

# Class Notes



**WI-FI TECHNOLOGY**  
FUNDAMENTALS COURSE

Module 1: Introduction and History of Wi-Fi

Session 1d:

# **BASIC FUNCTIONAL BUILDING BLOCKS OF A Wi-Fi AP/ROUTER**

By

Thanushya Mothikivalasa  
Rohini kaparapu  
Nishtala Kiranmai  
Jami Harika  
Shiny Sayyad

5<sup>th</sup> Oct 2023

## Introduction to Wi-Fi Routers:

Wi-Fi routers are crucial devices for wireless internet connectivity. They act as the gateway that allows your devices, such as smartphones and laptops, to connect to the internet wirelessly.

### How Phones Detect Wi-Fi Networks:

- When you open your device's Wi-Fi settings, you see a list of available networks. These networks are made visible to your device because of nearby Wi-Fi routers. These routers are responsible for broadcasting their presence, enabling your device to detect and connect to them.

### Importance of Wi-Fi Routers:

- Wi-Fi routers play a pivotal role in facilitating internet access. Even in areas with numerous Wi-Fi networks, like residential neighborhoods or commercial areas, it's the Wi-Fi routers that ensure you can access the internet seamlessly.

### Types of Wi-Fi Router:

There are two primary categories:

- Residential Wi-Fi Routers: These are commonly found in homes and provide personal internet access within households.
- Enterprise Wi-Fi Access Points: These devices are designed for corporate environments and are often discreetly installed on walls or ceilings.

### Exploring Wi-Fi Router Components:

- A Wi-Fi router comprises several internal components, each with a specific function. These components include radios, memory modules, CPUs, ethernet ports, power modules, LEDs, USB interfaces, and antenna connectors. Notably, radio modules are critical for wireless communication.

### Role of Radio Modules:

- Radio modules are central to Wi-Fi routers. They are responsible for managing wireless communication, enabling the transmission of Wi-Fi signals. These modules connect to antennas through RF cables, ensuring the seamless transmission of wireless data.

### Wi-Fi Modules in Client Devices:

- Client devices like laptops and smartphones contain built-in Wi-Fi modules essential for wireless connectivity. Many modern laptops come equipped with these modules, simplifying the process of connecting to wireless networks.

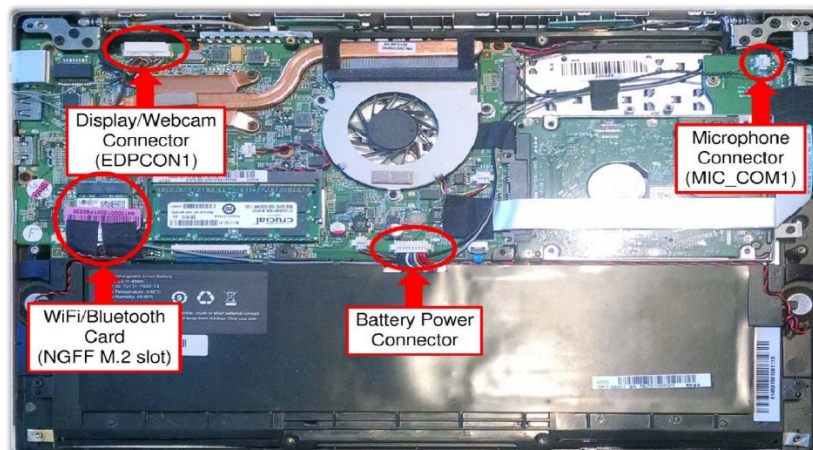
### Accessing Detailed Information:

- For in-depth information about specific Wi-Fi router models, you can visit the [fcc.io](https://www.fcc.io) website. There, you can access a wealth of data, including certification reports, test results, images, and comprehensive specifications, allowing you to gain a deeper understanding of Wi-Fi routers.

