



**Certified Network Defender v3**

**MODULE 13**

**ENTERPRISE WIRELESS  
NETWORK SECURITY**

---

EC-Council Official Curricula

This page is intentionally left blank.

## LEARNING OBJECTIVES

The learning objectives of this module are:

- LO#01: Understand the fundamentals of wireless networks
- LO#02: Understand the encryption mechanisms used in wireless networks
- LO#03: Understand the authentication methods used in wireless networks
- LO#04: Discuss the security measures that must be implemented for wireless networks

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Learning Objectives

This module deals with network security for wireless networks in enterprises. Wireless networks are widely used across organizations today and are prone to various attacks. Therefore, organizations need to focus on the planning for securing the wireless network across the organization. The following are the learning objectives of this module:

- Understand the fundamentals of wireless networks
- Understand the encryption mechanisms used in wireless networks
- Understand the authentication methods used in wireless networks
- Discuss the security measures that must be implemented for wireless networks



---

## LO#01: Understand the fundamentals of wireless networks

---

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### **LO#01: Fundamentals of Wireless Networks**

The objective of this section is to understand the fundamentals of wireless networks which includes the wireless network terminologies, components used in wireless networks, the uses of wireless networks, and their advantages and limitations. This section covers the different types of wireless technologies, wireless network standards, and topologies.

The infographic titled "Wireless Terminologies" features the CND logo in the top right corner. It contains eight colored boxes, each describing a different wireless technology or protocol. The boxes are arranged in two columns and four rows. The first row has a light blue box for OFDM and a light blue box for MIMO-OFDM. The second row has a purple box for DSSS and a purple box for TKIP. The third row has a red box for FHSS and a red box for LEAP. The fourth row has an orange box for SSID and an orange box for EAP. At the bottom right of the infographic, there is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

## Wireless Terminologies

**Orthogonal Frequency-division Multiplexing (OFDM):** Method of **encoding digital data** on multiple carrier frequencies

**Multiple-input multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM):** Air interface for fourth generation (4G) and fifth generation (5G) broadband wireless communications

**Direct-sequence Spread Spectrum (DSSS):** Original **data signal is multiplied** with a pseudorandom noise spreading code

**Temporal Key Integrity Protocol (TKIP):** A **security protocol** used in wireless protected access (WPA) as a replacement for wired equivalent privacy (WEP)

**Frequency-hopping Spread Spectrum (FHSS):** Method of transmitting radio signals by rapidly **switching a carrier** among many frequency channels

**Lightweight Extensible Authentication Protocol (LEAP):** It is a proprietary WLAN **authentication protocol** developed by Cisco Systems Inc.

**Service Set Identifier (SSID):** A 32 **alphanumeric unique identifier** given to a wireless local area network (WLAN)

**Extensible Authentication Protocol (EAP):** Supports **multiple authentication** methods, such as token cards, Kerberos, certificates, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Terminologies

### Orthogonal Frequency-Division Multiplexing

An orthogonal frequency-division multiplexing (OFDM) is a system modulation format that encodes digital data to multiple channels distributed across the frequency band. OFDM minimizes the attenuation in transmission, resulting in a high throughput. It is used by the 802.11 a, g, n and ac wireless standards.

### Direct-sequence Spread Spectrum

A direct-sequence spread spectrum (DSSS) is a modulation technique that transmits digital signals over airwaves. This transmission process requires spread spectrum modulation. The 802.11b network works on the DSSS technique. DSSS requires a large amount of bandwidth since it allows channel sharing.

### Frequency-hopping Spread Spectrum

A local area wireless network (LAWN) uses the frequency-hopping spread spectrum (FHSS) modulation technique. The transmission hop in FHSS occurs several times per second, allowing devices in a short range to work efficiently. Large systems using the same frequency do not affect the working of small devices.

### Multiple-input Multiple-output Orthogonal Frequency-division Multiplexing

The multiple-input multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM) influences the spectral efficiency of the fourth generation (4G) and fifth generation (5G) wireless communication services. Adopting the MIMO-OFDM technique reduces the interference and increases the robustness of the channel.

### **Service Set Identifier**

A service set identifier (SSID) is a 32 alphanumeric sequence character that acts as an identifier of a wireless network. The SSID permits connections to the required network from an available independent network. Devices connecting to the same wireless local area network (WLAN) must use the same SSID to establish a connection.

### **Temporal Key Integrity Protocol**

A temporary key integrity protocol (TKIP) is an encryption protocol that is a part of a WLAN. It encrypts each data packet with a unique encryption key. A TKIP is a set of algorithms and is more secure than wired equivalent privacy (WEP).

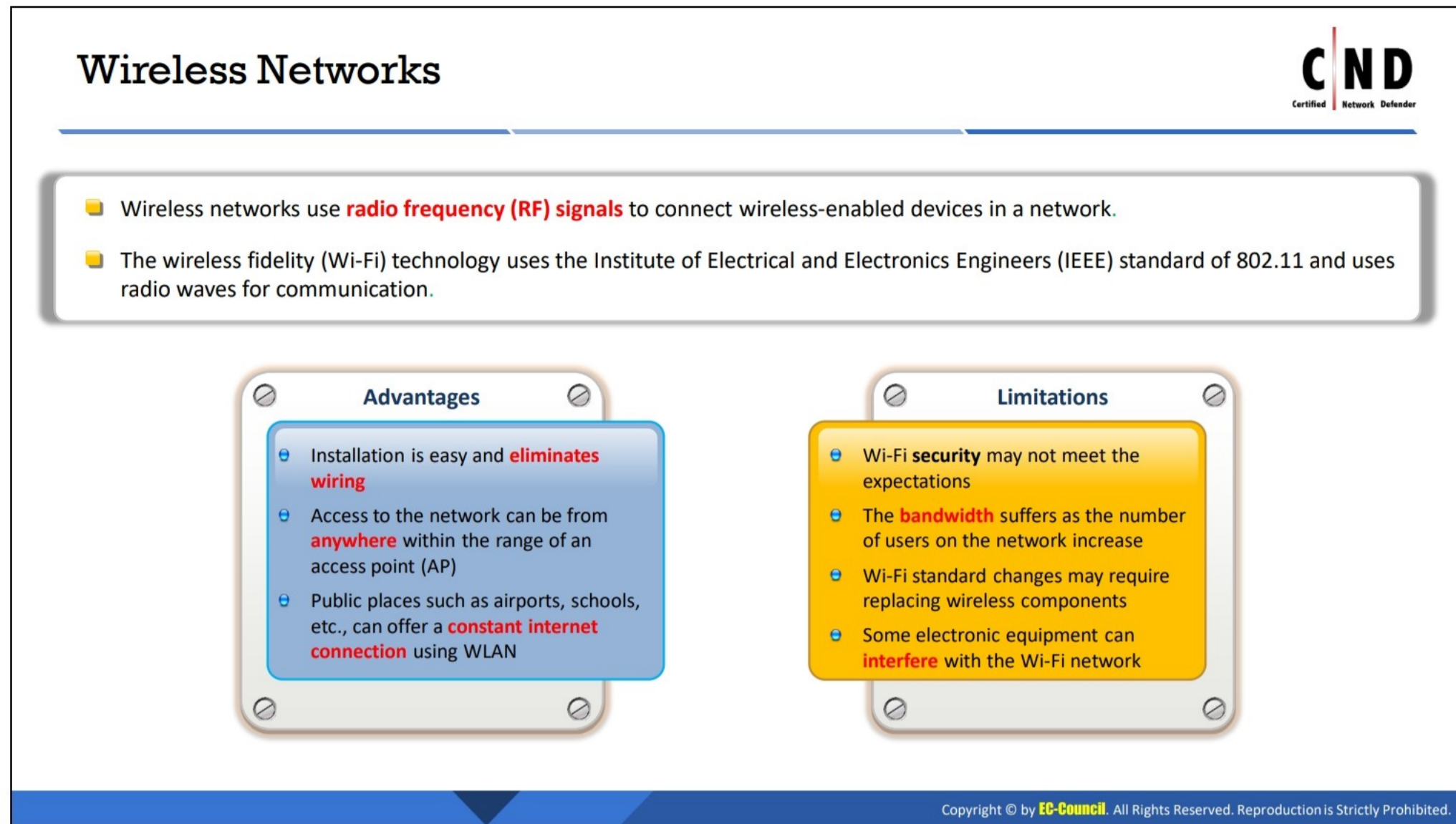
### **Lightweight Extensible Authentication Protocol**

The lightweight extensible authentication protocol (LEAP) is a proprietary Cisco authentication version protocol that is used in wireless networks and point-to-point connections. The authentication protocol depends on WEP keys which change with the frequent authentication process between a client and a server.

### **Extensible Authentication Protocol**

The extensible authentication protocol (EAP) is used by the point-to-point protocol (PPP). It supports multiple authentication types such as smart cards, token cards, public key encryption, etc. EAP has several authentication methods such as the EAP transport layer security (EAP-TLS), EAP subscriber identity module (EAP-SIM), EAP authentication and key agreement (EAP-AKA), and EAP tunneled transport layer security (EAP-TTLS).

## Wireless Networks



The infographic is titled "Wireless Networks" and features the CND logo in the top right corner. It contains two main sections: "Advantages" and "Limitations". The "Advantages" section is a blue box with three bullet points: "Installation is easy and eliminates wiring", "Access to the network can be from anywhere within the range of an access point (AP)", and "Public places such as airports, schools, etc., can offer a constant internet connection using WLAN". The "Limitations" section is a yellow box with four bullet points: "Wi-Fi security may not meet the expectations", "The bandwidth suffers as the number of users on the network increase", "Wi-Fi standard changes may require replacing wireless components", and "Some electronic equipment can interfere with the Wi-Fi network". At the bottom of the infographic, there is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

- Wireless networks use **radio frequency (RF) signals** to connect wireless-enabled devices in a network.
- The wireless fidelity (Wi-Fi) technology uses the Institute of Electrical and Electronics Engineers (IEEE) standard of 802.11 and uses radio waves for communication.

### Advantages

- Installation is easy and **eliminates wiring**
- Access to the network can be from **anywhere** within the range of an access point (AP)
- Public places such as airports, schools, etc., can offer a **constant internet connection** using WLAN

### Limitations

- Wi-Fi **security** may not meet the expectations
- The **bandwidth** suffers as the number of users on the network increase
- Wi-Fi standard changes may require replacing wireless components
- Some electronic equipment can **interfere** with the Wi-Fi network

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Networks

The computer world is heading towards a new era of technological evolution by using wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing the physical connection or cable, individuals are able to use networks in newer ways that make data portable, mobile, and accessible.

A wireless network environment opens up many new expansions and workflow possibilities. With the availability of a wireless network, there is no need to worry when a user wants to move their PC from one office to the next or when they want to work in a location that does not have an ethernet port.

Wireless networking is very useful in public places including libraries, coffee shops, hotels, airports, and other establishments that offer WLAN connections.

The most important aspect in wireless networking is an access point through which a user can communicate with another mobile or fixed host. An access point is a device that contains a radio transceiver (that sends and receives signals) along with a registered jack 45 (RJ-45) wired network interface, which allows a user to connect to a standard wired network using a cable.

## Wireless Technologies

In a wireless network, data transmission occurs by means of electromagnetic waves that carry signals over the communication path.

## Types of Wireless Technologies

- **Wi-Fi**

Wireless fidelity (Wi-Fi) is a part of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of wireless networking standards. This technology uses radio waves or microwaves to allow electronic devices to exchange data or connect to the internet. Many devices such as personal computers, laptops, digital cameras, smartphones, etc., support Wi-Fi technology. Wi-Fi operates in the frequency band between 2.4 GHz and 5 GHz. A Wi-Fi network uses radio waves to transmit the signals across the network. For this purpose, a computer should have a wireless adapter to translate the data into radio signals and pass them through an antenna and router. This is where the message is decoded and the data is sent to the internet or through another network. Hotspots are areas that have Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the internet through a hotspot.

- **Bluetooth**

In the Bluetooth technology, data is transmitted between cell phones, computers, and other networking devices over short distances. Signals transmitted via Bluetooth cover short distances of up to 10 m as compared to other modes of wireless communication. Bluetooth transfers the data at a speed of less than 1 Mbps and operates in the frequency range of 2.4 GHz. This technology comes under IEEE 802.15 and uses a radio technology called FHSS for transferring data to other Bluetooth-enabled devices.

- **RFID**

The radio-frequency identification (RFID) technology uses radio frequency (RF) electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. RFID devices work within a small range of up to 20 ft.

- **WiMax**

The worldwide interoperability for microwave access (WiMax) technology uses long distance wireless networking and high-speed internet. It belongs to the IEEE 802.16 family of wireless networking standards. WiMax signals can function over a distance of several miles with data rates reaching up to 75 Mbps. It uses a fixed wireless application and mobile stations to provide high-speed data, voice, video calls, and internet connectivity to users. The WiMax forum developed WiMax and states that nearly 135 countries have deployed over 455 WiMax networks.

## Wired vs. Wireless Networks

The differences between a wired and a wireless network are as follows:

Wired networks	Wireless networks
High bandwidth	Low bandwidth
Low bandwidth variation	High bandwidth variation
Low error rates	High error rates
More secure	Less secure
Less equipment dependent	More equipment dependent
Symmetric connectivity	Possible asymmetric connectivity
High-power machines	Low-power machines
High-resource machines	Low-resource machines
Low delay	High delay
Connected operation	Disconnected operation

Table 13. 1: Differences Between a Wired and a Wireless Network

### Advantages of a Wireless Network

- **Accessibility:** Devices connected to a wireless network can be accessed from any location within the coverage area.
- **Flexibility:** Devices may be carried from one location to another within the coverage area. This enables the users to access the internet from any location.
- **Efficiency:** A wireless network improves the efficiency of employees in an organization, as they are able to access the internet and perform suitable actions in order to complete a work within the stipulated time. They can work on the go and do not require an office.
- **Easy to set up:** The setting up of a wireless network requires a low cost and less time, thus making it easier to use as compared to a wired network.
- **Security:** Advanced security features have been employed for the security of wireless networks.
- **Expandable:** It is easy to expand the coverage area of a wireless network for a particular location.

### Disadvantages of a Wireless Network

- Electromagnetic interference caused by another network or other devices might interrupt the network, leading to system failure and slow/lost signals.
- Some locations are not suitable for wireless networking and are termed as black spots where no signals are available.

## Wireless Network Standards



Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbps/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11 (Wi-Fi)	2.4	22	1, 2	DSSS, FHSS	20	100
802.11a	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
	3.7				—	5000
802.11b	2.4	22	1, 2, 5.5, 11	DSSS	35	140
802.11d	It is an enhanced version of 802.11a and 802.11b that enables global portability by allowing variation in frequencies, power levels, and bandwidth.					
802.11e	It provides guidance for prioritization of data, voice, and video transmissions by enabling quality of service (QoS).					
802.11g	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	125	450

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Network Standards (Cont'd)



Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbps/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11i	This is a standard for WLANs that provides <b>improved encryption</b> for networks that use the 802.11a, 802.11b, and 802.11g standards					
802.11n	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	MIMO-OFDM	70	150
	2.4	40	15, 30, 45, 60, 90, 120, 135, 150		70	150
802.11ac	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3	MIMO-OFDM	35	
		40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200		35	
		80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3		35	
		160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7		35	
802.11ax	2.4/5/6	40	Up to 2294 <sup>[F]</sup>	MIMO-OFDM	30	120
		80	Up to 4803 <sup>[F]</sup>			
		80+80	Up to 10530			
802.11be	2.4/5/6	320	30 Gbps - 46 Gbps (3750-5750)			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Network Standards (Cont'd)



Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbits/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11ad	60	2160	6.75 Gbit/s	OFDM, single carrier, low-power single carrier	60	100
802.12	This standard defines the demand priority and media access control protocol for increasing the Ethernet data rate to 100 Mbps.					
802.15	This standard defines the communication specifications for wireless personal area networks (WPANs)					
802.15.1 (Bluetooth)	2.4		1-3 Mbps		10	
802.15.4 (Zigbee)	2.4	868, 900				
802.15.5	A standard for mesh networks with enhanced reliability via route redundancy					
802.16	A group of broadband wireless communication standards for <b>metropolitan area networks (MANs)</b>					

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Wireless Network Standards

The IEEE standards correspond to the various wireless networking transmission methods. They are as follows:

- **802.11 (Wi-Fi):** This standard corresponds to WLANs and uses FHSS or DSSS as the frequency hopping spectrum. It allows an electronic device to connect to the internet using a wireless connection that is established in any network.
- **802.11a:** This standard is the second extension to the original 802.11 standard. It operates in the 5 GHz frequency band and supports a bandwidth of up to 54 Mbps by using OFDM. It has a fast maximum speed, but is more sensitive to walls and other obstacles.
- **802.11b:** IEEE expanded the 802.11 standard by creating the 802.11b specifications in 1999. This standard operates in the 2.4 GHz industrial, scientific and medical (ISM) radio band and supports a bandwidth of up to 11 Mbps by using DSSS modulation.
- **802.11d:** This standard is an enhanced version of the 802.11a and 802.11b standards. It supports the regulatory domains. The particulars of this standard can be set at the media access control (MAC) layer.
- **802.11e:** This standard defines the quality of service (QoS) for wireless applications. The enhanced service is modified using the MAC layer. This standard maintains the quality of video and audio streaming, real-time online applications, voice over internet protocol (VoIP), etc.
- **802.11g:** This standard is an extension of the 802.11 standard. It supports a maximum bandwidth of 54 Mbps using the OFDM technology and uses the same 2.4 GHz band as

802.11b. It is compatible with the 802.11b standard, which implies that 802.11b devices can work directly with an 802.11g access point.

