COMMONROOM NETWORKS FOUNDATION www.commonroom.info

ISEA Institute for Social Entrepreneurship in Asia

Foreign, Commonwealth & Development Office

RHIZOMATICA

APC

SCHOOL OF COMMUNITY NETWORK LEARNING SERIES

2026

INTRODUCTION TO COMPUTER NETWORKS



Page is intentionally left empty

for Beginners

◆ ◇ ◆ ◇ ◆ ◇ ◆

INTRODUCTION TO COMPUTER NETWORKS

English Version

Bahasa Indonesia version is Published by

Common Room Networks Foundation

Bandung, West Java, Indonesia

Supported by the Association for Progressive Communications (APC)

First English Edition
June 2026

Publication Credits (Indonesia)

Programme Coordinator	Gustaff H. Iskandar
Chief Editor	Tisha Anwar
Administration	Reina Wulansari, Daffa Naufal, Sara Verawati
Ilustrasi	Sam & Ridha Kelana

Contributing Institutions

ICT Watch Indonesia	Heru Tjatur, Donny B.U., and Mataharitimoer
Relawan TIK	Fajar Eri Diyanto
APJII	Andri Aslan
Institut Teknologi Garut (ITG)	Ade Sutedi, Adi Susetyaningsih, Andri Ikhwana, Dedi Sadudin Taptajani, Dewi Rahmawati, Dewi Tresnawati, R. Dini Destiani Siti F., Eko Walujodjati, Leni Fitriani, Ridwan Setiawan, Muhammad Rikza N., and Rinda Cahyana
PokdarTIK	Erni Sulistyowati
Phytonesia	Andri Johandri
Bitread	Auliya Millatina Fajwah, Anita Khairunnisa, Acep Zaelani, Nana Sukmana, and Nakita Rizky Oktaviani

English Translation

Translation Project Coordinator	Akhmat Safrudin
Translator	Rudi Dwi Hartanto

Indonesia Publisher

Common Room Networks Foundation (Common Room)

Jl. Cigadung Asri I No. 3, Kel. Cigadung, Kec. Cibeunying Kaler, Kota Bandung, West Java 40191, Indonesia

Website: http://www.commonroom.info Email: email.commonroom@gmail.com

English Version is Published with The Support From APC

Association for Progressive Communications (APC)

Foreword

During the global COVID-19 pandemic, which began spreading across Indonesia in early 2020, internet infrastructure and services became an essential necessity, not only for daily communication, but for virtually every aspect of life: public services, long distance learning, healthcare, and pandemic response.

Although recent years have seen meaningful improvements in internet infrastructure and service coverage across Indonesia, the challenge of the digital divide remains a real and present problem, particularly for residents of rural and remote areas. This divide is driven by a complex combination of factors, including geographical constraints, insufficient infrastructure, limited device access, high bandwidth costs, inadequate digital skills and literacy, a shortage of local content, and persistent gender gaps in technology access.

The School of Community Network Programme (*Sekolah Internet Komunitas*) was established in Indonesia as a collaborative initiative to address these digital divide challenges. Developed jointly by Common Room and the Association for Progressive Communications (APC), and also supported by the Foreign, Commonwealth and Development Office (FCDO — UK), the programme involves ICT Watch, *Relawan TIK,* APJII, and the Garut Institute of Technology (ITG).

This book series forms part of the curriculum and training material framework to be developed within the School of Community Network Programme. The series encompasses ten thematic areas, from policy and regulation to foundational knowledge of computers and internet networks, and practical guidance on internet use for a variety of purposes. We sincerely hope that this guide will contribute to the long-term effort to overcome the digital divide in Indonesia and beyond through the translated module by building digital skills, knowledge, and literacy. especially among communities in rural and remote regions.

Bandung, December 2021

Gustaff H. Iskandar
Common Room Networks Foundation

Table of Contents

Foreword ii
Chapter 1 — Introduction to Computers 1
A. Overview of Computers 2
B. Fundamental Concepts of Computer Systems 4
C. Understanding Computer Networks 5
D. The Importance of Computer Networks 6
E. Types of Computer Networks 9
Chapter 2 — Network and Computer Devices 17
A. Definition of Network Devices 18
B. Common Types of Network Devices 18
Chapter 3 — Network Topology 27
A. Overview of Network Topology 28
B. Types of Computer Network Topologies 28
Chapter 4 — Network Addressing and Security 35
A. Network Addressing Systems 36
B. How IP Addressing Works 37
C. IP Address Version 4 (IPv4) 38
D. Network Layer 40
Chapter 5 — Network Installation 43
Chapter 6 — Network Security Systems 49
A. Introduction to Network Security 50
B. Types of Network Security Threats 52
C. Firewalls 56
Chapter 7 — IP Routing 59
A. Overview of IP Routing 60
B. Routing Configuration 61
References 67

Index 68

CHAPTER

01

INTRODUCTION TO COMPUTERS

In this chapter, you will hopefully learn:

- ✓ Explain the origin and meaning of the term 'computer'.
- ✓ Identify the three core elements of a computer: hardware, software, and brainware.
- ✓ Describe the five fundamental subsystems of a computer system.
- ✓ Define a computer network and state the conditions required to form one.
- ✓ Distinguish between the major types of computer networks by coverage area and transmission medium.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

□	Basic familiarity with everyday electronic devices (smartphones, tablets, or computers).
□	No prior technical knowledge is required for this chapter.
□	Ability to read and understand simple technical descriptions in English.

A. Overview of Computers

What comes to mind when you first hear the word 'computer'? Perhaps an electronic machine capable of performing calculations? If so, you are correct. The term originates from the Latin word *computare*, meaning "**to calculate**."

In essence, a computer is an assemblage of electronic machinery composed of millions of interdependent components that work together to form an organised, functional system.

> *A computer is fundamentally capable of performing operations automatically, based on instructions or programmes provided by its operator.*

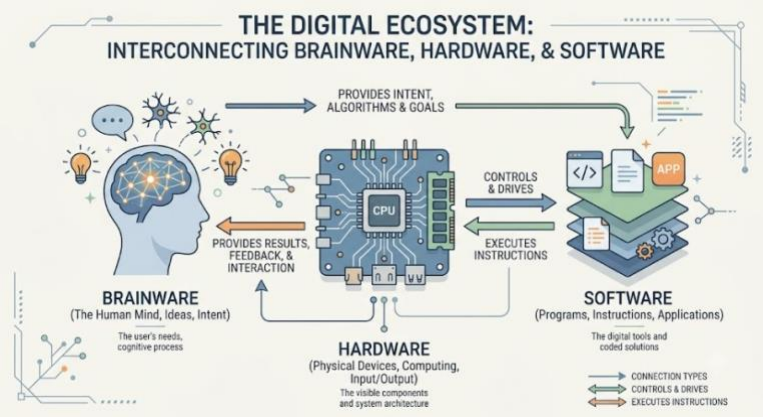


Figure 1 Working Together as a unit (source: personal documentation)

A computer comprises three principal elements: hardware, software, and brainware. Hardware refers to the physical components of a computer — those that can be physically touched, moved, or seen. Software refers to the collection of instructions (programmes or procedures) that direct the computer to process and execute tasks automatically. Brainware refers to the human being who operates the computer.



Figure 2 Brainware as much as it is hardware and software (source: personal documentation)

B. Fundamental Concepts of Computer Systems

Every computer system consists of five fundamental hardware subsystems: input devices, a central processing unit, output devices, peripheral devices, and secondary storage. These are described as follows:



Figure 3 Keyboard, Mouse, Graphical Tablet.