### Functions of Modern Wi-Fi Routers:

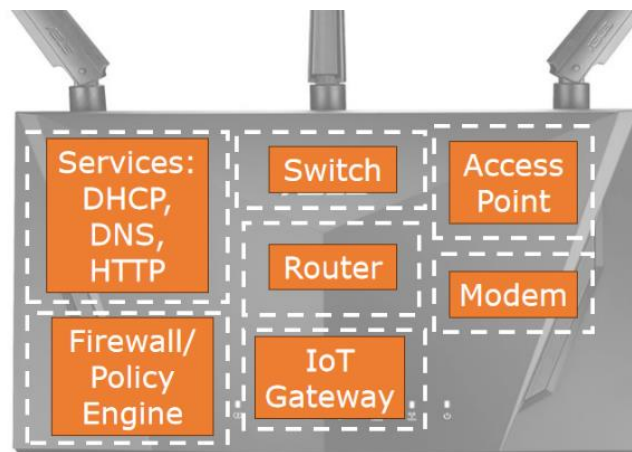
- Modern Wi-Fi routers serve multifunctional roles. They act as access points, allowing wireless device connectivity. They also function as switches, enabling multiple device connections within your local network. Additionally, they provide routing capabilities, allowing communication between your local network and the wider internet.

### WI-FI client



- A device that can connect to a Wi-Fi network is known as a Wi-Fi client, and it can be anything such as a smartphone, smart TV, laptop, etc.
- In the early days, we used to use PCMCIA cards embedded with Wi-Fi radios in Wi-Fi clients. However, modern devices have evolved, and now many come with built-in Wi-Fi radios, as shown in the above picture.

### A modern day wifi router



A router is a networking device that connects to the Internet Service Provider (ISP) to access the internet and then distributes that internet connection to various devices within a local area network (LAN). It acts as a gateway, directing data traffic between the local network and the wider internet.

Apart from the basic routing function, a modern-day router has much more functionality to it and they can be understood as follows:

**Access Point:**

A modern-day Wi-Fi router serves multiple functions, and one of its key roles is acting as an access point. Now, think of an access point as a gateway that transforms your wired network into a wireless one. It operates strictly at Layer Two, which means it's working with the physical and data link layers. Essentially, it's converting the information it receives from your wired connections into a format suitable for wireless transmission.

**Switch:**

A switch is a common networking device, often utilized in wired networks. In the context of a Wi-Fi router, it serves as a Layer Two device, enabling the connection of multiple devices within a local area network (LAN). The router, with its Ethernet ports, can function like a typical switch, facilitating the switching of data among connected devices.

**Services: DHCP, DNS, HTTP:**

Additionally, a modern Wi-Fi router hosts various services, including DHCP for assigning IP addresses, DNS for name resolution, and HTTP for web server functions. The web server allows users to configure the router through a graphical interface, adjusting settings like network configurations, security, and firewall policies.

**Modem:**

Some routers also integrate modem functionality, converting signals from sources like coaxial cables into a format compatible with Wi-Fi or Ethernet. This is particularly common in routers provided by cable internet service providers.

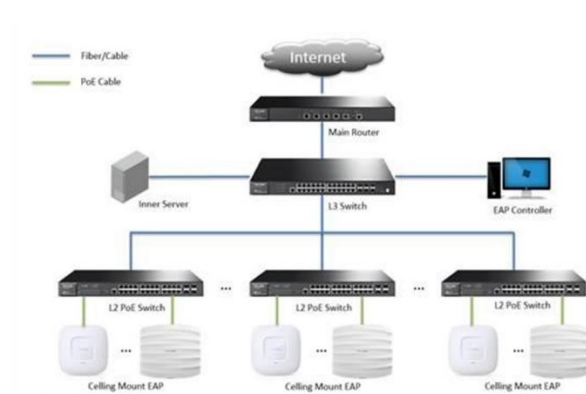
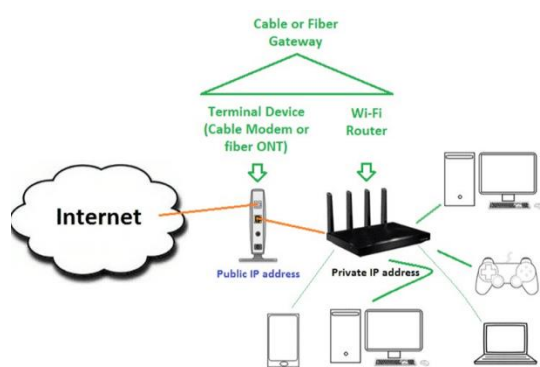
**Firewall/policy engine:**

The router typically includes firewall and policy engines. These features enable the router to inspect packet data, identify specific types of traffic (e.g., from malicious websites), and apply rules, such as parental controls.

