PRINCIPLES OF WIRELESS NETWORKS

by

Nimota M. Ibrahim
PGD/MCS/2004/2005/1172

Submitted to the Department of Mathematics/Computer Science, Federal University of Technology, Minna in partial fulfillment for the award of Postgraduate Diploma in Computer Science.

April, 2006

CERTIFICATION

This is to certify that the project titled "Principles of Wireless Networks" was carried out by NIMOTA M. IBRAHIM in the Department of Mathematics/Computer Science, Federal University of Technology, Minna for the award of Postgraduate diploma in Computer Science

.....	.....
Mr. P.E. Ndajah	Date
Project Supervisor	

.....	.....
Dr. L.N. Ezaeko	Date
Head of Department	

.....	.....
External Examiner	Date

DEDICATION

This work is dedicated to my husband Mr. Abdulmumin Ajia

ACKNOWLEDGEMENT

First of all, I wish to acknowledge the contribution of my able lecturers especially Prof. K.R. Adeboye, the Head of Department, Dr. L.N. Ezeako, Dr. N.I. Akinwande, Dr. y.M. Aiyesinmi, Dr. Victor Onomza, Dr. A.A. Abubakar, my supervisor, Mr. P.E. Ndajah and all others who have been toiling to see that I have a wonderful time under them.

I also wish to acknowledge my family especially my husband Mr. Abdul Ajia and my mother Mrs. Ramota Ibrahim and my sisters Fausat, Biodun, Bimbo, Aishat and my friend Ann without encouragement this work would not have been possible.

ABSTRACT

Wireless networks are the reason why worldwide communication is possible. Understanding the principles of wireless networks is quite vital to progress in the information age. Outlined in this work are these principles that make wireless networking a possibility. Security of networks which becoming a dominant topic in networks is discussed. Different algorithms are available to ensure security of networks. Non of these methods is foolproof but improvements are in progress.

TABLE OF CONTENTS

Chapter One

1.1 Wireless Network *1*

1.2 Wireless Networking Protocols *1*

1.3 Radio Physics 3

3.4 Bandwidth *7*

1.5 Absorption 10

1.6 Understanding the Fresnel zone 16

CHAPTER TWO

2.1 Designing the Physical Network *20*

2.2 The TCP/IP Model 23

2.3 Link planning 33

2.4 TCP/IP factors over a satellite connection 34

2.5 Long Round-Trip Time (RTT) 35

2.6 Transmission Errors 37

CHAPTER THREE

3.1 Waveguides *39*

3.2 Antennas and Radiation patterns *40*

3.3 Types of Antennas 42

3.4 Amplifiers *47*

3.5 Networking Hardware 49

3.6 Professional wireless products *52*

CHAPTER FOUR

4.0 Security 58

4.1 Wireless Network Security 58

4.2 Physical security *60*

4.3 Threats to the network *62*

4.4 Authentication *66*

4.5 Privacy *72*

CHAPTER FIVE

5.1 Conclusion 79

5.2 Recommendations 79

References

CHAPTER ONE

WIRELESS NETWORK

A wireless network is a network that does not use a physical medium for the purpose of data transmission. However it is difficult not to have some sort of wiring even in wireless networks. If you are a network administrator, you may wonder how wireless might fit into your existing network infrastructure. Wireless can serve in many capacities, from a simple extension (like a several kilometer Ethernet cable) to a distribution point (like a large hub).

1.2 Wireless Networking Protocols

The primary technology used for building low-cost wireless networks is currently the 802.11 family of protocols, also known in many circles as *Wi-Fi* The 802.11 family of radio protocols (802.11a, 802.11b, and 802.11g) have enjoyed an incredible popularity in the United States and Europe. By implementing a common set of protocols, manufacturers world wide have built highly interoperable equipment. This decision has proven to be a significant boon to the industry and the consumer. Consumers are able to use equipment that implements 802.11 without fear of "vendor lock-in". As a result, consumers are able to purchase low-cost equipment at a volume which has benefited manufacturers There are many protocols in the 802.11 family, and not all are directly related to the radio protocol itself. The three wireless standards currently implemented in most readily available gear are:

• 802.11b. Ratified by the IEEE on September 16, 1999, 802.11b is probably the most popular wireless networking protocol in use today. Millions of devices supporting it have shipped since 1999. It uses a modulation called *Direct Sequence Spread Spectrum (DSSS)* in a portion of the ISM band from 2.412 to 2.484GHz. It has a maximum rate of 11Mbps, with actual usable data speeds up to about 5Mbps.

• 802.11g. As it wasn't finalized until June 2003, 802.11g is a relative late-comer to the wireless marketplace. Despite the late start, 802.11g is now the de facto standard wireless networking protocol as it now ships as a standard feature on virtually all laptops and most handheld devices.

802.11g uses the same ISM range as 802.11b, but uses a modulation scheme called *Orthogonal*

Frequency Division Multiplexing (OFDM). It has a maximum data rate of 54Mbps (with usable throughput of up to 25Mbps), and can fall back to 11Mbps DSSS or slower for backwards compatibility with the hugely popular 802.11b.

• 802.11a. Also ratified by the IEEE on September 16, 1999, 802.11a uses OFDM. It has a maximum data rate of 54Mbps, with actual throughput of up to 27Mbps. 802.11a operates in the ISM band between 5.745 and 5.805GHz, and in a portion of the UNII band between 5.170 and

5.320GHz. This makes it incompatible with 802.11b or 802.11g, and the higher frequency means shorter range compared to 802.11b/g at the same power. While this portion of the spectrum is relatively unused compared to 2.4GHz, it is unfortunately only legal for use in a few parts of the world. Check with your local

authorities before using 802.11a equipment, particularly in outdoor applications. 802.11a equipment is still quite inexpensive, but is not nearly as popular as 802.11b/g. In addition to the above standards, there are a number of vendor-specific extensions to equipment, touting speeds of 108Mbps, stronger encryption, and increased range. Unfortunately these extensions will not operate between equipment from different manufacturers, and purchasing them will effectively lock you into that vendor for every part of your network. New equipment and standards (such as 802.11n, 802.16, MIMO, and WiMAX) promise significant increases in speed and reliability, but this equipment is just starting to ship at the time of this writing, and availability and vendor interoperability is unclear.

1.3 Radio Physics

Wireless communications make use of electromagnetic waves to send signals across long distances. From a user's perspective, wireless connections are not particularly different from any other network connection: your web browser, email, and other applications all work as you would expect. But radio waves have some unexpected properties compared to Ethernet cable.

For example, it's very easy to see the path that an Ethernet cable takes: locate the plug sticking out of your computer, follow the cable to the other end, and you have found it! Running many Ethernet cables alongside each other won't cause problems, since the cables effectively keep their signals contained within the wire itself. But how do you know where the waves emanating from your wireless card

are going? What happens when these waves bounce off of objects in the room or other buildings in an outdoor link? How can several wireless cards be used in the same area without interfering with each other? In order to build stable high-speed wireless links, it is important to understand how radio waves behave in the real world.

What is a wave?

We are all familiar with vibrations or oscillations in various forms: a pendulum, a tree swaying in the wind, the string of a guitar - these are all examples of oscillations. What they have in common is that something, some medium or object, is swinging in a periodic manner, with a certain number of cycles per unit of time. This kind of wave is sometimes called a *mechanical* wave, since it is defined by the motion of an object or its propagating medium. When such oscillations travel (that is, when the swinging does not stay bound to one place) then we speak of waves propagating in space. For ex-ample, a singer singing creates periodic oscillations in his or her vocal cords. These oscillations periodically compress and decompress the air, and this periodic change of air pressure then leaves the singers mouth and travels, at the speed of sound. A stone plunging into a lake causes a disturbance, which then travels across the lake as a *wave*.

A wave has a certain *speed*, *frequency*, and *wavelength*. These are connected by a simple relation:

Speed =Frequency *Wavelength

The wavelength (sometimes referred to as lambda) is the distance measured from a point on one wave to the equivalent part of the next, for example from the top of one peak to the next. The frequency is the number of whole waves that pass a fixed point in a period of time. Speed is measured in meters/second, frequency is measured in cycles per second (or Hertz, abbreviated *Hz*), and wavelength is measured in meters. For example, if a wave on water travels at one meter per second, and it oscillates five times per second, then each wave will be twenty centimeters long:

1 meter/second =5 cycles/second *W

W =1 /5 meters

W =0.2 meters =20 cm

Waves also have a property called *amplitude*. This is the distance from the center of the wave to the extreme of one of its peaks, and can be thought of as the "height" of a water wave. Waves in water are easy to visualize. Simply drop a stone into the lake and you can see the waves as they move across the water over time.

Electromagnetic forces

Electromagnetic forces are the forces between electrical charges and cur-rents. Our most direct access to those is when our hand touches a door handle after walking on synthetic carpet, or brushing up against an electrical fence. A more

powerful example of electromagnetic forces is the lightning we see during thunderstorms. The *electrical force* is the force between electrical charges. The *magnetic force* is the force between electrical currents. Electrons are particles that carry a negative electrical charge. There are other particles too, but electrons are responsible for most of what we need to know about how radio behaves.

Let us look at what is happening in a piece of straight wire, in which we push the electrons from one and to the other and back, periodically. At one moment, the top of the wire is negatively charged - all the negative electrons are gathered there. This creates an electric field from plus to minus along the wire. The next moment, the electrons have all been driven to the other side,

and the electric field points the other way. As this happens again and again, the electric field vectors (arrows from plus to minus) are leaving the wire, so to speak, and are radiated out into the space around the wire. What we have just described is known as a dipole (because of the two poles, plus and minus), or more commonly a *dipole antenna*. This is the simplest

form of omnidirectional antenna. The motion of the electric field is commonly referred to as an *electromagnetic wave*.

Let us come back to the relation:

Speed =Frequency *Wavelength

In the case of electromagnetic waves, the speed is c, the speed of light.

c =300,000 km/s =300,000,000 m/s =3*10 8 m/s

c =f *λ

Electromagnetic waves differ from mechanical waves in that they require no medium in which to propagate. Electromagnetic waves will even propagate through the vacuum of space.

3.4 Bandwidth

A term you will meet often in radio physics is *bandwidth*. Bandwidth is simply a measure of frequency range. If a range of 2.40 GHz to 2.48 GHz is used by a device, then the bandwidth would be 0.08 GHz (or more commonly stated as 80MHz).

It is easy to see that the bandwidth we define here is closely related to the amount of data you can transmit within it - the more room in frequency space, the more data you can fit in at a given moment. The term bandwidth is often used for something we should rather call a data rate, as in "my Internet connection has 1 Mbps of bandwidth", meaning it can transmit data at 1
megabit per second.

Behaviour of radio waves

There are a few simple rules of thumb that can prove extremely useful when making first plans for a wireless network:

- The longer the wavelength, the further it goes
- The longer the wavelength, the better it travels through and around things
- The shorter the wavelength, the more data it can transport

Longer waves travel further

Assuming equal power levels, waves with longer wavelengths tend to travel further than waves with shorter wavelengths. This effect is often seen in FM radio, when comparing the range of an FM transmitter at 88MHz to the range at 108MHz. Lower frequency transmitters tend to reach much greater distances than high frequency transmitters at the same power.

Longer waves pass around obstacles

A wave on water which is 5 meters long will not be stopped by a 5 mm piece of wood sticking out of the water. If instead the piece of wood were 50 meters big (e.g. a ship), it would be well in the way of the wave. The distance a wave can travel depends on the relationship between the wavelength of the wave and the size of obstacles in its path of propagation. It is harder to visualize waves moving "through" solid objects, but this is the case with electromagnetic waves. Longer wavelength (and therefore lower frequency) waves tend to penetrate objects better than shorter wavelength (and therefore higher frequency) waves. For example, FM radio (88-108MHz) can travel through buildings and other obstacles easily, while shorter waves (such as GSM phones operating at 900MHz or 1800MHz) have a harder time penetrating buildings. This effect is partly due to the difference in power levels used for FM radio and GSM, but is also partly due to the shorter wavelength of GSM signals.

Shorter waves can carry more data

The faster the wave swings or beats, the more information it can carry –every beat or cycle could for example be used to transport a digital bit, a '0' or a '1', a 'yes' or a 'no'. There is another principle that can be applied to all kinds of waves, and which is extremely useful for understanding radio wave propagation. This principle is known as the *Huygens Principle*, named after Christiaan Huygens, Dutch mathematician, physicist and astronomer 1629 - 1695.

Imagine you are taking a little stick and dipping it vertically into a still lake's surface, causing the water to swing and dance. Waves will leave the center of the stick - the place where you dip in - in circles. Now, wherever water particles are swinging and dancing, they will cause their neighbour particles to do the same: from every point of disturbance, a new circular wave will start.

This is, in simple form, the Huygens principle. In the words of *wikipedia.org*:

"The Huygens' principle is a method of analysis applied to problems of wave propagation in the far field limit. It recognizes that each point of an advancing wave front is in fact the center of a fresh disturbance and the source of a new train of waves; and that the advancing wave as a whole may be regarded as the sum of all the secondary waves arising from points in the medium already traversed. This view of wave propagation helps better understand a variety of wave phenomena, such as diffraction."

This principle holds true for radio waves as well as waves on water, for sound as well as light - only for light the wavelength is far too short for human beings to actually see the effects directly.

