互联网协议（IP）及其攻击

N3.1. 为什么需要分片？

N3.2. IPv4 分片的实际字节偏移等于 Fragment Offset 字段乘以 8。为什么要以 8 字节为单位？

N3.3. 接收方如何知道哪个片段是最后一个片段？

N3.4. 在尚未收到最后一个分片时，接收方能否确定原始数据报的总长度？为什么？

N3.5. 能否利用分片让接收方尝试重组一个超过 65535 字节的 IPv4 数据报？IPv4 Total Length 字段只有 16 位，这种数据报是否合法？

N3.6. 假设路径上所有网络的 MTU 都是 1500，从分片字段可表示范围来看，一组分片最多能描述多大的重组数据报？这与合法 IPv4 长度上限有何关系？

N3.7. 某 UDP 数据报含 500 字节应用载荷，网络 MTU 为 200，需要分片。把应用载荷分成 160、160、180 字节三部分。已知 IP ID 为 1234，请填写每个分片的字段。注意首片还包含 8 字节 UDP 头。

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

N3.8. 若一个数据报的前两个分片到达，但第三个分片始终丢失，操作系统会把前两个分片交给传输层。这个说法对吗？请解释。

N3.9. 请创建两个数据包来模拟泪滴攻击。请编写 Python 代码。

N3.10. 请创建两个数据包来模拟 Ping-of-Death 攻击。请编写 Python 代码。

N3.11. 下列路由表包含四条规则及对应接口。发送到以下地址时分别会使用哪个接口？

（1） `192.200.60.5`

（2） `192.168.30.5`

（3） `192.168.60.5`

请解释原因。

```
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. 在抓到的某个 IP 数据包中，以太网头的目的 MAC 与 IP 头的目的 IP 并不属于同一台主机。这通常是什么场景？

N3.13. 什么是路由器实现的反向路径过滤？这样一个机制的目的是什么？

N3.14. 哪种攻击能把一个攻击数据包放大成多个响应包？请说明其原理。

N3.15. 路由器在什么情况下会发送 ICMP Redirect？

N3.16. 下列是主机 A 和路由器 R 的路由表。A 向 `93.184.216.34` 发送数据包时，会收到 ICMP Redirect 吗？若会，由哪台机器发送？假设相关主机和路由器都允许 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. 沿用问题 N3.16. 的设置，修改主机 A 的路由表，使它向 `93.184.216.34` 发送数据包时不再触发 ICMP Redirect。

N3.18. 说明攻击者如何利用伪造的 ICMP Redirect 发起中间人攻击。

N3.19. 能否用 ICMP Redirect 攻击让受害者把下一跳设置为局域网之外的远程主机？