E-Mail Forensics:
Tracing and Mapping Digital Evidence from IP Address

WAN CHUNG CARY HO
Bachelor of Electrical & Electronic Engineering (University of Auckland)
Master of Engineering Studies (University of Auckland)

a thesis submitted to the graduate faculty of design and creative technologies
AUT University
in partial fulfilment of the
requirements for the degree of
master of forensic information technology

Master of Forensic Information Technology

Auckland, New Zealand
2010

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

....

Signature

Acknowledgements

This thesis was completed at the Master of Forensic Information Technology lab of the AUT University in the New Zealand. While conducting this research project I received support from many people in one way or another. Without this support this thesis would not have been completed in its present form. It is my pleasure to take this opportunity to thank all of you. I would like to apologise to those I do not mention by name here; however, I highly value your kind support.

First, I would like to deeply thank my supervisor, Dr. Brian Cusack. Dr. Cusack provided me with careful and thoughtful guidance from choosing the thesis topic to the structure of the thesis. Despite his busy schedule, Dr. Cusack still gave some of his valuable time every week to monitor the progress of the thesis. Without his suggestions and encouragement, this thesis would never have been completed.

I would also like to acknowledge the friendship and support given to me by Tom Laurenson who provided me with a Macintosh computer during the testing phase of the research, James Liang who provided me with great help in searching for the literature review articles and the encouragement from all other MFIT students.

I want to thank my father, Che Biu Ho, my mother, Shirley Ho, my brother, Alan Ho and my girlfriend Jenny Chu for their continuous encouragement, support and care during the period of my study.

Abstract

Email communication is one of the major activities on the Internet. Because of its popularity and importance in people's lives, many criminal activities such as email bombing and phishing are also related to email communication. No matter how much evidence is collected about the crime, if the suspect is not caught, the evidence becomes useless. Hence email traceback plays an important role in email forensics.

Email header traceback is the most commonly used method for tracing back the source of email attacks. The source IP address in the email header is frequently used in email forensics to trace back the attacking location. Due to the effectiveness of the traceback method, most of the email forensic software only focuses on the power of mass email analysis and deleted email recovery. However, to prevent being traced back, an attacker likes to hide the true location by spoofing the source IP address in the email. Then email header traceback becomes less effective.

The purpose of the thesis is to search for a suitable traceback method for use in email forensics when the source IP address is spoofed. There are four main categories of IP traceback mechanisms: link testing hop by hop tracing, messaging, logging and marking. These IP traceback mechanisms are designed to trace back Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks when the source IP address is spoofed. However, most of these IP traceback mechanisms involve complicated design and are difficult to implement in email forensic environments. Moreover, the trade-off between resource consumption and traceback speed often limits the usage of these IP traceback mechanisms.

To provide a simple and fast traceback method in email forensics, the hop count distance method is proposed in the thesis. This method has a simple architecture with only three operation blocks: the packet signature identification, default hop count estimation & validation and the hop count distance calculation block. Since the hop count distance method depends only on the Time-To-Live field of the packet to calculate the hop count distance, it is totally independent of the source IP address. Also, from capturing the attacking packet to calculating the hop count distance between the source and destination, the traceback process takes less than a minute.

To ensure that the accuracy of the hop count distance method is not affected by its simplicity, the individual components of the method must be tested carefully. Therefore, the objective of the research is to work out the accuracy of the hop count distance method. A

testing network is set up and 8 hypotheses are tested to find out the accuracy of the hop count distance method.

Table of Contents

Chapter – 1 Introduction

Chapter – 2 Literature Review

Chapter – 3 Research Methodology

Chapter – 4 Review of Findings

Chapter – 5 Discussions

Chapter – 6 Conclusions

Appendix

List of Tables

List of Figures

List of Formulas

List of Abbreviations

CPU	Central Processor Unit
DGA	Data Generation Agent
DNS	Domain Name Service
DoS	Denial of Service
DDoS	Distributed Denial of Service
HCR	Hop Count Radius
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Provider
PPM	Probabilistic Packet Marking
RAM	Radom Access Memory
SPIE	Source Path Isolation Engine
SCAR	SPIE Collection And Reduction Agent
SMTP	Simple Mail Transfer Protocol
STM	SPIE Traceback Manager
TLT	Transform Lookup Table
TTL	Time-To-Live
URL	Universal Resource Locator

Chapter One

INTRODUCTION

1.0 BACKGROUND

Email plays an important role in most people's lives and it has become the main communication method among business entities. Personal information, business plans or proposals and other sensitive information may be all sent by email. When valuable information is sent by email and most of the email communication is vulnerable to different attacks, email becomes as easy and valuable target for the criminals.

To protect people from email attacks, different securities mechanisms have developed such as tunnelling and encryption. These securities mechanisms provide enough security for private email communication that is between two or more people who know each other. But most of the email communications on the Internet involves people that they may not know each other and the public email communication still suffers from varies attacks such as email bombing and phishing.

When email becomes a target for digital attacks or is used as a tool to commit crime, there will be digital evidence associated with the email. Email forensics has been developed to search for the digital evidence associated with email. This digital evidence can be used to identify or even trace back the attacker for the email attack. When the attacker launches an email attack from any country through the Internet, the question of where the attacker is located is raised.

Because the Internet is vast and that is linked and managed by different networks in different countries, the first thing to track down the attacker is to narrow down the searching scope for the investigation. The proposed "hop count distance" method in the thesis is designed to use the Time-To-Live (TTL) field in the IP packet in order to filter the possible locations where the attacks launched.

In order to further narrow down the location of the attacker, the traceback evidence associated with the attacking source such as the evidence associated with the attacking tools and collected by the monitoring equipment will be discussed.

Section 1.1 describes the problem that the thesis topic attempts to solve. Section 1.2 describes the purpose of the thesis and how the problem can be solved in the thesis. Section 1.3 stated the restrictions of the experiment in the thesis.

1.1 PROBLEM

Since email communication is so widely used, people have their own email accounts as well as email accounts related to their work. Hundreds or thousands of emails are stored in the individual or company's mailboxes. Therefore, most of the email forensic software such as *encase*, *x-ways forensics* or *Intella* are designed to search for digital evidence in millions of emails. In addition to email analysis, deleted email recovery is also built into the email forensics software.

By using the email forensics software, digital evidence such as email message or email address related to criminal activity can be recovered. However, when the investigator wants to search for the physical location of the possible suspect, most of the email forensics software does not provide the functionality to trace back the source of the email. The investigator has to depend on other email traceback software to discover the source where the email was sent from. Most of the email traceback software relies on the source Internet Protocol (IP) address in the email header to trace back the source. If the source IP address was spoofed, the email traceback software would not be able to trace back the source of email.

There are other IP traceback mechanisms designed to trace back the Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks when the source IP address was spoofed. These IP traceback mechanisms such as iTrace or Probabilistic Packet Marking (PPM) are very efficient in tracing back the source of attacks in different environment. However, they are too complicated and resource-hungry to implement in an email forensics environment.

Therefore, hop count distance method is proposed in this thesis to provide a simple and fast traceback method when the source IP address has been spoofed. The hop count distance method depends on the hop count value inside the TTL field in the IP packet to determine the approximate location of the email source. By capturing only a single IP packet, the hop count distance from the source to the destination can be worked out within a minute. With the appropriate Internet topology around the victim of the attack, the approximate location of the email source can be estimated within a day.

Although the hop count distance method cannot pinpoint the exact location of the source, it can provide valuable information to help the investigator to narrow down the searching scope and hence accelerate the traceback process. The application of the hop count distance method is not limited to email forensics. With further research, it may also be applied to tracing back DoS or DDoS attacks.

1.2 PURPOSE

The first step in tracing back the source of an attack is to understand how the attack was launched. Different types of email attacks are reviewed in chapter 2 to show the intention, the aim and the way these attacks are launched. A simple commonly used email header traceback method is described to show how these email attacks can be traced back. Since the email header traceback method depends on the real source IP address, an attacking source with spoofed source IP address cannot be traced back.

There are four categories of IP traceback mechanisms namely: link testing hop by hop tracing, messaging, logging and marking, they are all designed to trace back DoS or DDoS in the Internet. These IP traceback mechanisms are effective to trace back the source that used spoofed source IP address under DoS or DDoS attack. However, most of these IP traceback mechanisms involve complicated network design and consume a lot of resources during traceback. There is always a trade-off when designing the IP traceback mechanism. If more resources are spent on the capturing network, there will be less time for path reconstruction. On the other hand, if fewer resources are spent on the capturing network, then more packets need to be collected for analysis at the victim side and hence the path reconstruction process is slowed down.

To fill in the gap between resource-intensive IP traceback mechanisms and the real source IP address-dependent email header traceback, the hop count distance method is proposed. The hop count distance method has a simple structure involving only three operation blocks: the packet signature identification, default hop count estimation and validation and the hop count distance calculation. The hop count distance method depends on the packet's TTL value to estimate the default hop count value being assigned by the operating system and to work out the hop count distance between the source and victim. A single packet needs to be captured in the hop count distance method and then the hop count distance can be calculated within a minute and the searching scope of investigation can be narrowed down to a day. Because the hop count distance method does not depend on the source IP address, it can be used to trace back the source when its IP address has been spoofed.

Accuracy is the heart of all methods and the research objective of this study is to work out the hop count distance method accuracy. Chapter 3 reviews the methodologies from five publications closely related to the hop count distance method. The testing framework on the hop count distance method is then constructed to be used for collecting data needed for testing the accuracy of the method. It was designed to collect data from nineteen Internet cafes with hop count value ranges from 3 to 10 and the distance ranges from 250m to 189km.

Chapter 4 shows all the data collected over a month by the testing framework from nineteen Internet cafes in Auckland city area. The data was analysed and presented in different format for discussion in chapter 5.

Chapter 5 demonstrates the achievement of the research objective. The research objective is to work out the accuracy of the hop count distance method and the accuracy was affected by two components or uncertainties: the default hop count estimation and the Internet hop count stability. These two uncertainties were affected by eight factors and eight hypotheses were established to test the factors

The efficiency of the hop count distance method was then examined and it depends on the Hop Count Radius (HCR), (i.e. the hop count distance between the source and the victim), and the hop count distribution in the area where the hop count distance method is applied. An example was used to demonstrate how the hop count distance method efficiency varies when different size of HCR applied on the area with the same hop count distribution. Chapter 5 also show how the hop count distribution is closely matched to the population distribution in New Zealand. Hence by studying the population distribution of an area, the hop count distribution can be determined.

Other traceback related evidence associated with the attacking source such as the physical location, the operating hour of the Internet café, the attacking tools availability and the monitoring equipment can provide additional help in tracing back the suspect. Once the hop count distance method can narrow down the searching scope to one week and with the help of the surveillance camera record at the attacking source, there will have a high probability that the possible suspect of the attack can be identified.

1.3 RESTRICTIONS

On the Internet, when email clients wants to communicate with each other, the email sender will first connect to the Domain Name Service (DNS) server and check for the Mail eXchanger (MX) record in the DNS server to obtain the location of the email server that can forward the email to the email receiver. Then the email sender will forward the email to the email server.

However, in the testing framework, the email client was configured with email server address and hence can forward the email directly to the email server without connecting to the DNS server. Because the experimental data aim to collect in the thesis is focus on the TTL value of the captured email packet, the differences between experimental and real email communication should be small enough to ignore.

Another restriction on testing of the hop count distance method is the testing scope and duration of the Internet hop count stability. Because the Internet hop count stability was tested for only a month in New Zealand. The Internet hop count stability result may be limited to a relative short period of time and can only be applied in New Zealand.

Chapter Two

LITERATURE REVIEW

2.0 INTRODUCTION

The Internet provides a platform for people to communicate. In this platform, millions of online transactions are performed every day. According to the report released by "Mediamark Research, "70.5% of U.S. adults Internet users used e-mail, 30.7% of them paid bills online, 22.4% of them played games online and 34.2% of them made a purchase through Internet for personal use"" (as cited in Burns, 2006).

At the same time Internet also has a dark side involving online fraud, e-mail spamming and hacking. Due to the anonymous nature of the Internet, it is extremely hard for the investigator to capture the offender.

> The 2008 Annual Report states that complaints of online crime hit a record high in 2008. IC3 received a total of 275,284 complaints, a 33.1% increase over the previous year…non-delivery of merchandise and/or payment ranked number one (32.9%). Internet auction fraud was the second most reported offense (25.5%) followed by credit/debit card fraud (9.0%) (Internet Crime Complaint Center [IC3], 2009, p.1).

The first step to trace the Internet hackers in the real world is to retrieve the source Internet Protocol (IP) address of the received packet. If the source IP address is a real public IP assigned by an Internet Service Provider (ISP), then the next step is to check which ISP the source IP address belongs to. Afterwards, the investigator can start to trace back the hackers in the real world based on the location of the corresponding ISP.

However, the hacker's intent is to hide their origin by spoofing their source IP addresses. To trace back these hackers, different IP traceback mechanisms were developed and "most of them fall into four main categories: link testing-hop-by-hop tracing, messaging, logging and packet marking" (Karthik, Arunachalam, & Ravichandran, 2008).

These traceback mechanisms were developed for various network environments and have their distinct features for tracing back the hackers. Most of them depend on collecting large number of packets from the routers along the attacking path. Without collecting sufficient packets, tracing back the hackers is extremely hard and sometimes impossible. These mechanisms are reviewed in section 2.2.

Section 2.1 reviews different types of email attacks and how to trace back email from its header. Also, various email forensic software such as *Intella* and *Nuix Forensic Desktop* are reviewed. Section 2.3 summarises all the issues and problems in email traceback followed by a conclusion in section 2.4.

2.1 EMAIL FORENSICS

The large and complex email communication system is connected to many businesses worldwide. Business transactions involves billions of profit are made every day in the Internet. And hence email communication systems have become a target for electronic crime. Many different tools and methods have been developed to carry out criminal attacks on emails. Therefore, email forensics has been developed to recover from attacks and to search for attacks evidence in emails.

In addition to the passive investigation for evidence, email forensics can also trace back the attack to the source of origin in order to allow the investigator to get close or even to pinpoint the location of the suspect in the real world.

2.1.1 Background

In order to understand how to trace back the source of attacks, different types of email attacks are reviewed, as well as the different aspects of an attack such as: the intention, duration, attacking path of the attack and how an attack is launched.

2.1.2 Different Types of Email Attacks

Email bombing, malware attachment, email spoofing and phishing are the most common types of attacks associated with email communication systems. Different kinds of attacks pose different threats on the email system, network bandwidth and/or to the end users.

These attacks can be launched alone or combined with others to form a more powerful and untraceable attacks. The results from these attacks can be as minimal as disturbing a user's normal email usage or as major as affecting the operation of millions of computers worldwide.

2.1.2.1 Email Bombing

The intention of email bombing is to deny the mail service from the end users. Email is used as a tool to attack the email system itself, particularly the user's mailbox.

Huge amounts of junk emails with size range between several hundred kilo bytes and couple of million bytes are sent to particular mail boxes intending to fill them up and stop the end users from receiving their normal emails. With the tremendous amount of emails being sent to the email communication system, the system may crash and affect some other email recipients too. The network bandwidth may also be occupied by the useless junk emails thus reducing the network efficiency.

> Email bombing is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site…the messages will be large…in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact (CERN, 2002a, p.1).

2.1.2.2 Malicious Software (Malware) Attachment

Most often malware attachments will not attack the email communication system directly, they would only start their operations if activated by the end users. Depending on what has been attached (virus, Trojan, worm or spyware), the effect can be as light as disturbing users by spyware or can be as serious as a Trojan which can then be used to launch a further attack on the whole network including the email communication system. The motivation of the attack also ranges from revenge to gaining business advantages.

> Email social engineering attacks usually involve prompting the user to open an attachment or follow an unsolicited link. When the file or link is opened, the system becomes directly infected with malware or is subjected to exploits attempting to install malware (Lanelli & Hackworth, 2005, p.5).

2.1.2.3 Phishing

The main purpose of phishing is to get sensitive information such as username, password and/or credit card information from the end users. It starts by sending email to the victim and pretending as the trust entity (friends or relatives) of the victim. Then after gaining the trust from the victim, the attacker usually directs the victim to a fake web site and asks them to input their sensitive information in order to steal it.

Because phishing has to deliver a fake message to misdirect the end users, it wouldn't cause any harm on the email and end user's email system. In most cases, phishing by email will be combined with email spoofing in order to gain the victim's trust and hide the true identity of the attacker from the victim.

> Phishing was identified as the use of electronic mail messages, designed to look like messages from a trusted agent, such as a bank, auction site, or online commerce site. These messages usually implore the user to take some form of action, such as validating their account information…included in the message is a URL for the victim to use, which then directs the user to a site to enter their personal information (Milletary, 2005, p.2).

2.1.2.4 Email Spoofing

Email spoofing as its name implies is sending email to the receiver with a fake sender's identity. Other email attacks are often launched with email spoofing to hide the hacker's identity and to gain trust from the end users. Since they would trust the hackers, the end users may be misled by the hackers and incur lost of sensitive information and/or even money. The attack has little effect on the network bandwidth usage and normal email activities.

Most often the FROM field within the email header is spoofed with the trust entity of the receivers. Some viruses will even search the victim's address book and send emails to the victim's friends on behalf of them.

> A user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (CERN, 2002b, p.1).

2.1.3 Email Traceback

From the above sections, it appears that email is an easy medium to use for Internet attacks. It is easy for the hackers to hide their identity from being traced by the investigators because of the anonymous nature of the Internet.

However, email communication leaves a unique footprint in the email system and it is possible to trace back the hackers when the format of the email header is analysed. Email header traceback for two forms of email communication, namely POP/IMAP mail and web mail, will be discussed in the following sections.

2.1.3.1 POP/IMAP Mail

With POP/IMAP email communication, Simple Mail Transfer Protocol (SMTP) protocol is used. The following example illustrates how email traceback is performed.

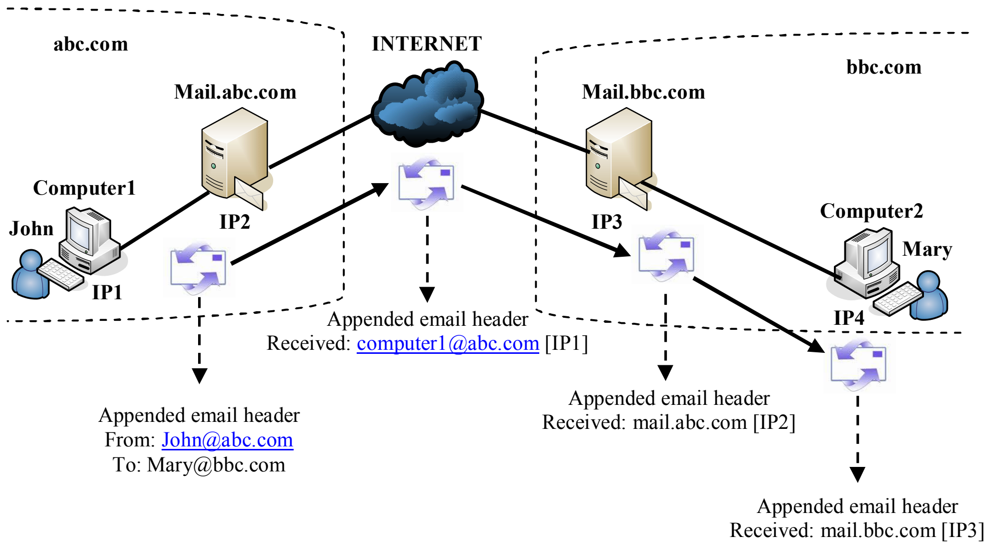


Figure 2.1: POP/IMAP Email Header Appendage

As shown in figure 2.1 when John uses a computer named Computer1 with IP address IP1 in a domain abc.com to send an email to Mary with computer named Computer2 with IP address IP4 in a domain bbc.com, the email will first be sent to the email server named mail.abc.com with IP address IP2.

The email client on Computer1 will generate and append to the email header “From:John@abc.com(Sender),To: Mary@bbc.com...”. Once the email server mail.abc.com receives the email, it will generate and append to the email header

"Received: from computer1@abc.com (computer1@abc.com [IP1]) by mail.abc.com…".

After the email is forwarded to the email server mail.bbc.com with IP address IP3, mail.bbc.com will generate and append to the email header "Received: from mail.abc.com (mail.abc.com [IP2]) by mail.bbc.com…".

When Mary retrieves the email from mail.bbc.com, Computer2 will generate and append "Received: from mail.bbc.com [IP3] by Computer2 (computer2@bbc.com)..." to the email header. By inspecting the recipient email's header, the path of the email that travelled from John to Mary can be traced back.

Although email header traceback works in most situations, it has its own limitations. First of all, the sender's computer name and its corresponding IP address can be tampered by the sender to hide the true identity; in other words, the sender's name and IP address can be spoofed.

Moreover, the sender can use an email server anywhere on the Internet to send email hence the email server being used for sending email may have no correlation with the email sender. Therefore, the email header traceback can only trace up to the email server that the sender used to send the email. Although many ISPs restrict their email server usage only to their own clients with proper authentication, there are still plenty of email servers freely available anywhere in the Internet.

> These professional bulk mailers use other mail servers as a relay point for their mail…If an e-mail server is not configured to disallow relay mail, a spammer (a person who sends unsolicited bulk e-mail) can send his or her batch of mail to a SMTP server not on his or her ISP's network and then out to the intended targets. The relay server is a dumping-off point that looks like a legitimate host, with the original source almost completely hidden (Schultz, 2000, p.65).

2.1.3.2 Web Mail

Web mail is another form of email communication. Emails can now be sent through the web interface instead of being handled by traditional email client applications such as Microsoft Outlook and Outlook Express.

When web mail is used, the actual email is not created on the sender's computer. Instead the email-related data is sent through the web browser to the web server and the email is created on the email server linked with the web server. An example illustrating how web mail works in Microsoft Exchange Server environment is described below:

> Outlook Web Access is a Messaging Application Programming Interface (MAPI) application that … use Collaboration Data Objects (CDO) to access mailbox and public folder information stored on a Microsoft Exchange Server computer. Outlook Web Access also uses Microsoft Active Server Pages technology on the Web server…to generate HTML pages…The Microsoft Exchange Server receives and processes requests from Outlook Web Access that resemble requests from any MAPI client (Microsoft, 2004, p.5).

Web mail makes the traceback much harder than POP/IMAP email. Email senders can freely register with any web service providers on the Internet such as hotmail, gmail and/or yahoo mail without providing their true identities and locations. Hence email header traceback can only trace back to the email server administered by the web service provider.

Sometimes, the sender's computer IP address can be discovered from the web server and email server's logs, but the IP address can still be spoofed so web mail also suffers from the same problems as POP/IMAP mail.

2.1.4 Email Forensics Software

Most of the email forensics software such as *Encase*, *X-ways Forensics*, *Final Forensics*, *Paraben Email Examiner*, *Intella*, *Nuix Forensics Desktop* and *Forensic Toolkit (FTK)* come with very powerful features such as analysis, filtering, indexing and keyword searching for various kinds of mailboxes including Outlook, Outlook Express or Foxmail.

Some of them can recover deleted emails from the mailbox. Instead of tracing back to the origin of the email, they are mainly designed to search for forensic evidence among millions of emails.

Other software in the market that performs email traceback works by reading the email header's information and therefore has the same limitations related to the email header traceback.

2.2 IP TRACEBACK

Along with growth of the Internet, IP traceback mechanisms have been developed to trace back illegal activities on the Internet. Because of the seriousness of the issues, most of the IP traceback mechanisms are designed to trace back either DoS or DDoS attacks. These attacks are reviewed in sections 2.2.2 and 2.2.3. In section 2.2.4, some common traceback mechanisms against such attacks are reviewed.

2.2.1 Background

As its name implies, the DoS attack tries to terminate the service on or to interrupt the services between the client and target computer. Most of the DoS attacks focus only on a particular target such as a computer or a company's network, and are often carried out with a certain intention such as gaining money or revenge. It will be quicker and easier to trace back these attacks after considering the possible attacker's motivation.

2.2.2 Denial of Service (DoS) Attack

DoS attack is the common name that represents hundreds of different attacks and it only describes the final effect of these attacks. DoS can be as simple as using a large PING packet to flood the network bandwidth of the computer or as complicated as exploiting the design flaws that exist in the application or the operating system.

> Denial-of-service effect…sending messages to the target that interfere with its operation, and make it hang, crash, reboot, or do useless work…to exploit a vulnerability present on the target machine or inside the target application…the target application, machine, or network spends all of its critical resources on handling the attack traffic and cannot attend to its legitimate clients (Mirkovic, Dietrich, Dittrich, & Reiher, 2004, p.2).

An example shows how a DoS attack is launched against the network bandwidth. To drain all network bandwidth from a computer, a PING flooding can be launched by overwhelmingly large PING packets sent to the target computer.

When the network interface card buffer is filled up with millions of large PING packets and all of the available bandwidth to the target computer is flooded by large PING packets, the computer will be disconnected from the network.

To avoid or mitigate the effect of a PING flooding, the latest design operating system and network communication device, such as a router, will reject PING packets larger than certain size. Since these attacks are often launched from one or two locations, the attacking path will then be more distinct and hence easier to be traced back.

Although a DoS attack explained above can seriously affect the computer operation, its scale and seriousness can never be compared with its variation, the DDoS attack.

2.2.3 Distributed Denial of Service (DDoS) Attack

Since year 2001, a new form of DoS attack known as DDoS attack has emerged. Although it can be seen as a variation of DoS attack, the area and depth of influence from the DDoS attack are unpredictable.

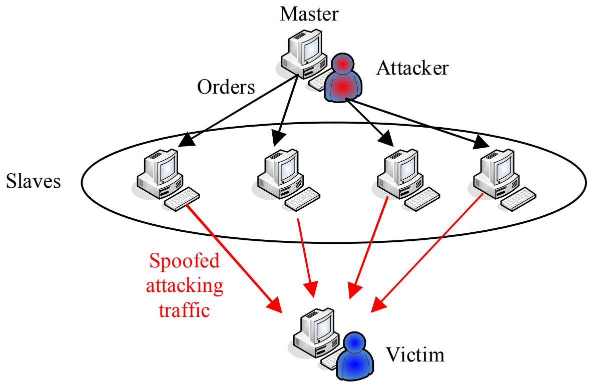


Figure 2.2: DDoS Attack

As shown in figure 2.2, the attacker (master) spreads special malware among the infected computers (slaves) to control their operation. After hundreds or even thousands of computers are infected, the attacker turns the infected computers into zombies (botnets) by ordering them to attack the victim computer.

The zombies will then send thousands or millions of packets to the victim computer either crashing down the computer or consuming all bandwidth available to the victim computer. When the attack is being launched, most of the infected computers' users don't even notice that they are involved in the DDoS attack.

> DDoS…uses a very large number of machines…many automated tools for DDoS can be found on hacker Web pages and in chat rooms…second characteristic of some DDoS attacks…use of seemingly legitimate traffic...when comparing the attack message with a legitimate one, there are frequently no telltale features to distinguish them…extremely hard to respond to the attack without also disturbing the legitimate activity (Mirkovic et al., 2004, p.2-3).

A notorious example for DDoS attack is reviewed here. In October of 2002, the backbone Domain Name Service (DNS) root servers were under DDoS attack and 9 out of 13 root servers' service disrupted. "With the reports that the attack had been the largest ever…it is rare to have attacks against all 13 at the same time" (Lemos, 2002, p1).

The backbone root domain name servers are used to translate the domain name into its corresponding IP address. Without the root domain name servers, Internet users cannot use the domain name to access the Internet. Instead they must use the IP address of the website.

The above example shows that a DDoS attack doesn't need to be launched at a large scale; it can be only focused on the crucial services and will still be able to affect millions of users. In a DDoS attack, the attacking traffic from the master often spoofs its source address to make the traceback much harder. Attackers can even use a "stepping stone" (Lee & Shields, 2002, p.14) to further hide their true locations. Once launched, a DDoS attack evolves into reflective DDoS attack as described by (Paxson, 2001) and tracing back it becomes a difficult task for investigators.

With either DoS or DDoS attack, the attackers usually hide their locations in Internet by spoofing the packet's source IP address. When the receiver captures the offending packet for analysis, they can only see the spoofed IP address of the source. Hence, different IP traceback mechanisms have been developed to deal with the above situation.

2.2.4 IP Traceback Mechanisms

Since routers are the core connectivity devices that direct all traffic in the Internet, most of the IP traceback mechanisms consider routers in their design. Four categories of traceback mechanisms utilising different router's resources are discussed below.

2.2.4.1 Link Testing-hop-by-hop Tracing

Link testing-hop-by-hop IP traceback mechanism starts by analysing the attacking traffic in the router closest to the victim. Since most of the routers have more than two interfaces and each interface is connected to different routers on the network, the traceback mechanism uses different approaches to discover through which interface the attacking traffic has come into the router. Once this is established, the method traces and links to another router that is in the direction of the source. This process is repeated one by one until the router closest to the attacker is reached.

Within the router, input debugging and controlled flooding are commonly used to discover where the attacking traffic comes from.

2.2.4.1.1 Input debugging

When related to routers, debugging means picking up the real time traffic's information and showing it either in real time on the router's console or recording them in a log file. By default, most routers will not turn on their debugging feature as debugging consumes large amount of the router's CPU and RAM.

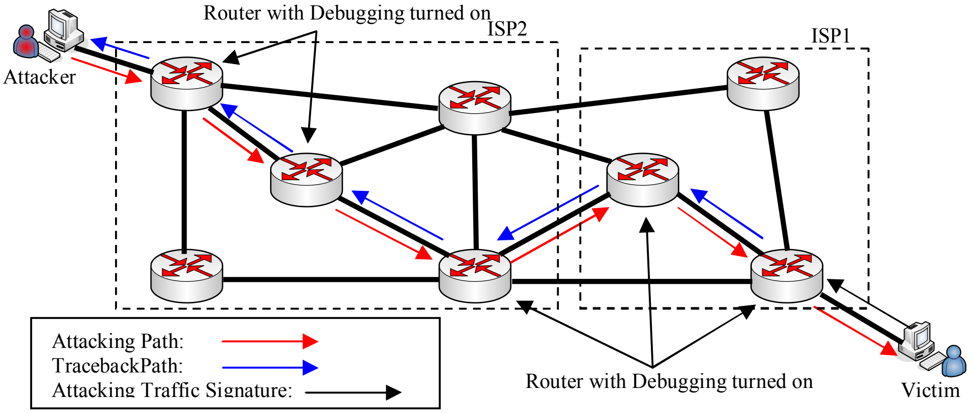

Router with Debugging turned on
ISP2
ISP1
Attacker
Attacking Path:
TracebackPath:
Attacking Traffic Signature:
Router with Debugging turned on
Victim

Figure 2.3: Input Debugging Approach

As shown in figure 2.3, the victim's side must collect and analyse the attacking traffic's signature or patterns and send this to the victim's ISP. The network operator in the ISP will then use the attacking signature as the parameter to turn on the debugging feature of the router. When the incoming traffic passing through the router matches the attacking signature, the corresponding interface which passed the incoming traffic will be show up to the network operator. The network operator can discover which interface the attacking traffic is coming from. Then the router link to this interface will be analysed by another network operator in another ISP with the same attacking traffic signature. The same process will be repeated until the attacking path is discovered (Savage, Wetherall, Karlin, & Anderson, 2001).

The debugging approach depends heavily on the cooperation between the network operators in different ISPs. Because there is currently no policy to force ISP to perform any traceback mechanism and ISPs have to spend extra effort for doing traceback, some ISPs may refuse or may have lack of resources to do so. Even if an ISP is willing to cooperate, a network operator may not be available, or may not have enough technical skills to perform the task. All this could make the debugging approach extremely hard to apply.

2.2.4.1.2 Controlled flooding

As the input debugging approach requires cooperation between ISPs as well as human resources, the controlled flooding has been developed to overcome the issue.

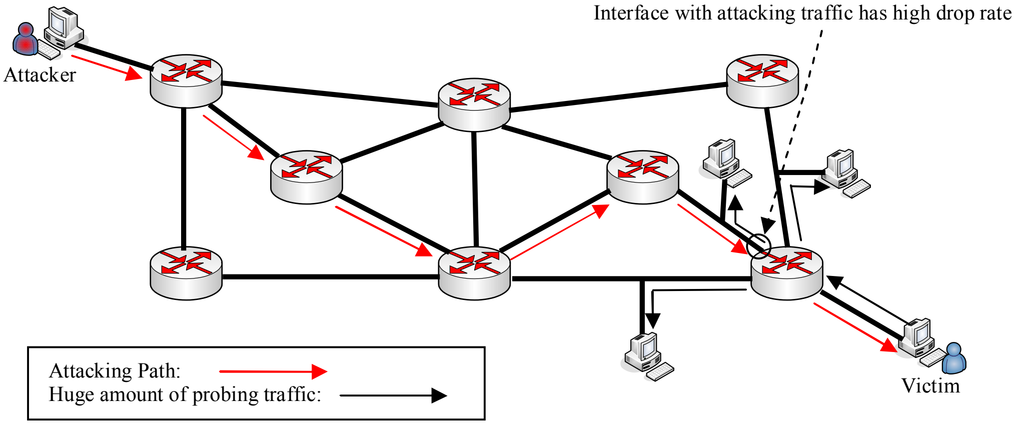

Interface with attacking traffic has high drop rate
Attacker
Victim
Attacking Path:
Huge amount of probing traffic:

Figure 2.4: Controlled Flooding Approach

As shown in figure 2.4, instead of requiring the network operator in the individual ISP to analyse the attacking traffic, the victim’s computer will actively probe individual routers along the attacking path.

The victim’s computer randomly chooses a computer connected to each interface of the closest router and send huge amount of traffic to these computers.

Then the interface with attacking traffic will have higher rate of packet drop then the other interfaces. The router linked to the interface with attacking traffic will then be probed again until the router closest to the source is found (Burch & Cheswick, 2000).

Although this approach totally bypasses the cooperation issues between ISPs, the network operator performing the approach must have a good understanding of a large portion of the Internet topology. Moreover, the DoS nature of the probing activities may raise legal issues during the traceback operation. Finally, in case of multiple sources attack such as a DDoS attack, it will be very hard to distinguish the interface(s) with attacking traffic because of the noisy nature of the traceback mechanism.

As link testing-hop-by-hop tracing mechanism can only be applied on real time traffic, i.e. it is only able to trace back the source during the attack, it is not efficient and is difficult to implement in real network environment.

2.2.4.2 Messaging (ICMP-based Traceback: iTrace)

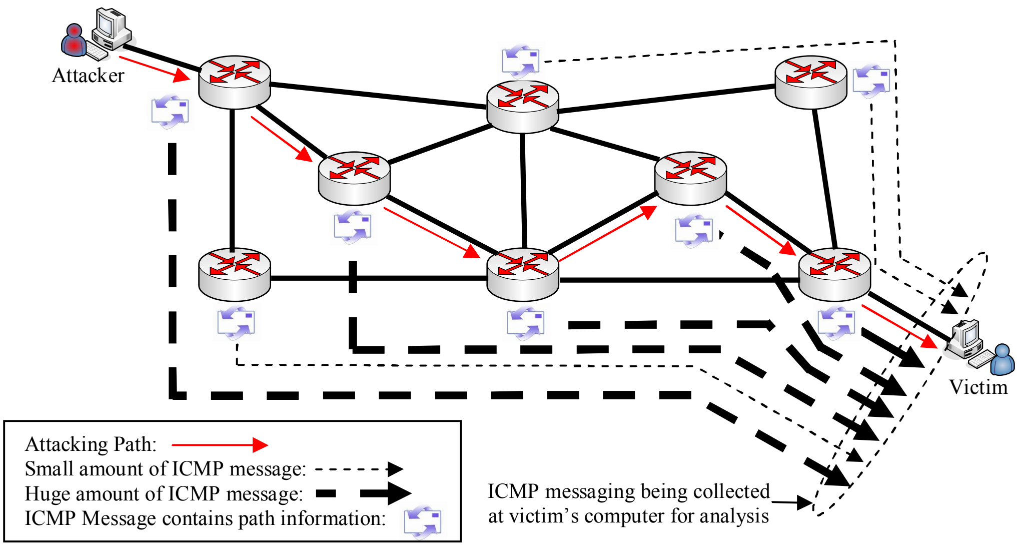

Attacker
Victim
Attacking Path:
Small amount of ICMP message:
Huge amount of ICMP message:
ICMP Message contains path information:
ICMP messaging being collected at victim's computer for analysis

Figure 2.5: Messaging

As shown in figure 2.5, in the iTrace traceback mechanism, the intermediate routers (routers between the source and destination) will generate a special ICMP packet according to the probability of 1 out of 20,000 once it received an IP packet. The ICMP packet will be sent to either the source or the destination host with equal probability. The router's path information is stored in the ICMP packet and is collected and analysed at the destination host. As the ICMP packets may also be sent back to the source, this allows the sources to identify the reflector attack (Savage et al., 2001).

However, with only forward or back link information, two routers can be identified in the path, while with two links information, three routers can be identified. Because only partial path information is contained in the ICMP packet, it will be extremely difficult to identify several attack paths under the DDoS attack.

Lee, Thing, Xu, and Ma (2003) suggest the modification of iTrace called iTrace-CP to modify the path information that is stored in the ICMP packet. With iTrace-CP, the destination host will be able to receive either the full path or partial path information from the source. To construct the full or partial path, the destination host has to match the original IP packet with its corresponding ICMP packet.

The original IP packet must be stored at the destination host to wait for either full or partial path information from its corresponding ICMP packets which requires a large amount of storage. Three approaches have been developed to overcome the storage limitation and they are: Basic Packet Identification (BPI), hashed-based packet identification and hashed-based packet identification with indicator bit.

Under a DoS attack and especially a DDoS attack, the router closest to the victim receives more traffic compared to the source's router. Hence, more ICMP packets are generated closest to the victim's computer but fewer are generated near the source. To overcome the issue, intention-driven ICMP traceback is used (Izaddoost, Othman, & Rasid, 2007). This method introduces a new extra bit called 'intention bit' in the router's routing table and forwarding table to control the generation probability of ICMP packet.

ICMP-based traceback has several advantages over other traceback mechanisms. It uses out-band messaging to send path information and hence has no compatibility issues. Also, it relies on the end system to store and process the data for path reconstruction, hence reduces the computational and storage overhead on the individual router. It has an excellent post-mortem capability, which is the ability to analyse the traffic and to reconstruct the attacking path after the attack.

However, ICMP-based traceback also has some drawbacks, such as the ICMP traceback message may be filtered or slow down from normal traffic or some routers in the Internet are not capable to have the input debugging feature that the ICMP traceback message requires. Furthermore, the attacker can send false ICMP traceback messages in order to confuse and slow down the path reconstruction process.

2.2.4.3 Logging

One of the most well known logging traceback mechanisms is called Source Path Isolation Engine (SPIE). Snoeren et al. (2002) define routers in the network as Data Generation Agents (DGAs) and subdivide the whole network into different zones that are handled by SPIE Collection And Reduction agents (SCARs) within the individual zone. A SPIE Traceback Manager (STM) is also defined as a central unit and be triggered by the Intrusion Detection System (IDS) at the victim site as shown in figure 2.6.

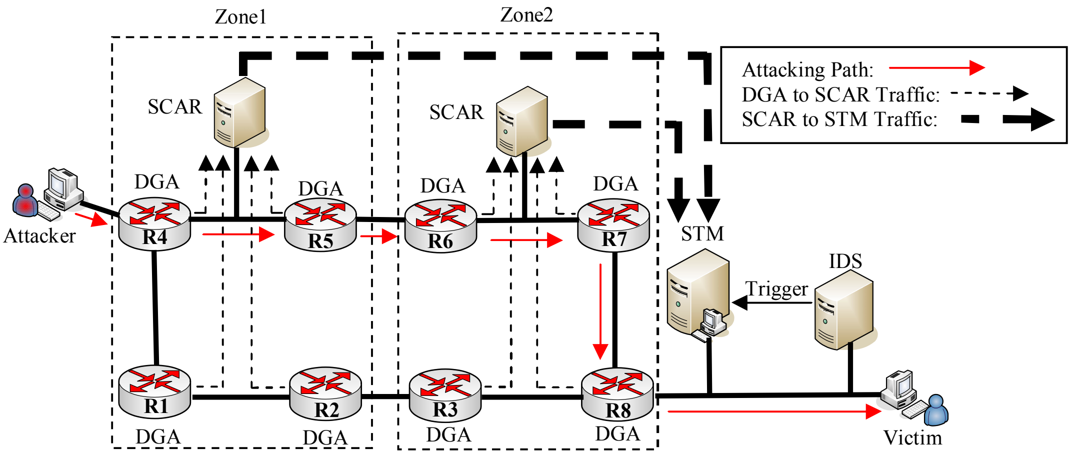


Figure 2.6: Source Path Isolation Engine

During normal operation, DGA records every packet passing through and hence each DGA requires massive amount of storage. To save storage space, each packet is reduced by hashing the IP header and the initial 8 bytes of the payload into a packet digest that can be used to uniquely identify the original packet.

