

# Computer Networks

☰ Chapter No.	28
▼ Status	Completed

## ▼ Reasons to Use a Network

- A network allow computers to **communicate** with each other
- A network allow computers to share information **centrally**
- A network allow computers to **share** copies of software
- A network allows multiple computers to have **access** to the same data and program files

## ▼ Local Area Network (LAN)

- The computers in a LAN are usually in **close proximity** to each other
- Computers which are a part of the same LAN can share **files** and **hardware**, such as printers and scanners

## ▼ Computers in a LAN are typically connected using **cables** or **wireless signals**

- For a **wireless LAN**, a **central router broadcasts a signal** to which **all computers on the network connect to**
- **Security systems** need to be put in place to ensure that **unauthorised computers** do not connect to the wireless network

## ▼ A **server** is a computer that controls a network

- A **file server** is responsible for storing program files, the network operating system and users' data files
- A **domain controller server** is responsible for the authentication of user log-ons
- A **print server** is responsible for for managing shared devices

## • A **client** is a computer on the network

## ▼ The **network operating system** (OS) provides the set of instructions which all computers on the LAN must follow

### ▼ The network OS carries out tasks such as:

- Controlling **access** to the network

- Management of the **filing system**
- Management of all **applications** and **programs** available from the server
- Management of all **shared peripherals**

#### ▼ Structure of a LAN

▼ The **topology** of a network is the way in which computers are connected in the network

- Each topology has its own advantages and disadvantages, which affects the **hardware components** that have to be used

#### ▼ Bus Topology

- In a bus topology, all the computers are connected to a **central communication line**, called the bus
- If the central communication line fails, the **entire network fails**

#### ▼ Star Topology

- In a star topology, all the computers are connected to a **central connection point**, such as a hub or a switch
- If one connection between a computer and the central connection point fails, **only that computer is affected**
- If the central hub fails, the **entire network fails**

#### ▼ Hardware in a LAN

##### ▼ Hub

- A **hub** receives data from individual computers and broadcasts it back to all the devices connected to it

##### ▼ Switch

- A **switch** reads the destination label of the data and sends it only to the device for which the data is intended for
- A switch **connects devices together to form a network**
- A switch reduces the **amount of traffic** on the network by setting up a **temporary dedicated circuit** between the sender and the receiver and **releasing** that circuit once the data is transferred

#### ▼ Bridge

- A **bridge** connects two LAN segments
- A bridge **connects networks together to form a larger network**
- Each device has a **media access control (MAC) address** and a bridge maintains a table showing which MAC addresses are connected to which port
- A bridge does not **vet** the data's content to see whether it should be transferred

#### ▼ Router

- A **router**, similar to a bridge, connects two LAN segments, however it also exercises a degree of decision making, unlike a bridge
- A router **connects networks together to form a larger network**
- ▼ A router **can decide**, based on the sender and receiver, whether to allow data to be transmitted from one device to another
  - Hence, a router can be used as a **security device**

#### ▼ Gateway

- A **gateway** connects a LAN to a WAN
- A gateway ensures that the data transmitted between two networks is **appropriate** and it **monitors** the usage of the connection
- A gateway can be considered a **single point of entry** to a LAN from a larger network

#### ▼ Wide Area Networks (WAN)

- The computers in a WAN are **much further** as compared to those in a LAN
- A WAN may be spread out across a country or even internationally
- Hence, it is not possible to connect the computers **directly** using cables or wireless signals
- ▼ One way that computers can be connected to a WAN is through the use of existing infrastructure such as **telephone lines**
  - In the past, the **digital** electrical signals produced by a computer were different from the **analog** signals transmitted by the telephone lines
  - A device called a **modem** (short for modulator-demodulator) was needed to convert digital computer signals to analog signals so that they could

be transmitted by telephone lines

- At the **receiving end**, another modem would convert the analog signals back to digital signals for the receiving computer

## ▼ Comparison Between LANs and WANs

### LAN vs WAN

Aa LAN	☰ WAN
<u>It is a computer network that cover a small geographic areas and can be used by an organisation to connect devices within a site or branch</u>	It is a computer network that covers a broad area and can be used by an organisation to connect sites and branches
<u>The transmission medium is twisted pair cabling or Wi-Fi</u>	The transmission medium is fibre-optic cabling
<u>Faster data transfer rate</u>	Slower data transfer rate
<u>It is connected to end-systems, such as user systems or servers</u>	It is not connected to any end-systems
<u>Design and maintenance is easy.</u>	Design and maintenance is difficult

