

Electrical & Electronic Practice E

ELE3915

John Leis

Version 5.1 – March 2004

Contents

1	Network Hardware: Introduction	1
1.1	Important Notes re Completing this Laboratory Exercise	1
1.2	Networking Basics	2
2	Network Setup and Network Applications under Windows	7
2.1	Important Notes re Completing this Laboratory Exercise	7
2.2	Network Setup	7
2.3	Windows Network Tools	10
2.4	Packet Analyzer	10
2.5	Web Server	11
3	Linux Installation (Linux Part 1)	15
3.1	Important Notes re Completing this Laboratory Exercise	16
3.2	Hardware Setup	16
3.3	Windows Network Setup	17
3.4	Disk Partitioning	17
3.5	Linux Installation	19
3.6	Linux Filesystems	21
3.6.1	CD-ROM	22
3.6.2	Floppy Disk Files	22

3.7	Installing Packages	23
3.8	Disk Restoration	23
4	Linux Networking (Linux Part 2)	24
4.1	Important Notes re Completing this Laboratory Exercise	25
4.2	Linux Network Setup	25
4.2.1	Ethernet Card	25
4.2.2	Host-to-Network Routing	26
4.2.3	Network Router Setup	27
4.2.4	Name Services	28
4.2.5	Network Monitoring	29
4.3	Serial Line Interconnection	29
4.3.1	Serial Ports under Linux	29
4.3.2	Serial Terminal	31
4.3.3	PPP: Point to Point Protocol	31
4.4	NFS: Network File System	34
4.4.1	NFS Server	34
4.4.2	NFS Client	35
4.5	SMB (Samba): Unix-Windows Network File Sharing	36
4.6	DHCP: Dynamic Host Configuration Protocol	37
4.7	Web Server Installation	41
4.8	Web Server Scripting using PHP	44
4.9	Domain Name Server Installation	46
4.10	Disk Restoration	52
4.11	Further Work	52

5	FreeBSD	54
5.1	Notes on this Laboratory Exercise	54
5.2	Setup Notes	55
5.3	Disk Restoration	57

Practice Courses for Electrical, Electronic and Computer Engineering Programmes

Introduction

The purpose of the system of practice courses is to develop practical skills, the ability to function effectively as part of a team, and in the case of Bachelor of Engineering students, an understanding of the responsibilities of a professional engineer.

Practice courses are zero unit, zero tuition cost courses which are assessed on a pass/fail basis ie no other grades are possible. Their nominal duration is 50 hours, of which 30 to 40 hours will be laboratory work, group projects or other structured activities. The remainder is set aside for assimilation, report writing and assessment.

For day mode students, practice activities will usually be synchronized with relevant academic units, and distributed over a full academic year. Day students will normally complete two practice courses a year.

For external students, the practice courses are available as intensive on-campus residential schools, normally of one week duration. Students will usually complete one residential school per year. However, the timing of these has been arranged such that the more critical courses can be completed in pairs over a two week period, in order to minimize visits to campus.

The practice courses which apply to Electrical and Electronic engineering programmes are shown in Table 1, and those for Computer Systems Engineering (including BEng/BIT), Instrumentation and Control Engineering and Software Engineering are shown in Table 2.

Notes on Tables regarding Residential Schools for External Students

1. ELE1911 may be delayed for one year and completed together with ELE2912 over a two week period.
2. ELE2913 (or ELE3913) may be delayed for one year and completed together with ELE3914 over a two-week period.
3. ELE3914 can be delayed and completed together with ENG3902 over a two week period.

Table 1: Practice courses for Electrical and Electronic majors.

Practice Course		Usage			Res Schools External Students	
Number	Name	ADEE	BEngTech (EE)	BEng EE	Yr	Month Week
ENG1901	Engineering Prac 1	*	*	*	2	Feb wk15 (note 5)
ELE1911	Elec & Electr Prac A	*	*	*	3	Feb wk15 (note 1)
ELE2912	Elec & Electr Prac B	*	*	*	4	Feb wk15
ELE2913	Elec & Electr Prac C	*	*	*	4	Sep wk10 (note 2)
ELE3914	Elec & Electr Prac D		*	*	5	Oct wk11 (note 3)
ELE3915	Elec & Electr Prac E			*	6	Oct wk11 (note 4)
ENG3902	Professional Prac 1			*	7	Sep wk10
ENG4903	Professional Prac 2			*	8	Sep wk10

Table 2: Computer Systems, Instrumentation and Control, and Software Engineering majors.

Practice Course		Usage						Res Schools Ext Students	
Number	Name	AD (CS)	BET (CS)	BEng (CS)	BEng/ BIT	BEng (IC)	BEng (SW)	Yr	Month Week
ENG1901	Engineering Prac 1	*	*	*	*	*	*	2	Feb wk15(5)
ELE1911	Elec & Electr Prac A	*	*	*	*	*		3	Feb wk15(1)
ELE2912	Elec & Electr Prac B	*	*	*	*	*		4	Feb wk15
ELE3913	Comp Sys Eng Prac		*	*	*	*		4/5	Sep 10 (2)
ELE3914	Elec & Electr Prac D					*		5	Oct 11 (3)
ELE3915	Elec & Electr Prac E			*	*		*	6/7	Oct 11 (4)
ELE3916	S/W Eng Team Prac		*				*	6	Oct 11 (4)
ENG3905	Mechatronic Prac					*		6	Oct 11
ENG3902	Professional Prac 1			*	*	*	*	7	Sep 10
ENG4903	Professional Prac 2			*	*	*	*	8	Sep 10

Numbers in parentheses refer to notes below.

As far as possible, students should follow the Recommended Enrolment pattern for their programme, as shown in the university handbook

4. ELE3915 (or ELE3916) can be delayed and completed together with ENG4903 over a two-week period.
5. ENG1901 is also available in the September recess, in week 10.
6. Information regarding year in which residential schools should be undertaken does not apply to the BEng/BIT in external mode. This may only be undertaken by students who are eligible for at least two years advanced standing. Hence the year in which practice courses are undertaken will depend very much on individual enrolment patterns.

External Students

Students studying in external mode will complete each practice course by attending a one week intensive residential school, and submitting written reports as required. The practice courses should not be completed until all pre-requisite courses have been completed. Students should either have completed the co-requisite courses, or be currently enrolled in them.

Students are expected to attend for the **full duration** of the nominated residential school period. This should be the whole of the week, i.e. 8 am Monday to 5 pm Friday, except where alternative arrangements have been made because a Public Holiday falls within the week.

Students planning to attend should check the following web site for the final timetable 2 or 3 weeks before the residential school: <http://www.usq.edu.au/dec/outreach/>

Prior to attendance at residential schools, students should refresh their knowledge of any courses listed as pre- or co-requisites. It is advisable to bring to the residential school the study books for these courses, as you will probably wish to refer to them during the week.

During the on-campus Orientation programme at the start of the residential school, students will be given details of:

1. Any changes to the timetable
2. What groups they might be in: and
3. Any other relevant information.

Because of space constraints in the USQ Handbook it has not been possible to describe the pre- and co-requisite requirements in great detail. These are described more fully in the Practice Books provided to you when you enrol in these courses, and you should check these carefully. Each practice course should be completed at the stage in your programme where you will gain maximum benefit from attendance. This will be made easier if students follow the recommended enrolment pattern for their programme.

External students will not normally complete more than one practice course per year. However, the completion of some practice courses can be delayed by one year, to allow two residential schools to be completed end to end over a two-week period. This feature is designed to assist external students who travel to USQ from remote locations or from overseas.

External students in the Electrical and Electronic Engineering and Instrumentation and Control majors should note that there are two practice courses in their fourth year, one in February and one in September. In the case of Associate Diploma students following the recommended enrolment pattern, this is will correspond to their final year

Day students

Day students will normally complete practical activities in association with related academic courses, and these will be credited to the relevant practice courses. However, there may be a few activities which do not occur in parallel with a related academic course e.g printed circuit board activities for Bachelor of Engineering students.

The practice course system has to suit both day students and external students. For this reason, for day students following the recommended enrolment pattern, the activities in a practice course will extend over a complete academic year. Hence at the end of Semester 1 students will be given the interim grade IM (Incomplete, Make up work required). The IM will be converted to a P (Pass) grade when all components of the practice course have been completed. An IM grade is not normally allowed to persist for more than two years, so once students enrol in a practice unit, they should ensure that they complete all activities within two years.

Students who are following a non standard enrolment pattern are advised to enrol in a practice course in the first year that they start to complete relevant laboratory work, providing that they expect to complete all activities within two years.

Claiming Exemption

As is the case with any other course, you may apply for exemption from a practice course, on the basis of previous equivalent study, training or work experience. When making any application for exemption it is your responsibility to provide:

1. Proof of completion.
2. Details of what you have completed previously, with regard to subject matter and also contact hours or workload.

In some cases this may take the form of a letter from your employer on company letterhead, verifying that you have had relevant experience or training. It is recommended that you draw up a table of all the activities within the practice course, and then summarize beside each your relevant experience or training. This should then be attached to the letter of verification from your employer.

Do not submit original certificates. Copies should be verified as true copies by a Justice of the Peace (or an official of equivalent standing in the case of an overseas application).

If you are granted an exemption from a course, then this will appear on your academic record, and you will not have to enrol in the course.

If you have already been granted exemption from practice courses, as part of a block of exemptions in recognition of previous study, then further claims for exemption from subsequent practice courses will not normally be considered. This is because the awarding of a block of exemptions involves a trade-off between work the student has completed but has not been given credit for, and work the student has not completed but has been given credit for. The awarding of further exemptions will upset this balance.

Course content and Pre-Requisite Knowledge

This practice course contains experimental work relevant to the academic courses specified as pre/co-requisites.

External students

The residential school for this course is in the second week of the February recess. External students following a standard enrolment pattern should complete this residential school at the end of their second year of enrolment, after completion of all of the courses specified as above as co-requisites.

It is advisable to bring to the residential school the study books and texts for the co-requisite courses listed above.

It is permissible to delay the residential school for one year so that it can be completed in conjunction with the residential school for ELE2912 Electrical and Electronic Practice B over a two-week period.

Day students

Day students following one of the standard enrolment patterns shown in the USQ Handbook or Faculty Guide to Courses should enrol in Practice Courses as indicated in the enrolment pattern. The laboratory work for this practice course will be completed in association with the academic courses listed above as co-requisites.

Staff Associated with this Practice Course

Examiner:

Dr Wei Xiang

Office Z467

Email wei.xiang@usq.edu.au

Web <http://www.usq.edu.au/users/xiangwei/>

Moderator:

Dr John Leis

Assessment

Your result for this class is assessed on a Pass/Fail basis. In order to obtain a pass, you are required to:

1. Satisfactorily complete at least 80% of the activity hours associated with the class.
2. Submit a brief report on your work at the end of the term.

At the conclusion of each practical session you **must** present this practice book to your supervisor for his signature, which certifies that you have completed the activity. If you wander out of the laboratory without checking with the supervisor, there may be no record that you have completed the activity, and you may have to repeat the experimental work.

To obtain a Pass you must have **completed at least 80% of the activity hours associated with the course**, which will be interpreted as 80% of each group of activities. This flexibility is intended to allow for sickness and unforeseen accidents or emergencies. It is not acceptable to omit a complete group of activities. In normal circumstances it is expected that students should complete all of the activities.

In order to address the second requirement, a brief **report** of your work in each activity is required. This is not intended to be onerous, and although there are no specific length requirements, you may use 6-8 pages as a guide. It is recommended that you keep a workbook/diary to keep notes as you progress. This may then be formatted into your end-of-term report, and will ease its preparation considerably. **Please include a copy of the “Completion Form” with all appropriate signatures with your report. The signatures must be obtained during the laboratory exercises.**

You will be required to produce the Activity Completion Log from this practice book to verify that you have completed (or been exempted from) all of the activities required to achieve a pass in this course.

Introduction

The laboratory exercises in this class focus on operating systems, data communications and networking. The exercises are designed around group-based learning and problem solving:

Exercises in operating-system installation, hardware configuration and networking for both Windows and Unix.

Problem solving scenarios related to network operational problems and software installation & configuration.

Project work where teams are required to install and configure applications such as web servers and other networked systems.

I'm sure you'll find the exercises interesting and challenging, and that they will increase your competence in the subject areas covered. Hopefully, they will also pose a number of intriguing questions for you to explore in your future studies.

*John Leis
November 2002*

Acknowledgement

The author would like to acknowledge the assistance and expertise provided by Mr Chris Snook of the Faculty of Engineering in preparing the Unix-based exercises.

On-Line Resources

The home page for this class contains links to additional resources. CD-ROMs with software resources will be provided for use during the laboratory sessions. See <http://www.usq.edu.au/users/leis/> for more information.

Course Specifications

All USQ course specifications are available online – see <http://www.usq.edu.au/course/>

Completion Form – Electrical & Electronic Practice E

Complete this form, detach and hand in with your report due one week after the completion of the lab exercises.

Please print clearly on your lab report your surname in CAPITAL LETTERS, followed by your given name — for example:

SMITH, John

Your name as stated on the assignment must match exactly your name as submitted on your enrolment form.

Student Name: _____

Student Number: _____

Examiner: _____

Other Staff: _____

Group/Lab Time: _____

Year/Semester: _____

Hours 3 hrs/wk	Laboratory Name	Supervisor Name+Signature	Date Completed
1	Introductory Session		
1	Workplace Health & Safety Exercise		
2	Network Hardware: Introduction		
8	Network Configuration & Testing under Windows		
4	Installing Linux		
20	Networking Linux		

Before undertaking any laboratory work, I have read & understood the section on “Workplace Health and Safety”

Student to sign & date: _____

Overall Completion (Examiner to sign & date): _____

Timetable

The following sections give suggested timetables for completion of the activities. Note that the actual times taken may vary, and supplementary exercises may be added by the lab instructor. Note that the FreeBSD exercise is not included in the activity list below; it may be substituted for the Linux exercises in cases where students have sufficient familiarity with Linux, or as an additional exercise.

On-Campus

Week	Activity
1	intro + safety + library exercise
2	Ex 1 Network Basics
3	Ex 2 Windows Networking
4	Ex 2 Windows Networking
5	Ex 3 Linux Installation
6	Ex 3 Linux Installation
7	Ex 4.1-4.2 Linux LAN
8	Ex 4.3 Linux Serial & PPP
9	Ex 4.4 Linux NFS
10	Ex 4.5 SMB
11	Ex 4.6 DHCP
12	Ex 4.7 Apache
13	Ex 4.10 Restore

Off-Campus (Residential School)

Day/Time	Activity
Mon AM	intro + safety + library exercise
Mon PM	Ex 1 Network Basics (& start Ex 2)
Tue AM	Ex 2 Windows Networking (continued)
Tue PM	Ex 3 Linux Installation
Wed AM	Ex 4.1-4.2 Linux LAN
Wed PM	Ex 4.3 Linux Serial & PPP
Thur AM	Ex 4.4 Linux NFS
Thur PM	Ex 4.5 SMB
Fri AM	Ex 4.6 DHCP, 4.7 Apache, 4.10 Restore

Workplace Health and Safety¹

Workplace Safety

The workplace is a dangerous place. On average, 2900 Australians are killed and 650 000 are injured each year at work. This is more than were killed and wounded in the Vietnam war! You have a duty to yourself, your family and your workmates to work safely. In part this is a matter of knowledge, knowing the things to do and not to do, but perhaps more importantly it is a matter of attitude. It is relatively easy to give you the knowledge you need, it is much more difficult to develop a safe working attitude. That requires maturity which in turn requires time. For this reason a Safety Activity is included in each of the practice classes; to provide a gradual development of knowledge and attitude.

Aims of Activity

This activity aims to make you aware of:

1. The safety rules applying at your workplace; the specific hazards in your workplace and the signage used to identify them; the protective measures, including clothing available; and
2. Your obligations under workplace health and safety legislation.