To further save storage space for the hashed packets, a special space-efficient data structure named bloom filter is used to store the hashed packets. Each bloom filter contains its own Transform Lookup Table (TLT) to store the type of transformation and the information required to reconstruct the attack path within a period of time.

When an attack is detected by the victim's IDS, it triggers the STM. After verifying the authenticity and integrity of the IDS, STM then requests all SCARs in its domain to poll their corresponding DGAs for digest tables within certain time period as soon as possible, i.e. before the digest tables are overwritten. Once the SCARs receive the digest table, they process it and work out the partial attack routine. The STM then poll a partial attack routine from all SCARs and combines them to form a complete attacking path within its own domain.

Because SPIE log all network traffic and stores it as hash in the bloom filter to save storage space, the connection bandwidth and storage on the router limit its traceback time frame. When the connection bandwidth is large and the storage in the router is small, the time remaining for the SCARs to poll the digest tables from DGAs will be very small.

To make sure that digest tables related to the attacking path do not get overwritten by the new digest tables in the DGAs, many different storage architectures have been developed to save more space for the hash, such as Block-based Bloom Filter (BBF), Hierarchical Bloom Filter (HBF), Fixed Block Shingling (FBS), Variable Block Shingling (VBS), Enhanced Variable Block Shingling (EVBS), Winnowing Block Shingling (WBS), Winnowing Multi-Hashing (WMH) and Variable Doubles (VD) (Ponec, Giura, Brönnimann, & Wein, 2007).

Since all network traffics within the domain are logged, SPIE can trace back to the source of a single attack packet. SPIE can handle massive amount of traffic under DDoS attack and it is very hard to be bypassed. Still SPIE is not very scalable due to the huge amount of computational and storage overhead. Also only a very narrow time frame is available for SCARs to poll the DGAs in a high speed connection.

A One-Bit Random Marking and Sampling (ORMS) scheme by Sung, Xu, Li, and Li (2008) is designed to solve the problem. An extra bit is introduced in the packet to indicate whether the packet is sampled by the adjacent router or not. To further improve the correlation rate, more than one bit can be marked within the packet's IP header. With ORMS, the SPIE can be scaled to a very high link connection up to OC-768.

2.2.4.4 Marking

Different marking traceback schemes have been developed and the core differences between them are the marking algorithms being used to improve the efficiency of the traceback. One of the well known marking mechanisms called Probabilistic Packet Marking (PPM) is reviewed below.

As shown in figure 2.7 and described by Savage et al. (2001), PPM used the algorithm known as 'node sampling' to mark the packet. Node sampling inserts router's address information into a field, most often this is the packet identification field, in the packet header. Due to the insertion and probabilistic behaviour, the packet size never increases regardless of the distance it traverses and the router's overhead is reduced.

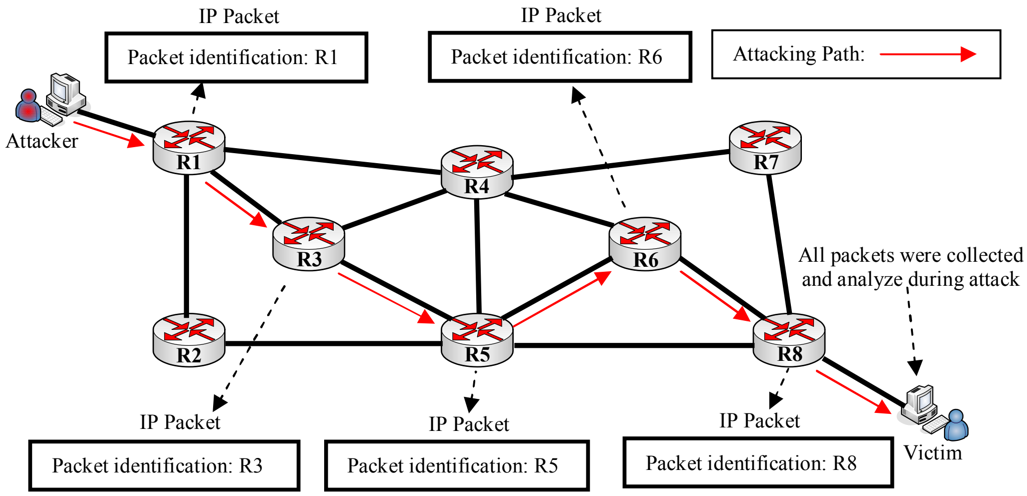

IP Packet
Packet identification: R1
IP Packet
Packet identification: R6
Attacking Path:
Attacker
R1
R2
R3
R4
R5
R6
R7
R8
All packets were collected and analyze during attack
IP Packet
Packet identification: R3
IP Packet
Packet identification: R5
IP Packet
Packet identification: R8
Victim

Figure 2.7: PPM Marking Using Node Sampling

With PPM, the attacker cannot insert false address information in advance in order to mislead the path reconstruction process. Due to the sampling nature of PPM, the victim host will only receive partial path information from individual packets and must receive large amount of attacking packets before the path reconstruction can be completed.

Under DoS or DDoS attack, thousands or millions of packets are sent to the victim and hence victim will have no difficulty in collecting enough attacking packets for path reconstruction. However, to analyse the huge amount of attacking packets with the addressing information among the packets showing no correlation to each others, the path reconstruction process will be extremely slow.

Due to the probabilistic sample nature of PPM under a DoS or DDoS attack, the router closer to the victim will receive more traffic than the router closer to the source. Finally, when multiple attackers exist with the same distance away from the victim, it is extremely hard to distinguish between them. Hence another algorithm named “edge sampling” (Savage et al., 2001) has been developed to solve the issue.

With edge sampling, attacks from multiple sources can be distinguished from different edge-IDs contained in the packet. However, fitting the 72 bits edge-ID into the 16-bit IP identification field is a real challenge for the edge sampling implementation. Another sampling method named Compressed Edge Fragment Sampling (CEFS) (Song and Perrig, 2001) that uses exclusive OR operation on the addresses has been introduced to solve the issue.

The last concern with PPM is the compatibility issue. The IP identification field is used to identify individual IP fragments if the packet has been fragmented during transmission. The statistics in Devasundaram (2006) show that less than 0.25% of packets are fragmented. Since fragmentation decreases the network performance, most of the network today will implement automatic Minimum Transfer Unit (MTU) discovery to prevent packets from being fragmented along different communication media.

Packet marking is characterises with relatively low computational and storage overhead compared to log-based traceback mechanism and the attack can be traced back “post-mortem”.

2.3 SUMMARY OF ISSUES & PROBLEMS

The greatest problem in IP traceback is that the attackers can arbitrarily change the source IP address in the IP packet to hide their true locations in the Internet. Because all Internet users must acquire an IP address from their ISPs and ISP has good understanding of which IP address was assigned to the user, ISP can provide great help by preventing the user from sending their packets without a valid source IP address.

With the cooperation from ISP, source IP address filtering can be applied to validate the packet being passed from the ISP to the Internet, meaning that a user cannot spoof the source IP address. Therefore, tracing back to the source of attacks will become much faster and easier.

Although source IP address filtering will consume extra router's resources and slightly slow down the routing process, with the modern router's capabilities the performance degradation can be ignored. To avoid attackers using the ISP without source IP address filter applied on the routers, all ISPs must agree to setup the source IP address filter.

However, there is still no regulation in place to force ISPs to set up filters and also different ISPs may encounter various issues when setting up the filter. Even if all ISPs in the world agreed to apply the source IP address filter, it might still take a while for all ISPs to implement it. At the moment, tracing back to the source must still rely on various traceback mechanisms (Aljifri, 2003).

In the world of email forensics, software has been developed to search and recover digital evidence within massive amounts of emails. The trend of software design is to focus on the power of email analysis instead of on email traceback. Usually, email traceback relies on other utilities available on the Internet and most of them require a real source IP address from the email. With a real source IP address in place, the traceback utilities can be quite efficient and accurate in tracing back to the origin. However, hackers like to hide their locations by spoofing the source IP address within the emails and the email traceback utilities become useless.

Four categories of trace back mechanisms, link testing hop-by-hop tracing, messaging, logging and marking, are reviewed in this chapter to see whether they can be used for email traceback on spoofed source IP address.

Link testing hop by hop tracing requires less resources from the router compared to the other trace back mechanisms. However, it involves cooperation between ISPs and can only be performed in real time.

Messaging uses out-of-band ICMP message for path communication and has no compatibility issue. However, false ICMP messages may be generated by the attacker to slow down or even misdirect the path reconstruction process.

Logging provides an infrastructure to track all packets and hence can trace back the source of a single packet. However, it requires massive amount of storage space in the router and only has a very short polling interval for effective traceback.

Marking utilizes the internal space of the packet to carry the path information hence reduces extra traffic flow in the network. However, it poses the great challenge to fit enough valuable path information into a tiny space within the packet.

These mechanisms are effective against DoS or DDoS attack with the source IP address of the packet being spoofed. But they are complicated and very hard to implement. Also, they requires huge amount of memory for data storage and high computational power for path reconstruction. Most of them involve the collection of million packets before path reconstruction can be carried out. The above constraints restrict their usage for email traceback.

2.4 CONCLUSION

After reviewing the literature, it is apparent that the email header traceback described in section 2.1.3 is only able to trace back the source email server from which the offending email has been sent by the attacker. Then the source IP address retrieved from the offending IP packet must be used to search for the router to which the attacker is attacked. If the source IP address was spoofed, most of the email forensics software would not be able to trace back the source.

IP traceback mechanisms are designed to trace back the DoS or DDoS attacks. Most of the implementation of it is complicated and resource-hungry, so it is not suitable to apply them in the environment with fewer resources such as email forensics.

The hop count distance method is proposed in chapter 3 to provide simple and fast traceback still requires less resource for implementation. Chapter 3 also describes the problem associated with hop count distance method, the factors affecting the default hop count value estimation and the Internet hop count stability. Then the testing framework for the hop count distance method is described and applied to collect the data necessary to examine the method.

Chapter Three

RESEARCH METHODOLOGY

3.0 INTRODUCTION

Chapter 2 reviews the characteristics of email header traceback in section 2.1.3 and IP traceback mechanisms in section 2.2.4. These traceback mechanisms have their own drawbacks when applied to email forensics. The hop count distance model will be proposed in order to fill the gap between the email traceback and the IP traceback mechanisms. Because the hop count distance model is different from other traceback mechanisms, there is no information available about how accurate the model would be. Therefore, the accuracy of the hop count distance model must be examined first.

The hop count distance model contains three blocks, but only the packet signature identification and default hop count estimation & validation blocks need to be examined. The architecture of the hop count distance model is simple compared to the complex IP traceback mechanisms. Therefore, the individual blocks in the hop count distance model must be closely examined to determine if the simplicity of the model doesn’t affect its accuracy.

To work out a suitable framework for testing the hop count distance method, several methodologies from different publications related to the hop count distance model are first reviewed. Then a review on the hop count distance method is presented and a data map related to the method is constructed to show the main question associated with the hop count distance method and what kind of data needs to be collected in order to find the answer. Once the testing framework is setup, a detailed explanation is provided on how data is collected, processed, analysed and presented. The limitations of the research are also discussed.

Section 3.1 reviews the methodologies discussed in five publications that are related closely to the research topic. Section 3.2 provides a diagram and data map for the hop count distance method to show how the method works and what kind of data should be collected. Section 3.3 shows the framework for testing the hop count distance method. Section 3.4 provides detailed description of how the relevant data collected from model testing is collected, processed, analysed and presented. Section 3.5 outlines the limitations of this research and is followed by conclusions in the final section.

3.1 REVIEW OF OTHER PUBLICATIONS

The hop count distance method can reduce the searching scope of investigation even if the source IP address of the attacking traffic is spoofed and it relies heavily on the packet's TTL field to work out the hop count distance between the attacking source and the victim. Hence five publications related closely to the characteristics of the hop count distance method are reviewed.

The first publication by Wang, Jin, and Shin (2007) is about hop-count filtering that is an effective defense against spoofed DDoS traffic and is reviewed in section 3.1.1. The default hop count estimation and Internet hop count stability described in the publication provide valuable information for designing the testing framework.

The second publication (Izaddoost, Othman, & Rasid, 2007) is about an accurate ICMP traceback model used in case of DoS/DDoS attacks and is reviewed in section 3.1.2. The publication describes the simulation tool Network Simulator 2 (NS2) used to test the traceback model. NS2 has been used for testing many traceback mechanisms and is reviewed to see whether it can be used to test the hop count distance method.

The third publication by Snoeren et al. (2002) is about single-packet IP traceback and is reviewed in section 3.1.3. The traceback mechanism described in the publication allows the investigator to trace back the source by only a single packet. Since the hop count distance method can help the investigator to narrow down the scope of investigation by using a single packet as well, the similarity between the methods may provide useful information for the design of the testing frame of the hop count distance method.

The fourth publication (Wu, Tseng, Yang, & Jan, 2009) is about DDoS detection and traceback with decision tree and grey relational analysis. The testing tool introduced in the publication is known as DEfense Technology Experimental Research laboratory (DETERlab) testbed and provides a powerful traceback testing capability in both software and hardware. Hence the publication is reviewed in section 3.1.4 to see whether DETERlab is suitable for testing the hop count distance method or not.

The fifth publication by Devasundaram (2006) is about performance evaluation of a TTL-based dynamic marking scheme in IP traceback. In the publication, the TTL field is used to measure the distance which is similar to the hop count distance method, hence the publication is reviewed in section 3.1.5.

3.1.1 Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic

Wang, Jin, and Shin (2007) propose a hop-count filtering method to defend against spoofed DDoS attacks. The basic idea of the hop-count filtering method is to identify spoofed IP packets by using the source IP address and hop count value in the IP packet and then filter the spoofed IP packet under DDoS attack.

The rationale is that most spoofed IP packets do not carry hop count values that are consistent with the IP addresses being spoofed at the victim computer. Hence an IP-to-hop-count (IP2HC) mapping table is built during normal computer operation to distinguish between the attacking and the normal traffic. The simulation results show that close to 90% of spoofed traffic was identified.

Once the accurate IP2HC mapping table is built, the inspection algorithm checks the source IP address and the final TTL value in each packet. The final TTL value will be used to estimate the default hop count value created by the operating system then the default hop count value will be subtracted by final TTL value to create the hop count distance between the source and the victim. The source IP address is then combined with the hop count distance and checked against the IP2HC mapping table for validation.

As the Internet hop count stability plays a crucial role in hop count filtering, the stability of hop count value tested by traceroute command at ten-minute intervals among 113 sites between 1st January and 30th April, 2003. The test proved that 95% of the paths had fewer than five observable daily changes.

The idea of hop-count filtering has its similarities to the hop count distance method. First, it has to estimate the default hop count value assigned by the operating system. It only uses the first power of 2 greater than the final hop count value to estimate the default hop count value although the estimation cannot be used to distinguish the default hop count value between 60 and 64. Since the Macintosh operating system uses 60 for the default hop count value.

Wang, Jin, and Shin (2007) believe that operating systems associated with the default hop count value of 30 and 60 typically are older operating systems and it is expected they only occupy a very small share of the market. However, in the experiment, operating system estimation software such as *p0f* was used to increase the estimation accuracy. The software is able to identify Macintosh and other seldom used operating systems and then lookup their corresponding default hop count values.

The second similarity is that both methods require stable hop count across the Internet, hence have to test the Internet hop count stability. Because the test was conducted seven years ago and since then the Internet has changed significantly, further tests on hop count stability should be conducted during the examination of the hop count distance method.

3.1.2 Accurate ICMP Traceback Model under DoS/DDoS Attack

To test the real time behaviour of a network, a well-known tool named Network Simulator 2 (NS2) was used. NS2 is an open-source simulation tool that runs on Linux and can provide real-time network simulation under different scenarios (Haddad & Gordon, 2002).

The model Intention-driven iTrace proposed by Izaddoost, Othman, & Rasid (2007) was tested by NS2 on *fedora core 6.0*. Intention-driven iTrace was developed to increase the efficiency of the original ICMP traceback. In an original ICMP trace back environment, for every packet arrives the router will generate an ICMP message and send it to the source or destination according to a very low probability, about 1/20,000.

Under DoS or DDoS attacks, a router near the victim side will receive far more traffic compared to the attacker side router and hence much more ICMP traffic will be generated near the victim side of the router. The basic idea of ICMP traceback is to analyse and reconstruct the attacking path on the victim's computer from the ICMP message generated by the routers along the attacking path.

If less ICMP traffic close to the source of attack is collected, the victim computer needs to collect more packets before the attacking path can be reconstructed and hence lowers the efficiency of the traceback. Intention-driven iTrace introduces an extra bit from the router on the packet to increase the probability of ICMP message being generated by the router near the source.

With NS2, the router's parameters can be tuned to simulate the proposed model and different attacks can be generated on the model. In the hop count distance method, simulations of the router's hop count deduction and the packet's hop count parameter are required but NS2 doesn't provide the necessary functionalities. Moreover, Internet hop count stability data can only be obtained from real Internet environment hence the software simulation is not suitable for testing the hop count distance method.

3.1.3 Single-Packet IP Traceback

Snoeren et al. (2002) developed the IP traceback mechanism named Source Path Isolation Engine (SPIE) to enable traceback of the source from even a single IP packet. The idea of tracing back from a single IP packet has similarity with the hop count distance method that depends on a single IP packet's signature to help narrow down the trace back scope.

The SPIE network infrastructure consists of Data Generation Agents (DGAs), SPIE Collection and Reduction Agents (SCARs) and a SPIE Traceback Manager (STM). Routers act as DGAs with each SCAR in charge of a zone of DGA. At the time an attack is detected by the Intrusion Detection System (IDS), IDS will trigger the STM. STM will then pull all the SCARs in different zones for data and SCAR in each zone will request data from DGAs in its zone.

Every DGA will make a copy of the packet that passes through and stores it locally. As the amount of data is huge, only the packet digest will be stored in a Bloom filter for a short period of time. So, the pulling mechanism from STM must be fast enough to retrieve valuable data from DGAs. The bloom filter is a space efficient data structure for data storage and can increase the amount of storage significantly.

To test the traceback mechanism, an extensive simulation has run on the actual network topology of a national tier-one ISP made up of roughly 70 backbone routers with links ranging from T-1 to OC-3. An attack was simulated by randomly selecting a source and a victim, and sending 1000 attack packets at a constant rate between them.

Uniformly distributed background traffic is simulated by selecting a fixed maximum false-positive rate for the digest table at each off-path router.

The testing methodology described in the publication is a real time multiple attack simulation. It utilised part of the real Internet's network and simulated about 1,000 attacks across the network to obtain data about the network real time behaviour.

Because the hop count distance method requires no special installation and tuning of the Internet router, it is also possible to perform the test on part of the real Internet network in order to obtain the Internet real time behaviour data of the Internet hop count stability. To obtain more realistic result from the simulation, the effect of background traffic in the Internet should be taken into account. Therefore, the test should be conducted during different periods of time to include the peak and non-peak background traffic.

3.1.4 DDoS Detection and Traceback with Decision Tree and Grey Relational Analysis

Another testing method known as DEfense Technology Experimental Research laboratory (DETERlab) testbed, was introduced to test the traceback method (Wu, Tseng, Yang, & Jan, 2009).

> DETER allows security researchers to replicate threats of interest in a secure environment and to develop, deploy and evaluate potential solutions. The testbed has a variety of hardware devices and supports many popular operating systems. Researchers obtain exclusive use of a portion of a testbed, configured into a user-specified topology, and shielded from the outside world via a firewall. DETER's hardware infrastructure was enhanced by a collection of software tools for traffic generation, statistics collection, analysis and visualization, developed in its sister project EMIST (Mirkovic et al., 2007, p.1).

Wu et al. (2009) designed a system to detect DDoS attacks based on a decision-tree method. After detecting an attack, a traffic-flow pattern-matching technique is used to trace back the approximate locations of the attacker. The system consists of two parts: protection agents and sentinels. The protection agents reside on the victim site to handle the DDoS attack detection and path reconstruction. The protection agent obtains and analyses the signature from layer 3 to layer 4 of the incoming traffic then, based on the decision tree and rules, it determines whether any abnormality exists.

If an attack is detected, the agent creates a secure SSH-tunnel with the sentinels deployed on all routers to collect corresponding traffic with the attacking signature. The agents then reconstruct the attacking path from the collected data.

DETER provides not just software but also hardware infrastructure to simulate the network environment. Although it provides more powerful features compared to NS2, it still doesn't provide the hop count information required for testing the hop count distance method. Therefore, DETER would not be considered for testing the hop count distance method.

3.1.5 Performance evaluation of a TTL-based dynamic marking scheme in IP traceback

Devasundaram (2006) proposes an algorithm that dynamically sets the value of the marking probability based on the 8-bit TTL field in the IP header. It utilises the variable TTL value as an estimation of the distance travelled by a packet and thereby its position in the attack path to derive the marking probability value. Since the hop count distance method is also based on the TTL field in the IP header to estimate the distance between the source and destination, the methodology by Devasundaram is reviewed to find out if it can be utilised by the hop count distance method.

In a traditional Probabilistic Packet Marking (PPM) traceback, the marked packets from distant routers have more chance to be remarked by the next hop router and hence the efficiency of the path reconstruction can be reduced. Under the dynamic marking scheme, a router will mark the packet's TTL field to indicate the router's position along the attacking path and hence the router can extract the TTL information to determine the marking probability dynamically.

As the TTL field can be directly accessed by the router, the dynamic marking scheme provides a good compatibility with the existing routing structure and creates no overhead on the existing packet.

The algorithm was simulated by the simulator developed in C# 2005 with topological map of routers obtained from the Internet Mapping Project. Although the simulator developed above is concerned with the TTL field in the IP packet, it is not designed to test hop count distance method and program simulation may not be able to accurately reflect the actual Internet environment, especially on testing the Internet hop count stability.

When operating system estimation is tested by program simulation, the result may be too ideal to be used in the real world as well. In the real world, even the same kind of operating system may have different language versions and may come with different operating system parameters that may affect the operating system estimation result. Real world simulation can provide more realistic test of the hop count distance method and the generated result can estimate the accuracy of the method much better.

The default hop count estimation method described in Wang, Jin, and Shin (2007) is the same as the estimation method used for the hop count distance method. To increase the estimation accuracy, the operating system estimation should be used. The Internet hop count stability test should also be performed again because the stability test described in the publication was carried out seven years ago.

The NS2 testing software used in Izaddoost, Othman, & Rasid (2007) does not provide the required functionality for testing the hop count distance method. The third reviewed publication Snoeren et al. (2002) provides an idea for a real Internet test for the hop count distance method. The background traffic for the real Internet test must also be taken into account.

Although the tool DETERlab testbed provides rich software functionalities and powerful hardware platform for testing the traceback as described in the fourth reviewed publication (Wu, Tseng, Yang, & Jan, 2009), testing for hop count distance from the packet TTL is not available in DETERlab. Finally, the method that uses the TTL field to estimate the packet's travel distance described in Devasundaram (2006) was tested by custom developed software. Software simulation of the hop count distance method will only provide ideal results for the Internet hop count stability and for the default hop count estimation and hence it will not be considered.

3.2 THE HOP COUNT DISTANCE METHOD

The hop count distance method depends on the packet's signature and the hop count value to determine the approximate location of the attacker even when the source IP address of the packet is spoofed. It may not work as precisely as the traceback mechanisms used in DoS or DDoS attack but it require far less resources and is much faster in determining the approximate location of the attacker. Thus, it may be suitable for use in email forensics environment.

A model is constructed based on the hop count distance method as shown in figure 3.1.

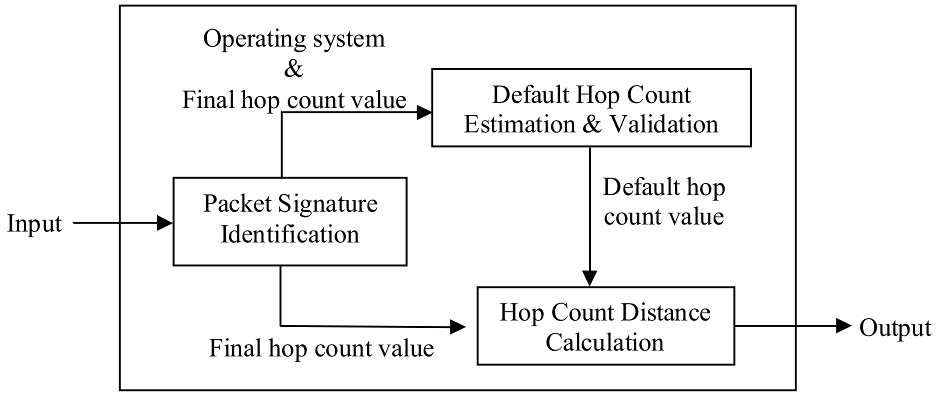

Operating system
&
Final hop count value
Default Hop Count Estimation & Validation
Input
Packet Signature Identification
Default hop count value
Hop Count Distance Calculation
Final hop count value
Output

Figure 3.1: Hop Count Distance Model

The hop count distance model consists of three blocks: packet signature identification, default hop count estimation and validation, and hop count distance calculation block. The basic function of the model is to work out the hop count distance between the source and destination hosts from the TTL field in the IP packet.

3.2.1 Packet Signature Identification Block

IP packet signature is the footprint of the packet when it is created by the operating system. Different operating systems leave different signatures on the packets which they create. By analysing the received packet's signature, the operating system which sent the packet can be determined.

Although the operating system can only be estimated, the estimation can be very close to the actual type of operating system if the method uses a passive fingerprinting tool such as p0f or SinFP, provided the packet's signature are not modified by applications from the packet sender. As described in the readme file from p0f software by Zalewski and Stearns (2001, p.1):

> Usually initial TTL (8 bits), windows size (16 bits), maximum segment size (16 bits), don't fragment flag (1 bit), sackOK option (1 bit), nop option (1 bit), windows scaling option (8 bits) and initial packet size (16 bits)…67-bit signature for every system…determine initial TTL of a packet…it is equal to the first power of 2 greater than TTL.

The term "initial TTL" described above means the same as the term "default TTL" used in the thesis. Although the default TTL value has been estimated already as the first power of 2 greater than the final hop count value by the p0f algorithm, it will be more precise to combine the estimated default TTL value with other TCP parameters and come up with a better estimation on the operating system being used, especially in distinguishing the packet with TTL field pair of (30, 32) and (60, 64).

Packet signature identification block collects the default TTL, windows size, maximum segment size, 'don't fragment' flag, sackOK option, nop option, windows scaling option and initial packet size then comparing these parameters with the operating system identification database in order to work out the operating system that has sent the packet.

Then the block sends the resulting operating system and final hop count value retrieved from the packet to the default hop count estimation & validation block for default hop count calculation.

3.2.2 Default Hop Count Estimation & Validation Block

The default hop count value inserted by the operating system into the TTL field of the packet differs depending on the operating system. Since the introductory of Windows 98 and NT4.0 with SP6+, the TTL value of the packet has been set to 128 in Windows environment. All versions of Solaris set their TTL value to 255. HP/UX 10.01, Linux and FreeBSD 2.1R, set their default TTL value to 64. Irix, MacOS/MacTCP 2.0x use the default value of 60 in the TTL field. The TTL field of the packet can be modified by software such as *netconfig*, *set_ttl* and *ttlfix*, so the hop count distance method is only valid for the group of users who don't have enough knowledge or skill to modify the TTL field.

In the default hop count estimation & validation block, the operating system estimated by the packet signature identification block will be used to look up the corresponding default hop count value assigned by different operating systems. If the operating system estimation result from the packet signature identification block is unknown, then the final hop count value from the packet signature identification block will be used to estimate the default hop count value as the first power of 2 greater than the final hop count value.

Finally, the default hop count value will be passed for the TTL validation check. To check for TTL validation, an assumption about the maximum hop count distance (30 hops) that a packet can pass through in the Internet is made first.

If the default hop count value of the packet is 128, in order to have a correct estimation, the possible final hop count value for the packet are in the range between 64 and 127 according to the operating system estimation. With the above assumption, each packet can only pass through 30 routers in the Internet. So, the valid ranges of TTL when the default hop count value of the packet is 128 are between 94 and 157.

Again if the default hop count value of a packet is 64, the valid ranges of final hop count value are between 62 and 93. If the default hop count value fall within these ranges, then it can be passed to the hop count distance calculation block. Otherwise, an alert is raised to indicate that the IP packet signature has been altered.

3.2.3 Hop Count Distance Calculation Block

Because the hop count distance method depends highly on the hop count value of the packet to determine the distance between the source and destination, although the hop count value on the Internet may not be the same all the time, it is essential to study the stability of the hop count value between the source and destination.

Hop count value stability was examined by (Wang & Shin, 2007). In year 2003, around 10,000 routes to 113 sites were tested for three months and it was found that 95% of the paths had fewer than five observable daily changes. So, it appears that the hop count is quite stable in the Internet. However, while the Internet environment has been changing rapidly, the test was conducted by Wang et al 7 years ago. Therefore, the hop cont stability will be examined again at the time when the hop count distance model is tested.

Another factor that may affect the hop count stability in the Internet is whether the router will decrement the TTL field of the IP packet by more than one or not. This depends on how long the packet has been held in the router. As mentioned by Baker (1995) the TTL field is measured in seconds and is used to limit the time that a packet can travel in the network. When the router handles the packet for less than one second, it will decrement the packet by at least one.

If the router holds the packet for more than one second, it may decrement the TTL field of the packet by one for each second. In fact, the TTL field is decremented by more than one very rare in the Internet. Most of the routers can process a packet in the nanosecond range (Crowley, Franklin, Hadimioglu, & Onufryk, 2002) hence the TTL field is decremented only by one for all routers in the Internet. It can be assumed in the model.

The final factor that may affect the hop count stability in the Internet is that the router can also be configured to propagate the TTL field across the ISP's Multi-Protocol Label Switching (MPLS) network by the propagate-ttl command. Hence the routers within the MPLS network can be hiden for an outsider. In other words, the MPLS network's router will not decrement the TTL field (Pepelnjak & Guichard, 2002). Most of the ISPs that deploy MPLS in their core choose to hide the routers at all times, so the hop count value across the ISP will be consistent and hence the above factor will not affect the model.

At the end, in the hop count distance calculation block, the default hop count value is subtracted by the final hop count value and output with the hop count distance between the source and destination.

3.3 HOP COUNT DISTANCE METHOD DATA MAP

After reviewing the methodologies described in five publications and the hop count distance method, the next step before the construction of the testing framework is to consider what data needs to be collected. The operation of the hop count distance method is presented in the block diagram in figure 3.2 first. Figure 3.3 shows the data map of the hop count distance method.

As shown in figure 3.2, when the source computer sends a packet to the receiver, the packet is assigned with the default hop count value in the IP header TTL field by the operating system or application. When the packet passed through any router in the Internet, the hop count value in the TTL field is decremented by the router by at least one.

At the time receiver received the packet, the final hop count value from the TTL field in the packet can be extracted and used to estimate the default hop count value from the packet's signature. Then the hop count distance between the source and destination can be worked out by subtracting the final hop count value from the default hop count value.

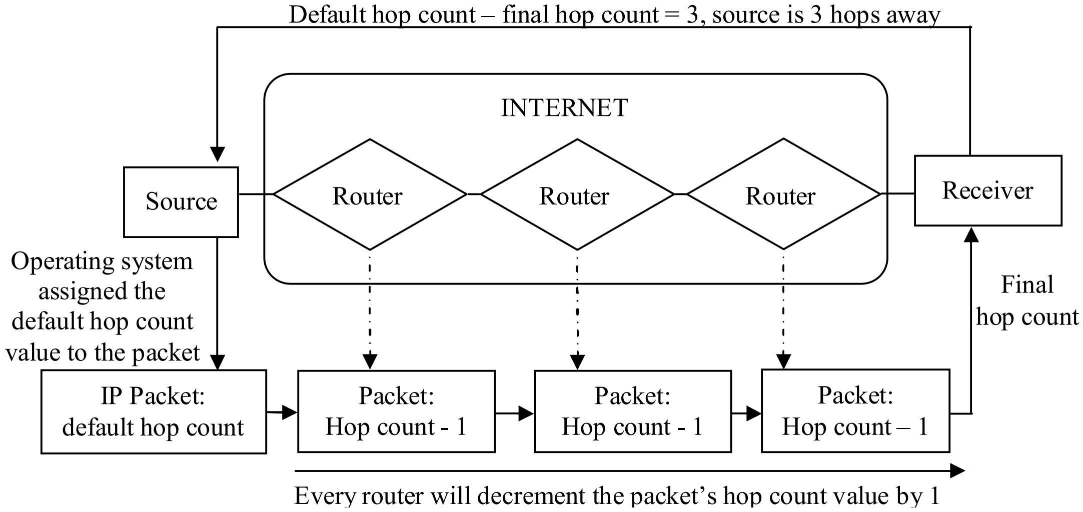

Default hop count – final hop count = 3, source is 3 hops away
INTERNET
Source
Router
Router
Router
Receiver
Operating system assigned the default hop count value to the packet
Final hop count
IP Packet: default hop count
Packet: Hop count - 1
Packet: Hop count - 1
Packet: Hop count – 1
Every router will decrement the packet's hop count value by 1

Figure 3.2: Hop Count Distance Method Diagram

As shown in figure 3.3, the main question for the hop count distance method is its accuracy. There are two uncertainties that affect the accuracy of the hop count distance method. The first one is the accuracy of the default hop count estimation. The default hop count estimation accuracy is further affected by four hypotheses. The first hypothesis is the default hop count value is intact. When the default hop count value is intact from the attacking source computer, there is a high probability to obtain accurate default hop count value estimation. If hypothesis 1 fails, then hypothesis 2 should be verified to find out if the default hop count estimation accuracy is affected by changes in the default hop count value.

Since Network Address Translation (NAT) is commonly used in today's network environment, NAT is considered under hypothesis 3 to find out whether it will change the default hop count value of the packet. If so, hypothesis 4 will be used to test how the accuracy of the default hop count estimation will be affected by NAT.

The second uncertainty is the Internet hop count stability. There are four hypothesises that will affect the Internet hop count stability. Hypothesis 5 assumes that all packets travel between the same source and destination using the same path. If so, hypothesis 6 is to verify the Internet hop count stability along the same path between the source and destination. Otherwise, hypothesis 7 will be used to verify the Internet hop count stability across different paths between same source and destination. Finally, hypothesis 8 assumes that the hop count decrement on each router along the same path is consistent by one.

After verifying all eight hypothesises, the accuracy of the default hop count estimation and the Internet hop count stability can be worked out. This will allow for the hop count distance accuracy to be determined. Therefore, the testing framework described in the next section will need data for testing the eight hypothesises.

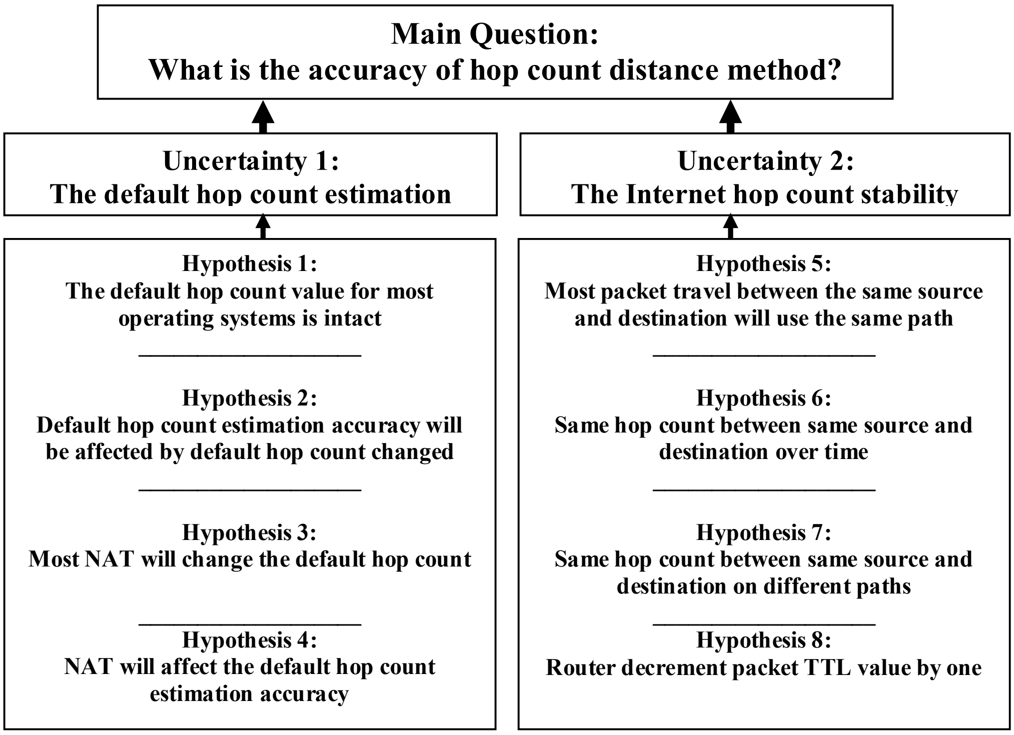

Main Question:
What is the accuracy of hop count distance method?
Uncertainty 1:
The default hop count estimation
Uncertainty 2:
The Internet hop count stability
Hypothesis 1:
The default hop count value for most operating systems is intact
Hypothesis 2:
Default hop count estimation accuracy will be affected by default hop count changed
Hypothesis 3:
Most NAT will change the default hop count
Hypothesis 4:
NAT will affect the default hop count estimation accuracy
Hypothesis 5:
Most packet travel between the same source and destination will use the same path
Hypothesis 6:
Same hop count between same source and destination over time
Hypothesis 7:
Same hop count between same source and destination on different paths
Hypothesis 8:
Router decrement packet TTL value by one

Figure 3.3: Data Map

3.4 HOP COUNT DISTANCE METHOD TESTING FRAMEWORK

A framework for testing both the default hop count value of the IP packet and the Internet hop count stability is proposed in this study and is shown in figure 3.4.

