The Internet Protocol (IP) and Attacks

N3.1. Why do we need fragmentation?

N3.2. In IP fragmentation, the actual offset of a fragment is the value in the offset field multiplied by 8. Why is this multiplication needed?

N3.3. How do the receiver know which fragment is the last one?

N3.4. Without seeing the last fragment, can the receiver know the total size of the entire packet? Why or why not?

N3.5. Is it possible to spoof a packet with a size larger than `65535`, which is the up limit of the IP packet size (the length field in the IP header has only 16 bits)?

N3.6. If the MTU (Maximum Transmission Unit) of all the networks on the Internet is 1500, what is the largest IPv4 packet that one can send?

N3.7. We have a UDP packet, which contains 500 bytes of payload data. The MTU of the network is 200, so we need to conduct fragmentation. We decide to break the payload into three pieces of the following sizes: 160, 160, and 180. Please set the following field for each fragment. The ID field of the packet is 1234.

Fragment	ID	Flags	Offset	Total_length	Prototype
1	?	MF=?	?	?	?
2	?	MF=?	?	?	?
3	?	MF=?	?	?	?

N3.8. If a packet's 1st and 2nd fragments have already arrived, but the 3rd fragment never comes, the OS will deliver the 1st and 2nd fragments to the upper layer (transport layer). Is this true of false? Please explain.

N3.9. Please create two packets to emulate the Teardrop attack. Please write Python code.

N3.10. Please create two packets to emulate the Ping-of-Death attack. Please write Python code.

N3.11. The following routing entries show four routing rules and the corresponding interfaces. What interface will be used to route packets to (1) `192.200.60.5`, (2) `192.168.30.5`, (3) `192.168.60.5`, respectively? Please explain why.

```
A: 0.0.0.0/0         dev interface-a
B: 192.168.0.0/16    dev interface-b
C: 192.168.60.0/24   dev interface-c
D: 192.168.60.5/32   dev interface-d
```

N3.12. In some Ethernet frame that contains an IP packet, the destination MAC address in the Ethernet header and the destination IP address in the IP header are not the same computer. What is this scenario?

N3.13. What is reverse path filtering implemented by routers? What is the purpose of such a mechanism?

N3.14. What attack would allow an attacker to turn one attack packet into many? Please describe this attack in more details.

N3.15. How does a router know whether it should send out an ICMP redirect message or not?

N3.16. The following entries are the content of the routing tables on a host A and router R. When we send a packet to `93.184.216.34` from host A, will we see an ICMP redirect message from somewhere? If so, which machine would send out such a message? Assuming that all the computers involved are configured to allow ICMP redirect.

```
// On host A
default via 192.168.30.9 dev eth0
192.168.30.0/24 dev eth0 proto kernel scope link src 192.168.30.5
10.9.0.0/24 via 10.9.0.9 dev eth0

// On router R (192.168.30.9)
default via 192.168.30.1 dev eth0
192.168.30.0/24 dev eth0 proto kernel scope link src 192.168.30.9
10.9.0.0/24 dev eth1 proto kernel scope link src 10.9.0.9
```

N3.17. The setup is the same as Question N3.16. Please modify the routing table on host A, so there will be no more ICMP redirect message if we send out packets to `93.184.216.34`.

N3.18. Please describe how to use ICMP redirect message to launch MITM attacks.

N3.19. Can we use ICMP redirect attack to redirect the victim to send its packets to a remote machine (i.e., a machine outside of the LAN).