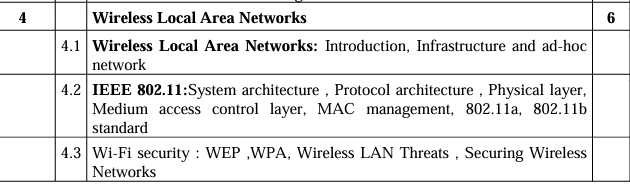
MODULE 4



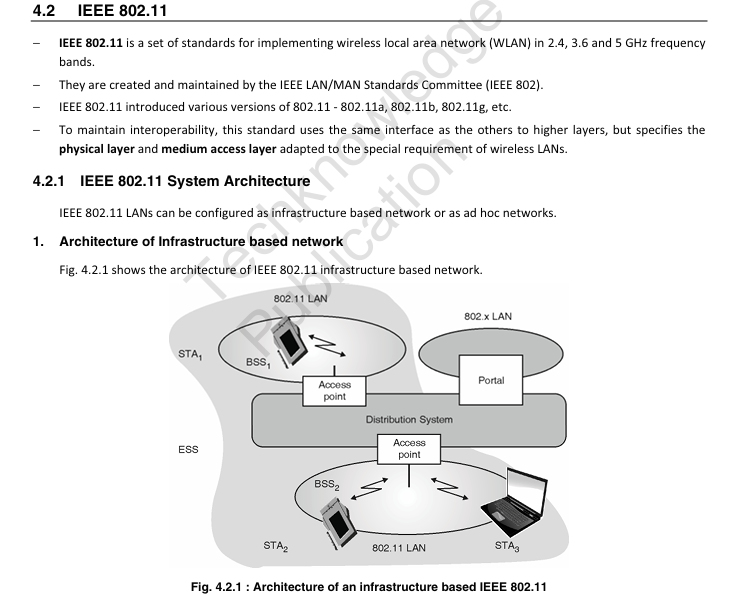


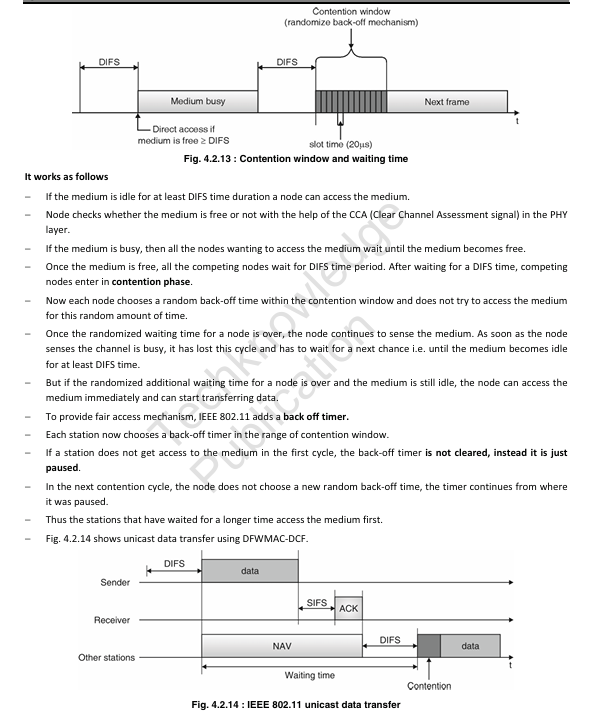
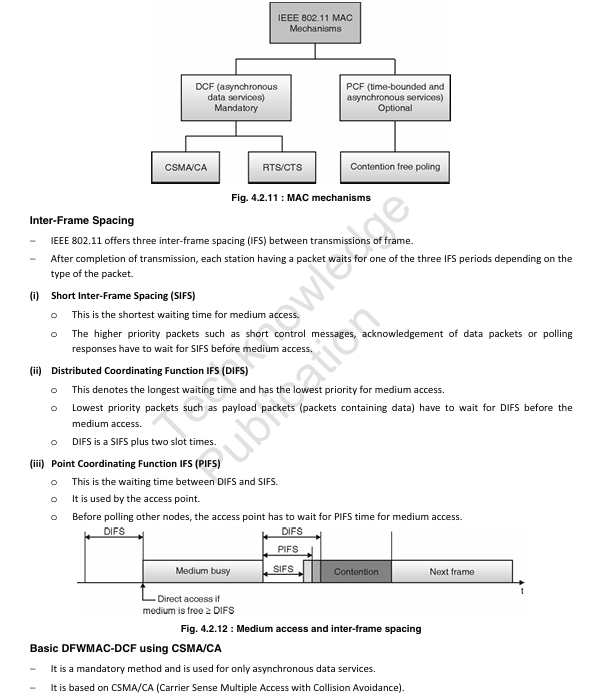
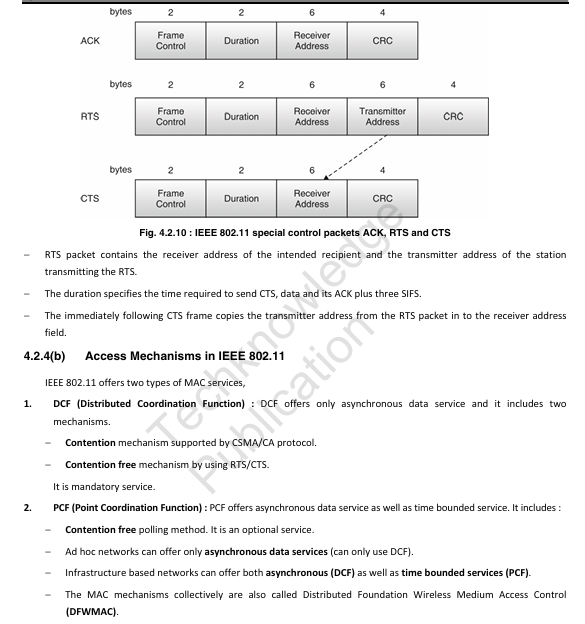
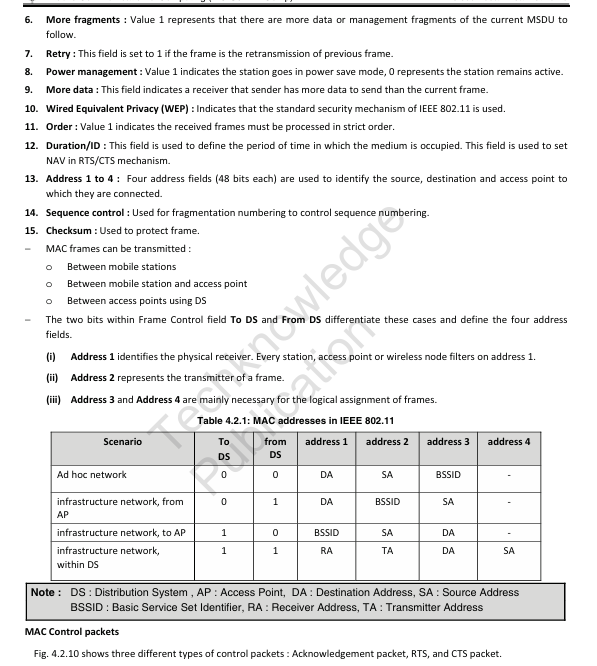
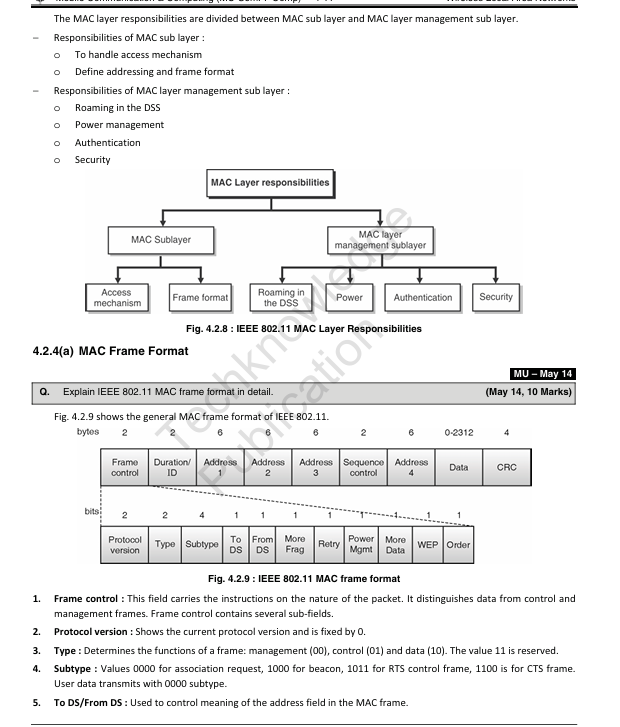
