# 网络协议分析

**课内实验：ARP欺骗流程**

实验时间：2020.10.15

目录

[网络协议分析 1](#_Toc53697652)

[一、ARP欺骗原理 2](#_Toc53697653)

[二、ARP欺骗实现的方法 2](#_Toc53697654)

[三、ARP欺骗的实现过程 4](#_Toc53697655)

[前提介绍： 4](#_Toc53697656)

[模拟方式： 5](#_Toc53697657)

[四、ARP欺骗的结果 6](#_Toc53697658)

[五、实验思考 8](#_Toc53697659)

杭州电子科技大学

网络空间安全学院

廖越强 18271422

## 一、ARP欺骗原理

在基于以太网技术的局域网中，ARP协议是建立在主机之间相互信任的基础上的，ARP协议虽然是一个高效的数据链路层协议，但同时也是一个“无状态”协议，并且存在以下可以利用的缺陷：

ARP高速缓存表根据所接收到的ARP协议包随时进行动态更新

ARP协议没有连接的概念，即任意主机即使在没有ARP请求的时候也可以进行作答

ARP协议没有认证机制，只要接收到的协议包格式是正确的，主机就会毫无条件地根据协议包内容刷新本机ARP缓存，并不检查该协议包的合法性。

那么根据ARP协议的这些缺陷，用来进行ARP欺骗的的发包形式主要有两种：

a. 假冒ARP reply（单播）

b. 假冒ARP request（广播）

由于ARP欺骗在中间人攻击中会导致ip地址冲突，并且是广播包，容易暴露攻击行为，所以在实际的基于ARP欺骗的中间人攻击中极少使用，一般都是针对特定的主机。

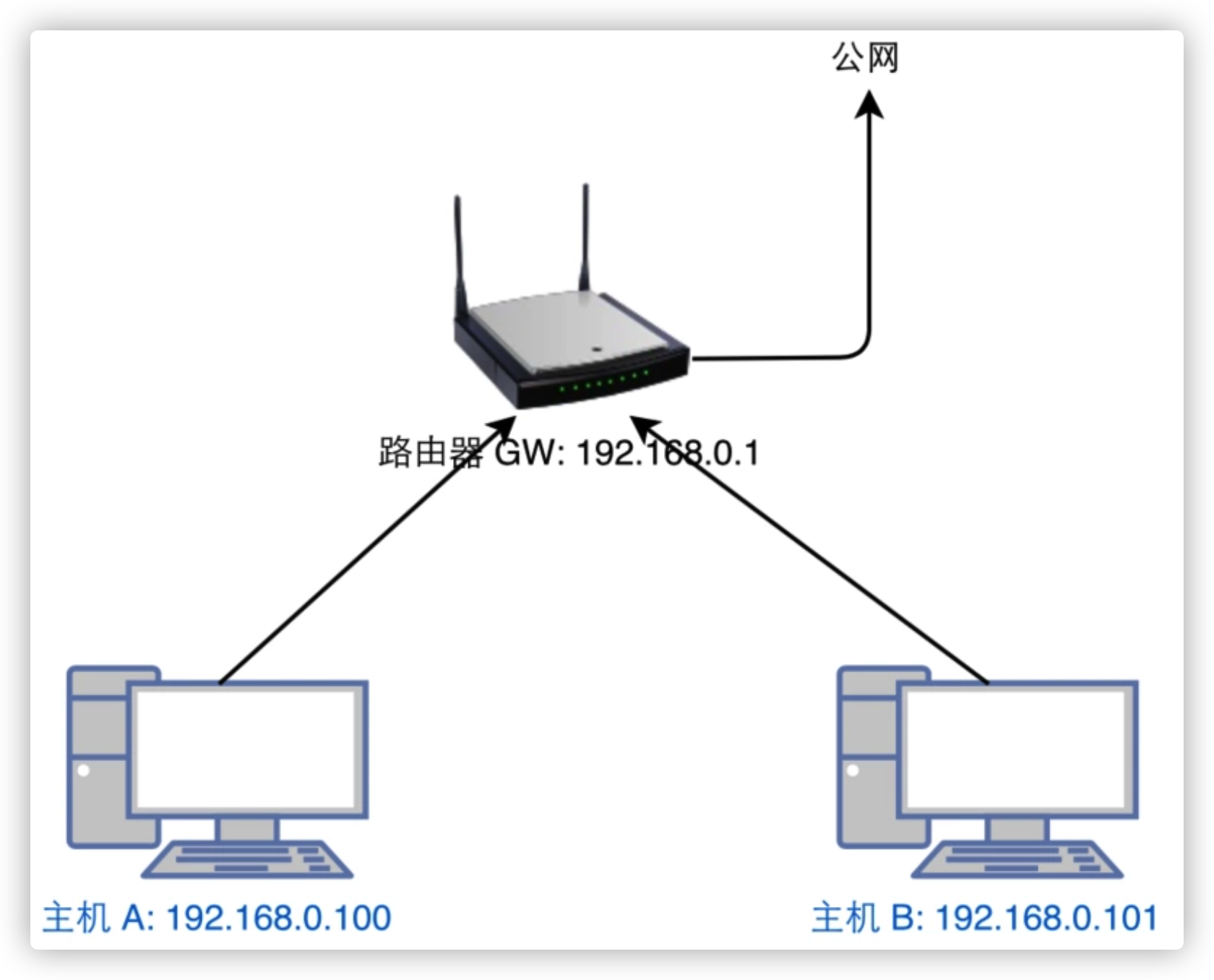
ARP欺骗攻击的**核心思想**就是向目标主机发送伪造的ARP应答，用伪造的ip-mac地址之间的映射更新目标主机的ARP缓存

