Tishk International University
Science Faculty
IT Department

Wireless Networking

Lecture 6: Wireless LAN

4th Grade - Fall Semester

Instructor: Alaa Ghazi

Topics

- Introduction
- History of Wi-Fi
- WLAN Components (AP and Wireless NIC)
- WLAN Installation Types
- Network Diagram
- THE WiFi STANDARDS
  - IEEE 802.11b
  - IEEE 802.11a
  - IEEE 802.11g
  - IEEE 802.11n
- Wi-Fi Applications
- Basic Wi-Fi Security Techniques
- WiFi Protocol Stack View
- Wireless LAN MAC Addresses
- 802.11 Association Operation
- Ethernet Media Access Control (CSMA/CD)
- 802.11 Media Access Control (CSMA/CA)

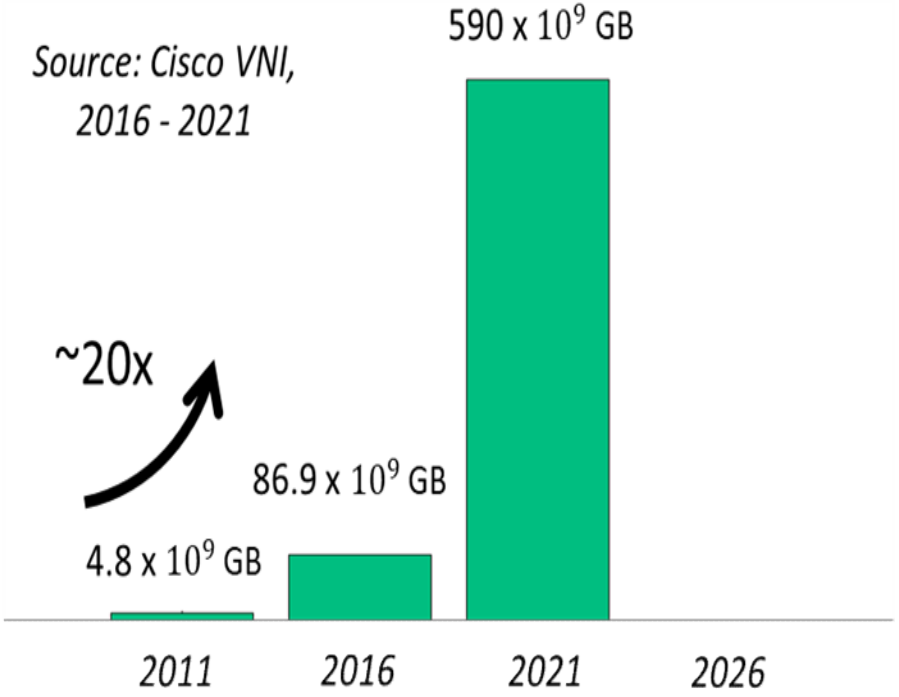
Topics

- 802.11 Physical Layer
  - 2.4 GHz Channels
  - 5 Ghz Channels
- Enabling technologies
  - FHSS
  - DSSS
  - OFDM
- WiFi Application Example: Citywide Wireless Video Surveillance

INTRODUCTION

- **Wi-Fi** (Wireless Fidelity) is a generic term that refers to the IEEE 802.11 communications standard for Wireless Local Area Networks (**WLANs**).
- Wi-Fi works on physical and data link layer.

new apps require ***multi-Gbps*** speeds …



… generating huge volumes of data

History of Wi-Fi

- In 1985 it was allowed to use scientific, medical, and industrial bands of the wireless spectrum. Allowing those bands to be used without government license (inside US), for communication purposes.
- In 1997 the IEEE 802.3 committee agreed on a basic specification that allowed for a wireless data-transfer rate of 2 Mbps. This is the 802.11 base version.
- Two variants 802.11b (operates in 2.4GHz band), and 802.11a (operates in 5.8GHz band) were agreed on in December 1999 and January 2000 respectively.

WLAN components

There are two basic components in wireless network

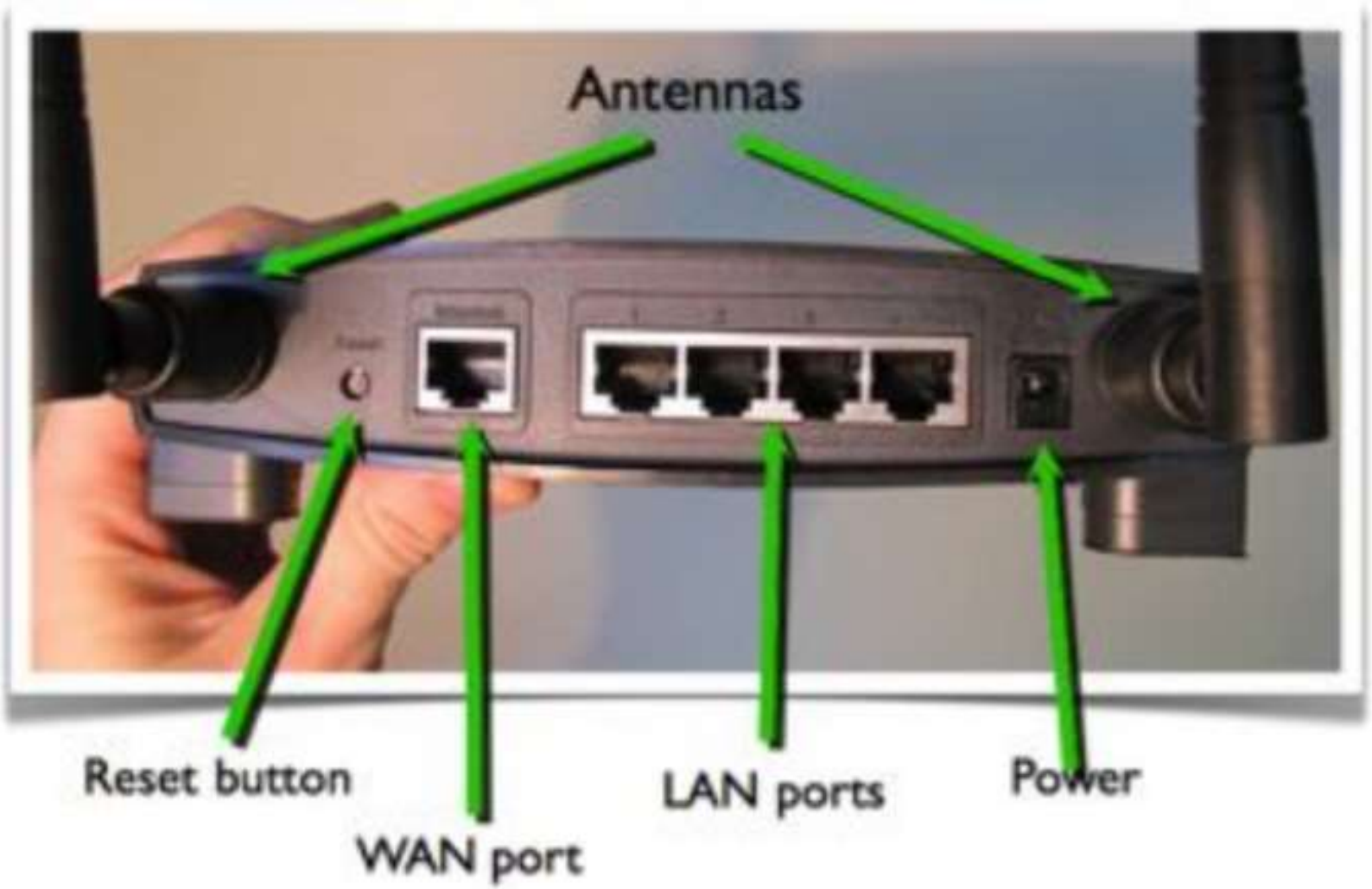
1- Wireless Access Point (AP)

- Is a central component (like a hub or switch)
- Its function is to operate as a hub for wireless devices
- It has at least one antenna
- It has a wired port to connect the wireless AP to a wired network

2- Wireless Network Interface Card (Wireless NIC)

Wireless NIC does the same job as wired NIC ,but instead of having a socket to plug some cable into, the wireless NIC will have a radio antenna.