- **802.11i:** This standard is used as a standard for WLANs and provides improved encryption for networks. 802.11i requires new protocols such as TKIP and advanced encryption standard (AES).
- **802.11n:** This standard was developed in 2009. It aims to improve the 802.11g standard in terms of the bandwidth. It operates on both the 2.4 and 5 GHz bands and supports a maximum data rate up to 300 Mbps. It uses multiple transmitters and receiver antennas (MIMO) to allow a maximum data rate along with security improvements.
- **802.11ac:** This standard provides a high throughput network at the frequency of 5 GHz. It is faster and more reliable than the 802.11n standard. It involves gigabit networking which provides an instantaneous data transfer experience.
- **802.11ax:** 802.11ax also known as Wi-Fi 6. It is the sixth generation of the Wi-Fi standard. It is designed to operate in all ISM bands between 1 and 6 GHz.
- **802.11be:** Formally known as Extremely High throughput (EHT), it will be based on 802.11ax, with the primary focus on indoor and outdoor Wide Area Network (WAN) operation with fixed and walking speeds in the frequency bands 2.4 GHz, 5 GHz, and 6 GHz.
- **802.11mc:** It enables computing devices to accurately measure the distance to the nearest Wi-Fi access point (AP) and determine the indoor location of the AP with a round-trip delay of 1-2 metres.
- **802.11ad:** 802.11ad involves the inclusion of a new physical layer for 802.11 networks. This standard works on the 60 GHz spectrum. The data propagation speed in this standard is significantly different from the bands operating at 2.4 GHz and 5 GHz. With a very high frequency spectrum, the transfer speed is much higher than that of 802.11n.
- **802.12:** This standard dominates media utilization by working on the demand priority protocol. Based on this standard, the ethernet speed increases to 100 Mbps. It is compatible with the 802.3 and 802.5 standards. Users currently on these standards can directly upgrade to the 802.12 standard.
- **802.15:** This defines the standards for a wireless personal area network (WPAN). It describes the specification for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth):** Bluetooth is mainly used for exchanging data between fixed and mobile devices over short distances.
- **802.15.4 (Zigbee):** The 802.15.4 standard has a low data rate and complexity. Zigbee is the specification used in the 802.15.4 standard. It transmits long distance data through a mesh network. This specification handles applications operating at a low data rate, but longer battery life. Its data rate is 250 kbits/s.
- **802.15.5:** This standard deploys itself on a full mesh or a half mesh topology. It includes network initialization, addressing, and unicasting.

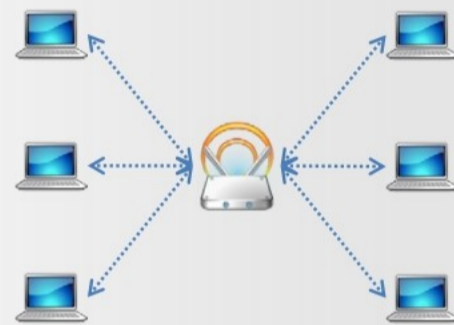
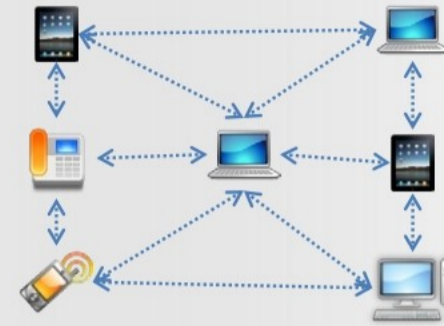
- **IEEE 802.16:** This standard is also known as WiMax and is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

## Wireless Network Topologies



### Ad-hoc Standalone Network Architecture (Independent Basic Service Set (IBSS))

- Devices exchange information with each other similar to that in a **peer-to-peer** communication mode without the need of an AP for communication
- To setup this mode properly, first configure the wireless adapter for all the devices. They should all have the **same channel name** and SSID in order to activate the connections



### Infrastructure Network Topology (Centrally Coordinated Architecture/ Basic Service Set (BSS))

- Devices in the wireless network are connected through an **AP**
- An AP connects to the internet via a modem
- Installed in large organizations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Network Topologies

In order to plan and install a wireless network, it is necessary to determine the type of architecture that would be suitable for the network environment.

There are two types of wireless topologies:

### Standalone Architecture (Ad-hoc Mode)

The ad-hoc mode is also called as the independent basic service set (IBSS) mode. Devices connected over a wireless network communicate with each other directly, similar to that in the peer-to-peer communication mode. The ad-hoc mode does not implement a wireless access point (WAP)/access point (AP) for communication between devices. The wireless adaptors on each device are configured on the ad-hoc mode rather than on the infrastructure mode. Adaptors for all the devices must use the same channel name and SSID in order to establish the network connections successfully.

The ad-hoc mode works effectively for a small group of devices and it is necessary to connect all the devices with each other in close proximity. The network performance degrades as the number of devices increases. It becomes cumbersome for a network administrator to manage the network in this mode, because devices connect and disconnect regularly. It is not possible to bridge this mode with a traditional wired network and it does not allow internet access until a special gateway is present.

The ad-hoc mode works better in a small area and does not require any access points (such as a router or a switch), thus minimizing the cost. This mode acts as a backup option and appears when there is a problem or a malfunction in the APs or a centrally coordinated network (infrastructure mode). This mode uses the functionality of each adaptor to enable security authentication and to use wireless services.

The key characteristics of an ad-hoc wireless network are as follows:

- The AP encrypts and decrypts text messages.
- Each AP operates independently and has its own respective configuration files.
- The network configuration remains constant with changes in the network conditions.

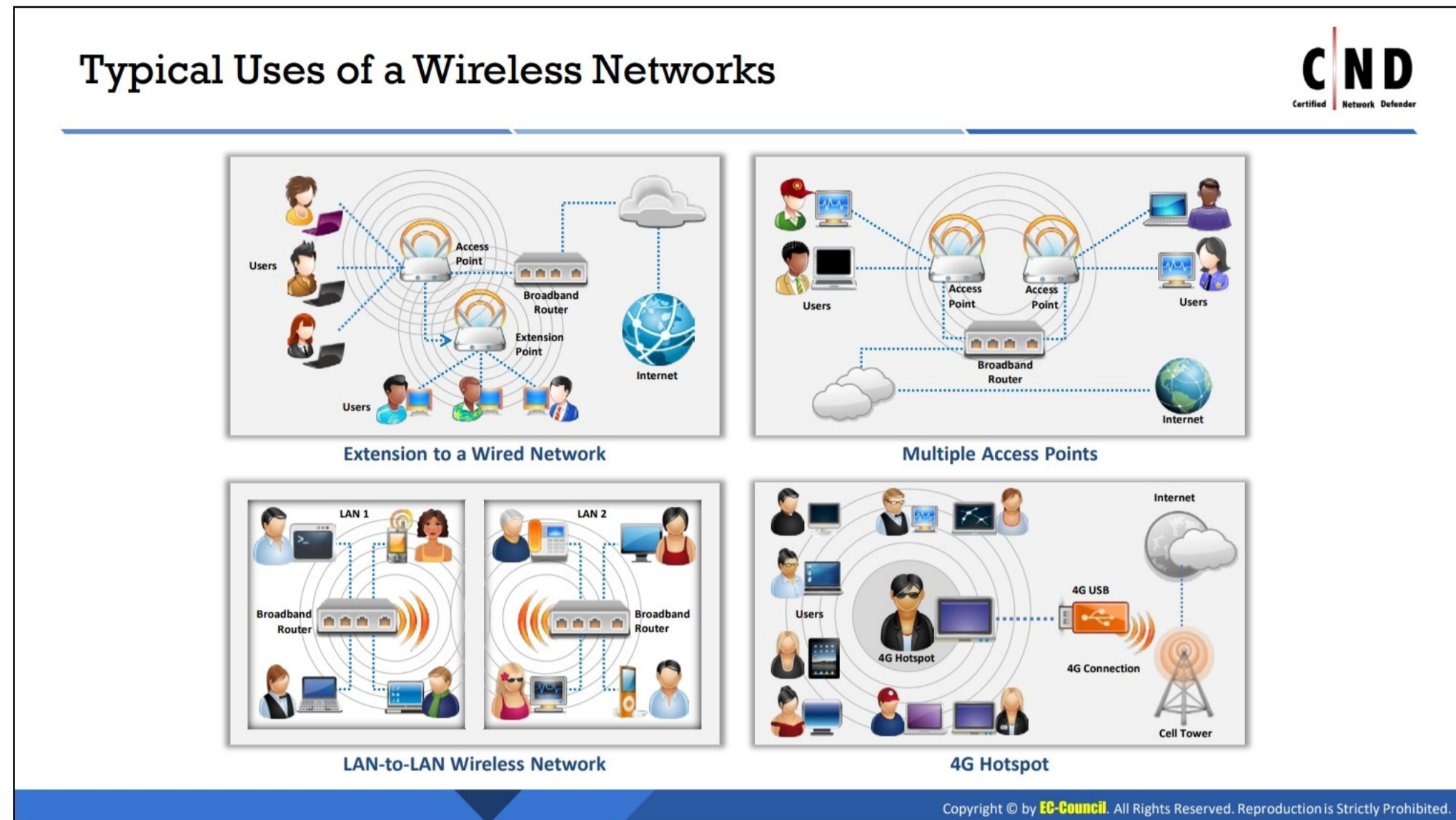
### **Centrally Coordinated Architecture (Infrastructure Mode)**

A centrally coordinated architecture (infrastructure mode) or a basic service set (BSS) mode is an architecture where all wireless devices connect to each other through an AP. This AP (router or switch) receives internet access by connecting to a broadband modem. This mode will work effectively when deployed in large organizations. It simplifies the network management and helps address the operational issues. It assures resiliency while allowing a number of systems to connect across the network.

This mode provides enhanced security options, scalability, stability, and easy management. The downside is that it is expensive, since an AP (router or switch) is required to connect the devices to each other.

The following are the key characteristics of the infrastructure mode:

- It increases or decreases the range of the wireless network by adding and removing the APs.
- The controller reconfigures the network according to the changes in the RF footprint.
- The controller regularly monitors and controls the activities on the wireless network by reconfiguring the AP elements to maintain and protect the network.
- The wireless centralized controller manages all the AP tasks.
- The wireless network controller performs various crucial tasks such as user authentication, policy creation and enforcement, fault tolerances, network expansion, configuration control, etc.
- It maintains backups of other APs in a different location and these are used when a particular AP malfunctions.



### Typical Uses of a Wireless Networks

Wireless networks are classified on the basis of the connection used and the geographical area.

#### Wireless Networks Based on the Connection

- **Extension to a wired network:**

Extension to a wired network can be obtained by placing APs between a wired network and wireless devices.

In this network, the AP acts as a hub that provides connectivity for wireless computers. It can also connect a wireless LAN to a wired LAN, which allows the wireless computers the access to LAN resources such as file servers or existing internet connectivity.

The two types of APs used in this type of wireless network are:

1. **Software APs** that can be connected to a wired network and which run on a computer with a wireless network interface card
2. **Hardware APs (HAPs)** which provide a comprehensive support of most of the wireless features. With a suitable networking software support, users on the wireless LAN can share files and printers situated on the wired LAN and vice versa.

The network may be extended further in accordance with the size of the location and interference from other devices. This enables a wired/wireless connection across the location for multiple users.

- **Multiple APs:**

Wireless computers connect using multiple APs. If a single large area is not covered by a single AP, multiple APs or extension points are used. Extension points are not defined in the wireless

standard. When using multiple APs, each AP must cover its neighbors. This allows the users to move around seamlessly using a feature called roaming. Some manufacturers develop extension points which act as wireless relays, and thus extend the range of a single AP. Multiple extension points can be strung together to provide wireless access to distant locations from the central AP.

- **LAN-to-LAN wireless networks:**

APs provide wireless connectivity to local computers and computers on a different network. All HAPs have the capability of directly connecting to other HAPs. Building interconnecting LANs by using wireless connections is large and complex. Several LAN-enabled PCs can be connected to an AP for wireless communication.

- **4G hotspot:**

A hotspot provides internet access over a WLAN with the help of a router connected to the internet service provider (ISP). Multiple devices can be connected at the same time using a Wi-Fi network adapter. Hotspots use the service from cellular providers for 4G internet access. Computers generally scan for hotspots thereby identifying the SSID (network name) of the wireless network.

### **Wireless Network Based on the Geographic Area Coverage**

Wireless networks are classified into WLAN, wireless wide-area network (WWAN), wireless personal area network (WPAN), and wireless metropolitan-area network (WMAN) based on the area they cover geographically.

#### **1. WLAN:**

- A WLAN connects users in a local area with a network. The area may range from a single room to an entire campus.
- It connects wireless users and the wired network.
- It uses high-frequency radio waves.
- WLAN is also known as a LAWN.
- In 1990, IEEE created a group to develop a standard for wireless equipment.
- In the peer-to-peer mode, wireless devices within each other's range communicate directly with each other without using a central AP.
- In the infrastructure mode, the access point is wired to the internet with the wireless users. An access point functions as a mediator between the wired and wireless networks.

#### **Advantages:**

- WLAN is flexible to install.
- Wireless networks are easy to set up and use.
- Wireless networks are robust. If one base station is down, users can physically move their PCs in the range of another base station.

- It has a better chance of surviving in case of a disaster.

**Disadvantage:**

- Data transfer speeds are normally slower than wired network.

**2. WWAN**

- WWAN covers an area larger than the WLAN.
- It handles cellular network technology such as code-division multiple access (CDMA), global system for mobile communications (GSM), general packet radio service (GPRS), and cellular digital packet data (CDPD) for data transmission.
- This technology can cover a particular region, nation, or even the entire globe.
- The system has a built-in cellular radio (GSM/CDMA) which helps users to send or receive data.
- In WWAN, the wireless data consists of fixed microwave links, digital dispatch networks, wireless LANs, data over cellular networks, wireless WANs, satellite links, one-way and two-way paging networks, laser-based communications, diffuse infrared, keyless car entry, the global positioning system, and more.

**3. WPAN**

- WPAN interconnects devices positioned around an individual, in which the connections are wireless.
- WPAN has a very short range. It can communicate within a range of 10 m. A WPAN interconnects the mobile network devices that people carry with them or have on their desk.
- The main concept in WPAN technology is *plugging in*.
- When any two WPAN devices come within a range of a few meters to the central server, they communicate with each other, similar to a wired network.
- Another characteristic of a WPAN is the ability to lock out other devices and prevent interference.
- Every device in a WPAN can connect to any other device in the same WPAN. However, to do so, they should be within the physical range of each another. Bluetooth is the best example of WPAN.

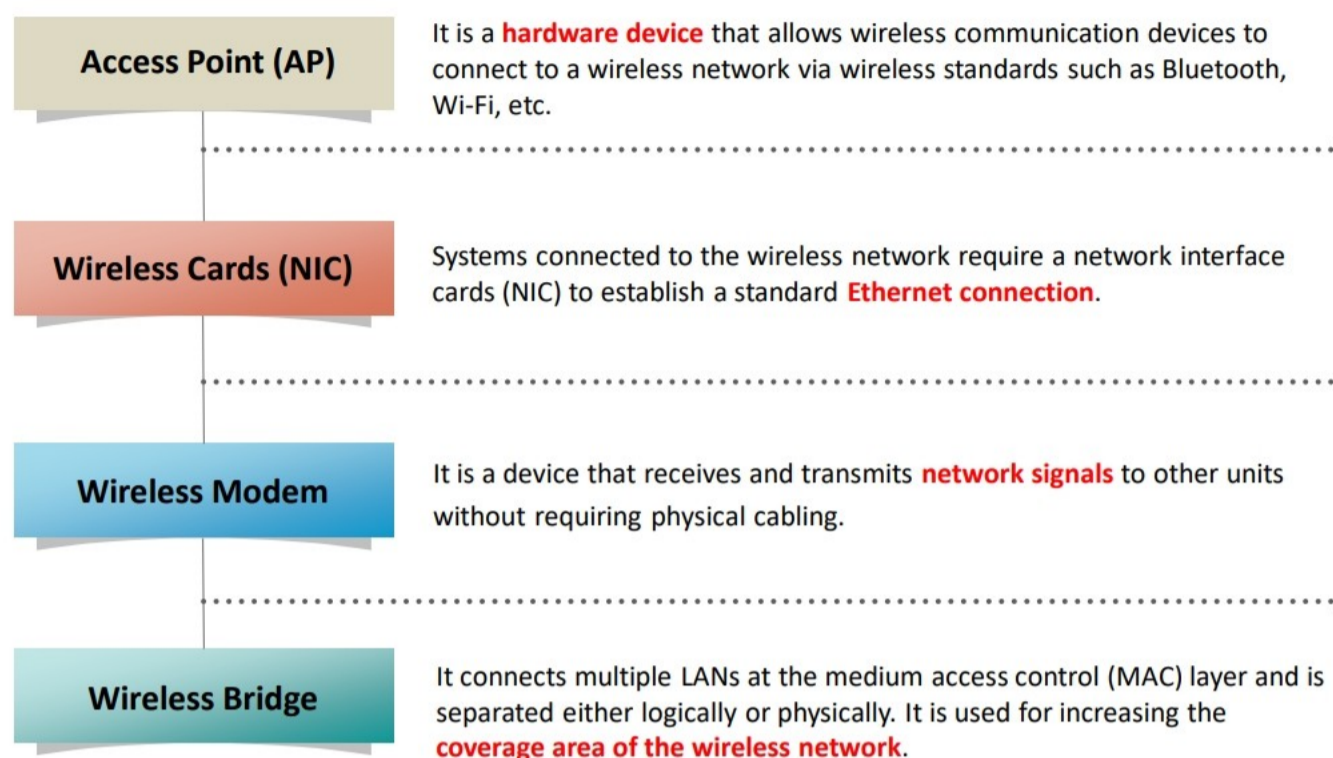
**4. WMAN**

WMAN covers a metropolitan area such as an entire city or a suburb.

- It accesses broadband area networks by using an exterior antenna.
- It is a good alternative for a fixed-line network. It is simple to build and is inexpensive.
- In a WMAN, the subscriber stations communicate with the base station that is connected to a central network or hub.