## 二、ARP欺骗实现的方法

ARP欺骗是一种以ARP地址解析协议为基础的一种网络攻击方式，那么什么是ARP地址解析协议呢？

首先我们要知道，一台电脑主机要把以太网数据帧发送到同一局域网的另外一台主机，它的底层是通过48bit的Mac地址来确定目的接口的，但是我们在应用层是使用IP地址来访问目标主机的，所以ARP的作用就是当一台主机访问一个目标IP地址的时候，它为该主机返回目标IP主机的Mac地址，并且这个过程是自动完成的，应用层的程序是不用关心这件事的.

在讲ARP欺骗之前我们先来了解一下正常情况下一台主机是如何通过路由器上网的:



如上图，我们以A主机ping 8.8.8.8为例:

1.主机A上执行ping 8.8.8.8

2.主机A准备根据默认路由将数据包发送给192. 168.0.1，但是最开始的时候主机A不知道

192.168.0.1的Mac地址，所以主机A广播一条ARP Request，询问192.168.0.1的Mac地址是什么

3.路由器收到该ARP请求，发现自己是192.168.0.1于是向主机A回复一条ARP Reply，告诉主机A192.168.0.1的Mac地址是xxxGW.

4.主机A收到该ARP Reply，并使用该Reply中的MAC地址封一个ICMP Request包，然后将包发出去

5.路由器收到该ICMP包，发现目标IP是公网IP，便将该包放送到公网，公网返回ICMP Reply给路由器

6.路由器准备将ICMP Reply发送给192. 168.0.100，但是同第2步，路由器最开始的时候也不知道

192.168.0.100的Mac地址是多少，所以路由器会广播一条ARP Request，询问192. 168.0.100的Mac地址是什么

7.主机A收到ARP Request，发现自己是192.168.0.100，于是向路由器回复ARP Reply，告诉路由器192.168.0.100的Mac地址是xxxA.

