## Evolution of Networking

8.1 Evolution of Networking

### Switching Techniques

8.2 Switching Techniques

### Data Communication Terminologies

8.3 Data Communication Terminologies

### Networking Concepts

8.4 Networking Concepts

### Transmission Medium

8.5 Transmission Medium

### Network Devices

8.6 Network Devices

### Network Topology

8.7 Network Topology

### Network Protocol

8.8 Network Protocol

### Mobile Telecommunication Technologies

8.9 Mobile Telecommunication Technologies

### E-Mail (Electronic Mail)

8.10 E-Mail (Electronic Mail)

### Protocols for Chat and Video Conferencing

8.11 Protocols for Chat and Video Conferencing

### Network threats (Malware)

8.12 Network threats (Malware)

### Prevention from threats

8.13 Prevention from threats

### Firewall

8.14 Firewall

### HTTPS

8.15 HTTPS

### Information Technology Act, 2000

8.16 Information Technology Act, 2000

### Cyber Law

8.17 Cyber Law

### Cyber Crime

8.18 Cyber Crime

### Hacking

8.19 Hacking

### IPR (Intellectual Property Rights) Issues

8.20 IPR (Intellectual Property Rights) Issues

### Introduction to web services

8.21 Introduction to web services

### E-Commerce

8.22 E-Commerce
8.1 Evolution of Networking:

**ARPANET:** The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

**Internet:** A network of networks.

**WWW:** World Wide Web started on 6\(^{th}\) August 1991, started by ‘Berners Lee’.

**Interspace:** Interspace is a client/server software program that allows multiple users to communicate online with real-time audio, video and text chat in dynamic 3D environments. Interspace provides the most advanced form of communication available on the Internet today.

8.2 Switching Techniques:

It is a way to send a message from sender to receiver. Information may be switched as it travels through various communication channels. There are three typical switching techniques available for digital traffic.

- Circuit Switching
- Packet Switching
- Message Switching

<table>
<thead>
<tr>
<th>Circuit Switching</th>
<th>Packet Switching</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires point to point connections during calls.</td>
<td>Sends data in small blocks, called packets. Packets reassembled in proper sequence at the receiver end.</td>
</tr>
<tr>
<td>Required dedicated connection</td>
<td>Not required dedicated connection</td>
</tr>
<tr>
<td>Circuit-switched networks were used for phone calls</td>
<td>packet-switched networks handled data</td>
</tr>
</tbody>
</table>
8.3 Data Communication Terminologies:

Channel: A channel is a separate path through which signals can flow. A channel has a certain capacity for transmitting information, often measured by its bandwidth in Hz or its data rate in bits per second.

Bandwidth: Bandwidth refers to the amount of information that can be transmitted over a network in a given amount of time, usually expressed in bits per second or bps.

Data Transfer Rate: The data transfer rate of a computer network connection is normally measured in units of bits per second (bps).

Larger units are Kbps, Mbps and Gbps, KBps, MBps, GBps

bps means bit per second.

Bps means Byte per second

1 kilobit per second (Kbps) = 1000 bits per second (bps).
1 megabit per second (Mbps) = 1000 Kbps or \(1000^2\) bps.

1 gigabit per second (Gbps) = 1000 Mbps

1 Terabit per second (Tbps) = 1000 Gbps

**8.4 Networking Concepts:**

**Network:**- To connect the more than one devices via a medium, is called network.

**Why do we need network?**

1. Communication
2. Resource sharing
3. Reduce Cost

**Types of Network:**

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Personal Area Network (PAN)
1. **LAN:**
   * Use in small local area, like in an institute or an organization.
   * Devices are connected via physical medium.
   * Limited distance, up to 150 Meter.
   * Example – **Intranet**

2. **MAN:**
   * Larger than LAN.
   * Used in Metropolitan cities.
   * Range up to 50 KM.