**IOT Gateway:**

modern Wi-Fi routers may extend their capabilities to accommodate IoT (Internet of Things) devices. Some routers come with built-in IoT gateway functionality, incorporating Bluetooth, Zigbee, or other radio technologies to facilitate communication with various IoT devices within a household.

## Residential Wi-Fi vs. Enterprise Wi-Fi



**Residential Wi-Fi:** In residential settings, like homes, simplicity is key. You just need to connect your Wi-Fi router to the internet to access it. All essential network functions, such as routing and security, are contained within the router itself.

**Enterprise Wi-Fi:** In contrast, Enterprise Wi-Fi networks, like those in large offices, are vastly different. Consider a scenario with hundreds of Wi-Fi access points. Rather than integrating all networking functions into each access point, you can centralize these functions in a formal organization. This centralized management involves a dedicated IT team, a wiring closet, and network infrastructure.

### Wi-Fi Router vs. Access Point

**Wi-Fi Router:** Most residential Wi-Fi routers combine various functions, including routing, security, and internet access. They are all-in-one devices that manage everything in a home network.

**Access Point:** In Enterprise networks, access points primarily serve as Wi-Fi hotspots, focusing solely on providing wireless connectivity. They do not handle routing or complex network functions. All other functions are handled elsewhere in the network.

- **Centralized Management:** In Enterprise networks, network configuration and management are centralized. Instead of configuring each access point individually, you can manage settings from a central location, which simplifies the process, especially when dealing with numerous access points.
- **Pushing Functions:** In Enterprise networks, you can delegate tasks like switching, routing, firewall management, and more to the network infrastructure. Access points become simpler devices with the primary function of providing wireless access.



- **Scaling Challenges:** In residential networks, managing a single Wi-Fi router is straightforward. However, in an Enterprise with numerous access points, individually configuring each one becomes impractical. The solution is centralization to manage all access points efficiently.
- **Benefits of Centralization:** The key advantage of centralizing network functions in an Enterprise is ease of management, especially as the network scales. It ensures consistent configurations, simplifies troubleshooting, allows for uniform updates, and streamlines configuration changes across the network.
- **Cloud-Based Management:** Over time, Enterprise network management transitioned from physical controllers to virtual and cloud-based solutions. Cloud controllers offer the advantage of managing multiple locations worldwide from a single interface, making distributed office management more accessible.
- **Enterprise Access Points:** In Enterprise networks, access points are a critical component, but their role is simplified. They primarily serve as wireless access points, allowing devices to connect to the network without handling other complex network functions.

Finally, residential Wi-Fi and Enterprise Wi-Fi networks differ significantly in terms of complexity, centralization of management, and the roles of access points. Centralized management and pushing functions to the network infrastructure are crucial aspects of efficiently managing large-scale Enterprise networks. The evolution towards cloud-based management further enhances the flexibility and scalability of these networks.

## Accessing the Residential Wi-Fi Router's Configuration Interface

To configure a residential Wi-Fi router, you can log into its web-based configuration interface. This interface is typically accessible through a web browser. For instance, you can access the configuration page of an ASUS gaming router.

### Configuration Options for Residential Wi-Fi Routers

Within the configuration interface, you have a wide range of options:

#### Wireless Settings:

We can access the wireless settings, where you can:

- Set up your Wi-Fi network name (SSID).
- Define and change the Wi-Fi password for network security.
- Configure encryption methods (like WPA2 or WPA3) for protecting your wireless network.

#### Router Modes:

You can switch your router to different modes, such as:

- Access Point (AP) mode: Turns your router into a simple wireless access point.
- Repeater mode: Expands the coverage area of your Wi-Fi network.
- Bridge mode: Connects separate network segments.
- Mesh node: Part of a mesh Wi-Fi system that improves coverage and stability.

**Advanced Features:** Many modern residential Wi-Fi routers are quite sophisticated. They offer features like:

- Firewalls: You can set up firewalls for added security.
- Policy Configuration: Configure specific rules and policies for your network.

### How to Access the Router Configuration Page

- To access your router's configuration page, follow these steps:
- Connect a device (e.g., a computer or smartphone) to your Wi-Fi network.
- The router assigns an IP address to your device, typically something like "192.168.1.1" or "192.168.0.1."
- Open a web browser on your device.
- Enter the router's IP address into the browser's address bar and press Enter.
- This action should take you to the router's web-based configuration interface.