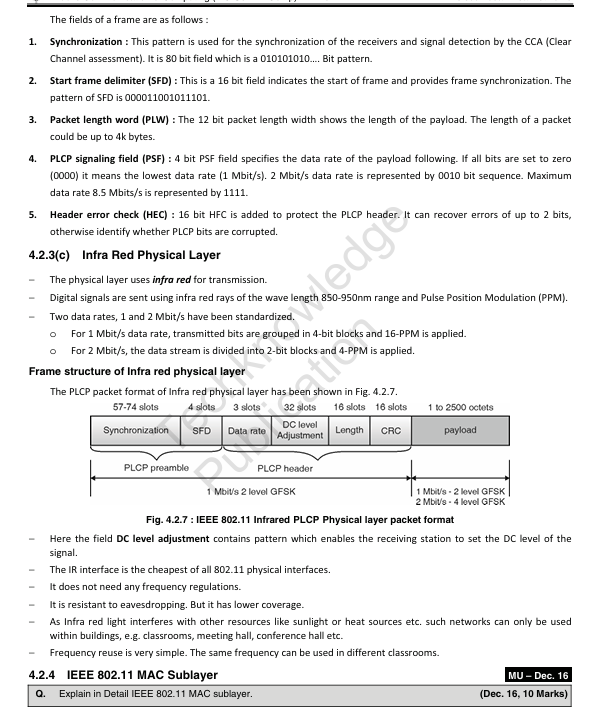
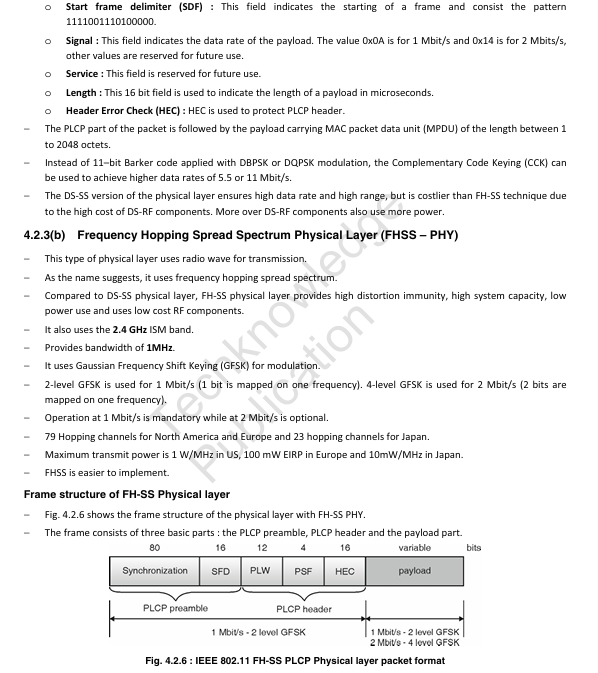
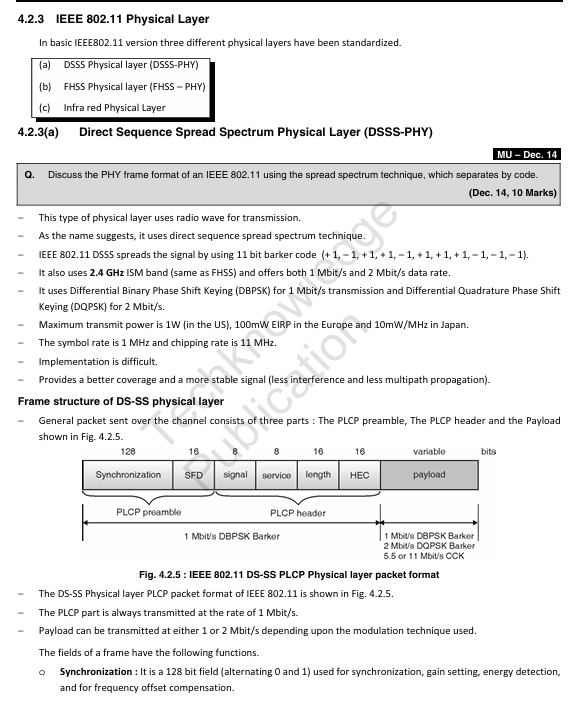
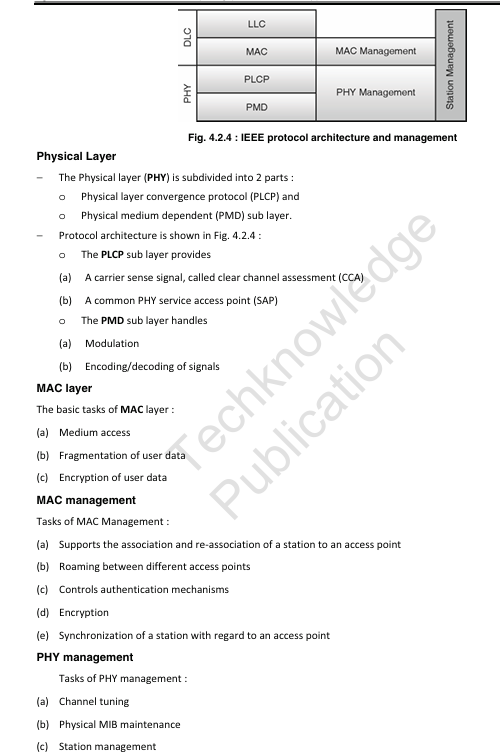
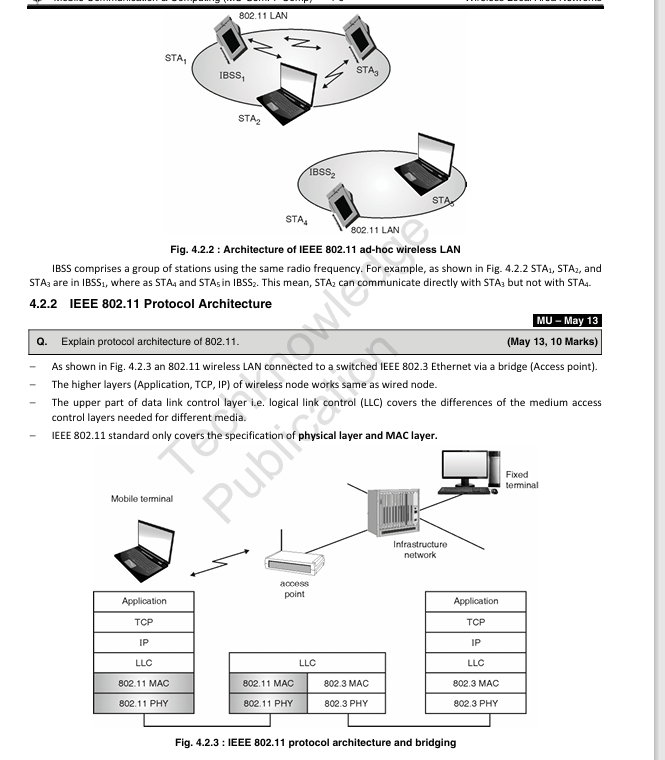
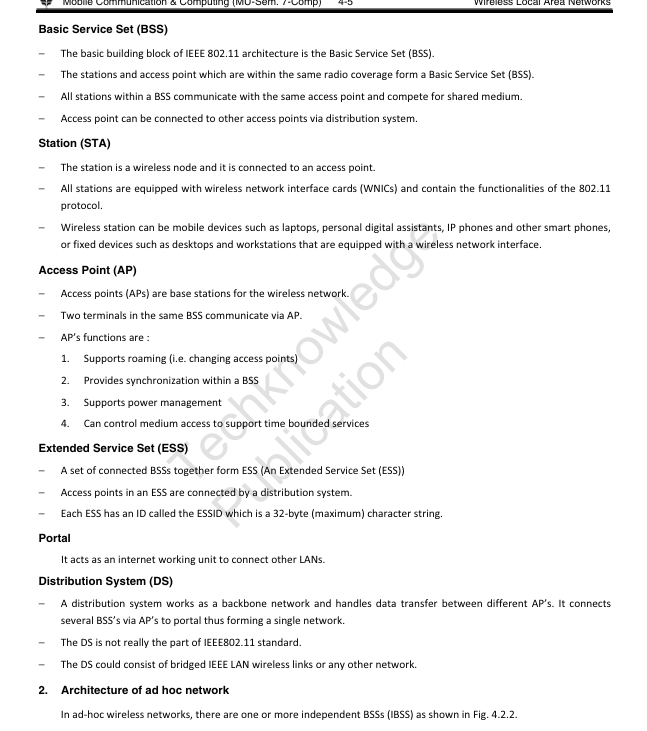
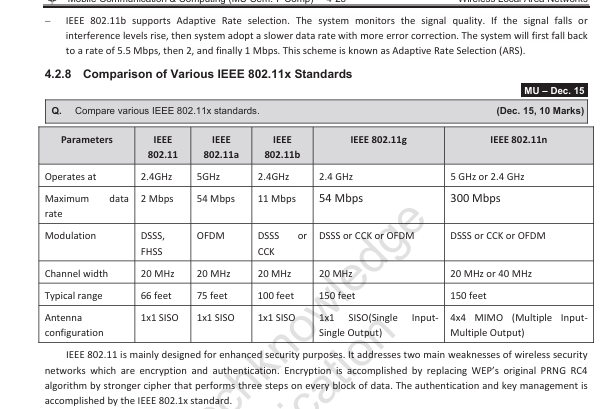