Wireless Router = AP + Ethernet Router



Types of Wireless NIC

For Desktop

PCI adapter **(Internal)**

USB adapter **(External)**

For Laptop

miniPCI adapter **(Internal)**

USB adapter **(External)**

For Mobile

Built-in WiFi adapter

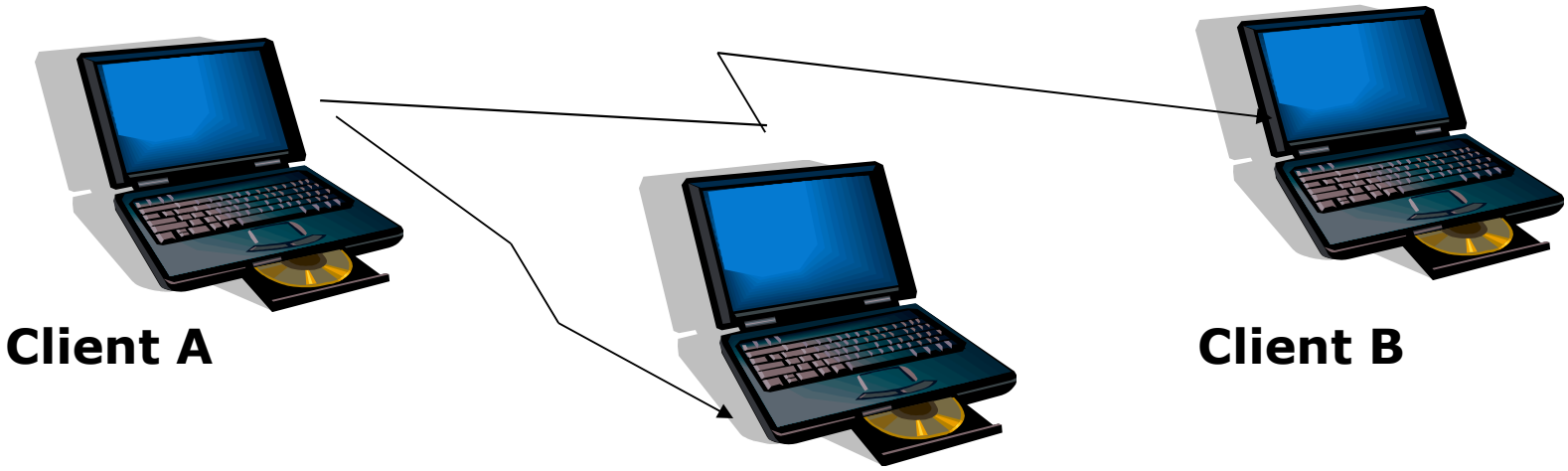
COMMS	WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, DLNA, Wi-Fi Direct, hotspot
	Bluetooth	4.0, A2DP, LE
	GPS	Yes, with A-GPS, GLONASS
	NFC	Yes
	Infrared port	Yes
	Radio	No
	USB	microUSB 2.0, USB On-The-Go

WLAN Installation Types - Ad-Hoc mode

In this mode , the wireless NICs or other devices can communicate directly without the need for an AP

To setup a basic ad-hoc wireless network , two wireless clients are needed.

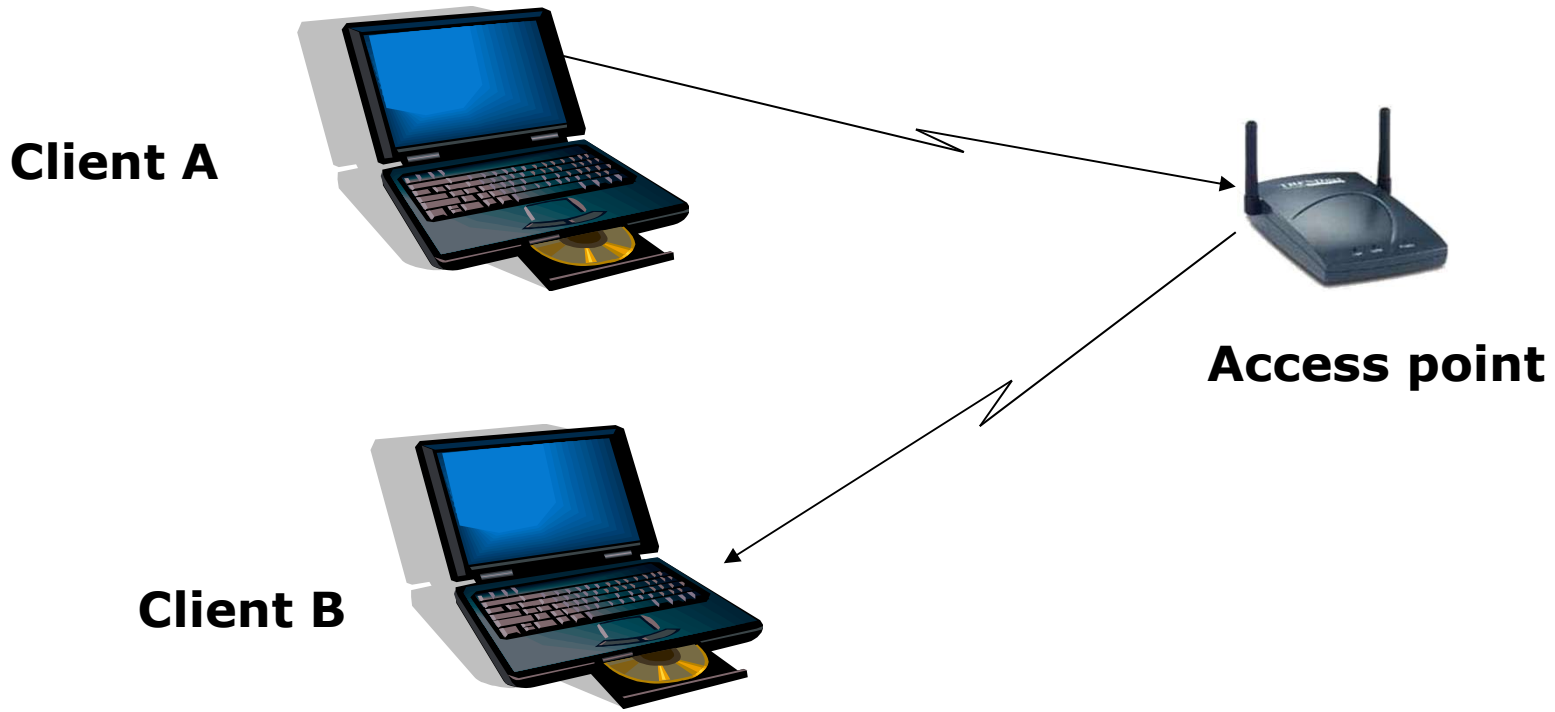
It is also called decentralized mode.



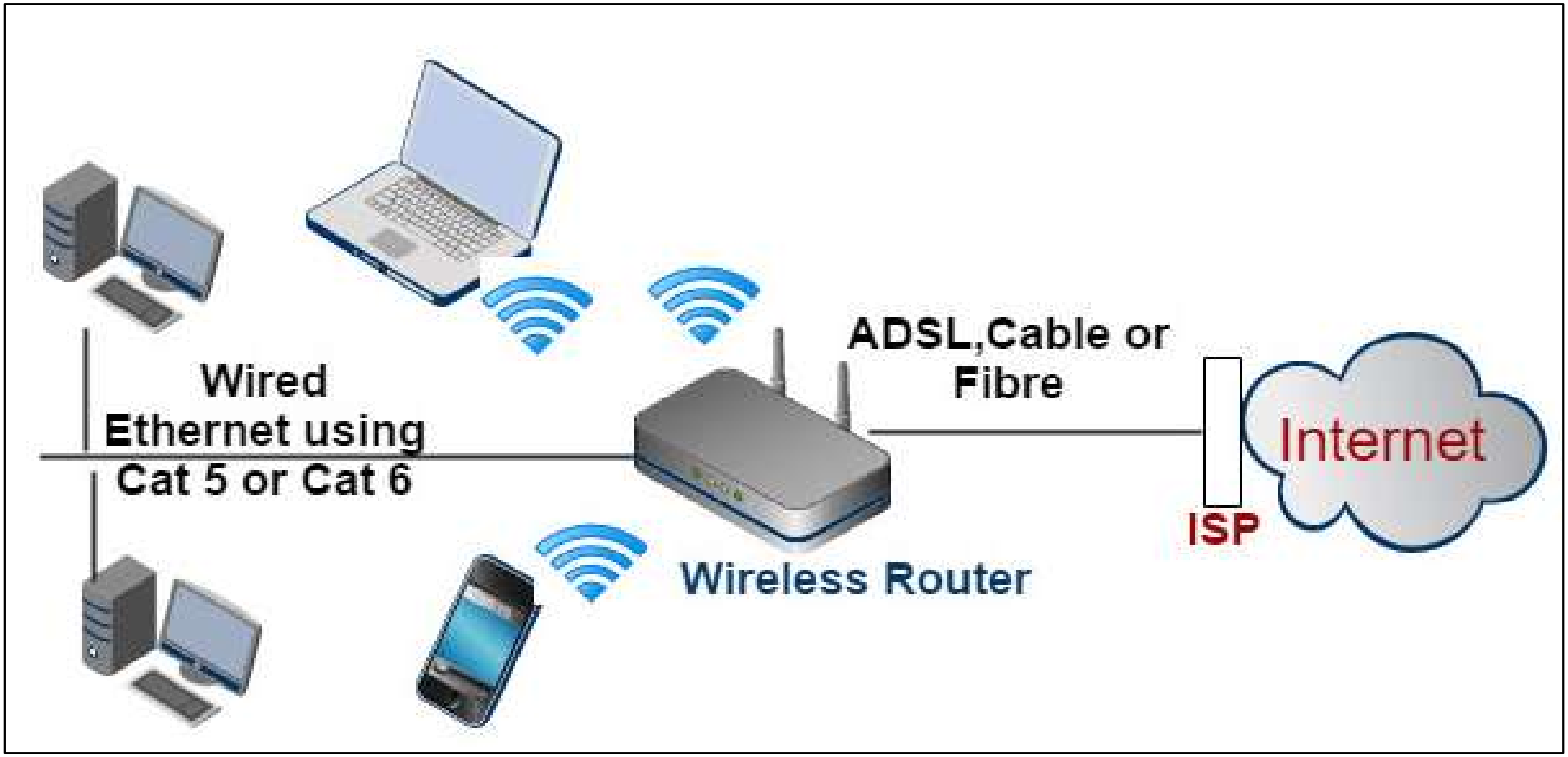
Installation type - Infrastructure Mode

•In this mode , Wireless clients will only communicate with an access point (instead of each other as in ad-hoc mode).

•The access point will facilitate communication between the wireless nodes as well as communication with a wired network.



