Wireless Communication

Lecture 11

Mobile IP and Wireless Application Protocol

Mobile IP Uses

- Enable computers to maintain Internet connectivity while moving from one Internet attachment point to another
- Mobile – user's point of attachment changes dynamically and all connections are automatically maintained despite the change
- Nomadic - user's Internet connection is terminated each time the user moves and a new connection is initiated when the user dials back in
  - New, temporary IP address is assigned

Operation of Mobile IP

- Mobil node is assigned to a particular network – home network
- IP address on home network is static – home address
- Mobile node can move to another network – foreign network
- Mobile node registers with network node on foreign network – foreign agent
- Mobile node gives care-of address to agent on home network – home agent

Capabilities of Mobile IP

- Discovery – mobile node uses discovery procedure to identify prospective home and foreign agents
- Registration – mobile node uses an authenticated registration procedure to inform home agent of its care-of address
- Tunneling – used to forward IP datagrams from a home address to a care-of address

Discovery

- Mobile node is responsible for ongoing discovery process
  - Must determine if it is attached to its home network or a foreign network
- Transition from home network to foreign network can occur at any time without notification to the network layer
- Mobile node listens for agent advertisement messages
  - Compares network portion of the router's IP address with the network portion of home address

Agent Solicitation

- Foreign agents are expected to issue agent advertisement messages periodically
- If a mobile node needs agent information immediately, it can issue ICMP router solicitation message
  - Any agent receiving this message will then issue an agent advertisement

Move Detection

- Mobile node may move from one network to another due to some handoff mechanism without IP level being aware
  - Agent discovery process is intended to enable the agent to detect such a move
- Algorithms to detect move:
  - Use of lifetime field – mobile node uses lifetime field as a timer for agent advertisements
  - Use of network prefix – mobile node checks if any newly received agent advertisement messages are on the same network as the node's current care-of address

Co-Located Addresses

- If mobile node moves to a network that has no foreign agents, or all foreign agents are busy, it can act as its own foreign agent
- Mobile agent uses co-located care-of address
  - IP address obtained by mobile node associated with mobile node's current network interface
- Means to acquire co-located address:
  - Temporary IP address through an Internet service, such as DHCP
  - May be owned by the mobile node as a long-term address for use while visiting a given foreign network

Registration Process

- Mobile node sends registration request to foreign agent requesting forwarding service
- Foreign agent relays request to home agent
- Home agent accepts or denies request and sends registration reply to foreign agent
- Foreign agent relays reply to mobile node

Registration Operation Messages

- Registration request message
  - Fields = type, S, B, D, M, V, G, lifetime, home address, home agent, care-of-address, identification, extensions
- Registration reply message
  - Fields = type, code, lifetime, home address, home agent, identification, extensions

Registration Procedure Security

- Mobile IP designed to resist attacks
  - Node pretending to be a foreign agent sends registration request to a home agent to divert mobile node traffic to itself
  - Agent replays old registration messages to cut mobile node from network
- For message authentication, registration request and reply contain authentication extension
  - Fields = type, length, security parameter index (SPI), authenticator

Types of Authentication Extensions

- Mobile-home – provides for authentication of registration messages between mobile node and home agent; must be present
- Mobile-foreign – may be present when a security association exists between mobile node and foreign agent
- Foreign-home – may be present when a security association exists between foreign agent and home agent

Tunneling

- Home agent intercepts IP datagrams sent to mobile node's home address
  - Home agent informs other nodes on home network that datagrams to mobile node should be delivered to home agent
- Datagrams forwarded to care-of address via tunneling
  - Datagram encapsulated in outer IP datagram

Mobile IP Encapsulation Options

- IP-within-IP – entire IP datagram becomes payload in new IP datagram
  - Original, inner IP header unchanged except TTL decremented by 1
  - Outer header is a full IP header
- Minimal encapsulation – new header is inserted between original IP header and original IP payload
  - Original IP header modified to form new outer IP header
- Generic routing encapsulation (GRE) – developed prior to development of Mobile IP

Wireless Application Protocol (WAP)

- Open standard providing mobile users of wireless terminals access to telephony and information services
  - Wireless terminals include wireless phones, pagers and personal digital assistants (PDAs)
  - Designed to work with all wireless network technologies such as GSM, CDMA, and TDMA
  - Based on existing Internet standards such as IP, XML, HTML, and HTTP
  - Includes security facilities

