Computer Network

CSYE 6225: Network Structure & Cloud Computing
Northeastern University

Instructor: Raja Alomari,PhD

M2: Overview

Topics include:

- Network Types, Network Topologies.
- IP addresses (IPv4, IPv6) and Mac addresses.
- TCP, Port, DNS, OSI model/layers, TCP/IP, TCP/IP versus OSI.
- Network Traffic and Monitoring.
- Basic Network Security, Authentication vs Authorization, DHCP, VPN, Firewall.
- Basics of Internet of Things (IoT).

Computer Networks

Objectives:

- Understand Computer Networks, Types, and Topologies.
- Understand OSI Models and TCP/IP.
- Understand Network Traffic and Monitoring.
- Understand the Basics of Network Security, Including Authentication, Authorization, Firewalls, and VPNs.

Hands-on:

- Run commands to monitor network activities.

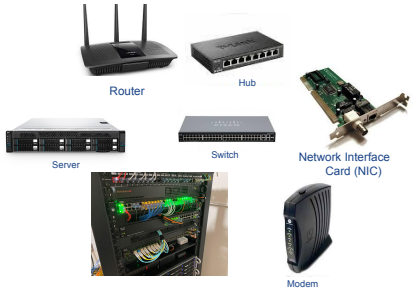
What is a Computer Network?

Definition:

- A computer network is a collection of interconnected devices that can communicate and share resources.

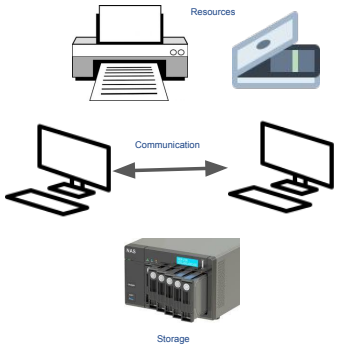
Components:

- Devices (Computers, Servers, Smartphones)
- Networking Hardware (Routers, Switches)
- Transmission Media (Cables, Wireless Signals)



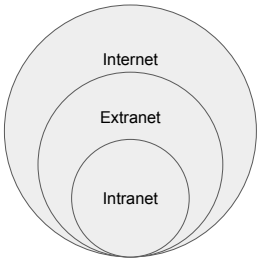
Importance of Computer Networks

- Facilitate communication and collaboration
- Enable resource sharing (files, printers, internet)
- Support remote access and services
- Enhance productivity and efficiency



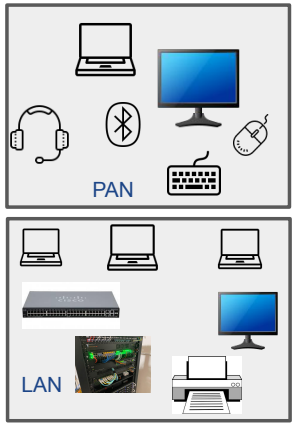
Examples of Networks

- **Internet:** Global network connecting millions of private, public, academic, business, and government networks
- **Intranets:** Private networks within organizations for internal communication and resource sharing
- **Extranets:** Networks that allow controlled access to outsiders, such as business partners or customers.



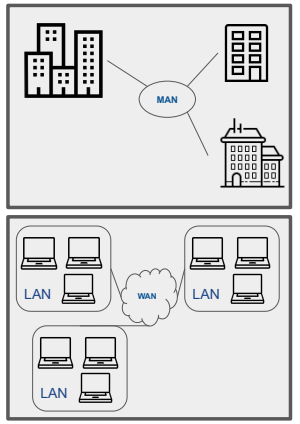
Types of Networks

- Personal Area Network (PAN):
  - Short-range network for personal devices (e.g., Bluetooth)
- Local Area Network (LAN):
  - Network covering a small geographical area like a home, office, or building.



