Data Communications with CNZ

BTECH 451A&B PROJECT REPORT

Department of Computer Science

NAME: Arun Manohar Vejendla

UPI: avej002

ID: 4866880

Email: avej002@aucklanduni.ac.nz

University of Auckland

2011

Abstract

This report explains the work completed up to date for the final year BTech project at Computers New Zealand (CNZ). It covers the project overview, describes the themes and presents a short description of CNZ. The main goal of this project is to test and record performance levels for various wireless bridges that have been shipped from Taiwan; to check whether they meet the expectations of CNZ. Secondary goal is to look into an IP video surveillance problem at CNZ.

Initial benchmarks or background information for learning was not provided in the sense that previous BTech projects at CNZ focused mainly on IP video surveillance experimentations; but did not involve any wireless bridge testing. Therefore there is no transfer of learning from previous years. The main part of this report will describe the research involved especially on the wireless technologies and standards that are present in the current world which helped me understand the overall themes of the project in depth. Chapter two explains the specifications, application modes and the limitation for the CAP501-5D devices that I have used for this project.

The rest of the report illustrates the results gathered from my investigations which were significantly important when considering the goals and requirements of CNZ; hence the business personnel can make use of the results which can help them improve their already existing implementations at some level. It also includes the short comings throughout the first half of the year and how the work involved in second part of the year influence the shape of the project. Recommendations and further conclusions on this project according to my supervisors point to view have also been recorded. Details on how this project helped me learn in a professional environment and how it can possibly shape my future; the configuration details which are necessary for every user to make the communication work between the devices are present in the last chapters of this report.

Contents

Abstract.....2

Chapter 1: Introduction.....4
1.1 The Project.....4
1.2 Company Background.....4
1.3 Project themes.....4
1.4 Project Goals.....5
1.5 Project Schedule.....5

Chapter 2: Bridge CAP501-5D.....6
2.1 CAP 501-5D Specifications.....6
2.2 Modes of CAP 501-5D.....7

Chapter 3: Testing Indoors and Outdoors.....9
3.1 Equipment Setup.....9
3.2 Configuration Steps.....9
3.3 Indoor Experimentation Setup.....11
3.4 Limitations.....13
3.5 TX Power Tests.....13
3.6 Antenna Polarization Tests.....14
3.7 Outdoor Testing Plans.....16
3.8 Blind Outdoor Testing.....18
3.9 Improved Outdoor Testing.....19
3.10 Work of Bridge – Model B.....26
3.11 Commercial Project.....28

Chapter 4: IP Video Surveillance.....29
4.1 Problem.....29
4.2 Solution: Cisco MediaNet.....29
4.3 Other Work.....32

Chapter 5: Problems Encountered and Solutions.....32
5.1 Technical.....32
5.2 Non-Technical.....34
5.3 Future Considerations.....34

Chapter 6: Achievement and Future Work.....35
6.1 Achievements.....35
6.2 Project Deliverables.....35
6.3 Short Comings.....36
6.4 Future Work.....36
6.5 Conclusion.....37

Acknowledgements.....38
References.....38
Appendix.....39

Chapter 1

Introduction

The Bachelor of Technology in Information Technology is a four year honours degree programme with selection of courses from Computer Science and Information Systems. The third and fourth years of the programme allowed me to explore my own interests. In the final year, students do a one year compulsory project for a company based on their interest.

1.1 The Project

My final year BTech project is a data communication project which will be carried out at a company called Computers New Zealand (CNZ) located in Albany, North Shore. Two organisations are involved in this project; the science faculty that offers the BTech Project and CNZ that sponsored this project. This report will describe the final year project carried out in 2011 by me, Arun Vejendla.

1.2 Company Background

CNZ is a total information system and solutions provider which is under the management of Compucon House [1]. CNZ has skills and capabilities to implement information and automation systems for meeting client's business objectives. Their determination is to increase the client's productivity and competitiveness. CNZ expertise is focussed on 2 inter-related solutions for business customers:

(a) Information Systems

(b) Video Surveillance Systems

The Compucon brand is well known in the industry for its reliability and computer range. CNZ builds on this foundation and provides 5-star customer and technical services to meet customer expectations and solution deadlines [2].

- Visit the website for more information: www.cnz.co.nz

1.3 Project Themes

There are two themes to this project.

1. Testing wireless bridges (based on a radio that CNZ sourced from Taiwan) in various configurations to establish the performance specifications. The product that CNZ imported has 2 variants. Model A is a wireless bridge and it consists of a radio and a built-in flat panel antenna. Model B is a radio only and it has the same housing as

Model A but it does not have any built-in antenna inside the housing. For Model B to act as a Wireless Access Point, we will need to connect it to an external antenna. We have a choice of different external antennas. The radio has been certified to IEE 802.11n standards and is suitable for operation in 5GHZ spectrum. I am expected to test the wireless bridges in the workshop and in real life environments and to state the maximum performance and limitations.

2. CNZ has been involved in video for surveillance use. One camera typically requires 3Mbps of bandwidth. Suppose the surveillance system has 30, 60 and 90 cameras respectively, the video will have very substantial impact on any 100Mbps local area network. I am expected to provide a solution to the system administrators on how the video traffic should be managed.

1.4 Project Goals

Primarily, the key objective for the year is to focus on theme one which involves two versions of Model A bridges; one with a 200 milliwatt (mW) radio and the other with 500 milliwatt (mW) radio. These bridges have been tested in both short (less than a kilometre) and long ranges (kilometres). The testing is conducted in an accurate manner in order to achieve results that are useful for commercial purposes; so that CNZ can decide which model to use in their future implementations. Theme A took an enormous amount of time so less emphasis was placed on theme two but it is still done.

1.5 Project Schedule

Session	Theme A	Theme B
1	Introduction to Outdoor Wireless Technologies	Introduction to IP video surveillance and problem
2	Validation of product specifications & performance	Investigation of readily available solutions in the industry
3	Testing the performance under different scenarios	Investigation the existence of an existing IPVS system
4	Definition of industry & regulatory requirement for wireless networks	Propose an alternative solution or recommendations on system
5	Propose packaged solutions for sample projects	Formulate business packages/solutions suitable for range of IPVS requirements
6	Complete documentation for installation and technical support	Testing of software or management of video surveillance over the internet
7	Presentation of project theme and formalize all deliverables	Presentation of project theme and formalize all deliverables

The table above shows the initial schedule for both first and second semester but it did change as the year went on due to the typical problems and delays a normal project implicates.

For the first few weeks of semester one, I have been advised by my company supervisor to conduct research on the existing wireless technologies, protocols, various types of antennas and the bridge CAP501-5D to understand the concepts of data communications. These will be explained further in the report. The project then turned practical, which involved my first look at the hardware devices provided by CNZ to establish a simple point to point connection at home; to get the configuration and communication working. Once I finished the configuration and setup, CNZ advised me to move onto the actual indoor testing of the products and to provide them with some analysis and values. I have also done research work on IP video surveillance (theme two) in semester one while I was planning for 'line of sight' for outdoor testing and waiting to sort out the UPS (Uninterruptable power supply) problem.

For the second semester, all the work has gone into conducting outdoor experiments. I have conducted tests where the two wireless bridges communicated over a kilometre. The testing involved many failures eventually leading to successful results which will be explained further in chapter 4.

Chapter 2

Bridge CAP 501-5D

CNZ has provided me with several bridges named 'WiBorne CAP 501-5D'. This chapter describes the specifications and modes that the device operates in.

2.1 CAP 501-5D Specifications

WiBorne CAP 501-5D is a high power outdoor wireless bridge, access point, router and CPE (customer premises equipment - generally located at customers end). This bridge acts as a point of connection to wireless networks for service providers that provide last mile services. CAP 501-5D has an option of built-in 5GHz 15dBi dual polarity directional antenna or 2 N-type connectors without antenna (one of the first connectors capable of carrying microwave signals). It consumes 200mW (23.0103 dBm – power ratio in decibels) or 500mW (26.9897 dBm) of high power depending on the version. This bridge connects to Wi-Fi mesh or WDS infrastructure to provide the customers with an Ethernet connection for local access. CAP 501-5D works point to point or in point to multipoint topologies. This device supports standards 802.11n and 802.11a and the security is provided using WEP, Wi-Fi

protected access (WAP and also WPA2). It has weather proof housing for physical protection. This device also provides quality of service which means proper management of bandwidth and traffic prioritization is taken care of, in other words the most important data is sent first and the least important is sent after the high priority data is sent first [3] [4].

2.2 Modes of CAP 501-5D

First of all, the device CAP 501-5D can be used in four different modes such as AP mode (or can be a combination of both AP + WDS), WDS mode, CPE mode and Client Bridge + universal repeater mode.

Access point mode (AP mode):

An access point can be either a main, relay or remote base station. The main base station is connected to a wired network. The relay base station is station that relays data between the base, relay and remote stations. The remote base station accepts connections from wireless devices such as laptops. There are two types of AP modes. One is pure AP mode (access point without WDS link) and the other AP/WDS mode. In pure AP mode, generally CAP 501-5D device can be deployed as a fixed access point that connects to a wired network (LAN) that is available and acts as a source of wireless connection point (AP) for other wireless devices so that they could access the internet.

Figure 1:

In AP+WDS mode, an access point can be deployed as a fixed wireless AP that provides a WDS link to expand the network. This mode enables wireless interconnection of several access points in a network and also accepts the wireless connection of clients. In the diagram below, AP+WDS mode is shown and we can see that using a WDS link we can expand the network wirelessly so in this case another wireless AP (CAP 501-5D bridge) is connected so it also accepts many wireless clients to provide wireless access to internet

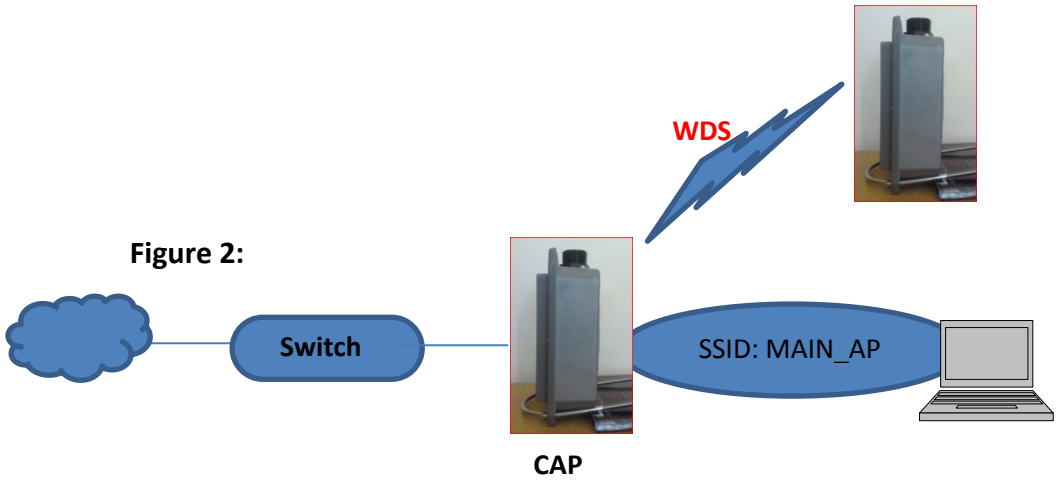


Figure 2:

AP Mode provides single point of control and security for the wireless LANs which helps in keeping the network secure and also controlled.

WDS mode (Wireless distribution system):

WDS mode is also called the repeater mode. Wireless distribution system is a system that provides the wireless interconnection of bridges in the network that is using the standard IEEE 802.11. In this case, the devices are our CAP 501-5D and only they are allowed to communicate with each other but not the clients such as laptops. Because this mode allows the access points to be interconnected, the wireless network will be expanded without the need of physical wiring. It allows one access point to receive data wirelessly from another access point and forward that data to its own wireless clients. The access point allows one or more WDS links but do not allow any wireless clients such as laptops have a direct connection to it. The connections can be point to point (shown in the diagram below), point to multipoint and multi-point.

