UTILISATION OF SUBNETWORKS THROUGH DISTRIBUTED GATEWAY.

A project paper submitted to the Graduate School in partial fulfillment of the requirements for the degree of Master of Science (Information Technology), Universiti Utara Malaysia.

by

Ahmad Basri Bin Hashim

Sekolah Siswazah
(Graduate School)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certification of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

AHMAD BASRI BIN HASHIM

calon untuk Ijazah
(candidate for the degree of) Sarjana Sains (Teknologi Maklumat)

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

UTILISATION OF SUBNETWORKS THROUGH DISTRIBUTED GATEWAY

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan, dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia
(Name of Supervisor) : Roshidi bin Hj. Din

Tandatangan
(Signature) :

Tarikh
(Date) : 9 Oktober 2000

PERMISSION TO USE

In presenting this project paper in partial fulfilment of the requirements for a post graduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this project paper in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in his absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this project paper or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project paper.

Requests for permission to copy or to make other use of materials in this project paper, in whole or in part, should be addressed to:

Dean of Graduate School

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darulaman

ABSTRACT

There is increasing use of Internet in a LAN environment. Reliance on hardware and software that are mostly costly and difficult to maintain brings about problems for organisations with a small budget. Moreover, many networks available in these types of organisations, especially schools and colleges, are not fully utilised. This is especially true in terms of access to the Internet, Besides being a viable alternative to proxy server softwares, IP masqeurading allows the interconnection of subnetworks and distribution of gateways in a multiple internal LAN environment. For the server, which acts as the gateway to the Internet, Freesco, an IP masqeurading distribution which is Linux based, is used. The Windows 2000 OS is used on the client machines, A distributed gateway based on alternative routes to other gateways in different subnetworks will minimise the event of users having disconnection problems. Hence this ensures reliable and continuous Internet connection through an alternative subnetwork in the event of a connection failure in an adjoining subnetwork.

ABSTRAK

Terdapat peningkatan ketara penggunaan Internet dalam persekitaran LAN. Penggantungan kepada perkakasan dan perisian yang mahal dan sukar untuk diselenggara memberi masaalah kepada organisasi yang mempunyai sumber kewangan yang terhad. Kebanyakkan sistem rangkaian yang terdapat dalam organisasi sebegini , seperti di sekolah dan kolej, tidak di manfaatkan sepenuhnya. Perkara ini lebih ketara dalam isu seperti akses ke Internet. Selain daripada menjadi alternatif kepada perisian pelayan proxy, IP masqeurading membolehkan sambungan antara sub rangkaian dan pengagihan gateway dalam persekitaran LAN. Bagi pelayan, yang bertindak sebagai gateway kepada Internet, Freesco, suatu distribusi IP masqeurading yang berasaskan sistem operasi Linux, di gunakan. Windows 2000 digunakan untuk komputer pelanggan. Gateway yang disebarkan kepada sub rangkaian yang lain akan meminimakan permasaalahan terputus sambungan. Oleh itu, ini dapat memastikan sambungan ke Internet yang berterusan dan efisien walau pun dalam keadaan sambungan yang terputus dalam suatu sub rangkaian.

ACKNOWLEDGEMENTS

In the name of Allah, Most Beneficient, Most Merciful. Praise be to Allah, with His wish, this report has been completed.

The writer wishes to thank and acknowledge those people involved with this project, in particular the supervisor, Encik Roshidi Bin Hj. Din, for his advise and support.

Thank you to the lecturers from the computer unit, Maktab Perguruan Tuanku Bainun, Bukit Mertajam, Pulau Pinang for supporting this project from the start and for giving permission to use the computer labs. The writer is particularly appreciative of the support given by the head unit.

Thank you very much to my supportive family for their sacrifice. They have always been my source of inspiration throughout my studies at UUM.

Last but not least, thanks to the UUM lecturers, the Principal and colleagues at MPTB for their direct or indirect contribution in completing this report.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDIX

CHAPTER 1

INTRODUCTION

1.0 Introduction

Today's wired organisation relies on access to the Internet for email and web access. Networked PCs require access via the local area network (LAN) rather than through a dedicated modem and telephone line connection at each PC. Many computer labs, especially in schools and teacher training colleges use LAN connections and are able to access the Internet through an Internet Service Provider (ISP). Some of these LANs rely on hardware solutions like routers or internet sharing hubs. Some use proxy server softwares that are easily available in the market. While proxy server software is a reasonably cheap solution compared to having each PC connecting to a modem, problems of persistent disconnections are not uncommon. Furthermore, any applications that we might want to use on the PC, like Netscape, some telnet and file transfer protocol (FTP) clients must have proxy server support. Internet protocol masquerading (IP Masq) doesn't require any such special application support.

Unlike proxy servers, IP Masq servers don't need any configuration changes to all the client machines. In addition Masq servers require minimal hardware resources (Roth, 2000).

In most small organisations, a subnetwork is connected to the Internet through a single gateway. The drawback is that client machines are automatically cut off from the Internet in the event the gateway, either in the form of proxy servers, or IP masq servers, breaks down. An alternative gateway for this subnetwork will minimise disconnection problems.

IP masquerade is a networking feature in Linux. If a Linux host is connected to the Internet with IP masquerade enabled, then client machines connected to it can reach the Internet as well.

Splitting a network into two seperate domains will benefit each subnetwork with a lower traffic load. A local ethernet bridge or router can fascilitate connection between two subnetworks. Bridge remembers in which subnetwork computers are located. A computer sends packets to another computer and both situated in the same part of network bridge will not pass to other parts of a network. This helps reduce traffic within and between different parts of network.

IP masquerade also allows connection through an alternative gateway (a second Linux host connected to the Internet) in case there is a connection failure in the first gateway. Thus the presence of a bridge or router will not only reduce traffic in a subnetwork but can help divert Internet connection to an alternative gateway, ensuring utilisation of subnetworks.

Client machines using Windows 2000 as the operating system (OS) not only can access the Internet using the Linux host as the gateway. Windows 2000 provides features such as allowing client machines to access alternative Domain Name Systems (DNS). This will enable a client machine in one subnetwork to access a Linux host gateway in another subnetwork in the event of a connection failure in the first gateway. Thus, utilisation of interconnected two distinct subnetworks, each connected to the Internet via a Linux gateway could again be realised.

1.1 Problem statement

Many computer labs in learning institutes use PCs based on the Intel microprocessor. These PCs usually use networks which are ethernet based. The networks are mostly constructed on a lab by lab basis. This deprives users in one computer lab from utilising applications and other utilities like Internet connection which are available from other labs. Users should be given alternative routes, especially in the issue of access to the Internet.

Subnetworks can be connected using an ethernet bridge or router. Most of these devices that are available in the market are costly. A cheaper alternative, using a software oriented approach would help reduce costs.

While there are several solutions available for LAN-Internet connection in the market, cost has always been a major issue. Small organisations including schools and colleges have very limited budget to purchase the necessary software and hardware.

LAN-Internet connection using proxy servers are mostly Windows based. This will usually require costly hardware resources. One of the more popular proxy server software is WinGate. WinGate runs as a service in Windows 95/98/2000

and NT. This means that other than having to purchase hardware that can support the Windows 95 OS, organisations using WinGate as an Internet proxy server have to spend on the OS besides the WinGate software, prices of which are illustrated in Table 1, obtained from the Wingate pricing page (2000).

3-User WinGate Home 4.0	$39.95
6-User WinGate Home 4.0	$69.95
50-User WinGate Standard 4.0	$499.95
Unlimited-User WinGate Standard 4.0	$699.95
Unlimited-User WinGate Pro 4.0	$949.95

Table 1 Year 2000 U.S. Pricing for Wingate proxy server

Table 1 indicates that the cost of software alone, including the OS, runs into thousands of ringgit. If hardware costs are added to this, just setting up a proxy server would be beyond the means of organisations with a tight budget.

1.2 Objectives

The purpose of the proposed study is to offer a reliable and cheap LAN-Internet solution besides utilising two interconnected subnetworks for Internet access.

The main objective is in finding an affordable solution for reliable LAN-Internet connection and also for maximum utilisation of subnetworks.

The specific objectives are:

1. To implement LAN-Internet connection through the use of IP masquerading servers as an alternative to proxy server software.

2. To ensure reliable and continuous Internet connection through an alternative subnetwork in the event of a connection failure in an adjoining subnetwork.

1.3 Limitations

Some constraints and limitations identified include:

- MS Windows 2000 require more memory, disk space, and processor power, which in other words means substantial and costly hardware upgrades for the client machines. The Linux OS could be an alternative although this will take time for familiarisation on the part of users.

- Even though the Freesco servers themselves are stable, frequent Internet disconnections, mainly due to PSTN lines or from the ISP could result in user dissatisfaction.

- Hardware failure of both gateways will result in total Internet disconnection, although this scenario is highly unlikely. A more common problem could be either one of the gateways being down at any one time.

1.4 Importance of project

Most LAN-Internet connections, especially in academic institutions like schools and colleges, are based on seperate connections in several computer labs. Proxy server software has been the most popular choice in getting Internet connection. This is a reasonable solution since it is affordable compared to using the hardware oriented approach which is costly.

- The IP masquerading alternative needs to be given due attention since it will drastically reduce hardware and software costs. Another important feature of IP masquerading is that it is based on the Linux OS.

- Linux is getting more popular as it is basically a free OS. What is more significant is its open source feature. This is suitable for an academic environment which allows users the freedom to explore and edit the OS itself.

- The fact that the Malaysian Institute of Microelectronic Systems (MIMOS) is spearheading efforts in the use of Linux in schools reflects it's growing importance in Malaysia. This will indirectly encourage students to develop skills in designing software from young.

- The seperate LAN-Internet connections is based on one gateway per network. This restricts users from getting access from other LAN-Internet connections. A distributed gateway based on alternative routes to other gateways in different subnetworks will minimise the event of users having disconnection problems.

1.5 Scope

This project involves two ethernet based subnetworks located in two adjoining computer labs. The two labs are seperated by a distance of about 30 metres between the nearest PCs. Machines used are x86 and compatibles.

For Internet connection, two 56kpbs modems with public services telephone network (PSTN) connections are used. Each gateway will be installed with Linux IP masquerading as the server.

The project looks at the subnetworks from the following angles:

I. Internet access is based on dial up PSTN connections. This project is concerned with common Internet services like world wide web, ftp, telnetting, etc.

II. Cost reduction is viewed from the server perspective. The use of IP masquerading on the server is viewed as an alternative to proxy software based servers and this will show a vast reduction in costs.

III. Interconnection of subnetworks is based on and restricted to two adjoining sub LANs. Subnetworks will be connected based on routing.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This review focuses on issues in networking including definitions and design in internetworking. Also covered are hardware for internetworking such as bridges and routers. LAN Internet connection solutions using application level gateways are also discussed.

2.1 Local Area Network

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a school computer lab, or building (Forouzan, 1998). Rarely are LAN computers more than a mile apart. In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The

workstations can be less powerful than the file server, and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards in each computer. Beyda (1998) supports this description when he states that a local area network is a privately owned data communications system that provides reliable high-speed, switched connections between devices in a single building, campus, or complex. Networks that extend outside a single building, campus, or complex are not considered local area networks LANs are distinguished from other types of data networks in that they are optimised for a moderate size geographic area such as a single office building, a warehouse or a campus. The Institute of Electrical and Electronic Engineers (IEEE) states that LAN is a shared medium peer to peer communications network that broadcasts information for all stations to receive. As a consequence, it does not provide privacy. The LAN enables stations to communicate directly using a common physical medium on a point-to-point basis without any intermediate switching node being required. The network is generally owned, used and operated by a single organisation. This is in contrast to Wide Area Networks (WANs) that interconnect communication facilities in different parts of a country or are used as a public utility. These LANs are also different from networks, such as backplane buses, that are optimised for the interconnection of devices on a desktop or components within a single piece of equipment (IEEE 802 Standard ,1990).

