Q1.

> enable

# config t

(config)# ip dhcp pool LAB8

(dhcp-config)# network 172.168.10.0 255.255.255.0

(dhcp-config)# default-router 172.168.10.1

(dhcp-config)# exit

(config)# ip dhcp excluded-address 172.168.10.1 172.168.10.6

(config)# ip dhcp excluded-address 172.168.10.244 172.168.10.254

(config)# exit

Q2.

1)      ICMP pings use IP addresses, which are part of the network layer (3rd layer in the OSI model). However, as the packet needs to be sent using a layer 2 protocol (Ethernet in this case), it needs to be encapsulated in a layer 2 frame. Ethernet does not understand layer 3 addresses, as it uses MAC addressing.

2)      Examining the ARP packet, while *“parked up”*at the switch, we can see that the source MAC address is the MAC address of the host: PC0. The destination MAC address is FFFF.FFFF.FFFF, indicating the use of a MAC broadcast address. This packet will be addressed to each end device in the subnet, except for the packet source, in an attempt to find the end device with the matching target IP address. In the ARP packet are also seen the source and target IP addresses, however the target MAC address is still confirmed to be unknown.

3)      The switch learns the switch port associated with the MAC address of the host sending the packet.

Q3.

1)      In the previous step, the switch associated the switch port of the packet source and learned that it doesn’t need to broadcast the packet backwards. As the MAC address is a broadcast one, every other switch port in the VLAN will receive the message.

2)      Examining the packets at PC1, PC2 and Router2, we can see that the devices successfully opened the broadcast message, however the encapsulated target IP address didn’t match the devices own IP address. The ARP process drops the frame at the devices.

Q4.

1)      Similarly to Q3 2), the wireless devices successfully decapsulate the message from the Ethernet frame and as the request’s target IP address does not match the receiving port’s address, the frame is dropped.

Q5.

1)      The ARP reply message has now contained the target MAC address of PC0, it is now a unicast message, rather than broadcast. The switch has got that address associated with a specific port in its MAC table, and as such it only forwards the message on that particular port.

2)      PC0 learns the MAC address of the Wireless end device.

3)      The ICMP message is an Echo Request.

Q6.

1)      At Layer 2, the switch recognized the MAC addresses associated with the message and so, it only forwarded the message to the associated port.

2)      I) The source address is the MAC address of PC0 and the destination MAC address is the MAC address of the target wireless device.

ii) Address 1: Destination MAC address.  
    Address 2: Transmitter MAC address.

    Address 3: Source MAC address.

3)      In 802.11, address 1 is the MAC address of the receiver of the frame, hence this is where the destination MAC address is placed. The address 2 field is MAC filled in by the intermediate device itself. Address 3 is the MAC address of the device sending the frame, in this case it’s PC0.

Q7.

1)      The switch knew the MAC addresses of devices associated with the frame and only used the appropriate ports to forward the frame.

2)      This ICMP message is an Echo Reply.

3)      PC0 learned that the Wireless end device is live and reachable.