



# 2.7 ARP协议 简介

Address Resolution Protocol即地址解析协议，解析IP地址与MAC地址的对应关系。

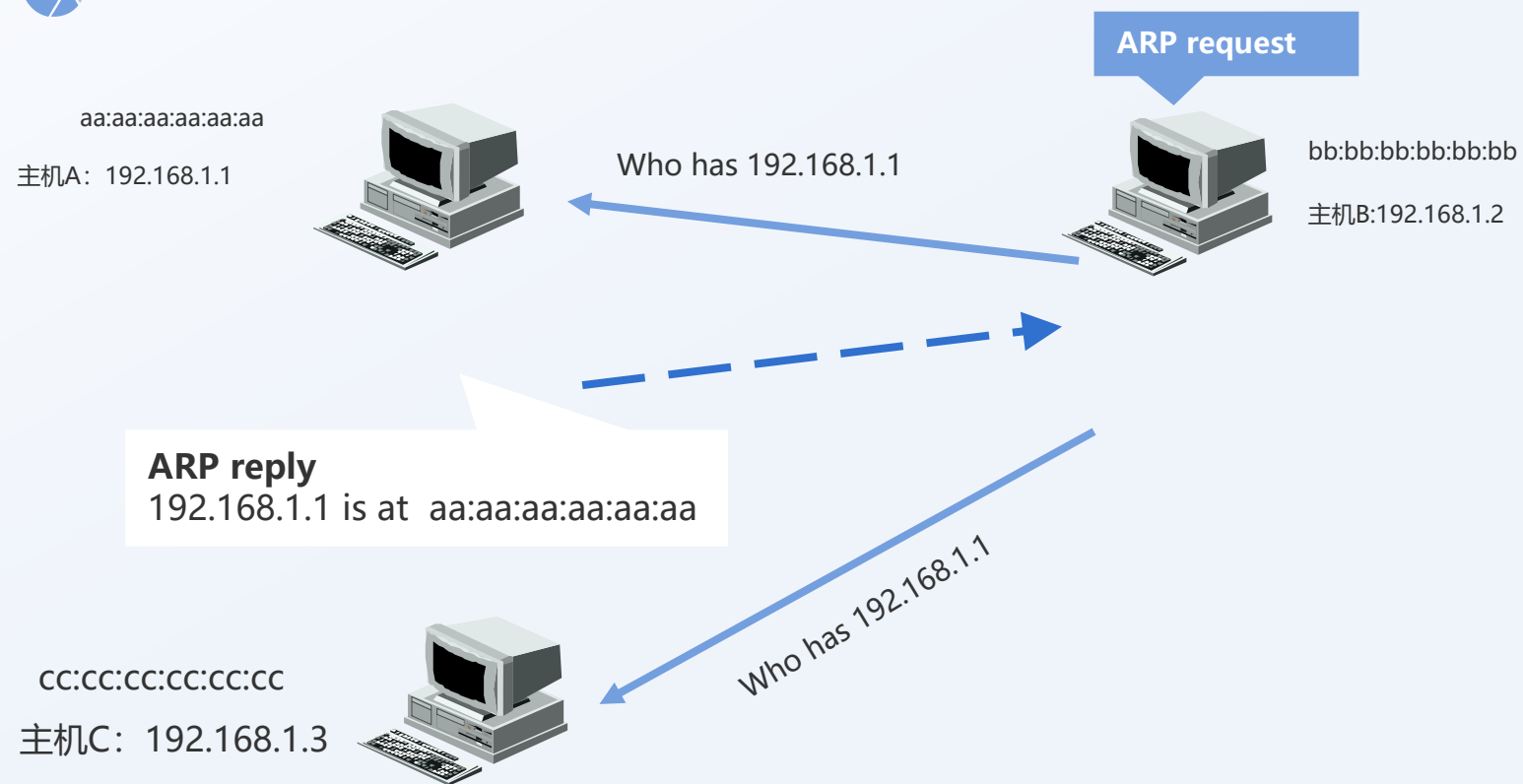
ARP协议的基本功能就是：查询目标设备的MAC地址，完成数据封装。



## 2.7 ARP协议简介



ARP协议工作原理



## 2.7 ARP协议简介

```
em32\cmd.exe
版本 6.1.7601
Microsoft Corporation。保留所有权利。

C:\>arp -a

- 0xb
物理地址          类型
6c-0b-84-92      动态
44-39-c4-38      动态
6c-0b-84-01      动态
6c-0b-84-01      动态
00-01-6c-4e      动态
6c-0b-84-01      动态
44-39-c4-38      动态
```