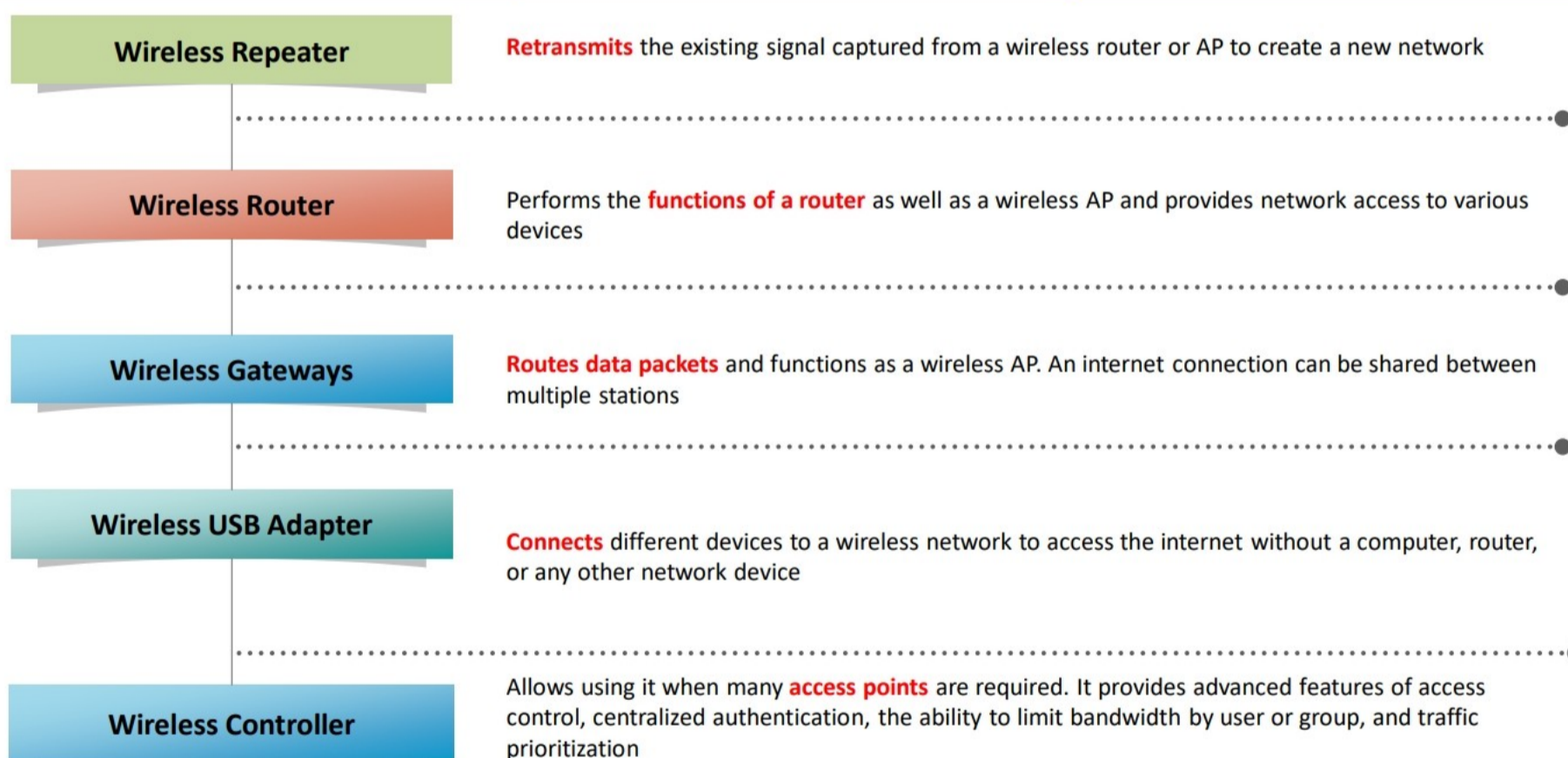
- A WMAN uses a wireless infrastructure or optical fiber connections to link the sites.
- A WMAN links between the WLANs. Distributed queue dual bus (DQDB), is the MAN standard for data communications, specified by the IEEE 802.6 standard. On the basis of DQDB, the network can be established over 30 mi with a speed of 34 to 154 Mbits/s.

## Components of a Wireless Network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Components of a Wireless Network (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Components of a Wireless Network (Cont'd)

Antenna Converts electrical impulses into **radio waves** and vice-versa

### Types of Antenna

<b>Directional Antenna</b> Used for broadcasting and obtaining radio waves from <b>a single direction</b>	<b>Omnidirectional Antenna</b> It provides a <b>360° horizontal radiation</b> pattern. It is used in wireless base stations
<b>Semi-directional antenna</b> It provides point-to-point communication for <b>short-to-medium distance</b> communication	<b>Yagi Antenna</b> A <b>unidirectional antenna</b> commonly used in communications in the frequency band from 10 MHz to very high frequency (VHF) and ultra high frequency (UHF)
<b>Dipole Antenna</b> Bidirectional antenna, used for supporting <b>client connections</b> rather than site-to-site applications	<b>Reflector Antennas</b> These are used for <b>concentrating electromagnetic energy</b> that is radiated or received at a focal point
<b>Parabolic Grid Antenna</b> It is based on the principle of a <b>satellite dish</b> and can pick up Wi-Fi signals from a distance of 16 km or more	<b>Aperture Antenna</b> It is used for <b>space applications</b> because they are more practical for space applications

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Components of a Wireless Network

The key components of a wireless network are as follows:

- **Access point:**

An access point (AP) is a hardware device that uses the wireless infrastructure network mode to connect wireless components to a wired network for transmitting data. It serves as a switch or hub between a wired LAN and a wireless network. It has a built-in transmitter, receiver, and an antenna. The additional ports in the WAP help in expanding the network range and provide access to additional clients. The number of APs depends on the network size. However, multiple APs provide access to a larger number of wireless clients and, in turn, expand the range of the wireless network. The transmission range and distance that a client has to be from a wireless AP is a maximum default value; APs transmit usable signals well beyond the default range. The distance to which a wireless AP signal is transmitted depends on the wireless standards, obstructions, and environmental conditions between the clients and the APs.

The transmission range and number of devices that a WAP can connect depends on the wireless standard used and the signal interference between the devices. In the wireless infrastructure network design, multiple APs can be used to cover an extensive area or a single AP can be used for covering a small geographical area such as buildings, homes, etc.

- **Wireless network cards:**

Wireless network cards or wireless network adapters (wireless network interface cards (NICs)) are cards that locate and communicate to an AP with a powerful signal, giving network access to the users. It is required on each device to connect to the wireless network. Laptops or desktop computers generally have built-in wireless NICs or have slots

to attach them. These include two types of plug-in cards. One is called a personal computer memory card international association (PCMCIA) card and the other is a peripheral component interconnect (PCI). Laptops have slots to insert the PCMCIA plug-in cards, whereas desktop computers have internal slots to add PCI cards. The functionality of a wired and a wireless network card is similar. The difference between the two cards is that a wired network card has a port to connect over a network, whereas a wireless network card has a built-in antenna to connect over a wireless network. Typically, computers having a PCI bus or USB ports can connect to the wireless NIC.

Data transmitted using an NIC provides the following features:

- Customization of the computer's internal data from parallel to series before transmission
- Division of data into small blocks which incorporates sending and receiving addresses
- It informs when to send the packets to the destination.
- It delivers the packet.

▪ **Wireless modem:**

A wireless modem is a device that allows PCs to connect to a wireless network and access the internet connection directly with the help of an ISP. They receive and transmit network signals to other units without a physical cable. Wi-Fi routers have the capacity to transmit an internet service within a confined range, whereas wireless modems can be used in almost any location where a mobile phone is present. Portable devices such as laptops, mobile phones, PDAs, etc., use wireless modems to receive signals over the air, similar to a cellular network. There are various types of wireless modems. Users can choose a wireless modem based on their requirements. The common types of wireless modems include:

- **Cards:** They are the oldest form of wireless connection. There are two types of cards, namely, data cards and connect cards, which are available from mobile providers and are used by laptops, PCs, and routers. They are small in size and easy to use.
- **USB sticks:** They connect quickly to the internet using a wireless modem. They resemble a universal serial bus (USB) flash drive and fit easily into the USB port of a laptop. Computers require installation of special drivers and software to use them. They are portable.
- Mobile hotspots
- Wireless routers

The following features are considered while deciding on a wireless modem:

- Speed of the modem
- Protocols it can support, such as ethernet, GPRS, integrated services digital network (ISDN), Evolution-data optimized (EVDO), Wi-Fi, CPCD
- Frequency band 900 MHz, 2.4 GHz, 23 GHz, 5 Hz

- Radio technique such as a DSSS or frequency hopping
- Total number of channels for transmitting and receiving data
- Maximum signal strength
- Full duplex or half duplex capability

▪ **Wireless bridge:**

A wireless bridge connects multiple LANs at the medium access control (MAC) layer. These bridges separate networks either logically or physically. They cover longer distances than APs. Few wireless bridges support point-to-point connections to an AP, while some support point-to-multipoint connections to several other APs. Wireless bridging helps in connecting two LAN segments through a wireless link. Two segments reside on the same subnet and look like two ethernet switches connected with a cable to all computers within the subnet. Broadcasts reach all the machines on that subnet allowing dynamic host configuration protocol (DHCP) clients in one segment to obtain the respective addresses from a DHCP server from a different segment. A wireless bridge can be used for connecting computers in one room to computers in another room without a cable.

▪ **Wireless repeater (range expanders):**

This device retransmits the existing signal captured from the wireless router or an AP to create a new network. It works as an AP and a station simultaneously. The clients who are too far away from the router or AP can integrate with the same WLAN via a repeater. It implies that this device extends the signal by taking it from a wireless AP and transmits it to the uncovered area. These repeaters require an omnidirectional antenna. They capture, boost, and retransmit the signals.

▪ **Wireless Router:**

A wireless router is a device in a WLAN which interconnects two types of networks using radio waves to the wireless enabled devices such as computers, laptops, and tablets. It functions as a router in the LAN, but also provides mobility to users. Wireless routers have the ability to filter the network traffic based on the sender's and receiver's IP address. A wireless router provides strong encryption, filters MAC addresses and controls SSID authentication.

▪ **Wireless gateways:**

A wireless gateway is a key component of a wireless network. It is a device that allows internet-enabled devices to access the network. It combines the functions of wireless APs and routers. Wireless gateways have the feature of network address translation (NAT), which translates the public IP into a private IP and DHCP.

▪ **Wireless USB adapter:**

A wireless USB adapter enables internet access via a USB port on a computer. It also supports communication links and syncs between two or more devices. There are three main varieties of a wireless adapter:

- Cellular
- Bluetooth
- Wi-Fi

▪ **Wireless Controller:**

The wireless LAN controller monitors and manages a large number of wireless access points and enables wireless devices to access a wireless network architecture, known as WLAN. It is typically a central point in the network, to which all wireless access points on the network are connected directly or indirectly.

**Antenna:**

An antenna is a device that is designed to transmit and receive electromagnetic waves at radio frequencies. It is a collection of metal rods and wires that captures radio waves and translates them into an electrical current. The size and shape of an antenna is designed depending on the frequency of the signal they are designed to receive.

- An antenna that receives high frequency signals is highly focused, whereas a low-gain antenna receives or transmits over a large angle.
- A transducer translates the RF fields into an alternating current (AC) and vice-versa.

**Functions of Antennas**

The following are the functions of antennas:

▪ **Transmission line:**

Antennas transmit or receive radio waves from one point to another. This power transmission takes place in free space through the natural media such as air, water, and earth. Antennas avoid power that is transmitted through other means.

▪ **Radiator:**

A radiator radiates energy powerfully. This radiated energy is transmitted through the medium. A radiator is always the size of half the wavelength.

▪ **Resonator:**

The use of a resonator is necessary in broadband applications. Resonances that occur must be attenuated.

**Antenna Characteristics**

The characteristics of an antenna are as follows:

- **Operating frequency band:** Antennas operate at a frequency band between 960 MHz and 1215 MHz.
- **Transmission power:** Antennas transmit power at 1200 W peak and 140 W on an average.

- **Typical gain:** Gain is the ratio of the power input to the antenna to the power output from the antenna. It is measured in decibels relative to an isotropic antenna (dBi). The gain is generally 3.0 dBi.
- **Radiation pattern:** The radiation pattern of an antenna is obtained in the form of a 3-dimensional plot and is generally represented in terms of two parameters, namely, elevation and azimuth.
- **Directivity:** The directivity gain of an antenna is the calculation of radiated power in a particular direction. It is generally the ratio of the radiation intensity in a given direction to the average radiation intensity.
- **Polarization:** It is the orientation of electromagnetic waves from the source. There are a number of polarizations such as linear, vertical, horizontal, circular, left hand circular polarized (LHCP), and right hand circular polarized (RHCP).

**There are five types of wireless antennas:**

- **Directional antenna:**

A directional antenna can broadcast and receive radio waves from a single direction. In order to improve the transmission and reception, a directional antenna is designed to work effectively in a specified direction. This also helps in reducing interference.

- **Omnidirectional antenna:**

Omnidirectional antennas radiate electromagnetic radiation in all directions. They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. These antennas are efficient in areas where wireless stations use the time-division multiple access technology. A good example of an omnidirectional antenna is the one used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of where it is.

- **Advantage:**

- Omnidirectional antennas can deal with signals from any direction.

- **Disadvantages:**

- The coverage area of an omnidirectional antenna may be limited owing to the interference of walls and other obstacles with the radiated signal.
- It is difficult for an omnidirectional antenna to work in an internal environment.

- **Parabolic grid antenna:**

A parabolic grid antenna relies on the principle of a satellite dish, however it does not have a solid backing. Instead, this type of antenna has a semi-dish formed by a grid made of aluminum wire. These grid parabolic antennas can achieve very long distance Wi-Fi transmissions by making use of the principle of a highly focused radio wave beam. This type of antenna can transmit weak radio signals millions of miles back to Earth.

- **Advantage:**

- This antenna is wind resistant.
- **Disadvantages:**
  - This antenna is expensive, since it requires a feed system for reflecting the radio signals.
  - In addition to the feed system, the antenna requires a reflector. Assembling of these components makes the installation time consuming.

▪ **Yagi antenna:**

Yagi antenna, also called as the Yagi-Uda antenna, is a unidirectional antenna commonly used in communications using the frequency band from 10 MHz to very high frequency (VHF) and ultra high frequency (UHF). The main objectives of this antenna are to improve the gain of the antenna and to reduce the noise level of the radio signal. It has a unidirectional radiation emission and response pattern and concentrates the radiation and response. It consists of a reflector, dipole, and directors. This antenna generates an endfire radiation pattern.

○ **Advantages:**

- A Yagi antenna has a good range and ease of aiming the antenna.
- The Yagi antenna is directional, focusing the entire signal in a cardinal direction. This results in high throughput.
- The installation and assembly of this antenna is easy and less time consuming as compared to other antennas.

○ **Disadvantage:**

- The antenna is very large, especially when built for high gain levels.

▪ **Dipole antenna:**

A dipole is a straight electrical conductor, measuring half a wavelength from end to end and is connected to the center of the RF feed line. This antenna is also called as a doublet antenna. It is bilaterally symmetrical, and thus is inherently a balanced antenna. A balanced parallel-wire RF transmission line usually serves this kind of an antenna.

○ **Advantages:**

- A dipole antenna offers balanced signals. With the two-pole design, the device receives signals from a variety of frequencies.

○ **Disadvantages:**

- Although an indoor dipole antenna might be small, an outdoor dipole antenna can be much larger, making it difficult to manage.
- To achieve the perfect frequency, antennas are required to undergo multiple combinations. This can be a hassle especially in the case of outdoor antennas.

- **Reflector antennas:**

Reflector antennas are used for concentrating electromagnetic energy that is radiated or received at a focal point. These reflectors are generally parabolic.

- **Advantages:**

- If the surface of the parabolic antenna is within the tolerance limit, it can be used as a primary mirror for all the frequencies. This can prevent interference while communicating with other satellites.
- The larger the antenna reflector in terms of wavelengths, the higher is the gain.

- **Disadvantage:**

- Reflector antennas reflect radio signals.
- The manufacturing cost of the antenna is high.

- **Semi-directional antenna:**

A semi-directional antenna is a type of antenna that uses radio frequency (RF) signals to send and receive signals from one place to another. It's used for communication over short to medium distances, whether it's inside or outside.

- **Aperture Antenna:**

An aperture antenna is a type of antenna that has an opening that allows electromagnetic waves to be transmitted or received. It is typically used in aeroplanes or spacecraft.



---

**LO#02: Understand the encryption mechanisms used in wireless networks**

---

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

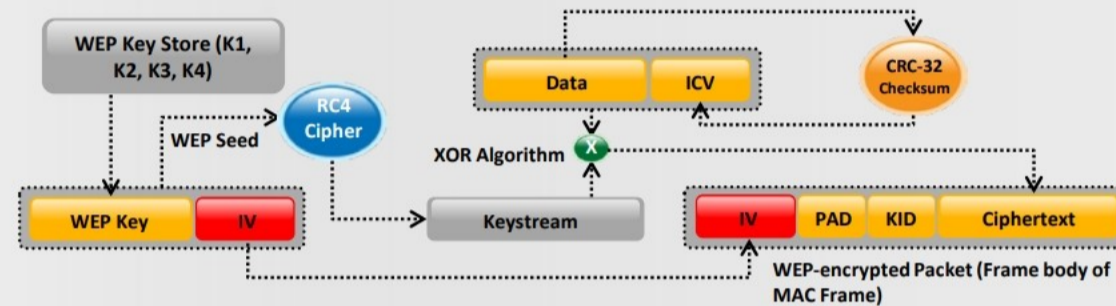
### **LO#02: Encryption Mechanisms Used in Wireless Networks**

The objective of this section is to explain the various encryption mechanisms used in wireless networks, such as WEP encryption, wireless fidelity (Wi-Fi) protected access (WPA) Encryption, Wi-Fi protected access 2 (WPA2) encryption, Wi-Fi protected access 3 (WPA3) encryption. This section also describes the limitations of these encryption mechanisms.

## Wired Equivalent Privacy Encryption



- Wired Equivalent Privacy (WEP) is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to a wired LAN
- A 24-bit arbitrary number known as an initialization vector (IV) is added to the WEP key. The WEP key and the IV together are called as a **WEP seed**.
- The 64-, 128-, and 256-bit WEP versions use 40-, 104-, and 232-bit keys respectively.
- The WEP seed is used as the input for the **Rivest cipher 4 (RC4) algorithm** to generate a keystream (the keystream is bit-wise XORed with the combination of data and integrity check value (ICV) to produce the encrypted data.)
- The **32-bit cyclic redundancy check algorithm (CRC-32) checksum** is used for calculating a 32-bit ICV for the data which, in turn, is added to the data frame.
- The IV field (IV+PAD+KID) is added to the **cipher text** to generate an MAC frame.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wired Equivalent Privacy Encryption

The 802.11 MAC implementation specifies a protocol called wired equivalent privacy (WEP). The objective of WEP is to make the WLAN communication as trustworthy as a wired LAN communication. WEP contributes two vital segments to the architecture of wireless security. They are the validation of data and the secrecy of the data. WEP uses a mechanism in which a key is used in common with a cipher, called Rivest cipher 4 (RC4), that is symmetric.

A standard 64-bit WEP is used as a string of 10 hexadecimal (base 16) characters (0-9, A-F). Each character has 4 bits and 10 digits of 4 bits is  $10 \times 4 = 40$  bits (WEP-40). The 40 bit keys are attached to another 24 bit initialization vector (IV) which completes the 64-bit WEP ( $4 \times 10 = 40$  bits + 24-bit IV = 64-bit WEP key).

