Introduction to the Internet Lab

What you will learn in this lab:

• Overview of the equipment
• Saving your data
• Navigating your way around Linux
• Working with protocol analyzers: tcpdump, ethereal

Version New 24, March 12, 2003
Table of Contents

Prelab 1 ........................................................................................................................................... 3

Question Sheet for Prelab 1 ........................................................................................................... 4

Lab 1 ............................................................................................................................................... 5

Setup for Lab 1 ........................................................................................................................................................................... 6

Part 1. Becoming Familiar with the Equipment ................................................................................. 7

Part 2. Using the Linux Operating System .......................................................................................... 10

Part 3. Saving Your Data .................................................................................................................... 11

Part 4. Copying Files to a Floppy Diskette .......................................................................................... 12

Part 5. Locating Configuration Files in Linux ................................................................................. 16

Part 6. Using Ping ................................................................................................................................. 18

Part 7. Basics of tcpdump ................................................................................................................... 19

Part 8. Basics of Ethereal .................................................................................................................... 21

Checklist Form for Lab 1 ................................................................................................................ 25

Feedback Form for Lab 1 ............................................................................................................... 26
Prelab 1

1. **Man Pages:** The PCs run the Linux operating system, a Unix-like operating system. This assignment asks you to review some Unix commands. Man pages exist on every lab machine. You can also find the manual pages (“man pages”) online at

   http://www.tcpip-lab.net(links)/manual.html

   On this web page, select the operating system “Red Hat Linux/i386 7.3”. For each of the following commands, type the name of the command as a search term. The search will return the appropriate man page.

   Read the man pages of the following commands:

   - man, pwd, ls, more, mv, cp, rm, mkdir, rmdir, chmod, kill, ping, tcpdump

2. **Ethereal:** The man page for *ethereal*, a network analyzer tool, can be found on every lab machine. You can also read about the *ethereal* network analyzer at the website

   http://www.tcpip-lab.net(links)/ethereal.html

   Read the introduction and the manual pages of *ethereal*. 
Question Sheet for Prelab 1

Answer the questions in the space provided below. Use extra sheets of paper if needed and attach them to this document. Submit the answers to the prelab with your lab report.

1. What will happen if you type “man man” in Linux?

2. How can you use the command “ls” to find out about the size of file /etc/lilo.conf?

3. What happens if you have two files with names file1 and file2 and you type “mv file1 file2”? Which option of “mv” issues a warning in this situation?

4. What is the command that you issue if you are in directory “/” and want to copy the file /mydata to directory /labdata?

5. What is the command that you issue if you are in directory “/” and want to copy all files and directories under directory /mydirectory to directory /newdirectory?

6. What happens if you type the command “rm *” in a directory?

7. What is the command that you issue if you want to delete all files and directories under the directory /mydirectory?
Lab 1

In Lab 1, you will acquaint yourself with the equipment of the Internet Lab, the Linux operating system, and some traffic measurement tools.

![Network configuration for Lab 1.](image)

Figure 1.1. Network configuration for Lab 1.

**Note:**
- Before you get started, please reboot the Linux PCs by typing the `reboot` command at the root prompt.
- Do not switch the KVM switch while a Linux PC is rebooting, otherwise the keyboard and mouse will not work properly.
- Save your files to a floppy disk before the end of the lab. You will need the files when you prepare your lab report.
Setup for Lab 1

- All four Linux PCs are connected to a single Ethernet segment via a single hub as shown in Figure 1.1.
- IP addresses for the Linux PCs are configured as follows:

<table>
<thead>
<tr>
<th>Linux PC</th>
<th>IP Addresses of Ethernet Interface eth0</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>10.0.1.11/24</td>
</tr>
<tr>
<td>PC2</td>
<td>10.0.1.12/24</td>
</tr>
<tr>
<td>PC3</td>
<td>10.0.1.13/24</td>
</tr>
<tr>
<td>PC4</td>
<td>10.0.1.14/24</td>
</tr>
</tbody>
</table>

Table 1.1 IP addresses for Lab 1

- The notation 10.0.1.11/24 means that the IP address is 10.0.1.11 and the network prefix is 24 bits long. A network prefix of 24 bits corresponds to a netmask set to 255.255.255.0. With this netmask, all hosts are on the 10.0.1.0/24 network.
Part 1. Becoming Familiar with the Equipment

The equipment that you are working with in the lab has a setup similar to Figure 1.2 shown below and described in detail in Section 1 of the Introduction.

