The use of wireless technology to overcome bandwidth constraints by constructing a secure wireless metropolitan area network

by

Jacobus Retief Benade

DISSERTATION

submitted in fulfilment of the requirements for the degree

MASTER OF SCIENCE

in

COMPUTER SCIENCE

in the

FACULTY OF SCIENCE

at the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: DR E MARAIS

NOVEMBER 2005

Contents

List of Figures

CHAPTER 1 – INTRODUCTION

CHAPTER 3 - WIRELESS TECHNOLOGIES AND THEIR SUITABILITY IN THE CONSTRUCTION OF A WIRELESS MAN

CHAPTER 4 - TECHNOLOGICAL EVALUATION ACCORDING TO SET CRITERIA

CHAPTER 5 – NODE TYPES, LAYOUTS AND STRUCTURES

CHAPTER 6 – NODE EQUIPMENT REQUIREMENTS

CHAPTER 7 - PHYSICAL DESIGN AND LAYOUT

CHAPTER 8 – SECURITY

CHAPTER 9 – NETWORK MANAGEMENT AND MAINTENANCE

List of Tables

CHAPTER 2 – LEGAL ASPECTS OF WI-FI, LONG-RANGE CONNECTIONS AND APPLICATIONS OVER WIRELESS

CHAPTER 3 - WIRELESS TECHNOLOGIES AND THEIR SUITABILITY IN THE CONSTRUCTION OF A WIRELESS MAN

CHAPTER 4 - TECHNOLOGICAL EVALUATION ACCORDING TO SET CRITERIA

CHAPTER 5 – NODE TYPES, LAYOUTS AND STRUCTURES

CHAPTER 6 – NODE EQUIPMENT REQUIREMENTS

CHAPTER 8

List of Abbreviations

AES	Advanced encryption standard
AES-CCMP	AES-Counter Mode CBC-MAC Protocol
CCMD	
CD-ROM	Compact disc-read only memory
CPE	Consumer premises equipment
CRC	Cyclical Redundancy checking
DSSS	Direct-sequence spread spectrum
EAP	Extensible authentication protocol
EMC	
FCC	Federal communications commission
GHZ	Gigahertz
IBA	Independent Broadcasting Authority
ICASA	Independent Communications Authority of South Africa
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industry, science and medicine
ISP	Internet service provider
LAN	Local Area Network
LOS	Line of sight
MAN	Metropolitan Area Network
mBits/s	Megabits per second
MHZ	Megahertz
MIT	Massachusetts Institute of Technology
Mv	Milliwatt
OFDM	Orthogonal Frequency devisioning multiplexing
PDF	Portable document format
Q.S	
RADIUS	Remote Authentication dail-in User Service
RF	Radio frequency
SATRA	South African Telecommunications regulatory authority
SSID	Service Set ID
TKIP	Temporal Key Integrity Protocol
WEP	Wired equivalent Privacy
WiFi	Wireless fidelity
WLAN	Wireless LAN
WPA	WiFi protected Access

Chapter 1 – Introduction

1.1 Background

The Internet has influenced our lives greatly. The way we communicate evolved with the arrival of the Internet and has continued to evolve along with the Internet. While initially being used by Academia and large organizations such as the American Department of Defense, the Internet soon became a buzzword in the average home. E-mail has changed the way companies and individuals communicate, and the World Wide Web has changed the way all Internet users access information.

Lately the ability to communicate globally and instantly via text services such as MSN, audio services such as Skype, or audio and video services such as Microsoft NetMeeting has become popular.

These new services consume ever-increasing amounts of bandwidth; in turn these high quality services have driven the need for high-speed always-on Internet connections to businesses and homes.

The development of 802.11b and later on 802.11g wireless local area network (LAN) standards have brought wireless networking to the home user. Cheap Wi-Fi-certified hardware has enabled many people to access their high-speed Internet connections from anywhere within their home, or even on the move. The convenience that Wi-Fi has brought has resulted in the increased use of the broadband services mentioned above.

The end result is that the Internet changed the way we communicate, and continues to do so with the help of Wi-Fi.

1.2 Problem Statement

In an ideal world the required connectivity to allow everyone to use high-speed services such as video streaming would be available. However, this is not an ideal world.

Locally the average South African's ability to access the Internet has lagged behind that of their counterparts from America or Europe. Local Internet service providers (ISPs) often do not offer access to high-speed services in remote areas, and if a user does have access, it comes at costs much higher than equivalent services from America or Europe. In fact in a 2005 study of 39 countries the International Telecommunications Union found that in terms of broadband costs South Africa was ranked 38th [MyB05].

Local service providers also enforce a cap on the amount of information that can be downloaded within a given period. Along with the increased cost, reduced availability and enforced caps result in true access to high-speed services such as streaming video, video conferencing, remote desktop management and telecommuting becoming impossible.

Without the ability of South Africans to access these emerging services, it will not be long before South Africa starts to lose ground in the global information market.

While Wi-Fi is also cheaply available in South Africa, most of the deployment of Wi-Fi remains for home networks due to the limited availability of broadband services, and has not had the same effect on the availability of the Internet as it has elsewhere in the world. This not only reduces the effective number of Wi-Fi deployments in South Africa, but also results in South Africa falling behind in global communication trends. How can this problem be remedied?

1.3 Approach to Solve the Problem

While the international Internet landscape does seem healthier than its local counterpart, it is not without problems. Ample downstream bandwidth is available, but upstream bandwidth is very often limited or restricted in various ways by an ISP. This has led to many projects that are designed to overcome these limitations.

By using cheap off-the-shelf Wi-Fi equipment people are able to connect two distant points to each other, and often these points are kilometres away from each other. By combining many of these point-to-point connections, community metropolitan area networks (MANs) have started to form.

Utilizing cost-effective, locally available Wi-Fi equipment allows for a community-funded and managed MAN within South African cities to be formed. Such a network would offer bandwidth in excess of any current broadband offering by any local ISP. Wi-Fi utilizes unlicensed frequency bands and would mean that such a network would not require licensing; the cost savings would be passed directly on to the users of such a network.

Internationally wireless MANs have been started in many cities. Most of them have a specific goal in mind; while some simply encourage community spirit [FPS05], others have more direct applications in mind. Some of these applications are:

1. Research [AWW04].
2. Unrestricted high-speed backbone [BARWN].
3. Broadband access for public services such as fire and police departments [BARWN].
4. Pervasive wireless network coverage of entire communities [WiS05].
5. Distance learning [BAB05].
6. Video communications [BAB05].

All of the above applications are run over networks based on 802.11 technology. This technology has no limit on the possible application, meaning that local MANs that are constructed using 802.11 technology can be used for all of the above applications and many more.

By constructing a wireless MAN the public can take advantage of broadband services at a fraction of current costs and reduce the burden that current broadband users are placing on local infrastructure. This dissertation will serve as a guide to constructing a MAN in a South African context.

1.4 Dissertation Structure

This dissertation focuses on the knowledge needed to build a MAN within the South African environment. This includes legal, technological, security, physical, topological and management information that will be needed in the network's construction, management and maintenance.

The dissertation is broken up into five sections; section 1 covers the law of South Africa and contains Chapter 2. Chapter 2 covers the legal aspects involved in the construction, management and possible applications for the network.

Section 2 determines the appropriate technologies to be used when constructing the network. Chapter 3 creates evaluation criteria to determine if a technology is suitable, and also covers a few basic aspects of wireless products that are needed to create evaluation criteria. Chapter 4 evaluates the wireless technologies that the Institute of Electrical and Electronic Engineers (IEEE) has set out to determine if they are in fact suitable for the specific deployments within a wireless MAN. These technologies include 802.11b, 802.11g, 802.11a and WiMAX (802.16).

Section 3 covers topological information of a wireless MAN. Chapter 5 discusses basic topologies in which wireless products are used and proceeds to review the topologies of current wireless MANs. A custom topology is then defined that attempts to eliminate some of the disadvantages that current wireless MAN topologies have.

Section 4 covers the physical aspects related to the construction of a wireless MAN. Chapter 6 determines the additional equipment that will be needed to create the various wireless links that were mentioned in Chapter 5. This equipment includes the antennas needed to focus the signal, cables to connect the access points to the antennas as well as connectors that are used in conjunction with the cables. A formula is also given to determine if the antenna and access point combination is adequate to create a long-range link at the desired distance and speed. Chapter 7 briefly discusses the geographical aspects of placing an access point and illustrates that geographical obstacles can be overcome and used to the deployer's advantage.

The final section of this dissertation covers the management aspects of a wireless MAN. Chapter 8 discusses security technologies that are used by wireless products and illustrates that they are not always suitable in a wide area environment. A hybrid solution is proposed that allows for a greater level of security than current wireless MANs. Chapter 9 discusses general management aspects and briefly touches on how to manage a network on a metropolitan scale and what tools and utilities might be used.

Fig 1.1 illustrates the chapter breakdown.

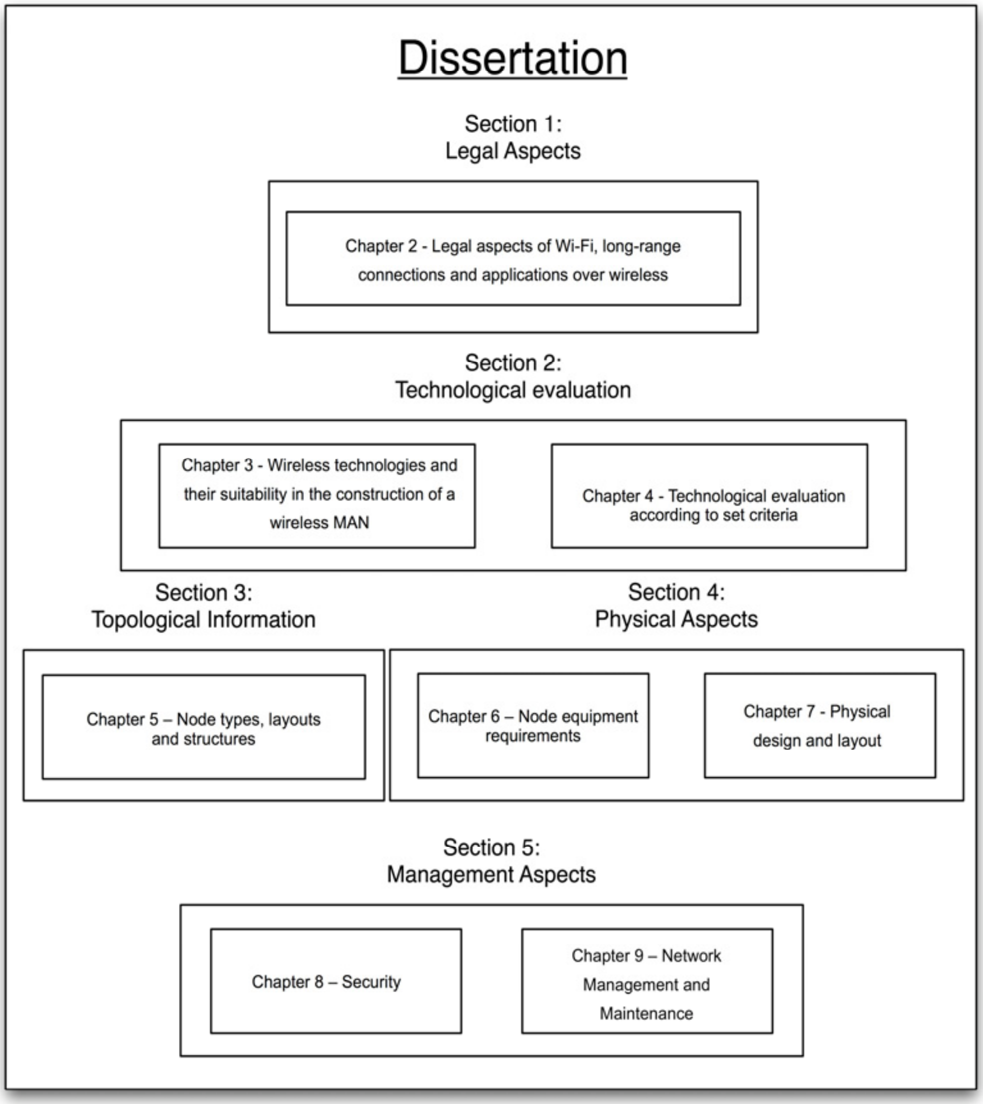

Dissertation
Section 1:
Legal Aspects
Chapter 2 - Legal aspects of Wi-Fi, long-range connections and applications over wireless
Section 2:
Technological evaluation
Chapter 3 - Wireless technologies and their suitability in the construction of a wireless MAN
Chapter 4 - Technological evaluation according to set criteria
Section 3:
Topological Information
Section 4:
Physical Aspects
Chapter 5 – Node types, layouts and structures
Chapter 6 – Node equipment requirements
Chapter 7 - Physical design and layout
Section 5:
Management Aspects
Chapter 8 – Security
Chapter 9 – Network Management and Maintenance

Fig 1.1 - Dissertation breakdown

Finally, Chapter 10 concludes the dissertation.

Chapter 2 - Legal aspects of WiFi, long-range connections and applications over wireless

2.1 Introduction

Many people do not realize that there are numerous legal issues related to all wireless products, not only WiFi products. While internationally the use and application of WiFi products are virtually unlimited, in South Africa the Telecommunications Act of 1996 imposes many limitations on not only the technologies itself, but also on their applications.

These limitations are imposed in an attempt to control the industry and help in its growth. However, some of the limitations might influence the construction and use of a wireless MAN and should be analysed.

This chapter discusses the Telecommunications Act and the limitations it imposes, requirements it sets for legal usage of products, as well as amendments that have been made to allow technologies to be used more freely.

In addition to the Telecommunications Act, the ISM bands, legal issues related to the hardware, the Independent Communications Authority of South Africa (ICASA's) view on WiFi and legal usage of the technology as sanctioned by ICASA will also be discussed.

2.2 Telecommunications Act of 1996

The Telecommunications Act of 1996 governs almost all of the telecommunications industry. With the exception of broadcasting, it is intended to regulate all telecommunications activities, as well as control the radio frequency spectrum. WiFi products (and all wireless products for that matter) impose information on electromagnetic waves. In terms of the

Telecommunications Act, electromagnetic waves are simply another definition for “radio” [oSA96].

In 2000, Act 13 called for the dissolution of the South African Telecommunications Regulatory Authority as defined in the Telecommunications Act. This meant the dissolution of both the Independent Broadcast Authority (IBA) and the South African Telecommunications Regulatory Authority (SATRA). The Act called for the establishment of the ICASA [oSA00].

The Telecommunications Act also states that ICASA is vested with the control, planning, administration, management and licensing of the radio frequencies that wireless products use [oSA96].

Of great importance is the licensing of the frequency spectrum. All wireless products use a section of the available radio spectrum, and in the construction and use of a wireless MAN the frequency used might require the user to apply for a licence first.

One of the limitations imposed by the Telecommunications Act is that unless the Minister (of Communication) issues an invitation, nobody may apply for a licence to provide one of the following services [oSA96]:

1. A public switched telecommunications service.
2. A mobile cellular telecommunications service.
3. A national long-distance telecommunications service.
4. An international telecommunications service.

Fortunately the construction of a wireless MAN does not require any of the above services. Services that are required are those related to private networks and the interconnection of those networks. This means that the minister does not have to be involved in the construction of a public wireless MAN.

Logically the next step would be to look at the licensing requirements and limitations for private telecommunications networks as well as those related to interconnection, as the construction of a wireless MAN will resemble large numbers of private networks that are interconnected.

The Telecommunications Act appears to treat LANs and private telecommunications networks as the same thing, meaning that it places no limitation on the use of a private network. The network can carry not only voice or data, but also anything that the operator desires [oSA96]. This poses no limitations on possible applications of a private wireless network.

The Act does, however, place a few limitations in terms of licensing interconnected private telecommunications networks. If a private telecommunications network is built using Telkom-provided facilities or equipment or those of other manufacturers, no licence is needed. A licence will, however, be needed by any private telecommunications network that is at any point interconnected to another part of itself via Telkom or any other licensed public switched telecommunications network [oSA96]. This means that a private network can exist without any limits, but once it is connected to another segment of itself via a public network, a licence is needed. The Act explains that a licence is needed if a private telecommunications network does not span continuous pieces of land owned by the same person, people or organization [oSA96]. This means that a wide area network such as a wireless MAN will require a licence to interconnect private networks, and the interconnections will have to be over Telkom connections or those of any other licensed public switched telecommunications network.

In terms of interconnecting, the Act specifies that Telkom or any other public switched telecommunications network will have to interconnect a private telecommunications network without question unless the request is unreasonable. ICASA has the power to override Telkom or any other public switched telecommunications network if it finds that the request is technically possible and will promote the increased or more efficient use of telecommunications services [oSA96].

The statements within the Telecommunications Act on interconnection make all of the current publicly available MANs in South Africa illegal. Parts of the public network are interconnected to itself using equipment and services that neither Telkom nor any other public switched telecommunications network provides. Current public MANs, per definition, also span large continuous pieces of land that are not owned by the same person.

A possible way around the legal hurdle could lie in the wording of the interconnection section of the Act. If current MANs can convince ICASA that future or existing MANs will promote increased use of telecommunications services or help the efficient use of existing telecommunications services, ICASA might overrule Telkom's obvious resistance to allow existing MANs to continue or future MANs to be created.

2.3 ISM Bands

As mentioned earlier, ICASA controls the radio frequency spectrum, and for the following reasons [oSA96]:

1. To ensure that the radio frequency spectrum is utilized and managed in an ordered and efficient manner,
2. with the aim of ensuring that users of the frequency are protected from interference or any other factors that limit the ability to use the frequency.
3. To avoid obstacles with the introduction of new technologies and telecommunications services.

ICASA also has to comply with any standards set by the International Telecommunications Union and its radio regulators [oSA96].

Nationally as well as internationally a few frequency bands are allocated by the respective control bodies to be used without a licence. These bands are called the industrial, scientific and medical (ISM) bands [Gas02].

The ISM bands in South Africa are as follows:

Table 2.1 - ISM bands

Land mobile below 1000 MHz	
	6765 – 6795 kHz
	13553 – 13567 kHz
	26957 – 27283 kHz
	40.660 – 40.700 MHz
	433.050 – 434.790 MHz
Microwave above 1000 MHz	
	2.400 – 2.4835 GHz
	5.725 – 5.875 GHz
	24 – 24.250 GHz
	61 – 61.5 GHz
	122 – 123 GHz
	244 – 246 GHz

Source: ICA

Products that operate within the ISM bands do not require a licence, allowing numerous products to be designed and manufactured without a cost penalty to the end-user.

Products that operate within the ISM band are ideal for the construction of a public MAN, as they have no additional licensing cost to the constructors and users of the network [KK03].

There is, however, a downside to the ISM bands: these frequencies are not controlled by the respective international bodies, and anyone that operates equipment in South Africa within these bands has to deal with collisions and interference by themselves without any assistance from ICASA. This means that users of a wireless MAN will have to contend with interference from other products in the same specific ISM band [KK03], including other wireless MAN users. Later chapters will deal with methods to reduce or eliminate potential interference.

Products such as Bluetooth, WiFi and many cordless phones owe their success to the ISM bands. These products can be made available to the consumers without worrying about additional radio frequency licensing costs.

When a product does not operate within the ISM band, no person is allowed to transmit or operate any form of radio apparatus, unless the person wishing to operate or maintain the station applies for and receives a certificate of proficiency. Additionally, a licence to operate in a non-ISM band gives ICASA the right to examine or request examinations to be conducted to determine the efficiency of any person or station using a frequency or frequency group [oSA96]. These examinations will require time and increase equipment costs.

Even if a licence for the frequency or frequency group can be obtained, a licence for the service that the licensee wants to use or provide the frequency or frequency group for has to be obtained as well [oSA96].

The licence will entitle the owner or any person in his/her employ to use the frequency or frequency group in any way prescribed [oSA96].

The additional effort of obtaining the right to use a frequency or frequency group as well as the licence to use the frequency for the intended purpose will increase the costs of construction and use of any network, including a wireless MAN. On the other hand, the use of a licensed frequency will mean that all communications are conducted with a guarantee of no collision or interference and the frequency can be used to its maximum potential.

2.4 Hardware and Related Legal Issues

The Telecommunications Act prescribes not only licensing, but also who can supply hardware, service hardware and the types of hardware that can be used [oSA96].

ICASA has the right to prescribe the types of equipment or services that are not allowed, as well as any circumstances in which the use of telecommunications equipment does not require any approval [oSA96].

The reason for this limit on hardware is frequency efficiency. By restricting hardware that is allowed to be used, ICASA can ensure that a frequency or frequency group is used at the best efficiency, as there will be no conflicting hardware that will also operate in the same frequency or frequency group [oSA96].

A further reason for the limitation on hardware is that radio frequencies may be harmful to a person [KK03]. The American Federal Communications Commission (FCC) lists all wireless products on its website and if a wireless product obtained locally has an FCC number, the owner of the said product may view any health-related information on the FCC website.

Hardware items have to be approved by ICASA first. ICASA has the following requirements when someone wishes to have hardware approved [ICA]:

1. The hardware has to be certified by an accredited testing house or laboratory. The testing facility will have to certify that equipment is functioning correctly and according to specification and the target application, and test reports on both RF and EMC must also be provided. The applicant will have to provide ICASA with a certified copy of the accreditation. The copy can be in a variety of formats ranging from paper format to a PDF on a CD-ROM. Applicants must also include a completed application form, as well as all required payments.

2. Full technical diagrams including those of the circuits, as well as photographs and diagrams describing the full working of each application are needed.
3. Hardware licences will only be issued to South African registered companies, and full details will accordingly have to be provided, including a physical address and the company's registration number.

Fortunately most, if not all, of the hardware that will be used by a wireless MAN will be components acquired off-the-shelf. Hardware that is available in credible computer stores should already have been approved by ICASA. The buyer of the hardware can check for the ICASA sticker to verify that the hardware has been licensed. The advantage of approval means that the equipment will use the frequency or frequency group to its maximum potential.

2.5 ICASA's View of WiFi

In the previous sections all the requirements for licensing the service, hardware and frequency or frequency group were given. The fact is that most of the hardware that will be used in the construction of a wireless MAN will be WiFi-certified hardware. For this reason it is important to know what ICASA's view of WiFi is.

While ICASA has no official view on WiFi, it has a lot to say on wireless LANs.

On 19 June 2003 ICASA requested in a Government Gazette that independent participants comment on the provisioning of wireless Internet access across a wireless LAN [ICA04]. While this seems to be a trivial matter, the findings had great importance for WiFi in general and not only the provisioning of wireless Internet.

The results were published on 16 October 2003 in the Government Gazette [ICA04].

The very first important conclusion that was made was that while initially only the use of wireless Internet access was under discussion, a generalization could be made to wireless data access. Thus the discussion then became about all data travelling across a wireless network, not just Internet traffic. Another finding was that wireless local area networks (WLANs) were to be viewed as local access networks simply with a different medium of transmission [ICA04].

Many of the participants argued that WLAN equipment that was situated on the premises of a LAN owner could be considered to be customer premises equipment (CPE), and according to Telkom SA's licence, the definition of CPE is as follows: "An item of approved equipment which does not form part of the Public Switched Telecommunications Network but is connected or intended to be connected to terminal connection equipment, whether fixed or portable, and by means of which signals are initially transmitted or received." [ICA04]

LANs have traditionally been viewed as CPE and, as previously stated, ICASA considers WLANs as LANs with a different medium. This finding is an important one on the legal status of WLANs. WLANs do not need any new legislation, and more importantly they are restricted to any legal restrictions to which LANs are subject [ICA04].

One of the main questions that ICASA had from the independent participants was whether anyone providing public access to a LAN was actually providing a telecommunications service and whether it should be licensed. The Radio Act Declaration of 1995 (Notice 1790 of 1995), section 2(d), placed a restriction on LAN owners. The owner of a LAN could only provide the LAN on his/her/its own premises and between computers of the same user [ICA04].

According to this restriction, it was illegal to provide any commercial service to any public member, as these members could not be considered to be from the same user.

ICASA, however, stated that the limitation was unnecessary; no argument could be made in terms of the use of frequency spectrum efficiency that justified the restriction requiring the LAN to be between computers of the same user. Accordingly, ICASA has amended the regulation and deleted the limitation that required that a LAN had to be between computers of the same user [ICA04].

ICASA found that no licence is required when any service is provided to customers on the LAN owner's premises. However, once a LAN owner provides services beyond the premises' borders that he/she/it resides on, a telecommunications service is then being provided by the LAN owner and the owner will be required to acquire a licence for that service [ICA04].

What this means is that because WLANs are considered equivalent to LANs, WLANs can do everything that a LAN can do, and that includes providing public access to the WLAN of a person(s)/business. This means that a wireless MAN can provide access to members of the public.

Lastly, as stated previously, the Telecommunications Act does not impose a limit on the type of information that a private telecommunications network can provide; thus no limits are imposed on WLANs.

2.6 Conclusion

The legal aspects to wireless technologies are many and diverse and range from the allowable uses to the certification of hardware and licensing of frequencies.

The Telecommunications Act was created to govern the telecommunications industry, and as such it provides a good basis for a variety of telecommunications services while keeping economic growth and expanded use of telecommunications services in mind. The Act covers a wide variety of topics and fully encompasses all the aspects in relation to any type of telecommunications network, not only wireless networks.

In terms of wireless networking and, more specifically, the construction of a wireless MAN, the Telecommunications Act of 1996 provides a large amount of valuable information. In relation to licensing the Act states that current or future public wireless MANs are illegal due to the fact that private telecommunications networks will have to be or are interconnected, and these interconnections are illegal because the points of interconnection do not belong to the same person.

ICASA is more forgiving when it comes to the frequencies that WiFi products use. ICASA's adherence to international ISM band standards allows for all WiFi products that operate within these bands to be used without the need for a licence from ICASA. As a result the use of conventional ISM band WiFi products will greatly reduce the costs of construction of a wireless MAN and will encourage its usage as well as construction.

ICASA further imposes strict limitations on hardware with the goal to protect the frequency spectrum for legitimate licence holders. While the ISM band does not have any control, hardware certification is still needed to ensure that it complies with other requirements. Fortunately the large number of WiFi products that are brought into the country results in a mitigation of cost to the buyer due to the ability to spread the cost over many units.

With the exception of interconnection and the limit of not being able to provide a service outside a user's premises, the construction of a public accessible wireless MAN is completely legal and can be constructed with low-cost equipment that is certified to be interoperable thanks to steps taken by ICASA.

With knowledge about the legal status and requirements of wireless products, including WiFi, the next step is to evaluate whether the variety of wireless technologies available are suitable in the construction of wireless MANs.

In the next chapter an evaluation criteria will be created that aims to serve as a guide to determine if a technology is suitable for use in the construction of a wireless MAN.

Chapter 3 - Wireless technologies and their suitability in the construction of a wireless MAN

3.1 Introduction

When designing any network, including a wireless MAN, a set of requirements has to be compiled first. Of the many different requirements, technical requirements also have to be considered [BBL02].

In this chapter all the aspects are covered of any wireless technology that will ultimately influence the technology's suitability for an intended application. In the case of this dissertation, this application is the construction of a wireless MAN.

Technical aspects such as encoding methods, bandwidth needs, distance needs, power consumption, power output, user location and services offered will be considered, as these factors form but a few of the technical specifications that greatly influence a technology's ability to match requirements for a technology that could be used in a wireless MAN.

3.2 Types of Deployments

Before an in-depth investigation can follow, base criteria will be needed for evaluating every technology for suitability in the construction of a wireless MAN.

Intel defines three key types of deployments that make up a wireless MAN.
They are [Int]:

1. Backhaul.
2. Large area coverage (hot zones).

3. Last mile.

A complete wireless implementation would mean that all three deployments would have to be wireless, and that criteria for all three deployments would have to be developed.

3.2.1 Backhaul

Backhaul defines the connection of a group of aggregate users to each other over a great distance [Int]. An example of a backhaul connection would be the network connection that connects departmental networks within an organization [Pro]. Such an interdepartmental connection would require the speed to allow all the traffic that crosses the network to cross with no delay. However, connecting a large number of users over great distances requires range as well as speed to carry all the required traffic.

Another key aspect that will have to be addressed is the initial cost. Along with the bandwidth, the wireless option has to be cost-effective [Pro]. Fortunately, wireless backhaul connections are available at greatly reduced costs compared to their wired counterparts [Pro].

Thus considerations in relation to a wireless long-range backhaul are:

1. Range.
2. Speed/bandwidth.
3. Cost.

Backhaul connections will form an integral part of a wireless MAN. As any organization grows, groups that are connected together will also grow. A wireless MAN is no different; users will be added on a constant basis and the required infrastructure will be needed to connect the groups of users.

3.2.2 Large area coverage (hot zones)

Large area coverage is usually achieved by connecting large numbers of wireless nodes in a mesh-type network [Int]. This is similar to a wireless ad hoc network where multiple connections are made from multiple nodes in a network to multiple other nodes within that network (Fig 3.1). So while a node may not be in direct contact with another, at least one connection is present to the destination node via one to many other connections.

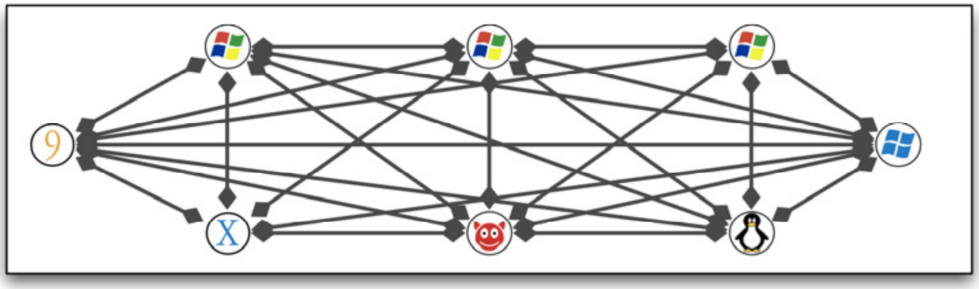


Fig 3.1 - Mesh network structure

The advantages of a mesh-type wireless network are as follows [Int]:

1. Balanced traffic and access: Due to multiple routes traffic can travel either the most convenient or the most effective path to its destination. A further advantage is that with multiple nodes that allow access to clients an overloaded AP can simply refuse additional clients and redirect them to an AP that is capable of carrying the load, or that client can then connect to an AP of its choice that does allow access and would not be overloaded or has a low utilization.
2. Robustness and resilience: Mesh networks are traditionally more robust than single hop networks because they are not dependent on a single node for their operation. What this means is that if a single node fails, the network would be completely disabled in a single hop network. In multiple hop networks other nodes can pick up the slack of the node that has stopped functioning correctly.

3. Reduced cost: The use of WiFi as a technology means that there are many clients available to service providers. This is because many WiFi-certified products are already on the market or exist within a lot of client-based equipment such as laptops. Even without Wi-Fi there is an abundance of standardized technologies that have reduced costs due to their standardization and can provide a mesh connection with little additional cost.

Mesh networks do, however, have a few disadvantages. The disadvantages are related to the multiple nodes that characterize a mesh network.

As information travels or hops from one node to another, there is an increased latency as the information goes further to the outer edges of the mesh. This is due not only to the time it takes to receive and retransmit the information, but also the repackaging of the information. The increased latency makes Voice over IP (VoIP) or any other form of multimedia that requires some form of quality of service (QoS) very difficult [Int]. With the increase of multimedia related traffic such as VoIP, video chat and streaming audio, it will become essential in the future for all networks to support QoS.

Also due to the increased latency the bandwidth is reduced to the outer borders or edge of the mesh [Int]. In addition to the bandwidth reduction due to latency, APs sometimes interpret another distant signal as noise, mainly because of signal deterioration, reflection or bouncing of the signal off of surfaces. As a result information will have to be retransmitted, further decreasing the bandwidth in the inner sections of the mesh as well as in the outer regions.

An additional requirement to create a mesh network is that there has to be some mesh routing protocol in place. Wi-Fi currently has no default IEEE-specified mesh topology, and some form of proprietary method is commonly used. These proprietary methods are not always compatible [Int].

Based on the above discussion the criteria for a mesh network are as follows:

1. Mesh routing protocol (standardized or proprietary).
2. Low latency.
3. Speed/bandwidth.
4. Low cost of client equipment.
5. QoS.

3.2.3 Last mile

The last mile problem describes the problem that ISPs have when clients wishing to buy a product the ISP markets cannot be connected to the network because of the ISPs' inability to offer the capacity or any form of connectivity [Fli2a] [Lig].

Ultimately Internet traffic will travel over a wireless MAN, but other non-Internet traffic will as well. The Internet traffic travelling over the wireless MAN allows for the last mile problem to be considered. Many ISPs have identified the last mile problem and any technology that can overcome the last mile is an appropriate technology for use in a wireless MAN.

Wi-Fi is used extensively by wireless ISPs (WISPs) to solve the last mile problem. The reason for this is [Fli2a]:

1. Range.
2. Speed/bandwidth.
3. Low cost.
4. Easy availability of hardware.

The last mile problem provides a convenient evaluation method as many wireless links in a wireless MAN will be of the long-range type.

3.3 Evaluation Criteria

Most of the requirements set out above overlap. There are, however, unique aspects to each one. It is these aspects that will be the determining factor that will decide if a technology can be used for that specific deployment.

Almost all the deployments mention:

1. Cost.
2. Range.
3. Speed.

These three elements therefore warrant closer scrutiny.

Understanding what which factors influence the range that a WiFi product is capable of can lead to an understanding of the factors that influence any wireless product's range.

3.4 Range

Every wireless device has some form of wireless transmitter and receiver [KK03]. Properties of these transmitters and receivers include the frequency they operate on, their power output and management systems, as well as receiver sensitivity.

The transmission of electrical signals over the air requires the electric signal to be converted to electromagnetic waves. An electromagnetic wave is an energy-carrying wave that spreads out as it propagates; examples of this propagation include light and sound. The electromagnetic waves have been divided into groups called an electromagnetic spectrum [KK03], or as ICASA calls it, a frequency spectrum [ICA]. The frequency spectrum used by a wireless device has certain inherent properties, requirements and limitations. These properties influence the abilities of the technologies, including their abilities to perform over long ranges. These properties will be discussed later in the chapter.

In addition to the frequency spectrum used, the amount of power used by the wireless device also influences the way a technology functions. An example of this is Bluetooth. Designed as a personal area network device, class 1 Bluetooth consumes 100 milliWatt (mW) of energy and class 3 Bluetooth 1 mW of energy [Boa99]. However, class 1 Bluetooth has a range of 100 metres, while class 3 Bluetooth only has a range of 10 metres [Boa99].

Receiver sensitivity can also influence the working of a wireless product. It is defined as the power of the weakest signal the receiver can detect [DS]. The weaker the signal a receiver can detect, the better the sensitivity. The power a signal carries is measured in dBm and is also directly related to mW. A 0 dBm signal is equal to 1 mW of energy and smaller values in dBm also translate to lower mW ratings [Gei05]. So the lower the dBm, the lower the mW of power that the signal carries.

Atheros and Broadcom introduced new wireless chipsets in 2004 that serve as a base controller for WiFi products. Broadcom claims that its range was extended by up to 50% while Atheros claimed up to 300% in open air scenarios [AC104]. Both these technologies have increased their range as a result of enhancements made to the receiver's sensitivity.

3.4.1 Frequency spectrums

One key characteristic relevant to wireless communications is the ability to penetrate objects. Infrared technologies suffer greatly as many obstacles reflect infrared. Radio waves, on the other hand, go through or around many objects or obstacles [Mil00]. When even rain can become a limiting factor, the ability of certain frequencies to go through objects becomes increasingly important [Fli02].

Currently the three most popular spectrums used for data transmission are [KK03]:

1. Infrared.
2. Microwave.
3. Radio.

Infrared-based technologies are possibly one of the simplest and cheapest WLAN technologies. Infrared does not spread out as easily as other frequency spectrums and as a result does not easily suffer interference, nor does it create interference. Correctly directed infrared signals can travel great distances, which makes them ideal for point-to-point connections. Infrared, however, suffers greatly when a bigger area has to be covered. It bounces off nearby objects and can suffer interference from natural and artificial light sources [KK03]. While infrared does have cost advantages and functions very well when adequately directed, its limited effective range has meant that it is successful only in the personal area network arena [Dhi01].

Microwave-based technologies use 500 mW of energy or less. Most current implementations have a short range of approximately 365.76 m. Because microwave-based technologies do not have to rely on spread spectrum technologies, they also have much higher throughput [KK03].

Radio-based LANs are by far the most popular WLAN technology. The FCC in the United States places requirements and considerations on the 2.4 GHz band. They include the following:

1. Devices in the 2.4 GHz band must use spread spectrum technologies.
2. When using frequency hopping spread spectrum there have to be either 79 1 MHz channels [Mil00] or more than 15 5 MHz channels [Mar02].
3. Interference must be anticipated and handled [Mar02].