The Activity

Specifically, you are required to summarize the safety facilities and procedures relating to a selected workplace. Usually this will be one of the laboratory areas in which you undertake practical work exercises. You are also required to identify the hazards that you perceive exist in the workplace. If necessary, seek assistance from the laboratory supervisor to identify the safety equipment/clothing, procedures and hazards.

Description of Workplace

Draw a plan of the selected workplace (and associated areas) clearly showing major pieces of equipment and the location of:

- emergency exits
- fire detectors

¹Original document supplied by DEC/USQ, May 1998.

- fire extinguishers
- first aid kits
- other safety equipment

Protective (Safety) Clothing

List here any protective clothing that you are **required to wear** — for example, safety glasses, safety helmet, etc.

E1
E2
E3
E4
E5
E6

Safety Instructions

List here the safety instructions / procedures that you have been given.

P1
P2
P3
P4
P5
P6

Perceived Hazards

List here in order of seriousness (worst first) the hazards that you see in the selected workplace, and against each indicate (using the E and P codes above) the safety clothing and/or procedures intended to limit those hazards.

Description of hazard	Relevant safety clothing	Relevant safety procedure

Legislation

In Queensland the umbrella legislation for safety in the workplace is the Workplace Health & Safety Act 1995. This sets the overall climate for safety in this state, it defines the responsibilities of employers and employees, it sets up mechanisms for establishing and maintaining safe working practices and it sets penalties for non-compliance. A summary of the major aspects of the Workplace Health & Safety Act is below. Read that summary and then complete the following:

Persons in control of workplaces must:

Employees must not:

A person (employer or employee) who does not meet his/her obligations under this Act can be fined a sum of up to _____ or imprisoned for up to _____ months.

To avoid these penalties a person must prove that:

Summary of the Workplace Health & Safety Act

The following summarizes very briefly those aspects of Workshop Health & Safety Legislation 1995 that apply directly to you at this point in your career. It is taken from A Guide to Workplace Health & Safety Legislation 1995 prepared by the Queensland Government Division of Workplace Health and Safety in April 1996. Does the Act apply to you? The Act applies to:

- employers.
- self-employed persons.
- persons in control of workplaces.
- workers and other persons at workplaces – like customers and visiting salespersons.

What is the main aim of the Act?

The goal is to make sure your health and safety is not put at risk as well as making sure you don't actually become sick or injured because of your association with workplaces or workplace activities.

How does the Act achieve this aim?

The Act sets out a framework to achieve its objective. This includes:

- Imposing workplace health and safety obligations on persons who may affect the workplace health and safety of others by their action or lack of action.
- Making workplace health and safety compliance standards that must be followed.
- Making workplace health and safety advisory standards that give practical advice about ways to identify and manage exposure to risk for workplace health and safety.
- Electing workplace health and safety representatives and establishing workplace health and safety committees to foster consultation between workers and employers.

What are your workplace health and safety obligations?

The Act imposes obligations on all persons who may affect the workplace health and safety of others by their action or lack of action. Employers must ensure the workplace health and safety of:

- Each of their workers.
- Themselves and others who may be affected by the way they conduct their business and work activities — for example, visitors, salespersons, passing pedestrians.
- Self-employed persons must ensure that the workplace health and safety of themselves and others is not affected by the way they conduct their business and work activities.

Persons in control of workplaces must:

- Minimize the risk of injury or disease to persons coming to perform work at the workplace.
- Minimize the risk of injury or disease from any plant or substance they provide for the purpose of work to persons who are not their workers.
- Ensure appropriate, safe access to and from the workplace for persons who are not their workers.

Workers and other persons must follow instructions given by the employer for the workplace health and safety of themselves and others. At a construction workplace they must follow the instructions of the principal contractor. They must not:

- Wilfully or recklessly interfere with or misuse anything provided for workplace health or safety.
- Wilfully put at risk the workplace health and safety of any person.
- Wilfully injure themselves.

Workers must use personal protective equipment if it is provided by the employer and they have been trained in its use.

How do you meet your obligations?

A person who has a workplace health and safety obligation under the Act must fulfil that obligation. Compliance Standards must be followed. When there is a compliance standard about a risk, the only way a person can meet his or her obligation for that risk is to comply with the standard. Advisory Standards should be followed. When there is an advisory standard about risk, a person can meet his or her obligation in two ways. The person can either follow the standard or adopt another way to manage the risk that is more suited to the person's business or work activity. A person who breaches an obligation can be prosecuted. The maximum penalty for this is \$24,000 or 6 months imprisonment for an individual. There are certain defences a person can use in a proceeding for a breach of an obligation. These include the person proving that:

- He or she followed a relevant compliance standard.
- He or she followed a relevant advisory standard – or that he or she used another way to manage exposure to the risk and took reasonable precautions and exercised proper diligence.
- He or she chose appropriate ways to manage a risk, took reasonable precautions and exercised proper diligence to prevent the breach when there was no relevant compliance or advisory standard.

Exercise 1

Network Hardware: Introduction

Aim The aim of this experiment is to investigate the operation of a network using Ethernet and TCP/IP on a Windows workstation. The network will be set up as an isolated network in the laboratory. At the end of the session, all computers should be able to access all others on the network in the laboratory.

Platform At least two networked computers running Windows are required.

1.1 Important Notes re Completing this Laboratory Exercise

- This lab exercise does not require connection to the campus network. All networking is to be done using local hubs and cabling. No machine should be connected to the campus network via the wall sockets. All machines used should be checked/restored to the correct setup after the lab with correct IP addresses and subnet masks.
- The examples output data and configuration files are shown for illustration only. You should use the IP address and subnet mask as assigned to your particular machine(s) during the laboratory class. Using IP addresses incorrectly can cause major network disruptions to other users, and you will be held responsible. If unsure, ask the supervisor.
- The following examples were generated using a subnet mask of 255.255.248.0. You should work through and understand the examples given. The recommended subnet mask for most this practical work is 255.255.255.0 (except where specified otherwise).
- Certain Internet addresses may be used within private networks, and are not routed to the outside world. From RFC1918:

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	10.255.255.255	(10/8 prefix)
172.16.0.0	172.31.255.255	(172.16/12 prefix)
192.168.0.0	192.168.255.255	(192.168/16 prefix)

We will refer to the first block as “24-bit block” the second as “20-bit block”, and to the third as “16-bit block”. Note that (in pre-CIDR notation) the first block is

nothing but 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 256 contiguous class C network numbers.

An enterprise that decides to use IP addresses out of the address space defined in this document can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise, or the set of enterprises which choose to cooperate over this space so they may communicate with each other in their own private internet.

As before, any enterprise that needs globally unique address space is required to obtain such addresses from an Internet registry. An enterprise that requests IP addresses for its external connectivity will never be assigned addresses from the blocks defined above.

In addition, RFC3927 specifies a “zero-config” address with the 169.254/16 prefix, as follows:

To participate in wide-area IP networking, a host needs to be configured with IP addresses for its interfaces, either manually by the user or automatically from a source on the network such as a Dynamic Host Configuration Protocol (DHCP) server. Unfortunately, such address configuration information may not always be available. It is therefore beneficial for a host to be able to depend on a useful subset of IP networking functions even when no address configuration is available. This document describes how a host may automatically configure an interface with an IPv4 address within the 169.254/16 prefix that is valid for communication with other devices connected to the same physical (or logical) link.

IPv4 Link-Local addresses are not suitable for communication with devices not directly connected to the same physical (or logical) link, and are only used where stable, routable addresses are not available (such as on ad hoc or isolated networks). This document does not recommend that IPv4 Link-Local addresses and routable addresses be configured simultaneously on the same interface.

1.2 Networking Basics

1. **Note:** This exercise does **not** require connection to the campus network, or the external Internet. Do not connect any part of the network to the wall network sockets. If unsure ask the person in charge.
2. Table 1.1 shows the suggested network addresses, with subnet mask 255.255.255.0. **You are to fill in the Ethernet address of your machine, the address of others on the network, as you complete the following exercises.** Note that these addresses are **not** to be used for machines connected to the campus network or anywhere outside the lab. Also, the hostname is arbitrary for the purposes of the exercise, however **for a system connected to the Internet all names and IP addresses must be registered correctly with the Internet Assigned Numbers Authority (IANA).** For the exercise, use a hostname of “lab n ”, where n is the computer number.
3. Figure 1.1 shows the physical setup, whilst Figure 1.2 shows the network topology. Locate your machine and check how it is physically connected to the others.

No.	Barcode	IP Address	Ethernet Address	LAN Card	
				3Com 3C905C-TX	Realtek 8029
WorkGroup1					
1	998-xxxx	139.86.64.1	00-50-DA-93-7D-D2	*	
2	998-9644	139.86.64.2	00-50-DA-93-7E-01	*	
3/R1	998-9649	139.86.64.3	00-50-DA-93-7D-D8	*	
		139.86.67.1	00-00-1C-40-69-BF		*
4/R2	998-xxxx	139.86.64.4	00-01-02-58-95-BD	*	
		139.86.65.1	00-00-1C-00-FF-75		*
WorkGroup2					
5/R3	998-9691	139.86.65.2	00-50-DA-93-7D-FF	*	
		139.86.66.1	00-00-1C-40-69-FD		*
6	998-9650	139.86.65.3	00-50-DA-93-7D-D1	*	
7	998-9682	139.86.65.4	00-50-DA-93-7D-E9	*	
WorkGroup3					
8	998-9655	139.86.66.2	00-50-DA-93-7D-A8	*	
9	998-9681	139.86.66.3	00-50-DA-93-7D-A6	*	
WorkGroup4					
10	998-9654	139.86.67.2	00-01-01-97-FD-30	*	
11	998-9687	139.86.67.3	00-50-DA-93-7D-AC	*	
12	998-9646	139.86.67.4	00-50-DA-93-7D-E5	*	
13	998-9692	139.86.67.5	00-50-DA-93-7D-AE	*	

Table 1.1: Machine identity and network addresses. The Ethernet addresses should be filled in/checked as you complete the exercises. The computer name is the word “lab” followed by the computer number (lab1, lab2, ... lab13).

4. LAN (Local Area Network) cards or NICs (Network Interface Cards) used in this laboratory are currently one of three types, as shown in Table 1.2. The diagnostic programs for use under DOS, and the Windows network drivers, are located on the supplied CD, and on the c: drive of each machine under `lanocard` for machines with one card, and in a subdirectory of the appropriate name under `lanacards` for machines with more than one card.

Machine	NIC	setup/diagnostic
ABA	3COM 3c905C-TX	3c90xcfg
DELL	3COM 3c905C-TX	3c90xcfg
Routers	3COM 3c905C-TX + RealTek 8029 PCI/PnP	rset8029

Table 1.2: Machine network interface cards. Machines with a second NIC have RealTek 8029 cards. DELL NICs are built into the motherboard.

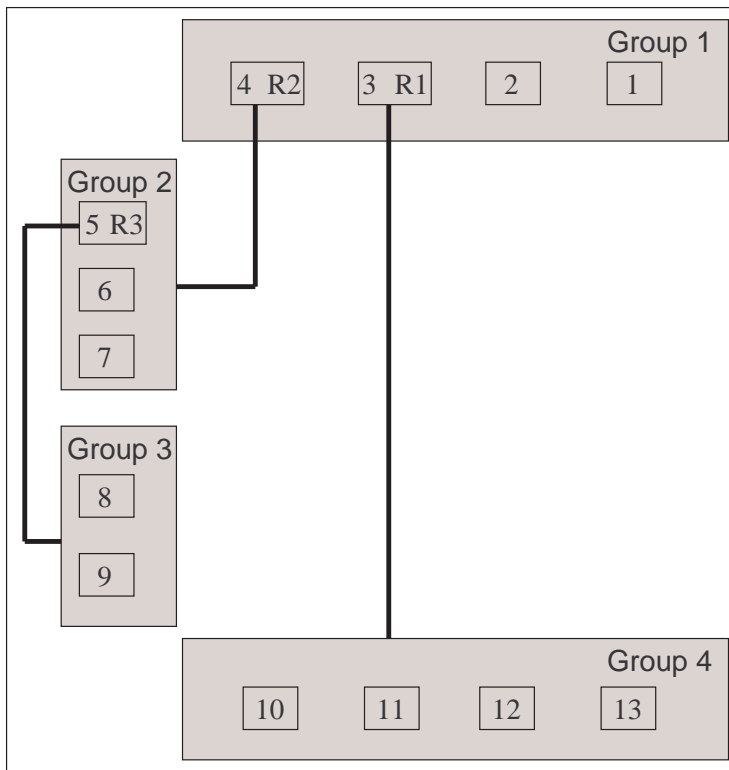


Figure 1.1: Physical layout of the benches in the lab.

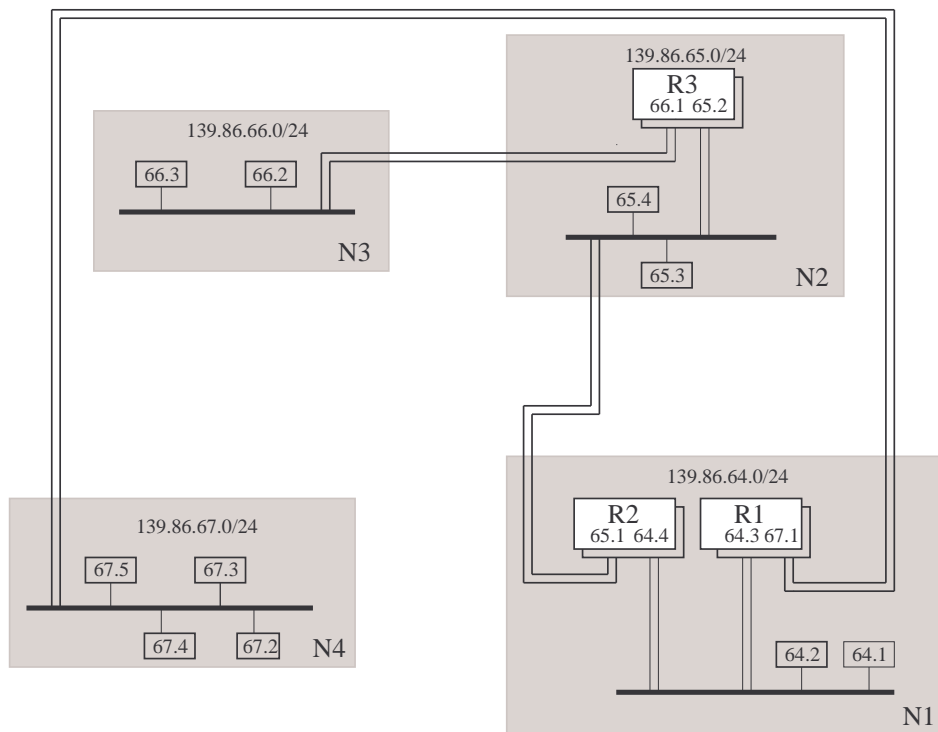


Figure 1.2: Network topology.

