BTECH 451A

END OF SEMESTER PROJECT REPORT

Arun Manohar Vejendla

Department of Computer Science

University of Auckland

UPI: avej002

ID: 4866880

avej002@aucklanduni.ac.nz

JUNE 2011

Contents:

Abstract

In telecommunications, wireless communication may be used to transfer information over short distances (a few meters as in television remote control) or long distances (thousands or millions of kilometres for radio communications). The term is often shortened to "wireless". It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking.

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a, b, g, n; Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi hot spots have been popular over the past few years. Some businesses charge customers a monthly fee for service, while others have begun offering it for free in an effort to increase the sales of their goods [2].

This project is mainly about learning the wireless technologies and standards that are present in the current world so that it could help me gain understanding on the overall themes of the project. The first theme includes analysis and testing of wireless bridges and the second theme involves video surveillance systems. I have to help the company called Computers New Zealand (CNZ) by performing experiments and fulfilling their objectives so that they can make use of the outcomes which in turn can help them improve their already existing implementations

This report is a summary of the project work done during the first semester, and it will be used as a reference for future goals during next semester. The first chapter of this report introduces this project, which includes the company and describes the themes and goals for this project. The second chapter informs in detail about the LAN and wireless LAN technologies that are important to understand for the experimentation. The third chapter shows how communication take place. Chapter four introduces the bridges that are provided by CNZ and their capabilities. Chapter seven shows the legislation details and how extensively we can use the bridges. Chapter eight shows the hands on experimentation including the configuration details. Finally, the rest of the report provides information regarding the additional testing methods, the short comings, future goals for next semester and summaries.

Chapter 1: Project Overview:

Two organisations are involved in this project. The science faculty that offers the BTECH Project and the company that I will be doing the project for. This chapter introduces the information of the project which is sponsored by the company for BTECH students during the final year of degree.

Company Background:

The project is sponsored by the company Computers New Zealand Limited (CNZ). CNZ is a total information system and solutions provider with skills and capabilities to implement information and automation systems for meeting clients' business objectives and increasing their productivity and competitiveness. CNZ expertise is focussed on 2 inter-related solutions for business customers:

(a) Information Systems

(b) Video Surveillance Systems

CNZ is a registered Solution Integrator of Compucon New Zealand. 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 [1].

Project Themes:

There are two themes to this project.

1. Testing wireless bridges and access points (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 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 bridge (1 version) and wireless access points (up to 3 versions) in the workshop and real life environments, and to state the maximum performance and limitations of all versions.

2. Investigation of the impact of video on data transmission on a local area network to establish some performance specifications. 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 guidelines to system administrators on how the video traffic should be managed. Cisco MediaNet has special and proprietary firmware for managing video in data networks. I am expected to learn about MediaNet and recommend if CNZ can use standard network switches to achieve the same purposes.

Project Schedule:

The picture below shows the schedule for both first and second semester and the objectives that I have to accomplish each session.

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

For the first two sessions, I have been advised by my company supervisor to conduct research on the existing wireless technologies, protocols, various types of antennas and the power over Ethernet technologies and the bridge CAP501-5D. These will be explained further in the report. From session three onwards, the project involved the first look at the hardware devices provided by CNZ and to establish a simple point to point connection. Once I finished the configuration and setup, CNZ advised me to move onto the actual testing and provide them with some analysis and values.

What I have gained from this project?

- **Hands on experience:**

  - Industrial: hardware's and software's

- Academic: research and technologies

- **Experimenting:**

  - Wireless technologies (various configurations, modes to enable wireless networking e.g. PoE, antennas). E.g. applying theory in practice

- **Perform real life data communication analysis and documentation**

  - Testing, validation and promoting through CNZ

- **Gain consultancy, design and implementation skills**

  - Testing in various environments helps me choose products wisely in real life scenarios and working with this company gives broad real time knowledge

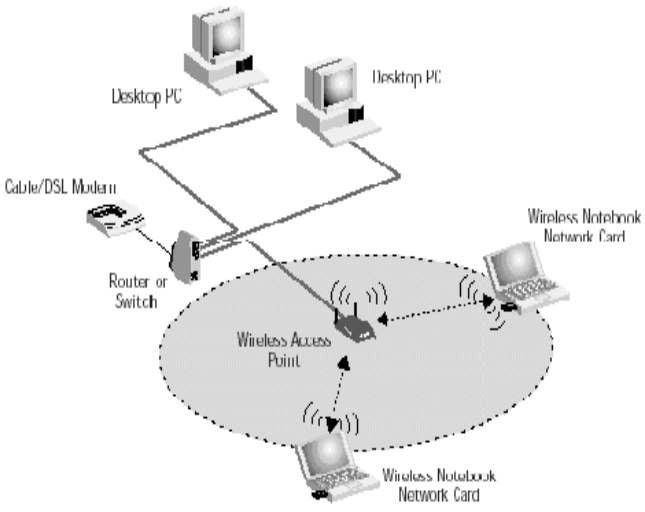
- **Trouble shooting:** due to the real world problems I may come across

Chapter 2: Networks and Wireless

This chapter provides the information about the local area network and the wireless local area network technologies and standards. It is important to discuss this because; this project is based on the wireless communication, testing and analysis.

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's are usually privately owned [3]. 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 from other network types 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 to the right, 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

Wireless LAN provides networking capability to a group of wireless devices in a close proximity to each other such as in office building, schools, universities and home. 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. certain shopping malls and businesses are offering free wireless access to their customers. There are many standards associated to wireless local area networks and they are explained below [4].

