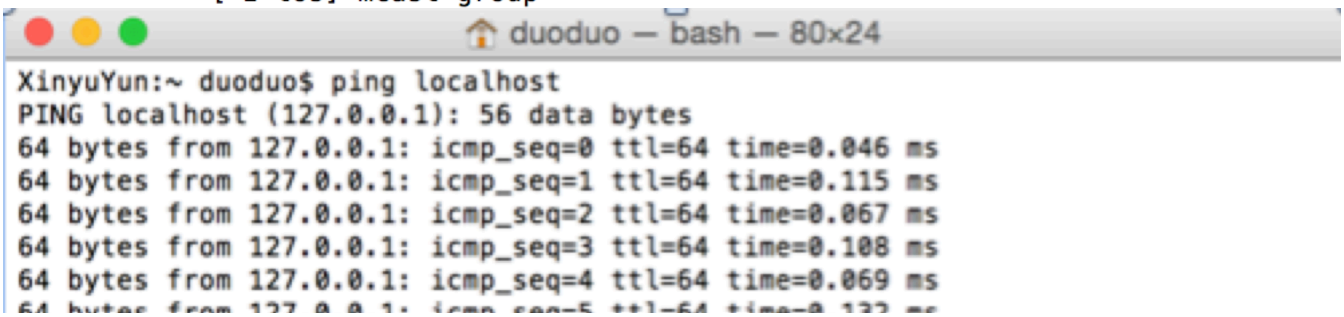
Lab 1 Report – Xinyu Yun

Procedure:
a. Use **`ping`** and **`tracert`** on your workstations to familiarize yourself with these commands. Also search for these terms in the Internet Encyclopedia. List a few of the flags that are used with these two commands. (7)

1- Ping your workstation's loopback interface using the command: (3)
`ping localhost` or `ping 127.0.0.1`
It is a good way to test your machine's basic network configuration.
Was the ping successful? If the ping is successful, then TCP/IP is properly installed and functioning on this workstation.

Screenshot:

```
XinyuYun:~ duoduo$ ping
usage: ping [-AaDdfnoQqRrv] [-b boundif] [-c count] [-G sweepmaxsize]
            [-g sweepminsize] [-h sweepincrsize] [-i wait] [-k trafficclass]
            [-l preload] [-M mask | time] [-m ttl] [-p pattern]
            [-S src_addr] [-s packetsize] [-t timeout][-W waittime] [-z tos]
            host
       ping [-AaDdfLnoQqRrv] [-b boundif] [-c count] [-I iface] [-i wait]
            [-k trafficclass] [-l preload] [-M mask | time] [-m ttl] [-p pattern
] [-S src_addr]
            [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
            [-z tos] mcast-group
```



2- Ping your default gateway and your DNS server. Use the *ipconfig* command on your Windows workstation to identify your DNS server and your default gateway. (3)

Comments:
As I tested in my macbook, I used "dig localhost" to find my DNS server

```
XinyuYun:~ duoduo$ dig localhost

; <<>> DiG 9.8.3-P1 <<>> localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5893
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;localhost.                     IN      A

;; ANSWER SECTION:
localhost.              596206  IN      A       127.0.0.1

;; AUTHORITY SECTION:
localhost.              596206  IN      NS      localhost.

;; Query time: 5 msec
;; SERVER: 172.30.80.1#53(172.30.80.1)
;; WHEN: Wed Sep 30 12:05:05 2015
;; MSG SIZE  rcvd: 57
```

After finding the DNS address, below is the ping result:

```
XinyuYun:~ duoduo$ ping -c 5 172.30.80.1
PING 172.30.80.1 (172.30.80.1): 56 data bytes
64 bytes from 172.30.80.1: icmp_seq=0 ttl=64 time=2.245 ms
64 bytes from 172.30.80.1: icmp_seq=1 ttl=64 time=2.362 ms
64 bytes from 172.30.80.1: icmp_seq=2 ttl=64 time=2.260 ms
64 bytes from 172.30.80.1: icmp_seq=3 ttl=64 time=2.250 ms
64 bytes from 172.30.80.1: icmp_seq=4 ttl=64 time=2.360 ms

--- 172.30.80.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.245/2.295/2.362/0.054 ms
```

b. Use ping to measure Round Trip Time (RTT) for 10 messages of size 64, 256, and 4096 bytes. Graph (10 each plot) the message size versus RTT for:

1- two hosts on a LAN (two workstations in the lab or in your house)

Answer:

Here I select 2 devices in my housing LAN

Host 1: 192.168.199.124 (my android pad)

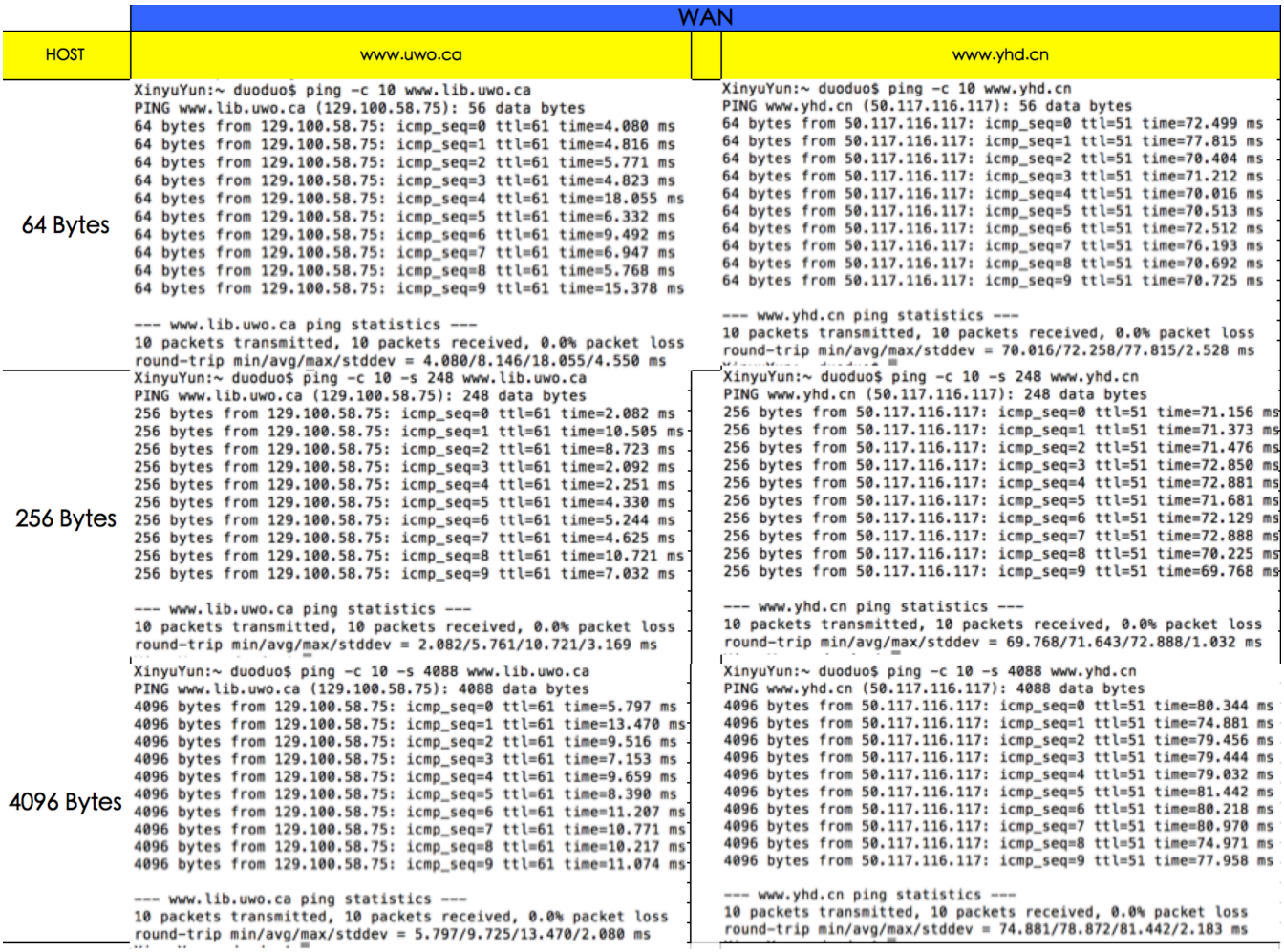
Host 2: 192.167.199.230 (my other laptop)

