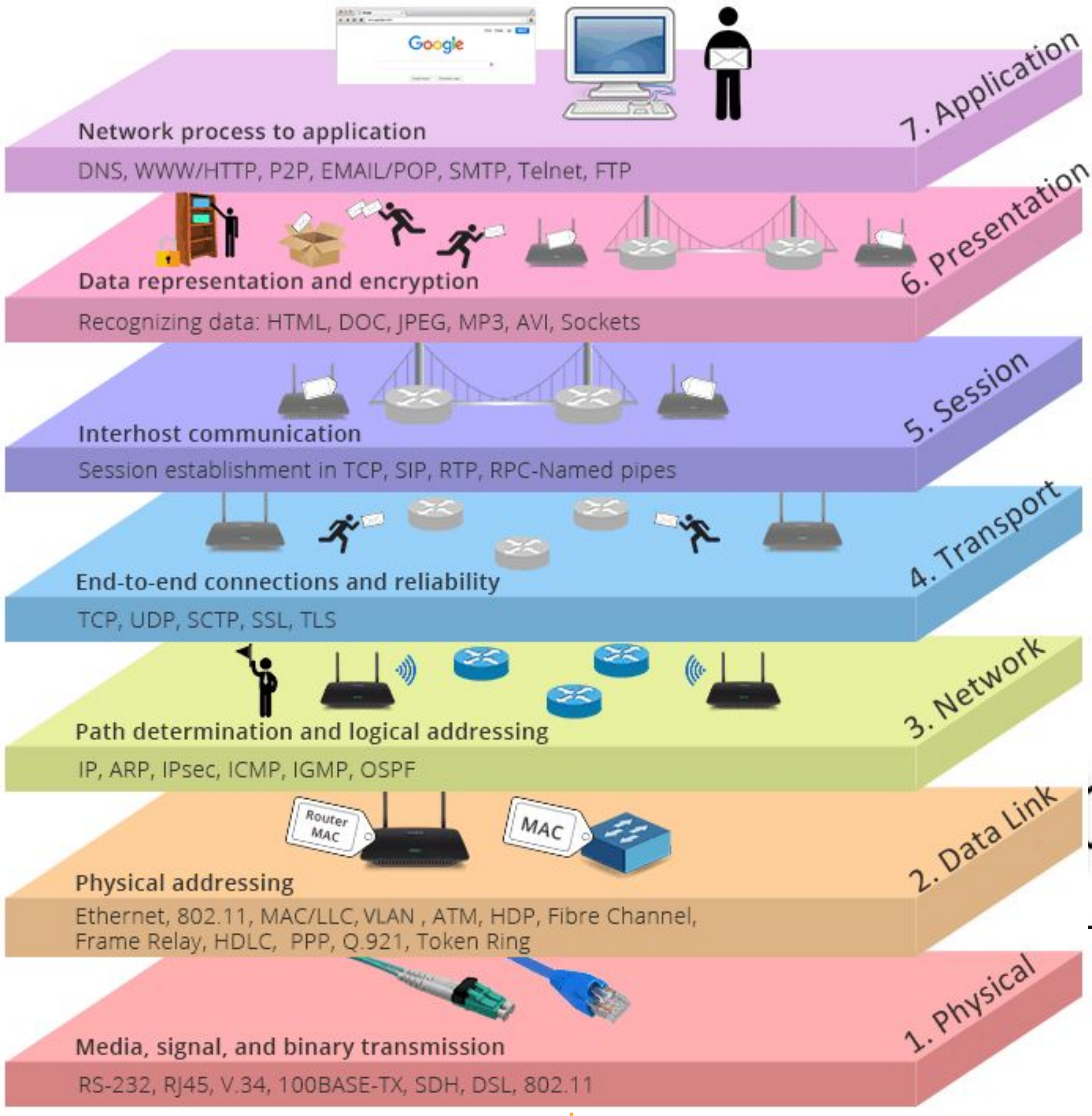
# Unit 4

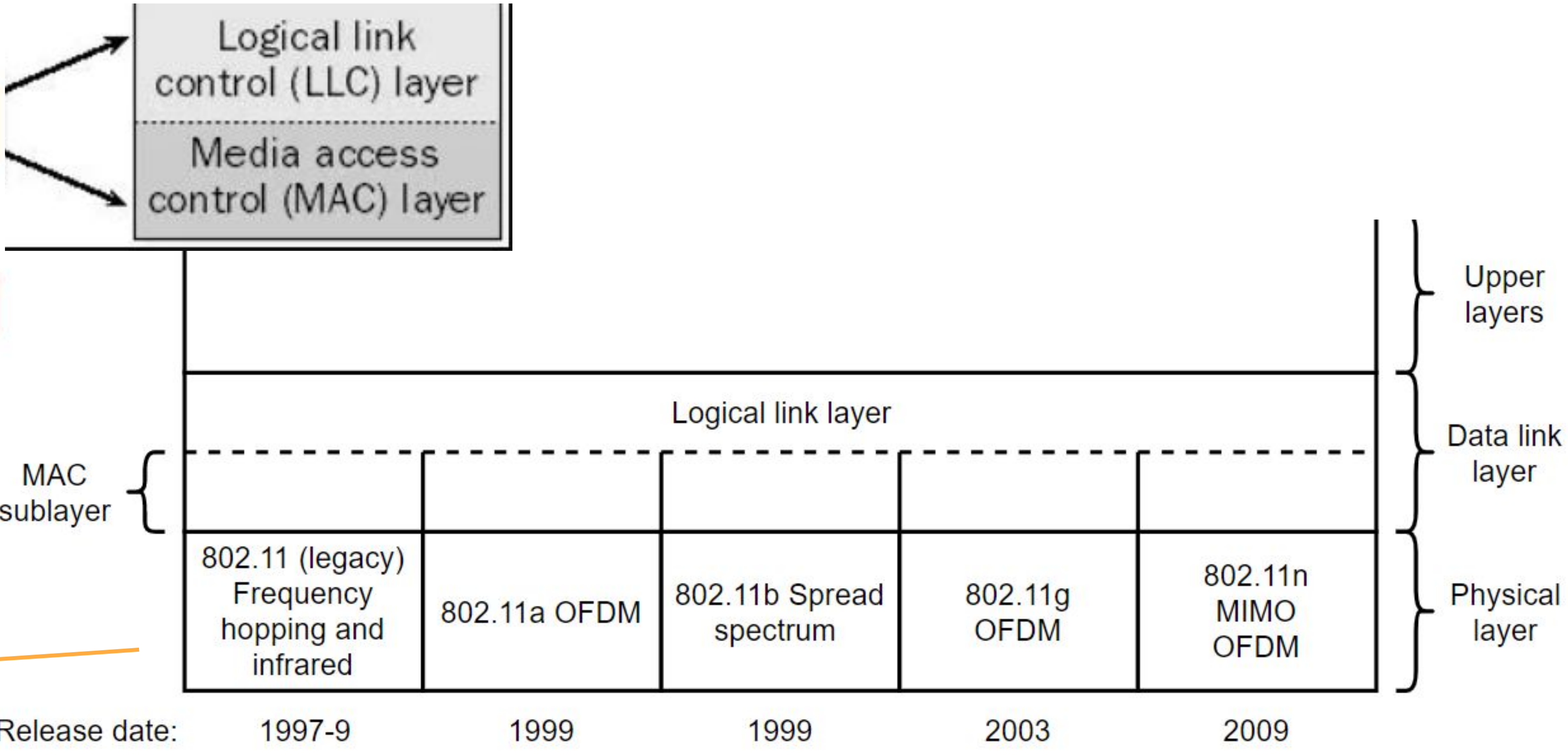
## Wireless Network Security

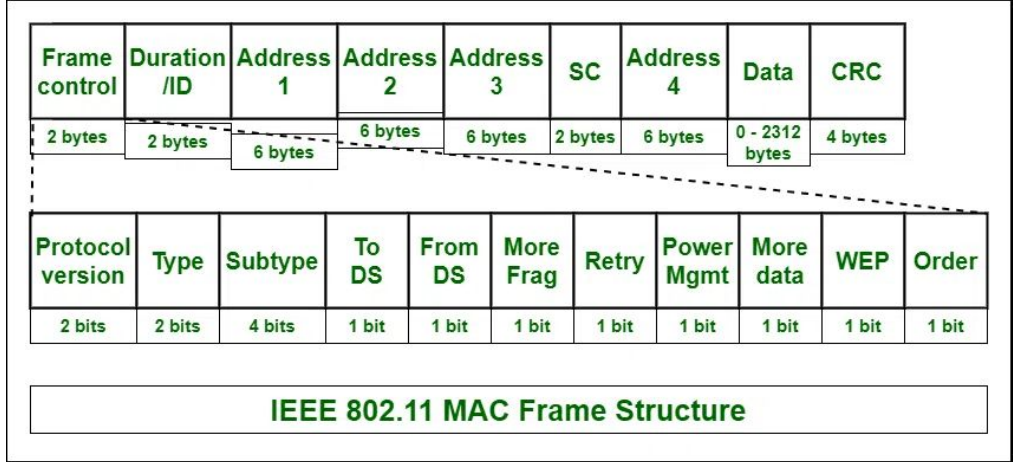
# Wireless Network Security: Best Practices and Protocols

Explore the essential 802.11 protocols, authentication methods, and encryption standards that form the foundation of robust wireless network security. Dive into the vulnerabilities, attacks, and countermeasures to safeguard your wireless infrastructure.

