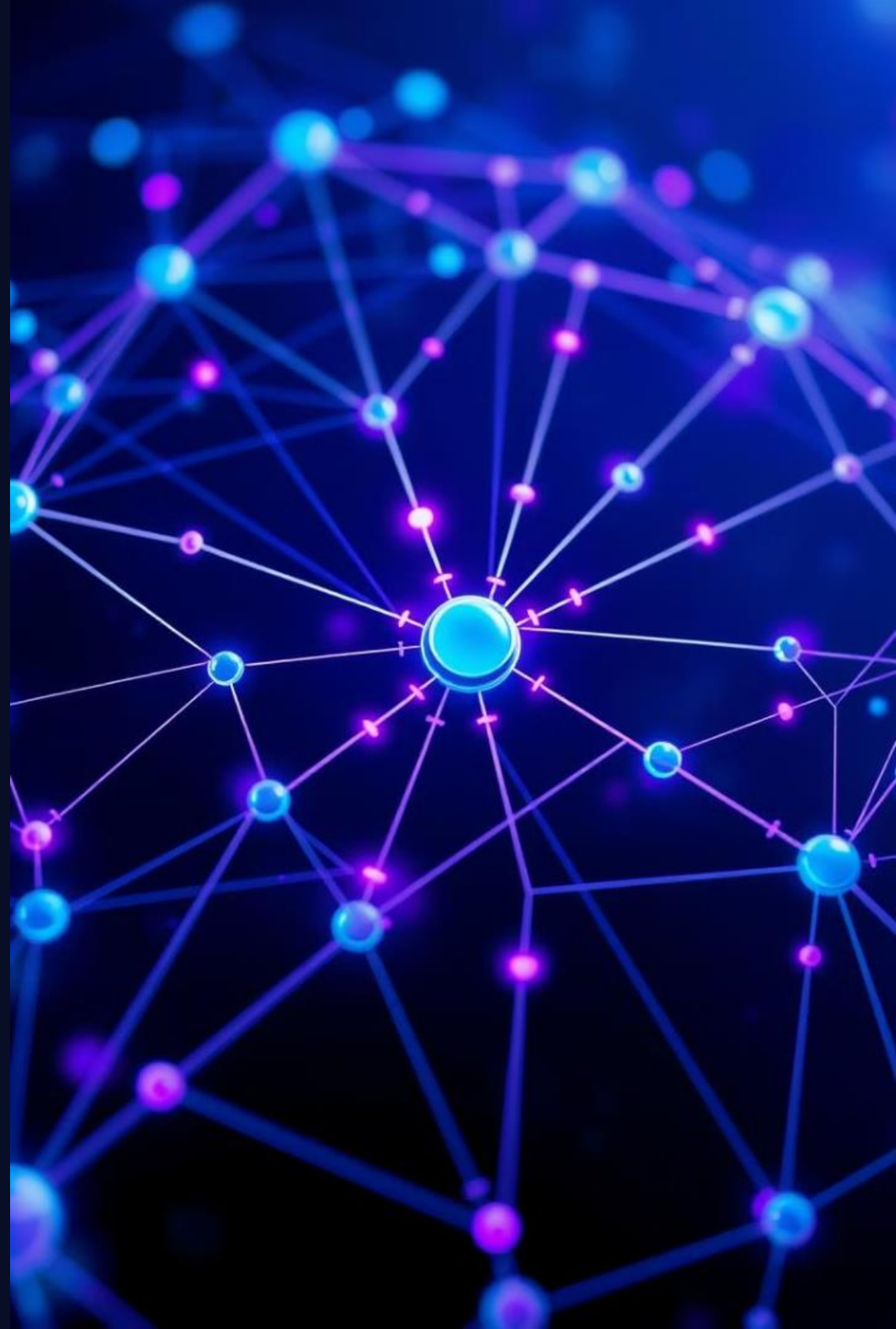
Level 1: Fundamental Networking Concepts

This presentation outlines the key concepts, skills, and assessments for the Fundamental Networking Concepts course. It covers topics from basic network types and devices to advanced troubleshooting and emerging technologies.

CONTENT OF THE SESSIONAL COURSE

MD. TARIQUL ISLAM
Lecturer , Department of CSE
University of Global Village (UGV), Barishal



Course Learning Outcomes

1

CLO1

Understand fundamental networking concepts, including network types, devices, and topologies.

2

CLO2

Apply networking protocols, IP addressing, subnetting, and configure LAN, MAN, and WAN networks.

3

CLO3

Design and implement secure and scalable enterprise-level networks using VLANs, VPNs, routing protocols, and NAS.

4

CLO4

Troubleshoot and resolve network issues using diagnostic tools, network monitoring tools, and OSI model layers.

5

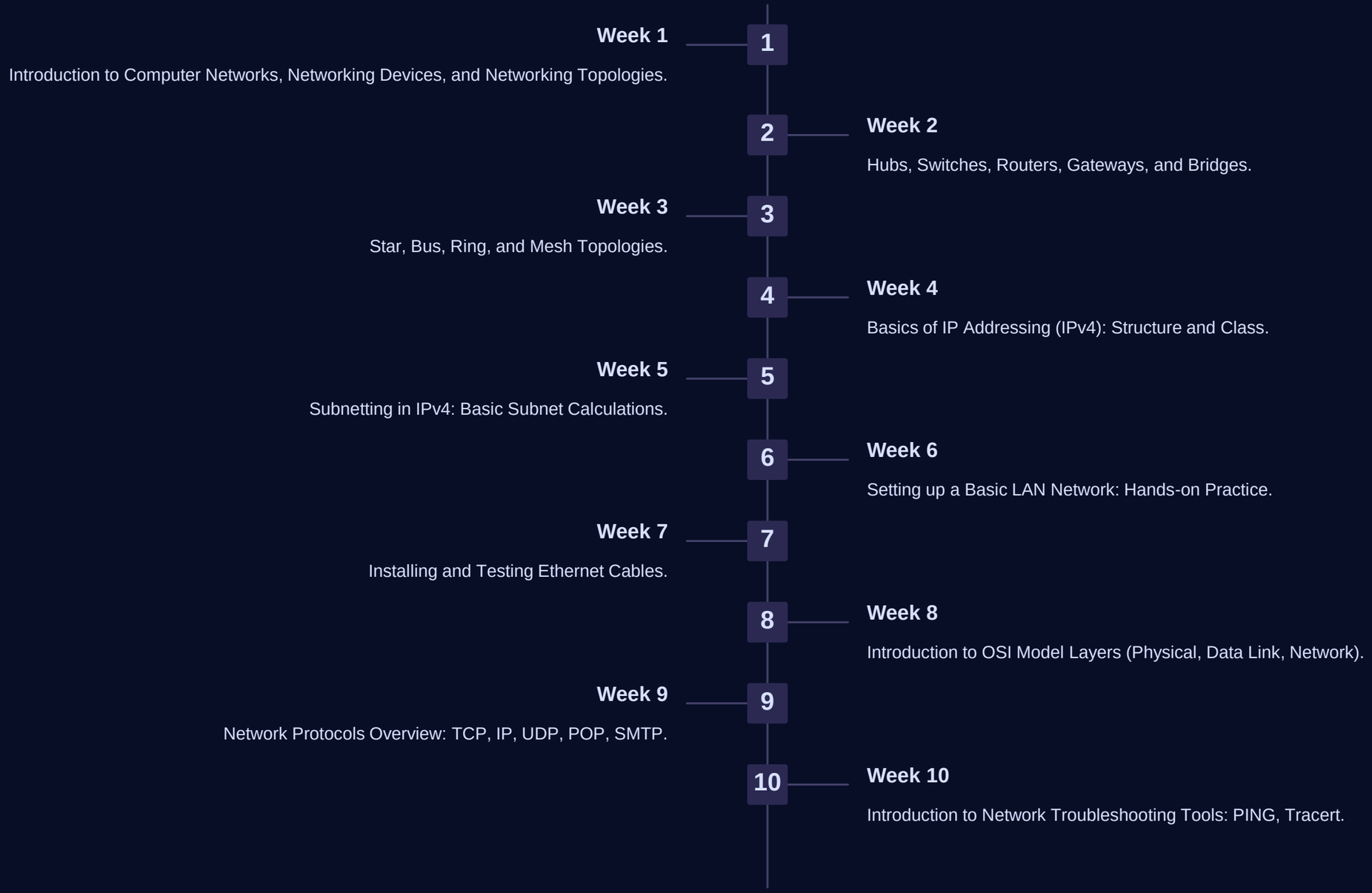
CLO5

Integrate emerging technologies (SDN, IoT, Cloud Networking) and advanced network security practices into systems.

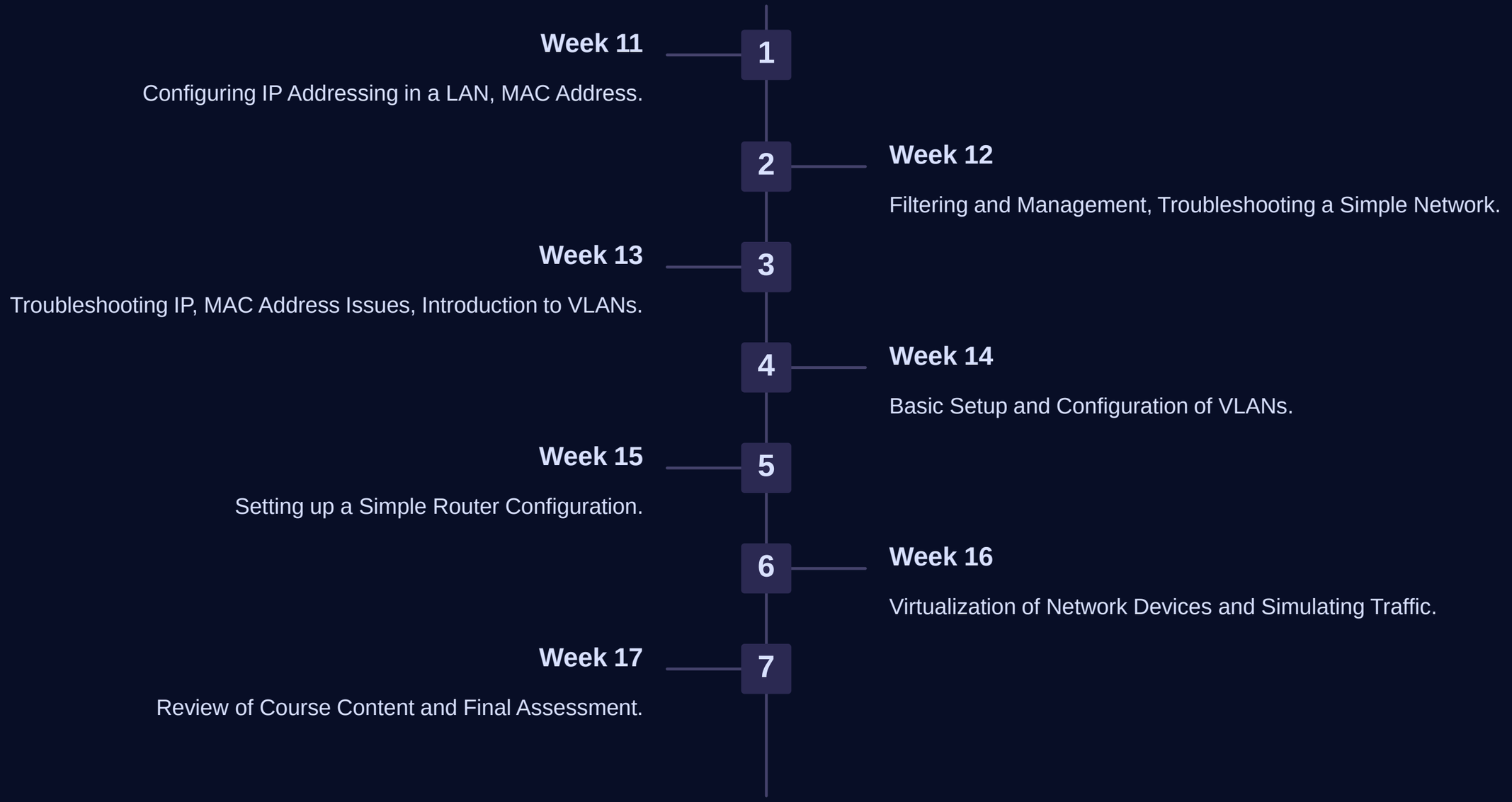
Course Content Overview

- Introduction to Computer Networks: LAN, MAN, WAN
- Networking Devices: Hubs, Switches, Routers, Gateways, Bridges
- Networking Topologies: Star, Bus, Ring, Mesh
- Basics of IP Addressing (IPv4) and Subnetting
- Setting up Basic LAN Networks
- Install and Test Networking Cables (Ethernet, Coaxial)
- Introduction to OSI Model Layers
- Testing Network Connectivity (PING, Tracert)

Course Plan: Weeks 1-10



Course Plan: Weeks 11-17



Assessment Pattern

Continuous In-course Evaluation (CIE)

- Lab Participation: 10 marks
- Assignments: 10 marks
- Quizzes: 10 marks

Final Project Evaluation

- Project Implementation: 10 marks
- Project Presentation: 5 marks
- Project Report: 5 marks

Recommended Books and Resources

Textbook

"Computer Networking: A Top-Down Approach" by James Kurose and Keith Ross.

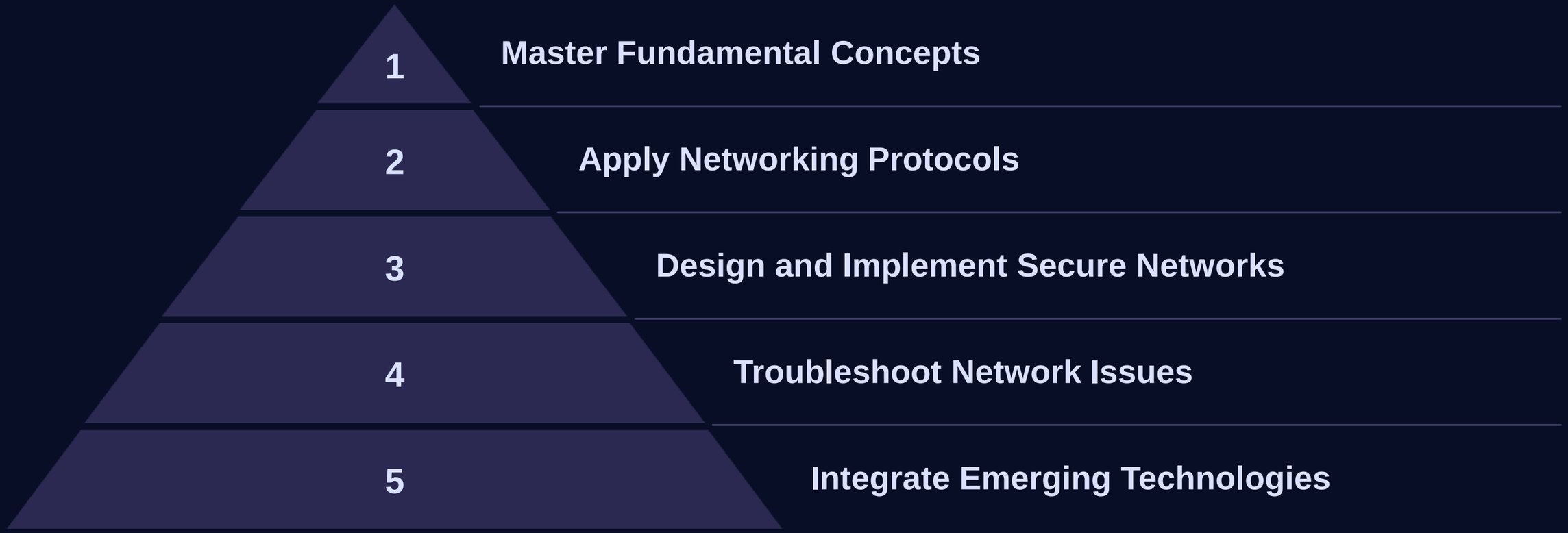
Reference Books

- "Computer Networks" by Andrew S. Tanenbaum
- "Network Security Essentials" by William Stallings

Online Resources

- https://www.udemy.com/topic/network-security/
- https://www.tutorialspoint.com/network_security/index.htm
- https://www.youtube.com/c/NetworkChuck
- https://www.youtube.com/user/professormesser
- https://www.youtube.com/results?search_query=cisco+packet+tracer+tutorial

Key Takeaways and Next Steps



This course provides a strong foundation in networking concepts, equipping you with the skills to design, implement, and troubleshoot networks. Continue exploring advanced topics and emerging technologies to stay ahead in the dynamic field of networking.

WEEK-01

Introduction to Computer Networks: Concepts of LAN, MAN, WAN

Welcome to the lab! Today we'll explore the fundamentals of computer networks, specifically focusing on the distinctions between LAN, MAN, and WAN. By the end, you'll have a solid understanding of these essential networking concepts and their applications.

by Md. Tariqul Islam

Objectives

Fundamentals of Computer Networks

We'll start by defining what a computer network is and how it works. We'll cover the basics of network communication, including protocols, addressing, and routing.

LAN, MAN, and WAN

We'll then delve into the differences between Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs). We'll discuss their characteristics, applications, and how they are used in the real world.

Required Equipment

Computers

We will be using standard desktop or laptop computers for this lab. Each computer should have a network interface card (NIC) for connecting to the network.

Network Switch

A network switch will be used to connect the computers together. It acts as a central point for communication and allows multiple devices to share the network.

Cables

We will use Ethernet cables to connect the computers to the switch. These cables transmit data signals between devices over a wired connection.

Network Interface Card

The NIC is a hardware component that allows a computer to connect to a network. It is responsible for transmitting and receiving data over the network.

Network Topologies

1 Star Topology

In a star topology, all devices are connected to a central hub or switch. This is a common topology for LANs as it offers centralized control and ease of management.

2 Bus Topology

A bus topology has a single cable that acts as a backbone, to which all devices are connected. Data travels along the bus, reaching all devices. This topology is simple and cost-effective, but suffers from performance issues with heavy traffic.

3 Ring Topology

In a ring topology, devices are connected in a closed loop. Data travels in one direction around the ring, passing through each device. This topology is efficient, but if one device fails, the entire network can be disrupted.

4 Mesh Topology

A mesh topology has multiple connections between devices, creating a robust and redundant network. While highly reliable, it's expensive and complex to implement.

LAN (Local Area Network)

Definition

A LAN connects devices within a limited geographical area, typically a single building or office. It's commonly used in homes, offices, schools, and other organizations.

Characteristics

LANs offer high bandwidth, low latency, and are usually privately owned and managed. They can be wired or wireless, using technologies like Ethernet and Wi-Fi.

Applications

Common applications of LANs include file sharing, printer sharing, internet access, and gaming within a local area. It's the backbone of most modern office environments.

MAN (Metropolitan Area Network)

1

Definition

A MAN covers a larger geographical area than a LAN, typically a city or a large campus. It's designed to connect multiple LANs within a metropolitan area.

2

Characteristics

MANs offer high bandwidth, but typically have lower bandwidth than WANs. They are often managed by a service provider and serve a larger community than LANs.

3

Applications

MANs are used for applications like high-speed internet access, government and corporate networks, and connecting educational institutions within a city.

WAN (Wide Area Network)

1

Definition

A WAN spans a vast geographical area, often connecting different cities, countries, or continents. It's used to connect organizations and individuals across the globe.

2

Characteristics

WANs utilize high-speed communication lines, often leased from telecommunication providers. They offer very high bandwidth but are often expensive and complex to maintain.

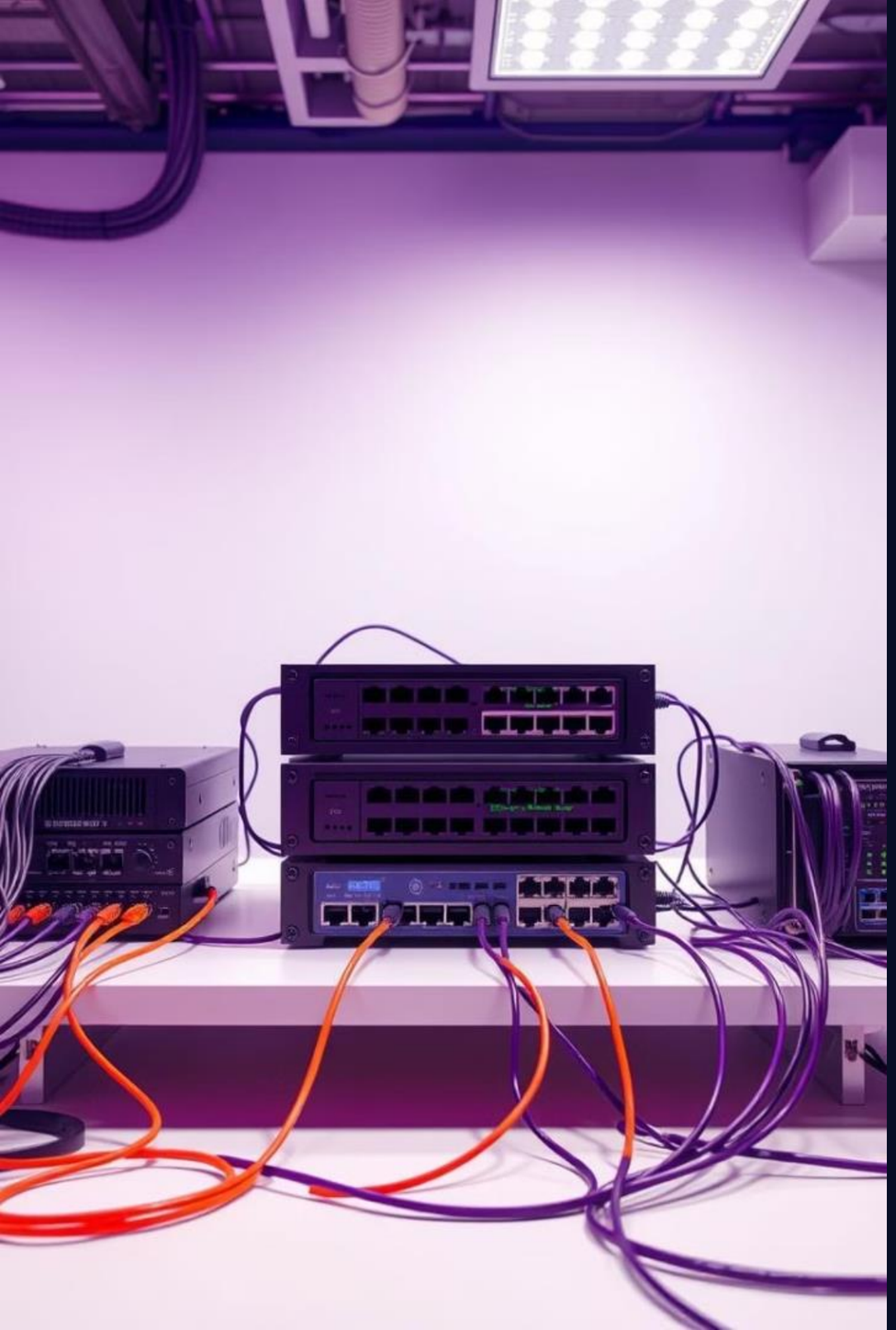
3

Applications

WANs are essential for global communication, allowing organizations to share data, conduct video conferences, and collaborate on projects across continents.

Conclusion and Key Takeaways

In this lab, we've learned about the fundamentals of computer networks and the distinct features of LANs, MANs, and WANs. We've discussed their applications, characteristics, and how they differ based on their scope and purpose. Now you can confidently distinguish between these network types and understand their role in today's interconnected world.



Week-02
Networking Devices: Hubs, Switches, Routers, Gateways

by Md. Tariqul Islam

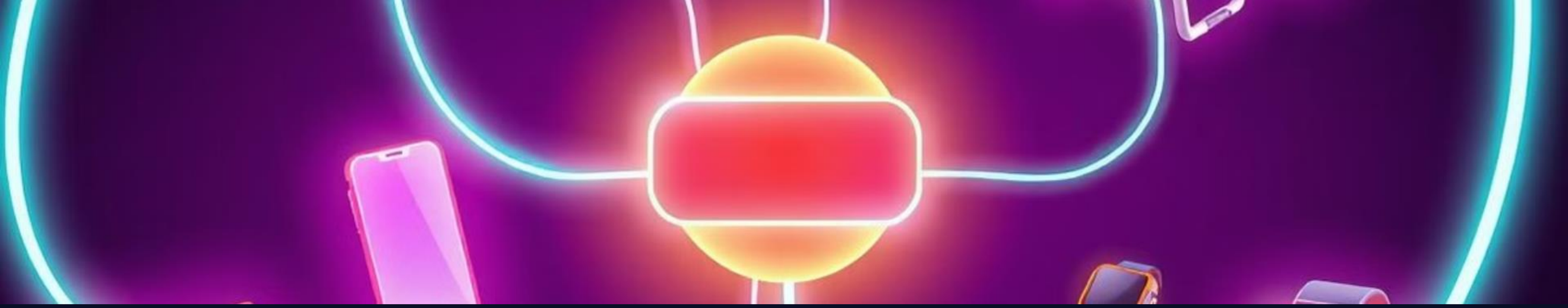
Lab Objectives and Overview

Understand Networking Basics

Explore the functions of hubs, switches, routers, and gateways in a network.

