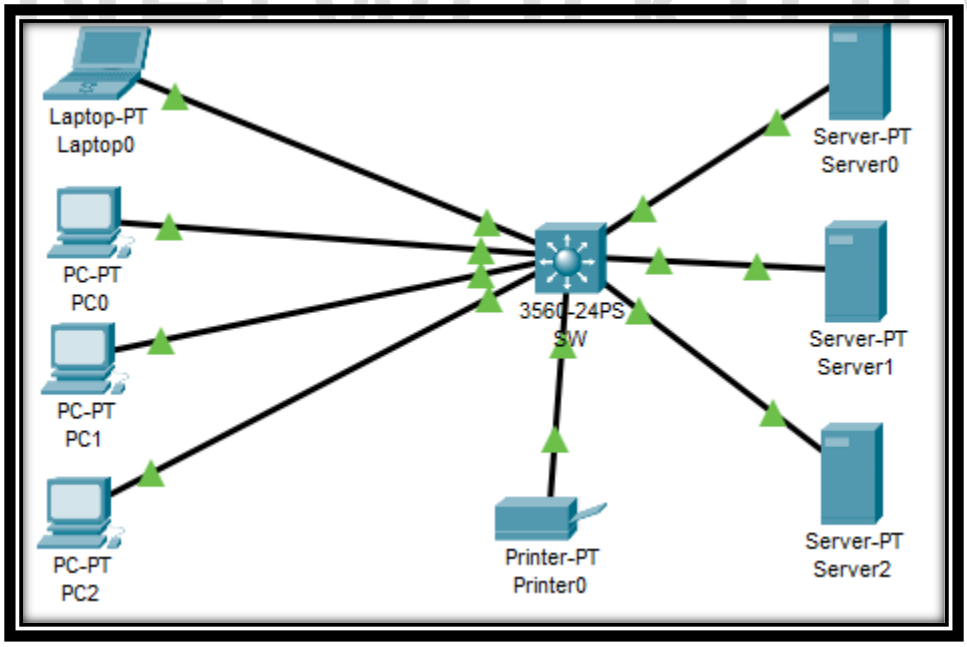

Networkforyou
Welcome
To
Network for you
Wireless
Networkforyou

Communication: Transferring of data from one point to another point is known as communication.

- If device is using wired to connect other device then it is known as wired communication.
- If device is not using wired to connect other devices then it is known as wireless Communication.
- A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network.
- The most common wired networks use cables connected at one end to an Ethernet port on the network router and at the other end to a computer or other device.

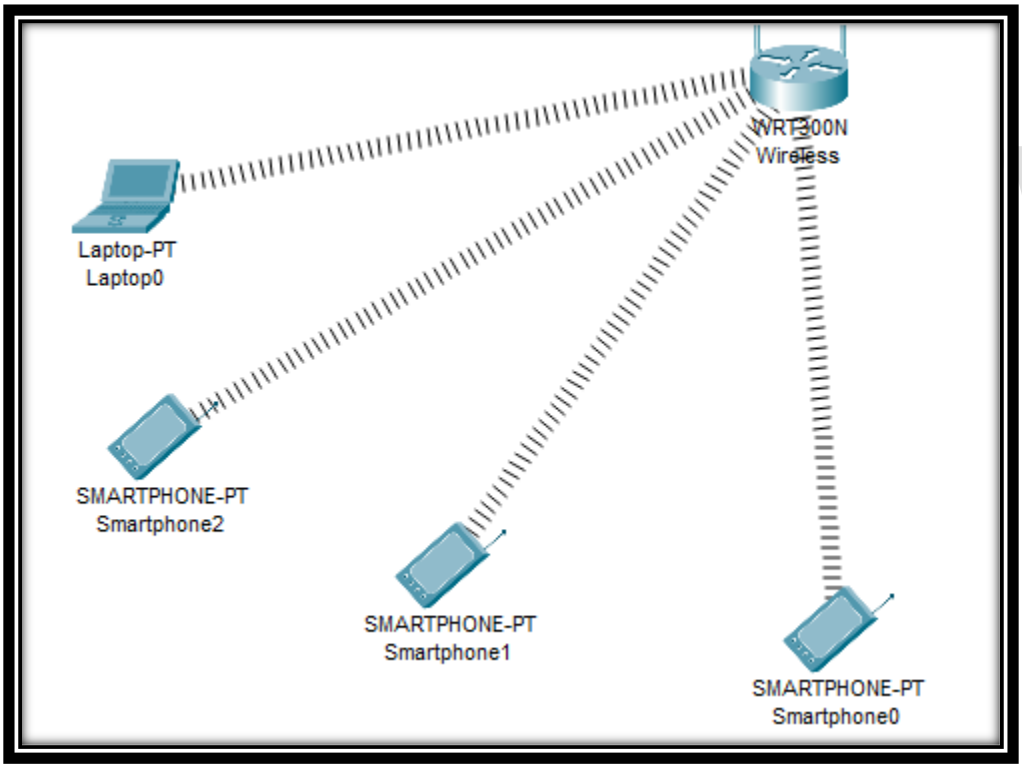
Wired network:

- In computing terminology, the term "wired" is used to differentiate between wireless connections and those that involve cables.
- A wired setup uses physical cables to transfer data between different devices and computer systems.
- The cables can be copper wire, twisted pair or fiber optic.
- Wired network is used to carry different forms of electrical signals from one end to the other.
- Most wired networks use Ethernet cables to transfer data between connected PCs.
- Ethernet works or operates in a narrow range and it is little bit difficult to configure as compared to wireless networking technologies.



Wireless Network:

- Wi-Fi stands for Wireless Fidelity.
- WIFI services are defined in the IEEE 802.11 standard.
- IEEE stands for Institute of Electrical and Electronics Engineers.
- Wireless network refers to the use of infrared or radio frequency signals to share information and resources between devices.
- Wireless technologies are designed to reduce the time and different type of obstacles created by the cables.
- Wireless network does not use wires for data or voice communication; it uses radio frequency waves.
- Many types of wireless devices are available today; for example, cellular mobile, handheld PCs, satellite receivers, laptop, wireless sensors etc.
- Easy to setup.
- Fewer Configurations (One person could do it).



Access Point:

- A device that allows wireless devices to connect to a wired network using Wi-Fi.
- Access Point is a device that creates wireless local area network, or Wireless LAN.
- Access Point is a device creates Wireless LAN usually in an office or large building.
- AP is the device that allows multiple wireless devices to connect with each other.
- AP connects multiple wireless devices together in single or multiple wireless networks.
- AP is a networking device that is used to form wireless local area network in home.
- An access point connects to a wired router, switch, or hub via an Ethernet cable.
- AP is hardware device used to connect computer, laptops and mobile with each other.
- Wireless networks are suitable for those places where cables are difficult to install.
- An access point can also be used to extend the wired network to the wireless devices.
- The AP converts the wireless frequency subject into digital signals and then vice versa.

AP Categories:

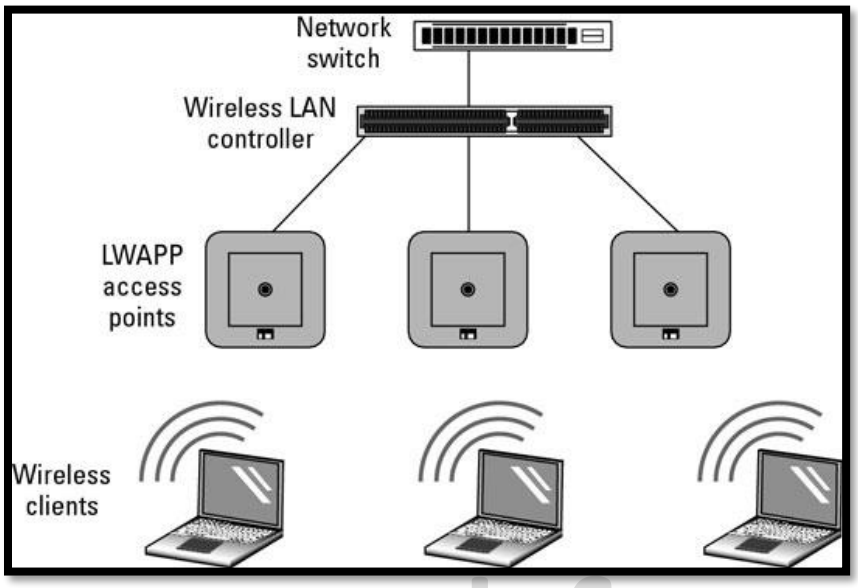
Autonomous APs:

- These are standalone devices configured using a command line interface or a GUI.
- Autonomous APs are useful in situations where only couple of APs is required in office.
- Such as home router is autonomous AP because entire configuration resides on device.
- If wireless demands increase, more Access Points (APs) would be required to deploy.
- Each AP operates independent of other APs & each AP require manual configuration.
- Each AP operates independent of other APs & each AP requires manual management.
- Autonomous Access Points is Standalone mode and Management address for remote.

Controller-Based APs:

- These devices require no initial configuration and are often called lightweight APs (LAPs).
- LAPs use Lightweight Access Point Protocol to communicate with WLAN controller (WLC).
- Controller-based APs are useful in situations where many APs are required in the network.

- As more APs are added, each AP is automatically configured and managed by the WLC.



Cisco AP Modes

From the WLC, you can configure a lightweight AP to operate in one of the following special-purpose modes:

Local: The default lightweight mode that offers one or more functioning BSSs on a specific channel. During times when it is not transmitting, the AP scans the other channels to measure the level of noise, measure interference, discover rogue devices, and match against intrusion detection system (IDS) events.

Monitor: The AP does not transmit at all, but its receiver is enabled to act as a dedicated sensor. The AP checks for IDS events, detects rogue access points, and determines the position of stations through location-based services.

FlexConnect: An AP at a remote site can locally switch traffic between an SSID and a VLAN if its CAPWAP tunnel to the WLC is down and if it is configured to do so.

Sniffer: An AP dedicates its radios to receiving 802.11 traffic from other sources, much like a sniffer or packet capture device. The captured traffic is then forwarded to a PC running network analyzer software such as Live Action Omni peek or Wireshark, where it can be analyzed further.

Rogue detector: An AP dedicates itself to detecting rogue devices by correlating MAC addresses heard on the wired network with those heard over the air. Rogue devices are those that appear on both networks.

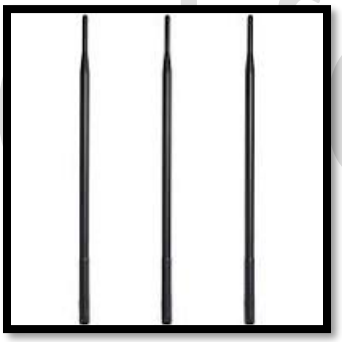
Bridge: An AP becomes a dedicated bridge (point-to-point or point to- multipoint) between two networks. Two APs in bridge mode can be used to link two locations separated by a distance. Multiple APs in bridge mode can form an indoor or outdoor mesh network.

Flex+Bridge: FlexConnect operation is enabled on a mesh AP.

SE-Connect: The AP dedicates its radios to spectrum analysis on all wireless channels. You can remotely connect a PC running software such as Meta Geek Chanalyzer or Cisco Spectrum Expert to the AP to collect and analyze the spectrum analysis data to discover sources of interference

Antennas:

- In Simple words we can say Antenna is metallic wire use to transmit or receive RF signal.
- Wireless routers have different types of antennas; some routers have antennas built in.
- Sometimes the Wi-Fi routers will have a choice of antenna you can attach to the router.
- Antennas come in many sizes & shapes, each with its own gain value & intended purpose.
- There are many specific types of antennas, but two basic types are used most of time.
- Most business class APs requires external antennas to make them fully functioning units.



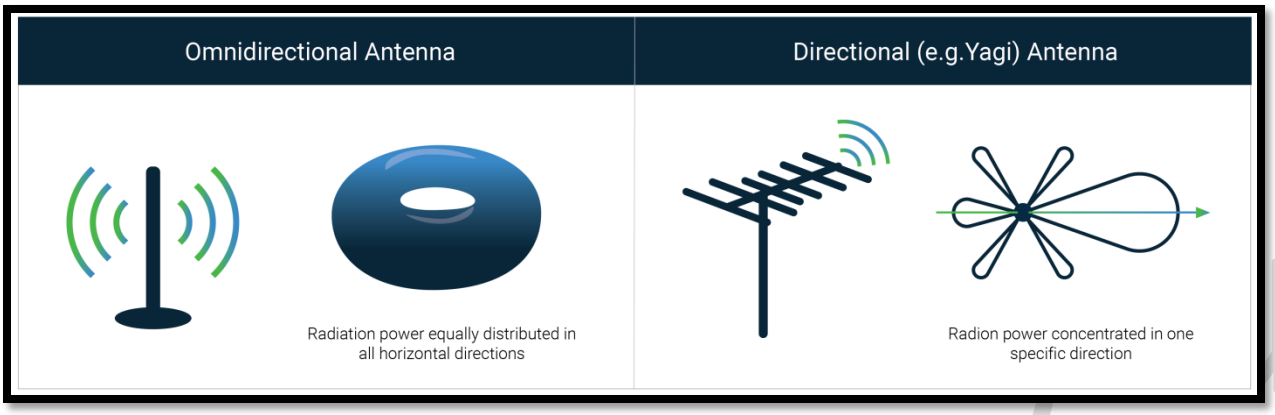
Omnidirectional Antennas:

- An omnidirectional antenna sends a signal out equally in all directions around it.
- Using omnidirectional antennas has benefit of creating connections in any direction.
- You don't have to do as much planning to connect with multiple neighbors or buildings.
- Omnidirectional Antenna If there is enough signal between nodes, they should connect.
- All-direction strength of antennas comes with drawback of transmitting weaker signal.
- Since signal is going in all directions, it spreads out & gets weaker with distance very fast.
- If the nodes or clients, PC, Laptop or end point are far away, they may not connect well.
- Provide 360-degree coverage & are ideal in houses, office, conference rooms & outside.

Directional Antennas:

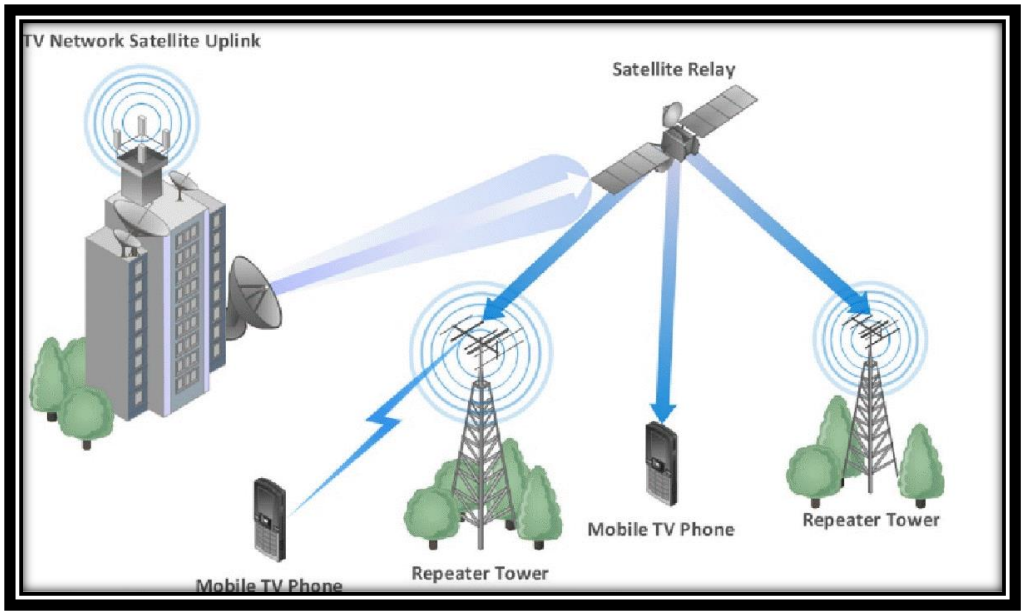
- Next type of antenna is known as directional. It sends out a signal in a more focused way.
- This Type of Antennas, Directional antennas focus the radio signal in a given direction.
- Using directional antennas has benefit of increasing distance signal travel in one direction.
- Power that would be sent out in all directions with omnidirectional nodes is now focused.
- This type of Directional antennas is commonly used in point-to-point configurations and connecting two distant buildings.

Examples of directional: Wi-Fi antennas include Yagi and parabolic dish antennas.



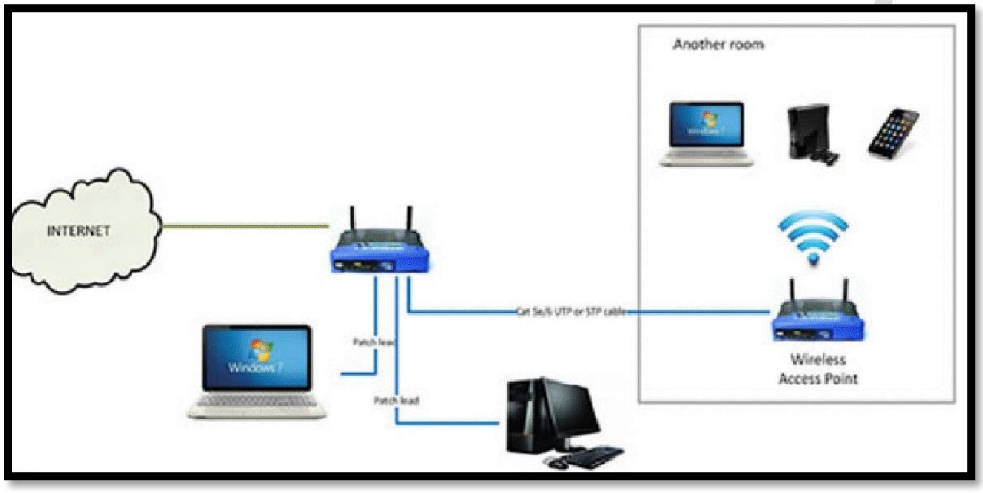
There are basically three different types of wireless networks – WAN, LAN and PAN:

Wireless Wide Area Networks (WWAN):



- Interconnecting devices over large areas, such as cities or countries (Very large distance coverage) like multiple satellite systems or antenna sites looked after by an ISP.
- Mobile telecommunication cellular network technologies such as 2G, 3G, 4G LTE and 5G to transfer data.

Wireless Local Area Network (WLAN):

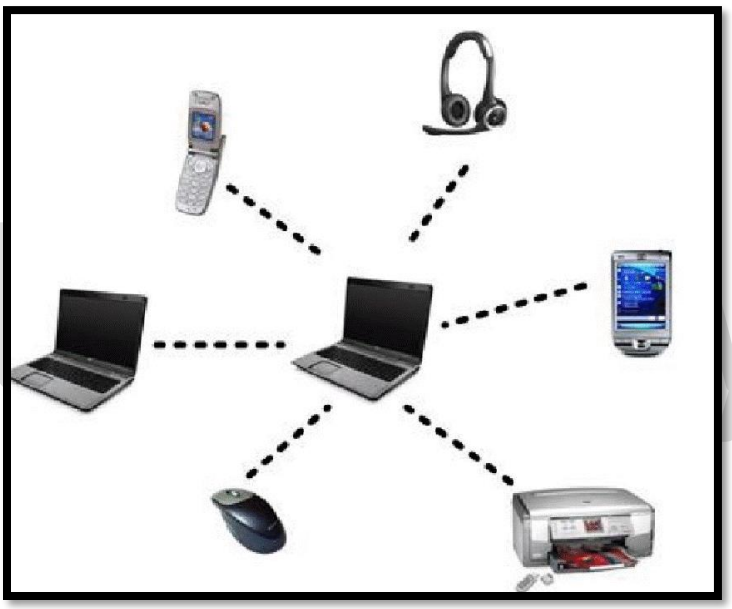


- WLAN are wireless networks that use radio waves.
- The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network.

- The range of a WLAN can be anywhere from a single room to an entire campus.
- Devices within 100m of a wireless access point.

Wireless Personal Area Network (WPAN):

- WPANs are short-range networks that use Bluetooth technology.
- Devices are within 10 meters of each other.
- Bluetooth is often used.
- They are commonly used to interconnect compatible devices near a central location, such as a desk.
- A WPAN has a typical range of about 30 feet.



