1 Packet Switching

1. In packet-switching networks, the source host segments long application-layer messages (for example images or music files) into smaller packets and sends the packets into the network. The receiver re-assembles the packets back into the original message. Figure 1 illustrates the end-to-end transmission of a message with and without segmentation. Consider a $7.5 \times 10^6$ bits long message that is to be sent from the source to the destination as shown in the figure. Suppose that each link in the figure is 1.5 Mbps. Ignore propagation, queuing and processing delays.

(a) Consider sending the message from source to destination without message segmentation. How long does it take to move the message from the source host to the first packet switch? Keep in mind that each packet switch uses a store and forward packet switching. What is the total time to move the message from the source host to the destination host?

(b) Now suppose that the message is segmented into 5,000 packets, with each packet being 1500 bits long. How long does it take to move the first packet from the source host to the first packet switch?

(c) How long does it take to move the file from the source host to the destination host when message segmentation is used? Compare and comment.

(d) What are the drawbacks of message segmentation?
2 Traceroute: Theory

1. Consult the man page for traceroute (man traceroute from the Linux command line or on the web at http://linux.die.net/man/8/traceroute). Consider the following traceroute output:

```
[dave@pyxis]~$ traceroute -n ethz.ch
traceroute to ethz.ch (129.132.128.139), 30 hops max, 60 byte packets
  1  192.33.93.1  0.822 ms  0.856 ms  0.893 ms
  2  10.10.1.81  1.222 ms  1.267 ms  1.265 ms
  3  10.1.17.242  1.252 ms  0.988 ms  1.117 ms
  4  192.33.92.185  1.815 ms  1.891 ms  1.778 ms
  5  * * *
  6  * * *
```

Figure 2: Traceroute output

(a) What does each of the three measurements next to each IP address on lines 1–4 mean?
(b) Give one possible reason why hops 5 and 6 show “* * *”

3 Traceroute: Practice

1. In the last exercise, you used traceroute to identify routers on the path to a given destination. In this exercise, you will use traceroute as a starting point to familiarize yourself with another useful tool: Wireshark, which is an open-source packet analyzer that enables you to inspect incoming and outgoing packets from any network interface of your machine. It can parse multiple networking protocols and display the relevant fields in its graphical user interface. As a starting point you will have to download and install Wireshark. We suggest to run it on Linux (possibly on a virtual machine).

   After successfully starting Wireshark, you will have to start capturing traffic from your machine. You can select from which interfaces to capture traffic through the capture options. To ensure that Wireshark will display traffic from all interfaces, you can choose the “any” option. For more details on Wireshark usage and features please consult online tutorials, which are widely available. While capturing traffic, run the following command:

```
traceroute -M icmp mit.edu
```

   Ideally, Wireshark has captured—among other traffic—packets that are related to your traceroute command.

   1. Locate the “Echo (ping) request” packets. What are the source and destination IP addresses and to which entities do they correspond? For these packets, locate the TTL value in the IP header. What do you observe?

---

1 We refer to the Linux traceroute utility. Utilities on other platforms may use different parameters to set the protocol.

2 If you run many applications that heavily exchange traffic, you may find it difficult to identify the relevant packets in the capture. To help in this direction, you can try to apply display filters.
2. Locate the corresponding ICMP replies to the ping requests and compare the source IP addresses with the traceroute results. What do you notice? Why does each packet appear multiple times?

3. Capture again the traffic with the following traceroute command: `traceroute mit.edu`. Do you observe any difference in the traceroute results? What is the difference when you look at the captured packets? Is there a conceptual difference between the two traceroute commands? Try to briefly explain.

4. For both incoming and outgoing packets, try to locate MAC addresses. What addresses do you observe and to which entities do they correspond?