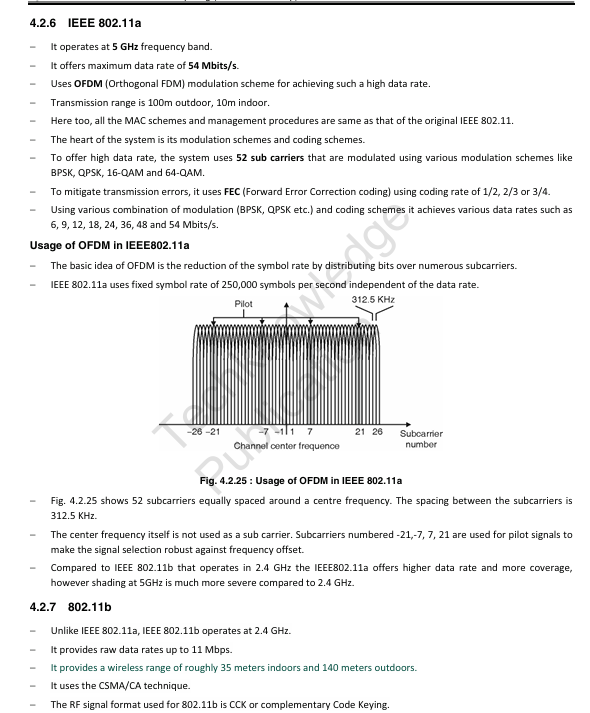
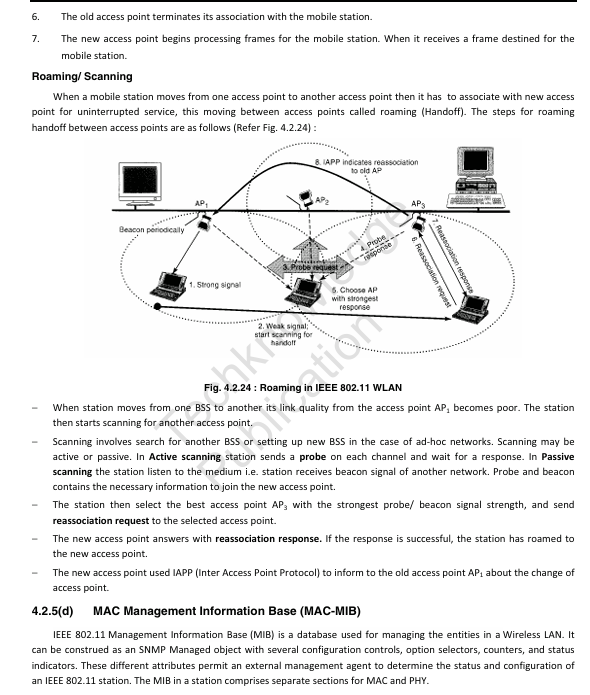
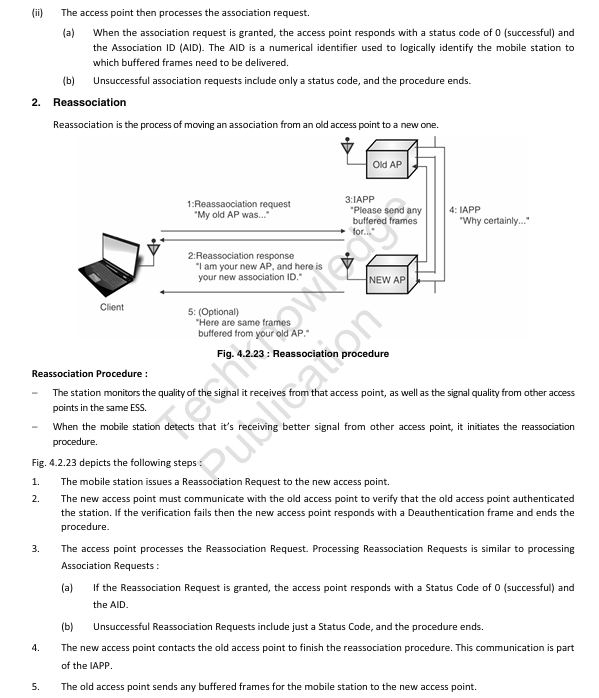
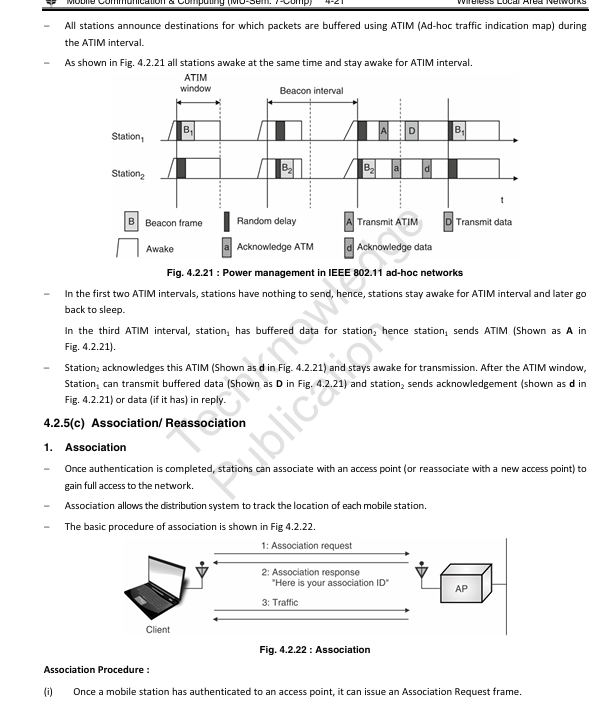
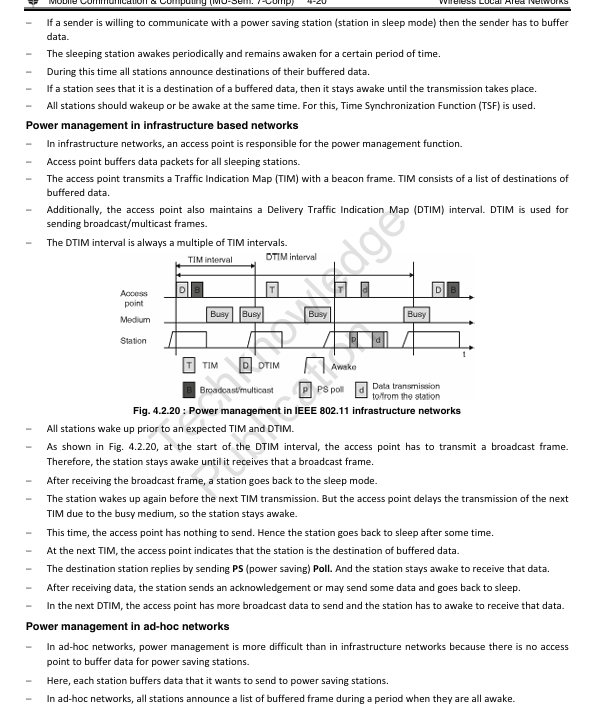
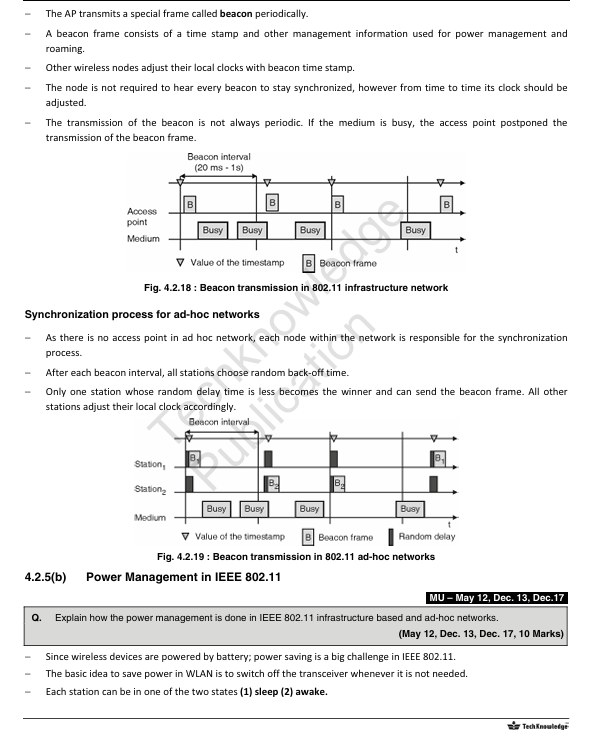
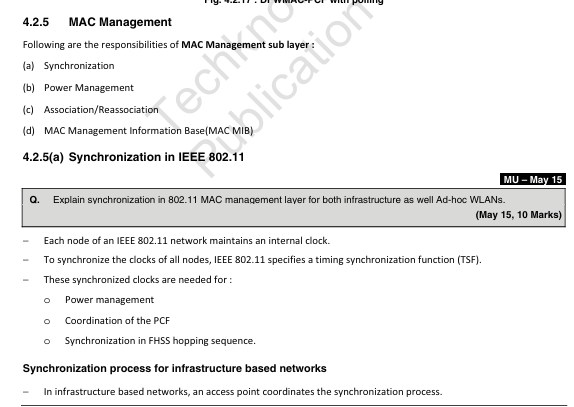
-> WiFi Security – Threats