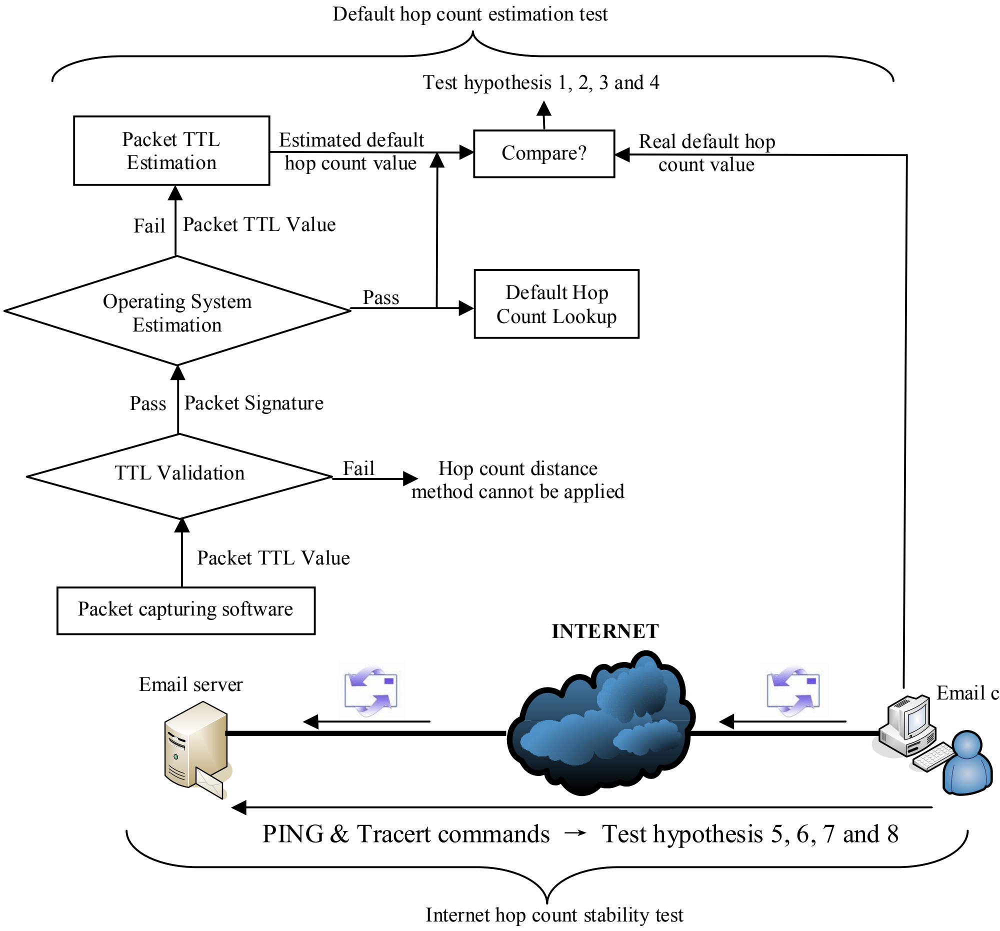

Default hop count estimation test
Test hypothesis 1, 2, 3 and 4
Packet TTL Estimation
Estimated default hop count value
Compare?
Real default hop count value
Fail
Packet TTL Value
Operating System Estimation
Pass
Default Hop Count Lookup
Pass
Packet Signature
TTL Validation
Fail
Hop count distance method cannot be applied
Packet TTL Value
Packet capturing software
INTERNET
Email server
Email client
PING & Tracert commands → Test hypothesis 5, 6, 7 and 8
Internet hop count stability test

Figure 3.4: Testing Framework

As shown in figure 3.4, when an email is sent from a testing location through the Internet to the email server, it is captured by the packet capturing software. The packet capturing software then passes the packet TTL value or the final hop count value to the TTL validation block for validation. The validation was fails if the default hop count value has been modified to a point where the hop count distance method cannot be applied. Otherwise, the packet signature is passed to the operating system estimation software for operating system estimation.

A lookup table is used to work out the default hop count value assigned by that operating system. If the operating system estimation software fails to recognise the operating system, the received packet's TTL will be used to estimate the default hop count value. The data collected from the estimated default hop count value and the actual hop count value will be used to calculate the hop count distance and test hypothesis 1, 2, 3 and 4.

Ping command is used to test the Internet hop count stability across different intervals. Tracert command will be used to check if the same path is used for communication between the same source and destination. Data collected from ping and tracert command is used to test hypothesis 5, 6, 7 and 8.

Data is collected from 19 different testing locations in different intervals within the same day and also across different days in order to exam the Internet hop count stability from small to medium scope. Once the data for testing the eight hypothesises are collected, the accuracy of the two uncertainties can be calculated. Then the hop count distance method accuracy will be worked out as the product of default hop count estimation accuracy and the Internet hop count stability with the valid interval of the hop count distance method restricted by the Internet hop count stability.

The statistics cited in netmarketshare (2010), show that Windows operating system occupies 91.06% market share, Macintosh operating system occupies 4.91% and Linux occupies 0.85%. Due to the low market share of Macintosh compared to that of Windows operating system, the probability for Macintosh operating system being estimated is low and the overall accuracy percentage from Macintosh operating system estimation will be small. Then default hop count estimation accuracy of around 90% is expected.

Wang, Jin, and Shin (2007) tested the Internet hop count stability over three months in year 2003 for 10,000 routes to 113 sites with 95% stable. As the scale, depth and duration of the Internet stability test in the thesis is smaller than the test conducted by Wang et al. (2007), above 95% of Internet stability is expected in the experiment.

The hop count distance method is used for tracing back to the source when the source IP address of the packet is spoofed. However, it only represents the logical aspect of the whole traceback process. To get a complete view on the traceback process, from the victim to the physical location of the suspect, other data related to the physical traceback has also been collected during the research. These data include the properties of the testing location and the surveillance camera installed at the testing location.

3.5 DATA

To test the functionality and accuracy of the model, emails from nineteen testing locations have been sent across the Internet and are collected by the email server in the laboratory. The corresponding hop count distance of these emails is calculated by the model and compared to the actual hop count value to test for the functionality of the hop count distance method.

Emails have also been sent by different operating systems to test for the default hop count estimation accuracy. Emails at different intervals have been sent to test for the hop count stability during the research.

3.5.1 Data Collection

To collect data for processing and analysis, an email server (Axigen) named mailserver1 has been set up to receive emails from various clients through the Internet. The email server is installed with packet capturing software (Wireshark).

Email client software (Mozilla Thunderbird) is installed on the email server, and on the client computers in the test locations for email communication.

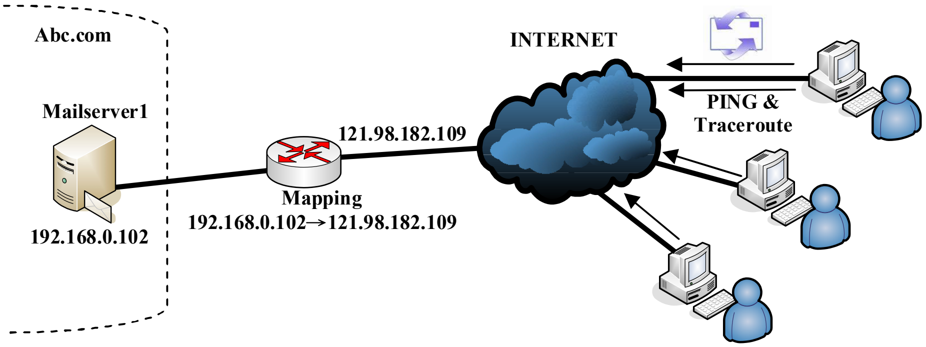


Figure 3.5: Testing Network

As shown in figure 3.5, the email server with the virtual IP address 192.168.0.102 must establish a NAT mapping to the public IP address 121.98.182.109 assigned by the ISP. The ADSL router is configured to allow the inbound SMTP traffic from the Internet.

An email account named John within the domain named abc.com is configured on the email server. The email client software on the client computer has user account name John set up and its SMTP and POP3 settings point to the public IP address on the router. The email client software on the email server also has user account name John set up and points to mailserver1 for SMTP and POP3 settings.

Packet capturing software Wireshark runs on the email server and is configured to capture only email packets. In each testing location, eight emails are sent through different intervals. Also, ping and tracert are run along the communication path to the router with IP address 121.98.182.109 within different intervals. The interval between successive tests are 1 minute, 2 minutes, 4 minutes, 8 minutes, 15 minutes, 30 minutes and 60 minutes. Data is collected at the same location on three different days to test the Internet hop count stability for a wider scope. Tracert and ping information is embedded into email's content to help identify the individual emails.

3.5.2 Data Processing

Once data is collected, the packet's TTL value is extracted and checked against the TTL validation block to ensure the TTL value is within the valid range or the default hop count value has been modified to the point that the hop count distance method cannot be applied. Afterwards, the passive fingerprinting tool (p0f) will be used on the information recorded by the packet-capturing software and the type of the corresponding operating system will be estimated. The default hop count value of the estimated operating system will be looked up.

If the operating system estimation returns an unknown result, then the packet TTL estimation is used on the TTL field of the IP packet to estimate the default hop count value. Finally, the final hop count value of the packets is retrieved from the packet-capturing software record and the hop count distance is calculated.

The hop count stability within a day is calculated by choosing the most frequent hop count value as a Standard Hop Count (SHC) along the path. Then all hop count values for all intervals as Total Hop Count (THC) are added and calculated by the following formula.

$$\text{Hop count stability} = 1 - \left| \text{THC}/(7 \times \text{SHC}) - 1 \right| \times 100\% \qquad \text{Formula 3.1}$$

The hop count stability for the three-day experiment is calculated by multiplying the individual hop count stability for each day, adding them up and then dividing the sum by 3. The count hop variation each day is calculated by applying the standard deviation formula on the hop count in different intervals. The hop count variation across different days is calculated by multiplying the individual standard deviation each day within the period of time, adding them up and then dividing by 3 – the total number of days. The average hop count diameter is calculated by averaging the SHC in individual testing paths.

The percentage of hop count change within the same interval across different days is calculated by counting the number of hop count change in the same interval across different days and divided by the total number of times the test is conducted on the same path. The minimum, average and maximum validation period of hop count distance method is calculated from the data collected from the tracert command.

The minimum validation time for the hop count distance method is calculated as the minimum number of days for successive testing. The maximum validation time for hop count distance method is calculated as the difference between the first and last testing days among all testing locations. The average validation time for hop count distance method is calculated by first calculating the average validation day at each location, then averaging over all nineteen locations. Tracert data from the same testing location is compared and examined for any differences. Tracert data from different testing locations is linked together with the email server mailserver1 at the centre to show the Internet hop count distribution. .

The other traceback data collected from the Internet café including the surveillance camera, their corresponding video record and storage duration is processed as a percentage among all nineteen testing locations.

3.5.3 Data Analysis

The actual default hop count values obtained at the testing locations by the ping command is compared with the expected default hop count values assigned by the operating systems to test for hypothesis 1. Also, the estimated default hop count values are compared with the actual default hop count values and the accuracy is calculated to test hypothesis 2, 3 and 4. The eight tracert and ping test results from each testing day and across all three testing days will be compared to test hypothesis 5, 6, 7 and 8.

Then the default hop count estimation accuracy and the Internet hop count stability are calculated. Finally, the estimated hop count distances are calculated and compared with the actual hop count distances to obtain the accuracy of hop count distance method. The minimum, average and maximum validation day are used to define the minimum, average and maximum day that the hop count distance method will be valid for.

Both hop count stability and variation within a day reveal how accurate the hop count distance method can be within a day. Hop count stability and hop count variation across different days reveal how accurate the hop count distance method is over a longer period of time. The average hop count diameter reveals the size and depth of the research. Tracert data can be used to test the consistency of the path and to show the depth of the test in tree format. The percentage of hop count change within the same interval across different days reveals in which interval or under what time the hop count distance method becomes most effective and provides the best accuracy.

Surveillance camera related data is used to estimate the probability of successful traceback of the physical location and to indicate whether the hop count distance method can be used in conjunction with the physical traceback mechanisms or not.

3.5.4 Data Presentation

Testing locations geographic distribution and Internet distribution are presented as a graph for better understanding on how testing locations are distributed around the email server. Then number of hop count versus number of locations is presented in a table for easy comparison.

Hop count versus physical distance are shown in a bar chart for better comparison on how hop count changes with distance. Another table is used to shown the relationship between hop count and distance per hop to identify the change of distance per hop according to the hop count.

Internet hop count stability at all locations for three days is presented as a table and hop count distance accuracy is presented in a bar chart.

Percentage of surveillance camera installed and record keeping at testing locations are presented in a pie chart. Finally, the record keeping duration is presented as a bar chart.

3.6 LIMITATIONS OF THE RESEARCH

In this research, there are three categories of factors limiting the usage of the hop count distance method. The first category is related to the nature of connection between attacker and victim. The hop count distance method can only be used when the offender has a direct connection to the victim. If the offender uses a proxy or other email servers to send emails, the hop count distance method will not be able to analyse the hop count distance between the source and destination.

The operation of the hop count distance method depends heavily on the default hop count value of the packet. If the value has been altered by the application or by the user, the accuracy of the hop count distance method will be affected. The method relies on the packet's properties such as windows size, maximum segment size and the 'don't fragment' flag to estimate the original operating system that sent the packet. If these values have been artificially altered, the hop count distance method accuracy will also be affected.

The second category is related to the nature of the Internet. Because the core of the hop count distance method relies on the hop count to determine the distance between source and destination, if the Internet hop count stability between the source and destination varies, the accuracy of hop count distance method decreases accordingly.

The third category of limitations is related to the experimental restrictions. The hop count distance method can only be tested on nineteen testing locations in the experiment. As the mail exchanger (MX) record of the email server used in the laboratory has not been registered in the Internet Root DNS server, it is not possible to allow other Internet users to send their emails and to conduct a more diverse experiment for data collection. So, the accuracy of the hop count distance method obtained in the laboratory experiment may be different from the accuracy of the method once it is applied to the real world and this limits the depth of the research. Moreover, since the experiment is only conducted in the Auckland region of New Zealand, the results may only reflect the situation in this particular region of New

Zealand. Hence, applying the hop count distance method to other regions in New Zealand or even other countries may yield different outcomes.

3.7 CONCLUSION

The packet TTL field plays an important role in the hop count distance method since the method depends on the TTL field to trace back the origin when the source IP address is spoofed. It is different from traditional IP traceback mechanisms described in chapter 2 section 2.2.4. Therefore, the testing methodologies described in five different publications are related to the hop count distance method are reviewed in section 3.1. The testing methods, factors considered and the software or hardware used for testing as described in these publications are taken into consideration for constructing the testing framework of the hop count distance method.

The main concern with the hop count distance method is its accuracy. A data map of the hop count distance method is constructed to show the relationship between the accuracy and the corresponding uncertainties and the hypotheses associated with the uncertainties. Two uncertainties with eight hypotheses are associated with the issue of the accuracy.

Finally, the testing framework for testing the hop count distance method is constructed. Results of hop count estimation of about 90% and Internet hop count stability of above 95% are expected from the experiment. The data collection process is designed to collect data from 19 testing stations installed with an email client (thunderbird). The server was installed with email server software (Axigen) and the packet capturing tool (Wireshark). The operating system estimation data is processed by the passive fingerprinting software p0f.

The hop count distance method has some limitations, for example it is unable to trace back an indirect connection. Altering the packet's parameters such as default hop count value and the operating system's signature will affect the accuracy of the hop count distance method. Also, the Internet hop count stability tested on Auckland region may not be reflect accurately the actual situation in the whole of New Zealand or in other countries.

All data collected from the testing framework is presented in chapter 4 as well as processed and analysed data. Finally, analysed data will be presented in different charts, graphs and figures for the discussion in chapter 5.

Chapter Four

REVIEW OF FINDINGS

4.0 INTRODUCTION

Chapter 3 explains how the testing framework for the hop count distance method is set up with an email server to collect data for analysis from nineteen different locations. The testing took about a month to complete with stations located in the range from 250 metres to 189 kilometres. The hop counts ranged from three hops to ten hops from the email server. These locations were further grouped into different areas to analyse the relationship between hop count and the actual distance. There were seven testing stations located in Auckland City.

Section 4.1 discusses the differences between the designed data collection and the actual data collection processes. Although it is not possible to simulate an actual attack on these testing locations, it is possible to examine the environment in which the attacker may launch their attack and the kinds of restrictions and/or difficulties they may face when launching their attacks from the testing locations.

Section 4.2 shows all the findings related to the testing stations and these results are further grouped under Internet hop count stability and operating system estimation. Section 4.3, summarises and analyses the collected data. The data is presented in different ways in section 4.4. Some conclusions are presented in section 4.5. All raw data is presented in Appendices A, B and C.

4.1 VARIATION BETWEEN DESIGN & ACUTAL PROCESS DURING THE DATA COLLECTION PHASE

Although attackers may launch their attack from different locations throughout the whole country, such as any public locations with wireless connection to the Internet or from home, Internet cafés were chosen for the testing locations.

The hypothesis was that Internet cafés only provided computers with Windows operating system installed. In fact computers in all nineteen Internet cafés used for the experiment were only installed with Windows operating system.

Some of the Internet cafés were operated by people from different countries such as Korea, India or China and the operating system being used was the version designed specifically for their own country; hence they had different settings from the English version. Moreover, some of the operating systems used may even be pirate versions and the packet signature from the operating system may be different from the genuine operating system, hence would affect the operating system estimation. In order to test the operating system estimation on Linux, different kinds of Linux bootable CD were used to start up computers in the Internet cafés.

Another issue with Internet cafés is their different policies that regulate how their clients use the computers to access the Internet. Some of the Internet cafés do not allow their clients to download programs from the Internet, others may prevent clients from running special programs such as command prompt and some even do not provide CD-ROM and/or USB slots for clients to use.

Most of the Internet cafés equipped with surveillance camera and the video being captured has been kept for reviewed. These can help the investigator to further track down the suspect. The operating hours of the Internet cafés also provided valuable information for the investigator to trace the possible locations of the suspect. Combined with the attacking packet's timestamp, the information about operating hours of the Internet cafes can help the investigator to filter out the unlikely locations for the attacks.

4.2 FINDINGS

Nineteen testing locations were selected and their names, hop count, physical distance and direction to the email server are listed in table 4.1. The Internet cafés hop count value ranges from 3 to 10 and the distance ranges from 250m to 189km distributed around the email server from east, west, north-west, south and south-west.

Three locations were located in the eastern and Newmarket district, seven locations were located in Auckland CBD, two locations were located in Henderson and one location was located in Mt. Albert, Glen Innes, Otara and Rotorua.

Table 4.1: Testing Locations Name, Hop Count and Physical Distance

Testing locations	Hop count	Distance
Eastern District		
1. MC Internet Highland Park	4	250m (East)
2. Blitz Computer Gaming Arena	3	550m (East)
3. Cyber World	3	625m (East)
Newmarket District		
4. Starzone Internet Café	4	1200m (West)
5. Login 1	7	1200m (West)
6. Galaxy Internet Café	3	1225m (West)
CBD		
7. Big World Internet Café	3	1475m (West)
8. DIC World Internet	3	1400m (West)
9. Net2	4	1425m (West)
10. Mega Web	5	1325m (West)
11. I-Life Zone Internet Café	3	1450m (West)
12. Bros Internet Café	3	1425m (North West)
13. iPlay Internet and game	3	1425m (North West)
Henderson		
14. Web City	5	2775m (West)
15. Manish Café	7	2825m (West)
Mt. Albert		
16. Big World Internet Café (Mt. Albert)	4	1850m (West)
Glen Innes		
17. XY Internet Café	8	375m (North West)
Otara		
18. Sunway Internet Café	9	925m (South)
Rotorua		
19. E-Funz	10	189km (South East)

Internet cafés and their corresponding surveillance camera facilities are listed in table 4.2 that shows whether the Internet café was monitored by surveillance camera or not. A video record is usually kept in the Internet café. Out of the thirteen testing locations that had surveillance cameras installed, twelve would save the camera record for later review. One location keeps the record for at least one week, two keep it for at least two weeks and six keep it for at least one month.

Table 4.2: Internet Café & Surveillance Camera Facilities

Testing locations	Surveillance Camera?	Record?	Keep how long?
1	Yes	Yes	Not sure
2	Yes	Yes	One month
3	Yes	Yes	Two weeks
4	Yes	Yes	Not sure
5	No	-	-
6	Yes	Yes	Forever
7	No	-	-
8	Yes	Not sure	Not sure
9	Yes	Yes	At least one week
10	Yes	Yes	Two weeks
11	No	-	-
12	Yes	Yes	Not sure
13	Yes	Yes	One month
14	No	-	-
15	Yes	Yes	One month
16	No	-	-
17	Yes	Yes	One month
18	No	-	-
19	Yes	Yes	One month

Table 4.3 shows the operating hours of the Internet cafés. Nine locations were opened 24 hours. Other locations have different operating hours.

Table 4.3: Internet Café Operating Hours

Testing locations	Operating hours
1	Mon-Thu: 12pm-10pm, Fri: 12pm-2am, Sat: 10am-2am, Sun: 11am-11pm
2	Mon-Fri: 10am-late, Sat & Sun: 9am-late
3	Mon-Thu: 12pm-12am, Fri: 12pm-late, Sat: 11am-late, Sun: 1pm-11pm
4	24hours
5	Mon-Fri: 9am-9pm, Sat & Sun: 10am-8pm
6	24hours
7	24hours
8	24hours
9	24hours
10	24hours
11	Mon-Fri: 9am-7pm, Sat: 9am-5pm, Sun: closed
12	24hours
13	24hours
14	Mon-Sun: 9am-11pm
15	Mon-Thu: 1pm-10:30pm, Fri & Sat: 10:30am-10:30pm, Sun: 10:30am-9:30pm
16	24hours
17	Mon-Sat: 9:30am-10:00pm, Sun: 12pm-9pm
18	Mon-Sat: 9:30am-6pm, Sun: 9am-5pm
19	Mon-Sat: 10am-10pm, Sun: 10am-8pm

Table 4.4 shows the estimated hop count distance for the unexpected email traffic from other locations on different dates. The two highlighted dates indicated a very high volume (15 times and 126 times) of unexpected email traffic from the same IP address 84.246.224.229.

Table 4.4: Unexpected Email Traffic Hop Count Distance Estimation

Date	Unexpected locations IP address	Operating system estimation by p0f	Default hop count from operating system estimation	Packet TTL	Default hop count estimated from packet TTL	Estimated hop count distance
June 6	123.204.164.114	Windows 2000	128	115	128	13
June 7	219.232.243.172	Unknown	-	45	64	19
June 20	121.34.3.41	Windows 2000	128	111	128	17
June 24	124.217.225.230	Windows 2000	128	114	128	14
June 26	84.246.224.229 x 15	Linux 2.5	64	48	64	16
June 27	121.98.147.136	Unknown	-	61	64	3
June 30	183.7.134.222	Windows 2000	128	112	128	16
July 3	84.246.224.229 x 126	Linux 2.5	64	48	64	16
July 8	183.7.148.138	Windows 2000	128	112	128	16
July 9	120.82.112.106	Windows 2000	128	114	128	14
	124.217.225.230	Windows 2000	128	115	128	13
	183.7.136.80	Windows 2000	128	112	128	16
	183.7.136.252	Windows 2000	128	112	128	16
	114.45.53.31	Windows 2000	128	116	128	12
July 10	123.204.210.78	Windows 2000	128	115	128	13
	120.82.111.31	Windows 2000	128	114	128	14
	183.7.136.252	Windows 2000	128	112	128	16

Table 4.5 shows the IP address to location lookup result. The countries where the IP were assigned are shown in the table.

Table 4.5: Unexpected Email Traffic IP Address to Location Lookup

Locations	Host	Country
120.82.111.31	?	China
219.232.243.172	?	China
121.34.3.41	?	China
183.7.148.138	?	China
120.82.112.106	?	China
183.7.136.80	?	China
183.7.136.252	?	China
121.98.147.136	147-98-121-136.bitstream.orcon.net.nz	New Zealand
124.217.225.230	?	Malaysia
183.7.134.222	?	Brazil
84.246.224.229	?	France
114.45.53.31	114-45-53-31.dynamic.hinet.net	Taiwan
123.204.210.78	123-204-210-78.adsl.dynamic.seed.net.tw	Taiwan
123.204.164.114	123-204-164-114.adsl.dynamic.seed.net.tw	Taiwan

Table 4.6 shows the hop count distance, and the ping test TTL result as well as the estimated hop count distance as presented in table 4.4.

Table 4.6: Hop Count Distance Comparison

Country	Locations	Ping test TTL	Hop	Estimated hop count
Taiwan	123.204.164.114	241	14	13 (-1)
China	219.232.243.172	45	19	19 (0)
China	121.34.3.41	46	18	17 (-1)
Malaysia	124.217.225.230	Timeout	-	13/14
France	84.246.224.229	52	12	16 (+4)
New Zealand	121.98.147.136	62	2	3 (+1)
Brazil	183.7.134.222	111	17	16 (-1)
China	183.7.148.138	Timeout	-	16
China	120.82.112.106	Timeout	-	14
China	183.7.136.80	Timeout	-	16
China	183.7.136.252	Timeout	-	16
Taiwan	114.45.53.31	115	13	12 (-1)
Taiwan	123.204.210.78	Timeout	-	13
China	120.82.111.31	Timeout	-	14

4.2.1 Data for Internet hop count stability test

The email packet's hop count values for all 19 testing locations and for the three testing days are shown in table 4.7. All testing locations have the same final hop count values for all three testing days. The final hop count values range from 60 to 125. Packet TTL tested by the TTL validation block are all valid.

Table 4.7: Packet Hop Count from Testing Locations

Testing locations	Date	TTL	Valid?
1	June 11, 12, 15	124	Yes
2	June 7, 8, 10	61	Yes
3	June 7, 8, 10	125	Yes
4	June 13, 14, 15	124	Yes
5	June 13, 14, 15	121	Yes
6	June 13, 14, 15	61	Yes
7	June 20, 23, 24	61	Yes
8	June 9, 20, 21	125	Yes
9	June 9, 18, 20	124	Yes
10	June 18, 20, 21	123	Yes
11	June 21, 23, 24	125	Yes
12	June 6, 9 16	61	Yes
13	June 6, 9, 18	61	Yes
14	June 25, 27, 28	123	Yes
15	June 25, 27, 28	121	Yes
16	June 25, 27, 28	60	Yes
17	June 18, 19, 26	120	Yes
18	July 7, 10, 12	119	Yes
19	July 8, 9, 10	118	Yes

Tracert results for these locations are listed in table 4.8. When the tracert results are the same for all three testing days, “all” is shown under the Test column. Otherwise, when the individual tests yield different results, the test number is indicated. Sixteen locations have consistent tracert results for all tests on all three days. Two locations have two different tracert results and one location has three different tracert results in the three days for different tests. The locations with different tracert results all have the same hop count along the communication path.

Table 4.8: Packet Tracert Test Results

Locations	Date	Test	Tracert
1	June 11, 12, 15	All	1. 192.168.0.254 2. 192.168.2.254 3. lo1.ras1.nct.orcon.net.nz [60.234.8.201] 4. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
2	June 7, 8, 10	All	1. sx763.dummy.porta.siemens.net [10.1.1.1] 2. lo1.ras1.nct.orcon.net.nz [60.234.8.201] 3.121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
3	June 7, 8, 10	All	1. 10.1.1.1 2. lo1.ras1.nct.orcon.net.nz [60.234.8.201] 3.121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
4	June 13, 14, 15	All	1. 60.234.59.1 2. 60.234.20.213 3. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4.121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
5	June 13 June 14	All All	1. 202.89.47.62 2. atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57] 3. gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132] 4. gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242] 5. orcon2.ape.net.nz [192.203.154.67] 6. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 7. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
	June 15	All	1. 202.89.47.62 2. atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57] 3. gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136] 4. gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246] 5. orcon2.ape.net.nz [192.203.154.67] 6. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 7. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
6	June 13, 14, 15	All	1. 60.234.54.1 2. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 3. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
7	June 20, 23, 24	All	1. 60-234-21-25.bitstream.orcon.net.nz [60.234.21.25] 2. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 3. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
8	June 9, 20, 21	All	1. 60-234-21-81.bitstream.orcon.net.nz [60.234.21.81] 2. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 3.121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
9	June 9, 18, 20	All	1. 60.234.54.129 2. 60-234-21-49.bitstream.orcon.net.nz [60.234.21.49] 3. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4.121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
10	June 18, 20, 21	All	1. 202-169-205-1.linktelecom.co.nz [202.169.205.1] 2. gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11] 3. orcon2.ape.net.nz [192.203.154.67] 4. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 5. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
11	June 21, 23, 24	All	1.sx763.dummy.porta.siemens.net [192.168.2.1] 2. lo1.ras1.nct.orcon.net.nz [60.234.8.201] 3. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
12	June 6 June 9. June 16	1, 5, 8 1, 5, 6, 7, 8 1, 5, 6	1. 60.234.56.254 2. 60.234.56.129 3.121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
	June 6 June 9: June 16:	2, 3, 4 2, 3, 4 2, 3, 4	1. 60.234.56.129 2. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 3. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
	June 6 June 9 June 16	6, 7 - 7, 8	1. 60.234.56.254 2. 60.234.56.129 3. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
13	June 6, 9, 18	All	1. 60-234-21-33.bitstream.orcon.net.nz [60.234.21.33] 2. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 3. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
14	June 25, 27, 28	All	1. 202-169-202-61.linktelecom.co.nz [202.169.202.61] 2. gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11] 3. orcon2.ape.net.nz [192.203.154.67] 4. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 5. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
15	June 25, 27, 28	All	1.mygateway1.ar7 [10.1.1.1] 2. lo1.akl-grafton-bras1.ihug.net [203.109.128.90] 3. gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101] 4. gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]

			5. orcon2.ape.net.nz [192.203.154.67] 6. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 7. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
16	June 25, 27, 28	All	1. 202.68.95.233 2. orcon2.ape.net.nz [192.203.154.67] 3. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
17	June 18, 19, 26	All	1. my.router [192.168.1.1] 2. 10.1.1.1 3. 202.180.81.31 4. vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82] 5. vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49] 6. orcon2.ape.net.nz [192.203.154.67] 7. gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 8. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
18	July 7	All	1. RTA1025W.home [192.168.1.1] 2. lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122] 3. ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65] 4. ggis-gige-v906.telstraclear.net [203.98.18.67] 5. g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49] 6. ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36] 7. orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102] 8. gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6] 9. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
	July 10 July 12	All All	1. RTA1025W.home [192.168.1.1] 2. lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122] 3. ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65] 4. ggis-gige-v906.telstraclear.net [203.98.18.67] 5. g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50] 6. ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36] 7. orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102] 8. gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6] 9. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
19	July 8, 9, 10	All	1. 192.168.1.254 2. 203.97.2.25 3. xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201] 4. ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65] 5. ggis-gige-v906.telstraclear.net [203.98.18.67] 6. g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50] 7. ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36] 8. orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102] 9. gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6] 10. 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]

4.2.2 Data for default hop count estimation

The operating system estimation results obtained from running the program p0f and the actual operating system that was used are shown in table 4.9. It can be seen that out of the nineteen testing locations that all used the Windows XP operating system, only 13 are accurately estimated. The other six are indicated as 'unknown' by p0f. Macintosh and all versions of Linux are indicated as 'unknown', while Schillix OpenSolaris is estimated by p0f as Solaris 10.

Table 4.9: Operating System Estimation Results by P0f

Testing locations	Operating system used	Estimation from p0f	NAT used?
1	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	Yes
2	Windows XP Pro sp3	Unknown	Yes
3	Windows XP Home sp2	Windows XP/2000, Windows 2000 SP2+, XP SP1	Yes
4	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	No
5	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	No
6	Windows XP Pro sp3	Unknown	No
7	Windows XP Pro sp2	Unknown	No
8	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	No
9	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	No
10	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	No
11	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	Yes
12	Windows XP Pro sp3	Unknown	No
13	Windows XP Pro sp3	Unknown	Yes
14	Windows XP Home sp3	Windows 2000 SP4, XP SP1	No
15	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	Yes
16	Windows XP Pro sp3	Unknown	No
17	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	Yes
18	Windows XP Pro sp3	Windows 2000 SP4, XP SP1	Yes
19	Windows XP Pro sp2	Windows 2000 SP4, XP SP1	Yes
Macintosh Computer	Macintosh OSX	Unknown	-
Linux Bootable CD	Ubuntu 10.4	Unknown	-
Linux Bootable CD	Puppy Linux	Unknown	-
Bootable CD	Schillix OpenSolaris	Solaris 10	-
Linux Bootable CD	Helix 3.0	Unknown	-

4.3 ANALYSIS

The default hop count estimation from both operating system and the packet TTL for all locations are presented in table 4.10. It shows the actual default hop count value and whether the estimation was correct or not. Twenty two out of 24 default hop count values were correctly estimated. Macintosh and Schillix OpenSolaris estimations were incorrect. The default hop count value obtained from testing location 2 was not consistent with the actual default hop count value from the result.

Table 4.10: Default Hop Count Estimation

Testing locations	Default hop count	OS estimation	OS estimated default TTL	Packet TTL	Packet TTL estimated default TTL	Correct estimation?
1	128	Windows 2000 SP4, XP SP1	128	124	128	Yes
2	128	Unknown	-	61	64	Yes
3	128	Windows XP/2000, Windows 2000 SP2+, XP SP1	128	125	128	Yes
4	128	Windows 2000 SP4, XP SP1	128	124	128	Yes
5	128	Windows 2000 SP4, XP SP1	128	121	128	Yes
6	64	Unknown	-	61	64	Yes
7	64	Unknown	-	61	64	Yes
8	128	Windows 2000 SP4, XP SP1	128	125	128	Yes
9	128	Windows 2000 SP4, XP SP1	128	124	128	Yes
10	128	Windows 2000 SP4, XP SP1	128	123	128	Yes
11	128	Windows 2000 SP4, XP SP1	128	125	128	Yes
12	64	Unknown	-	61	64	Yes
13	64	Unknown	-	61	64	Yes
14	128	Windows 2000 SP4, XP SP1	128	123	128	Yes
15	128	Windows 2000 SP4, XP SP1	128	121	128	Yes
16	64	Unknown	-	60	64	Yes
17	128	Windows 2000 SP4, XP SP1	128	120	128	Yes
18	128	Windows 2000 SP4, XP SP1	128	119	128	Yes
19	128	Windows 2000 SP4, XP SP1	128	118	128	Yes
Macintosh Computer	60	Unknown	-	56	64	No
Ubuntu 10.4 Linux	64	Unknown	-	61	64	Yes
Puppy Linux	64	Unknown	-	61	64	Yes
Schillix OpenSolaris	64	Solaris 10	255	61	64	No
Helix 3.0	64	Unknown	-	61	64	Yes

The hop count distance calculations for nineteen testing locations are presented in table 4.11. Among the results, 22 out of 24 hop count distance estimation were correctly estimated with hop count distance range from 3 to 10 hops. Two hop count distance estimations results associated with the Macintosh and the Schillix OpenSolaris operating system were incorrect.

Table 4.11: Hop Count Distance Calculation

Testing locations	Default hop count	Estimated default hop count	TTL	Estimated hop count distance	Actual hop count distance
1	128	128	124	4	4
2	128	64	61	3	3
3	128	128	125	3	3
4	128	128	124	4	4
5	128	128	121	7	7
6	64	64	61	3	3
7	64	64	61	3	3
8	128	128	125	3	3
9	128	128	124	4	4
10	128	128	123	5	5
11	128	128	125	3	3
12	64	64	61	3	3
13	64	64	61	3	3
14	128	128	123	5	5
15	128	128	121	7	7
16	64	64	60	4	4
17	128	128	120	8	8
18	128	128	119	9	9
19	128	128	118	10	10
Macintosh Computer	60	64	56	8	4
Ubuntu 10.4 Linux	64	64	61	3	3
Puppy Linux	64	64	61	3	3
Schillix OpenSolaris	64	255	61	194	3
Helix 3.0	64	64	61	3	3

Hop count stability for the nineteen locations over the three days experiments are shown in table 4.12. It shows that the Internet hop count is 100% stable on individual testing days and also across all three testing days for all nineteen testing locations.

Table 4.12: Internet Hop Count Stability

Testing locations	Internet hop count stability		
	First day	Second day	Third day
1	100%	100%	100%
2	100%	100%	100%
3	100%	100%	100%
4	100%	100%	100%
5	100%	100%	100%
6	100%	100%	100%
7	100%	100%	100%
8	100%	100%	100%
9	100%	100%	100%
10	100%	100%	100%
11	100%	100%	100%
12	100%	100%	100%
13	100%	100%	100%
14	100%	100%	100%
15	100%	100%	100%
16	100%	100%	100%
17	100%	100%	100%
18	100%	100%	100%
19	100%	100%	100%

Table 4.13 shows whether the tracert results were consistent on individual testing days and also across the three testing days or not. Also, it indicates whether the same hop count was used when the communication took different routes. Sixteen locations had the same routes on individual and across different testing days. Two locations, location 5 and 18, have inconsistent tracert data over the three testing days. Location 12 doesn't have consistent tracert data either for the individual or over the three testing days. Also, location 2 didn't have the same hop count when different routes were taken.

Table 4.13: Tracert Path Validation

Tracert Data					
Testing locations	**Same routes for all eight tests**			**Same routes across three days**	**Same hop count when routes are different?**
	First day	**Second day**	**Third day**		
1	Yes	Yes	Yes	Yes	-
2	Yes	Yes	Yes	Yes	-
3	Yes	Yes	Yes	Yes	-
4	Yes	Yes	Yes	Yes	-
5	Yes	Yes	Yes	No	Yes
6	Yes	Yes	Yes	Yes	-
7	Yes	Yes	Yes	Yes	-
8	Yes	Yes	Yes	Yes	-
9	Yes	Yes	Yes	Yes	-
10	Yes	Yes	Yes	Yes	-
11	Yes	Yes	Yes	Yes	-
12	No	No	No	No	No
13	Yes	Yes	Yes	Yes	-
14	Yes	Yes	Yes	Yes	-
15	Yes	Yes	Yes	Yes	-
16	Yes	Yes	Yes	Yes	-
17	Yes	Yes	Yes	Yes	-
18	Yes	Yes	Yes	No	Yes
19	Yes	Yes	Yes	Yes	-

The Internet hop count validation period varied. The minimum number of days between the individual tests was 1 day. The maximum number of days between two testing was 11 days. The average number of three days among the testing period is 6 days.

The default hop count accuracy and the hop count distance accuracy are calculated as follows:

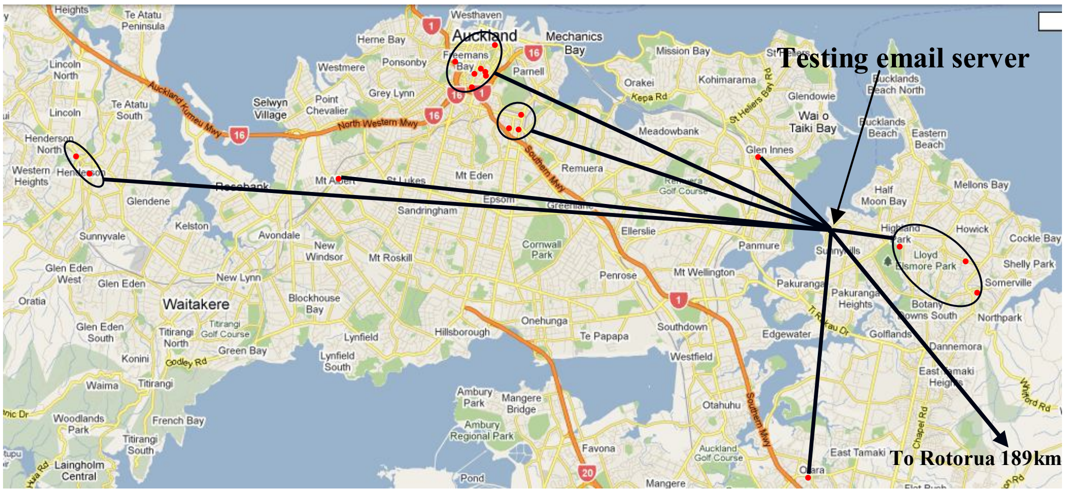
Default hop count accuracy: Number of correct estimation ÷ Total number of estimation x 100%

Default hop count accuracy: (22 ÷ 24) x 100% = 91.7%

Hop count distance accuracy: default hop count accuracy x Internet hop count stability = (0.917 x 1) x 100% = 91.7%

4.4 PRESENTATION OF DATA

The geographic distribution of the testing locations is shown in figure 4.1. Red dots on the map represent the individual testing locations. Black circles represent the grouping of testing locations in different districts. Because testing location 19 is in Rotorua which is about 189km away, it is shown in the bottom right hand corner of the map by a point arrow. Figure 4.1 shows that the testing email server was surrounded by nineteen testing locations all around.



Testing email server

To Rotorua 189km

Figure 4.1: Testing Locations Geographic Distribution

The distribution of the testing locations on the Internet is shown in figure 4.2. Router connections from different testing locations and their corresponging ISP to the email server are shown. All testing locations connect to the ISP of the email server through three routers.