When communication needs go beyond the local area, direct connection cables and LANs may not meet the distance requirements. Even with special cables and signal conditioners, these connectivity alternatives are limited to a radius of approximately six miles. When these limitations fall short of the distance requirements in a connectivity link, it is often necessary to communicate through a wide area telephone connection (Jordan, 1994).

The local area network (LAN) has come to play a central role in information distribution and office functioning within businesses and other organisations, including tertiary intstitutions. The major factors driving widespread use of LANs have been the profileration of personal computers, workstations, and servers (Fitzgerald, 1996).

With the dropping price of LAN hardware and software, LANs have become more numerous and larger. And with the increasing use of the Internet, the role of LAN has become essential in providing reliable and affordable access to the Internet.

Ethernet is the most widely used LAN technology. The original and most popular version of Ethernet supports a data transmission rate of 10 Mb/s. Newer versions of Ethernet called "Fast Ethernet" and "Gigabit Ethernet"

support data rates of 100 Mb/s and 1 Gb/s (1000 Mb/s). An Ethernet LAN may use coaxial cable, special grades of twisted pair wiring, or fiber optic cable. "Bus" and "Star" wiring configurations are supported. Ethernet devices compete for access to the network using a protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network (Tannenbaum, 1996).

2.2 Subnetworks

To make clear that the total communications facility may consist of multiple networks, the constituent networks are referred to as subnetworks. A network access protocol, such as Ehternet logic, is used to connect a computer to a subnetwork. This protocol enables the host to send data across the subnetwork to another host or, in the case of a host on another subnetwork, to a router (Stallings, 1997).

A bridge is a device that allows us to segment a large network into two smaller, more efficient networks. A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network (Tannenbaum, 1996).

The bridge manages the traffic to maintain optimum performance on both sides of the network. We might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol (Walrand, 1998). On an individual LAN datalink, each station on the LAN typically receives all messages that are transmitted. A receiving station uses the destination MAC address field in each frame it receives to determine if it should process the frame. With an extended LAN implemented using bridges, the bridges can filter some of the frames, but broadcast traffic generated on one LAN is propogated to all the stations on the extended LAN. Routers can be used to

interconnect a number of individual LANs or extended LANs in such a way that the traffic generated on one LAN is better isolated from the traffic generated on other LANs in the internet. A router performs its functions in the OSI model Network layer, as shown in Figure 3 (Martin, 1994).

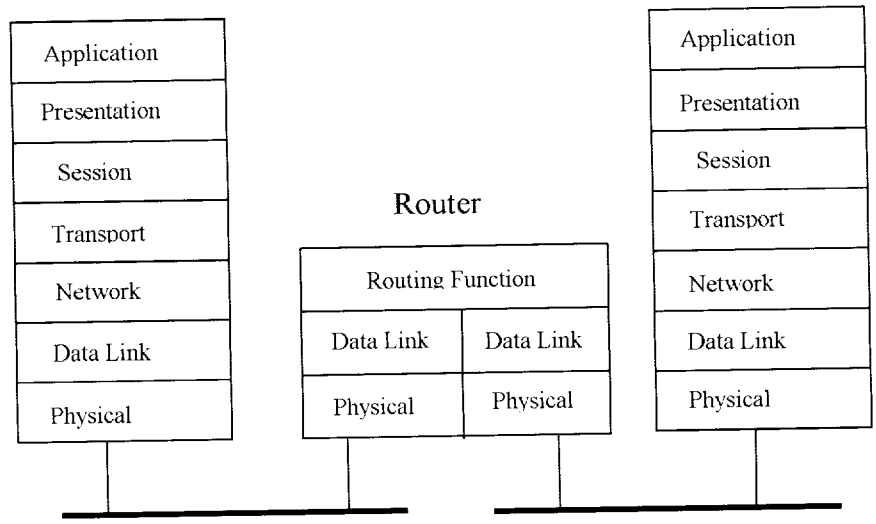


Figure 1 A router performs it's functions in the network layer

Most commercial routers available in the market today are beyond the means of most small organisations, especially schools and government funded colleges. An alternative cheap routing device, using the old 486 machines, could go a long way in overcoming the issue of cost in these types of organisations. Besides controlling LAN traffic, this device can also act as an Internet gateway, through the use of IP masq servers, for several existing subnetworks.

Routing can be divided into two processes i.e forwarding and topology discovery (Cisco Systems technology information, 2000). Forwarding involves looking up addresses on routing tables and making forwarding decisions. Discovery is what builds those routing tables. Large router networks like the Internet employ topology. These networks involve millions of host systems and subnets, and tens of thousands of different network paths. Some dynamic processes are essential to keep the routing tables in these networks up-to-date with respect to where devices are located and how packets can reach their destinations. Replacing discovery with manual control would generate many errors that traffic would never get from one place to another.

Though topology discovery is critical to big IP networks, it is not necessarily critical to all networks. Discovery lets routers find routes and subnetworks. But discovery is only valuable in networks where routes and subnets vary.

A subnet is a collection of IP users who can reach one other at LAN Level 2 i.e the Medium Access Control (MAC) layer. Anyone who wants to reach a user in another subnet has to use the Level 3 process of LAN internetworks i.e routing. Thus, routers have to know where subnets are.

In most LANs today, subnet addresses are assigned in a fairly static way, because IP addresses either have to have parameters as individual systems or be assigned using a Dynamic Host Configuration Protocol (DHCP) server (Gaskin, 1999). Once this process is set up, most managers leave addresses alone, so most private IP networks have relatively few changes in subnet addresses.

The dynamic discovery of routes is useful only if the network contains alternate routes. In other words, there is no reason to search for an alternate path to a destination if the network is built in a way that doesn't provide alternate paths. Many LAN hubs, switches, and routers are connected in a tree structure that provides no alternate paths.

Ideally, a private IP network would assign addresses based on topology. The highest-level division would be by site, such as designating one site as 10.1.x.x, another as 10.2.x.x, and so on. The next level would be to assign addresses by area within site, and so forth. Some users find site-based addresses helpful, but they can't adopt topology addressing within a site due to configuration changes. However, LAN switching will probably stabilize network structure for most users.

If static routing is used throughout, network managers will have to take care to prevent routing loops, and also insure that any new subnets are added to the tables if the current entries won't match the new subnets. For many, the benefits in eliminating topology updates and convergence delays will be well worth the trouble

Route selection is trivial when only a single path to the destination exists. However, if any part of that path should fail, there is no way to recover. Therefore, most networks are designed with multiple paths so there are alternatives in case a failure occurs.

Routing protocols compare route metrics to select the best route from a group of possible routes. Route metrics are computed by assigning a characteristic or set of characteristics to each physical network. The metric for the route is an aggregation of the characteristics of each physical network in the route (Cisco Systems technology information, 2000).

2.3 Proxy Servers

Proxy servers enable multiple users to connect to the Internet with just one dialup connection, and one account. They don't require a dedicated server. All that's required is that one of the machines in the network needs a modem and Internet access. That machine will be the one used for the proxy server. Another advantage of a proxy server is if the software is setup correctly, we have a secure connection to the Internet without fear of unauthorized access from the Internet to our LAN. Most proxy servers also set up a cache file on the host machine, so when pages are revisited by the other computers on the LAN, they load quickly. Most proxy servers will also allow us to log the pages that were visited by the other computers on the network. Depending on the proxy software we use, some require a server and client installation, others only need to be installed on the machine with the modem. Pricing varies from freeware up to thousands of ringgit depending on the number of users on the system.

One disadvantage is that in order to achieve a connection via a proxy server, the client software should be changed to support that proxy service. For example, to connect to a telnet server over a proxy, the user first have to be

authenticated by the proxy server then by the destination telnet server (Murhammer, 1998). This requires two user steps to make a connection rather than one.

Proxy servers work at the application level of the TCP/IP protocol stack (Murhammer, 1998). Figure 2 shows an example of FTP proxy server as viewed from the TCP/IP layers.

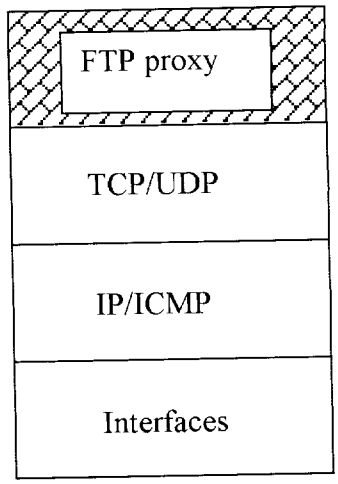


Figure 2 FTP proxy server application level

One example of proxy server software is AnalogX Proxy which is a small and simple server that allows any other machine on your local network to route it's requests through a central machine.

AnalogX Proxy run on the machine with the Internet connection; configure the other machines to use a proxy. You're surfing the web from any other machine on your network. It supports HTTP (web), HTTPS (secure web), POP3 (receive mail), SMTP (send mail), NNTP (newsgroups), FTP (file transfer), and Socks4/4a and partial Socks5 protocols. It also works with Internet Explorer, Netscape, AOL Instant Messenger, Microsoft Messenger, etc (Analog Proxy overview, 2000). An example screenshot is as in Figure 3.

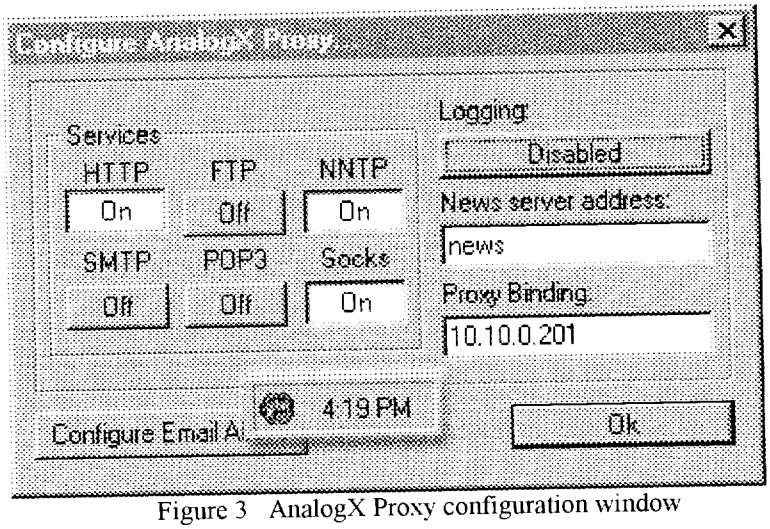


Figure 3 AnalogX Proxy configuration window

2.4 Linux

The word Linux refers specifically to the kernel, is also widely to refer to an entire operating system built around the Linux kernel. Linux is not public domain, nor is it shareware. It is free software, commonly called freeware or open source software and we may give away or sell copies, but we must include the source code. If we distribute any modifications, you are legally bound to distribute the source for those modifications. Linux is still free as of version 2.0, and will continue to be free. Because of the nature of the General Public License (GPL) to which Linux is subject, it would be illegal for it to be made not free. Linux runs on 386/486/Pentium machines with ISA, EISA, PCI and VLB buses (Linux Information Sheet, 2000).

