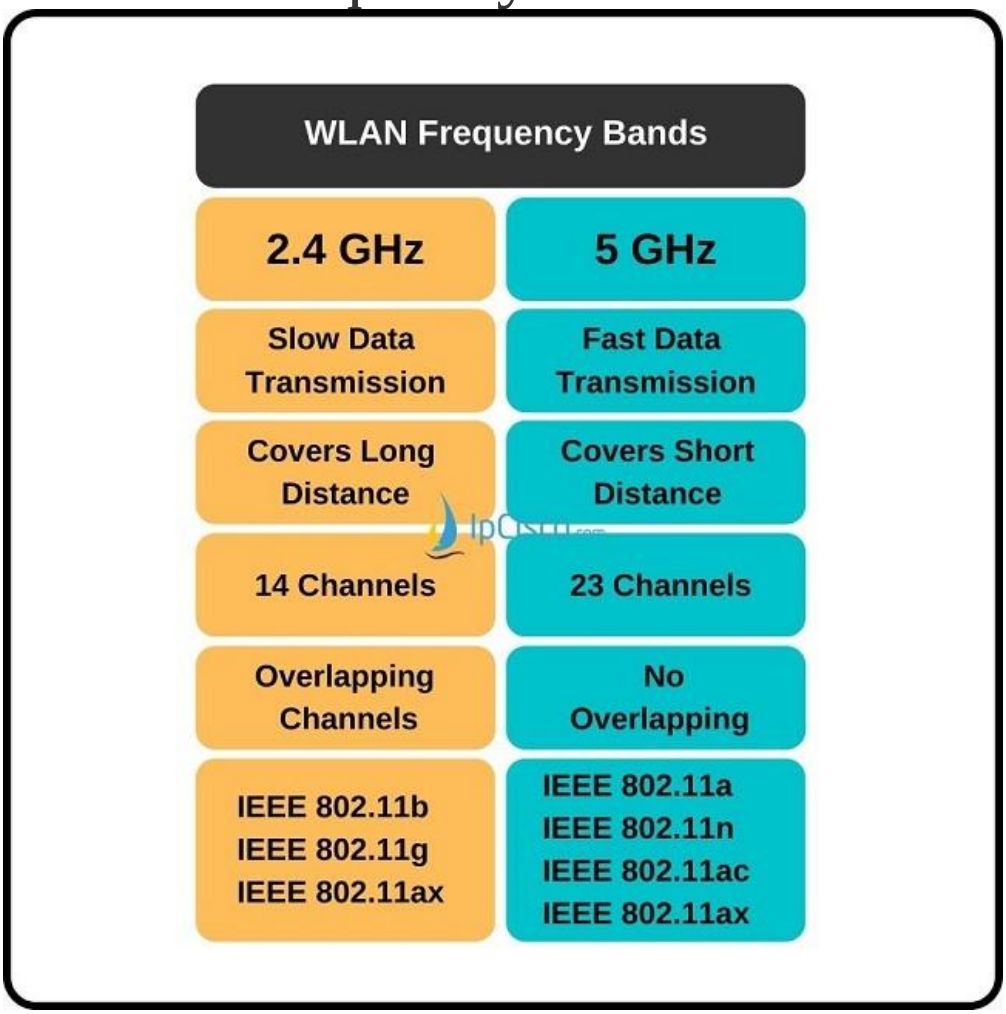
WLAN Frequency Bands



WLAN Frequency Bands are the **frequency ranges** used in **wireless communcation**. **Two frequncy bands** are used in wireless communication. These are **2.4GHz** and **5GHz** Bands. Here, we will talk about frequency, hertz terms, frequency bands and human hearing frequencies beside **WLAN Frequency Bands**. This lesson is also a new lessons in **CCNA 200-301**.

Table of Contents

Frequency, Hertz, Frequency Spectrum

Hertz(Hz) is the smalles unit used to measure **frequency**. It is the unit of **cyles per second**. Frequency is the definion for how often something happens. A frequency of 1 Hertz means that something happens once a second period.

On a **piano**, note **Middle C** is **261.65 (262) Hertz**. What is this means? This means that when you play this piono button once, every seconds **262 vibrations** occurs!

By the way, "**Hertz**" name is coming from German physicist **Heinrich Rudolf Hertz**.

There are other higher frequency units. All the frequency units are given below:

Unit	**Abreviation**	**Hertz**
Hertz	Hz	1 Hertzh
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1.000.000 Hz
Gigahertz	GHz	1.000.000.000 Hz

By the way human can hear a very low frequency bands if we compare with animals. Human can hear the sounds between **20 and 20.000 Hz**. While human can hear only this range;

Dolphins can hear **1000 Hz – 130.000 Hz**,

Bats can hear **3000 Hz – 120.000 Hz**

Rats can hear **200 Hz – 76.000 Hz**

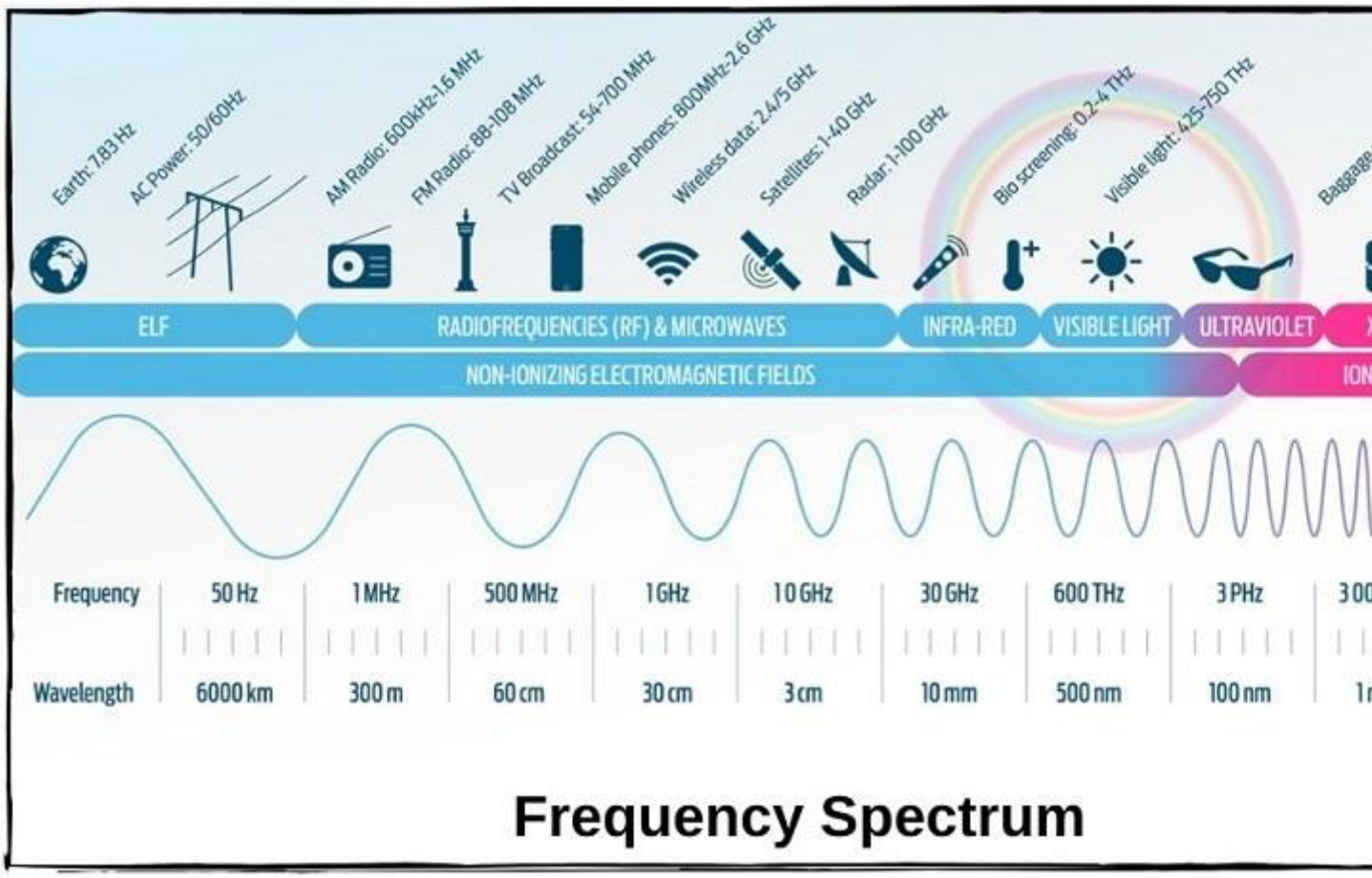
Dogs can hear **15 Hz – 50.000 Hz**

Cats can hear **60 Hz – 65.000 Hz**

And one of the biggest animals, **elephants** hears **16 Hz – 12.000 Hz**. Lower range than us althought their big ears.

There is a standard frequency range from **0 Hz** to **1000…00 Hz (22 zeros)**. The lower frequencies are too low to hear and the higher ones includes light, X ray, Gamma and cosmic rays.

You can find all these frequency ranges below:



The frequency range between **3 kHz** and **300 GHz** is called "**Radio Frequency (RF)**". Many different radio communication is done on this band. AM/FM radio, shortwave radio, tv,microwave,radar etc. Here, especially microwave band is important form us. Because it includes the frequency ranges, **2.4 GHz** and **5 GHz** used in Wireless Network Communication.

Wireless LAN Bands and Channels

There are **two wireless LAN bands** used in wireless LANs. These are **2.4 GHz** and **5 GHz** bands.

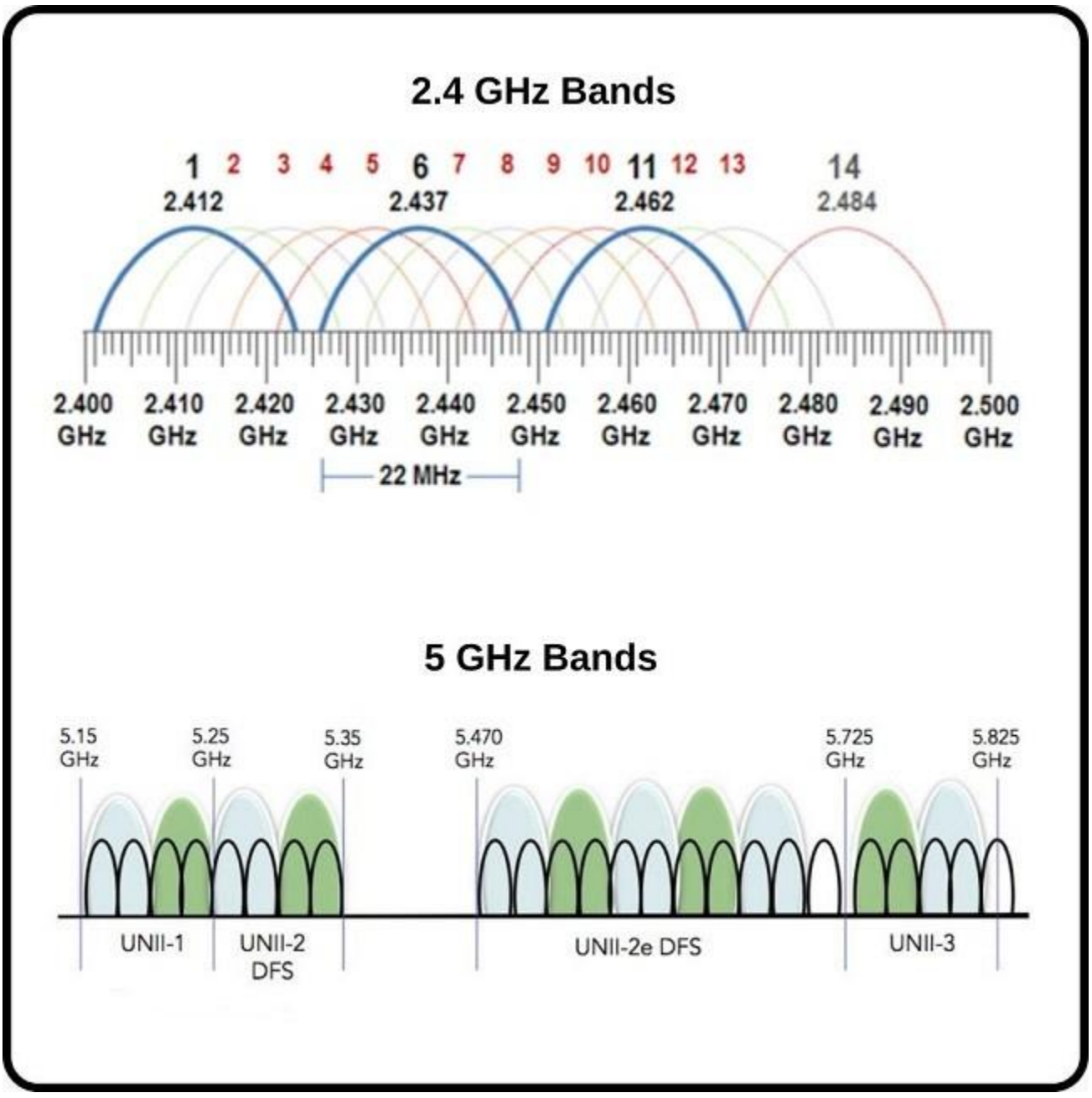
2.4 GHz band lies between **2.400 GHz** and **2.4835 GHz**, but briefly called **2.4 GHz**.

5 GHz band lies between **5.150 GHz** and **5.825 GHz**, but birefly called **5 GHz**.

Beside, **5 GHz** band includes below separate bands:

- **150** to **5.250 GHz**
- **250** to **5.350 GHz**
- **470** to **5.725 GHz**
- **725** to **5.825 GHz**

These bands also divided into different channels and each channel is assigned to a frequency.



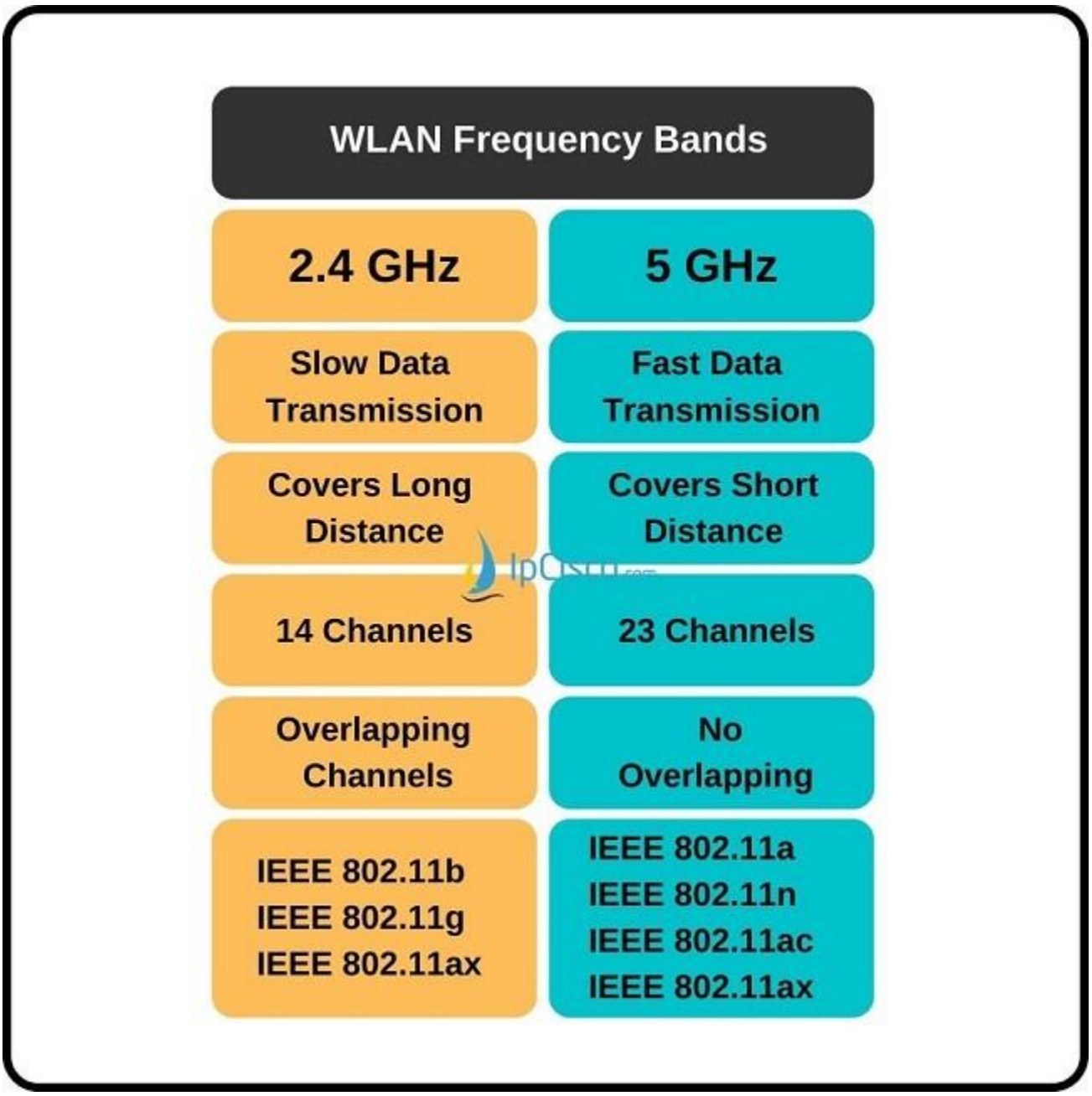
5 GHz band has **23 separate channels** that are not overlap. 5 GHz band has unoverlapping channels. So, using any channel with 5GHz do not affect other Access Points.

2.4 GHz band has **14 channels** but each channels of 2.4GHz is too wide, and each channel covers the frequency range of other four channels. So overlapping occurs. Using only **channel 1, 6** and **11** avoid overlapping.

Differences Between 2.4 GHz and 5 GHz

2.4 GHz and 5. GHz bands are the two bands used in Wireless LANs. What are the difference between these two bands? Why we use 2.4 GHz? Why we select 5 GHz instead of 2.4 GHz? Here, we will learn differences between 2.4 GHz and 5 GHz.

The most important difference between 2.4 GHz and 5 GHz is speed. 5 GHz is faster that 2.4 GHz. While 2.4 GHz band has a lower speed, it has a longer range coverage than 5 GHz. 5 GHz band has less coverage range.



2.4 GHz has 14 channels and each channel overlaps at least 4 other channel frequencies. So, overlapping can be an issue with 2.4 GHz. 5 GHz band has separate 23 channels. Each of these channels are separate, so there is not overlapping like 2.4 GHz.

2.4 GHz uses long waves and 5 GHz uses shorter waves. So, 5 GHz less penetrate walls and solid places. But, shorter waves prıvide more speed. So, for uploading and downloading 5 GHz is better.

2.5 GHz bans is more crowded that 5 GHz. Old devices, wireless home devices are mostly use 2.4 GHz. So, if you are in a crowded place, using 5 GHz is better than 2.5 GHz.

Wireless Standards and WLAN Bands

There are various wireless standards has developed from 1997 to now. These standards has provided a unity in wireless World andcompatibility between different vendor wireless products.

At 1997 **IEEE 802.11** was developed and at that time it support up to **2 Mbps** data rate and using 2.4 GHz band.

At 1999 **IEEE 802.11b** was developed and the data rate sjupported up to **11 Mbps** by using 2.4 GHz band. Again **IEEE.802.11a** wa developed in this year and data rate increased to **54 Mbps** with 5 GHz band.

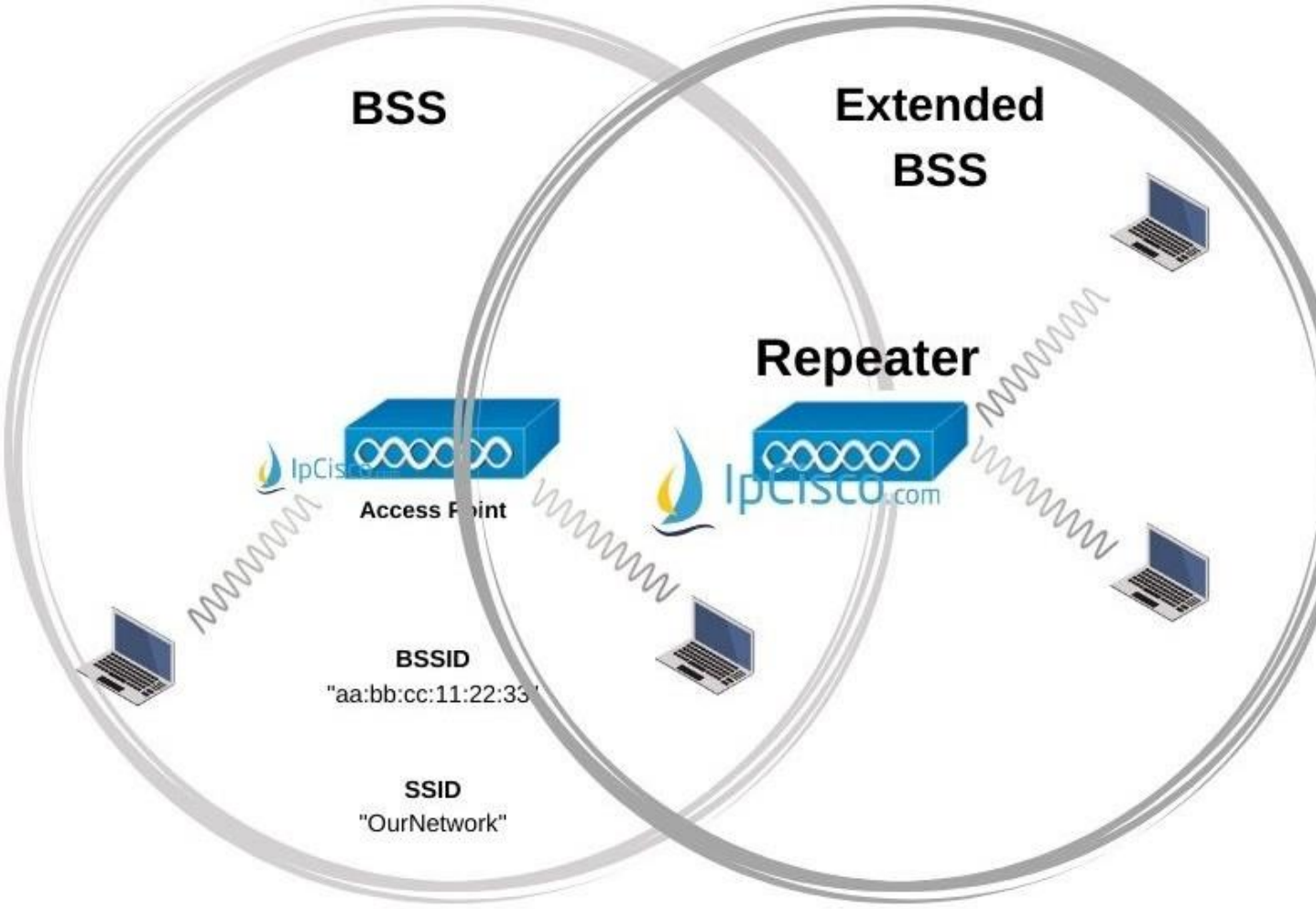
At 2003 **IEEE 802.11g** was introduced and this time 2.4 GHz band also support up to **54 Mbps** as before 5 GHz band did.

