*Benjamin Rayner & Eduardo Sanchez*

*ECE 358 – Lab 3*

Encapsulation and Network Utilities

Table of Contents

[Protocol Header Analysis 1](#_Toc120307023)

[Network Utilities 4](#_Toc120307024)

# Protocol Header Analysis

**Student ID: 20837049 – Frame 9**

0000 00 22 19 f4 30 97 00 15 60 f8 c6 00 08 00 45 00

0010 00 5c 7f 33 00 00 7f 11 82 c8 81 61 0b 2c 81 61

0020 2b a7 fd 1a 13 8d 00 48 cb f0 80 c8 00 06 c2 0f

0030 1b bd d4 ed 0f b3 31 e8 d5 41 58 a4 78 8c 00 00

0040 6b 70 02 2d 55 00 81 ca 00 08 c2 0f 1b bd 01 0c

0050 31 32 39 2e 39 37 2e 31 31 2e 34 34 06 0a 76 6c

0060 63 20 31 2e 31 2e 31 31 00 00

Ethernet Header:

00 22 19 f4 30 97: Ethernet destination address is 00 22 19 f4 30 97 (unicast).

00 15 60 f8 c6 00: Ethernet source address is 00 15 60 f8 c6 00 (unicast).

08 00: The payload type is IP (0x0800).

IP Header:

**4**5: This is an IP version 4 datagram.

4**5**: The header length is 5x4 = 20 bytes. (No options field)

00:

(**0** **0** **0** 0 0 0 0 0 in binary): The datagram has lowest routine precedence.

(0 0 0 **0** **0** **0** 0 0 in binary): The 3 types of service (ToS) bits.

**0** 0 0 *Normal Delay*

0 **0** 0 *Normal Throughput*

0 0 **0** *Normal Reliability*

(0 0 0 0 0 0 **0** **0** in binary): The last two bits must be zero (for future use).

00 5c: The total length of the IP datagram is 92 (0x005c) bytes.

7f 33: The identification of this datagram is 0x7f33 (for fragmentation).

00 00:

(0 **0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 in binary): Don’t fragment flag unset.

(0 0 **0** 0 0 0 0 0 0 0 0 0 0 0 0 0 in binary): More fragment flag unset.

(0 0 0 **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** in binary): Fragment offset is 0.

This means that the datagram can be fragmented, and that this is the last fragment. When reassembled, place at index 0. (Only 1 fragment)

7f: Time to live = 127 (0x7f), meaning that datagram can exist for at most 127 more hops.

11: The Protocol on top is UDP (0x11).

82 c8: This is the checksum of the datagram.

81 61 0b 2c: Source IP address is 129.97.11.44.

81 61 2b a7: Destination IP address is 128.97.43.167.

UDP Header:

fd 1a: The source port is 64794 which is a dynamic port arbitrarily assigned by the operating system.

13 8d: The destination port is 5005 which is a registered port chosen for a particular application on a server.

00 48: Length of whole UDP segment (header + data) is 72 bytes.

cb f0: Checksum of the whole UDP segment.

Upper Layers:

Rest of bits include upper layer headers and upper layer data.

Overall comment on given frame: Frame 9 contained a UDP message with data and is sent to a server on port 5005.

**Student ID: 20837049 – Frame 19**

0000 00 1d 7e 46 ec 49 00 22 19 f4 30 97 08 00 45 00

0010 00 50 d1 f3 40 00 40 06 19 f7 c0 a8 01 88 81 61

0020 0b 2c 81 c1 1f 90 09 57 5a 25 3c 33 18 cb f0 10

0030 1d 85 4f 00 00 00 01 01 08 0a 00 00 97 6b 21 44

0040 66 86 01 01 05 1a 3c 35 f2 7b 3c 35 f8 23 3c 39

0050 75 cb 3c 39 7b 73 3c 39 d5 f3 3c 39 db 9b

Ethernet Header:

00 1d 7e 46 ec 49: Ethernet destination address is 00 1d 7e 46 ec 49 (unicast).

