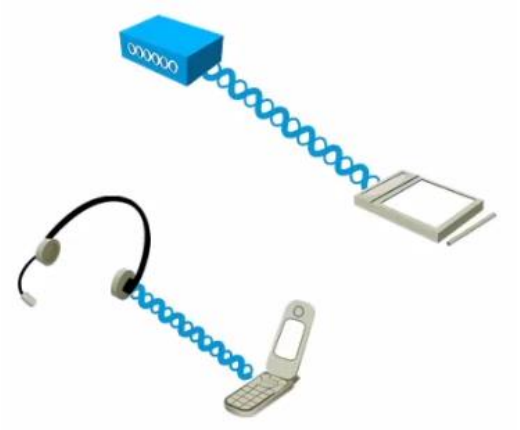
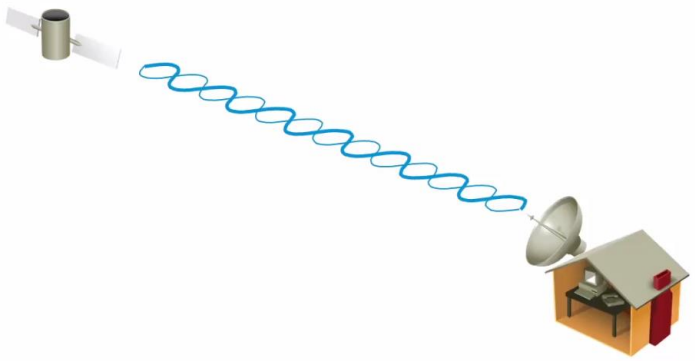
Understanding WPAN,WLAN,WMAN and WWAN

- First Wireless transmission in 1870
- Every time you connect to device without cable is wireless connection





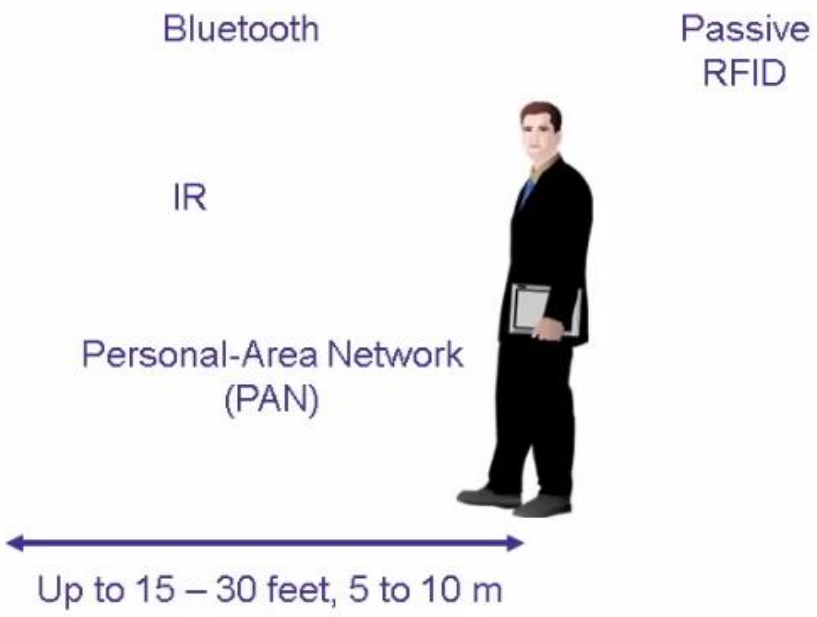
What is Wi-Fi and how you classify wireless communication ?

Classification:

- Based on Application you are using
- Based on throughput you are trying to achieve
- Based on distance

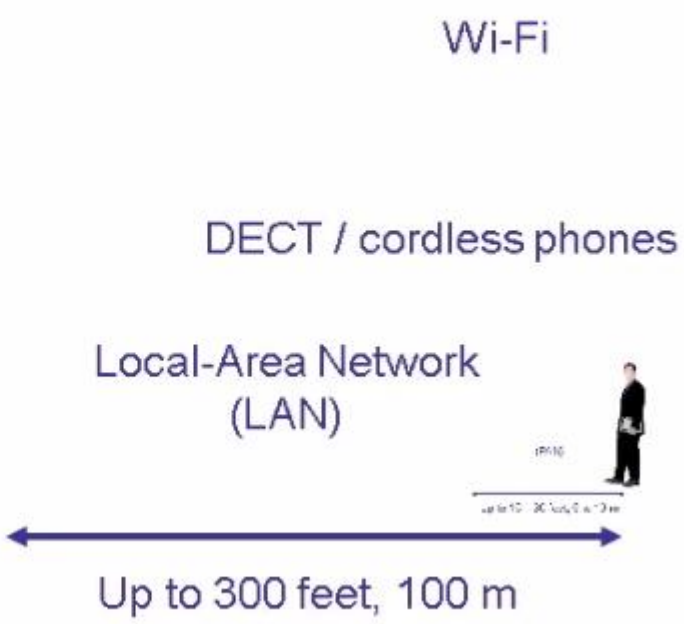
Classification based on Distance

- Wireless…
  - Personal-Area Network (WPAN) - up to 30 feet / 10 m

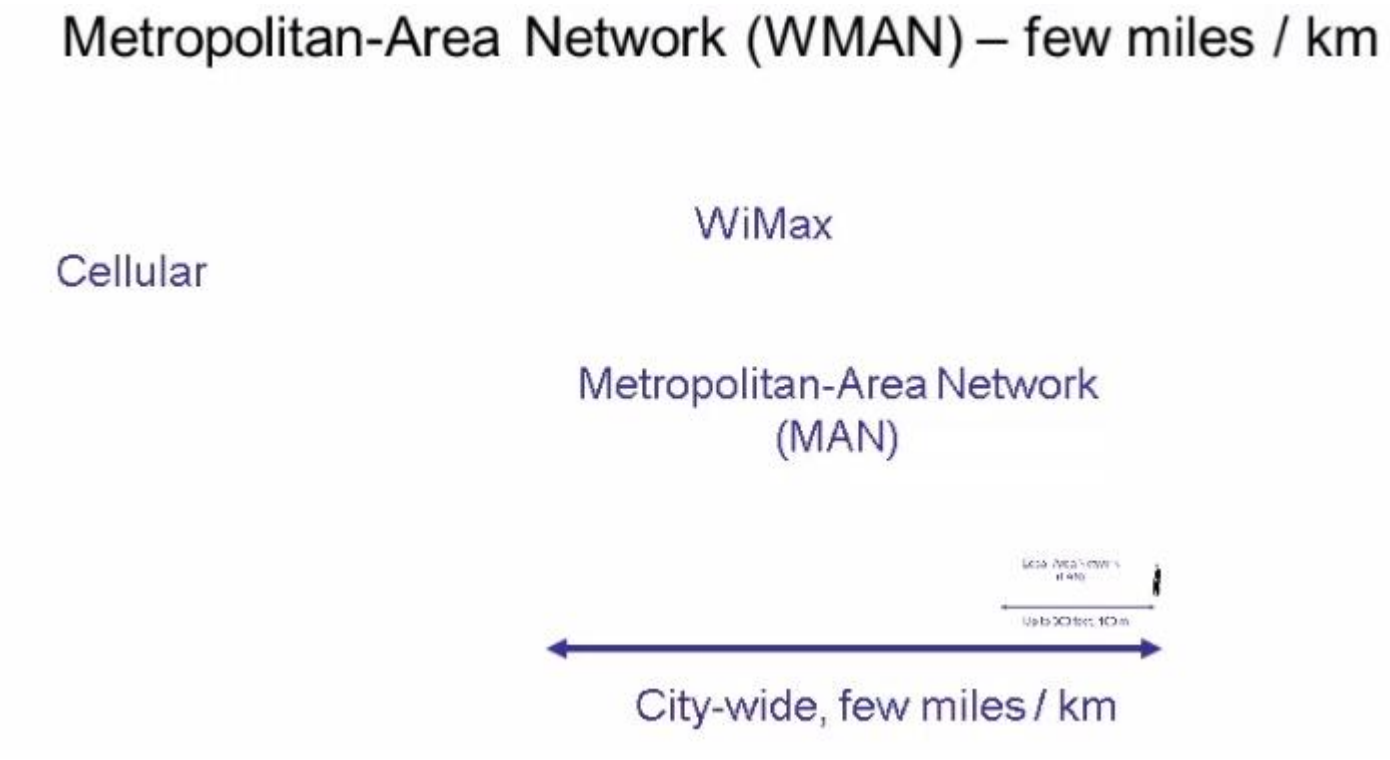


Classification based on Distance contd..

- Local-Area Network (WLAN) – up to 300 feet / 100 m



Classification based on Distance contd..



Classification based on Distance contd..

- Wide-Area Network (WWAN) – several hundreds/thousands miles / km

Cellular

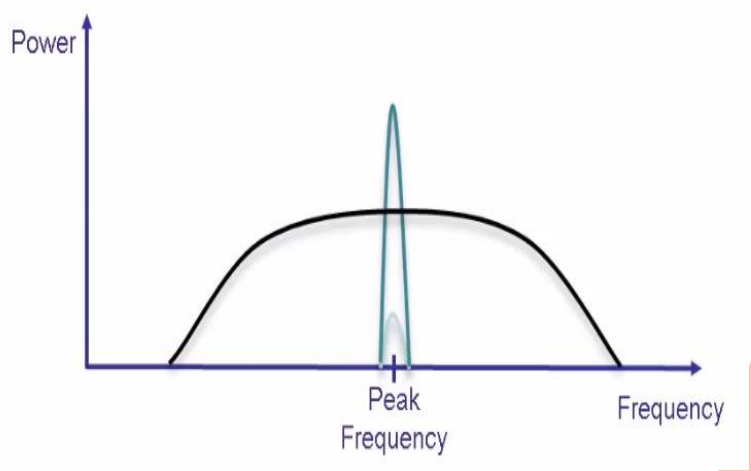
Wide-Area Network
(WAN)

Long range radios

Satellite

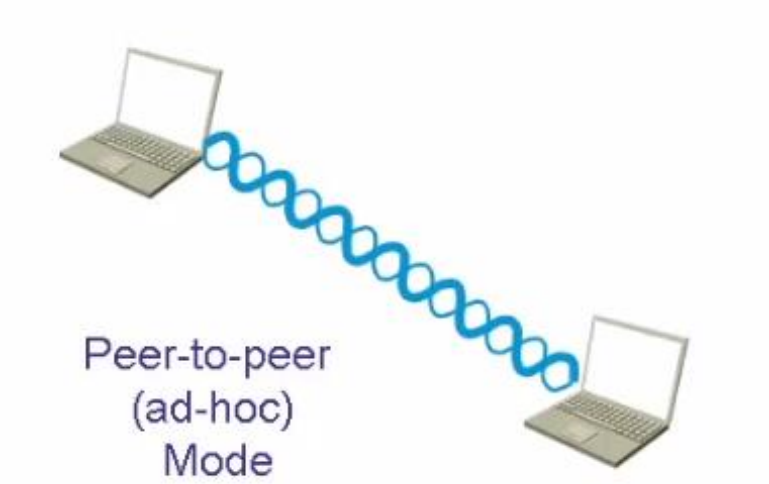
Communication characterized according to power and frequency utilization

- Frequency is set between sender and receiver to exchange information
- Depending upon the type of application
  - Narrow frequency range is chosen in radio for audio
    - For long range radio communication increase power
  - To send lot more than voice like TV signal on top of voice
    - Signal spread beyond peak frequency



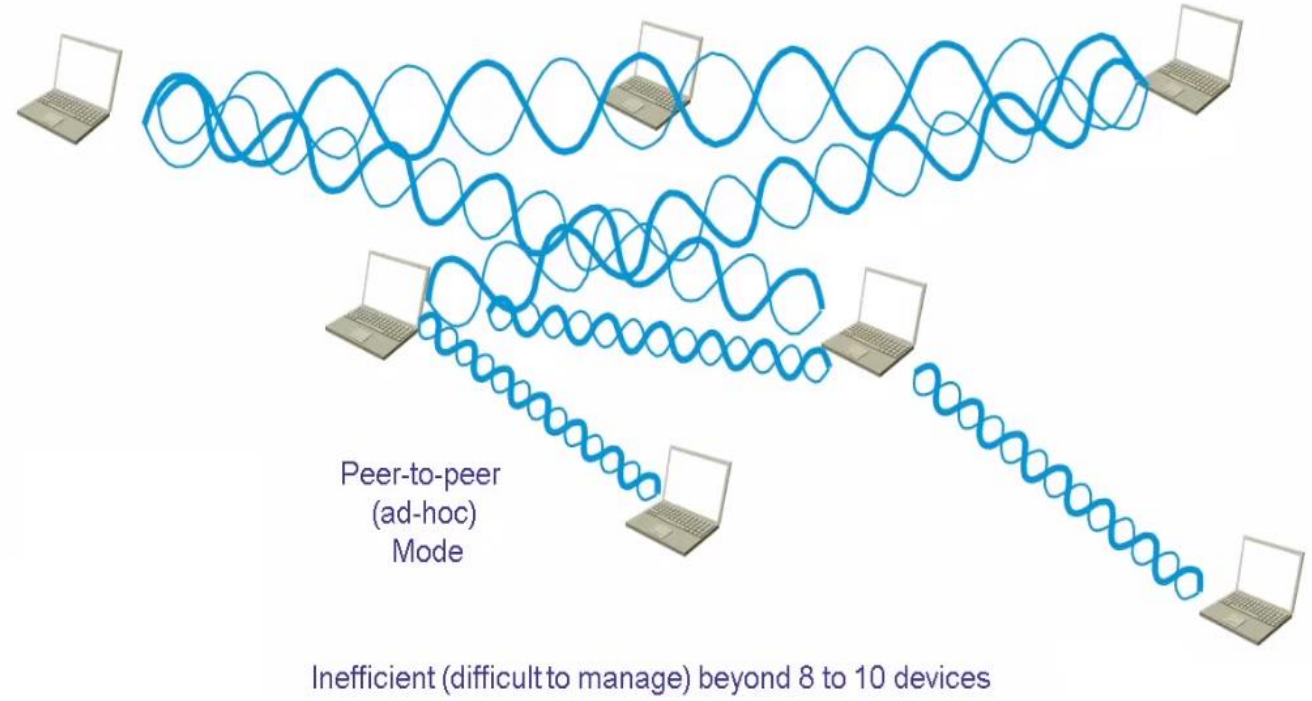
How you communicate with Wi-Fi depending upon use of Access Point