8.路由器收到ARP Reply，并使用该Reply中的MAC地址将第5步收到ICMP Reply包重新封包，并发送出去

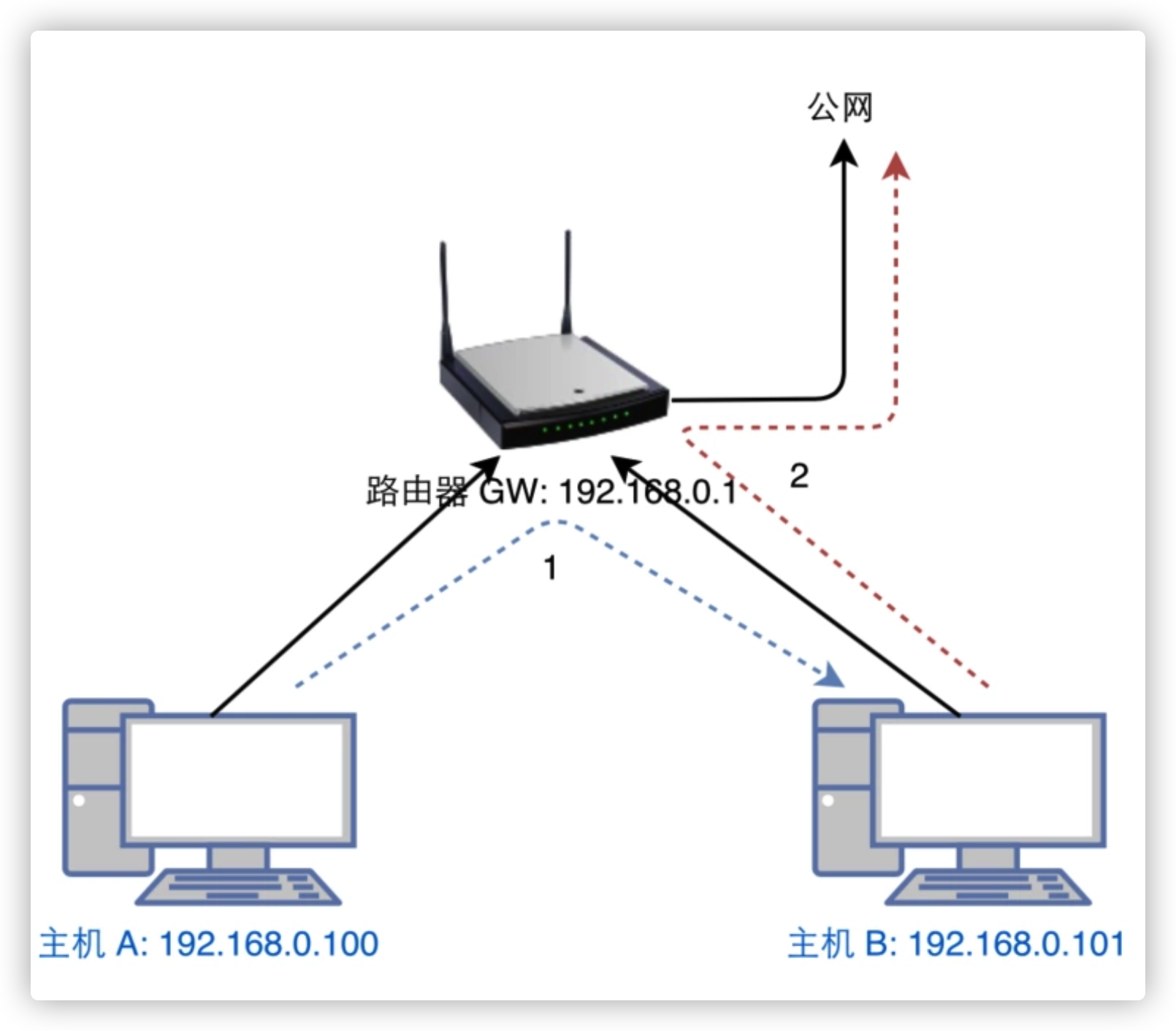
9.主机A收到ICMP Reply

至此，正常的上网流程结束.然后对照上面的流程回答下面两个问题:

1.如果主机B无脑的向主机A发送ARP Reply， 告诉A 192.168.0.1的MAC是xxxB，会发生什么？

2.如果主机B无脑的向路由器GW发送ARP Reply，告诉GW 192.168.0.100的MAC是xxxB，会发生什么？

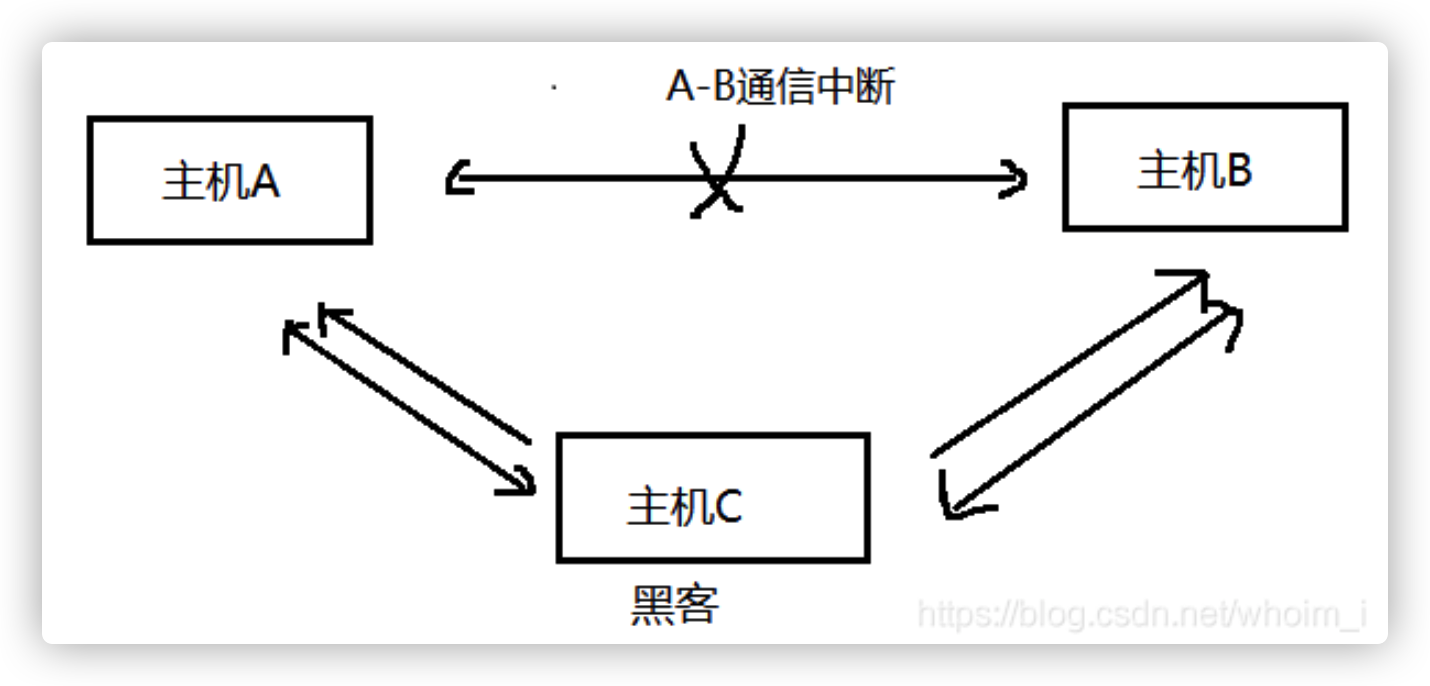
答案如下图:



如果主机B做了.上面说的两件事的话，那么主机A访问网络的所有数据都会先经过主机B，并且回来的数据也都会经过B，至此，整个ARP欺骗完成.

综合下来，就是正常的一次ARP请求报文被不怀好意的终端截取到并将所请求IP的MAC地址和黑客终端的MAC终端绑定在一起，以致于请求用户想要访问或者发送给正常对象时候被黑客给获取，达到欺骗的效果。

