Introductory overview of Wi-Fi, WLAN Architecture, Switch, Router, Gateway, Subnet, Firewall & DMZ, and their role in the world of Enterprise Wi-Fi

Suraj Rojanala

Wi-Fi and IEEE 802.11

Wi-Fi is an IEEE 802.11-based wireless certification set that allows connections between Wi-Fi capable devices and communications between them through radio frequency signals using half-duplex (cannot send and receive at same time) wireless communication. IEEE 802.11 is the standard on which the Wi-Fi certifications are based.

Radio Frequency waves are electromagnetic waves occurring on the radio frequency portion of the electromagnetic spectrum, which ranges from about 3 kHz to 300 GHz in most definitions, and these RF waves are characterized by certain properties such as wavelength, frequency, amplitude, and phase. Some of these properties are used to encode and modulate the data onto the RF wave. As shown in the figure below, Wi-Fi operates between 300MHz to 60GHz of the RF spectrum

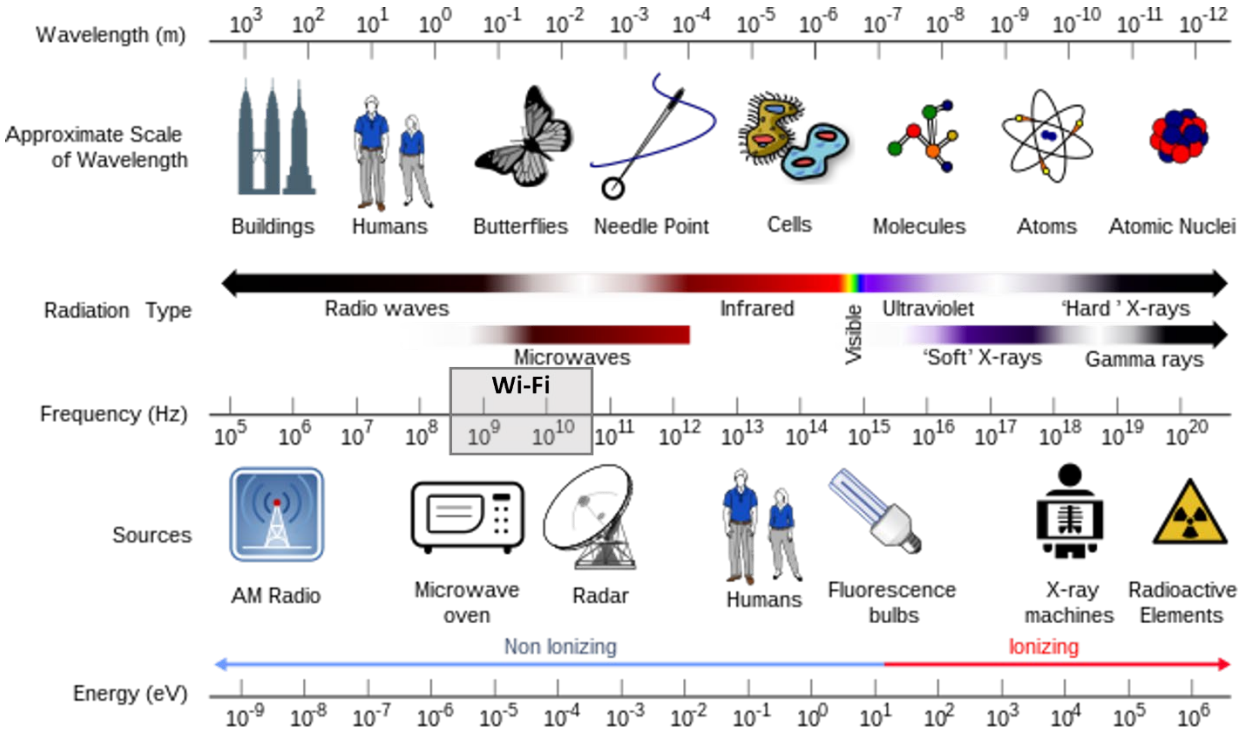

Figure: RF Spectrum (SOURCE: Wikimedia Commons with modification)

This 802.11 Wireless technology (Wi-Fi) defines communication mechanisms only at the physical layer (layer 1) and the MAC sublayer of the data-link layer (layer 2) of the OSI model. Since Wi-Fi operates at layer 2 and below the exchange unit used for communication is called a **wireless frame** and the Wi-Fi capable devices use these frames to communicate data between them.

The Wi-Fi capable device (access point, smart phone, laptop, etc.) radiates the RF signal from the antenna(s) which must be transmitted with enough power so that it is received and understood by the receiver. Of course, different antennas radiate the signal in different patterns and the radiated RF signal loses its power as the RF wave travel outwards (free space path loss) or when it encounters an obstacle

based on the propagation behaviors (absorption, reflection, scattering, refraction, and diffraction) of the RF wave.

802.11 Topologies

The three primary 802.11 are types or network structures are listed below

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

Basic Service Set (BSS):

An **infrastructure BSS** (the structure that uses the simple acronym BSS) is a group of wireless devices served by a single access point that may use a distribution system for interconnection with other networks. All the devices in a BSS use the same channel to communicate. An **independent BSS (IBSS)** is a group of wireless devices interconnecting and communicating without the use of an access point and without the use of a distribution system for interconnection with other networks (covered more later).

Every BSS has a string logical name that is advertised by the access point, according to the 802.11 standard. This Identifier is called a **Service Set Identifier (SSID)**. The SSID is the network name of the network in which the BSS is participating in nearly all deployments (even if the network is a single BSS). The layer 2 identifier of each individual BSS is the 48-bit MAC address of the radio network interface of an access point serving the BSS, which is defined as the **Basic Service Set Identifier (BSSID).** The physical area of coverage provided by an access point in a BSS is known as the **Basic Service Area (BSA)**. The BSA is the area in which client stations may successfully locate, connect to, and communicate with the access point.