	LAN	
HOST	192.168.199.124	192.168.199.230
64 Bytes	XinyuYun:~ duoduo$ ping -c 10 192.168.199.124 PING 192.168.199.124 (192.168.199.124): 56 data bytes 64 bytes from 192.168.199.124: icmp_seq=0 ttl=64 time=94.278 ms 64 bytes from 192.168.199.124: icmp_seq=1 ttl=64 time=111.244 ms 64 bytes from 192.168.199.124: icmp_seq=2 ttl=64 time=31.303 ms 64 bytes from 192.168.199.124: icmp_seq=3 ttl=64 time=48.906 ms 64 bytes from 192.168.199.124: icmp_seq=4 ttl=64 time=69.751 ms 64 bytes from 192.168.199.124: icmp_seq=5 ttl=64 time=13.874 ms 64 bytes from 192.168.199.124: icmp_seq=6 ttl=64 time=106.298 ms 64 bytes from 192.168.199.124: icmp_seq=7 ttl=64 time=125.551 ms 64 bytes from 192.168.199.124: icmp_seq=8 ttl=64 time=48.696 ms 64 bytes from 192.168.199.124: icmp_seq=9 ttl=64 time=150.003 ms --- 192.168.199.124 ping statistics --- 10 packets transmitted, 10 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 13.874/79.990/150.003/42.003 ms	XinyuYun:~ duoduo$ ping -c 10 192.168.199.230 PING 192.168.199.230 (192.168.199.230): 56 data bytes 64 bytes from 192.168.199.230: icmp_seq=0 ttl=64 time=40.088 ms 64 bytes from 192.168.199.230: icmp_seq=1 ttl=64 time=44.588 ms 64 bytes from 192.168.199.230: icmp_seq=2 ttl=64 time=65.661 ms 64 bytes from 192.168.199.230: icmp_seq=3 ttl=64 time=86.023 ms 64 bytes from 192.168.199.230: icmp_seq=4 ttl=64 time=102.969 ms 64 bytes from 192.168.199.230: icmp_seq=5 ttl=64 time=136.239 ms 64 bytes from 192.168.199.230: icmp_seq=6 ttl=64 time=47.587 ms 64 bytes from 192.168.199.230: icmp_seq=7 ttl=64 time=57.220 ms 64 bytes from 192.168.199.230: icmp_seq=8 ttl=64 time=126.550 ms 64 bytes from 192.168.199.230: icmp_seq=9 ttl=64 time=106.414 ms --- 192.168.199.230 ping statistics --- 10 packets transmitted, 10 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 40.088/81.334/136.239/33.460 ms
256 Bytes	PING 192.168.199.124 (192.168.199.124): 248 data bytes 256 bytes from 192.168.199.124: icmp_seq=0 ttl=64 time=41.811 ms 256 bytes from 192.168.199.124: icmp_seq=1 ttl=64 time=7.075 ms 256 bytes from 192.168.199.124: icmp_seq=2 ttl=64 time=90.823 ms 256 bytes from 192.168.199.124: icmp_seq=3 ttl=64 time=109.450 ms 256 bytes from 192.168.199.124: icmp_seq=4 ttl=64 time=129.464 ms 256 bytes from 192.168.199.124: icmp_seq=5 ttl=64 time=50.188 ms 256 bytes from 192.168.199.124: icmp_seq=6 ttl=64 time=6.244 ms 256 bytes from 192.168.199.124: icmp_seq=7 ttl=64 time=9.057 ms 256 bytes from 192.168.199.124: icmp_seq=8 ttl=64 time=112.185 ms 256 bytes from 192.168.199.124: icmp_seq=9 ttl=64 time=13.910 ms --- 192.168.199.124 ping statistics --- 10 packets transmitted, 10 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 6.244/57.021/129.464/46.575 ms	XinyuYun:~ duoduo$ ping -c 10 -s 248 192.168.199.230 PING 192.168.199.230 (192.168.199.230): 248 data bytes 256 bytes from 192.168.199.230: icmp_seq=0 ttl=64 time=178.182 ms 256 bytes from 192.168.199.230: icmp_seq=1 ttl=64 time=115.738 ms 256 bytes from 192.168.199.230: icmp_seq=2 ttl=64 time=115.953 ms 256 bytes from 192.168.199.230: icmp_seq=3 ttl=64 time=30.218 ms 256 bytes from 192.168.199.230: icmp_seq=4 ttl=64 time=86.895 ms 256 bytes from 192.168.199.230: icmp_seq=5 ttl=64 time=68.985 ms 256 bytes from 192.168.199.230: icmp_seq=6 ttl=64 time=206.830 ms 256 bytes from 192.168.199.230: icmp_seq=7 ttl=64 time=203.370 ms 256 bytes from 192.168.199.230: icmp_seq=8 ttl=64 time=123.191 ms 256 bytes from 192.168.199.230: icmp_seq=9 ttl=64 time=40.439 ms --- 192.168.199.230 ping statistics --- 10 packets transmitted, 10 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 30.218/116.980/206.830/59.932 ms
4096 Bytes	XinyuYun:~ duoduo$ ping -c 10 -s 4088 192.168.199.124 PING 192.168.199.124 (192.168.199.124): 4088 data bytes 4096 bytes from 192.168.199.124: icmp_seq=0 ttl=64 time=115.487 ms 4096 bytes from 192.168.199.124: icmp_seq=1 ttl=64 time=127.930 ms Request timeout for icmp_seq 2 4096 bytes from 192.168.199.124: icmp_seq=3 ttl=64 time=68.790 ms 4096 bytes from 192.168.199.124: icmp_seq=4 ttl=64 time=90.148 ms 4096 bytes from 192.168.199.124: icmp_seq=5 ttl=64 time=109.623 ms 4096 bytes from 192.168.199.124: icmp_seq=6 ttl=64 time=127.392 ms 4096 bytes from 192.168.199.124: icmp_seq=7 ttl=64 time=144.988 ms 4096 bytes from 192.168.199.124: icmp_seq=8 ttl=64 time=17.633 ms 4096 bytes from 192.168.199.124: icmp_seq=9 ttl=64 time=16.374 ms --- 192.168.199.124 ping statistics --- 10 packets transmitted, 9 packets received, 10.0% packet loss round-trip min/avg/max/stddev = 16.374/90.929/144.988/44.715 ms	XinyuYun:~ duoduo$ ping -c 10 -s 4088 192.168.199.230 PING 192.168.199.230 (192.168.199.230): 4088 data bytes 4096 bytes from 192.168.199.230: icmp_seq=0 ttl=64 time=39.014 ms 4096 bytes from 192.168.199.230: icmp_seq=1 ttl=64 time=73.599 ms 4096 bytes from 192.168.199.230: icmp_seq=2 ttl=64 time=74.466 ms 4096 bytes from 192.168.199.230: icmp_seq=3 ttl=64 time=117.918 ms 4096 bytes from 192.168.199.230: icmp_seq=4 ttl=64 time=318.892 ms 4096 bytes from 192.168.199.230: icmp_seq=5 ttl=64 time=55.151 ms 4096 bytes from 192.168.199.230: icmp_seq=6 ttl=64 time=64.661 ms 4096 bytes from 192.168.199.230: icmp_seq=7 ttl=64 time=81.857 ms 4096 bytes from 192.168.199.230: icmp_seq=8 ttl=64 time=101.559 ms 4096 bytes from 192.168.199.230: icmp_seq=9 ttl=64 time=316.761 ms --- 192.168.199.230 ping statistics --- 10 packets transmitted, 10 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 39.014/124.388/318.892/98.961 ms

Per to my test result in LAN, when the package sizes are similar, like 64 or 256 bytes, the RTT will depend on the network situation; if the package is extremely bigger, like 64 bytes vs 4096 bytes, the message with bigger package will take longer time.

