Introduction to the Wireless Security

INTRODUCTION TO WIRELESS COMMUNICATION

- One of the medium of communication.
- Transfer of information without any wire, cables, or any electrical conductor.
- Used for both long and short distances.
- Radio Frequency,Infrared light,Laser light etc is used.
- Wireless communication offer speed,flexibility,and network efficiency.


Smart watch
Cellular phones
Smart Glasses
GSM
Bluetooth
WLAN
WiFi
GPS
5G
LTE
4G LTE
aptops
Palmtop
Tablets
Bluetooth
Speakers

- **Radio frequency (RF) signal**:- Refers to a wireless electromagnetic signal used as a form of communication, Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from **30Hz to 300 GHz.**

Application of RF:-

1. Television broadcasting
2. Satellite communication
3. Radar systems
4. Computer and mobile platform networks

- **IR light:-** It is a very similar to visible light, except that it has a slightly longer wavelength. This means IR is undetectable to the human eye perfect for wireless communication. Frequencies range from **300 GHz to 400THz**.

Application of IR light:-

1. Remote control
2. Infrared thermometer
3. Optical fiber

Advantage of wireless communication.

- Wireless networks are cheaper to install and maintain.
- Data is transmitted faster and at a high speed.
- Reduced maintenance and installation cost compared to other form of networks.
- Wireless network can be accessed from anywhere, anytime.
- Wireless network can be expandable.

Disadvantage of wireless communication

- As communication is done through open space, it is less secure.
- Unreliability.
- It has a limited amount of bandwidth for communication and breaches of network security.
- Wireless networks can be easily hacked.
- Wireless networks are usually inexpensive, but the cost of installation is very high, setting up a wireless network is very costly.
- Difficult to set up little experience people.

Application of Wireless Communication

- Satellite system
- Television remote control
- **Wi-Fi**
- Paging system
- **Security systems CCTV(Closed-Circuit television)**
- Cellphones
- **Computer interface devices (Wireless LAN CARD)**
- Bluetooth
- GPS
- GSM
- **Accessing the internet. (Home Broadband Router)**
- For locating and tracing someone.

- Most wireless devices today are Half-Duplex.
- Half-Duplex wireless devices are those that cannot transmit and receive signal simultaneously.
- Mesh topology commonly used for wireless network.

Wireless IEEE standards.

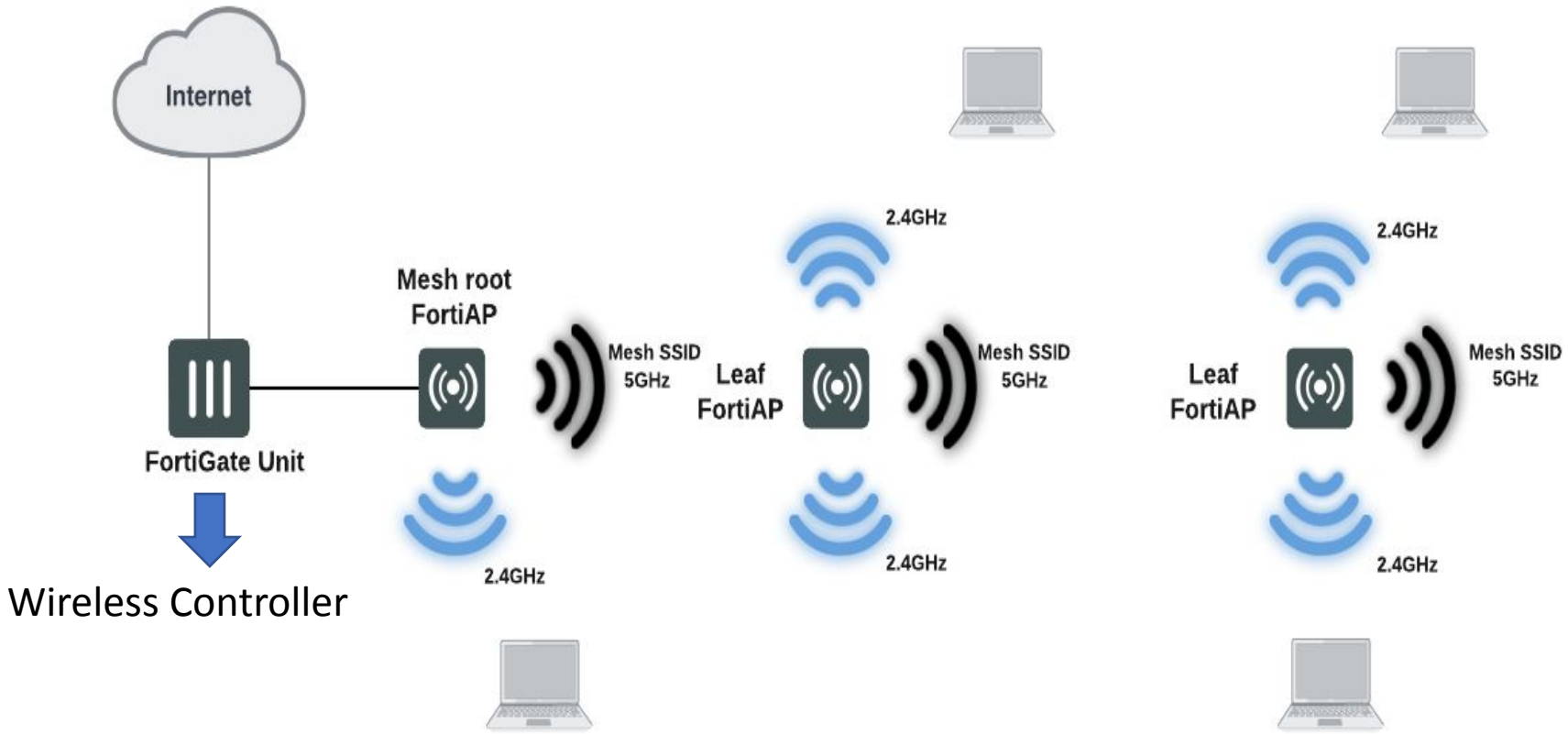
- Wireless standards are a set of services and protocols that indicate how your Wi-Fi network (and other data transmission networks) acts.