- Here just need to set connection



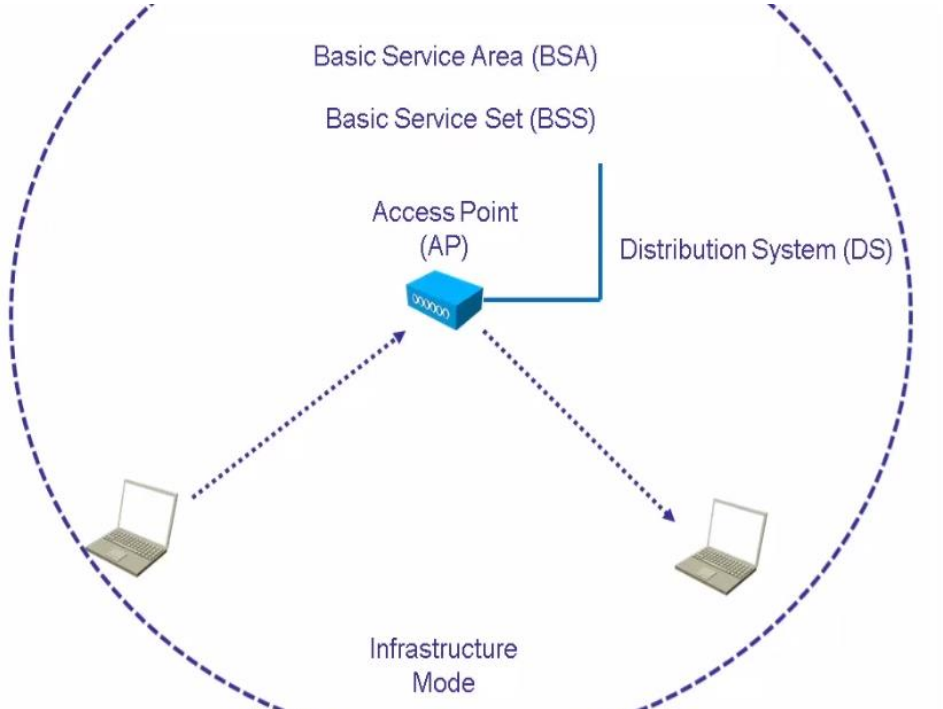
How you communicate with Wi-Fi depending upon use of Access Point cont….

- All devices need to communicate with all others creates complexity and collision due to lack of coordination tends to increase in loss of packet



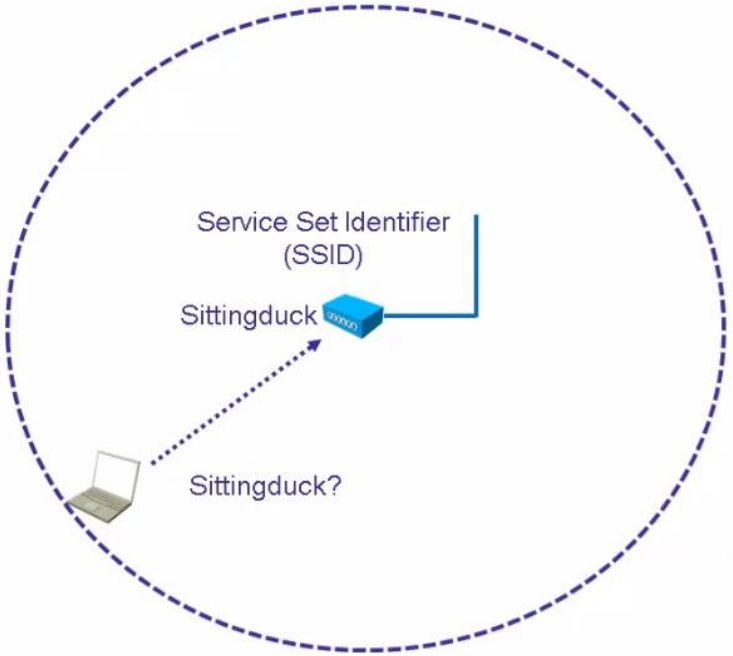
How you communicate with Wi-Fi depending upon use of Access Point cont….

- So need of central device that regulates who sends to whom called AP
- AP works as bridge between wireless world and wired world
- Here Distribution system is the function of the AP to be able to distribute frame to the wired connection
- BSA is area covered by AP
- Function of AP to connect is called BSS



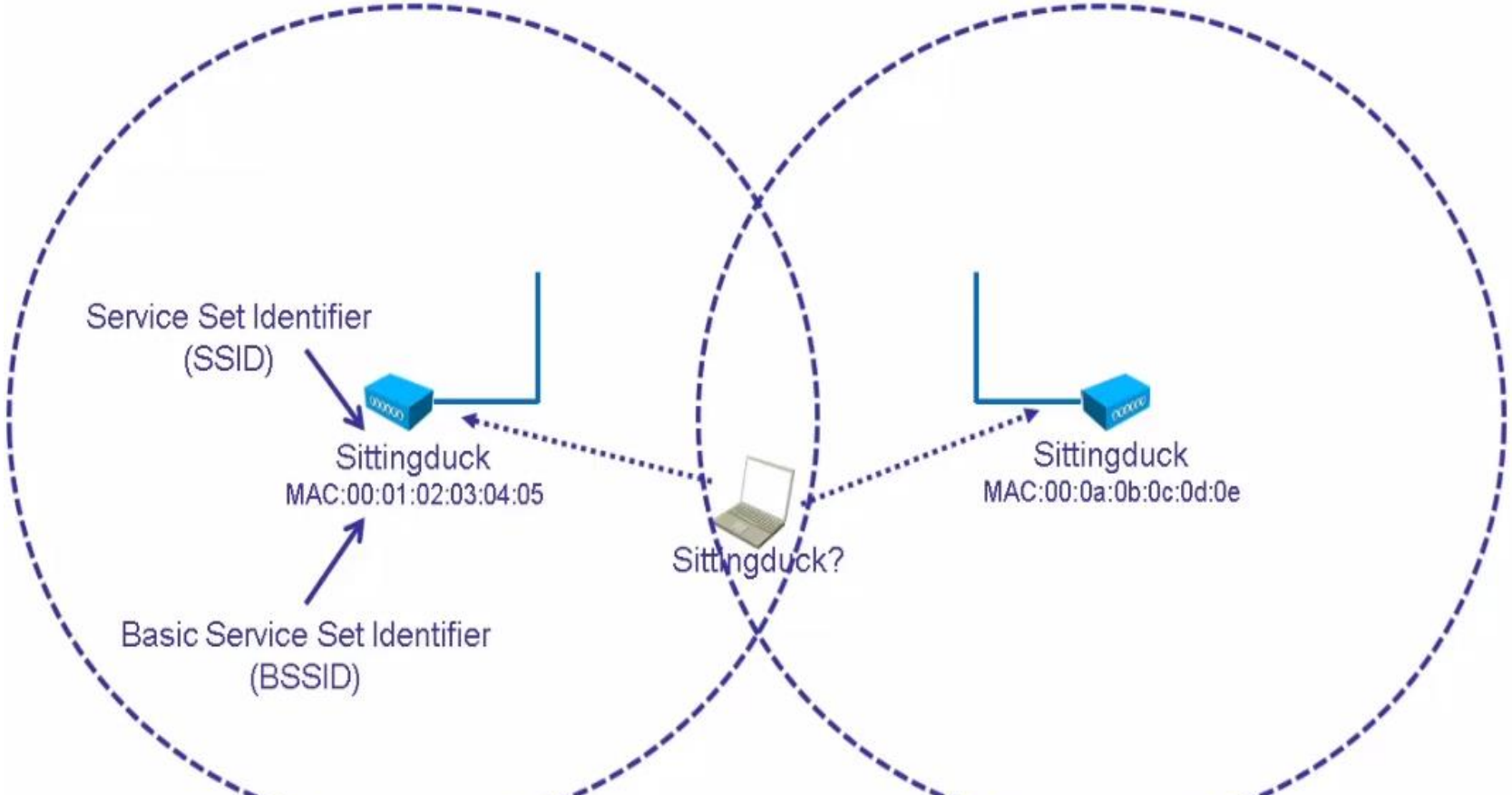
SSID and Roaming cont....

- Whenever device need to connect AP , it tries to connect network name (String)
- If AP is configured to support that connection it will reply
- Name itself is called SSID



SSID and Roaming cont.

- In Enterprise Environment many Aps may be offering same SSID
- Client care about specific SSID not specific AP, client is unaware of AP but end device knows
- BSSID is mac of AP and always unique all over the world

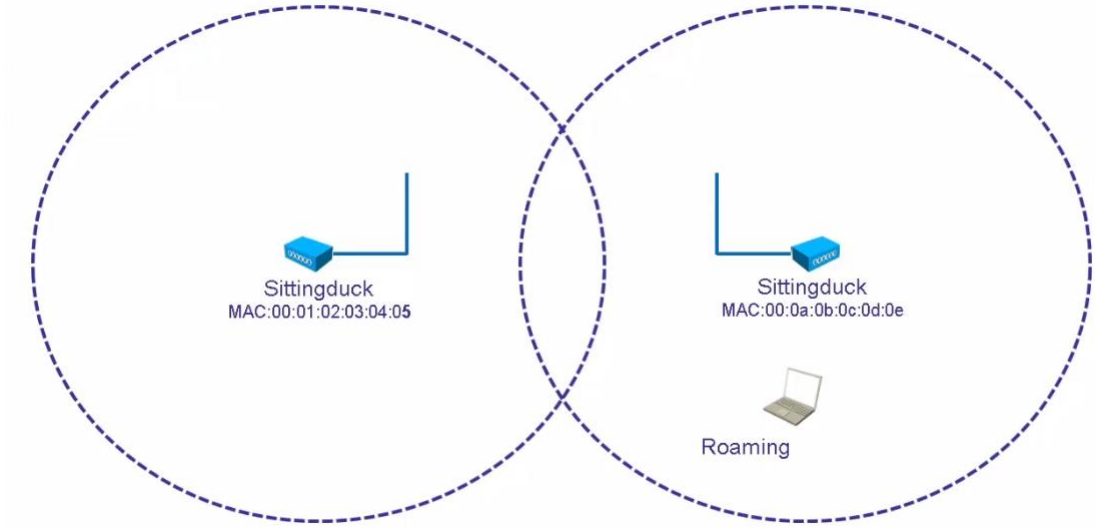


SSID and Roaming cont.

- Same AP serving many SSID
- Each SSID is string, many AP can serve the same SSID
- Each AP has unique mapping from that name to MAC Add (BSSID)
- Here the logic is to allow you to set more that one SSID on given AP, vendor of enterprise class AP provide a range of possible MAC addresses to each AP
- Generally 8 to 16 MAC
- Each SSID has unique mapping to its BSSID
- AP with more that one BSSID is called MBSSID

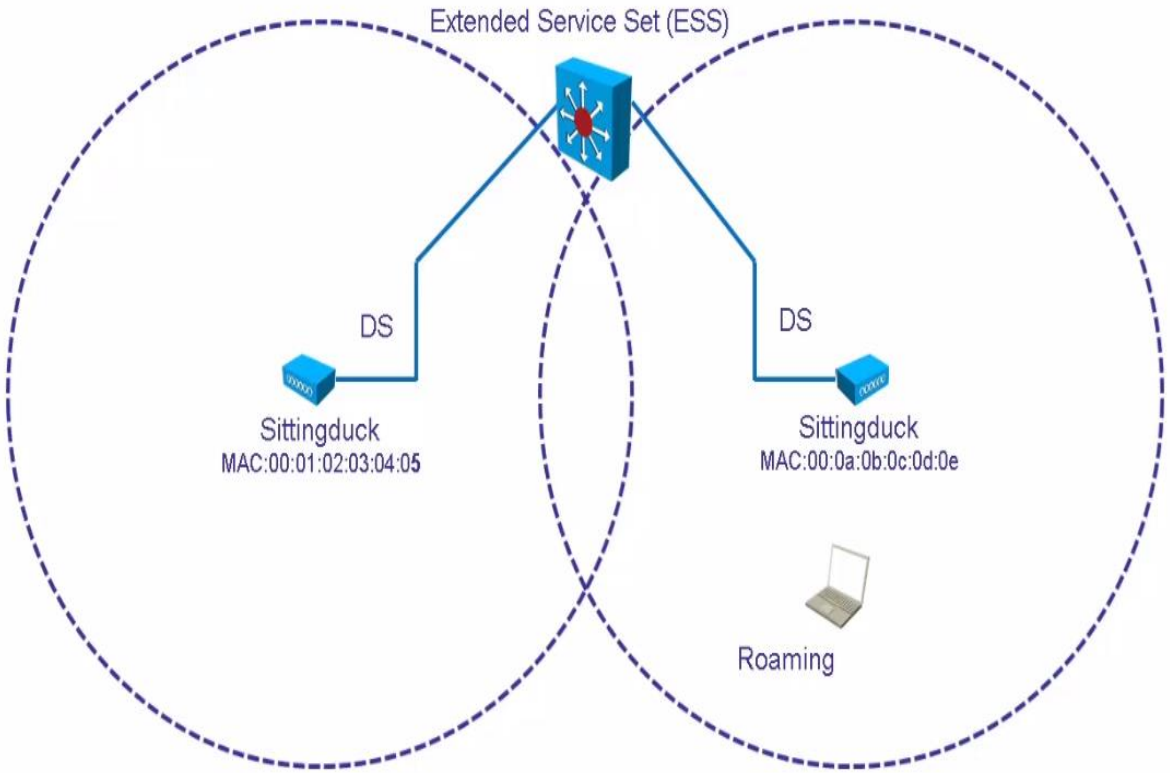
Roaming

- Moving from BSA of left to right AP, job of End device is to jump from on BSSID to other so that you feel your are in same SSID
- Do not loose connection ☺



