**UNIT V: Support for Mobility:** Wireless Application Protocol: Architecture, Wireless Datagram Protocol, Wireless Transport Layer Security, Wireless Transaction Protocol, Wireless Session Protocol, Wireless Application Environment, Wireless Markup Language, WML Scripts, Wireless Telephone Application.

Wireless Application Protocol(WAP):

- WAP stands for Wireless Application Protocol. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices.
- It is a set of communication protocols designed to enable wireless devices, such as mobile phones, to access and interact with the Internet and other network services.
- WAP was developed in the late 1990s and early 2000s as a way to provide a standardized method for accessing web content on mobile devices.
- It uses a markup language called Wireless Markup Language (WML) and a scripting language called WMLScript to create web pages that can be viewed on small mobile screens.
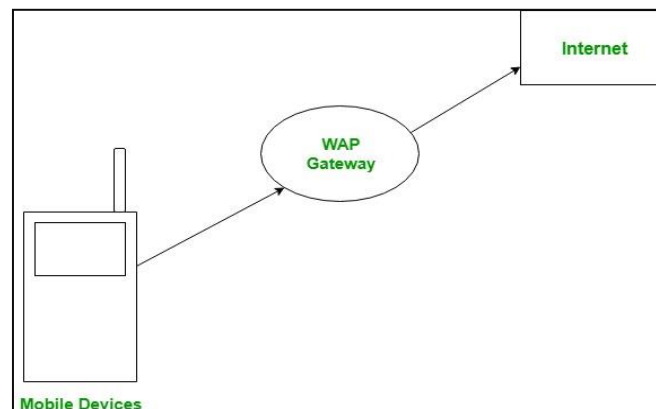

Working of WAP Model:

- The WAP model consists of 3 levels known as Client, Gateway and Origin Server.
- 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.
- The request he/she sends via mobile to WAP gateway is called as encoding request.
- The sent encoding request is translated through WAP gateway and then forwarded in the form of a conventional HTTP URL request over the Internet.
- 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.
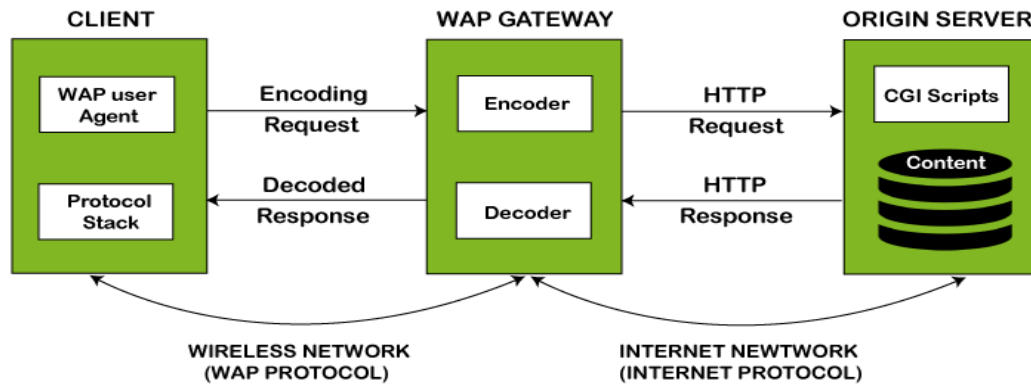
WAP Architecture:
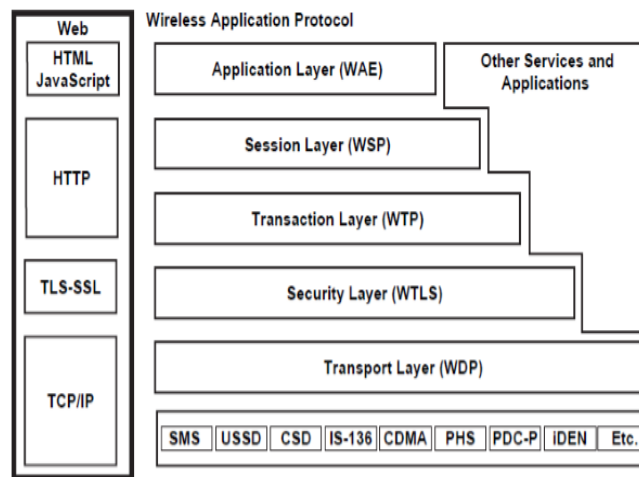
Application Layer: This layer consists of the Wireless Application Environment (WAE), mobile device specifications, and content development programming languages, i.e., WML.