Hands-on Configuration

Practice configuring these devices with real-world scenarios and examples.



Needed Equipment for the Lab

Networking Devices

Hub, Switch, Router, Gateway (e.g., Cisco or Netgear)

Computers

At least two workstations with network interfaces.

Cabling

Ethernet cables to connect devices (UTP or STP).

Hub Functionality and Configuration

Shared Medium

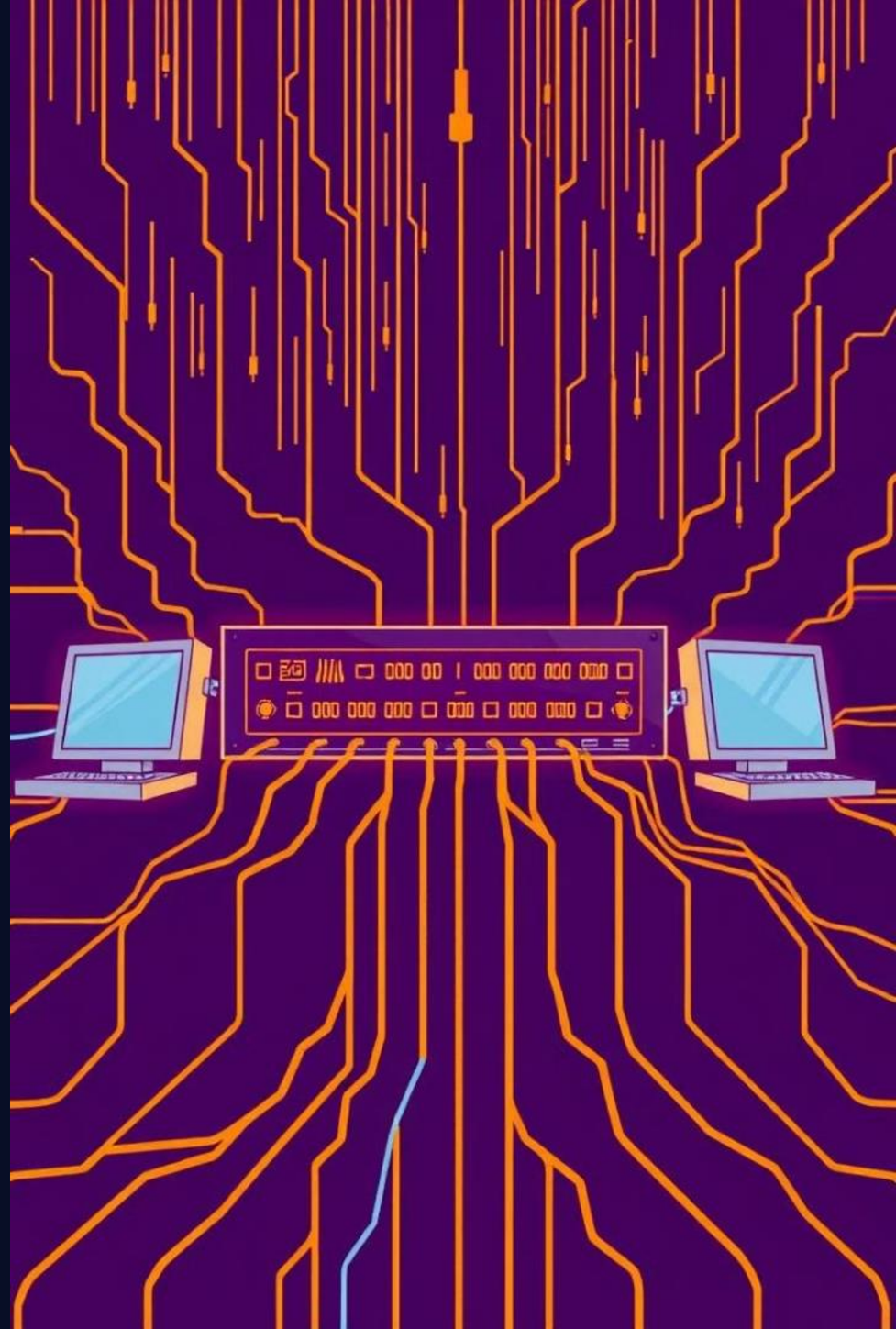
Transmits data to all connected devices.

Simple Configuration

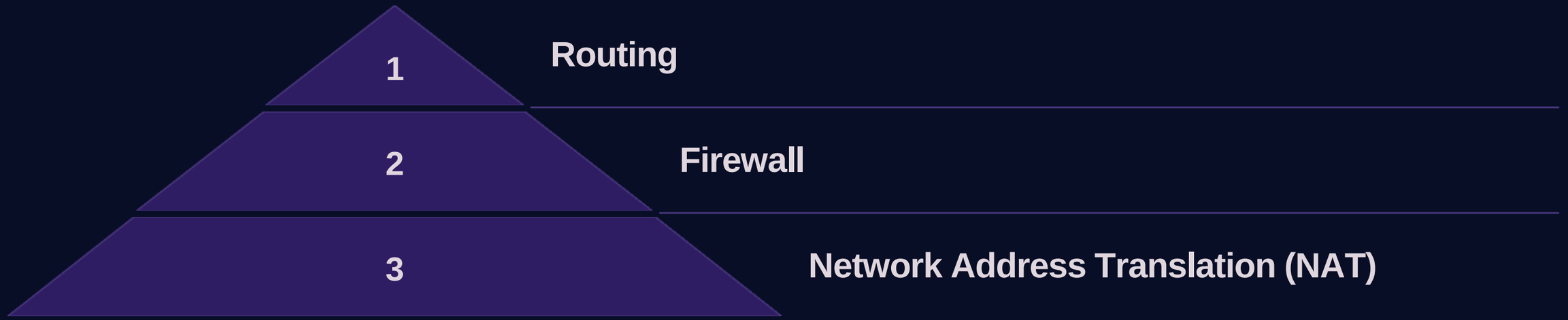
Typically plug-and-play, few settings.

Switch Functionality and Configuration

1. Learns MAC addresses of connected devices.
2. Creates separate paths for communication.
3. Offers more advanced features like VLANs.



Router Functionality and Configuration



Gateway Functionality and Configuration

1

Connection

Connects to different network types.

2

Protocol Translation

Converts data between protocols.

Lab Safety Requirements and Precautions

1

Static Electricity

Use grounding straps to prevent damage to equipment.

2

Cabling

Handle cables carefully to avoid damage.

3

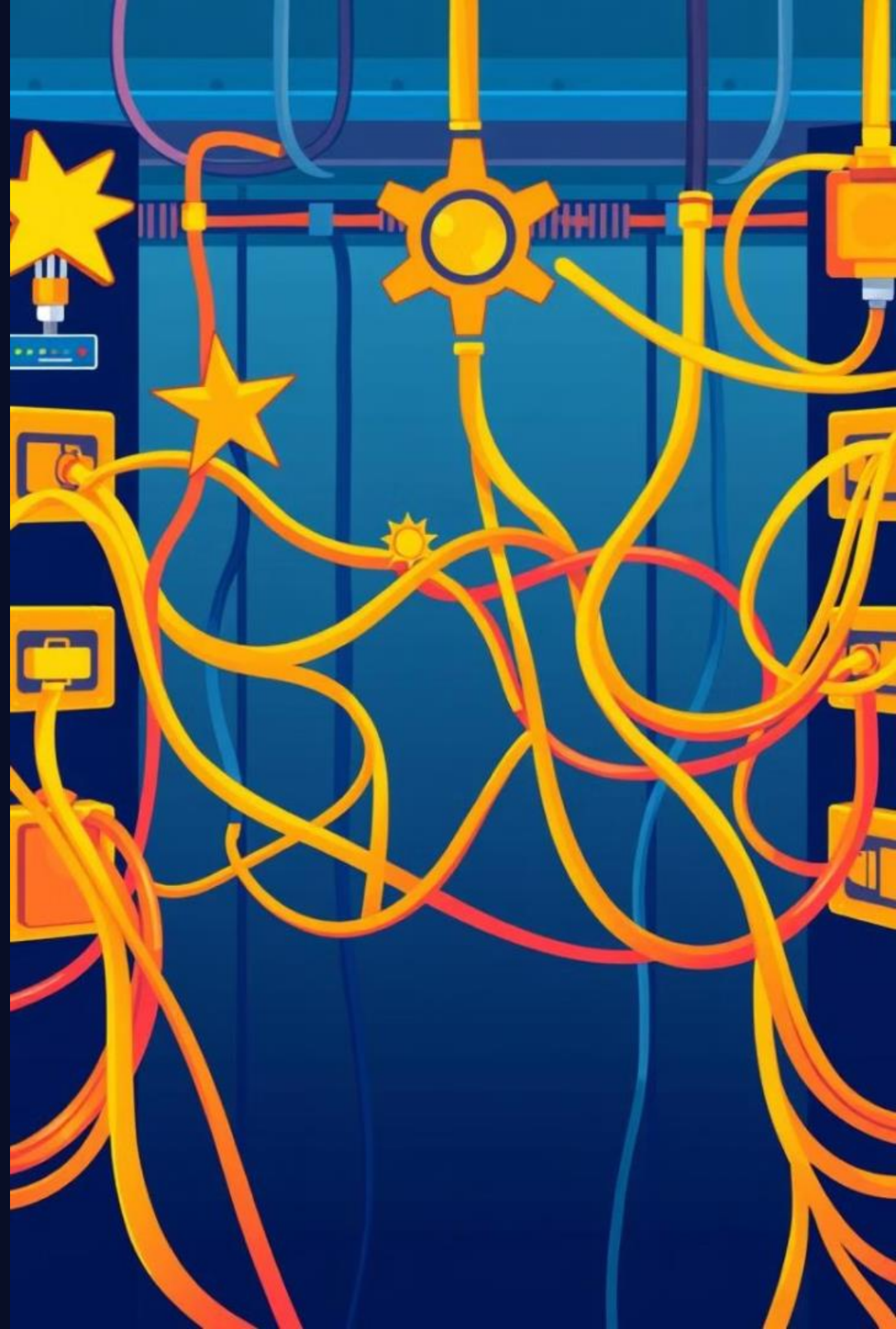
Power Management

Turn off devices when not in use.

Week-03
Networking Topologies: Star, Bus, Ring, Mesh

Welcome to this lab module on networking topologies, where we'll explore and experiment with four fundamental network designs: Star, Bus, Ring, and Mesh. We'll learn about their advantages, disadvantages, and real-world applications.

by Md. Tariqul Islam



Networking Lab Overview

Lab Objectives

Understand the basic principles of each topology, including its physical layout and data transmission characteristics.

Identify the strengths and weaknesses of each topology, considering factors like cost, performance, scalability, and reliability.

Lab Procedures

We'll use a combination of diagrams, hands-on activities, and simulations to illustrate the key concepts.

You'll be working with actual network equipment, such as network cables, switches, and routers, to simulate different topologies.

Required Equipment

1

1. Computers

Several workstations are needed for connecting to the network and running simulations.

2

2. Network Cables

Various types of network cables, such as Ethernet cables, will be used to connect devices.

3

3. Switches

Network switches are essential for connecting devices in a star topology.

4

4. Router

A router is needed for connecting networks and managing network traffic.

Safety Considerations

Electrical Safety

Handle electrical equipment with care and ensure proper grounding.

Cable Management

Keep cables organized and prevent tripping hazards.

Proper Use of Tools

Use tools safely and appropriately to avoid accidents.

Star Topology: Diagram and Explanation

Centralized Hub

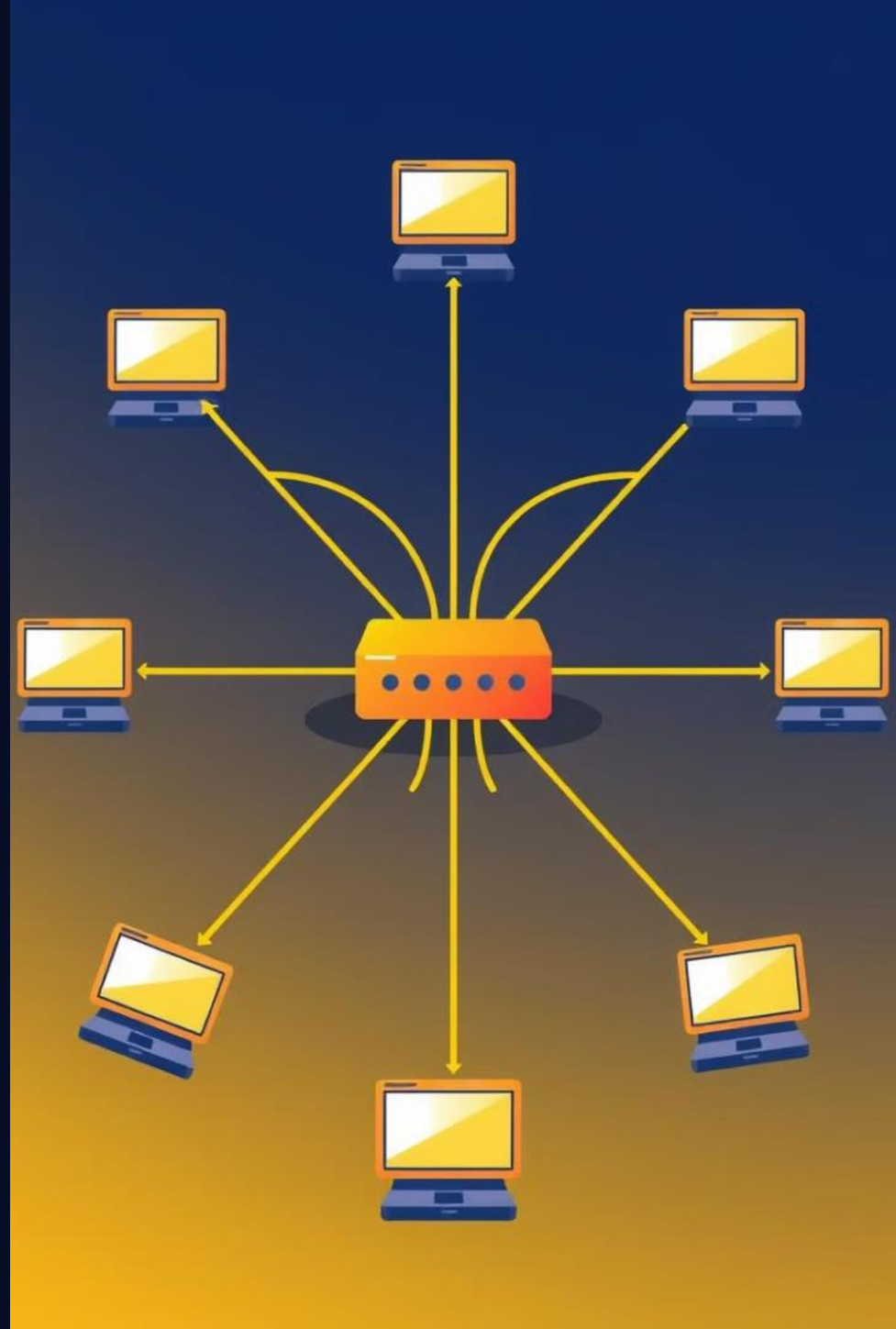
All devices connect to a central hub, typically a switch.

Dedicated Connections

Each device has a dedicated connection to the hub, minimizing interference.

High Performance

Data transmission is fast and efficient.



Bus Topology: Diagram and Explanation

1

Shared Medium

Devices share a single cable, making it a cost-effective option.

2

Simple Setup

Easy to install and configure.

3

Performance Issues

Data collisions can occur, slowing down network performance.

Ring Topology: Diagram and Explanation

1

Circular Network

Devices are connected in a closed loop, with data traveling in a single direction.

2

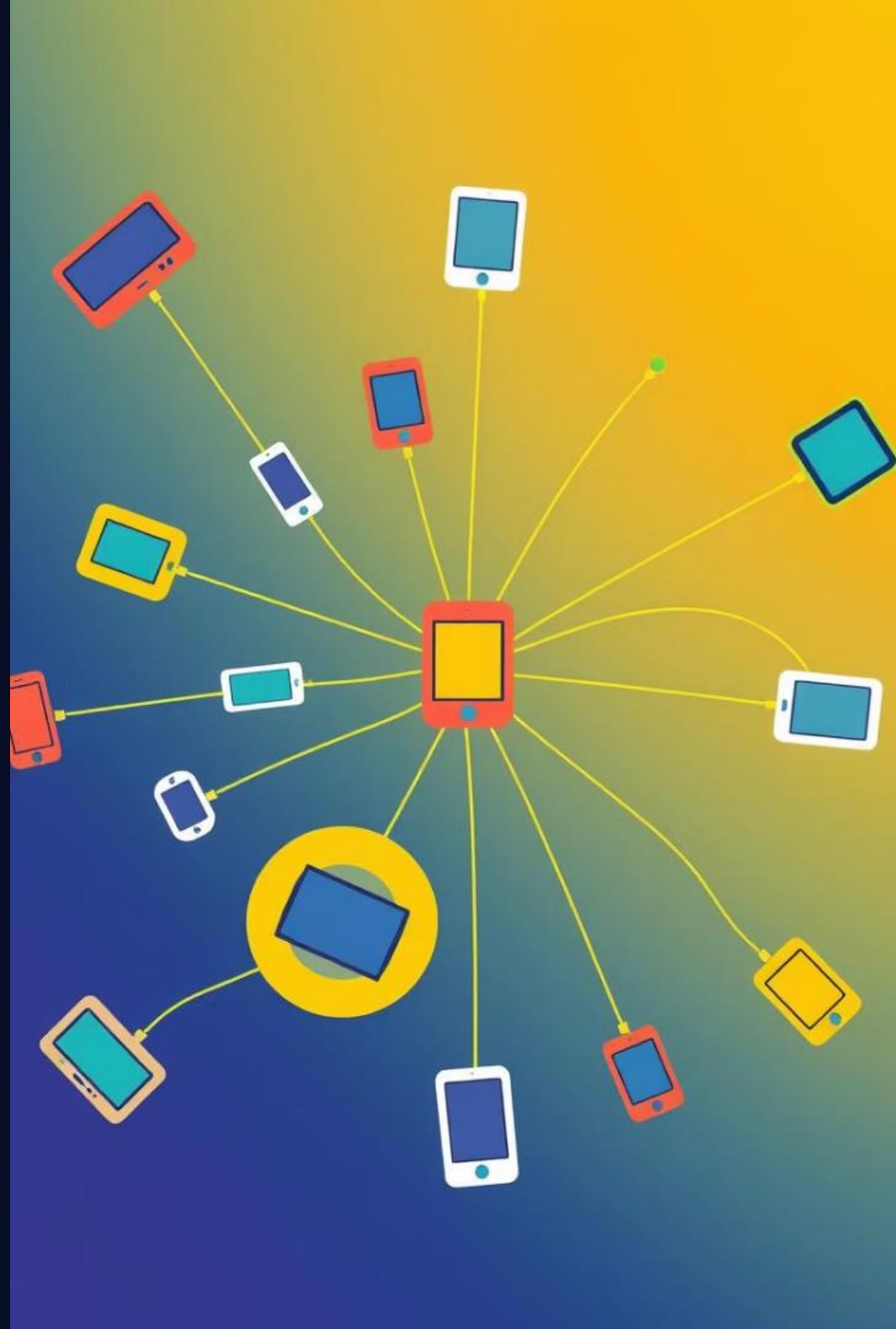
High Bandwidth

Data transmission is efficient and fast.

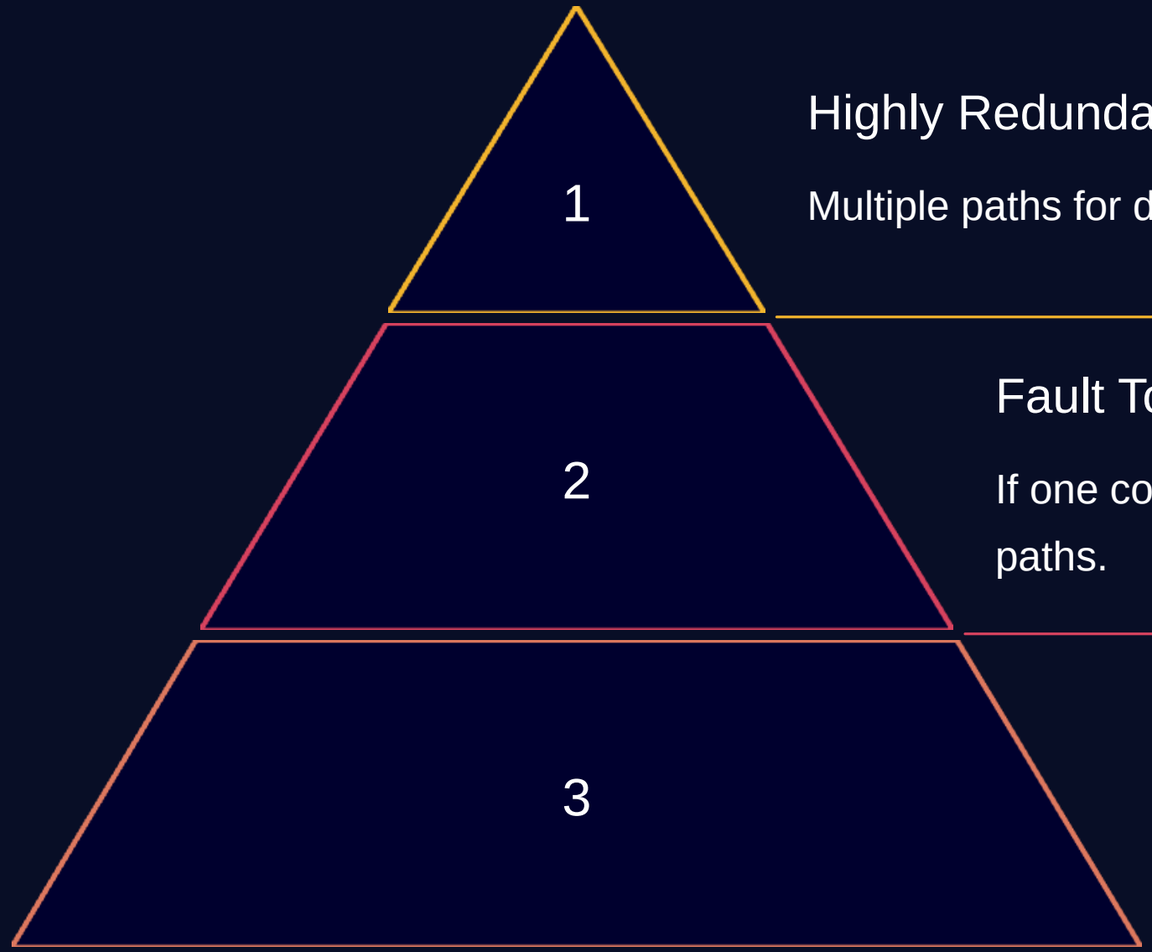
3

Single Point of Failure

If one device fails, the entire network can be disrupted.



Mesh Topology: Diagram and Explanation



Highly Redundant

Multiple paths for data transmission.

Fault Tolerant

If one connection fails, data can still be transmitted through other paths.

Expensive and Complex

Requires a lot of cabling and configuration.

Week-04

Basics of IP Addressing (IPv4): Structure and Class

This lab module introduces the fundamentals of IPv4 addressing, covering its structure, classification, and subnet division. You will gain hands-on experience configuring IPv4 addresses on Cisco network devices.

by Md. Tariqul Islam

Needed Equipment

Cisco Routers

Multiple Cisco routers will be used to demonstrate IP addressing concepts.

Cisco Switches

Switches will connect workstations and routers for network communication.

Cables

Ethernet cables connect devices together, transmitting data over the network.