As Linux is developed using an open and distributed model, instead of a closed and centralized model like most other software means that the current development version is always public so that anybody can use it. The result is that whenever a version with new functionality is released, it almost always contains bugs, but it also results in a very rapid development so that the bugs are found and corrected quickly (Cornes, 1997).

In contrast, the closed and centralized model means that there is only one person or team working on the project, and they only release software that they think is working well. Often this leads to long intervals between releases, long waiting for bug fixes, and slower development. The latest release of such software to the public is sometimes of higher quality, but the development speed is generally much slower.

In recent years Linux has exploded on the global server market. One main impetus is that Linux has a global community that is constantly developing new and better programs and drivers and delivering them over the Internet. This is a clear advantage over commercial in-house development in which the number of developers is limited to the amount that can fit within the office or budget. Linux can be used for a large variety of functions including software development, networking, and as an end-user platform. Linux is a low-cost, highly stable alternative to other more expensive operating systems. Additionally, one of the greatest features of Linux is the ability to adapt the operating system to individual needs.

2.5 IP Masquerading

Some operating systems, most notably Linux, have the capability to perform IP routing with the addition of changing the IP address in the packets, i.e. as the data is passed through from the LAN to the Internet. In IPRoute this feature is called Network Address Translation (NAT). The Linux version of NAT is referred to as IP Masquerading (Linux IP Masquerading, 2000).

IP Masquerading is a feature of the TCP/IP stack. The TCP/IP stacks in most commercial operating systems don't support IP Masquerading. At the moment only independent TCP/IP programmers feature IP Masquerading. As Linux comes with full source code, it makes it easier to implement IP Masquerading.

Masquerading allows a set of machines to invisibly access the Internet via the Masq gateway. To other machines on the Internet, all this outgoing traffic will appear to be from the IP Masq server itself. In addition to the added functionality, IP Masquerade provides the foundation to create a very secure networking environment. With a well built firewall, breaking the security of a well configured masquerading system and internal LAN should be considerably difficult.

The Linux IP masquerade resource (2000) states that whether the bandwidth is enough for sharing depends on what what we are going to do. If a few users often download files at the same time, then we should expect prolonged waiting time. However, if the users are only surfing the web and doing telnet, then it should be enough. IP masquerade can also be useful on a larger user base when it is dedicated for retrieving emails from, for example, a popmail server. The Internet connection is not limited to a modem line, we can use an ISDN line, DSL, cable modem, satellite link, or even T1/E1 if available.

Some examples of IP masquerade application support are chat categories like talk, phone and interactive communications systems; games; utilities applications, services, and programs of general usefulness; web programs specific to the web or web systems (Masq applications, 2000).

2.6 The Linux Router Project (LRP)

The Linux Router Project is a project to build a Linux based router. The Linux Router Project is a networking-centric micro-distribution of Linux. LRP is small enough to fit on a single 1.44MB floppy disk, and makes building and maintaining routers, access servers, thin servers, thin clients, network

appliances, and typically embedded systems next to trivial. LRP can be run on a 386SX machine with just 8MB. No harddisk is required. However, for more advanced routing purposes, a faster machine is suggested. It is also possible to boot LRP on a zip-drive or harddisk to accommodate for larger routers with multiple services running.

LRP supports all of the current routing capabilites of Linux with its 2.2 kernel. Examples are: BGP, OSPF, RIP, Cipe, Fair Queueing, Quality of Service, Traffic Shaping, and so on. LRP can also support other network protocols such as IPX or Appletalk. Figure 4 shows a typical set up of a simple LAN using LRP for Internet access. Connection can be made by LRP by using either a modem, ISDN or a cable modem.

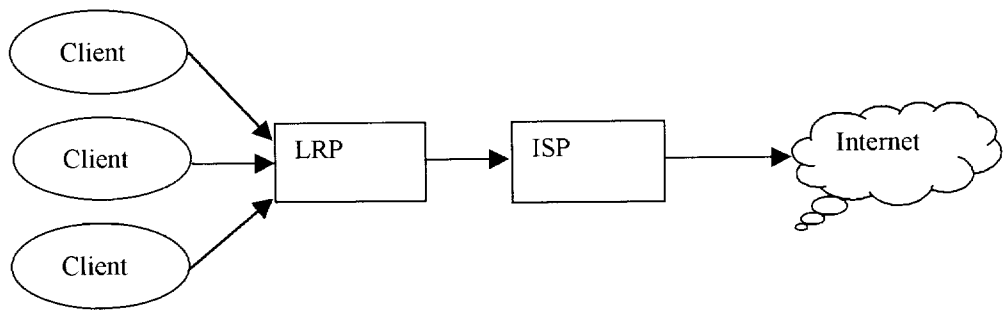


Figure 4 Clients accessing Internet through LRP

The Linux Router Project is aimed at both home users and businesses. It can be used to build a dialup gateway for a home LAN, but it can also be used for advanced routing tasks in corporate networks. Its flexibility, its size, the fact that it can use all of Linux's routing capabilities and it's modular design make the Linux Router Project one of the best applications of Linux in its field.

In comparison to commercial routers, a Linux Router can perform at the same level, as long as we adjust the hardware accordingly. The total cost for building a router is far below that for a commercial router. All an ethernet router requires for example, is two ethernet cards and a 486/66 with 16 MB of RAM (Wormgoor, 2000).

Even more advanced configurations are possible. Other possibilities using LRP are:

- Bridging
- Firewalling: Transparent Proxy, Port forwarding
- Traffic Management: Shaper, FairQ, QOS
- Advanced IP Routing: RIP, OSPF, BGP, Tunneling, IPSec
- Other protocols: IPX, appletalk

In terms of security, Linux is inherently secure because of its open source model. LRP can use all of Linux's security features. These are compiled into the kernel by default and can be turned on by the config scripts. One example is the prevention of IP Spoofing. This will prevent others from using our PC as a third-party host in ping attacks.

Because LRP is not just a router, but can also be configured as a firewall, it is easier to secure your company's network using LRP than it is using a commercial router. The LRP is based on IP Masquerading (Linux Router Project, 2000). Using IP Masquerading we can close off our entire internal network from the outside world. We can then open up specific ports such as POP, SMTP or the web to our internal network. Only these services will then be available to the outside.

The LRP works through a boot medium which contains a linux kernel, generic root archive, and package archives of addtional features to be merged with the rest of the root at boot time. When the disk is booted these archives are uncompressed and extracted into a ramdrive (/dev/ram0) then the ramdrive is mounted as root. The entire system runs solid state from ram. Any changes made to the root must be backed up to the boot medium, or they will be lost

after a reboot. The procedure to back up is menu based, and if need be, can be automated to take place at regular intervals.

Table 2 shows a brief summary of LRP characteristics.

Multi Interface	Ethernet, WAN (DS1+), Wireless, ISDN, Serial, Parallel
Multi Protocol	RIP in base, BGP IP-IP OSPF and others via packages
IP Control	Policy firewall, IP Masquerade (NAT), port redirection, port translation, port load balancing, transparent proxy, numberless interface spanning, interface load balancing, interface aliasing
Support	Vast resources, and HOW-TO's. Active mailing list. Commercial software support and hardware solutions available

Table 2 Characteristics of LRP

2.7 Differences between IP Masquerade and proxy services

A proxy server uses only one public IP address, like IP Masq, and acts as a translator to clients on the private LAN (web browser, etc.). This proxy server receives requests like telnet, FTP, world wide web, etc. from the private network on one interface. It would then in turn, initiate these requests as if someone on the local box was making the requests. Once the remote Internet server sends back the requested information, it would re-translate the TCP/IP addresses back to the internal Masq client and send traffic to the internal requesting host. Proxy servers can also do caching (Squid for web caching). So, if we have 30 proxied hosts all loading Netscape at once and if they were installed with the default homepage URL, we would have 30 copies of the same Netscape web page coming over the WAN link for each respective computer. With a caching proxy server, only one copy would be downloaded by the proxy server and then the proxied machines would get the web page from the cache. Not only does this save bandwidth on the Internet connection, it will be faster for the internal proxied machines (Roth, 2000).

Many Network Access Terminal (NAT) is similar to a proxy server in the sense that the server will do IP address translating and fake out the remote

server, for example the world wide web, as if the Masq server made the request instead of an internal machine.

The major difference between a Masq and proxy server is that Masq servers don't need any configuration changes to all the client machines. Just configure them to use the linux box as their default gateway (Roth, 2000).

CHAPTER 3

METHODOLOGY

3.0 Introduction

The project was conducted as follows:

1. Choosing a suitable IP Masquerading software
2. Setting up and configuring a LAN Internet gateway
3. Interconnecting sub LANs for access to the Internet
4. Ensuring a continuous Internet connection in all sub LANs

For this project, the freesco 2.6 distribution downloaded from http://www.freesco.org was used for the Internet gateway, mainly because it provides ease of use and flexibility, in particular for interconnection of sub LANs.

There are few changes to the current LAN Internet connection set up i.e using the proxy server approach. Changes made to client machines are minimal. The only major change is the computer server which utilises the routing approach.

A comparison of the proxy server model and the IP masquerading model is as follows:

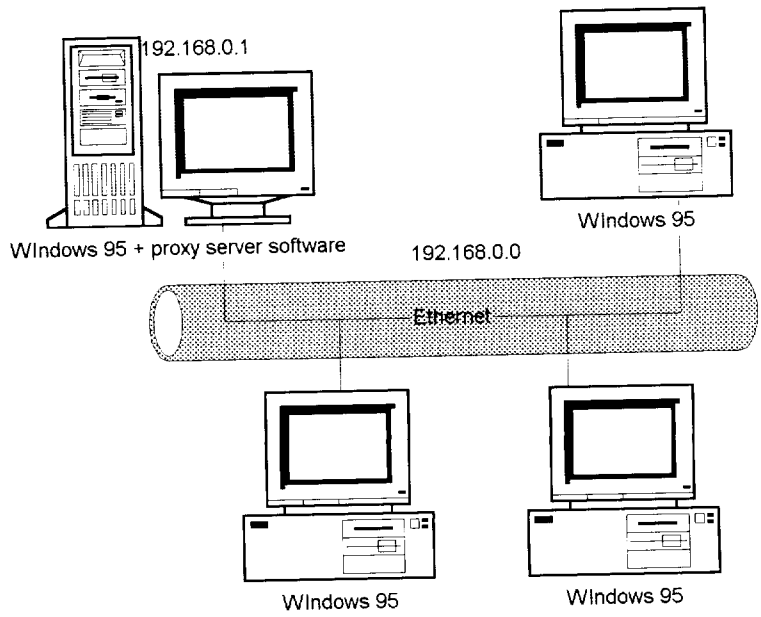


Figure 5 Existing computer lab model

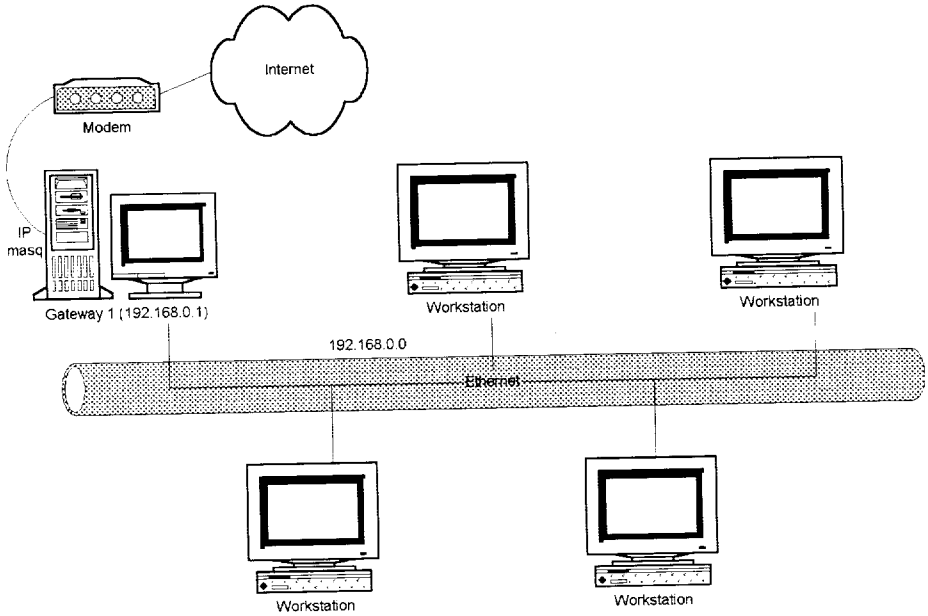


Figure 6 An example of computer lab model using the IP masquerading method

The minimum requirements for the gateway are:

- CPU - any 386 or better
- RAM - min (with swap) 6 MB, normal 8 MB, recommended 16 MB
- FDD - 1.44 MB
- HDD - not required for 8-16 MB RAM system, but recommended.
- Ethernet adapter(s) - 3COM509, 3COM595, 3COM905, Realtek NE2000 compatible, Realtek NE2000 PCI compatible, ISA/PCI NE2000 compatible supported out of box.
- Modem(s) - most modems except winmodems will work with FREESCO.