1. Input Devices

Input devices are responsible for entering data into the computer. Common examples include the keyboard, mouse, touchscreen, scanner, barcode reader, fingerprint reader, camera, and microphone.

2. PC Unit

Personal Computer Unit (System Unit)

The system unit is the enclosure that houses a computer's core processing hardware — everything except external peripherals like the monitor, keyboard, and mouse. Inside it, several components work together to process data: the Central Processing Unit (CPU), Random Access Memory (RAM), storage (an HDD or SSD), the motherboard that connects everything, and often a Graphics Processing Unit (GPU) for handling visual output.

Within the system unit, the CPU serves as the data processing hub — effectively the 'brain' of the computer. It handles core computational activities such as arithmetic operations, sorting, searching, writing, and reading instructions. The CPU works closely with RAM (temporary working memory), ROM (permanent firmware), the motherboard (the circuit board

linking every component), and cache memory (small, ultra-fast memory sitting between the CPU and RAM). Alongside the CPU, the GPU handles specialised tasks like rendering graphics and, increasingly, parallel processing for AI workloads, while the SSD or HDD provides long-term storage for the operating system, programs, and files.

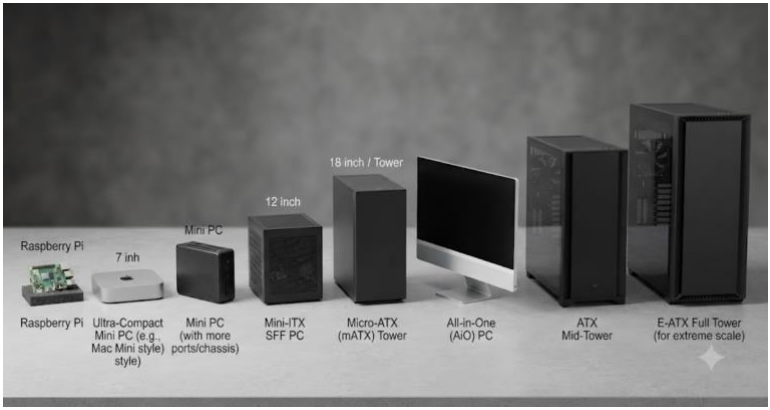


Figure 4 Various Shape and Sizes of PC, horses for courses. There are also limiting factor of smaller PC such as thermal and expansion.

How the System Unit Has Evolved: Traditionally, the system unit was a large tower case — bulky enough to house full-sized components and multiple expansion slots. Over the past two decades, however, miniaturisation in chip design has allowed the same processing power to fit into dramatically smaller enclosures, giving rise to a wide range of form factors:

- **Full tower / mid tower PCs** — the traditional desktop, offering maximum room for expansion, upgrades, and cooling.
- **Mini PCs** — compact desktop units (such as the Intel NUC) that shrink the tower down to a fraction of its size while still running full desktop operating systems.

- **Mac Mini —** Apple's take on the mini PC, packing an entire system unit into a housing barely larger than a hardback book.
- **Raspberry Pi —** a credit-card-sized single-board computer (SBC) that places the CPU, RAM, and connectivity directly onto one small circuit board, without a traditional enclosure at all. Despite its size, it's a fully functional computer capable of running an operating system.
- **All-in-One (AIO) PCs —** where the system unit is built directly into the back of the monitor, eliminating the separate case entirely.

This trend illustrates that the "system unit" is no longer defined by a fixed size or shape. It's simply the collection of core processing components, however they're packaged. What once required a large tower can now fit in your palm, reflecting the same broader trend of miniaturisation that shrank computers from room-sized mainframes to the pocket-sized devices we carry today.



Figure 5 Inside of a standard PC Unit (Getty Images/Grigorev V)

The Foundation: The Motherboard, Think of this as the central nervous system or the "spine" of the computer. It is the large printed circuit board that every single other component plugs into. It doesn't process data itself, but it provides the electrical pathways for the processor, memory, and storage to communicate with each other.

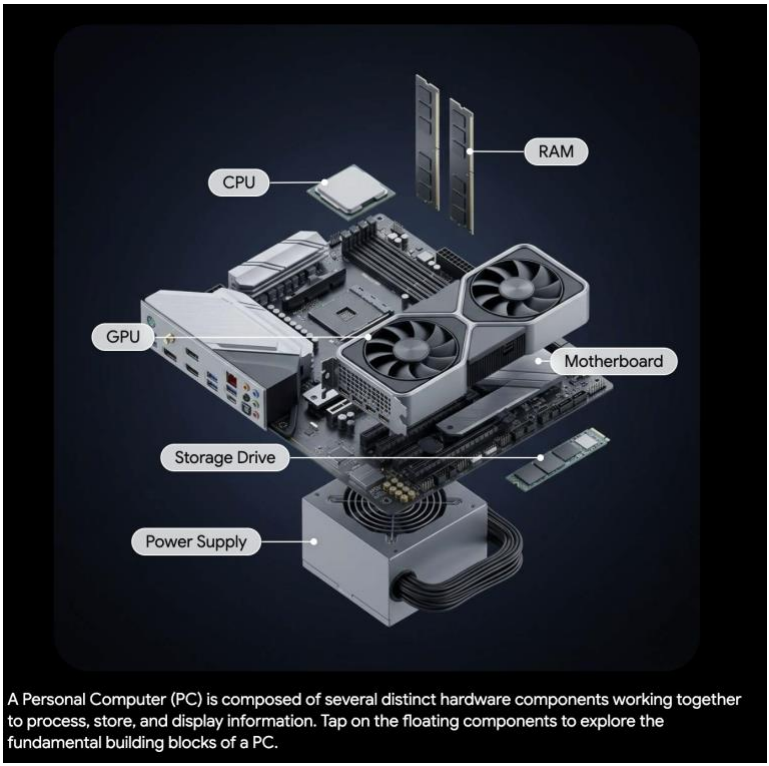


Figure 6 Dive deeper into how these parts are laid out and connected on the motherboard.

Processing & Speed, The Processor (The actual CPU) This is the true "brain" of the operation. It is a small, square microchip slotted directly into the motherboard (usually hidden under a large metal cooling fan). It executes the actual math—calculating, sorting, and executing every instruction from your software.

RAM (Random Access Memory) This is the computer's short-term working memory. When you open a web browser or load a game, the data is moved from your storage drive into the RAM so the processor can access it quickly.

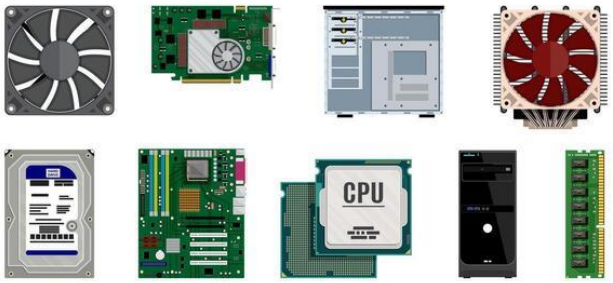


Figure 7 CPU, Motherboard, Random Access Memories (RAM), Hard Disk Drive (HDD), Fan, Case.

3. Output Devices

Output devices present the results of CPU processing in forms such as text (letters, numbers, special characters, and symbols), graphics, images, audio, and machine-readable formats. Common output devices include the monitor or display screen, speakers, printers, plotters, and fax machines.