Workstations

Workstations will act as endpoints, configured with IPv4 addresses.

Lab Objectives

IPv4 Address Structure

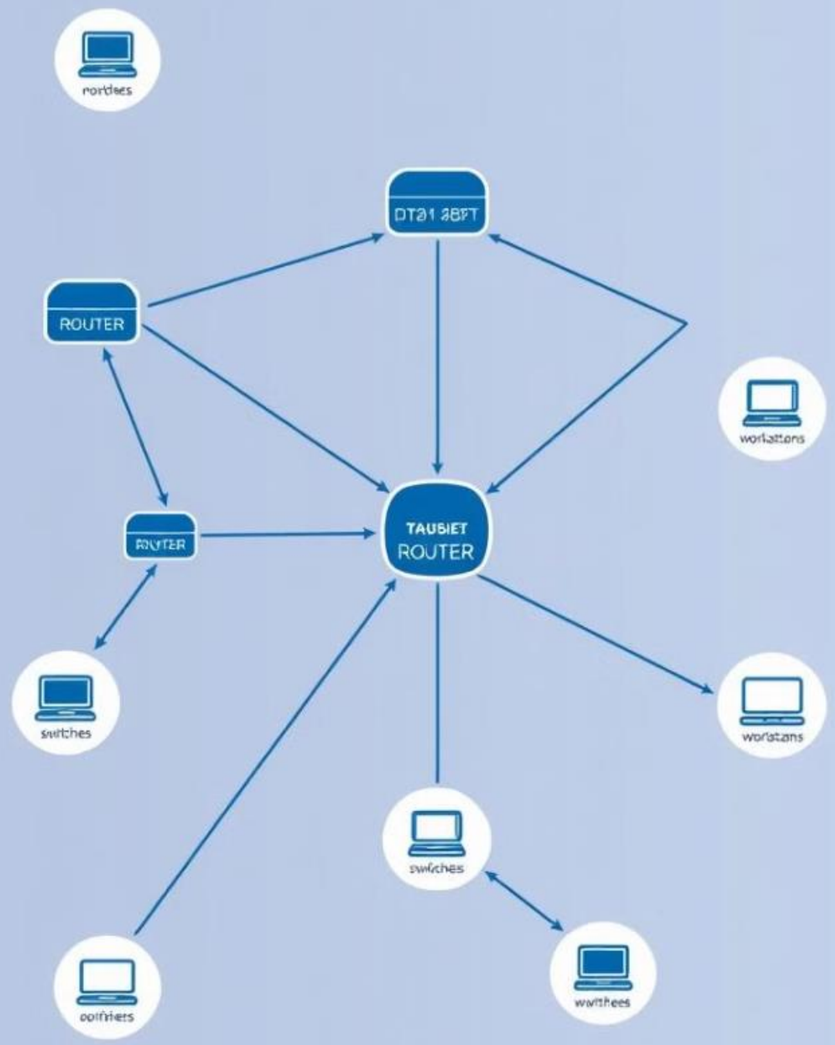
Learn the format of IPv4 addresses, including network and host portions.

IPv4 Address Classes

Understand the different classes of IPv4 addresses (A, B, C) and their features.

Subnetting

Explore the concept of subnetting, dividing a network into smaller subnets.



IPv4 Address Structure

Network Bits

Identify the network portion of the address, determining the network to which a device belongs.

Host Bits

Identify the host portion of the address, distinguishing individual devices within a network.

IPv4 Address Classes

Class A

Large networks, typically used by large organizations or ISPs.

Class B

Medium-sized networks, suitable for organizations with moderate network needs.

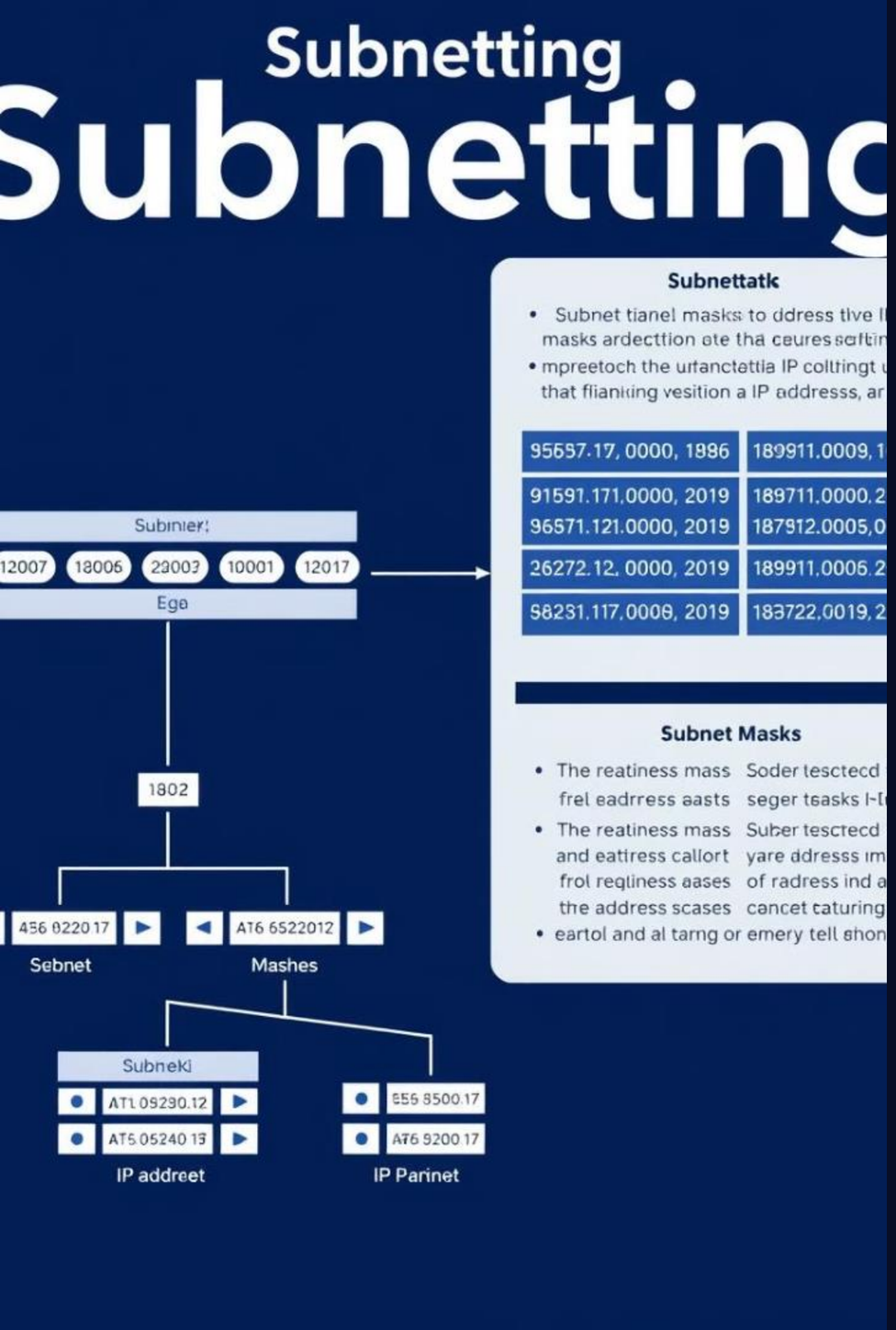
Class C

Small networks, commonly used for home networks or small businesses.

IPV4 ADDrESS

IPV4 address classes roots siegplets networing and bifffer reyiact tannplee, peopiant on your bit of apranes.

IP.A	Bit NeCls811	31..96..(103) 12:96 30	Examplend 34.901.(1019 12101 37	34..84.(103) 15.16 20
A4	1970060	52330.909	51383.205	5199.805
T2	1978000	52393.100	17347.756	1985.976
C8	5558300	53383.035	19383.869	2968.061
C5	5358531	52388.201	19323.993	2588.972
14	1653300	53383.330	53383.963	5498.630
C7	1563500	33383.190	15383 266	4406.284
C4	2373582	53381.666	55185.369	5888.680
T.8	04:0302	15894.1262	26164.2022	2.688.861
E3	06.0001	10194.5577	57354.0031	1.667.962
E6	49:03971	57498.5517	17374.0067	17.30.665



Subnetting

Network Segmentation

Subnetting divides a network into smaller, manageable units.

Enhanced Security

Improved security by isolating subnets and restricting access.

IP Address Conservation

Optimize IP address usage by allocating addresses efficiently.

Subnet Mask

1. Identifies the network portion of an address.
2. Determines which bits are for the network and which are for the host.
3. Enables the identification of the subnet to which a device belongs.

Subnet Calculator

1

Network Address

Enter the base network address.

2

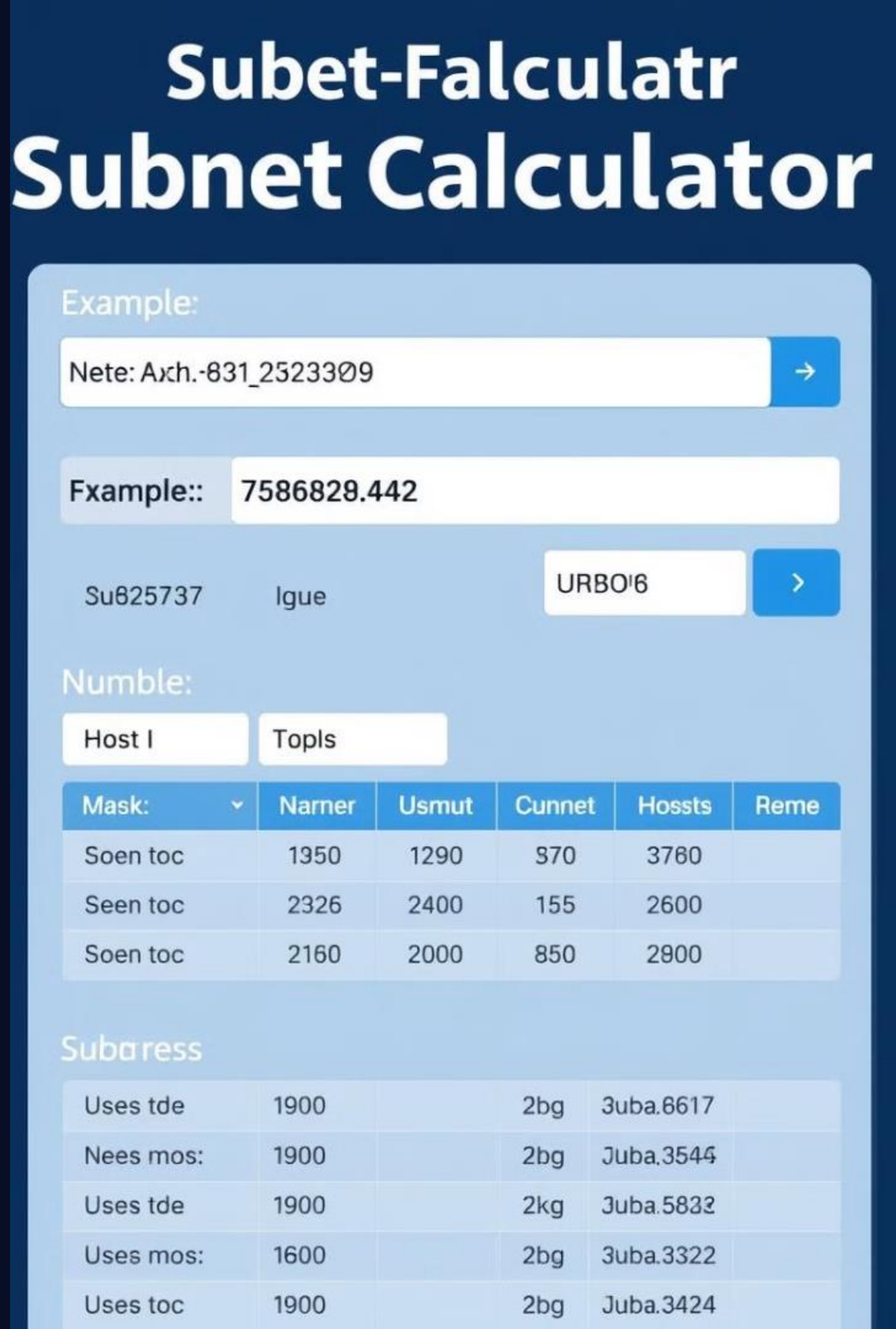
Subnet Mask

Specify the desired subnet mask.

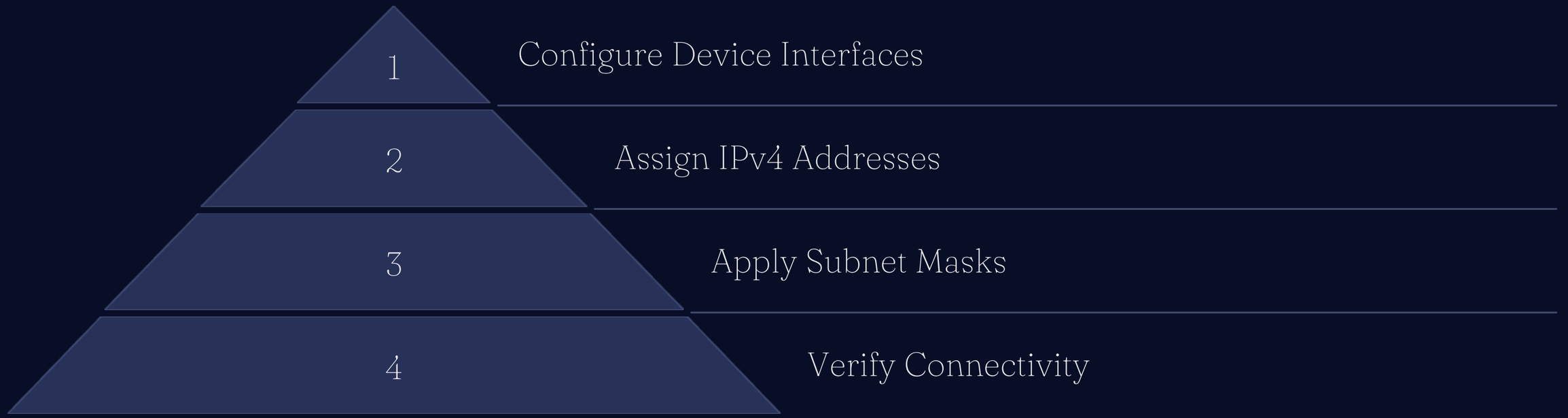
3

Results

View the calculated subnet information.



Lab Setup: IPv4 Configuration



Conclusion: Key Takeaways and Lab Exercises

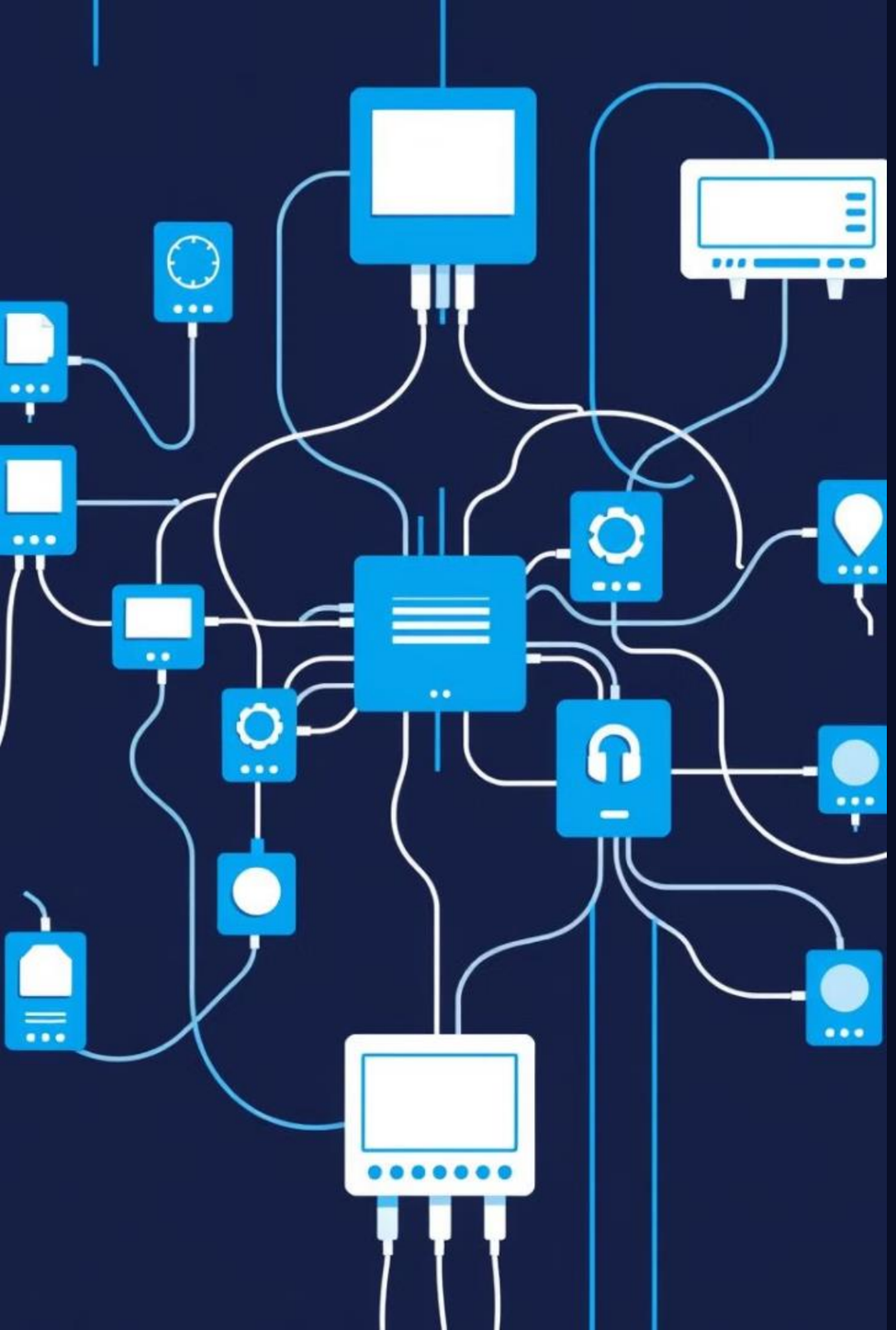
1 IPv4 Address Structure

2 Address Classes

3 Subnetting

4 Lab Exercises

Practice configuring IPv4 addresses and subnet masks.



Week: 5
Subnetting in IPv4: Basic Subnet Calculations

by Md. Tariqul Islam

Objectives and Equipment

Objectives

- Understand subnet masks and CIDR notation.
- Calculate subnet information.
- Allocate and assign IP addresses.
- Identify broadcast addresses and usable hosts.

Equipment

- Computer with network access.
- Text editor or spreadsheet software.
- Optional: Network simulator or virtual environment.

Subnet Masks and CIDR Notation

1 Subnet Mask

A subnet mask is a 32-bit value used to separate a network address from a host address.

2 CIDR Notation

Classless Inter-Domain Routing (CIDR) uses a slash followed by the number of bits used for the network portion of the address.

Determining Subnet Information

Network Address

Subnet Mask

The subnet mask indicates the network portion of the IP address.

Number of Subnets

Determined by the number of bits borrowed from the host portion of the address.

Hosts per Subnet

Calculated by subtracting the number of bits borrowed from the total number of host bits.

IP Address Allocation and Assignments

Network Address

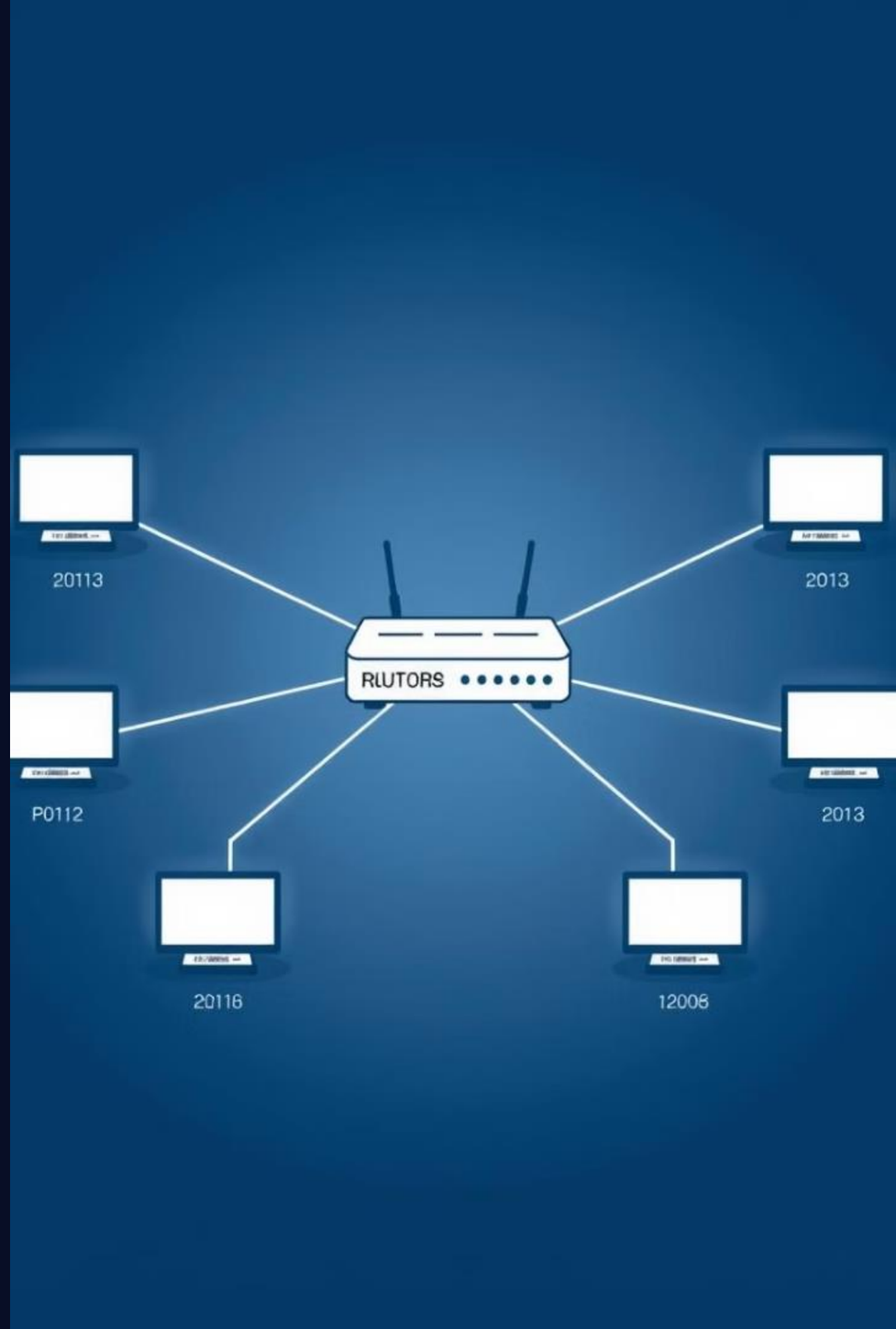
The first IP address in a subnet is reserved for the network itself.

Broadcast Address

The last IP address in a subnet is reserved for broadcasting messages to all hosts.

Usable Hosts

All other IP addresses within a subnet are available for host assignments.



Broadcast Addresses and Usable Hosts

1

Broadcast Address

The broadcast address is used to send messages to all devices on a subnet.

2

Usable Hosts

The number of usable hosts per subnet can be calculated using the formula 2^(number of host bits) - 2.

IP A ddchesse adcleeɛhase

Network adress	Subnet maslk		Ne•-- lust raddress	Dyaadcast erdcdress	Use Host range	Use - ted inpolange
120100	2000	134	226	4.5	199	129
120160	2007	3.4	305	6.4	152	132
120700	2008	1.9	315	6.5	158	271
120160	2275	9.9	306	4.7	350	121
10074	2027	1.8	313	4.9	217	213
12072	2019	3.9	256	4.8	220	243
22027	2020	205	106	3.6	295	734
100100	2011	275	208	3.6	250	474
220741	2019	208	205	325	230	339

Practical Examples and Scenarios

10

Scenario 1

Divide a network into 8 subnets.

20

Scenario 2

Allocate IP addresses to 20 devices on a subnet.

Hands-on Subnet Calculation Exercise



For this exercise, you will need to divide a network into subnets and assign IP addresses to specific devices.

Week: 06
Setting up a Basic LAN Network: Hands-on Practice

by Md. Tariqul Islam

Needed Equipment

Router

A gateway to connect the LAN to the internet or a larger network.