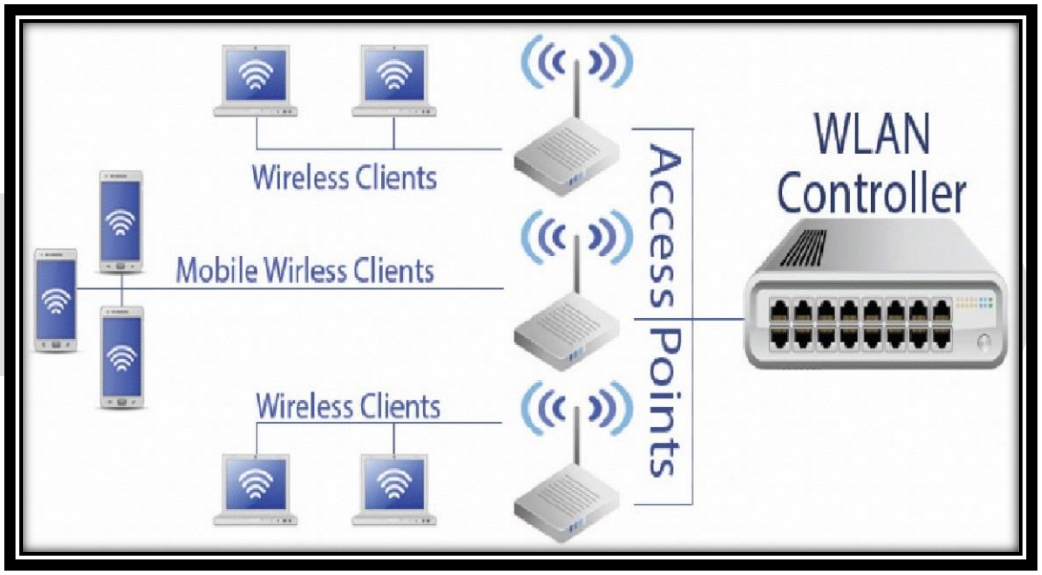
Wireless communication usually involves a data exchange between two devices.

- A wireless LAN goes even further; many devices can participate in sharing the medium for data Exchanges.
- Wireless LANs must transmit a signal over radio frequencies (RF) to move data from one device to another.
- Transmitters and receivers can be fixed in consistent locations, or they can be mobile and free to move around.

- Wireless devices must adhere to a common standard (IEEE 802.11).
- Wireless coverage must exist in the area where devices are expected to use it.

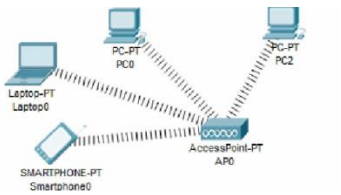
Wireless LAN – Devices:

- Wireless clients with Wireless NIC.
- Laptops, IP Phones, Smartphones and Printer.
- Access Points.
- Wireless LAN Controller (WLC).



Wireless Access Point (WAP):

- Provides centralized location to connect devices with in the LAN.
- Without wire (it is using RF Signals).
- Allows other WIFI devices to connect to a wired network.
- Provide wireless Internet in Public palaces, like shops, Airport and coffee shops.

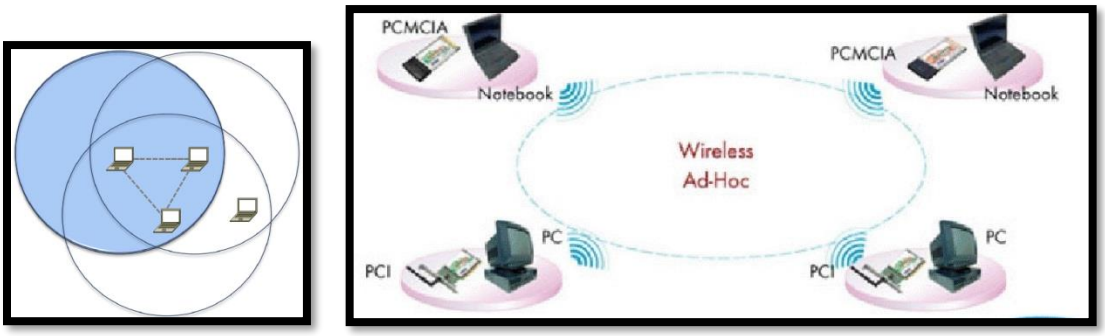


Wireless LAN Controllers (WLC):

- Provides Centralized management of all access points in the networks.
- Make it easier to manager large wireless scale deployments.

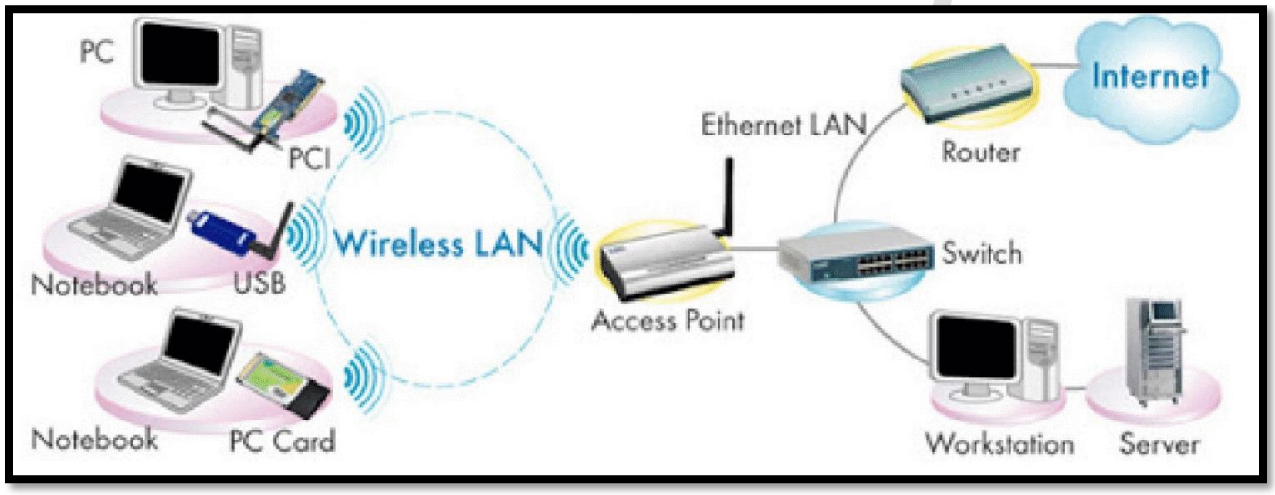
Ad Hoc Networks:

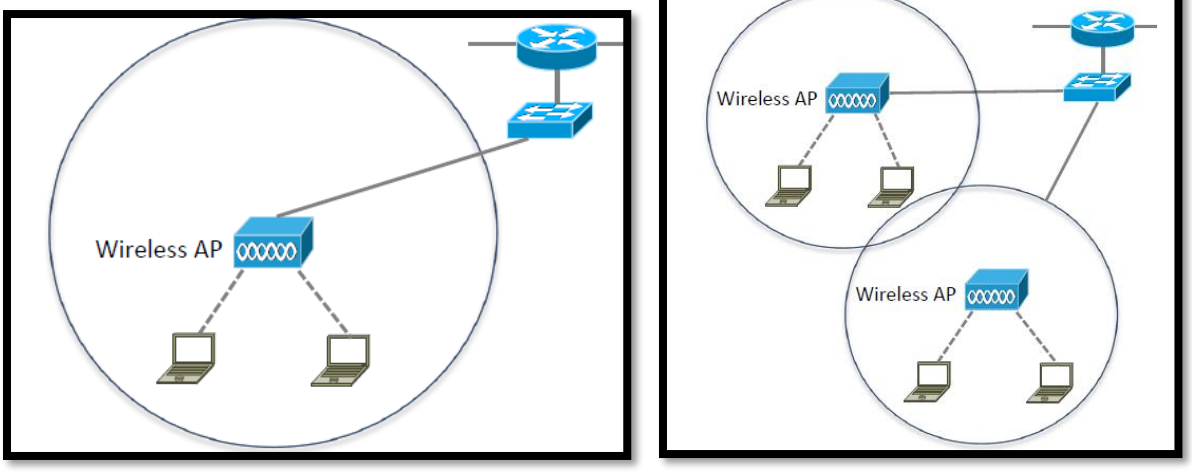
- Two or more wireless stations communicate directly with each other.
- IBSS Independent Basic Service Set.
- Ad hoc networks rely on multi-hop transmissions among the nodes in the same channel.
- Nodes communicate with each other through the intermediate nodes.
- So, the efficient performance and availability of each node is important in ad hoc network environment.
- Ad Hoc also called computer to computer or peer mode.



Infrastructure Mode:

- Stations communicate via a Wireless Access Point (AP).
- This can provide access to a wired network.
- Requires a central access point that all devices connect to.
- Devices on the network all communicate through a Access Point (AP).
- Like Laptop or smart mobile send packet to the access point and it send to the other devices.
- Most wireless networks function in infrastructure mode.
- Access points acts as a bridge to other wireless or wired network.





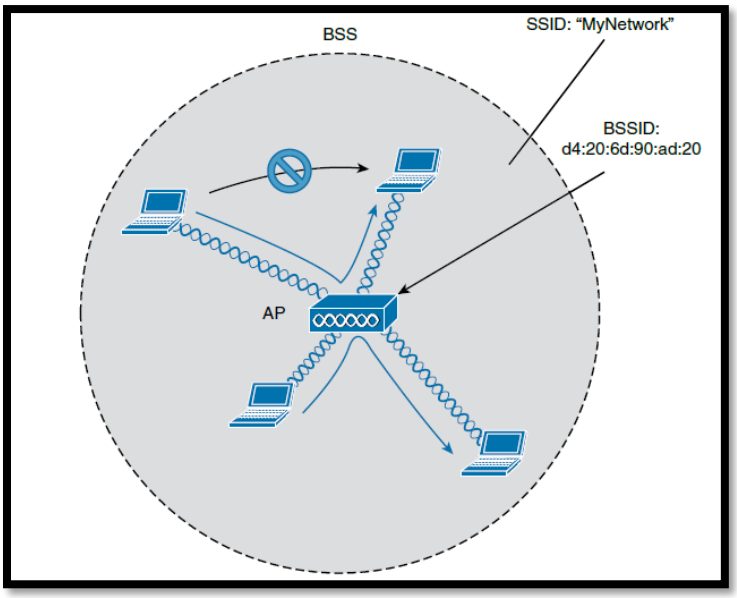
- **Multiple Access Points can be deployed to provide the required coverage area**
- **Wireless stations work in either Ad-HOC or Infrastructure Mode they cannot operate in both at the same time.**
- **BSSID is the MAC address of the AP's radio for that service set. SSID is the service set identifier or network name for the basic service set(BSS). ESSID is the same as the SSID but is used across multiple access points as part of the same WLAN.**

Wireless LAN terminology:

- SSID
- Basic Service Set (BSS)
- Basic Service Area (BSA)
- Distribution system
- Extended Service Set (ESS)
- 802.11

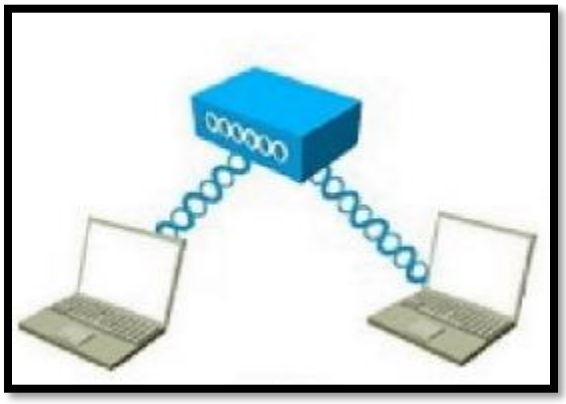
SSID (Service Set Identifier):

- SSID stand for Service Set Identifier.
- SSID is the name for a WIFI network.
- Unique ID used for naming wireless networks.
- Client devices use this name to identity and join wireless networks.
- A single Access Point can support multiple SSIDs.
- Different SSIDs can have different security settings and be mapped to different VLANs.



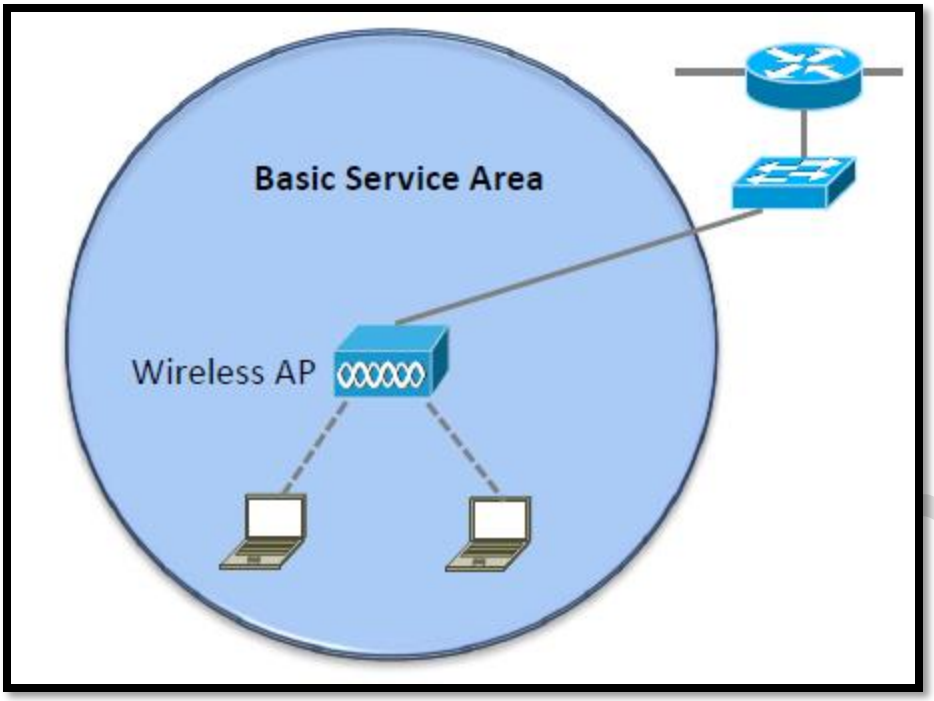
BSS (Basic Service Set):

- BSS stand for Basic Service Set.
- With a Basic Service Set (BSS), wireless clients connect to a wireless network through an AP.
- The idea behind a BSS is that the AP is responsible for the wireless network. A BSS we use for most wireless networks
- Each wireless client advertises its capabilities to the AP, and the AP grants or denies permission to join the network.
- The BSS uses a single channel for all communication.
- The AP and its wireless clients use the same channel to transmit and receive.



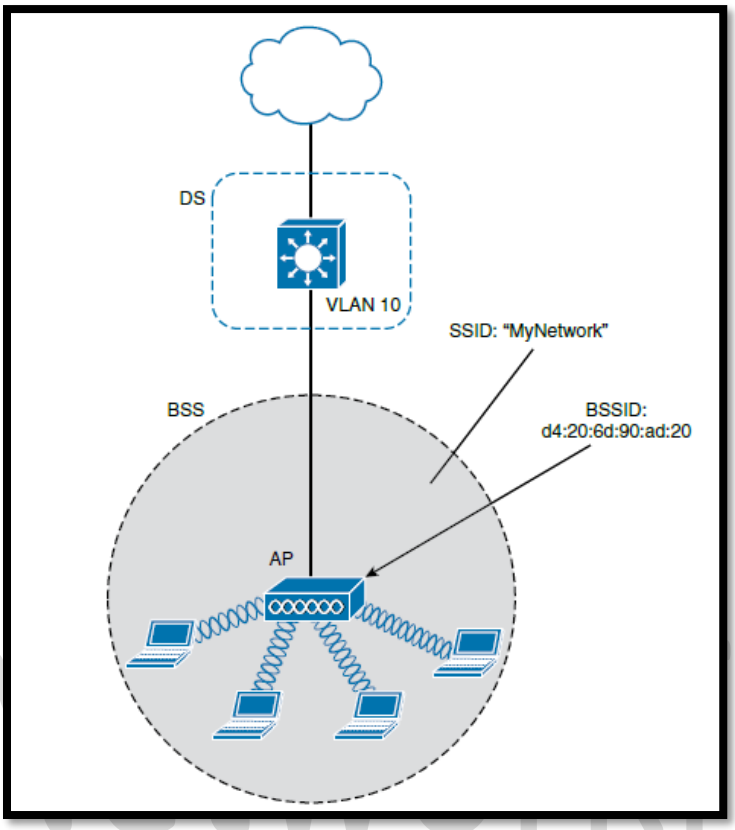
BSA (Basic Service Area):

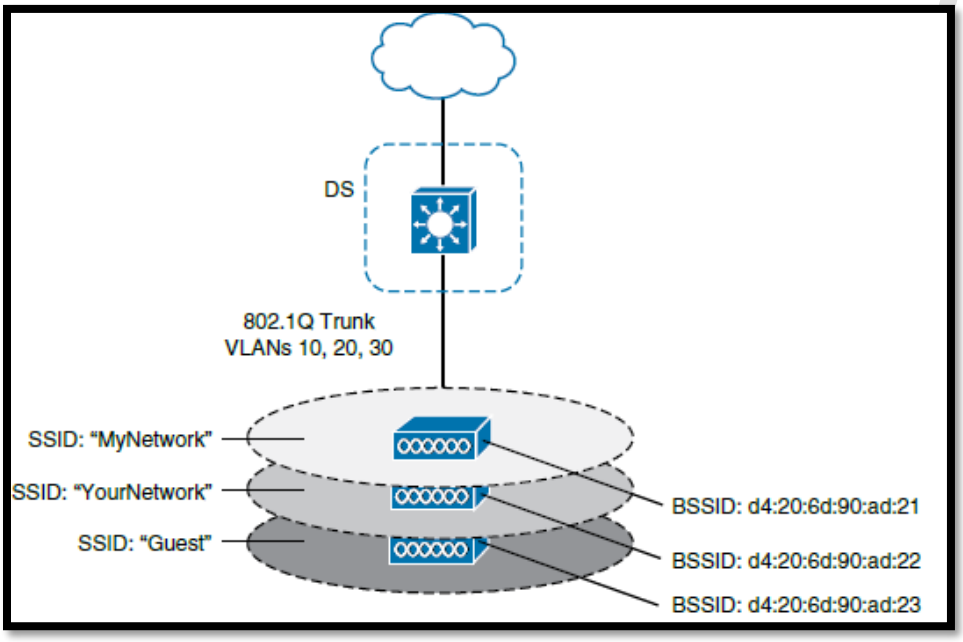
- BSS stand for Basic Service Area.
- The BSA is the Wireless Coverage area of an Access Point.
- Also known as a wireless cell.



Distribution System:

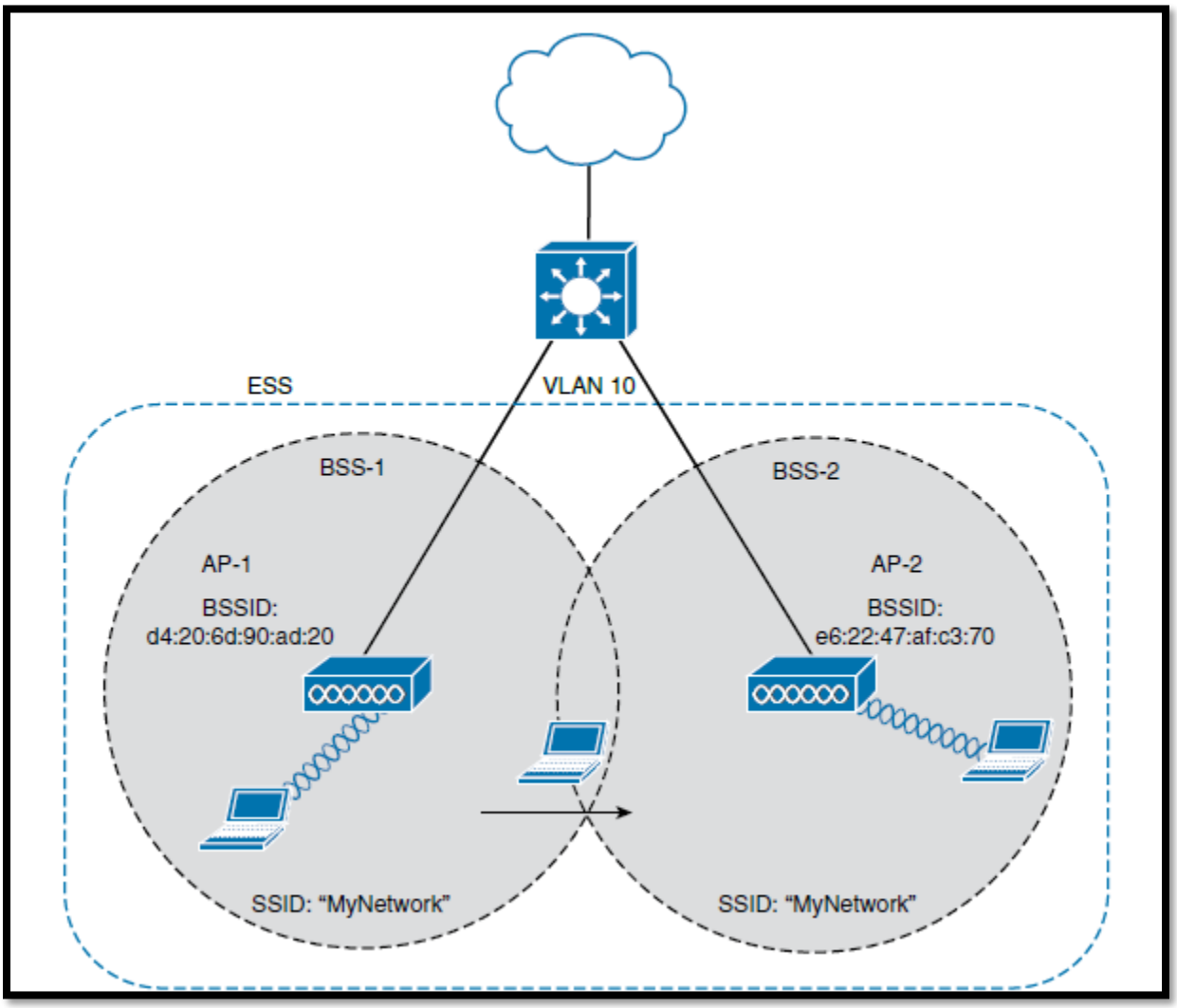
- Notice that a BSS involves a single AP and no explicit connection into a regular Ethernet network.
- In that setting, the AP and its associated clients make up a standalone network.
- But the AP's role at the center of the BSS does not just stop with managing the BSS; sooner or later,
- Wireless clients will need to communicate with other devices that are not members of the BSS.
- Fortunately, an AP can also uplink into an Ethernet network because it has both wireless and wired capabilities.
- The 802.11 standard refers to the upstream wired Ethernet as the distribution system (DS) for the wireless BSS, as shown below.