Another WEP standard used is the 128-bit WEP which uses a 104-bit key. The 128-bit key is entered as a 26 hexadecimal character. Here,  $26 \text{ digits} \times 4 \text{ bits} = 104\text{-bit key}$ . Once again, adding a 24-bit IV gives  $104\text{-bit} + 24 \text{ bit} = 128\text{-bit WEP key}$ .

Similarly, 152-bit and 256-bit WEP are also available which use a 128-bit and a 232-bit key respectively. Adding the 24-bit IV to the 128-bit key and 232-bit key provides the 152-bit and 256-bit WEP.

Following are the steps involved in the working of WEP when using RC4:

- Packets to be transmitted are passed through an integrity check algorithm in order to generate a checksum (the checksum avoids a message from being changed).
- The 24-bit IV together with a 40-bit WEP key produces the 64-bit key.
- RC4 uses this key to generate the key stream. The key stream should have the same length as the plain text or the original message along with the checksum included.

- The keystream is exclusive ORed (XORed) with the original message or the plain text along with the checksum. This generates a cipher text or an encrypted packet.
- The client on the other hand, receives the encrypted text and XORs it with the same key stream to generate the plain text or the original message. The client validates with the checksum in order to authenticate the message.

### Problems with WEP

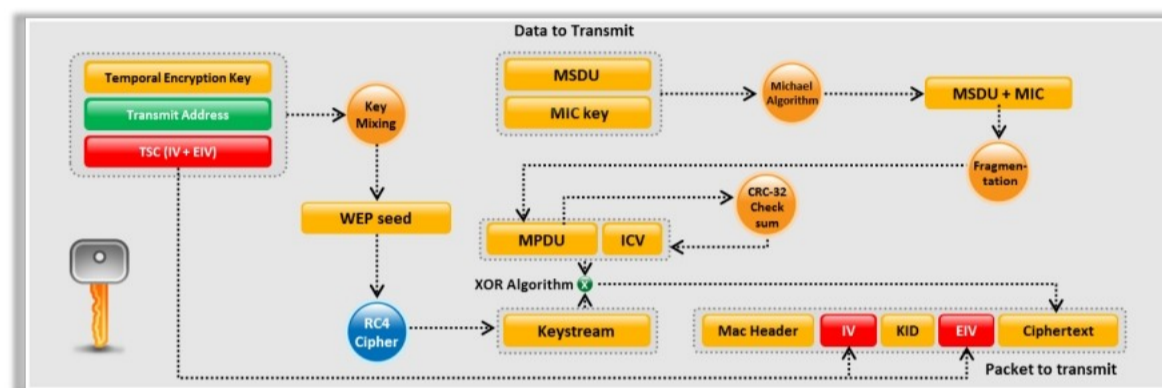
WEP has the following problems:

1. The 32-bit cyclic redundancy check algorithm (CRC32) is insufficient to ensure complete cryptographic integrity of a packet:
  - By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
2. IVs are 24-bit:
  - An AP broadcasting 1500 byte packets at 11 Mb/s would exhaust the entire IV space in five hours.
3. Known plaintext attacks:
  - When there is an IV collision, it becomes possible to reconstruct the RC4 key stream based on IV and the decrypted payload of the packet.
4. Dictionary attacks:
  - WEP is based on a password.
  - The small space of the IV allows the attacker to create a decryption table, which is nothing but a dictionary attack.
5. Denial-of-service:
  - Associate and disassociate messages are not authenticated.
6. An attacker can eventually construct a decryption table of the reconstructed key streams:
  - With about 24 GB of space, an attacker can use this table to decrypt WEP packets in real-time.
7. The lack of a centralized key management makes it difficult to change the WEP keys with any regularity.
8. IV is a value that is used for randomizing the key stream value, and each packet has an IV value:
  - The standard allows only 24 bits that can be used within hours at a busy AP.
  - IV values can be reused.
9. The standard does not dictate that each packet must have a unique IV, and thus vendors use only a small amount of the available 24-bit possibilities:
  - A mechanism that depends on randomness is not truly random and attackers can easily figure out the key stream and decrypt other messages.

## Wi-Fi Protected Access Encryption



- Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. It uses a TKIP that utilizes the **RC4 stream cipher encryption** with 128-bit keys and 64-bit message integrity check (MIC) in order to provide strong encryption and authentication
- The temporal encryption key, the transmit address, and the TKIP sequence counter (TSC) are used as the input for the RC4 algorithm to generate a **keystream**
- A MAC service data unit (MSDU) and MIC are combined using the **Michael algorithm**.
- The combination of the **MSDU** and the **MIC** is fragmented in order to generate the MAC protocol data unit (MPDU)
- A 32-bit ICV is calculated for the MPDU and the combination of the MPDU and the ICV is then bit-wise XORed with the keystream to produce the **encrypted data**.
- The IV is added to the encrypted data to generate the **MAC frame**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Wi-Fi Protected Access Encryption

Wireless fidelity (Wi-Fi) protected access (WPA) is used as a security standard for Wi-Fi connections. WPA provides refined data encryption and user authentication techniques. WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended IVs and re-keying mechanisms.

WEP normally uses a 40-bit or 140-bit encryption key, whereas TKIP uses 128-bit keys for each packet. The message integrity check for WPA avoids the chances of the attacker changing or resending the packets. TKIP uses a Michael integrity check algorithm with a message integrity check (MIC) key to generate the MIC value.

WPA requires 802.1x authentication and changes the unicast and global encryption keys. TKIP is used in a unicast encryption key, which changes the key for every packet, thereby enhancing the security. This change in key for each packet is coordinated between the client and the AP. In a global encryption key, the APs advertise the change in the key to the connected wireless clients.

#### What is a TKIP?

TKIP is comprised of three main elements that increase encryption:

- A key integration function for individual packets.
- An enhanced MIC function named Michael.
- An improved IV including the sequencing guidelines.

TKIP is a short-term fix for WEP, organized as a simple software/firmware upgrade. A number of design weaknesses have been incorporated in order to sustain reverse compliance with the large number of existing hardware in the field. TKIP detects all of the identified weaknesses linked with WEP.

The following steps are involved in the working of WPA:

- The IV or the temporal key sequence, the transmit address or the MAC destination address, and the temporal key are combined with a hash function or a mixing function to generate a 128-bit and a 104-bit key. This key is then combined with RC4 to produce the keystream which should be of the same length as the original message.
- The MAC destination and source addresses and the MIC keys are combined with a hash function in order to produce the MIC value.
- The MIC value is fragmented to produce the MAC protocol data unit (MPDU). The checksum is later attached to the MPDU.
- The MPDU along with the checksum is XORed with the keystream to produce the cipher text.
- This cipher text may be XORed again by the client using the same keystream in order to produce the original message

### Types of WPA

1. **WPA-Personal:** This version makes use of setup passwords and protects unauthorized network access.
2. **WPA-Enterprise:** It confirms the network user through a server.

### Features of WPA

- **WPA authentication:** WPA requires 802.1x authentication. It uses a pre-shared key (PSK) for the environment without the remote authentication dial-in use service (RADIUS) infrastructure and uses the extensible authentication protocol (EAP) and RADIUS for environments with a RADIUS infrastructure.
- **WPA key management:** It is necessary to change both the unicast and global encryption keys while using WPA. TKIP keeps changing the key for every frame when using an unicast key. In the case of a global key, WPA enforces the wireless AP to report the changed key to the connected wireless clients.
- **Temporal key management:** In WPA, encryption with TKIP is required. TKIP changes the WEP using a new encryption algorithm that is stronger than the standard WEP algorithm.
- **Michael algorithm:** 802.11 and WEP data uses a 32-bit integrity check value (ICV) to check the message integrity. In WPA, the Michael technique identifies the algorithm that determines an 8-byte MIC with the help of the methods present in the wireless devices.
- **AES Support:** WPA supports AES as a substitute for WEP encryption. This support is optional and depends on the vendor driver support.
- **Supporting a mixture of WPA and WEP wireless clients:** A wireless AP maintains both WEP and WPA simultaneously in order to help the gradual transition of WEP-based wireless networks to WPA.

## Wi-Fi Protected Access 2 Encryption



- Wi-Fi protected access 2 (WPA2) is an **upgrade to WPA**. It includes mandatory support for counter mode cipher block chaining (CBC)-MAC protocol (control mode CBC-MAC protocol or CCMP), **an AES-based encryption mode** with strong security

### WPA2-Personal

- WPA2-Personal uses a setup password (**pre-shared key** (PSK)) to protect unauthorized network access
- In the PSK mode, each wireless network device encrypts the network traffic using a **128-bit key** that is derived from a passphrase of 8 to 63 ASCII characters

### WPA2-Enterprise

- It includes **EAP** or **RADIUS** for a centralized client authentication using multiple authentication methods such as token cards, Kerberos, certificates, etc.
- Users are assigned **login credentials** by a centralized server which they must present when connecting to the network

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wi-Fi Protected Access 2 Encryption

Wi-Fi protected access 2 (WPA2) depends on the IEEE 802.11i standard for data encryption and has replaced the WPA technology in 2006. This protocol provides better protection compared to WPA and WEP. It uses AES to encrypt the data over wireless networks and supports the counter mode cipher block chaining (CBC)-MAC protocol (counter mode CBC-MAC protocol or CCMP) encryption mechanism.

There are two modes of authentication in WPA2:

- WPA2-Personal:** This mode is mostly used in home networks. It supports homes or locations where authentication servers are not used. Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. The router uses a combination of a passphrase, a network SSID and a TKIP to generate a unique encryption key for each wireless client. These encryption keys keep changing constantly.
- WPA2-Enterprise:** This mode is mostly used for securing wireless networks in organizations. It supports networks that include the authentication servers. It uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates, etc. WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent sharing of keys.

### Working of WPA2

During a CCMP implementation, additional authentication data (AAD) are generated using a MAC header and are included in the encryption process which uses both AES and CCMP encryptions. As a result, it protects the non-encrypted portion of the frame from alteration or distortion. The protocol uses a sequenced packet number (PN) and a portion of the MAC header to generate a

nonce which it uses in the encryption process. The protocol gives plaintext data, temporal keys, AAD, and nonce as the input to the encryption process that uses the AES and CCMP algorithms. A PN is included in the CCMP header to protect against replay attacks. The results from the AES and the CCMP algorithms produce encrypted text and an encrypted MIC value. The assembled MAC header, CCMP header, encrypted data, and encrypted MIC forms the WPA2 MAC frame. The following diagram depicts the functions of WPA2.

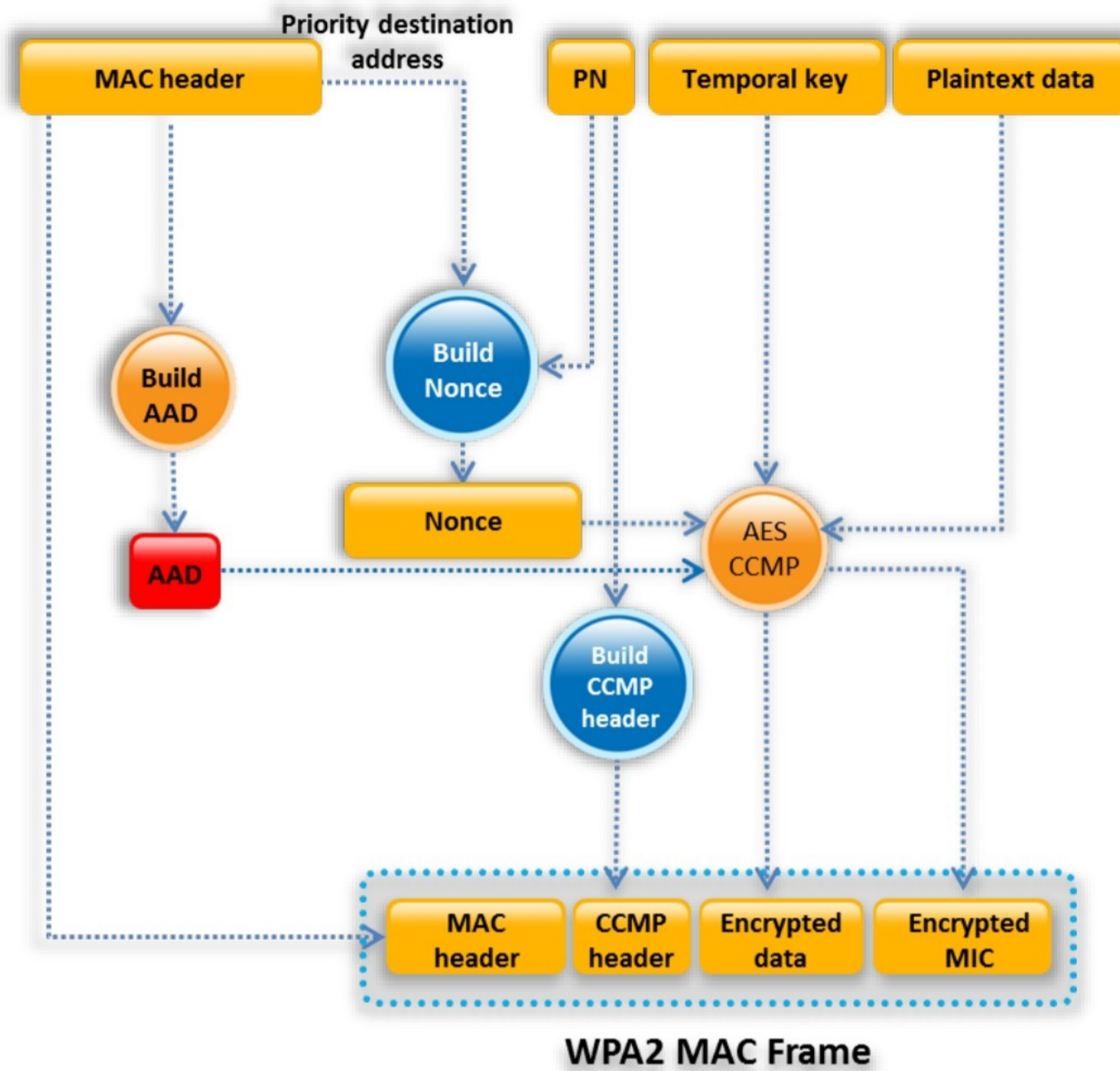



Figure 13.1 : Schematic showing the working of WPA2.

- Additional authentication data is taken from the MAC header in order to add to the implementation of the CCMP implementation of WPA2.
- The packet number (PN) attached in the CCMP header creates the nonce used for the encryption process.

## Wi-Fi Protected Access 3 Encryption



- Wi-Fi protected access 3 (WPA3) is the advanced implementation of WPA2, providing trailblazing protocols and uses **AES-Galois/counter mode protocol (GCMP) 256-bit** encryption algorithm

### Modes of Operation

#### WPA3 - Personal

- It is mainly used for delivering **password-based authentication** using the simultaneous authentication of equals (SAE) protocol, also known as dragonfly key exchange.
- It is resistant to offline dictionary attacks and key recovery attacks.

#### WPA3 - Enterprise

- It protects sensitive data by using many **cryptographic algorithms**
- It provides authenticated encryption using GCMP-256
- It uses the hashed message authentication mode using the secure hash algorithm (HMAC-SHA-384) to generate the cryptographic keys
- It uses the elliptic curve digital signature algorithm (ECDSA-384) for exchanging keys

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wi-Fi Protected Access 3 Encryption

Wi-Fi protected access 3 (WPA3) was announced by Wi-Fi Alliance on January 2018 as the advanced implementation of WPA2 and providing trailblazing protocols. The WPA3 protocol provides two variants similar to WPA2, i.e., WPA3-Personal mode and WPA3-Enterprise mode.

WPA3 provides cutting-edge features to simplify Wi-Fi security and provides capabilities necessary for supporting different network deployments ranging from corporate networks to home networks. It provides cryptographic consistency by using encryption algorithms such as AES, TKIP, etc., to defend against network attacks. It provides network resilience through protected management frames (PMF) that delivers a high-level of protection against eavesdropping and forging attacks. It disallows outdated legacy protocols.

### Modes of Operations

WPA3 offers the following two modes of operations:

- **WPA3-Personal:** This mode is mainly used to deliver password-based authentication. WPA3 is more rigid to attacks as it uses the modern key establishment protocol, termed as simultaneous authentication of equals (SAE) which is also known as dragonfly key exchange that replaces the concept of PSK used in the WPA2-Personal mode.

WPA3-Personal mode offers the following features:

- **Resistant to offline dictionary attacks:** It prevents passive password attacks such as brute-force passwords.
- **Resistant to key recovery:** Even when a password is determined, it is highly impossible to capture and determine the session keys maintaining the forward secrecy of network traffic.

- **Natural password choice:** It allows users to choose passwords such as weak or popular phrases, which are easier to remember.
- **Easy accessibility:** It can provide robust protection without changing the previous methods used by the users for connecting to a network.
- **WPA3-Enterprise:** This mode is based on WPA2. It offers better security across the network and protects sensitive data by using many cryptographic concepts and tools.

Some of the security protocols used by WPA3-Enterprise mode are as follows:

- **Authenticated encryption:** It helps in maintaining the authenticity and confidentiality of the data. For this, WPA3 uses 256-bit Galois/counter mode protocol (GCMP-256).
- **Key derivation and validation:** It helps in generating a cryptographic key from a password or master key. It uses a 384-bit hashed message authentication mode (HMAC) using the secure hash algorithm and this is termed as HMAC-SHA-384.
- **Key establishment and verification:** It helps in exchanging cryptographic keys among two parties. For this purpose, WPA3 uses the elliptic curve Diffie-Hellman (ECDH) exchange and elliptic curve digital signature algorithm (ECDSA) using a 384-bit elliptic curve.
- **Frame protection and robust administration:** WPA3 uses a 256-bit broadcast/multicast integrity protocol Galois message authentication code (BIP-GMAC-256).