IEEE 802.11 is a set of protocols and standards for executing WLAN (wireless local area network) computer communication in the 5, 3.6, and 2.4 GHz frequency bands.
They're made and maintained by the IEEE 802 or the IEEE LAN/MAN Standards Committee. IEEE 802.11-2007 is the latest base version of this standard. What's more, the 802.11 family is composed of a volume of airborne modulation methods that utilize identical and basic protocol.
The most ubiquitous and widely used versions of this standard are the 802.11g and 802.11b protocols, which were improvements to the earliest standard.
Meanwhile, the first wireless networking standard is the aforementioned 802.11-1997 as well. Regardless the most widely accepted one was the 802.11b, which was then followed by 802.11g and 802.11n.


7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11





| Frame control | Duration /ID | Address 1 | Address 2 | Address 3 | SC | Address 4 | Data | CRC |
|---|---|---|---|---|---|---|---|---|
| 2 bytes | 2 bytes | 6 bytes | 6 bytes | 6 bytes | 2 bytes | 6 bytes | 0 - 2312 bytes | 4 bytes |

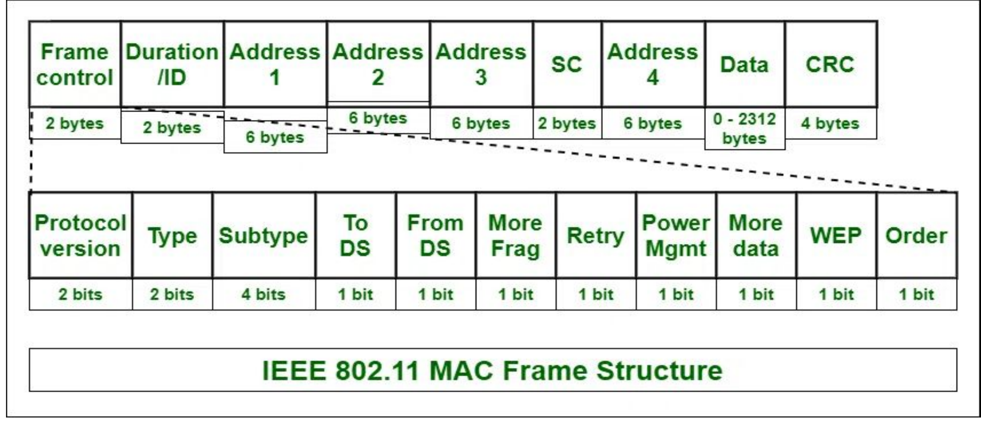
| Protocol version | Type | Subtype | To DS | From DS | More Frag | Retry | Power Mgmt | More data | WEP | Order |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 bits | 2 bits | 4 bits | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit |

IEEE 802.11 MAC Frame Structure

## Frame Control

It is 2 bytes long and defines type of frame and control information.

- **Version: Indicates the current protocol version.**
- **Type**: Determines the function of frame i.e. management(00), control(01) or data(10).
- **Subtype**: Indicates subtype of frame like 0000 for association request, 1000 for beacon.
- **To DS**: When set indicates that the destination frame is for DS(distribution system).
- **From DS:** When set indicates frame coming from DS.
- **More frag (More fragments)**: When set to 1 means frame is followed by other fragments.
- **Retry: I**f the current frame is a re-transmission of an earlier frame, this bit is set to 1.
- **Power Mgmt (Power Management):** It indicates the mode of a station after successful transmission of a frame. Set to '1' field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
- **More data:** It is used to indicate to the receiver that a sender has more data to send than the current frame.
- **WEP**: It indicates that the standard security mechanism of 802.11 is applied.
- **Order:** If this bit is set to 1 the received frames must be processed in strict order.



| Frame control | Duration /ID | Address 1 | Address 2 | Address 3 | SC | Address 4 | Data | CRC |
|---|---|---|---|---|---|---|---|---|
| 2 bytes | 2 bytes | 6 bytes | 6 bytes | 6 bytes | 2 bytes | 6 bytes | 0 - 2312 bytes | 4 bytes |

| Protocol version | Type | Subtype | To DS | From DS | More Frag | Retry | Power Mgmt | More data | WEP | Order |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 bits | 2 bits | 4 bits | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit | 1 bit |

IEEE 802.11 MAC Frame Structure

## Duration / ID

It contains the value indicating the period of time in which the medium is occupied (in µs).

