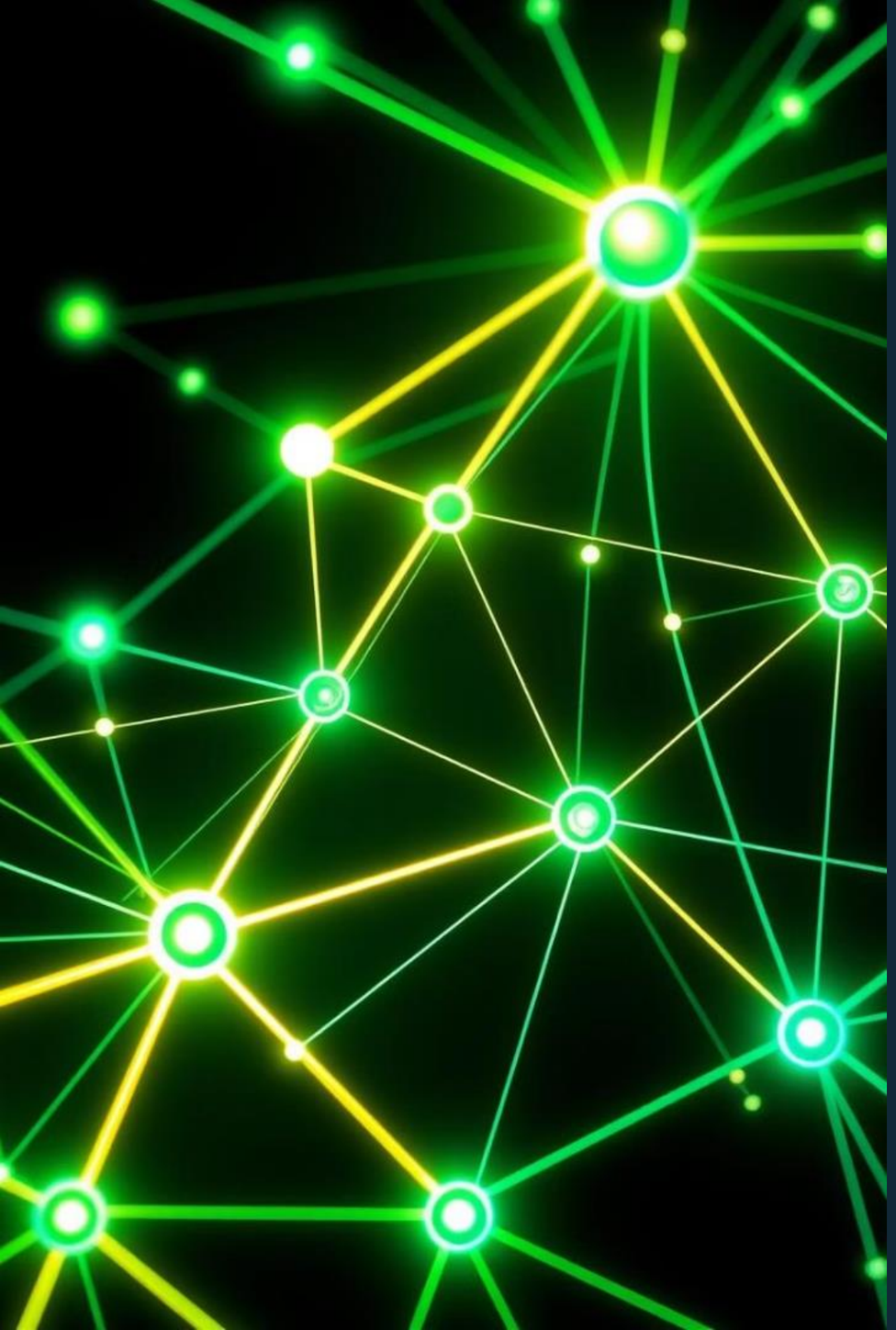


Level 2: Intermediate Network Configuration

This presentation outlines the curriculum for the Intermediate Network Configuration course, covering key topics, learning outcomes, and assessment methods.

CONTENT OF THE SESSIONAL COURSE

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

Course Overview

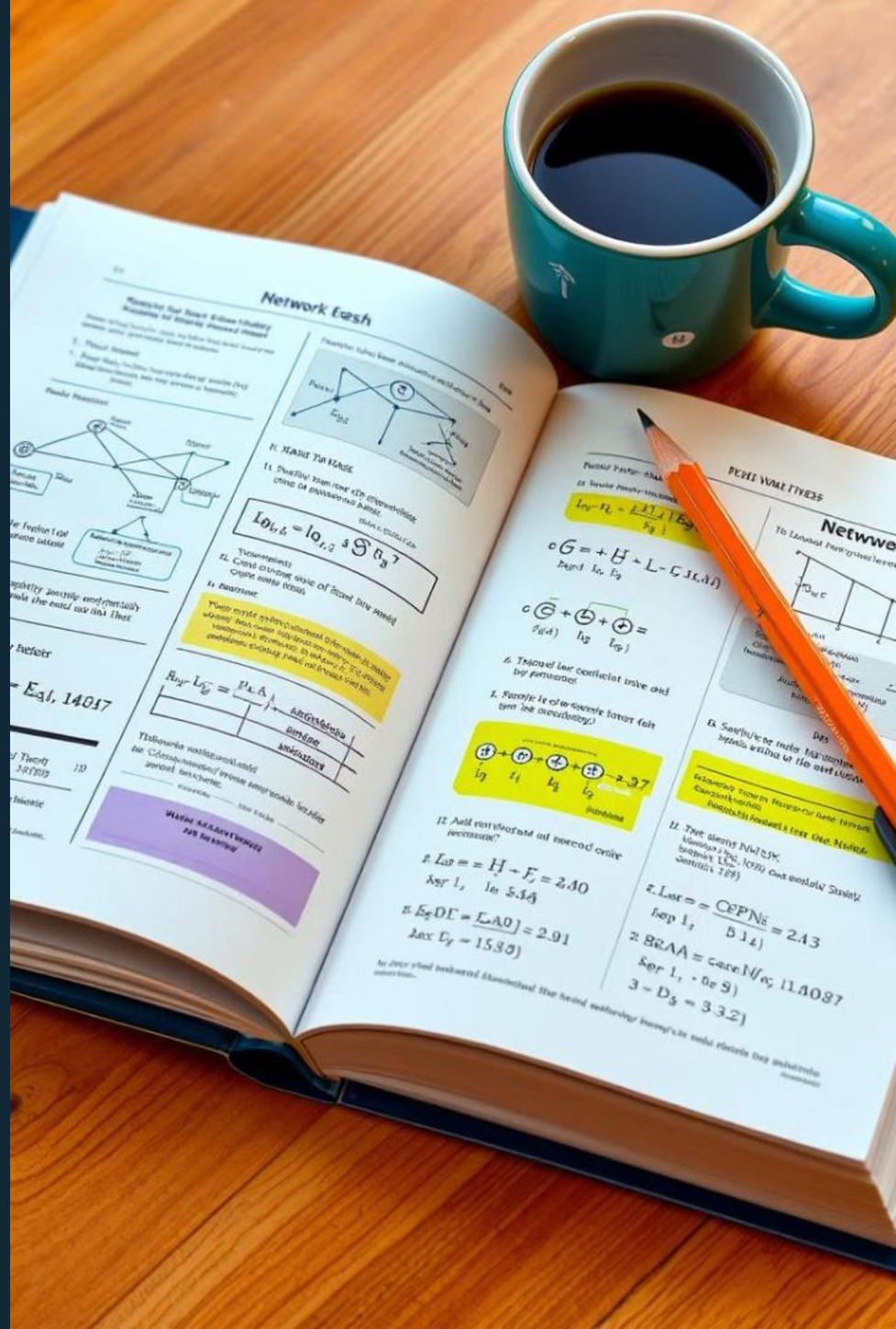
Course Code	Credits	Exam Hours	CIE Marks
Level:02	01	01	30

Learning Outcomes

CLO1	Demonstrate understanding of fundamental networking concepts, including network types, devices, and topologies.	Level 1
CLO2	Apply networking protocols, IP addressing (IPv4/IPv6), subnetting, and configure LAN, MAN, and WAN networks.	Level 1 & 2
CLO3	Design and implement secure and scalable enterprise-level networks using VLANs, VPNs, routing protocols, and NAS.	Level 2 & 3
CLO4	Troubleshoot and resolve network issues using diagnostic tools, network monitoring tools, and OSI model layers.	Level 3
CLO5	Integrate emerging technologies (SDN, IoT, Cloud Networking) and advanced network security practices into systems.	Level 4

Course Content

Serial No.	SUMMARY OF COURSE CONTENT	Hours	CLOs
1	IPv4 Addressing, Subnetting, and Supernetting	6	CLO2
2	Introduction to IPv6 Addressing and Configuration	6	CLO2
3	Configuring Network Devices (Switches, Routers, VLANs)	9	CLO2, CLO3
4	Network Protocols: TCP, UDP, IP, POP, SMTP	6	CLO2
5	Configuring Broadcast and Collision Domains	6	CLO2
6	Basics of Virtual Private Networks (VPNs)	6	CLO3
7	Network Troubleshooting using Diagnostic Tools	7	CLO4
8	Intermediate LAN and WAN Setup	6	CLO2

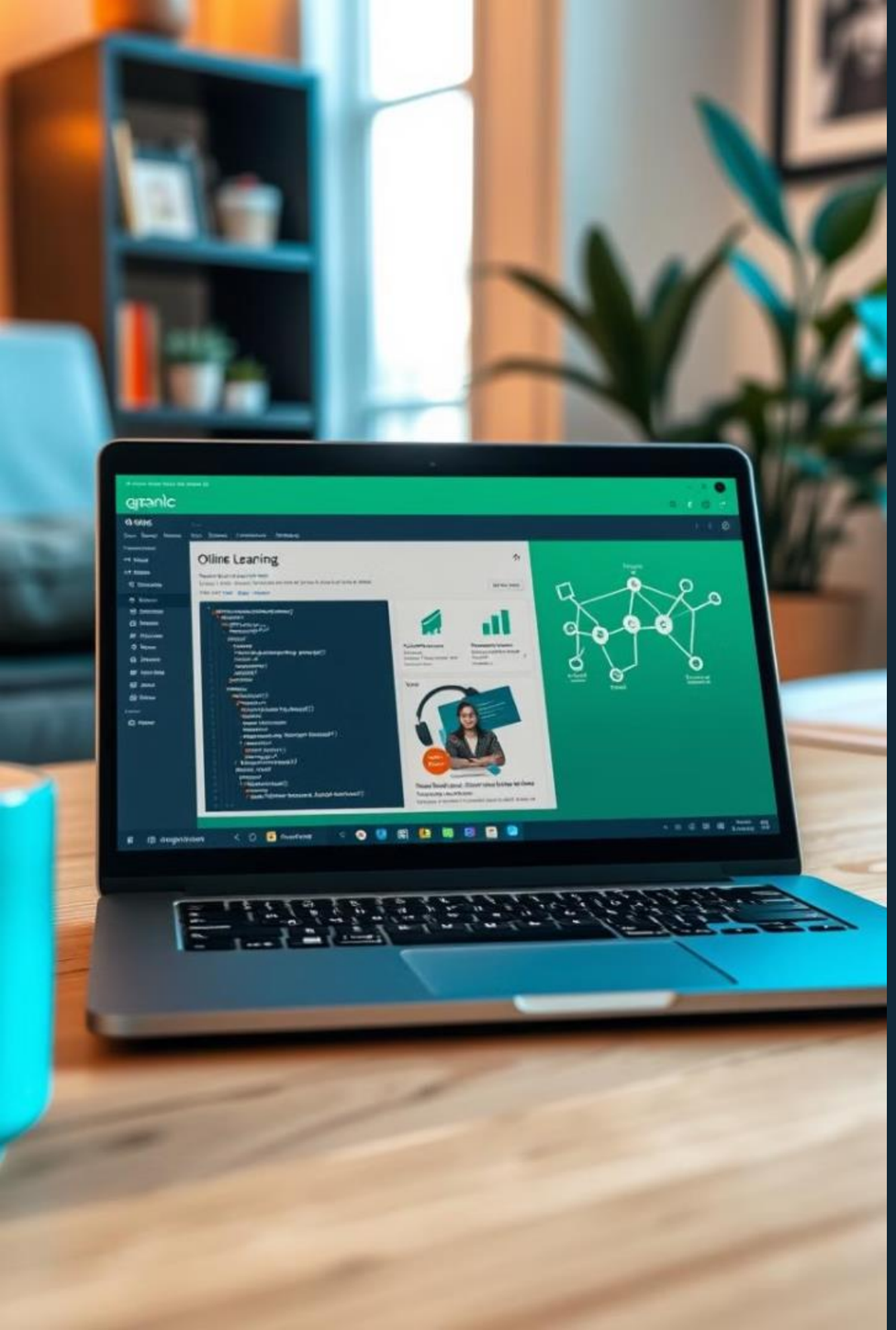


Course Plan

Week No.	Topics	Teaching-Learning Strategy(s)	Class Hour	Practice Hour	Assessment Strategy(s)	Alignment to CLO
1	Advanced IP Addressing: Subnetting in Detail	Lecture, Hands-on Lab	5h	5h	Lab Assignment, Quiz	CLO1
2	Introduction to Routing Protocols: RIP, OSPF, BGP	Lecture, Demonstration, Group Work	5h	5h	Quiz, Lab Report	CLO2
3	IPv6 Addressing and Configuration	Hands-on Lab, Problem Solving	5h	5h	Lab Assignment, Quiz	CLO2
4	Setting up Static and Dynamic Routing	Hands-on Lab, Group Work	5h	5h	Lab Assignment, Quiz	CLO3
5	DHCP Setup and Configuration	Hands-on Lab, Group Work	5h	5h	Lab Report, Quiz	CLO3
6	Configuring and Troubleshooting NAT	Hands-on Lab, Problem Solving	5h	5h	Lab Assignment, Quiz	CLO4
7	Introduction to VPNs and Configuring a Site-to-Site VPN	Hands-on Lab, Demonstration	5h	5h	Lab Report, Practical Test	CLO4
8	MAC Address Table and VLAN Tagging in Network Devices	Hands-on Lab, Group Work	5h	5h	Lab Report, Quiz	CLO4
9	Access Control Lists (ACLs) Configuration	Hands-on Lab, Problem Solving	5h	5h	Quiz, Lab Assignment	CLO3
10	Network Performance and Troubleshooting: Packet Sniffing with Wireshark	Hands-on Lab, Group Work	5h	5h	Lab Report, Practical Test	CLO5

Course Plan

Week No.	Topics	Teaching-Learning Strategy(s)	Class Hour	Practice Hour	Assessment Strategy(s)	Alignment to CLO
11	Network Monitoring Tools: SNMP, Syslog	Hands-on Lab, Demonstration	5h	5h	Lab Report, Quiz	CLO5
12	QoS Configuration and Traffic Management	Hands-on Lab, Problem Solving	5h	5h	Quiz, Lab Report	CLO5
13	Advanced Routing with OSPF and BGP	Hands-on Lab, Group Work	5h	5h	Lab Assignment, Quiz	CLO2
14	Load Balancing and Redundancy in Networking	Lecture, Hands-on Lab	5h	5h	Lab Report, Quiz	CLO5
15	High Availability Networks and Clustering	Hands-on Lab, Group Work	5h	5h	Practical Test, Lab Report	CLO4
16	Enterprise-Level Network Design	Lecture, Problem Solving, Case Studies	5h	5h	Final Project, Quiz	CLO5
17	Review of Intermediate Networking Topics	Group Discussion, Q&A Session	5h	5h	Final Exam, Project Submission	CLO5



Recommended Resources

Textbooks

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

2. "Computer Networks" by Andrew S. Tanenbaum

3. "Network Security Essentials" by William Stallings

Online Resources

1. Udemy: https://www.udemy.com/topic/network-security/

2. TutorialsPoint: https://www.tutorialspoint.com/network_ security/index.htm

3. YouTube: NetworkChuck, Professor Messer

Assessment Pattern

1. **Continuous In-course Evaluation (CIE)**

   30 marks

2. **Lab Participation**

   10 marks

3. **Assignments**

   10 marks

4. **Quizzes**

   10 marks

5. **Final Project Evaluation**

   20 marks

Key Takeaways

This course provides a comprehensive understanding of intermediate network configuration, equipping students with the skills to design, implement, and troubleshoot secure and scalable networks.

The course emphasizes hands-on learning through labs, assignments, and a final project, fostering practical skills and knowledge.

Week-01 Advanced IP Addressing: Subnetting in Detail

This presentation will dive into the world of subnetting, providing you with a deep understanding of this essential networking concept.

by Md. Tariqul Islam

Learning Objectives

Understanding Subnetting

Define subnetting and its purpose within network design.

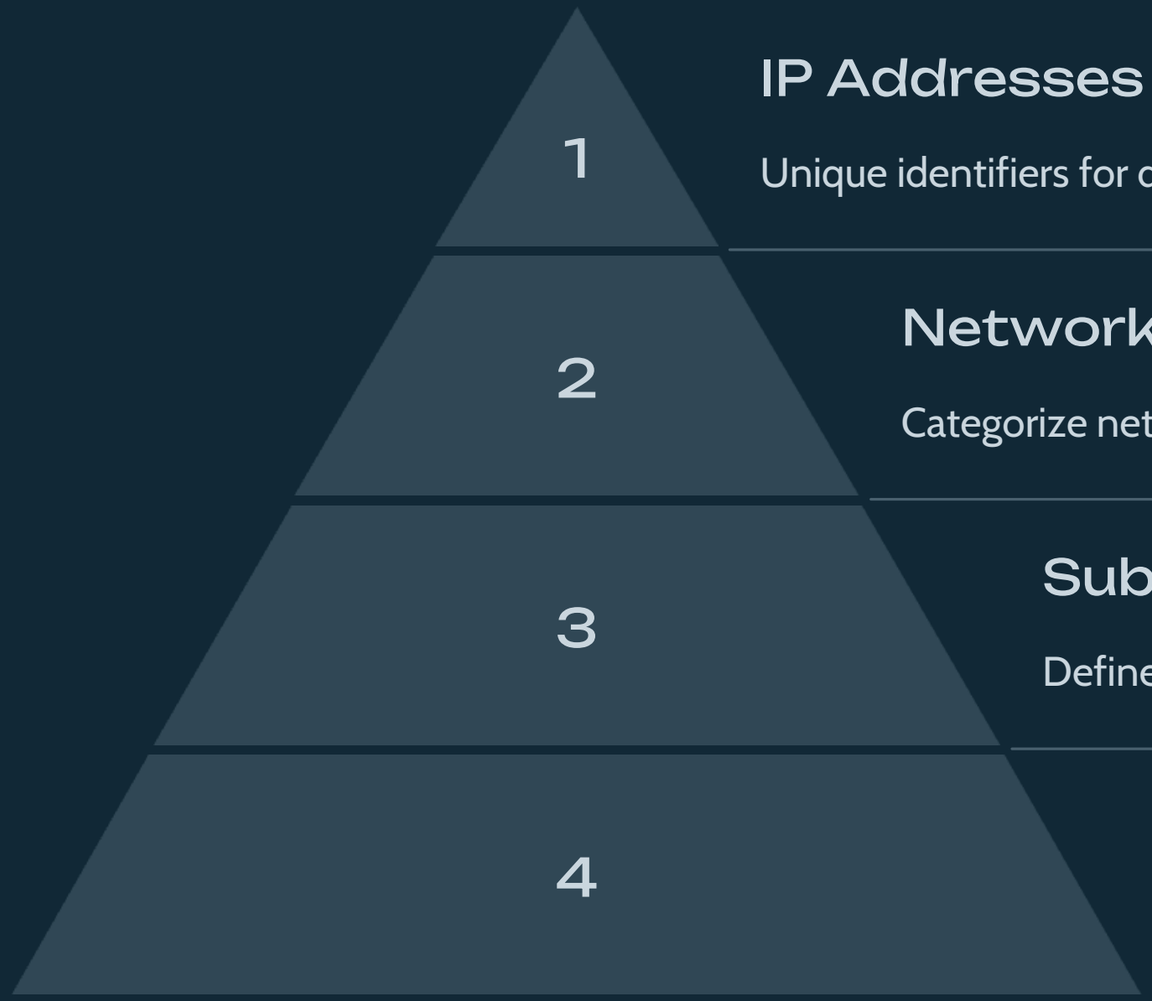
Subnet Mask Calculation

Learn how to calculate subnet masks and determine network and host addresses.

Troubleshooting Subnetting Issues

Identify and troubleshoot common problems related to subnetting configuration.

IP Addressing Fundamentals



IP Addresses

Unique identifiers for devices on a network.

Network Classes

Categorize networks based on address ranges.

Subnet Masks

Define network and host portions of an IP address.

CIDR Notation

Concise representation of IP addresses and subnet masks.

Subnet Mask Calculation

1

Subnet Mask

Divide network into smaller subnets.

2

Network Address

Identifies the specific network.

3

Host Address

Identifies a device within a network.

4

Broadcast Address

Allows communication to all devices in a subnet.

Subnetting Examples and Exercises

Example 1

Calculate subnet masks for various scenarios.

Example 2

Identify network and host addresses within a subnet.

Exercise 1

Apply subnetting concepts to practical scenarios.

Exercise 2

Solve subnetting problems and troubleshoot issues.

Troubleshooting Subnetting Issues

Connectivity Problems

Unable to reach devices within a subnet.

Address Conflicts

Two or more devices assigned the same IP address.

Subnet Mask Mismatch

Inconsistent subnet masks between devices.

Practical Applications of Subnetting

1

Network Segmentation

Improve security and performance by isolating traffic.

2

Address Conservation

Maximize available IP addresses for a growing network.

3

Network Administration

Simplify network management and troubleshooting.

Summary and Key Takeaways

Subnetting is a fundamental networking concept that allows you to optimize your network by dividing it into smaller, manageable subnets. By understanding how to calculate subnet masks and troubleshoot issues, you can improve network security, efficiency, and performance.

Week-02 Introduction to Routing Protocols: RIP, OSPF, BGP

This lab module will provide a comprehensive introduction to routing protocols, including RIP, OSPF, and BGP.

 **by Md. Tariqul Islam**

Course Overview and Learning Objectives

Course Overview

This lab module covers the fundamental concepts of routing protocols and provides practical experience configuring and troubleshooting them.

Learning Objectives

By the end of this lab, you will be able to:

- Understand the basics of routing protocols
- Configure RIP, OSPF, and BGP on network devices
- Troubleshoot common routing protocol issues
- Analyze routing protocol data to optimize network performance

Fundamental Networking Concepts: Review

1 **IP Addressing**

Understanding IP addresses and subnetting is crucial for routing protocols.

2 **Network Layers**

Routing protocols operate at the network layer of the OSI model.

3 **Routing Table**

The routing table stores information about network destinations and the paths to reach them.

Routing Protocol Basics - RIP, OSPF, BGP

RIP (Routing Information Protocol)

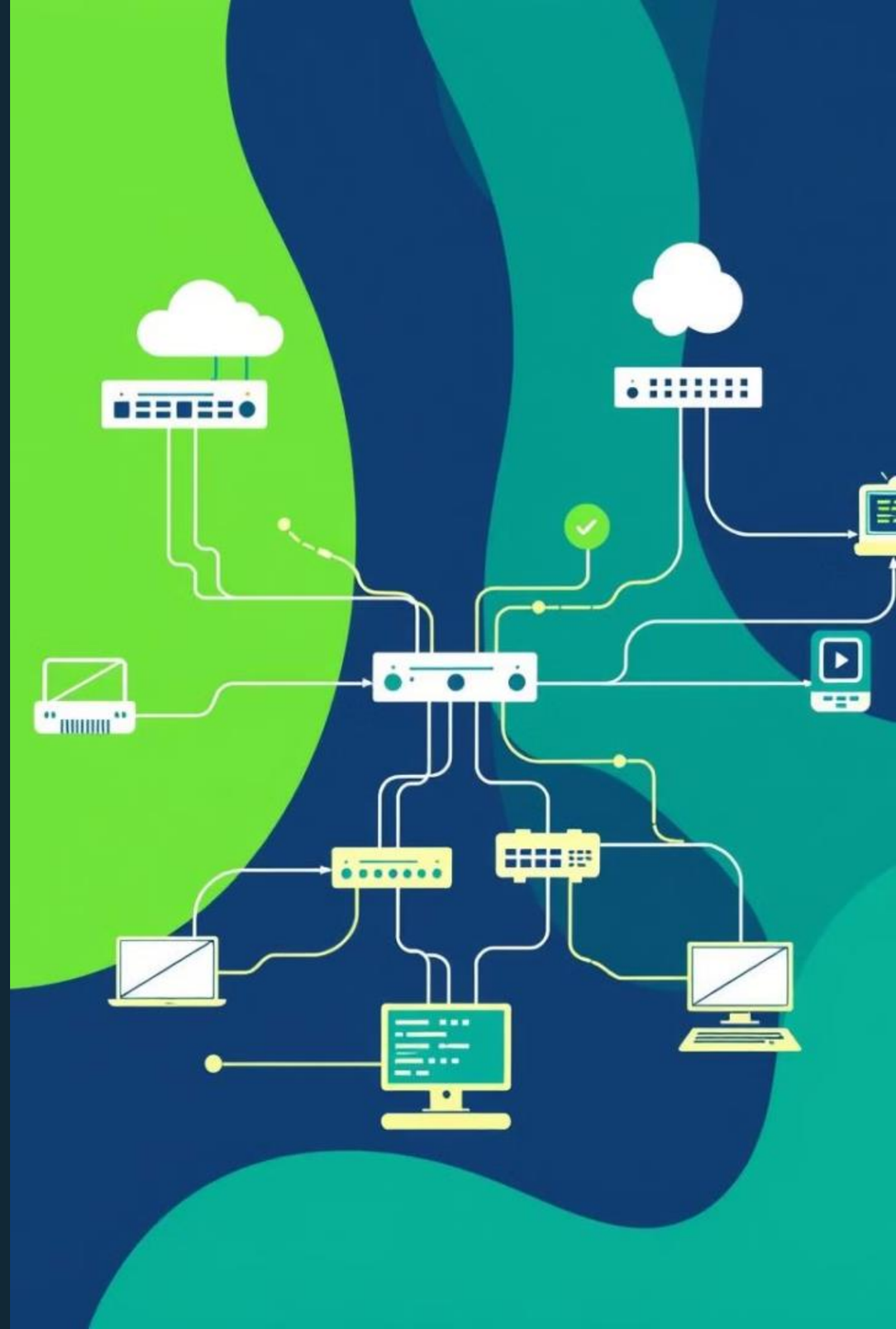
A distance-vector routing protocol that uses hop count as a metric.

OSPF (Open Shortest Path First)

A link-state routing protocol that uses a shortest path algorithm.

BGP (Border Gateway Protocol)

An inter-domain routing protocol used to exchange routing information between autonomous systems.



Practical Lab Setup and Configuration

1

Hardware Setup

Connect network devices, including routers, switches, and computers.

2

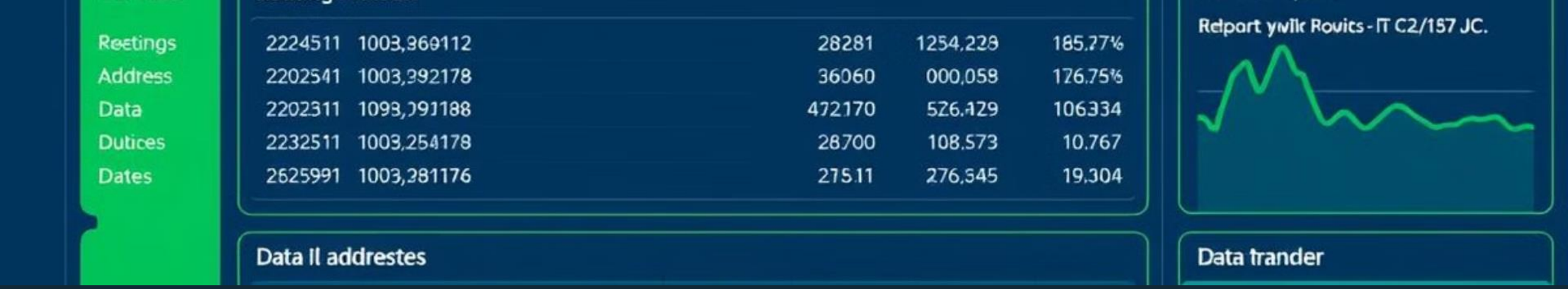
Software Configuration

Configure IP addressing, subnetting, and routing protocols on the devices.

