CHAPTER 2

THEORETICAL FOUNDATION

Theories about wireless networks especially 802.11 and 802.16 will be discussed in this chapter. This chapter functions as a foundation to the research of the thesis. General information about Wifi and Wimax is essential to become the underlying material for the development of the thesis. The material will also cover the trend and usage of each technology. Telecommunication companies have already been using Wifi by providing hotspots in the urban areas. This fact becomes an interesting point of view in comparing Wifi with Wimax. In Indonesia Wimax has not been implemented. Therefore Wimax research will have more attention in order to satisfy the needs of the thesis.

2.1 Wireless Network

The basis of Wifi and Wimax are wireless network technology. The evolution of networking technology made an impact in the development of network infrastructures. The Internet is a growing technology that changes the world. Today it has become an important factor in human needs. People use it for education, entertainment, and communication purposes. Using it they can browse for whatever information they wish to acquire. One benefit of the Internet is the control that people have over the information. A teenager wish to use online social networking website, people exchange emails, an office meeting using teleconference, and more applications using the Internet. Internet is becoming a life style. Therefore people

need Internet wherever they go, in relation to the level of mobility and business people have.

In the early days of networking, people must use a stationary computer in order to connect to the network. The computer connects to the Local Area Network using wires. Then the LAN connects to the modem. However, today people have the need for mobility. They need the technology of networking that can satisfy their need for mobility. Nowadays coffee shops, campus lobby, even in parks, and other public places are now equipped with wireless networking technology. This trend is caused by people's need of Internet. Today people can bring devices such as laptops, Palm devices, and smart phones to connect to a local area network using wireless networking technology. These devices have wireless networking capability. People just have to search for the nearest wireless network, and connect to the Internet.

The evolution of wireless networking grows from time to time. Wireless networking standards of 802.11 (Wifi) is commonly used as the basis of wireless LAN. The technology of wireless WAN (Wide Area Network) is an interesting topic to be discussed. Wireless WAN covers more area than wireless LAN. The coverage is nationwide and provided by telecommunication carriers. While wireless LAN covers a small fixed area, Wireless WAN has a broader coverage. Mobile Users such as a traveler traveling from city to city can benefit from this technology. Moreover, they can connect when they are not stationary with a great distance difference between one place to another. The technology of Wireless WAN that will be discussed is 802.16 (Wimax).

2.2 Wifi Technology

Wireless LAN is a technology that connects two or more devices without the use of wires [1]. It allows user to have mobility in using their devices. Gadgets such as laptops, smart phones, PDAs benefits from this technology, as they can connect to a nearest network wirelessly. The standard of Wireless LAN is 802.11 as given by the IEEE (Institute of Electrical and Electronics Engineers).

2.2.1 Characteristics

Wifi has the same concept as Local Area Network, however it uses radio frequencies to send and receive data. The connection underlies high-speed wireless networking. The radius of a Wireless LAN is 50 meters indoor and 250 meters outdoor. Wifi is another name for wireless LAN. Wifi stands for wireless fidelity. In order to work, Wifi needs an access point that is connected by wire. It is used to transmit Wifi signal to devices that wants to connect to the wireless network [2].

Wifi has a transfer rate up to 54 Megabits per second in the 5 GHz Band. There are several types of Wifi. The standard version of 802.11 has the transfer rate of 2 Mbps. The next technology is 802.11b, with transfer rate up to 11 Mbps in the 2.4 GHz band, and then the next generation is 802.11g with 54 Mbps, 802.11a with 54 Mbps, and the latest one is 802.11n with the largest transfer rate of 540 Mbps [3]. The evolution of wireless LAN technology affects the way consumer buys devices in regard to the usage of networking especially wireless networking. Laptops nowadays are equipped with Wifi technology. In the campus world, Wifi is commonly used. Libraries, labs, even the campus lobby provides hotspot to the students. This shows that the usage of Internet is essential for studying or for the need of entertainment. Other than campuses, airports, hotels, offices, shopping malls are nowadays provided

with Wifi connection. In hoping that the user will be more convenient, Wifi are sometimes provided freely.

2.2.2 Operation Modes

The simplest way of connecting to a Wifi network is using an access point. The access point can be a form of a router, a Wifi modem, or a Wifi transmitter access point. The user must have adapter cards to receive and send data to the access point, which is connected to the Internet with wires. The communication between wireless networks works like a two-way radio network. First, the adapter converts data into radio signal, and then it sends them to the router, which decodes the signal and sends it to the Internet through Ethernet cable. It also works vice versa. Wifi has the advantage of easy installation and inexpensive.