ARP Cache

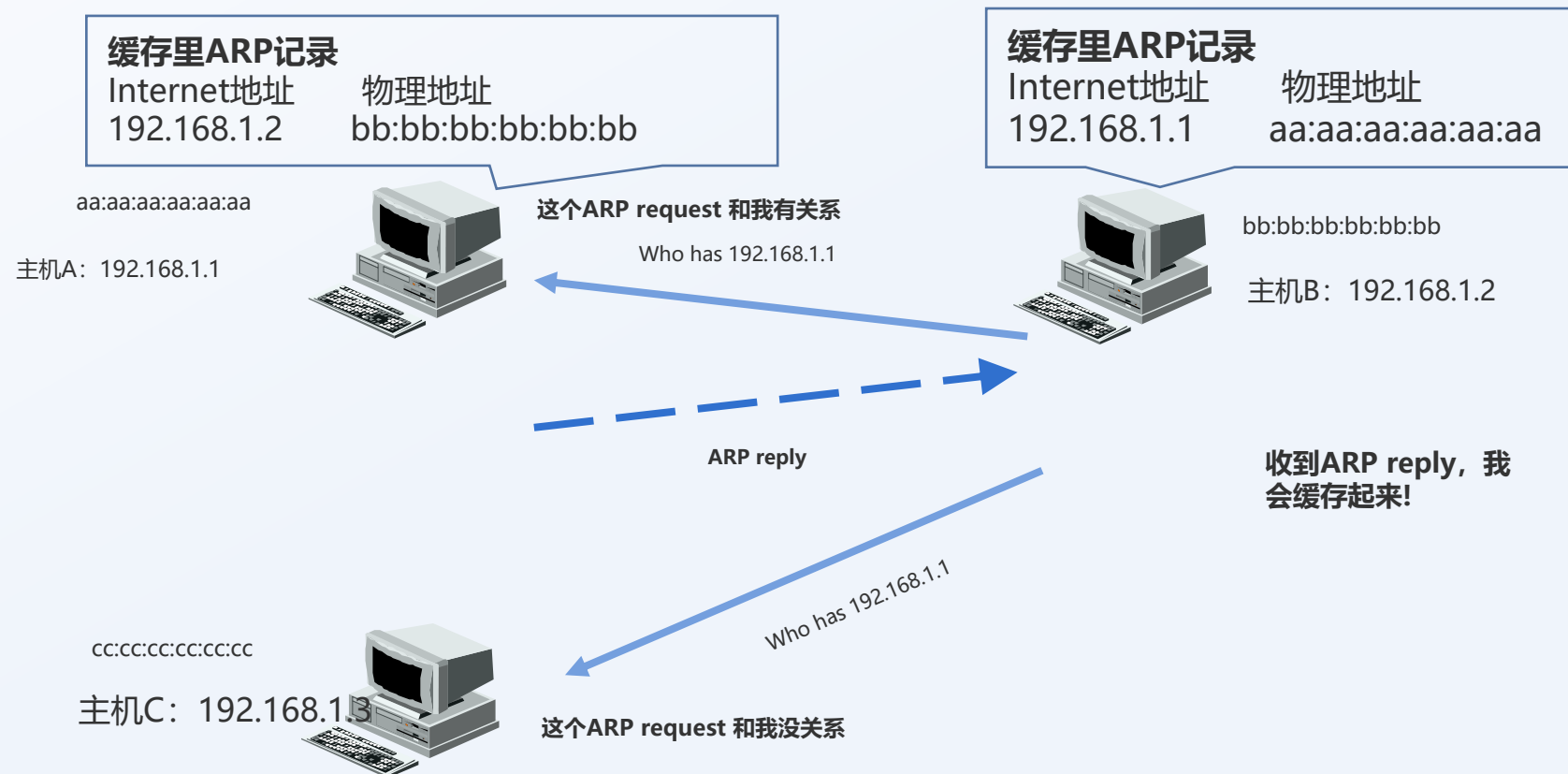
- 在安装了以太网网络适配器（既网卡）或TCP/IP协议的计算机中，都有ARP Cache用来保存IP地址以及解析的MAC地址。
- Windows 系统默认的ARP缓存表的生存时间是120秒，最大生命期限是10分钟。



