COMPUTER NETWORKS

LAB BRIEF

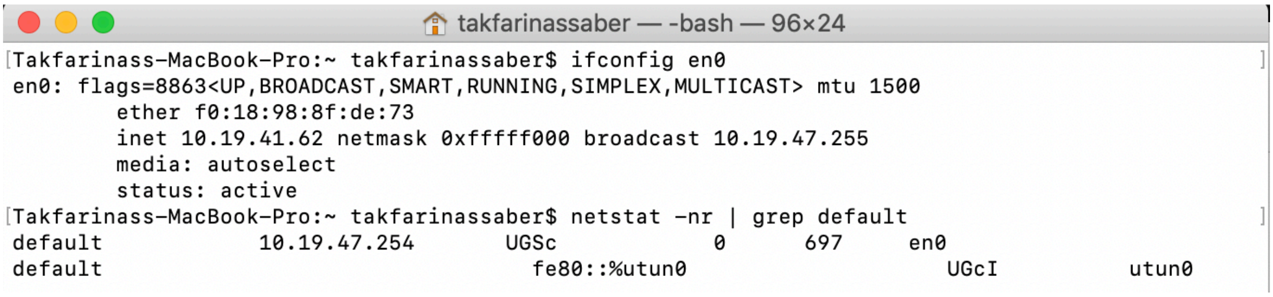
We will be looking at and using some networking utilities. These are different programs that can be used to find out information about the network we are using and the data that is being sent over it. We will see two very simple tools in ipconfig(ifconfig) and tracert(traceroute), and then look at a tool used by network engineers to inspect all aspects of traffic on the network with Wireshark. This is not just a lab, but also a **research** assignment. In the Wireshark tutorial you will come up to some concepts you do not know. Look up these concepts online and try to figure out what they are and what the question is asking.

BASIC UTILITIES

First we will look at some basic utilities for finding out about the network.

ipconfig (unix: “ifconfig en0”, then “netstat -nr | grep default”)

This is a command line program for finding basic information about your network connections. You should see information about each network interface available and information such as IP address.To use this simply open a command prompt (or “terminal” on unix) and type the command. You should see something like this where the IP address and default gateway is shown.



```
Takfarinass-MacBook-Pro:~ takfarinassaber$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether f0:18:98:8f:de:73
        inet 10.19.41.62 netmask 0xfffff000 broadcast 10.19.47.255
        media: autoselect
        status: active
Takfarinass-MacBook-Pro:~ takfarinassaber$ netstat -nr | grep default
default            10.19.47.254       UGSc            0      697     en0
default                                 fe80::%utun0                      UGcI          utun0
```

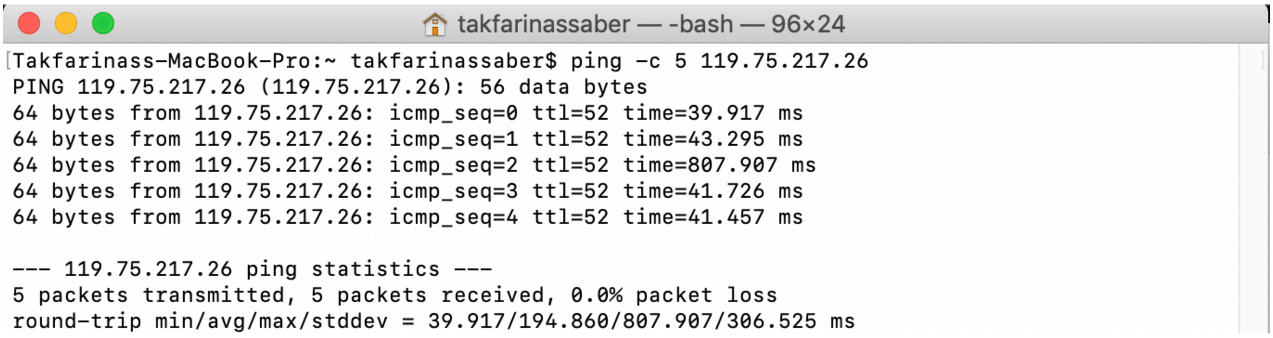
Question 1

What is your IP address and default gateway?

Ping

Ping is a hugely popular tool in network debugging. Let’s use it and figure out what it does.
In the terminal use the command:
>ping [ip address]
e.g. : to test your gateway connection
>ping 10.19.47.254

What does “-c 5” in this command do?



```
Takfarinass-MacBook-Pro:~ takfarinassaber$ ping -c 5 119.75.217.26
PING 119.75.217.26 (119.75.217.26): 56 data bytes
64 bytes from 119.75.217.26: icmp_seq=0 ttl=52 time=39.917 ms
64 bytes from 119.75.217.26: icmp_seq=1 ttl=52 time=43.295 ms
64 bytes from 119.75.217.26: icmp_seq=2 ttl=52 time=807.907 ms
64 bytes from 119.75.217.26: icmp_seq=3 ttl=52 time=41.726 ms
64 bytes from 119.75.217.26: icmp_seq=4 ttl=52 time=41.457 ms

--- 119.75.217.26 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 39.917/194.860/807.907/306.525 ms
```

Try ping your neighbours computer, does it respond?

Try ping a few servers we know (**Note:** use your own WiFi connection. Ping might be blocked in BJUT).

>ping -c 5 www.bjut.edu.cn
>ping -c 5 www.baidu.com
>ping -c 5 www.google.com

Question 2

How do we tell if the ping has “worked”?
How do we tell if the ping has not “worked”?
What in your opinion is the function of the ping command?

tracert (unix - traceroute)

This program is designed to trace the route between two computers. For example if we want to find the route between our computer and baidu.com we would open a command prompt

type the command: **tracert baidu.com**

Each line represents another gateway/router/device between your computer and the target.

How does trace route operate?

Question 3

How many hops to get to the BJUT webserver?

How many hops to get to the baidu.com server?

Why is this the case?

Note - A lot of information can be obtained with tracert if it is interpreted properly.

PACKET ANALYSIS

We are going to use a program called Wireshark to perform packet analysis. This will look at all the packets being sent in a network and allow you to investigate the packets.

Open the wireshark program:

Follow the Wireshark tutorial in the slides on moodle. This is a good introductory tutorial on wireshark.

Question 4

Go through the steps and answer the 7 exercises on your document.
Some of the topics in the tutorial are unknown to you (such as SYN attacks). Do a little research and find out what these concepts are before answering the questions.
The following files are needed for the tutorial and are available on moodle (Lab 7 Traces.zip):

01telnet.pcap, 02massivesyn.pcap, 02massivesyn.pcap, 03Jim.pcap, 03risa.pcap, 04chat.dmp, 05ftp1.pcap, 06foobar.pcap, 07covertinfo.pcap.

There are traces of real packets that were captured in real time. They were saved and we will reload them and investigate.