At 2009 **IEEE 802.11n** was developed and it support up to **600 Mbps** with both 2.4 GHz and 5 GHz. With this standard, **High Throughput (HT)** was supported.

At 2013 **IEEE 802.11ac** was introduced and it support up to **6.93 Gbps** with only 5 GHz. With this standard, **Very High Throughput (VHT)** was supported.

At 2019 **IEEE 802.11ax** was introduced and it support up to **4 Times Faster** than IEEE 802.11ac with both 2.4 GHz and 5 GHz. It is the standard of **Wi-Fi6**.

Other Wireless Network Extention Types



Wireless networks can be extended for various reasons. This can be used for new users, to cover new locations, to increase wireless network capability. To do this, there are various devices and **Access Point Modes** used with new antennas.

Here, we will talk about this **wireless devices** and Access Point Modes to extend our wireless network. We will learn:

- **Wireless Repeater**
- **Workgroup Bridge**
- **Outdoor Bridge**

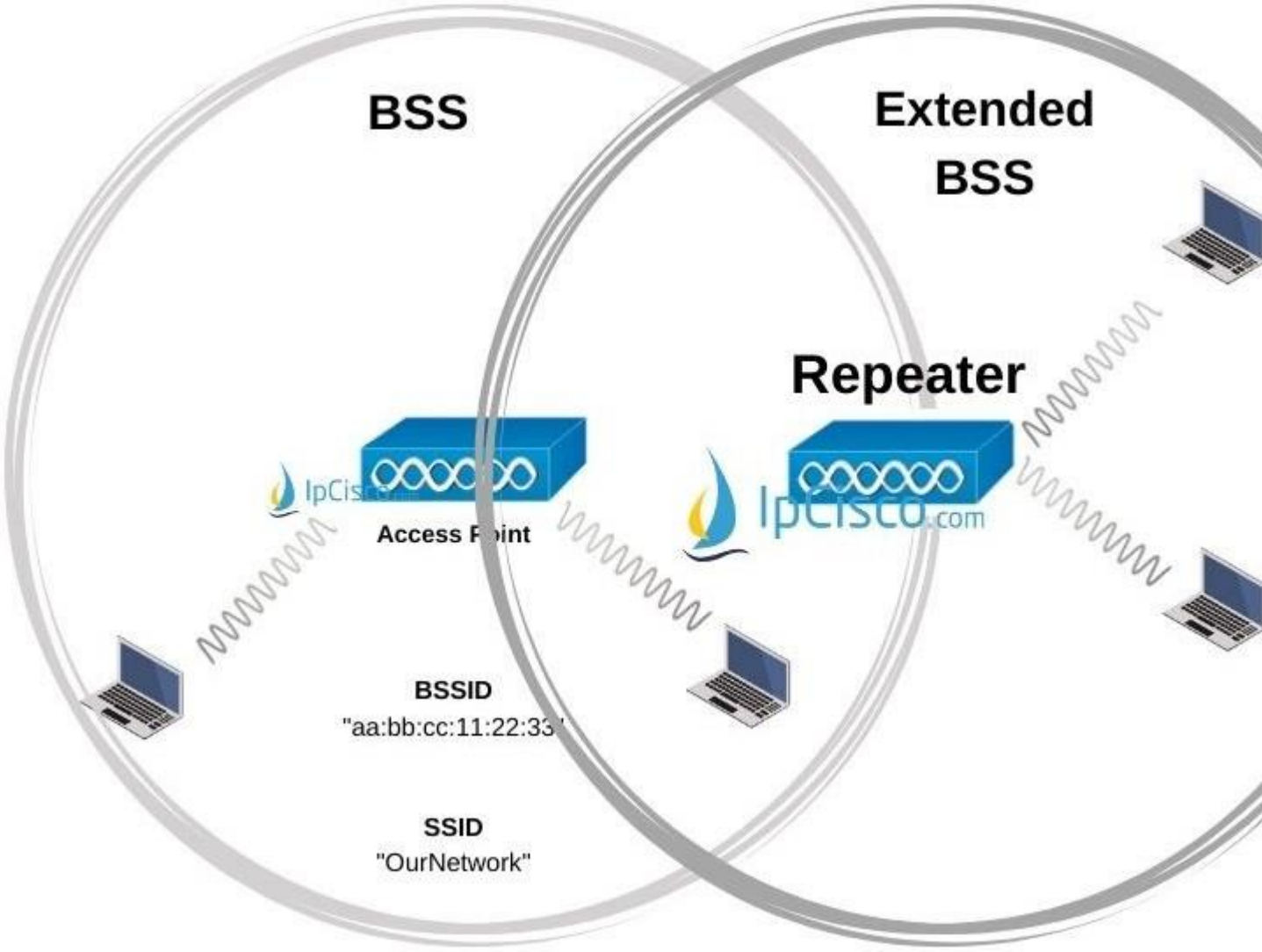
- **Mesh Network**

  Let’s start.

Table of Contents

Wireless Repeater

To extend our wireless network, we have talked about adding additional Access Points to our network. But there is also another way to extend our BSS coverage. By using a **repeater**, we can extend our BSS fort he users that are located a little remote places. If the normal coverage is not enough for such users, repeater strenghts the signals again and take the user in BSS. It receives the signal and then sends to further distances. The coverage of the repater is like a donut as Access Points.

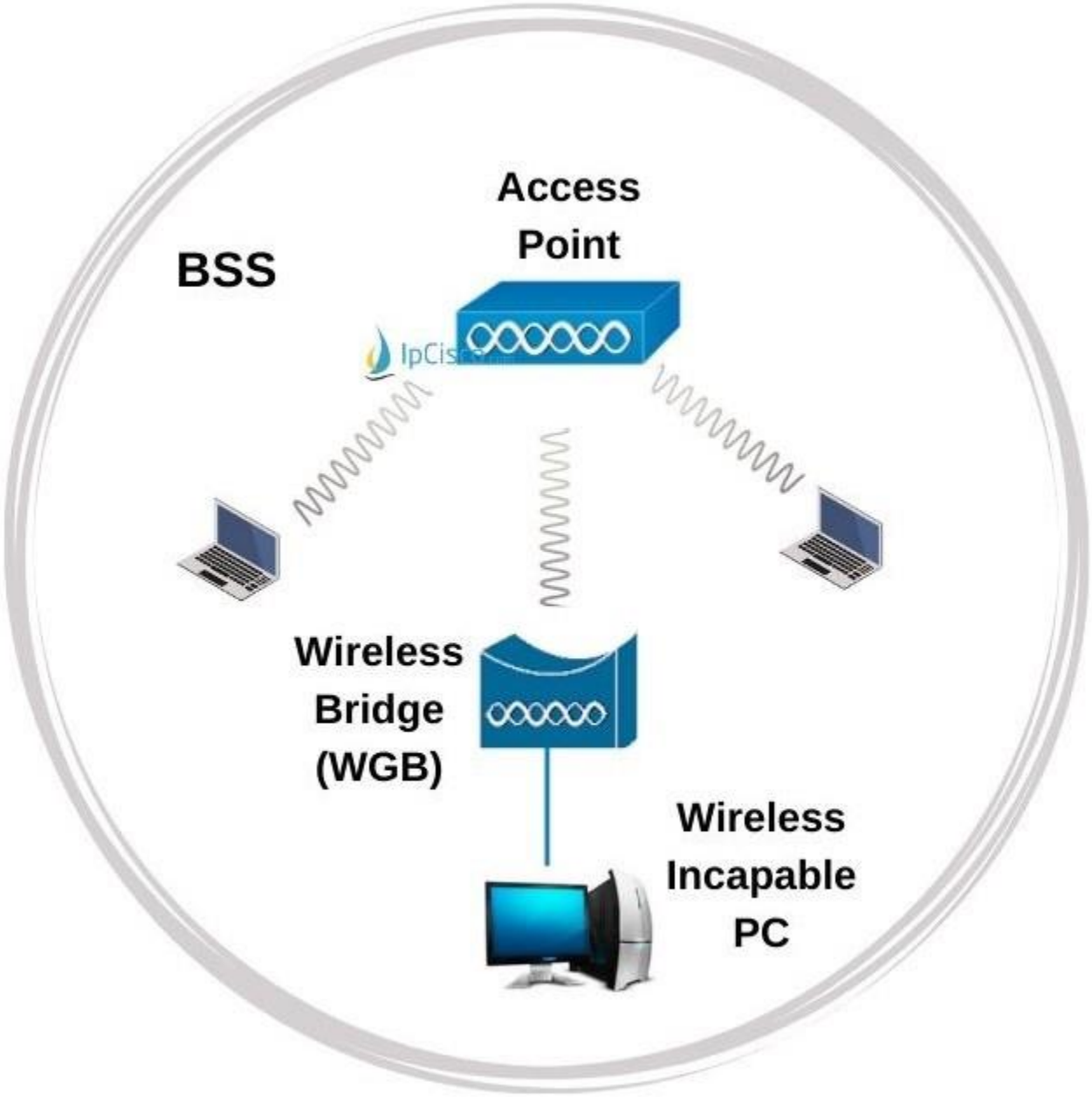


For the operation of a wireless network with a repeater, repeater can work in the same channel with the Access Point or not. If a repeater has one channel, it operates in the same channel with Access Point. But sometimes, repeaters has two channels and they keep received and repated signals isolated.

Workgroup Bridge

Workgroup Bridges (WGB) are used to provide wireless connection to wireless uncapable devices. For example, if you have a device that has now wireless interface and can use only Ethernet connection, you can give this device **wireless capability** with a **Workgroup Bridge (WGB).** Here, WGB is

used between Accesss Point and your wireless uncapable device. You can conenct your device to WGB with Ethernet, with wired connection and then WGB connects tom the Access Point with a wirelesss connection. By doing this, your device that has no wireless capability, can connect your wireless network.



Here, there are **two types** of Wireless Workgroup Bridges. These are :

- **uWGB (Universal Workgroup Bridge)**
- **WGB (Workgroup Bridge)**

uWGB (Universal Workgroup Bridge) is the device that can be used only for one device. It connects one device to your wirelessw network.

WGB (Workgroup Bridge) is the device that can connect multiple devices to your wireless network. It is a Cisco proprietary solution.

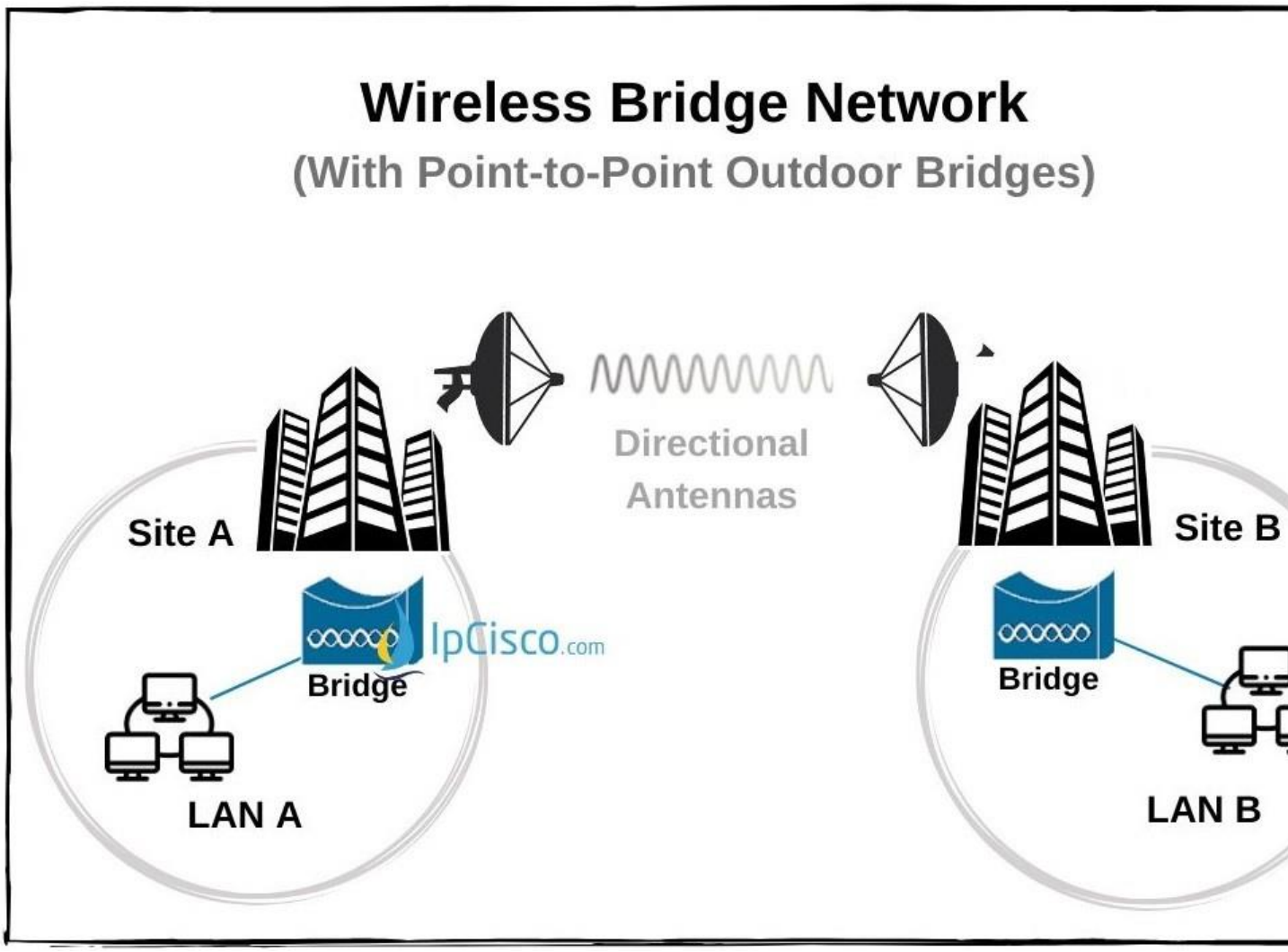
Outdoor Bridge

Sometimes different wireless networks are connected over long distances. To do this, Access Points can be used in **Bridge Mode** with additional **strong antennas**. This type of connection is called **Wireless Outdoor Bridge.** You can connect your companies two buildings or two sites in different cities.

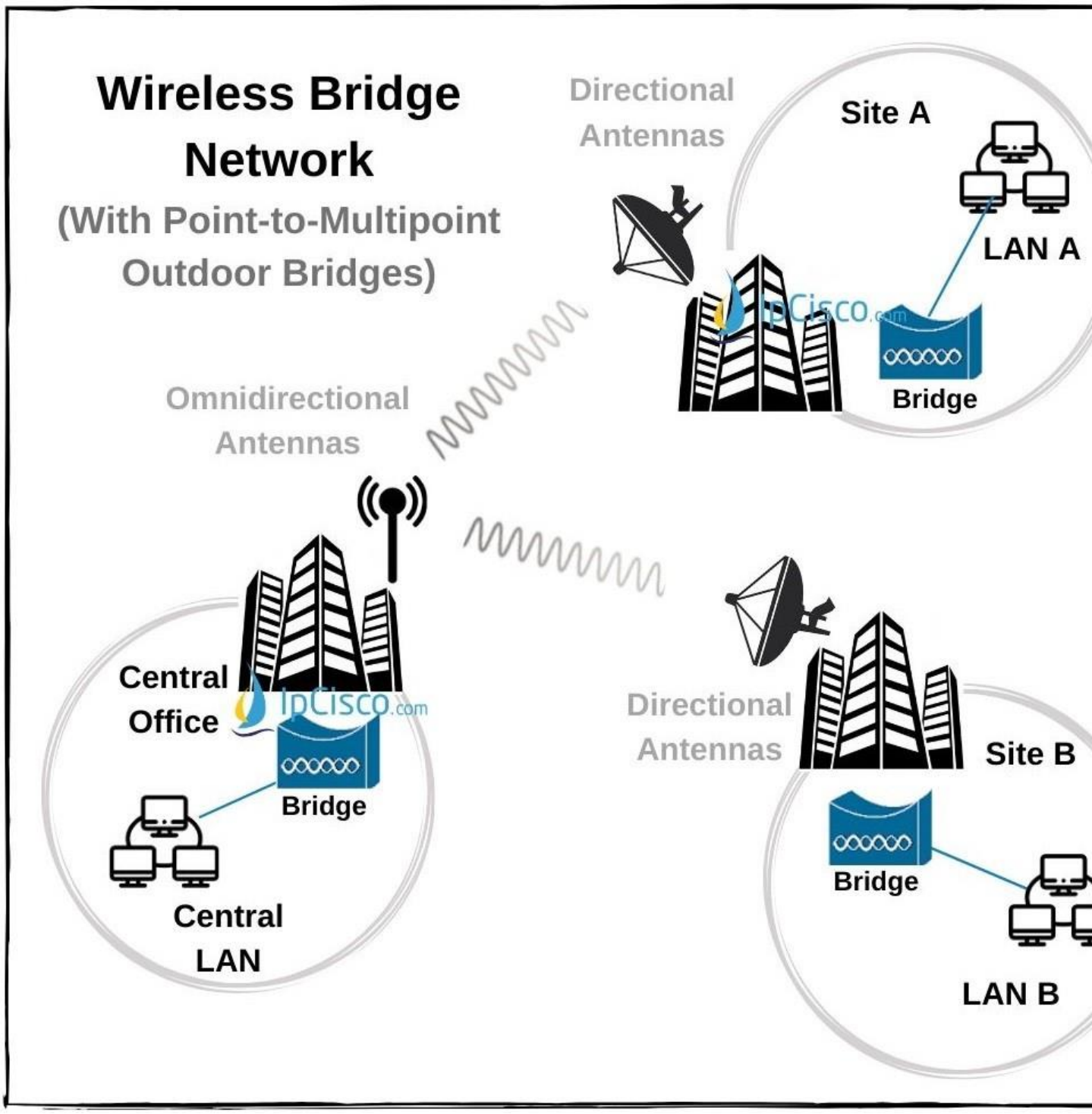
There are **two** different Outdoor Bridge Connections. These are:

- **Point-to-Point**
- **Point-to-Multipoint**

Point-to-Point connection is used between two locations. Here, there are two Outdoor Bridge at the each end and they use Directional Antennas to send signals. This is used to connect one site to another.

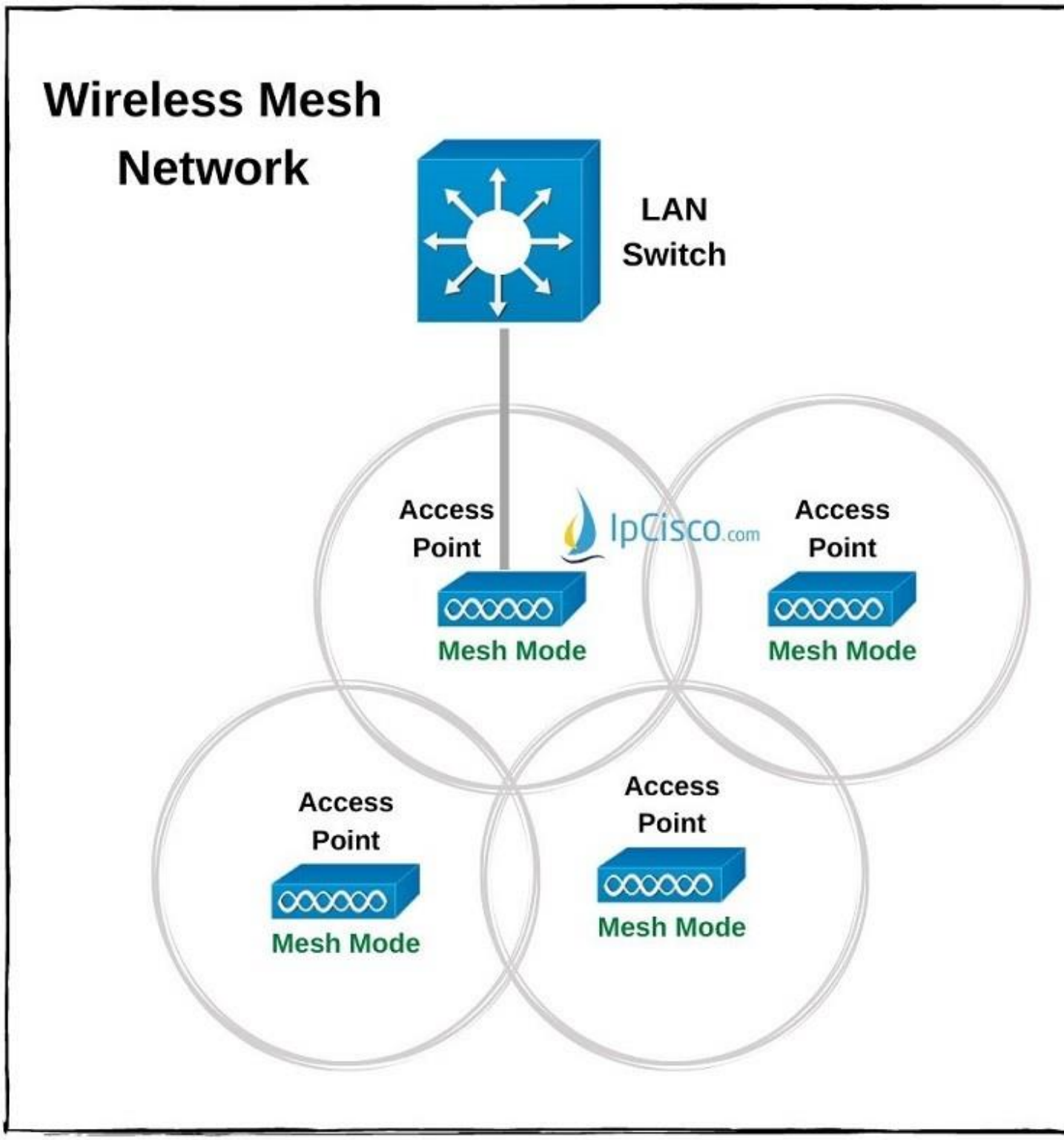


Point-to-Multipoint is used to connect a central location to one more sites. This type of connection uses both Omnidirectional and Directional antennas with Outdoor Bridges. The central site has Outdoor Bridge with Omnidirectional antenna to send the signals similarly to each site. Branch sites has Outdoor Bridge with directional antennas. Because they need signal strength through onlu one direction.