This project was implemented at Maktab Perguruan Tuanku Bainun, Pulau Pinang using Pentium 133 MHz and Celeron 500 MHz for client machines and Pentium 133 MHz for the servers.

The LAN was created by direct connection of computers using:

- 10base2 cables
- Network terminators
- Network interface cards (NIC), 1 per networked computer
- Server

For this project ISA NE2000 compatible NICs are used.

For Internet access, dial up lines with 56 kpbs modems were used. While leased lines can be expensive and not always readily available, the telephone network is accessible everywhere. So, dial-up connection over telephone lines was chosen for connecting LANs to Internet. Point to Point (PPP) protocol is used over voice phone lines.

3.1 LAN Internet connection through the use of IP masquerading servers.

For implementation of the above, the following has to be resolved.

1. Setup of servers i.e gateway 1 for network 192.168.0.0 and gateway 2 for network 192.168.10.0.

2. Configuration of client machines in networks 192.168.0.0 and 192.168.10.0.

For this project, a Pentium 133 PC, with 41MB HDD, 1.44 MB FDD and 16 MB RAM was used for gateway 1 of first network and for gateway 2, the hardware used is similar to gateway 1. DNS server is set as 192.168.0.1 for

gateway 1 and for gateway 2, the DNS server is set as 192.168.10.1. For client machines in both networks, there were not much configuration being made since IP addressing was set automatic because DHCP was enabled.

3.2 Internet connection through an alternative subnetwork

For interconnection of both networks 192.168.0.0 and 192.168.10.0 in the second phase of the project, there are two practical choices, namely:

- Bridging
- Routing

For this project, routing was used. Routers can be used to interconnect extended LANs in such a way that the traffic generated on one LAN is better isolated from the traffic generated on the other LAN (Walrand, 1998). Two network interface cards (NIC) were installed to fascilitate interconnection of the sub LANs. Thus both gateways not only provide access to the Internet but also act as internal routers interconnecting both sub LANs.

The second phase of the project interconnects two sub LANs as illustrated in Figure 7.

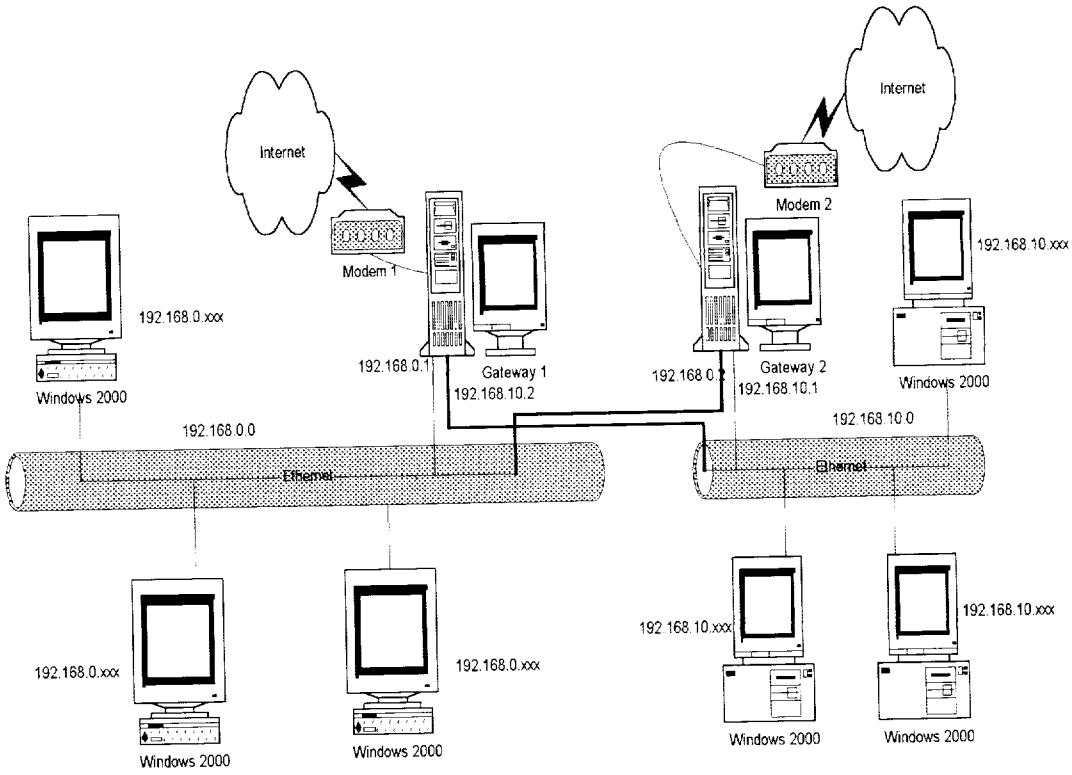


Figure 7 An example of two interconnected sub LANs using IP masquerading

This approach enables clients on network 192.168.0.0 to also access the Internet through gateway 2 and clients on network 192.168.10.0 to access the Internet through gateway 1 in the event of a connection failure in either networks.

The set up for both gateways are now different from the first phase where the sub LANs were seperated. The IP addresses of the first and second network interfaces respectively in gateway 1 are 192.168.0.1 and 192.168.10.2 whereas for gateway 2, the IP addresses are 192.168.10.1 and 192.168.0.2.

The client machines on both subnetworks were configured so that each PC on each subnetwork is able to access the Internet either from gateway 1 or gateway 2. With Windows 2000 installed on all client machines, network 192.168.0.0 was configured with the preferred DNS server being 192.168.0.1 and the alternate DNS server is 192.168.0.2. Client machines on network 192.168.10.0 were similarly configured with the preferred DNS server now being 192.168.10.1 and alternate DNS server is 192.168.10.2.

Since all internal IP masqueraded machines should not have official Internet assigned addressees, there must be specific and accepted way to allocate addresses to those machines without conflicting with anyone else's Internet addresses.

RFC 1918 is the official document on which IP addresses are to be used on a non-connected or private network. There are 3 blocks of numbers set aside specifically for this purpose. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

The first block is referred as 24-bit block, the second as 20-bit block, and to the third as 16-bit block. The first block is a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 255 contiguous class C network numbers. For this project, the preference is to use the 192.168.0.0 network with a 255.255.255.0 Class-C subnet mask for the first sub LAN and 192.168.10.0 network with a 255.255.255.0 Class-C subnet mask for the second sub LAN. 192.168.0.1 and 192.168.10.1 are the internal gateways to get out to the external network. 192.168.0.0, 192.168.10.0 and 192.168.0.255, 192.168.10.255 are the network

and broadcast addresses respectively (these addresses are reserved). These addresses are avoided to enable the network to work properly.

DNS server converts Internet addresses between human readable form (example: www.abc.net) and computer readable form (example: 195.2.83.113) and back This local caching DNS server can reduce traffic between the local network and and Internet Service Provider (ISP) and increase speed of connections to servers on the internet (Gaskin, 1999). To set up DNS server we have to know the ISP DNS address. For this project, since the ISP used is the one provided by TMNet, the ISP DNS address is 202.188.0.133.

DHCP server provides automatic configurations of the local networks computers. It makes the job of network administrator easier. Every computer on the network must have his own IP address and it must also know the DNS address and gateway. DHCP server supply every computer on the network with this information (Gaskin, 1999). For this project, the DHCP is enabled for configuration on the local clients and DHCP server will do the rest, otherwise we have to enter all this addresses manually.

We can have full access to the gateway via telnet connection. Unlike http control service in the Freesco web panel, it doesn't have any restrictions and we can edit the config files from the workstation via telnet connection.

Another component required to use Internet resources is application software for workstations, which are IBM PC compatibles with the MS Windows 2000 operating system. This version of MS Windows is better equipped with Internet client software, in particular Internet Explorer compared to previous versions.

The other applications covered in each workstation have at least the following Internet services:

- Telnet (client with a VT100 / VT220 emulation).
- FTP (client with graphical user interface).
- WWW (Netscape Navigator version 4.0 onwards besides Windows 2000 built in Internet Explorer).

Helper applications were also included to support:

- MPEG audio and video files.
- PostScript files.
- PDF (Portable Document Format) files.
- Compressed files (ZIP, Z, GZ, TAR)

The majority of the above applications are free, some of them are low cost shareware.

CHAPTER 4

FINDINGS

4.0 Introduction

This project looks at the development of computer lab models based on the IP masquerading LAN Internet gateway as well as the interconnection of two sub LANs for connection to the Internet.

4.1 LAN-Internet connection through the use of IP masquerading servers.

Configuration of client machines were done without any problems. For the first network, i.e 192.168.0.0, every client machine were able to detect each other using the built in Packet Internet Groper (PING) program for Windows 2000. With Dynamic Host Configuration Protocol (DHCP) enabled, every client on the network have their own assigned IP addresses. The same is true for the second network, 192.168.10.0. Unlike proxy servers, through IP masquerading there is no need for any configuration of browser programs on client machines for access to the Internet.

For server set up, the freesco distribution was downloaded in 3 minutes and initially installed on a 1.44 MB floppy disk. Once booted from the floppy, it was copied and moved to the hard disk without any problems. This was to make use of swap file from the hard disk to increase amount of memory. Setting up the gateway from the hard disk in network 192.168.0.0 was done without any problems. The modem and the NIC were also detected without much problems. The same was observed for network 192.168.10.0.

Once the freesco gateways at 192.168.0.1 and 192.168.10.1 were up and running, clients in each network were able to utilise the web control panel. However this was restricted to trusted users with password access provided by the administrator. Figure 8 shows an example of a web control panel screen as viewed from client in network 192.168.0.0.

Once the network setup enabled the PCs to communicate and gateways were properly configured, web access and other basic Internet services was readily available. This shows that a basic PC with minimal hardware and software resources can be a reliable LAN Internet server, thus drastically reducing costs as compared to a proxy software server based approach.

