Lab 1 Ethernet Frame

Ethernet is a popular link layer protocol of LAN (covered in §4.3 of the textbook). Modern computers connect to Ethernet switches (§4.3.4) rather than use classic Ethernet (§4.3.2). Review the Section §4.3 before doing this lab.

Objective

- Understand the details of Ethernet frames, e.g., frame format.
- Understand functions of Ethernet address (i.e., MAC address), e.g., unicast, broadcast and multicast address.
- Know LLC header format.

Requirements

You need to install following tools on your computer beforehand:

- **Wireshark:** refer to previous labs for details.
- **ping:** This lab uses "*ping*" to send and receive messages. *ping* is a standard command-line utility for checking that another computer is responsive. It is widely used for network troubleshooting and comes pre-installed on Windows, Linux, and Mac. While *ping* has various options, simply issuing the command "*ping* www.jnu.edu.cn" will cause your computer to send a small number of *ICMP ping requests* to the remote computer (here www.jnu.edu.cn), each of which should elicit an *ICMP ping response*.

Exercise

Task 1: Capture a Trace

Proceed as follows to capture a trace of network traffic:

1. Pick a remote web server or other publicly reachable Internet host and use ping to send some ping messages and check that it sends replies. For example, "*ping* www.baidu.com" or "*ping* www.jnu.edu.cn".

   Tips:

   - You should see several replies indicating that the *ping* messages reached the remote host and were returned. The figure below shows a successful example.
   - Note that some versions of *ping* will continue to bounce messages off of a remote server until you tell the program to stop by signaling it with **Ctrl + C**.
   - If your *ping* does not succeed, try another server.

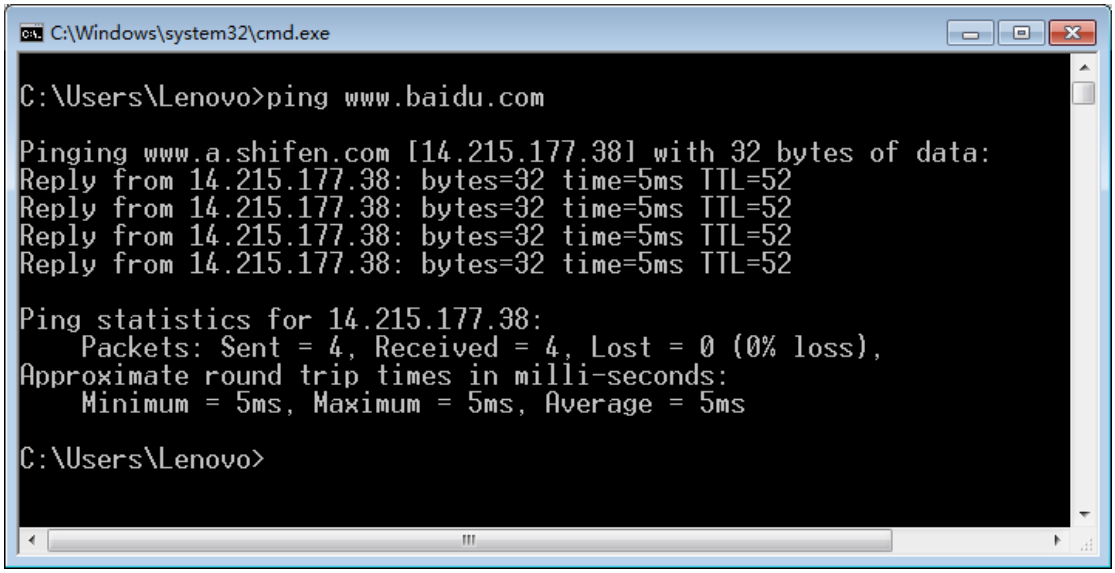

Figure 1: Using ping to bounce messages off a remote host

2. Start the capture of Wireshark, repeat the *ping* command above. This time, the packets will also be recorded by Wireshark.
3. After the *ping* command is completed, return to Wireshark and stop the trace. You should now have a short trace similar to that shown in the figure below.
   Tips: You can use filter "*icmp*" to display only packets for *ping*, since the *ping* command uses ICMP protocol.