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 WAP:

- WAP is a very fast-paced technology.
- It is an open-source technology and completely free of cost.
- It can be implemented on multiple platforms.
- It is independent of network standards.
- It provides higher controlling options.
- It is implemented near to Internet model.

Disadvantages of WAP:

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

Applications of WAP:

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

WIRELESS DATAGRAM PROTOCOL(WDP):

- The Wireless Datagram Protocol (WDP) is a protocol that is used in wireless communication networks to transmit data between devices.
- It is a network-layer protocol that is used to encapsulate higher-level protocols, such as the Internet Protocol (IP), for transmission over wireless networks.
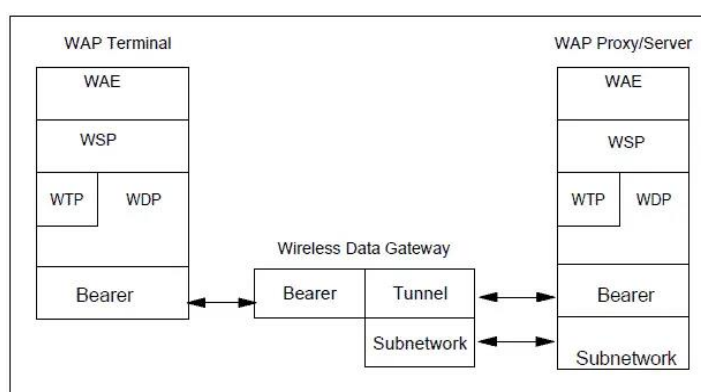
WAE: WAE stands for Wireless Application Environment. It is a set of specifications and tools for developing wireless applications that can be used across a variety of mobile devices and networks.

WSP: WSP stands for Wireless Session Protocol.It operates on top of the Wireless Datagram Protocol (WDP), which is responsible for transmitting data packets between devices over wireless networks.

WDP:WDP stands for Wireless Datagram Protocol. It is a network-layer protocol that is used to encapsulate higher-level protocols, such as the Internet Protocol (IP), for transmission over wireless networks.

Working of transmission in WDP:

The transmission of data using WDP typically involves several steps, including:

1. **Packetization:** The data to be transmitted is broken down into small packets, each with its own WDP header.
2. **Addressing:** The source and destination addresses are added to the WDP header of each packet, along with other routing information.
3. **Routing:** The packets are transmitted over the wireless network, using a variety of routing protocols to ensure that they are delivered to the correct destination.
4. **Segmentation and reassembly**: If the packets are too large to be transmitted in a single data transmission, they may be segmented into smaller packets for transmission and reassembled at the destination device.
5. **Error detection and correction:** The WDP header includes a checksum value that is used to detect errors in the data transmission. If errors are detected, the packets may be retransmitted or error correction techniques may be used to recover the lost data.
6. **Quality of Service (QoS):** The WDP header may include QoS parameters that specify the level of service required for the data transmission, such as priority or delay requirements.

WIRELESS TRANSPORT LAYER SECURITY(WTLS):

➢ WTLS is a cryptographic protocol that is used to secure communication over the internet.
➢ The devices exchange certificates and encryption keys to establish a secure connection, and data transmitted over the wireless network is encrypted using these keys.
➢ This ensures that the data is only readable by the intended recipient and cannot be intercepted by anyone else.
➢ Transport Layer Securities (TLS) are designed to provide security at the transport layer.
➢ TLS was derived from a security protocol called Secure Socket Layer (SSL).