2- two nodes on a WAN (for instance, your workstation and a host in East Asia)

Here I select a website (www.yhd.cn) in China and UWO library host (www.lib.uwo.ca) in public Internet:

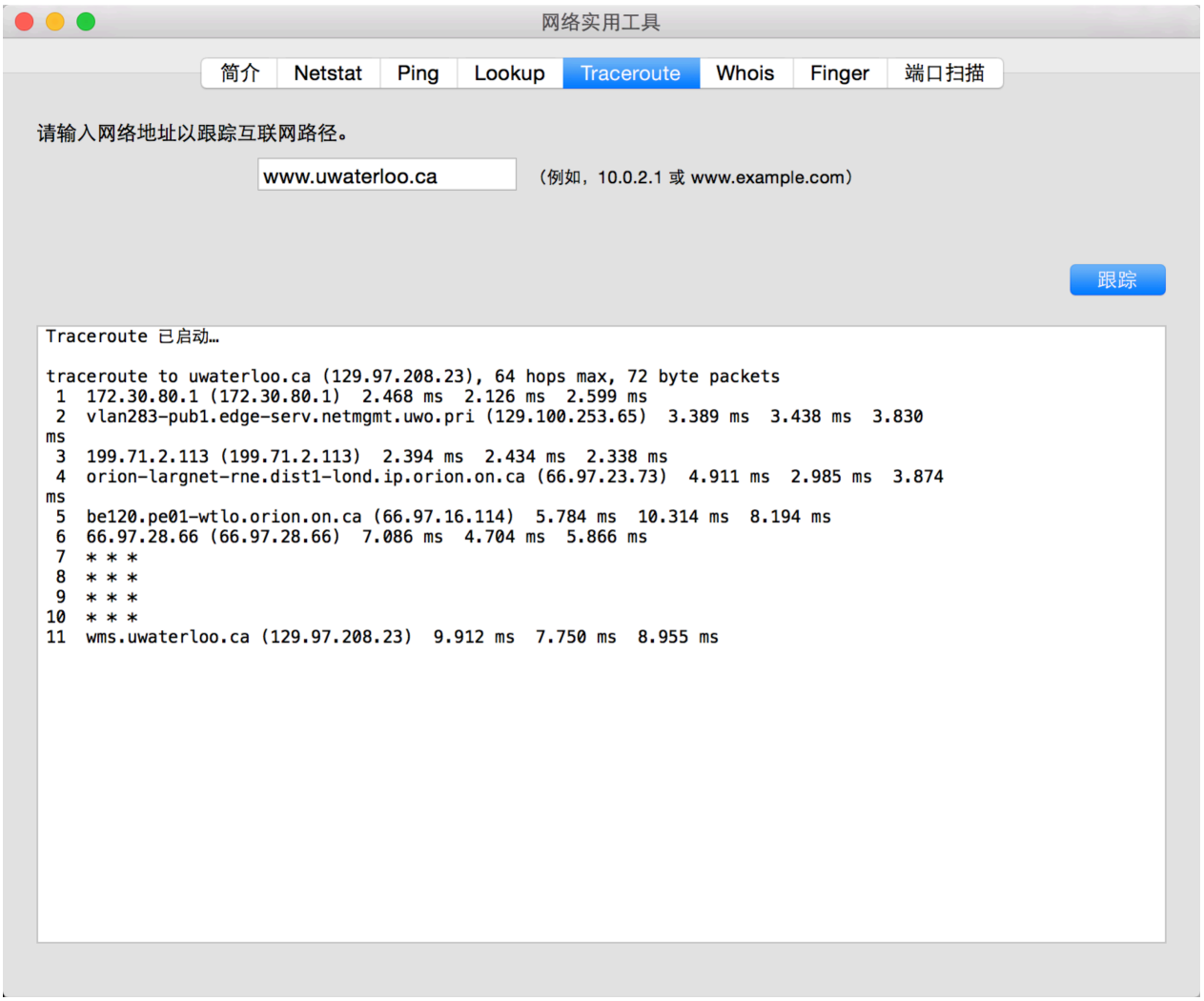


As analyzing my test results above, in WAN for same host the package size seems not affect the RTT so much, however in WAN the host distance will have a big influence, that RTT to ping the host in China takes obviously long time than that to ping UWO library.

c. Use the tracert utility on your lab workstation to find the route to a host:

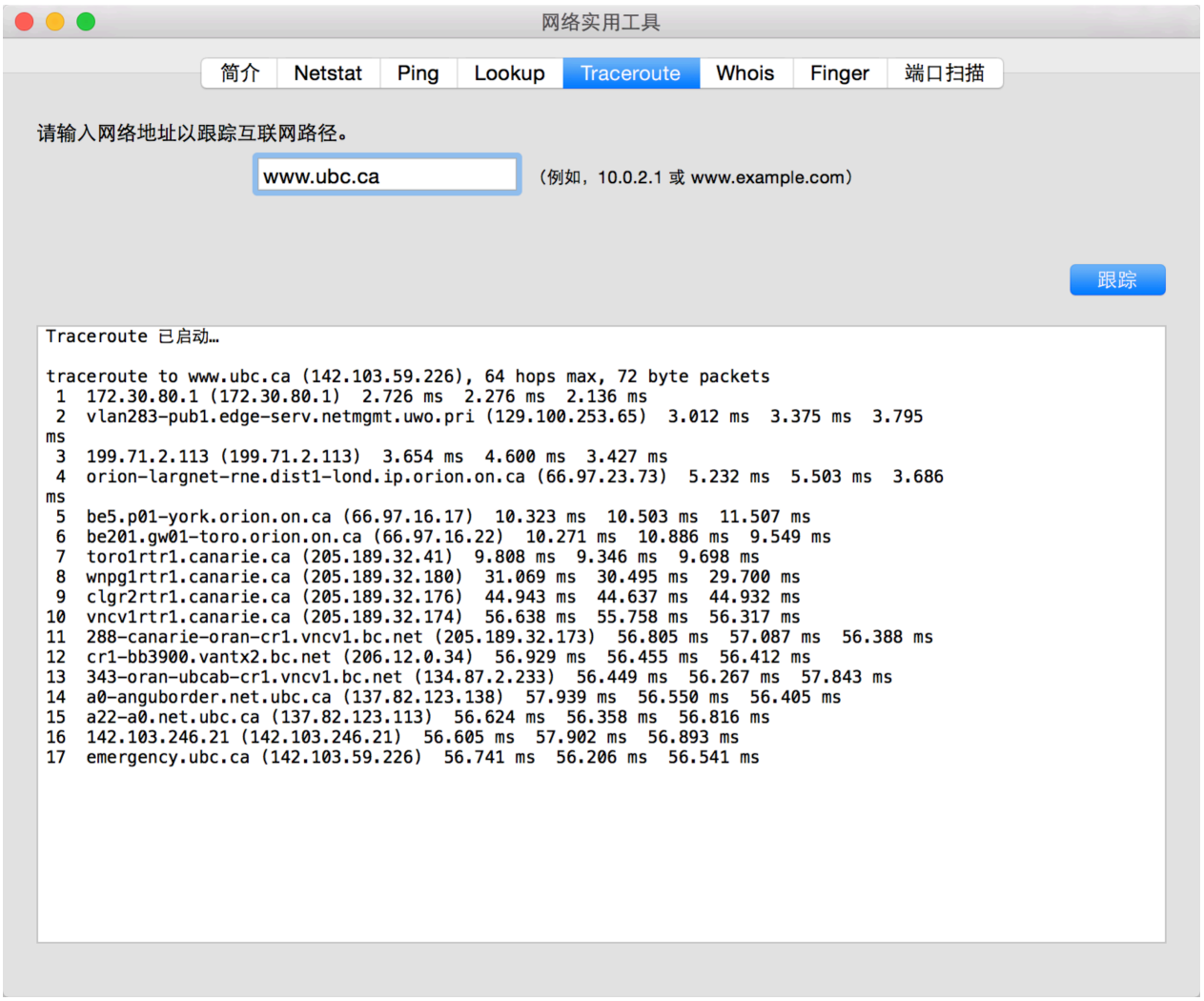
1- in another city in Ontario (3)

Here I chose ‘uwaterloo.ca’ as the destination, as the result shown bellowed, it took 11 hops to the destination host, which past through 4 ISPs. The “***” means the accordant server where 3 test message packages sent did not response in default response time.



