

UNIT-II

2.1 THE NETWORK INFRASTRUCTURE FOR E-COMMERCE

Introduction to Information Superhighway (I-Way)

Electronic commerce needs a network infrastructure to transport the content (data) used for business purpose. Information superhighway is also known as interactive or multimedia superhighway. The information superhighway is a term coined by Vice President Albert Gore when giving a speech on January 11, [1994](#) describing the future of computers accessing and communicating over a world-wide network.

Basically, the term I-way describes a high-capacity (broadband), interactive (two-way) electronic pipeline to the home or office that is capable of simultaneously supporting a large number of electronic commerce applications and providing interactive connectivity between users and services and between users and other users. It is envisioned to [provide](#) very [high](#) speed [access](#) to [information](#) in all [forms](#) (text, [graphics](#), audio, [video](#)) [via](#) a [telephone](#) or wireless [connection](#).

2.2 INTERNET AND INTRANET BASED E-COMMERCE- ISSUES, PROBLEMS AND PROSPECTS

The Internet, intranet, and extranet are the most popular platforms for e-commerce. In Internet is the most common platform for B2C e-commerce; the intranet is most the common for platform for corporate internal management; and the extranet is the most common platform for B2B e-commerce.

Network Type	Typical Users	Access	Type of information
The Internet	Any individual with dial-up access or LAN	Unlimited public; no restrictions	General public, and advertorial

Intranet	Authorized employees only	Private and restricted	Specific, corporate, and proprietary
Extranet	Authorized groups from collaborating companies	Private and authorized outside partners	Shared in authorized collaborating groups

The Internet

1. The Internet is a public and global communication network that provides direct connectivity to anyone over a local area network (LAN) or **Internet Service Provider (ISP)**.
2. The Internet is a public network that is connected and routed over gateways. End users are connected to local access providers (LANs or ISPs), who are connected to the Internet access providers, to network access providers, and eventually to the Internet backbone.
3. Since access to the Internet is open to all, there is a lack of control that may result in an unruly proliferation of information.

The Intranet:

1. An intranet is a corporate LAN or wide area network (WAN) that uses Internet technology and is secured behind company's firewalls (see security and protection).
2. The intranet links various servers, clients, databases, and application programs like Enterprise Resource Planning (ERP). Although intranets are developed on the same TCP/IP protocol as the Internet, they operate as a private network with limited access.
3. Only authorized employees are able to use it. Intranets are limited to information pertinent to the company and contain exclusive and often proprietary and sensitive information.
4. The firewalls protect the intranets from unauthorized outside access; the intranet can be used to enhance the communications and collaboration among authorized employees, customers, suppliers, and other business

partners.

5. Since the intranet allows access through the Internet, it does not require any additional implementation of leased networks. This open and flexible connectivity is a major capability and advantage of intranet. Intranets provide the infrastructure for many **intrabusiness commerce** applications.

The Extranet

1. An extranet, or “extended intranet”, uses the TCP/IP protocol network of the Internet, to link intranets in different locations.
2. Extranet transmission is usually conducted over the Internet, which offers little privacy or transmission security.
3. Therefore, when using an extranet, it is necessary to improve the security of connecting portions of the Internet. This can be done by creating tunnels (see paragraph on security and protection) of secured data flows, using cryptography and authorization algorithm.
4. The Internet with tunneling technology is known as a **virtually private network (VPN)**.
5. Extranets provide secured connectivity between corporation’s intranets and the intranets of its business partners, material suppliers, financial services, government, and customers.
6. Access to intranets is usually limited by agreements of the collaborating parties, is strictly controlled, and is only available to authorized personnel.
7. The protected environment of the extranet allows groups to collaborate, sharing information exclusively, and exchanging it securely.
8. Since an extranet allows connectivity between businesses through the Internet, it is an open and flexible platform suitable for supply chain management.
9. To increase security, many companies replicate the database they are willing to share with their business partners and separate them physically from their regular intranets.

