

COMPUTER NETWORKS WORKSHOP

Recourse Person

W.M.T.Ravindra Wanninayake

MDTU-Chief
Secretariat NWP

Computer Networks workshop @ 26th and 28th November 2024

01. Network Basics

- 1.1 What is a network?
- 1.2 Types of networks: LAN, WAN, MAN, WLAN.
- 1.3 Components of a network: Routers, switches, servers, firewalls, etc.
- 1.4 Networking models: OSI model and TCP/IP model.

02. Networking Terminology

- 2.1 IP Addressing (IPv4 and IPv6).
- 2.2 Subnetting and CIDR notation.
- 2.3 DNS, DHCP, NAT, and VPNs.
- 2.4 Protocols like TCP, UDP, HTTP, FTP, and SMTP.

03. Hands-on Practice

- 3.1 Use simulation tools like Cisco Packet Tracer or GNS3.
- 3.2 Practice setting up networks with free tools such as VirtualBox or VMware for virtualization.
- 3.3 Setting up a basic LAN.
- 3.4 Configuring IP addresses.
- 3.5 Using the ping and traceroute commands to test connectivity.
- 3.6 Troubleshooting network issues.

04. Learn About Network Security

- 4.1 Basics of firewalls and intrusion detection/prevention systems (IDS/IPS).
- 4.2 Secure protocols (HTTPS, SSL/TLS, SSH).
- 4.3 Understanding common threats like DDoS, man-in-the-middle (MITM) attacks, and phishing.

05. Understand Wi-Fi and Wireless Networking

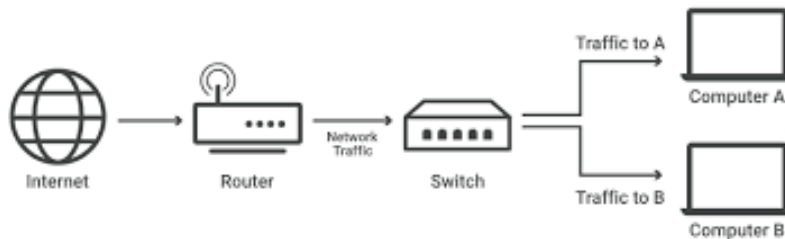
- 5.1 Learn about Wi-Fi standards (e.g., 802.11b/g/n/ac/ax).
- 5.2 Practice configuring a wireless router and securing it (WPA3, strong passwords).

06. Experiment with Tools

- 6.1 Network Analyzers: Tools like Wireshark to analyze and troubleshoot networks.
- 6.2 Command-Line Tools: Learn networking commands like ipconfig, ifconfig, netstat, and nslookup.

01. Network Basics

- **1.1 What is a network?**



A **network** is a system of interconnected devices or nodes (such as computers, servers, smartphones, printers, or other hardware) that communicate and share resources, data, or services with each other. These devices are linked using communication channels such as cables (wired) or wireless technologies.

Key Features of a Network

- ✓ **Connectivity:** Networks enable devices to connect and communicate.
- ✓ **Resource Sharing:** Devices can share hardware (printers, scanners) and software (applications, files).
- ✓ **Data Transmission:** Facilitates the exchange of information (emails, files, multimedia).
- ✓ **Scalability:** Networks can grow as more devices are added.

- **1.2 Types of networks: LAN, WAN, MAN, WLAN.**

LAN (Local Area Network):

- ✓ Covers a small area (e.g., a home, office, or building).
- ✓ Typically, faster and more secure due to limited reach.
- ✓ Example: Office computers connected to a single router.



WAN (Wide Area Network):

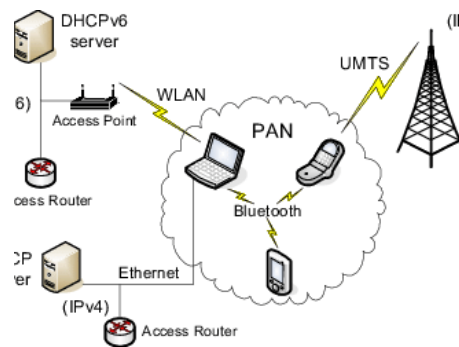
- ✓ Covers large geographic areas (e.g., cities, countries, or globally).
- ✓ The Internet is the most common example.
- ✓ Connects smaller networks (LANs) using routers and telecommunication links.

MAN (Metropolitan Area Network):

- ✓ Spans a city or campus.
- ✓ Larger than a LAN but smaller than a WAN.
- ✓ Example: A city-wide Wi-Fi network.



PAN (Personal Area Network):



- ✓ Used for individual devices within a short range (a few meters).
- ✓ Example: Connecting your smartphone to Bluetooth headphones.
- ✓ WLAN (Wireless LAN):
- ✓ Similar to LAN but uses wireless connections like Wi-Fi.

• 1.3 Components of a network: Routers, switches, servers, firewalls, etc.

A network is made up of various hardware and software components that work together to enable communication, resource sharing, and data exchange. Below are the key components of a network and their functions:

A. Routers

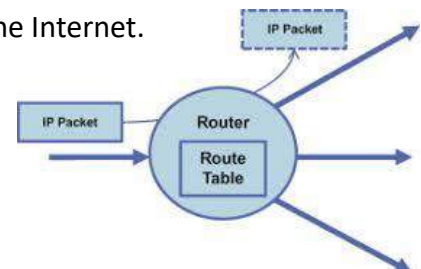
Function: Connects different networks and directs data packets to their destination.

How it Works: Uses IP addresses to determine the best route for data.

Example: A home router connects your local devices to the Internet.

Key Features:

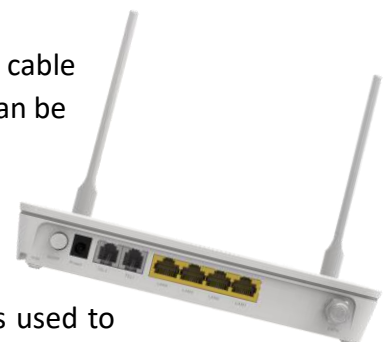
- ✓ Enables WAN connectivity.
- ✓ Provides Network Address Translation (NAT).
- ✓ Offers firewall and security features.



An ONT

An ONT (Optical Network Terminal) box and a router are not the same, although they may be used together as part of a larger network setup.

An ONT is a device that is used to terminate the fiber optic cable and convert the optical signal into an electrical signal that can be used by a home or business network. It is typically used in fiber-to-the-home (FTTH) or fiber-to-the-premises (FTTP) networks to connect a building to the wider network.



A router, on the other hand, is a networking device that is used to connect multiple devices to a network and facilitate communication between them. It acts as a central hub for data traffic and can provide features such as wireless connectivity, network security, and traffic prioritization.

In some cases, an ONT and a router may be combined into a single device, such as a fiber optic modem or a gateway. However, it's important to note that these terms refer to distinct pieces of hardware with different functions.

B. Switches



Function: Connects devices within the same network (e.g., computers, printers, servers) to enable communication.

How it Works: Uses MAC addresses to forward data only to the intended device.

Types:

- ✓ **Unmanaged Switch:** Simple plug-and-play device.
- ✓ **Managed Switch:** Offers advanced features like VLANs, traffic prioritization, and monitoring.

C. Servers



Function: Provide centralized resources, data, and services to devices on the network.

Types:

- ✓ **File Server:** Stores and shares files.
- ✓ **Web Server:** Hosts websites.
- ✓ **Database Server:** Manages and serves databases.
- ✓ **Application Server:** Runs specific software applications.

Example: A company's email server handles incoming and outgoing emails.

C. Firewalls

Function: Protects the network by controlling incoming and outgoing traffic based on security rules.

Types:

- ✓ **Hardware Firewalls:** Physical devices placed between a network and external threats (e.g., Internet).
- ✓ **Software Firewalls:** Installed on devices to protect individual systems.

Key Features:

- ✓ Blocks unauthorized access.
- ✓ Monitors traffic for threats.
- ✓ Protects against malware and hackers.

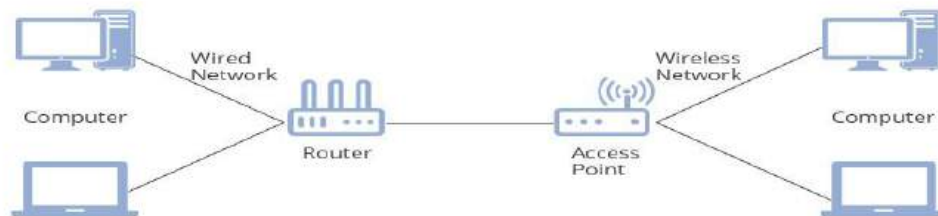
D. End Devices

Function: Devices that users interact with to access the network.

Examples:

- ✓ Computers, laptops, and tablets.
- ✓ Smartphones.
- ✓ Printers and scanners.

E. Access Points



Function: Extends a wired network to enable wireless connectivity.

How it Works: Connects to a router or switch and broadcasts a Wi-Fi signal.

Example: Wi-Fi hotspots in offices or public spaces.

F. Transmission Media

Function: Carries data between network devices.

Types:

- ✓ **Wired Media:** Ethernet cables, fiber optics.
- ✓ **Wireless Media:** Radio waves (Wi-Fi, Bluetooth).

G. Modems

Function: Converts digital data from a device into signals suitable for transmission over communication lines (e.g., DSL or cable).

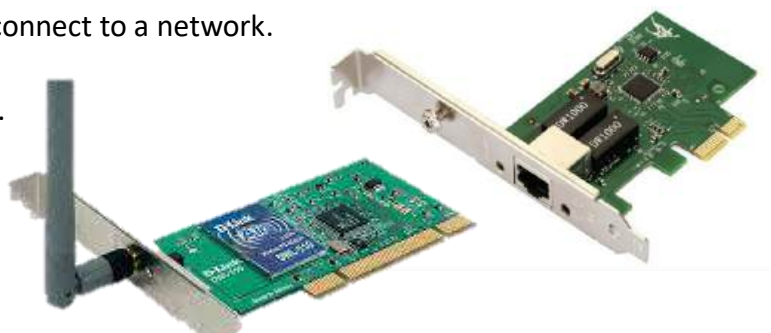
Example: Connects a home network to the Internet via an Internet Service Provider (ISP).

H. Network Interface Cards (NICs)

Function: Allows a device to connect to a network.

Types:

- Wired NICs (Ethernet).
- Wireless NICs (Wi-Fi).



I. Hubs

Function: Broadcasts data to all devices on a network.

Limitation: Unlike switches, hubs cannot filter traffic and are less efficient.

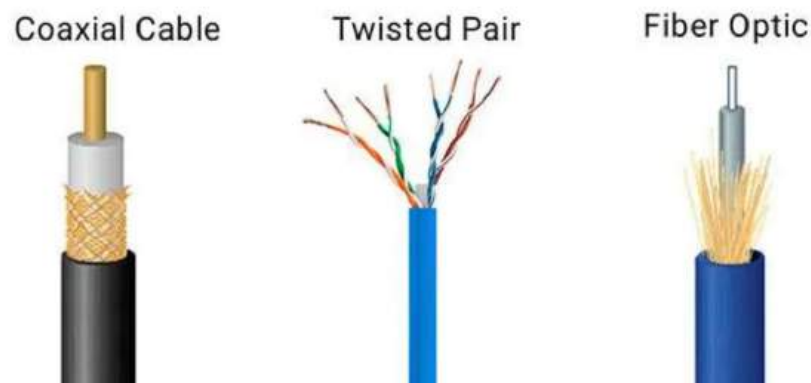
J. Load Balancers

Function: Distributes network traffic evenly across multiple servers to ensure reliability and performance.

Example: Used in data centers to handle high traffic on websites.

K. Network Cables

Function: Physically connect devices in a wired network.



Types:

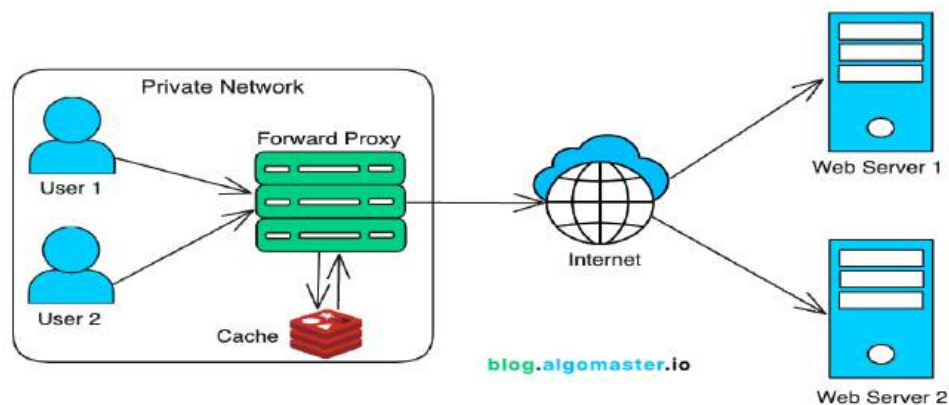
- ✓ **Twisted Pair Cables:** Common in Ethernet networks.
- ✓ **Fiber Optic Cables:** For high-speed, long-distance communication.

L. DNS Servers

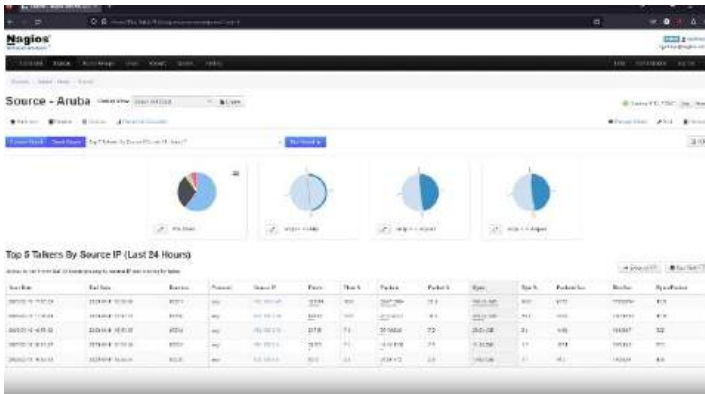
Function: Translates human-readable domain names (e.g., www.ravi.com) into IP addresses.