Switches

Connect multiple devices on a network, creating a hub for communication.

Ethernet Cables

Transmit data between network devices using RJ-45 connectors.

Computers

The devices that will access the network and share resources.

Lab Objectives

1 **Understand LAN networking concepts**

Learn about network topologies, IP addressing, and network protocols.

2 **Configure network equipment**

Gain practical experience with router and switch configuration settings.

3 **Connect devices to a LAN**

Establish connectivity between computers and other devices on the network.

4 **Troubleshoot common networking issues**

Identify and resolve network problems using troubleshooting techniques.

Network Topology Diagram

Router

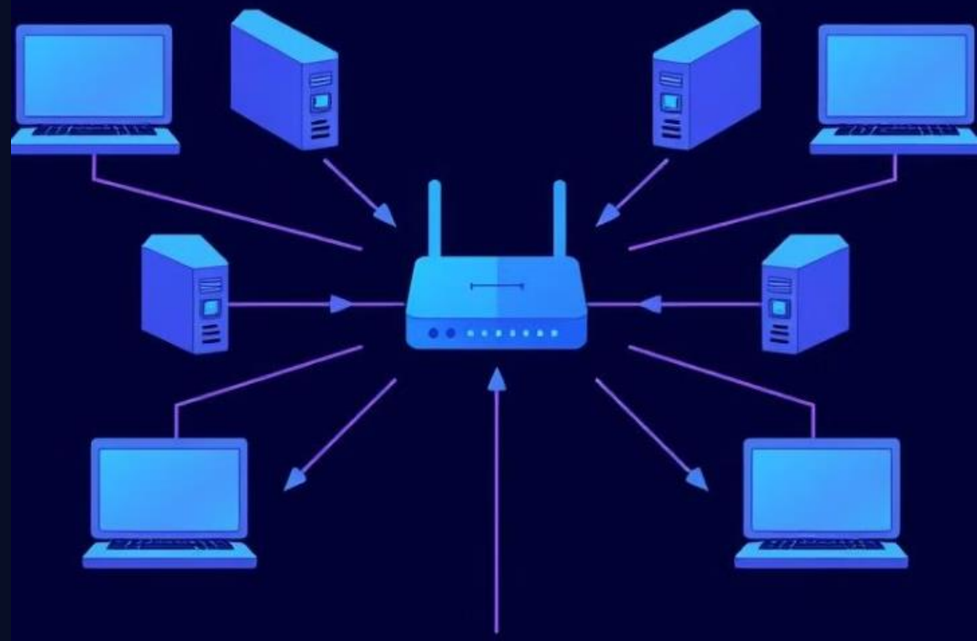
Connects to the internet or a larger network, managing data flow.

Switch

Connects multiple devices on the LAN, facilitating communication between them.

Computers

Access network resources and communicate with each other.



Configuring Router: WAN and LAN Interfaces

1

Configure WAN Interface

Set up the internet connection with the ISP's credentials.

2

Configure LAN Interface

Assign an IP address range for devices on the LAN network.

3

Configure Firewall

Enable security measures to protect the network from unauthorized access.

Configuring Switches: Ports and VLANs

1

2

3

Configure Ports

Assign IP addresses to each port connected to a device on the LAN.

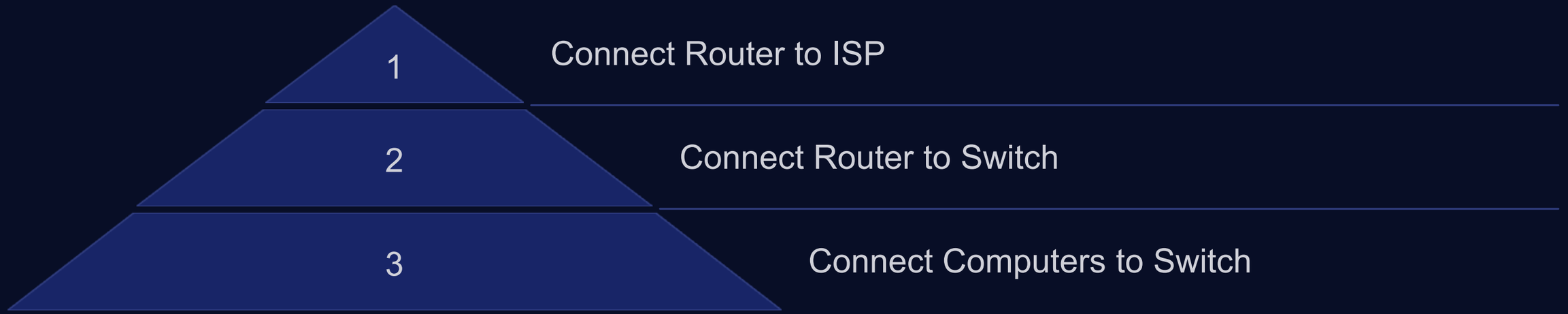
Create VLANs

Segment the network into virtual LANs for improved security and traffic management.

Assign Devices to VLANs

Group devices together based on their function or location.

Connecting Devices to LAN



Troubleshooting Connectivity Issues

1

Check Cables

Ensure cables are securely connected and not damaged.

2

Verify IP Addresses

Confirm that devices have valid IP addresses.

3

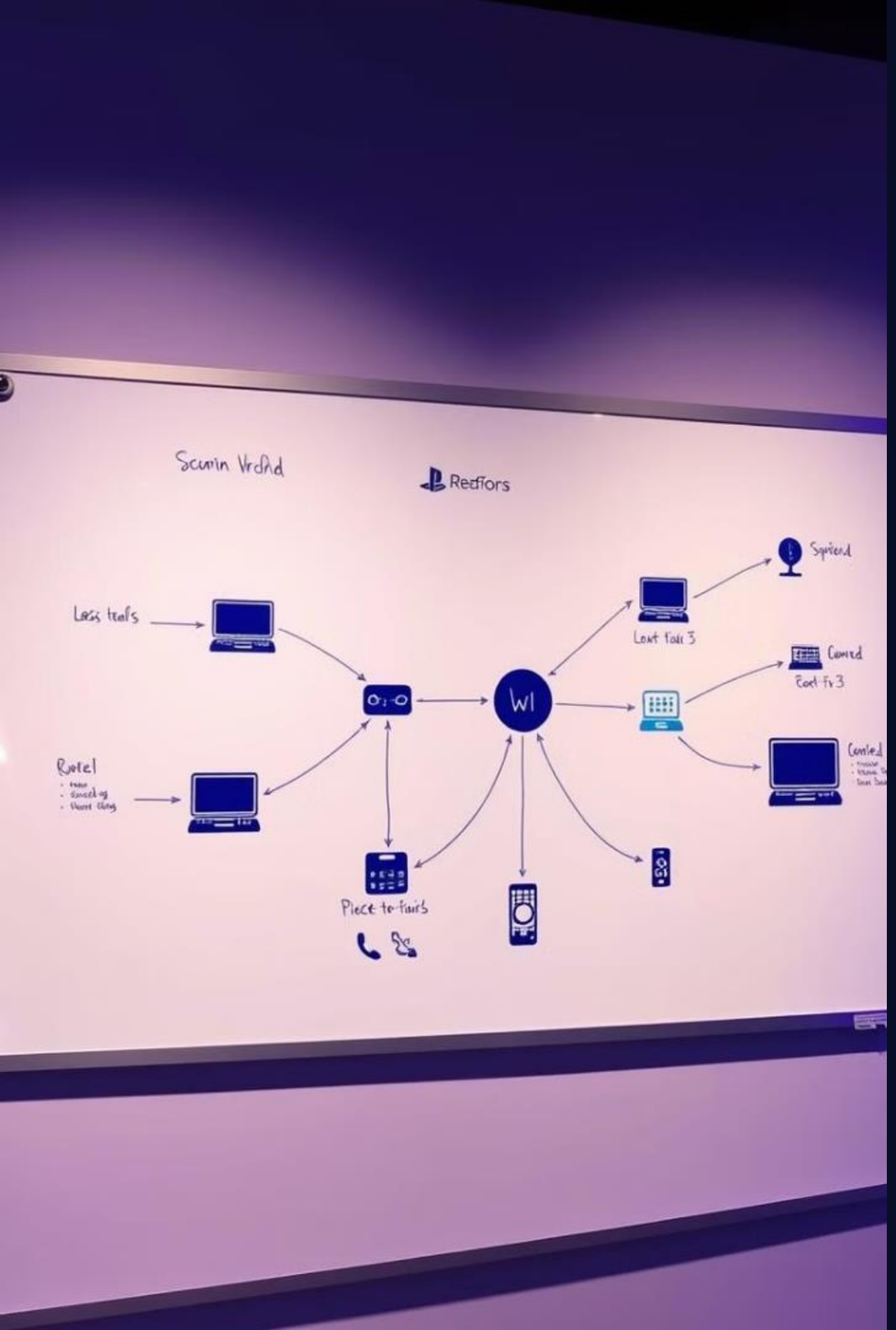
Check Network Settings

Ensure network settings on devices are configured correctly.

4

Use Network Tools

Utilize tools like ping and traceroute to diagnose connectivity issues.



Documenting the Network Setup

1

Network Diagram

Create a visual representation of the network.

2

IP Addresses

Record the IP addresses assigned to each device.

3

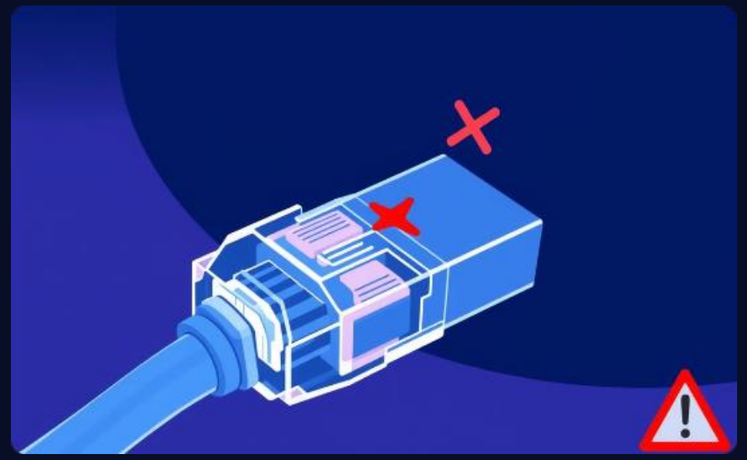
Configuration Settings

Document router and switch configurations.

Safety Requirements

Electrical Safety

Use surge protectors and avoid touching live wires.



Network Safety

Be cautious when connecting devices to the network.

Equipment Safety

Handle network equipment carefully and avoid dropping it.

Week:07
Installing and Testing Ethernet Cables

This presentation will walk you through the process of installing and testing Ethernet cables for reliable network connectivity.

by Md. Tariqul Islam

Objectives, Equipment, and Preparation

Objectives

Understand the purpose and components of Ethernet cables. Install Ethernet cables correctly and securely. Test network connectivity using appropriate tools.

Equipment

Ethernet cables, RJ-45 connectors, wire strippers, crimping tool, cable tester, network devices (router, switch), laptop or computer.

Preparation

Review cable types and specifications. Gather necessary tools and equipment. Familiarize yourself with network device configuration.

Ethernet Cable Overview and Specifications

1 **Twisted-Pair Technology**

Ethernet cables use twisted-pair wires to reduce interference.

2 **RJ-45 Connector**

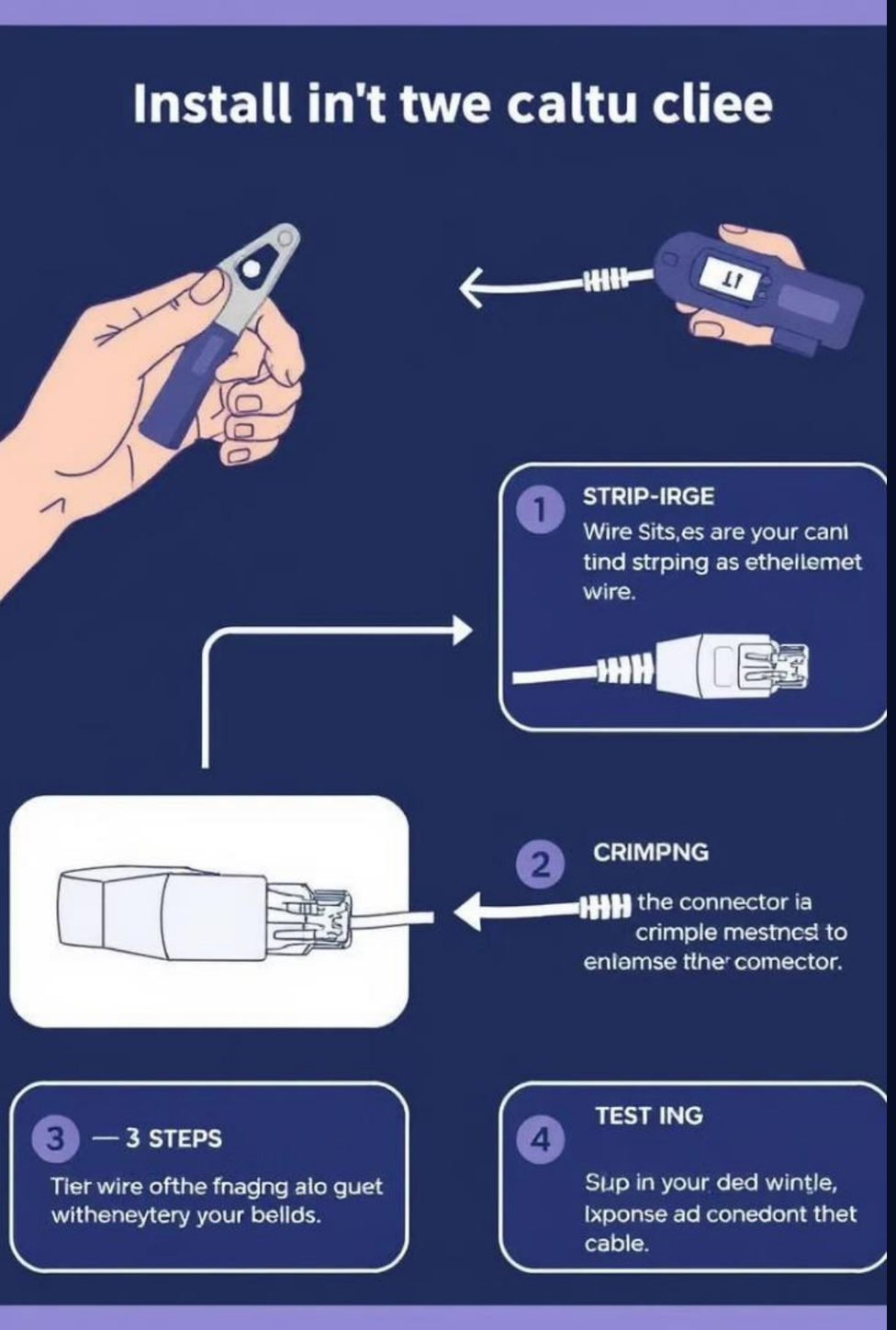
The connector on each end of the cable plugs into network devices.

3 **Cable Categories**

Different categories (Cat5e, Cat6, Cat6a) support varying data speeds and bandwidths.

4 **Cable Types**

UTP (Unshielded Twisted Pair) and STP (Shielded Twisted Pair) differ in their shielding.



Detailed Installation Procedure with Visuals

1

Wire Stripping

Use wire strippers to remove the outer insulation and expose the individual wires.

2

Wire Ordering

Arrange the wires according to the 568A or 568B standard.

3

Crimping

Insert the wires into the RJ-45 connector and crimp them securely.

4

Testing

Use a cable tester to verify proper wiring and connectivity.

Safety Considerations and Practical Examples

Safety Tips

Always use wire strippers and crimping tools correctly. Avoid excessive force during crimping. Disconnect power from network devices before working with cables.

Practical Example

Install an Ethernet cable from a router to a computer, ensuring a secure connection and testing the network afterward.

Troubleshooting

If there is no network connectivity, check cable connections, crimping, and network device configuration.

Data Collection and Troubleshooting

Signal Strength

Measure the signal strength to identify potential cable issues.

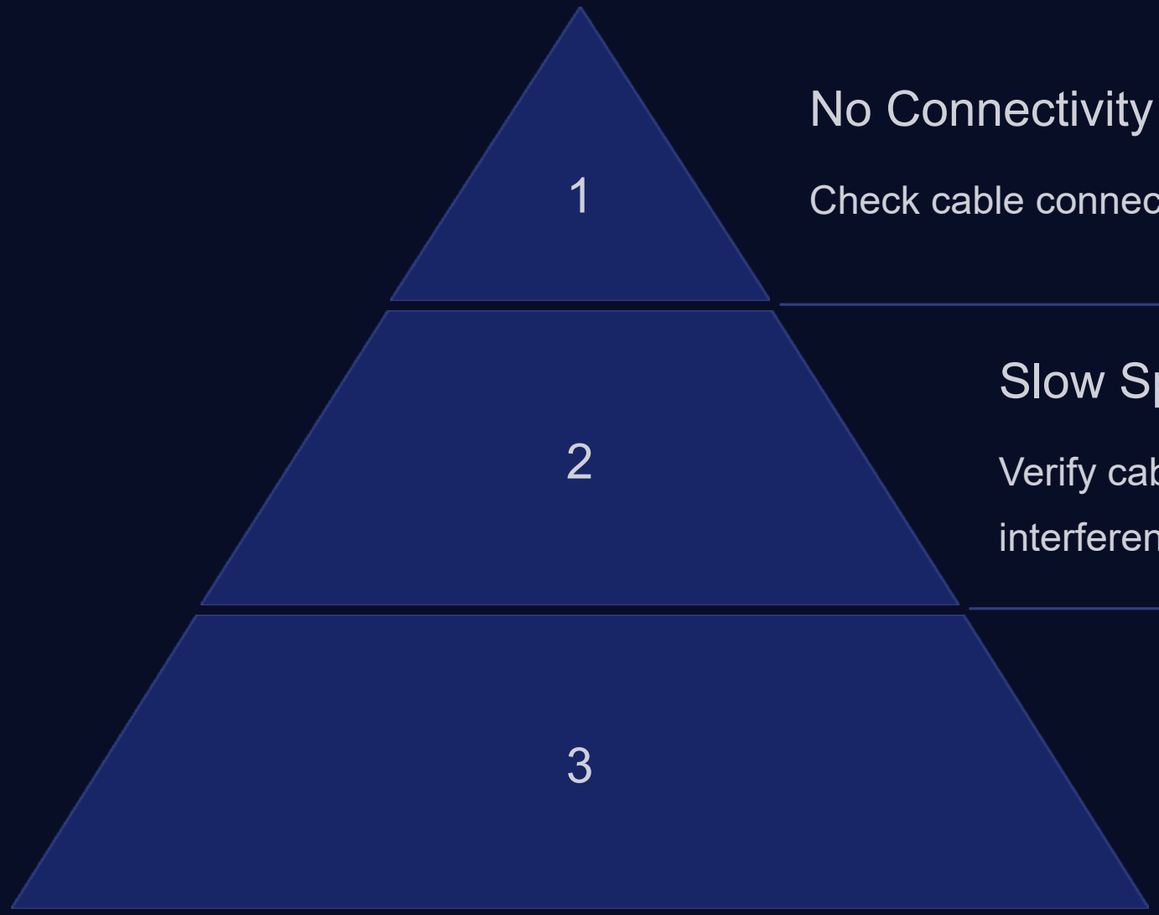
Latency

Check for excessive latency, which can indicate slow network performance.

Packet Loss

Monitor packet loss, which can indicate network errors or interruptions.

Common FAQs and Responses



No Connectivity

Check cable connections, crimping, network device configuration, and power.

Slow Speed

Verify cable category, network device settings, and potential interference.

Intermittent Connection

Inspect cable for damage, check network device status, and rule out environmental factors.

Summary of Key Takeaways

Installing and testing Ethernet cables requires careful attention to detail, proper tools, and safety precautions. With the right knowledge and practices, you can establish reliable network connectivity.

Week:08
Introduction to OSI Model Layers (Physical, Data Link, Network)

This presentation will introduce the core concepts of the OSI Model, focusing on the physical, data link, and network layers. We'll also cover practical aspects of installing and testing Ethernet cables.

by Md. Tariqul Islam

Objectives, Equipment, and Preparation

Objectives

- Understand the OSI Model's layers
- Learn about physical layer components
- Explore data link layer protocols
- Gain experience with Ethernet cable installation
- Master Ethernet cable testing and troubleshooting techniques

Equipment

- Ethernet cable
- RJ-45 connectors
- Network tester
- Laptop or computer
- Screwdriver

OSI Model: Physical Layer Fundamentals

Connectors

RJ-45 connectors are commonly used for Ethernet cables. They have eight pins, each carrying electrical signals.

Cables

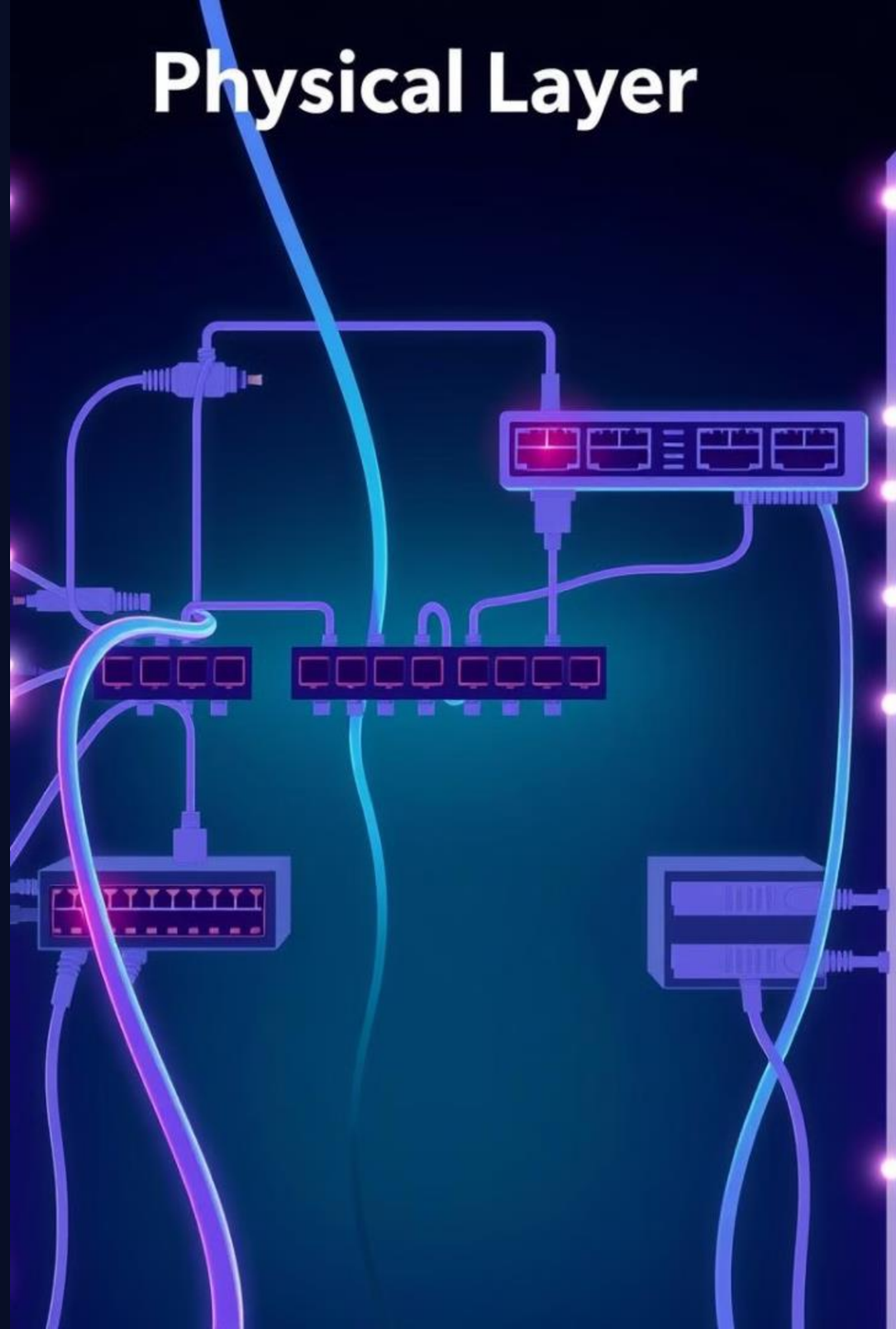
Twisted-pair cables are the most common type for Ethernet. They reduce interference by twisting pairs of wires together.