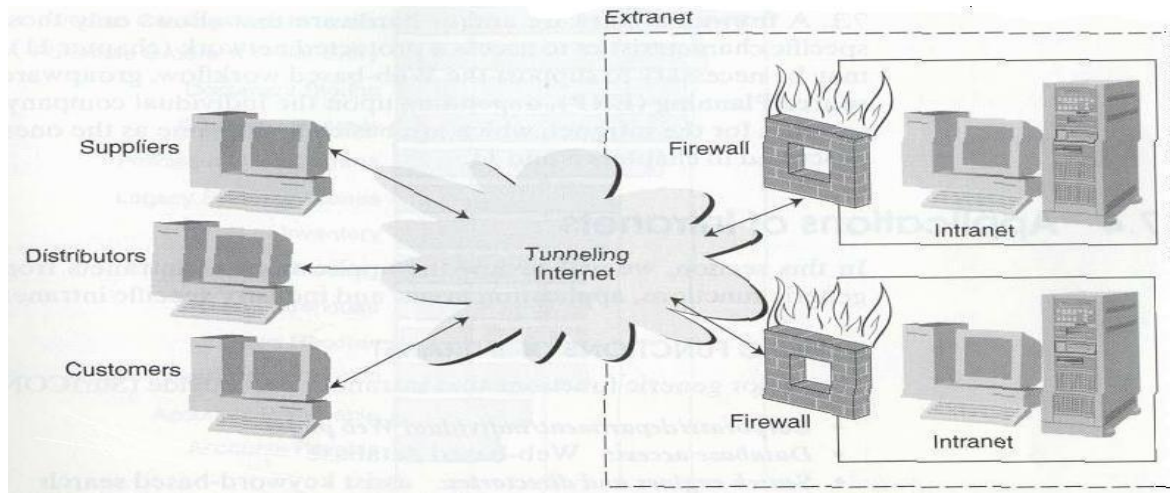


Figure Diagrammatic Contrast of the Internet, Intranet, and Extranet
Q. Compare internet, intranet and extranet? Or different between internet, intranet, and extranet?

Internet	Intranet	Extranet
It is a global system of interconnected computer networks.	It is a private network specific to an organization.	It is a private network that uses public network to information with suppliers vendors
Not regulated by any one	It is regulated by an organization	It is regulated by multiple organizations.
Thus content in the network is accessible to every one connected.	Thus content in the network is accessible only to members of organization.	The content in the network is accessible to members of organization and external members with access to network.
It is largest in terms of number of connected device.	It is small network with minimal number of connected device.	The number of devices connected is comparable with intranet.
It is owned by no one.	It is owned by single	It is owned by single/multiple

	organization	organization.
It is means of sharing information through out the world.	It is means of sharing sensitive information through out organization	It is means of sharing information between members and external members.
Security is depending of the user of device connected to network.	Security is enforced via a firewall.	Security is enforced via a firewall that separates internet and extranet.
Users can access internet anonymously.	Users should have valid username/password to access intranet.	Users should have valid username/password to access extranet.

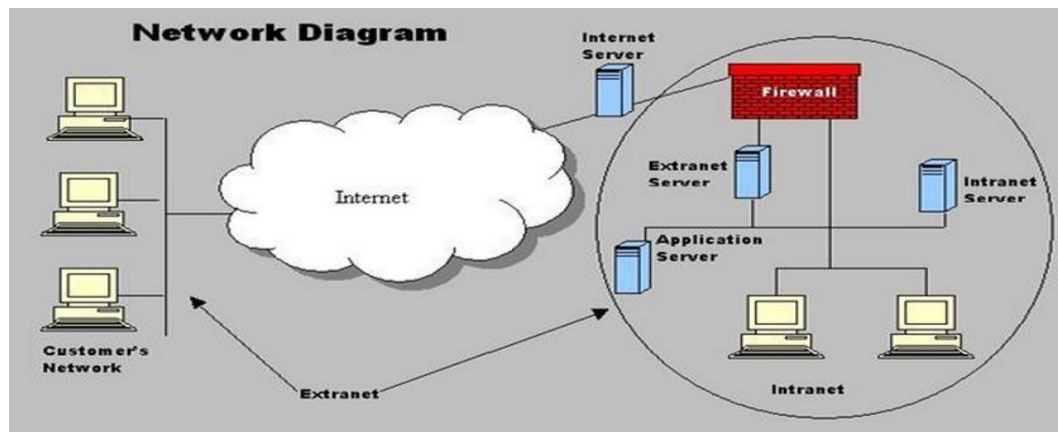


Fig: Relationship of Intranet and Extranet with Internet.

