Wireless Access Protocol (WAP)

NiePin & Zhou Hu

HUT

TML Latoratory

T-110.456

Agenda

- WAP Introduction
  - Environment and Limits
  - Protocol Stack Overview
- Specification
  - WAE
  - WTLS
  - WTP
- Applied Fields and Future of WAP
- Conclusion

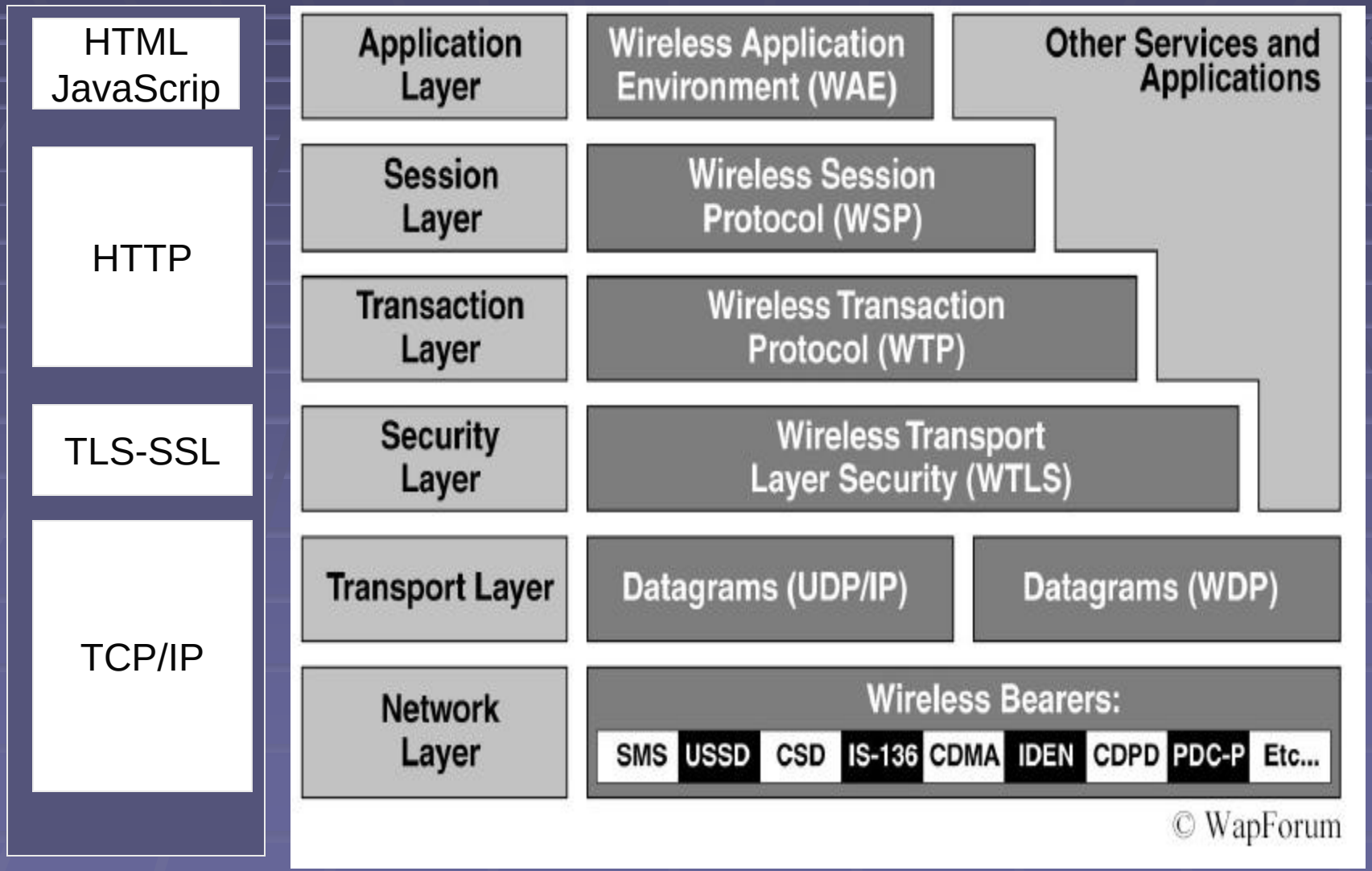
WAP Introduction

- Goal: To bridge the gap between the mobile network and Internet
- WAP is a global standard produced by WAP forum founded in 1997 with the help of Nokia, Ericsson, Motorola and Unwired Planet.
- There are two different editions: WAP 1.x and WAP 2.x
- Generally, WAP related technologies are referenced with counterparts in Internet model with some changes suitable for mobile network