This principle will help us to understand diffraction as well as Fresnel zones, the need for line of sight as well as the fact that sometimes we seem to be able to go around corners, with no line of sight. Let us now look into what happens to electromagnetic waves as they travel.

1.5 Absorption

When electromagnetic waves go through 'something' (some material), they generally get weakened or dampened. How much they lose in power will depend on their frequency and of course the material. Clear window glass is obviously transparent for light, while the glass used in sunglasses filer out quite a share of the light intensity and also the ultraviolet radiation. Often, an absorption coefficient is used to describe a materials impact on radiation. For microwaves, the two main absorbent materials are:

• Metal. Electrons can move freely in metals, and are readily able to swing and thus absorb the energy of a passing wave.

• Water. Microwaves cause water molecules to jostle around, thus taking away some of the waves energy may well consider metal and water perfect absorbers: we will not be able to go through them (al-though thin layers of water will let some power pass). They are to microwave what a brick wall is to light. When talking about water, we have to remember that it comes in different forms: rain,

fog and mist, low clouds and so forth all will be in the way of radio links. They have a strong influence, and in many circumstances a change in weather can bring a radio link down.

There are other materials that have a more complex effect on radio absorption. For trees and wood, the amount of absorption depends on how much water they contain. Old dead dry wood is more or less transparent, wet fresh wood will absorb a lot.

Plastics and similar materials generally do not absorb a lot of radio energy-but this varies depending on the frequency and type of material. Before you build a component from plastic (e.g. weather protection for a radio device and its antennas), it is always a good idea to measure and verify that the material does not absorb radio energy around 2.4GHz. One simple method
of measuring the absorption of plastic at 2.4GHz is to put a sample in a microwave oven for a couple of minutes. If the plastic heats up, then it absorbs radio energy and should not be used for weatherproofing.

Lastly, let us talk about ourselves: humans (as well as other animals) are largely made out of water. As far as radio networking is concerned, we may well be described as big bags of water, with the same strong absorption. Orienting an office access point in such a way that its signal must pass through many people is a key mistake when building office networks. The same goes
for hotspots, cafe installations, libraries, and outdoor installations.

Reflection

Just like visible light, radio waves are reflected when they come in contact with materials that are suited for that: for radio waves, the main sources of reflection are metal and water surfaces. The rules for reflection are quite simple: the angle at which a wave hits a surface is the same angle at which it gets deflected. Note that in the eyes of a radio wave, a dense grid of bars acts just the same as a solid surface, as long as the distance between bars is small compared to the wavelength. At 2.4GHz, a one cm metal grid will act much the same as a metal plate. Although the rules of reflection are quite simple, things can become very complicated when you imagine an office interior with many small metal objects of various complicated shapes. The same goes for urban situations: look around you in city environment and try to spot all of the metal objects. This explains why *multipath effects* (i.e. signal reaching their target along different paths, and therefore at different times) play such an important role in wireless networking. Water surfaces, with waves and ripples changing all the time, effectively make for a very complicated reflection object which is more or less impossible to calculate and predict precisely. We should also add that polarization has an impact: waves of different polarization in general will be reflected differently. We use reflection to our advantage in antenna building: e.g. we put huge parabolas behind our radio transmitter/receiver to collect and bundle the radio signal into a fine point.

Diffraction

Diffraction is the apparent bending of waves when hitting an object. It is the effect of "waves going around corners". Imagine a wave on water traveling in a straight wave front, just like a wave that we see rolling onto an ocean beach. Now we put a solid barrier, say a wooden solid fence, in its way to block it. We cut a narrow slit opening into that wall, like a small door. From this opening, a circular wave will start, and it will of course reach points that are not in a direct line behind this opening, but also on either side of it. If you look at this wavefront - and it might just as well
be an electromagnetic wave - as a beam (a straight line), it would be hard to explain how it can reach points that should be hidden by a barrier. When modeled as a wavefront, the phenomenon makes sense.

The Huygens Principle provides one model for understanding this behavior. Imagine that at any given instant, every point on a wave front can be considered the starting point for a spherical "wavelet". This idea was later extended by Fresnel, and whether it adequately describes the phenomenon is still a matter of debate. But for our purposes, the Huygens model describes the
effect quite well.

Through means of the effect of diffraction, waves will "bend" around corners or through an opening in a barrier. The wavelengths of visible light are far too small for humans to observe this effect directly. Microwaves, with a wave-length of several centimeters, will show the effects of diffraction when waves hit walls,

mountain peaks, and other obstacles. It seems as if the obstruction causes the wave to change its direction and go around corners.

Note that diffraction comes at the cost of power: the energy of the diffracted wave is significantly less than that of the wave front that caused it. But in some very specific applications, you can take advantage of the diffraction effect to circumvent obstacles.

Interference

When working with waves, one plus one does not necessarily equal two. It can also result in zero.

This is easy to understand when you draw two sine waves and add up the amplitudes. When peak hits peak, you will have maximum results (1 + 1 = 2).

This is called *constructive interference*. When peak hits valley, you will have complete annihilation ((1 + (-)1 = 0) - *destructive interference*.

This can actually be tried with waves on water and two little sticks to create circular waves - you will see that where two waves cross, there will be areas of higher wave peaks and others that remain almost flat and calm. In order for whole trains of waves to add up or cancel each other out perfectly, they would have to have the exact same wavelength and a fixed phase relation, this means fixed positions from the peaks of the one wave to the other's.

In wireless technology, the word Interference is typically used in a wider sense, for disturbance through other RF sources, e.g. neighbouring channels. So, when wireless networkers talk about interference they typically talk about all kinds of disturbance by other networks, and other sources of microwave. Interference is one of the main sources of difficulty in building wireless links, especially in urban environments or closed spaces (such as a conference space) where many networks may compete for use of the spectrum.

Whenever waves of equal amplitude and opposite phase cross paths, the wave is annihilated and no signal can be received. The much more common case is that waves will combine to form a completely garbled waveform that cannot be effectively used for communication. The modulation techniques and use of multiple channels help to deal with the problem of interference,

but does not completely eliminate it.

Line of sight

The term *line of sight*, often abbreviated as *LOS*, is quite easy to under-stand when talking about visible light: if we can see a point B from point A where we are, we have line of sight. Simply draw a line from A to B, and if nothing is in the way, we have line of sight.

Things get a bit more complicated when we are dealing with microwaves. Remember that most propagation characteristics of electromagnetic waves scale with their wavelength. This is also the case for the widening of waves as they

travel. Light has a wavelength of about 0.5 micrometers, microwaves as used in wireless networking have a wavelength of a few centimeters.

Consequently, their beams are a lot wider - they need more space, so to speak. Note that visible light beams widen just the same, and if you let them travel long enough, you can see the results despite of their short wavelength. When pointing a well focused laser at the moon, its beam will widen to well over 100 meters in radius by the time it reaches the surface. You can see this effect for yourself using an inexpensive laser pointer and a pair of binoculars on a clear night. Rather than pointing at the moon, point at a distant mountain or unoccupied structure (such as a water tower). The radius of your beam will increase as the distance increases. The line of sight that we need in order to have an optimal wireless connection

from A to B is more than just a thin line - its shape is more like that of a cigar, an ellipse. Its width can be described by the concept of Fresnel zones.

1.6 Understanding the Fresnel zone

The exact theory of Fresnel (pronounced "Fray-nell") zones is quite complicated. However, the concept is quite easy to understand: we know from the Huygens principle that at each point of a wavefront new circular waves start, We know that microwave beams widen. We know that waves of one frequency can interfere with each other. Fresnel zone theory simply looks at a line from A to B, and then at the space around that line that contributes to what is arriving at point B. Some waves travel directly from A to B, while others travel on paths off axis.

Consequently, their path is longer, introducing a phase shift between the direct and indirect beam. Whenever the phase shift is one full wavelength, you get constructive interference: the signals add up optimally. Taking this approach and calculating accordingly, you find there are ring zones around the direct line A to B which contribute to the signal arriving at point B.

Here is one formula for calculating the first Fresnel zone:

r =17.31 *sqrt(N(d1*d2)/(f*d))

where r is the radius of the zone in meters, N is the zone to calculate, d1 and d2 are distances from obstacle to the link end points in meters, d is the total link distance in meters, and f is the frequency in MHz. Note that this gives you the radius of the zone. To calculate the height above ground, you need to subtract the result from a line drawn directly between the tops of the

two towers. For example, let's calculate the size if the first Fresnel zone in the middle of a

2km link, transmitting at 2.437GHz (802.11b channel 6): r =17.31 sqrt(1 *(1000 *1000)/(2437 *2000))r =17.31 sqrt(1000000 /4874000)

r =7.84 meters

Assuming both of our towers were ten meters tall, the first Fresnel zone would pass just 2.16 meters above ground level in the middle of the link. But how tall could a structure at that point be to clear 60% of the first zone? r =17.31 sqrt(0.6 *(1000 *1000)/(2437 *2000))

r =17.31 sqrt(600000 /4874000) r =6.07 meters

Subtracting the result from 10 meters, we can see that a structure 3.93 meters tall at the center of the link would block up to 60% of the first Fresnel zone. To improve the situation, we would need to position our antennas higher up, or change the direction of the link to avoid the obstacle.

CHAPTER TWO

LITERATURE REVIEW

2.0 NETWORK DESIGN

Before purchasing equipment or deciding on a hardware platform, you should have a clear idea of the nature of your communications problem. Most likely, you are reading this book because you need to connect computer networks together in order to share resources and ultimately reach the larger global Internet. The network design you choose to implement should fit the communications problem you are trying to solve. Do you need to connect a re-mote site to an Internet connection in the center of your campus? Will your network likely grow to include several remote sites? Will most of your net-work components be installed in fixed locations, or will your network expand to include hundreds of roaming laptops and other devices?

When solving a complex problem, it is often useful to draw a picture of your resources and problems. In this chapter, we will look at how other people have built wireless networks to solve their communication problems, including diagrams of the essential network structure. We will then cover the net-working concepts that define TCP/IP, the primary networking language currently spoken on the Internet. We will then demonstrate several common methods for getting your information to flow efficiently through your network and on to the rest of the world.

2.1 *Designing the Physical Network*

It may seem odd to talk about the "physical" network when building wireless networks. After all, where is the physical part of the network? In wireless networks, the physical medium we use for communication is obviously electromagnetic energy. But in the context of this chapter, the physical net-work refers to the mundane topic of where to put things. How do you ar-range the equipment so that you can reach your wireless clients? Whether 27.they fill an office building or stretch across many miles, wireless networks are naturally arranged in these three logical configurations:

- Point-to-point links
- Point-to-multipoint links
- Multipoint-to-multipoint clouds

The physical network layout you choose will depend on the nature of the problem you are trying to solve. While different parts of your network can take advantage of all three of these configurations, any individual link will fall into one of the above topologies. The application of each of these topologies is best described by example.

Point-to-point

Point-to-point links typically provide an Internet connection where such access isn_t otherwise available. One side of a point-to-point link will have an Internet connection, while the other uses the link to reach the Internet. For example, a

university may have a fast frame relay or VSAT connection in the middle of campus, but cannot afford such a connection for an important
building just off campus. If the main building has an unobstructed view of the remote site, a point-to-point connection can be used to link the two together. This can augment or even replace existing dial-up links. With proper antennas and clear line of sight, reliable point-to-point links in excess of thirty kilo-meters are possible.

Point-to-multipoint

The next most commonly encountered network layout is ***point-to-multipoin***t. Whenever several nodes are talking to a central point of access, this is a point-to-multipoint application. The typical example of a point-to-multipoint layout is the use of a wireless access point that provides a connection to several laptops. The laptops do not communicate with each other directly, but must be in range of the access point in order to use the network.

A classic example of a wide area ***point*** (remote site on the hill) ***to multipoint*** (many buildings in the valley below) connection. Note that there are a number of performance issues with using point-to-multipoint over very long distance, which will be addressed later in this chapter. Such links are possible and useful in many circumstances, but don't make the classic mistake of installing a single high powered radio tower in the middle of town and expecting to be able to serve

thousands of clients, as you would with an FM radio station. As we will see, data networks behave very differently than broadcast radio.

Multipoint-to-multipoint

The third type of network layout is ***multipoint-to-multipoin***t, which is also referred to as an ***ad-hoc*** or ***mesh*** network. In a multipoint-to-multipoint net-work, there is no central authority. Every node on the network carries the traffic of every other as needed, and all nodes communicate with each other directly. The benefit of this network layout is that even if none of the nodes are in range of a central access point, they can still communicate with each other. Good mesh network implementations are self-healing, in that they automatically detect routing problems and fix them as needed. Extending a mesh network is as simple as adding more nodes. If one of the nodes in the "cloud" happens to be an Internet gateway, then that connection can be shared among all of the clients.

Two big disadvantages to this topology are increased complexity and lower performance. Security in such a network is also a concern, since every participant potentially carries the traffic of every other. Multipoint-to-multipoint networks tend to be complicated to troubleshoot, due to the large number of changing variables as nodes move around. Multipoint-to-multipoint clouds typically do not have the same capacity as point-to-point or point-to-multipoint networks, due to the additional overhead of managing the network routing and

increased contention in the radio spectrum. Nevertheless, mesh networks are useful in many circumstances.