2.3 INTERNET AS A NETWORK INFRASTRUCTURE

Network Concept: In general, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. Networks are used to make work and communication more efficient. A network connects computers, but can also connect other devices such as shared printers, removable media drives, scanners, and other equipment.

Networks enable people to share resources, including printers, hard disks, and applications, which can greatly reduce the costs of providing these resources to each person in a company. Networks are built around this idea, connecting shared sources resources to their consumers. Several terms are used to describe these network devices, including hosts, nodes, workstations, peers, servers, and clients. Any device capable of communicating on the network is also referred to generically as a node.

A typical network like the one in figure below has three basic hardware components: one or more servers or host computers (including microcomputers and mainframes), clients (PCs), and a circuit or network system, which is the path over which they communicate. There are also devices in the circuit that perform special functions such as hubs, switches, routers, bridges, and gateways.

2.4 NETWORK ACCESS EQUIPMENTS:

Network Devices: Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

8. NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

2.5 INTRODUCTION TO BROADBAND TECHNOLOGY

Broadband is defined as a high bandwidth connection to the Internet. Broadband is easier and faster to use than the traditional telephone and modem as information can be sent and downloaded much quicker. It involves large volumes of information being carried at high speeds to your PC. This allows websites, text, graphics, music and videos to be experienced in real time. Broadband, therefore, has many features that can be taken advantage of in the home or office:

- The connection to the Internet is always on, allowing for constant Internet access and no need to dial up.
- The phone line is unaffected; this means that you can make telephone calls whilst the Internet is on.
- Websites, music and videos can be downloaded at a fast rate.
- You can receive uninterrupted real time services, such as Internet radio, streaming video and voice-over-ip, phone calls.

In general, broadband refers to telecommunication in which a wide [band](#) of frequencies is available to transmit information. Because a wide band of frequencies is available, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).

FRAME RELAY

- Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide Area Networks (WANs).
- It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation.
- Also, it provides a congestion control mechanism to reduce the network overheads due to congestion. It does not have an error control and flow management mechanism.

Frame Relay Network

Working:

- Frame relay switches set up virtual circuits to connect multiple LANs to build a WAN. Frame relay transfers data between LANs across WAN by dividing the data in packets known as frames and transmitting these packets across the network.
- It supports communication with multiple LANs over the shared physical links or private lines.
- Frame relay network is established between Local Area Networks (LANs) border devices such as routers and service provider network that connects all the LAN networks.
- Each LAN has an access link that connects routers of LAN to the service provider network terminated by the frame relay switch.

- The access link is the private physical link used for communication with other LAN networks over WAN.
- The frame relay switch is responsible for terminating the access link and providing frame relay

Advantages:

- High speed
- Scalable
- Reduced network congestion
- Cost-efficient
- Secured connection

Disadvantages:

- Lacks error control mechanism
- Delay in packet transfer
- Less reliable

Asynchronous Transfer Mode (ATM) in Computer Network[ATM]

Why ATM networks?

1. Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).
2. Telephone networks support a single quality of service and are expensive to boot.
3. Internet supports no quality of service but is flexible and cheap.
4. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

Asynchronous Transfer Mode (ATM):

- It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells.

- Cells are transmitted asynchronously and the network is connection-oriented. ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching.
- *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.
- Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic.
- Thus it can carry multiple types of traffic with **end-to-end** quality of service.
- ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use “Packet” or “cell” Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

Advantages

1. It offers large bandwidth.
2. It is easy and simple to integrate with MAN, LAN, and WAN networks.
3. It utilizes a simplified network infrastructure.
4. It is designed to transfer voice, video, and image data over a single network. It is utilized for mixed traffic, real-time and non-real-time traffic.
5. It makes effective use of network resources by utilizing the bandwidth-on-demand concept.
6. It is less vulnerable to noise deterioration.