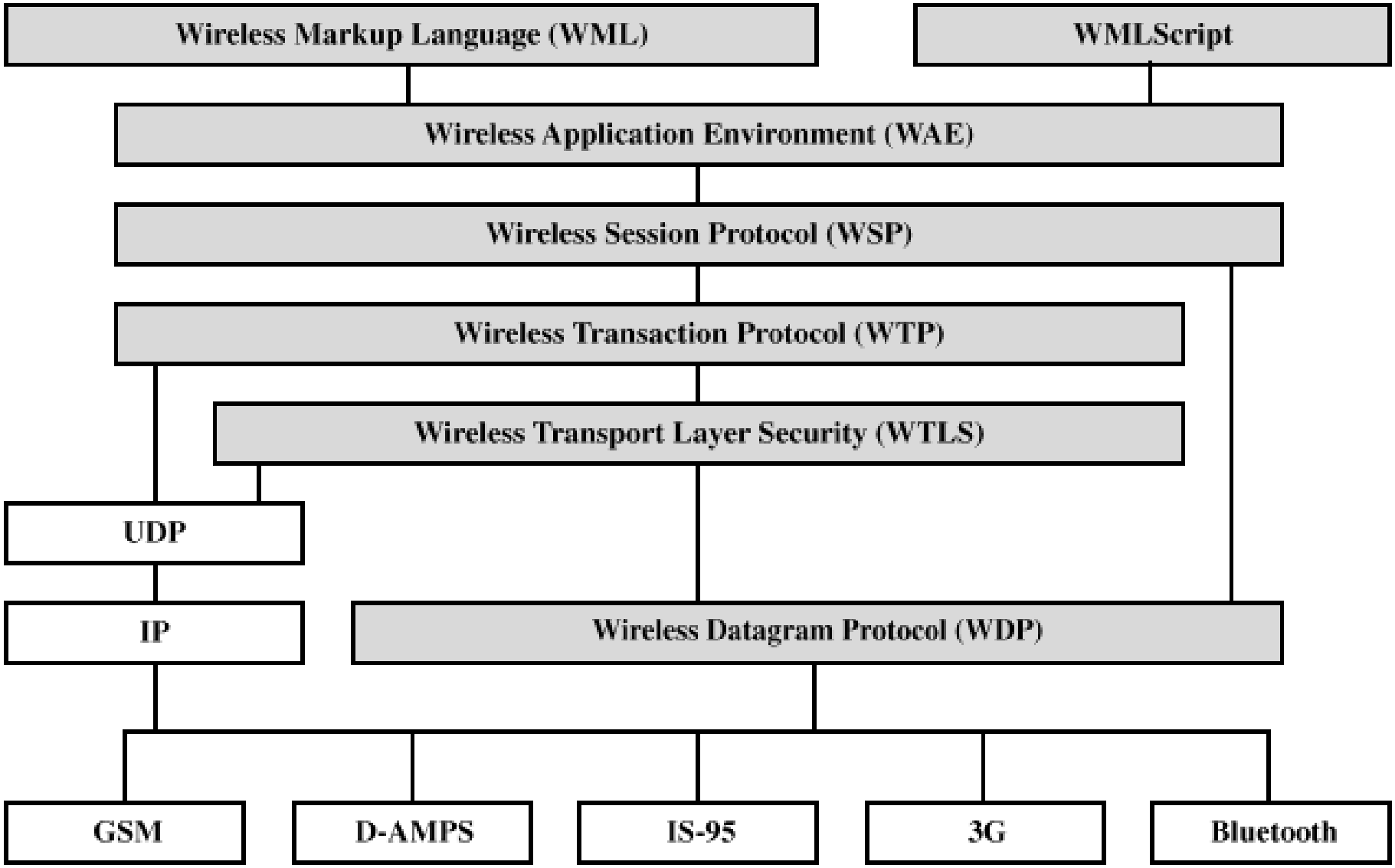