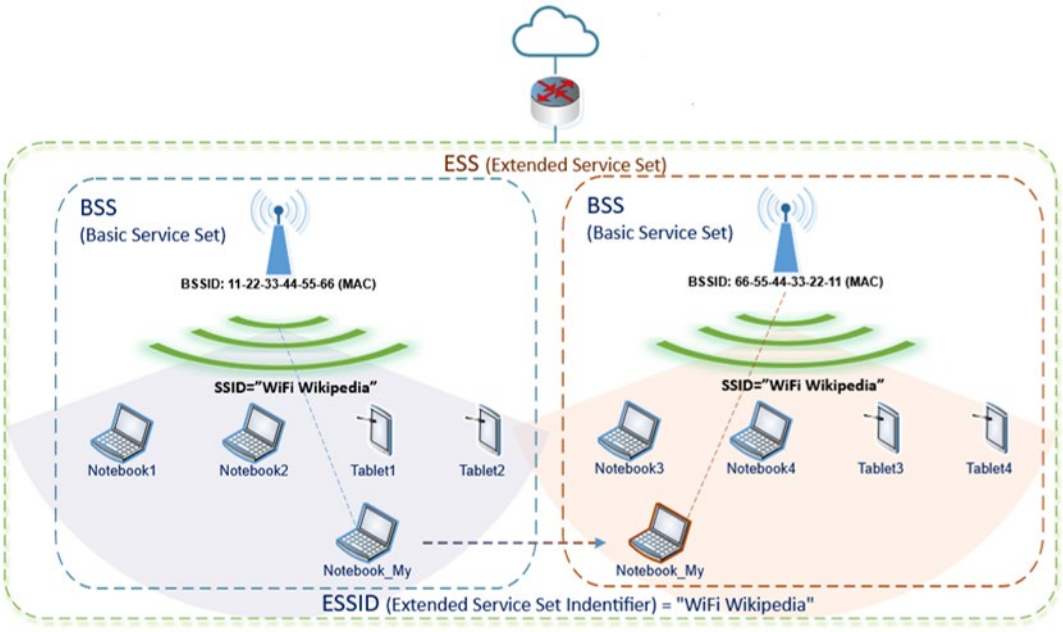

Figure: BSS and ESS (SOURCE: Wikimedia Commons)

Extended Service Set (ESS):

An **Extended Service Set (ESS)** is one or more Basic Service Sets connected by a **distribution system medium (DSM)**. Usually, an extended service set is a collection of multiple access points and their associated client stations, all united by a single DSM. The DSM is usually an 802.3 Ethernet network used to interconnect the access points and provide access to other resources as well. However, the DSM may use other networking technologies, both wired and wireless, as well.

The most common example of an ESS has access points with partially overlapping coverage cells (BSAs) to provide seamless roaming to the wireless client stations. In nearly all extended service sets, the access points all share the same SSID name. The network name of an ESS is often called an **Extended service set identifier (ESSID)**, though this is not a term used in the 802.11 standard for traditional wireless LANs. Networks that use the new Fast Initial Link Setup (FILS) options may use a homogeneous ESSID (HESSID) in the FILS indication element of a frame, so the term ESSID has become part of the standard as well for those deployments. This latter option would be implemented most commonly for interworking with external networks as defined in section 11.22 of the 802.11-2020 standard.

Independent Basic Service Set (IBSS):

An IBSS, as explained previously, is an 802.11 topology where client stations can directly communicate without any need of an access point. An IBSS network consists solely of client stations and is also called an **adhoc** or **peer-to-peer** network. The first station that starts up an IBSS randomly generates a BSSID in the MAC address format. This randomly generated BSSID is a virtual MAC address and is used for layer 2 Identification purposes within the IBSS.

Access Point:

An access point is a half-duplex portal device that directs traffic either to the network backbone (wired medium) or back into the wireless medium, depending on the destination. In simple terms, an access point is a hub with a radio card and an antenna or antennas. The radio card inside an access point must contend for the half-duplex medium in the same fashion as the client station radio, hence the term half-duplex.

How Data is transferred between wireless and wired mediums by Access point:

Being a layer 2 device, an access point uses layer 2 addressing scheme of the wireless frames to eventually forward the layer 3-7 information which is the payload of a wireless 802.11 data frame. This upper layer information that is contained in the body of an 802.11 data frame is called the MAC service data unit (MSDU). The eventual destination of this payload is usually to a wired network device through a wired infrastructure. Because the wired infrastructure is a different physical medium, an 802.11 data frame must be effectively converted into an 802.3 ethernet frame which is done by the 802.11 *integration service.*

The job of the integration service is to remove the 802.11 header and trailer and then encase the MSDU payload inside an 802.3 frame. The 802.3 frame is then sent on the Ethernet network. The integration service performs the same action in reverse when an 802.3 frame payload must be converted into an 802.11 frame that is eventually transferred by the access point radio.

If 802.11 user traffic is forwarded at the edge of the network, the integration service exists in an access point. The integration service mechanism normally takes place inside a WLAN controller when 802.11

user traffic is tunneled back to a WLAN controller. So, the location of the integration service depends on the wireless LAN architecture being implemented in the network, which in turn depends on the three logical planes (Management, Control and Data) of operation.

What is a WLAN?