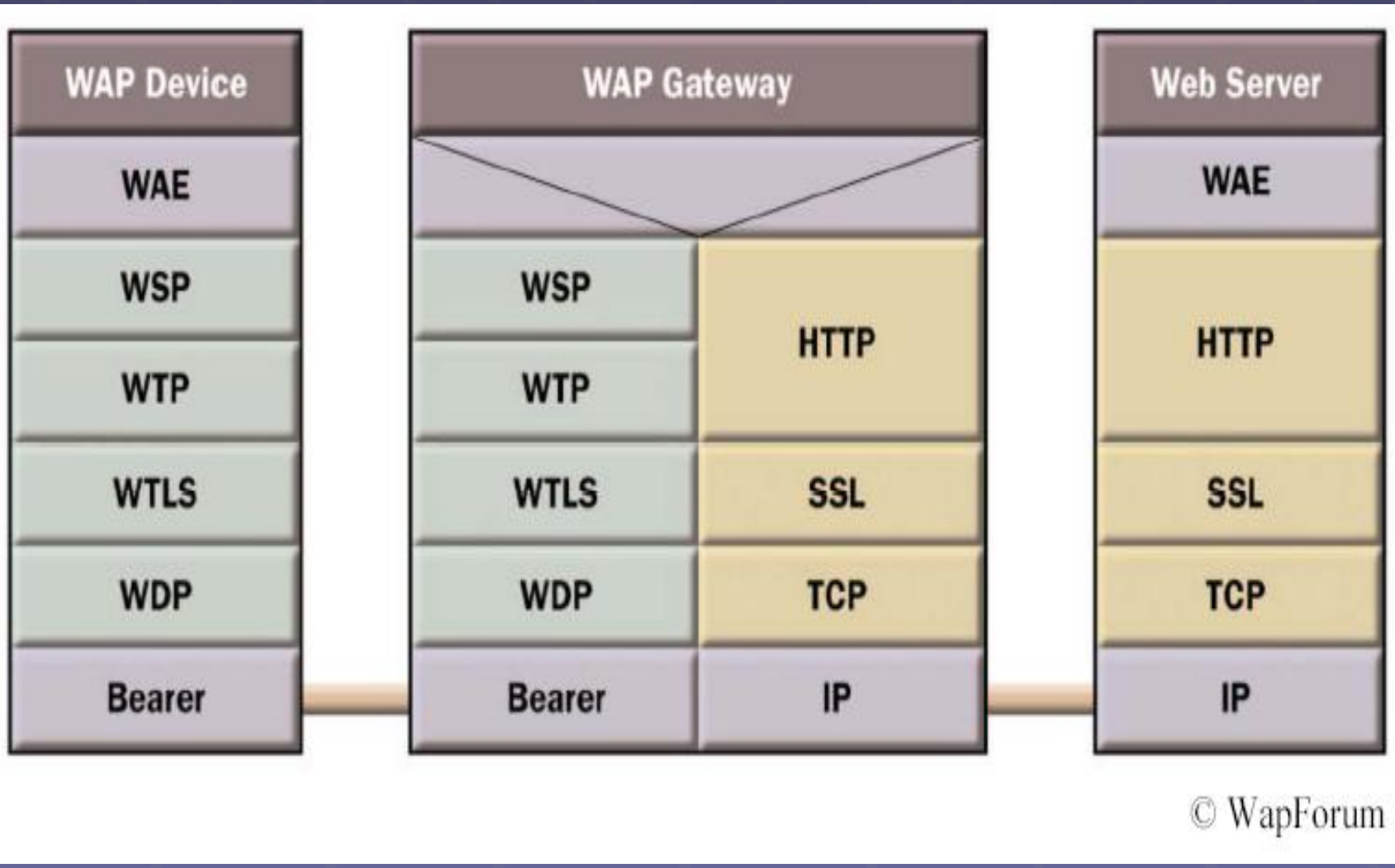
Environment and Limits

- Environment
  - Narrowband (EDGE 80-160kbps, HSCSD: Nokia6610i-43.5kbps)
  - High latency
  - Typical burst errors
- Limits
  - Week CPU (Intel PXA255 400MHz, bus 200MHz)
  - Little memory (Nokia7710-90MB internal memory 128MB MMC card; Nokia6822---3.5MB internal memory)
  - Limited on electrical power (Nokia6822---Talk Time: 3-8 hours)
  - Limited user I/O (no keyboard, mouse; few interfaces)