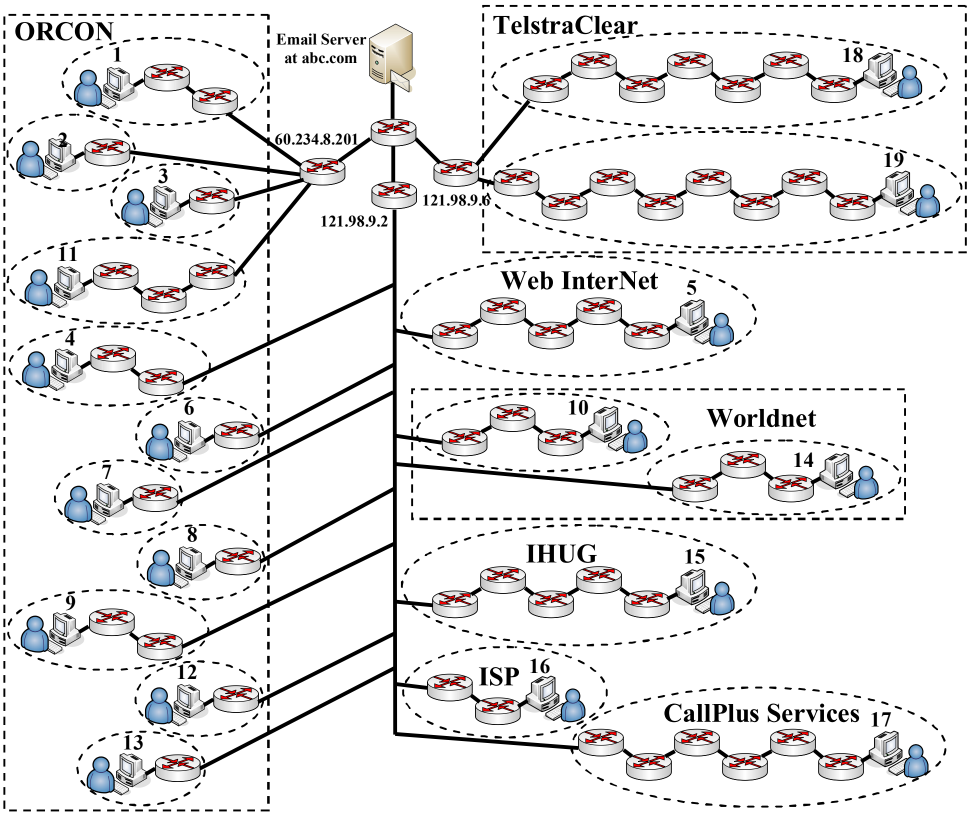


Figure 4.2: Testing Locations Internet Distribution

Table 4.14 summarises the number of hop counts and their corresponding number of locations. For example, seven locations three hops away from the email server.

Table 4.14: Number of Hop Count vs Number of Locations

Number of hops	Number of locations
3	7
4	4
5	3
7	2
8	1
9	1
10	1

Figure 4.3 represents the hop count value of different locations and their corresponding distance. Up to a distance of 1425 metres, the hop count values are randomly distributed. However, for distances longer than 1425 metres, the hop count values increase with the actual distance.

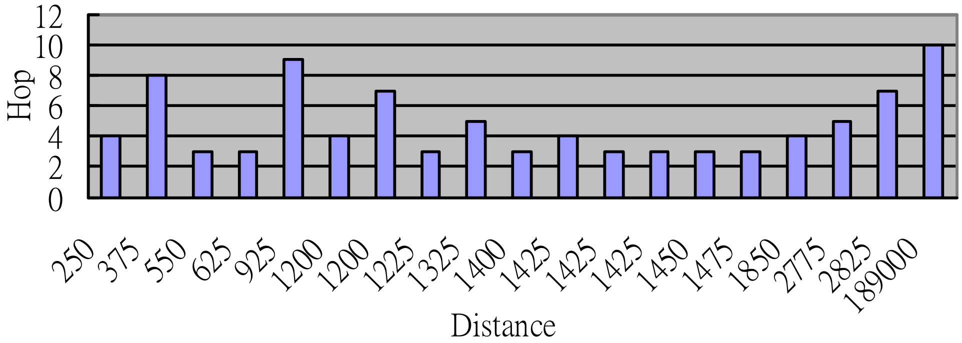


Figure 4.3: Number of Hop Count vs Physical Distance

Table 4.15 shows the number of hops for each testing location and their corresponding distances per hop value. For example, seven locations are three hops away from the email server where the distance per hop ranges from 183.3 to 491.7. To calculate the average distance per hop value, the maximum and the minimum values are excluded and the average distance per hop is found to be 345.3.

Table 4.15: Number of Hop Count vs Distance Per Hop

Testing locations	Hops	Distance per hop
2	3	183.3
3	3	208.3
6	3	408.3
7	3	466.7
8	3	491.7
11	3	475
12	3	475
13	3	483.3
1	4	62.5
4	4	300
9	4	356.3
16	4	462.5
10	5	265
14	5	555
5	7	171.4
15	7	403.6
17	8	46.9 (Min)
18	9	102.8
19	10	18900 (Max)
	Average	345.3

Hop count distance accuracy is shown in Figure 4.4. With the default hop count accuracy of 91.7% and the hop count is 100% stable, the hop count distance accuracy is 91.7%.

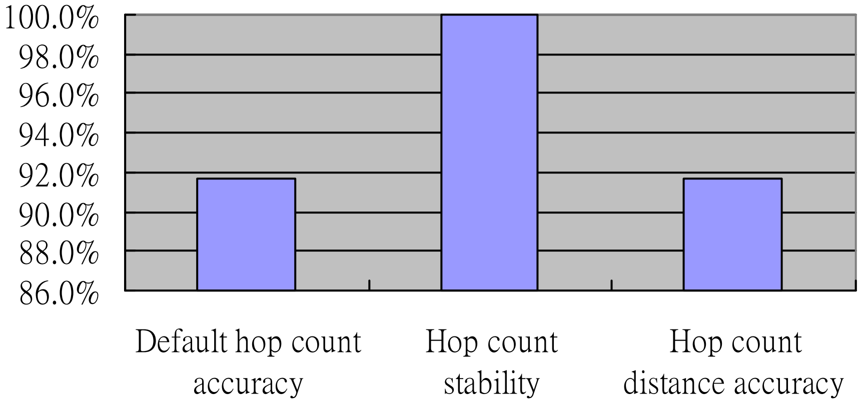


Figure 4.4: Hop Count Distance Accuracy

Figure 4.5 shows the percentage of testing locations with installed surveillance cameras. 68% of Internet cafés had surveillance camera installed and 32% did not.

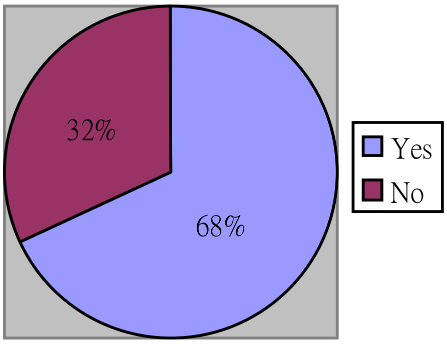


Figure 4.5: Percentage of locations with Surveillance Camera Installed

Figure 4.6 shows the percentage of testing locations that keep surveillance camera record. 63% of Internet cafés keep the record of surveillance cameras for later review and 37% of them do not.

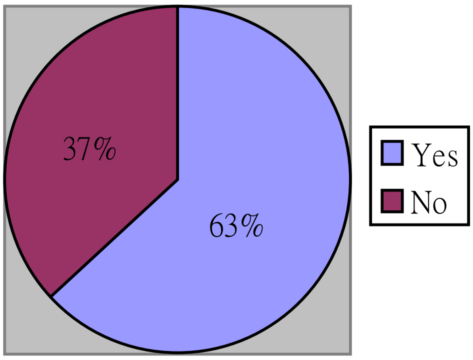


Figure 4.6: Percentage of locations that keep surveillance records

Figure 4.7 shows the surveillance cameras record keeping duration for the testing location. One testing location keeps the record for one week, two locations will keep the record for at least two weeks and six locations will keep the record for more than four weeks.

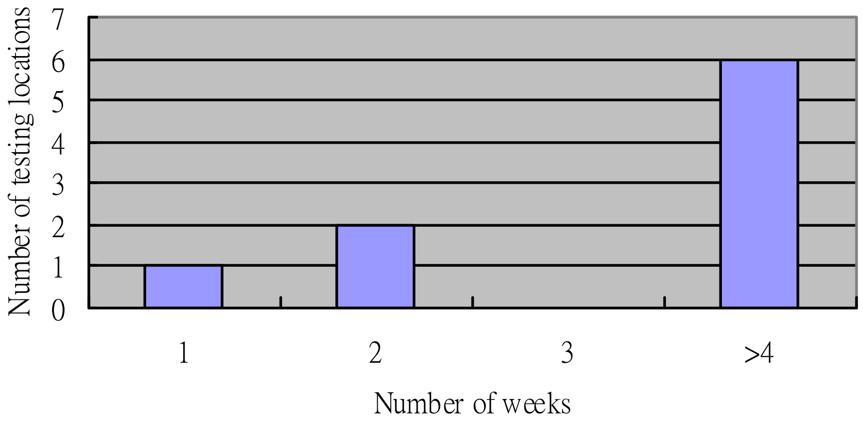


Figure 4.7: Record Keeping Duration

4.5 CONCLUSION

There are some slight differences between the design of the data collection and the actual process. These variations include the operating system that was used, the tools available and the policies of the Internet cafés.

In section 4.2, the actual hop counts and their corresponding distances for the individual testing locations as well as the available surveillance camera facilities at the testing locations are presented.

In section 4.3, the default hop count is estimated and the corresponding hop count distance value is calculated. The Internet hop count is 100% stable and the tracert data verification shows that some email communications may not take the same path every time. The Internet hop count validation period is calculated to be minimum of 1 day, average of 6 days and maximum of 11 days. Finally, the default hop count accuracy and the hop count distance accuracy are calculated as 91.7% and 91.7% respectively.

In section 4.4, map of the physical testing locations and also their corresponding Internet distributions are presented. Other related data such as number of hops versus number of locations is presented in a table format. A bar chart is used to present the hop count versus its corresponding distance. A table also presents the corresponding hop count from different testing locations and the distance per hop value.

Hop count distance stability and hop count distance accuracy are presented in a bar chart. A pie chart is used to present the percentage of testing locations with surveillance cameras and whether the camera record is kept for later review or not. A bar chart is used to show the record keeping duration of testing locations.

The following Chapter 5 discusses the results obtained from the experiment are used to find out how the hop count distance method performs. It also shows and how other collected data can also help in tracing back to the source. The inconsistent results presented in Chapter 4 will are also discussed.

Chapter Five

DISSCUSIONS

5.0 INTRODUCTION

Chapter 4 presents the experimental results related to the operating system estimation, Internet hop count stability and other traceback related evidence. These data are used to test different aspects of the hop count distance method. Chapter 5 uses the collected data to illustrate how the research objective is achieved. Then traceback related data is used to demonstrate how the whole traceback process can be accelerated by considering varied factors associated with the attacking source. Finally, the data related to operating system estimation and Internet hop count stability is used to show different properties of the hop count distance method.

This chapter tests the eight hypotheses by using the experimental results presented in Chapter 4. The two uncertainties related to the hop count distance method are also quantified. Finally, the main question associated with the hop count distance method is answered. The traceback factors related to the attacking source, including the physical location, the operating hours, the attacking tools availability and the monitoring equipment on site are also discussed.

With the achievement of the research objective, any inconsistent data related to default hop count estimation and Internet hop count stability is discussed to discover any restrictions or difficulties that might exist when applying the hop count distance method in the real world. A discussion on the accuracy, limitations, efficiency and the actual usage of the hop count distance method follows. Unexpected SMTP attempted traffic is compared with the experimental results and the differences between them are also discussed.

Section 5.1 shows the achievement of the research objective. Section 5.2 discusses the traceback factors associated with the attacking source. Section 5.3 discusses the different components of the hop count distance method. Section 5.4 discussed the unexpected SMTP attempts on the email server and section 5.5 concludes the chapter.

5.1 RESEARCH OBJECTIVE

The objective of the research is to test the accuracy of the hop count distance method. Accuracy is of crucial importance for this method. Once the accuracy of the method achieves certain level, the functionality and the usage of the method can then be discussed. From the methodology described in chapter 3, the accuracy of the hop count distance method is expected to be at least 90% or above. Since chapter 4 shows how data is collected and presented, this chapter attempts to prove the research objective based on the findings.

From the data map presented in chapter 3 section 3.3, it becomes apparent that the hop count distance method accuracy is restricted by two uncertainties: the default hop count estimation and the Internet hop count stability. Each uncertainty is affected by four hypotheses. Experimental data is used to test the eight hypotheses. Supported by the tested hypothesises, the accuracy of the uncertainties can be calculated. Finally, the hop count distance method accuracy can be worked out after the two uncertainties have been quantified.

Section 5.1.1 shows how the hypotheses are tested by using the experimental data. Section 5.1.2 shows the quantitative results for the two uncertainties and how the research question is answered.

5.1.1 Testing the Hypotheses

The results obtained from testing the eight hypotheses are shown in tables 5.1 to 5.8. Table 5.1 shows that hypothesis 1 is proved and the default hop count value for most operating systems is intact.

Table 5.1: Hypothesis 1 Test

Hypothesis 1: The default hop count value for most operating systems is intact	
All testing locations used Windows XP operating system and the default hop count value assigned by the Windows XP operating system is 128. Macintosh operating system default hop count value is 60. Linux operating system default hop count value is 64. Testing data from chapter 4 table 4.10	
For	Against
For locations 1-5, 8-11, 14-15 and 17-19 the default hop count value is 128. Macintosh and four Linux derived operating systems have the default hop count of 60 and 64 respectively	For locations 6-7, 12-13 and 16 the default hop count value is 64
Summary: Fourteen locations and five different operating systems are tested; the default hop count value for most of the operating systems is intact but at five locations the default hop count value is modified. Hence the hypothesis is proved.	

Table 5.2 shows that the hypothesis 2 is refuted and hence the default hop count estimation accuracy is not affected by the changed default hop count.

Table 5.2: Hypothesis 2 Test

<table>
<tr><td colspan="2">Hypothesis 2: Default hop count estimation accuracy will be affected by default hop count changed</td></tr>
<tr><td colspan="2">Testing data from chapter 4 table 4.10</td></tr>
<tr><td>For</td><td>Against</td></tr>
<tr><td>-</td><td>At all locations the default hop count value estimation is correct. With the incorrect estimation from Macintosh and Schillix OpenSolaris, the default hop count values are intact</td></tr>
<tr><td colspan="2">Summary:
Doesn’t matter if the default hop count value is intact, the estimation is still correct. For the incorrect estimations, the default hop count values are intact. Hence the hypothesis is not proved.</td></tr>
</table>

Table 5.3 explains why the hypothesis 3 is refuted and hence most NATs will not change the default hop count.

Table 5.3: Hypothesis 3 Test

<table>
<tr><td colspan="2">Hypothesis 3: Most NATs will change the default hop count</td></tr>
<tr><td colspan="2">Only locations 1-3, 11, 13, 15, 17-19 used NAT for translation, testing data from chapter 4 table 4.9 and table 4.10</td></tr>
<tr><td>For</td><td>Against</td></tr>
<tr><td>At location 2 NAT changed the default hop count from 128 to 64</td><td>At locations 1, 3, 11, 13, 15, 17-19 NAT didn’t change the default hop count value</td></tr>
<tr><td colspan="2">Summary:
Only at one out of nine locations the default hop count was changed by NAT. Hence the hypothesis is not proved.</td></tr>
</table>

Table 5.4 shows that the hypothesis 4 is refuted and hence NAT will not affect the default hop count estimation accuracy.

Table 5.4: Hypothesis 4 Test

<table>
<tr><td colspan="2">Hypothesis 4: NAT will affect the default hop count estimation accuracy</td></tr>
<tr><td colspan="2">Only locations 1-3, 11, 13, 15, 17-19 used NAT for translation, testing data from chapter 4 table 4.10</td></tr>
<tr><td>For</td><td>Against</td></tr>
<tr><td>-</td><td>The default hop count estimations from all locations with NAT are correct</td></tr>
<tr><td colspan="2">Summary:
At all locations with NAT transaction the default hop count estimations are correct. The hypothesis is not proved.</td></tr>
</table>

Table 5.5 shows that hypothesis 5 is proved and hence most packets that travel between the same source and destination will use the same path.

Table 5.5: Hypothesis 5 Test

<table>
<tr><td colspan="2">Hypothesis 5: Most packets that travel between the same source and destination will use the same path</td></tr>
<tr><td colspan="2">Testing data from chapter 4 table 4.14</td></tr>
<tr><td>For</td><td>Against</td></tr>
<tr><td>Locations 1-4, 6-11, 13-17 and 19 all used the same path for communication between same source and destination</td><td>Locations 5, 12 and 18 used different paths between same source and destination</td></tr>
<tr><td colspan="2">Summary:
Sixteen locations used the same path for communication between same source and destination while only three locations used different paths. Hence the hypothesis is proved.</td></tr>
</table>

Table 5.6 shows that hypothesis 6 is proved and hence the same hop count is maintained between the same source and destination over time.

Table 5.6: Hypothesis 6 Test

<table>
<tr><td colspan="2">Hypothesis 6: Same hop count between same source and destination over time</td></tr>
<tr><td colspan="2">Testing data from chapter 4 table 4.7</td></tr>
<tr><td>For</td><td>Against</td></tr>
<tr><td>All locations have same hop counts between same source and destination over time</td><td>-</td></tr>
<tr><td colspan="2">Summary:
All locations have same hop count between the same source and destination over time. Hence the hypothesis is proved.</td></tr>
</table>

Table 5.7 shows that hypothesis 7 is proved and hence the same hop count exists between the same source and destination on different communication paths.

Table 5.7: Hypothesis 7 Test

<table>
<tr><td colspan="2">Hypothesis 7: Same hop count between same source and destination on different paths</td></tr>
<tr><td colspan="2">Testing data from chapter 4 table 4.14. Only locations 5, 12 and 18 used different paths for communication between same source and destination</td></tr>
<tr><td>For</td><td>Against</td></tr>
<tr><td>Location 5 and 18 have same hop count when different routes were used</td><td>Location 12 has different hop counts across different routes</td></tr>
<tr><td colspan="2">Summary:
Two locations have same hop count between same source and destination on different paths but only one location has different hop count values on different paths. Hence the hypothesis is proved.</td></tr>
</table>

Table 5.8 shows that hypothesis 8 is proved and hence the router along the communication path decrements the packet TTL value by one.

Table 5.8: Hypothesis 8 Test

Hypothesis 8: Router decrements packet TTL value by one	
By comparing the actual hop count decremented data from chapter 4 table 4.7 with the number of routers data from table 4.8	
For	Against
Routers along the communication path between Locations 1-11, 13-19 and the email server decremented the packet TTL value by one	One router along the communication path between location 12 and the email server did not decrement the packet TTL value
Summary: Routers at the eighteen locations decremented the packet TTL value by one but only one location didn't. Hence the hypothesis is proved.	

Once all eight hypotheses are proved, the two uncertainties can be calculated as shown in the next section.

5.1.2 Uncertainties Quantified and the Main Question is Answered

With the support from hypotheses 1 to 4, the first uncertainty related to the default hop count estimation can be calculated as 91.7% as shown in table 5.9.

Table 5.9: Uncertainty 1 Test

Uncertainty 1: The default hop count estimation			
Hypothesis 1	Hypothesis 2	Hypothesis 3	Hypothesis 4
Proved. So, can assume most of the operating systems default hop count value is intact	Not proved. So, can assume the default hop count estimation accuracy will not be affected by changes in the default hop count	Not proved. So, can assume most NAT will not change the default hop count	Not proved. So, can assume NAT will not affect the default hop count estimation accuracy
Summary: With the backup from the proved and unproved hypotheses 1 to 4, the default hop count accuracy can be calculated as 22÷24 x 100% = 91.7%			

With the support from hypotheses 5 to 8, the second uncertainty related to the Internet hop count stability can be calculated as 100% as shown in table 5.10

Table 5.10: Uncertainty 2 Test

<table>
<tr><td colspan="4">Uncertainty 2: The Internet hop count stability</td></tr>
<tr><td>Hypothesis 5</td><td>Hypothesis 6</td><td>Hypothesis 7</td><td>Hypothesis 8</td></tr>
<tr><td>Proved. So, can assume most packets travel between the same source and destination using the same path</td><td>Proved. So, can assume same hop count between the same source and destination over time</td><td>Proved. So, can assume same hop count between the same source and destination on different paths</td><td>Proved. So, can assume routers decrements packet TTL value by one</td></tr>
<tr><td colspan="4">Summary:
With the backup from proved hypotheses 5 to 8, the Internet hop count stability can be worked out from table 4.12 as 100% stable</td></tr>
</table>

After the two uncertainties are quantified, the hop count distance method accuracy can be calculated as 91.7% as shown in table 5.11.

Table 5.11: Main Question Answered

<table>
<tr><td colspan="2">Main question: What is the accuracy of hop count distance method?</td></tr>
<tr><td>Uncertainty 1</td><td>Uncertainty 2</td></tr>
<tr><td>The uncertainty 1 was supported by tested hypotheses 1 to 4 and calculated with the accuracy of 91.7%</td><td>The uncertainty 2 was supported by tested hypotheses 5 to 8 and worked out as 100% stable</td></tr>
<tr><td colspan="2">Summary:
The accuracy of the hop count distance method was determined by the above uncertainties. To work out the correct hop count distance, both the uncertainty 1 and 2 must be considered. The accuracy of the hop count distance method can be calculated as the product from uncertainty 1 and 2. Hence the accuracy is 0.917 x 1 x 100% = 91.7%</td></tr>
</table>

After the achievement of the research objective, a discussion follows below on factors that affect the traceback process and how the achievement of the research objective will affect different aspects of the hop count distance method.

5.2 TRACEBACK EVIDENCE ASSOCIATED WITH THE SOURCE

Most tracebacks involve a long communication path from the victim to the source. The traceback related evidence scattered along the communication path can help narrow down the searching scope of the investigation.

Most of the important evidence is located in the attacking source. By collecting the traceback related data such as the physical location, operating hours, attacking tools availability and monitoring equipments at the location of the attacking source, the information about the suspect can be obtained.

5.2.1 Traceback Evidence: The Physical Location

To collect digital evidence from the physical location, it is important to understand how and why the location was chosen by the attacker to launch the attack. In the experiment, nineteen Internet cafés were chosen to simulate attacking locations in the Auckland area. Although an attacker can attack from any locations with wireless connections, only Internet cafés with wire connection to the Internet were chosen for the experiment.

There are several reasons that the attacker may choose an Internet café to launch an attacks. One of them may be the public nature of the Internet café. Some of the popular Internet cafés may have a couple of hundreds customers every day and the attacker can hide their true identity among those customers. Also, the attacker may think that the investigator can only trace back to the private living location but not to the Internet café.

Another possible reason may be the operating system reload procedure at the Internet cafés. Most Internet cafés will reboot the computer operating system for each new customer and the old data from the previous customer is then erased including the digital evidence. If the attacker launched the attack from home, digital evidence may still reside in the home computer and may be discovered by the investigator.

Wireless Internet connection has its own unique properties and is more difficult to trace back. Therefore, it should be included in another future research. If the hop count distance method works for tracing back Internet café locations, it can still be applied for locations with wireless Internet access. Due to the above reasons, Internet cafés were chosen as the testing locations in the research.

These nineteen locations were carefully chosen and they were distributed around the email server in order to collect data from all directions. Also, these locations covered the distance range from 250 metres to 189 kilometres, an area of about 1.6km^2 and hop count distance from 3 hops to 10hops. With the above coverage, the experiment can provide realistic data to simulate the possible attack locations of the attacker. Furthermore, the relationship between hop count distance and physical distance can be worked out to uncover the approximate physical location of the attacker.

> In 2006, just over 1.3 million people lived in Auckland Region, and it accounted for nearly a third of the New Zealand

> population. The largest population in Auckland Region was concentrated in Auckland City with just over 400,000 or 31% of the regional population (Department of Labour, 2006).

The latest population report from the Department of labour (2006) shows that high concentration of population (31%) were located in Auckland City. and According to Chiesa, Ducci, & Ciappi (2009), 45% of hackers live in large towns and cities, 34% in small towns and 21% in very small towns and villages. Therefore, attackers are more likely to live in high population density area such as Auckland City. Seven out of the nineteen testing locations were chosen in Auckland City.

5.2.1.1 Hop Count Distance versus Physical Distance

The output from the hop count distance method is the hop count distance. How it relates to the physical distance plays an important role on the traceback in physical world. It is reasonable to think that more routers need to be used for communicating over longer distances. In other words, more hops are used for long distance communication.

However, as shown in the hop count versus physical distance figure 4.3, hop count didn't increase with the physical distance. It shows a random distributed pattern when the physical distance is below 1425 metres. For distance longer than 1425 metres, the hop count starts to increase with the physical distance.

The reason that the hop count doesn't increase with the physical distance when it is below 1425 metres may be caused by another router's functionality. Instead for extending the physical distance, a router can also be used to segment a large network. When a network becomes larger, the broadcast traffic can consume a large amount of bandwidth and hence slow down the network. By using a router to segment the network, the broadcast traffic is prevented from passing through the router and hence the broadcast traffic in each network segment is reduced.

Therefore, the whole network performance is increased. Most large ISPs may use routers to segment the network and hence the hop count may be increased even for a short physical distance range. When the physical distance between the communications is larger than 1425 metres, ISPs depend on more routers to extend the physical distance and hence the hop count increases according to the physical distance.

Table 4.15 shows that the average distance per hop was calculated as 345.3 metres. In other words, each hop on average covered the physical distance of 345.3 metres. So, when an error of ± one hop occurs in the hop count distance method, it means that an approximate physical distance error of ± 345.3 metres exists. Hence the physical distance searching scope can be adjusted accordingly.

As indicated in figure 4.2, there are fourteen Internet cafes that are 3 to 5 hops away from the email server. Among them, eleven Internet cafes use the same ISP as the email server. In other words, when the hop count distance is small (3 to 5 hops), there are about 11 out of 14 or 78.6% of chance that the attacker used the same ISP as the victim. Hence the victim's ISP should be the first place where the investigator should start the traceback.

5.2.1.2 Hop Count Distance Distribution

Because the hop count distance method relies on the hop count distance to locate the possible suspect, the hop count distance distribution will affect the efficiency of the hop count distance method and should be studied. Table 4.14 shows that the number of locations decreases with the increase in hop count distance. In other words, there are more locations with lower hop count to the email server.

As shown in figure 4.2, eleven out of nineteen testing locations use the same ISP as the email server. Because the same ISP is used by the testing location and the email server, more locations with lower hop count distances (3 to 5 hops) is expected. Moreover, the experiment is conducted in the Auckland City area with the highest population in the whole country.

A city with high population means high population density and requires more routers to connect people together. Hence a high density low hop count distance distribution in this the area is expected. From the experimental data shown in table 4.14, the hop count distribution density can be worked out and can be used to demonstrate the hop count distance method efficiency in section 5.3.3.1.

5.2.2 Traceback Evidence: Operating Hours of the Internet Cafe

Since Internet cafés were chosen as testing locations, the operating hours of the Internet cafés can provide the investigator with valuable information to trace back the attacker. From the discussion in section 5.1.1, it becomes apparent that there is a has high probability for the attacker to launch the attack from an Internet café and hence the attacking time would be restricted by the operating hours of the

Internet cafe. These may vary from different days to different times in a day. By comparing the attacking packet's timestamp captured during the traceback process with the operating hours, possible locations of the attacker can be narrowed down to fewer places.

If all the Internet cafes are opened for twenty four hours per day and seven days per week, it is not possible to narrow down the investigation scope by the operating hours. However, the experimental data shows that there are nine locations open for twenty four hours per day seven days per week. Other ten locations have different operating hours each day. Hence in this case, there is a 10 ÷19 x 100% or 52.6% chance that the operating hour of the Internet café can be used to further narrow down the location of the suspect.

The log file for computer usage at an Internet café combined with the packet's timestamp can help the investigator to filter the possible computers where the attacker launched the attack. Digital evidence may then be collected from the computer. Furthermore, if the attacker paid by debit or credit card, the transaction time record can also help to narrow down the suspect when the packet timestamp was used. Finally, the packet's timestamp can also be combined with the surveillance camera record to help identify the true identity of the suspect.

5.2.3 Traceback Evidence: Attacking Tools Availability

When an Internet café is chosen as the attacking source by the attacker, some corresponding attacking tools are also necessary. There are two possible ways for the attacker to obtain the attacking tools in an Internet café. One way is by downloading. The attacker can prepare all the attacking tools online from home or other locations and download these tools through the Internet to a computer at the Internet café. Another way is to save these tools on storage devices such as USB flash device, portable hard disk drive or CD/DVD and bring in the tools personally into the Internet café.

By observing the computer usage policies at different Internet cafés, it was found that some of the Internet cafés didn't allow their clients to download files from the Internet. Also, some of the Internet cafes didn't provide USB connections for flash drive or disabled the USB function in the computer. Some of them even remove all CD/DVD devices from the computers.

Due to different computer usage policies from different Internet cafés, the investigator can further narrow down the possible locations or computers where the attacker launched the attack. For example, if an attack was launched from a specific Internet café without flash USB and CD/DVD devices, then the investigator can suspect that the attacker downloaded the tools from the Internet.

By inspecting the log files at the Internet café and the corresponding ISP, the web site or place where the attacker might have visited to download the attacking tools can be worked out and hence these places can be searched further for any digital evidence left by the attacker.

On the other hand, if the Internet café doesn't allow their customers to download files or programs, then most likely the attacker acquired the attacking tools from the flash USB drive, portable hard disk or CD/DVD. From the surveillance camera installed on site, customers who connect a flash USB drive or a portable hard disk to the computer can be identified and this can help to identify the suspect.

5.2.4 Traceback Evidence: Monitoring Equipment

Most of the Internet cafés have installed surveillance cameras to fight crime and also to monitor the computer usage of their customers. Figure ? shows that 68% of Internet cafés have surveillance cameras and 63% of them will keep the record for later review as shown in Figure ?.

With the surveillance camera installed, tracing back to the physical attacker in the Internet café becomes more easily. The investigator can now use the hop count distance method to quickly filter out all the other locations without the matching hop count distance, then the resources for searching can be focused on a much smaller number of locations, thus increase the searching efficiency.

If the attacker was monitored by surveillance cameras, the record combined with log files from the Internet café and the corresponding ISP, can provide more information such as which computer was used to launch the attack, what possible attacking tools were used and sometimes even the identity of the attacker may be identified.

One of the great advantages of the hop count distance method is the speed. Once the attacking packet is captured, the hop count distance between the attacking source and the victim can be worked out within a minute. If the Internet topology around the victim's computer is presented, within an hour, the possible searching scope of suspect's location can be worked out within an hour.

As about 11%, 22% and 44% of Internet café will keep the video record for at least a week, two weeks and four weeks respectively as shown in figure 4.7, combining this with the fast filtering capability of the hop count distance method, there should be enough time for the investigator to locate the suspect from the video recording stored in the Internet café before it is overwritten.

5.2.5 Traceback Evidence: Router Physical Location Tracking

Once the hop count distance method works out the logical routers to which the attacker is possibly connected, the physical location of the routers needs to be identified. To work out the physical location of a router, Internet topology map from the ISP may facilitate the mapping between the logical router and physical location of the router. Although it is hard to acquire the Internet topology of a large area, the first place that the investigator can look for is the victim's ISP.

As described in section 5.1.1, when the hop count distance between the attacking source and the victim is small (3 to 5 hops), the victim and the attacker may have used the same ISP for their Internet connection. Therefore, when the hop count distance between the source and the victim is 3 to 5 hops, it is more effective to focus the searching on the victim's ISP first.

ISP used by the victim can provide useful help to identify the possible source of attack such as the topology map of its own network. In the case of the hop count distance method, once the hop count distance is worked out and sent to the victim's ISP, the hop count distance can be used by the ISP to work out the corresponding point of presence and report it to the investigator. ISP has a lot of routers that interconnect its own network, other networks and its own customers. A point of presence is the router which connects to ISP's customer.

5.2.5.1 Active Search for the Suspect Router by Program

When the attacking source is far away from the victim, in other words, it may reside in another ISP or even another country, it will not be easy to get the topology map from other ISPs connected with the victim's ISP. Also, even if the other ISPs would like to cooperate with the investigator, the whole process may be slow and time consuming. Thus, to work out the possible point of presence using the hop count distance as the input is essential. Programs such as

traceroute can work out all the router(s) along the path between the source and destination.

> If you execute the **traceroute** *ip-address* command on a source device (such as a host, or a router acting as a host), it sends IP packets toward the destination with Time To Live (TTL) values that increment up to the maximum specified hop count. This is 30 by default. Typically, each router in the path towards the destination decrements the TTL field by one unit while it forwards these packets. When a router in the middle of the path finds a packet with TTL = 1, it responds with an Internet Control Message Protocol (ICMP) "time exceeded" message to the source. This message lets the source know that the packet traverses that particular router as a hop (Cisco, 2005).

However, traceroute only takes the destination name or IP address as the input. To work out the possible point of presence from the victim's computer, a program may need to be developed to take the hop count distance as the input and to report all the routers within the hop count distance radius to the victim's computer.

IP2Location Internet IP address 2010 report by IP2Location (2010) shows that New Zealand and the United States own 0.2620% and 37.4607% of all IP addresses respectively. In other words, the size of New Zealand's portion of Internet is much smaller than that of the United States. If only compared the IP address ownership between these two countries, the United State Internet portion is more than one hundred and forty times larger than New Zealand.

The program developed to output all the possible routers by taking the hop count distance as an input may result in huge amount of outputs in a country like the United States with large networks connected to the Internet.

Some properties of the hop count distance method can be introduced to further narrow down the output result. As the method looks for the point of presence which the router(s) is connected to the ISP's customers and most points of presence routers are the leaf routers that are connected to the end of the network, the program can send one more hop testing signal to test whether there is another router behind. If there is no response, then probably there is no router behind and the router that matches the hop count distance to the victim is most likely the point of presence and can be sent as an output.

Another way to narrow down the searching result is introducing more useful information into the program. As shown in figure 4.2 in Chapter 4, the email server was connected to other areas through three different routers in the ISP. If the victim's computer can communicate with the ISP and work out the specific router with specific interface where the attacking traffic came from, then the direction of the attacking source can be worked out.

The ISP can use an IP traceback mechanism (such as input debugging described in section 2.2.4.1.1) to find out which router and which interface the attacking traffic was coming from. With the router and its corresponding interface as the input of the program, the results from the program can be narrowed down significantly.

5.2.5.2 Router Name Mapping

Even the hop count distance method helps the investigator to narrow down the possible point of presence that the attacker connects to, another problem exists, and namely where the physical location is of the point of presence. The point of presence result only gives the investigator the logical router's name that connects to ISP customers. There are several ways to work out the physical locations of the point of presence.

The first one is to contact the corresponding ISP that owns the point of presence. By inspecting the interface's IP address of point of presence and using the IP address locator such as the one from WhatIsMyIPAddress.com, the corresponding ISP and its physical location can be worked out.

Another way to work out the router's physical location and the ISP that it belongs to is by its naming convention. Although there is no standard or regulation on routers' naming and every ISP may name their routers in different ways, valuable location related and ISP specific information may still be retrieved from the logical naming of the router. Most of the ISPs name their routers according to their names, locations, and functionalities. In the case of the ISP Sprint, its own naming convention for a backbone router is:

sl-[bb | gw | dr | st | pe | crs]##-xxx.sprintlink.net

which "##" will be a number, "xxx" will be a city code and "bb", "gw", "dr", "st", "pe" and "crs" are internal codes used to denote the router function.

For example, when the name is sl-bb10-dc it means the router is SprintLink Backbone 10 router located in Washington, DC. Or sl-gw5-fw means the router is SprintLink Gateway 5 router located in Fort Worth, TX. Or sl-crs1-orl means the router is SprintLink Backbone 1 router located in Orlando, FL (Sprint, 2010).

Although the naming convention is not 100% correct and may not denote the physical location of the city where the router resides, it serves as a good source of information of the approximate location of the router and the ISP to which the router belongs.

Due to the cultural differences between countries, the Internet network architecture may vary and further research of the hop count distance method must be performed in other countries to obtain the country specific network information and to derive the most effective way of applying the hop count distance method in or across different countries. Until then, the hop count distance method may still be able to distinguish whether the attacking source is coming from New Zealand or from outside it when the hop count distance from the victim doesn't exceed the border routers that connect New Zealand to the outside world. If the attacking source is found inside New Zealand, searching resources can be used for internal searching or cross countries cooperation needs to be conducted first before the traceback.

To see how accurately and reliably the hop count distance method works in the real Internet testing framework, a discussion is followed in the next section.

5.3 HOP COUNT DISTANCE METHOD

The core components of the hop count distance method are the default hop count estimation and the Internet hop count stability. These two components determine the hop count distance method accuracy and the Internet hop count stability also determines the valid time for the hop count distance method.

5.3.1 Default Hop Count Estimation

To estimate the default hop count value, two methods are used. The first one is the estimation from the packet's TTL field value by using the first power of 2 that is greater than the packet's TTL value. For simplicity in the discussion, the above estimation is named packet TTL estimation.

Before the estimation, the packet's TTL value will be checked against the TTL validation block to ensure the default hop count value has not been changed at the source. An assumption is made to define the valid range of the packet's TTL value by assuming that the maximum hop count that a packet can travel in the Internet is 30 hops.

For the most commonly used default TTL values assigned by the operating system such as 64 and 128, the valid packet's TTL ranges are 34-63 and 98-127 respectively. When the packet's TTL falls outside the above ranges, an error is returned to indicate the default hop count value from the source has been changed. Otherwise, the packet's TTL value is passed as input for default hop count estimation.

From testing hypotheses 1 and 2 as described in section 5.1.1, the default hop count value for most of the operating systems is intact and the default hop count estimation accuracy will not be affected by changes in the default hop count. Hence, checking the packet's TTL value against the TTL validation block can be omitted.

The packet TTL estimation can work out the default hop count values without returning any error. However, the default hop count value that can be estimated is only a power of 2, in other words, the possible default hop count values can only be 2, 4, 8, 16, 32, 64, 128 and 256.

As described in Chapter 3, the default hop count value of Irix, MacOS/MacTCP 2.0x is 60. All Solaris default hop count values are 255. Because the Macintosh and Solaris operating system default hop count values are 60 and 255 respectively, according to the packet TTL estimation, the estimation result for Macintosh and Solaris operating system default hop count value will be 64 and 256 respectively. Hence the default hop count estimation for the Macintosh and Solaris operating systems have to depend on the operating system estimation.

As described in Chapter 3 section 3.3, netmarketshare (2010) statistics show that Windows operating system occupied 91.06% of market share, Mac OS occupied 4.91% and Linux occupied 0.85%. Due to the small market share percentage, the default hop count estimation of Macintosh and other operating systems with minor market share were ignored in the research presented by Wang, Jin, & Shin (2007).

However, improving the hop count estimation accuracy can greatly increase the accuracy of the hop count distance method. So, an extra default hop count estimation method is introduced to estimate the operating system that sends the packet from its packet's signature. Then the operating system is looked up for the corresponding default hop count value. With the operating system estimation introduced, the default hop count value of 30, 255 and even some other values may be estimated.

The downside of the operating system estimation is it can return with Unknown estimation. If the packet's signature cannot match that of any operating system in the database, "unknown" will be returned and the default hop count value can never be worked out. To overcome this limitation, the default hop count value is first examined by the operating system estimation. If the result is unknown, the packet TTL estimation will then be used.

5.3.1.1 Discussion on Changes in Default Hop Count Value

As shown in table 4.10 in Chapter 4, p0f correctly estimated Windows operating system with default hop count value of 128 at thirteen testing locations from locations 1, 3 to 5, 8 to 11, 14 to 15, and 17 to 19. However, p0f failed to estimate the operating system in six testing locations. Except in testing location 2, all other five testing locations, (6, 7, 12, 13, and 16) have the default hop count value of 64.

As mentioned in Chapter 4 section 4.1, the operating system used at all testing locations was Windows operating system that has the default hop count value of 128 instead of 64. It is obvious that the default hop count value of the Windows operating systems have been changed. By checking the packet's TTL validation in table 4.7 for the above five locations, we found that the packet's TTLs were all valid. Due to the "unknown" result from the operating system estimation, the packet TTL estimation was used and correctly estimated the default hop count value.

The reason that the default hop count value was changed to 64 in Windows operating system may be due to some security enhancement. As described by Harris, Harper, Eagle, Ness, & Lester (2005), a passive fingerprinting tool such as p0f is often used by the attacker to discover the operating system of the victim's computer before the actual attack is launched. To enhance the security, the default operating system's attribute such as the default hop count value can be changed to prevent the operating system being estimated by a passive fingerprinting tool.