Network Diagram of Typical WiFi Home Network



THE WiFi STANDARDS

- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11g
- IEEE 802.11n

IEEE 802.11b

- Appeared in late 1999
- Operates at 2.4GHz radio spectrum
- 11 Mbps (theoretical speed)
- 4-6 Mbps (actual speed)
- Least Expensive
- Suffers from interference from mobile phones and Bluetooth devices which can reduce the transmission speed.

IEEE 802.11a

- Introduced in 2001
- Operates at 5 GHz (less popular)
- 54 Mbps (theoretical speed)
- 15-20 Mbps (Actual speed)
- More expensive than 802.11b
- Not compatible with 802.1lb

IEEE 802.11g

- Introduced in 2003
- Combine the feature of both standards (a,b)
- 54 Mbps Theoretical Speed
- Works at 2.4 GHz radio frequencies
- Compatible with 802.11b

IEEE 802.11n

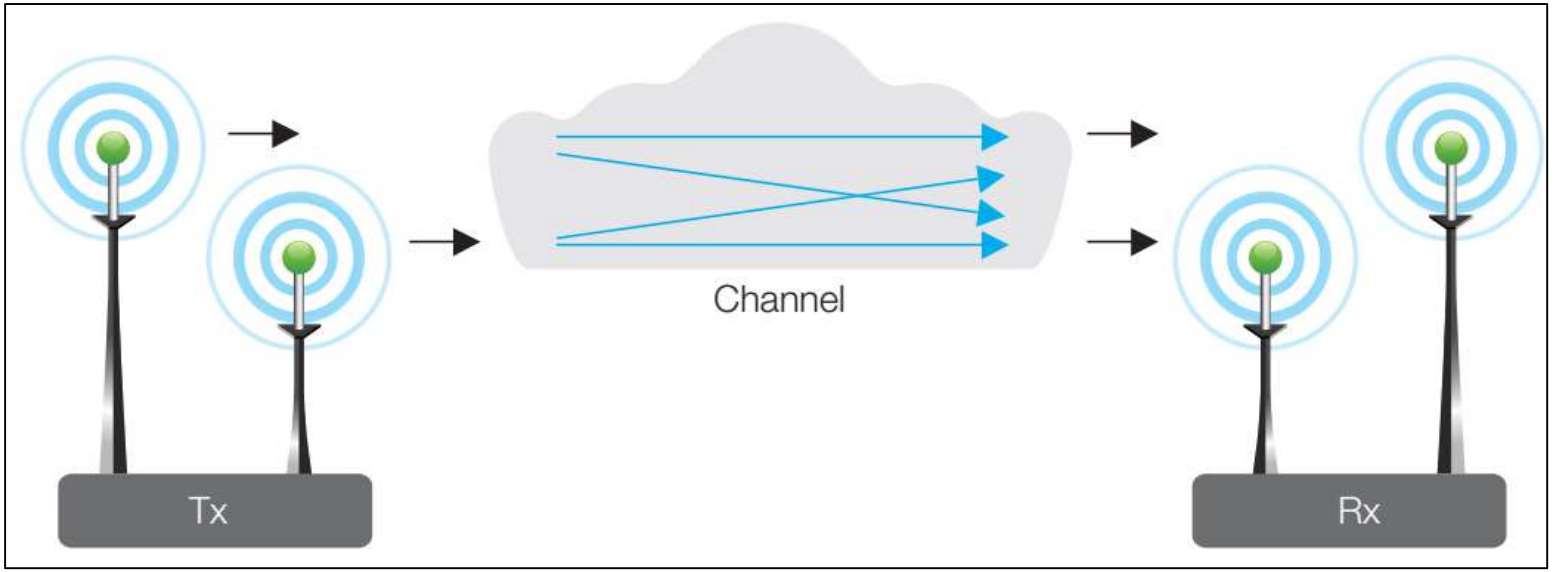
- Introduced in 2009
- 802.11n has become popular because it improves performance.
- The five-fold increase in bandwidth, along with improved reliability from
- MIMO technology has delivered a better user experience
- The actual speed depends on number of antennas
- 2.4 & 5 GHz radio frequencies

802.11n Modes

- **Legacy Mode** – packets are transmitted in the legacy 802.11a/g format.
- **Mixed Mode** – packets are transmitted with a preamble compatible with 802.11a/g so they can be decoded by legacy devices while the rest of the packet is transmitted in the new mode.
- **Green Field** – optional mode where the packets are transmitted without the legacy compatibility part.

Multi Input Multi Output (MIMO)

- **MIMO in WLAN is increasing data rates through the use of multiple spatial streams (known as spatial multiplexing).**
- **MIMO technology increase the diversity or redundancy of the transmission through spatial diversity.**
- **For example, if a SISO system were able to achieve a data rate of 100 Mb/s, an 8x8 MIMO system with 8 spatial streams could achieve a maximum data rate of 800 Mb/s.**



Wi-Fi Applications

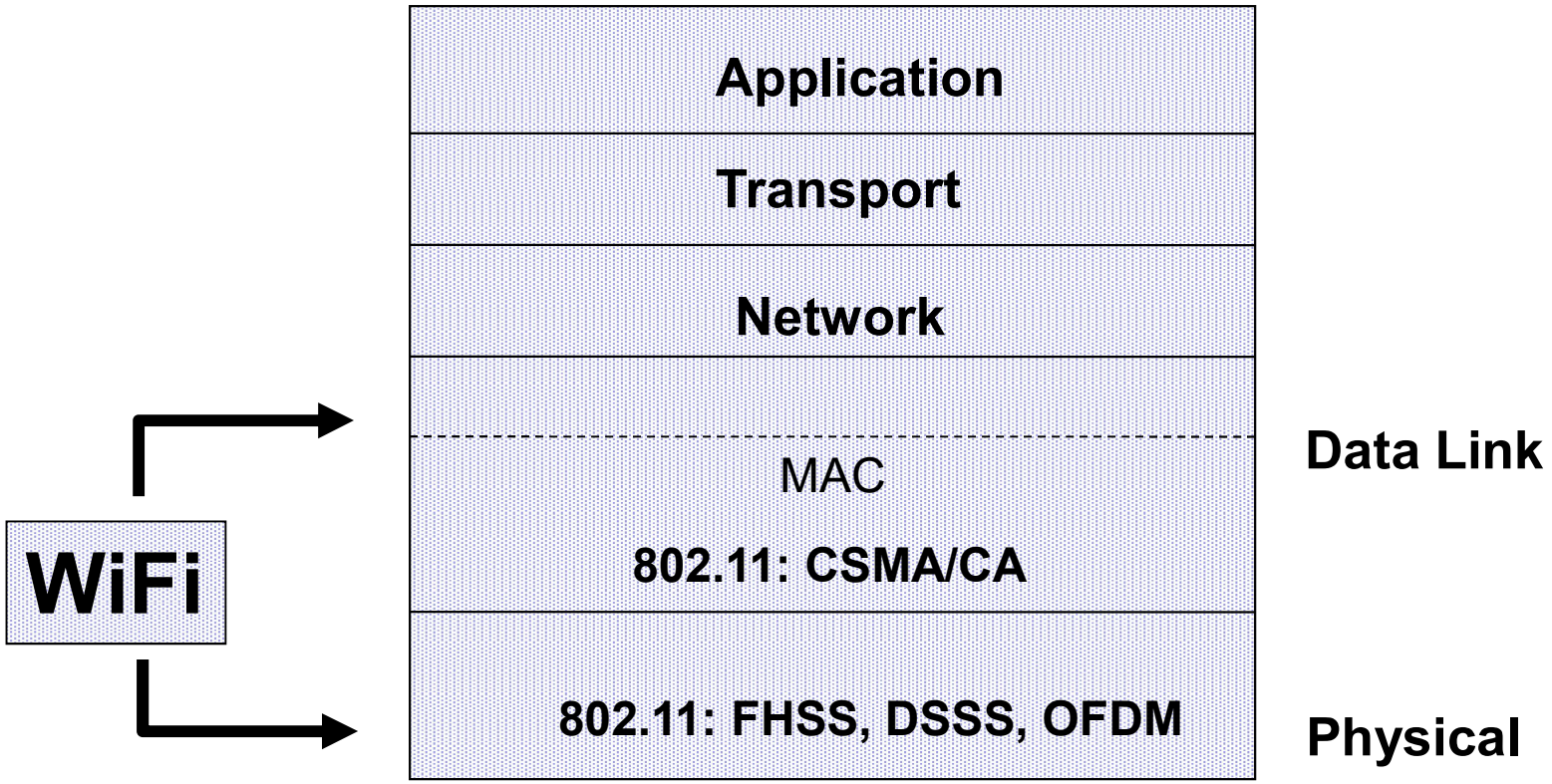
- Home
- Small Businesses
- Large Corporations & Campuses
- Health Care
- Wireless ISP (WISP)
- Travelers
- Wi-Fi Camera

Basic Wi-Fi Security Techniques

1. **WEP:** (Wired Equivalent Privacy) : The original encryption technique specified by the IEEE 802.11 standard. It uses RC4 stream cipher with 64-bit or 128-bit keys. It is no longer used because it can be easily hacked.
2. **WPA:** (Wi-Fi Protected Access): A new standard that provides improved encryption security over WEP. It keeps RC4 stream cipher with 256-bit. After authentication each client gets new encryption key.
3. **WPA2**: Is an improved version of WPA that uses Advanced Encryption Standard (AES) for Encryption.