M. Proxy Servers

Function: Acts as an intermediary between a client and the Internet to enhance security and improve performance.



N. Network Management Software



Function: Monitors and manages the network's health, performance, and security.

Example: Tools like SolarWinds, Nagios, and PRTG.

These components work together to ensure seamless

communication, efficient data transfer, and secure access within a network. Understanding their roles is critical for designing, managing, and troubleshooting networks.

- 1.4 Networking models: OSI model and TCP/IP model.

Networking models are frameworks that standardize how data is transferred over a network. They provide a structured way to understand and implement networking protocols and technologies.

OSI Model (Open Systems Interconnection)

The OSI model is a conceptual framework that standardizes the functions of a network into 7 layers. Each layer serves a specific purpose and interacts with the layers above and below it.

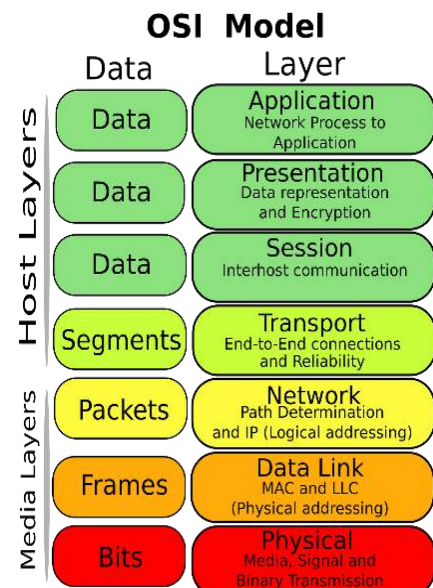
Layers of the OSI Model

Physical Layer (Layer 1):

- ✓ Handles the physical connection between devices.
- ✓ Transmits raw data (bits) over cables, radio waves, etc.
- ✓ Example: Ethernet cables, fiber optics, connectors.

Data Link Layer (Layer 2):

- ✓ Provides error detection and correction for data transmission.
- ✓ Organizes data into frames.
- ✓ Example Protocols: Ethernet, Wi-Fi (802.11).



Network Layer (Layer 3):

- ✓ Handles routing and addressing of data packets.
- ✓ Determines the best path for data delivery.
- ✓ Example Protocols: IP (IPv4, IPv6).

Transport Layer (Layer 4):

- ✓ Ensures reliable data delivery through segmentation and error recovery.
- ✓ Example Protocols: TCP (reliable), UDP (fast but unreliable).

Session Layer (Layer 5):

- ✓ Manages sessions (connections) between devices.
- ✓ Example: Establishing a connection for a video call.

Presentation Layer (Layer 6):

- ✓ Translates data into a format the application can understand (e.g., encryption, compression).
- ✓ Example: JPEG, MP4, SSL/TLS.

Application Layer (Layer 7):

- ✓ Interfaces with user applications and provides network services.
- ✓ Example Protocols: HTTP, FTP, SMTP.

Advantages of the OSI Model:

- ✓ **Standardization**: Provides a clear framework for developing networking protocols.
- ✓ **Modularity**: Each layer can be developed independently.
- ✓ **Troubleshooting**: Makes it easier to identify and fix network issues by isolating layers.

TCP/IP Model (Transmission Control Protocol/Internet Protocol)

The TCP/IP model is a more practical and widely-used model that describes how data is transmitted over the Internet. It has 4 layers, combining some of the OSI layers.

Layers of the TCP/IP Model

Network Access Layer (Link Layer):

- ✓ Combines the OSI's Physical and Data Link layers.
- ✓ Handles hardware addressing and the physical transmission of data.
- ✓ Example: Ethernet, Wi-Fi.

Internet Layer:

- ✓ Corresponds to the OSI's Network Layer.
- ✓ Handles logical addressing, routing, and packet delivery.
- ✓ Example Protocols: IP (IPv4, IPv6), ICMP.

Transport Layer:

- ✓ Similar to the OSI Transport Layer.
- ✓ Ensures end-to-end communication, error recovery, and data segmentation.
- ✓ Example Protocols: TCP (reliable), UDP (unreliable but faster).

Application Layer:

- ✓ Combines the OSI's Application, Presentation, and Session layers.
- ✓ Provides high-level services to applications and users.
- ✓ Example Protocols: HTTP, FTP, DNS, SMTP.

Advantages of the TCP/IP Model:

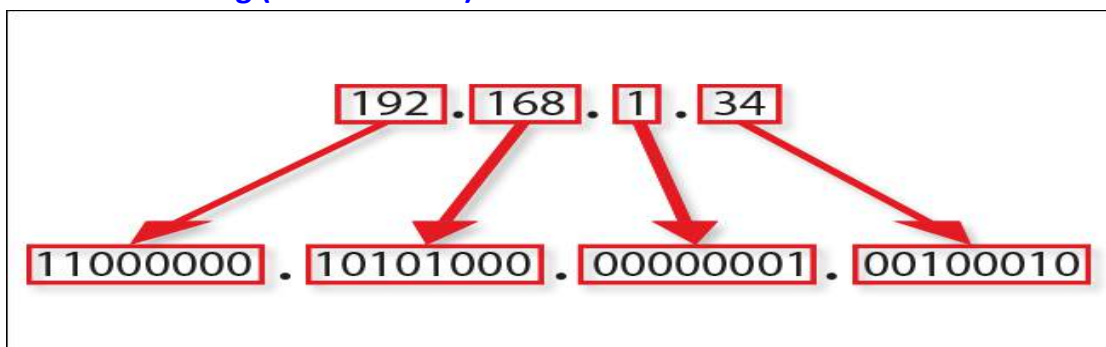
- ✓ **Widely Adopted:** Basis of Internet communication.
- ✓ **Simplified Layers:** More practical than the OSI model.
- ✓ **Interoperability:** Supports diverse hardware and software platforms.

Comparison: OSI vs. TCP/IP Models

Feature	OSI Model	TCP/IP Model
Number of Layers	7	4
Approach	Theoretical and conceptual	Practical and implementation-focused
Application Layer	Separate Application, Presentation, and Session layers	Combined into one layer
Transport Layer Protocols	Protocol-independent (e.g., TCP, UDP)	Primarily TCP and UDP
Usage	Educational and troubleshooting	Standard for Internet communication
Development	Developed by ISO	Developed by DARPA

02. Networking Terminology

- **2.1 IP Addressing (IPv4 and IPv6).**



An IP (Internet Protocol) address is a unique identifier assigned to devices on a network. It allows devices to locate and communicate with each other over the Internet or a local network.

IPv4 (Internet Protocol Version 4)

Characteristics of IPv4:

Address Format:

- ✓ IPv4 addresses are written in **dotted decimal notation**.
- ✓ Example: 192.168.1.1
- ✓ Each address consists of **4 octets** (8 bits each), separated by dots.

Address Space:

- ✓ **32-bit address** (2^{32} unique addresses).
- ✓ Supports around **4.3 billion addresses**.

Classes:

- ✓ IPv4 addresses are divided into **classes** based on the first octet:
 - **Class A:** Large networks (1.0.0.0 – 126.0.0.0).
 - **Class B:** Medium-sized networks (128.0.0.0 – 191.255.0.0).
 - **Class C:** Small networks (192.0.0.0 – 223.255.255.0).
 - **Class D:** Reserved for multicast (224.0.0.0 – 239.255.255.255).
 - **Class E:** Reserved for experimental purposes (240.0.0.0 – 255.255.255.255).

Five Different Classes of IPv4 Addresses

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

Private IP Ranges:

- ✓ Reserved for internal networks (cannot be routed on the Internet):
 - **10.0.0.0 – 10.255.255.255.**
 - **172.16.0.0 – 172.31.255.255.**
 - **192.168.0.0 – 192.168.255.255.**

Subnet Mask:

- ✓ Defines the network and host portions of an address.
- ✓ Example: 255.255.255.0 means the first 24 bits are for the network.

Limitations:

- ✓ **Address Exhaustion:** The rapid growth of devices caused a shortage of IPv4 addresses.
- ✓ Limited scalability.

IPv6 (Internet Protocol Version 6)

Address Format:

- ✓ Written in **hexadecimal notation**, separated by colons.
- ✓ Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- ✓ Leading zeros can be omitted (e.g., 2001:db8::8a2e:370:7334).

Address Space:

- ✓ **128-bit address** (2^{128} unique addresses).
- ✓ Supports **340 undecillion** addresses, eliminating the risk of address exhaustion.

Types of IPv6 Addresses:

- ✓ **Unicast**: For a single interface (one-to-one communication).
- ✓ **Multicast**: For multiple interfaces (one-to-many communication).
- ✓ **Anycast**: Delivered to the nearest interface in a group (one-to-one-of-many communication).

Features:

- ✓ Built-in **support for security** (IPsec).
- ✓ No need for **NAT** (Network Address Translation) because of abundant addresses.
- ✓ **Simplified header structure** for faster processing.

IPv6 Address Prefixes:

- ✓ **Global Unicast**: Public IPv6 addresses (e.g., 2000::/3).
- ✓ **Link-local**: Automatically assigned for communication within a local link (e.g., FE80::/10).
- ✓ **Unique Local**: For private networks (e.g., FC00::/7).

Differences Between IPv4 and IPv6

Feature	IPv4	IPv6
Address Format	Dotted decimal (e.g., 192.168.1.1)	Hexadecimal (e.g., 2001:db8::1)
Address Size	32 bits	128 bits
Address Space	~4.3 billion addresses	~340 undecillion addresses
Header Size	20 bytes	40 bytes
Security	Optional (IPsec is not mandatory)	Built-in (IPsec support)
NAT Required	Yes, due to address scarcity	No, due to abundant addresses
Broadcast	Supported	Not supported (uses multicast)
Auto-configuration	Limited	Robust (link-local addressing)

Why IPv6 Is Important

- I. **Address Exhaustion:** IPv4 addresses are running out due to the increasing number of Internet-connected devices.
- II. **Scalability:** IPv6 provides a virtually unlimited address pool.
- III. **Efficiency:** Simplified routing and processing due to a streamlined header.
- IV. **Enhanced Features:** Improved support for mobile devices and security.

- **2.2 Subnetting and CIDR notation.**

Subnetting and CIDR (Classless Inter-Domain Routing) are essential concepts in IP networking that allow efficient allocation and management of IP addresses.

Subnetting

Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks (subnets). It helps optimize the use of IP addresses and improves network performance by reducing congestion.

Why Subnetting is Needed:

- ✓ **Efficient IP Utilization:** Avoid wasting IP addresses.
- ✓ **Network Management:** Makes large networks easier to manage.
- ✓ **Improved Security:** Isolates traffic between different parts of the network.
- ✓ **Reduced Broadcast Traffic:** Limits the range of broadcast domains.

Subnet Mask:

Defines the division between the network and host portions of an IP address.
Example for IPv4: 255.255.255.0 (indicating 24 bits for the network and 8 bits for hosts).

Network and Host Portions:

The network portion identifies the subnet.

The host portion identifies specific devices within the subnet.

Example of Subnetting:

Given the network 192.168.1.0/24:

- ✓ /24 means 24 bits are for the network portion (subnet mask: 255.255.255.0).
- ✓ This allows 256 IP addresses (2^8), but only 254 are usable (excluding the network and broadcast addresses).

If we divide this network into 4 subnets:

- ✓ Each subnet will have 64 IPs (2^6).
- ✓ Subnets:
 - **192.168.1.0/26**
hosts: 192.168.1.1 to 192.168.1.62, broadcast: 192.168.1.63)
 - **192.168.1.64/26**
(hosts: 192.168.1.65 to 192.168.1.126, broadcast: 192.168.1.127)

- **192.168.1.128/26**
(hosts: 192.168.1.129 to 192.168.1.190, broadcast: 192.168.1.191)
- **192.168.1.192/26**
(hosts: 192.168.1.193 to 192.168.1.254, broadcast: 192.168.1.255).

CIDR Notation

What is CIDR?

- ✓ CIDR is a method of representing IP addresses and their associated subnet mask using a slash (/) followed by the number of network bits.
- ✓ Example: 192.168.1.0/24
 - /24 indicates that the first 24 bits represent the network portion.

Why CIDR is Useful:

1. Eliminates rigid IP classes (Class A, B, C) by allowing flexible subnet sizes.
2. Reduces address waste and improves routing efficiency.
3. Aggregates multiple IP addresses into a single route (route summarization).

CIDR Prefix and Subnet Mask:

CIDR Notation	Subnet Mask	# of Usable Hosts
/8	255.0.0.0	16,777,214
/16	255.255.0.0	65,534
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/30	255.255.255.252	2

1. Find the Subnet Mask:

- For /28, the subnet mask is 255.255.255.240 (28 bits for the network).

2. Calculate the Number of Subnets:

- Formula: $2^{(\text{borrowed bits})}$ (bits added to the network portion).
- Example: Borrow 4 bits from the host portion in /24. This gives $2^4 = 16$ subnets.

3. Calculate the Number of Hosts per Subnet:

- Formula: $2^{(\text{remaining host bits})} - 2$ (subtracting 2 for network and broadcast).
- Example: /28 leaves 4 bits for hosts: $2^4 - 2 = 14$ usable hosts.

4. Identify Subnet Ranges:

- Example for 192.168.1.0/28:
 - Subnet 1: 192.168.1.0 - 192.168.1.15 (usable: 192.168.1.1 - 192.168.1.14).
 - Subnet 2: 192.168.1.16 - 192.168.1.31 (usable: 192.168.1.17 - 192.168.1.30).