Spread spectrum has a few unique properties. They are as follows:

1. The bandwidth of the transmitted message is much larger than the bandwidth required by the original message.
2. The bandwidth of the transmitted message is determined by the original message.

There are currently two popular spread spectrum technologies [KK03]:

1. Direct sequence spread spectrum.
2. Frequency hopping spread spectrum.

3.4.1.1 Direct sequence spread spectrum

Direct sequence spread spectrum uses a carrier wave that remains fixed to a specific frequency band. The transmitted data is not really sent over a single narrowband like microwave transmissions. Rather, it is spread over a much larger bandwidth using an encoding scheme. The spread signal is then de-spread at the recipient. The power requirements of a microwave transmission are exactly the same as a spread spectrum transmission, but the spread is different (Fig 3.2). The result is that it is more difficult to detect the presence of a spread spectrum signal [Wir00].

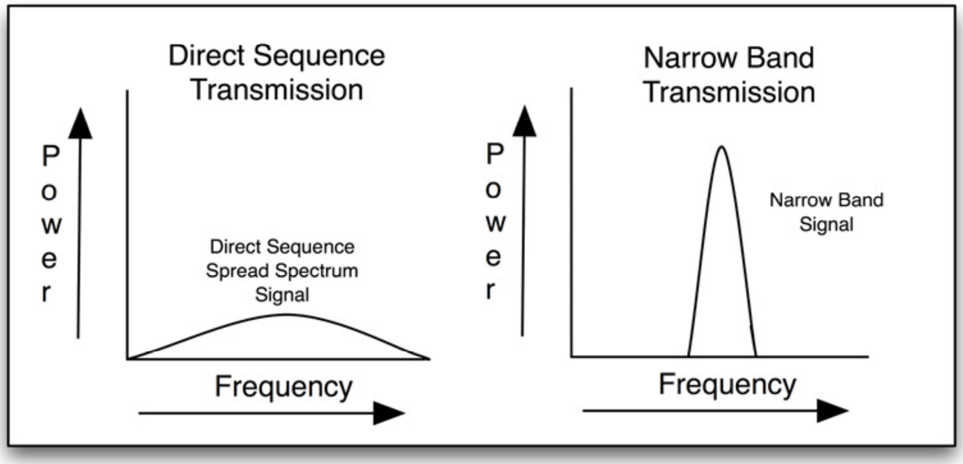


Fig 3.2 - Narrowband transmission vs. direct sequence transmission [Wir00]

Direct sequence spread spectrum also has a level of redundancy built in. A transmission is actually transmitted at least ten times. If, for some reason, interference does occur, only one of the messages has to be reconstructed from one of the ten sent messages or parts of them. As natural interference occurs, it is logical to think that a disruption of signal will take place. Interference, however, mostly occurs in short powerful bursts. A property of spread spectrum is that it will eliminate these natural interferences in the de-spreading process [Wir00] (Fig 3.3).

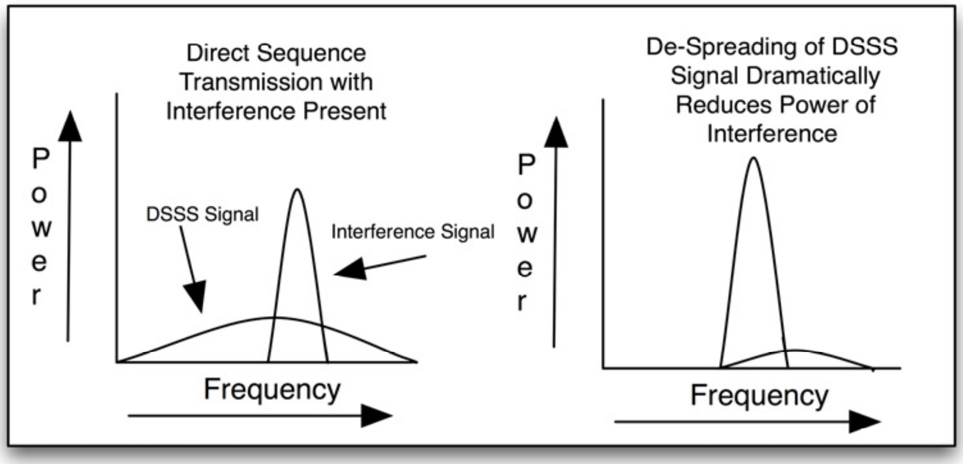

Direct Sequence Transmission with Interference Present
Power
DSSS Signal
Interference Signal
Frequency
De-Spreading of DSSS Signal Dramatically Reduces Power of Interference
Power
Frequency

Fig 3.3 - Interference elimination ability of DSSS [Wir00]

3.4.1.2 Frequency hopping spread spectrum

Frequency hopping spread spectrum, on the other hand, attempts to achieve minimal interference by sending its transmission over different frequencies at different times. A device is allowed to transmit only for a short time on a given channel before it must hop to the next pseudo random channel in the sequence. The time that a device is allowed to transmit over a specific channel is called the dwell time and it is limited to 400 microseconds. The goal of this hopping is to create as little interference as possible, and to keep susceptibility to interference as minimal as possible [Wir00].

A long-range wireless link would need to be secure, robust and provide a high throughput. Table 3.1 compares direct sequence spread spectrum and frequency hopping spread spectrum, and indicates that direct sequence spread spectrum is the better method to propagate a signal when range and throughput are important.

Table 3.1 - Direct sequence spread spectrum vs. frequency hopping spread spectrum

Direct sequence spread spectrum	**Frequency hopping spread spectrum**
No dwell time	400 microsecond dwell time
Single channel operations	Multi-channel initial search to synchronize
No re-sync needed	Re-sync needed with every hop
Higher overall throughput	Lower overall throughput
Long outdoor range (40 km)	Shorter outdoor range (10 km)
Short latency	High latency

Source: Wir00

In addition to the spectrums used and the encoding methods deployed in each spectrum, all wireless signals also exhibit characteristics due to their propagation.

Radio frequencies (RFs), in addition to their own frequency-specific properties, also exhibit general properties that affect the distance a signal can travel. These general properties are related to the propagation of the signal.

3.4.2 RF propagation principles

The general RF propagation principles are as follows [Spu04]:

1. Free space loss.
2. Attenuation.
3. Scatter.

3.4.2.1 Free space loss

Free space loss defines the power loss due to natural signal spreading.

As the signal travels away from the transmitter, natural geometric spreading of the signal occurs due to the energy expanding.

There is a formula that allows for the free space loss to be calculated. Formula 3.1 defines the calculation of free space loss where λ represents the signal wavelength, r the distance from the transmitter and FSL the free space loss measured in dB.

$$FSL = r^2 (4\pi)^2 / \lambda^2$$

Formula 3.1 – Free space loss [Spu04]

Formula 3.1 can be simplified when assuming that 802.11-based equipment is being used. Formula 3.2 represents the free space loss working with the assumption that the frequency is in the 2.45 GHz range.

$$FSL = 40 + 20*\log(r)$$

Formula 3.2 - Free space loss in the 2.45 GHz band [Spu04]

3.4.2.2 Attenuation

When a signal passes through solid objects some of the signal's strength is absorbed. In general the thicker the object, the more power is absorbed. However, the thickness of the substance is not the only factor determining power loss [Spu04]. Certain substances such as metals also greatly contribute to power loss.

Due to many factors, including unknown compositions of barrier objects, it is sometimes very difficult to calculate the exact level of attenuation. Sputnik is a company that produces hardware and software for deployments of wireless technology in the use of hotspots, campus area networks and WISPs, and as such has vast experience with factors influencing attenuation.

Sputnik uses a general range for attenuation based on experience. The approximate levels of attenuation are as follows [Spu04]:

1. Trees contribute between approximately 10 and 20 dB of loss for each tree in the direct path of the signal. Loss depends on the size, type and foliage density. Larger trees with dense foliage offer greater levels of loss than their smaller counterparts. Signal loss can also be seasonal as trees lose their cover in the winter. In a wireless MAN, trees will be of great concern.
2. Walls account for between 10 and 15 dB of loss. Sputnik lists an internal wall as a lesser barrier than external walls. However, in South Africa wall densities of internal and external walls in the average South African home do not differ. It is only in business environments where dry walls are found; dry walls have less attenuation to signals. This fact is true for South Africa but not other countries as dry walls are common in personal residences in other countries. Mostly external walls will offer resistance in a wireless MAN, but antennas and the signal will most likely be outdoors, so walls will offer limited attenuation.

3. Building floors account for between 12 and 27 dB of loss. Dried wooden floors are at the lower end while thick concrete floors with high levels of steel are at the upper end of creating attenuation. Floors should offer very little resistance to a wireless MAN, mainly due to signals not needing to travel through floors, but most likely coming from outside the building.
4. Surprisingly, mirrors offer the greatest level of attenuation. The reflective surface within mirrors is conductive and almost completely absorbs the signal.

3.4.2.3 Scattering

Attenuation is the absorption of energy; scattering is the reflection of energy.

Many surfaces do not absorb energy, but reflect the signal back in the direction from which the signal came. The reflected energy interferes with the original signal and makes it more difficult for the receiver to decode the intended signal. While wireless chipset manufacturers have attempted to reduce the effects of scattering by increasing chipset sensitivity, the effect and categorization of scattering is still being researched intensively [Spu04].

Scattering is also called multipath, fading, Rayleigh fading and signal dispersion [Spu04].

In sections 3.4.2.1 to 3.4.2.3 the common factors influencing RF propagation were mentioned. While it is difficult to calculate the exact loss of the signal due to attenuation and scattering, Sputnik defines an allowable loss of signal that is simply an approximation of the loss. The resulting overall loss of the signal can be represented within formulae 3.3 and 3.4 when assuming operation within the 2.45 GHz frequency range. In both formulae 3.3 and 3.4 L represents the total loss measured in dB, r the distance from the transmitter, n the level of scattering, λ the signal wavelength and $L_{\text{allowable}}$ the allowable level of attenuation and scattering.

$$L = r^{n} (4\pi)^{2} / \lambda^{2} + L_{\text{allowable}}$$

Formula 3.3 – Total loss [Spu04]

$$L = 40 + 10*n*\log(r) + L_{\text{allowable}}$$

Formula 3.4 – Total loss in the 2.45 GHz frequency band [Spu04]

3.5 Speed

While power greatly influences range, it also has an effect on speed. The use of more power is why WiFi products have a larger data rate than Bluetooth, even though both operate in the 2.4 GHz spectrum [Woj04].

The ISO layer is a common reference model for all network products. The bottom-most layer is the physical layer; it dictates how the 1's and 0's will ultimately be transmitted over whatever media [otICSB99].

The IEEE is the body that controls most of the physical layer standards. While standards are there to provide guidance and compatibility, there is nothing that prevents a company from deviating from the standard. Atheros has done so with its Super G technology.

By deviating from the official specifications, Atheros claims to be able to transmit 108 megabits instead of the default 54 megabits 802.11g offers [AC204]. The unfortunate downside to this is that some of the methods used to offer the theoretical speed increase might disrupt other networks. Initial Atheros Super G products used a feature called channel bonding to increase speed. Channel bonding uses more than one channel for transmission, making it very difficult for other products to use the second channels, and was criticized by Atheros' competitors [Gri].

Increased speed technologies might seem very alluring when buying equipment for the construction of a wireless MAN node. However, to ensure maximum compatibility it is recommended that standards set by bodies such as the IEEE be upheld.

3.6 Cost and Ease of Availability

Gordon Moore stated in 1965 that the number of transistors would double every 18 months. The law applies to the wireless market, too, even though Moore probably did not intend it to. The costs of wireless products have fallen in line with Moore's law and as a result wireless products have become cheaper for consumers [Moo65].

The reduced costs of the components that go into wireless products have meant that products can be made available cheaper to the end consumer. The price of a Bluetooth chip in 2001 was between US$20 and $30 [Ame01], and the goal price of the Bluetooth special interest group (SIG) was $5. The increased availability of Bluetooth products in the market is an indication that the reduced cost does in fact increase adoption and availability.

3.7 Conclusion

With many possible wireless technologies available it is important to determine if a specific technology is suitable for a target deployment. A wireless MAN has its own unique set of requirements and the technology that will be used in such a network needs to satisfy most, if not all, of those needs.

Intel defines three different deployments, each with its own set of requirements. The deployments are backhaul connections, large area coverage or hot zones and lastly last mile connections. Using these three deployments, it is possible to construct a wireless MAN, and by choosing technologies that are suitable to these deployments, it is possible to choose the technologies that are most appropriate in building a wireless MAN.

An analysis of each of the three deployments indicates that each has its own specific criteria, that overlap in criteria does occur and that it is possible to use a single technology for all three deployments, provided that not only the overlapping criteria but the specific criteria of each deployment are met.

The combined criteria are as follows:

1. Range:
    - i. Frequency.
    - ii. Power output.
    - iii. Receiver sensitivity.
2. Speed:
    - i. Physical layer parameters.
3. Cost (client and station equipment).
4. Availability.
5. Latency.
6. Mesh routing protocols (standard or proprietary).
7. QoS.

An important criterion is the frequency on which a technology operates. The three factors that influence the propagation of a signal will largely determine the range of which a wireless device is capable.

Free space loss can be calculated with formula 3.2. It was, however, found that while free space loss can be calculated exactly, it is the incalculable attenuation that will most likely result in the most interference for any outdoor wireless network. More specifically, trees will be the largest contributing factor.

A technology that meets all the requirements set out above will be ideal for all three deployments. However, if no such technology exists, multiple technologies will have to be used that each on their own satisfies each deployment's respective needs.

In the next chapter a few common, proprietary and as yet unreleased technologies will be evaluated according to the evaluation criteria set out in this chapter with the goal of determining if there is a single technology or a combination of technologies that are suitable in the construction of a wireless MAN.

Chapter 4 - Technological evaluation according to set criteria

4.1 Introduction

In the previous chapter an investigation was made into creating evaluation criteria for wireless technologies and their suitability in the construction of any of the three deployments in a wireless MAN.

In this chapter a few common technologies are evaluated according to the set criteria with the end goal of determining the suitability of the technology under evaluation. All of the criteria listed in the previous chapter will be considered and a tabulated rating will be given at the end of each technology.

Firstly why standards are needed, and what happened when there was a lack of standards will be discussed.

4.2 Need for Standards

In the early days of wireless technologies almost everything was proprietary. Each vendor had their own implementation, which had its own set of specifications. Frequencies might have been the same but encoding schemes might have differed. The unfortunate result of this diversity was that buyers of these proprietary technologies were locked into a single company when choosing replacements and they were forced to rely on that single company for support [BBL02]. In many cases the manufacturers chose to keep their implementation closed, forcing users to stick with that manufacturer. This meant that wireless products were too expensive for the average consumer.

A need arose for standardization that would simplify the market and allow for consumer technologies to be obtainable by the intended consumers.

4.3 Do Standards mean Compatibility?

Even though a product may be standardized, that product may not be compatible with competitors.

With 802.11 a standard was brought to the market. Unfortunately 802.11 had three different physical layer specifications. While it did make things much better, different vendors adopted different versions of the physical layer. Due to one of the specifications having limitations, only two actual versions of 802.11 were available on the market [BBL02].

The IEEE has since improved on 802.11. Every following specification has had a complete set of rules. Most of those specifications allow for full backward compatibility; 802.11b, for example, is compatible with 802.11 and 802.11g is compatible with 802.11b [Fli02].

802.11a operates in a different frequency spectrum from 802.11b equipment, resulting in the complete lack of compatibility [Fli02].

The frequency used, however, does not mean compatibility; nor does even a basic IEEE specification, for that matter. In the early days of 802.11g many manufacturers brought products to the market that used a variety of techniques that were supposed to increase the transfer rates even more. The downside to these extensions was that to use these enhancements all the equipment had to come from that specific manufacturer. This included not only the APs but client side hardware as well. A good example of this was Atheros's initial implementations of its Super G technology [Gri].

Even though standards were created to enhance compatibility, not all technologies can be compatible with each other. Each technology is designed with a specific goal or problem to solve and as such cannot always work well with other technologies. In an environment as heterogeneous as a wireless MAN, equipment from the same vendor might not always be an option. The possible inability to agree on hardware is limited due to the difficulty in meeting people that live great distances from each other. Even when it is an option to use non-standard equipment, the equipment will need to be able to integrate with other standardized equipment. Fortunately the wide adoption of TCP/IP allows many different types of hardware to work together, including proprietary wireless equipment.

4.4 The Institute of Electrical and Electronic Engineers

The IEEE was formed in 1961 and has as an organization the goal of developing industry standards in electrical engineering and communications. The IEEE has three subsections related to wireless technologies [KK03]:

1. Wireless local area network technologies (802.11).
2. Wireless personal area network technologies (802.15).
3. Wireless metropolitan area networks (802.16).

The active standards within the 802.11 task group are [BBL02]:

1. 802.11b.
2. 802.11a.
3. 802.11g.

The active standard within the 802.15 task group is 802.15.1 (Bluetooth) [BBL02]. The active standard within the 802.16 task group is 802.16-2004 (WiMAX) [IEEE05].

Of great interest in the construction of a wireless MAN will be the local area network technologies and the metropolitan area networking technologies, as they will most likely offer the range and speed needed in any of the deployments mentioned in the previous chapter. Features found in personal area network technologies may qualify them for use in a wireless MAN. However, per definition, personal area is about 10 m, so most personal area network technologies are designed to function within that 10 m space. This induced limitation eliminates these technologies from being used in a wireless MAN.

4.5 802.11b

In 1999 the 802.11b standard was drafted and accepted by the networking industry. It was intended as an extension to 802.11, and featured full backward compatibility. 802.11b is a physical layer specification; it adheres to the OSI specification and fits in on level 1 [otICS99].

802.11b is intended for the 2.4 GHz ISM spectrums, meaning that while the use of 802.11b is licence-exempt, users of these technologies should expect interference [otICS99].

The 2.4 GHz ISM band range varies from country to country. In South Africa the band ranges from 2400 MHz to 2483.5 MHz. In America there are 11 channels of 11 MHz each. In other countries where the ISM band may be bigger there are up to 13 channels [otICS99] (Table 4.1).

As stated, the South African ISM band ranges from 2.400 GHz to 2.4835 GHz. However, ICASA does not specify official channels for the ISM bands but there can be 13 channels in the sanctioned ISM band (Table 4.1), meaning that this corresponds to European channels. The official IEEE channel allocation for 802.11b is given in Table 4.1.

Table 4.1 – Channel allocation of the 2.4 GHz ISM band

Regulatory domain							
Channel	Frequency (MHz)	USA	Canada	Europe	Spain	France	Japan
1	2412	X	X	X	-	-	-
2	2417	X	X	X	-	-	-
3	2422	X	X	X	-	-	-
4	2427	X	X	X	-	-	-

Channel	Frequency (MHz)	USA	Canada	Europe	Spain	France	Japan
5	2432	X	X	X	-	-	-
6	2437	X	X	X	-	-	-
7	2442	X	X	X	-	-	-
8	2447	X	X	X	-	-	-
9	2452	X	X	X	-	-	-
10	2457	X	X	X	X	X	-
11	2462	X	X	X	X	X	-
12	2467	-	-	X	-	X	-
13	2472	-	-	X	-	X	-
14	2484	-	-	-	-	-	X

Source: otICS99

It was stated earlier that 802.11b uses 11 MHz channels. However, in Table 4.1 the spacing is only 5 MHz. Fig 4.1 and Fig 4.2 indicate the channels that are non-overlapping in North America and Europe, respectively.

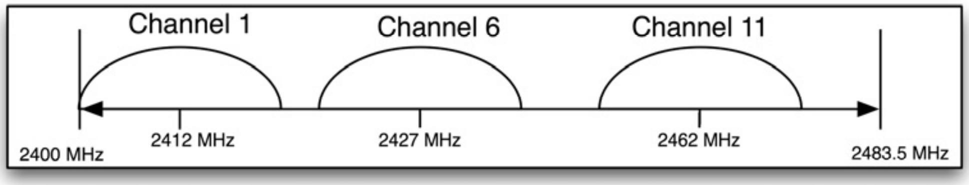


Fig 4.1 – North American non-overlapping channels [otICS99]

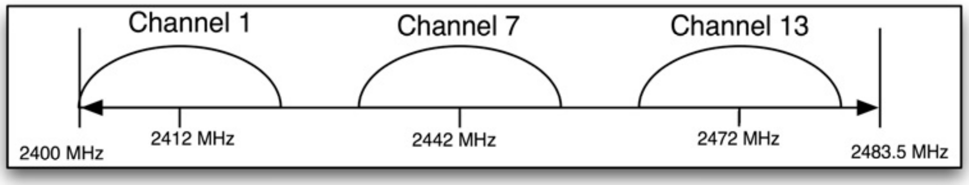


Fig 4.2 – European non-overlapping channels [otICS99]

So why does the IEEE state that there are 11 to 14 channels if in reality there are only three non-overlapping channels? The reasoning for the increased number of channels is overlapping (Fig 4.3 and Fig 4.4).

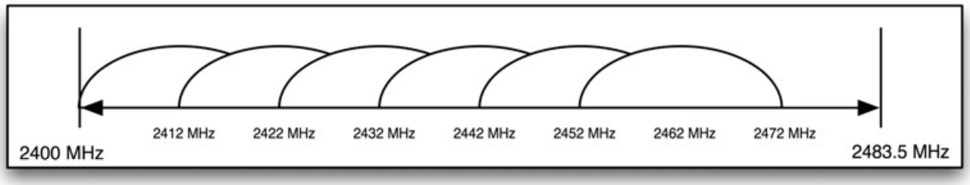


Fig 4.3 – American overlapping channels [otICS99]

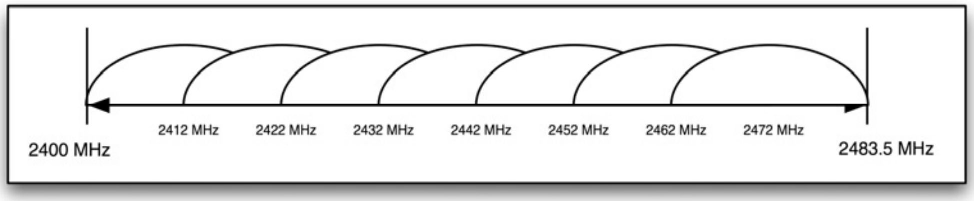


Fig 4.4 – European overlapping channels [otICS99]

The IEEE designated power output levels differ from country to country and are governed by respective control body regulations.

Table 4.2 – Power output as specified by the IEEE for geographical locations

Maximum power output	Geographical location
1 000 mW	USA
100 mW	Europe/SA
10 mW/MHz	Japan

Source: otICS99

The receiver sensitivity specified by the IEEE is -76 dBm [otICS99]. However, most manufacturers do not comply with this requirement. Cisco offers -85 dBm on its enterprise classed Aironet 350 series [Cis]. As described in Chapter 3, lower dBm values mean that the receivers in the Aironet 350 series are in fact more sensitive, because they can detect signals that have much less power at that distance from the transmitter.

The IEEE specifies that 802.11b operates up to speeds of 11 Mbps and 5.5 Mbps in addition to the 802.11 2 Mbps and 1 Mbps rates that 802.11 featured [otICS99].

The pressure newer wireless products such as 802.11g have put on 802.11b has resulted in 802.11b products becoming very cheap. With falling costs the price and availability of stock of 802.11b products should be high [Fli03]. However, once manufacturers completely phase in 802.11g products, availability of 802.11b could be limited.

The IEEE never included any form of official QoS specification in 802.11b. Instead, all traffic is provided a best effort service [Sha] similar to wired Ethernet networks. Every packet that will travel over an 802.11b link will be treated the same as every other packet. The equal treatment of packets means that no guarantee can be made in terms of bandwidth availability, latency or jitter in multimedia applications [Sha]. This means that 802.11b falls short when it comes to the QoS and latency requirements made in the previous chapter.

802.11b summary

Table 4.3 summarizes the previous section in which 802.11b was evaluated according to the evaluation criteria set out in Chapter 3.

Table 4.3 – Summary of 802.11b

Criteria	Subcriteria	Findings
1. Range	a. Frequency	802.11b operates in the 2.4 GHz ISM bands and is therefore free from licensing costs, but is prone to interference.
	b. Power output	Power output is dependent on country. See Table 4.1.
	c. Receiver sensitivity	Minimum required sensitivity is -76 dBm, but most enterprise grade receivers are much more sensitive.
2. Speed	a. Physical layer parameters	The IEEE specifies speeds of 11 Mbit, 5.5 Mbit, 2 Mbit as well as 1 Mbit.
3. Cost (client and station equipment)		The availability of newer standards has pushed prices of 802.11b equipment down.
4. Availability		Availability of 802.11b within enterprise or consumer equipment might be limited as manufacturers attempt to migrate to newer and better standards.
5. Latency		Due to channel overlap equipment might consider traffic on other channels as noise, which will result in the packet being

Criteria	Subcriteria	Findings
		retransmitted. As a direct result packets might take longer to correctly arrive at the desired destination.
6. Mesh routing protocols (standard or proprietary)		Any routing protocol that works with the TCP/IP stack is capable of acting as a routing protocol for 802.11b.
7. QoS		No official IEEE QoS specification.

4.6 802.11a

In 1999 the IEEE also ratified 802.11a as an extension to 802.11. The primary difference is that the 802.11a physical layer is designed to operate in the 5 GHz band instead of the 2.4 GHz band in which 802.11, or its extension 802.11b, was designed to function. While 802.11b has a peak data transfer rate of 11 Mbits/s, 802.11a differs and has a peak transfer rate of 54 Mbits/s [otICSA99].

The evaluation of 802.11a for its suitability in the construction of a wireless MAN has to start with one of the primary differences from 802.11b: the frequency band used.

The 5 GHz band is not an ISM band in the United States. In the United States the 5 GHz band is called the Unlicensed National Information Infrastructure (UNII) band, but in South Africa ICASA also calls it an ISM band [ICA].

One of the most important factors influencing range in relation to a frequency is path loss. Path loss is the amount of energy a signal loses as it travels through the air. Path loss for the 5 GHz band is a lot higher than its 2.4 GHz ISM counterpart. Path loss can be calculated with the following formula where path loss is in dB, λ is wavelength in metres, d is distance in metres, d_0 is the reference distance in metres, and the path loss exponent n is 2 for free space [CP02]:

$$\text{Path Loss (d)} / 20\text{Log}_{10} = 4\pi d_0/\lambda + 10n\text{Log}_{10}(d/d_0)$$

Formula 4.1 – Path loss

In the above formula the variable of interest is λ. As the frequency increases, so do the wavelength and the path loss. This means that the energy the wave carries decreases as the frequency increases and this decreased energy level results in the range suffering. The formula implies that products that make use of higher frequencies will not have the same range as lower frequency equipment at the same power levels. The power of the signal will therefore be of great importance when range comes into play on higher frequency products, and as a result the power will also be of importance when considering 802.11a as a possible deployment technology.The power levels for the 5 GHz spectrums in the United States are indicated in Table 4.4.

Table 4.4 – Transmit power levels for the United States

Frequency band (GHz)	Maximum output power with up to 6 dBi antenna gain (mW)
5.15 – 5.25	40 (2.5 mW/MHz)
5.25 – 5.35	200 (12.5 mW/MHz)
5.725 – 5.825	800 (50 mW/MHz)

Source: otICSA99

In South Africa only the 5 GHz band is in the 5.725 to 5.825 [ICA] band, meaning that locally we can have equipment that has a power output of 800 mW.In terms of available channels the 5 GHz spectrums have eight non-overlapping channels with full bandwidth available [KK03]. Combined with the lower interference that the 5 GHz spectrum has and the larger number of available channels, a much greater number of users at higher speeds can be accommodated with 802.11a than with 802.11 or 802.11b [KK03].

One other difference is that 802.11a uses an alternative encoding method. Orthogonal frequency division multiplexing (OFDM) divides high-speed channels into smaller low-speed channels. At the receiver the multiple smaller subchannels are combined to once again create a single master channel. An advantage of these multiple subchannels is that higher data rates are easier to obtain. Another advantage of these smaller channels is that with the lower amounts of information that each channel carries, interference and reflective surfaces will not result in great losses [KK03].

Thus far it has been determined that 802.11a does have a higher speed on offer, a more resilient encoding method in terms of interference and reflection as well as more non-overlapping channels than 802.11 or 802.11b. These advantages do, however, come at a price: the 5 GHz band does not allow for signals to travel as far compared to their 2.4 GHz counterparts.

The IEEE did not specify minimum receiver sensitivity, but it does specify receiver sensitivity for each of the speeds 802.11a offers. Table 4.5 tabulates the receiver sensitivity for each speed:

Table 4.5 – Receiver sensitivity requirement

Data rate (Mbits/s)	Minimum sensitivity (dBm)
6	-82
9	-81
12	-79
18	-77
24	-74
36	-70
48	-66

54	-65

Source: otICSA99

The results of evaluating 802.11a against the criteria set out in Chapter 3 largely resemble those found in evaluating 802.11b in section 4.5. The similarity in evaluation results is largely due to the fact that both 802.11a and 802.11b were designed as an extension to 802.11, and thus both inherit a few things from a common parent. The differences spring from only two aspects, namely the frequency and encoding method used.

802.11a summary

Table 4.6 summarizes the conclusions made in relation to 802.11a. 802.11a does offer increased speed over 802.11b, but at the expense of a shorter range. As range is a very important factor in all three deployments, many might look twice at 802.11a before choosing it for deployment in a wireless MAN. On the other hand, the reduced interference and increased number of non-overlapping channels might help if the deployment is in an environment where range is not such a determining factor, but number of users of the wireless system and decreased latency due to less collisions are important. Mesh-type networks will clearly benefit from these advantages, as increased number of users and latency sensitivity are key characteristics of mesh networks.

Table 4.6 – Summary of 802.11a

Criteria	Subcriteria	Findings
1. Range	a. Frequency	802.11a operates within the 5 GHz frequency range. According to the free space formula, higher frequency devices have a shorter range.

	Subcriteria	Findings
	b. Power output	Power output is dependent on the country, but may be higher than 802.11b.
	c. Receiver sensitivity	the official 802.11a standard does not officially specify general receiver sensitivity, but rather indicates a level for each speed.
2. Speed	b. Physical layer parameters	The IEEE specifies speeds of 6, 9, 12, 18, 24, 36, 48 and 54 Mbits/s.
3. Cost (client and station equipment)		Costs much higher compared to 802.11b [Fli03].
4. Availability		Mostly available in dual cards like the Dell 4150 Wi-Fi cards.
5. Latency		Channels have less interference and have no overlap, resulting in lower latency.
6. Mesh routing protocols (standard or proprietary)		Any routing protocol that works with the TCP/IP stack is capable of acting as a routing protocol for 802.11a.
7. QoS		No official IEEE QoS specification.

4.7 802.11g

In 2003 the IEEE ratified 802.11g as an extension to the original 802.11. 802.11g attempts to be a silver bullet that eliminates the disadvantages of 802.11b and 802.11a, while still keeping the advantages. As will be seen, 802.11g achieves this goal in many situations but still has a few limitations.

Key changes include the adoption of 802.11a's OFDM encoding and operation within the 2.4 GHz ISM band. The IEEE also made 802.11g compatible with 802.11b while operating at lower speeds by permitting 802.11g to encode using DSSS as well as ODFM [Fli03]. The use of ODFM permits 802.11g to exhibit more resistance to interference from other devices as well as multipath loss.

The use of OFDM does allow 802.11g to offer data rates similar to 802.11a, meaning rates up to 54 Mbits/s.

The use of the 2.4 GHz ISM band does allow for greater distances to be achieved according to the free space (Path) loss formula presented in Formula 4.1, but in turn has to deal with a lot more interference than 802.11a. The increased interference is primarily due to the sheer number of devices that operate in the 2.4 GHz band, including 802.11b, Bluetooth and a variety of cordless phones [Fli03].

The use of the 2.4 GHz ISM band imposes restrictions, and as such the IEEE designed 802.11g to inherit a few things from 802.11b that were placed within the 802.11b specification to ensure compliance with the restrictions. 802.11g inherits all the power output limitations that the 2.4 GHz band induces, resulting in power output that matches that presented for 802.11b in Table 4.2. In addition to power output levels 802.11g also inherits its receiver sensitivity levels from 802.11b, resulting in no additional sensitivity of devices that are produced in adherence to IEEE specification for 802.11g. Channel allocation is also shared with 802.11b, meaning that there are only three non-overlapping channels. The channel overlapping and crowded spectrum will most likely influence latency as well, due to packet retransmitting.

The costs of 802.11g products are expected to drop sharply as production increases. Manufacturers are also more likely to push 802.11g, as it offers not only increased speed but compatibility with 802.11b, and as a result should be a good upgrade choice [Fli03].

While 802.11g does offer increased speed as well as backward compatibility with the popular 802.11b standard, it operates in a more crowded frequency band. Furthermore, the IEEE has not addressed some of the limitations that 802.11b had, it still does not offer any quality of service or any form of integrated routing algorithms.

802.11g summary

The results of evaluating 802.11g are given in Table 4.7 below. The increased range that the 2.4 GHz spectrums offer as well as the interference resilience OFDM offers are welcome when it comes to the use of 802.11g in the deployment of a wireless MAN. On the other hand, there are fewer non-overlapping channels than with 802.11a, as well as increased interference from other devices. This interference will potentially increase latency and make 802.11g a weaker candidate when deploying it in a latency sensitive mesh environment. Backwards compatibility and reduced cost over 802.11a might in the end be a determining factor, and will result in many choosing 802.11g over 802.11a.

Table 4.7 – 802.11g summary

Criteria	Subcriteria	Findings
1. Range	a. Frequency	802.11g operates in the 2.4 GHz ISM bands and is therefore free from licensing costs, but is prone to interference from a wide range of devices.
	b. Power output	Power output is dependent on country, but is similar to 802.11b.
	c. Receiver sensitivity	Minimum required sensitivity is similar to 802.11b, but manufacturers have increased

Criteria	Subcriteria	Findings
		over the minimum specifications.
2. Speed	c. Physical layer parameters	The IEEE specifies maximum speeds of 54 Mbit/s but it also offers fallback speeds compatible with 802.11b.
3. Cost (client and station equipment)		Increased sales of 802.11g products have pushed prices down.
4. Availability		Manufacturers have attempted to push 802.11g as an alternative to 802.11b and as a result the availability of 802.11b-based equipment has reduced and pushed the prices of 802.11g-based equipment down as well.
5. Latency		The use of OFDM provides 802.11g with an increased level of resistance to interference in comparison to 802.11b.
		However, more devices are operating in the 2.4 GHz band than other ISM bands and the amount of traffic increases failed transmission rates and in turn increases latency.
6. Mesh routing protocols (standard or proprietary)		Any routing protocol that works with the TCP/IP stack is capable of acting as a routing protocol for 802.11g.
7. QoS		No official IEEE QoS specification.

4.8 802.16 – WiMAX

During 2001 the IEEE task group responsible for wireless MANs ratified their first standard for 802.16. It was designed to function in a point-to-multipoint infrastructure in frequencies between 10 GHz and 66 GHz, and features speeds ranging between 70 Mb/s and 268 Mb/s. While this all sounded very good, there was very little interest in it initially, as the original 802.16 only operated in line-of-sight (LOS) environments and neglected to offer the ability to operate in non-licensed frequencies. However, in 2003 the IEEE ratified an extension to the base 802.16 specification called 802.16a [O'S04].

802.16a expanded upon the base 802.16 and elicited a great deal of interest from not only the public, but industry as well. It took into account the emerging interest in the unlicensed bands as well by supporting frequencies ranging from 2 GHz to 11 GHz, as well as the need for non-line-of-sight (non-LOS) operations, which were impossible to do at the frequencies specified by the original 802.16 standard [Fit04].

In addition to the lower frequencies and non-LOS operation, the specification added three new physical layer specifications. One of these additional layers matches the physical layer for the European HyperMAN standard, effectively allowing for compatibility with that standard. In addition to the three physical layers, time division duplex and frequency division duplex encoding were also added as possible encoding options, further extending the possible adoption of the standard internationally [O'S04].

The addition of a time-division multiple access protocol in the media access control layer between the station and subscribers allows for intelligent scheduling, resulting in the ability to improve latency. Other QoS features include the ability to automatically request the retransmission of a section of data, per connection QoS as well as automatic power management. These QoS features will allow for anyone that uses WiMAX as a deployment technology to offer low latency communications as well as a wide range of multimedia offerings, including VoIP [Int].

The use of licensed frequencies when using 802.16a differs from every other technology discussed so far, as they all operate in unlicensed bands, and this difference warrants closer scrutiny.

