Lab Exercise – Ethernet

Ethernet broadcast and multicast are two types of communication methods used in computer networks to efficiently manage and direct data to multiple destinations.

Ethernet Broadcast

1. *Definition*: In Ethernet networking, a broadcast is a message that is sent from one device to all other devices in the same local network segment. It's like a shout in a room—everyone hears it. Broadcasts are identified by a special MAC address (`FF:FF:FF:FF:FF:FF`), which is recognized by all network interfaces as a broadcast address.

2. *Usage*: Broadcasting is used for numerous network activities, such as ARP requests (when a device wants to find another device's physical MAC address using its IP address) or DHCP requests (when a device first connects to a network and requests network configuration parameters from a DHCP server).

3. *Limitations*: While useful, broadcasting can lead to a lot of unnecessary network traffic, as all devices in the broadcast domain must process each broadcast packet. This can lead to network congestion and reduced performance, especially in large networks, a phenomenon known as a broadcast storm.

Ethernet Multicast

1. *Definition*: Multicast is a more efficient form of communication where data is sent from one source to multiple destinations who are interested in receiving the specific data stream. Multicast uses a special range of MAC addresses (starting with `01:00:5E` in IPv4 and `33:33` in IPv6). Devices that want to receive a specific multicast group will listen to messages sent to the multicast MAC address associated with that group.

2. *Usage*: Multicast is often used for streaming media (like video or audio broadcasts) or for other applications where data needs to be distributed to multiple recipients simultaneously without putting unnecessary load on the source or network. It's like a conference call where only interested parties dial in and listen.

3. *Management*: Multicast traffic can be controlled on a network through protocols like IGMP (Internet Group Management Protocol) for IPv4 networks and MLD (Multicast Listener Discovery) for IPv6. These protocols allow routers to maintain information about which hosts are interested in receiving multicast traffic for specific multicast groups, optimizing the delivery paths for multicast packets.

Key Differences
- *Scope*: Broadcasts are sent to all devices in the network segment, whereas multicasts are only sent to specific group members.
- *Efficiency*: Broadcasting can lead to unnecessary processing by all devices in a network, while multicasting is more efficient, reducing network load by only sending packets to interested receivers.
- *Control*: Multicast traffic can be more finely controlled and optimized within a network through IGMP and MLD, compared to broadcast traffic.

Understanding and managing broadcast and multicast traffic is crucial for network administrators to ensure efficient data distribution and maintain overall network performance.

Objective

To explore the details of Ethernet frames. Ethernet is a popular link layer protocol. Modern computers connect to Ethernet switches rather than use classic Ethernet.

Step 1: Load the Lab Trace

Download and open the trace file at https://kevincurran.org/com320/labs/wireshark/trace-ethernet.pcap