Key Differences: Subnetting vs. CIDR

Feature	Subnetting	CIDR
Purpose	Dividing a network into smaller subnets	Aggregating or allocating IP ranges
Addressing	Often rigid (class-based)	Flexible (classless)
Efficiency	Improves address allocation in a network	Reduces routing table size in the Internet

- **2.3 DNS, DHCP, NAT, and VPNs.**

These are foundational concepts and technologies in computer networking that enable connectivity, address management, and security.

DNS (Domain Name System)

What is DNS?

DNS translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.168.1.1) that computers use to locate each other on a network.

How It Works:

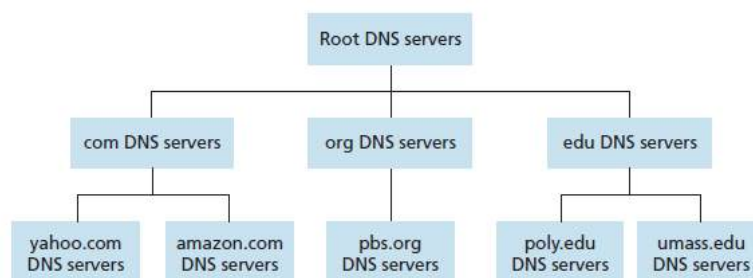
- ✓ **User Request:** A user enters a URL into their browser.
- ✓ **DNS Query:** The browser sends a query to a DNS server.
- ✓ **Resolution:** The DNS server checks its database or queries other servers to resolve the domain name into an IP address.
- ✓ **Response:** The IP address is returned to the browser, which then communicates with the web server.

Types of DNS Servers:

- ✓ **Recursive Resolver:** Finds the IP address by querying other servers on behalf of the user.
- ✓ **Root Servers:** Directs the query to the appropriate top-level domain (TLD) server (e.g., .com or .org).
- ✓ **Authoritative DNS Server:** Provides the actual IP address for the domain.

Benefits:

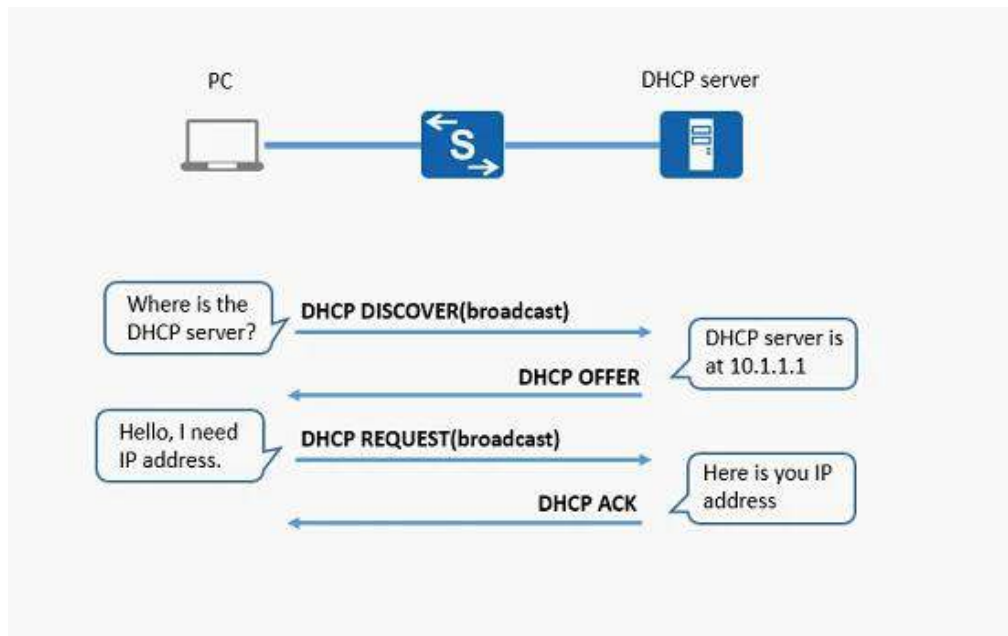
- ✓ Simplifies user access to websites.
- ✓ Allows easy updates to IP addresses without affecting end-users.



DHCP (Dynamic Host Configuration Protocol)

What is DHCP?

- ✓ DHCP automatically assigns IP addresses and other network configurations (subnet mask, default gateway, DNS server) to devices on a network.



How It Works:

- ✓ **DHCP Discover:** A device sends a broadcast request to find a DHCP server.
- ✓ **DHCP Offer:** The server responds with an available IP address and configuration.
- ✓ **DHCP Request:** The device requests to lease the offered IP address.
- ✓ **DHCP Acknowledge:** The server confirms and assigns the IP address to the device.

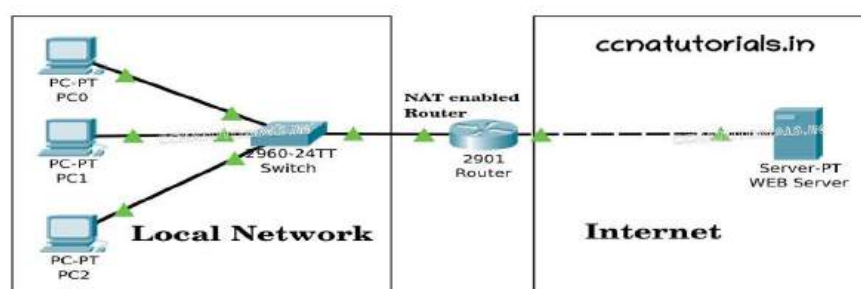
Benefits:

- ✓ Eliminates the need for manual IP configuration.
- ✓ Reduces IP conflicts and simplifies network management.

NAT (Network Address Translation)

What is NAT?

NAT allows multiple devices on a private network to share a single public IP address for accessing the Internet.



How It Works:

When a device on a private network communicates with the Internet, the NAT-enabled router replaces the private IP address with its public IP address in the outgoing packet. It keeps track of this mapping so that responses can be sent back to the correct device.

Types of NAT:

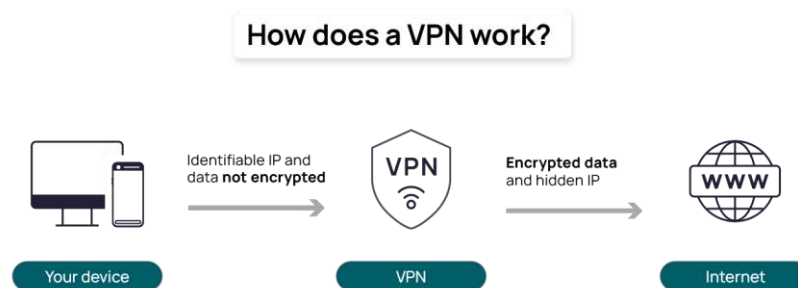
- ✓ **Static NAT:** Maps one private IP to one public IP.
- ✓ **Dynamic NAT:** Maps a private IP to an available public IP from a pool.
- ✓ **PAT (Port Address Translation):** Maps multiple private IPs to a single public IP using different port numbers.

Benefits:

- ✓ Conserves public IP addresses.
- ✓ Adds a layer of security by hiding internal IPs.

VPN (Virtual Private Network)

What is a VPN?



A VPN creates a secure, encrypted tunnel between a device and a remote network over the Internet.

How It Works:

- ✓ **Encryption:** VPN software encrypts all outgoing data.
- ✓ **Tunneling:** Data is sent through a virtual tunnel to the VPN server.
- ✓ **Decryption:** The VPN server decrypts the data and forwards it to the destination.

Types of VPNs:

- ✓ **Remote Access VPN:** Connects individual devices to a network securely.
- ✓ **Site-to-Site VPN:** Connects entire networks securely over the Internet.
- ✓ **Client-to-Site VPN:** Allows remote devices to connect to a corporate network.

Benefits:

- ✓ Protects sensitive data from eavesdropping.
- ✓ Hides the user's IP address and location.
- ✓ Allows access to geo-restricted content.

Comparison Table

Feature	DNS	DHCP	NAT	VPN
Purpose	Translates domain names to IPs	Assigns IP addresses dynamically	Shares public IPs among devices	Secures and encrypts connections
Function	Name resolution	Automatic IP configuration	Traffic translation and mapping	Encrypted, private communication
Use Case	Accessing websites	Simplifying IP management	Internet access for private networks	Secure remote work or privacy
Benefits	User-friendly browsing	Time-saving, reduces errors	Saves IP addresses, adds security	Privacy, security, and access

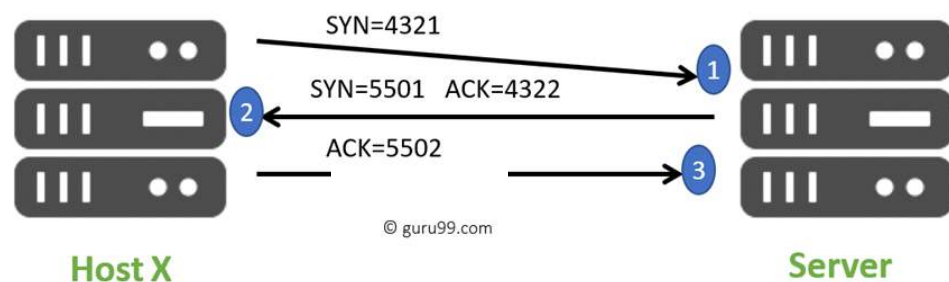
However

- DNS and DHCP focus on usability and automation in networking.
 - NAT conserves IP resources and adds security to Internet communication.
 - VPNs ensure secure and private communication, making them vital for modern connectivity.
- **2.4 Protocols like TCP, UDP, HTTP, FTP, and SMTP.**
 Protocols define rules for communication between devices in a network. They ensure data is transmitted reliably, securely, and efficiently.

TCP (Transmission Control Protocol)

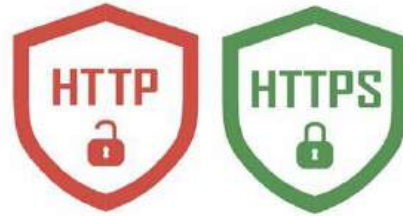
Overview:

TCP is a connection-oriented protocol that ensures reliable delivery of data. It guarantees that data packets are delivered in the correct order, without loss, duplication, or corruption.



Key Features:

- ✓ **Three-Way Handshake:** Establishes a reliable connection before data transfer.
 - SYN: Client requests a connection.
 - SYN-ACK: Server acknowledges and agrees.
 - ACK: Client confirms.
- ✓ **Error Checking:** Uses checksums to detect errors.
- ✓ **Flow Control:** Prevents sender from overwhelming the receiver.
- ✓ **Acknowledgment:** Receiver acknowledges received data.



Common Uses:

- ✓ Web browsing (HTTP/HTTPS)
- ✓ Email (SMTP/IMAP/POP3)
- ✓ File transfer (FTP)

UDP (User Datagram Protocol)

Overview:

UDP is a connectionless protocol that focuses on fast, efficient transmission. It does not guarantee reliable delivery, making it lightweight and faster than TCP.

Key Features:

- ✓ No connection setup (no handshake).
- ✓ No guarantee of order or delivery.
- ✓ Low overhead, making it suitable for time-sensitive applications.

Common Uses:

- ✓ Video and voice streaming.
- ✓ Online gaming.
- ✓ DNS queries.

TCP vs. UDP:

Feature	TCP	UDP
Reliability	Reliable, ensures delivery	Unreliable, no guarantees
Speed	Slower due to error checking	Faster, minimal overhead
Use Case	Critical data transfer	Time-sensitive applications

HTTP (Hypertext Transfer Protocol)

Overview:

- ✓ HTTP is the foundation of data communication on the web.
- ✓ It defines how requests and responses are exchanged between clients (browsers) and servers.

Key Features:

- ✓ Stateless: Each request is independent of others.
- ✓ Text-based: Uses human-readable text commands (e.g., GET, POST).
- ✓ Layer: Operates over TCP.

Common Uses:

- ✓ Browsing websites.
- ✓ API communication.
- ✓ HTTPS (HTTP Secure):
- ✓ Adds encryption via TLS/SSL for secure communication.

FTP (File Transfer Protocol)

Overview:

- ✓ FTP is a protocol for transferring files between a client and a server.
- ✓ It supports both text and binary file transfers.

Key Features:

Uses two channels:

- ✓ Control Channel: For commands and responses.
- ✓ Data Channel: For file transfer.
- ✓ Authentication: Requires username and password.
- ✓ Can be active or passive:
- ✓ Active Mode: Server initiates the data connection.
- ✓ Passive Mode: Client initiates both connections.

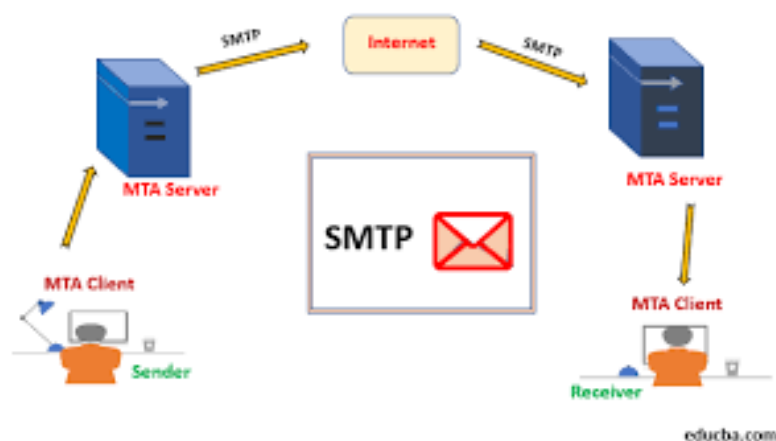
Common Uses:

- ✓ Uploading/downloading files.
- ✓ Managing website files.

SMTP (Simple Mail Transfer Protocol)

Overview:

- ✓ SMTP is used for sending emails from a client to a mail server or between servers.



Key Features:

- ✓ Text-based: Uses plain text commands.
- ✓ Push Protocol: Initiates communication to deliver emails.
- ✓ Works with other protocols like POP3 or IMAP for retrieving emails.