00 22 19 f4 30 97: Ethernet source address is 00 22 19 f4 30 97 (unicast).

08 00: The payload type is IP (0x0800).

IP Header:

**4**5: This is an IP version 4 datagram.

4**5**: The header length is 5x4 = 20 bytes. (No options field)

00:

(**0** **0** **0** 0 0 0 0 0 in binary): The datagram has lowest routine precedence.

(0 0 0 **0** **0** **0** 0 0 in binary): The 3 types of service (ToS) bits.

**0** 0 0 *Normal Delay*

0 **0** 0 *Normal Throughput*

0 0 **0** *Normal Reliability*

(0 0 0 0 0 0 **0** **0** in binary): The last two bits must be zero (for future use).

00 50: The total length of the IP datagram is 80 (0x0050) bytes.

d1 f3: The identification of this datagram is 0xd1f3 (for fragmentation).

40 00:

(0 **1** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 in binary): Don’t fragment flag set.

(0 0 **0** 0 0 0 0 0 0 0 0 0 0 0 0 0 in binary): More fragment flag unset.

(0 0 0 **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** **0** in binary): Fragment offset is 0.

This means that the datagram can’t be fragmented, and that there are no fragments after this datagram. With a fragment offset equals to zero, we know that this is the only fragment of the datagram.

40: Time to live = 64 (0x40), meaning that datagram can exist for at most 64 more hops.

06: The Protocol on top is TCP (0x06).

19 f7: This is the checksum of the datagram.

c0 a8 01 88: Source IP address 192.168.1.136.

81 61 0b 2c: Destination IP address is 129.97.11.44.

TCP Header:

81 c1: The source port is 33217 which is a registered port chosen for a particular application on a server.

1f 90: The destination port is 8080 which is often used for HTTP web traffic.

09 57 5a 25: The Seq. no is 156719653.

3c 33 18 cb: The Ack. no is 1009981643.

**f**0: Data offset is 60 (15 x 4) bytes. This is the length of the TCP header.

10:

(0 0 **0** **1** **0** **0** **0** **0** in binary): The 6 different TCP flags.

**0** 1 0 0 0 0 *URG = 0*

0 **1** 0 0 0 0 *ACK = 1*

0 1 **0** 0 0 0 *PSH = 0*

0 1 0 **0** 0 0 *RST = 0*

0 1 0 0 **0** 0 *SYN = 0*

0 1 0 0 0 **0** *FIN = 0*

Only ACK flag is set, meaning that the value carried in the acknowledgement field is valid.

1d 85: The receiver window size is 7557 (0x1d85) bytes.

4f 00: Checksum for the whole TCP segement.

00 00: Urgent pointer (Not used in this segment)

01 01 .. db 9b: Rest of the TCP header are options.

Upper Layers:

No upper layers present (no data).

Overall comment on given frame: Frame 19 contained a pure TCP ACK (no data) to port 8080. This is most likely an ACK to setup an HTTP connection.

# Network Utilities

2. a)

**Arp** manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries

to the table, delete one or display the current content.

**ARP** stands for Address Resolution Protocol, which is used to find the media access control

address of a network neighbour for a given IPv4 Address.

b)

emrglinux6.eng.uwaterloo.ca (129.97.92.125) at f8:bc:12:33:3b:48 [ether] on enp0s31f6

emsolserv4.eng.uwaterloo.ca (129.97.92.73) at 3c:ec:ef:3f:b8:8a [ether] on enp0s31f6

ecekvm0.uwaterloo.ca (129.97.92.95) at ec:f4:bb:e2:4e:c0 [ether] on enp0s31f6

ecetesla4.uwaterloo.ca (129.97.92.171) at b4:96:91:8e:a5:7d [ether] on enp0s31f6

eceserv2.uwaterloo.ca (129.97.92.161) at 00:25:90:5d:b6:2d [ether] on enp0s31f6

ecesyslog2.uwaterloo.ca (129.97.92.183) at b4:96:91:6a:e7:fc [ether] on enp0s31f6