Figure 1.2. Internet Lab Equipment Rack

Equipment Rack Components:

1. a 19" equipment rack
2. 4 Cisco Routers
3. 4 Ethernet Hubs
4. 4 hosts
5. 1 Monitor, 1 keyboard, 1 mouse, 1 KVM switch
6. Cables and connectors
Please take a few minutes to compare the following description with the actual equipment:

1. A 19" rack that houses most of the equipment.

2. Four Linux PCs, which are labeled as PC1, PC2, PC3, and PC4. The PCs have the Linux Red Hat 7.3 operating system installed. All four Linux PCs have floppy drives and CDROM drives. All Linux PCs have two Ethernet network interface cards (NICs) installed, which are labeled `eth0` and `eth1` on the back of the computer.

3. Four Cisco routers, which are labeled as Router1, Router2, Router3, and Router4.

4. The Cisco routers either have a slotted chassis where network interface cards are inserted into the slots of the chassis, e.g., Cisco 2600 series routers, or the routers have a fixed set of network interfaces, e.g., Cisco 2500 series routers. Regardless of the type of chassis, each Cisco router in the Internet Lab has at least 2 Ethernet interfaces and at least one serial interface.

5. Four Ethernet hubs which each have at least 4 ports. The data rates of the ports are 10 Mbps or dual speed at 10/100 Mbps.

6. A monitor, a keyboard, a mouse, and a KVM (Keyboard-Video-Mouse) switch. The KVM switch connects the keyboard, monitor, and mouse to the four Linux PCs. The KVM switch gives you control over all four Linux PCs from one keyboard, one monitor and one mouse, but you can only access one computer at a time\(^1\).

7. Ethernet cables. Note that there are two kinds of Ethernet cables: straight-through Ethernet cables and crossover Ethernet cables. The crossover cables should be color-coded or labeled. Otherwise, use the description in Section 1 of the Introduction to identify if an Ethernet cable is straight-through or crossover. In Lab 1, only straight-through Ethernet cables are used.

**Exercise 1-a. Using the KVM switch, logging in to a Linux PC and exploring the desktop**

The steps of logging into a Linux system are explained in Section 2.1.1 of the Introduction. Use the instructions to log in as the root user.

1. Set the KVM switch to PC1 (the 1\(^{st}\) light or the number “1” should light up). Log in as root.
2. Use the KVM switch to switch to PC3 (the 3\(^{rd}\) light or the number “3” should light up) and log in as root.
3. Explore the desktop environment of PC3.
4. Use the instructions in Section 2.1.2 of the Introduction and create a terminal window. Recall that all Linux commands are typed from a terminal window.

\(^1\) Please note that when rebooting a Linux PC, do not switch the KVM switch to another Linux PC. You have to wait until the Linux PC is fully booted before you can make the switch. A Linux PC needs a monitor, a keyboard and a mouse to reboot. Switching before it is done will cause the process to hang and you will have to start again.
5. Set the KVM switch to PC1 and reboot PC1 by typing `reboot` on the command line at the PC1% prompt in the terminal window:

`PC1% reboot`

**Exercise 1-b. Setup of the Network**

In Lab 1, the four Linux PCs must be connected to an Ethernet hub as shown in Error! Reference source not found.. All Linux PCs are attached to the same Ethernet hub.

1. Attach each Linux PC to the same Ethernet hub with (straight-through) Ethernet cables. Connect the Ethernet interface with label `eth0` of each Linux PC to one of the hubs using an Ethernet cable.

   **Note:** Make sure that you do not use an uplink port of the Ethernet hub. Uplink ports, which are described in Section 1.1.2 of the Introduction, are used to interconnect. If the Linux PC is properly connected, the status light of the connected port displays a green light.

2. When you rebooted the Linux PCs, the IP addresses of the computers are configured as shown in Table 1.1. The IP addresses listed in the table are associated with the Ethernet card of the Linux PC, which is labeled `eth0`. In this lab, the second Ethernet card of the Linux PCs, labeled `eth1`, is not used.