## WEP vs. WPA vs. WPA2 vs. WPA3



Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1- 2 <sup>64</sup>	192-bits	ECDH and ECDSA	BIP-GMAC-256



WEP, WPA	❌	Should be replaced with more secure WPA and WPA2
WPA2	✅	Incorporates protection against forgery and replay attacks
WPA3	✅	Provides enhanced password protection, secured IoT connections and encompasses stronger encryption techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### WEP vs. WPA vs. WPA2 vs. WPA3

WEP initially provided data confidentiality on wireless networks. However, it was weak and failed to meet any of its security goals. WPA fixed most of the problems of WEP. WPA2 makes wireless networks almost as secure as wired networks. WPA2 supports authentication, so that only authorized users can access the network. WEP should be replaced with either WPA or WPA2 in order to secure a Wi-Fi network. Though WPA and WPA2 incorporate protection against forgery and replay attacks, WPA3 can provide an enhanced password protection mechanism and secured internet of things (IoT) connections, and it encompasses stronger encryption techniques. The table shows a comparison between WEP, WPA, WPA2, and WPA3 in terms of the encryption algorithm used, size of the encryption key, the IV it produces, key management, and data integrity.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1- 2 <sup>64</sup>	192-bits	ECDH and ECDSA	BIP-GMAC-256

Table 13.2: Differences between WEP, WPA, WPA2, WPA3

## Issues in WEP, WPA, and WPA2

### Issues in WEP:

Why is WEP encryption inefficient in securing wireless networks? The answers lie in the following issues and anomalies of WEP:

- **CRC32 is inefficient in ensuring complete cryptographic integrity of a packet:** By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- **IVs are 24-bit:** The IV is a 24-bit field, which is too small, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mb/s would exhaust the entire IV space in five hours.
- **Known plaintext attacks:** In the case of occurrence of an IV collision, it becomes possible to reconstruct the RC4 key stream based on the IV and the decrypted payload of the packet.
- **Dictionary attacks:** WEP is based on a password and is prone to password cracking attacks. The small space of the IV allows the attacker to create a decryption table, which is a dictionary attack.
- **Denial-of-Service:** Associate and disassociate messages are not authenticated.
- **An attacker can eventually construct a decryption table of the reconstructed key streams:** With about 24 GB of space, an attacker can use this table to decrypt WEP packets in real-time.
- **A lack of centralized key management makes it difficult to change WEP keys with any regularity.**
- **IV is a value that is used to randomize the key stream value and each packet has an IV value:** The standard IV allows only a 24-bit field, which is too small, and is sent in the cleartext portion of a message. It is used within hours at a busy AP. IV is a part of the RC4 encryption key and leads to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic. Identical key streams are produced with the reuse of the same IV for data protection, since the IV short key streams are repeated within a short time. Wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the key stream and decrypt the ciphertext.
- **The standard does not dictate that each packet must have a unique IV, and thus vendors use only a small part of the available 24-bit possibilities:** A mechanism that depends on randomness is not truly random and the attackers can easily figure out the key stream and decrypt other messages.
- **Use of RC4 was designed to be a one-time cipher and not intended for multiple message use.**

- **An attacker can construct a decryption table of the reconstructed key stream and can use it to decrypt the WEP packets in real-time.**

Since most organizations have configured their network clients and APs to use the same shared key, or the four default keys, the randomness of the key stream relies on the uniqueness of the IV value. The use of IV and a key ensures that the key stream for each packet is different. However, in most cases, the IV changes, whereas the key remains constant. Since there are only two main components to this encryption process and only one remains constant, the randomization of the process decreases to an unacceptable level. A busy AP can use all 224 available IV values within hours, which requires the reuse of IV values. Repetition in a process that relies on randomness, leads to failure.

The point that makes the IV issue worse is that the 802.11 standard does not require each packet to have a different IV value. This is similar to having a “Beware of Dog” sign posted, but only a Chihuahua to provide a barrier between intruders and the valued assets. In many implementations, the IV value changes only when the wireless NIC reinitializes, usually during a reboot. IV values having 24 bits provide enough possible IV combinations, however most implementations use a handful of bits, not even utilizing all the available bits completely.

The following are the reasons for generating weak initialization vectors in WEP:

- To generate different packets in WEP, the RC4 algorithm uses a key scheduling algorithm (KSA) to create an IV and adds it to the base key, which makes the first few bytes of the plaintext easily predictable.
- The IV value is not explicit to the network, and thus the same IV can be used with the same secret key on multiple wireless devices.
- The way in which the IV is appended to the beginning of the security key makes it vulnerable to the Fluhrer-Mantin-Shamir (FMS) attacks, which allow attackers to execute script tools to crack the secret key by examining the link.
- Most of the weak IVs depends on a WEP key and reveal accurate information about the key bytes from the first RC4 output byte as well as smaller clues from other bytes.
- Using additional processing on the recovered bytes, parts of the pseudo-random generation algorithm (PRGA) can be emulated to extract the key information in the byte of an IV.
- There is no effective detection of message tampering. Although methods such as checksum and ICV can check the message integrity, they have certain drawbacks. Some secure methods for computing MIC require high computational processing when introduced to TKIP.
- WEP directly uses the master key and has no built-in provision to update the keys.

A security flaw in the WEP implementation of RC4 results in the generation of weak IVs, which attackers can easily exploit to deduce the base WEP key. An attacker can use WLAN sniffing tools to capture packets encrypted with the same key and use tools such as Aircrack-ng, WEPCrack, etc., to decrypt the weak IVs, thereby exposing the base WEP key.

### Issues in WPA:

WPA improves over WEP in many ways by using TKIP for data encryption and helps in a secured data transfer. However, WPA also suffers from various security issues.

Some of the security issues of WPA are as follows:

- **Weak password:** If users depend on weak passwords, the WPA pre-shared key is vulnerable to various password cracking attacks.
- **Lack of forward secrecy:** If an attacker is able to capture a pre-shared key, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted.)
- **Vulnerable to packet spoofing and decryption:** Clients using WPA-TKIP are vulnerable to packet injection attacks and decryption attacks and this further allows attackers to hijack the transmission control protocol (TCP) connections.
- **Predict the group temporal key:** An insecure random number generator (RNG) in WPA allows attackers to discover the group temporal key (GTK) generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the traffic that is being transmitted over the internet.
- **Guessing an IP address:** Vulnerabilities in TKIP allow attackers to guess the IP address of the subnet and inject small packets onto the network to downgrade the network performance.

### Issues in WPA2:

WPA2 is more secure than WEP and WPA, but also has some security issues which are discussed below:

- **Weak password:** If users depend on weak passwords, the WPA2 pre-shared key is vulnerable to various attacks such as eavesdropping, dictionary, and password cracking attacks.
- **Lack of forward secrecy:** If an attacker is able to capture a pre-shared key, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted.)
- **Vulnerable to man-in-the-middle and denial-of-service attacks:** The Hole 96 vulnerability in WPA2 allows attackers to exploit a shared GTK to perform man-in-the-middle and denial-of-service (DoS) attacks.
- **Predict the GTK:** An insecure RNG in WPA2 allows attackers to discover GTK generated by the AP. This further allows the attackers to inject malicious traffic in the network and decrypt all the traffic that is being transmitted over the internet.
- **Key reinstallation attack vulnerabilities:** WPA2 has a significant vulnerability known as a key reinstallation attack (KRACK). This exploit may allow attackers to perform packet sniffing, hijacking connections, injecting malware, and decrypting the packets.

- **Wireless DoS attack:** Attackers can exploit the WPA2 replay attack detection feature to send forged group addressed data frames with a large PN to perform a DoS attack.
- **Wi-Fi protected setup PIN recovery:** In some cases, disabling WPA2 and Wi-Fi protected setup (WPS) can be a time-consuming process, where the attacker needs to control the WPA2 PSK used by the clients. When the WPA2 and WPS are enabled, the attacker can easily disclose the WPA2 key by finding out the WPS PIN by using simple steps.

## Wi-Fi Easy Connect/ Device Provisioning Protocol (DPP)

Wi-Fi Easy Connect (Device Provisioning Protocol (DPP)), **simplifies and enhances** the security of Wi-Fi device provisioning and network setup while minimizing security risks

**The following are some of the DPP security features**

- DPP establishes secure communications between the device being provisioned and the provisioning device (such as a smartphone or tablet) with **public key cryptography**
- DPP uses PKI (**Public Key Infrastructure**) to manage and distribute public key and ensures the authenticity of the public keys used for secure communication
- DPP utilizes **QR codes to transfer network information** such as network SSID, network credentials, and cryptographic keys between the provisioning device and the new device. This prevents eavesdropping compared to manual entry
- DPP provides **passwordless Wi-Fi configuration**, which enables the setup of Wi-Fi connections without pre-shared keys (PSKs) or passwords. This reduces the risk of password-related attacks
- DPP allows **mutual authentication**, meaning both the provisioning device and the device being added to the network verify each other's authenticity and prevents rogue devices from joining the network
- DPP uses **forward secrecy** as it generates unique keys for each provisioning session. Hence, if a long-term key is compromised, it cannot be used to decrypt past or future provisioning sessions.
- Some DPP implementations leverage tamper-resistant hardware, such as **hardware security modules (HSMs)**, to store and protect sensitive cryptographic keys
- DPP allows **network segment** creation, so IoT devices can be provisioned securely and isolated from more sensitive network segments

**1. Scan the QR code to establish a network**

**2. Scan the Client device to enroll device**

**3. Connected devices on network**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Wi-Fi Easy Connect/ Device Provisioning Protocol

Wi-Fi Easy Connect (Device Provisioning Protocol (DPP)), simplifies and enhances the security of Wi-Fi device provisioning and network setup while minimizing security risks. It incorporates the highest security standards as well. It brings consistency, flexibility, simplicity to Wi-Fi network management.

The following are some of the DPP security features:

- DPP establishes secure communications between the device being provisioned and the provisioning device (such as a smartphone or tablet) with public key cryptography.
- DPP uses public key infrastructure (PKI) to manage and distribute public key and ensures the authenticity of the public keys used for secure communication.
- DPP utilizes QR codes to transfer network information such as network SSID, network credentials, and cryptographic keys between the provisioning device and the new device. This prevents eavesdropping compared to manual entry.
- DPP enables passwordless Wi-Fi configuration, which enables the setup of Wi-Fi connections without pre-shared keys (PSKs) or passwords. This reduces the risk of password-related attacks.
- DPP allows mutual authentication, meaning both the provisioning device and the device being added to the network verify each other's authenticity and prevent rogue devices from joining the network.
- DPP uses forward secrecy as it generates unique keys for each provisioning session. Hence, if a long-term key is compromised, it cannot be used to decrypt past or future provisioning sessions.

- Some DPP implementations leverage tamper-resistant hardware, such as hardware security modules (HSMs), to store and protect sensitive cryptographic keys.
- DPP allows network segment creation, so IoT devices can be provisioned securely and isolated from more sensitive network segments.

### Working of Wi-Fi Easy Connect

With Wi-Fi Easy Connect, one device which is rich in user interface (such as a smart phone) is chosen as the central point of configuration. This device must have the capability to scan a QR code, or NFC tag, or download device information from the cloud. This selected device is called a configurator and other devices are called enrollees. A secure connection is established between the configurator and enrollee by scanning the NFC tag or QR code or downloading data associated with the device from the cloud. This initiates the protocol, triggering the automated provisioning of the necessary credentials for the enrollee to gain network access.

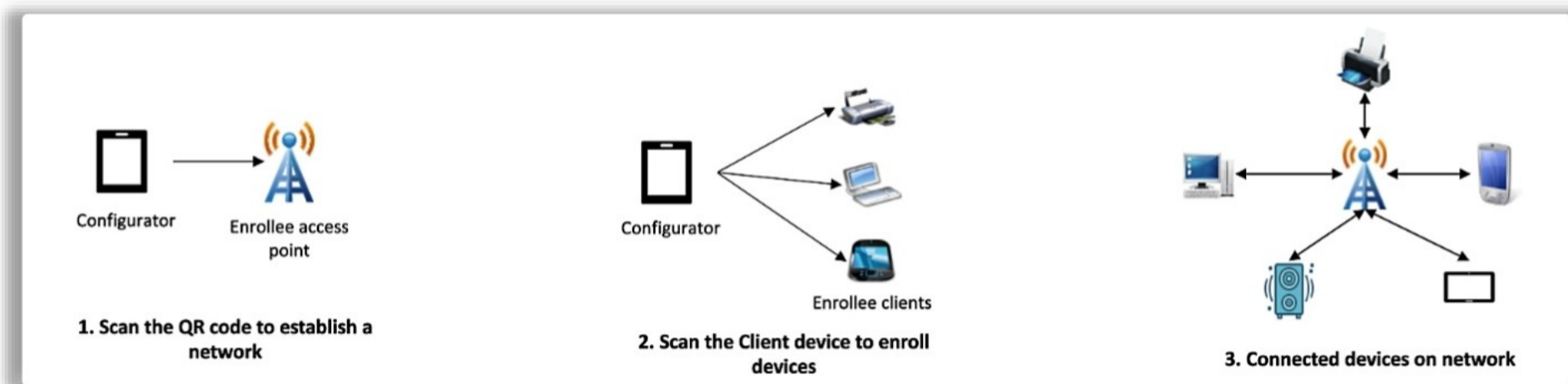


Figure 13.3: Connected Devices on the Network



---

**LO#03: Understand the authentication methods used in wireless networks**


---


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

**LO#03: Authentication Methods Used in Wireless Networks**


The objective of this section is to explain the various authentication methods such as the open system authentication, shared key authentication, etc., used in wireless networks.

## Open System Authentication

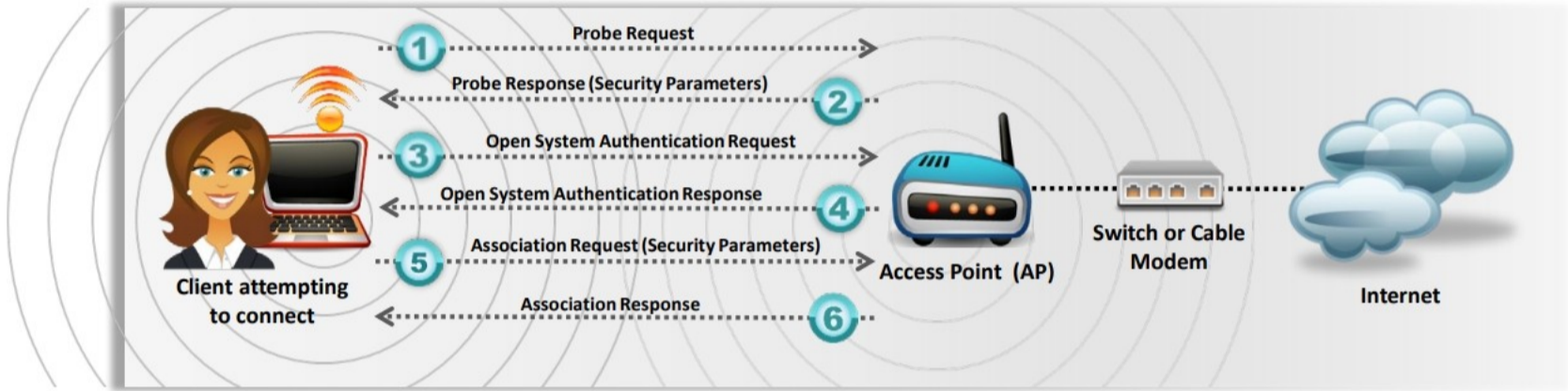




**Open System Authentication:**  
Any wireless device can be **authenticated** with the APs, allowing the device to transmit data only when its WEP key **matches** with the **WEP key** of the AP



**Open System Authentication Process**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Open System Authentication

Open system authentication is a null authentication algorithm that does not verify whether it is a user or a machine requesting network access. It uses cleartext transmission to allow the device to associate with an AP. In the absence of encryption, the device can use the SSID of an available WLAN to gain access to a wireless network. The enabled WEP key on the AP acts as an access control to enter the network. Any user entering the wrong WEP key cannot transmit messages via the AP even if the authentication is successful. The device can only transmit messages when its WEP key matches with the WEP key of the AP. This authentication mechanism does not depend on a RADIUS server on the network.

In the open system authentication process, any wireless client that wishes to access a Wi-Fi network sends a request to the wireless AP for authentication. In this process, the station sends an authentication management frame containing the identity of the sending station for authenticating and connecting with the other wireless stations. The AP then returns an authentication frame to confirm access to the requested station and completes the authentication process.

#### Advantage

- This mechanism can be used with wireless devices that do not support complex authentication algorithms.

#### Disadvantage

- There is no way to check whether someone is a genuine client or an attacker. Anyone who knows the SSID can easily access the wireless network.

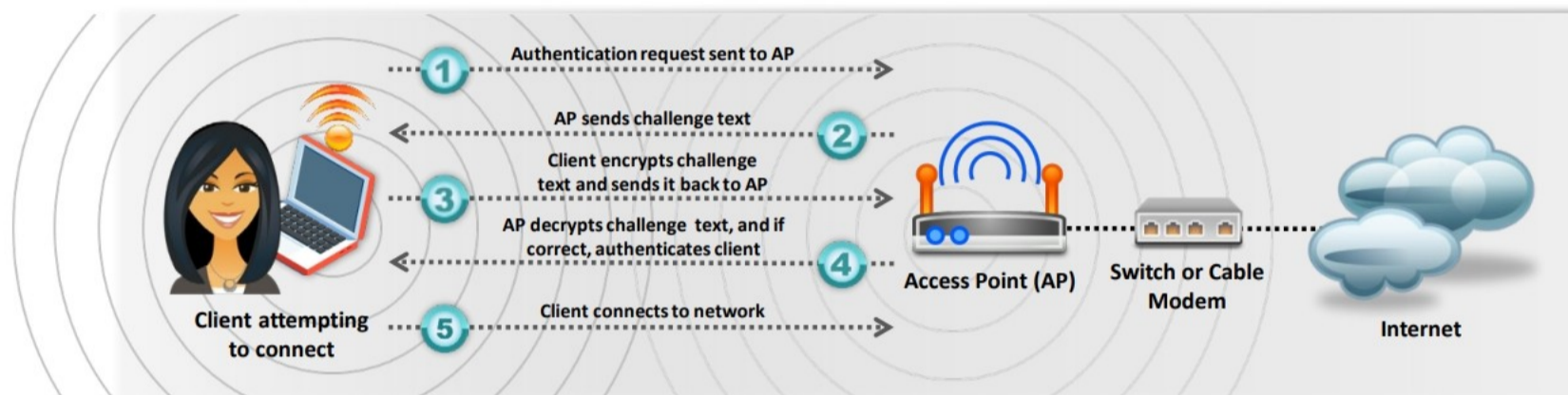
## Shared Key Authentication



### Shared Key Authentication:

The station and the AP use the **same WEP key** to provide authentication. This indicates that this key should be **enabled** and configured manually on both the **AP** and the **client**

### Shared Key Authentication Process



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Shared Key Authentication

In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels.