## 2.7 ARP协议简介



ARP缓存的更新



## 2.7 ARP协议简介

接受ARP  
request单播包

无法判断来源和数据包内容的真伪

ARP协议实现的特点

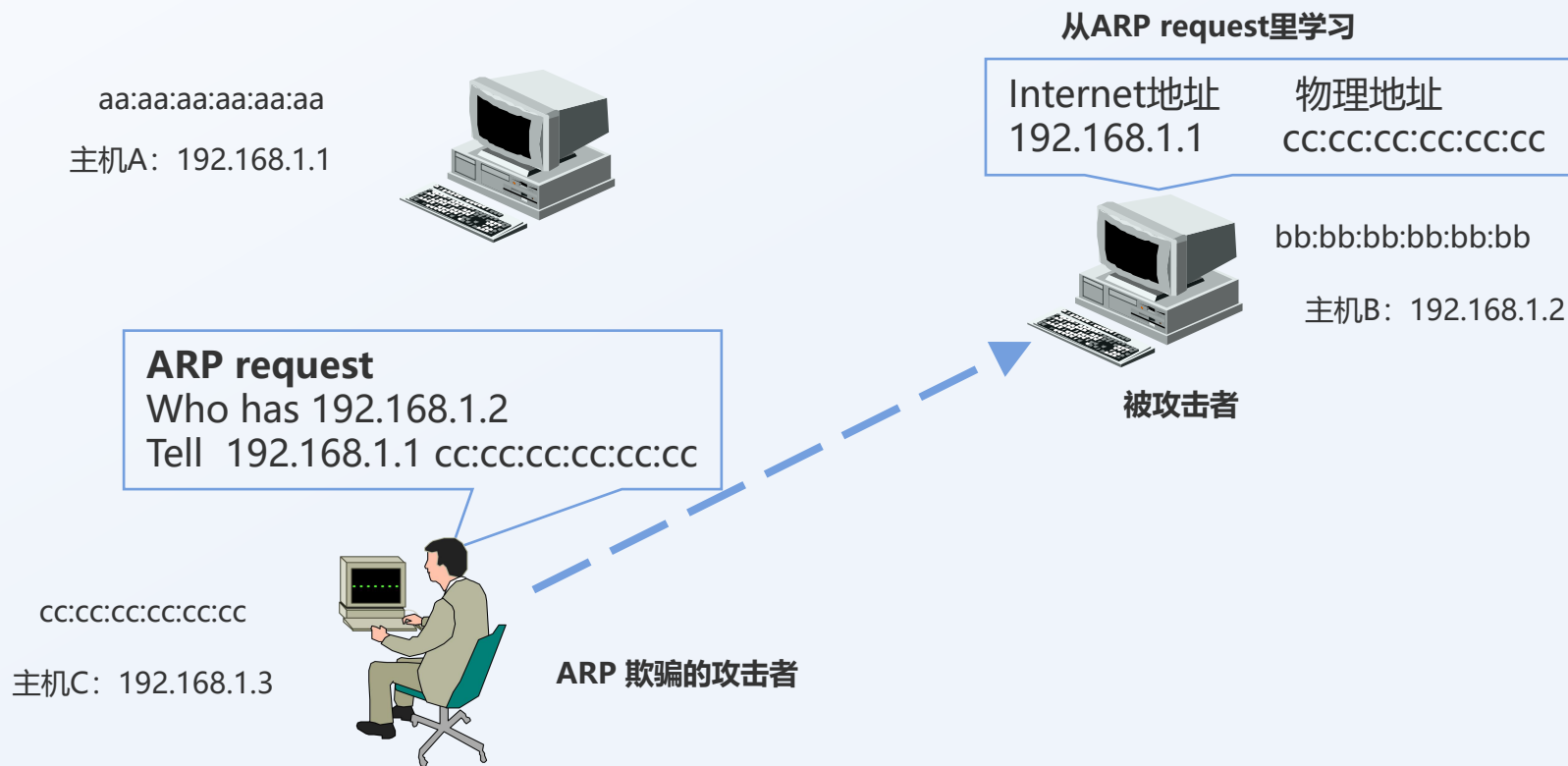
无需请求可以应答



## 2.7 ARP协议简介



### 基于ARP request的欺骗

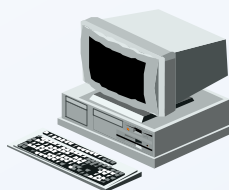


## 2.7 ARP协议简介



基于ARP reply的欺骗

aa:aa:aa:aa:aa:aa  