3. **WAN:**
   * Large network
   * Public
   * Example – **Internet**

4. **PAN:**
   * For very small distance
   * Private Communication
   * Example: **Bluetooth**

**8.5 Transmission Medium:**

A medium which is used to connect the devices and transfers the data from one device to another device.
8.6 Network Devices:

1. Modem
2. Hub
3. Switch
4. Gateway
5. Bridge
6. Router
7. Repeater
8. NIC (Network Interface Card)
9. RJ45 Connector

1. Modem:
   - The full form of modem is Modulator and demodulator.
   - A modem is a device or program that enables a computer to transmit data over telephone or cable lines.
   - A modem converts analog signal to digital signal and vice-versa.
   - Modem connects computer to internet.
   - There are two types of modem:
     a. Internal Modem
b. External Modem

2. Hub:
   - A network device that contains multiple ports.
   - Provides multiple connections.
   - When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
   - Two types of hub:
     a. Active Hub
     b. Passive Hub

3. Switch:
   - A switch is called smart hub.
   - Provides multiple connections
   - A device that filters and forwards packets between LAN segments.
Hub passes the frame to every port.

<table>
<thead>
<tr>
<th>HUB</th>
<th>SWITCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub passes the frame to every port.</td>
<td>Passes the frame to a specific port, because it keeps a record of MAC address.</td>
</tr>
<tr>
<td>Creates lot of traffic on network</td>
<td>Less traffic</td>
</tr>
<tr>
<td>Hub shares its bandwidth with each and every port, so bandwidth divided among all the nodes, which will degrade performance.</td>
<td>Switch allocates full bandwidth to each of its port. So user always access maximum amount of bandwidth.</td>
</tr>
<tr>
<td>Slow speed</td>
<td>Fast speed</td>
</tr>
</tbody>
</table>

4. Gateway:

   - A gateway is a network point that acts as an entrance to another network.
   - Used to connect two dissimilar networks.

5. Bridge:

   A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol, such as Ethernet.
6. **Router:**

A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs. Routers are located at gateways, the places where two or more networks connect.

A router acts as a dispatcher, choosing the best path for information to travel so it’s received quickly.

7. **Repeater:**

Network repeaters regenerate and amplify the weak signals to transmit the information for long distance.
8. **NIC** (Network Interface Card): NIC card has a physical address of a system; this physical address known as **MAC** address.

A MAC address is a 6-byte address with each byte separated by a colon. First 3-bytes have Manufacturer id and last 3-bytes represent Card id.

```
10:BE:05:56:3F:CB
```

- Manufacturer id
- Card id

9. **RJ45 Connector:** It is used for connecting computers onto Ethernet-based local area networks (LAN). RJ stands for Registered Jack. It is a standardize networking interface. 45 is the number of the interface standard. It has 8-pins.

8.7 **Network Topology:**

The term Topology refers to the way/layout in which the various nodes or computers of a network are linked together.

The following factors are considered while selecting a topology:

1. Cost
2. Reliability
3. Scalability
4. Bandwidth capacity
5. Ease of installation
6. Ease of troubleshooting
7. Delay involved in routing information from one node to another.

**Types of Topologies**
1. **Bus Topology**

It consists of one continuous length of cable (trunk) that is shared by all the nodes in the network and a terminating resistor ( terminator ) at each end that absorbs the signal when it reaches the end of line. Without a terminator the electrical signal would reach the end of copper wire and bounce back, causing errors on the network.

Data communication message travels along the bus in both directions until it is picked up by a workstation or server NIC. If the message is missed or not recognized, it reaches the end of the cabling and dissipates at the terminator. Bus Network Topology requires a multipoint connection.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Easy to install and the use for small networks.</td>
<td>1. If the main cable fails the entire network collapses.</td>
</tr>
<tr>
<td>2. Requires less cable</td>
<td>2. Difficult to reconfigure, due to more connections.</td>
</tr>
<tr>
<td>3. Failure of one node does not affect the network functioning.</td>
<td>3. Difficult to troubleshoot</td>
</tr>
<tr>
<td>4. Cost is less</td>
<td>4. Slow, due to traffic on single cable</td>
</tr>
<tr>
<td>5. New node can be easily added</td>
<td>5. Only one device transmits at a time, other devices wait for their turn.</td>
</tr>
</tbody>
</table>