The Logical Network

Communication is only possible when the participants speak a common language. But once the communication becomes more complex than a simple ongoing broadcast, ***protocol*** becomes just as important as language. All of the people in an auditorium may speak English, but without a set of rules in place to establish who has the right to use the microphone, the communication of an individual's ideas to the entire room is nearly impossible. Now imagine an auditorium as big as the world, full of all of the computers that exist. Without a common set of communication protocols to regulate when and how each computer can speak, the Internet would be a chaotic mess where every machine tries to speak at once. ***TCP/IP*** refers to the suite of protocols that permit conversations to happen on the global Internet. By understanding TCP/IP, you can build networks that will scale to virtually any size, and will ultimately become part of the global Internet.

2.2 The TCP/IP Model

Data networks are often described as being built on many layers. Each layer depends on the operation of all of the underlying layers before communication can take place, but only needs to exchange data with the layer above or beneath it. The TCP/IP model of networking describes five layers

- *Physical*
- *Physical*
- *Data Link*
- *Internet*
- *Transport*
- *Application*

The ***physical layer*** is the physical medium over which communications take place. This can be a copper CAT5 cable, a fiber optic bundle, radio waves, or just about any other medium. The next layer up is referred to as the ***data link layer***. Whenever two or more nodes share the same physical medium (for example, several computers plugged into a hub, or a room full of laptops all using the same radio

channel) they use the data link layer to determine whose turn it is to transmit on the medium. Common examples of data link protocols are Ethernet, Token Ring, ATM, and the wireless networking protocols (802.11a/b/g). Communication on this layer is said to be ***link local***, since all nodes connected at this layer can communicate with each other directly. On networks modeled

after Ethernet, nodes are referred to by their ***MAC address***, which is a unique 48 bit number assigned to every networking device when it is manufactured.

Just above the data link layer is the ***Internet layer***. For TCP/IP, this is the Internet Protocol ***(I***P). At the Internet layer, packets can leave the link local network and be retransmitted on other networks. Routers perform this function on

a network by having at least two network interfaces, one on each of the networks to be interconnected. Nodes on the Internet are reached by their globally unique ***IP address***s. Once Internet routing is possible, a method is needed to reach a particular service at a given IP address. This function is filled by the next layer, the ***transport laye***r. TCP and UDP are common examples of transport layer protocols. Some protocols at the transport layer (such as TCP) ensure that all of the data has arrived at the destination, and is reassembled and delivered to the next layer in the proper order. Finally, at the top of the pile we have the ***application laye***r. This is the layer that most network users are exposed to, and is the level at which human communication happens. HTTP, FTP, and SMTP are all application layer protocols. The human sits at the top of all of the layers, and needs little or no knowledge of the layers beneath to effectively use the network.

One way to look at the TCP/IP model is to think of a person delivering a letter to an office building downtown. They first need to interact with the road itself (the physical layer), pay attention to other traffic on the road (the data link layer), turn at the proper place to connect to other roads and arrive at the correct address (the Internet layer), go to the proper floor and room number
(the transport layer), and finally find the recipient or a receptionist who can take the letter from there (the application layer). The five layers can be easily remembered by using the mnemonic "Please Don't Look In The Attic," which of course stands for "Physical / Data Link / Internet / Transport / Application." Before packets can be forwarded and routed to the Internet, layers one (the

physical) and two (the data link) need to be connected. Without link local connectivity, network nodes cannot talk to each other and route packets. To provide physical connectivity, wireless network devices must operate in the same part of the radio spectrum. As we saw in chapter two, this means that 802.11a radios will talk to 802.11a radios at around 5GHz, and 802.11b/g radios will talk to other 802.11b/g radios at around 2.4GHz. But an 802.11a device cannot interoperate with an 802.11b/g device, since they use completely different parts of the electromagnetic spectrum.

.More specifically, wireless cards must agree on a common channel. If one 802.11b radio card is set to channel 2 while another is set to channel 11, then the radios cannot communicate with each other. When two wireless cards are configured to use the same protocol on the same radio channel, then they are ready to negotiate data link layer connectivity. Each 802.11a/b/g device can operate in one of four possible modes:

1. ***Master mode*** (also called ***AP*** or ***infrastructure mode***) is used to create a service that looks like a traditional access point. The wireless card creates a network with a specified name (called the ***SSID***) and channel, and offers network services on it. While in master mode, wireless cards

manage all communications related to the network (authenticating wire-less clients, handling channel contention, repeating packets, etc.) Wireless cards in master mode can only communicate with cards that are associated with it in managed mode.

2. ***Managed mode*** is sometimes also referred to as ***client*** mode. Wireless cards in managed mode will join a network created by a master, and will automatically change their channel to match it. They then present any necessary credentials to the master, and if those credentials are accepted, they are said to be ***associated*** with the master. Managed mode cards do not communicate with each other directly, and will only communicate with an associated master.

3. ***Ad-hoc mode*** creates a multipoint-to-multipoint network where there is no single master node or AP. In ad-hoc mode, each wireless card communicates directly with its neighbors. Nodes must be in range of each other to communicate, and must agree on a network name and channel.

4. ***Monitor mode*** is used by some tools (such as Kismet, chapter six) to passively listen to all radio traffic on a given channel. When in monitor mode, wireless cards transmit no data. This is useful for analyzing problems on a wireless link or observing spectrum usage in the local area. Monitor mode is not used for normal communications. When implementing a point-to-point or point-to-multipoint link, one radio will typically operate in master mode, while the other(s) operate in managed mode. In a multipoint-to-multipoint mesh, the radios all operate in ad-hoc mode so that they can communicate with each other directly.

Internet networking

IP addresses, network addressing, routing, and forwarding are important and related concepts in Internet networking. An ***IP address*** is an identifier for a network node such as a PC, server, router, or bridge. ***Network addressing*** is the system used to assign these identifiers in convenient groups. ***Routing*** keeps track of where in the network these groups may be found. The results of the routing process is kept in a list called a ***routing table***. ***Forwarding*** is the action of using the routing table to send a data packet to either the final destination or to the "next hop" which is closer to the destination.

IP addresses

In an IP4 network, the address is a 32-bit number, normally written as four 8-bit numbers expressed in decimal form, separated by periods. Examples of IP addresses are 10.0.17.1, 192.168.1.1, or 172.16.5.23.

Network addressing

Interconnected networks must agree on an IP addressing plan. In the global Internet, committees of people allocate groups of IP addresses with a consistent, coherent method to ensure that duplicate addresses are not used by different networks and so that a shorthand can be used to refer to groups of addresses. These groups of addresses are called sub-networks, or ***subnets***

for short. Larger subnets can be further subdivided into smaller subnets. Sometimes a group of related addresses is referred to as an ***address space***. On the Internet, no person or organization really owns these groups of ad-dresses

because the addresses only have meaning if the rest of the Internet community agrees with their usage. By agreement, the addresses are allocated to organizations according to their need and size. An organization which has been allocated an address range may then allocate a portion of that address range to another organization as part of a service agreement. Addresses which have been allocated in this manner, starting with internationally recognized committees, and then broken down hierarchically by national or smaller regional committees are referred to as ***globally routed IP addresse***s.

Routing

The Internet is constantly changing and growing. New networks are continually added, and links between networks are added and removed, fail and come back. It is the job of ***routing*** to determine the best path to the destination, and to create a routing table listing the best path for all the different destinations. ***Static routing*** is the term used when the routing table is created by manual configuration. This is sometimes convenient for small networks but can easily become very difficult and error prone for large networks. Worse, if the best path to a network becomes unusable because of equipment failure or other reasons, static routing will not make use of the next best path.

Dynamic routing is a method in which network elements, in particular routers, exchange information about their state and the state of their neighbours in the network, and then use this information to automatically pick the best path and

create the routing table. If something changes, such as a router failing or a new router being put into service, then the dynamic routing proto-cols
make adjustments to the routing table. The system of packet exchanges and decision making is known as a ***routing protocol***. There are many routing protocols that are used in the Internet today, including OSPF, BGP, RIP, and EIGRP.

Wireless networks are like wired networks in that they need dynamic routing protocols, but they are also different enough from wired networks that they need different routing protocols. In particular, wired network connections typically work well or don't work at all (eg., either an Ethernet cable is plugged in, or it isn_t). Things are not so clear when working with wireless networks. Wireless communication can be affected by objects moving into the path of the signal, or by interfering signals. Consequently, links may work well, or poorly, or vary between the two extremes. Since existing network protocols don't take the quality of a link into account when making routing decisions, the IEEE 802.11 committees and the IETF are working on standardizing protocols for wireless networks. It is currently unclear when a single standard for dealing with variable link quality will emerge. In the meantime, there are many ongoing ad-hoc programming attempts to address the problem. Some examples include ***Hazy Sighted Link State (HSLS)***, ***Ad-hoc On-demand Distance Vector (AODV)***, and ***Optimized Link State Routing (OLSR)***. Another is ***SrcRR***, a combination of DSR and ETX implemented by the M.I.T. Roofnet project. Later in this chapter

we will see an example of how to implement a network using OLSR to make routing decisions.

Forwarding

Forwarding is straightforward compared to addressing and routing. Each time a router receives a data packet, it consults its internal routing table. Starting with the high order (or most significant) bit, the routing table is searched for the entry that matches the most number of bits in the destination address. This is called the address ***prefix***. If an entry with a matching prefix is found in the routing table, then the ***hop count*** or ***time to live (TT***L) field is decremented. If the result is zero, then the packet is dropped and an error packet is returned to the sender. Otherwise, the packet is sent to the node or interface specified in the routing table. For example, if the routing table contains these entries

Destination Gateway Genmask Flags Metric Iface

10.15.6.0 0.0.0.0 255.255.255.0 U 0_ eth1

10.15.6.108 10.15.6.7 255.255.255.255 UG 1_ eth1

216.231.38.0 0.0.0.0 255.255.255.0 U 0_ eth0

0.0.0.0 216.231.38.1 0.0.0.0 UG 0_ eth0

...and a packet arrives with the destination address of 10.15.6.23, then the router would send it out on interface eth1. If the packet has a destination of 10.15.6.108, then it would be forwarded to the gateway 10.15.6.7 (since it is

more specific and matches more high-order bits than the 10.15.6.0 network route).

A destination of 0.0.0.0 is a special convention referred to as the ***default gatewa***y. If no other prefixes match the destination address, then the packet is sent to the default gateway. For example, if the destination address was 72.1.140.203, then the router would forward the packet to 216.231.38.1 (which would presumably send it closer to the ultimate destination, and so on). If a packet arrives and no entry is found (i.e., there is no default gateway defined and no prefix matches a known route), then the packet is dropped and an error packet is returned to the sender. The TTL field is used to detect routing loops. Without it, a packet could endlessly be sent back and forth between two routers who each list the other as the next best hop. These kinds of loops can cause so much unnecessary traffic on a network that they threaten its stability. Use of the TTL field doesn't fix routing loops, but it does help to prevent them from destroying a network due to simple mis-configuration.

Estimating capacity

Wireless links can provide significantly greater ***throughput*** to users than traditional Internet connections, such as VSAT, dialup, or DSL. Throughput is also referred to as ***channel capacity***, or simply ***bandwidth*** (although this term is unrelated to radio bandwidth). It is important to understand that a wireless devices listed speed (the ***data rat***e) refers to the rate at which the

radios can exchange symbols, not the usable throughput you will observe. As mentioned earlier, a single 802.11g link may use 54Mbps radios, but it will only provide up to 22Mbps of actual throughput. The rest is overhead that the radios need in order to coordinate their signals using the 802.11g protocol. Note that throughput is a measurement of bits over time. 22Mbps means

that in any given second, up to 22 megabits can be sent from one end of the link to the other. If users attempt to push more than 22 megabits through the link, it will take longer than one second. Since the data can't be sent immediately, it is put in a ***queue***, and transmitted as quickly as possible. This backlog of data increases the time needed for the most recently queued bits to the traverse the link. The time that it takes for data to traverse a link is called ***latency***, and high latency is commonly referred to as ***lag***. Your link will eventually send all of the queued traffic, but your users will likely complain as the lag increases. How much throughput will your users really need? It depends on how many users you have, and how they use the wireless link. Various Internet applications require different amounts of throughput.

2.3 Link planning

A basic communication system consists of two radios, each with its associated antenna, the two being separated by the path to be covered. In order to have a communication between the two, the radios require a certain minimum signal to be collected by the antennas and presented to their input socket. Determining if the link is feasible is a process called ***link budget*** calculation. Whether or not

signals can be passed between the radios depends on the quality of the equipment being used and on the diminishment of the signal due to distance, called ***path loss***.

Internet link optimization

Network throughput of up to 22Mbps can be achieved by using standard, unlicensed 802.11g wireless gear. This amount of band-width will likely be at least an order of magnitude higher than that provided by your Internet link, and should be able to comfortably support many simultaneous Internet users.

But if your primary Internet connection is through a VSAT link, you will en-counter some performance issues if you rely on default TCP/IP parameters. By optimizing your VSAT link, you can significantly improve response times when accessing Internet hosts

2.4 TCP/IP factors over a satellite connection

A VSAT is often referred to as a ***long fat pipe network***. This term refers to factors that affect TCP/IP performance on any network that has relatively large bandwidth, but high latency. Most Internet connections in Africa and other parts of the developing world are via VSAT. The high latency in satellite networks is due to the long distance to the satellite and the constant speed of light. This distance adds about 520 ms to a packet's round-trip time (RTT), compared to a typical RTT between Europe and the USA of about 140 ms.