3

Verification and Testing

Verify connectivity and test routing protocol functionality.



Troubleshooting and Optimization Techniques

1

Network Monitoring

Monitor routing protocol behavior using tools like ping, traceroute, and network management systems.

2

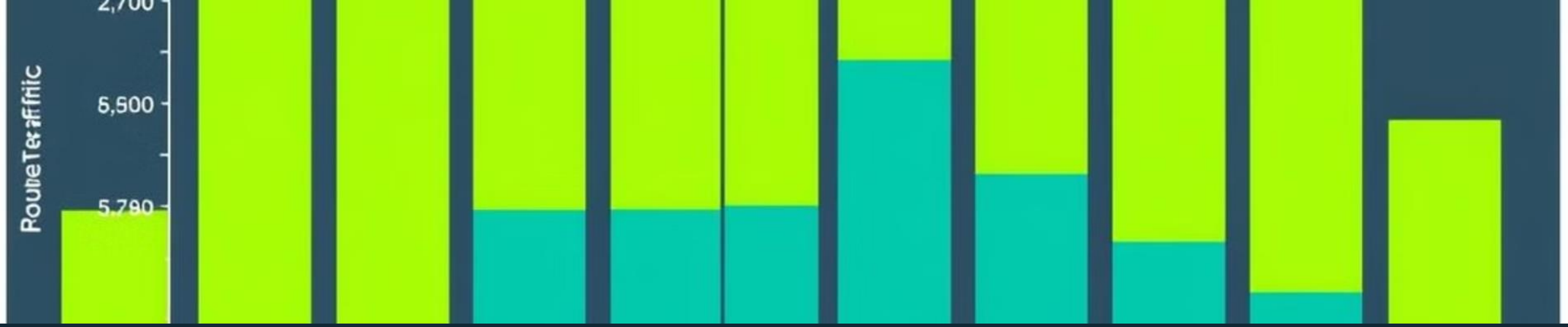
Log Analysis

Analyze routing protocol logs to identify and resolve issues.

3

Route Optimization

Adjust routing protocol parameters to optimize network performance and traffic flow.



Data Collection and Analysis

1

Traffic Monitoring

Collect routing protocol data using network monitoring tools.

2

Data Analysis

Analyze data to identify trends, bottlenecks, and areas for improvement.

3

Report Generation

Generate reports summarizing routing protocol performance and recommendations.

Conclusion and Key Takeaways

This lab module has provided a comprehensive overview of routing protocols. You've gained practical experience configuring, troubleshooting, and optimizing these protocols. Key takeaways include understanding the basics of routing protocols, configuring RIP, OSPF, and BGP, troubleshooting common routing protocol issues, and analyzing routing protocol data to optimize network performance.

Week-03
IPv6 Addressing and Configuration

Welcome to the final lab module of our Fundamental Networking Concepts course. Today we'll delve into IPv6, the next generation of internet addressing, and explore its configuration and practical applications.

by Md. Tariqul Islam

Learning Objectives

Understand IPv6 Address Structure

Explore the fundamental concepts of IPv6 addresses and their notation, including hexadecimal representation and prefix lengths.

Configure IPv6 on Devices

Learn to assign IPv6 addresses to devices and configure network interfaces for IPv6 communication.

Verify IPv6 Connectivity

Master methods for confirming IPv6 connectivity using ping, traceroute, and other tools.

Troubleshoot IPv6 Issues

Develop practical skills for identifying and resolving common problems related to IPv6 implementation.

Equipment and Preparation

Two or More Computers

Ensure your lab environment includes at least two computers capable of supporting IPv6 networking.

Network Switch or Router

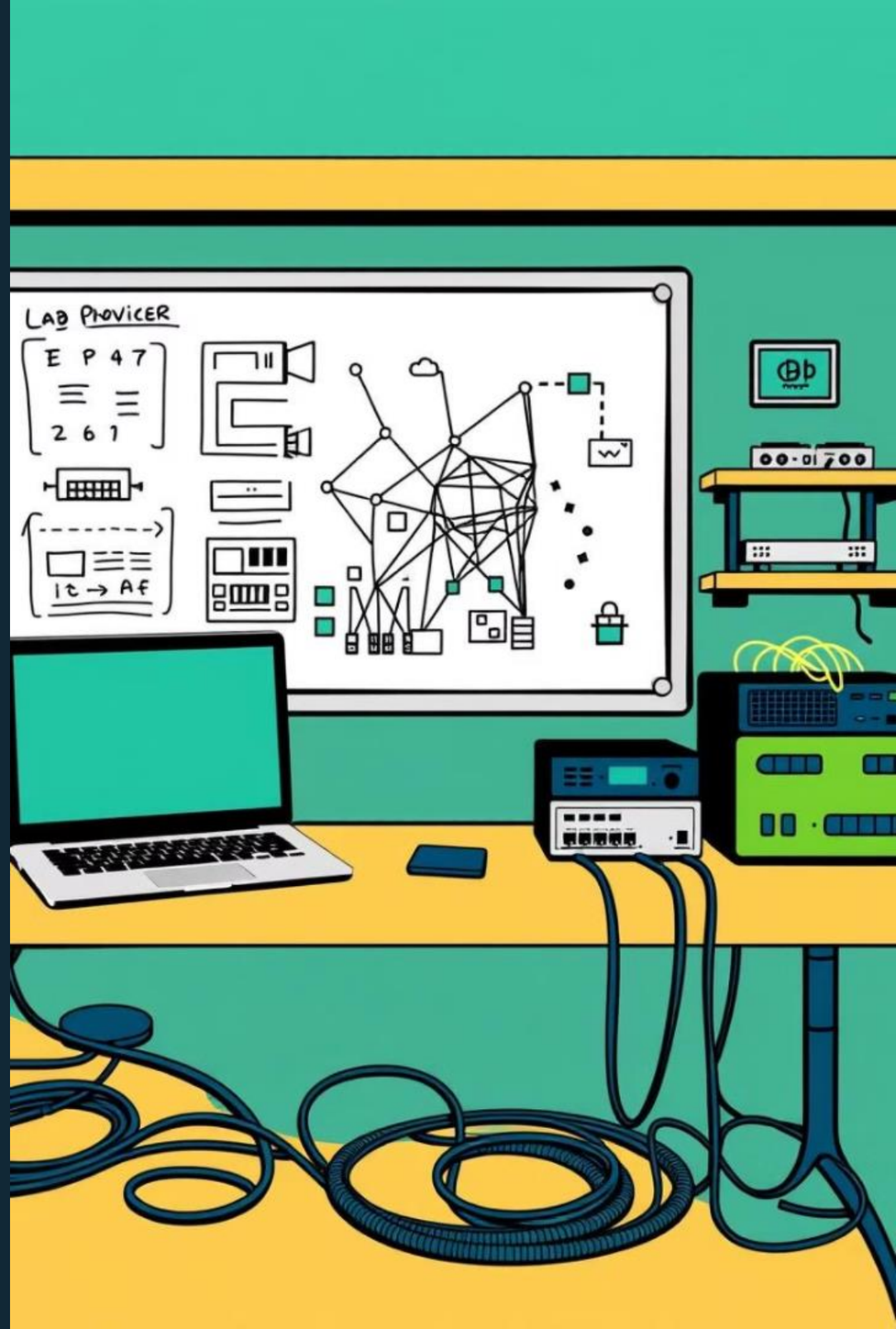
A network switch or router is required to connect the computers and facilitate IPv6 communication.

Network Cables

Sufficient network cables are needed to connect the computers to the switch or router.

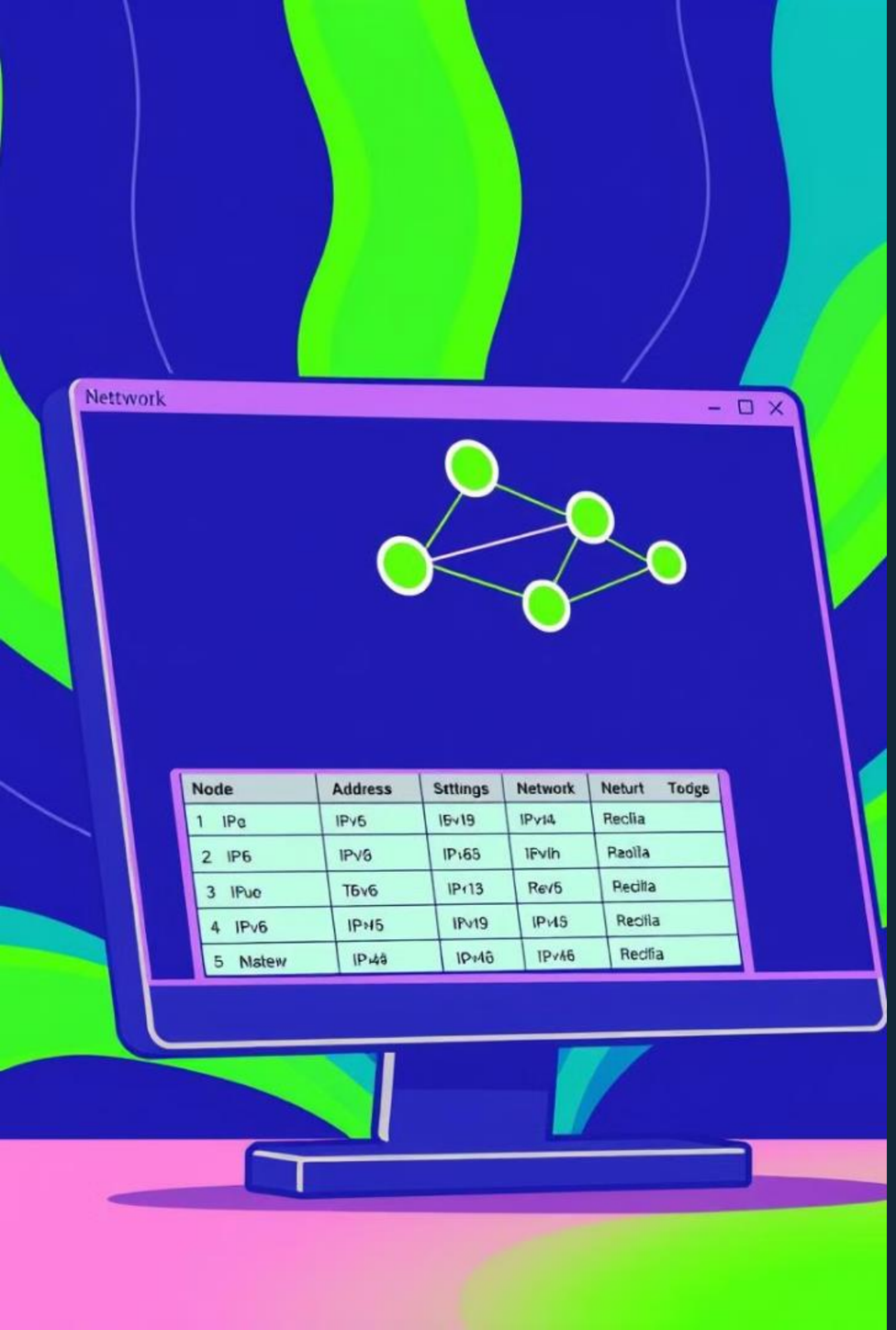
IPv6-Enabled Operating System

Make sure your computers run an operating system that supports IPv6 networking.



IPv6 Address Structure and Notation

1. IPv6 addresses are represented using 128 bits, written in hexadecimal notation.
2. An IPv6 address is divided into 8 groups of 16 bits, separated by colons (':').
3. Each group is represented by 4 hexadecimal digits, ranging from 0000 to FFFF.
4. The address structure includes network prefixes, subnet masks, and host identifiers.
5. Understanding IPv6 address notation is crucial for network configuration and troubleshooting.



IPv6 Address Assignment and Configuration

Configure Router Interface

Assign a unique IPv6 address and subnet mask to the router's network interface.

Assign IPv6 Addresses to Devices

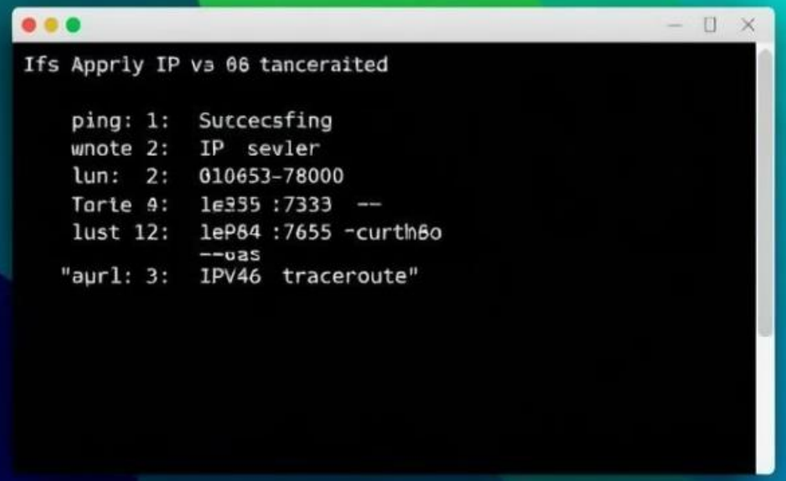
Configure static or dynamic IPv6 addresses for computers and other devices.

Define IPv6 Routing and Security

Configure routing tables and security settings to enable IPv6 communication and protect your network.

Enable IPv6 on Network Interfaces

Enable IPv6 support on all network interfaces of your devices.



Verifying IPv6 Connectivity

1

Ping Test

Use the ping command with an IPv6 address to test connectivity between devices.

2

Traceroute

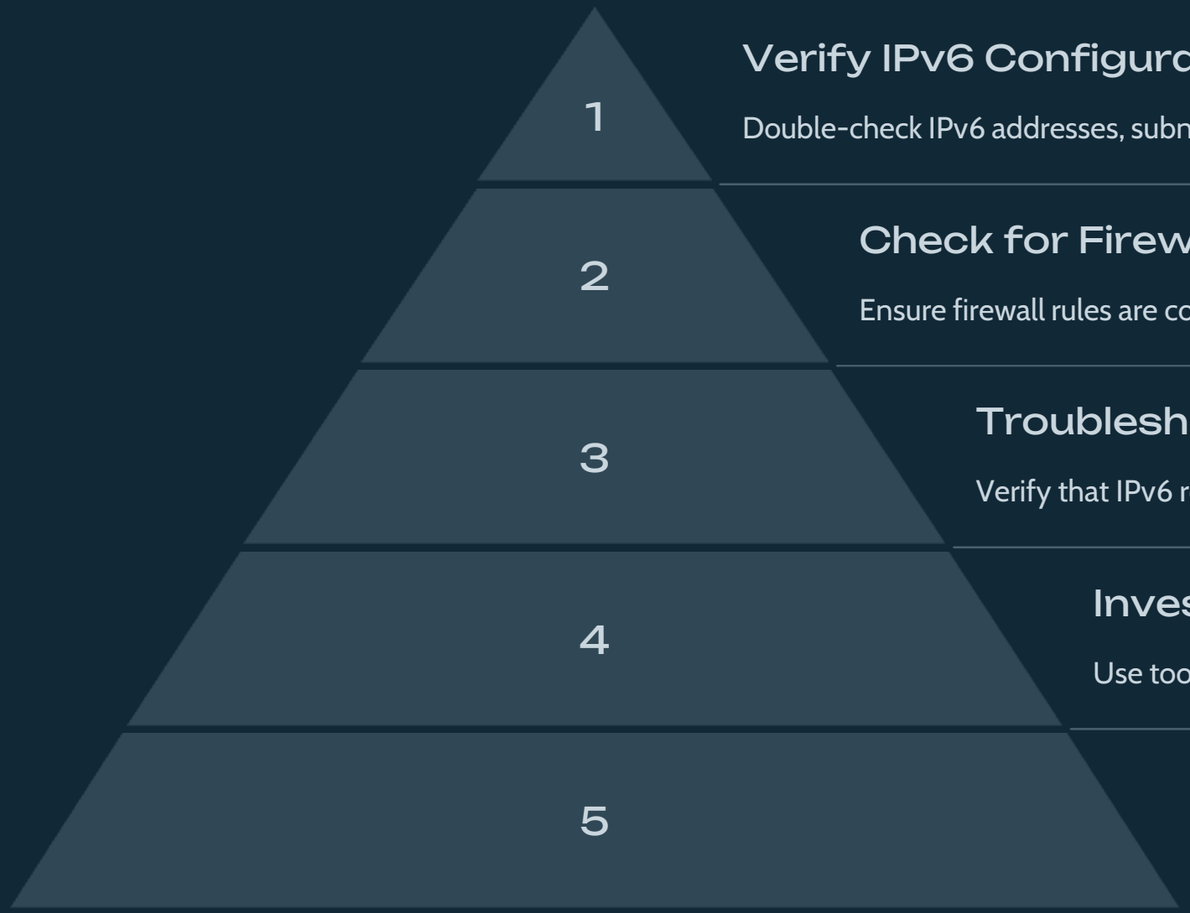
Utilize the traceroute command to trace the path of IPv6 packets between devices.

3

Network Monitoring Tools

Employ network monitoring tools like Wireshark to analyze IPv6 traffic and troubleshoot connectivity issues.

IPv6 Troubleshooting and Best Practices



Verify IPv6 Configuration

Double-check IPv6 addresses, subnet masks, and other settings on all devices.

Check for Firewall Rules

Ensure firewall rules are configured to allow IPv6 traffic.

Troubleshoot Routing

Verify that IPv6 routes are correctly configured and reachable.

Investigate Network Connectivity

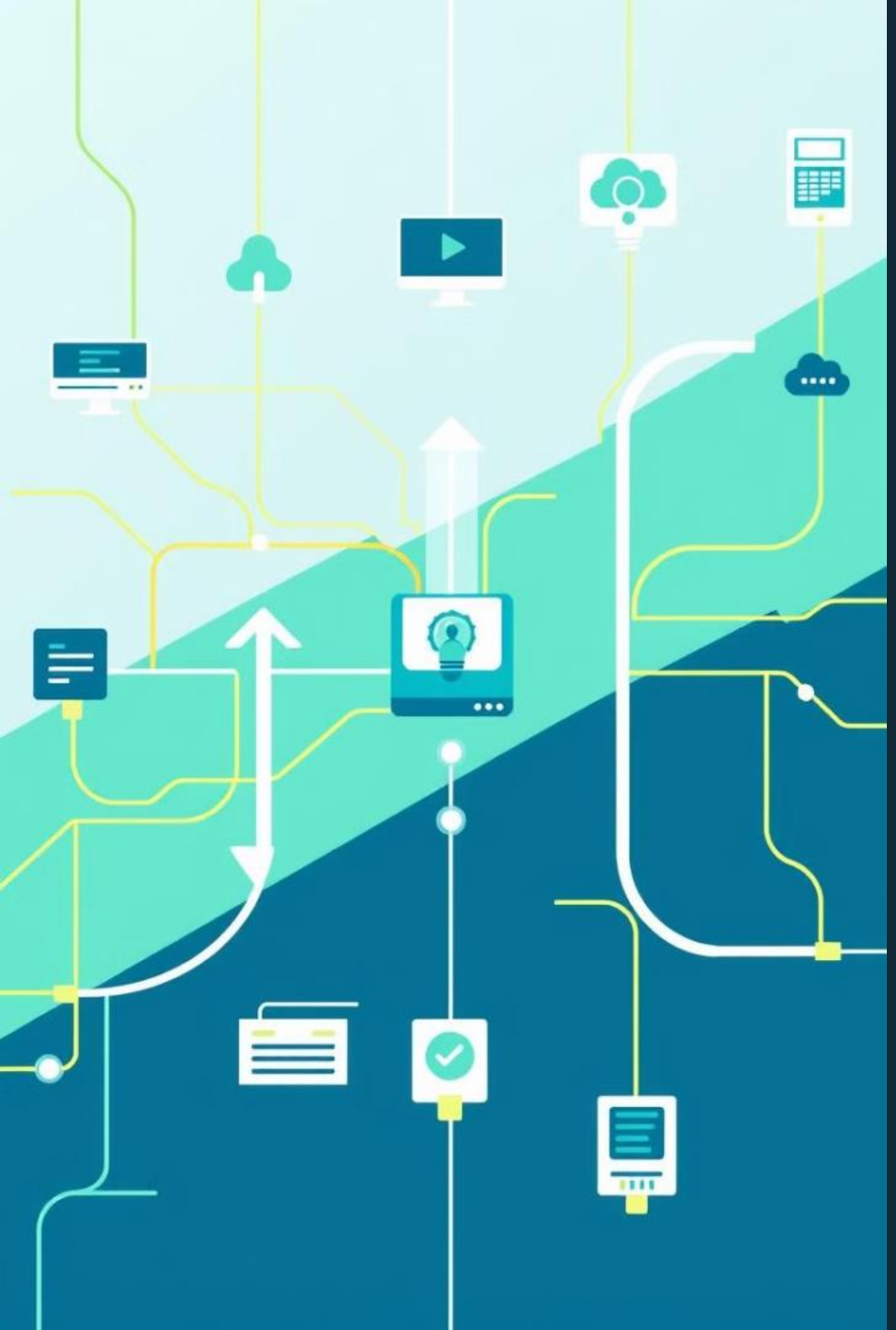
Use tools like ping and traceroute to identify points of failure.

Consult Documentation and Resources

Refer to vendor documentation and online resources for troubleshooting guidance.

Key Takeaways and Assessment

Congratulations! You've successfully completed this lab module on IPv6 addressing and configuration. You now possess a foundational understanding of IPv6, its structure, and its practical implementation.



Week:04
Setting up Static and Dynamic Routing

by Md. Tariqul Islam

Objectives, Equipment, and Preparation

Objectives

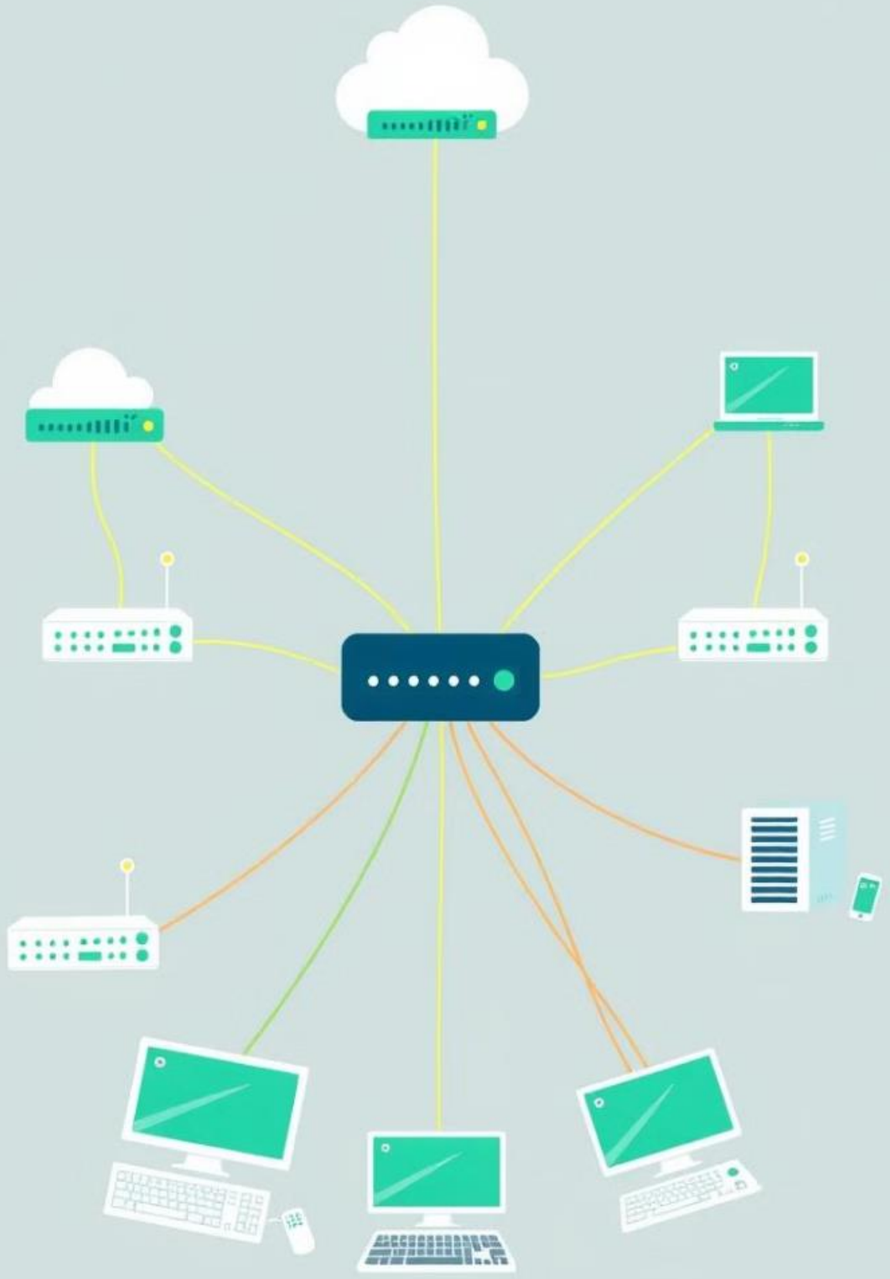
Understand static and dynamic routing concepts. Configure and troubleshoot routing protocols.

Equipment

Network devices (routers, switches), PC with network management software, Ethernet cables.

Preparation

Review network basics. Familiarize yourself with routing concepts. Gather necessary equipment.



Fundamentals of Static Routing

1 Defining Static Routes

Manually configured routes that specify the path for data packets.

2 Advantages

Predictable routing, suitable for small networks with limited changes.

3 Disadvantages

Requires manual updates, less flexible for dynamic network changes.