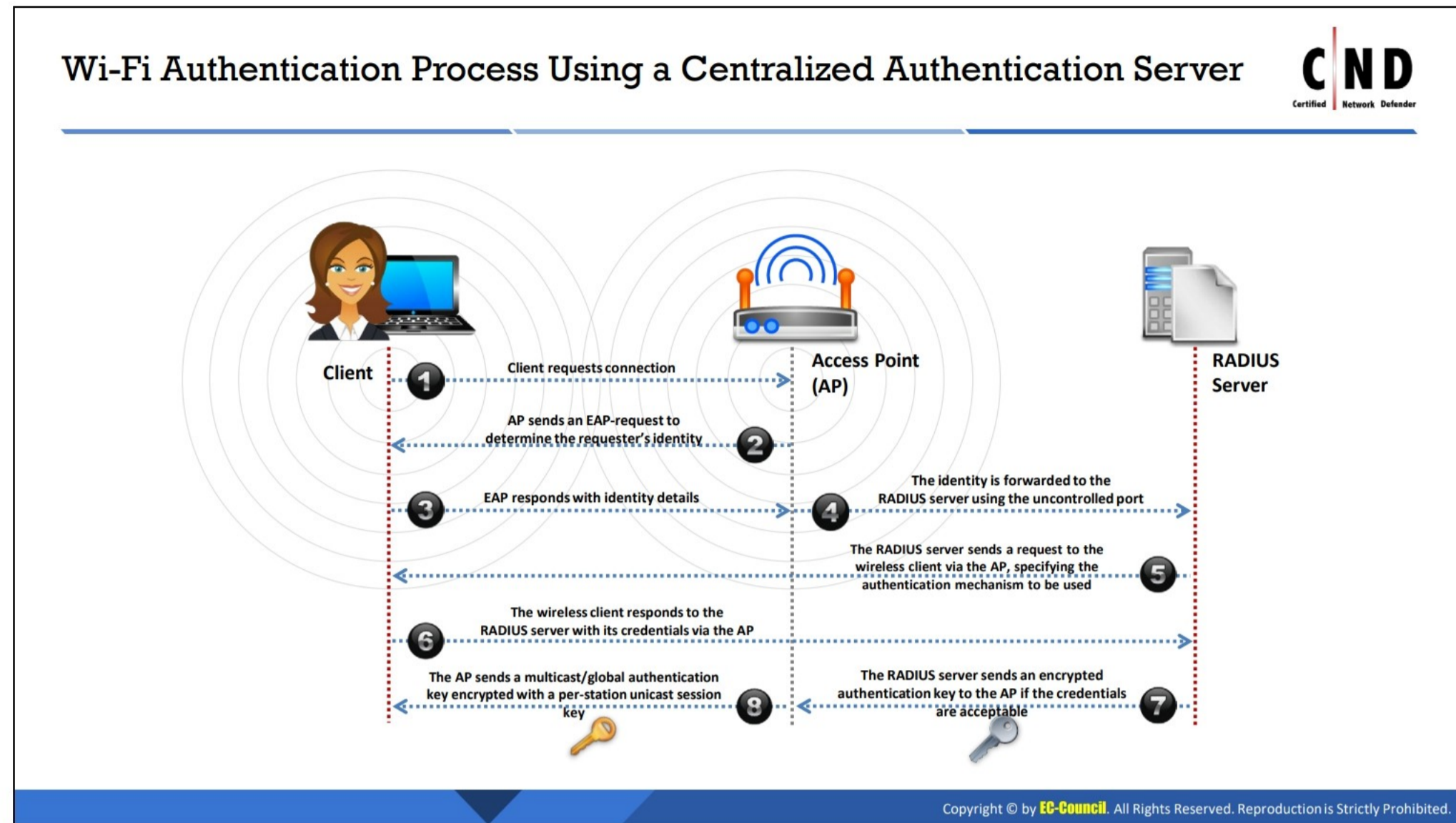
The following steps illustrate the establishment of a network connection using the shared key authentication process:

- The station sends an authentication frame to the AP.
- The AP sends the challenge text to the station.
- The station encrypts the challenge text by making use of its configured 64-bit or 128-bit key and sends the encrypted text to the AP.
- The AP uses its configured WEP key to decrypt the encrypted text. It compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, the AP authenticates the station.
- The station connects to the network.

The AP can reject the station if the decrypted text does not match the original challenge text. In this case, the station will be unable to communicate with either the ethernet network or the 802.11 network.

### Disadvantage

- This mechanism is not suitable for large networks, as it requires long-key strings configured on each device, which is a highly cumbersome task.



### Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1x standard provides centralized authentication. For 802.1x authentication to work on a wireless network, the AP must be able to securely identify the traffic from a specific wireless client. In this Wi-Fi authentication process, a centralized authentication server, namely RADIUS, sends the authentication keys to both the AP and the clients that want to authenticate with the AP. This key enables the AP to identify a particular wireless client.



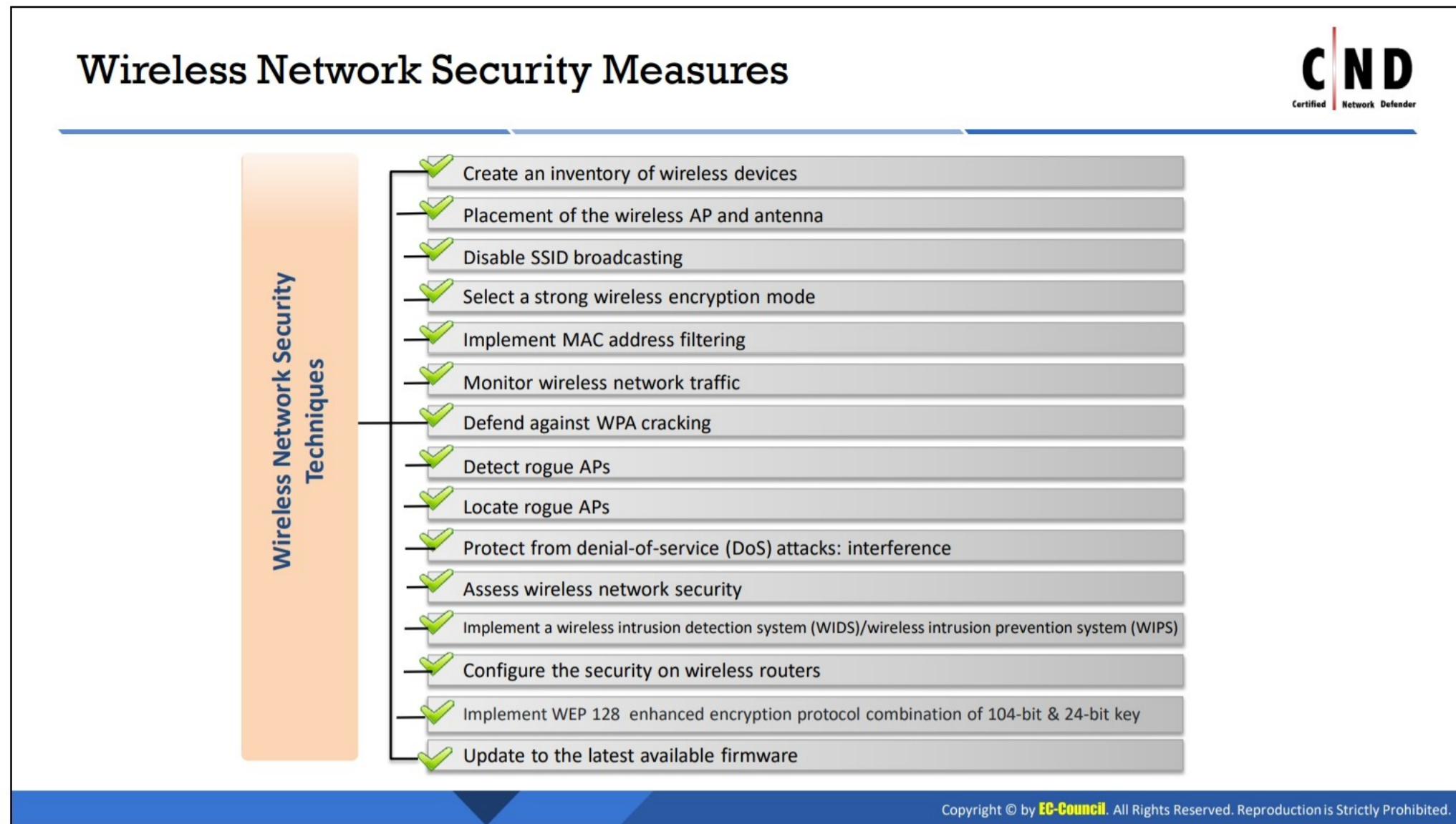
---

LO#04: Discuss the various security measures that must be implemented in wireless networks

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### **LO#04: Various Security Measures in Wireless Networks**

The objective of this section is to explain the various security measures that must be implemented to secure the wireless network.



## Wireless Network Security Measures

A wireless network can be insecure if proper care has not been taken while configuring it. Insecure configurations can pose a great risk to the wireless networks. Thus, a wireless network should be configured as per the wireless security policy of the organization.

The following points should be clearly stated in the organization's wireless security policy:

- Identity of the users who are using the network
- Determine whether the user is allowed access or not
- Clearly define who can and cannot install the APs and other wireless devices in the enterprise
- Describe the type of information that users are allowed to communicate over the wireless network
- Provide limitations on APs such as location, cell size, frequency, etc., in order to overcome the wireless security risks
- Clearly define the standard security settings for wireless components
- Describe the conditions in which wireless devices are allowed to use the network

Furthermore, a successful and effective wireless security implementation should involve the following:

- Centralized implementation of security measures for all wireless technology
- Security awareness and training programs for all employees

- Standardized configurations to reflect the security policies and procedures of the organization
- Configuration management and control to make sure the latest security patches and features are available on wireless devices.

The following activities help in defending and maintaining the security of a wireless network:

- Creating an inventory of the wireless devices
- Placement of the wireless AP and antenna
- Disable SSID broadcasting
- Selecting a strong wireless encryption mode
- Implementing MAC address filtering
- Monitoring wireless network traffic
- Defending against WPA cracking
- Detecting rogue APs
- Locating rogue access points
- Protecting from DoS attacks
- Assessing the wireless network security
- Deploying a wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS)
- Configuring the security on wireless routers
- Implement WEP 128 enhanced encryption protocol combination of 104-bit & 24-bit key
- Update to the latest available firmware

## Creating an Inventory of Wireless Devices



- Identify and document all the client devices according to the make/models/applications, encryption, firmware, wireless channel, etc.
- This helps the network defenders to **manage and monitor** the wireless devices in the network

#	Make	Model	Operating System	Strongest Authentication Mode	Best Firmware Level	802.11 Radio Type	Maximum Output Power
A	Intermec	CK31	Win CE .NET	WPA2/802.1x	4.20	b/g	17 dBm
B	Symbol	9090G	Windows Mobile	WPA2/802.1x	5.1.70	a/b/g	20 dBm
C	Vocollect	Talkman T5	Proprietary Voice	WPA-PSK	4.20	b only	12 dBm
D	Symbol	6846	MS-DOS	WEP	--	b only	20 dBm
E	Xybernaut	S310LX	Windows XP	WPA2/802.1x	5.0	a/b/g	20 dBm

Source: <http://www.acrylicwifi.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Creating an Inventory of Wireless Devices

The use of wireless devices in various organizations is continuously growing. Therefore, it becomes increasingly important for organizations to track and manage their wireless assets for security purposes. Maintaining an accurate and up-to-date inventory of wireless devices is required for proper security.

A network device inventory helps in consolidating all the updated network data and devices. The inventory can help in quickly identifying the non-functioning devices as well as rogue network devices that are present on the network. A list of devices that are not connected to the network should also be added to the list. This helps in detecting unknown devices in the network. A regular scanning of the inventory is important. Through scanning, the administrators can determine the rogue network devices, problematic devices, potential vulnerabilities, devices that need a patch/update, etc., in a network. A network is only as secure as its weakest link. Information about all the devices should be maintained regardless of their configuration settings or the vendor.

An inventory should be maintained either manually or with the help of an effective inventory tracking solution. At times, an inventory tool may not auto-update the network device. In such scenarios, information of a device should be manually added in the inventory list.

## Placement of a Wireless AP

- Proper mounting of a wireless AP is necessary to avoid outside access and **improve performance**
- No AP is ideal for all locations as AP vendors design their APs to be installed in **specific locations**
- An AP should be mounted in a location recommended by the manufacturer
- Guidelines for AP mounting:
  - Place APs in central locations
  - Install an AP on the ceiling
  - Avoid placing APs too high on ceilings
  - Avoid mounting an AP on a wall as it may restricts its 360° coverage
  - Avoid installing APs in corridors
  - Avoid installing APs above suspended ceilings
  - Use locks and a plastic sarel enclosure to secure the AP from theft
  - Avoid enclosing the AP in a metal cage
  - Keep the AP away from metal objects

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Placement of a Wireless AP

Choosing an appropriate location for an AP is very important as it plays a vital role in achieving a high network performance, coverage, and speed. Many organizations have their APs placed across their interior spaces. Every AP requires installation at a specific location and angle since their installation at random locations will restrict the network performance. In addition, the coverage area needs to be planned wisely. Overlap is good. Care must be taken to not create dead-zones.

The following guidelines help in choosing the appropriate locations for APs and to achieve maximum coverage, performance, and speed:

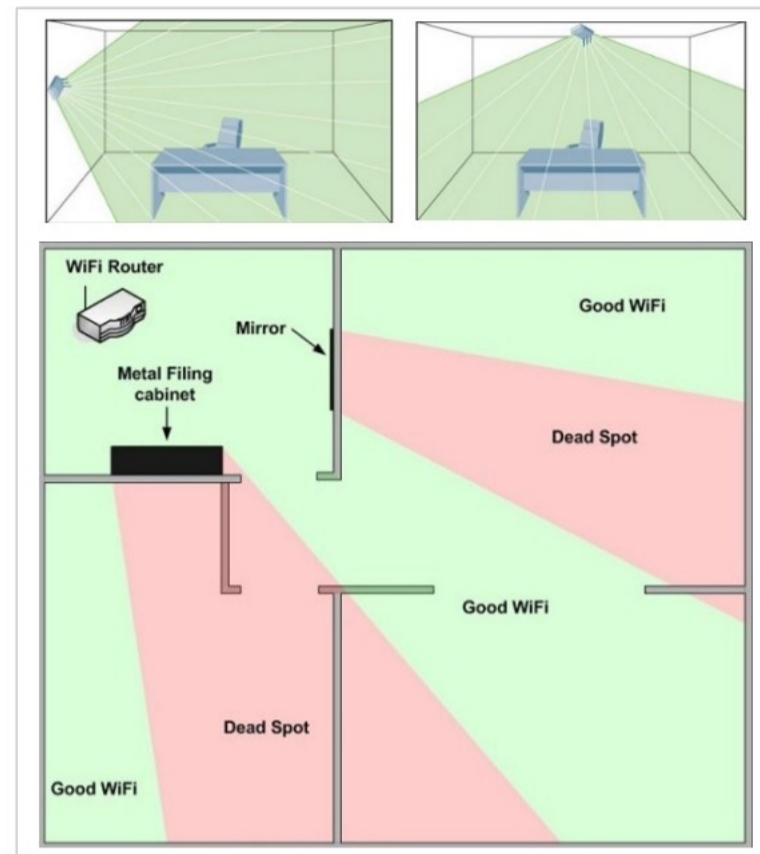
- APs with an antenna cover a circular area and can be obstructed by walls, metal shutters, or furniture. It is a good practice to set up APs at a location with no interference. An AP should be placed within the line of sight so that users can optimize the maximum network performance from it.
- The ideal placement of an AP is the ceiling. However, this location will not always be feasible in organizations having very high ceilings. Setting up an AP correctly on the ceiling is also important. An AP that is facing upwards will not provide good coverage and will drastically impact the network performance. It is beneficial to place the AP upside down to get an optimal network performance.
- Placing APs on a desk is not part of a good network infrastructure implementation. APs, if placed on a desk encounter large amounts of interference such as phones, Bluetooth devices, furniture, etc., which will nullify the wireless connectivity and affect the network performance of the organization. In addition, if an AP is on a desk, it is not secure and it is easier to tamper with and/or remove.

- APs placed near metal sources will reduce the range of travel. Metal interference acts as a mirror for APs. This also implies that APs should not be kept in a closet or in a metal case.
- Antennas of the external APs must not be pointed in the same direction. The antennas should always be tilted in opposite directions. Antennas facing upward are not part of an optimal network setup.

## Placement of a Wireless Antenna



- Placement of an antenna depends on the type, angle, and location of the AP, and the coverage required.
- Guidelines for antenna placement:
  - Use the trial and error method to select an appropriate location and direction.
  - Place the AP antenna in a **perpendicular direction**.
  - Avoid keeping the antenna at an angle of 45°
  - Point the antenna gain towards users
  - Know the antenna radiation patterns
  - Do not place obstructions or objects that interfere with the function of the antenna
  - The use of external antennas as integrated antennas has a limitation
  - Tilt the antennas downwards when installed on the ceiling
  - Use omnidirectional antennas pointing downwards for attenuating the signals traveling up to the AP
  - Avoid using simple dipole antennas as an optimal solution
  - Use single frequency antenna elements rather than dual tuned elements



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Placement of a Wireless Antenna

### Guidelines for the Placement of a Wireless Antenna

- A wireless device should be placed in the center of a room with proper positioning of the antennas. The antennas should be positioned vertically, especially in a spacious interior.
- Third party applications should be used for finding the best location for placing the device. Applications such as HeatMapper builds a map of the interior and on the basis of this map provides a guideline for placing the device in the best location.
- An appropriate band and channel must be chosen for the wireless antenna to work on. A reliable frequency starts from 2.4 GHz. A frequency that is compatible with the wireless device and which can travel through walls should be selected. For analyzing an appropriate channel, applications such as a WiFi Analyzer should be used.
- The wireless antenna should be replaced in order to achieve good networking results. Omnidirectional antennas that will help in improving the range of the wireless environment should be setup.
- Wireless devices should be avoided from being mounted near objects that interfere with electromagnetic radiation. Cathode-ray tube (CRT) televisions (TVs), monitors, and loudspeakers are some of the devices that should not be placed near the wireless device.
- The trial and error method should be used for determining the best location of the wireless device.

## Disable SSID Broadcasting



- If the SSID is broadcast, the AP will announce its presence and name, allowing everyone to attempt to authenticate and connect to the wireless network.
- The SSID broadcast should be **disabled**. In this scenario, an AP will only broadcast its presence, but not its name.
- This **discourages unauthorized association** requests to the network and permits connections from legitimate users to the wireless network who have the correct SSID.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Disable SSID Broadcasting

A wireless network SSID can either be broadcast or hidden. By broadcasting the SSID, anyone can find and access it. If the SSID is hidden, the user has to know the exact SSID in order to connect to the wireless network. Network defenders should always disable SSID broadcasting on their devices.

