Assignment No. 04

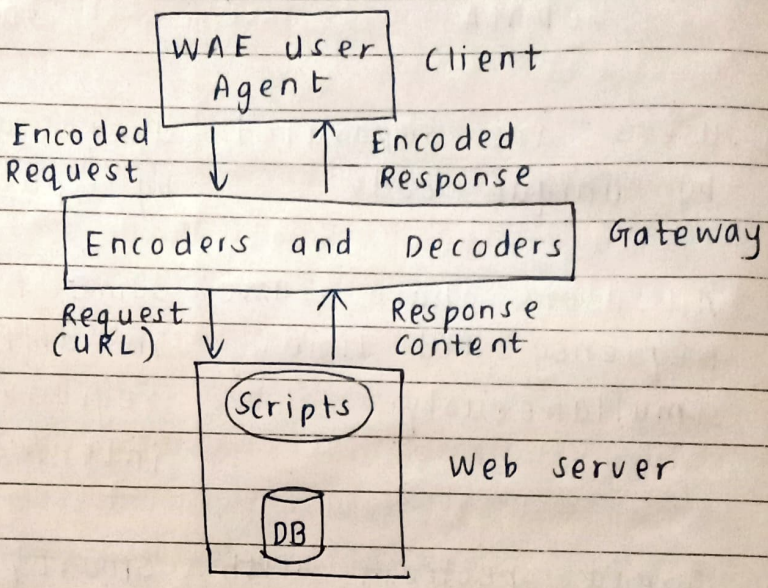
Page No.
Date

Unit IV

Fundamentals of Cellular and LTE Technology
Wireless Communication Protocols

Q1 What is WAP? Explain Wireless Application Protocol architecture in details.

Ans.



WAP Architecture

WAP architecture is made up of several components that work together to deliver web content to mobile devices.

1. WAP Gateway

Acts as a bridge between the ~~bridge~~ mobile device and the internet. It translates requests from the mobile device to standard HTTP requests that can be understood by web servers. It also converts the responses from web servers to a suitable format for the mobile device.

2. WAP Client

This is the application on the mobile device that interacts with the WAP Gateway. It is responsible for sending

requests and displaying the content received from the gateway.

3. WAP Server
Hosts WAP-enabled content and services. It is similar to a web server but is specifically designed to serve content to WAP clients.

4. Content Provider
Supplies the content that is accessed through WAP. This could be a website, a service, or an application designed for mobile users.

Q.2. What is NFC? What are the characteristics of NFC?

Ans. NFC (Near-Field Communication) is a short-range wireless communication technology that allows two electronic devices to exchange data when they are brought within a few centimeters (typically less than 4 cm) of each other.

- It is based on Radio Frequency Identification (RFID) technology and operates 13.56 MHz frequency.

e.g. Tapping your smartphone to make a contactless payment, or pairing devices by bringing them close together.

