实验 3 - ARP

一. 实验目的

1. 学习 ARP 协议相关概念;
2. 学习 ARP 协议的工作原理;
3. 分析 ARP 请求响应数据包;

二. 实验环境

1. eNSP 网络环境仿真平台
2. wireShark 抓包工具
3. 网络测试仪
4. 华为实体路由器

三. 实验基本原理

概念

1. ARP （地址解析协议）

   > 根据 IP 地址获取物理地址

2. ARP 请求

   > 向局域网内的全部主机广播包含目标 IP 地址的 ARP 请求

3. ARP 响应

   > ARP 响应中携带了目标的物理地址

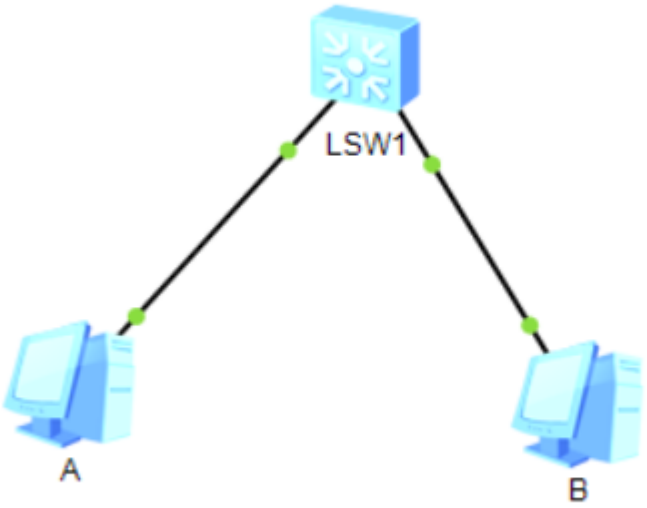
4. ARP 缓存

   > 主机收到 ARP 响应后会将 IP 地址与物理地址存入 ARP 缓存

四. 虚实联合仿真及结果分析

3.1

网络拓扑



查看主机 A ARP 表

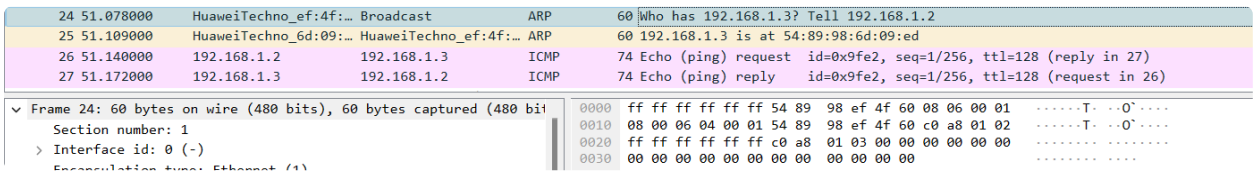
```
PC>arp -a

Internet Address      Physical Address      Type
192.168.1.3           54-89-98-6D-09-ED     dynamic

PC>
```

抓包分析 ARP 工作原理及相关数据报文

ARP 请求



请求报文分析

```
Ethernet II, Src: HuaweiTechno_ef:4f:60 (54:89:98:ef:4f:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: HuaweiTechno_ef:4f:60 (54:89:98:ef:4f:60)
      Address: HuaweiTechno_ef:4f:60 (54:89:98:ef:4f:60)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HuaweiTechno_ef:4f:60 (54:89:98:ef:4f:60)
    Sender IP address: 192.168.1.2
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.1.3
```

```
0000  ff ff ff ff ff ff 54 89  98 ef 4f 60 08 06 00 01   ····--··T· ··O`····
0010  08 00 06 04 00 01 54 89  98 ef 4f 60 c0 a8 01 02   ····--··T· ··O`····
0020  ff ff ff ff ff ff c0 a8  01 03 00 00 00 00 00 00   ···--··· ····--··
0030  00 00 00 00 00 00 00 00  00 00 00 00              ···--··· ····
```

```
0000   ff ff ff ff ff ff 54 89 98 ef 4f 60 08 06 00 01
......T...O`....
0010   08 00 06 04 00 01 54 89 98 ef 4f 60 c0 a8 01 02
......T...O`....
0020   ff ff ff ff ff ff c0 a8 01 03 00 00 00 00 00 00
................
0030   00 00 00 00 00 00 00 00 00 00 00 00                ............
```

