UNIT-V

WIRELESS APPLICATION PROTOCOLS

Wireless Application Protocol:

- Wireless application protocol commonly known as a WAP, which is used to enable the access of internet in the mobile phones (or) PDA's
- It is a global specification that empowers mobile users with wireless devices to easily access and interact with internet information and services.
- WAP is an application communication protocol.
- WAP is used to access services and information.
- WAP is for handheld devices such as Mobile Phones.
- WAP enables the creating of web applications for mobile devices.
- WAP uses the Mark Up Language WML (not HTML) , WML is defined as an extension of XML of application.

Purpose of WAP:

- To enable easy, fast delivery of relevant information and services to mobile users.

Handheld Devices:

- Mobile Phones
- Pagers
- Two Way Radios
- Smart Phones
- Communicators

WAP works with wireless Network Such as

- CDMA
- GSM
- TDMA
- TETRA
- DECT

OS that is compatible with WAP:

- WAP is a communication protocol and an application environment
- WAP is independent of OS that means WAP can implemented on any OS.
- It ca built on any OS including Palm OS, Windows CE, OS/9, Java OS.

- It provides service interoperability even between different devices.

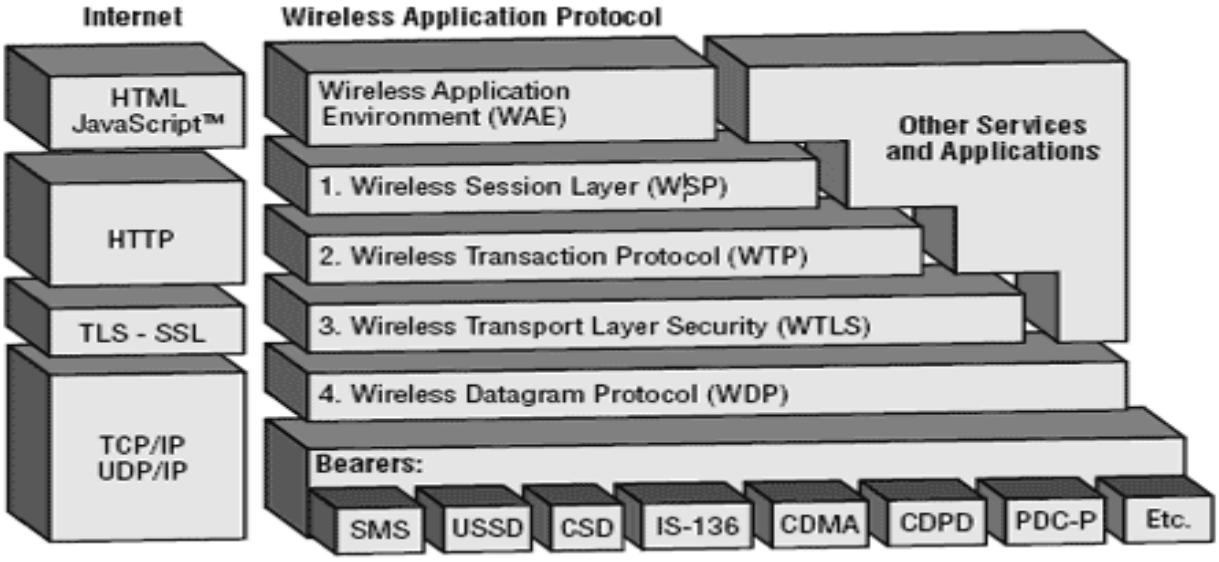
When creating a Framework for the development of contents and applications across a wide range of wireless bearer networks and wireless devices.

The Solutions must be:-

- **interoperable,** i.e., allowing terminals and software from different vendors to communicate with networks from different providers
- **scalable,** i.e., protocols and services should scale with customer needs and number of customers
- **efficient,** i.e., provision of QOS suited to the characteristics of the wireless and mobile networks
- **reliable,** i.e., provision of a consistent and predictable platform for deploying services
- **Secure,** i.e., preservation of the integrity of user data, protection of devices and services from security problems.

