

# 实验一 ARP 模拟攻击测试与防护

## 实验目的：

- 1、在不影响网络安全可靠运行的前提下，对网络中不同类型的协议数据进行捕获；
- 2、能对捕获到的不同类型协议数据进行准确的分析判断，发现异常；
- 3、快速有效地定位网络中的故障原因，在不投入新的设备情况下解决问题；
- 4、熟悉协议封装格式及原理，明确网络协议本身是不安全的。

## 实验要求：

- 1、复习网络层次及协议对应关系，协议封装，重点对 ARP 协议数据结构进行分析；
- 2、工具及软件选用：安装 Sniffer Pro 软件、捕获前的设置；
- 3、捕获 ARP 协议数据，并进行分析；
- 4、明确 ARP 协议的缺陷，制定模拟 ARP 攻击方法；
- 5、实施 ARP 协议模拟攻击与攻击结果检查；
- 6、确定 ARP 攻击流量并加以分析；
- 7、针对此类攻击的防范。

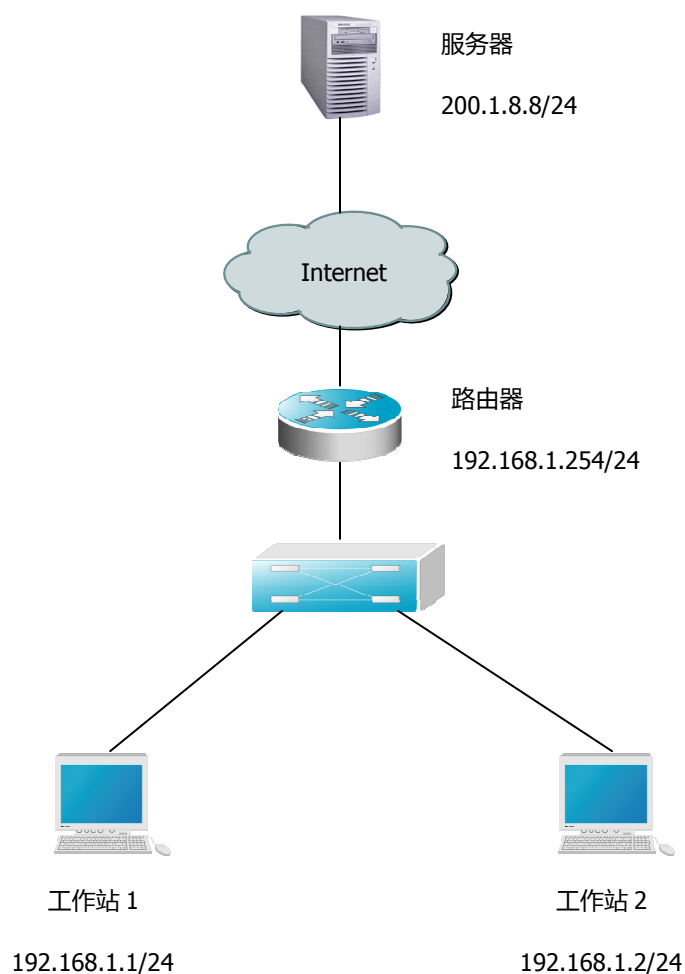
## 实验工具与软件：

- 1、协议分析软件 Sniffer portable；
- 2、S2126G（一台）；PC 机（三台）；R1700（一台）；直连线（4 条）

## 实验原理：

在以太网同一网段内部，当一个基于 TCP/IP 的应用程序需要从一台主机发送数据给另一台主机时，它把信息分割并封装成包，附上目的主机的 IP 地址。然后，寻找 IP 地址到实际 MAC 地址的映射，这需要发送 ARP 广播消息。当 ARP 找到了目的主机 MAC 地址后，就可以形成待发送帧的完整以太网帧头（在以太网中，同一局域网内的通信是通过 MAC 寻址来完成的，所以在 IP 数据包前要封装以太网数据帧，当然要有明确的目的主机的 MAC 地址方可正常通信）。最后，协议栈将 IP 包封装到以太网帧中进行传送。

## 实验拓扑



### 实验详细过程描述

在拓扑图中，当工作站 1 要和工作站 2 通信（如工作站 1 Ping 工作站 2）时。工作站 1 会先检查其 ARP 缓存内是否有工作站 2 的 MAC 地址。如果没有，工作站 1 会发送一个 ARP 请求广播包，此包内包含着其欲与之通信的主机的 IP 地址，也就是工作站 2 的 IP 地址。当工作站 2 收到此广播后，会将自己的 MAC 地址利用 ARP 响应包传给工作站 1，并更新自己的 ARP 缓存，也就是同时将工作站 1 的 IP 地址/MAC 地址对保存起来，以供后面使用。工作站 1 在得到工作站 4 的 MAC 地址后，就可以与工作站 2 通信了。同时，工作站 1 也将工作站 4 的 IP 地址/MAC 地址对保存在自己的 ARP 缓存内。