A Wireless Local Area Network (WLAN) is a network that uses wireless communications to build a local area network and is defined in the 802.11-2020 standard. WLANs typically use multiple 802.11 access points connected by a wired network backbone. In enterprise deployments, WLANs are used to provide wireless end users with access to the organization's network resources and network services and a gateway to the Internet. To further understand the WLAN architecture types let us look at the below terms:

> *Management Plane*: The functions of the management plane within an 802.11 WLAN include WLAN Configuration, WLAN Monitoring, and reporting.
>
> *Control Plane:* The Control plane is often defined by protocols that provide the intelligence and interaction between equipment in a network. Few examples are Dynamic RF, Roaming Mechanisms, Client load balancing, Mesh Protocols.
>
> *Data plane:* The data plane is where user data is forwarded. The three devices that often participate in the data plane of an enterprise network are the access points, client stations, and WLAN controllers.

These concepts should not be confused with or *absolutely* associated with the control, management, and data frames defined in the 802.11 standard. For example, while data frames are mostly about user data, some data frames, specifically, null data frames, are used for other purpose than the direct transmission of user data.

WLAN Architecture:

WLAN vendors offer three Primary WLAN architectures, and these architectures are differentiated based on where the Management, Control and Data planes operate:

1. Autonomous WLAN Architecture
2. Centralized WLAN Architecture
3. Distributed WLAN Architecture

Autonomous WLAN Architecture:

The **autonomous WLAN architecture** uses standalone access points where all three planes of operation exist and operate on the edge of the network architecture (in the access points). All configuration settings exist in the autonomous access point itself and therefore the management plane resides individually in each autonomous access point.

The integration service within an autonomous access point translates the 802.11 traffic into 802.3 traffic.

Since the access points operate independently of one another, autonomous architectures do not provide important wireless functions like Radio Resource Management (RRM), fast roaming mechanisms (beyond WPA2- and WPA3-Personal), etc.

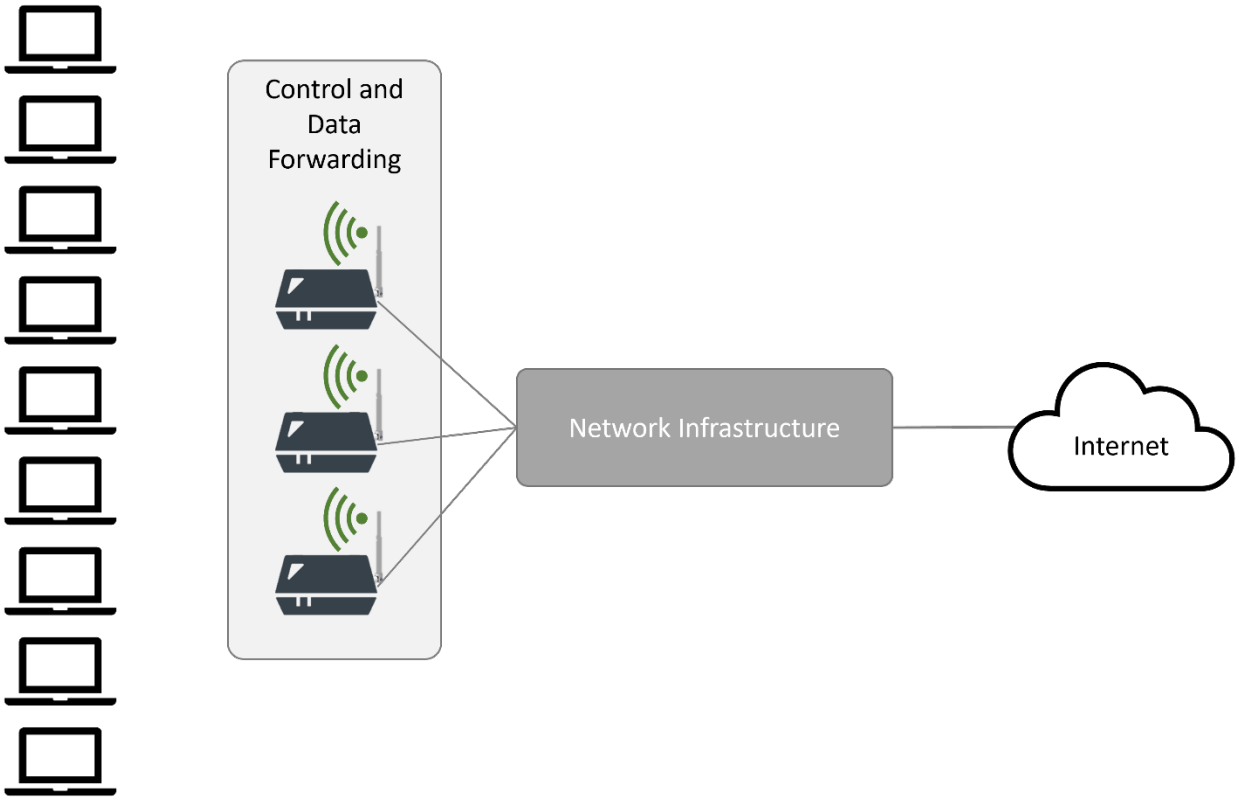

Figure: Autonomous WLAN Architecture

One major disadvantage of using the traditional autonomous access point is that there is no central point of management, each access point needs to be configured separately and for a large deployment which involve many access points, the process is time consuming and cumbersome. It's also easy to introduce inconsistencies to the configuration. Therefore, for larger networks the other two architectures are typically preferred.

Centralized WLAN Architecture:

In the **centralized WLAN architecture**, autonomous access points have been replaced with controller-based access points, also known as lightweight or thin access points. This model uses a central WLAN controller that resides in the core of the network and all the three planes (management, control, and data) were moved out of access points and into a WLAN controller hence the term controller-based. The access point still manages time-sensitive operations and may handle the data forwarding at the edge to avoid a central location in the network for all the data, which may require significant processor and memory capacity at the controller.

Access points are configured and managed from the WLAN controller using the control and provisioning of wireless access points (CAPWAP) protocol or a proprietary protocol.