1. Architecture:

The following figure gives an overview of the WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the World Wide Web. The basis for transmission of data is formed by different bearer services.



Requirements of Architecture:

- Leverage existing standards whenever possible.
- Define Layered and extensible Architecture

- Support as many wireless networks as possible
- Provide support for secure applications and communication
- Optimize for efficient use of device resources

- **WTLS:** The next higher layer, the security layer with its wireless transport layer security protocol WTLS offers its service at the security SAP (SEC-SAP). WTLS is based on transport layer security (TLS, formerly SSL, secure sockets layer). WTLS has been optimized for use in wireless networks with narrow-band channels. It can offer data integrity, privacy, authentication, and (some) denial-of-service protection.
- **WTP:** The WAP transaction protocol (WTP) layer provides transaction support, adding reliability to the datagram service provided by WDP at the transaction SAP (TR-SAP).

- **WSP:** The session layer with the wireless session protocol (WSP) currently offers two services at the session-SAP (S-SAP), one connection-oriented and one connectionless if used directly on top of **WDP.** A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web.

- **WAE:** The application layer with the wireless application environment (WAE) offers a framework for the integration of different www and mobile telephony applications.

Working of WAP

WAP does not always force all applications to use the whole protocol architecture. Applications can use only a part of the architecture. For example, if an application does not require security but needs the reliable transport of data, it can directly use a service of the transaction layer. Simple applications can directly use WDP.

Different scenarios are possible for the integration of WAP components into existing wireless and fixed networks. On the left side, different fixed networks, such as the traditional internet and the public switched telephone network (PSTN), are shown. One cannot change protocols and services of these existing networks so several new elements will be implemented between these networks and the WAP-enabled wireless, mobile devices in a wireless network on the right-hand side.

2. Wireless Datagram Protocol:

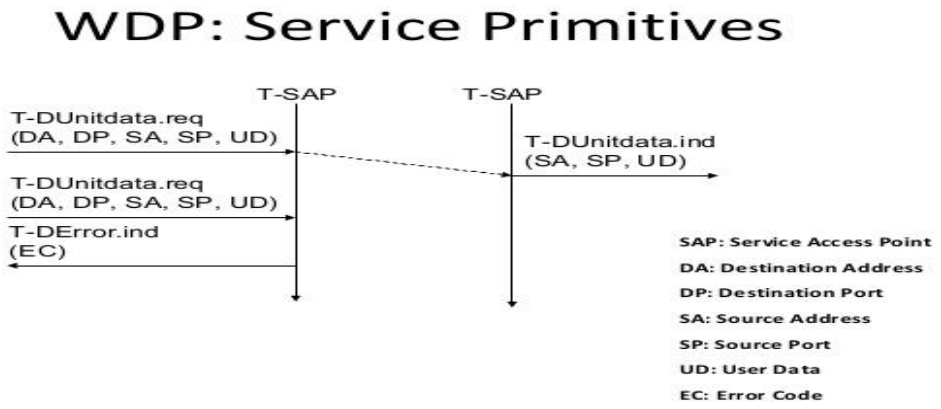
- The Wireless Datagram Protocol (WDP), a protocol in WAP architecture, covers the Transport Layer Protocols in the Internet model.
- WDP offers to the upper layers an invisible interface independent of the underlying network technology used.

- In consequence of the interface common to transport protocols, the upper layer protocols of the WAP architecture can operate independent of the underlying wireless network.
- The wireless datagram protocol (WDP) operates on top of many different bearer services capable of carrying data. At the T-SAP WDP offers a consistent datagram transport service independent of the underlying bearer.

- WDP offers source and destination port numbers used for multiplexing and demultiplexing of data respectively. The service primitive to send a datagram is TDUnitdata.req with the following parameters.

    1) Destination address (DA)
    2) Destination port (DP)
    3) Source address (SA) Source port (SP)
    4) User data (UD)

Destination and source address are unique addresses for the receiver and sender of the user data.