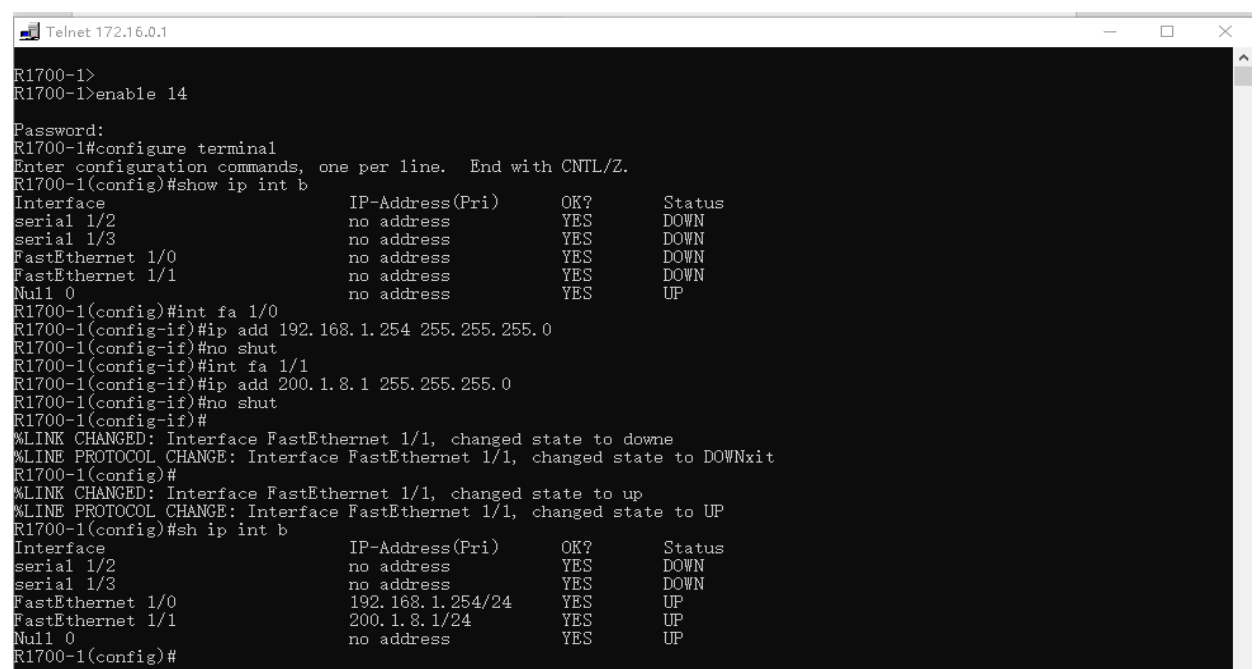
如果想查看 ARP 缓存中的所有记录，可以在用命令 `arp -a`，如果想清除 ARP 缓存中的动态记录，可以在用命令 `arp -d`。

ARP 攻击的特点是：当同一局域网内的一台或多台计算机感染了 ARP 攻击程序后，会不断发送伪造的 ARP 攻击包，如果这个攻击包的源 MAC 地址伪造为一个假的 MAC 地址（M1），源 IP 伪造成网关的 IP 地址，目的 MAC 为广播地址。这样所有同一网段内的主机都会收到，误以为网关的 MAC 地址已经变为 M1，于是进行 ARP 缓存更新，把网关的真实 IP 与这个假的 MAC 地址进行关联。当这些被攻击的主机想进行外部网络访问时会把数据送到网关，即封装网关的 IP 与 MAC，主机会先查询本机内的 ARP 缓存记录，查找网关 IP 对应的 MAC 地址，由于这个 MAC 是假的，所以外发的数据无法送达网关。因此，造成的现象就是被攻击的主机无法访问外网或互联网。