Standard 802.11:

IEEE (Institute of Electrical and Electronics Engineers) has defined the specifications for a wireless LAN. 802.11 is the first wireless LAN (WLAN) standard created by IEEE which supports a network bandwidth of 2Mbps. But because most of the applications that 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 was created at the same time as 802.11b. 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

Note: Because 802.11b and 802.11a operate at different frequencies, the two standards are incompatible with each other. In other words, the hybrid standard 802.11a/b equipment can be used to implement both standards side by side but each connected product must use one or the other standard but not the same standard

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	- Prone to interference from appliances operating on 2.4

	- 2.4 Ghz frequency operation so the range of signal is good and signals not easily obstructed by walls and other obstacles	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

Chapter 3: What is a Protocol?

Network protocols are a set of rules that allow devices to communicate successfully. Protocols provide the format and structure of the message, the process by which the networking devices share information, setting up and termination of data transfer sessions. Many diverse types of devices can communicate using the same set of protocol. This is because protocols specify network functionality, not the underlying technology to support this functionality. For e.g. there are two parties, one speaks mandarin and the other speaks Spanish. The communication will most likely fail unless they both agree on a single language

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

This is the TCP/IP model – internet protocol suite:-

Application: represents data to the user

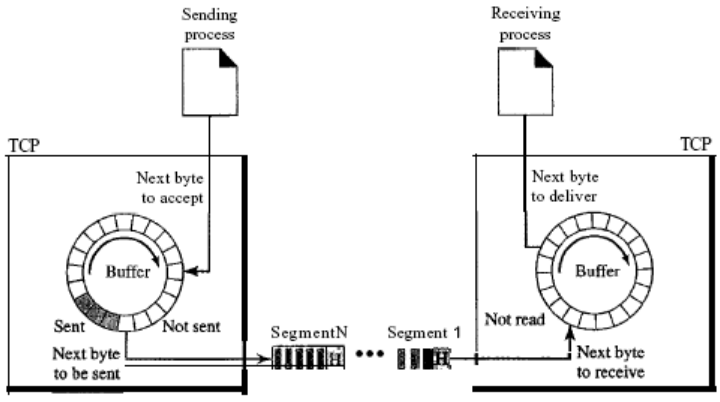
Transport: supports communication between diverse devices across diverse networks

Internet: determines the best path though the network

Network Access: controls the hardware devices and media that make up the network

Delivery of packets or datagrams can be accomplished using a connection-orientated or connectionless network service. In a 'connection-orientated service', the source station must first make a connection with the destination device before sending any packets. Once the connection between the devices is established, the sender sends the packets in a sequence one after other. There is relationship between packets. All the packets are sent on the same path in a sequential order. Each packet is logically connected to the packet travelling before it and after it and once all the packets are delivered, then the connection is terminated. In this case, the route from source to destination is only done once and the switches that receive the packets do not recalculate the path for the packets. In connectionless service, network layer protocol treats each packet independently and the packets may be sent along the same path or different paths to the destination even though they belong to one message. This is called a datagram approach and the internet is follows this connectionless approach. In such networks, packets may arrive in different order

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



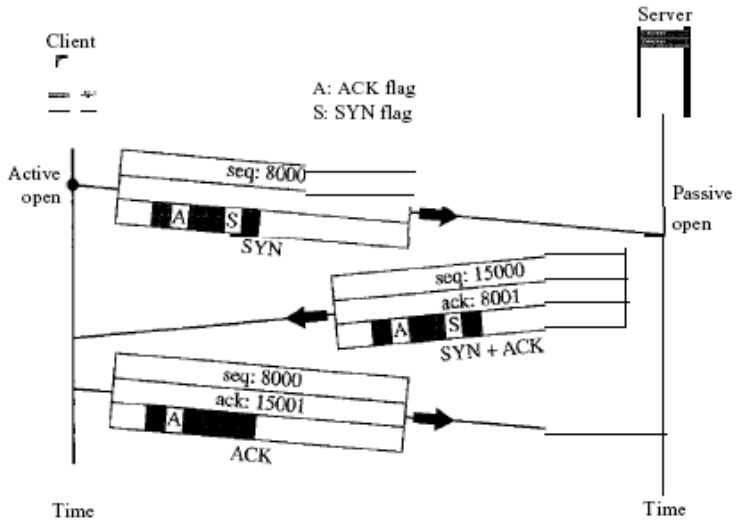
The IP layer, as service provider for TCP needs to send the data in packets but not as in steam of bytes so the TCP groups a number a number of bytes into a packet called TCP segment. These buffer provide flow and error control. The buffer on the sender's end work as follow, the grey area (picture above) 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

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



First the client sends a SYN segment to synchronize the sequence numbers so that communication can take place. Then the server sends SYN+ACK, where SYN tells the client that the server wants to communicate and the ACK is the acknowledgement of the clients SYN segment. Finally the client send back ACK segment acknowledging the second segment

sent by the server. After the SYN+ACK, the two ends know the initial sequence numbers and initial window sizes. Now both ends may start sending data as long as they are within the allowed sending window. In the disconnection phase the client sends a FIN segment to the server letting the server know that communication must end and then the server's TCP informs its process regarding this and send back a FIN+ACK segment informing the client about the acknowledgment and the message that it is closing connection as well and finally client send back ACK to acknowledge the servers message.