eceubuntu2.eng.uwaterloo.ca (129.97.92.76) at 90:b1:1c:29:84:87 [ether] on enp0s31f6

ecelinux1.eng.uwaterloo.ca (129.97.92.199) at 00:25:90:6b:bb:9c [ether] on enp0s31f6

eceterm1.uwaterloo.ca (129.97.92.174) at 52:54:00:d3:13:ce [ether] on enp0s31f6

emrglinux4.eng.uwaterloo.ca (129.97.92.41) at 18:03:73:fb:21:93 [ether] on enp0s31f6

eceterm3.uwaterloo.ca (129.97.92.176) at a8:5e:45:51:f2:bd [ether] on enp0s31f6

iccad1.uwaterloo.ca (129.97.92.11) at b8:2a:72:ce:1d:78 [ether] on enp0s31f6

v92-e2-rt-1782a.nsx.uwaterloo.ca (129.97.92.1) at cc:98:91:6c:3a:c2 [ether] on enp0s31f6

ececmc.uwaterloo.ca (129.97.92.146) at ec:0d:9a:3a:d6:62 [ether] on enp0s31f6

ece252-2.uwaterloo.ca (129.97.92.121) at 52:54:00:1b:fe:a1 [ether] on enp0s31f6

bbcr-winserv.eng.uwaterloo.ca (129.97.92.202) at 80:18:44:ef:38:0e [ether] on enp0s31f6

maslab-hps2.uwaterloo.ca (129.97.92.69) at 18:c0:4d:77:5e:6f [ether] on enp0s31f6

? (169.254.169.254) at <incomplete> on enp0s31f6

nsercapps.uwaterloo.ca (129.97.92.179) at 52:54:00:a6:1d:e3 [ether] on enp0s31f6

ciuw2.uwaterloo.ca (129.97.92.4) at 00:30:48:ff:8e:2e [ether] on enp0s31f6

rfdesign5.uwaterloo.ca (129.97.92.47) at 08:94:ef:2f:48:46 [ether] on enp0s31f6

ecetesla2.uwaterloo.ca (129.97.92.170) at b4:96:91:8e:a4:ed [ether] on enp0s31f6

eceserv1.uwaterloo.ca (129.97.92.160) at ec:0d:9a:3a:cd:12 [ether] on enp0s31f6

cadconnect\_r20.eng.uwaterloo.ca (129.97.92.59) at 00:0c:29:27:08:f0 [ether] on enp0s31f6

cdrserver.eng.uwaterloo.ca (129.97.92.49) at ac:1f:6b:62:17:31 [ether] on enp0s31f6

eceweb-new.uwaterloo.ca (129.97.92.130) at 52:54:00:2e:10:81 [ether] on enp0s31f6

ecelinux4.eng.uwaterloo.ca (129.97.92.198) at <incomplete> on enp0s31f6

ferrero.uwaterloo.ca (129.97.92.52) at 00:25:90:a3:f1:8c [ether] on enp0s31f6

winserv1.uwaterloo.ca (129.97.92.10) at 00:30:48:c3:00:ca [ether] on enp0s31f6

ecebackup1.eng.uwaterloo.ca (129.97.92.143) at 00:0e:1e:87:ba:f0 [ether] on enp0s31f6

deepgpu3.eng.uwaterloo.ca (129.97.92.22) at a0:42:3f:39:b4:30 [ether] on enp0s31f6

ecelinux2.eng.uwaterloo.ca (129.97.92.145) at b8:2a:72:da:e9:90 [ether] on enp0s31f6

ece252-1.uwaterloo.ca (129.97.92.120) at 52:54:00:15:46:0a [ether] on enp0s31f6

emsolserv5.eng.uwaterloo.ca (129.97.92.78) at 3c:ec:ef:3f:b7:b4 [ether] on enp0s31f6