Figure 2-1 Wifi network [20]

There are two types of operation in Wireless LAN, ad-hoc mode and client/server mode. The client/server mode is sometimes referred as the infrastructure mode. The configuration involves terminal and base station. The station is in a form of an access point (AP), which creates a coverage area. Terminals such as laptops or computers

connect and communicate with the access point. The access points connect with the Internet using wires [4].

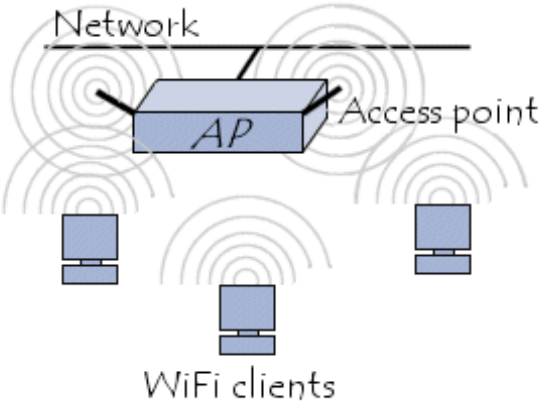

Figure 2-2 infrastructure mode [4]

The second mode is the ad-hoc mode. This mode consists only independent stations that also can be an access point. In other way, the terminals themselves create the network. This is possible with the help of network adapters. With the mobility of terminals, the ad-hoc mode is specified as a movable network, however the range is limited [4].

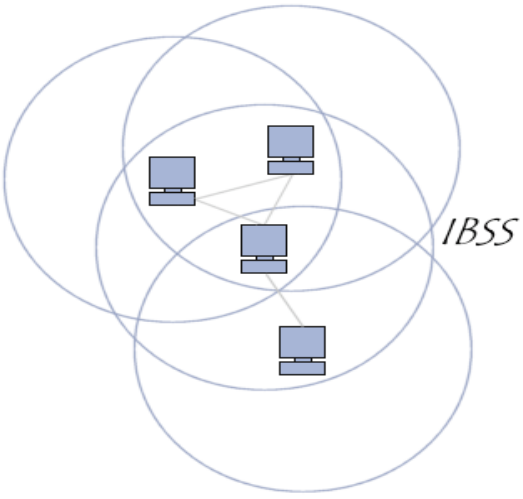

Figure 2-3 Ad-hoc mode [4]

The ad-hoc mode let stations or computers for a peer-to-peer network and each one acts as an access point and a client at the same time. The formation is called independent basic service set (IBSS). IBSS is a network formed between two or more stations. Each station has a range of wireless network. The overall range of the network is determined by each station's range. This makes exchange of data possible between users [4].

2.2.3 Protocols

There are two protocol layer specifications for 802.11, Physical (PHY) and Media Access Control (MAC). PHY is layer one, and MAC is layer two. Layer one (PHY) defines the modulation scheme and signaling technology used for transmission through radio frequencies. Layer two (MAC) defines how to access the physical layer. MAC layer also specifies services related to the radio resources and mobility management. There are three specifications of the physical layer. First one is infrared, and the other two is radio frequency (RF) transmission methods. There are two transmission methods. Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). Modulation techniques for the DSSS are Differential Bi and Quadrature Phase Shift Keying. Both techniques are also called DBPSK and DQPSK. FSHP uses 2 – 4 Gaussian Frequency Shift Keying (GFSK) as the modulation specifications. Wireless LAN devices must have the same physical layer standard to be interoperable. A device with DSSS cannot work with FHSP one [5].

802.11 standard has several generations of protocols that evolves based on the networking technology of the specification.

802.11 (Legacy)

The original version of wireless LAN protocol is 802.11. It was released in 1997 and clarified in 1999. However, nowadays it is not used or produced. The net bit rates for this protocol are 1 or 2 megabits per second (Mbit/s). It has three alternative physical layer technologies. The first one is diffused infrared technology, which operates at 1 megabit per second. The second one is Frequency-Hopping Spread Spectrum (FHSS) with the operation speed of 1 or 2 megabits per second. The last one is direct sequence spread spectrum, which also performs at 1 or 2 megabits per second. As an alternative to the infrared technology, FHSS and DSSS used microwave transmission at 2.4 GHz frequency. 802.11 with DSSS technology were replaced by 802.11b [3].