Figure 8 Printer, Projector, Vertical Screen, Speakers, haptic feedback, etc are the computer output devices

As system units have shrunk and diversified, output devices have evolved alongside them. A traditional tower PC drives a separate external monitor, but Mac Minis and mini PCs are just as likely to be connected to a television or portable USB-C monitor. A Raspberry Pi, being a bare circuit board, typically outputs via HDMI to whatever display is available. From a dedicated touchscreen to a repurposed old monitor, making it a favourite for DIY projects. All-in-One PCs collapse the distinction entirely by building the output device (the screen) and the system unit into a single enclosure.

4. Peripheral Devices

Peripheral devices expand the capabilities of a computer system, for example by enabling file and data sharing between computers, connecting to networks, or adding new functionality. They include modems, Ethernet cards (network cards), TV cards, graphics cards, and sound cards.



Figure 9 Network Interface Cards.

Historically, many of these peripherals were separate expansion cards installed inside a full tower case. In smaller form factors, most of this functionality has been miniaturised directly onto the motherboard: mini PCs, Mac Minis, and laptops now come with Wi-Fi, Ethernet, and sound built in as standard, with little to no room for internal expansion cards.

Devices like the Raspberry Pi go a step further, integrating networking, audio, and general-purpose input/output (GPIO) pins directly onto the single board itself, allowing hobbyists to attach sensors, motors, and other custom peripherals without needing a case at all.

5. Secondary Storage

Secondary storage systems provide long-term data storage for files and programmes outside of the computer's temporary working memory (RAM). Common examples include hard disk drives (HDDs), solid-state drives (SSDs), flash drives, and — in older systems — optical discs (CDs/DVDs).

The shift toward smaller system units has closely paralleled a shift in storage technology. Traditional tower PCs typically used

bulky HDDs with spinning magnetic disks; smaller, more portable form factors are only practical because SSDs (with no moving parts) have become compact, power-efficient, and increasingly affordable. Mini PCs and Mac Minis rely almost exclusively on SSDs, either standard or in the ultra-compact M.2 format that mounts directly onto the motherboard as a small chip rather than a separate drive. A Raspberry Pi typically forgoes an internal drive altogether, booting instead from a microSD card, a storage format small enough to fit the device's minimal footprint while still holding a full operating system.

C. Understanding Computer Network

> *A computer network is defined as two or more devices that are interconnected – either physically or logically.*

Computer networks gave rise to the internet, which has become profoundly influential in modern life. An understanding of computer networks forms the foundational knowledge required to develop future technologies that operate through internet connectivity.

A computer network requires the following conditions to be established:

- At least two computers connected via wired or wireless means.
- The presence of users operating those computers.
- Data communication activities, such as file transfer.
- Shared use of resources during operation.

Computer networks possess four defining characteristics:

Scalability	The network can be adjusted to meet evolving needs and technological developments.

Resource Sharing	The network enables the exchange of data and resources, including both hardware and software.
Connectivity	All devices on the network must be able to connect with one another.
Reliability	The performance and dependability of the network can be measured and evaluated.

D. The Importance of Computer Networks

Computer networks facilitate the rapid and effective exchange of data or information between senders and recipients.

Computer networks simplify access to data. Any publicly available data can be retrieved and shared with others. When social media is used for long-distance communication, that interaction is made possible by computer networking.

More specifically, computer networks enable three forms of information exchange:

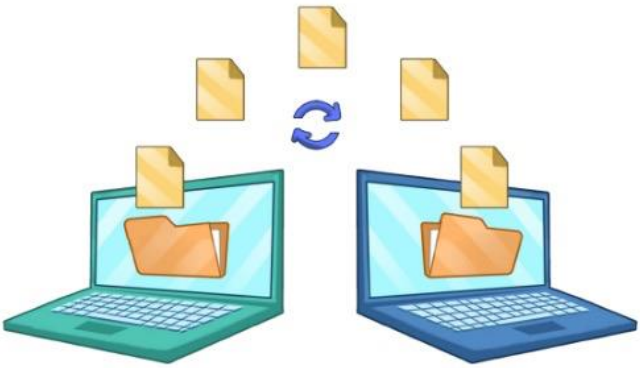


FIGURE 10 FILE EXCHANGE (PERSONAL DOCUMENTATION)

1. File Exchange

Files and documents represent collections of data-formatted information. The demand for file sharing has grown considerably. Computer networks enable connected devices to exchange files in a wide variety of formats quickly and efficiently.

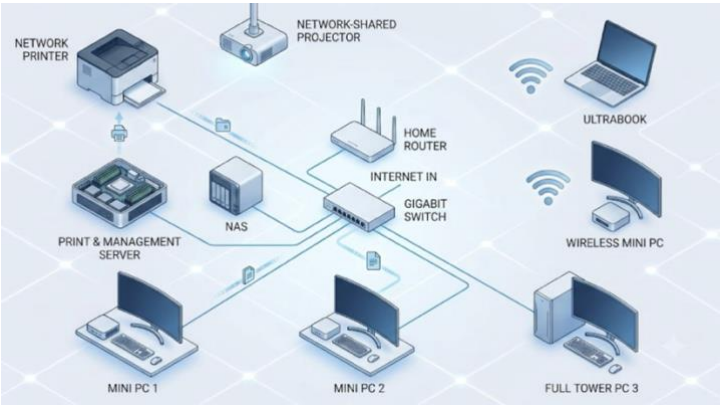


Figure 11 Illustration of Resource Sharing. Network Attached Storage, Projectors, Printers can be used by multiple devices due to its status of being available to user connected to the network.

2. Resource Sharing

A computer network allows users to share hardware resources, such as printers or hard disks, among all connected computers. In the future, virtually all everyday objects and equipment may be connected through computer networks, a concept known as the Internet of Things (IoT). This resource sharing is an important aspect in managing internet networks in a local scope.

3. Programme Sharing

Computer networks enable hardware and software to communicate with one another, enabling tasks to be completed more rapidly, effectively, and efficiently. Today, computers are interconnected across global networks.

E. Types of Computer Networks

Computer networks may be categorised in several ways, including by geographical coverage area, transmission medium, and other criteria. Each classification is examined below.

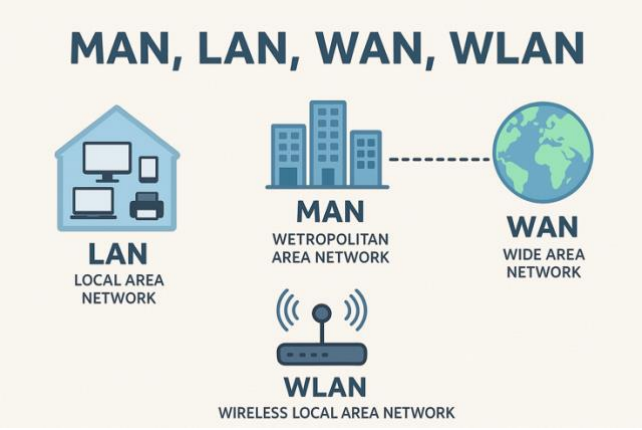


Figure 12 Understanding the classification by coverage area is the basic step to understanding when to apply smaller or broader protocol

1. Classification by Coverage Area

Networks may be classified by their coverage area into the following types: LAN, MAN, WAN, PAN, SAN, EPN, and VPN.

a. Local Area Network (LAN)

A Local Area Network (LAN) is a group of interconnected computers that form a network through a shared medium.

A LAN connects computers within a limited physical area. Common LAN environments include internet cafes, schools, offices, libraries, and computer laboratories. A standard LAN supports up to approximately 100 computers connected via cable — typically UTP or STP cable — using IEEE 802.3 Ethernet technology. Modern LAN deployments may also utilise Wi-Fi (IEEE 802.11b), referred to as a Wireless LAN (WLAN). Transfer speeds range from 10 Mbps to 1,000 Mbps.