1. *You should see a screen similar to the following:*

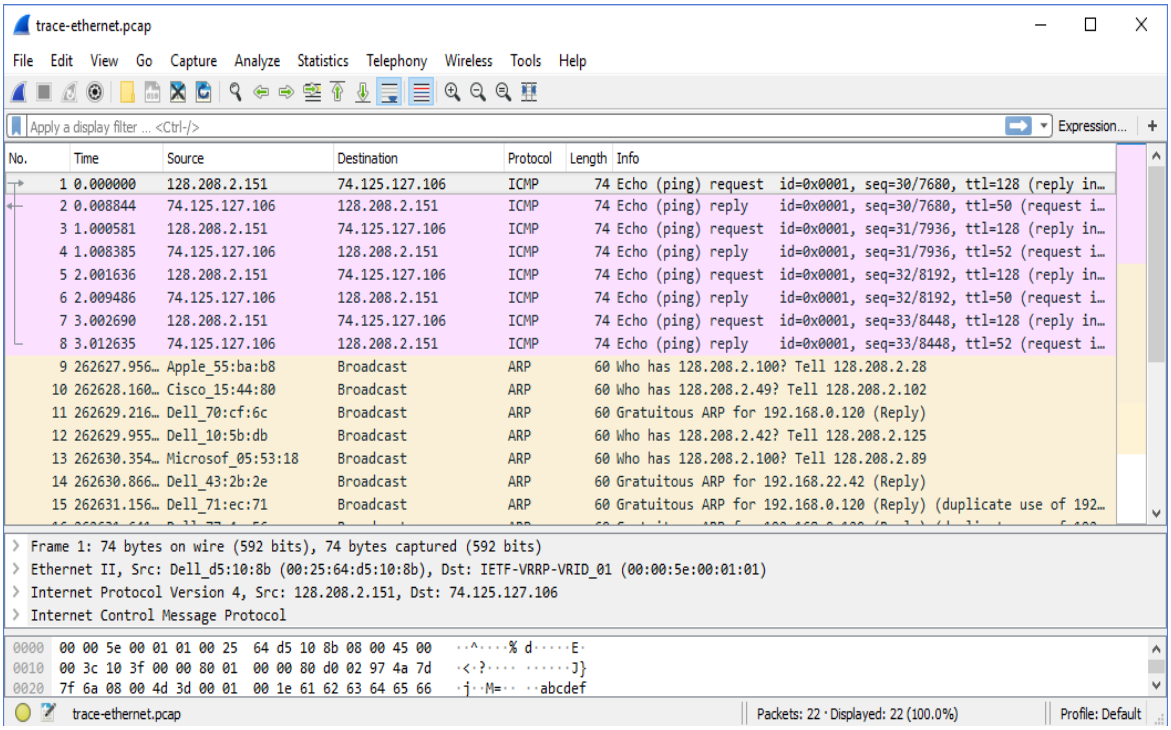


Figure 1: Ethernet trace opening screen

Primer on MAC Addresses

A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications on the physical network segment. It's a fundamental component used in the network layer of the OSI model. Here's a breakdown of what a MAC address represents and its role in networking:

Characteristics of a MAC Address:

1. Length and Format: A MAC address is a 48-bit (6-byte) number. It's commonly expressed in hexadecimal format, divided into pairs by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E).

2. Universality and Uniqueness: Ideally, every network interface card (NIC) or device that connects to a network should have a unique MAC address. This uniqueness is crucial for the local network's operations, ensuring that each device can be individually identified.

3. Assignment and Composition: The MAC address is generally assigned by the manufacturer of the network interface card (NIC) and is stored in its hardware, such as the card's read-only memory or other firmware mechanisms. A MAC address consists of two parts:

   - The OUI (Organizationally Unique Identifier): The first three bytes of the MAC address specify the manufacturer or organization. This part is assigned by the IEEE (Institute of Electrical and Electronics Engineers) and ensures that each manufacturer has a unique code.

   - The NIC Specific: The last three bytes are assigned by the manufacturer and are unique for each device.

4. Role in Networking: MAC addresses are used in the data link layer (Layer 2) of the OSI model. They are crucial for various network protocols and activities. For instance, in Ethernet networks, when a packet is sent on the local network, the MAC address is used to ensure that it reaches the correct destination on that local network.

5. Broadcast and Multicast MAC Addresses: There are special MAC addresses for broadcast and multicast communications. The broadcast MAC address (`FF:FF:FF:FF:FF:FF`) targets all devices on the local network, and multicast MAC addresses target a specific group of devices.

Operational Use:

- In an Ethernet LAN, when a packet is to be sent to a device within the same network, the sender uses the recipient's MAC address to directly send the packet to the correct device.

- When communicating over the internet or between different networks, devices use IP addresses. However, for the packet to move from a device to its gateway or between devices on the same network, the MAC address is used. This process is facilitated by protocols like ARP (Address Resolution Protocol), which maps IP addresses to MAC addresses.

While MAC addresses are designed to be permanent and unique, they can be changed or spoofed in software, a process often used in network security or privacy management. However, in a typical, secure, and well-managed network, the MAC address serves as a reliable and essential identifier for network hardware.

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 figure, we have selected the first packet in the trace. Note that we are using the term "packet" in a loose way. Each record captured by Wireshark more correctly corresponds to a single frame in Ethernet format that carries a packet as its payload; Wireshark interprets as much structure as it can.