5.3.1.2 Discussion on Inconsistent Data in Default Hop Count Value

In testing location 2, the default hop count value is 128 but p0f still returns "unknown" for the estimation result. After further inspection on the received packet's TTL value of 61 in location 2, the default hop count value of the operating system in location 2 should be 64 instead of 128.

In order to explain the inconsistent result, the process of getting actual default hop count value from the operating system is reviewed. To get the default hop count value of the operating system, the IP address assigned to the network card is obtained by running the command `ipconfig` under Windows command prompt. Then the `PING` command is used to ping the operating system's IP address and the resulting TTL value is the default hop count value assigned by the operating system.

Several more tests are conducted the same way as described above on different computers running Windows operating system in testing location 2 and the results are all the same as before, the default TTL is 128. From the above results, the possibility that the default hop count value was changed only on the testing computer is eliminated.

The next test is conducted to obtain the public IP address assigned to location 2. Most Internet cafes use the free private IP addresses for their customer's computer and use the public IP address assigned by ISP for Internet access. By using Network Address Translation (NAT) on the Internet café's router, one public IP address rent from ISP can be shared by many customers using private IP addresses.

After visiting the website www.ip2location.com at testing location 2, the public IP address assigned by the ISP to location 2 was obtained. Then the public IP address was ping from the testing computer and the resulting TTL value was 64.

From the above tests, the possible reason for inconsistent data obtained from location 2 can be explained. The operating system used in location 2 is still Windows and the default hop count value assigned is 128. However, when the packet was sent through the Internet café's router to the Internet, NAT operation was performed by the router on the packet. At the same time, the default hop count value of the packet was replaced by the router's default hop count value which is 64. Hence, the receiving packet's TTL value was 61 and the operating system estimation returned "unknown" as a result.

5.3.1.3 Discussion on Macintosh Operating System Estimation Result

An "unknown" result was returned for the Macintosh operating system estimation. Because the result was "unknown", the packet TTL estimation was used to estimate the default hop count value and the result was 64. The default hop count value for the Macintosh operating system used in the experiment is 60, so an incorrect estimation existed.

The version of Macintosh operating system used in the experiment was OS X 10.5.8 and was released on October 2007. Among the series of Macintosh operating systems, starting from Mac OS X 10.1 to 10.6, Mac OS X 10.5.8 is relatively new and the p0f application should be able to identify it. The only reason that p0f failed to recognise the Mac OS X 10.5.8 is some changes in the operating system attributes after the Mac OS X 10.5.8 was used for about three years.

5.3.1.4 Discussion on Linux Variants Estimation Results

All Linux bootable CD variants, Ubuntu 10.4 Linux, Puppy Linux, and Helix 3.0 returned "unknown" results from the operating system estimation. The reason for the "unknown results" may be caused by the nature of the Linux bootable CD variants. All variants can be stored on a bootable CD and a computer can be started in Linux variant operating system from the CD.

In order to put the whole operating system into a CD with a size of only about 700MB and to provide as much functionality as possible, Linux variants were shrunk and trimmed as much as possible. Different shrinking and trimming result in different kind of Linux bootable CD variants with different functionalities. Most of the Linux operating system fingerprints are lost during the shrinking and trimming process and hence the operating system estimation software p0f couldn't recognise these Linux bootable CD variants correctly.

Because the operating system estimation results were "unknown" for the Linux variants, the packet TTL estimation was used to estimate the default hop count value. The packet TTL estimation correctly estimated the default hop count values for all three Linux variants. To improve the operating system estimation test on Linux, different Linux distribution such as Red Hat, Slackware, SuSE, Debian or Fedora should be used. These Linux distributions are not trimmed or shrunk and preserve most of the Linux properties needed for the estimation.

5.3.1.5 Discussion on Schillix OpenSolaris Estimation Result

For the Schillix OpenSolaris bootable CD, a correct operating system estimation result was obtained. It was estimated as Solaris 10 operating system. From Schillix website at schillix.berlios.de it can be seen that Schillix is based on the source code of OpenSolaris and was derived from Solaris 10 operating system, hence it preserves many of its properties. However, instead of using the default hop count value of 255 from Solaris 10, Schillix OpenSolaris uses the default hop count value of 64. Therefore the resulting default hop count value estimation was incorrect. When the packet TTL estimation was used to estimate the default hop count value of Schillix OpenSolaris, a correct result was obtained as shown in table 4.10.

The purpose of introducing the operating system estimation is to increase the default hop count estimation accuracy. However, table 4.10 shows that the packet TTL estimation worked well without the operating system estimation. The accuracy of the default hop count estimation is increased from 91.7% to 95.8% when only packet TTL estimation was used.

P0f only failed to recognise the Windows operating systems when the default hop count values were changed and out of its estimation scope. It could still recognise all thirteen Windows operating systems that had their original default hop count values. Linux variants bootable CDs are also out of the estimation scope of the p0f application. Further tests can still be conducted on other Linux distributions. Only one Macintosh operating system was tested and the result may not be able to accurately reflect the operating system estimation for Macintosh operating systems.

Although the operating system estimation didn’t work on some of the Windows operating systems where the default hop count value was changed to 64, Linux variants bootable CD, Schillix OpenSolaris bootable CD and Macintosh operating system, several examples in (Harris et al., 2005) still show correct estimation on MacOS X 10.2.6, Windows 2000 and Windows XP operating systems. Therefore it is still worthwhile to subject the operating system estimation for further testing.

5.3.2 Internet Hop Count Stability

The Internet hop count stability was tested eight times in seven intervals within two hours at each testing location. The same test was also conducted on three different days at each testing location.

If the Internet hop count changed during the test, different lengths of intervals can show in which interval the hop count has changed most often. The three testing days and times were randomly chosen to cover a wider range of testing periods including the peak and non-peak hours. The expected result for Internet hop count stability is above 95% and the actual result chapter 4 table 4.12 shows that the Internet hop count stability across all three days at all testing locations was 100% stable.

The 100% stable Internet hop count was tested from nineteen testing locations in Auckland that covered an area of 1.6km^2 and hop count distances from 3 hops to 10 hops, all in New Zealand. As described in section 5.1.1, about 31% of New Zealand population is concentrated in Auckland City and about 45% of hackers live in large towns and cities. The research result should be able to closely reflect the actual Internet hop count stability in the Auckland area.

Table 5.12: New Zealand Population Distribution (Source: Census 2006)

Region		Population percentage	
Auckland	Auckland City	31.7%	-
Canterbury	Christchurch	13.3%	66.8%
Wellington	Wellington City	11.4%	40%
Waikato		9.3%	
Bay of Plenty		6.7%	
Manawatu-Wanganui		5.8%	
Otago		5.1%	
Tasman		4.4%	
Northland		4.1%	
Taranaki		3%	
Southland		2.7%	
Gisborne & Hawkes Bay		2.5%	

Table 5.12 shows that although Wellington is the capital of New Zealand and Wellington region has 11.4%, the third large of New Zealand's population, the next research location should be conducted in Christchurch. Among all the regions in New Zealand, Christchurch belongs to Canterbury region and Canterbury region has about 13%, the second large of New Zealand's population

in the area. 66.8% of Canterbury region population is also concentrated in Christchurch and only about 40% of the Wellington region population concentrated in Wellington City. Moreover, since Christchurch is located in the south island of New Zealand, if future research is conducted in Christchurch, the north and the south islands of New Zealand will be covered and a more complete view on how the hop count distance method works in New Zealand could be obtained.

As described in section 5.1.4, the New Zealand portion of Internet network is about hundred and forty times smaller than the United States portion of the Internet network. Therefore, the Internet hop count stability in other countries such as the United States will be expected to be lower than that in New Zealand and must be tested before the hop count distance method can be applied.

5.3.2.1 Hop Count Distance Validation Timeframe

Internet hop count stability not only affects the hop count distance method accuracy but also determines the validation period of the hop count distance method. From chapter 4, it can be seen that the minimum number of days that the hop count distance method can be applied with 100% accuracy is one day because the minimum time between tests was one day. The maximum time between tests was eleven days hence the maximum number of days that the hop count distance method can be applied with 100% Internet hop count stability is eleven days. As the test was conducted on three different days during different period of times, an average time for the hop count distance method to apply with 100% Internet hop count stability is 6 days.

5.3.2.2 Discussion on Different Paths being Used for Communication

Although the hop count on Internet was tested with 100% stability within a short period of time, the actual path being used for communication may not be the same. Different paths used for communication may affect the hop count distance calculation. To understand whether the packet took the same path between the source and destination, the tracert command was used.

Results from tracert command were shown in chapter 4 table 4.13. Sixteen testing locations used the same routes to send data between the source and destination for all eight tests within and across all three days. Locations 5 and 18 used same routes for sending data between the source and destination for all eight tests within the same day but took different routes to send data on each of the three testing days. However, the same hop count value was recorded even when different routes were used for data communication. Only in location 12 did the data traffic use different routes between the source and destination within the same day for different tests and across three testing days. Different hop counts were also observed when data used different routes for communication.

By analysing the data from table 4.8, in the first two days tests from location 5, same route was used for data communication but on the third day different route was used. Different routes were used were for hop 3 and hop 4 along the communication path. On the first and second testing day, data travelled to the hop 3 router with name gi4-15.cr1.alb.maxnet.net.nz and IP address of 123.100.64.132 and hop 4 router with name gi-0-0-0.bdr1.alb.maxnet.net.nz and IP address of 123.100.64.242. On the third testing day, data travelled along the hop 3 router with name gi4-15.cr2.alb.maxnet.net.nz and IP address of 123.100.64.136 and hop 4 router with name gi0-0-1.bdr1.alb.maxnet.net.nz and IP address of 123.100.64.246.

As the name and IP address on hop 3 and hop 4 routers of the first and second testing days are very similar to the name and IP address of the routers on the third testing day, hop 3 and 4 routers most likely belong to the load balancing network along the communication path. Load balancing network balances the load between the source and destination on different paths hence different routes are shown under tracert data with similar name and IP address allocation. Again, in location 18, similar name and IP address pair existed on hop 5 router that most likely belongs to the load balancing network as well.

Among eight different tests on the three testing days at location 12, three different routines with different patterns were used for data communication and the data are shown in table 4.8. As shown in figure 5.1 on the first traffic pattern, tracert data was first sent to the IP address 60.234.56.254, then 60.234.56.129 and finally to the router with IP address 121.98.182.109 to which the email server is connected. Because the default gateway setting in the testing computer was 60.234.56.254, the first router that tracert sent the traffic to should be the router with IP address 60.234.56.254. Then the traffic was redirected to another router in the same subnet with IP address 60.234.56.129 and finally was routed to the destination 121.98.182.109. The first and fifth tests during all three days followed the first traffic pattern.

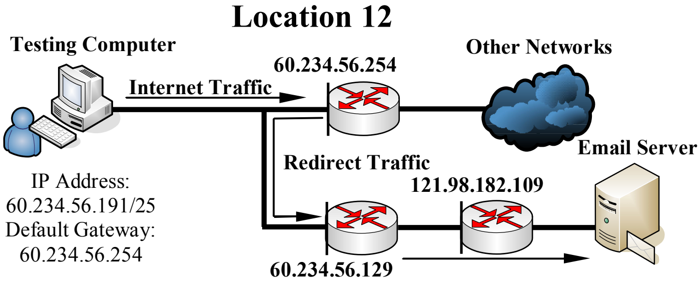


Figure 5.1: Traffic Flow for First Traffic Pattern

As shown in figure 5.2 on the second traffic pattern, traffic was first sent to the router with IP address 60.234.56.129, then was routed through router with IP address 121.98.9.2 and finally to the destination router with IP address 121.98.182.109. The second, third and fourth tests during the three days followed the second traffic pattern.

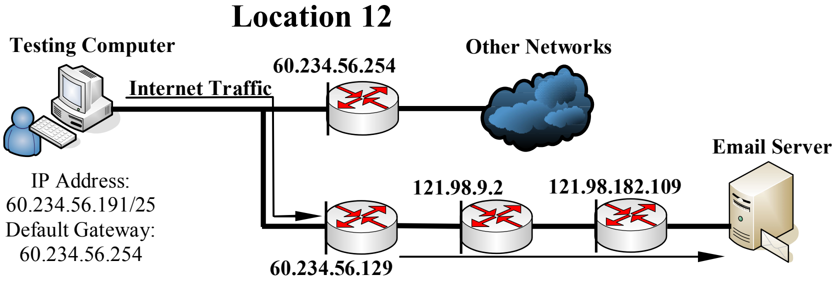


Figure 5.2: Traffic Flow for Second Traffic Pattern

The first and second traffic pattern shows that the testing computer was connected to the network with two routers with IP address 60.234.56.254 and 60.234.56.129 respectively. Router with IP address 60.234.56.129 was connected to the Internet and router with IP address 60.234.56.254 may be connected to some other networks. Because the default gateway setting on the testing computer was 60.234.56.254 and the testing traffic was sent to the Internet, the traffic is sent to router with IP address 60.234.56.254 first and then is redirected to the router with IP address 60.234.56.129.

The reason that the traffic in the second traffic pattern didn't follow the first traffic pattern should be the caching and learning mechanism in the testing computer. The testing interval between test 1 and test 5 was about fifteen minutes. Testing intervals after test 5 were fifteen, thirty and sixty minutes respectively. These testing intervals showed some sort of caching and learning behaviour of the testing computer.

At the first attempt, there was no cached information available and the testing computer had to depend on the default gateway setting to send the Internet traffic. After the first attempt, routing information was cached in the testing computer and it learnt that the shortest path to send Internet traffic was directly through the router with IP address 60.234.56.129. So, the traffic from test 2 to test 4 followed the cache information and sent the Internet traffic directly to the router with IP address 60.234.56.129.

When test 5 was conducted fifteen minutes after the first test had been conducted, the cached information had expired and was erased. Then the testing computer had to send the traffic followed the first traffic pattern again. Hence all test 5, two test 6, one test 7 and two test 8 results also followed the first traffic pattern. Several more tests were conducted and found the caching interval was about ten minutes.

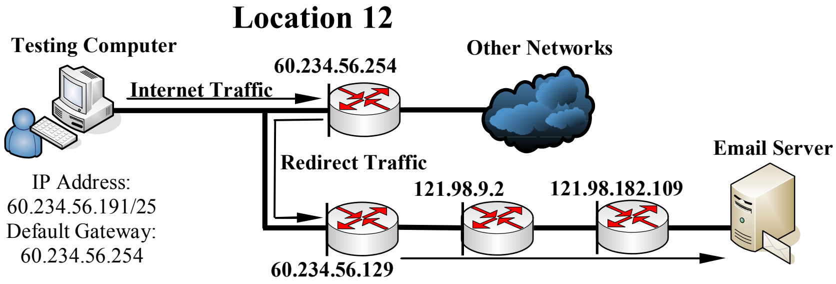


Figure 5.3: Traffic Flow for Third Traffic Pattern

As shown in figure 5.3 on the third traffic pattern, all four routers with IP addresses 60.234.56.254, 60.234.56.129, 121.98.9.2 and 121.98.182.109 were used to route the Internet traffic. One test 6, two test 7 and one test 8 followed the third traffic pattern. As described before, during test 6, 7 and 8 the testing computer had to send the Internet traffic to the router with IP address 60.234.56.254 then the Internet traffic is redirected to the router with IP address

60.234.56.129. However, in the third traffic pattern, traffic was routed through the router with IP address 121.98.9.2 first before being routed by the router 121.98.182.109. The total number of hop count became four.

Table 5.13: Tracert Raw Results Extracted from Appendix C

Date	Test	Tracert Result
June 6	6	1 <1 ms <1 ms <1 ms 60.234.56.254 2 <1 ms <1 ms <1 ms 60.234.56.129 3 1 ms <1 ms 1 ms gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4 34 ms 34 ms 34 ms 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
	7	1 <1 ms <1 ms <1 ms 60.234.56.254 2 <1 ms <1 ms 4294967295 ms 60.234.56.129 3 1 ms 1 ms 1 ms gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4 30 ms 30 ms 33 ms 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
June 16	7	1 8 ms 4294967295 ms <1 ms 60.234.56.254 2 23 ms 2 ms 4294967295 ms 60.234.56.129 3 44 ms 62 ms 6 ms gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4 127 ms 28 ms 29 ms 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
	8	1 4 ms 4 ms 4 ms 60.234.56.254 2 4294967293 ms 4294967293 ms 4294967293 ms 60.234.56.129 3 72 ms 2 ms 4 ms gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2] 4 31 ms 31 ms 29 ms 121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]

By inspecting the raw data records from table 5.13, the processing times for the records on June 6 test 7, June 16 test 7 and June 16 test 8 were abnormal. The records highlighted in table 5.13, show that the processing time on router with IP address 60.234.56.129 reached 4294967295ms. In other words, the router took about 49.7 days to process the packet. The irrational 49.7 days processing time may indicate that latency or error was introduced during packet processing in the router with IP address 60.234.56.129.

Under normal circumstances as shown in first traffic pattern, the traffic redirected from router with IP address 60.234.56.254 to router with IP address 60.234.56.129 will be sent directly to the router with IP address 121.98.182.109 as described before. However, with the unexpected latency or error, it is possible that the routing update information between routers with IP address 60.234.56.254 and 60.234.56.129 was delayed and hence the routing entry points to the router 121.98.9.2 still existed in the routing table of the router with IP address 60.234.56.129. Finally, four hops were being used to route the traffic as shown in the third traffic pattern.

With the load balancing nature, the same hop count on different load balancing routes was used, so in locations 5 and 18 the Internet hop counts were still stable enough for the hop count distance method to work. In location 12, under normal circumstances as shown in the first and second traffic pattern, the caching and learning mechanisms still maintain the same hop count for the hop count distance method to work. When delay or error was introduced to the router, the hop count shown in the result became unstable. However, from the capturing result for twenty four emails as shown in table 4.7, the hop count distance travelled by all these emails from location 12 were three hops. The abnormal result may only have affected the tracert traffic instead of the normal email communication traffic.

5.3.3 Hop Count Distance Method Accuracy, Usage and Efficiency

The hop count distance method accuracy is represented by the product of default hop count estimation accuracy and the Internet hop count stability. From chapter 4 figure 4.4, the default hop count accuracy is 91.7% and the Internet hop count stability is 100%. Then the hop count distance method accuracy is 91.7% and is valid for an average of 6 days.

Again, as the research was conducted in the Auckland area of New Zealand, the 91.7% accuracy will reflect the traceback in the Auckland area. If the method was to be applied in other regions of New Zealand or other countries with similar Internet network portion size as that of New Zealand, the accuracy may still be the same. As described in section 5.2.2, Auckland region has the largest population in New Zealand. When the Internet stability in Auckland region is 100%, it is expected that the other regions with less population can still maintain the same Internet hop count stability.

If the hop count distance method had to be applied in bigger countries such as the United States, the hop count distance method accuracy may be slightly decreased due to the decrease in Internet hop count stability in the United States.

5.3.3.1 Hop Count Distance Method Efficiency

The hop count distance method was used to help the investigator to narrow down the possible locations of the suspect in order to accelerate the traceback process. The power of the hop count distance method is determined by how much irrelevant information can be filtered out. The more irrelevant information can be filtered out by the hop count distance method, the more efficient the hop count distance method is.

The efficiency of the hop count distance method is affected by two factors. First is the hop count distribution of the location where the hop count distance method is applied. It is reasonable to expect that the region with high population will have more routers to connect people together and hence will have higher hop count density than regions with low population. Because routers are unevenly distributed between high population areas such as cities and low population areas such as small towns and the hop count distance depends on the routers to count the distance between the source and destination, the efficiency of the hop count distance method will highly depend on the router distribution.

The second factor is the hop count distance between the victim and the attacking source. Again, due to the uneven distribution of routers, different hop count distances will affect the filtering efficiency. To simplify the discussion, the radius of the hop count distance from the victim to the attacking source was defined as Hop Count Radius or HCR.

The hop count distance method efficiency can be discussed under six different scenarios. In figures 5.4 to 5.9, the red dots indicate the routers. In the city area, router density is higher than the router density in suburbs. The first scenario has the lowest filtering efficiency. In the first scenario, a small HCR exists and the victim is located inside the high hop count density region such as large city or town. Because a large city or town have a high hop count density and small HCR value, it is more possible that hop count distance values exist. Then the filtering efficiency is low.

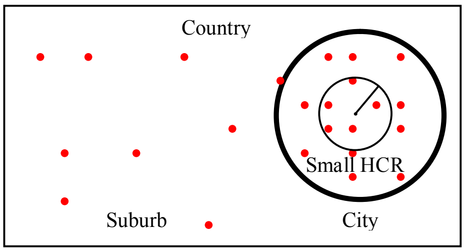


Figure 5.4: Scenario 1

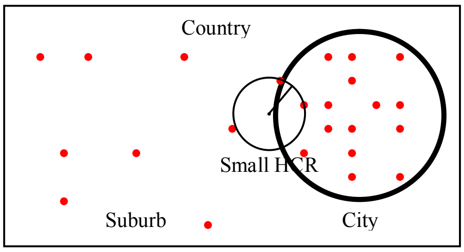


Figure 5.5: Scenario 2

In the second scenario with a small HCR, the victim is located outside but reasonable close to a large city or town. Because the victim is out of the city or town, the number of possible small hop count distances is decreased. Then the filtering efficiency becomes higher than the one in the first scenario.

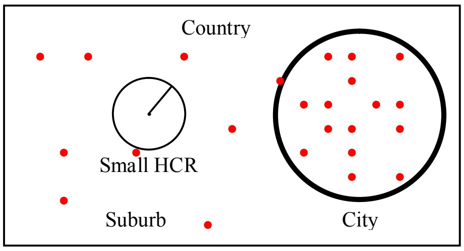


Figure 5.6: Scenario 3

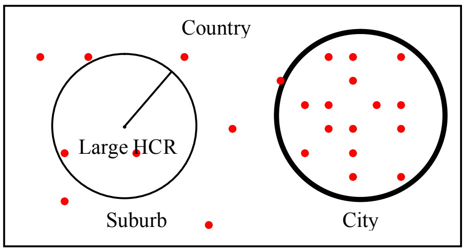


Figure 5.7: Scenario 4

In the third scenario with a small HCR, the victim is located away from a large city or town. Because the victim is located in the region with low hop count density, the hop count distances from the routers in the region to the victim become large. When the HCR is small, the hop count filtering efficiency is higher compared to the first and second scenarios.

In the fourth scenario with a large HCR the victim is located outside and away from the region with high hop count density. In other words, the victim is located in low hop count density region with more hop count distances with large value. Hence, the hop count filtering efficiency is low.

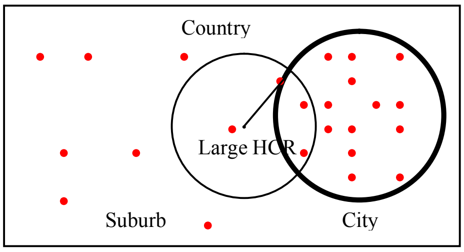


Figure 5.8: Scenario 5

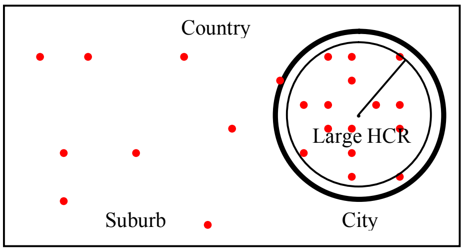


Figure 5.9: Scenario 6

In the fifth scenario with large HCR, the victim is located outside but close to the high hop count density region. Because of the additional smaller hop count distance values established from the high hop count density region, filtering efficiency will be slightly higher than in the fourth scenario.

Finally from the sixth scenario with large HCR value again, the victim is located inside the high hop count density region. Many small hop count distances exist, and the large HCR of the hop count distance can filter out relatively high amount of irrelevant small hop count distances and hence the efficiency will be higher than the one in scenario five.

To illustrate how the hop count distance efficiency work, two examples are shown, one with a small HCR and another one with large a HCR.

When the data from table 4.14 is used in the first scenario with the HCR value of 3 hops, the hop count filtering efficiency can be calculated by dividing the number of filtered locations by the total number of locations in the region. With HCR value of 3 hops, twelve locations were filtered and hence the hop count filtering efficiency will be 12 ÷ 19 x 100% or about 63%.

When the same set of data is applied on the sixth scenario with HCR value of 10 hops, the number of filtered locations is eighteen and hence the hop count filtering efficiency will be 18 ÷ 19 x 100% or about 95%.

The above two examples shows that the efficiency of the hop count distance method can almost be doubled with different values of HCR when applied on the same region. Although experimental data are only taken from nineteen samples, the samples covered an actual distance from 250 metres to 189 kilometres, hop counts from 3 hops to 10 hops and the area of about 1.6km^2. The distribution of hop count density should closely reflect the actual distribution.

5.3.3.2 Hop Count Density Distribution

The hop count density distribution in New Zealand should be proportional to the New Zealand's population distribution. When a region has high density of population, it should also have high density of hop count.

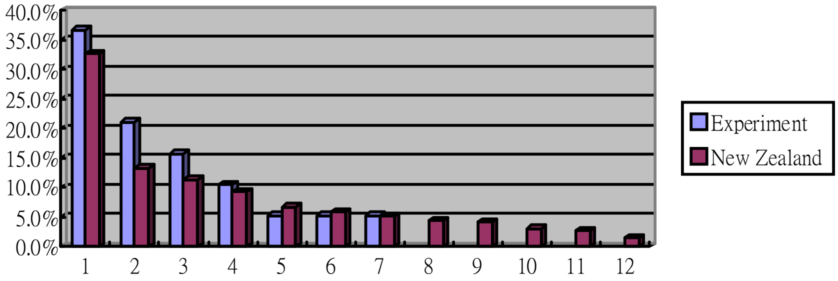


Figure 5.10: Population Distribution in 12 regions of New Zealand & Hop Count Distribution for Experimental Data

As shown in figure 5.10, the population distribution in twelve regions of New Zealand is shown and compared with the hop count density from 3 hops to 10 hops. Figure 5.10 shows that population distribution is closely related to the hop count density distribution.

As the experimental data only includes hop count distance of three to five and seven to ten hops results, five regions cannot be compared and the distribution is not closely matched. If more testing locations were involved with hop count distance of six hops and eleven to fourteen hops, then population distribution from the eighth to twelfth regions can be compared. The hop count density distribution should then closely match the New Zealand's population distribution.

Although the attacking source is unknown to the investigator, by carefully examining the hop count distance method accuracy and the validation period, the hop count distance tested in the Auckland area may still be applied in other countries. The efficiency of the hop count distance method can be worked out when the hop count distribution and HCR are available.

5.3.4 Hop Count Distance Method Limitations

The first limitation that restricts the usage of the hop count distance method is the indirect connection between the attacking source and the victim. Because the hop count distance method depends on the packet's TTL value to determine the location of the attacking source, a direct connection between the source and victim must exist so that the packet's TTL value can reflect the real path travelled by the packet.

In email communication, many intermediate email servers are required to temporary store and send on the email. New packets will be created by the intermediate email servers along the communication path between the source and destination. Therefore, the hop count value obtained from the email packet cannot be used in hop count distance method. To overcome the issue and to apply the hop count distance method to trace back email, the trace back process is divided into two portions. The first portion is from the victim to the email server from which the offender sends the email. As described in chapter 2 section 2.1.3.1, by using the information from the email header, the email server of the offender can be traced back.

When packet capturing software is installed or from the log file of the email server, the attacking packet of the offending email can be captured and the hop count distance method can be applied. Once the hop count distance between the attacking source and victim is worked out, the hop count distance method can filter out the other paths with unmatched hop count value. The searching scope can be narrowed down immediately.

If the attacker uses a proxy server or a stepping stone (Lee & Shields, 2002, p.14) to send email, the hop count distance method can only be able to narrow down the searching scope to the proxy server or to the stepping stone instead of the true attacker.

When the packet signature other than the default hop count value is changed, only the operating system estimation will be affected. As proved in hypotheses 1 and 2 in section 5.1.1, packet TTL estimation is able to work out the default hop count value for the Windows and Linux operating systems.

In case the attacker hides behind a firewall or a router with NAT, the hop count distance method can still trace back to the firewall or router with NAT. As proved in hypotheses 3 and 4 and discussed in section 5.2.1, even when at testing location 2 the default hop count value was changed by the router, if the hop count value is a power of 2, then the hop count distance can still be worked out from the packet TTL estimation.

Although the accuracy of the hop count distance method is affected by the packet's signature, it is not as serious as estimated before. In section 5.2.1, the most commonly used default hop count values of 64 and 128 had the allowable packet's TTL ranges of [34-63] and [98-127] respectively. Even if the default hop count value was changed arbitrarily, when the resulting packet's TTL value still falls within the above allowable ranges, the correct default hop count value is still worked out.

The possible range of TTL values is between 0 and 255. When the default hop count value is 64, once the final packet's TTL falls in the range of [34-63], a correct estimation can be made. The chance for correct estimation with arbitrarily changed default hop count value will then be 30 out of 255 or about 11.8%. For a default hop count value of 128, the chance for correct estimation will be 11.8% as well. The total probability for correct estimation with arbitrarily changed default hop count value when the original default hop count value is either 64 or 128 is then 23.6%.

Another limitation of the hop count distance method is the Internet hop count stability. Although Internet hop count stability has been tested as 100% stable on an average of 6 days in New Zealand, error may still exists during the real implementation of the hop count distance method. Analysing the effect of the hop count distance method on the unstable Internet hop count communication path is essential.

To detect the instability of Internet hop count, the stability of Internet hop count in the region where the hop count distance method is applied should be closely monitored. Most of the time, the Internet hop count is very stable and the instability often occurs for a very short period of time. A couple of days up to a week of monitoring after the attack can provide useful information on Internet hop count stability in the region where the hop count distance method will be applied.

As discussed in section 5.1.1, a one hop difference represents an average actual distance of 345.3 metres. So, if one hop error was detected after the hop count distance method was applied, the physical searching distance error will then be about ±345.3 metres.

As discussed in section 5.2.3, hop count distribution across New Zealand is not the same as in a large city area. The ±345.3 metres error is only based on the average data taken from a high density region, Auckland city. If the victim is located in low hop count density region such as southland or northland in New Zealand, the distance per hop value will be larger and should be worked out in future research.

5.4 DISCUSSION ON THE UNEXPECTED SMTP TRAFFIC

During the data collection phase, the email server received some extra SMTP connection requests from fourteen other unexpected locations and that was captured by the Wireshark. Because the testing email server was not listed under the Mail eXchanger (MX) record of the Internet domain name server, Internet users should not have attempted to establish SMTP connections with the testing email server.

As shown in chapter 2 section 2.1.3.1, the possible reason that these attempts were made is that some Internet users were searching for any available SMTP server to send their email without authentication in order to prevent being traced back. As highlighted in table 4.4, the fact that the location with IP address 84.246.224.229 attempted to establish the SMTP connection fifteen times within two minutes on June 26 and attempted to establish the SMTP connection 126 times within seven minutes on July 3 indicated that a hacking attempt was made on the email server.

P0f estimated twelve out of fourteen (85.7%) of them. As discussed in section 5.3.1, most of them were made from computers with Windows operating system and also some Linux operating system was also estimated. The two unknown results can be estimated by the packet TTL estimation and their default hop count value of 64. The two unknown results with default hop count value of 64 have a high probability to be the Linux variants operating systems as described in section 5.3.1.4. The default hop count from the operating system estimation is consistent with the default hop count estimated from packet TTL estimation. Therefore, there is a high probability that the default hop count was estimated correctly.

Table 4.5 shows the IP address and the corresponding physical locations where the IP address has been assigned. It indicated that seven of the unexpected SMTP attempts came from China, three of them came from Taiwan, and one each was from Malaysia, Brazil, France and New Zealand. In table 4.5, the location with IP address 121.98.147.136 used the ISP namely Orcon Internet the same with the ISP connecting the email server in New Zealand and table 4.4 shows the estimated hop count distance of three hops. The result is consistent with the discussion in section 5.2.1.1 that there are 78.6% that the attacker and victim used the same ISP when the hop count distance is small (3 to 5 hops). The results from table 4.4 and 4.5 also show that when the hop count distance was larger than twelve hops, the SMTP attempts all came from other countries.

Table 4.6 showed the ping test TTL results conducted from the email server back to the unexpected locations. Only seven locations returned positive responses. The other seven locations timed out and five of them were in China. The timeout response may indicate that a dynamic IP address assignment was used during the time of the SMTP attempt. It is also possible that the router or a computer was setup to filter the PING traffic.

Some of the estimated hop count distances from table 4.6 were one hop less than the hop count distance estimated from ping test TTL. The possible reason may be that the sender attempted to establish SMTP connection through a proxy server or stepping stone as explained in section 5.3.4. Some other results showed the estimated hop count distance larger than the hop count distance estimated from ping test TTL. The possible reason is that the computer that made the SMTP attempt was using private IP address behind a router with NAT. So the ping test could only reach the router's public IP address and was not routed through the router as shown in figure 5.11.

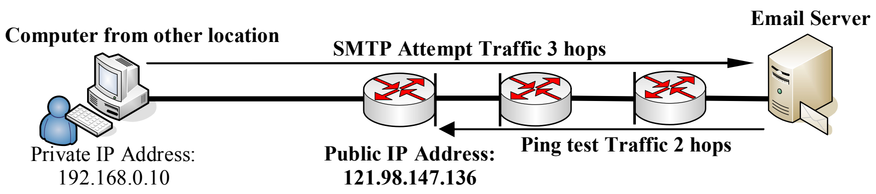


Figure 5.11: Hop Count Distance from Ping Test & SMTP Attempt

An estimated hop count distance that is the same with the hop count distance estimated from ping test TTL may indicate that the computer is assigned with public IP address directly connected to the Internet.

5.5 CONCLUSION

Tracing back to the source location where the attacker launched the attack is the ultimate goal of every traceback method. The Internet cafés chosen as the testing locations in this study were the possible locations where the attacker launched the attack. With carefully chosen testing locations, the distribution of attacking locations and the configurations of each testing location can be examined to acquire more information related to the attacker in order to help the traceback.

Therefore, nineteen locations have been chosen with distance ranging between 250m to 189km, hop count distance from 3 hops to 10 hops and covered a 1.6km^2 of Auckland region area. Since an attacker is more likely to launch their attacks from a large city such as Auckland, seven testing locations were chosen in the Auckland city area.

After about a month of data collection, the data was used to test the eight hypotheses that affected the two uncertainties related to the main question. The main question is to work out the hop count distance method accuracy. When the two uncertainties were quantified, the main question associated with the objective of the research was answered. The hop count distance method accuracy is 91.7%.

The possible traceback evidence that may be related to the source of attack, including the physical location, operating hours of the Internet café, attacking tools availability and the monitoring equipment were discussed. From the physical location, the hop count for distance smaller than 1425 metres was independent to the physical distance.

For distance greater than 1425 metres, the number of hop count increased with the physical distance. When the hop count distance between the source and victim was small (3 to 5 hops), there was about 78.6% chance that the victim and the source used the same ISP. Hence, the investigator can start searching the possible location of the attacker from the same ISP that the victim used.

In the hop count distance method, the attacking time is recorded on the attacking packet's timestamp. When the timestamp is combined with surveillance camera records, customer payment information, log files and the operating hours of an Internet café, the location or even the true identity of the suspect may be identified. The experiment showed that there was about 52.6% chance that the investigator can use the operating hours to further narrow down the scope of investigation.

In order to start an attack from an Internet café, some attacking tools must be brought in by the attacker or downloaded from the Internet. Surveillance cameras may be able to capture the use of these tools through the USB or CDROM device. Otherwise, from the log files at the ISP and the Internet café, the place that the attacker downloaded the attacking tools may be found out and the digital evidence may then be collected.

With 68% of Internet cafés equipped with surveillance cameras and 63% of them keeping the record for later review, the identity of the attacker can be identified. Since the hop count distance method can narrow down the possible locations of the suspect within a couple of days and also about 77% of the Internet café keep their surveillance camera record for at least a week, there should be enough time for the investigator to check the records before they are overwritten.

When trying to acquire the Internet topology around the victim, the victim's ISP should be the first place to look. Future research could develop a program that takes the hop count distance as the input and outputs the possible points of presence locations. Special properties of the Internet such as most of the point of presence routers are leaf routers, can be added in the program to improve its precision and efficiency. Naming conventions from the point of presence routers can provide the investigator with additional information such as the location of the router and the ISP to which the router belongs.

The hop count distance method is the heart of the traceback process. It has accuracy of 91.7% valid for an average of 6 days in the Auckland region. Two components, the default hop count estimation and Internet hop count stability, affected the accuracy of the hop count distance method and the validation period.

There was some inconsistent data for the default hop count estimation at testing locations 2, 6, 7, 12, 13 and 16. The operating system estimation failed to recognise the operating systems at those locations. However, with the packet TTL estimation, the default hop count value from these locations can still be estimated correctly. The operating system estimation also failed to recognise the Linux variants, Macintosh and Schillix OpenSolaris operating systems. Packet TTL estimation can still be able to estimate the default hop count values of Linux variants and Schillix OpenSolaris operating systems but not the Macintosh operating system.

The Internet hop count stability is 100% stable in Auckland region within three testing days. With nineteen testing locations that covered the area of 1.6km^2, the result should closely reflect the actual hop count stability in the Auckland area. According to the population distribution in New Zealand, the next research area for the hop count distance method should be Christchurch as it holds 66.8% of Canterbury population that is the second largest in New Zealand. When applying the hop count distance method to the country with Internet portion much larger than New Zealand, the Internet hop count stability is expected to be slightly lower and further testing would be required to prove the validity of the method.

The inconsistent data in locations 5 and 18 were due to the load balancing nature of the network. The inconsistent data in location 12 was mainly due to the caching and learning mechanism in the testing location network. Also, latency and/or error may be introduced to distort some of the results.

The efficiency of the hop count distance method determines the filtering capability for other irrelevant information and is affected by the hop count distance radius (HCR) and the hop count distribution in the area where the hop count distance method is applied. Six scenarios with different HCR and hop count distribution showed the efficiency of the hop count distance method. An example provided in chapter 4 showed that the efficiency of the hop count distance method can vary between 63% and 95% with different HCRs. The sample data in chapter 4 was not large, only nineteen locations. However, by comparing the hop count distribution of the sample with the population distribution in New Zealand, it becomes apparent that the hop count distribution closely follows the trends of population distribution. Hence the sample of efficiency data should be able to reflect the hop count distance method efficiency in New Zealand.

From the data collected on unexpected SMTP connection attempts it appears that the testing email server was searched for unauthenticated SMTP connection by fourteen other locations. Thirteen locations were from other countries. The unexpected SMTP connection attempted in New Zealand was from the ISP named Orcon Internet which is 3 hops away from the testing email server and the result is consistent with the experimental result.

The hop count distance method is restricted by the direct connection between the source and destination when applying it for email traceback. To overcome the issue, the email header traceback should be first applied to trace back the email server that the attacker used to send email. Then the hop count distance method can be used on the email server to trace back the attacker. In case the attacker used a proxy server or a stepping stone to send the email, the hop count distance method is only able to trace back the proxy server or the stepping stone. For most of the network using NAT, as the tested hypotheses 3 and 4 show the default hop count estimation cannot be affected by the NAT settings. Hence the hop count distance method can still work in the environment with NAT.

The testing of hypotheses 1 and 2 shows that most of the default hop count value for the operating system is intact. In the experiment, even when the default hop count value is changed, the default hop count estimation accuracy is not affected. In case the attacker intends changing the default hop count value arbitrarily, there is still 23.6% chance for correct estimation on default hop count value of 64 and 128 from most of the common operating systems.

Finally, as the experiment was conducted in the Auckland area with high hop count distribution in New Zealand, the ±345.3 metres of physical distance error per hop can only represented the high hop count distribution area in New Zealand. Other areas with different hop count distribution may have hop count distance that is very different to the physical distance error. This would require some additional research to work out the correct hop count to physical distance value.

Chapter Six

CONCLUSIONS

6.0 INTRODUCTION

Chapter 5 discusses different aspects of the hop count distance method. These include how various traceback evidence about the attacking source can be collected and combined with the hop count distance method to accelerate the traceback process. The hop count distance method accuracy is calculated along with the average validation period to show that the research objective has been achieved. There are some limitations associated with the hop count distance method and further research can be conducted to overcome these limitations or to search for suitable areas where the hop count distance method can be applied. An overview for the whole thesis is presented here to review all the work done on the thesis topic.