DS
VLAN 10
SSID: "MyNetwork"
BSS
BSSID:
d4:20:6d:90:ad:20
AP


DS
802.1Q Trunk
VLANs 10, 20, 30
SSID: "MyNetwork"
SSID: "YourNetwork"
SSID: "Guest"
BSSID: d4:20:6d:90:ad:21
BSSID: d4:20:6d:90:ad:22
BSSID: d4:20:6d:90:ad:23

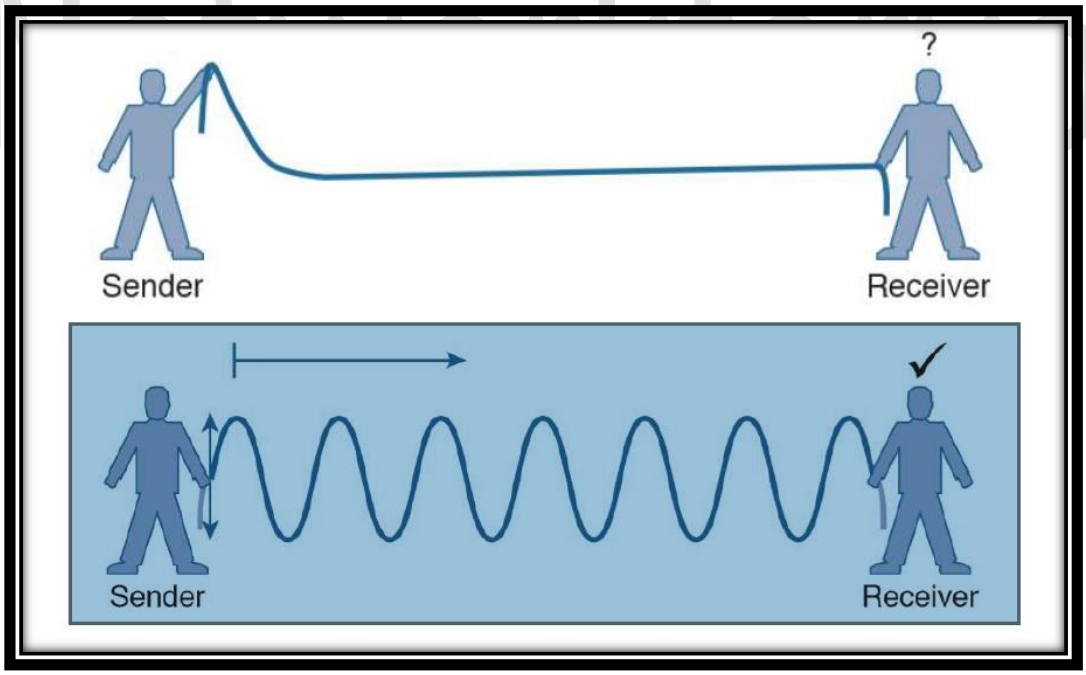
ESS (Extended Service Set):

- ESS Stand for Extended Service Set.
- Normally one Access Point cannot cover the entire area where clients might be located so we need to use Extended Service Set.
- Example you need to have wireless Coverage throughout an entire floor of Office or Hotel or Hospital or any large building.
- Simply need to add more Access points to coverage large area.



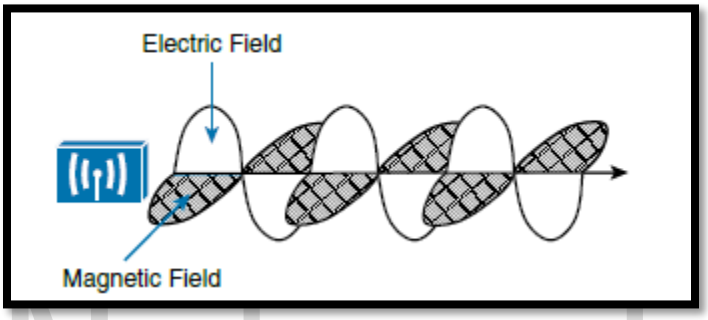
RF Overview:

- To send data across a wired link, an electrical signal is applied at one end and carried to the other end.
- The wire itself is continuous and conductive, so the signal can propagate rather easily.
- A wireless link has no physical strands of anything to carry the signal along. How, then, can an electrical signal be sent across the air, or free space?
- Consider a simple analogy of two people standing far apart. One person wants to signal something to the other.
- They are connected by a long and somewhat loose rope; the rope represents free space.
- The sender at one end decides to lift his end of the rope high and hold it there so that the other end of the rope will also rise and notify the partner.
- After all, if the rope were a wire, he knows that he could apply a steady voltage at one end of the wire and it would appear at the other end.
- As showing below picture shows the end result; the rope falls back down after a tiny distance, and the receiver never notices a change.



- The sender tries a different strategy. He cannot push the rope, but when he begins to wave it up and down in a steady, regular motion, a curious thing happens.
- A continuous wave pattern appears along the entire length of the rope, as shown in above picture.

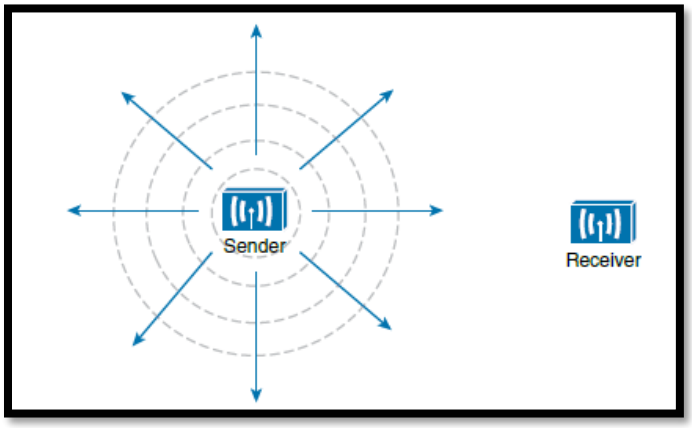
- In fact, the waves (each representing one up and down cycle of the sender's arm) actually travel from the sender to the receiver.
- In free space, a similar principle occurs. The sender (a transmitter) can send an alternating current into a section of wire (an antenna), which sets up moving electric and magnetic fields that propagate out and away as traveling waves.
- The electric and magnetic fields travel along together and are always at right angles to each other, as shown in below picture.
- The signal must keep changing, or alternating, by cycling up and down, to keep the electric and magnetic fields cycling and pushing ever outward.



- Electromagnetic waves do not travel in a straight line. Instead, they travel by expanding in all directions away from the antenna.
- To get a visual image, think of dropping a pebble into a pond when the surface is still. Where it drops in, the pebble sets the water's surface into a cyclic motion.
- The waves that result begin small and expand outward, only to be replaced by new waves.
- In free space, the electromagnetic waves expand outward in all three dimensions.

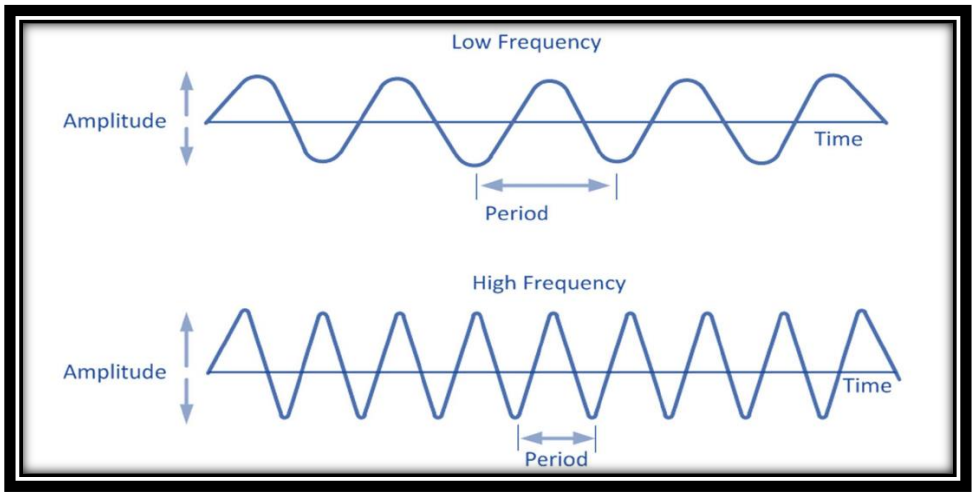
Receivers and Transmitters:

- In Wireless Network when a device sends out a wireless signal, it is called a transmitter.
- When another device picks up wireless signal & understands information called receiver.



Frequency:

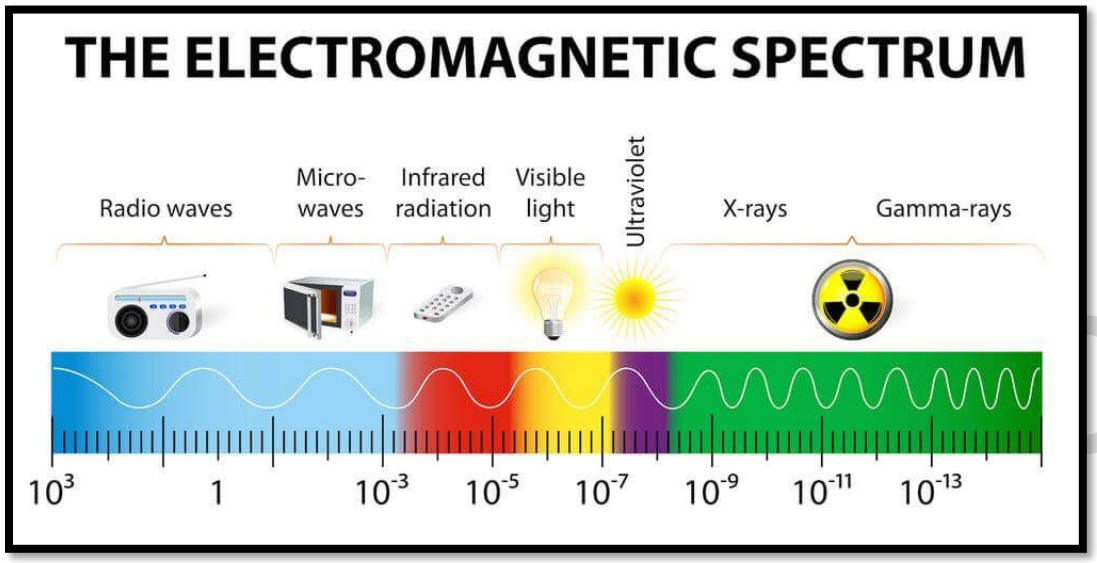
- Wireless signals occupy spectrum/wide range, of frequencies: rate at which signal vibrates.
- Frequency refers to the number of times an event or a value occurs.
- If signal vibrates slowly, it has low frequency, if vibrates very quickly, it has high frequency.
- Frequency is measured in Hertz, which is count of how quickly signal changes every second.
- Higher frequencies give higher data rates, higher frequency more waves in given time cycle.
- The Wireless technology uses the unlicensed radio spectrum/range to send & receive data.
- Unlicensed spectrum is accessible to anyone who has wireless router & wireless technology.
- Frequency is number of times signal makes one complete up and down cycle in 1 second.

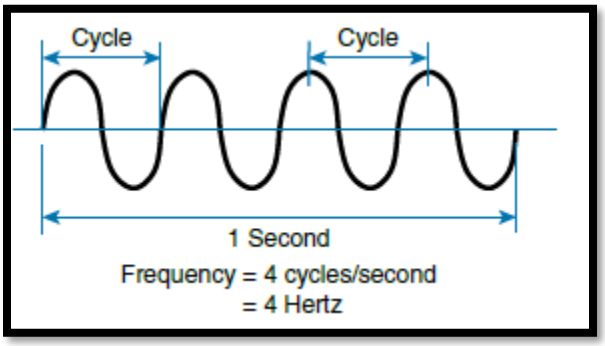


https://emanim.szialab.org/index.html

Radio Frequencies:

- All wireless devices operate in the radio waves range of the electromagnetic spectrum.
- The Wireless LAN networks operate in the 2.4 GHz frequency band and the 5 GHz band.
- WLAN devices have transmitters & receivers tuned to specific frequencies of waves range.
- Specifically, the following frequency bands are allocated to the 802.11 wireless LANs.
- Wireless LAN 2.4 GHz (UHF) - 802.11b/g/n/ax and WLAN 5 GHz (SHF) - 802.11a/n/ac/ax.
- The strength of an Radio Frequency signal is usually measured by its power, in watts(W).





Terminologies:

Cycle:

- Cycle can begin signal rises from center line, falls through center line & rises again.

- Cycle can be measured from the center of one peak to the center of the next peak.
- In above image, during that 1 second, signal progressed through four complete cycles.

Hertz:

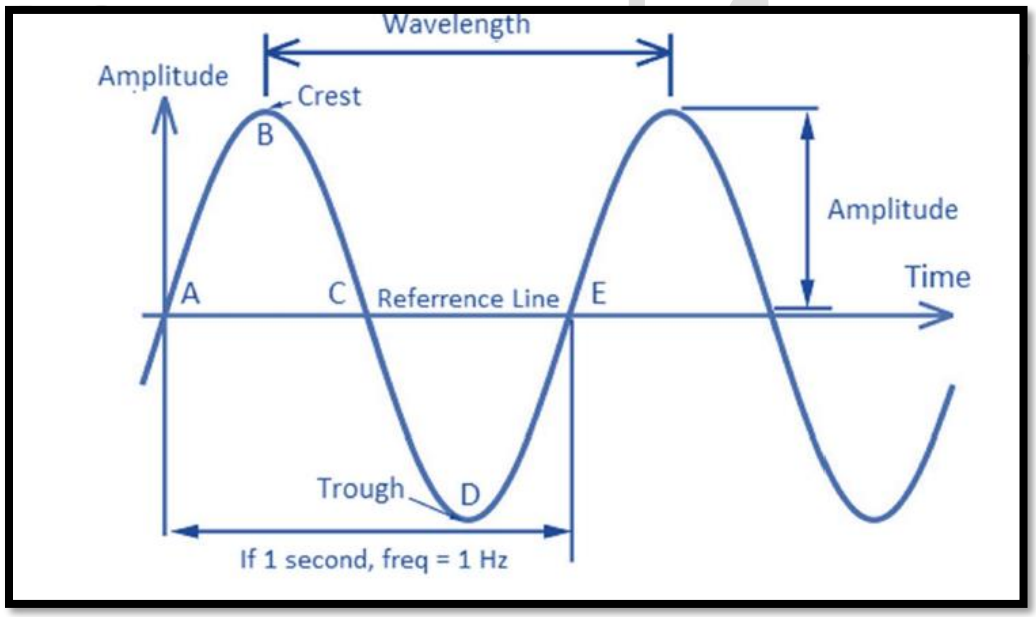
- Hertz is most commonly used frequency unit & is nothing than one cycle per second.

Amplitude:

- Amplitude the height from the top peak to the bottom peak of the signal's waveform.
- It is power or intensity of signal, the frequency is how often the signal repeated itself.
- Higher the amplitude it will produce the higher range, lower amplitude lower range.

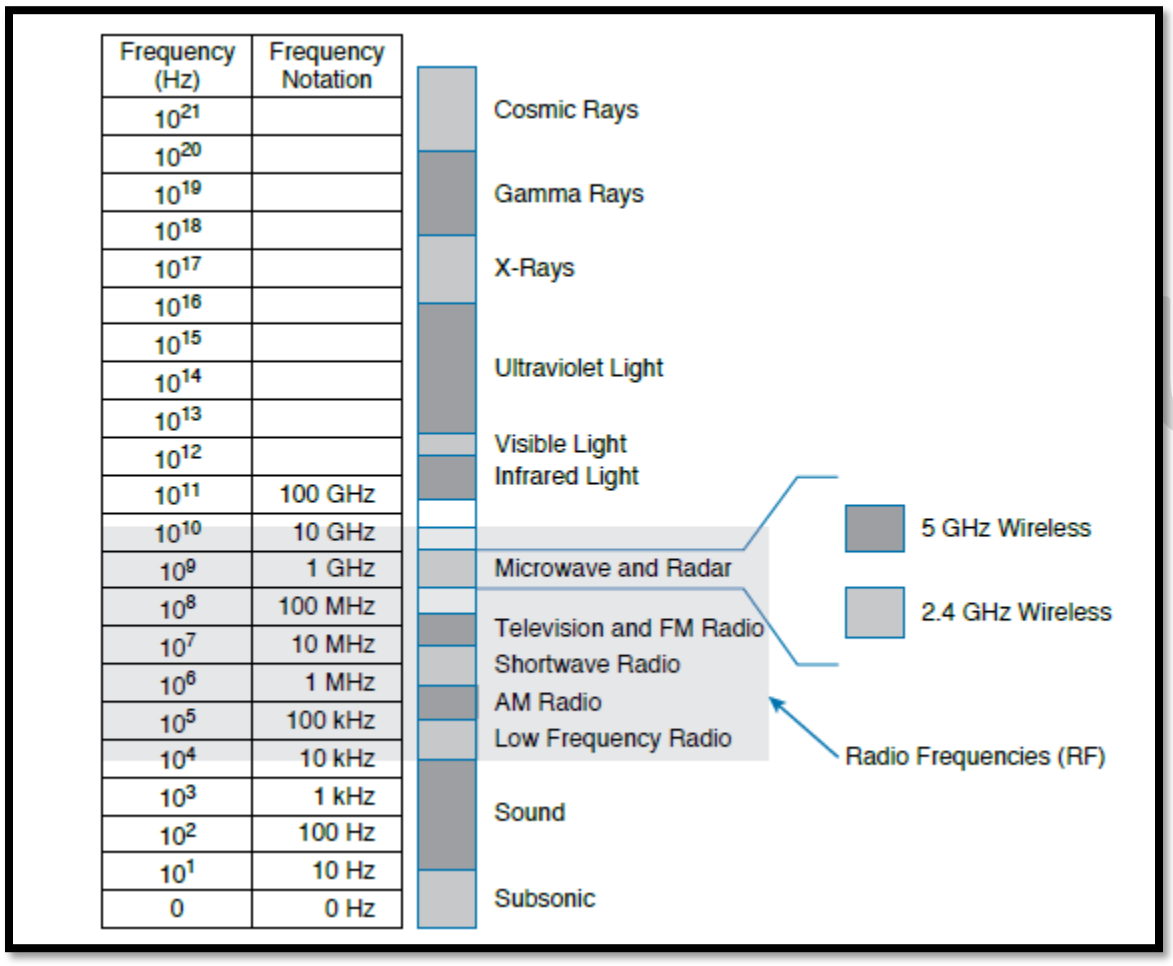
Wavelength:

- In wavelength they are the crest which is the high point, the trough which is low point.
- The wavelength is the distance from one crest or higher point, or trough, to another.