802.11a

The next generation of wireless network protocol is 802.11a. The standard was made official in 1999. It is an upgrade from the original version with higher data rate of 54 Mega bits per second. It uses the 5 GHz band using the same core protocol as 802.11. The physical layer uses orthogonal frequency-division multiplexing (OFDM) technology, which provides better data rate of 54 Mbps. 802.11a has the advantage in using the 5 GHz band. It is less used than the crowded 2,4 GHz band. However, there is a disadvantage to this. 5 GHz band uses a smaller wavelength, therefore signals are more readily absorbed by walls and other solid objects, rather than 802.11b which uses the 2,4 GHz band. The signal range of 802.11a can be up to 30 meters outdoor and 10 meters indoor [6].

802.11b

In October 1999, 802.11b was released and made official and appeared on the market in early 2000. It has maximum transfer rate of 11 Mbps using the 2.4 GHz band. With 2.4 GHz band, it has the maximum range of 30 meters indoor and 90 meters outdoor. It uses the same media access methods as the original with the extension and upgrade to the DSSS modulation technique. The modulation technique used is complementary code keying (CCK). 802.11b was a success in terms of sales. It has better throughput than the original 802.11 but has lower price [7].

802.11g

The next protocol introduced was 802.11g. Introduced in June 2003, it operates in 2.4 GHz band, however the transmission scheme used is OFDM, the same as 802.11a. The maximum transmission rate is 54 Mbps. Devices of 802.11g are backward compatible with 802.11b hardware. 802.11g is an enhancement of 802.11b in terms of data rate. Maximum range is the same as 802.11b [8].

802.11n

IEEE 802.11n is an upgrade to other standards with 40 MHz channels to the physical layers and it supports MIMO (Multiple In Multiple Out) function. It also adds frame aggregation to the MAC layer. MIMO is a technology of using multiple antennas to improve communication performance rather than using single antenna. Previous 802.11 standards use 20 MHz channel width to transmit data. 802.11n has the channel width of 40 MHz. It also has the capability to switch between 2,4 GHz or 5 GHz frequencies. The maximum data rate is a whopping 540 Mbps with the 40 MHz maximum four spatial streams. It has the largest range of 50 meters indoor and 250 meters outdoor [9].

Protocol (year)	Related Terms	Speed (max)	Range (indoor)	Frequency	Compatibility
802.11a (1999)	Wi-Fi Wireless 'a'	54 Mbit/s	~10 meters (30')	5 GHz	None
802.11b (1999)	**Wi-Fi Wireless 'b' 11b**	**11 Mbit/s**	**30 meters (100')**	**2.4 GHz**	**Forward compatible with "g"**
802.11g (2003)	**Wi-Fi Wireless G 54g or 54G**	**54 Mbit/s**	**30 meters (100')**	**2.4 GHz**	**Backwards compatible with 802.11b**
802.11n (2008)	MIMO Wireless 'n'	540 Mbit/s	50 meters (160')	2.4 GHz or 5 GHz	Devices backwards compatible with 802.11b/g

Table 2-1 Wifi comparison [21]

2.2.4 Radio Frequency Channels

In wireless networks, there exists frequency bands are divided into channels for communication. Each country has a regulatory for channels to be used, allowed number of users, and the maximum power level to the ranged frequencies. The regulation exists because there is a constraint on RF channels used in various service of a country. The 802.11b/g/n standard specifies 2,4 GHz range of frequencies split to 14 channels of 5 MHz each, with the exception of 12 MHz spacing before channel 14 [3].

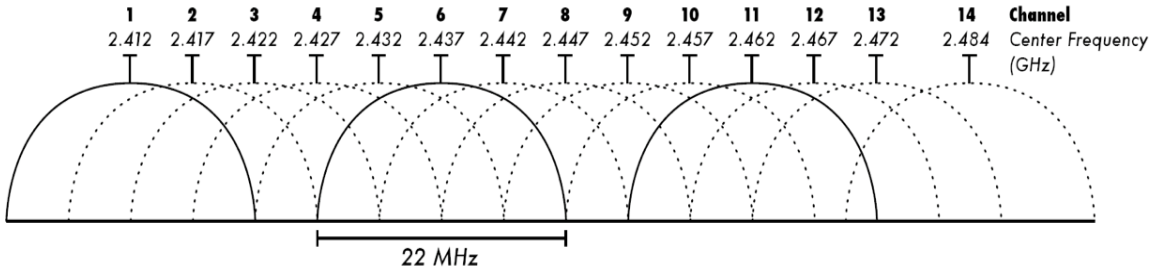

Figure 2-4 Wifi channel in 2,4 GHz band [3]

The protocol requires that each channel use a 22 MHz band. For a proper transmission, there need to be a 25 MHz separation to avoid interference. Therefore

channel 1, 6, and 11 are generally used. Figure 2-4 below explains the overlapping channels if all channels were used [3].