Chapter 4: Bridge CAP 501-5D

CNZ has provided me with equipment such as bridges, Power over Ethernet devices and physical cabling so that I can establish a point to point connection to start off with and test the wireless communication in terms of throughput, response times using software

NIC limitation

NOTE: The CAP 501-5D bridges used for this project 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.

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 of high power. 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 [6].

Applications of Wireless network

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 [6].

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.

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

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:

WDS mode is also called the repeater mode. Wireless distribution system is a system that provides the wireless interconnection of access points in the network that is using the standard IEEE 802.11. In this case, the AP 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, point to multipoint and multi-point as shown in the diagram below.

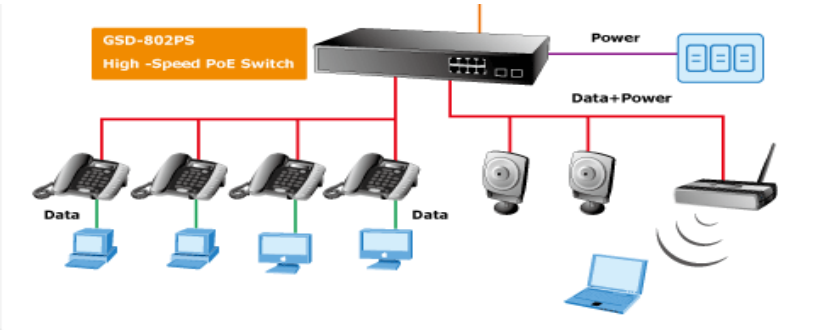
According to the specifications and objectives provided by my company supervisor, WDS is the mode that has been used for the testing so far in this project because it allows a connection between two bridges; hence communication between two ends (laptops)

Chapter 5: Power over Ethernet

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 – PoE

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

Chapter 6: Antennas

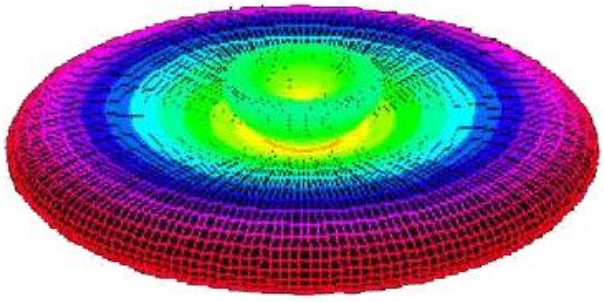
What is an antenna?

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-

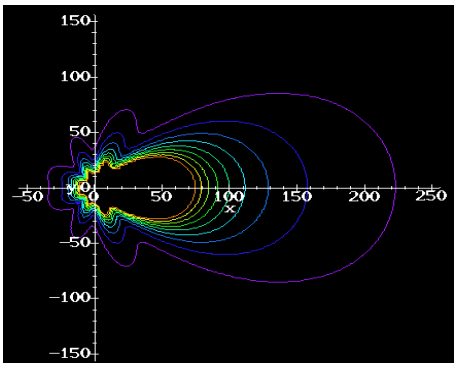
Omni means all or every. Omni-directional means that the antenna sends and receives data or information in all directions. These antennas are oriented vertically and are used for called non directional antennas as they radiate equally in all horizontal directions - horizontal plane but not in a particular direction. 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. As the gain of the antenna increases, the elevation becomes flatter but at the same time the range increases i.e. suppose you place a donut on a flat surface and squish it, the thickness of donut decreases but at the same time the donut becomes flatter in horizontal direction (as shown in below picture) which means the range increase and this same principle is used in these antennas as well. The frequency range at which this antenna operates is around 800, 900, 1800 and 2.4GHz.



Reference: http://wirelessantennahelp.com/omni_directional.htm

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 (shown in the picture: bottom right) 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. The power of the antenna and the frequency it receives and transmits data depends on the arrangement of the length and spacing of parts. These antennas are used for medium ranges such as 3-5miles and are operated at a frequency of 800MHz to 1900MHz



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

Parabolic or Dish -

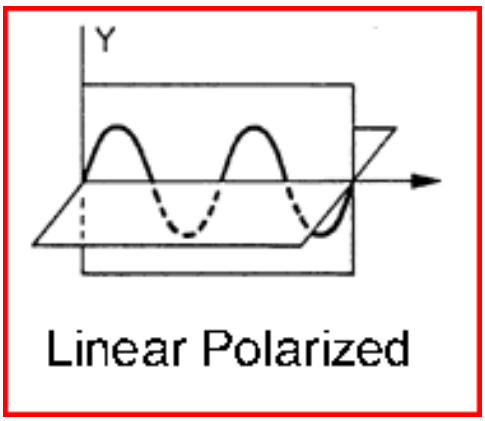
Parabolic antennas are also called dish antennas. These antennas give us the best range for the signal but they are very difficult to aim from source to destination. These antennas are used for very long distance where point to point communication devices are stationery or fixed. Parabolic antennas are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