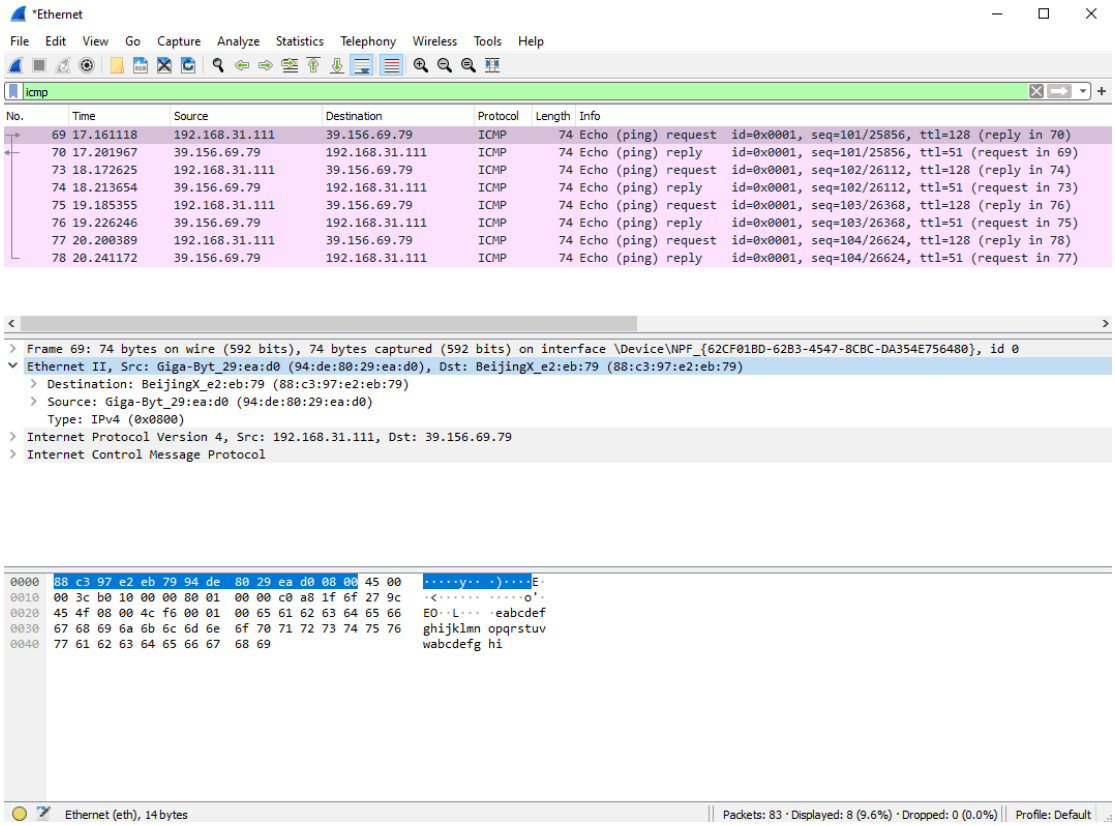

Figure 2: Trace of *ping* traffic, showing Ethernet details of the first packet

Task 2: Inspect the Trace and Ethernet Frame Structure

1. Select any packet in the trace (in the top panel) to see details of its structure (in the middle panel) and the bytes that make up the packet (in the bottom panel).

Tips:

- Note that we are using the term "packet" in a loose way.
- Each record captured by Wireshark corresponds to a single frame in Ethernet format that carries a packet as its payload.
- Wireshark interprets as much structure as it can.