Chapter 2 shows that in email forensics tracing back to the source has relied on the real source IP address. Without the real source IP address, different complicated and resource consuming IP mechanisms need to be used for traceback. Hence the hop count distance method is proposed to provide a traceback method in email forensics when the source IP address is spoofed.

After reviewing the methodologies presented in five publications, chapter 3 explain the objective of the research. Also, the operation of the hop count distance method was discussed. Then the data map of the hop count distance method was presented to show what data needs to collect. Finally, the construction of the testing framework for data collection was discussed.

After one month of testing and data collection, the outcomes were presented in chapter 4. Chapter 5 discusses various traceback related evidence including the physical location, operating hours, attacking tools availability and monitoring equipment. The hop count distance is also discussed in terms of its accuracy, usage and efficiency. The unexpected SMTP attempted traffic is also compared with the experimental results and the degree of consistency between experimental data and actual data is discussed.

Chapter 6 concludes all the findings in section 6.1 and the research achievements and limitations are presented in section 6.2. Further research is recommended showed in section 6.3 followed by a conclusion.

6.1 SUMMARY OF KEY FINDINGS

Most of the findings of the study are related to the attacking source. The first finding is the relationship between the hop count and the physical distance. In the Auckland city area, the hop count shows a random distributed pattern when the physical distance is less than 1425 metres. For distance greater than 1425 metres, the hop count starts to increase with the physical distance. Also, the average distance per hop in the Auckland city area was found to be 345.3 metres. Moreover, there is a 78.6% chance that the attacking source and victim used the same ISP when the hop count distance is small (3 to 5 hops) in the Auckland city area. The hop count distribution is related proportionally to the population distribution in New Zealand.

Another factor that can help the investigator to find the suspect location is the operating hours of the Internet café. There is about 52.6% chance that the investigator can use the operating hours of the Internet café to determine the possible location of the suspect. The availability of attacking tools in the Internet café can also help to narrow down the searching scope of the investigation. The experimental results show that 68% of the Internet cafés are equipped with surveillance cameras and 63% of them keep the record for later review. Among them, 77% keep the video record from the surveillance cameras for at least one week.

An additional program is required to narrow down the outcomes from the hop count distance method if it is applied in countries with large Internet networks. Router naming can provide help in mapping the digital evidence such as router's location or ISP from virtual to real world.

Six scenarios for the application of the hop count distance method showed how the efficiency varies from one scenario to another. The differences between these scenarios are the size of Hop Count Radius (HCR) as described in section 5.3.3.1 and the hop count distribution of the location where the hop count distance is applied. The example shows that the efficiency of the hop count distance method applied in locations with the same hop count distribution and different HCRs can range from 63% to 95%.

As the hop count distribution affects the hop count distance method efficiency, the hop count distribution in New Zealand is studied from the existing sample data. The hop count distribution is found to closely match the population distribution in New Zealand. So, by studying the population distribution, the hop count distribution can be revealed.

One of the unexpected SMTP connections attempted to the testing email server was in New Zealand. The connection originated 3 hops away from the testing email server and used the same ISP (Orcon Internet) as the email server.

6.2 RESEARCH OBJECTIVE ACHIEVEMENT AND LIMITATIONS

The research objective to find the accuracy of the hop count distance method was achieved with 91.7% accuracy. The valid timeframe for the hop count distance method is minimum one day, maximum of eleven days and an average of 6 days. The hop count distance method was limited by the indirect connection between the attacking source and the victim. When proxy server or stepping stone was used between the attacking source and the victim, hop count distance method can only trace back to the proxy server or stepping stone.

The accuracy of the hop count distance method is affected by the default hop count estimation. When the default hop count value assigned by the operating system is not an exact power of 2, the estimation must rely on the operating system estimation. If the operating system estimation cannot work out the default hop count value, the calculated hop count distance will be incorrect. When the default hop count value assigned by the operating system is intact, the packet TTL estimation can estimate the default hop count value correctly. When the default hop count value is arbitrarily changed, there is still a 23.6% chance that a correct estimation can be made for the most commonly used default hop count values of 64 and 128.

Another factor that affects the hop count distance method accuracy is the Internet hop count stability. If the hop count distance method is applied to a larger country where the Internet network is larger than that of New Zealand, the Internet hop count stability needs to be examined again to work out the accuracy and a valid timeframe.

6.3 FURTHER RESEARCH

As explained in section 6.2, the research objective was achieved for the Auckland city area. Since the Auckland city area has the highest hop count distribution that is proportional to the population distribution in the area, further research should be conducted in areas with low hop count distribution in order to observe how the hop count distance method works there. The result from the low hop count distribution areas may be different and can be used to fine tune the outcomes from the thesis.

The hop count distance method was tested for this study on the wired Internet access network at Internet cafés. With the more common and widely used wireless Internet access connection, future research should be focused on that. The hop count distance method could be applied on attacking sources with wireless access to the Internet. The usability and limitations of the hop count distance method to trace back the wireless Internet connection can then be examined. Some adjustments on the hop count distance method for wireless Internet connections can then be made.

The research was carried out in New Zealand with relatively small Internet network portion when compared to countries such as the United States. To apply the hop count distance method worldwide, it must be first tested in other countries with different usage of the Internet or with different Internet hop count stability. After the hop count distance method is tested in other countries, a cross-countries application can be conducted to test the accuracy, usage, limitations and efficiency of the hop count distance method.

The application of the hop count distance method is not limited to email forensics. In a DoS scenario, if the attacking source has a direct Internet connection to the victim, the hop count distance method can be used to trace back the source when the source IP address is spoofed.

In a DDoS scenario, the attacker distributes the malware to the infected or zombie computers randomly in order to prevent being traced back. However, the malware distribution may not be random due to many factors such as computer usage behaviour of the users, the location of the computers or the anti-virus protection on the computers. When the hop count distance method is applied in the above scenario, the unevenly distributed hop count distance outcomes from different sources may indicate the direction of the attacking source.

For example, if a large number of packets are captured at locations five hops away and only a few packets are captured in other hop count distances, the possible attacking sources are located in the five hops distance radius. Further research need to be conducted to test the accuracy and effectiveness of the hop count distance method for DoS or DDoS traceback.

6.4 CONCLUSION

The hop count distance method provides a fast and simple way to trace back to the source of attacks in email forensics when the source IP address is spoofed. An accuracy of 91.7% with an average valid timeframe of 6 days can provide the investigator with a reliable traceback method for tracing back to the source. The efficiency of the traceback method depends on the HCR and the hop count distribution of the area where the hop count distance method is applied. Variations of HCR and hop count distribution can result in efficiency change from 63% to 95%.

The hop count distance method only provides the core for traceback. By combining the traceback evidence associated with the attacking source, the physical location, the attacking computer or even the actual attacker may be identified.

The hop count distance method usage is limited by the indirect connection between the attacking source and the victim. Also, the default hop count estimation and the Internet hop count stability affect the accuracy of the hop count distance method. The default hop count estimation accuracy is affected by operating system estimation and packet TTL estimation.

An extensive test of the accuracy of the operating system estimation should be conducted. The packet TTL estimation still has a 23.6% of chance to correctly estimate the most commonly used default hop count values of 64 or 128 even though the default hop count value was arbitrarily changed at the source. When applying the hop count distance method in other countries with different size of Internet network, the Internet hop count stability may be different from that in New Zealand and requires further research.

Further research can also be carried out to investigate the application of the hop count distance method in other areas, for examples with wireless Internet connection, DoS or DDoS across different countries.

REFERENCES

Aljifri, H. (2003). *IP traceback: A new denial-of-service deterrent?* Retrieved May 7, 2009 from: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1203219

Baker, F. (1995). *Requirements for IP version 4 routers*. Retrieved 27th May, 2010 from http://www.faqs.org/rfcs/rfc1812.html

Burch, H., & Cheswick, B. (2000). *Tracing anonymous packets to their approximate source*. In Proc. 2000 USENIX LISA Conf., Dec 2000, pp. 319-327

Burns, E. (2006). *New online activities show greatest growth*. Retrieved October 3, 2009 from: http://www.clickz.com/3624155

Census. (2006). *Statistics New Zealand*. Retrieved October 18, 2010 from: http://www.stats.govt.nz/Census/2006CensusHomePage.aspx

Chiesa, R., & Ducci, S., & Ciappi, S. (2009). *Profiling hackers: The science of criminal profiling as applied to the world of hacking*. London: Taylor & Francis.

Cisco. (2005). *Using the traceroute command on operating systems.* Retrieved October 12, 2010 from: http://www.cisco.com/en/US/tech/tk364/technologies_tech_note09186a00801ae32a.shtml

Conseil Européen pour la Recherche Nucléaire (CERN). (2002a). *Email bombing and spamming*. Retrieved April 14, 2010 from: http://www.cert.org/tech_tips/email_bombing_spamming.html

Conseil Européen pour la Recherche Nucléaire (CERN). (2002b). *Spoofed/forged email*. Retrieved April 14, 2010 from: http://www.cert.org/tech_tips/email_spoofing.html

Crowley, P., & Franklin, M. A., & Hadimioglu, H., & Onufryk, P. Z. (2002). *Network processor design, volume 2: Issues and practices*. San Francisco, CA: Morgan Kaufmann.

Department of Labour. (2006). *Labour market reports: annual in-depth regional report – Auckland region*. Retrieved October 12, 2010 from http://www.futureofwork.govt.nz/publications/lmr/regional/indepth/auckland/aidr-auckland-08_04.asp

Devasundaram, S. S. (2006). *Performance evaluation of a TTL-based dynamic marking scheme in IP traceback*. Retrieved May 27, 2010 from http://etd.ohiolink.edu/send-pdf.cgi/Devasundaram%20Shanmuga%20Sundaram.pdf?akron1164051699

Haddad, I. F., & Gordon, D. (2002). *Network simular2 : a simulation tool for Linux*. Retrived October 8, 2010 from http://www.linuxjournal.com/article/5929

Harris, S., & Harper, A., & Eagle, C., & Ness, J., & Lester, M. (2005). *Gray hat hacking: The ethical hacker's handbook*. Emeryville, CA: McGraw-Hill/Osborne.

Internet Crime Complaint Center (IC3). (2009). *IC3 2008 annual report on Internet crime released*. Retrieved October 3, 2009 from: http://www.ic3.gov/media/2009/090331.aspx

IP2Location. (2010). *IP2Location Internet IP address 2010 report.* Retrieved October 10, 2010 from: http://www.ip2location.com/ip2location-internet-ip-address-2010-report.aspx

Izaddoost, A., & Othman, M., & Rasid, M. F. A. (2007). *Accurate ICMP traceback model under DoS/DDoS attack*. Retrieved May 11, 2009 from: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=4426009&isnumber=4425923

Karthik, S., & Arunachalam, V. P., & Ravichandran, T. (2008). A comparitive study of various IP traceback strategies and simulation of IP traceback. *Asian Journal of Information Technology, 7*(10), 454-458. Retrieved September 30, 2009 from: http://docsdrive.com/pdfs/medwelljournals/ajit/2008/454-458.pdf

Lanelli, N., & Hackworth, A. (2005). *Botnets as a vehicle for online crime.* Retrieved April 14, 2010 from: http://www.cert.org/archive/pdf/Botnets.pdf

Lee, H. C. J., & Thing, V. L. L., & Xu, Y., & Ma, M. (2003). *ICMP traceback with cumulative path, an efficient solution for IP traceback*. Retrieved May 11, 2009 from: https://users.cs.jmu.edu/aboutams/Public/IP%20TraceBack/ICMP%20Traceback%20with%20Cumulative%20Path.pdf

Lee, S. C., & Shields, C. (2002). *Technical, legal, and societal challenges to automated attack traceback*. Retrieved May 18, 2009 from https://users.cs.jmu.edu/aboutams/Public/IP%20TraceBack/Technical-%20Legal%20and%20Social%20Chalenges%20to%20Automated%20Attack%20Traceback.pdf

Lemos, R. (2002). *Assault on net servers fails.* Retrieved 18th May, 2009 from http://news.cnet.com/Assault-on-Net-servers-fails/2100-1002_3-963005.html

Microsoft. (2004). *Planning and deploying outlook web access 5.5.* Retrieved October 10, 2010 from: www.microsoft.com/*exchange/techinfo/planning/55/*OWA*55*_Deploy*Plan*.doc

Milletary, J. (2005). *Technical trends in phishing attacks*. Retrieved April 14, 2010 from: http://www.cert.org/archive/pdf/Phishing_trends.pdf

Mirkovic, J., & Dietrich, S., & Dittrich, D., & Reiher, P. (2004). *Internet denial of service attack and defense mechanisms*. Upper Saddle River, NJ: Prentice Hall PTR.

Mirkovic, J., & Wei, S., & Hussain, A., & Wilson, B., & Thomas, R., & Schwab, S., & Fahmy, S., & Chertov, R., & Reiher, P. (2007). *DDoS benchmarks and experimenter's workbench for the DETER testbed.* Retrieved May 27, 2010 from http://www.cs.purdue.edu/homes/fahmy/papers/trident07.pdf

Netmarketshare. (2010). *Operating system market share*. Retrieved October 8, 2010 from http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10

Paxson, V. (2001). *An analysis of using reflectors for distributed denial-of-service attacks*. Retrieved April 14, 2010 from: http://www.icir.org/vern/papers/reflectors.CCR.01/index.html

Pepelnjak, I., & Guichard, J. (2002). *MPLS and VPN architectures: CCIP edition*. Indianapolis, IN: Cisco Press.

Ponec, M., & Giura, P., & Brönnimann, H., & Wein, J. (2007). *Highly efficient techniques for network forensics*. Retrieved May 7, 2009 from: http://isis.poly.edu/~fornet/docs/pubs/ccs097-ponec.pdf

Raven. (2006). *How to trace an email*. Retrieved November 23, 2009 from: http://www.onimoto.com/cache/50.html

Savage, S., & Wetherall, D., & Karlin, A., & Anderson, T. (2001). *Practical network support for IP traceback*. Retrieved May 10, 2009 from: http://www.cs.washington.edu/homes/tom/pubs/traceback.pdf

Schultz, K. (2000). Backtracking e-mail [Electronic version]. *How to hunt spammers*, 8(7), 64-65. Retrieved April 14, 2010 from: http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/g0807/26g07/26g07.asp&guid=

Snoeren, A. C., & Patridge, C., & Sanchez, L. A., & Jones, C. E., & Tchakountio, F., & Kent, S. T., & Strayer, W. T. (2002). *Single-packet IP traceback*. Retrieved May 6, 2009 from: http://cseweb.ucsd.edu/~snoeren/papers/spie-ton.pdf

Song, D. X., & Perrig, A. (2001). *Advanced and authenticated marking schemes for IP traceback*. Retrieved 5th May, 2009 from http://www.cs.berkeley.edu/~dawnsong/papers/iptrace.pdf

Sprint. (2010). *Sprintlink router naming convention*. Retrieved October 15, 2010 from: https://www.sprint.net/index.php?p=faq_namingconvention

Sung, M., & Xu, J. J., & Li, J., & Li, L. E. (2008). Large-scale IP traceback in high-speed Internet. *Practical techniques and information-theoretic foundation*. Retrieved May 15, 2009 from: http://www.cc.gatech.edu/~mhsung/pub/ddos_sp.pdf

Wang, H., & Jin, C., & Shin, K. G. (2007). *Defense against spoofed IP traffic using hop-count filtering*. Retrieved October 1, 2009 from: http://www.cs.wm.edu/~hnw/paper/hcf.pdf

Wu, Y. C., & Tseng, H. R., & Yang, W., & Jan, R. H. (2009). *DDoS detection and traceback with decision tree and grey relational analysis*. Retrieved October 6, 2010 from: http://www.cis.nctu.edu.tw/~wuuyang/papers/DDoS%20Detection%20and%20Traceback.pdf

Zalewski, M., & Stearns, W. (2001). *Passive OS fingerprinting tool version 1.8.2.2*. Retrieved April 5, 2010 from: http://www.stearns.org/p0f/devel/README

Appendix A

PACKET TTL FROM WIRESHARK

Data from iplay Internet & Game			
	TTL		
Email captured	June 6: 60.234.58.80	June 9: 60.234.58.99	June 18: 60.234.58.99
1	61	61	61
2	61	61	61
3	61	61	61
4	61	61	61
5	61	61	61
6	61	61	61
7	61	61	61
8	61	61	61
Data from Cyber World			
	TTL		
Email captured	June 7: 121.98.146.102	June 8 : 121.98.146.102	June 10: 121.98.146.102
1	125	125	125
2	125	125	125
3	125	125	125
4	125	125	125
5	125	125	125
6	125	125	125
7	125	125	125
8	125	125	125
Data from Blitz			
	TTL		
Email captured	June 7: 121.98.147.136	June 8: 121.98.147.136	June 10: 121.98.147.136
1	61	61	61
2	61	61	61
3	61	61	61
4	61	61	61
5	61	61	61
6	61	61	61
7	61	61	61
8	61	61	61
Data from DIC World			
	TTL		
Email captured	June 9: 60.234.47.104	June 20: 60.234.47.104	June 21: 60.234.47.95
1	125	125	125
2	125	125	125
3	125	125	125
4	125	125	125
5	125	125	125
6	125	125	125
7	125	125	125
8	125	125	125

Data from Net2			
	TTL		
Email captured	June 9: 60.234.54.145	June 18: 60.234.54.145	June 20: 60.234.54.145
1	124	124	124
2	124	124	124
3	124	124	124
4	124	124	124
5	124	124	124
6	124	124	124
7	124	124	124
8	124	124	124
Data from Bros			
	TTL		
Email captured	June 6: 60.234.56.190	June 9: 60.234.56.190	June 16: 60.234.56.186
1	61	61	61
2	61	61	61
3	61	61	61
4	61	61	61
5	61	61	61
6	61	61	61
7	61	61	61
8	61	61	61
Data from MC Internet			
	TTL		
Email captured	June 11: 121.98.206.188	June 12: 121.98.206.188	June 15: 121.98.206.188
1	124	124	124
2	124	124	124
3	124	124	124
4	124	124	124
5	124	124	124
6	124	124	124
7	124	124	124
8	124	124	124
Data from Starzone			
	TTL		
Email captured	June 13: 60.234.59.46	June 14: 60.234.59.46	June 15: 60.234.59.46
1	124	124	124
2	124	124	124
3	124	124	124
4	124	124	124
5	124	124	124
6	124	124	124
7	124	124	124
8	124	124	124

Data from Login1			
	TTL		
Email captured	June 13: 202.89.47.16	June14: 202.89.47.23	June 15: 202.89.47.19
1	121	121	121
2	121	121	121
3	121	121	121
4	121	121	121
5	121	121	121
6	121	121	121
7	121	121	121
8	121	121	121

Data from Galaxy			
	TTL		
Email captured	June 13: 60.234.54.20	June 14: 60.234.54.32	June 15: 60.234.54.13
1	61	61	61
2	61	61	61
3	61	61	61
4	61	61	61
5	61	61	61
6	61	61	61
7	61	61	61
8	61	61	61

Data from XY Internet			
	TTL		
Email captured	June 18: 203.100.218.143	June 19: 119.224.26.10	June 26: 203.184.48.74
1	120	120	120
2	120	120	120
3	120	120	120
4	120	120	120
5	120	120	120
6	120	120	120
7	120	120	120
8	120	120	120

Data from Mega Web			
	TTL		
Email captured	June 18: 202.169.205.57	June 20: 202.169.205.55	June 21: 202.169.205.54
1	123	123	123
2	123	123	123
3	123	123	123
4	123	123	123
5	123	123	123
6	123	123	123
7	123	123	123
8	123	123	123

Data from Big World Internet			
	TTL		
Email captured	June 20: 60.234.22.131	June23: 60.234.22.131	June 24: 60.234.22.131
1	61	61	61
2	61	61	61
3	61	61	61
4	61	61	61
5	61	61	61
6	61	61	61
7	61	61	61
8	61	61	61
Data from I-Life Zone Internet			
	TTL		
Email captured	June 21: 121.98.141.16	June 23: 121.98.141.16	June 24: 121.98.141.16
1	125	125	125
2	125	125	125
3	125	125	125
4	125	125	125
5	125	125	125
6	125	125	125
7	125	125	125
8	125	125	125
Data from Big World Albert			
	TTL		
Email captured	June 25: 202.20.6.138	June 27: 202.20.6.138	June 28: 202.20.6.138
1	60	60	60
2	60	60	60
3	60	60	60
4	60	60	60
5	60	60	60
6	60	60	60
7	60	60	60
8	60	60	60
Data from Web City			
	TTL		
Email captured	June 25: 202.169.202.9	June 27: 202.169.202.20	June 28: 202.169.202.20
1	123	123	123
2	123	123	123
3	123	123	123
4	123	123	123
5	123	123	123
6	123	123	123
7	123	123	123
8	123	123	123

Data from Manish-Cafe			
	TTL		
Email captured	June 25: 118.93.29.77	June27: 118.93.29.77	June 28: 118.93.29.77
1	121	121	121
2	121	121	121
3	121	121	121
4	121	121	121
5	121	121	121
6	121	121	121
7	121	121	121
8	121	121	121
Data from Sunway			
	TTL		
Email captured	July 7:121.72.214.93	July 10: 121.72.212.11	July 12: 121.72.163.7
1	119	119	119
2	119	119	119
3	119	119	119
4	119	119	119
5	119	119	119
6	119	119	119
7	119	119	119
8	119	119	119
Data from e-funz			
	TTL		
Email captured	July 8: 203.97.2.26	July 9: 203.97.2.26	July 10: 203.97.2.26
1	118	118	118
2	118	118	118
3	118	118	118
4	118	118	118
5	118	118	118
6	118	118	118
7	118	118	118
8	118	118	118

Appendix B

PING & TRACERT RAW DATA

iPlay Internet & Game – June 6

1.
```
Ethernet adapter Local Area Connection 2:
     Connection-specific DNS Suffix  . :
     IP Address. . . . . . . . . . . . : 192.168.2.10
     Subnet Mask . . . . . . . . . . . : 255.255.255.0
     Default Gateway . . . . . . . . . : 192.168.2.254

Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

  1     1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    35 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2.
```
Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    33 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3.
```
Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    34 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4.
```
Reply from 121.98.182.109: bytes=32 time=708ms TTL=59

  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    30 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5.
```
Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

  1 <1 ms     1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2    59 ms     6 ms     3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    31 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6.
```
Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     3 ms    11 ms     5 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    34 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7.
```
Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    31 ms    32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8.
```
Reply from 121.98.182.109: bytes=32 time=35ms TTL=59

  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

iPlay Internet & Game – June 9

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms    29 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1     6 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    31 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=28ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    37 ms    32 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1     7 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    45 ms    30 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1     2 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    29 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms <1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2    27 ms     1 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

iPlay Internet & Game – June 18

1. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     4 ms     4 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms  1225 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2    20 ms     5 ms     6 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    29 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms     29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     2 ms      2 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms     30 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms     29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3     *        32 ms     32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-33.bitstream.orcon.net.nz [60.234.21.33]
  2     1 ms      1 ms      2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms     29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Bros – June 6

1. Windows IP Configuration

```
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 60.234.56.190
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 60.234.56.254
```

Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2    28 ms <1 ms <1 ms   60.234.56.129
  3     1 ms     33 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.129
  2     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3   298 ms    270 ms    339 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.129
  2     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms     33 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1    51 ms <1 ms <1 ms   60.234.56.129
  2     1 ms      2 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms     29 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms     34 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms <1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms     34 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms   4294967295 ms   60.234.56.129
  3     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms     30 ms     33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms     33 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.2.109]
```

Bros – June 9

1. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
 1 <1 ms <1 ms <1 ms   60.234.56.254
 2 <1 ms <1 ms <1 ms   60.234.56.129
 3 <1 ms     33 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.18.109]
```

2. Reply from 121.98.182.109: bytes=32 time=3762ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.129
  2    47 ms      6 ms      2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms     29 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=247ms TTL=59

```
  1   220 ms   199 ms   269 ms   60.234.56.129
  2   424 ms   359 ms   469 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3   283 ms   339 ms   359 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=409ms TTL=59

```
  1   306 ms   359 ms   359 ms   60.234.56.129
  2   276 ms   179 ms   159 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3   347 ms   449 ms   429 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms     34 ms     33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3    61 ms     30 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms      *        33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=34ms TTL=59

```
  1     3 ms      3 ms      3 ms   60.234.56.254
  2     3 ms      3 ms      3 ms   60.234.56.129
  3     1 ms     35 ms     43 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Bros – June 16

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms     33 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=34ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.129
  2     3 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms     30 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=34ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.129
  2     1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    35 ms     34 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=160ms TTL=59

```
  1     *       162 ms    129 ms   60.234.56.129
  2   106 ms    139 ms    139 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3     *       222 ms      *      121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
  4   232 ms    189 ms    219 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2 <1 ms <1 ms <1 ms   60.234.56.129
  3     4 ms     30 ms     33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60.234.56.254
  2     1 ms <1 ms <1 ms   60.234.56.129
  3     1 ms     34 ms    100 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=219ms TTL=59

```
  1     8 ms   4294967295 ms <1 ms   60.234.56.254
  2    23 ms      2 ms   4294967295 ms   60.234.56.129
  3    44 ms     62 ms      6 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4   127 ms     28 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=27ms TTL=59

```
  1     4 ms      4 ms      4 ms   60.234.56.254
  2   4294967293 ms   4294967293 ms   4294967293 ms   60.234.56.129
  3    72 ms      2 ms      4 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms     31 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Blitz – June 7

1.

```
 Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  . : dummy.porta.siemens.net
    IP Address. . . . . . . . . . . . : 10.1.1.104
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 10.1.1.1
```

Reply from 121.98.182.109: bytes=32 time=46ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    28 ms     92 ms     18 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    46 ms     45 ms     48 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=45ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    16 ms    17 ms    16 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  3206 ms    43 ms    45 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=45ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    17 ms    15 ms    15 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    48 ms    44 ms    44 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=50ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    17 ms    16 ms    15 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    49 ms    50 ms    48 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=45ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    17 ms    17 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    44 ms    49 ms    50 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=43ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    16 ms    18 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    45 ms    44 ms    44 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=47ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    20 ms    25 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    44 ms    44 ms    45 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=42ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [10.1.1.1]
  2    19 ms    50 ms    44 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    49 ms    44 ms    50 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Blitz – June 8

1. Reply from 121.98.182.109: bytes=32 time=135ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    16 ms    17 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    47 ms    45 ms    45 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=43ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    17 ms    16 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    44 ms    45 ms    47 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=42ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    16 ms    19 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    45 ms    47 ms    47 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=55ms TTL=62

```
  1     1 ms <1 ms <1 ms   10.1.1.1
  2    18 ms    19 ms    16 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    46 ms    48 ms    45 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=49ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    17 ms    24 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    45 ms    44 ms    51 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=47ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    36 ms    16 ms    18 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    44 ms    48 ms    45 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=45ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    22 ms    16 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  1273 ms    44 ms    44 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=45ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    15 ms    16 ms    15 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  2531 ms    46 ms    44 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Blitz – June 10

1. Reply from 121.98.182.109: bytes=32 time=46ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    17 ms    19 ms    18 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3     *        50 ms    49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=46ms TTL=62

```
  1 <1 ms     1 ms     1 ms   10.1.1.1
  2    77 ms    72 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    47 ms    48 ms    45 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=72ms TTL=62

```
  1     1 ms <1 ms <1 ms   10.1.1.1
  2    18 ms    17 ms    18 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    46 ms    50 ms    49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=48ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    18 ms    18 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    58 ms    48 ms    46 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=47ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    48 ms    18 ms    17 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    47 ms    50 ms    49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=46ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    19 ms    32 ms    16 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    46 ms    49 ms    49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=49ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    16 ms    23 ms    22 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    49 ms    49 ms    49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=50ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    19 ms     17 ms     19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    47 ms     45 ms     49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Cyber World – June 7

1. Ethernet adapter Local Area Connection:

```
     Connection-specific DNS Suffix   . :
     IP Address. . . . . . . . . . . . : 10.1.1.25
     Subnet Mask . . . . . . . . . . . : 255.0.0.0
     Default Gateway . . . . . . . . . : 121.98.146.102

C:\>ping 121.98.182.109
Reply from 121.98.182.109: bytes=32 time=51ms TTL=62

C:\>tracert 121.98.182.109
  1      2 ms <1 ms <1 ms   10.1.1.1
  2    25 ms     25 ms     24 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms     63 ms     55 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=57ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    28 ms     24 ms     28 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    78 ms   1569 ms     55 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=136ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms     31 ms     35 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    56 ms     56 ms     66 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=73ms TTL=62

```
  1 <1 ms      1 ms      1 ms   10.1.1.1
  2    27 ms     26 ms     28 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    98 ms     76 ms    140 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=56ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    48 ms     43 ms     48 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    55 ms     54 ms     74 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=55ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    59 ms     61 ms     24 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    62 ms     97 ms     53 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=186ms TTL=62

```
  1      1 ms <1 ms <1 ms   10.1.1.1
  2   116 ms    193 ms    130 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   162 ms    233 ms    153 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=128ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2   260 ms    204 ms    178 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   176 ms    219 ms    203 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Cyber World – June 9

1. Reply from 121.98.182.109: bytes=32 time=66ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    24 ms     24 ms     24 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    53 ms     55 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=56ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    24 ms     24 ms     25 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms     55 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=55ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms     25 ms     26 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    53 ms     54 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=51ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms     26 ms     25 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    57 ms     54 ms     56 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=52ms TTL=62

```
  1 <1 ms <1 ms      1 ms   10.1.1.1
  2    33 ms     34 ms     32 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms     54 ms     59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=57ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms     24 ms     31 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    61 ms     52 ms     55 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=136ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2   184 ms    216 ms    291 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   421 ms    432 ms    472 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=406ms TTL=62

```
  1     1 ms <1 ms <1 ms   10.1.1.1
  2   256 ms    297 ms    248 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   335 ms    261 ms    244 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Cyber World – June 10

1. Reply from 121.98.182.109: bytes=32 time=57ms TTL=62

```
  1     1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms     24 ms     24 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms     56 ms     58 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=53ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    24 ms     25 ms     24 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    56 ms     55 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=56ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    89 ms     25 ms     24 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms     53 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=56ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms    24 ms    24 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    57 ms    55 ms    54 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=58ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    24 ms    24 ms    24 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms    54 ms    55 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=54ms TTL=62

```
  1 <1 ms <1 ms <1 ms   10.1.1.1
  2    26 ms    24 ms    24 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    56 ms    54 ms  3335 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=55ms TTL=62

```
  1     1 ms <1 ms <1 ms   10.1.1.1
  2    30 ms    27 ms    36 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    54 ms    54 ms    55 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=53ms TTL=62

```
  1     1 ms <1 ms <1 ms   10.1.1.1
  2    25 ms    24 ms    24 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    53 ms    55 ms  1553 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

DIC World – June 9

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
C:\>tracert 121.98.182.109
  1 <1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    35 ms    33 ms    32 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    75 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     3 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    30 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     2 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms    35 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    30 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1 <1 ms     2 ms     8 ms  60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     2 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    30 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=34ms TTL=59

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms     1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     2 ms     3 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    35 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

DIC World – June 20

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1 <1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3     *       36 ms    32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1     1 ms     1 ms     1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    30 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2    51 ms     2 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms  1800 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=42ms TTL=59

```
  1     8 ms     1 ms     2 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    33 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1     4 ms     1 ms     3 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    34 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1     1 ms <1 ms     1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     3 ms     3 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    35 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=34ms TTL=59

```
  1     1 ms <1 ms     1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2 <1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    30 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=34ms TTL=59

```
  1     1 ms <1 ms     1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     2 ms     1 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    37 ms    32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

DIC World – June 20

1. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    33 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     2 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1     1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms      2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1     6 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     3 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    33 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms    29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1     1 ms <1 ms      1 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     1 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    30 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1     2 ms     2 ms      2 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     3 ms     3 ms      3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    31 ms     31 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=35ms TTL=62

```
  1     1 ms     2 ms      2 ms   60-234-21-81.bitstream.orcon.net.nz [60.234.21.81]
  2     3 ms     3 ms      3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    31 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Net2 – June 9

1. Reply from 121.98.182.109: bytes=32 time=34ms TTL=61

```
C:\>tracert 121.98.182.109
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2    14 ms     1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    38 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=33ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2 <1 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    30 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=42ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2     1 ms    38 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3    25 ms     5 ms     22 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    30 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=36ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2    16 ms     7 ms     4 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    28 ms    30 ms    28 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2     9 ms     9 ms     8 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     2 ms     3 ms     4 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2    11 ms    26 ms     4 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     7 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4     *       51 ms    32 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=37ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2    <1 ms    <1 ms    <1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3    12 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    29 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2    <1 ms    <1 ms    <1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     3 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    30 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Net2 – June 18

1. Reply from 121.98.182.109: bytes=32 time=30ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2    <1 ms    <1 ms    <1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     2 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    33 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=30ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2    54 ms    <1 ms    <1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    43 ms    32 ms    29 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2    <1 ms    <1 ms    <1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    29 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=34ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2     7 ms     5 ms     1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3    19 ms     1 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    30 ms    28 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=32ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2     2 ms    <1 ms    <1 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3    59 ms     2 ms    15 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    31 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=29ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2 <1 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms      *       36 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=32ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2 <1 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     7 ms     1 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    30 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=40ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2    27 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3    11 ms     3 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    36 ms    40 ms    42 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Net2 – June 20

1. Reply from 121.98.182.109: bytes=32 time=30ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2     2 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    30 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=30ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2 <1 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     2 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    35 ms    37 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2    11 ms    12 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     2 ms     3 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    35 ms    32 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=802ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2 <1 ms <1 ms     1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     1 ms     3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    35 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=40ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2     7 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     2 ms     2 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    34 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=30ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2     4 ms <1 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     1 ms     3 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    34 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=30ms TTL=61

```
  1 <1 ms <1 ms <1 ms   60.234.54.129
  2     7 ms     4 ms <1 ms   60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     3 ms     3 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    33 ms    48 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=31ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.129
  2     1 ms     2 ms     2 ms  60-234-21-49.bitstream.orcon.net.nz [60.234.21.49]
  3     3 ms     3 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    37 ms    31 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Starzone – June 13

1. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
C:\>tracert 121.98.182.109
  1     1 ms    <1 ms    <1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     1 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms     1 ms     1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3    34 ms     4 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    40 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms     1 ms     1 ms  60.234.59.1
  2    33 ms     1 ms     1 ms  60.234.20.213
  3    56 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    31 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1     2 ms     1 ms     2 ms  60.234.59.1
  2     1 ms    <1 ms     1 ms  60.234.20.213
  3    40 ms     2 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    36 ms    35 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    35 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=36ms TTL=58

```
  1     1 ms     1 ms    <1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     2 ms     3 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    32 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms    <1 ms    <1 ms  60.234.59.1
  2    <1 ms     1 ms    <1 ms  60.234.20.213
  3     2 ms     2 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    31 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1     1 ms     1 ms     1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     2 ms     2 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Starzone – June 14

1. Reply from 121.98.182.109: bytes=32 time=50ms TTL=58

```
  1  <1 ms  <1 ms     1 ms  60.234.59.1
  2     1 ms     1 ms  <1 ms  60.234.20.213
  3     2 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    35 ms    32 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=71ms TTL=58

```
  1     1 ms  <1 ms     1 ms  60.234.59.1
  2     2 ms     1 ms     1 ms  60.234.20.213
  3     1 ms     3 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    30 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms     1 ms  <1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1    13 ms     2 ms     1 ms  60.234.59.1
  2    13 ms     1 ms     1 ms  60.234.20.213
  3     7 ms     5 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    37 ms    34 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1     1 ms  <1 ms     1 ms  60.234.59.1
  2    10 ms     1 ms     1 ms  60.234.20.213
  3     2 ms     3 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=35ms TTL=58

```
  1     1 ms  <1 ms  <1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     4 ms     2 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    34 ms    36 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1     1 ms     1 ms     1 ms  60.234.59.1
  2    63 ms     1 ms     1 ms  60.234.20.213
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    31 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=30ms TTL=58

```
  1     2 ms     2 ms     1 ms  60.234.59.1
  2     1 ms  <1 ms     1 ms  60.234.20.213
  3     2 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    33 ms    32 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Starzone – June 15

1. Reply from 121.98.182.109: bytes=32 time=69ms TTL=58

```
  1  <1 ms     2 ms     1 ms  60.234.59.1
  2    35 ms     1 ms  <1 ms  60.234.20.213
  3    13 ms     2 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    35 ms    33 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1     1 ms    <1 ms     1 ms  60.234.59.1
  2     2 ms     1 ms     2 ms  60.234.20.213
  3    11 ms     4 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    39 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1     1 ms     1 ms     1 ms  60.234.59.1
  2     1 ms     1 ms     2 ms  60.234.20.213
  3     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    41 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms     1 ms    <1 ms  60.234.59.1
  2     2 ms     2 ms     1 ms  60.234.20.213
  3     3 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    33 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=36ms TTL=58

```
  1     1 ms     2 ms     1 ms  60.234.59.1
  2     1 ms     2 ms     2 ms  60.234.20.213
  3     2 ms     3 ms     4 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    31 ms    99 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms     1 ms     2 ms  60.234.59.1
  2     1 ms     1 ms     2 ms  60.234.20.213
  3     2 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    30 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=35ms TTL=58

```
  1     1 ms     1 ms     1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     2 ms     2 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    33 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1     1 ms    <1 ms     1 ms  60.234.59.1
  2     1 ms     1 ms     1 ms  60.234.20.213
  3     2 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    34 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

MC Internet – June 11

1. Reply from 121.98.182.109: bytes=32 time=48ms TTL=61

```
C:\>tracert 121.98.182.109
  1     1 ms    <1 ms    <1 ms  192.168.0.254
  2    <1 ms     1 ms     1 ms  192.168.2.254
  3    79 ms    19 ms    20 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    54 ms    51 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=53ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  192.168.0.254
  2    <1 ms    <1 ms     1 ms  192.168.2.254
  3   119 ms    55 ms    20 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    56 ms   420 ms    48 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=49ms TTL=61

```
  1    <1 ms    <1 ms    <1 ms  192.168.0.254
  2    <1 ms    <1 ms    <1 ms  192.168.2.254
  3    20 ms    19 ms    20 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    49 ms    51 ms    47 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=49ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    19 ms    19 ms    21 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    48 ms    49 ms    51 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=48ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms     1 ms     1 ms  192.168.2.254
  3    27 ms    29 ms    18 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    49 ms    65 ms    48 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=49ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms <1 ms <1 ms   192.168.2.254
  3    74 ms    20 ms    20 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    50 ms    49 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=47ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    21 ms    20 ms    19 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    50 ms    49 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=47ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    22 ms    28 ms    48 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    51 ms    50 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

MC Internet – June 12

1. Reply from 121.98.182.109: bytes=32 time=49ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms     1 ms     1 ms  192.168.2.254
  3    20 ms    18 ms    20 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    53 ms    49 ms    51 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=50ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    19 ms    19 ms    19 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    52 ms    48 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=47ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms     1 ms <1 ms   192.168.2.254
  3    20 ms    19 ms    23 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    52 ms    49 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=51ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    20 ms    19 ms    19 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    52 ms    49 ms    49 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=51ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    20 ms     19 ms     19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    52 ms     49 ms     49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=49ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms <1 ms <1 ms   192.168.2.254
  3    20 ms    148 ms     27 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    50 ms     49 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=50ms TTL=61

```
  1     1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms     1 ms   192.168.2.254
  3    27 ms     31 ms     23 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    48 ms     50 ms      *      121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
  5    49 ms     50 ms     48 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=56ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms      1 ms      1 ms   192.168.2.254
  3    29 ms     24 ms     23 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    49 ms     58 ms     51 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

MC Internet – June 15

1. Reply from 121.98.182.109: bytes=32 time=55ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms <1 ms <1 ms   192.168.2.254
  3    21 ms    103 ms     34 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    49 ms     49 ms     49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=48ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    19 ms     20 ms     19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    47 ms     54 ms     49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=50ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms      1 ms <1 ms   192.168.2.254
  3    19 ms     20 ms     19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    52 ms     53 ms    100 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=74ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    21 ms     21 ms     19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    47 ms     50 ms     54 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=47ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms      1 ms <1 ms   192.168.2.254
  3    20 ms     22 ms     19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    51 ms     49 ms    101 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=48ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms <1 ms <1 ms   192.168.2.254
  3    19 ms    20 ms    19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    60 ms    54 ms    49 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=52ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2     1 ms <1 ms     1 ms   192.168.2.254
  3    19 ms    18 ms    27 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    50 ms    50 ms    92 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=56ms TTL=61