**Exercise 1-c. Testing connectivity between computers**

After connecting the four Linux PCs to the Ethernet hub, all four computers should be able to communicate with each other. The following steps verify that the Linux PCs are properly connected. The test consists of running a remote terminal session between two Linux PCs, using the `Telnet` application.

1. Set the KVM switch to PC1. Start a `Telnet` session from PC1 to PC2, by typing:

   `PC1% telnet 10.0.1.12`

   If you see a login prompt from PC2, PC1 and PC2 are connected to the network. When the login prompt appears, type `Ctrl-d` and type `quit`, to terminate the connection.

2. Set the KVM switch to PC3. Start a `Telnet` session from PC3 to PC4 by typing:

   `PC3% telnet 10.0.1.14`

   If you see a login prompt from PC4, PC3 and PC4 are connected to the network. When the login prompt appears, type `Ctrl-d` and type `quit`, to terminate the connection.
Part 2. Using the Linux Operating System

Here you explore the Linux system by trying out commands that are typed in a terminal window. Some basic Linux commands are reviewed below. See the man pages for a more detailed description.

Exercise 2.

Review the Linux commands discussed in Section 2 of the Introduction. If you are not familiar with Linux or other Unix-like systems, try out some Linux commands by performing the following tasks on PC1.

1. Create a terminal window on PC1.
2. Change to the home directory of the root account.
3. Create a directory test in that directory.
4. Copy the file /etc/hosts to directory test.
5. Change to directory test.
6. Change the name of file hosts to hostfile.
7. List the content of directory test.
8. Edit file hostfile with gedit. Run gedit in the background.
9. Switch gedit to run in the foreground.
10. Change the content of the hostfile in the editor and save the results. Quit the editor.
11. List the content of hostfile.
12. Remove all files in directory test.
13. Remove directory test.

The following is a sequence of commands that performs the above tasks. Note that there are different ways to achieve the same results.

Answers:

1. The steps to create a terminal window are described in Section 2.1.2 of the Introduction.
2. PC1% cd
3. PC1% mkdir test
4. PC1% cp /etc/hosts test
5. PC1% cd test
6. PC1% mv hosts hostfile
7. PC1% ls
8. PC1% gedit hostfile &
9. PC1% fg
10. Change the content in the gedit window, save the content by clicking on Save, and quit by clicking on Exit.
11. PC1% more hostfile
12. PC1% rm -i *
13. PC1% cd ..
    PC1% rmdir test
Part 3. Saving Your Data

Most lab exercises ask you to save data that is displayed on your monitor to a file. The purpose of this exercise is to make you familiar with some methods to save data to a file.

Note: Whenever you create a file, place the file in the directory /labdata. Since other students will most likely purge the files in this directory, please remember to save your files to a floppy diskette at the end of your lab session.

Here are three methods to save data to a file on a Linux system. The methods are described in more detail in Section 2.1.5 of the Introduction.

1. **Save data to a file with the redirection operators:** Linux provides an easy way for redirecting the output of a command to a file via the redirection operators > and >>.

2. **View and save data at the same time:** You can view data on the monitor and save data to a file at the same time. For example, to display the output of command `ls` in a terminal window, and also to file with name `fname`, you can use the command:

   ```
   PC1% ls | tee fname
   or
   PC1% ls > fname & tail -f fname.
   ```

3. **Save data with a text editor (in conjunction with copy and paste):** If you have experience with a Unix-like operating system, you may have your favorite text editor (e.g. `vi`, `emacs`, `pico`, etc.). If you have never edited a file on a Unix-like system, we recommend the `gedit` editor. To edit a file with name `fname` using `gedit`, simply type:

   ```
   PC1% gedit fname
   ```

   If you use the text editor `gedit`, you can copy text by highlighting the text, and pressing `Ctrl-c`. The text is then pasted by pressing `Ctrl-v`. If you are using a different text editor you may use the copy and paste features of the X11 window manager (see Section 2.1.2 of the Introduction) to copy data to a file.

**Exercise 3.**

On PC1, try each of the above methods to save data to a file. Save the output of the command “ls –l /etc” to a file named “/labdata/etcfile_x”, where “x” refers to the method used for saving, “1” for method 1, “2” for method 2, etc.
Part 4. Copying Files to a Floppy Diskette

In all labs, you need the data saved in the lab sessions to complete the lab report. Since the equipment of the Internet Lab is not connected to the Internet, the most convenient way to transfer your saved data is with a 1.44MB floppy disk. This part of the lab acquaints you with the basic commands for accessing a floppy drive on a Linux system.