实验前的准备工作：

### 1、 搭建实验环境

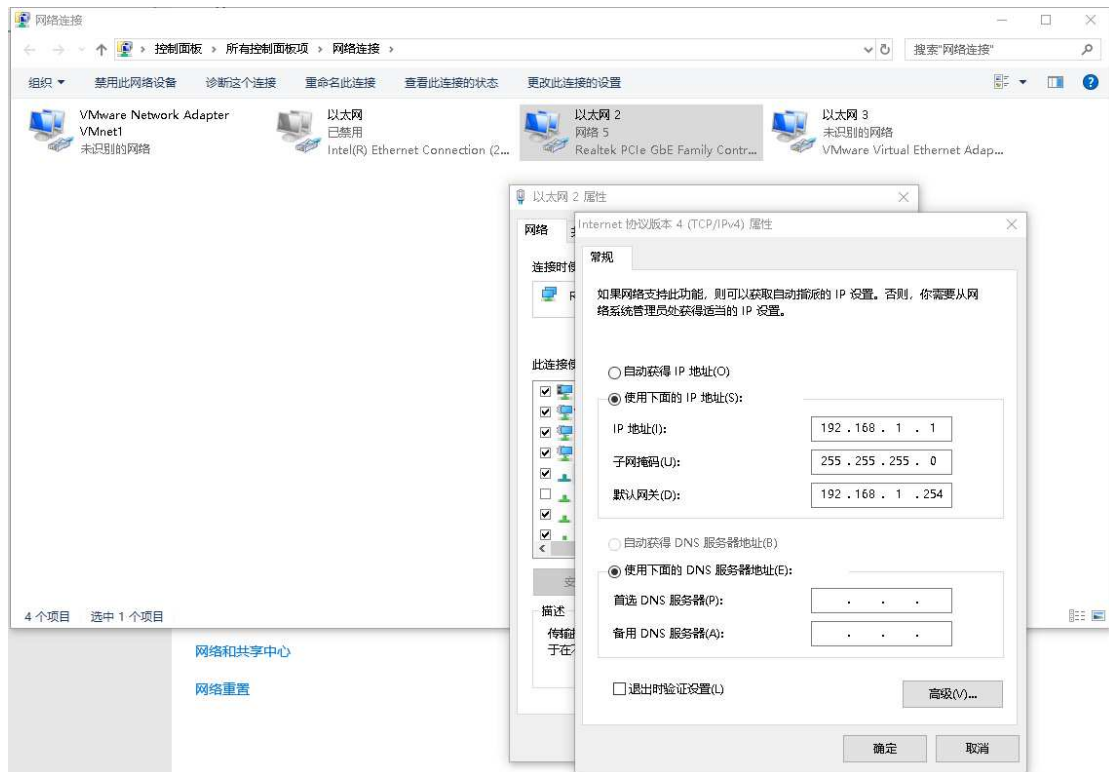
- 1) 按照拓扑图，在实验台中正确连线。
- 2) 登录路由器，正确配置设备（登录方式，启动 IE，在地址栏中输入：<http://172.16.0.x:8080>,注意 x：1-8，哪一排的 pc 输入哪个数字），配置设备如下图：



```
Telnet 172.16.0.1
R1700-1>
R1700-1>enable 14
Password:
R1700-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1700-1(config)#show ip int b
Interface                               IP-Address(Pri)    OK?    Status
serial 1/2                             no address         YES    DOWN
serial 1/3                             no address         YES    DOWN
FastEthernet 1/0                       no address         YES    DOWN
FastEthernet 1/1                       no address         YES    DOWN
Null 0                                 no address         YES    UP
R1700-1(config)#int fa 1/0
R1700-1(config-if)#ip add 192.168.1.254 255.255.255.0
R1700-1(config-if)#no shut
R1700-1(config-if)#int fa 1/1
R1700-1(config-if)#ip add 200.1.8.1 255.255.255.0
R1700-1(config-if)#no shut
R1700-1(config-if)#
%LINK CHANGED: Interface FastEthernet 1/1, changed state to down
%LINE PROTOCOL CHANGE: Interface FastEthernet 1/1, changed state to DOWN
R1700-1(config)#
%LINK CHANGED: Interface FastEthernet 1/1, changed state to up
%LINE PROTOCOL CHANGE: Interface FastEthernet 1/1, changed state to UP
R1700-1(config)#sh ip int b
Interface                               IP-Address(Pri)    OK?    Status
serial 1/2                             no address         YES    DOWN
serial 1/3                             no address         YES    DOWN
FastEthernet 1/0                       192.168.1.254/24   YES    UP
FastEthernet 1/1                       200.1.8.1/24       YES    UP
Null 0                                 no address         YES    UP
R1700-1(config)#
```

注意：password 为 student，输入完成直接回车，没有显示，两个以太网接口必须为 up（满足两个条件自动为 up。一个是 ip 地址并要开启，一个是必须和其他设备相连），设置好了以后关闭配置窗口。

- 3) 正确设置 3 台 pc 的 ip 地址，要注意的是设置以太网 2（也就是 realtek 网卡，不要动以太网即 inter 网卡，然后关闭以太网），如下图 pc1 的 ip 地址：



然后 3 台 pc 都能 ping 通自己的网关且能互相 ping 通。下图为 pc1(攻击机)的 ping 的结果

```
C:\Users\Administrator>ping 192.168.1.254

正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.1.254 的回复: 字节=32 时间<1ms TTL=63

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>ping 200.1.8.8

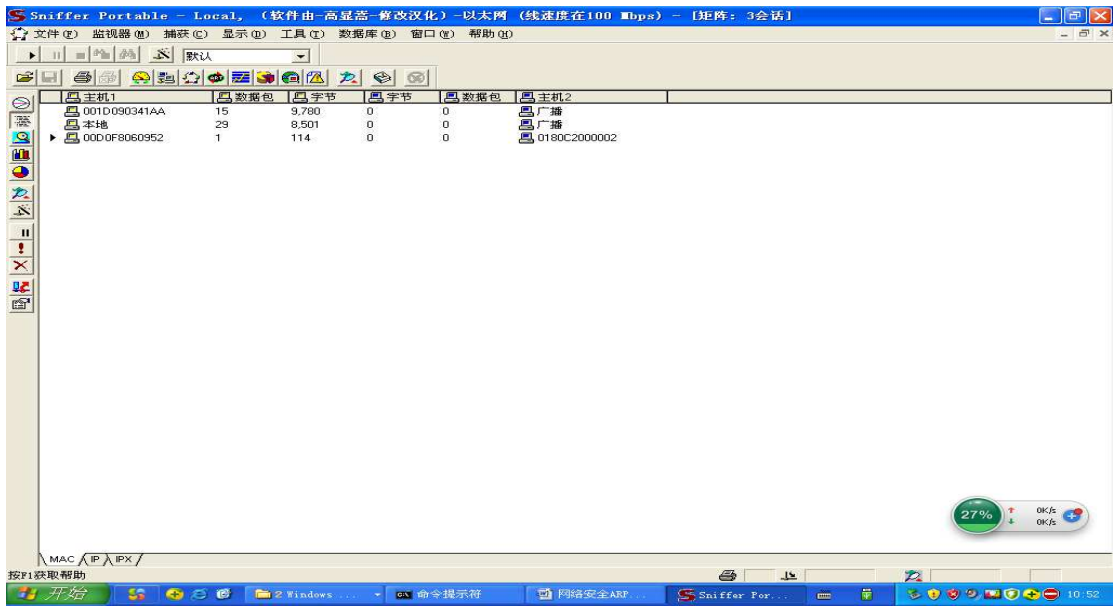
正在 Ping 200.1.8.8 具有 32 字节的数据:
来自 200.1.8.8 的回复: 字节=32 时间<1ms TTL=127
来自 200.1.8.8 的回复: 字节=32 时间<1ms TTL=127
来自 200.1.8.8 的回复: 字节=32 时间<1ms TTL=127
来自 200.1.8.8 的回复: 字节=32 时间<1ms TTL=127
```