Benefits of WTLS:

- **Encryption:** TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:** TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:** TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:** Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:** Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Working of Wireless TLS:
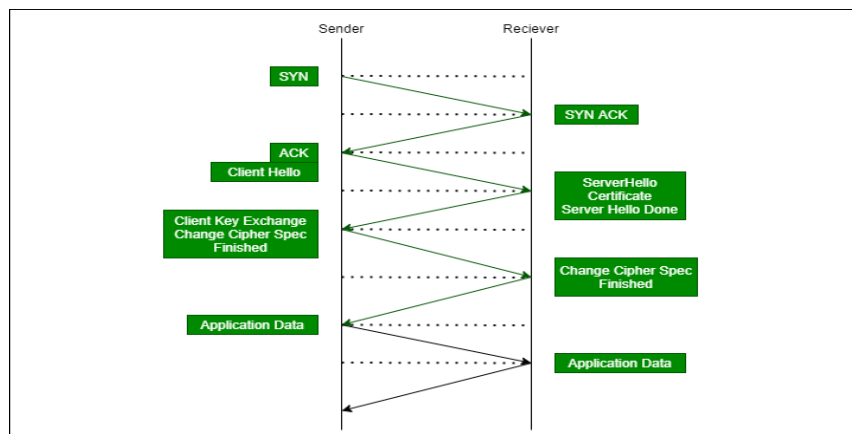
1. **Handshake protocol:** TLS begins with a handshake protocol, which is used to establish a secure connection between two devices. During the handshake, the devices exchange information about their cryptographic capabilities, authenticate each other's identities, and negotiate a shared secret key that will be used for encryption and decryption of data.

2. **Encryption:** Once the handshake is complete, TLS uses a combination of symmetric and asymmetric encryption to secure the data transmission. The symmetric encryption algorithm is used to encrypt the data, while the asymmetric encryption algorithm is used to encrypt the secret key that is used for symmetric encryption. This ensures that the data is securely encrypted and only the intended recipient can decrypt it.

3. **Message authentication:** TLS also includes a message authentication code (MAC) to ensure the integrity of the transmitted data. The MAC is calculated using a combination of the secret key and the message, and is sent along with the encrypted data. The recipient can verify the MAC using the same secret key to ensure that the data has not been tampered with during transmission.

4. **Certificate verification:** TLS uses digital certificates to verify the identity of the server and client. During the handshake protocol, the server presents its digital certificate to the client, which verifies the certificate to ensure that it is valid and issued by a trusted certificate authority (CA). This helps to prevent man-in-the-middle attacks and ensure that the communication is secure.

WIRELESS TRANSACTION PROTOCOL(WTP):

➤ A wireless transaction protocol (WTP) is a communication protocol used to facilitate secure and reliable wireless transactions between mobile devices and payment systems.

➤ WTP is typically used in mobile payment applications and allows users to pay for goods and services using their mobile phones or other wireless devices.

➤ The main goal of WTP is to ensure that wireless transactions are secure, fast, and reliable.

➤ WTP is often implemented as part of a larger mobile payment system, which may include a mobile wallet, a payment gateway, and other components.

➤ Some popular WTPs include Near Field Communication (NFC), Bluetooth Low Energy (BLE), and QR code-based payment systems.

➤ A special feature of WTP is its ability to provide a user acknowledgement or, alternatively, an automatic acknowledgement by the WTP entity. If user acknowledgement is required, a WTP user has to confirm every message received by a WTP entity.

➤ A user acknowledgement provides a stronger version of a confirmed service because it guarantees that the response comes from the user of the WTP and not the WTP entity itself.
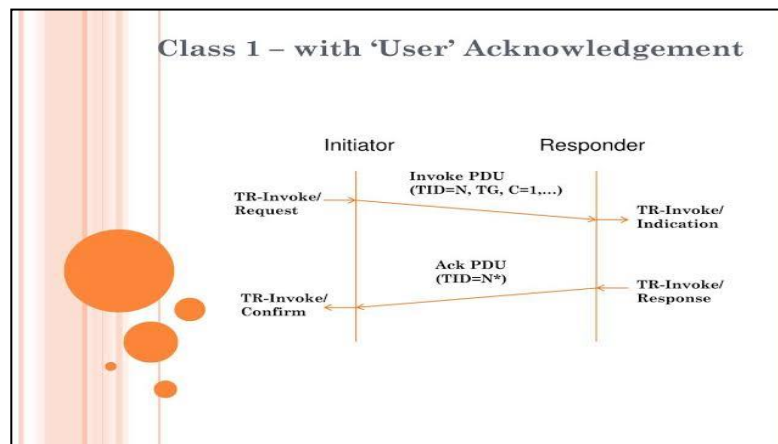
WTP TRANSACTIONS:

There are 3 WTP transactions. They are:

1. WTP class 0
2. WTP class 1
3. WTP class 2

WTP class 0 : This class provides the lowest level of reliability and is used for transactions that can tolerate occasional packet loss. Class 0 does not provide any guarantees regarding the delivery of data and does not support retransmission or acknowledgement of packets.
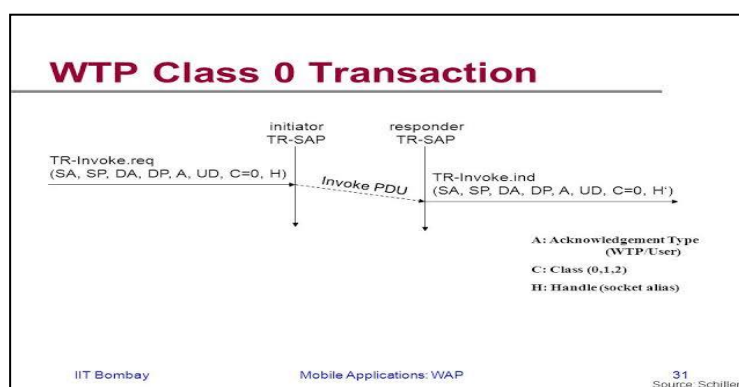
WTP Class 1: This class provides a moderate level of reliability and is used for transactions that require more reliable delivery than Class 0. Class 1 provides acknowledgments for each packet and supports retransmission in case of packet loss.

WTP Class 2: This class provides the highest level of reliability and is used for transactions that require near-perfect delivery. Class 2 is typically used for applications such as voice and video communication. Class 2 provides acknowledgments for each packet, supports retransmission in case of packet loss, and uses error correction techniques to ensure the accuracy of the data.

Fig 4.9 Basic Transaction , WTP Class 2,with user Acknowledgement
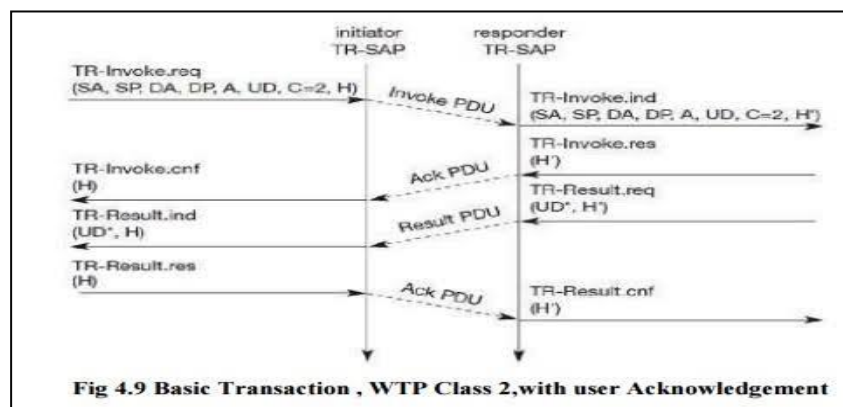
Wireless Session Protocol(WSL):

- ➢ WSP is responsible for establishing and maintaining a session between the client and server in the WAP architecture.
- ➢ The protocol defines the format of messages that are exchanged between the client and server during the session.
- ➢ These messages include requests and responses related to web browsing, email, and other WAP applications.
- ➢ WSP supports both connection-oriented and connectionless sessions.

> ➤ In connection-oriented sessions, a connection is established between the client and server, and data is exchanged over this connection until it is terminated.

> ➤ In connectionless sessions, each message is sent independently and does not require a dedicated connection between the client and server.

WSP offers the following general features needed for content exchange between cooperating clients and servers:

- **Session management:** Session management is used to facilitate secure interactions between a user and some service or application and applies to a sequence of requests and responses associated with that particular user.

- **Capability negotiation**: Clients and servers can agree upon a common level of protocol functionality during session establishment. Example parameters to negotiate are maximum client SDU size, maximum outstanding requests, protocol options, and server SDU size.

