UNIT-V NETWORKING TECHNOLOGIES (20BHM513)

5.1 MOBILE IP

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped.

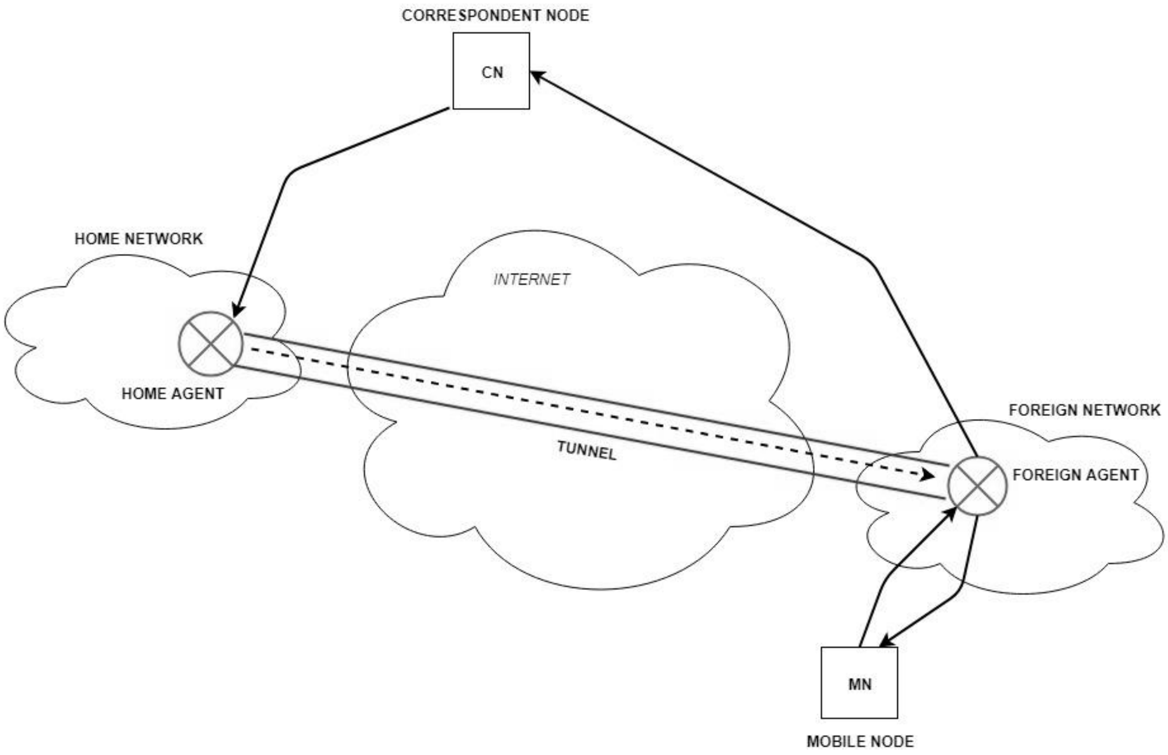
Terminologies:

1. **Mobile Node (MN)** is the hand-held communication device that the user carries e.g. Cell phone.
2. **Home Network** is a network to which the mobile node originally belongs as per its assigned IP address (home address).
3. **Home Agent (HA)** is a router in-home network to which the mobile node was originally connected
4. **Home Address** is the permanent IP address assigned to the mobile node (within its home network).
5. **Foreign Network** is the current network to which the mobile node is visiting (away from its home network).
6. **Foreign Agent (FA)** is a router in a foreign network to which the mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node.
7. **Correspondent Node (CN)** is a device on the internet communicating to the mobile node.
8. **Care-of Address (COA)** is the temporary address used by a mobile node while it is moving away from its home network.
9. **Foreign agent COA,** the COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as a common COA.

Co-located COA, the COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.

Mobile IP Working:

The correspondent node sends the data to the mobile node. Data packets contain the correspondent node's address (Source) and home address (Destination).