Using floppy disks in Linux
If you want to save data to an unformatted floppy disk, you first need to format the disk. Before you can use a formatted floppy disk on a Linux system, you must `mount' the floppy disk. The process of mounting is discussed in Section 2.1.3 of the Introduction. Once a floppy disk is mounted, you can use it exactly as a hard drive, that is you can list files (`ls'), copy files (`cp'), rename files (`mv'), etc. When you are done with a floppy disk, you must `unmount' the floppy disk before you remove it from the drive.

1. **Test if a floppy is in use.** If there is a floppy disk in the floppy drive, first make sure that the floppy disk is currently not in use. You can do this by typing:

   ```bash
   PC1% df
   ```
   If you see the line `/dev/fd0 … /mnt/floppy', then `unmount' the floppy drive by typing:

   ```bash
   PC1% umount /mnt/floppy
   ```

2. **Formatting a floppy disk (for new disks).** Use the command `mkfs` ("make filesystem") to format a new floppy disk. Formatting erases any content on the floppy disk, and there is no means to recover the data that was previously on the disk. The syntax for formatting a floppy is:

   ```bash
   PC1% mkfs –t msdos /dev/fd0
   ```
   The option `–t msdos' enforces compatibility with Microsoft Windows systems. The file parameter `/dev/floppy' specifies the floppy disk drive. An alternative command to format a floppy disk is

   ```bash
   PC1% mformat a:
   ```
   This command formats a floppy disk in drive a: with the MS-DOS FAT16 file system, a file format that is compatible with Microsoft Windows systems.

3. **Mounting.** Before you can use a formatted floppy disk, you must `mount' the file system on the floppy disk. The command for mounting a floppy disk is:

   ```bash
   PC1% mount /mnt/floppy
   ```
   The files on the floppy disk are now accessible from the directory `/mnt/floppy'.

4. **Using the file system.** After mounting you can perform any read and write operation on the floppy disk. Everything that you read from or write to directory `/mnt/floppy' will be read from or written to the floppy disk. You can copy files to and from this directory, add or delete subdirectories or files, and make this directory the current directory.
5. **Unmounting.** Before you remove the floppy disk from the floppy drive, you must first "unmount" the file system on the floppy disk. If you skip this step, you will likely lose data and ruin the floppy disk! When you "unmount" a disk, the current working directory should not be /mnt or any of its subdirectories. If necessary, change the current working directory with the `cd` command. The command for unmounting is:

```
PC1% umount /mnt/floppy
```

Note the spelling of the command (It is `umount` and not `unmount`). You can safely eject the floppy disk after you have unmounted the file system.

In the event that the system has trouble unmounting the floppy drive, try using these optional arguments with the `umount` command:

```
PC1% umount -f /mnt/floppy
PC1% umount -l /mnt/floppy
```

The following describes an alternative method to work with floppy disks on a Linux system. This method does not require you to run the mount and umount commands, but it only offers a limited set of commands to read from or write to a floppy disk:

- **mmd dirname**
  Creates a subdirectory with name `dirname`.
  **Example:** PC1% mmd a:/labdata01

- **mdir dirname**
  Lists the contents of a directory on the floppy disk. If no argument is given, the command lists the root directory on the floppy disk.
  **Example:** PC1% mdir a:/labdata01

- **mcd dirname**
  Changes the working directory on the floppy disk. If no name is given, it changes to the top most level (root directory on the floppy disk).
  **Example:** PC1% mcd a:/labdata01

- **mcopy fname newfile**
  **mcopy fname [ fnames ... ] dirname**
  Copy MS-DOS files to and from the floppy drive.
  **Example:** PC1% mcopy /labdata a:

- **mmove fname newfile**
  **mmove fname [ fnames ... ] dirname**
  Move or rename an existing MSDOS file or subdirectory within the floppy disk.
  **Example:** PC1% mmove a:/myfile a:/labdata01

- **mdel fname [fnames ...]**
  Deletes one or multiple file(s).
  **Example:** PC1% mdel a:/labdata01/myfile
**mdeltree dirname**  
Removes a directory and all files and subdirectories from an MS-DOS file system.  
**Example:** PC1% mdeltree a:/labdata01

**mtype fname**  
Displays the contents of file *fname*.  
**Example:** PC1% mtype a:/labdata01/myfile

---

**Exercise 4-a. Saving data to a floppy disk**

1. Use the above commands to save the file `/labdata/etcfile_1`, on PC1 from Exercise 3 to a floppy disk.

2. On PC1, run the command
   
   ```
   PC1% df
   ```

   to obtain a list of all file systems currently mounted on your system. Save the output of the command to a file and save the file to the floppy disk.

