to ensure the network's reliability, performance, and security.

1.1.2. **The goal of the report** is to provide a clear overview of the network's health, highlight potential issues, and document the steps taken to maintain optimal network performance.

1.2. Elements of Maintenance report

1.2.1. Client Information:

✔ **Client Name:** The name of the organization or client for whom the WAN maintenance was performed.

- **Network Details:** A brief description of the client's WAN setup, including the types of network devices, geographical locations, and the primary purpose of the network (e.g., connecting branch offices, supporting remote access).
- **Point of Contact:** Contact information for the client's IT administrator or network manager.

1.2.2. Status Before Maintenance:

- **Initial Assessment:** A summary of the network's condition before the maintenance, including any reported issues, errors, or areas of concern.
- **Performance Metrics:** Include relevant data such as network uptime, bandwidth usage, packet loss, or error rates before the maintenance activity.
- **Logs and Alerts:** Document any alerts from network monitoring tools, logs of network events, or incidents that prompted the maintenance activity.

1.2.3. Implementation of the Solution:

- **Maintenance Activities:** A detailed description of the actions taken during the maintenance process, including:
- **Preventive Measures:** Routine tasks such as software updates, firmware upgrades, security patch installations, and configuration reviews.
- **Corrective Actions:** Troubleshooting steps, repairs, hardware replacements, or software fixes applied to address specific network issues.
- **Step-by-Step Process:** A step-by-step account of how the solution was implemented, including any changes to network configurations, system reboots, or testing procedures performed.
- **Challenges Encountered:** Any obstacles faced during maintenance, such as hardware incompatibilities, software conflicts, or unexpected network behavior, and how they were resolved.

1.2.4. Used Tools, Materials, and Equipment:

- **Hardware Tools:** List of physical tools used, such as network testers, cable crimpers, or replacement hardware components (e.g., routers, switches).

- **Software Tools:** Network management and diagnostic software used during maintenance, such as network monitoring tools, firmware update utilities, or configuration management software.
- **Materials:** Any consumables used, such as network cables, connectors, or cooling fans.
- **Documentation:** Reference to any manuals, guidelines, or standard operating procedures followed during maintenance.

1.2.5. Status After Maintenance:

- **Post-Maintenance Assessment:** A summary of the network's condition after the maintenance activities were completed. This should include improvements in network performance, stability, and security.
- **Performance Metrics:** Updated metrics such as network uptime, latency, bandwidth usage, and error rates, demonstrating the impact of the maintenance.
- **Verification and Testing:** Details of the testing procedures carried out to ensure the network is functioning correctly, including connectivity tests, speed tests, and security scans.

1.2.6. Recommendations:

- **Future Maintenance:** Suggestions for future preventive maintenance activities, such as scheduled software updates, regular performance monitoring, and periodic security audits.
- **Improvements:** Recommendations for enhancing network performance and reliability, such as upgrading network devices, optimizing configurations, or implementing new security measures.
- **Training and Awareness:** Advice on training staff to better manage and monitor the network, including best practices for network maintenance and security.
- **Long-Term Planning:** Strategic suggestions for long-term network development, such as scalability plans to support growth, adoption of new technologies, or transition to cloud-based solutions.

Practical Activity 4.5.2: Elaborating WAN Maintenance Report

Task:

1: Refer to the key reading 4.5.2 and perform the following task:

Prepare a detailed WAN maintenance report based on what you did on your school WAN maintenance.

2: Presents the steps to Prepare a detailed WAN maintenance report.

3: Prepare a detailed WAN maintenance report about your school WAN.

4: Ask for clarification if any.

5: For more clarifications, read the key readings 4.5.2.

6: Perform the activity in the application of learning 4.5.

Key readings 4.5.2.Elaborating WAN Maintenance Report

WAN Maintenance Report

1. Client Information

Client Name: [Insert client name]

Contact Information: [Insert phone number, email address]

Location: [Insert physical location]

Date of Maintenance: [Insert date]

Technician(s): [Insert name(s) of technician(s) involved]

2. Status Before Maintenance

Issue Summary: [Briefly describe the WAN issue(s), e.g., intermittent connectivity, latency problems, etc.]

Impact on Operations: [Explain how the issue affected network performance or the client's business operations, e.g., downtime, slow data transfer, etc.]

Initial Diagnosis: [Describe the findings based on the initial assessment or network monitoring results.]

3. Implementation of Solution

Procedure: [Outline the steps taken to resolve the issue, including any troubleshooting methods used.]

Repairs and Configurations: [List the specific actions, configurations, or fixes applied during maintenance, e.g., replacing faulty cables, reconfiguring network devices, etc.]

Preventive Measures: [Describe any preventive measures implemented to avoid future issues, such as software updates, hardware replacements, or regular monitoring setup.]

4. Used Tools, Materials, and Equipment

Tools: [List the tools used, e.g., network analyzers, cable testers, etc.]

Materials: [List the materials used, such as cables, connectors, replacement parts, etc.]

Equipment: [Mention any hardware or software involved in resolving the issue.]

5. Status After Maintenance

Final Diagnosis: [Describe the status of the WAN after the maintenance was performed, noting any remaining issues or improvements.]

Tests Performed: [Explain the tests conducted to ensure the WAN was functioning properly after the maintenance, e.g., bandwidth tests, latency checks, etc.]

System Functionality: [State whether the system is fully functional and stable.]

6. Recommendations

Short-Term: [Provide immediate recommendations to keep the WAN running efficiently, such as regular monitoring or minor updates.]