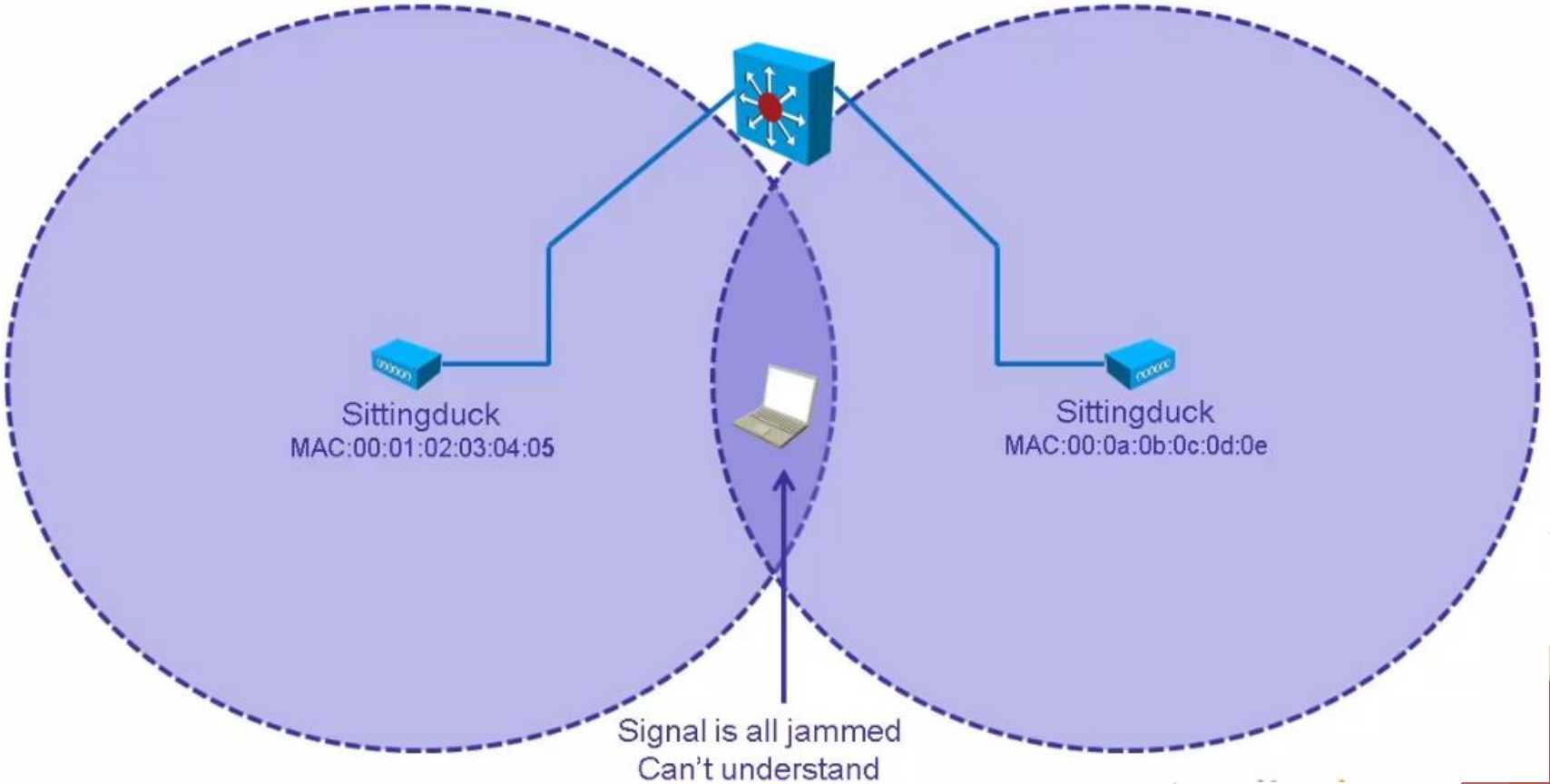
Roaming cont..

- If AP is connected to wired network e.g. to connect to internet, AP has to connect to back plane and connect to internet
- This communication over the wired connection is called Extended Service Set
- AP Basic Service Set is extended beyond the AP itself to get other AP
- ESS is communication of two APs over wired network
- DS → Distribution System
- When two DS communicate i.e. ESS

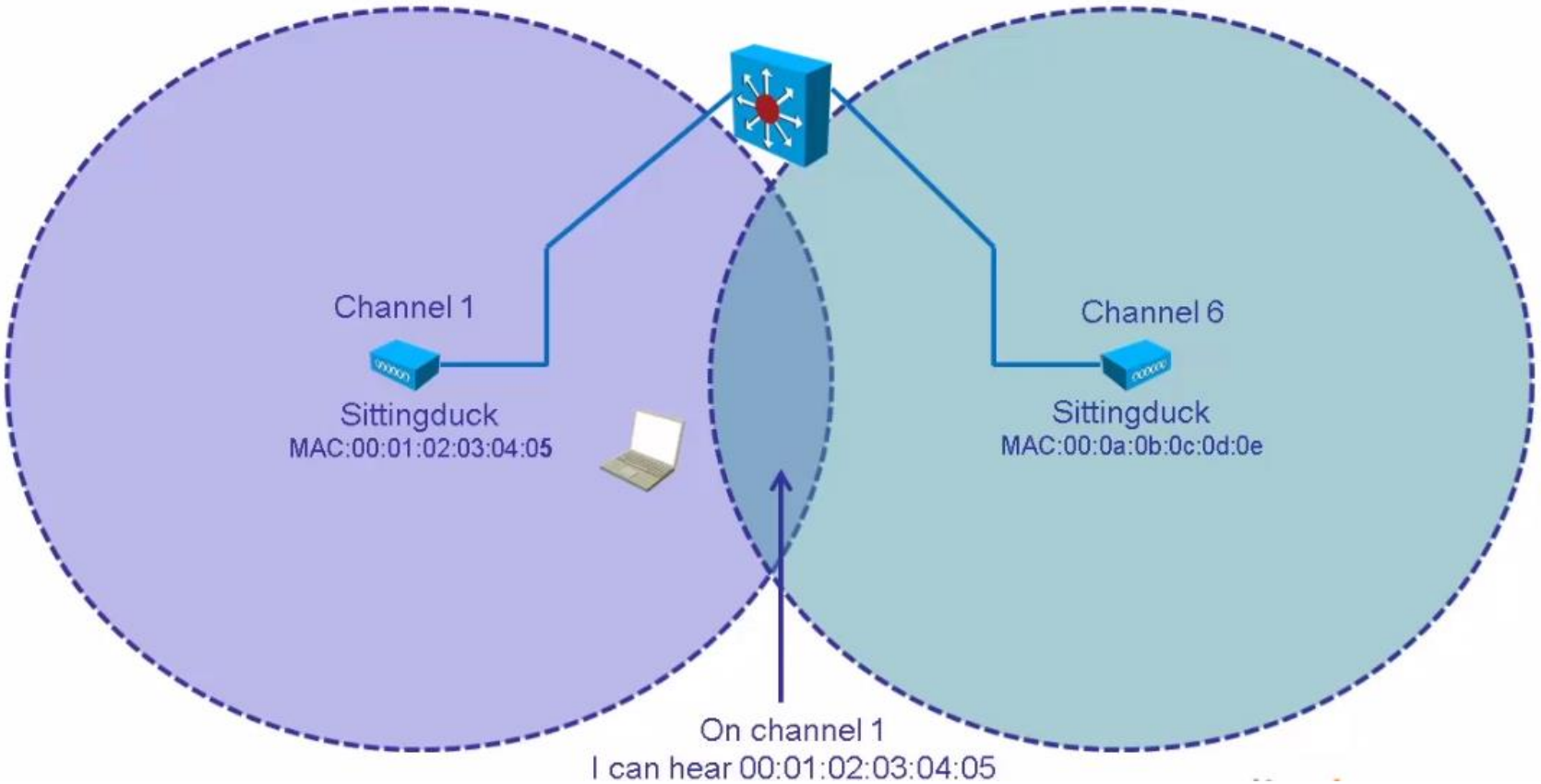


Roaming cont..

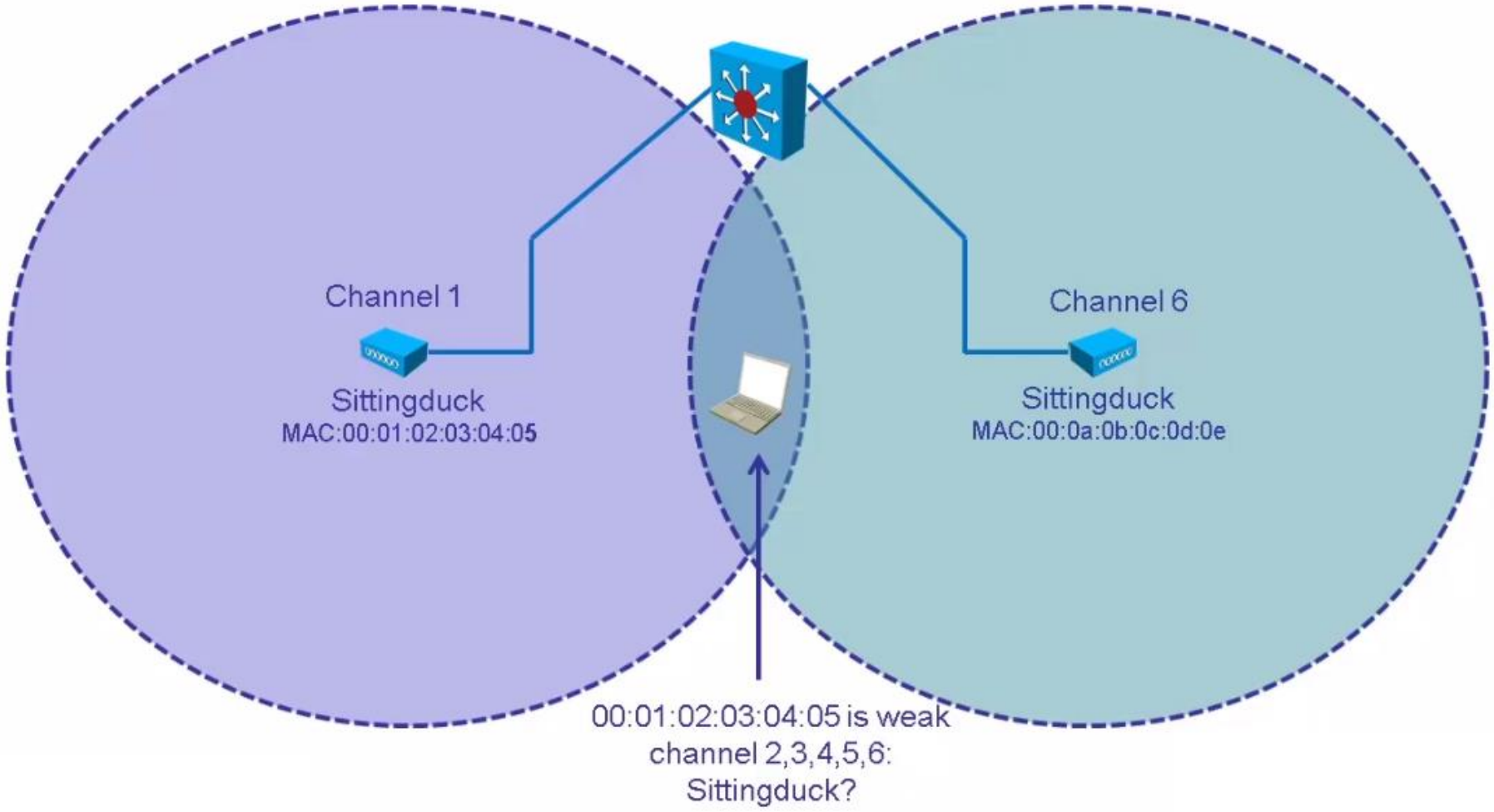
- If two APs are in same frequency, signal going to reach to the client at the same time
- So ? :/
  - Client get heavily confused and you goanna drop some packet



Roaming cont..

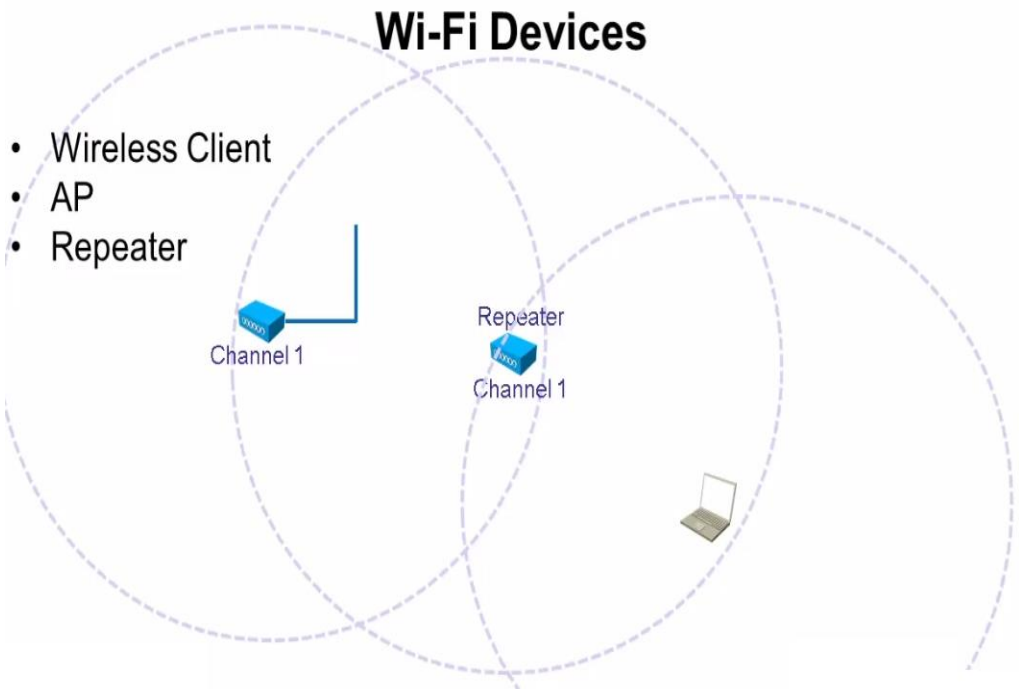


Roaming contd..