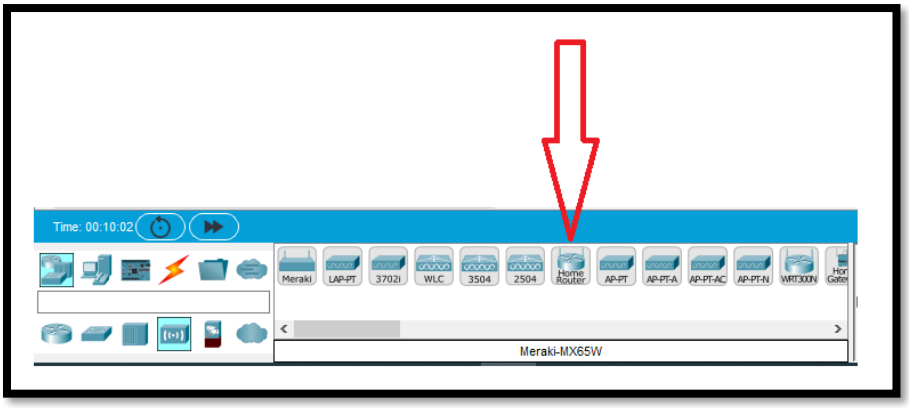


Frequency Unit Names:

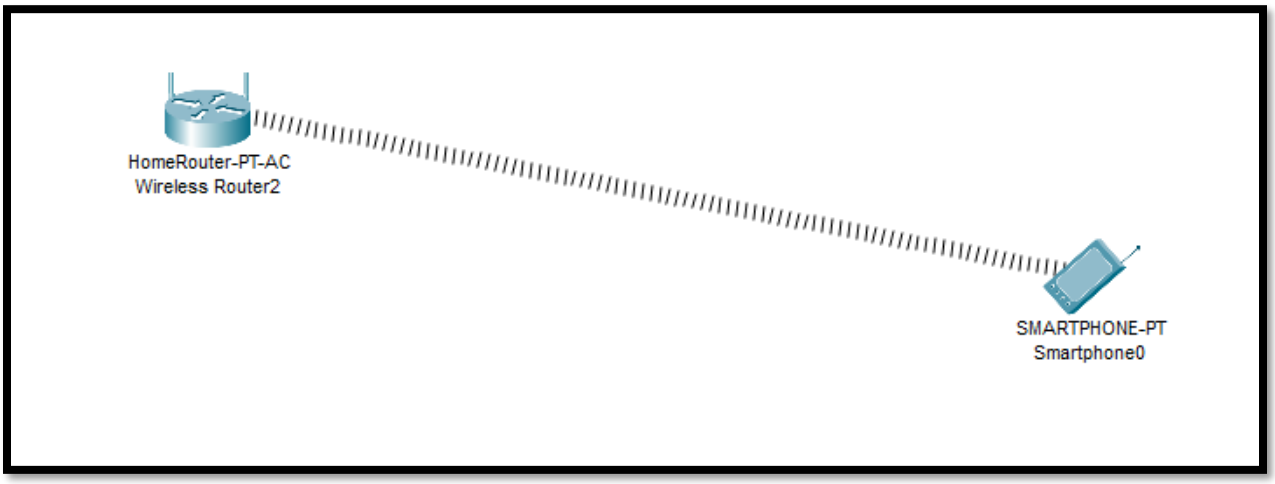
Unit	Abbreviation	Meaning
Hertz	Hz	Cycles per second
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1,000,000 Hz
Gigahertz	GHz	1,000,000,000 Hz



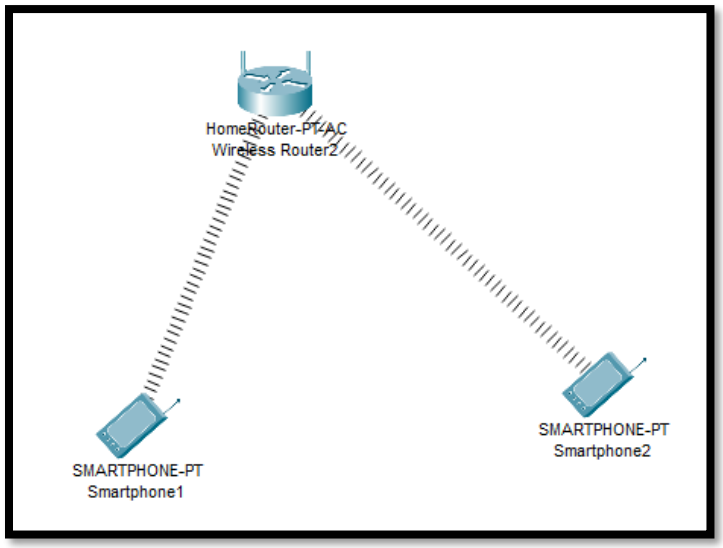
Design Home Router:



Take this Home Router



- We need to set Network SSID we can set any name as given below.
- We have three Network SSID we can set all three as given below.
- Then we need to assign password as given below screen short.

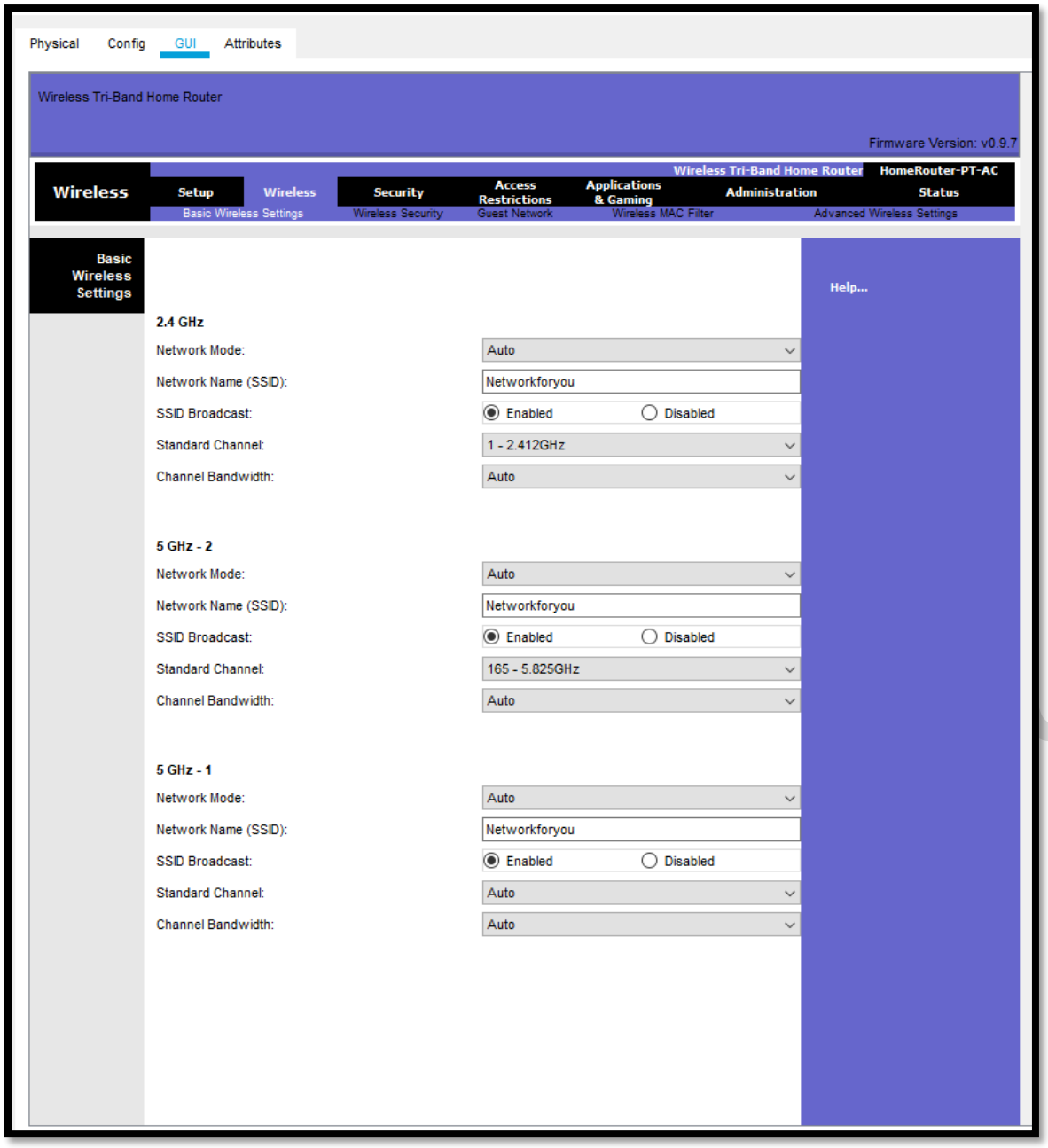


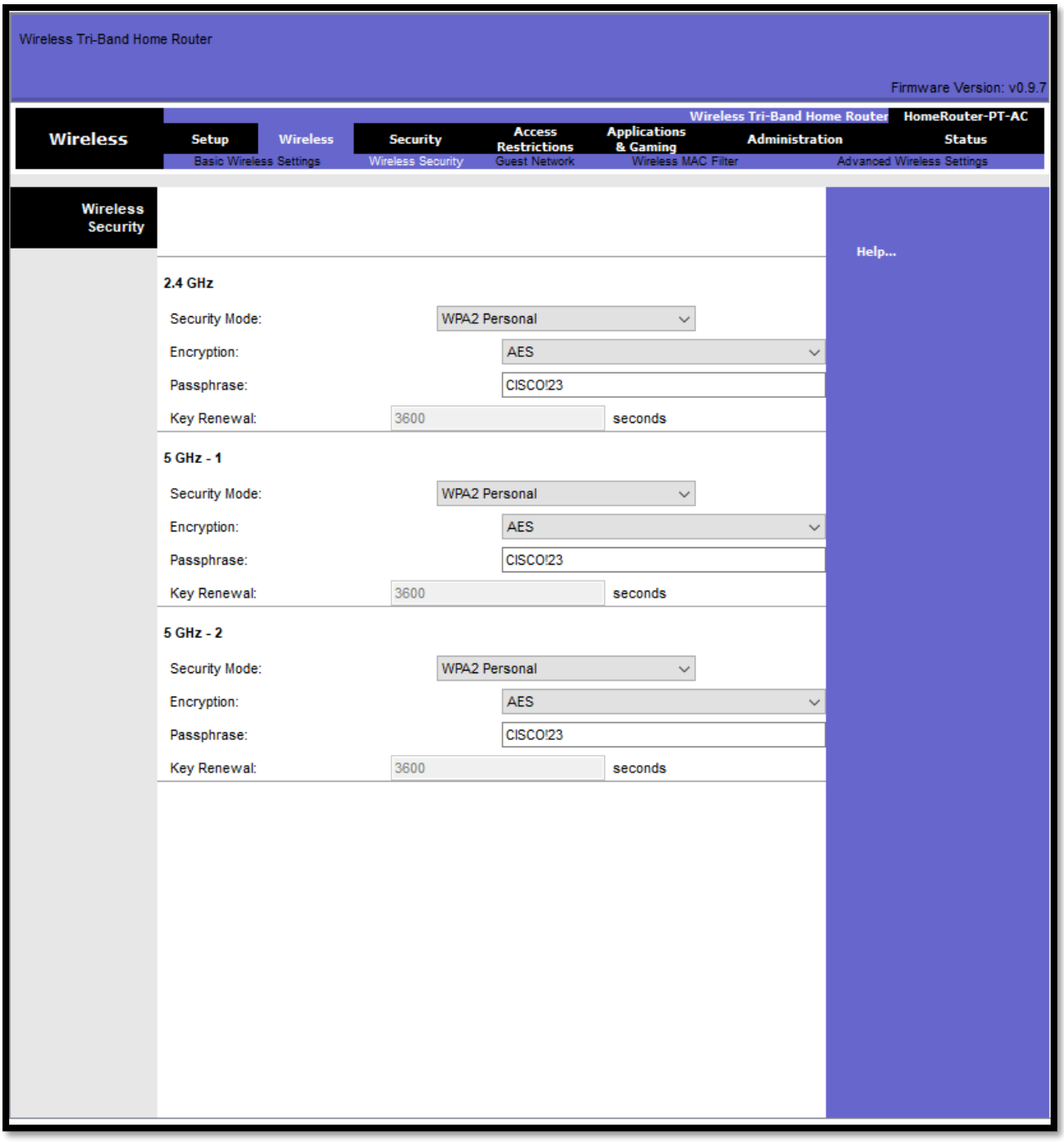
Smartphone1

Physical Config Desktop Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.102

Pinging 192.168.0.102 with 32 bytes of data:

Reply from 192.168.0.102: bytes=32 time=28ms TTL=128
Reply from 192.168.0.102: bytes=32 time=36ms TTL=128
Reply from 192.168.0.102: bytes=32 time=23ms TTL=128
Reply from 192.168.0.102: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 36ms, Average = 23ms

C:\>ipconfig

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::290:CFF:FE7B:5CED
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.101
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

3G/4G Cell1 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:43FF:FED0:7A9D
   IPv6 Address.....: ::
   Autoconfiguration IPv4 Address..: 169.254.122.157
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```


Physical
Config
GUI
Attributes
Wireless Tri-Band Home Router
Firmware Version: v0.9.7
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Wireless Tri-Band Home Router
HomeRouter-PT-AC
Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Advanced Wireless Settings
Basic Wireless Settings
Help...
2.4 GHz
Network Mode: Auto
Network Name (SSID): Networkforyou
SSID Broadcast: Enabled Disabled
Standard Channel: 1 - 2.412GHz
Channel Bandwidth: Auto
5 GHz - 2
Network Mode: Auto
Network Name (SSID): Networkforyou
SSID Broadcast: Enabled Disabled
Standard Channel: 165 - 5.825GHz
Channel Bandwidth: Auto
5 GHz - 1
Network Mode: Auto
Network Name (SSID): Networkforyou
SSID Broadcast: Enabled Disabled
Standard Channel: Auto
Channel Bandwidth: Auto



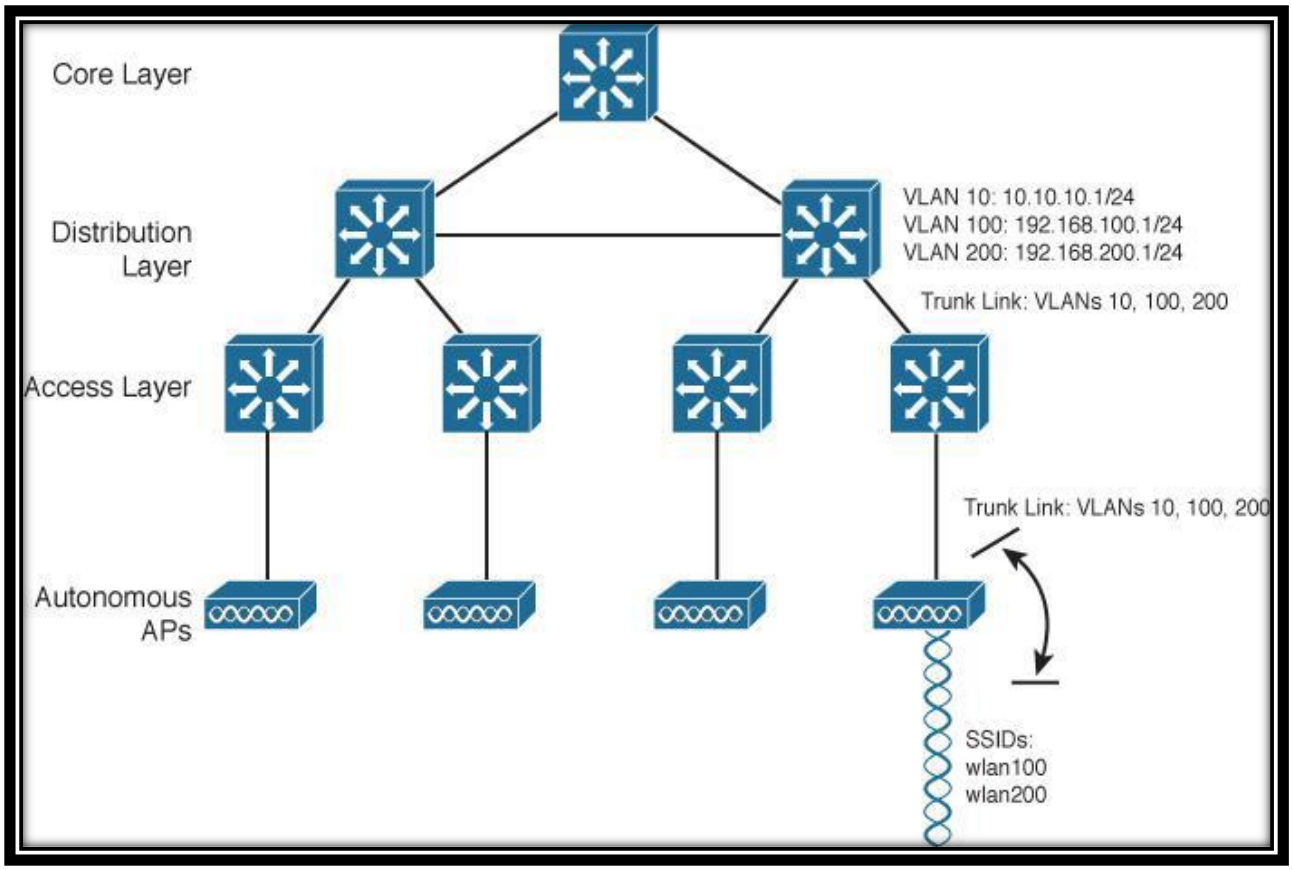
https://emanim.szialab.org/index.html

Wireless Architectures:

Let have a look on different CISCO Wireless Architectures use in Enterprise Networks.

Autonomous AP Architecture:

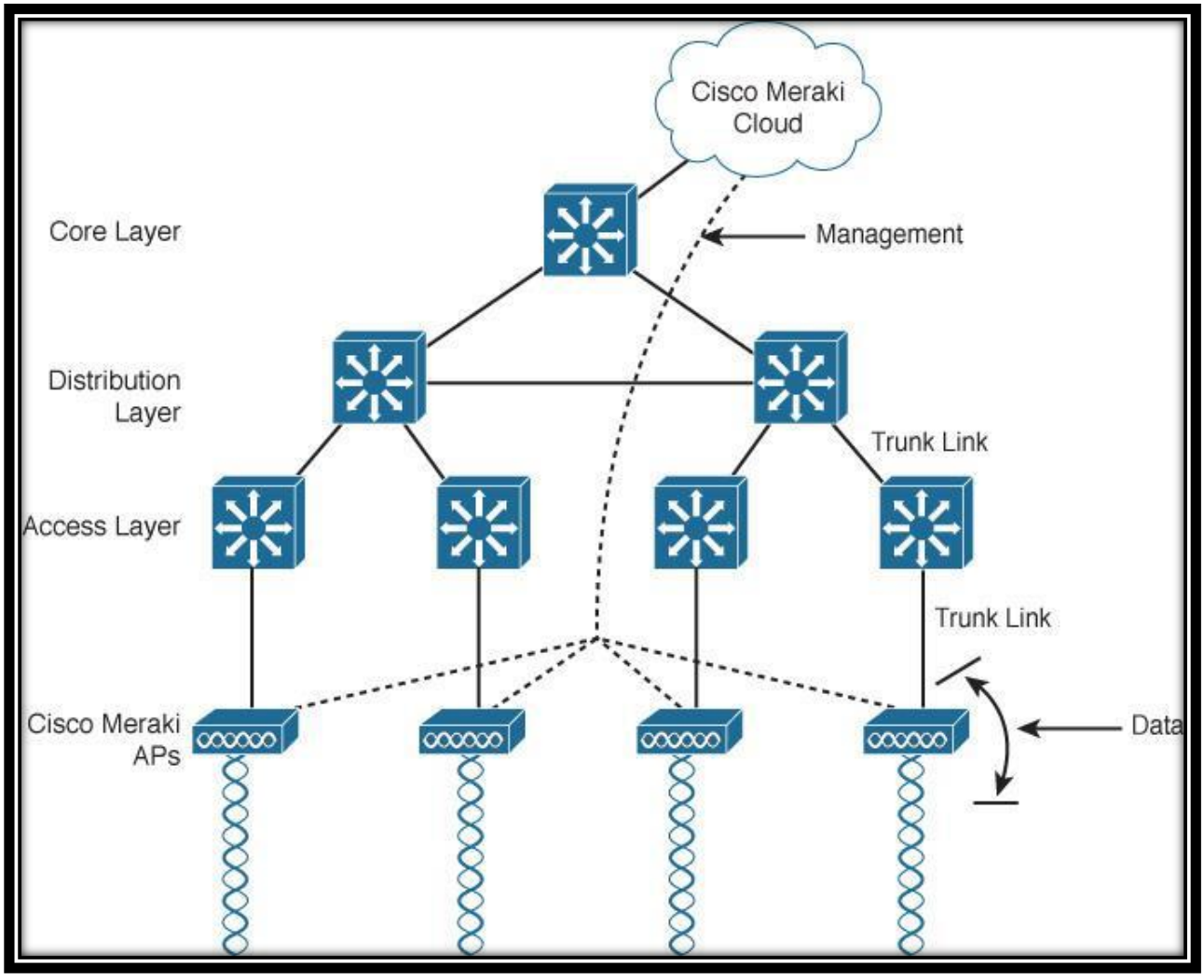
- Autonomous Architecture, access points (APs) are stand-alone.
- Autonomous AP has all required intelligence to serve wireless clients & to connect wired.
- The Autonomous APs are stand-alone access points (AP) with fully integrated intelligence.



Autonomous APs work alone; we need to configure one by one this is a drawback for using Autonomous Aps.

