Study on Long Range WiFi Network

BHUTAN INFOCOMM AND MEDIA AUTHORITY
ROYAL GOVERNMENT OF BHUTAN THIMPHU, BHUTAN

July 2022

1. Background

Many people want reliable internet access throughout their homes, as well as in their surroundings. But this becomes challenging and expensive in most cases, like in the larger buildings. However, long-range WiFi networks provide a solution to this. Long-range WiFi networks are low-cost, unregulated point-to-point network connections, as an alternative to other fixed wireless, cellular networks or satellite internet access that can help improve internet connection throughout customer premises. It can share the internet connection with another building or simply extend the WiFi signal outside.

Outdoor point-to-point (P2P) arrangements can be extended with many miles between stations, through use of directional antennas. There are two ways to extend the range of the wireless signals viz: *long range outdoor network* and *long-range point to point network*.

This study will focus on the point-to-point long range WiFi network and the main objective is to learn the working process and associated costs involved for its connecting network.

2. How does Long Range WiFi Networks work?

All connectivity devices supply the strongest signal when you are closest to them. The further you move away the weaker the signal becomes. For that reason, both outdoor and point to point networks use high-power and high-gain antennas to extend the range of your wireless signal, but do so in different ways and require different equipment.

A. Long-Range Outdoor Networks:

It makes use of your existing internet connection and relays it outside to improve your outdoor WiFi connection. Long-range WiFi networks are used to extend WiFi connection outside or give the user the ability to access a network from approximately 1.5 km under perfect conditions. The distance at which it will extend the signal or grab the signal will depend on the out-door antenna type and obstructions that block the WiFi signal's path.

The main reason for WiFi connections not reaching outdoors is due to building material and obstacles blocking or weakening the signal. Outdoor extenders can bypass all of the obstacles and extend the internet into consumer premises. Many people use range extenders and mesh networks to improve their internet coverage outdoors. Those devices work well, but they have to be within a certain distance from the router and only cover a certain range.

Outdoor WiFi Access Points (AP) can be used to extend the range even further. The AP can be mounted on a pole, j-pole, tripod, or any existing mast outside. The antennas on the AP should have a clear line of sight with the area you want to have coverage in. To extend your internet

connection, the AP needs to be wired with your router/switch. The wires help bypass the building material and obstacles that weaken or block the WiFi signals.
Between the home router and the AP, a small PoE (power over ethernet) adapter is used to feed power and data to the AP. Ethernet cables are used to establish the connection between the router and AP. One end of the first cable connects to the ethernet port on the back of the router, and the other end connects to the LAN port on the adapter. The second cable connects to the AP and the PoE port on the adapter. To officially initiate the connection between the router and the AP, the PoE adapter needs to be plugged into a wall outlet. Once connected, the antennas on the AP will broadcast the signal into the desired area. As a result, all devices outside will be able to enjoy a reliable WiFi connection. To extend the WiFi range even further, you can connect a long-range WiFi antenna to the AP using an SMA connect.