Channel	Lower Frequency	Central Frequency	Upper Frequency	Overlapping Channels
1	2.401	2.412	2.423	2,3,4,5
2	2.406	2.417	2.428	1,3,4,5,6
3	2.411	2.422	2.433	1,2,4,5,6,7
4	2.416	2.427	2.438	1,2,3,5,6,7,8
5	2.421	2.432	2.443	1,2,3,4,6,7,8,9
6	2.426	2.437	2.448	2,3,4,5,7,8,9,10
7	2.431	2.442	2.453	3,4,5,6,8,9,10,11
8	2.436	2.447	2.458	4,5,6,7,9,10,11,12
9	2.441	2.452	2.463	5,6,7,8,10,11,12,13
10	2.446	2.457	2.468	6,7,8,9,11,12,13,14
11	2.451	2.462	2.473	7,8,9,10,12,13,14
12*	2.456	2.467	2.468	8,9,10,11,13,14
13*	2.461	2.472	2.483	9,10,11,12,14
14*	2.473	2.484	2.495	10,11,12,13

Table 2-2 802.11 B/G RF channels [10]

2.2.5 Security

Security is an important factor in networking. Nowadays, there are many ways to break the security of a network. It can be clarified that there are security holes in wired networking. Hacking, bandwidth stealing, denial of service attacks, are few of the risks in networking. Now, the evolution of wired networking into wireless networking introduces us to new risks. Therefore, It is important to know how to secure the network.

WEP (Wired Equivalent Privacy)

WEP is a data transmission encryption of Wifi that is used to solve data transfer security. Data are encrypted to gain confidentiality and integrity. It uses RC4

symmetrical algorithm using 64-bit or 128-bit keys. Packets are encrypted first, then data are sent to the receiver. The receiver then decrypts the ciphertext into plaintext.

WPA (Wifi Protected Access)

WPA is created by the Wifi alliance to improve the disadvantages of WEP. It relies on authentication protocol and it has a strong encryption algorithm. The encryption algorithm TKIP (Temporary Key Integrity Protocol) provides a better security than RC4. It generates random keys and has the ability to change keys several times per second. This improves security greatly. However, WPA can only be used in infrastructure mode, which means it cannot be used on peer-to-peer wireless networks. WPA requires installing an authentication server (RADIUS server). It is used to identify users and set their privileges. For smaller networks, they can use WPA-PSK. It is a simplified version of WPA, only using same encryption key on all devices. It does not need a RADIUS server [11].

WPA 2

In June 2004, 802.11i standard was released. The standard specifies the use of AES (Advanced Encryption Standard). The standard has another name, which is WPA 2. Unlike WPA, WPA 2 supports both ad-hoc and infrastructure mode. The 802.11i standard defines two operation modes. The first one is WPA personal. It implements secure infrastructure based on WPA without the need to have an authentication server. The second mode of WPA 2 is WPA enterprise. This mode requires the network to have an authentication server and a network controller [12].

2.3 Wimax Technology

Wimax stands for Worldwide Interoperability for Microwave Access. It is a solution for point to multipoint network. Wimax supports wireless high-speed broadband Internet access and it has coverage similar to cell phone networks. The IEEE standard is 802.16. People can connect to universal Internet access anywhere they go. It operates similar to Wifi network, however with greater speeds, greater distances, and larger user. In rural and urban areas, there exist blackout areas. Blackout areas are areas that do not have coverage of network caused by no telephone or cable companies running wires to the remote areas. With Wimax, blackout area problem can be solved, as it can cover wireless networks up to 30 miles. The maximum bit rate for Wimax is 100 Mbps.

Many applications use Wimax as a backbone. One common application for Wimax is to provide last mile broadband access wirelessly. Wimax are also used for connecting Wifi hotspots to the Internet, provides data and communication services, and portable connectivity [13].