- **Content encoding:** WSP also defines the efficient binary encoding for the content it transfers. WSP offers content typing and composite objects, as explained for web browsing.
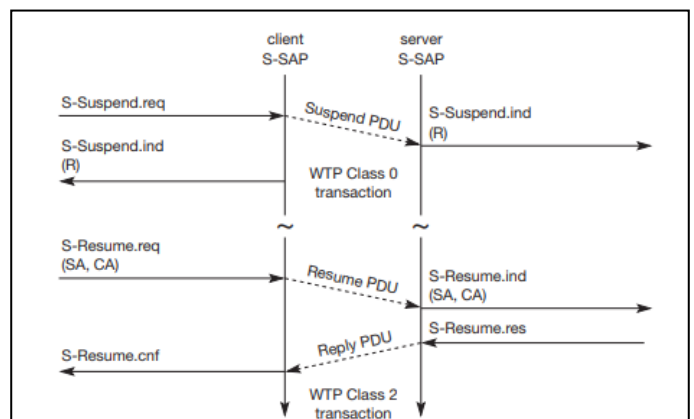
WAP has specified the **wireless session protocol/browsing (WSP/B)** which comprises protocols and services most suited for browsing-type applications.

- **HTTP/1.1 functionality:** WSP/B supports the functions HTTP/1.1 offers, such as extensible request/reply methods, composite objects, and content type negotiation.

- **Exchange of session headers:** Client and server can exchange request/reply headers that remain constant over the lifetime of the session

- **Asynchronous requests:** Optionally, WSP/B supports a client that can send multiple requests to a server simultaneously.
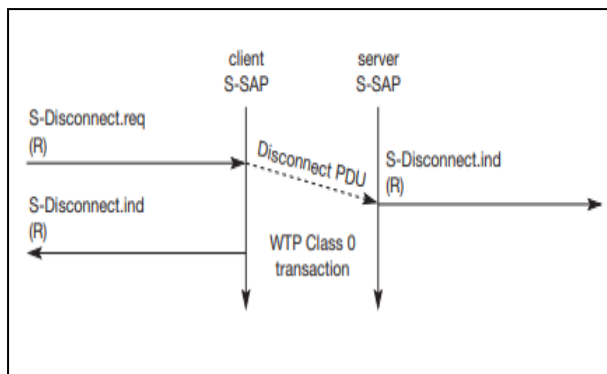
WSP/B over WTP:
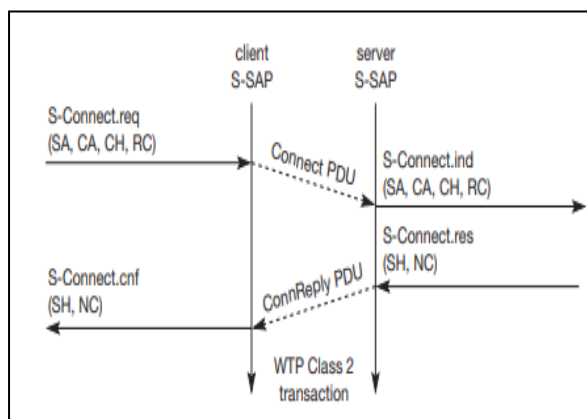
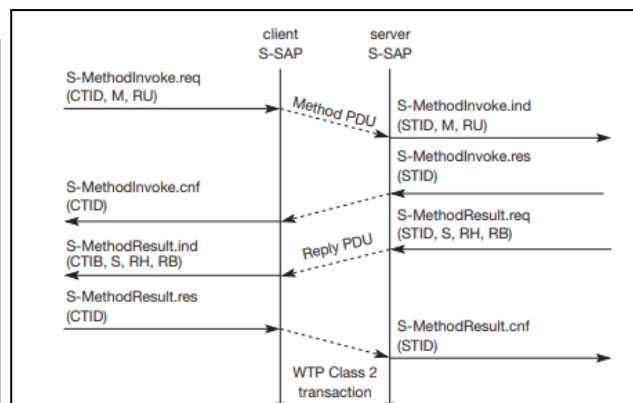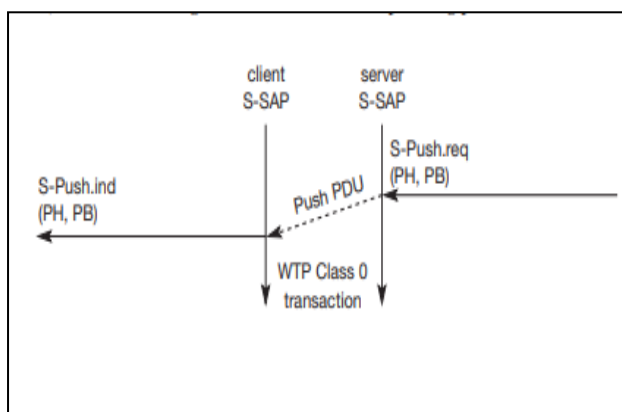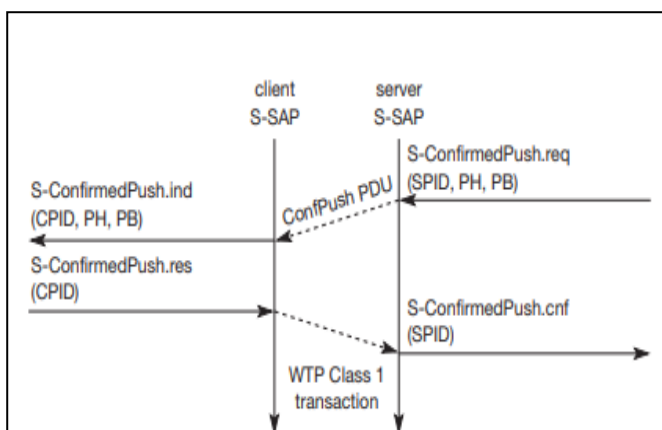WSP/B session establishment   WSP/B session suspension and resume