Protocol Stack (WAP 1.0)

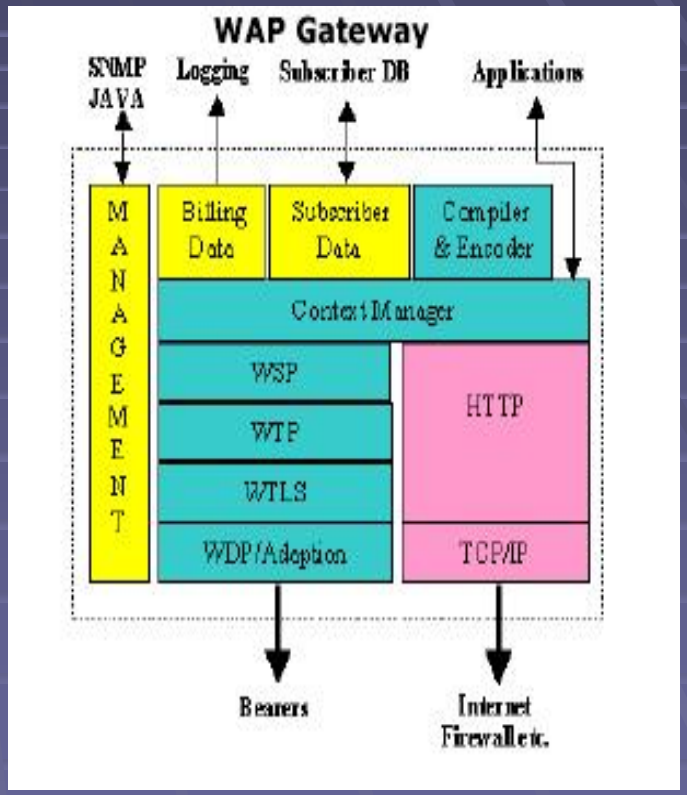


WAP 1.x Communication Model

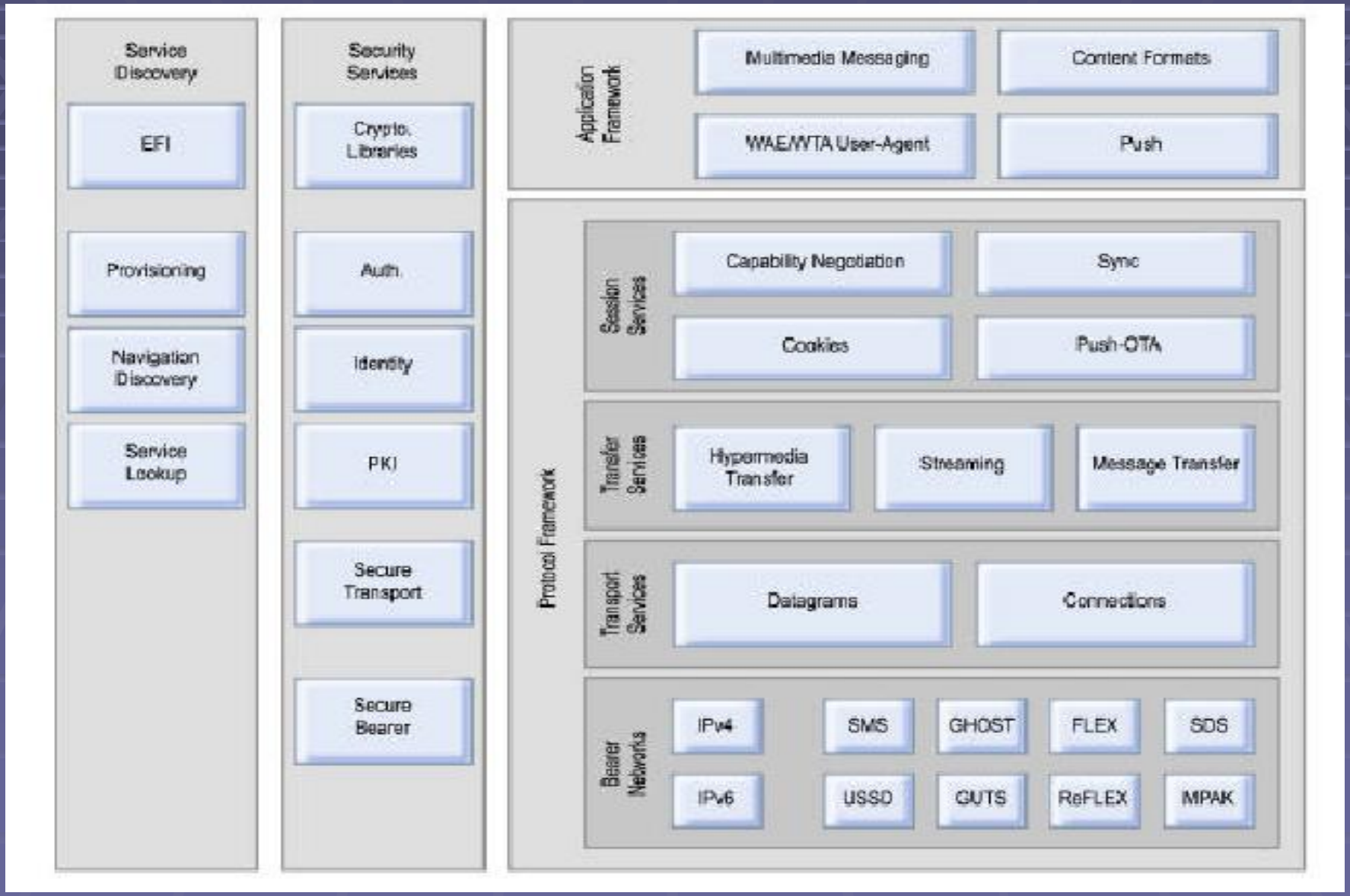


WAP Gateway

- A main difference between WAP and WWW model. It is a ***logical*** component.
- Main Tasks
  - Conversion between WML/WAP protocol type and HTML/HTTP/IP type, i.e. Encoding and Decoding
  - WMLScript Compiling
  - Data Compression for OTA transmission
  - Support different trust models
  - End-user authentication system
- Problems
  - Data is decrypted and again encrypted here
  - No end-to-end security → man-in-the-middle-attack