5. Note: if problems are experienced in getting Windows to correctly recognize the network cards, check the BIOS Plug-and-Play setting. It may be necessary to set "Plug-and-Play" to "No".
6. Disconnect the Ethernet 10BASE-T cable from the RJ45 connector at the rear of the computer. Note that these connectors are physically very similar to a standard telephone connectors (but of course electrically quite different). Reconnect the cable to the connector on the LAN card. Do not connect the cables to the built-in sockets on the wall.
7. Boot the computer in single-tasking (DOS-only) mode from a bootable floppy disk.
8. Run the NIC (Network Interface Card) configuration/diagnostic program in DOS (single-tasking) mode. Check the Ethernet ("hardware") address(es).
9. Connect all the PC's in your network group to the hub. Note the power supply requirements for the hub and ensure you use the correct plugpack supply. Run the card diagnostics program to perform card and network self-tests.
10. Set up the network with the IP and hardware addresses as nominated previously:
Start-Settings-Control Panel-Network, TCP/IP if present. If not, select Add-Protocol-Microsoft-TCP/IP
11. Enter the following configurations:
IP Address (as given)
Netmask (as given)
12. In the "file sharing" section, enter the following configurations:
Computer Name (eg, "lab1")
Workgroup Name (eg, "WorkGroup2")
Logon to Domain disabled.
13. Reboot the computer when requested by Windows. Enter a user name and press OK at the login box. Do not press cancel as subsequent networking may be affected.
14. Click start-run and type `wiipcfg`¹. Note the following:
 - (a) The Ethernet card manufacturer (typically 3Com, Lantech/Realtek, Intel) and identification number.
 - (b) The *48-bit Ethernet card address*. These are written as six, 8-bit hexadecimal numbers separated by a dash (or sometimes a colon). This address is sometimes referred to as the "hardware address", as it is encoded into the memory of the Ethernet card by the manufacturer. The number is unique to every card – the first 3 numbers (such as 00-00-1C) may be used to identify the manufacturer.
 - (c) See the class web page for references on Ethernet.
 - (d) The *32-bit Internet Protocol (IP) address*. These addresses are written as four, 8-bit decimal numbers separated by a dot.
 - (e) The *32-bit subnet mask*. This is normally written as four, 8-bit decimal numbers but is best interpreted in binary. The 1's in the subnet mask define the network portion of the Internet address, whilst the 0's in the subnet mask define the host address on the local network. (Remember that the Internet is an "interconnection of networks").

¹This command is `ipconfig` in later versions of Windows.

15. In a DOS box, type
`ping other-machine-IP-address`
`ping` sends out test packets which are returned from the remote machine to check connectivity and return times. Check that the ping is successful. If not, check the configurations and cabling.
16. You may create a static hostname in the file `hosts` under the `c:\windows` directory. Follow the format given in the file `hosts.sam`, then check that you can ping the named host (rather than the IP address).
17. Delete the local network address cache by typing
`arp -d other-machine-IP-address`
18. Typing `arp -a` should show “No Entries”.
19. Type `ping other-machine-IP-address` then `arp -a`
20. One entry will be found, because `other-machine-IP-address` is on the same subnet as the current machine.
21. Repeat the `ping` command with another machine’s address. Then `arp -a` should show two entries.
22. Type `ping localhost`. This address is also called the “loopback” address, and always maps to IP address 127.0.0.1
23. Routing and domain names will be examined in the exercise “Network Configuration and Testing under Windows”.
24. Check that you can “ping” all other machines that should be directly accessible to your machine (on the same network). Note that the router machines (R1, R2, and R3) have two network cards, and hence are able to access two sub-networks.

Exercise 2

Network Setup and Network Applications under Windows

Aim The aim of this experiment is to investigate the operation of a network using Ethernet and TCP/IP on a Windows workstation. It is recommended that the lab exercise “Network Hardware: Introduction” be completed prior to undertaking this exercise.

Platform A Windows networked computer is required. For some file-sharing experiments, two networked computers running Windows are required.

2.1 Important Notes re Completing this Laboratory Exercise

- This lab exercise does not require connection to the campus network.
- The examples output data and configuration files are shown for illustration only. You should use the IP address and subnet mask as assigned to your particular machine(s) during the laboratory class. Using IP addresses incorrectly can cause major network disruptions to other users, and you will be held responsible. If unsure, ask the supervisor.
- The following examples were generated using a subnet mask of 255.255.248.0. You should work through and understand the examples given. The subnet mask for this area has now changed to 255.255.255.0 and you must use this mask.

2.2 Network Setup

1. Disconnect the Ethernet 10BASE-T cable from the RJ45 connector at the rear of the computer. Note that these connectors are physically very similar to standard RJ11 telephone connectors. Reconnect the cable to the connector on the LAN card.
2. Boot (or reboot) the computer. Enter a user name and press `OK` at the login box. Do not press `cancel` as subsequent networking may be affected.
3. Start a DOS shell.

4. The following examines local area network (LAN) sharing using the NetBIOS protocol (note that it is distinct from TCP/IP examined later).
5. Click `Start-Settings-ControlPanel-Network`, then the `identification` tab, and enter the computer name as given in the previous exercise (`lab2` etc).
6. Click `OK`, then `file` and `Print Sharing`, and ensure that file and print sharing is enabled.
7. Share a folder on one computer by selecting the folder, right-clicking, then selecting “sharing”.
8. On another computer go to `Network Neighborhood` and find the shared folder. It may be necessary to select “refresh” in the browse window. Alternatively, in a DOS shell, type
`net view`
9. In a DOS shell, type `net use /? | more`
10. Now connect to the remote computer and folder (assumed here `lab2` and `temp`, respectively – substitute the correct ones): `net use p: \\lab2\temp`
11. The drive `p:` should now be visible and contain the remote files. Change to this drive and verify the permissions available.
12. Check the share using `net use`. Note the space between “net” and “use”. Investigate `net help` to examine further commands.
13. Explore the NetBIOS status using `net use`, `netstat -a` and `nbtstat`. Use the `/?` option to each of these to determine the command-line arguments and options.
14. Disconnect from the share using `net use p: /delete`
15. The remainder of the lab examines the wide area network protocol called TCP/IP. This is different to the NetBIOS protocol examined above.
16. Type `wiipcfg`¹. Note the following:
 - (a) The Ethernet card manufacturer (3Com, Lantech/Realtek, Intel, etc) and identification number.
 - (b) The *48-bit Ethernet card address*. These are written as six, 8-bit hexadecimal numbers separated by a dash (or sometimes a colon). This address is sometimes referred to as the “hardware address”, as it is encoded into the memory of the Ethernet card by the manufacturer. The number is unique to every card – the first 3 numbers (such as 00-00-1C) may be used to identify the manufacturer.
 - (c) See the class web page for references on Ethernet.
 - (d) The *32-bit Internet Protocol (IP) address*. These addresses are written as four, 8-bit decimal numbers separated by a dot.
 - (e) The *32-bit subnet mask*. This is normally written as four, 8-bit decimal numbers but is best interpreted in binary. The 1’s in the subnet mask define the network portion of the Internet address, whilst the 0’s in the subnet mask define the host address on the local network. (Remember that the Internet is an “interconnection of networks”).

¹This command is `ipconfig` in later versions of Windows.

- (f) The *default gateway*. The machine at this address is on the local network, and routes (forwards) packets for machines on other networks. The host number on gateways is normally chosen to be a low number (1 or 2).
17. Click on `more info`. Note the following:
 - (a) The “fully-qualified” host name (such as `lab2.eng.usq.edu.au`), which is divided into:
 - i. The “hostname” of the machine itself – such as “lab2”.
 - ii. The domain – here “eng.usq.edu.au”.
 - (b) The DNS Server. This is the address of a host running a Domain Name Server process, which translates host names into IP addresses.
 - (c) If a DHCP (Dynamic Host Configuration Protocol) is specified, then the local machine does not have a fixed (static) IP address for all time. Rather, it is allocated a temporary number by the DHCP server for the duration of its connection. This is used in machines which are not connected 100% of the time – such as PC laboratory machines and home PC’s connected via a modem.
 18. Record all of the parameters for later use and exit `winipcfg`.
 19. In a DOS box, type


```
ping 139.86.64.6
```

`ping` sends out test packets which are returned from the remote machine to check connectivity and return times.
 20. Delete the local network address cache by typing


```
arp -d 139.86.64.6
```
 21. Typing `arp -a` should show “No Entries”.
 22. Type `ping 139.86.64.6` then `arp -a`
 23. One entry will be found, because 139.86.64.6 is on the same subnet as the lab machine.
 24. Type `ping localhost`. This address is also called the “loopback” address, and always maps to IP address 127.0.0.1
 25. Routing is performed on the Internet over gateways – each “hop” forwards the packets until the destination is reached. Type `tracert 139.86.64.226` and see the route for a machine on the local subnet².
 26. Routing on individual machines is done by checking the local network, and then forwarding unresolved addresses to the next highest gateway. Type `route print` to see the routing tables for the current machine. You should see something like the following:

Network Address	Netmask	Gateway Address	Interface
0.0.0.0	0.0.0.0	139.86.64.1	139.86.64.226
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
139.86.64.0	255.255.248.0	139.86.64.226	139.86.64.226

²The Unix equivalent is `traceroute`, and works in a similar fashion.

In the above table, machines on the local network 139.86.64.0 (i.e. network address with host address 0) are directly connected. The address 127.0.0.1 is for loopback to the same machine (packets do not reach the network, but are transferred through the software protocol stacks), and address 0.0.0.0 denotes a “default” route for all other packets to the router at 139.86.64.1

27. Note that

```
netstat -r -n
```

will show similar information (`-r` for routing information, and `-n` for numeric addresses).

28. Record the default route for your machine, including Gateway and Interface addresses.

29. The syntax of the `route` command is

```
route command destination mask netmask gateway
```

command may be `print`, `add` or `delete`. The keyword `mask` is required if entering a `netmask`³. Delete the route to a gateway by entering:

```
route delete 0.0.0.0 139.86.64.1
```

30. Type `route print` to check that the default route has been deleted.

31. Type `ping 139.86.208.20`. It should fail, as the address is *not* on the local subnet. Before proceeding, verify this for yourself by writing down the subnet mask in binary, and checking that the 139.86.208.20 not on the local subnet.

32. To restore the default route, you would use:

```
route add 0.0.0.0 mask 0.0.0.0 139.86.64.1
```

Note that the netmask of 0.0.0.0 must also be specified, as it is a direct route to a specific host.

33. The `telnet` application allows you to connect to a specific port (normally a “telnet” or terminal port) on a remote machine. Protocol *ports* are used to connect to specific services. The default port for the telnet service is 23. Ports below 1024 are reserved for “well-known” services.

2.3 Windows Network Tools

1. A graphical tool which incorporates many network diagnostics is the `cyberkit` application.
2. Install `cyberkit`, and note the various facilities such as `ping`, `tracert` and `nslookup` (for name-service lookup). This is a useful diagnostic tool for future use.

2.4 Packet Analyzer

1. A protocol or packet analyzer will now be installed. Both a command-line tool called `windump` and a graphical application called `analyzer` will be examined. The files required will be supplied.

³On Unix systems, this keyword is `netmask`.

2. First, the packet filter must be installed. Detailed instructions are given in the html file according to the name of the operating system required. The following is an abbreviated guide for Windows 95 only:
 - (a) Run `packet95.exe` to unzip files to a temporary directory.
 - (b) In the Control Panel, go to Networks and click Add.
 - (c) Choose Protocol and click Add.
 - (d) Click Have Disk. Browse to the "packet" files unzipped previously. (select Skip File if the Windows 95 CD is requested).
 - (e) Reboot. The Control Panel-Network should now show Network Packet Driver.
3. The command-line packet capture utility `windump` will now be installed.
4. Copy `WinDump.exe` to a convenient location and run it from the command line.
5. Note the packets captured. Try a `ping` command and watch the network traffic.
6. The graphical packet capture utility `analyzer` will now be installed.
7. Locate `analyzer.exe` and run it. Install to a convenient location.
8. Run the extracted `Analyzer.exe`. Choose Captures-LAN Adapter, then Captures-Begin.
9. Note the MAC (Medium Access Control) or Ethernet addresses, the "layer 3" output column, and the detail in the lower panel.
10. Try a `ping` command and capture the network traffic.

2.5 Web Server

1. Now the Apache web server will be installed.
2. Initial documentation is provided in `win32.html`.
3. A web browser must be operational on the machines on the network.
4. If using Windows 95 it may be necessary to run `w95ws2setup`.
5. If using Windows 95 it may be necessary to run `instmsi`. Try running `msiexec` first to check.
6. Run `msiexec /i apacheversion.msi`, where `apacheversion` corresponds to the file name supplied. Alternatively, simply double-click in the `.msi` file.
7. Run through the install program. Use defaults for all configurations.
8. To start/stop/restart the HTTP server, use

```
apache -k start
apache -k stop
apache -k restart
```
9. Note: When the configuration files are changed it is necessary to stop & start, or restart, the server. The configuration files are only read on startup.

10. Note: if changing configurations parameters, it will be necessary to refresh the web browser pages using *control-refresh*, to force a request of a new page. Otherwise, the locally stored (cached) page will be displayed.
11. Note that the base directory for the Apache installation is
`c:/Program Files/Apache Group/Apache`
12. Start the server. Using a web browser firstly on the local computer, check that a default page is visible from the server using a URL of the form `http://139.86.64.226/`
13. Repeat from a web browser on another machine on the network.
14. Under the base directory are configuration files (in the `conf` directory), log files (in the `log` directory), and executables (in the `bin` directory).
15. Examine the log files `access.log` and `error.log`
16. Edit the configuration file `httpd.conf`. Note the `DocumentRoot` parameter.
17. Add the file `test.html` to the document root directory:

```
<!-- doctype html -->

<html>
  <body>
    <h1 align=center>
      <font color="blue"> This is a test
    </font>
    </h1>

    <h1 align=center>
      <font color="red"> This is a test
    </font>
    </h1>
  </body>
</html>
```

18. Check that the page of the form `http://139.86.64.226/test.html` is visible.
19. Search the configuration file for a line containing `DirectoryIndex`. Change this to:

```
DirectoryIndex index.html test.html
```

and restart the server.

20. Check that the page of the form `http://139.86.64.226/` is visible. This means the default file, if none is specified, has been changed as specified.
21. Search the configuration file for the entry
`<Directory "c:/Program Files/Apache Group/Apache/htdocs">`
Find the section dealing with access permissions:

```
Order allow,deny
Allow from all
```

This means the “allow” rules are processed first, followed by the “deny” rules.

22. Change this to something of the form

```
Order deny,allow
deny from all
allow from 139.86.65.
```

23. Restart the http server. Verify that web browsers can access the pages on the server according to the above rule. In this case, all machines are denied access except those on network 139.86.65.x
24. Password protection of web pages will now be added.

25. Run the `htpasswd` program in the `bin` directory to create a password configuration file in the `conf` directory:

```
htpasswd -c users.conf fred
```

This creates a password file with an entry for user “fred”. Move the `users.conf` to the `conf` directory. Note that the password file is encrypted, and will appear something like

```
fred:$apr1$f.5.....$QND8rKZJU7N3GQBU5J0zk/
```

26. Search the configuration file for the entry
`<Directory "c:/Program Files/Apache Group/Apache/htdocs">`
 Find the section after this called `AllowOverride`. Change this to

```
AllowOverride AuthConfig
```

27. Now in the `htdocs` directory, create a file called `.htaccess` containing:

```
AuthName      "Realm Name"
AuthType      basic
AuthUserFile  "c:/Program Files/Apache Group/Apache/conf/users.conf"
require valid-user
```

28. Restart the server, and check that the browser requests a password for all files in that directory.
29. The `telnet` application allows you to connect to a specific port (normally a telnet or terminal port) on a remote machine. The default port (as used above) is 23. Connect to the web server on port 80 via HTTP (HyperText Transfer Protocol) :
- ```
telnet machinename 80
```

30. Type

```
GET / HTTP/1.0
```

Note that the characters will not echo, and that a space after “GET” and before “HTTP” is mandatory. Hit return *twice* (this is part of the HTTP protocol). You should see the text for the page delivered to your telnet application as HTML (HyperText Markup Language).

31. Use

```
netstat -n -a
```

to see the connection information. Note the IP addresses and ports in use.

32. Close the telnet window.
33. Now run the packet capture application `Analyzer.exe` and generate some network traffic by requesting web pages with `control-refresh`.
34. Note the HTTP client requests (GET) and server responses.
35. Access a password-protected web page whilst capturing the network packets. Locate the HTTP requests/responses — are the passwords visible in plaintext?