## ▼ The Internet

### ▼ There is no agreed definition of the structure of the internet

- The Internet can be described as a WAN, but this severely understates its **size** and **complexity**
- The Internet is not **centrally designed** or **organised**, but it instead **evolved organically** to arrive at its current form, and it is continuing to evolve

### ▼ A **hierarchy** exists within the structure of the Internet

#### ▼ An **Internet service provider (ISP)** is an organisation which allows users to access the Internet

- **Access ISPs** connect to middle tier or **regional ISPs**, which in turn connect to first tier or **backbone ISPs**
- Connections between ISPs are handled by **Internet exchange points (IXPs)**

#### ▼ The **World Wide Web (WWW)** is a distributed application available on the internet

- It consists of a **very large collection of websites**, each of which contains one or more webpages

#### ▼ Functions of the Internet

- Provide content from the WWW
- Electronic mail
- File transfer

#### ▼ Intranets

- An **intranet** is a network offering the same facilities as the Internet, but solely from within a particular organisation
- Information is made available from a **web server** and clients access material using **web browser software**

#### ▼ Access to an intranet is usually **restricted** to people within the organisation

- Security can be ensured by using **passwords** and **secure transmission lines**
- **Access controls** can be used to ensure that only specific people can access specific facilities and data on the intranet

#### ▼ As there is a **smaller volume** of content on an intranet, the content is more likely to be **relevant** to the organisation

- The amount of control means that the content on an intranet is more likely to be **updated**
- As membership is restricted and users can be easily identified, comments are more likely to be **relevant** and **sensible**
- An **extranet** is the part of an intranet that is accessible to users not in the organisation

#### ▼ Communication Protocols

- A **protocol** is a set of rules for data transmission which are agreed upon by both the sender and receiver

#### ▼ Some Items Covered by Communication Protocols

- Type of **wire** connecting two parts of the system and the **connections** used
- **Bit rate** used

- Parity used

▼ A **handshake signal** is the signal produced when two devices, which are communicating with each other, make initial contact

- This data is exchanged so that both devices can establish that they are **ready** for the communication to start and that they **agree** on the rules being used

▼ In addition to the actual data being transmitted, communication between a sender and a receiver also consists of **handshaking** and other **overheads**

- In some networks, as much as 40% or more of the transmitted data consists of these overheads
- This **increases** the time needed to transmit the actual data through the network, but it is necessary to ensure that the message is **received correctly**

#### ▼ Packet Switching

▼ When data is sent from one computer to another, the computers may not be **directly connected** to each other

- Hence, the data has to pass through **other devices**

▼ In packet switching:

- The data is split up into a number of equally-sized packets (datagrams)
- Each packet has a header which consists of the **address of the destination** and the **packet sequence number**
- These packets are then sent to other nodes, with **each packet finding the most efficient path to the destination node**
- Each time a packet reaches a node, which is an '**intersection point**', the node decides which direction to send it on to
- When the destination node receives all the packets, they are likely to be **out of sequence**, hence the destination node uses the **packet sequence numbers** to **reassemble** the packets in the correct sequence in order to receive an **accurate** message

▼ In **circuit switching**, the network reserves a route from the origin node to the destination node

- The message is sent from the origin node to the destination node as **one continuous message** and does not need to be reassembled when it

arrives

- However, this means that part of the network cannot be used by anyone else for the duration of the transmission

#### ▼ Internet Protocol Suite

- A **protocol suite** refers to a collection of related protocols
- The dominant protocol suite for Internet use is known as **TCP/IP**

#### ▼ TCP/IP Model

- Each layer **except** the physical layer represents software installed on an end-system or a router
- ▼ The software for each layer must provide the capability to receive and transmit data in **full-duplex mode** to an **adjacent layer**
  - **Full-duplex** refers to a communication mode in which both parties can communicate with each other simultaneously
- A protocol in an upper layer is **served** by protocols in the lower layers

#### ▼ TCP/IP Layers

##### ▼ Application Layer

- Provides **high-level functionality** to end users
- E.g. HTTP, SMTP, FTP

##### ▼ Transport Layer

- Provides functionality to **transmit messages between any two programs**
- E.g. TCP, UDP

##### ▼ Network Layer

- Provides functionality to **determine a route between any two devices**
- E.g. IP, ARP

##### ▼ Data Link Layer

- Provides functionality to **transmit packets from one device to an adjacent device**
- E.g. IEEE 802.2, MAC

##### ▼ Physical Layer

- Provides functionality to **transmit individual bits through a transmission medium**
- E.g. IEEE 802.3 Ethernet
- The TCP protocol operates on the **transport layer**
- ▼ The **lower layers** operate with a different protocol suite
  - A **router** does not know about the application or transport layers