- 4) 启动 winxp 虚拟机 (启动虚拟机的方式和 dns 实验一样, 注意在虚拟机中必须关闭防火墙且能 ping 通所有 ip) 且安装 sniffer 软件。
- 5) Pc2 (靶机) 也使用 winxp 虚拟机, win10 系统又发现机制, 这种程度的攻击不起作用。

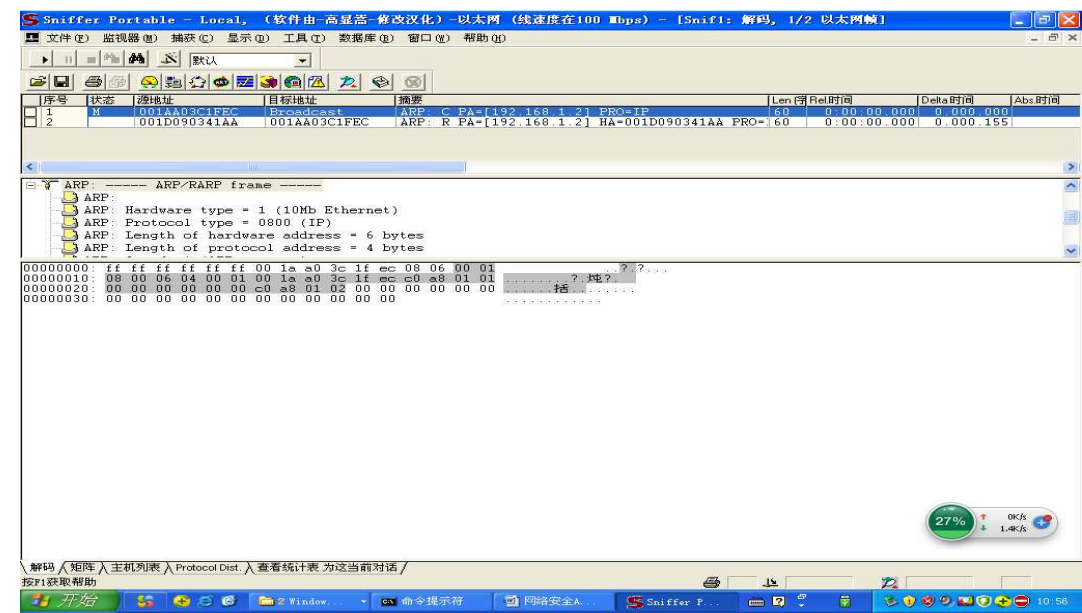
# 实验步骤

## 1、网络协议分析软件 sniffer pro 的配置

启动 sniffer pro 软件，在主窗口的工具栏上点选捕获设置（Define Filter）按钮，可以对要捕获的协议数据设置捕获过滤条件。默认情况下捕获所有从指定网卡接收的全部协议数据。捕获到数据后停止查看按钮会由灰色不可用状态变为彩色的可用状态。