Hubs

Hubs act as central points in a network, connecting multiple devices together.

Network Interface Cards (NICs)

NICs are network adapters that allow devices to communicate over a network. They translate data into electrical signals.



OSI Model: Data Link Layer Concepts

MAC Addressing

Each device has a unique MAC address, used to identify it on the network.

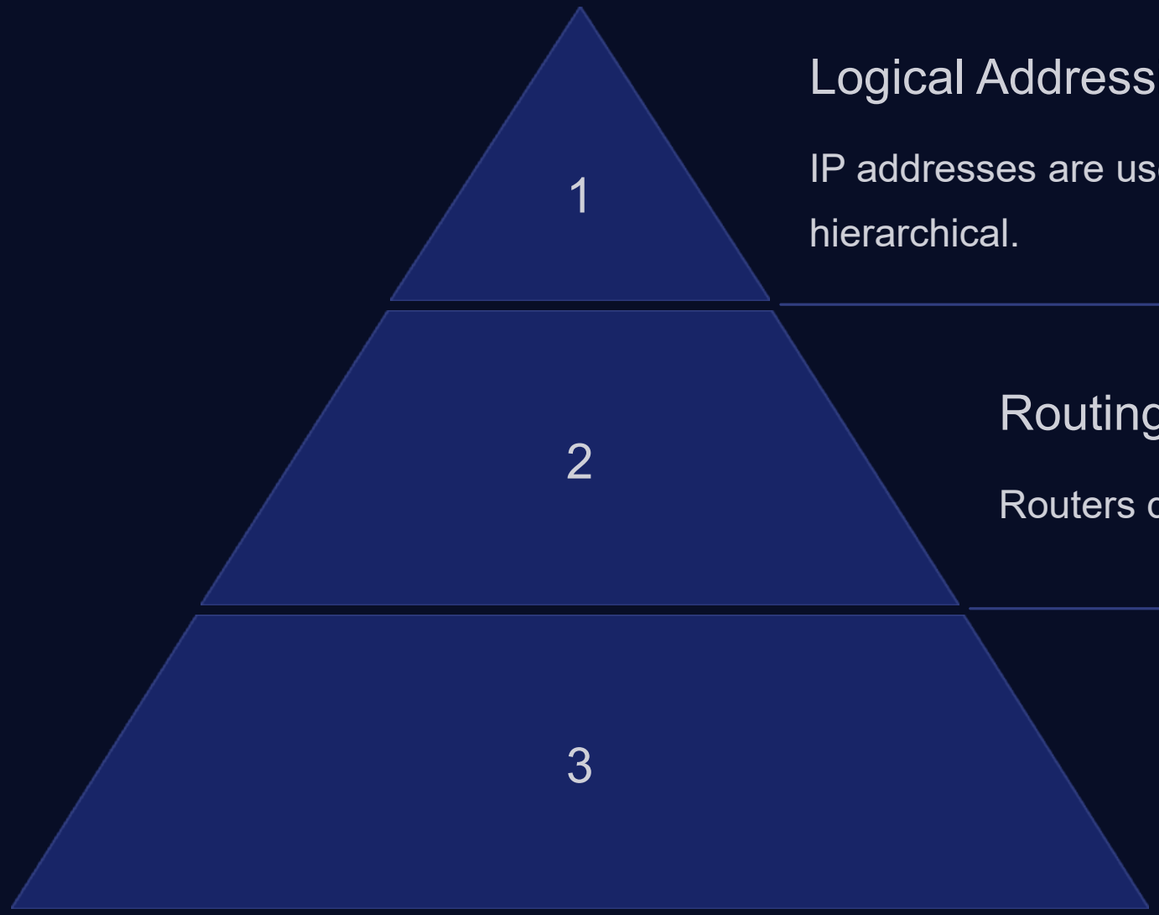
Frame Formatting

Data is encapsulated into frames with header and trailer information.

Error Detection

CRC checks are used to detect and correct errors during transmission.

OSI Model: Network Layer Functionality



Logical Addressing

IP addresses are used to identify devices on the network. They are unique and hierarchical.

Routing

Routers determine the best path for data to travel through the network.

Packet Switching

Data is broken down into packets, which are sent independently across the network.

Ethernet Cable Installation Procedure

1. Strip the outer insulation from the cable.
2. Separate the individual wire pairs.
3. Crimp the wires onto the RJ-45 connector.
4. Test the cable for connectivity using a network tester.

Ethernet Cable Testing and Troubleshooting

1

Cable Tester

Use a network tester to verify cable continuity, wiring order, and signal strength.

2

Troubleshooting

Check for loose connections, damaged cables, or incorrect wiring.

3

Troubleshooting Tips

Test all components of the network, including switches, routers, and devices.

Summary and Key Takeaways

The OSI Model provides a framework for understanding how networks function. The physical, data link, and network layers are crucial for data transmission. Mastering Ethernet cable installation and troubleshooting is essential for network professionals.

Week-09
Network Protocols Overview

Welcome to the introductory lab module on network protocols.

Objectives and Equipment

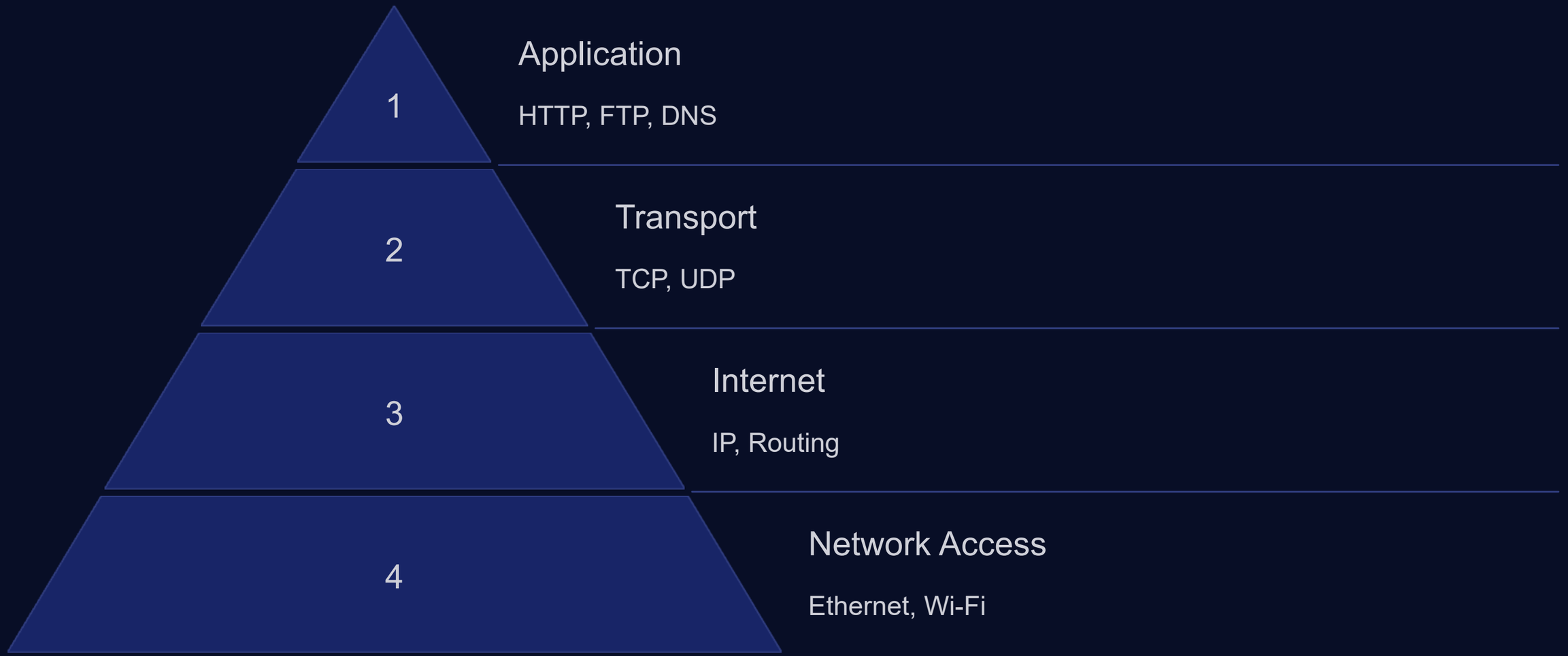
Objectives

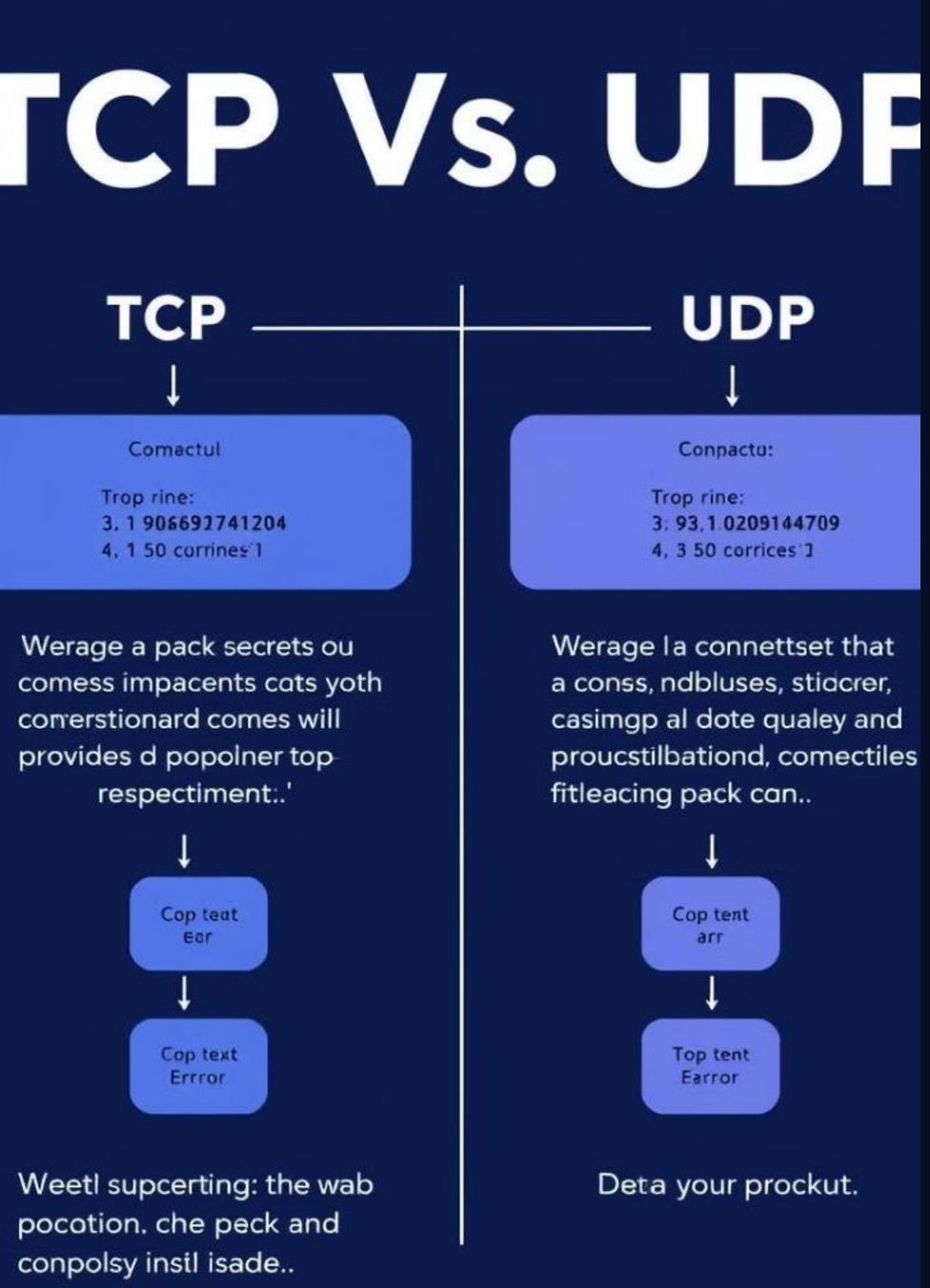
Understand the role of TCP/IP in communication. Identify the functionalities of UDP and its use cases. Learn about email protocols like POP and SMTP. Perform hands-on lab exercises.

Equipment

Laptop or computer with internet access. Network cable or Wi-Fi connection. Web browser and text editor.

TCP/IP Model Explained





UDP and its Applications

User Datagram Protocol (UDP)

Connectionless protocol. Faster but less reliable than TCP. Commonly used for streaming, gaming, and voice calls.

Key Features

Minimal overhead. No connection setup. Packet loss is expected.

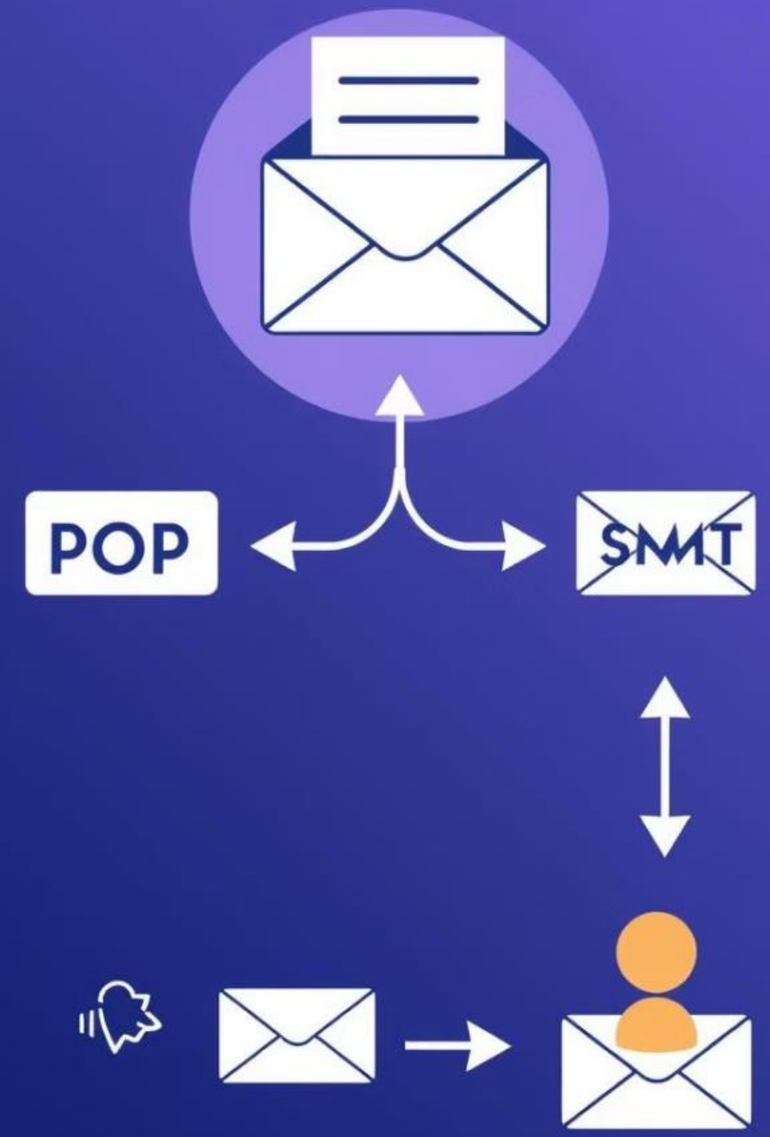
Email Protocols: POP and SMTP

Post Office Protocol (POP)

Downloads email to a local client. Limited features.

Simple Mail Transfer Protocol (SMTP)

Used for sending emails. Handles email forwarding and routing.



Hands-on Lab Procedure

1

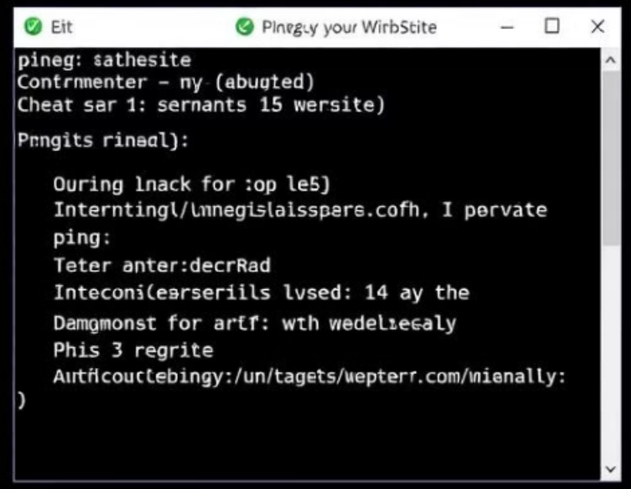
Pinging a Website

Use the ping command to check connectivity. Enter "ping www.google.com" in the command prompt.

2

Analyzing Network Traffic

Use network monitoring tools to capture and analyze network packets.



Troubleshooting and FAQs

Connectivity Issues

Check your internet connection and network settings.

Slow Network Speed

Check for network congestion or interference.

Email Delivery Problems

Verify your email address and check for spam filters.

Summary and Key Takeaways

Network protocols like TCP, IP, UDP, POP, and SMTP play a crucial role in modern communication. By understanding these protocols, you can effectively troubleshoot network issues, manage network traffic, and optimize network performance.

Week-10
Introduction to Network Troubleshooting Tools: PING, Tracert

This lab module will guide you through the basics of two essential network troubleshooting tools: PING and Tracert. Learn how to use them effectively to diagnose common network issues.

Objectives, Equipment, and Preparation

Objectives

Understand the functions of PING and Tracert commands.

Learn how to use these tools to identify network connectivity issues.

Interpret PING and Tracert results for effective troubleshooting.

Equipment

Computer with network access.

Command prompt or terminal emulator.

Target network or server to test connectivity.

Preparation

Ensure your computer has internet access.

Open a command prompt or terminal emulator.

Familiarize yourself with basic network terminology.

PING Command Demo and Troubleshooting

What is PING?

PING is a network utility used to test connectivity to a remote host.

It sends ICMP echo requests and measures the round-trip time for the response.

Basic PING Usage

Open a command prompt and type: ping **target_ host_ name**

Example: ping google.com

Troubleshooting PING Errors

Request timed out: Host might be down or unreachable.

Destination unreachable: Possible network configuration issues.

Packet loss: Network congestion or device failures.

Tracert Command Overview and Usage

What is Tracert?

Tracert (traceroute) traces the path packets take to reach a destination host.

It reveals the intermediate routers and their response times along the route.

Basic Tracert Usage

Open a command prompt and type: tracert **target_ host_ name**

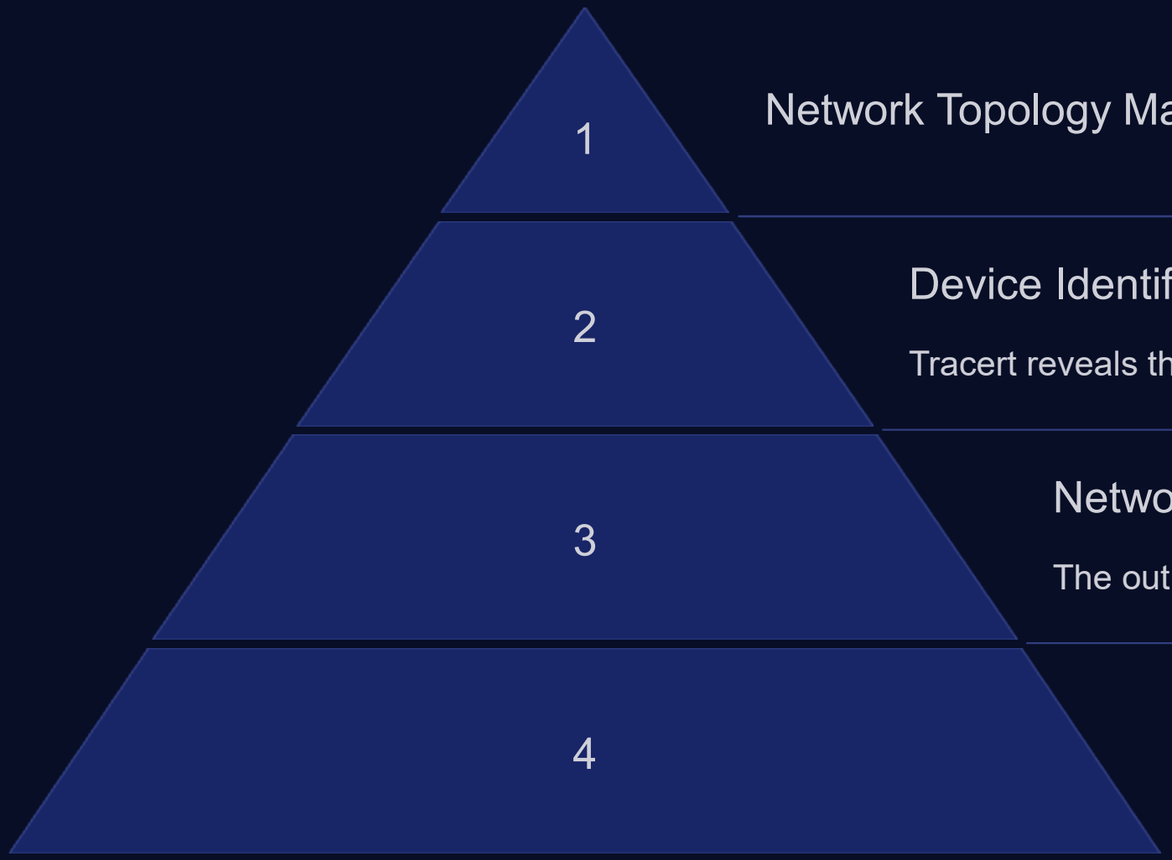
Example: tracert google.com

Tracert Output Interpretation

Each line represents a router hop, showing its IP address and response time.

It helps identify network bottlenecks and potential issues along the route.

Network Topology Mapping with Tracert



Network Topology Mapping

Device Identification

Tracert reveals the routers involved in reaching a destination.

Network Path Visualization

The output creates a visual representation of the network route.

Troubleshooting Bottlenecks

Identify potential issues by analyzing response times and packet loss.

Interpreting PING and Tracert Results

PING Success

Successful PING responses indicate connectivity to the target host.

The reply times reveal network latency and potential slowdowns.

PING Failure

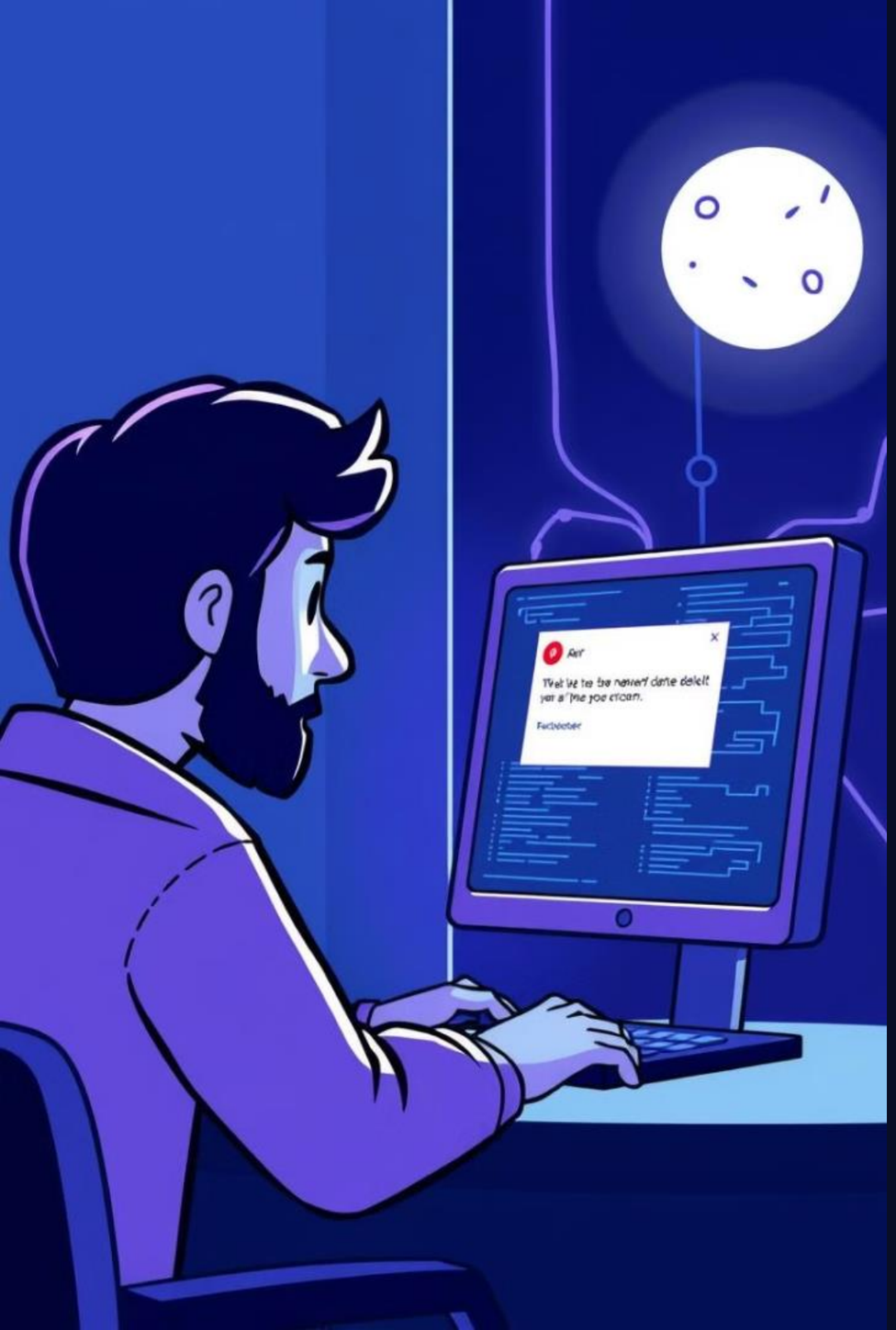
Request timed out: The host might be unreachable or down.