WiFi Protocol Stack View

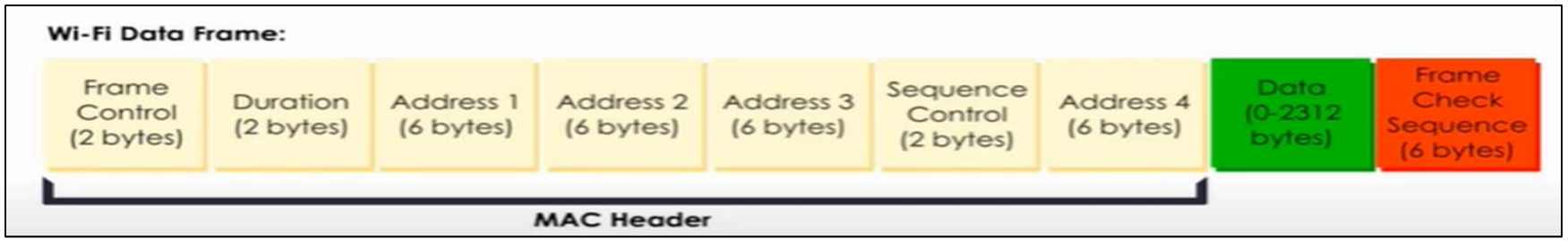
- 802.11 WiFi provides a link-local connection.
- It does not provide any routing functionality.
- Routing is implemented by higher level protocols.



Wireless LAN MAC Addresses

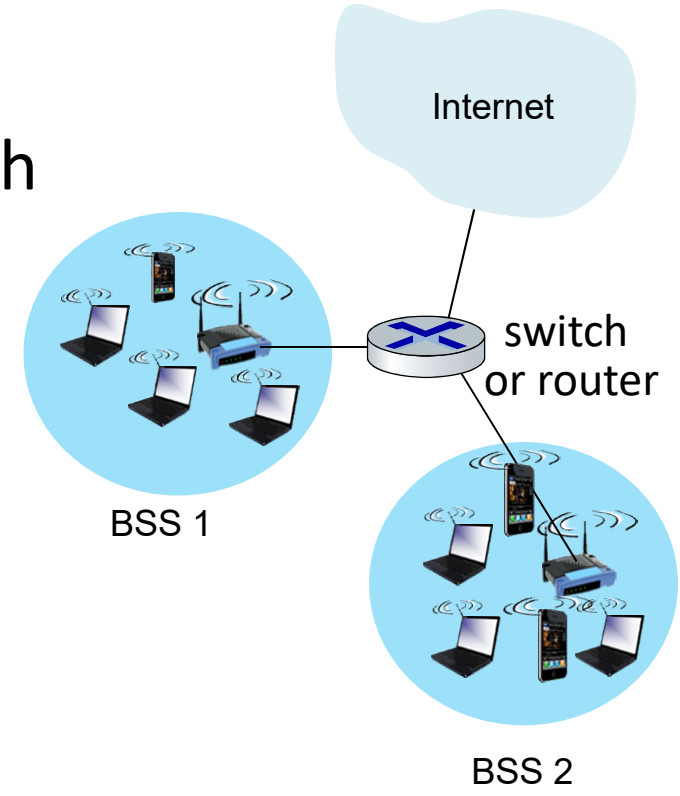
- MAC (or LAN or physical) address:
  - function: *get frame from one interface to another physically-connected interface (same network)*
  - Size is 48 bit or 6 bytes (for most LANs)
  - *The MAC address is burned* in NIC ROM, but also is software settable

```
awm22@rio:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:30:48:fe:c0:64
          inet addr:128.232.33.4  Bcast:128.232.47.255  Mask:255.255.240.0
          inet6 addr: fe80::230:48ff:fefe:c064/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:215084512 errors:252 dropped:25 overruns:0 frame:123
          TX packets:146711866 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:170815941033 (170.8 GB)  TX bytes:86755864270 (86.7 GB)
          Memory:f0000000-f0020000
```



802.11 Association Operation

- Basic Service Set (BSS) in infrastructure mode contains:
  - wireless clients
  - access point (AP): base station
- Admin chooses frequency for AP
- Wireless client communicates with base station (AP)
- New client must associate with an AP through:
  - Passive Scanning, or
  - Active Scanning



802.11: Passive/Active Scanning

passive scanning:

(1)beacon frames sent from APs

(2)association Request frame sent: Client to selected AP

(3)association Response frame sent from selected AP to Client

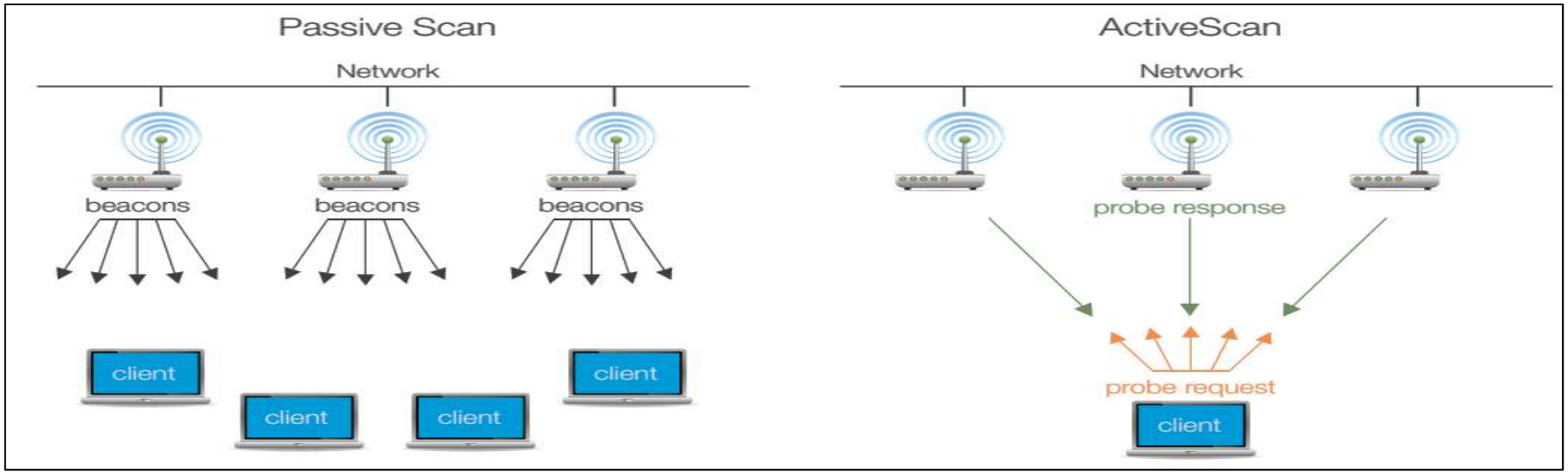
active scanning:

(1) Probe Request frame broadcast from Client

(2) Probe Response frames sent from APs

(3) Association Request frame sent: Client to selected AP

(4) Association Response frame sent from selected AP to Client



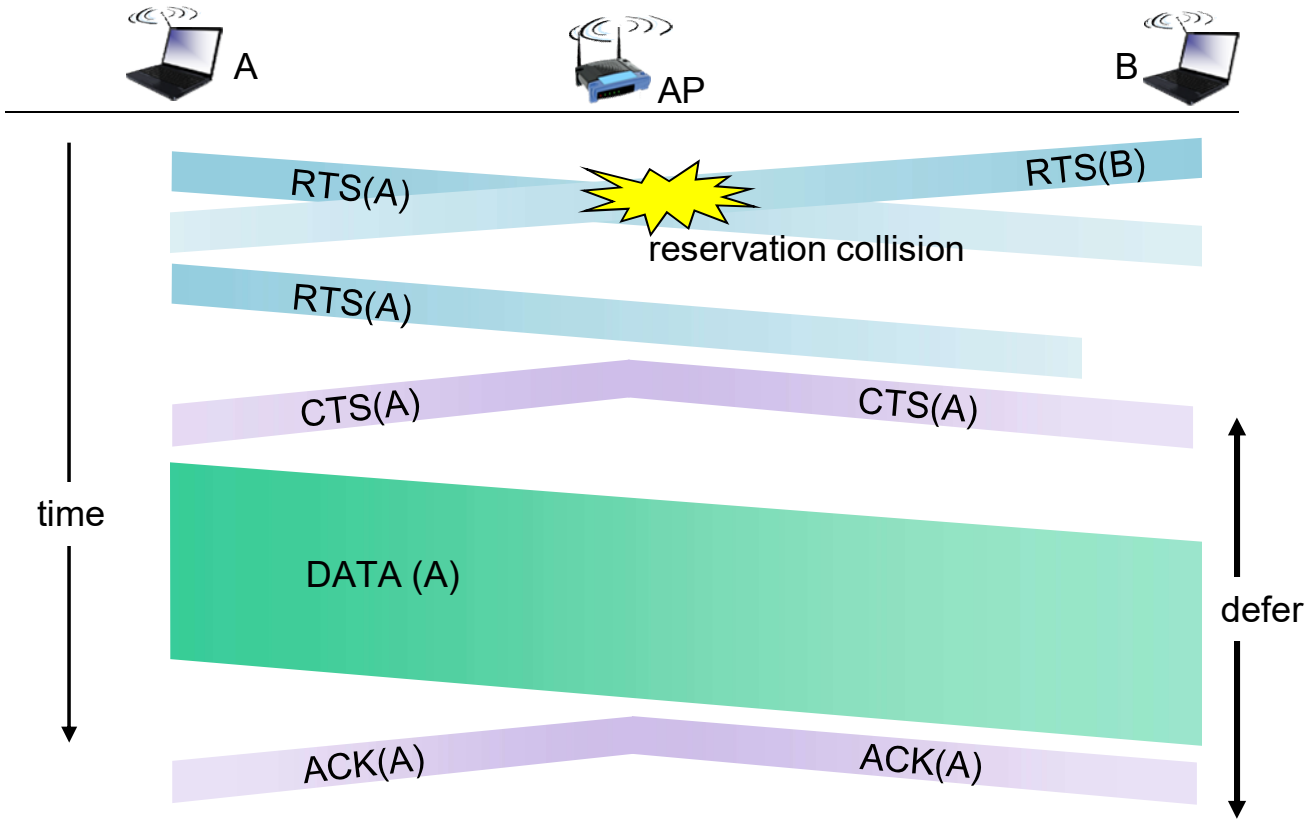
Ethernet Media Access Control (CSMA/CD)

- **Carrier Sense Multiple Access (CSMA)**: listen before transmit
  - If channel sensed idle: transmit entire frame
  - If channel sensed busy, defer transmission
- Human analogy: don't interrupt others!
- **Collision detection (CD)**: listen while transmitting
  - No collision: transmission is complete
  - Collision: abort transmission & send jam signal
- **Random access**: Choose random time for re-transmission
- Collision detection easy in Ethernet, but difficult in wireless.