## Address 1 to 4

These fields contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address is defined by DS bits in the frame control field.

## SC (Sequence Control)

It consists of 2 sub-fields i.e. sequence number (12 bits) and fragment number (4 bits). Sequence number is used to filter duplicate frames.

## Data

It is a variable length field which contains information specific to individual frames which is transferred transparently from a sender to the receiver.

## CRC (Cyclic Redundancy Check)

It contains 32 bit CRC error detection sequence to ensure error free frame.

## IEEE 802.11 –

1. It was developed in 1997.
2. Speed is about 2 Mbps (2 megabits per second)

# 802.11 Protocols

- Wi-Fi stands for Wireless Fidelity, and it is developed by an organization called IEEE (Institute of Electrical and Electronics Engineers) they set standards for the Wi-Fi system.
- Each Wi-Fi network standard has two parameters :
  - **Speed** – This is the data transfer rate of the network measured in Mbps (1 megabit per second).
  - **Frequency** – On what radio frequency, the network is carried on. Two bands of frequency for Wi-Fi are 2.4 GHz and 5 GHz. In short, it is the frequency of radio wave that carries data.

| **Version** | **Introduced in** | **Frequency band used** | **Maximum speed provided** |
|---|---|---|---|
| IEEE 802.11a | 1999 | 5 GHz | 54 Mbps |
| IEEE 802.11b | 1999 | 2.4 GHz | 11 Mbps |
| IEEE 802.11g | 2003 | 2.4 GHz | 54 Mbps |
| IEEE 802.11n | 2009 | Both 2.4 GHz and 5 GHz | 600 Mbps |
| IEEE 802.11ac | 2013 | 5 GHz | 1.3 Gbps |
| IEEE 802.11ax | 2019 | Both 2.4 GHz and 5 GHz | Up to 10 Gbps |

# WAP Security issues

- Wireless access points are easy to install. As a result, many individuals within companies have taken it upon themselves to set up an authorized access point, without informing the network administrator. Typically, these access points are not protected, which means they can be used by an attacker just as they can by a valid user.
- Rogue access points can also be used to lure valid users away from their corporate network. If an attacker can set up an access point with a stronger signal than the valid one, the target's computer automatically connects to the attacker's AP.
- When a computer connects to an access point, it generally stores the details of that connection locally. The next time the computer is turned on, the wireless network card immediately looks for the connection and re-establishes the connection – without user intervention.

# WLAN Authentication and Encryption

WLAN Encryption Methods

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access 2 (WPA2)

# Wired Equivalent Privacy (WEP)

**Features of WEP**

- WEP was introduced as a part of the IEEE 802.11 standard in 1997.
- It was available for 802.11a and 802.11b devices.
- WEP uses encryption of data to make it unrecognizable to eavesdroppers.
- It uses RC4, a stream cipher, for encryption and CRC-32 checksum for confidentiality and integrity
- The two widely used standards were WEP-40 and WEP-104.
- In WEP-40, a 40 bit WEP key is concatenated with a 24 bit initialization vector, to generate a 64 bit RC4 key.
- In WEP-104, a 104 bit WEP key is concatenated with the 24 bit initialization vector, to generate a 128 bit RC4 key.
- WEP operates at the data link and physical layer.
- It incorporates two authentication methods:
  - Open System authentication
  - Shared Key authentication

# Wi-Fi Protected Access (WPA)

- WPA was initially released in 2003. The Wi-Fi Alliance defined WPA as a response to serious weaknesses found in the WEP protocol.
- New updates and features of WPA3 include:
- 256-bit Galois/Counter Mode Protocol encryption (GCMP-256);
- 384-bit Hashed Message Authentication Mode (HMAC);
- 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256);
- an equivalent 192-bit cryptographic strength (in WPA3-EAP enterprise mode);