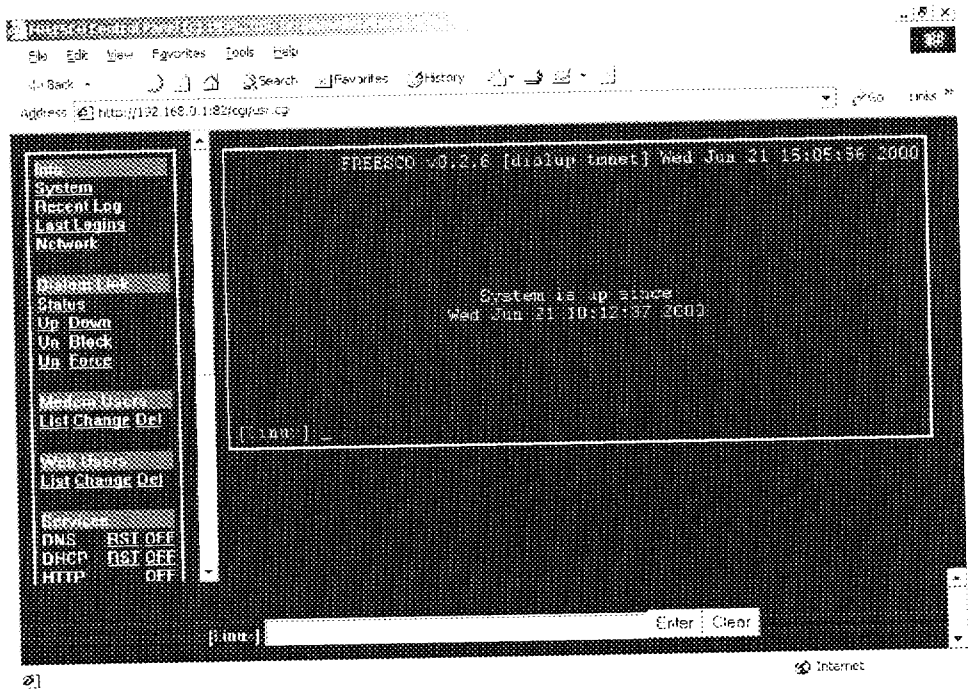


Figure 8 Freesco web control panel

4.2 Continuous Internet connection through an alternative subnetwork.

Freesco 2.6 was installed in both servers without much problems except for the detection of the two NICs on each server for alternative Internet connections. However, this was eventually overcome by first checking the BIOS and making sure there was no conflict with an existing serial port or IRQ. After checking the file var/log/log it was learned that names eth0 and eth1 have been

swapped. The alternative was to swap the interface names in advanced setup in freesco through options 72 and 73 from memory, change "first network interface" to eth1 and second to eth0.

With the gateways also functioning as internal routers in each network, client machines in each network were able to communicate with each other through these routers.

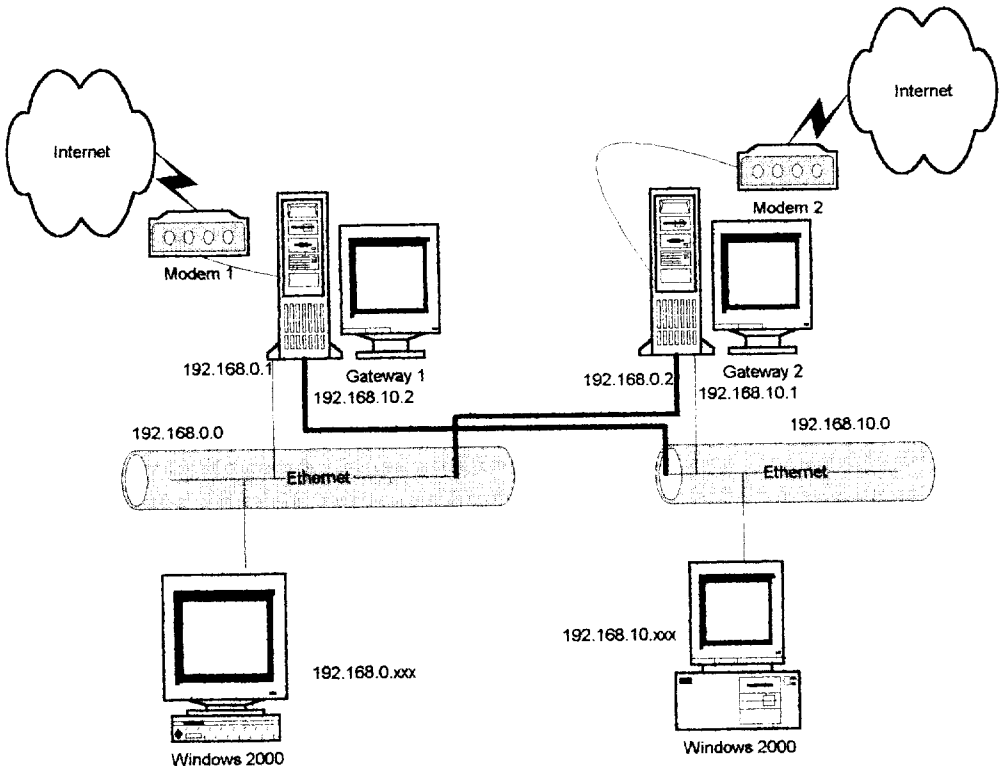


Figure 9 Distributed gateway

Once the network setup enabled the PCs to communicate and gateways were properly configured, access to the Internet was not a problem. Both gateways in networks 192.168.0.0 and 192.168.10.0 were very stable especially in low traffic. Heavy traffic affected access speeds, especially when both computer labs, consisting of 20 PCs each, were fully occupied although this situation of maximum use of Internet in both sub LANs was rare. However, speed problems were negligible for basic use such as surfing the web.

Modem 1	**Modem 2**	**Clients in network**	**Internet**
On	Off	192.168.0.0 and 192.168.10.0	On
Off	On	192.168.0.0 and 192.168.10.0	On

Table 3 Internet access in subnetworks

As shown in Table 3 (refer also Figure 9), it was also found that a disconnection of modem in one sub LAN, did not affect access to the Internet as long as connection in the other sub LAN was secure. This conforms with findings in the paper 'Designing Large-Scale IP Internetworks' from Cisco Systems technology information (2000) that most networks are designed with multiple paths so there are alternatives in case a failure occurs. Other factors

beyond control, for example PSTN line disturbances and TMnet server problems affected Internet access.

4.3 Hints and other findings

- There are several online technical documentations, including HOWTOs on IP masquerading.

- For editing and configuration purposes on freesco via telnet, there are some problems with the built in Windows 2000 telnet program. Try a different telnet client, like PuTTY.

- It is recommended to use hard disk drive compared to floppy disk. Its faster on booting and least succeptable to error. The swap file is a good feature especially if we are using it as a print server.

- In internet options in the browser software make sure access to the Internet via a proxy server is disabled. However do check connect to the Internet via LAN.

- If we want to run the gateway without display and keyboard/mouse hardware as well, be sure to configure the BIOS to operate without a keyboard so that the machine will automatically boot without errors after power failures or other problems.

- To immediately boot the gateway so that Internet connection will be available when client machines boot up, edit the user script, /rc/rc_user and put a line under the startup section: control up.

- Use internal ISA modems because it has some advantages over external modems, for several reasons:

    1) They have built in 16550A UART chips, which means we get proper performance on old machines even if the ports in the machines are only slow 16450/8250's.

    2) They're usually slightly faster because we don't have the added latency of sending the data over a serial cable.

CHAPTER 5

DISCUSSION AND CONCLUSION

5.0 Discussion

Computer labs with Internet access based on IP masquerading can be a viable alternative to those based on the current set up of proxy servers mostly using ethernet networks and dial up modems on PSTN telephone lines. The presence of distributed gateways also ensures broken access to the Internet is kept to a minimum. This is an important feature in IP masquerading which provides an option for alternate gateways where this is not available in proxy server softwares. The server set up, using the freesco 2.6 distribution is not too complex and if suitable hardware is chosen, any problems that may arise can be easily overcome. Although client PCs need not necessarilly be Windows based, Windows 2000 was maintained in the PCs as it was originally installed in the previous proxy server based network. The ethernet wired with 10 base2 coaxial cables is the current network design with very minor changes being made for this project. The only alterations made were for the purpose of interconnection of sub LANs using the two NICs installed in both gateways.

5.1 Suggestion for a computer lab model

Computer labs today needs to be networked and have access to the Internet. Unfortunately, this has become a costly affair, more so for schools and colleges with very limited budget. The increasing popularity of Linux as the alternative to Windows could be a blessing for these types of organisations. In line with the Malaysian National Information Technology Council's proposal (Computimes; August 7, 2000) to create equitable access to information among the people, the further decrease on hardware and software costs can be a contributing factor towards realising this goal and hence address the digital divide among the people. The recent encouraging breakthrough in the development of molecular electronics (IN-TECH; August 1, 2000) which promises to revolutionise computer processor speed with tremendous cost savings is another positive development.

Used 486 machines can be purchased at minimal cost these days. These machines, with some extra RAM and hard disk space added on, are enough for Linux to run on.

Suggestion for Server

1. Freesco IP masquerading server using Pentium 100 MHz.

2. Print servers based on freesco IP masquerading using 486DX-100 MHz machines.

Suggestion for Clients

1. 486DX-100 MHz machines using the Linux OS.

2. Office suite based on the Linux OS, for example Staroffice, which is another free application.

3. For Internet browsing, Netscape for Linux.

A possible design of interconnected computer labs could be as follows.

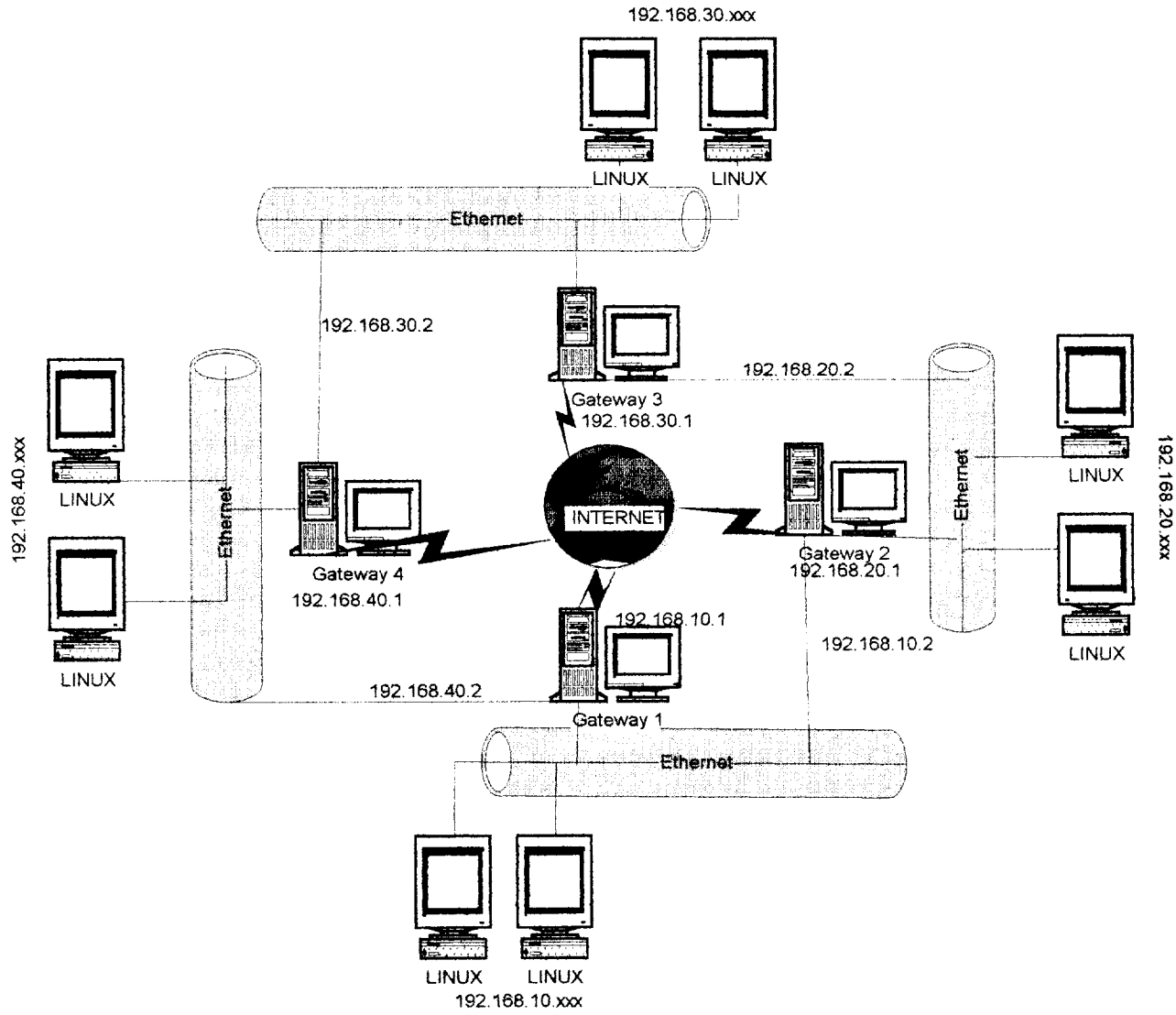


Figure 10 Distributed gateway of subnetworks in a Linux only environment

5.2 Conclusion

Freesco was developed in the open source tradition as an alternative to routing products offered by the more established networking hardware solution providers. This provides management one way to decrease expenses.

