**Lab Exercise 1 - Ethernet**

**Objective**

To explore the details of Ethernet frames. Ethernet is a popular link layer protocol. Review Ethernet before doing this lab.

**Requirements**

**Wireshark:** This lab uses the Wireshark software tool to capture and examine a packet trace.

**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 Window, Linux, and Mac. While ping has various options, simply issuing the command “ping www.bit.edu.cn” will cause your computer to send a small number of ICMP ping requests to the remote computer (here www.bing.com), each of which should elicit an ICMP ping response.

**Turn in**

Hand in the trace file you captured and exercise report including your answers to the questions and figures you drew.

**Step 1: Capture a Trace**

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.bit.edu.cn”. You should see several replies indicating that the pings reached the remote host and were returned.



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

1. Launch Wireshark and start a capture of Ethernet frames with a filter of “icmp”, making sure that “enable MAC name resolution” is checked. The latter will translate Ethernet (MAC) addresses to provide vendor information. Also check that the Link-layer header type pulldown says “Ethernet”.



Figure 2: Setting the capture options for ping traffic

1. When the capture is started, repeat the ping command above. This time, the packets will also be recorded by Wireshark.
2. After the ping command is complete, return to Wireshark and uses the menus or buttons to stop the trace. You should now have a short trace similar to that shown in the figure below.



Figure 3: Trace of ping traffic, showing Ethernet details of the first packet

**Step 2: Inspect the Trace**

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). Now we can inspect the details of the packets.

In the middle panel, expand the Ethernet header fields (using the “+” expander or icon) to see their details. 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.

**Step 3: Ethernet Frame Structure**

To show your understanding of the Ethernet frame format, **draw a figure** of the ping message that shows the position and size in bytes of the Ethernet header fields. Your figure can simply show the frame as a long, thin rectangle. The leftmost fields come first in the packet and are sent on the wire first. On this drawing, show the range of the Ethernet header and the Ethernet payload. Add a dashed box at the end to represent the 4-byte checksum; we know it is there even if Wireshark does not show us this field.

Figure 4: Ethernet frame structure

**Step 4: Scope of Ethernet Addresses**

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 ad-dress 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. 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.

**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. Label your computer and the remote server with their IP addresses. Show where the Ethernet and the rest of the Internet fit on the drawing.

Figure 5: Logical structure of the network

**Step 5: Broadcast Frames**

The trace that you gathered above captured unicast Ethernet traffic sent between a specific source and destination, e.g., your computer to the router. It is also possible to send multicast or broadcast Ethernet traffic, destined for a group of computers or all computers on the Ethernet, respectively. We can tell from the address whether it is unicast, multicast, or broadcast. Broadcast traffic is sent to a reserved Ethernet address that has all bits set to “1”. Multicast traffic is sent to addresses that have a “1” in the first bit sent on the wire; broadcast is a special case of multicast. Broadcast and multicast traffic is widely used for discovery protocols, e.g., a packet sent to everyone in an effort to find the local printer.

Start a capture for broadcast and multicast Ethernet frames with a filter of “ether multicast”, wait up to 30 seconds to record background traffic, and then stop the capture. If you do not capture any packets with this filter then use the trace that we supplied. On most Ethernets, there is a steady chatter of background traffic as computers exchange messages to maintain network state, which is why we try to capture traffic without running any other programs. The capture filter of “ether multicast” will capture both multicast and broadcast Ethernet frames, but not regular unicast frames. You may have to wait a little while for these packets to be captured, but on most LANs with multiple computers you will see at least a packet every few seconds.

Examine the multicast and broadcast packets that you captured, looking at the details of the source and destination addresses. Most likely one has the broadcast Ethernet address, as broadcast frames tend to be more common than multicast frames. Look at a broadcast frame to see what address is used for broadcast by Ethernet. Expand the Ethernet address fields of either broadcast or multicast frames to see which bit is set to distinguish broadcast/multicast or group traffic from unicast traffic.

**Answer the following questions:**

1. What is the broadcast Ethernet address, written in standard form as Wireshark displays it?
2. Which bit of the Ethernet address is used to determine whether it is unicast or multicast/broadcast?