(12230325)

Practical Activity #1: Using Wireshark to Examine Ethernet Frames

**Part 1: Examine the Header Fields in an Ethernet II Frame**

**Q1: What is significant about the contents of the destination address field?**  
The destination address field can be either a unicast or a broadcast address. In the case of a broadcast (ff:ff:ff:ff:ff:ff), the frame is intended for all devices on the local network segment1.

**Q2: Why does the PC send out a broadcast ARP prior to sending the first ping request?**  
The PC sends a broadcast ARP to discover the MAC address of the default gateway, as it needs this information to send packets outside its local subnet1.

**Q3: What is the MAC address of the source in the first frame?**  
The MAC address of the source is f4:8c:50:62:62:6d1.

**Q4: What is the Vendor ID (OUI) of the Source’s NIC?**  
The Vendor ID (OUI) is the first three octets: f4:8c:501.

**Q5: What portion of the MAC address is the OUI?**  
The OUI is the first 6 hexadecimal digits (first 3 octets) of the MAC address1.

**Q6: What is the Source’s NIC serial number?**  
The serial number is the last 6 hexadecimal digits: 62:62:6d1.

**Part 2: Use Wireshark to Capture and Analyze Ethernet Frames**

**Q7: What is the IP address of the default gateway for the host H3?**  
The default gateway for H3 is 10.0.0.11.

**Q8: What is the MAC address of the PC’s NIC?**  
This can be found using ip address on H3; assume it is 5a:d0:1d:01:9f:be (as shown in the ARP cache example)1.

**Q9: What is the default gateway’s MAC address?**  
The gateway’s MAC address is the one associated with 10.0.0.1 in the ARP cache, which you would see in Wireshark or ARP output1.

**Q10: What type of frame is displayed?**  
The frame type is Ethernet II1.

**Q11: What is the source IP address?**  
The source IP address is the IP of H3 (e.g., 10.0.0.11)1.

**Q12: What is the destination IP address?**  
The destination IP address is the gateway (10.0.0.1) or the remote host, depending on the ping target1.

**Q13: What device and MAC address is displayed as the destination address in the Echo reply?**  
The destination device is H3, and the MAC address is 5a:d0:1d:01:9f:be1.

**Q14: In the first echo (ping) request frame to 172.16.0.40, what are the source and destination MAC addresses?**

* Source: H3’s MAC address (e.g., 5a:d0:1d:01:9f:be)
* Destination: Gateway’s MAC address (since the destination is not on the local subnet)1.

**Q15: What are the source and destination IP addresses contained in the data field of the frame?**

* Source: H3’s IP address (e.g., 10.0.0.11)
* Destination: 172.16.0.401.

**Q16: Why has the destination IP address changed, while the destination MAC address remained the same?**  
The destination IP changes because the ping is now targeting a remote host, but the destination MAC remains the gateway’s MAC because the packet must be sent to the gateway for routing outside the local network1.

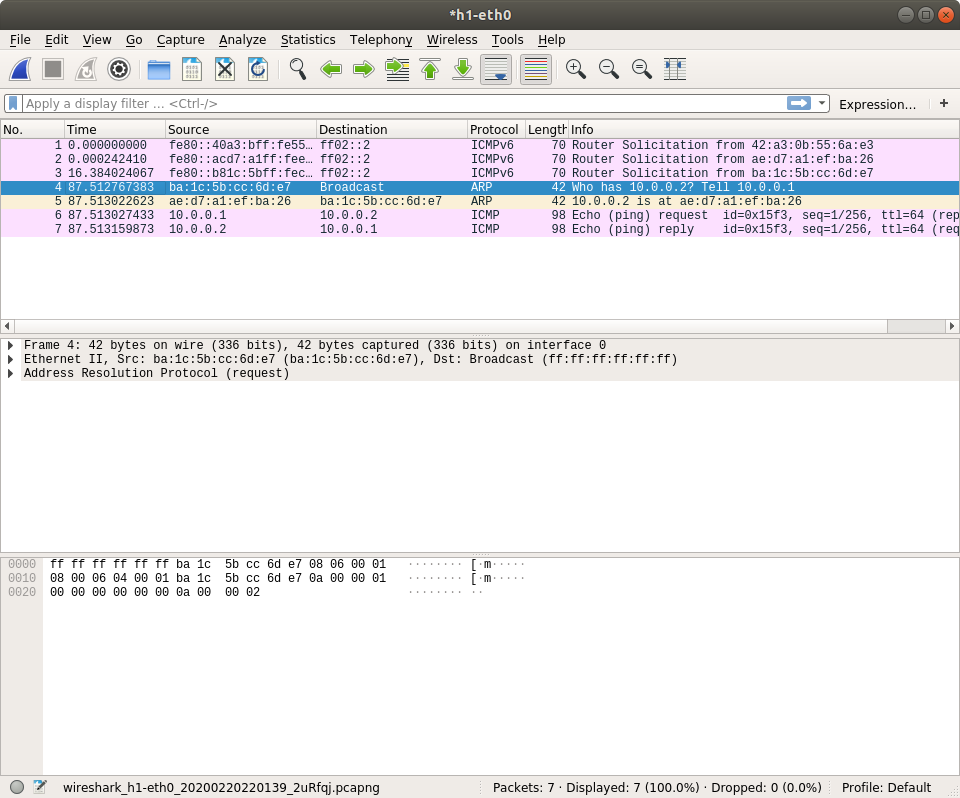
**Q17: What does the preamble contain?**  
The preamble contains synchronizing bits, processed by the NIC hardware, and is not shown in Wireshark captures1.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.