Implementing Dynamic Routing Protocols

RIP (Routing Information Protocol)

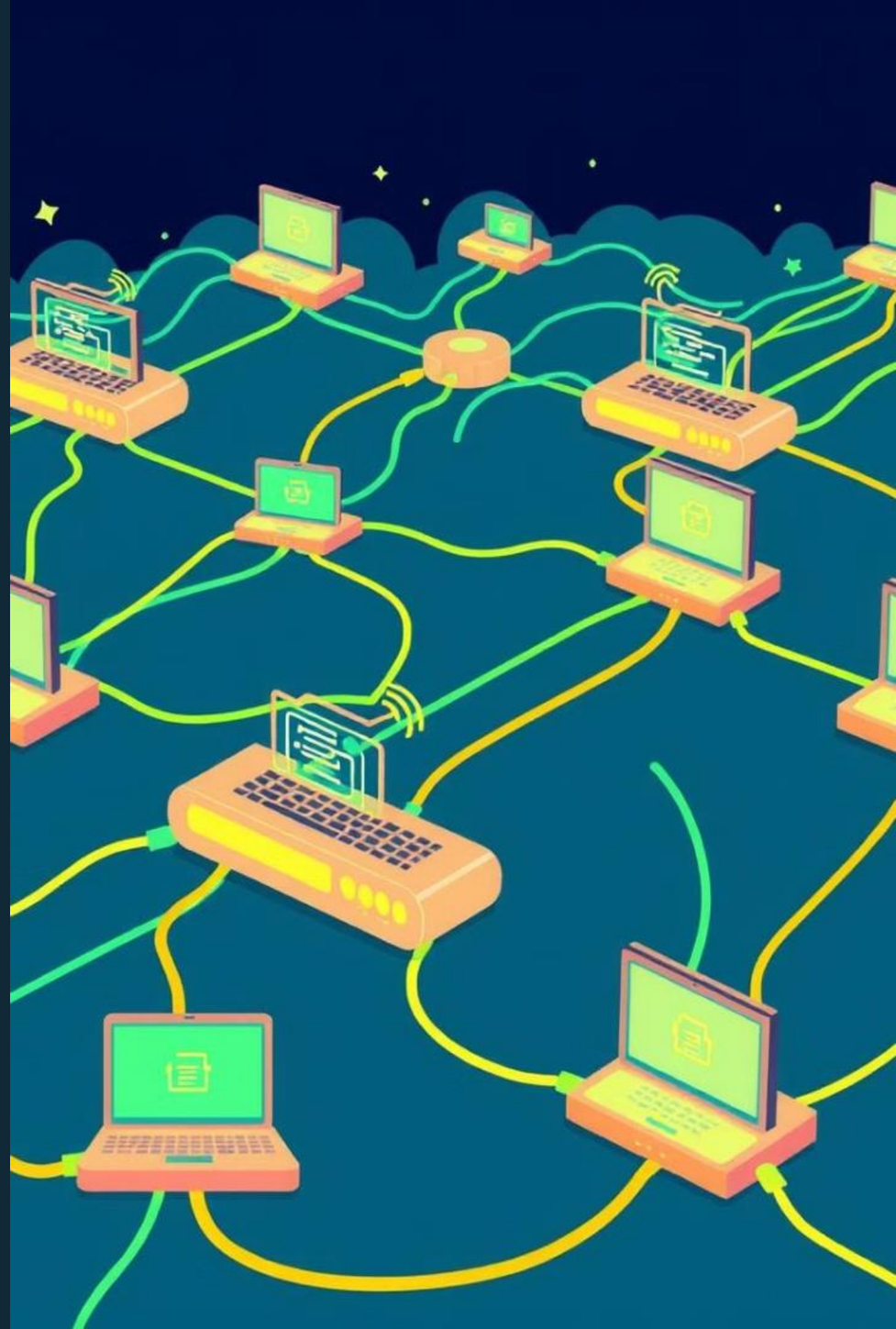
Distance-vector protocol, simple but limited to smaller networks.

OSPF (Open Shortest Path First)

Link-state protocol, more efficient for larger networks, complex configuration.

BGP (Border Gateway Protocol)

Inter-domain routing protocol, used for large-scale internet connectivity.



Configuring and Troubleshooting Routing

Router Configuration

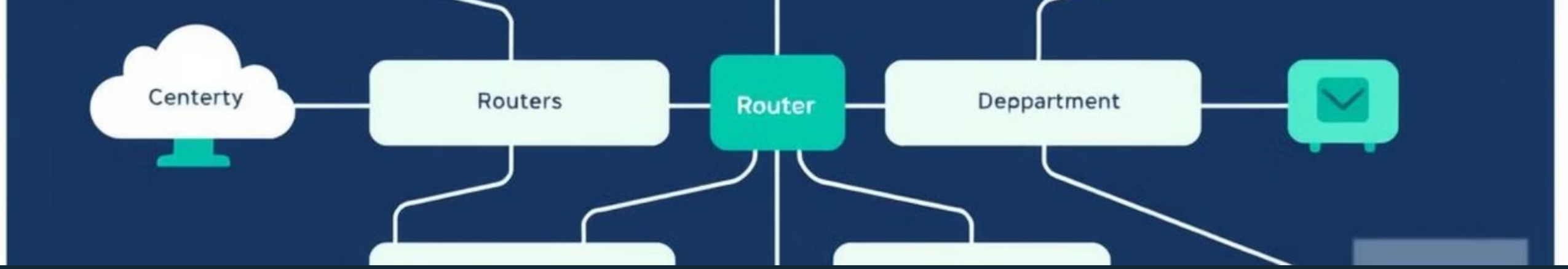
Configure routing protocols, network interfaces, and routing policies.

Troubleshooting Techniques

Analyze routing tables, ping tests, traceroute, and network device logs.

Security Considerations

Implement access control lists, security policies, and monitoring tools.



Practical Examples and Use Cases

Connecting Branch Offices

Establish routing between branch offices using dynamic routing protocols.

1

VPN Tunneling

Create secure connections between remote locations using routing protocols and VPNs.

3

2

Load Balancing

Distribute network traffic across multiple servers for optimal performance.

Data Collection and Interpretation

1

Network Monitoring Tools

Collect data on network performance, traffic patterns, and security events.

2

Performance Analysis

Identify bottlenecks, optimize network resources, and improve user experience.

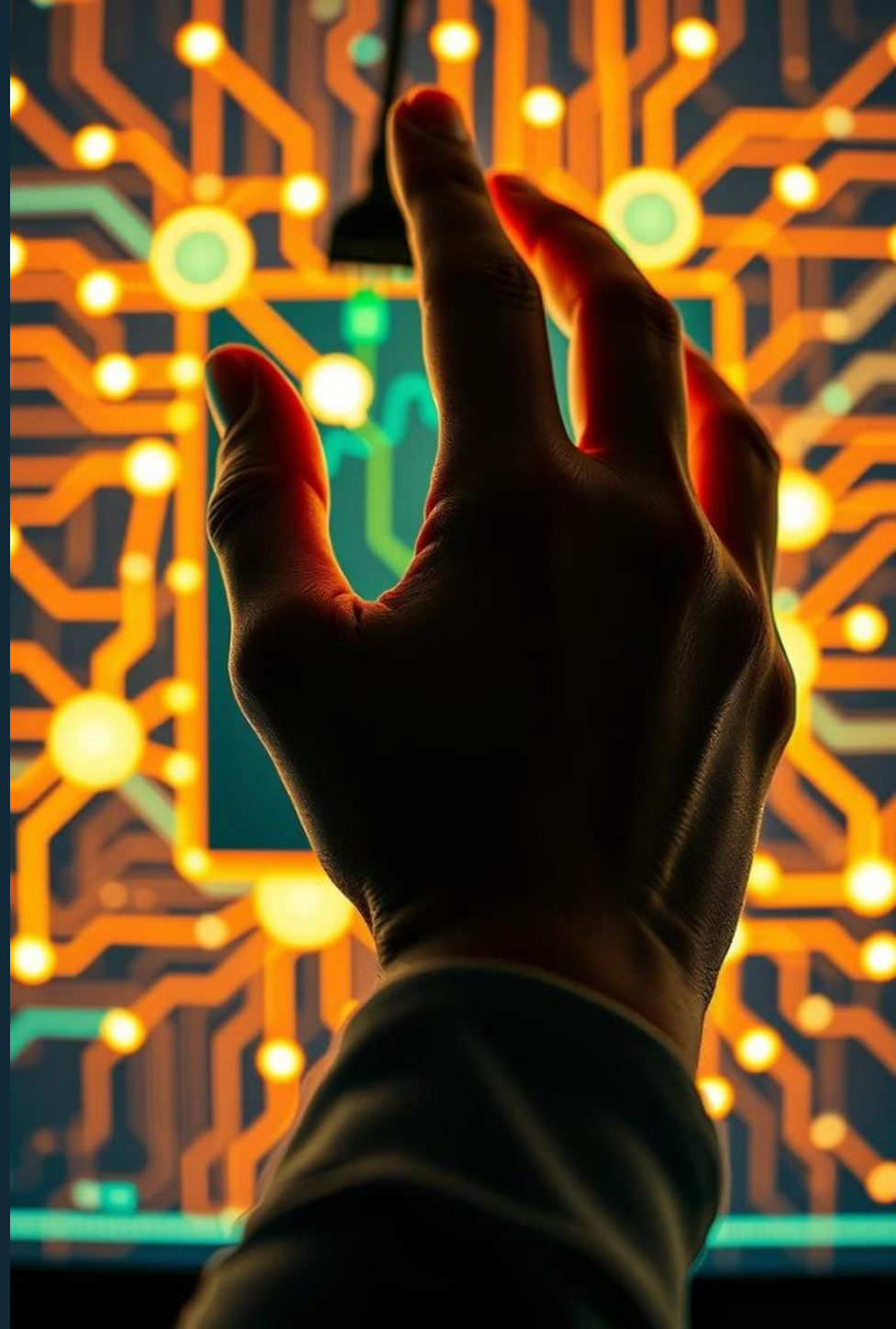
3

Troubleshooting

Identify and resolve routing issues based on collected network data.

Summary and Key Takeaways

Static routing is simple but less flexible, while dynamic routing offers greater scalability and adaptability. Routing protocols allow for efficient data packet routing across networks. Understanding network monitoring tools is essential for maintaining network health and troubleshooting issues.



Week-05
DHCP Setup and Configuration

This presentation provides a step-by-step guide to configure a DHCP server and assign IP addresses to client devices on a network.

by Md. Tariqul Islam

Objectives, Equipment, and Preparation

Objectives

- Configure a DHCP server on a router.
- Assign IP addresses to client devices.
- Troubleshoot common DHCP issues.

Equipment

- Router with DHCP capabilities
- Client devices (PCs, laptops, etc.)
- Network cables

Preparation

- Connect the router to the network.
- Ensure client devices are powered on.
- Access the router's web interface.

DHCP Server Configuration

IP Address Pool

Define a range of IP addresses that the server will allocate to clients.

Subnet Mask

Specify the subnet mask, which determines the network portion of the IP address.

Default Gateway

Configure the default gateway, which directs network traffic to the internet.

DNS Server

Set the DNS server address, which translates domain names to IP addresses.

DHCP Address Allocation

1

Request

Client devices send a DHCP request to the server.

2

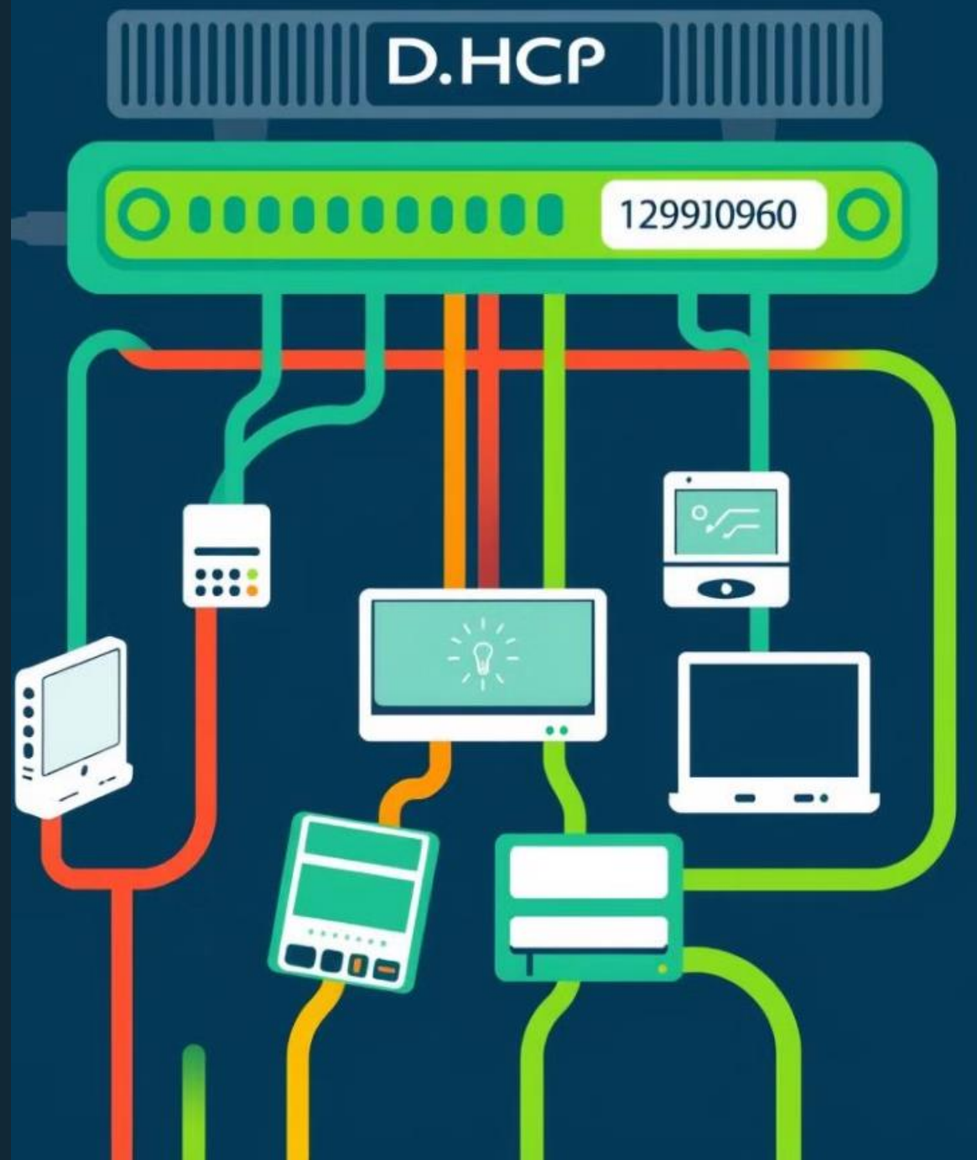
Offer

The server offers an available IP address to the client.

3

Acknowledge

The client accepts the offered IP address and acknowledges the server.



Troubleshooting DHCP Issues

1 IP Address Conflict

Two devices may be assigned the same IP address.

2 DHCP Server Down

The DHCP server may be malfunctioning or unavailable.

3 Incorrect Network Settings

Client devices may have incorrect network settings.

Practical Examples and Scenarios

Home Network

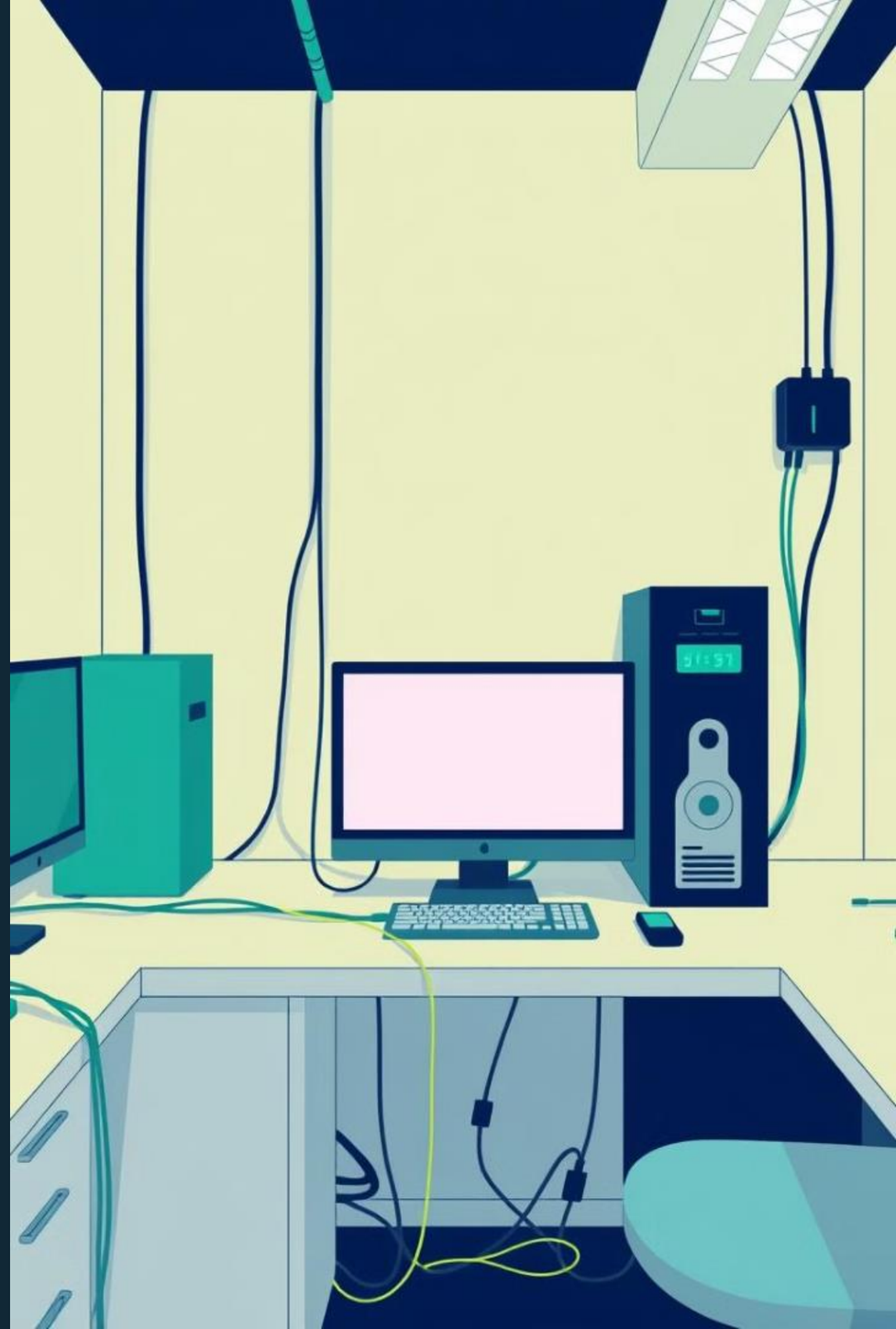
Assign IP addresses to devices in a home network.

Small Office

Provide automatic IP address allocation to employees' computers.

Public Wi-Fi

Enable DHCP for public Wi-Fi networks in cafes or hotels.



Data Collection and Monitoring

Server Logs

Monitor DHCP server logs for errors or unusual activity.

Network Monitoring Tools

Use network monitoring tools to track DHCP server performance.

Data Analysis

Analyze collected data to identify trends and improve network performance.

Summary of Key Takeaways

1

DHCP Simplifies IP Address Allocation

Automated process for assigning IP addresses to devices.

2

Essential for Network Management

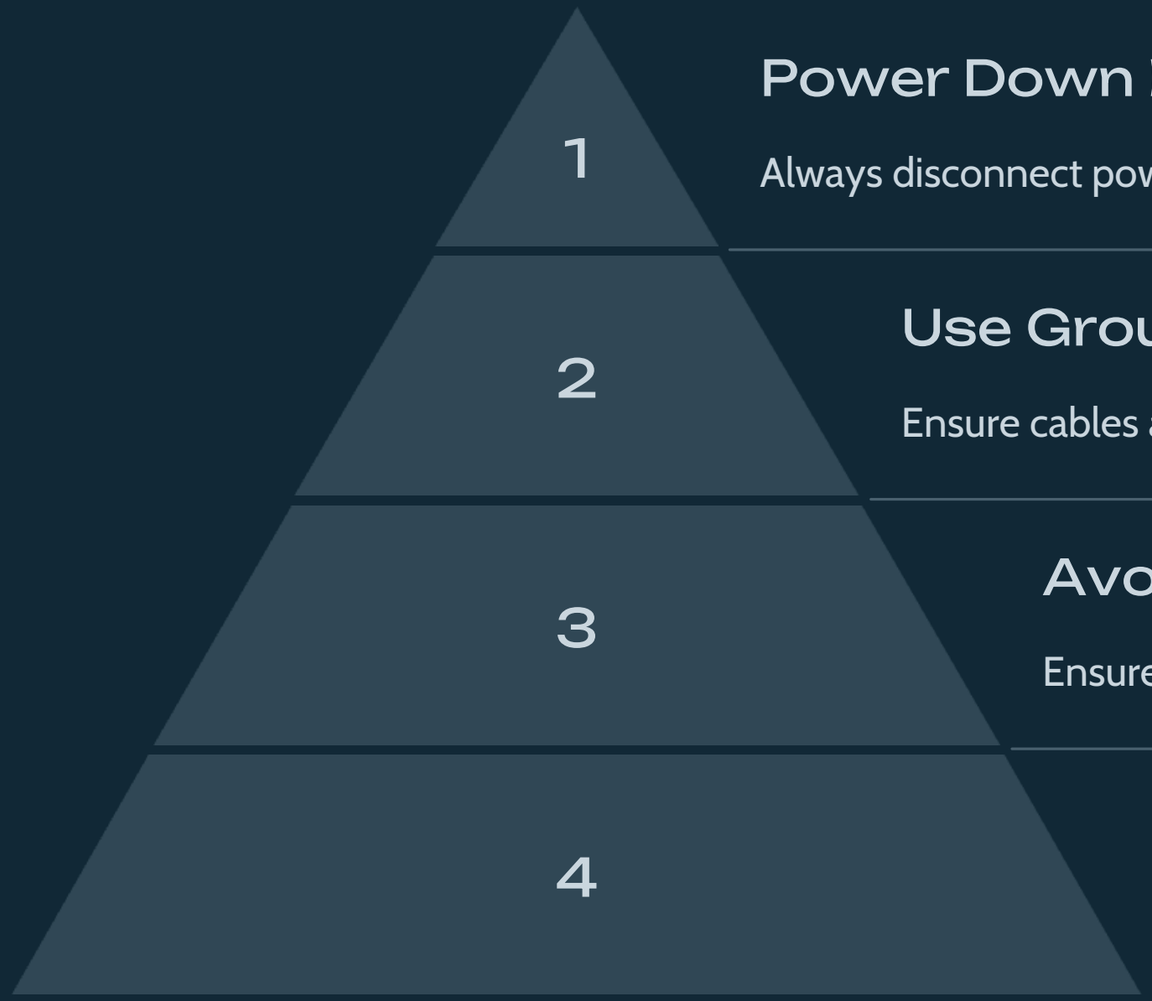
Provides network stability and efficient resource allocation.

3

Troubleshooting Is Key

Understanding common issues ensures smooth network operation.

Safety Tips



Power Down Equipment

Always disconnect power before working on network devices.

Use Grounded Cables

Ensure cables and equipment are grounded to prevent electric shocks.

Avoid Overloading Circuits

Ensure sufficient power capacity for all network devices.

Proper Ventilation

Ensure adequate airflow to prevent overheating.

Next Steps

1

Practice

Set up a DHCP server in a lab environment or on a home network.

2

Explore Advanced Features

Learn about DHCP options and advanced configurations.

3

Network Monitoring

Implement network monitoring tools to track DHCP server performance.

Week-06 Configuring and Troubleshooting NAT

This lab will guide you through the process of configuring and troubleshooting Network Address Translation (NAT), a key networking concept.

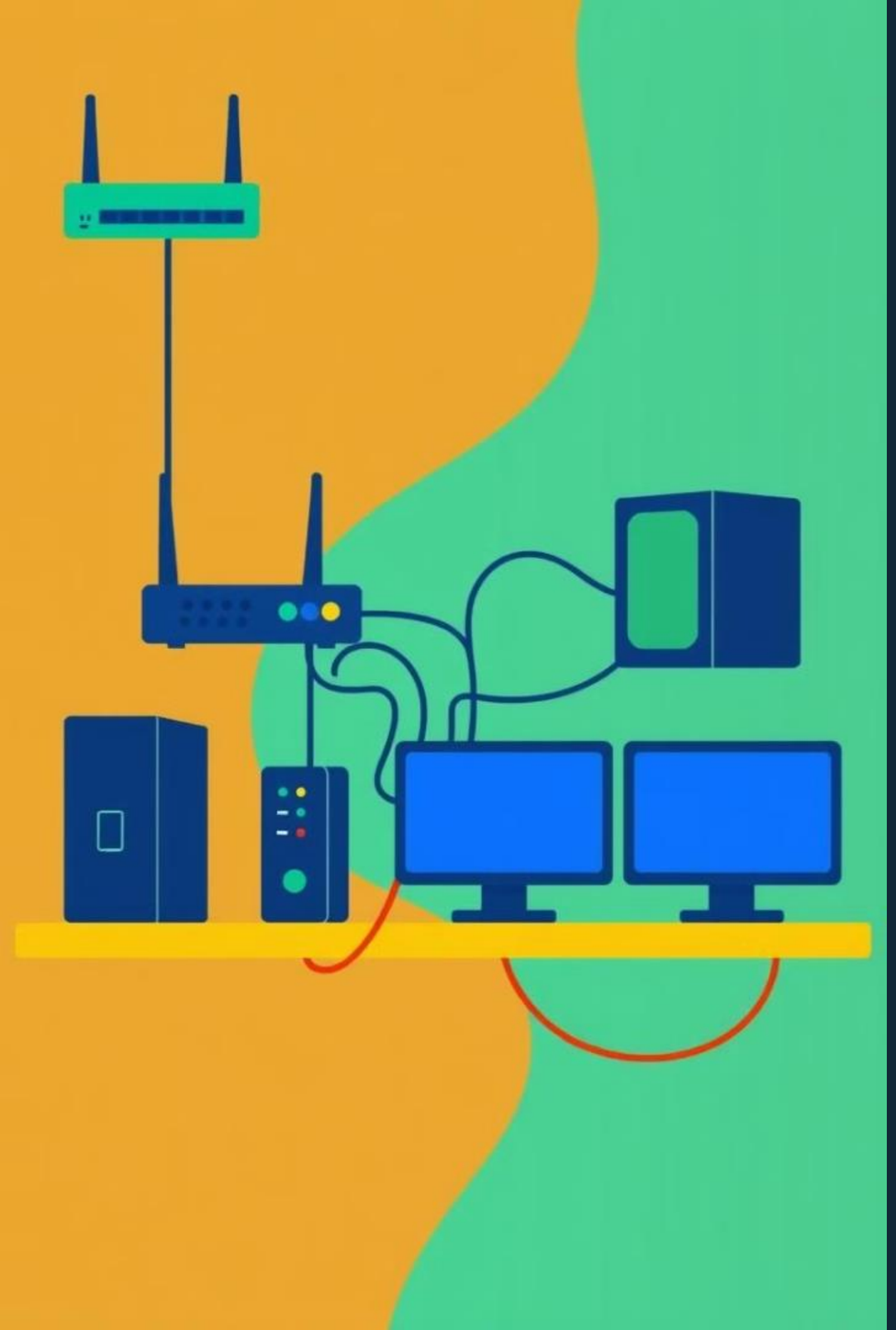
by Md. Tariqul Islam

Objectives

Understand the purpose and operation of NAT.

Configure NAT on a router.

Troubleshoot common NAT issues.



Equipment and Preparation

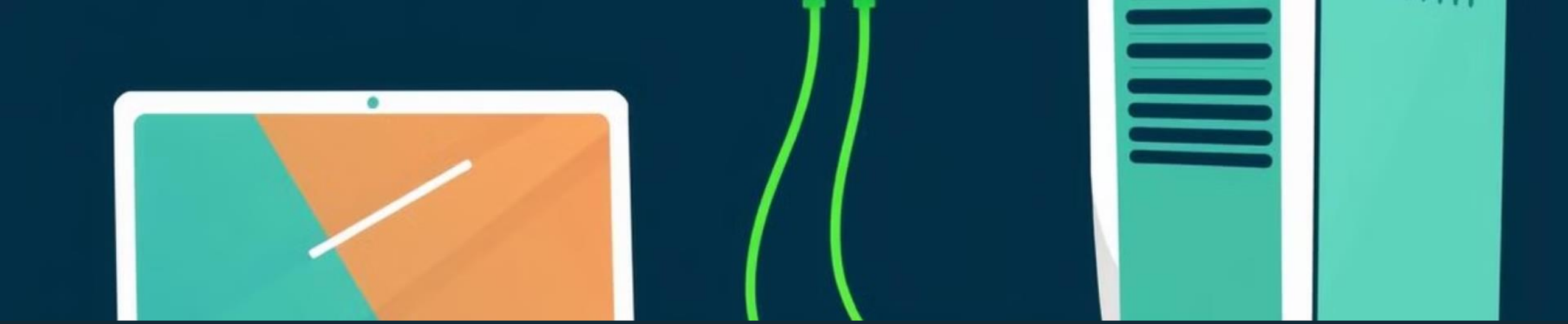
Equipment	Description
Router	A device that connects different networks and performs NAT.
Switch	A device that connects multiple devices on a local network.
PCs	Computers used to test NAT functionality.
Console cables	Cables used to connect to the router's console port for configuration.

Router

The router is the central device in this lab. Ensure it is powered on and connected to the network.

Switch

Connect the switch to the router's appropriate interface. The switch will connect the PCs to the network.