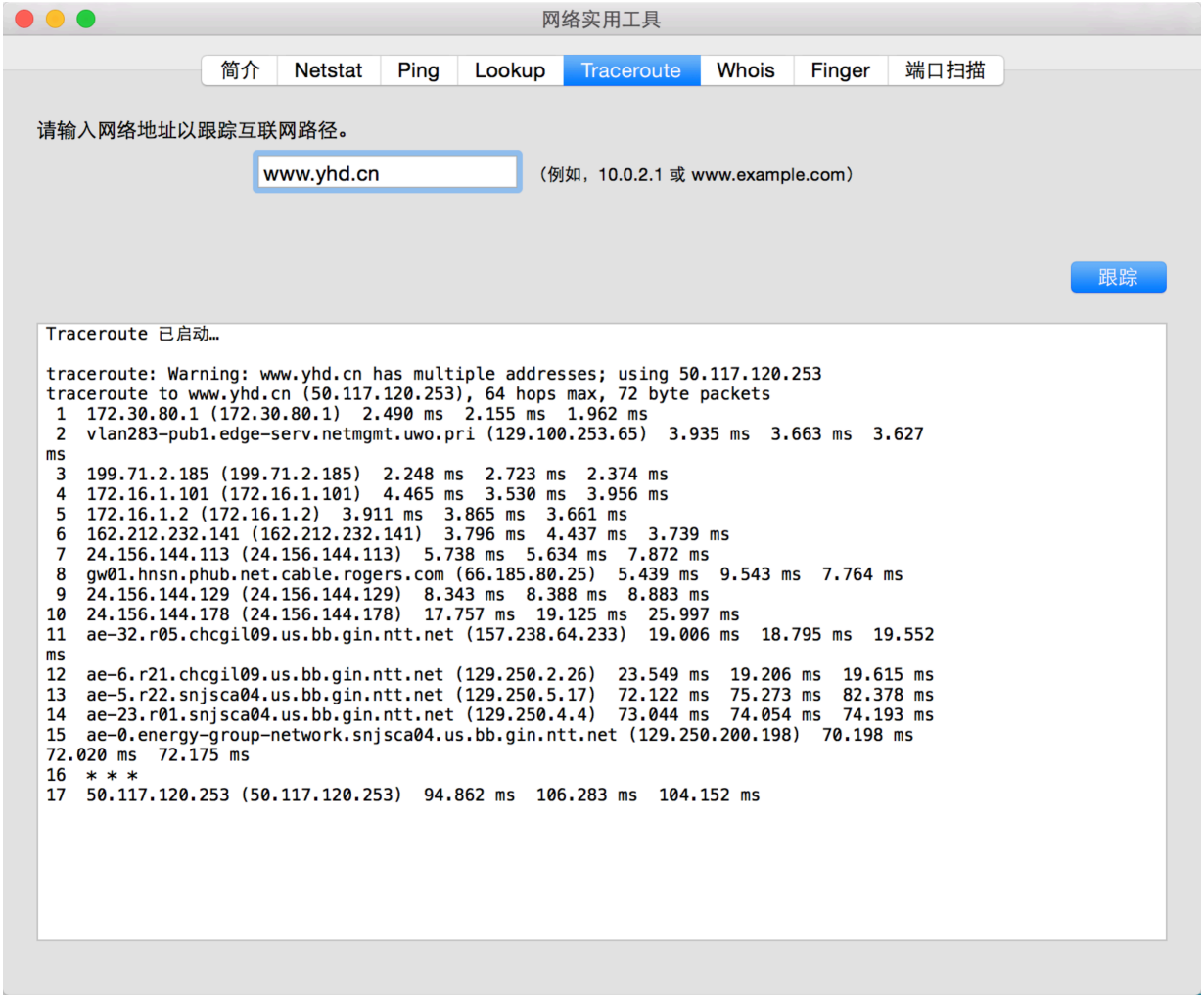
2- on the east or west coast of Canada (3)

Here I sent the traceroute to UBC that is located in west coast of Canada, it took 17 hops to the destination host, in which 14 ISPs got involved ranging from providers in ON and BC.



3- outside Canada (3)

Here I chose a shopping website (www.yhd.cn) in China, as showed bellowed, it took 17 hops and 7 ISPs were past from Canada, US. The “***” means the accordant server where 3 test message packages sent did not response in default response time.



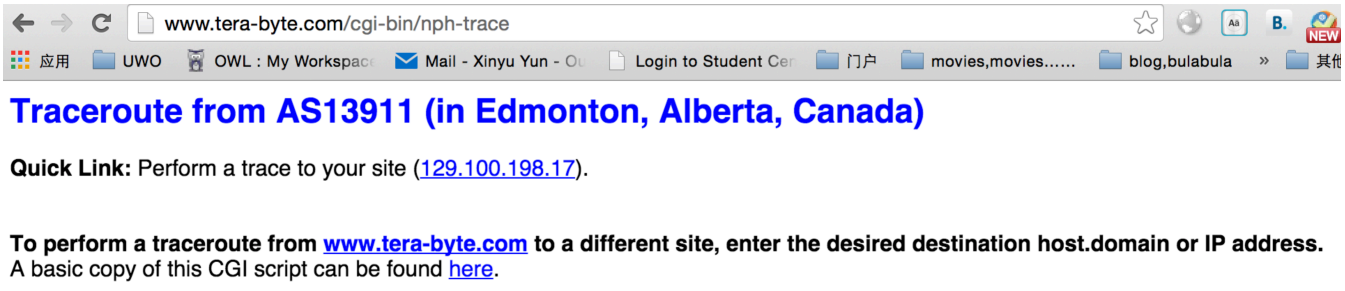
Analyze your results.

(e.g. How many hops did it take to reach the destination host? (3) How many ISPs did you traverse? Why do you see “* * *” (3) on some of the output lines?)

d. Use the trace route utilities at the site www.traceroute.org to find the routes between two hosts on different continents. Trace the route again between these two hosts after at least an hour. Provide reasons why the two routes could differ.

Answer:

Here I chose the tera-byte located in Alberta to test the traceroute, the destination host is ‘www.yhd.cn’ which is located in China.



1st Test

Traceroute Output

FROM www.tera-byte.com TO www.yhd.cn

```
traceroute: Warning: www.yhd.cn has multiple addresses; using 50.117.120.253
traceroute to www.yhd.cn (50.117.120.253) from 216.234.191.172, 30 hops max, 40 byte packets
 1  cat6509-vlan2.edm.tera-byte.com (216.234.161.1)  0.385 ms
 2  *
 3  tcore3-edmonton_bel.net.bell.ca (64.230.119.232)  22.194 ms
 4  tcore4-vancouver_tengige0-15-0-5.net.bell.ca (64.230.77.109)  20.291 ms
 5  tcore3-seattle_hundredgige0-9-0-0.net.bell.ca (64.230.79.96)  18.824 ms
 6  bx4-seattle_ae2.net.bell.ca (64.230.125.231)  18.056 ms
 7  *
 8  ae-7.r20.sttlwa01.us.bb.gin.ntt.net (129.250.5.46)  63.274 ms
 9  ae-3.r23.snjsca04.us.bb.gin.ntt.net (129.250.3.124)  63.376 ms
10  ae-41.r01.snjsca04.us.bb.gin.ntt.net (129.250.4.24)  68.526 ms
11  ae-0.energy-group-network.snjsca04.us.bb.gin.ntt.net (129.250.200.198)  53.154 ms
12  *
13  50.117.120.253 (50.117.120.253)  53.791 ms
```

2nd Test

Traceroute Output

FROM www.tera-byte.com TO www.yhd.cn

```
traceroute: Warning: www.yhd.cn has multiple addresses; using 50.117.116.117
traceroute to www.yhd.cn (50.117.116.117) from 216.234.191.172, 30 hops max, 40 byte packets
 1  cat6509-vlan2.edm.tera-byte.com (216.234.161.1)  0.481 ms
 2  *
 3  tcore3-edmonton_bel.net.bell.ca (64.230.119.232)  25.381 ms
 4  tcore4-vancouver_tengige0-15-0-5.net.bell.ca (64.230.77.109)  20.147 ms
 5  tcore4-seattle_hundredgige0-5-0-0.net.bell.ca (64.230.79.94)  20.051 ms
 6  bx4-seattle_ae3.net.bell.ca (64.230.125.233)  18.050 ms
 7  *
 8  ae-7.r20.sttlwa01.us.bb.gin.ntt.net (129.250.5.46)  63.279 ms
 9  ae-3.r23.snjsca04.us.bb.gin.ntt.net (129.250.3.124)  61.460 ms
10  ae-41.r01.snjsca04.us.bb.gin.ntt.net (129.250.4.24)  68.507 ms
11  ae-0.energy-group-network.snjsca04.us.bb.gin.ntt.net (129.250.200.198)  53.291 ms
12  *
13  50.117.116.117 (50.117.116.117)  54.037 ms !Z
```

As showed above, the fifth hop used different host in the traceroute.

e. Briefly discuss why ping would not necessarily provide an accurate estimate of the round trip time for packets exchanged by two hosts on the Internet?