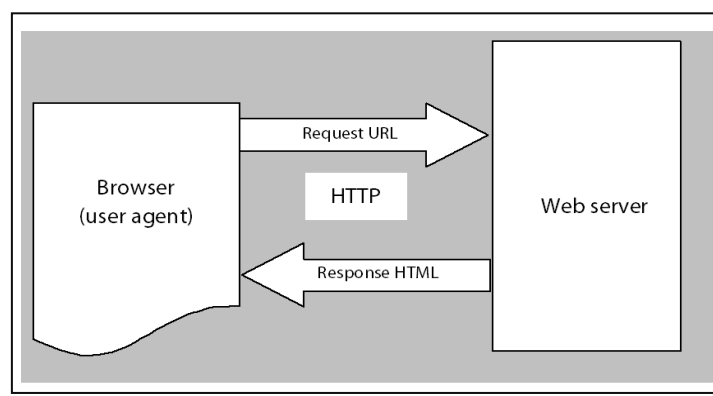WSP/B session termination

WSP/B completed transaction

WSP/B non-confirmed push

WSP/B confirmed push

Wireless Application Environment(WAE):

The Wireless Application Environment, or WAE, provides an architecture for communication between wireless devices and Web servers.

➢ Wireless Application Environment (WAE) is a software framework that provides a platform for the development and deployment of mobile applications over wireless networks.

➢ It is designed to support the creation of applications that can run on a variety of mobile devices, including smartphones, tablets, and other portable devices.

➢ WAE is based on a set of specifications and protocols that define how applications interact with the underlying mobile network infrastructure.

