Introduction to WiFi

Prof SRN Reddy, IGDTUW

Overview of IEEE 802

- **802.1 Bridging and Architecture**
- **802.3 Ethernet**
- **802.11 Wireless LAN (WLAN)**
- **802.15- Wireless Personal Area Network(WPAN)**
- **802.16 Broadband Wireless Access (BWA)**
- **802.18 Radio Regulatory TAG (Technical Advisory Group)**
- **802.19 Coexistence**
- **802.21 Media Independent Handover**
- **802.22 Wireless Regional Area Networks(WRAN)**

WiFi (Wireless Fidelity)

- WiFi (Wireless Fidelity) is an alternative to Wired Technology
- It is used for connecting devices in wireless mode.
- Wi-Fi is a generic term that refers to the IEEE 802.11x communications standard for Wireless Local Area Networks (WLANs).
- Wi-Fi Network connect computers

  to each other

  to the internet

  to the wired network.
- Wi-Fi works on physical and data link layer.

Wi-Fi and the IoT

- Wi-Fi services can be deployed within edge devices used for
  - industrial
  - transport
  - home networks
  - and other IoT applications
- Different applications have different priorities in terms of
  - data rates
  - range
  - power demand
  - cost.
- Compact form factors, rapid connection setup and highly scalable deployment can also be important
- Several different standers in WiFi has been developed

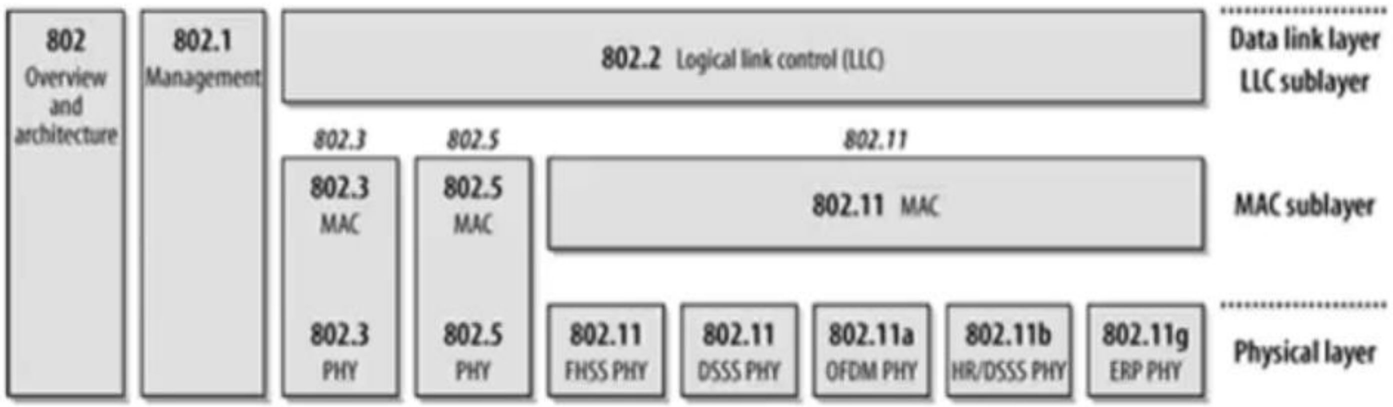
WiFi Applications

- Home
- Small Businesses
- Large Corporations & Campuses
- Health Care
- Wireless Internet Service Providers (WISP)
- Travellers
- Wi-Fi Camera
- Education Institutions

Overview of 802.11 Networks

- 802.11 is a member of the IEEE 802 family, which is a series of specifications for local area network (LAN) technologies.
- IEEE 802 specifications are focused on the two lowest layers of the OSI model because they incorporate both physical and data link components.
  - The MAC(Media Access Control) is a set of rules to determine how to access the medium and send data
  - The details of transmission and reception are left to the PHY