192.168.1.1



**ARP reply**  
192.168.1.1 is at cc:cc:cc:cc:cc:cc

cc:cc:cc:cc:cc:cc  
192.168.1.3

ARP 欺骗的攻击者



Internet地址  
192.168.1.1

物理地址  
cc:cc:cc:cc:cc:cc



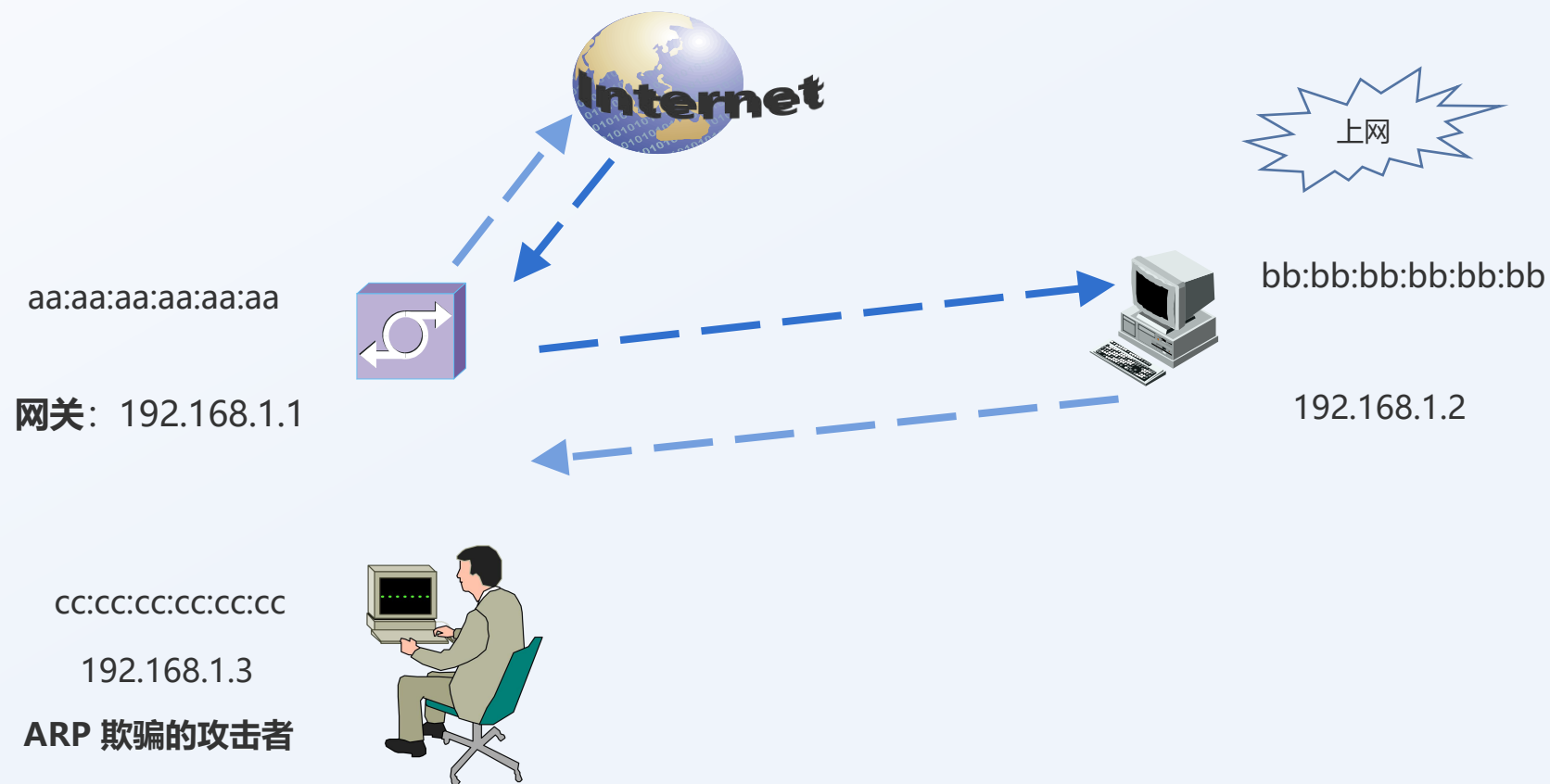
bb:bb:bb:bb:bb:bb  
192.168.1.2  
被攻击者

收到ARP reply,  
我会缓存起来!