Packets reach the home agent. But now mobile node is not in the home network, it has moved into the foreign network. The foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.

Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

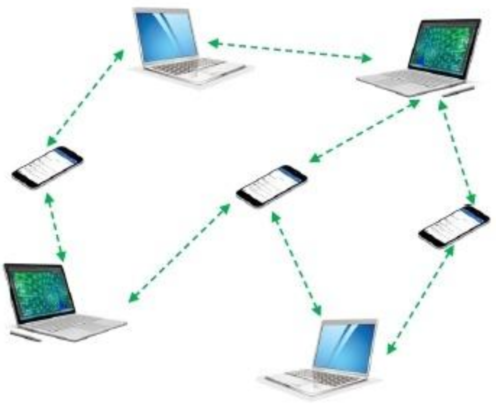
Now, the home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on another side of the tunnel, receives the data packets, decapsulates them, and sends them to the mobile node. The mobile node in response to the data packets received sends a reply in response to the foreign agent. The foreign agent directly sends the reply to the correspondent node.

5.2 AD-HOC NETWORK

A wireless Ad Hoc network or mobile ad hoc network is a Decentralized type of Wireless Network.

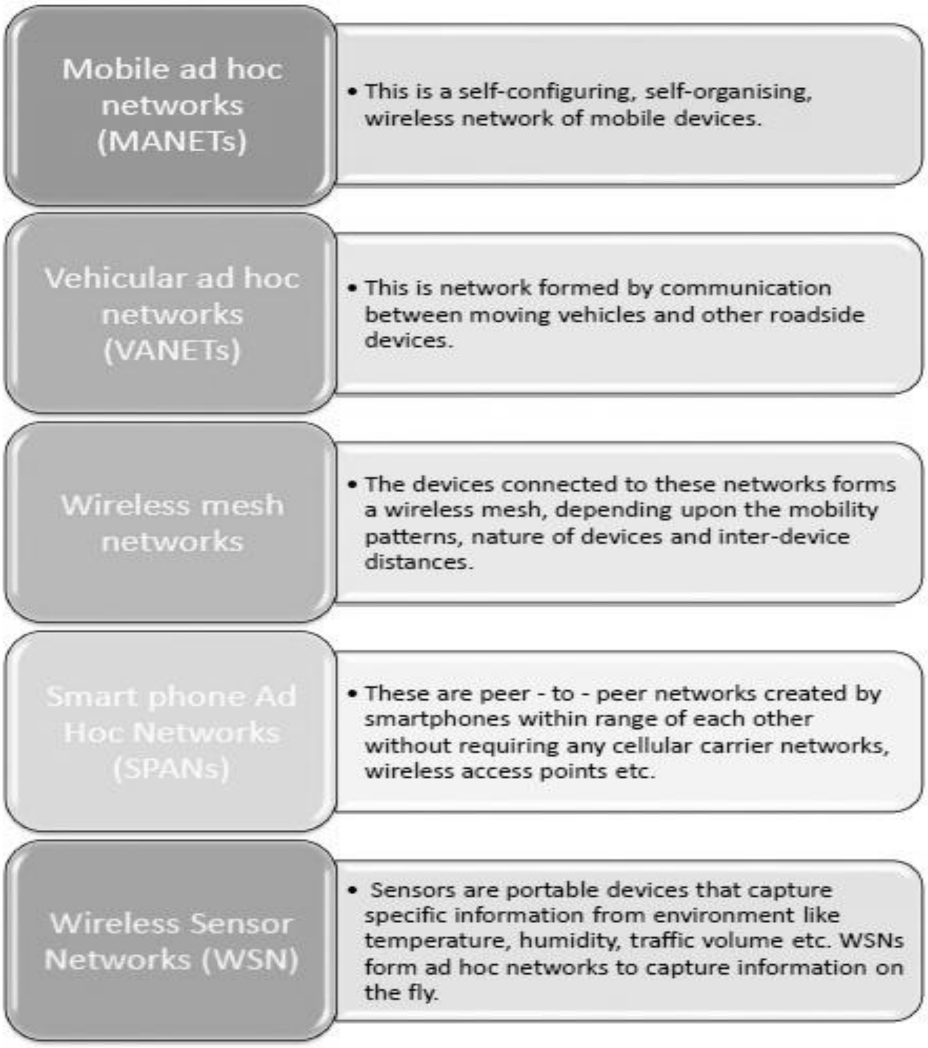
An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin words that literally means "for this," implying improvised or impromptu.