Antenna Polarization

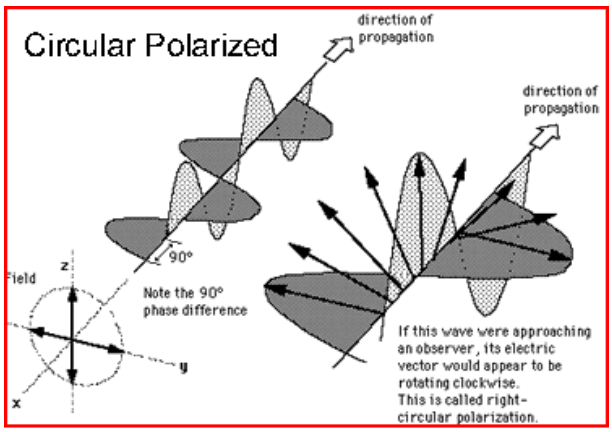
Polarization of antenna can be defined as the orientation of electric field of radio wave with respect to the earth's surface. Most devices use the horizontal, vertical or circular polarization. Polarization is determined by the physical structure of the antenna and by its orientation. An antenna will have one polarization when it is vertically mounted and a different polarization when it is horizontally mounted. Linear polarization (vertical and horizontal polarization) is mostly used in radio communications. Vertical polarization is

mostly used in mobile communications because vertically polarized antennas have an Omni directional radiation pattern (360deg radiation pattern); in other words the antenna do not have to be re-orientated (change position). Linear polarized antennas radiates in one plane containing the direction of the propagation whereas a circular polarized antenna, the plane rotates in a circle. The below picture show the planes of the two polarizations:

Linear Polarization:



Circular Polarization:



Effects:

It is important to consider the antenna polarization when installing antennas. Each antenna should be properly aligned to achieve the best signal strength between two stations. In linearly polarized systems, misalignment of 45degree in polarization will degrade the signal by at least 3dB and a misalignment of 90degrees in polarization will attenuate the signal by at least 20dB. Vertical polarization is generally used to radiate signals over short to medium ranges but Horizontal polarization is used for long distances in order to reduce the interference from the other vertically polarized systems generating signals

Long Range Wi-Fi

Since the development of Wi-Fi standards and how rapidly each of the standard evolved; one of the key issue is to provide long range Wi-Fi communications for both organizations and also residential users. Now to see why we require long range communication:

Business uses:

- Coverage can be provided to a large office, business or a campus.
- Establish point-to-point link between large skyscrapers or between two destinations.
- To provide Internet to remote construction sites, research labs or rural areas

As an example, we will consider the business case in CNZ where many point to point connections that involve many devices. As the amount of devices increase, so does the costs and equipment needed to drive that system. So in order to decrease many point to point connections but still provide communication from the initial end to the final end which is the same distance, we need long range Wi-Fi between each device in the path between the initial and final devices.

So, one way of increasing this range is by using the power amplifiers; also known as 'range extender amplifiers'. These amplifiers are normally small and usually supply half a watt of power to the antenna and these amplifiers may increase the range of existing network by more than 5times; so every 6dB gain doubles the range.

Higher gain antennas or specially designed directional antenna and adaptors can be used to increase the range without a significant increase in the transmission power. A popular approach, such as USB WLAN hardware is placed at the focal point of parabolic cooking utensil such as a round bottomed scoop – called WokFi technique (Wi-Fi antenna made out of Asian cookware scoops). This technique helps yield gains between 12-15dB; which is enough for line of sight that ranges several kilometres.

As USB leads do not invite the losses generally associated with costly microwave coax, extending the USB adapter closer to a window or away from shielding metal objects and foliage, may dramatically improve the link. The above diagram shows a Wi-Fi amplifier supplying 1 watt of power to the antenna.

EIRP (equally isotropically radiated power)

Is also called the effective isotropically radiated power and this tells us the amount of power radiated by an isotropic antenna (which equally radiates power in all directions) to produce a peak density observed in the direction of antenna gain [8]. The EIRP and the power is stated in dBm (decibels in milliwatts) or dBW (decibels in watts); cable loss is stated in dB (decibels) and the gain of the antenna is stated in dBi (referenced to isotropic antenna)

EIRP calculation:

1) Determine the numbers for the transmitter output power, antenna gain and the line loss (normally stated on the device brochure)
2) Use the formula and substitute values:
3) **EIRP Formula: Tx Output power + antenna gain – line loss**
4) **EIRP Formula: Power (in watts) x 10^(dBi/10) – when line loss not considered**

Example of CAP 501-5D EIRP calculation 1:

1) Radio: 200mW = 0.2 (200/1000)Watts
2) Antenna: 15dBi

EIRP = Power (in watts) x 10^ (dBi/10)

= 0.2 watts x 10^ (15dBi/10)

= 6.325 Watts (we can use the formula dBw = 10log10 (Power/1mW) or dBm = 10log10 (Power/1mW) + 30 to get the dBm and DBw value of EIRP); therefore it is 8.01dBw

Example of CAP 501-5D EIRP calculation 2:

1) Radio: 200mW = 0.2 (200/1000)Watts
2) External flat panel Antenna: 23dBi

EIRP = Power (in watts) x 10^ (dBi/10)

= 0.2 watts x 10^ (23dBi/10)

= 39.90 Watts

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.

Schedule

Frequency Range:	5725 MHz to 5825 MHz
Emission Characteristics:	Digital modulation
Peak Transmitter Power	1 watt (0 dBW)
Peak Power Spectral Density:	<17 dBm in any 1 MHz bandwidth
Peak Radiated Power:	200 Watts (23 dBW) e.i.r.p.

The above picture shows the legal limits. Under the frequency band 5.725 to 5.825 the peak radiated power should be 200watts (23dBW). This shows that the above calculations on the different antennas do fall in the limits imposed.