Each country requires different things from a licensee of a frequency; these requirements include power output, encoding method and the level of efficiency of the frequency used. In addition to the requirements set by each government, the number of frequency licences varies from licensee to licensee. One company might license 10 MHz in a low power output spectrum while another company licenses 2.5 MHz in a high output frequency spectrum. Clearly a product that operates within the licensed band comes with many requirements that differ from country to country as well as frequency to frequency. As stated above, WiMAX offers a wide variety of physical layers as well as encoding methods. While the different physical layers hindered 802.11, with WiMAX they are a requirement. Facilitating the variable availability of the frequency band 802.16a as well as the soon to be ratified 802.16REVd offers the potential deployer the ability to use channel sizes ranging from 1.25 MHz to 20 MHz [O'S04].

The WiMAX forum is a group of companies that aims to ensure standardization and compatibility of 802.16-based equipment. The forum believes that most deployments of licensed frequency using WiMAX equipment will be used in the 2.5 GHz range as well as the 3.5 GHz licensed frequency range [O'S04].

Of great interest in the construction of a public wireless MAN is the unlicensed bands, due to not having licensing fees. Many international startup wireless ISPs have used the unlicensed band wireless equipment to offer services to underserved areas. It is those underserved areas that will probably benefit the most from the advantages of a public wireless MAN. It is also these underserved areas that will most likely not be able to afford the licensing costs of licensed band equipment. The downside to the unlicensed bands is, of course, interference. WiMAX addresses many problems that the 802.11 family has, especially range and QoS, but it does have a few problems of its own. The WiMAX forum expects unlicensed band equipment to be available only in early 2006 [Goh04].

The revolution of WiMAX is not complete yet. The IEEE plans to release 802.16REVd as well as 802.16e. The latter will add mobility features to the specification. Table 4.8 illustrates how the WiMAX forum sees the current 802.16, 802.16a/REVd and the future 801.16e.

Table 4.8 – IEEE 802.16 standard

	802.16	802.16a/REVd	802.16e
Spectrum	10 GHz to 66 GHz	< 11 GHz	< 6 GHz
Channel conditions	LOS	Non-LOS	Non-LOS
Speed	32 to 134 Mb/s at 28 MHz channels	Up to 75 Mb/s at 20 MHz channels	Up to 15 Mb/s at 5 MHz channels
Mobility	Fixed	Fixed and portable	Regional roaming
Channel bandwidth	20, 25 and 28 MHz	Selectable, ranging from 1.25 MHz to 20 MHz	Same as 802.16REVd
Range	1.6 km to 8 km	1.6 km to 8 km, maximum of 48 km depending on variables	1.6 km to 4.8 km
Completed	Dec. 2001	802.16a: Jan 2003 802.16REVd: Third quarter 2004	Estimated to be end of 2005

Source: O'S04

802.16 summary

The WiMAX forum has spent vast resources in creating interoperability testing. With the multiple physical layers and encoding methods it is clear that testing is a necessity, but a difficult task. The downside to the extensive testing is that WiMAX equipment is yet to clear any form of interoperability testing. Combined with local legal requirements set out by ICASA, it will still most likely be a long time before licensed and unlicensed band equipment is available to consumers.

However, delays do not eliminate WiMAX as a potential candidate for usage in one of the deployments specified in Chapter 3. Table 4.8 summarizes the variety of 802.16 standards. If the standard can accomplish what it promises, it will be an ideal technology for use in any deployment. High speeds, low latency and a variety of other QoS features combined with the promise of longer ranges result in WiMAX being suitable with every deployment set out in Chapter 3.

Table 4.9 – 802.16 summary

Criteria	Subcriteria	Findings
1. Range	a. Frequency	The wide variety of frequencies supported by 802.16a range from 2 GHz to 11 GHz. Of great importance in terms of cost is the support for unlicensed bands.
	b. Power output	No official output has been specified for unlicensed equipment. Power output of equipment in licensed bands depends on the frequency band used and the local government.
	c. Receiver sensitivity	No official sensitivity is specified.

Criteria	Subcriteria	Findings
2. Speed	d. Physical layer parameters	Speeds range up to 75 Mb/s in non-LOS usage. However, the ability to use channels of varying sizes allows for numerous speed options.
3. Cost (client and station equipment)		Currently not available to consumer.
4. Availability		Currently still in certification testing.
5. Latency		Low latency is promised with the addition of time-division multiple access protocol in the media access control layer.
6. Mesh routing protocols (standard or proprietary)		Any routing protocol that works with the TCP/IP stack is capable of acting as a routing protocol for 802.16a.
7. QoS		802.16a offers a variety of QoS features.

4.9 Conclusion

In this chapter the aim was to evaluate a few standards that will most likely be used in the deployments set out in Chapter 3, as well as evaluate their suitability for those deployments.

The IEEE serves as a body that aims to develop standards, and it is these standards that were evaluated. However, even though the IEEE sets out standards they are not always fully adopted, or they are extended with proprietary techniques and as a result make deployments using these technologies more difficult on occasion.

Starting with the first announced standard, 802.11b serves as a basis for the remaining 802.11 standards. It operates in the 2.4 GHz unlicensed spectrum with speeds up to 11 Mb/s. However, it has limited range and no QoS features, making use of 802.11b as a deployment technology difficult.

802.11a was released next and offered increased speed as well as a more adaptable encoding algorithm. However, this was at the expense of decreased range due to the higher frequency used.

The IEEE attempted to create a bridging standard with 802.11g by using the same encoding algorithm but with the 2.4 GHz frequency spectrum instead of the 5 GHz spectrum that 802.11a uses. However, 802.11g has to contend with the larger amount of interference in the 2.4 GHz band.

With 802.16 the IEEE attempted to create the perfect metropolitan wireless technology, but failed. The revised 802.16a and 802.16REVd have elicited interest from a large number of companies and solve many of the problems that limited the 802.11 families from fully functioning as a deployment in a wireless MAN. The downside, however, is that there is no 802.16 equipment currently available to the end consumer, and unlicensed band equipment is not expected to be available for even longer.

Currently there is no single perfect solution for any of the deployments considered in Chapter 3. However, most of them are good enough.

The choice of deployment technology will ultimately depend on the people that will construct the particular deployment.

With the knowledge of the abilities and shortcomings of wireless technologies, I can now proceed to determine what topologies these technologies are capable of and attempt to construct a topological model that will span an entire metropolitan area network but using supported topologies.

Chapter 5 – Node types, layouts and structures

5.1 Introduction

In the previous chapter technologies were reviewed to determine their suitability in the construction of a wireless MAN. Assuming that an appropriate technology can be selected for each deployment, there is still the matter of how each deployment fits together.

Like wired networks, wireless networks have a wide variety of possible topologies. While wireless and wired networks have some topologies in common, others differ. This difference is mainly due to the different physical mediums and deployments used.

Intel defines three types of deployments for large wireless networks [Int]:

1. Backhaul.
2. Large area coverage (mesh).
3. Last mile.

In Chapter 3 each of the deployments listed above was given along with a basic description. In this chapter some of the possible topologies that can be used by these three deployments will be highlighted, as well as advantages and disadvantages for the topology under inspection. I will then proceed to give topologies used by a few current wireless MANs, and finally give a custom topology that attempts to overcome some of the limitations of the existing topologies.

5.2 Backhaul

Backhaul connections typically go from one group of aggregate users to another using a single connection (Fig 5.1). The keywords in the definition are "groups of aggregate users". A backhaul connection would need to be able to carry the services these two disjointed groups of users would need, wherever they are [Int].

The logical topology for a wireless backhaul connection is exactly the same as for wired backhaul connections, but with wireless backhaul connections much greater distances can be covered and at a much lower cost, and with greater flexibility than their physical alternatives [Pro].

Most current backend and backhaul connections deployed by phone companies, railway and government agencies worldwide are point-to-point connections [Has], and are used to connect offices and buildings kilometres apart and carry data ranging from audio and video to email [Pro]. Fig 5.1 illustrates a typical backhaul connection.

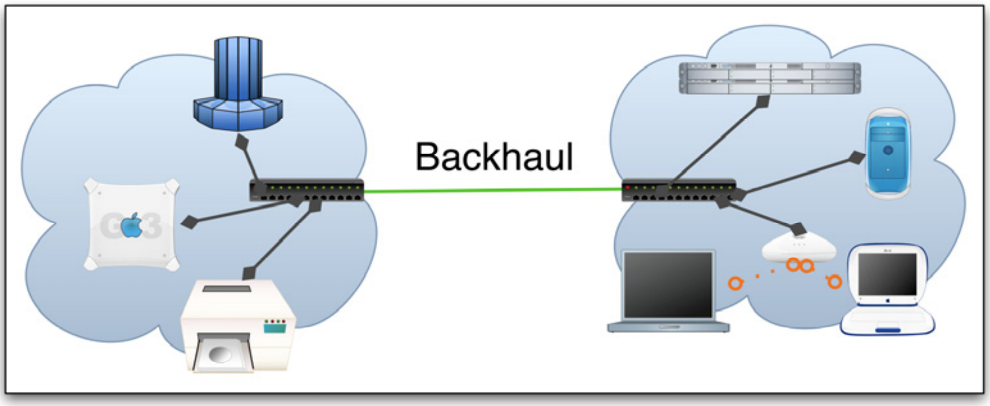


Fig 5.1 – Backhaul topology

Since point-to-point connections involve only two points of access, the only concerns are with what is in between the two points and how it will affect the setup and maintenance of that link. This is where the physical and wireless backhaul connections start to differ.

Wired backhaul connections would need to be concerned with the physical aspects such as trenches needed for the cabling. High-speed cable backhaul connections are not always available everywhere, but it is very easy to add a wireless backhaul connection to those under connected locations in a very cost-effective manner [Pro]. It is for this reason of cost-effectiveness that many point-to-point connections are constructed using wireless technology. A wireless backhaul connection has no connection to the physical aspects governing wired backhaul connections and is a big selling point.

Wireless point-to-point connections, on the other hand, would be concerned with the air in between the wireless link [Fli2a]. Most technologies discussed in Chapter 4 require line-of-sight to operate over great distances. LOS means that the two points have to be visible to each other. Of all the technologies reviewed, WiMAX does not require LOS, but with devices not being available to end-users the true ability to operate in non-LOS environments is yet to be proved.

Because no person or company can be in control of what happens between the two points of a wireless connection, the LOS requirement is a major disadvantage to wireless backhaul connections. An example of this is that while in the winter there might be LOS, in the summer trees and their leaves might impair the connection. In a metropolitan environment not only can naturally occurring environmental aspects (such as trees) interfere, but general radio frequency propagation can also become very challenging and troublesome [Viv].

The possibility of interference means that any technology used will have to be resilient to interference, be it environmental, natural or man-made [Viv].

In addition to the requirements set out in Chapter 3, any technologies used for a backhaul connection will have to offer not only range and speed to connect two groups of aggregate users together, but they must also have the ability to function in point-to-point connections and offer a level of resilience to various types of interference, as well as have a controllable or predictable level of radio propagation.

5.3 Large Area Coverage (Mesh Networks)

Section 5.2 mentioned large groups of aggregate users. In a wireless MAN these aggregate groups are not always very close to each other. This means that even though people may be in the same geographical area, meaning a suburb or even a street, the geographical area in question may still be very large.

One of the key advantages to wireless mesh networks is that they cover large areas through the creation and use of multi-hop networks [AWW04]. Wireless mesh networks and their multi-hop nature make the cost-effective coverage of large areas easy. It is for this reason that wireless mesh network topologies are investigated in this research with the end goal to cover large areas.

Wired networking environments do have mesh networks and they often cover large areas. However, in a true mesh every network device is attached to every other device directly (Fig 5.2). While there is a great level of improved performance and resilience, the sheer number of physical connections becomes limiting and results in true meshes being very rare. Wireless mesh networks, however, do not need to be physically connected due to the wireless physical layers and they incur less costs. The result is true, or near true, wireless meshes being possible [Int].

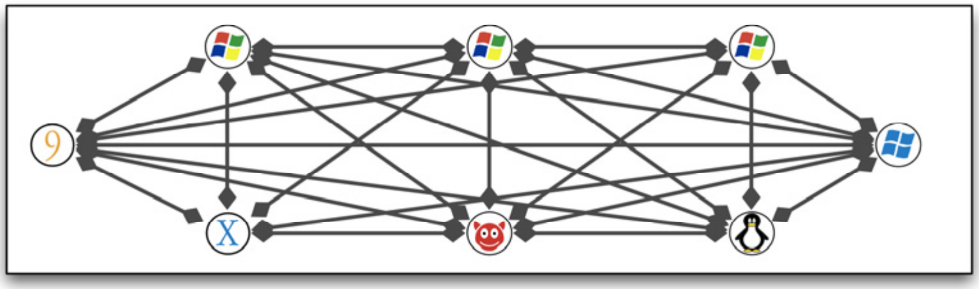


Fig 5.2 – True mesh topology [Bel05]

True or near true wireless mesh networks (WMNs) have two types of nodes, namely [AWW]:

1. Client.
2. Router.

The distinction between client and router is very blurred. Clients have the necessary functions to operate in a mesh network, and as such may also be able to perform the functions of a router. It is this possible difference in functionality that gives rise to the three topologies of WMNs [AWW].

The first of the three WMN topologies is infrastructure or backbone WMNs. Infrastructure WMNs have many routers that connect to each other and form multiple links between them. They create self-forming, self-healing and self-organizing networks with full routing capabilities. The clients, on the other hand, do not perform any routing functions. If the clients have the ability to do so, they can directly connect to the routers; if they do not have the ability to directly connect to the router, they can connect via Ethernet, Wi-Fi or any other connection medium that is capable of communicating with the router [AWW]. Fig 5.3 illustrates an infrastructure WMN; the broken lines indicate a wireless link, solid lines wired links and the clouds the different forms of clients.

5.3 Large Area Coverage (Mesh Networks) - Continued

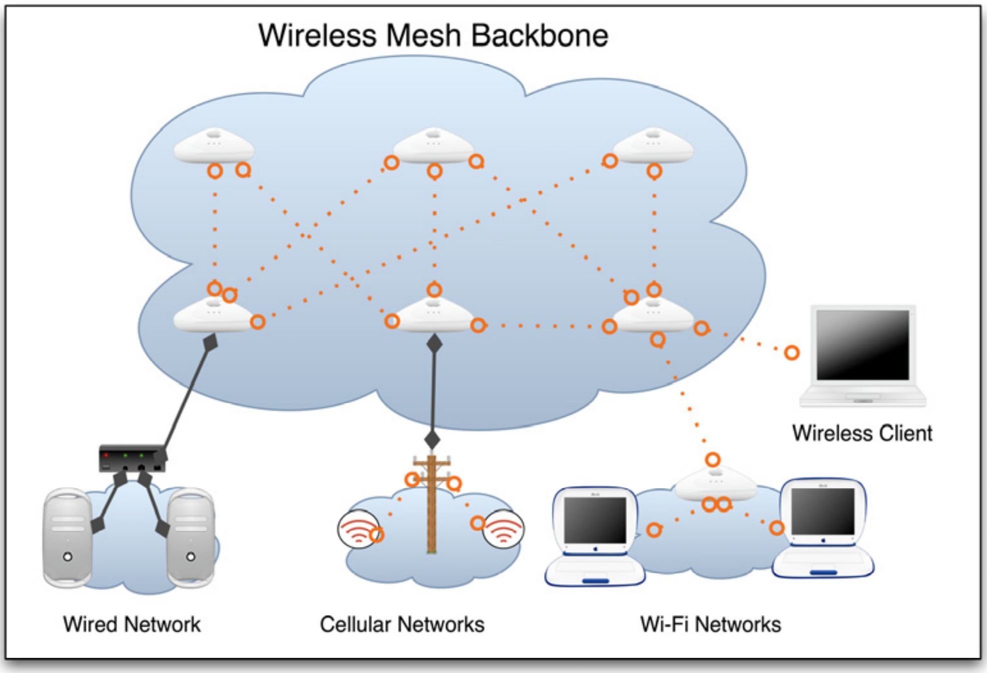


Fig 5.3 – Infrastructure WMN [AWW]

The second type of WMN topology is client WMNs. The difference between infrastructure WMNs and client WMNs is that client WMNs do not have routers. All clients are capable of performing routing functions and as such act as routers and clients at the same time (Fig 5.4) [AWW].

5.3 Large Area Coverage (Mesh Networks) - Continued

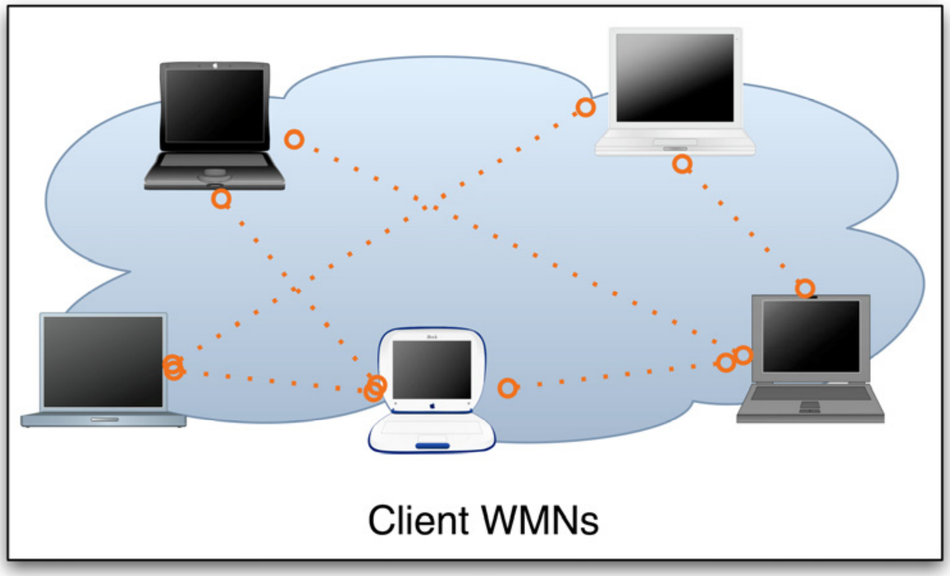


Fig 5.4 – Client WMN [AWW]

The third and final type of WMN is the hybrid WMN. It is a topology where both infrastructure and client WMNs are visible. Fig 5.5 illustrates a hybrid WMN where the broken lines indicate wireless links, solid lines wired links and the clouds the different forms of clients [AWW].

5.3 Large Area Coverage (Mesh Networks) - Continued

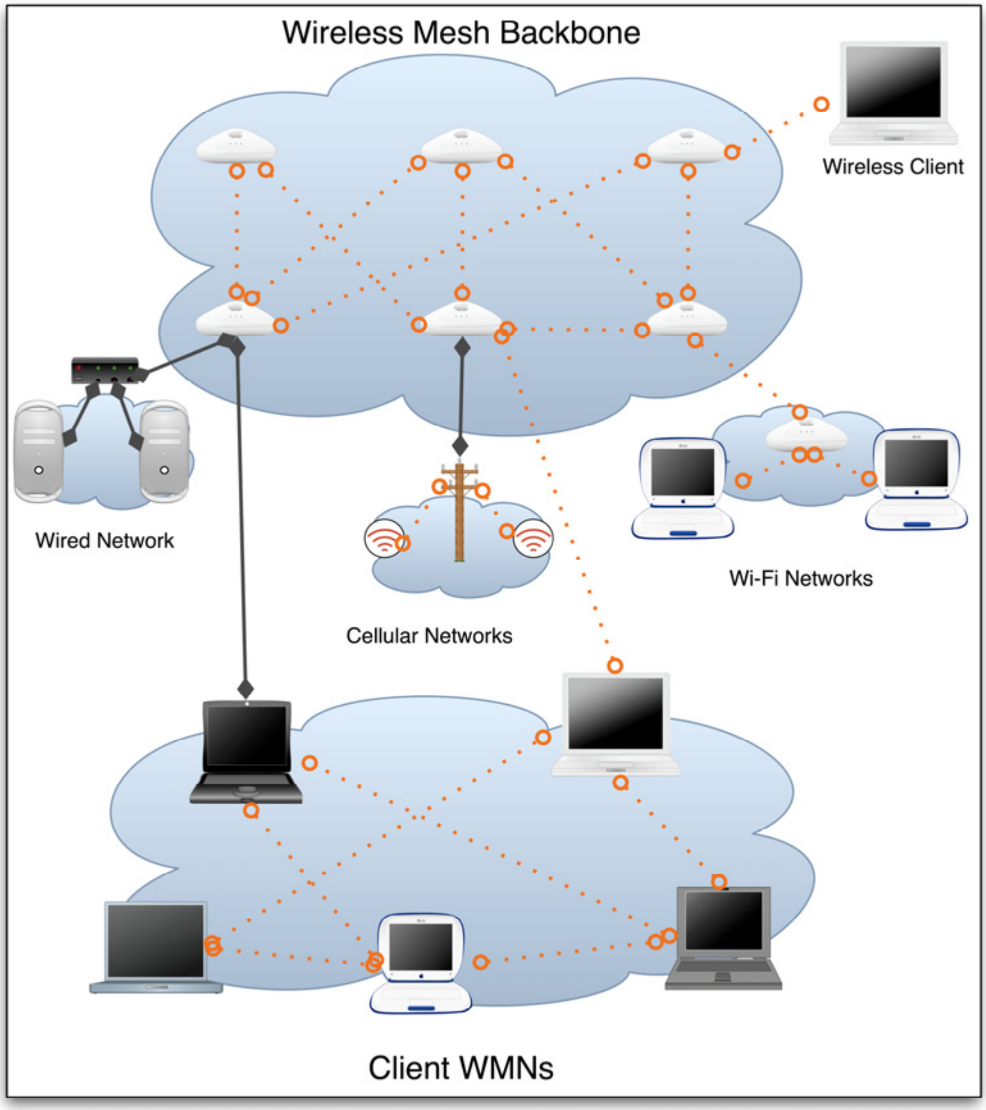


Fig 5.5 – Hybrid WMN [AWW]

5.3.1 Characteristics of a WMN

Mesh networks have a very flexible topology; they do, however, have a few disadvantages. Before proceeding with the advantages and disadvantages, a few characteristics of WMNs need to be mentioned. Most of the WMN characteristics listed have some comparable or related aspect within current wireless MANs. A good understanding of WMNs is needed to understand the current MANs, as well as future MANs and their potential.

The characteristics of WMNs are as follows [AWW]:

1. Multi-hop wireless networks.
2. Self-forming, self-healing and self-organizing.
3. Mobility dependent on node types.
4. Multiple types of network access.
5. Compatibility and interoperability with existing wireless networks.

The five characteristics mentioned above need more discussion. A clear comparison will also be drawn between WMNs and wireless MANs.

5.3.1.1 Multi-hop wireless network

Within the traditional WMN the objective when building a WMN was to cover greater areas without sacrificing any channel space. An additional objective was to provide users with no LOS access to the network facilities and in essence non-LOS connectivity [AWW].

The very nature of a wireless MAN requires great distances to be covered. With no single land-based wireless technology that can span an entire metropolitan area from one central point, multiple points of access have to be used, using either the same or different technologies. These multiple points thus have to communicate with each other to span the entire metropolitan area. The large coverage area that multiple points of access allow means that data travelling from one point in the wireless MAN to another have to hop from one point of access to another.

It is extremely difficult to obtain LOS with every possible point of access within a metropolitan area. Through the use of multiple points, non-LOS operation between two distant points is achieved through the multiple hops.

Clearly there is great similarity between the characteristics of a WMN and the very nature of a wireless MAN.

5.3.1.2 Self-forming, self-healing and self-organizing

Because of the flexibility in the design of a WMN and the supposed low upfront cost in the creation of a WMN, multiple nodes are added quickly and effortlessly. By increasing the level of nodes a level of fault tolerance is created as multiple paths are created from one node to another. With the level of fault tolerance, as well as the increased number of nodes the placement of points of access become less restrictive and organizational aspects fall away [AWW].

Wireless MANs also achieve a great level of fault tolerance (self-healing), but only over time. As the public selectively adds nodes as desired (self-forming and self-organizing), distances between points of access become smaller. As distances become smaller, the number of areas without coverage is decreased, and the appropriate placement of points also becomes reduced (self-organizing).

While the approach to achieving the characteristics may seem different, the end results are the same. Both WMNs and a wireless MAN will have self-forming, self-healing and self-organization properties.

5.3.1.3 Mobility dependent on node types

Different node types in a WMN have different mobility characteristics. Clients may be stationary or mobile, while routers are normally stationary [AWW].

Depending on the construction of the wireless MAN, nodes may also be stationary or mobile. Clients that connect to the points of access may be laptop users, while the points of access will most likely be stationary.

The Oxford English Dictionary defines mobility as “the ability to move or be moved freely and easily” [Sim89]. This definition defines human mobility well, but the detail for wireless device mobility is lacking. An example of this is that while cell phone users may be able to travel at 120 km/h and have network connectivity and can be truly mobile, Wi-Fi-enabled laptops will not have coverage at 120 km/h and will not have the same level of mobility.

The reason for different levels of mobility is the size of the different coverage areas. A cell coverage area is much bigger than a Wi-Fi coverage area. Even with an entire MAN built out of Wi-Fi equipment, Wi-Fi client equipment would continuously have to pair with a new access point.

5.3.1.4 Multiple types of network access

With WMNs users may be able to access any service of the WMN, including any services that are provided by networks to which the WMN is attached. These services include backhaul access, peer-to-peer access and backhaul access to the Internet [AWW].

The overall goal of a public wireless MAN is the ability to access services provided by other users of the MAN, as well as to provide services to others. To be able to access or provide services the very network will have to feature the ability to provide these services over any appropriate and available connection, be it backhaul connectivity to the other side of the city or direct peer-to-peer connectivity.

5.3.1.5 Compatibility and interoperability with existing wireless networks

WMNs built on 802.11-based devices have to comply with their respective IEEE specifications and have the needed features to be able to function and access the services of a mesh. However, compatibility with respective standards is not enough. The deployment may be very diverse due to the ad hoc method of constructing the network, and many different technologies may be used, including wired technologies. For this reason interoperability with diverse technologies is also essential for WMNs [AWW].

A public wireless MAN does not have a central controlling body. Instead, it has many individuals with unique characteristics and, more importantly, unique budgets. It is these unique individual aspects that will result in any public wireless MAN having many different types of technologies that will have to be compatible or interoperable.

As with self-forming, self-healing and self-organizing, the approach taken may not be the same, but the end result is very much the same. Both WMNs and wireless MANs have the need for compatibility and interoperability due to characteristics inherent in both network types.

Sections 5.3.1.1 to 5.3.1.5 listed five characteristics of WMNs. WMNs were compared with wireless MANs with the aim of showing that most current wireless MANs are in essence some form of WMN.

Before proceeding with the disadvantages of WMNs I would like to summarize the advantages. They are as follows [FIn]:

1. Extensive range due to multi-hop architecture.
2. Self-forming, self-healing and self-organizing.

5.3.2 Disadvantages of WMNs

The advantages listed above further illustrate how WMNs are closely related to wireless MANs. However, the disadvantages indicate that a true WMN structure might not be the best structure to use in a wireless MAN.

In 2004 authors Ian Akyildiz, Xudong Wang and Weilin Wang published an article entitled “Wireless mesh networks: A survey”. In the article they frequently mention aspects where WMNs are either lacking, limited or still need to be actively researched. These lacking aspects and limitations are considered in this dissertation as the disadvantages of WMNs.

The summarized disadvantages are as follows [AWW]:

1. Limited scalability.
2. QoS.
3. Increased costs.
4. Security.
5. Limited mobility.
6. Routing protocols.

5.3.2.1 Limited scalability

One key disadvantage of WMNs is that in their current form they do not scale very well. The reason for this limited scalability is that as node density increases, the throughput drops considerably.

As nodes are added, more and more pathways are created over which data can travel. With the increased number of pathways, the routing protocols have to perform much better to ensure that data is transmitted over the optimal path. However, most current routing protocols are insufficient when they are applied to mesh topologies.

The Massachusetts Institute of Technology (MIT) created an experimental multi-hop roof network called Roofnet. The network consists of approximately 50 nodes interconnected with Ethernet networks and Internet gateways. In April 2004 the average TCP throughput and latency were measured to the nearest Internet gateway in the Roofnet network. With one hop to the gateway and 18 nodes in the group the average throughput was 357.2 KB/s with a latency of 9.7 ms. When the nodes were decreased to seven in total but the number of hops increased to four, the average throughput dropped to 47 KB/s and the average latency jumped to 43.0 ms. Roofnet is constructed using 802.11 MAC equipment. The measurements indicate the limited scalability of a non-WMN optimized specification and the lack of an adequate routing protocol [AWW].

With the coverage area of a wireless MAN potentially being much larger than a conventional WMN, the scalability of a metropolitan-sized WMN is also decreased considerably due to the possible increase in the number of clients.

5.3.2.2 QoS

As with the Internet, the applications of a WMN can be very diverse and will most likely include services that have various QoS requirements.

Thus in addition to end-to-end transmission delays, additional performance metrics have to be considered to cater for the variety of QoS requirements. These QoS related metrics include [AWW]:

1. Aggregate and per-node throughput: The variety of paths a packet can travel through brings the different possible pathways into consideration. If a single node has a low latency as well as a low throughput, a simple end-to-end transmission delay routing protocol will choose that specific path, resulting in that path becoming congested. Packets that do not travel over the congested link will arrive out of order and result in completely lacking QoS.
2. Packet:loss ratio: Packet:loss ratio defines the percentage of packets that get lost within a given set of frames or window. With wireless mesh networks the packet loss over one link may be very high, and result in a higher packet:loss ratio at the destination. The increased packet:loss ratio combined with delays due to the multi-hop nature of a mesh network can contribute to the decreased throughput in large mesh networks.

5.3.2.3 Increased cost

As mentioned earlier in this chapter, to perform as a mesh client or router, additional capabilities are needed over those capabilities of a conventional wireless node.

These features may include additional routing software, but in some cases to increase throughput the particular implementation may include expensive directional and smart antennas, multi-input/multi-output (MIMO) systems and multi-radio/multi-channel systems [AWW].

These additional capabilities are software or hardware features. These features may be proprietary, thus not offering the reduced cost that open implementations offer. Either way, the additional costs of hardware or software, proprietary or open, will be carried over to the end-user and increase costs of deploying a WMN on a metropolitan scale.

5.3.2.4 Security

Without the guarantee of appropriate security and reliability, customers or conventional users will find very little incentive to connect to any WMN. Although many security methods have been proposed for conventional wireless LANs, WMNs differ considerably and do not always fit into the proposed security method.

Security issues of a WMN arise due to the distributed nature and the ad hoc architecture. Current wireless networks, for example, suggest the use of a RADIUS as an authentication method. However, with the distributed nature there can be no single central authority that can maintain the RADIUS server and issue certificates needed for authentication [AWW].

The end result is that many security breaches occur due to vulnerabilities in the channels used and the nodes in the shared wireless medium. The absence of clear infrastructure and the ever-continuing and dynamic change of the network's topology also contribute to security breaches [AWW].

General consensus suggests that to increase security in WMNs would be to include security features in the network protocols, such as secure routing. While many security mechanisms have been suggested, one single solution on one of the OSI layers cannot correct security flaws on other layers; thus a multi-layer approach is required [AWW].

5.3.2.5 Limited mobility

One of the key reasons many people choose to go wireless is the offer of mobility. For this reason mobility is of considerable importance to the clients of any wireless network.

However, when mobility comes into consideration in a WMN, a few additional aspects have to be considered. Routers now need to keep better track of users as they travel from one point to another and go out of range of one router and enter the coverage area of another. To better track clients, topological information has to be exchanged. This information may not always be available to the client, especially in an area that might cover an entire metropolitan area [AWW].

5.3.2.6 Routing protocols

As indicated by the Roofnet example in section 5.3.2.1, routing algorithms currently cannot keep up with WMNs. Under increased loads mobility becomes a problem, scalability affects the performance of the network and QoS features may be limited.

Routing protocols can become extremely complex and are an entirely self-contained research field. WMN routing protocols are in general very complex and must be able to take more aspects into consideration than they currently do.

Some of these aspects are [AWW]:

1. Performance metrics: While many current routing protocols are based on minimum hop count, in some cases this is not an accurate metric. If a connection between two nodes becomes weak, the throughput will decrease. To solve this problem link quality will have to be considered as a metric as well. In a few cases round trip times can also be used as a performance metric.
2. Fault tolerance with link failures: One objective of a WMN is to offer redundancy, and as such link failures have to be handled gracefully.
3. Scalability: Setting up a path from one side of an ever-changing mesh network can be very difficult and take very long. Even after a path has been set up, the path may change due to the dynamic nature of a WMN and invalidate the path.

In this section it was indicated that while mesh topology may be a very adaptable and flexible topology with great coverage capability, it has many disadvantages, and that when a WMN is spread over a large area, the disadvantages are exaggerated and can greatly impair the network's performance. For this very reason a true wireless mesh may not be the best topology to use within a metropolitan area network.

5.4 Last Mile Connections

The last 20 years saw the rapid deployment of fibre optics between the 25 biggest US metropolitan cities and the US Internet backbone. However, the rapid increase of available bandwidth was not available to most consumers. The problem stemmed from the fact that there was no adequate technology to connect the end consumer to the high-speed networks available to them only a short distance away. This problem was aptly called the last mile problem [Lig].

In South Africa the problem is very similar. While locally we do not have the abundance of fibre connecting our cities together, we still have the last mile problem. For years the only option to connect an ISP was by using modems. As time passed Telkom eventually released DSL, Sentech released MyWireless and the iBurst product range was also introduced to bridge the last mile in South Africa.

MyWireless and iBurst are wireless products that solve the last mile problem. With a few single access points and multiple clients connecting to each individual access point, MyWireless and iBurst both are point-to-multipoint topologies (Fig 5.6). The choice of a point-to-multipoint topology also agrees with Intel's view that when WiMAX is used to solve the last mile problem, it should also be used in a point-to-multipoint topology [Int].

Fig 5.6 illustrates a point-to-multipoint topology. The cloud represents the groups of users and the dotted lines illustrate the wireless connections between the multiple clients and the central access point.

5.4 Last Mile Connections - Continued

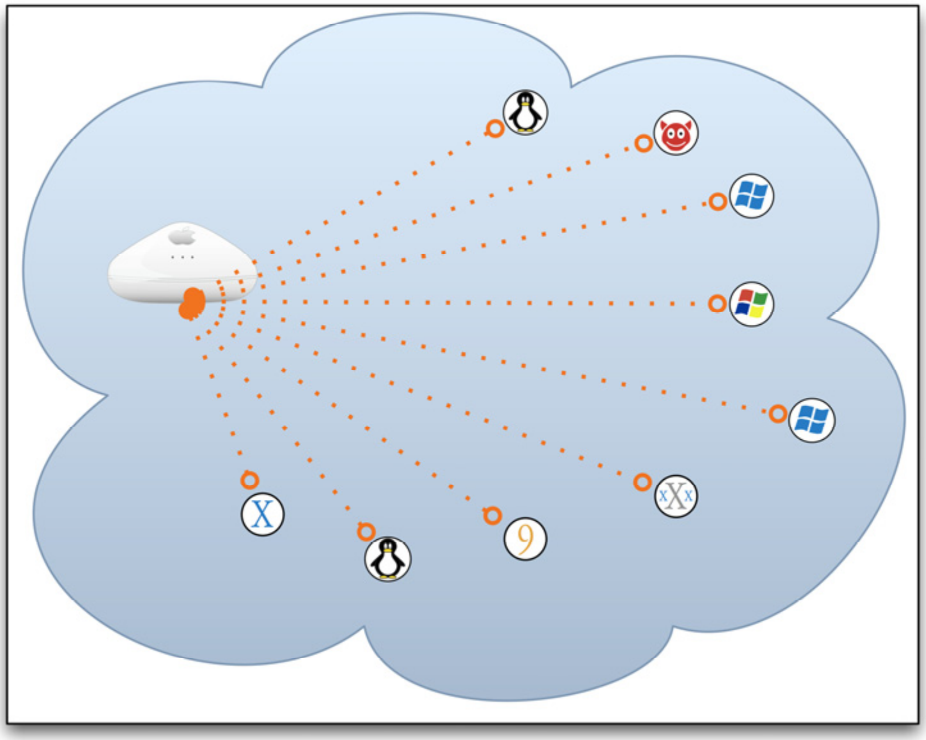


Fig 5.6 - Point-to-multipoint connection

A point-to-multipoint topology allows many users to connect to a central point. This centralization of access results has a few advantages. In stark contrast to mesh networks, security can now be easily managed. The central point of access resembles an access point from a Wi-Fi network, and with extensive work done in the Wi-Fi arena concerning security, many security alternatives are now available to point-to-multipoint wireless topologies.

Centralization of the access point allows for not only an enhanced level of security, but also for a single point and its clients to be easily managed, effectively allowing for incredible control over all features of the access point.