* Characteristics of NFC

1. Short-Range Communication
Operates within a distance of about 0-4 cm for security and accuracy.

2. High Frequency (13.56 MHz)
Works at a globally accepted ISM (Industrial, Scientific, and Medical) frequency band.

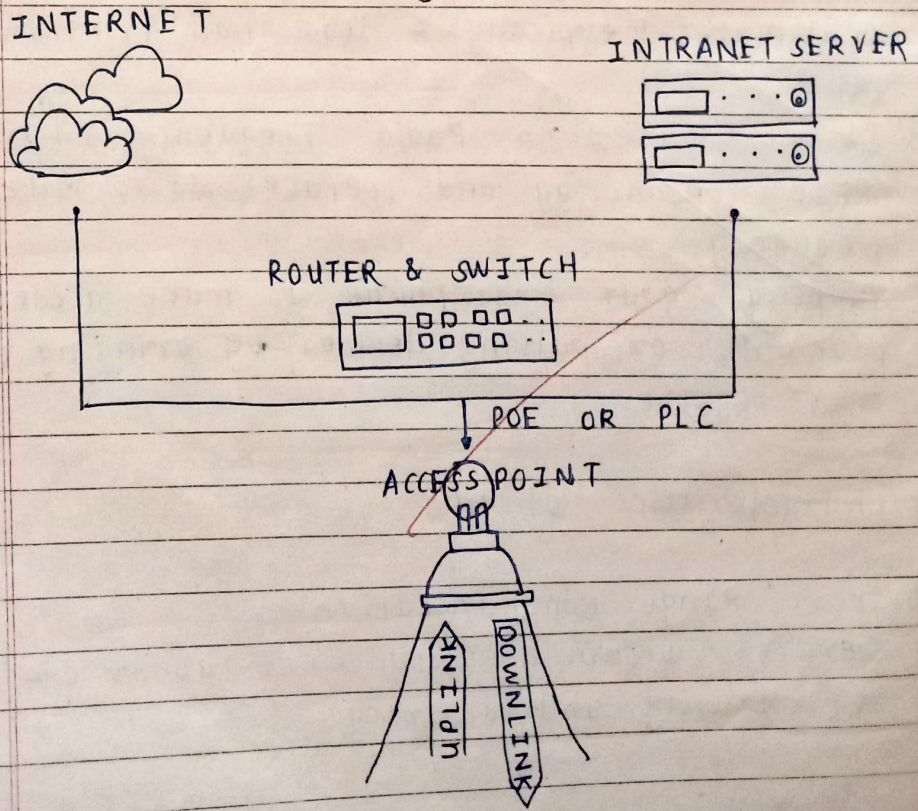
3. Low Data Transfer Rate
Typical speed: 106 Kbps to 424 Kbps - enough for small data exchanges like payments or authentication.

4. Simple and Fast Connection Setup
Establishes communication instantly without pairing or manual configuration (unlike Bluetooth).

5. Secure Data Exchange
Short range makes it difficult for hackers to intercept communication. Often used in secure transactions (credit/debit card tap payments).

Q.3. What is Li-Fi? Explain the working principle of LiFi Technology.

Ans.



- Light Fidelity, also known as Li-Fi, uses the power of light to transmit data. This technology harnesses light signals to connect to the internet. Unlike Wi-Fi, which uses radio waves to create a wireless connection, Li-Fi relies on light to transmit data. Through this process, Li-Fi promises speeds that are 100 times faster than Wi-Fi.
- Li-Fi functions as a Visible Light Communications system; at its core, data is transferred from LED light bulbs. These bulbs carry pulses of light that produce information similar to Morse code. This process can't be seen by the naked eye. The game changers in this scenario are the compatible devices that can synthesize this information rapidly.

* Working Principle.

1. Data source Input
   The internet data (binary form - 0s and 1s) is first fed into a Li-Fi transmitter
2. LED Light Modulation
   - LED bulb acts as the transmitter.
   - The current supplied to the LED is varied (modulated) according to the data signal.
   - When the LED is ON, it represents binary 1, and when OFF, it represents 0.
   - These rapid light intensity changes happen millions of times per second, so humans don't notice any flicker.
3. Transmission of Light signals
   The modulated light carries the data through the air.

It travels in a line-of-sight path to the receiver.