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). Note the following:

- The frames in this trace are DIX Ethernet, called "Ethernet II" in Wireshark.
- There is no preamble in the fields shown in Wireshark. The preamble is a physical layer mechanism to help the NIC identify the start of a frame. It carries no useful data and is not received like other fields.
- There is a destination address and a source address. Wireshark is decoding some of these bits in the OUI (Organizationally Unique Identifier) portion of the address to tell us the vendor of the NIC, e.g., Dell for the source address.
- There is a Type field. For the ping messages, the Ethernet type is IP, meaning the Ethernet payload carries an IP packet. (There is no Length field as in the IEEE 802.3 format. Instead, the length of a DIX Ethernet frame is determined by the hardware of a receiving computer, which looks for valid frames that start with a preamble and end with a correct checksum, and passed up to higher layers along with the packet.)
- There is no Data field per se – the data starts with the IP header right after the Ethernet header.
- There is no pad. A pad will be present at the end if the frame would otherwise be less than 64 bytes, the minimum Ethernet frame size.
- There is no checksum in most traces, even though it really does exist. Typically, Ethernet hardware that is sending or receiving frames computes or checks this field and adds or strips it. Thus it is simply not visible to the OS or Wireshark in most capture setups.
- There are also no VLAN fields. If VLANs are in use, the VLAN tags are normally added and removed by switch ports so they will not be visible at host computers using the network.

Note: Answers to these questions are at the end of the lab notes.

Q1. What is the MAC address of the source of # 1 from IP address 128.208.2.151?

Q2. Click on # 12 and expand the [+] Address Resolution Protocol section in middle pane. What does Target MAC address: 00:00:00:00:00:00 mean?

Q3. Click again on # 12 and expand the [+] Address Resolution Protocol section in middle pane. Why is the protocol type listed as IP when it is not an IP packet?

Step 3: Ethernet Frame Structure

Try to understand the Ethernet frame format. Note the range of the Ethernet header and the Ethernet payload. See the frame structure below in Figure 2.

To work out sizes, observe that when you click on a protocol block in the middle panel (the block itself, not the "+" expander) then Wireshark will highlight the bytes it corresponds to in the packet in the lower panel and display the length at the bottom of the window. You may also use the overall packet size shown in the Length column or Frame detail block.

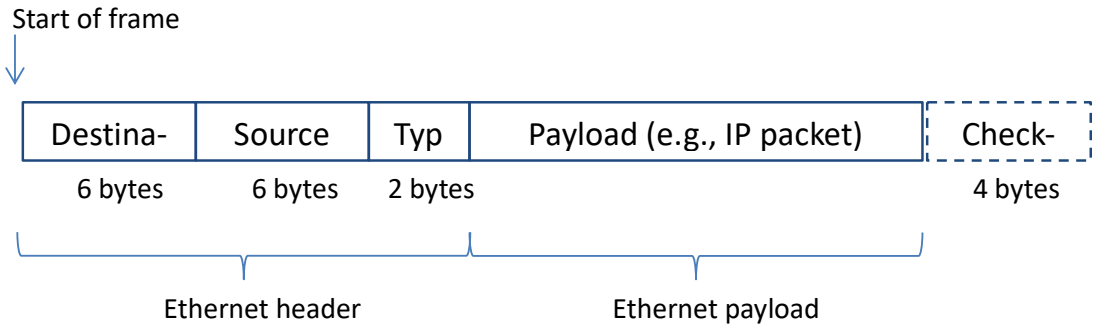


Figure 2: Structure of an Ethernet frame

There are several features to note:

- The destination address comes before the source address.
- The pad is not shown because the packets we examined (ping) are large enough that no pad is needed.
- Unlike many protocols, Ethernet has a trailer (the checksum, and pad if present) as well as a header. The checksum is handled by the hardware and not visible to Wireshark.
- The Ethernet header is 14 bytes long.

Note: Answers to these questions are at the end of the lab notes.

- Q1. Click on # 12 and expand the [+] Address Resolution Protocol section in middle pane. What does opcode (1) signify? What does opcode (2) signify?

  (note: In some Wireshark versions, opcode (1) is listed as (0x0001) & opcode (2) is listed as (0x0002)

- Q2. Click on # 12 and expand the [+] and give the hexadecimal value for the two-byte Ethernet Frame type field?

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 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 AP in the case of 802.11. 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.

