CODELIVLY

LEARN CYBERSECURITY

NETWORKING STUDY NOTES

FOLLOW

www.codelivly.com

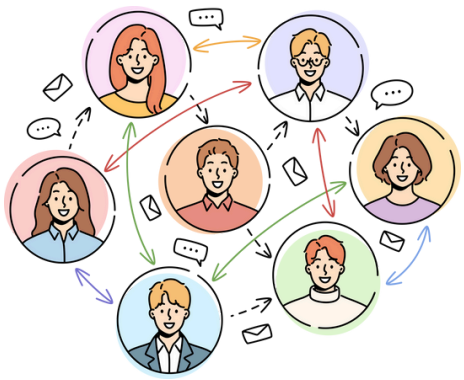
LEARN THE BASICS

I. What is Networking?

Networking is the foundational concept of interconnecting devices — such as computers, servers, and mobile phones — to facilitate communication and the sharing of resources. At its core, networking establishes a framework for devices to exchange data efficiently and securely. It is akin to constructing a digital highway system, where information travels between devices, enabling collaboration, access to shared files, and the operation of critical services.

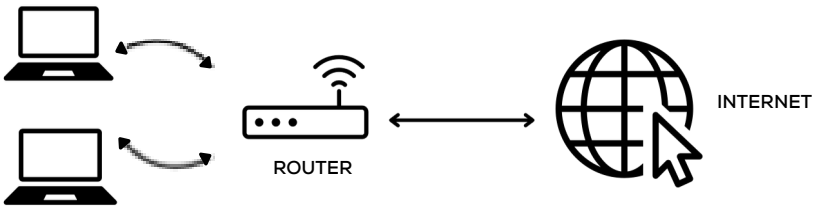
Key Components of Networking

1. Nodes: These are the devices within the network, including computers, phones, and other digital devices.
2. Links: These represent the physical and wireless connections that facilitate communication between nodes, such as Ethernet cables and Wi-Fi signals.

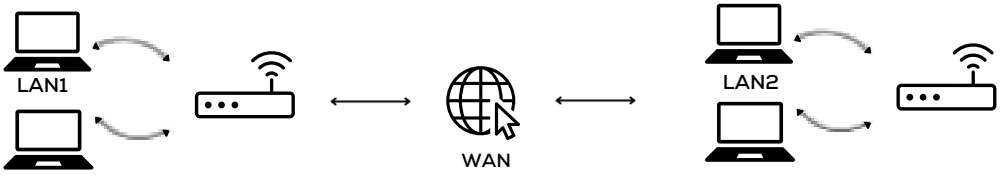


3. Common Network Types:

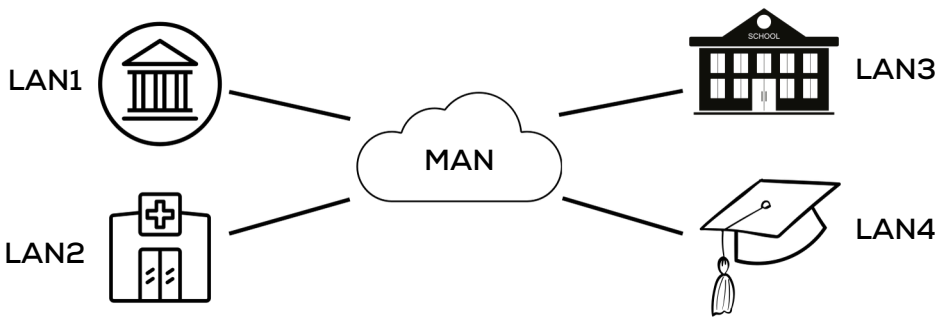
- **Local Area Network (LAN):** Covers a small geographical area like a home, school, or office. LANs typically offer high-speed connections.



- **Wide Area Network (WAN):** Spans a large geographical area and connects multiple smaller networks, including the internet itself, enabling global communication.



- **Metropolitan Area Network (MAN):** Designed to cover a city or a large campus, providing connectivity within municipal or regional boundaries.



II. IP Addressing

Definition

An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network that uses the IP for communication. The IP address serves two principal functions: host or network interface identification and location addressing.