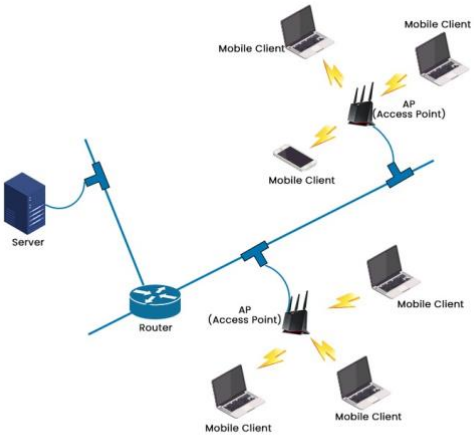


Figure 13 Wireless LAN
(source : personal documentation)

b. Metropolitan Area Network (MAN)

A MAN offers a wider coverage area than a LAN, typically ranging from 5 to 50 kilometres. It is generally used by organisations to facilitate coordination across multiple locations within a city or metropolitan area. A MAN is formed by interconnecting multiple LANs and is well-suited for campuses or companies with facilities in several locations.

c. Wide Area Network (WAN)

A WAN extends beyond the coverage of both LAN and MAN, capable of connecting users across cities, countries, and continents. WAN infrastructure requires routers, modems, CSU/DSU units, access servers, WAN switches, and core routers. Common WAN protocols include HDLC, PPP, X.25, Frame Relay, and ISDN.

d. Personal Area Network (PAN)

A PAN interconnects a computer with personal devices such as printers, speakers, and mobile phones. It has a very limited range and is not suited for long-distance communication. PAN devices may connect via Bluetooth, Wi-Fi, or data cable.

e. Storage Area Network (SAN)

A SAN is a high-speed, dedicated network comprising multiple servers and storage media. It handles very large volumes of data traffic without reducing the bandwidth available on existing LAN or WAN connections.

f. Enterprise Private Network (EPN)

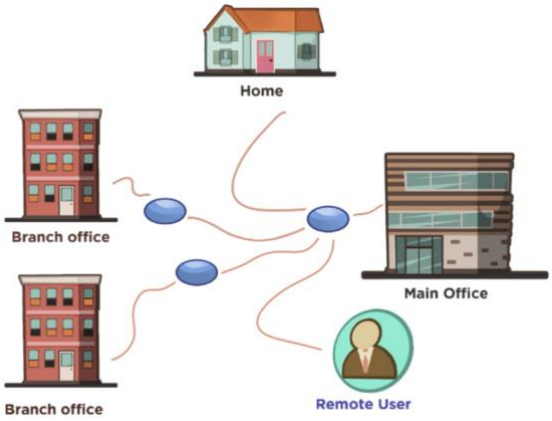


Figure 14 Enterprise Private Network (Personal Documentations)

An EPN is used by large organisations to connect administrative offices, production facilities, retail outlets, and other operational sites for the purpose of sharing network resources. Private data is stored and shared within the organisation's boundaries.

g. Virtual Private Network (VPN)

A VPN is a secure method of accessing a LAN via the internet or another public network, enabling private and secure data packet transmission. VPN technology provides three layers of digital data protection:

- Confidentiality: All data is encrypted so that even if intercepted, it cannot be read by unauthorised parties.
- Data Integrity: VPN technology safeguards the completeness and accuracy of data throughout transmission.

- Origin Authentication: VPN validates the sources of all incoming data, approving only those that pass authentication.



Figure 15 Virtual Private Network

A VPN creates a virtual tunnel through a public network, ensuring more secure and private communication.

2. Classification by Transmission Medium

a. Wired Networks

Wired networks use physical cable as the transmission medium. Three main cable types are used: coaxial cable (two concentric conductors), twisted pair cable (intertwined wire pairs), and fibre optic cable (glass or plastic fibres transmitting light signals).

b. Wireless Networks

Wireless networks use the atmosphere as the transmission medium, with electromagnetic waves facilitating device interconnection. One of the most widely recognised wireless technologies is Bluetooth

CHAPTER

02

NETWORK AND COMPUTER DEVICES

In this chapter, you will hopefully learn:

- ✓ Define what a network device is and explain its role in a computer network.
- ✓ Identify and describe the function of common network devices: server, NIC, repeater, hub, bridge, router, access point, and switch.
- ✓ Differentiate between managed and unmanaged switches.
- ✓ Explain the types and modes of wireless access points.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

□	Understanding of the basic concept of a computer network (Chapter 1).
□	Familiarity with the terms hardware and software.
□	Basic understanding of what a LAN is.

A. Definition of Network Devices

A device is a piece of equipment, while a network is a system formed by two or more interconnected items. Two or more computers are able to connect and share data resources through the network devices that link them together.

Building a computer network requires a number of core devices, each serving a specific function. This chapter provides a concise overview of the primary network devices that play a role in creating a network capable of connecting multiple computers.

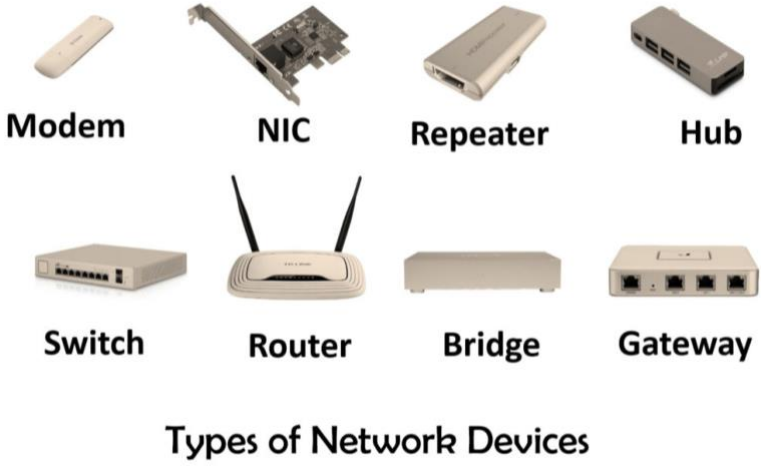


Figure 16 Types of Network Devices

B. Common Types of Network Devices

1. Server

A server is a computer system that provides specific services, most notably data storage. One of the most common types is the web server. A web server handles HTTP and HTTPS requests, receives requests from a browser, and returns web pages in the form of HTML and CSS documents.

2. Network Interface Card (NIC)

A NIC is a network card that connects a computer to a network. Without a NIC, computers cannot communicate with one another. Most computers and laptops are sold with a built-in NIC. Additional NICs may be installed if connectivity to more than one network node is required.

3. Repeater



Figure 17 Wifi Repeater could help amplifies signal in weak spots and areas

A repeater extends the coverage range of a Wi-Fi signal from a primary access point and amplifies the signal strength. Cable repeaters are also used to maintain data signal strength over longer network cable runs.

4. Hub

A hub functions as a multi-port repeater, connecting two or more computers within a network and enabling communication and data

exchange. It contains multiple Ethernet ports; any device connected to a port joins the LAN.

Hubs are classified into two types:

Active Hub	Has its own power supply and can clean, amplify, and relay network signals, thereby extending the maximum distance between nodes.
Passive Hub	Collects cables from nodes and draws power from an active hub, but cannot extend the distance between nodes.

5. Bridge

A bridge connects two or more LAN networks that use the same protocol. Functions of a bridge include:

- Connecting two LANs of the same type to form a larger combined network.
- Connecting multiple separate networks, whether of the same or different types.
- Functioning as a router on larger networks (referred to as a 'bridge router').
- Copying data frames from one network to another while maintaining connectivity.