图解：



## 三、ARP欺骗的实现过程

现假设网络中有三台主机A,B,C。主机A,B为合法主机，C为攻击者。攻击分为三个步骤：

攻击者利用ARP欺骗，将自己插入到两台合法主机的通信路径中间。主机A,B间通讯变为A<——>C<——>B。

截获两台合法主机间通信的数据，根据自己情况过滤或者修改，为了保证A,B两台主机的通信，转发被捕获的数据。

**在本次实验中，ARP请求包和应答包的更改假设已经单播发送到访问用户的终端上，即本次实验不涉及ARP请求包与应答包的发送和收取，而改为正常访问用户更改本地的ARP缓存表来模拟被攻击之后的结果。**

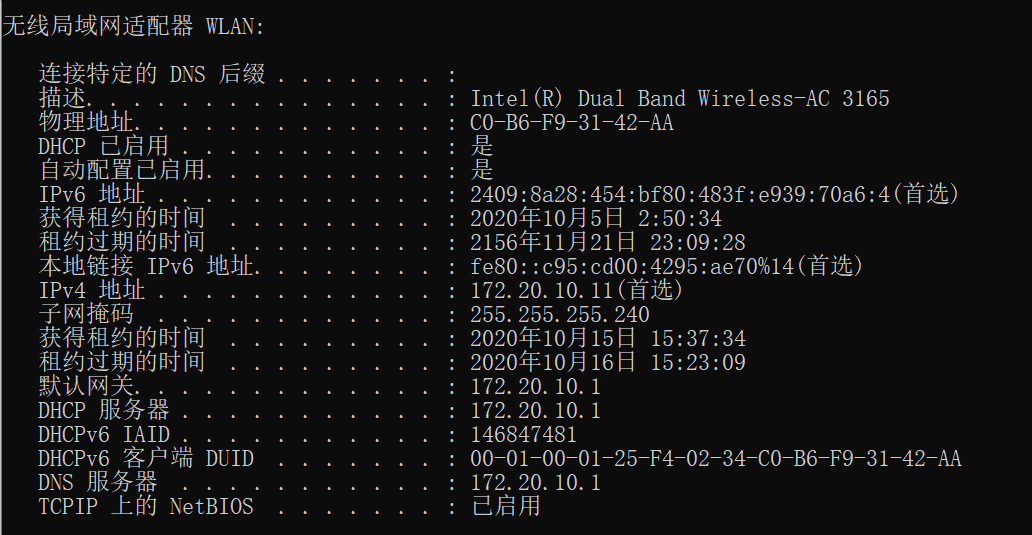