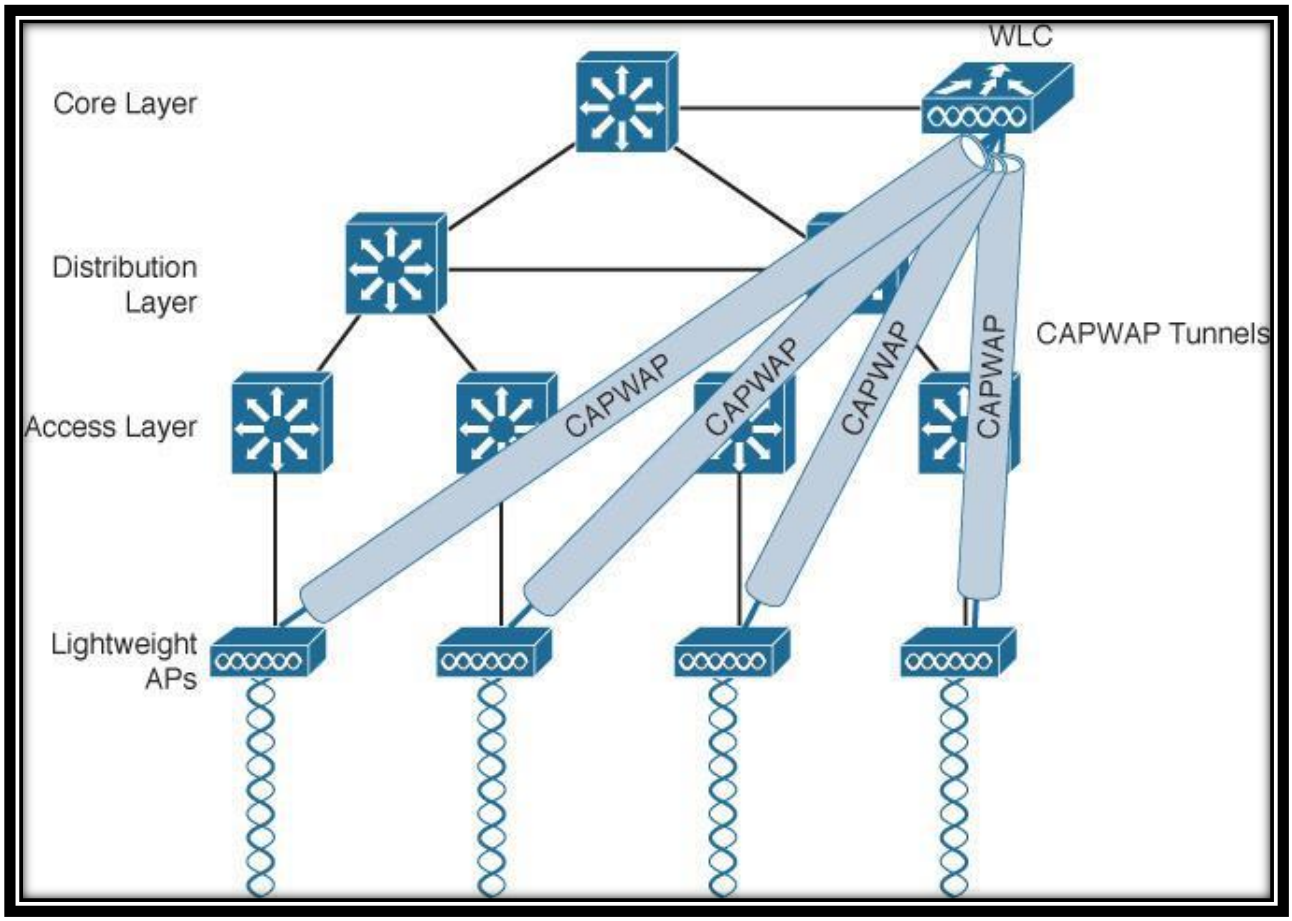
Cloud-Based Architecture:

- Cloud-based AP management function is pushed out of the Enterprise into Internet cloud.
- Cisco Meraki is a cloud based solution that offers centralized management of the Wireless.
- Network is arranged same as autonomous AP, but managed would be redirected to a cloud.
- Where AP management function is pushed out of enterprise and into the Internet cloud.
- From cloud, can push out code upgrades & configuration changes to APs in the enterprise.
- Cloud-Based all of APs are managed, controlled, and monitored centrally from the cloud.



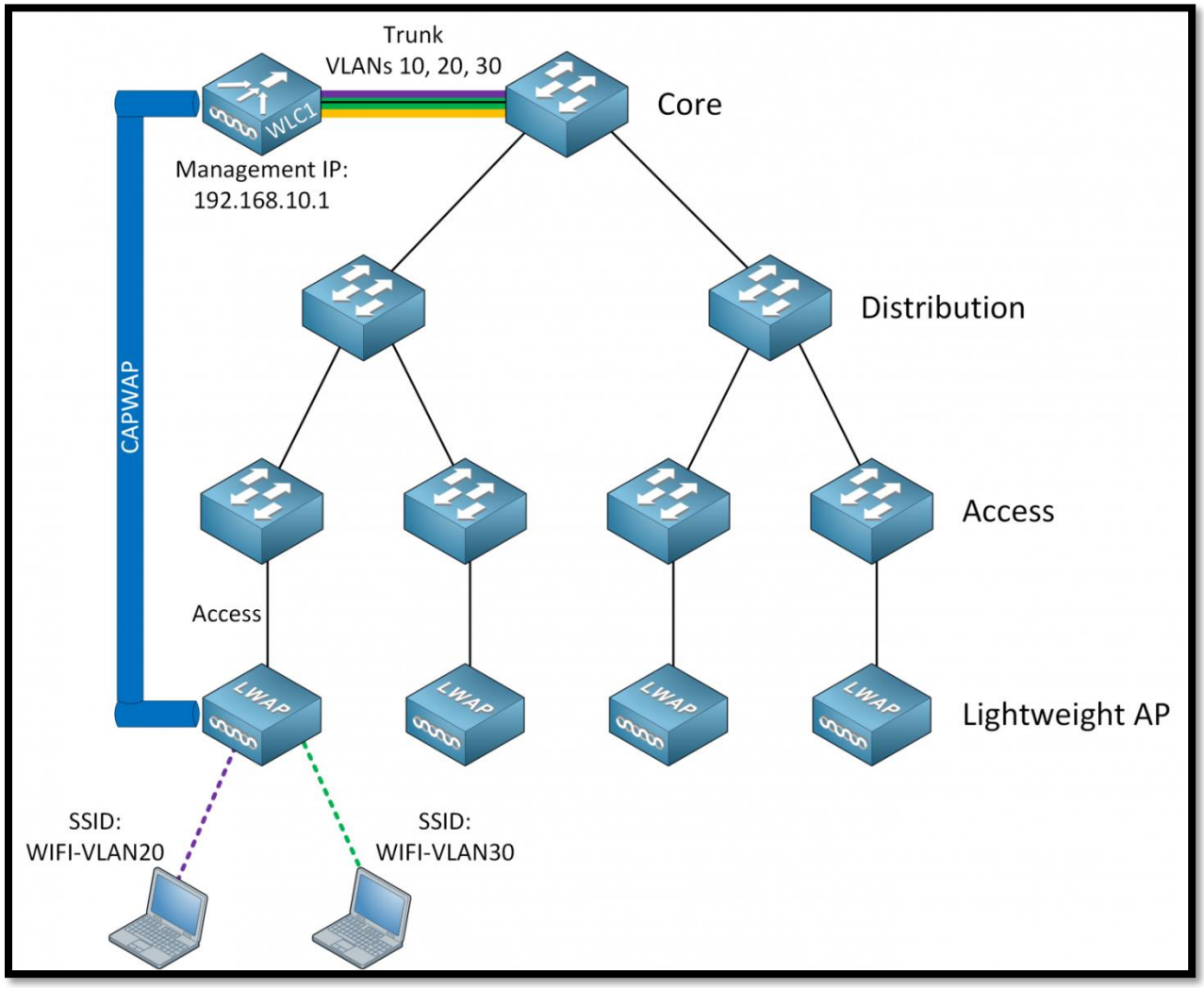
Centralized Wireless Network:

- WLC for multiple APs, where do set up WLC so that it can cover as much APs as it can.
- For that we set the WLC in the core layer, to have a centralized view of the network.
- If you want to deploy a WLC to support the multiple lightweight APs in your network.
- One approach is locate WLC in central location that maximize number of APs joined it.
- Traffic to & from wireless users travel over CAPWAP tunnels (Control and Provisioning of Wireless Access Points (CAPWAP) tunneling protocol) reach into center of network.
- Centralized WLC provides convenient place to enforce security policies that affect all users.
- All management functions are usually performed on a wireless LAN Controller (WLAC).



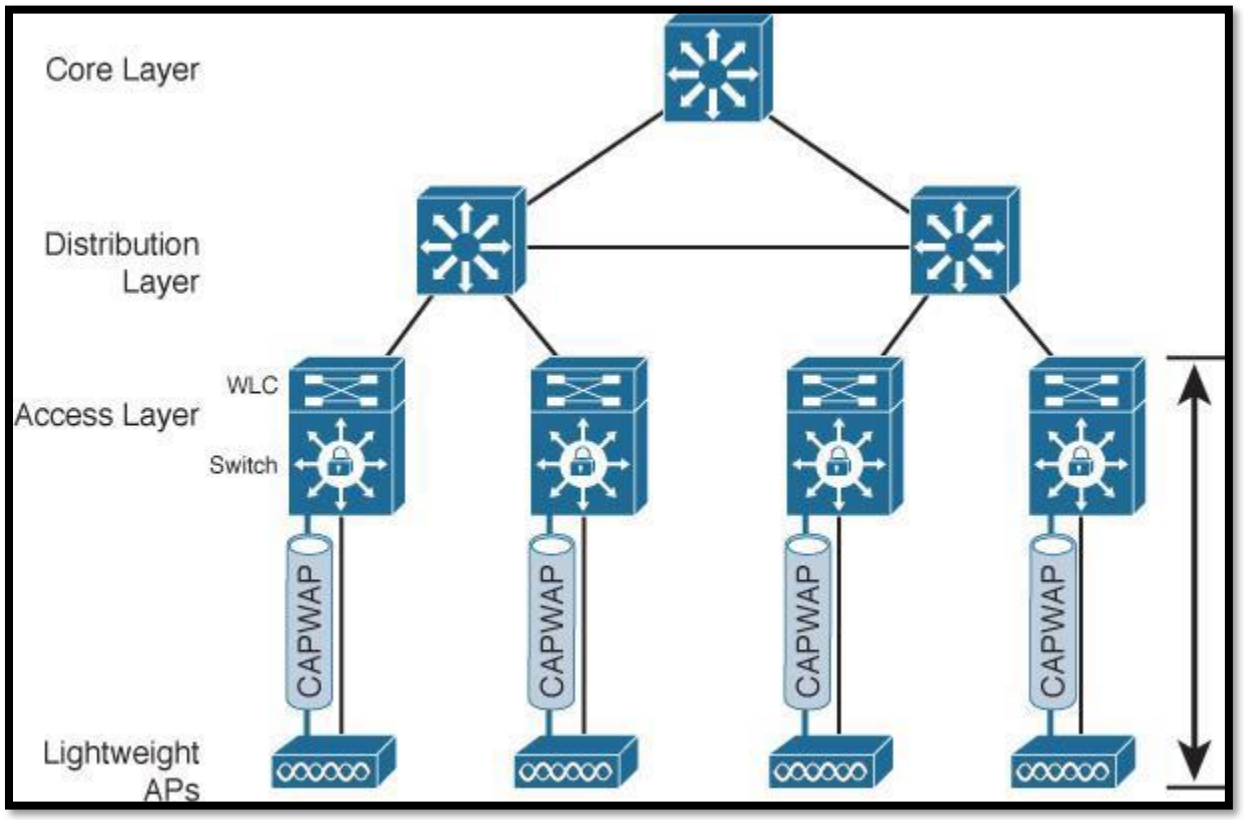
Split-MAC Architecture:

- Split-MAC means is that management process is divided into two separate streams of data.
- Access points get configuration from designated controller.
- Wireless Controller has the ability to see all access points & coordinate them accordingly.
- Entire data process is going to be handled by the Wireless Access Points (AP) themselves.
- Real-time functions always stay in the AP and the management functions go to the WLC.



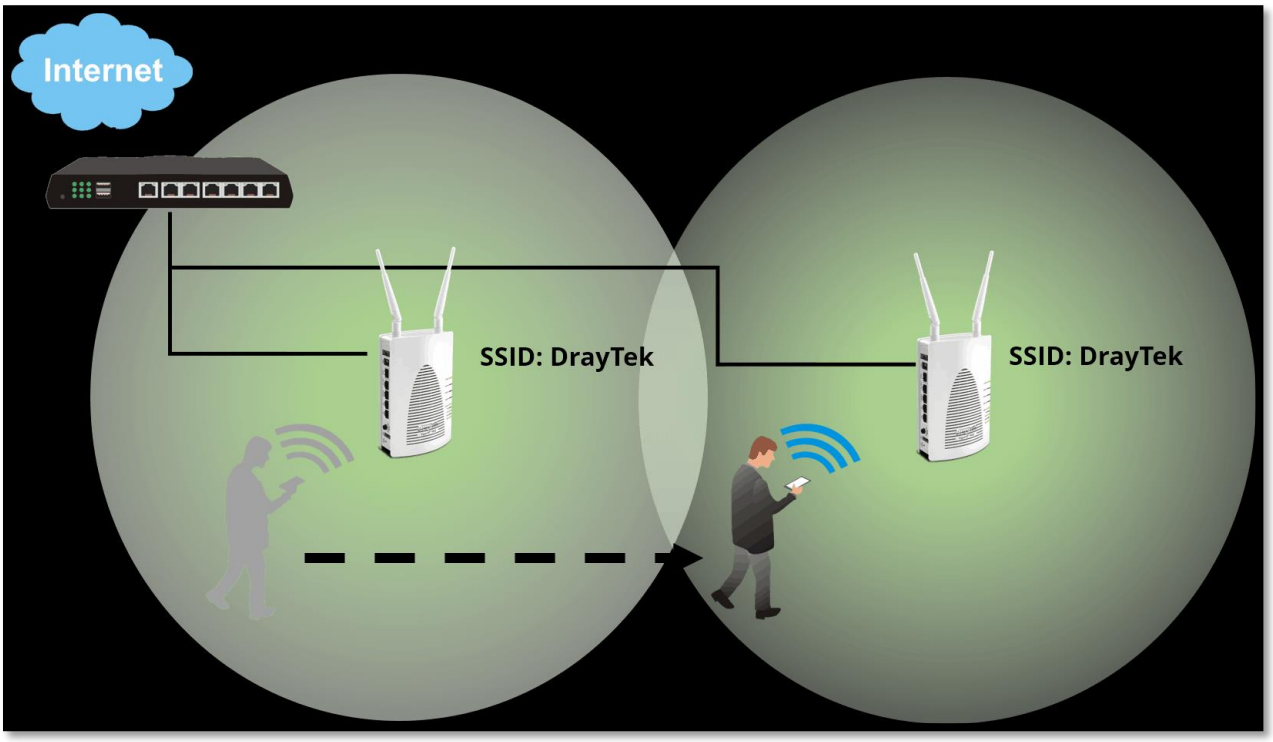
Converged Wireless Network Architecture:

- When we want a WLC to be closer to the APs and is more about a distributions functions.
- In that case, the Wireless LAN Controller (WLC) is move further down to the Access layer.
- In this Architecture the WLC function is moved closer to the LAPs and the wireless users.
- In this Architecture, the WLC function becomes distributed, rather than the centralized.
- The access layer turns out to be a convenient location for the Wireless LAN Controllers.
- With all types of user access merged into one layer called converged wireless network.
- In this architecture converged controllers are known as Wireless Control Modules (WCMs).
- One other advantage of the converged network architecture relates to wireless scalability.
- Connect Wireless LAN Controller and an Access Point both to the same access Layer switch.
- Now LAPs are reaching the Wireless LAN Controller through the Access/Distribution switch.
- This leads to a shorter distance CAPWAP, hence faster Wi-Fi and less delay for connectivity.



ROAMING OVERVIEW:

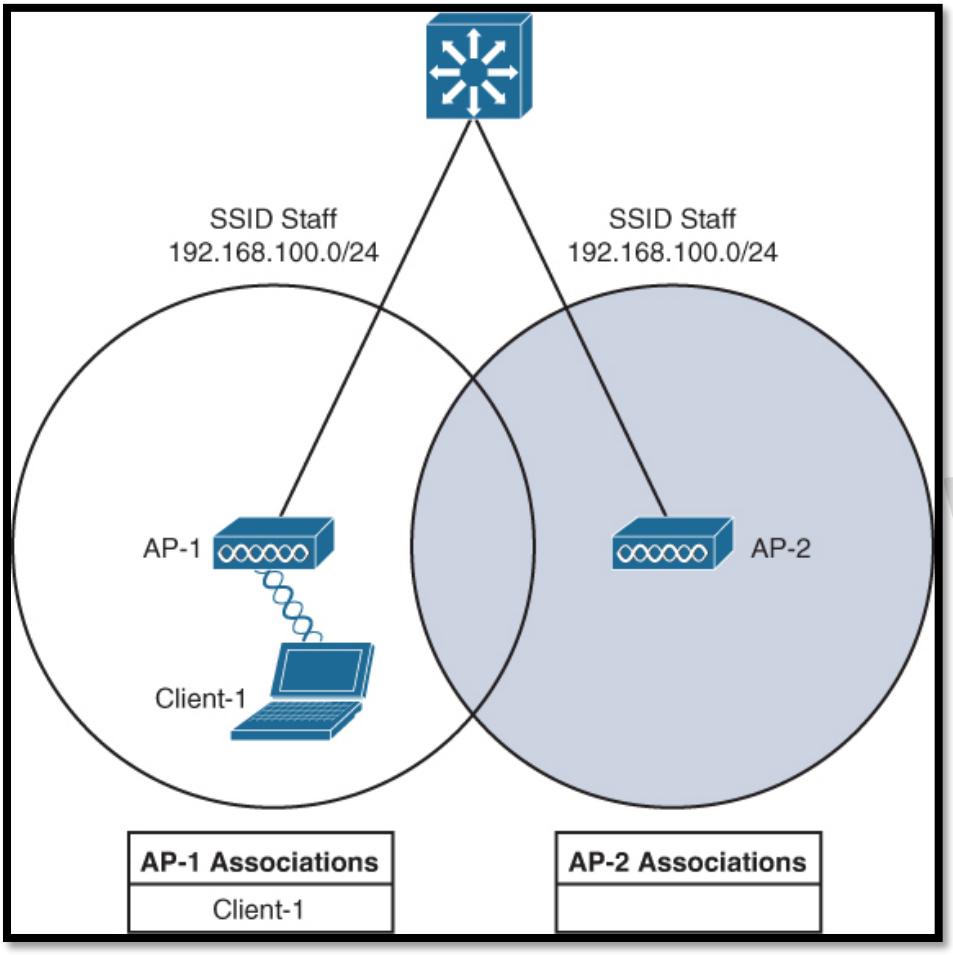
- Wireless roaming is when a wireless client (station) moves around in an area with multiple access point (AP), it may automatically switch to another AP which has better signal strength.



Roaming Between Autonomous Aps:

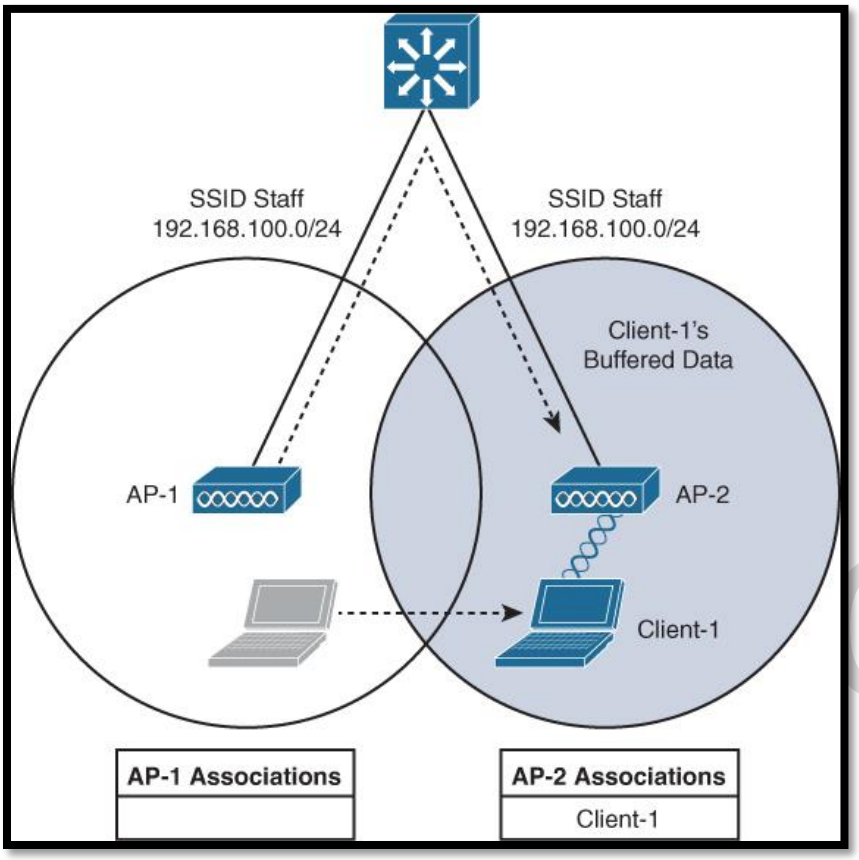
- As we know that a wireless client must associate and authenticate with an AP before it can use the AP's BSS to access the network.
- A client can also move from one BSS to another by roaming between APs.
- A client continuously evaluates the quality of its wireless connection, whether it is moving around or not.
- If the signal quality degrades, perhaps as the client moves away from the AP, the client will begin looking for a different AP that can offer a better signal.
- The process is usually quick and simple; the client actively scans channels and sends probe requests to discover candidate APs, and then the client selects one and tries to reassociate with it.
- A client can send Association Request and Reassociation Request frames to an AP when it wants to join the BSS.
- Association Requests are used to form a new association, while Reassociation Requests are used to roam from one AP to another, preserving the client's original association status.