Types of Networks

- Metropolitan Area Network (MAN):
  - Network covering a city or a large campus
- Wide Area Network (WAN):
  - Network covering a large geographical area, often a country or continent



Types of Networks: Others

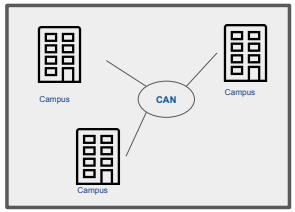
Campus Area Network (CAN):

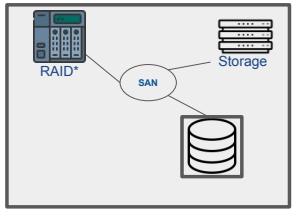
- Interconnects multiple LANs within a limited geographical area like a university or corporate campus

Storage Area Network (SAN):

- High-speed network that connects and provides shared pools of storage devices

*RAID: Data Storage Virtualization Technology. Stands for: Redundant Array of Independent (or Inexpensive) Disks



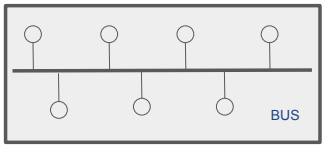


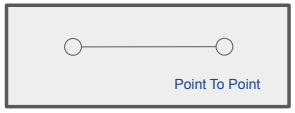
Storage: SAN vs NAS

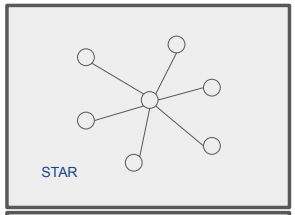
Criteria	SAN (Storage Area Network)	NAS (Network Attached Storage)
Performance	High performance, low latency, suitable for mission-critical applications.	Moderate performance, suitable for general file sharing and backup.
Complexity	Requires specialized knowledge and management tools.	Easier to set up and manage, accessible to non-specialized users.
Scalability	Highly scalable for large enterprise environments.	Moderately scalable, suitable for small to medium-sized setups.
Cost	Generally more expensive due to specialized hardware and network infrastructure.	More cost-effective, leveraging existing network infrastructure.
Deployment	Often deployed in large enterprises with dedicated storage requirements.	Commonly used in small to medium-sized businesses and departments within larger organizations.

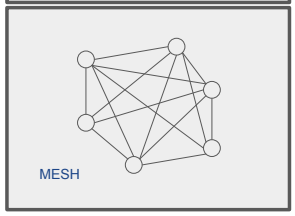
Network Topologies

- The arrangement of various elements (links, nodes, etc.) in a computer network.



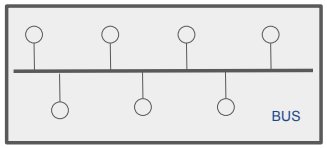


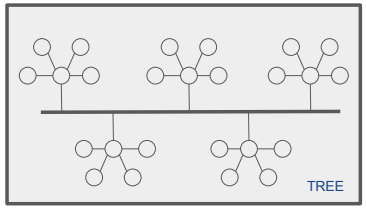




Network Topologies: Bus, Tree.

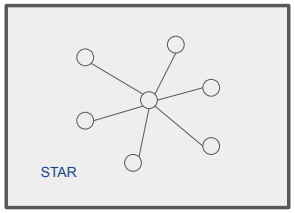
- All devices share a single communication line
- Simple and cost-effective
- Limited by the number of devices and distance



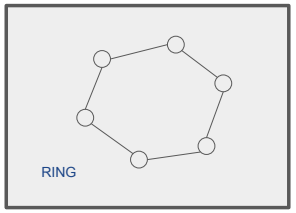


Network Topologies: Star, Ring, Hybrid.

- All devices are connected to a central hub
- Easy to install and manage
- If the hub fails, the entire network is affected



- Each device is connected to two other devices, forming a ring
- Data travels in one direction (or both in a dual ring)
- Failure in a single device can impact the entire network



Network Models: OSI and TCP/IP Models.

OSI Model

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data link Layer
Physical Layer

TCP/IP Model

Application Layer
Transport Layer
Network Layer
Network Access Layer

OSI Model

Application Layer: Network services to end-users, e.g., HTTP, FTP, SMTP, DNS.

Presentation Layer: Data translation, encryption, and compression, e.g., SSL/TLS, JPEG, GIF.

Session Layer: Manages sessions between applications, e.g., NetBIOS, RPC.

Transport Layer: Ensures complete data transfer, e.g., TCP, UDP.

Network Layer: Path determination and logical addressing, e.g., IP, Router.

Data Link Layer: Reliable transmission of data frames between two nodes, e.g., switch.

Physical Layer: Transmission and reception of raw bit streams over a physical medium, e.g., ethernet cables, hubs.