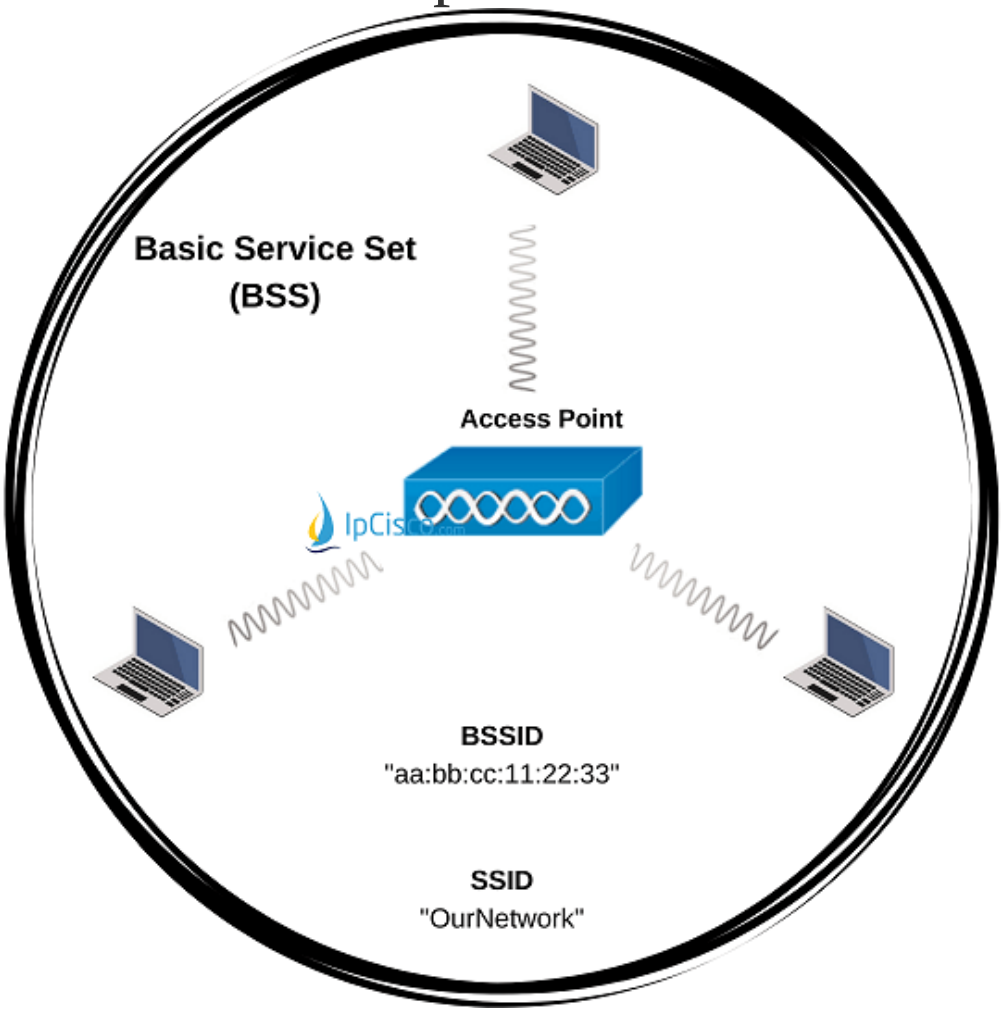
Mesh Network

AS we have talked about before, Access Points can be connected together over Ethernet. But how can we do this for a large area? We can use wireless Access points in **Mesh Mode** to overcome this issue. By doing this, Access points can connect together over wireless network. One side of this type network is also connected to a wired network on Ethernet.



One more channels can be used by an Access Point in Mesh Mode. Each AP has a BSS and users can bridged between different APs over different channels.

Wireless Principles



In this **wireless principles** lesson, we will cover antenna types used in wireless LANS and we will learn **wireless topology types** like BSS, ESS, IBSS.

Wireless communication is a communication type that is done over **Radio Frequency (RF) Signals**. As all communication types, here there is a sender and a receiver. Data can transfer through both direction as **bidirectional** or can only from one side to another as **unidirectional**. For this communication both sides of the communication must use the **same frequency** or in other words **same channel**.

Radio Frequency (RF) Spectrums and **the Satellite Orbits** of wireless communication are managed by International **Telecommunication Union-Radio Communication Sector (ITU-R)** all over the World.

Beside **Telecommunication Union-Radio Communication Sector (ITU-R)** that manages RF spectrums and satellite orbits, wireless networking standards are managed by two organization all over the World. These are **IEEE** and **Wi-Fi Alliance**. **IEEE** defined the technical standards of 802.11. So, network vendors produce their products according to these standards. The **Wi-Fi Aliance** is the non profit organization that certifies the wireless products of the vendors as they are compatible with the 802.11 standard.

Table of Contents

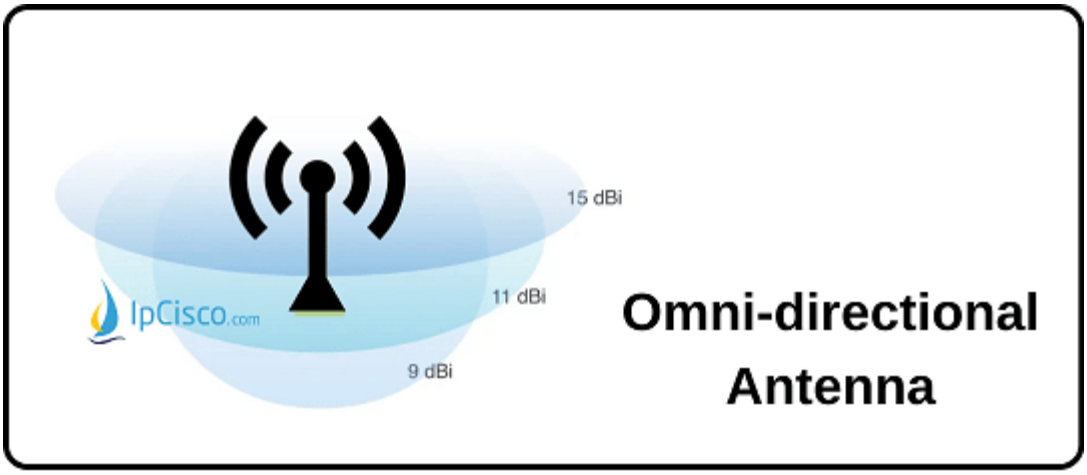
Omnidirectional and Directional Antennas

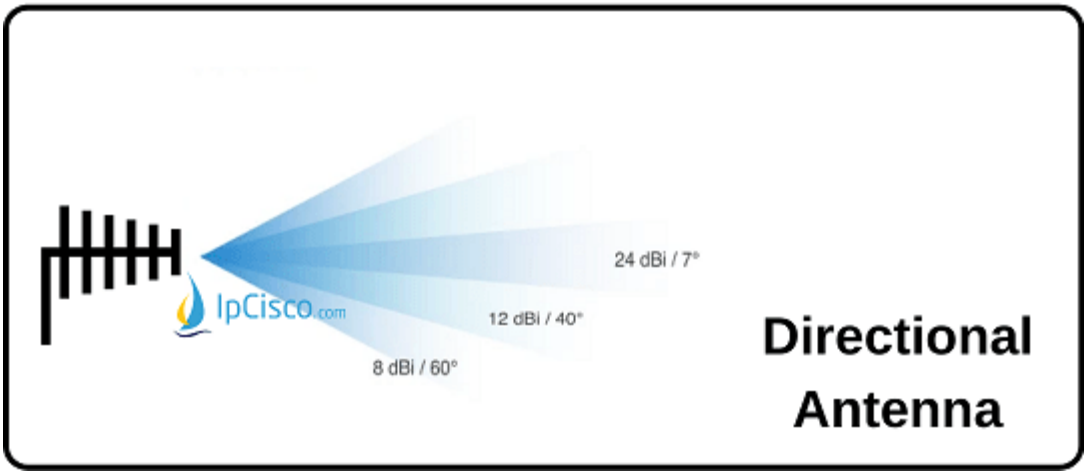
In **wireless principles,** Antennas are very important. Radio Frequencies are generated by antennas. These antennas can be located in wireless devices or can be a separate device. There are different types of antennas in wireless communication. Here, we will talk about two different types of wireless antennas.These are:

- **Omnidirectional Antennas**
- **Directional Antennas**

Omnidirectional Antennas receive and radiate equal power in all the horizontal directions. This can be liken to a donut. Here, around the antenna a donut shape is createw with signals. The antenna that is used by Access Points are Omnidirectional Antennas.

Omnidirectional Antennas are mainly used for point-to-multipoint configurations. Point-to-multipoint means that, they are the distributor of wireless signals and the wireless available devices receive signals from it.





Directional Antennas receive and radiate in only one direction. The strenght of directional antennas is more thanb omnidirectional antennas. You can arrange the direction of this type of anennas. Yagi Antennas are directional antennas

Directional Antennas are mainly used for point-to-point configurations. Sometimes, they can be used for point-to-multipoint configurations also.

During wireless communicaton and wireless signal distribution fort his communication, because of some factors, signals distortion occurs. In other

words, different types of objects affect signals. So, which factors or which type of objects influent wireless signal distortion? These are given below:

- **Absorption Objects**
- **Scattering Objects**
- **Reflection Objects**

Absorption Objects are the objects which **absorb** Radio Frequenct (RF) Signals. In a buildings, walls, ceilings are examples of Absorption Objects.

Scattering Objects are the objects which **disperse** Radio Frequenct (RF) Signals. In a room, carpets or different types of Wall paintings can be examples of Scattering Objects.

Reflection Objects are the objects which **reflect** Radio Frequenct (RF) Signals. Metal and glass are examples of Reflection Objects.

Wireless Topologies

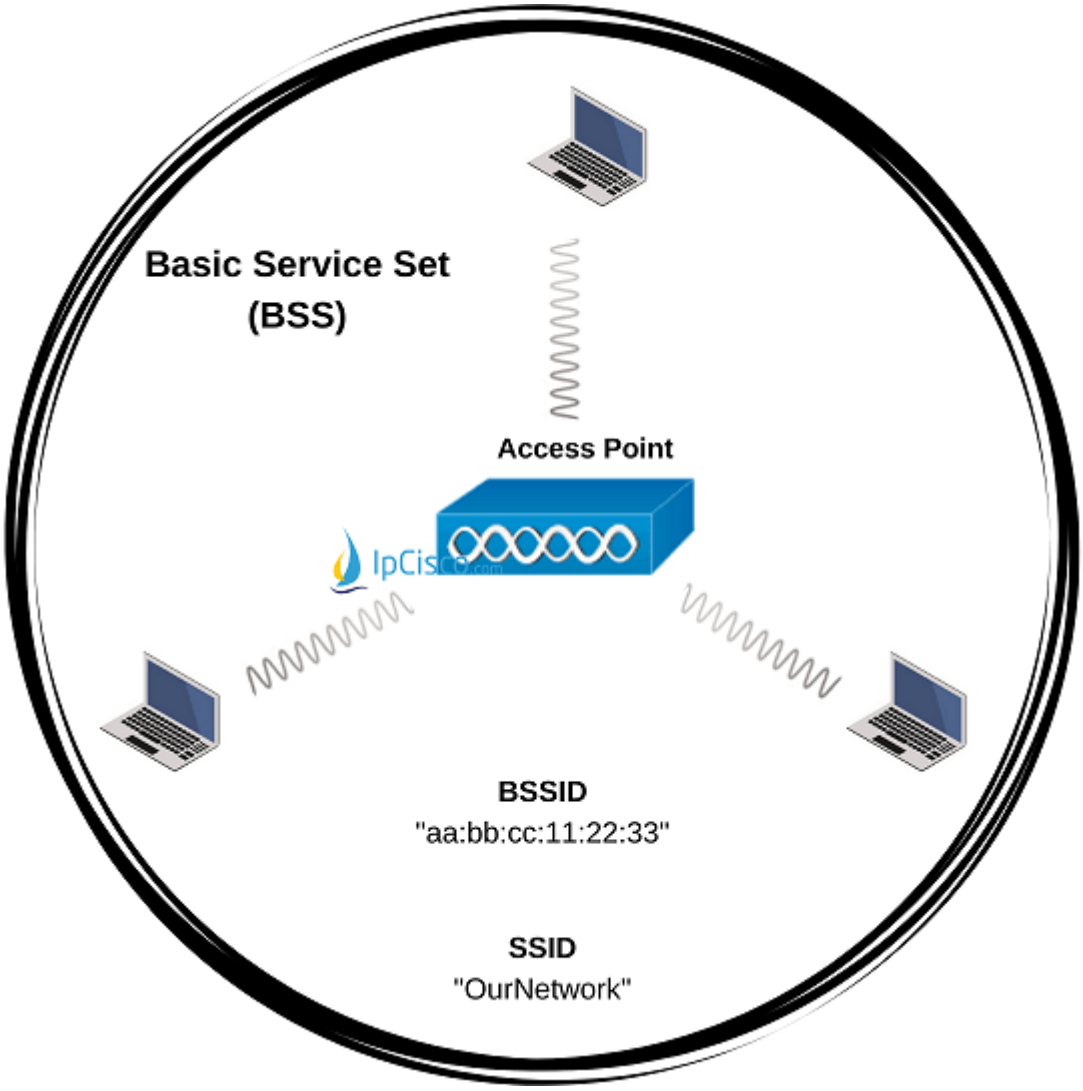
In **wireless principles,** there are different wireless topologies used. These wireless topologies are given below:

- **Basic Service Set (BSS)**
- **Extended Service Set (ESS)**
- **Independent Basic Service Set (IBSS)**

Basic Service Set (BSS)

The first wireless topology of **wireless principles** is **Basic Service Set (BSS). Basic Service Set (BSS)** is a **closed group of devices** consist of a central wireless source and its clients that get service from this central source, that can communciate with 802.11 wireless standard. The central device can be an **Access Point (AP)** and the clients are the devices that are wireless capable. In other words, we can say that, BSS is a group of wireless devices served by a a single Access Point (AP). All the devices in a BSS, use the same channel to communicate.

Every BSS has a string logical name that is advertsed by Access Point. This identifier is called **Service Set Identifier (SSID)**. In other words, SSID is the **network name** of BSS. It is not necessary for an SSID to be unique. But, there is another identifier that is used by devices and must be unique like and it identifies Access Point uniquely. It is the MAC address of Access Point and specifically called **BSSID (ID of BSS)**.



Access Points use Omnidirectional Antennas. So, their signals are usable in a circle or donut like area. So, the physical borders of this area is has a specific name in wireless standard. This is **Basic Service Area (BSA)**.

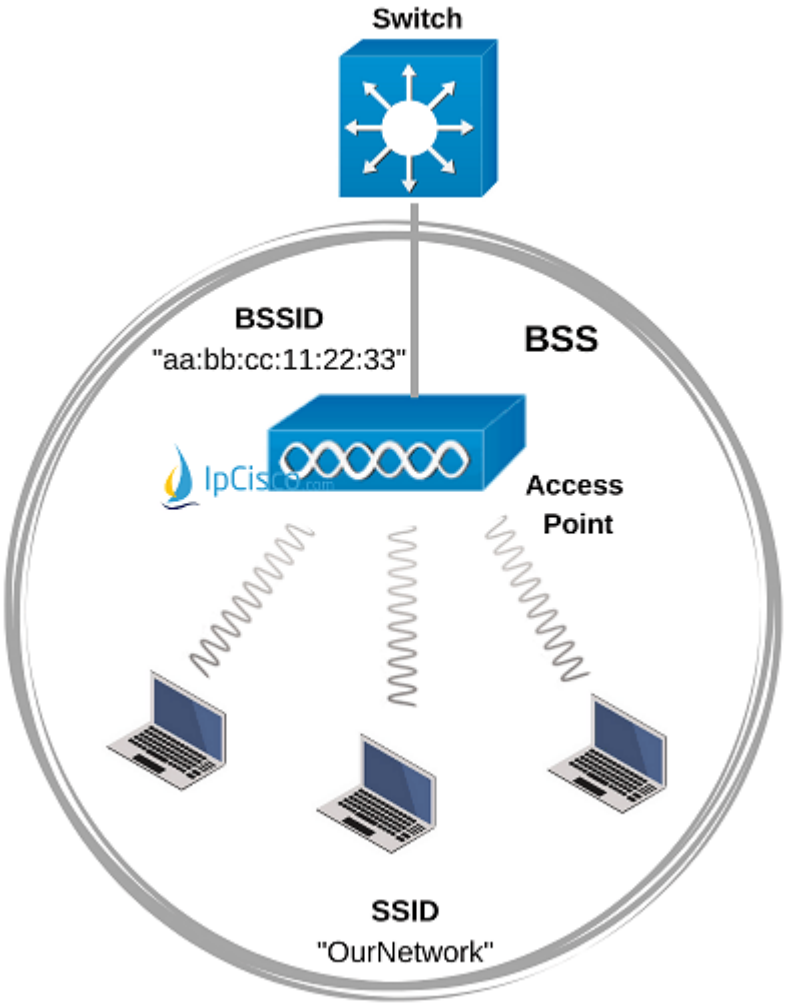
BSS Operation

As we have talked about before, in a BSS, there is an Access Point and connected clients to this Access Point. Here, a client must be accepted by the

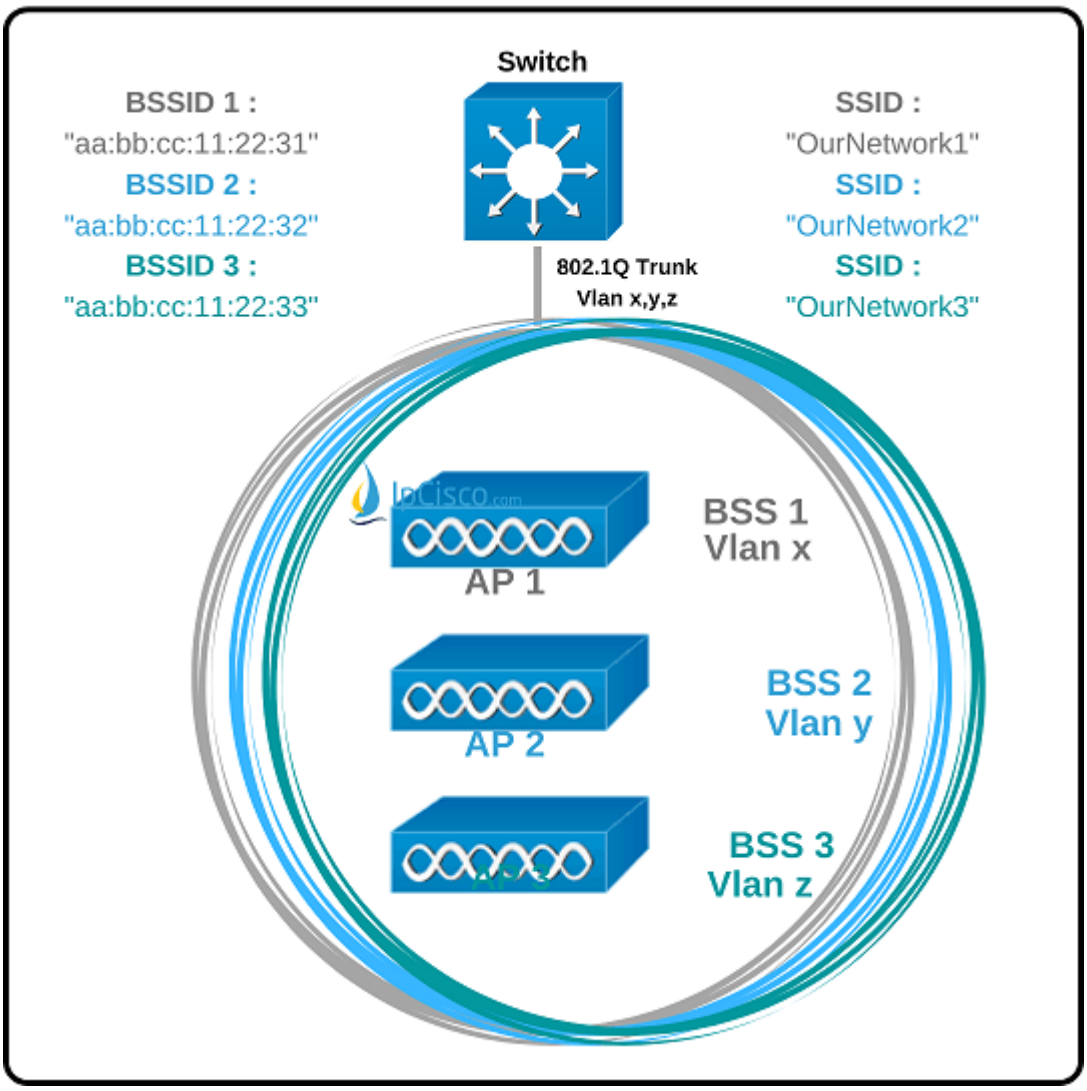
Access point to get service from it. Firstly client sends an association request to the AP and then AP replies that it accepts this request. By doing this, association is established. If AP do not accept, then the device can not be a client of this BSS.