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.



Classifications of Ad Hoc Networks

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below −



Mobile ad hoc networks (MANETs)

- This is a self-configuring, self-organising, wireless network of mobile devices.

Vehicular ad hoc networks (VANETs)

- This is network formed by communication between moving vehicles and other roadside devices.

Wireless mesh networks

- The devices connected to these networks forms a wireless mesh, depending upon the mobility patterns, nature of devices and inter-device distances.

Smart phone Ad Hoc Networks (SPANs)

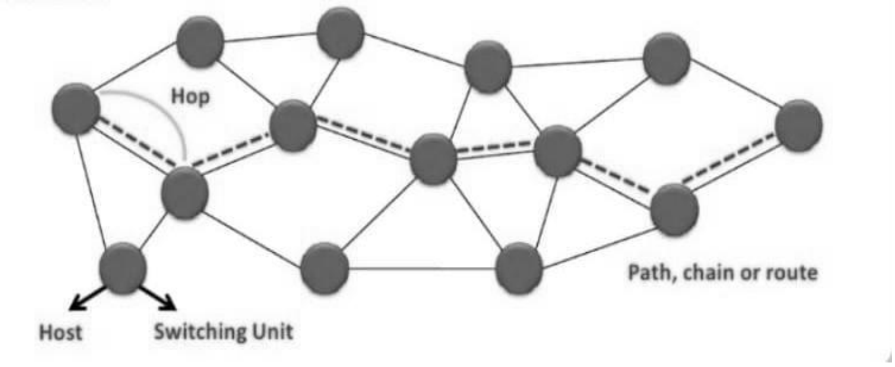
- These are peer - to - peer networks created by smartphones within range of each other without requiring any cellular carrier networks, wireless access points etc.

Wireless Sensor Networks (WSN)

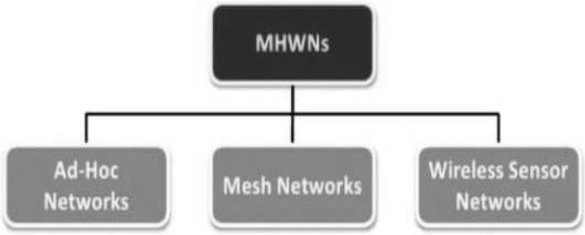
- Sensors are portable devices that capture specific information from environment like temperature, humidity, traffic volume etc. WSNs form ad hoc networks to capture information on the fly.

Multi-hop Wireless Networks (MHWNs): It is defined as a collection of nodes that communicate with each other wirelessly by using radio signals with a shared common channel.

There are several names for MHWNs; it could be called packet radio network, Ad-Hoc network or mobile network.



The nodes here could be named stations or radio transmitters and receivers.



It is a type of MHWNs.

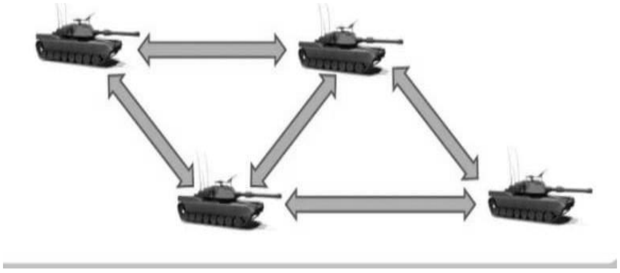
Nodes in the network are mobile in general.