7	Application Layer
6	Presentation Layer
5	Session Layer
4	Transport Layer
3	Network Layer
2	Data link Layer
1	Physical Layer

Developed by ISO (International Organization for Standardization)

TCP/IP Model

Application Layer: High-level protocols and services for applications, e.g., HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).

Transport Layer: Reliable data transfer, Flow control and congestion control, e.g., TCP, UDP.

Internet Layer: Logical addressing and routing, Packet switching and control, e.g., IP, ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

Network Interface Layer: Data encapsulation, addressing, and error detection e.g., ethernet cables, WIFI.

Application Layer
Transport Layer
Internet Layer
Network Interface

Developed by the Department of Defense (DoD)

Network Hardware and Transmission Media


Router


Hub


Modem


Switch

Network Hardware and Transmission Media

Routers

Connects multiple networks

Routes data packets between networks

Determines the best path for data


Router

Switches

Connects devices within a single network (LAN)

Operates at the Data Link layer (Layer 2) or Network layer (Layer 3)

Efficiently forwards data to the correct device


Switch

Network Hardware and Transmission Media

Hubs

Simple devices that connect multiple Ethernet devices

Broadcasts incoming data to all ports

Operates at the Physical layer (Layer 1)


Hub

Bridges

Connects and filters traffic between two network segments

Operates at the Data Link layer (Layer 2)

a bridge does not assign IP addresses, keep a log of network activity, or provide a firewall.


Bridge

Network Hardware and Transmission Media

Gateways

Connects different network architectures and protocols

Operates at various layers depending on the implementation

Translates data between different network formats


Gateway

Modems

Modulates and **dem**odulates analog signals for digital data transmission

Connects networks over telephone lines, cable, or satellite

Examples: DSL modems, Cable modems


Modem

Network Hardware and Transmission Media

Wireless Access Point (AP)

Enables wireless devices to connect to a wired network.

Extends network coverage, supporting multiple simultaneous connections.

Provides encryption (WPA2, WPA3) and authentication for secure access.

Wireless AP

Access Point Controller

Centralizes management for multiple wireless access points, allowing for configuration, monitoring, and maintenance.

Used in medium to large enterprises managing numerous networks across different locations.

AP Controller

Network Hardware and Transmission Media

Repeater

Receives and amplifies a signal to extend the transmission distance.

Extending the range of a network, particularly in large buildings or areas with signal interference.

Repeater

Proxy Server

Intermediates requests from clients seeking resources from other servers, providing caching, filtering, and access control.

Enhancing security, controlling internet usage, and improving performance through caching.

Proxy Server

Network Hardware and Transmission Media

Load Balancer

Distributes network or application traffic across multiple servers to ensure no single server becomes overwhelmed.

Improving the availability and reliability of applications by balancing loads

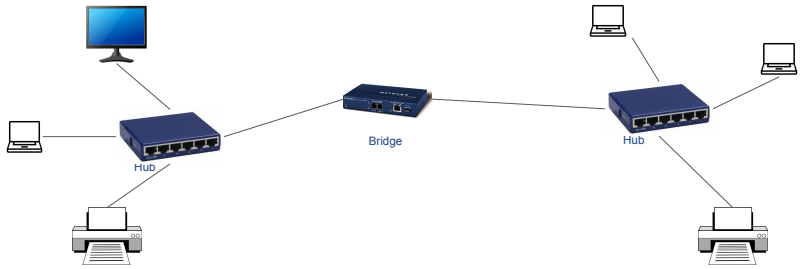
Load Balancer

Network Interface Card (NIC)

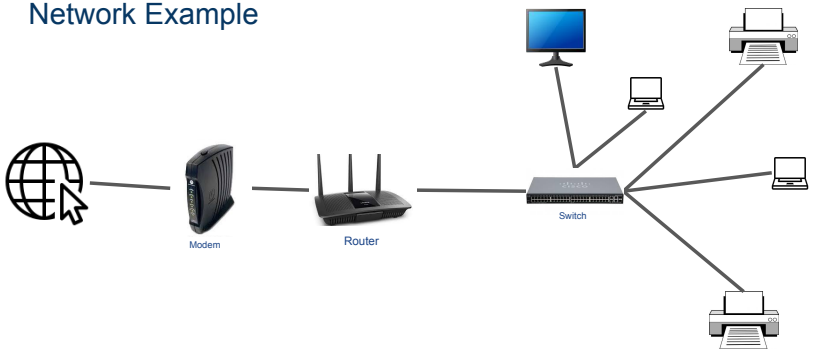
Hardware component that connects a computer to a network, allowing it to communicate with other devices.