Source: Schiller

- If a higher layer requests a service the WDP cannot fulfill, this error is indicated with the **T-DError.ind** service primitive An **error code (EC)** is returned indicating the reason for the error to the higher layer.

- If any errors happen when WDP datagrams are sent from one WDP entity to another (e.g. the destination is unreachable, no application is listening to the specified destination port etc.), the wireless control message protocol (WCMP) provides error handling mechanisms for WDP.

- WCMP contains control messages that resemble the internet control message protocol

- WDP management entity supports WDP and provides information about changes in the environment, which may influence the correct operation of WDP. Important information is the current configuration of the device, currently available bearer services, processing and memory resources etc. Design and implementation of this management component is considered vendor-specific and is outside the scope of WAP.

3. Wireless Transport Layer Security (WTLS)

The main Concept of this protocol is Security. Suppose, the Application requested a security service, the WTLS can be integrated into the WAP Architecture on the top of WDP.

WTLS provide different levels of security ie, as follows:

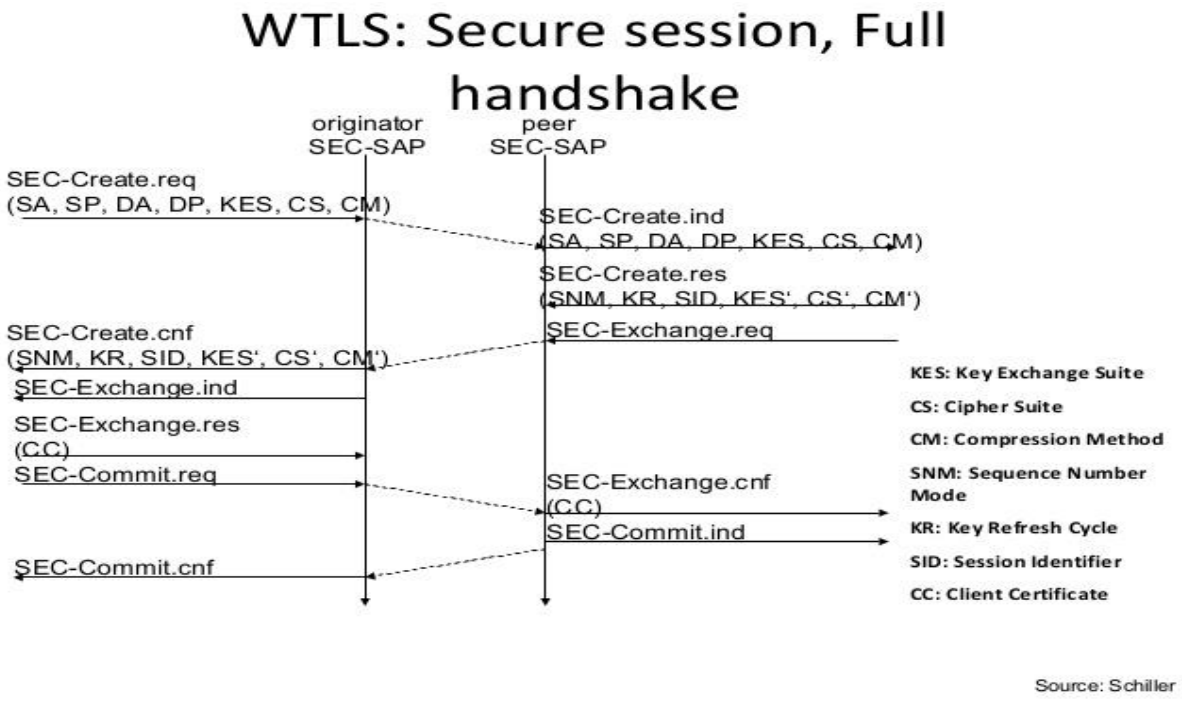
- Privacy
- Data Integrity
- Authentication

It has optimized for low Bandwidth, High Delay Bearer Networks.

WTLS takes the low processing power and very limited memory capacity of the mobile devices for cryptographic Algorithms.