In addition to enhanced security and easier administration, the fact that the signal originates at a single point means that the RF link can be controlled from a central point [PH02]. The ability to control the radio signal from a central point implies the ability to control range as well as the number of nodes that can access the central access point.

With point-to-point topologies both points act as a server and client, and the overall cost is increased due to the complexity of the hardware. Point-to-multipoint, on the other hand, allows the cost of the client side terminal equipment to be spread over many clients, resulting in an overall cost reduction to clients [Has].

The downside to the centralization, however, is that a central point of failure is introduced. Unlike with a mesh with its extreme adaptability, when a central point of access goes down, all clients are effectively disconnected from the network [PH02].

Another disadvantage of a single point of access is that even though coverage can be controlled, there is always a limit to the extent of coverage. The choice of location to place an access point to facilitate the best possible coverage can also be very difficult. The ideal placement location may not be available, and even if it is, moving an established access point will create coverage for some but remove it for others.

Table 5.1 summarizes the advantages and disadvantages of point-to-multipoint topologies.

Table 5.1 - Point-to-multipoint topology – advantages and disadvantages

Point-to-multipoint topology	
Advantages	Disadvantages
1. Increased security	1. Central point of failure
2. Central point of administration	2. Limited coverage
3. Control over radio frequency	3. Difficult placement
4. Reduced cost	

5.5 Node Types of Current Wireless MANs

The concept of a wireless MAN is not a new one; a few groups of people have attempted to construct a wireless MAN with varying degrees of success.

In many cases the open wireless networks started out as a way to connect students to their respective campus networks, but over time they grew to a more generic wireless MAN with coverage spanning the entire city. An example of a large wireless network starting as a student project is the MIT Roofnet network. Initially started as a way to research wireless mesh networking, the network soon expanded beyond the research purposes and became a network that covers a large area of Boston and allows for MIT students to access the MIT network as well as MIT’s Internet connection [AWW].

With various network deployments, different effective topologies have been created and in almost all cases they have defined their own node types. The primary reason for the custom node types in the respective wireless MANs are to cater for and utilize the evolution and growth of a wireless MAN.

The evolution of a wireless MAN is very important. Due to the public nature of the network, it will not be possible to construct or plan for the network in a single attempt.

The following four wireless MAN project node types are reviewed:

1. Seattle Wireless.
2. Bay Area Research Wireless Network (BARWN).
3. Southampton Open Wireless Network (SOWN).
4. Johannesburg Wireless User Group (JAWUG).
5. Bristol Wireless.

5.5.1 Seattle Wireless

Seattle Wireless is a non-profit effort to build a completely wireless community network in the Seattle area. The use of inexpensive and off-the-shelf components have allowed for the effort to grow from grassroots through self-interest and sheer community spirit [FPS05]. Seattle Wireless also shares Internet access, something that is currently illegal in South Africa [oSA96].

Seattle Wireless defines five node types:

1. Client Node.
2. DxNode.
3. CxNode.
4. BxNode.
5. AxNode.

The first node type is the basic client that accesses the network. Access is given to any client that is within range and has an access point compatible device. The complete flexibility of the client due to no specific hardware requirements allows for clients to easily and affordably access the Seattle Wireless network.

The second node type in the Seattle Wireless network is called a DxNode. A DxNode is defined as any node that does not have an upstream connection; this means that it is a completely independent and isolated point of access. A DxNode node owner would simply start a node with an access point. The access point forming the DxNode would use the node owner's wireless technology of choice. A DxNode is configured with a single interface and with an omnidirectional antenna. The goal of the wide coverage area provided by the omnidirectional antenna is to make the network available to as many people as possible. Seattle Wireless expects a DxNode to be upgraded to a CxNode or higher-level node as time progresses. Clients connect to a DxNode just as they would to any appropriate access point of that technology. The DxNode owner also handles addressing and assigning IP addresses (Fig 5.7) [DxS].

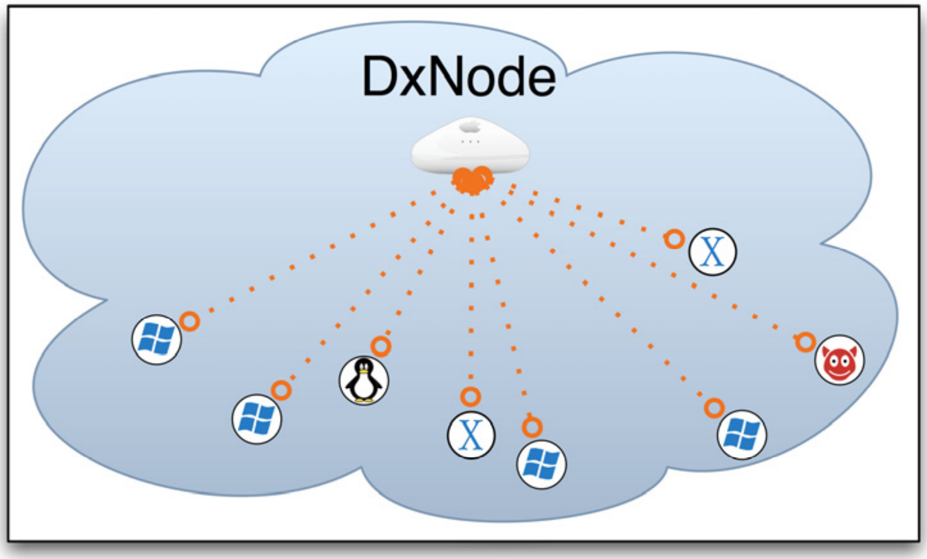


Fig 5.7 – DxNode [DxS]

The third type of Seattle Wireless node is a CxNode. The primary difference between a CxNode and a DxNode is that a CxNode possesses a single upstream connection. This upstream connection allows clients connected to the CxNode to access the rest of the network. The upstream connection may be a tunnel set up through the Internet if another wireless link is not possible. Seattle Wireless states, however, that a wireless link is preferred. The wireless upstream link would be made using a dedicated wireless interface functioning in ad hoc mode, and would be connected to a directional antenna. Clients connecting to the CxNode would simply do so as if they were connecting to a DxNode. Unlike with a DxNode, addressing for the clients would not be handled by the owner of the DxNode, but be assigned by the BxNode in the area. Address allocations by Seattle Wireless to CxNodes are presently based on physical location (Fig 5.8) [CxS].

5.5.1 Seattle Wireless - Continued

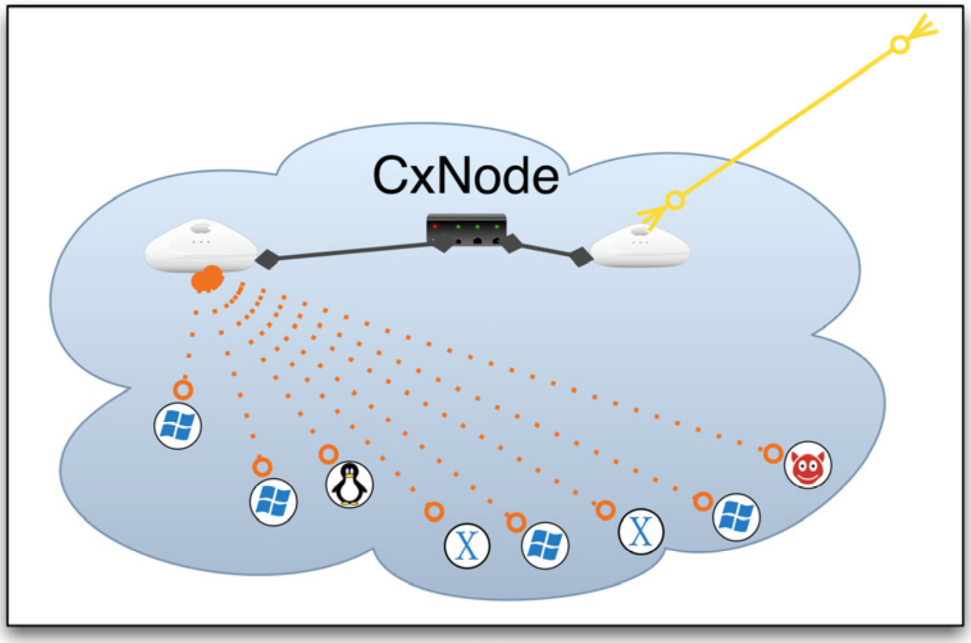


Fig 5.8 – CxNode [CxS]

The next evolution of a node in the Seattle Wireless network is a BxNode. A BxNode needs three wireless interfaces. One interface would be connected to a CxNode, while the remaining two are connected to other BxNodes or routers in the BxNode cloud; the connection is made using directional antennas. In addition to providing routing services to CxNodes connected to the BxNodes, BxNodes also have to provide DHCP services to the CxNode. Seattle Wireless states that each BxNode will be assigned a single class B address and class C addresses should be assigned to CxNodes (Fig 5.9) [BxS].

5.5.1 Seattle Wireless - Continued

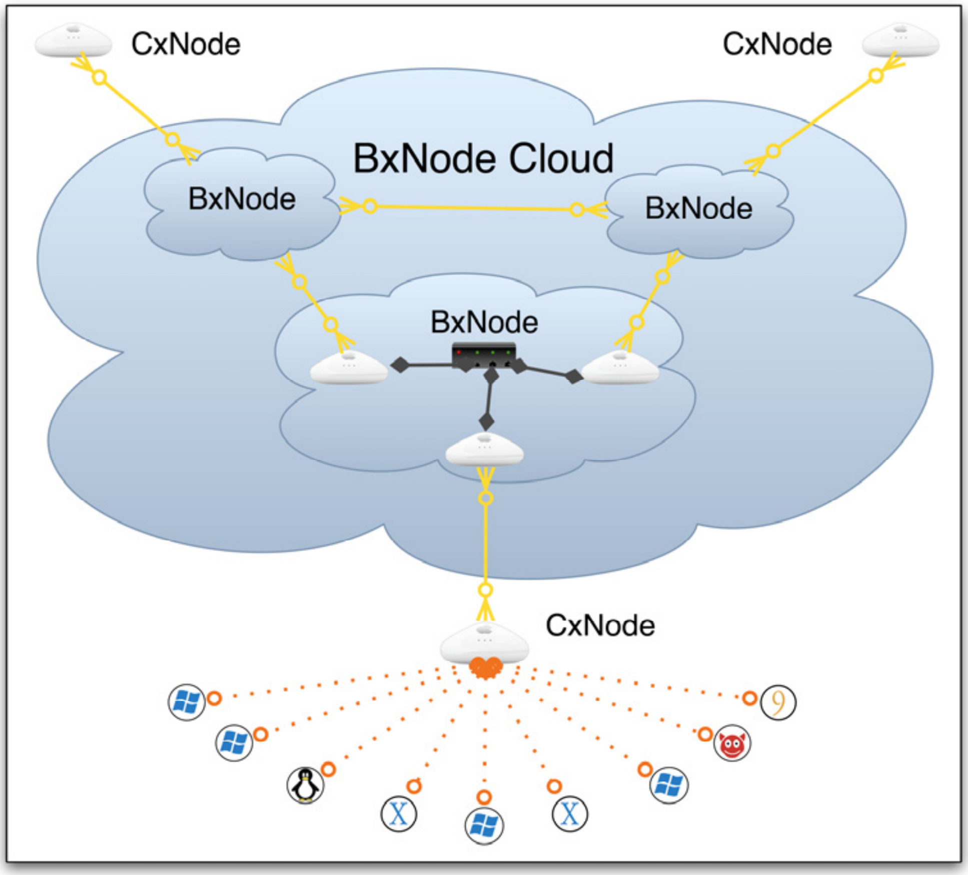


Fig 5.9 - BxNode [BxS]

The final type of node in the Seattle Wireless network is an AxNode. An AxNode is simply a “Super BxNode” [AxS], meaning that the primary difference between an AxNode and a BxNode is that an AxNode has *n* wireless interfaces (where *n* >= 4). An AxNode only provides intelligent routing through the BxNode cloud, but does not connect to CxNodes. The addressing is similar to BxNodes (Fig 5.10) [AxS].

5.5.1 Seattle Wireless - Continued

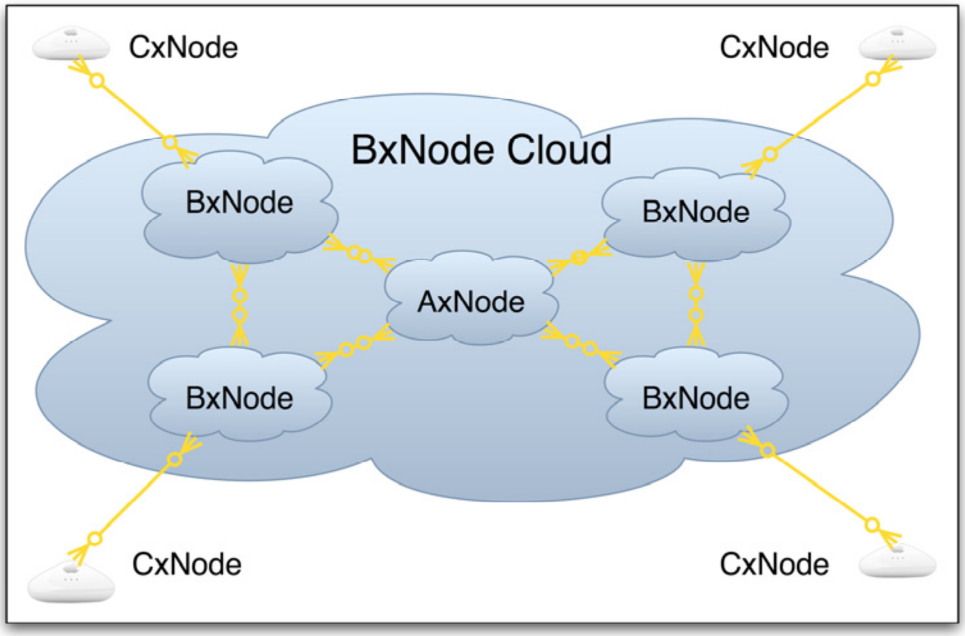


Fig 5.10 – AxNode [AxS]

5.5.2 Bay Area Research Wireless Network (BARWN)

BARWN is based in the San Francisco bay area. Unlike the Seattle Wireless project, BARWN is not an attempt to cover the entire San Francisco bay area with a wireless network. Its aim is simply to create a backbone that can be connected to in any way and that has no service restrictions [PP].

The unrestricted service approach is one of the prime reasons BARWN is being built. With so much downstream bandwidth available in the bay area either via DSL or cable Internet, users have no problem with downstream bandwidth limitations. However, upstream connections are capped or ports are closed, severely limiting functionality. BARWN's goal is to provide a stable infrastructure and organization and deliver unrestricted high-speed information over the "last mile" to consumers and public services in the San Francisco bay area, including the police and fire protection services [PP].

There are only a few backhaul connections within the BARWN. They use conventional Wi-Fi equipment equipped with directional antennas to create the long-range backhaul links between the many hills that dot the San Francisco bay area. These backhaul links are the simple backhaul connection topology defined in section 5.2.

5.5.3 Southampton Open Wireless Network (SOWN)

SOWN differs from BARWN considerably. While BARWN only aims to provide the backhaul connectivity needed for a wireless MAN, SOWN aims to provide a completely free-to-use wireless network in Southampton, UK [SHP]. The primary goal of the network is to create a wireless backbone across all of Southampton, as well as have truly pervasive coverage everywhere while encouraging community spirit. SOWN intends to achieve truly pervasive coverage by encouraging everyone to open up their access point to others [WiS05].

A key difference between SOWN and Seattle Wireless is that SOWN features security by using 802.1x authentication [SHP]. In addition to security features, SOWN also allows clients to fully roam from one point of access to another. Roaming is achieved by using a central register called a mobile location register (MLR); the access points are also forced to run an application that facilitates the mobility and interaction with the MLR [STM].

Although SOWN states that the network is a full mesh, its current size does not allow for any true mesh features. The current SOWN network has only four nodes and is connected in a line fashion (Fig 5.11) [STP].

5.5.3 Southampton Open Wireless Network (SOWN) - Continued

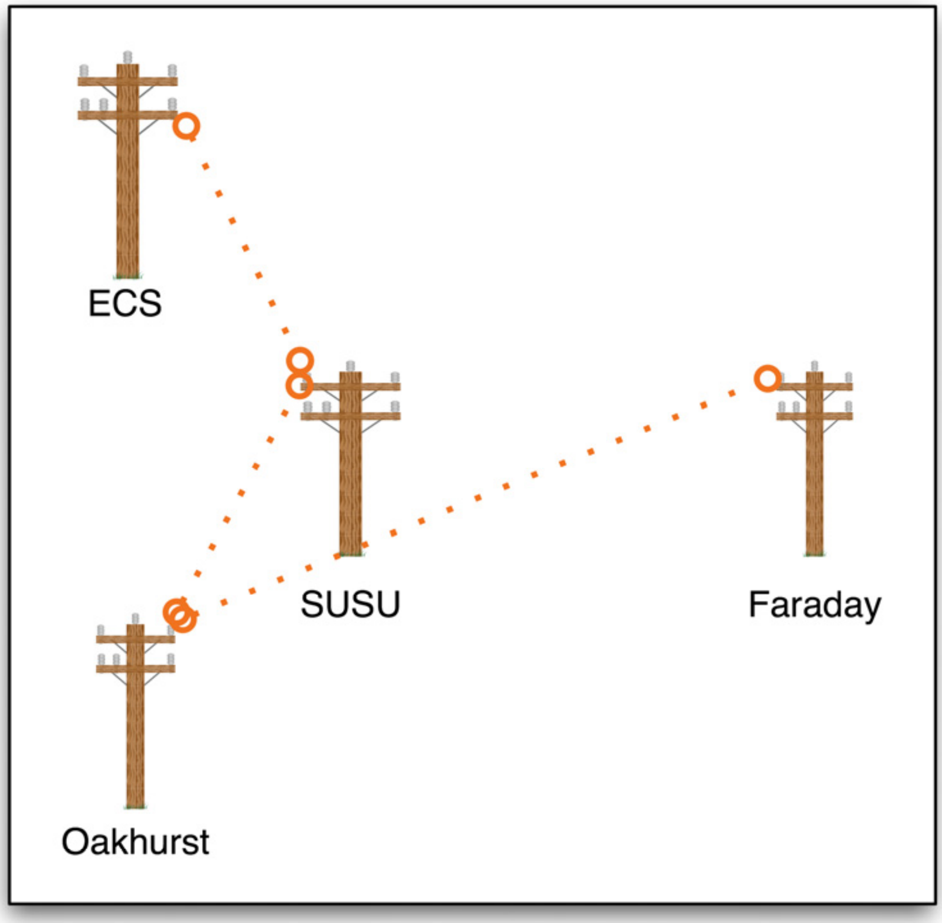


Fig 5.11 – SOWN topology [STP]

Disadvantages of SOWN are:

1. Once the SOWN scales, the throughput will decrease considerably due to the mesh topology.
2. Currently the line structure employed can result in large segments of the network failing if a single link fails.
3. The central repository that facilitates mobility and security creates a central failure point.

5.5.4 Johannesburg Wireless User Group (JAWUG)

JAWUG is a group of private citizens that aim to connect groups of computers together across the Johannesburg area. More specifically, they intend to do so using 2.4 GHz equipment. The choice of the 2.4 GHz band means that JAWUG is limited to 802.11b- and 802.11g-based equipment [JFP].

JAWUG, like Seattle Wireless, defines custom node types. The three basic node types JAWUG defines are [JNT]:

1. BasicNode.
2. TransitNode.
3. BackboneNode.

BasicNode is, as the name implies, very basic, and is reminiscent of a client in the Seattle Wireless network. It is essentially a wireless connection to any other point in the network. Any device operating in the 2.4 GHz spectrum is allowed, including PCI, PCMCIA and wireless routers. In addition to the wireless access device, an antenna and necessary cables are also required [JBN1].

The second node is called a TransitNode. It is essentially a BasicNode but with *n* possible other connections to other nodes (where $n > 1$). JAWUG expects that a person will start out with a BasicNode and have their node evolve to a TransitNode [JTN].

The third and final type of node in the JAWUG network is a BackboneNode. A BackboneNode is an essential part of the JAWUG network, primarily because it performs routing functions as well. Thus in essence a BackboneNode is simply a TransitNode with routing functionality added [JBN2].

The disadvantages of the JAWUG network are:

1. Initial requirement of antenna equipment makes setup costs expensive.
2. No direct access available to clients using standard access equipment.
3. All links are restricted to 802.11b- or 802.11g-based equipment.

5.5.5 Bristol Wireless

Bristol Wireless is a co-operative set up to give people living within Bristol broadband intranet access using wireless networks. Bristol Wireless aims to create a digital environment built by the people of Bristol for the people of Bristol. It also aims to introduce profit-free broadband Internet access that would facilitate, amongst other things, distance learning and video communications [BAB05].

Joining Bristol Wireless requires either any 802.11b or 802.11g wireless device. For a simple one-PC network Bristol Wireless recommends a PCI wireless card along with a suitable antenna. Within a multi-PC environment a wireless network bridge is recommended instead of a PCI wireless card [BJT05].

Bristol Wireless states that the initial network ran on a 802.11b network, with the effective bandwidth at approximately 6 Mbps. Currently the network deploys 802.11g hardware that has a theoretical bandwidth of 54 Mbps, more than enough to stream audio and video over the network [BNS105], indicating that 802.11g might be better suited to multimedia-rich or bandwidth-intense applications than 802.11b.

Bristol Wireless does not feature any form of security, but encourages users to take the same precautions as they would when using the Internet [BNS205].

Building an access point that provides a service to clients is very similar to the hardware requirements for a simple multi-PC environment. While both access provider and client have a Linksys WRT-54G wireless router as the recommended access point, the main difference is that an access provider features an omnidirectional antenna with enhanced routing capabilities and the client uses a directional antenna instead of an omnidirectional one [BNH05]. An important difference is that unlike previously discussed networks, Bristol Wireless seems to closely control the positioning of new access points. The reasoning behind the monitoring is that with the use of omnidirectional antennas the placement of unnecessary access points would degrade performance [BBN05].

Bristol Wireless has conducted tests and recommended that the http and ftp protocols be used to transfer files. Although no protocol is restricted, the use of the SMB and NFS networking protocols are discouraged as they are not very good for the network's overall health [BWP05].

5.6 Node Types of Current Wireless MANs – Comparison

In section 5.5 five different wireless MAN topologies were reviewed. All differ greatly in topology and design. Seattle Wireless and JAWUG define their own node types, while BARWN and SOWN simply use the structures reviewed in sections 5.2, 5.3 and 5.4.

The topologies have very few things in common, and at the same time few things differ. The following is a list of the aspects that the four wireless MANs have in common, or that differ:

1. Custom node design.
2. Node evolution or growth ability.
3. Specific hardware usage.
4. Logical topology.
5. Cost of node setup.
6. Ease of client access.
7. Security.
8. Mobility.

Table 5.2 summarizes the five networks reviewed, and compares them under the above eight aspects.

Table 5.2 - Wireless MAN summary

	Seattle Wireless	BARWN	SOWN	JAWUG	Bristol Wireless
Custom node design	Total of 5 nodes in the network, 4 are of a custom design and are called AxNodes, BxNodes, CxNodes and DxNodes.	Uses simple point-to-point connections with the primary goal of providing a backhaul connection. No custom node types are defined.	Claims to be a true mesh, but defines clients and routers both as nodes.	Total of 3 nodes are defined. All 3 are custom nodes, but there is no definition matching a client node as in Seattle Wireless.	Defines a client and an access point.
Node evolution or growth	Up to a point the natural expansion of a node is catered for, but an AxNode cannot serve any node type other than an AxNode or BxNode. This means that an AxNode cannot serve any clients. This may hinder the availability of service during the early phases of a network's formation. The limitation, however, allows for the	No growth or evolutions of nodes are defined. A node may serve as a point of access to multiple long-range links but the classification would remain the same.	No explicit node evolution, and clients are not allowed to become routers.	BasicNodes can become TransitNodes over time. TransitNodes can become BackboneNodes with the addition of a dedicated router.	Node evolution would simply require the client to exchange the directional antenna for an omnidirectional one.

	Seattle Wireless	BARWN	SOWN	JAWUG	Bristol Wireless
	AxNode to be specialized and function optimally as router.				
Specific hardware usage	Does not restrict users to any type of hardware or any standard. All wireless technologies are supported, including proprietary technologies. Open policy allows for points of access to be easily added, but the variety of possible technologies that might be deployed could make it difficult as clients might not have the specific technologies or a technology with the specific extensions. Currently promoting	Uses 2.4 GHz equipment. With end-users or clients that can directly access the backbone, the choice of technology is no limitation. However, the need for LOS operation requires that both points of access be visible to each other. The terrain of San Francisco does not allow for LOS to be easily achieved.	Currently has a limited number of nodes, all based on 802.11 products operating in the 2.4 GHz ISM band. Routers are set up using conventional PC equipment.	Requires all nodes to use either 802.11b- or 802.11g-based equipment. The limitation makes it easier for clients to connect using sanctioned hardware, but the use of alternative technologies that may suit the desired goal is restricted.	Currently uses 802.11g-based networks.

	Seattle Wireless	BARWN	SOWN	JAWUG	Bristol Wireless
	802.11b in the hope that it will become the default technology.				
Logical topology	Hybrid	Backhaul point-to-point	Mesh, actual topology currently a line formed out of multiple point-to-point connections.	Mesh	Hybrid
Cost of node setup	Open nature allows for any client hardware to be used at the client's desired cost level. Exotic access point technologies may require expensive client hardware. When coverage depends on expensive hardware, the client may have no option but to buy the expensive equipment.	The use of ISM equipment makes for low-cost installations, but over great distances the cost of suitable antennas and adequate cabling might increase cost.	The use of 802.11-based equipment within node construction allows for equipment to be cost-effective and easily available. The hardware used in the current routers is retired workstations and was available relatively inexpensively.	Use of 802.11-based equipment decreases costs, but the required antennas and cables increase costs.	All equipment used in node construction benefit from reduced cost due to standardization and conformance to IEEE specifications of the equipment used.
Ease of client access	Client equipment functions as with usual client access	Client access not allowed.	Clients do not require dedicated software to roam or	No direct client access is provided; direct access to	Direct access by clients is not possible, but.

	Seattle Wireless	BARWN	SOWN	JAWUG	Bristol Wireless
	points; this makes access to Seattle Wireless very easy.		access SOWN, which makes for easy access, similar to Seattle Wireless. However, security measures require the client to be able to authenticate using 802.1x. Obtaining rights to access the network may also be difficult.	other distant nodes is encouraged.	
Security	No security is enforced. Providers are not limited and can provide security on their own.	No implicit security. LOS makes signal interception difficult.	Use of a central 802.1x authentication server.	No security.	No security.
Mobility	No mobility.	No mobility.	Mobility is allowed using dedicated software at the routers and a centrally located database.	No mobility.	No mobility.

5.7 Custom Wireless MAN Topology

Designing a wireless MAN that features all the advantages mentioned in 5.6 is nearly impossible. An example of this is Seattle Wireless's open policy on technology usage. Seattle Wireless imposes no restriction on the possible technologies that can be used. While this open policy makes it relatively easy for any person wishing to add a node, it makes it difficult for a client to have all the possible wireless technologies that will be required to access the entire network. Another example is SOWN security. SOWN offers a level of security that no other wireless MAN reviewed offers. The level of security does come at a price, however; registration to the network is required, and a suitable server has to be in place that controls security and access. The need for an authentication server also places strain on a certain point of the network as well as a central point of failure. In a wireless MAN access should be easy and there should be no central point of failure that can bring the entire network down. Bristol Wireless does not feature explicit security but does mention that users should take steps similar to those they would take while using the Internet.

The natural evolution of a network is also important. Like wired networks, a wireless network will also be able to grow at and support an acceptable rate of change [HMC91].

Clearly it is impossible to achieve all the desired advantages and eliminate all the disadvantages. A hybrid topology called the "Benade Wireless MAN Topology" is presented that results in an even matched ratio of advantages to disadvantages.

The nodes defined are:

1. Client node.
2. Access node.
3. Transit node.

4. Super-transit node.
5. Backhaul node.
6. Security node.

The first node of importance is a client node. A client node resembles the clients within Seattle Wireless and is simply any Wi-Fi-compliant client. A client node will access the network like it would any access point. Addressing will be automatic via a DHCP server in the access point to which the client node connects.

The access node resembles a DxNode within Seattle Wireless. It is any Wi-Fi-compliant access point. An antenna (most likely omnidirectional) is required to allow for larger coverage of the surrounding area. The access node will also serve as a DHCP server and allocate addresses automatically within the possible range of addresses. Geographical aspects such as coverage area and population density will determine the range of addresses available to the access node. The relationship between client node and access node is represented in Fig 5.12.

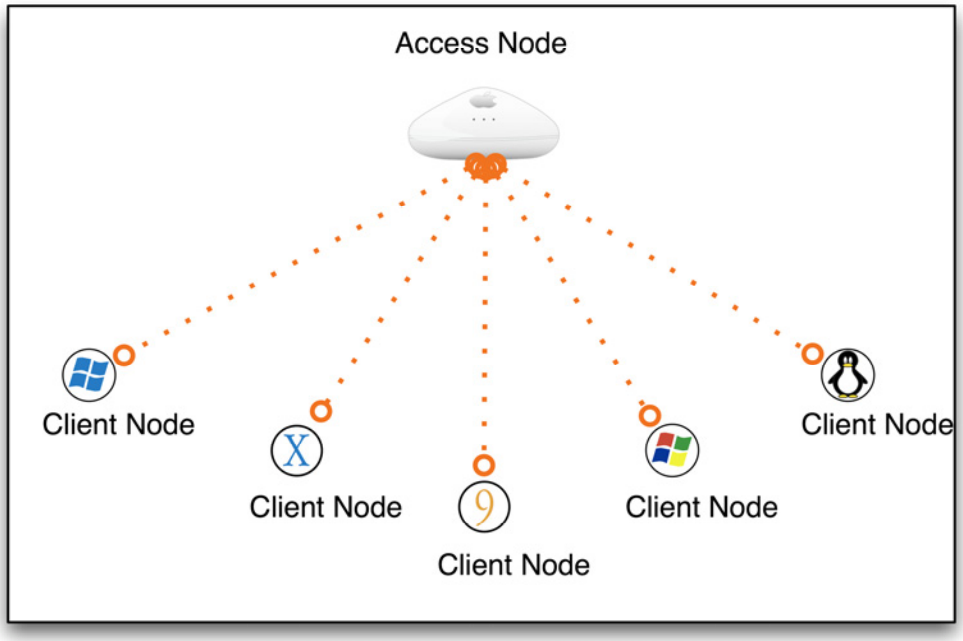


Fig 5.12 – Relationship between client nodes and access nodes

A transit node is a completely independent node with its own radio interface. It connects to one other transit node by using high gain directional antennas. A transit node may also connect to an access node, but the connection will have to be direct or over an Ethernet connection on the same premises. Wireless links are not permissible. While a single classification or node type is warranted, the ability of an access point owner to provide access to surrounding areas is not forced and purely the owner's choice when using two distinct node types. A transit node may in effect be connected to any number of client nodes, but only if the transit node is connected to the client nodes via a direct connection to an access node. In essence a transit node simply serves as a long-range connection from a single person or multiple clients via a client node to another transit node or super-transit node, and forms part of the geographical (geo) cloud. The address to a transit node is based on the geographical location of the node (Fig 5.13). Transit nodes are comparable to bridges, gateways or routers in traditional wired networks. If the node features routing capabilities as well as the ability to deal with addressing, it strongly resembles a router. Without routing functionality a transit node would represent a bridge within a wired network [HMC91].

5.7 Custom Wireless MAN Design - Continued

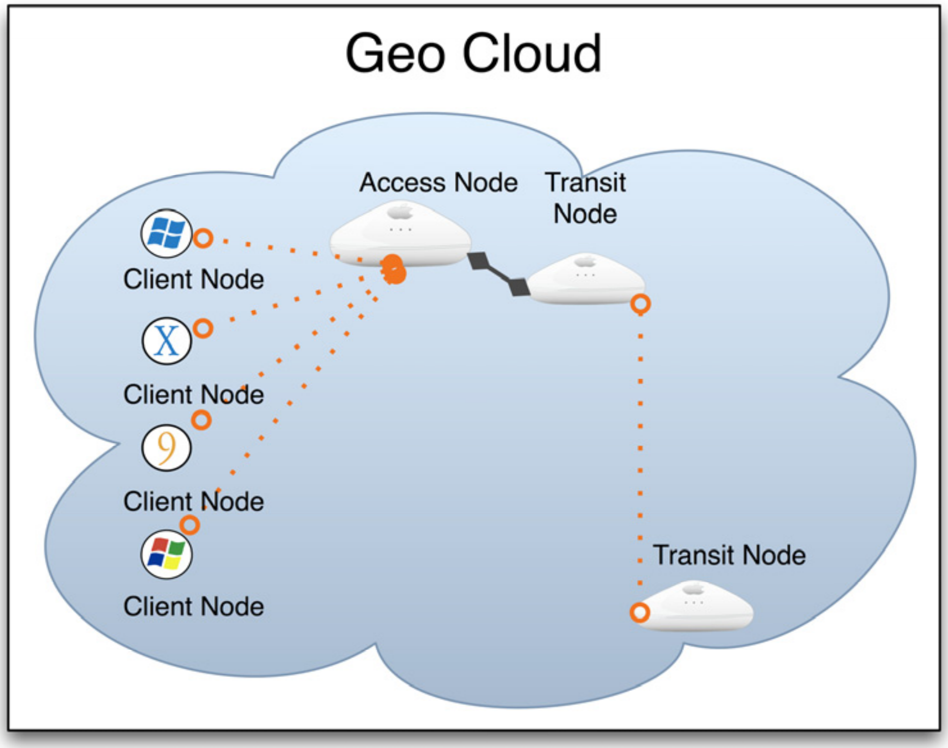


Fig 5.13 - Transit node and a geo cloud

A super-transit node is an enhanced or evolutionary version of a transit node and can feature an unlimited number of wireless interfaces, resulting in a lower bound of two other transit node connections. Similar to a transit node, a super-transit node can connect to a single access node, but it can also connect to any number of access nodes as well as any number of other transit nodes. A super-transit node should, due to the sheer number of wired and wireless interfaces, also have routing capabilities between the client nodes and the transit nodes, respectively.

A backhaul node serves not only as the backbone connection between one geo cloud and another, but also as a security border to a geo cloud. To serve both functions a backhaul node would need to be equipped with the necessary technology to serve as a backbone connection, but also feature a firewall that protects the geo cloud from any attacks from the other geo clouds (Fig 5.14).

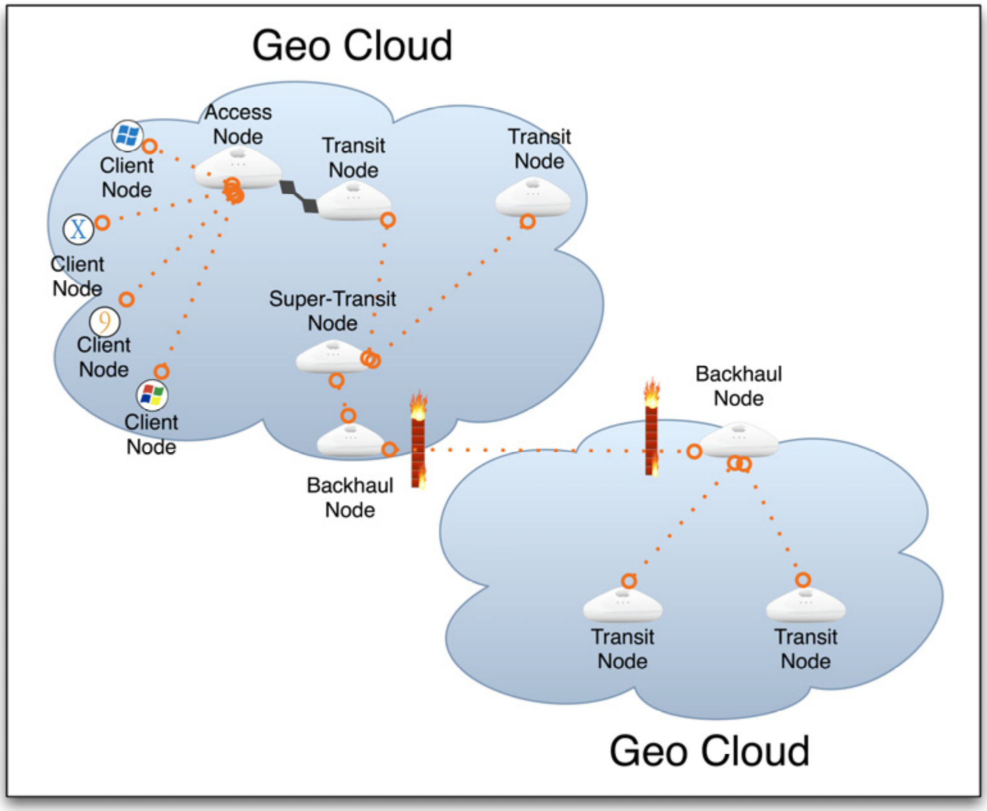


Fig 5.14 – Backhaul nodes and connection through firewalls

The final node is the security node. Only a single instance of a security node is found within a geo cloud. The choice of authentication method is left to the managers of the geo cloud and its presence is not compulsory or required (Fig 5.15).

