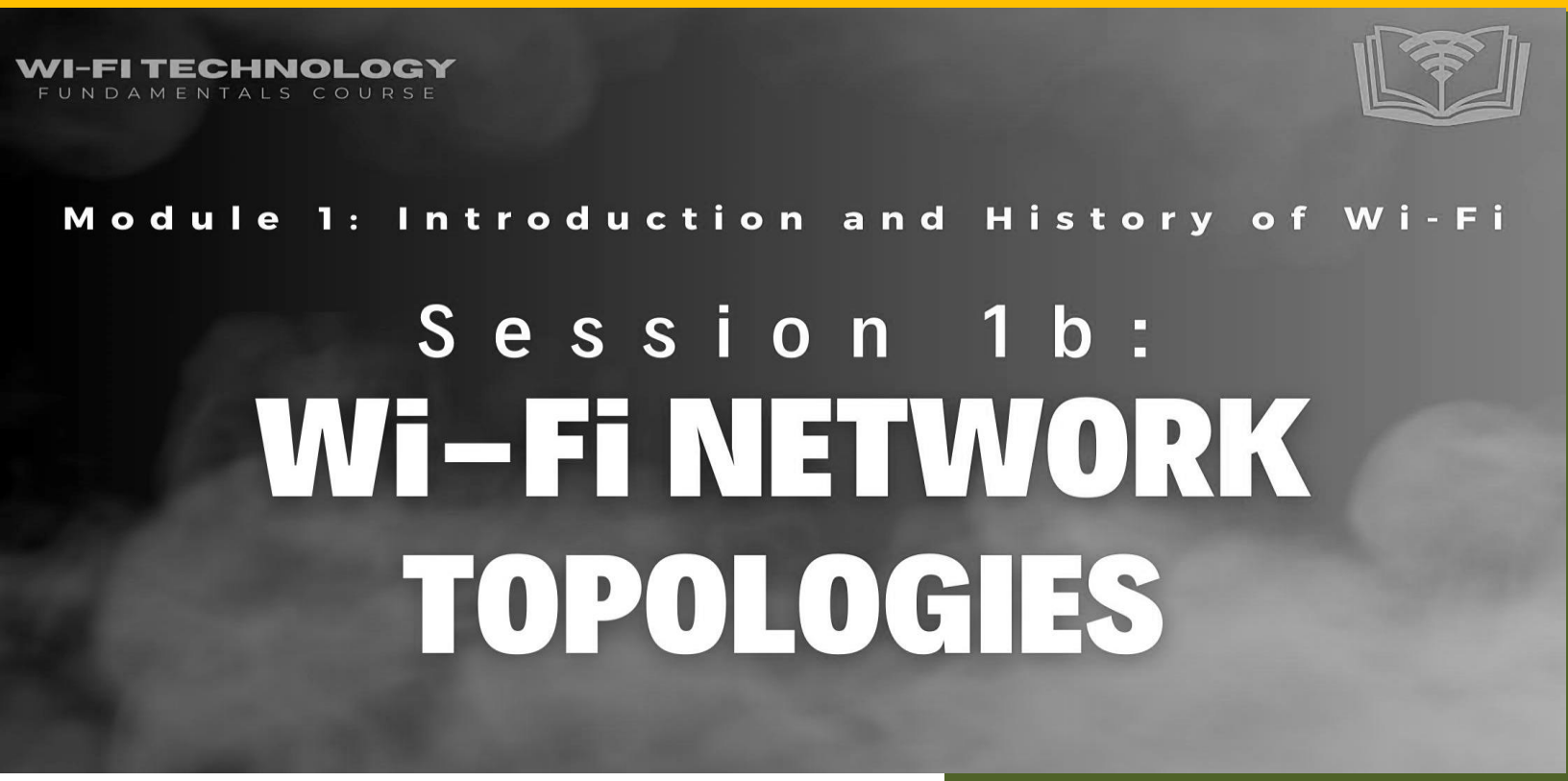
Class Notes



Notes Prepared By

Thanushya Mothikivalasa
Rohini kaparapu
Nishtala Kiranmai
Jami Harika
Shiny Sayyad

1st Oct 2023

Essential Networking Hardware and Their Roles:

1.Hubs and Switches:
These devices are part of the network infrastructure and help in connecting multiple devices within a local network. Switches are more advanced and efficient than hubs as they can intelligently forward data to specific devices, while hubs simply broadcast data to all connected devices.