WTLS supports Datagram and connection oriented Transport Layer Protocols.

When comparing to GSM, the security relation is between peers; whereas WTLS not only provided between Mobile Device and Base Station, it can provide more features and also Handshake feature is implemented.



- Before Data can be exchanged via WTLS, a secure session has to be established.
- The above figure illustrates the sequence of service primitives needed and called as
  "Full Handshake"
- The originator and peer of the secure session can both interrupt session establishment any time.
- The first step to initiate the session with the Sec-Create primitive.
  Parameters are SA, SP of the originator.
  DA, DP of the Peer.
- The originator proposes a key exchange suite (KES) and a cipher suite and a compression method.
- Similarly, the peer response with parameters for the sequence number mode (SNM); Key Refresh Cycle (KR), Session Identifier (is unique with each peer), KES, CS, CM.
- The peer also issues a SEC-Exchange Primitive – This indicates that the peer wishes to perform public key authentication with the client and ie., the peer requests the client certificate from the originator.
- After Setting up a secure connection between 2 peers, user data can be exchanged. This process is done using the Simple-Unit data Primitive.

4. Wireless Transaction Layer Protocol

Goals

- different transaction services that enable applications to select reliability, efficiency levels
- low memory requirements, suited to simple devices (< 10kbyte)
- efficiency for wireless transmission

WTP

- supports peer-to-peer, client/server and multicast applications
- efficient for wireless transmission
- support for different communication scenarios

Class 0: unreliable message transfer

- unconfirmed Invoke message with no Result message
- a datagram that can be sent within the context of an existing Session

Class 1: reliable message transfer without result message

- confirmed Invoke message with no Result message
- used for data push, where no response from the destination is expected

Class 2: reliable message transfer with exactly one reliable result message

- confirmed Invoke message with one confirmed Result message
- a single request produces a single reply

WTP Services and Protocols

WTP (Transaction)

– **provides reliable data transfer based on request/reply paradigm**

- no explicit connection setup or tear down
- optimized setup (data carried in first packet of protocol exchange)
- seeks to reduce 3-way handshake on initial request

– supports

- Header compression
- Segmentation /re-assembly
- Retransmission of lost packets
- Selective-retransmission
- Port number addressing (UDP ports numbers)
- flow control

– Message oriented (not stream)

– supports an Abort function for outstanding requests

– supports concatenation of PDUs

– supports User acknowledgement or Stack acknowledgement option

- acks may be forced from the WTP user (upper layer)
- default is stack ack

5. Wireless Session Layer Protocol:

The WAP session protocol (wsp) layer provides lightweight session layer to allow efficient exchange of data between applications.

It creates Session between the WAP Client and WAP Gateways. Each Session has a unique id and must be started and stop.

- Wireless Session Protocol (WSP) is an open standard for maintaining high level session. Wireless session is nothing but a normal Web browsing session that starts when the user connects to one URL and ends when the user leaves that URL.
- By establishing the session means that the session wide properties need only to be defined once at the beginning of the session.
- This has the benefit of saving bandwidth due to the nature of the wireless communication. The session establishing process will not have lengthy hand shaking mechanisms.
- WSP is based on HTTP 1.1 with few enhancements. WSP provides the upper-level application layer of WAP with a consistent interface for two session services.
- The first is a connection-oriented service that operates above a transaction layer protocol WTP and the second is a connection less service that operates above a secure or non-secure datagram transport service. Therefore, WSP exists for two reasons.
- First, in the connection-mode it enhances the HTTP 1.1's performance over wireless environment. Second, it provides a session layer so the whole WAP environment resembles ISO OSI Reference Model.
- WSP offers the following general features needed for content exchange between cooperating clients and servers
    1) Session Management
    2) Capability Negotiation
    3) Content Encoding

WSP is a general purpose session protocol; WAP has specified the Wireless Session Protocol/Browsing (WSP/B), which comprises protocols and services most suited for browsing type applications.