#### SSID Broadcast in the Enabled State

By enabling the SSID broadcast, the wireless router will broadcast its presence and name. When scanning for available wireless connections, if the SSID is broadcast, the name and presence of the network will be identified. It may be locked with a password, but anyone will be able to see it.

#### SSID broadcast in the Disabled State

If the SSID broadcast is disabled, then the wireless router will broadcast its presence, but will not display the name. Instead “unnamed network” will be displayed as a connection present within a user’s range. The user can connect to the wireless network after naming it and providing it with the correct authentication credentials.

## Selecting a Strong Wireless Encryption Mode

A strong **wireless encryption mode** should be selected for the wireless network.

**Order of preference for choosing an encryption mode :**

1. WPA3
2. WPA2 Enterprise with RADIUS
3. WPA2 Enterprise
4. WPA2 PSK
5. WPA Enterprise
6. WPA
7. WEP

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Selecting a Strong Wireless Encryption Mode

A strong wireless encryption mode should be used for keeping the wireless network safe from various types of attacks. There are various encryption modes that can be used for an organization's wireless network.


#### Order of preference for choosing an encryption mode

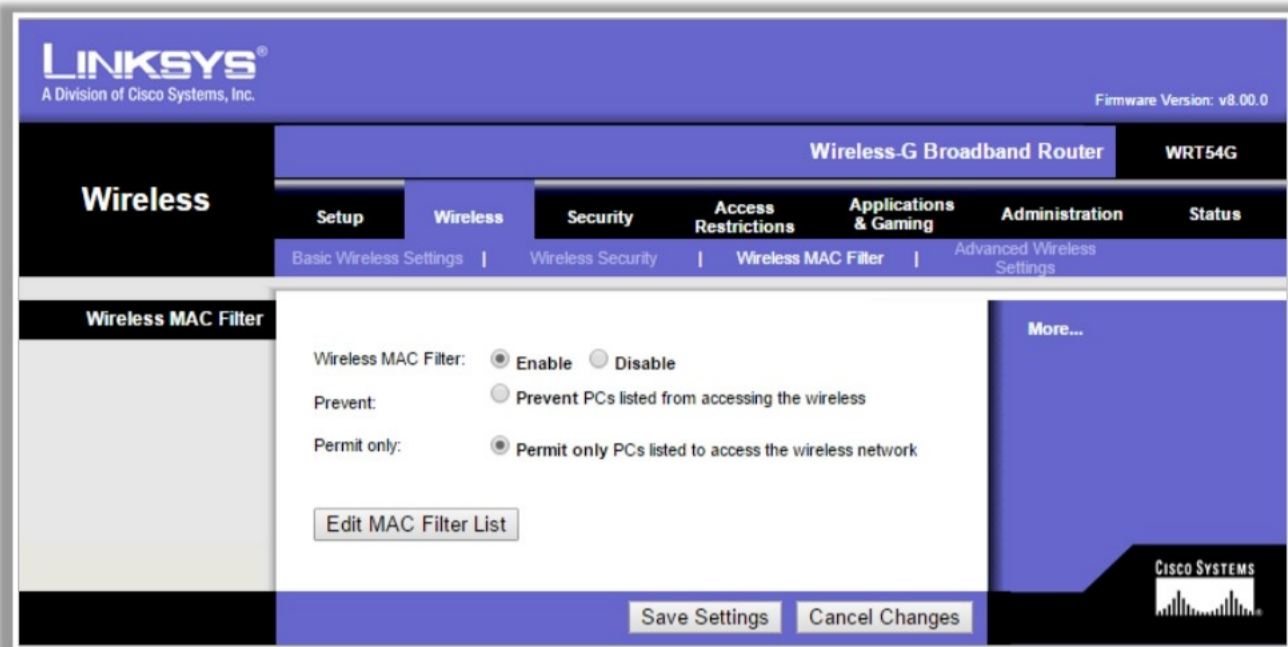
1. WPA3
2. WPA2 Enterprise with RADIUS
3. WPA2 Enterprise
4. WPA2 PSK
5. WPA Enterprise
6. WPA
7. WEP

#### Order of preference for choosing a Wi-Fi security method

1. WPA3
2. WPA2 + AES
3. WPA + AES
4. WPA + TKIP/AES
5. WPA + TKIP
6. WEP
7. Open Network (no security at all)

## Enable MAC Address Filtering





- MAC address filtering enables the administrator to block all **unauthorized devices** from accessing the network and only allow known MAC addresses to connect to the network.
- If MAC address filtering is enabled, the AP or the router stores and **maintains a list of MAC addresses** for the wireless clients.
- When a client tries to connect to the network, the AP **compares the list of stored MAC addresses** with the client's MAC address and allows network connection only if the MAC address is found in the stored list

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Enable MAC Address Filtering

Most wireless routers have MAC address filtering capabilities. This filtering feature permits access to known MAC addresses only and restricts all others.

MAC address filtering has two options, open or closed. In a closed MAC filter, only the listed addresses are permitted to access the network. This option is a more secure way of accessing the network. In an open MAC filter, the addresses listed in the filter are prevented from accessing the network. This is not always practical in a large network.

MAC address filtering maintains a list of all known MAC addresses. When a user tries to enter the network, the AP checks the user's MAC address against the list of MAC addresses stored locally. If the user's MAC address matches an address in the list, then the AP allows the user to enter and access the wireless network.

In this technique, the client authentication is based on MAC addresses. This type of authentication is more secure compared to an open and shared authentication method. However, an attacker can bypass this filtering technique with the help of a MAC spoofing attack. This authentication method minimizes the number of unauthorized users accessing the network.

## Monitoring the Wireless Network Traffic



Wireless network traffic analysis helps in identifying **intrusion attempts** on a wireless network

A continuous **monitoring** and **analysis** of the wireless network traffic should be done for scanning any abnormalities

The **Wireshark sniffing tool** can be used for conducting the monitoring and analysis of wireless network traffic

No.	Time	Source	Destination	Protocol	Length	Info
91	9.506788	f0:4f:7c	192.168.0.1 (RA)	802.11	46	Request-to-send, Flags=.....C
95	9.510746	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
104	9.758296	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
106	9.760111	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
113	9.982961	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
127	10.437934	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
129	10.439835	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
142	11.409057	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
145	11.412945	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
172	13.945555	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
202	19.027036	f0:4f:7c	192.168.0.1 (RA)	802.11	46	Request-to-send, Flags=.....C
206	19.030961	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
209	19.033943	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
221	20.338898	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
223	20.340934	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
291	29.168548	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C
293	29.182313	f0:4f:7c	192.168.0.1 (RA)	802.11	58	802.11 Block Ack, Flags=.....C


Source: <http://www.wireshark.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Monitoring the Wireless Network Traffic

The traffic of a wireless network should be monitored in order to find any abnormalities or signs of an attack. Similar to a wired network, the network traffic on a wireless network can be monitored using packet sniffing utilities such as Wireshark. This can be done by selecting the user's wireless network interface and starting the process of sniffing the traffic on it. In particular, the user can look for traffic based on the 802.11 standard wireless protocols denoting the wireless network traffic. Further, various filters can be applied to filter out the traffic of the user's interest.

## Defending Against WPA Cracking



### Passphrases

- The only way to crack WPA is to sniff the **password** pairwise master key (PMK) associated with the “handshake” authentication process. If this password is extremely complicated, it might be **almost impossible to crack**

### Passphrase Complexity

- Select a **random passphrase** that is not made up of dictionary words.
- Select a complex passphrase which contains a minimum of **20 characters** and change the passphrase at regular intervals

### Client Settings

- Use WPA3 /WAP2 **encryption** only
- Set the client settings properly (e.g., validate the server, specify the server address, do not prompt for new servers, etc.)

### Additional Controls

- Use a **virtual private network (VPN)** such as a remote access VPN, Extranet VPN, Intranet VPN, etc.
- Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Defending Against WPA Cracking

The following countermeasures can help a user to defeat WPA cracking attempts:

- Construct a strong WPA password/key.
- Do not use words from the dictionary.
- Do not use words with numbers appended at the end.
- Do not use double words or simple letter substitution such as p@55w0rd.
- Do not use common sequences from your keyboard such as qwerty.
- Do not use common numerical sequences.
- Avoid using personal information in the key/password.

A WPA password should be constructed according to the following rules:

- It should have a random passphrase.
- It should have at least 12 characters in length.
- It should contain at least one uppercase letter.
- It should contain at least one lowercase letter.
- It should contain at least one special character such as @ or !
- It should contain at least one number.

## Detecting Rogue Access Points

### Wireless Scanning

- Performs a wireless network scanning to detect the presence of **wireless APs** in the vicinity
- Discovery of an AP not listed in the wireless device inventory indicates the presence of a rogue AP
- Use **wireless discovery tools** such as inSSIDer, NetSurveyor, NetStumbler, Vistumbler, Kismet, etc., to detect wireless networks

### Wired Network Scanning

- Use network scanners such as **Nmap** to identify APs on the network. This will help in locating rogue devices on the wired network.

### Simple Network Management Protocol (SNMP) Polling

- Use the **SNMP** to identify the IP devices attached to the wired network.
- Use the SNMP detection utilities such as SolarWinds SNMP scanner, Lansweeper SNMP scanner, etc., to identify the SNMP-enabled devices on the network.

**Note:** To use SNMP polling, the SNMP service on all IP devices in the network should be enabled.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Rogue Access Points (Cont'd)

- Rogue access points are **unauthorized devices** that can be used as entry points for **potential attackers**
- To maintain the security and integrity of the network, it is essential to **detect** rogue access points
- Once a rogue access point is detected, a **response plan** should be in place to investigate and mitigate the risk
  - **Disable** or **remove** the identified rogue device
  - Secure the network to prevent further unauthorized access

### Techniques to Detect Rogue Access Points

Wireless Intrusion Detection Systems (WIDS) WIDS are dedicated systems or software that continuously monitor wireless network traffic to detect and report anomalies, including rogue access points.

Wireless Site Surveys Regular wireless site surveys can help identify unauthorized access points. Tools such as NetSpot, Ekahau, or professional site survey map network's coverage can help look for **unexpected devices**.

Scanning Tools Scanning tools such as Kismet, Aircrack-ng, or WiFi Pineapple identify nearby wireless networks and devices and identify rogue access points broadcasting

Signal Strength Analysis Rogue access points might have a **different signal strength** from that of authorized access points. Tools such as inSSIDer can help analyze signal strength and interference

MAC Address Monitoring Maintain a list of **MAC addresses** for authorized access points check regularly for unfamiliar MAC addresses in the network.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Rogue Access Points

A wireless AP is termed as a rogue AP when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue APs on a trusted network for their malicious intent.

### Types of Rogue APs

1. Wireless router connected via a “trusted” interface

2. Wireless router connected via an “untrusted” interface
3. Installing a wireless card into a device that is already on a trusted LAN
4. Enabling wireless on a device that is already on a trusted LAN

The methods mentioned below should be used for detecting wireless networks in the vicinity of the network and the detected wireless APs should be compared with the wireless device inventory for the environment. If an AP that is not listed in the inventory is found, it can generally be considered as a rogue AP.

#### 1. **Wireless scanning:**

- It performs an active wireless network scanning to detect the presence of wireless APs in the vicinity.
- It helps in detecting unauthorized or hidden wireless APs that can be malicious.

The following Wi-Fi discovery tools can be used for scanning the wireless network.

##### **i) inSSIDer**

Source: <https://www.metageek.com>

InSSIDer is an open source, multi-platform Wi-Fi scanner software. It provides the user information on the proper channeling of a wireless network, while offering the ability to check co-channel effects and overlapping networks. This application uses a native Wi-Fi application program interface (API) and the user’s NIC and sorts the results on the basis of the MAC address, SSID, channel, received signal strength indicator (RSSI), MAC, vendor, data rate, signal strength and time last seen.

##### **Features:**

- Inspects WLAN and the surrounding networks to troubleshoot competing APs
- Tracks the strength of the received signal in dBm over time
- Filters APs
- Highlights APs for areas having a high Wi-Fi concentration
- Exports Wi-Fi and global positioning system (GPS) data to a keyhole markup language (KML) file for viewing it in the Google Earth software
- Shows which Wi-Fi network channels overlap and are compatible with GPS devices.

##### **ii) NetSurveyor**

Source: <http://nutsaboutnets.com>

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information on the nearby wireless APs in real-time and displays it in useful ways. It displays the data using a variety of diagnostic views and charts. It records and provides data playback.

##### **Features:**

- Provides six graphical diagnostic views

- Generates reports in the Adobe PDF format that includes a list of APs and their properties along with images
- Supports most wireless adapters installed with a network driver interface specification (NDIS) 5.x driver or later.

### iii) Vistumbler

Source: <http://www.vistumbler.net>

Vistumbler Features:

- Finds wireless APs
- Provides GPS support
- Exports/imports APs from Vistumbler TXT/VS1/VSZ or Netstumbler TXT/Text NS1
- Exports AP GPS locations to a Google Earth KML file or GPS exchange format (GPX)
- Enables live Google Earth tracking: auto KML automatically shows APs in Google Earth
- Speaks, signal strength using sound files, Windows sound API, or musical instrument digital interface (MIDI)

### iv) NetStumbler

Source: <http://www.netstumbler.com>

Uses of NetStumbler:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detects the causes of wireless interference
- Detects unauthorized (rogue) APs
- Aiming directional antennas for long-haul WLAN links

### v) Kismet

Source: <https://www.kismetwireless.net>

Kismet is a wireless network and device detector, sniffer, wardriving tool, and has a WIDS framework.

## 2. Wired network scanning:

- Wired network scanners such as Nmap are used for indentifying a large number of devices on a network by sending specially crafted TCP packets to the device (Nmap-TCP fingerprinting).
- It helps locate rogue APs attached to a wired network.

## Nmap

Source: <https://nmap.org>

A user can scan their entire address space using the -A option to identify rogue AP. When the scan is completed, the user should search for WAP characteristics in the result.

### 3. Simple network management protocol polling:

- Simple network management protocol (SNMP) polling is used for identifying the IP devices attached to a wired network.
- SNMP detection utilities such as SolarWinds SNMP Scanner, Lansweeper SNMP Scanner, etc., can be used for identifying SNMP enabled devices on the network.

#### i) SolarWinds SNMP scanner

Source: <https://www.solarwinds.com>

With the SNMP discovery tool of the SolarWinds network monitoring software, a user can regularly discover and monitor SNMP-enabled devices on their network.

#### ii) Lansweeper SNMP scanner

Source: <https://www.lansweeper.com>

Lansweeper is an SNMP scanner that scans all available SNMP-enabled devices to retrieve detailed information through the SNMP tool.

Rogue access points are unauthorised devices that can be used as entry points for potential attackers. A rogue access point can be plugged into a firewall or switch, or a wireless card into a server. They can be lethal to security. To maintain the security and integrity of the network, it is essential to detect rogue access points.

Following are some techniques to detect rogue access points:

- **Wireless Intrusion Detection Systems (WIDS):** WIDS are wireless access points that detect and alert when a wireless device is detected. It scans for rogue devices every few milliseconds. These are dedicated systems or software that continuously monitor wireless network traffic to detect and report anomalies, including rogue access points.
- **Wireless site surveys:** Regular wireless site surveys can help identify unauthorized access points. Tools such as NetSpot, Ekahau, or professional site survey map network's coverage and look for unexpected devices.
- **Scanning tools:** Scanning tools such as Kismet, Aircrack-ng, or WiFi Pineapple identify nearby wireless networks and devices and identify rogue access points broadcasting. These tools scan wireless controllers and devices. These tools provide details of all the endpoints connected to it, when the rogue access point was connected, and for how long it has been active.
- **Signal Strength Analysis:** Rogue access points might have a different signal strength from that of authorized access points. Multiple sniffers are used to collect the signal strength. Tools like inSSIDer can help analyze signal strength and interference.

- **MAC address monitoring:** Maintain a list of MAC addresses for authorized access points and check regularly for unfamiliar MAC addresses in the network. When a device tries to connect to the network, the router checks the MAC address of the device against the list. If the MAC address is on the list the access is granted or else denied.

Once a rogue access point is detected,

- A response plan should be in place to investigate and mitigate the risk. It must address the rogue access point, secure the physical location, or reconfigure the network settings to prevent similar incidents.
- Disable or remove the identified rogue device immediately. Disabling can be done using a network access control system to deactivate the switch or port to which the rogue device is connected.
- Secure the network to prevent further unauthorized access. Implement intrusion detection systems that continuously scan for rogue access points. Create network access policies and controls to prevent unauthorized access.

## Locating Rogue Access Points



AirCheck G2 Wi-Fi Tester is a handheld tool that identifies and locates authorized or rogue wireless APs in the network



Source: <https://www.netally.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Locating Rogue Access Points

Once a rogue AP is detected in the network, its location can be traced using a tool such as the handheld wireless tester AirCheck G2 Wi-Fi Tester. It helps to find the exact location of any wireless AP. The AirCheck Wi-Fi G2 Tester must be carried to track the rogue AP. It detects the access point based on the signal strength.

#### AirCheck Wi-Fi Tester

Source: <https://www.netally.com>

This device tracks down rogue and other APs by graphing the signal strength over time or by using an audible indication, which can be muted.

## Protecting from RF Interference



- **Excessive RF interference** should be detected and monitored in order to avoid DoS attacks such as RF jamming, signal bombing and war spamming
- **RF spectrum analyzing tools** should be used for detecting RF interference. Such tools provide notification about excessive RF interference on a wireless network.
- RF spectrum analyzers:
  - **AirMagnet Spectrum XT**  
<https://www.netally.com>
  - **WiFi Surveyor**  
<http://rfexplorer.com>
  - **Ekahau Spectrum Analyzer**  
<http://www.ekahau.com>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Protecting from RF Interference

Wireless networks are often susceptible to DoS attacks, since wireless networks have a shared medium of transmission. DoS attacks may occur in the various levels of the open system interconnection (OSI) network layer. The DoS attack in the physical layer is carried out by signal jamming or intentional interference.

Wireless networks use radio frequencies for communication and RF spectrum analyzing tools can be helpful in detecting the RF interference.

Some of the available RF spectrum analyzers are:

#### 1. AirMagnet Spectrum XT

Source: <https://www.netally.com>

AirMagnet Spectrum identifies the RF interference that impacts the performance of a wireless network.