Disadvantages

1. ATM switches are more expensive than LAN hardware. Additionally, ATM NIC is more expensive than Ethernet NIC.
2. The cell header generates greater overhead.
3. Congestion can cause cell losses.
4. As ATM is a connection-oriented technology, the time needed to set up and pull down the connection is greater than the time needed to use it.
5. Complex mechanisms are utilized to achieve QoS.

ISDN

ISDN or **Integrated Services Digital Network**, is a circuit-switched telephone network system that transmits both data and voice over a digital line.

You can also think of it as a set of communication standards to transmit data, voice, and signaling. These digital lines could be copper lines. It was designed to move outdated landline technology to digital.

ISDN is a circuit-switched telephone network system, but it also provides access to packet-switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream direction.

ISDN connections have a reputation for providing better speeds and higher quality than traditional connections. Faster speeds and better connections allow data transmissions to travel more reliably.

ISDN Services:

ISDN provides a fully integrated digital service to users. These services fall into 3 categories- bearer services, teleservices, and supplementary services.

1. Bearer Services –

Transfer of information (voice, data, and video) between users without the network manipulating the content of that information is provided by the bearer network. There is no need for the network to process the information and therefore does not change the content..

2. Teleservices –

. Teleservices rely on the facilities of the bearer services and are designed to accommodate complex user needs. The user need not be aware of the details of the process. Teleservices include telephony, teletex, telefax, videotex, telex, and teleconferencing.

3. Supplementary Service –

Additional functionality to the bearer services and teleservices are provided by supplementary services. Reverse charging, call waiting, and message handling are examples of supplementary services which are all familiar with today's telephone company services.

2.6 M-Commerce

Mobile commerce or simply M-Commerce means engaging users in a buy or sell process via a mobile device. For instance, when someone buys an Android app or an iPhone app, that person is

engaged in m-commerce. There are a number of content assets that can be bought and sold via a mobile device such as games, applications, ringtones, subscriptions etc.

Types of m-commerce

M-commerce is categorized based on the following three basic functions:

Meta rebranded Facebook Pay as Meta Pay, which lets users pay for digital items in the metaverse.

- **Mobile shopping** enables customers to buy a product using a mobile device with an application such as Amazon or a web app. A subcategory of mobile shopping is app commerce, which is a transaction that takes place over a native app.
- **Mobile banking** is online banking designed for handheld technology. It enables customers to access accounts and brokerage services, conduct financial transactions, pay bills and make stock trades. This is typically done through a secure, dedicated app provided by the banking institution. Mobile banking services may use SMS or chatbots and other conversational app platforms to send out alerts and track account activities. For example, the WhatsApp chatbot lets customers view their account balance, transfer funds, review loans and conduct other transactions in real time through WhatsApp.
- **Mobile payments** are an alternative to traditional payment methods, such as cash, check, credit and debit cards. They enable users to buy products in person using a mobile device. Digital wallets, such as Apple Pay, let customers buy products without swiping a card or paying with cash. Mobile payment apps, such as PayPal, Venmo and Xoom serve the same purpose and are popular options. Mobile consumers also use QR codes to pay for things on their mobile phones. With mobile payments, users send money directly to the recipient's cell phone number or bank account.

How mobile commerce works

With most m-commerce enabled platforms, the mobile device is connected to a wireless network that is used to conduct online product purchases and other transactions.

For those in charge of developing an m-commerce application, important key performance indicators to monitor include the following:

- total mobile traffic;
- total application traffic;
- average order value; and
- the value of orders over time.

Similarly, tracking the mobile add-to-cart rate will help developers see if users are becoming customers. M-commerce developers may also be interested in logging average page loading times, mobile cart conversion rates and SMS subscriptions.

Mobile payment products operate through a form of peer-to-peer sharing. Once a mobile device is paired with a user's bank card information, the phone can be waved over a payment terminal to pay for a product. Contactless payment using a mobile device uses near-field communication technology.

M-commerce vs. e-commerce

Electronic commerce, or e-commerce refers to buying and selling goods and services over the internet. E-commerce and m-commerce are similar, but they come with a few distinctions from each other, such as the following:

Mobility. E-commerce transactions can be conducted through a desktop computer where the user is in a fixed spot. This reduces mobility as it can be difficult to move around a desktop device. M-commerce offers greater mobility as it's conducted through handheld devices that can be used anywhere there's an internet connection, including buses, trains and airplanes or when exercising at the gym.