Common Commands:

- ✓ HELO/EHLO: Introduce the client to the server.
- ✓ MAIL FROM: Specify the sender.
- ✓ RCPT TO: Specify the recipient.
- ✓ DATA: Begin the message body.

Common Uses:

- ✓ Sending emails.
- ✓ Transmitting messages between mail servers.

Protocol	Purpose	Type	Common Uses	Reliability
TCP	Reliable data transmission	Transport	Web browsing, email	High
UDP	Fast, connectionless transmission	Transport	Streaming, gaming, DNS	Low
HTTP	Web communication	Application (over TCP)	Browsing, API communication	High
FTP	File transfer	Application (over TCP)	Uploading, downloading files	High
SMTP	Sending email	Application (over TCP)	Email delivery	High

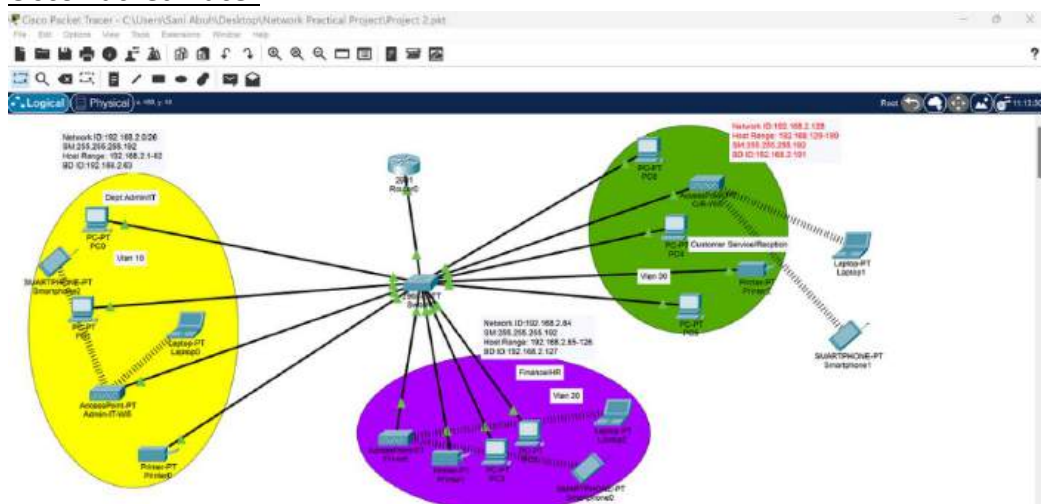
Understanding these protocols is essential for troubleshooting networks and designing applications that rely on efficient data transmission. Each protocol has unique strengths and is suited for specific use cases.

03.Hands-on Practice

- **3.1 Use simulation tools like Cisco Packet Tracer or GNS3.**

Simulation tools like Cisco Packet Tracer and GNS3 allow you to design, configure, and simulate complex networks in a virtual environment without requiring physical hardware. These tools are widely used in networking education and by professionals to practice and test configurations.

Cisco Packet Tracer



Overview:

- Cisco Packet Tracer is a free network simulation tool provided by Cisco.
- It is user-friendly and designed primarily for students and beginners in networking.
- It supports a wide range of Cisco devices and basic network protocols.

Key Features:

- **Drag-and-Drop Interface:** Easy-to-use graphical interface for creating network topologies.
- **Simulation Mode:** Step-by-step visualization of packet flow.
- **Activity Wizard:** Create guided learning activities and scenarios.
- **Multi-User Collaboration:** Multiple users can work on a single project simultaneously.

Use Cases:

- Practicing for Cisco certifications (CCNA, CCNP).
- Learning basic network concepts like routing, switching, and VLANs.
- Testing basic network designs and protocols (e.g., OSPF, RIP, STP).

How to Start:

1. Download and Install:

- Visit [Cisco Networking Academy](#).
- Create an account and download Packet Tracer.

2. Create a Network:

- Drag routers, switches, PCs, and other devices into the workspace.
- Connect them using cables (copper or fiber).

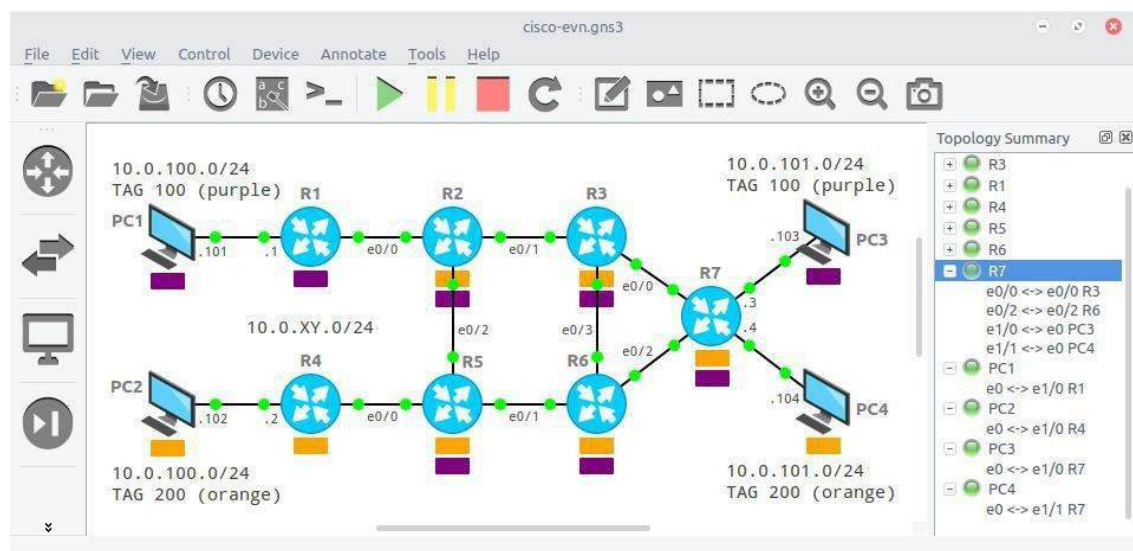
3. Configure Devices:

- Open the CLI (Command Line Interface) for devices to input commands.

4. Simulate Traffic:

- Use the simulation mode to analyze packet flow and troubleshoot issues.

GNS3 (Graphical Network Simulator)



Overview:

- GNS3 is a more advanced and versatile tool than Cisco Packet Tracer.
- It is open-source and supports real Cisco IOS images, providing near-realistic network behavior.
- Ideal for professionals and advanced learners.

Key Features:

- **Real Device Emulation:** Uses Cisco IOS or other vendor images for accurate simulations.
- **Third-Party Integration:** Supports virtual machines (VMs) like VirtualBox or VMware.
- **Wide Protocol Support:** Emulates advanced protocols and features, including MPLS, BGP, and QoS.
- **Scalability:** Build complex and large-scale networks.

Use Cases:

- Preparing for advanced certifications (CCNP, CCIE).
- Testing real-world scenarios and advanced configurations.
- Integrating virtual devices with physical networks.

How to Start:

1. Download and Install:

- Visit [GNS3 Website](#) and download the software.

2. Set Up:

- Install the GNS3 VM for optimal performance.
- Import Cisco IOS images or other device templates.

3. Build a Network:

- Drag devices onto the workspace and connect them.

4. Configure Devices:

- Use the CLI for in-depth configuration and troubleshooting.

5. Simulate Traffic:

- Test protocols, routing, and network behavior.

- **3.2 Practice setting up networks with free tools such as VirtualBox or VMware for virtualization.**

This section is fully covered with practical in Wariyapola IT Lab #1



- **3.3 Setting up a basic LAN.**

This section is fully covered with practical in Wariyapola IT Lab #1

- **3.4 Configuring IP addresses.**

(This section is fully covered with practical in Wariyapola IT Lab #1)

Comparison of Cisco Packet Tracer and GNS3

Feature	Cisco Packet Tracer	GNS3
Skill Level	Beginner to Intermediate	Intermediate to Advanced
Cost	Free (requires NetAcad account)	Free (open-source)
Device Support	Limited to Cisco devices	Supports Cisco and multi-vendor
Simulation Accuracy	Basic (ideal for learning)	High (real IOS emulation)
Scalability	Limited	Supports large-scale networks
System Requirements	Low	High

Choosing the Right Tool

If you are...	Tool Recommendation
A beginner learning the basics of networking	Cisco Packet Tracer
Preparing for Cisco certifications	Cisco Packet Tracer
Testing advanced, multi-vendor scenarios	GNS3
Working with real IOS images	GNS3

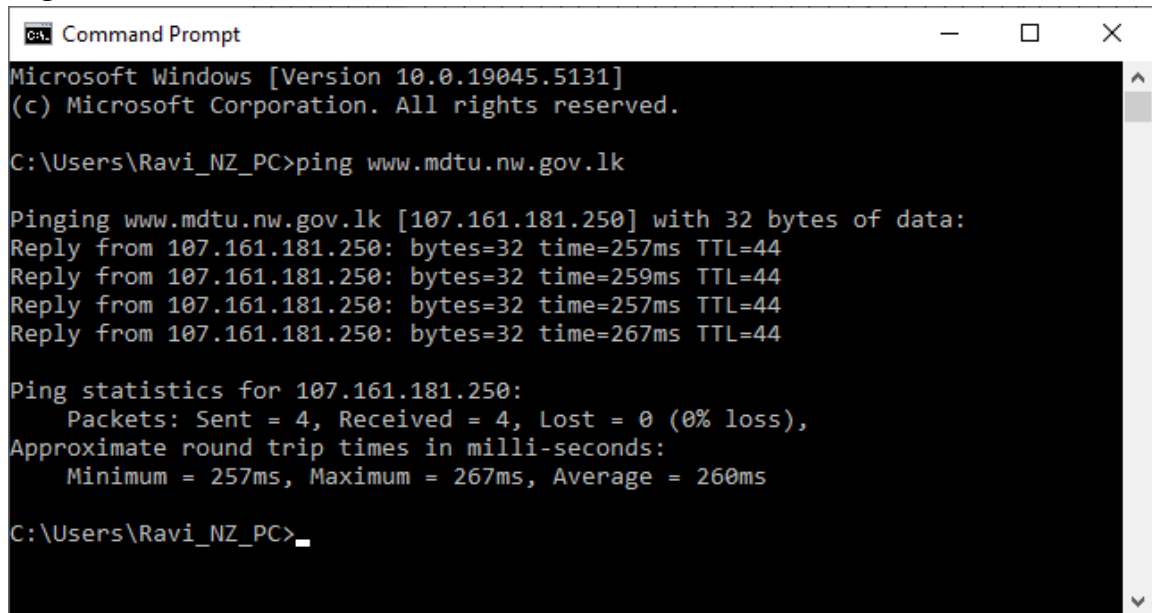
Tips for Learning with Simulation Tools:

- 1. Start Small:**
 - Build basic networks with a few devices.
 - Gradually add complexity as you learn new concepts.
- 2. Follow Tutorials:**
 - Use online resources, YouTube, and networking courses.
- 3. Practice Real-World Scenarios:**
 - Simulate tasks like setting up VLANs, configuring OSPF, or troubleshooting.
- 4. Document Your Work:**
 - Keep notes on configurations and troubleshooting steps for future reference.
- 5. Experiment Freely:**
 - Use the tools to test configurations without fear of breaking anything.

By practicing with these tools, you'll gain hands-on experience and a deeper understanding of networking concepts.

- **3.5 Using the ping and tracert commands to test connectivity.**

Ping Command



```
Command Prompt
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ravi_NZ_PC>ping www.mdtu.nw.gov.lk

Pinging www.mdtu.nw.gov.lk [107.161.181.250] with 32 bytes of data:
Reply from 107.161.181.250: bytes=32 time=257ms TTL=44
Reply from 107.161.181.250: bytes=32 time=259ms TTL=44
Reply from 107.161.181.250: bytes=32 time=257ms TTL=44
Reply from 107.161.181.250: bytes=32 time=267ms TTL=44

Ping statistics for 107.161.181.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 257ms, Maximum = 267ms, Average = 260ms

C:\Users\Ravi_NZ_PC>
```

Overview:

- The **ping** command sends ICMP Echo Request packets to a target IP address or domain name and waits for a reply (ICMP Echo Reply).
- It helps verify if a device (host) is reachable over the network and can also indicate network latency.

How It Works:

- **Ping** tests if the destination device (server, router, etc.) is online and responsive.
- It also measures the round-trip time (RTT) for the packet to travel to the target and back.

Syntax:

ping <hostname or IP address>

Example:

ping www.google.com

or

ping 8.8.8.8

Output Explanation:

- **Reply from <IP>: bytes=32 time=10ms TTL=56:** Indicates a successful ping. The device responded with the time it took for the packet to travel (10ms).
- **Request Timed Out:** The target device didn't respond, which could indicate network issues or that the device is down.
- **Destination Host Unreachable:** This may indicate a problem with the routing or no route to the target device.

Uses:

- **Basic Connectivity:** Verify if a device is reachable.
- **Latency Testing:** Measure the round-trip time (RTT) for packets.
- **Packet Loss:** Check if packets are lost during transmission.

- **Network Troubleshooting:** Identify if there is a network issue between you and a target host.