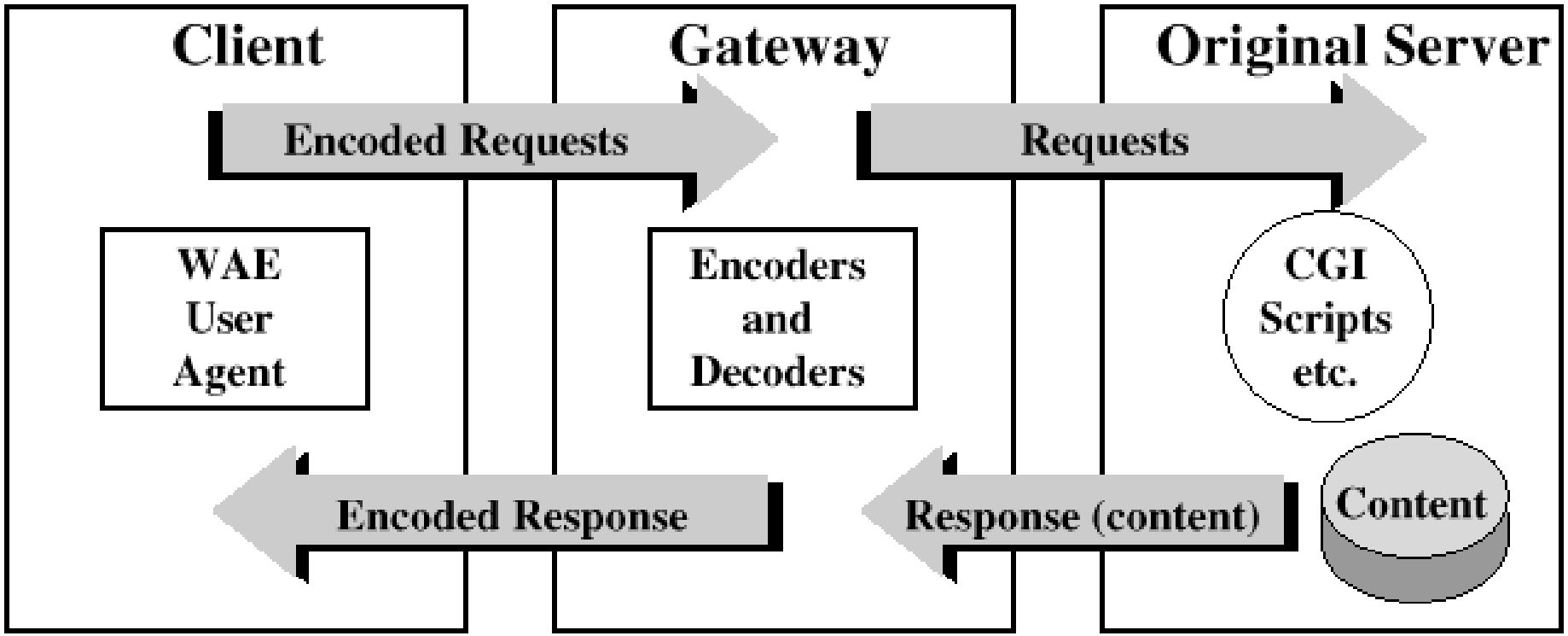