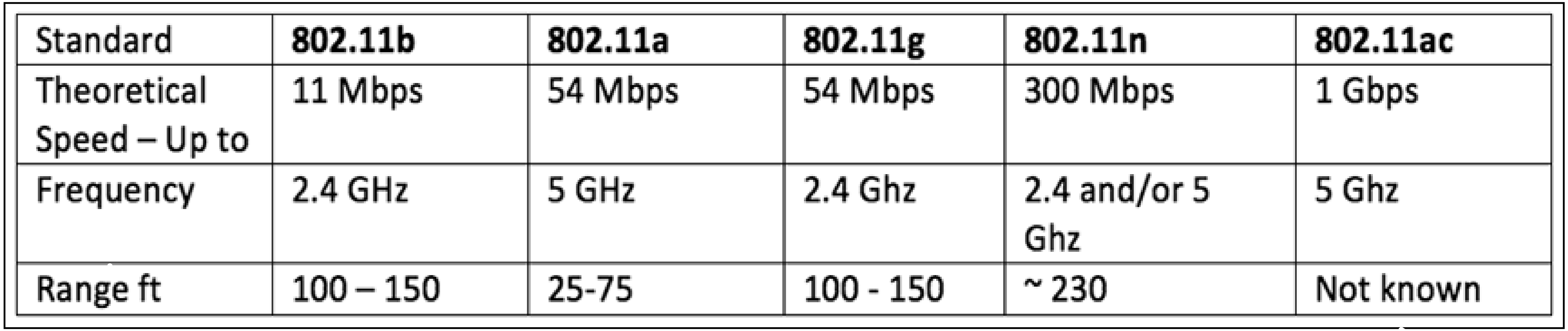
Figure 2-1. The IEEE 802 family and its relation to the OSI model



IEEE 802.11 Physical Layers

- Issued in four stages
- First part in 1997: IEEE 802.11
  - Includes MAC layer and three physical layer specifications
  - Two in 2.4-GHz band and one infrared
  - All operating at 1 and 2 Mbps
- Two additional parts in 1999:
  - IEEE 802.11a-1999: 5-GHz band, 54 Mbps/20 MHz, OFDM
  - IEEE 802.11b-1999: 2.4 GHz band, 11 Mbps/20 MHz
- Fourth part:
  - IEEE 802.11g-2003 : 2.4 GHz band, 54 Mbps/20 MHz, OFDM

Comparison of Wi-Fi standards



Standard	**802.11b**	**802.11a**	**802.11g**	**802.11n**	**802.11ac**
Theoretical Speed – Up to	11 Mbps	54 Mbps	54 Mbps	300 Mbps	1 Gbps
Frequency	2.4 GHz	5 GHz	2.4 Ghz	2.4 and/or 5 Ghz	5 Ghz
Range ft	100 – 150	25-75	100 - 150	~ 230	Not known

Rane 170

Components of a Wi-Fi Network

- Access Point (AP) - The AP is a wireless LAN transceiver or “base station” that can connect one or many wireless devices in the same time to the Internet.

- Safeguards - Firewalls and anti-virus software protect networks from uninvited users and keep information secure.

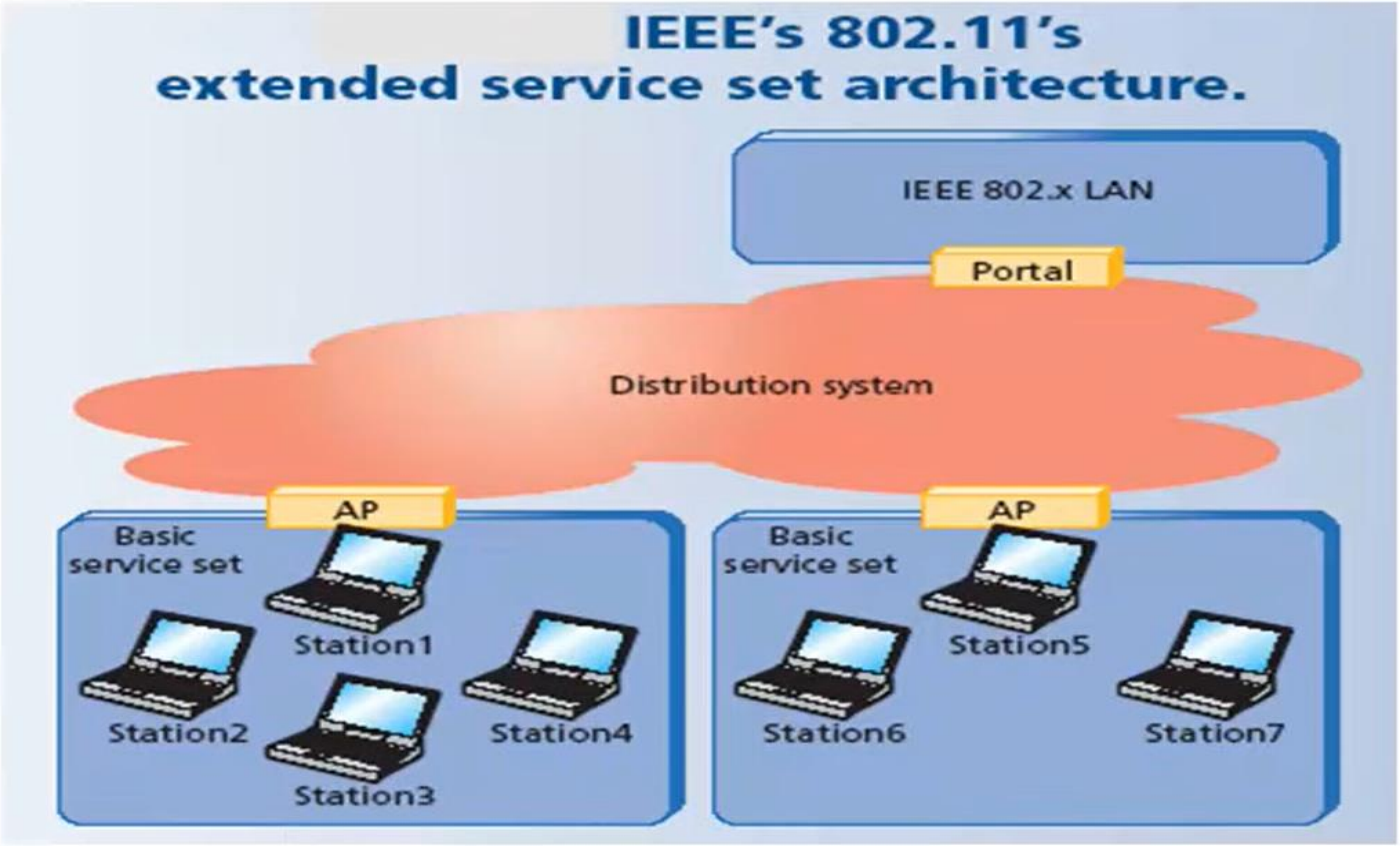
- Wi-Fi cards (Adapters) - allow computers to connect to the Internet and to other computers without using wires. They send data via radio waves to routers that pass it on to broadband modems or internal networks