## Exercise 3

# Linux Installation (Linux Part 1)

**Aims** The aims of this laboratory task are:

1. To become familiar with low-level partitioning of disks and how they are used by operating systems.
2. To install Linux – an implementation of the Unix operating system.

It is recommended that the lab exercises “Network Hardware: Introduction” and “Network Configuration and Testing under Windows” be completed prior to undertaking this exercise.

**Hardware** The hardware supplied may vary, but requires the following for completion of the entire exercise:

1. PC's with CD drive and network interface card(s).
2. Ethernet hubs (or switches).
3. 10BASET cabling.
4. A blank floppy for DOS-only reboot and for saving disk partition tables, boot sector information and file allocation tables.

**Software** The following software will be supplied:

1. Linux CD with RedHat Linux distribution. One CD contains all the necessary software for setup.
2. Sample configuration files for network (linux directory).
3. Sample source code & script files (linux directory).
4. LAN card configuration programs.
5. Sample configuration files.
6. Documentation files on Linux CD (HOWTO and FAQ).

Note that you will be required to save some configuration data on a blank disk.

### 3.1 Important Notes re Completing this Laboratory Exercise

- At the end of this exercise, the machines are to be restored to their original configuration. This requires the “boot” and “root” disks as detailed in the instructions. It is very important that these steps are followed, and that the disks are kept for restoring the hard disk images when directed to do so.
- This lab exercise does not require connection to the campus network.
- Note that instructions given herein are only in abbreviated form – students are expected to consult other references including:
  - Linux documentation on CD - called “HOWTO’s ” and “FAQ’s” (Frequently Asked Questions).
  - Unix manual pages – use `man command` to get the help entry on `command` if known, or `man -k keyword` for possible keyword matches. Use `man -s<section> topic` to get a specific section.
  - The Linux Internet sites – start from the local mirror at <http://mirror.aarnet.edu.au/>.
  - Books held in the library.

Portions of this document have been adapted from the various Linux HOWTO documents. They should serve as more extensive references when more details are desired than are provided here.

### 3.2 Hardware Setup

This section requires you to record the important hardware parameters and check the Ethernet network card.

1. If the LAN card is installed for the first time, Windows will detect Plug’n’Play PCI cards automatically. You may need to install the new driver files from the manufacturer’s supplied floppy (typically `a:\win95`) and install Windows protocol drivers (Windows distribution CD or `c:\cabs` ). Note that often the manufacturer’s drivers are more up-to-date than the drivers supplied with an operating system, and that the device/chipset names can be somewhat similar (and confusing).
2. Enter the system BIOS (usually Delete, F2 or F10 on bootup) and record any important system information:
  - (a) Disk size, number of heads, sectors etc.
  - (b) Installed RAM, CPU and clock rates.
  - (c) Video RAM and video chip type.
  - (d) Audio card information.
  - (e) Input/Output port information (parallel ports, serial ports etc).

Note: on later systems, `msinfo32` will display this information, and allow it to be saved as a text file.

3. Copy the Ethernet (LAN) disk to `c:\lancard`.
4. Boot the computer in DOS-only mode from a bootable floppy disk.
5. Run the setup program (`3c90xcfg` (3COM) or `rset8209` (Realtek), depending on the LAN card manufacturer).
6. Run the LAN card diagnostics to check the card.
7. Record the LAN card address. This will be six, 8-bit numbers such as 00-00-1c-01-08-78.
8. Note the I/O (Input/Output) address start (for example, 0x1020<sup>1</sup> and IRQ (interrupt) number (for example, 11).

### 3.3 Windows Network Setup

This section requires you to enter (or check) the network addresses under Windows.

1. Click Start-Settings-ControlPanel-Network
2. If TCP/IP is not already present, click Add-Protocol-Microsoft-TCP/IP.
3. Click on TCP/IP, then Properties.
4. The IP address, host name and network mask (netmask) should be as allocated in the “Network Hardware: Introduction” experiment.

### 3.4 Disk Partitioning

The systems will be setup as “dual-boot” – that is, two operating systems will be installed (Linux, a Unix implementation) and Microsoft Windows. Windows is already installed on each machine, and it is first necessary to *partition* the disk into two separate logical disks on the one physical disk.

**Note that this stage requires extreme care and attention to detail, as errors may render all files or even the disk itself unusable.**

If no bootable operating system is installed, it would be necessary to use `fdisk` to create initial disk partitions, followed by `format` to create the filesystem (under DOS) or `mkfs` under Unix. In some cases it may even be necessary to perform a low-level disk “hardware” format, which requires the diagnostic program appropriate to the disk manufacturer (Quantum, Seagate, Western Digital, etc).

---

<sup>1</sup>0x is often used to indicate hexadecimal, as in the C language.

Lab machines supplied for the these exercise have been configured to boot, and hence this step is not necessary. You should now consult the supervisor for further explanation.

There are two methods of partitioning: one is to use the `fips` tool to shrink the Windows partition, and manually set up the required Linux/Unix partitions. Another method is to use the built-in tools in the Linux installation to perform the partitioning. **You should ask the lab supervisor which method ought to be used at this time.** If not using `fips`, skip over to the section entitled “Linux Installation”.

To use `fips` to manually partition the disk, proceed as follows:

1. The first step is to partition the physical drive into logical drives. Linux will use several logical drives, for booting, virtual memory swap and the filesystem. The ABA computers have 10G hard drives, which have been partitioned using `fdisk` to 2G only. This partition will be “sliced” into four partitions for the linux installation, so that when completed the setup should be something similar to the following:

| Logical Drive | Size (approx) | Use         |
|---------------|---------------|-------------|
| c:            | 1G            | DOS/Windows |
| /             | 700M          | Linux root  |
| /boot         | 50M           | Linux boot  |
| swap          | 256M          | Linux swap  |

2. Boot into Windows. Double-click on MyComputer. Right-click on the c: drive icon, and select Properties.
3. Record the used and free disk space for later use.
4. Format two (2) floppy disks for use.  
**Never assume that so-called “preformatted” disks are actually formatted! You should always format them yourself.**
5. Format one of these floppies as a **bootable** disk using `format /s` and copy the `format` and `fdisk` programs onto the disk from the C: drive. **Check that you can boot your computer from this disk. If not, do not proceed, and ask the lab supervisor for instructions.**
6. From the directory `dosutils` on the CD, copy the files `fips.exe` and `restorrb.exe` onto the formatted floppy. **It is very important that this disk be kept aside for use later.**
7. Run `scandisk` on the hard disk to check for errors and incorrectly linked files.
8. Run `defrag`. Run a “full defragmentation”, even if the application recommends that it’s not necessary. Whilst it’s running, select `show details` to see the disk clusters being moved.
9. Record the “used” and “free” space on the drive.
10. Carefully go through the `fips` documentation on the CD.
11. Reboot off the bootable floppy disk.  
**You must boot in single-task DOS mode so that exclusive access to the disk is guaranteed.**
12. Change directory to A: and run `fips -d`.

13. Check the size allocations on the C: drive using `dir c: /v`
14. Split partition 1 (bootable partition).
15. Make a copy of the root and boot sectors as prompted, and record the disk physical information (bytes per sector, sectors per cluster etc).
16. Reduce the old (Windows) partition size. 1G for the new Windows partition and 1G for the new (Unix) partitions is appropriate.  
Note that it is not possible to shrink the old partition down below what is currently being used.
17. Once done using `fips`, the new partition will *not* be visible until after a reboot.  
**Note that the new partition will not be visible until after a reboot, so reboot immediately in order to force a re-read of the partition table.**
18. Reboot and check that the size of the C: drive has been reduced as was specified, using `dir c: /v`. Note that the new (D:) drive will not yet be visible, in that if you try to view it by typing `dir d: /v` you will get a disk failure error on that logical drive. This is to be expected, as there is no filesystem created yet on that partition.
19. Format the D: disk partition, and label the new partition as "linux".
20. Reboot to Windows and check that the new partitions are visible under Windows.
21. The linux partition will be further split into root, boot and swap partitions in the next steps, for a total of four logical partitions.
22. **When all the Linux laboratory exercises (this one and the next one) are completed, please restore the root and boot sectors using the first saved floppy image `rootboot.000`.**  
To do this:
  - (a) Boot from the DOS boot floppy.
  - (b) Run `restorrb` to restore the root and boot sectors from file `rootboot.000`.
  - (c) Reboot the computer in DOS mode in order to force a re-read of the partition table.
  - (d) Type `dir c:` to check the unused space.
  - (e) Reboot into Windows.
  - (f) Double-click on `MyComputer`. Right-click on the c: drive icon, and select `Properties`.
  - (g) Check that the total disk space equals that found originally on the PC.
  - (h) Run `scandisk` and then `defrag` to check the disk.

## 3.5 Linux Installation

The Linux operating system will now be installed. It may be installed via CD-ROM, a boot floppy, or from a network connection. The following assumes a boot floppy installation.

This section will be slightly different, depending on whether `fips` was used to manually partition the disk in the previous section. If `fips` was used, then the partitions created in the previous stage will be visible during the setup, and will only necessary to format the new partitions for use

with Linux. The following assumes that the partitions have already been set up using `fips`. If `fips` was not used, the partitioning will occur during this section of the exercise, and you will be prompted at the appropriate stage by the setup program.

1. Use the `rawrite` utility to write the file `boot.img`. Note that you cannot simply copy the boot image onto the floppy: it must be written sector-by-sector using `rawrite` (found in the `dosutils` directory of the CD).
2. After boot loading, a menu screen will appear. Follow the installation instructions, noting the following points. You should perform a minimal Linux installation, as most packages required for this exercise will be added later on.
3. Under Unix, the `hard disk` partitions are given mnemonic names `hda1`, `hda2`, etc.
4. Make sure you select “manual partition” in the installation.
5. Using the “Disk Druid” partitioning tool, delete the D: partition and add partitions as follows. Note that if `fips` was not used to manually partition previously, the partitions will have to be created at this stage. Make sure you leave the existing C: DOS/Windows drive alone.

| Device                 | Mount Point        | Size (approx) | Use                                    |
|------------------------|--------------------|---------------|----------------------------------------|
| <code>/dev/hda1</code> | –                  | 1G            | Existing C: DOS/Windows → do not touch |
| <code>/dev/hda2</code> | <code>/boot</code> | 50M           | Linux boot                             |
| <code>/dev/hda5</code> | <code>/</code>     | 700M          | Linux root                             |
| <code>swap</code>      | –                  | 256M          | Linux swap                             |

6. Notes:

- (a) A “rule of thumb” for swap space is to allocate about twice the amount of physical RAM.
  - (b) Many Unix systems require a slightly different partitioning scheme, with separate `/tmp`, `/var`, `/usr` partitions. There are advantages in doing this in practice — ask the lab instructor for further explanation.
7. Unix uses “mount points” for filesystems, meaning that sections of the filesystem used for different purposes may exist on different logical partitions, or even different physical disks<sup>2</sup>.
  8. Give the Linux Native partition a mount point of `/`
  9. Mark the `hda6` partition (256M) as “Linux Swap”.
  10. This will now make a filesystem of type `ext2` on the Linux boot and root partitions.
  11. When prompted for what packages to install, choose “custom” and select a minimal subset for now – more will be installed later once the system is running.
  12. Select 3-button mouse emulation.
  13. Do not configure the Local Area Network (LAN) at this stage – it will be done later after the system is installed.
  14. Install the bootloader in the Master Boot Record (MBR) on device `/dev/hda` (the primary physical drive).

<sup>2</sup>Later this will be seen with networked disks and other disk media.

15. Select the default boot partition to be the DOS partition.
16. Select an appropriate root (“superuser”) password. Note that this password gives access to all system resources, and in “real” systems should be kept in a known but highly secret location<sup>3</sup>.
17. Remove the CD and/or floppy and reboot.
18. For the boot loader to start Linux, type `linux` at the LILO: prompt.
19. Log in as `root` and view the files `/proc/ioports` and `/tmp/install.log`
20. XWindows is the graphical windowing system for Unix. Under Linux it is called XFree86. If the need arises to re-configure the graphical display, log in as `root` and run `Xconfigurator`<sup>4</sup>.
21. To run XWindows, type `startx` at the shell prompt. If you encounter video startup problems with X windows, press `ctrl-alt-backspace` and run `Xconfigurator` again. Press `ctrl-alt-numpad+` to change the video mode.
22. **Note on rebooting:** As the system kernel buffers open files in memory, it is imperative that the system be shut down “cleanly” and filesystem buffers flushed. You should log in as `root` and use one of `reboot`, `halt` or `shutdown -h now`. Do not switch off the power or softboot (`ctrl-alt-delete`) unless the system has been shut down cleanly. See also the `fsck` command.
23. Add a normal user account (called “auser”) using:  

```
useradd -d /home/auser -s /bin/bash auser
passwd auser
```

and set user `auser`’s initial password. Check the user logon sequence and permissions by setting up a remote terminal (telnet) session and logging in:  

```
telnet localhost
```

Check permissions (r/w/x) on files and directories, including `/home/auser`.
24. Several “virtual consoles” are provided under Linux. These are selected by using ALT-F1 to F6. To check the status of the current terminal processes use `ps`. To check background processes (including system “daemons”) use `ps ax`. Note the Process Identifier (PID) shown, as well as the controlling terminal (tty). To terminate a process, use `kill -9 PID` or `kill -SIGKILL PID`, where PID is the process ID, and the argument -9 is the signal number. The signal may be specified as a mnemonic (SIGKILL or SIGHUP, for example).
25. Switching between video modes is done using the key combination `control+alt+plus` (or `minus`). `Control+alt+backspace` kills the X server.

## 3.6 Linux Filesystems

This section examines the filesystem layout by showing how to access hard disks, floppy disks and CD-ROMs. Networked disks will be dealt with in a later section.

<sup>3</sup>If you forget the root password, type `linux single` at the LILO prompt.

<sup>4</sup>May be `redhat-config-xfree86` on some versions.

### 3.6.1 CD-ROM

1. Examine the `mount` command (`man mount`).
2. Examine the `fstab` file:  

```
cat /etc/fstab
```
3. Put the CD in the drive, and look at the CD mount point:  

```
ls -la /mnt/cdrom
```

There should be no files present.
4. Mount the CD file system using  

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```
5. The `/dev` directory contains device special files for various I/O devices. Disk devices are marked as `b` (for block).
6. If `/etc/fstab` contains an entry for CDROM, the type argument (`-t`) above is unnecessary.
7. The mount point should now contain the files on the CD:  

```
ls -la /mnt/cdrom
```
8. `/etc/mntab` shows the filesystems currently mounted.
9. Note that the eject button on the CD will now not eject the CD: you must unmount the CD using  

```
umount /dev/cdrom
```

and eject it using  

```
eject /dev/cdrom
```

Note that removable devices should be unmounted before removal!

### 3.6.2 Floppy Disk Files

The following shows how to access a floppy disk as if it were an extension of the Unix filesystem.

1. Floppy disks may be accessed at a mount point as with CD-ROMs. Use  

```
mount -t vfat /dev/fd0 /mnt/floppy
```

where type `vfat` is for Windows 95 long filenames (use `msdos` for 8+3 filenames), `fd0` is the name of the block special file, and `/mnt/floppy` is the mount point.
2. Use 

```
ls -la /mnt/floppy
```

 to see the floppy disk filesystem.
3. Use 

```
umount /dev/fd0
```

 to unmount the floppy. Note that removable devices should be unmounted before removal!
4. Note that Unix uses a forward slash `/` for the path separator, even though the it is a DOS filesystem. Linux files on the main Linux disk partition are an `ext2` filesystem which is quite different to a DOS filesystem.
5. Check to see that `/etc/mntab` contains an entry for the floppy when mounted.