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax	802.11be
Wi-Fi Alliance Name	Wi-Fi 1	Wi-Fi 2	Wi-Fi 3	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6/6E	Wi-Fi 7
Year Released	1999	1999	2003	2009	2014	2019	2024/2025
Frequency	5GHz	2.4GHz	2.4GHz	2.4GHz & 5GHz	2.4GHz & 5GHz	6: 2.4GHz & 5GHz/6E: 2.4GHz,	2.4GHz, 5GHz, & 6GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps	40Gbps

Enterprise wireless system.

Top vendors

1. Ruckus
2. Cisco
3. Fortinet
4. Alcatel lucent
5. HPE Aruba



What is wireless security?

- Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks , which include Wi-Fi networks.
- Wi-Fi networks are particularly vulnerable to cyberattacks because they use radio waves to transmit data.
- This means that anyone within range of the Wi-Fi signal can potentially intercept and read the data being sent.

Wireless security protocol

What is the need for Wireless Security Protocols?

Wireless Security Protocols such as Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) are used to ensure wireless security.

There are four wireless security protocols currently available:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)
- Wi-Fi Protected Access 3(WPA 3)

The evolution of wireless protocol

- Wireless protocols protect your wireless network from hacking by encrypting private data as it is being broadcast over the airwaves.
- The Wired Equivalent Privacy (WEP) is the first wireless security protocol that was developed in 1997.
- However, this protocol contained several flaws, therefore, the Wi-Fi Protected Access (WPA) was developed to deal with the flaws that were found in the WEP protocol.

Limitation of WEP

- First 802.11 security standard.
- WEP uses a shared-secret key, which is 40-bits in length.
- Easily hacked due to 24-bit initialization vector(IV) and weak authentication.
- There is only 16.7 million variation of the key.
- Weak encryption of data.
- Hacker can easily obtain challenges phrase and encrypted response.
    - Crack the WEP key
    - Correctly decrypt capture data traffic
- Each client and AP must be configured with matching WEP key.
- Managing key can be difficult in enterprise WLAN.

How WEP Works

- Uses RC4 (Rivest cipher) stream cipher and 64-bit or 128-bit key .
- It encrypts messages one byte at a time via an algorithm.
- Static master key must be manually entered in each devices .

- Should you see it :NO

WPA

- WPA was initially released in 2003.
- Better key management.
- Master key are never directly used.
- Contain impressive message integrity checking. (Prevent from man of middle attack)
- A different key is scrambled and use for each packet, resulting in a more complex secret key.