Figure 12.8 WAP Protocol Stack

WAP Programming Model



Wireless Markup Language (WML) Features

- Text and image support – formatting and layout commands
- Deck/card organizational metaphor – WML documents subdivided into cards, which specify one or more units of interaction
- Support for navigation among cards and decks – includes provisions for event handling; used for navigation or executing scripts

WMLScript

- Scripting language for defining script-type programs in a user device with limited processing power and memory
- WMLScript capabilities:
  - Check validity of user input before it's sent
  - Access device facilities and peripherals
  - Interact with user without introducing round trips to origin server

WMLScript

- WMLScript features:
  - JavaScript-based scripting language
  - Procedural logic
  - Event-based
  - Compiled implementation
  - Integrated into WAE

Wireless Application Environment (WAE)

- WAE specifies an application framework for wireless devices
- WAE elements:
  - WAE User agents – software that executes in the wireless device
  - Content generators – applications that produce standard content formats in response to requests from user agents in the mobile terminal
  - Standard content encoding – defined to allow a WAE user agent to navigate Web content
  - Wireless telephony applications (WTA) – collection of telephony-specific extensions for call and feature control mechanisms

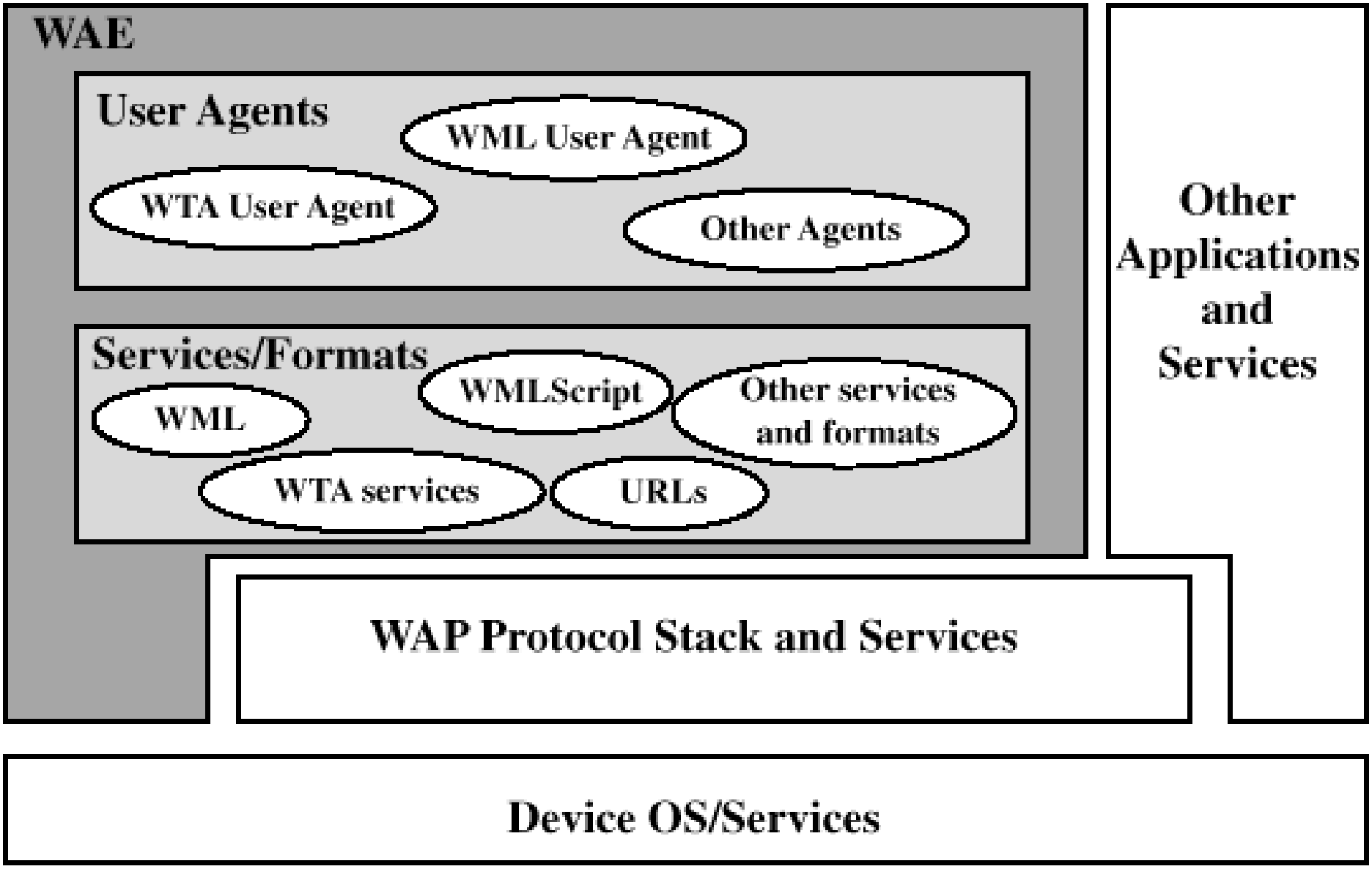


Figure 12.11 WAE Client Components [WAPF98]

Wireless Session Protocol (WSP)

- Transaction-oriented protocol based on the concept of a request and a reply
- Provides applications with interface for two session services:
  - Connection-oriented session service – operates above reliable transport protocol WTP
  - Connectionless session service – operates above unreliable transport protocol WDP

Connection-mode WSP Services

- Establish reliable session from client to server and release
- Agree on common level of protocol functionality using capability negotiation
- Exchange content between client and server using compact encoding
- Suspend and resume a session
- Push content from server to client in an unsynchronized manner