## ▼ IP Addressing

- ▼ An Internet Protocol (IP) address is used to define **where** data is being transmitted
  - The aim is to assign a **unique** and **universally recognised** address for each device connected to the Internet
- ▼ Currently, the Internet functions with **IP version 4 (IPv4)** addressing
  - **32 bits (4 bytes)** are used to define an IPv4 address
  - IPv4 was devised in the late 1970s, before the **advent of modern technological devices**, and therefore its creators did not anticipate the **sudden growth** in the number of networked devices
  - As the **number of Internet users** in the world grows and as each person has an increasing **number of devices**, the IPv4 addressing system will become **inadequate** very soon
- ▼ The original system was designed as a hierarchical address with a **group of 16 bits (2 bytes) defining a network (netID)** and a **group of 16 bits (2 bytes) defining a host on the network (hostID)**
  - ▼ Example IP Address
    - 10111110 00001111 00011001 11110000
    - The first 16 bits (2 bytes) are the netID and the next 16 bits (2 bytes) are the hostID
  - ▼ As 32 bits (4 bytes) is very long, it is common to **abbreviate** the IP address using **dotted decimal notation**
    - Each set of **8 bits (1 byte)** is converted into its **denary equivalent**
  - ▼ Example IP Address Using Dotted Decimal Notation
    - 190.15.25.240
    - The netID is 190.15 and the hostID is 25.240



- ▼ Networks are split into five different classes

#### Network Classes & Properties

<u>Aa</u> Network Class	<u>IPv4</u> Range	<u>classID</u>	<u>Number of Bytes in netID</u>	<u>Number of Remaining Bits in netID</u>	<u>Number of Bytes in hostID</u>	<u>Type of Network</u>
<u>A</u>	0.0.0.0 to 127.255.255.255	0	1	7	3	Very large
<u>B</u>	128.0.0.0 to 191.255.255.255	10	2	14	2	Medium
<u>C</u>	192.0.0.0 to 223.255.255.255	110	3	21	1	Small
<u>D</u>	224.0.0.0 to 239.255.255.255	1110	-	-	-	Multi-cast
<u>E</u>	240.0.0.0 to 255.255.255.255	1111	-	-	-	Experimental

- ▼ This system does not permit a lot of **flexibility** as the difference in the **number of hosts** between the different network classes are **very large**

- Class A Network = 16,777,216 Hosts
- Class B Network = 65,536 Hosts
- Class C Network = 256 Hosts

- ▼ Solutions to Increase the Flexibility of IP Addressing

#### ▼ Solution 1 - Classless Inter-Domain Routing (CIDR)

- Each IP address is given a **suffix** which indicates how many bits are **used for the netID**

#### ▼ Example

- 195.12.6.14/21
- The first 21 bits represent the netID

#### ▼ Solution 2 - Sub-Netting

- A **subnetwork** which connects to the Internet using **one IP address** is created
- The subnetwork then allocates each of its IP addresses to **each LAN**

### ▼ Solution 3 - Network Address Translation (NAT)

- NAT involves connecting an intranet to the Internet using a **NAT box**, which only has one IP address which is visible over the Internet
- The NAT box's IP address can be used as a **sending address** or a **receiving address**
- Hosts connect to the **private network** created by the NAT box
- The IP addresses allocated to the hosts come from the range of IP addresses which are **reserved for private networks**
- Each of these IP addresses occur **once** in a network, but can be used **simultaneously by other private networks**

### ▼ A new system for IP addressing, **IPv6**, is being developed to increase the **number of available addresses**

- **128 bits (16 bytes)** are used to define an IPv6 address

### ▼ Domain Name System (DNS)

- The **domain name system (DNS)** maps human-readable domain names to IP addresses and provides a system for finding the IP address for a given individual domain name
- The system is stored as a **hierarchical distributed database** which is installed on a large number of domain name servers covering the entire Internet

#### ▼ The domain is named by the path upward from it

- For example, acjc.moe.edu.sg refers to the .acjc subdomain within the .moe subdomain within the .edu subdomain of the .sg top-level domain
- The domain name is part of a **universal resource allocator (URL)** which identifies a webpage or an email address

#### ▼ When a **domain name** is typed into a web browser, the following steps take place:

1. The web browser asks the DNS server for the **IP address of the website**.
2. If the domain is **under the jurisdiction** of that server, then the correct IP address can be sent back to the user's computer.
3. If it is **not under the server's jurisdiction**, it may be in the server's **cache of recently requested IP addresses**. If so, the IP address is retrieved and sent back to the user's computer.