Answer:

Ping is one of the most frequently used tools in networking. It uses the ICMP [2] echo request message to send one PDU to a target host. The receiving host returns the PDU in an echo reply message as fast as possible to the sending host. The host can then compare its transmission time with the arrival time of the reply to estimate the round trip time, RTT [<Accuracy Evaluation of Ping and J-OWAMP>].

As we tested in previous lab, every time the request to destination may pass through the different route, the router will calculate different routes due to the load balance. So the delay time will be not same in each route.

f. Another useful tool/utility that is helpful in network performance monitoring is netstat. What information does it provide? List at least three other such utilities and briefly describe their use.

Answer:

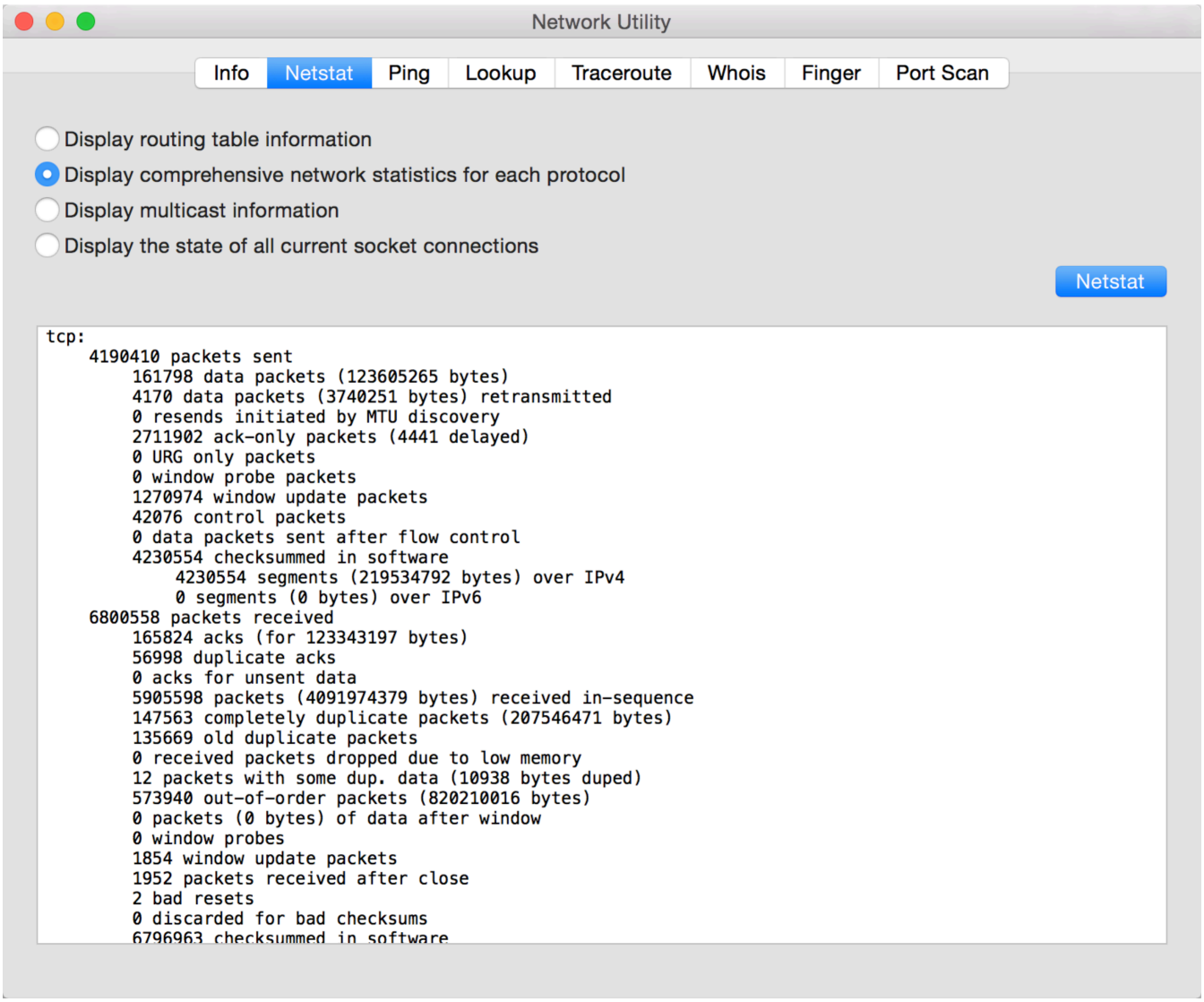
The 'netstat' stands for network statistics. This command displays incoming and outgoing network connections as well as other network information.

As I tested using tool in my MacBook, the information is provided by 'netstat':

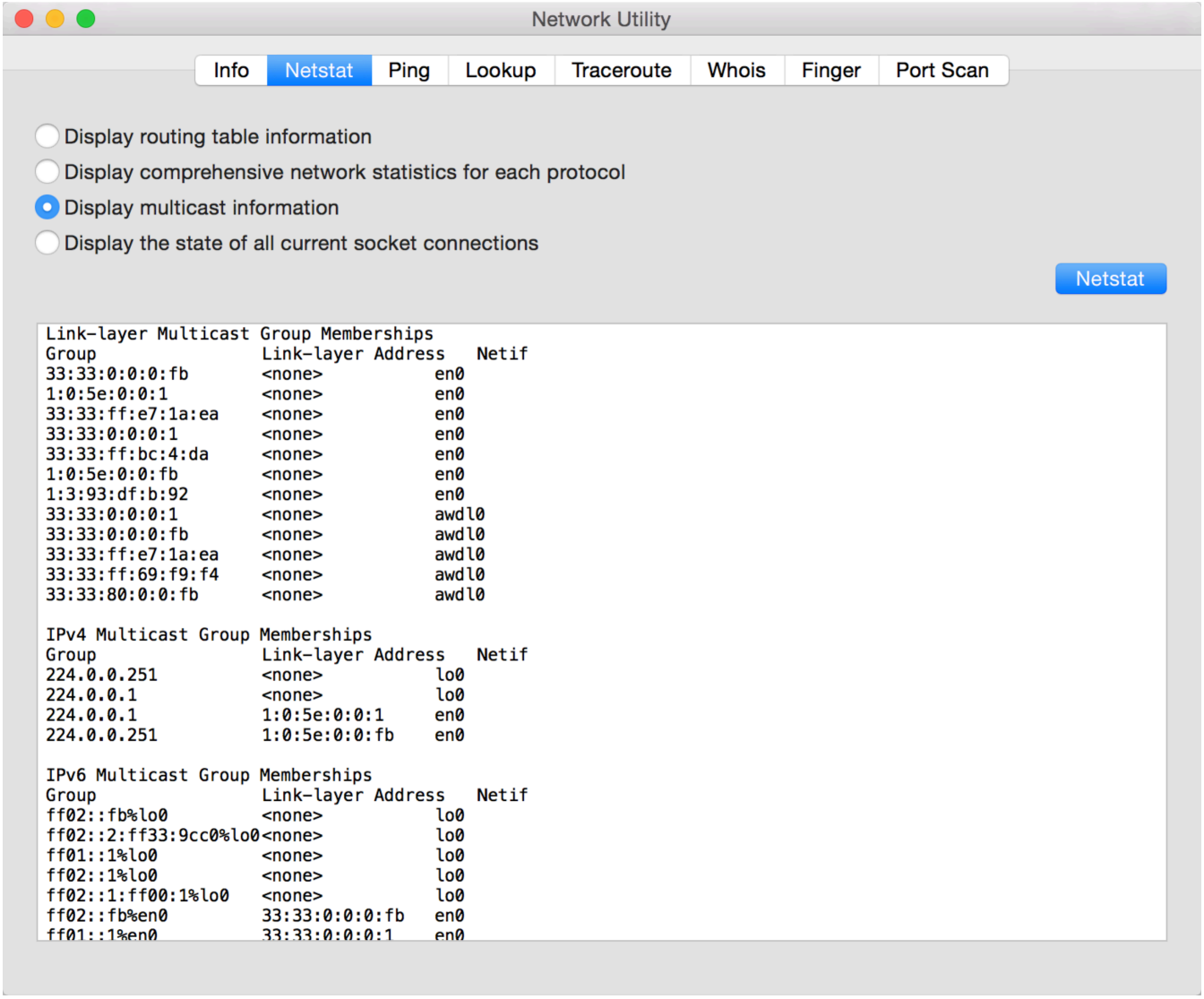
1. Display routing tables in both IPV4 and IPV6 with destination, gateway, flags, referred times, used times.