Types of IP Addresses

1. **IPv4:** This 32-bit address format is depicted in numerical dot notation, such as *192.168.1.1*. Despite its widespread use, IPv4 addresses are limited, prompting the need for an alternative to accommodate more devices.
2. **IPv6:** With 128 bits, this newer version greatly expands the number of available addresses. It is represented in hexadecimal notation, as seen in *2001:0db8:85a3::7334*, and includes enhanced security features.

Public vs. Private IP Addresses

- **Public IPs** are assigned by Internet Service Providers (ISPs) and are necessary for online network devices that host websites or deliver services over the Internet.
- **Private IPs** are used within a local network environment.

They are not routable on the global internet, with network address translation (NAT) used to map these private addresses to a public counterpart for external communication.

III. Key Networking Protocols and Ports

TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol that ensures the reliable delivery of data packets across a network. It establishes a connection through a handshake process before transmitting data, thereby guaranteeing that all packets reach the destination in the correct sequence.

Common TCP Ports and Their Applications

- **Port 80:** Used for HTTP, facilitating standard web browsing.
- **Port 443:** Supports HTTPS, ensuring secure and encrypted web browsing.
- **Port 21:** FTP, used for the transfer of files between systems.
- **Port 22:** SSH, provides secure remote access to computers.
- **Port 25:** SMTP, employed for sending emails.
- **Port 3306:** MySQL, used for database communication.
- **Port 3389:** RDP, allows remote desktop connections.

IV. 20 Common Network Protocols Explained

Application Layer Protocols

HTTP (HyperText Transfer Protocol)

- Purpose: Facilitates the transfer of web pages and other web resources from servers to clients. Example:
- Retrieving information from a website like *http://example.com*. Cybersecurity Relevance:
- Susceptible to interception and eavesdropping due to lack of encryption, making HTTPS a preferred alternative for secure communication.

HTTPS (HTTP Secure)

- Purpose: Extends HTTP with security capabilities using SSL/TLS encryption to protect data during transfer. Example: Conducting transactions on websites such as
- *https://bank.com* or online shopping platforms. Cybersecurity Benefit: Encrypts and secures data
- transmission, protecting against eavesdropping and man-in-the-middle attacks.

FTP (File Transfer Protocol)

- Purpose: Enables the transfer of files between systems over a network.
- Example: Uploading or downloading website files to and from a server.

- Cybersecurity Concern: Inherent lack of encryption for data in transit; can be mitigated by using SFTP or FTPS for secure file transfer.

SFTP (Secure File Transfer Protocol)

- Purpose: Uses SSH (Secure Shell) to encrypt file transfers, ensuring secure and confidential data exchange.
- Example: Transferring sensitive files, such as encrypted backups or confidential documents.
- Cybersecurity Benefit: Provides robust security by encrypting both commands and data, preventing data breaches during transmission.

SMTP (Simple Mail Transfer Protocol)

- Purpose: Used for sending emails from clients to servers or between servers. Example: Email services
- like Gmail use SMTP for sending outgoing emails. Cybersecurity Concern: Vulnerable to email spoofing
- and phishing attacks if not paired with authentication mechanisms such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

IMAP (Internet Message Access Protocol)

- Purpose: Allows users to access and manage their emails stored on a server, enabling synchronization across multiple devices. Example: Checking email on a
- smartphone, tablet, and computer, with all devices reflecting the same messages and organization.

- Cybersecurity Benefit: Can be configured to use SSL/TLS encryption for secure email retrieval, protecting against data snooping on unsecured networks.

DNS (Domain Name System)

- Purpose: Resolves human-readable domain names to machine-readable IP addresses, enabling users to access websites using familiar names. Example:
- Converting a request for google.com into the IP address 142.250.190.14. Cybersecurity Concern: Exposed to DNS
- spoofing and cache poisoning, where attackers redirect users to malicious sites.

DHCP (Dynamic Host Configuration Protocol)

- Purpose: Automatically assigns IP addresses and other network configuration parameters to devices, facilitating easy connectivity to networks. Example: A
- laptop automatically obtaining an IP address when connecting to a Wi-Fi network. Cybersecurity Risk:
- Vulnerable to attacks from rogue DHCP servers, which can distribute incorrect or malicious network settings.