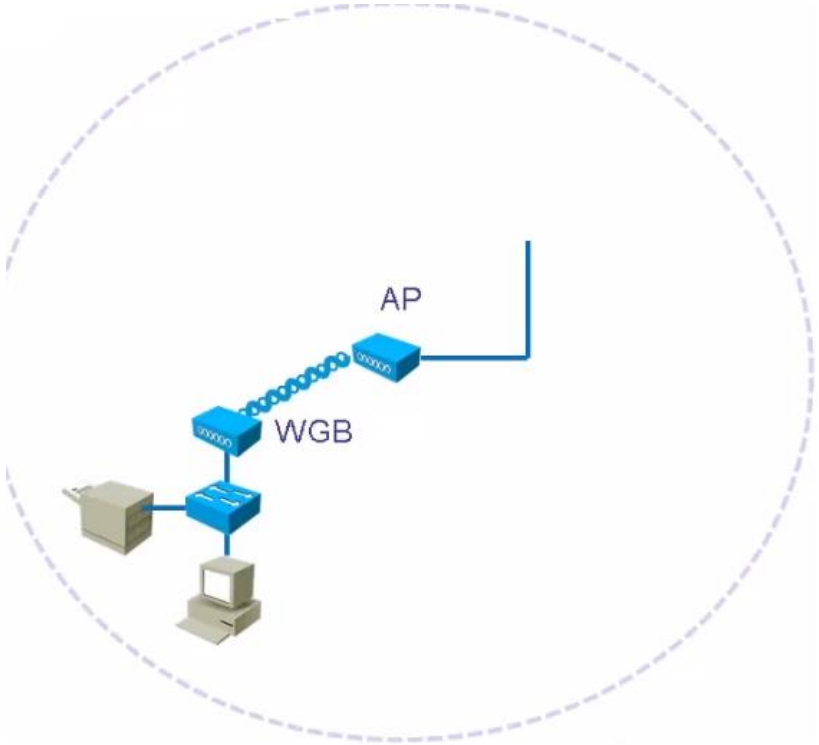
Wi-Fi Devices WGBs, Repeaters, Bridges and Mesh

- Repeater – There is not always possibility to stay near to AP.
  - Insert AP at the middle that doesn't connect to the wired network . It just going to repeat the signal from the AP and the client, that AP is called Repeater
  - Need to be in same channel as the AP
- What is its limitation?
  - Whenever one device sending other can't send at same time so repeater extends coverage but impacts in throughput



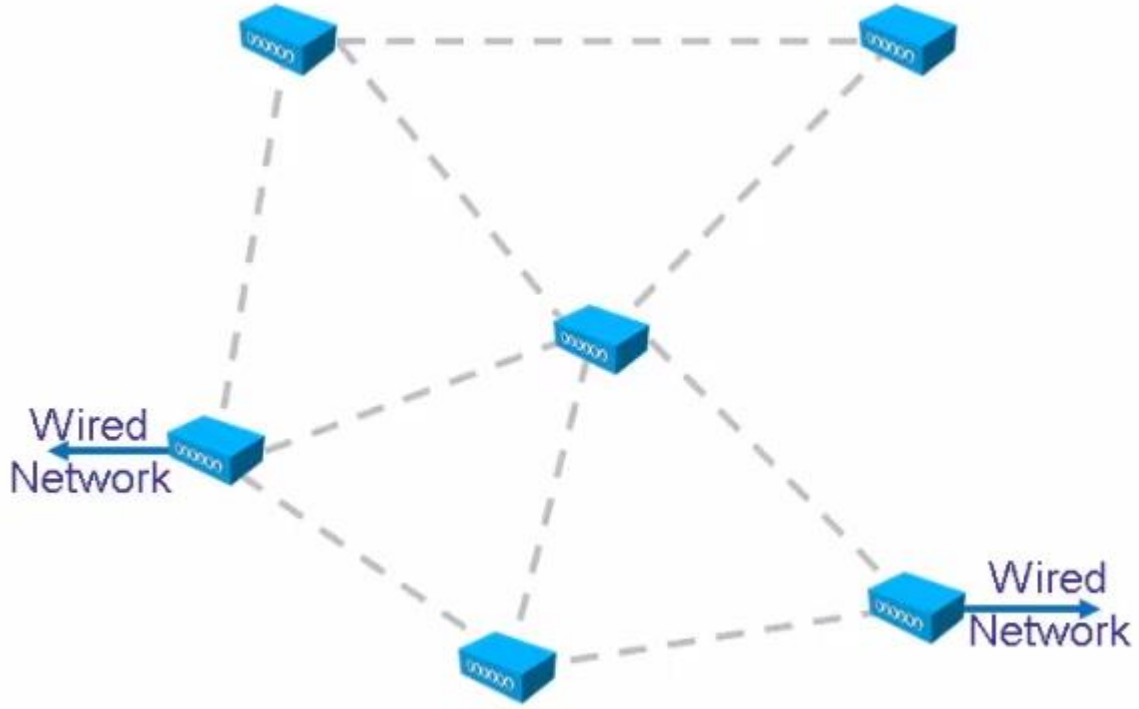
Wi-Fi Devices WGBs, Repeaters, Bridges and Mesh cont….

- What if we have to connect device without wireless card in Wireless Environment?
  - Solution? Yes ☺
    - Configure some AP as client not as an AP That function is called Work Group Bridge
    - WGB connects wired devices to Wireless Network



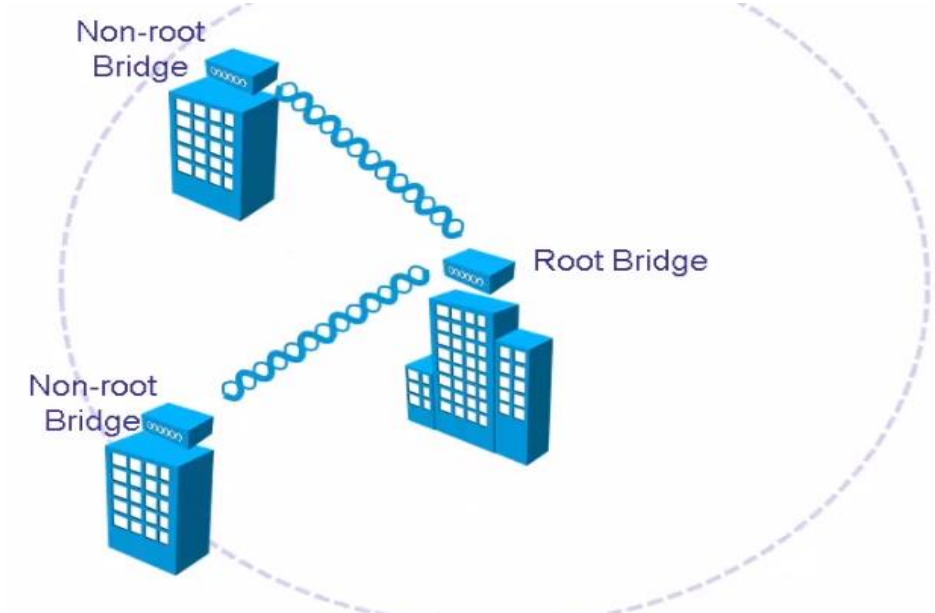
Wi-Fi Devices WGBs, Repeaters, Bridges and Mesh cont….

- Mesh: In some scenarios where there is many bridges p2p or point to multipoint connection is not enough any more
  - Here some devices may have connection to wired network
  - Here APs form complex Mesh, each communicating hopping through other if necessary



Wi-Fi Devices WGBs, Repeaters, Bridges and Mesh cont….

- Bridge mostly found in outdoor network when you need to communicate between buildings or sites
  - Here point to point communication or point to multipoint connection with other Aps
  - AP at center is called Root Bridge and others are Non Root Bridge
  - Non-root Bridge don’t communicate directly they all go through Root Bridge

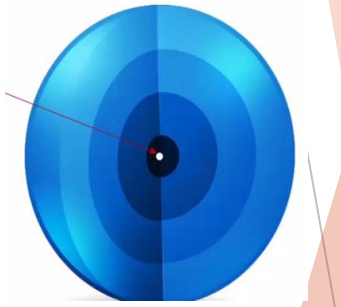


The Roles of the IEEE and the Wi-Fi Alliance

- Have you heard about IEEE 802.11 protocol ?
- IEEE (Institute of Electrical and Electronic Engineers) -> world wide organization that creates protocols
  - In 1980 they define protocol for communication at short or long range, its 11 group is called WIFI
  - IEEE creates protocol, defines what package will be sent, how does that packet look like and how they should be exchanged
- Wi-Fi Alliance creates certification based on part of 802.11 standard.
  - These certification can be very wide
  - This is aimed at making sure that there is compatibility between vendors
  - If the device is Wi-Fi certified then it should communicate with other device that is Wi-Fi certified
  - Some vendor may implement some proprietary features that are not contained in 802.11 standard

Antenna Power

- Antenna sends radio frequency signal not electricity
- They don’t amplify it
- They simply sends it in one specific direction or in many direction
- Antenna's power is compared with referenced antenna called Isotropic Antenna
  - Theoretical antenna, one dot thick radiating power in all directions equally
  - Need to send power to antenna
  - Practical antenna don’t radiate equally in all directions
- Using the right power is critical to achieve the right coverage

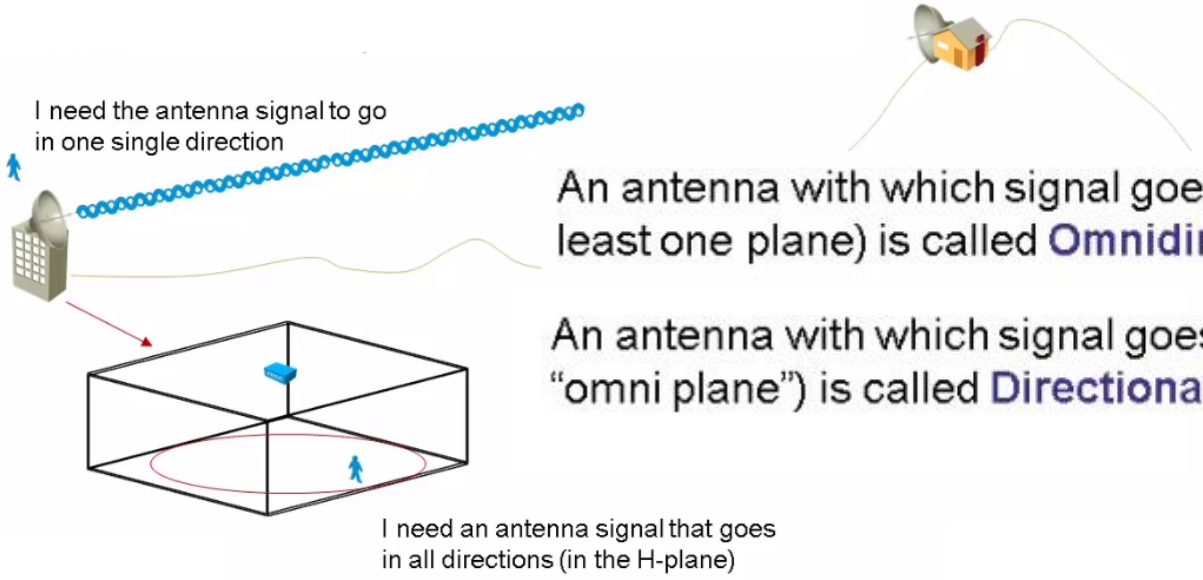


Antenna

- Wi-Fi use Antenna but they are different
- Choosing the right antenna allows you to send the what amount of power, where do you need it to achieve exactly the coverage you want
- You goanna choose same antenna to cover meeting room, ware house or hall etc.
- More energy into antenna means stronger signal at any distance
- More distance means less signal
- Antenna Radiation patterns change with frequency
- Because of the relationship between received power and square of distance
  - Doubling the distance divides received power by 4

Antenna contd..