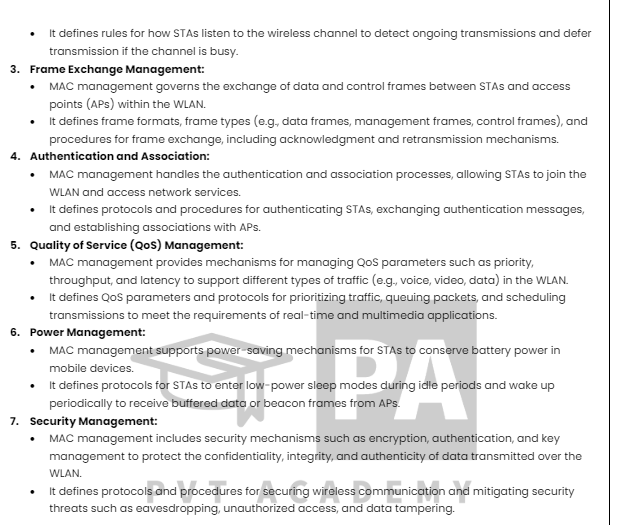
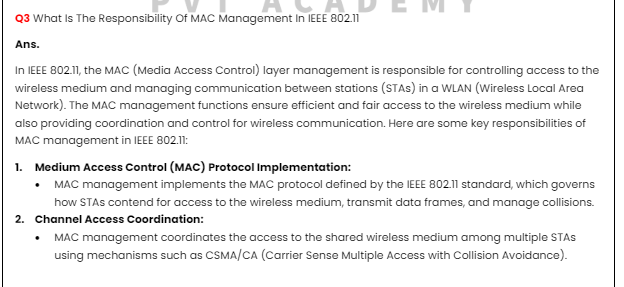
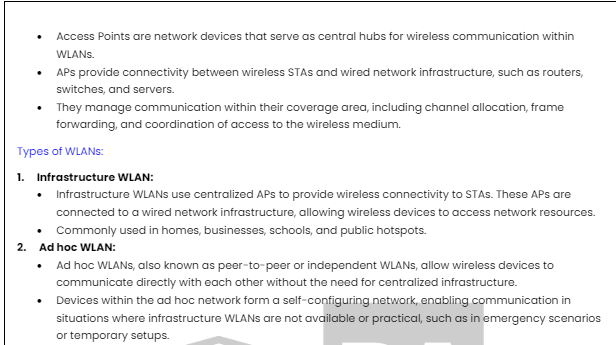
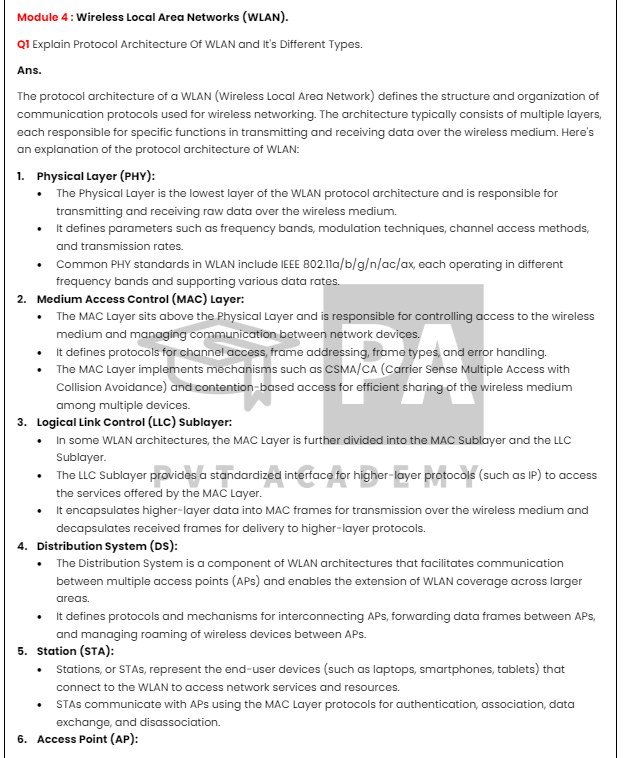
-> IEEE 802.11 Architecture