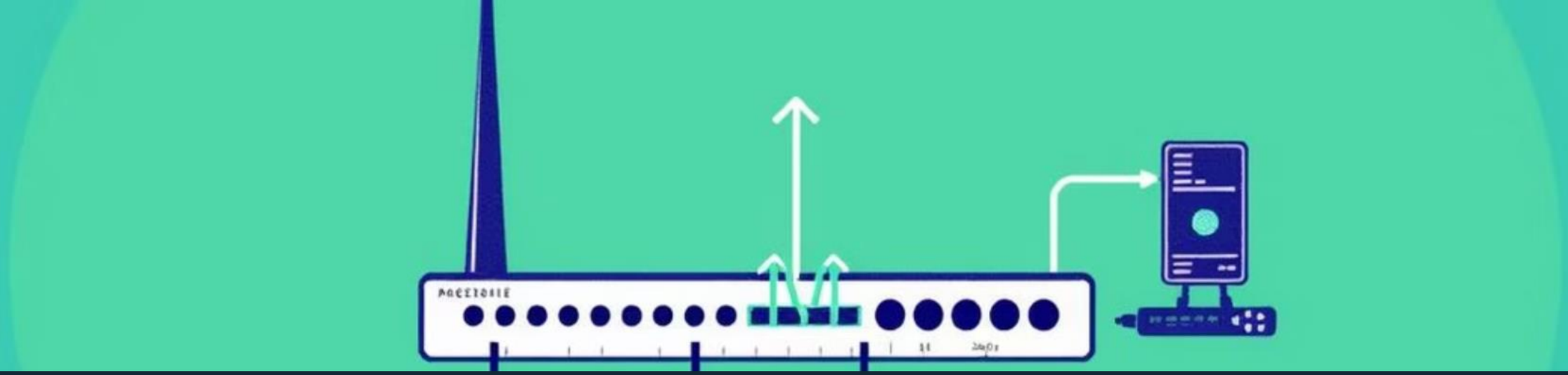


PCs

Connect the PCs to the switch using network cables. Ensure they have IP addresses and are functioning properly.

Console Cables

Connect the console cable to the router's console port and the other end to a terminal emulator program on your computer.



Connecting the Network Devices

Follow the connection diagram to connect the router, switch, and PCs. Verify all connections are secure.

Week-07 Configuring the Router for NAT

Access the router's configuration terminal using the console cable. You will configure NAT using CLI commands.

Enabling NAT

1

1. Access the router's configuration terminal.

Connect to the router using a console cable and enter configuration mode.

2

2. Create a NAT pool.

Define a range of IP addresses that will be used for NAT translation.

3

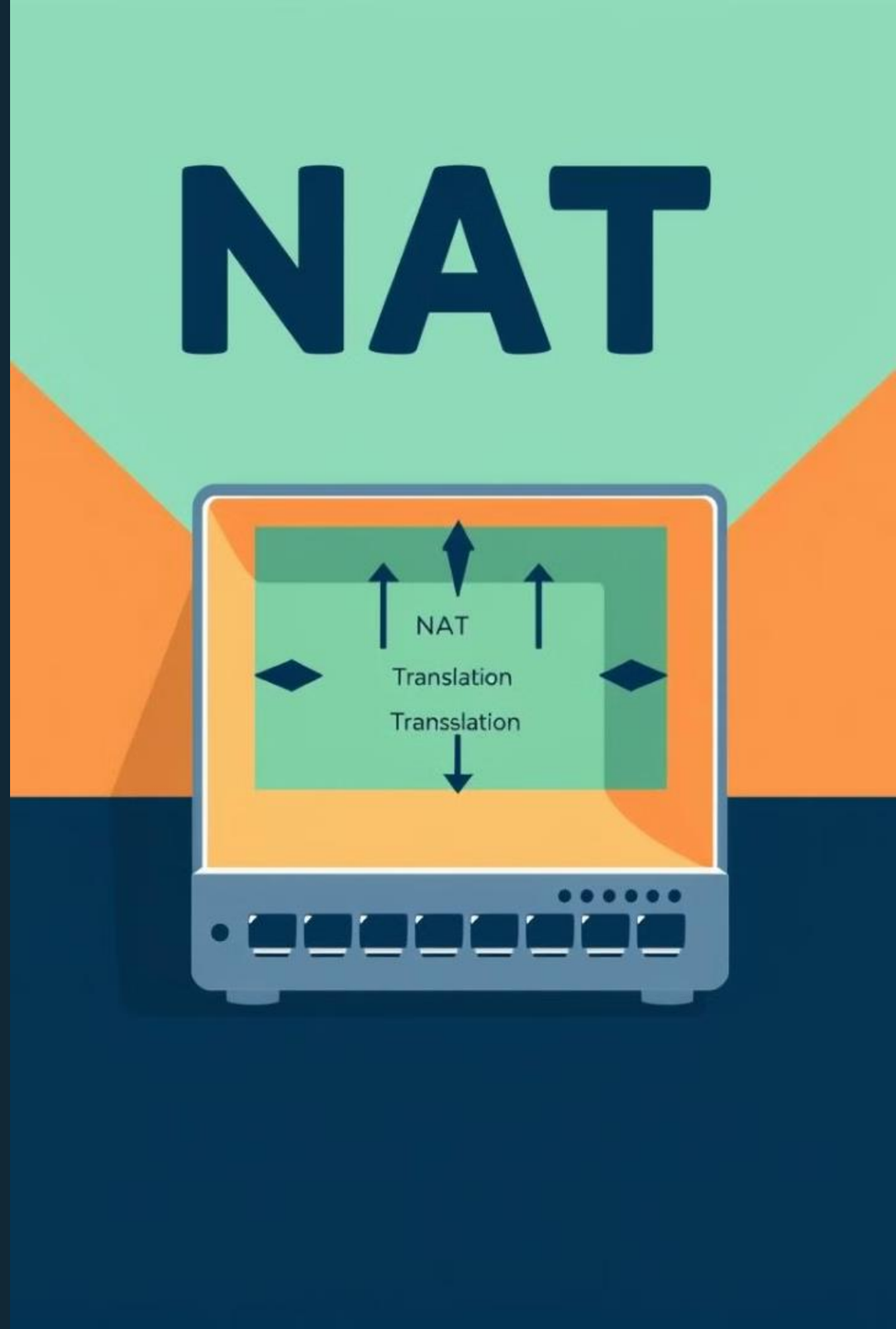
3. Configure NAT translation rules.

Specify the conditions for NAT translation, such as the source address, destination address, and protocol.

4

4. Verify the configuration.

Use commands to verify that NAT is enabled and configured correctly.



Week-07 Introduction to VPNs and Configuring a Site-to-Site VPN

This presentation will introduce you to Virtual Private Networks (VPNs), focusing on setting up a secure Site-to-Site VPN connection.

by Md. Tariqul Islam

Objectives

Understanding VPN Basics

Learn the fundamental concepts of VPN technology, including its benefits, types, and how it works.

Configuring a Site-to-Site VPN

Gain practical skills in configuring a Site-to-Site VPN connection using industry standard practices.

Troubleshooting Common Issues

Develop the ability to troubleshoot common problems and diagnose VPN connection failures.

Equipment and Preparation

Two Routers

One for each network you want to connect using a VPN.

Network Cables

To connect your devices to the routers and ensure stable network connectivity.

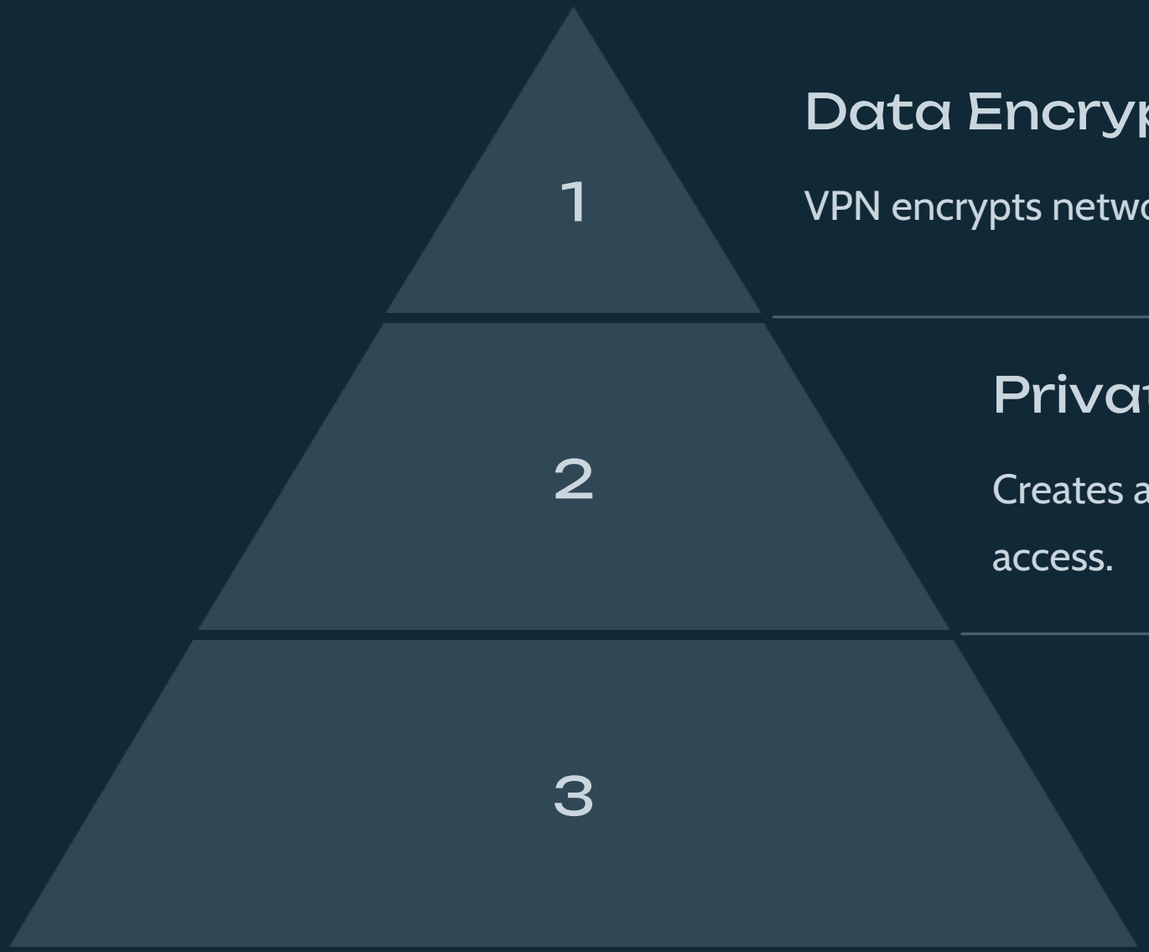
VPN Software

Pre-installed on your routers or downloaded from the manufacturer's website.

Network Management Software

Optional, but helpful for monitoring network traffic and troubleshooting VPN connections.

VPN Fundamentals



Data Encryption

VPN encrypts network traffic between devices, ensuring secure communication.

Private Tunnel

Creates a virtual tunnel, hiding your network traffic from unauthorized access.

Remote Access

Allows users to access network resources from remote locations securely.

Site-to-Site VPN Configuration

1

Configure VPN Settings

Enable VPN on both routers, set protocols, and configure security settings.

2

Create a Tunnel

Establish a VPN tunnel between the two routers, specifying IP addresses and encryption keys.

3

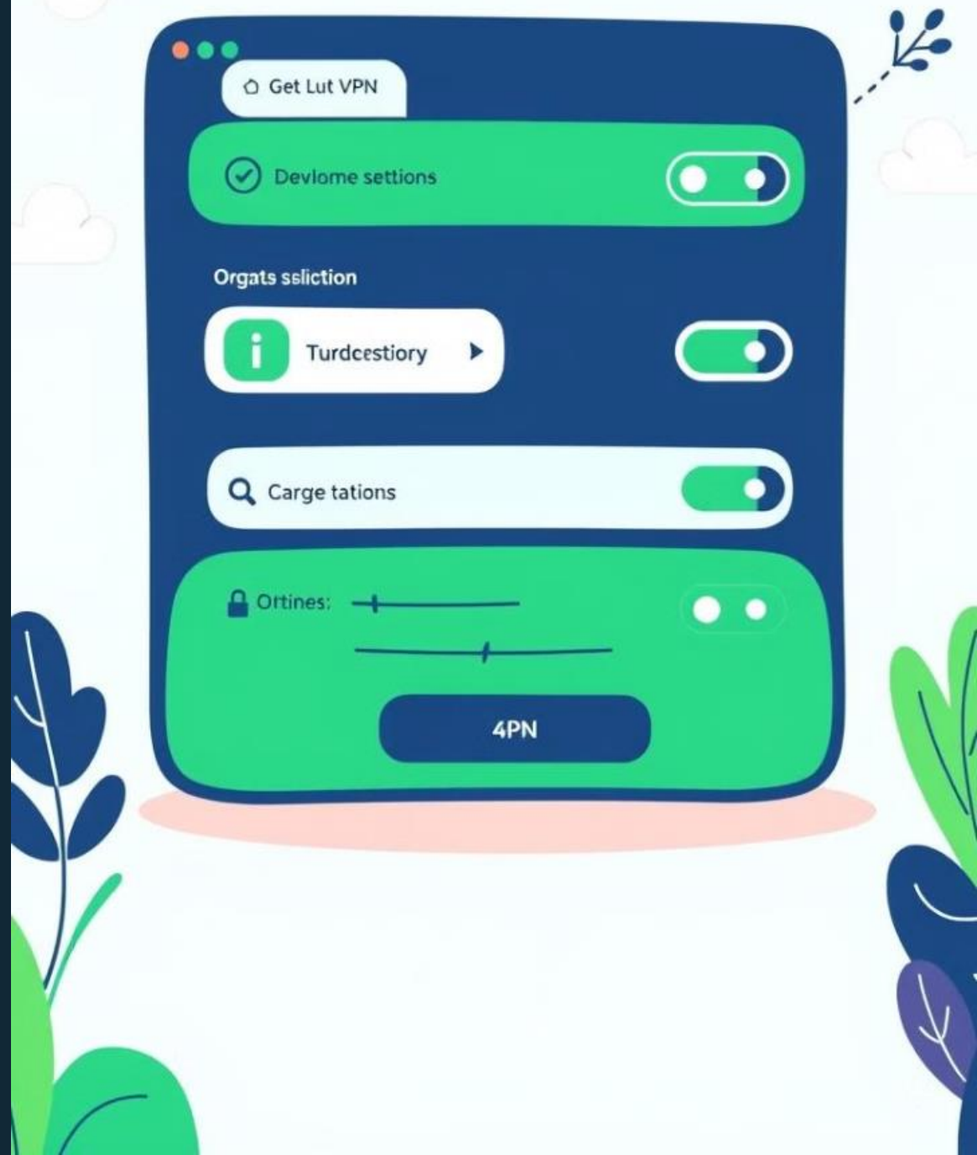
Test Connectivity

Verify the VPN connection by pinging devices on the remote network.

4

Configure Firewall Rules

Adjust firewall rules to allow traffic through the VPN tunnel.



Troubleshooting and FAQs

Connectivity Issues

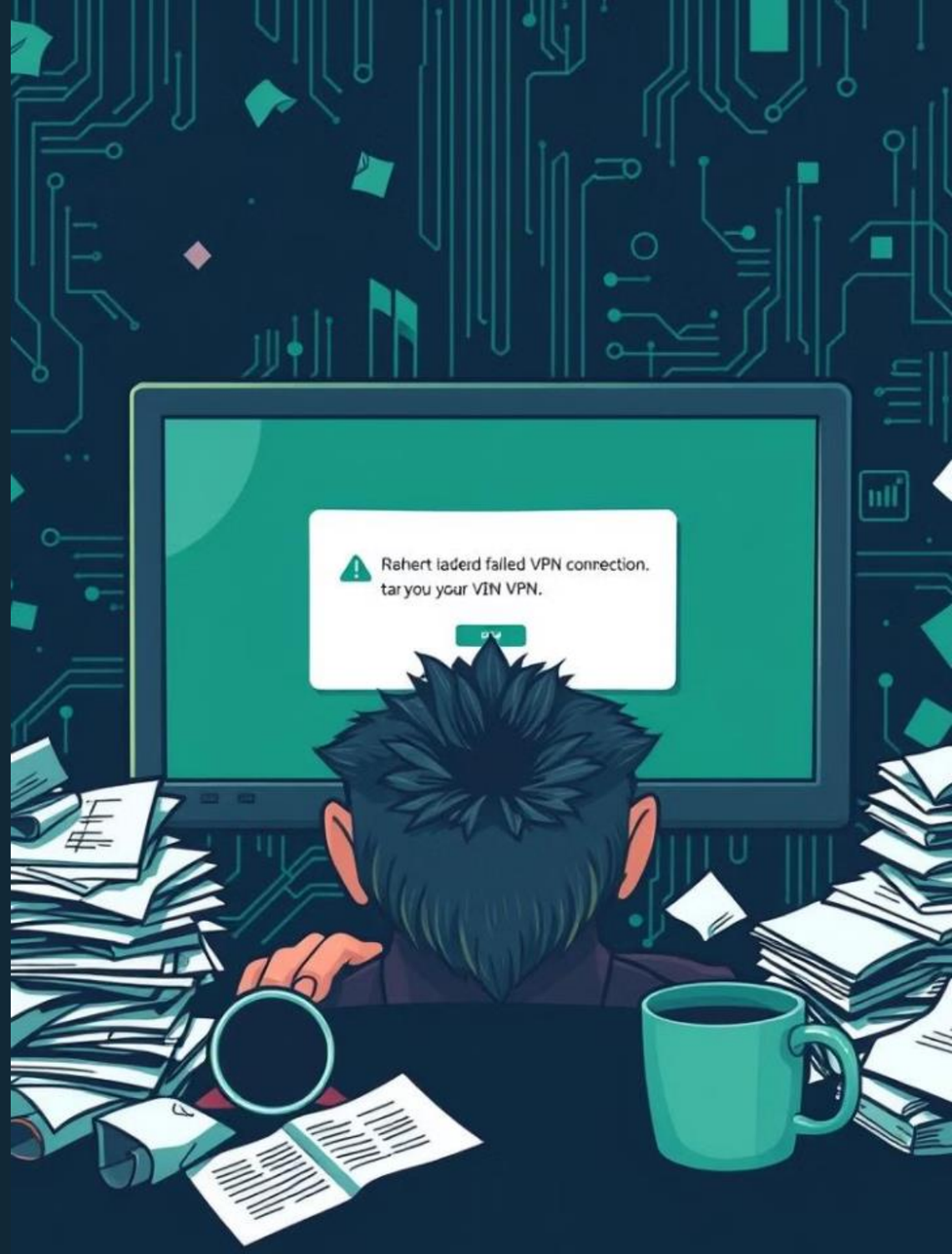
Check network cables, firewall settings, and VPN configurations.

Authentication Errors

Ensure correct username, password, and pre-shared keys are used.

Performance Issues

Consider upgrading network hardware or optimizing VPN settings.



Practical Examples and Use Cases

1

Remote Branch Offices

Connecting geographically dispersed branch offices to central servers.

2

Secure Data Sharing

Sharing confidential data securely between partners or clients.

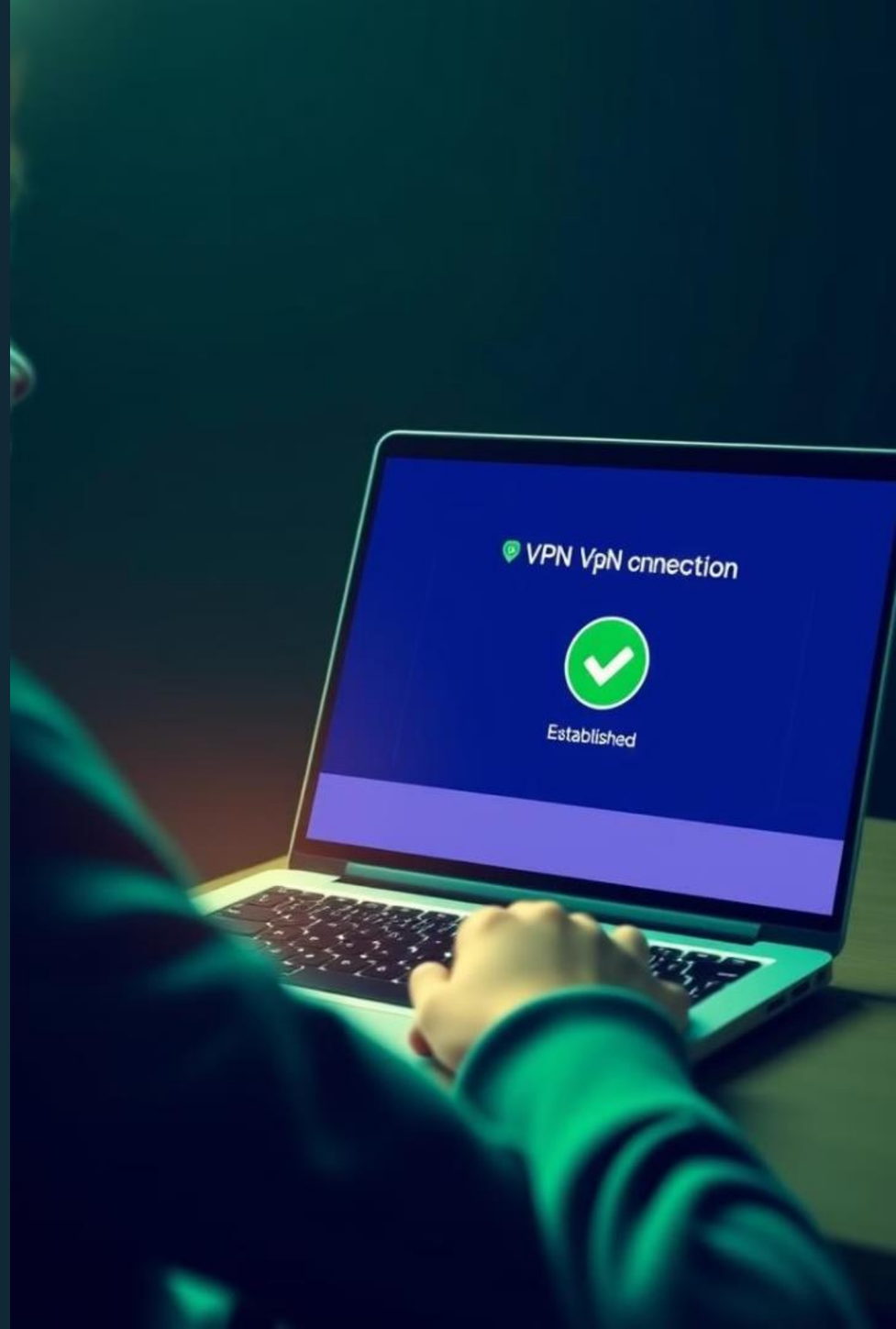
3

Mobile Workforces

Enabling remote employees to access company resources securely.

Summary and Key Takeaways

VPNs provide a secure and reliable way to connect networks and access resources remotely. Configuring a Site-to-Site VPN requires careful planning, understanding VPN fundamentals, and troubleshooting potential issues. VPNs enhance data security, improve remote access, and enable seamless collaboration across geographical boundaries.



Week-08
MAC Address Table and VLAN Tagging in Network Devices

This presentation introduces MAC address table and VLAN tagging concepts in network devices.

by Md. Tariqul Islam

Objectives

Understanding MAC Address Table

Learn the structure and function of MAC address tables in network devices.

Exploring VLAN Tagging Concepts

Explore how VLAN tagging allows for logical segmentation of networks.

Equipment

Router

A device that connects different networks and forwards data packets based on their destination addresses.

Switch

A device that learns the MAC addresses of connected devices and forwards data frames based on destination MAC addresses.

Network Cables

Physical connections used to transmit data between network devices.

Workstations

Computers or devices used to access the network and interact with network resources.

Preparation

1

Gather Equipment

Ensure all necessary hardware is available and functional.

2

Draw Network Topology

Create a visual representation of the network setup for clarity and understanding.

3

Review Concepts

Refresh your knowledge of MAC addresses, VLANs, and network devices.

Procedure 1: Observe MAC Address Table on a Network Switch

1. Connect to the switch console using a terminal emulator (e.g., PuTTY).
2. Use the "show mac address-table" command to display the MAC address table.
3. Examine the table structure, including MAC address, port, and age.

MAC Address Table Structure

MAC Address	Port	Age
00:00:00:00:00:01	G0/1	120 seconds
00:00:00:00:00:02	G0/2	300 seconds

Dynamic vs. Static MAC Entries

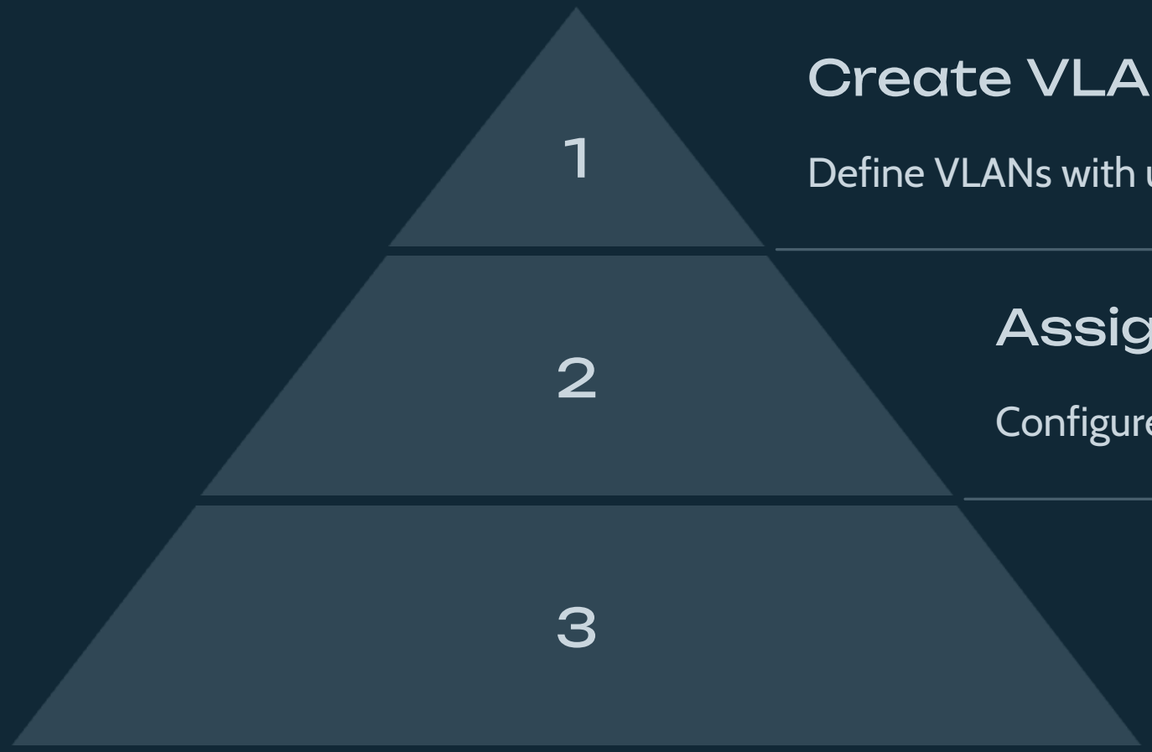
Dynamic MAC Entries

Added automatically when a device connects to the switch. Entries expire if the device disconnects.

Static MAC Entries

Manually configured on the switch. These entries persist even if the device is disconnected.

Procedure 2: Configure VLAN Tagging on a Network Switch



Create VLANs

Define VLANs with unique IDs and names.

Assign Ports to VLANs

Configure ports to belong to specific VLANs.

Configure Trunk Ports

Enable trunk ports to carry traffic from multiple VLANs.