### Exploring Residential Wi-Fi Router Features

Residential Wi-Fi routers come with a variety of features and settings, making them powerful devices for managing your home network. These features include:

- **Quality of Service (QoS):** You can prioritize specific types of network traffic, ensuring smooth performance for activities like online gaming or streaming.
- **Port Forwarding:** If you run specific applications or services at home, you can configure port forwarding to allow external access to these services.
- **Firmware Updates:** Keeping your router's firmware up-to-date is essential for security and performance. You can usually check for and install firmware updates through the configuration interface.
- **Security Settings:** Apart from setting up a password for your Wi-Fi network, you can configure other security measures to protect your network from potential threats.

## Scale and Complexity of Enterprise Networks

In Enterprise networks, the focus is on scale and managing an entire network, not just individual Wi-Fi routers. This can include everything from building facilities to cloud-based networks.

**Centralized Management in Enterprise:** In Enterprise networks, management is centralized at the network level, allowing for more efficient control. This can encompass various locations worldwide.

## Meraki - Cloud Controller for Enterprise Networks

**Meraki Overview:** Meraki is an example of a cloud-based controller for Enterprise networks. It provides a centralized platform for managing large-scale networks, offices, and even remote workers.

**World View of the Network:** Meraki offers an overview of the entire network, including offices in different countries and remote workers. This is achieved through a single dashboard.

### Managing Devices in an Enterprise Network

- **Device Management:** In an Enterprise network, device management extends beyond Wi-Fi access points. It also includes managing security cameras, sensors, and other connected devices.
- **Access Point Details:** Meraki allows you to drill down into specific access points. You can view details like the network they are part of, the number of connected devices, and even security alerts or attacks.

### Troubleshooting and Debugging

- **Troubleshooting:** The cloud controller provides valuable troubleshooting tools. You can identify issues such as disconnections, failures, and security alerts, enabling effective network maintenance.

### Monitoring and Configuration

- **Monitoring:** The cloud controller offers real-time monitoring, including data rates, throughput, and application traffic. You can see how much traffic is coming from various sources like email or video streaming.
- **Configuration:** Beyond monitoring, you can configure the network and apply policies, restrictions, and firewall settings from a central dashboard. These changes can be pushed to access points across different locations, simplifying network management.

### Benefits of Cloud-Based Network Management

- **Benefits:** Cloud-based management simplifies the management of large-scale Enterprise networks. It allows for centralized control, remote access, and efficient scaling. This ease of management is invaluable for organizations with extensive network infrastructure.



## Difference Between Wi-Fi Router and Access Point

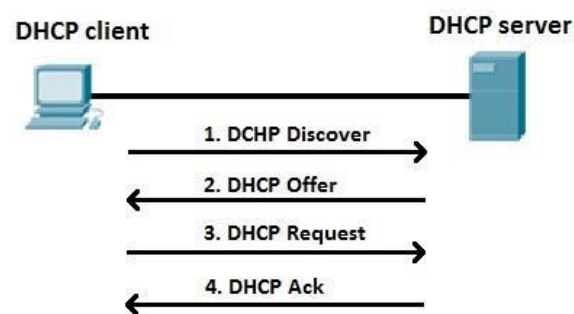
Characteristic	Access Point	Router
Function	Extends an existing wired network	Connects different networks together
Layer in the OSI model	Layer 2 (Data Link Layer)	Layer 3 (Network layer)
Primary Purpose	Wireless connectivity for devices	Manages network traffic and routing
DHCP Functionality	Typically, does not provide DHCP	Usually provides DHCP services
IP Address Assignment	Requires an external DHCP server	Assigns IP addresses to devices
NAT (Network Address Translation)/PAT (Port Address Translation)	Does not perform Network Address Translation	Performs NAT / PAT for IP sharing
Network Management	Limited network management features	Offers advanced network management features
Security	Limited security features	Includes firewall and security options
Internet Connection Sharing	Does not share an internet connection on its own	Shares an internet connection among devices
Routing	Does not perform routing functions	Routes data between different networks
Examples	Standalone wireless access points, Wi-Fi extenders	

## Dynamic Host Configuration Protocol

### What is DHCP, why is it necessary?

DHCP assigns IP addresses to devices on a network.

- When a device connects to a network, it sends a DHCP discover message to find an available IP address.
- The DHCP server (usually within the Wi-Fi router for residential setups) responds with a DHCP offer, including an IP address.
- The device requests the offered IP address.
- The server acknowledges the request and assigns the IP address to the device.