How a Wi-Fi Network Works

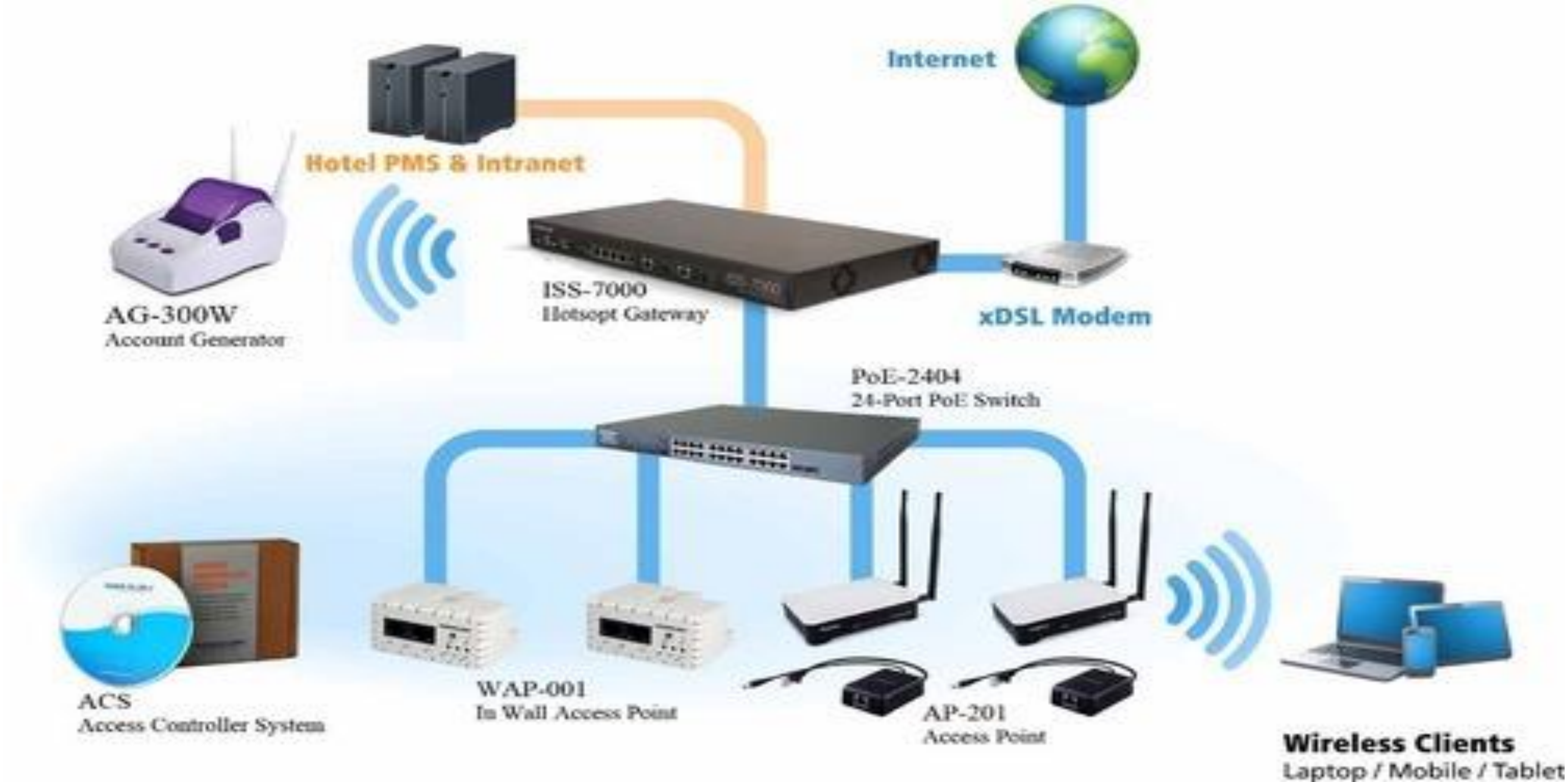
- A Wi-Fi hotspot is created by installing an access point to an internet connection.
- An access point acts as a base station.
- When Wi-Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.
- A single access point can support up to 30 users and can function within a range of 100 – 150 feet indoors and up to 300 feet outdoors.
- Many access points can be connected to each other via Ethernet cables to create a single large network.