以太网头部 Ethernet II

- 目的 MAC 地址：前 48 bits `ff ff ff ff ff ff`

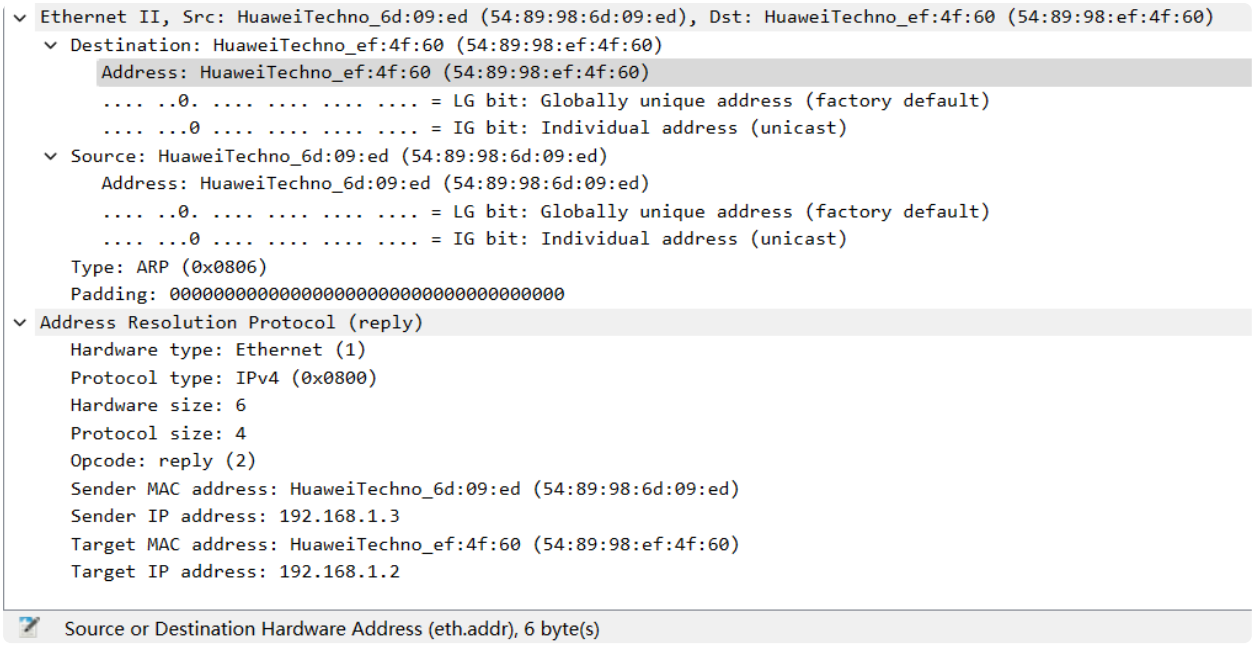
  > 广播！🤡

- 源 MAC 地址：`54 89 98 ef 4f 60`
- 请求类型：ARP `08 06`

IP 头部

- Hardware type：`00 01` Ethernet (1)
- 协议类型：`08 00` IPv4
- ...

响应报文分析




```
0000   54 89 98 ef 4f 60 54 89 98 6d 09 ed 08 06 00 01
T...O`T..m......
0010   08 00 06 04 00 02 54 89 98 6d 09 ed c0 a8 01 03
......T..m......
0020   54 89 98 ef 4f 60 c0 a8 01 02 00 00 00 00 00 00
T...O`..........
0030   00 00 00 00 00 00 00 00 00 00 00 00                ............
```