# Difference between WEP and WPA

| WEP | WPA |
|---|---|
| WEP stands for Wired Equivalent Privacy. | WPA stands for Wi-Fi Protected Access. |
| It is a security protocol for wireless networks which provides data confidentiality comparable to a traditional wired network. | It is a security protocol which is used in securing wireless networks and designed to replace the WEP protocol. |
| Wired Equivalent Privacy (WEP) was introduced in 1999 means before WPA. | Wi-Fi Protected Access (WPA) was developed by the Wi-Fi Alliance in 2003 means after WEP. |
| It provides wireless security through the use of an encryption key. | It provides wireless security through the use of a password. |
| Data Privacy (Encryption) method is Rivest Cipher 4 (RC4). | Data Privacy (Encryption) method is Rivest Cipher 4 (RC4) and Temporal Key Integrity Protocol (TKIP). |
| Authentication method in WEP is Open system authentication or shared key authentication. | Authentication method in WPA is WPA-PSK and WPA-Enterprise. |
| Data integrity is provided through CRC 32. | Data integrity is provided through Message integrity code. |
| It uses 40 bit key and 24 bit random number. | WPA key is 256 bit key. |
| Key management is not provided in WEP. | Key management is provided through 4 way handshaking mechanism. |
| In WEP no protection against reply attacks. | In WPA sequence counter is implemented for reply protection. |
| It is possible to deploy on current hardware infrastructure. | It is possible to deploy on both previous and current hardware infrastructure. |

## What is WPA2?

WPA2 has been a pivotal aspect of Wi-Fi security for many years, offering strong encryption and authentication methods to protect wireless networks. It relies on the Advanced Encryption Standard (AES) for secure data transmission and utilizes a specific handshake process to establish trusted connections between devices and access points. Despite its effectiveness, WPA2 has experienced vulnerabilities such as the KRACK exploit, highlighting the necessity for a more resilient security protocol.