选择停止查看按钮会出现如下图所示对话框，选择最下面的解码选项卡。即可以看捕获后的数据的解码：



## 2、下面利用 sniffer pro 软件对 ARP 协议进行分析

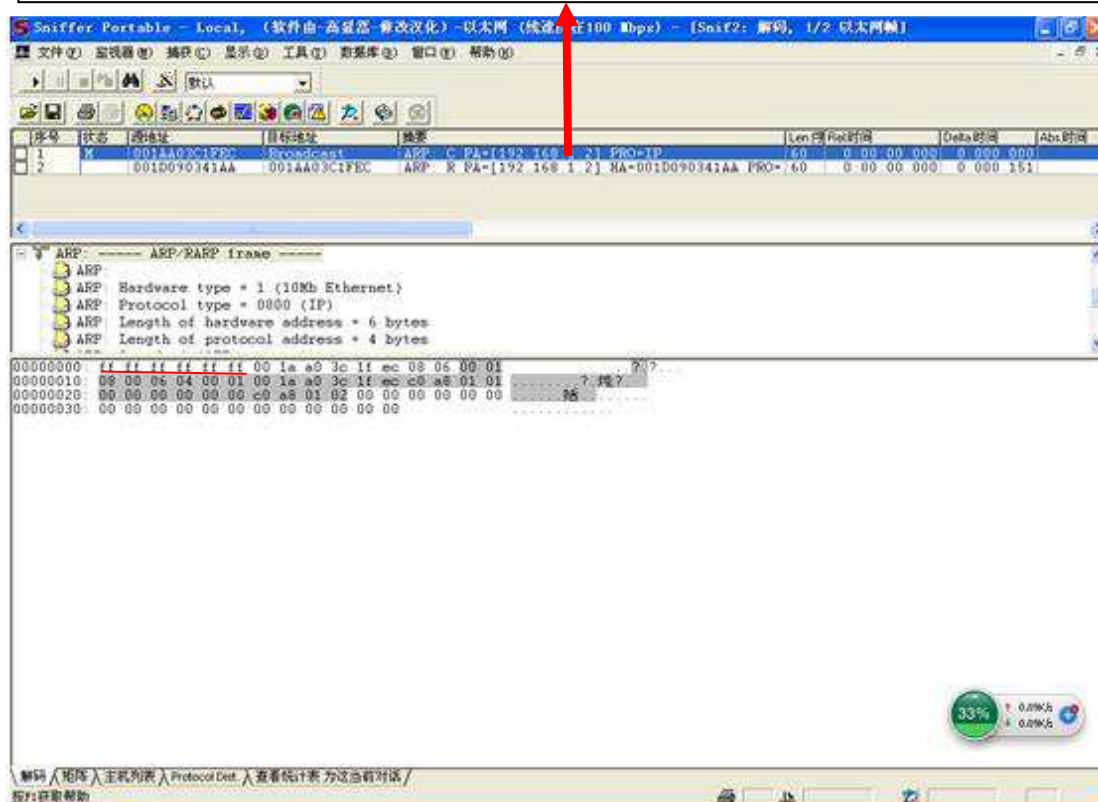
在工作站 1 上进行，分析步骤如下：

- 1) 设置 Sniffer Pro 捕获 ARP 通信的数据包（工作站 1 与工作站 2 之间），在工作站 1 上安装并启动 sniffer pro 软件，并设置捕获过滤条件（Define Filter），选择捕获 ARP 协议。如下图所示：



- 2) 要想工作站 1 发送 ARP 请求给工作站 2，并得到 ARP 回应，首先要确保工作站 1 的 ARP 缓存中没有工作站 2 的记录，所以先在工作站 1 上利用 `arp -a` 查看一下是否有此记录，如果有，则利用 `arp -d` 清除，为了看到效果在执行完清除命令后可以再执行一下 `arp -a` 看是否已经清除，这里不再重复了。
- 3) 确认已经清除工作站 1 的 ARP 缓存中关于工作站 2 的 IP 与 MAC 地址对应关系记录后，就可以启动 Sniffer Pro 进行协议数据捕获了。
- 4) 在没有互相通信需求下，工作站 1 是不会主动发送 ARP 请求给工作站 2，所以也就捕获不到 ARP 的协议数据，此时要在工作站 1 与工作站 2 之间进行一次通信，如可以在工作站 1 上 ping 工作站 2，即：`ping 192.168.1.2`。
- 5) 有 ICMP 数据回应后可以发现，Sniffer Pro 已经捕获到了协议数据。选择停止并查看，结果如下图所示，工作站 1 发送给工作站 2 的 ARP 查询请求数据帧的具体协议数据：

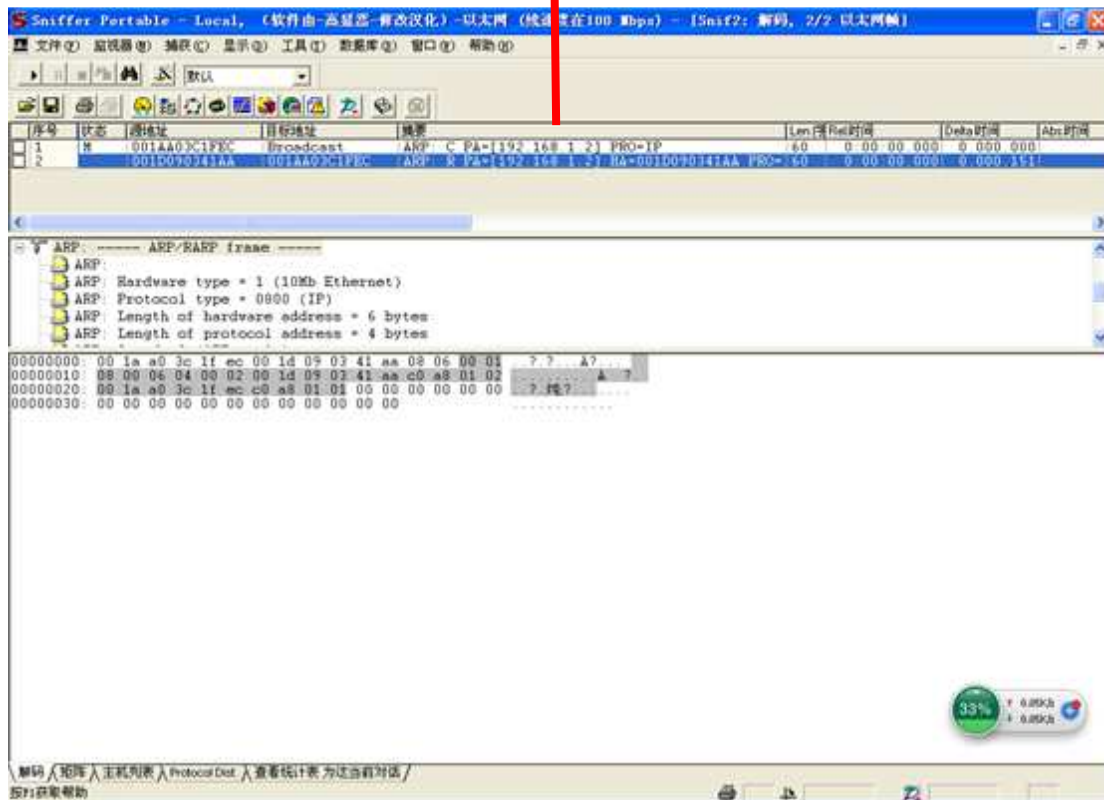
序号为 1 的数据是工作站 1 发给工作站 2 的 ARP 查询请求（是一个广播帧，所以目的地址为 FFFFFFFF）