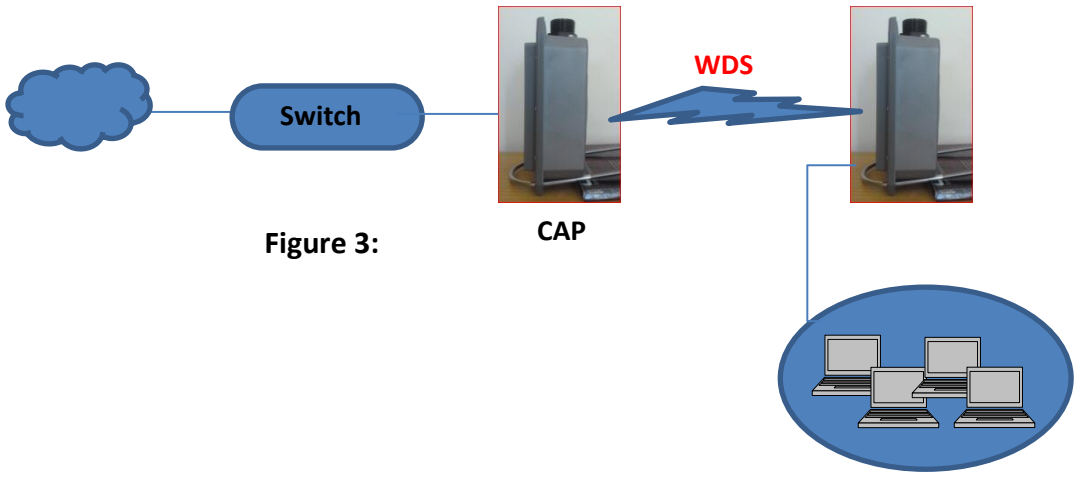


Figure 3:

According to the specifications and objectives provided by my company supervisor, WDS is the mode that has been used for testing in this project because it allows a connection between two bridges; hence communication between two ends (laptops).

Chapter 3

Testing Indoors and Outdoors

This Chapter will first illustrate my first trial, indoor testing results and then move onto the details of outdoor experimentation.

Note: Assume I used 200mW version bridges in all the experiments unless specified

3.1 Equipment Setup

- Two 'CAP 501-5D' bridges
- 4 cat5 cables
- Two PSE devices
- Two power cables
- Two laptops (one with vista and other with windows 7 operating system used)

Regarding the equipment, the two bridges are used so that it is possible for one computer or laptop to communicate with the other laptop; because we are concerned about a point to point connection. The cat5 cables are capable of transporting both power and data at the same time to the powered device (in this case, the CAP 501-5D bridges) and this is also known as Power over Ethernet technology (refer Appendix). The PSE devices act as a medium so that the cat5 cables can carry power and data; the cat5 cables are connected to the PSE devices in an organised arrangement. I have used two different operating systems; one with windows vista and the other with windows 7. It is recommended to use both laptops with the same operating system to avoid extra details and conflicts because; obviously if you perfect configuring a laptop and the bridge under one operating system, the other laptop and bridge will be easier to configure because it just the repetition of the same process again.

3.2 Configuration Steps

Configuration and how it is done is shown below very briefly because it is very complicated to put that much detail into this report.

Step1: Hardware configuration:

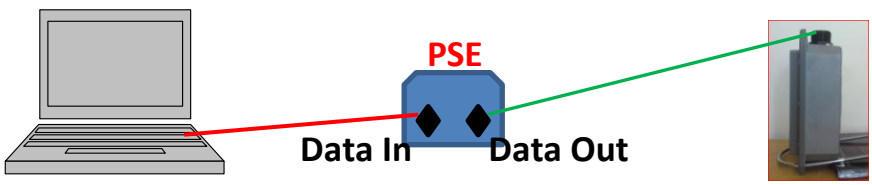


Figure 4:

This is the first step – to set up the hardware in an accurate manner. By looking at the above picture we can see that it is important to figure out which cable goes into which slot of the PSE device; otherwise the communication won't take place between the two laptops. So, one of the cat5 cables that is connected to the laptop must go into the 'data in' slot of the PSE device and the other cable that is connected to the CAP501-5D bridge must go into the data out slot. Finally, to finish off the hardware setup we must attach the power cable into the PSE injector and connect it to the power outlet.

Step2: Network adaptor configuration:

It is important to assign a static IP address to our laptops network adaptor before configuring the access point (CAP501-5D bridge) in the subnet of 192.168.2.x range; for example 192.168.2.10, 192.168.2.200.

Step 3: Firewalls and antivirus:

These applications must be disabled or removed for configuring the access points (bridges). If the applications are not disabled, they will not let the web interface open up; which is crucial in order to configure the access point. To open up the web interface, type in the default IP address – 192.168.2.254 into internet explorer or other web browser and press enter.

Step 4: Configuring WDS link

This step is crucial for the communication between two laptops

- Make sure you have two bridges for the communication to take place
- Select system → under operating mode → select WDS mode
- Note the MAC address of the remote bridge (present on the device) – not the one you are configuring at the moment
- Click on WDS setup →make sure enable is ticked → Enter remote bridges MAC address
- Click on save → go to system → click on save&reboot button.

Now, the configuration for one access point has been setup, now follow the same procedure with another laptop and remote bridge.

Note: But make sure that this remote bridge's IP address is not the default 192.168.2.254 anymore, we have to change it but within the same range. This is because two devices cannot have the same IP addresses.

❖ For detailed configuration notes, refer to the 'Configuration&Support' pdf under my BTech website resources

3.3 Indoor Experimentation Setup

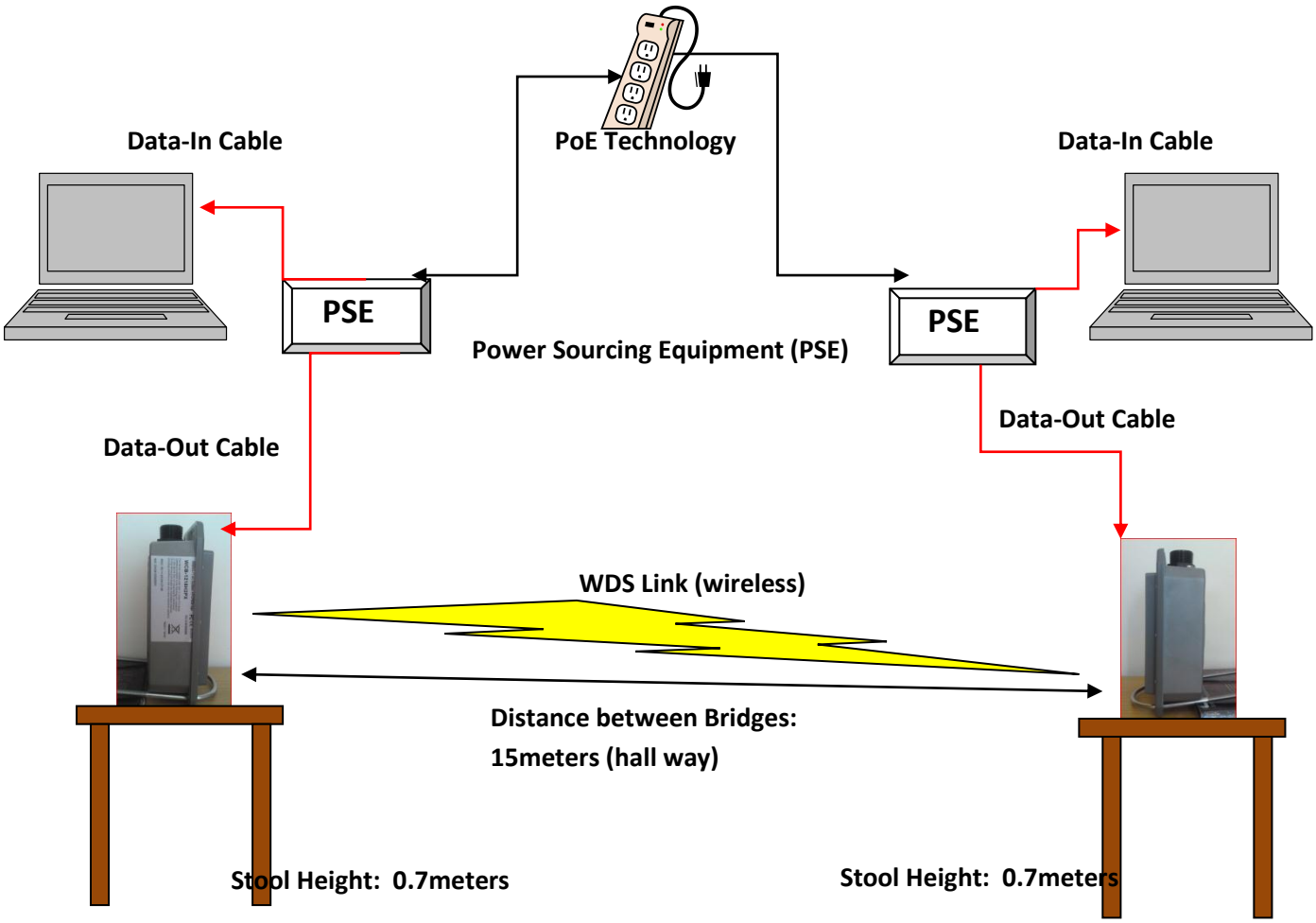


Figure 5:

My First Trial:

The above diagram shows the way I arranged my equipment for my indoor tests. Before I talk about the results, the IP addresses and MAC addresses used for this experiment are shown below mainly to clarify the 192.168.2.**x** range needed for these experiments

Laptop 1:

- IP address: 192.168.2.10 – network adaptor
- Subnet mask: 255.255.255.0

Main access point (attached to laptop one):

- 00:11:A3:0A:C7:40

Laptop 2:

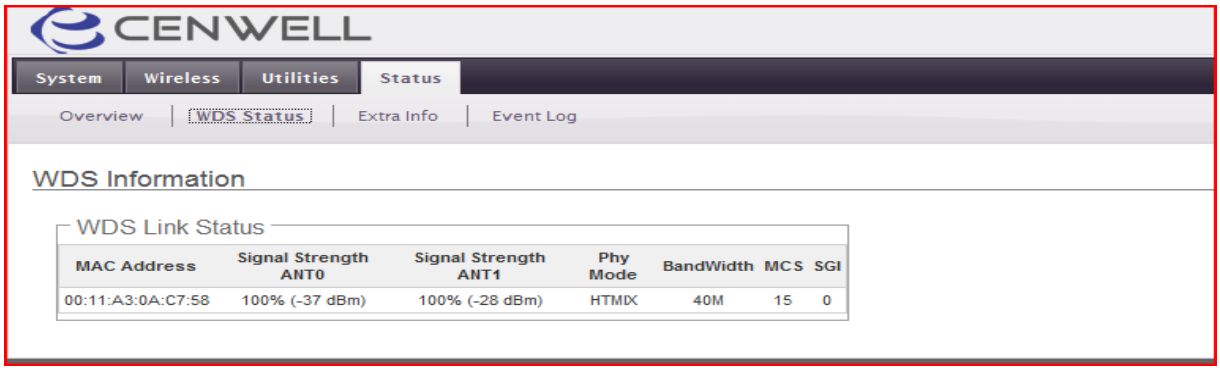
- IP address: 192.168.2.100 – network adaptor

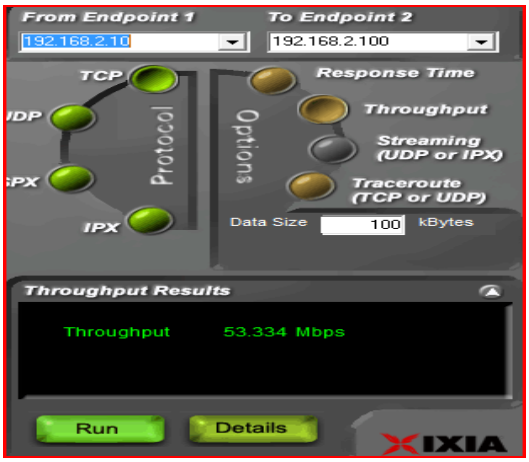
- Subnet mask: 255.255.255.0

Remote access point (attached to laptop two):

- 00:11:A3:0A:C7:58

The below screenshot shows the WDS link status between the two bridges. It shows the bandwidth, the signal strength of the two connected bridges.





QCheck software has been used to analyse the throughput over a range of data sizes. This software allows us to measure data rates, response times for many protocols [5]. For example, the TCP (refer Appendix) throughput measured for a 100kBytes of data is 53.334Mbps as shown on the QCheck picture to the right.