ecelinux3.eng.uwaterloo.ca (129.97.92.201) at 00:25:90:6b:bb:34 [ether] on enp0s31f6

maslab-hps1.uwaterloo.ca (129.97.92.68) at 18:c0:4d:47:10:50 [ether] on enp0s31f6

cst.uwaterloo.ca (129.97.92.43) at 90:e6:ba:1e:c1:5d [ether] on enp0s31f6

eceubuntu4.uwaterloo.ca (129.97.92.188) at 30:5a:3a:83:93:e3 [ether] on enp0s31f6

banff.eng.uwaterloo.ca (129.97.92.136) at ac:1f:6b:46:c6:14 [ether] on enp0s31f6

iccad3.uwaterloo.ca (129.97.92.13) at b0:83:fe:cb:66:53 [ether] on enp0s31f6

manta.uwaterloo.ca (129.97.92.158) at 38:ea:a7:8d:42:e8 [ether] on enp0s31f6

deepfind.eng.uwaterloo.ca (129.97.92.111) at 00:02:c9:4f:a5:6c [ether] on enp0s31f6

vision-pc32.eng.uwaterloo.ca (129.97.92.194) at 18:c0:4d:85:37:4d [ether] on enp0s31f6

vlsisrv2.uwaterloo.ca (129.97.92.93) at 00:25:90:4b:1f:ae [ether] on enp0s31f6

ecetesla1.uwaterloo.ca (129.97.92.169) at b4:96:91:8e:a6:15 [ether] on enp0s31f6

cycloud2.eng.uwaterloo.ca (129.97.92.129) at 50:eb:f6:1f:ce:a2 [ether] on enp0s31f6

ivc2.uwaterloo.ca (129.97.92.151) at 44:a8:42:26:37:48 [ether] on enp0s31f6

jrl-server.eng.uwaterloo.ca (129.97.92.126) at ac:1f:6b:62:17:3a [ether] on enp0s31f6

iccad.uwaterloo.ca.eng.uwaterloo.ca (129.97.92.86) at b0:83:fe:cb:97:fc [ether] on enp0s31f6

deepgpu0.eng.uwaterloo.ca (129.97.92.39) at 00:13:3b:10:0d:f1 [ether] on enp0s31f6

deepgpu2.eng.uwaterloo.ca (129.97.92.142) at ac:1f:6b:41:5a:48 [ether] on enp0s31f6

memslinux1.uwaterloo.ca (129.97.92.31) at 00:25:90:23:ee:96 [ether] on enp0s31f6

emrglinux5.eng.uwaterloo.ca (129.97.92.21) at f8:bc:12:33:1f:6c [ether] on enp0s31f6

swen-129-97-92-252.dynamic.uwaterloo.ca (129.97.92.252) at 00:30:64:1a:2e:d9 [ether] on enp0s31f6

maslab-lps1.uwaterloo.ca (129.97.92.67) at 3c:ec:ef:47:b9:2d [ether] on enp0s31f6

eceterm2.uwaterloo.ca (129.97.92.175) at 52:54:00:b2:34:ba [ether] on enp0s31f6

ecesystem.uwaterloo.ca (129.97.92.165) at 52:54:00:0c:98:ec [ether] on enp0s31f6

bbcr.uwaterloo.ca (129.97.92.32) at 00:04:23:ae:15:34 [ether] on enp0s31f6

rpsrvr1.uwaterloo.ca (129.97.92.54) at e0:69:95:dd:07:6b [ether] on enp0s31f6

ecetesla3.uwaterloo.ca (129.97.92.187) at 30:5a:3a:7b:98:de [ether] on enp0s31f6

hph5.eng.uwaterloo.ca (129.97.92.12) at 78:2b:cb:60:1f:3f [ether] on enp0s31f6

ciuw1.uwaterloo.ca (129.97.92.2) at 00:30:48:ff:8e:a6 [ether] on enp0s31f6

cadpass1.eng.uwaterloo.ca (129.97.92.100) at 52:54:00:5e:d8:ce [ether] on enp0s31f6