**Lab Report**

Attach the files you saved to your lab report.

**Exercise 4-b. Convention for saving data on floppy disks**

Instead of using one floppy disk for each Linux PC, we recommend that you use the FTP program (see Section 2.2.2 of the Introduction) to copy files to a single Linux PC that contains your floppy disk. We recommend the following convention for saving data from the Linux PCs.

**Convention for saving data on floppy disks:**

1. During the lab exercises, save files on each Linux PC in directory `/labdata`.
2. At the end of a lab session, use a floppy in only one Linux PC, e.g., PC1.
3. Use the file transfer protocol FTP for copying saved files from the other Linux PCs to PC1.

The steps below illustrate the convention.

1. On each Linux PC, create a file `/labdata/etcfile_1` as described in Exercise 3.

2. On PC1, create new directories, one for each remote Linux PC: `/labdata/PC2`, `/labdata/PC3`, and `/labdata/PC4`.
3. Use FTP to copy the file `/labdata/etcfile_1` from PC2.

   PC1% cd /labdata/PC2
   PC1% ftp 10.0.1.12

   Log in as root.

   ftp> cd /labdata
   ftp> get etcfile_1
   ftp> quit

4. Repeat Step 3 for PC3 and PC4.

5. Insert a floppy disk into the floppy drive of PC1. If necessary, format the disk, then mount it.

6. Copy all files under directory `/labdata` to the floppy drive.
Part 5. Locating Configuration Files in Linux

Linux has numerous configuration files which set the environment variables of the operating system. For example, if you want to set up your Linux PC as an IP router, you merely need to change a single line in one of the configuration files. Studying configuration files also provides a way of learning what network configuration options are available to you.

In all labs, you will use Red Hat 7.3 or later and Linux kernel version 2.4. Below is a list of the most important network configuration files.

Important: Please do not modify configuration files unless asked to do so. Certain changes to the configuration files may require a re-installation of the operating system.

Note: Configuration files are fundamentally different across different versions of Unix-like operating system (e.g., AIX, Solaris, Linux, FreeBSD). Sometimes the structure of configuration files changes between releases of the same Unix version. For example, the configuration files of different Linux distributions, such as, Red Hat and Slackware, are quite different. Furthermore, the configuration files between different versions of the same Linux distribution can have significant differences.

/proc/sys/net/ipv4/ip_forward
This file defines the global parameters of the network configuration, such as the hostname, domain name, and the IP address of the default gateway. It also includes a line to determine whether the Linux PC acts as a router or not.

/proc/sys/net/ipv4/conf/lo/ipv4_address
/proc/sys/net/ipv4/conf/eth0/ipv4_address
/proc/sys/net/ipv4/conf/eth1/ipv4_address

These files define the configuration of the network interfaces. There is one configuration file for each network interface. The files ifcfg-eth0 and ifcfg-eth1 are for the two installed Ethernet interface cards. The file ifcfg-lo is for the loopback interface.

/etc/sysctl.conf
This file specifies many kernel options related to the network configuration.

/etc/hosts
This file specifies the mapping between the symbolic names and IP addresses for network devices. This file also determines the name of the local Linux system.

/etc/sysconfig/static-routes
This file contains the settings of the static routing table, which is set when booting the Linux PC. It may not exist or may be empty if no static routes have been previously assigned.

**Exercise 5.**

1. On PC1, explore the above files using the `more` command:

   ```bash
   PC1% more /etc/hosts
   ```

   Please do not make any changes to these files.

2. Save the content of the above files.

**Lab Report**

- Which files must be edited to change the name of a Linux PC, e.g., from `PC1` to `machine1`?

- Which files include information that determines whether a Linux PC performs IP forwarding?