WLAN Architecture: Infrastructure Basic Service Set (BSS)

- An Infrastructure BSS is the Basic Service Set Used when bridging a wireless LAN to a wired LAN.
- The other type of BSS is an ad-hoc BSS, where no infrastructure or administrator is needed.
- With ad-hoc networks, peer to peer communication is used.



WiFi N/W Example



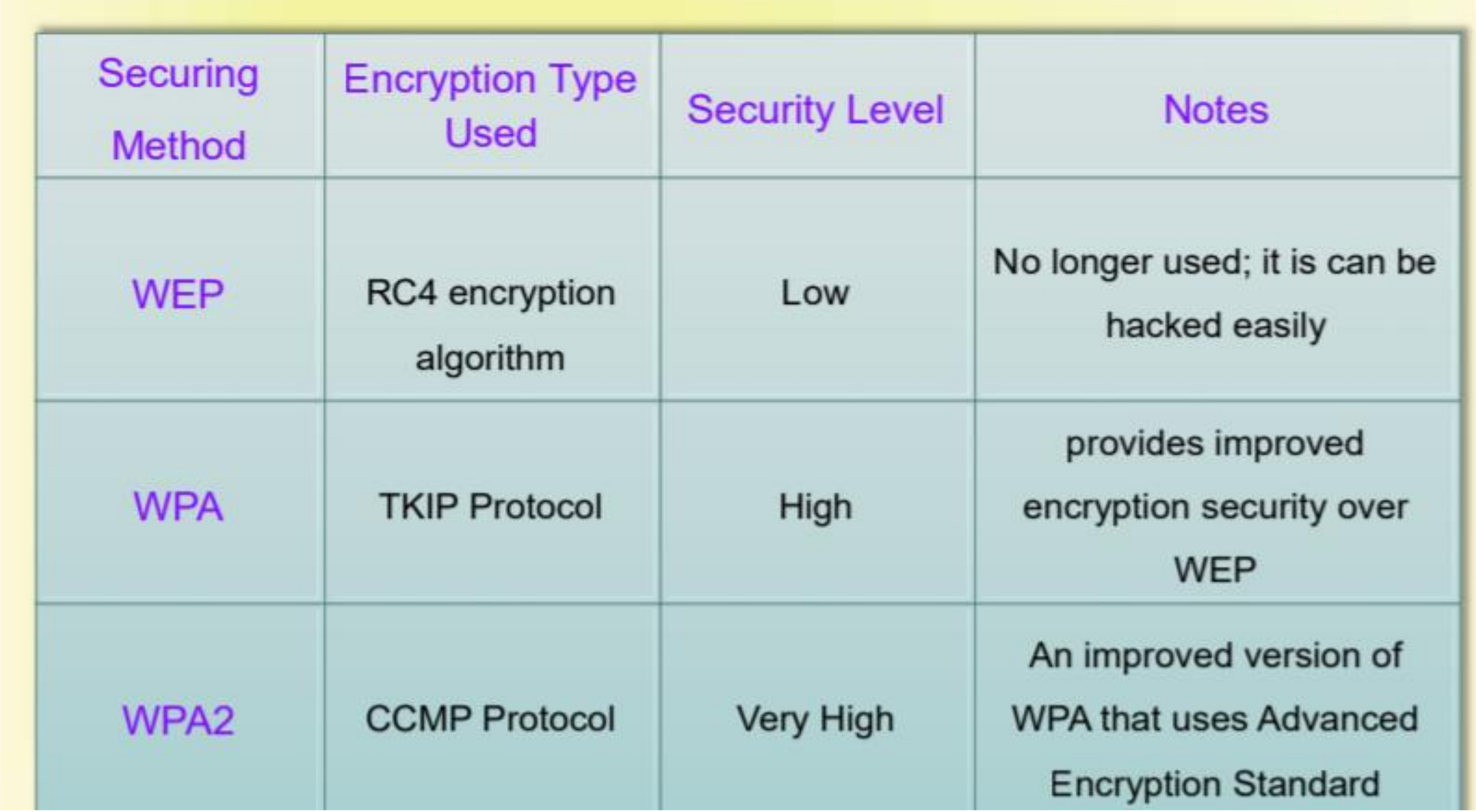
Why WiFi

- Low cost
  - Volume production of WiFi Chips
  - Greater functionality – security, power management, robust, mature firmware and drivers add value to use
  - Integration into several different microcontrollers
- Low power
  - Lower cost, more power-friendly solutions based on 802.11n and 802.11ac
  - Modern, lower-power semiconductor process technologies 5nm to 7 nm
- Compact form-factor
  - These semiconductor processes also mean that Wi-Fi solutions can be as small as other wireless technologies’, and even ruggedized
- Rapid connection set-up time
  - 802.11ai developed to support
- Massive, scalable deployments
  - Wi-Fi can address IoT applications up to possibly even tens of millions of nodes across enormous geographies, through a long inter-node range and mesh architectures

S. No	WiFi	HOTSPOT
1.	Wifi is a wireless communication technology that is used for LAN(Local Area Networks).	Hotspot provides internet to wireless devices by using wifi.
2.	There is no hotspot without wifi.	Hotspot is created using wifi.
3.	Wifi is used between wireless devices and an access point for interconnection.	hotspot is created using an access point device that is connected to the router.
4.	Wifi provides high speed as compared to hotspot in the case of multiple users.	The hotspot offers lower speed than wifi in the case of many users.
5.	Wifi services are provided by the local area Internet service provider.	Whereas the hotspot services are largely provided by cellular or phone corporations.