- shows a simple scenario with two APs and one client.
- The client begins with an association to AP 1.
- Because the APs are running in autonomous mode, each one maintains a table of its associated clients.
- AP 1 has one client; AP 2 has none.

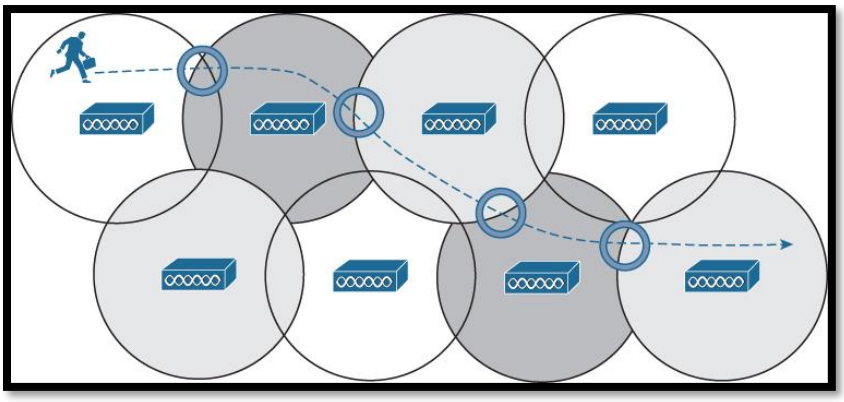


- Suppose that the client then begins to move into AP 2's cell.
- Somewhere near the cell boundary, the client decides that the signal from AP 1 has degraded and it should look elsewhere for a stronger signal.
- The client decides to roam and reassociate with AP 2.
- Notice that both APs have updated their list of associated clients to reflect Client 1's move from AP 1 to AP 2.

- If AP 1 still has any leftover wireless frames destined for the client after the roam, it forwards them to AP 2 over the wired infrastructure—simply because that is where the client's MAC address now resides.

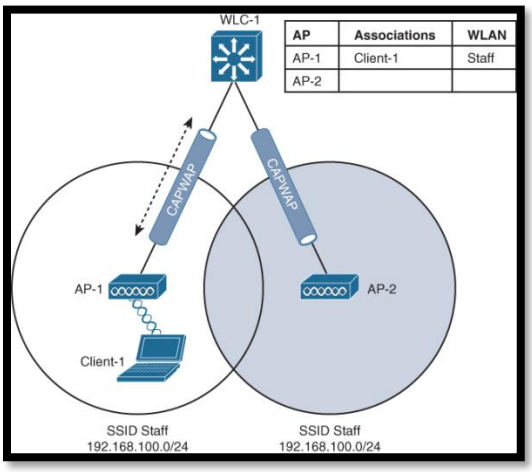


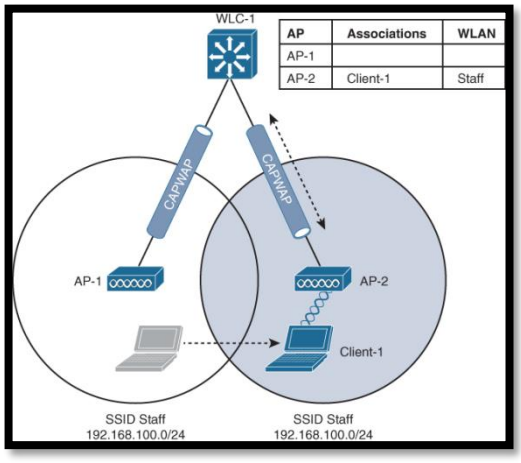
- Naturally, roaming is not limited to only two APs; instead, it occurs between any two APs as the client moves between them, at any given time.
- To cover a large area, you will probably install many APs in a pattern such that their cells overlap.
- When a wireless client begins to move, it might move along an arbitrary path.
- Each time the client decides that the signal from one AP has degraded enough, it attempts to roam to a new, better signal belonging to a different AP and cell.



Intracontroller Roaming

- In a Cisco wireless network, lightweight APs are bound to a wireless LAN controller through CAPWAP tunnels.
- The roaming process is similar to that of autonomous APs; clients must still reassociate to new APs as they move about.
- The only real difference is that the controller handles the roaming process, rather than the APs, because of the split-MAC architecture.
- Client 1 is associated to AP-1, which has a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel to controller WLC
- The controller maintains a client database that contains detailed information about how to reach and support each client.
- The actual database also contains client MAC and IP addresses, quality of service (QoS) parameters, and other information.



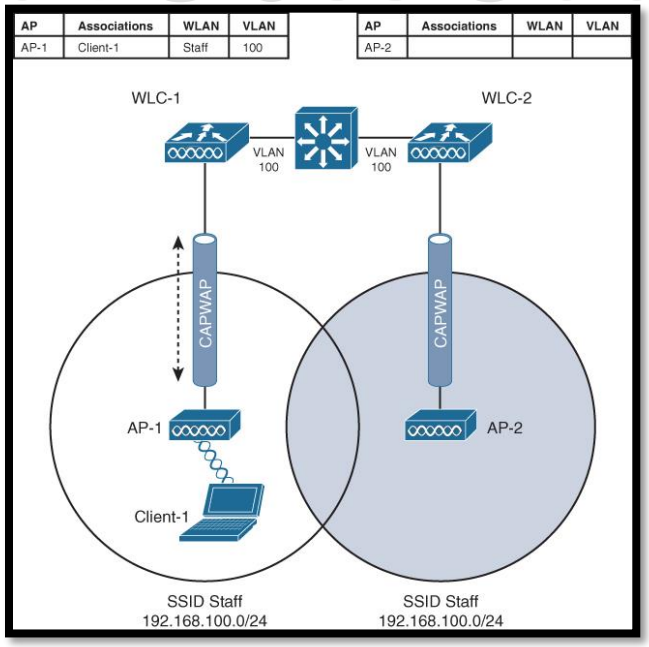


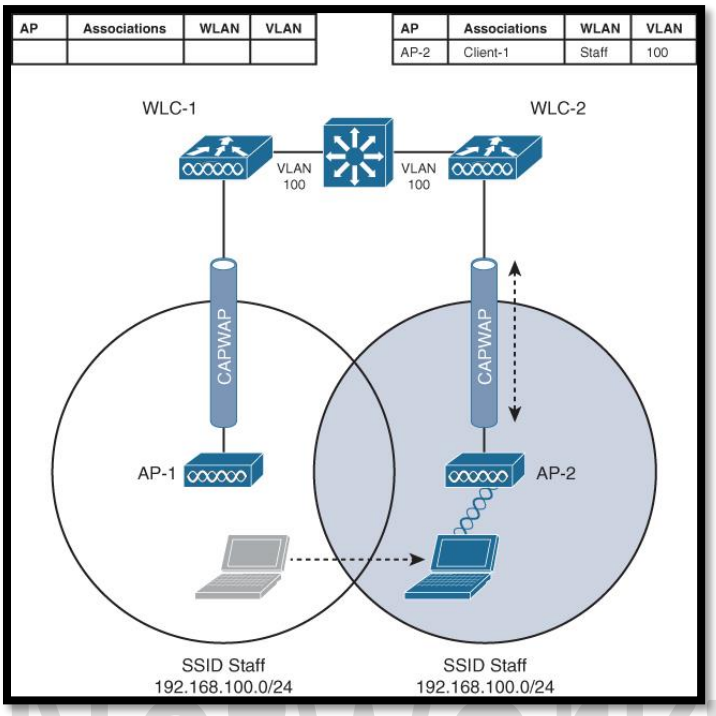
ROAMING BETWEEN CENTRALIZED CONTROLLERS:

- As a wireless network grows, one controller might not suffice.
- When two or more controllers support the APs in an enterprise, the APs can be distributed across them.
- As always, when clients become mobile, they roam from one AP to another—except they could also be roaming from one controller to another, depending on how neighboring APs are assigned to the controllers.
- As a network grows, AP roaming can scale too by organizing controllers into mobility groups.

Layer 2 Roaming:

- When a client roams from one AP to another and those APs lie on two different controllers, the client makes an intercontroller roam.
- Controller WLC 1 has one association in its database—that of Client 1 on AP 1.
- When the client decides to roam and reassociate itself with AP 2,it actually moves from one controller to another, and the two controllers must coordinate the move. One subtle detail involves the client's IP address.
- Before the roam, Client 1 is associated with AP 1 and takes an IP address from the VLAN and subnet that are configured on the WLAN supplied by controller WLC 1.
- In Figure WLAN Staff is bound to VLAN 100, so the client uses an address from the 192.168.100.0/24 subnet.





- When the client roams to a different AP, it can try to continue using its existing IP address or work with a DHCP server to either renew or request an address.
- Figure shows the client roaming to AP 2, where WLAN Staff is also bound to the same VLAN 100 and 192.168.100.0/24 subnet.
- Because the client has roamed between APs but stayed on the same VLAN and subnet, it has made a Layer 2 intercontroller roam.
- Layer 2 roams (commonly called local-to-local roams) are nice for two reasons: The client can keep its same IP address, and the roam is fast (usually less than 20 ms).

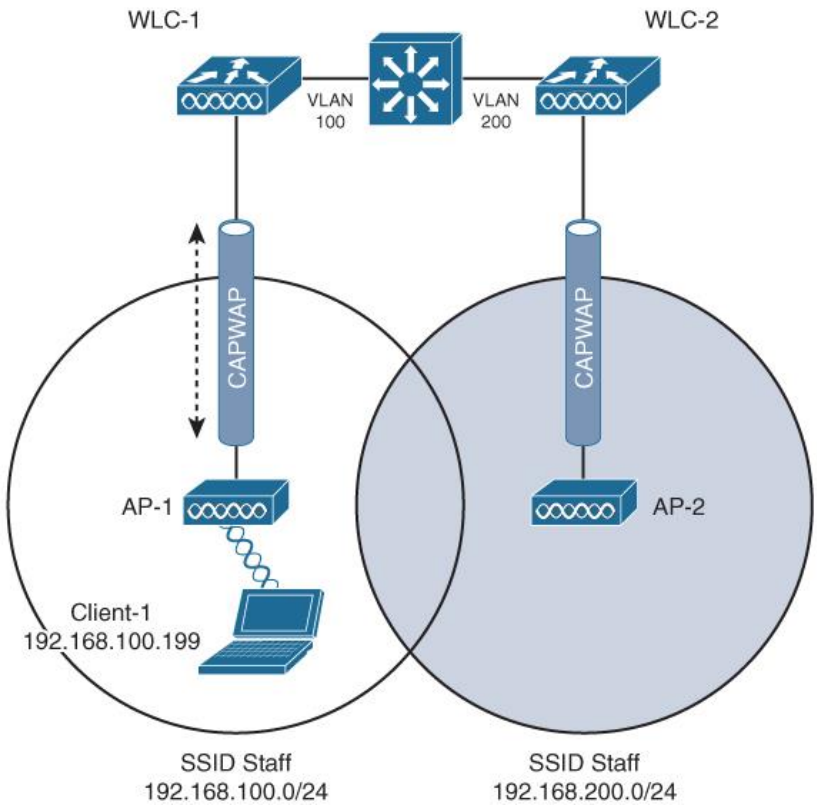
Layer 3 Roaming:

- What if a wireless network grows even more, such that the WLAN interfaces on each controller are assigned to different VLANs and subnets? Breaking a very large WLAN up into individual subnets seems like a good idea from a scalability viewpoint.
- However, when a wireless client roams from one controller to another, it could easily end up on a different subnet from the original one.
- Clients will not usually be able to detect that they have changed subnets.

- They will be aware of the AP roam but little else. Only clients that aggressively contact a DHCP server after each and every roam will continue to work properly. But to make roaming seamless and efficient, time consuming processes such as DHCP should be avoided.
- No worries—the Cisco wireless network has a clever trick up its sleeve.
- When a client initiates an intercontroller roam, the two controllers involved can compare the VLAN numbers that are assigned to their respective WLAN interfaces.
- If the VLAN IDs are the same, nothing special needs to happen; the client undergoes a Layer 2 intercontroller roam and can continue to use its original IP address on the new controller. If the two VLAN IDs differ, the controllers arrange a Layer 3 roam (also known as a local-to-foreign roam) that will allow the client to keep using its IP address.
- Figure illustrates a simple wireless network containing two APs and two controllers. Notice that the two APs offer different IP subnets in their BSSs: 192.168.100.0/24 and 192.168.200.0/24. The client is associated with AP-1 and is using IP address 192.168.100.199. On the surface, it looks like the client will roam into subnet 192.168.200.0/24 if it wanders into AP 2's cell and will lose connectivity if it tries to keep using its same IP address.

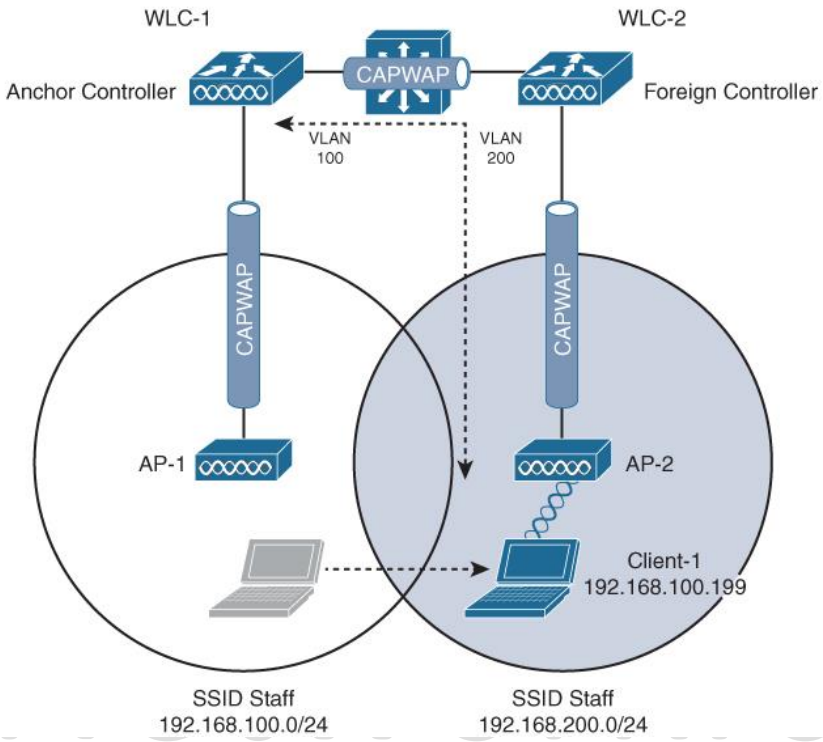
AP	Associations	WLAN	VLAN
AP-1	Client-1	Staff	100

AP	Associations	WLAN	VLAN
AP-2			



AP	Associations	WLAN	VLAN
WLC-2	Client-1 (Mobile)	Staff	100

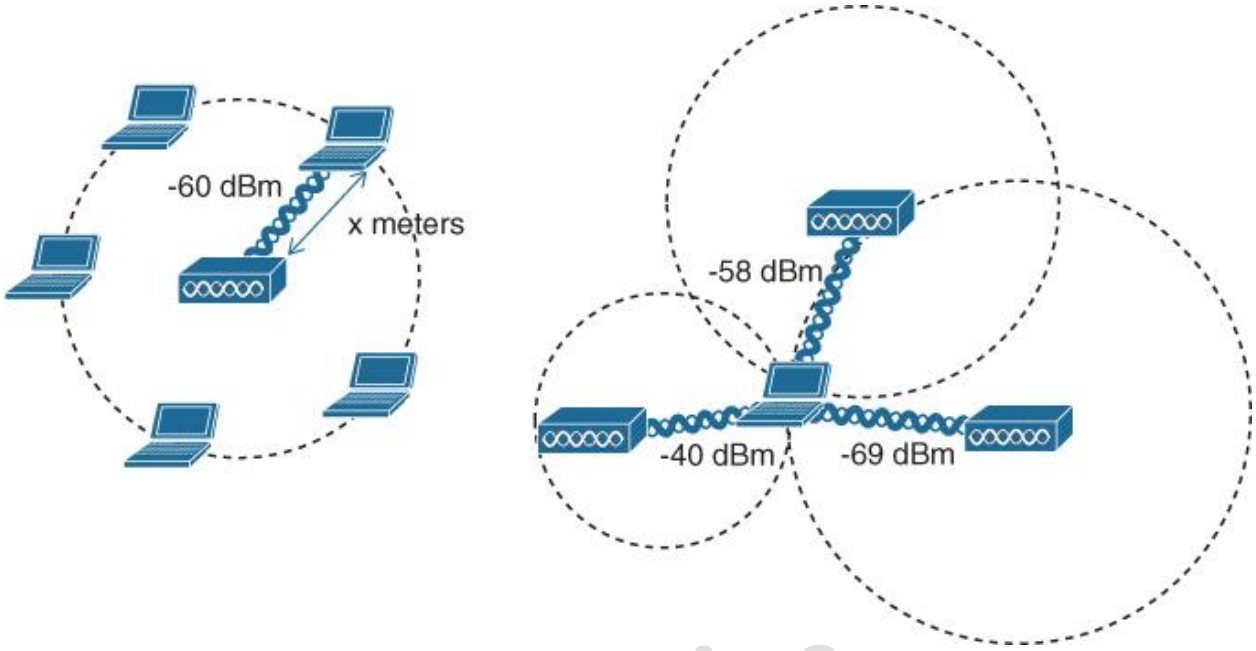
AP	Associations	WLAN	VLAN
AP-2	Client-1	Staff	



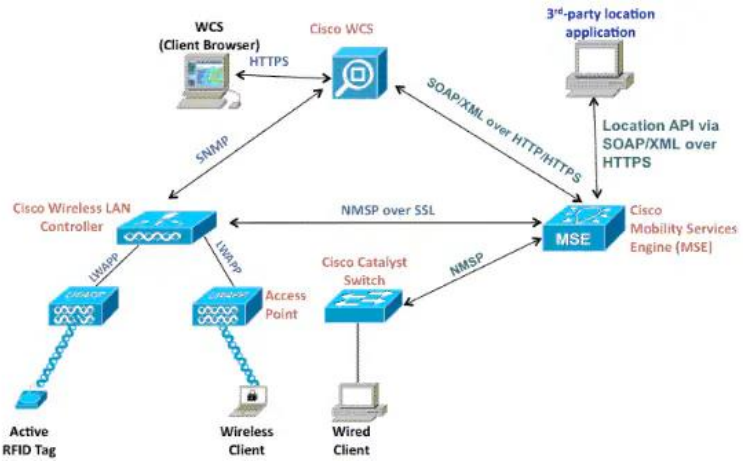
- A Layer 3 intercontroller roam consists of an extra tunnel that is built between the client's original controller and the controller it has roamed to.
- The tunnel carries data to and from the client as if it is still associated with the original controller and IP subnet. Figure shows the results of a Layer 3 roam.
- The original controller (WLC 1) is called the anchor controller, and the controller with the roamed client is called the foreign controller.
- Think of the client being anchored to the original controller no matter where it roams later. When the client roams away from its anchor, it moves into foreign territory.
- As we know Cisco controllers use CAPWAP tunnels to connect with lightweight APs. CAPWAP tunnels are also built between controllers for Layer 3 roaming.
- The tunnel tethers the client to its original anchor controller (and original IP subnet), regardless of its location or how many controllers it roams through.
- Anchor and foreign controllers are normally determined automatically.
- When a client first associates with an AP and a controller, that controller becomes its anchor controller.
- When the client roams to a different controller, that controller can take on the foreign role.