Communication between the devices in BSS can be done over Access Point. All the traffic pass through AP and this provide a security mechanims by managing the traffic on a central node. But, the signals are over the air, so without an encryption it is not secure. So, various wireless encryption methods are used.

Clients can communicate in the BSS. What if they would like to communicate outside this BSS. Fort his, Access Point is used. Access Points has also uplinks to the outside of the BSS with Ethernet. Though this link, clients can communciate with outside of BSS. This process is called **Distribution System (DS)** in wireless 802.11 standard.



Normally without VLAN configuration, one SSID is used by a single VLAN. But we can extend this for multiple VLANs with multiple SSIDs. Here, VLANs and SSIDs are different but the coverage area of the BSS is sam efor each network. Because the physical device, Access Point is the same device. Fort his type of network, different BSSIDs are used and in Cisco, this BSSIDs are determined by incrementing the last digit of the radios's MAC address.



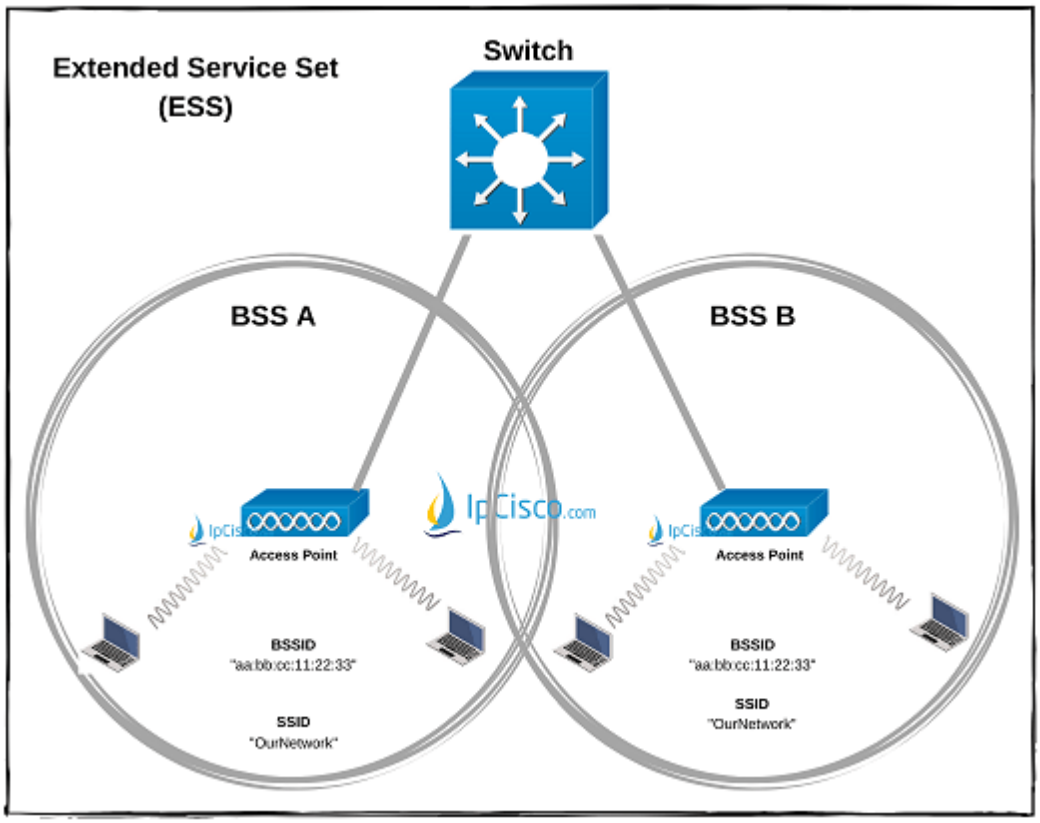
Extended Service Set (ESS)

Access Points are limited devices. They can cover a BSA and it is called a **Cell**. But in many companies network area is very large that only one Access Point can not cover all the area. So, additional Access Points are used to cover all the area. This Access Points are connected through an Ethernet Switch and they become a single continuous and seamless connection from the client perspective. User can

go from one cell to another without conenction interrupt. So, combining one more Access Point in a swithed network is called **Extended Service Set (ESS)**.

In a network that has multiple Access Points, all SSIDs must be defined on each Access Point for seamless and continuous connection. Here, each Access Point's BSSID is different but SSIDs are same.

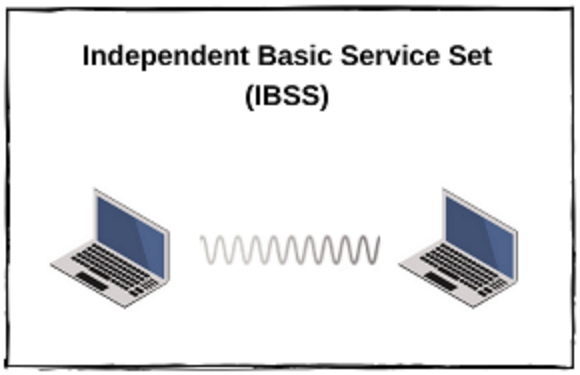
Passing from one AP to another is called **roaming**. This is simply, similar logic with Mobile Operator roaming. If a client change BSA, then check for a new AP and if finds then connected to this new AP.



Independent Basic Service Set (IBSS)

In 802.11 Standard, clients can directly communicate together without any need to an Access Point. This type of wireless communciation is callled **Independent Basic service Set (IBSS)**. Another name of this is **ad hoc network**. Such wierless connection is used generally whenever two laptop want to share information, a PC want top rint someting from a printer etc.

For Independent Basic Service Set operation, one device works as leader. The other become client. So, the leader device advertise the network and the other want to joinm this network.



In this lesson we have covered **wireless principles.** We have learned wireless topology types like BSS, ESS, IBSS, beside antanna types used in wireless.

WLAN Components

In Cisco, there are two types of Wireless Solutions. One of them is using only **Autonomous Access Points** and the other is using **Light Weight Access Points (LWAP)** with **Wireless LAN Controllers.** So, **What are Access Points? What is a WLC?** Let's learn each of these devices in Wireless Networks.

Table of Contents

What Are Access Points (AP) ?

Access Points are one of the important devices in a WLAN. So, **what is an Access Pioint? An Access Point (AP)** is a the device that receives the signals from **WLC** and deploys this signals to the hosts according to a coverage area.

There are two types of Access Points. These are:

- **Autonomous Access Point (AP)**
- **Lightweight Access Point (LWAP)**

Autonomous Access Points (AP) are independant devices. They do not need WLC. These APS can be managed centrally also by **Cisco Works Wireless LAN Solution Engine (WLSE)**. With **Autonomous Access Points (AP), SSID** and **VLAN** must be statically configured in all the access point for roaming.

Lightweight Access Points (LWAP) are used together with Wireless LAN Controllers (WLCs). In this architecture **Lightweight Access Points** is responsible for real time processes. The roles of WLC are more: Authentication, Security, QoS, Mobilliy Mangement, Forwarding etc.

User traffic between AP and WLC is tunneled with different protocols. The protocols used between WLC and LWAP are:

- **Lightweight Access Point Protocol (LWAPP)**
- **Control and Provisioning of Wireless Access Points Protocol (CAPWAP)**

Both of these protocols work with **UDP**.

Wireless LAN Controller can be or can not be in the same ip subnet with **Lightweight Access Point.** The only important thing is they can reach together over IP.

What is WLC (Wireless LAN Controller) ?

Wireless LAN Controller (WLC) is a central device with which you can do configurations, you can manage your operations etc. in a wireless network. With this capabilities, **WLCs** reduces deployment, operations and management cost in a wireless network.

There are **two** types of **APs**. These are:

- **Autonomous Access Point (AP)**

- **Lightweight Access Point (LAP)**

Lightweight Access Points (LAPs) can be managed with Wireless LAN Controllers (WLC). A **WLC** can manage **6 to 300 Access Points** accourding to its capacity.

SSID, VLAN etc. configurations are done on **WLCs**.

WLC and the LAN switch has a link between them. This link can be one link or a Link Aggregation can be used on it.

There are common standards or protocols of wireless networks. Cisco Wireless Controllers support **802.11a/n/ac** and **802.11b/g/n** protocols.

According to the need, wireless network sizes change. For different size wireless networks, we can use different types of **Wireless Controllers.**

There are **three** important terms about **WLC**. These are:

- **Ports**
- **Interface**
- **WLAN**

Ports are the physical connection parts from WLC to any device.

Interfaces are the logical connection mapping to a VLAN.

Cisco WLC Models

There are different types of Wireless LAN Controllers in Cisco. Some of these Cisco WLC Models are retired and not supported any more. Some of them are

neww technology. Here, we will talk about a new WLC Series. They are **Cisco Catalyst 9800 Series Wireless Controllers.**

Cisco Catalyst 9800 Series Wireless Controllers more reliable and more secure WLCs. They use IOS-XE as an operatins system. Ther are different WLC models in this series for different needs. These Models are given below:

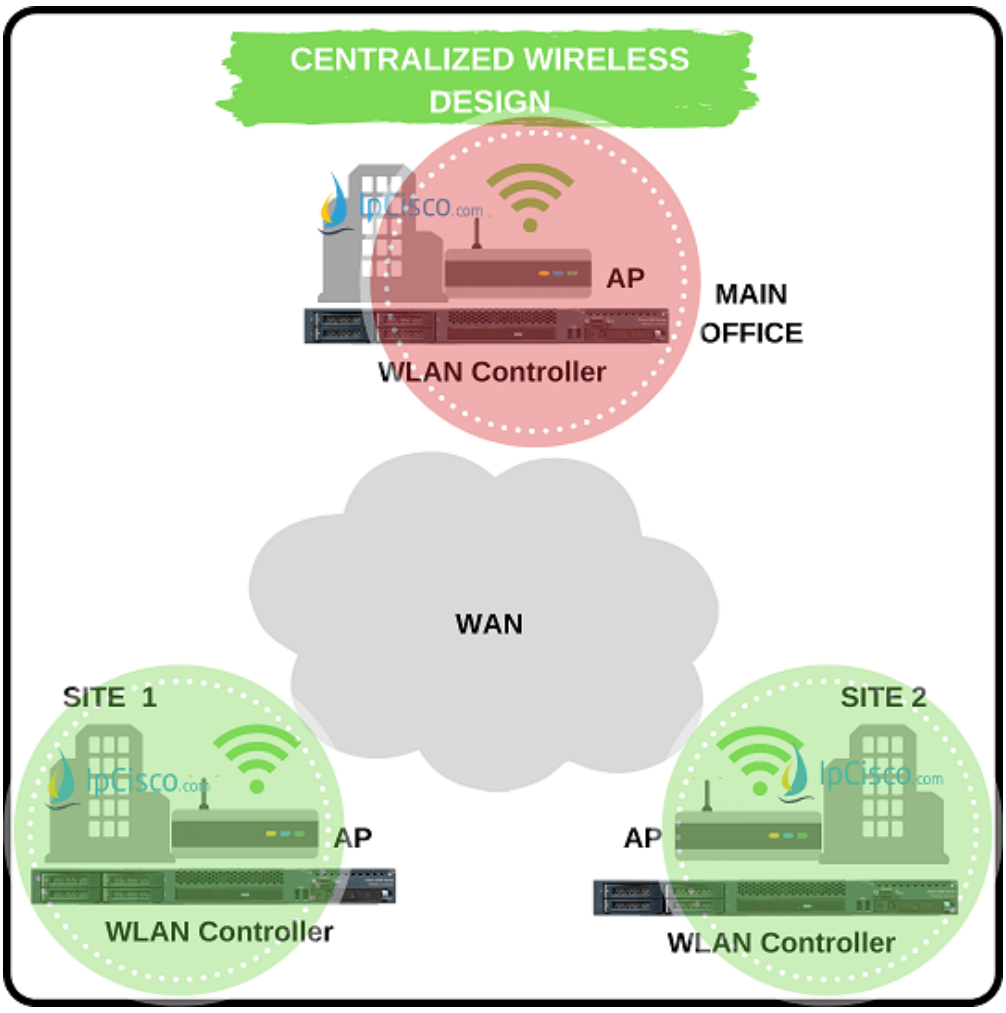
- **Catalyst 9800-L**
- **Catalyst 9800-40**
- **Catalyst 9800-80**
- **Catalyst 9800-CL**

Beside, there are embedded versions that are for Access Points and Switches:

- **Embedded wireless for an AP**
- **Embedded wireless for a Switch**

Now, let’s telk about these WLC Models detailly.

Wireless Network Design Models



Cisco has different **Wireless Network Design Models** for different types of networks. These **Design of Wireless Network Models** are given below :

- **Centralized Network Design**
- **FlexConnect Network Design**
- **SD-Access Network Design**

Centralized Network Design or in other words Local Design is the wireless design type in which **WLAN Controller and Access Points** are in the same site. There are separate WLAN Controllers in different sites.

FlexConnect Network Design is the wireless design type which is used with a central WLAN Controller and connected Access Points. Here, every site do not need to have a WLAN Controller.

SD-Access Network Design ois an integrated design with which users can benefit from both wired and wireless network. We use such a design also for less latency.

Now, let's talk about these **Wireless Network Design Models** detailly.

Table of Contents

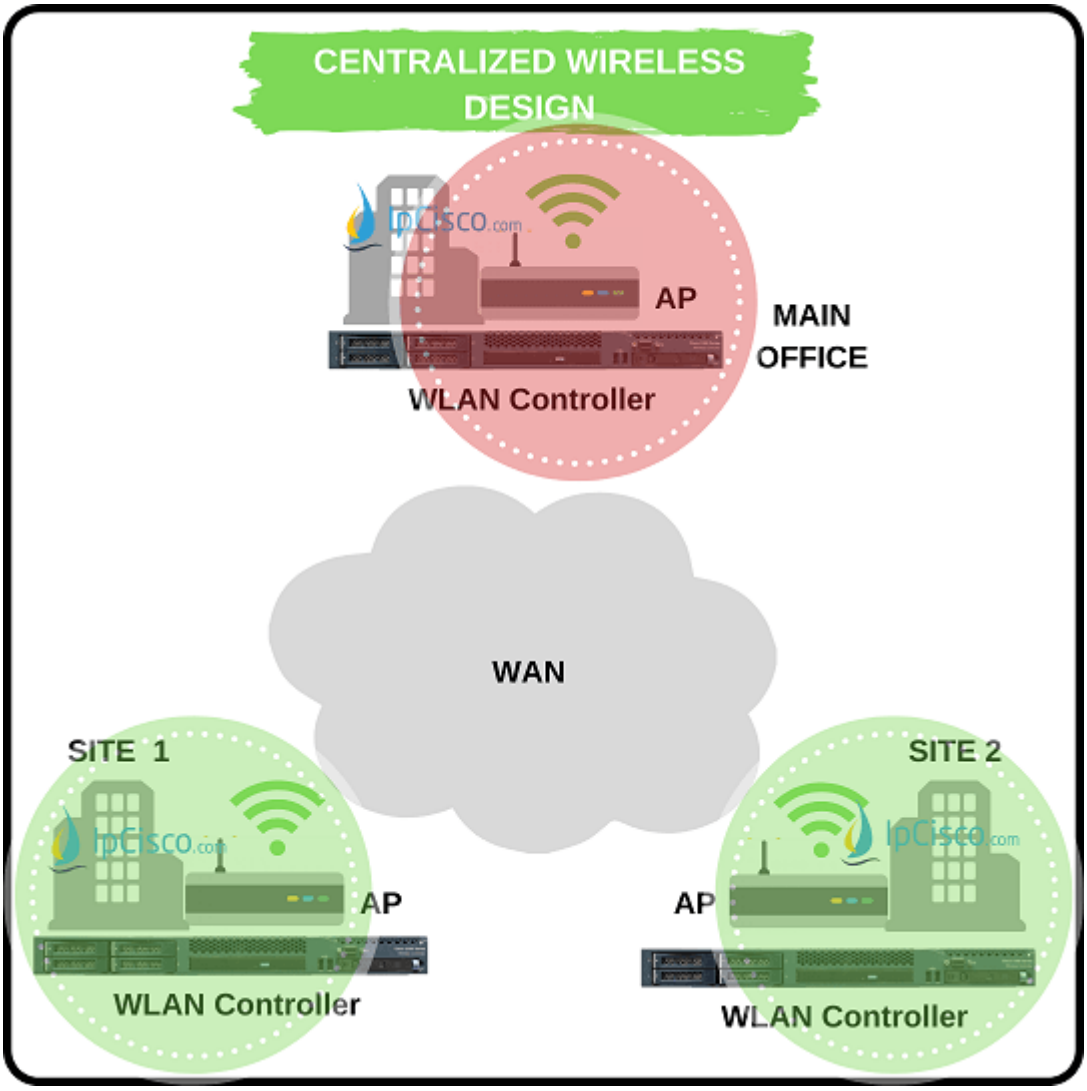
Centralized Design

In **Centralized Wireless Network Design (Local Wireless Design)** , there are centralized WLAN Controllers in each site and Access Points are connected to this WLAN Controller (WLC). This type of wireless design is esy to configure and provide quich troubleshooting. So, for large networks, **Centralized Wireless Design** is ideal solution.

The main components, **WLCs** and **APs** in **Centralized Wireless Design** are connected together over a tunnel. This tunnel is done with a specific protocol, **CAPWAP (Control and Provisioning of Wireless Access Points)**.

So, How can we determine if we need **Wireless Network Controller** or not on a site? In other words, when we need to use a Wireless Controller on our Site? If your site has below qualifications, you should use a WLC on your site.

- If you have a separate **datacenter** in your site,
- If you have a **distribution layer** on your site,
- If you have more than **100 Access Points** in your site,
- If your **latency** is more than **100 ms** in your site.



For **Centralized Wireless Network Design** Cisco recommends some special Wireless Devices. If your network will be large, you can use;

- **Cisco 8500 Series WLAN Controller**
- **Cisco 5500 Series WLAN Controller**

If your network will be small, then you can use;

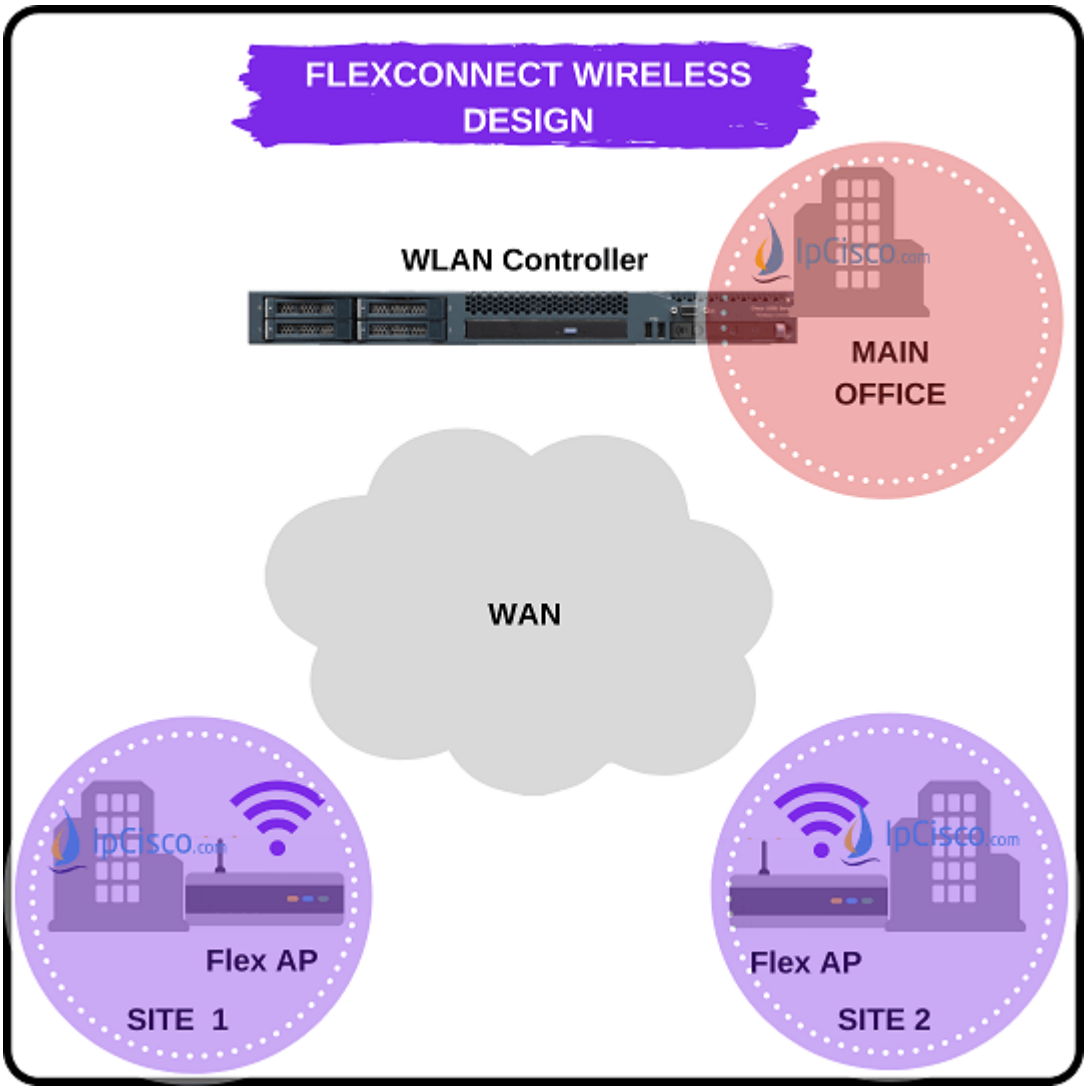
- **Cisco 3500 Series WLAN Controller**

FlexConnect Design

FlexConnect Wireless Design is the wireless solution in which you do not need to use a specific WLAN Controller in each site. Here, the management and configuration of Access Point in the sites are done frokm the central location. This type of solution is a cost-effective, so, it is good for small networks.