802.11 Media Access Control (CSMA/CA)

- **Carrier Sense Multiple Access with collision Avoidance (CSMA/CA)**
- **Hidden Node Problem**: In wireless networks, when a sending device checks whether the channel is idle, it can only check within its broadcast range. So two devices can send data to the AP at the same time, and AP would not be able to receive any data due to the data collisions.
- **How CSMA/CA works**: Once the channel is determined to be idle, client send Request to Send (RTS) packet. The AP device then sends a Clear to Send (CTS) reply to the request. This way it knows which device asked to send first and can ensure that only that device will send its message, not responding to further RTS signals until the original sender has finished.

Collision Avoidance: RTS-CTS exchange



802.11 Physical Layer

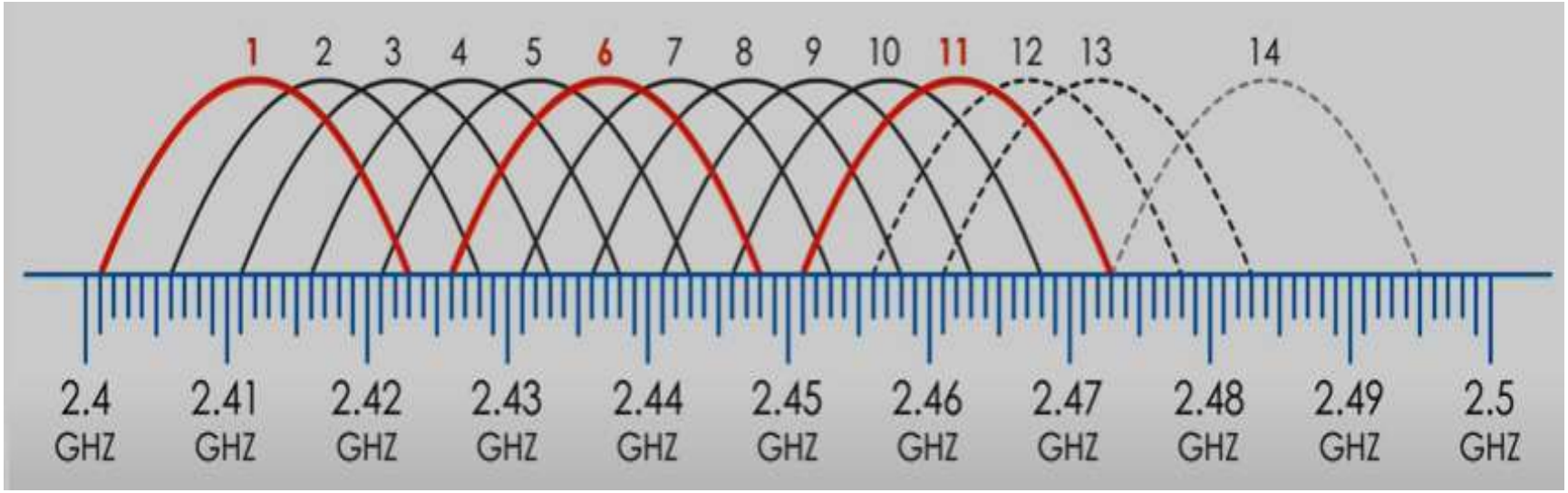
- The 802.11 physical layer works on two frequencies ranges:
  - 2.4 GHz and
  - 5 Ghz.

- The 802.11 physical layer specifications use a range of key enabling technologies that enable them to robustly achieve high data rates with reasonable spectrum utilization. The enabling technologies are:

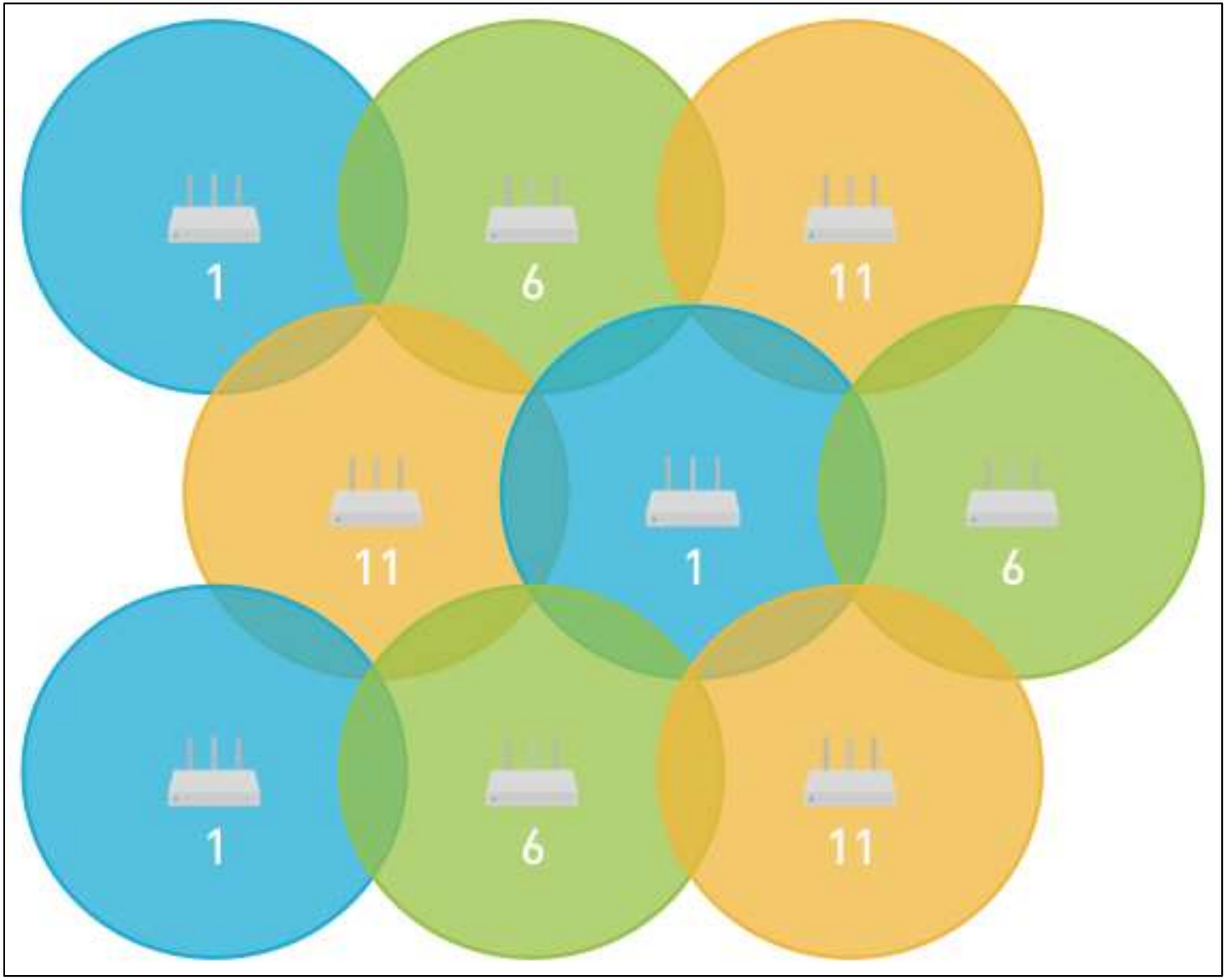
  - FHSS
  - DSSS
  - OFDM

2.4 GHz Channels

- 2.4 GHz WLAN/Wi-Fi Technology (802.11 b/g/n) uses the frequency band from 2401 to 2484 MHz. This bandwidth is divided among 14 channels. Each of the WLAN / Wi-Fi Channels are spaced 5 MHz apart, except the last two channels which are spaced 12 MHz apart.
- The non-overlapping channels are: 1, 6, and 11.