Chapter 7: Legislation

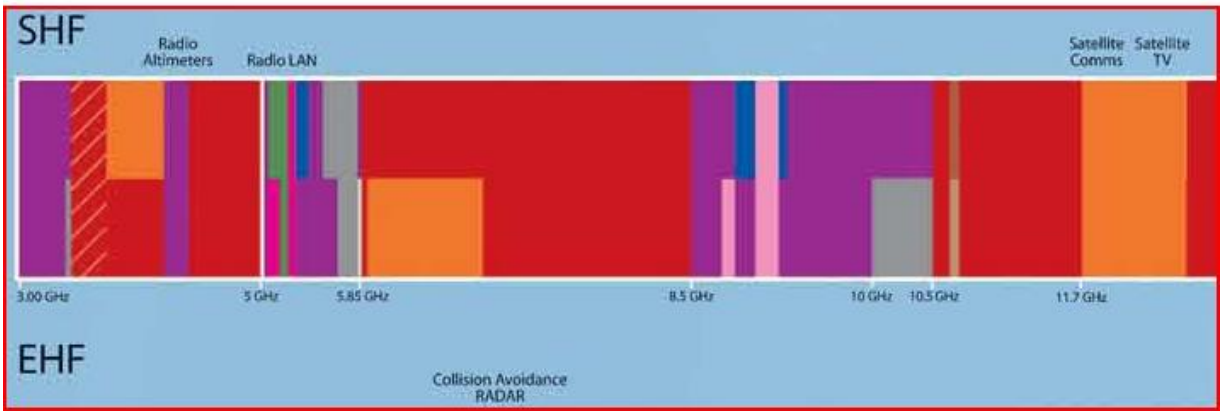
Let us now discuss about the legislation and the rules imposed by the government regarding the wireless communications, radio devices and the spectrum use.

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. Efficient and responsible use of this spectrum is important to consider because it provides safety of life, satellite navigation, telecommunications, broadcasting, land mobile and a lot of other services that is essential for the New Zealand economy in order to function well [7].



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 5.22 GHz band. It is necessary to find out whether this device can comply with the legislation or not and this is shown below.

License [7]:

License Name:

- General User radio License for Short range devices

License Number:

- 227313

License:

- People may transmit radio waves using Short Range Devices (SRDs), also known as Restricted Radiation Devices (RRDs), Low Interference Potential Devices (LIPDs), or Spread Spectrum Devices (SSDs) but must follow the terms, restrictions and conditions as stated below [1].

Low (MHz)	High (MHz)	Reference Frequency (MHz)	Maximum Power dBW e.i.r.p.	Remarks
5150.000000	5250.000000	5200.000000	-7.0	Special Conditions 8 and 16
5250.000000	5350.000000	5300.000000	0.0	Special Conditions 9 and 17
5470.000000	5725.000000	5597.500000	0.0	Special Conditions 9 and 18
5470.000000	5725.000000	5597.500000	-10.0	Special Condition 7
5725.000000	5875.000000	5800.000000	6.0	Special Condition 13
5725.000000	5875.000000	5800.000000	3.0	Special Condition 10

Special Conditions [1]:

7) Use is limited to radio location

8) The use is limited to wireless LAN indoors systems only

9) Use is limited to wireless LAN

10) Use is limited to road transport and traffic telematics

16) In the band 5150 to 5250 MHz, the maximum permitted power density is 10 dBm/MHz (10 mW/MHz) e.i.r.p. OR equivalently –36 dBW/25 kHz (0.25 mW/25 kHz) e.i.r.p.

17) Indoor-Only Systems: In the band 5250 to 5350 MHz, the maximum permitted mean power is –7 dBW (200 mW) e.i.r.p. and the maximum permitted mean power density is –20 dBW/MHz (10 mW/MHz) e.i.r.p., provided Dynamic Frequency Selection and Transmitter Power Control are implemented. If Transmitter Power Control is not used, then the e.i.r.p. values must be reduced by 3 dB

Indoor and Outdoor Systems: In the band 5250 to 5350 MHz, the maximum permitted mean power is 0 dBW (1 W) e.i.r.p. and the maximum permitted mean power density is –13 dBW/MHz (50 mW/MHz), provided Dynamic Frequency Selection and Transmitter Power Control are implemented in conjunction with the following vertical radiation angle mask where q is the angle above the local horizontal plane (of the Earth):

Maximum permitted mean power density	Elevation angle above horizontal
–13 dB(W/MHz)	for 0° ≤q <8°
–13 – 0.716(q – 8) dB(W/MHz)	for 8° ≤q <40°
–35.9 – 1.22(q – 40) dB(W/MHz)	for 40° ≤q ≤45°
–42 dB(W/MHz)	for 45° <q;

18) In the band 5470 to 5725 MHz, the maximum permitted transmitter power is –6 dBW (250 mW) with a maximum permitted mean power of 0 dBW (1 W) e.i.r.p. and a maximum permitted mean power density of –13 dBW/MHz (50 mW/MHz), provided Dynamic Frequency Selection and Transmitter Power Control are implemented. If Transmitter Power Control is not in use, then the maximum permitted mean power shall be reduced by 3 dB.