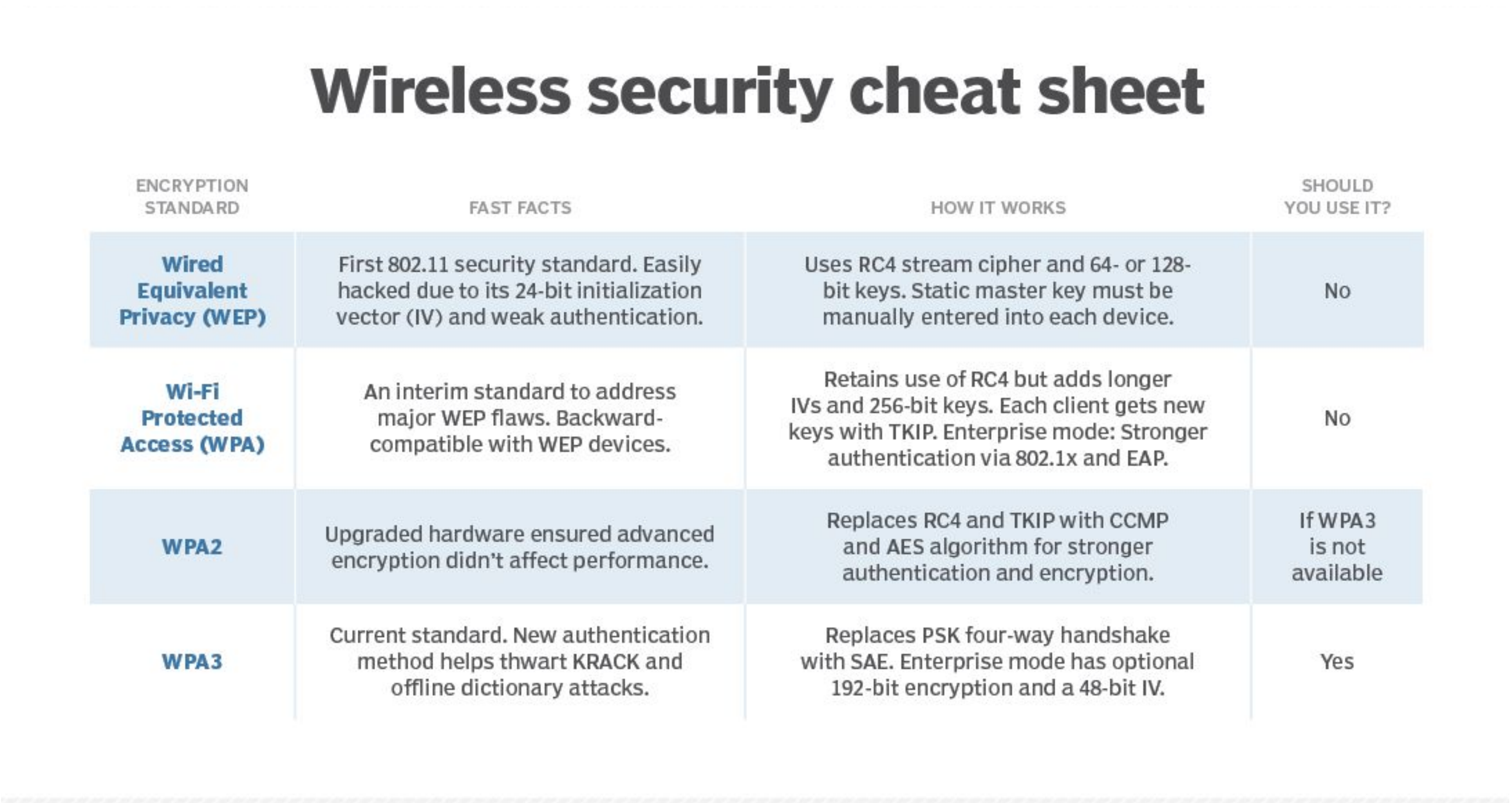
## Features of WPA2

- **Advanced Encryption Standard (AES)**
  - WPA2 utilizes the Advanced Encryption Standard (AES), a highly secure encryption algorithm, to ensure robust protection for data transmitted across wireless networks.
- **4-Way Handshake Authentication**
  - WPA2 uses the 4-way handshake method for authentication, establishing trusted connections between devices and access points.
- **Widely Supported Compatibility**
  - WPA2 is widely supported across various devices and networks, with existing hardware and software often compatible without requiring extensive updates.
- **Established Protocol**
  - WPA2 (Wi-Fi Protected Access 2), a well-known protocol extensively used in networks globally, has consistently provided reliable security for wireless connections.
- **Resistance to Brute Force Attacks**
  - WPA2 incorporates mechanisms to resist brute force attacks by limiting the number of login attempts and employing techniques such as key derivation functions to make password cracking more difficult.
- **Robust Key Management**
  - WPA2 has strong ways to manage keys. It has the pairwise transient key (PTK) and group temporal key (GTK) to make keys for encoding and checking safely. This makes the network more secure.

## What is WPA3?

- WPA3 boosts Wi-Fi security with personalized data encryption and advanced authentication through techniques like Simultaneous Authentication of Equals (SAE). Additionally, it introduces Wi-Fi Easy Connect to securely link devices with restricted displays, thereby bolstering network security further.
- **Features of WPA3**
  - **Individualized Data Encryption**
    - WPA3 uses special encryption for information that keeps it safe and private. Each tool and connection gets its own unique key to lock up data. This stops hackers from getting your personal information.
  - **Simultaneous Authentication of Equals (SAE)**
    - WPA3 utilizes SAE, a stronger authentication method compared to the 4-way handshake used in WPA2, adding an extra layer of security against unauthorized access.
  - **Enhanced Resistance to Modern Attacks**
    - WPA3 gives better security from current dangers and weaknesses, especially those that were very well exploited in WPA2, like the KRACK attack.
  - **Wi-Fi Easy Connect**
    - In the new WPA3, there is Wi-Fi Easy Connect. This makes it easy for people to link devices with small screens. People can set up safe links with Wi-Fi Easy Connect without making security weak.
  - **Forward Secrecy**
    - WPA3 implements forward secrecy, ensuring that even if a hacker captures and later cracks the encryption key, they cannot decrypt past network traffic. Each session key is unique, preventing retroactive decryption of captured data.
  - **Protection Against Dictionary Attacks**
    - WPA3 strengthens protection against dictionary attacks by introducing a new mechanism that detects and blocks repeated failed authentication attempts, making it significantly harder for attackers to guess passwords or passphrases through automated methods

| Features | WPA3 | WPA2 |
|---|---|---|
| **Encryption** | Implements individualized data encryption for heightened security. | Relies on the robust Advanced Encryption Standard (AES) for encryption. |
| **Authentication** | Utilizes Simultaneous Authentication of Equals (SAE) for stronger authentication. | Uses the 4-way handshake method to authenticate devices and access points. |
| **Security** | Offers enhanced resistance to modern attacks and vulnerabilities. | Vulnerable to exploits like KRACK, requiring additional precautions. |
| **Provisioning** | Method Introduces Wi-Fi Easy Connect for secure device provisioning. | Relies on traditional methods, often involving a pre-shared key. |
| **Compatibility** | Requires updates in hardware and software for full implementation. | Widely supported across devices, potentially needing firmware updates for full support. |
| **Implementation** | Still in the adoption phase, with gradual integration into devices and networks. | Established protocol, already widely deployed across networks worldwide. |