-> WEP , WPA Protocols

-> Bluetooth Protocol Stack Architecture (Piconet , Scatternet)

Q. Explain Protocol Architecture of WLAN and its different types || Q. Explain protocol architecture of WLAN and its different types – 10M || Q. What is the responsibility of MAC management in IEEE 802.11? || Q. What is responsibility of MAC Management in IEEE 802.11 || Q. Explain protocol architecture of IEEE 802.11 W diagram – 10M x2 

iske baad thodha content is skipped 



Q. Explain Wireless LAN Threats || Q. Explain Wireless LAN threats – 10M || Q. Explain in short wireless LAN security threats – 5M || Q. Explain different security threats in WLAN and discuss the available solutions

**.8 Explain various security threats in WLAN and discuss the available solutions**.

Wireless Local Area Networks (WLANs) are susceptible to various security threats due to their inherent characteristics, such as shared medium, broadcast nature, and lack of physical boundaries. Here are some common security threats in WLANs along with available solutions:

1. \*\*Eavesdropping\*\*:

- \*\*Threat\*\*: Attackers can intercept wireless communications between devices, leading to unauthorized access to sensitive information such as passwords, financial data, or confidential business information.

- \*\*Solution\*\*:

- Encryption protocols such as WPA2 (Wi-Fi Protected Access 2) or WPA3 provide encryption for data transmitted over the WLAN, preventing eavesdroppers from deciphering intercepted traffic.

- Use of Virtual Private Networks (VPNs) for securing data traffic between endpoints, especially when accessing sensitive information over public Wi-Fi networks.

2. \*\*Unauthorized Access (Wi-Fi Hacking)\*\*:

- \*\*Threat\*\*: Attackers can gain unauthorized access to WLANs by exploiting vulnerabilities in network protocols or using brute force attacks to crack weak passwords.

- \*\*Solution\*\*:

- Implement strong authentication mechanisms such as WPA2-Enterprise or WPA3-Enterprise, which use protocols like Extensible Authentication Protocol (EAP) for secure authentication.

- Regularly update WLAN access points with the latest firmware patches to address known vulnerabilities and security flaws.

- Enforce the use of strong, complex passwords or passphrase for WLAN access, and periodically update them.

3. \*\*Rogue Access Points\*\*:

- \*\*Threat\*\*: Unauthorized access points deployed by attackers within the vicinity of the WLAN can trick devices into connecting to them, leading to potential data interception or manipulation.

- \*\*Solution\*\*:

- Use wireless intrusion detection systems (WIDS) or wireless intrusion prevention systems (WIPS) to detect and mitigate rogue access points automatically.

- Implement strict access control policies and regularly scan the network environment for unauthorized devices or access points.

4. \*\*Denial of Service (DoS) Attacks\*\*:

- \*\*Threat\*\*: Attackers can flood the WLAN with excessive traffic or deauthenticate legitimate users, causing disruptions in service and denying access to authorized users.

- \*\*Solution\*\*:

- Deploy network-based intrusion detection and prevention systems (NIDS/NIPS) to detect and block malicious traffic targeting the WLAN.

- Enable features such as MAC address filtering and rate limiting on WLAN access points to mitigate the impact of DoS attacks.

- Implement network segmentation and isolation to minimize the impact of attacks on critical resources.