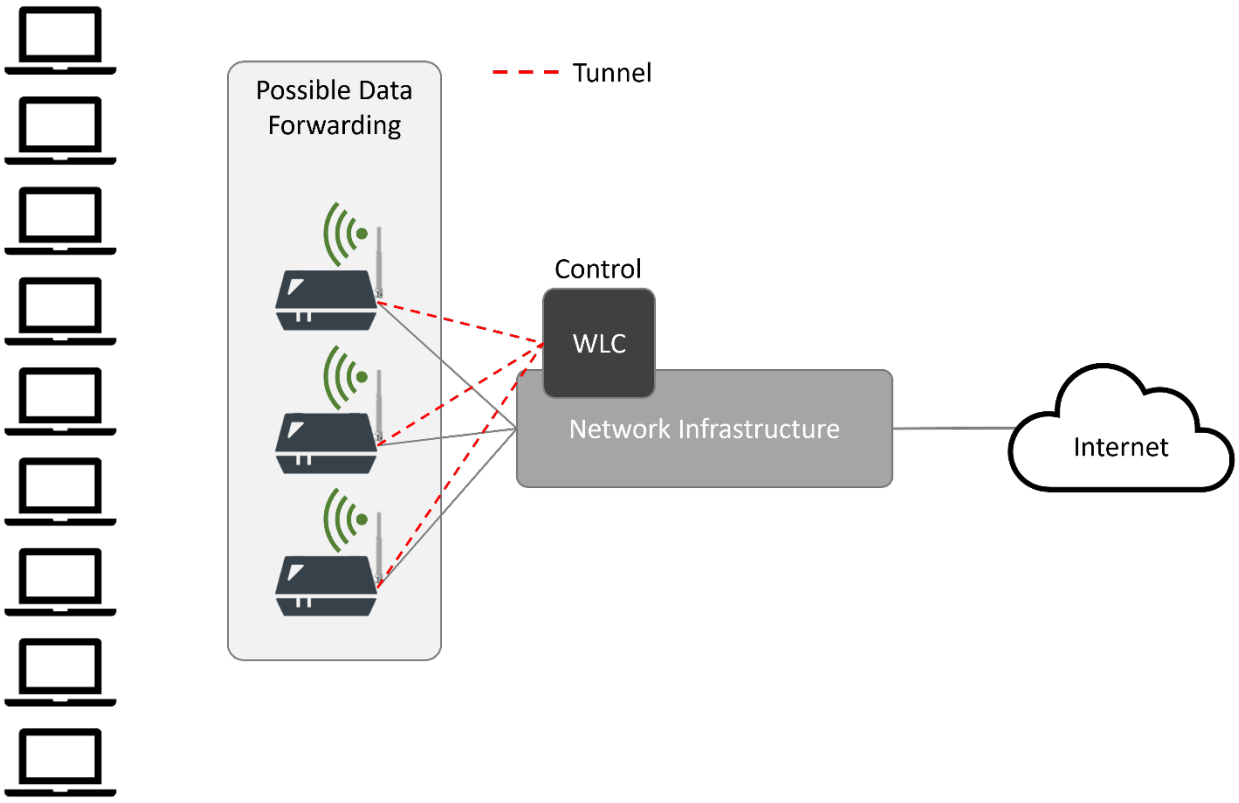

Figure: Centralized WLAN Architecture

Since the WLAN controller takes care of the control plane, RRM, client load balancing, and other control plane activities like fast roaming mechanisms, firewall capabilities, captive portal for guest users, etc., can be implemented.

A key feature of most WLAN controllers configured in centralized mode is that the integration service (IS) operates within the WLAN controller. In other words, all 802.11 traffic that is destined for wired-side network resources must first pass through the WLAN controller and be translated into 802.3 traffic by the integration service before being sent to the final wired destination.

So how does an 802.11 frame traverse between a lightweight access point and a WLAN controller? The answer is inside an IP-encapsulated tunnel. Each 802.11 fame is encapsulated entirely within the body of an IP packet. Many WLAN vendors use Generic Routing Encapsulation (GRE), which is a commonly used network tunneling protocol. The CAPWAP management protocol can also be used to tunnel user traffic.

Again, remember that a centralized WLAN architecture may use **centralized data forwarding** or **distributed data forwarding** (sometimes called access layer forwarding as well). With distributed data forwarding, the architecture is still a centralized architecture with control and management at the center, but the data is forwarded to the final destination directly from the access points. Centralized data forwarding requires that all data pass through the access points to the controller from where it is forwarded to the final destination.

Distributed WLAN Architecture:

A **distributed WLAN architecture** combines an autonomous access point with a suite of cooperative protocols without requiring a WLAN controller. The protocols enable multiple standalone access points to be organized into groups that share control plane information between the access points to provide functions such as layer 2 roaming, layer 3 roaming, firewall policy enforcement, cooperative RF management, security, and mesh networking. One way to describe a distributed architecture is to think of it as a group of autonomous access points with most of the WLAN controller intelligence and capabilities shared among them.

In a distributed architecture, all user traffic is forwarded locally by each independent access point, hence the data plane resides in the access points at the edge of the network.

Although the control plane and data planes have moved back to the Aps in a distributed WLAN architecture, the management plane remains centralized. Configuration and monitoring of all access points in the distributed model is handled by a Wireless Network Management System (WNMS) Sever.

NOTE: A cloud architecture may be centralized, distributed, or even autonomous/semi-autonomous, depending on the model used by the vendor and the options available. Many cloud solutions are "controller in the cloud" type models and others are more like wireless network management systems (WNMS) in the cloud, where the access points are onboarded, managed, and monitored, but no continual Wi-Fi control is performed in the cloud and instead it is performed autonomously on a moment-by-moment basis.