For **FlexConnect Wireless Design,** we need to use a WLAN Controller on central site.This can be a Shared WLC or a Separate WLC.

When you have a **Local Mode WLC**, if it has additional capacity and required capabilities to support **Flexconnect APs**, you can use this **Local Mode WLC** as **Shared WLC**.



If you use a **separate WLC**, you can use one of the below **Cisco WLC Models**:

- **Cisco 8500 Series**
- **Cisco 5500 Series**
- **Cisco 3500 Series**

Also in **FlexConnect Wireless Design, CAPWAP Tunnel** is used between WLC and APs.

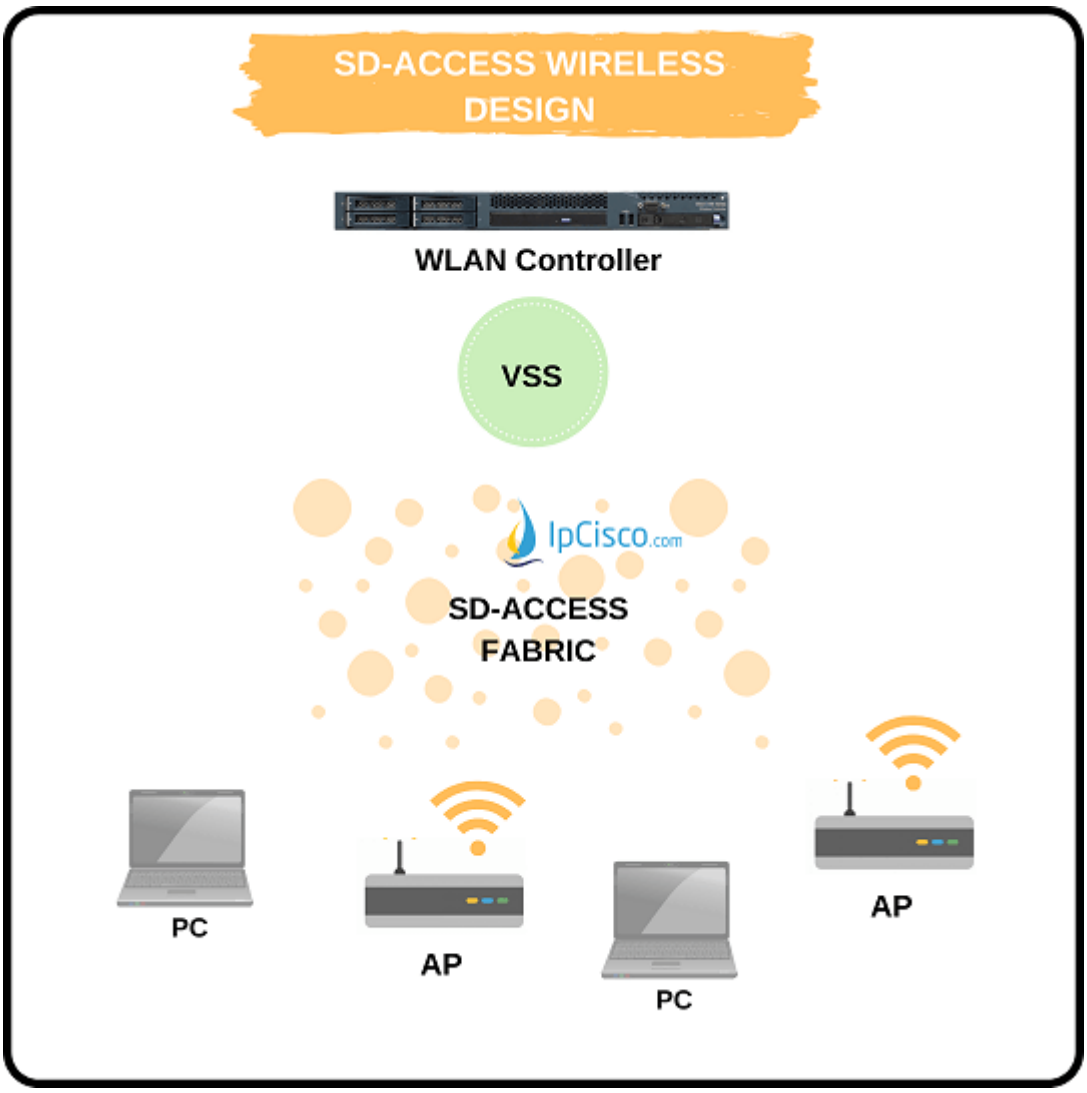
So, when we can use **Cisco FlexConnect Design** on a site? We can use **Cisco FlexConnect Design** if;

- We have **50** or **fewer APs** in the site,
- The site is a small LAN consist of a **single access layer switch,**
- The site is **one of the remote sites** that connects to a central site,
- If your **latency** is less than **100 ms** in your site.

SD-Access Design

SD-Access Wireless Design solution is an integrated solution to **SD-Access Wired Design.** Here, users can benefit rom both of these architectures, wireless and wired.

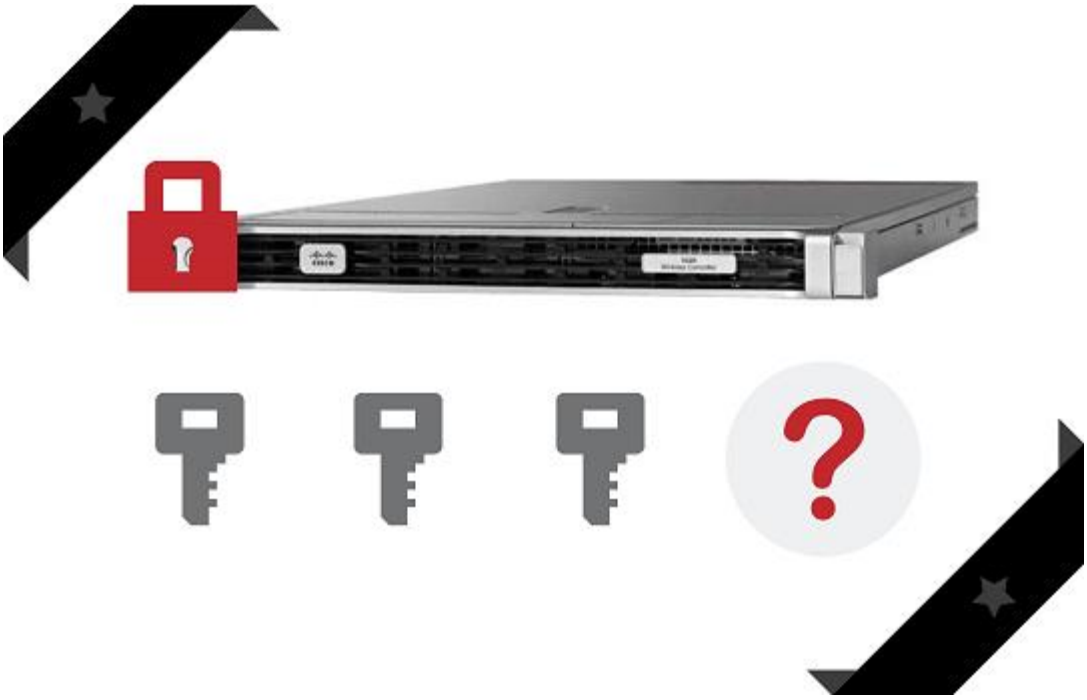
In **SD-Access Wireless Design, Fabric WLCs** are used for the communication of **Fabric Control Plane** and **Fabric APs** are used for encapsulation into **VXLAN data path**.



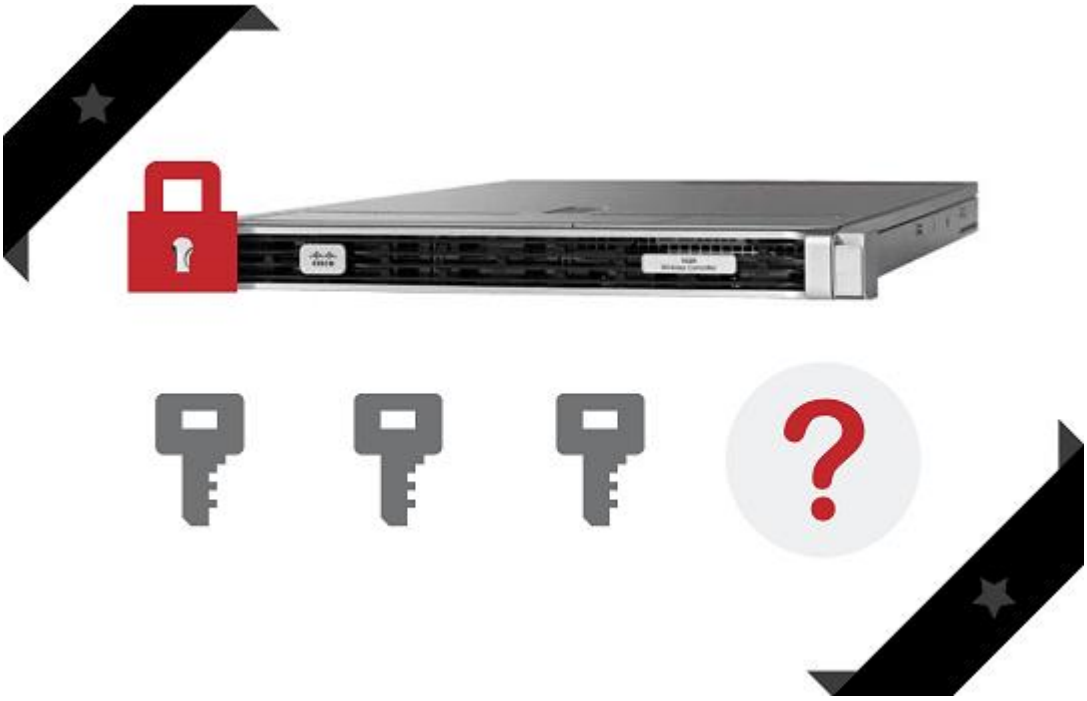
When we can use **SD-Access Wireless Design**? To use **SD-Access Wireless Design,** we need to have;

- **SD-Access Wired Network**
- **Fabric Mode WLC and Fabric Mode APs**
- **20ms or Less latency between APs and WLC**

WLC Management Access Connections



To access a network device there are various methods. These network access methods are also used to access wireless components. So, here, we will talk about these access methods.



Access Methods used in Wireless networks can be divide into 4 categories. These are given below:

- **Telnet / SSH**

- **HTTP / HTTPS**
- **Console**
- **TACACS+ / RADIUS**

Table of Contents

Telnet / SSH

Telnet and **SSH** access can be done on **CLI** by using **WLC Mangement Interface IP Adddress**. On CLI, you should use **ssh** or **telnet** keyword and then you should use the Maagement IP address. If the Telnet/SSH service is on and there is no restriction for telnet/SSH session, you can access the wireless device with this method.

As you know, **telnet** is **insecure** and **SSH** is the **secure** way in this type of method. By default, **telnet** is **disabled** on **Cisco WLCs**.
But, **SSH** is **enabled** by default. So, if you want to use telnet, you should enable it.

To access to a WLC with Telnet or SSH, they must be aneble on WLC. You can enable these services on CLI with the below commands:

- **config network telnet enable**
- **config network ssh enable**

You can check the status of this configurations with "**show network summary**" command.

- **show network summary**

RF-Network Name..... TestNetwork1

Web Mode..... Enable

Secure Web Mode..... Enable

Secure Web Mode Cipher-Option High..... Disable

Secure Web Mode Cipher-Option SSLv2..... Disable

Secure Shell (ssh)..... Enable

Telnet..... Disable

To see the active Telnet sessions you can use the below command:

- **show login-session**

ID	User Name	Connection From	Idle Time	Session Time
00	admin	EIA-232	00:00:00	00:19:04

On GUI, you can also adjust the Telnet/SSH parameters like **Telnet Login Timeout, Maximum Number of Sessions** etc. related with Telnet and SSH from "**Management > Telnet-SSH**" part. After applying adn saving, the configuration is Ok.

We can also adjust telent priviledges from "**Management > Local Management Users**" part.

HTTP / HTTPS

To access **GUI (Graphical User Interface)** of the WLC, we can use HTTP and HTTPS. HTTP is insecure and http is secure way to connect. By default HTTP is disablled but it can be enabled to use. And HTTPS is enabled by default.

To access WLC GUI, we can use HTTP/HTTPS over a browser. Here, service port interface or the management interface is used to access GUI.

To access GUI, **192.168.1.1** is the **default** IP Address.

- https://ip-address

  or

- http://ip-address

To access GUI over browser, webmode must be enable on WLC. By default it is disabled. You can enable it with below command on CLI:

- **config network webmode enable**

To allow only secure connection with HTTPS, you can use the below command on the controller CLI:

- **config network secureweb enable**

Console Connection

Console Connection is the connection type that can be done over console port of the wireless device. You should be next to the device for thic connection. You

can plug in your console cable to your laoptop and the console port of the wireless device and then you can access through both CLI and GUI.

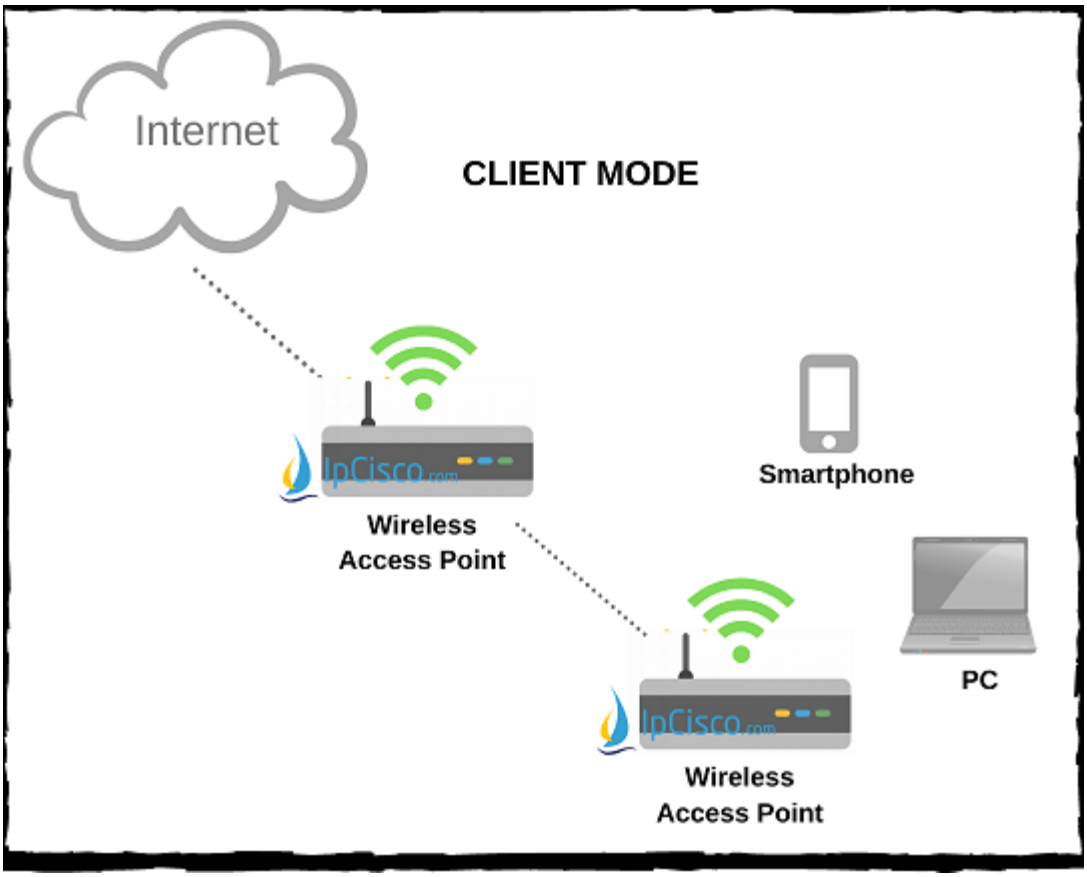
To do this, **Console connection** must be enabled on Cisco WLC. By **default** it is **enabled**.

RADIUS /TACACS+

To access a wireless device **RADIUS** or **TACACS**+ authentications can be used. For this access,user credentials (user, passwords) are defined in **a RADIUS Server** or **TACACS+ Server** and before the access, user credentials are checked. If the correct credentials (user, passwords) are given, then user access accepted.

All users have special usernam and passwords. And these information is stored in a remote **RADIUS Server** or **TACACS+ Server**. While accessing the **Cisco WLC**, the user name and the password is requested from the user. If user write the correct information, he/she can accees **Cisco WLC**.

Wireless Access Point Modes



Cisco Wireless Access Points can be used for different aims. We use some of them to connect host devices or we use them for troubleshooting activities. There are also other usages fo this **Access Point Modes**. So, what are **theseWireless Access Point Modes**? **What Wireless Access Point** is used for which reason?

There are different **Access Point Modes** that we can configure on **Cisco Access Points**. These **Wireless AP Modes** are given below:

- **Local Mode**
- **Client Mode**
- **Sniffer**
- **SE-Connect**
- **Rogue Detector**
- **Flexconnect**
- **Bridge**
- **Monitor**
- **REAP/H-REAP**

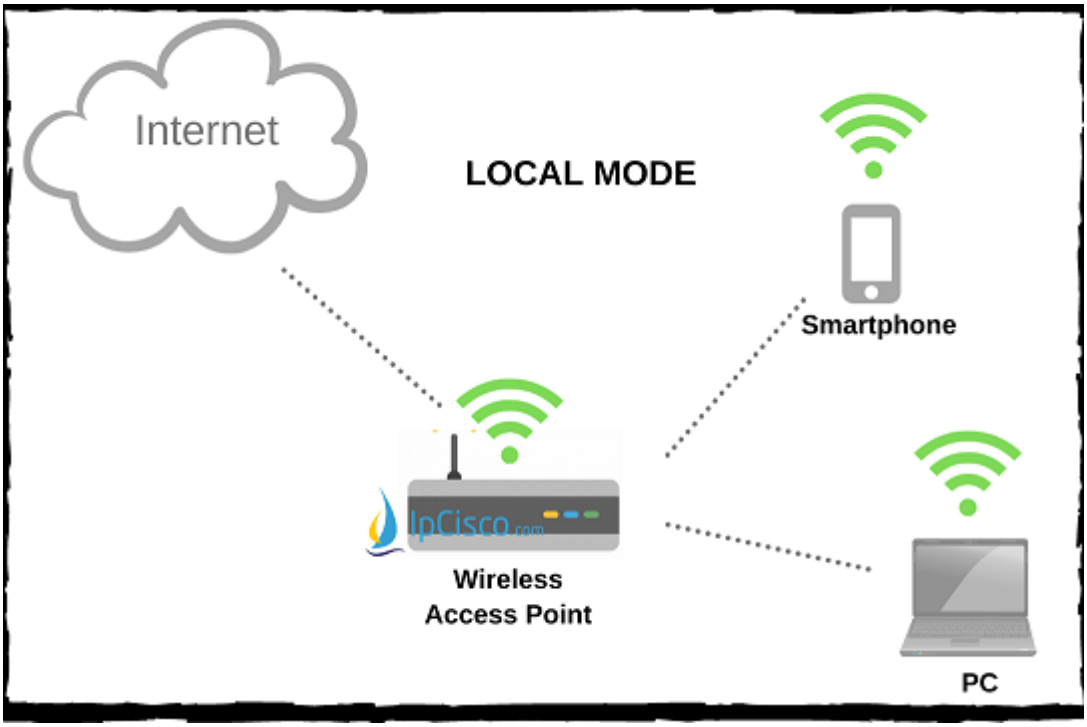
Now, let's talk about a little more about each of these **Wireless AP Modes**.