WSP Transaction Types

- Session establishment – client WSP user requests session with server WSP user
- Session termination – client WSP user initiates termination
- Session suspend and resume – initiated with suspend and resume requests
- Transaction – exchange of data between a client and server
- Nonconfirmed data push – used to send unsolicited information from server to client
- Confirmed data push – server receives delivery confirmation from client

Wireless Transaction Protocol (WTP)

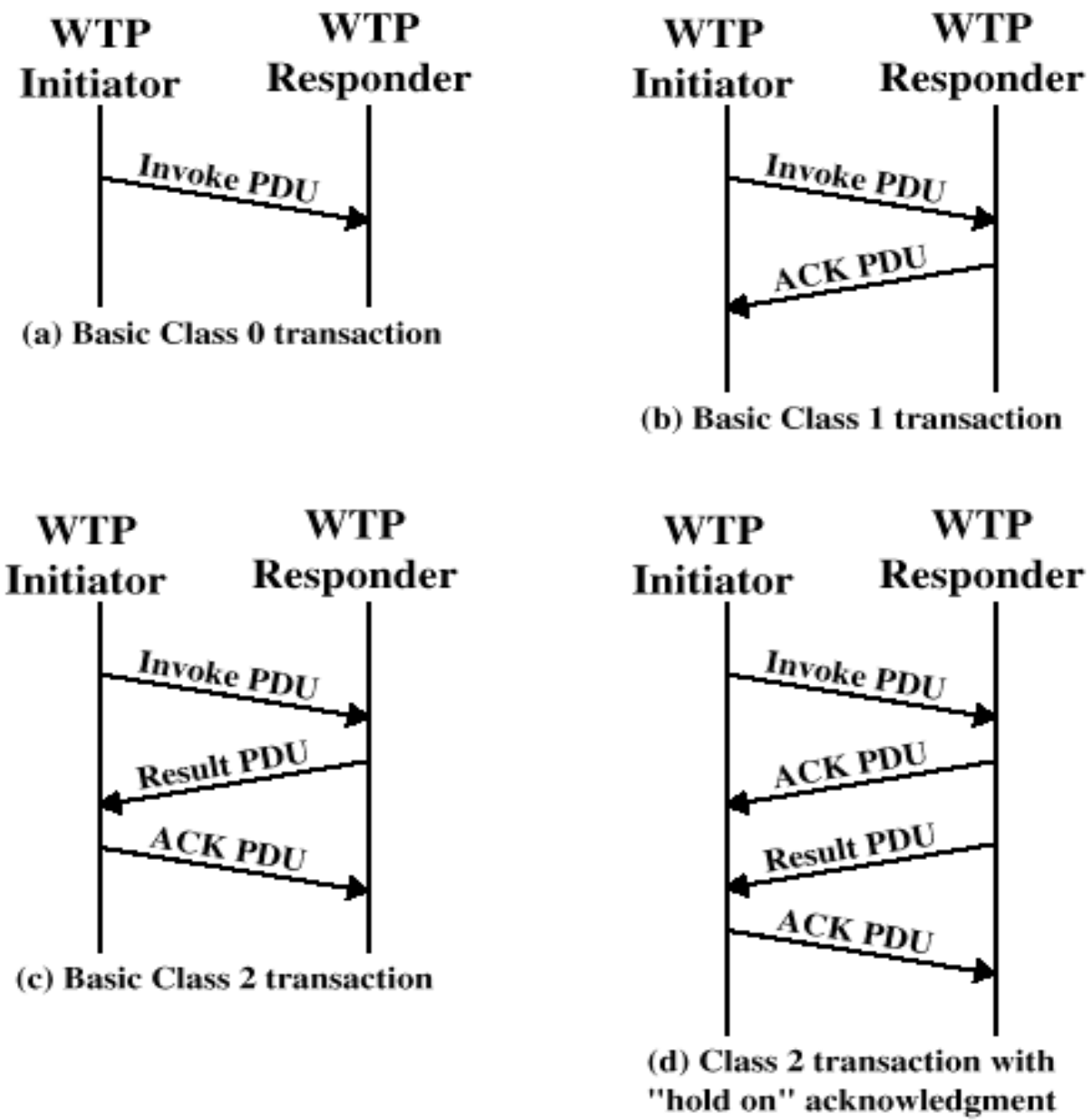
- Lightweight protocol suitable for "thin" clients and over low-bandwidth wireless links
- WTP features
  - Three classes of transaction service
  - Optional user-to-user reliability: WTP user triggers confirmation of each received message
  - Optional out-of-band data on acknowledgments
  - PDU concatenation and delayed acknowledgment to reduce the number of messages sent
  - Asynchronous transactions