2. **Ring Topology**

The physical ring Topology is a circular loop of point-to-point links. Message travel around the ring from node to node in a very organized manner. Each workstation checks the message for a matching destination address. If the address doesn’t match the node simply regenerates the message and sends it on its way. If the address matches, the node accepts the message and sends a reply to the originating sender.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Easy to troubleshoot</td>
<td>1. Requires more cable</td>
</tr>
<tr>
<td>2. There is no master computer on controller.</td>
<td>2. More Expensive</td>
</tr>
<tr>
<td>3. There are no collisions.</td>
<td>3. A break in cable ring brings down entire network</td>
</tr>
<tr>
<td>5. Easy fault detection and isolation</td>
<td></td>
</tr>
</tbody>
</table>
3. **Star Topology**

The physical star Topology uses a central controlling hub with dedicated legs pointing in all directions – like points of a star. Each network device has a dedicated point-to-point link to the central hub. There is no direct link between these computers and the computers can communicate via central controller only.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Easier to add new node or modify any existing node without disturbing network.</td>
<td>1. Central node dependency. If the central controller or hub fails, entire system collapses.</td>
</tr>
<tr>
<td>2. Fast Speed</td>
<td>2. Cabling cost is more</td>
</tr>
<tr>
<td>3. If any local computer or link fails, the entire system does not collapse</td>
<td>3. Difficult to install</td>
</tr>
<tr>
<td>4. Easy fault detection and isolation</td>
<td></td>
</tr>
<tr>
<td>5. Central node control</td>
<td></td>
</tr>
</tbody>
</table>

4. **Mesh Topology**

In mesh topology, each node is connected to every other node in the network i.e. each node has a dedicated point to point link to every other node as shown. Dedicated means that the link carries the traffic only between two devices it connects.

In this way there exist multiple paths between two nodes of the network. In case of failure of one path, the other one can be used.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. It is robust. Failure of one node does not collapse the entire system.</td>
<td>1. Network installation and reconfiguration difficult.</td>
</tr>
<tr>
<td>2. No traffic congestion</td>
<td>2. High cabling cost. If there are n nodes in the network then each node has (n-1) connections.</td>
</tr>
<tr>
<td>3. Dedicated links ensure faster transmission</td>
<td></td>
</tr>
<tr>
<td>4. Point to point links makes fault identification and isolation easier.</td>
<td></td>
</tr>
</tbody>
</table>
5. Tree Topology

This topology has Hierarchical structure. This topology connects the node via hubs. Hub, which is present at top level, is called root hub or active hub. Another hub is called secondary hub or passive hub.

![Tree Topology Diagram](image)

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. New node can be added easily.</td>
<td>1. If the backbone line breaks, the entire segment goes down.</td>
</tr>
<tr>
<td>2. Signal can travel for long distance.</td>
<td>2. More difficult to configure</td>
</tr>
<tr>
<td>3. Isolate and prioritize communication.</td>
<td>3. Higher cabling cost</td>
</tr>
</tbody>
</table>

6. Hybrid Topology:

It is a composition of more than one topology.

![Hybrid Topology Diagram](image)
8.8 Network Protocol:

1. TCP: Transmission Control Protocol – 4 layers

<table>
<thead>
<tr>
<th>Application Layer</th>
<th>Transport Layer</th>
<th>Internet</th>
<th>Network Interface</th>
</tr>
</thead>
</table>

2. IP: Internet Protocol

Each computer has unique address over internet, is called IP address. An IP address is an identifier for a computer or device on a TCP/IP network.

An IPv4 address (dotted-decimal notation)

172.16.254.1

10101100, 00010000, 11111110, 00000001

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes

Two types:

I. IPv4 (32-bits or 4-bytes): IPv4 addresses are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 192.168.1.1.

II. IPv6 (128-bits or 16-bytes)

3. FTP (File Transfer Protocol): use to transfer files from one computer to another computer.

4. PPP (Point to Point Protocol)

5. HTTP (HyperText Transfer Protocol): To transfer the hypertext pages over internet.

6. Telnet (TELcommunication NETwork): A network protocol that allows a user on one computer to log into another computer (remote) that is part of the same network or on the internet.
7. **GSM**: GSM (Global System for Mobile communication) is a digital mobile telephony system that digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot.