You can also check **WLC Management Access Connections**

Table of Contents

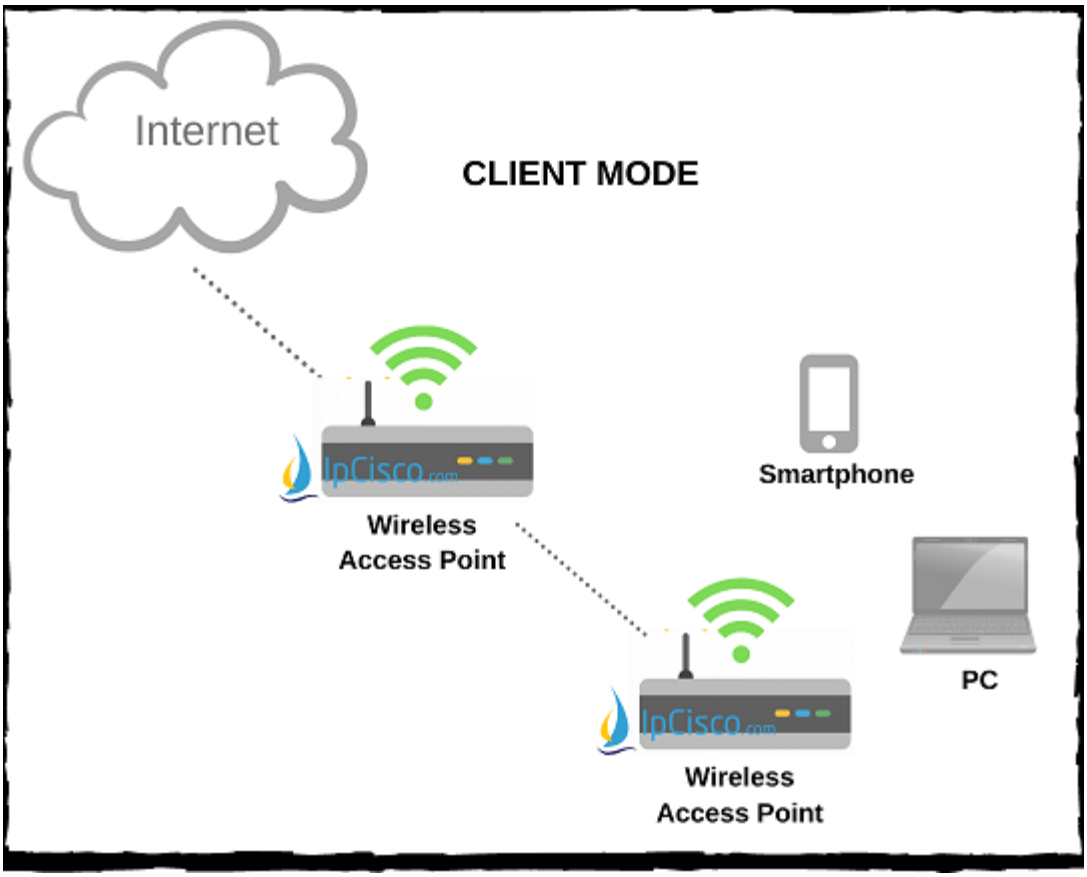
Access Point Mode (Local Mode)

Access Point Mode or in other words **Local Mode** is the basic mode that is used to connect wireless clients like laptops, smartphones,tablets etc. In this modes, clients can communicate with **Access Point**. **Access Point Mode (Local Mode)** is the **default** mode and here Access Point maintains a **Tunnel** towards its Wireless Controller.



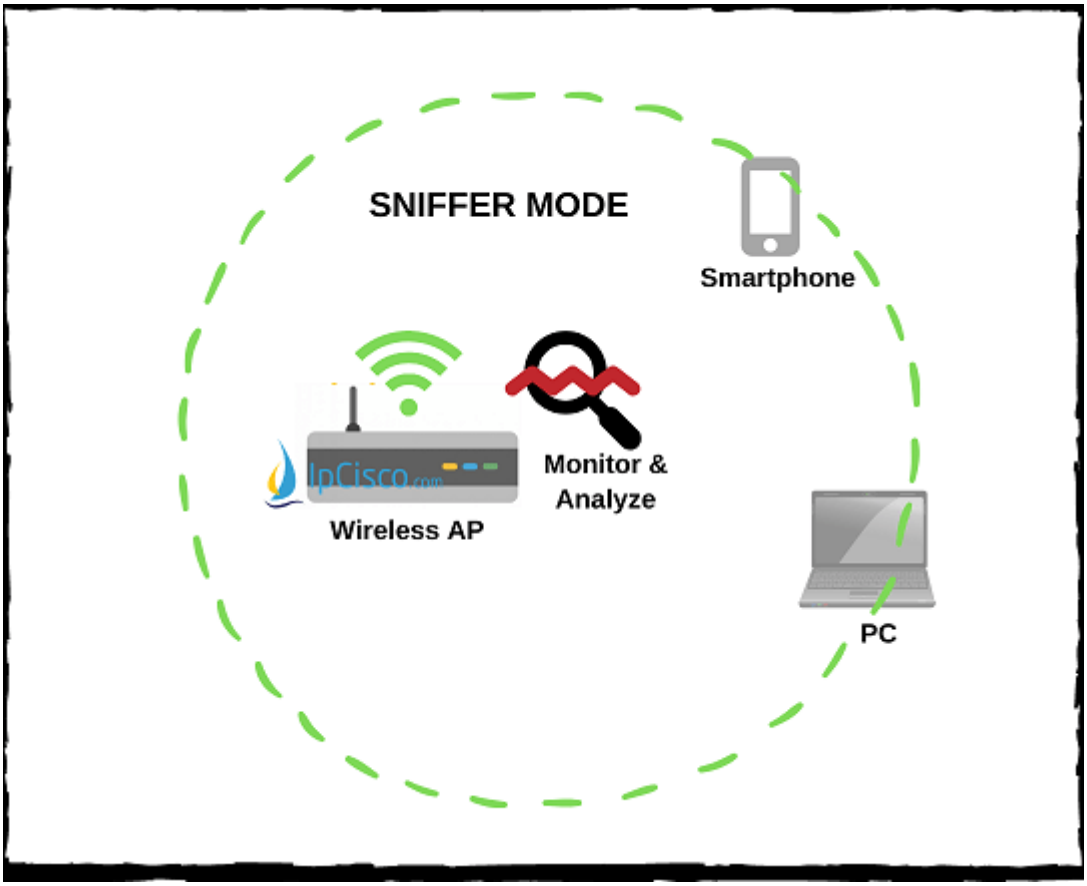
Client Mode

Client Mode is the mode with which access point can connect to another access point as a client. **Client Mode** can be sued in such a scnearion: For example internet of your company is provided by a remote access point and to get internet form this remote access point to your area, you can use your access point in **Client Mode**.



Sniffer

Sniffer Mode is used for troubleshooting activities to monitor and analyze the wireless traffic with various tools like wireshark. It is a passive monitoring mode.

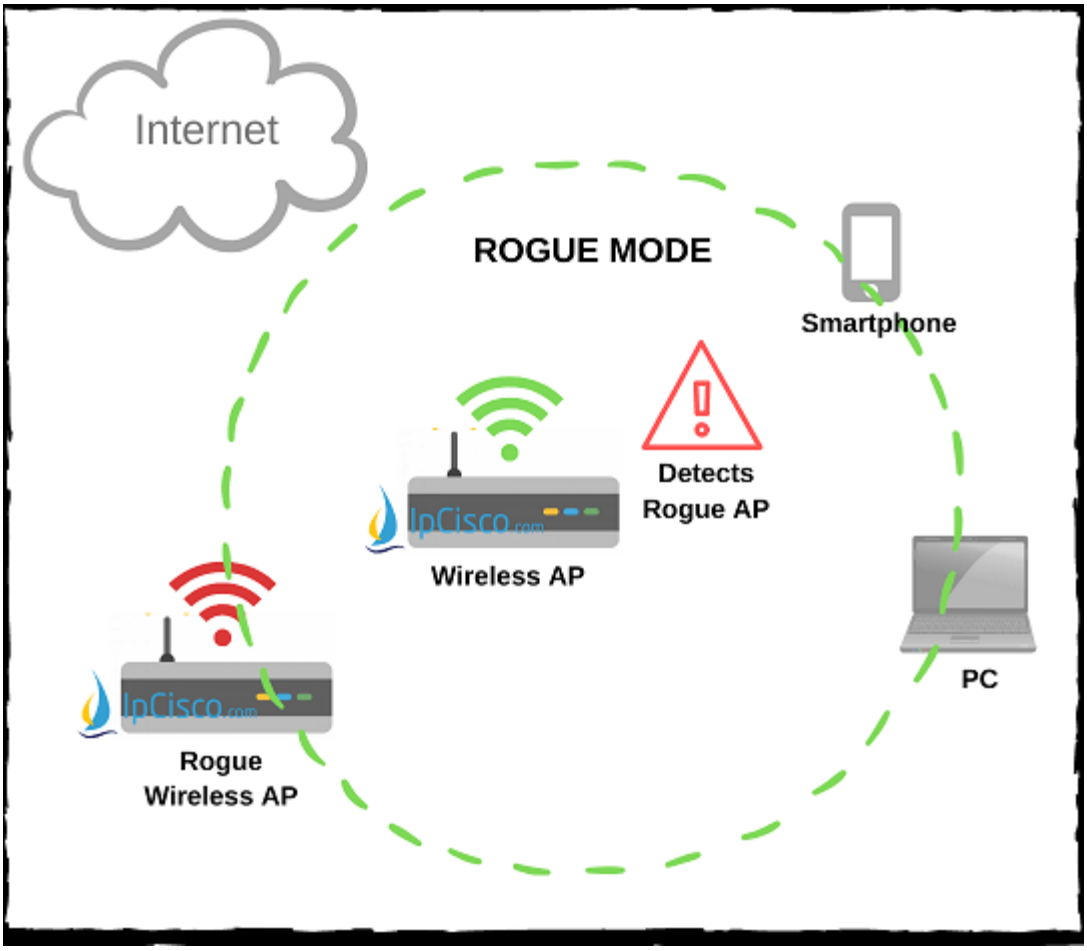


SE-Connect

SE-Connect Mode is the mode with which you can collect information about the RF Spectrum of your wireless connection by connecting Cisco Spectrum Expert. This is a mode that is mainly used for troubleshooting.

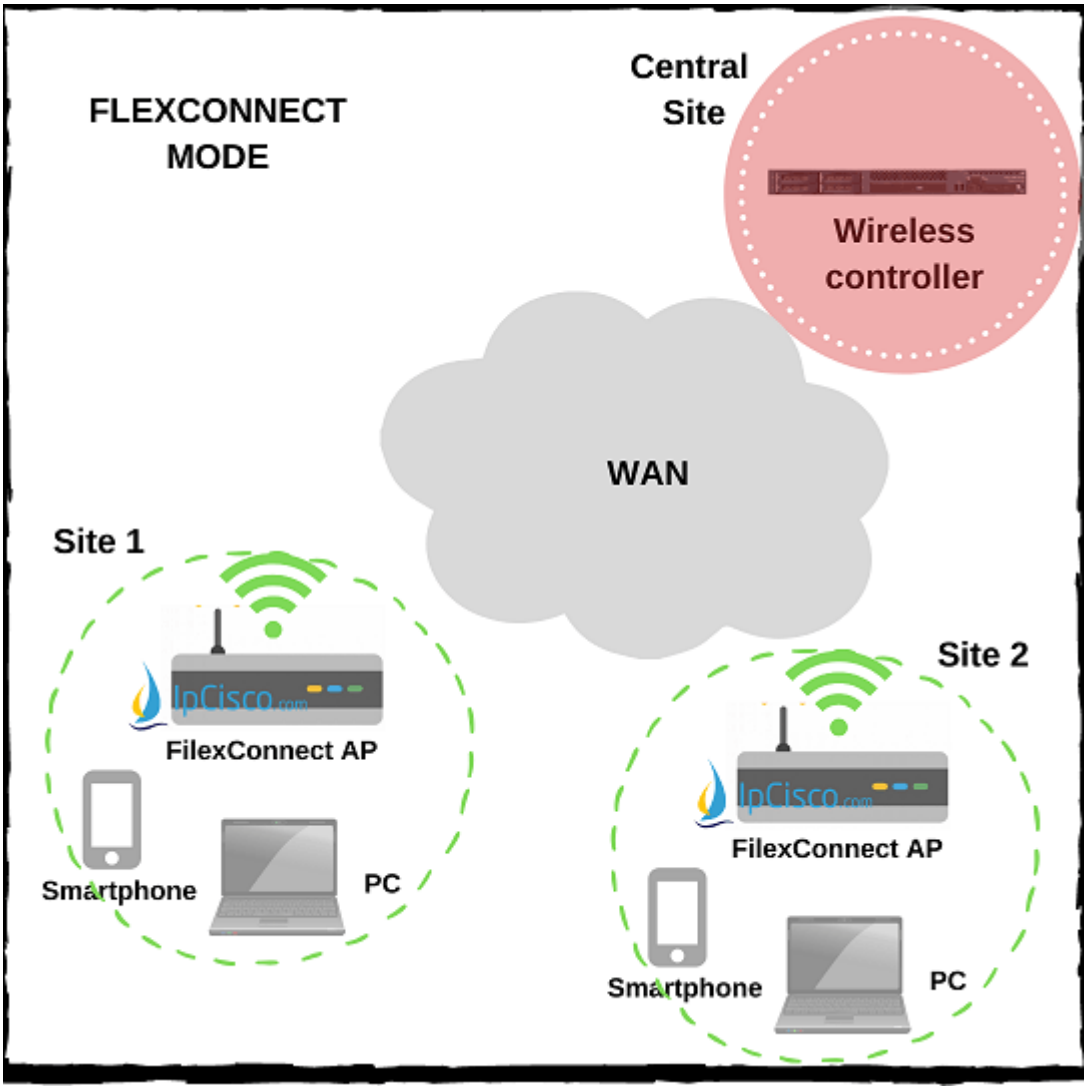
Rogue Detector

Rogue Detector Mode is the Access Point mode that is used to detect rogue devices. This detectiion is done via their MAC addresses.



Flexconnect

If you do not want to use a WLC at every brach, **Flexconnect** mode is the mode that you should use. With this **Flexconnect** mode, your Access Points do not need to connect WLC always. Even if your connection is lost to WLC, then it continues to switch your traffic locally without WLC.



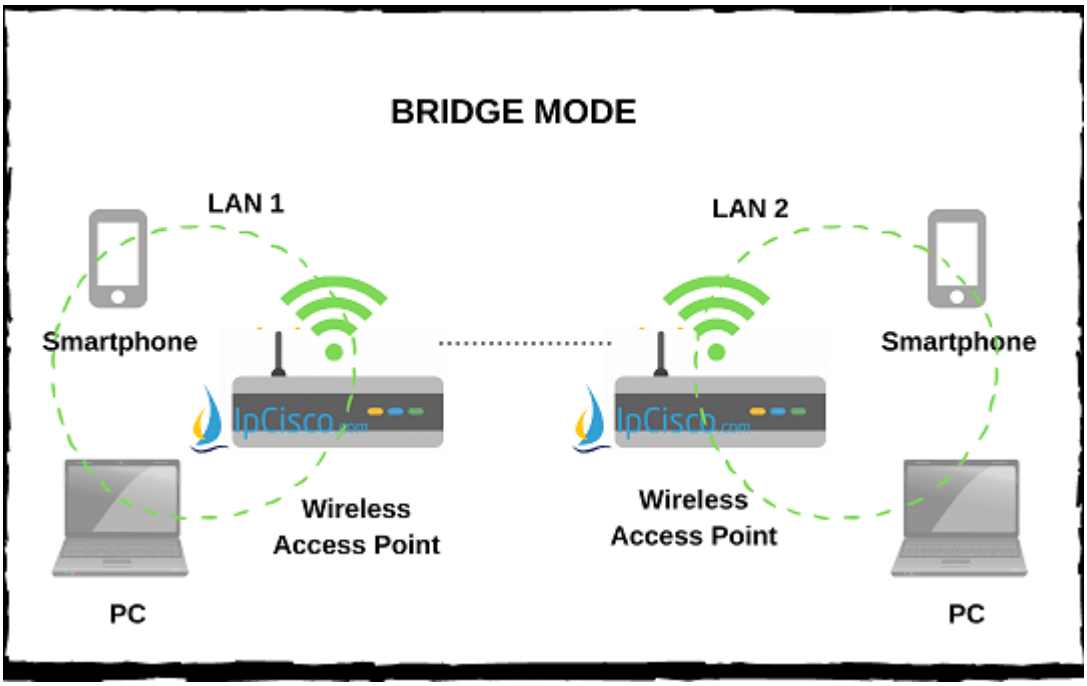
Bridge

In **Bridge Mode**, **Access Points** are used to connect **two** networks. There are **two sub modes** coming with Bridge mode. There are:

- **Point-to-Point**
- **Point-to-Multipoint**

With **Point-to-Point Bridge** Mode, we can connect the LAN of a router to a remote access-point.

With **Point-to-Multipoint Bridge** Mode, we can connect two LANs with one wireless link.



Wireless Security Protocols

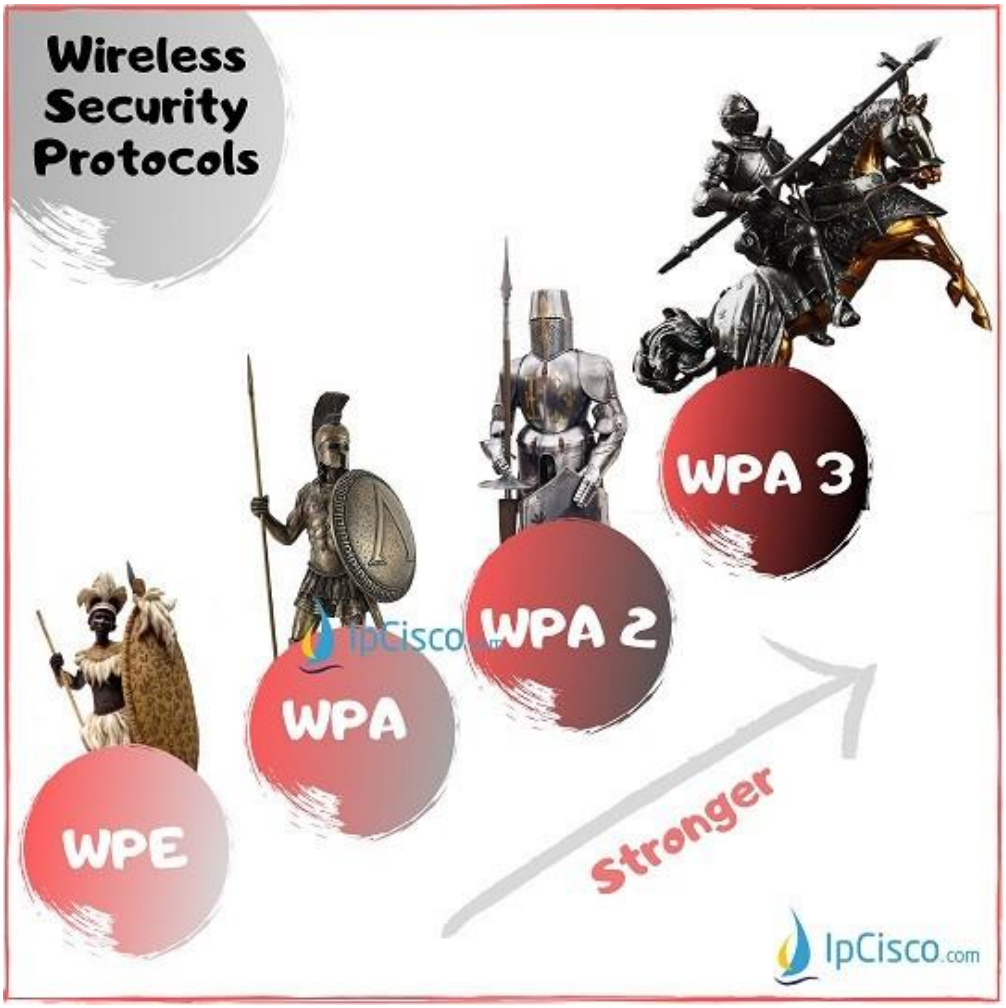


Table of Contents

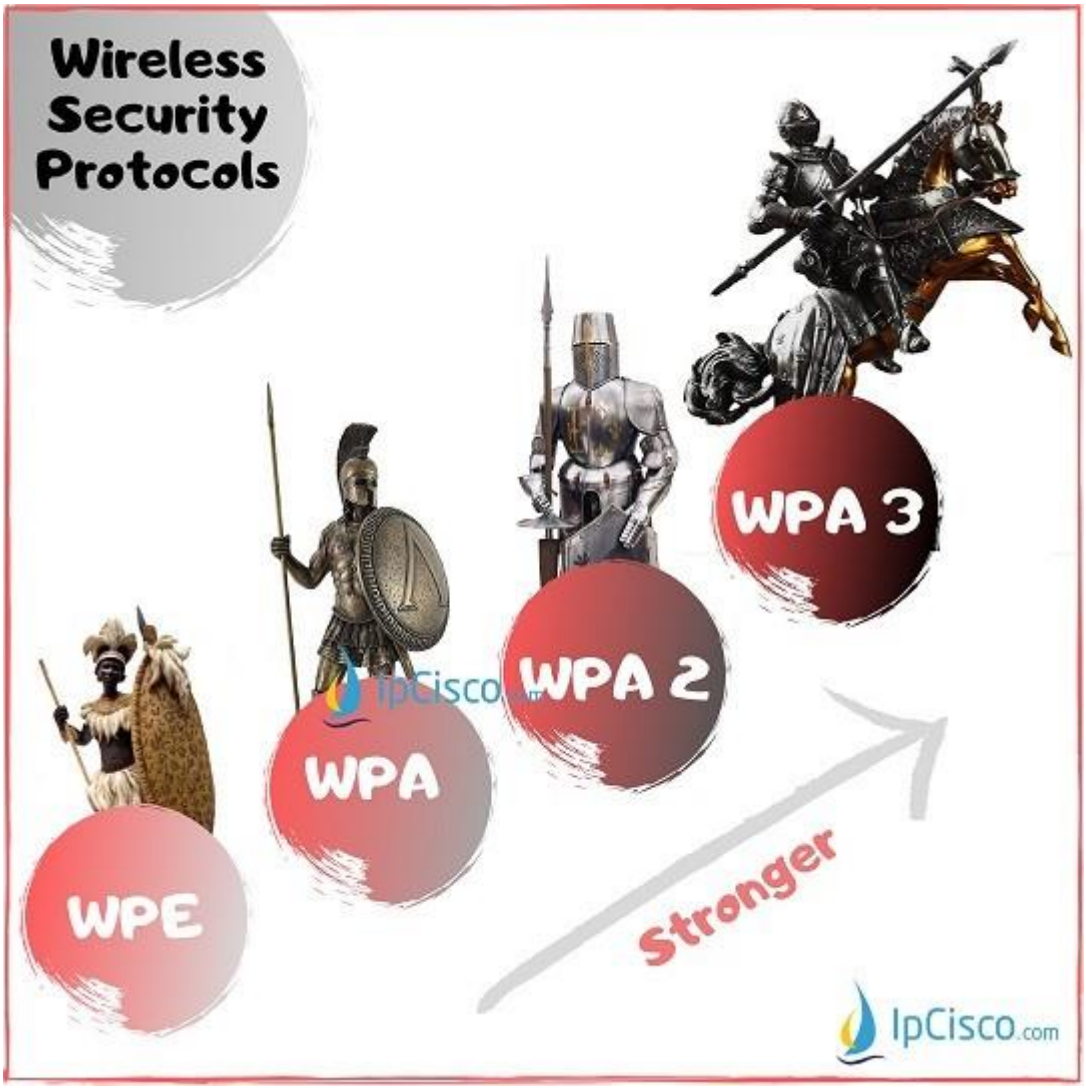
What are the Wireless Security Protocols?