- Attach the content of the file `/etc/sysconfig/network-scripts/ifcfg-eth0` to your lab report.
Part 6. Using Ping

One of the most basic, but also most effective tools to debug IP networks is the ping command. The ping command tests whether another host or router on the Internet is reachable. The ping command sends an ICMP Echo Request datagram to an interface, and expects an ICMP Echo Reply datagram in return. The different uses of the ping command are explained in Section 2.2.3 of the Introduction.

Note:

- On Linux systems, ping continues to send packets until you interrupt the command with the Ctrl-c keys.
- When using ping on the Linux PCs, we recommend to always send at least two ICMP Echo Request packets. We have observed that in many occasions, the first ICMP Echo Request may be dropped at the receiver.

Exercise 6. Issuing ping commands

1. From PC1, send 5 ping messages (using the –c option) to PC2. Save the output.

   PC1% ping –c 5 10.0.1.12

2. On PC2, issue a ping to the IP address of PC1. Also, issue a ping command to the loopback interface, 127.0.0.1. Limit the number of pings to 5. Save the output.

Lab Report

- Include the output you saved in this exercise.

- Explain the difference between pinging the local Ethernet interface and the loopback interface. Specifically, on PC1, what is the difference between typing “ping 10.0.1.11” and “ping 127.0.0.1”. (This is a conceptual question on the role of the loopback interface. The response to the ping command does not provide you with the answer to this question.)

- (To be completed after the lab). Find a host connected to the Internet. Send ping messages to a number of web servers on the Internet and collect statistics on the maximum round-trip delay of the ICMP Echo Request/Echo Reply. Try to find a host with a very long round-trip time. To avoid overloading the destination, do not send more than 3 ping packets to any destination machine. Save the output data and include it in your lab report.
Part 7. Basics of tcpdump

Tcpdump allows you to capture traffic on a network and display the packet headers of the captured traffic. Tcpdump can be used to identify network problems or to monitor network activities. See Section 3 of the Introduction for more details on the tcpdump command and its use for network traffic analysis.

Exercise 7-a. Simple tcpdump exercise

Use tcpdump to observe the network traffic that is generated by issuing ping commands.

1. Switch to PC1. Start tcpdump so that it monitors all packets that contain the IP address of PC2, by typing
   
   PC1% tcpdump –n host 10.0.1.12

2. Open a new window and execute
   
   PC1% ping –c 1 10.0.1.12

3. Observe the output of tcpdump. Save the output to a file.

   If you use the tee or tail commands to simultaneously view and save the output from tcpdump, you need to use the –l option of tcpdump. For example:

   tcpdump –n –l > filename & tail –f filename
   tcpdump –n –l | tee filename

   **Note:** It may be necessary to hit Ctrl-c to terminate the tcpdump session. In some situations, it may be best to simply redirect the output of tcpdump straight to a file (e.g., tcpdump > filename) and view it afterwards with the more command or a text editor.

Lab Report:

Include the saved output in your lab report. Explain the meaning of each field in the captured data.

Exercise 7-b. Another tcpdump traffic capture

1. On PC1, start capturing packets using the tcpdump -n command.

2. Issue a ping to the non-existing IP address 111.111.111.111:
   
   PC1% ping –c 1 111.111.111.111

3. Issue a ping to the broadcast address 10.0.1.255 using the command:
4. Save the outputs of `ping` and `tcpdump` to a file.

Lab Report

Include the saved output in your lab report and interpret the results. How many of the Linux PCs responded to the broadcast `ping`?
Ethereal is a network protocol analyzer with a graphical user interface. Using ethereal, you can interactively capture and examine network traffic, view summaries and get detailed information for each packet. In Section 3 of the Introduction we provide more details on the use of ethereal.

Exercise 8. Running ethereal

This exercise walks you through the steps of capturing and saving network traffic with ethereal. The exercise is conducted on PC1.

1. **Starting ethereal**: On PC1, start ethereal by typing

   ```
   PC1% ethereal
   ```

   This displays the ethereal main window on your desktop as shown in Figure 1.3.

   ![Ethereal Main Window](image)

   **Figure 1.3. Ethereal Main Window.**
2. Selecting the capture options: Use the instructions in Figure 1.4 to set the options of ethtool in preparation for capturing traffic. Use the same options in other labs, whenever ethtool is started.