Distribution System:

A **distribution system (DS)** is used to connect a set of basic service sets (BSSs) via integrated LANs to create an Extended Service Set (ESS). The DS consists of two main components:

Distribution System Service (DSS): System services built inside an access point in the form of software to provide switchlike intelligence to an access point. These software services are used to manage communications between access points and allow for wireless clients to communicate with other wireless clients in the same ESS.

Distribution System Medium (DSM): A logical physical medium used to connect access points is known as a distribution system medium (DSM). The most common example is an 802.3 medium. Hence let us look at the 802.3 Medium and above and their part in Wi-Fi world.

Switch:

A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the Open System Interconnection (OSI) model (details on the OSI model can be readily found on the Internet). It is used to form a wired Ethernet LAN. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer 3 switches or multilayer switches.

Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers, on the same network within a building or campus. A switch enables connected devices to share information and communicate with to each other.

Wireless access points are usually connected to a switch which, in turn, may supply power to the access points via **power over ethernet (PoE)**. PoE uses the extra wires in the Ethernet cable to provide power to the edge device rather than requiring wall power. **Virtual Local Area Networks (VLANs)** allow for logical separation of traffic in a LAN and are used in switched 802.3 networks for both security and segmentation purposes. Individual SSIDs can be mapped to individual VLANs, and users can be segmented by the SSID/VLAN pair, all while communicating though a single access point (Ex: Guest VLAN for Guest users, Voice VLAN for Voice over Wi-Fi client phones).

The configuration required on the switchport for the Access points really depends on the type of WLAN architecture in use.

A controller-based access point is typically connected to an access port on an ethernet switch that is tied to a single VLAN. The non-controller models (autonomous and distributed WLAN architectures) however require support for multiple VLANs at the edge. The access point is therefore often connected to an 802.1Q trunk port on an edge switch that supports VLAN tagging.

Hence for a centralized WLAN architecture the config for an ap connected on interface 'x' is as below

Switch(config-int-x) # Switchport mode access

Switch(config-int-x) #Switchport access vlan <vlan id>

And for the autonomous and distributed WLAN architectures the config for an access point connected on interface 'x' is as below

Switch(config-int-x) # Switchport mode trunk

Switch(config-int-x) # Switchport trunk native vlan <vlan id>

Switch(config-int-x) #Switchport trunk allowed vlan<native vlan id, vlan ids mapped to SSIDs>

The native VLAN is the untagged VLAN. These examples are based on the configuration of a common Cisco switch.

Gateway:

A gateway is used to join two dissimilar networks, which may use different primary protocols. For instance, a gateway is used to join two layer 3 IP networks that use different network addresses or to join two layer 2/3 networks that use different protocols, such as Ethernet and IP on one and 802.15.4 and IP on another.

The working principle of a gateway is to differentiate what is inside the network and what is outside the network and to allow appropriate traffic to be converted (if required) and pass through. It very well might be a server, firewall, router, or another device that empowers traffic to stream all through the network. Gateways serve as an exit and entry point for a network or subnetwork. In most IP-based networks, the only traffic that does not go through at least one gateway is traffic flowing among nodes on the same LAN segment.

The default gateway always resides in the same subnet as the end device IP and is used as the destination of all traffic that is not destined for the same subnet.

To further explain the role of a gateway in Wi-Fi, when the wireless traffic received from the wireless client is converted to 802.3 wired traffic by the Integration Service in the WLC or AP, the 802.3 (Ethernet) wired traffic is sent to the default gateway by the WLC or by the switch to which the AP is connected if the destination address is in a different subnet. The default gateway will further route the traffic on a hop-by-hop basis. Hence the default gateway needs to be configured on the devices within each network segment.

The command to configure a default gateway on switches is:

L3-Switch (Config)# Ip default-gateway <x.x.x.x>

where x.x.x.x is the IP address of the default gateway, usually the first or last usable address in a network is configured as a default-gateway Ip.

Router:

While switches allow different devices on a network to communicate, routers allow different networks to communicate. In fact, most "default gateways" are really just routers within enterprise networks.

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: forwarding data packets to their intended IP addresses, and filtering data packets to only allow authorized communications[1].

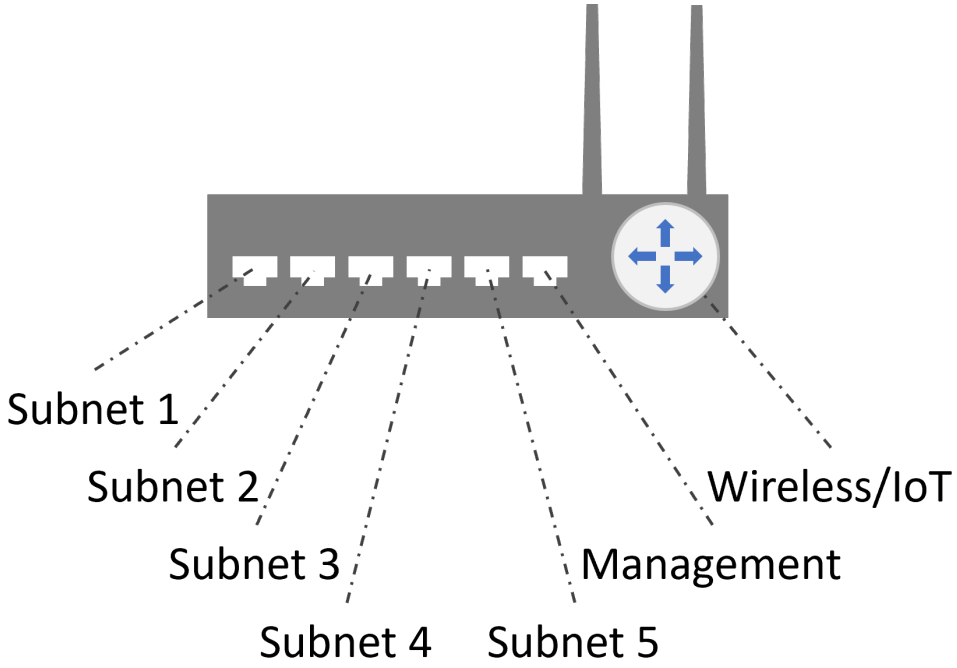

Figure: Router connecting various networks

[1] www.cloudflare.com/learning/network-layer/what-is-a-router/

There are several types of routers, but most routers pass data between or within LANs (local area networks) and across WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area, typically a building[2].