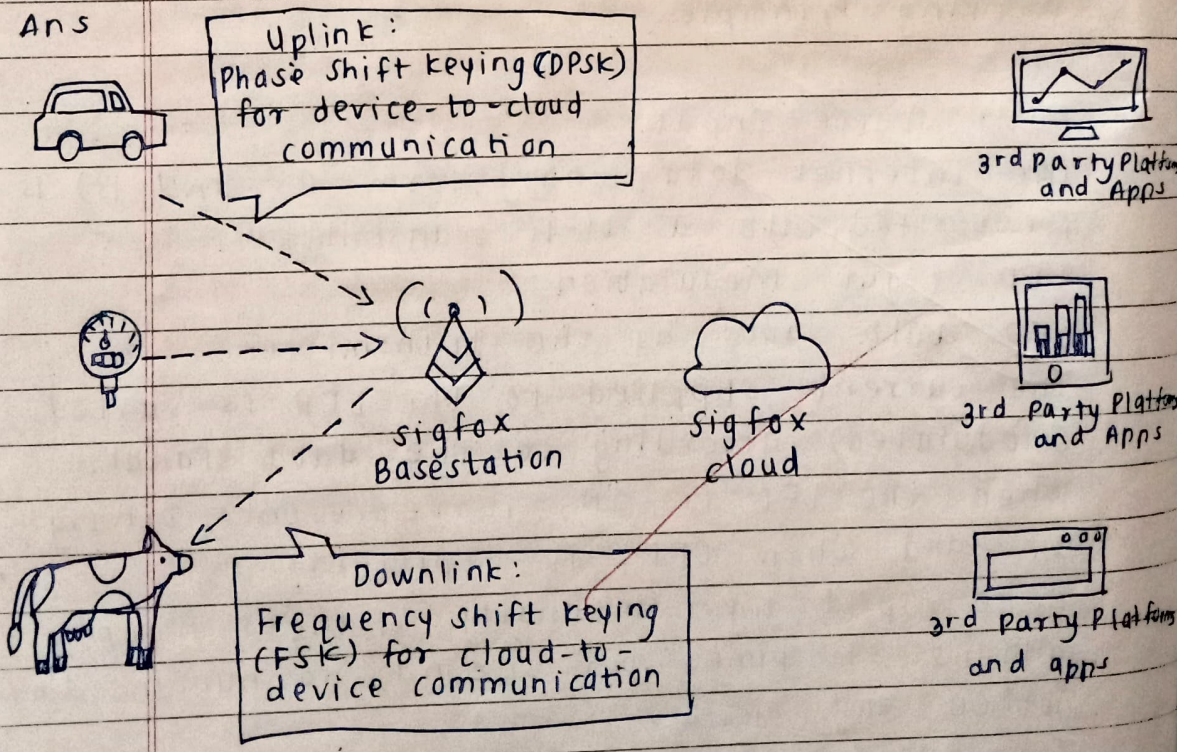
4. Photodiode Receiver
   - A photodiode (light sensor) at the receiver end detects the light variations.
   - It converts the received light signals back into electrical signals.

5. Data Processing
   The electrical signals are then decoded into digital data - such as text, audio, video, or internet information.

6. Bidirectional Communication (Uplink and Downlink)
   For two-way communication, separate LEDs or infrared transmitters are used for the uplink (device → light source).

Q 4. Explain in detail sigfox protocol.

Ans



The sigfox protocol is a Low-Power Wide Area Network (LPWAN) technology for the Internet of Things (IoT) that uses Ultra-Narrow Band (UNB) communication in the sub-GHz ISM band to transmit small data packets over long distances with low power p· consumption. Key features include binary phase-shift keying BPSK modulation, triple diversity (time, frequency, space) for reliability, a subscription based network, and a restriction on data payload size (12 bytes uplink, 8 bytes downlink) and message frequency.