This research is far from complete in terms of providing a cost effective solution in the utilisation of sub networks for Internet access but the free and open source environment of Linux of which this project's IP masquerading is based on, can be further exploited to addresss issues such as bandwidth. If this can be overcome it will hopefully increase user satisfaction, particularly access to the Internet in a LAN environment. Coupled with the potential of the increased use of diskless computers and the future development of molecular electronics, further cost reduction is possible.

Implementing a functional internetwork is no simple task. Many challenges must be faced in areas like connectivity, reliability, network management and flexibility. Each area is key in establishing an efficient and effective internetwork.

Another essential consideration, reliable service, must be maintained in any internetwork. Individual users and entire organizations depend on consistent, reliable access to network resources. Furthermore, network management must provide centralized support and troubleshooting capabilities in an internetwork. Configuration, security, performance, and other issues must be adequately addressed for the internetwork to function smoothly. Flexibility, the final concern, is necessary for network expansion and new applications and services, among other factors.

REFERENCES

Roth, Steve., (2000). Proxies vs. NAT.
http://www.homepclan.com/proxynat.htm (15 June 2000)

Martin, James., (1994). Local Area Networks (2nd Edition). Englewood Cliffs, N.J.: Prentice Hall International, Inc.

Beyda, William J., (1996). Data Communications, From Basics to Broadband (2nd Edition). Englewood Cliffs, N.J.: Prentice Hall International, Inc.

Wingate Pricing Page (2000)
http://wingate.deerfield.com/pricing/(15 June 2000)

Local and Metopolitan Area Networks Overview and Architecture., (1990). IEEE 802 Standard

W. Murhammer, Martin., (1998). TCP/IP Tutorial and Technical Overview (6th Edition).Upper Sadle River, N.J.: Prentice Hall International, Inc.

Cornes, Phil.,(1997). The Linux A-Z. Hertfordshire.: Prentice Hall Europe

Stallings, William., (1997). Local and Metropolitan Area Networks (Fifth Edition). Upper Sadle River, N.J.: Prentice Hall International, Inc.

E. Gaskin, James., (1999).Mastering Netware 5. Alameda, CA.: Sybex, Network Press.

Freesco - free replacement for commercial routers (2000). http://www.linuxsupportline.com/~router/(10 June, 2000)

Jordan, Larry & Churchill, Bruce.,(1994). Communications and Networking for the PC (Fith Edition). Indianapolis, Indiana.: New Riders Publishing.

Analog Proxy overview (2000). http://www.analogx.com/contents/download/network/proxy.htm (12 April, 2000)

Linux IP Masquerading (2000). http://www.indyramp.com/masq/ (2 July, 2000)

Wormgoor, Mark.,(2000). Linux Router Project - Abstract for Linuxtag. http://www.linuxrouter.org/ (21 July, 2000)

IN-TECH, The Star. (18 July 2000).

Linux Router Project (LRP) (2000) http://www.linuxrouter.org/ (29 July, 2000)

Masq applications (2000)
http://www.tsmservices.com/masq/ (18 July, 2000)

Cisco Systems technology information (2000)
http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2003.htm#xtocid1338 (10 July, 2000)

Linux Information Sheet.
http://www.ibiblio.org/mdw/HOWTO/INFO-SHEET-1.html (30 August, 2000)

Linux IP Masquerade Resource(2000).
http://mirrors.indyramp.com/ipmasq/ipmasq-HOWTO-1.82-3.html#ss3.2 (30 August, 2000)

Fitzgerald, Jerry & Dennis, Alan., (1996). Business Data Communications and Networking (5th Edition). New York.: John Wiley.

Forouzan, Behrouz., (1998). Introduction to Data Communications and Networking. San Francisco.: McGraw Hill.

Stallings, William., (1997). Data and Computer Communications (Fifth Edition). Upper Sadle River, N.J.: Prentice Hall International, Inc.

Stamper, David A. (1994). Local Area Networks. Redwood City.: Benjamin/Cummings Publishing Company.

Tannenbaum, Andrew S. (1996). Computer Networks (3rd Edition). Upper Sadle River, N.J.: Prentice Hall International, Inc.

Walrand, Jean (1998). Communication Networks: A First Course (2nd Edition). San Francisco.: McGraw Hill.

Computimes, The New Straits Times. (7 August, 2000).

APPENDIX A

1.0 INSTALLATION OF FREESCO 2.6

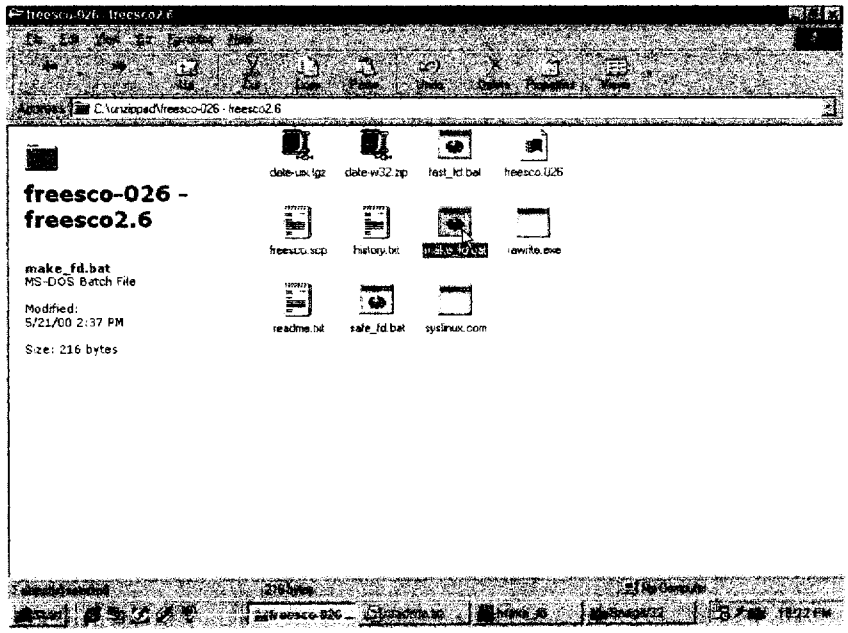
This installation is suitable on the Intel microprocessor as well as others compatible with it.

1.1 Installing on a floppy disk

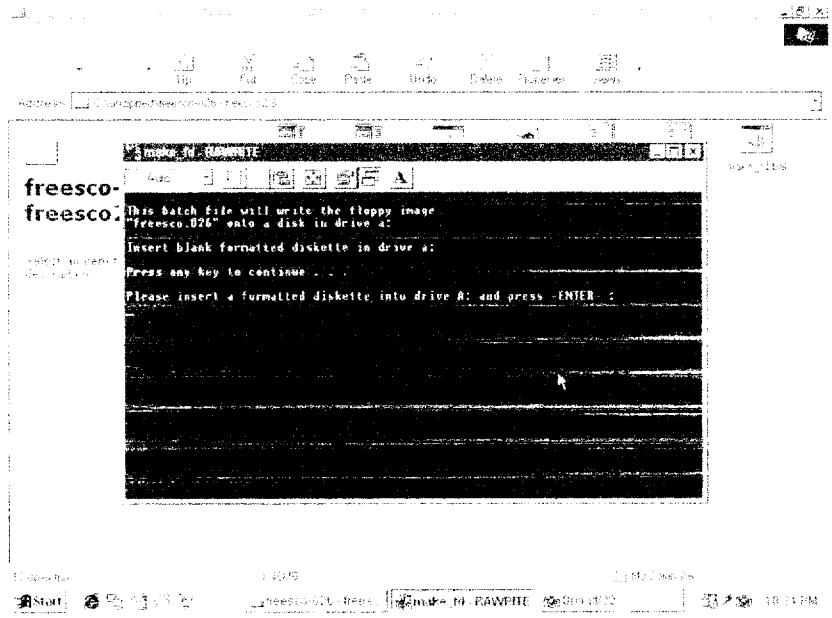
1. After downloading from http://www.freesco.org, the following file is obtained.

2. Unzip the the above file using a suitable application, e.g. Winzip.

3. The following files are then obtained. Click make_fd.bat.



4. Insert a floppy disk and press Enter.



1.2 Installing on a hard disk

I. Boot from floppy as prepared in 1.1. Login as root, password: root and execute:

move2hdd.

II. Remove the floppy disk and boot from hard disk to set up the server.

Setup of the server (Gateway 1)

This setup is for the server in the first phase of the project in which the subnetworks 192.168.0.0 and 192.168.10.0 are not yet interconnected. The following setup is shown for gateway 1 (192.168.0.1). Gateway 2 (192.168.10.1) should be similarly configured with relevant changes done where necessary.

Type *setup* from the Linux prompt.

[Linux] setup

The following message will appear.

Three steps of setup:

1) choose router type and set it up

2) change advanced settings

3) save config, exit and reboot system

Press ENTER to continue

d) Dialup line router: ISP <- modem0 -> router <- eth0 -> local net 1

Type D when prompted for choice as follows.

Choice []? D

The following dialog will appear. The default answers are in brackets.