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

Frequency Range	International Region 3 Allocation	New Zealand Allocation	Summary of Usage	References and Policies
5030-5150MHz	AERONAUTICAL RADIONAVIGATION 5.367 5.444 5.444A	RADIOLOCATION RADIONAVIGATION	Radiolocation, Radionavigation - possible future use for microwave landing system (Microwave Landing System)	
5150-5250MHz	AERONAUTICAL RADIONAVIGATION FIXED- SATELLITE (Earth- to- space) 5.447A MOBILE except aeronautical mobile 5.446A 5.446B 5.446 5.447B 5.447C	AERONAUTICAL RADIONAVIGATION MOBILE except aeronautical mobile	5150- 5350MHz Short Range Device usage, RLAN in particularUsage of 5150- 5250MHz restricted to indoor wireless LANs.	General User Radio Licence for Short Range Device POLDOC Other Services 002: Protection of Mobile Satellite Services Uplinks in the Band 5150- 5350MHz
5250-5255MHz	EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION SPACE RESEARCH 5.447D MOBILE except aeronautical mobile 5.446A 5.447F 5.448A			
5255-5350MHz	EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION SPACE RESEARCH (active) MOBILE except aeronautical mobile 5.446A 5.447F 5.448A	MOBILE except aeronautical mobile	Wireless LAN	

According to the above information, yes it is free to use the 5.22GHz 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. But the devices must be operated indoors only due the special conditions and restrictions mentioned above.

According to the RSM website, reference: http://www.rsm.govt.nz/cms/policy-and-planning/policy-documents-operational/other-services/other-services-002 [7]; this policy states that the 'NO wireless LAN devices must be granted approval' for use in the band 5.150-5.250 and this is because the ITU has designated the use of this band for the non-geosynchronous satellite feeder links in the mobile satellite services (MSS). But the RRD's (restricted range devices) used in this band will be reviewed once ITU has recommended technical parameters for the sharing of MSS links with the RDD devices. But the band 5.250 – 5.350GHz will be available still for the use of wireless LAN services under the general radio user license. So, following the 'General user radio license' special conditions is very important to avoid interference between the MSS up-links and RDD devices.

Recommendation

Because these CAP 501-5D devices are high capable devices especially in point to point communication as we have learned in previous discussions, 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; but following the special conditions (9) and (17) mentioned on top.

Limits imposed by RSM on the power level

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.

The above picture (focussing on the information under the green rectangle) shows the maximum power imposed by the RSM group under the general user radio license.

Chapter 8: Point to Point connection

Equipment used:

- 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)

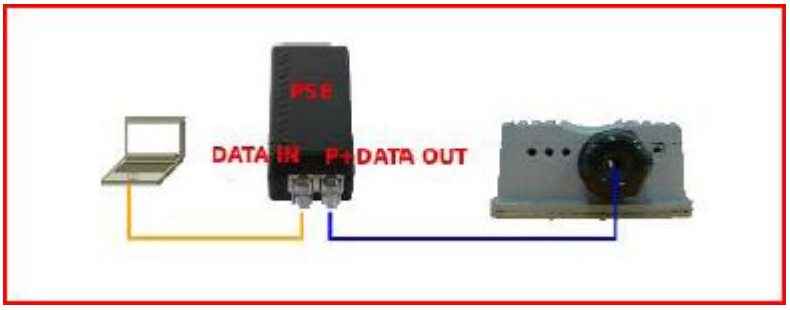
Regarding the equipment, the two bridges are used so that it is possible for one computer or laptop to communicate with the other laptop; because we are concerned about a point to point connection at this stage. The cat5 cables are capable of transporting

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 (details under Power over Ethernet chapter). 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. The power cables on the other hand are used to connect the PSE devices to the main power outlet. Finally, the laptops I have used are with 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.

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:



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 and everything else is the same as shown above.

First Experiment Results

Before we talk about the results, the IP addresses and MAC addresses used for this experiment are shown below

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

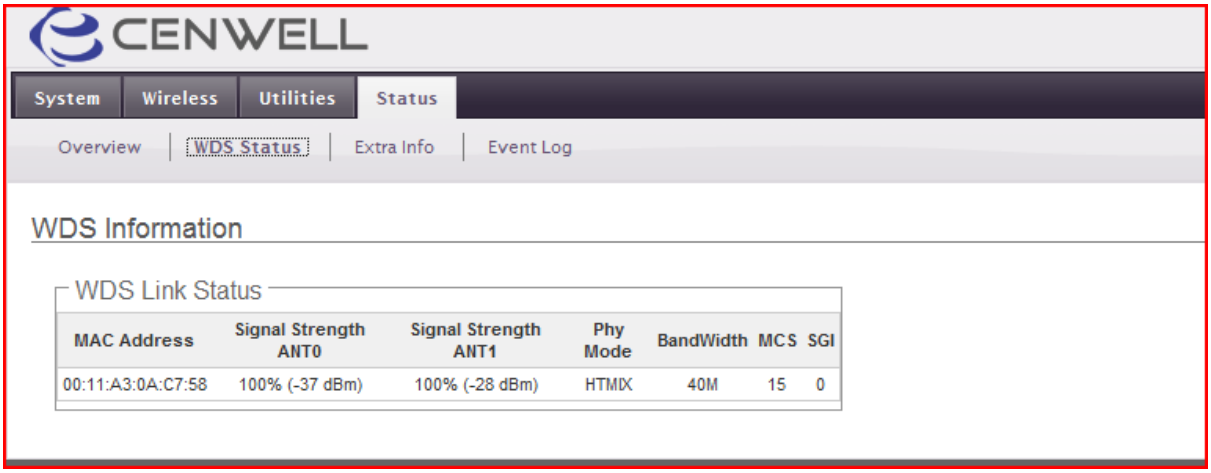
Laptop 2:

- IP address: 192.168.2.100 – network adaptor
- Subnet mask: 255.255.255.0

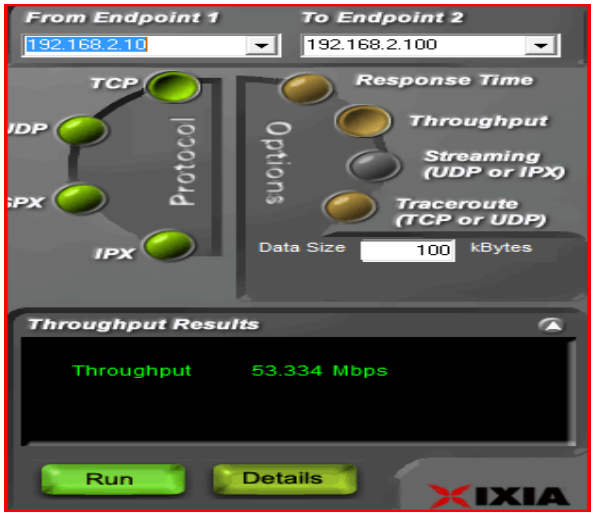
Remote access point (attached to laptop two):

- 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.



There are many software's that are available such as Qcheck, IPerf and DU meter to measure the communication performance; but in this experiment, Qcheck has used to analyse the throughput over a range of data sizes. For example, the throughput measured for a 100kBytes of data is 53.334Mbps as shown on the Qcheck picture to the right.

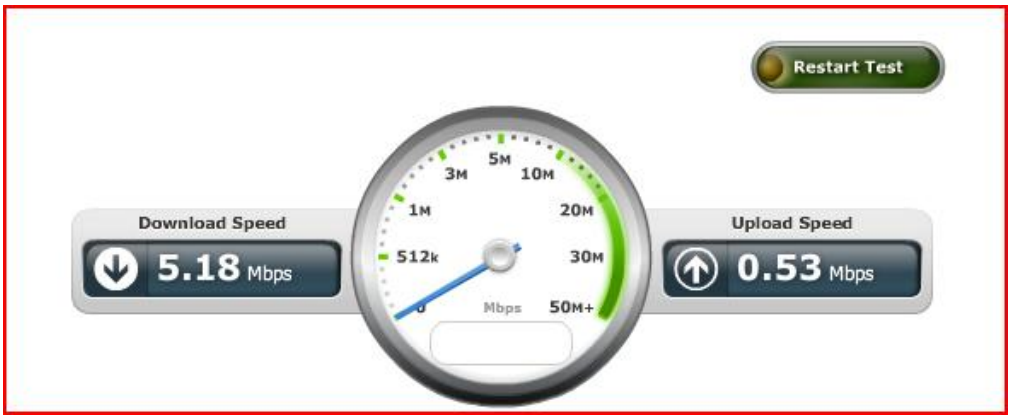


Now we present a range of values measured:

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

By using Qcheck we are only limited to a maximum data size of 1000kbytes, so experimenting using real data sizes such as sending a large file from one laptop to another would be a real advantage because, it shows the real time throughput of the

communication process. But looking at the above measurements, the data rates are quite high. This can be shown using the telecom broadband speed as an example at my home:



The above picture shows a real time throughput and when compared to the measured data, it is way lower. This is because; when the bridge experiment was conducted both of the bridges are in a small room, i.e. very close together but whereas in this real time test of the telecom network, my laptop and the service provider are apart – quite a large distance; therefore the data rate is much lower. So this experimentation is more valuable if it can be done outdoors over large distances because, the separation of two bridges in distance, increases the chances of obtaining real time data measurement.

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. This test has been conducted to check whether increasing the power levels 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

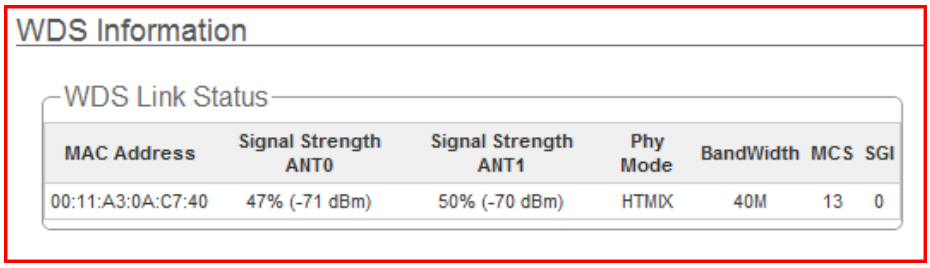
Increased Signal strength with TX value (25%):

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%):

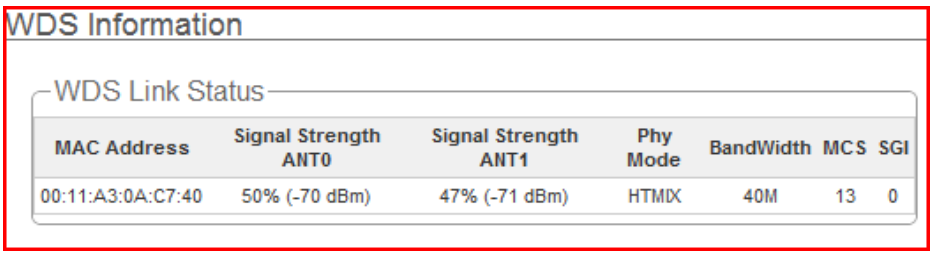


WDS Information

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%):