* How it Works

1. Device Transmission
An IoT device sends a small data message using BPSK modulation over the UNB frequency band.

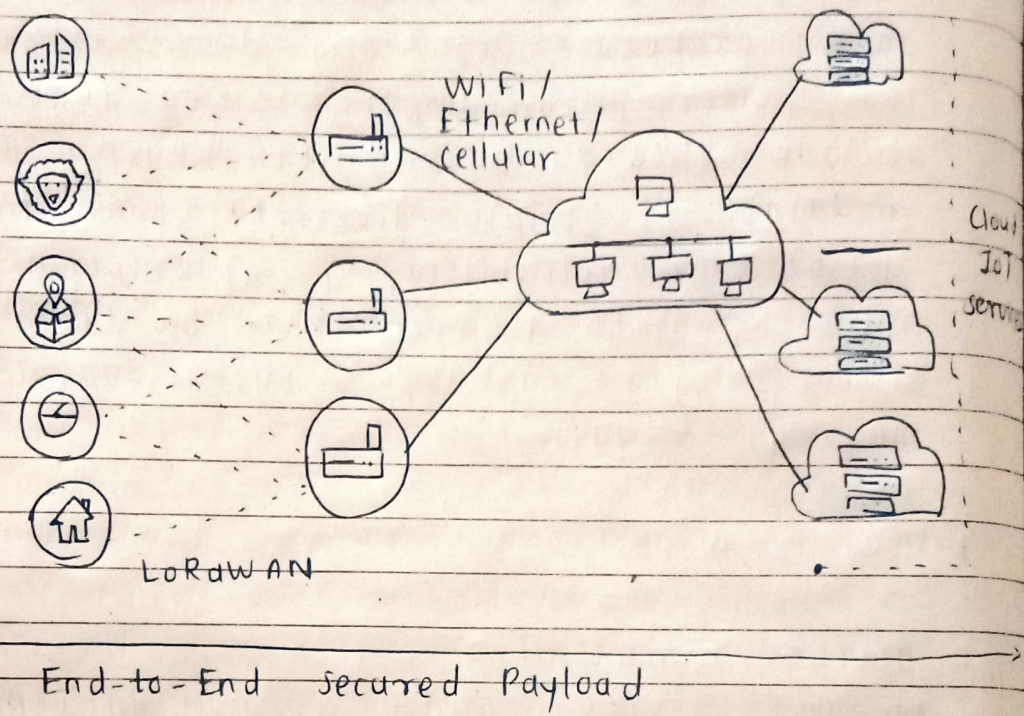
2. Base station Reception
The message is picked up by multiple nearby sigfox base stations, which use cooperative reception for reliability.

3. Cloud Relay
The base stations relay the message to the sigfox cloud via an IP-based network.

4. Application Integration
The cloud then pushes the message to a customer's server or IoT platform for processing

Q 5 What is LoRaWAN? Elaborate LoRaWAN network elements.

Ans.



LoRaWAN (Long Range Wide Ared Network) is a Low Power wide Area Network (LPWAN) protocol designed for IoT applications that require long-range communication, low power consumption, and secure data transmission.

* LoRaWAN Network Elements

1. End Devices (Nodes)
These are IoT devices or sensors (like temperature sensors, smart meters, GPS trackers). They collect data and send it wirelessly to gateways using the LoRa modulation. Operate on low power - often battery power. e.g. Smart parking sensors, weather stations.

2. Gateways
Act as a bridge between end devices and the network server Receiver LoRa signals from many end devices From forward data via IP connection (Ethernet, Wi-Fi, or cellular) to the network server One gateway can serve thousands of nodes.

3. Network Server
The central controller of LoRaWAN network Filters duplicate messages from gateways. Manages device authentication and security Handles adaptive data rate and routing of packets to the correct application server.

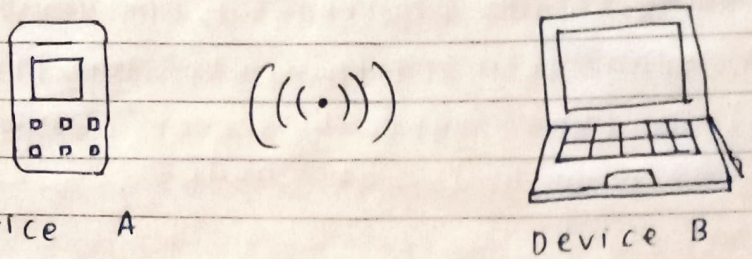
4. Application Server
Receives processed data from the network server Decodes, stores, and displays data for end users Interfaces with business logic, dashboards, or external systems e.g Displays temperature readings on a web dashboard.

5. Join Server (Optional)
Handles the activation and authentication of end devices using unique keys. Ensures secure device onboarding through Over-The-Air Activation (OTAA).

Q.6. What is Wi-Fi Direct? What are the different types of Wi-Fi Direct?

Ans. Wi-Fi Direct is a technology that allows devices to connect directly to each other over Wi-Fi without needing a wireless router or access point.
It's used for file sharing, printing, screen

mirroring, and media streaming between devices like smartphones, laptops, and smart TVs.