WTP Transaction Classes

- Class 0: Unreliable invoke message with no result message
- Class 1: Reliable invoke message with no result message
- Class 2: Unreliable invoke message with one reliable result message

WTP PDU Types

- Invoke PDU – used to convey a request from an initiator to a responder
- ACK PDU – used to acknowledge an Invoke or Result PDU
- Result PDU – used to convey response of the server to the client
- Abort PDU – used to abort a transaction
- Segmented invoke PDU and segmented result PDU – used for segmentation and reassembly
- Negative acknowledgment PDU – used to indicate that some packets did not arrive



n

Figure 12.14 Examples of WTP Operation

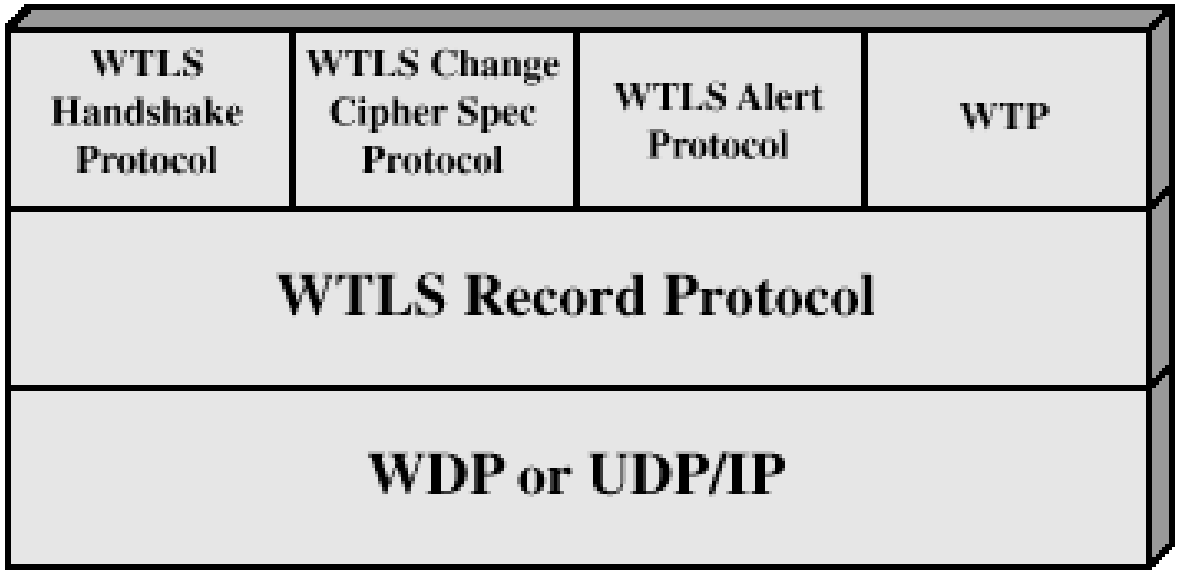
Wireless Transport Layer Security (WTLS) Features

- Data integrity – ensures that data sent between client and gateway are not modified, using message authentication
- Privacy – ensures that the data cannot be read by a third party, using encryption
- Authentication – establishes authentication of the two parties, using digital certificates
- Denial-of-service protection – detects and rejects messages that are replayed or not successfully verified

WTLS Protocol Stack

- WTLS consists of two layers of protocols
  - WTLS Record Protocol – provides basic security services to various higher-layer protocols
  - Higher-layer protocols:
    - The Handshake Protocol
    - The Change Cipher Spec Protocol
    - The Alert Protocol