ece252-3.uwaterloo.ca (129.97.92.122) at 52:54:00:4a:9d:a3 [ether] on enp0s31f6

? (129.97.92.203) at e0:4f:43:e6:28:97 [ether] on enp0s31f6

iccad5.eng.uwaterloo.ca (129.97.92.193) at d4:be:d9:b1:2b:81 [ether] on enp0s31f6

rfdesign4.uwaterloo.ca (129.97.92.45) at 00:25:90:e1:20:b4 [ether] on enp0s31f6

ecetesla0.uwaterloo.ca (129.97.92.168) at 00:25:90:5e:d0:9c [ether] on enp0s31f6

sync-2.uwaterloo.ca (129.97.92.35) at 18:03:73:fb:1d:e2 [ether] on enp0s31f6

winserv2.uwaterloo.ca (129.97.92.15) at 00:30:48:d6:8b:68 [ether] on enp0s31f6

deepgpu1.eng.uwaterloo.ca (129.97.92.138) at ac:1f:6b:41:11:de [ether] on enp0s31f6

alchemy.uwaterloo.ca (129.97.92.150) at 3c:ec:ef:05:73:32 [ether] on enp0s31f6

weis.eng.uwaterloo.ca (129.97.92.17) at 18:03:73:fa:f8:c2 [ether] on enp0s31f6

Explanation: The arp command outputted the kernel’s current IPv4 network neighbour cache. It shows a list of entries with the following format: *address* *(IP address*) at *HWaddress* [*HWtype*] on *interface*

3. a)

**Ifconfig** is used to configure the kernel-resident network interfaces. It is used at boot

time to set up interfaces as necessary. After that, it is usually only needed when debug‐

ging or when system tuning is needed.

If no arguments are given, **ifconfig** displays the status of the currently active interfaces.

If a single **interface** argument is given, it displays the status of the given interface

only; if a single **-a** argument is given, it displays the status of all interfaces, even

those that are down. Otherwise, it configures an interface.

b)

enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 129.97.92.172 netmask 255.255.255.0 broadcast 129.97.92.255

inet6 fe80::1582:2c3a:8da1:b445 prefixlen 64 scopeid 0x20<link>

ether 30:5a:3a:83:92:bf txqueuelen 1000 (Ethernet)

RX packets 4379619161 bytes 2024800731803 (2.0 TB)

RX errors 0 dropped 42352 overruns 0 frame 0

TX packets 5411200068 bytes 3573047039883 (3.5 TB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 16 memory 0xf7000000-f7020000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 612042414 bytes 335086289663 (335.0 GB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 612042414 bytes 335086289663 (335.0 GB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Explanation: The command displayed the status of all interfaces. This includes whether the interface is up, maximum transmission unit, transmission and receiver packets and errors.

There are two interfaces currently up and running and 0 interfaces that are down.

4. a)

**Netstat** prints information about the Linux networking subsystem. The type of information

printed is controlled by the first argument, as follows:

**(none)**

By default, **netstat** displays a list of open sockets. If you don't specify any address fam‐

ilies, then the active sockets of all configured address families will be printed.

**--route,** **-r**

Display the kernel routing tables. See the description in **route**(8) for details. **netstat** **-r**

and **route** **-e** produce the same output.

**--groups,** **-g**

Display multicast group membership information for IPv4 and IPv6.

**--interfaces,** **-i**

Display a table of all network interfaces.

**--masquerade,** **-M**

Display a list of masqueraded connections.