2.Routers:
Routers connect different networks, such as a local network to the wider internet. They handle data routing between networks, making sure data packets reach their intended destinations.

3.Gateways:
Gateways are devices or software that translate data between different network protocols or data formats. They can bridge the gap between two dissimilar networks.

4.Bridges:
Bridges are devices used to connect two or more network segments, creating a larger network. They operate at the data link layer (Layer 2) of the OSI model.

5.Modems:
Modems (short for modulator-demodulator) are used to convert digital data from computers into analog signals for transmission over analog communication lines, such as telephone lines. They also perform the reverse conversion when receiving data.

What is a WiFi Access Point?

1.Wireless Portal:
- Wi-Fi access points serve as wireless portals, enabling devices to connect wirelessly to a network.
- They bridge the gap between wired connections and wireless devices.

2.Connectivity:
- APs provide connectivity by allowing devices such as smartphones, tablets, and laptops to wirelessly join the network.
- They facilitate wireless communication between devices and the network.

3.Coverage:
- Wi-Fi access points offer coverage within their range, typically around 100 meters.
- They radiate signals to create a coverage area, allowing devices to connect from various locations within that range.

4.Medium Access:
- APs manage medium access control in scenarios with multiple devices.
- They ensure that devices can access the wireless medium without causing interference or congestion.

5.Security:
- Security is a vital function of APs. They implement security protocols and encryption to protect data transmitted over the network.

- They control access to the network and authenticate devices.

6.Quality of Service (QoS):
- QoS is maintained by APs to prioritize certain types of data traffic.
- They ensure that critical data, like voice or video calls, receives the necessary bandwidth and low latency.

7.Mobility:
- Wi-Fi access points support mobility, allowing devices to seamlessly roam within the coverage area.
- Handoffs between APs are managed to ensure uninterrupted connectivity as devices move.

8.Virtual Networks:
- APs can create virtual networks on a single physical device, segregating network traffic.
- This enables the setup of multiple networks, such as guest networks, on the same access point while maintaining network isolation.

Basic WiFi Topologies:

Infrastructure Mode:
- **Description:** Infrastructure mode is the most common Wi-Fi topology used in enterprise and residential deployments. It involves connecting Wi-Fi devices to a wired network via Wi-Fi access points (APs).
- **Use Cases:** Typically used in offices, homes, and public spaces where multiple devices need to connect to a wired network wirelessly.

Repeater Mode:
- **Description:** In Repeater Mode, a Wi-Fi device extends the coverage of an existing wireless network by wirelessly connecting to an existing access point and retransmitting the signal.
- **Use Cases:** Useful for extending Wi-Fi coverage in areas with weak or no signal, such as large homes or buildings.

Bridge Mode:
- **Description:** Bridge Mode involves connecting two separate network segments or LANs wirelessly. It creates a larger network by linking two or more isolated networks.
- **Use Cases:** Used to connect network segments in separate buildings or locations without the need for physical cables.

Ad-Hoc Mode:
- **Description:** Ad-Hoc Mode allows Wi-Fi devices to connect directly to each other without the need for an access point. Devices can communicate in peer-to-peer fashion.
- **Use Cases:** Often used for device-to-device communication, such as file sharing between laptops or mobile devices.

Other Topologies:

Mobile Hotspot Mode:

- **Description:** Mobile Hotspot Mode turns a Wi-Fi-enabled device, like a smartphone or tablet, into a portable wireless hotspot, allowing other devices to connect to the internet through it.
- **Use Cases:** Commonly used when you need internet connectivity on the go, such as when travelling or in areas with no Wi-Fi access.