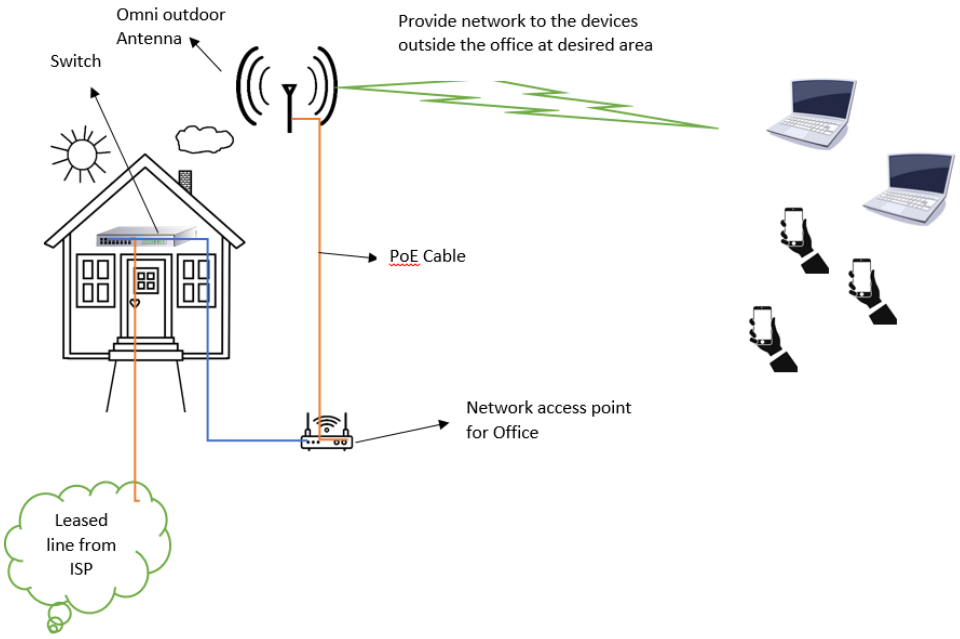

Figure no.1: Network diagram for long range outdoor WiFi network

B. Long Range Point to Point Networks:

They bridge user internet connection between two buildings or two stations. It can be also achieved by getting an added internet plan or a WiFi hotspot, but it can get expensive. In the long run, point to point networks can help save money while enjoying reliable internet in two different locations for a single ISP source connection. Customer Premises Equipment (CPE) antennas are used to relay WiFi signals from a user base station to a distant building.

The building can be a few feet to a few miles away from the main structure, it just depends on the size. Under perfect conditions, routers can only cover areas up to 150 - 300 feet. That's not enough to reach a detached building in most cases. Therefore, the P2P long-range systems help stretch the internet connection between the two buildings separated by considerable distances which would not be possible with the routers. According to one of the ISPs using a long range WiFi network, the Ubiquiti antenna they are using can extend the range up to 30-40 km having a perfect line of sight and they also mentioned that the distance coverage depends upon the antenna type and line of sight.

A long-range WiFi antenna (usually a directional WiFi antenna) and a WiFi repeater are needed to pull in the signal from the source building with a reliable internet connection. Some models only need one antenna for the detached building, others require an additional antenna for the source building. Ideally, the antennas should be mounted on the roof of the buildings. For optimal use, the antenna on the detached building needs to have a clear line of sight with the source building or the second antenna.

The figure below shows the set-up of the Long Range P2P WiFi network.

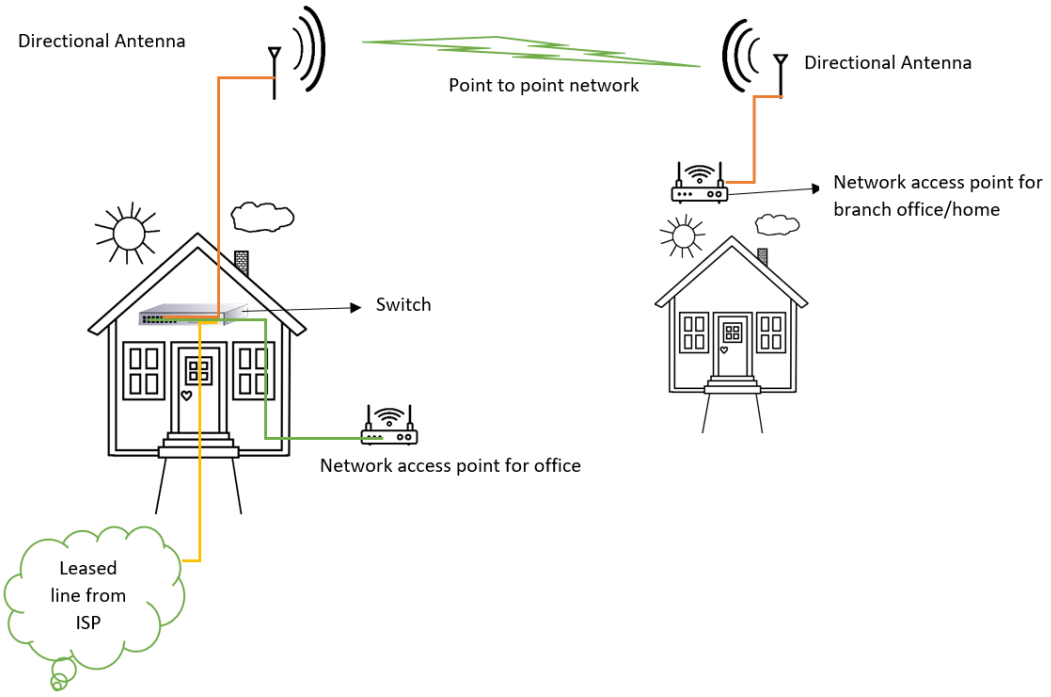

Figure no.2: Network diagram for point to point long range WiFi network

Inside the detached/receiver building, a router is needed that will be used to broadcast the wireless signal into the desired areas. Any router will work just fine, but a router that will support the amount of data consumption and the number of users are demanded.