The wireless hosts in such networks, communicate with each other without the existing of a fixed infrastructure and without a central control.

A mobile ad-hoc network can be connected to other fixed networks or to the Internet. Most of the Ad-Hoc networks use the allocated frequencies for the Industrial, Scientific and Medical (ISM) band.

Advantages and Applications:

- Ad-hoc networks have several advantages over the traditional networks, like:
- Ad-hoc networks can have more flexibility.
- It is better in mobility.
- It can be turn up and turn down in a very short time.
- It can be more economical.
- It considered a robust network because of its non-hierarchical distributed control and management mechanisms.
- Incase if we need to exchange information and the network's infrastructure has been destroyed.
- It is suitable for military communications at battlefield where there is no network infrastructure



5.3 DSDV PROTOCOL

We consider a collection of mobile computers, (nodes) which may be far from any base station. The computers (nodes) exchange control messages to establish multi-hop paths in the same way as the Distributed Bellman-Ford algorithm. These multi-hop paths are used for exchanging messages among the computers (nodes).

Each node maintains a routing table which stores

- next hop, cost metric towards each destination
- a sequence number that is created by the destination itself

Each node periodically forwards routing table to its neighbors

- Each node increments and appends its sequence number when sending its local routing table
- Each route is tagged with a sequence number; routes with greater sequence numbers are preferred
- Each node advertises a monotonically increasing even sequence number for itself

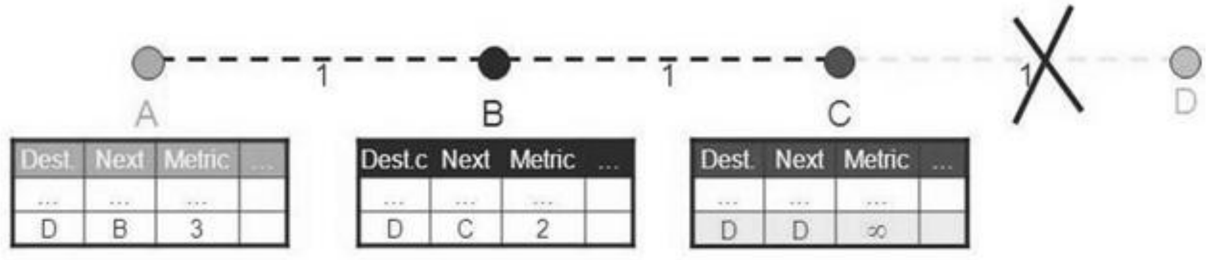
When a node finds that a route is broken, it increments the sequence number of the route and advertises it with infinite metric

- Destination advertises new sequence number

5.4 DISTANCE-VECTOR:

- Distance-Vector also known as Distributed Bellman-Ford or RIP(Routing Information Protocol)
- Every node maintains a routing table
  - all available destinations
  - the next node to reach to destination
  - the number of hops to reach the destination
- Periodically send table to all neighbors to maintain topology.

Distance Vector (Broken Link): Ex with table information



Dest.	Next	Metric	...
...	...	...	
D	B	3	

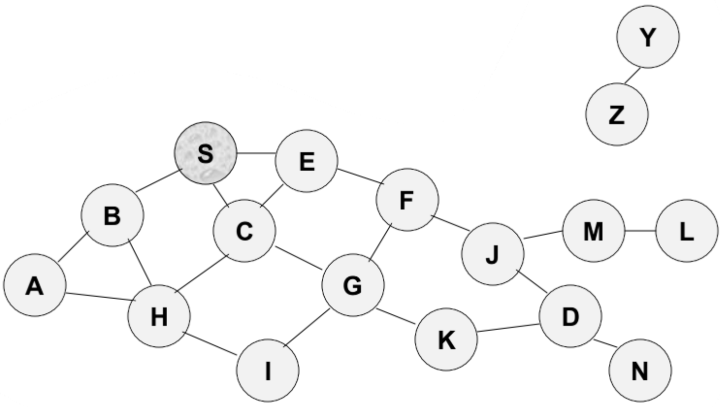
Dest.c	Next	Metric	...
...	...	...	
D	C	2	

Dest.	Next	Metric	...
...	...	...	
D	D	∞	

5.5 DYNAMIC SOURCE ROUTING (DSR)

- Dynamic Source Routing (DSR) is a type of routing used in Mobile Adhoc Network (MANET).
- It was developed at CMU in 1996.