Wi-Fi Direct

* Types of Wi-Fi Direct connections

1. Device-to-Device (Peer-to-peer) Mode
- The most common form of Wi-Fi direct.
- Two devices connect directly to each other without an access point.
- One device automatically becomes the Group Owner (GO) like a temporary access point, and the other becomes a Client.
- e.g. Sending files between two smartphones using Wi-Fi Direct share.
- Use case: File transfer, printing, simple data sharing.

2. Group (Multi-Device) Mode
- A Wi-Fi Direct Group can include one Group owner and multiple clients.
- The Group owner handles device management and data routing.
- Devices can join or leave dynamically
- Use case: Multi-player gaming, classroom device networks, multi-device control apps

3. Persistent Group Mode
- Once two devices have connected using Wi-Fi Direct, they can remember the connection.
- Next time, they reconnect automatically without repeating authentication steps.
- Use case: Smart home devices (e.g. a phone reconnecting to a Wi-Fi Direct smart bulb automatically).

4. Temporary (Non-Persistent) Group Modp
- The connection is created for a single session and forgotten afterward.
- Devices need to go through setup again for future connections.
- Use Case: One time file transfers or short-term connections

5. Wi-Fi Direct + Internet Connectivity (Hybrid Mode)
- Some modern devices allow using Wi-Fi Direct while maintaining an active internet connection through another interface (like mobile data or Wi-Fi network).
- This allows devices to communicate directly and stay online simultaneously.
- Use case: screen casting to a smart TV while still using the internet on your phone.

Q.7. Write short notes on: Bluetooth security, WEP, WPA 2.

Ans. 1. Bluetooth Security
- Bluetooth is a short-range wireless communication technology used for connecting devices like phones, headphones, and laptops.
- To ensure secure communication, Bluetooth

uses several security features.

- Authentication: Confirms the identity of connected devices using a PIN or pairing code.
- Encryption: Data transmitted between devices is encrypted to prevent eavesdropping.
- Authorization: Controls access so only trusted devices can connect.
- Secure Simple Pairing (SSP): Introduced in Bluetooth 2.1+, it uses public key cryptography to strengthen security during pairing.
- Threats: Bluejacking (sending unwanted messages), Bluesnarfing (data theft), and Bluebugging (remote control attacks).

2. WEP (Wired Equivalent Privacy)

- WEP is the oldest Wi-Fi security protocol, introduced in 1997 as part of the IEEE 802.11 standard.
- It was designed to provide data confidentiality similar to that of a wired network.
- Uses RC4 encryption algorithm and a 40-bit or 104-bit key with a 24-bit Initialization Vector (IV).
- Provides basic encryption and authentication, but is highly vulnerable to attacks due to weak key management.
- Can be easily cracked using freely available tools.

3. WPA2 (Wi-Fi Protected Access 2)

WPA2 is a Wi-Fi security protocol introduced in 2004 as an improved version of WPA

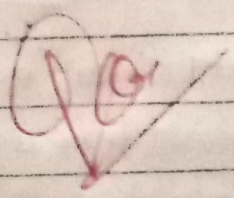
It uses AES (Advanced Encryption Standard) for strong data protection.

Uses CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for encryption and integrity

Supports two modes:

- Personal Mode (WPA2-PSK) - Uses a pre-shared key (for homes)
- Enterprise Mode (WPA2-Enterprise) - Uses a RADIUS server for user authentication (for organizations)

Provides high-level security for modern security for modern Wi-Fi networks.



Q3

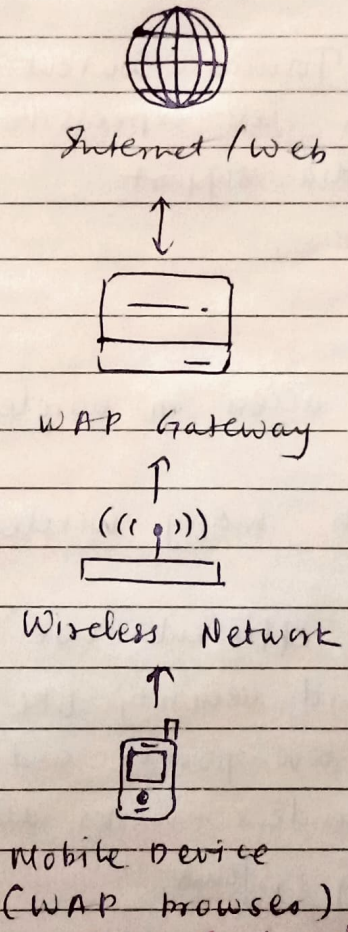
Any

Elective IV - Wireless Communication

Unit 04 Wireless Communication Protocols

Q 3 a) What are the different challenges in WAP? Also write down the advantages and disadvantages of WAP.