5. \*\*Man-in-the-Middle (MitM) Attacks\*\*:

- \*\*Threat\*\*: Attackers intercept and alter communication between devices in the WLAN, allowing them to eavesdrop on sensitive information or inject malicious payloads into the data stream.

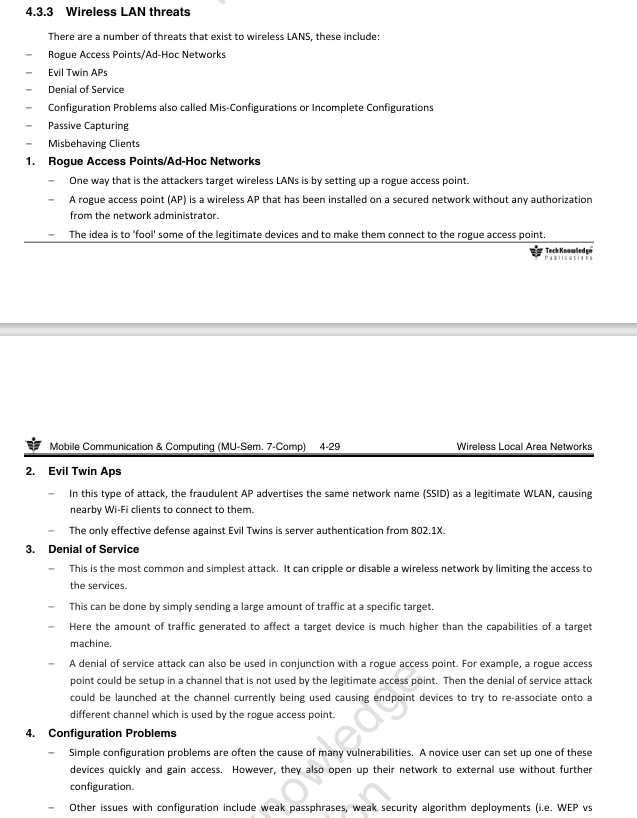
- \*\*Solution\*\*:

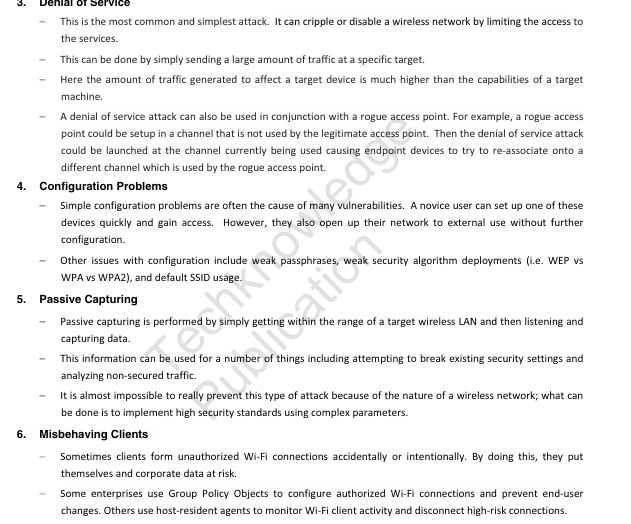
- Use encryption protocols such as Transport Layer Security (TLS) for securing communication between endpoints, especially for web-based applications and services.

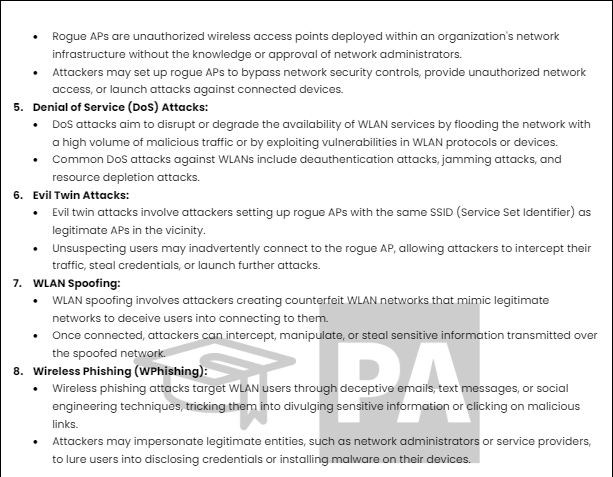
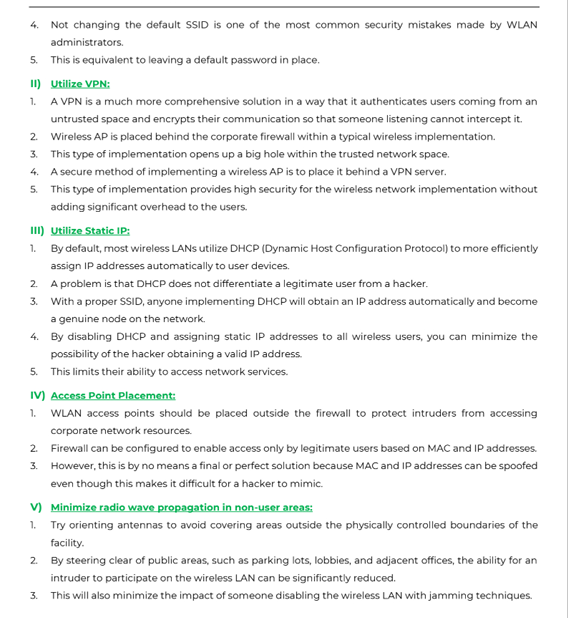
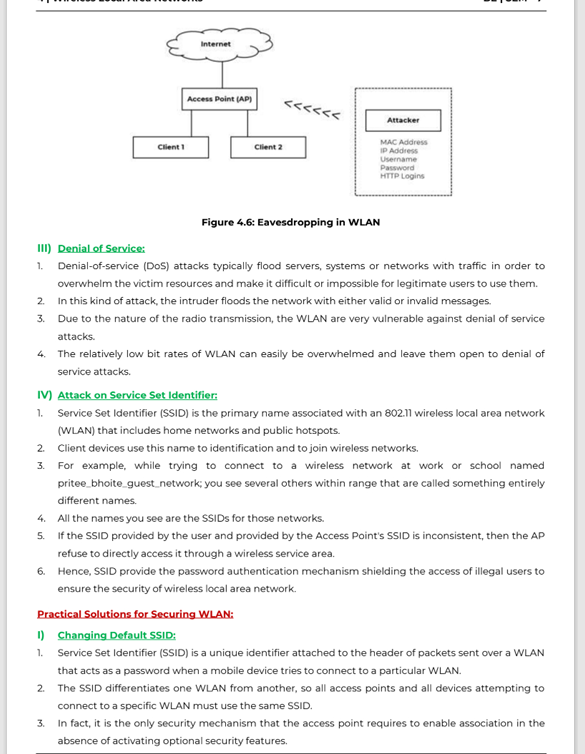
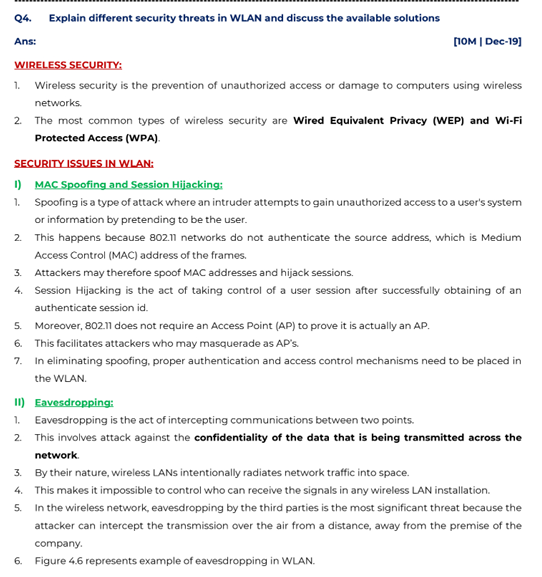
- Implement techniques like certificate-based authentication to verify the identity of communicating parties and detect potential MitM attacks.