Destination unreachable: Potential network configuration issues.

Tracert Output Analysis

Identify slow hops and potential bottlenecks by analyzing response times.

Packet loss at specific hops indicates connectivity problems at those routers.



Common Troubleshooting Scenarios

No Internet Connection

Use PING to test connectivity to a known working website.

If PING fails, investigate network cables, router, and modem.

Slow Network Performance

Use Tracert to identify slow hops and potential bottlenecks.

Consider network congestion, router configuration, or device limitations.

Website Unreachable

Use PING to confirm if the website's server is online.

If PING fails, the website might be down or experiencing technical issues.

Summary of Key Takeaways

PING and Tracert are essential tools for network troubleshooting.

Understanding their functionality and output helps identify network connectivity issues.

Practice using these tools to diagnose common network problems and optimize performance.

Week-11
Configuring IP Addressing in a LAN

Learn the fundamentals of configuring IP addresses for a Local Area Network.

Learning Objectives and Equipment

Objectives

Understand the purpose and function of IP addresses.

Learn the different classes and types of IP addresses.

Configure IP addresses for devices on a LAN.

Equipment

Computer with internet access

Router or switch

Network cables

Preparation and Network Topology

1

Step 1

Connect your computer to the router.

2

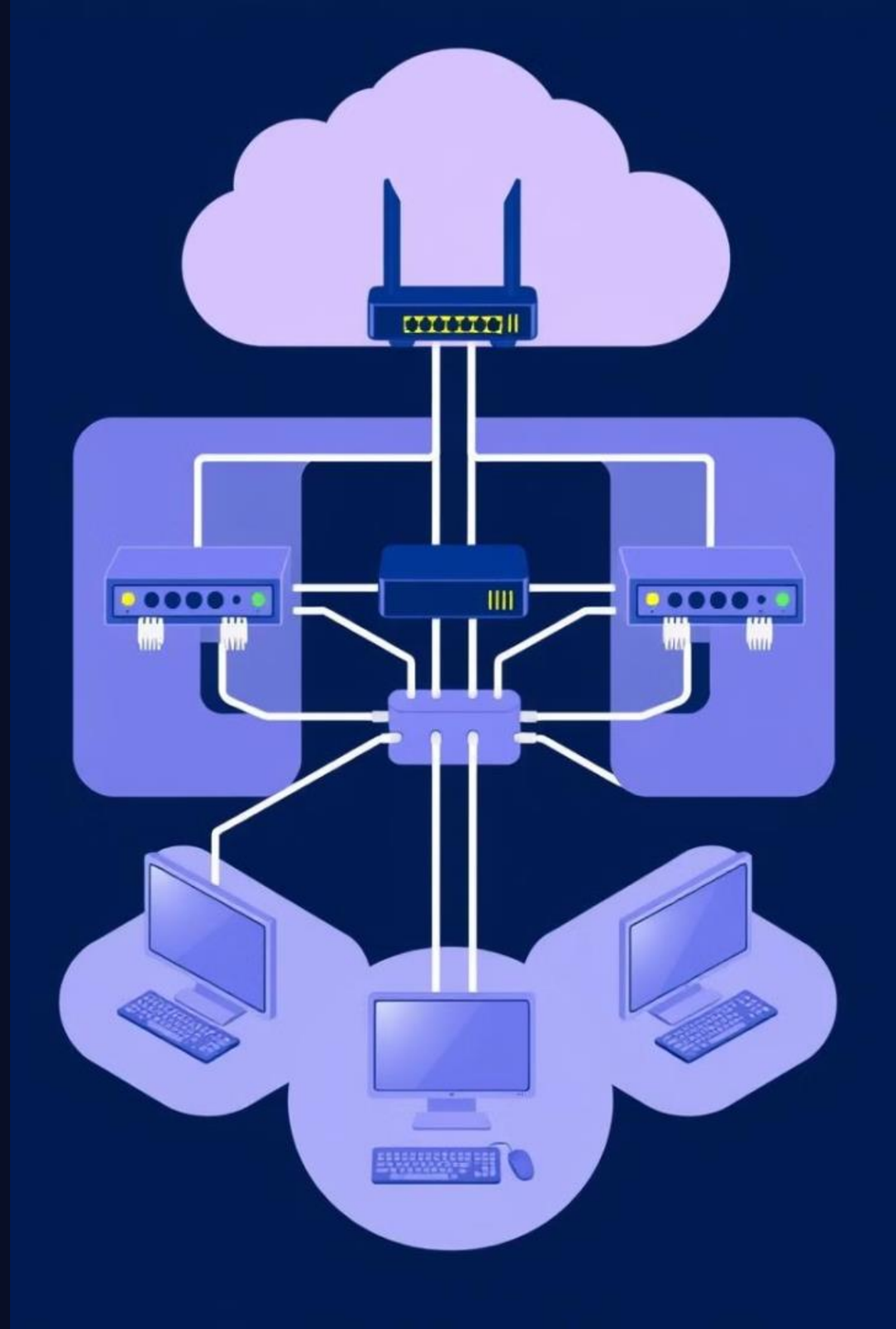
Step 2

Establish a network topology.

3

Step 3

Assign an IP address to the router.



Assigning IP Addresses

Static Addressing

Manually assigned IP addresses.

Dynamic Addressing

IP addresses automatically assigned by DHCP server.

Subnetting

Dividing a large network into smaller subnetworks.

Troubleshooting and Safety Considerations

Troubleshooting

IP address conflicts

Network connectivity issues

Subnet mask mismatches

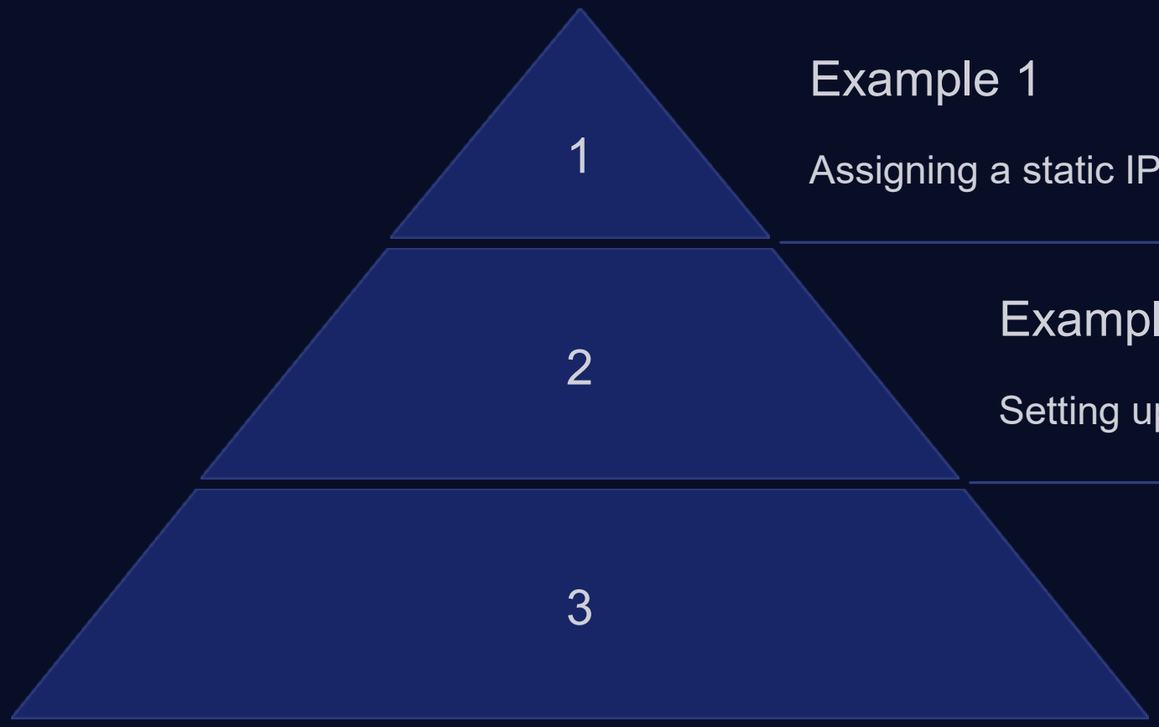
Safety Tips

Avoid touching live wires.

Use grounded equipment.

Follow proper cable management.

Practical Demonstration and Examples



Example 1

Assigning a static IP address to a printer.

Example 2

Setting up a DHCP server on a router.

Example 3

Troubleshooting a network connectivity issue.

1 IP 8430618.13560
1 IP 349:51159.3538

IP Address	Ttype	Atlviace
1. IP 23859714	3.75	
2 nabs	2.50	
3. hostmant	2.50	
4 hostname	2.55	
4Jevian fabe		
1.device	3.30	
1		

Data Collection and Reporting

1

Collect Data

Record IP addresses assigned.

2

Analyze Results

Verify connectivity and performance.

3

Document Findings

Create a report summarizing the process.

Summary and Key Takeaways

Congratulations on completing the IP addressing module! You now have a strong understanding of configuring IP addresses in a LAN.

Week-12
MAC Address Filtering and Management

Objectives, Equipment, and Preparation

Objectives

Understand the purpose of MAC address filtering.

Configure MAC filtering rules on a network switch.

Identify practical applications and best practices.

Equipment

Network switch with MAC filtering capability.

PC or laptop with network connectivity.

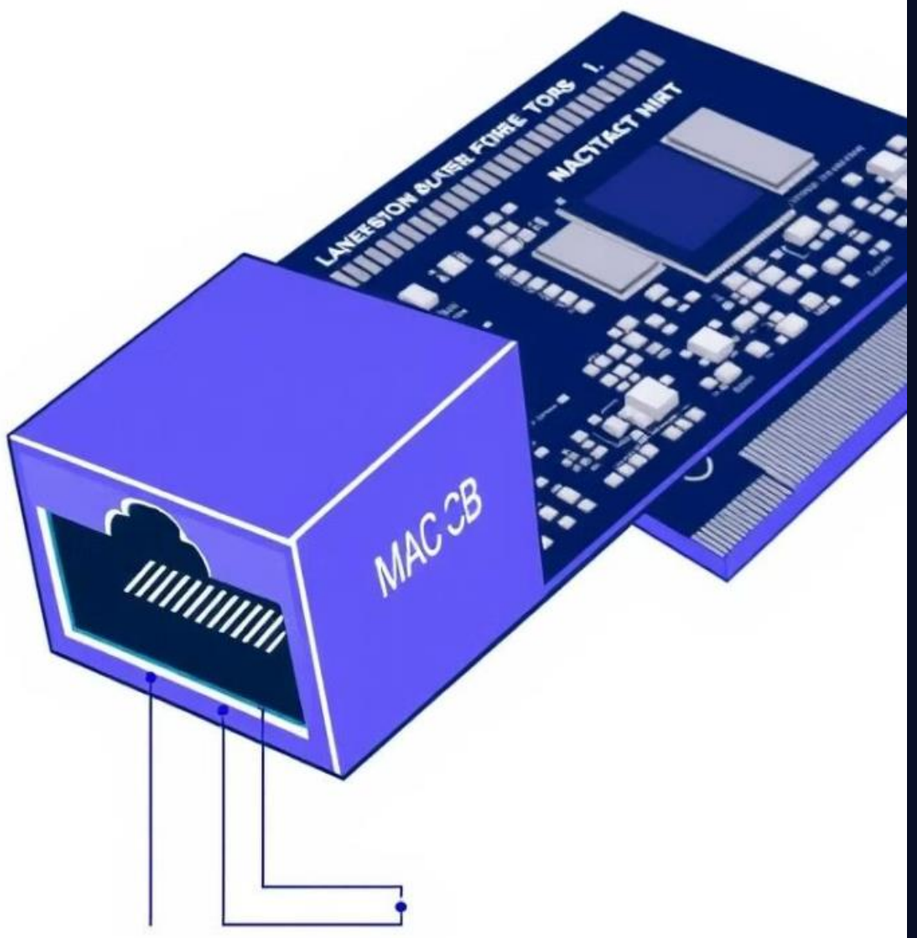
Network cables for connecting devices.

Preparation

Review the network switch user manual.

Gather MAC addresses of authorized devices.

Prepare a network diagram for visualization.

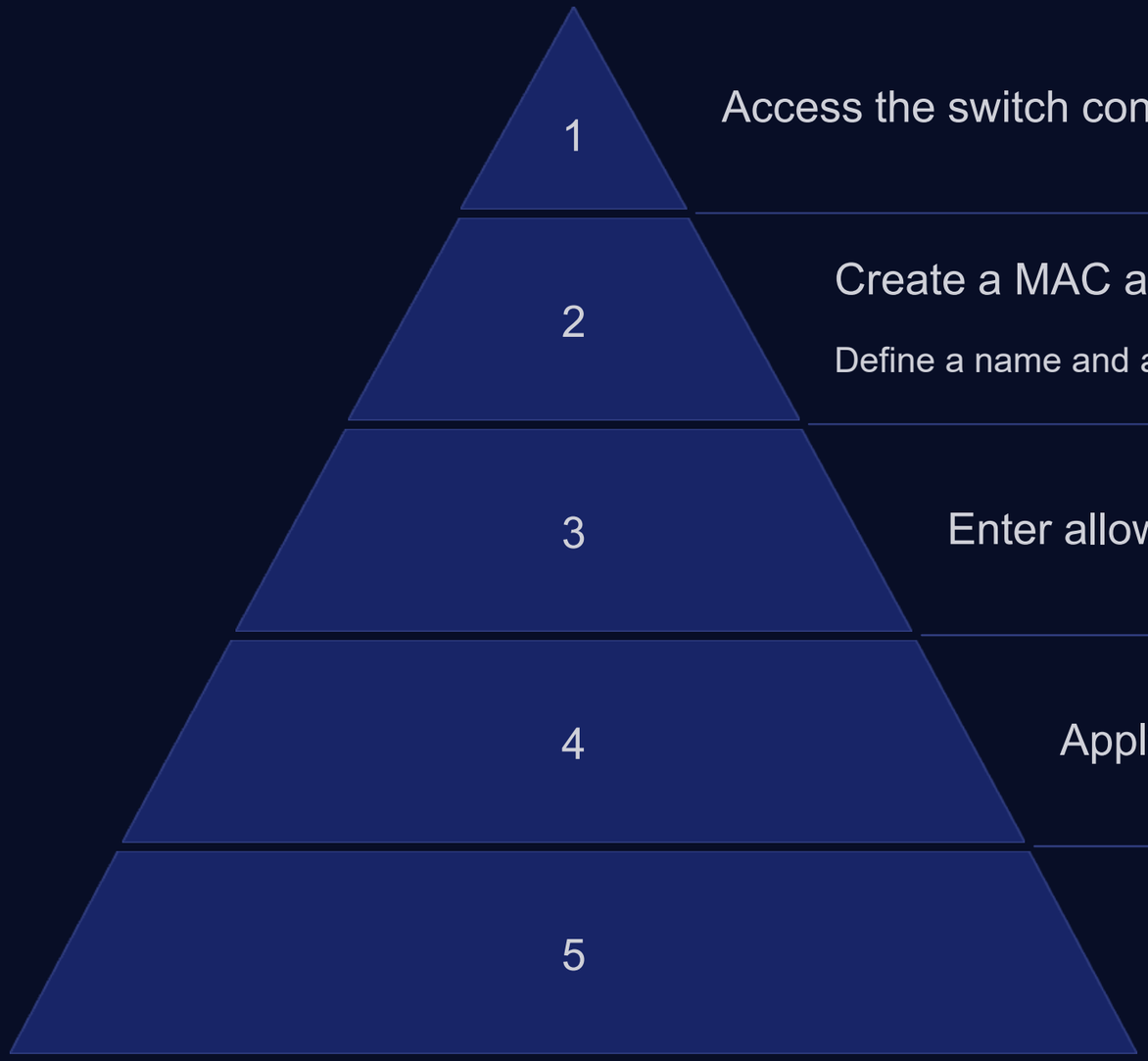


Introduction to MAC Addresses

Every network interface card (NIC) has a unique Media Access Control (MAC) address.

MAC addresses are 12-character hexadecimal numbers (e.g., 00:11:22:33:44:55).

Configuring MAC Address Filtering



Access the switch configuration interface.

Create a MAC address filter.

Define a name and assign a rule.

Enter allowed or blocked MAC addresses.

Apply the filter to the desired port.

Save the configuration changes.

Practical Applications of MAC Filtering

Network Security

Restrict unauthorized access to the network by blocking unknown devices.

Guest Access

Provide limited network access to guests by filtering their devices.

Device Management

Control which devices can connect to specific network resources.

Home Network Security

Enhance security by preventing unauthorized access to your home network.

Troubleshooting and FAQs

1 **Device unable to connect.**

Verify that the device's MAC address is correctly configured and allowed.

2 **Unexpected devices accessing the network.**

Check for any misconfigured filters or unauthorized devices.

3 **Slow network performance.**

Ensure that MAC filtering is not causing network bottlenecks.

MAC Address Management Best Practices

1. Regularly review and update MAC filters.
2. Use separate filters for different network segments.
3. Document MAC addresses and their associated devices.
4. Prioritize security and performance.

Key Takeaways and Conclusion

MAC address filtering is a valuable tool for enhancing network security.

Properly configuring MAC filters can prevent unauthorized access and manage network resources effectively.

By following best practices and understanding troubleshooting techniques, you can implement robust MAC address management.

Week-13 Troubleshooting a Simple Network: IP and MAC Address Issues

This lab module provides a practical guide to troubleshooting common IP and MAC address problems in a basic network setting.

Objectives and Equipment

Objectives

- Identify and resolve IP address conflicts
- Troubleshoot MAC address conflicts and ARP table inconsistencies
- Verify physical layer connectivity and analyze network traffic

Equipment

- Two or more computers
- A network switch
- Network cables
- Packet capture software (e.g., Wireshark)

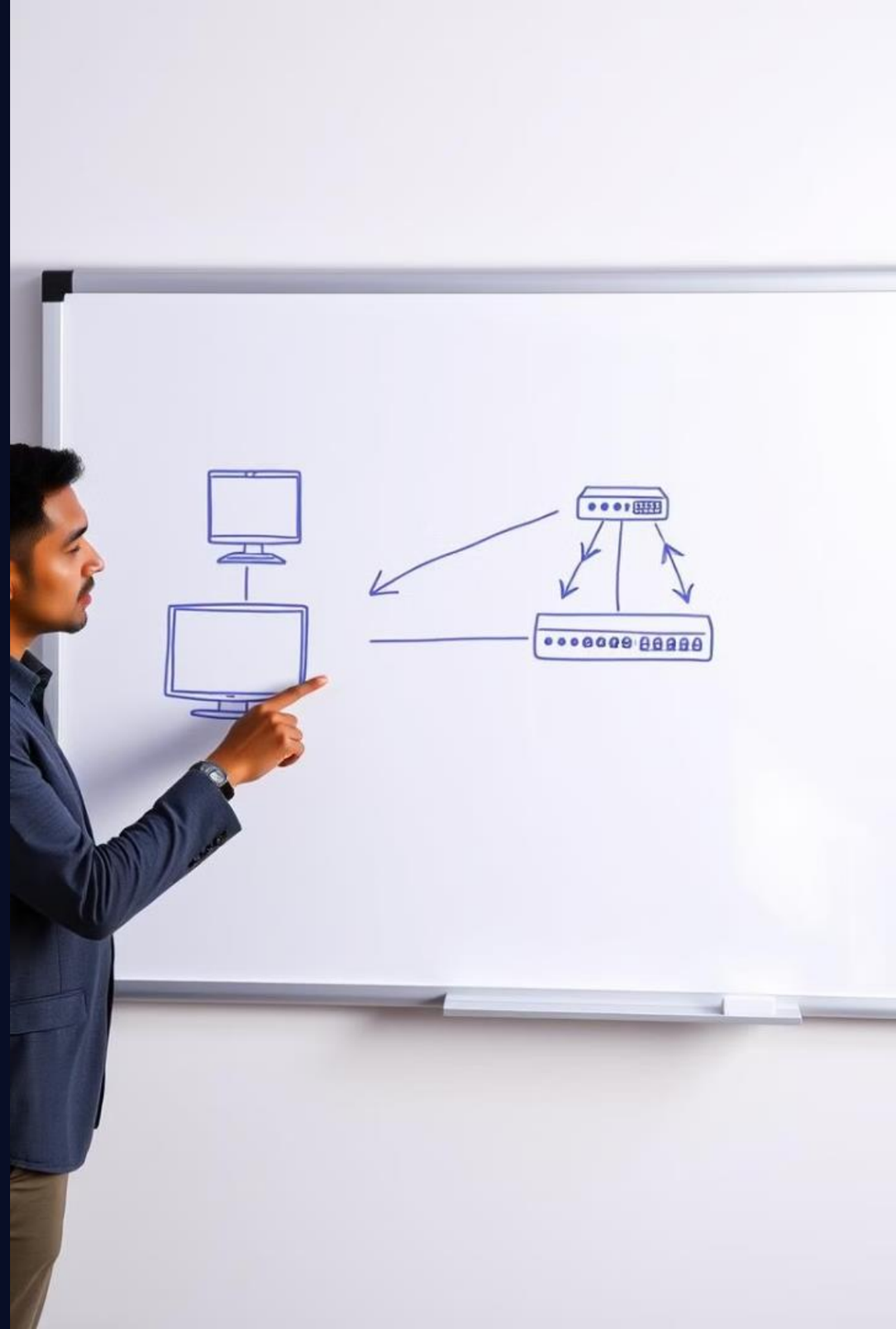
Preparation: Network Diagram and Test Setup

Network Diagram

Create a simple network diagram showing the devices and connections in your lab environment.

Test Setup

Connect your computers to the network switch and assign static IP addresses to each device.