8. **CDMA**: Code Division Multiple Access (CDMA) is a digital air interface standard, claiming eight to fifteen times the capacity of traditional analog cellular systems.

Each user is **separated by a unique code**; all users can share the same frequency band. CDMA is a *spread spectrum technology*, which means that it spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal.

9. **GPRS**: General Packet Radio Service is a packet-switching technology that enables data transfers through cellular networks (wireless). It is used for mobile internet, MMS and other data communications. In theory the speed limit of GPRS is 115 kbps, but in most networks it is around 35 kbps.

10. **WLL**: Wireless Local Loop is a system that connects subscribers to the local telephone station wirelessly.

---

Fig. : Architecture of WLL

**FSU : Fixed Subscriber Unit**  **BSC : Base Station Controller**  **BTS: Base Transceiver Station**
8.9 Mobile Telecommunication Technologies:

Firstly, when wireless generation started, it was analog communication. That generation is 1G. They used various analog modulation for data transfer. Now when the communication migrated from analog to digital, the foundation of latest communication were led. Hence came 2G.

1G Technology:

- 1G refers to the first generation of wireless telephone technology, mobile telecommunications which was first introduced in 1980s and completed in early 1990s.
- It’s Speed was upto 2.4kbps, allowed the voice calls in one country.
- It used Analog Signal and AMPS was first launched in USA in 1G mobile systems

Drawbacks:
- Poor Voice Quality
- Poor Battery Life
- Large Phone Size
- No Security
- Limited Capacity
- Poor Handoff Reliability

2G Technology:

- 2G technology refers to the 2nd generation which is based on GSM.
- It was launched in Finland in the year 1991 and used digital signals.
- It’s data speed was upto 64kbps.
**Features include:**

- It enables services such as text messages, picture messages and MMS (multi media message).
- It provides better quality and capacity.

**Drawbacks:**

- 2G requires strong digital signals to help mobile phones work. If there is no network coverage in any specific area, digital signals would weak.
- These systems are unable to handle complex data such as Videos.

**3G Technology:**

- 3G technology refer to third generation which was introduced in year 2000s.
- Data Transmission speed increased from 144kbps- 2Mbps.
- Typically called Smart Phones and features increased its bandwidth and data transfer rates to accommodate web-based applications and audio and video files.

**Features Include:**

- Providing Faster Communication
- Send/Receive Large Email Messages
- High Speed Web / More Security
- Video Conferencing / 3D Gaming
- TV Streaming/ Mobile TV/ Phone Calls
- Large Capacities and Broadband Capabilities
- 11 sec – 1.5 min. time to download a 3 min Mp3 song.

**Drawbacks:**

- Expensive fees for 3G Licenses Services
- It was challenge to build the infrastructure for 3G
- High Bandwidth Requirement
- Expensive 3G Phones.
- Large Cell Phones
4G Technology:

- 4G technology refers to or short name of fourth Generation which was started from late 2000s.
- Capable of providing 100Mbps – 1Gbps speed.
- One of the basic terms used to describe 4G is MAGIC.

Features Include:

- Mobile Multimedia
- Global Mobility Support
- Integrated Wireless Solution
- Customized Personal Services
- Also known as Mobile Broadband Everywhere
- The next generations of wireless technology that promises higher data rates and expanded multimedia services.
- Capable to provide speed 100Mbps-1Gbps.
- High QOS and High Security
- Provide any kind of service at any time as per user requirements, anywhere.
- More Security
- High Speed
- High Capacity
- Low Cost Per-bit

Drawbacks:

- Battery usage is more
- Hard to implement
- Need complicated hardware
- Expensive equipment required to implement next generation network.
The basic difference between 3G and 4G is in data transfer and signal quality.