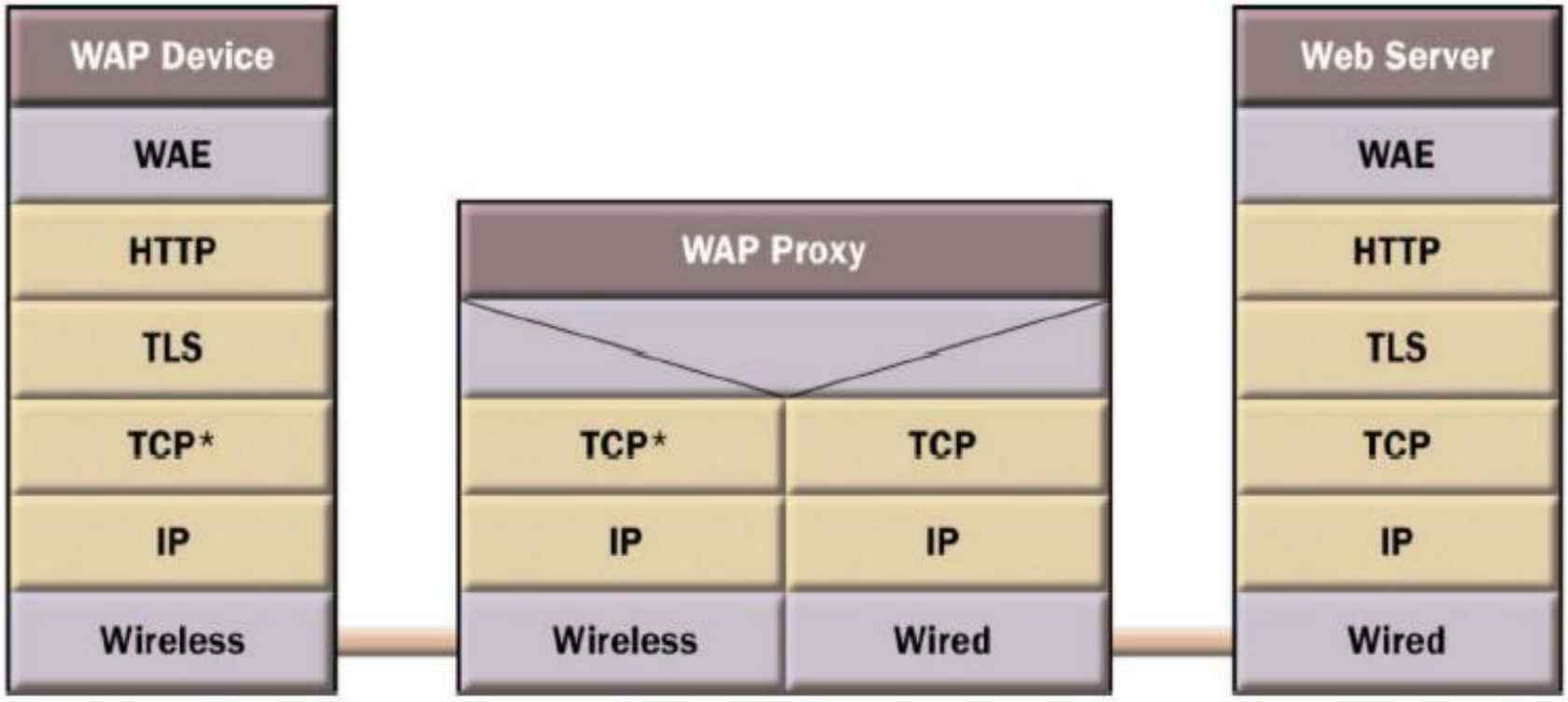


Protocol Structure (WAP 2.0)