Tracert (Traceroute) Command

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.1550]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>tracert 192.168.1.1
Tracing route to 192.168.1.1 over a maximum of 30 hops
  0  <1 ms    <1 ms    <1 ms    192.168.49.2
  1  <1 ms    <1 ms    <1 ms    192.168.1.1
Trace complete.
C:\Windows\system32>_
```

Overview:

- **Tracert** (in Windows) or **Traceroute** (in Linux/macOS) traces the route packets take from your device to a destination IP or domain name.
- It shows each hop along the route, which is typically a router or gateway, and the time taken to reach each hop.
- Tracert is useful for identifying where delays or packet loss occur along the network path.

How It Works:

- Tracert sends a series of ICMP Echo Requests with incrementally increasing Time-to-Live (TTL) values.
- Each time the TTL expires, the router sends an ICMP "Time Exceeded" message back to the sender, revealing its IP address.
- This process continues until the destination is reached or the maximum hop count is reached.

Syntax:

tracert <hostname or IP address> (Windows)
 traceroute <hostname or IP address> (Linux/macOS)

Example:

tracert www.google.com
 or
 traceroute www.google.com

Output Explanation:

- **Hop 1:** The first router in the path, usually your local gateway.
- **Hop 2:** The second router along the path to the destination.
- **TTL Expired in Transit:** If the packet is not received in time by the destination, the hop will show "Request Timed Out."
- **Time (ms):** The time in milliseconds it took to reach each hop.

Uses:

- **Network Path Analysis:** Shows the path your data takes and helps identify where issues occur (e.g., slow routers).
- **Diagnosing Latency Issues:** Helps pinpoint where delays occur on the network.

- **Detecting Routing Problems:** Identifies incorrect routes or unreachable destinations.

Comparison Between Ping and Tracert

Command	Ping	Tracert (Traceroute)
Purpose	Checks if a device is reachable and measures round-trip time	Traces the path and measures delay across each hop to the destination
Response	Reply from the target with RTT (Round-Trip Time)	Displays the route and time taken for each hop (router) along the way
Output	Single reply time for each packet	Multiple hops with time taken for each hop
Use Case	Basic connectivity test and latency check	Diagnose routing problems, network delays, or packet loss along the path

Example Scenario: Troubleshooting Network Connectivity

1. Ping Test:

- You are unable to access a website. First, use **ping** to test if the website's server is reachable.

ping www.example.com

- If you get a reply, it confirms the server is reachable.
- If you get a timeout or unreachable message, it indicates a connectivity problem.

2. Traceroute Test:

- If the ping test fails, use **tracert** (or **tracert**) to check where the connection is breaking down.

tracert www.example.com

- Each hop will display the router addresses along the way. If the traceroute reaches a point where packets stop being returned, it shows where the network issue occurs.

Additional Tips:

- Use **ping -t** (Windows) or **ping -i** (Linux/macOS) to continuously ping a target and monitor real-time connectivity.
- **Tracert/Traceroute** results can show if there's a problem with a specific router or network segment. If a particular hop shows high latency or timeout, it may be the source of the problem.

Both **ping** and **tracert** are essential tools in the network engineer's toolkit for diagnosing connectivity issues and ensuring the network is functioning optimally.

• 3.6 Troubleshooting network issues.

(This will do at Wariyapola Lab #1)



04.Learn About Network Security

- **4.1 Basics of firewalls and intrusion detection/prevention systems (IDS/IPS).**

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are critical components of network security. They are designed to monitor, filter, and control network traffic to protect against unauthorized access, attacks, and malicious activity.

Firewalls

Overview:

A **firewall** is a network security device (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between trusted internal networks and untrusted external networks (e.g., the internet).

Types of Firewalls:

1. Packet-Filtering Firewall:

- Examines packets of data and filters them based on defined rules such as IP address, port number, or protocol type.
- **Stateless:** Each packet is evaluated in isolation without considering the state of previous packets.

2. Stateful Inspection Firewall:

- Tracks the state of active connections and makes decisions based on the context of the traffic, not just individual packets.
- **Stateful:** Maintains a table of active connections and ensures packets belong to established sessions.

3. Proxy Firewall:

- Acts as an intermediary between the user and the destination server. The proxy server evaluates requests and forwards or blocks them.
- Hides the internal network from external networks

4. Next-Generation Firewall (NGFW):

- Combines traditional firewall features with advanced capabilities like application awareness, deep packet inspection (DPI), intrusion prevention, and SSL decryption.
- Can inspect traffic at a much deeper level, including filtering traffic by application type, behavior, and context.

How Firewalls Work:

- Firewalls define rules that specify which traffic is allowed or denied based on various criteria such as:

- **IP addresses** (source and destination)
 - **Ports** (which services or applications are allowed)
 - **Protocols** (TCP, UDP, ICMP, etc.)
 - **Traffic direction** (incoming vs. outgoing)
- Firewalls can be configured to:
 - **Block** certain types of traffic (e.g., all inbound traffic from specific IP addresses).
 - **Allow** traffic from trusted sources (e.g., allowing only HTTP and HTTPS traffic from specific networks).

Firewall Examples:

- **Hardware firewalls:** Standalone devices, often used to protect entire networks.
- **Software firewalls:** Installed on individual computers or servers, protecting them from inbound and outbound threats.

Intrusion Detection Systems (IDS)

Overview:

An **Intrusion Detection System (IDS)** is a device or software application that monitors network or system activities for signs of malicious behavior or policy violations. An IDS alerts administrators when suspicious activity is detected but does not take action to prevent it.

Types of IDS:

1. **Network-Based IDS (NIDS):**
 - Monitors network traffic for signs of suspicious behavior or known attack patterns.
 - Typically placed at critical points in the network to analyze inbound and outbound traffic.
2. **Host-Based IDS (HIDS):**
 - Monitors activities on individual devices (e.g., servers, workstations).
 - Detects signs of malicious activity or breaches on the device, such as unauthorized file access or changes to system configurations.
3. **Signature-Based IDS:**
 - Compares network traffic or system activity against a database of known attack signatures (patterns of malicious behavior).
 - Can detect known attacks but is ineffective against new or unknown threats (zero-day attacks).
4. **Anomaly-Based IDS:**
 - Monitors baseline network behavior and flags activity that deviates from this baseline.
 - Can detect new or previously unknown attacks but may have higher false positives.

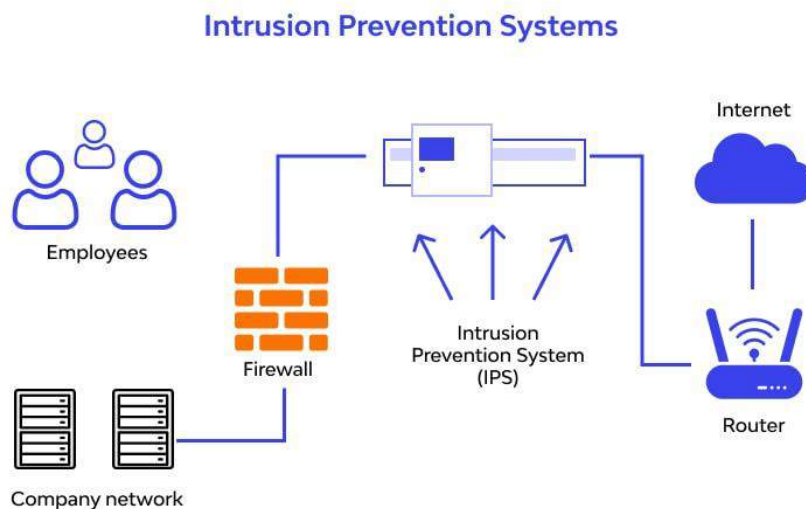
How IDS Works:

- IDS typically uses a combination of pattern matching (signature-based) and statistical analysis (anomaly-based) to detect malicious activity.
- Once an attack is detected, IDS systems generate an **alert** to notify network administrators.

Limitations:

- IDS is purely **reactive**, meaning it only detects and alerts on suspicious activity but does not prevent attacks.
- It may produce false positives (incorrectly flagging legitimate traffic as suspicious) or false negatives (failing to detect an actual attack).

Intrusion Prevention Systems (IPS)



Overview:

An **Intrusion Prevention System (IPS)** is similar to an IDS but goes a step further by actively blocking or preventing detected malicious activities in real-time.

How IPS Works:

- IPS sits in-line with network traffic, meaning that it can **block** malicious packets before they reach their destination.
- It uses similar detection methods to IDS (signature-based, anomaly-based, or a combination) but also takes action to **prevent** the attack from succeeding.

Types of IPS:

1. Network-Based IPS (NIPS):

- Monitors and protects network traffic at the perimeter of the network.
- Can block harmful traffic before it enters or exits the network.

2. Host-Based IPS (HIPS):

- Installed on individual devices to monitor traffic and activities on the host machine.
- Protects the host from attacks like buffer overflow, malware, and unauthorized access.

IPS vs IDS:

- **IDS:** Detects and alerts on suspicious activity.
- **IPS:** Detects and actively prevents suspicious activity.

Differences Between IDS and IPS

Feature	IDS	IPS
Function	Detects and alerts on threats	Detects and prevents threats
Action Taken	Alerts admins	Blocks malicious traffic
Placement	Can be passive, not in-line	In-line (actively filters traffic)
Response Time	Reactive (delayed response)	Proactive (real-time response)

How Firewalls, IDS, and IPS Work Together

- **Firewalls** act as the first line of defense, controlling and filtering network traffic based on predefined rules.
- **IDS** monitors for suspicious activity and sends alerts when it detects potential threats.
- **IPS** not only detects but also prevents malicious activity in real-time by blocking harmful traffic.
Together, these security devices form a multi-layered defense strategy:
- The **firewall** filters traffic to allow only legitimate access.
- The **IDS** provides alerts for potential threats.
- The **IPS** prevents malicious actions from being executed, ensuring comprehensive protection.

- **4.2 Secure protocols (HTTPS, SSL/TLS, SSH).**

Secure protocols are essential in ensuring the confidentiality, integrity, and authenticity of data transmitted over networks, especially on the internet. Let's look into **HTTPS**, **SSL/TLS**, and **SSH**—three fundamental protocols used to secure communications.

HTTPS (HyperText Transfer Protocol Secure)

Overview:

- **HTTPS** is the secure version of **HTTP** (HyperText Transfer Protocol). It is used to securely transmit data over the internet, particularly in web browsing.
- **HTTPS** encrypts the data between the client (browser) and the server using **SSL/TLS** protocols, making it harder for attackers to intercept or alter the data in transit.

How HTTPS Works:

- **Encryption:** **HTTPS** encrypts the communication between the client and the server, ensuring that any data sent (such as passwords, credit card information, etc.) cannot be easily intercepted or read by unauthorized parties.

- **Authentication:** It authenticates the server to ensure that the client is communicating with the correct server (and not an imposter or "man-in-the-middle").
- **Integrity:** HTTPS ensures the integrity of the transmitted data, meaning that it hasn't been tampered with during the transfer.

How It Works in Practice:

- When you visit a website that uses HTTPS, your browser will establish a secure connection to the server by using the **SSL/TLS** protocol to encrypt the communication.
- The website's **SSL/TLS certificate** contains a **public key** that is used to establish a secure, encrypted connection with the server.

Indication of HTTPS:

- In modern browsers, **HTTPS** is indicated by a **padlock icon** in the address bar, and the URL starts with "**https://**".
- If the connection is not secure, the browser will typically warn users with a "**Not Secure**" message.

SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Overview:

- **SSL** (Secure Sockets Layer) and its successor, **TLS** (Transport Layer Security), are cryptographic protocols that provide security over a network.
- SSL/TLS is most commonly used in HTTPS to encrypt web traffic, but it can also be used to secure other protocols such as email (SMTP, IMAP, POP3) and file transfer (FTP).
- While SSL is deprecated due to security vulnerabilities, TLS is still widely used and considered secure.

Key Features:

- **Encryption:** Encrypts data to prevent unauthorized parties from reading the transmitted data.
- **Integrity:** Uses **message authentication codes (MACs)** to ensure the integrity of the transmitted data, preventing tampering during transmission.
- **Authentication:** Ensures the identity of the communicating parties, typically through the use of digital certificates (which contain public keys).

SSL/TLS Handshake:

1. **Client Hello:** The client sends a message to the server to start the process, which includes supported encryption methods.
2. **Server Hello:** The server responds with its choice of encryption, sending its **SSL/TLS certificate**, which contains the public key.
3. **Key Exchange:** The client and server exchange keys (using asymmetric encryption) to establish a shared secret key for symmetric encryption.
4. **Data Transfer:** Data is transmitted using the established encryption key.

5. **Connection Termination:** When the session is complete, the client and server signal each other to safely terminate the secure connection.

SSL/TLS in HTTPS:

- When a website uses **HTTPS**, the browser and the server use SSL/TLS to encrypt the connection.
- SSL/TLS certificates are issued by **Certificate Authorities (CAs)**, which verify the identity of the server and help establish trust between the client and the server.

TLS Versions:

- **SSL** (now obsolete) was replaced by **TLS** because SSL had known vulnerabilities.
- The most commonly used versions of TLS today are **TLS 1.2** and **TLS 1.3**, with TLS 1.3 being the most recent and secure version.

SSH (Secure Shell)

Overview:

- **SSH** is a secure network protocol that provides a way to securely access and manage devices (like servers and network devices) over an unsecured network (e.g., the internet).
- SSH is primarily used for remote login, remote command execution, and secure file transfers (SFTP or SCP).
- It replaces older protocols such as **Telnet** and **rlogin**, which transmitted data, including usernames and passwords, in plain text, making them vulnerable to eavesdropping.

Key Features:

- **Encryption:** SSH uses encryption to secure the entire communication session, including authentication and data transfer.
- **Authentication:** SSH supports multiple forms of authentication, such as:
 - **Password-based:** The user enters a password for authentication.
 - **Public key-based:** The user generates a private-public key pair. The public key is stored on the server, and the user authenticates using the private key.
- **Data Integrity:** SSH ensures data integrity by using cryptographic checksums, which prevent the data from being tampered with in transit.
- **Port Forwarding:** SSH allows for tunneling of other protocols (e.g., HTTP or FTP) through the encrypted SSH connection.

How SSH Works:

- **Client and Server:** SSH operates using a client-server model. The client initiates the connection to the SSH server, typically using an SSH client like OpenSSH, PuTTY, or a terminal with SSH support.
