

CO1507 Introduction to Networking

Lab 17: Linux

FYI The dollar sign '\$' seen throughout this worksheet is NOT part of any command you must type, instead the dollar represents the prompt itself at which YOU begin typing.

You may skip past early sections very quickly if you feel confident you have already covered the command / etc. as part of co1508. Later parts of the worksheet should be new to you.

In this lab we will assume that you already have experience installing a Linux based operating system in your other module co1508. Here we will use a ready-made VMWare image and focus on learning about the Linux operating system, terminal commands, and various networking related utilities.

Download the image from blackboard. Open the Virtual machine within VMWare.

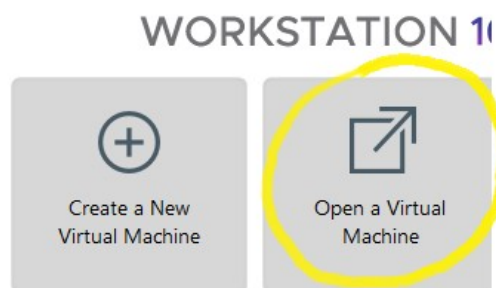


Figure 1VMWare

Click on the 'Open a Virtual Machine' and navigate to the image files you downloaded.

Using Linux

If VMWare asks you if you copied it, **yes** you did, if it asks you to 'take ownership' **do so**.

To login the password for the user named 'student' is '**network**'.

Linux could almost be regarded as a clone of the commercial UNIX operating system used in 1970s mainframes. UNIX like operating systems and have been in use for over 40 years. Linux is very common software on many types of servers. Although Linux is a fully graphical operating system like Windows, a lot of the real power still resides with the command line tools so it is useful to familiarise ourselves with it.

Meet the Shell

The command-line in Linux is the shell. The shell is a program that takes keyboard commands and passes them to the operating system to carry out.

The shell program in Linux is referred to as bash (Bourne Again Shell, an enhanced replacement for "sh" the original UNIX shell program written by Steve Bourne).

When using a graphical user interface, we need another program called terminal emulator to interact with the shell, e.g. 'QTerminal' etc.

Launch the 'QTerminal' terminal emulation program located in the menu found by clicking the button in the bottom left corner of the screen. This is the same program you used to install VMWare tools earlier.

Navigating the file system

Next, we learn to navigate the file system on our Linux system. We have already introduced the following command:

`ls`

As we have previously discussed, this command lists the directory contents. Additional commands you should know to navigate are the following:

`pwd` # which prints the name of the current working directory.

`cd` # which changes the directory.

Before we get to practice with these commands, we must understand the file system tree. Like Windows, a Linux-based system organizes the files in a hierarchical directory structure.

The first directory in the file system is called the root directory (/) The root directory contains files and subdirectories, which contain more files and subdirectories and so on. The root directory must not be confused with a directory called 'root'.

It is important to note that there are no 'drive letters' such as 'C:' 'N:' etc. in Linux. Everything within the file system is located within the same hierarchy beginning at /, which is usually also the directory of the primary hard disc partition.

Other partitions, and devices like pen drives can be mounted elsewhere within the file system e.g., /media/mypendrive. Do not worry about how to do this for now, when plugging in a pen drive in Ubuntu Linux this mounting task is done automatically for the user.

- Execute the appropriate command to display your current working directory. What is it?
- List all the files and directories in the current working directory. What command did you use?

Changing the current working directory requires the use of the `cd` command. This must be followed by a pathname, the pathname of the desired working directory. A pathname is the route we take along the branches of the tree to get to the directory we want. Pathnames can be specified in one of two ways:

1. As absolute pathnames, e.g. /usr/bin, root is represented by the leading slash
2. As relative pathnames, e.g. start with a dot (.), or a double dot (..)

Type the following at the command line and record the working directory in your notes (use `pwd`) after each command.

- `$ cd /usr/bin`
- `$ cd .`
- `$ cd ..`
- `$ cd -`
- `$ cd ~username` # Where username is the username of a valid user on the system e.g. your own

The `ls` command is probably the most used command in Linux. With it, we can see directory contents and determine a variety of important file and directory attributes.

Besides the current working directory, we can specify the directory to list even multiple directories, like so; NB: It is very important that you notice the spaces in the following commands.

- `$ ls /usr`
- `$ ~ /usr`

We can also change the format of the output to reveal more detail:

- `$ ls -l`
- `$ ls -al`

Long format (`-l`) contains a great deal more information than the standard output. All (`-a`) shows hidden files and folders. You can specify long and all together by typing `ls -al`

Example long format output:

```
-rw-r--r-- 1 jonathan jonathan 32059 2012-04-03 11:05 kitten.jpg
```

In the left-hand column is a 10-character string consisting of the symbols `d`, `r`, `w`, `x`, `-`, and, occasionally, `s` or `S`. If `d` is present, this means the entry is a directory, otherwise `-` will be the starting symbol of the string and represents a file.