The factors that most significantly impact TCP/IP performance are **long RTT**, **large bandwidth delay product**, and **transmission errors**. Generally speaking, operating systems that support modern TCP/IP implementations should be used in a satellite network. These implementations

support the RFC 1323 extensions: • The ***window scale*** option for supporting large TCP window sizes (larger than 64KB).

• ***Selective acknowledgement (SACK)*** to enable faster recovery from transmission errors.

• Timestamps for calculating appropriate RTT and retransmission timeout values for the link in use.

2.5 Long Round-Trip Time (RTT)

Satellite links have an average RTT of around 520ms to the first hop. TCP uses the slow-start mechanism at the start of a connection to find the appropriate TCP/IP parameters for that connection. Time spent in the slow-start stage is proportional to the RTT, and for a satellite link it means that TCP stays in slow-start mode for a longer time than would otherwise be the case. This drastically decreases the throughput of short-duration TCP connections. This is can be seen in the way that a small website might take surprisingly long to load, but when a large file is transferred acceptable data rates are achieved after a while.

Furthermore, when packets are lost, TCP enters the congestion-control phase, and owing to the higher RTT, remains in this phase for a longer time, thus reducing the throughput of both short- and long-duration TCP connections.

Large bandwidth-delay product

The amount of data in transit on a link at any point of time is the product of bandwidth and the RTT. Because of the high latency of the satellite link, the bandwidth-delay product is large. TCP/IP allows the remote host to send a certain amount of data in advance without acknowledgment. An acknowledgment is usually required for all incoming data on a TCP/IP connection. However, the remote host is always allowed to send a certain amount of data without acknowledgment, which is important to achieve a good transfer rate on large bandwidth-delay product connections. This amount of data is called the ***TCP window size***. The window size is usually 64KB in modern TCP/IP implementations.

On satellite networks, the value of the bandwidth-delay product is important. To utilize the link fully, the window size of the connection should be equal to the bandwidth-delay product. If the largest window size allowed is 64KB, the maximum theoretical throughput achievable via satellite is (window size) / RTT, or 64KB / 520 ms. This gives a maximum data rate of 123KB/s, which is 984 Kbps, regardless of the fact that the capacity of the link may be much greater.

Each TCP segment header contains a field called ***advertised window***, which specifies how many additional bytes of data the receiver is prepared to accept. The advertised window is the receiver's current available buffer size. The sender is not allowed to send more bytes than the advertised window. To maximize performance, the sender should set its send buffer size and the

receiver should set its receive buffer size to no less than the bandwidth-delay This buffer size has a maximum value of 64KB in most modern TCP/IP implementations.

2.6 Transmission Errors

In older TCP/IP implementations, packet loss is always considered to have been caused by congestion (as opposed to link errors). When this happens, TCP performs congestion avoidance, requiring three duplicate ACKs or slow start in the case of a timeout. Because of the long RTT value, once this congestion-control phase is started, TCP/IP on satellite links will take a longer time to return to the previous throughput level. Therefore errors on a satellite link have a more serious effect on the performance of TCP than over low latency links. To overcome this limitation, mechanisms such as ***Selective Acknowledgment (SACK)*** have been developed. SACK specifies exactly those packets that have been received, allowing the sender to retransmit only those segments that are missing because of link errors. The Microsoft Windows 2000 TCP/IP Implementation Details White Paper states *"Windows 2000 introduces support for an important performance feature known as Selective Acknowledgment*

(SACK). SACK is especially important for connections using large TCP window sizes."

SACK has been a standard feature in Linux and BSD kernels for quite some time. Be sure that your Internet router and your ISPs remote side both sup-port SACK.

CHAPTER THREE

WAVE GUIDES

Above 2 GHz, the wavelength is short enough to allow practical, efficient energy transfer by different means. A waveguide is a conducting tube through which energy is transmitted in the form of electromagnetic waves. The tube acts as a boundary that confines the waves in the enclosed space. The skin effect prevents any electromagnetic effects from being evident out-side the guide. The electromagnetic fields are propagated through the waveguide by means of reflections against its inner walls, which are considered perfect conductors. The intensity of the fields is greatest at the center along the X dimension, and must diminish to zero at the end walls because the existence of any field parallel to the walls at the surface would cause an infinite current to flow in a perfect conductor.

Wave guides, of course, cannot carry RF in this fashion.

There are an infinite number of ways in which the electric and magnetic fields can arrange themselves in a waveguide for frequencies above the low cutoff frequency. Each of these field configurations is called a mode. The modes may be separated into two general groups. One group, designated TM (Transverse Magnetic), has the magnetic field entirely transverse to the direction of propagation, but has a component of the electric field in the direction of propagation. The other type, designated TE (Transverse Electric) has the electric field entirely transverse, but has a component of magnetic field in the direction of propagation.

3.2 *Antennas and Radiation patterns*

Antennas are a very important component of communication systems. By definition, an antenna is a device used to transform an RF signal traveling on a conductor into an electromagnetic wave in free space. Antennas demonstrate a property known as *reciprocity*, which means that an antenna will maintain the same characteristics regardless if whether it is transmitting or receiving. Most antennas are resonant devices, which operate efficiently over a relatively narrow frequency band. An antenna must be tuned to the same frequency band of the radio system to which it is connected, otherwise the reception and the transmission will be impaired. When a signal is fed into an antenna, the antenna will emit radiation distributed in space in a certain way. A graphical representation of the relative distribution of the radiated power in space is called a *radiation pattern*.

Input Impedance

For an efficient transfer of energy, the *impedance* of the radio, antenna, and transmission cable connecting them must be the same. Transceivers and their transmission lines are typically designed for 50_ impedance. If the antenna has an impedance different than 50_, then there is a mismatch and an impedance matching circuit is required. When any of these components
are mismatched, transmission efficiency suffers.

Directivity and Gain

Directivity is the ability of an antenna to focus energy in a particular direction when transmitting, or to receive energy from a particular direction when receiving. If a wireless link uses fixed locations for both ends, it is possible to use antenna directivity to concentrate the radiation beam in the wanted direction. In a mobile application where the transceiver is not fixed, it may be impossible to predict where the transceiver will be, and so the antenna should ideally radiate as well as possible in all directions. An omnidirectional antenna is used in these applications.

Gain is not a quantity which can be defined in terms of a physical quantity such as the Watt or the Ohm, but it is a dimensionless ratio. Gain is given in reference to a standard antenna. The two most common reference antennas are the *isotropic antenna* and the *resonant half-wave dipole antenna.*

The isotropic antenna radiates equally well in all directions. Real isotropic antennas do not exist, but they provide useful and simple theoretical antenna patterns with which to compare real antennas. Any real antenna will radiate more energy in some directions than in others. Since antennas cannot create energy, the total power radiated is the same as an isotropic antenna. Any additional energy radiated in the directions it favors is offset by equally less energy radiated in all other directions. The gain of an antenna in a given direction is the amount of energy radiated in that direction compared to the energy an isotropic antenna would radiate in the same direction when driven with the same input power. Usually we are only

interested in the maximum gain, which is the gain in the direction in which the antenna is radiating most of the power. An antenna gain of 3dB compared to an isotropic antenna would be written as 3dBi. The resonant half-wave dipole can be a useful standard for comparing to other antennas at one frequency or over a very narrow band of frequencies. To compare the dipole to an antenna over a range of frequencies requires a number of dipoles of different lengths. An antenna gain of 3dB compared to a dipole

antenna would be written as 3dBd. The method of measuring gain by comparing the antenna under test against a known standard antenna, which has a calibrated gain, is technically known

as a *gain transfer* technique. Another method for measuring gain is the 3 antennas method, where the transmitted and received power at the antenna terminals is measured between three arbitrary antennas at a known fixed distance.

3.3 Types of Antennas

A classification of antennas can be based on:

• Frequency and size. Antennas used for HF are different from antennas used for VHF, which in turn are different from antennas for microwave. The wavelength is different at different frequencies, so the antennas must be different in size to radiate signals at the correct wavelength. We are particularly interested in antennas working in the microwave range, especially in the 2.4 GHz and 5 GHz frequencies. At 2.4 GHz the wavelength is

12.5cm, while at 5 GHz it is 6cm.

• Directivity. Antennas can be omnidirectional, sectorial or directive. *Omni-directional*

antennas radiate roughly the same pattern all around the antenna in a complete 360° pattern. The most popular types of omnidirectional antennas are the *dipole* and the *ground plane*. *Sectorial antennas* radiate primarily in a specific area. The beam can be as wide as 180 de-grees, or as narrow as 60 degrees. *Directional* or *directive antennas* are antennas in which the beamwidth is much narrower than in sectorial antennas. They have the highest gain and are therefore used for long distance links. Types of directive antennas are the Yagi, the biquad, the horn, the helicoidal, the patch antenna, the parabolic dish, and many others.

• Physical construction. Antennas can be constructed in many different ways, ranging from simple wires, to parabolic dishes, to coffee cans. When considering antennas suitable for 2.4 GHz WLAN use, another classification can be used:.• Application. Access points tend to make point-to-multipoint networks, while remote links are point-to-point. Each of these suggest different types of antennas for their purpose. Nodes that are used for multipoint access will likely use omni antennas which radiate equally in all directions, or sectorial antennas which focus into a small area. In the point-to-point case, antennas are used to connect two single locations together. Directive antennas are the primary choice for this application.

1/4 wavelength ground plane

The 1/4 wavelength ground plane antenna is very simple in its construction and is useful for communications when size, cost and ease of construction are important. This antenna is designed to transmit a vertically polarized signal. It consists of a 1/4 wave element as half-dipole and three or four ¼ wavelength ground elements bent 30 to 45 degrees down. This set of elements, called radials, is known as a ground plane. This is a simple and effective antenna that can capture a signal equally from all directions. To increase the gain, the signal can be flattened out to take away focus from directly above and below, and providing more focus on the horizon. The vertical beamwidth represents the degree of flatness in the focus. This is useful in a Point-to-Multipoint situation, if all the other antennas are also at the same height. The gain of this antenna is in the order of 2 - 4 dBi.

Yagi antenna

A basic Yagi consists of a certain number of straight elements, each measuring approximately half wavelength. The driven or active element of a Yagi is the equivalent of a center-fed, half-wave dipole antenna. Parallel to the driven element, and approximately 0.2 to 0.5 wavelength on either side of it, are straight rods or wires called reflectors and directors, or simply passive

elements. A reflector is placed behind the driven element and is slightly longer than half wavelength; a director is placed in front of the driven element and is slightly shorter than half wavelength. A typical Yagi has one reflector and one or

more directors. The antenna propagates electromagnetic field energy in the direction running from the driven element toward the directors,

and is most sensitive to incoming electromagnetic field energy in this same direction. The more directors a Yagi has, the greater the gain. As more directors are added to a Yagi, it therefore becomes longer. Following is the photo of a Yagi antenna with 6 directors and one reflector.

Yagi antennas are used primarily for Point-to-Point links, have a gain from 10 to 20 dBi and a horizontal beamwidth of 10 to 20 degrees.

Horn

The horn antenna derives its name from the characteristic flared appearance. The flared portion can be square, rectangular, cylindrical or conical. The direction of maximum radiation corresponds with the axis of the horn. It is easily fed with a waveguide, but can be fed with a coaxial cable and a proper transition. Horn antennas are commonly used as the active element in a dish antenna. The horn is pointed toward the center of the dish reflector. The use of a horn, rather than a dipole antenna or any other type of antenna, at the focal point of the dish minimizes loss of energy around the edges of the dish reflector. At 2.4 GHz, a simple horn antenna made with a tin can has a gain in the order of 10 - 15 dBi.

Parabolic Dish

Antennas based on parabolic reflectors are the most common type of directive antennas when a high gain is required. The main advantage is that they can be

/made to have gain and directivity as large as required. The main disadvantage is that big dishes are difficult to mount and are likely to have a large windage. Dishes up to one meter are usually made from solid material. Aluminum is frequently used for its weight advantage, its durability and good electrical characteristics. Windage increases rapidly with dish size and soon becomes a severe problem. Dishes which have a reflecting surface that uses an open mesh are frequently used. These have a poorer front-to-back ratio, but are safer to use and easier to build. Copper, aluminum, brass, galvanized steel
and iron are suitable mesh materials.

BiQuad

The BiQuad antenna is simple to build and offers good directivity and gain for Point-to-Point communications. It consists of a two squares of the same size of 1/4 wavelength as a radiating element and of a metallic plate or grid as reflector. This antenna has a beamwidth of about 70 degrees and a gain in the order of 10-12 dBi. It can be used as stand-alone antenna or as feeder
for a Parabolic Dish. The polarization is such that looking at the antenna from the front, if the squares are placed side by side the polarization is vertical.

Other Antennas

Many other types of antennas exist and new ones are created following the advances in technology.

• Sector or Sectorial antennas: they are widely used in cellular telephony infrastructure and are usually built adding a reflective plate to one or more phased dipoles. Their horizontal beamwidth can be as wide as 180 degrees, or as narrow as 60 degrees, while the vertical is usually much narrower.

Composite antennas can be built with many Sectors to cover a wider horizontal range (multisectorial antenna).

• Panel or Patch antennas: they are solid flat panels used for indoor cover-age, with a gain up to 20 dB.