VLAN Tagging Process

1

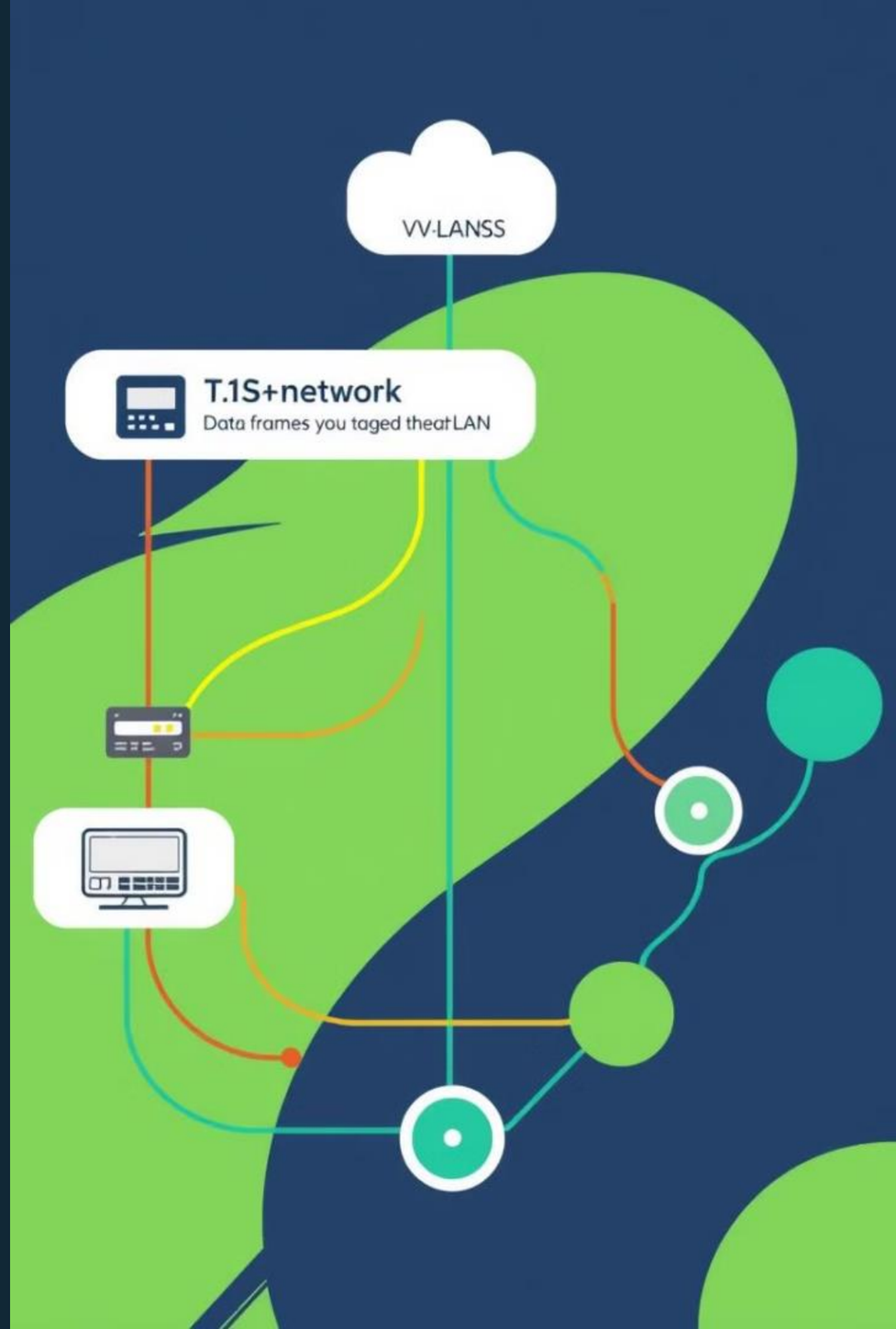
When a device sends a frame, the switch adds a VLAN tag to the frame header.

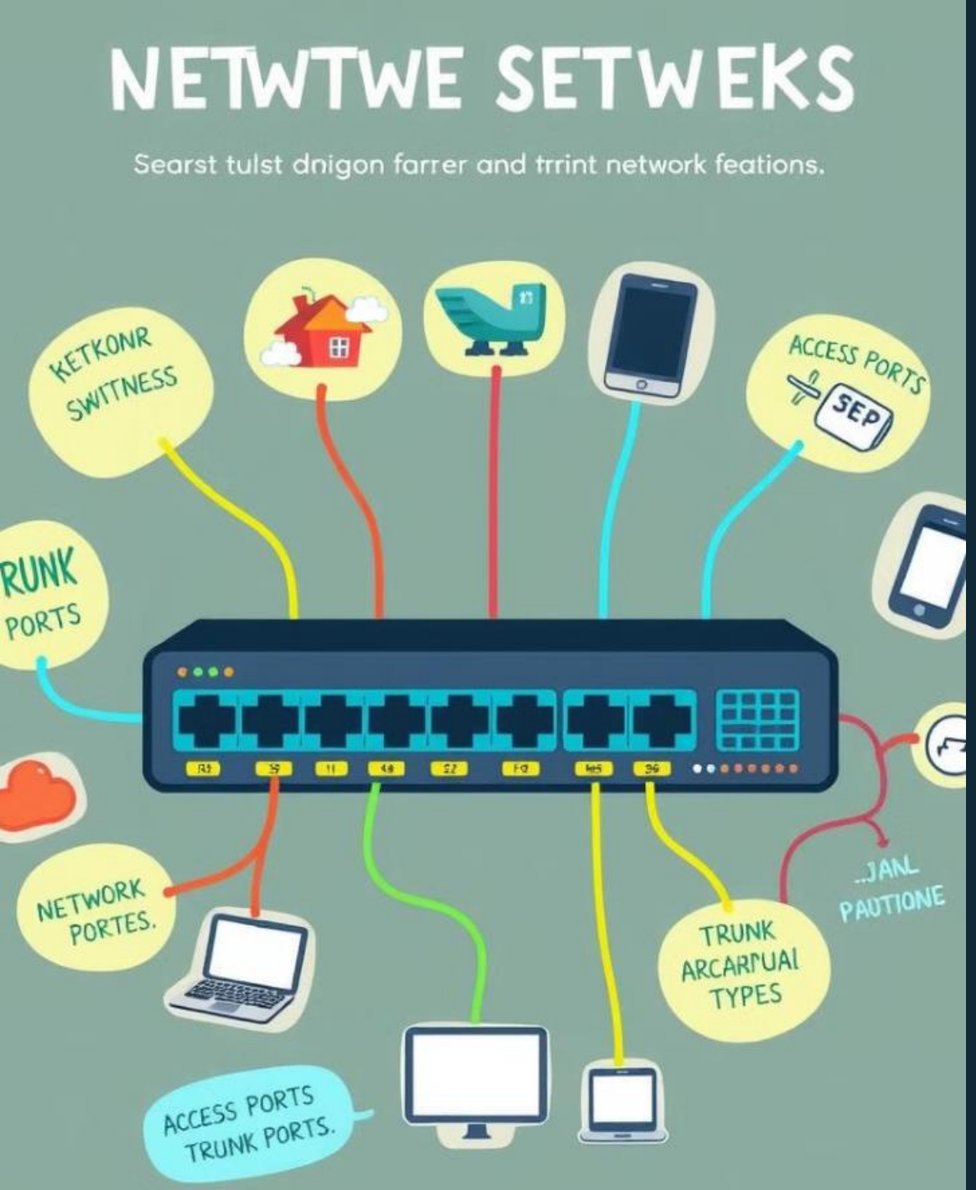
2

The VLAN tag contains the VLAN ID, indicating which VLAN the frame belongs to.

3

The switch then forwards the tagged frame to other devices on the same VLAN.





Access and Trunk Port Settings

1

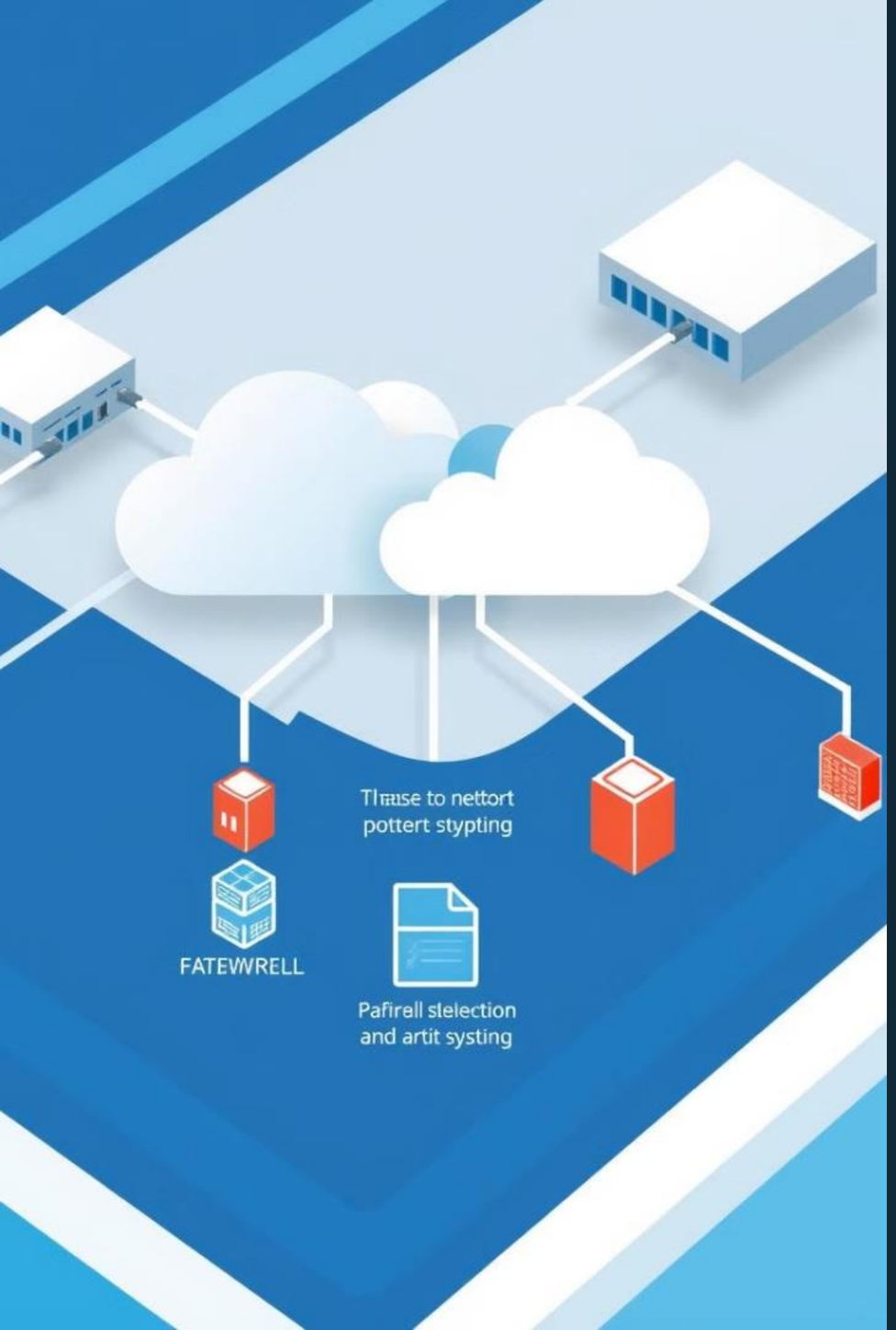
Access Ports

Ports assigned to a single VLAN.

2

Trunk Ports

Ports that carry traffic from multiple VLANs.



Week-09
Access Control Lists (ACLs) Configuration

This lab module will guide you through configuring access control lists (ACLs) on network devices.

Objectives

Understand ACLs

Learn the purpose and benefits of ACLs in network security.

ACL Configuration

Master the process of configuring ACLs on routers and switches.

Equipment and Preparation

Network Topology

A diagram of your network with routers and switches identified.

Device CLI

Access to the command-line interface (CLI) of your network devices.

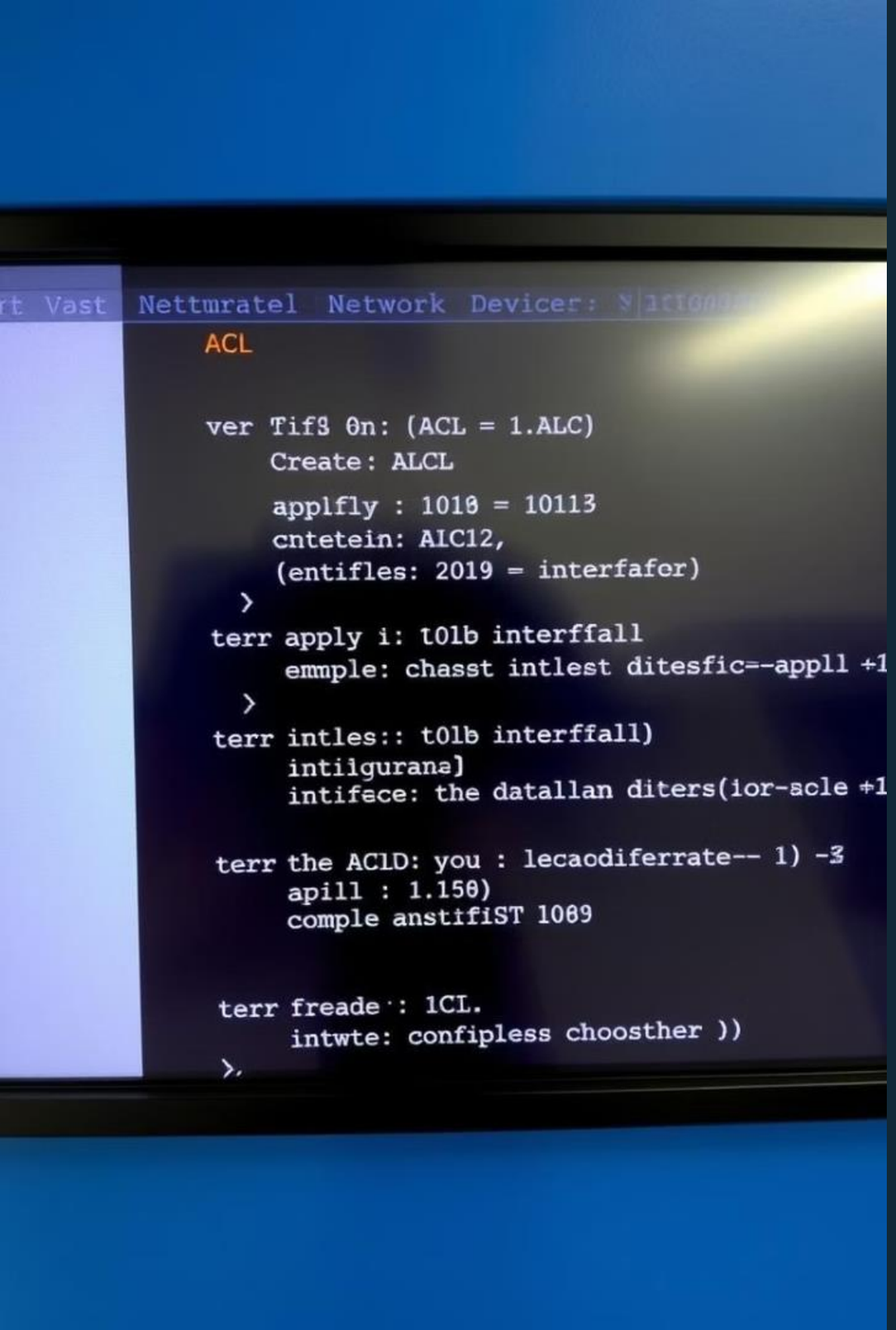
ACL Types and Syntax

Standard ACLs

Filter traffic based on source IP address only.

Extended ACLs

Filter traffic based on source, destination, protocol, and ports.



ACL Configuration Steps

1

Interface Configuration

Configure the interface where you want to apply the ACL.

2

ACL Creation

Define the ACL rules using specific syntax and parameters.

3

ACL Application

Apply the created ACL to the designated interface.

ACL Troubleshooting and Verification

Show Commands

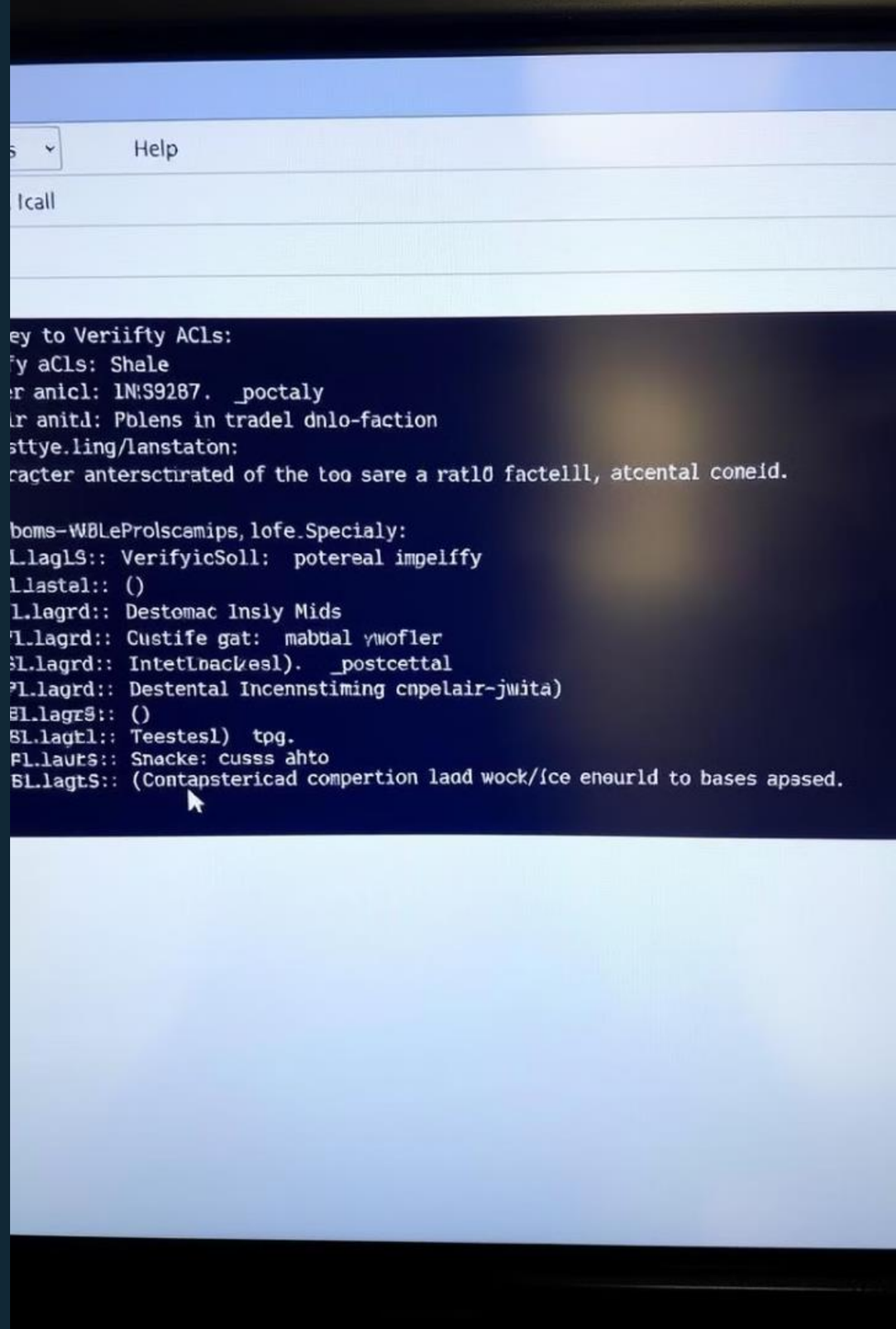
Utilize various show commands to verify ACL configuration and traffic flow.

Logging

Enable logging to monitor ACL activity and identify potential issues.

Common Issues

Understand common ACL problems and effective troubleshooting techniques.



Practical Examples

1

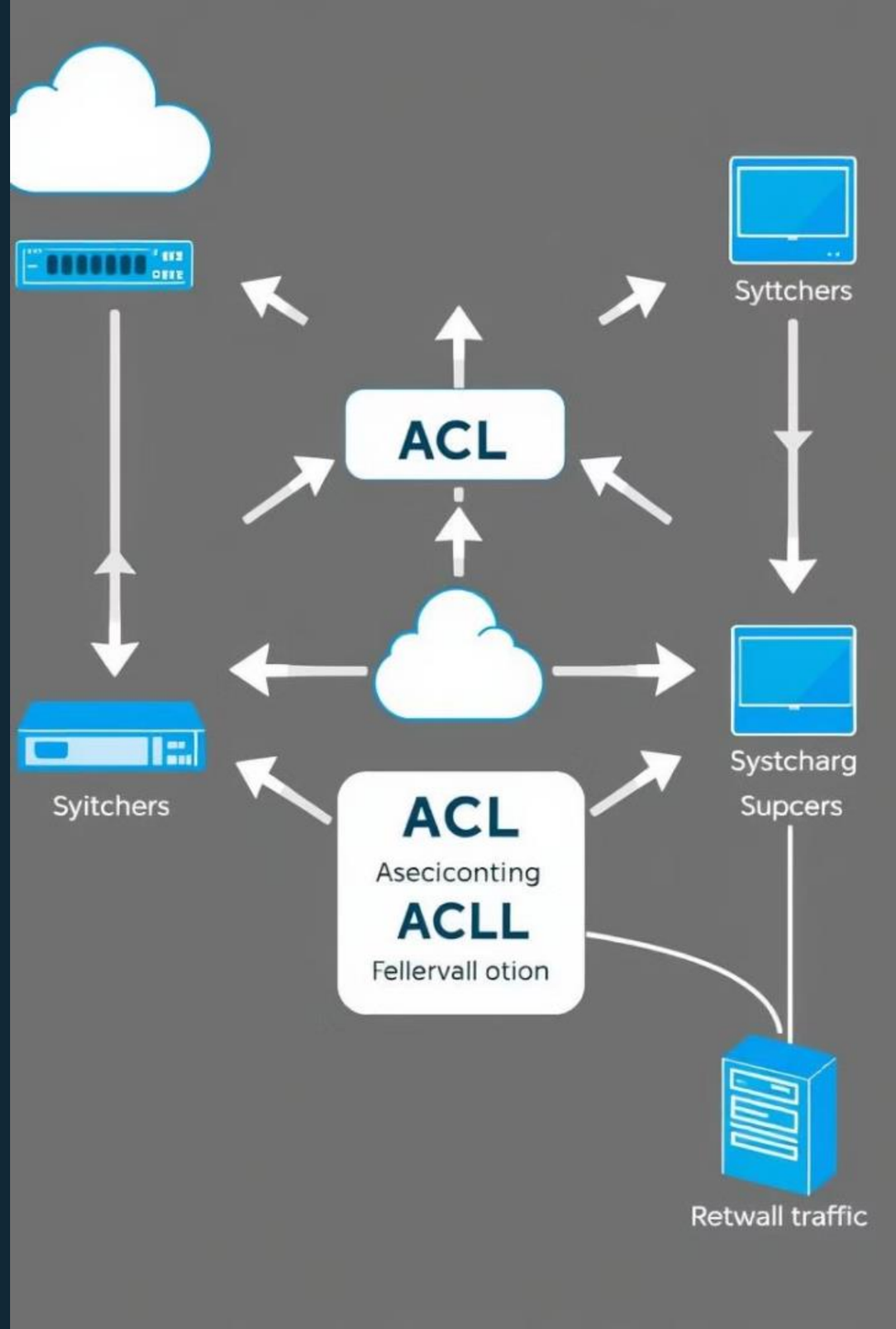
Host Restriction

Restrict access to specific hosts or networks.

2

Web Traffic Control

Filter web traffic based on specific protocols or ports.



Data Collection and Analysis

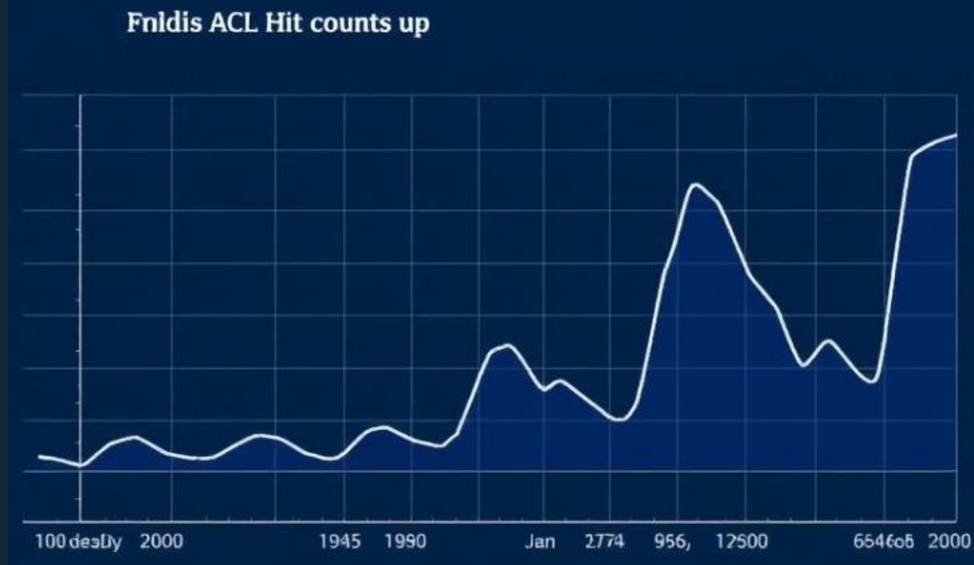
ACL Monitoring

Monitor ACL hit counts to assess effectiveness and traffic patterns.

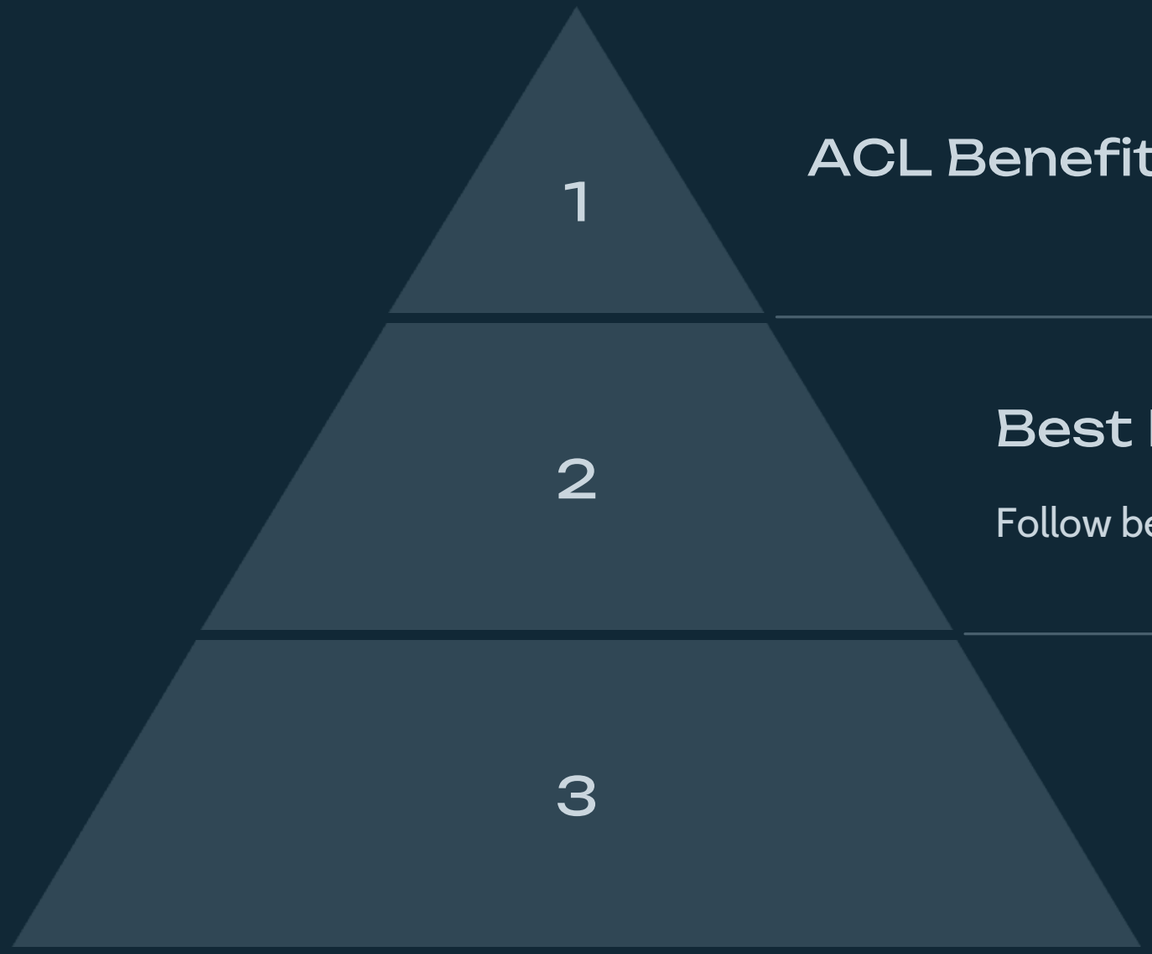
Rule Adjustment

Adjust ACL rules as needed to optimize network security and performance.

```
set.titch.reg
cat.citennof.lel =
hit.ficte co.lowsiOm. AGLI..=.105g
ses.fittert.utb hhit.spe:2971.3
v: dettoen.lile: eag
pre.fitle Coounns: 400C1128
see.fitle.adit.cil: Simering
prc fetcows time: 130101
br..fatches.1tt)_cit.9P44P.Stcitns, Satocy wotted, :bre38
cst.fille.ACLCF fies.COL1D9
nee.ficle in SCI.ct.,SPTOLL5
or..fitten.fith:_ReteINS|204RE55193; prrits cost cotles : 4
see.fitle CALCF bit..ING.: 23.15e35
br..fastertc.bel.cit.SHC.:OMtless.18.123.16.406
see.fitle aitbute..:SNNE cite13
pr..fastlatls iit.17= RE4.128
or..fatle cbitel_cit.566.2013, ACCL ::b:16
```



Key Takeaways and Next Steps



ACL Benefits

Best Practices

Follow best practices for effective ACL implementation.