Transparent Bridge	Acts as a connector that is invisible (transparent) to network stations.
Source Routing Bridge	Locates frames by disseminating special discovery frames across the network.

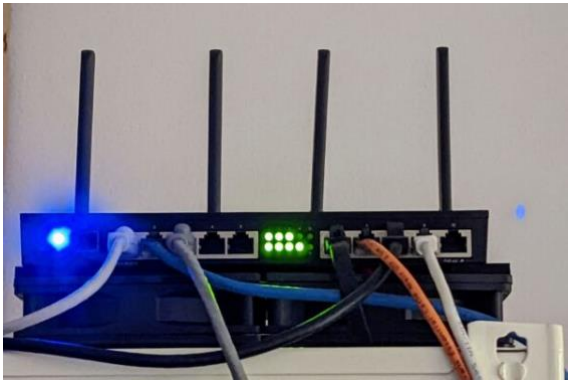


Figure 18Wireless Routers

6. Router

A router is a hardware device for connecting networks to the internet. It transmits data packets via a process called routing, forwarding packets through an internetwork connection. Routers connect LAN and WAN networks and dynamically update their routing tables. Routing information is stored in a routing table.



Figure 19 A Router with 4 antennas

7. Access Point (AP)

A wireless access point (WAP) consists of an antenna, transceiver, and RJ-45 port, and is used to create a wireless network (WLAN). Access points are available in three configurations:

Indoor AP	Designed for enclosed spaces with limited coverage. Commonly used in cafes and internet cafes.
Outdoor AP	Designed for open areas with wide coverage. Commonly used on campuses, in large buildings, or at companies.
AP Router	Can be used indoors or outdoors; specifically designed for client-server networks.

Access point operating modes include: AP mode, Repeater mode, Bridge mode, Client mode, Wireless Router mode, and AP Client Router mode.

8. Switch

A switch is a network component that connects multiple computer devices, enabling data packet exchange. It operates at the Data Link layer (Layer 2), performs error-checking before forwarding data, and supports full-duplex communication.

Managed Switch	Provides multiple management interfaces to control switch operation. Includes advanced features such as VLAN and STP support.
Unmanaged Switch	Provides basic switching functionality without customisation options. Typically lower in cost.

CHAPTER

03

NETWORK TOPOLOGY

In this chapter, you will hopefully learn:

- ✓ Define the concept of network topology.
- ✓ Describe the structure and operation of ring, star, mesh, bus, and tree topologies.
- ✓ List the advantages and disadvantages of each topology type.
- ✓ Identify which topology is best suited to a given scenario.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Knowledge of common network devices such as hubs, switches, and NICs (Chapter 2).
☐	Understanding of what a LAN and a node are.
☐	Familiarity with UTP and coaxial cable types.

A. Overview of Network Topology

Network topology refers to the method used to connect multiple computers. The connecting medium may be either wired or wireless. Network topology defines the manner in which each computer or host within a network is able to communicate with all others.

B. Types of Computer Network Topologies

1. Ring Topology

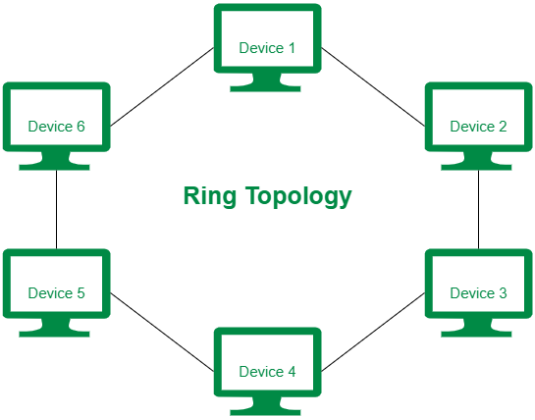


Figure 20 *Ring Topology Network*
(source:personal documentation)

Ring topology has a circular design in which each node is connected to two adjacent nodes, forming a closed loop. Each node also functions as a repeater for passing signals onward. Every node in a ring topology requires two NICs.

Ring topology is typically used for small networks and requires UTP cable. Data flows in a single direction, and a token ring tool facilitates data forwarding. Advantages:

- Straightforward to construct; unidirectional flow eliminates data collisions.
- Cable-efficient and cost-effective to install.
- Faults within the network are comparatively easy to identify.

2. Star Topology

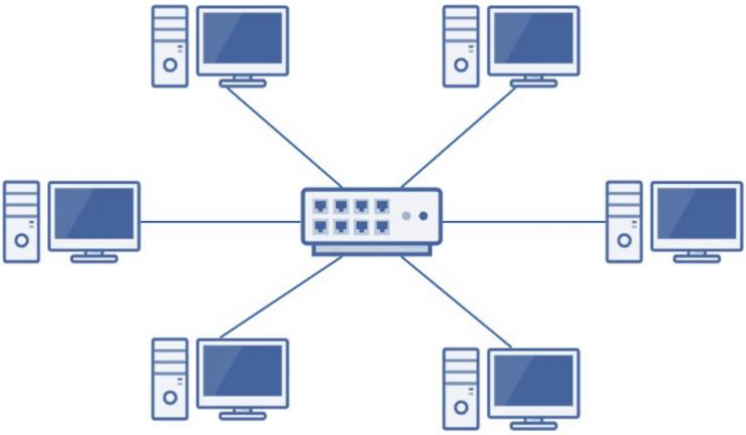


Figure 21 Star Topology Network (Personal Documentation)

Star topology connects each node via cable to a central concentrator (a hub or switch). The concentrator manages all communication traffic between nodes. Commonly used in schools, internet cafes, and offices. Steps to establish a star topology network:

1. Ensure the hub or switch is powered on.
2. Connect each node to the hub or switch using UTP cable with RJ-45 connectors.
3. Verify connectivity by checking indicator lights, then conduct a data transfer test.

4. Assign an IP address to each node within the same network address.
5. Test connectivity using the ping tool.

Advantages:

- Supports server nodes and client nodes within a single network.
- Simple maintenance; a fault in one node does not affect others.
- All computers share equal network speeds for sending and receiving data.
- Easily expandable without disrupting the network.

Disadvantages:

- Additional cabling required for each new node.
- The quality of the central concentrator directly affects data transfer performance.
- Installation costs may be high due to the volume of cabling and equipment.

3. Mesh Topology

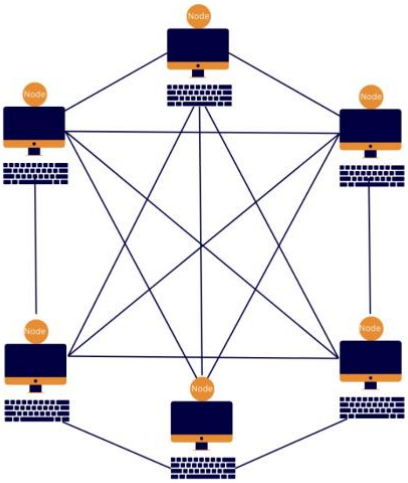


Figure 22 Mesh Topology

Mesh topology connects each node directly to every other node via cable. Each node may possess more than one NIC. Data sent between nodes travels directly to its destination without an intermediate node. Advantages:

- Network faults are detected more rapidly.
- A fault at one node does not affect the operation of other nodes.
- Faster inter-computer data transfer, as no central node is required.

Disadvantages:

- High implementation cost due to the large quantity of cabling required.
- Complex installation; each node may require multiple NICs.
- Not practical for office environments; best suited to small networks.