6) 工作站 2 应答工作站 1 的 ARP 回应数据帧的具体协议数据格式如下图所示：



序号为 2 的数据是工作站 2 发给工作站 1 的 ARP 查询应答（是一个单播帧，因为工作站 2 已经知道工作站 1 的 MAC 地址，所以目的地址为 001d090341aa）



## ARP 协议攻击模拟

下面利用 Sniffer Pro 软件进行基于 ARP 协议的攻击模拟，即让拓扑图中的所有主机不能进行外网访问（无法与网关通信），下面在工作站 1 上实施攻击模拟，步骤如下：

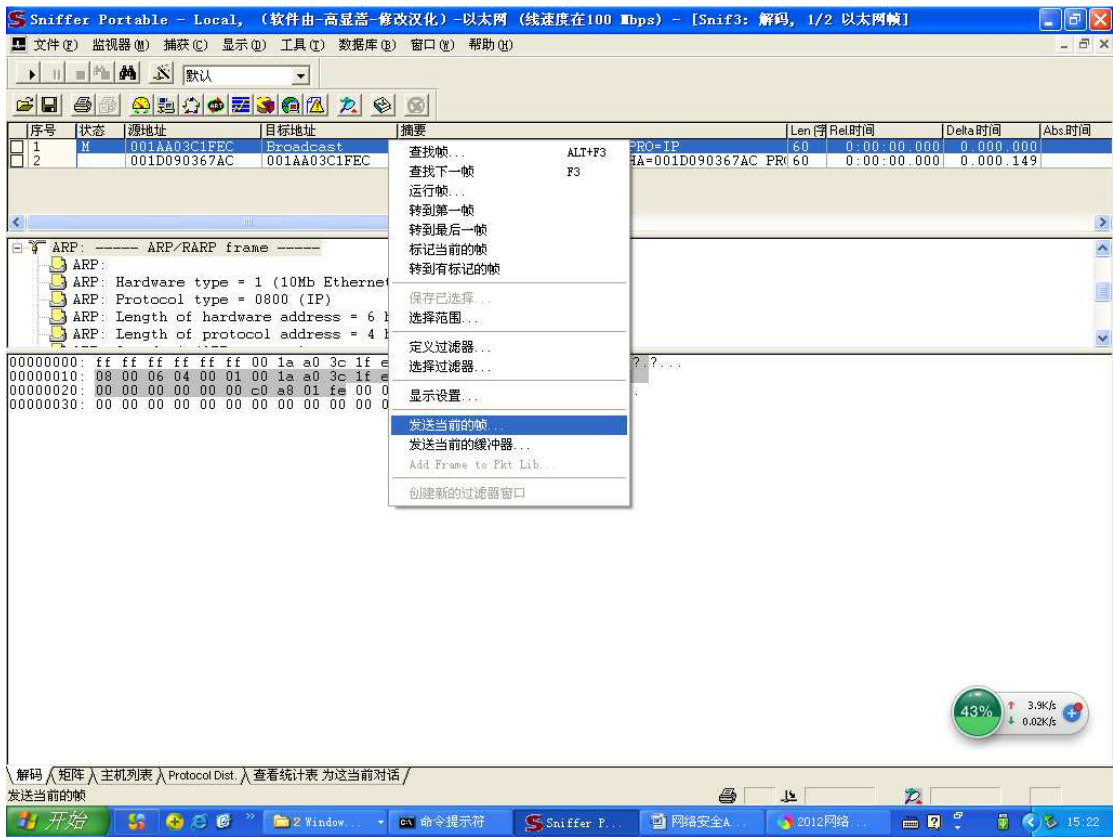
1) 要进行模拟实施攻击，首先要构造一个数据帧，这很麻烦，这时可以捕获一个 ARP 的数据帧再进行改造（~~可以捕获一个网关的 ARP 数据帧~~）。设置 Sniffer Pro 捕获 ARP 通信的数据包（工作站 1 与网关之间），在工作站 1 上再次启动 Sniffer Pro 软件，并设置捕获过滤条件（Define Filter），选择捕获 ARP 协议。

2) 要想工作站 1 发送 ARP 请求给网关，并得到 ARP 回应，首先启动 Sniffer Pro 捕获，然后利用 `arp -d` 清除 ARP 缓存。

3) 在没有互相通信需求下，工作站 1 是不会主动发送 ARP 请求给网关的，所以也就捕获不到 ARP 的协议数据，此时要在工作站 1 与网关之间进行一次通信，如可以在工作站 1 上 ping 网关，即：ping 192.168.1.254。