SNMP (Simple Network Management Protocol)

- Purpose: Monitors and manages network devices such as routers and switches, collecting and organizing information about managed devices on IP networks.
- Example: Network administrators monitoring traffic load on routers to optimize performance and uptime.

- Cybersecurity Concern: SNMP versions 1 and 2c use plain text community strings for authentication, which are susceptible to interception, necessitating the use of SNMPv3 for enhanced security.

Telnet

- Purpose: Provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection, primarily for accessing remote servers and devices.
- Example: System administrators accessing and managing a server or network device from a remote location. Cybersecurity Concern: Inherently insecure as
- it transmits all session data, including sensitive information like usernames and passwords, in clear text, making it susceptible to eavesdropping.

Transport Layer Protocols

TCP (Transmission Control Protocol)

- Purpose: Ensures reliable, ordered, and error-checked delivery of a stream of packets on the network.
- Example: TCP is used for web browsing and downloading files, where data integrity and order are crucial. Cybersecurity
- Concern: Vulnerable to session hijacking, where attackers take over a TCP session to steal data or identity.

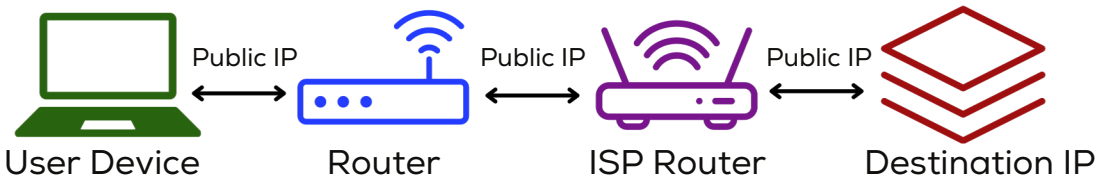
UDP (User Datagram Protocol)

- Purpose: Provides a connectionless transmission model with minimal delay, sacrificing reliability for speed and efficiency.
- Example: Frequently used in time-sensitive applications such as video streaming and online gaming where occasional packet loss is preferable to the delay caused by error correction.
- Cybersecurity Concern: Susceptible to UDP flood attacks which are a type of Denial of Service (DoS) attack that overwhelms a target with UDP packets to disrupt service.

Network Layer Protocols

IP (Internet Protocol)

- Purpose: The primary protocol in the Internet Layer of the Internet Protocol Suite, responsible for routing data packets between devices across networks.
- Example: Data transmission using IPv4 or IPv6 addresses that identify sending and receiving devices.
- Cybersecurity Concern: IP spoofing, where an attacker disguises as a different IP address to launch attacks such as session hijacking and man-in-the-middle (MITM) attacks.



ICMP (Internet Control Message Protocol)

- Purpose: Used for sending error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. Example: The “ping”
- command uses ICMP to test connectivity between two network nodes. Cybersecurity Concern: Can be
- exploited to perform Denial of Service (DoS) attacks, such as the Ping of Death and ICMP flood.

Data Link Layer Protocols

ARP (Address Resolution Protocol)

- Purpose: Resolves IP addresses into MAC addresses, the physical hardware identification for devices on a local area network (LAN).
- Example: When a device communicates over a network, ARP is used to link the IP address to the correct hardware address on the local network.
- Cybersecurity Concern: ARP spoofing allows attackers to intercept, modify, or stop data-in-transit by linking an attacker’s MAC address with the IP address of another host.

Ethernet

- Purpose: Standardizes communications on physical and data link layers for wired local area networks.

- Example: Ethernet is used in office and home networks to connect devices like computers, printers, and routers. Cybersecurity Concern: Eavesdropping on
- unencrypted Ethernet traffic, where attackers gain unauthorized access to data flowing through the network.

Security Protocols

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

- Purpose: Protocols designed to secure communications over computer networks by encrypting data and providing authentication.
- Example: Used in securing web browsers connections, ensuring that all data passed between the web server and browsers remain private and integral.
- Cybersecurity Benefit: Protects against man-in-the-middle attacks by securely encrypting the data transmitted between the client and server.

IPsec (Internet Protocol Security)

- Purpose: A suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream.
- Example: Often used in Virtual Private Networks (VPNs), securing data communications between a VPN client and a VPN server.