```
  1 <1 ms <1 ms <1 ms   192.168.0.254
  2 <1 ms <1 ms <1 ms   192.168.2.254
  3    20 ms    27 ms    19 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  4    47 ms    49 ms    50 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Login1 – June 13

1. Reply from 121.98.182.109: bytes=32 time=30ms TTL=58

```
C:\>tracert 121.98.182.109
  1 <1 ms <1 ms <1 ms   202.89.47.62
  2     2 ms     1 ms     1 ms   atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     2 ms     1 ms     1 ms   gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms   gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms   orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    31 ms    34 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1     1 ms <1 ms <1 ms   202.89.47.62
  2     2 ms     1 ms     2 ms   atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms   gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms   gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms   orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     4 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    35 ms    33 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1     1 ms <1 ms <1 ms   202.89.47.62
  2     1 ms     1 ms     1 ms   atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms   gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     3 ms     2 ms     1 ms   gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms   orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    33 ms    35 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1     1 ms     1 ms     1 ms   202.89.47.62
  2     2 ms     5 ms     1 ms   atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms   gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     2 ms     2 ms     3 ms   gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     3 ms     2 ms     3 ms   orcon2.ape.net.nz [192.203.154.67]
  6    11 ms     5 ms     5 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    35 ms    37 ms    32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1     1 ms     3 ms <1 ms   202.89.47.62
  2    18 ms    12 ms    31 ms   atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms   gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms   gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms   orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     9 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms     *       34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1     1 ms <1 ms     1 ms  202.89.47.62
  2     2 ms     2 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     3 ms     7 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     6 ms     4 ms    28 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    34 ms    35 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1 <1 ms <1 ms <1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3    12 ms    13 ms    13 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     8 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     4 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    35 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
 1 <1 ms <1 ms <1 ms  202.89.47.62
  2    22 ms     2 ms   112 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     3 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    34 ms    35 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Login1 – June 14

1. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1 <1 ms <1 ms     1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3    74 ms   198 ms     2 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     2 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     4 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    35 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1 <1 ms     1 ms <1 ms  202.89.47.62
  2     1 ms     1 ms     2 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     2 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5    17 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    33 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1 <1 ms <1 ms <1 ms  202.89.47.62
  2     1 ms     2 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    36 ms    33 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1 <1 ms <1 ms <1 ms  202.89.47.62
  2     2 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=34ms TTL=58

```
  1     1 ms    <1 ms    <1 ms  202.89.47.62
  2     2 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     3 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=35ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     6 ms     5 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    35 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=35ms TTL=58

```
  1    <1 ms     1 ms     1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     4 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    35 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=35ms TTL=58

```
  1    <1 ms     1 ms    <1 ms  202.89.47.62
  2    39 ms    23 ms     4 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr1.alb.maxnet.net.nz [123.100.64.132]
  4     1 ms     1 ms     1 ms  gi0-0-0.bdr1.alb.maxnet.net.nz [123.100.64.242]
  5    64 ms     2 ms     3 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms    13 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    35 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Login1 – June 15

1. Reply from 121.98.182.109: bytes=32 time=35ms TTL=58

```
  1     1 ms    <1 ms    <1 ms  202.89.47.62
  2   218 ms     2 ms    14 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     2 ms     1 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     2 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    35 ms    35 ms   100 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     2 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     4 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    33 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=36ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  202.89.47.62
  2   249 ms     5 ms    10 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms    14 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    35 ms    35 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1    <1 ms    <1 ms     1 ms  202.89.47.62
  2   152 ms    15 ms     6 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     8 ms     3 ms     4 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    32 ms    35 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1     1 ms    <1 ms    <1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     9 ms     3 ms     4 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    31 ms    35 ms    45 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=33ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  202.89.47.62
  2     2 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     2 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     3 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7     *       70 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=32ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  202.89.47.62
  2    58 ms    12 ms   284 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     2 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     2 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     6 ms     3 ms    14 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    34 ms    35 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=31ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  202.89.47.62
  2     1 ms     1 ms     1 ms  atm4-0-0-135.ar02.akl1.maxnet.net.nz [210.55.230.57]
  3     1 ms     1 ms     1 ms  gi4-15.cr2.alb.maxnet.net.nz [123.100.64.136]
  4     1 ms     1 ms     1 ms  gi0-0-1.bdr1.alb.maxnet.net.nz [123.100.64.246]
  5     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  6     4 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    34 ms    35 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Galaxy – June 13

1. Pinging 121.98.182.109 with 32 bytes of data:
Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     1 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms    29 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    30 ms  3608 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1     7 ms     5 ms     4 ms  60.234.54.1
  2     1 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    35 ms    33 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1    12 ms     1 ms    <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    34 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=32ms TTL=59

```
  1    26 ms    <1 ms    <1 ms  60.234.54.1
  2     2 ms     3 ms     4 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    41 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1    27 ms    <1 ms    <1 ms  60.234.54.1
  2     2 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3  3251 ms    30 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2   127 ms    17 ms   136 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    37 ms    31 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Galaxy – June 14

1. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1    <1 ms     1 ms    <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    30 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     2 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    30 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     2 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    35 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     2 ms     2 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    30 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=33ms TTL=59

```
  1    <1 ms    <1 ms    <1 ms  60.234.54.1
  2     3 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    33 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

```
  1    <1 ms    <1 ms     1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    31 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=29ms TTL=59

```
  1    33 ms    29 ms    30 ms  60.234.54.1
  2    27 ms     5 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=30ms TTL=59

```
  1 <1 ms     2 ms <1 ms  60.234.54.1
  2     2 ms     2 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    35 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Galaxy – June 15

1. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms  60.234.54.1
  2   261 ms    34 ms     7 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    31 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=103ms TTL=62

```
  1 <1 ms <1 ms <1 ms  60.234.54.1
  2   206 ms    22 ms    10 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms   415 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1 <1 ms <1 ms <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    33 ms    29 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1 <1 ms <1 ms <1 ms  60.234.54.1
  2     4 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    30 ms    29 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1 <1 ms <1 ms <1 ms  60.234.54.1
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=36ms TTL=62

```
  1     4 ms     3 ms     1 ms  60.234.54.1
  2     5 ms     6 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3   132 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1    25 ms <1 ms <1 ms  60.234.54.1
  2     1 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms    30 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

XY Internet – June 18

1. Reply from 121.98.182.109: bytes=32 time=162ms TTL=58

```
C:\>tracert 121.98.182.109
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     2 ms     1 ms     1 ms  10.1.1.1
  3   234 ms   219 ms     *      202.180.81.31
  4   139 ms    33 ms    43 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   100 ms    40 ms    33 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   208 ms     *      178 ms  orcon2.ape.net.nz [192.203.154.67]
  7   264 ms    74 ms   186 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8    65 ms   120 ms   154 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=267ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3     *      203 ms   122 ms  202.180.81.31
  4    53 ms    58 ms    33 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   179 ms   166 ms   105 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   167 ms   122 ms   188 ms  orcon2.ape.net.nz [192.203.154.67]
  7   204 ms   105 ms    53 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8     *      281 ms   257 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=301ms TTL=58

```
  1     1 ms <1 ms     1 ms   my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3     *      193 ms   208 ms  202.180.81.31
  4   259 ms   277 ms   299 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   319 ms   204 ms   124 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   256 ms     *      249 ms  orcon2.ape.net.nz [192.203.154.67]
  7   236 ms   229 ms   202 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8    68 ms    65 ms    64 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=271ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     1 ms     2 ms  10.1.1.1
  3   253 ms   259 ms   254 ms  202.180.81.31
  4   246 ms   238 ms   238 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   313 ms   244 ms     *      vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   245 ms   243 ms   305 ms  orcon2.ape.net.nz [192.203.154.67]
  7   245 ms   302 ms   311 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   371 ms   334 ms   274 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=272ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     2 ms     3 ms     8 ms  10.1.1.1
  3     *      309 ms     *      202.180.81.31
  4   225 ms   292 ms   282 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   187 ms   284 ms   319 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   230 ms     *      309 ms  orcon2.ape.net.nz [192.203.154.67]
  7   375 ms   178 ms   205 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   171 ms   134 ms   170 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=76ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     1 ms     3 ms  10.1.1.1
  3    95 ms   146 ms   145 ms  202.180.81.31
  4   131 ms   142 ms   140 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   137 ms     *      127 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   122 ms   130 ms   131 ms  orcon2.ape.net.nz [192.203.154.67]
  7   120 ms   131 ms   135 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   109 ms     *       72 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=62ms TTL=58

```
  1     1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     2 ms     2 ms     1 ms  10.1.1.1
  3    31 ms    58 ms    31 ms  202.180.81.31
  4    37 ms    33 ms    33 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   110 ms     *       39 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6    39 ms    62 ms    32 ms  orcon2.ape.net.nz [192.203.154.67]
  7    34 ms    69 ms     *     gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8    63 ms    63 ms    65 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=62ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     3 ms     1 ms     1 ms  10.1.1.1
  3    31 ms    33 ms    32 ms  202.180.81.31
  4    33 ms    32 ms    30 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5    33 ms     *      31 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6    32 ms    32 ms    33 ms  orcon2.ape.net.nz [192.203.154.67]
  7    34 ms    33 ms     *     gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8    64 ms    64 ms    64 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

XY Internet – June 19

1. Reply from 121.98.182.109: bytes=32 time=65ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     2 ms     2 ms     2 ms  10.1.1.1
  3   327 ms   362 ms   293 ms  202.180.81.31
  4   261 ms   244 ms   282 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5    34 ms     *      41 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6    32 ms    33 ms     *     orcon2.ape.net.nz [192.203.154.67]
  7   200 ms    64 ms     *     gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8    64 ms   372 ms   170 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=168ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3   131 ms   249 ms    43 ms  202.180.81.31
  4     *     584 ms     *     vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5    35 ms    32 ms    34 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   293 ms   303 ms   365 ms  orcon2.ape.net.nz [192.203.154.67]
  7   266 ms   271 ms   262 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   209 ms   270 ms   229 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=115ms TTL=58

```
  1     3 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3    42 ms    66 ms   124 ms  202.180.81.31
  4     *      86 ms    33 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5    46 ms     *     153 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   202 ms   144 ms     *     orcon2.ape.net.nz [192.203.154.67]
  7   133 ms    35 ms    33 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   156 ms   144 ms    84 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=2244ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     3 ms    14 ms     1 ms  10.1.1.1
  3   498 ms   315 ms   351 ms  202.180.81.31
  4   282 ms     *     232 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   236 ms   279 ms     *     vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   244 ms     *     239 ms  orcon2.ape.net.nz [192.203.154.67]
  7   243 ms     *     213 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   365 ms     *     228 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=270ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3   259 ms   334 ms   385 ms  202.180.81.31
  4   297 ms     *     225 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   219 ms     *        *     vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   208 ms   321 ms   245 ms  orcon2.ape.net.nz [192.203.154.67]
  7     *        *     247 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   262 ms     *     300 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=432ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     2 ms     1 ms     1 ms  10.1.1.1
  3   388 ms   313 ms   380 ms  202.180.81.31
  4   362 ms   278 ms   292 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   208 ms   281 ms   282 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   286 ms     *      211 ms  orcon2.ape.net.nz [192.203.154.67]
  7   228 ms   195 ms   250 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   201 ms   389 ms   290 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=357ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     2 ms     1 ms     1 ms  10.1.1.1
  3   300 ms   340 ms     *     202.180.81.31
  4   418 ms     *      382 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   246 ms     *      209 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6     *      299 ms     *     orcon2.ape.net.nz [192.203.154.67]
  7     *      253 ms   305 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   320 ms   325 ms     *     121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=382ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     2 ms     3 ms  10.1.1.1
  3   297 ms   369 ms   371 ms  202.180.81.31
  4   335 ms   345 ms     *     vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5     *      305 ms   319 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6     *      331 ms   197 ms  orcon2.ape.net.nz [192.203.154.67]
  7   209 ms     *      176 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8     *      171 ms   205 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

XY Internet – June 26

1. Reply from 121.98.182.109: bytes=32 time=186ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     2 ms     5 ms  10.1.1.1
  3   267 ms   276 ms   195 ms  202.180.81.31
  4     *      243 ms     *     vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   223 ms   243 ms   266 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   356 ms   241 ms     *     orcon2.ape.net.nz [192.203.154.67]
  7   323 ms   313 ms   343 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8     *      384 ms   240 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=274ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     2 ms     2 ms  10.1.1.1
  3     *      220 ms   188 ms  202.180.81.31
  4   245 ms   110 ms   146 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   207 ms   166 ms   169 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   187 ms   251 ms   213 ms  orcon2.ape.net.nz [192.203.154.67]
  7   428 ms   345 ms     *     gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8  1877 ms   331 ms   340 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=316ms TTL=58

```
  1 <1 ms <1 ms <1 ms   my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3   160 ms     *      185 ms  202.180.81.31
  4   279 ms     *      243 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   235 ms   262 ms   246 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6     *      302 ms   229 ms  orcon2.ape.net.nz [192.203.154.67]
  7   286 ms   380 ms     *     gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   347 ms   272 ms   380 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=291ms TTL=58

```
  1     1 ms     2 ms     2 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3     *      230 ms   192 ms  202.180.81.31
  4   234 ms   208 ms   202 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   207 ms   298 ms   276 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   201 ms   207 ms   283 ms  orcon2.ape.net.nz [192.203.154.67]
  7   252 ms   187 ms   193 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   275 ms   245 ms   234 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=314ms TTL=58

```
  1 <1 ms <1 ms     1 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3   243 ms     *      165 ms  202.180.81.31
  4   207 ms   297 ms   318 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   220 ms   251 ms   195 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6   172 ms   291 ms   262 ms  orcon2.ape.net.nz [192.203.154.67]
  7   405 ms   335 ms   362 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8   226 ms    86 ms    74 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=65ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     2 ms     1 ms     1 ms  10.1.1.1
  3   193 ms   242 ms     *     202.180.81.31
  4   479 ms     *      286 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   193 ms   174 ms     *     vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6     *      267 ms   287 ms  orcon2.ape.net.nz [192.203.154.67]
  7   395 ms     *      221 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8     *        *        *     Request timed out.
  9   271 ms   306 ms   259 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=64ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     3 ms     2 ms     1 ms  10.1.1.1
  3    31 ms    33 ms     *     202.180.81.31
  4   125 ms     *      164 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5   150 ms     *      248 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6     *      176 ms   125 ms  orcon2.ape.net.nz [192.203.154.67]
  7   256 ms     *      271 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8     *      201 ms   154 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=61ms TTL=58

```
  1 <1 ms <1 ms <1 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.1.1
  3   147 ms    91 ms    71 ms  202.180.81.31
  4    84 ms    58 ms    33 ms  vlan94-cpcak3-e1.tranzpeer.net [202.180.82.82]
  5    32 ms     *      133 ms  vlan7-cpcak3-s1.tranzpeer.net [202.180.81.49]
  6    33 ms    32 ms    33 ms  orcon2.ape.net.nz [192.203.154.67]
  7     *       39 ms    34 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  8    92 ms    63 ms    64 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Mega Web – June 18

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=60

```
  1     1 ms <1 ms     1 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2 <1 ms <1 ms <1 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    40 ms     1 ms     9 ms  orcon2.ape.net.nz [192.203.154.67]
  4     3 ms     2 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    34 ms    35 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=30ms TTL=60

```
  1 <1 ms <1 ms <1 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2 <1 ms <1 ms <1 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     2 ms     1 ms     1 ms  orcon2.ape.net.nz [192.203.154.67]
  4     4 ms     2 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    34 ms    39 ms     *     121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
  6    39 ms    39 ms    40 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=50ms TTL=60

```
  1     1 ms     1 ms <1 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2 <1 ms <1 ms <1 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     3 ms     2 ms     1 ms   orcon2.ape.net.nz [192.203.154.67]
  4     2 ms     2 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    31 ms    34 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=33ms TTL=60

```
  1     1 ms     2 ms <1 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2 <1 ms <1 ms <1 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     1 ms     1 ms     1 ms   orcon2.ape.net.nz [192.203.154.67]
  4     3 ms     3 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    31 ms    35 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=322ms TTL=60

```
  1 <1 ms <1 ms <1 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     3 ms    17 ms     6 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     2 ms     2 ms     *      orcon2.ape.net.nz [192.203.154.67]
  4     8 ms    10 ms    13 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    30 ms    32 ms    40 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=36ms TTL=60

```
  1    12 ms    11 ms    10 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2 <1 ms <1 ms <1 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     2 ms     1 ms     2 ms   orcon2.ape.net.nz [192.203.154.67]
  4     2 ms     2 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    31 ms    34 ms    38 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=39ms TTL=60

```
  1     5 ms     6 ms     4 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     9 ms     5 ms     2 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     1 ms     1 ms     1 ms   orcon2.ape.net.nz [192.203.154.67]
  4    11 ms     5 ms     3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    33 ms    34 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=43ms TTL=60

```
  1 <1 ms     1 ms     1 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     5 ms     6 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    18 ms     4 ms     3 ms   orcon2.ape.net.nz [192.203.154.67]
  4    37 ms     7 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    36 ms    34 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Mega Web – June 20

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=60

```
  1     5 ms    24 ms     7 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    13 ms    23 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     5 ms    23 ms    23 ms   orcon2.ape.net.nz [192.203.154.67]
  4     5 ms     6 ms    17 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    36 ms    54 ms    40 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=45ms TTL=60

```
  1     8 ms    23 ms    23 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2 <1 ms <1 ms <1 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    11 ms     6 ms    16 ms   orcon2.ape.net.nz [192.203.154.67]
  4     3 ms     2 ms     2 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    48 ms    47 ms    47 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=47ms TTL=60

```
  1     2 ms     2 ms     3 ms   202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    14 ms    21 ms    23 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    36 ms     8 ms    10 ms  orcon2.ape.net.nz [192.203.154.67]
  4     3 ms    22 ms    25 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    40 ms    47 ms    47 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=39ms TTL=60

```
  1     4 ms     3 ms     4 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    22 ms     7 ms    23 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    11 ms    18 ms     6 ms  orcon2.ape.net.nz [192.203.154.67]
  4     *        6 ms    10 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    50 ms    42 ms    46 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=43ms TTL=60

```
  1    15 ms    25 ms    25 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    <1 ms    <1 ms    <1 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     1 ms     1 ms     1 ms  orcon2.ape.net.nz [192.203.154.67]
  4     3 ms     1 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    30 ms    35 ms    32 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=45ms TTL=60

```
  1    22 ms     6 ms    17 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     4 ms     6 ms    16 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    18 ms    23 ms    21 ms  orcon2.ape.net.nz [192.203.154.67]
  4    16 ms    23 ms    23 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    49 ms  2888 ms    43 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=40ms TTL=60

```
  1    10 ms     2 ms     1 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    11 ms    25 ms     3 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    18 ms    19 ms    23 ms  orcon2.ape.net.nz [192.203.154.67]
  4    11 ms    18 ms     9 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    57 ms    32 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=36ms TTL=60

```
  1    <1 ms    <1 ms    <1 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     3 ms     2 ms    14 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    18 ms     5 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  4    10 ms    15 ms    16 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    51 ms    47 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Mega Web – June 21

1. Reply from 121.98.182.109: bytes=32 time=52ms TTL=60

```
  1     7 ms    23 ms    23 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    15 ms     6 ms    17 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    12 ms    24 ms     7 ms  orcon2.ape.net.nz [192.203.154.67]
  4     9 ms    20 ms    10 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    48 ms    39 ms    47 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=32ms TTL=60

```
  1    10 ms     6 ms    19 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     1 ms    <1 ms     1 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     7 ms     9 ms    13 ms  orcon2.ape.net.nz [192.203.154.67]
  4    11 ms     9 ms    13 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    38 ms     *      117 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=50ms TTL=60

```
  1    46 ms    22 ms    18 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     7 ms     4 ms     3 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    28 ms    21 ms    22 ms  orcon2.ape.net.nz [192.203.154.67]
  4     9 ms    23 ms    24 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    34 ms    48 ms    47 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=47ms TTL=60

```
  1    17 ms     9 ms    13 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    10 ms    12 ms    17 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    12 ms     3 ms     1 ms  orcon2.ape.net.nz [192.203.154.67]
  4    36 ms   129 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    34 ms    53 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=44ms TTL=60

```
  1     7 ms    23 ms     9 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    11 ms    25 ms    13 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    22 ms    24 ms     8 ms  orcon2.ape.net.nz [192.203.154.67]
  4     6 ms     7 ms   112 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    56 ms    57 ms    56 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=62ms TTL=60

```
  1    15 ms    50 ms    28 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    11 ms    25 ms    23 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    19 ms    24 ms    19 ms  orcon2.ape.net.nz [192.203.154.67]
  4    11 ms    19 ms    22 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    55 ms    46 ms    48 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=34ms TTL=60

```
  1    92 ms    24 ms     8 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2     5 ms     8 ms    13 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    14 ms    22 ms     8 ms  orcon2.ape.net.nz [192.203.154.67]
  4    82 ms    79 ms    14 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    36 ms    46 ms    47 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=36ms TTL=60

```
  1    15 ms     9 ms    15 ms  202-169-205-1.linktelecom.co.nz [202.169.205.1]
  2    <1 ms    <1 ms    <1 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     3 ms     6 ms     7 ms  orcon2.ape.net.nz [192.203.154.67]
  4     2 ms     2 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    32 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Big World Internet – June 20

1. Ethernet adapter Local Area Connection:

```
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 60.234.22.131
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 60.234.22.129
```

Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1     1 ms    <1 ms    <1 ms  60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    30 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1    <1 ms    <1 ms    <1 ms  60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=74ms TTL=62

```
  1     8 ms     1 ms    <1 ms  60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     3 ms     1 ms     1 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=29ms TTL=62

```
  1    12 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     2 ms     1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms     30 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms     29 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1 <1 ms      1 ms      1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms   2157 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=669ms TTL=62

```
  1      1 ms      1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms     33 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms     29 ms     31 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Big World Internet – June 23

1. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1      1 ms      1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms     30 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=34ms TTL=62

```
  1      1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3      *        34 ms     32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      2 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms     29 ms     30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=34ms TTL=62

```
  1    38 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2    11 ms      4 ms      3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms     31 ms     33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1 <1 ms      1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms     29 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=31ms TTL=62

```
  1      1 ms      1 ms      1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2      1 ms      1 ms      1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms     32 ms     29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     2 ms     2 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    29 ms     *       33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     2 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    31 ms    33 ms    31 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Big World Internet – June 24

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=62

```
  1     1 ms <1 ms     1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    33 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1     1 ms     1 ms     3 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     3 ms     2 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1     2 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    30 ms    29 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=34ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=34ms TTL=62

```
  1     1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    32 ms    29 ms  2609 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=33ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    30 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=30ms TTL=62

```
  1     1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     2 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    34 ms    29 ms    29 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=1581ms TTL=62

```
  1 <1 ms <1 ms <1 ms   60-234-21-25.bitstream.orcon.net.nz [60.234.21.25]
  2     1 ms     1 ms     1 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  3    33 ms    29 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

I-Life Zone – June 21

1. Reply from 121.98.182.109: bytes=32 time=416ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   325 ms   301 ms   152 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   262 ms   188 ms    98 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=167ms TTL=62

```
  1     1 ms <1 ms     1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   128 ms   115 ms    74 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   325 ms   124 ms   126 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=347ms TTL=62

```
  1     1 ms     1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   225 ms   200 ms   368 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   348 ms   164 ms   237 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=300ms TTL=62

```
  1 <1 ms <1 ms     1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   280 ms   328 ms   309 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  1120 ms   396 ms   387 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=2978ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   220 ms   208 ms   165 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   223 ms   246 ms   320 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=84ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    57 ms    58 ms    57 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    86 ms    88 ms    90 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=85ms TTL=62

```
  1     2 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    57 ms    58 ms    58 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    87 ms    87 ms    90 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=84ms TTL=62

```
  1     1 ms     1 ms     1 ms  sx763.dummy.porta.siemens.net [192.168.2.1]
  2    58 ms    57 ms    58 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    86 ms    87 ms    90 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

I-Life Zone – June 23

1. Windows IP Configuration

```
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . : dummy.porta.siemens.net
        IP Address. . . . . . . . . . . . : 192.168.2.247
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1
```

Reply from 121.98.182.109: bytes=32 time=67ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    42 ms    37 ms    40 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  3880 ms    70 ms    69 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=66ms TTL=62

```
  1     1 ms <1 ms     1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    38 ms    38 ms    38 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    69 ms    68 ms    70 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=69ms TTL=62

```
  1     1 ms <1 ms     1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    46 ms    38 ms    45 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    69 ms    68 ms    74 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=67ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    38 ms    38 ms    38 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    71 ms    67 ms    69 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=69ms TTL=62

```
  1 <1 ms <1 ms     1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    38 ms    39 ms    38 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    69 ms    68 ms    71 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=67ms TTL=62

```
  1     1 ms     1 ms     1 ms  sx763.dummy.porta.siemens.net [192.168.2.1]
  2    38 ms    37 ms    38 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    67 ms    69 ms    69 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=66ms TTL=62

```
  1     1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    46 ms    39 ms    43 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    72 ms    68 ms    67 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=67ms TTL=62

```
  1     1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2    39 ms    39 ms    39 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3    69 ms    70 ms    70 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

I-Life Zone – June 24

1. Reply from 121.98.182.109: bytes=32 time=284ms TTL=62

```
  1     1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2  2681 ms  2418 ms  2987 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  2276 ms  1957 ms  1579 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=590ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   623 ms   103 ms    61 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3     *      439 ms    98 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=486ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   577 ms   326 ms    87 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3   283 ms   176 ms   744 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=1255ms TTL=62

```
  1 <1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2  1236 ms  1015 ms  1565 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  1187 ms  1217 ms  1233 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=589ms TTL=62

```
  1     1 ms <1 ms     1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2   360 ms    72 ms   220 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  1678 ms    92 ms    95 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=2768ms TTL=62

```
  1     1 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
  2  1301 ms  1526 ms  1223 ms  lo1.ras1.nct.orcon.net.nz [60.234.8.201]
  3  1437 ms  1381 ms  1394 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=330ms TTL=62

```
 1 <1 ms <1 ms      1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
 2    128 ms     60 ms     62 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
 3     92 ms     98 ms   1034 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=87ms TTL=62

```
 1      2 ms <1 ms <1 ms   sx763.dummy.porta.siemens.net [192.168.2.1]
 2     62 ms     73 ms     60 ms   lo1.ras1.nct.orcon.net.nz [60.234.8.201]
 3     93 ms    102 ms     95 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Big World Internet Mt. Albert – June 25

1. Reply from 121.98.182.109: bytes=32 time=34ms TTL=61

```
 1      4 ms      2 ms      5 ms   202.68.95.233
 2      4 ms     14 ms      5 ms   orcon2.ape.net.nz [192.203.154.67]
 3     16 ms      6 ms     19 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     41 ms     40 ms     35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=35ms TTL=61

```
 1      2 ms      1 ms      1 ms   202.68.95.233
 2     15 ms      1 ms      3 ms   orcon2.ape.net.nz [192.203.154.67]
 3     16 ms      7 ms     10 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     33 ms     37 ms     32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=45ms TTL=61

```
 1     20 ms      2 ms      5 ms   202.68.95.233
 2     10 ms      5 ms      6 ms   orcon2.ape.net.nz [192.203.154.67]
 3     23 ms      5 ms      4 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     38 ms     35 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=45ms TTL=61

```
 1     15 ms      5 ms      1 ms   202.68.95.233
 2     30 ms      7 ms     34 ms   orcon2.ape.net.nz [192.203.154.67]
 3     29 ms      6 ms      8 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     46 ms     39 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=54ms TTL=61

```
 1     23 ms      3 ms      2 ms   202.68.95.233
 2     28 ms     11 ms      6 ms   orcon2.ape.net.nz [192.203.154.67]
 3     18 ms      3 ms      3 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4      *        46 ms     50 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=33ms TTL=61

```
 1      6 ms      3 ms      3 ms   202.68.95.233
 2     18 ms     21 ms      3 ms   orcon2.ape.net.nz [192.203.154.67]
 3     17 ms     34 ms     24 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     35 ms     34 ms    285 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=33ms TTL=61

```
 1      6 ms      8 ms     19 ms   202.68.95.233
 2      4 ms     12 ms     11 ms   orcon2.ape.net.nz [192.203.154.67]
 3      7 ms     10 ms     18 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     62 ms     38 ms     37 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=58ms TTL=61

```
 1     19 ms      3 ms      2 ms   202.68.95.233
 2     17 ms      4 ms      2 ms   orcon2.ape.net.nz [192.203.154.67]
 3      3 ms      8 ms      4 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
 4     40 ms     34 ms     41 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Big World Internet Mt. Albert – June 27

1. Reply from 121.98.182.109: bytes=32 time=31ms TTL=61

```
  1     2 ms     1 ms     1 ms  202.68.95.233
  2     3 ms    18 ms    16 ms  orcon2.ape.net.nz [192.203.154.67]
  3    16 ms     2 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    39 ms    38 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=40ms TTL=61

```
  1     2 ms     2 ms     1 ms  202.68.95.233
  2    12 ms     2 ms    17 ms  orcon2.ape.net.nz [192.203.154.67]
  3     3 ms     2 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    48 ms    38 ms    40 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=43ms TTL=61

```
  1     2 ms     1 ms     1 ms  202.68.95.233
  2     4 ms     2 ms     1 ms  orcon2.ape.net.nz [192.203.154.67]
  3    17 ms     5 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    38 ms    34 ms    42 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=35ms TTL=61

```
  1     2 ms     1 ms     1 ms  202.68.95.233
  2     3 ms     8 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3     3 ms     3 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    56 ms    42 ms    32 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=45ms TTL=61

```
  1    23 ms     4 ms     2 ms  202.68.95.233
  2    12 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3    11 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    50 ms    49 ms    39 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=36ms TTL=61

```
  1     2 ms     1 ms     2 ms  202.68.95.233
  2     4 ms     2 ms    24 ms  orcon2.ape.net.nz [192.203.154.67]
  3     6 ms     3 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    38 ms    77 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=33ms TTL=61

```
  1     2 ms    18 ms     1 ms  202.68.95.233
  2     1 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3    21 ms     5 ms     3 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    34 ms    41 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=55ms TTL=61

```
  1     3 ms     5 ms     1 ms  202.68.95.233
  2    15 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3    18 ms     4 ms    17 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Big World Internet Mt. Albert – June 28

1. Reply from 121.98.182.109: bytes=32 time=38ms TTL=61

```
  1     5 ms     1 ms     5 ms  202.68.95.233
  2    21 ms     5 ms    24 ms  orcon2.ape.net.nz [192.203.154.67]
  3    14 ms    19 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    51 ms    33 ms    41 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=34ms TTL=61

```
  1     2 ms     1 ms     5 ms  202.68.95.233
  2     2 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3    10 ms    20 ms     4 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    44 ms    32 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=38ms TTL=61

```
  1     3 ms     1 ms     1 ms  202.68.95.233
  2    40 ms    18 ms     4 ms  orcon2.ape.net.nz [192.203.154.67]
  3    25 ms     3 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    56 ms    41 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=50ms TTL=61

```
  1    13 ms     1 ms     2 ms  202.68.95.233
  2    22 ms     5 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3     8 ms     4 ms     2 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    44 ms    31 ms    28 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=34ms TTL=61

```
  1     1 ms     1 ms    16 ms  202.68.95.233
  2    14 ms    20 ms    29 ms  orcon2.ape.net.nz [192.203.154.67]
  3     8 ms     9 ms     6 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    31 ms    39 ms    30 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=44ms TTL=61

```
  1    15 ms     8 ms     1 ms  202.68.95.233
  2     4 ms     2 ms     2 ms  orcon2.ape.net.nz [192.203.154.67]
  3     4 ms     5 ms     5 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    32 ms    35 ms    29 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=47ms TTL=61

```
  1    12 ms     5 ms     1 ms  202.68.95.233
  2    21 ms     1 ms     1 ms  orcon2.ape.net.nz [192.203.154.67]
  3    22 ms     2 ms    16 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    41 ms    36 ms    34 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=43ms TTL=61

```
  1     7 ms     1 ms     2 ms  202.68.95.233
  2     4 ms     5 ms    29 ms  orcon2.ape.net.nz [192.203.154.67]
  3    25 ms   160 ms     7 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  4    35 ms    51 ms    60 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Web City – June 25

1. Ethernet adapter Local Area Connection:

```
    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . . : 202.169.202.9
    Subnet Mask . . . . . . . . . . . : 255.255.255.192
    Default Gateway . . . . . . . . . : 202.169.202.61
```

Reply from 121.98.182.109: bytes=32 time=36ms TTL=60

```
  1     3 ms     3 ms     3 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2     4 ms     4 ms     4 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     4 ms     4 ms     3 ms  orcon2.ape.net.nz [192.203.154.67]
  4     4 ms     4 ms     5 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    34 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=33ms TTL=60

```
  1     3 ms     3 ms     4 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2     4 ms     3 ms     4 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    77 ms     4 ms     4 ms  orcon2.ape.net.nz [192.203.154.67]
  4   11 ms    9 ms    5 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   37 ms   36 ms   38 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=45ms TTL=60

```
  1    3 ms    4 ms    3 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    3 ms    4 ms    4 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    4 ms    4 ms    4 ms  orcon2.ape.net.nz [192.203.154.67]
  4   15 ms     *      9 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   38 ms   41 ms   54 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=34ms TTL=60

```
  1    3 ms    3 ms    3 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    6 ms    8 ms    4 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   54 ms   37 ms   14 ms  orcon2.ape.net.nz [192.203.154.67]
  4    4 ms    5 ms    5 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   40 ms   41 ms   42 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=50ms TTL=60

```
  1   55 ms   99 ms   78 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   26 ms   27 ms    7 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   21 ms   33 ms   37 ms  orcon2.ape.net.nz [192.203.154.67]
  4   66 ms   24 ms   22 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    *     262 ms  144 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=34ms TTL=60

```
  1   15 ms   13 ms   42 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   33 ms   40 ms   24 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   27 ms   27 ms   14 ms  orcon2.ape.net.nz [192.203.154.67]
  4   48 ms   35 ms   41 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   77 ms   48 ms   39 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=99ms TTL=60

```
  1   98 ms  112 ms  145 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   93 ms   84 ms   76 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   90 ms   80 ms   98 ms  orcon2.ape.net.nz [192.203.154.67]
  4   91 ms   73 ms   73 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   95 ms  101 ms  129 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=38ms TTL=60

```
  1   20 ms    6 ms   11 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   10 ms   14 ms   24 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   19 ms   27 ms   22 ms  orcon2.ape.net.nz [192.203.154.67]
  4   17 ms    6 ms   17 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   54 ms   47 ms   35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Web City – June 27

1. Reply from 121.98.182.109: bytes=32 time=58ms TTL=60

```
  1   15 ms   14 ms   14 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   28 ms   34 ms   27 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    9 ms    3 ms   14 ms  orcon2.ape.net.nz [192.203.154.67]
  4   12 ms   28 ms   14 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   37 ms   41 ms   37 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=43ms TTL=60

```
  1    3 ms   24 ms   16 ms  202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   16 ms    4 ms    4 ms  gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   38 ms   14 ms   14 ms  orcon2.ape.net.nz [192.203.154.67]
  4   10 ms   13 ms   16 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   58 ms   49 ms   37 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=50ms TTL=60

```
  1    20 ms    15 ms    13 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    16 ms     7 ms    19 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    54 ms    36 ms    30 ms   orcon2.ape.net.nz [192.203.154.67]
  4    31 ms    37 ms    41 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    63 ms     *       39 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=113ms TTL=60

```
  1    87 ms    63 ms    53 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    58 ms    37 ms     5 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    33 ms    38 ms    93 ms   orcon2.ape.net.nz [192.203.154.67]
  4    67 ms    39 ms    68 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    84 ms   135 ms   161 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=62ms TTL=60

```
  1    36 ms    44 ms    45 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    57 ms    22 ms    47 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    40 ms    48 ms     *      orcon2.ape.net.nz [192.203.154.67]
  4    69 ms    58 ms    50 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    73 ms    75 ms    69 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=176ms TTL=60

```
  1    45 ms    36 ms    79 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    40 ms    75 ms    53 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    51 ms    43 ms    47 ms   orcon2.ape.net.nz [192.203.154.67]
  4   101 ms    68 ms    65 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    80 ms    80 ms    62 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=44ms TTL=60

```
  1     4 ms     3 ms     3 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2     4 ms     4 ms     3 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     4 ms    12 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4     5 ms     5 ms     5 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    38 ms    44 ms    46 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=94ms TTL=60

```
  1     3 ms     3 ms     7 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    37 ms    26 ms    34 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    13 ms    12 ms    13 ms   orcon2.ape.net.nz [192.203.154.67]
  4    70 ms     5 ms     9 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    30 ms    35 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Web City – June 28

1. Reply from 121.98.182.109: bytes=32 time=37ms TTL=60

```
  1    48 ms    14 ms    19 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2     4 ms     4 ms    20 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     4 ms     4 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4    55 ms     5 ms   140 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   117 ms    86 ms    47 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=31ms TTL=60

```
  1     3 ms     3 ms     3 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2     4 ms     4 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3     4 ms     4 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4     7 ms     9 ms    21 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    34 ms    43 ms    36 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=32ms TTL=60

```
  1    18 ms    35 ms    17 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2     4 ms     4 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    7 ms     4 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4    4 ms     4 ms     5 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   33 ms    33 ms    30 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=31ms TTL=60

```
  1   10 ms     6 ms     6 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    4 ms     3 ms    13 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    4 ms     4 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4   11 ms    13 ms    13 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   33 ms    32 ms    48 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=33ms TTL=60

```
  1    3 ms     3 ms     3 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    4 ms     4 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    6 ms    13 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4    5 ms     5 ms     9 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   31 ms    33 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=29ms TTL=60

```
  1   14 ms     7 ms     7 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    3 ms     4 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    4 ms     4 ms     4 ms   orcon2.ape.net.nz [192.203.154.67]
  4    5 ms     5 ms     4 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   34 ms    34 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=50ms TTL=60

```
  1   10 ms     3 ms    12 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2   14 ms    13 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3   32 ms    23 ms    29 ms   orcon2.ape.net.nz [192.203.154.67]
  4   16 ms     7 ms     5 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5    *       36 ms    42 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=31ms TTL=60

```
  1    3 ms     3 ms     3 ms   202-169-202-61.linktelecom.co.nz [202.169.202.61]
  2    3 ms     4 ms     4 ms   gi-0-50.akl-dom-2.linktelecom.co.nz [202.169.192.11]
  3    9 ms     4 ms     3 ms   orcon2.ape.net.nz [192.203.154.67]
  4    5 ms     6 ms     4 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  5   31 ms    35 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Manish-Cafe – June 25

1. Ethernet adapter Local Area Connection:

```
    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . . : 10.1.1.6
    Subnet Mask . . . . . . . . . . . : 255.0.0.0
    Default Gateway . . . . . . . . . : 10.1.1.1
```

Reply from 121.98.182.109: bytes=32 time=73ms TTL=58

```
  1    1 ms    <1 ms    <1 ms   mygateway1.ar7 [10.1.1.1]
  2   50 ms    50 ms    49 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3   41 ms     *       44 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4   43 ms    42 ms    45 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5   44 ms    41 ms    45 ms   orcon2.ape.net.nz [192.203.154.67]
  6   47 ms    47 ms    43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7   73 ms    74 ms    73 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=267ms TTL=58

```
  1    1 ms    <1 ms     1 ms   mygateway1.ar7 [10.1.1.1]
  2   56 ms    66 ms    63 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3   43 ms    50 ms    44 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4   43 ms    42 ms    42 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5   44 ms    43 ms    43 ms   orcon2.ape.net.nz [192.203.154.67]
  6   45 ms    47 ms    43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    77 ms    72 ms    74 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=74ms TTL=58