Ans



WAP Architecture

Challenges in Wireless Application Protocol (WAP)

1. Limited Bandwidth: Early wireless networks had very low data rates, causing slower access and delays.
2. High Latency: Wireless communication often experiences delays due to signal processing and network congestion.
3. Small Display and Input Constraints: WAP devices (like old mobile phones) had small screens and numeric keypads, limiting web experience.

Now outdated and replaced by

4. Security Concerns: WAP uses a gateway that translates protocols, which can create a potential security gap (WAP gap problem)
5. Unstable connectivity: Wireless connection can drop easily due to mobility, weather, or interference.
6. Device compatibility: Different mobile devices and vendors supported WAP differently, reducing application consistency.
7. Limited Content Format: Content was created using WML, which is less expressive than HTML and limited in media support.

Advantages

- Allows internet access on wireless devices (mobile phones, PDAs)
- Compatible with many wireless networks (GSM, GPRS, 3G)
- Low cost and efficient use of bandwidth.
- Supports standard security like WTLS
- Optimized for low-power and low-memory devices
- Platform independent - works across different devices and operating systems.

Disadvantages

- Low speed compared to modern mobile internet
- Poor user experience due to small screens and limited formatting
- Security gap caused by protocol conversion at WAP Gateway
- Limited multimedia support

- Now outdated and replaced by modern technologies (HTML5, Wi-Fi - 4G/5G)

NOV-DEC 2023

Q3 a) Examine Wireless Application Protocol for effectiveness in wireless communication environment

Any

Wireless Application Protocol (WAP) was developed as an open global standard to enable mobile devices such as early cell phones and PDAs to access internet-based content and services over wireless networks. Before the advent of modern web technologies (e.g., HTML5, 4G/5G, responsive design), WAP served as a bridge between limited mobile hardware and the expanding internet.

Key Features

1. Lightweight Markup Language (WML): Designed specifically for small screens and low bandwidth to optimize content delivery.
2. WAP Gateway: Acts as an intermediary between the mobile device and the Internet, converting the WAP requests into HTTP and vice versa.
3. Wireless Security Layer (WTLS): Provides data integrity, authentication, and encryption similar to SSL to secure data transmission.
4. Compatibility with Multiple Wireless Bearers: Works across GSM, CDMA, GPRS, SMS, and early 2G/2.5G networks

Overall Effectiveness

- Network Efficiency: Very effective for early low-bandwidth networks.
- Security Effective with WTLS for early m-commerce

- User Experience: Poor by modern standards
- Content Availability: Limited
- Long-term Viability: Replaced by modern mobile web and apps.

Q.4 a) Write short notes on UMTS security, Bluetooth security, WEP, WPA 2

Ans

1. UMTS Security

Universal Mobile Telecommunication System (UMTS) is a 3G mobile communication system that introduced enhanced security features compared to 2G networks like GSM.

- Mutual Authentication: Both user and network authenticate each other using AKA (Authentication and Key Agreement) protocol.
- Stronger Encryption: Uses advanced ciphering algorithms such as KASUMI for confidentiality.
- Integrity Protection: Ensures that signaling data is not tampered with using integrity keys.
- Temporary Identities: Uses TMSI (Temporary Mobile Subscriber Identity) to protect user identity from being exposed.
- Protection Against Cloning and Eavesdropping.

Overall, UMTS security significantly improved network trustworthiness and reduced risks like SIM cloning and impersonation seen in GSM.