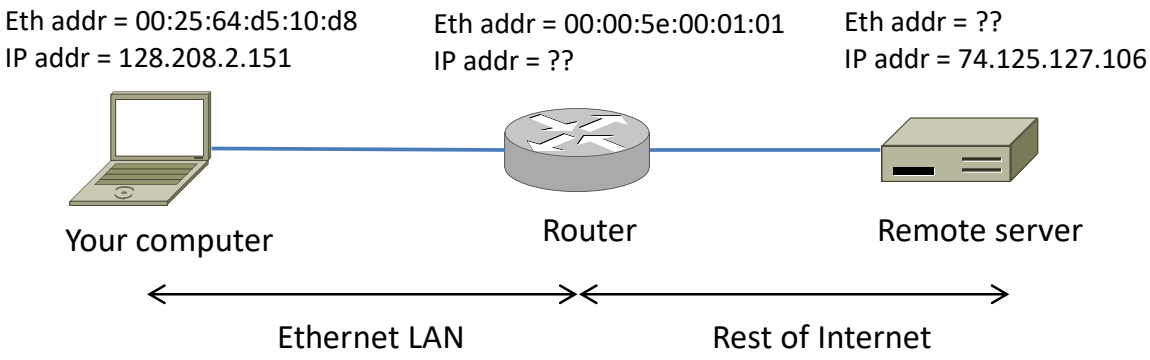


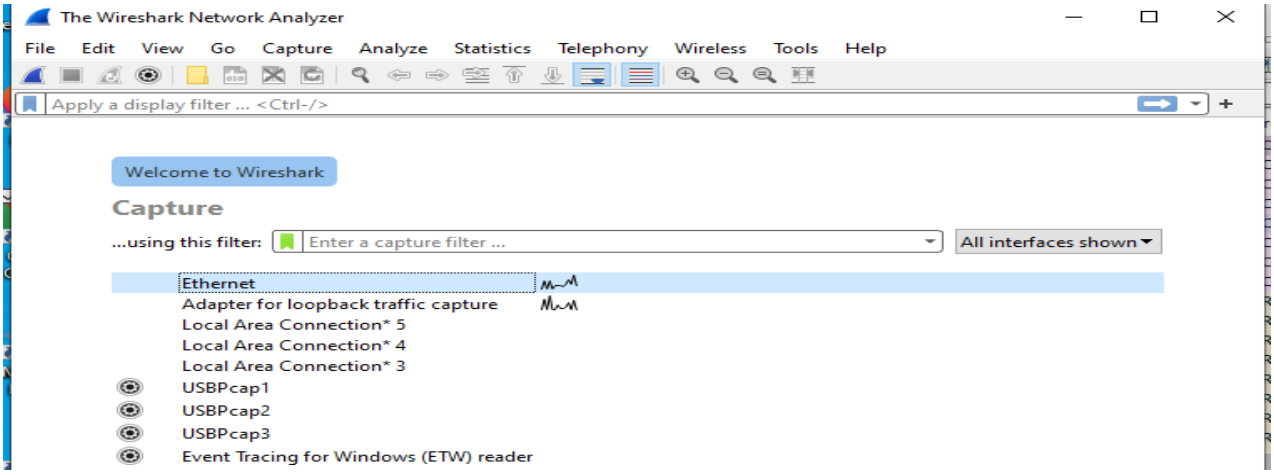
Figure 3: Ethernet and IP addresses of network devices