4) 有 ICMP 数据回应后可以发现，Sniffer Pro 已经捕获到了协议数据。选择停止并查看，在第 1 帧数据包上点击右键，并选择发送当前的帧…。如下图所示：



5) 出现如图 16 所示对话框，其中的数据 (Data) 即是工作站 1 发出去查询网关 MAC 地 ARP 请求数据，已经放入发送缓冲区内，此时可以进行修改了。



工作站 1 发送给网关的 ARP 查询请求	
目的 mac 地址：为广播地址	
源 mac 地址为工作站 1 的 MAC 地址 ( 001aa03c1fec )，伪造一下改成为网关的假地址：001122334455	
发送本次 arp 请求的 arp 协议 ( ip ) 地址为 192.168.1.1 ( 十六进制为 c0a80101 )，伪造一下改成网关的 ip 地址：192.168.1.254 ( 十六进制为 c0a801fe )	
被查询的目标 ip 地址为 192.168.1.254 ( 十六进制为 c0a801fe )，伪造一下改成工作站 1 的 ip 地址 ( 十六进制为 c0a80101 )	

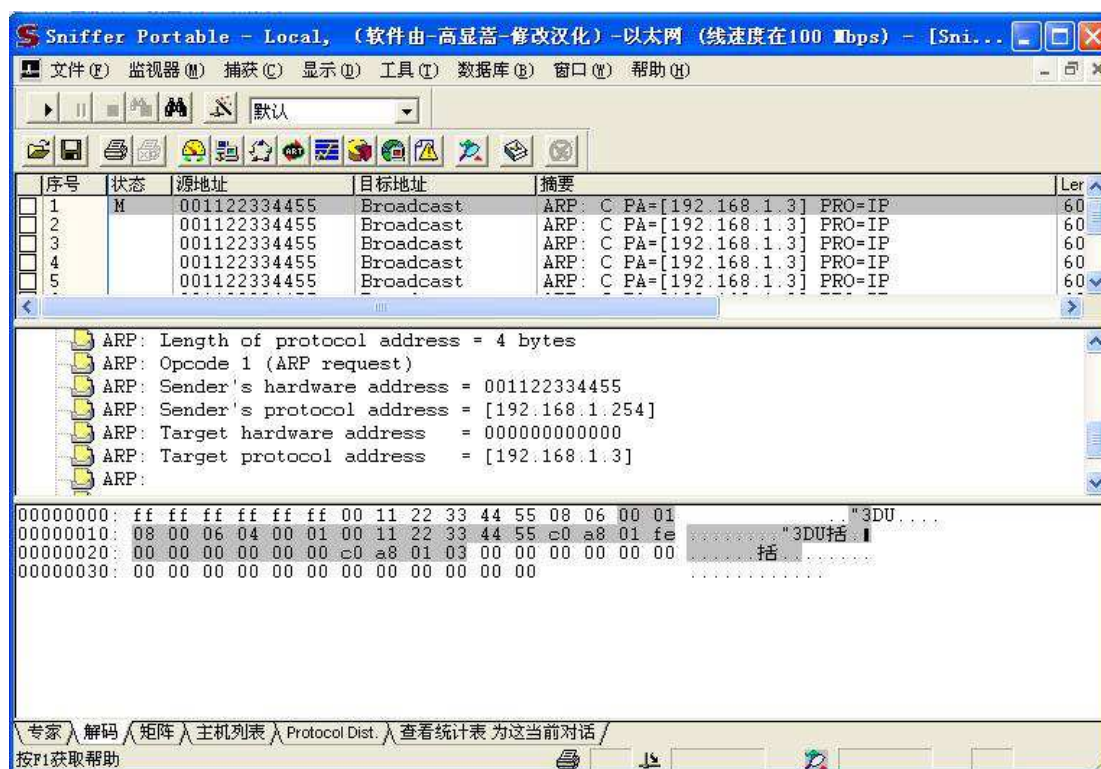
6) 对工作站 1 发出去查询网关 MAC 地 ARP 请求数据 ( Data ) 进行如上图所示的伪造修改，即这个帧是被伪造为网关 IP ( 192.168.1.254，十六进制数为：c0a801fe ) 地址和 MAC 地址 ( 伪造为假的：001122334455 ) 发出去的查询 192.168.1.3 ( 十六进制数为：c0a80103 当然可以随便一个 192.168.1.0/24 网段的地址 ) 的 MAC 地址的 ARP 广播帧，这样所有本地网段内的主机都会收到并更新记录，以为网关 ( IP 为 192.168.1.254 ) 的 MAC 地址变为了 001122334455，并将这一错误关联加入各自的 ARP 缓存中 ( 包括工作站自身 )。

7) 在发送此伪造帧之前，在工作站 2 用 arp -a 看看是否有网关的 mac 地址，没有必须 ping 192.168.1.254，得到网关的 mac 地址 ( 计算机 mac 地址表的修改必须满足两个条件，1、收到 arp 应答包；2、收到广播包，广播包的原 ip 必须包含在计算机的 arp 表中 )，当然最好在工作站 2 中启动 sniffer 软件并选择开始抓包。

8) 修改后的帧缓冲区中的数据如下图所示，修改后在发送 ( Send ) 次数下选择发送 10 次，发送类型 ( Send Type ) 下选择每隔 10 毫秒一次。后点击确定，伪造的数据帧即开始按此间隔时间发送 10 次了。