3.4 Amplifiers

As mentioned earlier, antennas do not actually create power. They simply direct all available power into a particular pattern. By using a *power amplifier*, you can use DC power to augment your available signal. An amplifier connects between the radio transmitter and the antenna, and has an additional lead that connects to a power source. Amplifiers are available that work at 2.4GHz, and can add several Watts of power to your transmission. These devices sense when an attached radio is transmitting, and quickly power up and amplify the signal. They then switch off again when transmission ends. When receiving, they also add amplification to the signal before

sending it to the radio.

• They are expensive. Amplifiers must work at relatively wide bandwidths at 2.4GHz, and must switch quickly enough to work for Wi-Fi applications. These amplifiers do exist, but they tend to cost several hundred dollars per unit.

• You will need at least two. Whereas antennas provide reciprocal gain that benefits both sides of a connection, amplifiers work best at amplifying a transmitted signal. If you only add an amplifier to one end of a link with insufficient antenna gain, it will likely be able to be heard but will not be able to hear the other end.

• They provide no additional directionality. Adding antenna gain provides both gain and directionality benefits to both ends of the link. They not only improve the available amount of signal, but tend to reject noise from other directions. Amplifiers blindly amplify both desired and interfering signals, and can make interference problems worse.

• Amplifiers generate noise for other users of the band. By increasing your output power, you are creating a louder source of noise for other users of the unlicensed band. This may not be much of an issue today in rural areas, but it can cause big problems in populated areas. Conversely, adding antenna gain will improve your link and can actually decrease the noise level for your neighbors.

• Using amplifiers probably isn't legal. Every country imposes power limits on use of unlicensed spectrum. Adding an antenna to a highly amplified signal will likely cause the link to exceed legal limits. Using amplifiers is often compared to the inconsiderate neighbor who wants

to listen to the radio outside their home, and so turns it up to full volume. They might even "improve" reception by pointing their speakers out the window. While they may now be able to hear the radio, so must everyone else on the block. This

approach may scale to exactly one user, but what hap-pens when the neighbors decide to do the same thing with their radios? Us-ing

amplifiers for a wireless link causes roughly the same effect at 2.4GHz. Your link may "work better" for the moment, but you will have problems when other users of the band decide to use amplifiers of their own. By using higher gain antennas rather than amplifiers, you avoid all of these problems. Antennas cost far less than amps, and can improve a link simply .by changing the antenna on one end. Using more sensitive radios and good quality cable also helps significantly on long distance shots. These techniques are unlikely to cause problems for other users of the band, and so we recommend pursuing them long before adding amplifiers.

3.5 Networking Hardware

In the last couple of years, an unprecedented surge in interest in wireless networking hardware has brought a huge variety of inexpensive equipment to the market. So much variety, in fact, that it would be impossible to catalog every available component.

Wired wireless

With a name like "wireless", you may be surprised at how many wires are involved in making a simple point-to-point link. A wireless node consists of many components, which must all be connected to each other with appropri-ate

cabling. You obviously need at least one computer connected to an Eth-ernet network, and a wireless router or bridge attached to the same network.

Radio components need to be connected to antennas, but along the way they may need to interface with an amplifier, lightning arrestor, or other de-vice. Many components require power, either via an AC mains line or using a DC transformer. All of these components use various sorts of connectors, not to mention a wide variety of cable types and thicknesses.

Choosing wireless components

In a world of competitive hardware manufacturers and limited budgets, the price tag is the single factor that usually receives the most attention. The old saying that "you get what you pay for" often holds true when buying high tech equipment, but should not be considered an absolute truth. While the price tag is an important part of any purchasing decision, it is vital to understand precisely what you get for your money so you can make a choice that fits your needs.

When comparing wireless equipment for use in your network, be sure to consider these variables:

• Interoperability. Will the equipment you are considering work with equipment from other manufacturers? If not, is this an important factor for this segment of your network? If the gear in question supports an open protocol (such as 802.11b/g), then it will likely interoperate with equipment from other sources.

• Range. Range is not something inherent in a particular piece of equipment. A device's range depends on the antenna connected to it, the surrounding terrain,

the characteristics of the device at the other end of the link, and other factors. Rather than relying on a semi-fictional "range" rating supplied by the manufacturer, it is more useful to know the *transmission power* of the radio as well as the *antenna gain* (if an antenna is included). With this information, you can calculate the theoretical range as described in chapter three.

• Radio sensitivity. How sensitive is the radio device at a given bit rate? The manufacturer should supply this information, at least at the fastest and slowest speeds. This can be used as a measure of the quality of the hardware, as well as allow you to complete a link budget calculation. As we saw in chapter three, a lower number is better for radio sensitivity.

• Throughput. Manufacturers consistently list the highest possible bit rate as the "speed" of their equipment. Keep in mind that the radio symbol rate (eg. 54Mbps) is never the actual throughput rating of the device (eg. About 22Mbps for 802.11g). If throughput rate information is not available for the device you are evaluating, a good rule of thumb is to divide the device "speed" by two, and subtract 20% or so. When in doubt, perform through-put testing on an evaluation unit before committing to purchasing a large amount of equipment that has no official throughput rating.

• Required accessories. To keep the initial price tag low, vendors often leave out accessories that are required for normal use. Does the price tag include all power adapters? (DC supplies are typically included; power over Ethernet injectors typically are not. Double-check input voltages as well, as equipment is often provided with a US-centric power supply). What about pigtails, adapters, cables,

antennas, and radio cards? If you intend to use it outdoors, does the device include a weatherproof case?

• Availability. Will you be able to easily replace failed components? Can you order the part in large quantity, should your project require it? What is the projected life span of this particular product, both in terms of useful running time in-the-field and likely availability from the vendor?

• Other factors. Be sure that other needed features are provided for to meet your particular needs. For example, does the device include an external antenna connector? If so, what type is it? Are there user or throughput limits imposed by software, and if so, what is the cost to in-crease

these limits? What is the physical form factor of the device? How much power does it consume? Does it support POE as a power source? Does the device provide encryption, NAT, bandwidth monitoring tools, or other features critical to the intended network design? By answering these questions first, you will be able to make intelligent buying decisions when it comes time to choose networking hardware. It is unlikely that you will be able to answer every possible question before buying gear, but if you prioritize the questions and press the vendor to answer them before committing to a purchase, you will make the best use of your budget and build a network of components that are well suited to your needs.

3.6 Professional wireless products

There is an abundance of equipment on the market for long distance, point-to-point (P2P) links. Most of this equipment is ready to go right out of the box, only

the antenna cables need to be attached and sealed. When thinking about a long *distance link*, there are three main factors to consider: total link distance, uptime requirements, and of course, link speed requirements. Most of the commonly available commercial products for longer range links now use OFDM technology and operate in the 5.8 GHz ISM band. There are some products available that use open standards, but most use a proprietary protocol of some sort. This does mean that in order to form a link, the radios on both sides will have to be from the same manufacturer. For mission critical links it is a good idea to choose a system that uses the identical equipment on both sides of the link. This way only one spare unit needs to be stocked, and if need be, can replace either side of the link. There are some good products on the market that use different equipment at either end of a link. These can be used in a network as long as it is done with care, or else spares will need to be available in both kinds of radios.

Redline Communications

Redline first came to market with its AN-50 line of products. This was the first point-to-point product available with data rates above 50 Mbps that small operators could actually afford. They only use 20 MHz of spectrum per channel. There are three different models available in their AN-50 line. All three have the same basic feature sets, only the total bandwidth changes. The standard model has 36 Mbps throughput, the economy model has 18Mbps, and the full version has 54 Mbps. The bandwidth controls are software upgradeable and can be added into the system as the demand for bandwidth increases.

Redline radios consist of an indoor unit, an outdoor unit, and an antenna. The indoor unit fits in a standard 19 inch rack, and occupies 1U. The outdoor unit mounts on the same bracket that holds the antenna in place. This out-door unit is the actual radio. The two units are linked by a coax interface cable. Beldon RG6 or RG11 cable is used for this interface cable. This is the same cable used for satellite TV installations. It is inexpensive, easy to find, and eliminates the need for expensive low loss cable, like the Times Micro-wave LMR series or Andrew Corporation Heliax. Also, keeping the radio mounted so close to the antenna keeps the cable related loss to an absolute minimum.

There are two features to note on the Redline radios. The first is the *General Alignment Mode*, which turns on a beeper that changes tone as the modulation technique changes. Faster beeping means a faster connection. This allows for a much easier alignment as the link can be mostly aligned by the tones alone. Only a final tuning will be needed, and a graphical Windows application is available to help with this. The other feature is a *Test* button. Whenever radio changes are made but are not sure to be correct, pressing the test button instead of the *Save* button will make the new changes active for five minutes. After five minutes, the configuration reverts back to the setting before the test button was pushed. This allows the changes to be tried out, and if things don't work out and the link goes down, the link will come back after five minutes. Once the changes have been tried out, simply con-firm the

new settings in the configuration, and press the save button instead of the test button.

Redline has other models available. The AN-30 has four T1/E1 ports, in addition to a 30 Mbps Ethernet connection. The AN-100 follows the 802.16a standard, and the upcoming RedMax promises WiMax compliance. For more information about Redline Communications products, see http://*www.redlinecommunications.com/*

Alvarion

One of the biggest advantages of working with Alvarion products is Alvarion's very well established worldwide distribution network. They also have one of the largest worldwide market shares for all kinds of wireless Internet connectivity hardware. There are distributors and resellers within most regions. For longer distance links there are two products of interest: The VL series, and the Link Blaster. While the VL series is actually a point-to-multipoint system, a single client radio connecting to a single access point will function just fine for a point-to-point link. The only thing that should be considered is using a more directional antenna at the access point, unless there is a future link planned that could connect to that access point. There are two speeds available for the VL series, 24 Mbps and 6 Mbps. Budget, uptime, and speed requirements will guide the decision between which CPE to use. The Link Blaster looks and feels a lot like a Redline AN-50. That's because it is one. Very soon after the Redline AN-50 came on the market, an OEM agreement between the two companies was

signed, and the Link Blaster was born. Although the indoor unit is in a different case, and the antennas are marked differently, the electronics inside the units are identical. The Link Blaster does cost more than a Redline; this money buys you a more rugged design and an additional level of support. In many cases, an Alvarion reseller may be closer and easier to ship product from then some Redline re-sellers.

This will be something that will have to be locally researched. It may be worth the extra money to have a product that is locally available and sup-ported. Alvarion does have some 2.4 GHz point-to-point products available. Most of their product range in the 2.4 GHz ISM band uses frequency hopping spread spectrum (FHSS) and will create a lot of noise for local direct sequence spread spectrum (DSSS) on the same tower. If a DSSS based distribution system is being planned for, then a FHSS backhaul is not going to be an effective option. For more information about Alvarion products, see *http://www.alvarion.com/*

Rad Data Communications

The Rad Airmux product line is relatively new to the market, and has some great potential. The Airmux 200 is a 48 Mbps radio, uses CAT5 cable, and comes with one of the most friendly price tags of any commercial solution. The units are small and easy to handle on a tower. The downside that may be found is a lack of a local distribution system in the developing world. There are two models available within the Airmux line. One uses internal antennas, and the other uses external antennas. Experience with Airmux radios in early 2005 shows there is

an issue in the timing configurations. This only becomes apparent when the link distance is more then 12 miles, or 19 km. It doesn't matter which antennas are being used. Until this bug is fixed, these radios should only be used for links under 19 km. When that guide is followed these radios preform very well, especially for their price point. For more information about Rad Data Communications products, see *http://www.rad.com/*

Cisco Systems

Cisco wireless solutions have two big advantages to their credit. They have a very well established distribution, support, and training network throughout most of the world. There are distributors and resellers all over the place. This can be a big help when it comes time to procure equipment, and even more important if equipment breaks and needs replacing. The next big ad-vantage is that for the most part, they use open standards. Most of their available equipment follows 802.11a/b/g standards. Experience has shown that their web based configuration tools are not as easy to understand as those found in many other products, and the equipment tends to come with a price tag that makes other non-commercial, open standard solutions more viable.

More information about Cisco can be found at *http://www.cisco.com/*

Others

There are many more solutions available on the market now, and more arriving all of the time. Good solutions are available from companies like Trango

Broadband *(http://www.trangobroadband.com/)* and Waverider Communications *(http://www.waverider.com/)*. When considering which solution to use, always remember the three main factors; distance, uptime and speed. Be sure to check and make sure that the radios operate in an unlicensed band where you are installing them.

CHAPTER FOUR

SECURITY

4.1 Wireless Network Security

In a traditional wired network, access control is very straightforward: If a person has physical access to a computer or network hub, then they can use (or abuse) the network resources. While software mechanisms are an important component of network security, limiting physical access to the network devices is the ultimate access control mechanism. Simply put, if all terminals and network components are only accessible to trusted individuals, then the network can likely be trusted.

The rules change significantly with wireless networks. While the apparent range of your access point may seem to be just a few hundred meters, a user with a high gain antenna may be able to make use of the network from several blocks away. Should an unauthorized user be detected, it is impossible to simply "trace the cable" back to the user's location. Without transmitting a single packet, a nefarious user can even log all network data to disk. This data can later be used to launch a more sophisticated attack against the network. Of course, even in wired networks, it is never quite possible to completely trust all users of the network. While such a system might be completely "secure", it is useless for communication. When you make security decisions for your network, remember that 'above all else, the network exists so that its users can communicate with each other. Security considerations are important, but should not get in the way of the network's users.