6.	Wifi is more secure in comparison to hotspot.	Hotspots are less secure than private wifi as they are typically used in public places.
7.	In wifi, electromagnetic waves under the radio frequency band 2.4GHz are used for communication.	In the hotspot, wifi technology is used in order to connect the devices to the access point for sharing the internet.

Wi-Fi Security

- WEP(Wired Equivalent Privacy) : The original encryption technique specified by the IEEE 802.11 standard.
- WPA(Wi-Fi Protected Access): A new standard that provides improved encryption security over WEP- TKIP Protocol
  - Temporal Key Integrity Protocol(TKIP) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the WEP
- WPA2 : is an improved version of WPA that uses Advanced Encryption Standard (AES) technology. It uses Counter Mode CBC-MAC Protocol(CCMP)



Securing Method	Encryption Type Used	Security Level	Notes
WEP	RC4 encryption algorithm	Low	No longer used; it is can be hacked easily
WPA	TKIP Protocol	High	provides improved encryption security over WEP
WPA2	CCMP Protocol	Very High	An improved version of WPA that uses Advanced Encryption Standard

Advantages

- No Wires - A truly wireless networking solution.
- No Waiting - Fast, easy deployments.
- No Worries - A wireless networking system that is secure, easy to manage, and built to grow with you.
- Ease of Installation - Quick, easy setup.
- Security - Many Types Of Security(WEP,WPA,WPA2)
- Fast data transfer rates

Limitations

- Limited range
- Interference from other devices : such as telephones, microwave ovens.
- High power consumption :making battery life and heat a concern.
- Data security risks :a huge challenge for Wi-Fi networks

References

- https://www.wi-fi.org/who-we-are
- https://in.element14.com/wi-fi-architecture-implementation-and-applications
- http://www.cs.nchu.edu.tw/~hwtseng/Wireless%20Networks/2CSMA_CA.pdf