Ethernet cables set up the connection between the repeater and the router. Between the two devices, a PoE adapter is used to provide the repeater with power and data. An ethernet cable connects the repeater to the adapter, and an ethernet cord connects the adapter to the internet port on the back of the router. After the cables are connected, the PoE adapter and the router can be plugged into a wall outlet.

Plugging in the adapter and the router won't automatically cause the internet to start flowing from one building to another. The router in the detached/receiving building will need to be configured. After the configuration process, the antenna will pull in the signal from the source directional antenna and the router in the receiving building will broadcast the signal inside the building for multiple users to enjoy.

However, some people only need an internet connection for one device. There are two methods that can be used to achieve this: The ethernet cable connected to the router is what carries the internet connection. Users can simply unplug the cable and connect it to a desktop, laptop, or a smart TV. Rather than using a router, you could use a USB WiFi adapter. The USB connects to your computer and picks up the WiFi signal through its antenna.

If the user wants to increase the range of the antenna, they can detach the standard antenna and connect any long-range wireless antenna. A coaxial cable would be needed to connect the antenna to the USB adapter. With the new antenna, users can pick up an internet connection from a further distance. A great benefit point to point systems offer is a better connection in areas with free internet.

3. Features of a Long-Range WiFi Network device.

One of the most important components of long-range WiFi systems is the long-range antennas. Without them, it would be impossible to send and receive signals at high speeds over long distances. The type of antenna and the strength of the antenna will determine the range and the coverage area of the signal. Before purchasing a long-range WiFi network, users have to be familiar with the types of antennas available, the antenna’s strength, and the antenna’s frequency bands.

A. Outdoor WiFi antennas: Omni-directional and Directional antennas

(i) Omni-directional Antennas

Omni-directional antennas send and receive signals from a 360-degree angle and they have a circular beamwidth, allowing them to send and receive signals from every direction. Their range is shorter than a directional antenna, but the coverage area is larger. They are ideal for long-range outdoor networks.

(ii) Directional Antennas

The Directional antennas focus all of their power in one direction. Therefore, they can send and receive signals from a farther distance than an omni-directional antenna. However, their coverage area is a lot smaller. Rather than having a circular beamwidth, they have a triangle-shaped beamwidth. They will work best for point to point use cases. The most common directional antennas are parabolic grids, panels, and yagi antennas.The distance coverage depends upon the type of antenna used, while it can have minimum distance upto to 1.6 km and maximum distance upto 30+km under perfect condition (line of sight). ISP provider Bitcom in Bhutan had used Motorola Canopy AP & SM 2.4 GHz and presently they are using Ubiquiti as an antenna for the setup.

a. Ubiquiti 5 GHz High Performance airMAX ac Bridge

Figure no.3: Ubiquiti 5 GHz High Performance airMAX ac Bridge

Features:

- Model: PBE-5AC-Gen2,and PBE-5AC-ISO-Gen2
- Software : airOS8
- Range: 15 Km
- Frequency Band: 2412-2472MHz | 5150-5875MHz

- Transmitter power: 25dBm (max)
- Receiver Sensitivity: -96dBm (min)
- Data Throughput: 450Mbps +
- Max Power Consumption: 8.5 Watt
- Operating Temperature: -40°C to 70°C

b. Ubiquiti Full-Duplex, Point-to-Point Gigabit Radio

Figure no.4: Ubiquiti Full-Duplex, Point-to-Point Gigabit Radio

Features:

- Models: AF-24, AF-24HD, AF-5, AF-5U
- Max Power Consumption: 40W
- Operating Temperature: 40 to 55
- Operating Frequency: 5470 - 5950 MHz (for AF-5) and 5725 - 6200 MHz (for AF-5U)
- Maximum range: 100+ Km
- Data Throughput: 1.2+Gbps
- Gain: 23dBi
- Max Transmitted Power: 47dBm
- Receiver Sensitivity: -95dBm

c. Motorola Canopy AP & SM 2.4 GHz.

Features:

- Advertised: up to 8 km with integrated antenna. Up to 24 km with a passive reflector only on the subscriber module side.
- Antenna alignment: Audible antenna alignment alarm
- Data Rate: 20 Mbps, 14 Mbps useful throughput
- Latency: 5-7 ms
- POE: Supported (802.3af)
- Radio type: Time Division Duplexing/Time division Multiple Access (TDD/TDMA)
- Receiver Sensitivity: -86 dBm (typ)
- Antenna type: 2.4 GHz 60 Degree Integrated Sector Antenna
- Security: DES, Proprietary Scrambling Mechanism; optimal AES Encryption
- Item Type: Access Point (AP)
- Operating modes: Point to Multipoint, Point to Point

Figure no.5: Motorola Canopy AP & SM 2.4 GHz

(iii) Gain of the antenna

The Gain (dB) measurements show how much signal strength can be gained from the antenna. Higher dB measurements are better. The strength and reach of the antennas are measured in dBi. Unlike dB, a higher dBi measurement does not always mean that it's better. There is a trade-off associated with larger dBi measurements. As the dBi number increases, the antennas are able to reach further but the coverage area decreases.