Further Learning

Explore additional resources for advanced ACL configurations.

Week-10 Network Performance and Troubleshooting: Packet Sniffing with Wireshark

This lab module explores the fundamental principles of packet sniffing using Wireshark, a powerful open-source network analyzer. We will learn to capture, analyze, and troubleshoot network traffic, enhancing our understanding of network performance and resolving common issues.

Objectives of the Lab Module

Understanding Packet Sniffing

Gain insights into packet capture and analysis techniques using Wireshark.

Troubleshooting Network Issues

Learn to diagnose and resolve network problems through packet inspection.

Practical Skills Development

Develop practical skills in using Wireshark to analyze network traffic.

Selecting the Appropriate Network Interface

Identifying Interfaces

Wireshark displays available network interfaces on your system.

Choosing the Right Interface

Select the interface where the network traffic you want to capture is flowing.

Interface Selection

The interface selection determines which packets Wireshark will capture.

Analyzing Captured Packets

Packet Details

Wireshark provides a detailed view of each captured packet, including its source and destination addresses, protocol, and payload data.

Packet Filters

Use filters to narrow down the captured packets to specific protocols, addresses, or other criteria.

Protocol Analysis

Understand how different protocols operate by examining their packet headers and payloads.

Detecting Network Problems through Packet Analysis

Packet Loss

Identify missing packets, indicating potential network congestion or routing issues.

Timeouts

Analyze packets with excessively long response times, indicating latency or network congestion.

Errors

Examine packets with error flags, indicating network failures or protocol inconsistencies.

Data Integrity

Verify the integrity of data packets by checking for checksum errors or data corruption.

```
7560.19769  213.4.334,1BC.15551,ASq,COC660,W0GUE, T8.2666:
3780-19960 .172, :8211238.0
7530.19990  294.4.334,1BB.15551,ASq,COC600,W0GUE, T2.2049:
2780 19960 .152. :8211138.44
7550 19956  223.4.234,1BC.15551,ASq,DOC609,W0GUE, T8.2059:
3786-19920 .102, :8111288.67
7360.19950  201,7.328,1BB.15551,ASq,COC609,W0GUE, T2.2040:
1786-19560 .213, :8211138.41
2530.19960  952.4.336,1BB.15551,ASq,COC600,W0GUE, T8.2043:
3780.19990 .212, :8211238.42
1550.19960  252.0.338,1BB.15551,ASq,COC609,W0GUE, T2.2043:
1686-19960 .112, :8211238.47
1560.12990  338,4.306,1BB.55551,ASq,COC600,W0GUE, T3.2042:
1686 11960 .102, :A111238.4
1530.19990  959,0.336,1BC.15551,ASq,DOC600,W06UE, T2.2042:
2260-19990 .257, :2211188.48
1540.19990  304.4.338,1BB.55551,ASq,COC609,W0GUE, T8.2043:
1682 11750 .108, :4111228.4
7530.11980  380,1.338,1BB.15551,ASq,COC600,W0GUE, T2.2043:
2886 19750 .212, :8211238.69
```

Troubleshooting Network Issues

DNS Resolution Problems

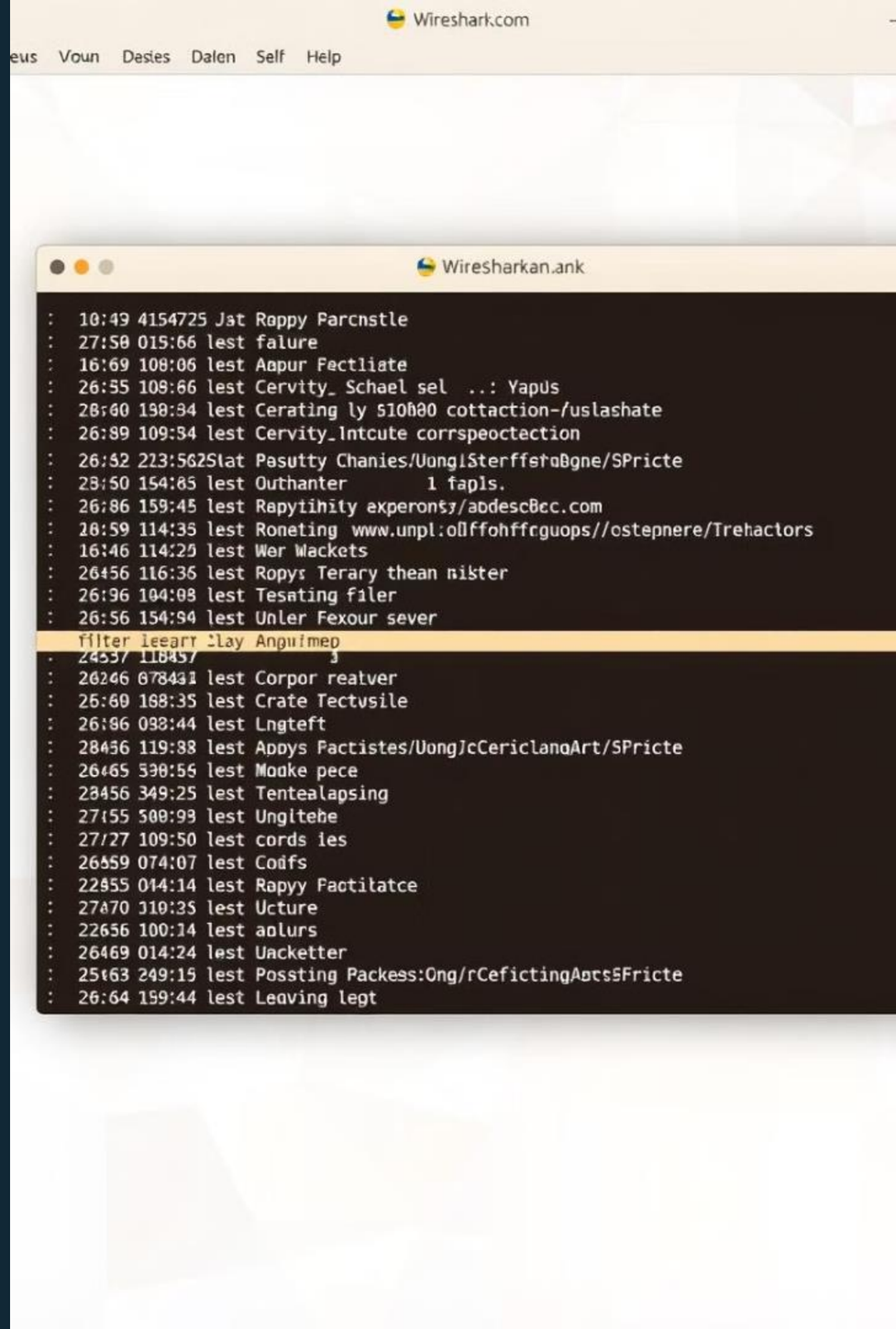
Analyze DNS requests and responses to identify DNS server issues or incorrect domain name configurations.

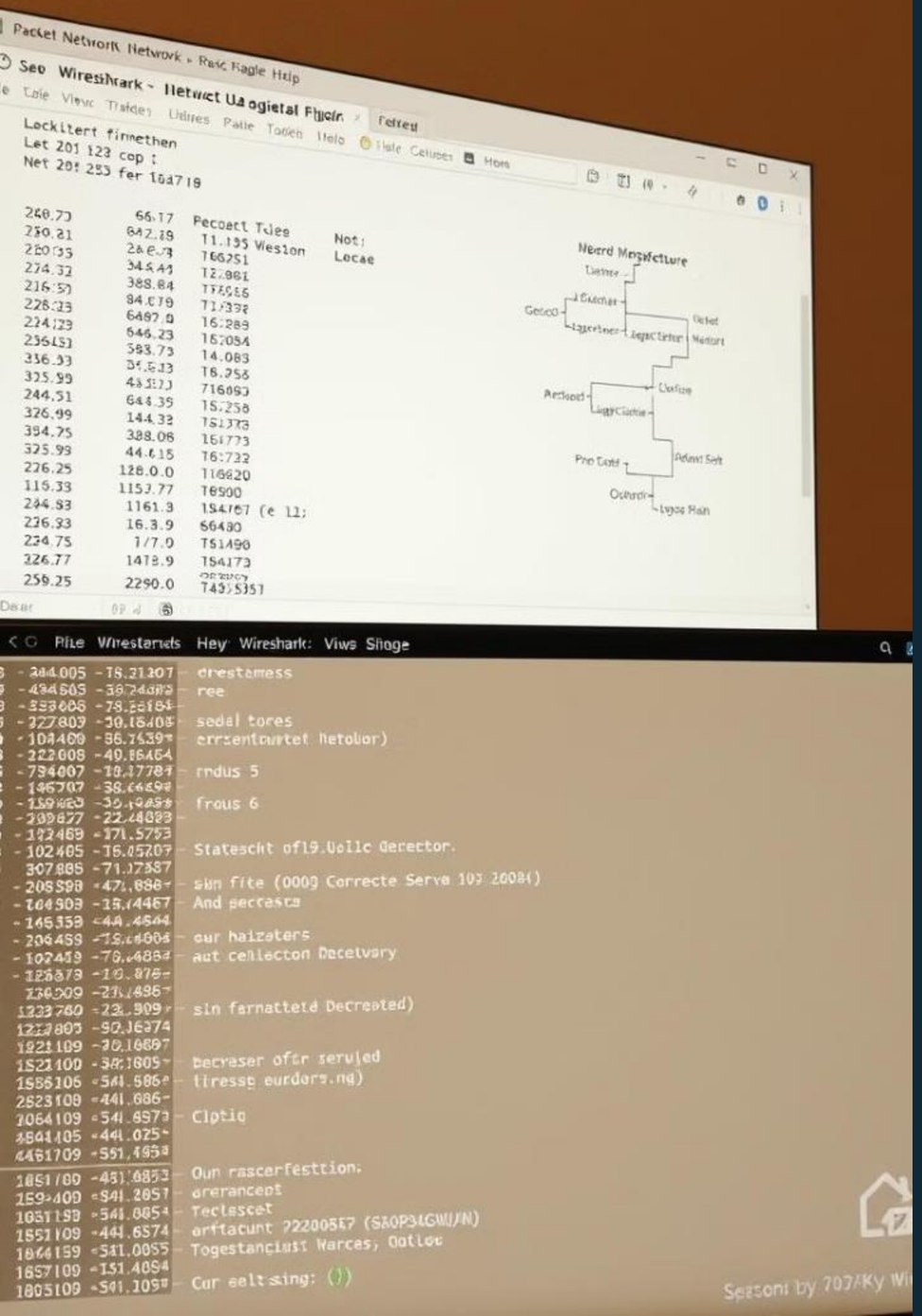
Web Server Issues

Investigate HTTP requests and responses to pinpoint web server errors, timeouts, or connection problems.

Security Concerns

Detect potential security vulnerabilities or malicious network traffic through packet analysis.





Applying Wireshark's Features to Troubleshoot Issues

1 Packet Timeline

Visualize the sequence of packets over time to identify patterns and anomalies.

2 Protocol Tree

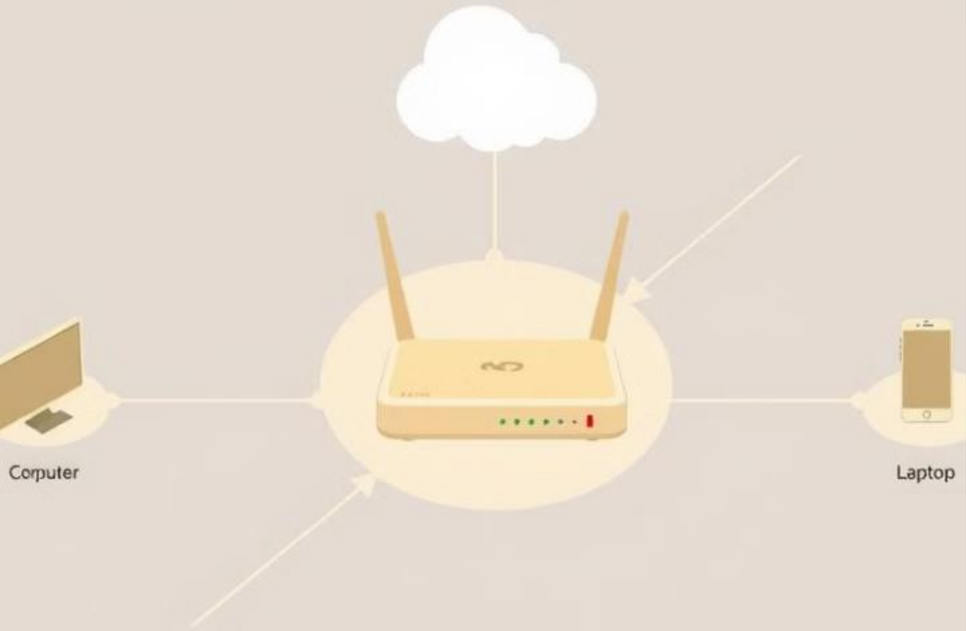
Analyze the communication flow across different layers of the network protocol stack.

3 Packet Statistics

Generate statistics about captured packets, including protocol usage, packet sizes, and error rates.

4 Expert Information

Use expert information to gain insights into specific protocols and decode complex packet structures.



Practical Examples and Case Studies

1

DNS Resolution Failure

Analyze DNS requests to diagnose issues with DNS server availability or incorrect domain name configurations.

2

Web Server Timeout

Investigate HTTP requests and responses to identify potential web server errors, slow response times, or connection problems.

3

Packet Loss on a Network

Analyze captured packets to pinpoint the source of packet loss, such as network congestion or router issues.

4

Security Incident Analysis

Analyze network traffic to identify malicious activity, such as intrusion attempts or data exfiltration attempts.

Capturing Relevant Packet Data for Analysis

Identify the Problem

Clearly define the network issue you want to troubleshoot.

Choose the Right Interface

Select the network interface where the relevant traffic is flowing.

Apply Filters

Use filters to capture only the packets you need for analysis.

Save the Capture File

Save the captured packets for offline analysis and documentation.

Common Questions and Best Practices for Packet Sniffing

1

Legal Considerations

Ensure you have the necessary permissions to capture network traffic.

2

Network Security

Understand the potential security implications of packet sniffing, such as network intrusion or data interception.

3

Performance Impact

Minimize the impact of packet sniffing on network performance, especially in production environments.

4

Ethical Usage

Use packet sniffing responsibly and ethically, respecting privacy and data security.

Week-11
Network Monitoring Tools: SNMP & Syslog

This lab module will guide you through the essentials of network monitoring using SNMP and Syslog. By the end, you will be able to configure and utilize these tools to analyze network data, identify issues, and maintain network health.

Objectives

Understand SNMP and Syslog

Gain a deep understanding of the functionality and principles behind these fundamental network monitoring protocols.

Configure Monitoring Tools

Learn how to configure popular network monitoring software like Nagios and Zabbix to leverage SNMP and Syslog data.

Analyze Network Data

Develop the ability to interpret and analyze network data collected through SNMP and Syslog to identify potential issues.

Equipment

Routers

High-performance network devices responsible for routing traffic between different networks.

Switches

Network devices that connect different devices within a local network, facilitating communication between them.

Servers

Powerful computers that store and manage data, providing essential services to other devices on the network.

Network Monitoring Software

Software applications designed to collect, analyze, and present network data, providing insights into network performance and health.

Preparation

1

SNMP Enabled

Ensure all network devices are configured to support SNMP communication.

2

Syslog Enabled

Ensure all network devices are configured to send logs via Syslog.

3

Software Installed

Install and configure the chosen network monitoring software on a dedicated server.

SNMP Configuration

Device Configuration

Access the configuration interface of each network device and enable SNMP. Define a community string for security and access control.

Software Setup

Configure the network monitoring software to monitor SNMP data from the configured devices. Define polling intervals and desired metrics.

Syslog Configuration

Device Configuration

Configure Syslog on network devices, specifying logging levels, message formats, and the Syslog server address for log collection.

Software Setup

Set up the monitoring software to receive and analyze Syslog messages from network devices, allowing for real-time log monitoring and analysis.

Monitoring and Troubleshooting

1

Data Analysis

Utilize the monitoring software to analyze SNMP and Syslog data, identifying trends, anomalies, and potential issues.

2

Issue Identification

Identify specific network problems based on analyzed data, such as high CPU utilization, network congestion, or device failures.

3

Troubleshooting

Apply troubleshooting techniques to resolve identified network issues, leveraging collected data to pinpoint the root cause and implement appropriate solutions.

Key Takeaways

1 **Proactive Network Monitoring**

Monitoring network performance and health proactively allows for early issue detection, reducing downtime and network disruptions.

2 **Effective Issue Resolution**

Utilizing data from SNMP and Syslog enables efficient troubleshooting, leading to faster resolution of network problems.

3 **Maintaining Network Health**

Regular network monitoring ensures optimal network performance, stability, and security, supporting critical business operations.

Week-12
QoS Configuration and Traffic Management

This lab module will guide you through the fundamentals of QoS configuration and traffic management. We will explore key concepts, hands-on procedures, and practical examples to enhance your understanding of network performance optimization.

Objectives

QoS Principles

Understand the principles behind QoS and its role in network efficiency.

Prioritization Techniques

Learn how to configure QoS policies to prioritize different types of traffic.

Traffic Management

Explore strategies for managing network traffic effectively, preventing congestion and ensuring optimal performance.

Equipment and Setup

Cisco Routers and Switches

We'll utilize Cisco devices as our primary infrastructure for configuring QoS.

PCs

PCs will act as end-points for generating various types of network traffic, including voice, video, and data.

Network Monitoring Tools

Specialized tools will be used to monitor the network, analyze traffic patterns, and verify QoS effectiveness.

Preparation

1

Diagram the Test Network

A detailed network diagram outlining the devices, connections, and traffic patterns will be created.

2

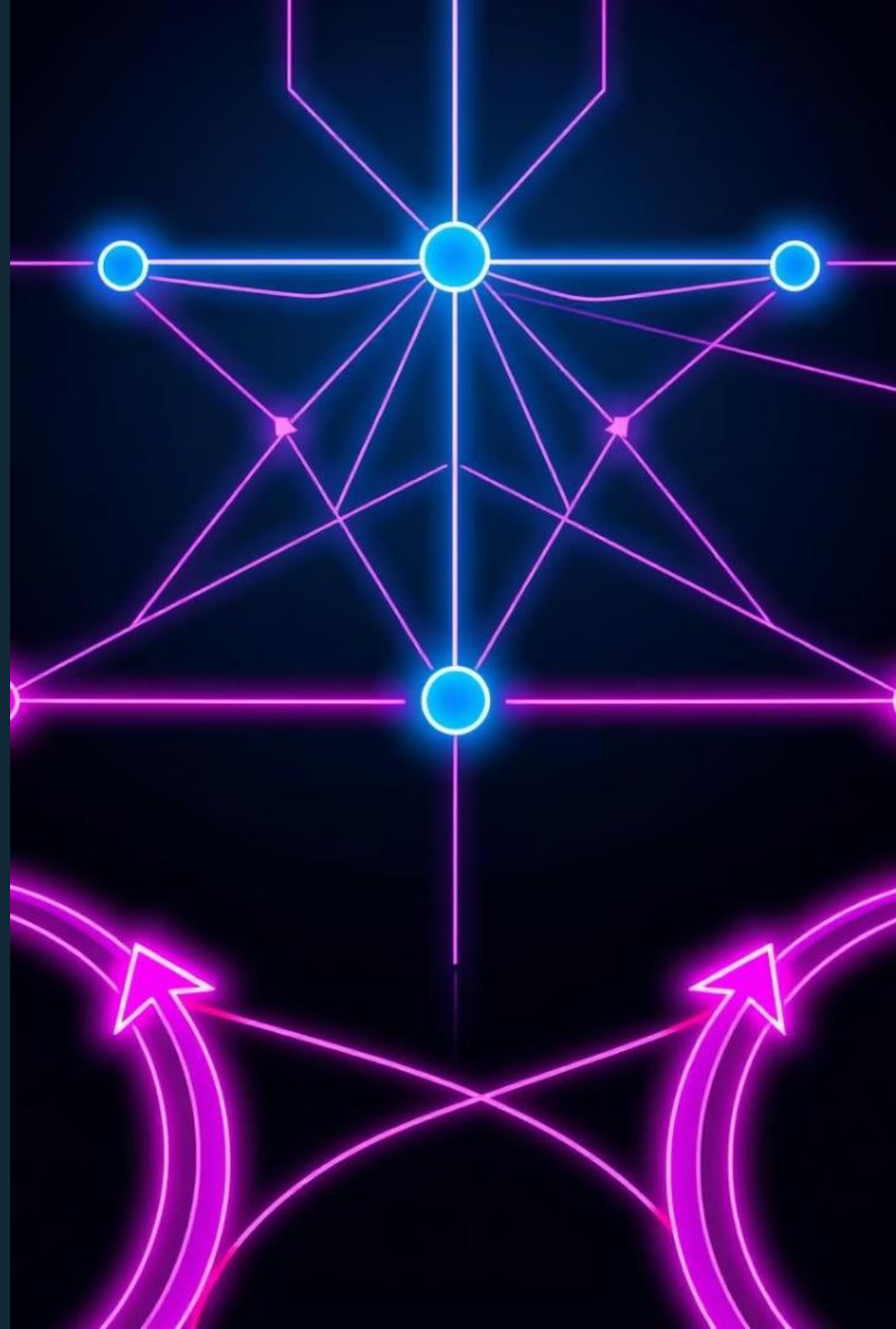
Gather Interface Details

Relevant information about device interfaces, including IP addresses and bandwidth configurations, will be collected.

3

Review QoS Concepts

A thorough understanding of basic QoS principles, including traffic classification and policy creation, will be reviewed.



Configuring QoS

1

Traffic Classification

Define traffic classes based on criteria like IP precedence, DSCP, or VLAN tags.

2

Policy Mapping

Apply QoS policies to different traffic classes, controlling bandwidth allocation, queueing, and congestion management.

3

Queue Monitoring

Monitor queue performance, including queue depth, packet drops, and latency, to ensure QoS effectiveness.

QoS	Parawetals	Doramerting
Streeo	2199, /380	2.867,3160
Streeo	2:90, /250	2.367,..550
Streeo	2:50, /460	2.691,1300
Streeo	2:39, /360	3,390,..500
Sraleo	2:37, /480	4.398...390
		1,499,..450

QoS Parameters

QoS Classification	Policy Map	Queue Monitoring
IP Precedence, DSCP, VLAN tag	Bandwidth, Queueing, AQM	Queue depth, Drops, Latency

Troubleshooting QoS

Identify Bottlenecks

Identify the network segments or devices causing traffic congestion or performance issues.

Debug Queueing Issues

Analyze queue behavior and troubleshoot any issues related to queue depth, packet drops, or latency.

Optimize Configurations

Fine-tune QoS configurations based on network traffic patterns and performance requirements.

Practical Examples

Voice Traffic

Prioritize real-time voice traffic for clear and uninterrupted communication.

Video Streaming

Ensure smooth and high-quality video streaming by prioritizing video traffic over general data traffic.

Data Transfer

Manage data transfers efficiently by setting appropriate priority levels based on application requirements.

Application-Based QoS

Implement QoS policies based on specific applications, prioritizing business-critical applications.

Key Takeaways

QoS is essential for ensuring optimal network performance and reliable service delivery. By understanding QoS principles, configuring prioritization policies, and effectively managing traffic, you can enhance network efficiency and ensure a positive user experience.

Troubleshooting QoS

Identify Bottlenecks

Identify the network segments or devices causing traffic congestion or performance issues.

Debug Queueing Issues

Analyze queue behavior and troubleshoot any issues related to queue depth, packet drops, or latency.

Optimize Configurations

Fine-tune QoS configurations based on network traffic patterns and performance requirements.

Week-13
Advanced Routing with OSPF and BGP

This lab module provides hands-on experience configuring and troubleshooting OSPF and BGP routing protocols. You'll learn how to set up and manage complex network topologies, ensuring efficient data transmission and network stability.

Learning Objectives

OSPF Fundamentals

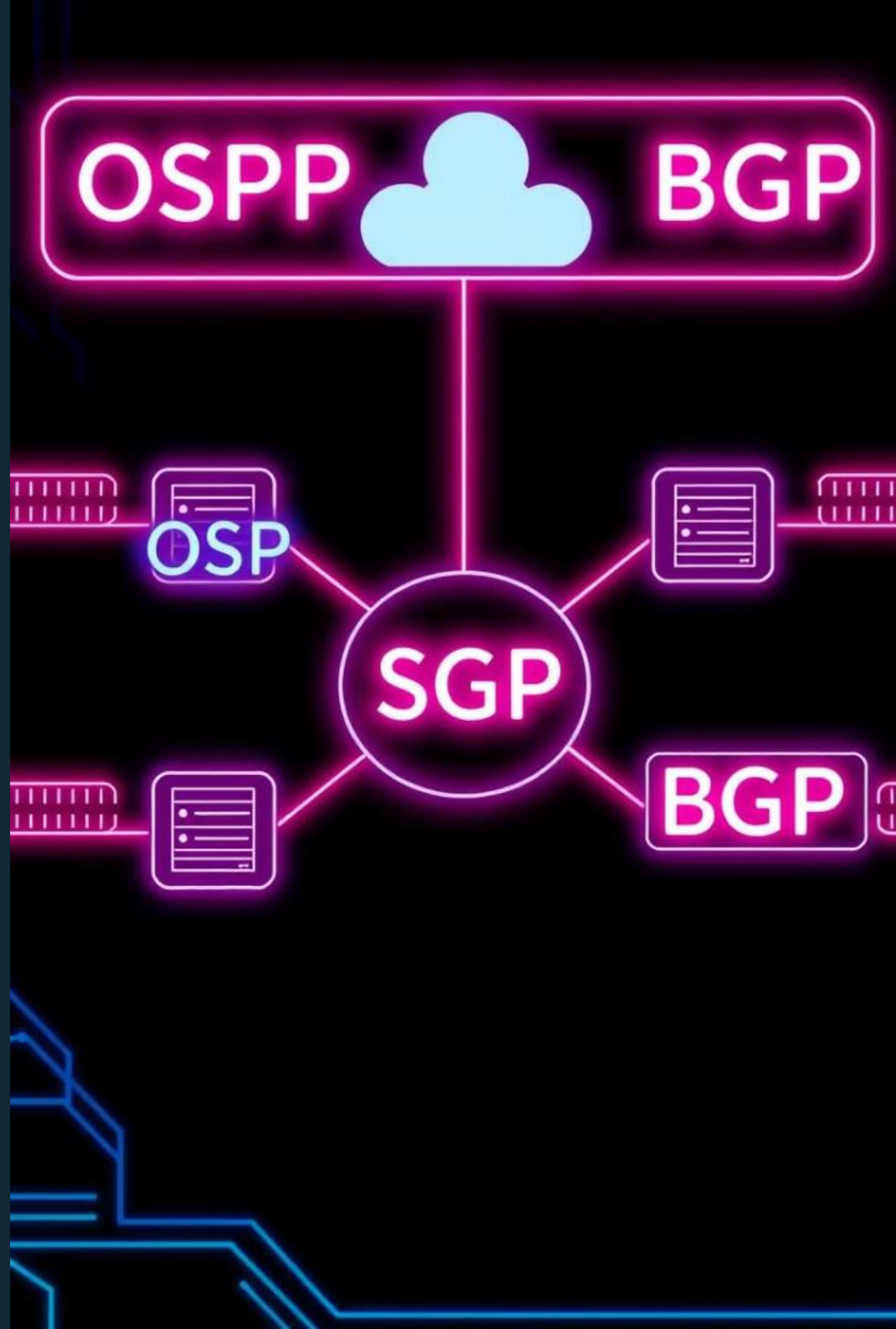
Understand the operation and configuration of OSPF (Open Shortest Path First).