Step 5: Broadcast Frames

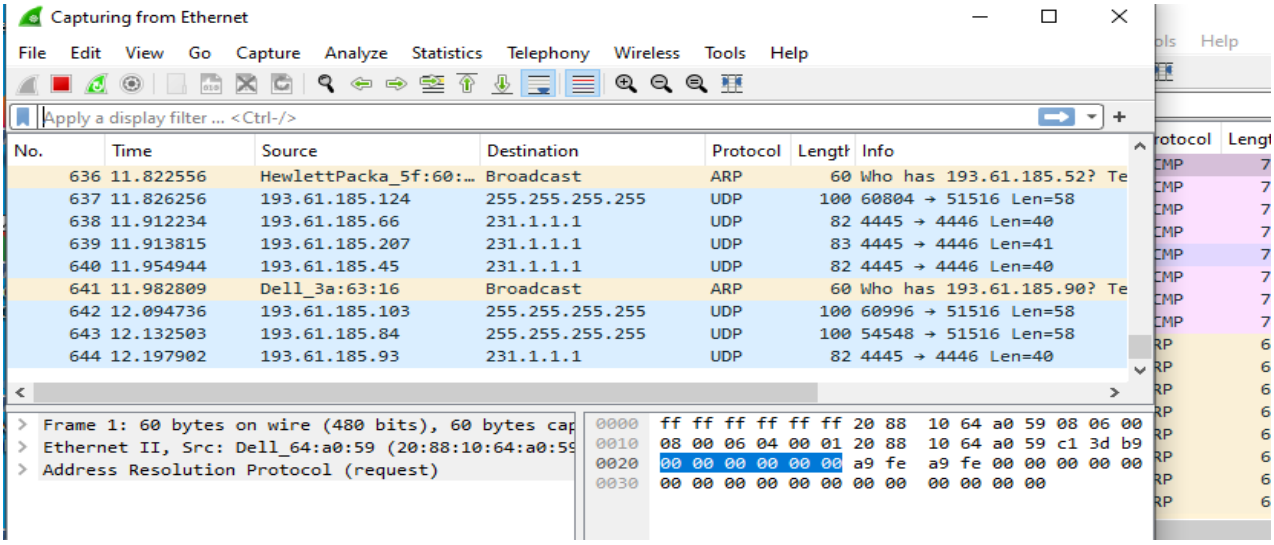
It is possible to send multicast or broadcast Ethernet traffic, destined for a group of computers or all computers on the Ethernet, respectively. We can tell from the address whether it is unicast, multicast, or broadcast. Broadcast traffic is sent to a reserved Ethernet address that has all bits set 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.

1. Open a new Wireshark Window. You can do this by simply typing *Wireshark* in the Windows Run Box in lower left.

2. Next choose the Ethernet Interface (as shown below).

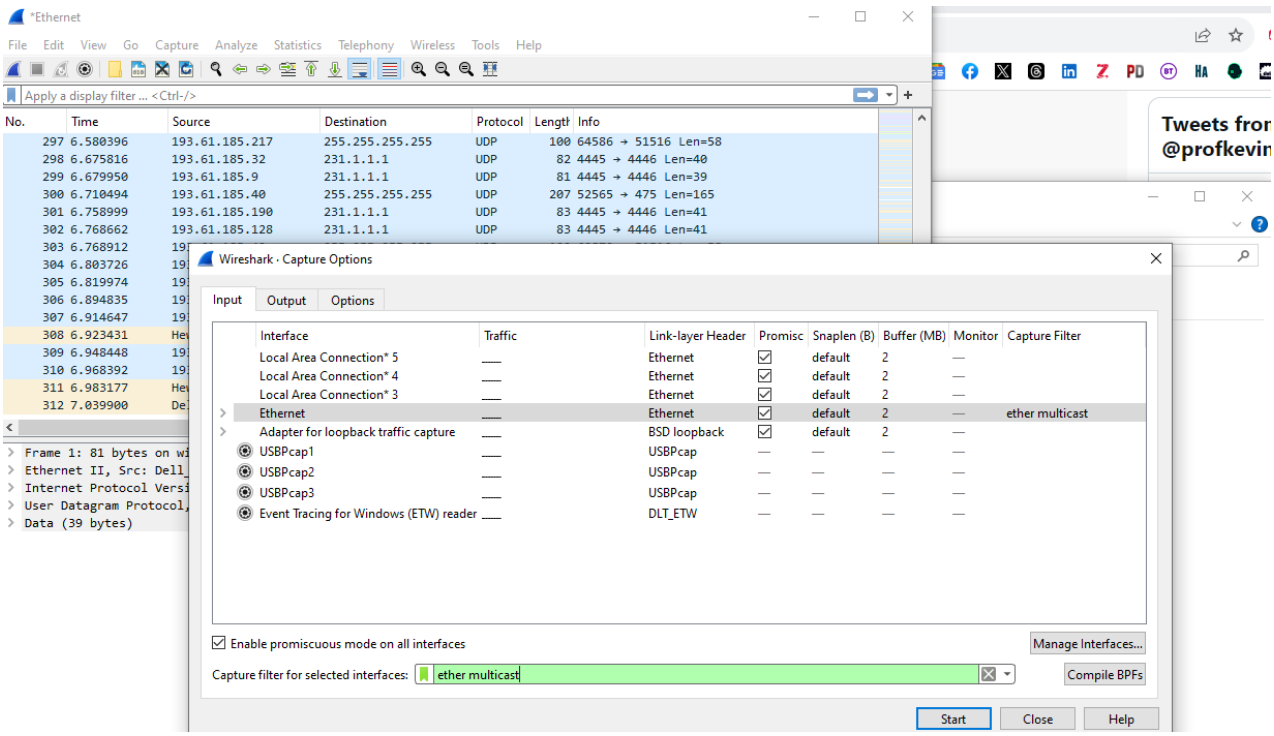


You should now start to see packets being captured.