## 3.7 Installing Packages

RedHat Linux uses the RedHat Package Manager (RPM) to install sets of files (“packages”) for various applications. To install a package:

1. Mount the CD-ROM as described previously.
2. Change to `RedHat/RPMS` under the mount point.
3. Look for a file with the required name – for example  

```
ls -la mtool*
```

having an extension `.rpm`
4. Use the install command  

```
rpm -i package.rpm
```

where *package* is the name of the package that you wish to install. Note that the option `--replacepks` may be required in some cases.
5. As an example, the “mtools” package allows an alternate method to mounting and unmounting the floppy drive. It is suitable for quickly viewing or copying a small number of DOS format files. It will provide commands such as `mmdir` and `mcopy` for accessing the floppy drive. You may require the `-t` switch for transferring Unix format text files to DOS and vice-versa. Another potentially useful package is “Midnight Commander” (`mc`), which is a menu-based file system interface for text terminals.
6. The RedHat Package Manager (RPM) has many options — for example, to query what packages contain, you might need to use  

```
rpm -q --filesbypkg --all
```

or  

```
rpm -q --filesbypkg -p *
```

## 3.8 Disk Restoration

If `fips` was used during the installation, please restore the root and boot sectors using the saved floppy image after **all** of the Linux laboratory exercises are completed. To do this:

1. Boot from the DOS boot floppy.
2. Run `restorrb` to restore the root and boot sectors from file `rootboot.000`.
3. Reboot the computer in DOS mode in order to force a re-read of the partition table.
4. Type `dir c:` to check the unused space.
5. Reboot into Windows.
6. Double-click on `MyComputer`. Right-click on the `c:` drive icon, and select `Properties`.
7. Check that the total disk space equals that found originally on the PC.
8. Run `scandisk` and then `defrag` to check the disk.

## Exercise 4

# Linux Networking (Linux Part 2)

**Aims** The aims of this laboratory task are:

1. To install, configure and test networking for both Microsoft Windows and Linux networking.
2. To install and configure some important network applications (as time permits):
  - (a) Unix-to-Unix file sharing (Network File System or NFS).
  - (b) Unix-to-Windows file sharing (SMB, or "Samba").
  - (c) Dynamic Host Configuration Protocol (dynamic IP address assignment, or DHCP)
  - (d) Web clients and Web server.
  - (e) Domain Name Server (DNS).

**Hardware** The hardware supplied may vary, but requires the following for completion of the entire exercise:

1. Intel-based PC's (CD drive for Linux CD installation required).
2. 3Com and/or Lantech 8029 network cards (1 or 2 per PC).
3. Lantech Ethernet hubs or switches.
4. 10BASET cabling.
5. A blank floppy for DOS-only reboot and for saving disk partition tables, boot sector information and file allocation tables.
6. 2Omega ZIP drives.

**Software** The following software will be supplied:

1. Linux CD with RedHat Linux distribution. One CD contains all the necessary software for setup.
2. Sample configuration files for network (linux directory).
3. Sample source code & script files (linux directory).
4. LAN card configuration programs.
5. Sample configuration files.
6. Documentation files on Linux CD (HOWTO and FAQ).

Note that you will be required to save some configuration data on a blank disk.

## 4.1 Important Notes re Completing this Laboratory Exercise

- The practical “Linux Installation” should be completed and the installation thoroughly tested before attempting this laboratory exercise.
- At the end of this exercise, the machines are to be restored to their original configuration. This requires the “boot” and “root” disks as detailed in the instructions. It is very important that these steps are followed, and that the disks are kept for restoring the hard disk images when directed to do so.
- This lab exercise does not require connection to the campus network.
- **Note 4 – very important:** The examples output data and configuration files are shown for illustration only. You should use the IP address and subnet mask as assigned to your particular machine(s) during the laboratory class. Using IP addresses incorrectly can cause major network disruption to other users, and you will be held responsible. If unsure, ask the supervisor.
- The following examples were generated using a subnet mask of 255.255.248.0. You should work through and understand the examples given. The subnet mask for this area has now changed to 255.255.255.0 and you must use this mask.
- The following exercises are focused on learning the various protocols and software systems. Security of any computer system must be a paramount consideration. Only a cursory treatment of this important matter has been given here – for real applications it is necessary to consult the appropriate security HOWTO and FAQ sections, together with one of the many published books on Linux.

## 4.2 Linux Network Setup

This section gives a basic overview of how to configure local and wide-area networking.

### 4.2.1 Ethernet Card

To set up the Ethernet card (also called NIC or Network Interface Card):

1. `ifconfig` should show that no network interface is present (only the local loopback address `lo`).
2. Add a line of the form  
`alias eth0 ne2k-pci`  
or  
`alias eth0 3c59x`  
to `/etc/conf.modules` to define the driver object module to be loaded. Some older ISA and non-PnP cards may need explicit specification of the I/O and interrupt parameters, for example:

```
alias eth0 ne
options ne io=0x220 irq=3
```

3. eth0 is the primary Ethernet interface. Install a driver for the interface using `modprobe eth0`
4. `ifconfig -a` should show interface eth0 “down” (not running).
5. The appropriate IP network parameters for the laboratory were given earlier under “Windows Network Setup”. Assuming the workstation being configured has IP address 139.86.64.223, enable the interface using `ifconfig eth0 up 139.86.64.223 netmask 255.255.248.0`
6. Connect the 10BASET network cable and check again using `ifconfig` that the interface is receiving packets. You should see something like the following.

```
lo Link encap:Local Loopback
 inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
 UP BROADCAST LOOPBACK RUNNING MTU:3584 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0

eth0 Link encap:Ethernet HWaddr 00:00:1C:01:08:78
 inet addr:139.86.64.223 Bcast:139.86.71.255 Mask:255.255.248.0
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:648 errors:0 dropped:0 overruns:0 frame:6
 TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0
 Interrupt:11 Base address:0x1020
```

7. The “ping” command sends out a test packet which should be returned by the software protocol stack on the remote machine. Again assuming this machine is 139.86.64.223, type `ping 139.86.64.223`  
This gives “network unreachable” which at first may not make sense, because it is the same physical machine (ie does not need to access the network at all). However, it is necessary to add the routing before any connections will operate. This is covered in the following subsection.

### 4.2.2 Host-to-Network Routing

To configure routing once the Ethernet card is operational, you must do the following:

1. The commands `route` or `netstat -rn` show the current routing table information.
2. Add a route to the local network:  
`route add -net 139.86.64.0 netmask 255.255.248.0 eth0`  
This will provide a route to machines on the local network (denoted by 0 in the host portion of the address).

3. Machines on the same subnet will now be visible, but outside the subnet will not. For example, another machine
 

```
ping 139.86.64.222
```

 will work satisfactorily, but
 

```
ping 139.86.128.2
```

 will not (yet) work.
4. Add a default route to the gateway:
 

```
route add default gw 139.86.64.1
```

 where 139.86.64.1 is the address of the router.
5. Machines on other networks will now be visible:
 

```
ping 139.86.128.2
```

 should work correctly.
6. Add the hostname and domain name:
 

```
hostname lab1
```

```
domainname eng.usq.edu.au
```

 (Remember to use the correct hostname).
7. The routing tables (`route -n` or `netstat -rn`) should show something similar to the following:

| Kernel IP routing table |             |               |       |       |
|-------------------------|-------------|---------------|-------|-------|
| Destination             | Gateway     | Genmask       | Flags | Iface |
| 139.86.64.0             | *           | 255.255.248.0 | U     | eth0  |
| 127.0.0.0               | *           | 255.0.0.0     | U     | lo    |
| default                 | 139.86.64.1 | 0.0.0.0       | UG    | eth0  |

### 4.2.3 Network Router Setup

This section requires machines with two Ethernet cards to be installed and separate subnets set up. You will need to set up subnetworks as appropriate for your network cabling, and will need to co-operate with other groups in the lab.

Before starting, draw a diagram of the networks containing IP addresses, Ethernet device names on Linux, and Ethernet addresses.

For the machines designated as routers:

1. Edit `/etc/conf.modules` and add the driver specification:
 

```
alias eth1 3c59x
```

 to `/etc/conf.modules` to define the driver object module to be loaded. Note that this may vary depending on the cards installed. If in doubt, boot Windows and check under Start, settings, control panel, system, device manager, network adapters, properties, resources.
2. Use `ifconfig -a` to determine the current status of the cards.
3. Use `modprobe` to probe the cards and load the drivers.

4. Configure the `eth0` and `eth1` interfaces with correct IP address, subnet mask and gateway.
5. Add routes for each network card using the `route add -net` command.
6. The routing tables (`route -n` or `netstat -rn`) should show something similar to the following:

| Kernel IP routing table |         |               |       |        |       |
|-------------------------|---------|---------------|-------|--------|-------|
| Destination             | Gateway | Genmask       | Flags | Metric | Iface |
| 139.86.64.0             | *       | 255.255.255.0 | U     | 0      | eth0  |
| 139.86.67.0             | *       | 255.255.255.0 | U     | 0      | eth1  |
| 127.0.0.0               | *       | 255.0.0.0     | U     | 0      | lo    |

7. Check that another machine on the *same* subnet is visible via `ping`.
8. Set the TCP/IP configuration to use the correct gateway using the `route add default gw` command.
9. From one of the machines try to ping a machine on *another* subnet. This will fail. The “continuous” option to ping may be useful to continuously ping the remote machine. Even though the interfaces and routes to each subnet are set up, forwarding of the IP packets by the kernel is not enabled by default.
10. To forward IP packets, the kernel IP forwarding must be enabled. To do this, set enter the single value 1 in the file `/proc/sys/net/ipv4/ip_forward`

To disable IP forwarding, enter the value of 0 in this file. Try changing the value whilst the other machines on the subnet are executing a continuous ping (`ping -t`).

11. Further information may be obtained in the Security-HOWTO and the manual entries for “hosts.allow” and “hosts.deny”.

#### 4.2.4 Name Services

Domain name services may now be accessed. These provide mappings from names such as `www.usq.edu.au` to the corresponding IP number.

1. The file `/etc/hosts` contains *static* routes. Edit this file as appropriate, to contain at least the localhost (loopback) and host name/address.

|               |                                 |
|---------------|---------------------------------|
| 127.0.0.1     | localhost localhost.localdomain |
| 139.86.64.222 | lab222                          |
| 139.86.64.223 | lab223                          |

2. The file `/etc/resolv.conf` contains the addresses of the DNS (Domain Name Service) nameservers. Type `man resolver` for further information or consult a reference on DNS.

3. The resolver file should contain:

```
search eng.usq.edu.au usq.edu.au
nameserver 139.86.128.2 139.86.128.3
```

4. The file `/etc/nsswitch.conf` determines the search order for names (local file or DNS server). It should contain a line of the form:

```
hosts: files dns
```

5. Once the name service can be accessed, you should be able to connect to remote machines via a host name on the local subnetwork:

```
ping icarus
or a fully-qualified name elsewhere:
ping mirror.aarnet.edu.au
```

#### 4.2.5 Network Monitoring

1. Install the `tcpdump` package from CD.
2. Run `tcpdump` and investigate the various packet filtering options.

## 4.3 Serial Line Interconnection

Standard RS232 serial ports are used for a variety of uses, from a local character-mode terminal (normally using VT100 terminal emulation) through to a full Internet connection to a remote Internet Service Provider (ISP), using the Point-to-Point protocol (PPP) through a modem.

### 4.3.1 Serial Ports under Linux

The following shows how to set up a serial port for character-mode communications.

1. Serial terminals normally exist under the `/dev/tty` device file entries. The `stty` command is used to check the characteristics of the current terminal interface. Examine the settings for your current terminal in conjunction with the manual page.
2. Linux provides the `setserial` command to manipulate the hardware characteristics of the serial ports. From the Serial HOWTO, the association between serial (COM) ports and device special files is:

| Device Special File     | Serial Port | I/O Address | IRQ |
|-------------------------|-------------|-------------|-----|
| <code>/dev/ttyS0</code> | COM1        | 3F8 H       | 4   |
| <code>/dev/ttyS1</code> | COM2        | 2F8 H       | 3   |
| <code>/dev/ttyS2</code> | COM3        | 3E8 H       | 4   |
| <code>/dev/ttyS3</code> | COM4        | 2E8 H       | 3   |

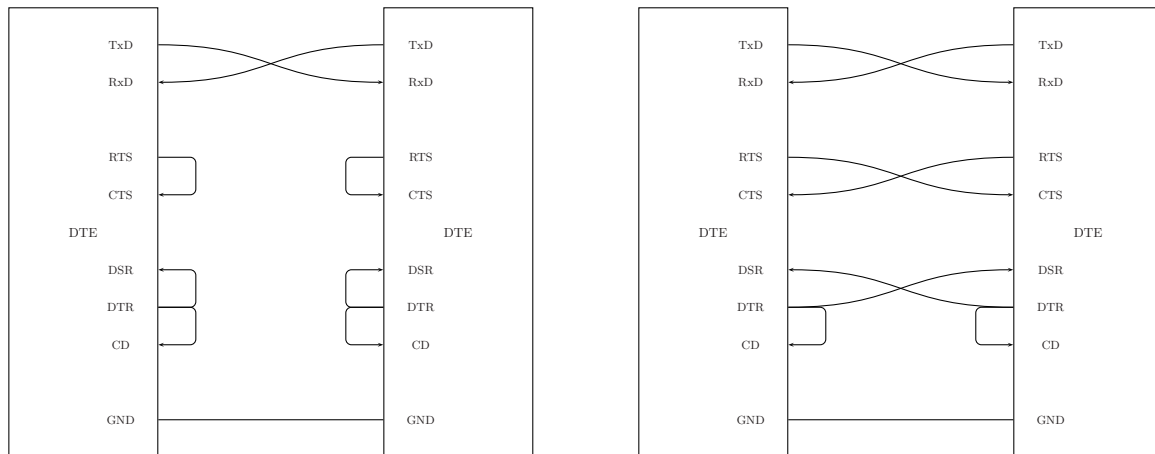


Figure 4.1: Null modem connection using inband XON/XOFF (software) flow control (left) and out-of-band (hardware) handshaking (right).

Examine the serial configuration for the COM1 port:

```
setserial /dev/ttyS0
```

3. Load the `statserial` package. Run this program, and check that the control line changes are detected.
4. `minicom` is a terminal emulation program. Install the package using `rpm`. The terminal emulation is normally the VT100 standard (sometimes VT550). This is normally configurable in the serial terminal program. The first time you run `minicom` it may need to be invoked in setup mode: `minicom -s`. The control keys `ALT-A 0` and `ALT-A X` configure the options and exit, respectively.
5. Serial interconnections were originally defined to connect a computer (Data-Circuit Terminating Equipment, or DTE) to a modem (Data Communications Equipment, or DCE). Figure 4.1 shows the required handshaking arrangement when connecting two PC's (DTE's) using software flow control. This is also called "inband" flow control, as it uses ASCII characters XON and XOFF to control the flow and prevent buffer overrun at either end. XON is ASCII character 17 (also called DC1 or device control 1) and may be generated from the keyboard using control-Q. XOFF is ASCII character 19 (also called DC3 or device control 3) and may be generated from the keyboard using control-S. (Note that other combinations such as control-L for clear screen are sometimes useful in terminal emulation) Figure 4.1 also shows the handshaking arrangement using hardware flow control using RTS (Request to Send) and CTS (Clear to Send) control lines.
6. Connect a Linux PC to a Windows terminal. On Windows run the terminal emulator `hyperterm`. On the Linux PC run `minicom`. Alternatively, connect two Linux PC's running `minicom`. Take care to set up the baud rates, parity, stop bits and especially handshaking. Typing on one keyboard should show the characters on the other screen (but note that the characters are not echoed to the same PC's screen).
7. If a modem is available, connect it to the serial port. Modems respond to the Hayes command set, which usually begin with `AT` (attention) followed by return. A modem manual will provide full commands and explanations. Some common commands are:

| Command    | Meaning                                     |
|------------|---------------------------------------------|
| ATZ        | Reset modem.                                |
| ATI        | Return identification string.               |
| ATDT123456 | Dial using tone dialling the number 123456. |
| +++        | Abort the current operation.                |

### 4.3.2 Serial Terminal

The following extends the previous section to enable a user to log-on to the Unix system via the serial port.