➢ These specifications include the Wireless Application Protocol (WAP), which is used for communication between the mobile device and the network, as well as the Wireless Markup Language (WML), which is a markup language used for creating mobile web pages.
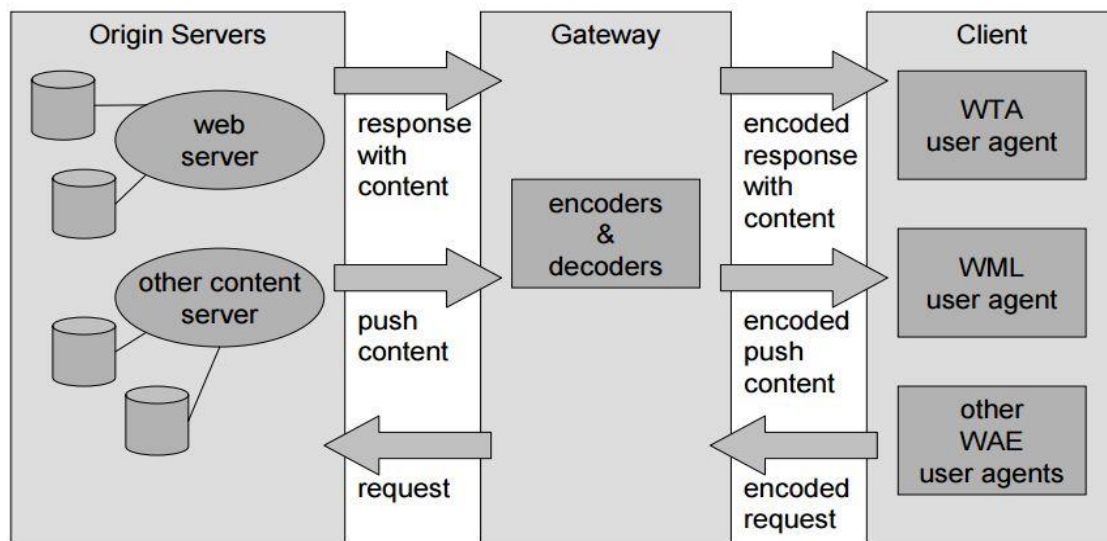
- A **client** issues an encoded request for an operation on a remote server.(encoding is necessary to minimize data sent over the air and to save resources on hand held devices)
- Decoders in a **gateway** translate this encoded request into a standard request understood by **origin servers**
- The origin servers will respond to this request by encoding the response and its content and transfers it to client.
- WAE logical model also includes push services.
- Several user agents reside within the client
- **WML user agent** supports WML, WMLscript or both.
- WTA user agent handles access to and interaction with,mobile telephone features (such as call control)
- The standard defines a **user agent profile (UAProf)** which describes capabilities of user agents.

Wireless Markup Language(WML):-

➢ Wireless Markup Language (WML) is a markup language used for creating content for mobile devices such as cell phones, smartphones, and PDAs.

➢ WML is similar to HTML (Hypertext Markup Language), which is used to create web pages for desktop computers. However, WML is optimized for the limited processing power and small screens of mobile devices. It is a lightweight markup language that supports only a limited set of tags and attributes.

➢ WML documents are written in plain text and are typically saved with a .wml extension. The WML document is then translated by the WAP gateway into a format that can be understood by the mobile device.

➢ WML documents typically consist of a deck of cards, with each card representing a page of content. Each card can contain text, images, links, and other types of content. WML also includes support for basic user input, such as forms and text input fields.

Features of WML:

- **Text and Images:** WML gives a clue about how the text and images can be presented to the user. The final presentation depends upon the user. Pictures need to be in WBMP format and will be monochrome.

- **User Interaction:** WML supports different elements for input like password entry, option selector and text entry control. The user is free to choose inputs such as keys or voice.

- **Navigation:** WML offers hyperlink navigation and browsing history.

- **Context Management:** The state can be shared across different decks and can also be saved between different decks.

WML Script:

WMLScript (Wireless Markup Language Script) is the client-side scripting language of WML (Wireless Markup Language). A scripting language is similar to a programming language, but is of lighter weight. With WMLScript, the wireless device can do some of the processing and computation. This reduces the number of requests and responses to/from the server.

This chapter will give brief description of all the important WML Script components.

WML Script Components

WML Script is very similar to Java Script. WML Script components have almost similar meaning as they have in Java Script. The WML Script program components are summarized here.

WML Script Operators

WML Script supports following type of operators.

- Arithmetic Operators
- Comparison Operators
- Logical (or Relational) Operators
- Assignment Operators
- Conditional (or ternary) Operators

Check for complete detail of The WML Operators.

WML Script Control Statements

Control statements are used for controlling the sequence and iterations in a program.

Statement	Description
if-else	Conditional branching
for	Making self-incremented fixed iteration loop
while	Making variable iteration loop
break	Terminates a loop
continue	Quit the current iteration of a loop

Check for complete detail of WML Script Control Statements.