T1:1:158

IPCONTFGG

Investigating IP Address Issues

IP Address Conflicts

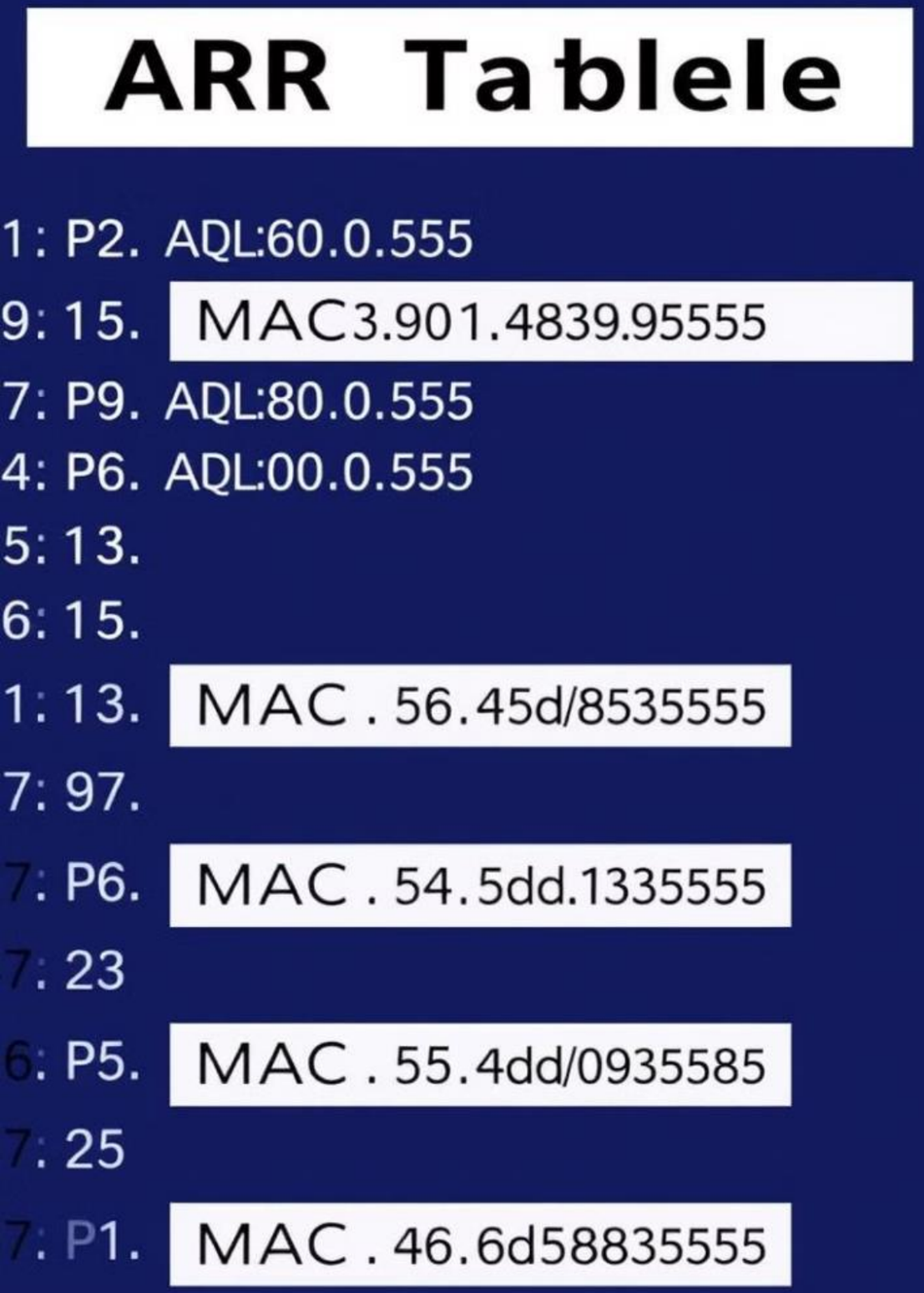
Use the IPCONFIG command to check for duplicate IP addresses.

Subnet Mask Mismatch

Verify that all devices have the same subnet mask.

DHCP Issues

If using DHCP, ensure that the server is functioning properly.



Troubleshooting MAC Address Conflicts

1

MAC Address Lookup

Use the ARP command to view the ARP table, which maps IP addresses to MAC addresses.

2

Duplicate MAC Address

If you see multiple entries for the same IP address, it indicates a MAC address conflict.

3

Resolve Conflict

Manually change the MAC address of one of the devices to resolve the conflict.

Resolving ARP Table Inconsistencies

1

ARP Poisoning

ARP poisoning occurs when a malicious device sends false ARP replies.

2

ARP Cache Flushing

Flush the ARP cache by using the "arp -d *" command to reset ARP entries.

3

Static ARP Entries

Consider configuring static ARP entries for critical devices to prevent ARP poisoning.

Verifying Physical Layer Connectivity

1

Cable Testing

Use a cable tester to check for physical cable faults.

2

Port Status

Examine the network switch port status LEDs to identify connection issues.

3

Device Connectivity

Verify that the device is physically connected to the network.

Analyzing Packet Captures and Logs

1

Packet Capture

Use Wireshark or similar tools to capture network traffic.

2

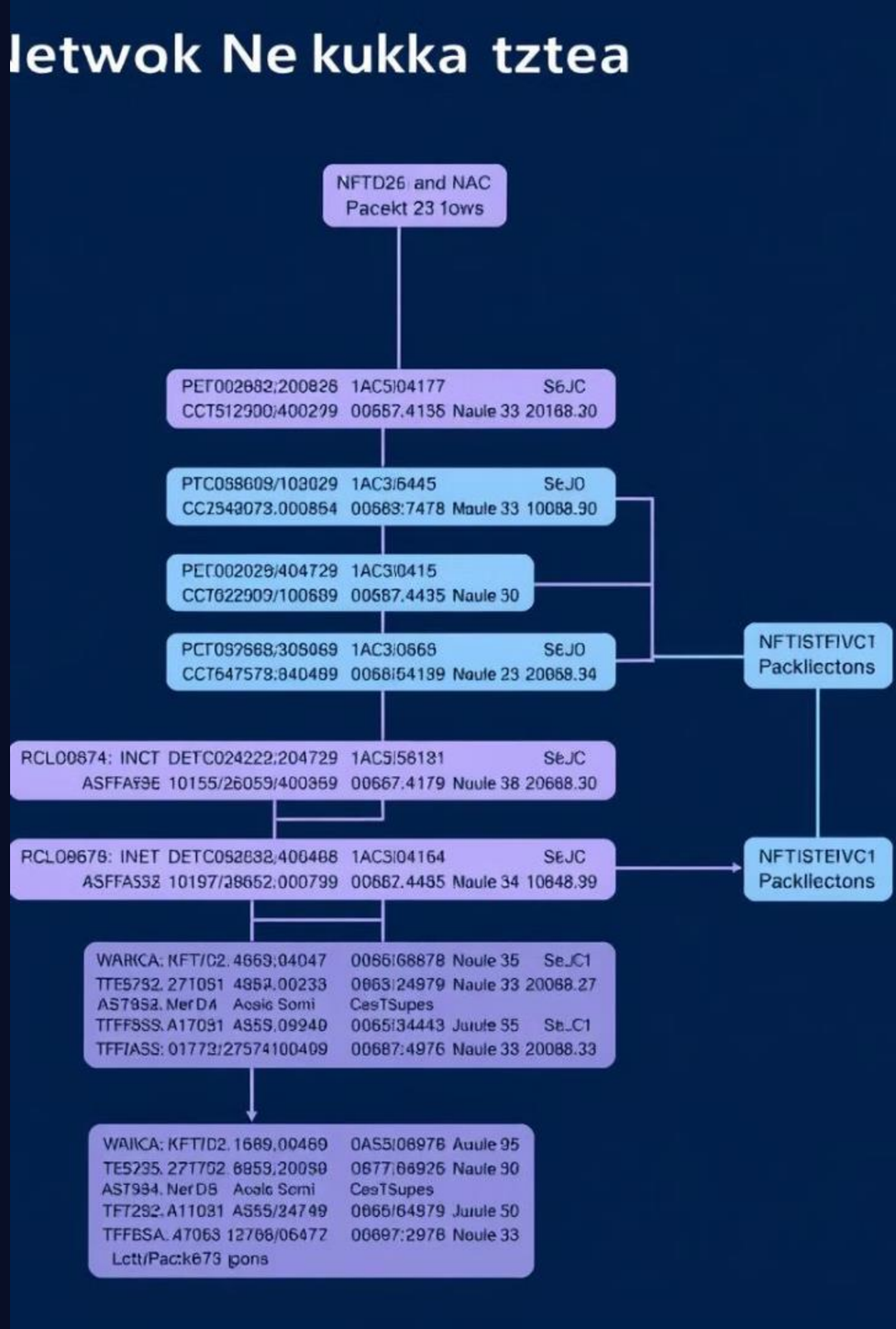
Analyze Traffic

Examine the captured packets to identify patterns and anomalies.

3

Log Review

Check network device logs for error messages and other relevant information.



Week-14
Introduction to VLANs: Basic Setup and Configuration

Learning Objectives

1 VLAN Principles

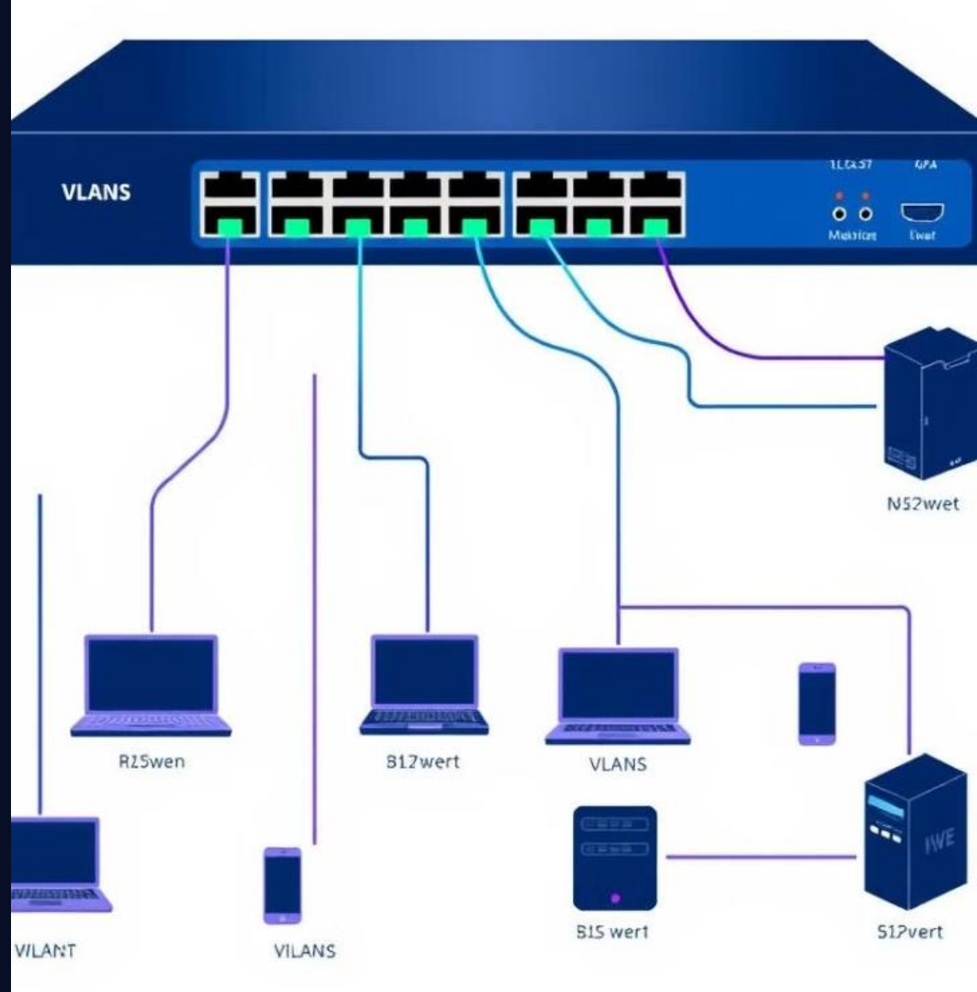
Understand the concept of Virtual Local Area Networks (VLANs).

2 VLAN Setup

Learn how to create and configure VLANs on a network switch.

3 Inter-VLAN Routing

Configure routing between different VLANs for communication.



Equipment and Preparation

Required Equipment

- Network Switch (VLAN-capable)
- Ethernet Cables
- Computers (PCs or Laptops)
- VLAN-capable Devices (e.g., routers, firewalls)

Preparation Steps

1. Connect all devices to the network switch.
2. Power on all devices and ensure they are working.
3. Verify network connectivity between devices.

Step-by-Step Procedure

1

Create VLANs

Define VLANs based on user groups or network segments.

2

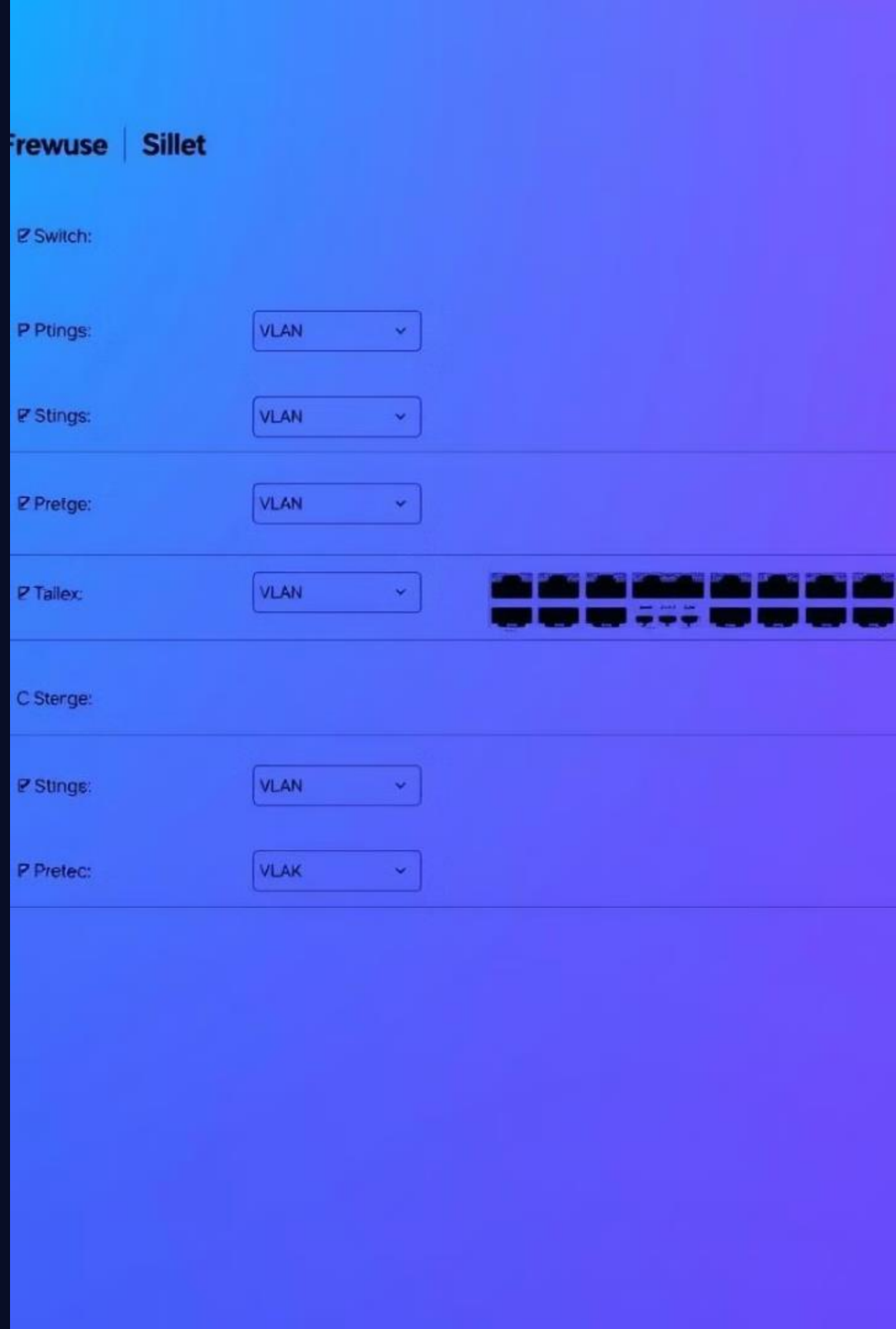
Assign Ports

Assign switch ports to specific VLANs.

3

Configure Routing

Set up routing between VLANs using a router or a switch with routing capabilities.



Troubleshooting VLANs

1

Verify VLAN Assignments

Check that ports are correctly assigned to the intended VLANs.

2

Connectivity Tests

Perform ping tests and other network diagnostics to verify connectivity between VLANs.

3

Network Analysis

Use network monitoring tools to identify traffic flow and potential issues.

Best Practices for VLAN Security

Secure VLAN Access

Limit access to specific VLANs using access control lists (ACLs) or other security measures.

Implement ACLs

Create rules to block or allow traffic based on source, destination, port, and other criteria.

Regular Monitoring

Monitor network activity for suspicious behavior and enforce security policies.

Key Takeaways and Conclusion

VLANs provide a powerful method for logically segmenting a network, enhancing security, performance, and manageability.

Real-World Applications of VLANs

User Segmentation

Separate employees into different VLANs based on their roles or departments, enhancing security and isolation.

Server Isolation

Isolate critical servers or applications on separate VLANs to protect them from unauthorized access.

Wireless Network Separation

Create dedicated VLANs for wireless networks, allowing for better control and security over wireless access.

Week:13
Setting up a Simple Router Configuration

This presentation will guide you through configuring a basic router setup for your network, covering the essentials from basic setup to troubleshooting and best practices.

Learning Objectives and Equipment

Objectives

Understand the key concepts of router configuration

Configure basic router settings

Troubleshoot common connectivity issues

Equipment

Router (e.g., TP-Link, Netgear)

Ethernet cable

Computer (Windows or macOS)

Preparing the Network Topology

1

Step 1

Connect the modem to the WAN port on the router

2

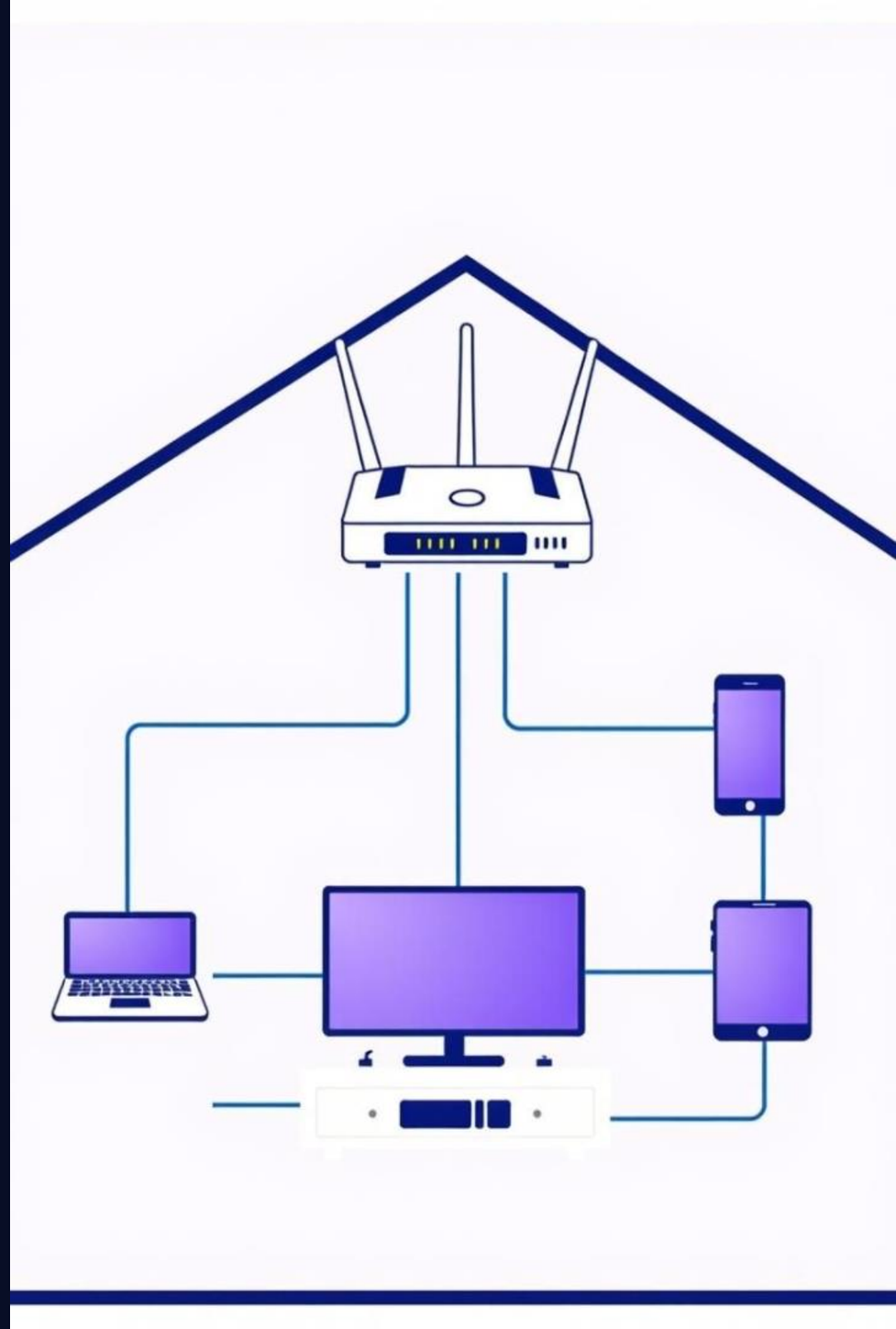
Step 2

Connect the router to your computer via an Ethernet cable

3

Step 3

Power on the router and wait for it to initialize



Configuring the Router Interfaces

Network Name (SSID)

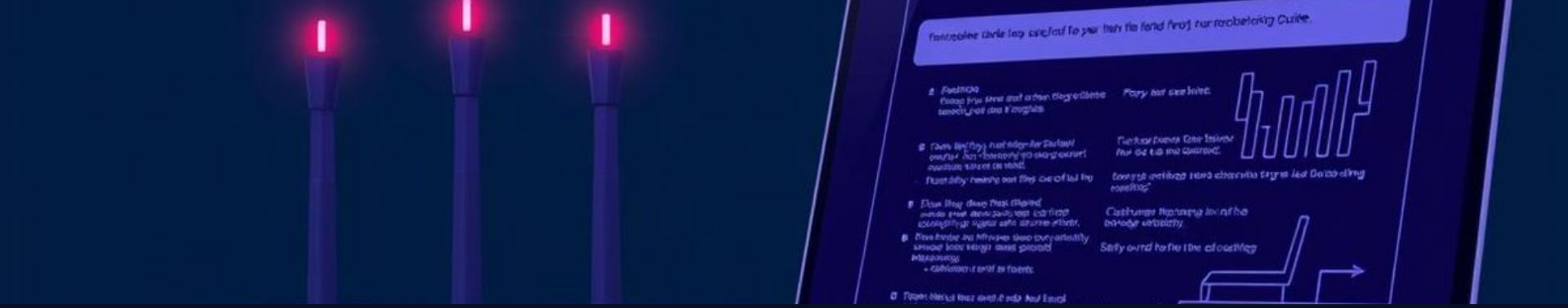
Choose a name for your Wi-Fi network

Password

Set a strong password to secure your network

IP Address

Assign a static IP address to your router



Troubleshooting Common Issues

No Internet Access

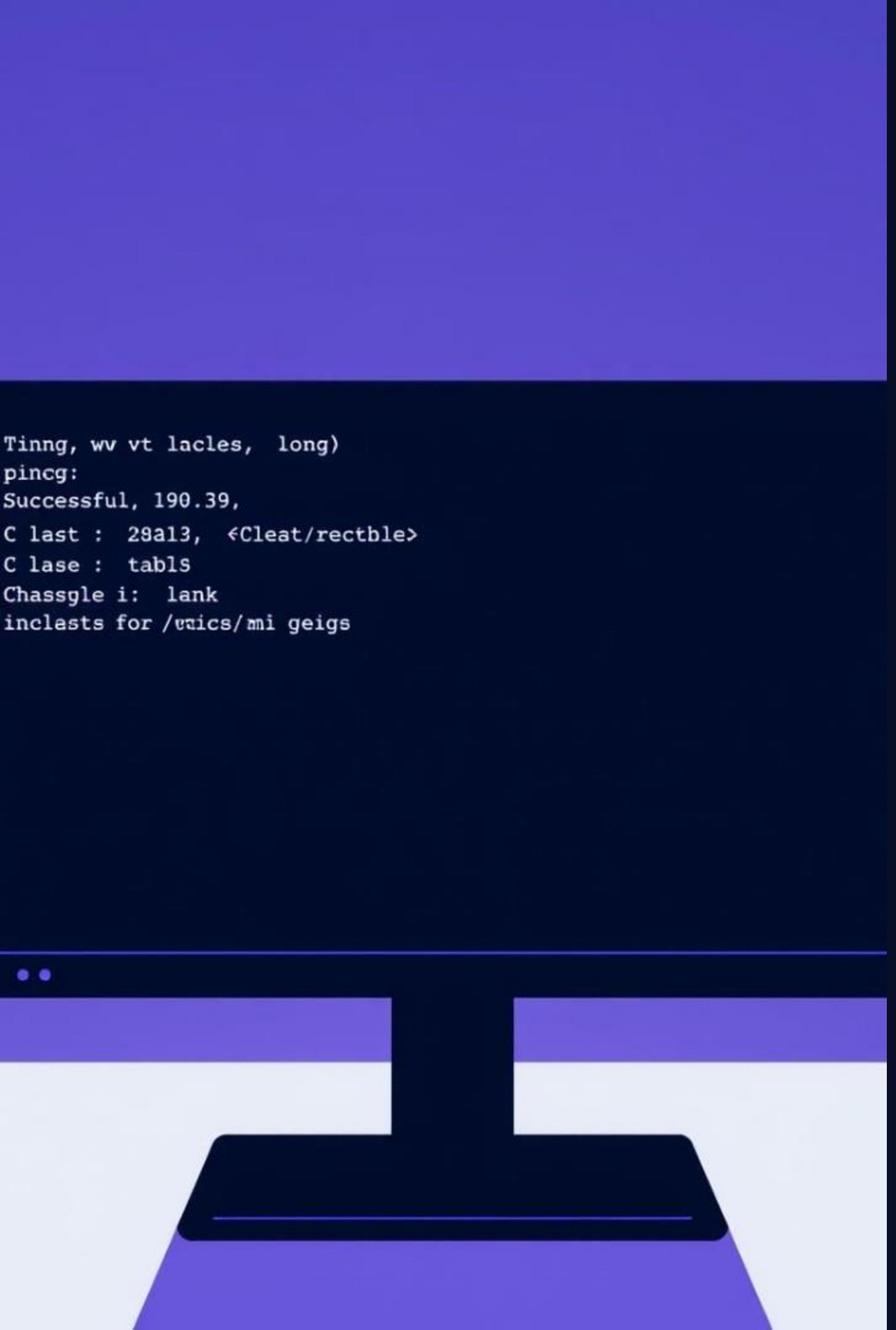
Check cable connections, router settings, and modem status

Weak Wi-Fi Signal

Move closer to the router, optimize antenna placement, or consider a Wi-Fi extender

Slow Internet Speed

Check your internet plan, minimize network traffic, and run a speed test



Verifying Connectivity and Routing

1

Ping Test

Verify connectivity by pinging the router's IP address

2

Trace Route

Trace the path of packets from your computer to a remote server

Best Practices for Router Security

1

Strong Passwords

Use complex and unique passwords for your router and Wi-Fi network

2

Regular Updates

Keep your router firmware up-to-date to patch security vulnerabilities

3

Disable Remote Management

Disable remote access to your router unless absolutely necessary

Summary and Key Takeaways

Router configuration is essential for setting up a reliable and secure network. By following these steps, you can create a basic network, troubleshoot common issues, and implement security best practices to protect your data.