In **Wireless LANs**, Access Point **Passwords** are important. But passwords are only the half of the security. **Password Encryption** is the second half. So,

according to used **Password Encryption**, your system is vulnerable, secured or more secured. To achieve various security levels, different password encryptions are used. So what are these **Wireless Security Protocols?** These **Wireless Security Protocols** are **WEP, WPA, WPA2** and **WPA3**.

- **WEP (Wired Equivalent Privacy)**
- **WPA (Wi-Fi Protected Access)**
- **WPA2 (Wi-Fi Protected Access 2)**
- **WPA3 (Wi-Fi Protected Access 3)**

Now, let's talk about these **Wireless Security Protocols** detailly.



You can also check **WLC Management Access Connections**

WEP (Wired Equivalent Privacy)

WEP (Wired Equivalent Privacy) is the first of **Wireless Security Protocols**. It has developed at 1999. It was developed to protect the wireless data between **Clients** and **Access Points (APs)** towards **hackers**.

At the beginning maximum 64-bit encryption was allowed in US. So, WEP was using **64-bit** encryption. After the restrictions, **128-bit** and **256-bit** WEP has developed.

WEP was widely used but it has too vulnerable to the **password hacks**. Cybersecurity experts detect many vulnerabilities of this first Wireless Security Protocol. So, Wi-Fi Alliance retired it offically at 2004. For today's World **WEP (Wired Equivalent Privacy)** is not a secure protocol and it is outdated.

WPA (Wi-Fi Protected Access 1)

Wi-Fi Protected Access (WPA) was developed at 2003 by Wi-Fi Alliance. Because of the vulnerabilities of WEP, a new protocol must be developed. It is done with **Wi-Fi Protected Access (WPA)**. **WPA** was using **256-bit WPA-PSK (Pre-Shared Key).**

With **WPA**, some additional security mechanisms has developed. Two of these new security mechanisms are "**Message Integrity Check**" and "**Temporal Key Integrity Protocol (TKIP)**". With **Message Integrity Check** mechanism, the message content became more secure towards hackers. With **TKIP**, key system had changed top **Per-Packet**. After a while instead of TKIP, **AES (Advanced Encryption Standard)** would be used.

There was **two** different modes of WPA. One of these WPA modes is used for **Enterprises** and the other is used for **Individuals**. These **WPA Modes** are:

- **Enterprise Mode (WPA-EAP)**
- **Personal Mode (WPA-PSK)**

Enterprise Mode, WPA-EAP was used for **Enterprises.** It was used with **Extensible Authentication Protocol (EAP)** and because of this it was more secured. WPA Enterprise mode was needed an Authentication Server.

Personal Mode, WPA-PSK was used for **Individuals**. Pre shared keys was used with this mode. The implementation and management of this mode was easier.

Althought **WPA** is more secure then **WEP**, it was not enought. Different security vulnerabilities was detected on **Wi-Fi Protected Access (WPA).**

WPA2 (Wi-Fi Protected Access 2)

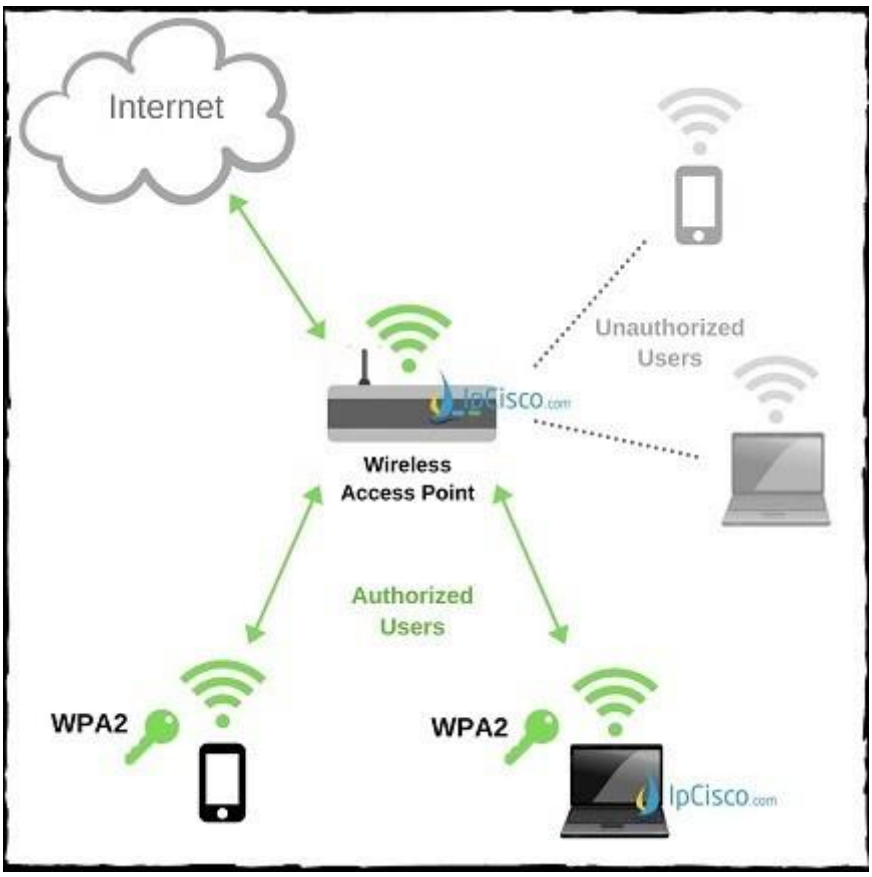
WPA2 (Wi-Fi Protected Access 2) has developed at 2006. It was advanced version of first WPA. Vulnerable parts of WPA become stronger with **WPA2**.

WPA2 offered new encryption and authentication mechanisms to provide more secured networks. These mechanisms was **AES (Advanced Encryption Standard)** and **CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol).** These mechanisms was being used instead of previous mechanism TKIP. For interoparability, TKIP was also used but as a fallback.

AES (Advanced Encryption Standard) had improved by United States Goverment. The main aim of this protocols was encrypting the top secret information. After a while, it is thought that using AES on small networks could also improve the security. And it is.

What is more with **WPA2**? There are also other improvements. For example, Clients can move from one Access Point to another Access Point with no reauthentication. Pre authentication or Pairwise Master Key can be used for this.

WPA2 can be good for **Home networks** but it is vulnerable for **Enterprise networks**. Because, attackers can have access to the network secured with WPA2. After accessing the network they can access passwords. **Dictionaty Attacks** are the most vulnerable part of WPA2 for passwords.



WPA3 (Wi-Fi Protected Access 3)

The last developed Security Standard for Wireless is **WPA3 (Wi-Fi Protected Access 3). WPA3** offers improved authentication and encryption. It will be used more with **802.11ax** standard. **WPA3** will be mandatory with **Wi-Fi 6**.

With **Wi-Fi 6**, better security will be needed and there will be more wireless devices. So, with these requirements security will become more important and **WPA3** will be used with **Wi-Fi 6.**

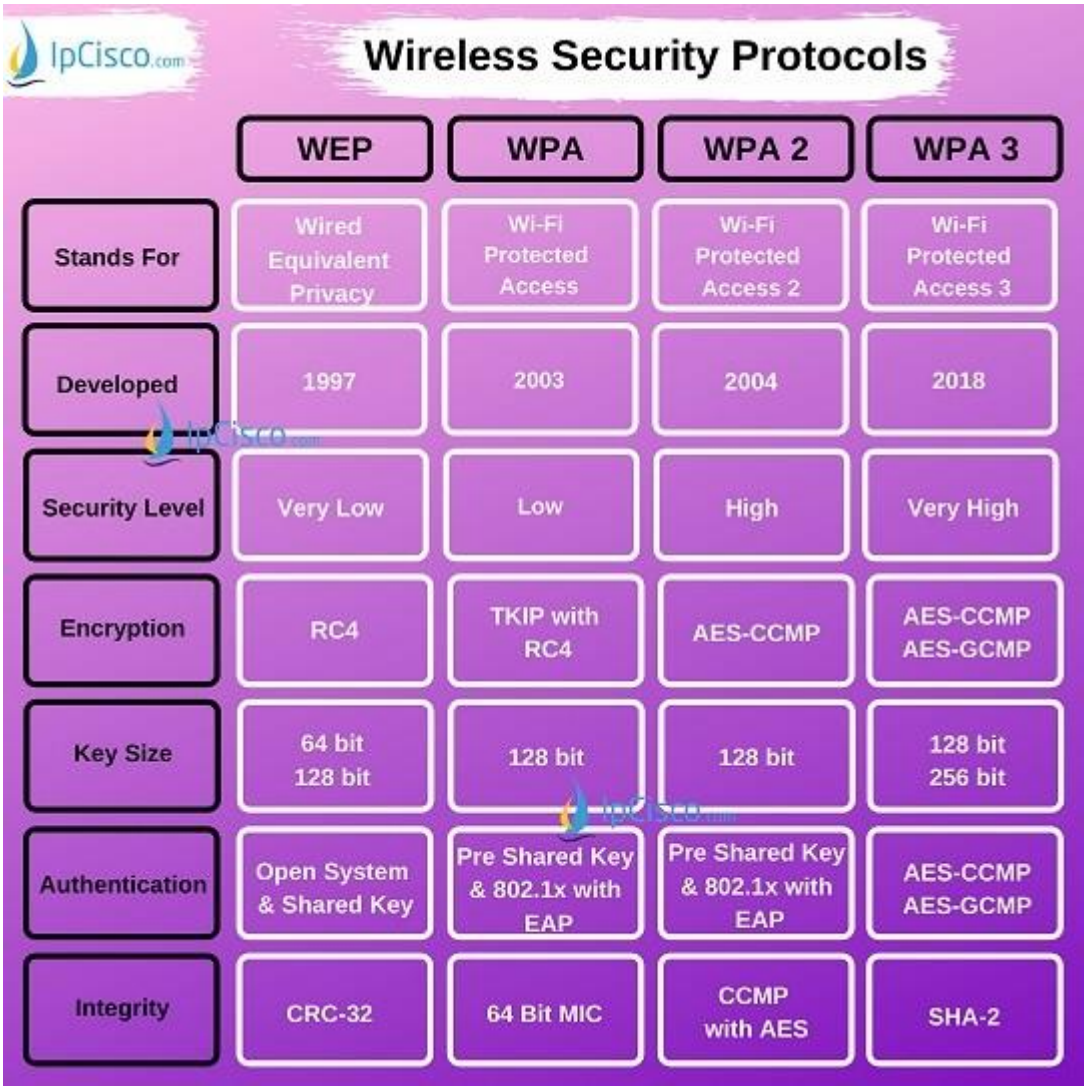
There is also another improvement with this **WPA3**. This is **OWE (Opportunistic Wireless Encryption). OWE** is a technology that is developed for **Public Networks**. With this technology, auto encryption will be done without user intervention. Think about this. You are in Starbucks and working with your PC. With WPA2, any attacker in the same public place with you, can do a **Man-in-the-Middle attack** towards your system. They can start a **Dictionary Attack** for your password. With **WPA3,** it is prevented.

WPA2 is vulnerable to **Dictionary Attacks** that is used to predict password with many different attempts. **Hackers** can do this atteck even if they are not in the same network with the victim. To prohibit this type of attack, **WPA3** offers a new **Key Exchange Protocol**. With this protocol, it will use a secure way, Simultaneous Authentication of Equal handshake. Before, with **WPA2**, Four way Handshake was being used and this is vulnerable.

WPA3 provide extra security and encryption if you compare with **WPA2**. With **WPA3**, **all the traffic** between you and and the other end will be **encrypted**, till the other end authenticated.

There is also another new connection type that is coming with WPA3. With this new type, you can use th **QR Codes** to connect the devices to the networks. For example, you can use your smart phone to scan the **QR Codes** of Printers, Access Points etc and you are connected after that to the access point,printer sor any ot devcei that will be in our lives with **Internet of Things (IoT)**. This type of communication will require extra security. So, **WPA3** is a good solution for this.

Comparison of Wireless Security Protocols



You can find a good comparison table for WEP, WPA, WPA2 and WPA3. In this table, you can find all the key differences of these **Wireless Security Protocols**

WIRELESS SECURITY

WEP

WIRED EQUIVALENT PRIVACY

Developed at 1999, retired at 2004 officially. Vulnerable to the password hacks. Not secure for todays network world. Not used today.

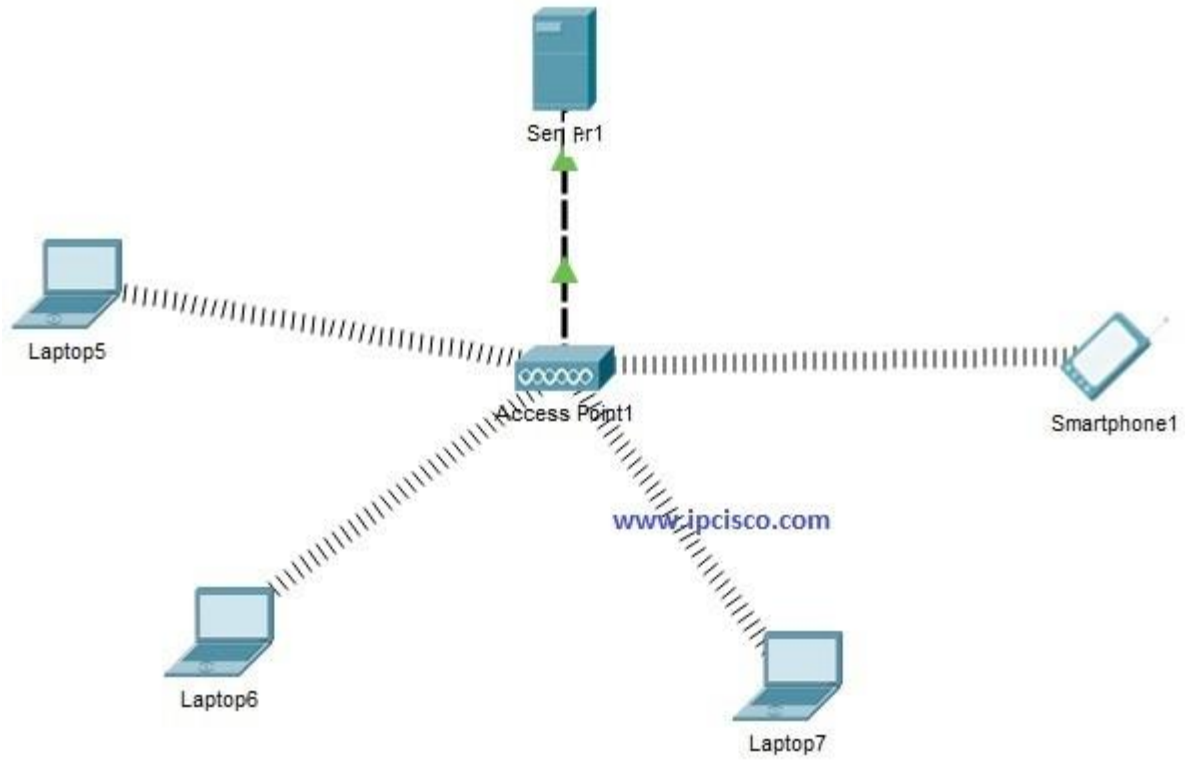
WI-FI PROTECTED ACCESS

Developed at 2003 because of the vulnerabilities of WEP. New security mechanisms are "Message Integrity Check" and "Temporal Key Integrity Protocol (TKIP). Has two different modes : Enterprise Mode (WPA-EAP) and Personal Mode (WPA-PSK). Has Vulnerabilities.

WPA

WI-FI PROTECTED

WLAN Configuration on Packet Tracer



Cisco WLAN Configuration

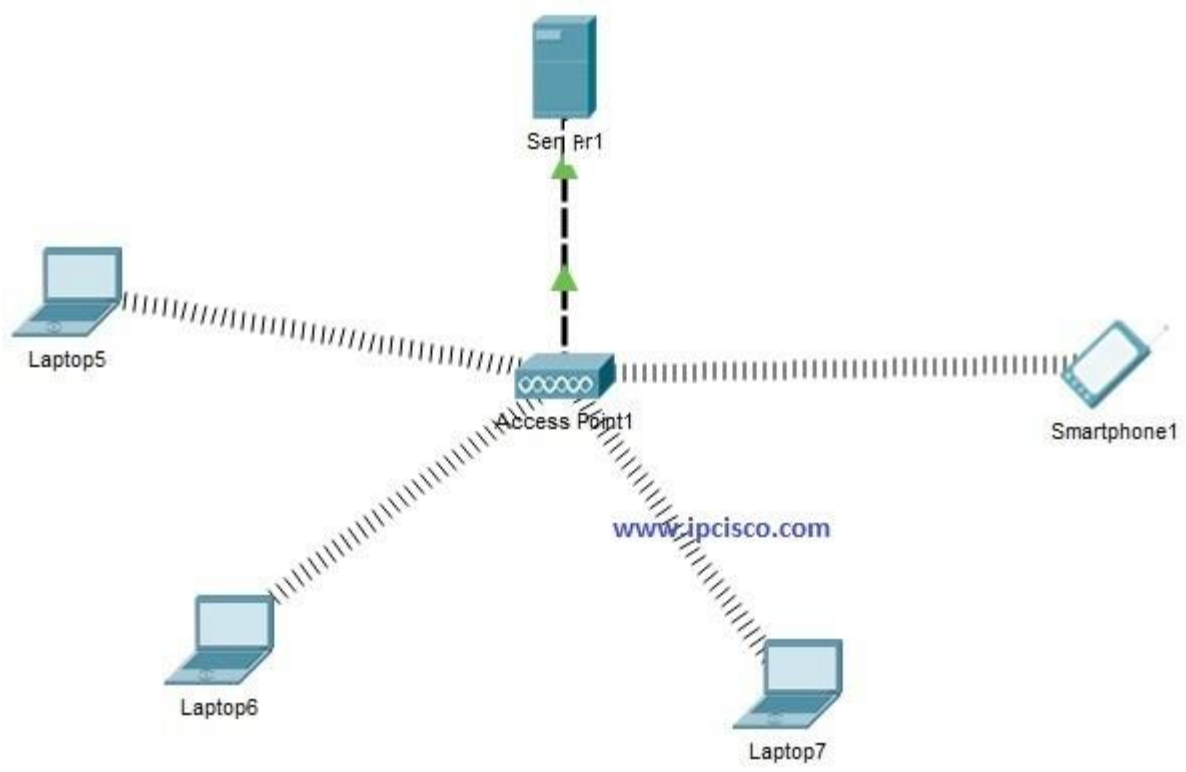
WLANs (Wireless LANs) are very common in today's World. Everywhere there are a lot of wireless networks. Even now, you are in many of these wireless signals. It is not an healthty life but they are in our lives. In this lesson we will focus **WLAN Packet Tracer Configuration** and we will learn **How to Configure a WLAN on Packet Tracer**.

For Our **WLAN Configuration on Packet Tracer**, we will use the below topology that is consist of one One Wireless Access Point, One Server , Three Laptops and One Smartphone. Smartphones are everywhere, even in **Cisco Packet Tracer** for many years :)

You can reach all Cisco packet tracer config files on **Cisco Packet Tracer Lab** Page.