Now I present the range of values measured:

Data Size (kBytes)	Throughput (Mbps)
100	53.334
300	75.000
500	81.633
700	82.353
900	85.714
1000	86.002

Mbps refers to Megabits per second and it is the data transfer speed between our devices. The throughput values (average rate of successfully delivered packets) are very important for this project because the aim of conducting these experiments is to see how well these

devices (different versions) perform in reality; therefore devices that achieve better throughput values means they are better to use in commercial implementations.

3.4 Limitations

The manufacturers claim is that CAP 501-5D is capable of transmitting at 300Mbps; according to the Wi-Borne CAP501-5D brochure and also the wireless standard 802.11n. The first glance at my results, it was a complete shock for me because the data rates are nowhere near the expected 300Mbps. The CAP 501-5D bridges used in this experiment has some limitations. The network interface card (NIC) within the device and the physical cabling is only capable of Fast Ethernet; which means it is only capable of transmitting data at the maximum 100Mbits per second. Hence, that is the reason why I only observed values closer to 100Mbps mark. This reason is proved in my weekly meeting with my company supervisor.

3.5 TX Power Tests

CNZ has implemented many bridges in Kaikohe already and they noticed that two bridges have a very poor signal level; therefore data rates are quite poor. I conducted the below tests to check whether adjusting the output power in these bridges may help CNZ improve the quality of signal between these two bridges

Initial Signal strength with default TX value (10%):

WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:40	29% (-78 dBm)	31% (-77 dBm)	HTMIX	40M	4	0

Increased Signal strength with TX value (25%):

WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:40	39% (-74 dBm)	39% (-74 dBm)	HTMIX	40M	4	0

Increased Signal strength with TX value (50%):

WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:40	47% (-71 dBm)	50% (-70 dBm)	HTMIX	40M	13	0

Increased Signal strength with TX value (75%):

WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:40	50% (-70 dBm)	47% (-71 dBm)	HTMIX	40M	13	0

Increased Signal strength with TX value (100% - maximum value):

WDS Information

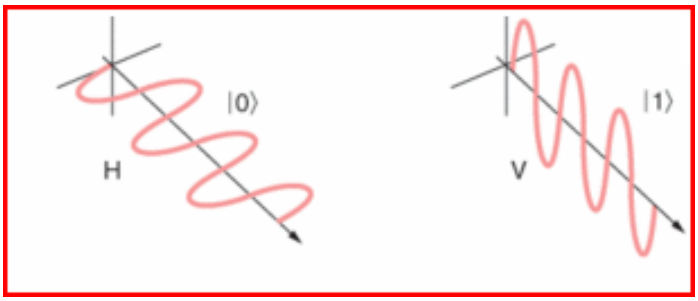
WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:40	65% (-64 dBm)	68% (-63 dBm)	HTMIX	40M	15	0

Increasing the TX value (output power) definitely makes the poor signal strength better. The initial signal strength was 29% at default 10%; TX value is increased to 25%, 50%, 75% and 100% and the signal strength is measured as shown in the above pictures. At 100% TX value, there is significant increase in the signal strength when compared to the initial records. Therefore, because the TX value is used to get appropriate coverage for our wireless network; I recommended CNZ to try this method to improve the signal strength between the two devices.

3.6 Antenna Polarization and Alignment

It is important to consider the antenna polarization when installing bridges and antennas. Polarization of antenna can be defined as the orientation of electric field of radio wave with respect to the earth's surface. Most devices use the horizontal, vertical or circular polarization. An antenna will have one polarization when it is vertically mounted and a different polarization when it is horizontally. For example, refer to the picture below: horizontal (left) and vertical polarization (right)



On the other hand, alignment of the antenna is very important as well. For example, misalignment of 10 degrees (considering the antenna has a Beamwidth of 10degress) will

degrade the signal by at least 3dB (assuming) and a much worse misalignment would definitely degrade the signal strength by a greater value.

Both bridges should be properly aligned to achieve the best signal strength between two stations. By curiosity and to better understand the polarization and alignment concepts, I tested the bridges positioned in various angles to see how it affects the signal strength and throughput; the results are shown below.

Test 1 = Access points: when totally facing opposite direction

WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:58	55% (-68 dBm)	31% (-77 dBm)	HTMIX	40M	13	0

Data Size (kBytes)	Throughput (Mbps)
100	13.333
400	10.423
600	17.778
800	5.937
1000	6.932

Now it is important to understand that the polarization is the same when the bridges are facing towards each other or when facing backwards. The reason why the throughput values are low here is because the back plate of the bridges (picture to the right) blocks of the signals reaching backwards; hence nothing to do with polarization.

Test 2 = rotated horizontally: one bridge facing the other (vertically); while the other bridge is rotated to its side (horizontally)

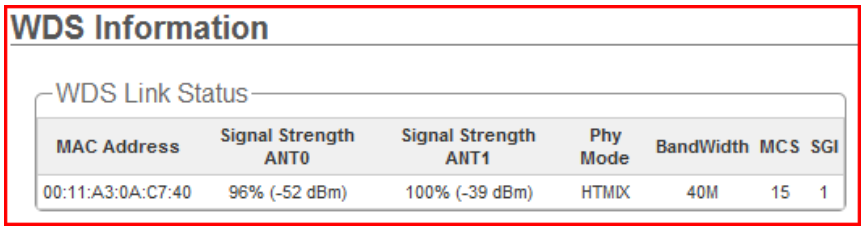
WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:58	89% (-55 dBm)	57% (-67 dBm)	HTMIX	40M	14	0

Data Size (kBytes)	Throughput (Mbps)
100	53.334
400	54.237
600	32.000
800	62.136
1000	80.808

Test 3 = Access points: when totally facing each other



Data Size (kBytes)	Throughput (Mbps)
100	57.143
400	65.306
600	75.000
800	72.727
1000	87.912

Test 2 and Test 3 shows the polarization effects. In test 2, because one bridge is vertical and the other horizontal; both vertical and horizontal polarization comes into play. For example, imagine the bridge's antenna is a shoebox with a thin long slit and it has a light inside on the transmitter side. If you take two such antennas and make them face each other so the slits line up, you get the maximum amount of light transferred from one box to the other (In our case, we get more throughput) as seen in test 3. But when you turn one of the boxes (antennas) so its slit is perpendicular to the slit on the other box, it minimises the light the other slit receives (as seen in test 2). This is the reason why test2 showed lower dates rates when compared to test 3.

The above discussion on polarization and also alignment shows how important it is to consider these issues especially on large scale outdoor projects. CNZ's can improve the signal strength between those two distant bridges by making sure that the flat panel antennas are aligned as accurately as possible and on top of that, both antennas must have the same type of polarization either horizontal or vertical like test3 to achieve best results.

3.7 Outdoor Testing Plans

I have come up with several plans for outdoor point to point connection which is around one kilometre shown further in the report. An additional piece of equipment is required for establishing communication between two bridges outdoors; this is called UPS (Uninterruptable Power System). This device has two batteries that supply power to my laptop and the bridge for a few hours. This enables remote working without any need for main power point. CNZ could only provide me with one UPS; so one side of the equipment is powered using the UPS and the other side is powered using the power point available at Tamaki campus building for example.

Plan1:

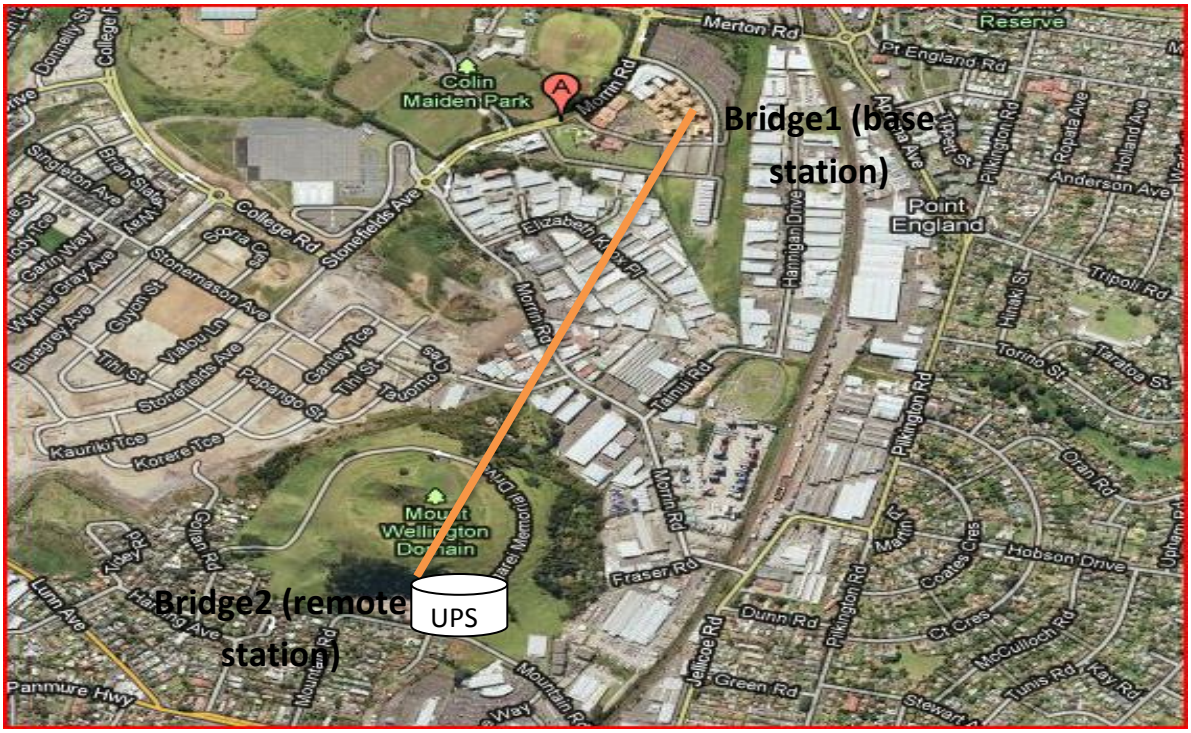
Figure 6:

The above is a map of Tamaki campus. The initial plan was to get my laptop powered in one of the campus buildings and conduct the experiment that stretches from campus to college road. The distance is around 900m. This plan was quickly turned down as I have observed many obstructions in the 'line of sight' path such as buildings, no entry areas, large trees and most of all, the path's visibility is poor (from source to destination and vice versa); hence it is not suitable for this experiment

Plan 2: Figure 7

The above orange line on the map shows a distance of 1.4-1.45 kilometres approximately. One of my friends live here; so I thought of using many long extension cables from his house stretching to the footpath and then setting up the experiment along the road (May road as shown in above picture). This would have been really good experiment as it may involve real world interferences from other Wi-Fi sources but I couldn't get access to his home as he was away and the second reason for turning this plan down is due to New Zealand legality issues.

Plan 3: Figure 8



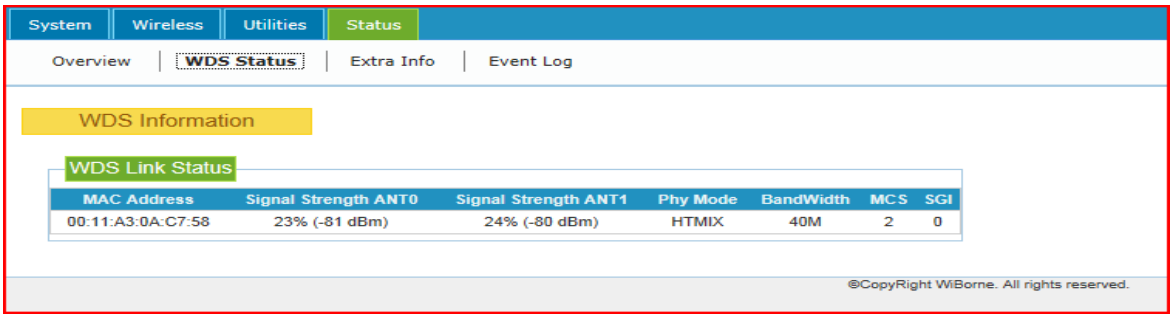
Finally after many more plans, CNZ and I are satisfied with the above plan and conducted the experiment here. One of the bridges is powered via power over Ethernet using an extension cable stretching from a power outlet present close to the entrance of building 723 of Tamaki campus. The other bridge (remote) is stationed on top of Mount Wellington which is 900-1100 meters away from Tamaki campus.