Selecting capture preferences in ethtool:

1. From the main window, select "Capture:Start".
2. This displays the following "Capture Preferences" window:

- Select eth0 in "Interface".
- Select "Capture packets in promiscuous mode".
- Select "Update list of packets in real time".
- Select "Automatic scrolling in live capture".
- Unselect "Enable MAC name resolution".
- Unselect "Enable network name resolution".
- Unselect "Enable transport name resolution".

![Figure 1.4 . General capture settings for ethtool.](image)

3. Starting the traffic capture: Start the packet capture by clicking “OK” in the “Capture Preferences” window.

4. Generating traffic: In a separate window on PC1, execute a ping command to PC3.

   PC1% ping -c 2 10.0.1.13

   Observe the output in the ethtool main window.
Click and highlight a captured packet in the *ethereal* window, and view the headers of the captured traffic.

4. **Stopping the traffic capture:** Click "Stop" in the window "Ethernet Capture".

5. **Saving captured traffic:** Save the results of the captured traffic as a plain text file. This is done by selecting “Print” in the “File” menu. When a “Print” window pops up, select the options and set a filename as shown in Figure 1.5.

---

**Selecting print options in the “Print” window for saving captured traffic to plain text files:**

- Select the format "Plain Text".
- Select the “File” checkbox and type the filename in the field next to the “File” button.
- Select “Print summary” if you want to save only some high level information on each packet. *Print summary* is usually sufficient.
- Select “Print detail” and "Expand all levels" if you want to save all details of all packets at all levels.
- Click the “OK” button to complete the save operation.

---

*Figure 1.5. Selecting print options.*
Note:

- In general, unless asked to do otherwise, always select the “Print summary” option when you include saved data in the lab report. This will help keep the length of the lab report reasonably small. If detailed information is required you will be asked to save “details” of the captured traffic. In this case, select the “Print detail” option.

- If you select “Save” in the “File” menu, the captured data is saved in the format of a libpcap file. This format can be interpreted by both tcpdump and ethereal. Measurements saved in libpcap format can be analyzed at a later time. However, libpcap files are not plain text files and are not useful for preparing your report.

- Unless you have the tcpdump and/or ethereal tools available on a system outside of the Internet Lab, which allows you to view and save captured traffic as text at a later time, always save captured traffic in plain text format.

Lab Report:

Include the file with the captured data in your lab report. Save the details of the captured traffic, using the “Print detail” option in the Print window. Describe the differences between the files saved by tcpdump (in Part 7) and by ethereal (in this part).
Checklist Form for Lab 1

Complete this checklist as you work through the laboratory exercises and attach the form to your lab report.

Name (Please Print): ________________________________

<table>
<thead>
<tr>
<th>Check-off for Part 1</th>
<th>Check-off for Part 2</th>
<th>Check-off for Part 3</th>
<th>Check-off for Part 4</th>
<th>Check-off for Part 5</th>
<th>Check-off for Part 6</th>
<th>Check-off for Part 7</th>
<th>Check-off for Part 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prelab 1 Question Sheet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedback sheet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Feedback Form for Lab 1

- Complete this feedback form at the completion of the lab exercises and submit the form when submitting your lab report.

- The feedback is anonymous. **Do not put your name on this form** and keep it separate from your lab report.

- For each exercise, please record the following:

<table>
<thead>
<tr>
<th>Difficulty (-2, -1, 0, 1, 2)</th>
<th>Interest Level (-2, -1, 0, 1, 2)</th>
<th>Time to complete (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2 = too easy</td>
<td>-2 = low interest</td>
<td></td>
</tr>
<tr>
<td>0 = just right</td>
<td>0 = just right</td>
<td></td>
</tr>
<tr>
<td>2 = too hard</td>
<td>2 = high interest</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 1. Getting familiar with the equipment</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2. Using the Linux operating system</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 3. Saving your data</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 4. Copying files using floppy disks</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 5. Locating configuration files in Linux</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 6. Using ping</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 7. Basics of tcpdump</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 8. Basics of ethereal</th>
<th>Difficulty</th>
<th>Interest Level</th>
<th>Time to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please answer the following questions:

- What did you like about this lab?

- What did you dislike about this lab?

- Make a suggestion to improve the lab.