Network Interface Card (NIC)

Network Example



Network Example



Transmission Media: Wired Media

Twisted Pair

Copper cables with twisted wire pairs

Examples: Cat5, Cat6 cables

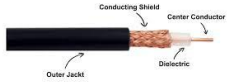
Used in LANs, telecommunication

Twisted Pair

Coaxial Cable:

Single copper conductor with a shield

Used in cable TV, broadband internet



Coaxial Cable

Fiber Optic Cable

Uses light to transmit data

High-speed, long-distance communication

Examples: Single-mode, multi-mode fibers

Fiber Optic

Transmission Media: Wireless Media

Radio Waves

Used in Wi-Fi, Bluetooth, AM/FM radio

Wide coverage, susceptible to interference

Microwaves

Used in satellite communication, cellular networks

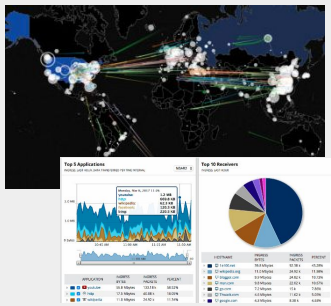
Line-of-sight transmission, higher frequency

Infrared

Short-range communication, remote controls

Limited by obstacles and distance

Network Traffic and Monitoring



Network Traffic: Main Types

Unicast:

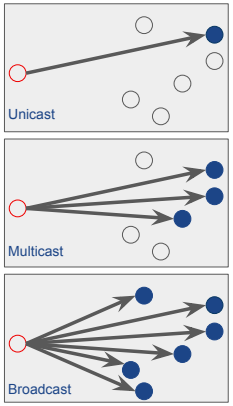
- One-to-one communication
- Example: Sending an email from one user to another

Multicast:

- One-to-many communication
- Example: Streaming a live video to multiple users

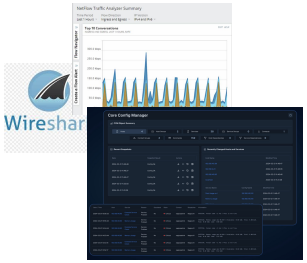
Broadcast:

- One-to-all communication within a network segment
- Example: ARP request (A request to all devices in the network to find the physical (MAC) address associated with a given IP address).



Monitoring: Traffic Patterns and Analysis

- Understanding traffic patterns helps in optimizing network performance
- Common patterns: Peak hours, periodic spikes, baseline traffic
- Importance of traffic analysis in detecting anomalies, bottlenecks, performance and security



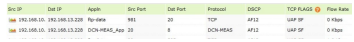
Monitoring: Traffic Patterns and Analysis

Wireshark

- Open-source tool for network protocol analysis
- Uses: Troubleshooting network issues, analyzing traffic patterns, security analysis.

NetFlow

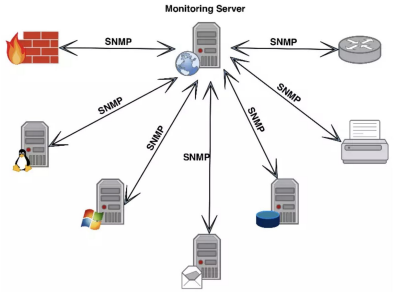
- Developed by Cisco for collecting and analyzing network traffic data
- Uses: Traffic accounting, usage-based billing, network planning



Monitoring: Traffic Patterns and Analysis

SNMP (Simple Network Management Protocol)

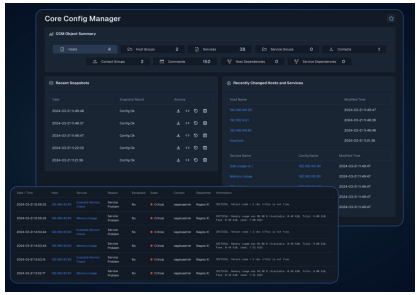
- Widely used protocol for network management
- Components: Managed devices, agents,network management systems (NMS)
- Uses: Monitoring network performance, detecting faults, configuring devices



Monitoring: Traffic Patterns and Analysis

Nagios

- Open-source monitoring solution
- Comprehensive monitoring system for network infrastructure
- Uses: Monitoring network services (HTTP, SMTP), host resources, alerts and notifications