Mesh Mode:

- **Description:** Mesh Mode involves a network of interconnected access points that work together to provide seamless Wi-Fi coverage. If one node fails, the network can still function.
- **Use Cases:** Ideal for large areas, homes, or businesses where consistent and robust Wi-Fi coverage is required.

Workgroup Bridge Mode:

- **Description:** Workgroup Bridge Mode allows a Wi-Fi device to bridge its wired clients to a remote network or access point wirelessly, useful for connecting distant wired devices.
- **Use Cases:** Commonly used in scenarios where running Ethernet cables is impractical, like point-to-point links between buildings.

IoT Gateway Mode:

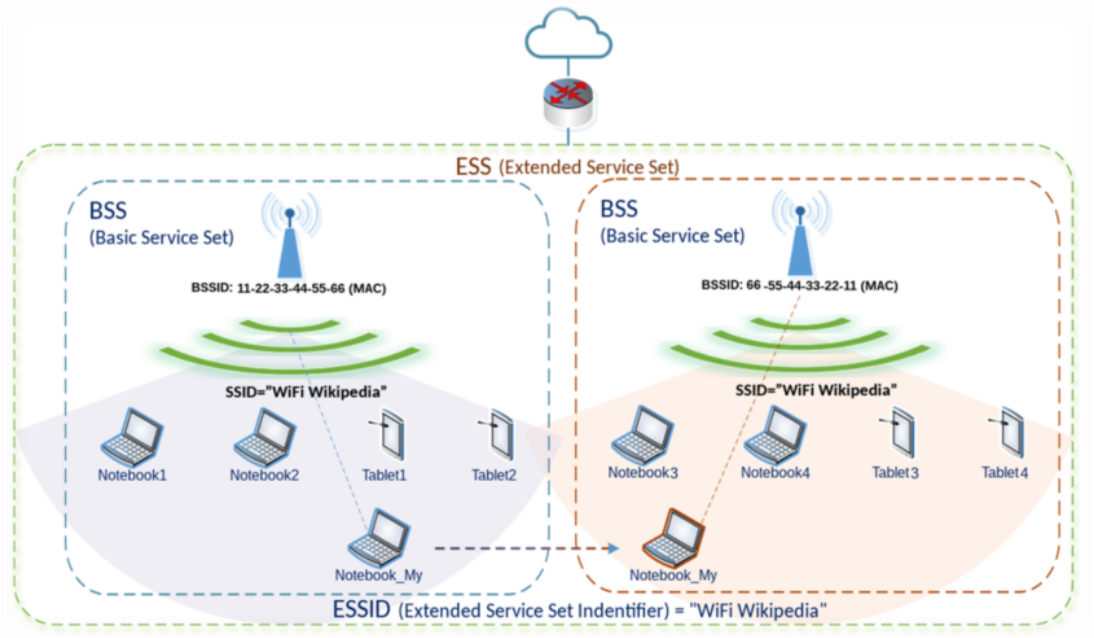
- **Description:** IoT Gateway Mode involves a gateway device that translates data between various network protocols or data formats, enabling IoT devices to connect to a network.
- **Use Cases:** Essential for connecting and managing various IoT devices that use different communication standards.

Infrastructure Mode:

- This mode is mainly used in Enterprise deployment, most Access Points deployed in enterprise mode. It allows multiple wireless devices to connect to a central access point or wireless router. In infrastructure mode, one or more wireless devices (e.g., laptops, smartphones, tablets) connect wirelessly to an access point, which is connected to a wired network or the internet. The access point serves as a hub, facilitating communication between the wireless clients and the wired network.
- An infrastructure mode consists of two fundamental concepts that help to organize and manage wireless connectivity. They are BSS and ESS.

Basic Service Set:

A basic service set is the basic building block of a Wi-Fi network in infrastructure mode. It represents a single wireless access point or single wireless router. Each BSS is identified by a unique name called the SSID (Service Set Identifier), which is the name you see when you look for available Wi-Fi networks on your device. Devices connected to the same BSS can communicate with each other directly.