- It falls on Reactive/On-Demand routing protocol.
- It is basically a protocol used for the discovery of route from source to destination in network.
- Unlike other protocols, the route is discovered only when it's needed.
- The process of route discovery occurs by flooding the route request packets throughout the mobile network.DSR uses caches to store routes.



DSR consists of two phases:

1) Route Discovery.
2) Route Maintenance.

1. Route Discovery:

- Route Discovery is the phase where the actual route from the source to the destination is discovered.
- This phase can be broken into two:
    a) RREQ-Route Request.
    b) RREP-Route Reply.

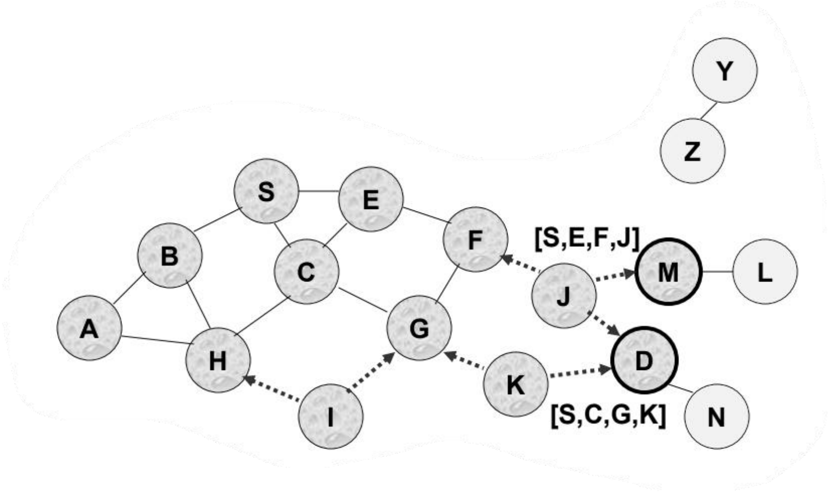
a) RREQ:

- The request for the route from source to destination is requested by the Source.

- Firstly, the source sends RREQ packet to its neighbour nodes when it needs to send some data to a destination.

- The RREQ packet from the sender contains source id and Destination info.

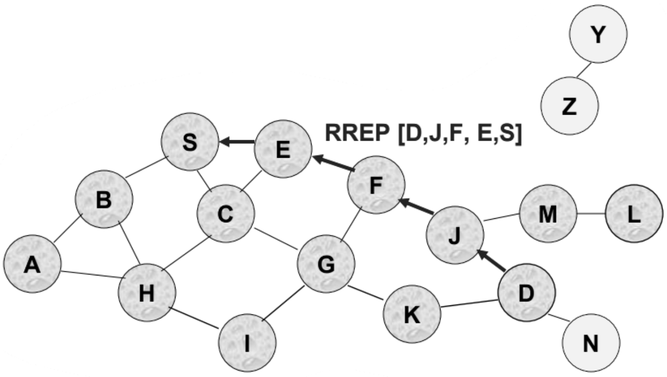
- The neighbour nodes check if they themselves are Destination.



- This takes place in every node until it reaches the destination.