- Choosing antenna based on coverage you want to achieve
- Different type of antenna because you need different type of coverage at different environment
  - In point to point connection you need signal to go in one direction
  - In meeting room you might room signal goes around all direction



An antenna with which signal goes in all directions (in at least one plane) is called **Omnidirectional Antenna**

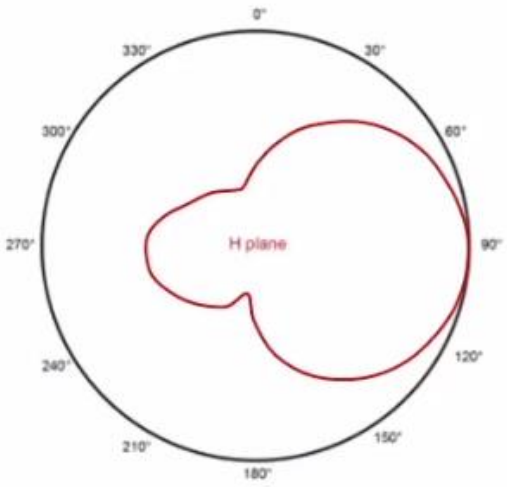
An antenna with which signal goes in one direction (no "omni plane") is called **Directional Antenna**

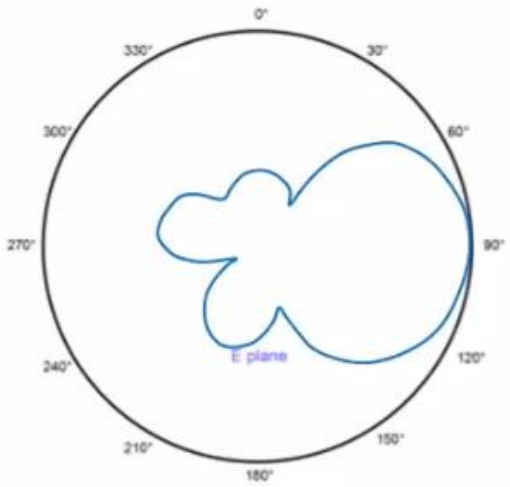
Antenna Types

- Antenna signal propagation is represented with radiation pattern (E-plane, H-plane)
- The radiation pattern shows the direction of maximal radiation, and the comparative loss as you move around antenna

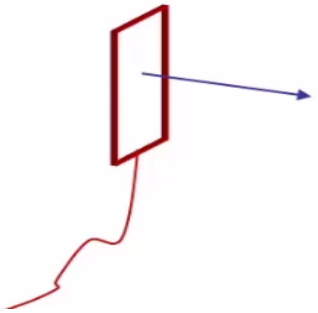
Directional Antennas

- Patch antenna





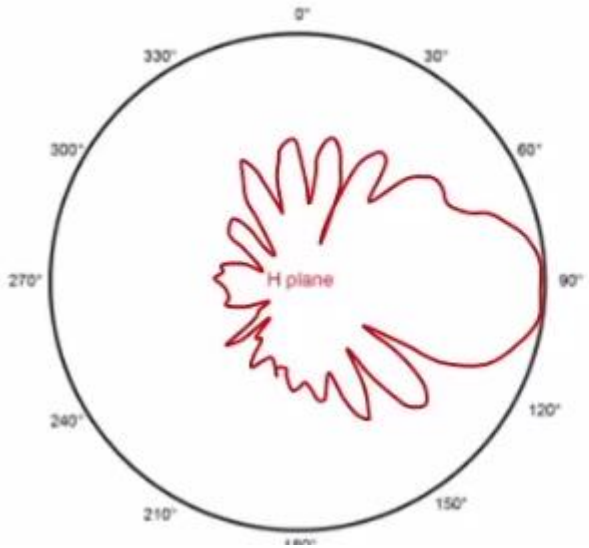
8.5 dBi patch, wall mount

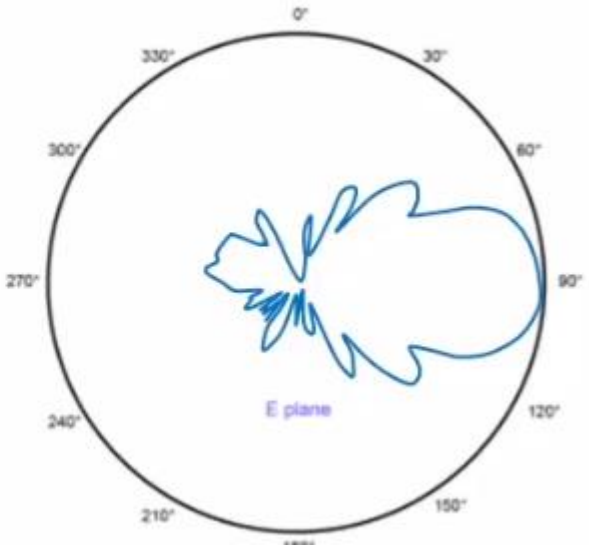


Antenna Type …

- Directional Antenna
  - Yagi Antenna

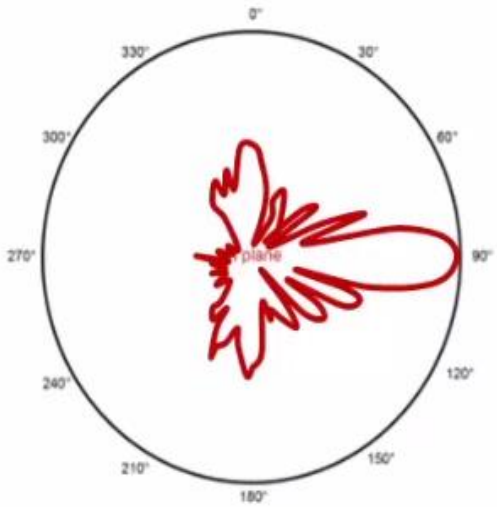
13.5 dBi Yagi

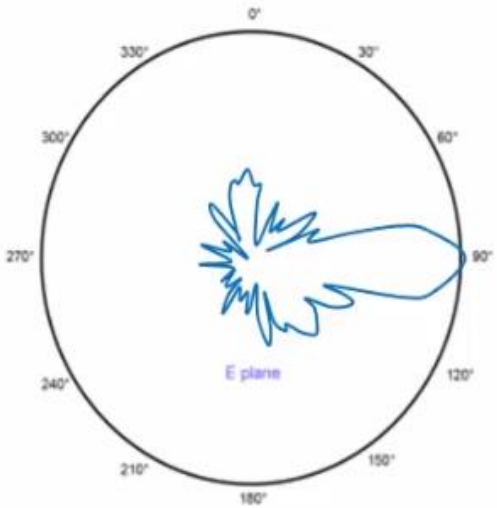


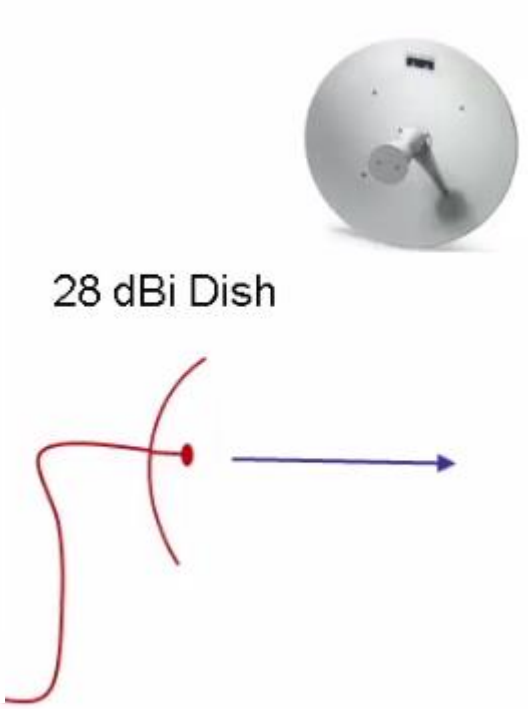


Antenna Type…

- Dish Antenna





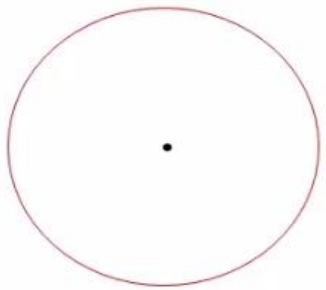


Long range point-to-point

Omnidirectional Antenna

- Omnis are found in access points that are placed in the center of the coverage area
- Omnis are also found in most client devices
  - You don’t know where the signal should go

“rubber duck”
Elevation Plane
(E-plane)



“rubber duck”
Horizontal Plane
(H-plane)

Antenna is often on screen side

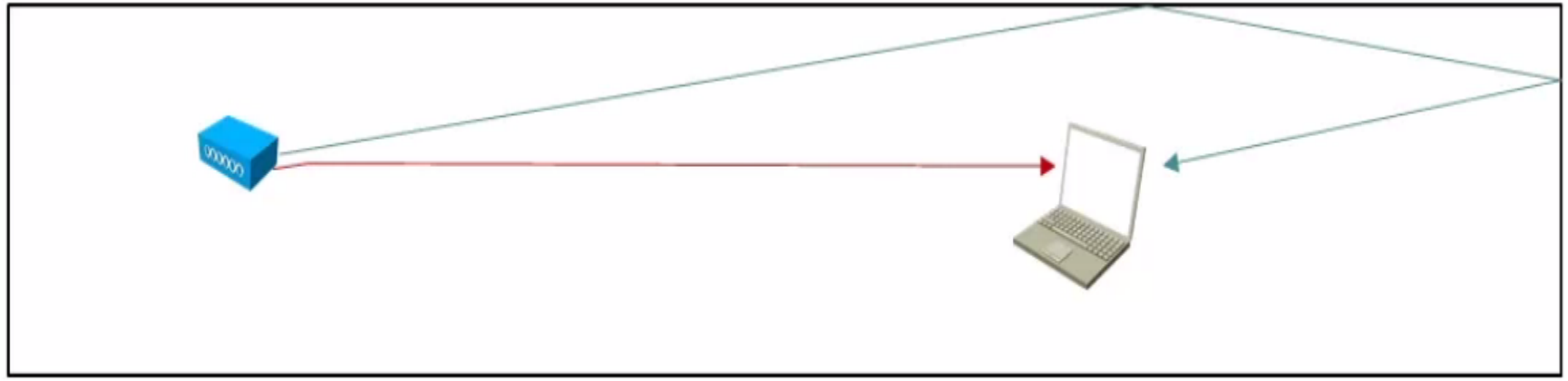
Polarization

- Antenna signal is not the same in E-plane and H-plane
- This is because the antenna single is not polarized – the signal sent has an orientation
- Electric field and Magnetic field are 90 degree in each

Electrical signal is vertical and magnetic is vertical, so antenna need to be put in vertical,
So orientation need to be match in P2P wireless link

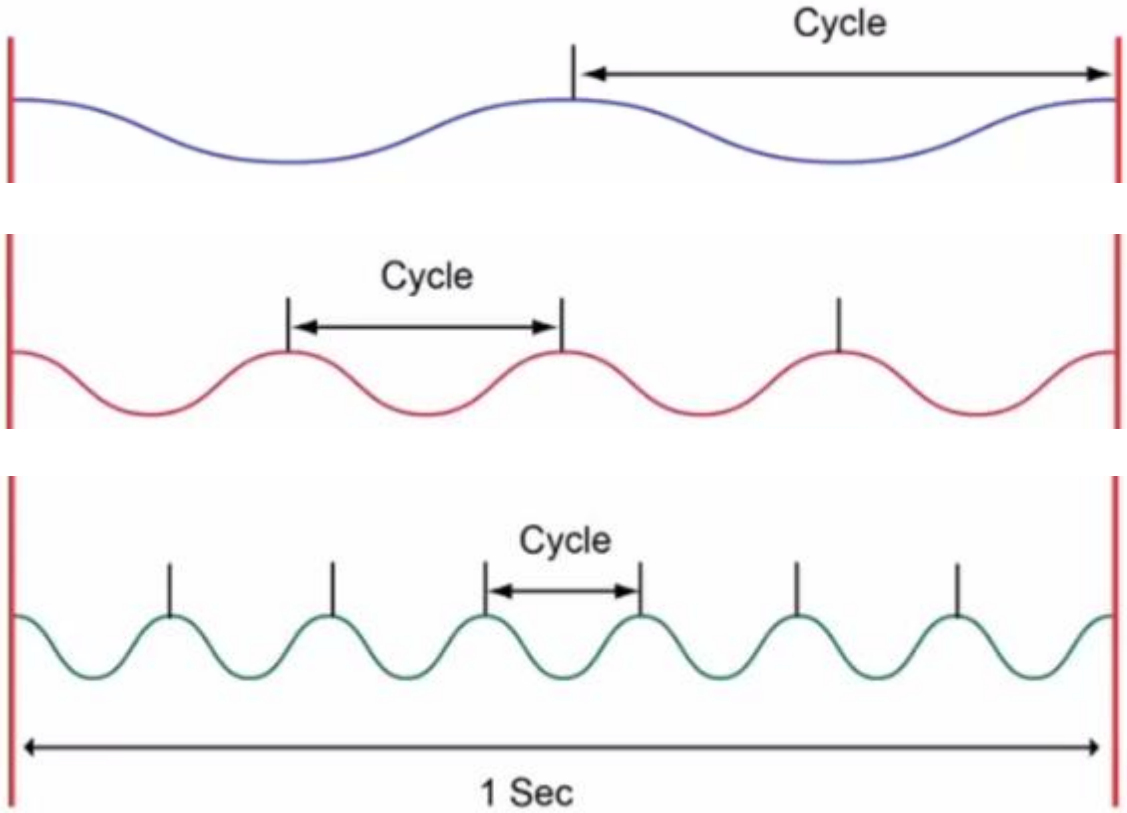
Polarization…

- Polarization is important… especially outdoor! Respecting polarization logic indoor is always a good idea
- Because signal bounces in indoor and reach destination, there is always a way
- Antenna should be vertical either up or down



Frequency

- RF waves are signal that go “up and down” in cycles
- Frequency shows how often a cycle happens: 1 time per second = 1 Hertz



