
The University of Queensland
School of Information Technology and Electrical Engineering
Semester Two, 2009

COMS3200 / COMS7201 – Assignment 3

Due: 5pm Friday October 30
(must be marked during your scheduled prac sessions)

Total Marks: 7

Weighting: 7% of final grade

Introduction

This assignment has several goals. You will learn how to use simple network diagnostic and query tools (part A). You will also be required to install and configure the Apache web server software on a PC (part B).

Both parts will be assessed by the tutor **during regular lab sessions, P1, and P4**, in Room 78-109 in week 12 or 13 of the semester. You should attend the practical sessions based on a schedule which assigns students to particular pracs. The schedule will be sent to the COMS3200/7201 students by email. 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. When you arrive to the scheduled session please write your name on the board and the tutor will mark you in that order

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 45 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.

Part A – Network Diagnostics (5 marks)

A1: Finding out about host's network configuration

On agave, 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 Agave which means that when you run the above command you will get Agave’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 your NIC (Network Interface Card). Who made your network card? [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 agave (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.

For example, consider the following traceroute to `www.yahoo.com`.

```
traceroute to www.yahoo.com (66.94.230.47), 30 hops max, 40 byte packets
 1 ss0-67.itee.uq.edu.au (130.102.67.250) 0.578 ms 0.415 ms 0.373 ms
 2 gw-iteefw.router.uq.edu.au (130.102.1.169) 0.688 ms 0.628 ms 0.615 ms
 3 zeus-falcon.router.uq.edu.au (130.102.1.149) 0.882 ms 0.726 ms 0.706 ms
 4 gigabitethernet1.er1.uq.cpe.aarnet.net.au (202.158.203.249) 0.806 ms 0.620 ms 0.668 ms
 5 gigheter0-2-5.bb1.a.bne.aarnet.net.au (202.158.203.241) 23.287 ms 18.830 ms 18.947 ms
 6 pos3-0-0.bb1.a.syd.aarnet.net.au (202.158.194.49) 36.135 ms 27.447 ms 39.880 ms
 7 pos2-0.bb1.a.pao.aarnet.net.au (202.158.194.74) 176.195 ms 176.010 ms 175.949 ms
 8 p4-4-1-0.r00.plalca01.us.bb.verio.net (129.250.10.225) 176.196 ms 176.181 ms 175.806 ms
 9 pl6-0-1-0.r20.plalca01.us.bb.verio.net (129.250.3.78) 176.025 ms 175.968 ms 176.070 ms
10 so7-0-0-2488M.ar2.PAO2.gblx.net (208.50.13.97) 179.698 ms 189.280 ms 179.688 ms
11 208.51.74.22 (208.51.74.22) 177.084 ms 177.037 ms 177.290 ms
12 ge-4-0-0-p440.msrl1.scd.yahoo.com (216.115.106.201) 179.542 ms ge-3-0-0-
p250.msrl2.scd.yahoo.com (216.115.106.181) 179.882 ms ge-4-0-0-p440.msrl1.scd.yahoo.com
(216.115.106.201) 179.558 ms
13 UNKNOWN-66-218-82-221.yahoo.com (66.218.82.221) 177.545 ms UNKNOWN-66-218-82-219.yahoo.com
(66.218.82.219) 177.148 ms UNKNOWN-66-218-82-221.yahoo.com (66.218.82.221) 177.044 ms
14 pl6.www.scd.yahoo.com (66.94.230.47) 179.555 ms 179.802 ms 179.789 ms
```

This traceroute 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 30ms 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: hssi9-0-0.la1.optus.net.au. It is a fair guess to say that this Optus international link goes to Los Angeles.

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

In the labs, run (in Unix):

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

In Windows, the equivalent command is `tracert`.

Determine some of the cities traversed by the traceroute probe for one of the last three destinations. You may find it useful to look at <http://www.sarangworld.com/TRACEROUTE/showdb-2.php3>.

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]**

What is the default time to live for IPv4? **[0.5 mark]**

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

```
netstat -r
```

On Windows you can 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
```

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.

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

What is the response to a correctly executed `get` command (`get README.local`) and what is the response for `get`-ing a file which does not exist (`get file`)? **[0.5 mark]**

A9: HTTP Protocol

HTTP is an ASCII based protocol so it is possible to simulate it using netcat. Use netcat to request the page www.itee.uq.edu.au

Note: You will need to download netcat for windows and run it from DOS Prompt. Netcat for windows can be downloaded from:

1. <http://joncraton.org/files/nc111nt.zip>
2. <http://www.governmentsecurity.org/forum/index.php?showtopic=677>

After downloading netcat, extract the file to a folder on your computer, then open command prompt window and change the directory to the folder where netcat is stored. Now run the following command:

**nc www.itee.uq.edu.au 80 (hit enter)
(type something on the next line and hit Enter)**

Examine the response. What HTTP response code is returned? **[0.5 mark]**

A10: DNS information

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

```
nslookup printhost
```

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

Repeat this query. Did you get the same result?

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

Part B - Web Server Configuration (2 marks)

This part of the prac requires you to install and configure the Apache web server on your Windows PC. Apache and servers based on Apache have above 50% of the world web server market (see <http://news.netcraft.com/>).

You can download the Apache installer from the course website. Documentation relating to use on Windows can be found at <http://httpd.apache.org/docs-2.0/platform/windows.html>.

You should install the web server and change the configuration so that it listens on a port number equal to the first five digits of your student number (e.g. if your student number is 41234567, your server should listen on port number 41234). Modify the default `index.html` page so that it contains your name and student number in the displayed text. Check you can see the page at

<http://hostname:portnumber/index.html> where hostname is replaced by the hostname of your PC and portnumber is replaced by the portnumber your server is listening on. Show the tutor that you have successfully performed this task [**2 marks**]

(It does not matter whether you install Apache as a service or not. Note that you may need to reimage your PC before this prac if another user has already installed Apache. You should also reimage your PC after this prac.)

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 are 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.