The University of Queensland
School of Information Technology and Electrical Engineering

Semester 1, 2014

COMS3200 / COMS7201 – Assignment 3

Due: by 6 June 2014
(must be marked during your scheduled prac sessions)
Total Marks: 5
Weighting: 5% of final grade

Introduction

In this assignment you will learn how to use simple network diagnostic and query tools.

The assignment will be assessed by the tutor **during regular lab sessions,** in weeks 12 and 13 of the semester. You should attend the practical sessions based on a schedule which assigns students to particular pracs. The schedule will appear on Blackboard. Your Si-net enrolment will be taken into account when the schedule is created. If you cannot attend your assigned session, please send an email to the lecturer.

The session is "Open-Book" – you can bring in any materials you wish. You cannot consult with other students during the session.

A separate answer sheet will be provided at the examination session for you to record your answers, and for the tutor to record your score. The tutor will also ask you an oral question or two. You have 30 minutes to complete the exercise.

It is expected that when you answer an oral question for the tutor, you will be able to display the necessary evidence on your screen.

If you have problems with any of the UNIX tools below, you can read the documentation using the command `man` *`cmd-name`* where *cmd-name* is replaced by the command of interest.

A1: Finding out about host's network configuration

On moss, run:

```
/sbin/ifconfig -a
```

This shows details of the network interfaces connected to the current computer. For the computers in the lab, there is only one network interface, for this example you are connected to Moss which means that when you run the above command you will get Moss's network interfaces.

There are similar commands for Windows (NT/2000/XP):

Run (from a command prompt window):

```
ipconfig /all
```

Look at the first 6 digits of the Ethernet (Physical or MAC) address. Open up a web browser and visit the "organizationally unique identifier" (OUI) registry: (http://standards.ieee.org/regauth/oui/index.shtml) to determine the vendor of the NIC (Network Interface Controller) for eth0 on moss. Who made the network controller? **[0.5 mark]**

A2: Checking that a host is alive

The **ping** command tests that a remote host is alive. It uses the ICMP protocol to send a message to the given host. You must provide either the hostname or IP address of the host as the parameter for this command.

If you are in the labs, ask a neighbour what their IP address is (find out using ipconfig), and then ping to their computer.

Because of the firewall between the ITEE PC lab and the outside world, you cannot ping general Internet hosts.

For the purpose of this prac, however, you should be able to ping to the following hosts from moss (ITEE Student UNIX server):

```
ping student.uq.edu.au
ping www.stanford.edu
ping www.cam.ac.uk
```

If you try from outside the firewall, you should be able to ping many hosts on the Internet.

Which of the following hosts is further away (based on average round-trip time):

```
www.stanford.edu
www.cam.ac.uk ?
```

Use Control-C to interrupt these after a few packets. What's the average round trip time to the site which is "furthest" away? **[0.5 mark]**

A3: Tracing the route of IP packets

The **traceroute** command is used to find out what routers a packet passes through to reach its destination. The hostnames of routers often have some indication of the city in them, so it is possible to make an educated guess at where the packets travel. The same command on Windows is **tracert**. Before using **tracert** command on the windows prompt in the lab, please enable Internet access first (eg. by opening an external website).

For example, consider the following **tracert** to www.yahoo.com.

```
  1    <1 ms    <1 ms    <1 ms  ss1.eait.uq.edu.au [10.240.129.251]
  2    <1 ms    <1 ms    <1 ms  falcon-a1-364.router.uq.edu.au [130.102.1.169]
  3    <1 ms    <1 ms    <1 ms  talon-falcon-2.router.uq.edu.au [172.16.1.75]
  4    <1 ms    <1 ms    <1 ms  uq-se1-talon.router.uq.edu.au [130.102.159.16]
  5    <1 ms    <1 ms    <1 ms  uq-gw1-uq-se1.router.uq.edu.au [130.102.159.0]
  6    <1 ms    <1 ms    <1 ms  tengigabitethernet2-2.er2.uq.cpe.aarnet.net.au
[113.197.8.33]
  7     *        *        *     Request timed out.
  8    17 ms    17 ms    17 ms  so-2-0-0.bb1.a.syd.aarnet.net.au [202.158.194.49]
  9   175 ms   175 ms   175 ms  so-2-2-0.bb1.a.pao.aarnet.net.au [202.158.194.174]
 10   175 ms   175 ms   175 ms  PAT1.pao.yahoo.com [198.32.176.135]
 11   176 ms   176 ms   176 ms  ae-1-d151.msr2.sp1.yahoo.com [216.115.107.79]
 12   176 ms   176 ms   176 ms  et-17-25.fab3-1-gdc.sp2.yahoo.com [98.136.16.27]
 13   176 ms   176 ms   176 ms  te-9-1.bas2-1-prd.sp2.yahoo.com [67.195.130.108]
 14   200 ms   176 ms   186 ms  ir1.fp.vip.sp2.yahoo.com [98.137.149.56]

Trace complete.
```

This tracert shows that the destination was reached in 14 hops, and indicates routers on the path. Check the time values. Notice when the average round trip time jumps sharply from around 17ms to around 175ms - this is when the packet travelled over the international link between Australia and the USA. Notice also the hostname of the first router the packet encounters in the USA: `so-2-2-0.bb1.a.pao.aarnet.net.au`.

In the ITEE labs you will be only able to run **tracert** to selected destinations. Other destinations are blocked by a firewall.