3.8 Blind Outdoor Testing

As I have conducted many indoor experiments, it helped me gain experience in using the devices, configuring them and this eventually helped me push further into more technical and real world outdoor testing. My first outdoor experiment which I call it a 'blind test' and the results are shown below. As my experience grew, the results got better. I call this a blind test because both bridges are held in hands (poor stability) and roughly facing each other (no alignment accuracy). This blind test involved many repetitions over three weeks.

200mW Testing:

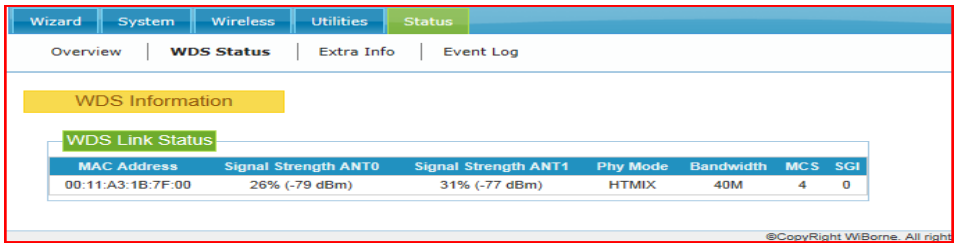
Signal Strength and throughput



Data Size (kBytes)	Throughput (Mbps)
100	1.333
200	1.682
300	19.835
400	15.534
500	5.682
600	9.006
700	9.859
800	6.005
900	1.193
1000	3.859

500mW Testing:

Signal Strengths and throughput



Data Size (kBytes)	Throughput (Mbps)
100	16.374
200	15.534
300	37.500
400	8.488
500	21.379
600	36.354
700	6.250
800	9.552
900	54.962
1000	24.316

‘Blind testing’ revealed significant differences in the data rates between the 200mW and 500mW versions. According to the outdoor throughput values mentioned above, 500mW version is a clear winner. For example, the maximum data rate achieved for the 200mW version is 19.835Mbps where as for the 500mW; the highest data rate achieved was 54.962Mbps. I have only observed two double digit throughput values (e.g. 12.000Mbps) for all 10data captures for the 200mW version but with the 500mW version, most of the 10 captures were double digit data rates.

However, for both versions; the signal strength (due to incorrect alignment – not accurately facing each other over long distance) is only around 24% and this had a major impact on the data rates (throughput); similar to the poor results we have seen in our previous tests. 802.11 operates at frequency 2.4GHz but the default channel used by ‘CAP-501-5D’ bridge is in the 5GHz range; so I thought the Wi-Fi sources around the area cannot be a major cause for the interference which can degrade the signal strength as they operate in different frequency bands but this is wrong according to my supervisor (refer to chapter 5.3). But the throughput achieved is not valuable for CNZ because they are very low.

3.9 Improved Outdoor Testing

I took into account all the downfalls such as alignment problems and UPS problems from my previous trials and improved my experiment’s accuracy; therefore I finally achieved better performance results compared to my previous submission. I went to Tamaki campus many times to conducts the tests; as I faced ‘after-hours’ access problems so I could not finish it in one attempt.

Last time, I have blindly tried to align both bridges (via naked eye - approximation) all the way from Tamaki campus to Mt. Wellington where there is no visibility of both bridges from one end to another as the source and destination are 900 – 1100 meters part. I have planned in various way to increase the accuracy of the alignment in order achieve better data rates. Some of the ways are using binoculars which enables me to have a close look at the destination and angle the device according (expensive solution and I could not get one), bright iPhone candle stick software to increase bridges visibility in night time at the destination but this will not provide accuracy at a level we want. Lasers are cheap and powerful and can reach long distances so this was my solution to the accuracy/alignment problem. I ended up buying two green lasers for 25dollars each: both 50mW (Max Output) with 532nm (Wavelength) and attached one bridge of each version as shown below. Before buying the lasers, I had a look at the New Zealand legislation for laser use [6]. I have taken the precautions and measures mentioned in the legislation before using the laser pointers. I have pointed the lasers in a non-populated area; for example, I used the laser pointers at night time so there is no one present at Tamaki campus during that time.

Figure 9:

At Tamaki campus: Laser firmly attached to the device to fire a ray to the other side – perfectly aligned with antennas angle

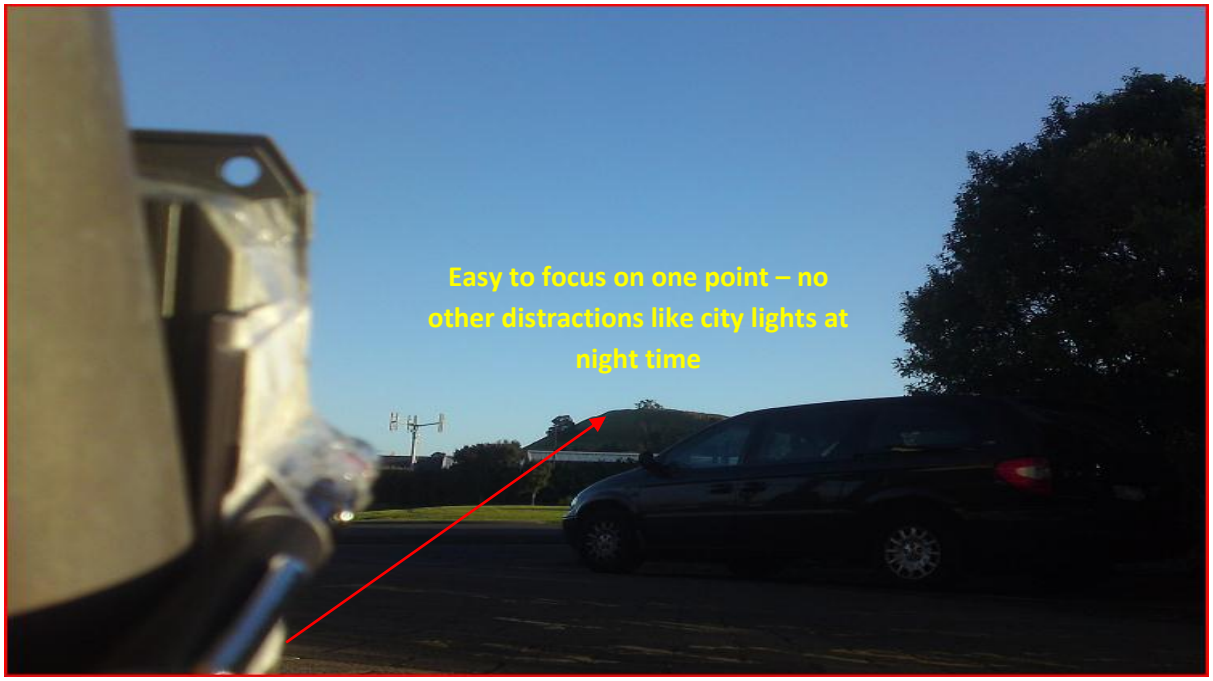
The first Method – I setup all the equipment on Mt. Wellington and fired the laser from the mountain to Tamaki campus (could see the city – lights all over the place). This was a very bad idea because of two reasons: Due to the uneven surface (sloping), the mounting procedure was hard so I held the bridge with my hands. The shaky hands made a huge difference on the other side because the green laser was all over the place and not at a single stationary location (the remote bridge). So I managed to achieve the same signal strength as before but not a better one. By the time, I tried to stabilize the bridge by placing it differently on the mountain, my UPS ran out. The second problem is due to the view; as I am doing this experiment at night time, the view from top of the mountain is just too big as there are lights everywhere and most of the time; I was lost wondering where Tamaki campus was. The below picture is from my second attempt and as you can see, it is hard to notice Tamaki campus with bare eyes even in day light. So this was a very unsuccessful and disappointing day

Figure 10:

The second Method – as I have realized the consequences of bridge not being stable at all from my first attempt, I tried a different method. This time, the laser is fired from Tamaki campus. The bridge is placed at a fixed stationary position and there is no movement at all as you can see from the below diagram. To turn the on the laser, it is a simple a push button which did not cause a major movement problem as the drain pipe supported the bridge. On the other side, I moved and angled the remote bridge according to the lasers ray that landed on the mountain and this is very important because the bridge must be on the same angle as the ray from Tamaki otherwise the alignment is not correct, therefore less throughput values. But the angle of ray was hard to see for a long time as the lasers consumed AAA cells very quickly and this was another problem.

Figure 11:

Figure 12:



I have conducted both and the vertical and horizontal testing; this is to show CNZ which orientation performs better. Therefore their future implementations can be improved.

Outdoor Vertical Test Results (both bridges are vertical – standing up):

First, I started my experiment with the 200mW bridges and then moved to the 500mW bridges. The captured results are shown below and will be explained further in the report: The results are done up to 3 iterations to see the consistency of the results after each attempt.

Status from 200mW Bridge (base station at Tamaki): 192.256.2.200:

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:40	20% (-82 dBm)	55% (-68 dBm)	HTMIX	40M	12	0

Status from 200mW Bridge Two (at Mt. Wellington): 192.256.2.254:

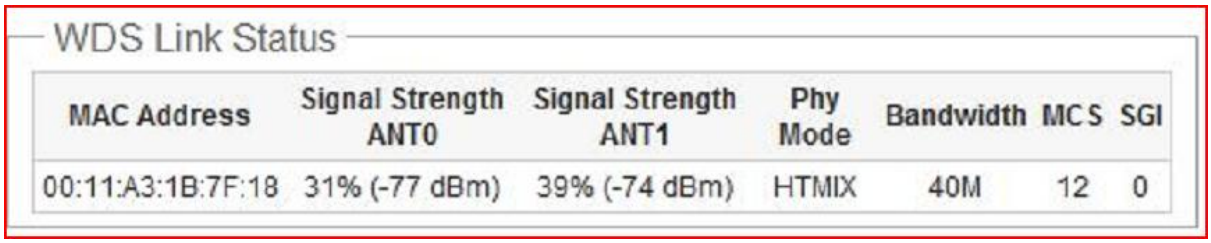
WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:C7:58	24% (-80 dBm)	60% (-66 dBm)	HTMIX	40M	14	0

Data Size (kBytes)	200mW: Throughput (Mbps) – 3 iterations	200mW: Response Time (ms) – 3 iterations

100	12.690 16.000 15.686	Minimum: (3,3,3)ms Average: (1,1,2)ms Maximum: (1,1,2)ms
200	17.778 19.227 21.622	Minimum: (2,3,4)ms Average: (1,1,2)ms Maximum: (1,1,1)ms
400	19.048 18.750 22.430	Minimum: (1,2,2)ms Average: (2,3,3)ms Maximum: (1,1,1)ms
600	17.844 26.669 22.857	Minimum: (1,1,2)ms Average: (1,2,2)ms Maximum: (1,1,1)ms
800	31.841 25.997 32.323	Minimum: (3,4,6)ms Average: (1,1,2)ms Maximum: (1,2,3)ms
1000	30.651 22.346 31.496	Minimum: (1,5,8)ms Average: (1,2,3)ms Maximum: (1,2,3)ms

Status from 500mW Bridge one (base station at Tamaki): 192.256.2.200:



Status from 500mW Bridge Two (at Mt. Wellington): 192.256.2.254:

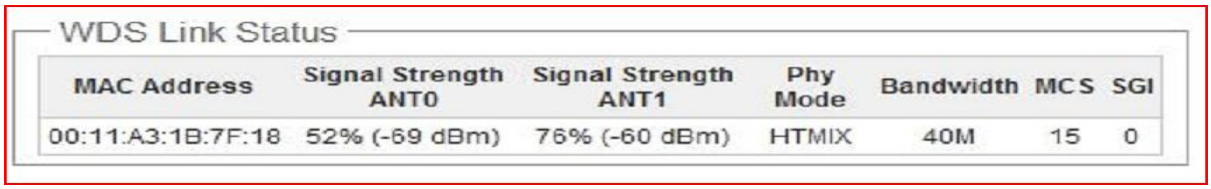
Data Size (kBytes)	500mW: Throughput (Mbps) – 3 iterations	500mW: Response Time (ms) – 3 iterations
100	25.807 22.557 22.857	Minimum: (2,2,2)ms Average: (1,2,2)ms Maximum: (2,2,2)ms

200	26.667 33.334 45.715	Minimum: (2,2,2)ms Average: (1,1,1)ms Maximum: (1,2,2)ms
400	51.613 50.994 45.715	Minimum: (1,1,1)ms Average: (1,2,2)ms Maximum: (1,2,2)ms
600	59.259 64.000 64.000	Minimum: (2,2,3)ms Average: (2,2,2)ms Maximum: (2,2,2)ms
800	58.182 65.979 62.136	Minimum: (1,1,2)ms Average: (2,2,2)ms Maximum: (2,2,2)ms
1000	55.944 67.797 50.794	Minimum: (1,2,2)ms Average: (2,2,2)ms Maximum: (2,2,2)ms

Using lasers significantly increased the alignment accuracy of the bridges and this enabled me to achieve better throughput values. For example, signal strength for 200mW bridges increased from 24% to 55% on ANT1 (of base station) and on the other hand, the signal strength for 500mW bridges increased from 31% to 39%. Due to better signal strength, the data rates have improved to high double digits when compared to blind test results.