Long-Term: [Suggest long-term strategies, like upgrading equipment, adding redundancy, or scheduling preventive maintenance checks.]

Technician Signature: _____

Date: _____

Points to Remember

- Maintenance Report is a comprehensive document that records the activities performed to ensure the network's reliability, performance, and security.
- The main goal of the report is to provide a clear overview of the network's health, highlight potential issues, and document the steps taken to maintain optimal network performance.
- Elements of Maintenance report are Client information, Status before maintenance, Implementation of solution, Used Tools, materials, and Equipment. Status after maintenance and Recommendation
- Clearly describe the issue, actions taken, and results without unnecessary details.
- Follow a logical structure—start with the issue, proceed to actions, findings, and then results.
- Attach relevant logs or screenshots to support your findings and actions.
- Avoid technical jargon where possible; make the report understandable to non-technical stakeholders.
- Include exact dates, times, and durations to provide a complete picture of the maintenance activity.
- Double-check all information for accuracy before finalizing the report.

Application of learning 4.5.

Suppose that your school has been experiencing intermittent network connectivity issues in its Wide Area Network (WAN). As a technician elaborate the WAN Maintenance report.

Q1. Circle the letter corresponding to the right answers:

i. Bandwidth as used in a WAN is referred to:

   a. The speed at which packets are lost.

   b. The amount of data that can be transferred per second.

   c. The time it takes for a packet to reach its destination.

   d. The security level of the network.

ii. During the installation of WAN monitoring tools, which of the following step ensures that the tool is compatible with your network environment:

   a. Customizing the tool's dashboard.

   b. Verifying system requirements.

   c. Setting up email notifications.

   d. Installing additional software modules.

iii. Why is it important to monitor bandwidth in a WAN:

   a. To detect security threats.

   b. To measure packet delivery times.

   c. To ensure that the network can handle traffic demands.

   d. To reduce the number of connected devices.

iv. . What is latency in WAN monitoring:

   a. The percentage of data packets lost during transmission.

   b. The time it takes for data to travel from source to destination.

   c. The total amount of data transmitted per second.

   d. The number of errors detected in the network of placing monitoring probes in a WAN.

v. Which of the following is an example of customizing WAN monitoring tools to improve network management:

   a. Installing antivirus software.

   b. Setting up custom alerts and thresholds for bandwidth usage.

c. Upgrading the network hardware.

d. Disabling real-time monitoring.

Q2. Match the elements of the column A with the column B in the column C, to find out the right monitoring activity with its corresponding task:

Column A	**Column B**	**Column C (Answers)**
1. Identify Monitoring Objectives	a. Placement of Monitoring Probes	…….
2. Perform installation of suitable tools	b. Brute force	…….
3. Customization of tools	c. Bandwidth	…….
4. Application of WAN security monitoring	d. Generate WAN performance report	…….
5. Generation of WAN monitoring report	e. Customize dashboard	…….
	f. Setting of preventive measures	
	g. Update network configurations	

Q3. Answer the following questions by using True if the statements below are correct or False if they are incorrect:

a. Preventive maintenance includes setting up preventive measures to avoid potential hardware or software failures.

b. Regularly updating firmware and software is not necessary if the system is functioning correctly.

c. Backing up data is a crucial part of preventive maintenance to ensure recovery in case of hardware or software failure.

d. A good preventive maintenance plan includes scheduling regular backups and system updates to minimize data loss.

e. Data backup is an optional step in preventive maintenance and is only necessary in case of critical failures.

f. Preventive maintenance involves identifying and addressing potential issues before they cause system downtime.

g. Data backup is an optional step in preventive maintenance and is only necessary in case of critical failures.

Practical assessment

You have been hired as the network technician for a mid-sized company, ABC CompanyLtd., which operates a wide area network (WAN) across three branch offices. The company is experiencing intermittent network performance issues and security threats. You are tasked with installing, customizing, and maintaining WAN monitoring tools, performing preventive

End

References

Baker, G. (2023). *Hardware Maintenance in WAN.* Chicago: TechSolutions Publishing.

Carter, J. (2021). *Comprehensive Guide to WAN Maintenance Reports.* San Francisco: NetworkTech Publishing.

Carter, O. (2020). *Evaluating Hardware Status for Network Performance.* Seattle: Network Engineering Press.

Clark, J. (2021). *Guide to Installing Network Monitoring Tools.* Los Angeles: Network Solutions Press.

Doe, J. (2020). *Effective Bandwidth Management.* Miami: Tech Insights Publishing.

Evans, E. (2021). *Customizing Network Monitoring Dashboards.* New York: IT Solutions Publishing.

Johnson, E. (2022). *Troubleshoot network configurations and Update network configurations.* London: Global Network Publishing.

Lee, D. (2020). *Monitoring Security Threats in WANs.* San Francisco: CyberTech Press.

Mitchell, L. (2022). *Elaborating a Maintenance Report for WAN.* New York : TechPress.

Thompson, D. (2021). *Assessing Hardware Connectivity in WAN.* Boston: Tech Systems Publishing.

network performance management. (n.d.). Retrieved from www.manageengine.com: https://www.manageengine.com/network-monitoring/network-performance-management.html

WAN monitoring. (n.d.). Retrieved from www.site24x7.com: https://www.site24x7.com/wan-monitoring.html

WAN monitoring software. (n.d.). Retrieved from www.research.aimultiple.com: https://research.aimultiple.com/wan-monitoring-software/

RTB | RWANDA TVET BOARD

October 2024