The nine remaining symbols indicate the permissions, or access rights, and are taken as three groups of 3.

- The left group of 3 shows the file permissions for the owner of the file (or directory)
- The middle group shows the permissions for the group of people added by the owner.
- The rightmost group shows the permissions for all others.

The symbols `r`, `w`, `x`, signify read, write, and execute permissions, respectively. Create a new file in your home directory. To do this issue the command

```
$ sudo touch newfile.txt
```

The ``touch`` command creates a file if no file is with that name is present and updates the time stamp on the file if one IS present.

Note down the permissions string for the new file.

Create a new directory in your home directory. To do this issue the command

```
$ mkdir myFolder
```

Move the file newfile.txt to myFolder using the command.

```
$ mv newfile.txt myFolder
```

Change your working directory to myFolder, to do this issue the command.

```
$ cd myFolder
```

What is the full file path of this directory? Issue the command:

```
$ ls -al
```

Who is the owner of the newfile.txt? Create ANOTHER new file called newfile2.txt, this time use the command:

```
$ touch newfile2.txt
```

Issue the command `ls -al` again, who is the owner of newfile2.txt? Why is the owner different this time? Issue the command.

```
$ echo hello > newfile2.txt
```

Issue the command:

```
$ cat newfile2.txt
```

to check this has worked.

Installing Apache web server

In Linux we can install software from the command line from online repositories. The listing of which repositories are available are held in the file /etc/apt/sources.list

First, we need to update our list of packages available to install. Issue the command:

```
$ sudo apt update
```

(You will be asked for your password as 'sudo' is asking to elevate your access level!). Apache is the world's most used web server software. We can install Apache with the commands.

```
$ sudo apt install apache2
```

This will take a minute or so.

If this fails...

If installation fails, please open Firefox (within Ubuntu) and check to see if you have internet access inside the VM. If not, then you need to power down the virtual machine and go to Windows start menu and look for "Virtual network editor" and open it. In virtual network editor CLICK change settings, and then restore defaults. This will take a few second but once done, boot up your VM again and all should be resolved.

Once installations are successfully completed, open Firefox and type `http://127.0.0.1` in the address bar. You should get the Apache test page.

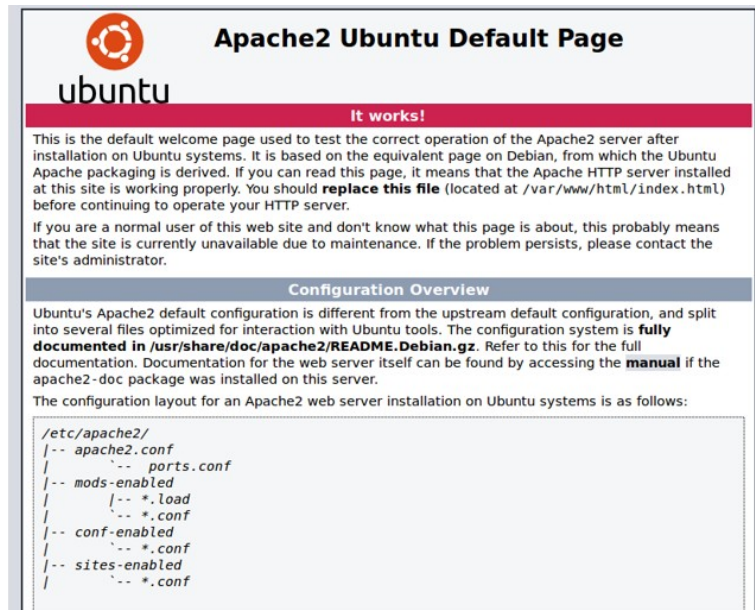


Figure 2 Apache Test Page

You can serve your own web pages by placing .html or .php files in the folder located at `/var/www/html`

Use the command:

```
$ sudo chmod 777 /var/www/html -R
```

This will grant all permissions to the folder (do not worry about this now – the topic of permissions will be covered in the lectures)

Navigate to the directory `/var/www/html` then type:

```
$ touch test.html followed by featherpad test.html &
```

This will open a text editor called Featherpad (like Windows notepad - actually better) into which you can write some HTML. Obviously if you were going to do any proper development, you'd want a code editor like Visual Studio Code, but that's not needed for today - we're only testing.