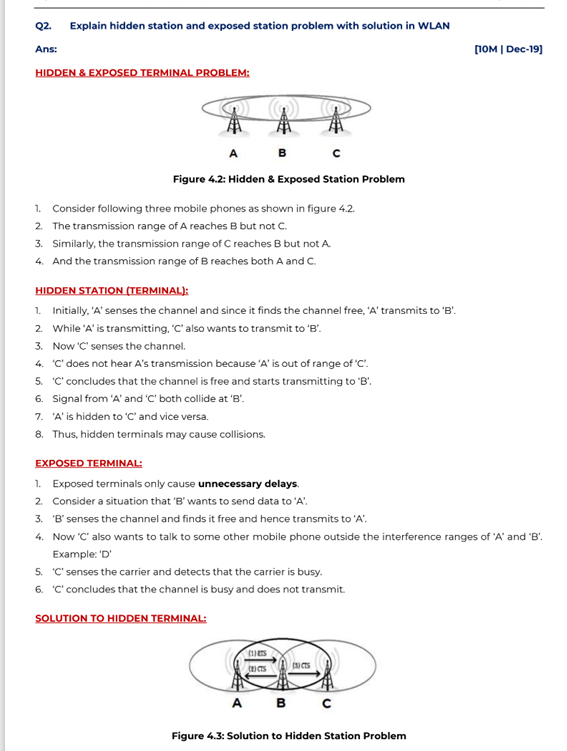
- Educate users about the risks of connecting to untrusted networks and encourage the use of VPNs or secure communication channels when accessing sensitive information.

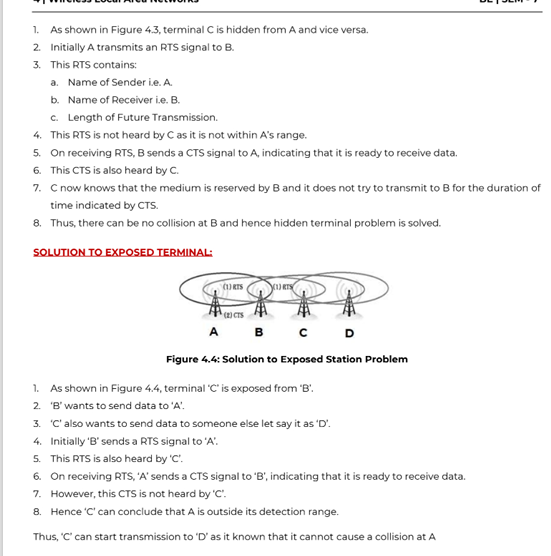
By implementing a combination of these security measures, WLAN administrators can mitigate the risks posed by various security threats and ensure the confidentiality, integrity, and availability of their wireless networks. Regular security audits and updates to security policies are essential to adapt to evolving threats and maintain a robust security posture.

****

****



Q. Explain hidden station and exposed station problem with solution in WLAN.-10M x2 



In wireless local area networks (WLANs), the hidden station and exposed station problems are significant issues that can affect the efficiency and performance of the network. These problems arise due to the nature of wireless communication, where signals are broadcast over the air and can interfere with each other.

### Hidden Station Problem

\*\*Scenario\*\*:

- In a WLAN, consider three stations: A, B, and C.

- Station A can communicate with Station B, and Station B can communicate with Station C.

- However, Station A cannot communicate directly with Station C due to the distance or obstacles in the environment.

\*\*Problem\*\*:

- When Station A wants to send data to Station B, it listens to the channel to check if it is free (using a method like Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA).

- If Station C is already transmitting to Station B, Station A will not detect Station C's transmission because it is out of range (hidden), and it may start transmitting as well.

- This simultaneous transmission from A and C causes a collision at Station B, leading to data loss and the need for retransmission, thereby reducing network efficiency.

### Exposed Station Problem

\*\*Scenario\*\*:

- In a WLAN, consider four stations: A, B, C, and D.

- Station A can communicate with Station B, and Station C can communicate with Station D.

- Station B can hear transmissions from Station A, and Station C can hear transmissions from Station D.

\*\*Problem\*\*:

- When Station B is transmitting data to Station A, Station C senses the channel and finds it busy (because it can hear Station B's transmission).

- Although Station C wants to transmit data to Station D, it refrains from doing so to avoid collision, even though Station D is out of the interference range of Station A.

- This leads to underutilization of the network because Station C unnecessarily defers its transmission.

### Solutions

#### 1. RTS/CTS Mechanism

The Request to Send/Clear to Send (RTS/CTS) mechanism is a solution implemented in WLANs to address both hidden and exposed station problems.

\*\*How RTS/CTS Works\*\*:

- \*\*RTS\*\*: When a station (e.g., A) wants to transmit data, it first sends an RTS packet to the intended recipient (e.g., B).

- \*\*CTS\*\*: Upon receiving the RTS, the recipient station (B) responds with a CTS packet.

- Both RTS and CTS packets contain information about the duration of the intended transmission.

\*\*Handling Hidden Stations\*\*:

- Stations near the sender (A) and receiver (B) that hear the RTS and CTS packets will refrain from transmitting for the specified duration.

- This helps prevent collisions caused by hidden stations (e.g., C), as they will wait until the transmission between A and B is complete.

\*\*Handling Exposed Stations\*\*:

- Stations that hear the RTS but not the CTS (or vice versa) can determine that they are not in the range of the actual data transmission.

- For example, if Station C hears the RTS from A but not the CTS from B, it can infer that it is outside the interference range and may proceed with its transmission to another station (e.g., D).

#### 2. Network Allocation Vector (NAV)

\*\*NAV\*\* is a timer mechanism used in conjunction with the RTS/CTS protocol.

\*\*How NAV Works\*\*:

- Stations update their NAV based on the duration information in RTS, CTS, or other control frames.

- The NAV timer indicates how long the channel will be occupied.

- Stations defer their transmissions until the NAV timer expires, avoiding collisions during ongoing transmissions.

### Conclusion

The hidden and exposed station problems are critical issues in WLANs that can lead to collisions and inefficient use of the network. Solutions like the RTS/CTS mechanism and NAV help mitigate these problems by coordinating access to the shared wireless medium. These techniques improve overall network performance by reducing collisions and ensuring more efficient use of the available bandwidth.