3. Next in the main menu at top of Wireshark, Choose **Capture** and then Choose **Options**. You should see a screen similar to below.

4. Type **ether multicast** into the capture filter box as shown below.

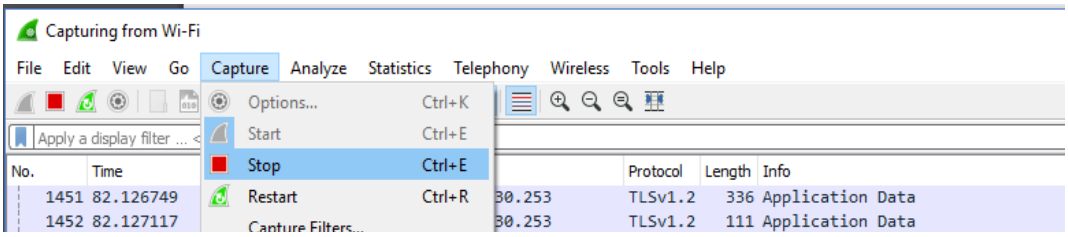


What we have done is to *start a capture for broadcast and multicast Ethernet frames with a filter of* "`ether multicast`". We did this by selecting ***Capture*** in the main menu and then selecting ***Option.***. This is not to be confused with the filter box on the live capture page which will not accept the filter expression above.

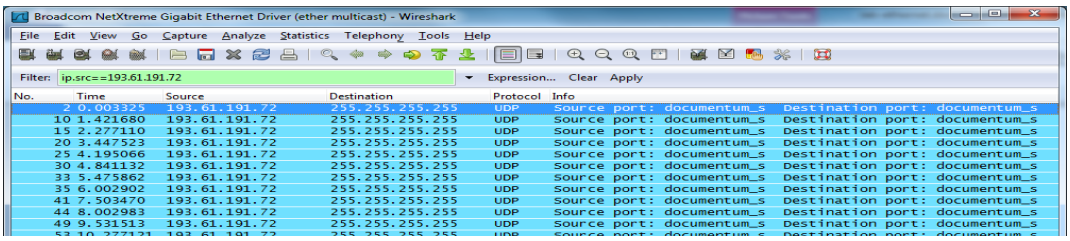
Examining Live Ethernet Multicast Traffic

1. *Wait up to 30 seconds to record background traffic, and then **stop** the capture (as shown below).. If you do not capture any packets with this filter then use the trace that we supplied.*

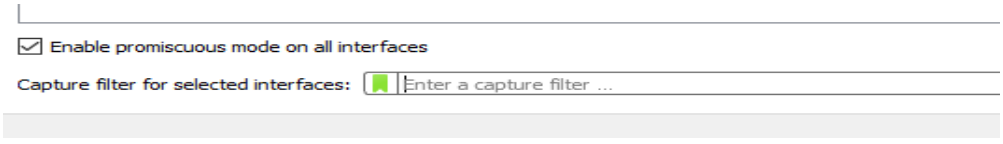
   On most Ethernets, there is a steady chatter of background traffic as computers exchange messages to maintain network state, which is why we try to capture traffic without running any other programs. The capture filter of "`ether multicast`" will capture both multicast and broadcast Ethernet frames, 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.



2. *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 (see below).



   NOTE: Before continuing, you should clear the capture filters of "ether multicast" by firstly selecting *Stop* from Capture and then again on Capture menu, selecting *options* and deleting the terms in the filter box. Basically, ensure the capture filter box as shown below is blank.



3. Answer the following questions. *(Note, answers are at the end, try to work it out first….)*

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

Step 6 - IEEE 802.3

We return again to *the trace file that you downloaded earlier from* -https://kevincur-ran.org/com320/labs/wireshark/trace-ethernet.pcap

You can reopen the trace file from the location you downloaded to e.g. Local Disk (C):\downloads or simply select *File menu* and O*pen Recent.* The trace file should be listed there.