2 cycles per second = 2 Hertz

4 cycles per second = 4 Hertz

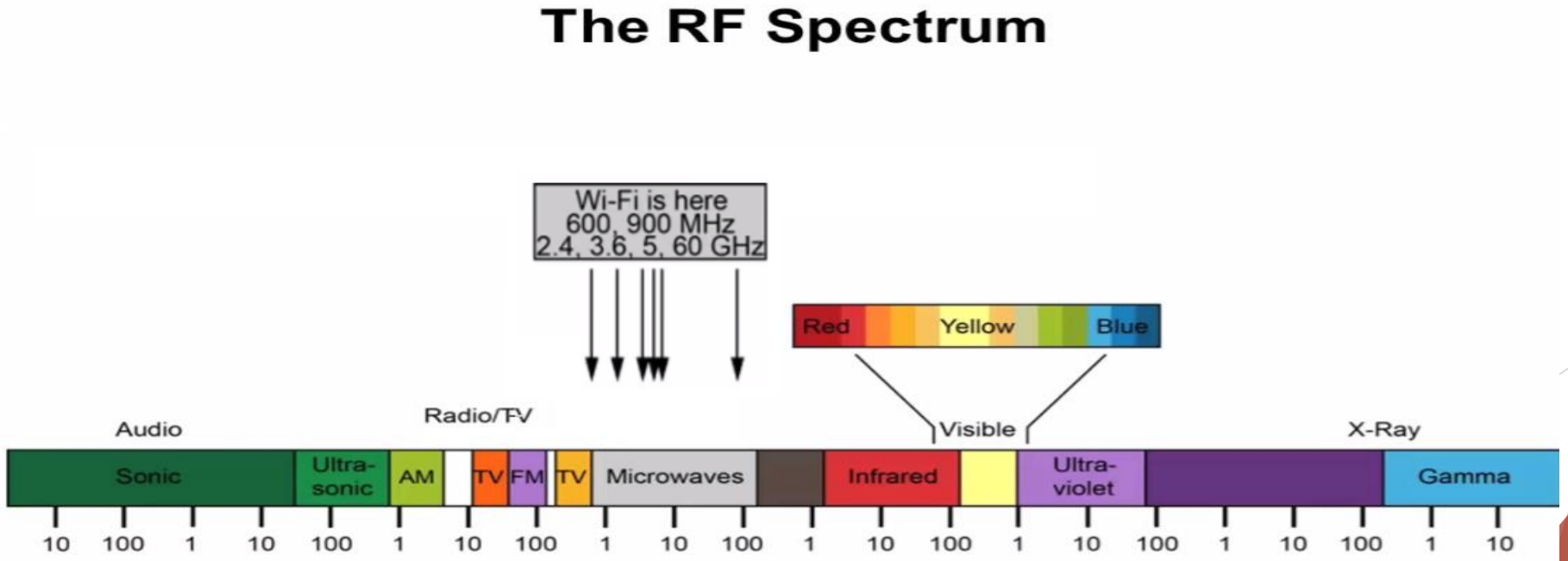
7 cycles per second = 7 Hertz

1 million cycles per second = 1 MHz

1 billion cycles per second = 1 GHz

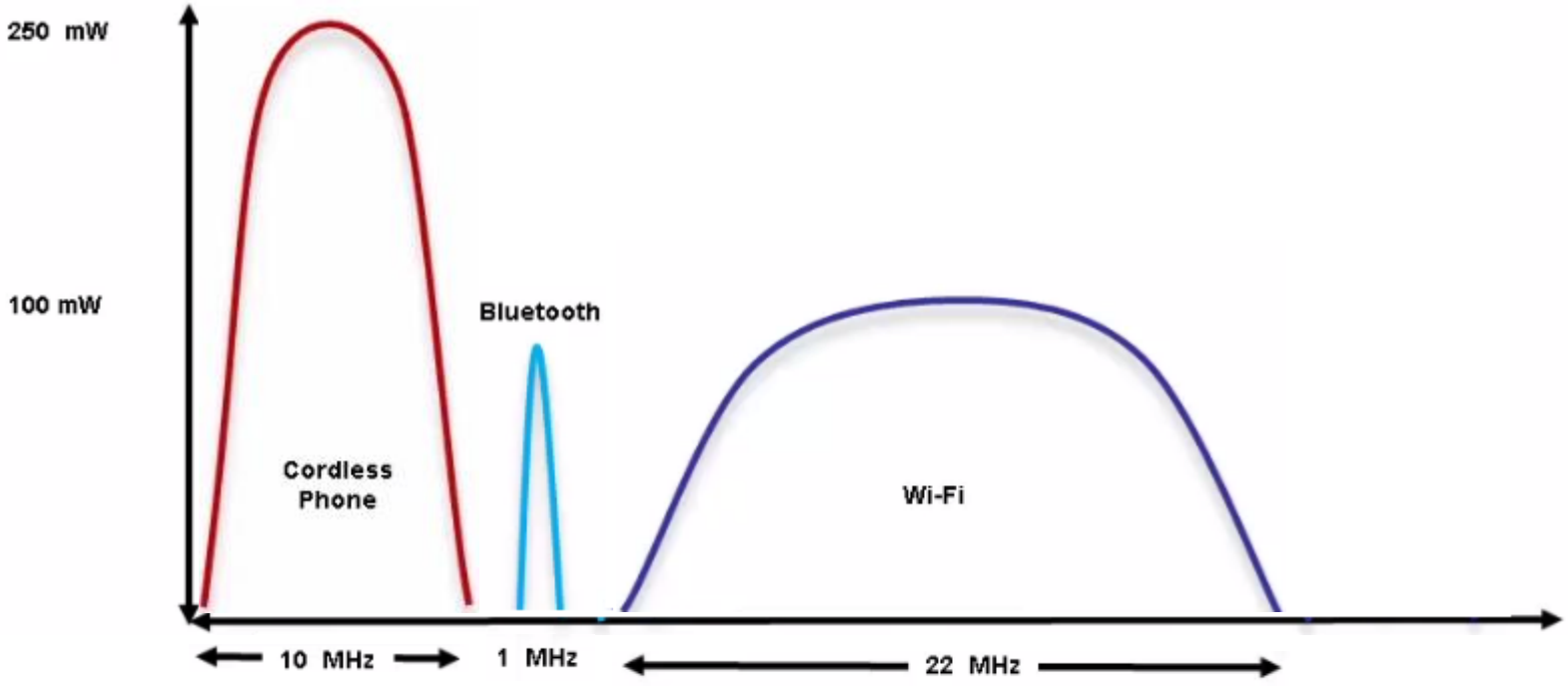
RF Spectrum

- Where Wi-Fi fits in the Spectrum?
- Spectrum is range of all possible frequencies and wavelengths of universe
- Longer wavelength are less prompt to obstacles but carry less energy so less information
- Wi-Fi started in the 2.4 GHz band, then 5 GHz
- Lower frequency has longer range



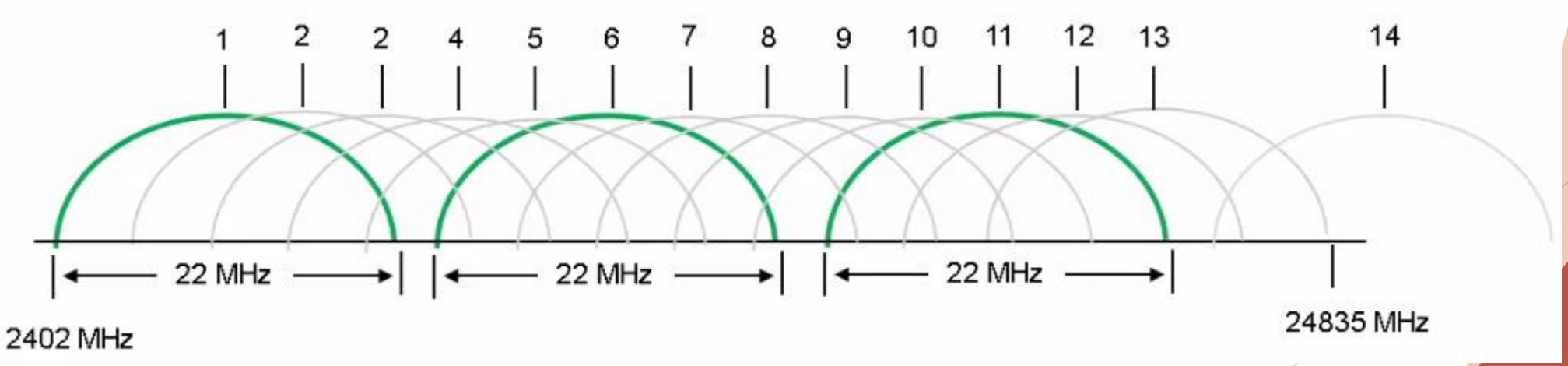
The 2.4 GHz Interferer Family

- “2.4 GHz” spans from 2.400 GHz to 2.4835 GHz
- Wi-Fi uses 22 MHz-wide channels, with power up to 100 mw
- Cordless Phone signal is stronger is more stronger so more destructive if it sits near our AP



Channels and overlaps

- 2.4 GHz has 11 to 14 “channels” but they are too close to one another to be used individually by Wi-Fi.
- You can’t use two consecutives channels without overlap
- Wi-Fi channels are 22 MHz wide
- So to exist several Wi-Fi system to co-exist we have to keep them in quite far apart channels (as per IEEE 25 MHz apart)

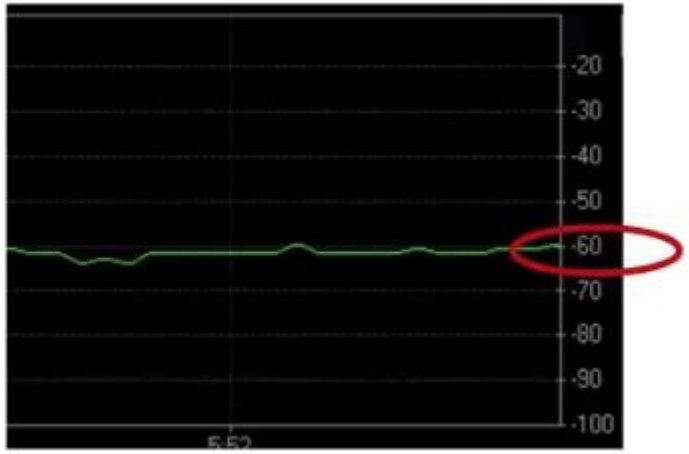


Need for speed

- IEEE 802.11 defines the 802.11 standard
- The standard tells how frames are send and at what speed they are send using what modulation and coding
  - Each enhancement to the standard receives a letter (e.g. 802.11a)
    - This could be for any enhancement not only for speed but also for security, QOS etc.
- 802.11/Wi-Fi has long been trying to catch up the Ethernet speeds
  - 802.3, 100 Mbps Ethernet (Copper), 1995
- 802.11, up to 2 Mbps (1997)
- 802.11b, up to 11 Mbps (1999)
- 802.11a, up to 54 Mbps (1999) in 5 GHz band
  - 802.3ab, 1Gbps Ethernet (Copper), 1999
- 802.11g, up to 54 Mbps (2003) in 2.4 GHz band
  - 802.3an, 10Gbps Ethernet (Copper) ,2006
- 802.11n, up to 600 Mbps (2009)
- 802.11ac, up to 7 Gbps, 2014
  - Complexity for vendor to adapt this standard, can found up to 450 Mbps card only due to engineering complexity to bring the standard into product

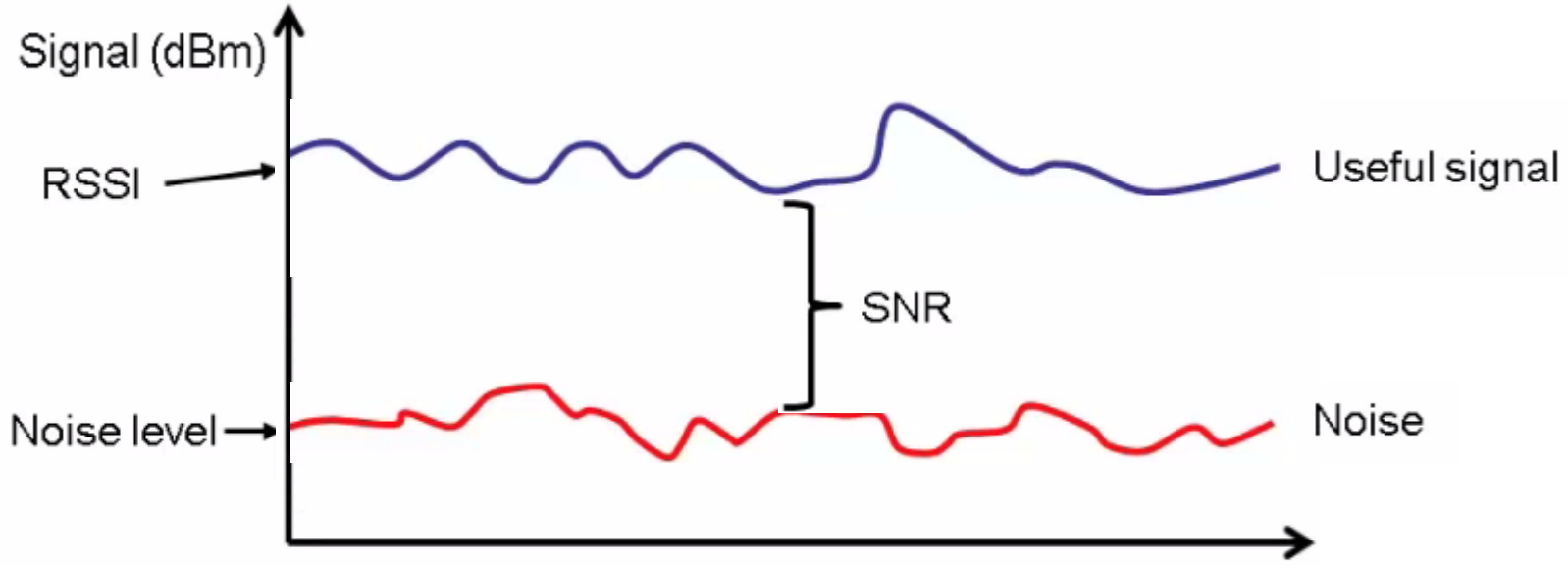
RSSI and SNR

- Received Signal Strength Indicator (RSSI) shows how much signal was received
- Usually a negative number (e.g.-76 dBm)
- Is Vendor dependent
  - 2 vendors cards at same spot may read different RSSI
  - RSSI shows ability to convert RF wave into 0s and 1s