- Cybersecurity Benefit: Provides confidentiality, data integrity, and authentication for data communications over a network.

File Sharing and Directory Services

NFS (Network File System)

- Purpose: Allows a user on a client computer to access files over a network in a manner similar to how local storage is accessed.
- Example: Accessing shared files on a remote server, typically used in corporate environments.
- Cybersecurity Concern: Vulnerable to unauthorized access if not properly secured with authentication and permissions.

LDAP (Lightweight Directory Access Protocol)

- Purpose: Provides a mechanism for accessing and maintaining distributed directory information services over an Internet Protocol network.
- Example: Used in managing and accessing the centralized directory information in organizations, such as for user and resource directory services.
- Cybersecurity Concern: Susceptible to unauthorized access and attacks if misconfigured, emphasizing the need for strict security policies and authentication controls.

V. Network Address Translation (NAT)

NAT is a critical network function that allows multiple devices on a private network to share a single public IP address for accessing the internet. This is common in residential and small business environments.

- Example: A home Wi-Fi router using NAT enables multiple devices, like laptops, phones, and TVs, to access the internet through one public IP address.
- Cybersecurity Relevance: NAT provides an additional layer of security by masking internal IP addresses from the external network. This obfuscation helps to prevent direct attacks on private IP addresses from external sources.

VI. Key Network Devices

Router

- Purpose: Serves as a gateway between different networks, such as connecting a home network to the internet. Security Role: Implements Access Control
- Lists (ACLs) which restrict or allow traffic based on predetermined security rules, thus blocking unauthorized access.

Switch

- Purpose: Connects multiple devices on the same Local Area Network (LAN) to enable communication between them, handling data transfer within the network.

Firewall

- Purpose: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Types: Packet-
- filtering firewalls inspect packets independently and block them based on source and destination addresses, ports, or protocols. Stateful firewalls keep
- track of active connections and make decisions based on the state of the connection as well as the set rules. Application-layer firewalls inspect the content of the
- traffic to block specific applications or services and prevent attacks that operate at the application layer.

Access Points (APs)

- Purpose: Extends the wireless coverage of a network, enabling wireless devices to connect to the network through Wi-Fi. Security Concern: Vulnerable to
- attacks if not properly secured. Insecure configurations, such as weak passwords, can lead to unauthorized access. Implementing WPA3 encryption is recommended to strengthen security.

IDS/IPS (Intrusion Detection System / Intrusion Prevention System)

- Purpose:

IDS: Monitors network traffic for suspicious activity and alerts administrators about potential threats.

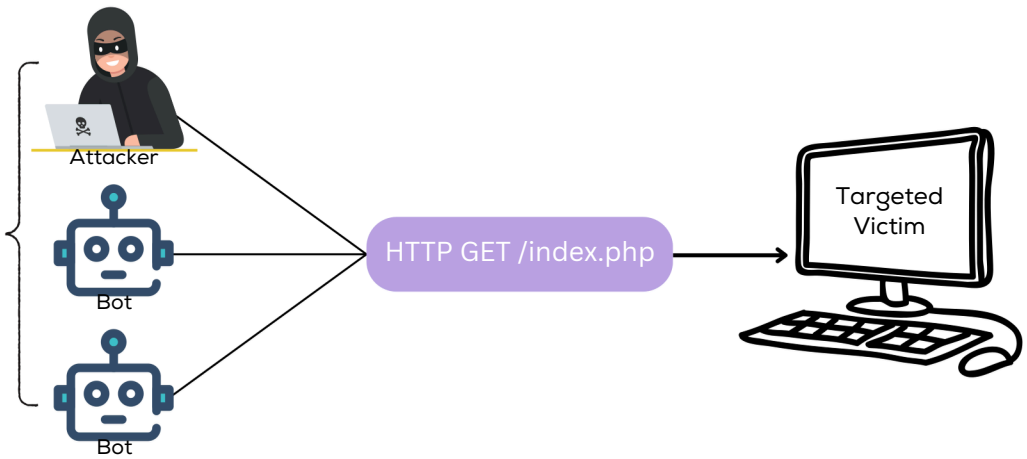
IPS: Similar to IDS but also capable of taking action to block detected threats, acting as a second layer of defense.