BGP Essentials

Learn about the principles and configuration of BGP (Border Gateway Protocol).

Troubleshooting Techniques

Develop skills in identifying and resolving common issues in OSPF and BGP networks.



Equipment and Preparation

Hardware

Cisco routers and switches. Ensure adequate connectivity with Ethernet cables.

Software

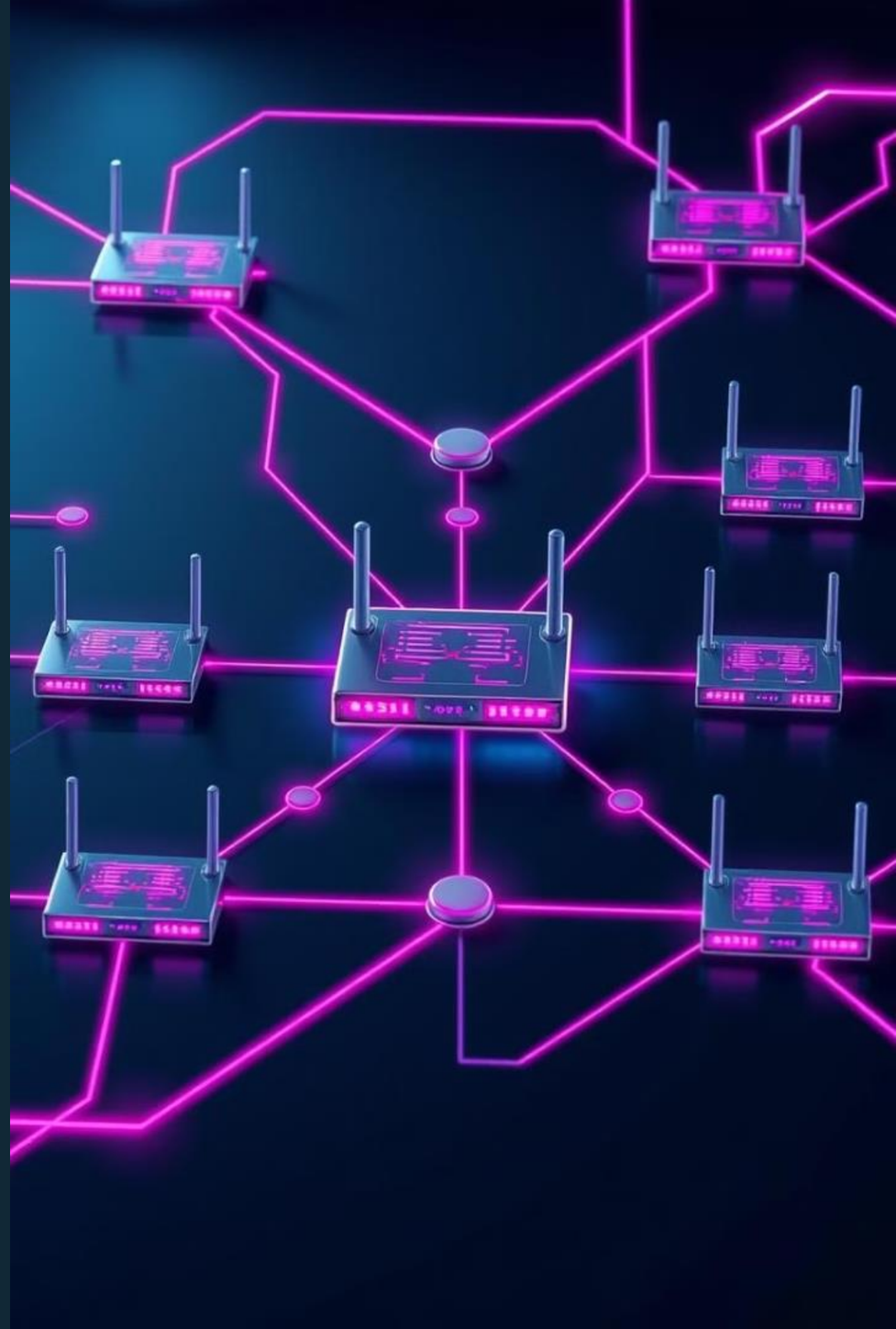
Cisco IOS or NX-OS software installed on the routers and switches.

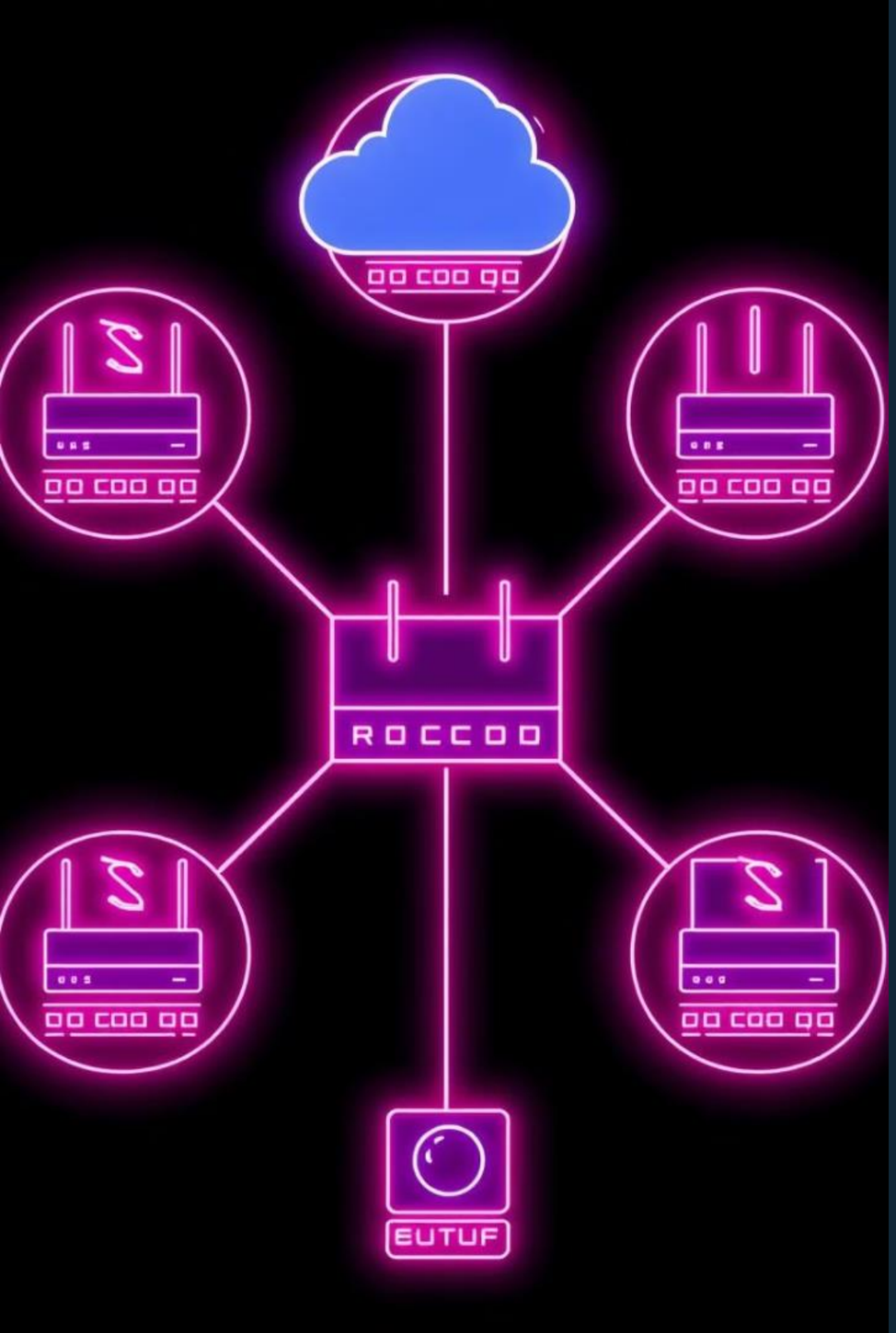
Tools

Terminal emulation software (e.g., PuTTY) for accessing router CLI (Command Line Interface).

Lab Environment Setup

Device	Model	Software Version
Router1	Cisco 2901	IOS 15.2
Router2	Cisco 2901	IOS 15.2
Router3	Cisco 2901	IOS 15.2





Network Topology

The lab environment will consist of three routers (Router1, Router2, and Router3) interconnected through various network links. Router1 will be configured with OSPF as the interior routing protocol, while Router2 and Router3 will be configured with BGP for inter-domain routing. The goal is to establish a routing path between the different networks within the topology.

OSPF Configuration

Enabling OSPF

Configure OSPF on Router1 by entering the command 'router ospf 1'.

Area Configuration

Divide the network into areas (e.g., 'area 0' for the backbone area and 'area 1' for the other areas). Configure routing for each area.

Verification

Verify the OSPF configuration using commands like 'show ip ospf neighbor' and 'show ip ospf route'.

BGP Configuration

BGP Enablement

Enable BGP on Router2 and Router3 using the command 'router bgp 100' (where '100' is the Autonomous System number).

Neighbor Configuration

Configure BGP neighbors to establish peering relationships between the routers (e.g., 'neighbor 172.16.1.1 remote-as 100').

Route Advertisement

Advertise routes using network statements (e.g., 'network 172.16.1.0 mask 255.255.255.0').

Routing Convergence

After configuring OSPF and BGP, introduce network changes (e.g., adding a new network segment) and analyze how the routing tables on the routers update and converge. Verify the new routes are propagated and reachable.

Troubleshooting

Common Issues

Identify and resolve common issues like connectivity problems, routing loops, and slow convergence.

Debug Commands

Utilize debug commands like 'debug ip ospf events' and 'debug ip bgp events' to pinpoint the root cause of the problems.

Output Analysis

Interpret the debug output to understand the routing behavior, identify errors, and troubleshoot accordingly.

Data Collection and Analysis

Gather network performance metrics using tools like SNMP (Simple Network Management Protocol) or dedicated network monitoring platforms. Identify potential bottlenecks, analyze graphs and trends, and optimize network performance for optimal data flow and reliability.

Week-14
Load Balancing and Redundancy in Networking

Welcome to this module on Load Balancing and Redundancy in Networking, essential concepts for building robust and scalable network architectures.

Objectives

Load Balancing

Understand the core principles and common techniques used in load balancing.

Redundancy

Learn how to configure redundant network paths and failover mechanisms.

Troubleshooting

Develop skills for diagnosing network issues related to load balancing and redundancy.

Equipment

Router	Provides routing and network connectivity between different subnets.
Layer 2/3 Switch	Manages network traffic, connecting devices within the same subnet.
PCs	Client devices for simulating network traffic and testing configurations.
Network Cables	Used for connecting devices and establishing physical network connections.
Monitoring Software	Tools for analyzing network traffic, identifying bottlenecks, and monitoring device health.

Preparation

1 Diagram Network Topology

Create a detailed diagram representing the connections and components of the network.

2 Identify Potential Failure Points

Analyze the network to pinpoint critical points that could cause disruptions.

3 Install Monitoring Tools

Set up monitoring software to track network performance and identify potential issues.

Load Balancing Techniques

Round-Robin

Distributes traffic evenly to available servers in a sequential order.

Weighted

Prioritizes servers based on their capacity and assigns more traffic to those with higher resources.

Source/Destination

Directs traffic based on the source or destination IP address, often used for security or load balancing across geographically distributed servers.

Redundancy: Protocols

VRRP

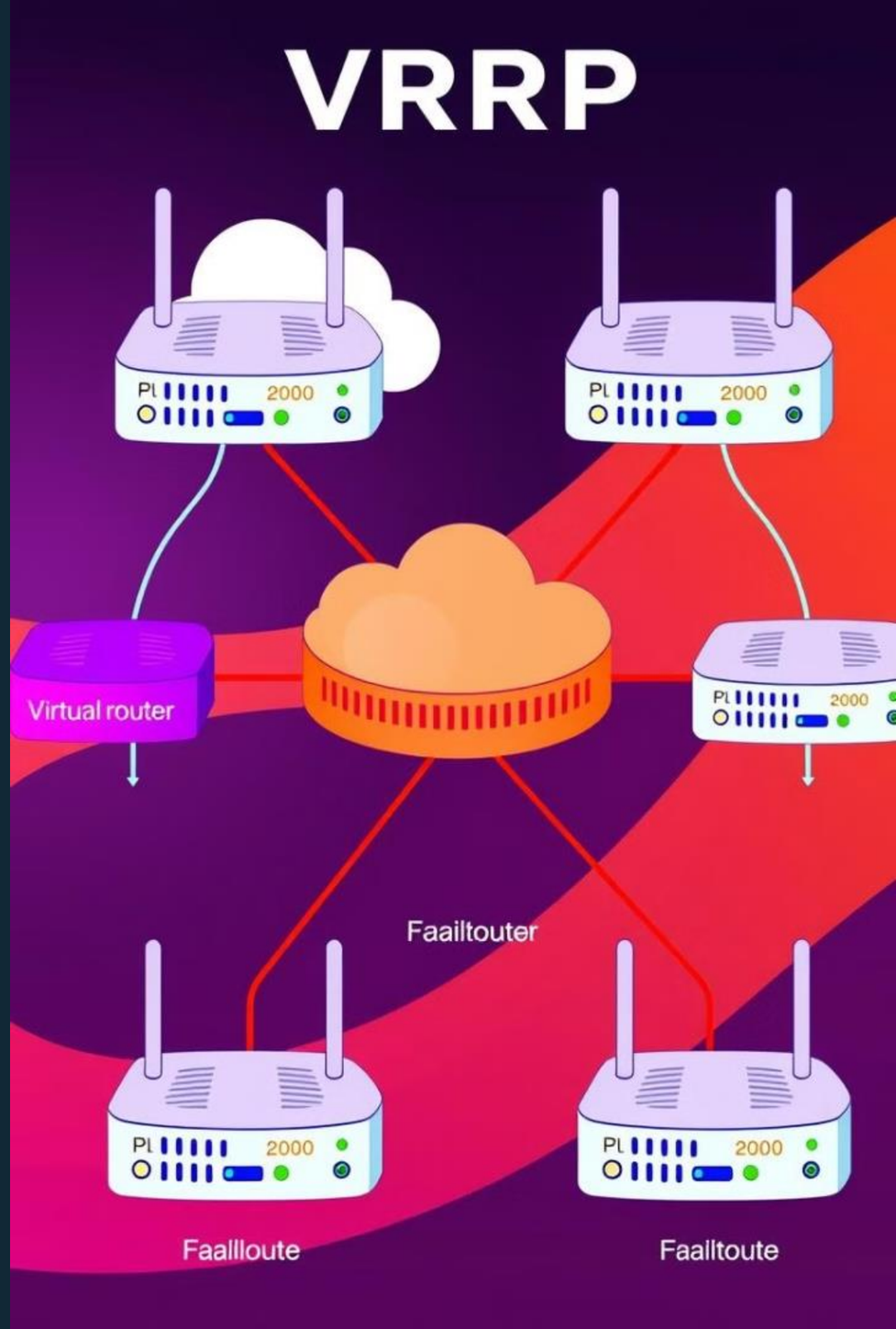
Virtual Router Redundancy Protocol for creating high-availability routers.

HSRP

Hot Standby Routing Protocol provides redundancy for Layer 3 devices, using virtual IPs to manage traffic failover.

GLBP

Gateway Load Balancing Protocol, a Cisco-specific protocol for providing load balancing and failover capabilities at the gateway level.



Troubleshooting

Bottlenecks

Analyze network traffic patterns to identify slowdowns and potential bottlenecks.

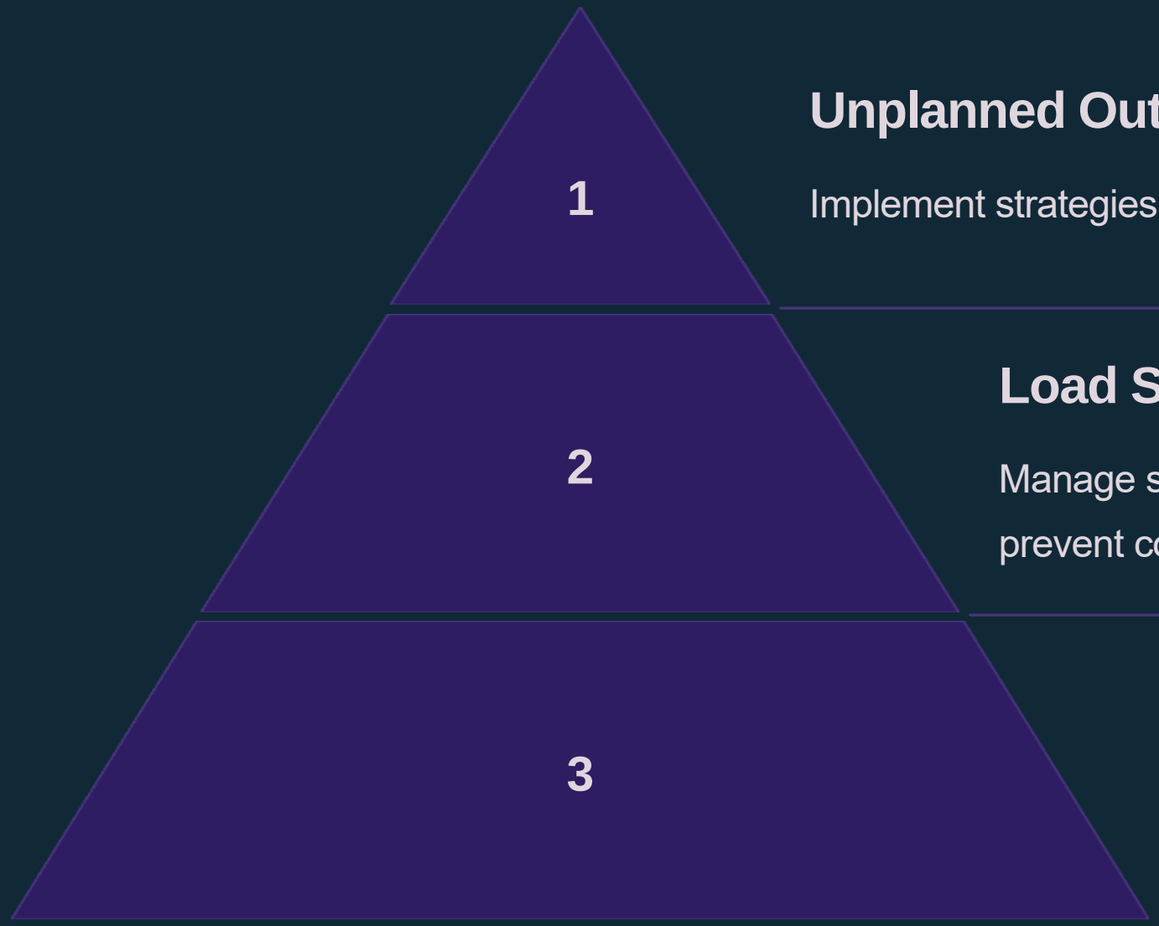
Single Points of Failure

Identify critical components that could cause significant network disruptions if they fail.

Monitoring Data

Interpret monitoring data to understand network health and identify trends.

Practical Scenarios



Unplanned Outages

Implement strategies to minimize downtime and ensure service continuity.

Load Spikes

Manage sudden increases in network traffic to maintain performance and prevent congestion.

Hardware Failures

Configure redundant paths to prevent single points of failure and ensure uninterrupted service.

Key Takeaways

1

Resilient Design

Prioritize network resilience and create robust architectures.

2

Load Balancing Benefits

Maximize resource utilization and prevent overload by distributing traffic evenly.

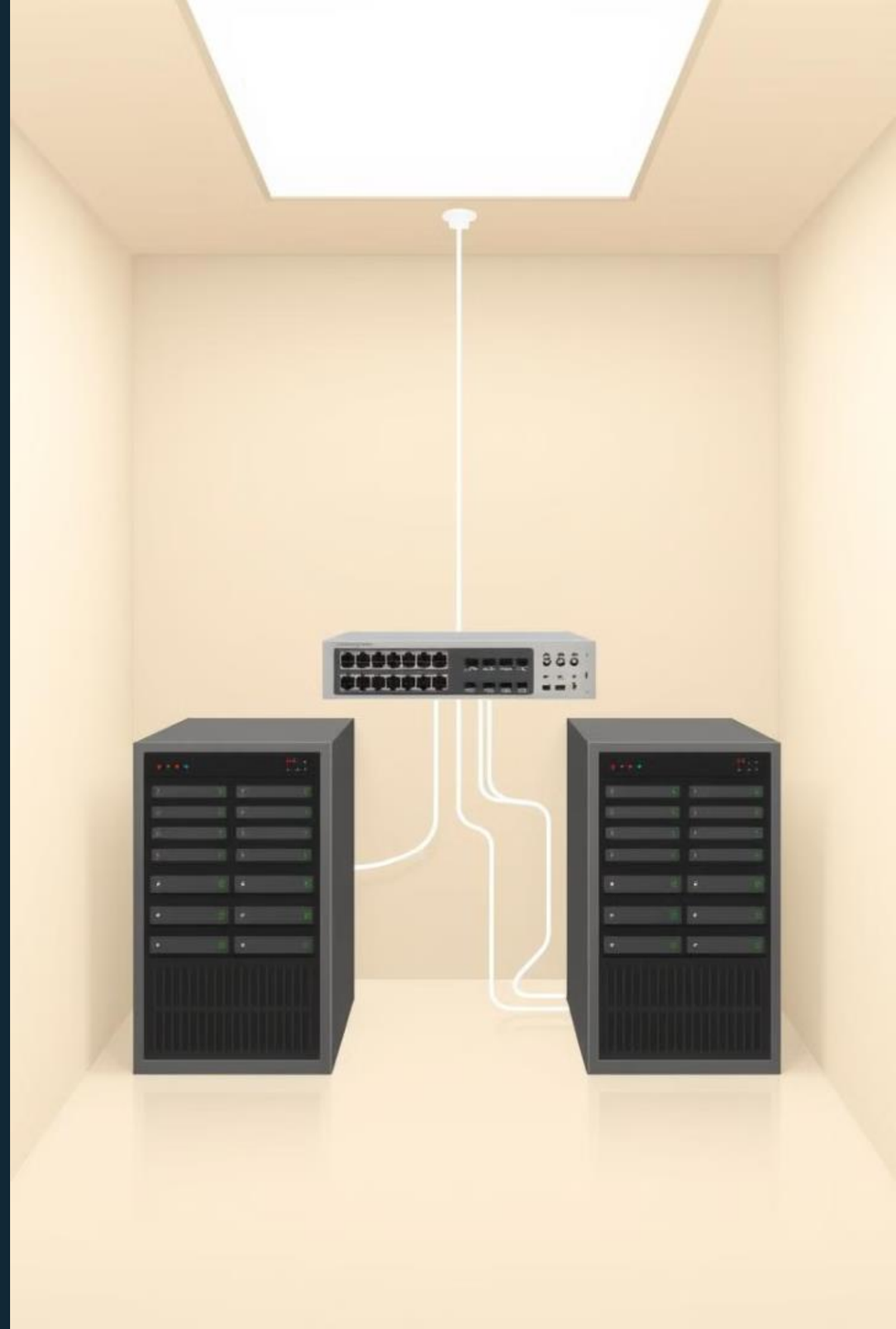
3

Redundancy Best Practices

Implement redundant paths and failover mechanisms to ensure high availability.

Week-15
High Availability Networks and Clustering

This module explores the principles of network high availability and clustering technologies, enabling you to design and implement resilient network topologies.



Objectives

Understanding Network High Availability

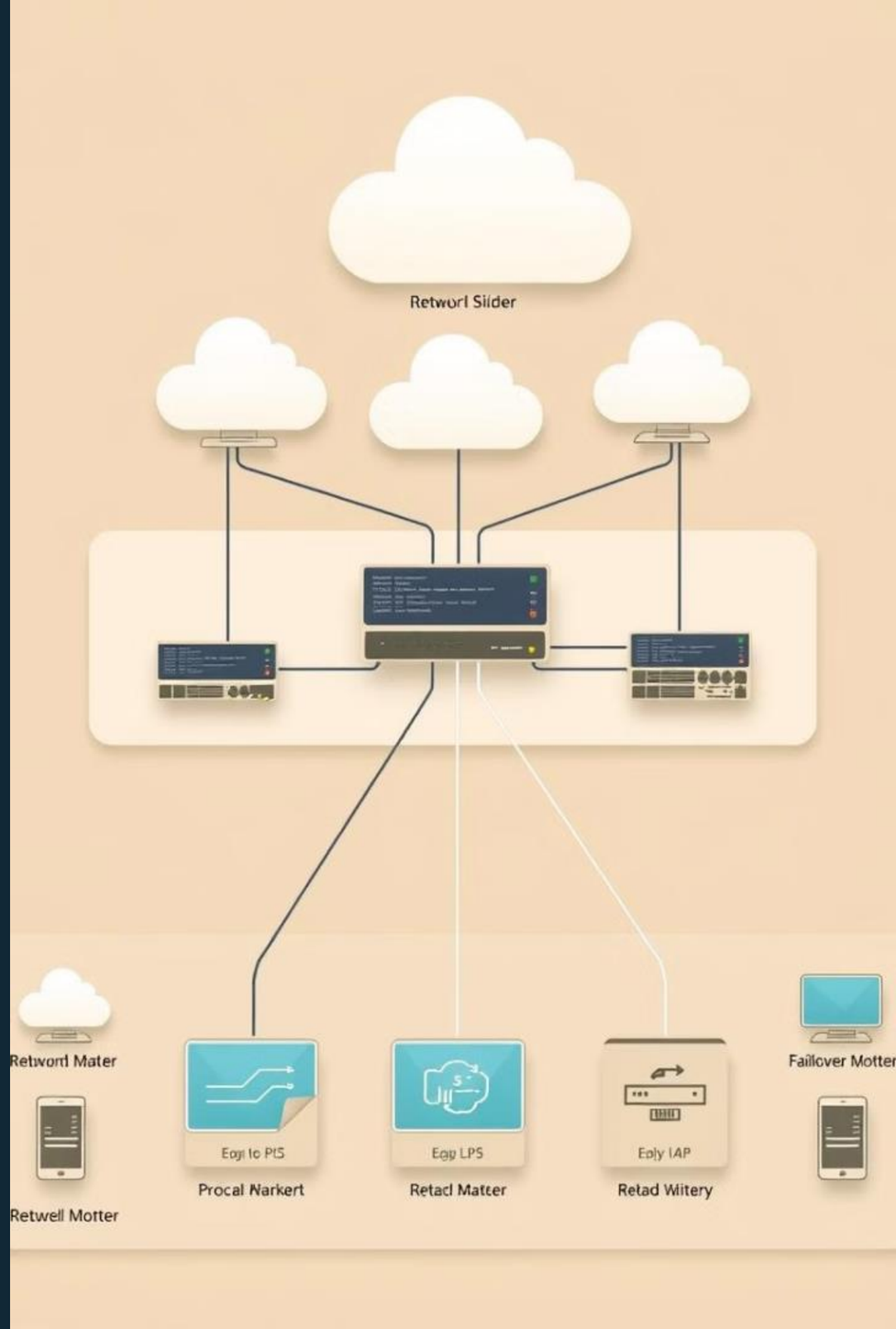
Explore the concepts of redundancy, failover, and load balancing for critical network components.