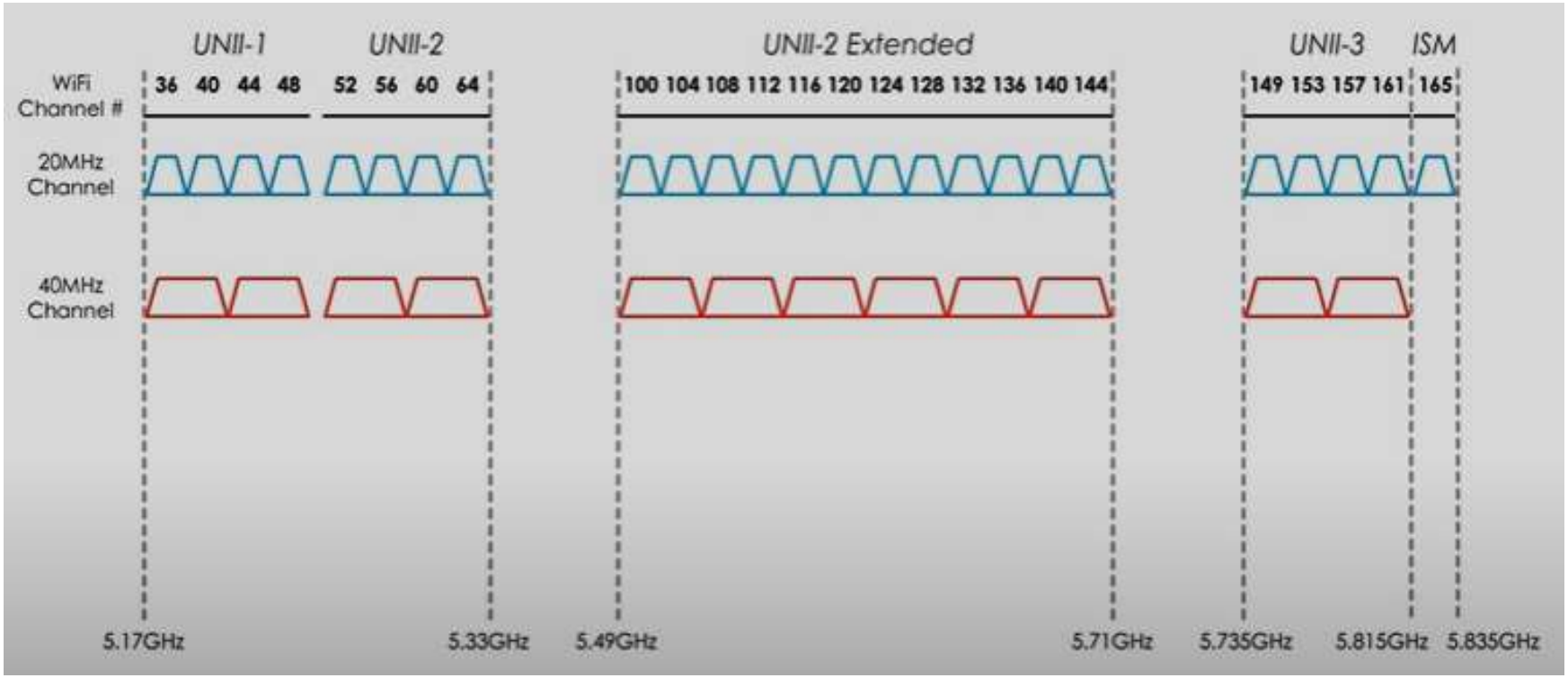
802.11b/g WiFi Channel Reuse



Typical Indoor WiFi Floor Plan (not required in the exam)

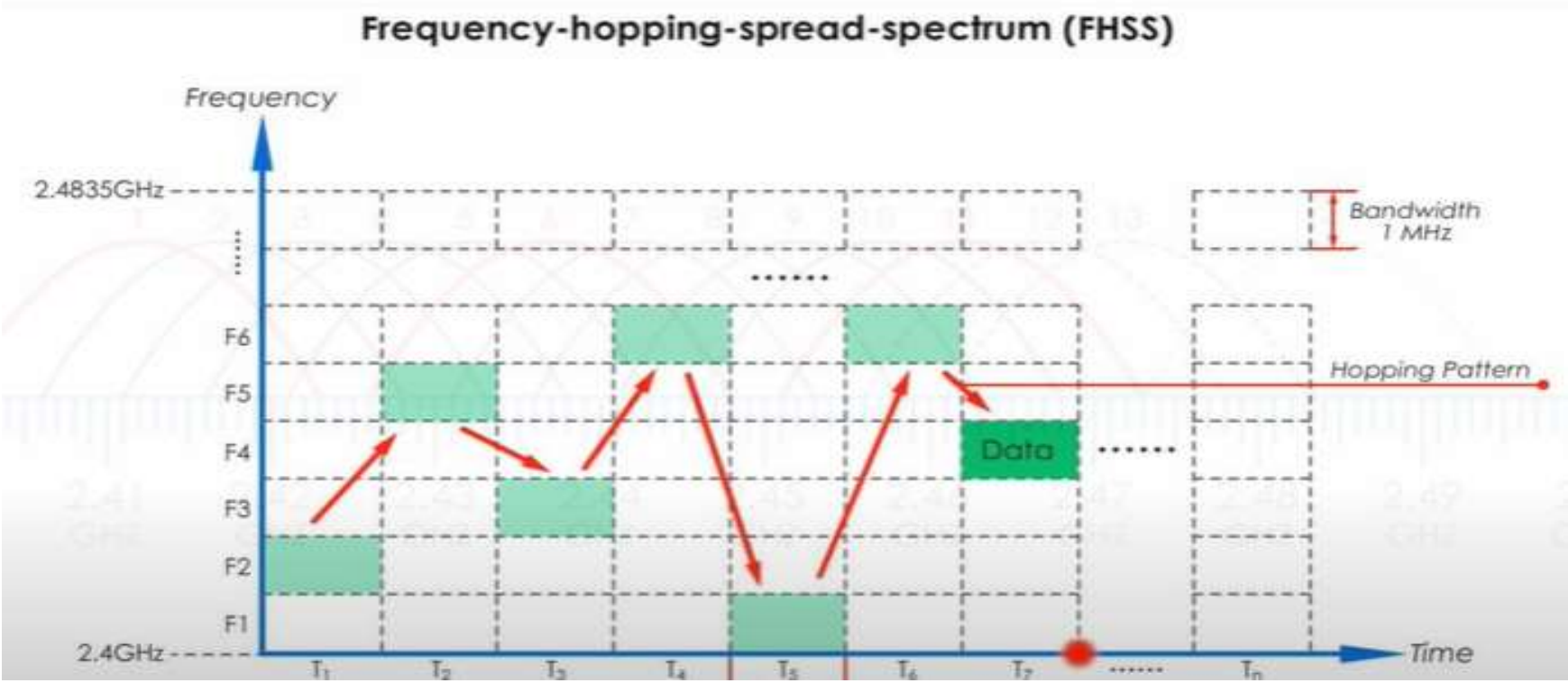
5 GHz Channels

- The 5 GHz Wi-Fi band covers a range from 5.725 GHz to 5.835 GHz.
- Using 20 MHz width, there are 24 non-overlapping channels available within the 5 GHz band.
- The 802.11n standard introduced **channel bonding**, which enabled 40 MHz widths.



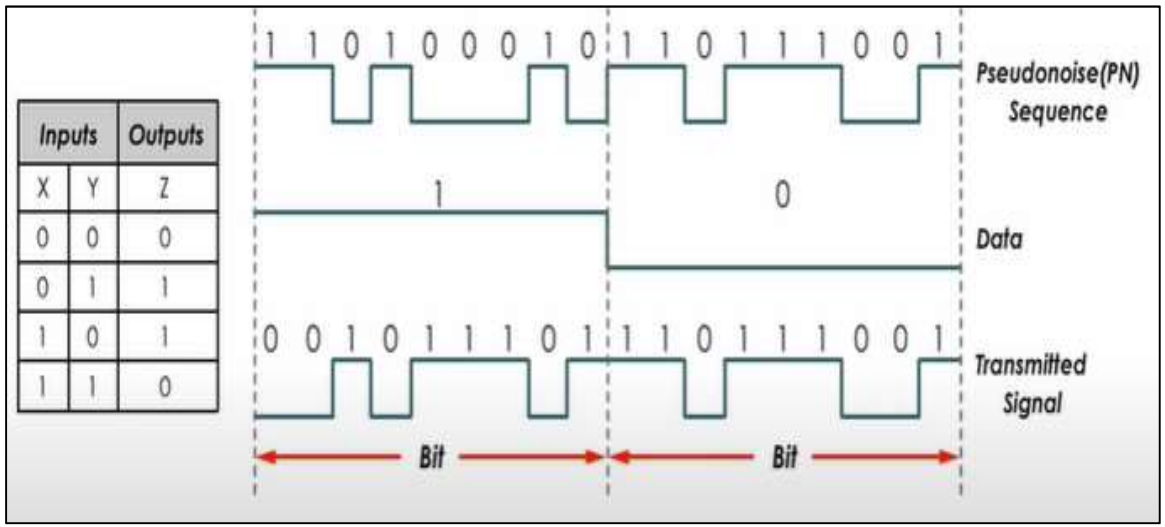
Frequency Hoping Spread Spectrum (FHSS)

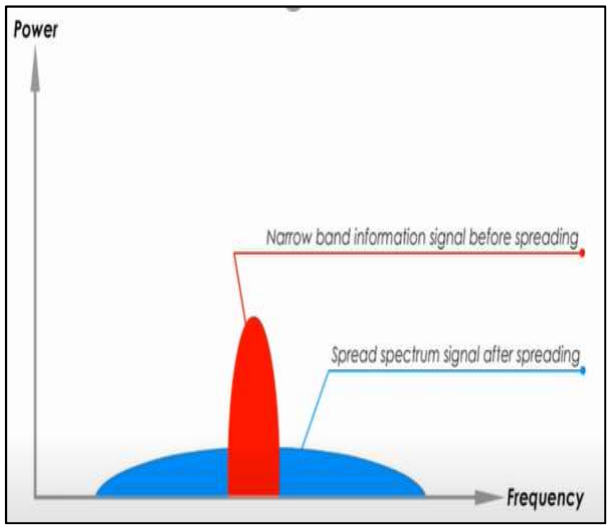
FHSS is a method of transmitting radio signals by shifting carriers across numerous channels with pseudorandom sequence which is already known to the sender and receiver.