Usually, this process is called DORA process while assigning an IP address to a device there are 4 messages that would take place they are:

- 1)DISCOVER
- 2)OFFER
- 3)REQUEST
- 4)ACKNOWLEDGE

**Lease:** The IP address assignment is temporary and comes with a lease duration. After the lease expires, the device may need to renew it.

## Network Address Translation

### What is NAT? Why Is it necessary?

Network Address Translation overcomes the shortage of public IP addresses.

- The Wi-Fi router has one public IP address and assigns private IP addresses within the local network.
- NAT (Network Address Translation)/PAT (Port Address Translation) maps multiple private IP addresses to a single public IP address.
- Allows devices within the private network to communicate with external networks using a single public IP address.

## Wireshark

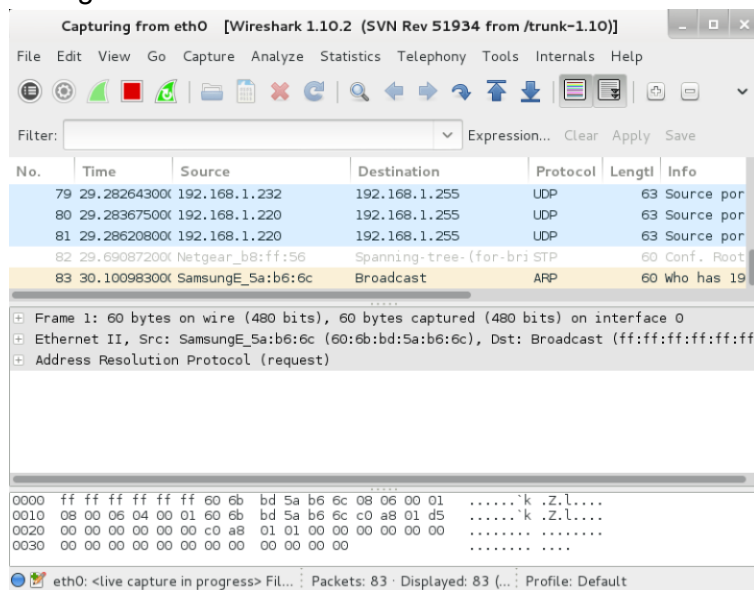
Wireshark is an open-source network packet analyzer. It is free and open-source software.

Wireshark is the most often-used packet sniffer in the world.

To work with Wireshark, we can download and install it in our system to do so refer to the link below. It has the steps to install Wireshark on windows system.

<https://www.geeksforgeeks.org/how-to-install-wireshark-on-windows/>

Once the installation is completed you can double click on the installed software and click on capture then the following window will be visible:



### This Window has 3 Panes

**1)Traffic Pane:** The traffic pane consists of the flow that is flowing from in and out of your connected devices such as Wi-Fi or any ISP.

**2)Packet Details and Diagram Pane:** The main function of the packet pane diagram is that you can see what a packet looks like.

**3)Packet Bytes:** The Packet bytes have its own significance which can help in analyzing the data which is based on the Bytes level. The Packet bytes are useful whenever we are trying to figure out the real data that we have captured because sometimes the bytes can also be modified.

### Wireshark does three things:

- **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

- Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see. There are many filtering techniques that can be performed in Wireshark software.
- Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

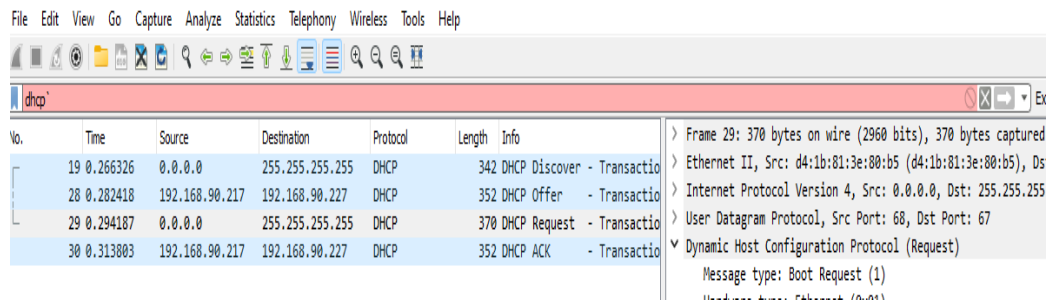
## DHCP Packet Capture

Capturing DHCP (Dynamic Host Configuration Protocol) packets in Wireshark and analyzing the DHCP DORA process (Discover, Offer, Request, Acknowledge) can provide valuable insights into how devices obtain IP addresses on a network. Here's a step-by-step explanation of capturing and analyzing DHCP packets in Wireshark for the DORA process:

- Start Wireshark on the computer that's connected to the network you want to monitor.
- In Wireshark, choose the network interface (e.g., Ethernet, Wi-Fi) that you want to capture DHCP packets from. Click on the interface name in the main Wireshark window to start capturing.
- As you start capturing, you'll see a list of packets scrolling in real-time. Look for the DHCP packets within this list. DHCP packets typically use UDP and can be identified by their source and destination port numbers (67 for the server and 68 for the client).
- To focus only on DHCP packets, you can apply a display filter. Type "dhcp" in the display filter field and press Enter. This will filter the displayed packets to only show DHCP-related traffic.

You'll notice a series of DHCP packets representing the DORA process:

1. **DHCP Discover (D):** The client broadcasts a DHCP Discover packet to find a DHCP server. Look for packets with the DHCP Discover message.
  2. **DHCP Offer (O):** The DHCP server responds with a DHCP Offer packet, suggesting an IP address to the client. Identify packets with the DHCP Offer message.
  3. **DHCP Request (R):** The client sends a DHCP Request packet to formally request the offered IP address. Look for packets with the DHCP Request message.
  4. **DHCP Acknowledge (A):** Finally, the DHCP server sends a DHCP Acknowledge packet, confirming that the client can use the provided IP address. Find packets with the DHCP Acknowledge message.
- Analyze the packet details to ensure that the DHCP process is working correctly. Check for any errors or unexpected behavior. For troubleshooting purposes, you can identify issues such as IP conflicts or DHCP server problems by closely examining the packet data.



No.	Time	Source	Destination	Protocol	Length	Info
19	0.266326	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID: 12345
28	0.282418	192.168.90.217	192.168.90.227	DHCP	352	DHCP Offer - Transaction ID: 12345
29	0.294187	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID: 12345
30	0.313803	192.168.90.217	192.168.90.227	DHCP	352	DHCP ACK - Transaction ID: 12345

Details for packet 29 (DHCP Request):

- Frame 29: 370 bytes on wire (2960 bits), 370 bytes captured
- Ethernet II, Src: d4:1b:81:3e:80:b5 (d4:1b:81:3e:80:b5), Dst: 01:00:00:00:00:00
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Request)
  - Message type: Boot Request (1)

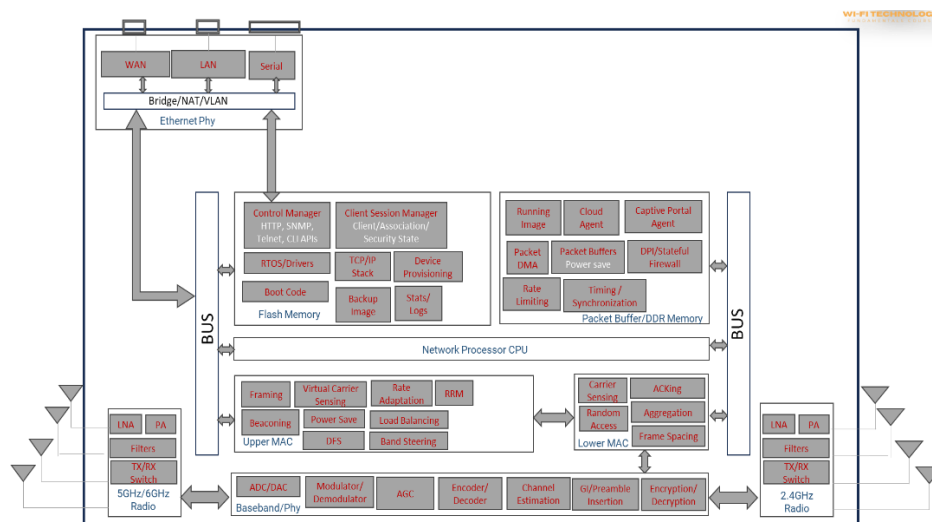


- The router maintains a NAT table that keeps track of which port number and IP address combination corresponds to each private IP address.
- Incoming packets with specific port numbers are routed to the appropriate device based on this mapping.