2.3.1 Wimax Background

The first generation of 802.16 specifies operation on 10 to 66 GHz frequency band. It was initially specified as a LOS (Line of Sight)-based point-to-multipoint broadband wireless network. In 2001 802.16 standard was completed. The standard was based on a single-carrier layer physical (PHY) layer. The MAC layer uses burst time division multiplexing (TDM) [14]

In 2003, a follow up to the standard was made official, which was 802.16a. It introduces an NLOS-based wireless network in the 2 to 11 GHz frequency. It uses orthogonal frequency division multiplexing (OFDMA)-based physical layer, whereas

orthogonal frequency division multiple access (OFDMA) were added to the MAC layer [14].

With further revisions, IEEE made the standard into 802.16-2004. It replaced preceding standards and became the first basis for Wimax solution. This standard is often referred as fixed Wimax, as it targeted fixed applications. In 2005, the standard was updated to 802.16e-2005 with the use of scalable orthogonal frequency-division multiple access (SOFDMA) [14].

Fixed Wimax provides broadband service that could include high-speed internet access, voice over IP, and other applications that needs high data rate. Point-to-multipoint applications are best suited to fixed Wimax technology. Those applications include:

- Broadband for Residential, Small office/home office (SOHO), and small- to medium- enterprise (SME)
- T1 Service to businesses
- Wireless backhaul for hotspots

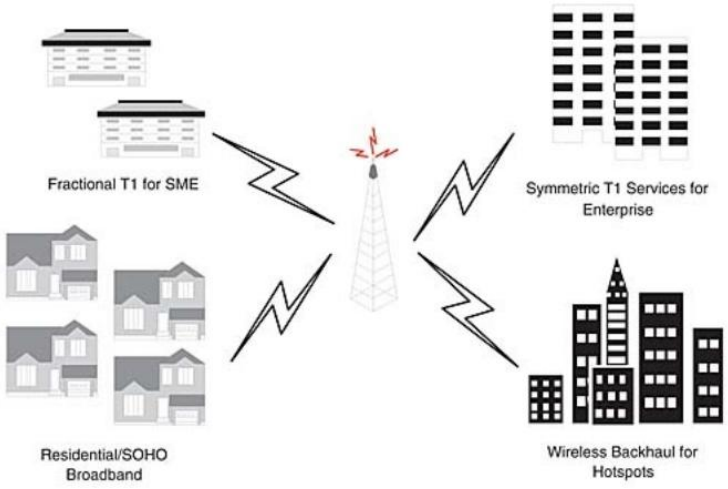

Figure 2-5 Point-to-Multipoint applications [17]

The next generation of Wimax protocol is 801.16e, which adds the capability of using multiple antennas with MIMO technology. Other advantages of 802.16e include benefits of power consumption, easy installation, coverage, bandwidth efficiency, and frequency reuse. 802.16e supports full mobility and it targeted mobile applications, thus the standard becomes a basis for mobile Wimax solution. It is often referred as mobile Wimax [14]. Mobile Wimax brings a new level of wireless broadband technology. It enables cell phone-like applications. It also has the capability of better building penetration [19]. The characteristics of 802.16 standards are summarized in table 2-6.

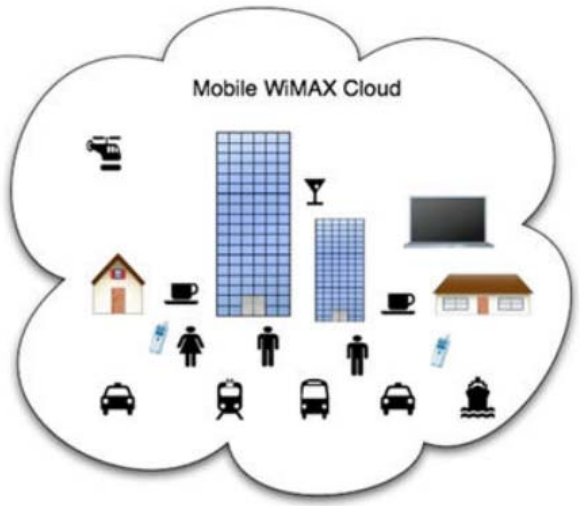

Figure 2-6 Mobile Wimax cloud [19]

	802.16	802.16-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/OFDMA	Burst TDM/TDMA/OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel bandwidths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz

Table 2-3 802.16 data standards [17]

In the business point of view, there are several advantages of Wimax. The first one is it can be an alternative to DSL and broadband home solution, as it upgrades the wireless technology. The second one, it is a competitor to the 3G world in mobile environments. Another one is it can become a backhaul for telecommunications tower and hotspots for Wifi. Therefore there are many business opportunities for Wimax. Today, ISPs and telecommunication provider competes to provide Wimax.