In the labs, run (on Windows prompt):

```
tracert www.stanford.edu
tracert www.cam.ac.uk
```

For www.stanford.edu, try to estimate the time taken for each of the hops along the route. Do you see any anomalies in your calculated hop times? If so, how can you explain them? **[0.5 mark]**

A4: Showing open connections and network statistics on the current machine

The Unix **netstat** command shows network status/statistics.

```
netstat –a
```

(You may need to pipe this to *more*, i.e. `netstat –a | more`)

The -a parameter indicates that all statistics should be shown, which in this case shows all open ports.

```
netstat –s
```

This shows TCP/IP protocol statistics, including TCP, UDP, IP and ICMP. Are there any errors there that you would not normally expect?

What percentage of outgoing TCP segments are retransmissions? **[0.5 mark]**

To view the routing table on the current machine, run:

```
netstat -r
```

On Windows you can can also use:

```
route print
```

Examine the routing table. Notice the different network destinations. The default destination (default gateway) for your machine (PC) is the entry in the routing table where the "Network Destination" field is all 0's (0.0.0.0) in Windows and localhost in Unix.

Try adding a new entry to the routing table (on Windows). In reality, this entry will do nothing because your computer only has one connection to the Internet (so all packets destined for external machines must travel along that one connection). On a computer that had two network connections, changing the routing table could be useful though.

```
route add 130.102.35.0 mask 255.255.255.0 130.102.75.254 metric 2
```

(Note: In the lab try Gateway IP address: 10.240.128.116 instead of 130.102.75.254)

This says that all packets destined for the network 130.102.35.0 (somewhere else on the UQ campus), using subnet mask 255.255.255.0 should be sent via the gateway whose IP address is 130.102.75.254 and the metric for this route (e.g. number of hops) is 2.

Now delete the route.

```
route delete 130.102.35.0
```

To see some help on the syntax of the route command, just type the command name on its own:

```
route
```

A5: ARP protocol

The **arp** command can be used to view a list of MAC addresses (Ethernet addresses) of other hosts that your host has communicated with. Just run:

```
arp -a
```

This can be useful for debugging network-related problems, for example where two hosts on the same network have been given the same IP address and are therefore conflicting.

On your PC, use ipconfig and arp –a to find the IP address and MAC address of the default gateway that your PC connects to. **[0.5 marks]**

A6: Windows networking

You can view Windows networking information from the command prompt as well. For example, to see a list of hosts in your "Network Neighbourhood", run:

```
net view
```

To view the list of shares on a particular machine (directories and printers that you can access on that machine), run:

```
net view \\pcname
```

(but replace "pcname" with the name of a machine in your network neighbourhood).

To view a list of shares that your machine is offering to others, run:

```
net share
```

To view a list of shares that your machine has already mounted off other machines, run:

```
net use
```

A7: Finding information about Internet domains

Whois is a tool specifically for querying the Internet Domain Name System (DNS). The DNS maintains information about Internet domains and hosts, including what the cryptic abbreviations in hostnames stand for, the geographic location of computers in a particular domain (or at least a hint as to where they might be located), and information about who owns or maintains the DNS information for a particular domain.

InterNIC were once the registry responsible for major domain names in the USA, including the .edu, .com, .gov .net and .org domains, but this control has now been spread across several agencies (check it on http://www.internic.com/regist.html). One of them is Network Solutions Inc. (http://www.networksolutions.com/). The centre responsible for Australian (and Pacific region) domains is called APNIC (http://www.apnic.net), the Asian-Pacific Network Information Centre. In Europe, the centre is known as RIPE (http://www.ripe.net), the Réseaux IP Européens.

Use the link to Network Solutions' Whois gateway: http://www.networksolutions.com/cgi-bin/whois/whois to find out who is the owner (registrant) of the *newsouthwales.com* domain **[0.5 mark]**

A8: Discover the protocol message exchange for FTP

The exchange of protocol information in FTP can be examined by enabling a debug mode in ftp programs. For the purpose of this exercise login to the student Unix server (e.g. through ssh to the moss server).

ftp to ftp.uq.edu.au, provide “ftp” as the login name and your email address as the password;
at ftp prompt set option *debug* (ftp> `debug`)

(Note: if the above does not work, try to login with your *student number* and then for password enter your *email password*).

Observe commands sent by the FTP client and responses from the FTP server for a series of commands: **`pwd, cd mirror, cd suse, dir, get README.local, get file`**.
What are the FTP commands sent for `get`?

(1) What is the response code to a correctly executed `get` command (i.e., get a file from the ftp server successfully) **[0.5 mark]** and (2) what is the response code for `get`-ing a file which does not exist (get file)? **[0.5 mark]**

A9: DNS information

The **nslookup** command can be used to query the DNS server. Try

```
nslookup print
```

What is print's IP address? **[0.5 marks]**

Repeat this query. Did you get the same result?

Use **whois command** on moss to find information about the `stanford.edu` domain and its name servers. And then find the IP address of the Argus name server. **[0.5 marks]**

Notes

Late Submission

Late completion of this assignment will not be possible – **you must complete this during the scheduled prac sessions.** In the event of exceptional personal or medical circumstances that prevent on-time completion, you should contact the course coordinator and be prepared to supply appropriate documentary evidence.

Clarifications

It is possible that there are inconsistencies in the above requirements and/or that not all details have been specified. Please ask if you unsure of the requirements. Please monitor your email, the course newsgroup, or the course website for clarifications and/or corrections to the above information. It will be assumed that students see such email or postings by the end of the next business day.

This is an individual assignment. You are reminded of the statements contained in the COMS3200 / COMS7201 course profile regarding collaboration and plagiarism.