5.7 Custom Wireless MAN Design - Continued

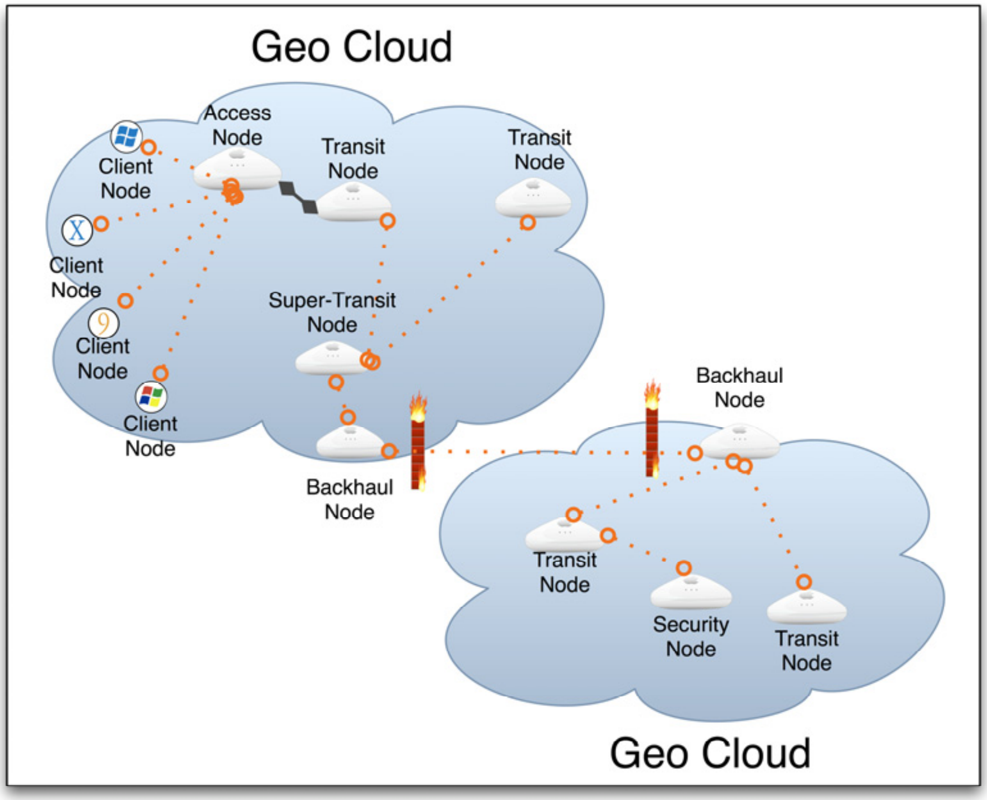


Fig 5.15 - Security node

The resulting topology resembles a large number of mini mesh networks interconnected via backhaul nodes that serve as the backbone that interconnects the mesh networks (Fig 5.15). While this topology does feature optional security with tightly controlled borders and has few restrictions on the use of technology, it does have a few disadvantages. The disadvantages are:

1. Single backbone connections between geo clouds may become congested and become a bottleneck to performance.
2. The formations of geo clouds have a strong relation to geographical features, but geographical features for the physical region spanning cloud may be restrictive to wireless networks.
3. Optional security creates the need for authentication and also central points of failure.

4. Some geo clouds may not enforce security and may create entire un-trusted geo clouds. Neighbouring clouds may enforce security and require all clients to be trusted. The policy of required authentication may restrict users from un-trusted clouds from services requiring trusted or authenticated clients.
5. Enforcing the use of Wi-Fi at client level may restrict the use of future technologies such as WiMAX.
6. Central management for a geo cloud is required but over a large population this may be difficult.

5.8 Conclusion

In this chapter three basic networking topologies, some important criteria as well as a few advantages and disadvantages were reviewed.

Clear similarities between mesh networks and the generic wireless MAN were also illustrated. It was also illustrated through the MIT Roofnet example that mesh networks in their current form cannot scale well and as a result true wireless meshes covering great distances will also scale badly. This makes a WMN topology inadequate for use in a wireless MAN.

A review of five existing wireless MAN topologies indicated that custom or hybrid designs are used as topologies for current large wireless MANs, but even with custom designs the particular network still has disadvantages. Even though a topology is of a custom nature it features the three types of topologies introduced in the beginning of the chapter. This indicates that even though they are custom topologies, fundamentally the three basic types of topologies are relevant in the design of a network.

A custom topology was presented that attempted to overcome a few limitations of the five existing networks but was not problem-free.

No perfect topology exists for something as dynamic as a wireless MAN. Hybrid topologies have to be deployed with the hope of creating a scalable, secure, reliable and affordable network.

This chapter presented the Benade wireless MAN topology to illustrate that hybrid topologies offer a better set of required features but still are not a perfect solution.

Chapter 6 – Node equipment requirements

6.1 Introduction

In Chapter 5 a variety of possible topologies for a wireless MAN were considered. All the nodes naturally used some sort of wireless interface. The construction of these nodes usually also required some sort of antenna assembly and appropriate cabling along with the wireless interface.

In this chapter basic antennas are reviewed, as well as common antenna types for the 2.4 GHz ISM band.

Additionally a review of cable types, their suitability for a specific frequency and application, as well as the connecters that connect to the cables, access points and antenna assemblies will follow.

6.2 Calculating Range

In Chapter 3, sections 3.4.2.1 to 3.4.2.3, the basic frequency propagation principles were discussed. Taking the discussion into consideration, the next logical question given knowledge about signal loss is how far a signal will be able to travel under certain conditions.

Formulae 3.3 and 3.4 have a variable *r* representing the range from a transmitter. Attempting to solve *r* will indicate the distance a signal can travel given certain characteristics. However, before calculating *r*, an unknown variable still exists. *L* represents the total loss, and can be set equivalent to the link margin.

In addition to environmental aspects mentioned in 3.4.2.1 to 3.4.2.3 the quality of the hardware also determines the distance a signal can travel. The quality can be represented as the link margin.

The link margin and in effect the quality of the hardware used can be determined by the following four factors [Spu04]:

1. Transmit power (TX_{power}).
2. Transmit antenna gain ($TX_{ant\ gain}$).
3. Receive antenna gain ($RX_{ant\ gain}$).
4. Minimum received signal strength or level (RSL).

The link margin is represented in formula 6.1:

$$L_{margin\ =}\ TX_{power} + TX_{ant\ gain} + RX_{ant\ gain} - RSL$$

Formula 6.1 – Link margin [Spu04]

The link margin factors can be determined from the transmitter manufacturer’s datasheet as well as the receiver’s datasheet. The RSL can be many values, as each data rate will have a different RSL. In most cases to achieve a basic signal, the lowest data rate RSL will have to be maintained.

Using formula 3.4 in conjunction with formula 6.1 it is possible to have different ranges at different connection speeds. Higher speed connections have lower RSL values, while lower speeds have higher RSL values, meaning that if a signal does not have adequate range, a lower speed could be chosen instead.

6.3 Antenna Principles

In section 6.2 a formula was presented that would allow the distance a signal can travel to be calculated. When using formula 6.1 and formula 3.4 in some cases the range is not adequate for the desired speed, so antennas are commonly used to increase range to or beyond desired levels.

Firstly, what needs mentioning is that antennas do not enhance a signal, they simply focus available signal [Fli2a]. A real-world example of this focusing is a flashlight. In natural environments a small light will not produce much light over great distances, but in a flashlight the light is simply focused and can produce greater amounts of light over greater distances; the primary difference is that the light is focused over a narrow beam [Bes02].

In the example provided in the previous paragraph the light bulb produces either a faint light in all directions or a very focused light in a specific direction. While these two options might be good enough for flashlights, the limited number of options is not suitable for wireless antennas. Fortunately there are a variety of ways to focus radio signals, all with different levels of focus.

The different levels of focus from the different types of antennas result in different characteristics for each antenna type. Some of these characteristics include:

1. Gain: The amount of signal gained in the direction of focus (measured in dB) [Bes02].
2. Impedance matching: Energy is transferred from the transmitter via the interconnecting cable to the antenna. For the most effective transfer of energy the transmitter, cable and the antenna have to have the same impedance. In some cases the antenna has different internal impedance and requires internal transformation via circuitry, resulting in the loss of energy [tec].
3. Voltage standing wave ratio (VSWR) and reflective power: VSWR indicates the quality of the impedance match. A VSWR of 2.0:1 or less is desired [tec].
4. Decibels: Decibels (dB) is the accepted way of measuring the loss or gain in an antenna system. Decibel values can be used throughout a complete antenna system, as they represent not only gain but also the loss and can be added as well as subtracted from each other. The formula 6.2 can be used for calculating dB:

$$\text{dB} = \log(\text{Power})$$

Formula 6.2 – Calculating decibel values [tec]

Using the formula provided above a relation between dB and power output can be seen. Every time the dB increases by 3 dB, the effective power doubles. The reverse is also true, meaning that every time the power is halved, the dB value is decreased by 3 dB [tec]. dB is used to indicate the ability of an antenna to focus the energy into a specific area or space. The relationship means that if a gain of 3 dB is experienced, the power in the field or space is doubled, and in effect also the range.

5. Polarization: This is the direction of the electrical waves transmitted by the antenna. A variety of options are possible, including vertical or horizontal. The important aspect when considering polarization is that with certain polarizations the receiving antenna has to be of the same polarization to be able to receive the signal correctly [Fli2a].
6. Radiation patterns: These patterns represent the relative field that is generated in different directions by the antenna. They represent not only the field that will be generated while transmitting, but also the field where reception will be enhanced [tec]. The fact that reception and transmission are enhanced means that an antenna does not need its exact match at the other end of a long-range link; the outer limits of the radiation pattern only need to overlap. This implies that a mobile client does not need any form of visible antenna as long as the mobile client functions within the radiation field generated by the antenna.
7. Beamwidth: The angle over which approximately 90% of the gain can be found. Fig 6.1 represents a 3° beamwidth. Beamwidth can be measured in the horizontal and vertical fields.

6.3 Antenna Principles - Continued

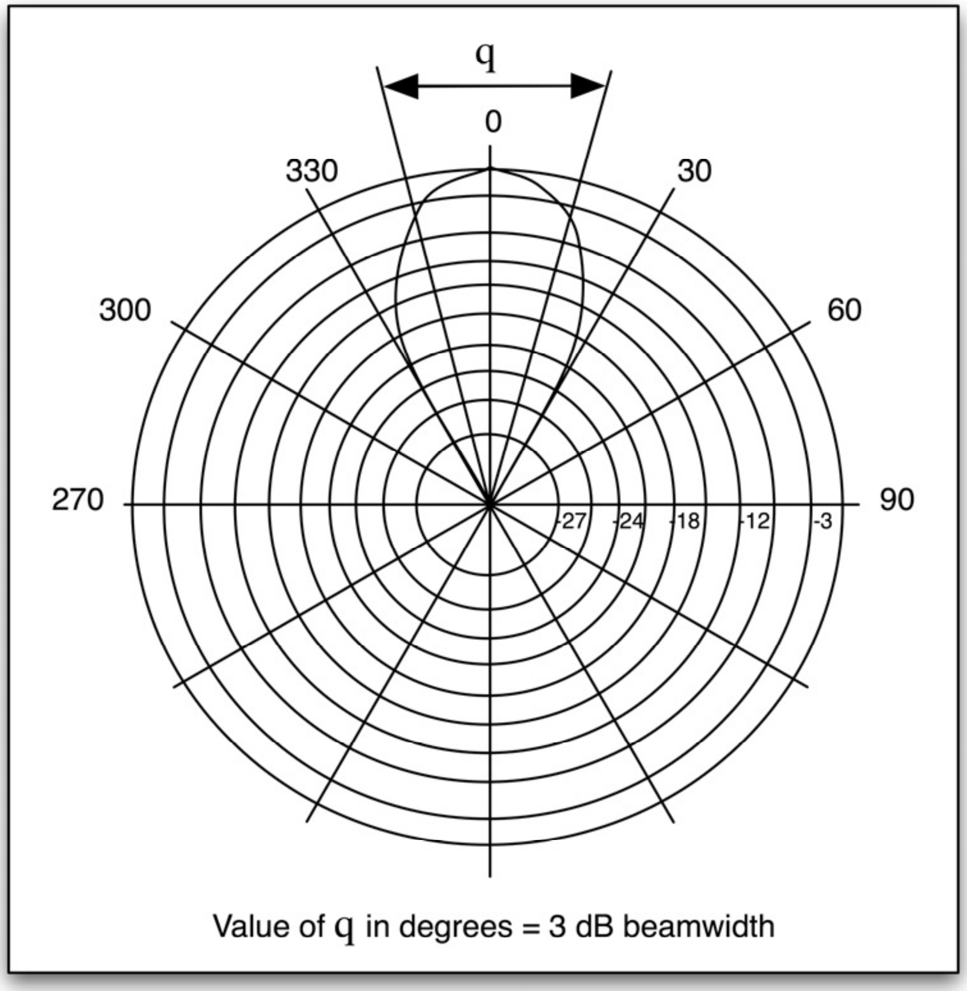


Fig 6.1 – 3° beamwidth [tec]

Another important aspect of any antenna is the frequency in which the antenna operates. Returning to the flashlight analogy, some sort of reflective surface is used to focus the light, but the reflective surface might not reflect all spectrums of light. Wireless antennas are similar. Antennas are designed to focus only a specific range of frequencies, meaning that an antenna offering a certain level of gain in one frequency may offer no gain in another frequency whatsoever.

Even though a reflective surface may be used, the surface may allow leakage and create lobes of signal at the back in addition to the front of the intended coverage area. The level of signal gain produced to the front and to the back is represented by the front to back ratio (F/B) [Bes02]. The F/B ratio is dependent on each antenna type and the manufacturer.

6.4 Common Antenna Designs

Most current consumer-deployed long-range wireless links are deployed using 802.11-based technologies, and as a result operate in the 2.4 GHz ISM band. Considering the many systems functioning in the 2.4 GHz ISM band, an adequate understanding of basic antenna principles can be achieved by understanding principles of 2.4 GHz ISM antennas.

The four most popular types of antennas used are [Fli2a]:

1. Omnidirectional antennas.
2. Sector antennas.
3. Yagi antennas.
4. Parabolic dish antennas.

Poynting manufactures and distributes antennas locally in South Africa. As most antennas feature unique specifications, an actual antenna needs to be used to review and illustrate the different concepts. Considering Poynting's experience in the local market, its products make ideal candidates for analysis.

Before comparing and reviewing the four antenna types, a reference standard is needed. Commonly the theoretical isotropic antenna and its radiation pattern are used to serve as a reference [Bes02].

6.4.1 Isotropic antenna

An isotropic antenna theoretically radiates signal equally into every direction and in effect creates a true sphere (Fig 6.2).

An isotropic antenna would have directivity or gain of 0 dB because it radiates into all directions. The comparison with an isotropic antenna means that the directivity and gain would be the same if the antenna were 100% efficient, but in reality wireless antennas are efficient in the range of 85% to 95%.

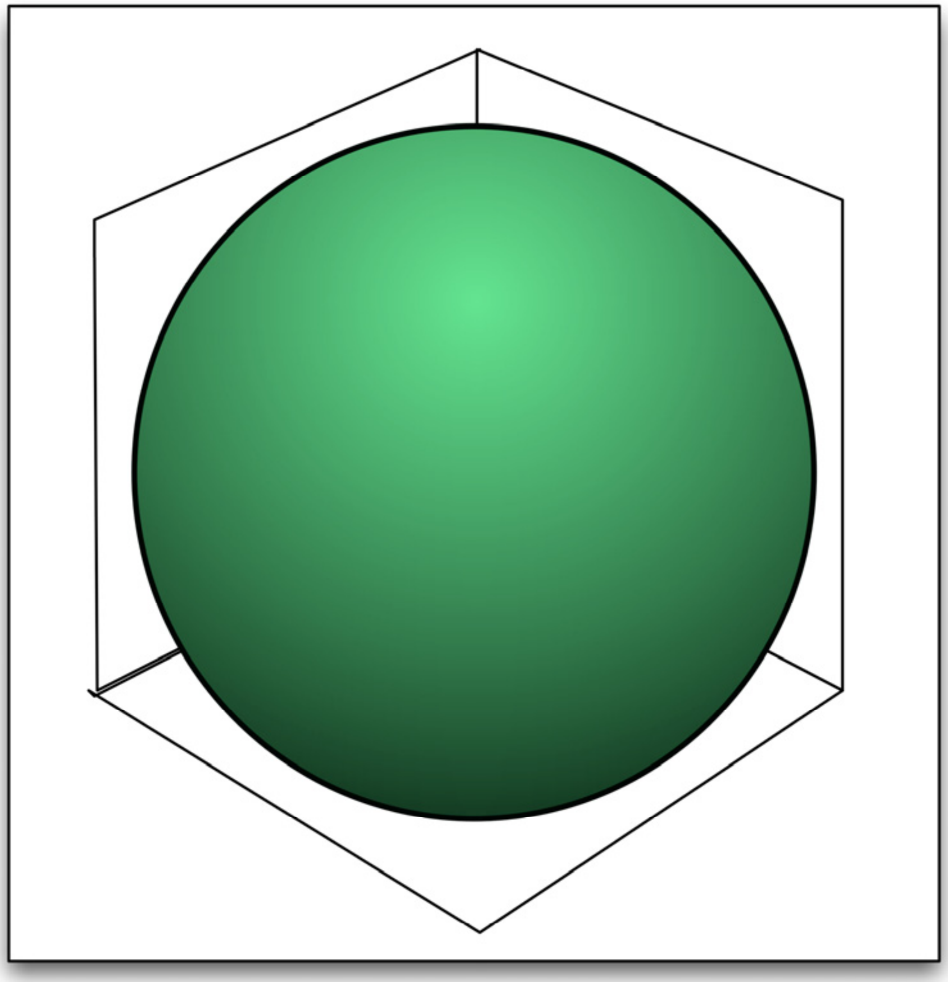


Fig 6.2 – Three-dimensional radiation pattern of an isotropic antenna [Bes02]

6.4.2 Omnidirectional antenna

Fig 6.3 is an example of an omnidirectional antenna.

Fig 6.3 – 3com 4 dBi omnidirectional antenna [3Co]

Omnidirectional antennas are used to create increased range within a 360° field, which would seem to match an isotropic antenna. The shape of the signal, however, is not a full sphere; it is in this difference that an omnidirectional antenna receives its gain. The way omnidirectional antennas receive their gain over an isotropic antenna is by flattening the signal [Fli02]. The resulting radio pattern resembles a doughnut for an omnidirectional antenna instead of a sphere for an isotropic antenna. The amount of energy transmitted remains the same, and while the vertical energy release is reduced with omnidirectional antennas, the excess energy available is now transmitted over the vertical plane, resulting in bigger coverage areas.

The characteristics of omnidirectional antennas allow for 360 degrees of reception but result in marginal gains. While an omnidirectional antenna provides a better signal in any direction, and in effect allows clients to function with increased signal in any direction, the increased coverage also results in more interference being picked up [Fli]. Increased coverage might bring previously unreachable stations within range. These newly discovered stations could increase interference and pose a possible security risk.

Poynting produces an omnidirectional antenna that is designed to operate in the 2.4 GHz to 2.5 GHz frequency spectrum. The antenna is targeted at hotspot deployments [Poy05].

Due to the large frequency range supported by the Poynting omnidirectional antenna, many of the characteristics mentioned in section 6.4 do not have single values and have a range of values for single criteria, this fact is summarizes in Table 6.1 .

Table 6.1 – Summary of the Poynting omnidirectional antenna

1. Gain	Max of 7.5 dBi, min of 6.5 dBi
2. Impedance matching	50 Ohm
3. VSWR	< 2.0:1, Fig 6.4 represents the VSWR levels of the Poynting omnidirectional antenna
4. Polarization	Vertical
5. Beamwidth – Horizontal	20°, Fig 6.5 represents the horizontal radiation pattern of the Poynting omnidirectional antenna
6. Beamwidth – Vertical	360°
7. Frequency	2.4 GHz to 2.5 GHz
8. Target deployment	Areas that need a marginally wider coverage area such as hotspots

Source: Poy05

6.4.2 Omnidirectional antenna - Continued

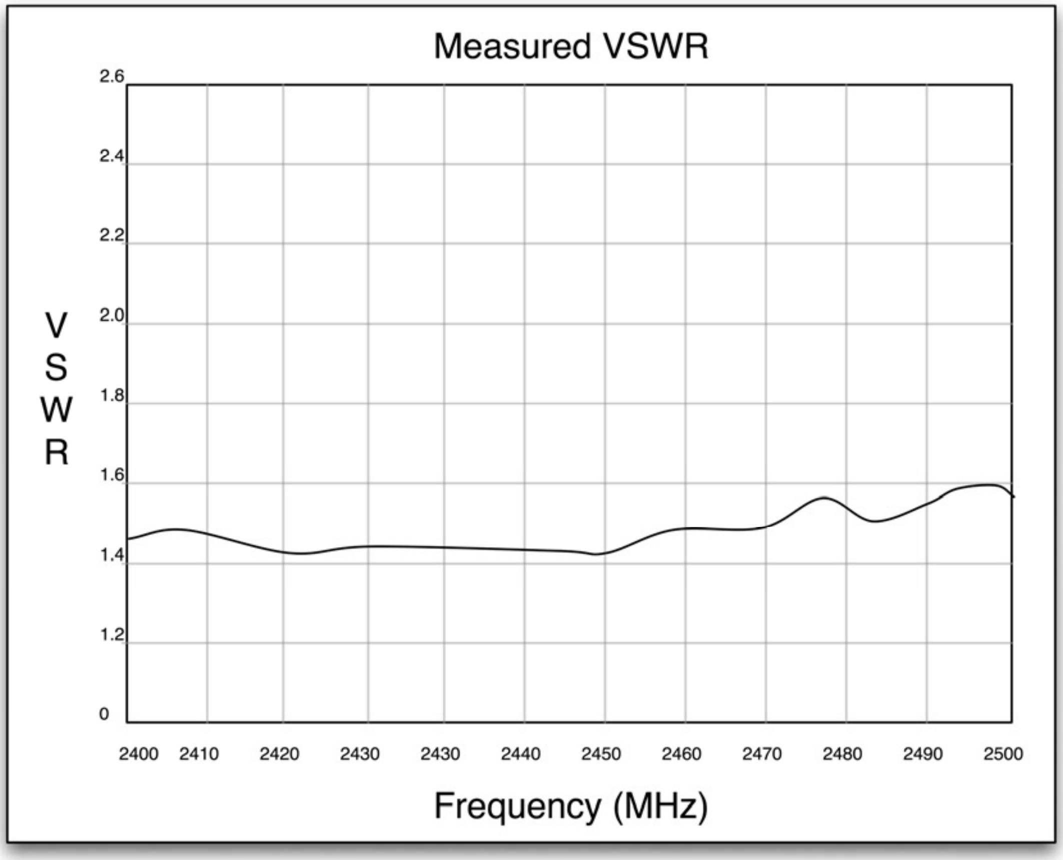


Fig 6.4 – VSWR of the Poynting omnidirectional antenna [Poy05]

6.4.2 Omnidirectional antenna - Continued

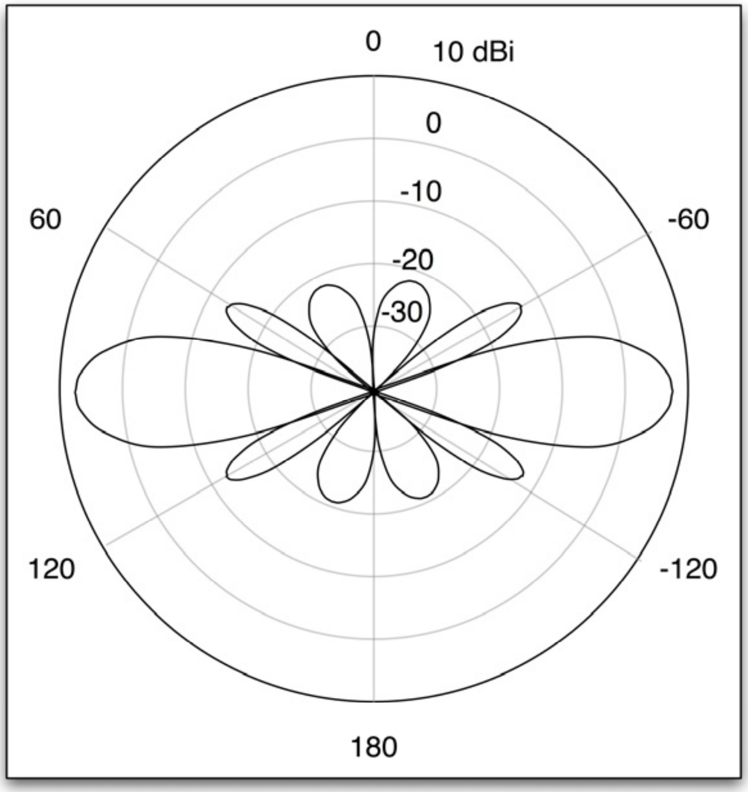


Fig 6.5 – Radiation pattern of the Poynting omnidirectional antenna [Poy05]

The Poynting omnidirectional antenna can serve as an ideal hotspot antenna, but only when placed above the level of the clients. The radiation pattern (Fig 6.5) indicates that the signal does travel downwards, and placing the antenna above the client would result in the efficient use of the antenna’s gain. Furthermore the VSWR (Fig 6.4) indicates that for most effective energy transfer the frequency used should be set below 2450 MHz. These are channels below channel 8 of the ISM band [otICSB99].

For deployment in a wireless MAN a Poynting omnidirectional antenna does not have much use. While coverage is increased, the limited increase in gain would not increase the range enough to cover a large enough area for a substantial number of users to be provided with wireless network coverage.

6.4.3 Sector antenna

Sector antennas increase gain even further than omnidirectional antennas. The tradeoff to achieve this higher gain is decreased vertical beamwidth. While omnidirectional antennas cover 360°, sector antennas cover between 60° (and sometimes lower) and up to a maximum of 180° [Fli]. The wide angle of coverage makes sector antennas ideal to cover large areas.

While isotropic antennas aim to create a full 360-degree signal in both vertical and horizontal fields, omnidirectional antennas flatten the signal and reduce the vertical field to achieve gain. Sector antennas go one step further and decrease the vertical beam and achieve even greater gain; the sacrifice is that the gain is in a certain direction only [Fli].

The shape of a sector antenna varies; some are flat panels that can be wall mounted, others are omnidirectional antennas cut through the middle [Fli]. Fig 6.6 and 6.7 illustrate two popular types of sector antennas.

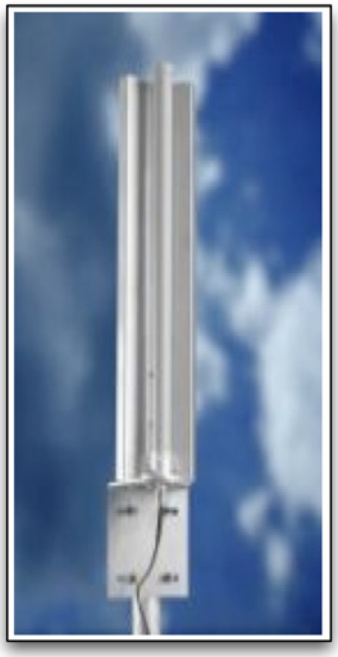


Fig 6.6 – Omnidirectional type sector antenna [Poy]

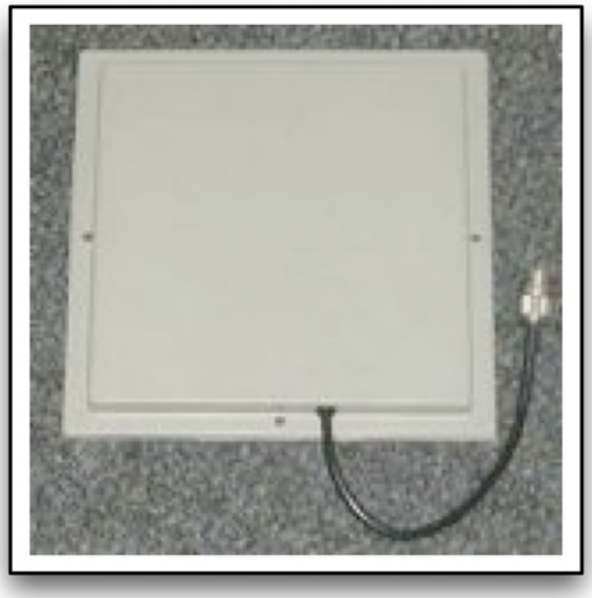


Fig 6.7 – Flat panel sector antenna [Poy]

Poynting produces a patch antenna with product code PATCH-A0006, functioning in the 2.4 GHz to 2.5 GHz frequency spectrum. The antenna is designed with base station-to-base station applications in mind. The antenna features a waterproof exterior, making it ideal for outdoor operation. Table 6.2 represents the characteristics of the Poynting patch antenna.

Table 6.2 – Summary of Poynting PATCH-A0006 sector antenna

1. Gain	Max of 13 dBi, min of 12 dBi (Fig 6.8)
2. Impedance matching	50 Ohm
3. VSWR	< 1.8:1 (Figure 6.9)
4. Polarization	Linear
5. Beamwidth – Horizontal	36°, Fig 6.10 represents the horizontal radiation of the Poynting patch antenna
6. Beamwidth – Vertical	36°
7. Frequency	2.4 GHz to 2.5 GHz
8. Target deployment	Larger range coverage than omnidirectional antennas, but without the need for a large beamwidth

Source: SA005

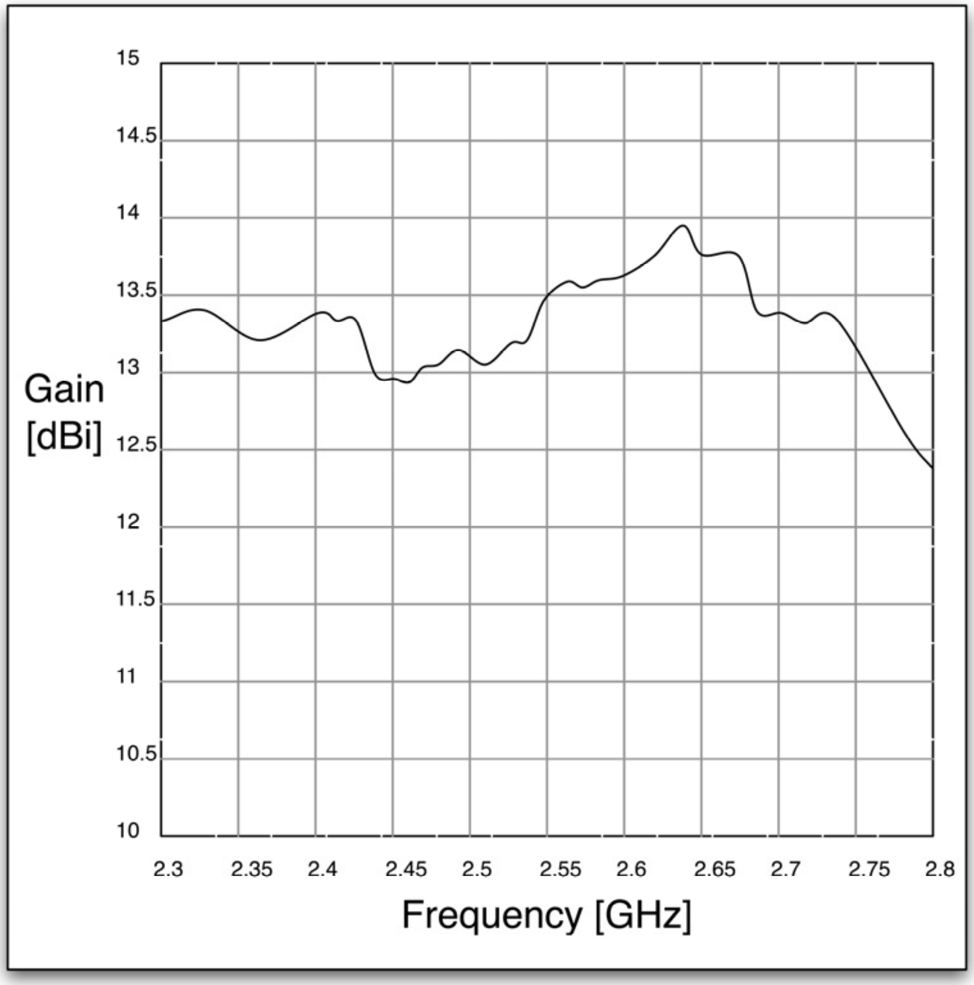


Fig 6.8 – Gain measured over frequency of the Poynting patch antenna [SA005]

Of interest in Fig 6.8 is the gain in the frequencies ranging from 2.4 GHz to 2.45 GHz, or the ISM bands. The gain of the Poynting patch antenna peaks at 14 dBi, but the gain in frequencies that the antenna will most likely be used for ranges from approximately 12.8 dBi to 13.4 dBi. To achieve maximum gain out of the Poynting patch antenna, the lower part of the ISM band will be used, meaning approximately the first five channels of WiFi equipment.

6.4.3 Sector antenna - Continued

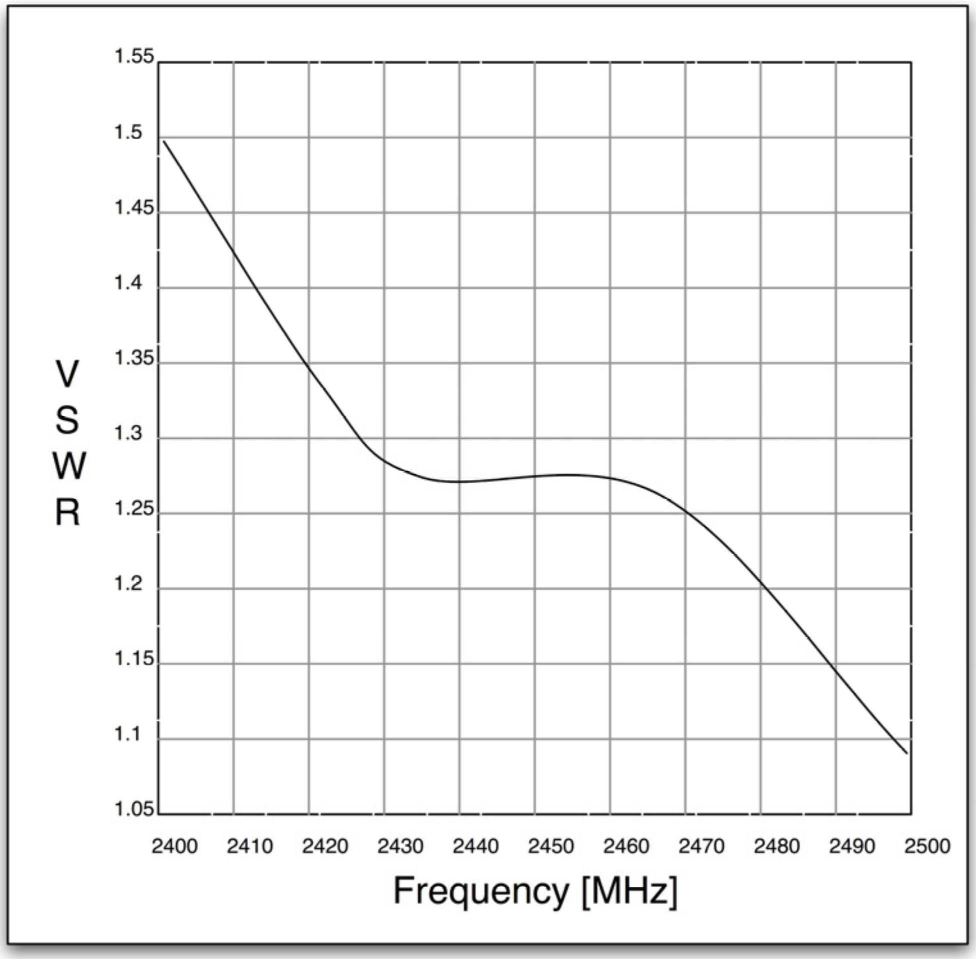


Fig 6.9 – VSWR of the Poynting patch antenna [SA005]

While Fig 6.8 indicates that the most gain is to be achieved over lower ISM frequencies, Fig 6.9 indicates that the most effective power transfer occurs in the higher frequency bands. However, VSWR levels are still well below the 2:1 levels.