Netstat

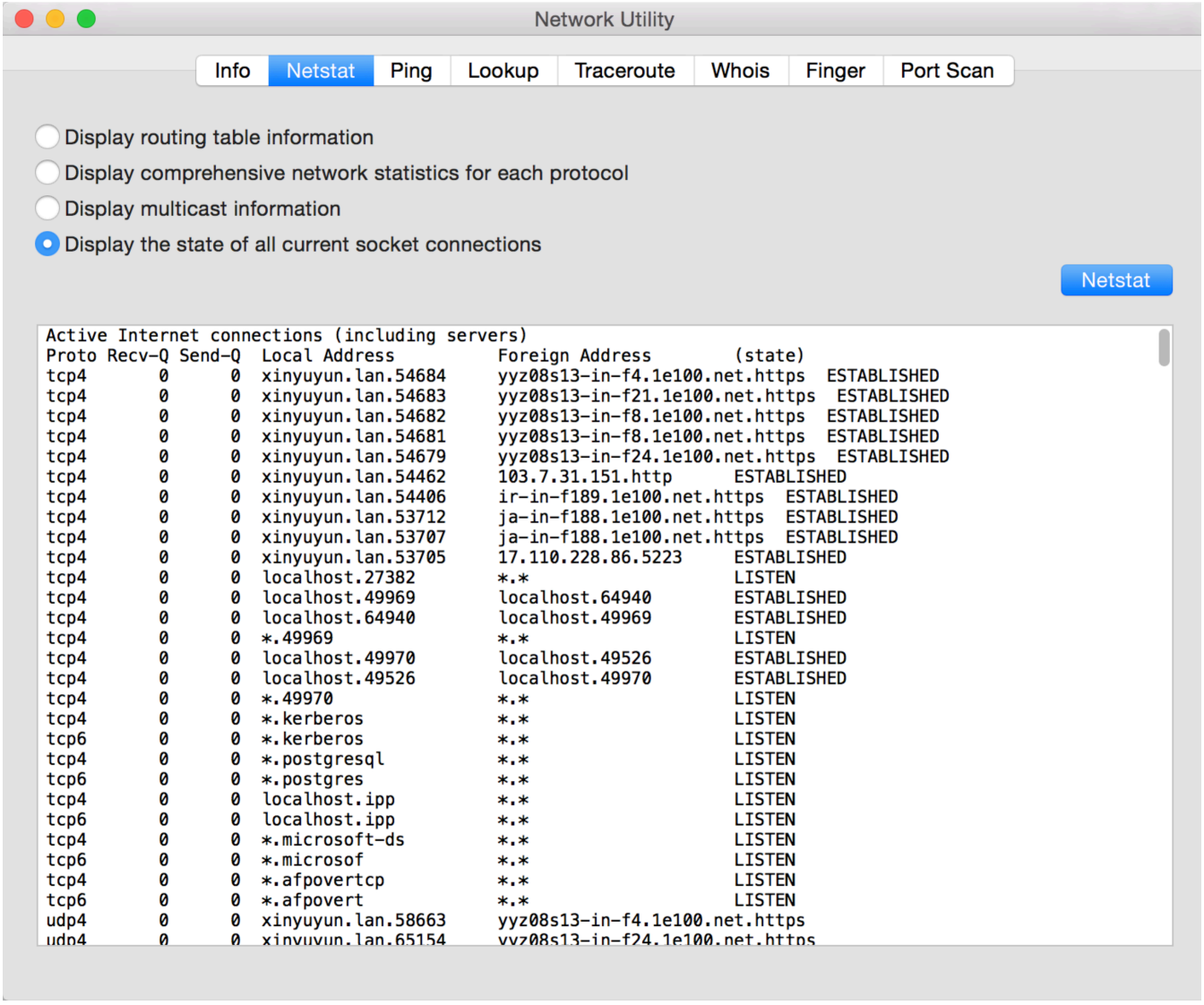
```
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            172.30.80.1        UGSc           24        0     en0
127                localhost          UCS             0        0     lo0
localhost          localhost          UH              8     4485     lo0
169.254            link#4             UCS             0        0     en0
172.30.80/21       link#4             UCS             0        0     en0
172.30.80.1/32     link#4             UCS             2        0     en0
172.30.80.1        0:a:f7:f:9a:2c     UHLWIir        26      305     en0   1159
172.30.86.180/32   link#4             UCS             0        0     en0

Internet6:
Destination        Gateway            Flags         Netif Expire
localhost          localhost          UHL             lo0
fe80::%lo0         fe80::1%lo0        UcI             lo0
fe80::1%lo0        link#1             UHLI            lo0
fe80::%en0         link#4             UCI             en0
xinyuyun.local     78:31:c1:bc:4:da   UHLI            lo0
fe80::%awdl0       link#8             UCI           awdl0
xinyuyun.local     76:ee:17:69:f9:f4  UHLI            lo0
ff01::%lo0         localhost          UmCI            lo0
ff01::%en0         link#4             UmCI            en0
ff01::%awdl0       link#8             UmCI          awdl0
ff02::%lo0         localhost          UmCI            lo0
ff02::%en0         link#4             UmCI            en0
ff02::%awdl0       link#8             UmCI          awdl0
```



3. display multicast information



4. display the state of all current socket connections with protocol, local address, foreign address and state



Other tools/utilities which are similar to netstat:

1) In linux, the 'ss' command is capable of showing more information than the netstat and is faster. (http://www.binarytides.com/linux-ss-command/)