9) 攻击结束后，在工作站 2 的 sniffer 软件可以看到已经有数据包了，单击“停止并显示”按钮，出现如下图所示的屏幕。



10) 然后用 `arp -a` 看看工作站的 arp 表，再 ping 192.168.1.254，此时就 ping 不通了，结果如下图所示：

```
命令提示符
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.2 --- 0x10003
    Internet Address      Physical Address      Type
    192.168.1.254         00-d0-f8-6b-87-55    dynamic

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.2 --- 0x10003
    Internet Address      Physical Address      Type
    192.168.1.254         00-11-22-33-44-55    dynamic

C:\Documents and Settings\Administrator>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

11)，最后分别在两台工作站上执行 arp -d 命令，重新 PING 网关后又可以进行连接并访问外网了，下图为工作站 1 访问服务器 web 页面。



至此针对 ARP 协议的分析、捕获与模拟攻击过程结束。

思考题：用户 A 发送 arp 报文请求网关的 mac 地址，这时处于同一 vlan 的用户 B 也会收到该 arp 报文，因此用户 B 可以发送 arp 响应报文，将报文的源 ip 填为网关 ip，而源 mac 填为自己的 mac 地址。用户 A 收到该 arp 响应后，就会认为用户 B 的机器就是网关，因此用户 A 通讯中发往网关的报文都将发往用户 B，这样用户 A 的通讯实际上都被截取了，造成 arp 欺骗的效果。

- 1) 在工作站 2 伪造网关发往工作站 1 的 arp 相应报文。
- 2) 在工作站 1 中查看 arp 变化，并是否能 ping 通网关。
- 3) 在 ping 的过程前，在工作站 2 启动 sniffer 软件抓包，看能否抓取 ping 包。

## 在交换机上实现ARP防护

### 1、实验原理

因此我们可以在二层交换机上配置防网关 arp 欺骗来防止针对网关的 arp 欺骗。防网关 arp 欺骗配置后，可以在端口上检查 arp 报文的源 ip 是否是我们配置的网关 ip，如果是，则将该报文丢弃，防止用户收到错误的 arp 响应报文。这样只有交换机上连设备能够下发网关的 ARP 报文，其它 pc 就不能发送假冒网关的 arp 响应报文或者是 arp 广播报文。

### 2、实验步骤

登录交换机，进入交换机特权用户配置模式

```
S2126G-1#conf
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S2126G-1(config)#int fa 0/1
```

```
2017-10-16 19:03:15 @5-CONFIG:Configured from outband
```

```
S2126G-1(config-if)#anti-arp-Spoofing ip 192.168.1.254
```

```
2017-10-16 19:04:45 @5-CONFIG:Configured from outband
```

```
S2126G-1(config-if)#exit
```

```
2017-10-16 19:04:47 @5-CONFIG:Configured from outband
```

```
S2126G-1(config)#int fa 0/2
```

```
2017-10-16 19:04:50 @5-CONFIG:Configured from outband
```

```
S2126G-1(config-if)#anti-arp-Spoofing ip 192.168.1.254
```

```
2017-10-16 19:04:52 @5-CONFIG:Configured from outband
```



```
S2126G-1(config-if)#exit
```

```
2017-10-16 19:04:53 @5-CONFIG:Configured from outband
```

```
S2126G-1(config)#exit
```

```
2017-10-16 19:05:08 @5-CONFIG:Configured from outband
```

```
S2126G-1#
```

### 配置注意

上链口、连接出口网关的端口（即连接路由器的端口）不能启用防网关欺骗，否则将导致源地址为网关 IP 或服务器 IP 的 ARP 报文被阻断，造成网络不通。

3、再次进行 arp 欺骗，看是否成功。

## 结果保存

进入路由器，然后输入 show running-config：

```
R1700-1#show running-config
```

```
Building configuration...
```

```
Current configuration : 650 bytes
```

```
version 8.51 (building 11)
```

```
hostname R1700-1
```

```
enable secret level 14 5 $1$bii3$txDzzzzz67w79x42
```

```
enable secret 5 $1$3KyL$v3szvFytyAxp6v3
```

```
no service password-encryption
```

```
interface serial 1/2
```

```
!
```

```
interface serial 1/3
```

```
clock rate 64000
```

```
!
```

```
interface FastEthernet 1/0
```

```
ip address 192.168.1.254 255.255.255.0
```

```
duplex auto
```

```
speed auto
!
interface FastEthernet 1/1
ip address 200.1.8.8 255.255.255.0
duplex auto
speed auto
!
interface Null 0

voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
line con 0
line aux 0
line vty 0 4
login
end
```

同理进入交换机

```
S2126G-1#show run
```

```
System software version : 1.66(3) Build Sep 7 2006 Rel
```

```
Building configuration...
```

```
Current configuration : 363 bytes
```

```
version 1.0
```

```
hostname S2126G-1
```



enable secret level 14 5 'T>H.Y\*T3UC,tZ[V4^D+S(\W54G1X)sv

enable secret level 15 5 'Stj9=G14X7R:>H.UUu\_;;C,tQ2U0<D+S

!

interface fastEthernet 0/1

Anti-ARP-Spoofing ip 192.168.1.254

!

interface fastEthernet 0/2

Anti-ARP-Spoofing ip 192.168.1.254

!

end

**心得与体会**