# Wireless security cheat sheet

| ENCRYPTION STANDARD | FAST FACTS | HOW IT WORKS | SHOULD YOU USE IT? |
|---|---|---|---|
| **Wired Equivalent Privacy (WEP)** | First 802.11 security standard. Easily hacked due to its 24-bit initialization vector (IV) and weak authentication. | Uses RC4 stream cipher and 64- or 128-bit keys. Static master key must be manually entered into each device. | No |
| **Wi-Fi Protected Access (WPA)** | An interim standard to address major WEP flaws. Backward-compatible with WEP devices. | Retains use of RC4 but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP. | No |
| **WPA2** | Upgraded hardware ensured advanced encryption didn't affect performance. | Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption. | If WPA3 is not available |
| **WPA3** | Current standard. New authentication method helps thwart KRACK and offline dictionary attacks. | Replaces PSK four-way handshake with SAE. Enterprise mode has optional 192-bit encryption and a 48-bit IV. | Yes |

Counter Mode with Cipher Block Chaining Message Authentication Code ProtocolExtensible Authentication Protocol

# Difference - Promiscuous vs. Monitor Mode

- Monitor mode (RFMON) enables a wireless NIC to capture packets without associating with an access point or ad-hoc network. This is desirable in that you can choose to "monitor" a specific channel, and you never need to transmit any packets.
- Promiscuous mode allows you to view all wireless packets on a network to which you have associated. The need to associate means that you must have some means of authenticating yourself with an access point. In promiscuous mode, you will not see packets until you have associated.
- In monitor mode the SSID filter mentioned above is disabled and all packets of all SSIDs from the currently selected channel are captured.

  Even in promiscuous mode, an 802.11 adapter will only supply packets to the host of the SSID the adapter has joined. Although it can receive, at the radio level, packets on other SSIDs, it will not forward them to the host.

Key points to remember:

**Promiscuous Mode:**

• Captures all traffic on the network you're connected to.

• Needs to be associated with an access point

• Useful for analyzing traffic on your own network.

• Can be used on both wired and wireless networks.

**Monitor Mode:**

• Captures traffic from any network within range, regardless of connection.

• Does not require association with an access point.

• Primarily used for wireless network analysis and penetration testing.

# Overview of 802.11 Protocols and Standards

1

## 802.11a/b/g

Legacy wireless protocols with varying speeds and frequencies.

2

## 802.11n

Introduced MIMO technology for increased throughput and range.

3

## 802.11ac/ax

Modern protocols delivering gigabit-level wireless connectivity.

# Understanding WAP and WLAN Authentication Methods

### WAP (Wireless Access Point)

Provides wireless connectivity to client devices within a network.