WML Script Functions

The user-defined functions are declared in a separate file having the extension .wmls. Functions are declared as follows −

```
function name (parameters) {
   control statements;
   return var;
}
```

The functions used are stored in a separate file with the extension .wmls. The functions are called as the filename followed by a hash, followed by the function name −

```
maths.wmls#squar()
```

WML Scripts Standard Libraries

The are six standard libraries totally. Here is an overview of them −

- **Lang** − The Lang library provides functions related to the WMLScript language core.

Example Function − abs(),abort(), characterSet(),float(), isFloat(), isInt(), max(), isMax(), min(), minInt(), maxInt(), parseFloat(), parseInt(), random(), seed()

- **Float** − The Float library contains functions that help us perform floating-point arithmetic operations.
  Example Function − sqrt(), round(), pow(), ceil(), floor(), int(), maxFloat(), minFloat()
- **String** − The String library provides a number of functions that help us manipulate strings.
  Example Function − length(), charAt(), find(), replace(), trim(), compare(), format(), isEmpty(), squeeze(), toString(), elementAt(), elements(), insertAt(), removeAt(), replaceAt()
- **URL** − The URL library contains functions that help us manipulate URLs.
  Example Function − getPath(), getReferer(), getHost(), getBase(), escapeString(), isValid(), loadString(), resolve(), unescapeString(), getFragment()
- **WMLBrowser** − The WMLBrowser library provides a group of functions to control the WML browser or to get information from it.
  Example Function − go(), prev(), next(), getCurrentCard(), refresh(), getVar(), setVar()
- **Dialogs** − The Dialogs library Contains the user interface functions.
  Example Function − prompt(), confirm(), alert()

WML Scripts Comments

There are two types of comments in WMLScript −

- **Single-line comment** − To add a single-line comment, begin a line of text with the // characters.
- **Multi-line comment** − To add a multi-line comment, enclose the text within /* and */.

These rules are the same in WMLScript, JavaScript, Java, and C++. The WMLScript engine will ignore all comments. The following WMLScript example demonstrates the use of comments −

```
// This is a single-line comment.

/* This is a multi-line comment. */

/* A multi-line comment can be placed on a single line. */
```

WML Script Case Sensitivity

The WMLScript language is case-sensitive. For example, a WMLScript function with the name WMLScript Function is different from wmlscript function. So, be careful of the capitalization when defining or referring to a function or a variable in WMLScript.

Whitespaces in WMLScript

Except in string literals, WMLScript ignores extra whitespaces like spaces, tabs, and newlines.

WML Script Statement Termination by Semicolons

A semicolon is required to end a statement in WMLScript. This is the same as C++ and Java. Note that JavaScript does not have such requirement but WML Script makes it mandatory.

WIRELESS TELEPHONY APPLICATIONS

Wireless telephony is the technology that operates by the transmission of information through space; there is no physical or fixed connection between sender and receiver devices. By using wireless telephony people can be transceivers information from airplanes, driving cars, swimming pools, and jog in the park.

Applications of wireless telephony:

As the hugged amount of valuable features wireless telephony is highly acceptable by industry and common people in their daily life. Various real-time application of wireless telephony are as follow;

To provide wireless data communications:

Wireless data communications are an essential component of mobile computing. To achieve fast and secure data transmission with high-speed wireless telephony is highly advanced technology. The various available technologies differ in local availability, coverage range, and performance, and in some circumstances, users must be able to employ multiple connection types and switch between them.

To transfer wireless energy:

Wireless telephony is applicable to wirelessly energy transfer processes, in this technology electrical energy is transmitted from a power source to an electrical load that does not have a built-in power source, without the use of interconnecting wires. There are two different fundamental methods for wireless energy transfer are as follow:

- Far-field methods that involve beaming power/lasers,
- Near-field using induction that involves radio or microwave transmissions.

Both methods utilize electromagnetism and magnetic fields.

To support wireless medical technologies:

The latest wireless technologies of wireless telephony, such as mobile body area networks (MBAN), have the capability to monitor blood pressure, heart rate, oxygen level, and body temperature. The MBAN works by sending low-powered wireless signals to receivers that feed into nursing stations or monitoring sites. This technology helps with the intentional and unintentional risk of infection or disconnection that arises from wired connections.