WAP 2.x Communication Model

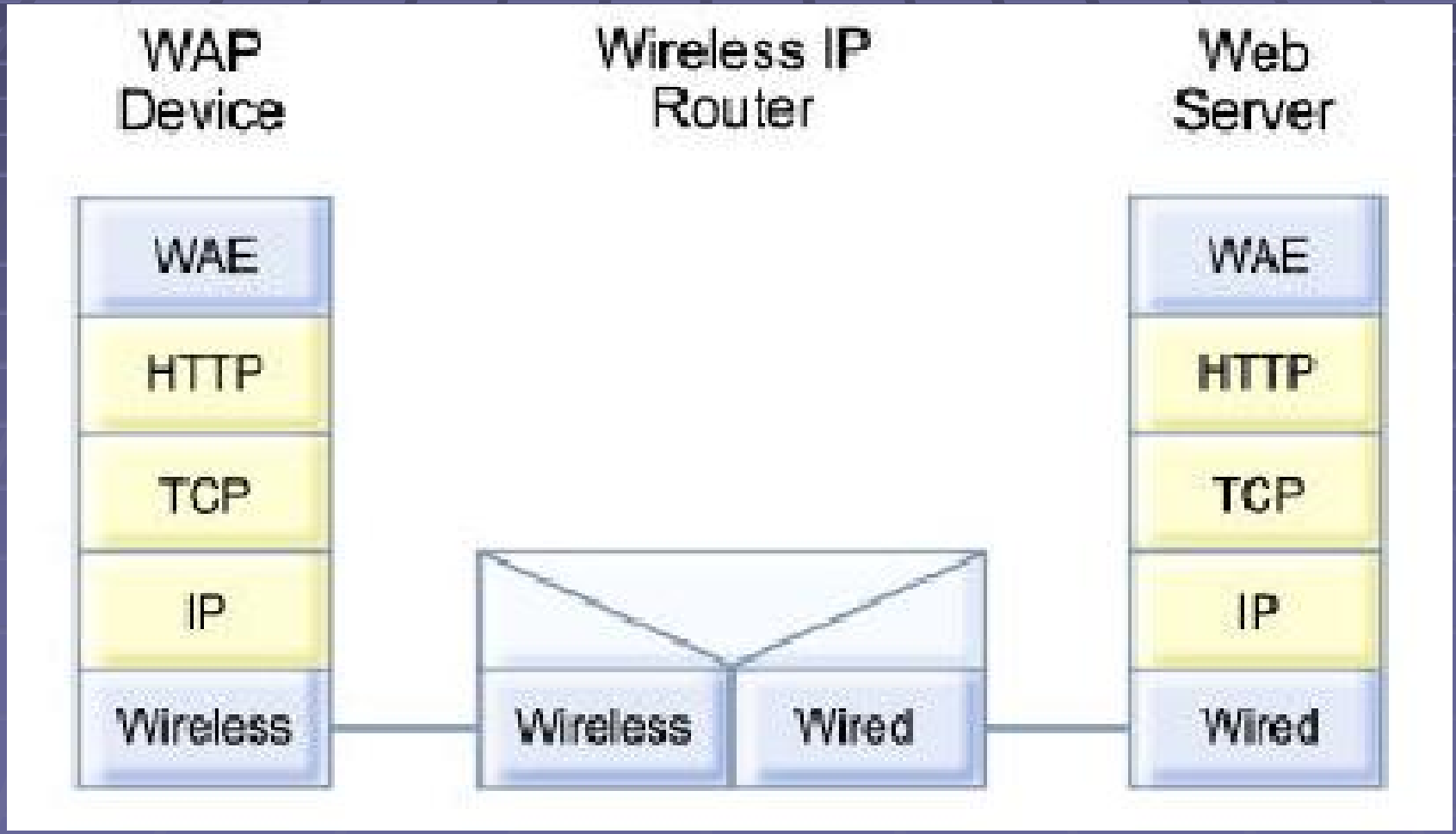
- WAP proxy support for TLS tunneling



TCP*: Wireless Profiled TCP (WP-TCP)

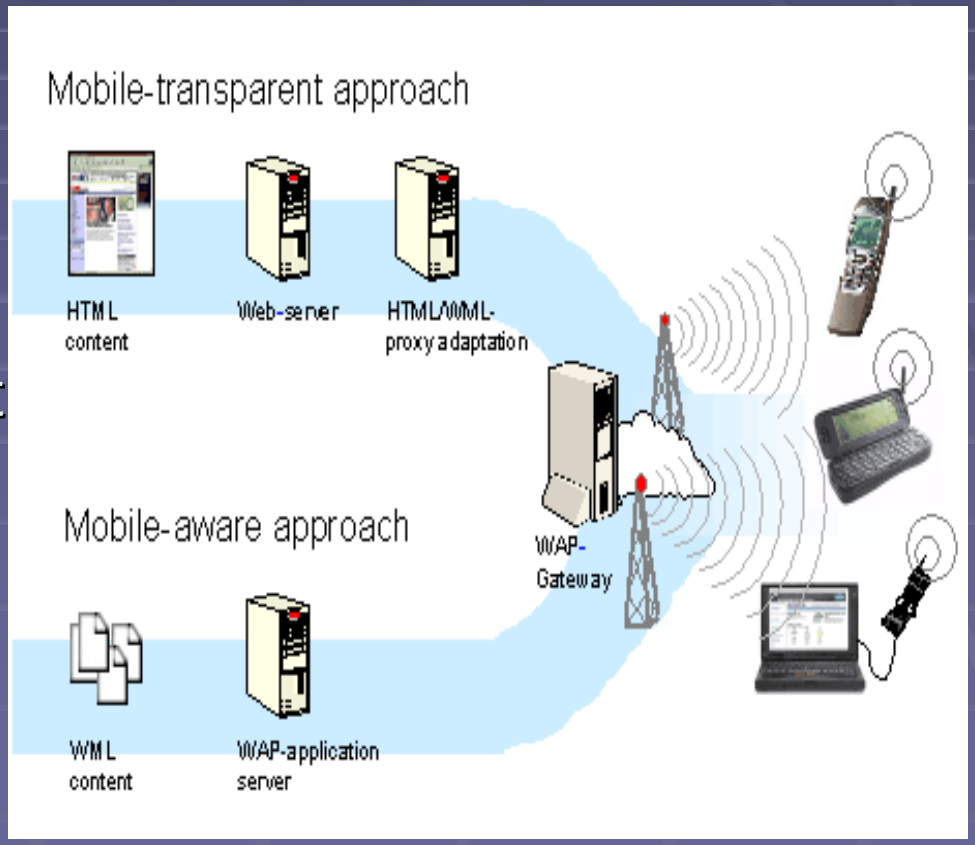
WAP 2.x Communication Model

- Direct Access



WAP Proxy

- An ***optional*** enhancement “WAP gateway”
- Main tasks
  - Protocol gateway translation (backward compatible to WAP 1.0)
  - Content encoding and decoding (Compact and Binary format)
  - WP-TCP and User agent profile management
  - Feature enhancement (e.g. location, privacy)
- Relation with WAP Gateway