1. Ensure that the previous section was completed satisfactorily.
2. Type `ps ax` to see that a `getty` process (or some variation) is running for the consoles. This process is responsible for sending the `login:` prompt then accepting and checking the password. Examine the manual entry for `getty`.
3. Install the `mgetty` package. Check the manual entry for `mgetty`.
4. Connect two PC's as previously and run `minicom` on the second PC. On the first, run a login on serial port COM1 from the command prompt:  

```
/sbin/mgetty -r -s 9600 -p"Please log in:" /dev/ttyS0
```
5. Note that when a user attempts to log in on the serial terminal the `mgetty` process exits. This is because it sends a hangup signal (SIGHUP) to its parent. The `getty` process is meant to be run from the `init` process, which starts all other processes.
6. Examine the manual for `init`. Use `ps ax | more` to find the PID of `init`.
7. The file `/etc/inittab` specifies the processes run by `init`. Examine the manual for `inittab`.
8. In the `inittab` file, find where the `getty`'s are spawned and add:  

```
SL1:3:respawn:/sbin/mgetty -r -s 9600 -p"log in:" /dev/ttyS0
```

It will be necessary to force `init` to re-read the `inittab` file:  

```
init q
```
9. Check that logins are re-started as you log in and out of the terminal connected to the serial port. Note that for security reasons, `root` is not allowed to log in to a serial port, only the console itself.
10. Check the log file:  

```
tail /var/log/mgetty.log.ttyS0
```

### 4.3.3 PPP: Point to Point Protocol

The serial port is often used to connect to a modem which dials an an Internet Service Provider (ISP). This gives the local (client) machine an IP address so that it may access internet services

as if connected on an Ethernet LAN. Because the connection is transient some restrictions apply, however. The protocol used is PPP (Point-To-Point Protocol).

This section will show the basics of how to setup a PPP server and client. PPP is a “peer protocol”, meaning that both sides are treated equally. This is unlike, for example, DHCP, where the server and client are expressly delineated (different software ports and executables for the daemons). Note that the emphasis here is on setting up the connection: the important aspect of security is not covered. This should not be neglected, as a server which does not authenticate connections allows free and potentially very damaging access from the outside world. See the PPP HOWTO or one of the many texts available for further information.

1. Install the PPP package. Examine the `pppd` (PPP daemon) manual entry.
2. Designate one machine as a server and one as a client. Connect the serial ports of these using the hardware handshaking interconnection as outlined previously.
3. Configure the Ethernet interface on the server. For this example it will be designated as 139.86.67.223:

```
ifconfig eth0 up 139.86.67.223 netmask 255.255.248.0
route add -net 139.86.64.0 netmask 255.255.248.0
```

4. Ensure that *no* networking at all is installed on the client. For this example it will be designated as 139.86.67.222 (this will be allocated via the PPP connection).
5. Check the `ifconfig -a` on both server (Ethernet only) and client (no networking yet).
6. The following two steps show the commands to start the server and client daemons. Enter the commands but do not press enter yet.
7. The *server* command line to start the PPP daemon will be (on one line):

```
pppd /dev/ttyS0 9600 -detach crtscts debug proxyarp 139.86.67.223:139.86.67.222
netmask 255.255.248.0 &
```

Here:

- `/dev/ttyS0` is the serial port COM1.
  - 9600 is the baud rate.
  - `-detach` stops the daemon from detaching from the controlling terminal. If the controlling terminal hangs up then the ppp daemon exits.
  - `crtscts` specifies hardware flow control via RTS and CTS lines.
  - `debug` outputs additional diagnostic messages.
  - `proxyarp` enables address resolution as if the machine were on an Ethernet.
  - The IP addresses are specified as “LocalAddress:RemoteAddress”.
  - The ampersand `&` is the Unix convention for putting a process in the background.
8. The *client* command line to start the PPP daemon will be:
 

```
pppd /dev/ttyS0 9600 crtscts debug defaultroute &
```

Here:

- defaultroute specifies IP packet forwarding to be done to the PPP link.
  - The IP address is allocated by the server during the LCP (link control protocol) phase.
9. If an oscilloscope is available connect it to the transmit line for monitoring.
  10. Start both processes and check the log file:  
tail -f /var/log/messages

The -f option to tail shows a continuous output as the log file is being written. If the oscilloscope is available note the packets being sent. The log file on the server should appear similar to the following:

```
May 4 17:18:20 localhost pppd[321]: pppd 2.3.5 started by root, uid 0
May 4 17:18:20 localhost pppd[321]: Using interface ppp0
May 4 17:18:20 localhost pppd[321]: Connect: ppp0 <--> /dev/ttyS0
May 4 17:18:20 localhost pppd[321]: found interface eth0 for proxy arp
May 4 17:18:20 localhost pppd[321]: local IP address 139.86.67.223
May 4 17:18:20 localhost pppd[321]: remote IP address 139.86.67.222
```

The log file on the client should appear similar to the following:

```
May 4 17:25:58 localhost pppd[329]: pppd 2.3.5 started by root, uid 0
May 4 17:25:58 localhost pppd[329]: Using interface ppp0
May 4 17:25:58 localhost pppd[329]: Connect: ppp0 <--> /dev/ttyS0
May 4 17:26:24 localhost pppd[329]: local IP address 139.86.67.222
May 4 17:26:24 localhost pppd[329]: remote IP address 139.86.67.223
```

11. Check the interface configuration using  
ifconfig -a

The interface on the server should appear similar to the following:

```
lo Link encap:Local Loopback
 inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
 UP BROADCAST LOOPBACK RUNNING MTU:3584 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0

eth0 Link encap:Ethernet HWaddr 00:00:1C:01:08:AA
 inet addr:139.86.67.223 Bcast:139.86.255.255 Mask:255.255.248.0
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:5 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0
 Interrupt:11 Base address:0x1020

ppp0 Link encap:Point-to-Point Protocol
 inet addr:139.86.67.223 P-t-P:139.86.67.222 Mask:255.255.248.0
 UP POINTOPOINT RUNNING MTU:1500 Metric:1
 RX packets:5 errors:0 dropped:0 overruns:0 frame:0
 TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0
 Memory:101c038-101cc04
```

The interface on the client should appear similar to the following:

```

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
 UP BROADCAST LOOPBACK RUNNING MTU:3584 Metric:1
 RX packets:95 errors:0 dropped:0 overruns:0 frame:0
 TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0

ppp0 Link encap:Point-to-Point Protocol
 inet addr:139.86.67.222 P-t-P:139.86.67.223 Mask:255.255.0.0
 UP POINTOPOINT RUNNING MTU:1500 Metric:1
 RX packets:77 errors:0 dropped:0 overruns:0 frame:0
 TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0
 Memory:1115038-1115c04

```

12. On the client try to connect to the server:  
`ping 139.86.67.223`  
 This should work due to the default route.
13. On the server try to connect to the client:  
`ping 139.86.67.222`

## 4.4 NFS: Network File System

NFS provides a method for Unix system to share files across a network, without explicitly copying the files themselves (such as via ftp). In keeping with the Unix philosophy of mountable volumes, the remote filesystems appear as part of the local filesystem hierarchy. Two systems are obviously required: an NFS *server* which shares files, and one (or more) NFS *clients* which are able to access those files permitted by the server. Security is an important issue – thus, permissions may be controlled (machine IP address, read-only access) with access logging.

The following files are of interest:

|                                 |                       |
|---------------------------------|-----------------------|
| <code>/var/log/messages</code>  | system log file       |
| <code>/var/log/secure</code>    | security log file     |
| <code>/var/lib/nfs/rmtab</code> | nfs log file          |
| <code>/proc/filesystems</code>  | supported filesystems |
| <code>/etc/fstab</code>         | filesystem table      |
| <code>/etc/mtab</code>          | mounted filesystems   |

### 4.4.1 NFS Server

1. Install the NFS package off CD (install the `nfs-server` package and *not* the `nfs-client` package).

2. The following assumes the IP address of the local machine (NFS server) is 139.86.64.222 and the files to be shared reside under `/home/auser` – you should modify for your situation as appropriate. The remote machine (client) is assumed to be 139.86.64.223
3. If another machine is not available for testing at this stage, the client and server may be on the same machine – this may be confusing to the newcomer, however.
4. Check that the local machine has a hostname to IP address mapping in its “hosts” file. The hosts file `/etc/hosts` consists of one-line entries, with the IP address, one or more spaces, followed by the host name. The host name does not have to be fully qualified in this situation (local network only).
5. Note that the *server* must also have an entry for the *client* in its “hosts” file, otherwise “permission denied” errors will occur on the remote (client) machine.
6. In the `/etc/exports` file, add  
`/home/auser 139.86.64.223(rw)`  
Normally the IP address would be replaced with a fully qualified domain name, but the workstations will not have domain names established as yet.
7. It is possible to omit the IP or hostname altogether in the exports file when testing – however, this allows virtually unrestricted access and should be avoided in practice.
8. The shared directory on the server must have execute (x) permission for “others” (o) set to enable sharing. Do this using the `chmod` command and use `ls -la /home` to check.
9. To start the NFS server, give the commands  
`rpc.mountd`  
`rpc.nfsd`  
This starts the daemon processes. If the exports file is modified, it is necessary to force the NFS daemon to re-read it. This is done using `exportfs -a`

#### 4.4.2 NFS Client

1. It is *not* necessary to install the NFS package off CD – the standard `mount` command is used (with variations).
2. Check that the server machine has a hostname to IP address mapping in `/etc/hosts`. Put an entry in this file for the remote machine as well.
3. Create a mount point:  
`mkdir /mnt/remote`
4. Mount the remote filesystem:  
`mount -t nfs 139.86.64.222:/home/auser /mnt/remote`  
(Change the IP address and directories as appropriate).
5. If a “permission denied” error occurs or no files are visible, you will need to check the permissions on the server-side shared directory and files. The directory should have execute permission for the user. Change if necessary using the `chmod` command and check using `ls -la`

6. Check that the filesystem is visible:

```
ls -la /mnt/remote
```

7. Unmount the filesystem:

```
umount /mnt/remote
```

8. Exercise: What happens to the NFS client if the NFS server unexports a filesystem using `exportfs` whilst the client is connected?

## 4.5 SMB (Samba): Unix-Windows Network File Sharing

Samba allows Unix files to be accessible on Windows/DOS systems via the SMB (Server Message Block) protocol. A networked workstation running Windows must be connected to the LAN for this section of the exercise.

1. Install the samba RPM package from the CD. This is the package whose name starts with “samba”, *not* the one starting with “smbfs”.
2. Examine `man smb.conf` for configuration details. Edit `/etc/smb.conf` and set:

```
workgroup = MYGROUP
Server String = I am a Samba Server
```

(or something else recognisable). If the LAN is not connected to the any NT domain, the Samba server must be configured as a domain master browser as per the following point.

3. Configure the machine as a domain master browser with logons enabled. If the LAN is isolated from a remote LanManager server, it will be necessary to do this before proceeding further. Set the following in `/etc/smb.conf`

```
workgroup = MYGROUP
remote browse sync = 139.86.64.255
remote announce = 139.86.64.255
domain master = yes
domain logons = yes
```

4. Setup the “share definitions” in `/etc/smb.conf` to have, at a minimum, home directories shared. Set `browseable` and `writable` to `yes`.
5. Note that the *server* must have an entry for *itself* in its “hosts” file. If not, the Samba log file will contain “could not get hostname” errors. The hosts file `/etc/hosts` consists of one-line entries each with an IP address, one or more spaces, followed by the host name. The host name does not have to be fully qualified in this situation (local network only).
6. Ensure that the server has a hostname consistent with the definition in `/etc/hosts` — if not, use the `hostname` command to set it.

7. The command  
`samba start`  
starts the daemons: `smbd` (LanManager SMB protocol, for filespace and print services) and `nmbd` (NetBios/WINS nameserver). Samba is normally installed to `/usr/sbin` on this system. Stop the services using `samba stop` and obtain status using  
`samba status`
8. Reboot Windows on the remote workstation and log on as one of the Unix users. You should be asked for a domain name as well as a login name and password. If the domain is not requested, check the Network settings in the Control Panel, under “Client for Microsoft Networks”. This should be configured to “Log on to NT Windows Domain”.
9. On the Windows client, choose `NetworkNeighbourhood` then `View-Refresh`. Note that it may take a minute or so for the server to advertise the shared filesystem.
10. Some (but not all) versions of Windows use an encrypted password by default, and it may be necessary to use plaintext passwords to work correctly with the Samba server. To do this, examine the registry using `regedit`, search for `EnablePlainTextPassword`, and set it to true (1).
11. If any “cannot connect” or “permission denied” errors occur, check the status of the server in `/var/log/samba/log.nmb`. Also check the file with the name of the remote machine in the same directory (use the `tail -f` command). If no files are visible on the Windows system or permission errors still occur, check the permissions on the server-side shared directory and files. The directory should have execute permission for the remote/Unix user. Change if necessary using the `chmod` command.
12. Once the Unix filesystem is visible on the PC, check  
`/var/log/samba/log.smb`, `log.smb` and `log.clientmachine`  
(the latter is the Windows client machine host name).

## 4.6 DHCP: Dynamic Host Configuration Protocol

DHCP allows the dynamic allocation of IP addresses to client machines. This may be useful in order to reduce the administrative load of physically assigning and checking IP addresses and netmasks on a LAN.

Performing the following lab experiment will require two machines: one for the DHCP client and one (or more) for the DHCP server. These should not have any networking installed, and hence it is recommended that you re-install a fresh copy of Linux before starting. Otherwise static IP assignments and routing may cause confusion.

The “HOWTO” document for DHCP is located in the `doc` directory under `mini`.

For the *server*:

1. As performed in an earlier experiment, install the Ethernet card drivers and configure networking as follows:
  - (a) Add a line of the form

```
alias eth0 ne2k-pci
```

to `/etc/conf.modules`. Some cards may need explicit specification of the I/O and interrupt parameters, for example:

```
alias eth0 ne
options ne io=0x240 irq=5
```
  - (b) `eth0` is the primary Ethernet interface. Install a driver for the interface using

```
modprobe eth0
```
  - (c) `ifconfig -a` should show interface `eth0` “down” (not running).
  - (d) The appropriate IP network parameters for the laboratory were given earlier under “Windows Network Setup”. Assuming the workstation being configured has IP address 139.86.64.223, enable the interface using

```
ifconfig eth0 up 139.86.64.223 netmask 255.255.248.0
```
  - (e) Add a route to the local network:

```
route add -net 139.86.64.0 netmask 255.255.248.0 eth0
```

This will provide a route to machines on the local network (denoted by 0 in the host portion of the address).
  - (f) Add a default route to the gateway:

```
route add default gw 139.86.64.1
```

where 139.86.64.1 is the address of the router.
  - (g) `ifconfig -a` should show interface `eth0` “up” (running).
2. Install the `dhcp` package off CD.
3. Examine `man dhcp` for configuration details.
4. Add the configuration file `/etc/dhcpd.conf` — it will be similar to the following:

```
default-lease-time 60;
max-lease-time 60;
option subnet-mask 255.255.248.0;
subnet 139.86.67.0 netmask 255.255.248.0
{
 range 139.86.67.228 139.86.67.230;
}
```

5. Note that the above specifies a configuration for IP address allocation of 60 seconds. This is useful for demonstration purposes but in a real setup would more likely be of the order of several hours to one day.
6. In addition, it is possible to set the configuration to always allocate a fixed IP address to a certain hardware (Ethernet) address, as the following example shows. See the HOWTO document for details.

```
host lab222
{
 hardware ethernet 00:00:1C:01:08:78;
 fixed-address 139.86.67.222;
}
```

7. Create the lease file using  

```
touch dhcpd.leases
```

This file may be under either `/etc` or `/var/state/dhcp`, depending on the version in use.
8. Set the IP broadcast address to operate correctly with DHCP<sup>1</sup>:  

```
route add -host 255.255.255.255 dev eth0
```
9. The installation creates the startup script in the normal startup files `/etc/rc.d/init.d`  
You may also wish to check `/etc/rc.d/rc3.d`  
where 3 is the runlevel (see the `runlevel` command).
10. Reboot or run the startup script:  

```
/etc/rc.d/init.d/dhcpd start
```

The `start` argument may be `stop`, `restart` or `status`
11. Checking will be performed after the client is setup.