Traffic Management

Load Balancing

Distributes network traffic across multiple servers or paths

Benefits: Increases reliability, reduces latency, improves performance

Traffic Shaping

Controls the flow and volume of traffic sent into a network

Benefits: Prevents congestion, ensures bandwidth availability for critical applications

Quality of Service (QoS)

Prioritizes certain types of traffic

Benefits: Guarantees performance for high-priority applications (e.g., VoIP, streaming)

Traffic Management: Techniques

Load Balancing Techniques

Round Robin: Distributes traffic evenly across all servers

Least Connections: Directs traffic to the server with the fewest active connections

IP Hash: Routes traffic based on the IP address of the client

Traffic Shaping Techniques

Rate Limiting: Limits the rate of traffic flow to a specified limit.

Packet Prioritization: Prioritizes packets based on type or application.

Bandwidth Allocation: Allocates specific bandwidth amounts to different types of traffic

Quality of Service (QoS) Implementation

Classifying and prioritizing traffic (e.g., real-time vs. non-real-time)

Using QoS tools and protocols (e.g., DiffServ, IntServ)

Benefits: Enhanced performance for critical applications, reduced latency

denial of service attacks

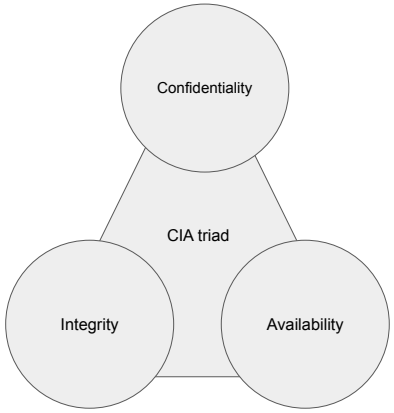
Network Security Basics

Network Security: Goals

Confidentiality: Ensuring data is accessible only to authorized users.

Integrity: Ensuring data is accurate and unaltered

Availability: Ensuring network resources are available when needed



Network Security: Authentication vs Authorization

Authentication

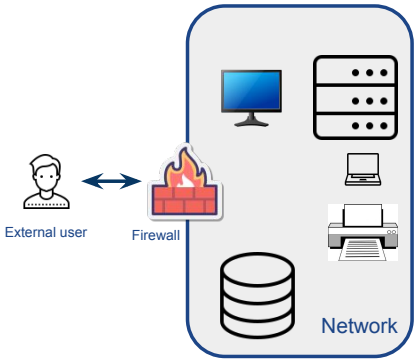
- Verifying the identity of users and devices
- Methods: Passwords, biometrics, two-factor authentication (2FA).

Authorization

- Determining what authenticated users are allowed to do
- Role-Based Access Control (RBAC), Access Control Lists (ACL)

Network Security: Firewalls

- Hardware or software that monitors and controls incoming and outgoing network traffic
- Types: Packet-filtering, stateful inspection, proxy, next-generation firewalls (NGFW).



Firewalls Types

Packet-Filtering Firewall:

- Filters traffic based on predefined rules (IP addresses, ports)
- Basic level of security

Stateful Inspection Firewall:

- Tracks the state of active connections and makes decisions based on the state and context

Proxy Firewall:

- Intercepts and inspects all traffic between external and internal networks

Next-Generation Firewall (NGFW):

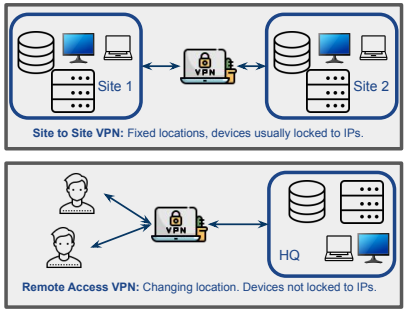
- Combines traditional firewall with additional features like intrusion prevention and application awareness

Virtual Private Networks (VPNs)

Purpose: Securely connects remote users to a private network over the internet

Types of VPNs

- Remote Access VPN: Allows individual users to connect to a private network remotely
- Site-to-Site VPN: Connects entire networks at different locations

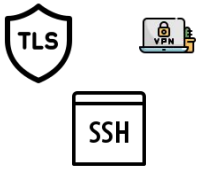


Network Security Protocols

SSL (Secure Sockets Layer)/TLS (Transport Layer Security): Encrypts data transmitted over the internet. TLS is successor and more secure. SSL is now considered deprecated,

IPSec (Internet Protocol Security): Secures IP communication by authenticating and encrypting each IP packet

SSH: Provides a secure channel over an unsecured network



Malware Protection

Types

Viruses: Malicious programs that attach to legitimate files and spread to other files and systems, causing damage.