**--statistics,** **-s**

Display summary statistics for each protocol.

b)

Kernel Interface table

Iface MTU RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg

enp0s31f 1500 4379848738 0 42352 0 5411509310 0 0 0 BMRU

lo 65536 612142964 0 0 0 612142964 0 0 0 LRU

Explanation: The command displayed a table containing all network interfaces. The table displays the interface name, the max transmission unit, received packets, received packet errors, received packets dropped, transmitted packets, transmitted packet errors, transmitted packets dropped and flags.

c)

Kernel IP routing table

Destination Gateway Genmask Flags MSS Window irtt Iface

default v92-e2-rt-1782a 0.0.0.0 UG 0 0 0 enp0s31f6

129.97.92.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s31f6

link-local 0.0.0.0 255.255.0.0 U 0 0 0 enp0s31f6

Explanation: This command displayed the kernel routing tables.

It showed the Destination, Gateway, general Netmask of route, flags, max segment size, window size, initial round trip time and interface name.

5. a)

**Nslookup** is a program to query Internet domain name servers. **Nslookup** has two modes:

interactive and non-interactive. Interactive mode allows the user to query name servers for

information about various hosts and domains or to print a list of hosts in a domain.

Non-interactive mode is used to print just the name and requested information for a host or

domain.

b)

1.

i)

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.169

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.172

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.76

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.187

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.188

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.168

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.171

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.170

ii)

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.169

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.172

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.76

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.187

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.188

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.168

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.171

Name: eceubuntu.uwaterloo.ca

Address: 129.97.92.170

2.

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

www.mit.edu canonical name = www.mit.edu.edgekey.net.

www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.

Name: e9566.dscb.akamaiedge.net

Address: 184.25.74.205

Name: e9566.dscb.akamaiedge.net

Address: 2600:141b:e800:138f::255e

Name: e9566.dscb.akamaiedge.net

Address: 2600:141b:e800:1384::255e

3.

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: www.gmail.com

Address: 142.251.41.37

Name: www.gmail.com

Address: 2607:f8b0:400b:803::2005

4.

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

www.facebook.com canonical name = star-mini.c10r.facebook.com.

Name: star-mini.c10r.facebook.com

Address: 31.13.80.36

Name: star-mini.c10r.facebook.com

Address: 2a03:2880:f10e:83:face:b00c:0:25de

Explanation: The command printed out the names and addresses of the desired hostname

6. a) **ping** uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP

ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams (“pings”) have an IP and ICMP

header, followed by a struct timeval and then an arbitrary number of “pad” bytes used to

fill out the packet.

**ping** works with both IPv4 and IPv6. Using only one of them explicitly can be enforced by

specifying **-4** or **-6**.

**ping** can also send IPv6 Node Information Queries (RFC4620). Intermediate hops may not be

allowed, because IPv6 source routing was deprecated (RFC5095)

b)

1.

PING prod.cds.ualberta.cloud (13.225.195.60) 56(84) bytes of data.

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=1 ttl=234 time=11.3 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=2 ttl=234 time=13.1 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=3 ttl=234 time=11.3 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=4 ttl=234 time=11.3 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=5 ttl=234 time=11.6 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=6 ttl=234 time=11.3 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=7 ttl=234 time=11.6 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=8 ttl=234 time=11.3 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=9 ttl=234 time=11.4 ms

64 bytes from server-13-225-195-60.yul62.r.cloudfront.net (13.225.195.60): icmp\_seq=10 ttl=234 time=11.3 ms

--- prod.cds.ualberta.cloud ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9011ms

rtt min/avg/max/mdev = 11.290/11.558/13.138/0.538 ms

2.

PING e.sni.global.fastly.net (151.101.126.217) 56(84) bytes of data.

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=1 ttl=53 time=4.09 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=2 ttl=53 time=3.99 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=3 ttl=53 time=4.00 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=4 ttl=53 time=3.99 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=5 ttl=53 time=3.99 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=6 ttl=53 time=4.09 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=7 ttl=53 time=4.04 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=8 ttl=53 time=4.16 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=9 ttl=53 time=4.07 ms

64 bytes from 151.101.126.217 (151.101.126.217): icmp\_seq=10 ttl=53 time=3.99 ms

--- e.sni.global.fastly.net ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9009ms

rtt min/avg/max/mdev = 3.988/4.040/4.164/0.057 ms

3.