(iv) Frequency band

All WiFi technology communicates through radio frequencies. The frequencies are in GHz (2.4GHz and 5GHz). The 2.4GHz band can reach further distances, but the data travels at slower

speeds. On the other hand, the 5GHz band is faster but has a shorter range. Many antennas are advertised as single-band or dual-band. Single-band antennas only work with one frequency band (2.4GHz or 5GHz), you can't change the band they are using. Dual-band antennas work with both frequencies, 2.4GHz and 5GHz. Some dual antennas allow you to switch between bands and others use both bands simultaneously[1].

4. Equipment Required for the Long Range P2P Network

Let us assume that the leased line internet is already available at the source location/building along with the network infrastructure such as internet switches. For instance, if we consider the BICMA office, we already have the leased line internet services with the internet switches. If we intend to share the BICMA internet to a new location/building separated by a certain distance using the Long Range P2P network, the following equipment is required. It is

(i) A pair of long range directional antennas (one at source and one at receiving end)
(ii) Ethernet cables for both the location (Source and destination)
(iii) Router/Switch at the destination end (considering that source already has)
(iv) Access points at the destination

5. Cost Approximation

The table below shows the approximate cost for establishing the long range P2P WiFi networks:

Sl.no	Materials	Quantity	Price (Nu)
1.	Router/Switch	2	10,000 *2 = 20000
2.	Ethernet cable	APR	5000
3.	Antenna	2	68000 per pair
4.	Total		93000

Therefore, for a single long range P2P connection, considering the internet is already available at the source, the approximate amount of Nu. 93000.00 is required to establish the internet sharing through a long range P2P connection.

[1] https://www.signalboosters.com/blog/what-is-a-long-range-wifi-network-and-how-does-it-work/

6. Security issues related to Long range wireless network sharing[2].

The risk of attacks occurring on wireless LANs is high. There are a number of reasons for the increase in attacks, but the main one is that the nature of a wireless network is to provide easy access to end users, but this ease of access creates a more open attack surface. Unlike a wired network that requires an attacker to physically access part of the network, a wireless network only requires that the attacker be in close proximity. One of the most important basic fundamentals that a person or company needs to be aware of when deploying a wireless network is the importance of frequencies. Frequencies are used by equipment that is being deployed, and it affects the amount of interference that the network will be subject to, depending on the specific environment.

There are two main frequency bands that are used for wireless LANs- 2.4 GHz and 5 GHz bands. From a security perspective, the choice of frequency does not greatly affect the security risk of the network. What it does affect is the number of available non-overlapping channels that are available on the network. But, for the most part, this will not affect security. That is, except when an attacker is attempting to jam or block a specific frequency to force wireless endpoints to switch Access Points (AP).

However, extending wifi range can potentially increase the risk of getting hacked. Security researchers from IBM have found a critical vulnerability with Wi-Fi extenders from TP-Link, a popular router company. The vulnerability allowed a potential attacker to get control of the extender, which could be used to redirect the victim's traffic and lead people to malware, IBM said in a blog post. These malware could be further used to hack into the internal networks or gain access to the device remotely. The device manufacturing company has patched the device to not allow such things to happen in the future.[3] This is only for some TP-Link Routers, therefore other Wi-Fi extenders may also be in threat of such things.

If a proper firewall is installed and the network access is blocked for the user to access only to the external network, then it might be able to prevent the internal network from getting accessed by the external user. Meanwhile, there are no security risks if there are no database servers maintained by a particular firm/office in that network. Such extension of WiFi services may be implemented only for insensitive office networks. The offices which have internal database servers hosted for its own purpose may not be recommended to implement such services.

---

[2] https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats
[3] https://www.helpnetsecurity.com/2019/06/18/vulnerable-tp-link-wi-fi-extenders/

7. Challenges of Long-Range Wi-Fi

Methods that increase the range of a Wi-Fi connection may also make it fragile and volatile, due to various factors including:

- Landscape interference

Obstacles are among the biggest problems when setting up long-range Wi-Fi. Trees and forests attenuate the microwave signal, and hills make it difficult to establish line-of-sight propagation. Rain and wet foliage can decrease range further with extreme amounts of rain.