以太网头部 Ethernet II

- 目的 MAC 地址：前 48 bits `54 89 98 ef 4f 60`

  > 发送 ARP 请求的源 MAC 地址！👍

- 源 MAC 地址：`54 89 98 6d 09 ed`
- 请求类型：ARP `08 06`

删除 ARP 表项

```
From 192.168.1.2: Destination host unreachable
From 192.168.1.3: bytes=32 seq=1 ttl=128 time=62 ms
From 192.168.1.3: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.3: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.3: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.3: bytes=32 seq=5 ttl=128 time=62 ms

--- 192.168.1.3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/49/62 ms

PC>arp -a

Internet Address      Physical Address      Type
192.168.1.3           54-89-98-6D-09-ED     dynamic

PC>arp -d


PC>arp -a

Internet Address      Physical Address      Type

PC>
```

3.2.1

假如公司某部门的一台交换机上连接了 3 位员工的 PC (A, B, C)

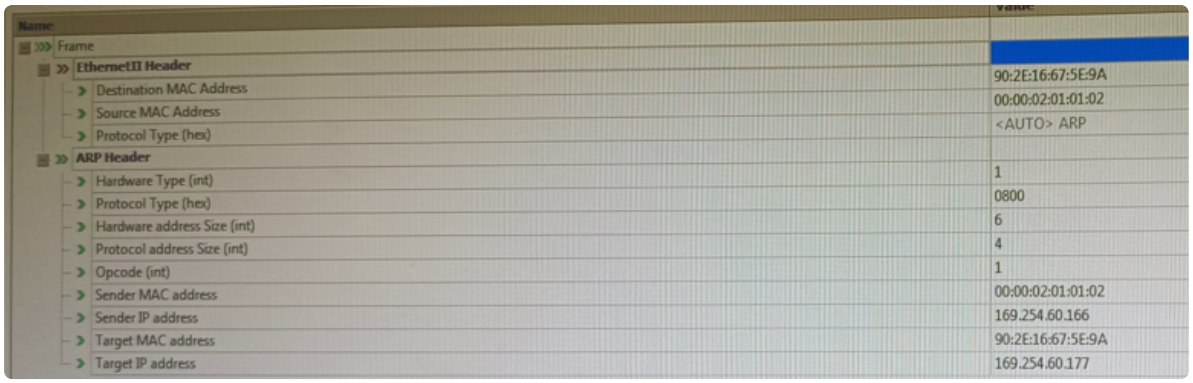
1. 模拟一次 ARP 欺骗的过程

借助 Renix, 网络测试仪, 交换机来模拟 ARP 欺骗的过程:

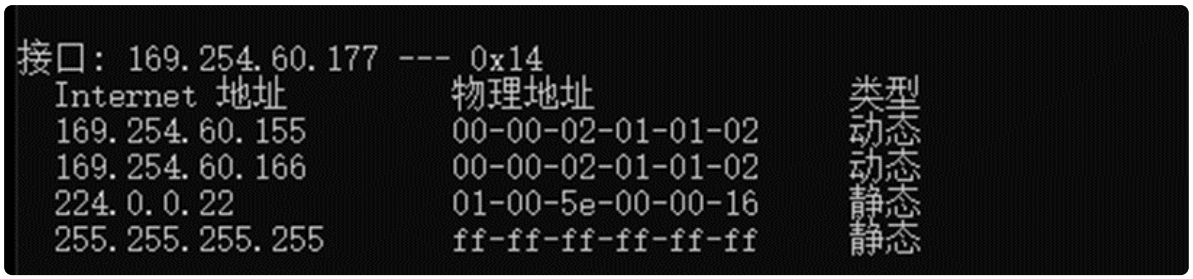
1. Renix 预约 3 个端口;
2. 接线, 将预约的三个端口接线至路由器, 路由器需要一个额外接口接线至个人 PC;
3. 为 3 个端口添加接口;
4. 1 号与 2 号接口作为虚拟 PC A, PC B, 3 号接口 IP 与 MAC 地址配置需要与个人 PC 一致, 作为 PC C;
5. 验证各接口之间能够互相通信;
6. 启动各接口 ARP/ND 学习, 测试个人 PC 与虚拟主机之间的通信, 检查 ARP 表项;

```
接口: 169.254.60.177 --- 0x14
  Internet 地址         物理地址              类型
  169.254.60.155        00-00-02-01-01-02     动态
  169.254.60.166        00-00-02-01-01-03     动态
  224.0.0.22            01-00-5e-00-00-16     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

7. 建立用于欺骗的 ARP 响应流；



8. 启动流；
9. 检查个人 PC ARP 表项，检查是否欺骗成功。



> 🚨 可以发现 Internet 地址 `169.254.60.166` 对应的物理地址修改为 `169.254.60.155` 实际对应的 IP 地址，即欺骗成功！

2. 配置防范 ARP 欺骗的安全策略

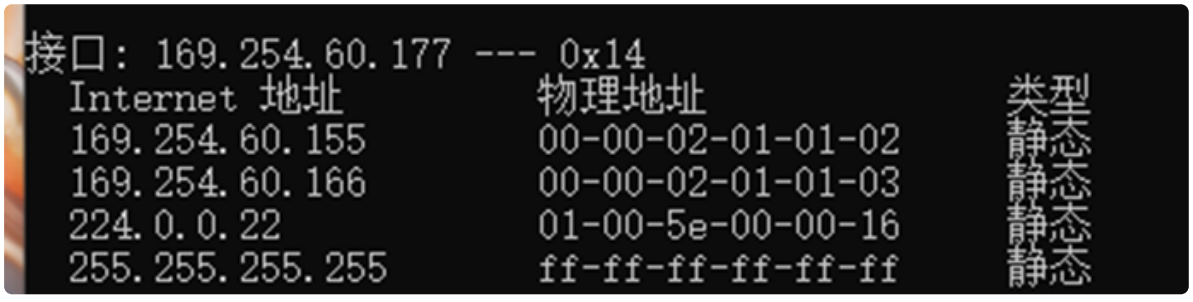
1. 配置静态 ARP 表项

```
netsh -c "i i" add neighbors 20 169.254.60.166 00-00-02-01-01-03
```

```
![[Pasted image 20240602003536.png]]
```

3. 验证配置的安全策略是否有效

1. 个人 PC 配置静态 ARP 表项；
2. 启动用于欺骗的 ARP 响应流；
3. 检查个人 PC ARP 表项，检查是否欺骗成功。



> 🚨 可以发现 Internet 地址 `169.254.60.166` 对应的物理地址没有修改为 `169.254.60.155` 实际对应的 IP 地址，即欺骗失败，安全策略有效!

3.2.2

1. 模拟一次 ARP 泛洪攻击

1. 建立用于泛洪攻击的 ARP 响应流；

2. 启动流，进行 ARP 泛洪攻击；
3. 检查个人 PC ARP 表项，查看是否被泛洪攻击。

😳 可以发现个人 PC 的 ARP 表项已经被泛洪攻击，产生了一堆的垃圾表项！