There are some IEEE 802.3 frames in the trace supplied. 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 (and do not forget to click Apply) to apply the filter. LLC is also present on top of IEEE 802.11 wireless, but it is not present on DIX Ethernet. You should now see three packets like in the figure below.

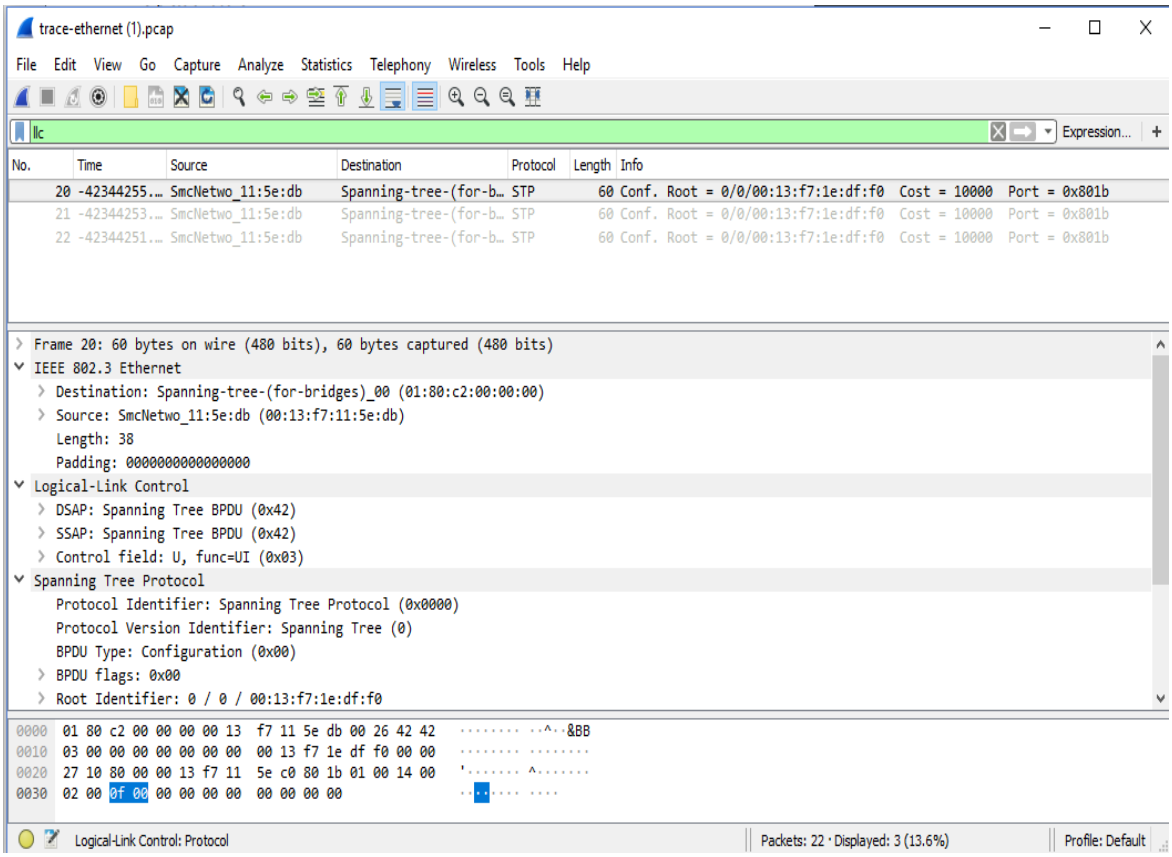


Figure 4: IEEE 802.3 frames with Ethernet and LLC header detail

Have a look at the details of an IEEE 802.3 frame, including the LLC header for instance no 20 in the supplied trace (first frame in capture).

The figure shows the details for our trace. Observe that the Type field is now a Length field. In our example, the frame is short enough that there is also padding of zeros identified as a Trailer or Padding.

The changes lead to a few questions for you to ponder:

1. How long are the combined IEEE 802.3 and LLC headers compared to the DIX Ethernet headers? 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.*

2. How does the receiving computer know whether the frame is DIX Ethernet or IEEE 802.3?

3. If IEEE 802.3 has no Type field, then how is the next higher layer determined? Use Wireshark to look for the demultiplexing key.