Outdoor Horizontal Test Results (both bridges are horizontal):

Status from 500mW Bridge One: 192.256.2.200:


WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	Bandwidth	MCS	SGI
00:11:A3:1B:7F:18	52% (-69 dBm)	76% (-60 dBm)	HTMIX	40M	15	0

Status from 500mW Bridge Two: 192.256.2.254:


WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	Bandwidth	MCS	SGI
00:11:A3:1B:7F:00	50% (-70 dBm)	63% (-65 dBm)	HTMIX	40M	15	0

Data Size (kBytes)	500mW: Throughput (Mbps) – 3 iterations	500mW: Response Time (ms) – 3 iterations
100	50.001 50.001 53.334	Couldn't get it- UPS died

200	64.000 64.000 61.539	Couldn't get it- UPS died
400	64.000 58.182 60.378	Couldn't get it- UPS died
600	60.750 65.954 64.000	Couldn't get it- UPS died
800	75.666 73.563 71.910	Minimum: (1,1,1)ms Average: (1,1,1)ms Maximum: (1,1,2)ms
1000	76.191 74.766 75.472	Minimum: (1,2,2)ms Average: (1,2,2)ms Maximum: (1,1,2)ms

Both horizontal and vertical testing results with my second method (ray from Tamaki to Mt. Wellington) have shown significant differences in data rates compared to all my previous outdoor attempts. 500mW horizontal testing has given me the best outdoor results and now I have proved the manufacturers claim of this device achieving better performance when horizontally placed. This test helped me achieve data rates that CNZ is after for their future commercial implementations. First of all, there is a difference of 20% at least in the signal strength when we compare both vertical and horizontal tests. For example, signal strength around 50% to a maximum 76% helped the throughput increase from a low 20-50Mbps to 50-75Mbps. These results can really help CNZ because, with throughput values such as 75Mbps (table above); they can operate 25 IP video surveillance camera data over the two bridges instead of only running 16 cameras.

Lastly, I will comment on the response time for all my results. As you can see from the vertical testing, the response times are quite high for both 200mW and 500mW bridges; this tells us that there is a lot of packet loss happening (will result in less throughput) and this could be due to interference from other sources, due to alignment issues or the range. Horizontal polarization is used for long distances in order to reduce the interference from the other vertically polarized systems generating signals. Vertical testing surely showed me higher packet loss (maximum response times around 3milliseconds) compared to horizontal testing (maximum response times around 2milliseconds) even when both types of test are conducted fairly in similar fashion. So better the response times, higher the throughput for the system.

3.10 Work on Bridge - Model B

One of the goals was to test 'Model B' Bridge which has a radio but it does not have any built-in antenna inside the housing. My objective was to search for a suitable directional antenna with N-Type connectors that is much powerful than model A's flat panel antenna (better than gain - 15dBi). I contacted a lot of local stores shown below via email and personally visited most stores to find the right antenna

PBtech - University of Auckland

Many PBtech branches do not have the stock in store so I was not able look at the antennas physically; but the store people did provide me with some information from their log sheets and website when I visited them. Because of the lack of expertise in this field, they could not give me more specifications. I did come across a few models that look suitable for our use. I could not find any directional antennas that are good for us.

Model 1: 4IPNET Wireless LAN Outdoor Antenna, Part No: NET4IP1007

- Frequency Range: 2.4GHz – 2.5GHz
- Antenna Gain: 15dBi
- Polarization: Vertical, Omni-Directional
- VSWR: = 1.3 : 1
- Maximum Input Power: 50 watts
- Vertical Beamwidth: 6 degrees
- Horizontal Beamwidth: 360 degrees
- Impedance: 50 ohms
- Dimension: 1480mm(L) x 70mm(D)
- Weight: 800g
- Connector Type: N-Type Female
- Housing Material: Fiberglass
- Operating Temperature: -40C to +60C
- Price: $131.00

Model 2: TPLink Outdoor Antenna, Part Number: NETTPL2416

This antenna is said to be compatible with most of wireless equipment's. Also, the weather proof design ensures that it can work normally for various demanding outdoor solutions.

- Frequency Range 2.4GHz-2.5GHz
- Impedance 50 Ohms, Gain 15 dBi
- VSWR 1.92 : 1 Max
- Polarization Linear Vertical
- Beamwidth (HPBW) Horizontal: 360°
- Vertical: 9 degrees
- Connector Type: N Female
- Dimension 1500mm
- Radiation Omni-directional
- Application Outdoor

- Operating Temperature -40-65C
- Storage Temperature -40-80C
- Operating Humidity 10%-90% non-condensing
- Storage Humidity 5%-90% non-condensing
- Safety Emission and others CE FCC Compliant with RoHS
- Price: $75

Store - Paradigm PCs:

I spoke to the shop person as they are based in Kapiti coast; I gave him the overview of the bridge and that it accepts N-type connection. I asked him whether they have any antennas especially for outdoor wireless LAN use that can fit the bridge. He showed me a few models on their website that I think are quite good.

Model – 4IPNET ANT-PD-242514 Outdoor directional Antenna

This antenna is purposely built for outdoor access points with N-Type connection. This antenna is said to increase the access point's coverage in wide range of environments and the specifications are shown below:

- Width 20.2 cm, Depth 2 cm, Height 20.2 cm, Weight 360 g
- Application: Outdoor
- Directivity: Directional
- Compatibility: 802.11 b/g/n
- Frequency Range: 2.4 - 2.5 GHz, Gain 8dBi or 14 dBi
- Voltage Standing Wave Ratio (VSWR) 1.5:1
- Horizontal Beamwidth: 30°
- Vertical Beamwidth: 30°
- Impedance: 50 Ohm
- Connector provided: 1 x N-Series connector female
- Min Operating Temperature -40 C, Max Operating Temperature 80 C
- Price: $118.00

Although I have searched a lot more stores; most of the stores only have Omni directional antennas and other directional antennas that are not suitable (that are less powerful e.g. shown above with only 8dBi, 14dBi gain) for CNZ's use. I have sent a lot of request to other stores that I cannot visit physically and still waiting on their response for the range of antennas for WLAN use.

3.11 Commercial Project

CNZ is satisfied with my progress and the results that I have achieved and provided them with from all my above experimentation seem to be valuable. This opened up a better path for me where my experience can grow more immensely compared to what I have learned so far. CNZ informed me about a real commercial project they are organising in which I can take part in.

Goal:

The main goal is to establish wireless (WDS) connections from CNZ to the surrounding businesses around Albany; their locations stretching from several hundred meters to 2.5 kilometres away from CNZ building (all located within the blue border below).

Progress:

I have accessed CNZ's roof to check the 'line of sight' to the neighbouring businesses. This is really important because we want to make sure whether the WDS links between CNZ and other clients is possible (whether two bridges can face each other without any obstructions). I have informed CNZ that the line of sight is very poor due to other taller buildings. I visited several places on the above map (Lovell Ct, Pickering road, Rosedale Park) and took photographs to check whether a point to point connection is possible. Unless, there is a higher ground or a tall pole mounting on the building; a connection is not possible. So this is where the project paused; as CNZ is waiting to sort out the antenna and mounting with experienced technicians.

Chapter 4

IP Video Surveillance

This chapter describes the investigation I have done to address the Video traffic problem. The research also involves phone calls and emails to vendors. Due to CNZ already having a

good IP video surveillance systems and surveillance work done in previous BTech projects; I did not have a big task on hand for this theme of the project.

4.1 Problem:

One IP video surveillance camera typically requires 3Mbps of bandwidth. Suppose CNZ increases the number of cameras to say 30, 60 and 90 respectively, the video will have very substantial impact on a local area network. How can the administrators manage the traffic?

4.2 Solution: Cisco MediaNet

MediaNet is an intelligent network optimized for rich media (e.g. video) that provides clever services in order to scale, optimize, and improve the performance of video, voice, and data on the network [7]. MediaNet technology helps the network managers and administrators to address the issues of traditional IP networks by minimizing the complexity, operating costs and helps to scale the infrastructure to achieve the best quality of service while optimizing the bandwidth use and efficiency.

MediaNet Characteristics:

MediaNet is an end to end IP architecture that provides rich media experiences. MediaNet is a combination of a smarter network and smarter endpoints with Cisco's MediaNet technology built into network elements and endpoints. The characteristics of MediaNet are:

- Media aware: detects and improves efficiency for different types of media and applications present to deliver the best experience to the user; some media and applications types are – video surveillance, steaming networks and Telepresence.
- Endpoint aware: where the media end points are automatically detected as well and configured
- Network aware: detects and also responds to the changes occurred within the device, the connection and the service availability

Current Capabilities in MediaNet:

Let us discuss about auto configuration. Auto-configuration has three parts:

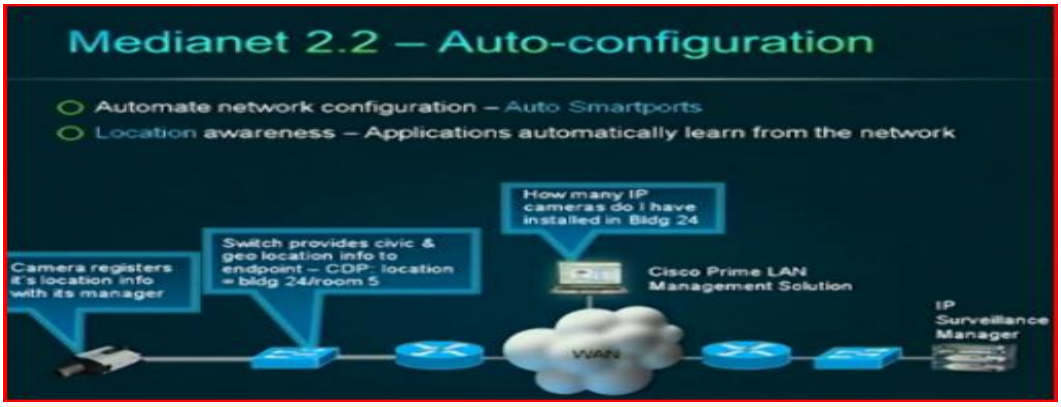
1. First, the endpoint with 'Media service interface' (MSI) announces and identifies itself on the network. These end points typically use the Cisco Discovery Protocol or MAC addresses to advertise themselves.

Cisco Discovery protocol (CDP): This is a data link layer protocol developed by the Cisco systems. This protocol is used to share information such as OS version number and IP address with the directly connected Cisco equipment such as a switch in the below picture. Cisco devices send CDP multicast announcement out of each of the interface. These packets will be received by the Cisco switches or other equipment that support CDP. By default CDP

announcement are sent every 60seconds and each device that receives these announcement stores that information in table. This information is refreshed or updates each time the device receives a new announcement.

2. Second, auto-smart port feature is implemented in the access switch images on Cisco IOS Software. Once a media endpoint is detected, for e.g. a camera in the screenshot below [7]; device specific configuration and quality of service macros are applied to the switch ports. A set of built-in macros for a variety of media endpoints are imbedded in the switch software; based on this auto smart ports dynamically configure the ports.

3. Finally, Cisco IOS software such as 'Cisco prime LAN management solution' allows the network manager to configure the device specific location information on the switches; this information is then transmitted to end point devices.

