MAC 层、ARP 及其攻击

N2.1. 混杂模式有什么用？

N2.2. MAC 地址如何被用于跟踪用户？

N2.3. 为什么环回接口被称为“环回”？

N2.4. loopback 接口与 dummy 接口有哪些相同点和不同点？

N2.5. 为什么 IPv4 局域网需要 ARP？

N2.6. 主机 `10.8.8.5/24` 尝试 ping `10.8.8.8`，并先发出 ARP 请求。该请求以太网头中的（1）目的 MAC 和（2）源 MAC 分别是什么？

N2.7. 主机 `10.8.8.5/24` 尝试 ping `10.8.8.8`，并先发出 ARP 请求。ARP 报文中下列字段分别是什么：（1）发送方 MAC；（2）发送方 IP；（3）目标 MAC；（4）目标 IP？

N2.8. 一台主机位于 `10.8.8.0/24`，默认路由器为 `10.8.8.1`。它 ping `93.184.216.34` 前会先发送 ARP 请求。该 ARP 请求的目标 IP 字段是什么？

N2.9. 主机 `10.8.8.5/24` 尝试 ping 同一子网中并不存在的 `10.8.8.100`。同一局域网的另一台计算机能嗅探到 ICMP Echo Request 吗？

N2.10. 主机 `10.8.8.5/24` 尝试 ping 互联网上并不存在的 `1.2.3.4`。`10.8.8.0/24` 中另一台嗅探主机能否看到发出的 ICMP Echo Request？

N2.11. 编写代码片段，伪造 ARP Request 以毒化主机 `10.8.8.5` 的 ARP 缓存。攻击机位于同一局域网。

N2.12. 编写代码片段，伪造 ARP Reply 以毒化主机 `10.8.8.5` 的 ARP 缓存。攻击机位于同一局域网。

N2.13. 编写代码片段，伪造 gratuitous ARP 消息以毒化主机 `10.8.8.5` 的 ARP 缓存。攻击机位于同一局域网。

N2.14. 能否直接从远程网络发起 ARP 缓存投毒攻击？请解释。

N2.15. 一份新闻报道称，XYZ 公司的网络受到了外部人员的攻击，这些外部人员显然是从远程计算机向公司网络发送大量欺骗性 ARP 请求/响应，尝试发起 ARP 缓存中毒攻击。请判断这是否属于不实报道。

N2.16. 在中间人攻击中，攻击者 M 想拦截并修改同一局域网内 A 发往 B 的数据包。M 需要完成哪些步骤？

N2.17. 在书中的中间人攻击中，M 用 ARP 缓存投毒把 A 发往 B 的数据包重定向到自己。(1) M 关闭 IP 转发时，原数据包会怎样？(2) M 开启 IP 转发时会怎样？(3) 若 M 要修改数据包，应开启还是关闭内核 IP 转发？

N2.18. 教材的中间人攻击中，攻击者 M 通过 ARP 缓存投毒把 A 发往 B 的报文重定向到 M。攻击程序如何取得该报文？

N2.19. 中间人攻击代码拦截并复制 A 发往 B 的报文后执行以下操作。为什么必须删除 IP 和 TCP 校验和字段？

```
newpkt = IP(bytes(pkt[IP]))
del(newpkt.chksum)
del(newpkt[TCP].chksum)
```

N2.20. 书中的中间人攻击代码嗅探 A 发往 B 的数据包时，在过滤器中使用 A 的 MAC 地址。能否改用 A 的 IP 地址？为什么？

N2.21. 机器 A、B、M 位于同一局域网，其 IP 与 MAC 地址如下。

```
A's IP:  10.9.0.5
B's IP:  10.9.0.6
M's IP:  10.9.0.9

A's MAC address: aa:bb:cc:dd:ee:05
B's MAC address: aa:bb:cc:dd:ee:06
M's MAC address: aa:bb:cc:dd:ee:09
```

M 上的攻击者希望利用 ARP 缓存投毒对 A、B 发起中间人攻击，拦截二者通信。请补全下列发送伪造 ARP Request 的程序。

```
# Constructing spoofed ARP request to Host A
ether1 = Ether(dst = ________________________)
arp1 = ARP(op=1)
arp1.psrc  = ____________________   # An IP address
arp1.hwsrc = ____________________   # An Ethernet address
arp1.pdst  = ____________________   # An IP address
sendp(____________________)

# Constructing spoofed ARP request to Host B
```

```
ether2 = Ether(dst = _________________________)
arp2 = ARP(op=1)
arp2.psrc  = ____________________
arp2.hwsrc = ____________________
arp2.pdst  = ____________________
sendp(__________________)
```