Once done, point your browser to `http://127.0.0.1/test.htm` and you should see your webpage.

Networking with your fellow classmates

Assuming we have booted Linux in **NAT** mode you will have access to the internet within the virtual machine, however you will not be able to communicate with other hosts on the network including your own PC within Windows as the host of the virtual machine.

To do this we switch to **bridged mode** then when you boot into Linux now you should get assigned an IP address by the DHCP server (meaning the DEV network DHCP server)

Shut down the Virtual Machine and change to 'Bridged' mode in the settings.

You then need to click edit and pick Virtual network Editor.

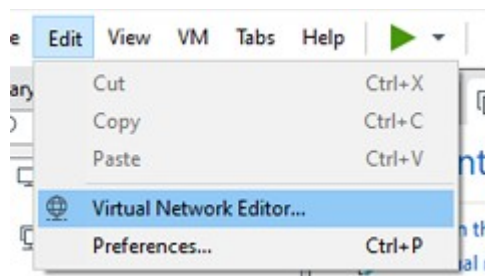


Figure 3 Virtual Network Editor

Edit 'VMnet0' and make sure instead of being bridged to 'Automatic' you choose your relevant adaptor. **IMPORTANT:** If you do not know what this is then you need to go and look at network and sharing settings under the control panel and figure out which device is currently connecting you to your local area network / Wi-Fi.

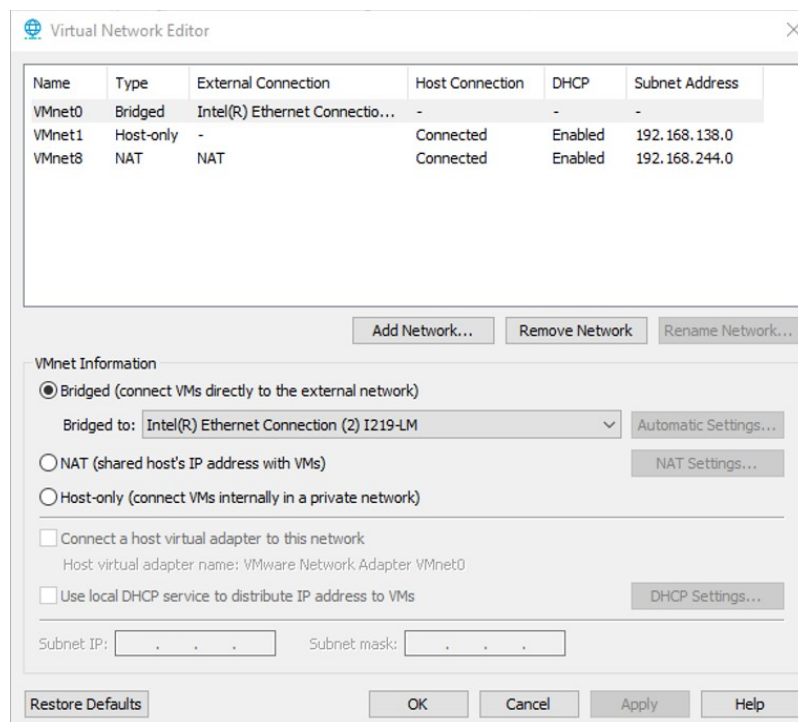


Figure 4 Virtual Network Editor

Use the command 'ip addr' or 'ip address' in full at the bash prompt to discover the network interface card configurations in Linux.

```
fred@fred-virtual-machine:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:9e:34:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.112/24 brd 192.168.1.255 scope global dynamic ens33
        valid_lft 86371sec preferred_lft 86371sec
    inet6 fe80::3561:b4e6:7b63:262d/64 scope link
        valid_lft forever preferred_lft forever
fred@fred-virtual-machine:~$
```

Figure 5 Terminal

In CM120 and CM142 the output may be different from my example and your interface card should pick up a 10.x.x.x IP address from the `DEV` DHCP server.

```
fred@fred-virtual-machine:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:9e:34:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.112/24 brd 192.168.1.255 scope global dynamic ens33
        valid_lft 86371sec preferred_lft 86371sec
    inet6 fe80::3561:b4e6:7b63:262d/64 scope link
        valid_lft forever preferred_lft forever
fred@fred-virtual-machine:~$ ping 192.168.1.68
PING 192.168.1.68 (192.168.1.68) 56(84) bytes of data.
64 bytes from 192.168.1.68: icmp_seq=1 ttl=128 time=0.358 ms
64 bytes from 192.168.1.68: icmp_seq=2 ttl=128 time=0.212 ms
64 bytes from 192.168.1.68: icmp_seq=3 ttl=128 time=0.167 ms
64 bytes from 192.168.1.68: icmp_seq=4 ttl=128 time=0.213 ms
fred@fred-virtual-machine:~$
```

Figure 6 Terminal

Once you know your IP address and have a web page to serve in the folder /var/www/html then you should be able to serve your page to another host. If we were on campus you could serve to another student in the classroom who is also using 'bridged' mode to join the room LAN.