```
  169.254.64.87         00-00-fb-f8-5d-cf     动态
  169.254.64.88         00-00-4a-52-c7-89     动态
  169.254.64.89         00-00-21-bb-c3-be     动态
  169.254.64.90         00-00-c0-d7-c9-03     动态
  169.254.64.91         00-00-86-29-ff-57     动态
  169.254.64.92         00-00-5a-a7-5e-36     动态
  169.254.64.93         00-00-28-d6-d9-e8     动态
  169.254.64.94         00-00-3d-94-ca-48     动态
  169.254.64.95         00-00-b9-68-7a-cb     动态
  169.254.64.96         00-00-fc-35-64-f2     动态
  169.254.64.97         00-00-3c-0c-75-34     动态
  169.254.64.98         00-00-dd-50-72-b2     动态
  169.254.64.99         00-00-6b-dd-bf-a8     动态
  169.254.64.100        00-00-7f-51-da-2f     动态
  169.254.64.101        00-00-1a-15-38-e7     动态
  169.254.64.102        00-00-b5-5a-ef-c2     动态
  169.254.64.103        00-00-27-7f-d6-5a     动态
  169.254.64.104        00-00-19-0e-97-d6     动态
  169.254.64.105        00-00-5e-ff-5a-50     动态
  169.254.64.106        00-00-62-15-de-78     动态
  169.254.64.107        00-00-cd-29-be-ea     动态
  169.254.64.108        00-00-57-0c-77-6d     动态
  169.254.64.109        00-00-f0-3d-af-5b     动态
  169.254.64.110        00-00-e2-22-56-7e     动态
  169.254.64.111        00-00-dd-f1-16-3f     动态
  169.254.64.112        00-00-62-d9-c5-27     动态
  169.254.64.113        00-00-db-47-7e-68     动态
  169.254.64.114        00-00-1b-fc-20-d6     动态
  169.254.64.115        00-00-97-79-c4-2e     动态
  169.254.64.116        00-00-48-99-9f-f9     动态
  169.254.64.117        00-00-fc-44-ae-2b     动态
  169.254.64.118        00-00-3d-31-78-d5     动态
  169.254.64.119        00-00-ce-34-ce-6c     动态
  169.254.64.120        00-00-48-17-23-e6     动态
  169.254.64.121        00-00-e7-ad-91-04     动态
  169.254.64.122        00-00-b9-cd-bd-46     动态
  169.254.64.123        00-00-e1-bd-ac-17     动态
  169.254.64.124        00-00-db-54-05-84     动态
  169.254.64.125        00-00-08-80-8e-97     动态
  169.254.64.126        00-00-67-08-77-0f     动态
  169.254.64.127        00-00-97-72-5d-da     动态
  169.254.64.128        00-00-46-44-65-14     动态
  169.254.64.129        00-00-c5-c4-5b-06     动态
  169.254.64.130        00-00-de-b9-d6-dc     动态
  169.254.64.131        00-00-5c-d0-f9-e0     动态
  169.254.64.132        00-00-11-5a-fe-fc     动态
  169.254.64.133        00-00-e9-ab-21-b5     动态
  169.254.64.134        00-00-46-92-ff-88     动态
  169.254.64.135        00-00-dc-47-5d-9d     动态
  169.254.64.136        00-00-09-fd-f0-1a     动态
  169.254.64.137        00-00-91-aa-10-dd     动态
  169.254.64.138        00-00-2e-cb-9f-55     动态
  169.254.64.139        00-00-89-0b-b7-fd     动态
  169.254.64.140        00-00-92-5e-f1-a4     动态
  169.254.64.141        00-00-3c-a5-e6-a2     动态
  169.254.255.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

2. 防ARP泛洪攻击

攻击行为

当网络中出现过多的 ARP 报文时，会导致网关设备 CPU 负载加重，影响设备正常处理用户的其它业务。另一方面，网络中过多的 ARP 报文会占用大量的网络带宽，引起网络堵塞，从而影响整个网络通信的正常运行。

安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- ARP 表项限制 设备基于接口限制学习 ARP 表项的总数目，可以有效地防止 ARP 表项溢出，保证 ARP 表项的安全性。
- ARP 速率抑制 设备对单位时间内收到的 ARP 报文进行数量统计，如果 ARP 报文的数量超过了配置的阈值，超出部分的 ARP 报文将被忽略，设备不作任何处理，有效防止 ARP 表项溢出。
- ARP表项严格学习 设备仅学习本端发送的 ARP 请求报文的应答报文，并不学习其它设备向交换机发送的 ARP 请求报文和非本端发送的 ARP 请求报文的应答报文，可以拒绝掉 ARP 请求报文攻击和非自己发送的 ARP 请求报文对应的应答报文攻击。
- ARP 端口级防护 设备基于端口对 ARP 上送速率进行监控，当某端口 ARP 上送控制面报文速率超过特定阈值时，会将该端口的 ARP 报文通过单独通道上送控制面，避免攻击影响正常的 ARP 报文。此外，设备还支持将攻击端口的 ARP 报文阻塞一段时间，而不是通过单独的通道上送。
- ARP用户级防护 设备对用户（基于 MAC 地址或者 IP 地址）上送控制面的 ARP 报文速率进行监控，当某用户 ARP 报文速率超过特定阈值时，会将该用户 ARP 报文丢弃一段时间。