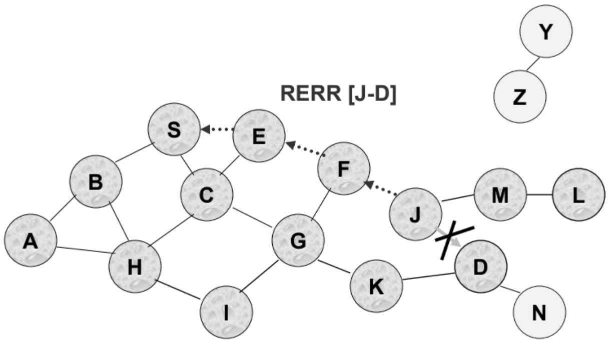
b) RREP:

- After Request is completed, the destination now sends the RREP (Reply).
- Now, the destination has the route. It reverses the route and send it to the source to locate itself(i.e. Destination)



2. Route Maintenance:

- It is a phase where the Maintenance takes place. When an unexpected error or failure occurs while discovering the route, we may have to overcome the failure in future, so the maintenance phase came in.
- Consider link between J and D fails .
- J sends a route error to S along route J-F-E-S when its attempt to forward the data packet S (with route SEFJD) on J-D fails.

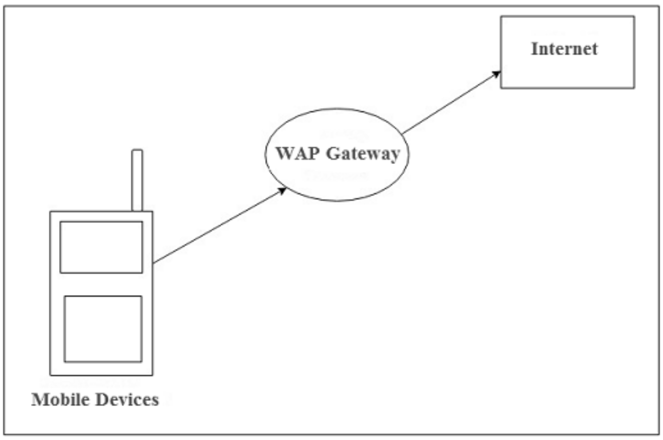


- Nodes hearing RERR (Route Error) update their route cache to remove link J-D.

5.6 WAP (Wireless Application Protocol)

WAP is a protocol that is introduced in 1999, which stands for Wireless application protocol. It offers Internet communications over wireless devices, such as mobile phones. In the early 2000s, it accomplished some popularity and was mainly superseded by more recent standards by the 2010s. Also, it offers a way of creating web applications for mobile devices, and it is designed for micro-browsers.

Most of the wireless networks are supported by WAP, as well as TDMA (Time Division Multiple Access), CDMA (Code Division Multiple Access), and GSM (Global System for Mobile Communication). Also, all operating systems can support a wireless application protocol. It enables access to the internet in mobile devices and uses the mark-up language like WML, which stands for Wireless Markup Language that is, referred to as XML 1.0 application. WAP offers the facility to connect interactive wireless devices (like mobile phones) to the internet and enhances wireless specification interoperability.



WAP may be created on any kind of operating system, and it acts in an open application environment. It is more beneficial for mobile users as it has the ability to deliver electronic information efficiently. In 1998, Nokia, Motorola, Ericson, and Unwired Planet founded the WAP Forum, whose objective was to standardize several wireless technologies with the help of protocols.

The WAP CSS (Cascading Style Sheet) makes capable of developers to format screen sizes in order to mobile device adaptability. When the WAP CSS content is used, then reformatting is not required. It controls page layout compatibility with different mobile device's display screens.

The transport layer handles the physical network issues, by which wireless gateways can be easily accessed by global wireless operations. A WAP gateway is a server, which provides the facility to access the wireless network. The WAP Forum offers specification development, WAP tool testing and also provides support for all mobile services. Now, the WAP Forum is referred to as the Open Mobile Alliance.

WAP Gateway

The Wireless Application Protocol (WAP) gateway is a software system that decodes and encodes requests and responses between the smartphone micro browsers and the internet. A request for accessing a website is sent via a WAP gateway as it provides security. It helps devices that are WAP-enabled wireless to communicate to applications and internet Web sites. You need a WAP gateway service if you want to access internet resources from a WAP-enabled wireless device. WML (Wireless Markup Language) helps to deliver web pages in a special format, which is compiled and forwarded through the WAP gateway.