1) HTTP/1.1 Functionality
2) Exchange of session Headers
3) Push and Pull Data Transfer
4) Asynchronous Requests

Sub concepts are

1) WSP/B session Establishment – pg 406
2) WSP/B session Suspension and Resume – pg- 407
3) WSP/B Session Termination – pg – 407
4) WSP/B Completed Transaction –pg- 408
5) WSP utilization of WTP as lower layer – pg- 409
6) WSP/B Asynchronous, unordered Requests – pg-410
7) WSP/B Non-confirmed Push – pg – 410
8) WSP/B Confirmed Path – pg- 411
9) WSP/B as Connectionless Session Service – pg- 411

NOTE: These are the sub concepts of WSP protocol explain with the neat diagrams

6. Wireless Application Environment:

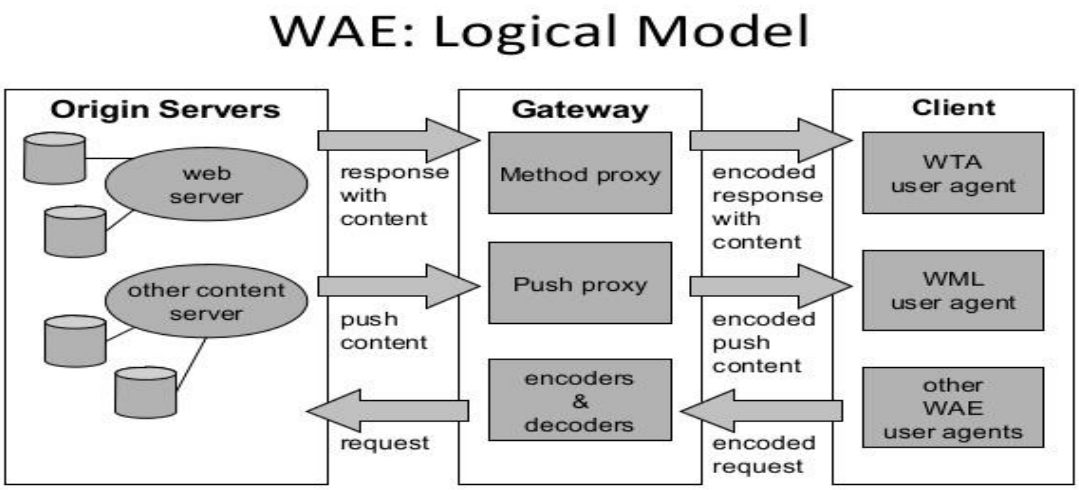
- The main idea behind the wireless application environment (WAE) is to create a general-purpose application environment based mainly on existing technologies and philosophies of the world wide web

- This environment should allow service providers, software manufacturers, or hardware vendors to integrate their applications so they can reach a wide variety of different wireless platforms in an efficient way.

- WAE has already integrated the following technologies and adapted them for use in a wireless environment with low power handheld devices.

    1) HTML (Raggett, 1998), JavaScript
    2) Handheld device mark-up language HDML (King, 1997) forms the basis of the wireless mark-up language (WML) and the scripting language WMLscript.
    3) The exchange formats for business cards and phone books vCard (IMC, 1996a) and for calendars vCalendar (IMC, 1996b) have been included.

A wide range of mobile telecommunication technologies have been adopted and integrated into the wireless telephony application (WTA)



- One global goal of the WAE is to minimize over-the-air traffic and resource consumption on the handheld device.

- 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 the handheld device as explained together with the languages WML and WMLscript.

- Decoders in a gateway now translate this encoded request into a standard request as understood by the origin servers. This could be a request to get a web page to set up a call. The gateway transfers this request to the appropriate origin server as if it came from a standard client. Origin servers could be standard web servers running HTTP and generating content using scripts, providing pages using a database, or applying any other (proprietary) technology.

- The origin servers will respond to the request. The gateway now encodes the response and its content (if there is any) and transfers the encoded response with the content to the client. The WAE logical model not only includes this standard request/response scheme, but it also includes push services. Then an origin server pushes content to the gateway. The gateway encodes the pushed content and transmits the encoded push content to the client.