1. List all connections

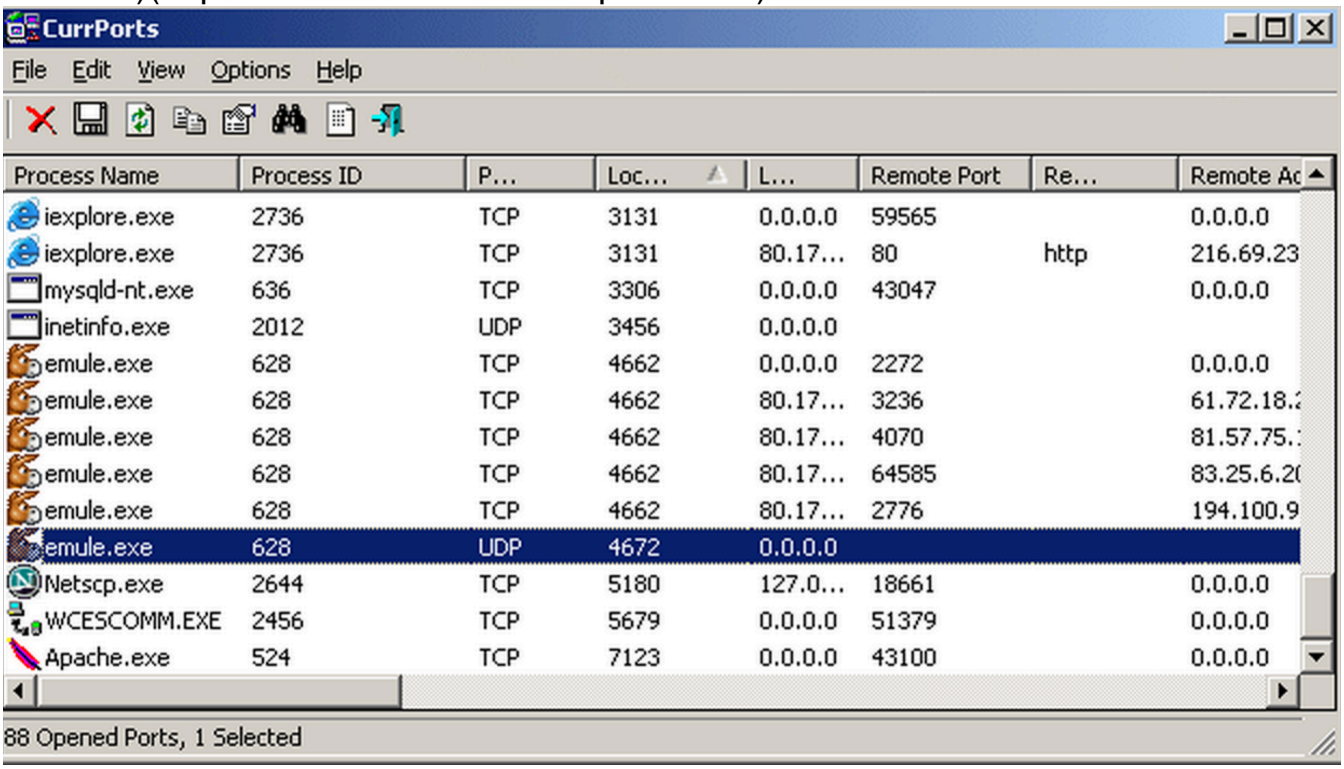
The simplest command is to list out all connections.

```
$ ss | less
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
u_str  ESTAB      0      0                    * 15545                  * 15544
u_str  ESTAB      0      0                    * 12240                  * 12241
u_str  ESTAB      0      0      @/tmp/dbus-2hQdRvvg49 12726                  * 12159
u_str  ESTAB      0      0                    * 11808                  * 11256
u_str  ESTAB      0      0                    * 15204                  * 15205
.....
```

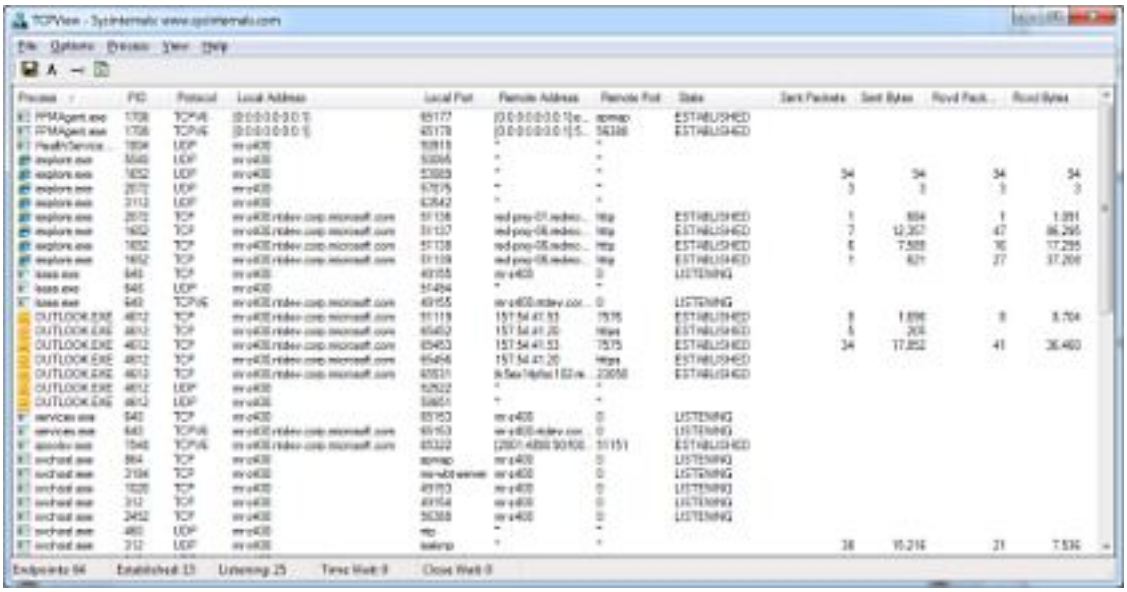
information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file , XML file, or to tab-delimited text file.

CurrPorts also automatically mark with pink color suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons)(http://www.nirsoft.net/utils/cports.html)



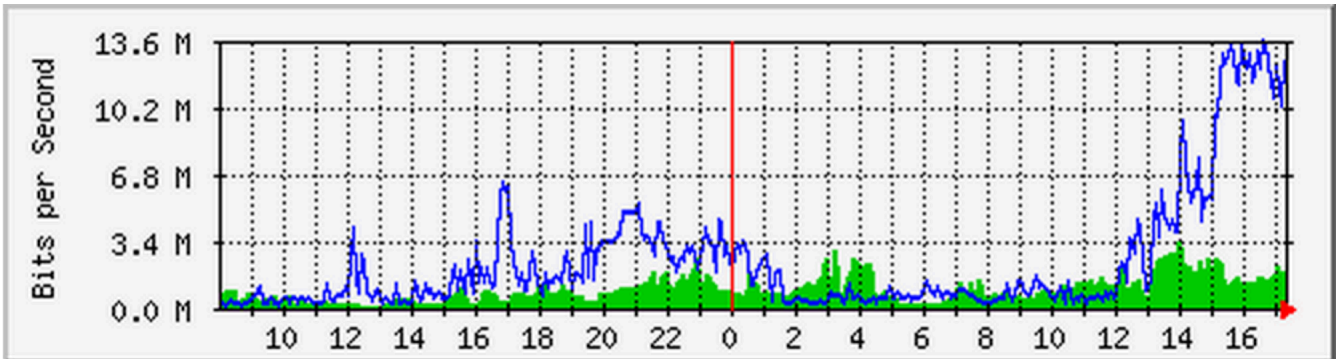
3) TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.
(https://technet.microsoft.com/en-us/sysinternals/bb897437.aspx)



g. Briefly describe the Multi Router Traffic Grapher (MRTG) tool and its use in network traffic analysis. How is this tool being used by ITS at UWO?

Answer:

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic. It is used to monitor SNMP network devices and draw pictures showing how much traffic has passed through each interface.



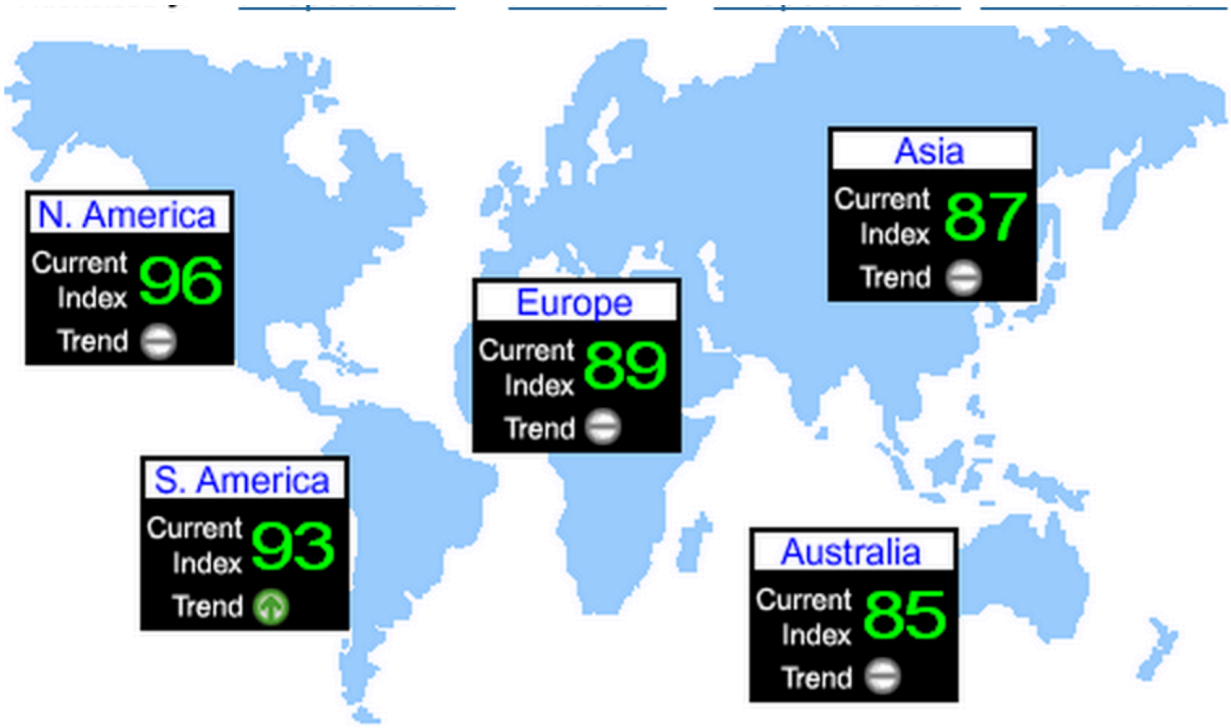
In UWO, the ITS can monitor the network usage during the rush hour, track and summarize the performance of routers in UWO.