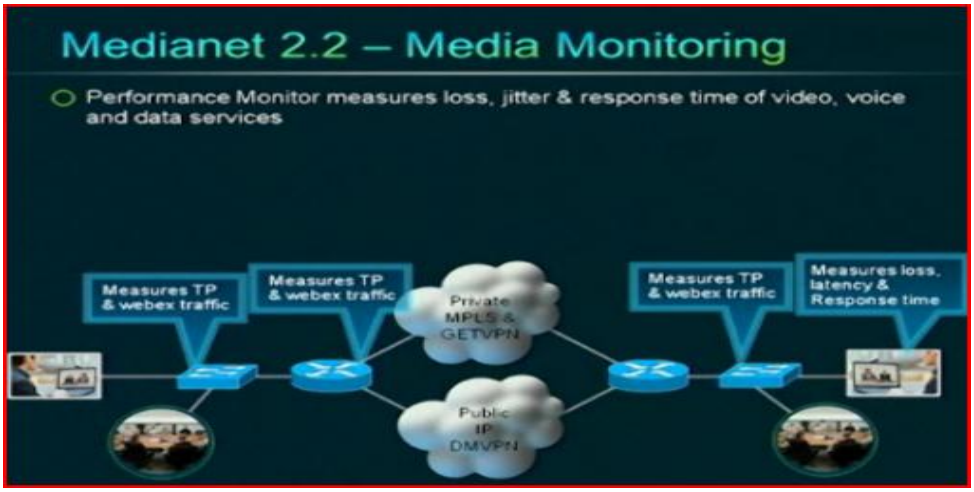


This auto configuration capability completely eliminates the manual steps and greatly simplifies the installation. So imagine having this capability available when deploying hundreds of physical security cameras; it will make life that much easier for the network manager.

Cisco says that MediaNet will resolve the common challenges that customers face when installing video systems [7]. Currently, there are no tools that will help an organization to assess what will happen when they run different types of video traffic on the network. In

the event of quality issues, there is no easy way to identify where the problem is; so post assessment of video quality if extremely difficult.

Cisco introduced media monitoring which is a collection of capabilities that will address these challenges. Performance monitor is a new instrument that is imbedded within the Cisco routers and endpoints. This tool monitors the traffic flows for video, voice and data services and reports issues related to packet loss, jitter and response times of the services.



On the other hand, media trace is an embedded diagnostic capability that can be dynamically activated anytime during the media session. Once this feature is enabled, it walks down the path of the media stream and collects the information regarding the flow in the network during that session

How can it help the Network managers or administrators at CNZ?

As we have talked in the above discussion that, once a Cisco MediaNet device or an end point detects quality issues, it automatically triggers the source and collects the information. This feature is very powerful because it is triggered dynamically while the problem is occurring [7].

The IPSLA (IP service level agreement) video operation by Cisco gives the administrator, the ability to generate synthetic traffic that truly mimics any type of traffic. For example, synthetic traffic can be generated before an important event to ensure that the network is able to meet the quality expectations or it can be used in pre or post deployment assessment.

CNZ switches vs. MediaNet

One of my objectives was to find out whether traditional switches existing at CNZ are capable of supporting MediaNet. I have called the Cisco services USA and asked them regarding the MediaNet and whether the other brands of the switches at CNZ are capable of providing or supporting the MediaNet services like the cisco switches. First of all, MediaNet

is a solution designed by Cisco but it can be used on other switches and brands also. According the technician/cisco representative, he advised me to use the Cisco switches to achieve the best performance and quality of service of IP video; he also said he cannot guarantee the same services and benefits when embedded into other brands due to the underlying technology and capabilities of those brands.

4.3 Other Work

I have also conducted extensive research and described the other brands of switches such as Korenix, Enterasys Systems and DLink which can provide capabilities similar to MediaNet [8]. This information will not be included in this report as it is insignificant because CNZ mainly focused on getting to know more about Cisco's MediaNet.

Chapter 5

Problems Encountered and Solutions

This chapter describes the problems that I have encountered throughout the year. Mainly the problems are going to be categorized as Technical and Non-Technical.

5.1 Technical

1. Connection:

During my first look at establishing the point the point connection; as I was going thought the notes on how to set up a WDS link between the two bridges, I faced a number of minor problems. First, I misunderstood the entire concept of the experiment as it my first time doing this; I started using my home modem to establish a connection to these bridges. Weekly meeting at CNZ helped me understand the correct procedure. Second, my local area connection would not show up even though I setup everything correctly. I spend a lot of time at home trying to figure out this problem because all the cabling is connected correctly to both the bridges and the laptops. The reason why this happened is because the original MAC addresses on the devices are printed wrong; hence I configured both bridges with wrong MAC addresses. Later I reset both the devices and reconfigured them with different addresses. Lastly, my local area connection frequently keeps breaking down once the connection (signal) is established between the bridges. I realised that one of my laptops kept going back to default 'Obtain IP address automatically' under the TCP/IP setting instead of using the static IP address that I have assigned. So whenever this happened, I always assigned the address again.

Trouble shooting: Whenever the wireless link the broke down between the two devices, I have started from the physical layer of the OSI model and went upwards to tackle where the problem existed. For example, check the cabling first, then the MAC addresses of devices and move onto network layer to check IP configuration.

2. UPS:

The UPS stops or goes to idle mode suddenly. Therefore, the bridge halts, bringing the WDS link down. So I have to turn the UPS on again and to re-establish the signal between the two sites and this kept happening frequently so I halted the experiment many times and went back home to charge the UPS overnight but this did not solve the problem.

The UPS is jumping into idle mode (Stops) due to the insufficient level power draw when only the bridge is connected to it; as the bridge uses only 0.5watts of power. But when I connected both my nearly drained laptop and the bridge together, the UPS worked for a long time continuously before reaching its limit. I have used also used a 20Watt light bulb (energy saver) to make the UPS continuously working for longer period

3. Alignment:

I observed very poor signal strengths; around 24% most of the time (according to my blind tests). The amount of data rates achieved is way too low for commercial purposes. I finalised with CNZ to use lasers for accuracy. The laser light at the destination was too bright and I realised it is as big as a soccer ball while expected it to be as small as a normal laser point. The ray form the laser is easy to see for a short period of time but it consumed many AAA cells.

As, I was not aware that even a slight movement can cause such a big effect (as the bridges were held in hands) in laser accuracy, the throughput data rates in many trails stayed low. Then this made me realise the importance of motionless bridges; hence both are placed stationary, one as it shown in figure 9 and the other on the Mt. Wellington.

5.2 Non-Technical

1. Group Member:

The outdoor experiment, due to its complexity; as it involves one set of equipment stationed at Tamaki Campus and the other on top of Mt. Wellington. CNZ advised me to get some help from my friend who can assist me on one side while I work on the other site. I had to teach my friend the basic operation and the experimentation of these bridges from scratch as he was monitoring one bridge at Tamaki campus. This took a lot of time because he was confused and when something did not work such as local area connection going down; I had to call him from the other side (Mt. Wellington) to check what is happening as the signal cannot be detected. In worst cases, I actually had to pack up the equipment on

my side and drive back all the way to Tamaki campus to check what went wrong as he couldn't figure it out while on phone.

2. Time and Security:

As you can see from all the above problems; each experiment itself consumed a lot of time. Time is crucial; I only have a limited time on my side before the UPS ran out. So working fast is important but due to technical problems, sometimes it took way too long to fix and to accurately point the laser. Hence I had to come back another day after charging the UPS overnight again. It took a lot of time to visit many stores in search of an antenna; as they were far away from my place

Both personal as well as equipment security is important because I have conducted tests on when it's dark (to be able to see the laser) with expensive gear. Mt. Wellington is recently on many television programs due to gang related issues. This made me take extra precaution and I took my friends along when they had some time to spare; to look after equipment while I work on the experiment.

Another time issue is the access to Tamaki Campus. All the doors are closed at 6pm and because I do not have a swipe card, the power supply for my equipment is not available. I had to persuade the campus security by explaining all the details of the project in order to get access most of the time. The first two to three times is hard but then the security personnel quickly recognised me and granted me access for the rest of the experiments

3. Weather:

Weather played a big role as this experiment is based outdoors. The period I conducted the outdoor testing is around winter and worked up to spring. The weather on top of the mountain was so cold; even with all the winter protection, it was very difficult to experiment with numb hands and slippery equipment (dew). A lot of times, I have stopped the experiment and went back the next day to continue. On top of this, there are heavy rains this year around that period; this made it even difficult because I could not progress as I wished. So time was a big factor again.

5.3 Future Considerations

Throughout the report, I have provided my own conclusions on the approaches I took and why some worked but others resulted in poor results. But it very important to consider what my academic supervisor has said about my findings

According to him, the major reason why I did not achieve excellent signal strength in majority of my outdoor test is due to the 'noise' or 'interference' but not totally due to the accuracy issue as I have assumed.

- As I was holding onto to the bridges while experimenting, I would have added thermal noise to the devices. One or two degrees is fine but anything above that should be considered. Normal human hands are definitely warmer than two degrees, so this would have been one of the major causes. In order to reduce such type of noise, I have been advised to use a tripod instead of holding the bridges with bare hands.

- The bridge at Tamaki (refer to picture 9) is placed very low above the ground. The ground would also add noise to the device. To avoid such problems, bridge must be placed at decent level of height; maybe a pole mounting or upper levels of the building.

- Certainly, I am not the only person working with these 5GHz (shared band) devices around the entire area (Tamaki, Mt. Wellington, Point England, and Ellerslie). So obviously interference would be present. Therefore the device's random access methods (to access the medium) such as CSMA/CA (carrier sense multiple access with collision avoidance) would try to prevent the collision by not sending the data as it notices some other device transmitting and this may be the reason why I have observed high response rates.

- Another important design fault is the use of the tape to position the laser in place. Lasers are very accurate and even a few centimetres off in position would have an impact on the overall performance (signal strength degrades).

- Supervisor has recommended CNZ to use many bridges operating with less power which are placed relatively close to each instead of using fewer bridges by increasing the distance. This is to overcome the interference problems

Chapter 6

Achievements and Future Work

This chapter shows what I have learned from this project, the short comings/failures and the future work. A numerous number of achievements have been earned through the project.

6.1 Achievements

Project Goals

Most of the goals have been accomplished. I have tested and established maximum performance levels and limitations for both 200mW and 500mW wireless bridges (theme1). The results that I provided CNZ with and the recommendation for future implementations (horizontally placed 500mW bridges) appear to be valuable according to my company

supervisor – theme one. I also recommended a few solutions for CNZ's already existing implementations at Kaikohe. For theme2, I provided CNZ with the MediaNet capabilities so that it could help manage the traffic and ease network administrator's effort.

Work experience

It is my first time doing such a big project (year-long). I was involved in an employer-employee relationship with CNZ. This enabled me to take responsibility in my work and meet commercial objectives; where someone (for e.g. CNZ) depended on my results and work. In the future workforce as I will be involved in the similar type of environment with much higher expectations, this experience to start with was priceless.

Organisation, management skills

This project involved weekly meetings with CNZ supervisor, meeting deadlines, presentations, writing reports, maintaining BTech website and mainly trying to organise my documentation in neat and safe manner. This enables the reader to understand when exactly and how I have done my work. Multiple versions of my experimentation is backed up regularly to avoid any problems; so it is more than just experimentation involved.

Applied skills

Although some knowledge in data communications and networking was gained over the four years in university, it was the first time dealing with a range of commercial devices to examine and establish their performance levels. Hand's on experience, in terms of learning new concepts on my own of various types of technologies and software was an excellent experience.

Design/test creation

Over the undergraduate years, most of the learning is done via straight forward theory (example, studying TCP/IP) but never really got to see how it actually works practically. However the requirements for this project are given at business level and as I put more work into the project, the more problems (e.g. packet loss) I faced and hence this enabled me to change my methodologies or strategies accordingly. There was no straightforward answer due to the range of problems that I have to investigate myself. Most important is the failures, each time I failed to achieve a goal; I learned something new which I can avoid the next time I conduct the experiment.

Trouble shooting

As I conducted the experiments in various environments, I faced many problems throughout the project; both technical and non-technical. These problems helped me learn a precise or a wise way to solve them and it is not as simple as restarting the computer to see if the problem disappeared.

6.2 Project Deliverables

I have provided a written report and a BTech 451A presentation at the end of the first semester. The BTech 415A&B final report and the final seminar for the entire year is also

presented and additionally, I provided a complete documentation for configuration and technical support for future users; all my deliverables are available from my BTech website.

6.3 Short Comings

1. For model B, most of the stores only have Omni-directional or less powerful directional antennas. The models that I recommended CNZ were turned down due to them being Omni or less powerful. In order to get powerful antennas, International websites do have some models but I am not sure whether I can trust them or rely on those models at this stage. So this is where I have paused in order focus on my other objectives while I was waiting for emails from vendors and this goal took a lot of time.