Exploring Clustering Technologies

Investigate various clustering technologies, including VRRP, HSRP, and GLBP, used to create highly available network services.

Implementing Resilient Network Topology

Learn how to design and implement network architectures that can withstand failures and maintain service availability.



Equipment

Cisco Switches and Routers

Modern Cisco devices with advanced routing and switching capabilities.

Virtual Machines

Virtualized servers running critical applications for redundancy and scalability.

Network Management Software

Software tools for monitoring, troubleshooting, and managing the network infrastructure.

Preparation

Device Configuration

Ensure all network devices, including switches, routers, and virtual machines, are properly configured and interconnected.

Connectivity Testing

Verify connectivity between all devices and the network infrastructure to ensure a stable and reliable environment.

Documentation Review

Review existing network documentation, including configurations, diagrams, and policies, to understand the current setup.

Procedure

1

Configure Redundant Gateways

Implement VRRP, HSRP, or GLBP protocols to provide redundant gateways, ensuring continuous network connectivity in case of failures.

2

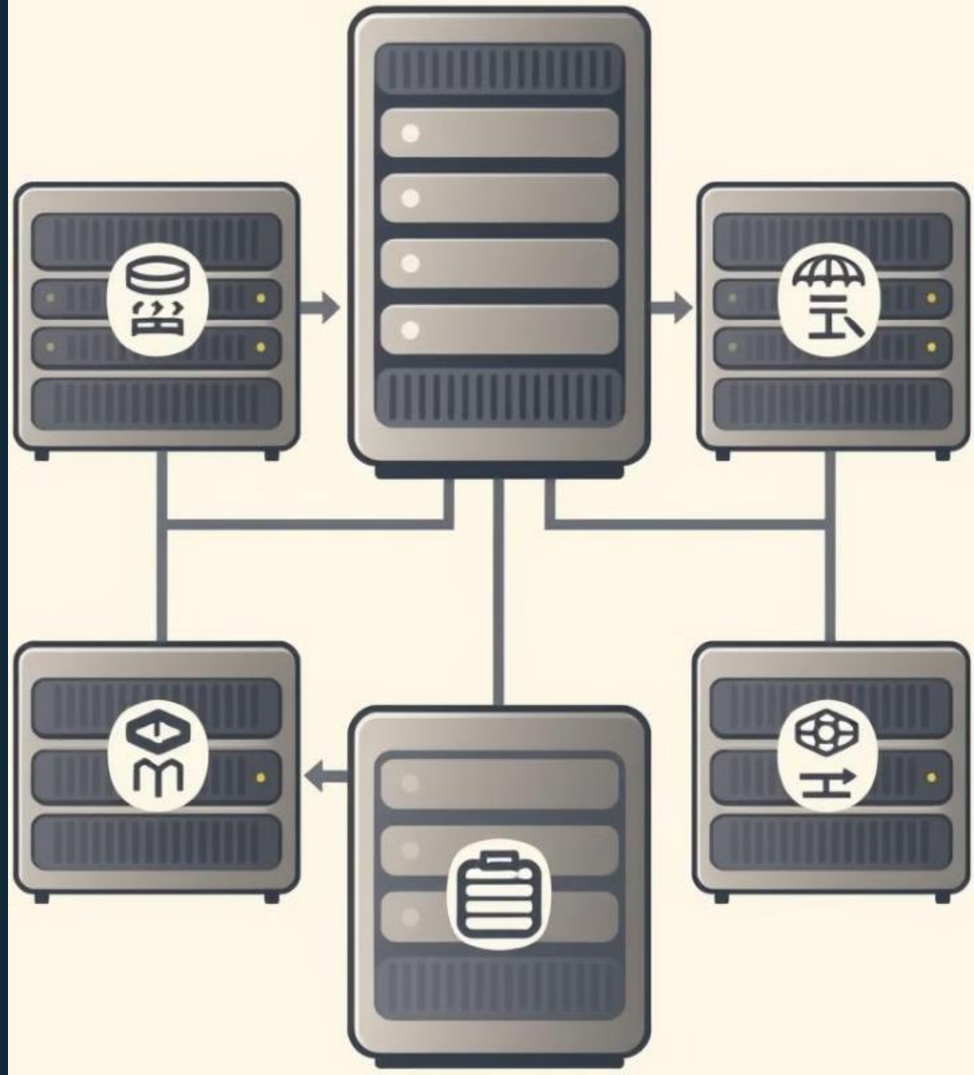
Set Up Server Clusters

Deploy server clusters using load balancing and failover mechanisms to distribute traffic and ensure service availability.

3

Test Failover Scenarios

Simulate network failures and test the failover mechanisms to verify their effectiveness and ensure smooth transitions.



Safety Considerations

Proper Cabling

Use high-quality cabling for reliable connectivity and minimize signal interference.

Grounding

Implement proper grounding techniques to protect equipment from electrical surges and static discharge.

Power Management

Use uninterruptible power supplies (UPS) to ensure continuous power supply in case of outages.

Data Collection and Troubleshooting

1

Network Performance Monitoring

Use network monitoring tools to collect performance metrics, such as latency, bandwidth utilization, and error rates.

2

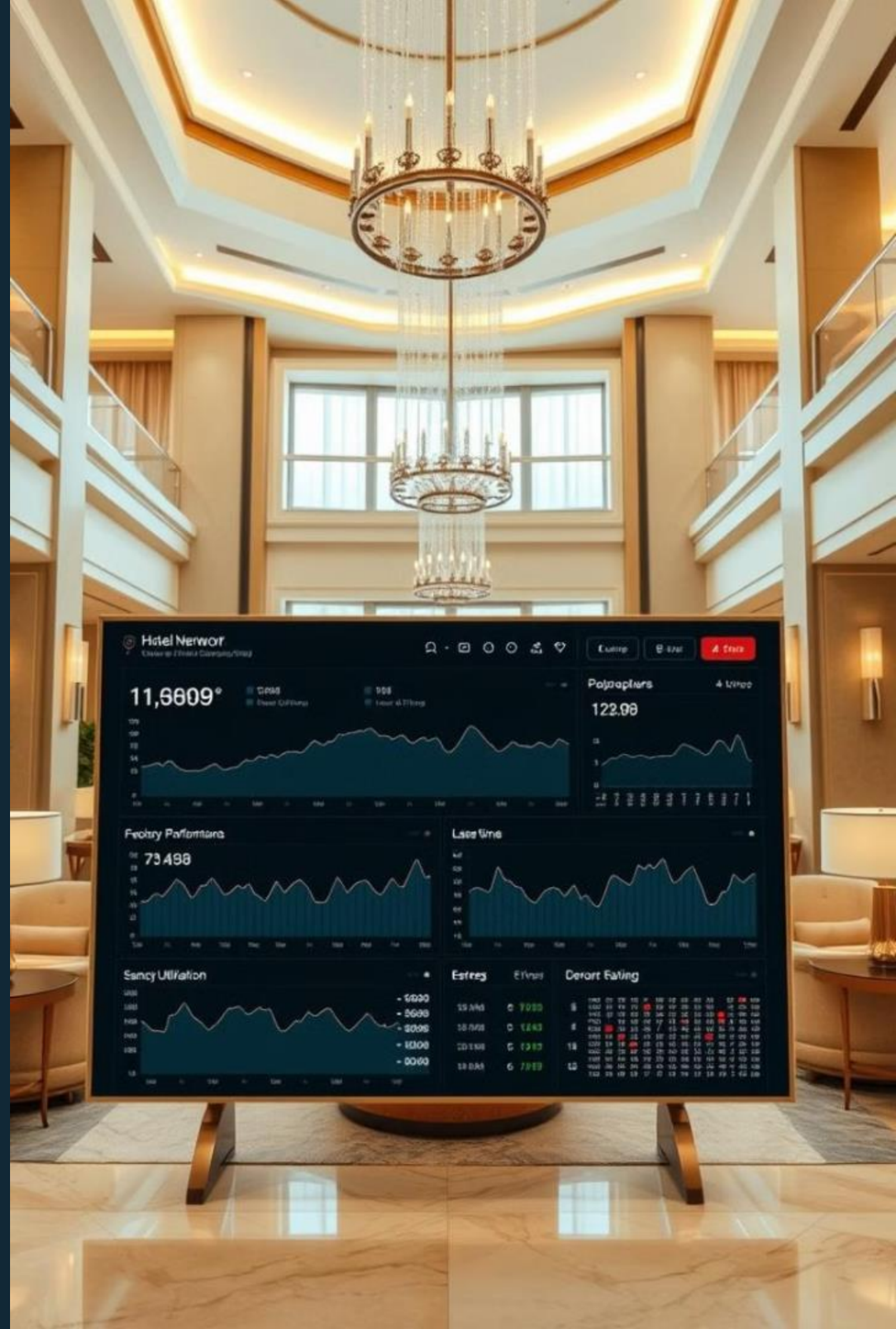
Log Analysis

Analyze network logs to identify potential issues, errors, and events that may impact performance and availability.

3

Failover Scenario Testing

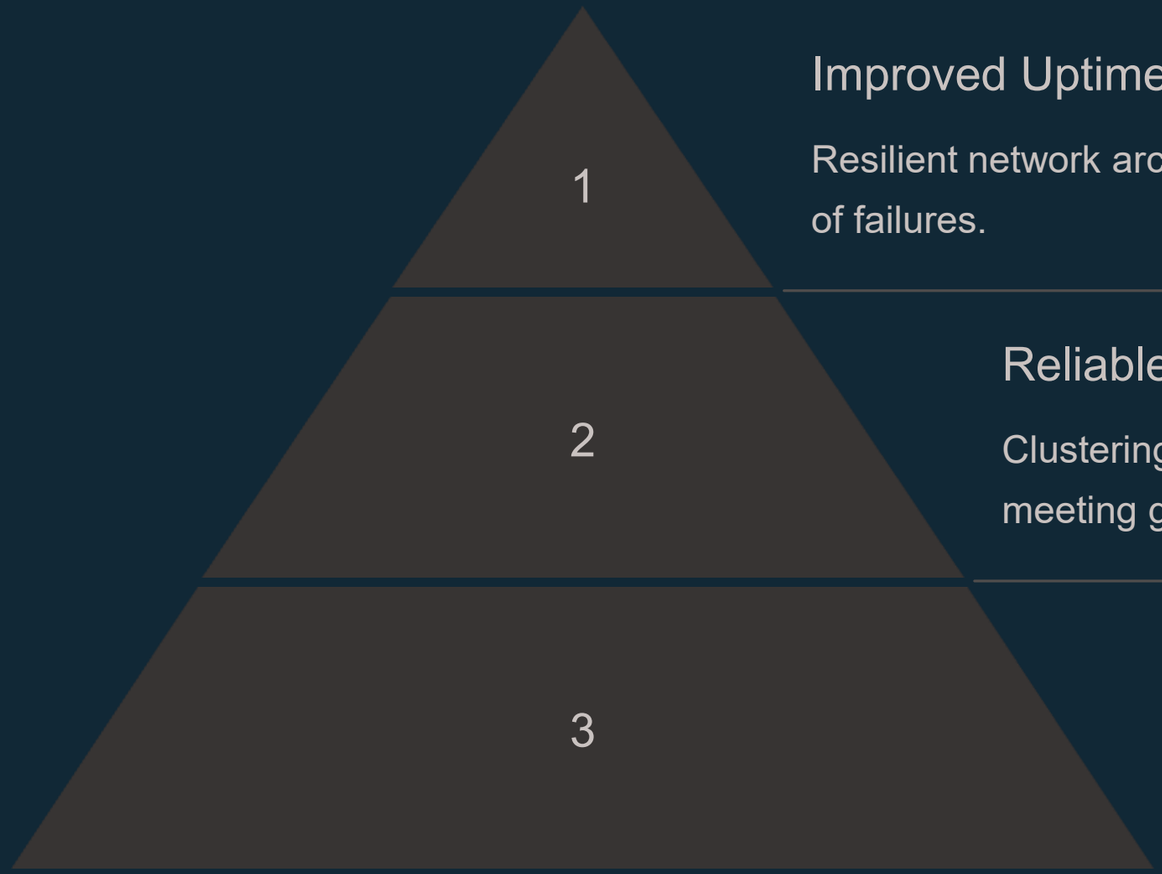
Regularly test failover scenarios to ensure smooth transitions and validate the effectiveness of redundancy mechanisms.



Common Issues and FAQs

Network Bottlenecks	Identify and address network bottlenecks by optimizing routing configurations, increasing bandwidth, and implementing load balancing techniques.
Software Upgrades	Plan and execute software upgrades carefully, minimizing downtime and ensuring compatibility with existing infrastructure.
Cluster Failures	Troubleshoot cluster failures by analyzing logs, testing connections, and verifying configuration settings, identifying and resolving root causes.

Key Takeaways



Improved Uptime and Service Availability

Resilient network architecture ensures uninterrupted service delivery, even in the face of failures.

Reliable and Scalable Network Architecture

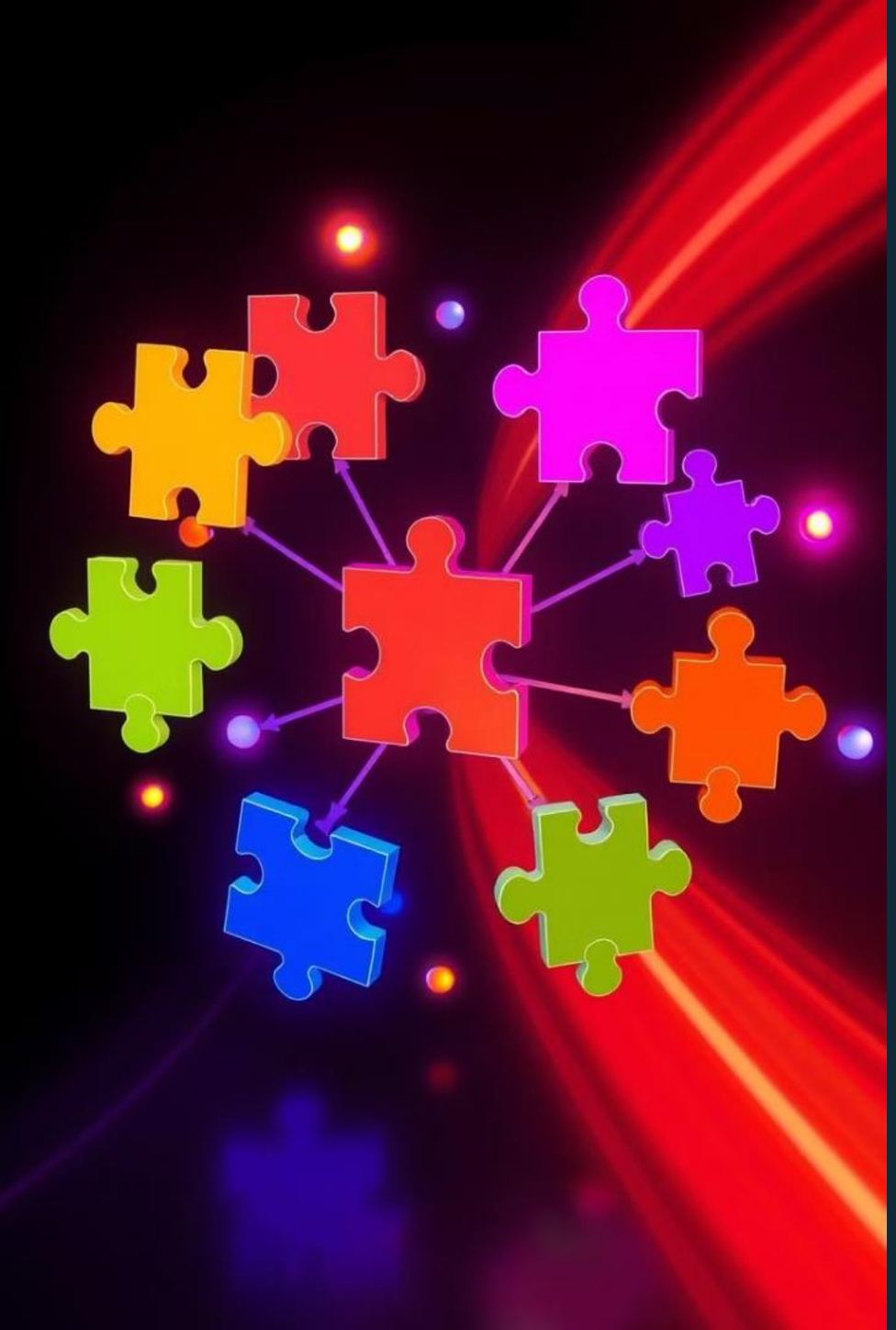
Clustering technologies enable reliable and scalable network infrastructure, meeting growing demands.

Fault Tolerance

Redundancy mechanisms and failover strategies enhance fault tolerance, minimizing downtime and service disruptions.

Week-16 Enterprise-Level Network Design

This lab module explores the intricacies of designing and implementing secure, scalable, and high-performance enterprise networks, providing a comprehensive understanding of key concepts and practical applications.



Objectives

Scalability

Design a network that can grow with your business needs.

Reliability

Ensure consistent network connectivity and minimal downtime.

Security

Protect your data and users from unauthorized access.

Performance

Optimize network speed and efficiency to maximize productivity.

Design and Implementation

Network Segmentation

Divide the network into smaller, manageable segments to improve security and performance.

Virtualization

Use virtual network devices to create flexible and efficient network infrastructure.

Routing Protocols

Configure routing protocols to optimize data flow between network devices.

Network Monitoring

Implement tools to track network performance and identify potential problems.

Performance Optimization

1

Bandwidth Management

Prioritize critical traffic and allocate bandwidth effectively.

2

Quality of Service (QoS)

Ensure high-quality network performance for voice, video, and other critical applications.

3

Network Load Balancing

Distribute network traffic across multiple devices to improve performance and availability.

4

Network Optimization Tools

Use software to identify and resolve network bottlenecks.

Secure Access

Firewalls

Protect your network from unauthorized access and malicious traffic.

VPN

Provide secure access to your network for remote users.

Identity Management

Control user access to network resources and enforce security policies.

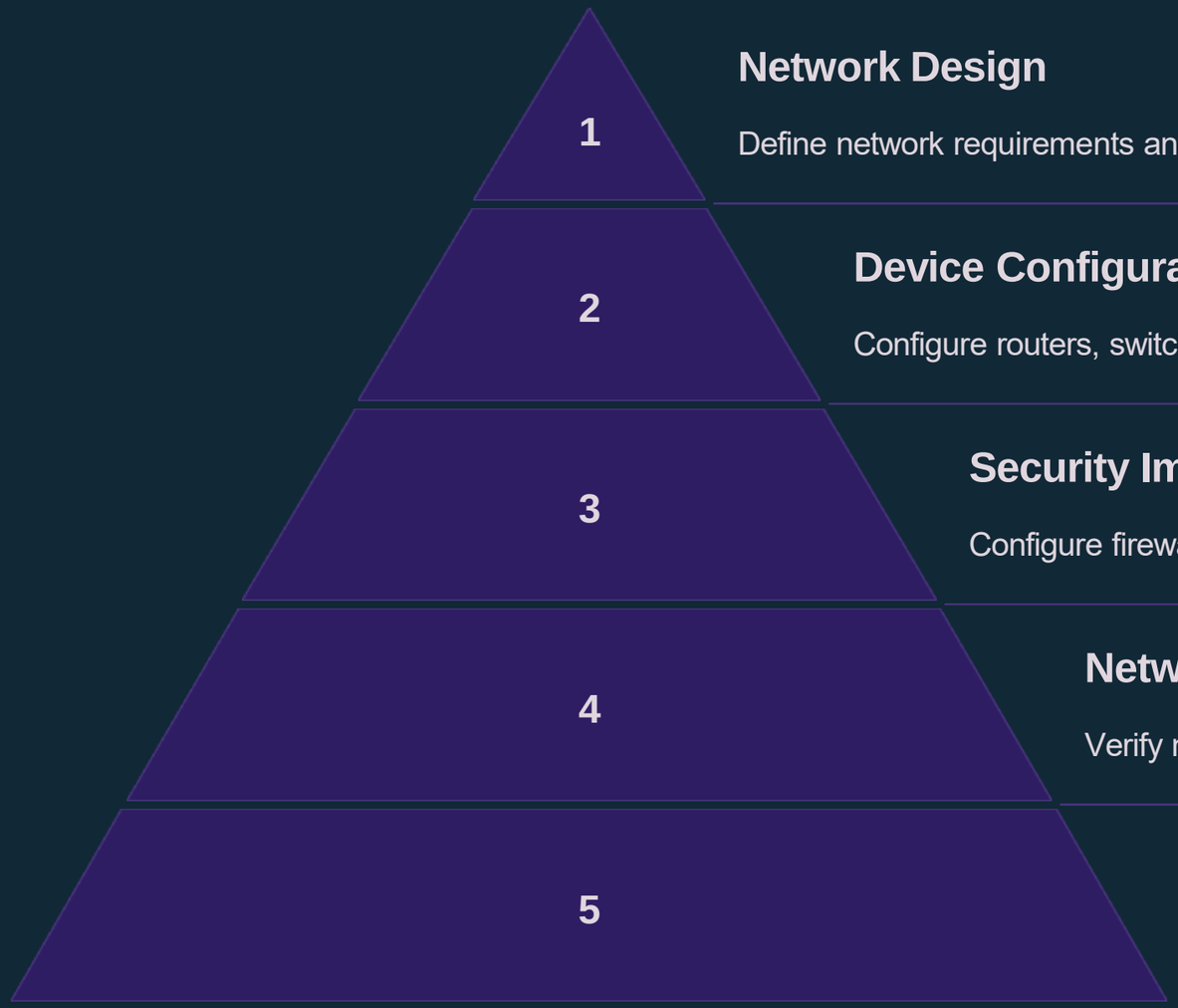
Intrusion Detection

Monitor network activity and detect potential security threats.

Equipment and Preparation

Device	Description
Core Router	Provides high-speed connectivity and routing between network segments.
Distribution Switches	Connect multiple access switches and provide network segmentation.
Access Switches	Connect end devices such as computers and printers.
Network Mapping Software	Visualize network topology and identify potential problems.
Diagnostic Tools	Analyze network traffic and troubleshoot issues.

Procedure



Network Design

Define network requirements and create a detailed topology.

Device Configuration

Configure routers, switches, and other network devices.

Security Implementation

Configure firewalls, VPNs, and other security measures.

Network Testing

Verify network connectivity and performance.

Documentation

Create detailed network documentation for future reference.

Safety and Practical Considerations

1

Safety First

Always wear appropriate safety gear and follow proper handling procedures for network equipment.

2

Power Considerations

Ensure proper power supply and grounding for all network devices.

3

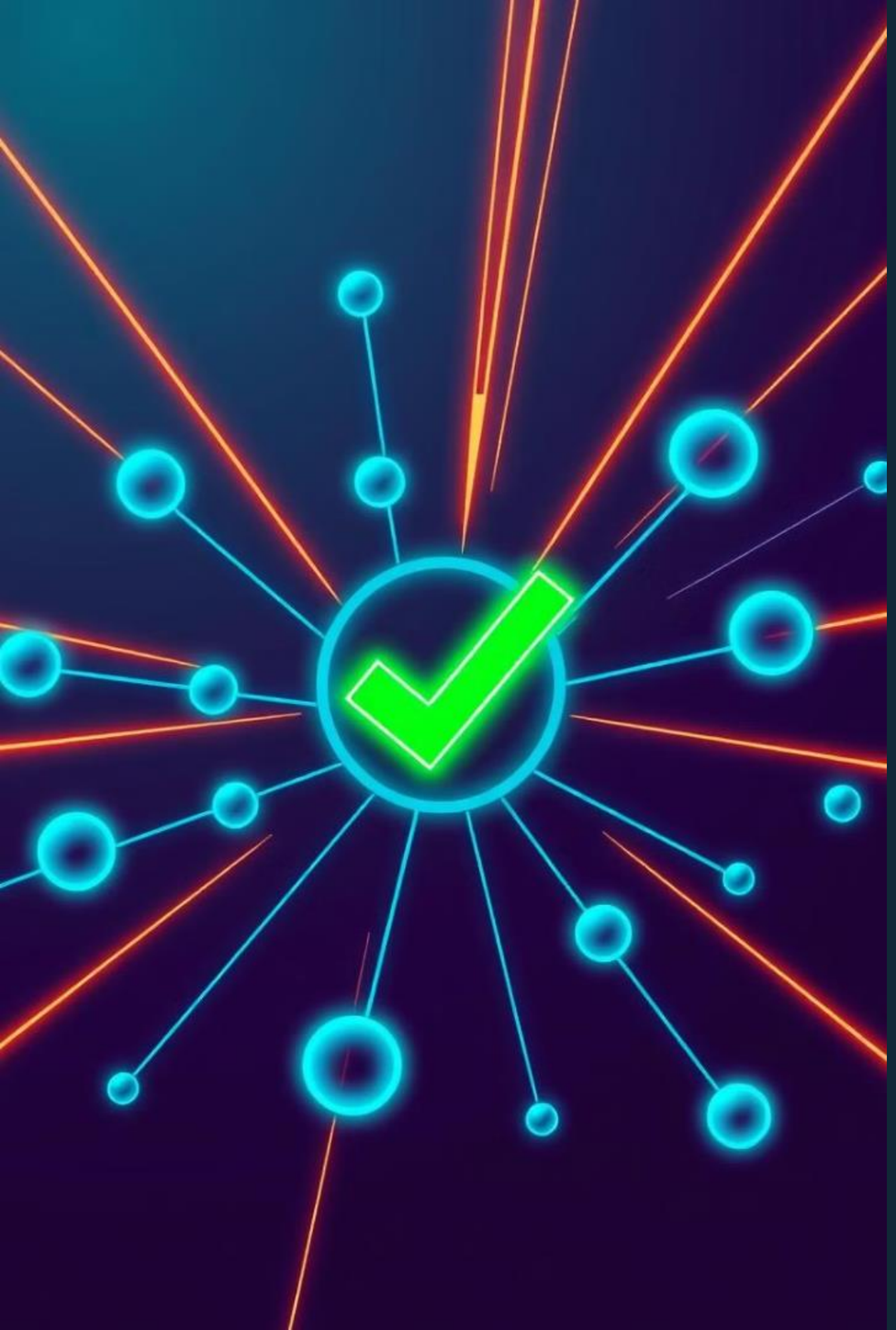
Network Access Control

Restrict access to network devices to authorized personnel only.

4

Environmental Monitoring

Monitor network environment for temperature, humidity, and other factors that may affect device performance.



Key Takeaways

1

Scalability

Design a network that can grow with your business needs.

2

Security

Protect your data and users from unauthorized access.

3

Reliability

Ensure consistent network connectivity and minimal downtime.

4

Performance

Optimize network speed and efficiency to maximize productivity.

Enterprise-Level Network Design

This lab module explores the intricacies of designing and implementing secure, scalable, and high-performance enterprise networks, providing a comprehensive understanding of key concepts and practical applications.