Location tracking. Many e-commerce apps make use of location tracking capabilities to pitch users opportunities based on their location. However, the location tracking capability of e-commerce is limited when it is used with a nonmobile device. For example, the location of an e-commerce shopper is tracked with their IP address. While the IP address provides a broad region of the user's location, it is not capable of identifying the exact location, which might affect the targeted advertising strategies of a business. M-commerce apps, on the other hand, can track locations using Wi-Fi and GPS-based technologies that enable location-specific content and personalized recommendations. For instance, a provider can send push notifications offering personalized discounts that target certain customers as they walk past a specific store in a mall.

Security. Credit cards are still commonly used for nonmobile e-commerce payments. They are considered riskier than other online payment methods, even with security measures, such as multifactor authentication. Most data breaches and identity thefts happen because of credit card misuse. M-commerce closes some security gaps through the addition of measures such as biometric authentication, mobile wallets, quick response or QR codes and even cryptocurrencies.

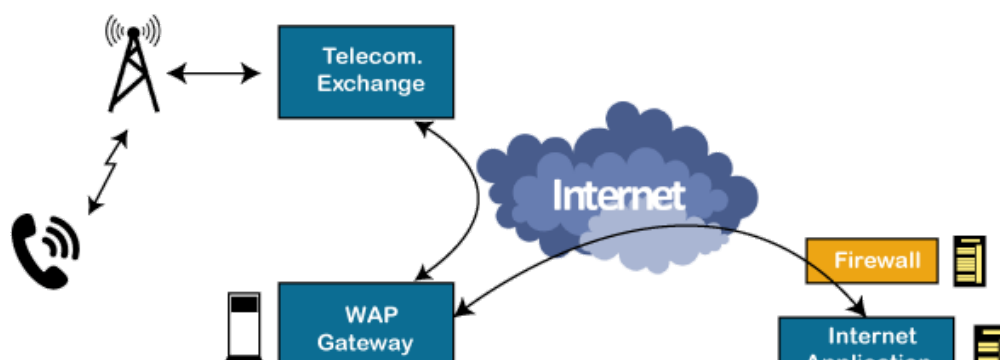
Reachability and convenience. M-commerce makes it easier to reach a target audience. With mobile apps, businesses can reach more people and make their buying experience easier and faster.

2.7 Working of Wireless Application Protocol

Wireless Application Protocol or WAP is a programming model or an application environment and set of communication protocols based on the concept of the World Wide Web (WWW), and its hierarchical design is very much similar to TCP/IP protocol stack design. See the most prominent features of Wireless Application Protocol or WAP in Mobile Computing:

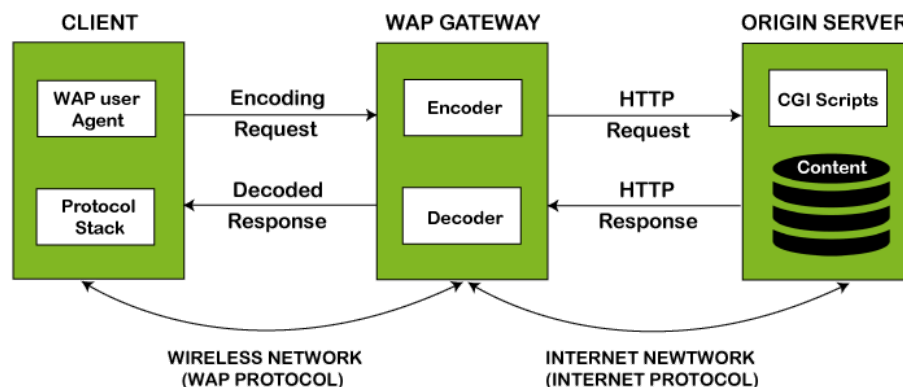
- o WAP is a De-Facto standard or a protocol designed for micro-browsers, and it enables the mobile devices to interact, exchange and transmit information over the Internet.
- o WAP is based upon the concept of the World Wide Web (WWW), and the backend functioning also remains similar to WWW, but it uses the markup language Wireless Markup Language (WML) to access the WAP services while WWW uses HTML as a markup language. WML is defined as XML 1.0 application.
- o In 1998, some giant IT companies such as Ericson, Motorola, Nokia and Unwired Planet founded the WAP Forum to standardize the various wireless technologies via protocols.
- o After developing the WAP model, it was accepted as a wireless protocol globally capable of working on multiple wireless technologies such as mobile, printers, pagers, etc.
- o In 2002, by the joint efforts of the various members of the WAP Forum, it was merged with various other forums of the industry and formed an alliance known as Open Mobile Alliance (OMA).
- o WAP was opted as a De-Facto standard because of its ability to create web applications for mobile devices.