Extended Service Set:

An extended service set is a group of interconnected BSSs that form a larger wireless network in infrastructure mode. All BSSs within an ESS typically share the same SSID and security settings, so devices can switch between them without requiring manual reconfiguration.

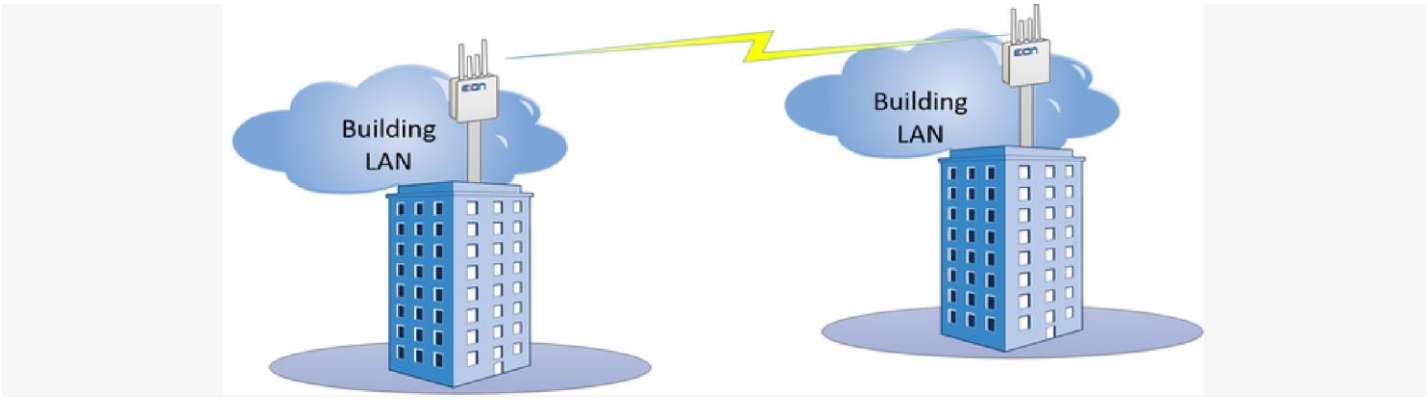
Repeater Mode:

- Repeater mode is used to extend the range of an existing wireless network by repeating the signal from an existing access point or router. A wireless repeater device receives the signal from an existing Wi-fI network and rebroadcasts it, effectively expanding the coverage area. Repeater mode is commonly used to eliminate Wi-Fi dead zones and extend the range of a Wi-Fi network in larger homes, offices, or spaces where the original signal doesn't reach.

- Here in the above image, we can see that a Wi-Fi extender is used to extend the coverage area. It is used to extend the range of a wireless network.

Bridge Mode:

- Bridge mode is used to connect two separate networks or network segments wirelessly, allowing them to communicate with each other.



- In bridge mode, two wireless devices act as bridges. Each bridge connects to a separate network or network segment and communicates with the other bridge over a wireless link. This allows devices on both networks to communicate as if they were on the same network. This mode is often used when you want to connect two distinct network segments and pass traffic between them without the device in bridge mode performing any network address translation or routing function.

Ad Hoc Mode:

Ad hoc mode, traditionally associated with networking, has expanded its role in modern device configuration, notably in cases where devices like Google Home lack user interfaces and additional interfaces. The challenge lies in the initial setup, which is typically accomplished through the **following steps:**

- **Installation and Activation:** Users start by powering on the device and installing a dedicated control app on their smartphones.
- **Device as an Access Point:** When the device is powered on, it takes on the role of an access point (AP) and emits a network signal.
- **Direct Connection:** The smartphone establishes a direct, point-to-point connection by connecting directly to this network.
- **Configuration:** Through the smartphone, users can access the device's interface, enabling them to configure settings such as Wi-Fi network selection and passwords.
- **Wi-Fi Integration:** After configuration, the device connects seamlessly to the specified Wi-Fi network, discontinuing its own network broadcast and functioning as a regular Wi-Fi station.