How it works:-

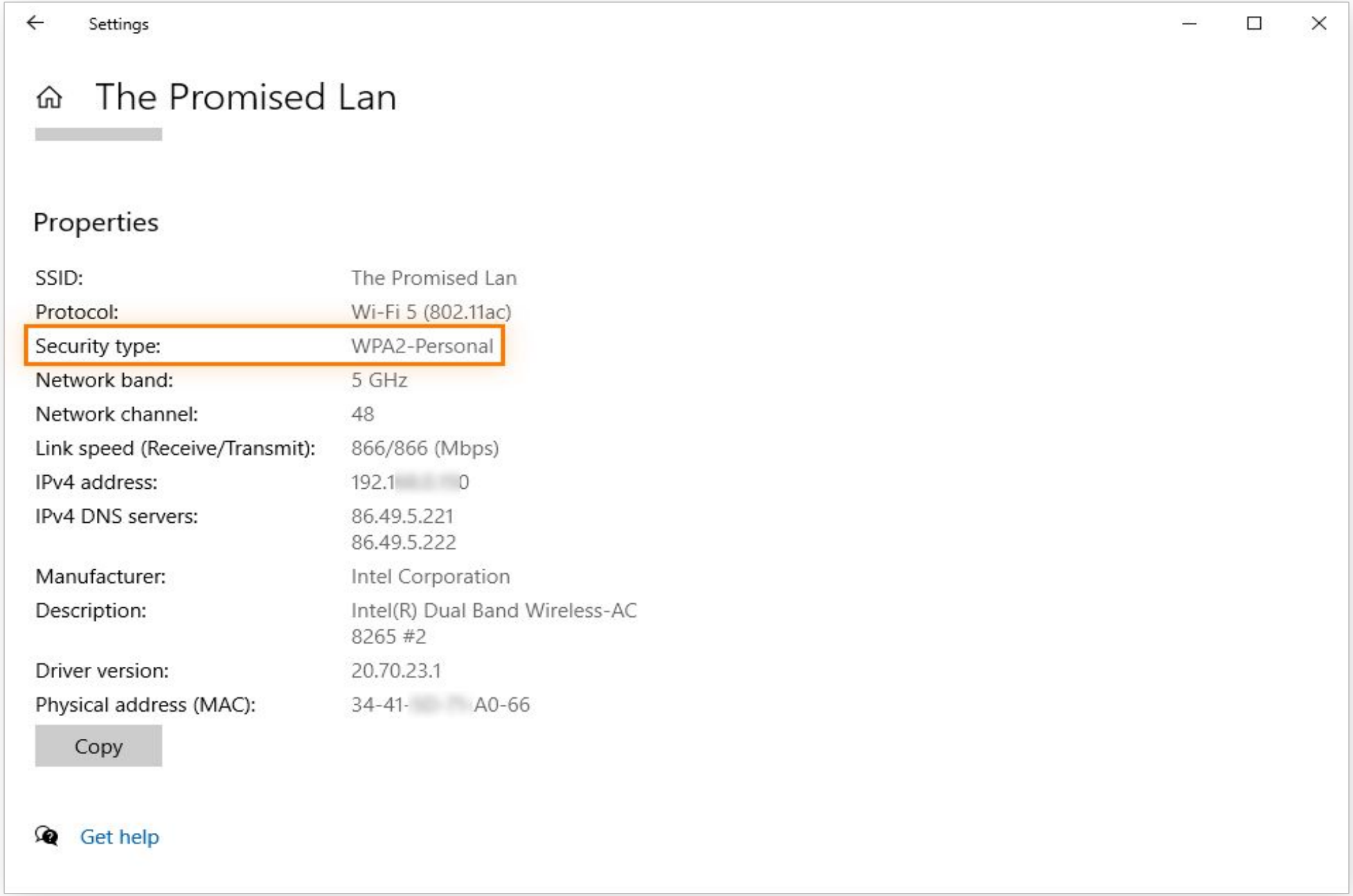
- Retain use of RC4 but add longer IV 48-bit and 256-bit key.
- Each client get key with TKIP.(Temporal Key Integrity Protocol)
- TKIP is a security protocol used in the IEEE 802.11

WPA 2

- WPA2 was released in 2004.
- It was developed with enhanced features and encryption capabilities.
- WPA2 ensures that data sent or received over your wireless network is encrypted, and only people with your network password have access to it.
- Uses the strongest encryption method: AES(**Advanced Encryption Standard)**

WPA 3

- WPA3 was released in 2018.
- WPA3 is the third iteration of security standard or protocol developed by wi-fi alliance to replace the WPA2
- It is the most recent wireless protocol which comes with more enhanced encryption abilities for both private and public networks.
- It protect against week password.
- 128 bit encryption in WPA3 personal mode.
- 192 bit in WPA3 Enterprise.
- It replace pre shared key exchange.


Settings
The Promised Lan
Properties
SSID: The Promised Lan
Protocol: Wi-Fi 5 (802.11ac)
Security type: WPA2-Personal
Network band: 5 GHz
Network channel: 48
Link speed (Receive/Transmit): 866/866 (Mbps)
IPv4 address: 192.1 0
IPv4 DNS servers: 86.49.5.221
86.49.5.222
Manufacturer: Intel Corporation
Description: Intel(R) Dual Band Wireless-AC 8265 #2
Driver version: 20.70.23.1
Physical address (MAC): 34-41- A0-66
Copy
Get help