For the *client*, either Windows or Linux may be used as a client. As the lab supervisor which one should be used. For a Windows client, all that is necessary is to select “Assign an IP address automatically” in the TCP/IP setup; skip the Linux client sections below and go straight to the Windows client setup section.

For a Linux client, proceed as follows:

1. Install the `dhcp` package off CD.
2. Examine `man dhcp` for configuration details.
3. Check via `ifconfig -a` that no Ethernet networking is installed.
4. As performed in an earlier experiment, install the Ethernet card drivers as follows.
5. Add the configuration for the network card into `/etc/conf.modules` as determined earlier, but do *not* set up the the IP address.
6. `ifconfig -a` should show interface `eth0` “down” (not running).
7. Install `tcpdump` if not already installed. Run `tcpdump` to monitor network traffic.
8. If Linux was installed for DCHP, start the client from the script:  

```
/etc/rc.d/init.d/dhcpd start
```

Otherwise, start from the binary `/sbin/dhcpd`
9. Checking will be performed in the next stage.

Check that DCHP is operational:

---

<sup>1</sup>From the DHCP mini-HOWTO. Some client/server combinations may require additional setup at this stage.

1. Note that because the client and server are background daemon processes, the request for an IP address may take several seconds to be answered by the DHCP server. Also, the following examples have been generated using a 60 second lease time – as stated above, a more realistic time is of the order of one hour to one day.
2. On the DHCP *server*:
  - (a) The file `/etc/dhcpd.leases` should contain something like:

```
lease 139.86.67.228
{
 starts 1 1999/05/03 17:51:16;
 ends 1 1999/05/03 17:52:16;
 hardware ethernet 00:00:1c:01:08:78;
 uid 01:00:00:1c:01:08:78;
}
```

- (b) The file `/var/log/messages` should contain something like<sup>2</sup>:

```
kernel: ne.c: PCI BIOS reports NE 2000 clone at i/o 0x1020, irq 11.
kernel: ne.c:v1.10 9/23/94 Donald Becker (becker@cesdis.gsfc.nasa.gov)
kernel: NE*000 ethercard probe at 0x1020: 00 00 1c 01 08 aa
localhost kernel: eth0: NE2000 found at 0x1020, using IRQ 11.
...
kernel: Swansea University Computer Society IPX 0.34 for NET3.035
kernel: IPX Portions Copyright (c) 1995 Caldera, Inc.
kernel: Appletalk 0.17 for Linux NET3.035
dhcpd: Internet Software Consortium DHCPD $Name: V2-BETA-1-PATCHLEVEL-6 $
dhcpd: Copyright 1995, 1996, 1997, 1998 The Internet Software Consortium.
dhcpd: All rights reserved.
dhcpd: Listening on Socket/eth0/139.86.64.0
dhcpd: Sending on Socket/eth0/139.86.64.0
dhcpd: DHCPDISCOVER from 00:00:1c:01:08:78 via eth0
dhcpd: DHCPOFFER on 139.86.67.228 to 00:00:1c:01:08:78 via eth0
dhcpd: DHCPREQUEST for 139.86.67.228 from 00:00:1c:01:08:78 via eth0
dhcpd: DHCPACK on 139.86.67.228 to 00:00:1c:01:08:78 via eth0
dhcpd: DHCPREQUEST for 139.86.67.228 from 00:00:1c:01:08:78 via eth0
dhcpd: DHCPACK on 139.86.67.228 to 00:00:1c:01:08:78 via eth0
dhcpd: DHCPREQUEST for 139.86.67.228 from 00:00:1c:01:08:78 via eth0
dhcpd: DHCPACK on 139.86.67.228 to 00:00:1c:01:08:78 via eth0
```

3. On the DHCP Linux *client*:
  - (a) The file `/etc/dhpcp/hostinfo-eth0` is created when a DHCP lease is allocated, and should contain something like:

```
LEASETIME=60
RENEWALTIME=30
REBINDTIME=52
IPADDR=139.86.67.228
NETMASK=255.255.248.0
BROADCAST=139.86.71.255
```

- (b) The file `/var/log/messages` should contain something like:

<sup>2</sup>You may need to use the `tail -f -n10` command here as the `messages` file may be quite long.

```
kernel: ne.c: PCI BIOS reports NE 2000 clone at i/o 0x1020, irq 11.
kernel: ne.c:v1.10 9/23/94 Donald Becker (becker@cesdis.gsfc.nasa.gov)
kernel: NE*000 ethercard probe at 0x1020: 00 00 1c 01 08 78
kernel: eth0: NE2000 found at 0x1020, using IRQ 11.
dhcpcd[588]: no DHCP OFFER messages
...
dhcpcd[594]: assigned IP address: 139.86.67.228
dhcpcd[594]: assigned subnetmask: 255.255.248.0
dhcpcd[594]: got in BOUND state
dhcpcd[594]: got in RENEWING state
dhcpcd[594]: got in BOUND state
dhcpcd[594]: got in RENEWING state
dhcpcd[594]: got in BOUND state
```

4. To setup a Windows machine to use DHCP, click Start-Settings-ControlPanel-Network
5. If TCP/IP is not already present, click TCP/IP-Properties.
6. Set the IP address to "Obtain an IP address automatically".
7. Click Start-run, then type `winipcfg`
8. Watch `tcpdump` running on Linux, and click `renew` on the Windows PC. You should see the traffic relating to the DHCP request and reply.
9. As an additional exercise, use a Windows machine as the DHCP client (check "obtain IP address automatically" in the Windows setup). The server operation remains unchanged.

## 4.7 Web Server Installation

First, install a Web browser:

1. Use `rpm -i` to install Netscape Communicator.
2. Start XWindows: `startx`
3. From a shell window, type `netscape`.
4. Configure proxy access, if external off-campus is desired. Select `edit-preferences-advanced-proxies`.
5. For the staff proxy, select automatic proxy configuration from `www.usq.edu.au/proxy/staff.proxy`.
6. For the student proxy, select proxy configuration as `proxy.connect.usq.edu.au` with port 8080.
7. If on-campus access is desired, check that `http://www.usq.edu.au/` is accessible.

8. If off-campus access is desired, check that `http://mirror.aarnet.edu.au/` is accessible.
9. If an internal network only is being used, leave all proxy fields blank for direct connection to the HTTP server.

Install a Web server:

1. Use `rpm -i` to install the Apache<sup>3</sup> web server. This is a “httpd”, or HTTP (HyperText Transfer Protocol) daemon.
2. The configuration files reside in `/etc/httpd/conf`.
3. In the configuration directory, edit `httpd.conf` and set `DocumentRoot` to be `/home/httpd/html`.
4. In the configuration directory, edit `httpd.conf` and set `ServerAdmin` to be the email address of the server administrator (normally `root@machine.domain`, but this may be omitted for now).
5. In the configuration directory, edit `httpd.conf` and set `ServerName` to be the name of the machine as in `/etc/hosts`. Normally this would be the fully-qualified name, but may be a local hostname for now.
6. In the configuration directory, edit `access.conf` and set `<Directory /home/httpd/html>`
7. The HTML files reside under `/home/httpd`. Beneath this path are directories `HTML` for HyperText Markup Language documents (static web documents with `.html` extension) and `cgi-bin` for Common Gateway Interface executables (dynamic web documents, containing binary executables, shell scripts or Perl scripts).
8. In the `html` directory, place the file `test.html` containing a simple HTML form such as the following:

```
<!-- doctype html -->

<html>

 <head>
 </head>

 <body>
 <h1 align=center>
 this is a test
 </h1>

 <h1 align=center>
 this is a test
 </h1>
 </body>

</html>
```

<sup>3</sup>Web server survey <http://www.netcraft.com/survey/>

9. Start the Apache Web Server:  

```
/etc/rc.d/init.d/httpd start
```

Do *not* simply type `httpd` on the command line, as this will run the binary executable `/sbin/httpd`. The above is a script which starts the daemon processes. You can look at it using  

```
more /etc/rc.d/init.d/httpd
```

Note that it's executed on startup as well (due to it's location in the "rc" path). Check it's running using `ps ax`
10. The web server may be started, stopped and restarted using:  

```
/etc/rc.d/init.d/httpd start
/etc/rc.d/init.d/httpd stop
/etc/rc.d/init.d/httpd restart
```

Note that if changes are made to the configuration files (`.conf` files) then you must restart the server as shown above.
11. Install `tcpdump` if not already installed. Then run `tcpdump` to monitor network traffic.
12. Assuming the web server is operating on workstation 139.86.64.222, start the web browser and enter the URL  

```
http://139.86.64.222/
```

This should retrieve the file `index.html` by default.
13. Fetch the URL  

```
http://139.86.64.222/test.html
```

and check that it's visible.
14. Copy the file `cgibasic.pl` from the supplied `\linux\httpd` directory on the second (non-linux) CD into the `cgi-bin` directory. Note that if the file is stored in a DOS/Windows partition, you will need to change the end-of-line delimiters from the existing CR-LF (carriage return followed by linefeed) to the Unix convention of a single linefeed. This may be done using the `dos2unix` utility if present, otherwise use `translate` as follows:  

```
cp cgibasic.pl cgibasic.pl.old
tr -d '\r' < cgibasic.pl.old > cgibasic.pl
```
15. Check that the perl interpreter runs the file ok:  

```
perl cgibasic.pl
```
16. Change its mode to executable:  

```
chmod +x cgibasic.pl
```

Check that it is then executable:  

```
./cgibasic.pl
```

Note that you may need to modify the `ScriptAlias` directive in `httpd.conf`. A line of the form `Options +ExecCGI` permits execution of CGI programs. The file `.htaccess`<sup>4</sup> is used for granting permissions on a per-directory basis.
17. Install the file `perlform.html` from the supplied `\linux\httpd` into the `html` directory.
18. Fetch the URL `http://139.86.64.222/perlform.html` and test the form submission.
19. Repeat the above from another workstation running only a Web browser.

---

<sup>4</sup>Note that Windows may rename this file with `.txt` extension — if so, change it in the file manager.

20. `telnet` to port 80 on the web server machine. Run `netstat` in another window to see the IP connection status — note IP addresses, well-known ports, and dynamic ports in use.
21. The log files are located in directory `/var/log/httpd`. Check the files `access_log` and `error_log`.
22. It is also possible to create CGI handlers using almost any interpreted script language (such as Perl or Unix shell script) or executable file (generated from C or some other language). The following steps will outline how this is done.
23. Copy `perlform.html` to `cgitest.html` and change the `ACTION=` line to point to `cgishow` in the CGI directory.
24. Run `tcpdump` on the Linux machine to monitor network traffic — you should see the HTTP request and reply. Note that because of caching, accessing a web page may not necessarily force a HTTP request and reply across the network.
25. If a C compiler is available (ask the lab instructor first), look at `cgishow.c` — this program is a simple echo server like the Perl example given previously. Of course, it must be compiled into an executable. If the Gnu C compiler (`gcc`) and associated libraries are installed the command line  

```
gcc cgishow.c -o cgishow
```

will compile the C source into binary executable. (Note: for `gcc` you may need to install `egcs` and associated packages.)
26. If a C compiler is available (ask the lab instructor first), investigate other supplied CGI programs: `cgishow.c`, `cgiget.c`, `cgipost.c`, `cgiembed.c`, `cgimg.c`.

## 4.8 Web Server Scripting using PHP

The “PHP” package provides scripting for the Apache web server. It allows such things as dynamic web pages to be created, user-forms to be processed, and database (SQL or Structured Query Language) queries to be returned via a web interface.

The previous section on the Apache web server must be completed before attempting to install PHP. The following is adapted from the documentation files `/usr/doc/php.ver/INSTALL.REDHAT` (where *ver* is a version/revision number) and the on-line documentation.

1. Install the packages `apache`, `apache-devel` and `freetype-devel` (`apache` should already be installed). Check that basic web pages can be served via Apache.
2. Find the following lines in `httpd.conf` and uncomment them:

```
LoadModule php_module modules/libphp.so
AddModule mod_php.c
```
3. Find the following lines in `httpd.conf` and uncomment them:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

4. Re-start the httpd daemon `/etc/rc.d/init.d/httpd restart`
5. In the web server html directory, create a file called `info.php` containing:  

```
<?php phpinfo(); ?>
```
6. Check that the URL `http://machine/info.php` is visible – it should return a large page of information via the above PHP function call.
7. Create a html page called `phpform.html` containing:

```
<!-- simple form processing with php -->

<html>
 <body>
 <!-- use either GET or POST methods, -->
 <!-- and change the PHP script accordingly -->
 <!--<form action="phpform.php" method="GET">-->
 <form action="phpform.php" method="POST">
 <input type="text" name="textfield">
 <input type="password" name="passwordfield">

 <input type="submit">
 </form>
 </body>
</html>
```

8. Create a file `phpform.php` containing:

```
<?php

 echo "Processing phpform.html

\n";

 // using GET method
 //$textfield=$_GET[textfield];
 //$passwordfield=$_GET[passwordfield];

 // using POST method
 $textfield=$_POST[textfield];
 $passwordfield=$_POST[passwordfield];

 echo "textfield = $textfield
\n";
 echo "passwordfield = $passwordfield
\n";
?>
```

9. Test by loading the URL `http://machine/form.html` into the web browser. Try with both GET and POST methods. What is the difference?

## 4.9 Domain Name Server Installation

The Domain Name Server (DNS) is responsible for translating host names such as `www.usq.edu.au` to IP addresses. A small number of hostname-to-IP mappings may be stored in the `/etc/hosts` file, however this is limited in scope as it requires manual configuration. Instead, name service mapping requests are forwarded on to a *nameserver* machine. Although this could be done on a single host, the service is delegated to one or more machines on each sub-network. If the service was performed on a single host, it would require an extremely large database and be correspondingly slow. Furthermore, it would be potentially unreliable due to network congestion. Unresolved queries are passed on to a higher-level domain nameserver.

Normally each machine is *not* set up as a nameserver, but rather knows the IP address of one nameserver (or two, for continued service in the event of failure) on a local network which provides this service. The vast majority of machines will be set up this way. However, this section will examine the basics of how to set up a nameserver. This is provided by the Berkeley Internet Domain Daemon (BIND) package, which (to confuse matters further) runs a process called `named` (pronounced “name-d”). The following are adapted from the DNS-HOWTO document in the RedHat Linux distribution.

A *caching nameserver* is one which simply stores (caches) name queries from your machine for later use. This speeds up later name queries. It does not answer name service queries from other machines.