The WAP gateway typically is a server that functions as an intermediary in an access request. The HTTP requests for a web site to the server, the server gets data from the requested website. Then, convert it into an encrypted form that displays on the client browser.

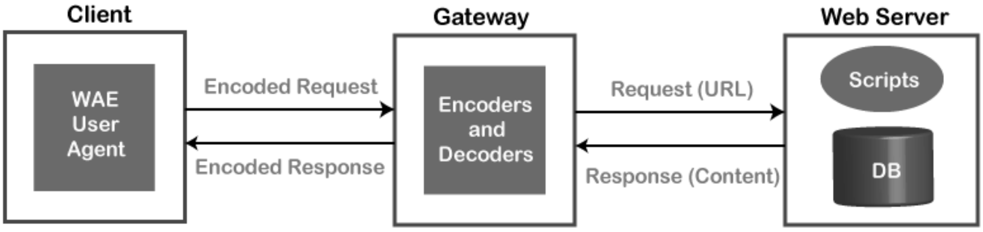
WAP browser

A WAP browser enables mobile devices to access compatible web pages. A large number of internet protocols can be used by the mini browser to convert web pages into plain text. Usually, in terms of WAP browser effectiveness, web developers create separate WAP web pages for mobile devices. The web content generally takes longer to load without WAP optimization, also may not translate the content correctly in order to mobile devices.

Advanced internet languages like extensible hypertext markup language (XHTML) and compact hypertext markup language (CHTML) are also supported by the WAP browsers today. It has made it possible for newer mobile devices to support advanced internet languages with the WAP browser to translate popular XHTML media elements. Older types of mobile devices that contain small display screens still use the WAP browser to translate web pages. Even modern mobile devices can handle displaying web pages in their entirety as they are increasingly powerful.

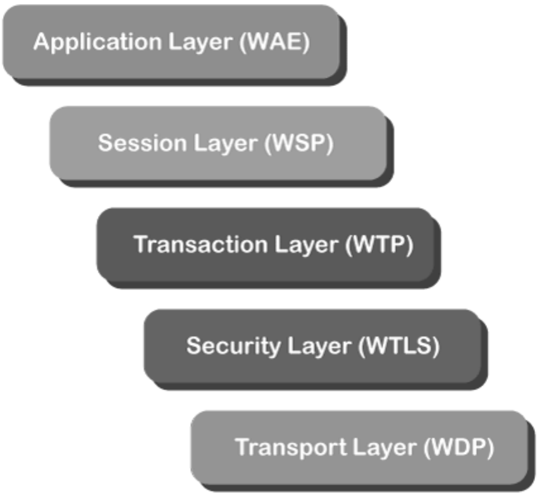
WAP Model

In the mobile device, the user opens the web browser and accesses the website and visit WebPages accordingly. The mobile device forwards the URL request to a WAP gateway through the network using the WAP protocol.



Then, the WAP gateway refers to this request over the internet after translating it into a conventional HTTP URL request. The specified Web server accepts the request and processes the request. Then, it returns the response to the mobile device in the WML file through the WAP gateway that will be displayed in the web browser on the device.

WAP Protocol stack



1. Application Layer (WAE)

The Wireless Application Environment contains content development programming languages like WML and mobile device specifications. It functions much like a JavaScript and holds the tools that wireless Internet content developers use. It includes scripting languages such as WML and WML Script that are used in conjunction with WML.

2. Session Layer (WSP)

It determines the session will be connection-oriented or connectionless between the device and the network and offers a reconnection and fast connection suspension. The data is passed both ways between the network and the device in the connection-oriented session. Then, WSP forwards the packet to the next layer WTP (Wireless Transaction Protocol). When the information is being streamed or broadcast from the network to the device, commonly, the connectionless session is used. Then, WSP forwards the packet to the WDP (Wireless Datagram Protocol) layer.