First of all, we can serve to the host machine. i.e., go back to Windows host machine, open a web browser, and enter 'http://' followed by the IP address you found within Linux. The webpage should be served from the Virtual machine to the Host Computer.

Next, give that IP address to a classmate in the room and ask them to enter the IP address into a browser address bar (either in Windows or their Linux VM (try both) it shouldn't matter) they should see YOUR webpage in their browser.

Networking tools: IFCONFIG

First, ensure that net-tools (ifconfig is part of net-tools) is installed on your system. Most Linux distributions come with it pre-installed, but if not, you can install it using the following commands:

```
$ sudo apt install net-tools
```

To see essential information about all active network interfaces, simply run:

```
$ ifconfig
```

This command displays details like interface names (e.g., `enp0s3`, `lo` for the loopback interface), IP addresses, and other relevant data.

If you want a concise list of active interfaces, use the `-s` option:

```
$ ifconfig -s
```

For more detailed information about all interfaces, use the `-v` option:

```
$ ifconfig -v
```

To view configuration details for all interfaces (including inactive ones), use `-a`:

```
$ ifconfig -a
```

Specify the interface name (e.g., `eth0`, `wlan0`) to focus on a particular interface:

```
$ ifconfig eth0
```

Networking tools: TCPDUMP

First, ensure that `tcpdump` is installed on your system. Most Linux distributions come with it pre-installed, but if not, you can install it using the following commands:

```
$ sudo apt install tcpdump
```

Basic Usage:

Open a terminal.

Run `tcpdump` with appropriate options and filters. For example:

```
$ sudo tcpdump
```

If you don't specify a network interface, `tcpdump` will choose one for you. To capture traffic from a specific interface, use:

```
$ sudo tcpdump -i eth0
```

To display packet data in HEX, use the following command:

```
$ sudo tcpdump -XX
```

Filtering Traffic:

You can filter captured traffic based on various criteria:

By port (e.g. http, https):

```
$ sudo tcpdump port 80
```

```
$ sudo tcpdump port 443
```

***HINT** You may have to do something to generate some traffic to look at (e.g., browse the web in another window)

By protocol (e.g., TCP, UDP, ICMP):

```
$ sudo tcpdump tcp
```

```
$ sudo tcpdump udp
```

```
$ sudo tcpdump icmp
```

***HINT** For the latter try opening two terminal emulator windows at the same time, in one ping another IP address and leave in running, in the second use TCPDUMP to view the packets.

By source or destination IP address:

```
$ sudo tcpdump host 192.168.1.10
```

Combine filters as needed:

```
$ sudo tcpdump port 22 and host 10.0.0.1
```

***HINT** Substitute the IP addresses for an **actual** host on the network or your own IP.

Networking tools: NMAP

First, ensure that nmap is installed on your system. Most Linux distributions come with it pre-installed, but if not, you can install it using the following commands:

```
$ sudo apt install nmap
```

Basic Usage:

Open a terminal. Run nmap with appropriate options and specify the target you want to scan. For example:

To scan a specific hostname:

```
$ nmap -v www.example.com
```

To scan a specific IP address:

```
$ nmap 8.8.8.8
```

***HINT:** Try scanning the default gateway address (find this by using the ipconfig command)

Common Scanning Techniques:

TCP SYN Scan (Stealthy and efficient):

```
$ nmap -sS www.example.com
```

Scan Multiple Hosts:

```
$ nmap 192.168.1.10 192.168.1.20
```

Scan a Whole Subnet:

```
$ nmap 192.168.1.*
```

Detect Firewall Settings:

```
$ sudo nmap -sA 192.168.1.10
```

Identify Hostnames:

```
$ sudo nmap -sL 192.168.1.10
```

Questions

1. Linux is a _____-like operating system.
2. Where is the home folder on a Linux system located for a user named 'Fred'?
3. How do we list files within the working directory in the Linux terminal?
4. What options are available relating to question 3 to alter the output?
5. What is the Linux equivalent of ipconfig on the Windows command line?
6. Explain the octal triad 740 when relating to permissions?
7. What is the octal triad equivalent of -rwxr-xr--
8. What command is used to CHANGE permissions on a file or folder?
9. What command is used to temporarily elevate users' privilege on the system?
10. List some common Linux command line networking utilities.