4.2 *Physical security*

When installing a network, you are building an infrastructure that people will depend on. And thus, the network must be reliable. For many installations, outages often occur due to human tampering, accidental or not. Networks are physical, wires and boxes, things that are easily disturbed. In many installations, people will not know what the equipment is that you have installed, or, curiosity leads them to experiment. They will not realize the importance that a cable goes to a port. People might move an Ethernet cable so that they can connect their laptop for 5 minutes, or move a switch be-cause it is in their way. A plug might be removed from a power bar because someone needs that receptacle. Assuring the physical security of an installation is paramount. Signs and labels will only be useful to few, who can read, or speak your language. Putting things out of the way, and limiting access is the best means to assure that accidents, or tinkering does not occur. In less developed economies proper fasteners, ties, or boxes will not be as easy to find. You should be able to find electrical supplies that will work just as well. Custom enclosures are also easy to manufacture and should be considered essential to any installation.

Switches

Switches, hubs or interior access points can with a wall plug be screwed directly onto a wall. Best to put this equipment as high as possible to reduce the chance that someone will touch the device or its cables.

Cables

Cables should be hidden and fastened. Better to bury cables, than to leave them hanging across a yard, where it might be used for drying clothes, or simply snagged by a ladder etc. To avoid vermin and insects find plastic electrical conduit. The marginal expense will be well worth the trouble. The conduit should be buried about 30cm deep (below the frost in cold climates).

It is also worth buying larger conduit than is presently required, so that future cables can be run through the same tubing. It is also possible to find plastic cable conduit that can be used in buildings. If not, simple cable attachments, nailed into the wall can be used to secure the cable and to make sure that it doesn't hang where it can be snagged, pinched or cut.

Power

It is best to have power bars locked in a cabinet. If that is not possible, Mount the power bar under a desk, or on the wall and use duct tape (gaffer tape, a strong adhesive tape) to secure the plug into the receptacle. On the UPS and power bar, do not leave empty receptacles, tape them if necessary. People will have the tendency to use the easiest receptacle, so make these critical ones difficult to use. If you do not, you might find a fan or light plugged into your UPS; though it is nice to have light, it is nicer to keep your server running!

Water

Protect your equipment from water and moisture. In all cases make sure that your equipment, including your UPS is at least 30cm from the ground, to avoid flooding. Also try to have a roof over your equipment, so that water and moisture will not fall onto it. In moist climates, it is important that the equipment has proper ventilation to assure that moisture can be exhausted. Small closets need to have ventilation, or moisture and heat can degrade or destroy your gear.

Masts

Equipment installed on a mast is often safe from thieves. Nonetheless, to deter thieves and to keep your equipment safe from winds it is good to over-engineer mounts. Equipment should be painted a dull, white or grey colour to reflect the sun and to make it look plain and uninteresting. Panel antennas are much more subtle and less interesting than dishes and thus should be preferred. Any installation on walls, should require a ladder to reach. Try choosing well lit but not prominent places to put equipment. Also avoid antennae that resemble television antennae, as those are items that will attract interest by thieves, where a wifi antenna will be useless to the average thief.

4.3 Threats to the network

One critical difference between Ethernet and wireless is that wireless net-works are built on a *shared medium*. They more closely resemble the old network hubs than modern switches, in that every computer connected to the network can

"see" the traffic of every other user. To monitor all network traffic on an access point, one can simply tune to the channel being used, put the network card into monitor mode, and log every frame. This data might be directly valuable to an eavesdropper (including data such as email, voice data, or online chat logs). It may also provide passwords and other sensitive data, making it possible to compromise the network even further. This problem can be mitigated by the use of encryption. Another serious problem with wireless networks is that its users are relatively *anonymous*. While it is true that every wireless device includes a unique MAC address that is supplied by the manufacturer, these addresses can often be changed with software. Even given the MAC address, it can be very difficult to judge where a wireless user is physically located. Multipath effects, high gain antennas, and widely varying radio transmitter characteristics can make it impossible to determine if a malicious wireless user is sitting in the next room or is in an apartment building a mile away.

While unlicensed spectrum provides a huge cost savings to the user, it has the unfortunate side effect that *denial of service (DoS)* attacks are trivially simple. By simply turning on a high powered access point, cordless phone, video transmitter, or other 2.4GHz device, a malicious person could cause significant problems on the network.

• *Unintentional users*. As more wireless networks are installed in densely populated areas, it is common for laptop users to accidentally associate to the wrong network. Most wireless clients will simply choose any available wireless

network when their preferred network is unavailable. The user may then make use of this network as usual, completely unaware that they may be transmitting sensitive data on someone else's network. Malicious people may even take advantage of this by setting up access points in strategic locations, to try to attract unwitting users and capture their data. The first step in avoiding this problem is educating your users, and stressing the importance of connecting only to known and trusted networks. Many wireless clients can be configured to only connect to trusted networks, or to ask permission before joining a new network. As we will see later in this chapter, users can safely connect to open public networks by

using strong encryption.

• *War drivers*. The "war driving" phenomenon draws its name from the popular 1983 hacker film, "War Games". War drivers are interested in finding the physical location of wireless networks. They typically drive around with a laptop, GPS, and omnidirectional antenna, logging the name

and location of any networks they find. These logs are then combined with logs from other war drivers, and are turned into graphical maps depicting the wireless "footprint" of a particular city.

The vast majority of war drivers likely pose no direct threat to networks, but the data they collect might be of interest to a network cracker. For example, it might be obvious that an unprotected access point detected by a war driver is located inside a sensitive building, such as a government or corporate office. A malicious

person could use this information to illegally access the network there. Arguably, such an AP should never have been set up in the first place, but war driving makes the problem all the more urgent. War drivers who use the popular program NetStumbler can be detected with programs such as Kismet. For more information about war driving, see si t e s such as *http://www.wifimaps.com/, http://www.nodedb.com/,* or *http://www.netstumbler.com/.*

• *Rogue access point*s. There are two general classes of rogue access points: those incorrectly installed by legitimate users, and those installed by malicious people who intend to collect data or do harm to the network. In the simplest case, a legitimate network user may want better wireless

coverage in their office, or they might find security restrictions on the corporate wireless network too difficult to comply with. By installing an inexpensive consumer access point without permission, the user opens the entire network up to potential attacks from the inside. While it is possible to scan for unauthorized access points on your wired network, setting a clear policy that prohibits them is very important. The second class of rogue access point can be very difficult to deal with. By installing a high powered AP that uses the same ESSID as an existing network, a malicious person can trick people into using their equipment, and log or even manipulate all data that passes through it. Again, if your users are trained to use strong encryption, this problem is significantly reduced.

• *Eavesdroppers*. As mentioned earlier, eavesdropping is a very difficult problem to deal with on wireless networks. By using a passive monitoring tool (such as Kismet), an eavesdropper can log all network data from a great distance away, without ever making their presence known. Poorly encrypted data can simply be logged and cracked later, while unencrypted data can be easily read in real time. You might want to demonstrate tools such as Etherpeg *(http://www.etherpeg.org/)* or Driftnet *(http://www.ex-parrot.com/~chris/driftnet/)*. These tools watch a wireless network for graphical data, such as GIF and JPEG files. While other users are browsing the Internet, these tools simply display all graphics found in a graphical collage. I often use tools such as this as a demonstration when lecturing on wireless security. While you can tell a user that their email is vulnerable without encryption, nothing drives the message home like showing them the pictures they are looking at in their web browser.

Again, while it cannot be completely prevented, proper application of strong encryption will discourage eavesdropping. This introduction is intended to give you an idea of the problems you are up against when designing a wireless network. Later in this chapter, we will look at tools and techniques that will help you to mitigate these problems.

4.4 Authentication

Before being granted access to network resources, users should first be *authenticated*. In an ideal world, every wireless user would have an identifier that is unique, unchangeable, and cannot be impersonated by other users. This turns

out to be a very difficult problem to solve in the real world. The closest feature we have to a unique identifier is the MAC address. This

is the 48-bit number assigned by the manufacturer to every wireless and Ethernet device. By employing *mac filtering* on our access points, we can authenticate users based on their MAC address. With this feature, the access point keeps an internal table of approved MAC addresses. When a wireless user tries to associate to the access point, the MAC address of the client must be on the approved list, or the association will be denied. Alternately, the AP may keep a table of known "bad" MAC addresses, and permit all devices that are not on the list.

Unfortunately, this is not an ideal security mechanism. Maintaining MAC tables on every device can be cumbersome, requiring all client devices to have their MAC addresses recorded and uploaded to the APs. Even worse, MAC addresses can often be changed in software. By observing MAC ad-dresses in use on a wireless network, a determined attacker can "spoof" an

approved MAC address and successfully associate to the AP. While MAC filtering will prevent unintentional users and even most curious individuals from accessing the network, MAC filtering alone cannot prevent attacks from determined attackers. MAC filters are useful for temporarily limiting access from misbehaving clients. For example, if a laptop has a virus that sends large amounts of spam or other traffic, its MAC address can be added to the filter table to stop the traffic immediately. This will buy you time to track down the user and

fix the problem. Another popular authentication feature of wireless the so-called *closed network*.

In a typical network, APs will broadcast their ESSID many times per second, allowing wireless clients (as well as tools such as NetStumbler) to find the network and display its presence to the user. In a closed network, the AP does not beacon the ESSID, and users must know the full name of the network before the AP will allow association. This prevents casual users from discovering the network and selecting it in their wireless client. There are a number of drawbacks to this feature. Forcing users to type in the full ESSID before connecting to the network is error prone and often leads to support calls and complaints. Since the network isn't obviously present in site survey tools like NetStumbler, this can prevent your networks

from showing up on war driving maps. But it also means that other network builders cannot easily find your network either, and specifically won't know that you are already using a given channel. A conscientious neighbor may perform a site survey, see no nearby networks, and install their own network on the same channel you are using. This will cause interference problems

for both you and your neighbor. By using passive monitoring tools (such as Kismet), a skilled user

can detect frames sent from your legitimate clients to the AP. These frames necessarily contain the network name. A malicious user can then use this name to associate to the access point, just like a normal user would. Encryption is probably the best tool we have for authenticating wireless us-ers. Through strong

encryption, we can uniquely identify a user in a manner that is very difficult to spoof, and use that identity to determine further net-work access. Encryption also has the benefit of adding a layer of privacy by preventing eavesdroppers from easily watching network traffic. The most widely employed encryption method on wireless networks is *WEP encryption*. WEP stands for *wired equivalent privacy*, and is supported by virtually all 802.11a/b/g equipment. WEP uses a shared 40-bit key to encrypt data between the access point and client. The key must be entered on the APs as well as on each of the clients. With WEP enabled, wireless clients cannot associate with the AP until they use the correct key. An eavesdropper

listening to a WEP-enabled network will still see traffic and MAC addresses, but the data payload of each packet is encrypted. This provides a fairly good authentication mechanism while also adding a bit of privacy to the network WEP is definitely not the strongest encryption solution available. For one thing, the WEP key is shared between all users. If the key is compromised

(say, if one user tells a friend what the password is, or an employee is let go) then changing the password can be prohibitively difficult, since all APs and client devices need to be changed. This also means that legitimate users of the network can still eavesdrop on each others' traffic, since they all know the shared key.

Captive portals

One common authentication tool used on wireless networks is the *captive portal*. A captive portal uses a standard web browser to give a wireless user the opportunity to present login credentials. It can also be used to present information (such as an Acceptable Use Policy) to the user before granting further access. By using a web browser instead of a custom program for authentication, captive portals work with virtually all laptops and operating systems. Captive portals are typically used on open networks with no other authentication methods (such as WEP or MAC filters). To begin, a wireless user opens their laptop and selects the network. Their computer requests a DHCP lease, which is granted. They then use their web browser to go to any site on the Internet. Instead of receiving the requested page, the user is presented with a login screen. This page can require the user to enter a user name and password, simply click a "login" button, type in numbers from a pre-paid ticket, or enter any other credentials that the network administrators require. The user then enters their credentials, which are checked by the access point or another server on the network. All other network access is blocked until these credentials are verified. Once authenticated, the user is permitted to access network resources, and is typically redirected to the site they originally requested.

Captive portals provide no encryption for the wireless users, instead relying on the MAC and IP address of the client as a unique identifier. Since this is not necessarily very secure, many implementations will require the user to re-

authenticate periodically. This can often be automatically done by minimizing a special pop-up browser window when the user first logs in.

Since they do not provide strong encryption, captive portals are not a very good choice for networks that need to be locked down to only allow access from trusted users. They are much more suited to cafes, hotels, and other public access locations where casual network users are expected.

In public or semi-public network settings, encryption techniques such as WEP and WPA are effectively useless. There is simply no way to distribute public or shared keys to members of the general public without compromising the security of those keys. In these settings, a simple application such as a captive portal provides a level of service somewhere between completely
open and completely closed.

Two popular open source captive portal implementations are NoCatSplash and Chillispot.

NoCatSplash

NoCatSplash provides a customizable splash page to your users, requiring them to click a "login" button before using the network. This is useful for identifying the operators of the network and displaying rules for network access. NoCatSplash is written in C, and will run on just about any Unix-like operating system including Linux, BSD, and even embedded platforms such as OpenWRT. It has a simple configuration file and can serve any custom HTML file as the splash page. It is

typically run directly on an access point, but can also work on a router or proxy server. For more information, see *http://nocat.net/*.

