1. In your pcaps the SSH traffic (hopefully) has the property that the destination MAC address matches the destination IP address and the source MAC address also matches the source IP address. The HTTP traffic and traceroute traffic (hopefully) don't have this property. Why? Also, briefly, how do machines find out the MAC addresses of other machines on their subnet (be sure to reference specific frames in the packet captures)?

The SSH traffic, such as frames 122 and 123 from crandall-9-moe-eth1.pcap, is being sent between two machines that are on the same subnet, so there is no need for a gateway router to forward the packet. Therefore the sources and destinations are always the same machines. For the HTTP traffic, such as frames 168 and 169, the destination IP address is not on the subnet, so in layer 2 the destination for packets leaving the subnet (e.g., 168) should be the MAC address of the gateway router. For packets coming back and entering the subnet, the source MAC address is the MAC address of the gateway router (e.g., 169). When a machine doesn't know the MAC address of another machine on the subnet (i.e., there is no entry in its ARP cache), it uses an ARP who-is request as in frame 1. The machine in that IP responds with an ARP is-at response as in frame 2.

2. Some traffic appears in both pcaps but some does not. Why? (Your answer should include an explanation of how the router makes routing decisions about the packets it forwards, citing specific examples of specific packets).

One simple answer (which I'll accept for at least partial credit, because the question was ambiguous) is that some traffic (like the ARP requests and the SSH) is contained within one subnet, and each pcap corresponds to what traffic was on the wire on one of the subnets.

The answer I was actually looking for is that traffic between, e.g., larry and the Internet will appear on moe's eth1 but will not appear on moe's eth2, because the traffic is routed by moe between larry and the Internet by forwarding to eth0 (outgoing) or eth1 (incoming), so eth2 never sees that traffic:

```
crandall@moe:~$ sudo ip route show
[sudo] password for crandall:
default via 10.0.2.2 dev eth0
10.0.2.0/24 dev eth0  proto kernel  scope link  src 10.0.2.15
192.168.9.0/26 dev eth1  proto kernel  scope link  src 192.168.9.1
192.168.9.64/26 dev eth2  proto kernel  scope link  src 192.168.9.65
```

For example, frames 168 and 169 of crandall-9-moe-eth1.pcap never appear in crandall-9-moe-eth2.pcap for this reason.

A more complicated answer that's not what I was looking for is that in the traceroute, when the TTL is set to 1 a packet will never make it to the other subnet since moe will drop it due to a TTL Time Exceeded error.

3. How many different socket connections are visible in your pcaps? How can you tell that different packets are part of the same socket? (Your answer should include information about what fields in the IP and/or TCP headers help decide what socket a packet is part of).

Focusing only on stream sockets, there are two sockets visible in either packet capture: one for the SSH connection and one for the HTTP connection. A socket can be defined by source IP address, destination IP address, source port, destination port, and protocol (which is always TCP in this case).

4. Watch https://www.youtube.com/watch?v=fJ2N5z7g5c8 and make some comments about what you found interesting about the history behind the concepts that your answers to questions 1-3 refer to (*e.g.*, gateways, packet switching, or the connection-oriented protocol known as TCP/IP). These is no correct answer to #4 but a good answer should give me some indication that you watched the video and understood the connection between the video and Lab 1.

What answers you give for #4 is pretty wide open, but I hope you noticed in the video the origins of some of the words we use (like protocol, gateway, packet) and some of the ideas that were foundational in the Internet (like packet switching and Ethernet as a shared medium).