Direct Spread Sequence Spectrum (DSSS)

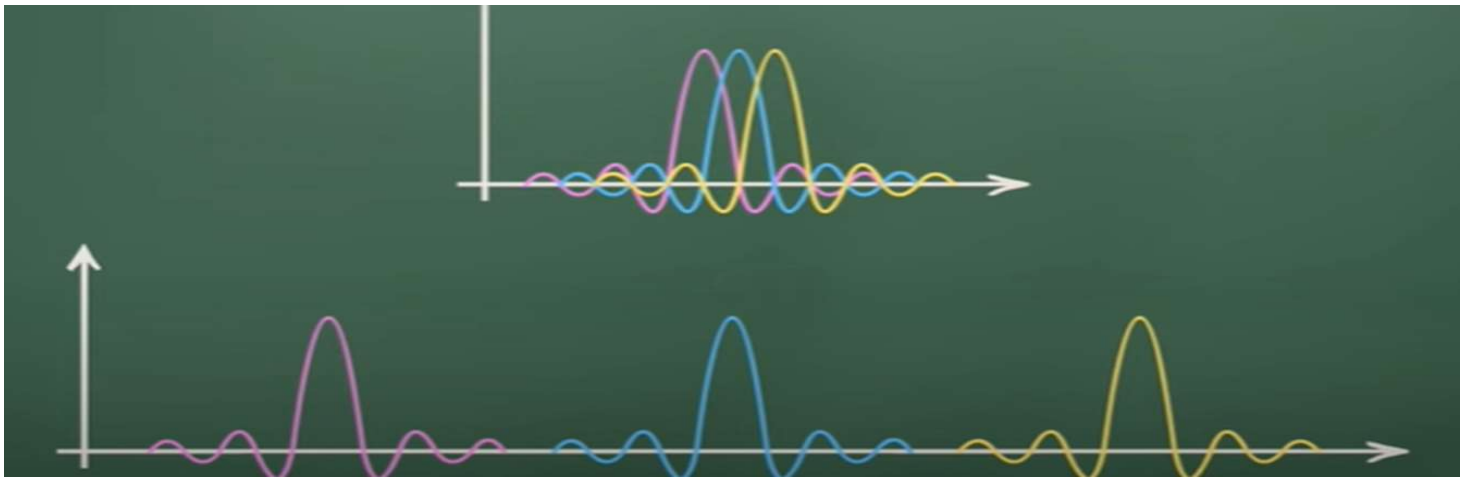
- In DSSS transmissions, the modulated signal is multiplied by a pseudorandom spreading code and the receiver is only able to demodulate the signal by applying the same spreading code in its tracking of the signal.
- DSSS offers protect against interference in the 2.4 GHz spectrum, which is also utilized by other wireless technologies.





Orthogonal Frequency Division Multiplexing (OFDM)

- OFDM was first adopted as part of the 802.11a specification, and then 802.11g specification.
- 802.11n uses OFDM for all bandwidth configurations.
- In OFDM the transmitter creates an array of subcarriers that all work together to transmit information over a range of frequencies.
- These subcarriers must be orthogonal to each other and they will have minimal interference to the other subcarriers, resulting in efficient use of bandwidth



WiFi Application Example: Citywide Wireless Video Surveillance

Designing a Citywide Wireless Surveillance System – "the right way" – is a highly complex task, underestimated by many.
When high motion is encountered, at 30 Frames Per Second (FPS) and 4CIF resolution, a single video stream requires as much as **4 Mbps** (using MPEG-4 encoding).
In most citywide surveillance systems, wireless technology enables a municipality to build out the system at an affordable cost point. However, if the wireless part of the network is not properly designed, the customer will be disappointed with the performance of the network.

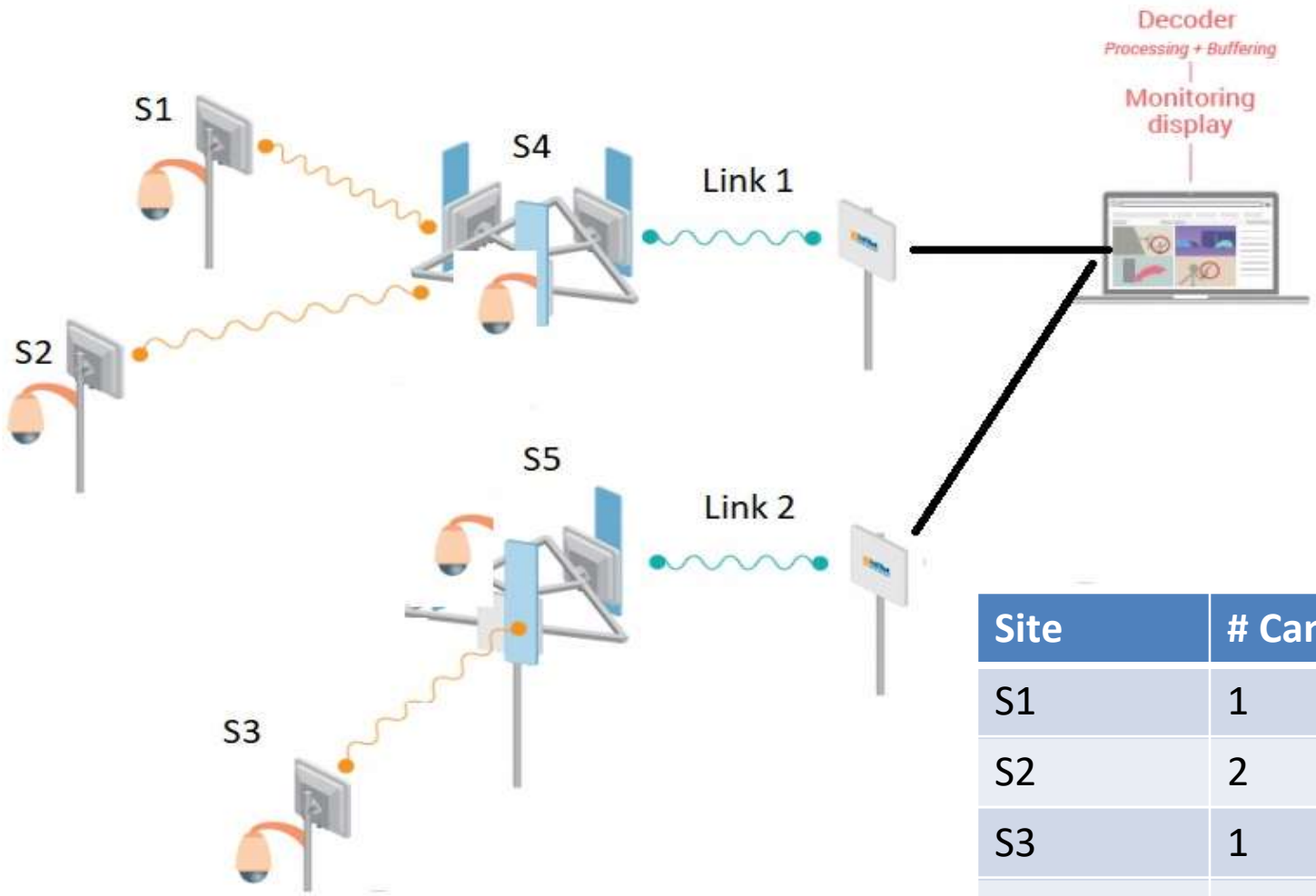
WiFi Application Example:
Citywide Wireless Video Surveillance

Example 1

Assume in the Network diagram below, and the number of cameras in each site as shown in the attached table.
If the Camera bandwidth requirement is 4 Mbps, then calculate the bandwidth required for Link 1 and Link 2 and then pickup the right Rx sensitivity for each link.
TX power of 30 dBm and Antenna Gain for Tx and Rx is 18 dBi
The antennas are integrated so there is no cable loss in Tx and Rx
Link 1 distance is 10 Km
Link 2 distance is 12 Km
Frequency is 5 GHz