<table>
<thead>
<tr>
<th>Technology</th>
<th>3G</th>
<th>4G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Transfer Rate</td>
<td>3.1 MB/sec</td>
<td>100 MB/sec</td>
</tr>
<tr>
<td>Internet Services</td>
<td>Broadband</td>
<td>Ultra Broadband</td>
</tr>
<tr>
<td>Mobile – TV Resolution</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>5-20 MHz</td>
<td>100 MHz</td>
</tr>
<tr>
<td>Frequency</td>
<td>1.6-2 GHz</td>
<td>2-8 GHz</td>
</tr>
<tr>
<td>Download and upload</td>
<td>5.8 Mbps</td>
<td>14 Mbps</td>
</tr>
</tbody>
</table>

8.10 E-Mail (Electronic Mail):

E-Mail is a method to send the messages in digital form. E-mail is a message that may contain text, files, images, or other attachments sent through a network to a specified individual or group of individuals.

SMTP (Simple Mail Transfer Protocol) is a protocol which is used to transfer the e-mail from sender side. This protocol is known as push protocol.

POP3 (Post Office Protocol version 3): This protocol is used to access e-mail from the server to receiver. This protocol is known as pull protocol.
IMAP (Internet Mail Access Protocol): Internet Message Access Protocol (IMAP) is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection.

8.11 Protocols for Chat and Video Conferencing:

VoIP: VoIP (voice over IP) is the transmission of voice and multimedia content over Internet Protocol (IP) networks. This protocol is used for chat and video conferencing over internet.

Wi-Fi: Wi-Fi (Wireless Fidelity) is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections.

WiMax: WiMAX technology is a broadband wireless data communications technology based around the IEE 802.16 standard providing high speed data over a wide area. The letters of WiMAX stand for Worldwide Interoperability for Microwave Access (AXess), and it is a technology for point to multipoint wireless networking.

8.12 Network threats (Malware):

Malware is an abbreviated term meaning “malicious software.” This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner.

1. Virus
2. Worms
3. Trojan Horse
4. Cookies
5. Spams
6. Spyware
7. Adware

1. Virus: A virus is a piece of program code that attaches itself to legitimate program code, and runs when the legitimate program runs. It can then infect other programs in that computer or network.

A virus can be repaired, and its damage can be controlled by using good backup procedure.

2. Worms: A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down. A virus modifies a program; a worm however does not modify a program. Instead it replicates itself again and again.
3. **Trojan horse**: A Trojan horse is a hidden piece of code, like a virus. A virus modifies information whereas A Trojan horse attempts to reveal confidential information to an attacker.

4. **Cookies**: A cookie is just one or more pieces of information stored as text strings in a text file on the disk of the client computer (i.e. the web browser).

5. **Spam**: Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

6. **Spyware** - Software that may be installed as part of another program. It may also be installed when a user visits a website with malicious code or when an already running process loads and installs it. This program is designed to report on what the user does to the program creator.

7. **Adware**: Software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

8.13 **Prevention from threats:**

- Use Genuine and licensed softwares. Avoid pirated softwares.
- Visit authentic and official websites.
- Never download the contents or files from suspicious websites.
- Never share your password or account number over email or message.
- Do not follow links from e-mails when performing financial transaction.
- Be aware of callers, pop-ups, websites or emails asking for personal information.
- Use firewall and reliable anti-virus software.
- Never share your personal information in public domain.
- Regularly change the passwords of your account.

8.14 **Firewall:**

A firewall is a device (or software feature) designed to control the flow of traffic into and out-of a network. In general, firewalls are installed to prevent attacks.

**Hardware Firewall vs Software Firewall:**

Hardware Firewall:

- Protect an entire network
- Implemented on router level
- Usually more expensive, harder to configure
Software Firewall:

- Protect a single computer
- Usually less expensive, easier to configure

**How does a software firewall work:**

- Inspects each individual “packet” of data as it arrives at either side of the firewall.
- Determines whether it should be allowed to pass through or if it should be blocked.

**Types of Firewall:**

1. Packet filtering firewall
2. Application level gateway
3. Circuit level gateway

**8.15 HTTPS:**

HTTPS stands for Hypertext Transfer Protocol Secure. It is the protocol where encrypted HTTP data is transferred over a secure connection. HTTPS does encryption of data between a client and a server, which protects against eavesdropping, forging of information and tampering of data.