### 前提介绍：

**普通用户IP：172.20.10.12**

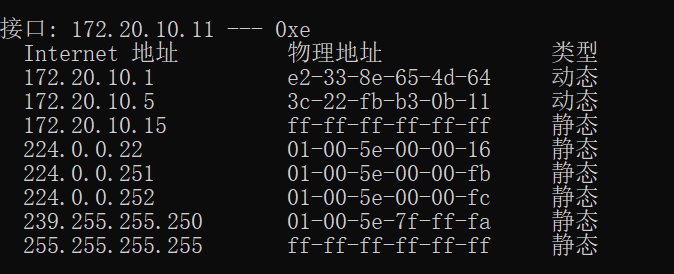
**被攻击者IP：172.20.10.5**

**攻击者IP：172.20.10.11**

**攻击者MAC相关信息：**



**被攻击者所在网段：**



### 模拟方式：

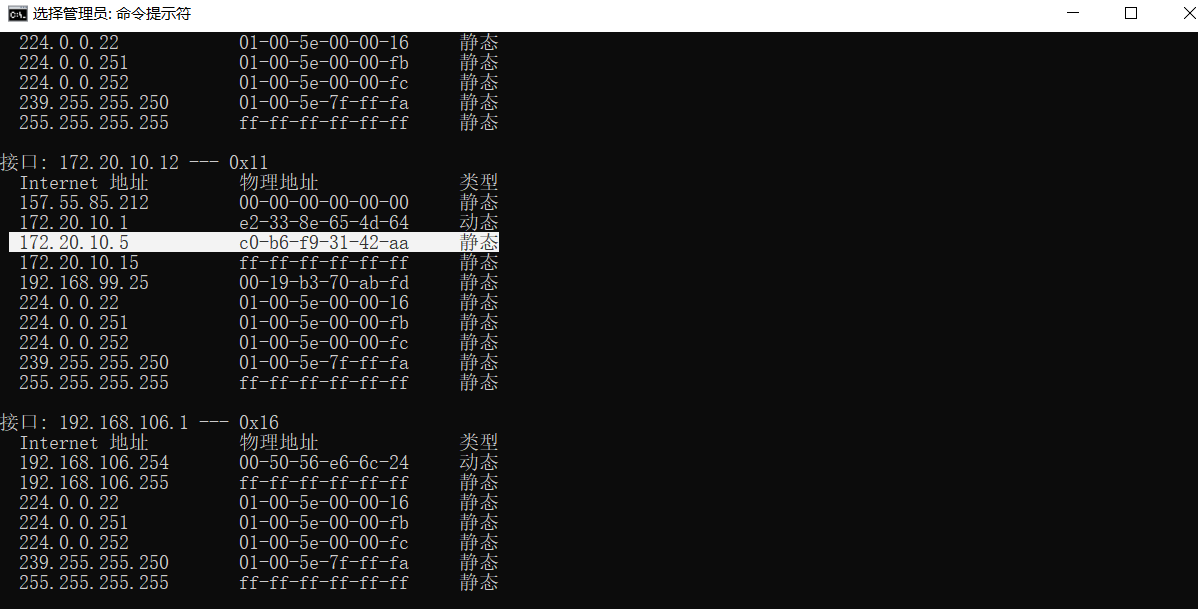
**普通用户加入一条静态命令**

**ARP -s [被攻击者IP] [攻击者MAC地址]**

**在本次实验为**

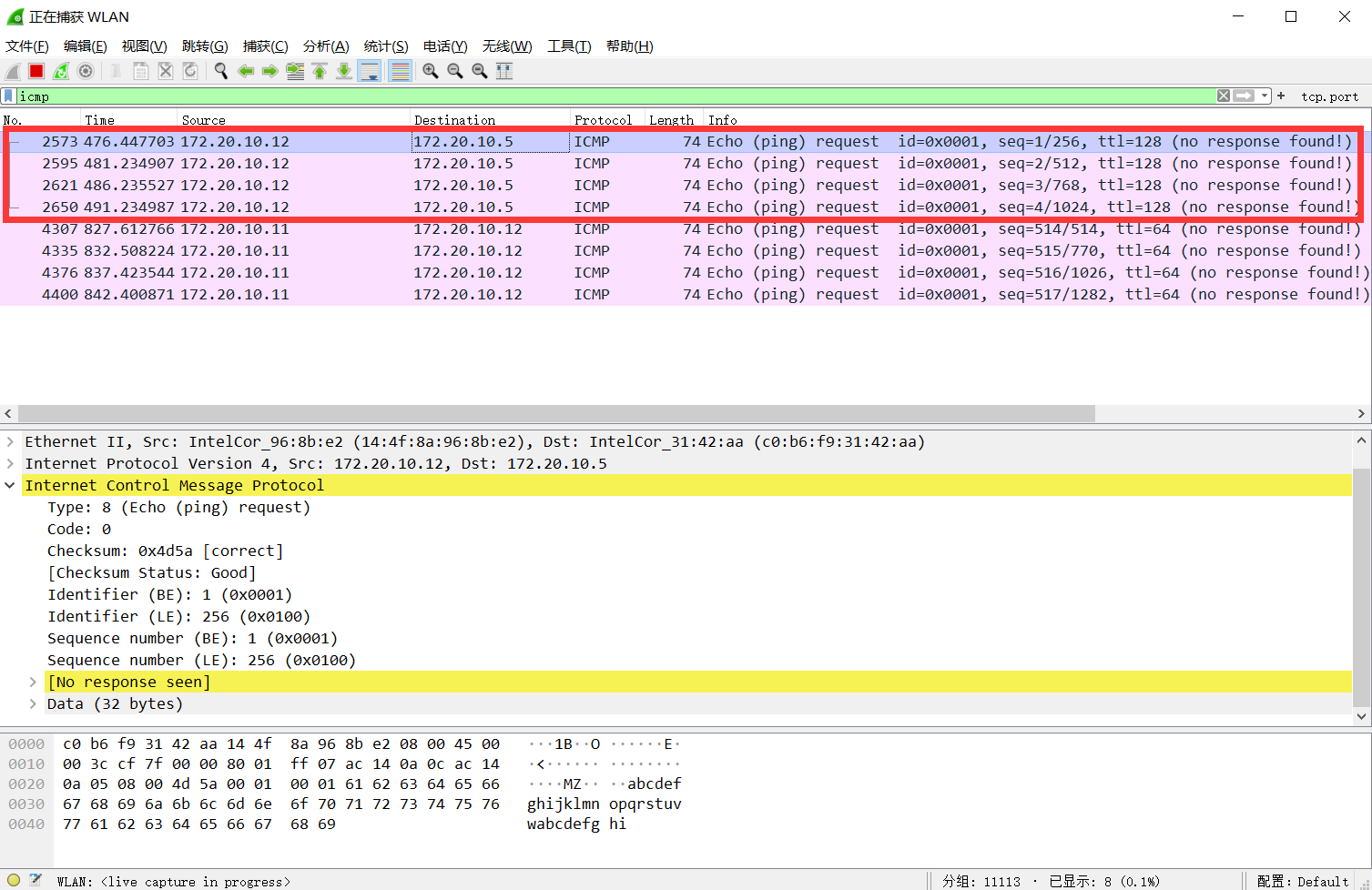
**ARP-s 172.20.10.5 C0-B6-F9-31-42-AA。**