Hence in the Wi-Fi world, routers help communication between wireless client devices connected on different SSIDs. As shown in above image devices connected to Home Wi-Fi can communicate with devices connected to IoT Wi-Fi or Guest Wi-Fi or even device connected using wired networking.

How routers communicate between multiple networks is based on static routes or the **routing protocols** (ex: RIP, OSPF, BGP) used to build the routing table to reach the other network. Therefore, the routes defined for the network statically or dynamically need to be verified while troubleshooting the connectivity between networks. Static routes are manually created in the router configuration sets (or through an external management engine) and dynamic routes are created collaboratively between routers themselves using the previously mentioned routing protocols.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches and some form of leased or licensed connections.

Subnet:

A subnet, or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical or physical partition of an IP network into multiple, smaller network segments. The practice of dividing a network into two or more networks is called **subnetting**. Logical subnetworks are defined by VLANs and physical subnetworks are defined by physical routers.

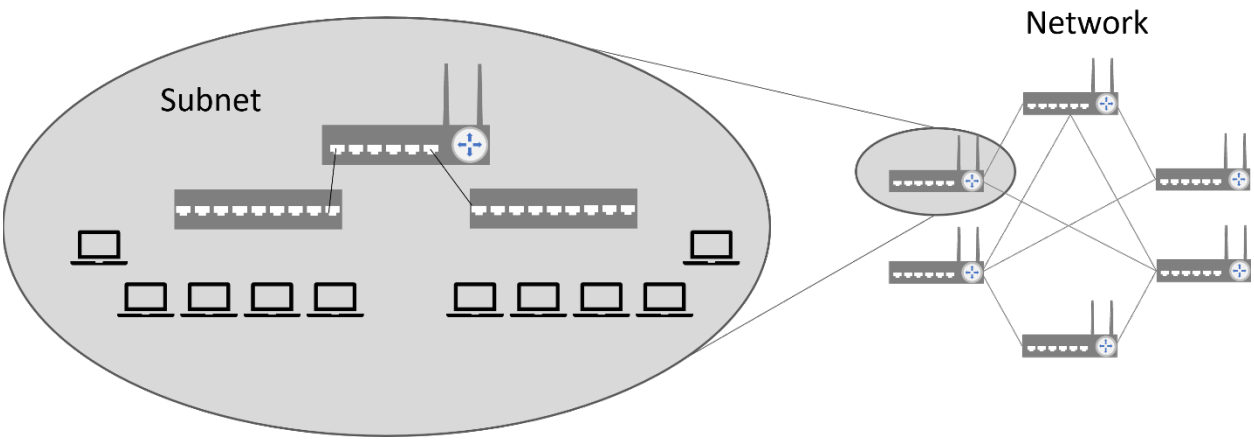

Figure: Subnet

[2] Ibid.

Each subnet allows its connected devices to communicate with each other, while default gateways (routers) are used to communicate between subnets.

Subnet Mask: When you connect a device to a network, the network assigns an IP address to the device. That IP address consists of two parts: the ***network portion*** and the ***host portion***. The network portion of the IP address identifies the overall network while the host portion identifies the device. A ***subnet mask*** is a binary number that distinguishes the network address and the host address within an IP address. While the number is binary, like IP addresses themselves, it is represented in what is called **dotted decimal notation**. So, 11111111.11111111.11111111.00000000 becomes 255.255.255.0 for the subnet mask. Where there is a 1 it is the network portion and where there is a 0 it is the host portion.

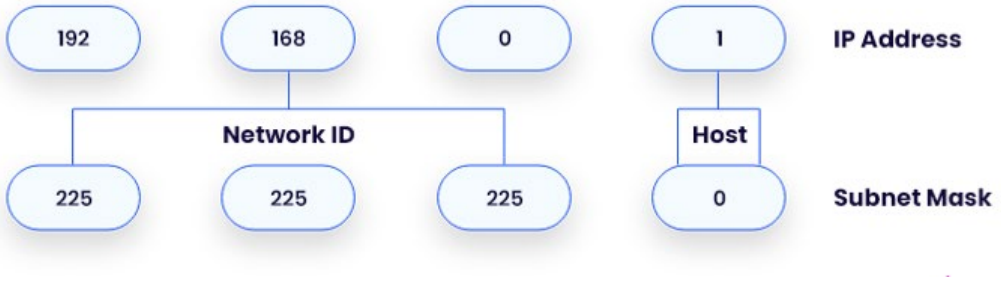

Fig: Parts of an IP address and Subnet mask (SOURCE: IPXO.COM)

The number of usable addresses for a subnet is defined by the host portion of the subnet mask and it is always a best practice in both wireless and wired networking to properly estimate the usable addresses for every subnet. Future growth of device counts also need to be considered prior to creating a subnet for wired and wireless devices.

In Wireless configuration for the SSIDs, it is always a best practice to use VLAN groups to assign for a particular SSID since that will avoid unnecessary downtimes when the VLAN/subnet assigned to SSID gets filled and adding a broader subnet causes the existing clients on the SSID to lose connectivity and cause network downtimes. With VLAN groups you can add multiple VLANs with required subnet size and does not cause any outages.