This setup offers the advantage of both local and remote control, as both the programmed device and the smartphone share a connection to the same access point, enabling cloud-based control. This approach is widely adopted in contemporary IoT devices, including thermostats and smart TVs, underscoring the pivotal role of Wi-Fi in the initial setup process.

WiFi Deployment Use Cases:

1.Enterprise Wi-Fi:
- Commonly used in offices, retail environments, and other business settings.
- Essential for providing wireless connectivity to employees and customers.
- Supports various devices and applications in a corporate environment.

2.City Mesh Wi-Fi:
- Involves covering an entire city or a portion with a Wi-Fi network.
- Aims to make public Wi-Fi a basic utility, similar to water and electricity.
- Utilizes Wi-Fi routers on street lamps, poles, and infrastructure.
- Offers faster connectivity compared to cellular networks and is often free for residents.

3.Multi-Dweller Unit (MDU) Wi-Fi:
- Deployed in places where multiple people live in close proximity, such as hostels, apartment buildings, or shared living spaces.
- Ensures individual security by providing each resident with a unique password.
- Requires a different approach from standard coverage, focusing on secure access.

4.Hospital Wi-Fi:
- Ubiquitous in Western hospitals, providing connectivity for guests, patients, doctors, nurses, and administrators.
- Vital for real-time monitoring, transmitting patient data, and managing medical equipment.
- Requires uninterrupted and secure connectivity due to mission-critical applications.

5.Vehicular Wi-Fi:
- Integrates Wi-Fi technology into vehicles, allowing them to communicate with each other and with infrastructure.
- Enhances public safety by sharing information about road conditions and potential dangers.
- Supports vehicle-to-vehicle and vehicle-to-infrastructure communication.

6.In-Flight Wi-Fi:
- Available on airplanes above a certain altitude.
- Connects to the internet via satellite or cellular networks.
- Enables passengers to access the internet during flights, enhancing the travel experience.

7.Stadium Wi-Fi:
- Deployed in large stadiums and venues to provide connectivity for thousands of spectators.
- Aims to overcome challenges related to concrete structures and high user density.
- Enables fans to access the internet, watch replays, and share their experiences during events.

8.Bus Wi-Fi:
- Found in corporate buses in developed countries.
- Provides Wi-Fi access to passengers during transit.
- Utilizes various backhaul methods, including cellular, satellite, or bus station Wi-Fi, depending on location.

9.Smart Home Wi-Fi:
- Connects various smart devices within a home, enabling automation, control, and monitoring.
- Central to the concept of the "smart home," where appliances and gadgets are interconnected for convenience.

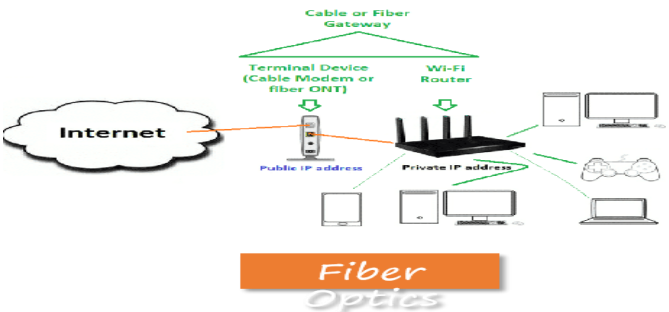
10.In-Train Wi-Fi:
- Deployed in high-speed trains travelling between cities and countries.
- Uses multiple routers inside the train for coverage.
- Utilises different backhaul methods depending on the train's location, including cellular, satellite, or even local station Wi-Fi.

Types of Wi-Fi Internet Connectivity Backhaul

Backhaul refers to the network connections that link smaller networks to a larger, central network or the internet. It is the primary communication link between the core network, or backbone, and the smaller sub-networks, such as those found in remote areas or at the edge of the main network.

We need backhaul technology to establish a connection to the internet. There are various technologies that facilitate backhaul, and below are a few of them.

FIBER OPTICS



Fiber Optic Cables:

- Fiber optic cables are thin strands of glass or plastic that transmit data using light signals.
- They can carry a large amount of data at incredibly fast speeds.