Q. Explain DSDV routing protocol used in ad hoc network – 10M

The Destination-Sequenced Distance-Vector (DSDV) routing protocol is a table-driven routing scheme for ad hoc mobile networks. It is an enhancement of the traditional Bellman-Ford routing algorithm with the aim of preventing routing loops and ensuring efficient routing by incorporating sequence numbers.

### Key Features of DSDV

1. \*\*Proactive Routing\*\*:

- DSDV is a proactive (or table-driven) routing protocol, meaning that it maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network.

2. \*\*Sequence Numbers\*\*:

- To avoid routing loops and ensure the freshness of routing information, each route entry is tagged with a sequence number. These sequence numbers are generally even if a link is present; otherwise, an odd number is used.

3. \*\*Periodic Updates\*\*:

- DSDV regularly updates the routing tables with periodic broadcasts of the routing information. These updates ensure that all nodes have consistent and up-to-date routing information.

4. \*\*Triggered Updates\*\*:

- In addition to periodic updates, triggered updates are used when significant network topology changes occur, such as the movement of nodes. Triggered updates help in quickly propagating the new information to maintain accurate routes.

### How DSDV Works

#### Routing Table

Each node in the network maintains a routing table. The routing table entries consist of:

- \*\*Destination Address\*\*: The IP address of the destination node.

- \*\*Next Hop\*\*: The IP address of the next hop node to reach the destination.

- \*\*Hop Count\*\*: The number of hops to reach the destination.

- \*\*Sequence Number\*\*: The sequence number assigned by the destination node, indicating the freshness of the route.

#### Periodic Updates

- \*\*Full Dump\*\*: Occasionally, a node will send the entire routing table to its neighbors. This is a full dump and contains all available routing information.

- \*\*Incremental Update\*\*: Between full dumps, nodes send incremental updates that contain only changes since the last full dump. This reduces the overhead.

#### Triggered Updates

- When a node detects a significant topology change, such as a new node joining the network or an existing node moving out of range, it immediately broadcasts a triggered update. This helps quickly propagate the new routing information.

### Example Scenario

1. \*\*Initialization\*\*:

- Each node starts by broadcasting a route advertisement packet with its own address and a sequence number.

2. \*\*Route Discovery\*\*:

- Nodes update their routing tables upon receiving route advertisements, choosing the route with the highest sequence number (i.e., the freshest route).

- If the sequence numbers are equal, the route with the lower hop count is preferred.

3. \*\*Maintaining Consistency\*\*:

- Nodes periodically broadcast their routing tables to keep the network consistent.

- If a node receives a route advertisement with a higher sequence number than its current entry, it updates its routing table.

### Advantages of DSDV

- \*\*Loop-Free Routing\*\*: Sequence numbers ensure that routes are loop-free and always contain the most recent path information.

- \*\*Proactive Maintenance\*\*: Regular updates help maintain consistent and accurate routing information across the network.

### Disadvantages of DSDV

- \*\*Overhead\*\*: Frequent updates, especially in large networks, can lead to significant overhead in terms of bandwidth consumption and power usage.

- \*\*Scalability\*\*: The protocol may not scale well to very large networks due to the overhead of maintaining up-to-date routing tables.

### Conclusion

DSDV is a proactive routing protocol suitable for small to medium-sized ad hoc networks where maintaining consistent and loop-free routing information is crucial. By leveraging sequence numbers and periodic updates, DSDV provides reliable and efficient route discovery and maintenance, though it may face challenges with scalability and overhead in larger networks.

Q. HIPERLAN – SHORT NOTE

### HIPERLAN: A Short Note

HIPERLAN (High Performance Radio Local Area Network) is a set of wireless communication standards developed by the European Telecommunications Standards Institute (ETSI) for high-speed wireless local area networks (WLANs). The HIPERLAN family includes multiple standards, with HIPERLAN/1 and HIPERLAN/2 being the most notable. These standards were designed to provide high data rates and robust performance, catering to both data and multimedia applications.

### HIPERLAN/1

#### Overview

- \*\*Standard\*\*: ETSI standard ETS 300 652.

- \*\*Data Rates\*\*: Supports data rates up to 23.5 Mbps.

- \*\*Frequency Band\*\*: Operates in the 5 GHz frequency band.

- \*\*Access Method\*\*: Uses a contention-based channel access method known as Elimination-Yield Non-preemptive Priority Multiple Access (EY-NPMA).

#### Key Features

- \*\*QoS Support\*\*: Provides support for Quality of Service (QoS) with priorities for different types of traffic.

- \*\*Mobility\*\*: Designed for mobile users, allowing seamless handovers between different access points.

- \*\*Power Management\*\*: Includes mechanisms for efficient power management to extend the battery life of mobile devices.

### HIPERLAN/2

#### Overview

- \*\*Standard\*\*: ETSI standard ETS 101 683.

- \*\*Data Rates\*\*: Supports data rates up to 54 Mbps.

- \*\*Frequency Band\*\*: Also operates in the 5 GHz frequency band.

- \*\*Access Method\*\*: Uses a time-division multiple access (TDMA) and dynamic time-division duplex (TDD) scheme.

#### Key Features

- \*\*QoS and Traffic Classes\*\*: Provides robust QoS support with traffic classes for different types of services such as voice, video, and data.

- \*\*Interoperability\*\*: Designed to interoperate with various network types, including Ethernet, ATM, and IP networks.

- \*\*Security\*\*: Implements strong security measures, including encryption and authentication, to ensure secure communication.

- \*\*Flexibility\*\*: Supports both ad-hoc and infrastructure modes, making it versatile for different deployment scenarios.

### Comparison with Other WLAN Standards

- \*\*IEEE 802.11\*\*: While HIPERLAN/1 and HIPERLAN/2 were European alternatives to the IEEE 802.11 standards, they did not achieve the same widespread adoption. IEEE 802.11 (Wi-Fi) became the dominant WLAN standard globally.

- \*\*Frequency Use\*\*: Both HIPERLAN standards use the 5 GHz band, similar to IEEE 802.11a, which allows for higher data rates but typically shorter range compared to 2.4 GHz used by IEEE 802.11b/g/n.

### Applications

- \*\*HIPERLAN/1\*\*: Targeted applications included mobile computing, multimedia communications, and wireless LANs in office and industrial environments.

- \*\*HIPERLAN/2\*\*: Focused on providing high-speed connectivity for applications such as video conferencing, real-time data transfer, and broadband internet access.

### Conclusion

HIPERLAN standards, particularly HIPERLAN/1 and HIPERLAN/2, were significant steps in the evolution of high-speed wireless networking, offering advanced features like QoS, robust security, and interoperability. Despite their technological strengths, they were eventually overshadowed by the IEEE 802.11 standards, which gained broader industry support and adoption. Nonetheless, HIPERLAN contributed to the development of wireless networking technologies and set the stage for future advancements in high-speed WLANs.

PENDING MOD 