```
  1     2 ms     2 ms     2 ms  mygateway1.ar7 [10.1.1.1]
  2    54 ms    52 ms     *     lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    48 ms    43 ms    45 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    41 ms    44 ms    44 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    42 ms    44 ms    45 ms  orcon2.ape.net.nz [192.203.154.67]
  6    49 ms    44 ms    44 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    74 ms    74 ms    73 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=77ms TTL=58

```
  1     1 ms     2 ms     2 ms  mygateway1.ar7 [10.1.1.1]
  2    54 ms    68 ms    55 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    41 ms    46 ms    42 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    44 ms    42 ms    42 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms   106 ms    73 ms  orcon2.ape.net.nz [192.203.154.67]
  6    45 ms    44 ms    42 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    73 ms    77 ms    72 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=76ms TTL=58

```
  1    <1 ms     2 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    51 ms    50 ms    48 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3   122 ms    42 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    45 ms    43 ms    42 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms    42 ms    43 ms  orcon2.ape.net.nz [192.203.154.67]
  6    47 ms    45 ms    45 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    77 ms    74 ms    76 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=87ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    53 ms    66 ms    44 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms    45 ms    80 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    59 ms    42 ms    72 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms    43 ms    43 ms  orcon2.ape.net.nz [192.203.154.67]
  6    46 ms    44 ms    43 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    74 ms    75 ms     *     121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
  8    90 ms    73 ms    74 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=69ms TTL=58

```
  1     5 ms     2 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    52 ms    61 ms    66 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms    43 ms    44 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    44 ms    42 ms    44 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    45 ms    47 ms     *     orcon2.ape.net.nz [192.203.154.67]
  6    47 ms    45 ms    45 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    75 ms    77 ms    79 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=77ms TTL=58

```
  1     1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    46 ms    69 ms    52 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    42 ms    43 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    44 ms    43 ms    42 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    48 ms    45 ms    44 ms  orcon2.ape.net.nz [192.203.154.67]
  6    83 ms    43 ms    45 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    71 ms    85 ms    74 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Manish-Cafe – June 27

1. Reply from 121.98.182.109: bytes=32 time=68ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    62 ms    50 ms    49 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms    42 ms    41 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms     43 ms     42 ms   orcon2.ape.net.nz [192.203.154.67]
  6    42 ms     43 ms     43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    75 ms     74 ms     94 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=69ms TTL=58

```
  1 <1 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    59 ms     46 ms     66 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms     42 ms     42 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms      *       43 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    45 ms     41 ms     43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    43 ms     43 ms    225 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    73 ms     74 ms     70 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=66ms TTL=58

```
  1 <1 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    55 ms     74 ms     44 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    42 ms      *       43 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms     43 ms     43 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    45 ms     42 ms     43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    46 ms     43 ms     43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    70 ms     75 ms     75 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=69ms TTL=58

```
  1 <1 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    48 ms     51 ms     53 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms     43 ms     42 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    42 ms     42 ms     41 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    43 ms     43 ms     43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    46 ms     45 ms     43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    72 ms     68 ms     70 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=70ms TTL=58

```
  1 <1 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    47 ms     50 ms     57 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    41 ms     43 ms     43 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms     43 ms     43 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms     43 ms     43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    94 ms     43 ms     43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    71 ms     71 ms   3694 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=68ms TTL=58

```
  1 <1 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    48 ms     50 ms     58 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    42 ms     43 ms     43 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms      *       42 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms     43 ms     42 ms   orcon2.ape.net.nz [192.203.154.67]
  6    49 ms     44 ms     42 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    73 ms     70 ms     75 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=68ms TTL=58

```
  1     2 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    52 ms     52 ms     47 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    41 ms     43 ms     43 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms     43 ms     42 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    43 ms     43 ms     43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    64 ms     45 ms     43 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    69 ms     69 ms     69 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=67ms TTL=58

```
  1     9 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    47 ms     48 ms     65 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    42 ms     43 ms     43 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms     43 ms     44 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    43 ms     79 ms     43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    44 ms    43 ms    42 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    72 ms    73 ms    70 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Manish-Cafe – June 28

1. Reply from 121.98.182.109: bytes=32 time=70ms TTL=58

```
  1     2 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    55 ms    50 ms    49 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    44 ms    43 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    45 ms    43 ms    42 ms  orcon2.ape.net.nz [192.203.154.67]
  6    43 ms    43 ms    42 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    69 ms    68 ms    70 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=66ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    50 ms    44 ms    46 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    41 ms    43 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    41 ms    44 ms    42 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    43 ms    43 ms    43 ms  orcon2.ape.net.nz [192.203.154.67]
  6    43 ms    45 ms    44 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    70 ms    70 ms    73 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=65ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    52 ms    51 ms    50 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms    42 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    42 ms    43 ms   150 ms  orcon2.ape.net.nz [192.203.154.67]
  6    47 ms    43 ms    45 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    71 ms    70 ms    70 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=68ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    58 ms    54 ms    50 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    41 ms    43 ms    42 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    42 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    43 ms    43 ms    43 ms  orcon2.ape.net.nz [192.203.154.67]
  6    44 ms    44 ms    44 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    72 ms    68 ms    69 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=69ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    53 ms    50 ms    49 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    42 ms    43 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    44 ms    43 ms    43 ms  orcon2.ape.net.nz [192.203.154.67]
  6    44 ms    43 ms    42 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    70 ms    67 ms    70 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=69ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    68 ms    54 ms    49 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms    43 ms    42 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5   101 ms    45 ms    42 ms  orcon2.ape.net.nz [192.203.154.67]
  6    44 ms    44 ms    43 ms  gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    74 ms    76 ms    72 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=3924ms TTL=58

```
  1    <1 ms    <1 ms    <1 ms  mygateway1.ar7 [10.1.1.1]
  2    54 ms    55 ms    45 ms  lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    43 ms    43 ms    43 ms  gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    43 ms    43 ms    43 ms  gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    45 ms    43 ms    42 ms   orcon2.ape.net.nz [192.203.154.67]
  6    43 ms    44 ms    44 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    71 ms    70 ms    74 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=68ms TTL=58

```
  1 <1 ms <1 ms <1 ms   mygateway1.ar7 [10.1.1.1]
  2    47 ms    45 ms    44 ms   lo1.akl-grafton-bras1.ihug.net [203.109.128.90]
  3    42 ms    42 ms    43 ms   gi6-0-0.akl-grafton-edge1.ihug.net [203.109.143.101]
  4    42 ms    43 ms    42 ms   gi5-0-0.akl-grafton-edge2.ihug.net [203.109.130.133]
  5    43 ms    43 ms    43 ms   orcon2.ape.net.nz [192.203.154.67]
  6    45 ms    45 ms    42 ms   gi-4-0-3-0.ras1.nct.orcon.net.nz [121.98.9.2]
  7    72 ms    69 ms    70 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Sunway – July 7

1. Ethernet adapter Local Area Connection:

```
   Connection-specific DNS Suffix  . : home
   IP Address. . . . . . . . . . . . : 192.168.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\>ping 121.98.182.109
Reply from 121.98.182.109: bytes=32 time=115ms TTL=56

C:\>tracert 121.98.182.109
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2    32 ms    31 ms    30 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3    31 ms    32 ms    30 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4    69 ms    81 ms   126 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5    31 ms    31 ms    56 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
  6   163 ms   140 ms   109 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7    31 ms    31 ms    32 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    32 ms    31 ms    33 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9    88 ms    79 ms    57 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=74ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2    39 ms    33 ms    31 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   143 ms    32 ms    34 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   116 ms   121 ms    35 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   126 ms    60 ms    44 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
  6    79 ms    66 ms    43 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7    61 ms    68 ms    67 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    65 ms   152 ms    72 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   109 ms    95 ms    88 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=99ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2    52 ms    71 ms    39 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3    33 ms    32 ms    30 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4    51 ms    39 ms    31 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5    31 ms    30 ms    44 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
  6    34 ms    43 ms    40 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7    31 ms    56 ms    37 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    66 ms    47 ms    70 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9    69 ms    61 ms   116 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=73ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2    32 ms    33 ms    31 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3    42 ms    37 ms    30 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4    52 ms    44 ms    31 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5    98 ms    49 ms    92 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
  6    32 ms    34 ms    32 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7    61 ms   126 ms    79 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8     *       98 ms    38 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9    79 ms    86 ms    79 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=75ms TTL=56

```
 1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2    51 ms    34 ms     35 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3    33 ms    32 ms     31 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4    33 ms    71 ms     32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5    31 ms    31 ms     44 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
 6    32 ms    30 ms   153 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   114 ms   226 ms   134 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8    33 ms    31 ms     50 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9    81 ms    59 ms     59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=115ms TTL=56

```
 1     1 ms      1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2    63 ms    30 ms     30 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3    45 ms   124 ms     49 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   119 ms    74 ms   128 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5    75 ms    34 ms     30 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
 6    35 ms    31 ms     31 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7    78 ms    46 ms     38 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   105 ms    84 ms     43 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   103 ms   194 ms   130 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=121ms TTL=56

```
 1     1 ms      1 ms      1 ms   RTA1025W.home [192.168.1.1]
 2    76 ms    50 ms      *      lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3     *         *       166 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4     *       101 ms     56 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   119 ms   145 ms   110 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
 6    67 ms    81 ms   130 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7     *         *        47 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8    78 ms    83 ms     50 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   113 ms   103 ms     64 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=78ms TTL=56

```
 1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2    67 ms    32 ms     52 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3    45 ms    30 ms     30 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   124 ms    31 ms     31 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5    32 ms    32 ms     33 ms   g0-1-0-4.akcr8.global-gateway.net.nz [210.55.202.49]
 6    80 ms    31 ms   112 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   183 ms   187 ms      *      orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8    35 ms    38 ms     32 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9    61 ms    60 ms     59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Sunway – July 10

1. Reply from 121.98.182.109: bytes=32 time=62ms TTL=56

```
 1     3 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2    34 ms    42 ms     32 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3    34 ms    32 ms     32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4    33 ms    33 ms     32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5    33 ms    33 ms     33 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6    33 ms    33 ms     32 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7    33 ms    32 ms     33 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8    34 ms    33 ms     34 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9    59 ms    60 ms     59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=59ms TTL=56

```
 1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2    33 ms    80 ms     33 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3    32 ms    32 ms     32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4    33 ms    32 ms     32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5    33 ms    33 ms     33 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6    33 ms    32 ms     33 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7    33 ms    34 ms     33 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   34 ms    33 ms    34 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   62 ms    59 ms    61 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=61ms TTL=56

```
 1    1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2   36 ms    32 ms    33 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3   36 ms    32 ms    32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   33 ms    33 ms    32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   33 ms    33 ms    33 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6   33 ms    32 ms    33 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   33 ms    32 ms    32 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   34 ms    34 ms    34 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   60 ms    58 ms    59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=60ms TTL=56

```
 1    1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2   32 ms    32 ms    32 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3   33 ms    32 ms    32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   32 ms    32 ms    32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   33 ms    33 ms    33 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6   33 ms    32 ms    32 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   33 ms    32 ms    33 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   34 ms    35 ms    35 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   62 ms    59 ms    60 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=62ms TTL=56

```
 1    1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2   33 ms    32 ms    32 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3   32 ms    32 ms    32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   33 ms    33 ms    32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   33 ms    32 ms    32 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6   33 ms    33 ms    32 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   33 ms    32 ms    33 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   34 ms    34 ms    34 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   61 ms    60 ms    64 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=60ms TTL=56

```
 1    1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2   33 ms    33 ms    33 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3   34 ms    32 ms    33 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   33 ms    35 ms    33 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   37 ms    40 ms    35 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6   44 ms    42 ms    50 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   33 ms    48 ms    34 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   35 ms    34 ms    34 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   70 ms    90 ms    76 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=63ms TTL=56

```
 1    2 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2   37 ms    32 ms    32 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3   32 ms    32 ms    32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   33 ms    32 ms    32 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   33 ms    33 ms    32 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6   34 ms    33 ms    33 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   34 ms    33 ms    33 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   34 ms    33 ms    33 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 9   64 ms    59 ms    59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=58ms TTL=56

```
 1    1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
 2   33 ms    55 ms    51 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
 3   32 ms    65 ms    32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 4   33 ms    46 ms    60 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 5   55 ms    72 ms    69 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 6   33 ms    78 ms    32 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 7   58 ms    61 ms   129 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 8   36 ms    65 ms    62 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
```

```
  9    62 ms    89 ms    59 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Sunway – July 12

1. Reply from 121.98.182.109: bytes=32 time=71ms TTL=56

```
  1     1 ms <1 ms     1 ms   RTA1025W.home [192.168.1.1]
  2    61 ms    30 ms    65 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   161 ms   152 ms   112 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4     *      128 ms   146 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   166 ms   173 ms   165 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6   115 ms   146 ms   135 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   134 ms    85 ms   120 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    86 ms   180 ms   220 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9    58 ms    84 ms   124 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=176ms TTL=56

```
  1     2 ms     1 ms     1 ms   RTA1025W.home [192.168.1.1]
  2   228 ms    94 ms    98 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   116 ms     *       32 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4    63 ms    32 ms   106 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   117 ms    41 ms    32 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6   138 ms   154 ms   131 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   222 ms   150 ms   166 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    48 ms    74 ms    74 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   115 ms   113 ms   135 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=183ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2    86 ms   150 ms   119 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   119 ms   124 ms   120 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   140 ms   103 ms    69 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   165 ms   165 ms    85 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6   197 ms   191 ms   124 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   240 ms   143 ms   118 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8   137 ms    98 ms   128 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   200 ms   168 ms   194 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=153ms TTL=56

```
  1     2 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2   128 ms   363 ms   170 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3    60 ms    93 ms   136 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   209 ms   209 ms   201 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5    83 ms    45 ms    46 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6   175 ms   217 ms   119 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   106 ms   100 ms   110 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8   252 ms   235 ms   166 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   175 ms   288 ms   155 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=200ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2   126 ms   107 ms   109 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   141 ms   119 ms   145 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   149 ms   142 ms   209 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   159 ms    67 ms   143 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6    77 ms    80 ms    48 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   129 ms   159 ms   184 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    88 ms   142 ms   161 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   206 ms    89 ms   158 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=149ms TTL=56

```
  1     1 ms     1 ms     1 ms   RTA1025W.home [192.168.1.1]
  2   198 ms   133 ms   135 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3     *      182 ms   148 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   107 ms   166 ms   153 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   125 ms   162 ms   156 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6   151 ms    124 ms    137 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   171 ms    220 ms    101 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8     *        86 ms    189 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   174 ms    133 ms      *      121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
 10     *       209 ms    201 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=145ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2   153 ms      *       155 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   171 ms    156 ms     89 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   115 ms    123 ms    119 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   203 ms      *       147 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6    85 ms     87 ms     72 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7   146 ms    151 ms    137 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8    82 ms     74 ms     73 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   165 ms    184 ms    130 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=164ms TTL=56

```
  1     1 ms <1 ms <1 ms   RTA1025W.home [192.168.1.1]
  2   156 ms    104 ms    134 ms   lo0.internet.ivpn.pe24.telstraclear.net [218.101.61.122]
  3   143 ms    193 ms    164 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  4   184 ms    152 ms    158 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  5   242 ms    158 ms    146 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  6   210 ms    184 ms    238 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  7    41 ms     65 ms     73 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  8   206 ms    211 ms    156 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
  9   126 ms    174 ms    235 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

E-Funz– July 8

1. Ethernet adapter Local Area Connection 3:

```
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.6
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254
```

Reply from 121.98.182.109: bytes=32 time=74ms TTL=52

```
  1 <1 ms <1 ms <1 ms   192.168.1.254
  2     4 ms      4 ms      3 ms   203.97.2.25
  3     5 ms      5 ms      9 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms      6 ms      5 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms      6 ms      6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     9 ms      6 ms      6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms      6 ms      6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8    16 ms     15 ms     26 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms      7 ms      7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    40 ms     38 ms     35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=100ms TTL=52

```
  1     1 ms      1 ms      1 ms   192.168.1.254
  2    62 ms     63 ms     72 ms   203.97.2.25
  3    46 ms     48 ms     38 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4    69 ms     47 ms     56 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    82 ms     72 ms     74 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6    75 ms     64 ms     75 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    29 ms     25 ms     22 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8    89 ms     68 ms     35 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9    92 ms     24 ms     23 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    50 ms     53 ms    109 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=127ms TTL=52

```
  1     1 ms <1 ms <1 ms   192.168.1.254
  2    68 ms     77 ms     93 ms   203.97.2.25
  3    69 ms     83 ms     69 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4    77 ms     87 ms     78 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    45 ms     55 ms     88 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6    83 ms     74 ms     59 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    84 ms    81 ms    92 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     *       46 ms    43 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9    61 ms    55 ms    54 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10   103 ms    99 ms    97 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=36ms TTL=52

```
  1    <1 ms    <1 ms    <1 ms  192.168.1.254
  2     4 ms     4 ms     4 ms  203.97.2.25
  3     5 ms     5 ms     5 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms     5 ms     5 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    56 ms    65 ms    59 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms     9 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     7 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     7 ms     8 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    42 ms    34 ms    39 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=35ms TTL=52

```
  1     1 ms    <1 ms    <1 ms  192.168.1.254
  2     4 ms     3 ms     5 ms  203.97.2.25
  3     5 ms     5 ms     7 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     6 ms     5 ms     5 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     *       28 ms    38 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    57 ms    52 ms    49 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8    77 ms    66 ms    72 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     9 ms     7 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    36 ms    34 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=155ms TTL=52

```
  1     1 ms    <1 ms    <1 ms  192.168.1.254
  2    93 ms    78 ms    59 ms  203.97.2.25
  3    47 ms    43 ms    59 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4    58 ms    62 ms    55 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    46 ms    31 ms    35 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6    39 ms    43 ms    50 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    62 ms    63 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms    89 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9    26 ms    73 ms    77 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    35 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=36ms TTL=52

```
  1     2 ms     1 ms    <1 ms  192.168.1.254
  2    65 ms    76 ms    62 ms  203.97.2.25
  3    53 ms    80 ms    81 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4    74 ms    74 ms    91 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    79 ms    94 ms    89 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6    87 ms    69 ms    66 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    73 ms    69 ms    72 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8    74 ms    66 ms    71 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9    69 ms    74 ms    81 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    36 ms    87 ms    56 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=60ms TTL=52

```
  1     1 ms    <1 ms     1 ms  192.168.1.254
  2    87 ms    93 ms    77 ms  203.97.2.25
  3    15 ms     6 ms     9 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     6 ms     8 ms    14 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     7 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     7 ms     6 ms     6 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     8 ms     6 ms    13 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     7 ms     7 ms     6 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9    18 ms     8 ms    10 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    36 ms    33 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

E-Funz– July 9

1. Reply from 121.98.182.109: bytes=32 time=128ms TTL=52

```
  1     1 ms <1 ms <1 ms   192.168.1.254
  2     5 ms     4 ms     4 ms   203.97.2.25
  3    52 ms    14 ms     5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     6 ms     5 ms     6 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms     6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     7 ms     7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    34 ms    34 ms    33 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=1950ms TTL=52

```
  1     1 ms <1 ms      1 ms   192.168.1.254
  2    66 ms    67 ms    74 ms   203.97.2.25
  3    92 ms   101 ms    79 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4    69 ms    24 ms    24 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms     9 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     7 ms     9 ms     6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     7 ms     7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    33 ms    34 ms    35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=35ms TTL=52

```
  1 <1 ms <1 ms <1 ms   192.168.1.254
  2     4 ms     4 ms     3 ms   203.97.2.25
  3     5 ms     5 ms     5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms     6 ms     5 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    15 ms     6 ms     6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6    22 ms     6 ms     6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms    48 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     7 ms     8 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    35 ms    32 ms    34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=34ms TTL=52

```
  1 <1 ms <1 ms <1 ms   192.168.1.254
  2    66 ms     4 ms     4 ms   203.97.2.25
  3    51 ms    72 ms   104 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4    86 ms    93 ms    93 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    81 ms    90 ms   102 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms    10 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    33 ms     6 ms     6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     7 ms     7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    34 ms   120 ms    32 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=34ms TTL=52

```
  1 <1 ms <1 ms <1 ms   192.168.1.254
  2     4 ms     5 ms     5 ms   203.97.2.25
  3     9 ms     5 ms     5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms     5 ms     5 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms    50 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    15 ms    18 ms     6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     8 ms     7 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9   129 ms     7 ms     7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    51 ms    47 ms    36 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=35ms TTL=52

```
  1 <1 ms <1 ms <1 ms   192.168.1.254
  2    79 ms     4 ms     5 ms   203.97.2.25
  3     5 ms     5 ms     8 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms     5 ms     5 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms     6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     6 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     7 ms     8 ms    13 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    34 ms    38 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=34ms TTL=52

```
  1    <1 ms     1 ms    <1 ms  192.168.1.254
  2     6 ms     4 ms     4 ms  203.97.2.25
  3     5 ms     5 ms     5 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms     5 ms     5 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     8 ms     6 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    10 ms     6 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     7 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9    82 ms     8 ms     9 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    34 ms    34 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=42ms TTL=52

```
  1     1 ms    <1 ms    <1 ms  192.168.1.254
  2     4 ms     4 ms     4 ms  203.97.2.25
  3     5 ms     5 ms     5 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     6 ms     6 ms     6 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     6 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms     6 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     7 ms     6 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     6 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9   182 ms    70 ms    64 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    38 ms    32 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

E-Funz– July 10

1. Reply from 121.98.182.109: bytes=32 time=32ms TTL=52

```
  1    <1 ms    <1 ms    <1 ms  192.168.1.254
  2     4 ms     3 ms     3 ms  203.97.2.25
  3     9 ms    14 ms    18 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     9 ms     5 ms     5 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     5 ms     7 ms     5 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     9 ms     6 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     7 ms     6 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     8 ms     8 ms    12 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    41 ms    33 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

2. Reply from 121.98.182.109: bytes=32 time=35ms TTL=52

```
  1     1 ms    <1 ms     2 ms  192.168.1.254
  2     4 ms     4 ms     3 ms  203.97.2.25
  3     9 ms    15 ms     5 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     6 ms     7 ms     5 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5     6 ms     6 ms     9 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6     6 ms     6 ms     6 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7     6 ms     6 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8     6 ms     6 ms     6 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9     8 ms     7 ms     7 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10    37 ms    34 ms    33 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

3. Reply from 121.98.182.109: bytes=32 time=31ms TTL=52

```
  1    <1 ms    <1 ms    <1 ms  192.168.1.254
  2     3 ms     3 ms     4 ms  203.97.2.25
  3     5 ms     5 ms     5 ms  xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
  4     5 ms     5 ms     5 ms  ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
  5    82 ms    26 ms     7 ms  ggis-gige-v906.telstraclear.net [203.98.18.67]
  6    76 ms    44 ms     6 ms  g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
  7    97 ms    42 ms     6 ms  ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
  8    90 ms    24 ms     6 ms  orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
  9   130 ms    80 ms     7 ms  gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
 10   124 ms    37 ms    35 ms  121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

4. Reply from 121.98.182.109: bytes=32 time=36ms TTL=52

```
 1 <1 ms <1 ms <1 ms   192.168.1.254
 2     4 ms      5 ms      5 ms   203.97.2.25
 3     5 ms      5 ms      5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
 4     6 ms      6 ms      7 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 5    12 ms      6 ms      5 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 6     6 ms      6 ms      6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 7     6 ms     10 ms     14 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 8     6 ms      6 ms      6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 9    30 ms      8 ms      9 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
10    77 ms     81 ms     63 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

5. Reply from 121.98.182.109: bytes=32 time=31ms TTL=52

```
 1     1 ms <1 ms <1 ms   192.168.1.254
 2    13 ms      7 ms      3 ms   203.97.2.25
 3     5 ms      5 ms      5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
 4    21 ms      5 ms      5 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 5     6 ms      6 ms      6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 6     8 ms      6 ms      7 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 7     6 ms      6 ms      6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 8     6 ms      6 ms      6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 9    14 ms      7 ms      7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
10    35 ms     37 ms     35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

6. Reply from 121.98.182.109: bytes=32 time=106ms TTL=52

```
 1 <1 ms <1 ms <1 ms   192.168.1.254
 2    96 ms    127 ms    124 ms   203.97.2.25
 3    59 ms     65 ms     57 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
 4    96 ms    106 ms    108 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 5    63 ms     54 ms     60 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 6   110 ms     31 ms      6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 7     6 ms      6 ms      6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 8    67 ms     46 ms     48 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 9    43 ms     17 ms      8 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
10    77 ms     32 ms     34 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

7. Reply from 121.98.182.109: bytes=32 time=72ms TTL=52

```
 1 <1 ms <1 ms <1 ms   192.168.1.254
 2   125 ms    104 ms    115 ms   203.97.2.25
 3     5 ms      5 ms      5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
 4    52 ms    174 ms    174 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 5     6 ms      6 ms      6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 6     6 ms      6 ms      6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 7     6 ms      6 ms      6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 8     6 ms      6 ms      6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 9     7 ms      8 ms      7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
10    36 ms     32 ms     35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

8. Reply from 121.98.182.109: bytes=32 time=3990ms TTL=52

```
 1 <1 ms <1 ms <1 ms   192.168.1.254
 2     4 ms      3 ms      4 ms   203.97.2.25
 3     5 ms      5 ms      5 ms   xe-1-0-0-830.internet.ie1.telstraclear.net [218.101.61.201]
 4     6 ms      6 ms      5 ms   ge-2-0-0-906.ie2.telstraclear.net [203.98.18.65]
 5    16 ms      6 ms      6 ms   ggis-gige-v906.telstraclear.net [203.98.18.67]
 6     6 ms      6 ms      6 ms   g0-1-0.tkcr3.global-gateway.net.nz [210.55.202.50]
 7     6 ms      6 ms      6 ms   ae2-10.tkcr4.global-gateway.net.nz [210.55.202.36]
 8     6 ms      6 ms      6 ms   orcon-dom.tkcr4.global-gateway.net.nz [203.96.66.102]
 9     7 ms      7 ms      7 ms   gi-5-0-3-0.ras1.nct.orcon.net.nz [121.98.9.6]
10    38 ms     33 ms     35 ms   121-98-182-109.bitstream.orcon.net.nz [121.98.182.109]
```

Appendix C

P0F ESTIMATION RESULTS

Date	Operating System Estimation
iPlay Internet & Game	
June 6	<Sun Jun 06 18:00:13 2010> 60.234.58.80:1227 - UNKNOWN [8192:61:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?] -> 192.168.0.102:25 (link: pppoe (DSL))
June 9	<Wed Jun 09 12:32:01 2010> 60.234.58.99:1083 - UNKNOWN [8192:61:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?] -> 192.168.0.102:25 (link: pppoe (DSL))
June 18	<Fri Jun 18 21:25:45 2010> 60.234.58.99:1119 - UNKNOWN [8192:61:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?] -> 192.168.0.102:25 (link: pppoe (DSL))
Bros	
June 6	<Sun Jun 06 21:55:20 2010> 60.234.56.190:1239 - UNKNOWN [65535:61:1:52:M1452,N,W2,N,N,S:.:?:?] -> 192.168.0.102:25 (link: pppoe (DSL))
June 9	<Wed Jun 09 21:11:41 2010> 60.234.56.190:1120 - UNKNOWN [65535:61:1:52:M1452,N,W2,N,N,S:.:?:?] -> 192.168.0.102:25 (link: pppoe (DSL))
June 16	<Wed Jun 16 12:41:38 2010> 60.234.56.186:1136 - UNKNOWN [65535:61:1:52:M1452,N,W2,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
Cyber World	
June 7	<Mon Jun 07 16:47:32 2010> 121.98.146.102:1385 - Windows XP/2000 (RFC1323 no tstamp) [GENERIC] Signature: [16384:125:1:52:M1360,N,W0,N,N,S:.:Windows:?]
June 8	<Tue Jun 08 16:58:12 2010> 121.98.146.102:1195 - Windows XP/2000 (RFC1323 no tstamp) [GENERIC] Signature: [16384:125:1:52:M1360,N,W0,N,N,S:.:Windows:?]
June 10	<Thu Jun 10 16:19:11 2010> 121.98.146.102:1876 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222) -> 192.168.0.102:25 (distance 3, link: (Google/AOL))
Blitz	
June 7	<Mon Jun 07 18:01:03 2010> 121.98.147.136:2471 - UNKNOWN [S4:61:1:56:M1452,S,T:.:?:?] (NAT!) (up: 764 hrs) -> 192.168.0.102:25 (link: pppoe (DSL))
June 8	<Tue Jun 08 18:11:26 2010> 121.98.147.136:1111 - UNKNOWN [S4:61:1:56:M1452,S,T:.:?:?] (NAT!) (up: 1006 hrs) -> 192.168.0.102:25 (link: pppoe (DSL))
June 10	<Thu Jun 10 17:31:23 2010> 121.98.147.136:1847 - UNKNOWN [S4:61:1:56:M1452,S,T:.:?:?] (NAT!) (up: 1479 hrs) -> 192.168.0.102:25 (link: pppoe (DSL))
DIC World	
June 9	<Wed Jun 09 15:15:29 2010> 60.234.47.104:1236 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 3, link: pppoe (DSL))
June 20	<Sun Jun 20 17:20:47 2010> 60.234.47.104:1220 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 3, link: pppoe (DSL))
June 21	<Mon Jun 21 18:10:05 2010> 60.234.47.95:1144 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 3, link: pppoe (DSL))
Net2	

June 9	<Wed Jun 09 18:00:38 2010> 60.234.54.145:2966 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 9	<Wed Jun 09 18:16:07 2010> 60.234.54.144:1531 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 18	<Fri Jun 18 23:40:47 2010> 60.234.54.145:1187 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 20	<Sun Jun 20 20:35:22 2010> 60.234.54.145:4953 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
MC Internet	
June 11	<Fri Jun 11 19:40:20 2010> 121.98.206.188:1333 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 12	<Sat Jun 12 17:50:38 2010> 121.98.206.188:51596 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 15	<Tue Jun 15 17:30:28 2010> 121.98.206.188:56291 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
Starzone	
June 13	<Sun Jun 13 12:50:38 2010> 60.234.59.46:1369 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 14	<Mon Jun 14 14:15:18 2010> 60.234.59.46:1125 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
June 15	<Tue Jun 15 10:54:45 2010> 60.234.59.46:1133 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 4, link: pppoe (DSL))
Login1	
June 13	<Sun Jun 13 14:00:29 2010> 202.89.47.16:2510 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 7, link: pppoe (DSL))
June 14	<Mon Jun 14 15:30:39 2010> 202.89.47.23:1327 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 7, link: pppoe (DSL))
June 15	<Tue Jun 15 12:06:26 2010> 202.89.47.19:1232 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 7, link: pppoe (DSL))
Galaxy	
June 13	<Sun Jun 13 17:21:13 2010> 60.234.54.20:1097 - UNKNOWN [T40:61:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?] (NAT2!) -> 192.168.0.102:25 (link: pppoe (DSL))
June 14	<Mon Jun 14 17:50:23 2010> 60.234.54.32:1103 - UNKNOWN [T40:61:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?] (NAT2!)-> 192.168.0.102:25 (link: pppoe (DSL))
June 15	<Tue Jun 15 14:25:37 2010> 60.234.54.13:1110 - UNKNOWN [T40:61:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?] (NAT2!)-> 192.168.0.102:25 (link: pppoe (DSL))
Mega Web	
June 18	<Fri Jun 18 17:50:23 2010> 202.169.205.57:3435 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 5, link: pppoe (DSL))
June 20	<Sun Jun 20 14:55:11 2010> 202.169.205.55:2151 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 5, link: pppoe (DSL))
June 21	<Mon Jun 21 15:55:24 2010> 202.169.205.54:1118 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 5, link: pppoe (DSL))
XY Internet	
June 18	<Fri Jun 18 13:20:48 2010> 203.100.218.143:37510 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 8, link: (Google/AOL))
June 19	<Sat Jun 19 14:26:19 2010> 119.224.26.10:46215 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 8, link: (Google/AOL))
June 26	<Sat Jun 26 12:52:43 2010> 203.184.48.74:23431 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 8, link: (Google/AOL))
Big World Internet	
June 20	<Sun Jun 20 23:00:16 2010> 60.234.22.131:1177 - UNKNOWN [65535:61:1:52:M1452,N,W2,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
June 23	<Wed Jun 23 15:50:01 2010> 60.234.22.131:1219 - UNKNOWN [65535:61:1:52:M1452,N,W2,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))

June24	<Thu Jun 24 15:49:55 2010> 60.234.22.131:1232 - UNKNOWN [65535:61:1:52:M1452,N,W2,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
I-Life Zone Internet	
June 21	<Mon Jun 21 13:02:26 2010> 121.98.141.16:1488 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 3, link: pppoe (DSL))
June 23	<Wed Jun 23 12:10:16 2010> 121.98.141.16:1214 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 3, link: pppoe (DSL))
June 24	<Thu Jun 24 13:20:21 2010> 121.98.141.16:1112 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 3, link: pppoe (DSL))
Big World Albert	
June 25	<Fri Jun 25 13:15:55 2010> 202.20.6.138:1097 - UNKNOWN [8192:60:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
June 27	<Sun Jun 27 10:45:39 2010> 202.20.6.138:1242 - UNKNOWN [8192:60:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
June 28	<Mon Jun 28 07:46:19 2010> 202.20.6.138:1308 - UNKNOWN [8192:60:1:64:M1452,N,W0,N,N,T0,N,N,S:.:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
Web City	
June 25	<Fri Jun 25 16:35:18 2010> 202.169.202.9:1436 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 5, link: pppoe (DSL))
June 27	<Sun Jun 27 13:40:57 2010> 202.169.202.20:2494 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 5, link: pppoe (DSL))
June 28	<Mon Jun 28 10:30:19 2010> 202.169.202.20:2420 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 5, link: pppoe (DSL))
Manish-Café	
June 25	<Fri Jun 25 18:56:18 2010> 118.93.29.77:1272 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 7, link: (Google/AOL))
June 27	<Sun Jun 27 15:30:57 2010> 118.93.29.77:1160 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 7, link: (Google/AOL))
June 28	<Mon Jun 28 13:45:50 2010> 118.93.29.77:1453 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 7, link: (Google/AOL))
June 28	<Mon Jun 28 15:24:34 2010> 118.93.29.77:57382 - UNKNOWN [S4:57:1:60:M1360,S,T,N,W6:.:?:?] (NAT!) (up: 0 hrs) -> 192.168.0.102:25 (link: (Google/AOL))
Sunway	
July 7	<Wed Jul 07 11:01:02 2010> 121.72.214.93:2109 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 9, link: pppoe (DSL))
July 10	<Sat Jul 10 16:21:07 2010> 121.72.212.11:1070 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 9, link: pppoe (DSL))
July 12	<Mon Jul 12 13:40:54 2010> 121.72.163.7:1447 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 9, link: pppoe (DSL))
E-funz	
July 8	<Thu Jul 08 15:45:50 2010> 203.97.2.26:1097 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 10, link: pppoe (DSL))
July 9	<Fri Jul 09 10:55:42 2010> 203.97.2.26:1207 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 10, link: pppoe (DSL))
July 10	<Sat Jul 10 11:07:00 2010> 203.97.2.26:1076 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 10, link: pppoe (DSL))
Others	
June 6	<Sun Jun 06 20:05:53 2010> 123.204.164.114:1194 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)-> 192.168.0.102:25 (distance 13, link: pppoe (DSL))
June 7	<Mon Jun 07 16:59:13 2010> 219.232.243.172:64482 - UNKNOWN [65535:109:0:48:M1452,N,N,S:A:?:?]-> 192.168.0.102:25 (link: pppoe (DSL))
June 20	<Sun Jun 20 15:39:38 2010> 121.34.3.41:4293 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 17, link: sometimes DSL (4))
June 24	<Thu Jun 24 13:30:13 2010> 124.217.225.230:48935 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 14, link: pppoe (DSL))

June 26	<Sat Jun 26 14:14:59 2010> 84.246.224.229:34484 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:02 2010> 84.246.224.229:34677 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:07 2010> 84.246.224.229:35108 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:10 2010> 84.246.224.229:35326 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:13 2010> 84.246.224.229:35522 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:16 2010> 84.246.224.229:35708 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:18 2010> 84.246.224.229:35884 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:21 2010> 84.246.224.229:36073 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:24 2010> 84.246.224.229:36274 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:27 2010> 84.246.224.229:36496 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:29 2010> 84.246.224.229:36688 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:33 2010> 84.246.224.229:36899 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:37 2010> 84.246.224.229:37212 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:40 2010> 84.246.224.229:37414 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	<Sat Jun 26 14:15:43 2010> 84.246.224.229:37617 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 3953 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
June 27	<Sun Jun 27 13:02:39 2010> 121.98.147.136:1296 - UNKNOWN [S4:61:1:56:M1452,S,T:.:?:?] (NAT!) (up: 177 hrs)-> 192.168.0.102:25 (link: pppoe (DSL))
June 30	<Wed Jun 30 11:04:37 2010> 183.7.134.222:2592 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 16, link: IPv6/IPIP)
July 3	<Sat Jul 03 12:11:14 2010> 84.246.224.229:34478 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 5612 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
	Total 126 packets received for mail server between 12:11:14 and 12:18:50 within 7 minutes
	<Sat Jul 03 12:18:50 2010> 84.246.224.229:55466 - Linux 2.5 (sometimes 2.4) (4) (NAT!) (up: 5614 hrs)-> 192.168.0.102:25 (distance 16, link: GPRS, T1, FreeS/WAN)
July 8	<Thu Jul 08 11:23:01 2010> 183.7.148.138:3235 - Windows 2000 SP4, XP SP1 -> 192.168.0.102:25 (distance 16, link: IPv6/IPIP)
July 9	<Fri Jul 09 01:00:36 2010> 120.82.112.106:4437 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 14, link: IPv6/IPIP)
	<Fri Jul 09 02:22:23 2010> 124.217.225.230:17019 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 13, link: pppoe (DSL))
	<Fri Jul 09 04:15:51 2010> 183.7.136.80:4480 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 16, link: IPv6/IPIP)
	<Fri Jul 09 17:25:54 2010> 183.7.136.252:3034 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 16, link: IPv6/IPIP)
	<Fri Jul 09 20:41:42 2010> 114.45.53.31:4318 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 12, link: IPv6/IPIP)
July 10	<Sat Jul 10 00:49:02 2010> 123.204.210.78:2445 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222) -> 192.168.0.102:25 (distance 13, link: pppoe (DSL))
	<Sat Jul 10 01:03:44 2010> 120.82.111.31:3806 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 14, link: IPv6/IPIP)
	<Sat Jul 10 10:25:58 2010> 183.7.136.252:1211 - Windows 2000 SP4, XP SP1-> 192.168.0.102:25 (distance 16, link: IPv6/IPIP)
Tom’s Macintosh	
July 1	<Thu Jul 01 16:05:51 2010> 124.197.15.100:6060 - UNKNOWN [65535:56:1:64:M1440,N,W3,N,N,T,S,E:P:?:?] (up: 1118 hrs)-> 192.168.0.102:25 (link: IPv6/IPIP)
Ubuntu 10.4 Linux Live CD Debian-derived	

July 6	<Tue Jul 06 15:09:38 2010> 121.98.146.102:44486 - UNKNOWN [S4:61:1:60:M1360,S,T,N,W6:.:?:?] (NAT!) (up: 0 hrs)-> 192.168.0.102:25 (link: (Google/AOL))
Puppy Linux Live CD	
July 6	<Tue Jul 06 15:00:12 2010> 121.98.146.102:34823 - UNKNOWN [S4:61:1:60:M1360,S,T,N,W6:.:?:?] (NAT!) (up: 0 hrs)-> 192.168.0.102:25 (link: (Google/AOL))
Schillix OpenSolaris	
July 6	<Tue Jul 06 16:25:26 2010> 121.98.146.102:59733 - Solaris 10 (beta) (NAT!)-> 192.168.0.102:25 (distance 3, link: (Google/AOL))
Helix 3.0 Live CD	
July 7	<Wed Jul 07 16:50:20 2010> 121.98.146.102:49231 - UNKNOWN [S4:61:1:60:M1360,S,T,N,W7:.:?:?] (NAT!) (up: 0 hrs) -> 192.168.0.102:25 (link: (Google/AOL))