Firewall:

A **firewall** is a network security device that monitors, and filters (accepts, rejects, or drops) incoming and outgoing network traffic based on an organization's previously established security policies.

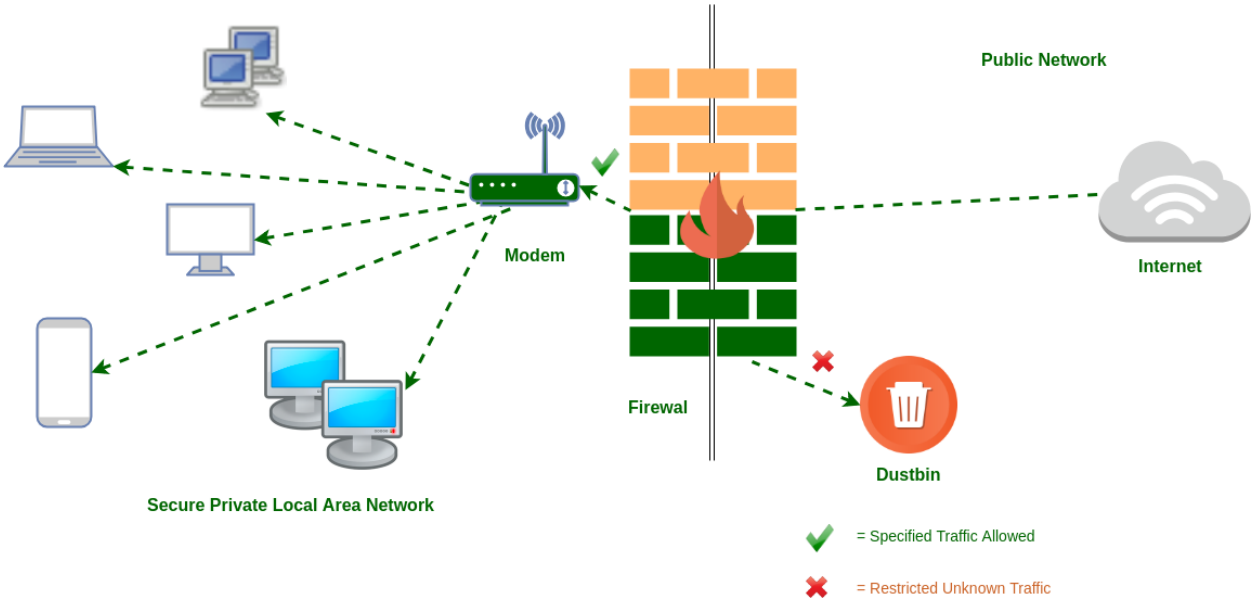

Figure: Firewall connected between public network and private LAN (SOURCE: GeeksforGeeks)

At its most basic, a firewall is the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out. The firewall is basically a router with advanced filtering functions.

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.

But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the dedicated capacity to keep threats out of the network. Hence, the firewall was introduced.

In the Wi-Fi world, for the communication between the access point and WLC or WNMS to work as expected, the ports used for these transport layer protocols (UDP/TCP) need to be opened on the firewall, these ports vary between different vendors manufacturing the Access points,

For example, Cisco uses CAPWAP protocol with UDP ports 5246 (for Control plane) and UDP 5247 (for data plane) to communicate between the wireless access point and WLC. Juniper uses TCP 443 to communicate between their Mist access point and Mist Cloud/Mist Edge appliance, etc., These ports need to be unblocked on the firewall for the access point to WLC/WNMS communication to work as expected.

Also, for the 802.1X authentication to pass between the Wireless Clients and RADIUS server UDP port 1645 or 1812 needs to be allowed on the firewall if it is located between the supplicant and authentication server. For accounting purposes UDP port 1646 or 1813 needs to be allowed.

Apart from the protocols, specific wireless client device types were assigned to use certain VLANs which are located behind the firewall. Configuration on the firewall interfaces should be verified when these specific client device types were unable to connect to the network. Wireless credit card readers used in

healthcare and Payment Card Industry (PCI) verticals better fits into this scenario. These Credit card readers connect to the corporate network on a VLAN but are landed in a different VLAN which is behind the firewall based on authorization policies configured for the devices. Assuming the VLAN configuration on the WLC is configured correctly and if the wireless device successfully authenticates but cannot get an IP address, the configuration on the firewall interface needs to be verified to see if it has proper DHCP helper addresses configured and other configuration settings that may block required traffic.

Demilitarized Zone (DMZ):

In computer security, a DMZ network (sometimes referred to as a "demilitarized zone") functions as a subnetwork containing an organization's exposed, outward-facing services (those accessible from the Internet). It acts as the exposed point to an untrusted network, commonly the Internet.

The goal of a DMZ is to add an extra layer of security to an organization's LAN. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ, while the rest of the organization's network is safe behind a firewall.

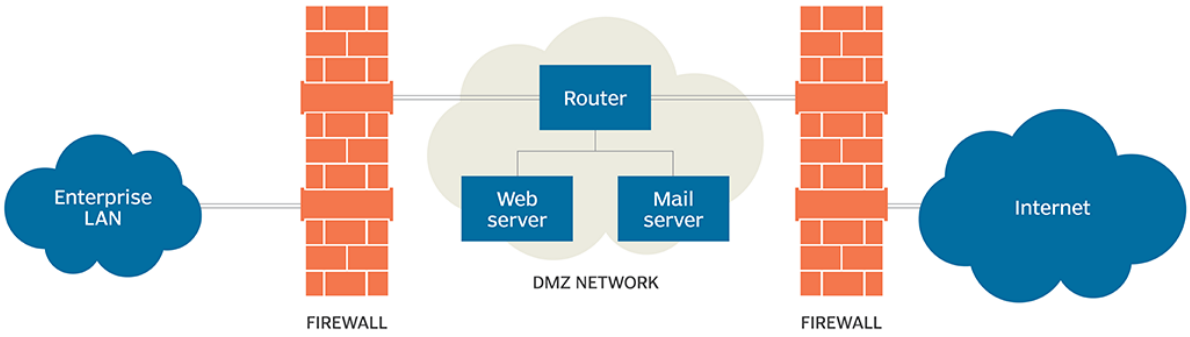

Figure: DMZ Network (SOURCE: TechTarget)

When implemented properly, a DMZ Network gives organizations extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

The DMZ network exists to protect the hosts most vulnerable to attack. These hosts usually involve services that extend to users outside of the local area network, the most common examples being email, web servers, and DNS servers. Because of the increased potential for attack, they are placed into the monitored subnetwork to help protect the rest of the network if they become compromised.