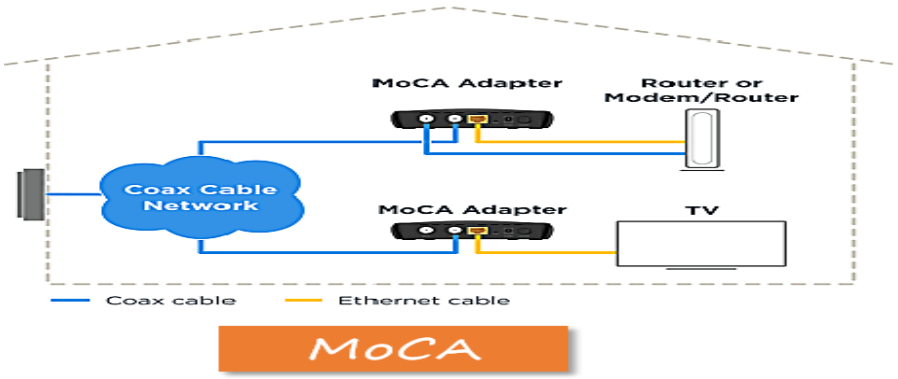
Advantages of Fiber Optic Backhaul:

- High Speed: Fiber optics can transmit data at very high speeds, allowing for faster internet connections.
- Bandwidth: They can handle a large amount of data simultaneously, providing more bandwidth for multiple users.
- Reliability: Fiber optics are less prone to interference and signal loss, resulting in a more reliable connection.

How it Works:

- Internet service providers (ISPs) use fiber optic cables to connect their local networks to larger data centers or internet exchange points.
- Data from your local network travels through these fiber optic cables to reach the broader internet.

MOCA



MoCA is a technology that uses the existing coaxial cables in your home, typically used for cable television, to transmit data.

Coaxial Cables:

- Coaxial cables are the thick cables commonly used for cable TV connections.
- They consist of a central conductor, insulation, a metallic shield, and an outer insulating layer.

Advantages of MoCA Backhaul:

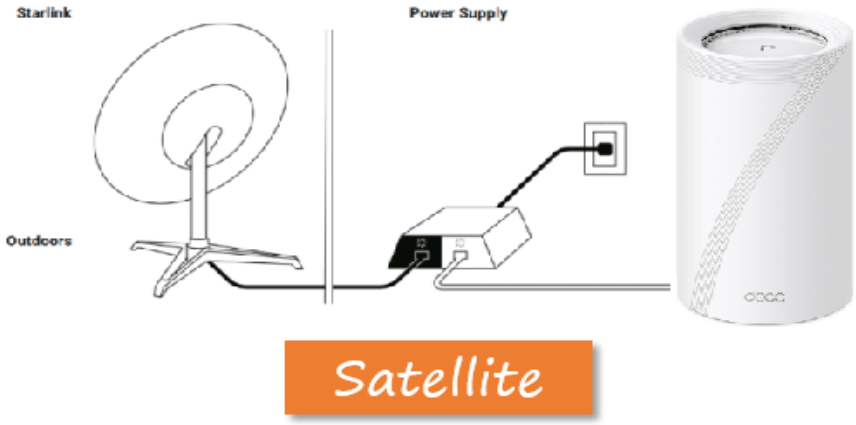
- Utilizing Existing Infrastructure: MoCA utilizes the coaxial cables that might already be in place for cable TV, reducing the need for additional wiring.
- Reliable Connection: Coaxial cables are known for providing a stable and reliable connection.
- High Speeds: MoCA can deliver high-speed data transmission, suitable for internet connectivity needs.

How it Works:

- MoCA adapters are connected to the coaxial outlets in your home.
- These adapters enable the existing coaxial cables to carry data signals, creating a network that links different devices within your home to the main internet connection.

SATELLITE:

Instead of using cables or wires, a satellite internet connection relies on signals sent to and from satellites orbiting the Earth.