6.4.3 Sector antenna - Continued

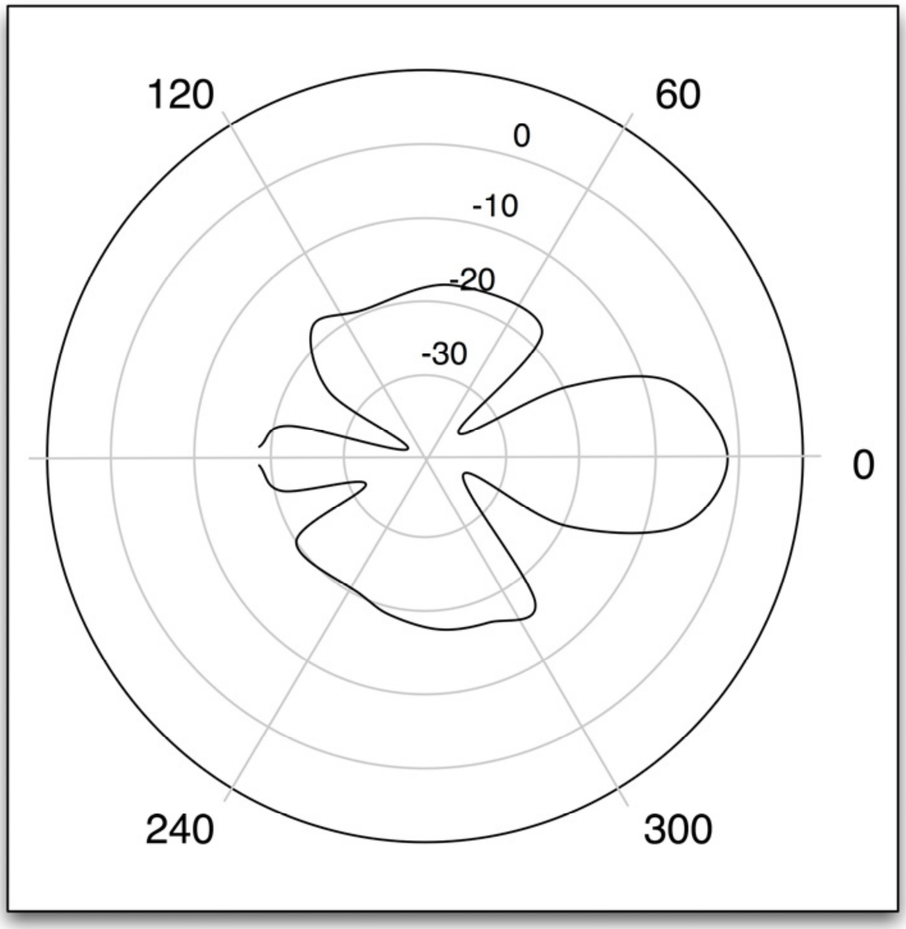


Fig 6.10 – Horizontal radiation pattern of the Poynting patch antenna [SA005]

While most patch antennas have a set beamwidth, Poynting also offers a sector antenna with a selectable beamwidth, either 180°, 120° or 60° [Poy]. The ability of an antenna’s beamwidth to be set offers great advantages; the most suitable beamwidth and gain can be selected for the application. In return for decreased beamwidth, increased gain allows for incremental deployments where requirements change over time and the antenna can be altered to adapt to those changes at no cost. Poynting also offers a patch antenna that features an integrated access point enclosure, eliminating any losses incurred by the use of cables [A0005].

6.4.4 Yagi antenna

Yagi antennas resemble television antennas (Fig 6.11) and offer beamwidth of between 15° and 60° [Fli].

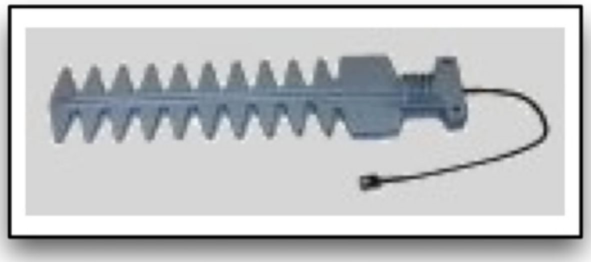


Fig 6.11 - Yagi antenna [Poy]

With Yagi antennas the more elements (or bars as depicted in Fig 6.11) added to the antenna, the bigger the gain, but the smaller the beamwidth [Fli]. The small beamwidth in conjunction with high gain makes Yagi antennas ideal for point-to-point connections [Poy]. Unlike sector antennas, Yagi antennas cannot be easily moved by wind and operate well outdoors, adding to their suitability for point-to-point connections.

Poynting offers a Yagi antenna that is designed to function as a wireless bridge or general point-to-point antenna. Table 6.3 represents a summary of the Poynting YAGI-A005 antenna.

Table 6.3 – Summary of the Poynting YAGI-A005 characteristics

1. Gain	Max of 13 dBi, min of 12 dBi (Fig 6.12)
2. Impedance matching	50 Ohm

3. VSWR	< 1.5:1 on frequencies between 2.4 GHz and 2.45 GHz, < 2.0:1 on frequencies between 2.45 GHz and 2.5 GHz (Fig 6.13)
4. Polarization	Linear
5. Beamwidth – Horizontal	44°
6. Beamwidth – Vertical	48°
7. Frequency	2.4 GHz to 2.5 GHz
8. Target deployment	Larger range coverage than omnidirectional antennas, but without the need for a large beamwidth

Source: YA005

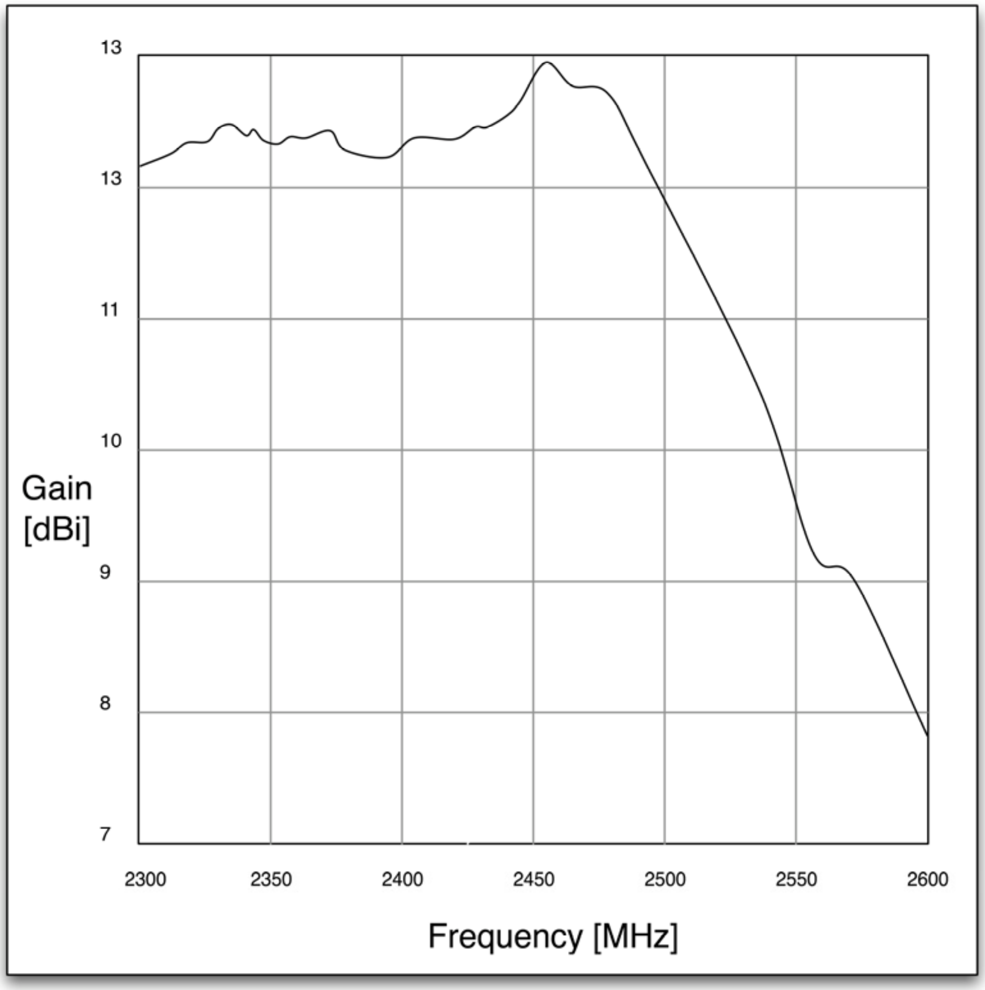


Fig 6.12 – Gain of the Poynting Yagi antenna [YA005]

Fig 6.12 clearly indicates a basic antenna principle stated in section 6.4. The principle is intended operation frequency. After 2500 MHz the gain of the Poynting Yagi falls sharply, clearly indicating that the antenna was not designed to operate in frequencies higher than 2.5 GHz. The antenna sees its highest gains in the upper ISM band, making the upper WiFi channels the best candidate for usage with the Poynting antenna.

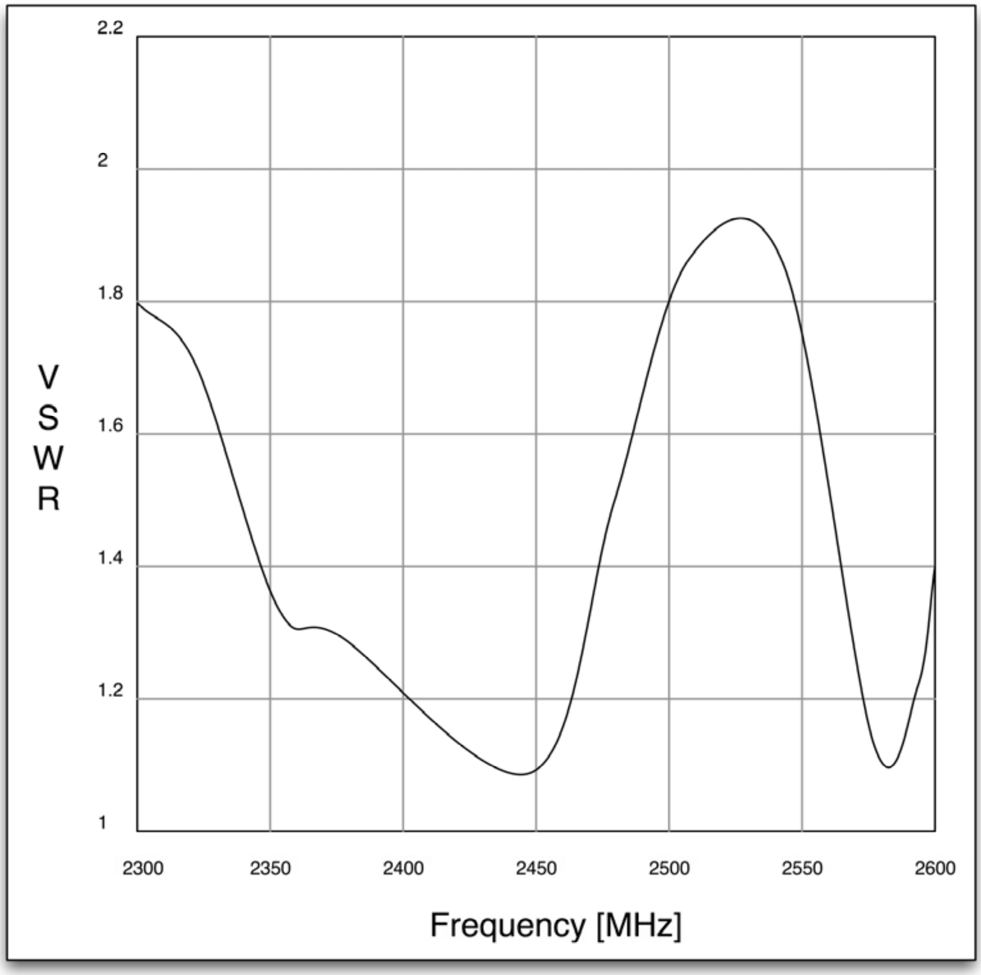


Fig 6.13 – VSWR of the Poynting Yagi antenna [YA005]

The low VSWR ratings in the higher ISM band illustrated in Fig 6.13 concur with the conclusion that the Poynting Yagi antennas are ideally used when set to function in the upper WiFi channels.

6.4.5 Parabolic dish

Parabolic dishes are the opposite of omnidirectional antennas; instead of attempting to cover the widest area possible, parabolic dishes attempt to achieve the greatest distance while sacrificing coverage area [Fli]. The ability of parabolic dishes to cover great distances makes them more ideal than Yagi antennas when used in the creation of long-range point-to-point connections [Poy].

Parabolic dishes consist of two components: the dish component acting as a reflector as well as the feed that acts as the transmitter. Poynting produces the feed connector used in parabolic dishes. Two different dishes are available to be used with the feed, and both options allow for different gain levels and effectively different ranges. The buyer has the option of which dish to use. The option to select the actual dish gives the deployer the ability to select the most suited dish for the target deployment [HA005]. Table 6.4 represents the different characteristics for the feed and two parabolic dish options.

Table 6.4 – Characteristics of the Poynting parabolic feed as well as optional parabolic dishes [HA005]

	Poynting feed	Feed with medium gain dish	Feed with high gain dish
1. Gain	Between 8.0 dBi and 9.5 dBi gain	Between 19 dBi and 21 dBi gain	Between 23 dBi and 25 dBi gain
2. Impedance matching	50 Ohm	50 Ohm	50 Ohm
3. VSWR	< 1.5:1	< 1.5:1	<1.5:1
4. Polarization	Circular	Circular	Circular
5. Beamwidth – Horizontal	Not given	Not given	Not given
6. Beamwidth – Vertical	Not given	Not given	Not given
7. Frequency	2.4 GHz to 2.5 GHz	2.4 GHz to 2.5 GHz	2.4 GHz to 2.5 GHz

8. Target deployment	Building-to-building connections, ISM-based point-to-point connections for wireless video transmission in the ISM band	Building-to-building connections, ISM-based point-to-point connections for wireless video transmission in the ISM band	Building-to-building connections, ISM-based point-to-point connections for wireless video transmission in the ISM band

Poynting does not provide the horizontal and vertical beamwidth, but other commercially available parabolic antennas are assumed to have beamwidth values in the range of 6° [Gas02]. With small beamwidth values of 6° parabolic dishes are not suitable for point-to-multipoint or large area coverage connections. Furthermore, antennas will have to be mounted very securely to ensure that weather conditions do not move the dish and possibly bring the entire connection down. The use of grid-based antennas instead of solid dishes can eliminate the effects of wind on the positioning of the antenna. In addition to weather influencing the antenna the initial setup of parabolic dishes is also complex. With small beamwidth values there is very little margin for error, and equipment such as a GPS and binoculars are often required.

6.5 Cables, Cable Characteristics and Connectors

Just like with antennas, the connector and cable types are also very important [Fli]. An example of this would be having an antenna that offers 18 dBi gain and a cable that loses 21 dBi. An example of cable loss would be LMR-400 cable that loses 6.8 dB signal every 30.48 meters [Gas02]. For this reason it is always recommended that the cable sets be kept as short as possible.

Most cables that are used in wireless deployments are coaxial cables. The basic construction of a coaxial cable is as follows:

1. Metallic central core acting as a conductor.
2. Insulation that protects the inner core.
3. Metal shield that shields the inner core from interference.
4. Outer layer that protects the metallic shield as well as the other cores from shock and impact.

Fig 6.14 illustrates the four points outlined above.

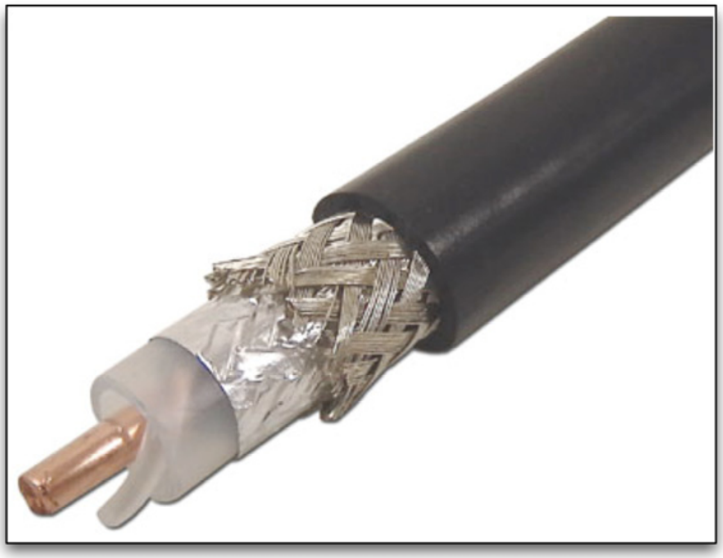


Fig 6.14 – Typical coaxial cable

To many people a cable is simply a wire and nothing more. Many do not realize that cables have to function in a wide range of harsh environments, including wide temperature variations, exposure to harsh chemicals, fluids and fuels. Ensuring that a cable is able to survive in the intended environment and function to the intended specifications is always a give and take, tradeoff situation. Optimizing one characteristic very often degrades another. It is, however, very important to ensure that all critical characteristics are present within a cable to eliminate potential flaws in the deployment of the cable [Sla97].

An example of characteristic tradeoffs would be cable targeted at a deployment within a factory. Such a cable would have to be resistant to impact and shock produced by large objects hitting the cable or being dropped on it. Making cables shock-resistant normally involves encasing the cable with either a thick metallic layer or a tough plastic casing that would reduce the cable's flexibility, making the cable difficult or impossible to use in a factory where flexibility is required [Sla97].

With a wide range of possible requirements the inexperienced wireless network deployer will have no clue what characteristics are important. Fortunately companies like Times Microwave Systems have considerable experience in the production of cables and have compiled a list of important criteria.

6.5.1 Cable characteristics

The important cable construction aspects that Times Microwave Systems set out are as follows [Tus04]:

1. Electrical criteria
    a. Frequency range.
    b. Attenuation (loss).
    c. Return loss (WSWR).
    d. Shielding.
    e. RF stability.
    f. Phase length.
    g. Power handling.
    h. Impedance.
2. Mechanical criteria
    a. Length.
    b. Flexibility.
    c. Flex life.
    d. Outer jacket or armour.
    e. Connector series.

   f. Attachment method.
3. Environmental criteria
   a. Operating temperature range.
   b. Operating altitude.
   c. Moisture resistance.
   d. UV resistance.

An ISM deployment is not a very complex deployment in terms of cabling, and does not require many exotic cable characteristics, but all characteristics are important to a certain extent. The next section discusses a few important characteristics of an ISM cable deployment, and creates a theoretical cable that would operate ideally in the 2.4 GHz ISM band with WiFi equipment.

Starting with electrical criteria, a cable would have to be optimized for the 2.4 GHz ISM band. It was indicated in Fig 6.12 that antennas do not offer equal gain over all frequencies, and cables are exactly the same. The upper limit of cable that is able to function without showing extreme loss of signal is called the cutoff frequency [Sla97].

Attenuation is the natural loss of the signal's amplitude as the signal travels through the cable. An ideal cable would offer the least amount of attenuation as possible to ensure that the maximum amount of energy is transferred effectively. Usually a cable is thickened to reduce the attenuation [Tus04]. The downside to the thickening is a cable that is less flexible and more expensive. Outdoor WiFi does not require a cable that is very flexible.

The VSWR is the amount of energy that is reflected back to the source. Similar to antennas, a 1:1 ratio is ideal, meaning that no energy is reflected. Ideally a cable for any assembly, not only ISM assemblies, would have a 1:1 VSWR [Tus04].

Impedance might seem the same as attenuation, but while attenuation is the natural degrading of a signal carried over a cable, impedance is the loss of signal because of imperfections in the cable. The imperfections can be classified under the following three types [Sla97]:

1. Line size transitions: Transitions within the cable or connectors will cause signal loss or other adverse effects.
2. Periodic discontinuities within the cable: Bad or low quality cables might, for example, consist of more than one metal. Different metals have different properties, and this in turn could adversely affect the signal.
3. Single-event discontinuities within the cable: Damaged cables may have damaged or broken cores, resulting in losses very similar to those found at weak connection points.

The length of a cable is also a critical consideration. Longer cables increase the likelihood of encountering imperfection and consequently loss of signal. Electromagnetic interference from external sources as well as increased impedance and attenuation also contribute to increased loss. Keeping the cable as short as possible is essential to minimize loss.

The flexibility of a cable only comes into play when the target deployment features a wide variety of curves or corners the cable has to go around. However, with ISM deployments the distance from the access point to the antenna is kept to a minimum to have minimal signal loss, and complex curves are avoided, mitigating the need for extreme flexibility.

LMR cables are produced by Times Microwave Systems, which is a very popular cable manufacturer for WiFi-based equipment [Fli]. Times Microwave, however, produces a variety of cables for many different wireless deployments based on many frequencies, not only ISM equipment deployments [TMS04].

Table 6.5 summarizes a few important characteristics of LMR cables that would very likely be used in a WiFi deployment.

Table 6.5 – Summary of important criteria of common LMR cables

Cable type	Diameter (mm)	Loss in dB/100 foot (30 meters) at 2500 MHz	Installation temperature range (°C)	Impedance (Ohms)	Cutoff frequency (GHz)
LMR-200	4.95	16.9	-40/+85	50	39
LMR-400	10.29	6.8	-40/+85	50	16.2
LMR-600	14.99	4.4	-40/+85	50	10.3
LMR-900	22.10	3.0	-40/+85	50	6.9
LMR-1200	30.48	2.3	-40/+85	50	5.2

Source: TMS04

It is clear given the information in Table 6.5 that thicker cables do in fact decrease the loss. What is of interest, however, is the sharp drop in cutoff frequency; while all the cutoff frequencies are above 2.4 GHz, the thicker low-loss cables almost become inadequate for 5 GHz ISM equipment, indicating that another type of cable might be needed.

6.5.2 Cable connectors

Connecters form a very important part of a cable assembly. They can have negative effects on the overall VSWR of the entire assembly.

The connector size should be as closely matched to the cable size as possible. The most adequate matching connector will have the same central connector diameter as the cable’s core diameter. When the cable core diameter differs from the connector core diameter, impedance is increased. A connector set often has different sizes of connectors on each end. The transition in size should be carefully chosen by the designer and electrical and mechanical elements should be considered [Sla97].

While it may seem that anyone wishing to use connectors has many things to consider, the choice and options are taken away from the deployer of WiFi networks. The access point manufacturers choose the connector they want, and inevitably force end-users to choose a certain set of connectors. Usually limited options are considered negative, but with cables this is a positive. Employers are not forced to have considerable knowledge about all the options. The limited options also allow for the few options to be optimized for lower loss, decreased cost and better overall quality.

Not all options are completely eliminated and a basic understanding of the basic types of connectors available is still needed. The most common connectors are [Fli2a]:

1. A Bayonet Navy Connector (BNC) is a quick-connect connector that became cheap and very popular with the death of 10base2. What is important to know is that BNC is not suited for 2.4 GHz use.
2. A TNC connector is a braided version of a BNC connector. It operates well up to the 12 GHz frequency and is frequently used with smaller high-loss cables.
3. An N connector is a large threaded connector found in many WiFi deployments. It is thicker than TNC, works well up to frequencies of 10 GHz and is ideal with thicker cables such as LMR-400.
4. UHF connectors look like a coarse-threaded version of the N connector. The comparable features allow for UHF connectors to be regularly

mistaken for N connectors, but UHF connectors are not designed for operation at microwave frequencies and should be avoided for use in all WiFi deployments.

5. The SMA connector is a very popular, small, threaded connector that works well up to 18 GHz. The small size, however, makes it impossible to use with SMA connectors that have larger low-loss cables.
6. The SMC connector is a smaller version of the SMA connector and is only suitable for very small, high-loss cables.

6.6 Conclusion

In this chapter the aim was to gain a more thorough knowledge of the basic concepts of antennas, cables and connectors that allow wireless networks to extend their range beyond that of the default hardware.

The quality of the actual hardware has a sizable influence when the range of an outdoor wireless link is to be determined. The required information is readily available from most manufacturers.

In proceeding to antenna principles, it was found that antennas are often used to enhance range, but that they do not increase the signal power, further indicating that the quality of the hardware is very important when attempting long-range connectivity.

One of the most important antenna characteristics was found to be gain. It was indicated that a gain of 3 dB would result in a doubling of the initial range, as would every 3 dB after that. Coupled with the radiation pattern and beamwidth characteristics, it was further indicated that gain does come at a price, usually decreased beamwidth, and that an understanding of the target deployment and antenna to be used is needed to adequately cover the desired range with a good signal.

Each antenna type has its own set of unique characteristics, and understanding the deployment and the use of an antenna is essential. Deploying an antenna simply because of its claimed gain is not advised; beamwidth may be inadequate for the large area coverage needed in a wireless MAN. Furthermore, an understanding of the radiation pattern will allow deployers to place and focus antennas in the best location needed for extreme long-range links.

Cables are used to connect the antennas to access points. A wide range of criteria were set for the design of a cable, but it was indicated that there would always be tradeoffs that have to be made when choosing a cable. While a variety of important characteristics and requirements were given, the average outdoor wireless networks do not require exotic cables and very often have to be pre-built for the exact deployment.

Connectors follow the same example as cables, as they also offer a wide range of possible options. The options are, however, limited as the antenna and access point manufacturers often choose a connector set, taking the option away from the deployer. It was indicated that size transitions adversely affect the quality of the signal and increase signal loss. For this reason the connectors and cable have to be closely matched in size to reduce possible loss.

While it may seem difficult to choose the optimal cable, connector and antenna combination, potential deployers have to remember that outdoor deployments using ISM equipment have been done repeatedly and that a considerable amount of information is available to draw from that simplifies the process greatly. Poynting produces antennas with selectable gain as well as integrated enclosures. Selectable gain antennas allow for flexible deployments, while options that allow the access point to be enclosed inside the antenna almost eliminate the need for cables as well as any possible associated losses. Both options reduce costs and allow for any potential deployer to eliminate unrequited guesswork.

Given topological information and an understanding of antennas and how they function in the real world, the next step would be to combine the topological information with that of the antennas and illustrate how geographical aspects can hinder or be used as an advantage in the construction of a wireless MAN.

Chapter 7 - Physical design and layout

7.1 Introduction

Given the knowledge about different technologies, their suitability for certain types of nodes and the use of antennas to increase range, the next step is to determine if a physical location of a node is suitable for the target deployment or node type.

In previous chapters various radio principles were discussed, and it was indicated that signals could suffer losses due to natural as well as man-made objects.

In this chapter the factors that result in interference as well as the complete loss of signal will be mentioned again.

Tools that are frequently used in determining if these factors are present will also be discussed.

The custom node topology devised in Chapter 5 will then be imposed on a geographical area to illustrate how certain nodes are more suited to certain locations.

7.2 Factors Influencing Loss

In Chapter 3 a discussion of radio propagation principles indicated that loss of signal is a result of the following three factors [Spu04]:

1. Free space loss.
2. Attenuation.

3. Scatter.

Free space loss is the natural loss of the signal’s power as it spreads [Spu04]. Free space loss does not indicate any external factors that would increase the free space loss of a signal, meaning that only the distance would be a determining factor. Using antennas to focus available signal can sidestep free space loss.

Attenuation occurs when an object that a signal passes through absorbs some or all of the energy of the signal [Spu04]. With attenuation external objects are clearly contributing factors. Different objects have different levels of attenuation; trees can result in a minimal loss of 10 dB while a mirror completely absorbs all signal.

Scattering is the reflection of energy by the object in the path of the signal [Spu04]. External objects are again contributing factors.

Over great distances there is not always a sure way to guarantee that no attenuation or scatter-inducing objects are present. Thus for long-range links LOS between the two points is recommended to ensure that minimal attenuation or scattering occurs [Fli2a]. The presence of LOS also makes it easier to ensure that focused signals do arrive correctly at the destination point [KK03]. Over great distances it is not always easy to see the other point of a connection and be sure of what lies between the two points [Fli2a], but there are tools available to determine exactly what is between two points.

7.3 Topographical Maps

Topographical maps are used to represent as much information as possible about a particular area with a given scale. Information on topological maps can include geographical outcrops, land utilization as well as vegetation, to name but a few [Law71]. Of great importance will be the contours and shape of a given area [Rai48].

As discussed in the previous section, LOS is critical and maps can be used to determine if there are any objects between two points of a connection. While topographical maps can prove invaluable in determining if a link is possible or not, information on the maps may be out of date and should only be used as a guide. The best way to determine if there is something in the path of a connection is to either physically track the entire path or attempt a connection and hope for the best [Fli2a].

Topographical software can be used to assist in determining if LOS is present [Fli2a], and is a good replacement for the paper-based alternatives. When using topographical software it is important to make sure that it has the following features [Fli2a]:

1. A cross-section view should be supported for a drawn path. A view from the top of a geographical area might not adequately indicate any obstacles that the link will have to deal with. Fig 7.1 illustrates this concept. Points A and C do have LOS, but points A and B do not.
2. Mapping software should allow for markers and points to be made on the map. The ability to support coordinates such as latitude and longitude will make the plotting of points much more precise and result in accurate plots.
3. GPS hardware allows for the precise measurements of latitude, longitude as well as the points level above sea level. When using a GPS for accurate measurements the topological software should support the GPS interface.

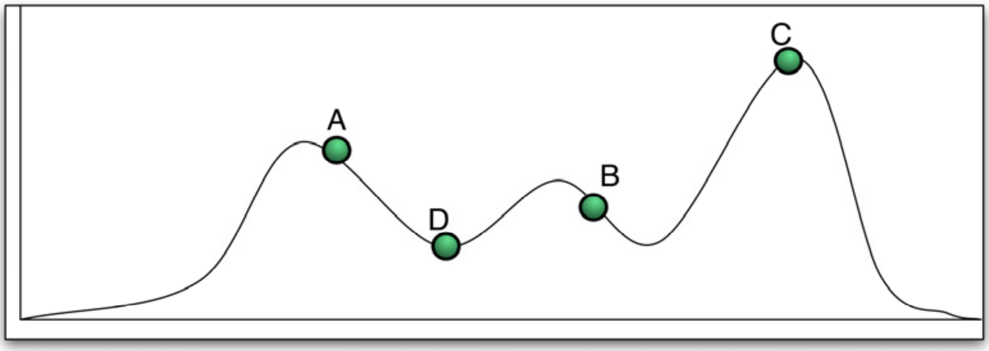


Fig 7.1 – Cross-section of topological map

Fig 7.1 is a representation of four points plotted onto a cross-section of a map. If all points are to be connected to the network, there is no simple way to do so. Points A and C have direct LOS, as does point A of point D and point C of point B, but point A does not have LOS of point B, neither does point C of point D. Connecting point D and point B directly will not be possible.

Points A and C are, however, in good locations, as they are high up on a hill [Fli2a]. If locations A and C are not too far from each other, they can provide indirect access from point D to point B. Point A would have to connect to points D and C, while point C would have to connect to points A and B, thus indirectly providing connectivity for points D and B.

7.4 Custom Node Topology imposed over a Geographical Area

Utilizing the Benade wireless MAN topology defined in Chapter 5 and imposing it onto the theoretical geographical area represented in Fig 7.1 indicates that certain nodes are better suited to certain geographical locations.

Client nodes would very likely be simple Wi-Fi equipment and have no antennas. For this reason client nodes will have to be in range of a strong signal that has very little interference. Since LOS greatly reduces interference a client node would have to be at a location that has a clean view of the access node. Access nodes, on the other hand, have to create a wide coverage area and have minimal interference for the coverage area. A high-lying geographical area allows coverage of a low-lying area with minimal interference [Fli2a], implying that either the client node or the access node should be higher than the other. An indication that access nodes would be better located on high points is the Poynting omnidirectional antenna. The antenna is designed for hotspots, and features a beamwidth with a downward tilt [Poy05]. This implies that within a hotspot where extended coverage and minimum interference are needed, similar to an access node, antennas are ideally placed above the client equipment.

Transit nodes and backhaul nodes require maximum range as well as effective throughput. While there is nothing prohibiting two transit nodes from being in a similar structure to a client node and an access node, unknown interference-inducing elements such as tree foliage growing back in the summer can increase interference [Spu04], and in turn reduce range and throughput of critical transit or backhaul nodes. For this reason it is recommended that critical nodes both be on high points where unknown factors cannot influence critical aspects of the connection.

Relating the custom node topology to Fig 7.1, points B and D would be ideal locations for client nodes while points A and C would be good locations for access nodes, backhaul nodes as well as transit nodes.

7.5 Conclusion

In this chapter the factors influencing loss were highlighted again. It was indicated that for long-range connections to work, LOS is critical. Given that very few geographical areas are completely flat, the natural shape of the land can be used as an advantage to the builders. In conjunction with topographical software and GPS equipment it is possible to increase the likelihood that a long-range connection can be made with minimal interference.

The Benade wireless MAN topology introduced in Chapter 5 can be imposed on a geographical area; nodes such as access nodes would be placed on high-lying regions that are easily accessible by client nodes in lower geographical areas. With minimal possible interference, links from one high point to another can potentially go further and at greater speeds, making these links ideal for backhaul and transit nodes.

Chapter 8 – Security

8.1 Introduction

In Chapter 5 different topologies were presented for a variety of different wireless MANs. Almost all of the topologies have no implicit security options, and while many would argue that security contradicts the very open nature of the specific networks, the open accessibility allows for a variety of security issues to arise.

The Internet also started with the same open principles as most current wireless MANs, but as users increased, the lack of security became a problem. Hackers defacing websites, viruses and spam make the lives of the common Internet user difficult due to lack of security.

The counterargument is that wireless MANs aim to provide services to users at no cost and should be as easily accessible as possible. Implementing difficult-to-use security that deters attackers will most likely also deter people from using the network, reducing the overall usefulness of such a network. The belief is that security should be the concern of the users and not the builders, meaning that the users should install anti-virus software and take security steps, and that the builders of a network should not be concerned with security at all.

The fact of the matter is that completely unprotected wireless networks allow for any casual snooper to see all traffic that passes over the connection. While many wireless MANs are public initiatives aimed at making a variety of services available to the builders and users, there is no guarantee that either a builder or user could not become a security risk to other people in the network. For this very reason everyone needs to have security in mind, or at least be aware of the possible risks involved in using any large uncontrolled network.

In this chapter a few common security technologies used in wireless networks will be reviewed, as well as their position in the OSI ISO model. The security requirements for different node types as well as the suitability of the technologies mentioned in section 8.3 to those specific requirements are also discussed.

8.2 Security Services and the ISO Model

An adequate security solution would ensure that access to the network is controlled, users' information is kept private and intact, and the network is protected from known types of attacks [KK03]. While wireless networks have unique security requirements due to their distinct physical medium, the basic required security services are still the same. They are [vSE03]:

1. Identification and authentication.
2. Authorization.
3. Confidentiality.
4. Integrity.
5. Non-repudiation.

In a public wireless MAN it is difficult to have all of the five above-mentioned security services due to the open nature of such a network. However, taking examples from the Internet could allow for a hybrid security model to be created that would allow for an open public wireless MAN to have security comparable to that of the Internet.

Some of the most common wireless security technologies have many different target areas; WEP, for example, was the initial WiFi security method for authentication as well as encryption of the physical medium. As flaws were found in WEP, newer methods for both authentication and encryption were devised but these methods required more processing power. The requirement for more processing power created a market for improvements to WEP on access points without the required level of processing power. This market allowed for an initially flawed security technology to find a home amongst the wireless deployments that did not require extreme levels of security, or where upgrade cost was prohibitive.

Before proceeding with the security technologies, an understanding of the OSI stack is needed to illustrate where the specific security technologies attempt to create a security barrier and how the technologies complement each other.

The OSI stack is composed of seven layers, each with unique functions. The seven layers are [Sha99]:

1. Physical layer: The physical layer is concerned with transmitting the data bits over the network.
2. Data link layer: The data link layer controls the flow of information over the network.
3. Network layer: The network layer deals with routing of information to the appropriate nodes.
4. Transport layer: The transport layer deals with end-to-end communication and is the first layer that does not actually deal with the network itself.
5. Session layer: The session layer establishes a logical connection and synchronizes communication.
6. Presentation layer: The presentation layer is responsible for presenting information in a format that is understandable to the user.
7. Application layer: The application layer works directly with the user or application and is responsible for the transparency of the underlying layers.