Other popular hotspot projects

NoCatSplash is just one simple captive portal implementation. Many other free implementations exist that support a diverse range of functionality. Some of these include:

• Chillispot *(http://www.chillispot.org/)*. Chillispot is a captive portal de-signed to authenticate against an existing user credentials database, such as RADUIS. Combined with the application phpMyPrePaid, pre-paid ticket based authentication can be implemented very easily You can download phpMyPrePaid from *http://sourceforge.net/projects/phpmyprepaid/*.

• WiFi Dog *(http://www.wifidog.org/)*. WiFi Dog provides a very complete captive portal authentication package in very little space (typically under 30kb). From a user's perspective, it requires no pop-up or javascript support, allowing it to work on a wider variety of wireless devices.

• m0n0wall *(http://m0n0.ch/wall/)*. m0n0wall is a complete embedded operating system based on FreeBSD. It includes a captive portal with RADIUS support, as well as a PHP web server.

4.5 Privacy

Most users are blissfully unaware that their private email, chat conversations, and even passwords are often sent "in the clear" over dozens of untrusted

networks before arriving at their ultimate destination on the Internet. However mistaken they may be, users still typically have some expectation of privacy when using computer networks. Privacy can be achieved, even on untrusted networks such as public access points and the Internet. The only proven effective method for protecting privacy is the use of strong *end-to-end encryption*.

Encryption techniques such as WEP and WPA attempt to address the privacy issue at layer two, the data-link layer. While this does protect eavesdroppers from listening in on the wireless connection, protection ends at the access point. If the wireless client uses insecure protocols (such as POP or simple SMTP for receiving and sending email), then users beyond the AP can still log the session and see the sensitive data. As mentioned earlier, WEP also suffers from the fact that it uses a shared private key. This means that legitimate wireless users can eavesdrop on each other, since they all know the private key. By using encryption to the remote end of the connection, users can neatly sidestep the entire problem. These techniques work well even on untrusted public networks, where eavesdroppers are listening and possibly even manipulating

data coming from the access point. To ensure data privacy, good end-to-end encryption should provide the following features:

- *Verified authentication of the remote end.* The user should be able to know without a doubt that the remote end is who it claims to be. Without authentication, a user could give sensitive data to anyone claiming to be the legitimate service.
- *Strong encryption methods.* The encryption algorithm should stand up to public scrutiny, and it should not be easily decrypted by a third party. There is no

security in obscurity, and strong encryption is even stronger when the algorithm is widely known and subject to peer review. A good algorithm with a suitably large and protected key can provide encryption that is unlikely to be broken by any effort in our lifetimes using current technology.

• *Public key cryptography.* While not an absolute requirement for end-to-end encryption, the use of public key cryptography instead of a shared key can ensure that an individual user's data remains private, even if the key of another user of the service is compromised. It also solves certain problems with distributing keys to users over untrusted networks.

• *Data encapsulation.* A good end-to-end encryption mechanism protects as much data as possible. This can range from encrypting a single email transaction to encapsulation of all IP traffic, including DNS lookups and other supporting protocols. Some encryption tools simply provide a secure channel that other applications can use. This allows users to run any pro-gram

they like and still have the protection of strong encryption, even if the programs themselves don't support it. Be aware that laws regarding the use of encryption vary widely from place to place. Some countries treat encryption as munitions, and may require a permit, escrow of private keys, or even prohibit its use altogether. Before implementing any solution that involves encryption, be sure to verify that use of this technology is permitted in your local area. In the following sections, we'll take a look at some specific tools that can pro-vide good protection for your users' data.

SSL

The most widely available end-to-end encryption technology is *Secure Sockets Layer*, known simply as *SSL*. Built into virtually all web browsers, SSL uses public key cryptography and a trusted *public key infrastructure (PKI)* to secure data communications on the web. Whenever you visit a web URL that starts with https, you are using SSL. The SSL implementation built into web browsers includes a collection of certificates from trusted sources, called *certificate authorities (CA)*. These certificates are cryptographic keys that are used to verify the authenticity of websites. When you browse to a website that uses SSL, the browser and the server first exchange certificates. The browser then verifies that the certificate provided by the server matches its DNS host name, that it has not expired, and that it is signed by a trusted certificate authority. The server optionally verifies the identity of the browser's certificate. If the certificates are approved, the browser and server then negotiate a master session key using the previously exchanged certificates to protect it. That key is then used to encrypt all communications until the browser disconnects. This kind of data encapsulation is known as a *tunnel*. The use of certificates with a PKI not only protects the communication from eavesdroppers, but prevents so-called *man-in-the-middle (MITM)* attacks. In a man-in-the-middle attack, a malicious user intercepts all communication between the browser and the server. By presenting bogus certificates to both the browser and the server, the malicious user could carry on two simultaneous encrypted sessions. Since the malicious user knows the secret on both connections, it is trivial to observe and manipulate data passing between

the server and the browser. Use of a good PKI prevents this kind of attack. In order to be successful, the malicious user would have to present a certificate to the client that is signed by a trusted certificate authority. Unless a CA has been compromised (very unlikely) or the user can be tricked into accepting the bogus certificate, then such an attack is not possible. This is why it is vitally important that users understand that ignoring warnings about expired or bogus certificates is very dangerous, especially when using wireless networks. By clicking the "ignore" button when prompted by their browser, users open themselves up to many potential attacks. SSL is not only used for web browsing. Insecure email protocols such as IMAP, POP, and SMTP can be secured by wrapping them in an SSL tunnel.

Most modern email clients support IMAPS and POPS (secure IMAP and POP) as well as SSL/TLS protected SMTP. If your email server does not provide SSL support, you can still secure it with SSL using a package like Stunnel *(http://www.stunnel.org/)*. SSL can be used to effectively secure just about any service that runs over TCP.

SSH

Most people think of SSH as a secure replacement for telnet, just as scp and sftp are the secure counterparts of rcp and ftp. But SSH is much more than encrypted remote shell. Like SSL, it uses strong public key cryptography to verify the remote server and encrypt data. Instead of a PKI, it uses a key fingerprint cache that is checked before a connection is permitted. It can use passwords, public

keys, or other methods for user authentication. Many people do not know that SSH can also act as a general purpose encrypting tunnel, or even an encrypting web proxy. By first establishing an SSH connection to a trusted location near (or even on) a remote server, insecure protocols can be protected from eavesdropping and attack.

OpenVPN

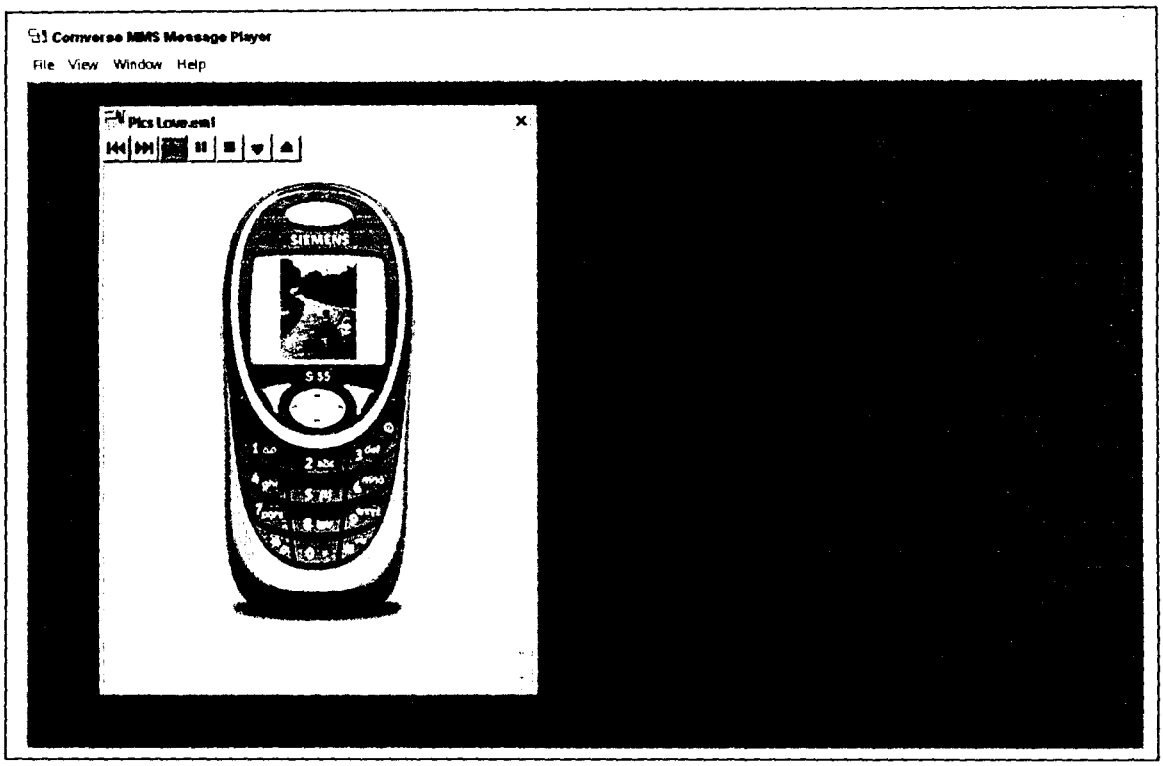
OpenVPN is a free, open source VPN implementation built on SSL encryption. There are OpenVPN client implementations for a wide range of operating systems, including Linux, Windows 2000/XP and higher, OpenBSD,.FreeBSD, NetBSD, Mac OS X, and Solaris. Being a VPN, it encapsulates all traffic (including DNS and all other protocols) in an encrypted tunnel, not just a single TCP port. Most people find it considerably easier to understand and configure than IPSEC. OpenVPN also has some disadvantages, such as fairly high latency. Some amount of latency is unavoidable since all encryption/decryption is done in user space, but using relatively new computers on either end of the tunnel can minimize this. While it can use traditional shared keys, OpenVPN really shines when used with SSL certificates and a certificate authority. OpenVPN has many advantages that make it a good option for providing end-to-end security.

- It is based on a proven, robust encryption protocol (SSL and RSA)

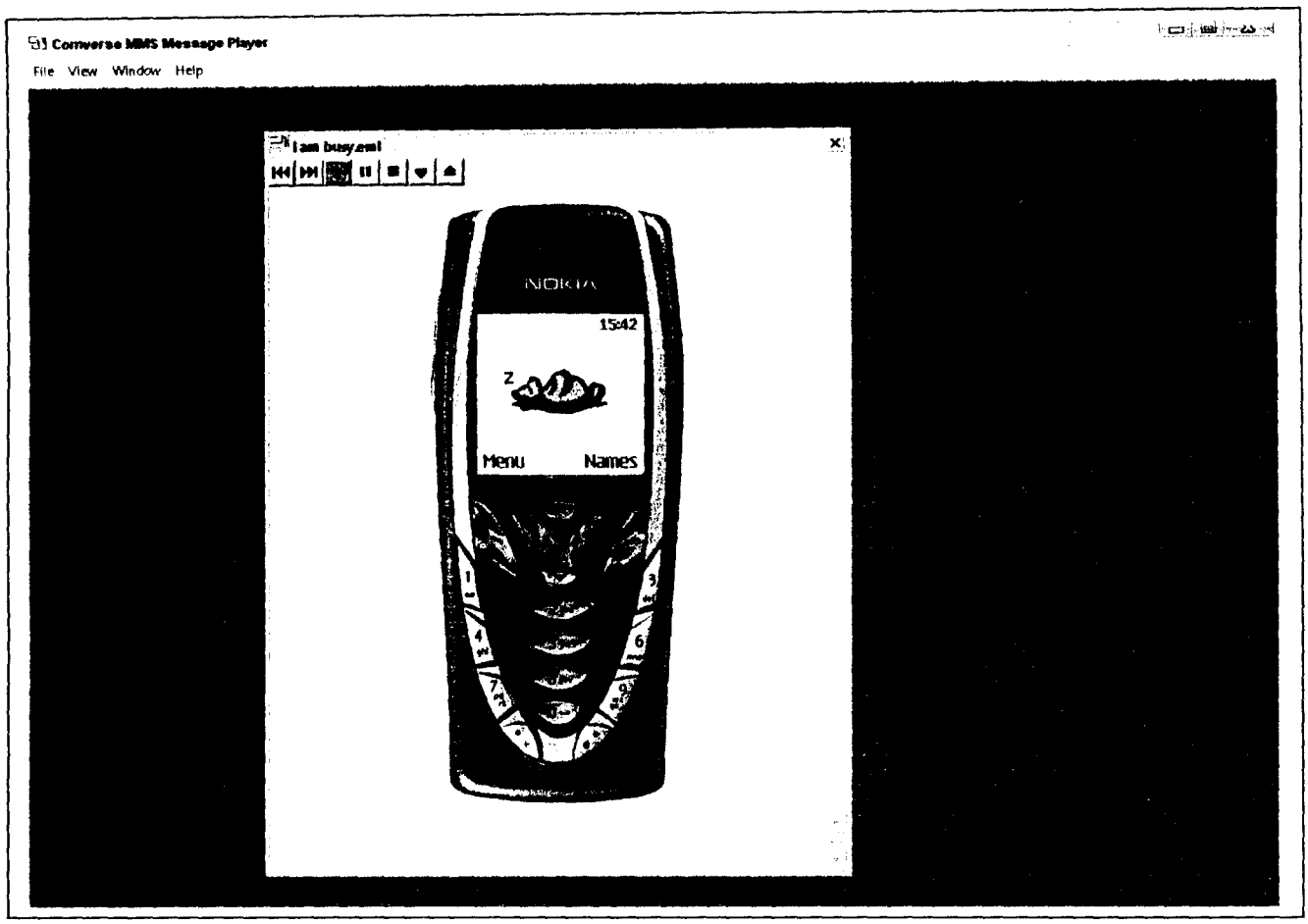
- It is relatively easy to configure
- It functions across many different platforms
- It is well documented
- It's free and open source.