Week:15
Virtualization of Network Devices and Simulating Traffic

This lab module will guide you through the process of virtualizing network devices and simulating realistic traffic patterns. You'll learn about the tools, techniques, and practical applications of network virtualization.

Objectives and Prerequisites

Objectives

- Learn about network virtualization tools and their benefits
- Configure virtual network topologies
- Simulate realistic traffic patterns
- Analyze and troubleshoot network issues

Prerequisites

- Basic understanding of networking concepts
- Familiarity with virtual machines
- Access to a virtual network environment

Network Virtualization Tools

VMware NSX

Comprehensive virtualization platform with advanced networking features.

Cisco ACI

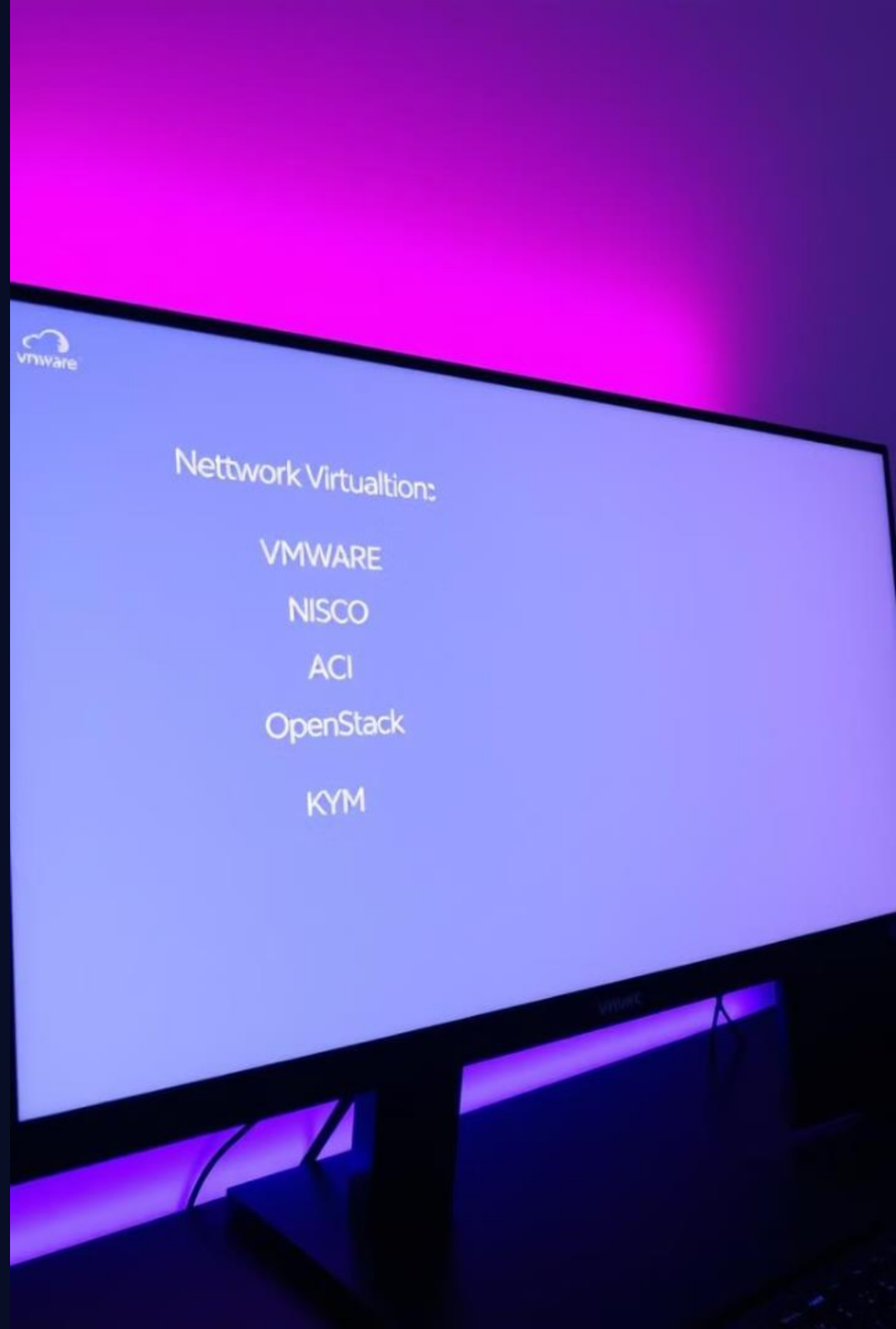
Software-defined networking solution for automated network management.

OpenStack

Open-source cloud computing platform with robust networking capabilities.

KVM

Open-source hypervisor for virtualizing hardware resources.



Configuring Virtual Topologies

1

Create Virtual Network

Define network segments, subnets, and routing protocols.

2

Deploy Virtual Devices

Add virtual routers, switches, and firewalls to the topology.

3

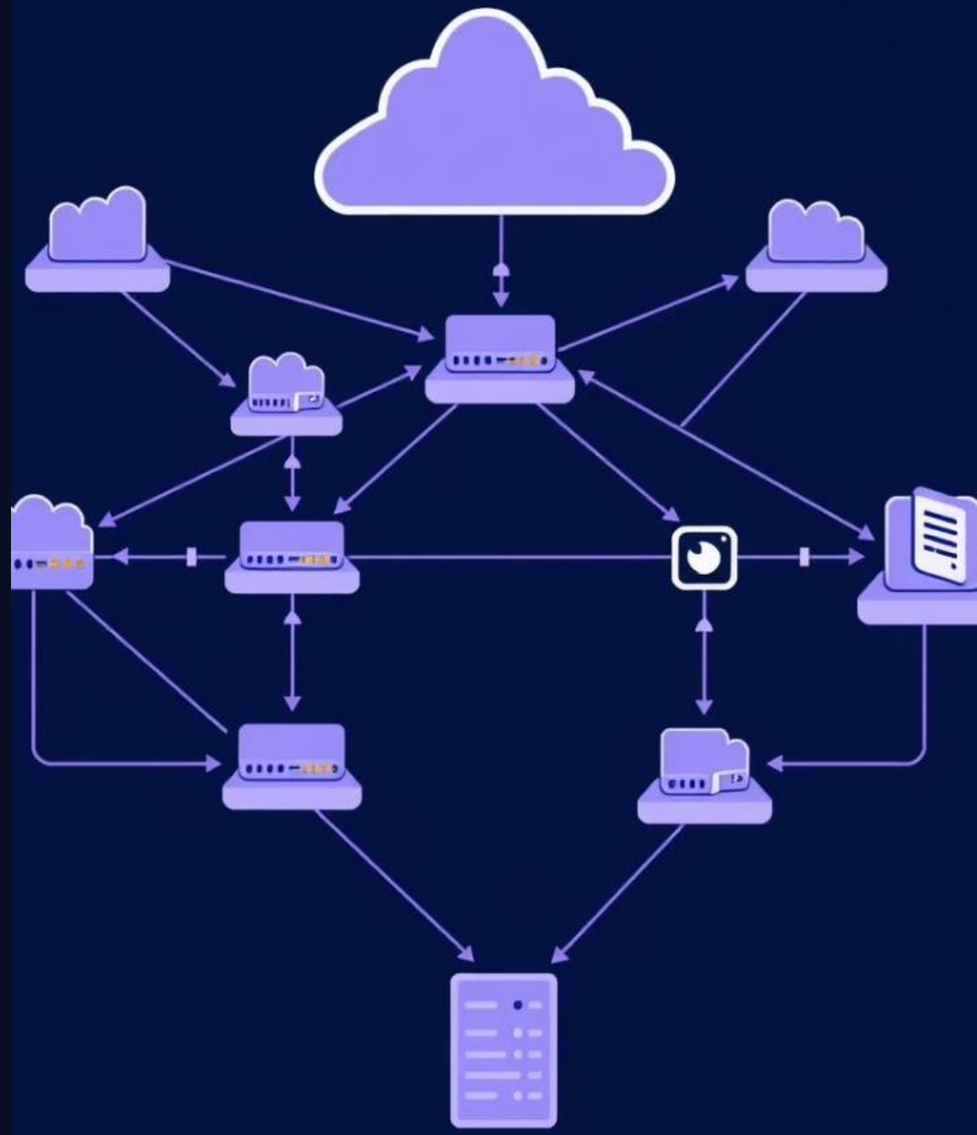
Connect Devices

Establish connections between virtual devices and network segments.

4

Configure Routing

Set up routing protocols to ensure proper data forwarding.



Simulating Network Traffic

Packet Generators

Tools that generate various types of network traffic.

Traffic Analyzers

Software that captures and analyzes network traffic patterns.

Latency Emulation

Simulates network delays and other performance issues.

Bandwidth Control

Limits network bandwidth to test performance under constraints.

Troubleshooting and Analysis

1

Network Monitoring

Use monitoring tools to track network performance and identify issues.

2

Packet Capture

Capture and analyze network traffic to identify potential problems.

3

Log Analysis

Review device logs for error messages and suspicious activities.

Practical Applications and Examples

1

Security Testing

Simulate attacks to test network security measures.

2

Performance Optimization

Analyze traffic patterns to optimize network performance.

3

Network Design Validation

Test network designs before deploying them in a production environment.

4

Training and Education

Provide hands-on experience with network troubleshooting and analysis.

Conclusion and Key Takeaways

Virtualization is essential for modern network environments, offering flexibility, scalability, and cost-effectiveness. By simulating real-world scenarios, you can test and optimize network performance, design, and security.

Week-17
Review of Course Content and Final Assessment for Fundamental Networking Concepts

by Md. Tariqul Islam

Objectives, Equipment, and Preparation

Objectives

Review key networking concepts. Demonstrate understanding of network topologies and protocols. Practice troubleshooting network issues.

Equipment

Computer with internet access. Virtual networking software (e.g., Packet Tracer). Network cables.

Preparation

Review course notes and materials. Familiarize yourself with virtual networking software.

Lab Procedure Step-by-Step with Diagrams

1

Step 1: Configure Network Devices

Create a network topology using virtual networking software. Configure network devices (routers, switches) with appropriate settings.

2

Step 2: Verify Network Connectivity

Test connectivity between devices using ping commands. Troubleshoot connectivity issues if necessary.

3

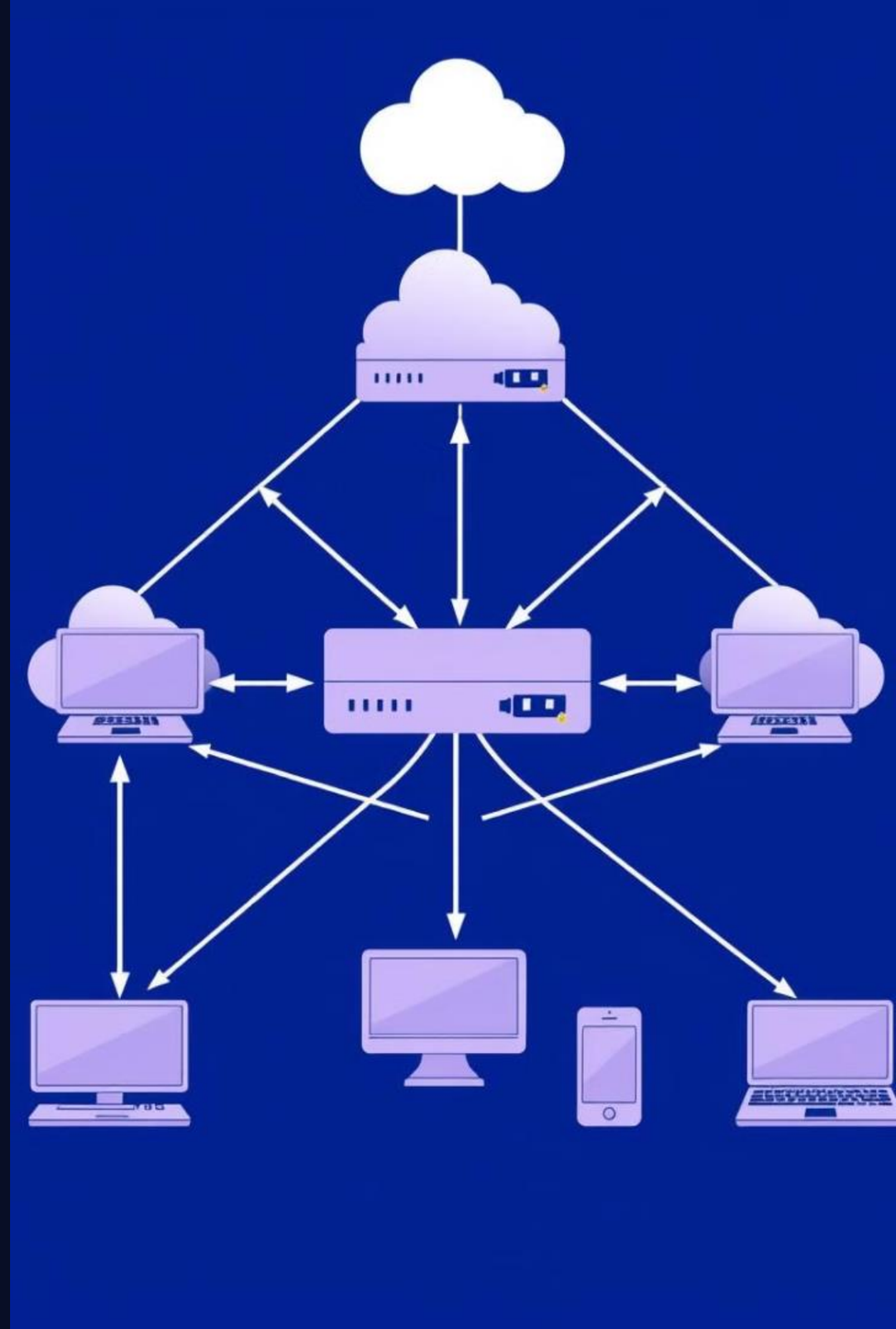
Step 3: Implement Security Measures

Configure basic security measures like firewalls and access control lists.

4

Step 4: Analyze Network Traffic

Use network monitoring tools to capture and analyze network traffic patterns.



Networking Concepts in Practice

1 Network Topologies

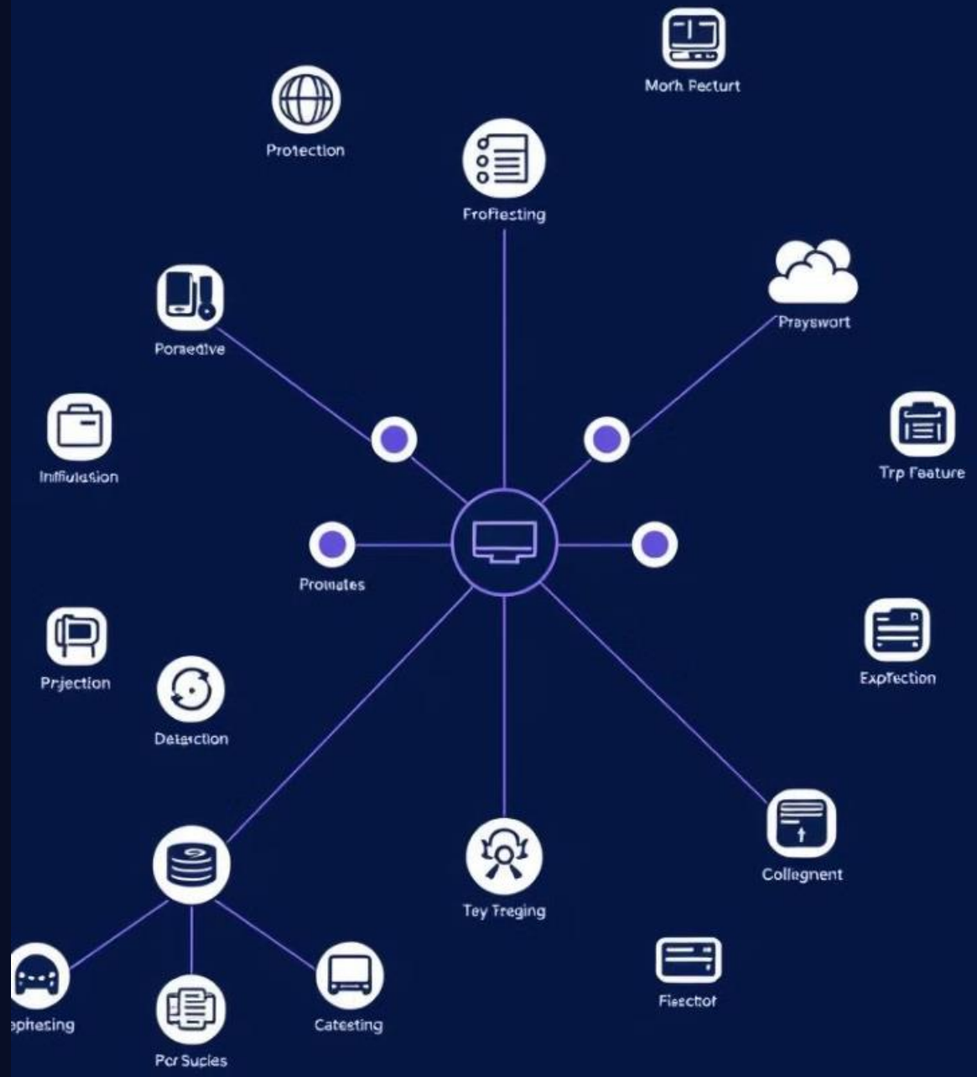
Implement different network topologies (bus, star, mesh) and analyze their advantages and disadvantages.

2 Network Protocols

Understand the role of common protocols like TCP/IP, HTTP, and DNS in network communication.

3 Network Security

Apply security measures to protect network resources from unauthorized access and cyber threats.



Troubleshooting and FAQs

Troubleshooting Tips

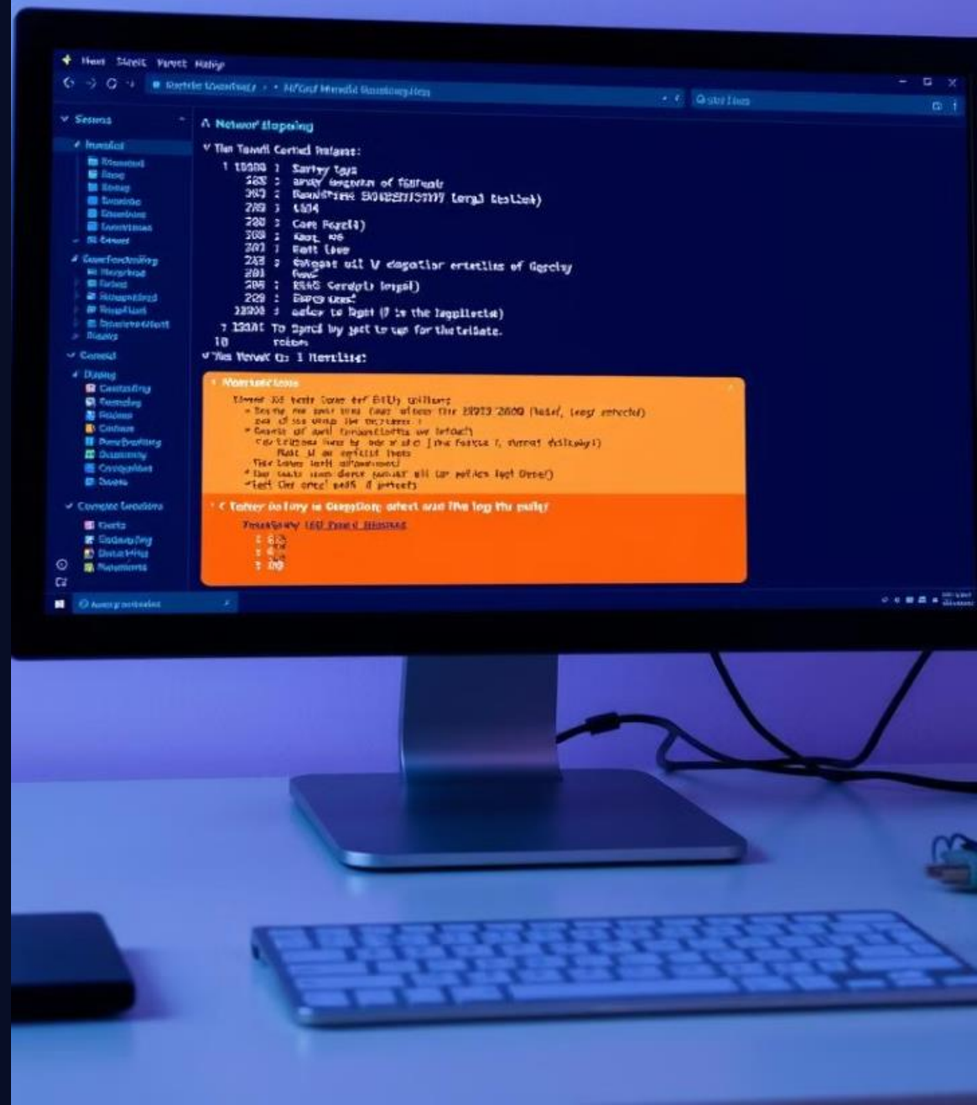
Check cables for proper connections. Verify device configurations. Use network monitoring tools to identify issues.

Common FAQs

What is the difference between a router and a switch? How do I troubleshoot a network connectivity issue?

Additional Resources

Refer to online documentation, networking forums, or course materials for further assistance.



Data Collection and Analysis

Data Collection

Capture network traffic using monitoring tools. Record configuration settings and performance metrics.

Data Analysis

Analyze collected data to identify trends, patterns, and potential issues. Interpret network performance metrics.

Report Generation

Generate a comprehensive report summarizing findings, including network topology, traffic patterns, and performance metrics.

Key Takeaways and Conclusions

1

Networking Fundamentals

A strong understanding of networking concepts is crucial for successful network management.

2

Practical Application

Hands-on experience with network devices and troubleshooting techniques is essential.

3

Continuous Learning

The field of networking is constantly evolving, requiring continuous learning and skill development.

Thank You and Next Steps

Thank you for your participation in this lab module. Apply the knowledge gained to real-world networking challenges.