Calculate Link budget for both Links

Example1-Network Diagram



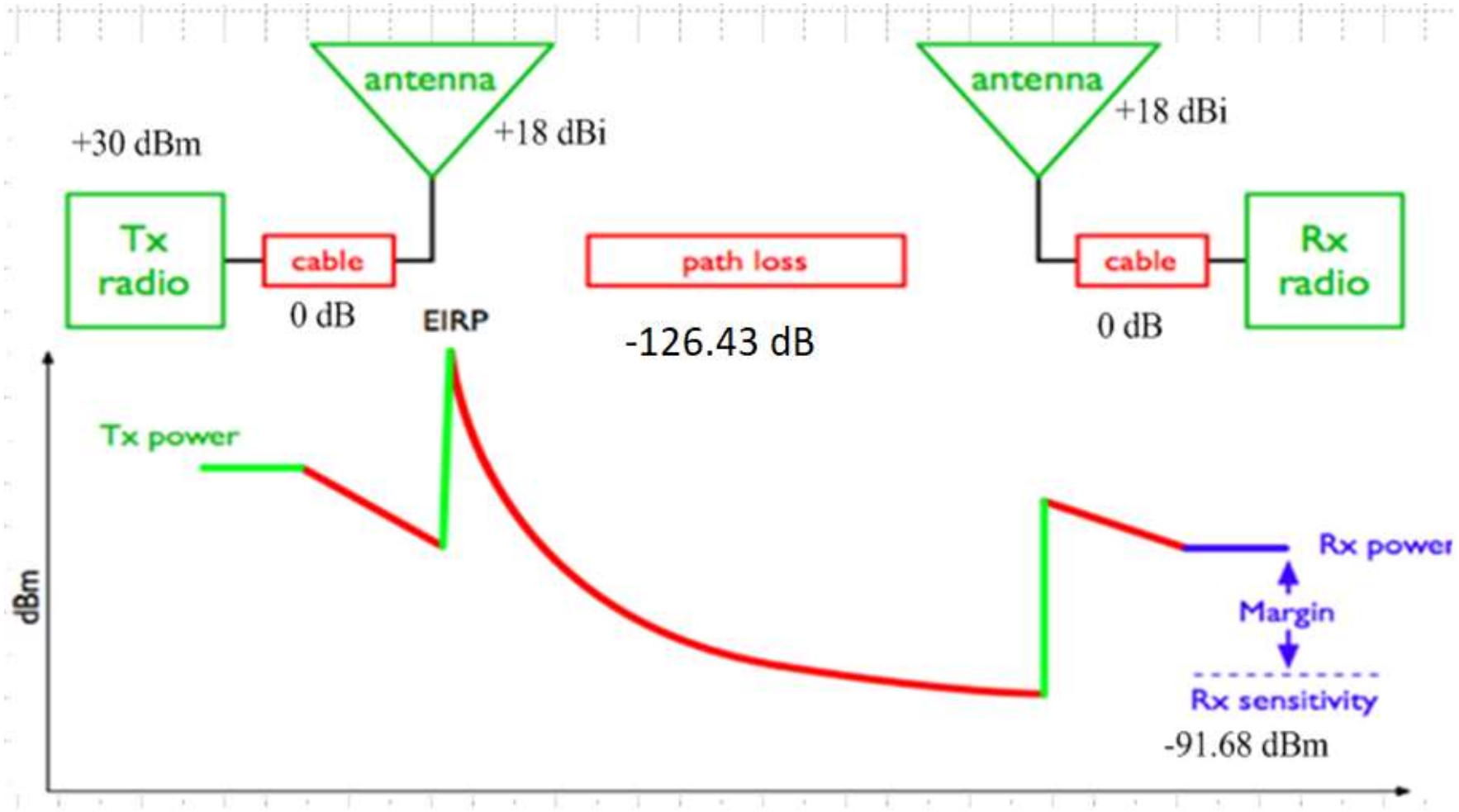
Site	# Cameras
S1	1
S2	2
S3	1
S4	1
S5	2

Example 1- Data Sheet

Parameters	SNR (Rx) [dB]	RESICEVER Sensitivity S_R [dB]	Usefull Channel Capacity Cmodulation [Mbps]
QPSK CTC 1/2	3.5	-98.6561	4.0816
QPSK CTC 3/4	6.5	-97.4170	6.1224
16-QAM CTC1/2	9.0	-96.1664	8.1633
16-QAM CTC 3/4	12.5	-94.4273	12.245
64-QAM CTC 2/3	16.5	-91.6767	16.327
64-QAM CTC 3/4	18.5	-90.1883	18.367

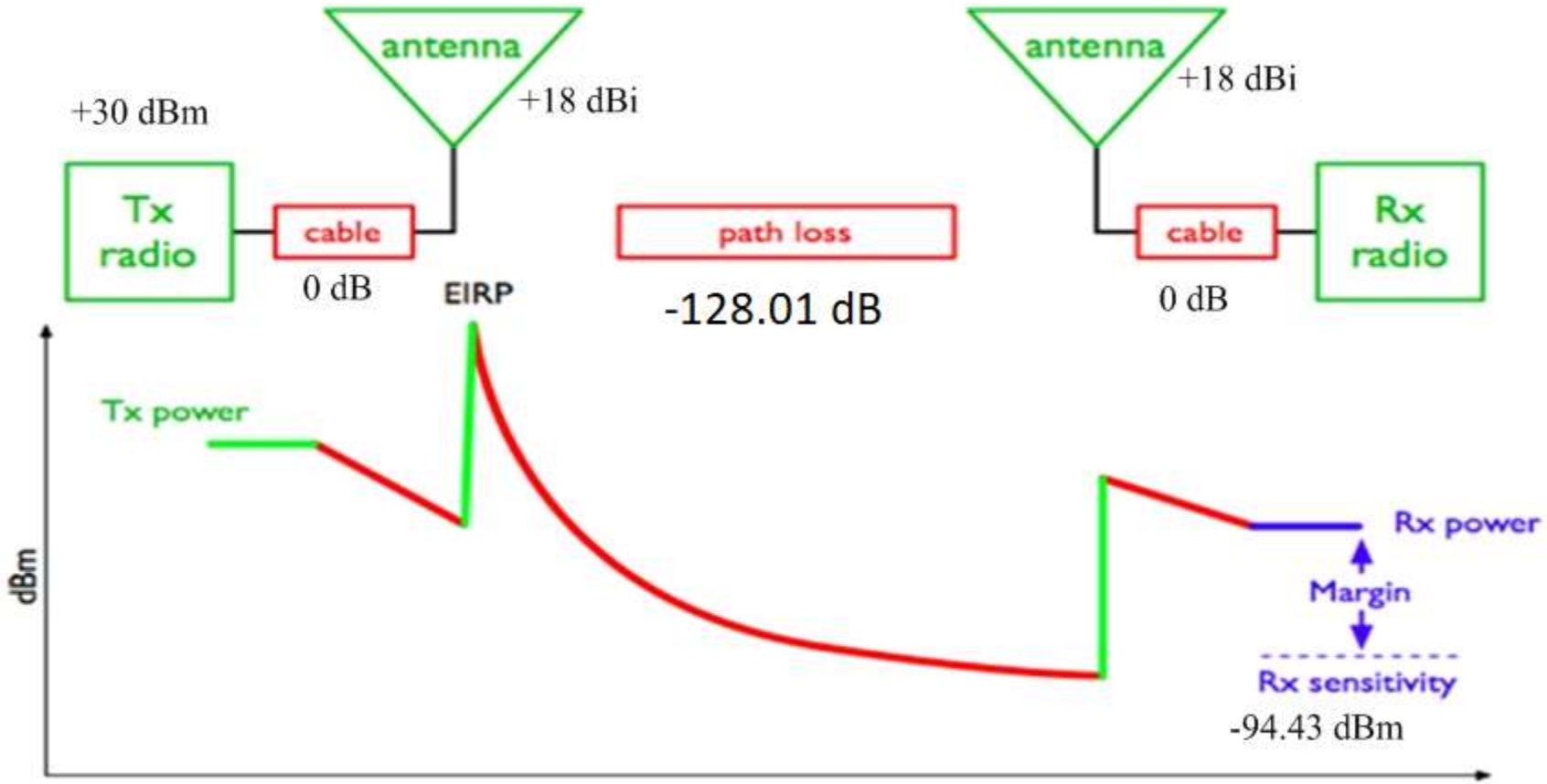
Example1 - Solution

First we need to calculate the data rate required in each link
Link 1 = S1 + S2 +S4 = 4 Cameras
So Link 1 data rate = 4 Mbps x 4 = 16 Mbps
Link 2 = S3 + S5 = 3 Cameras
So Link 2 data rate = 4 Mbps x 3 =12 Mbps
From the table pick the right receive sensitivity and then calculate the link budget.
Receive Sensitivity for Link 1 is -91.68 dBm
Link 1 FSL = 92.45 + 20 * log(f * d)
= 92.45 + 20 * log(5 * 10) = 126.43 dB
Receive Sensitivity for Link 2 is -94.43 dBm
Link 2 FSL = 92.45 + 20 * log(f * d)
= 92.45 + 20 * log(5 * 12) = 128.01 dB


antenna
+18 dBi
+30 dBm
Tx radio
cable
0 dB
EIRP
path loss
-126.43 dB
antenna
+18 dBi
cable
0 dB
Rx radio
Tx power
dBm
Rx power
Margin
Rx sensitivity
-91.68 dBm

Link 1: Link budget Calculation

+ 30	dBm	(TX Power AP)
0	dB	(Cable Losses AP)
+ 18	dBi	(Antenna Gain AP)
-126.43	dB	(free space loss @12 km , 5GHz)
+ 18	dBi	(Antenna Gain Client)
0	dB	(Cable Losses Client)
- 60.43	dBm	(expected received signal level)
-		
- 91.68	dBm	(sensitivity for speed 12 Mbps)
31.25	dB	(link budget)


antenna
+18 dBi
+30 dBm
Tx radio
cable
0 dB
EIRP
path loss
-128.01 dB
antenna
+18 dBi
cable
0 dB
Rx radio
Tx power
dBm
Rx power
Margin
Rx sensitivity
-94.43 dBm

Link 2: Link budget Calculation

+ 30 dBm (TX Power AP)
0 dB (Cable Losses AP)
+ 18 dBi (Antenna Gain AP)

-128.01 dB (free space loss @12 km , 5GHz)

+ 18 dBi (Antenna Gain Client)
0 dB (Cable Losses Client)

- 62.01 dBm (expected received signal level)
-
- 94.43 dBm (sensitivity for speed 12 Mbps)

32.42 dB (link budget)