WTLS Protocol Stack



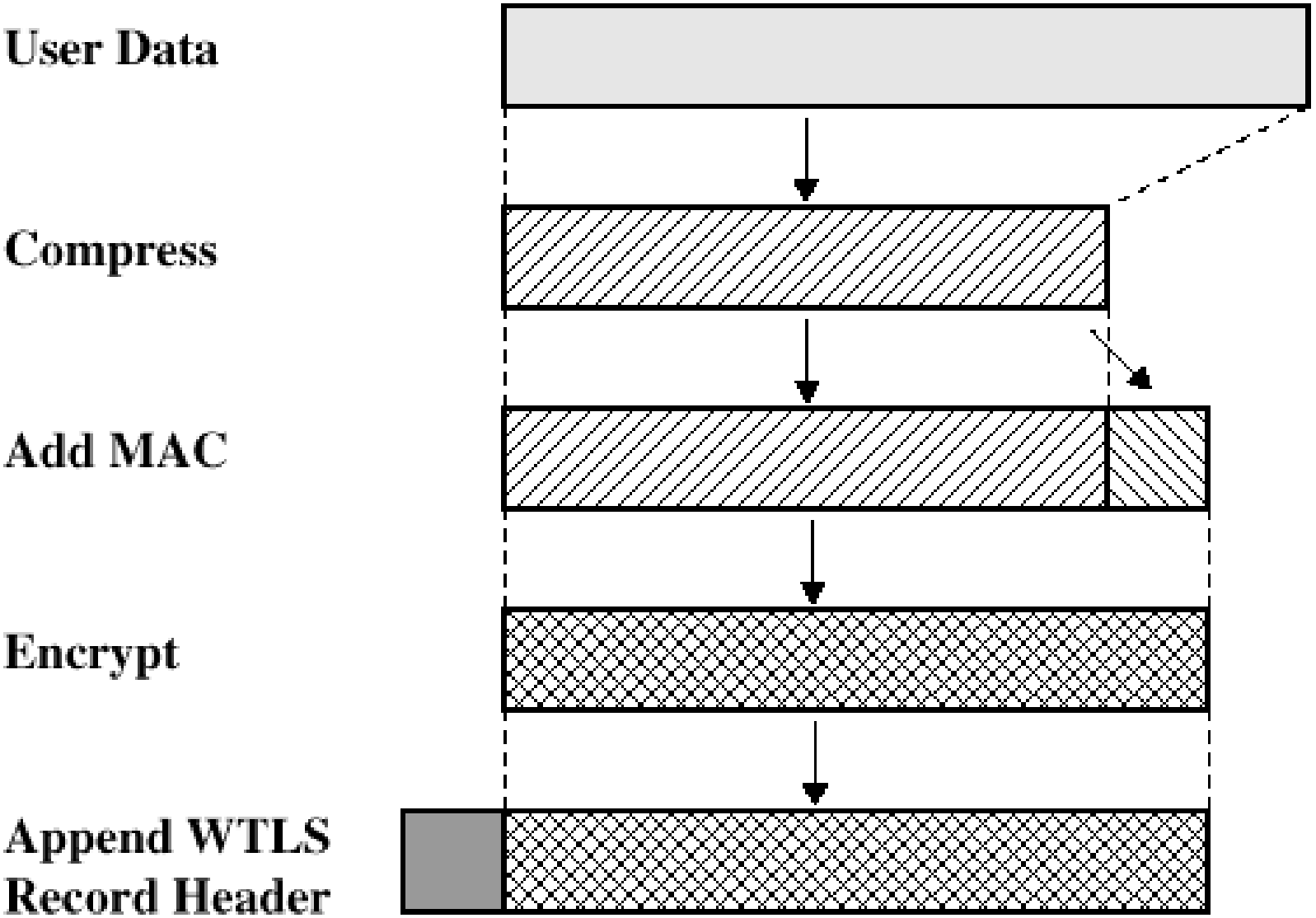


Figure 12.17 WTLS Record Protocol Operation

Phases of the Handshake Protocol Exchange

- First phase – used to initiate a logical connection and establish security capabilities
- Second phase – used for server authentication and key exchange
- Third phase – used for client authentication and key exchange
- Forth phase – completes the setting up of a secure connection

Wireless Datagram Protocol (WDP)

- Used to adapt higher-layer WAP protocol to the communication mechanism used between mobile node and WAP gateway
- WDP hides details of the various bearer networks from the other layers of WAP
- Adaptation may include:
  - Partitioning data into segments of appropriate size for the bearer
  - Interfacing with the bearer network

Wireless Control Message Protocol (WCMP)

- Performs the same support function for WDP as ICMP does for IP
- Used in environments that don't provide IP bearer and don't lend themselves to the use of ICMP
- Used by wireless nodes and WAP gateways to report errors encountered in processing WDP datagrams
- Can also be used for informational and diagnostic purposes