1. The file `/etc/hosts` contains local name mappings that do not require DNS queries. It should contain, at a minimum, entries for `localhost` and the local machine's name:

<code>127.0.0.1</code>	<code>localhost localhost.localdomain</code>
<code>139.86.64.222</code>	<code>lab222</code>

2. Install `bind` using `rpm -i` as usual.
3. Study `man named`
4. Copy the file `named.conf.caching` from `\linux\named` into `/etc/named.conf`. This file is shown below (with appropriate sections commented out):

```
// named.conf.caching - named.conf for caching-only nameserver
//
// file /etc/named.conf
// start named using ndc start, ndc stop or ndc restart

// Config file for caching only/slave/master name server

options
{
 directory "/var/named";
};

zone "."
{
 type hint;
 file "root.hints";
};

zone "0.0.127.in-addr.arpa"
{
 type master;
 file "pz/127.0.0";
};

// for operation as a master nameserver
//zone "eng.usq.edu.au"
//{
// notify no;
// type master;
// file "pz/eng.usq.edu.au";
//};

// for operation as a slave name server
//zone "eng.usq.edu.au"
//{
// type slave;
// file "sz/eng.usq.edu.au";
// masters{ 139.86.128.2; };
//};
```

5. Copy the file `root.hints` \linux\named to `/var/named/root.hints`. This is shown below:

```

; save as /var/named/root.hints

 6D IN NS G.ROOT-SERVERS.NET.
 6D IN NS J.ROOT-SERVERS.NET.
 6D IN NS K.ROOT-SERVERS.NET.
 6D IN NS L.ROOT-SERVERS.NET.
 6D IN NS M.ROOT-SERVERS.NET.
 6D IN NS A.ROOT-SERVERS.NET.
 6D IN NS H.ROOT-SERVERS.NET.
 6D IN NS B.ROOT-SERVERS.NET.
 6D IN NS C.ROOT-SERVERS.NET.
 6D IN NS D.ROOT-SERVERS.NET.
 6D IN NS E.ROOT-SERVERS.NET.
 6D IN NS I.ROOT-SERVERS.NET.
 6D IN NS F.ROOT-SERVERS.NET.

G.ROOT-SERVERS.NET. 5w6d16h IN A 192.112.36.4
J.ROOT-SERVERS.NET. 5w6d16h IN A 198.41.0.10
K.ROOT-SERVERS.NET. 5w6d16h IN A 193.0.14.129
L.ROOT-SERVERS.NET. 5w6d16h IN A 198.32.64.12
M.ROOT-SERVERS.NET. 5w6d16h IN A 202.12.27.33
A.ROOT-SERVERS.NET. 5w6d16h IN A 198.41.0.4
H.ROOT-SERVERS.NET. 5w6d16h IN A 128.63.2.53
B.ROOT-SERVERS.NET. 5w6d16h IN A 128.9.0.107
C.ROOT-SERVERS.NET. 5w6d16h IN A 192.33.4.12
D.ROOT-SERVERS.NET. 5w6d16h IN A 128.8.10.90
E.ROOT-SERVERS.NET. 5w6d16h IN A 192.203.230.10
I.ROOT-SERVERS.NET. 5w6d16h IN A 192.36.148.17
F.ROOT-SERVERS.NET. 5w6d16h IN A 192.5.5.241

```

6. Make a directory called `pz` under `/var/named`. Copy the file `127.0.0` to this subdirectory. This file is shown below:

```

; install as /var/named/pz/127.0.0

@ IN SOA lab222.eng.usq.edu.au. root.lab222.eng.usq.edu.au. (
 1 ; Serial
 8H ; Refresh
 2H ; Retry
 1W ; Expire
 1D) ; Minimum TTL
NS lab222.eng.usq.edu.au.
1 PTR localhost.

```

7. Modify the domain name in this file as appropriate (three locations).
8. Study `man resolver`.
9. The file `/etc/resolv.conf` contains the addresses of the DNS (Domain Name Service) nameservers. Change the `nameserver` line to the localhost address `127.0.0.1` – it should appear thus:

```
search eng.usq.edu.au usq.edu.au
nameserver 127.0.0.1
```

10. The file `/etc/nsswitch.conf` determines the search order for names (local file lookup or DNS server query). It should contain a line of the form:

```
hosts: files dns
```

11. The file `/etc/host.conf` should contain a line of the form:

```
order hosts, bind
```

12. Start the name service via the startup script:

```
ndc start
```

It may be stopped later using

```
ndc stop
```

and checked using

```
ndc status
```

13. Check the log file:

```
tail -f -n10 /var/log/messages.
```

14. Run `nslookup`. It should say “server is localhost” if the name server is running correctly on the local machine.

15. Try a query: type

```
phanes.eng.usq.edu.au
```

The IP address should be returned.

16. Try another query: type

```
www.usq.edu.au
```

17. Now try both of the above again. The note “non-authoritative answer” should be given, because the names have been cached by the local caching nameserver.

18. Type `exit` to exit `nslookup`.

19. Type `ndc stop` to stop the name daemon.

A *master* or *primary nameserver* is one which provides the main nameservice for a particular domain. It is in effect fully independent – unlike a caching nameserver – and sends updates to other slave nameservers.

1. The file `/etc/hosts` contains local name mappings that do not require DNS queries. It should contain, at a minimum, entries for `localhost` and the local machine’s name:

```
127.0.0.1 localhost localhost.localdomain
139.86.64.222 lab222
```

2. Install `bind` using `rpm -i` as usual.

3. Study `man named`.

4. Copy the file `named.conf.master` into `/etc/named.conf`. This file was shown previously, with the lines for master nameserver operation commented out.
5. Copy the file `root.hints` to `/var/named/root.hints`. This file was shown previously.
6. Make a directory called `pz` under `/var/named`. Copy the file `eng.usq.edu.au` to this subdirectory. This file is shown below:

```
; install as /var/named/pz/eng.usq.edu.au for primary nameserver
; install as /var/named/sz/eng.usq.edu.au for secondary nameserver

@ IN SOA lab222.eng.usq.edu.au. root.lab222.eng.usq.edu.au. (
 1 ; Serial
 8H ; Refresh
 2H ; Retry
 1W ; Expire
 1D) ; Minimum TTL
 NS lab222.eng.usq.edu.au.
localhost A 127.0.0.1

lab222 A 139.86.64.222
lab223 A 139.86.64.223

; try some aliases
newone A 139.86.64.222
otherone A 139.86.64.223
leis A 139.86.64.226
```

7. Modify the domain names in this file as appropriate.
8. Study `man resolver`.
9. The file `/etc/resolv.conf` contains the addresses of the DNS (Domain Name Service) nameservers. Change the `nameserver` line to the IP address of this workstation. It should appear thus:

```
search eng.usq.edu.au usq.edu.au
nameserver 139.86.64.222
```

10. The file `/etc/nsswitch.conf` determines the search order for names (local file or DNS server). It should contain a line of the form:

```
hosts: files dns
```

11. The file `/etc/host.conf` should contain a line of the form:

```
order hosts, bind
```

12. Start the name service via the startup script:

```
ndc start
```

It may be stopped later using

```
ndc stop
```

and checked using

```
ndc status
```

13. Check the log file:  
`tail -f -n10 /var/log/messages`
14. Run `nslookup`. Check that the server is this workstation.
15. Set the query type:  
`set q=any`
16. Try a query: type  
`lab222`  
The IP address should be returned.
17. Try another query on the a directly connected machine:  
`lab222`
18. Try another query using a fully-qualified name  
`lab222.eng.usq.edu.au`.
19. Try another query on the an in directly connected machine:  
`www.usq.edu.au`
20. Type `exit` to exit `nslookup`
21. Now a Windows machine will be set to use this machine as a nameserver.
22. On the Windows machine, click `Start-Settings-ControlPanel-Network`. Then click on `TCP/IP`, then `Properties`.
23. Delete and DNS entries, and add the IP address of the DNS server machine.
24. Click OK, and start a DOS box.
25. In the DOS box, try a ping connection using only the hostname:  
`ping lab222`
26. Try a ping connection using a fully-qualified domain name:  
`ping lab222.eng.usq.edu.au`
27. Try a ping connection using a domain name which is not registered on the local nameserver:  
`ping mirror.aarnet.edu.au`
28. Type `ndc stop` to stop the name daemon.

A *slave* or *secondary nameserver* is one which provides a secondary nameservice for a particular domain. The secondary nameserver contacts the primary nameserver for it's domain and transfers the name data (called a "zone transfer"). These lookups are referred to as "non-authoritative". To set up a secondary nameserver, complete the primary nameserver setup as above, halt the nameserver daemon, and do the following:

1. Uncomment the lines in the supplied `/etc/named.conf` pertaining to "slave" nameservice.
2. Comment out the lines in the supplied `/etc/named.conf` pertaining to "master" nameservice.

3. Make a directory called `sz` under `/var/named`. Copy the file `eng.usq.edu.au` to this subdirectory. This file was shown previously.
4. Start the name daemon and run `nslookup` as for the master nameserver section. The query answers should be “non-authoritative”.

## 4.10 Disk Restoration

**When this laboratory exercise is completed, please restore the root and boot sectors using the saved floppy image.** To do this:

1. Boot from the DOS boot floppy.
2. Run `restorrb` to restore the root and boot sectors from file `rootboot.000`.
3. Reboot the computer in DOS mode in order to force a re-read of the partition table.
4. Type `dir c:` to check the unused space.
5. Reboot into Windows.
6. Double-click on `MyComputer`. Right-click on the `c:` drive icon, and select `Properties`.
7. Check that the total disk space equals that found originally on the PC.
8. Run `scandisk` and then `defrag` to check the disk.

## 4.11 Further Work

A number of configuration aspects have been dealt with here. Some which have not include:

1. Security in general – user accounts, logon procedures and password files and network access points such as web servers. Look up `securetty` and `nologin`, the last command.
2. Security and internet firewalls – see for example the `ipfwadm` (`iptables` in later releases) package and manual entries on `hosts.allow` and `hosts.deny`.
3. Routing using the `gated` daemon.
4. Setting up a proxy server using `Squid`.
5. Systems programming under Linux using C.
6. Kernel compilation/rebuild under Linux.
7. Shell and administrative programming under Linux.
8. Graphical interface programming using `Tcl/Tk`.

9. Network monitoring using the `ntop` package.
10. Parallel processing – the `pvm` package.
11. A database using the `mSQL` package.
12. A web-viewable database using `Apache`, `PHP` and `mSQL`.
13. Investigate web security using `nmap`.

## Exercise 5

# FreeBSD

**Aims** The aims of this laboratory task are:

1. To become familiar with low-level partitioning of disks and how they are used by operating systems.
2. To install FreeBSD – an implementation of the Unix operating system.

**Hardware** The hardware supplied may vary, but requires the following:

1. PC's with CD drive and network interface card(s).
2. Ethernet hubs (or switches).
3. 10BASET cabling.
4. Three floppies (DOS bootable disk, two BSD installation disks).

**Software** The following software will be supplied:

1. FreeBSD CD. One CD contains all the necessary software for setup.
2. Other resources as per Linux exercises (LAN card setup programs).
3. Documentation files on FreeBSD CD.

### 5.1 Notes on this Laboratory Exercise

This exercise is provided as an additional extra for those students who may already be familiar with Linux, and wish to try an alternative Unix system – FreeBSD. In many ways, FreeBSD is a more “pure” Unix distribution than the various Linux distributions. The FreeBSD source code can be traced directly to the Berkeley Unix code, whereas Linux was developed independently.

The most fundamental difference between Linux and FreeBSD is that Linux is, strictly speaking, only a kernel, whereas FreeBSD is a complete distribution. Linux comes bundled with various applications, utilities, window managers and the like, written by various open-source contributors. The kernel itself remains tightly controlled, however all other areas of the system are generally

less controlled. This is at once both the strength and weakness of Linux: the wealth of contributions versus the difficulty in maintaining skills over minor and major variations, not to mention the possible stability problems. FreeBSD, on the other hand, comes as a complete distribution. In addition to the kernel, all the necessary components – utilities, tools, and so forth – are bundled together into one distribution. This is often cited as a key advantage: ease of use, and stability. Furthermore, some Linux distributions have a “flavour” more like System V Unix; others have more similarities with the Berkeley BSD Unix; most are a combination of the two. The minor variations in matters like configuration files, for example, makes Linux somewhat tedious to work with in some peoples’ view.

This exercise assumes a reasonable degree of familiarity with disk partitioning, installation and configuration of Linux. As such, the instructions are a brief guide only. It is intended to be completed by students who have some familiarity with these aspects.

Some useful sites are

<http://www.freebsd.org/>

<http://mirror.aarnet.edu.au/pub/FreeBSD/>

## 5.2 Setup Notes

The following are some notes on the setup process. They are not intended to form detailed instructions – the installation program is mostly self-explanatory; the installation guides (CD or web) have more detailed information.

### Hardware

1. The Dell Precision 210 PC’s are recommended for this task. Please consult the lab supervisor. These machines have:

Disk	6G
RAM	256M
NIC	3COM 3c90x
Display	NVIDIA RIVA TNT2/Pro Model 64, 32M RAM
Screen Mode	75Hz 1024x768, 64k colors

2. Collect as much information as possible from the BIOS and existing Windows configuration, and by inspecting the hardware.

### Disks

1. FreeBSD may be installed from CD, or from CD with floppy boot. The CD is readable from Windows, and installation floppies may be created from the `fdimage` utility under the `tools` directory. The image files `kern.flp` and `mfsroot.flp` reside under directory `floppies`.
2. Further installation instructions are contained on the CD in the `install.htm` file.

3. The nomenclature and handling of disks is different under FreeBSD compared to Linux. Linux uses disk “devices” such as `/dev/hda` for the primary (C) hard drive, and `/dev/hda1` to `/dev/hda4` for partitions. A typical configuration is

Mount point/name	Linux designation	Purpose
<code>/boot</code>	<code>/dev/hda1</code>	boot loader
<code>swap</code>	<code>/dev/hda2</code>	virtual memory swap
<code>/</code>	<code>/dev/hda3</code>	root filesystem

The partitions are tied to the BIOS partitioning scheme. FreeBSD uses *slices* in place of partitions, and partitions within each slice. Devices with “ad” are regular IDE disks, “fd” are floppy disks, and “acd” are CDs. The slices are shown as “s” followed by a number, and partitions are designated with a letter – so, for example, `ad0s1a` designates IDE disk 0, slice 1, partition a. A typical configuration is

Mount point/name	BSD designation	Purpose
<code>/</code>	<code>/dev/ad0s1a</code>	boot loader
<code>swap</code>	<code>/dev/ad0s1b</code>	virtual memory swap
<code>entire slice</code>	<code>/dev/ad0s1c</code>	designation not normally used
<code>/var</code>	<code>/dev/ad0s1d</code>	variable-sized filesystem
<code>/tmp</code>	<code>/dev/ad0s1e</code>	temporary space filesystem
<code>/usr</code>	<code>/dev/ad0s1f</code>	fixed space filesystem

4. Mounting filesystems is similar to Linux, with slightly different designators for file type and of course device special files. For example, to mount a CD use

```
mount -t cd9660 /dev/acd0 /cdrom
```

Look at `/etc/fstab` for other filesystems.

## Network

1. The network adapter is `x10` (ell-zero) for card `3c90x`

## X Window system

1. It is recommended that you install the KDE window manager.
2. The file `/etc/XF86Config` contains configuration information. Use `xf86config` after installation to change the configurations. The following parameters work satisfactorily:

<code>refresh</code>	70Hz
<code>resolution</code>	1024x768
<code>colors</code>	64k colors
<code>card</code>	364
<code>monitor</code>	7
<code>mouse type</code>	3 (bus mouse)
<code>keyboard</code>	5
<code>sync</code>	2
<code>video memory</code>	32M
<code>default color depth</code>	16 bits

**Other notes**

1. Additional software (“packages”) may be found in the `/packages` directory on CD. Packages are added using the `pkg_add` command.
2. The following control keys are useful:

<code>ctrl-alt- F1-F7</code>	select virtual console
<code>PrintScreen</code>	toggle virtual console
<code>ctrl-alt-backspace</code>	shutdown X server
<code>ctrl-alt-keypad</code>	change X server mode

**5.3 Disk Restoration**

At the end of the exercise, restore the disk as per the Linux exercise.