Satellite Advantages:

- Global Reach: Satellites can cover vast areas, making them ideal for connecting remote or rural locations where laying cables would be challenging.
- Quick Setup: Setting up a satellite connection is often faster than installing physical cables over long distances.

How it Works:

- Your home or office has a satellite dish that communicates with a satellite in space.
- When you send a request (like opening a webpage), the data travels from your device to the satellite, then to a ground station on Earth, and finally, it enters the larger internet.

Advantages of Satellite Backhaul:

- Remote Connectivity: It's a game-changer for places where laying cables is impractical.
- Speeds Improving: While traditionally considered slower than some other types of connections, satellite technology is evolving, and speeds are improving.

CELLULAR:

Cellular networks are the ones that your mobile phone uses to connect to the internet. They use radio waves instead of physical cables.

Cellular Connection Advantages:

- Wireless Convenience: No need for cables. You can connect to the internet using signals in the air.
- Mobility: You can access the internet from almost anywhere, not just at home.

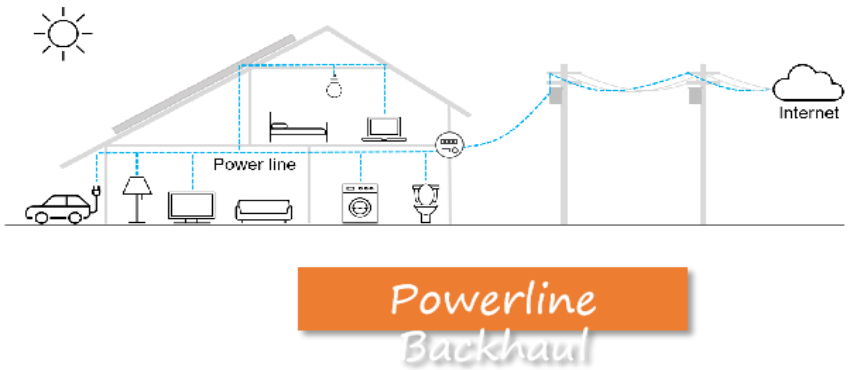
How it Works:

- Your device, whether a smartphone or another gadget, communicates with nearby cell towers.
- These towers are like internet relay stations. They receive and transmit your data to a central network, connecting you to the wider internet.

Advantages of Cellular Backhaul:

- On-the-Go Connectivity: It's not limited to a fixed location. You can access the internet wherever there's cellular coverage.
- Quick Setup: Setting up a cellular connection is often faster than laying cables, especially in remote areas.

POWER LINE BACKHAUL:
Powerline technology uses your home's electrical wiring to carry data signals.



Powerline Connection Advantages:

- Utilises Existing Wiring: No need for new cables. Powerline uses the electrical wiring already in your home.
- Easy Setup: Plug and play. You just need special adapters that connect to your power outlets.

How it Works:

- You plug one powerline adapter into an electrical outlet near your internet source (like your router)
- Another adapter goes into an outlet near the device you want to connect to the internet.
- Your data travels through your home's electrical wiring, jumping from one adapter to another, reaching its destination.

Advantages of Powerline Backhaul:

- No Extra Wires: You don't need to run new cables through your home. The existing power outlets become your internet connection points.
- Convenient Setup: It's like extending your internet network using the same outlets you use for powering devices.

WiFi Technology Challenges:

- **Loss of Signal Strength Due to Distance and Obstacles:**
  One significant challenge in wireless technology is the loss of signal strength as a result of the signal propagating through the air. When devices are close to each other, they can communicate effectively, but as the distance between them increases, signal strength decreases due to attenuation. Additionally, physical obstacles like buildings and walls can further reduce signal strength by causing reflections, diffractions, and scattering. Solutions to this problem often involve signal amplification and optimization of transmission power.

- **Multipath Interference:**
  Multipath interference occurs when multiple copies of a signal arrive at the receiver due to reflections and scattering. These signal copies may have different delays and phases, leading to constructive or destructive interference, causing fading and signal distortion. Adaptive equalization and diversity techniques, such as using multiple antennas, are used to mitigate multipath interference.