3. Transaction Layer (WTP)

The Wireless Transaction Protocol offers transaction support. It is a part of TCP/IP and runs on top of UDP, which stands for User Datagram Protocol.

4. Security Layer (WTLS)

The Wireless Transport Layer Security provides security in terms of data integrity, privacy and authentication that help to save your data. It also has the ability to work like Transport Layer Security. Also, it contains security features that have Transport Layer Security.

5. Transport Layer (WDP)

With the network carrier layer, the Wireless Datagram Protocol functions in conjunction and presents a constant data format to higher layers of WAP protocol stack.

5.7 COMPONENTS OF WAP

There are three major components of the WAP, which are as follows:

1. Protocol Support

- **IP networks:** Protocols supported contains the HTTP (known as WP-HTTP), TLS, and the wireless "profiled" versions of TCP (known as WP-TCP).
- **Non-IP networks:** It includes four layers: Wireless Transport Layer Security, Wireless Datagram Protocol, Wireless Session Protocol, and Wireless Transaction Protocol.

2. Application Environment

- **WML Specification:** WML stands for Wireless Markup Language, based on XML and XHTML.
- **WML Script Specification:** A scripting language that is used for running code on clients.
- **WAP Micro Browser:** Especially, it is designed to control the WAP device. WAP devices make capable of operating in a limited resource environment with the help of a WAP micro-browser.

3. Services and Capabilities

- **Customization of User Profile:** On the basis of client device capabilities and user preferences, WAP enables servers to customize content delivered to users.

- **Telephony Support:** Wireless application protocol allows telephone services to be operated from within a data environment. As a result, WAP phones can function as web devices and integrated voice.

5.8 WLAN

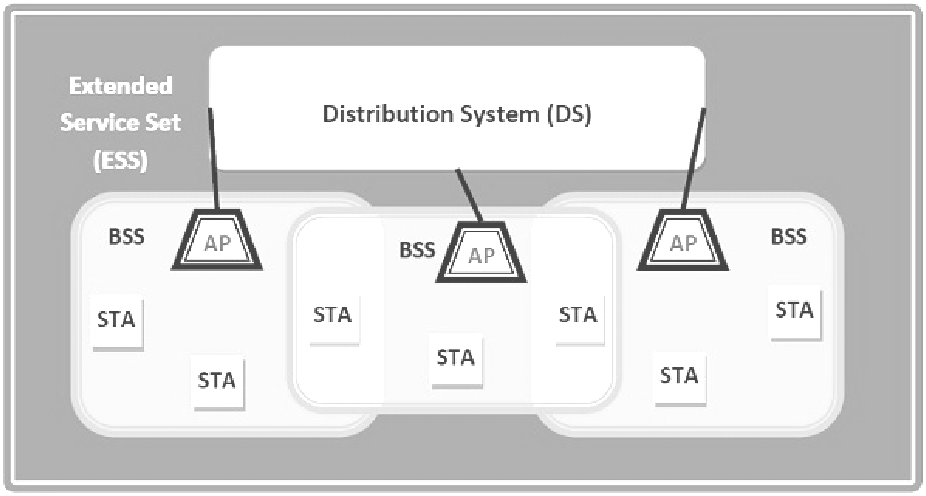
WLANs are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.

Components of WLANs

The components of WLAN architecture as laid down in IEEE 802.11 are −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types −
  - Wireless Access Point (WAP or AP)
  - Client
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories −
  - Infrastructure BSS
  - Independent BSS
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.



Types of WLANS

WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

- **Infrastructure Mode** − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** − Clients transmit frames directly to each other in a peer-to-peer fashion.

Advantages of WLANs

- They provide clutter-free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.
- The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.
- Installation and setup are much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

~~~~~~~ All the Best ~~~~~~~
~~~~~~~