## 2.7 ARP协议简介

ARP欺骗+中间人攻击

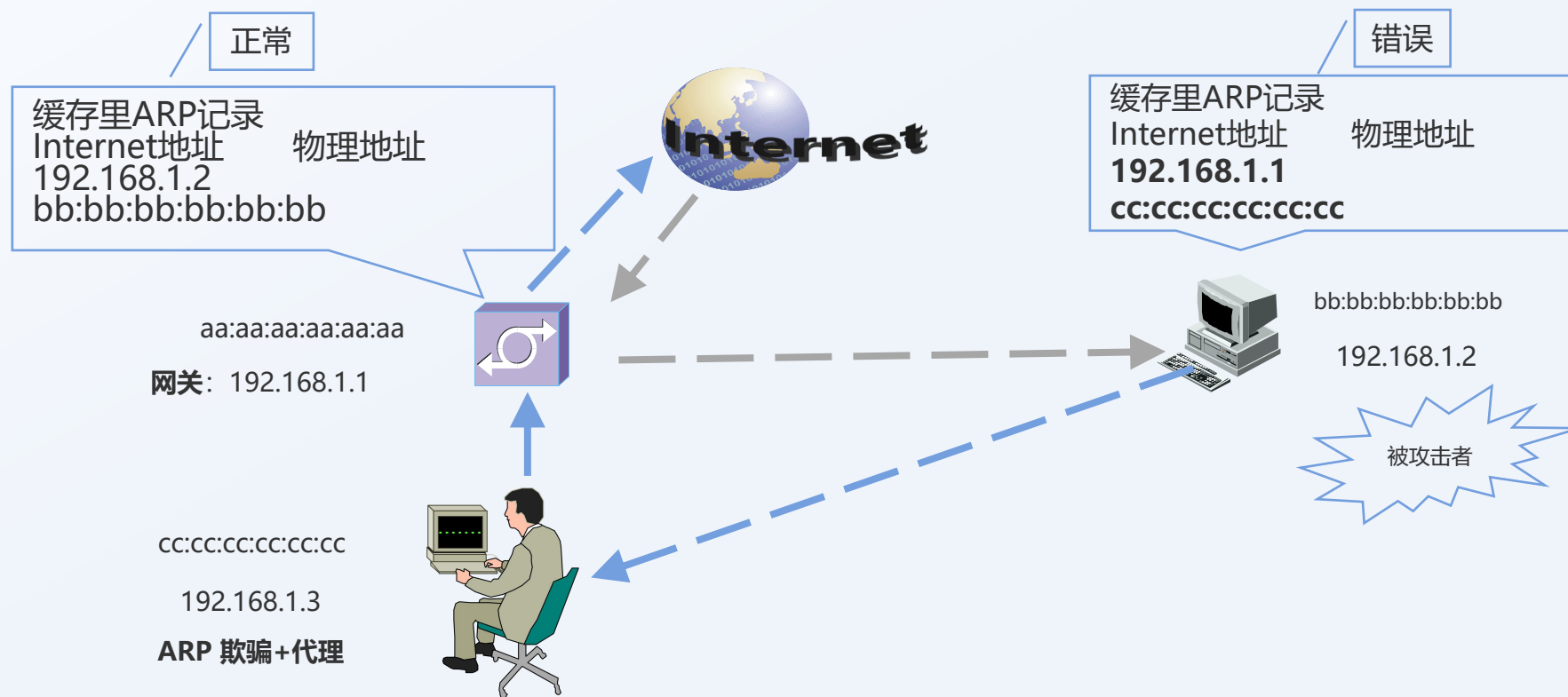




## 2.7 ARP协议简介

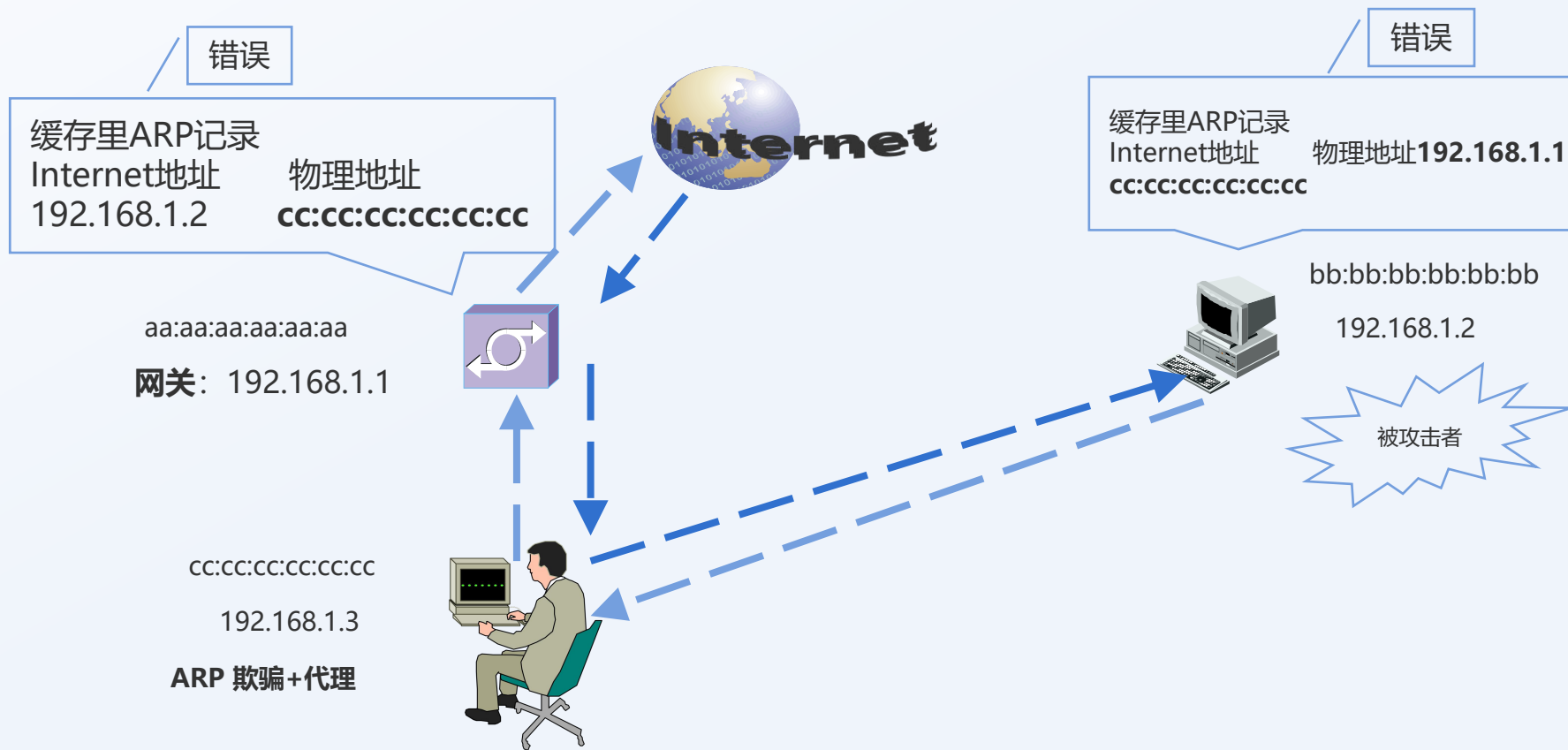


### ARP欺骗+中间人攻击（单项欺骗）



## 2.7 ARP协议简介

## ARP欺骗+中间人攻击（双项欺骗）



## 2.7 ARP协议简介



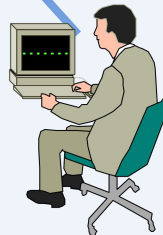
利用SwitchSniffer完成ARP欺骗

GW: 10.3.40.254  
00:0f:e2:50:4b:a0

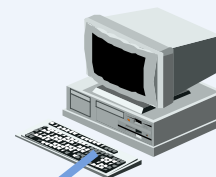


PC1: 10.3.40.100  
00:0c:29:e1:b4:ae

ARP 欺骗的攻击者



安装: SwitchSniffer  
wireshark



PC2: 10.3.40.5  
dc:4a:3e:46:45:0e

被攻击者



## 2.7 ARP协议简介

欺骗前  
PC2的  
arp缓存

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\N>arp -a

接口: 10.3.40.5 --- 0x12
Internet 地址      物理地址      类型
10.3.40.6          dc-4a-3e-46-44-15 动态
10.3.40.55         dc-4a-3e-46-44-24 动态
10.3.40.254        00-0f-e2-50-4b-a0 动态
229.22.33.5        01-00-5e-16-21-05 静态