The ideal security solution would address as many of the seven layers as possible. If one layer's security mechanism fails, the next layer would provide an additional barrier to deter any attempts to break into a system.

To illustrate this concept Meru Networks illustrate their multi-layered approach with the following figure:

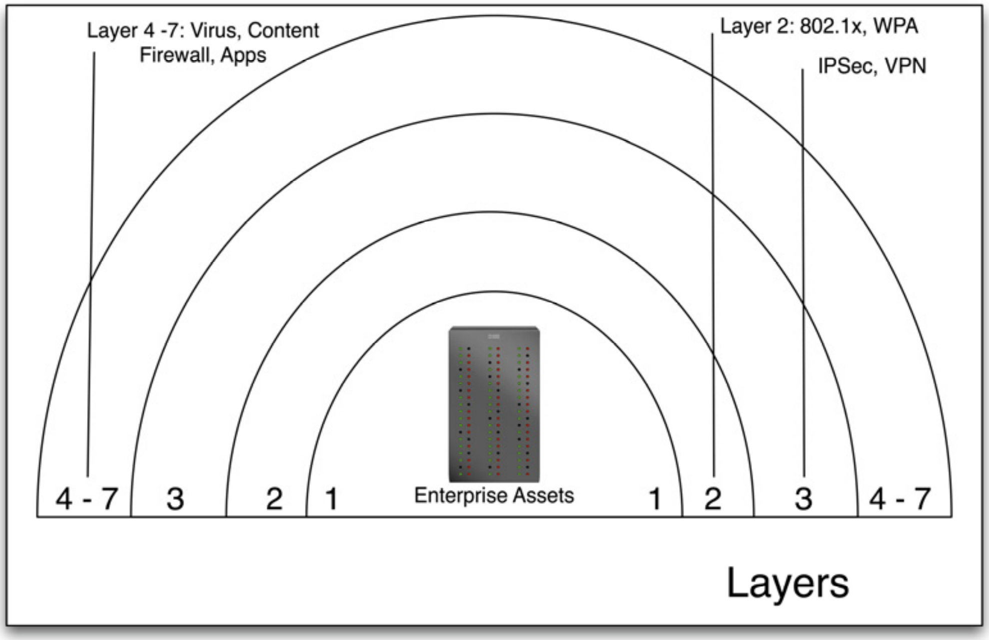


Fig 8.1 – Multi-layered security [Net04]

Meru’s multi-layered approach illustrated in Fig 8.1 presents an image in which different technologies on different layers can be added together to produce a very secure system. This is also reflected in current mesh network security designs [AWW]. The illustration does not include all possible technologies, for example WEP, SSL and SHTTP are not mentioned, and all three technologies can enhance security in open environments without drastically decreasing the ease of use.

While it is possible to layer many technologies to create a very secure system, a key consideration is that a wireless MAN encourages easy access; many technologies require complex setup, are proprietary and offer very little interoperability, and as a result could make a wireless MAN difficult to connect to and deter people from attempting to do so. In a paper by Haidong Xia and Joze Brustoloni usability and interoperability are favoured over security [XB04]. Table 8.1 illustrates this relationship.

Table 8.1 – Relationship between usability and security

WiFi application	Requirement		
	Security	Usability	Interoperability
Enterprise	High	Medium	Medium
Home	High	High	Medium
Access	Medium	High	High
Open	Low	High	High

Source: HX04

8.3 Wireless Security Technologies

There are many different security technologies, and all aim to secure different potential security vulnerabilities. Due to the distinct and easily accessible physical medium, WiFi had to feature some sort of security mechanism to restrict people from easily connecting to private corporate networks. I will start by reviewing these technologies that aim to restrict access to the physical medium.

8.3.1 WEP

WEP was the initial security mechanism for 802.11a, 802.11b and 802.11g and operates on the second level of the OSI stack [KK03] similar to WPA and 802.1x.

WEP was designed to ensure confidentiality, integrity and authentication. These services are, however, only provided at the access point. Once access is granted, the remaining wired network is completely unrestricted and unprotected by WEP. Thus confidentiality, integrity and authentication are not ensured for the rest of the network [Gas02].

In a wireless MAN the lack of security over the wired section of a network is not such a major concern, as it would not be in a corporate environment. As illustrated in Chapter 5 most of the access points will only be directly connected to other access points. This means that, unlike corporate environments where most services will be provided from within the wired section of the network, within a wireless MAN most services will be provided by the clients.

Considering that users provide the services and that neither user nor service is protected by WEP, service providers cannot guarantee confidentiality, integrity or authentication. Once a client is authenticated on a particular access point the user would require no authentication at all for services provided by other clients on other access points [KK03]. In essence the entire network, irrespective of the physical medium, provides authentication only at the particular access point and the remaining network carries no knowledge about any particular client.

Over the wireless link integrity is ensured by including a CRC checksum of the data within the frame body. Encrypting the data along with the CRC with the RC4 stream cipher ensures confidentiality. Using a pre-shared key as the basis for the RC4 encryption ensures authentication; however, it is this pre-shared key where most of the security flaws of WEP are found [Gas02].

Authentication within WEP has two modes of operation. They are [JK03]:

1. Open authentication.
2. Shared-key authentication.

Open authentication allows for any client to be associated with an access point [JK03]. While this might seem like no authentication at all, the official IEEE specifications consider open authentication the only required form of authentication for 802.11 [Gas02].

While open authentication might seem an ideal solution to a wireless MAN where open access is encouraged, it does not offer any security at all. Anyone would be able to join the network and to transmit over it, as well as see all unencrypted information that travels over the network [KK03]. This would allow any attacker to easily join the network and use any service provided, as well as attempt any form of malicious attack. Clearly a completely open network without authentication is not desired.

Shared-key authentication works on the premise that both parties have access to the same key. During authentication the access point sends a challenge to the client wishing to authenticate. The client then encrypts the challenge and sends the encrypted challenge back to the access point. If the access point is able to decrypt the message with the shared key and to successfully compare the newly unencrypted challenge with the original challenge, the client has been successfully authenticated and is allowed to access the network. All further transmissions are encrypted using the shared key [Gas02]. Fig 8.2 illustrates this process [Gas02]. An important fact about WEP shared-key encryption is that the RC4 cipher is a stream cipher. When the same key is used repeatedly with stream ciphers it becomes possible to extract the unencrypted text with very little effort. This reduces the effectiveness of stream ciphers. WEP uses a 24-bit value called the initialization vector (IV) which, when appended to the shared secret key, results in a completely unique and unrepeated key [KK03].

8.3.1 WEP - Continued

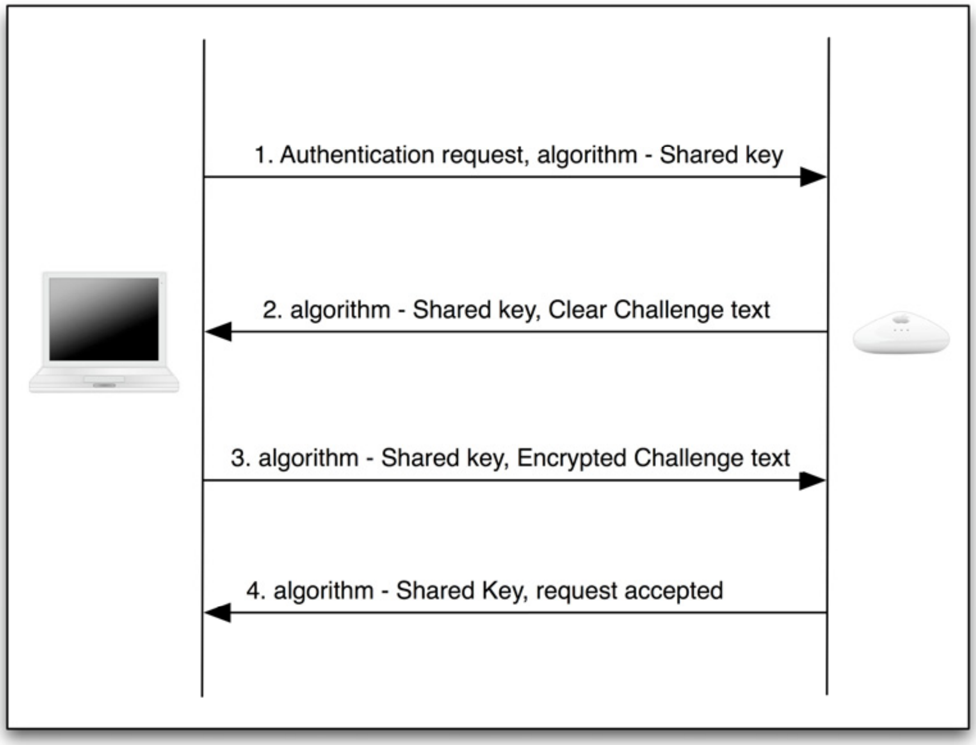

1. Authentication request, algorithm - Shared key
2. algorithm - Shared key, Clear Challenge text
3. algorithm - Shared key, Encrypted Challenge text
4. algorithm - Shared Key, request accepted

Fig 8.2 – WEP authentication process [Gas02]

The increased level of security that shared-key authentication brings comes at a price; the key used for encryption and authentication has to be known by any party wishing to join the network [Gas02]. In a wireless MAN this may not be possible as everyone that wishes to connect as a client cannot be given the key in advance. They would have to collect the key from the access point owner, something that is not very practical when the connection might be made over a distance of a few kilometres. When single long-range point-to-point connections are made, a secret shared key is, however, feasible.

The inability to connect to the network effortlessly would very likely deter most users from using the network. To ensure easy access a shared-key security method is not advisable where easy public access is important.

WEP is not a perfect security measure, though. While WEP was initially thought to be secure, flaws were soon found, and although the independent RC4 stream cipher has remained secure, its implementation as used by WEP reduces its effectiveness. Some of the security issues that eliminate WEP as a security measure for almost all scenarios are:

1. Manual key management has numerous problems which are similar to those of traditional key distribution, and include key distribution and change [Gas02].
2. The IV that is supposed to eliminate the possible occurrence of repeated key streams is only 24 bits long and results in a limited number of possible IV values. Some manufacturers do not utilize the IV to its full extent and even reuse the same IV value over and over. The small number of possible IV values along with the weak utilization of the IV system creates a security flaw. With only 24 GB of storage, a complete dictionary of all possible IV values as well as their secret key partner can be created. With a full dictionary available it is possible to extract the clear text or the secret key [BGW01].
3. The authentication process illustrated in Fig 8.2 allows for the average eavesdropper to have access to a clear text version of challenges as well as the encrypted version. With knowledge about the frame construction, IV and both versions of the challenge, it is possible for an attacker to authenticate with the access point without knowing the secret key [ASW01].
4. Weaknesses in WEP have been found due to improper use of the RC4 algorithm. The implementation allows for weak keys to be determined and as a result overcome the encryption that RC4 provides. The IV allows for weak keys to be easily determined, and even with an IV value of 128 bits instead of 24 bits, the time for extraction would only increase linearly instead of the expected exponential increase [BGW01].

WEP was devised to provide confidentiality, integrity and authentication on the second layer of the OSI stack. The flaws in the WEP protocol, however, eliminate WEP from any form of deployment, as the flaws remove confidentiality, integrity as well as adequate authentication due to the shared key. Although not a problem when deploying a point-to-point connection, the distribution of shared keys becomes very difficult when done with multiple people over large areas. The effect is increased difficulty in accessing the network easily.

8.3.2 WPA

The IEEE had started to work on a replacement security mechanism for WEP, called 802.11i, after initial security flaws within WEP were discovered, but the users and industry demanded an immediate replacement that would resolve the security gap that WEP had left. WiFi-protected access (WPA) was defined as an interim solution to the WEP security flaws and is based on draft version 3 of 802.11i [JK03]. WPA also provides security of the second level of the OSI stack.

One of the major differences between WEP and 802.11i is that 802.11i can use the advanced encryption standard (AES) instead of the RC4 stream cipher. While the AES is much more secure than RC4, it requires much more processing power than RC4 for encryption activities. Older access points do not have the required processing power and effectively eliminate the use of 802.11i on older access points. Along with AES, WPA also uses a patched version of WEP and RC4, and as a result allows for older access points not able to provide the processing power to utilize AES and the ability to use an improved and enhanced RC4 implementation. The end result is that WPA provides a clear and secure upgrade path for WEP users, making WPA a better-suited option for older equipment than 802.11i [AC304].

WPA offers two forms of authentication. They are [Wf]:

1. WPA-Enterprise.
2. WPA-Personal.

WPA-Enterprise uses 802.1x and one of the extendible authentication protocols (EAPs) for authentication. EAP handles the presentation of the user's credentials in the form of digital certificates, smart cards or any other form of authentication the system administrator chooses. EAP and 802.1x create a framework where clients mutually authenticate with an authentication server. The most popular and widely deployed authentication server that supports 802.1x and EAP is a RADIUS server [Wf].

While there are open-source RADIUS servers available that would reduce the costs, the need for a dedicated machine to host the server will result in a central person/authority being responsible for maintaining the server, as well as maintaining a database of ever-changing users. The need for central administration also means that anyone wishing to join the network would have to contact the central administration to gain access.

Central administration can be an advantage. Only a single central authority needs to be put in place and the entire network would then feature authentication via 802.1x, confidentiality via AES or the improved RC4. The use of 802.1x and AES or RC4 allows for a high level of integrity and non-repudiation and the ability to pinpoint a user to a certain authentication session [All05].

Complete integrity and non-repudiation cannot be guaranteed as there are still segments of the network where security may not feature. WPA also only secures the second layer of the OSI stack and serves to secure the actual wireless link of the connection. Anyone that can access the network can still attempt to attack services provided by others.

The central administration does, however, allow for a client to sign on to the network a single time and be able to securely connect to the network from all points that use WPA-Enterprise and the correctly associated RADIUS server. The ability to connect to the security of multiple points might seem similar to roaming. Most WPA-enabled access points unfortunately do not support roaming and the user would have to re-authenticate when leaving or entering the coverage area of an access point [JK03]. This removes the possibility of a truly metropolitan coverage area where roaming is an option.

Within a public wireless MAN it is very unlikely that RADIUS servers would be deployed to utilize WPA-Enterprise.

WPA-Personal does not require a RADIUS server and is targeted more at the small home or small business. WPA-Personal relies on a pre-shared secret key that has to be entered in the client equipment as well as the access point [JK03]. Once mutual authentication has taken place an random encryption key is generated for the respective users and from then on communications are encrypted with that generated key. To discourage any attempts to obtain the key, the key is rotated at random intervals. The net result is that the RC4 key is unique for each user and does not remain constant over time. This key change is called TKIP and is also found in WPA-Enterprise [AC304].

TKIP not only provides for a key change and exchange mechanism, but also adds a total of four fixes to WEP. The four fixes are [AC304]:

1. A message integrity check that improves over CRC.
2. Countermeasures that delete the authentication and encryption key if an attack is detected.
3. A per-packet key-mixing function.
4. Replay protection.

WPA-Personal is much more secure than WEP due to the improvements that TKIP brings to the table. WPA-Personal also requires that a pre-shared key be known at both the client and the access point. Similar to WEP, the shared key requirement of WPA-Personal makes it very difficult to use when easy secure access is needed over large areas.

WPA solves most of the problems that WEP had and also allows for an upgrade option for users of older equipment. The upgrade usually requires a firmware update [JK03]. While some might not want to upgrade firmware for fear of hardware damage, the alternative is insecure WEP.

In a wireless MAN, the hardware is very likely to be from different vendors and have different capabilities, meaning that it is possible that client equipment incapable of WPA will be found. Forcing someone to upgrade to a certain security level is not necessarily an option. Firmware upgrades could possibly seem to be a very daunting task to non-technical people, and the additional requirement of obtaining a key from an unknown person is likely to deter most non-technically minded people from using the wireless MAN.

Table 8.2 summarizes the differences between WEP and WPA.

Table 8.2 - Difference between WEP and WPA

	WEP	WPA
Encryption	Flawed implementation of RC4	Fixed implementation of WEP
Key size	40-bit keys	128-bit keys
Key type	Static key used for every user on the network	Dynamic session keys; each user has a unique key per session as well as per packet
Key distribution	Hand-typed and completely manual	Automatic
Authentication	Uses WEP key for authentication	802.11x and EAP

Source: Wf

8.3.3 802.11i/WPA2

Although 802.11i and WPA2 are not the same security technology, they have many things in common. WPA2 is based on the final specification of 802.11i but unlike the full 802.11i, it does not support fast roaming. In all other respects

802.11i and WPA2 are the same [All05], so for this reason WPA2 and 802.11i will be discussed together.

The key enhancement 802.11i/WPA2 has over WPA is the mandatory use of AES-CCMP instead of RC4/TKIP for encryption. The addition of AES for encryption is very important. The US government has adopted AES as its required standard for encryption. This means that US government agencies are required to use AES encryptions in their communications, which makes 802.11i/WPA2 the only viable option available to those agencies for wireless encryption. Other organizations that require high security, such as banks, would also use 802.11i/WPA2 instead of WPA [All05], due to its superiority over WEP and WPA.

Another key enhancement 802.11i/WPA2 has is that AES uses Counter-Mode/CBC-Mac Protocol (CCMP). Ultimately CCMP allows for 802.11i/WPA to use AES for encryption as well as integrity, meaning that there is a single encryption and integrity check module that uses the same algorithm and key [All05].

The downside to AES is that it requires much more processing power and would very likely require an organization deploying the network to buy new access points capable of the processing power required for AES [JK03].

All other aspects of 802.11i/WPA2 are similar to WPA. Two methods of authentication are available; the first, WPA2-Enterprise, also functions using 802.11x/EAP and the second, WPA2-Personal, also uses a pre-shared key [All05]. With so many aspects in common the discussion of WPA in relation to wireless MANs also applies to 802.11i/WPA2. WPA2-Enterprise in conjunction with a RADIUS server would make it possible for users to log in once for the entire network, and the centralized focus also eases registration in comparison to multiple distributed registrations.

While the centralization does create a central point of failure, the most likely deterrent to using 802.11i/WPA2 is the requirement to create an account before accessing the network as well as the relatively advanced hardware requirements to use AES. The lack of true roaming support in WPA2 might also deter users from using WPA2, and opt for 802.11i instead as it is the access points that would contain the feature of true roaming capabilities and not the client hardware. From the provider's perspective WPA2 would be the more likely candidate for selection as WPA2 hardware has been available for longer and is probably also cheaper.

AES might, however, make institutions join a public MAN if the entire network were to deploy either 802.11i or WPA2. The relatively strong encryption and need for registration and authentication before using the network would ease many security worries institutions like banks might have. The involvement of banks would encourage the public to join the network as long as the banks provide adequate high security and quality services.

The three above-mentioned technologies (WEP, WPA and 802.11i/WPA2) are aimed at securing access to the wireless medium. All three come with their own set of properties but the important aspect in relation to a wireless MAN is that all three require either a pre-shared key or a central authority to sign a person on.

8.3.4 Captive portals

The primary idea behind a captive portal is that instead of relying on the security mechanism of 802.11, the access point is left with no security enabled and is a completely open network. The access point is, however, configured with a firewall that initially only allows a user to access websites. Web traffic is redirected to an authentication site where the users are requested to authenticate themselves. The authentication backend can take place with a variety of authentication services including RADIUS. Fig 8.3 illustrates the process. Once a user is authenticated the firewall rules are relaxed to appropriate levels for the authenticated user [Fli2a].

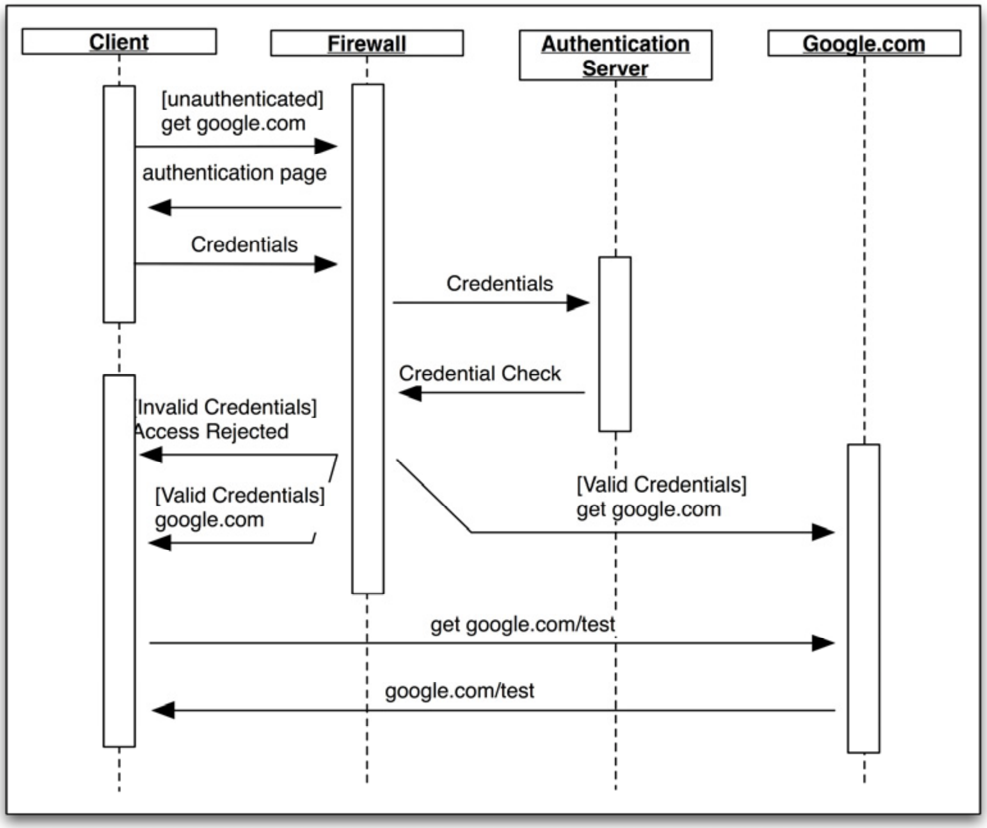


Fig 8.3 - Captive portal authentication [Fli2a]

Captive portals have the advantage that anyone wishing to join or connect does not have to have equipment supporting a specific level of security and can have the oldest equipment that is capable of connecting. Authentication as well as registration can be made on the website. The use of existing authentication methods such as RADIUS which support large numbers of clients allows for a single metropolitan authentication system that allows anyone to connect at any available access point throughout the network. The portal can also be configured to inform users about usage policies of the specific access point or the entire network, as well as being given general security information [Fli2a].

The disadvantage of a captive portal is that while it provides the easiest way to allow users to identify and authenticate themselves, it does not feature any security to the client as all information is transmitted over an unencrypted network. The lack of encryption ultimately facilitates the need for an additional security technology such as SSL to ensure confidentially and integrity [Fli2a].

Mapping the results found in the analysis of WEP, WPA, 802.11i/WPA2 and captive portals onto the requirements set out in Table 8.1 results in the following table:

Table 8.3 – Security technologies mapped onto target deployment vs. requirements

WiFi application	Requirement		
	Security	Usability	Interoperability
Enterprise	802.11i/WPA2 Enterprise	WPA-Enterprise	WPA-Enterprise
Home	802.11i/WPA2, WPA	WPA-Home	WPA-Home
Access	WPA, WEP	WPA, WEP	WEP
Open	Captive portal	Captive portal	Captive portal, WEP

Considering that this chapter focuses on security, the ‘Usability’ and ‘Interoperability’ columns of the above table take the ‘Security’ column as a guide. Although there are technologies that offer better interoperability than others, a technology with lower security capabilities was not considered as an option for usability or interoperability.

From Table 8.3 it is clear that captive portals offer the best security/usability/interoperability paring for open networks. Unfortunately captive portals offer no security, forcing the layers above the physical layer to be more secure if a truly secure system is to be deployed.

8.4 Security and Applications within a Wireless MAN

The types of applications that are available over a wireless MAN are in general not restricted at all, meaning that a wide variety of different applications can be found, all with unique security requirements and vulnerabilities. Because it is impossible to cover all possible applications, their security flaws and workarounds, only a few popular technologies that will be used by the most average home and business users will be mentioned.

With the popularity of the Internet it is very likely that people wishing to join or utilize any wireless MAN would expect services similar to the Internet. The ability to telecommute would also mean businesses might opt for their employees to be able to connect to the corporate network through the wireless MAN. To satisfy these needs and expectations certain applications are needed. The following steps are recommended to secure some of these services [SWS]:

1. Use SSH instead of Telnet.
2. E-mail (SMTP, POP3 and IMAP) should be avoided and their more secure alternatives should be used (SMTP with STARTTLS, SPOP3 and IMAPS).
3. SFTP or SCP is to be used instead of FTP, and https instead of http.

While there are many more technologies and possible applications, the focus of this chapter is securing a wireless MAN. The above-mentioned technologies are not specific to such a network and can be run on almost any network. For this reason this chapter will not go into detail on any specific application and the security factors of that application.

However, it is important to know that a public wireless MAN will be built by many different people, and that each person will configure their security differently. This means that while a person could connect elsewhere, there is a possibility that they might not be able to access services from the new location. In South Africa this is likely due to current legislation [oSA96]. It is also important to mention that a South African public wireless MAN may not be connected to the Internet. This means that services will have to be hosted from the wireless MAN itself, and that the provider of such services must take steps to ensure that services are provided securely and that they are protected from any sort of known attacks against that service.

For more information on general network security there is a wide variety of reading and sources available.

8.5 Custom Topology and Security

In section 8.4 it was indicated that due to the self-forming nature of a public wireless MAN each access point might have different security settings. The pre-existing topologies listed in Chapter 5 either have no security enforced or they have pre-defined security for the entire network. The Benade wireless MAN topology allows for optional security and better matches the dynamic formation of a public wireless MAN. For this reason the Benade wireless MAN topology and each of its node types will be discussed with regard to security.

Each of the following subsections will briefly discuss each of those nodes again, as well as list possible security options.

8.5.1 Client nodes

A client node is a person or a group of people wishing to connect to the public wireless MAN that has a capable hardware setup. In other words, any type of hardware ranging from a single user with a PDA to a full network can access the wireless MAN. Client nodes have to be in range of the access point and should have hardware capable of the required level of security.

With such a diverse set of possible hardware combinations the security options are also very diverse. The open nature of the wireless MAN can be compared to the Internet. Thus client nodes can be directly compared to Internet users, and as such have to take similar steps to Internet users to protect themselves. Therefore the use of firewalls and anti-virus software is recommended.

8.5.2 Access nodes

Access nodes offer access to client nodes, and can act as a possible gateway between clients and the rest of the public wireless MAN.

Continuing the comparison of a public wireless MAN to the Internet, access nodes are in a way very similar to an ISP. The owner of an access node is also presented with many security options. ISPs require identification and authentication and provide a relatively open unrestricted service. An access node owner can completely control the level of service availability without even requiring identification or authentication.

Assuming that a geo cloud opts to deploy a security node, the choice of security features are largely removed from the access node owner, as these features are now the collective responsibility of the geo cloud. If the cloud does not deploy a security node, access node owners can deploy any of the technologies mentioned in section 8.3. When deploying technologies that require a key, owners will have to keep in mind that client nodes will have to be issued with a key and all activities involved in the issuing and administration of the keys will be the responsibility of the access node owner.

When using a captive portal most administration responsibilities are removed from the access node owner. Client nodes can create an account themselves by using self-registration on the portal. As mentioned during the discussion of captive portals, there is no security of the physical layer. For this reason the captive portal authentication page should inform client nodes that they are not using a secured medium and that they are responsible for securing their own information [Fli2a].

An alternative security mechanism that access node owners can deploy is a hybrid solution by combining WPA or WPA2/802.11i with captive portals. WPA and WPA2/802.11i encrypt the physical layer with contentious rotating keys, but require a key for initial access. Captive portals do not require a key but offer no security. An access node owner can openly distribute the shared key and deploy a captive portal. With this method the physical medium is still protected by encryption using rotating keys and strong message integrity checks. Authentication is lacking due to the open key, but is then provided with the captive portal. Distribution of the WPA/WPA2/802.11i key can prove difficult but access node owners might choose to use their service set ID (SSID) as the key. The SSID is broadcast by default and users can easily obtain it.

8.5.3 Transit nodes and super-transit nodes

Transit nodes are simply nodes that facilitate point-to-point connections; a transit node may be connected to an access node, but is always connected to one other transit node. Super-transit nodes simply connect to more than one other transit node. The connection to an access node is achieved over a cable and is bound by physical security. The connection to another transit node is, however, wireless and is bound by the security methods mentioned in section 8.3.

Transit nodes can be compared to backhaul connections within an organization.

Securing inter-transit node connections is very different from securing an access node. Transit node owners are not concerned with easy access; they are most likely concerned with the range and speed of the link. Because the ease of connectivity is not a major concern, security measures do not have to cater for ease of access, but the use of enterprise security is not adequate either. Enterprise-level security is suitable for environments where many clients have to access networks very securely and where authentication servers most likely already exist.

In the one-to-one connection type of transit node a secure link is required. There are, however, no clients frequently authenticating and authentication servers are not usually present. It is therefore recommended that a pre-shared key be used with a technology such as WPA or WPA2 to protect the connection from casual eavesdroppers.

8.5.4 Backhaul nodes

Backhaul nodes form the long-range backhaul links that connect geo clouds and also secure the geo clouds from each other. The security measure is achieved with the use of a firewall.

The exact configuration of the firewall will depend on the firewall's abilities as well as the preferences of the geo cloud. When creating firewall rules the following have to be taken into consideration:

1. Services that have their origin within the geo cloud and whether the services are available to users of other clouds.
2. Services that have their origin from within other geo clouds and whether the service is available to users within the geo cloud.

8.5.5 Security nodes

The security node is a node responsible for whatever authentication was selected for a geo cloud. This node is completely optional.

The presence of a security node means that the entire geo cloud has agreed upon an authentication method for the particular geo cloud. This would happen as the number of access nodes stops increasing and the size of the geo cloud stabilizes. A centralized authentication server allows for a geo cloud to use some of the key-based security technologies in enterprise mode. Since geo clouds can be geographically based, the security needs and budget of a geographical area can be taken into consideration, meaning that security for a more prosperous area where applications like banking are required can be higher than a poor area where basic access is only desired.

I believe that over time security over an entire metropolitan area will become the same as hardware costs are driven down and the need for secure applications becomes greater. The use of security nodes and authentication servers will allow for a single sign-on to be possible for the entire network, while administration will remain decentralized. The failure of a single authentication server will most likely only be a temporary deterrent as the multitude of authentication servers can act as backup and mirror servers.

8.6 Conclusion

In this chapter the goal was to review common wireless security technologies. It was found that due to the open nature and dynamic formation of a public wireless MAN, there is no perfect security measure.

Key-based technologies such as WEP and WPA would introduce administration overheads to the owners of access points. Due to the large areas being covered classic key distribution problems are compounded. The result is that people could possibly shy away from using the network.

While some of the newer technologies feature better security than the WEP with its known flaws, the enhanced security does come at a price. More complex encryption algorithms within technologies such as WPA and 802.11i/WPA2 require considerably more processing power than what most first generation 802.11 access points can offer. This forces users of older equipment to either live with a flawed security mechanism or seek out expensive proprietary technologies. Due to the diverse nature of clients accessing a public wireless MAN the builders of such a network cannot require clients to have equipment capable of the latest security measures, as doing so would deter clients from connecting.

It was also found that while any possible application can be run over a wireless MAN, the insecure nature of the physical medium would require users to take similar measures to those taken by Internet users.

Services would most likely have to be provided from within the network, as Internet connectivity could not be ensured. This means that additional measures would have to be taken by these service providers to ensure their own security as well as those of the clients of the service they provide.

The overview of the security options for the Benade wireless MAN topology presented in Chapter 5 indicates that the best initial security measure for growing networks is captive portals. However, other nodes are not limited to any form of security, but it is recommended that shared-key authentication be used rather than unnecessary enterprise-level security for simple point-to-point connections. As indicated, as the network grows stronger security measures could be taken and these include single sign-on with enterprise-level security over the entire network.

Once a network is constructed and secured, there is no guarantee that it will remain fully functioning on a continuous basis. The next chapter will consider the factors that influence maintenance of a wireless MAN.

Chapter 9 – Network management and maintenance

9.1 Introduction

The previous chapter discussed the security concerns of a wireless MAN. This chapter will discuss management concerns.

Once a network is up and running there is no guarantee that it will run continuously without any flaws. As a network's size increases and more and more users are added, a structure needs to be in place to hold the network together and allow for growth [MG95]. Consumers or users of a network will choose to use a network based on service levels [HBR03]. Clearly where large amounts of money are spent and considerable effort is put into the network, a lack of users is not desired.

Problems that an Internet user comes across can stem from multiple sources. They, the ISP or the backbone the ISP is connected to could be having some sort of problem. Within a public wireless MAN there are also a variety of problems that can arise.

This chapter will discuss a few disasters that have struck traditional wired communications networks and draw a comparison with how such a disaster might influence a wireless MAN. User expectations of networks will then be discussed and compared with how realistic those expectations are of a wireless MAN.

The classes of tools available to network managers will be mentioned and a brief discussion of Simple Network Management Protocol (SNMP) will follow.

Issues that are specific to wireless networks will then be discussed and the chapter will conclude by mentioning maintenance issues for the custom nodes set out in Chapter 5.

9.2 Why Network Management is Needed

As traditional wired networks became more popular and were used more, people and organizations became more dependent on them. Failure of a network very often means considerable downtime and losses [Bat91][HBR03].

Examples of a few disasters that have struck wired networks include the fire that completely destroyed the Hillside Central Office on 8 May 1988. The Central Office served as a gateway for local, long-distance, fibre and cellular services. 500 000 customers were serviced by the office and when it was destroyed all services were completely disrupted. The office did have monitoring systems but at that time there were frequent storms and all warnings were dismissed as being erroneously generated by the storm. By the time the monitoring staff realized that the warnings were in fact real, the office had burnt to the ground. The lesson that was learnt was that errors should not be easily dismissed, and fire suppression techniques should be in place at crucial points in any network [Bat91].

Within a wireless MAN a fire would probably not disrupt the lives of 500 000 people unless the node were a crucial backbone node for the network. For anyone wishing to monitor a node, distributed management software could be used to deliver errors, but fire sensors or suppression techniques are very likely not a primary consideration when a person buys equipment for and constructs a node. The deployers of a public wireless MAN will take every cost savings measure they can and fire suppression techniques will probably never feature.

The Hillside Central Office example was a natural disaster that disrupted a network. A public wireless MAN will be built with components that are cost-effective, and methods to detect and circumvent natural disasters such as fires or floods are not likely to be considered.

Another example of a network disaster is the software glitch that severely limited the abilities of the entire AT&T network on 15 January 1990. Code that until that point had gone unused contained a flaw; the flaw quickly propagated though their entire SS7-based network. Although their service was severely impaired, the 15th of January is a public holiday in the US and traffic on their network was low. The overall impact was minimal, agreements with other networks were in place and excess traffic was redirected over third-party networks [Bat91].

Unlike the first example the AT&T disaster was a result of human error; the erroneous code was the culprit and was man-made. Of importance is that the flaw propagated itself over a network that had similar hardware [Bat91]. Within a public wireless MAN it is very unlikely that all equipment will be the same, which limits the possibility of something similar to the AT&T incident happening. Software or human flaws cannot, however, be eliminated, and erroneous settings and flawed software can still be detrimental to a point within the network. Routing traffic over other pathways helped AT&T [Bat91] and can also be used to increase the reliability of a wireless MAN.

Without software management AT&T would not have been able to isolate and redirect traffic through unaffected sections of their network [Bat91], and with adequate management the Hillside Central Office would not have been destroyed by fire. Managing any large network is a daunting task, but also a necessary one. Everyone involved in a network expects certain things from that network, and without network management it is difficult to meet those expectations in both the short and long run.

9.3 Expectations regarding a Network

In the previous section it was mentioned that without network management, user expectations cannot be adequately met. Expectations differ from group to group: a company deploying a hotspot would like the hotspot to make money [HBR03], the user of a hotspot, on the other hand, would like the hotspot to provide easy and fast access at an affordable price. In a survey of different environments, ranging from big to small, some of the requirements users had for a network were as follows [Ter92]:

1. Continued end-user service despite growth and change.
2. Capability to heal, bypass or circumvent failed network elements.
3. Capability to operate fully even when an important network element has failed.
4. Capability to monitor and diagnose unsatisfactory conditions though the entire network.
5. Real-time or near-real-time monitoring of network performance.
6. Human operators require a straightforward interface to management systems.
7. Improved security of the network as well as the network management system.
8. Integrated network management.