2. Bluetooth Security

Bluetooth is a short-range wireless communication technology used for connecting devices like phones, PCs, and headsets.

Security Components

- Pairing and Authentication: Devices use PIN or numeric comparison to authenticate.
- Encryption: Uses E0 stream cipher to protect data over the air.
- Security Modes:
  - Mode 1: No security
  - Mode 2: Service-level security
  - Mode 3: Link-level security
- Threats: Bluejacking, Bluesnarfing, Bluebugging, and man-in-the-middle attacks.
- Mitigation: Strong pairing keys, non-discoverable mode, regular software updates.

Bluetooth security focuses on preventing unauthorized access, eavesdropping, and device misuse.

3 WEP (Wired Equivalent Privacy)

WEP is a security protocol for wireless LANs (IEEE 802.11) designed to provide confidentiality comparable to wired networks.

- Uses RC4 encryption with 40-bit or 104-bit secret key plus 24-bit IV (Initialization Vector)
- Provides basic confidentiality and access control.
- Weaknesses:
  - Small IV size leads to key reuse
  - Vulnerable to passive attacks and key cracking tools (e.g., Aircrack)
  - No effective integrity protection (CRC-32 easily modified)

Due to significant vulnerabilities, WEP is now considered insecure and deprecated.

4. WPA 2 (Wi-Fi Protected Access 2)

WPA2 is the improved wireless network security standard replacing WEP and WPA.

- Uses AES - CCMP (Advanced Encryption Standard - Counter Mode with CBC-MAC) for strong data confidentiality and integrity.
- Supports Pre-Shared Key (PSK) mode for home networks and Enterprise mode with 802.1X authentication.
- Robust security against most brute-force and replay attacks.
- Vulnerabilities include key reinstallation attack (KRACK), mitigated through patches and updates.

WPA2 is widely used as a standard for secure Wi-Fi communication until replaced gradually by WPA3.

Nov - Dec 2024

Q.4 b) Explain the terms: Z-wave, RT, LoRaWAN, Wi-Fi, SPEED

Ans 1. Z-Wave

- Z-Wave is a wireless communication protocol primarily used for home automation and smart devices. It allows smart home products - such as smart lights, locks, and thermostats - to communicate with each other.
- Operates on low-power radio frequency (around 908/868 MHz, depending on region)
- Designed for short-range, low-bandwidth communication
- Uses mesh networking, where each device relays signals, increasing coverage
- Used in IoT smart home ecosystems such as security systems and energy monitoring.

2 RT Wi-Fi (Real-Time Wi-Fi)

RT Wi-Fi is an enhanced form of Wi-Fi designed to support real-time and time-sensitive communication with low latency and high reliability.

- Modified MAC protocol allowing deterministic data transmission.
- Suitable for industrial automation, robotics, drones, and smart factories
- Provides guaranteed delivery times compared to normal Wi-Fi which is best-effort

3. SPEED (Serial Packet Exchange over Ethernet for Devices)

SPEED is a communication protocol designed for industrial networks to exchange serial data packets over Ethernet.

- Supports high-speed communication between industrial controllers and field devices
- Replaces traditional serial connections with Ethernet-based transport.
- Useful in SCADA, automation systems, and real-time control.

* WAP Programming Model

The WAP (Wireless Application Protocol) programming model is similar to the traditional web-based client/server model, but optimized for mobile devices with limitations such as low bandwidth, small screens, and limited processing power.

Example Components

- Mobile Device (WAP Client): Runs a micro-browser that requests and displays wireless content (WML)

Wireless Network: Provides connectivity between WAP device and WAP gateway.

WAP Gateway/Proxy: Converts WAP requests to HTTP requests and vice versa. Includes encoding/decoding and protocol translation.

- Web Server/Application Server: Stores content (WML, WMLScript, images) and processes requests.