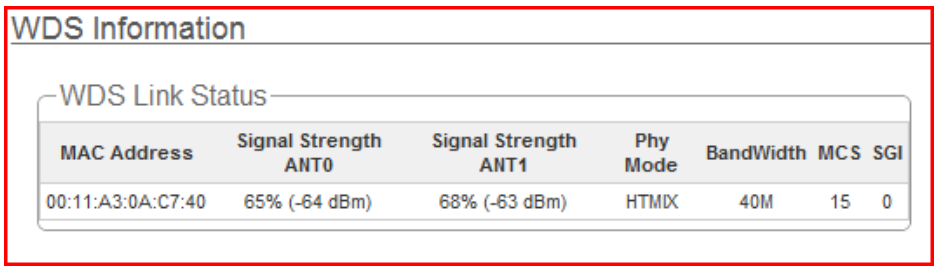


WDS Information

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 (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.

Chapter 9: Other Discoveries

This chapter informs about the experiments that are not included in this report and the shortcomings in this project so far

Various Tests:

First of all, it is important to go back to the first theme of the project. Mr.Edmond, my project supervisor has told me that, the bridges used in this experiment are capable of achieving data rates up to 300Mbps according to the Wi-Borne CAP501-5D brochure and also the wireless standard 802.11n. This is where I have conducted a lot of testing and analysis in various modes and configurations to achieve the 300Mbps data rate; but I failed to achieve these data rates and reported my actions and evaluation.

Further analysis on the hardware itself such as finding out radio type, network interface card and the cables showed me that the network interface card (NIC) within the bridge is only capable of fast Ethernet; where the maximum data rates reach 100Mbps. This is the reason why the data rates in my experiments are nowhere near 300Mbps but close to the 100Mbps mark. This reason is proved and is correct by contacting my supervisor regarding this matter.

I have conducted a lot of other tests and experiments focusing on various situations. The details are not included in this report. This is because the average report is around 30 pages; in other words, to avoid having too many pages but the types of tests are going to be briefed below.

After my initial test, once I got familiar with the configuration and setting up the devices. I have been advised by CNZ's manager to conduct indoor polarization tests. These tests involve the change in movement and angle of the bridges and measuring their efficiency. This is important in real world implementations because it is not always possible to accurately place the bridges that match perfectly especially when long distances are considered. The test is done when the two bridges are facing completely opposite to each other; this gave me the least amount of signal between the devices and hence the bandwidth is the lowest. The other tests involved measuring data rates (throughput) and response times when two bridges are completely facing each other; when one bridge is horizontal while the other is vertical; when both bridges are horizontal but facing different direction; when both bridges are horizontal but face the same direction; real world mock tests in rain when the angles are perfectly matched and also with angle changes; and finally the power tests to help CNZ improve their kaikohe project.

Short Comings

One of the objectives according to my supervisor and also the first theme of this project is for me to perform outdoor testing where the distance between the devices (both bridges) are at least 2kilometers. This is not yet accomplished due to two reasons; one is because CNZ implemented CAP501-5D bridges in kaikohe in a line of sight method (bridges in straight line facing each other). So, in order to conduct this experiment; a place where I can test over large distances where the bridges can be in line of sight is hard to find unless you go really far from city. The second problem is the UPS availability. This device acts like a generator to power the laptops and bridges while outdoors. The CNZ's manager has advised my company supervisor to put this operation on hold because they can only supply me with one UPS at this stage (one side can be powered but not the other) and don't want to waste money in buying a second UPS. So alternative approaches are being brainstormed

Chapter 10: Conclusion

This chapter summarises the entire report, and the project objectives that has been accomplished so far. Also, there will be some descriptions of the future goals for this project, which should be achieved during the next semester.

The first few sessions involved intense research about the technologies such as LAN, power over Ethernet that are involved in wireless communications and the limits and power levels imposed by the government. This information was very useful to understand the underlying complexity while performing the experiment practically by myself. I have gained knowledge of both software and hardware components required for data communications and analysis. This greatly helped me gain understanding which I did not have at the beginning of the semester. Also, since I have understood the concepts at the start of the project from the research and have some real time experimentation experience in configuring and establishing point to point connections, I have the confidence to apply these concepts and techniques in real life situations. This project has helped me to gain knowledge and some experience so far, which will be very useful in future.

Future Work

As we have talked about the short comings so far in this project regarding the outdoor testing. This is still under discussion with my company supervisor because alternatives are being thought about. It will be useful to implement or run these experiments on a large scale to gain more knowledge regarding the real time complexity. There is major change in direction for the next semester. I have to take hands approach with video surveillance systems and investigate the already existing solutions within the company and come up with good advice for the network administrators on how to manage the video on the traffic on the network

References

1. http://www.cnz.co.nz/
2. http://en.wikipedia.org/wiki/Wireless
3. http://en.wikipedia.org/wiki/Local_area_network
4. http://www.ieee.org/index.html
5. Behrouz A. Forouzan
   Data communications and networking, fourth edition
6. CAP5015D
   Outdoor wireless AP/Bridge/Router /CPE User guide, version 1.0.3
7. RSM
   http://www.rsm.govt.nz/cms
   http://www.rsm.govt.nz/cms/policy-and-planning/policy-documents operational/other-services/other-services-002
8. http://en.wikipedia.org/wiki/Equivalent_isotropically_radiated_power