2.3.2 Operation Modes

Wimax technology consists of two elements. The first one is the Wimax tower or Base station. The second one is Wimax receiver which is also called CPE (Customer Premises Equipment). Wimax tower broadcasts radio signal similar to a cell phone tower and the coverage can achieve up to 30 miles with LOS (Line-of-Sight) mode. The receiver can be in form of a PCMCIA card or laptop that has the technology built in similar to Wifi receiver, or in the form of outdoor antenna that is installed in rooftops to receive signal from the base station. The tower connects to the Internet. It usually connects to the Internet service provider. Between towers there exists backhaul connection using microwave link, therefore one tower connects to another wirelessly. With this infrastructure, rural areas are provided with network coverage [15].

There two ways Wimax provides service, line-of-sight and non line-of-sight. Line-of-sight means there is an antenna dish pointing to a tower in the roof or a pole. The line-of-sight is more stable and has more bandwidth. Stability is one of the advantages as the Wimax uses high frequency on this service. The frequencies reach on to 66 GHz. The other benefit is there is less interference. The non line-of-sight service uses lower frequencies. Small antenna on laptops or computers connects to the tower. The frequency ranges from 2 – 11 GHz. Wimax works similarly like Wifi. It sends and receives data using radio signals. Wimax are designed specifically for outdoor areas [15].

There are two operation modes of Wimax. Point-to-multipoint (PMP) and mesh. The PMP is used for providing broadband access such as the connection to Internet service provider (ISP) or as a backhaul for GSM/UMTS base stations. Point-to-

multipoint structure consists of base stations (BS) and subscriber stations (SSc). The base stations propagates signal in a form of up-link and down-link channels, and all stations will share the channel. The subscriber stations must be in the line-of-sight of the base in order to receive the signal. Figure 2-5 shows the structure of PMP and mesh mode [14].

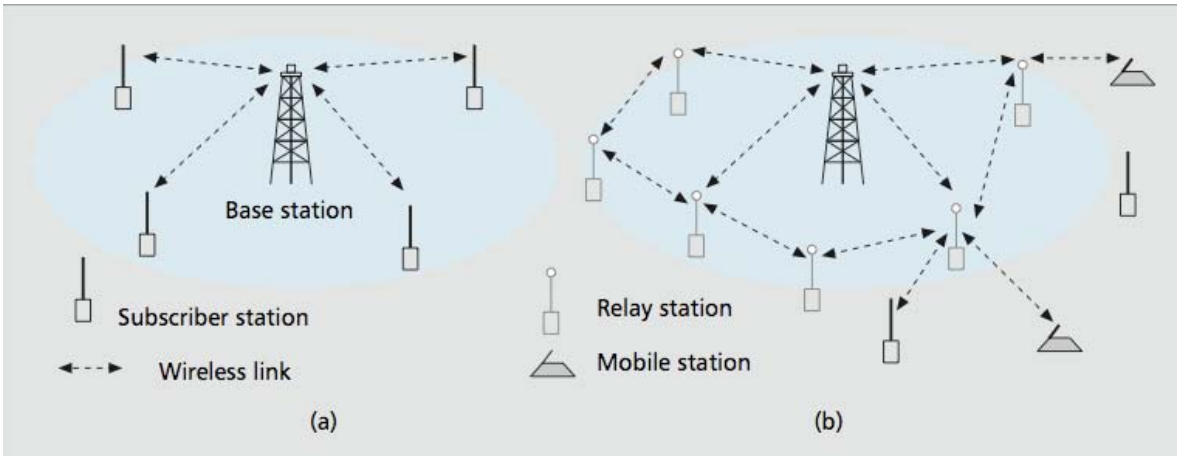

Figure 2-7 Wimax topology a. PMP b. mesh [14]

The mesh operation mode forms an ad-hoc topology. Each node can be a form of a router. Some stations can act as a base station, forwarding traffic to a different network. This mode is more flexible than PMP mode. There need not be a BS tower to form a network. This network is more mobile and flexible, as it can establish a WAN infrastructure quickly [14].