Hosts in the DMZ have tightly controlled access permissions to other services within the internal network because the data passed through the DMZ is not as secure. On top of that, communications between hosts in the DMZ and the external network are also restricted to help increase the protected border zone. This allows hosts in the protected network to interact with the internal and external network, while the firewall separates and manages all traffic shared between the DMZ and the internal network. Typically, an additional firewall will be responsible for protecting the DMZ from exposure to everything on the external network.

All services accessible to users on communicating from an external network can and should be placed in the DMZ, if one is used. The most common services are:

- Web Servers
- Mail Servers
- FTP Servers

Most organizations provide WLAN guest access for visitors, contractors, and BYOD type devices to allow Internet access. The security for guest WLAN users is much different than security provided for the corporate WLAN users. The guest SSID is often an open network that has no encryption security.

The guest VLAN associated to the guest SSID is usually segmented from corporate user traffic in a unique guest subnet. In enterprises where they have multiple locations with each location having its own local WLC (foreign WLC). Guest traffic is often routed to a demilitarized zone (DMZ). The DMZ has a WLC called the anchor WLC that is configured for wireless guest access. The WLC anchors the wireless guest traffic to the DMZ anchor WLC. After a successful handoff of the client to the DMZ anchor WLC, the DHCP IP address assignment, authentication of the client and so on are handled by the DMZ anchor. After it completes the authentication, the wireless client is allowed to send/receive traffic as shown in the below image.

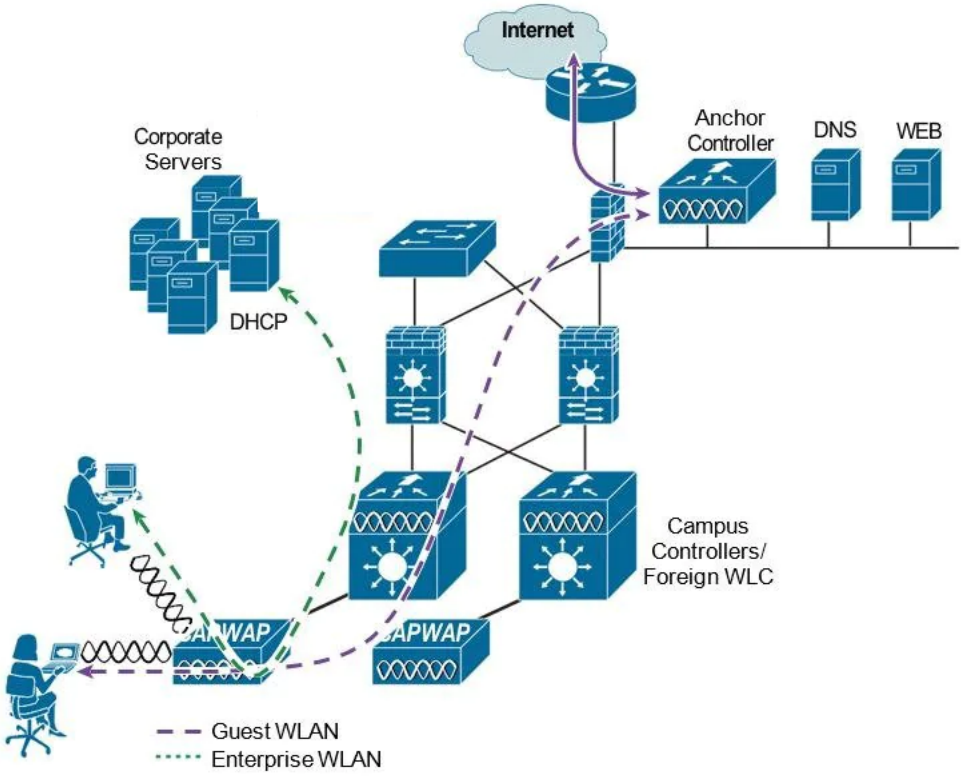

Figure: Guest user Traffic flowing through DMZ (SOURCE: Cisco)

For the mobility configuration to work between the anchor and foreign WLCs, the configuration of the anchor WLC (Ip address, MAC address, Group name, hash etc.) needs to be configured on Foreign WLCs and vice versa also Mobility Anchor Ip needs to be assigned in the WLAN settings for the Guest SSID on Foreign WLC.

Summary:

As you can see, basic networking components must be assembled together for a fully functional modern WLAN. This foundation paper has provided an overview of the components to get you started.

Sources Used:

Wi-Fi content: CWNA guide

https://en.wikipedia.org/wiki/Packet_switching

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-how.html

https://internetofthingsagenda.techtarget.com/definition/gateway

https://openautomationsoftware.com/open-automation-systems-blog/what-is-an-iot-gateway/

https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/

https://www.techtarget.com/searchnetworking/definition/subnet

https://www.ipxo.com/tutorial/what-is-subnet-mask/

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

https://www.barracuda.com/glossary/dmz-network

www.TechTarget.com