4. If not, the DNS server **sends out a request to a root server**, which provides an address for a DNS server for the next level domain, and so on, until a server which can provide the the IP address is found. The IP address is then **sent to the first DNS server**.
5. The first DNS server adds the **IP address and the associated URL** into its **cache** and sends the IP address back to the user's computer
6. The user's computer communicates with the website server and the required pages are **downloaded and displayed** on the web browser.

#### ▼ Dynamic Host Configuration Protocol (DHCP)

##### ▼ Discover

- The client discovers a DHCP server by **broadcasting a discover message**

##### ▼ Offer

- The DHCP server **offers an IP address** to the client

##### ▼ Request

- The client **broadcasts a request** to the DHCP server to release the chosen IP address

##### ▼ Acknowledge

- The DHCP server **sends the IP address to the client** for acknowledgement

#### ▼ Client-Server Architecture

- **Client-server architecture** is a distributed computer system where a client carries out part of the processing and a server carries out another part
- In order for the client and server to cooperate, software called **middleware** has to be present

#### ▼ Comparison of Client & Server Applications

##### **Client VS Server Applications**

<b>Aa</b> Client Application	<b>≡</b> Server Application
<u>Starts Second</u>	Starts first
<u>Needs to know which server to contact</u>	Does not need to know which client will contact it

<b>Aa</b> Client Application	<b>≡</b> Server Application
<u>Initiates contact when communication is needed</u>	Waits passively for contact from a client
<u>Communicates with server by sending and receiving data</u>	Communicates with client by sending and receiving data
<u>Can terminate after interacting with server</u>	Continues to run after servicing one client and waits for the next client

## ▼ Comparison of General Characteristics of Client & Server Software

### Client VS Server Software

<b>Aa</b> Client Software	<b>≡</b> Server Software
<u>Consists of an arbitrary program that becomes a client temporarily whenever remote access is needed</u>	Consists of a special-purpose and privileged program dedicated to providing a service
<u>Is invoked directly by a user and executes for only one session</u>	Is invoked automatically when a system boots and continues to execute through many sessions
<u>Runs locally on a user's device</u>	Runs on a dedicated computer system
<u>Actively initiates contact with a server</u>	Waits passively for contact from arbitrary remote clients
<u>Can access multiple services as needed, but only contacts one remote server at a time</u>	Can accept connections from many clients at the same time but usually offers only one service
<u>Does not require especially powerful hardware</u>	Requires powerful hardware and a sophisticated operating system

## ▼ Advantages of Client-Server Networks Over Peer-to-Peer Networks

- Server can control the **access rights to files and programs**
- If **one client fails**, the server and other clients are **not affected**
- Resources can be **updated faster**
- It is **easier to perform a backup** of the resources on the server



## ▼ Disadvantages of Client-Server Networks Over Peer-to-Peer Networks

- If the **server fails**, the **whole network fails**
- A centralised server is **expensive** to build up and requires **professional maintenance**, which can also be **costly**

## ▼ Thin & Thick Clients

- The client-server model offers **thin and thick clients**, which refer to both **hardware and software**
  - A **thick client** is a computer that does not rely on processing done by a server
  - A **thin client** is a computer that depends on a more powerful computer for processing
- ▼ Comparison of Thin & Thick Clients

#### Thin VS Thick Clients

<u>Aa</u> Name	 Thin Clients	 Thick Clients
<u>Description</u>	Heavily dependent on having a server to allow constant access to files and to allow applications to run uninterrupted Needs to be connected to a powerful computer or server to allow processing to take place	Can work offline or online and is still able to do processing whether it is connected to a server or not
<u>Hardware Advantages</u>	Less expensive to expand as low-powered and inexpensive devices can be used All devices are linked to a server so software updates can be installed centrally Server offers protection against hacking and malware More overall control of all the clients on the network	More robust as device can carry out processing even when it is not connected to a server Clients have more control as they can store their own programs and files
<u>Hardware Disadvantages</u>	High reliance on server so if the server goes down or if there is a break in communication, the devices cannot work Despite cheaper hardware, the initial costs are generally higher than that of thick clients	Less secure as clients have to keep their own data secure Each client needs to install software updates individually Data integrity issues as many client access the same data, which may lead to inconsistencies
<u>Software</u>	Always relies on a connection to a remote server or computer to work Requires very few local resources Relies on a good, stable and fast network connection to work Data is stored on a remote server or computer	Can run some features of the software even when not connected to a server Relies heavily on local resources More tolerant of a slow network connection Can store data locally