Like SSH and SSL, OpenVPN needs to connect to a single TCP port on the remote side. Once established, it can encapsulate all data down to the Networking layer, or even down to the Data-Link layer, if your solution requires it. You can use it to create robust VPN connections between individual machines, or simply use it to connect network routers over untrusted wireless networks. VPN technology is a complex field, and is a bit beyond the scope of this section. It is important to understand how VPNs fit into the structure of your network in order to provide the best possible protection without opening up your organization to unintentional problems.

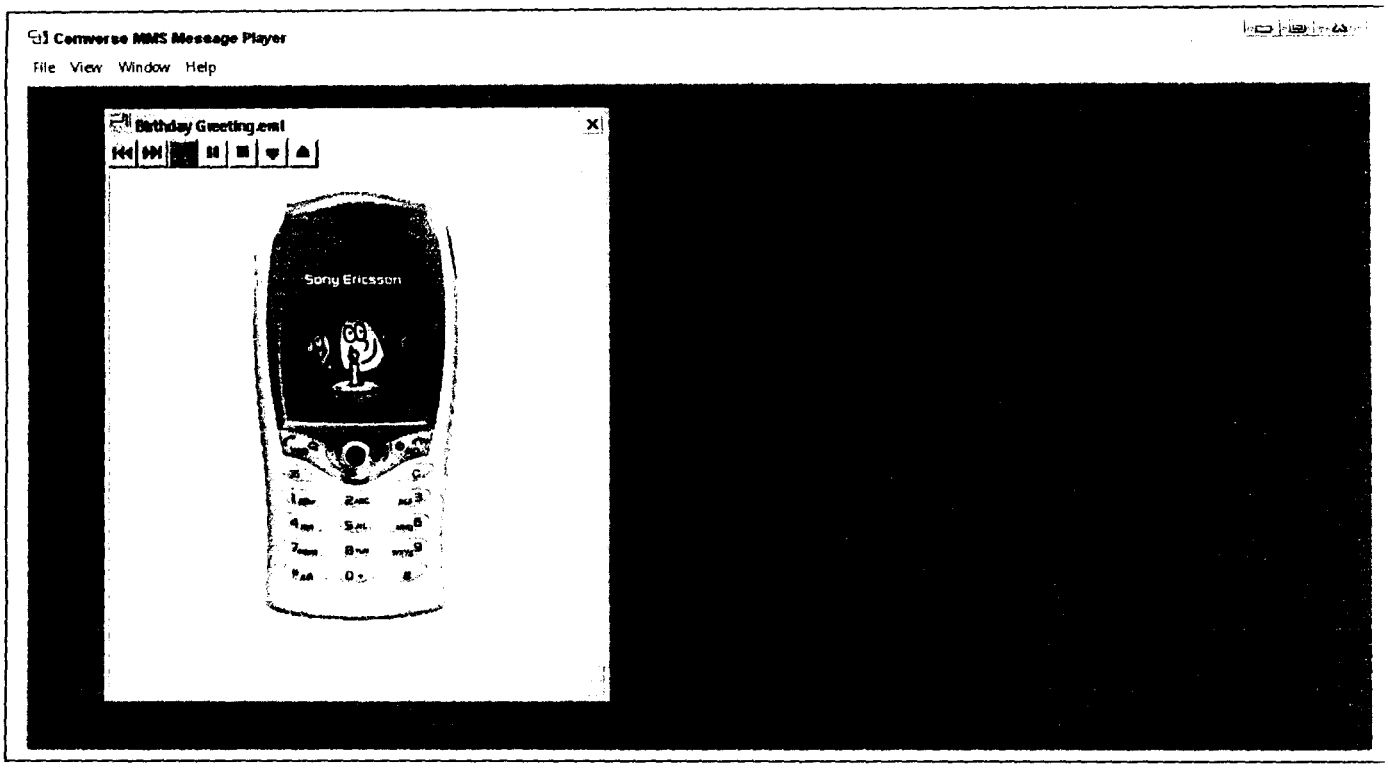
OUTPUT OF THE PROGRAMME



A Sample Multimedia Message Sending (MMS) running on A WAP browser using a Soap Protocol and a Siemens Simulator/Emulator. **Be Inspired**



A Sample Multimedia Message Sending (MMS) running on a WAP browser using a Soap Protocol and a NOKIA 7210 Simulator/Emulator. **I AM BUSY.**



A Sample Multimedia Message Sending (MMS) running on A WAP browser using a Soap Protocol and a SonyEricsson Simulator/Emulator. **Happy Birthday to you**.

CHAPTER FIVE

CONCLUSION

This work is an outlining of the principles of wireless networks. It takes ideas from the field radio physics combined with principles of cutting to fashion out a peculiar set of principles for wireless networks.

The proliferation of wireless networks and the resultant effect on man is enormous. We see the growth of the telecommunications industry with earnings in the range of oil revenues and as more and more people around the world get connected through wireless networks, it is expected that these networks will play more dominant roles in the economy of nations. For this reason any nation willing to become relevant in this era must have expertise in the field of communications using radio waves.

5.2 RECOMMENDATIONS

Further work is recommended. Here only the basic principles are outlined. Research in wireless networks is still young and more ground still needs to be covered especially by developing nations like Nigeria.

Security is one principal area of research that needs a lot of attention. This is because critical information can be lost or transferred to wrong hands should the security system fail.

REFERENCES

Bracewell, R.N. (2000). The Fourier Transform and its Applications. McGraw Hill Publishers, Singapore

Corrina Aichele et al., (2006). Wireless Networking in the Developing World. Limehouse Book Sprint Team, Lonndon

C.S. French (2000). Computer, Ashford Colour Press, Gosport

Prett,T and Bostian C.W. (1998). Satellite Communications. John Wiley and Sons, New York

Todd Lamle, (2000).Cisco Certified Network Associate Study Guide, Second edition. Sybex Inc., U.S.A

```
/*
 * SOAPSample.java
 */

import com.comverse.mms.mmspade.api.*;

import javax.mail.internet.AddressException;
import java.awt.*;
import java.io.File;
import java.io.IOException;

public class SOAPSample {

    private MultimediaMessage createMessage() {

        // first slide
        TextMediaElement text1 = new TextMediaElement("MMS\n\n");
        text1.setSize(TextSize.TextSizeLarge);
        text1.setColor(Color.blue);
        ImageMediaElement logo = null;
        MelodyMediaElement backgroundMusic = null;
        try {
            logo = new ImageMediaElement(new File("comverse-logo.gif"),
ContentTypes.GIF);
            backgroundMusic = new MelodyMediaElement(new
File("background.imy"), ContentTypes.IMELODY);
        } catch (IOException e) {
            System.out.println(e.toString());
        }
        SimpleSlide slide1 = new SimpleSlide();
        try {
            slide1.add(text1);
            slide1.setElementTiming("text", 1000,
ISlide.DEFAULT_TIMING);
            slide1.add(logo);
            slide1.add(backgroundMusic);
        } catch (ElementAlreadyExistsException e) {
            System.out.println(e.toString());
        } catch (ElementNotFoundException e) {
            System.out.println(e.toString());
        }

        // second slide
        TextMediaElement text2 = new TextMediaElement("Brings");
        text2.setSize(TextSize.TextSizeLarge);
        text2.setColor(Color.blue);
        ImageMediaElement future = null;
        try {
            future = new ImageMediaElement(new File("thefuture5.gif"),
ContentTypes.GIF);
        } catch (IOException e) {
            System.out.println(e.toString());
        }
        SimpleSlide slide2 = new
SimpleSlide(Layout.LayoutTextAboveImage);
        try {
```

```
            slide2.add(text2);
            slide2.add(future);
        } catch (ElementAlreadyExistsException e) {
            System.out.println(e.toString());
        }

        // third slide
        TextMediaElement text3 = new TextMediaElement("To your
mobile\n\n");
        text3.setSize(TextSize.TextSizeLarge);
        text3.setColor(Color.blue);
        ImageMediaElement mobile = null;
        try {
            mobile = new ImageMediaElement(new File("pele.gif"),
ContentTypes.GIF);
        } catch (IOException e) {
            System.out.println(e.toString());
        }
        SimpleSlide slide3 = new SimpleSlide();
        try {
            slide3.add(text3);
            slide3.add(mobile);
        } catch (ElementAlreadyExistsException e) {
            System.out.println(e.toString());
        }

        // fourth slide
        ImageMediaElement today = null;
        try {
            today = new ImageMediaElement(new File("today.gif"),
ContentTypes.GIF);
        } catch (IOException e) {
            System.out.println(e.toString());
        }
        SimpleSlide slide4 = new SimpleSlide(5000,
Layout.LayoutImageOnly);
        try {
            slide4.add(today);
        } catch (ElementAlreadyExistsException e) {
            System.out.println(e.toString());
        }

        // adding slides to content
        MessageContent content = new MessageContent();
        content.addSlide(slide1);
        content.addSlide(slide2);
        content.addSlide(slide3);
        content.addSlide(slide4);

        // adding content to message
        MultimediaMessage message = new MultimediaMessage();
        message.setContent(content);

        // setting subject
        message.setSubject("SOAP Sample MMS message");

        // setting sender
```

```
        MMSAddress sender = null;
        sender = new RFC2822Address("sample@comverse.com");
        if (sender != null)
            message.setFromAddress(sender);

        return message;
    }

    public static void main(String[] args) {
        if (args.length < 2) {
            System.out.println("Usage: SOAPSample <Recipient> <SOAP
Server Address>");
            System.exit(1);
        }

        SOAPSample sample = new SOAPSample();

        // create the MultimediaMessage object
        MultimediaMessage message = sample.createMessage();

        // create the Recipients object
        Recipients recipients = new Recipients();
        try {
            recipients.addRecipient(args[0]);
        } catch (AddressException e) {
            System.out.println(e.toString());
        }

        // create the SubmitOptions object
        SubmitOptions options = new SubmitOptions();
        options.requestDeliveryReport(false);

        // create the SubmitRequest object
        SubmitRequest request = new SubmitRequest(message, recipients,
options);

        // Creating the SOAPSender
        // -----------------------
        // the address of the SOAP server
        String soapServer = args[1];
        // the ID of the VASP
        String vaspID = "1";
        // the ID of the VAS
        String vasID = "1";
        // the address that will appear as the "Sender" of the message
(optional parameter, can be null)
        RFC2822Address senderAddress = new
RFC2822Address("admin@mms.demo.com");
        // the MM7 schema to use (optional parameter, can be null - the
default schema is the one used by Comverse MMSC)
        String mm7Schema = null;
        SOAPSender soapSender = null;
        try {
            soapSender = new SOAPSender(soapServer, vaspID, vasID,
senderAddress, mm7Schema);
        } catch (Exception e) {
```

```
            System.out.println("SOAPSender was not created:
"+e.getMessage());
            System.exit(1);
        }

        /*
        // if the SOAP server uses authentication, set the username and
password details:
        soapSender.setUsername("username");
        soapSender.setPassword("password");
        */

        /*
        // This is another way to create a SOAPSender, by creating a
properties file with the desired parameters.
        // (look at the soap.properties files for the correct parameter
names).
        Properties properties = new Properties();
        try {
            SOAPSender anotherSender = new SOAPSender(properties);
        } catch (IllegalArgumentException e) {
            System.out.println("Error in properties");
        }
        */

        // send the request
        IResponse response = soapSender.send(request);
        if (response.isSuccessful())
            System.out.println("Message was sent.");
        else
            System.out.println("Message was not sent: " +
response.getStatusText());
    }


}
```

% Abubakar Block Industry,
P. O. Box 840,
Bosso - Minna.

8th May, 2006.

The Secretary,
Evaluation and Implementation Committee,
Ibrahim Badamasi Babangida University,
Lapai.

Sir,

APPLICATION FOR A SUITABLE ACADEMIC OR NON-ACADEMIC POST.

I wish to apply for a lecturing or any suitable non-academic post in your institution.

I am an indigene of Bida Local Government of the State. I had my National Certificate of Education (NCE) in Chemistry/Mathematics from College of Education, Minna in 1995 and later obtained a Bachelor of Technology degree (Second Class, Upper division) in Chemistry/Polymer from the Federal University of Technology, Minna in 2005.

I have been teaching Chemistry at Secondary School level since 1996 and had acted as the Area Chemist in Gombe Area Office of the Petroleum Pipeline Products and Marketing Company (P.P.M.C.) during my one year Youth Service.

Attached are copies of my Curriculum Vitae and Credentials.

I will be very glad if my application is favourably considered and granted.

Thank you in anticipation.