4. Bus Topology

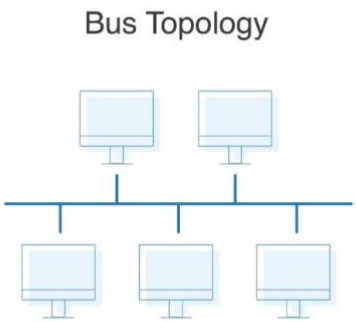


Figure 23 Bus Topology

Bus topology connects all nodes using BNC or coaxial cable. A single backbone cable serves as the main conduit. Nodes use T-connectors to attach to the backbone. Before transmitting, a node must check whether the backbone is free. Bus topology uses the CSMA/CD protocol to prevent data collisions.

Advantages:

- Simple installation; efficient use of cabling.
- Easily expandable; no concentrator required.

Disadvantages:

- Faults are difficult to isolate; a backbone fault disrupts the entire network.
- Performance degrades as the number of connected nodes increases.

6. Tree Topology

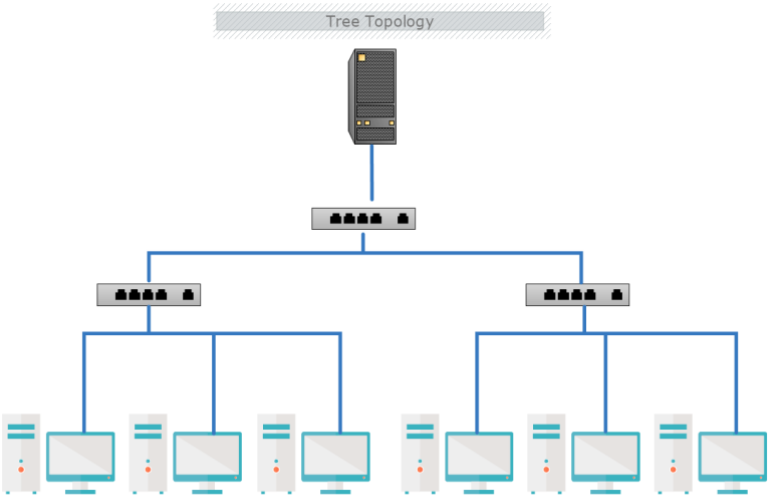


Figure 24 Tree Topology

Tree topology (also called hierarchical topology) combines characteristics of star and bus topologies, and is suitable for large-scale network deployments. It operates in a branching, hierarchical manner, with processes flowing from the highest-level node downwards.

Advantages:

- Easily expandable; a fault in one node does not affect others.
- Fault detection and data management are straightforward.

Disadvantages:

- Comparatively slow performance; requires a substantial amount of cabling.
- Backbone is susceptible to congestion under heavy traffic; maintenance is complex

CHAPTER

04

NETWORK ADDRESSING AND SECURITY

In this chapter, you will hopefully learn:

- ✓ Define an IP address and explain its purpose.
- ✓ Distinguish between Network ID and Host ID.
- ✓ Identify and describe the five IPv4 address classes.
- ✓ Explain the functions of the network layer, including logical addressing and routing.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Familiarity with the concept of a computer network and its devices (Chapters 1–2).
☐	Basic understanding of binary number representation is helpful but not required.
☐	Awareness of what a router does.

A. Network Addressing Systems

An IP address (Internet Protocol Address) is a numerical identity assigned to all computer devices so that they can communicate with one another over the internet.

Every computer, router, printer, or other network device possesses a unique IP address used to transmit data packets to the correct destination. IP addressing involves several aspects: IP address construction, address classes used for routing, and the distinction between public and private IPs. Two versions of IP address exist: IPv4 (32-bit, most widely used today) and IPv6 (128-bit, the emerging standard).

An IP address consists of two components:

Network ID	Identifies the network to which the IP address belongs. For example, in 192.168.38.1, the first three octets represent the Network ID.
Host ID	Identifies a specific endpoint — such as a server, computer, or other device — within the network.

The Network ID may be thought of as a residential estate, while the Host ID represents the individual house numbers within that estate.

B. How IP Addressing Works

An IP address consists of four octets, each containing between one and three digits with values ranging from 0 to 255. The TCP/IP

protocol interconnects all devices within a network, with IP addressing serving as the unique identifier for every device.

C. IP Address Version 4 (IPv4)

IPv4 classifies IP addresses into five categories, known as address classes:

Class	Format	Net ID	Host ID	First Octet	Use
A	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh	8 bits	24 bits	0–127	Very large networks
B	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh	16 bits	16 bits	128–191	Large and medium networks
C	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh	24 bits	8 bits	192–223	Small networks
D	1110mmmm.mmmmmmm.mmmmmmm.mmmmmmmm	N/A	N/A	224–247	IP multicasting (RFC 1112)
E	1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr	N/A	N/A	248–255	Reserved for experimental use

D. Network Layer

The network layer manages the route or path that data takes as it travels from one computer to another. This layer encompasses IP and IPX protocols, as well as router and brouter hardware. The network layer performs two primary functions:

Logical Addressing	The network layer defines an addressing scheme to identify devices on a network. The IP addresses of both sender and recipient are inserted into the packet header.
Routing	Routing is the protocol that determines the most appropriate route for transmitting data from the source to the destination.

CHAPTER

05

NETWORK INSTALLATION

In this chapter, you will hopefully learn:

- ✓ Identify the hardware and software components required for a LAN installation.
- ✓ Explain the role of a NIC in a bus-topology network.
- ✓ Follow the step-by-step procedure to configure TCP/IP on a computer.
- ✓ Verify network connectivity using the ping command.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Understanding of IP addressing, including IP address, subnet mask, and gateway (Chapter 4).
☐	Familiarity with Windows Control Panel and basic desktop navigation.
☐	Knowledge of what a LAN is and what a NIC does (Chapter 2).

A LAN installation comprises hardware and software components. Hardware includes the personal computer (PC), network interface card (NIC), and cabling. Software includes the network operating system, network adapter drivers, and network protocols.

A. Hardware Components

1. Personal Computer

A high-quality computer transmits and receives data across a network at greater speed. The choice of personal computer specification therefore has a significant bearing on network performance.

2. Network Interface Card (NIC)

For a bus topology, two NIC variants are used: Industry Standard Architecture (ISA) and Peripheral Component Interconnect (PCI). The PCI network card is the most widely deployed type in current use.

3. Cabling

The choice of cable type depends on the network topology. For a bus topology, suitable cable types include coaxial, twisted pair, and fibre optic.