- **Authentication:** The client must authenticate itself to the server. This can be done using either passwords or public-private key pairs.

- **Secure Connection:** After authentication, a secure encrypted session is established, allowing the client to execute commands or transfer files.

Example of Using SSH:

ssh username@hostname_or_ip_address

This command will initiate an SSH connection to the specified **hostname** or **IP address** using the provided **username**.

SSH Use Cases:

- **Remote Administration:** Admins can securely log into remote servers to configure, maintain, or troubleshoot them.
- **File Transfers:** SSH supports secure file transfers through **SFTP** (SSH File Transfer Protocol) or **SCP** (Secure Copy Protocol).
- **Tunneling and Port Forwarding:** SSH can tunnel other protocols, enabling secure access to internal network services over the internet.

Summary of Secure Protocols

Protocol	Purpose	Encryption	Common Use Cases
HTTPS	Secure communication for web browsing	Uses SSL/TLS for encryption	Securing web traffic (e.g., online banking, e-commerce)
SSL/TLS	Secure data transmission over networks	Provides encryption, integrity, and authentication	HTTPS, secure email, VPNs, and other secure protocols
SSH	Secure remote access and command execution	Provides strong encryption, authentication, and integrity	Remote server management, file transfers (SFTP, SCP), port forwarding

- **HTTPS** secures web traffic by encrypting data with SSL/TLS, ensuring privacy and integrity.
- **SSL/TLS** protocols provide secure communication for a variety of services, not just web traffic, and ensure the authenticity of the server.
- **SSH** offers secure access to remote systems, providing encrypted sessions for command execution and file transfers.

These protocols form the foundation of secure communication on the internet and are critical in safeguarding sensitive data from unauthorized access or tampering.

- **4.3 Understanding common threats like DDoS, man-in-the-middle (MITM) attacks, and phishing.**

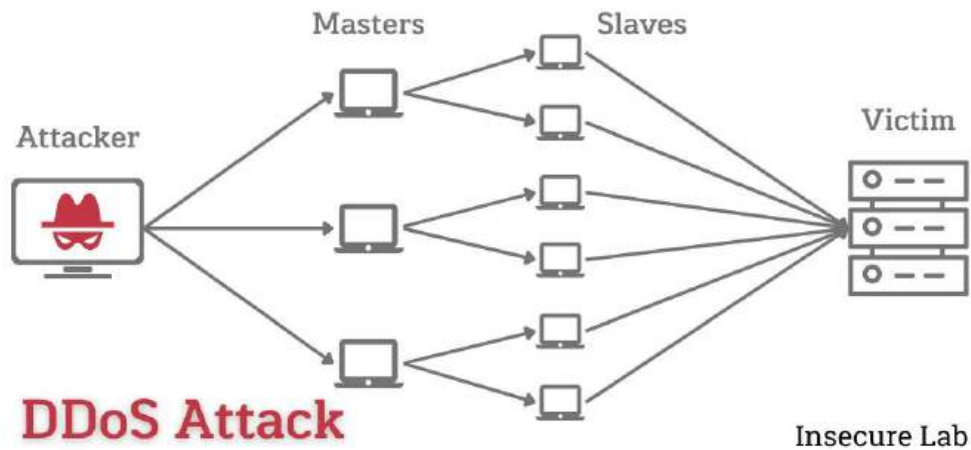
Network security threats are constantly evolving, and understanding the common types of attacks is crucial in defending against them. Some of the most common threats include DDoS attacks, Man-in-the-Middle (MITM) attacks, and Phishing. Let's explore each one:

DDoS (Distributed Denial of Service) Attack

Overview:

A **DDoS attack** is an attempt to overwhelm a target (usually a server, website, or network) with an excessive amount of traffic, causing it to become unavailable to legitimate users. The attack is **distributed**, meaning that it is carried out by many different machines or devices that can be controlled remotely, often without the owners' knowledge.

How DDoS Works:



- **Botnets:** Attackers often use a **botnet**, a network of infected devices (often called **zombies**) that can be controlled remotely. These devices may include computers, IoT devices, and other networked hardware.
- **Flooding Traffic:** The attacker directs the botnet to flood the target server or network with massive amounts of traffic, overwhelming the target's resources (such as bandwidth, memory, or CPU power).
- **Targeting Resources:** DDoS can target a variety of resources:
 - **Network layer:** Floods the network to consume bandwidth (e.g., SYN flood, UDP flood).
 - **Application layer:** Overloads specific services or applications (e.g., HTTP request floods).

Effects of DDoS:

- **Downtime:** The targeted website or service becomes unavailable, leading to business disruptions.
- **Loss of revenue:** Prolonged downtime can lead to loss of customers and revenue.
- **Damage to reputation:** Ongoing service outages can damage the organization's reputation.

Mitigation:

- **Traffic Filtering:** Use services like Cloudflare or Akamai to filter malicious traffic.

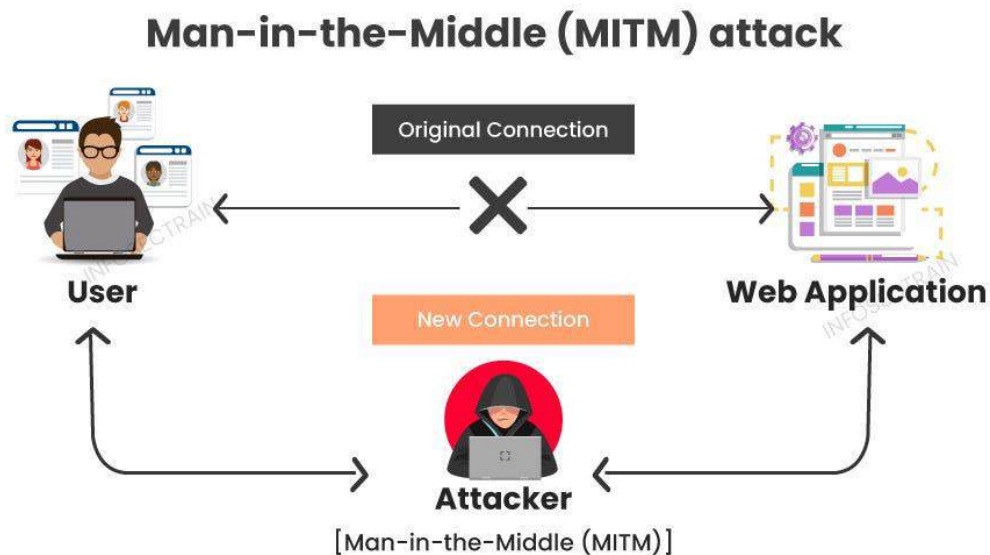
- **Rate Limiting:** Limit the number of requests a user can make in a short period of time.
- **Content Delivery Networks (CDNs):** Distribute traffic to multiple locations to balance load and reduce attack impact.
- **Firewalls and Intrusion Detection Systems (IDS):** Employ advanced firewalls and IDS to detect and block unusual traffic patterns.

Man-in-the-Middle (MITM) Attack

Overview:

A **Man-in-the-Middle (MITM) attack** occurs when an attacker intercepts and potentially alters the communication between two parties without their knowledge. This can happen in any form of communication, such as web browsing, emails, or any form of data transfer.

How MITM Works:



- **Interception:** The attacker positions themselves between the victim and the legitimate endpoint (such as a website or server). This can happen in a variety of ways:
 - **On a Wi-Fi network:** An attacker may set up a rogue Wi-Fi hotspot to intercept communication between the victim and the internet.
 - **DNS Spoofing:** The attacker redirects the victim's requests to a malicious website by corrupting DNS records.
 - **SSL Stripping:** The attacker downgrades a secure HTTPS connection to HTTP and intercepts the unencrypted data.
- **Data Manipulation:** Once the communication is intercepted, the attacker can:
 - **Eavesdrop:** Read sensitive information like usernames, passwords, credit card numbers, etc.

- **Modify Data:** Change data being sent between parties, such as altering a bank transaction or injecting malicious code into a website.

Effects of MITM:

- **Data Theft:** Sensitive information such as passwords, credit card numbers, and confidential business data can be stolen.
- **Altered Transactions:** The attacker can change messages, causing fraud or system malfunctions.
- **Loss of Trust:** MITM attacks can undermine user trust, especially in financial transactions or communications.

Mitigation:

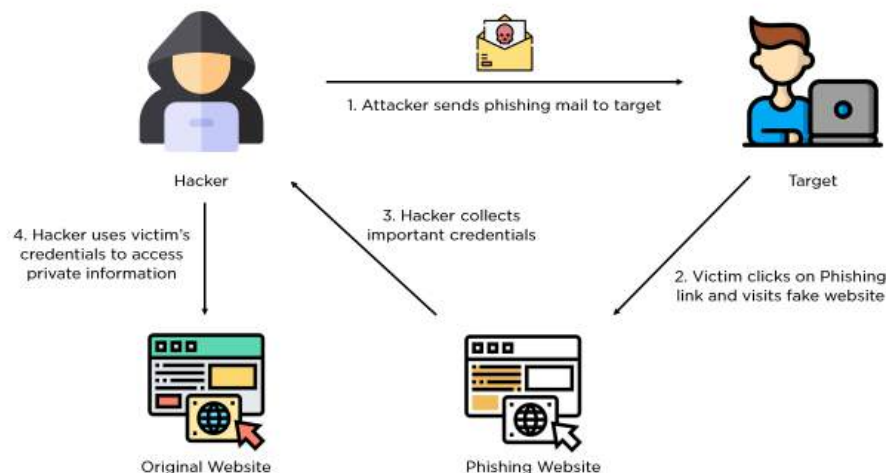
- **Encryption:** Use **HTTPS (SSL/TLS)** for all communications to ensure that data is encrypted and cannot be intercepted in plain text.
- **Public Key Infrastructure (PKI):** Employ strong certificate validation methods to prevent attackers from impersonating legitimate servers.
- **Multi-Factor Authentication (MFA):** Use additional layers of security (e.g., one-time passwords, biometrics) to verify the identity of users.
- **Secure Wi-Fi:** Avoid using unsecured Wi-Fi networks for sensitive transactions, and use a Virtual Private Network (VPN) when necessary.

Phishing Attack

Overview:

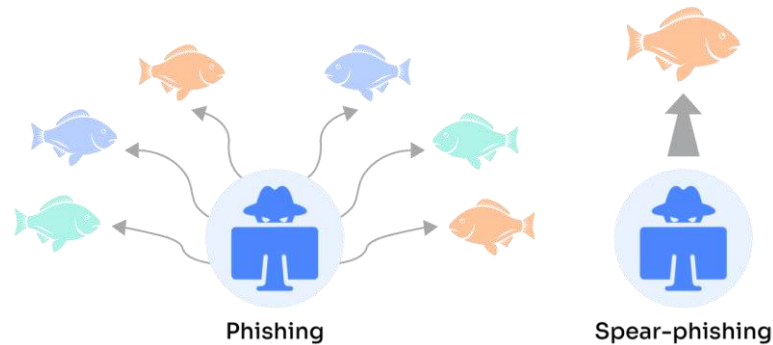
Phishing is a type of social engineering attack where the attacker impersonates a legitimate entity (such as a bank, service provider, or colleague) to deceive the victim into divulging sensitive information such as login credentials, financial data, or personal information.

How Phishing Works:



- **Email Phishing:** The most common form of phishing, where an attacker sends a fake email that appears to come from a trusted source. The email may contain:
 - **Malicious links:** Clicking the link may lead to a fake website designed to steal login credentials or infect the victim's system with malware.

- **Attachments:** Opening attachments may infect the victim's computer with viruses or ransomware.
- **Spear Phishing:** A more targeted form of phishing where the attacker customizes the message to a specific individual, often with personal information to make the attack more convincing.



- **Vishing (Voice Phishing):** Involves phone calls instead of emails. The attacker pretends to be from a legitimate organization and attempts to extract sensitive information.
- **Smishing (SMS Phishing):** Phishing via text messages where attackers send fake messages asking the victim to click on a link or provide personal information.

Effects of Phishing:

- **Data Breaches:** Attackers can steal personal and financial data, leading to identity theft or fraud.
- **Malware Infection:** Phishing emails often contain malicious links or attachments that can infect the victim's device with malware.
- **Financial Loss:** Victims may lose money if they disclose financial details or fall for fraudulent transactions.

Mitigation:

- **Awareness Training:** Educate users about the dangers of phishing, how to recognize suspicious emails, and how to avoid falling for phishing scams.
- **Email Filtering:** Use email security solutions that can detect and filter phishing emails.
- **Two-Factor Authentication (2FA):** Even if login credentials are compromised, two-factor authentication adds an extra layer of security.
- **Verify Links:** Hover over links in emails to check the actual URL and ensure it matches the expected destination.

- **Avoid Clicking Suspicious Links:** Do not click on links or open attachments from unknown or unsolicited sources.

Summary of Common Network Security Threats

Threat	Description	Effects	Mitigation
DDoS (Distributed Denial of Service)	Overloads a network or server with excessive traffic, making it unavailable.	Service downtime, loss of revenue, damage to reputation.	Traffic filtering, rate limiting, use of CDNs, firewalls, IDS/IPS.
MITM (Man-in-the-Middle)	An attacker intercepts and alters communication between two parties.	Data theft, altered transactions, loss of trust.	HTTPS, certificate validation, multi-factor authentication (MFA), secure Wi-Fi, VPNs.
Phishing	Deceptive attempt to obtain sensitive information via email, phone, or text.	Data breaches, malware infections, financial loss.	Awareness training, email filtering, 2FA, verify links, avoid suspicious messages.

Understanding these common threats—**DDoS**, **MITM**, and **Phishing**—is vital in securing networks and personal data. Protecting against these threats requires a combination of technology (like encryption and firewalls), user awareness, and proactive security measures. By staying informed and adopting strong security practices, you can mitigate the risks posed by these common network security threats.

05. Understand Wi-Fi and Wireless Networking

- **5.1 Learn about Wi-Fi standards (e.g., 802.11b/g/n/ac/ax).**

Wi-Fi standards are developed by the **IEEE (Institute of Electrical and Electronics Engineers)** and define the protocols and technologies for wireless communication over short distances. These standards determine the speed, frequency, range, and security of Wi-Fi networks. The most commonly used Wi-Fi standards are **802.11b**, **802.11g**, **802.11n**, **802.11ac**, and **802.11ax**. Each successive standard provides improvements in speed, coverage, and capabilities.

1. 802.11b (1999)

Overview:

- **Frequency:** Operates on the **2.4 GHz** band.
- **Maximum Speed:** Up to **11 Mbps**.
- **Range:** Typically around **100-150 feet** indoors.
- **Compatibility:** Most commonly supported in early Wi-Fi devices.

Pros:

- Widely supported in older devices.
- Fairly simple and inexpensive to implement.

Cons:

- Relatively slow speeds compared to newer standards.
 - Prone to interference from other devices that operate on the 2.4 GHz band (e.g., microwaves, Bluetooth devices).
-

2. 802.11g (2003)

Overview:

- **Frequency:** Operates on the **2.4 GHz** band (same as 802.11b).
- **Maximum Speed:** Up to **54 Mbps**.
- **Range:** Similar to 802.11b, typically around **100-150 feet** indoors.
- **Compatibility:** Backward compatible with 802.11b.

Pros:

- Much faster than 802.11b, with speeds suitable for basic internet browsing and streaming.
- Backward compatibility with 802.11b allows older devices to connect.

Cons:

- Still uses the congested 2.4 GHz band, which can result in interference and slower speeds.
 - Limited by the 2.4 GHz band's bandwidth, meaning the maximum speed is not sufficient for high-bandwidth applications like HD streaming.
-

3. 802.11n (2009)

Overview:

- **Frequency:** Operates on both **2.4 GHz** and **5 GHz** bands (dual-band).
- **Maximum Speed:** Up to **600 Mbps** (depending on the number of antennas and channels).
- **Range:** Better range than 802.11b/g, with improved coverage (about **150-200 feet** indoors).
- **Compatibility:** Backward compatible with 802.11b/g.

Pros:

- Dual-band operation (2.4 GHz and 5 GHz) allows for less interference and higher speeds.
 - **MIMO (Multiple Input, Multiple Output)** technology allows for better performance and increased range.
 - Faster speeds are ideal for HD video streaming, online gaming, and file transfers.

Cons:

- While better than earlier standards, 802.11n can still be impacted by congestion on the 2.4 GHz band.
-

4. 802.11ac (2013)

Overview:

- **Frequency:** Operates on the **5 GHz** band.
- **Maximum Speed:** Up to **1.3 Gbps** (depending on the number of channels and antennas).
- **Range:** Similar to 802.11n, but can be impacted by obstacles (around **100-150 feet** indoors).
- **Compatibility:** Backward compatible with 802.11a/n.

Pros:

- **Faster speeds** and greater bandwidth, ideal for activities like HD video streaming, large file transfers, and online gaming.
- Operates on the **5 GHz** band, which is less congested than the 2.4 GHz band.
- Supports **MU-MIMO (Multi-User, Multiple Input, Multiple Output)**, enabling simultaneous communication with multiple devices.

Cons:

- Shorter range compared to 2.4 GHz, meaning the signal may not reach as far in large spaces or through walls.
- **5 GHz** band has more difficulty penetrating obstacles like walls and floors.

5. 802.11ax (Wi-Fi 6) (2019)

Overview:

- **Frequency:** Operates on both **2.4 GHz** and **5 GHz** bands (dual-band).
- **Maximum Speed:** Up to **9.6 Gbps** (theoretical maximum; real-world speeds are typically lower).
- **Range:** Improved range compared to 802.11ac.
- **Compatibility:** Backward compatible with older Wi-Fi standards.

Pros:

- **Higher speeds** (up to 9.6 Gbps) and increased bandwidth to handle more devices, making it ideal for busy networks like public places, smart homes, and offices.
- **OFDMA (Orthogonal Frequency Division Multiple Access)** improves efficiency by dividing channels into smaller sub-channels, allowing multiple devices to use the same channel simultaneously without causing interference.
- **TWT (Target Wake Time)** allows devices to schedule when they wake up and communicate with the router, reducing power consumption.
- **Improved performance in crowded areas**, with better support for high-density environments like stadiums, airports, and offices.
- Supports **MU-MIMO** for simultaneous communication with multiple devices.

Cons:

- **Requires newer devices** that support Wi-Fi 6 to fully utilize the benefits (older devices are not compatible).
- **Higher cost** for routers and devices that support Wi-Fi 6.

Comparison of Wi-Fi Standards

Standard	Max Speed	Frequency Bands	Range	Key Features
802.11b	11 Mbps	2.4 GHz	100-150 feet	Older standard, slow speed, susceptible to interference.
802.11g	54 Mbps	2.4 GHz	100-150 feet	Faster than 802.11b, but still limited by the 2.4 GHz band.
802.11n	600 Mbps	2.4 GHz and 5 GHz	150-200 feet	Dual-band, MIMO technology, faster speeds.
802.11ac	1.3 Gbps	5 GHz	100-150 feet	Faster speeds, operates on 5 GHz, MU-MIMO support.
802.11ax	9.6 Gbps	2.4 GHz and 5 GHz	Improved range	Wi-Fi 6, improved efficiency, supports more devices, better performance in crowded areas.