**添加之后，正常访问用户的ARP缓存表如下**

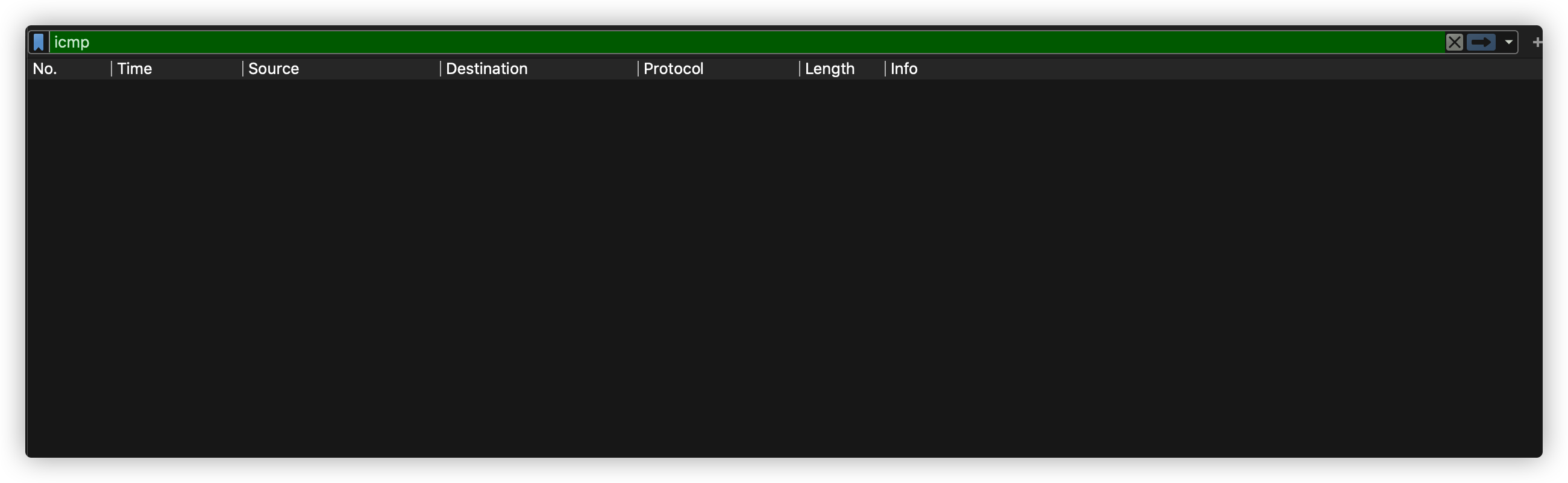
****

## 四、ARP欺骗的结果

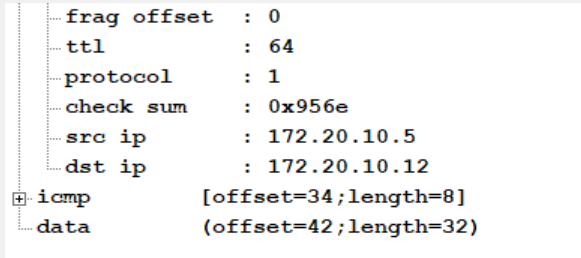
#### 1. 通过正常用户Ping访问被攻击者IP，在攻击者的Wireshark发现对应ICMP包：