Worms: Standalone malware that replicates itself to spread across networks, often causing significant harm.

Trojan Horses: Disguised as legitimate software, they trick users into installing them to gain unauthorized access.

Ransomware: Encrypts user data and demands a ransom for decryption, potentially leading to data loss and financial damage.

Risks and Impacts

Data Loss: Malware can delete or corrupt critical data, leading to permanent loss of important information.

Financial Loss: Ransomware demands, recovery costs, and potential fines from data breaches can be substantial.

System Damage: Viruses and worms can damage software and hardware, causing operational disruptions.

Security Breaches: Trojans and other malware can create backdoors, leading to unauthorized access and data theft.

Case Study: SolarWinds Supply Chain Attack

Date: Discovered in December 2020

Attackers compromised the Orion software update from SolarWinds

Over 18,000 organizations potentially affected, including government agencies and major corporations.

Attackers injected malicious code into a legitimate software update

Once installed, the malware created a backdoor for remote access

Attackers exfiltrated sensitive data over several months.

Details
https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

Case Study: Colonial Pipeline Ransomware Attack

Date: May 2021

Attack by DarkSide ransomware group

Resulted in the shutdown of a major US fuel pipeline

Led to fuel shortages and increased gas prices across the East Coast

Attackers gained access through a compromised VPN account

Deployed ransomware to encrypt critical systems

Demanded ransom payment in cryptocurrency to restore operations

Details
https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

Case Study: Log4Shell Vulnerability Exploit

Date: Disclosed in December 2021

Critical zero-day vulnerability in the Log4j logging library

Affected millions of Java applications and servers worldwide

Attackers exploited the vulnerability by sending a malicious string to the Log4j library

The vulnerability allowed remote code execution (RCE)

Used for deploying malware, stealing data, and launching further attacks

Details
https://www.dynatrace.com/news/blog/what-is-log4shell/

Case Study: Microsoft Exchange Server Hack

Date: Discovered in early 2021

Exploited vulnerabilities in Microsoft Exchange Server

Affected tens of thousands of organizations globally

Attackers used a combination of zero-day vulnerabilities

Gained access to email accounts and deployed web shells for persistence

Stole sensitive data and credentials

Details
https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

Case Study: Kaseya VSA Ransomware Attack

Date: July 2021

Attack on Kaseya VSA, a remote management software

Affected around 1,500 businesses through managed service providers (MSPs)

MSP providers remotely manage a customer's IT infrastructure.

Attackers exploited vulnerabilities in the VSA software

Deployed REvil ransomware to encrypt files and demand ransom

Attack leveraged MSPs to spread ransomware to multiple clients

Details
https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack

Recommended Certificates

CompTIA Network+

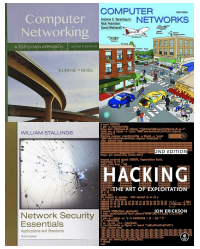
Cisco Certified Network Associate (CCNA)

AWS Certified Advanced Networking - Specialty

Juniper Networks Certified Internet Associate (JNCIA-Junos)

Recommended Readings

1. Computer Networking: A Top-Down Approach by James F. Kurose and Keith W. Ross
2. Computer Networks by Andrew S. Tanenbaum and David J. Wetherall
3. Network Security Essentials: Applications and Standards by William Stallings
4. Hacking: The Art of Exploitation by Jon Erickson



Security Risk

Module 2 Conclusion

- Understanding of basic network architectures, topologies, and protocols.
- OSI and TCP/IP Models: Layers, functions, and importance in network communication.
- Networking Devices: Roles and functions of routers, switches, firewalls, and other devices.
- Protocols: Key protocols like TCP, IP, HTTP, DNS, and their applications.
- Network Security: Importance of securing networks against threats and vulnerabilities.
- Overview of recent network attacks and best practices for defense.
- Hands-on: Use of networking tools and commands for troubleshooting and management.