#### 2. Wi-Fi Surveyor

Source: <http://rfexplorer.com>

Wi-Fi Surveyor provides the following services:

- Displays the RF environment
- Monitors the RF signals
- Troubleshoots the RF issues
- Detects sources of RF interference

This tool helps in detecting wireless devices and RF interference in the network that may affect the network's performance.

### 3. Ekahau Spectrum Analyzer

Source: <http://www.ekahau.com>

Ekahau Spectrum Analyzer is a device that assists in determining the devices causing the interference in a wireless network.

## Assessing the Security of a Wireless Network



A wireless security assessment is used for **detecting, locating, and mitigating** the risks posed by the current configuration of a wireless network

A security assessment/testing should be performed to detect **potential vulnerabilities** in the wireless network and mitigate them before attackers can exploit them

Wi-Fi security assessment tools such as AirMagnet WiFi Analyzer, Elcomsoft Wireless Security Auditor, etc., can be used for performing the security assessment.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Assessing the Security of a Wireless Network

A wireless network should be regularly checked for possible vulnerabilities. Parameters such as security, performance, and speed should be considered while performing the assessment. This helps to ensure that the wireless network is adequately protected from attacks. Different security assessment and vulnerability scanning tools should be used for finding the potential vulnerabilities.

The following should be considered in a typical wireless network security assessment:

- Check if a proper and up-to-date inventory is being maintained for all wireless network devices
- Check the location of APs to make sure that they are properly placed
- Check if the wireless antennas are pointing in the right direction
- Discover new wireless devices
- Document all the findings for new wireless devices
- If the wireless device found is using a Wi-Fi network, check if it is using weak encryption
- Create a rogue AP and check if it can be detected
- Check if the SSID is visible or hidden
- Check if MAC filtering has been enabled or not

The following tools can assist a user in assessing wireless security:

#### 1. AirMagnet Wi-Fi analyzer

Source: <https://www.netally.com>

AirMagnet Wi-Fi analyzer offers continuous evaluation of the wireless channels, devices, speeds, interference issues, and RF spectrum. It helps to automatically detect the security threats and wireless network vulnerabilities, common wireless performance issues including throughput issues, connectivity issues, device conflicts, and signal multipath problems.

This tool can detect Wi-Fi attacks such as DoS attacks, authentication/encryptions attacks, network penetration attacks, etc. It can easily locate unauthorized (rogue) devices or any policy violator. The tool examines 802.11a\b\g\n and 5 GHz channels for interference and can be installed in PCs, laptops, tablets, etc., in order to assess interference issues.

## 2. Elcomsoft Wireless Security Auditor

Source: <https://www.elcomsoft.com>

Elcomsoft Wireless Security Auditor helps in verifying how secure and busy a company's wireless network is. The tool attempts to break into a secured Wi-Fi network by analyzing the wireless environment, sniffing Wi-Fi traffic, and running an attack on the network's WPA/WPA2-PSK password.

## 3. WepAttack

Source: <http://wepattack.sourceforge.net>

WepAttack is a WLAN open source Linux tool for breaking 802.11 WEP keys. This tool is based on an active dictionary attack that tests millions of words to find the right key.

## 4. Aircrack-ng

Source: <http://www.aircrack-ng.org>

Aircrack-ng is a complete suite of tools used for assessing Wi-Fi network security.

It focuses on different areas of Wi-Fi security:

- **Monitoring:** It captures packets and exports data to text files for further processing by third party tools.
- **Attacking:** It replays attacks, de-authentication, fake APs, and others via packet injection.
- **Testing:** It checks Wi-Fi cards and driver capabilities (capture and injection).
- **Cracking:** WEP and WPA PSK (WPA 1 and 2)

## 5. WEPCrack

Source: <http://wepcrack.sourceforge.net>

WEPCrack is an open source tool for breaking 802.11 WEP secret keys. It cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling.

## 6. WepDecrypt

Source: <http://wepdecrypt.sourceforge.net>

WepDecrypt guesses the WEP keys based on an active dictionary attack, key generator, distributed network attack, and some other methods.

## 7. CommView for WiFi

Source: <http://www.tamos.com>

CommView for WiFi captures every packet on the air to display important information such as the list of APs and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, and the protocol distribution charts.

Wi-Fi vulnerability scanning tools can help a user in finding weaknesses in the wireless networks and secures them before attackers actually attack.

Some of the Wi-Fi vulnerability scanning tools include:

## 8. Nmap

Source: <http://nmap.org>

Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for scanning vulnerabilities on wireless networks. This tool saves the vulnerability scans as profiles to make them run repeatedly. The results of recent scans are stored in a searchable database.

## 9. Nessus

Source: <http://www.tenable.com>

Nessus is a vulnerability, configuration, and compliance scanner. It features high-speed discovery, configuration auditing, asset profiling, malware detection, sensitive data discovery, patch management integration, and vulnerability analysis of a wireless network.

## 10. Network Security Toolkit

Source: <http://networksecuritytoolkit.org>

Network Security Toolkit (NST) is a Fedora-based application that provides easy access to the open source network security applications. The toolkit includes an advanced user interface for system/network administration, navigation, automation, network monitoring, host geolocation, network analysis and configuration of many network and security applications found within the NST distribution.

## 11. Nexpose Community Edition

Source: <http://www.rapid7.com>

Nexpose is a vulnerability management application that analyzes vulnerabilities, controls, and configurations in order to find the security risks. It uses RealContext and RealRisk features and, in addition, the attacker's mindset to prioritize and drive risk reduction. This tool helps a user to understand the network and to prioritize and manage risks effectively.

## 12. WiFish Finder

Source: <https://sourceforge.net>

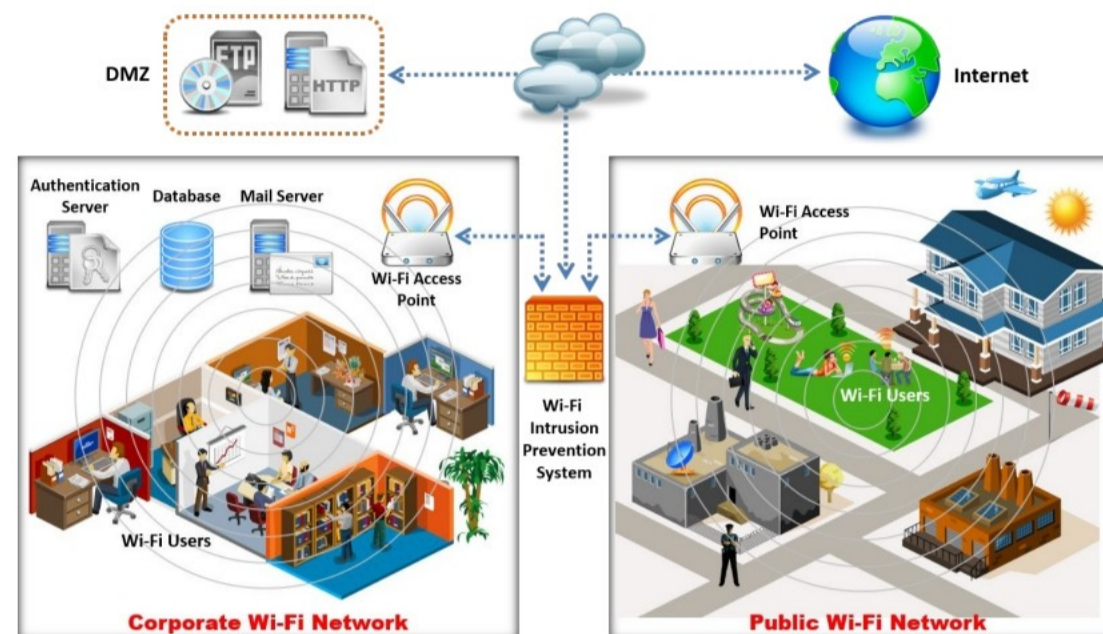
WiFish Finder is a vulnerability assessment tool that determines if active Wi-Fi devices are vulnerable to 'Wi-Fishing' attacks. A user can perform this assessment via a combination of passive traffic sniffing and active probing techniques. Most Wi-Fi clients keep a memory of

networks (SSIDs) that they have connected to in the past. Wi-Fish Finder builds a list of the probed networks and determines the security setting of each probed network. A client is a fishing target if it is actively seeking to connect to an OPEN or a WEP network.

## Implementing a Wireless Intrusion Detection System/ Wireless Intrusion Prevention System



- A wireless intrusion detection system (WIDS)/wireless intrusion prevention system (WIPS) helps in finding any **abnormalities** in the wireless network such as unauthorized network activity, policy violations, known patterns of wireless attacks, rogue wireless AP, unencrypted traffic, etc.
- The WIDS/WIPS tools such as Extreme AirDefense, Cisco Adaptive Wireless IPS, etc., can be used for securing the wireless networks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Implementing a Wireless Intrusion Detection System/ Wireless Intrusion Prevention System

Wireless intrusion detection systems (WIDS)/ wireless intrusion protection systems (WIPS) help in finding any abnormalities in the wireless network such as unauthorized network activity, policy violations, known patterns of wireless attacks, rogue wireless AP, unencrypted traffic, etc.

The following WIDS/WIPS tools can be used for securing the wireless networks:

### 1) Cisco Adaptive Wireless IPS

Source: <https://www.cisco.com>

The Cisco Adaptive WIPS provides specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. It provides the ability to detect, analyze, and identify wireless threats. It also delivers proactive threat prevention capabilities for a hardened wireless network core. It is impenetrable by most wireless attacks, allowing customers to maintain constant awareness of their RF environment.

### 2) Extreme AirDefense

Source: <https://www.extremenetworks.com>

Extreme AirDefense helps a user to manage, monitor, and protect their WLAN networks.

## Configuring the Administrative Security on Wireless Routers



- Change the **default password** on the wireless router
- Assign a **strong and complex password** to the router
- Choose the **HTTPS** for secure communication
- Disable remote router access
- Enable logging

The screenshot shows the 'Administration' page for a Wireless-G Broadband Router (WRT54G). The 'Router Password' section has fields for 'Password' and 'Re-enter to confirm'. The 'Web Access' section has 'Access Server' with radio buttons for 'HTTP' and 'HTTPS', and 'Wireless Access Web' with radio buttons for 'Enable' and 'Disable'. The 'Remote Router Access' section has 'Remote Management' with radio buttons for 'Enable' and 'Disable', and a 'Management Port' field set to '8080'. The 'UPnP' section has radio buttons for 'Enable' and 'Disable'. A sidebar on the right contains explanatory text for 'Local Router Access', 'Web Access', 'Remote Router Access', and 'UPnP'.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

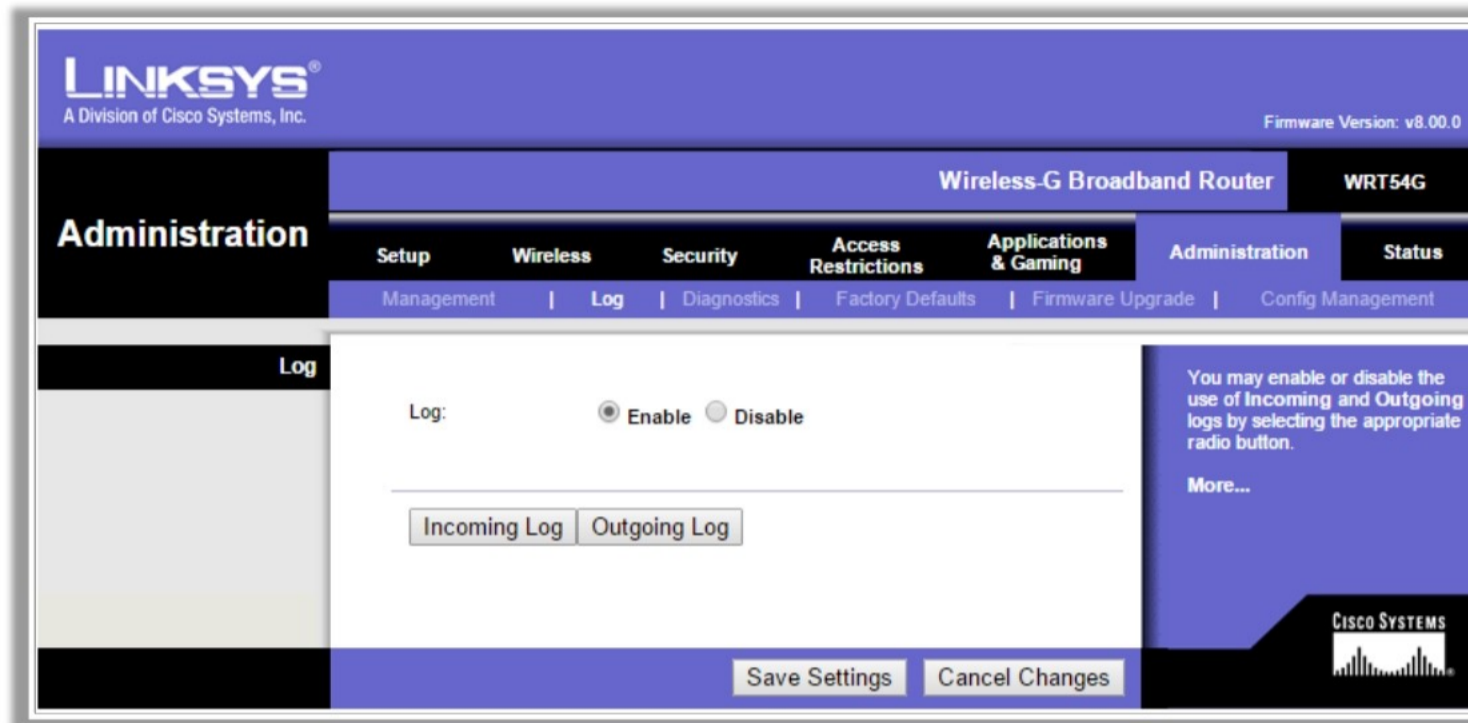
## Configuring the Administrative Security on Wireless Routers (Cont'd)



The image shows two side-by-side screenshots of the Linksys WRT54G router administration page. The left screenshot shows the 'Administration' page with 'HTTPS' selected under 'Access Server' and 'Disable' selected under 'Remote Management'. The right screenshot shows the same page with 'HTTPS' and 'Disable' highlighted in red boxes. Both screenshots show the 'Router Password', 'Web Access', 'Remote Router Access', and 'UPnP' sections. The right screenshot also shows a 'Save Settings' and 'Cancel Changes' button at the bottom.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Configuring the Administrative Security on Wireless Routers (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


### Configuring the Administrative Security on Wireless Routers

In order to harden the wireless router, the recommended security configurations should be applied on the wireless router. These security configuration settings help minimize any wireless attacks and provide the best performance, security, and reliability when using Wi-Fi.

The following are the security recommendations that must be considered:

1. Changing the default password of the wireless router
2. Assigning a strong and complex password to the router
3. Choosing the hypertext transfer protocol secure (HTTPS) for secure communication
4. Disabling the remote router access
5. Enabling the firewall to block certain WAN requests
6. Configuring an internet access policy
7. Specifying the blocked services, URL, keywords, etc.
8. Disabling the demilitarized zone (DMZ) option
9. Configuring the QoS settings
10. Avoid using the default IP ranges
11. Keep the router firmware up-to-date

## Additional Wireless Network Security Guidelines



<ul style="list-style-type: none"><li>■ Do not use the SSID, company name, network name, or any <b>easy to guess</b> string in the passphrases</li></ul>	<ul style="list-style-type: none"><li>■ Regularly change the <b>passphrases</b></li></ul>
<ul style="list-style-type: none"><li>■ Place a <b>firewall or packet filter</b> in between the AP and the corporate intranet</li></ul>	<ul style="list-style-type: none"><li>■ Disable the <b>network</b> when not required</li></ul>
<ul style="list-style-type: none"><li>■ Change the default <b>SSID</b></li></ul>	<ul style="list-style-type: none"><li>■ Place the wireless APs in a <b>secured location</b></li></ul>
<ul style="list-style-type: none"><li>■ <b>Regularly</b> check the wireless devices for configuration or setup problems</li></ul>	<ul style="list-style-type: none"><li>■ Keep the drivers on all wireless equipment updated</li></ul>
<ul style="list-style-type: none"><li>■ Implement a different technique for <b>encrypting traffic</b> such as IPSec over the wireless network</li></ul>	<ul style="list-style-type: none"><li>■ Use a centralized server for <b>authentication</b></li></ul>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Additional Wireless Network Security Guidelines

The following list contains the security recommendations and guidelines for additional wireless network security:

- The user should log out of the router's web interface when it is not in use.
- Everything should be password protected in order to avoid unauthorized access of the content in the system.
- The wireless access point should be password protected.
- The SSID value should be changed such that only the user understands it.
- The APs should be kept in the middle of the building in order to avoid wardriving.
- Broadcasting of SSIDs should be avoided as this can make it easy for an intruder to enter the network.
- The physical location of the WLAN threat should be identified.
- Information about the source and destination IP addresses, ports, MAC address, login names/IDs, duration, and timestamps for analysis and investigation should be gathered.
- Collection of connection logs can help in determining the unnecessary utilization of a wireless network in the organization.
- The network should be monitored using wireless intruder detection-prevention system (WIDPS) sensors and WLAN scanners in order to detect a rogue WLAN connection.
- Locations within close proximity of the organization must be scanned.

**Module 13: Enterprise Wireless Network Security**

- Security of the link through which information is passed among the components in the network should be monitored.
- A detection should be made of the laptops that are being illegitimately used as APs.

## Module Summary



- A wireless network uses the IEEE standard of 802.11 and uses radio waves for communication
- An AP is a hardware device that permits wireless communication devices to connect to a wireless network by using the wireless standards such as Bluetooth, Wi-Fi, etc.
- WPA is a data encryption method used for WLANs based on the 802.11 standards
- In the open system authentication technique, any wireless device can be authenticated with the AP, allowing the device to transmit data only when its WEP key matches the WEP key of the AP
- Wireless traffic analysis helps a user to identify intrusion attempts on a wireless network
- Active wireless network scanning and wired network scanning should be conducted in order to detect the presence of wireless APs in close proximity to an organization

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Module Summary

This module covered several fundamental concepts of wireless network security such as the security standards, topologies, encryption types, and different security measures that should be implemented in order to achieve a robust Wi-Fi security.

With the skills learned in this module, you will be able to:

- Configure a wireless router to provide a robust and secure wireless network
- Identify all the possible vulnerabilities and threats to the wireless network
- Defend against most wireless attacks on the wireless network

This page is intentionally left blank.