LOCATING DEVICES IN A WIRELESS NETWORK:

- Wireless networks are usually designed to provide coverage and connectivity in all areas where client devices are expected to be located.
- For example, a hospital building will likely have seamless wireless coverage on all floors and in all areas where users might go. Usually a user's exact location is irrelevant, as long as wireless coverage exists there. Locating a user or device is important in several use cases, and a wireless network can be leveraged to provide that information.
- For instance, a large store might be interested in tracking potential customers as they walk around and shop.
- The store might like to offer online advertising as customers enter various areas or walk near certain product displays.
- The same could be true of a museum that wants to present relevant online content as people move to each exhibit.
- A healthcare enterprise might want to track critical (and valuable) medical devices or patients as they move about the facility so that they can be quickly located.
- By tracking user locations, a large venue can provide way-finding information on mobile devices to help people navigate through buildings.
- Recall that before each wireless client can use the network, it must first be authenticated and associated by an AP.
- At the most basic level, a client can then be located according to the AP to which it is currently joined.
- That may not be granular enough for every use case because one AP might cover a large area.
- In addition, a client device might not roam very aggressively, so it could well stay associated with one AP that is now far away, even though another AP with a better signal is very near.
- To locate a device more accurately, an AP can use the **received signal strength (RSS)** of a client device as a measure of the distance between the two.
- Free space path loss causes an RF signal to be attenuated or diminished exponentially as a function of its frequency and the distance it travels.
- That means a client's distance from an AP can be computed from its received signal strength.
- If the distance is measured from a single AP only, it is difficult to determine where the client is situated in relation to the AP.
- In the case of an indoor AP with an omnidirectional antenna, the client could be located anywhere along a circular path of fixed distance because the received signal strength would be fairly consistent at all points on the circle.
- A better solution is to obtain the same measurement from three or more APs, then correlate the results and determine where they intersect.
- Figure illustrates the difference in determining a client's location with a single and multiple APs.

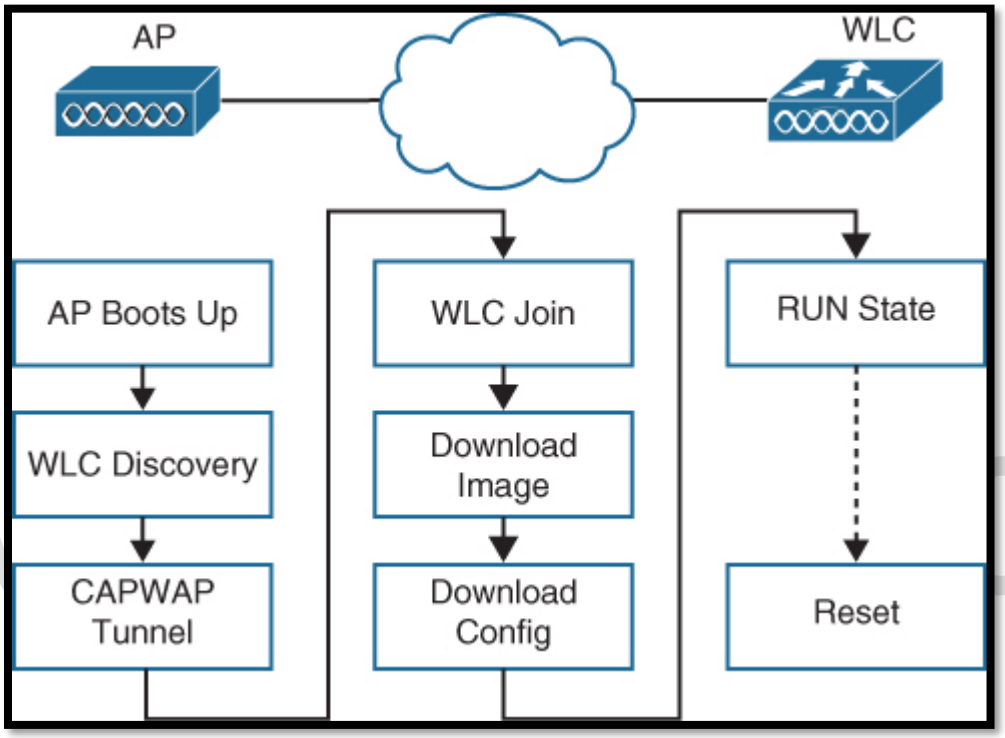


- The components of a wireless network can be coupled with additional resources to provide **real-time location services (RTLS).**
- Cisco APs and WLCs can integrate with management platforms **like Cisco Prime Infrastructure or DNA Center, along with location servers like Cisco Mobility Services Engine** (MSE), Cisco Connected Mobile Experiences (CMX), or Cisco DNA Spaces to gather location information in real time and present that information in a relevant way.
- The **Cisco MSE (Mobility Service Engine)** provides Context Aware Services (CAS) Ability to track the physical location of Network Devices, both wired and wireless, using wireless LAN controllers (WLCs) and Cisco Aironet Lightweight Access Points (LAPs)



AP States:

- From the time it powers up until it offers a fully functional basic service set (BSS), a lightweight AP operates in a variety of states.
- The AP enters the states in a specific order; the sequence of states is called a state machine.
- The sequence of the most common states, as shown in Figure is as follows:



1. AP boots: Once an AP receives power, it boots on a small IOS image so that it can work through the remaining states and communicate over its network connection. The AP must also receive an IP address from either a Dynamic Host Configuration Protocol (DHCP) server or a static configuration so that it can communicate over the network.

2. WLC discovery: The AP goes through a series of steps to find one or more controllers that it might join.

3. CAPWAP tunnel: The AP attempts to build a CAPWAP tunnel with one or more controllers. The tunnel will provide a secure Datagram Transport Layer Security (DTLS) channel for subsequent AP-WLC control messages. The AP and WLC authenticate each other through an exchange of digital certificates.

4. WLC join: The AP selects a WLC from a list of candidates and then sends a CAPWAP Join Request message to it. The WLC replies with a CAPWAP Join Response message.

5. Download image: The WLC informs the AP of its software release. If the AP's own software is a different release, the AP downloads a matching image from the controller, reboots to apply the new image, and then returns to step1 If the two are running identical releases, no download is needed.

6. Download config: The AP pulls configuration parameters down from the WLC and can update existing values with those sent from the controller. Settings include RF, service set identifier (SSID), security, and quality of service (QoS) parameters.

7. Run state: Once the AP is fully initialized, the WLC places it in the "run" state. The AP and WLC then begin providing a BSS and begin accepting wireless clients.

8. Reset: If an AP is reset by the WLC, it tears down existing client associations and any CAPWAP tunnels to WLCs. The AP then reboots and starts through the entire state machine again.

Wireless segmentation:

Wireless segmentation is the process of dividing a wireless network into smaller, more manageable segments. This can be done by using **groups, profiles, and tags**.

- Groups are collections of access points (APs) that are managed together. APs can be grouped based on their location, function, or other criteria.
- Profiles are sets of configuration settings that are applied to APs in a group. Profiles can be used to control things like the VLAN, security settings, and RF settings for the APs in a group.
- Tags are labels that can be attached to APs, groups, or profiles. Tags can be used to track and manage wireless devices.

By using groups, profiles, and tags, you can create a wireless network that is segmented into smaller, more manageable segments. This can help you to improve security, performance, and manageability of your wireless network.

Here are some of the benefits of using wireless segmentation with groups, profiles, and tags:

Improved security: Segmentation can help to improve security by isolating different types of traffic. For example, you could create a separate segment for guest users that has different security settings than the segment for your employees.

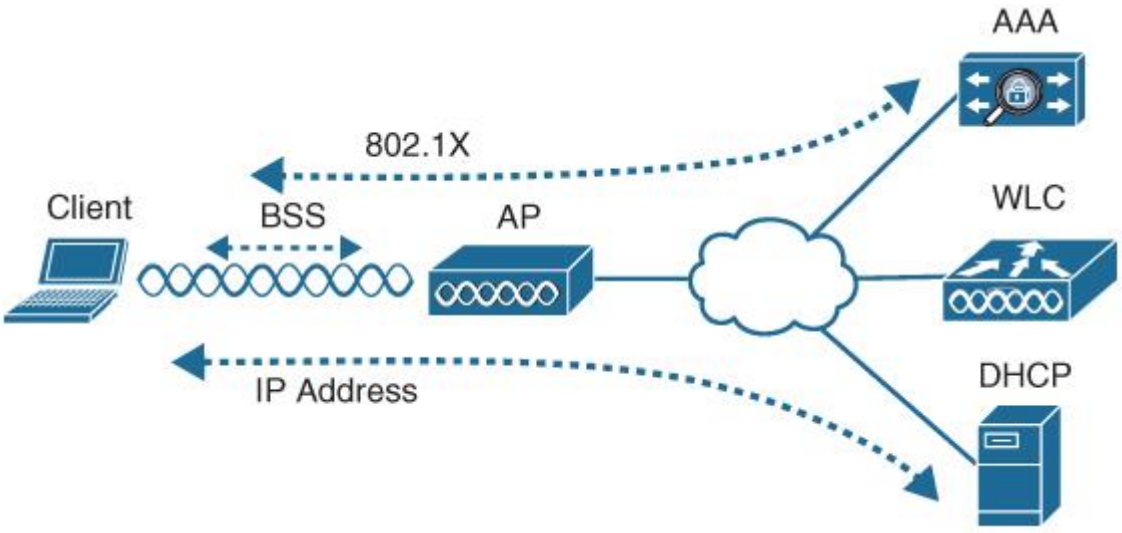
Improved performance: Segmentation can help to improve performance by reducing the amount of traffic on each segment. This is because traffic is only routed between the APs in the same segment.

Improved manageability: Segmentation can help to improve manageability by making it easier to track and manage wireless devices. For example, you could tag all of the APs in a specific location with the same tag. This would make it easy to find and manage all of the APs in that location.

If you are looking for a way to improve the security, performance, and manageability of your wireless network, then you should consider using wireless segmentation with groups, profiles, and tags.

Troubleshoot WLAN:

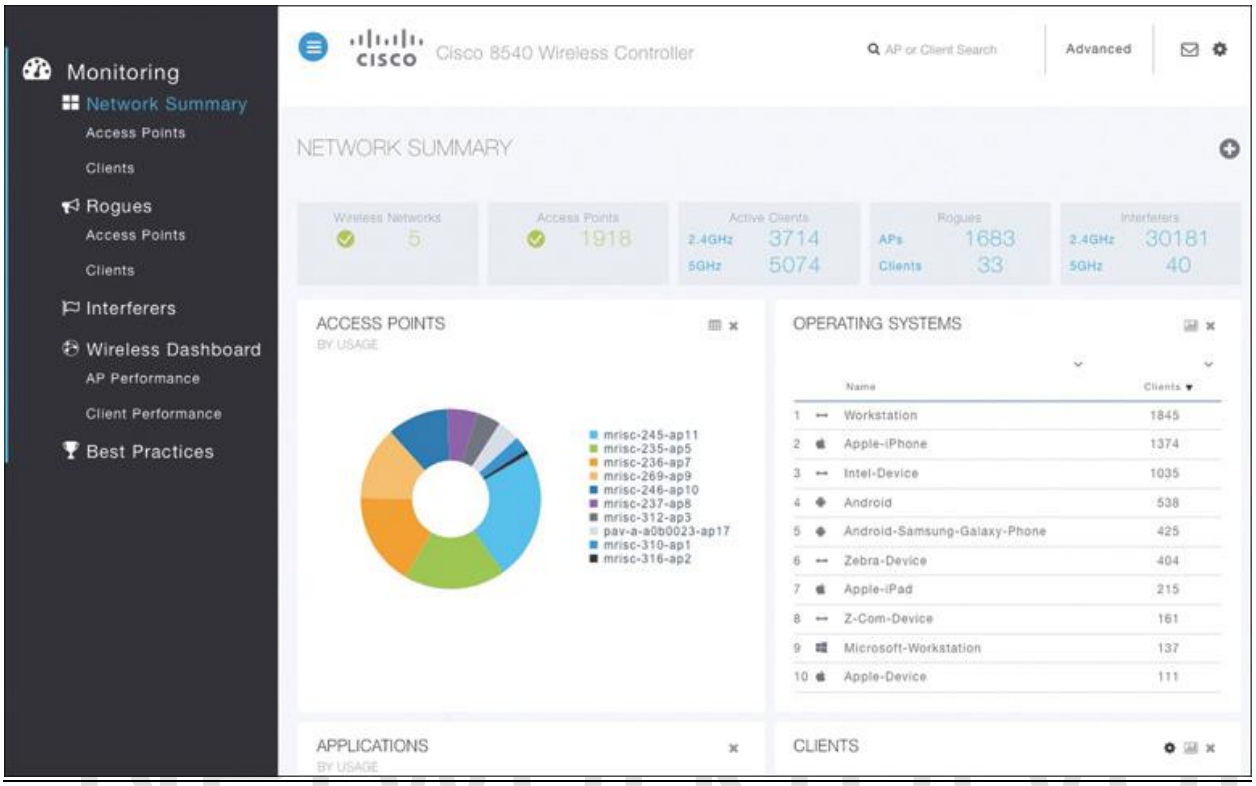
- When one or more network users report that they are having problems, your first course of action should be to gather more information.
- Begin with a broad perspective and then ask pointed questions to narrow the scope of possible causes. You do not want to panic or waste time chasing irrelevant things. Instead, ask questions and try to notice patterns or similarities in the answers you receive.
- For example, if you get reports from many people in the same area, perhaps an **AP is misconfigured or malfunctioning**. Reports from many areas or from single service set identifier (SSID) may indicate problems with a controller configuration.
- However, if you receive a report of only one wireless user having problems, it might not make sense to spend time troubleshooting a controller, where many users are supported. Instead, you should focus on that one user's client device and its interaction with an AP.
- As you prepare to troubleshoot a single wireless client, think about all the things a client needs to join and use the network. Below figure illustrates the following conditions that must be met for a successful association:
- **The client is within RF range of an AP and asks to associate.**
- **The client authenticates.**
- **The client requests and receives an IP address.**

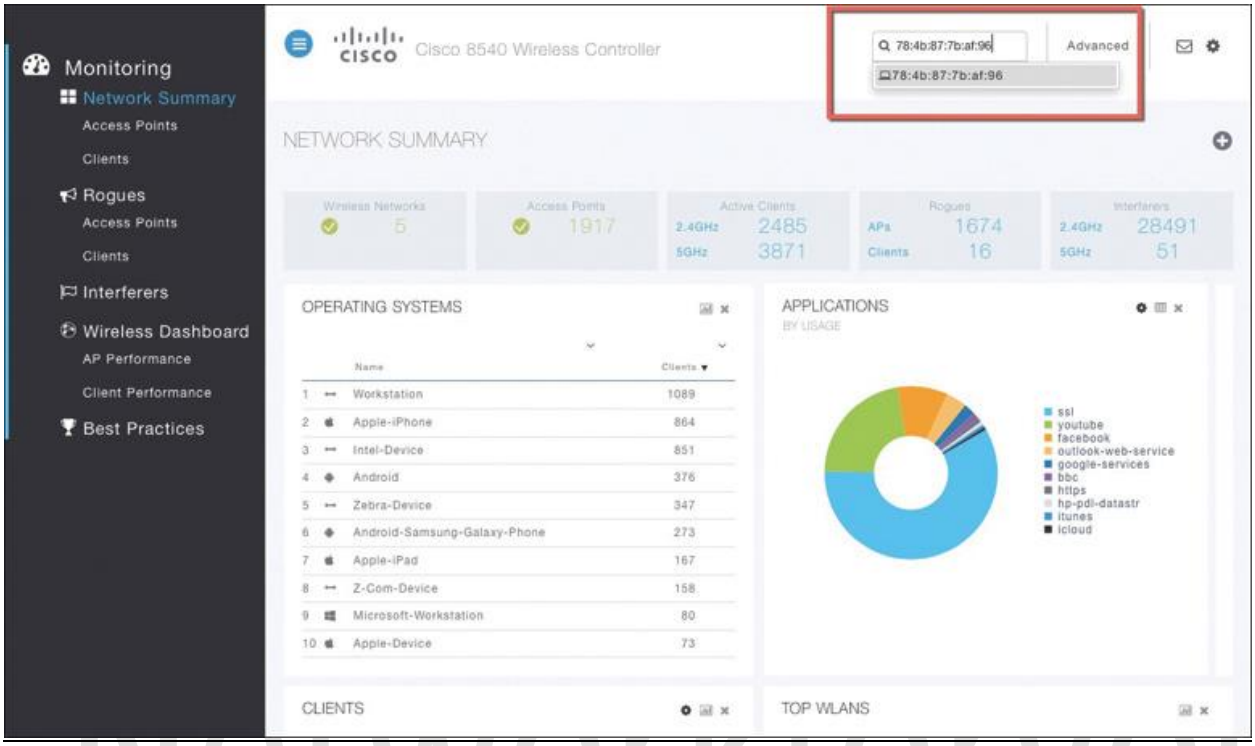


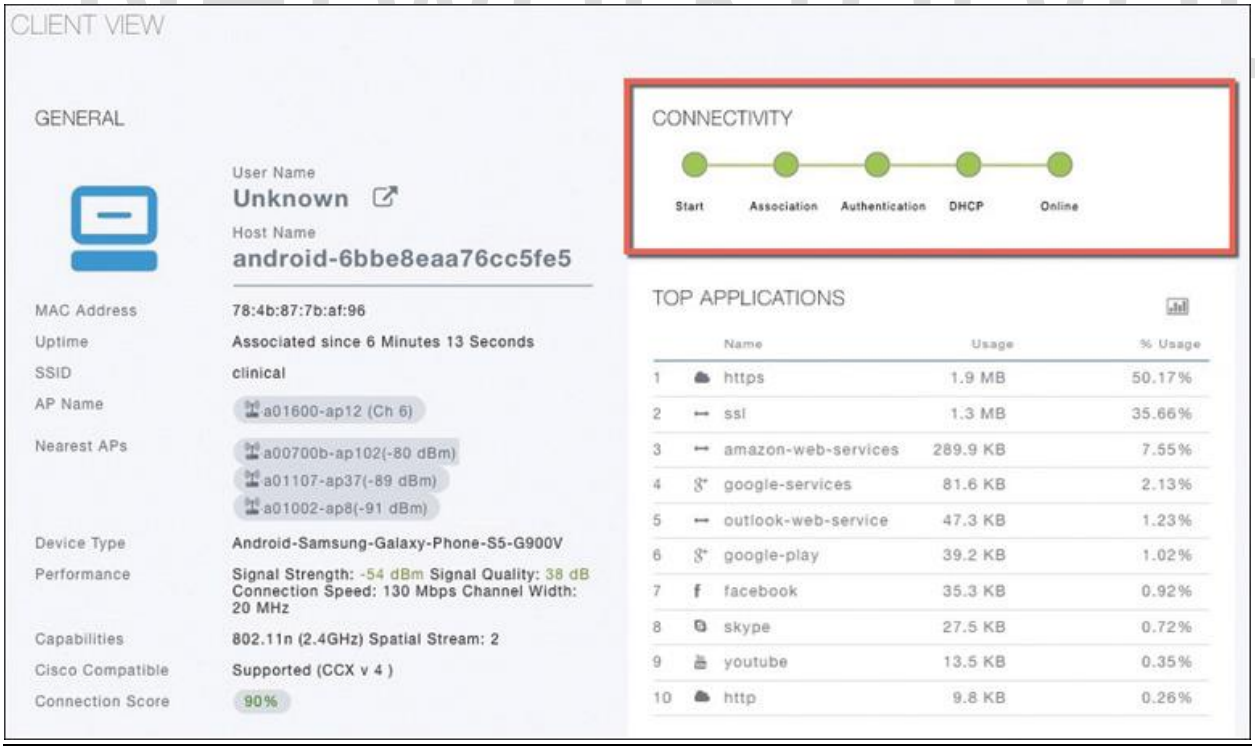
- Try to gather information from the end user to see what the client is experiencing. “I cannot connect” or “The Wi-Fi is down” might actually mean that the user’s device cannot associate, cannot get an IP address, or cannot authenticate.
- A closer inspection of the device might reveal more clues.
- Therefore, at a minimum, you need the wireless adapter MAC address from the client device, as well as its physical location.
- The end user might try to tell you about a specific AP that is in the room or within view. Record that information, too, but remember that the client device selects which AP it wants to use—not the human user. The device may well be using a completely different AP.