h. What is an “Internet traffic report”? What types of data are gathered by Internet sites that provide these reports? (

Answer:

The Internet Traffic Report monitors the flow of data around the world. It then displays a value between zero and 100. Higher values indicate faster and more reliable connections.

Generally, the report shows the global values in each area with index value, average response time and average packet loss % ranging from last 24 hours to last 30 days:

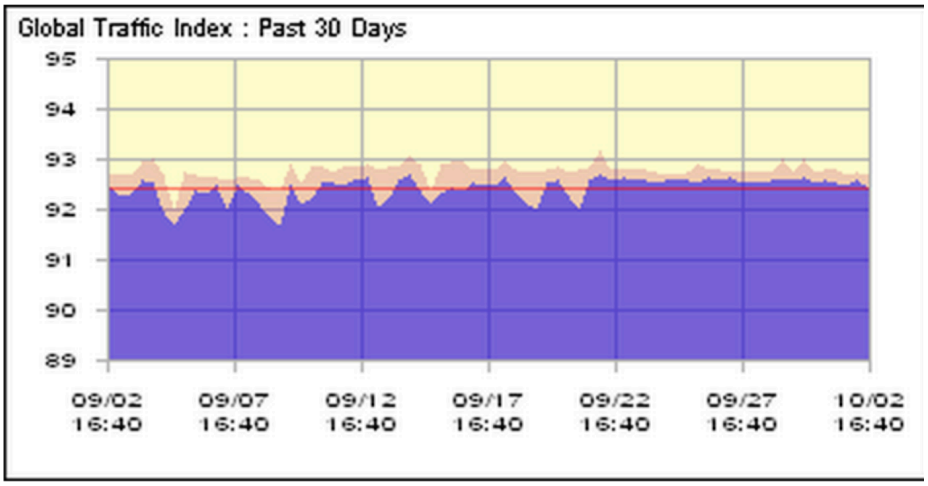


View Graphs or **Click a region to view more detailed information.**

Region	Current Index	Avg. Response Time (ms)	Avg. Packet Loss (%)
Asia	87	123	0 %
Australia	85	140	0 %
Europe	89	106	0 %
North America	96	37	0 %
South America	93	65	0 %

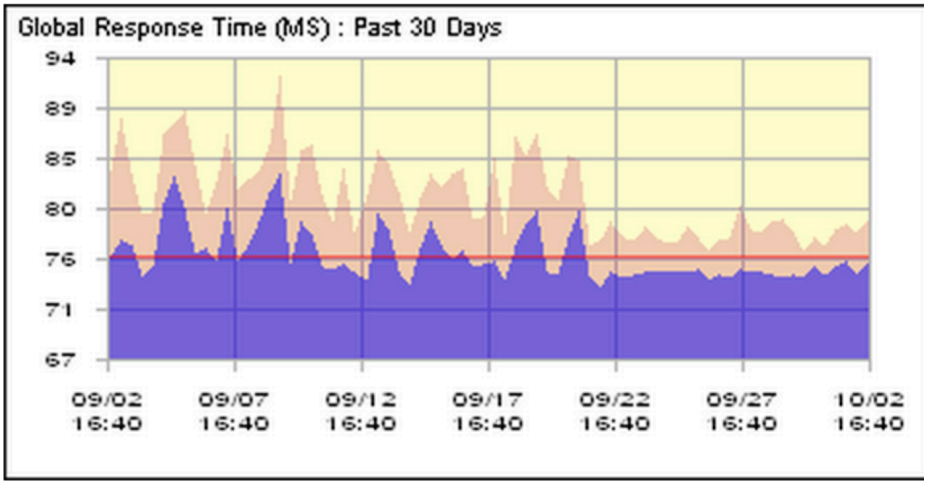
This graph shows the **Global Traffic Index** for the past 30 days.
View 24-hour graph
View 7-day graph
View 30-day graph

Red indicates the maximum
Purple indicates the average



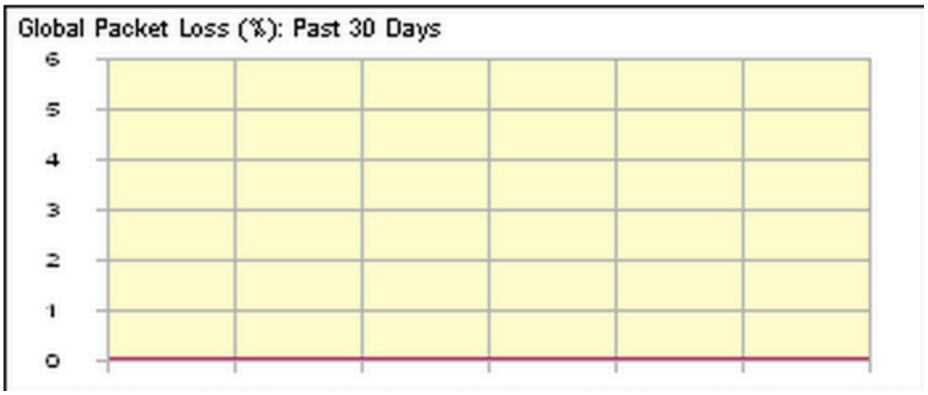
This graph shows the **Global Response Time** for the past 30 days.
View 24-hour graph
View 7-day graph
View 30-day graph

Red indicates the maximum
Purple indicates the average

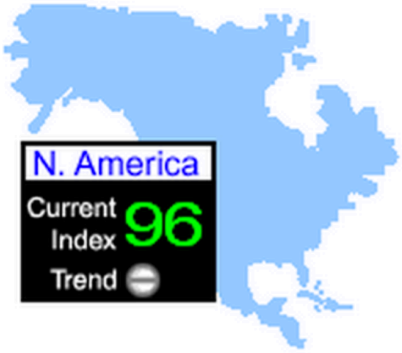


This graph shows the **Global Packet Loss** for the past 30 days.
View 24-hour graph
View 7-day graph
View 30-day graph

Red indicates the



When clicking the specific area, you will see the routers' details in this area with host name, location, index value, average response time and average packet loss %, also you can search the last 24 hours and click each host to check details.



North America

Avg. Response Time: 35
Avg. Packet Loss: 0 %
Total Routers: 37
Network up: 70 %

View Graphs or **Click a Router below for more detail.**

Router	Location	Current Index	Response Time (ms)	Packet Loss (%)
anhm7204.exo.com	California (Anaheim)	0	0	100
mc-gateway.lansmart.com	California (Fresno)	95	40	0
dnsauth1.sys.gtei.net	California (Los Angeles)	99	10	0
rx0ar-technicare.ed.bigpipeinc.com	Canada (Edmonton)	92	79	0
gw02.wlfdle.phub.net.cable.rogers.com	Canada (Ontario)	100	0	0