2. As you can see from my experimentation results in chapter 3, the response times for 500mW horizontal tests for data sizes 100 to 600 kBytes have not been recorded (packet loss is not measured) and the horizontal tests for 200mW bridges have not been done because the UPS ran out on that day.

6.4 Future Work

The commercial project mentioned in chapter 3 is a huge task. Unfortunately, very little work has been done before it came to a halt. But future work on this project will help CNZ achieve their wireless WDS connection to all the neighbouring businesses so that each of the companies can communicate with CNZ in Albany region using these bridges as a source (picture shown in chapter 3.10). Detailed goals and objectives are unknown or obscured at this stage.

The short comings discussed in the above section can really help CNZ get an idea on how their implementation can look. I hoped to work on both models to see which model of 501-5D can outperform the other; but due to time constraints, I did not get a chance to physically see model B, so only model A (both 200mW and 500mW versions) are tested.

6.5 Conclusion

The project started of slowly and quickly gained pace as the year went along. I have successfully achieved many goals involved in both themes. The major accomplishment and happiness was when my company supervisor appreciated me for the outdoor testing and the approaches I took to provide them with results that are useful for commercial purposes.

This project has helped me to gain knowledge and understanding of work in a professional environment. This will be very useful for my career and future study because it thought me that, even small details matter in such projects. I have come across many problems which helped me learn new skills, both technical and non-technical and gave me confidence that enabled me to achieve beneficial results that are much needed by CNZ.

In conclusion, this report includes the background information under 'Appendix which describes the 802.11 standards, technologies, and legislations. This report can be used as a helpful reference/benchmark for future work or development.

Acknowledgements

To conclude, I would like to thank a number of people who have helped me throughout the project.

Many thanks to the BTech project co-ordinator Dr. S Manoharan for answering all my queries in a constructive way and for extending my BTech website deadline.

I would like to thank my academic mentor Dr. Ulrich Speidel for supporting me and providing me with valuable ideas, information and help throughout the year.

I would also like to my industrial mentor Edmond Chan and CNZ for sponsoring this project. He has been patient with me throughout the year as I was lost at times and could not meet some deadlines. He gave me suggestions and much needed help when I was stuck.

References

Compucon
[1] http://www.compucon.co.nz/

Computers New Zealand
[2] http://www.cnz.co.nz/

Wi-Borne Bridge
[3] http://www.wiborne.com/datasheet/CAP-5015D-brochure.pdf
[4] Outdoor wireless AP/Bridge/Router/CPE User guide, version 1.0.3 (pdf on BTech website)

Software
[5] http://www.ixchariot.com/products/datasheets/qcheck.html

NZ Laser Use
[6] http://www.nrl.moh.govt.nz/publications/is24.pdf

MediaNet
[7] http://www.cisco.com/en/US/netsol/ns1094/index.html
[8] http://www.korenix.com/jetnet-series-industrial-ethernet-switch.htm

Appendix
[9] http://en.wikipedia.org/wiki/IEEE_802.11#802.11a
[10] Behrouz A. Forouzan, Data communications and networking, fourth edition
[11] http://www.rsm.govt.nz/cms

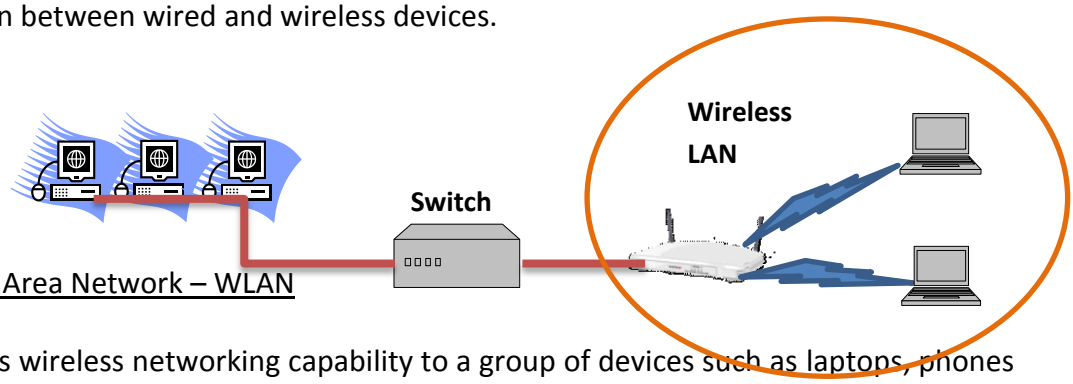
Appendix:

This section of the report contains background research useful for the understanding concepts and it is mainly for future readers and students

Networks and Wireless

Local Area Network (LAN):

Local area network is a simple computer network that connects computers and devices in a small geographical area such as school, home, university buildings or office. LAN can be as simple as two computers and a printer in some one's home or it can extend throughout the company or university building. Local area networks are limited to a few kilometres. LAN's are distinguished by their transmission media and topology. LAN is a wired network unless it's a wireless local area network (WLAN); wired LAN's are important to discuss because even though wireless local area network is present, at some point there will be an existing LAN infrastructure that the WLAN makes use off. In the picture below, a simple LAN with physical wiring is shown along with a WLAN where laptops are connected wirelessly to an access point but the access point is physical wired to an existing wired LAN for communication between wired and wireless devices.



Wireless Local Area Network – WLAN

WLAN provides wireless networking capability to a group of devices such as laptops, phones that support 802.11 (Wi-Fi - wireless). All the communication process is done without any physical wiring. WLAN is useful for providing each device with a connection through an access point to the internet. WLANs use radio frequencies to transmit and receive information. Wireless LANs are very popular these days because of the increase in laptops and due to its ease of installation. E.g. these days' shopping malls are offering free wireless access to their customers.

Standard 802.11:

802.11 is the first wireless LAN (WLAN) standard created by IEEE (Institute of Electrical and Electronics Engineers) which supports a network bandwidth of 2Mbps. But because most of the applications today need higher bandwidth for data transfer, wireless equipment of this standard are no longer manufactured.

Standard 802.11b:

IEEE expanded the original standard 802.11 to 802.11b. This standard supports bandwidth up to 11Mbps and uses the same unregulated radio signalling frequency of 2.4 GHz as the original 802.11 standard. Manufacturers prefer to use this frequency to reduce the production costs. Due to the signalling frequency being unregulated, 802.11b products can interfere with microwaves ovens, phones and other appliances when operating at the same 2.4 GHz frequency range. This interference problem can be solved easily by placing the 802.11b equipment away from the other appliances.

Standard 802.11a

This standard is normally found on business networks due to its high costs. 802.11a supports bandwidth up to 54Mbps and it signals at 5.7 GHz in a regulated frequency spectrum. The higher the frequency the range becomes shorter, the production costs increases and also the signals become weak. I.e. they cannot penetrate though the obstacles and walls as efficiently [9].

Standard 802.11g:
This standard is developed to combine the advantages of both 802.11a and 802.11b standards. 802.11g supports bandwidth up to 11Mpbs/54Mbps but operates at frequency 2.4 GHz. This standard is backward compatible with 802.11b which means 802.11g network access points (AP's) work with 802.11b wireless network adaptors and vice versa.

Standard 802.11n:

Is the latest IEEE standard in the Wi-Fi category which has not been finalised but IEEE approved the amendment and it is published in 2009; licensed only in the USA. This standard is meant to improve the network bandwidth by using multiple wireless signals and antennas- called MIMO technology. The data rates provided by this standard is over 100Mbps. 802.11n also provides bigger signalling range due to its increased signalling intensity. 802.11n equipment is backward compatible with the 802.11g equipment.

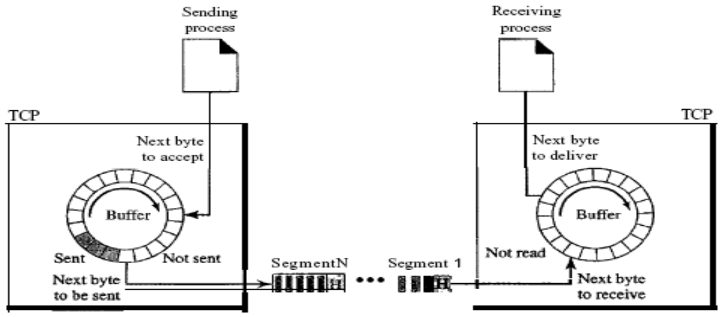
Standard	**Advantages**	**Disadvantage**
Standard 802.11	-------	No longer manufactured due to only 2Mbps data rate
Standard 802.11b	- Low cost - due to production costs being less - Up to 35 meters, range of signal is good	- Bandwidth is only up to 11Mbps – slow speed - Normal everyday appliances interfere with the 802.11b equipment when

		operating on unregulated signalling frequency
Standard 802.11a	- Regulated signalling frequency so the interference can be prevented from other appliances - Bandwidth of 54Mbps – fast speed for data transfer	- Higher costs due to big operation of frequency - Shorter signal range that can be obstructed easily by obstacles
Standard 802.11g	- Bandwidth of 54Mbps – fast speed for data transfer - 2.4 Ghz frequency operation so the range of signal is good and signals not easily obstructed by walls and other obstacles	- Prone to interference from appliances operating on 2.4 Ghz frequency signalling band - Costs more than 802.11b standard
Standard 802.11n	- Data rates more than 100Mbps – fastest speed - Can be enabled in the 5GHz or 2.4 Ghz so that interference can be avoided - Signal range up to 70 meters which is the best among the standards	- This standard is not finalized yet and costs more than standard 802.11g - - Use of multiple signals may interfere with 802.11b/g networks

The above standards are important in wireless implementations and it is essential to know the differences between each of the standard because the bridges that are used in this project support the standard 802.11n; which allows data rates up to 300Mbps

Transmission Control Protocol/Internet protocol (TCP/IP):

The internet layer contains Internet Protocol (IP) which is an important communication protocol used to transmit and receive datagram/packets across the internet using the internet protocol suite. Internet protocol suite (TCP/IP) is set of protocols used for internet that involves two main protocols called internet protocol (IP) and transmission control protocol (TCP). Internet protocol version 4 (IPv4) is an unreliable connectionless protocol that provides best effort delivery service. IPv4 provides no error or flow control and uses the datagram approach where datagram take different routers and may arrive in different order and also congestion or transmission errors cause lost packets. If senders send too fast, the routers or receivers cannot keep up therefore congestion of network. If reliability is important, then IPv4 must be paired with reliable protocol such as TCP. Transmission control protocol's job is to fix the problem that IP has. In the transport layer there are two protocols such as user datagram protocol (UDP) and TCP. User datagram protocol is a connectionless, unreliable transport protocol. UDP does not add any other services to IP but provides process to process communication instead of host to host communication and performs very little error checking. Even though UDP doesn't do much, it does have its advantage that it provides less overhead i.e. if a process wants to send a small message without any reliability then UDP can be used as transmitting takes much less interaction between the sender and receiver than TCP. TCP on the other hand is a connection-orientated, reliable protocol that provides flow control and proper retransmission after errors. TCP send data not as packet but as a stream of bytes and maintains buffers (sending and receiving buffers) for storage



The IP layer, as service provider for TCP needs to send the data in packets but not as in steam of bytes so the TCP groups a number a number of bytes into a packet called TCP segment. These buffer provide flow and error control. The buffer on the sender's end work as follow, the grey area (picture above) resembles that data that is sent but waiting for acknowledgement but the white area is the empty space where new data can be loaded into. On the receivers end the white space is used to load the receiving data so that the process can read it and once the data is read, the area is recycled so that new data can be loaded into.

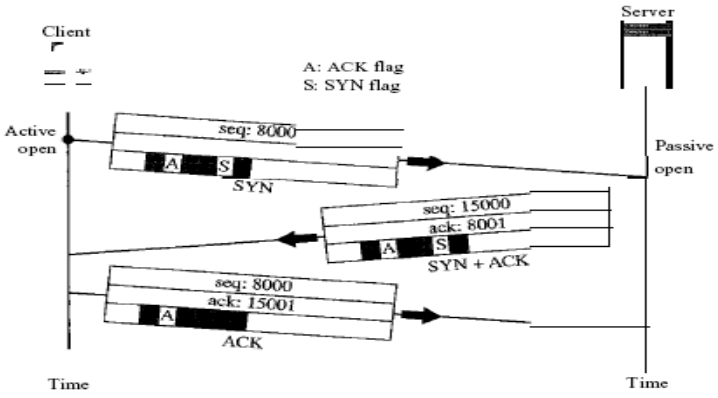
Flow control in TCP can be done by two approaches. One is Rate control where the sender determines the maximum safe sending rate of data and never exceeds it and the other is sliding window where the sender sends up to a 'window' full of data but then pauses for an acknowledgement. It is used to make the transmission more efficient as to control the flow

of data so that receiver does not get overwhelmed with data. The window size is adjusted according to the network capacity. TCP is a sliding window protocol [5].