PING d1zev4mn1zpfbc.cloudfront.net (18.67.39.28) 56(84) bytes of data.

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=1 ttl=243 time=4.08 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=2 ttl=243 time=4.20 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=3 ttl=243 time=4.18 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=4 ttl=243 time=4.10 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=5 ttl=243 time=4.11 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=6 ttl=243 time=4.11 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=7 ttl=243 time=4.11 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=8 ttl=243 time=4.15 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=9 ttl=243 time=4.10 ms

64 bytes from server-18-67-39-28.yto50.r.cloudfront.net (18.67.39.28): icmp\_seq=10 ttl=243 time=4.02 ms

--- d1zev4mn1zpfbc.cloudfront.net ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9011ms

rtt min/avg/max/mdev = 4.016/4.115/4.196/0.048 ms

Explanation: The command prints out the information of the received ICMP ECHO\_RESPONSE’s from the respective hostname. It shows the size, source address, source IP, ICMP sequence number, time to live(TTL) and the time at which it was received.

It also shows overall statistics at the end of the command

It transmitted 10 packets and received 10 (because of count (c10)).

7.a) **traceroute** tracks the route packets taken from an IP network on their way to a given host.

It utilizes the IP protocol's time to live (TTL) field and attempts to elicit an ICMP

TIME\_EXCEEDED response from each gateway along the path to the host.

b)

1.

traceroute to www.uwaterloo.ca (129.97.208.23), 30 hops max, 60 byte packets

1 v92-e2-rt-1782a.nsx.uwaterloo.ca (129.97.92.1) 1.247 ms 1.506 ms 1.563 ms

2 po340-1500-10-dist-rt.ns.uwaterloo.ca (172.16.15.132) 0.167 ms 0.358 ms 0.339 ms

3 \* po130-ftd-dist-sa-mc-campus-trust.ns.uwaterloo.ca (172.16.49.204) 0.344 ms \*

4 v500-dist-rt-untrust.nsx.uwaterloo.ca (129.97.13.1) 0.498 ms 0.717 ms 0.633 ms

5 po30-cn-rt-mc.ns.uwaterloo.ca (172.16.34.84) 0.613 ms 0.643 ms 0.676 ms

6 e2-1-cr-rt-mc.ns.uwaterloo.ca (172.16.16.67) 0.764 ms 1.157 ms 1.028 ms

7 xe4-0-1-22-cr-sa-bb2.ns.uwaterloo.ca (172.16.16.7) 0.952 ms 0.862 ms 0.868 ms

8 e1-25-20-cr-rt-mc-area2.ns.uwaterloo.ca (172.16.16.27) 1.990 ms 2.022 ms 2.087 ms

9 wms.uwaterloo.ca (129.97.208.23) 1.312 ms 1.147 ms 1.152 ms

10 wms.uwaterloo.ca (129.97.208.23) 1.192 ms !N 1.237 ms !N 1.150 ms !N

2.

traceroute to www.youtube.com (172.217.1.14), 30 hops max, 60 byte packets

1 v92-e2-rt-1782a.nsx.uwaterloo.ca (129.97.92.1) 1.004 ms 1.296 ms 1.375 ms

2 po340-1500-10-dist-rt.ns.uwaterloo.ca (172.16.15.132) 0.177 ms 0.327 ms 0.309 ms

3 po130-ftd-dist-sa-mc-campus-trust.ns.uwaterloo.ca (172.16.49.204) 0.404 ms \* \*