711 Hostname of this computer [router]?

712 Domain name [home]?

8xx How many network interface cards do you have (1-3) []? 1

811 I/O port address of 1st ethernet card [0x300]?

812 IRQ line of 1st ethernet card [11]?

720 Use DHCP client to configure 1st network interface y/n [n]?

721 Interface name eth0/arc0e/arc0 [eth0]?

722 IP address of 1st network interface [192.168.0.1]?

723 Network mask [255.255.255.0]?

724 IP range [192.168.0.11 192.168.0.60]?

411 Enable caching DNS server y/s/n [y]?

412 Enable DNS requests logging for debug purpose y/n [y]?

421 Enable DHCP server y/s/n [y]?

422 WINS address (if you have one, otherwise - '-') []?

423 Default-lease-time,max-lease-time (sec) [86400,86400]?

431 Enable public HTTP server y/s/n [y]?

432 Public HTTP server IP port [80]?

441 Enable time server and router control via HTTP y/s/n [y]?

442 Control HTTP server IP port [82]?

443 Host Time server address, '-' - disable time service [www.clock.org]?

444 Time offset to UTC(GMT) [+0800]?

451 Enable Print Server(s) y/s/n [n]?

46 Enable telnet server y/s/n [y]?

14 Savers - screen(min),hdd(x5 sec) 0 -off [0,0]?

15 Swap file size in kbytes (on boot device). 0 - disable [24768]?

13 Do you want to enable extra modules/programs y/n [n]?

16 Log sizes in bytes. syslog,logins_log [30000,3000]?

47 Do you want to export services y/n []?

480 Do you want DynDNS client y/n/- []?

30 ISP/connection name (1-8 chars) []? tmnet

31 ISP phone numbers []? T1515

32 Keep up the ppp link for N sec. 0 - use filter.cfg; 1 - forever. []? 1

33 ISP DNS address []? 202.188.0.133

34 ISP http proxy address, (otherwise '-') []?

35 Does your ISP give you a dynamic IP address [y]?

38 Authentification method - pap/chap/script [script]? chap

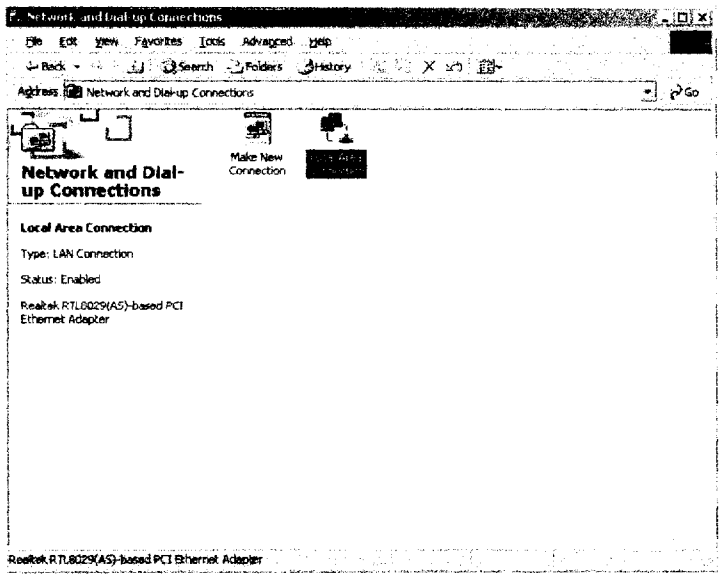
R0 Login name []? mptb

R1 Password []? mk3tmp

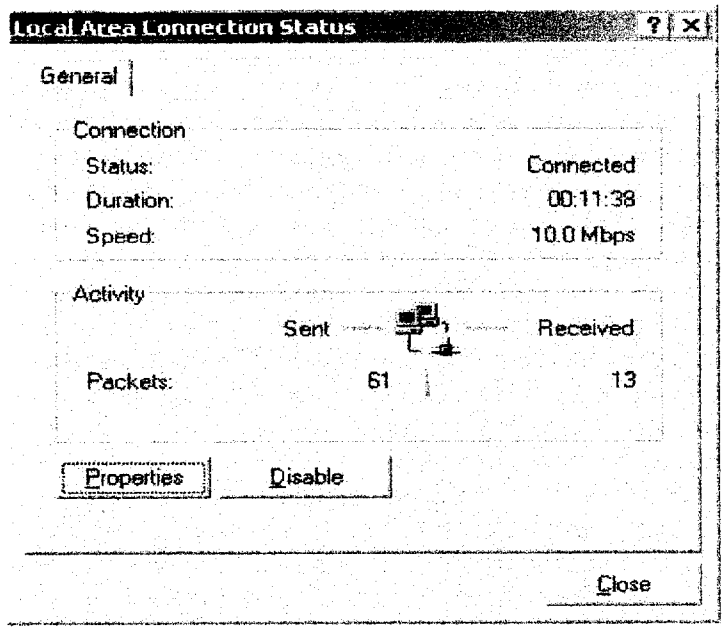
Press ENTER to continue

The server is now ready as an Internet gateway.

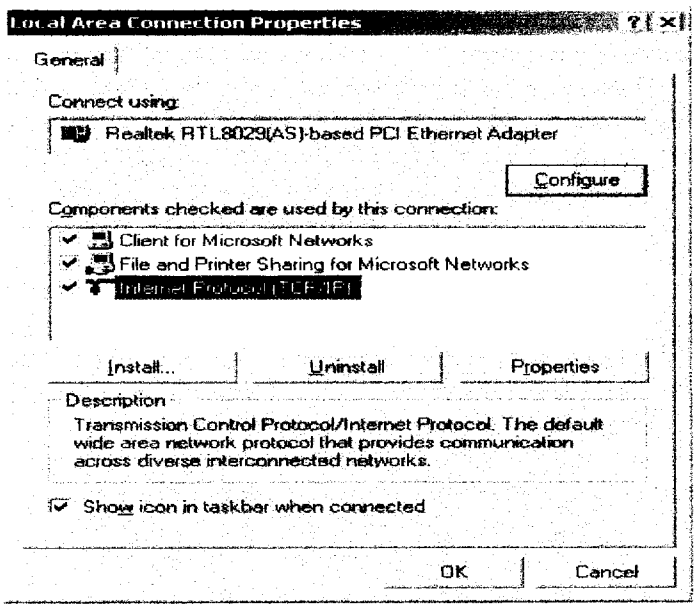
Setting up the client machines (first phase)



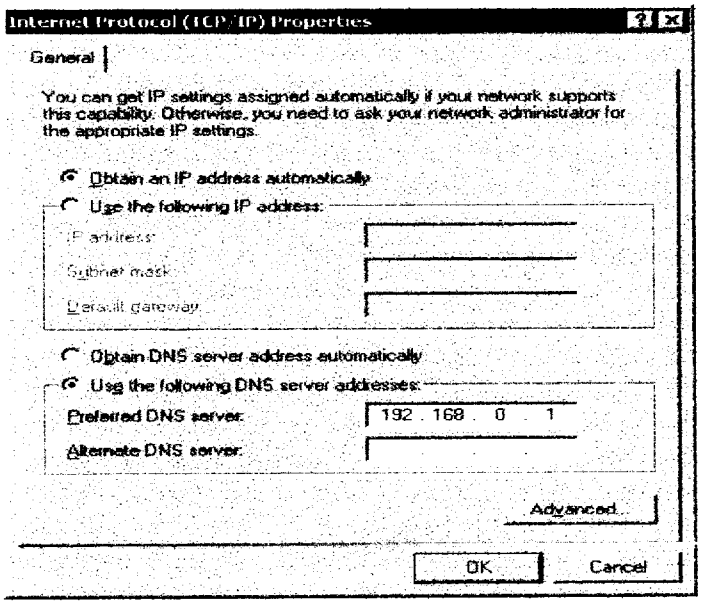
Right click Local Area Connection.



Click Properties.



Make sure the above components are checked. Double click TCP/IP.



Fill in the preferred DNS server. For gateway 1, 192.168.0.1. For gateway 2 in the other subnetwork, preferred DNS server is 192.168.10.1.

Setup of the server in an interconnected network

This setup is for the server in the second phase of the project in which the subnetworks 192.168.0.0 and 192.168.10.0 are interconnected. This server has IP addresses 192.168.10.1 and 192.168.0.2 to serve both subnetworks.

Type *setup* from the Linux prompt.

[Linux] setup

The following message will appear.

Three steps of setup:

1) choose router type and set it up

2) change advanced settings

3) save config, exit and reboot system

Press ENTER to continue

d) Dialup line router: ISP <- modem0 -> router <- eth0 -> local net 1

Choice []? D

The following dialog will appear. The default answers are in brackets.

711 Hostname of this computer [bestari]?

712 Domain name [home]?

8xx How many network interface cards do you have (1-3) []? 2

811 I/O port address of 1st ethernet card [0x220]?

812 IRQ line of 1st ethernet card [5]?

821 I/O port address of 2nd ethernet card [0x300]?

822 IRQ line of 2nd ethernet card [3]?

720 Use DHCP client to configure 1st network interface y/n [n]?

721 Interface name eth0/arc0e/arc0 [eth0]?

722 IP address of 1st network interface [192.168.10.1]?

723 Network mask [255.255.255.0]?

724 IP range [192.168.10.2 192.168.10.100]?

731 Interface name eth1/eth0:1/arc1e/arc0e:1/arc1/arc0:1 [eth1]?

732 IP address of 2nd network interface [192.168.0.2]?

733 Network mask [255.255.255.0]?

734 IP range [192.168.0.3 192.168.0.100]?

411 Enable caching DNS server y/s/n [y]?

412 Enable DNS requests logging for debug purpose y/n [y]?

421 Enable DHCP server y/s/n [y]?

422 WINS address (if you have one, otherwise - '-') []?

423 Default-lease-time,max-lease-time (sec) [86400,86400]?

431 Enable public HTTP server y/s/n [y]?

432 Public HTTP server IP port [80]?

441 Enable time server and router control via HTTP y/s/n [y]?

442 Control HTTP server IP port [82]?

443 Host Time server address, '-' - disable time service [www.clock.org]?

444 Time offset to UTC(GMT) [+0800]?

451 Enable Print Server(s) y/s/n [n]?

46 Enable telnet server y/s/n [y]?

14 Savers - screen(min),hdd(x5 sec) 0 -off [0,0]?

15 Swap file size in kbytes (on boot device). 0 - disable [24768]?

13 Do you want to enable extra modules/programs y/n [n]?

16 Log sizes in bytes. syslog,logins_log [30000,3000]?

47 Do you want to export services y/n []?

480 Do you want DynDNS client y/n/- []?

30 ISP/connection name (1-8 chars) []? tmnet

31 ISP phone numbers []? T1515

32 Keep up the ppp link for N sec. 0 - use filter.cfg; 1 - forever. []? 1

33 ISP DNS address []? 202.188.0.133

34 ISP http proxy address, (otherwise '-') []?

35 Does your ISP give you a dynamic IP address [y]?

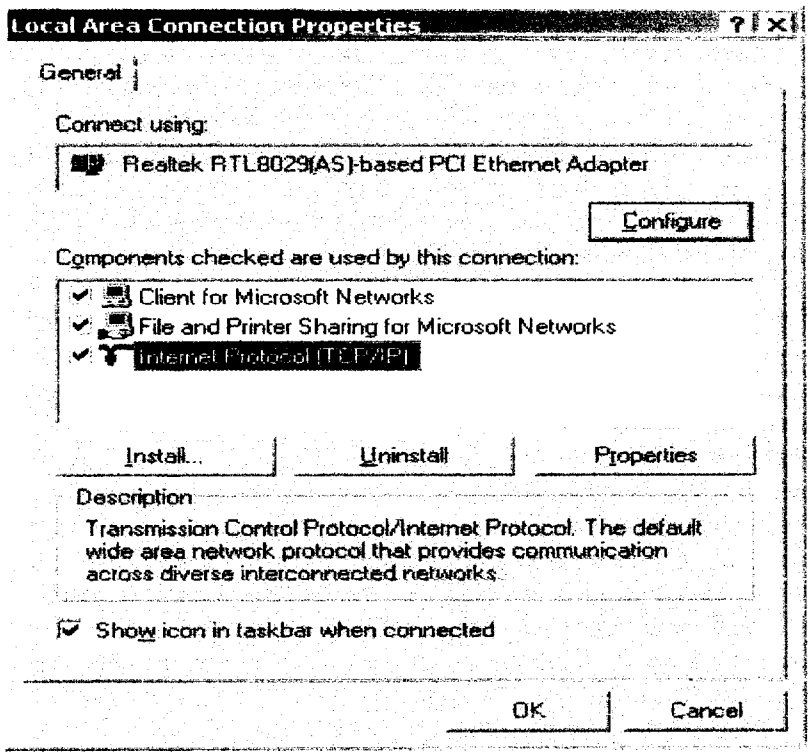
38 Authentification method - pap/chap/script [script]? chap