* Flow in WAP Programming model

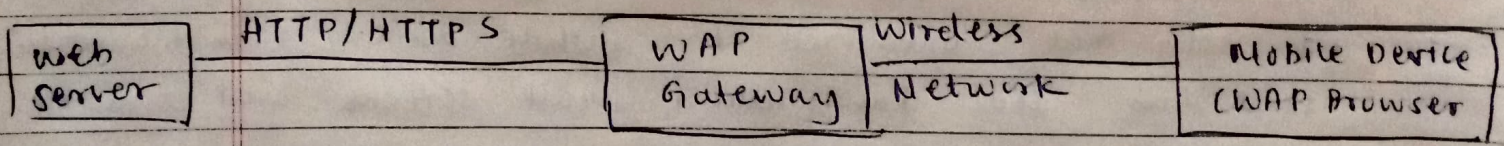
1. User selects a service on a mobile device (WAP browser)
2. Mobile device sends a requests through the wireless network to the WAP Gateway.
3. The WAP Gateway translates WAP requests to HTTP/HTTPS requests and sends them to the web server.
4. Web server returns content (WML pages or data).
5. Gateway converts HTTP response to WAP format and sends it to wireless device.

Mobile Device → Wireless Network → WAP Gateway/Proxy → Web Server (Content Provider)

* Traditional WAP Networking Environment

The traditional WAP networking environment defines how data moves between WAP-enabled mobile devices and the internet

* WAP Networking Architecture



* Components

- Mobile Device: Runs WAP browser to access WML pages

- Wireless Network (GSM / CDMA / GPRS / 3G): Provides transmission medium
- WAP Gateway: Acts as a bridge between mobile network and Internet, performs encoding, caching, security.
- Internet / Web Server: Hosts WML content and applications

* Characteristics
- Designed for low-speed wireless networks (9.6 Kbps typical in early GSM)
- Uses WML (Wireless Markup Language) instead of HTML.
- Uses WTLS for security (Wireless TLS).
- Uses compressed data to improve performance on slow networks
- Works well with limited bandwidth and simple devices

Traditional WAP	Modern Mobile Web
Uses WML pages	Uses HTML5 / CSS / JavaScript
Uses WAP Gateway for conversion	Direct connection via TCP/IP
Designed for small monochrome displays	Rich UI, high resolution screens
Slow, low bandwidth	High-speed 4G / 5G
~~Limited multimedia~~	broadband
Limited multimedia	Full multimedia support

* Thread (based on IEEE 802.15.4)

Thread is a low-power wireless networking protocol designed for IoT ~~(IoT~~ (Internet of Things) devices, especially in smart home systems. It is based on the IEEE 802.15.4 standard which defines the physical and MAC layers for low-rate wireless personal area networks (LR-WPAN).
- Low-power consumption (devices run for years on batteries)
- Mesh networking - devices relay data to extended range

Secure communication using AES-128 encryption.
IP-based (IPv6 support) - enables direct internet compatibility
Self healing - if one device fails, data finds an alternate path.
Used in systems such as Google Nest, Matter standard, Smart Home devices
Applications - Smart home automation, sensors, lighting, thermostats, security systems.

* RTCP (Real-Time Control Protocol)

RTCP stands for Real-Time Control Protocol, used together with RTP (Real-Time Transport Protocol) to manage real-time audio/video streaming.
Monitors quality of service (QoS) for streaming sessions.
Provides feedback such as packet loss, jitter, delay, bandwidth
Supports synchronization between audio and video streams
Identifies session participants
RTCP does not carry actual media data (RTP does)
Sends periodic control packets to report streaming performance
Applications
- Video conferencing (Zoom, Teams, Web Ex)
- Voice over IP (VoIP)
- Live media streaming

* RTSP (Real-Time Streaming Protocol)

RTSP stands for Real-Time Streaming Protocol, used to control the delivery of multimedia streams between a client and media server.

Provides commands similar to video playback controls:

- PLAY: Start streaming
- PAUSE: Temporarily stop
- RECORD: Save media
- TEARDOWN: End Session

★ Features

- Controls real-time media delivery over RTP/RTCP
- Supports both live streaming and on-demand playback
- Uses TCP or UDP
- Enables fast forward, rewind, seek in video streams

★ Applications

- CCTV and IP cameras
- Streaming media servers
- Surveillance systems
- OTT platforms (in some workflows)