**8.16 Information Technology Act, 2000**

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

The original Act contained 94 sections, divided in 19 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures.
Commission of cybercrime may be divided into three basic groups:

- Individual
- Organisation
- Society at Large

**Against Individual**
- Harassment via Emails
- Cyber Stalking
- Dissemination of obscene material
- Defamation
- Hacking/Cracking Indecent Exposure
- Computer Vandalism
- Transmitting a Virus
- Network Trespassing
- Unauthorized Control over Computer System
- Hacking/Cracking

**Against Organisation**
- Hacking & Cracking
- Possession of unauthorized Information
- Cyber- Terrorism against Government Organization
- Distribution of Pirated Software Etc

**Against Society at Large**
- Pornography
- Polluting the youth through indecent exposure
- Trafficking

**8.17 Cyber Law:** Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation.

**8.18 Cyber Crime:** Criminal activities carried out by means of computers or the Internet.

**8.19 Hacking:** gain unauthorized access to data in a system or computer.

**8.20 IPR (Intellectual Property Rights) Issues:**

**Intellectual Property Rights:** Intellectual property rights (IPR) is the term applied to the legal protection afforded to innovative and creative materials. It allows owner of IPR to gain from the use of the material and thereby to encourage innovation and creativity.
IPR Issues:

- Copyright law
- The law of confidence
- Patent law
- Design law
- Trademarks
- Copyright and computer programs
- Database copyright and the database right
- Criminal offences

8.21 Introduction to web services:

8.21.1 WWW: World Wide Web is an information system where websites and webpages are interconnected and accessible through URL. It is also known as Web.

8.21.2 HTML: HTML is the standard markup language for creating Web pages.

- HTML stands for Hyper Text Markup Language
- HTML describes the structure and design of Web pages using markup
- HTML elements are represented by tags
- Browsers do not display the HTML tags, but use them to render the content of the page
- The current version of HTML is HTML 5.0

A simple HTML Code:

```
<html>
<head>
<title>My first web page</title>
</head>
<body>
<h1>My First Heading</h1>
<p>My first paragraph</p>
</body>
</html>
```

OUTPUT

My First Heading
My first paragraph

8.21.3 XML:

- XML stands for EXtensible Markup Language
- XML is a markup language much like HTML
- XML was designed to store and transport data
• XML was designed to be self-descriptive
• XML is a W3C Recommendation

<table>
<thead>
<tr>
<th>S. No.</th>
<th>HTML</th>
<th>XML</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HyperText Markup Language.</td>
<td>eXtensible Markup Language.</td>
</tr>
<tr>
<td>2</td>
<td>designed to display data with focus on how data looks.</td>
<td>XML was designed to be a software and hardware independent tool used to transport and store data, with focus on what data is.</td>
</tr>
<tr>
<td>3</td>
<td>HTML is case insensitive.</td>
<td>XML is case sensitive.</td>
</tr>
<tr>
<td>4</td>
<td>HTML is used for designing a web-page to be rendered on the client side.</td>
<td>XML is used basically to transport data between the application and the database.</td>
</tr>
<tr>
<td>5</td>
<td>HTML has its own predefined tags.</td>
<td>Uses custom tags defined by the user.</td>
</tr>
<tr>
<td>6</td>
<td>HTML is not strict if the user does not use the closing tags.</td>
<td>XML makes it mandatory for the user to close each tag that has been used.</td>
</tr>
<tr>
<td>7</td>
<td>HTML does not preserve white space.</td>
<td>XML preserves white space.</td>
</tr>
<tr>
<td>8</td>
<td>HTML is about displaying data, hence static.</td>
<td>XML is about carrying information hence dynamic.</td>
</tr>
</tbody>
</table>

8.21.4 Domain Name:

Domain names are used to identify one or more IP addresses. Domain names are used in URLs to identify particular web page.