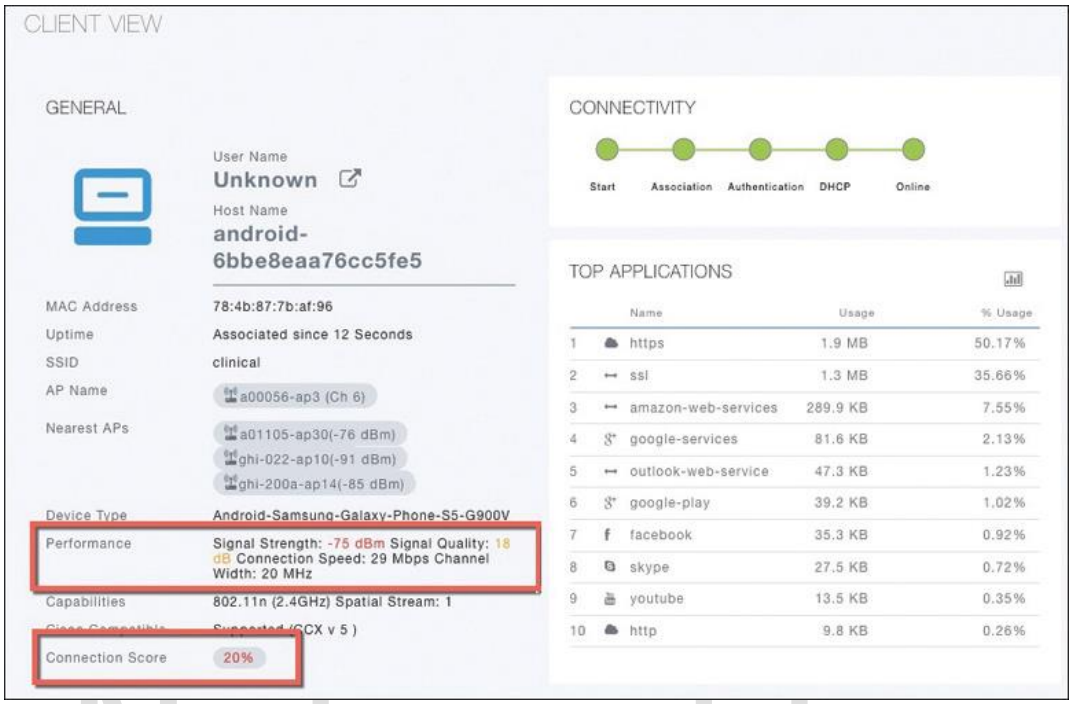
TROUBLESHOOTING CLIENT CONNECTIVITY FROM THE WLC:

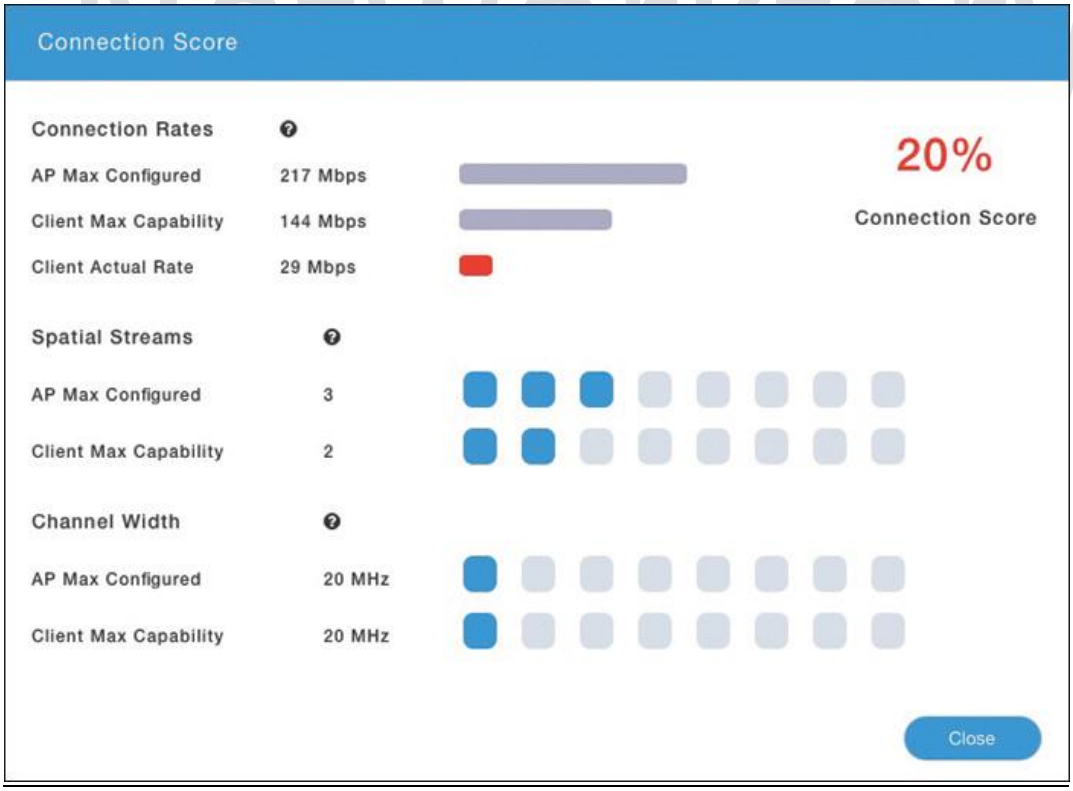
- Most of your time managing and monitoring a wireless network will be spent in the wireless LAN controller GUI.
- As a wireless client probes and attempts to associate with an AP, it is essentially communicating with the controller.
- You can access a wealth of troubleshooting information from the controller, as long as you know the **client’s MAC address.**
- Cisco WLCs have **two main GUI presentations**—**one for monitoring and one for more advanced configuration and monitoring.**
- When you open a browser to the WLC management address, you see the default screen that is shown in below figure.
- The default screen displays network summary dashboard information on the right portion and monitoring tools in the list on the left.

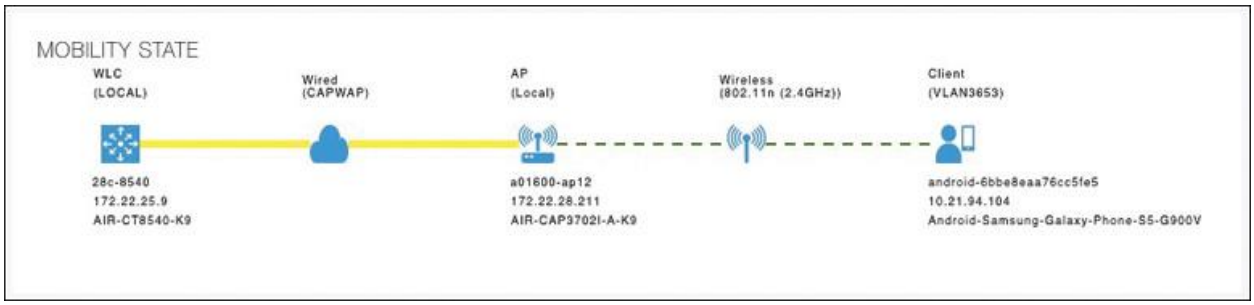



Monitoring
Network Summary
Access Points
Clients
Rogues
Access Points
Clients
Interferers
Wireless Dashboard
AP Performance
Client Performance
Best Practices
Cisco 8540 Wireless Controller
78:4b:87:7b:af:96
Advanced
78:4b:87:7b:af:96
NETWORK SUMMARY
Wireless Networks 5
Access Points 1917
Active Clients 2.4GHz 2485 5GHz 3871
Rogues APs 1674 Clients 16
Interferers 2.4GHz 28491 5GHz 51
OPERATING SYSTEMS
Name Clients
1 Workstation 1089
2 Apple-iPhone 864
3 Intel-Device 851
4 Android 376
5 Zebra-Device 347
6 Android-Samsung-Galaxy-Phone 273
7 Apple-iPad 167
8 Z-Com-Device 158
9 Microsoft-Workstation 80
10 Apple-Device 73
APPLICATIONS
BY USAGE
ssl
youtube
facebook
outlook-web-service
google-services
bbc
https
hp-pdl-datastr
itunes
icloud
CLIENTS
TOP WLANS


CLIENT VIEW
GENERAL
User Name
Unknown
Host Name
android-6bbe8eaa76cc5fe5
MAC Address 78:4b:87:7b:af:96
Uptime Associated since 6 Minutes 13 Seconds
SSID clinical
AP Name a01600-ap12 (Ch 6)
Nearest APs a00700b-ap102(-80 dBm) a01107-ap37(-89 dBm) a01002-ap8(-91 dBm)
Device Type Android-Samsung-Galaxy-Phone-S5-G900V
Performance Signal Strength: -54 dBm Signal Quality: 38 dB Connection Speed: 130 Mbps Channel Width: 20 MHz
Capabilities 802.11n (2.4GHz) Spatial Stream: 2
Cisco Compatible Supported (CCX v 4)
Connection Score 90%
CONNECTIVITY
Start Association Authentication DHCP Online
TOP APPLICATIONS
Name Usage % Usage
1 https 1.9 MB 50.17%
2 ssl 1.3 MB 35.66%
3 amazon-web-services 289.9 KB 7.55%
4 google-services 81.6 KB 2.13%
5 outlook-web-service 47.3 KB 1.23%
6 google-play 39.2 KB 1.02%
7 facebook 35.3 KB 0.92%
8 skype 27.5 KB 0.72%
9 youtube 13.5 KB 0.35%
10 http 9.8 KB 0.26%





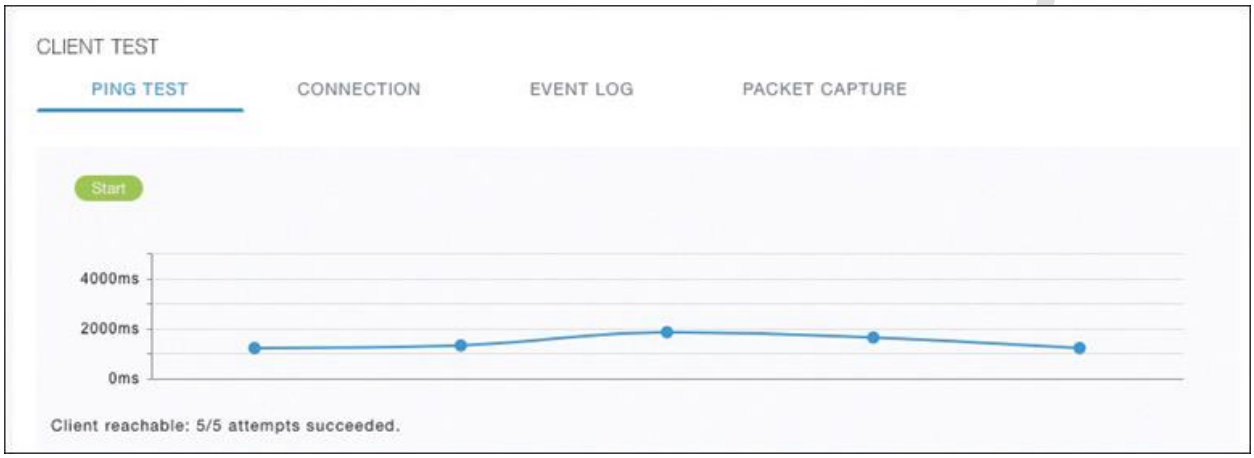


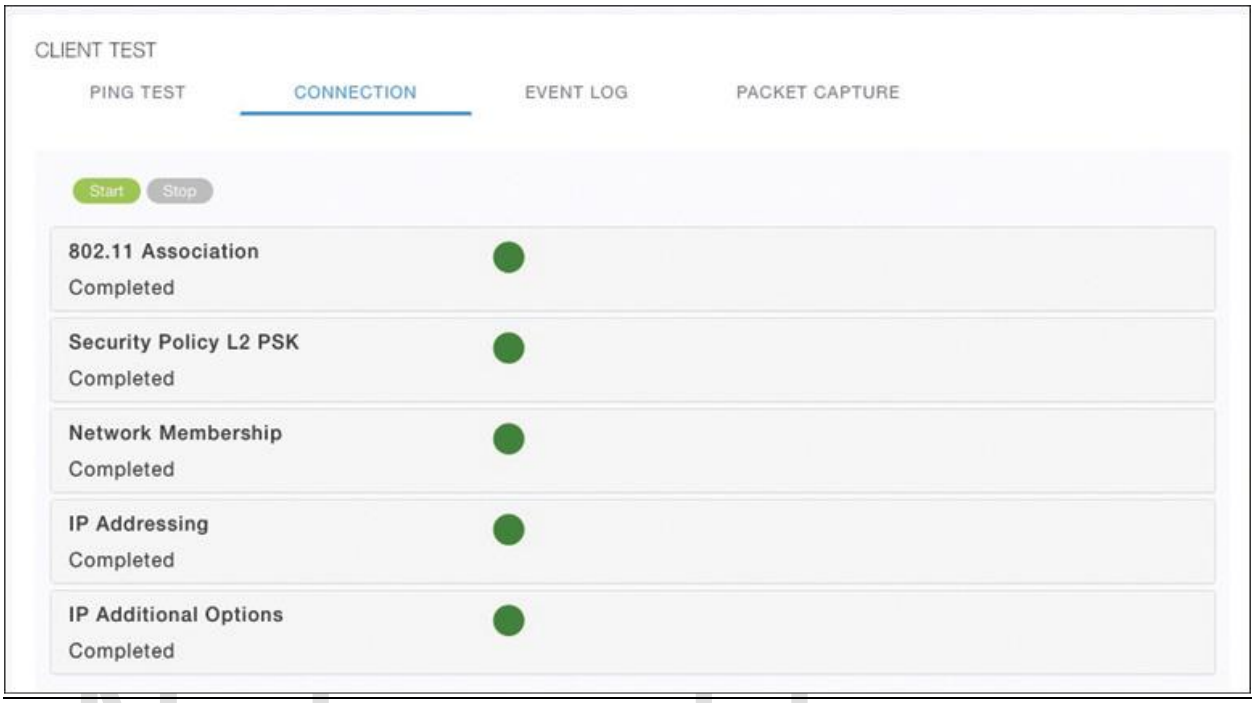
NETWORK & QOS

Description	Status
IP Address	10.21.94.104
IPv6 Address	Unknown
VLAN	3653
Source Group Tag	N/A
Fastlane Client	No
Mobility Role	No
WMM	Supported
U-APSD	Disabled
QoS Level	Silver

SECURITY & POLICY

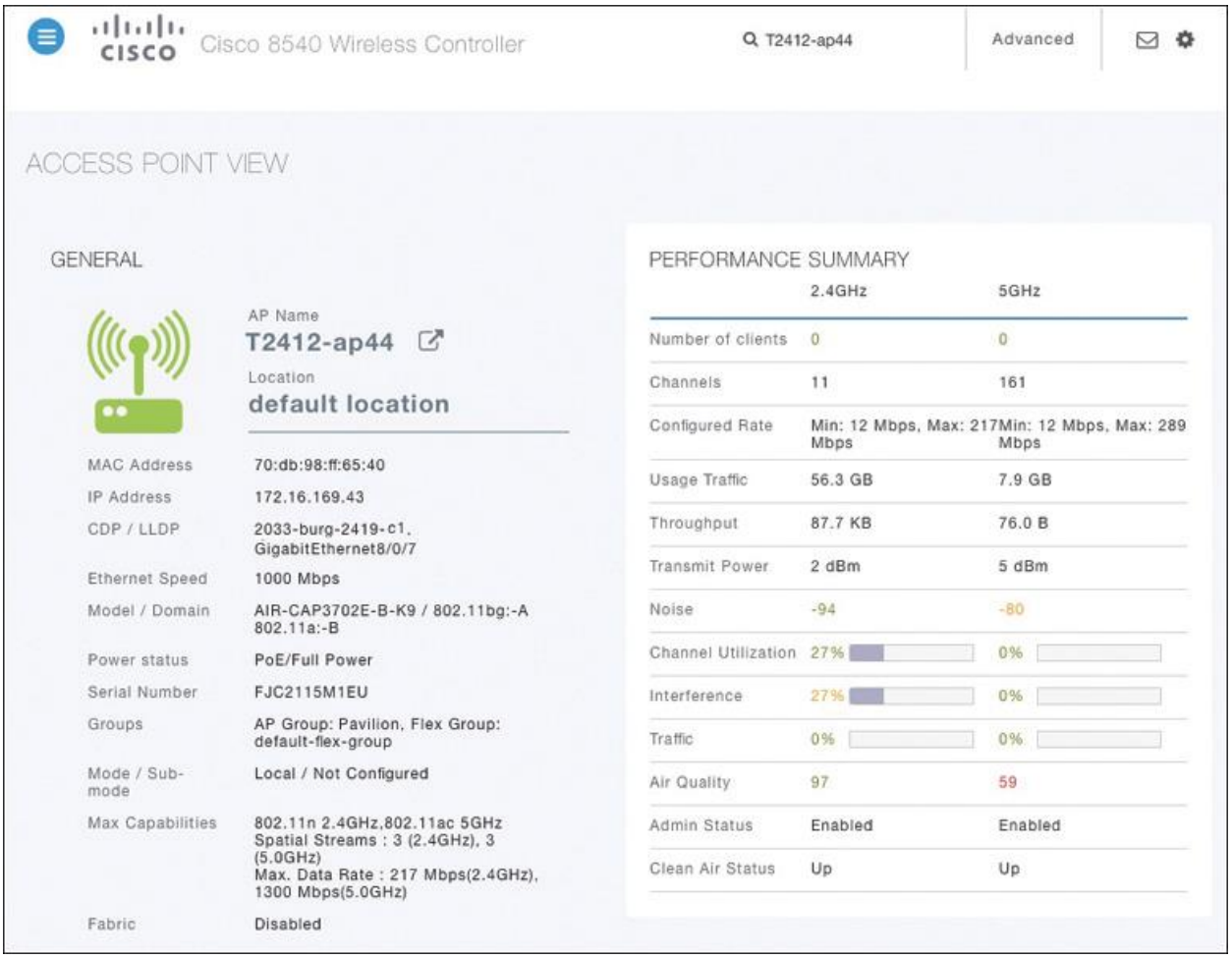
Description	Status
Policy	RSN (WPA2)
Cipher	CCMP (AES)
Key Management	PSK
EAP Type	N/A
ACL (IP/IPv6)	None/None
mDNS Profile	default-mdns-profile
AAA Role	None





TROUBLESHOOTING CONNECTIVITY PROBLEMS AT THE AP:

- In cases where you get reports from multiple users who are all having problems in the same general area, you might need to focus your efforts on an AP.
- The problem could be as simple as a defective radio, where no clients are receiving a signal. In that case, you might have to go onsite to confirm that the transmitter is not working correctly.
- Otherwise, the split-MAC architecture creates several different points where you can troubleshoot. Successfully operating the lightweight AP and providing a working BSS require the following:
- The AP must have connectivity to its access layer switch.
- The AP must have connectivity to its WLC, unless it is operating in FlexConnect mode.
- First, verify the connectivity between an AP and a controller. Usually you do this when a new AP is installed, to make sure it is able to discover and join a controller before clients arrive and try to use the wireless network. You can also do this at any time as a quick check of the AP's health.
- The easiest approach is to simply look for the AP in the list of live APs that have joined the controller. If you know which controller the AP should join, open a management session to it. Enter the AP's name in the search bar.
- If the search reveals a live AP that is joined to the controller, information is
- displayed in the Access Point View screen


Cisco 8540 Wireless Controller
T2412-ap44
Advanced
ACCESS POINT VIEW
GENERAL
AP Name
T2412-ap44
Location
default location
MAC Address 70:db:98:ff:65:40
IP Address 172.16.169.43
CDP / LLDP 2033-burg-2419-c1, GigabitEthernet8/0/7
Ethernet Speed 1000 Mbps
Model / Domain AIR-CAP3702E-B-K9 / 802.11bg:-A 802.11a:-B
Power status PoE/Full Power
Serial Number FJC2115M1EU
Groups AP Group: Pavilion, Flex Group: default-flex-group
Mode / Sub-mode Local / Not Configured
Max Capabilities 802.11n 2.4GHz,802.11ac 5GHz Spatial Streams : 3 (2.4GHz), 3 (5.0GHz) Max. Data Rate : 217 Mbps(2.4GHz), 1300 Mbps(5.0GHz)
Fabric Disabled
PERFORMANCE SUMMARY
2.4GHz 5GHz
Number of clients 0 0
Channels 11 161
Configured Rate Min: 12 Mbps, Max: 217 Mbps Min: 12 Mbps, Max: 289 Mbps
Usage Traffic 56.3 GB 7.9 GB
Throughput 87.7 KB 76.0 B
Transmit Power 2 dBm 5 dBm
Noise -94 -80
Channel Utilization 27% 0%
Interference 27% 0%
Traffic 0% 0%
Air Quality 97 59
Admin Status Enabled Enabled
Clean Air Status Up Up

PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	161
Configured Rate	Min: 12 Mbps, Max: 217 Mbps	Min: 12 Mbps, Max: 289 Mbps
Usage Traffic	56.3 GB	7.9 GB
Throughput	87.7 KB	76.0 B
Transmit Power	2 dBm	5 dBm
Noise	-94	-80
Channel Utilization	27%	0%
Interference	27%	0%
Traffic	0%	0%
Air Quality	97	59
Admin Status	Enabled	Enabled
Clean Air Status	Up	Up