Specification WAE

- A general runtime environment for providing service, instead of a protocol
- Aim: To enable operators, manufacturers, and content developers to develop advanced differentiating services and applications (e.g. microbrowser, email)
- Two basic components---In logical, can be integrated together depending on specific architectures and environment.
  - Microbrowser---facilitates browsing of WAP content
  - WTA (Wireless Telephony Application)---an interface to telephony application (call control, phonebook)
- Examples
  - SIM toolkit---build applications into smart card
  - WinCE
  - JavaPhone

Microbrowser

- A variation of standard browser that makes minimal demands on hardware, memory and CPU
- It can display information written in WML and interpret WMLScript files
- Crippleware, by desktop standards
  - Not support cookies
  - Not support HTML above version 3.2
  - Not support frames

WML

- Based on XML, stricter than HTML (e.g. case sensitive)
- The flow of building WML file: Edit->validate->compile+test->publish
- A WML document have multiple pages called ***card*** and this page is named ***deck***
  - Reason: Can retrieve the decks at the same time, i.e. Each request (a dial-up session) for a deck
  - A deck is embraced by <xml>…</xml>
  - A card is embraced by <card>…</card>

WMLScript

- Based on ECMAScript, similar to JavaScript
- Need to be compiled into byte code on server-side before running in Microbrowser
- Not embedded in the WML decks, but only the references to script URLs
- It can access the UML state model as well as the WML variables

Benefits of WAE

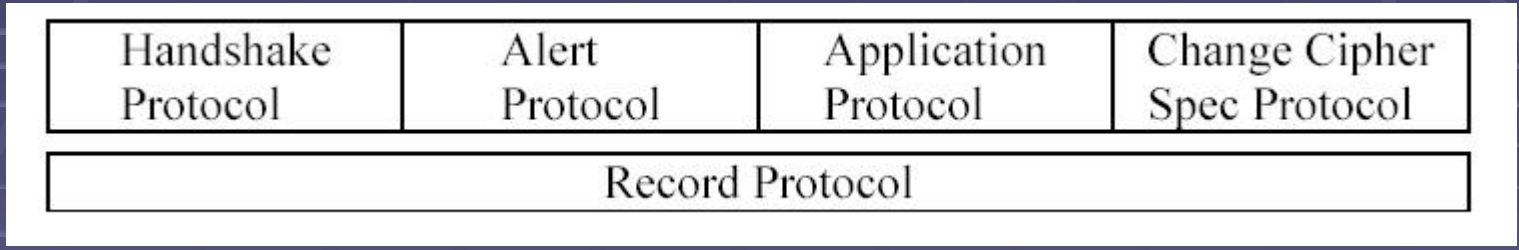
- open standard, vendor independent
- network-standard independent
- transport mechanism–optimized for wireless data bearers
- application downloaded from the server, enabling fast service creation and introduction, as opposed to embedded software (e.g. Java Applet)

WTLS

- An optional security layer with encryption facilities to provide the secure transport service
  - Symmetric cryptography---Privacy
  - Certificate---Authentication
  - MAC---Integrity
- Based on TLS 1.0, modifications are
  - Adding datagram support
  - Optimizing data size
  - Select fast algorithms

WTLS

- WTLS Internal Architecture



  - Handshake protocol: To agree on the protocol options to be used
  - Alert protocol: Contains the severity (3 types) of the message and an alert description
  - Application protocol: Contains the data that is exchanged between the two parties
  - Change Cipher Protocol: To signal transitions in ciphering strategies

WTLS

- Problems
  - Week encryption, anonymous authentication allowed
  - Possible attacks
    - A chosen plaintext recovery attack
    - A datagram truncation attack
    - A message forgery attack
    - Key-search shortcut for some exportable key
  - Main reasons
    - Key size too small (e.g. RSA key 35 bits)
    - Unreliable datagram could be lost, duplicated or reordered