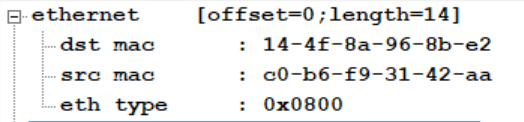
**同时，在被攻击方没有任何回应：**

****

#### 2. 攻击方伪造IP为被攻击者的报文，返回给普通用户

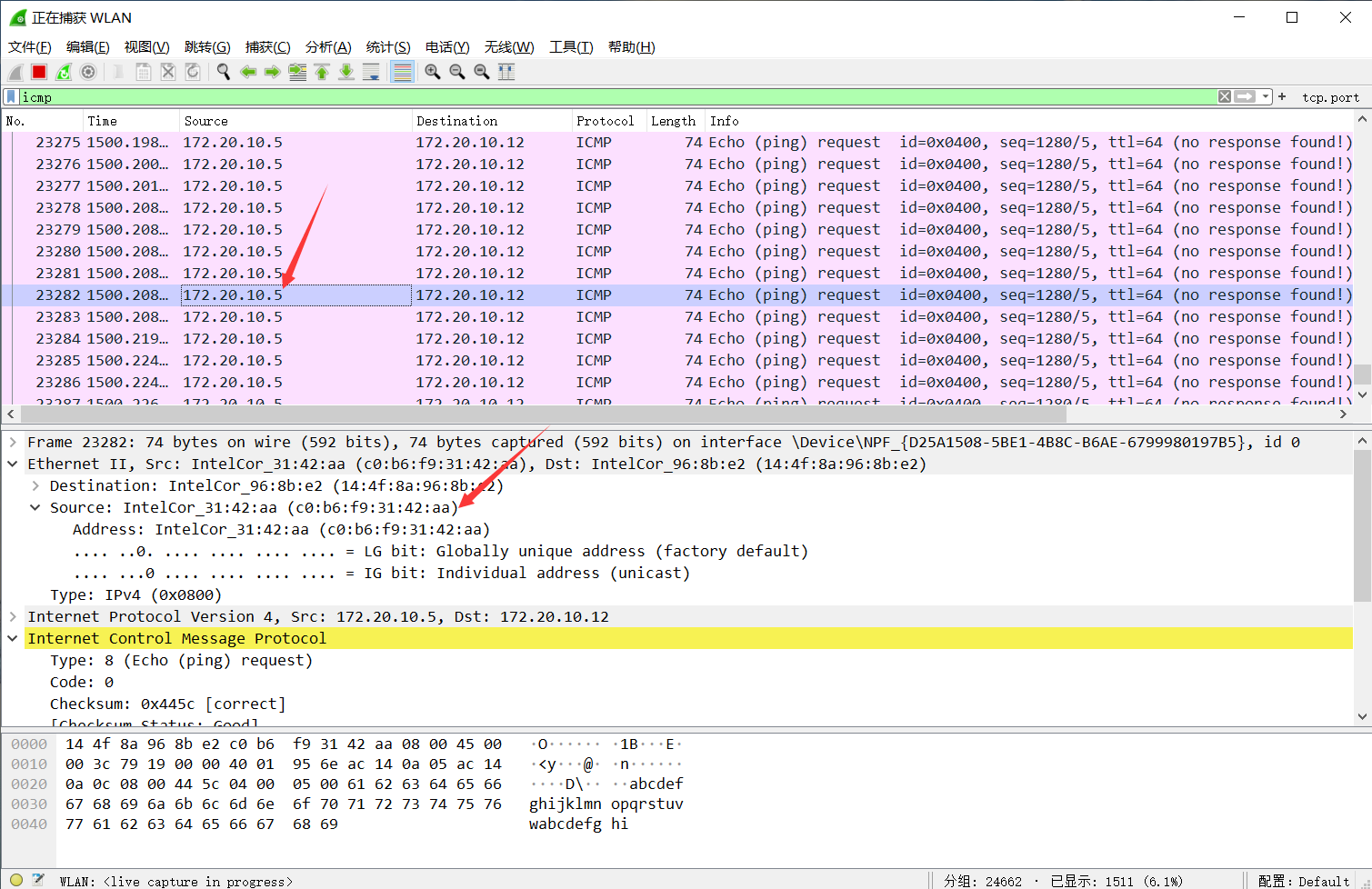


**源地址为被攻击者IP，目的地址为普通用户IP**



**源MAC地址为攻击者MAC地址，目的MAC地址为普通用户的MAC地址**

#### 3. 在普通用户通过Wireshark抓包，发现伪造的Ping请求：

****

**至此，实验模拟完成。**

## 五、实验思考

ARP攻击伴随ARP协议的诞生就一直困扰着人们。目前，为了解决ARP欺骗给局域网安全带来的严重问题，前辈们已经做了很多具有实践意义的工作。总体来说，由于动态表更新存在诸多问题，所以可以采取以下措施：

#### 1. 设置静态的ARP缓存

在计算机上使用ARP-s命令添加静态ARP缓存记录。若攻击者向主机发送ARP应答报文，目标机接收报文后并不会刷新ARP缓存表。从而避免了ARP欺骗的发生。这种方法在一定程度上限制了数据包的捕获以及冒充网关的欺骗攻击行为，但存在着以下局限性：

a：需要网络管理员手动设定静态ARP缓存，这无疑增加了网管员的工作量，而且不够灵活较为刻板。当主机自动获取到另一个ip地址或者更换新的网卡后，网络管理员不得不重新设定ip-mac绑定

b：攻击者可以对ARP病毒进行优化，通过相应的代码，破幻网络管理员在各种终端设备上所做的ip-mac绑定

c：ARP静态缓存的主要作用是使相关的主机与路由对于有关的ARP数据包不予理会，但攻击者仍然可以通过泛洪的方式发出数据包，这样就会造成内网拥塞，影响数据的正常传输。

#### 2. 使用ARP服务器

在ARP服务器中保存局域网服务器中各主机的ip地址和mac地址的映射信息，同时禁用各主机的ARP应答，保留服务器对ARP请求的应答。它的致命缺点就是一定要保证ARP服务器的安全，不然ARP服务器一旦被攻陷，后果不堪设想。

#### 3. 采用ARP防火墙

现在很多杀毒软件制造商都设计出了个人ARP防火墙模块，该模块也是通过绑定主机和网关等其他方式，来避免遭受攻击者所冒充的家网关攻击。在一定程度上可以防御ARP欺骗攻击。