For example,  [http://www.kvongcbrd.com/english-results.htm](http://www.kvongcbrd.com/english-results.htm)

<table>
<thead>
<tr>
<th>URL</th>
<th><a href="http://www.kvongcbrd.com/english-results.htm">http://www.kvongcbrd.com/english-results.htm</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>kvongcbrd.com</td>
</tr>
<tr>
<td>Web Page</td>
<td>english-results.htm</td>
</tr>
<tr>
<td>Protocol</td>
<td>http</td>
</tr>
</tbody>
</table>

Every domain name has a suffix that indicates which top level domain (TLD) it belongs to. There are only a limited number of such domains. For example:

- **gov** - Government agencies
- **edu** - Educational institutions
- **org** - Organizations (nonprofit)
- **mil** - Military
- **com** - commercial business
- **net** - Network organizations
- **in** - India
- **th** – Thailand
Because the Internet is based on IP addresses, not domain names, every Web server requires a Domain Name System (DNS) server to translate domain names into IP addresses.

8.21.5 **URL:** Uniform Resource Locator. It is the global address of documents and other resources on the World Wide Web.

8.21.6 **Website:** Collection of web pages which are interlinked to one another. These pages are hypertext pages and link between pages is known as hyperlink.

8.21.7 **Web browser:** It is application software through which user can access internet. Example: internet explorer, Google chrome, Mozilla Firefox, opera, UC browser

8.21.8 **Web Server:** A web server is a system that uses HTTP to accept request and serve the web pages as response to users. Every web server has IP address.

Example: Apache web server, Microsoft’s Internet Information Server (IIS) and **nginx** (pronounced engine X) from NGNIX.

8.21.9 **Web Hosting:** Web hosting is a service that allows organizations and individuals to post a website on the Internet. A web host, or web hosting service provider, is a business that provides the technologies and services needed for the website or webpage to be viewed in the Internet. Websites are hosted, or stored, on special computers called servers.

8.21.10 **Web Scripting:** Programming languages which are used to design dynamic web pages, are known as web scripting languages. There are two types of web scripting languages:

1. **Client Side Scripting**
2. **Server Side Scripting**

1. **Client Side Scripting:** The programming language which executes on client side is known as client side scripting.

There are many client-side scripting languages:
- JavaScript
- VBScript
- HTML (Structure)
- AJAX
- jQuery etc.

2. **Server Side Scripting:** Program that runs directly on the server.

There are several languages that can be used for server-side programming:
- PHP (Hypertext Preprocessor)
- ASP (Active Server Pages)
- Java and JSP (Java Server Pages)
- Python

8.21.11 **Cloud Computing:** Sharing the resources over internet. A user can access hardware and software remotely on a network or internet by paying some money or free. **Example:** Google drive, One drive etc.

8.21.12 **Web 2.0:** The second stage of development of the Internet, characterized especially by the change from static web pages to dynamic web pages and the growth of social media.

8.21.13 **VoLTE:** Voice over Long-Term Evolution (VoLTE) is a standard for high-speed wireless communication for mobile phones and data terminals.

8.22 **E-Commerce:**
E-Commerce stands for electronic commerce. E-commerce means buying and selling of goods, products and services over the internet. Transactions through internet or electronic media is also a part of e-commerce.

There are four types of transactions in e-commerce:

i. Business to Business (B2B)
ii. Business to Customer (B2C)
iii. Customer to Business (C2B)
iv. Customer to Customer (C2C)

The money/payment can be transferred using different ways, which are:

A. Online Banking
B. Mobile Banking
C. Payment Apps and services (e-Wallet, UPI)

**A. Online Banking:** Online Banking used different types of methods to make the payment. It includes Internet Banking and payment using Debit/Credit Cards.

**Internet Banking:** It is a simple way of paying for online purchases directly from the customer’s bank. Net banking does not require the user to have a card for payment purposes but the user needs to register with his/her bank for the net banking facility. While completing the purchase the customer just needs to put in their net banking userid and password.

**Payment using Debit/Credit Card:** It is similar to internet banking. To make the transaction using debit/credit card, a user should know the card number, name on the card, CVV/CVN number, Valid through etc.

**CVV:** Card Verification Value
**CVN:** Card Verification Number
B. Mobile Banking: Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet.

C. Payment Apps and Services: A user has to create an account with these apps. It is a prepaid account that allows a customer to store multiple credit cards, debit card and bank account numbers in a secure environment. This eliminates the need to key in account information every time while making payments. Once the customer has registered and created E-Wallet profile, he/she can make payments faster.

Example: BHIM, Paytm, PhonePe etc.