In terms of network scale, the smallest one is Personal Area Network (PAN). Bluetooth is an example for this. It connects devices in short distances. Local Area Network (LAN) is the most common one used in networking technology. It connects two or more computers or devices. Wifi is used in this scale, as it provides wireless LAN. The larger scale is Metropolitan Area Network (MAN). It connects cities and it serves as a provider of Internet access in outdoor rural areas. With wireless

technology, the 802.16 standard of Wimax involves in MAN. Ultimately, combination of MANs will create Wide Area Network.

2.3.3 Network Architecture

Wimax network architecture is based on IP protocol. Wimax Forum Network Working Group (NWG) defines the network reference model as an architecture framework for Wimax service. The architecture supports general wimax deployments. Fixed, nomadic, and mobile Wimax deployments use the same model.

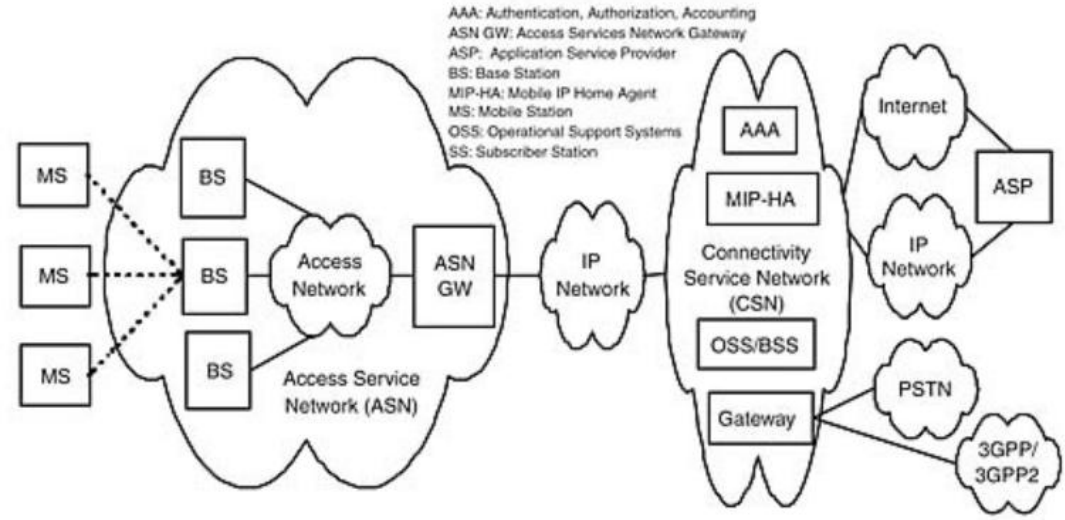

Figure 2-8 IP-based Wimax Network Architecture [18]

Base Station (BS): The BS functions as the air interface to the MS. It also has capabilities for micromobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management [18].

Access service network gateway (ASN-GW): ASN gateway is the layer 2 traffic aggregation point within the ASN. It also serves as location management and paging, radio resource management and admission control, caching of subscriber profiles and encryption keys, AAA client functionality, establishment and management of mobility tunnel with base stations, QoS and policy enforcement, and foreign agent functionality for mobile IP, and routing to the selected CSN [18].

Connectivity Service Network (CSN): The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs. Further, CSN can also provide gateways and interworking with other networks, such as PSTN (public switched telephone network), 3GPP, and 3GPP2 [18].

2.3.4 Wimax Physical Layer

The first layer, which is physical layer of 802.16, supports four specifications, which are Wireless-MAN-SC, SCa, OFDM (orthogonal frequency-division multiplexing), and OFDMA (orthogonal frequency-division multiple access) [14]. All modulations are designed specifically for NLOS (Non Line-of-sight) operation, except SC. OFDM has very high spectrum efficiency and it is able to handle multi-path-reflections and changing channel characteristics. These advantages are important for mobile applications. OFDM uses any bandwidth between 1,25 MHz to 20 MHz band. The bandwidth is divided into 256 carriers, which 200 are used. The other

carriers are used as a guard bands. From the 200 carriers 192 are used for data transmission and 8 carriers are used as pilots. Those pilots are used for synchronization and channel estimation. The modulation for the pilots is BPSK. The data can be modulated using BPSK, QPSK, 16 QAM, or 64 QAM [14].

