Exercise 1)

Q1)
For the case when we sent packets to a host on the same subnet(10.105.11.22),

the commands used are :
tcpdump -n host 10.105.11.22 -w /tmp/samesubnet.out
and after starting tcpdump, ping 10.105.11.22. After some time, stop the 2 commands.

4 ARP packets were exchanged.

Yes it does correspond to the remote host IP address.

Our host(10.105.11.24) sent an ARP packet on Broadcast asking the MAC address of 10.105.11.22 and that host replied with their MAC address. Another ARP packet was sent out from 10.105.11.22 to our host asking for our MAC address(This probably happened because the ARP cache table of 10.105.11.22 got cleared and asked us again).

Q2)
For the second case, I sent packets to 10.3.160.250.

The commands used were:
tcpdump -n host 10.3.160.250 -w /tmp/h3.out
and after starting tcpdump, ping 10.3.160.250. After some time, stop the 2 commands.

0 arp packets were exchanged.

This happened because the packets exchanged will go to the default gateway(router) first. Since our host already has the MAC address of the default gateway(router) stored in the arp cache table, no ARP packets will be exchanged.

Q3)
For the second case, I sent a packet to a non-existent host(10.105.12.253)[10.105.12.* corresponds to machines in NSL but 10.105.12.253 is not there]
The commands used were:
tcpdump -n host 10.105.12.253 -w /tmp/nslnonex.out
and after starting tcpdump, ping 10.105.12.253 -c 1.

Only 1 packet was sent because while ping-ing that IP, many packets will be sent so continous ARP packets will be broadcasted.
For a packet, only 3 ARP packets were sent on broadcast and then it gave up. The last ARP packet sent on broadcast at 1.996279s

---

Exercise 2:

Q1) Commands Used:

a) tcpdump -w /tmp/exercise2.out -i eth0 arp
b) arping -I eth0 -c 10 10.105.11.25
(10.105.11.25 is my own IP address, destination address has to be my own IP address to generate gratuitous ARP>))
c)arping -A -I eth0 -c 10 10.105.11.25
Then, I closed tcpdump and opened arp3.out in wireshark (wireshark -r /tmp/exercise2.out).
In wireshark, I sorted packets by Info field.

Q2) It is ensured that gratuitous ARP reaches all hosts in the physical network
by sending the ethernet frame as broadcast (destination address is ff:ff:ff:ff:ff:ff).

Q3) When gratuitous ARP is sent as reply, the target MAC address is that of my own machine and when it is sent as request, the target MAC address is broadcast . This is so because gratuitous ARP has been built upon ARP protocol and in it, the target MAC address is not known for a request but kn own for a reply.

Exercise 3)
The C code(sendUDP.c) is compiled to generate sendUDP executable

Q1)For this case, a packet of size 1000 Bytes was sent over the Ethernet to 10.3.160.250. Since this is less than Ethernet's maximum packet size(1500B), no fragmentation will occur.
The executable is executed as: ./sendUDP 10.3.160.250 1000 and packets are recorded using tcpdump -n host 10.3.160.250 -w socket.pcap

Total Length: 1028 B
Identification: 0x0000 (0)
Flags: 0x02 (Don't Fragment)
0th bit(Reserved bit) is Not Set
1st bit(Don't fragment) is Set
2nd bit(More fragment) is Not Set
Fragment Offset: 0
1028 B is the length because UDP header is 8 B and IP header is 20 B

Q2)
For this case, a packet of size 2000 Bytes was sent over the Ethernet to 10.3.160.250. Since this is greater than Ethernet's maximum packet size(1500B), fragmentation will occur.
The executable is executed as: ./sendUDP 10.3.160.250 2000 and packets are recorded using tcpdump -n host 10.3.160.250 -w socketfrag.pcap
2 packets are observed: 1 is a fragmented IPv4 protocol packet and the second packet follows UDP protocol

Packet 1)

Total Length: 1500 B
Identification: 0xd58c (54668)
Flags: 0x01 (More Fragments)

0th bit(Reserved bit) is Not Set
1st bit(Don't fragment) is Not Set
2nd bit(More fragment) is Set
Fragment Offset: 0

Packet 2)

Total Length: 548 B
Identification: 0xd58c (54668)
Flags: 0x01 (More Fragments)
0th bit(Reserved bit) is Not Set
1st bit(Don't fragment) is Not Set
2nd bit(More fragment) is Not Set
Fragment Offset: 1480

Exercise 4:

Q1) IP address of DHCP server is 10.129.1.53 and it is lisening on port 67.

Q2) No DHCP relay is involved in the forwarding. We can say this is so because the relay agent IP address is set to 0.0.0.0 in the offer packet.

Q3) DHCP server repiled to 10.129.26.130 . This is so because in the ARP discover packet, the client set the flag (in the header) to 0x0000 which signifies that it has an IP address and it wants to renew its lease.

Q4) The offered IP address to the client is 10.129.26.130 and it is valid for 10 minutes.

Q5) Additional information received from the dhcp server:
- a) DHCP server IP address
- b) IP address lease time
- c) Subnet mask
- d) Router IP address (Default Gateway)
- e) Domain name
- f) Domain name server

Exercise 5)
Q1) Type 0, Code 0 corresponds to Echo reply(Ping) and Type 8, Code 0 corresponds to Echo request(Ping)

The commands used for both of the above are:

First run tcpdump -n host 10.105.11.25 -w /tmp/ex5.out
and after this has started, run ping 10.105.11.25
After some time, close both!

First, an Echo request(Ping) packet is sent from my host(10.105.11.24) to 10.105.11.25
Then, an Echo reply(Ping) packet is received from 10.105.11.25 to my host(10.105.11.24)

Type 3, Code 3 corresponds to Destination port unreachable.
The commands used are:

First run tcpdump -n host 10.105.11.25 -w /tmp/socketex5.out
and after this has started, run ./sendUDP 10.105.11.25 2000
After some time, close both!

This happens because 10.105.11.25 is not listening on the port for UDP and thus we will get an ICMP from 10.105.11.25 which states that the Destination port is unreachable.

Exercise 6)

Q1)
tcpdump -w /tmp/exercise6.out

tracepath 10.129.1.153 -n

```
 1:  10.105.11.25                          0.081ms pmtu 1500
 1:  10.105.250.1                          1.184ms
 1:  10.105.250.1                          1.338ms
 2:  10.250.105.1                          1.549ms
 3:  192.0.20.2                           1.763ms
 4:  10.129.1.153                          2.615ms reached
    Resume: pmtu 1500 hops 4 back 61
```

Close tcpdump.

Q2)ICMP message has type 3, code 3 (destination unreachable (port unreachable)) and type 11, code 0 (TTL expiry).

Q3)
The host sends UDP segments to some destination (in this case, 10.129.1.153) with subsequent packets having TTL =1,2,3, ... and with unlikely destinatiomn ports (44444, 44445, 44446 and 44447 in our case).

As this packet goes to the subsequent routers, they decrease TTL by 1. If TTL becomes 0, then the router discards packet and sends an ICMP message back to the sender saying that TTL has expired (which includes router name and IP address). As a result, we can learn about which router the packet goes to after 1st, 2nd, 3rd, .. hops.

When the packet reaches the destination, it sends back an ICMP packet saying that the port is unreachable.
As a result, complete information about the path is now available.

Q4)The IP address of our machine's default router is 10.105.250.1