- Security Role: Both systems are crucial in enhancing network security. They help detect and prevent a wide range of cyber threats including malware, unauthorized access attempts, and traffic anomalies.

VII. Common Networking Attacks

DDoS (Distributed Denial of Service)

- Description: Attackers overload a network or server with a flood of internet traffic from multiple compromised sources, overwhelming resources and rendering the service unavailable to legitimate users.
- Example: A major e-commerce website going offline during a holiday sale due to a flood of inauthentic traffic requests. Cybersecurity
- Mitigation: Implementing
  DDoS protection services, such as traffic filtering and rate- limiting, along with a robust incident response strategy, can help mitigate these attacks.

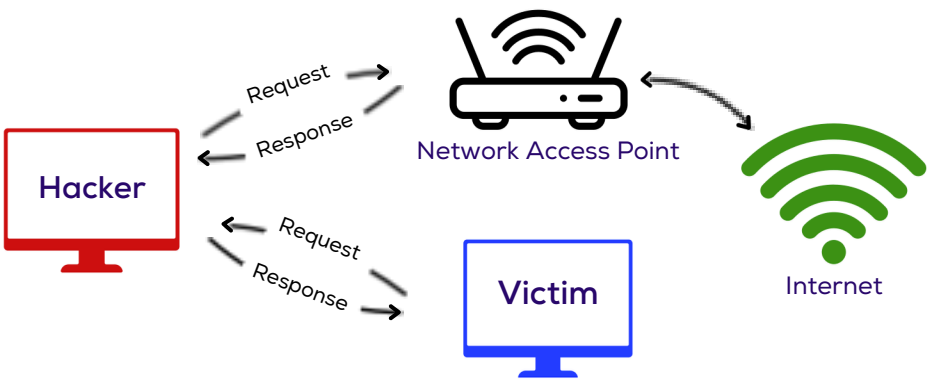


MITM (Man-in-the-Middle)

- Description: In this attack, an adversary intercepts communications between two parties to steal data or insert malicious content, often without either party knowing. Example: Capturing unencrypted HTTP traffic
- to obtain user login credentials. Cybersecurity Mitigation: Enforcing HTTPS on all sessions, using end-
- to-end encryption, and secure VPNs can effectively thwart MITM attacks.

ARP Spoofing

- Description: An attacker sends false ARP (Address Resolution Protocol) messages over a local network. This links the attacker's MAC address with the IP address of another host, such as the gateway, enabling the attacker to intercept, modify, or block data to and from the target. Example: Manipulating network traffic
- so that communications intended for a network gateway are sent to the attacker instead. Cybersecurity Mitigation: Deploying static ARP entries where feasible,
- utilizing network security monitoring tools to detect unusual ARP traffic, and employing packet filters can all defend against ARP spoofing.



DNS Spoofing (DNS Poisoning)

- Description: This technique involves corrupting the DNS resolution process to redirect users to malicious websites instead of legitimate ones, facilitating data theft or malware distribution. Example: Altering DNS
- entries so users trying to access *www.paypal.com* are redirected to a lookalike site that steals their credentials.
- Cybersecurity Mitigation: Implementing DNSSEC (Domain Name System Security Extensions), which uses digital signatures to verify the authenticity of response data, and using reputable DNS providers can help protect against DNS spoofing.

Phishing

- Description: A form of social engineering where attackers deceive victims into revealing personal, financial, or security data. This is often achieved through counterfeit communications that appear to come from trusted sources. Example: Receiving an
- email that mimics the style and branding of a legitimate bank, requesting users to verify account details via a deceptive link. Cybersecurity Mitigation: Training users
- to recognize phishing attempts, employing advanced email filtering solutions, and implementing multi-factor authentication (MFA) are effective strategies to minimize phishing risks.

VIII. Cybersecurity Best Practices for Networking

- Use Encryption
- Apply Strong Authentication
- Monitor Network Traffic
- Segment Networks
- Regularly Patch Devices and Software
- Use Firewalls and IDS/IPS
- Implement Access Control
- Backup Critical Data
- Educate Users
- Secure Wireless Networks

FOLLOW

CODELIVLY
LEARN CYBERSECURITY

CODELIVLY
LEARN CYBERSECURITY