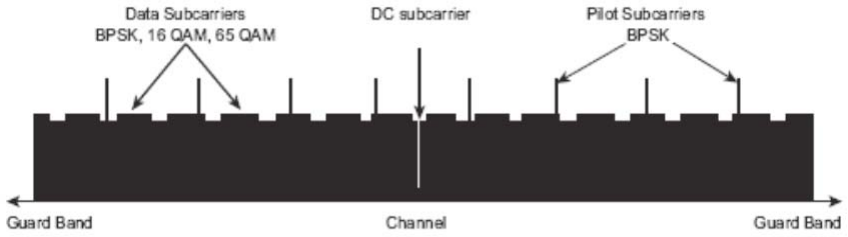

Figure 2-9 OFDM spectrum. [14]

2.3.5 MAC Layer

The second layer is the data link or MAC (Media Access Controller). 802.16 MAC uses a scheduling algorithm, which ensures that all subscriber stations get bandwidth without competing with other stations. Wimax specify three methods in dividing channels into downlink and uplink: TDD, FDD, and half-duplex FDD. TDD specifies base stations and subscriber station to transmit on the same frequency [14].

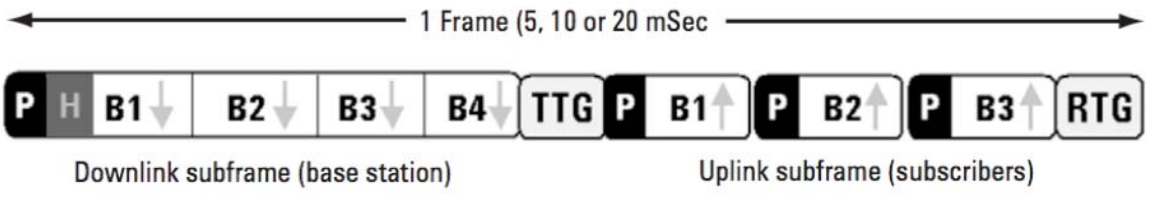

Figure 2-10 TDD frame [14]

On a typical TDD frame, it is divided into two subframes. Downlink subframe (on the base station) and uplink subframe (on subscribers). Each downlink and uplink is separated by a transition gap. Transmit/Receive Transition Gap (TTG) succeeds a downlink subframe. After a successful Uplink, a Receive/Transmit Transition Gap (RTG) follows [14].

The downlink subframe first contains the preamble (P) and followed by a header (H) and data bursts (B). The preamble is used for synchronizing and estimating a channel using QPSK modulation. It consists of two QPSK symbol. The first one uses 50, the second one uses 100 of the subcarriers. Information system and burst profile is specified at the header. It is used to help correct encoding [14].

The uplink subframe consists of several uplink subframes, which starts with a preamble. The preamble is in a form of OFDM symbol that is used to synchronize transmitter and receiver [14].

FDD stands for frequency division multiplexing. There are full duplex FDD and half duplex FDD. They are different on the way stations transmit and receive signal. In full duplex FDD, stations can transmit and receive on the same time. Whereas half duplex FDD, stations can only receive or transmit at a given time. They cannot do it simultaneously. The data burst contains data with a payload of 12 to 108 bytes. Also it contains control messages. Each burst uses the same modulation, however the modulation can change with each burst. Therefore data burst with the most vigorous modulation will be sent first [14].

Most Wimax uses TDD because of the less complexity and the cheaper implementation. FDD uses different frequency bands to upload and download. Therefore, in case of asymmetric data exchange FDD will not occupy the bandwidth.

2.3.6 Security

The fact that Wimax offers wireless broadband access in terms of greater scale brings attention to its security. Prevention of issues such as eavesdropping, denial of service, confidentiality, and other problems is essential to the deployment of Wimax. Wimax uses encryption to protect data, which are sent and received from client and base stations. It supports AES (Advanced Encryption Standard) and 3DES (an upgrade from Data Encryption Standard) [14]. There is also a dedicated security processor on each base station. The link between subscriber station and base stations are encrypted to offer privacy to data and increases security to the wireless broadband access. All traffic is encrypted using counter mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and uses AES to secure data transmission and provide data integrity [16]. Operators also benefits from this, as they can prevent theft of service. Another feature of Wimax is VLAN. It has a built in Virtual Local Area Connection for protecting data between stations that connects with the same base station.