In a city, buildings will impact integrity, speed and connectivity. Steel frames and sheet metal in walls or roofs may partially or fully reflect radio signals, causing signal loss or multipath problems. Concrete or plaster walls absorb microwave signals significantly, reducing the total signal. Hospitals, with their extreme amounts of shielding, can require extensive planning to produce a viable network.

- 2.4 GHz interference

Microwave ovens in residences dominate the 2.4GHz band and will cause "meal time perturbations" of the noise floor. There are many other sources of interference that aggregate into a formidable obstacle to enabling long-range use in occupied areas. Residential wireless phones, USB 3.0 Hubs, baby monitors, wireless cameras, remote car starters, and Bluetooth products are all capable of transmitting in the 2.4 GHz band.

Due to the intended nature of the 2.4 GHz band, there are many users of this band, with potentially dozens of devices per household. By its very nature, "long range" connotes an antenna system which can see many of these devices, which when added together produce a very high noise floor, whereby no single signal is usable, but nonetheless are still received. The aim of a long-range system is to produce a system which over-powers these signals and/or uses directional antennas to prevent the receiver "seeing" these devices, thereby reducing the noise floor.

Annexure

Some of the images of the long range P2P antenna deployed by the ISPs in sharing the internet is given in the pictures below:

Figure no.6: Long range WiFi with Ubiquiti antenna setup at Changangkha

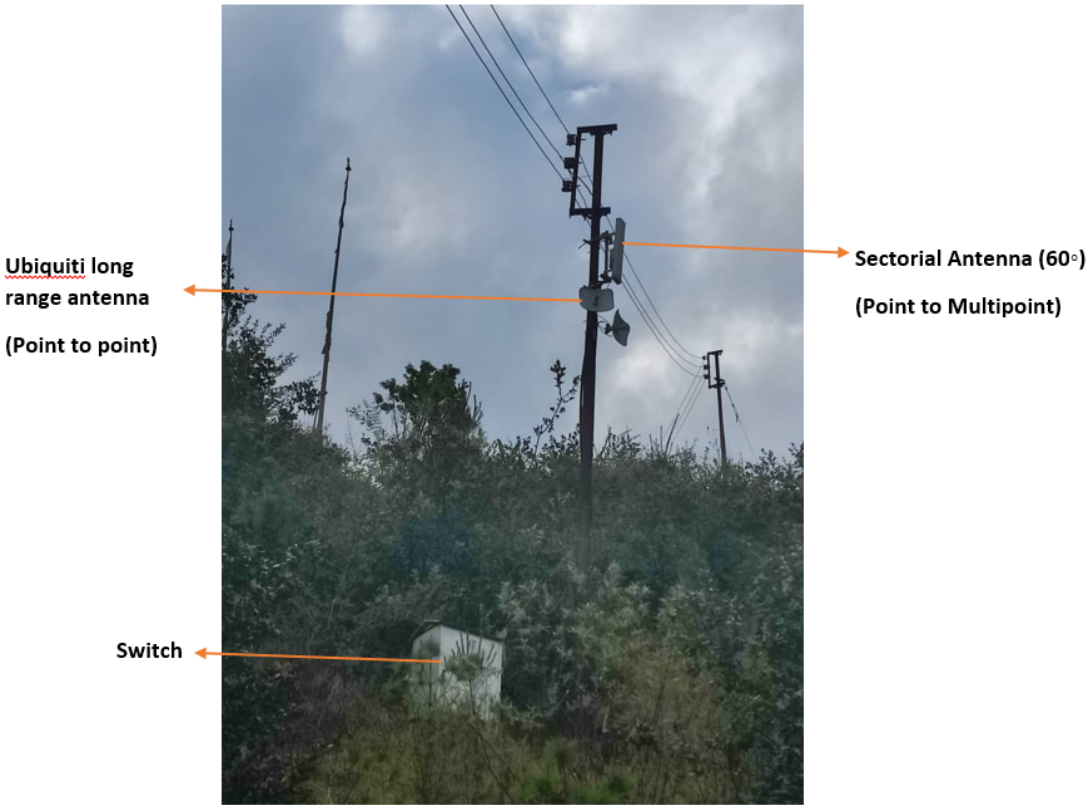

Figure no.6.1: Labeled Long range WiFi setup

Figure no.6.2: Long range WiFi Receiver at Lungtenphu BPC Sub-station