RSSI and SNR

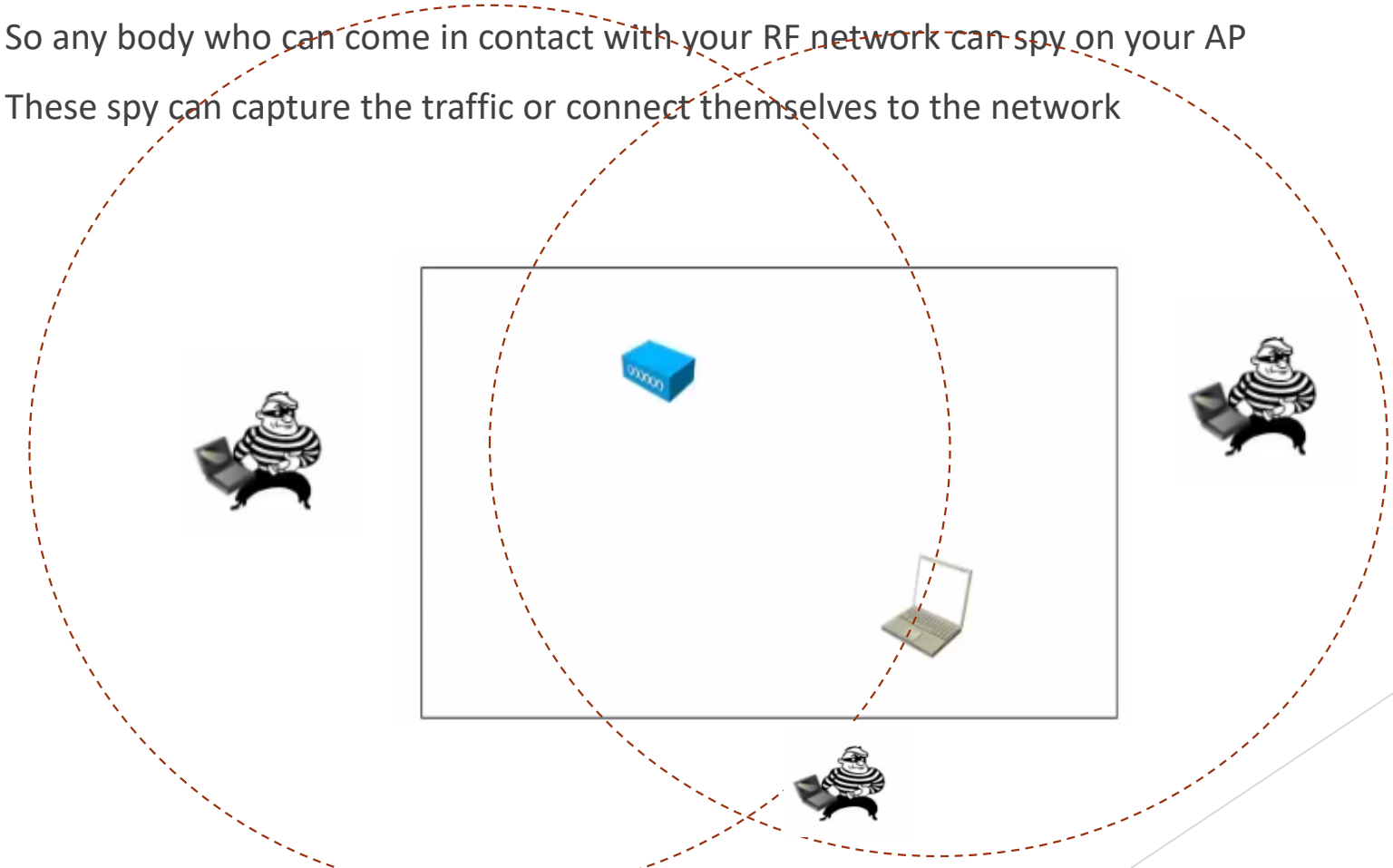
- There is RF everywhere (coming from earth heat, space, human activity,..)
- The amount of “unwanted RF” is called (background) noise
- RSS – noise level = Signal to Noise Ratio (SNR)



e.g. RSSI = -76 dBm
Noise floor: - 97 dBm
SNR = -76 - -97 = +31 dB

Securing Communication

- 802.11 is not just about speed, but also security
- Why can be easily reachable from outside even you are inside the building, because RF waves is not blocked by the wall
  - So any body who can come in contact with your RF network can spy on your AP
  - These spy can capture the traffic or connect themselves to the network



Securing Communication

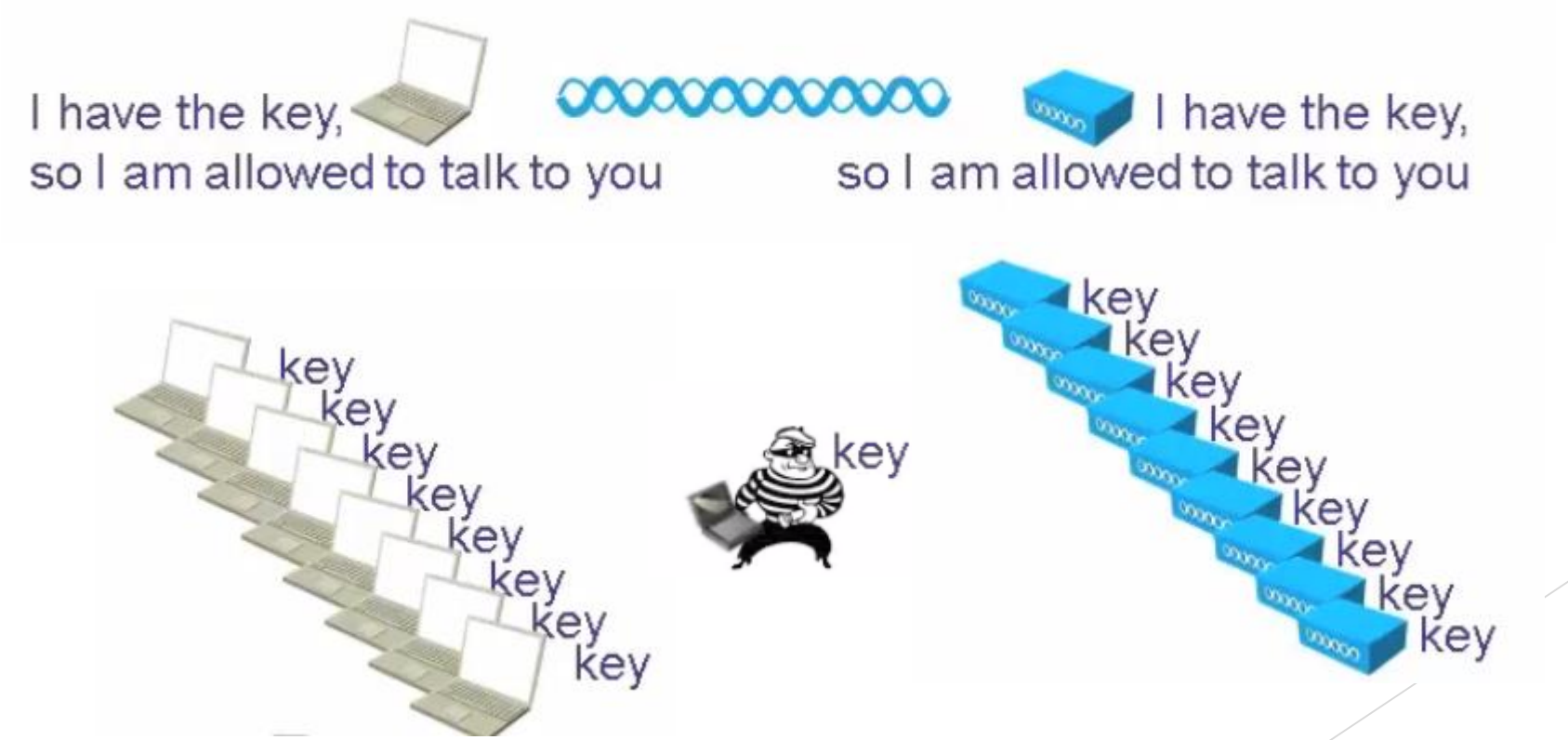
- Relies on 4 elements
  - Authentication – allow only valid users
  - Encryption – making data unreadable by spy
    - Key Distribution
    - Key Management (renewing keys, passing keys as you roam)

Authentication

- Prove you identity (and your right to connect)
  - Using password
  - Can be done on client and/or infrastructure side
  - 2 main techniques: shared key, individual authentication
    - Also: MAC authentication (not much use any more)
      - For 1000 of device it is hard and can MAC can be spoofed too

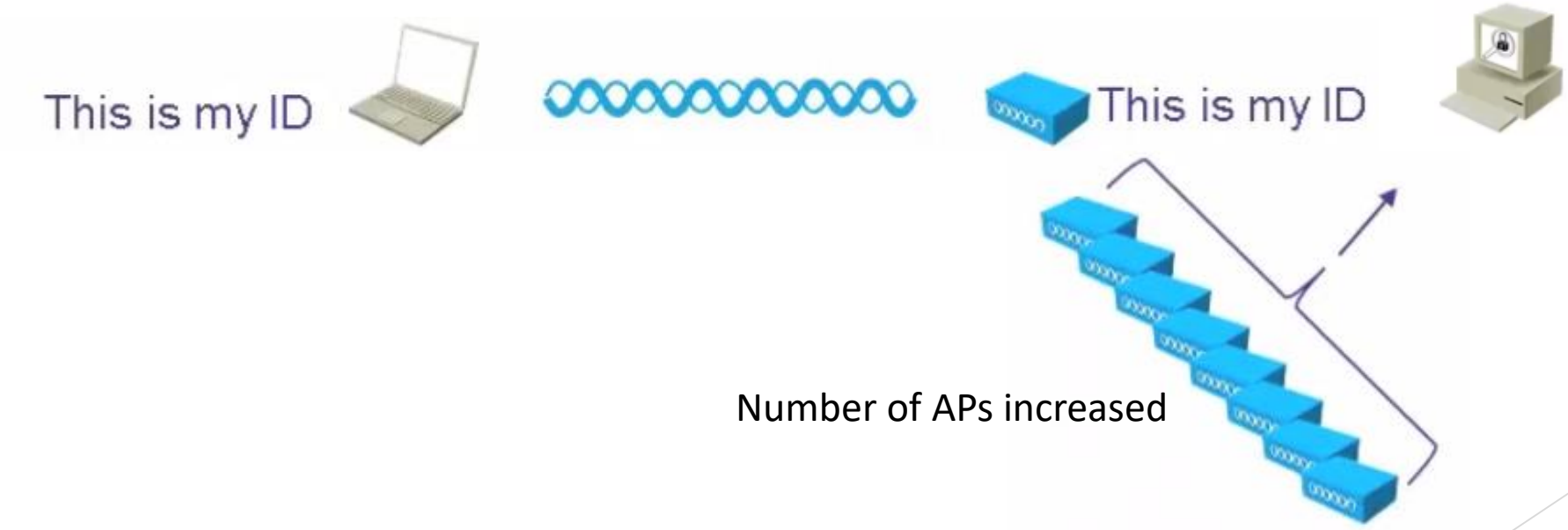
Authentication

- Shared Key
  - Same value is configured either side
    - Each AP and Each clients need to be configured password
    - So Good for only small environment like home



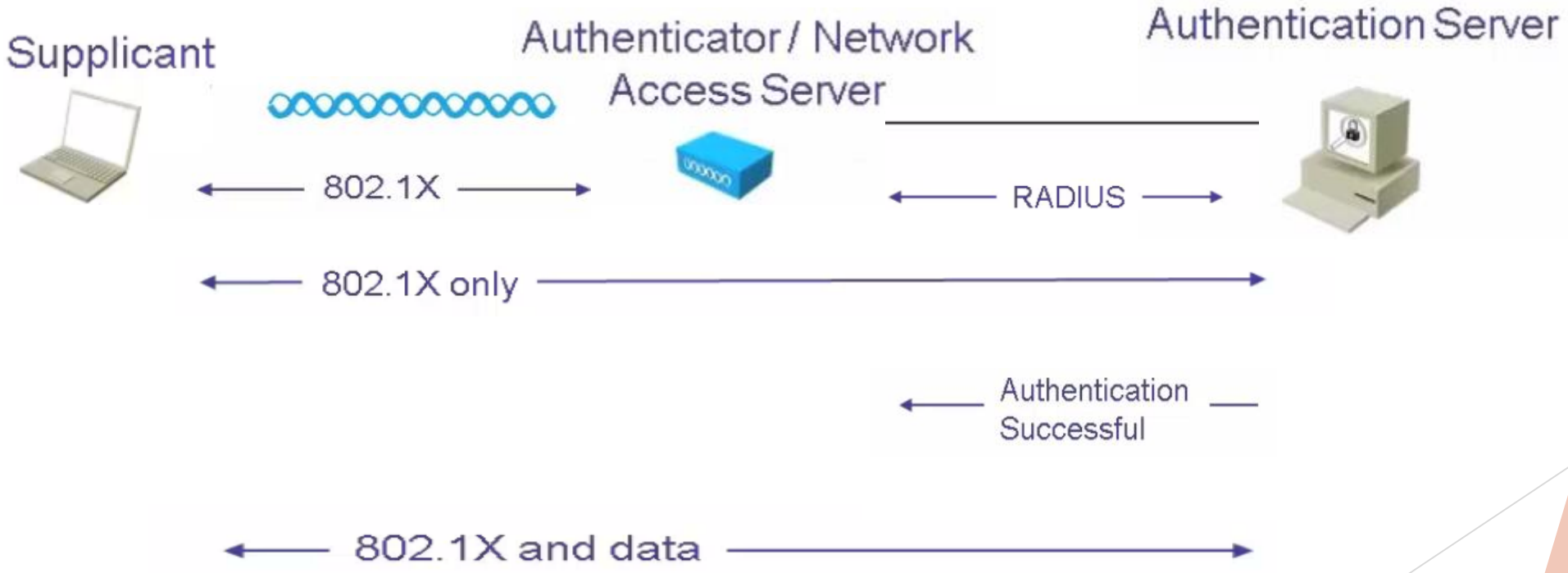
Individual authentication

- Each different individual users has different ID
- Highly Secure but what about Scalability ?
  - There is central server on which you configure all the identifiers, act as repository
    - Relates the query to identify the client to the server