- **Battery Life Constraints:**
  Battery life is a common challenge, especially for wireless devices like smartphones and IoT sensors. These devices need to transmit and receive data efficiently to conserve battery power. Techniques like power management, duty cycling, and low-power communication protocols are used to extend battery life.

- **Medium Access and Collisions:**
  In scenarios where multiple devices are trying to access the same wireless medium simultaneously, collisions can occur, leading to interference and degraded performance. Medium access control (MAC) protocols, such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), are used to manage access and avoid collisions by enforcing rules for device transmissions.

- **Limited Spectrum Availability:**
  The availability of unlicensed spectrum is finite, leading to challenges in managing frequency allocations efficiently. Spectrum management and channel reuse strategies are crucial to ensure effective utilization of available frequency bands.

- **Security Concerns:**

Wireless networks are vulnerable to various security threats, including eavesdropping, data breaches, and unauthorized access. Robust encryption, authentication, and security protocols are essential to protect against these threats.

- **Mobility and Quality of Service (QoS):**
  Ensuring seamless mobility for users as they move between access points or cells while maintaining consistent QoS, especially for real-time applications, is a significant challenge. Traffic prioritization and handover mechanisms address these concerns.

- **Limited range:**
  The constraint where Wi-Fi signals can only travel a certain distance from the access point or router before their strength diminishes significantly. This limitation poses challenges in terms of coverage and connectivity, especially in large spaces or outdoor environments. Addressing limited range challenges involves optimizing signal strength and deploying additional access points to ensure adequate coverage.

- **Interference:**
  The disruption or degradation of wireless signals caused by external factors, such as other electronic devices or neighboring Wi-Fi networks. This interference hinders the quality and reliability of wireless communication and is a significant challenge in ensuring stable Wi-Fi connections.

WiFi Network Management/Business Challenges:

In addition to technical challenges, there are business challenges associated with large-scale wireless technology deployments. These include planning and optimizing network coverage, addressing coverage gaps, ensuring return on investment (ROI), and developing sustainable business models, such as offering Wi-Fi services or monetizing network infrastructure.

- **Troubleshooting and Maintenance:**
  Network troubleshooting is essential to identify and resolve issues that can impact network performance. Tools and processes for diagnosing and resolving connectivity problems are critical for maintaining reliable wireless networks.

- **Spectrum Sharing and Interference:**
  As more wireless devices and technologies coexist, managing spectrum sharing and mitigating interference between different services and networks become increasingly important. Regulatory bodies and industry standards help address these challenges.

- **Monetization and Revenue Models:**
  Businesses need to consider revenue models for their wireless technology investments. Monetization strategies may involve charging for access, offering value-added services, or partnering with advertisers to provide free Wi-Fi in exchange for promotional opportunities.

- **Large-Scale Deployments:**
  Deploying wireless technology on a large scale requires careful planning, including determining the number of access points needed, optimizing coverage, and addressing interference in high-density environments like stadiums or office buildings.

- **Seamless roaming:**
  The capability of Wi-Fi devices to smoothly switch between different access points within the same wireless network without experiencing disconnections or disruptions. It's a critical aspect of ensuring uninterrupted connectivity for users as they move within a Wi-Fi network's coverage area. This capability addresses the challenge of maintaining consistent and reliable wireless connections, especially in environments with multiple access points, such as large office buildings, hotels, or public venues.

- **The need for infrastructure:**
  The essential physical and technological elements required to establish and maintain a Wi-Fi network. This infrastructure includes access points, routers, switches, cabling, and network management systems. It addresses the challenge of creating a robust and reliable network foundation to support wireless connectivity, ensuring that users can access the network seamlessly and efficiently.

- **Network planning:**
  The process of strategically designing and organizing a wireless network infrastructure. It involves determining the optimal placement of access points, channel allocation, coverage areas, and capacity to ensure efficient and reliable wireless connectivity. Network planning addresses the challenge of deploying a Wi-Fi network that meets performance, coverage, and capacity requirements while optimizing resource usage and minimizing interference.