C:\Users\N>
```

GW: 10.3.40.254  
00:0f:e2:50:4b:a0

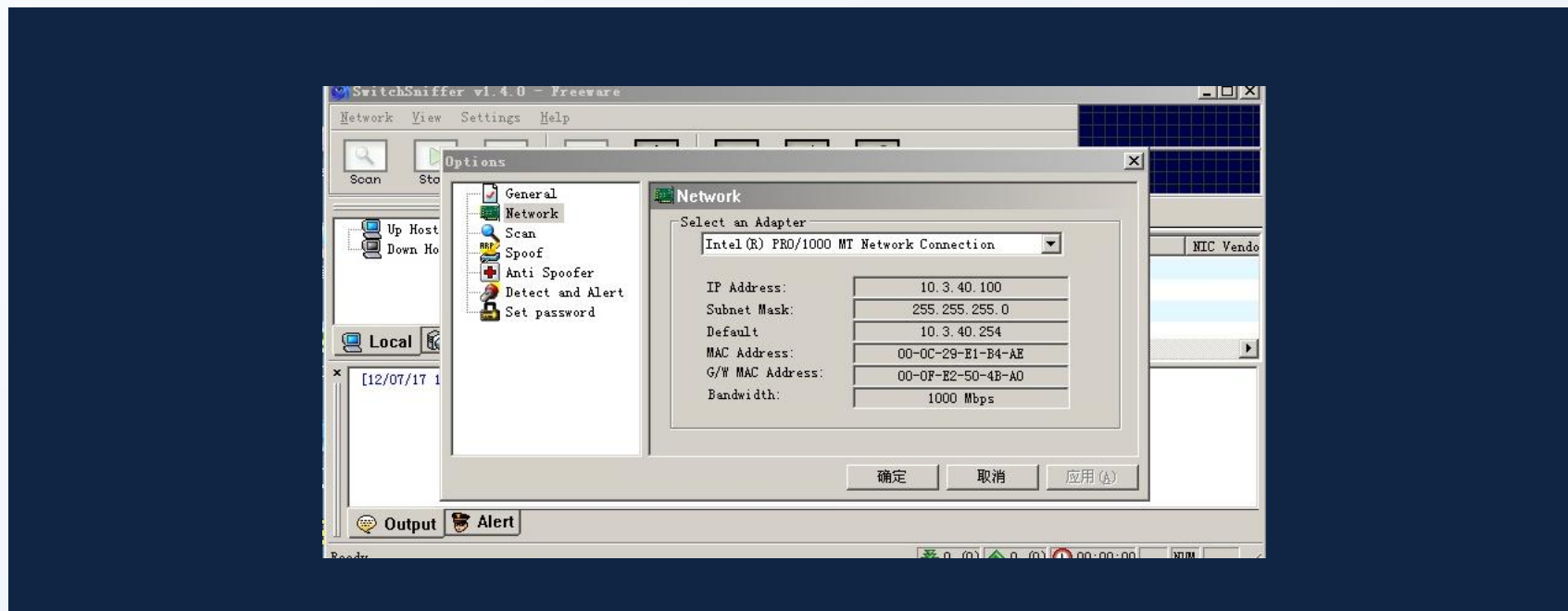