2. In the middle panel, expand the Ethernet header fields to see their details.

   Tips:

   - Our interest is the Ethernet header, and you may ignore the higher layer protocols (which are IP and ICMP in this case).
   - You can click on the Ethernet header to see the bytes that correspond to it in the packet highlighted in the bottom panel.

Answer the following questions:

1. Explain the fields of Ethernet frame you see in the trace.
2. Compare these fields with the Ethernet frame format introduced in the textbook (e.g., any fields that are missing in your trace? Their usage?).
3. What is the length of captured frames? Explain why does Ethernet frame have the minimum length requirement.

Task 3: Scope of Ethernet Addresses

Draw a figure that shows the relative positions of *your computer, the router, and the remote server*.

- Label *your computer* and the *router* with their Ethernet addresses, i.e., MAC addresses.
- Label *your computer* and the *re-mote server* with their IP addresses.
- Show where the Ethernet and the rest of the Internet fit on the drawing.

Tips:

- Each Ethernet frame carries a source and destination address. One of these addresses is that of your computer. It is the source for frames that are sent, and the destination for frames that are received. But what is the other address? Assuming you pinged *a remote Internet server*, it cannot be the Ethernet address of the remote server because an Ethernet frame is only addressed to go within one LAN. Instead, it will be the Ethernet address of the *router* or *default gateway*, such as your gateway (router). This is the device that connects your LAN to the rest of the Internet.
- In contrast, the IP addresses in the IP block of each packet do indicate the overall source and destination endpoints. They are your computer and the remote server.

Answer the following questions:

1. Which layer in TCP/IP model does MAC address apply to?

Task 4: Broadcast and Multicast Frames

1. Start a capture in Wireshark for broadcast and multicast Ethernet frames with a filter of "eth.dst[0] & 1" to capture both broadcast and multicast frames, wait up to 30 seconds (or more) to record background traffic, and then stop the capture.
2. Examine the multicast and broadcast packets that you captured, checking the details of the source and destination Ethernet addresses.

Tips:

- You may have to wait a little while for these packets to be captured. On most LANs with multiple computers, you will see at least a packet every few seconds.
- If you do not capture any packets with this filter, use the trace that we supplied on the course website.
- The capture filter of "eth.dst[0] & 1" will capture both multicast and broadcast Ethernet frames, but not regular unicast frames.
- Broadcast frames tend to be more common than multicast frames.

Answer the following questions:

1. What is the broadcast Ethernet address?
2. Which bit of the Ethernet address is used to determine whether it is unicast or multicast/broadcast?
3. What is the meaning of filter "eth.dst[0] & 1"?
4. If we use a filter "(eth.dst[0]&1) && !eth.dst==ff:ff:ff:ff:ff:ff", what packets will be captured?

Task 5: LLC Header (IEEE 802.3)

Recall that there are two types of Ethernet frame, IEEE 802.3 and DIX Ethernet. DIX is common and what we considered above, while IEEE 802.3 is rare. If you are rather lucky, you may see some *IEEE 802.3 frames* in the trace you have captured. If not, there are some of these packets in the trace that we supplied. The following figure shows an example.

To search for IEEE 802.3 packets, enter a display filter (above the top panel of the Wireshark window) of "llc" (that was lowercase "LLC") because the IEEE 802.3 format has the LLC protocol on top of it. LLC is also present on top of IEEE 802.11 wireless, but it is not present on DIX Ethernet.