Sliding window process:

TCP starts of slowly where the window size is small and starts sending packets until window is empty and the window size is increased as the data flow accelerates and window size is decreased if the data flow slows down and finally retransmits the data if the acknowledgement doesn't arrive [10].

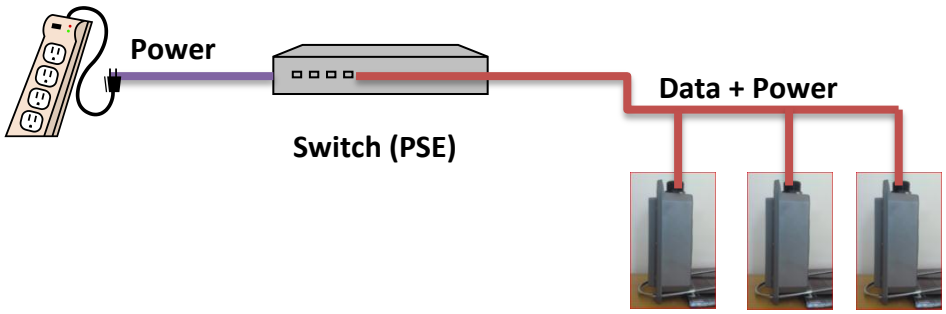
TCP transmits data in full duplex mode which means the data can be sent and received in both ways at the same time. In order to communicate, connection establishment must take place and it is called three way handshaking. A particular client program tells it's TCP that it wants to communicate with a certain server and then the 3-way hand shake begins [5]; it involves the establishment phase, data transfer phase and then then disconnection phase



Power over Ethernet (PoE)

For setting up a point to point wireless connection, this is the main technology used to power the equipment and how this technology works is shown below

Power over Ethernet is a technology where every day Ethernet cables are used to function as power cords. Power over Ethernet allows devices that require power – called 'powered devices', such as wireless access points, IP telephones and other portable wireless appliances receive power(direct current- DC) and also data over the Ethernet cables simultaneously without needing to upgrade the already existing infrastructure. This technology allows the installation of devices in places where the electric outlets are not within reach. Power sourcing equipment (PSE) such as a switch shown below provides power and also transmits data to the powered devices to the connected devices.



How PoE Works

Once the powered devices are connected to the port of some power sourcing equipment for e.g. a switch, the PSE will automatically determine whether the device connected to its port is a valid Powered Device or not. Then the PSE can supply up to 12.95 watts of power to the powered device along with the normal transmission of data.

The first step is the Powered device discovery - where the 802.3af standard for device detection applies direct current between sending and receiving wires and measuring the amount of current received. Once a PSE device approximately notices 25K ohm resistance and 150nF capacitance between the sending and receiving wire pairs, then the powered device is considered as valid

Once a Powered device is discovered to be valid, PD classification may be performed by the PSE by applying the direct current to the port. If the powered device supports 'optional power classification', then it applies a load on the wire to tell the PSE device the classification this device needs. Once the power class is determined by the PSE device the required power for PD is subtracted from the overall power budget (which is 12.4 watts per port). This allows proper management of power allocation in case a PSE device cannot supply maximum power to all its ports and this means a variety of PD devices can make use of the available power. Power classes according to the standard 802.3af are:

- class 0 = Power Usage 0.44 – 12.95 Watts
- class 1 = Power Usage 0.44 – 3.84 Watts
- class 2 = Power Usage 3.84 – 6.49 Watts
- class 3 = Power Usage 6.49 – 12.95 Watts

Note: Powered Devices that are unclassified are assumed to be of class 0

The 802.3af standard requires category 5 cables for higher power levels and category 3 cable for low power levels. Actually delivering the power through the cable depends on the cable being used. Category 5 Ethernet cable has four twisted pairs. Only two of them are used for data transfer and the power is supplied using two methods. One method allows us to use the two unused wires to supply power and the other is using the same data wires to supply power without destroying the data to be sent. According to 802.3af standard we cannot use both sets of wires in other words the PSE device can only power either spare wires or the data wires

Advantages of PoE

The wiring costs can be reduced because there is only a single cable running from the PSE device to the powered device that carries both power and data. This allows us to decrease the need for separate power installations in the building and connections needed for the powered devices. The installation and connection management is simple and a lot of space can be saved. The devices can be placed anywhere and is not limited to nearby power sources. Powered devices can be easily moved around if we know there is LAN cabling available. PoE is also very safe because all the powered devices are not connected to the main supply but instead to PSE's; so the voltages are lower

Antennas

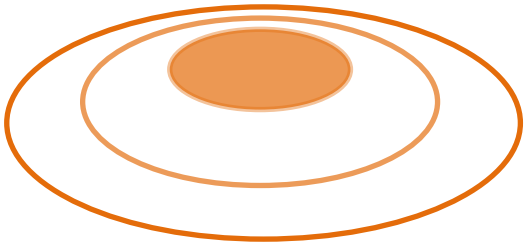
What is an antenna?

An antenna is a transducer which means it converts one type or energy into another. Antennas convert electromagnetic radiation into electric signals and vice versa. They transmit and receive radio waves and are essential for operating radio equipment such as radio, television, wireless LAN's and space communications.

Antenna Types

Omni-directional-

Omni means all or every. Omni-directional means that the antenna sends and receives data or information in all directions. Even though the coverage of this antenna is in 360 degrees, because of its dispersed nature, the signals are weak and the distance the signal can travel is short. For e.g. the routers and modems at home which are Omni-directional send signals in all directions so that multiple people in a room can access the internet but a person will fail to get connected when he moves a few meters away from that room proving that these antennas do not have a big range. These antennas are excellent for home users, small offices, parks and basically anywhere you need the coverage from central location. The best place to install these antennas is in open spaces, outdoors as the number of obstructions will limit the effectiveness of this antenna. They are used in devices that use radio waves such as mobile phones, Wi-Fi, global positioning system. The frequency range at which this antenna operates is around 800, 900, 1800 and 2.4GHz.



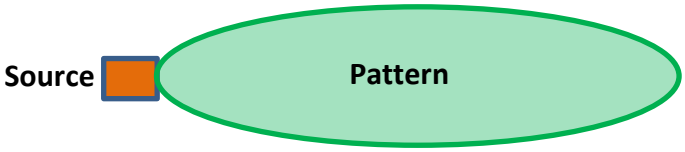
The picture (left) shows the Omni Direction radiation patter (in 360 degrees)

Yagi-

Yagi-Uda antenna or simply Yagi is a good choice for point to point or point to multipoint transmission of data where the destination antenna is close by or in a straight line. The antenna must be pointed to a specific direction one wants to send or receive data but when the direction of the antenna is wrong then its abilities are useless. Yagi antenna is a directional antenna which means the transmission and receiving can only be done in one direction hence the performance is increased, the signal strength and transmitting power is stronger and loss of signal is low. This directional antenna has the capability of reducing interference from other sources such as weather conditions, natural and manmade obstructions which means they can be used in places, areas where there is a lot of interference.

Flat-Panel -

Flat panel antenna is also a directional antenna. These antennas are rugged and completely weather proof that provide long life in harshest of environments. Flat panel antennas designed for high performance. The frequency range at which it operates is within 2400-2483 MHz and it take 100 watts as input power and yet perform reliably in temperatures around -40C to 70C. This antenna is used for both point to point and point to multipoint wireless communications and they are mainly used by the internet service providers due to the high costs of the antenna



Picture to the left shows the directional Radiation pattern - one direction only

Parabolic or Dish -

Parabolic antennas are also called dish antennas. These antennas give us the best range for the signal but they are very difficult to aim from source to destination. These antennas are used for very long distance where point to point communication devices are stationery or fixed. Parabolic antennas are used for satellite television, mobile telecommunication and radar.

Legislation

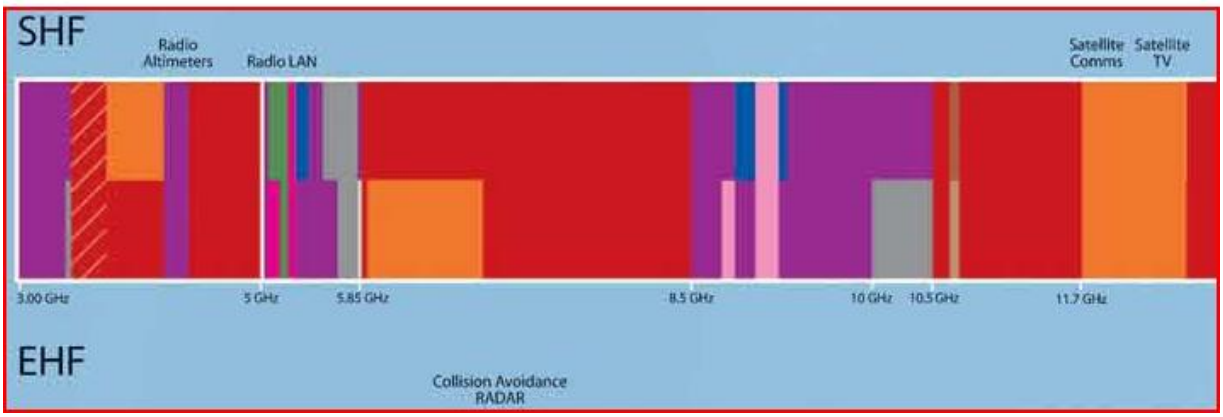
Let us now discuss about the legislation and the rules imposed by the government regarding the wireless communications, radio devices and the spectrum use.

What is Legislation?

A law that has been approved by a legislature or some other governing body is called legislation. Legislation has many purposes such as granting, to regulate, to declare or restrict, to authorize and to provide.

RSM Group and spectrum allocations, licenses

The below picture is the 'Radio Spectrum allocations in New Zealand'. Radio spectrum is a very important resource and it is managed by the Crown, through the ministry of economic development.



Reference [11]

Ministry of economic development is the key player responsible for providing the government with proper advice on the radio spectrum allocations to meet the client's demands; that are using the evolving technologies, services and products. Therefore, this ensures that the radio spectrum not only provides the economic benefits but also the social benefits to the New Zealand society. Now, the default channel used by 'CAP-501-5D' bridge is the 5 GHz band. It is necessary to find out whether this device can comply with the legislation or not and this is shown below.

License:

License Name:

- General User radio License for Short range devices

License Number:

- 227313

License:

5.15 - 5.25 GHz	200 mW peak eirp	any modulation	> indoor W-LAN only

Yes, it is free to use the 5 GHz band under the "General User radio License for Short range devices"; because the default channel for 501-5D falls under the 5.15-5.25GHz range. So the devices must be operated indoors only due the special conditions mentioned by rsm group.

Recommendation

Because these CAP 501-5D devices are high capable devices especially in point to point communication as we have learned in chapter 2 and 4, we could probably use a different frequency band such as 5.250 – 5.350GHz; under the 'general radio user license' as shown in the below picture so that we can use these devices in the wireless LAN environment without any restriction to a specific use such as – indoors only.

General user radio licence (GURL) provisions:

Frequency Range	Power	Modulation	Restrictions
2.4 - 2.4835 GHz	1 watt peak eirp	any modulation	
2.4 - 2.4835 GHz	4 watt peak eirp	frequency hopping or digital modulation only	
5.15 - 5.25 GHz	200 mW peak eirp	any modulation	> indoor W-LAN only
5.25 - 5.35 GHz	200 mW peak	any modulation	> W-LAN only
5.725 - 5.875 GHz	1 watt peak eirp	any modulation	
5.725 - 5.875 GHz	4 watt peak	frequency hopping or digital modulation only	
5.725 - 5.825 GHz (refer to Note 1)	200 watt peak eirp with a max 1 watt peak transmitter power	digital modulation only	> Fixed Radio Link Devices (FRL only > Peak power spectral density must not exceed 17dBM/MHz.