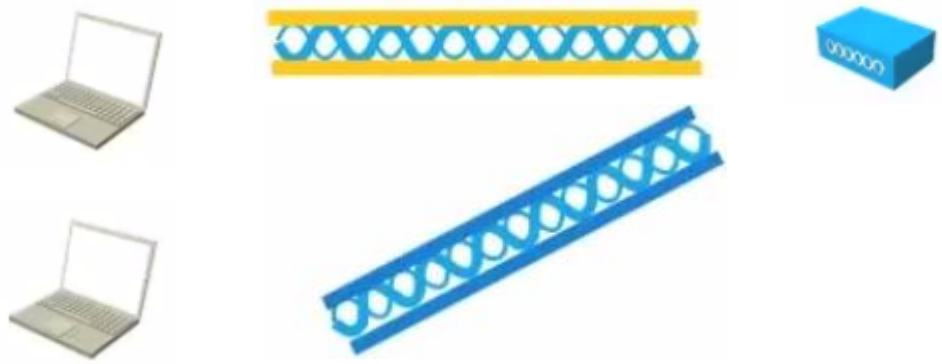
802.11i – EAP/802.1x

- 802.11i uses 2 other protocols to secure installation
  - 802.1x defines that you block a port until user/device is authenticated



Encryption

- Protect Communication from eves dropping
  - Unicast and Broadcast communication
- Unique key between each client and AP
- Common key between clients and AP to broadcast



Encryption

- How to create keys?
  - WEP, TKIP, AES-CCMP
- WEP can also use encryption as a form of authentication:
  - Start by exchanging challenge (test encryption)
  - This is very unsecure
    - Key was directly used for encryption

If we can encrypt and decrypt traffic, then this proves that we both have the shared-key

WEP (Wired Equivalent Privacy)

- WEP uses the RC4 algorithm
  - Its source code is available in internet
  - Many free applications are available that break RC4 encryption
  - RC4 is combination of static and dynamic element
    - Static=shared secret key , 40 bit or 104 bit alphanumeric value
    - Dynamic=Initialization Vector (IV), 24 bit alphanumeric value
    - IV is added to Shared Secret key
    - Static keys
    - Weak IV – clear text

WPA and WPA2

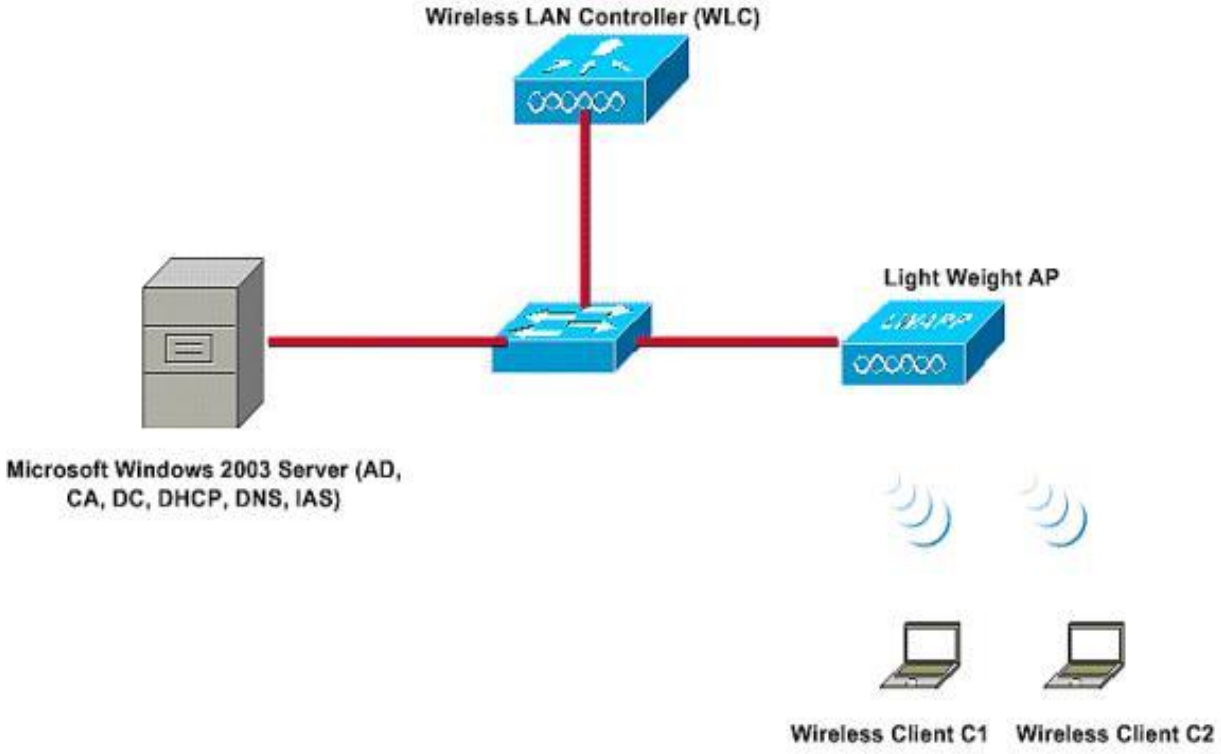
Methods	Encryption	Authentication
WPA-Personal	TKIP	PSK
WPA2-Personal	DES-CCMP	PSK
WPA-Enterprise	TKIP	802.1x/EAP
WPA2-Enterprise	DES-CCMP	802.1x/EAP

Some security issues

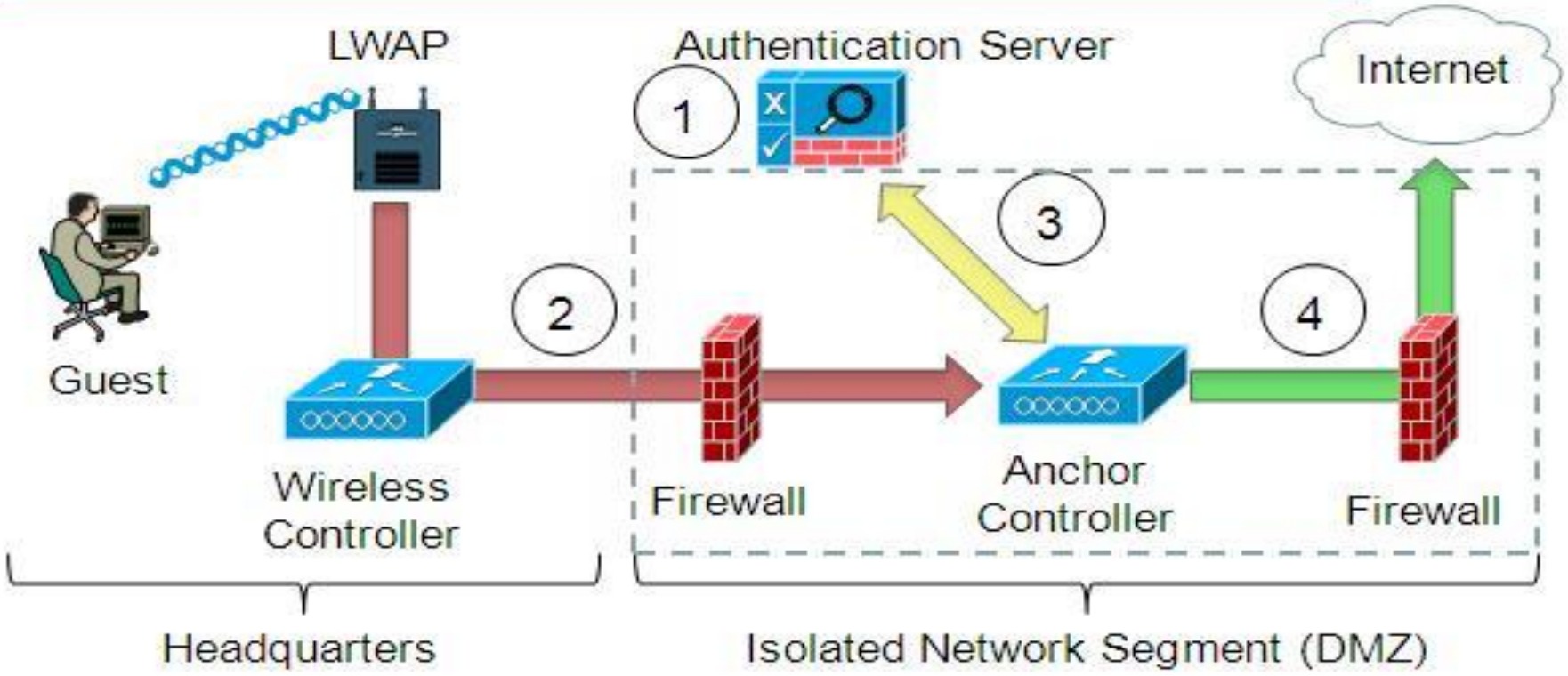
- If an employee (trusted entity) brings in a wireless router and plugs it into an unsecured switchport, the entire network can be exposed to anyone within range of the signals
- Ad-hoc networks can pose a security threat. Ad hoc networks are defined as [peer to peer] networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security

Wireless LAN Controller

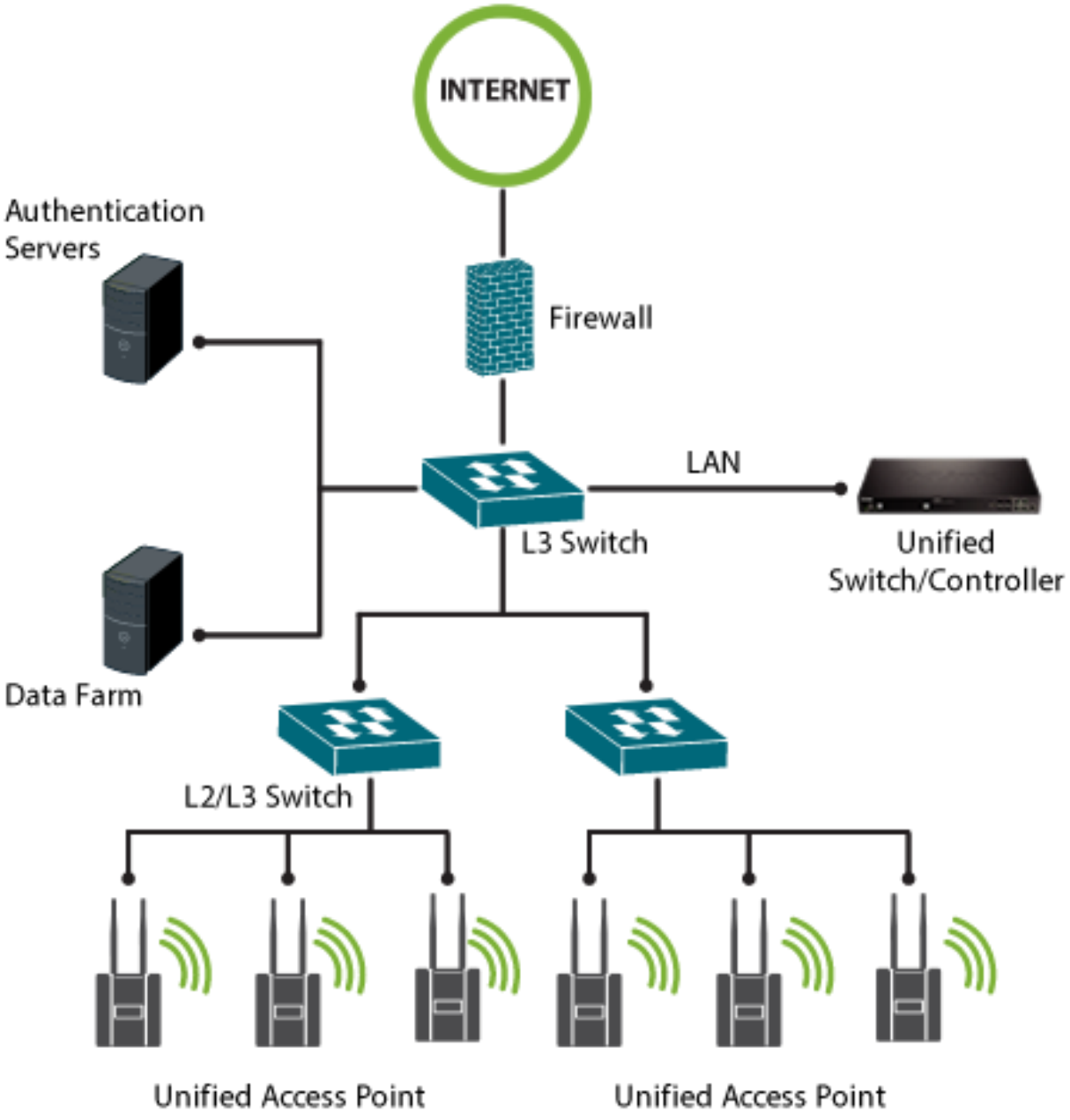
- A **wireless LAN (WLAN) controller** is used in combination with the Lightweight Access Point Protocol (LWAPP) to manage light-weight access points in large quantities by the network administrator or network operations center
- The wireless LAN controller is part of the Data Plane within the Cisco Wireless Model. The WLAN controller automatically handles the configuration of wireless access-points



How It Works



1. Guest account created/authorized for network access
2. Guest connects personal device to network, sent to an isolated network segment (DMZ)
3. Guest logs into network and credentials are verified
4. Guests are allowed Internet-only access


INTERNET
Authentication Servers
Firewall
LAN
L3 Switch
Unified Switch/Controller
Data Farm
L2/L3 Switch
Unified Access Point
Unified Access Point