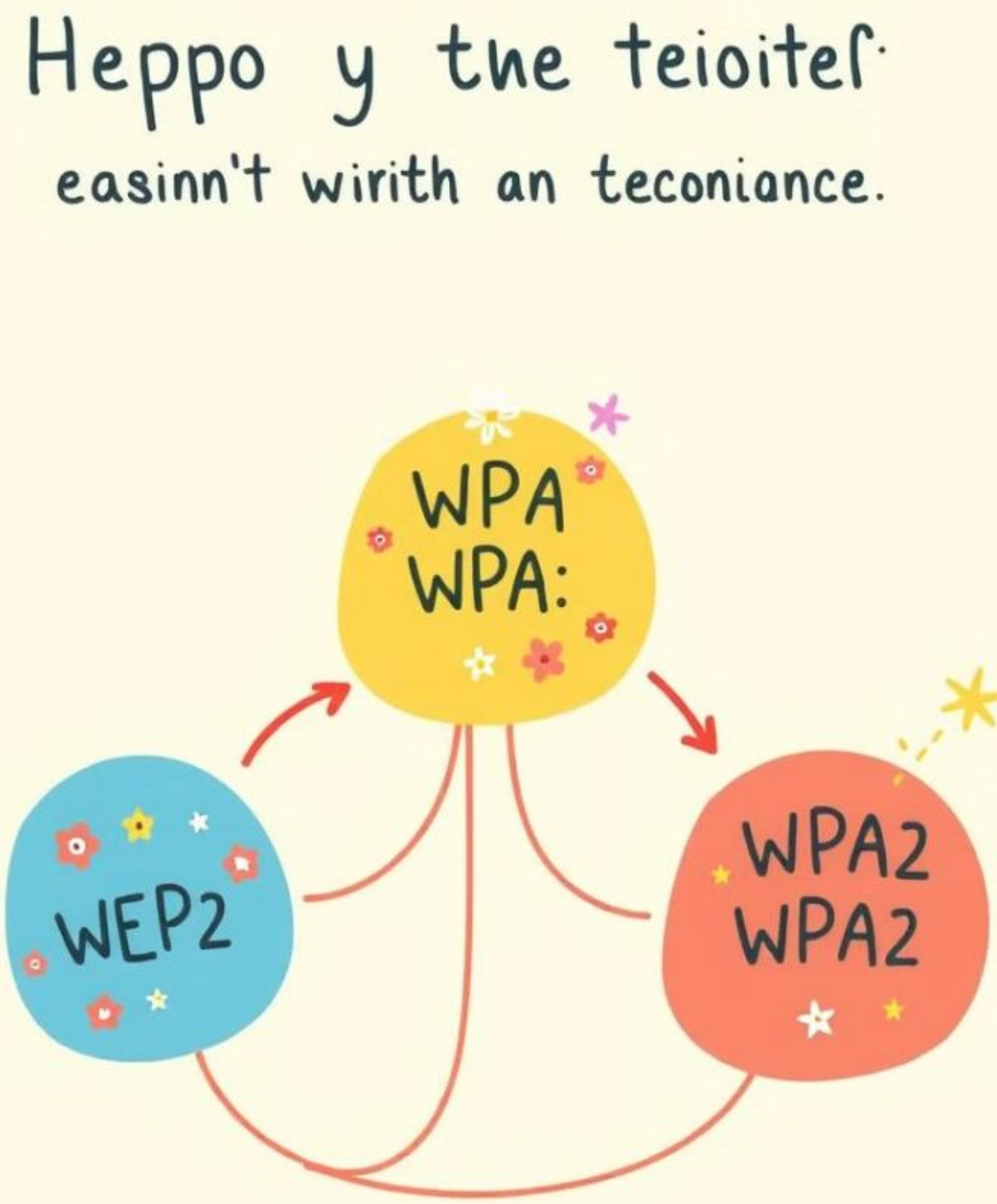
### Authentication Methods

- Open System
- Shared Key
- 802.1X
- PSK (Pre-Shared Key)

### WLAN (Wireless LAN)

The wireless network infrastructure that connects clients to resources.

# Encryption Protocols: WEP, WPA, and WPA2



Beck-Tews attack
Targets WPA's TKIP encryption.

### WEP (Wired Equivalent Privacy)

Legacy encryption protocol with known vulnerabilities.

### WPA (Wi-Fi Protected Access)

Improved encryption and authentication over WEP.

### WPA2 (Wi-Fi Protected Access 2)

Current industry standard for wireless encryption and security.

KRACK attack

Affects WPA2 and exploits the four-way handshake process to intercept data.

Session key negotiation

WPA and WPA2 have multiple vulnerabilities that affect session key negotiation. lead to attacks like arbitrary packet decryption and injection, and TCP connection hijacking.

# Vulnerabilities and Weaknesses in Encryption Protocols

1 WEP Weaknesses

Static encryption keys, IV (Initialization Vector) reuse, and lack of encryption integrity.

2 WPA Vulnerabilities

Potential for brute-force attacks on pre-shared keys (PSK).

3 WPA2 Limitations

KRACK (Key Reinstallation Attacks) vulnerability discovered in 2017.

# WLAN-Based Attacks: Types and Characteristics

### Rogue Access Point

Unauthorized WAP used to intercept network traffic.

### Denial of Service (DoS)

Disrupting WLAN availability through jamming or flooding attacks.

### Man-in-the-Middle

Intercepting and modifying communication between clients and WAP.

# Countermeasures Against WLAN Attacks

### Firewall

Implement robust firewall policies to monitor and control network traffic.

### Encryption

Deploy the latest WPA2 or WPA3 encryption standards.

### Access Control

Enforce strict access control and authentication mechanisms.

### Monitoring

Continuously monitor the WLAN for suspicious activities and intrusions.

# Penetration Testing Tools for WLAN Security Assessment

| | |
|---|---|
| Aircrack-ng | Wireless network security auditing and cracking tool |
| Kismet | Wireless network detection, mapping, and monitoring tool |
| Wireshark | Packet capture and analysis tool for network troubleshooting |
| Metasploit | Comprehensive penetration testing framework |

# Best Practices for Secure WLAN Configuration

1 Use WPA2 or WPA3

Implement the latest encryption protocols for maximum security.

2 Disable Legacy Protocols

Disable support for outdated and vulnerable protocols like WEP.

3 Manage Access Controls

Enforce strong authentication and authorization mechanisms.

4 Regularly Update Firmware

Keep wireless devices and access points up-to-date with security patches.

# Conclusion and Key Takeaways

1

### Evolving Protocols

Staying current with the latest 802.11 standards is crucial for robust wireless security.

2

### Vulnerability Awareness

Understanding encryption protocol weaknesses and WLAN attack vectors is essential.

3

### Proactive Measures

Implementing best practices and utilizing security tools can effectively mitigate risks.