R0 Login name []? mptb

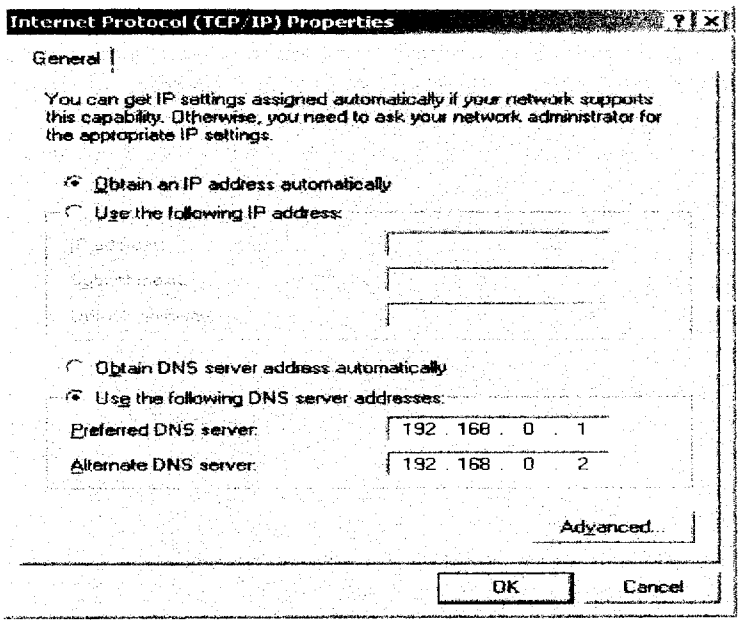
R1 Password []? mk3tmp

Setting up the client machines (second phase)

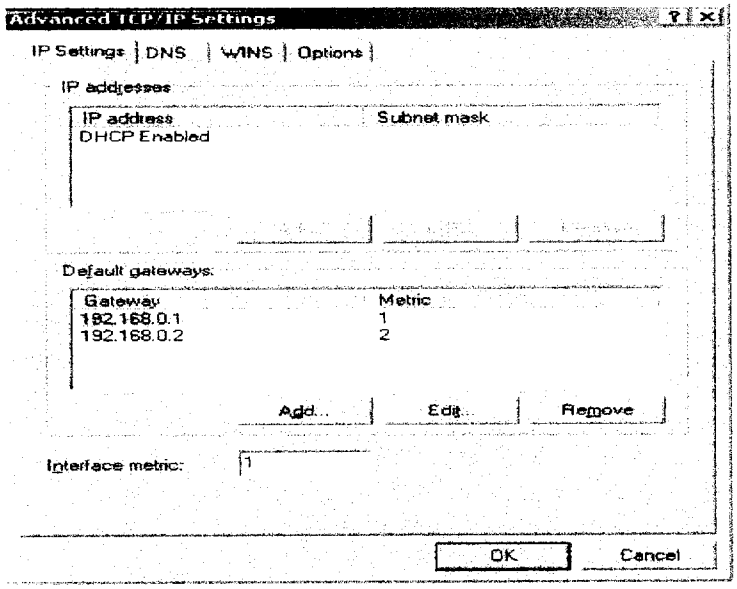
The two subnetworks are now interconnected through gateways 1 and 2.



Double click TCP/IP.

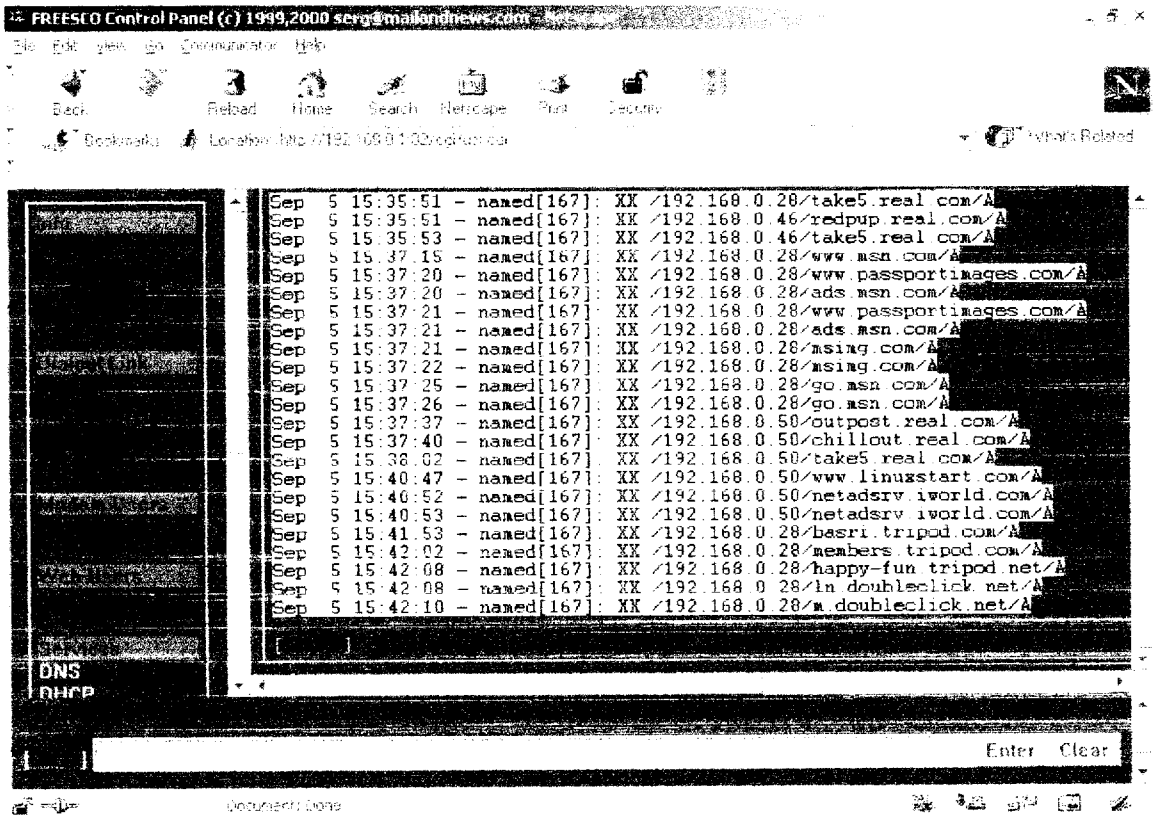


Clients on network 192.168.0.0 now have the option to access the Internet through gateway 1 at 192.168.0.1 or gateway 2 at 192.168.0.2



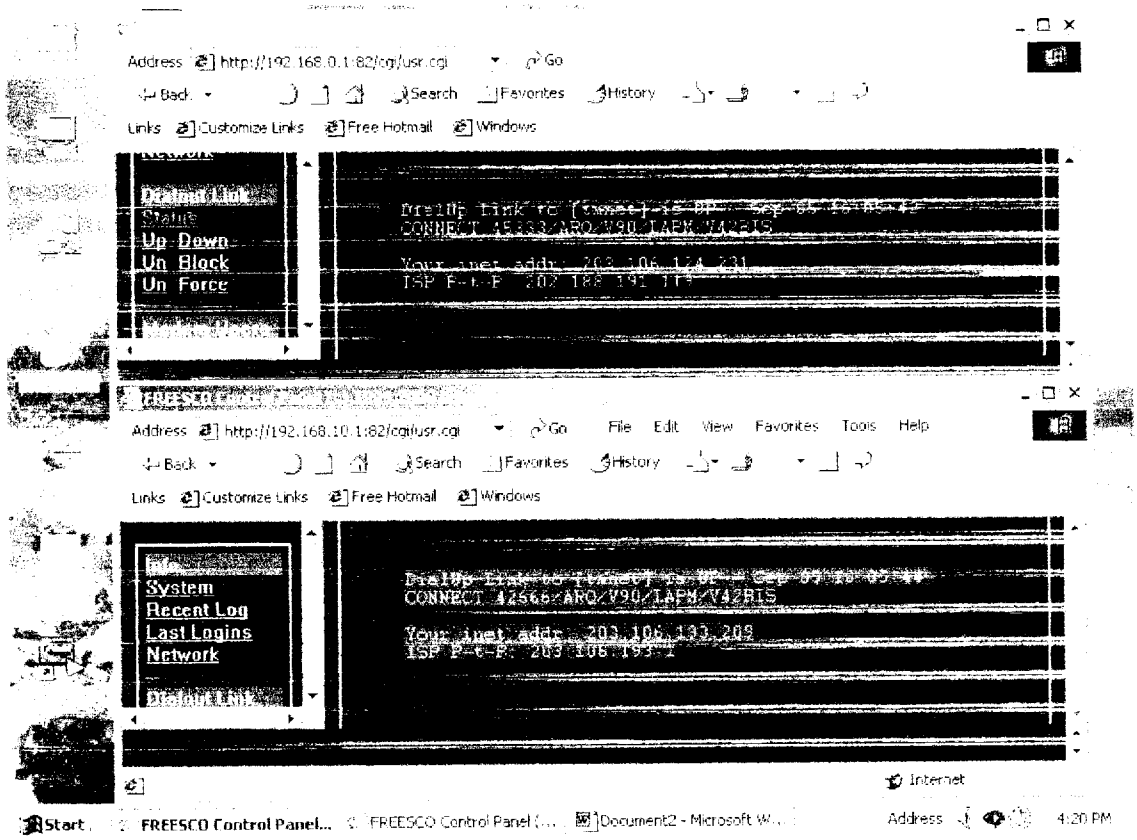
Appendix B

Web control panel



Recent log in freesco web control panel as viewed from client PC in network

192.168.0.0



Dialout Link Status in two freesco web control panels in an interconnected network situation as viewed from client PC in network 192.168.0.0

UNIVERSITI UTARA MALAYSIA

06010 UUM, Sintok, Kedah Darul Aman, Malaysia. Tel : 04 - 9241801 - 8 Cable : UTAMAS Telex : MA 42052 Fax/DL : 04 - 7005767

Sekolah Siswazah

UUM/SS/81007

20 Mei 2000

Maktab Perguruan Tunku Bainun
Bukit Mertajam, Pulau Pinang

Tuan/Puan,

PERMOHONAN KEBENARAN MENJALANKAN PENYELIDIKAN DI MAKTAB PERGURUAN TUNKU BAINUN

Adalah disahkan bahawa Ahmad Basri bin Hashim, no. matrik 81007 adalah pelajar siswazah program Sarjana Sains (Teknologi Maklumat) secara penuh masa di Universiti ini.

Sebagai memenuhi sebahagian syarat Pengijazahan Sarjana Sains (Teknologi Maklumat) beliau dikehendaki menjalankan penyelidikan seperti butir-butir berikut :

Tajuk : Utilisation of subnetworks through distributed gateway
Tempoh : 1 Jun 2000 - 7 September 2000
Tempat : Maktab Perguruan Tunku Bainun, Bukit Mertajam, Pulau Pinang

Sekian, terima kasih.

(PADMINI PILLAI)
b.p. Dekan

PP/sesiape/d.F/ah