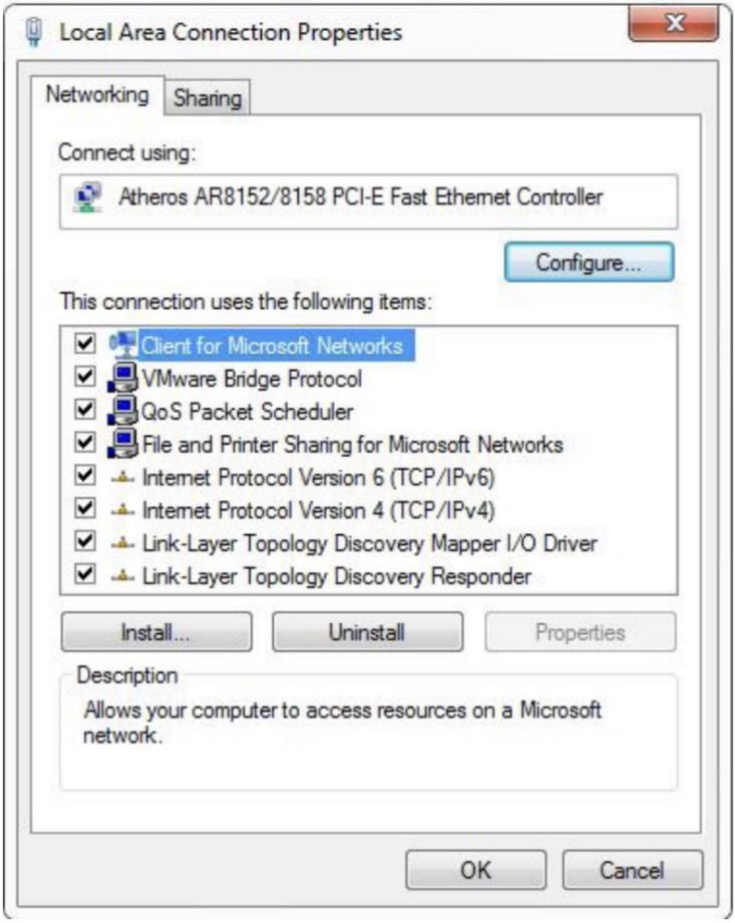
B. Installation Procedure

The following procedure describes the steps required to configure TCP/IP on a Windows-based system:

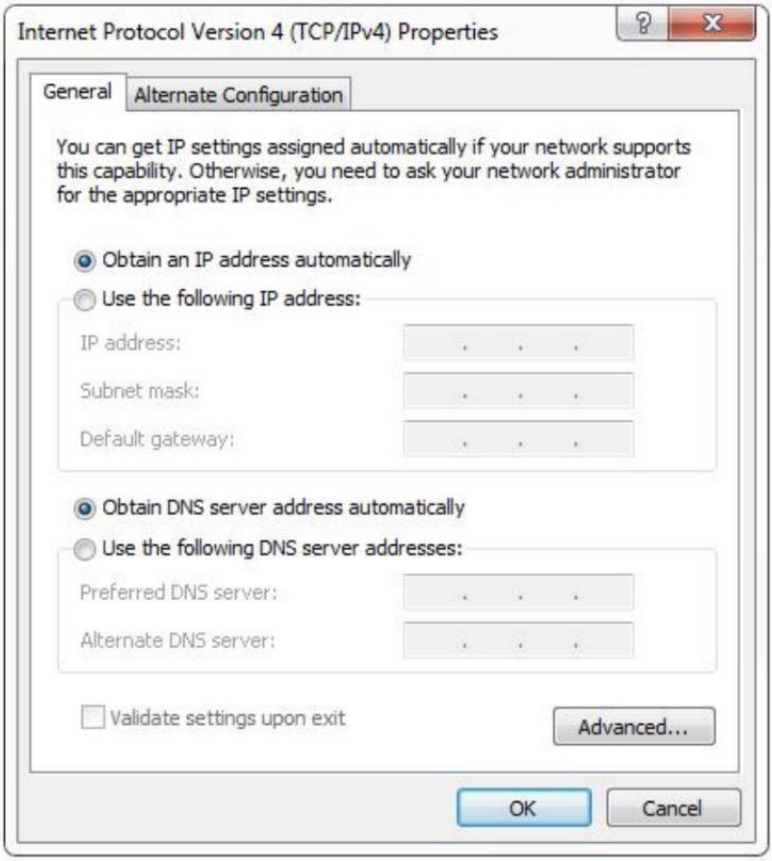
1. Navigate to Control Panel → Network Connections. The network connection icon will be displayed.



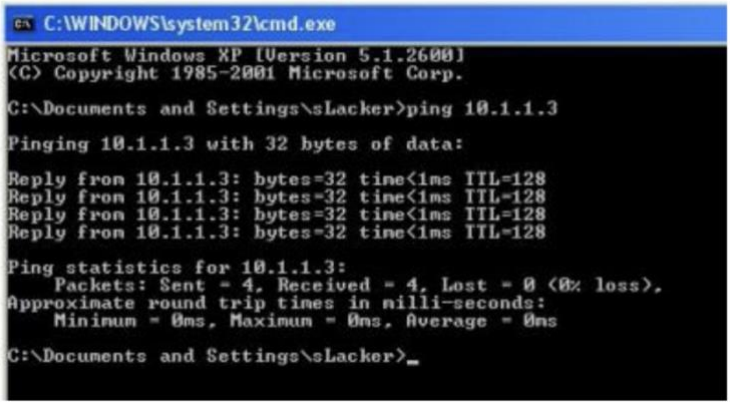
2. Right-click the network connection icon and select Disable. Then right-click again and select Properties. In the Properties window, double-click Internet Protocol (TCP/IP).



3. Enter the IP address and subnet mask. For example, if the network uses the range 192.168.0.1 – 192.168.0.200, enter the appropriate address and set the subnet mask to 255.255.255.0.



4. Click OK, then double-click the network connection icon to enable the LAN connection.



5. To verify connectivity, open the Command Prompt (Start → Run → type 'cmd' and press Enter) and type the ping command:
   `ping 192.168.0.2`

If the connection fails, the message "Request Timed Out" will appear. If the connection is successful, "Reply from..." responses will be displayed

CHAPTER

06

NETWORK SECURITY SYSTEMS

In this chapter, you will hopefully learn:

- ✓ Explain the four key properties of network security: privacy, message integrity, endpoint authentication, and non-repudiation.
- ✓ Describe six common types of network security threats.
- ✓ Define a firewall and distinguish between host-based and network-based firewalls.
- ✓ Explain how firewalls manage network traffic using accept, reject, and drop rules.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Understanding of what a computer network is and how data is transmitted (Chapters 1–2).
☐	Familiarity with the concept of IP addresses (Chapter 4).
☐	General awareness of online threats and internet safety is helpful.

A. Introduction to Network Security

Network security is one of the most critical considerations in the use of computer networks. It encompasses the measures taken to monitor and prevent unauthorised access, whether from internal or external sources. The network administrator holds primary responsibility for network security.

The four key properties of a network security system are:

Privacy	Only the intended parties should be able to understand the transmitted message. Privacy is maintained through data encryption.
Message Integrity	Data must arrive at the recipient exactly as it was sent. Internet transmission can expose data to alteration by unauthorised users.
Endpoint Authentication	Authentication ensures that the recipient can verify and trust the identity of the message or data sender.
Non-Repudiation	Prevents either party from later denying a commitment or action that was previously performed.

B. Types of Network Security Threats

No computer network is entirely immune from attack. Several categories of threat are known to exist:

1. Spoofing

Spoofing is an attack technique in which the attacker falsifies data so as to appear as a legitimate host. Variants include IP spoofing, DNS spoofing, identity spoofing, email spoofing, and web spoofing.



Figure 25 Spoofing Illustration

2. Distributed Denial of Service (DDoS)

A DDoS attack targets a server by exhausting its resources until it is no longer capable of performing its functions.