It is not stated whether an open network was included in the survey, but if the wireless MAN features mesh-like capabilities the network should be very resilient. The mesh routing protocols will compensate for connections that are temporarily out of service, giving the appearance of a continuous service without noticeable performance decreases. However, this is not possible if critical connections are experiencing difficulties. The need for real-time monitoring of the network performance is not an easy task, and the same is true of integrated network management. These last two factors will be discussed later in the chapter. Monitoring and diagnostics will be discussed in section 9.5.

9.4 Classes of Network Management Tools

Many different network management tools have appeared over the years, each with its own set of goals, and each tool satisfies some of the user expectations discussed above. However, there is no single tool that covers everything.

The reasons for the multitude of tools are [HAN99]:

1. Diverse classes of hardware. Ranging from a simple hub to complex distributed telecoms services, each type of hardware has its own software.
2. Tools must deal with different characteristics. One utility might deal with the signal strength of a wireless connection, while another might list clients authenticated on that access point.
3. Management tools are needed for infrastructures of different sizes. A small organization would need tools that can manage a small number of machines, while a large enterprise would need tools to potentially manage thousands of systems.
4. Tools must cater for users with different requirements. A tool might need to simply modify a simple parameter on a single machine, while another tool might need to install software packages over a distributed area on different platforms.
5. Complex or new technologies may only have special utilities to manage those technologies.

Considering the reasons for the large number of tools it is clear that within a wireless MAN no single utility will be able to serve all management purposes, as hardware is diverse, ranging from access points, and the software on the access points to antennas has different characteristics and specifications. The diversity will make a single integrated management system highly unlikely.

Deploying and maintaining a set of technologies will require the appropriate set of tools. Some of the tools used for general networks are [HAN99]:

1. Test equipment: Used for testing the characteristics of lines and attachment components.
2. Protocol analysers: Support the diagnosis of different protocol layers.
3. Tools from the Internet arena: Tools such as ping and traceroute will make up essential parts of a network maintenance kit.
4. Trouble ticker systems: Systems that would allow for monitoring and handling of problems.

More specific tools for wireless networks would include [Fli2a]:

1. A GPS that would assist with the initial positioning and error checking of antennas.
2. Topographical software that is regularly updated. The software would assist with initial installations as well as error checking when possible geographical anomalies might be to blame for failed connections.

One of the most powerful and currently the leading tool for hardware management is the Simple Network Management Protocol (SNMP) [MG95].

9.5 Simple Network Management Protocol

SNMP is a protocol that provides a mechanism to transport information between network components. Information such as device status, reports, performance measurements, alarms and general parameters are transferable over SNMP to capable managed devices.

Manipulation of device parameters also allows for any SNMP capable device to be managed by using SNMP and another capable device [MG95].

Creating a complete management system using SNMP would require five components, which are [MG95]:

1. Hardware platform: This is the actual system that the client software will run on, and it can range from a dedicated piece of hardware to a PC with an operating system such as Windows. In a wireless MAN the hardware platform will be very diverse but will very likely be normal PCs.
2. SNMP stack: Along with the stack, a collection of device parameters and variables such as device identifiers, permit administration and management of network devices are needed.

3. Transport layer: It is the transport layer's responsibility to transport information generated by the SNMP stack over the network to SNMP capable devices. An example of a transport layer protocol is TCP/IP.
4. Physical link: This is the connection the transport layer will use to convey information from one point to another. The vast majority of connections within a wireless MAN will be wireless, and as such will serve as the primary physical link.
5. Management application: It is the responsibility of the management application to analyse the information provided by the SNMP stack and present it in an understandable format. Many different vendors have management applications including Sun, IBM and HP. Open source or freeware alternatives will most likely be used due to their cost advantage.

The five components can be very diverse. For instance, the hardware platform may be a wireless access point or a router, and the management software can come from many different vendors. To keep complexity to a minimum the specifications of SNMP allow for the following considerations [MG95]:

1. Cost: The open nature of the specification allows for the costs of management applications to be minimized. Reduced cost will be of great importance within any open network.
2. Openness: The functions that a network device is capable of are not restricted and manufacturers can define their own functions to allow for the full utilization of their hardware.
3. Functionality: The implementation of SNMP is not platform-specific, meaning that a multitude of devices can implement the protocol, resulting in potential widespread deployment.
4. Availability: Due to the cost-effectiveness and unlimited functionality SNMP can be quickly implemented at a low cost.
5. Independence: The open and unrestricted functionality of SNMP allows for true hardware independent implementations, allowing for a management system that is functional on a true heterogeneous platform such as an open wireless MAN.

While the initial 1988 specification of SNMP was designed for Ethernet-based networks, support for other network types soon followed. These include Token Ring and Fiber Distributed Data Interface. SNMP support was also soon added to MAN technologies, making SNMP the standard management protocol for the communications industry [MG95]. The widespread acceptance across different communications indicates that SNMP is flexible and means that it could be adopted for MAN-specific hardware as well.

The functions of an SNMP capable device are defined by the management information bases (MIBs). There are different versions of MIBs and their development is ever-continuing [MG95]. This leaves vendors with an option of possible MIBs, and forces management software developers to support all versions of all possible MIBs. This will make the goal of a truly universal management system very difficult to achieve.

SNMP will be an essential tool in the management of any network. The distributed nature of a MAN and the diverse nature of the hardware due to the openness will mean that hardware will support different versions of SNMP and use different MIBs. Management software will have to be capable of functioning with devices that are diverse in their origin and functionality.

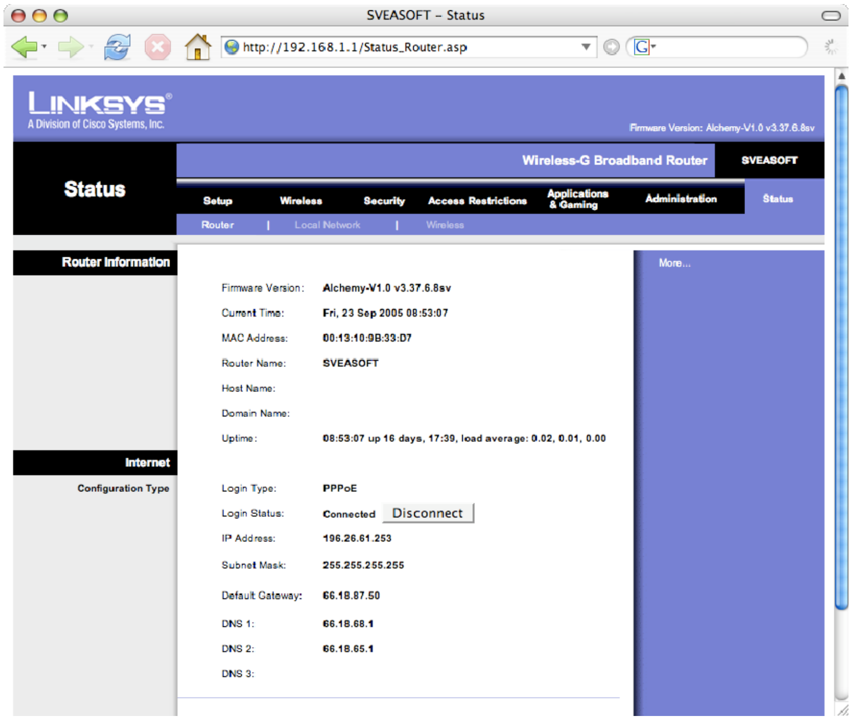
SNMP is an ideal management technology for an entire network. However, there are other issues that are more specific to wireless networks. As the vast majority of links will be wireless, it is important to discuss some of these wireless-specific issues.

9.6 Wireless Network Maintenance

The best way to ensure that an access point is functional is to actually be physically present and use the access point. However, with a network that is spread over a broad geographical area it could become very expensive and time-consuming to visit each physical site, and the ability to ping an access point is not adequate [HBR03]. Without actual physical insight into the status of the network point, decisions related to functionality cannot be made. For this reason every point of access should include some form of remote management [HBR03].

It should, however, be noted that access to the management software should be tightly controlled. Corporate networks cannot allow the wireless segment of their networks to be compromised. Allowing management software to be used over the wireless link can create a security backdoor. Thus access point management should only be possible over the wired segment of a network [KK03]. Within a public wireless MAN that covers a wide geographical area, it is not really an option to limit the management software to the wired segment of the network, as there really is no such segment. It is therefore recommended that the password to the access points be kept as secure and secret as possible, and that communications be secure, for example web-based management systems should be over HTTPS instead of unprotected HTTP [KK03].

There are a variety of possible methods for remote management. While many allow for management via a web interface or SNMP [Khw03], there are access points that utilize a proprietary system and require the use of custom software [Fli2a] [HBR03]. Fig 9.1 illustrates the Linksys WRT54G web interface and Fig 9.2 illustrates the Apple Airport management software.


SVEASOFT – Status
http://192.168.1.1/Status_Router.asp
LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: Alchemy-V1.0 v3.37.6.8sv
Wireless-G Broadband Router
SVEASOFT
Status
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Router | Local Network | Wireless
Router Information
More...
Internet
Configuration Type

Firmware Version: Alchemy-V1.0 v3.37.6.8sv

Current Time: Fri, 23 Sep 2005 08:53:07

MAC Address: 00:13:10:9B:33:D7

Router Name: SVEASOFT

Host Name:

Domain Name:

Uptime: 08:53:07 up 16 days, 17:39, load average: 0.02, 0.01, 0.00

Login Type: PPPoE

Login Status: Connected Disconnect

IP Address: 196.26.61.253

Subnet Mask: 255.255.255.255

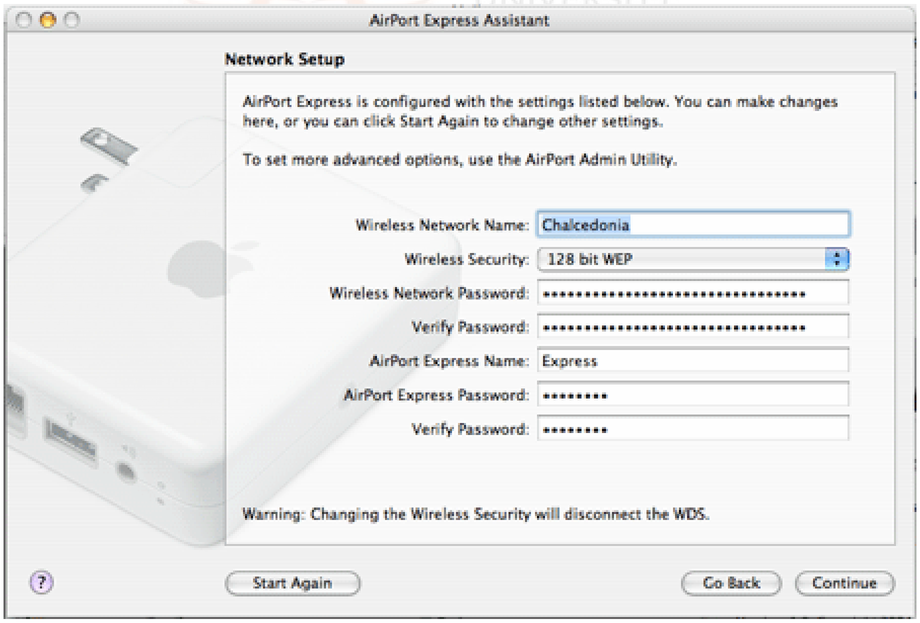
Default Gateway: 66.18.87.50

DNS 1: 66.18.68.1

DNS 2: 66.18.65.1

DNS 3:

Fig 9.1 – Linksys web management system



Network Setup

AirPort Express is configured with the settings listed below. You can make changes here, or you can click Start Again to change other settings.

To set more advanced options, use the AirPort Admin Utility.

Wireless Network Name: Chalcedonia

Wireless Security: 128 bit WEP

Wireless Network Password: ••••••••••••••••••••••••••••••••

Verify Password: ••••••••••••••••••••••••••••••••

AirPort Express Name: Express

AirPort Express Password: ••••••••

Verify Password: ••••••••

Warning: Changing the Wireless Security will disconnect the WDS.

Fig 9.2 – Apple Airport Management software

Remote management software is also essential when firmware upgrades are needed. Therefore an upgrade plan is needed that will address bug fixes, firmware updates as well as upgrading of technology [HBR03]. It is very difficult to have an upgrade plan that would encompass an entire metropolitan area when considering that there is no single owner. For this reason upgrades would very likely be at the will of the owners or upon request of the users.

The fundamental radio frequencies can also present problems [HBR03]. As mentioned in Chapter 3, tree foliage can influence the signal of outdoor wireless transmissions [Spu04]. This means that users might be able to connect during the winter months but have trouble during the summer months. Wind may move antennas and results will range from degraded performance to the complete loss of signal.

Within corporate environments and hotspots it is recommended that third-party audits be carried out frequently to ensure proper functionality [HBR03], but in a cost-sensitive open environment this is not a viable option. An alternative to third-party audits would be to have another nearby access point owner verify settings and their functionality. This would bring the independent view of a third party without the additional costs or complexities. The external third party would also bring knowledge that might assist in trouble shooting.

9.7 Maintenance and Management of a Wireless MAN

Each of the custom nodes defined in the Benade wireless MAN topology has its own maintenance and management issues due to its distinct functionality. Client nodes are concerned with the management of user access while backhaul nodes' primary concern is the stability and throughput of the connection.

As the Internet grew, Internet users started to abuse some of the services that were provided. An example is illegal file trading. ISPs were held responsible and they and hotspot owners were forced to start monitoring user activity to avoid legal actions against themselves [HBR03]. Within an open wireless MAN there is no single person to blame if something goes wrong. Access point owners might also not feel comfortable monitoring traffic due to privacy concerns. To eliminate any legal issues that may arise, the access point owners might request that clients agree to an end-user licence agreement. When legal action does have to be taken the client can be held responsible and crucial network nodes will be left unaffected.

For a client, ease of access would be the most important factor. However, if clients do not know about an access point in range, they will not be able to access the network. Just like with a hotspot, any client will have to be informed of the availability of the network. Information such as the SSID, obtaining login credentials or how to obtain any form of technical support must be made available somehow. Depending on the security of the access point, the user must also be informed of how to register for access and how to log in and out [HBR03].

Most advanced access points have the ability to monitor the RF side of the network as well [HBR03]. Since the entire wireless MAN will be built using RF links, the ability to monitor those RF statistics is of crucial importance, for not only the service provider, but all links including backhaul connections.

Hotspots are forced to use private IP addresses due to limited public addresses. This brings up many different complications, for example certain applications cannot function correctly from behind a network address translator (NAT) [HBR03]. A wireless MAN would also have to use a private address range. Along with the issues that hotspot owners face, address allocation will have to be handled with care and should be clearly managed.

9.8 Conclusion

Like traditional wired networks, wireless networks also require maintenance, and due to the wide area of deployment a wireless MAN will be more difficult to manage.

Many different types of tools are available to manage a network. Within the diversity of an open wireless MAN, different tools will be required for the many types of equipment that will be deployed. Although standardized protocols such as SNMP do exist, vendors can use a variety of different specifications in their deployment. There is also very likely to be equipment that forgoes SNMP and uses a custom proprietary technology. The diversity of SNMP and use of non-standard management systems will make an integrated network management system difficult.

The sheer diversity of SNMP implementations and proprietary tools means that there is no single software tool that will be able to manage all equipment in a wireless MAN, but multiple sets of tools could be used together for management purposes.

Diagnostic tools originating from the Internet will be invaluable; for example tools such as traceroute can be used to check for failures of certain connections. However, the best way to determine the status of a device is to physically be present within range of the device and use the device.

Along with maintenance, any network also has management issues. Adding and deleting users from access lists can be a daunting task considering the vast coverage area of a single access point, not to mention the entire network. Remote management software might be used but accessing it over the wireless link is a security risk, and should be used at the risk of the access point owner.

A method to distribute information about the network is also needed; information related to security as well as obtaining access cannot be easily accessed from the network itself and would need another method of distribution. Word of mouth, the Internet or even a newspaper can be used.

The management of any network is a difficult task; the distributed and diverse hardware of an open wireless MAN complicates matters considerably. Bad connections, broken connections throughout the network and other flaws will deter users from connecting, but over time experience would hopefully result in a stable, well-managed network. Increased growth will benefit the network as redundant links could be used to route traffic over what was initially destined for a disrupted connection.

The saving grace of an open network is that access is free and, provided the network has adequate coverage, it should encourage users to continue connecting to the network despite maintenance issues.

Chapter 10 - Conclusion

10.1 Conclusion

In this dissertation the possibility of constructing a wireless metropolitan area network was considered. The end goal of this dissertation was to provide a guide to the cheap construction of such a network. The network would be controlled by its users and would provide the users of the network with the ability to access services that they are currently unable to access over the South African telecommunications infrastructure. These services include a variety of broadband services such as streaming video.

While broadband services would very likely be the biggest reason for many people to build or utilize a MAN like the one outlined in this dissertation, such a network could be used for any function performed by a conventional network, but the large area of coverage does allow for a few additional functionalities.

With users of an existing network or one like the network outlined within this dissertation not being limited in any way, potential users can come from any field including the government sector, educational sector, corporate sectors ranging from small to big businesses as well as home and private users.

10.2 Possible Applications

Starting with possible applications for the government sector, city administration could use a public wireless MAN to make miscellaneous community information available to the public on a website; this could include information related to voting, voter registration, billing of public services, scheduling and any type of general information that the administration might need to distribute to the public. Additionally, emergency services could use a public wireless

MAN to distribute critical information to the public ranging from accident zones that are to be avoided to general home safety tips. In addition to relaying information to the public, a wireless MAN can also be used to detect and avoid disasters. An example of disaster recovery and detection could be an explosion at a power distribution facility. Cameras and sensors could be used to facilitate the detection of accidents or any dangerous situation; the correct steps could be taken to stop the explosion in time, and in the event that the explosion does take place, the public could be warned and the correct people could be notified automatically.

The educational sector can also greatly benefit from a wireless MAN. The cost-effective nature of the network outlined in this dissertation will allow for people in remote areas to access educational services. These services might range from full access to existing e-services offered by the educational institutions to full distance learning via video. As will be outlined in section 10.4, there are still many open research topics and an actual test network will make it easy for researchers to conduct the needed tests.

The business sector could also profit from a public wireless MAN. Both small and big businesses could offer their e-services cheaply to people using the network. This means that a small business could trail e-services with minimal financial risk, and bigger businesses could extend their client base to that previously beyond their reach. Larger organizations could allow their employees to work remotely and access corporate services via the wireless MAN. The MAN could also be used as a cheap alternative to expensive backhaul.

Even if a public wireless MAN were to be fully constructed and utilized, such a network would not replace commercial alternatives. Products such as iBurst and ADSL will always have a market as long as they offer products that have reach where a MAN has no coverage or they have international connectivity.

10.3 Dissertation Structure

A variety of issues in relation to the construction of such a network were considered. Chapter 5 indicated that there are already numerous such projects being executed worldwide, including in Johannesburg, this despite indications in Chapter 2 that locally such a network is illegal.

Chapters 3 and 4 reviewed current wireless technologies to determine their suitability in the construction of a wireless MAN. It was found that there is no ideal technology that offers everything needed, but current technologies are capable of providing basic connectivity.

Chapter 5 reviewed wireless topologies and found that no single topology is perfect, and more importantly few of them feature any security that would still allow for easy access, minimal management as well as high levels of security for all services. A custom topology was defined that attempts to overcome the limitations as well as maintain most of the advantages while keeping dynamic growth in mind.

Chapters 8 and 9 discussed the management and security issues of MANs. Both management and security are very difficult on open heterogeneous environments and a public wireless MAN is no exception. A hybrid security solution was proposed that allows for at least a few security requirements to be met.

10.4 Future Work

This dissertation set out only to provide a guide for the construction and management of a wireless MAN. It was, however, found that if the network is to feature the advantages of a true mesh network instead of a hybrid network, there is a considerable amount of research that still has to be conducted.

Mesh networks have limited scalability due to the routing protocols used. Increased latency due to the number of hops and the lack of implicit QoS within current wireless technologies make using a wireless mesh very difficult for delay sensitive services such as streaming real-time video. Better routing protocols can be researched and deployed as well as making all the levels of the OSI stack more aware of the new environment that a mesh introduces. On the physical layer alone there is the option to have multiple radios or MIMO systems. Without making the layers on higher levels aware of changes to lower levels, any enhancements to the lower level will not be utilized to their full potential. These changes complicate matters as changes to a single layer might cause a chain reaction that requires multiple levels to be modified.

Current measurement methods are not suited to the unique environment of a wireless mesh and should be reviewed before any of the above improvements are implemented.

In terms of security, mesh networks are primarily left out in the dark. Current wireless mesh vendors deploy proprietary security technologies that are not suited to the open and ad hoc environment of a mesh-based wireless MAN. While the Internet has brought about adequate security options on higher levels of the OSI stack, the physical layer is left unprotected and the ad hoc nature of an open network spread over a large geographical area complicates matters and could compound security risks.

Future technologies could also be added to a wireless MAN. As new technologies are released, they must also be reviewed as they in turn could result in many flaws being solved as well as introduce many more open issues that could be researched.

REFERENCE LIST

[3Co] 3Com®, *3Com® 4 dBi omnidirectional antenna.* Accessed on: 31/05/05 from: http://www.3com.com/images/products/en_US/prd_lg_3cwe490.jpg

[A0005] Poynting, *Bridgepoynt multipurpose (16dBi)*, Brochure (Product Code: WLAN-A0015). Accessed on: 04/01/06 from: http://www.poynting.co.za/antennas/pdf/wlan_a0015_broc_issue_1.pdf

[AC104] Atheros Communications Inc., *Atheros extended range XR technology*, Technical report. Accessed on: 18/10/05 from: http://www.atheros.com/pt/whitepapers/atheros_XR_whitepaper.pdf

[AC204] Atheros Communications Inc., *Super G: Maximizing wireless performance,* Technical report. Accessed on: 18/10/05 from: http://www.atheros.com/pt/whitepapers/atheros_superg_whitepaper.pdf

[AC304] Atheros Communications Inc., *Building a secure wireless network,* White Paper. Accessed on: 31/05/05 from: http://www.atheros.com/pt/whitepapers/atheros_security_whitepaper.pdf

[All05] Wi-Fi Alliance, *Deploying Wi-Fi protected access (WPA) and WPA2 in the enterprise,* White Paper, March 2005.

[Ame01] Sam Ames, *Broadcom gets sweet on bluetooth.* Accessed on: 15/10/05 from:http://news.com.com/Broadcom+gets+sweet+on+Bluetooth/2100-1033_3-267783.html

[ASW01] William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan, *Your 802.11 wireless network has no clothes*, Technical report. Department of Computer Science, University of Maryland, 2001.

[AWW04] Ian F. Akyildiz, Xudong Wang, and Weilin Wang, *Wireless Mesh Networks: A Survey*. Science Direct, 2004.

[AxS] *Axnode – seattlewireless*. Accessed on: 18/05/05 from: http://www.seattleWireless.net/index.cgi/AxNode

[BAB05] *Bristolwirelesswiki - about bristol wireless*. Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/AboutBristolWireless

[BARWN] The Bay Area Research Wireless Network: "The White Paper". Accessed on: 3/5/06 from: http://www.barwn.org/docs/White_Paper.pdf

[Bat91] Regis J Bates, *Disaster Recovery Planning Networks, Telecommunications, and Data Communications*. McGraw-Hill Inc., 1991.

[BBL02] Christian Barnes, Tony Bautts, Donald Lloyd, Eric Ouellet, Jeffrey Posiuns, David M. Zendziana, and Neal O'Farrell, *Hack Proofing your Wireless Network*. Syngress Publishing, Inc., 2002.

[BBN05] *Bristolwirelesswiki – become a node*. Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/BecomeANode

[Bel04] BelAir Networks. Capacity of wireless mesh networks. Accessed on: 01/03/05 from: http://www.belairnetworks.com/resources/whitepapers.cfm

[Bes02] Dr Steven R. Best, *Antenna performance and design considerations for optimum coverage in wireless communication systems*, White Paper. Accessed on: 31/05/05 from: http://www.cushcraft.com/comm/support/pdf/Antenna-Performance-C-14B37.pdf

[BGW01] Nikita Borisov, Ian Goldberg, and Davif Wagner, *Intercepting mobile communications: The insecurity of 802.11 intercepting mobile communications.* Annual International Conference on Mobile Computing and Networking, 2001.

[BJT05] *Bristolwirelesswiki - join the network.* Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/JoinTheNetwork

[BNH05] *Bristolwirelesswiki - node hardware*. Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/NodeHardware

[BNS105] *Bristolwirelesswiki - network speed.* Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/NetworkSpeed

[BNS205] *Bristolwirelesswiki - network security*. Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/NetworkSecurity

[Boa99] Bluetooth Quality Review Board, *Specification of the Bluetooth system*. Bluetooth Special Interest Group, 1999, Page 33.

[BWP05] *Bristolwirelesswiki - what protocols*. Accessed on: 26/07/05 from: http://www.bristolwireless.net/wiki/index.php/WhatProtocols

[BxS] *Bxnode – seattlewireless*. Accessed on: 18/05/05 from: http://www.seattlewireless.net/index.cgi/BxNode

[Cis] Cisco Inc., *Cisco Aironet 350 Series Access Points*, Datasheet. Accessed on: 03/01/06 from: http://www.cisco.com/warp/public/cc/pd/witc/ao350[Cis]ap/prodlit/carto_in.pdf

[CP02] David Cheung and Cliff Prettie, *A path loss comparison between the 5 GHz unii band (802.11a) and the 2.4 GHz ism band (802.11b)*, Intel, 2002. Accessed on: 18/10/05 from: http://sunstone.it/utenti/venezia/802_11a-vs-b_report.pdf

[CxS] *Cxnode – seattlewireless*. Accessed on: 18/05/05 from: http://www.seattlewireless.net/index.cgi/CxNode

[Dhi01] Amit Dhir, *The ABC's of 2.4 and 5GHz wireless LANs*, White Paper, 2001. Accessed on: 16/10/05 from: http://www.xilinx.com/esp/knowledge_center/collateral/wp148_wireless.pdf

[DS] Jr. David Steed, *The power of sensitivity improving range with receiver sensitivity*, White Paper. Accessed on: 18/10/05 from: http://www.maxstream.net/support/white-papers/the-power-of-sensitivity.pdf

[DxS] *Dxnode – seattlewireless*. Accessed on: 18/05/05 from: http://www.seattlewireless.net/index.cgi/DxNode

[Fit04] Kevin Fitchard, *The license game*, Telephony's Complete Guide to WiMAX (Electronic version), 2004.

[Fli03] Rob Flickenger, *Wireless Hacks*. O'Reilly, 2003.

[Fli2a] Rob Flickenger, *Building Wireless Community Networks*. O'Reilly, 2002.

[FPS05] *Frontpage - seattlewireless*. Accessed on: 18/05/05 from: http://www.seattlewireless.net/index.cgi/FrontPage

[Gas02] Matthew Gast, *802.11® Wireless Networks: The Definitive Guide*. O'Reilly, April 2002.

[Gei05] Jim Geier, *RF Math Made Easy*. Accessed on: 13/02/06 from: http://www.wi-fiplanet.com/tutorials/article.php/3525531

[Goh04] Nancy Gohring, *Unlicensed reborn*, Telephony's Complete Guide to WiMAX (Electronic version), 2004.

[Gri] Eric Griffith, *Channel bonding gets automatic*. Accessed on: 26/09/05 from: http://www.wi-fiplanet.com/news/article.php/3326671

[HA005] Poynting, *Wlan helical feed,* Brochure (Product Code: HELI-A0002). Accessed on: 03/01/06 from: http://www.poynting.co.za/antennas/pdf/heli_a0002_broc_issue_3.pdf

[HAN99] Heinz-Gerd Hegering, Sebastian Abeck, and Bernhard Neumair, *Integrated Management of Network Systems*. Morgan Kaufmann Publishers, Inc., 1999.

[Has] Abdul Hasib, *Prospect of wireless man in rural network infrastructure of Bangladesh*, White Paper. Accessed on: 18/10/05 from: http://www.buet.ac.bd/iict/hasib/IWIER%20paper.pdf

[HBR03] John Hammond, BartKessler, Juan Rivero, Chad Skinner, and Tim Sweeney, *Wireless Hotspot Deployment Guide.* Intel, 2003.

Accessed on: 16/10/05 from: http://mobilepipeline.bitpipe.com/detail/RES/1076340268_764.html

[HMC91] J. Houldsworth, M.Taylor, K. Caves, A. Flatman, and K. Crook, *Open system LANS and their global interconnection*, Electronics and Communications Reference Series. Butterworth-Heinemann Ltd, 1991.

[htt] *Sownwiki - home page.* Accessed on: 22/05/05 from:

http://www.sown.org.uk/

[ICA] ICASA. *Radio frequency (rf) equipment type*. Accessed on: 23/02/2005 from: http://www.icasa.org.za/default.aspx?

[ICA04] ICASA. 2004. *Government Gazette* (No. 27072 notice 2791).

[IEEE05] IEEE. Active IEEE 802.16 Task Groups and Study Groups. Accessed on 05/03/06 from: http://grouper.ieee.org/groups/802/16/tgs.html

[Int] Intel. *Understanding Wi-Fi and WiMAX as metro-access solutions*, White Paper. Accessed on: 16/10/05 from:

http://www.intel.com/netcomms/technologies/wimax/304471.pdf

[JBN1] *Jawug – basicnode*. Accessed on: 18/05/05 from:

http://www.jawug.za.net/BasicNode

[JBN2] *Jawug – backbonenode*. Accessed on: 18/05/05 from:

http://www.jawug.za.net/BacnodeNode

[JFP] *Jawug:frontpage*. Accessed on: 06/10/05 from: http://www.jawug.za.net/

[JNT] *Jawug:nodetypes*. Accessed on: 06/10/05 from: http://www.jawug.za.net/NodeTypes

[JTN] *Jawug – transitnode*. Accessed on: 18/05/05 from: http://www.jawug.za.net/TransitNode

[KK03] Jahanzeb Khan and Anis Khwaja, *Building Secure Wireless Networks with 802.11*. Wiley, 2003.

[Law71] G.R.P. Lawrence, *Cartographic Methods*. Butler & Tanner Ltd., 1971.

[Lig] LightPointe, *Optical wireless: Secure high-capacity bridging*, White Paper. Accessed on: 16/10/05 from: http://ostg.bitpipe.com/detail/RES/1099332381_268.html&src=TRM_TOPN

[Mar02] Roy Mark, *FCC amends part 15 wireless rules*, 2002. Accessed on: 16/10/05 from: http://wi-fiplanet.com/news/article.php/1136171

[MG95] Mathias Mein and David Griffiths, *SNMP Versions 1 & 2*. International Thomson Computer Press, 1995.

[Mil00] Miller Bret A, *Bluetooth Revealed.* Prentice Hall, 2000.

[Moo65] Gordon E. Moore, *Cramming more components into integrated circuits, Electronics*, 38(8):4, April 1965, Page 2.

[MyB05] MyBroadBand.co.za. *Myadsl: Broadband Internet community*. Accessed on: 12/10/05 from: http://www.mybroadband.co.za/nephp/?m=show&id=919

[Net04] Meru Networks, *Defining the requirements for third-generation wireless in security from location to application*, White Paper, 2004. Accessed on: 12/03/05 from: http://www.merunetworks.com/products_whitepapers.html

[O'S04] Dan O'Shea, *A standard argument: Why wimax will rule*, Telephony's Complete Guide to WiMAX (Electronic version), 2004.

[oSA00] Parliament of South Africa, *Independent Communications Authority of South Africa Act 13*, 2000, Page 4.

[oSA96] Parliament of South Africa, *Telecommunications Act*, 1996, November 1996.

[otICSA99] LAN/MAN Standards Committee of the IEEE Computer Society. *Part 11: wireless LAN medium access control (mac) and physical (phy) specifications: Higher-speed physical layer extension in the 5 GHz band,* Technical report, IEEE, 1999.

[otICSB99] LAN/MAN Standards Committee of the IEEE Computer Society. *Part 11: wireless LAN medium access control (mac) and physical (phy) specifications: Higher-speed physical layer extension in the 2.4 GHz band*, Technical report, IEEE, 1999.

[PH02] Robert Poor and Brent Hodges, *Reliable wireless networks for industrial systems*, White Paper, 2002. Accessed on: 16/10/05 from: http://www.ember.com/resources/whitepapers/reliable.html

[Poy] Poynting, *ISM products*. Accessed on: 31/05/05 from: http://www.poynting.co.za/antennas/ism.shtml

[Poy05] Poynting, *Vertically polarised omni-directional antenna*, Brochure (Product Code: OMNI-A0003). Accessed on: 3/01/06 from: http://www.poynting.co.za/antennas/pdf/omni-a0003_broc_issue_2.pdf

[PP] Tim Pozar and Matt Peterson, *The bay area wireless research network: "the white paper"*, White Paper. Accessed from: http://www.barwn.org/

[Pro] Proxim, Voice and data backhaul, Application Note. Accessed on: 16/10/05 from: http://www.proxim.com/solutions/backhaul/

[Rai48] Erwin Raisz, *General Cartography*. McGraw-Hill, 1948.

[SA005] Poynting, *Ism quad patch*, Brochure (Product code: PATCH-A0006). Accessed on: 02/01/06 from: http://www.poynting.co.za/antennas/pdf/patch-a0006_broc_issue_2.pdf

[Sha] Srikant Sharma, *Analysis of 802.11b MAC: A QOS, fairness, and performance perspective*. Accessed on: 16/10/05 from: http://www.ecsl.cs.sunysb.edu/tr/wlanrpe.pdf

[Sha99] William A. Shay, *Understanding Data Communications and Networks*. PWS Publishing, 2 edition, 1999.

[SHP] Sownwiki – home page. Accessed on: 01/03/05 from: http://www.sown.org.uk/

[Sim89] J. A. Simpson, *The Oxford English Dictionary*. Oxford University Press, 1989.

[Sla97] David Slack, *Microwave and RF cable assemblies: The neglected system component*. Applied Microwave & Wireless, pages 36, 38, 40, 42, 44, 45, November/December 1997.

[Spu04] Sputnik, *RF propagation basics*, White Paper, April 2004. Accessed on: 16/10/05 from: http://www.sputnik.com/docs/rf_propagation_basics.pdf

[STM] *Sownwiki - transparent mobility*. Accessed on: 22/05/05 from: http://www.sown.org.uk/index.php/TransparentMobility

[STP] *Sownwiki – topology*. Accessed on: 22/05/05 from: http://www.sown.org.uk/index.php/Topology

[SWS] *Securityissues – seattlewireless*. Accessed on: 24/10/05 from: http://www.seattlewireless.net/index.cgi/SecurityIssues

[tec] Radiall/Larsen Antenna technologies, *Basic antenna concepts*. Accessed on: 02/06/05 from: http://www.radialllarsen.com/technicalreference_basicantennaconcepts.htm

[Ter92] Kornel Terplan, *Communication Networks Management*, Prentice-Hall Inc., 1992.

[TMS02] Charles R. Elden and Tara M. Swaminatha, *Wireless Security and Privacy: Best Practices and Design Techniques*. Addison-Wesley, 2002.

[TMS04] Times Microwave Systems, *LMR wireless product catalog*, 2004.

[Tus04] Paul Tusini, *How to choose the best test cable*, *MICROWAVE PRODUCT DIGEST*, August 2004, Pages 10, 42.

[Viv] Vivato Inc., *Metropolitan wireless LAN/MAN deployment*, White Paper. Accessed on: 16/10/05 from: http://www.vivato.net/whitepapers/Technical_Whitepaper-Metro_Deployment.pdf

[vSE03] Sebastiaan H. von Solms and Jan H.P. Eloff, *Information Security*. B & D Printers, 2003.

[Wf] Wi-Fi.org, *Wi-fi protected access: Strong, standards-based, interoperable security for today's wi-fi networks*, White Paper. Accessed on: 16/10/05 from: http://www.wi-fi.org/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf

[Wir00] Wave Wireless, *Direct sequence vs. frequency hopping*, White Paper, 2000. Accessed on: 16/10/05 from: www.wavewireless.com/classroom/whitepapers/FHSSvDSSS.pdf

[WiS05] *Sownwiki - what is sown*. Accessed on: 22/05/05 from: http://www.sown.org.uk/index.php/WhatIsSown

[Woj04] Jeffrey Wojtiuk, *Bluetooth and wifi integration: Solving co-existence challenges*. RFDesign Magazine, October 2004, Page 20.

[XB04] Haidong Xia and Jose Brustoloni, *Detecting and blocking unauthorized access in wi-fi networks*. University of Pittsburg, Department of Computer Science, 2004, Accessed from: http://www.cs.pitt.edu/%7Ejcb/papers/net2004.pdf

[YA005] Poynting, *ISM yagi antenna*, Brochure (Product Code: YAGI-A0005). Accessed on: 02/01/06 from: http://www.poynting.co.za/antennas/pdf/yagi_a0005_broc_issue_3.pdf