Other WAP Security Components

- WIM---WAP Identification Module, can be implemented in SIM card
- WMLScript

Crypto API

(Non-repudiation)

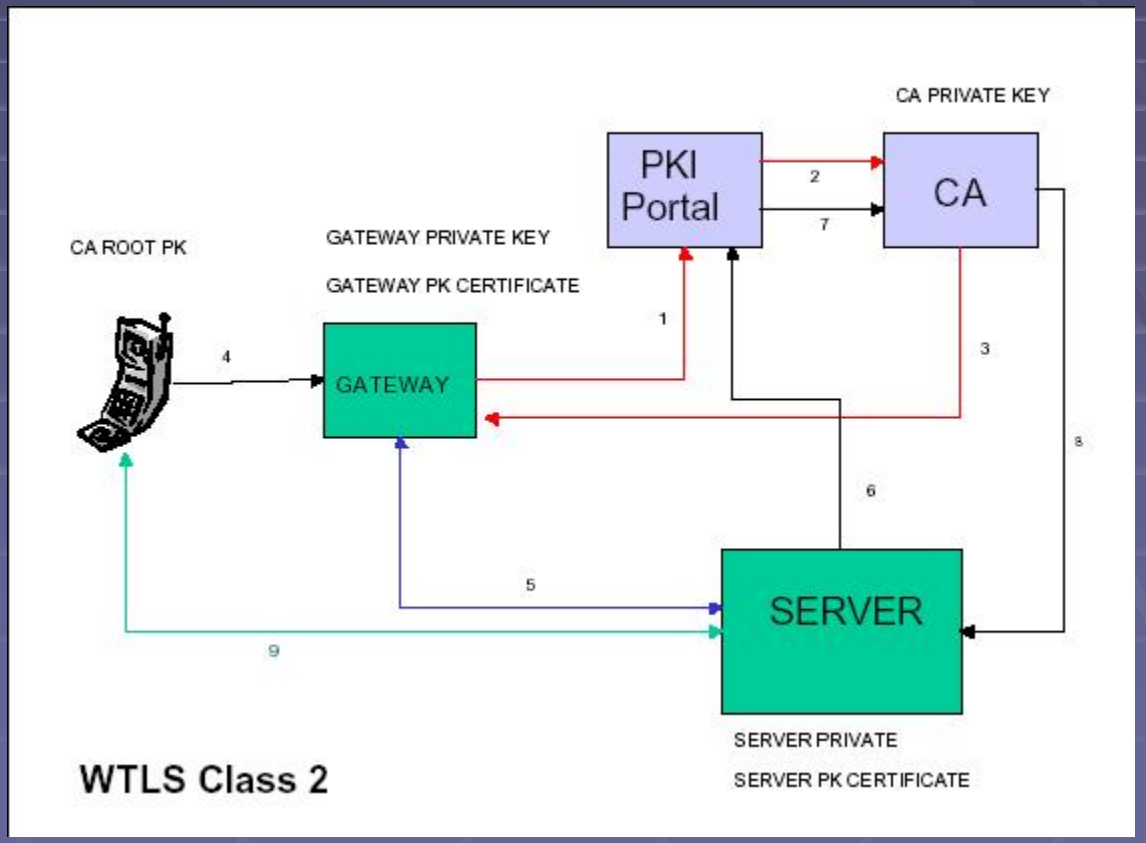
- WML

Access Control

- WPKI---

WAP Public

Key Infrastruture



References

- Books
  - WAP Tutorial: Ericsson Website
  - WPKI: www.wapforum.org
  - WAP Architecture: www.wapforum.org
  - WAP Security: HUT S-38.153
  - WAP Gateway: http://www.palowireless.com/wap/forums.asp
  - Attacks against WTLS, Mr.Markku-Juhani Saarinen
  - Content Networking In The Mobile Internet, Mr.Sudhir Dixit and Mr.Tao Wu
- Links
  - http://www.w3schools.com/wap/wap_basic.asp
  - http://www.palowireless.com/wap/forums.asp
  - http://www.iec.org/online/tutorials/wap/topic05.html
  - http://www.visualtron.com/wap_topic05.htm
  - http://www.mobileinfo.com/WAP/future_outlook.htm

Game Over