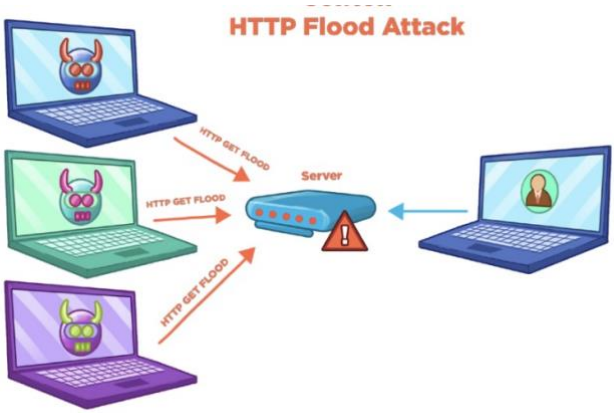


Figure 26 Illustration of Ddos Attack

2. Packet Sniffing

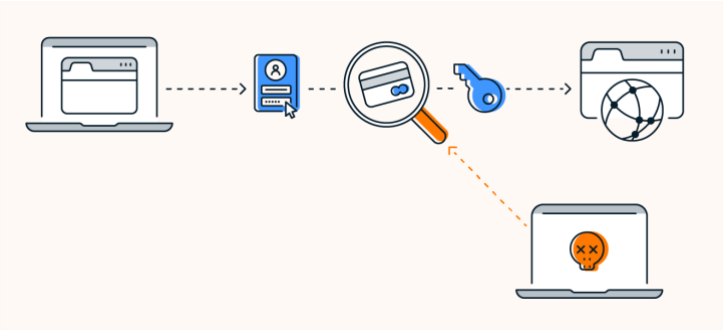


Figure 27 Packet Sniffing

Packet sniffing is the theft of data through the monitoring and analysis of data packets transmitted between a client and a server. The process proceeds in four stages:

- Collecting: capturing packets from the network.
- Conversion: converting raw packet data into readable form.
- Analysis: examining packet content.
- Data Breach: extracting and exploiting the captured data.

4. DNS Poisoning

DNS poisoning is an attack in which false IP address information is injected into a DNS server, diverting data packet traffic away from its intended destination.

5. Trojan Horse

A Trojan horse is an attack designed to extract information from a target system, such as passwords and system logs. It is a form of malware capable of causing significant damage to a system.

6. SQL Injection

SQL injection exploits a security vulnerability in the SQL layer of an application's database. This arises when user input is not correctly filtered. SQL injection remains one of the most commonly used attack vectors against websites.

C. Firewalls

> *A firewall is a system designed to prevent unwanted access to or from a network.*

A firewall may be implemented in hardware or software form, monitoring all incoming and outgoing traffic based on security rule configurations. Firewall actions are classified into three types:

Accept	Permits traffic to pass through the firewall.
Reject	Blocks traffic and returns an "unreachable error" message to the sender.
Drop	Blocks traffic silently, without returning any response.

Host-Based Firewall	A personal firewall installed on an individual computer, designed to prevent hacking and other malicious activity targeting that specific machine.
Network-Based Firewall	A system that protects an entire network from attacks originating both inside and outside the network perimeter.

CHAPTER

07

IP ROUTING

In this chapter, you will hopefully learn:

- ✓ Explain the importance of IP routing in computer network design.
- ✓ Distinguish between default, static, and dynamic routing.
- ✓ Describe the difference between IGP and EGP in dynamic routing.
- ✓ Configure static routing on two routers using Cisco Packet Tracer.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Solid understanding of IP addressing and address classes (Chapter 4).
☐	Familiarity with what a router does and how routing tables work.
☐	Access to Cisco Packet Tracer (free download from Cisco NetAcad) is recommended for the practical exercise.

A. Overview of IP Routing

IP routing is a fundamental concept in computer networking. Without a thorough understanding of routing, the design of data communications within a network cannot function effectively. Network administrators are required to be proficient in both static and dynamic routing techniques. The choice between static and dynamic routing is determined by the specific requirements of the network and the characteristics of existing network devices.

1. Default Routing

Default routing enables traffic to be routed without specifying individual destination IP addresses, giving access to all networks. It is represented by the IP address 0.0.0.0/0 in IPv4, where 0.0.0.0 represents all IP addresses and /0 represents all networks. A default route forwards packets whose destination IP address does not match any entry in the routing table.

2. Static Routing

Static routing is a manual technique requiring the explicit definition of specific IP addresses. It is commonly used to design routes within local networks and is generally not well-suited to rapidly evolving network environments.

3. Dynamic Routing

Dynamic routing employs routing protocols to automatically determine routes. It is well-suited to large and rapidly evolving networks. Dynamic routing continuously updates the routing table, enabling rapid detection of and adaptation to changes. Dynamic routing protocols are divided into two categories: Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP).

B. Routing Configuration

The following example demonstrates static routing configuration using two routers in Cisco Packet Tracer:

6. Ensure that the Cisco Packet Tracer application is installed on your device and open the application.
7. Design the desired network topology and define the IP addresses to be used.
8. Once the topology and IP addresses have been determined, configure the IP address, subnet mask, and default gateway on each PC device.
9. Configure Router0 in accordance with the defined topology and IP addressing scheme.
10. Configure Router1 in the same manner, adhering to the defined topology and IP addressing scheme.
11. Apply static routing to both routers as follows:

Device	Command	Description
Router 0	`#ip route 200.10.10.0 255.255.255.0 172.10.10.2`	Routes traffic to the destination network via the specified gateway.
Router 1	`#ip route 100.0.0.0 255.0.0.0 172.10.10.1`	Routes to a Class A destination (default netmask 255.0.0.0; single segment: 100.0.0.0).

12. Once configuration is complete, test connectivity via *Command-Line-Interface (CLI)* or by sending a direct message between devices.

This static routing exercise may be practised independently using Cisco Packet Tracer on a smartphone or laptop. Students are encouraged to create their own topology designs and experiment with different IP address ranges across Class A, B, and C address spaces.

References

Prabowo. (2020). Pengantar Jaringan Komputer [Introduction to Computer Networks]. Yogyakarta: Deepublish.

Sari, R.P. (2013). Laporan Praktikum Instalasi Jaringan Komputer [Computer Network Installation Laboratory Report]. Padang: Universitas Negeri Padang.

Yahfizham. (2019). Dasar-Dasar Komputer [Computer Fundamentals]. Medan: Perdana Publishing.

SMKN 1 Panjalu. (2020). Konsep, Prinsip, Cara Kerja dan Konfigurasi Routing Statis. Retrieved 13 September 2021 from: https://smkn1panjalu.sch.id/konsep-prinsip-dan-cara-kerja-routing-statis-administrasi-infrastruktur-jaringan-smk-tkj/

Index

Key terms and concepts referenced in this guide:

A

Access Point (AP) 23
Authentication, endpoint 50

B

Bridge 21
Bus topology 31
Brainware 2

C

Coaxial cable 15
CPU (Central Processing Unit) 4
CSMA/CD protocol 32

D

DDoS (Distributed Denial of Service) . 53
DNS poisoning 54
Default routing 60
Dynamic routing 60

E

M

MAN (Metropolitan Area Network) 10
Mesh topology 30

N

Network ID 36
Network layer 40
NIC (Network Interface Card) 18
Non-repudiation 51

P

PAN (Personal Area Network) 11
Packet sniffing 53
Privacy 50

R

Repeater 19
Ring topology 28
Router 22
Routing 40

S

SAN (Storage Area Network) 12

EPN (Enterprise Private Network) 12
Ethernet 9

F

Fiber optic cable 15
Firewall 56

H

Hardware 2
Host ID 36
Hub 20

I

Input device system 4
Internet of Things (IoT) 8
IP address 36
IPv4 38
IPv6 36

L

LAN (Local Area Network) 9
Logical addressing 40
SQL injection 55
Spoofing 52
Star topology 29
Static routing 60
Switch 24

T

TCP/IP 37
Tree topology 33
Trojan horse 55
Twisted pair cable 15

V

VPN (Virtual Private Network) 12

W

WAN (Wide Area Network) 11
WLAN (Wireless LAN) 9