2.7.1 WAP TECHNOLOGY



The following steps define the working of Wireless Application Protocol or WAP Model:

- o The WAP model consists of 3 levels known as Client, Gateway and Origin Server.
- o When a user opens the browser in his/her mobile device and selects a website that he/she wants to view, the mobile device sends the URL encoded request via a network to a WAP gateway using WAP protocol.
- o The request he/she sends via mobile to WAP gateway is called as encoding request.
- o The sent encoding request is translated through WAP gateway and then forwarded in the form of a conventional HTTP URL request over the Internet.
- o When the request reaches a specified Web server, the server processes the request just as it would handle any other request and sends the response back to the mobile device through WAP gateway.
- o Now, the WML file's final response can be seen in the browser of the mobile users.



WAP Protocol Stack

It specifies the different communications and data transmission layers used in the WAP model:

Application Layer: This layer consists of the Wireless Application Environment (WAE), mobile device specifications, and content development programming languages, i.e., WML.

Session Layer: The session layer consists of the Wireless Session Protocol (WSP). It is responsible for fast connection suspension and reconnection.

Transaction Layer: The transaction layer consists of Wireless Transaction Protocol (WTP) and runs on top of UDP (User Datagram Protocol). This layer is a part of TCP/IP and offers transaction support.

Security Layer: It contains Wireless Transaction Layer Security (WTLS) and responsible for data integrity, privacy and authentication during data transmission.

Transport Layer: This layer consists of Wireless Datagram Protocol (WDP). It provides a consistent data format to higher layers of the WAP protocol stack.

Advantages of Wireless Application Protocol (WAP)

Following is a list of some advantages of Wireless Application Protocol or WAP:

- o WAP is a very fast-paced technology.
- o It is an open-source technology and completely free of cost.
- o It can be implemented on multiple platforms.
- o It is independent of network standards.
- o It provides higher controlling options.
- o It is implemented near to Internet model.
- o By using WAP, you can send/receive real-time data.
- o Nowadays, most modern mobile phones and devices support WAP.

Disadvantages of Wireless Application Protocol (WAP)

Following is a list of some disadvantages of Wireless Application Protocol or WAP:

- o The connection speed in WAP is slow, and there is limited availability also.
- o In some areas, the ability to connect to the Internet is very sparse, and in some other areas, Internet access is entirely unavailable.
- o It is less secured.
- o WAP provides a small User interface (UI).

Applications of Wireless Application Protocol (WAP)

The following are some most used applications of Wireless Application Protocol or WAP:

- o WAP facilitates you to access the Internet from your mobile devices.
- o You can play games on mobile devices over wireless devices.
- o It facilitates you to access E-mails over the mobile Internet.
- o Mobile hand-sets can be used to access timesheets and fill expenses claims.
- o Online mobile banking is very popular nowadays.

- o It can also be used in multiple Internet-based services such as geographical location, Weather forecasting, Flight information, Movie & cinema information, Traffic updates etc. All are possible due to WAP technology.

2.7.2 Mobile Information Devices

Some of the most common forms of mobile computing devices are as follows.

- Portable computers - compacted lightweight units including a full character set keyboard and primarily intended as hosts for software that may be laptop etc.
- Mobile phones- including a restricted key set primarily intended but not restricted to for vocal communications, as cell phones, smart phones, phonepads, etc.
- Wearable computers - mostly limited to functional keys and primarily intended as incorporation of software agents, as watches, wristbands, necklaces, keyless implants, etc.
- Carputer - A carputer or carPC is a category of mobile computer or tablet designed or modified specifically to be installed and run in cars.