

# Practicals on Computer Networks and Distributed Systems

## Analysis of a simple tcpdump trace

All rights reserved © 2013-2024 by José María Foces Morán and José María Foces Vivancos

### Exercise 0. Setting the IP configuration of your Lab B6 host

Before doing this practice, set the following *static* IP configuration on your Lab B6 host. Edit `/etc/network/interfaces` appropriately for your main network device, for example, `eno1`, or `enp3s0`, etc.

- a. List network device labels in `/sys/class/net`.
- b. List all of the network devices physically connected to your host by issuing this command:

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

- c. The *main* network device should have the UP and RUNNING flags set, that is, if it is in fact connected to one of Lab B6 switches. Any device having UP and RUNNING set should function as the main device fine. In case you see no net device having the flags UP/RUNNING set, check that at least one device is connected to a switch. Now, you can edit `/etc/network/interfaces` to apply the configuration appearing below to the device that is selected as main.
- d. Set this IP address to the main device: `192.168.1.<n>`  
A Post-it note attached to your computer has integer `n` written on it. The valid range for `n` is in Lab B6 is `[100, 149]`.
- e. Set the Netmask as: `255.255.255.0`
- f. The default gateway must be set to IP address `192.168.1.1`
- g. Check the interfaces file syntax once again and reboot your system

### Exercise 1. Hand computation of the IP network number and the broadcast address

- a. Compute the IP Network Number resulting from the IP address that you set and the Netmask common to all of the Lab B6 hosts (Follow the instructions provided on the board)
- b. Check that the default gateway IP address that you entered belongs to the same IP block (Has the same IP Network Number) resulting in the preceding step
- c. Finally, compute the Broadcast IP Address to the network in Lab B6

### Exercise 2. IP connectivity checks

- Verify that your host has connectivity to localhost (`$ ping 127.0.0.1`)
- Issue the `/usr/sbin/route -n` command to print out your host's IP routing table. Observe the line identified with label 0.0.0.0; that line identifies your host's default gateway. What's its IP address? (It appears on the column titled Gateway)
- Verify that you have connectivity to your default gateway (`$ ping 192.168.1.1`)
- If the preceding step was successful, test connectivity to elsewhere in Internet. For example, test IP address 8.8.8.8

### Exercise 3. Observing the ICMP packets crossing your stack (ICMP – IP – SUB)

- Request a new terminal window (Term 2) to view the packets sent and received by the ping application as they cross your host's stack. To this end, run the `tcpdump` sniffer as root user by issuing these two commands in succession:

```
$ su
# /usr/bin/tcpdump -i <net device> -vvv -n -eX icmp
```

- On Term 1, verify that you have connectivity beyond your local net. An IP address you could test connectivity to is 193.146.96.2, or 193.146.96.3. Send a single echo packet by including the `-c 1` option of ping, so that the resulting `tcpdump` trace is easier to interpret:

```
$ ping -c 1 193.146.96.3
```

- Explain the resulting `tcpdump` trace (Term 2) by following the explanation offered on the board and on the Lab B6 TV screen. As reference, check out the following trace example:

The figure illustrates the process of decoding a `tcpdump` trace for an ICMP Echo/Echo Reply. It consists of three main parts:

- Network Diagram:** Shows a source host (IP 192.168.1.89) connected to an 'Inet' network, which is then connected to a destination host (IP 193.146.96.3).
- Packet Header Diagram:** Shows an 'Example Internet Datagram Header' with fields for Identification, Flags, Fragment Offset, Time to Live, Protocol, Source Address, and Destination Address.
- Terminal Screenshots:**
  - Term 1:** Shows a successful ping command: `administrator@debian-ule:~$ ping -c 1 193.146.96.3`. The output shows 64 bytes of data received from 193.146.96.3 with a TTL of 61 and a time of 1.33 ms.
  - Term 2:** Shows the `tcpdump` trace for the same ping. The first packet is an ICMP Echo Request (ID 16421, Seq 1) from 192.168.1.89 to 193.146.96.3. The second packet is an ICMP Echo Reply (ID 16421, Seq 1) from 193.146.96.3 to 192.168.1.89.

Handwritten annotations in pink highlight the 'ECHO REQUEST' and 'ECHO REPLY' packets in the terminal output and point to the corresponding fields in the packet header diagram.

Figure 1. Decoding a reference `tcpdump` trace to an ICMP Echo/Echo Reply