4 v500-dist-rt-untrust.nsx.uwaterloo.ca (129.97.13.1) 0.575 ms 0.504 ms 0.539 ms

5 po30-cn-rt-mc.ns.uwaterloo.ca (172.16.34.84) 0.682 ms 0.717 ms 0.700 ms

6 gi0-0-1-ext-rt-rac.ns.uwaterloo.ca (172.16.31.109) 1.308 ms 1.340 ms 1.256 ms

7 72.15.57.69 (72.15.57.69) 3.861 ms 3.828 ms 3.712 ms

8 \* \* \*

9 lo0.1.bdr02.151FrontStW01.YYZ.beanfield.com (72.15.48.47) 3.565 ms 4.995 ms 4.573 ms

10 \* \* \*

11 lo0-1.bdr01.151FrontStW01.YYZ.beanfield.com (72.15.48.10) 4.675 ms 4.710 ms 3.812 ms

12 142.250.173.68 (142.250.173.68) 4.484 ms 4.600 ms 4.579 ms

13 \* \* \*

14 172.253.69.112 (172.253.69.112) 6.061 ms 172.253.69.114 (172.253.69.114) 3.300 ms 172.253.69.112 (172.253.69.112) 6.140 ms

15 74.125.244.146 (74.125.244.146) 4.621 ms 74.125.244.162 (74.125.244.162) 4.325 ms 216.239.35.233 (216.239.35.233) 4.456 ms

16 \* \* \*

17 142.251.61.5 (142.251.61.5) 5.500 ms \* \*

18 \* \* 216.239.35.233 (216.239.35.233) 4.817 ms

19 \* 216.239.35.235 (216.239.35.235) 5.661 ms \*

20 \* \* \*

21 \* \* \*

22 \* \* \*

23 \* \* \*

24 \* \* \*

25 \* \* \*

26 \* \* \*

27 \* \* \*

28 \* \* \*

29 \* \* \*

30 \* \* \*

3.

traceroute to www.nytimes.com (151.101.125.164), 30 hops max, 60 byte packets

1 v92-e2-rt-1782a.nsx.uwaterloo.ca (129.97.92.1) 0.945 ms 1.121 ms 1.287 ms

2 po340-1500-10-dist-rt.ns.uwaterloo.ca (172.16.15.132) 0.179 ms 0.164 ms 0.303 ms

3 \* \* po130-ftd-dist-sa-mc-campus-trust.ns.uwaterloo.ca (172.16.49.204) 0.362 ms

4 v500-dist-rt-untrust.nsx.uwaterloo.ca (129.97.13.1) 0.514 ms 0.547 ms 0.652 ms

5 po30-cn-rt-mc.ns.uwaterloo.ca (172.16.34.84) 0.742 ms 0.780 ms 0.754 ms

6 gi0-0-1-ext-rt-rac.ns.uwaterloo.ca (172.16.31.109) 1.295 ms 3.534 ms 3.572 ms

7 72.15.57.69 (72.15.57.69) 3.980 ms 3.929 ms 3.816 ms

8 \* \* et31-1.lsr01.151FrontStW01.YYZ.beanfield.com (199.167.152.194) 11.763 ms

9 lo0.1.bdr02.151FrontStW01.YYZ.beanfield.com (72.15.48.47) 3.695 ms 3.659 ms 3.693 ms

10 \* \* \*

11 \* \* \*

12 \* \* \*

13 \* \* \*

14 \* \* \*

15 \* \* \*

16 \* \* \*

17 \* \* \*

18 \* \* \*

19 \* \* \*

20 \* \* \*

21 \* \* \*

22 \* \* \*

23 \* \* \*

24 \* \* \*

25 \* \* \*

26 \* \* \*

27 \* \* \*

28 \* \* \*

29 \* \* \*

30 \* \* \*

Explanation:

The command prints out the route taken to reach a host. Each line is a separate hop that the route takes. The line displays the router address, router IP address and time of each hop.

The command stops displaying new lines when the host is reached. For [www.uwaterloo.ca](http://www.uwaterloo.ca), it displays !N indicating the network is unreachable (this means it got to the ‘host’).

A star indicates that the router did not respond within the timeout (TTL). Youtube and NYtimes were not reached and the max hops of 30 was reached.