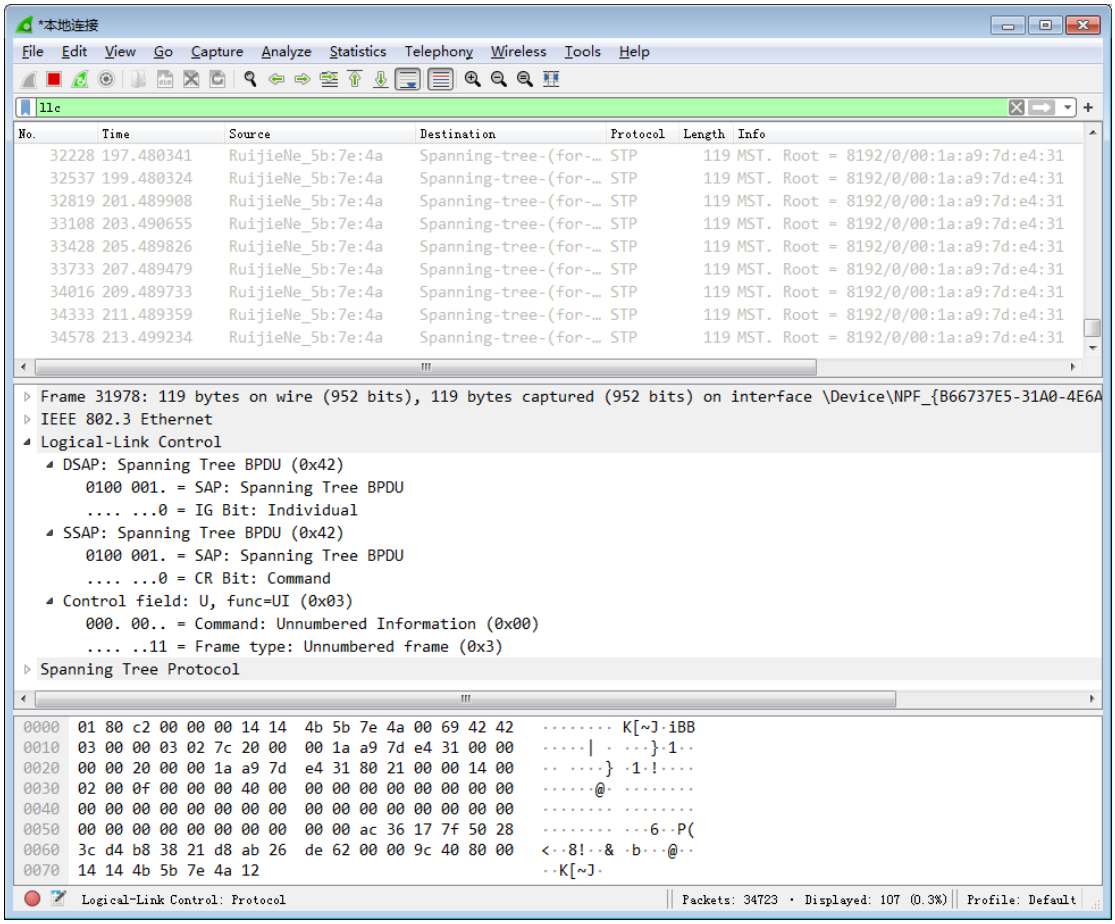

Figure 3: IEEE 802.3 frames with Ethernet and LLC header detail

Have a look at the details of an IEEE 802.3 frame, including the LLC header. The figure above shows the details in the supplied trace. Observe that the "Type" field is now a "Length" field.

In the example of Figure 3, the frame is short enough that there is also padding of zeros identified as a Trailer or Padding.

Answer the following questions:

1. What is the format of LLC header?
2. How long are the combined IEEE 802.3 and LLC headers compared to the DIX Ethernet headers?

   Tips: You can use Wireshark to work this out. Note that the Trailer/Padding and Checksum may be shown as part of the header, but they come at the end of the frame.
3. How does the receiving computer know whether the frame is DIX Ethernet or IEEE 802.3?

   Tips: You may need to both use Wireshark to look at packet examples and read your text near where the Ethernet formats are described.
4. If IEEE 802.3 frame has no Type field, how is the next higher layer determined? Use Wireshark to look for the demultiplexing key.

Questions:

1. Why IEEE 802 standard divides the data link layer into MAC sub-layer and LLC sub-layer?
2. What is the broadcast range (or scope) of a broadcast Ethernet frame?