### Residential NAT Functionality:

- NAT and DHCP are commonly used in residential Wi-Fi routers to enable multiple devices to share a single public IP address for internet access.
- This combination of functions is essential for managing network traffic in a residential environment.

## Anatomy/Functional Block Diagram of Wi-Fi AP



### Radio Modules:

- Typically, there are multiple radio modules, such as 5 GHz, 6 GHz, and 2.4 GHz radios.
- Each radio module comprises various components, including transceivers, filters, power amplifiers, noise amplifiers, and noise mitigation devices.

### Baseband:

- The baseband serves as the physical layer and performs essential functions like automatic gain control, modulation/demodulation, encoding/decoding, and channel estimation.

### Wireless Channel:

- In the wireless medium, the channel represents the communication path between devices.
- Real-world channels can be affected by interference, signal reflections, and changes in noise levels.



### **Lower MAC (Media Access Control):**

Lower MAC functions that require high-speed processing are handled in hardware. These functions include carrier sensing, random access, frame acknowledgment, aggregation, and interframe spacing.

### **Upper MAC:**

Upper MAC functions encompass software-driven tasks like frame creation, beacon transmission, RTS/CTS handling, virtual carrier sensing, power-saving modes, DFS (Dynamic Frequency Selection), and rate adaptation algorithms.

### **Network Processor:**

The network processor manages the overall operation of the access point. It handles various functions, including network management, security, and connectivity to the cloud controller.

### **Memory Modules:**

- Memory is divided into flash memory (permanent storage) and dynamic memory (packet buffer).
- Flash memory stores boot code, backup images, networking stacks, security state, logs, and configuration.
- Dynamic memory is used for packet buffering, especially when receiving data from the air interface or Ethernet.

### **Ethernet PHY (Physical Layer):**

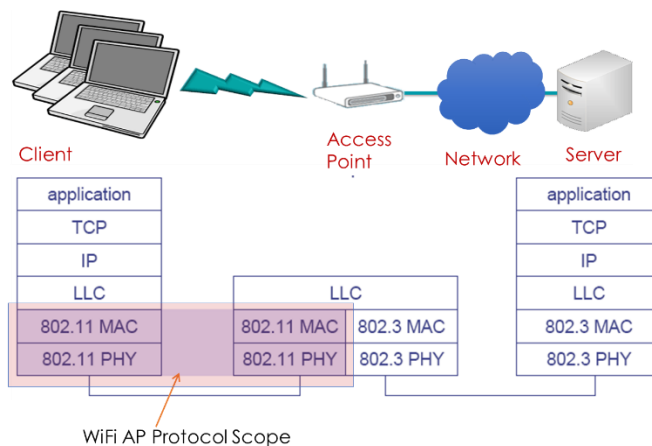
- Ethernet PHY interfaces include WAN, LAN, serial, and USB interfaces.
- Various modes can be configured, such as bridging, NATing, and VAN (Virtual Area Network) mode.

### **Cloud Connectivity:**

- Access points often connect to cloud controllers, requiring a cloud agent to facilitate this connection.
- Captive portal login agents may also be present to provide web-based authentication for users connecting to the access point.

This high-level overview of the functional blocks within a Wi-Fi access point/router provides a foundational understanding of the device's internal components and their roles.

## **Wi-Fi Infrastructure Network**



There are two essential layers in wireless networking: the physical layer and the MAC (Media Access Control) layer. These layers serve as the core elements that make wireless communication possible. What's important to note is that these layers are present not just in the access point but also in the devices (like laptops and smartphones) that connect to it.

### The Physical Layer (PHY):

- Think of this as the foundation of wireless communication. It's like the language that devices use to talk to each other without wires.
- We'll learn about how data is sent through the air, how different Wi-Fi frequencies are used, and how devices choose the best way to communicate wirelessly.

### The MAC Layer (Media Access Control):

- This layer manages how devices share the "talking space" in a wireless network. It ensures that everyone gets a fair chance to speak without interrupting each other.
- We'll explore the rules and techniques that devices follow to make sure they don't talk over each other, like taking turns and being polite.

By understanding these two layers, we get a complete picture of how Wi-Fi works, both in access points and in the devices, we use every day.