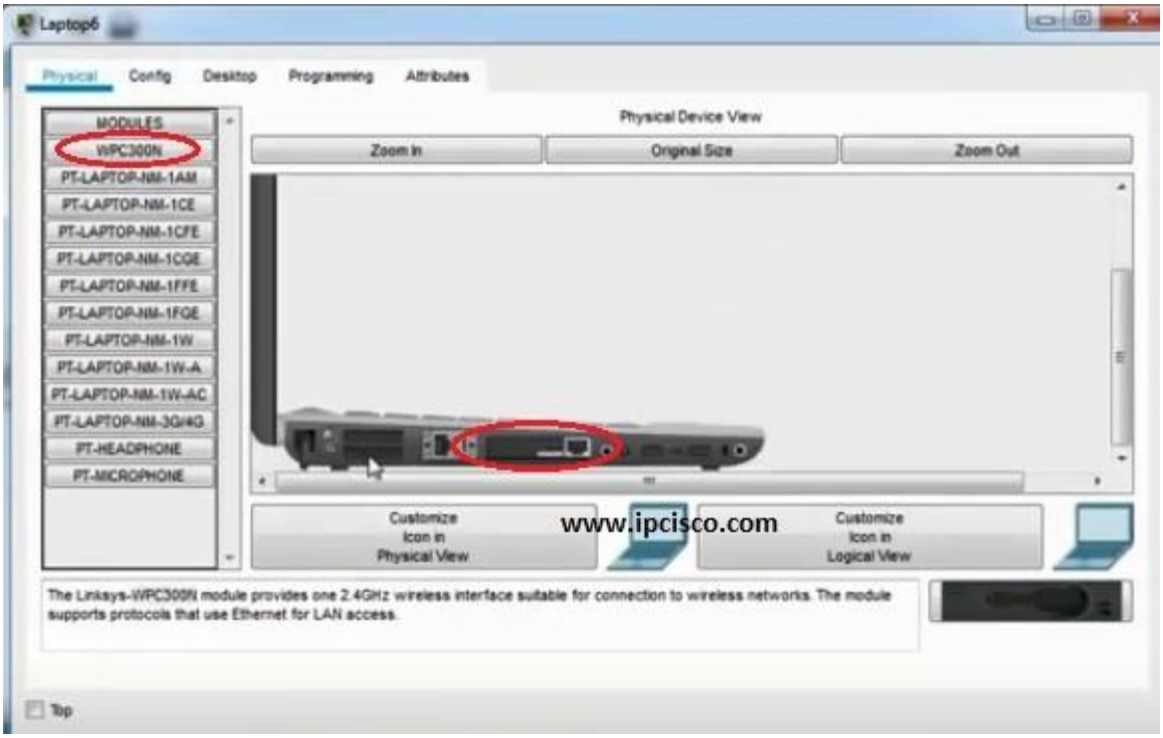
Now, let's sumamrize what will we do for **Packet Tracer WLAN Configuration** :

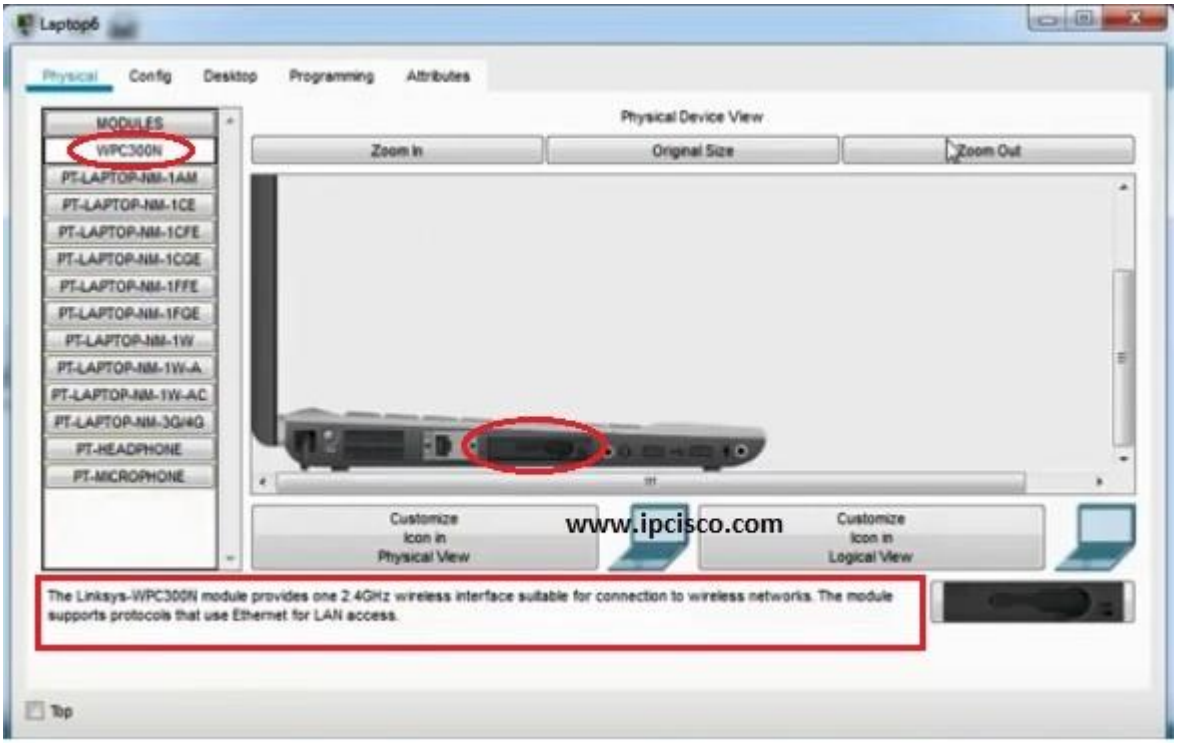
- **Place Wireless Interface Card to Laptops**
- **IP Check on WLAN Devices**
- **DHCP Server Configuration**
- **IP Check on WLAN Devices again**



Place Wireless Interface Card to Laptops

By **default** laptops has classic **Ethernet card**. To involve in a wireless network, we should have wireless interface card. So, in each laptop, we should turn off the laptop, remove the classical Ethernet, instead of it we place **Wireless Interface Card (WPC300N)**. Then, we power on the laptop again.





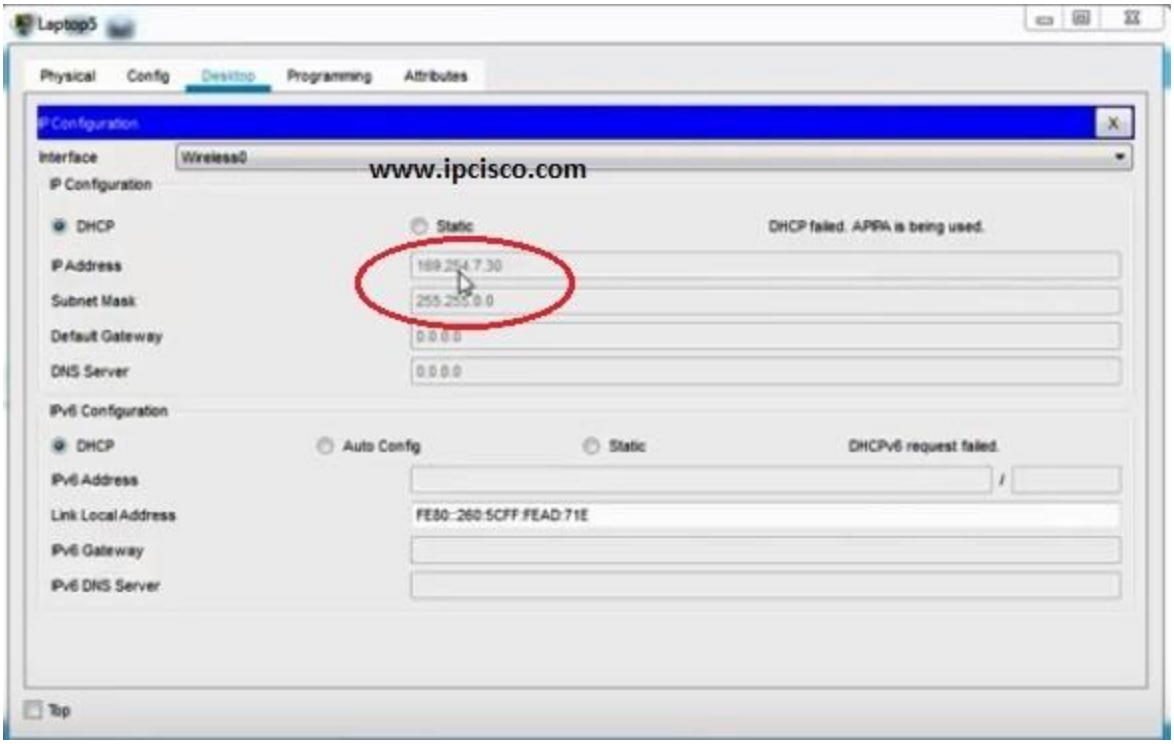
After this processi each laptop connects to th wireless Access Point in Packet Tracer. Smartphone devices in Packet Tracer connects to **Access Points (AP)** by default. So, there is nothing to do on them.

You can also check **GNS3 COnfigurations Lab** Page

IP Check on WLAN Devices

We will check the IPm addresses of the laptops. For now, chekcing only one of them is enough. Because, at the beginning if there is no Static IP Configuration and no DHCP, an IP from a special block is assigned to the devices. This is **APIPA (Automatic Private IP Addressing)** addresses. These addresses

are from the block "**169.254.x.x/25**". Simple, when we say this type of IP address in a device, we can say that it has no IP address.

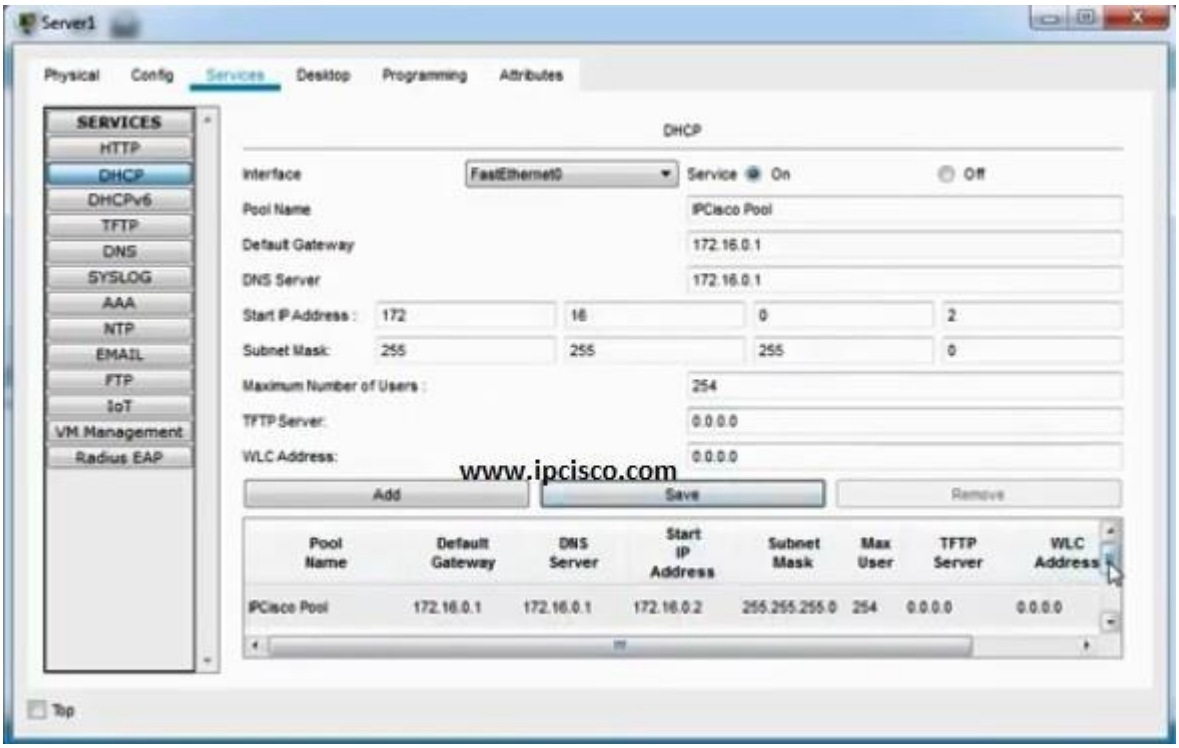


DHCP Server Configuration

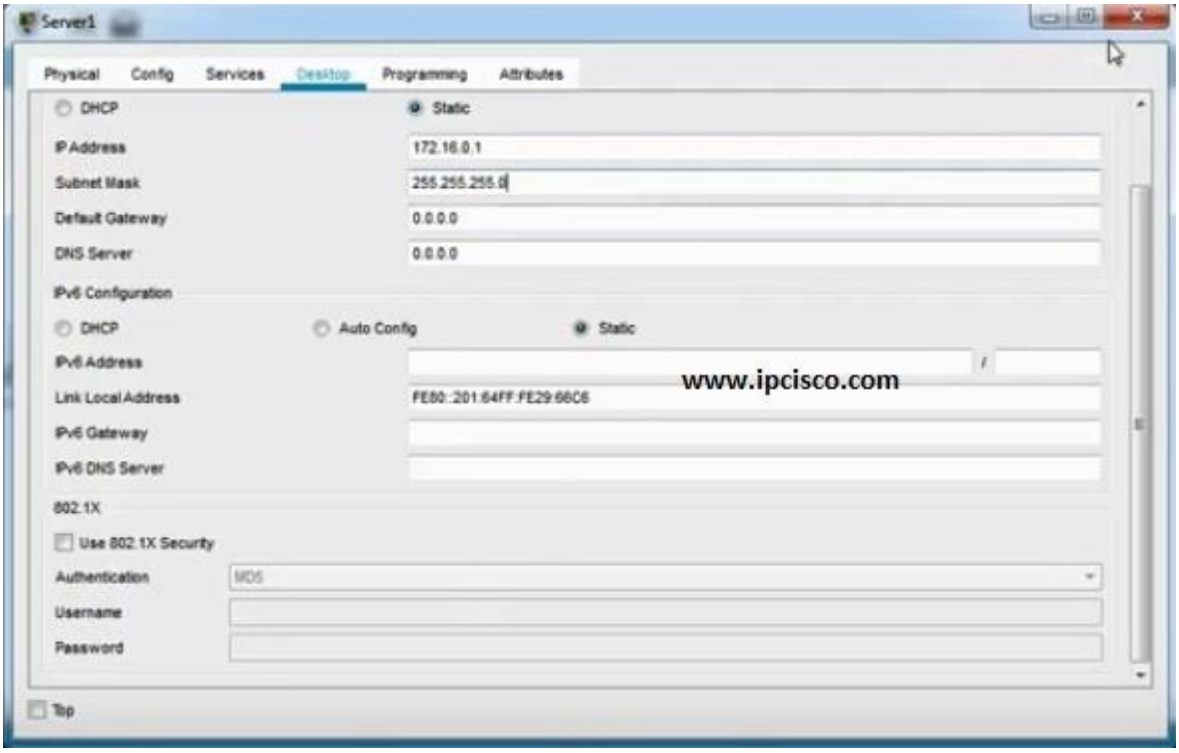
In this step, we will configure our **DHCP Server** in the WLAN. This server will give IP addresses to our devices who are connected to the **Access Point**.

In the Services tab of Server, we will go through the DHCP at the left hand. In here, we will define our IP Pool. For this configuration example our DHCP Pool's name is "**IPCisco Pool**". Beside, we will configure the **Default Gateway, DNS Server IP** addresses. After that we will configure the **starting IP** and **Subnet Mask**. DHCP server will start IP asssignition with this IP. And for this example, we have created **254** IP for our IP Pool. We also assign this value on this screen.

After this configuration, we should not forget to "**on**" our DHCP Service at the top and then, we add our DHCP Pool to the configuration with "**add**" button.



After DHCP Services configuration on **DHCP Server**, we will configure one more thing on this DHCP Server. This is the IP address and subnet mask of the Server. Here, our Servr IP address will be 172.16.0.1 and the mask will be 255.255.255.0.



DHCP Snooping Configuration on Packet Tracer

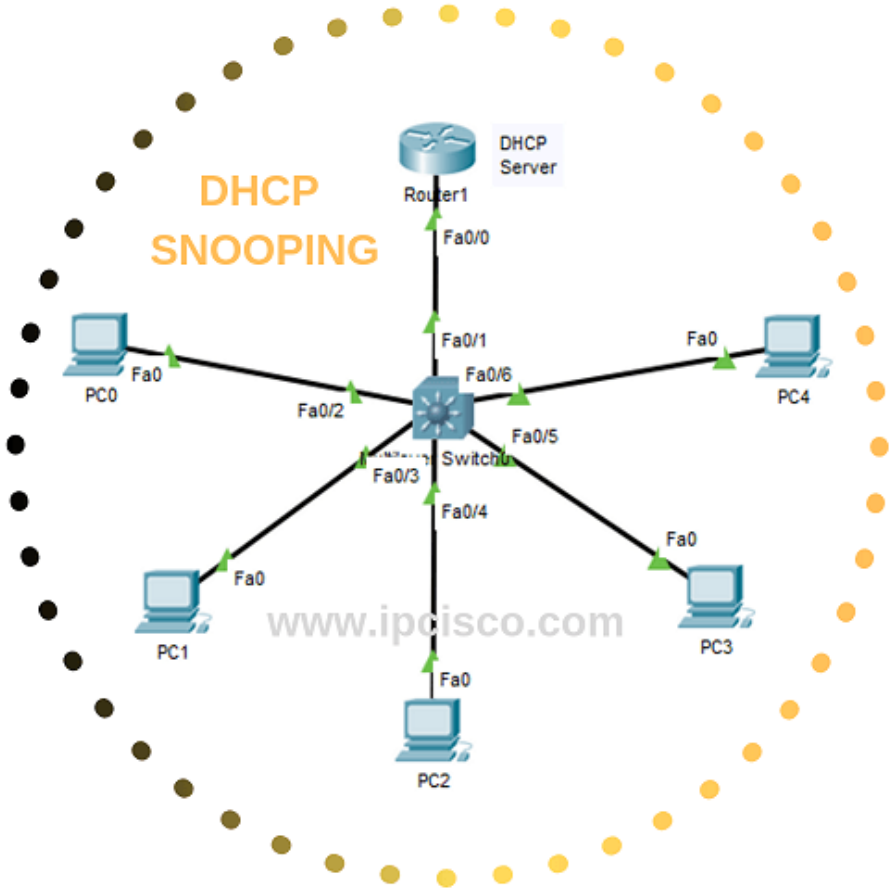


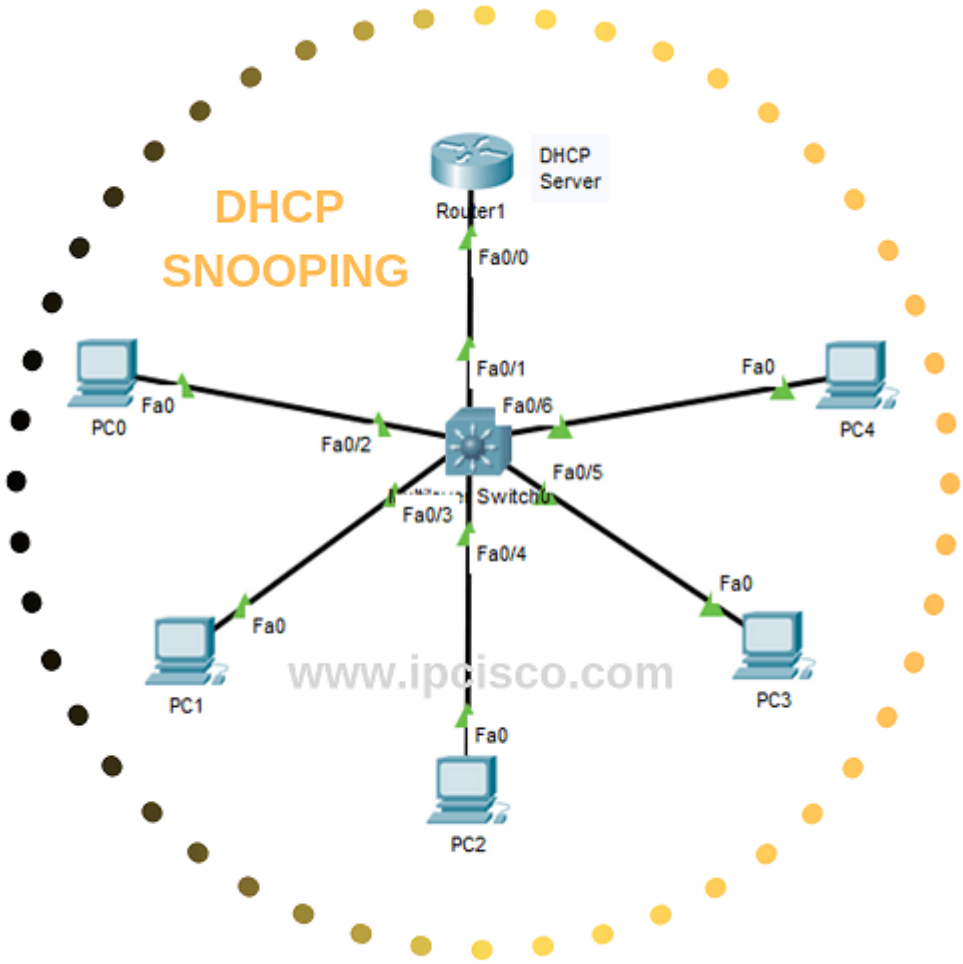
Table of Contents

How to Configure DHCP Snooping on Cisco Switches?

DHCP Snooping Configuration is an important security mechanims towards any malicious **DHCP** attacks. In this lesson, we will learn How to use this

important mechanims and **How to Configure DHCP Snooping** on Cisco swithes.

For our **DHCP Snooping Configuration Example**, we will use the below simple topology:



We will do the configuration below step by step:

- **Interface Configurations**
- **DHCP Pool Creation**
- **Enabling DHCP Snooping**
- **Setting Trusted Ports**
- **Setting Rate Limit**

- **DHCP Snooping Verification**

Now, let's focus on our **DHCP Snooping Example** and learn **DHCP Snooping Config** step by step.

Interface Configurations

Firstly, we will configure interace ip addresses of the router and the switch. Here, router will be our DHCP Server.

```
Router# config terminal
Router(config)# interface fastethernet 0/1
Router(config-if)# ip address 192.168.0.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
```

DHCP Pool Creation

Secondly, we will create our DHCP Server with DHCP Pool with the name XYX. Our DHCP Server will be the router above. And our DHCP Pool addresses will be the ip address in 192.168.0.0/24 block.

```
Router(config)# ip dhcp pool XYZ
```

```
Router(dhcp-config)# network 192.168.0.0 255.255.255.0
Router(dhcp-config)# end
Router# copy run start
```

Enabling DHCP Snooping

Here, we will enable **DHCP Snooping** on the switch. DHCP Snooping will work on it. DHCP Snooping can be enabled globallay with "ip dhcp snooping" command or it can be enabled on a specific or a range of VLANs with "**ip dhcp snooping vlan vlan-id**" command. Here, we will enable DHCP Snooping, globally.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# end
```

Setting Tursted Ports

In **DHCP Snooping** mechanims there are wo port types as we have talke about before in the **DHCP Snooping** lesson. One of them is trusted and the other is untrusted. Here, we will set the trusted ports. Here, simply, we will set one trusted port. The port on the switch that is connected to the **DHCP Server** (router).

We will go to the interface that is connected to the router and set it as trusted port with "**ip dhcp snooping trust**" command.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# end
```

Setting Rate Limit

There is one more important configuration steps here. We can also set DHCP Requests that can be received in a second. If this rate exceeds the configured one, the traffic is dropped. Here,let's set it 20.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# ip dhcp snooping limit rate 20
Switch(config-if)# end
```