Wi-Fi 6E (2021): Extended Bandwidth with 6 GHz

- **Wi-Fi 6E** extends the **802.11ax (Wi-Fi 6)** standard to include the **6 GHz** band, offering additional channels to avoid congestion and improve performance in crowded areas.
- It provides higher capacity and reduced latency, making it ideal for high-bandwidth activities like 4K/8K video streaming, virtual reality (VR), and gaming.

Each Wi-Fi standard is designed to meet the demands of modern wireless communication. **Wi-Fi 6 (802.11ax)** represents the most current and fastest technology, offering better efficiency, speed, and support for more devices in dense environments. While older standards like **802.11b/g/n/ac** are still used in some legacy devices, upgrading to a newer Wi-Fi standard can greatly improve performance, speed, and reliability in both home and business networks.

When setting up a network, it's important to consider the specific needs of your environment, including the number of devices, type of applications, and coverage area, to choose the best Wi-Fi standard for your situation.

40 mini

- **5.2 Practice configuring a wireless router and securing it (WPA3, strong passwords).**

Configuring a wireless router and securing it is crucial for ensuring your network is fast, reliable, and safe from unauthorized access. Below are the steps for configuring a wireless router and securing it using **WPA3 encryption** and strong passwords.

1. Access the Router's Admin Interface

To begin the configuration process, you'll need to access the router's admin interface. Here's how:

1. Connect to the router:

- Use a computer or mobile device connected to the router (either via Ethernet cable or Wi-Fi).

2. **Open a web browser** and enter the router's IP address (usually something like 192.168.1.1 or 192.168.0.1). Check the router's manual or sticker on the device for the correct IP address if you're unsure.
 3. **Login to the router:**
 - The default login credentials (username and password) are often "admin" for both, or "admin" for the username and "password" for the password. If you don't know the login credentials, check the router's manual or sticker.
 - **Change the default password immediately** to something strong once logged in.
-

2. Basic Router Configuration

Once you're logged into the router's interface, follow these steps to configure basic settings:

Set up the Router's Name (SSID):

1. Go to the **Wireless Settings** section of the admin interface.
2. **Change the default SSID (Service Set Identifier)** to something unique but not too personal (e.g., "HomeWiFi2024").
3. **Disable SSID broadcast** if you want to hide the network from general scanning. This will make it harder for unauthorized users to detect your network.

Configure the Wireless Network:

1. Choose the **Wi-Fi standard** (e.g., **802.11n**, **802.11ac**, or **802.11ax**), depending on what your router supports.
 2. Select the **radio band** (2.4 GHz or 5 GHz). Use 5 GHz for faster speeds if you are close to the router, and use 2.4 GHz for broader coverage if you need the signal to travel farther.
-

3. Set Up WPA3 Encryption

WPA3 is the latest and most secure Wi-Fi encryption standard. It is more resistant to attacks compared to older standards like **WPA2** and **WEP**. Here's how to enable WPA3:

1. **Go to the Wireless Security Settings** in the router's admin interface.
2. Under the **security mode**, select **WPA3-Personal** or **WPA3-Enterprise** (depending on your router's options).
 - **WPA3-Personal** is recommended for home users and offers better protection for personal devices.
 - **WPA3-Enterprise** is intended for larger networks with higher security needs.
3. If WPA3 is unavailable (some older routers may not support WPA3), choose **WPA2/WPA3 Mixed Mode** as an alternative. This allows devices that support WPA3 to use it, while devices that support only WPA2 can still connect.

Why WPA3?

- WPA3 provides **better encryption** for passwords, **protects against brute-force attacks**, and uses **forward secrecy**, meaning even if a password is compromised, previous sessions cannot be decrypted.
- **Improved security** for public networks with **Easy Connect** and **Protected Management Frames (PMF)**.

4. Set a Strong Password

Now that WPA3 encryption is enabled, you need a strong password to secure your Wi-Fi network. A weak password is one of the easiest ways for attackers to access your network.

Tips for a Strong Wi-Fi Password:

1. **Length:** At least 12-16 characters.
2. **Complexity:** Include a mix of **uppercase, lowercase, numbers, and special characters.**
3. **Avoid Common Words:** Don't use easily guessable words like your name, address, or common phrases.
4. **Random Passwords:** Consider using a password manager to generate and store a random password.

Example of a strong password: 9SzQ&8fR!s1B@t^L7w

5. Disable Unnecessary Features

For additional security, disable any features that you don't need:

- **WPS (Wi-Fi Protected Setup):** While WPS is convenient for quickly connecting devices, it is vulnerable to attacks. It's best to disable it unless absolutely needed.
 - **Remote Management:** Turn off the ability to manage your router from outside your network. You don't want anyone accessing your router settings from the internet.
 - **UPnP (Universal Plug and Play):** Disabling UPnP can prevent certain security vulnerabilities, especially in home networks.
-

6. Update Router Firmware

Keeping your router's firmware up-to-date is crucial for both security and performance. Router manufacturers often release updates that fix vulnerabilities and improve the functionality of the device.

1. Go to the **Firmware Update** section of the router's admin interface.
 2. Check for the **latest firmware version.**
 3. If an update is available, follow the instructions to update the firmware. **Do not interrupt** the process, as it could brick the router.
-

7. Enable the Router's Firewall

Most modern routers come with a built-in **firewall** that helps block unauthorized traffic from entering your network. Make sure this is enabled.

1. Go to the **Firewall** or **Security** section of the router's admin interface.
 2. Ensure the **firewall is enabled.**
 3. Optionally, configure any advanced firewall rules based on your needs (e.g., blocking specific ports or limiting access from certain IP addresses).
-

8. Monitor Your Network

- **Connected Devices:** Keep track of which devices are connected to your network. Most routers have a section where you can see the list of devices currently using your Wi-Fi.

- **Logs:** Regularly check the router's logs to identify any suspicious activity or unauthorized access attempts.
-

9. Test the Wi-Fi Security

Once everything is set up, it's important to test the security of your Wi-Fi network:

- **Try to connect to your Wi-Fi network** from a device that does not know the password. It should prompt for the WPA3 password before allowing access.
 - Use tools like **Wi-Fi Analyzer** (Android) or **WiFi Explorer** (macOS) to check your Wi-Fi signal and see if your SSID is visible to unauthorized users. If you chose to hide the SSID, it should not appear in scans.
-

Configuring and securing your wireless router is crucial for protecting your home or office network from threats and ensuring a reliable connection for all your devices. By enabling WPA3 encryption, setting a strong password, and regularly monitoring your network, you can significantly improve the security and performance of your Wi-Fi network. Always remember to keep your router's firmware up-to-date and disable unnecessary features to minimize potential vulnerabilities.

06.Experiment with Tools

- **6.1 Network Analyzers: Tools like Wireshark to analyze and troubleshoot networks.**

Network analyzers, or **packet sniffers**, are tools used to capture and analyze network traffic. They help identify problems, monitor network performance, and ensure security by examining the data being transmitted across the network. **Wireshark** is one of the most popular and powerful network analyzers available. It allows network administrators, security professionals, and developers to inspect network packets in real-time.

1. What is a Network Analyzer?

A **network analyzer** is a tool that captures and inspects the data packets traveling through a network. These tools help in:

- **Diagnosing network issues** like slow performance, dropped connections, or configuration errors.
- **Troubleshooting security problems** like identifying unusual traffic or network attacks.
- **Monitoring network activity** to ensure all communication is legitimate and authorized.

Wireshark is a packet analyzer that allows you to view the contents of data packets that travel across a network, helping you understand how communication occurs between network devices.

Introduction to Wireshark

Wireshark is a free, open-source tool used for network troubleshooting, analysis, and packet inspection. It captures packets in real-time and displays the information in a

detailed manner, allowing you to analyze traffic at various levels (link, network, transport, and application layers).

Wireshark Features:

- **Live capture and offline analysis:** You can capture packets in real-time or analyze saved packet capture files (.pcap).
 - **Deep inspection:** Wireshark provides deep inspection of hundreds of network protocols (e.g., HTTP, DNS, FTP, TCP/IP, and more).
 - **Filters:** Powerful filtering options to narrow down to specific types of traffic (e.g., by IP address, port, protocol).
 - **Packet decoding:** Wireshark can decode packets into human-readable formats, making it easier to understand the contents of communication.
 - **Graphical interface:** Wireshark's graphical user interface (GUI) provides an intuitive way to analyze packets, whereas it also supports command-line tools for automation.
-

3. Installing Wireshark

Wireshark is available for various operating systems, including Windows, macOS, and Linux. Here's how to install Wireshark on your system:

On Windows:

1. Download Wireshark from the official website: [Wireshark Download](#).
2. Run the installer and follow the prompts.
3. During installation, you can choose to install **WinPcap** or **Npcap** (required for packet capturing).

Capturing Packets with Wireshark

After installing Wireshark, follow these steps to capture network packets:

1. **Launch Wireshark:** Open the application.
2. **Select the network interface:** Choose the network interface (e.g., Ethernet or Wi-Fi) you want to capture traffic from. If you're using Wi-Fi, you may need to run Wireshark with elevated privileges (admin rights) to capture packets.
3. **Start capturing packets:** Click on the interface, and Wireshark will start capturing packets in real-time.
4. **Stop the capture:** After capturing the traffic, click the red square button in Wireshark to stop the capture.

Analyzing Packets with Wireshark

Once you've captured some packets, Wireshark provides several features to help analyze the data:

Packet List:

- The **Packet List** pane shows all captured packets in a list format.
- Each packet is displayed with details like the time of capture, source and destination IP addresses, protocol, and length.

Packet Details:

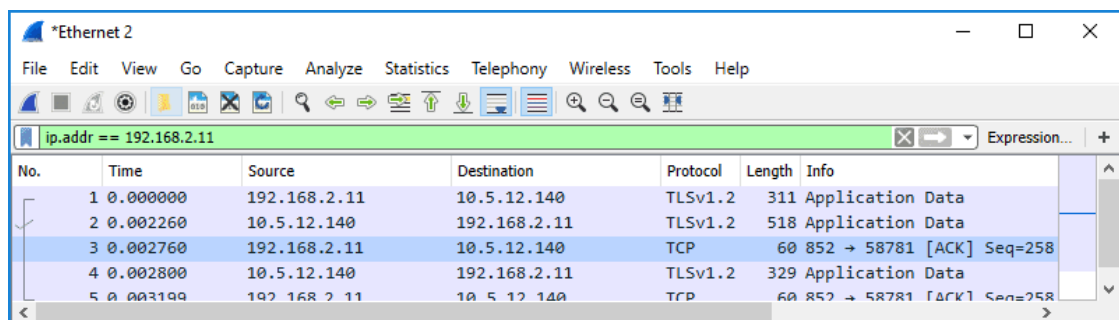
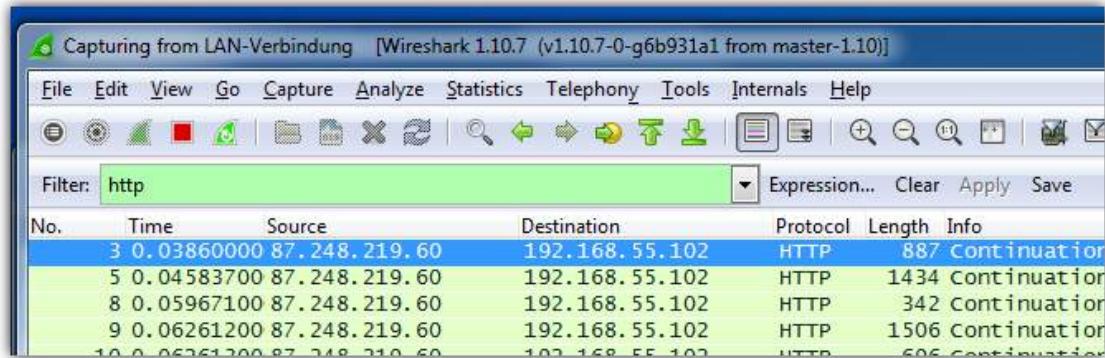
- The **Packet Details** pane shows a more detailed breakdown of a selected packet, displaying headers and protocols layer-by-layer (e.g., Ethernet, IP, TCP, HTTP).

Packet Bytes:

- The **Packet Bytes** pane shows the raw binary data of the selected packet in hexadecimal format.

Applying Filters:

Wireshark supports **display filters**, which allow you to focus on specific traffic. For example:



ip.addr == 192.168.1.1 && ip.addr == 192.168.1.2

To capture traffic from a specific IP address: **ip.src == 192.168.1.1**

To capture packets of a particular protocol (e.g., TCP, DNS, FTP): **tcp**

Follow TCP Streams:

- Wireshark allows you to "follow" a **TCP stream** (or other protocols) to see the entire conversation between two hosts, which is useful for analyzing web sessions, emails, etc.
- To do this, right-click on a TCP packet and select **Follow → TCP Stream**. This will display the entire communication in a readable format.

Common Use Cases for Wireshark

Wireshark is useful in various network troubleshooting and analysis scenarios, including:

Troubleshooting Network Issues:

- **Slow network performance:** Capture packets to identify bottlenecks, retransmissions, or congestion points.

- **Dropped packets:** Use Wireshark to identify lost or corrupted packets, which could indicate network issues or congestion.

Security Monitoring:

- **Identifying suspicious traffic:** Monitor for signs of **DDoS attacks**, **MITM attacks**, or abnormal traffic patterns.
- **Detecting malicious activity:** Look for unexpected open ports, suspicious IP addresses, or signs of malware activity.

Protocol Analysis:

- **Understanding network protocols:** Wireshark is a great tool for learning how various protocols work by examining their packets in detail.

Verifying Application Behavior:

- **Debugging application communication:** If an application is experiencing network issues, use Wireshark to verify that the application is sending and receiving the expected packets.

Best Practices for Using Wireshark

- **Capture with proper authorization:** Make sure you have permission to capture packets on the network, as packet sniffing can raise privacy and security concerns.
- **Limit the capture scope:** Capture only relevant traffic by applying filters to reduce the volume of data and focus on the problem at hand.
- **Save your captures:** Save packet captures (.pcap files) for later analysis or sharing with other team members.
- **Use Wireshark's built-in tools:** Leverage Wireshark's tools for protocol statistics, flow graphs, and expert analysis to quickly spot issues.

Wireshark is an essential tool for network administrators, security professionals, and anyone working with network traffic. It provides a detailed view of packet-level data, which can be invaluable in troubleshooting network problems, analyzing performance, and ensuring network security. By learning how to effectively capture and analyze packets using Wireshark, you'll gain insights into how networks function and how to resolve various issues that may arise in your network environment.

- **6.2 Command-Line Tools: Learn networking commands like ipconfig, ifconfig, netstat, and nslookup.**

Command-line tools are essential for troubleshooting, diagnosing, and configuring network-related issues. These tools allow network administrators and users to gather information about the network, troubleshoot connectivity problems, and configure network interfaces. Some of the most commonly used networking commands include **ipconfig**, **ifconfig**, **netstat**, and **nslookup**.

1. ipconfig (Windows)

ipconfig (Internet Protocol Configuration) is a command-line tool used on Windows systems to view and manage network interfaces and their configurations.

Common Uses of ipconfig:

- **View IP configuration:** To display the current IP address, subnet mask, and default gateway for all network interfaces:

```

Command Prompt

C:\Users\Ravi_NZ_PC>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 5:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2407:c00:4004:25ef:5004:b805:8528:4
    IPv6 Address. . . . . : 2407:c00:4004:25ef:a9c2:9c93:f25c:b001
    Temporary IPv6 Address. . . . . : 2407:c00:4004:25ef:61ab:1ada:a012:eb9c
    Link-local IPv6 Address . . . . . : fe80::c1f8:2555:217:d26%16
    IPv4 Address. . . . . : 192.168.8.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::5204:b8ff:fe05:8528%16
                                192.168.8.1

C:\Users\Ravi_NZ_PC>

```

View detailed information: To show detailed information about all network adapters (including DNS and DHCP): **ipconfig /all**

Release and renew IP address: When troubleshooting issues with network connectivity, you can release the current IP address and request a new one from the DHCP server: **ipconfig /flushdns**

Renew the IP: **ipconfig /renew**

Flush DNS cache: If you are facing issues with resolving domain names, you can clear the DNS resolver cache: **ipconfig /flushdns**

netstat (Network Statistics)

netstat (Network Statistics) is a command-line tool used to display network connections, routing tables, and interface statistics. It is available on most operating systems, including Windows, Linux, and macOS.

Common Uses of netstat:

View active network connections: To see all active connections (TCP and UDP), including local and remote addresses:

C:\Users\Ravi_NZ_PC>netstat

Show listening ports: To display all ports currently in the listening state (useful for checking services running on your machine): **netstat -a**

Show detailed connection information: To show information about active TCP connections, including the process ID (PID) of the service using the connection:

netstat -an

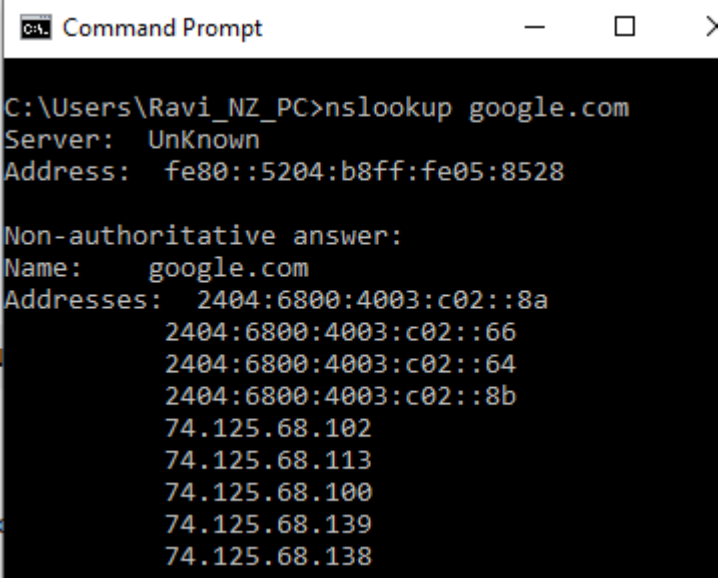
Show routing table: To display the system's routing table, which shows how packets are routed across the network: **netstat -r**

View network interface statistics: To see the statistics for each network interface, such as data packets sent and received: **netstat -i**

nslookup (Name Server Lookup)

nslookup (Name Server Lookup) is a tool used for querying Domain Name System (DNS) records. It allows you to find the IP address associated with a domain name (forward lookup) or find the domain name associated with an IP address (reverse lookup)

Find the IP address of a domain: To resolve a domain name (e.g., google.com) to an IP address: **nslookup google.com**



```
Command Prompt
C:\Users\Ravi_NZ_PC>nslookup google.com
Server: UnKnown
Address: fe80::5204:b8ff:fe05:8528

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4003:c02::8a
           2404:6800:4003:c02::66
           2404:6800:4003:c02::64
           2404:6800:4003:c02::8b
           74.125.68.102
           74.125.68.113
           74.125.68.100
           74.125.68.139
           74.125.68.138
```

Find the domain name for an IP address: To perform a reverse lookup and find the domain name for a given IP address: **nslookup 8.8.8.8**

Use a specific DNS server: By default, nslookup uses your system's configured DNS server. You can specify a different DNS server for the query:

nslookup google.com 8.8.8.8

Get specific DNS record types: You can use nslookup to query different types of DNS records, such as A, MX, or TXT records. For example, to get MX records (Mail Exchange) for a domain: **nslookup -type=MX google.com**

Interactive mode: You can enter interactive mode to perform multiple queries without typing nslookup each time. Just type nslookup and press Enter, then use commands like **set type=MX** to query different record types.

nslookup

> set type=MX

> google.com

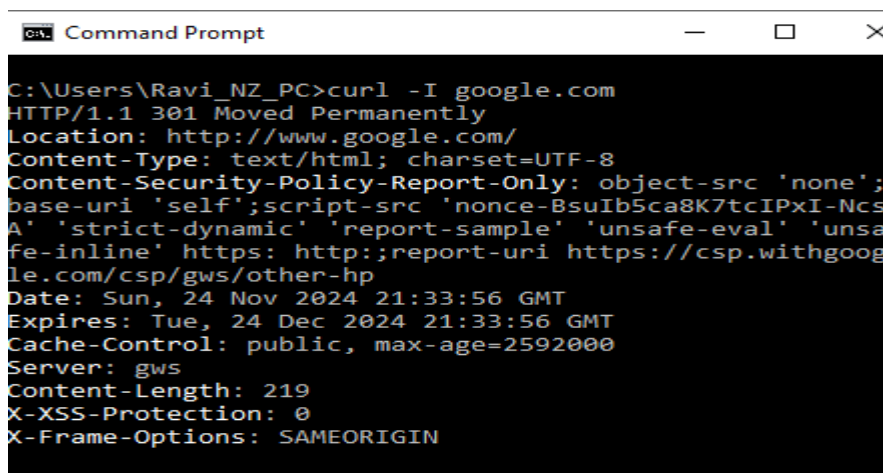
To send a specific number of packets → ping -n 4 google.com

Traceroute (Windows: tracert, Linux/macOS: traceroute):

- **Trace the route packets take:** Traces the path that packets take to reach a destination, showing the intermediate routers.
 - On Windows: → tracert google.com

Test HTTP/HTTPS connections: Used to test web server connectivity and fetch headers or content.

curl -I google.com



```
cmd Command Prompt
C:\Users\Ravi_NZ_PC>curl -I google.com
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';
base-uri 'self';script-src 'nonce-BsuIb5ca8K7tcIPxI-Ncs
A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsa
fe-inline' https: http:;report-uri https://csp.withgoog
le.com/csp/gws/other-hp
Date: Sun, 24 Nov 2024 21:33:56 GMT
Expires: Tue, 24 Dec 2024 21:33:56 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

Telnet:

- **Test specific port connectivity:** Used to test if a particular port is open on a remote host

telnet google.com 80

Understanding and using these command-line networking tools is essential for diagnosing network problems, configuring network interfaces, and troubleshooting connectivity issues. By mastering commands like ipconfig, ifconfig, netstat, and nslookup, you will be better equipped to monitor network traffic, troubleshoot issues, and ensure smooth network operation. These tools provide invaluable insights into your network's health and security.

-The End-

******* Wish you all the best from Ravindra Wanninayake *******