IP1: 10.3.40.100  
00:0c:29:e1:b4:ae

ARP 欺骗的攻击者

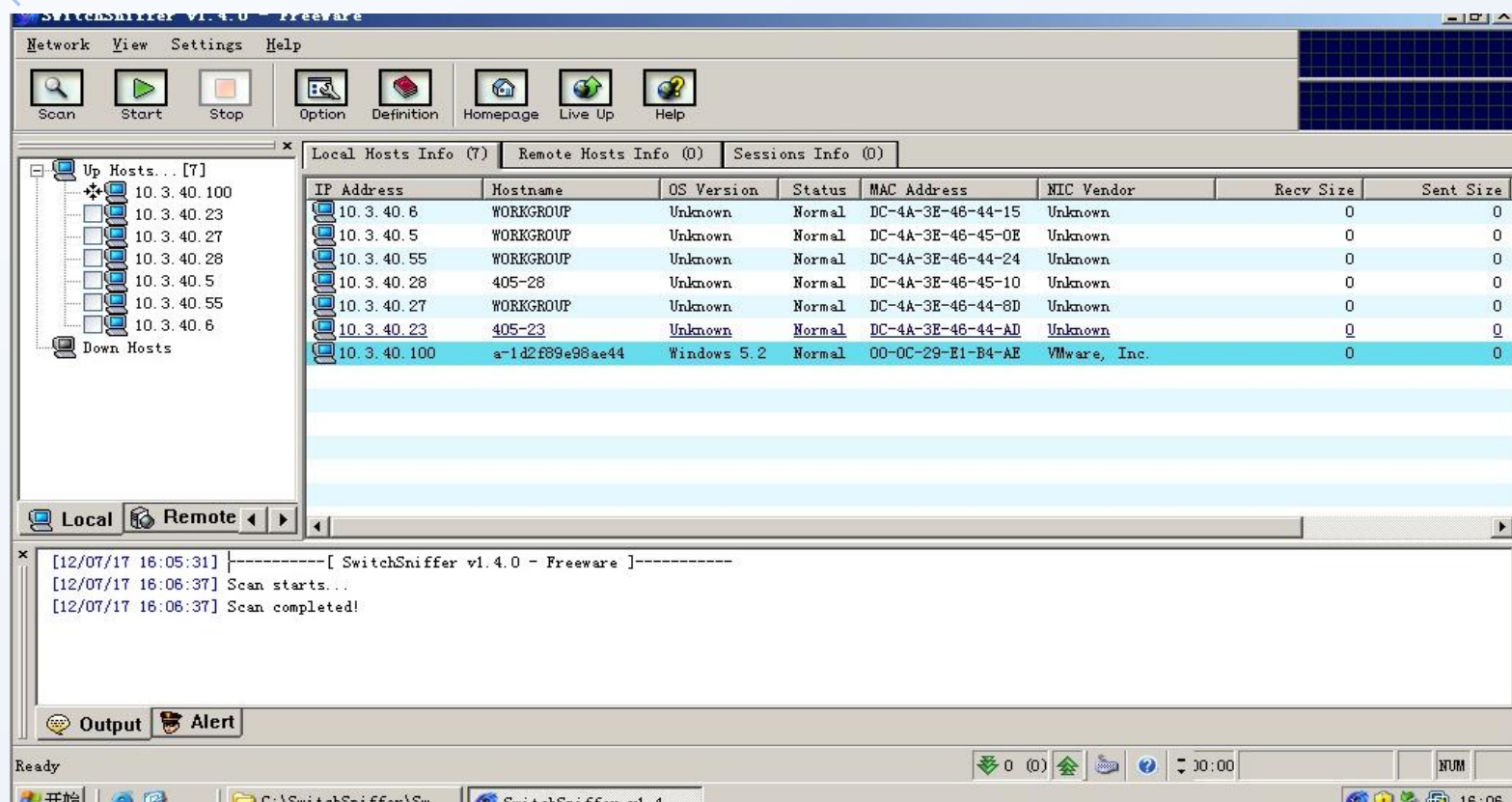


## 2.7 ARP协议简介

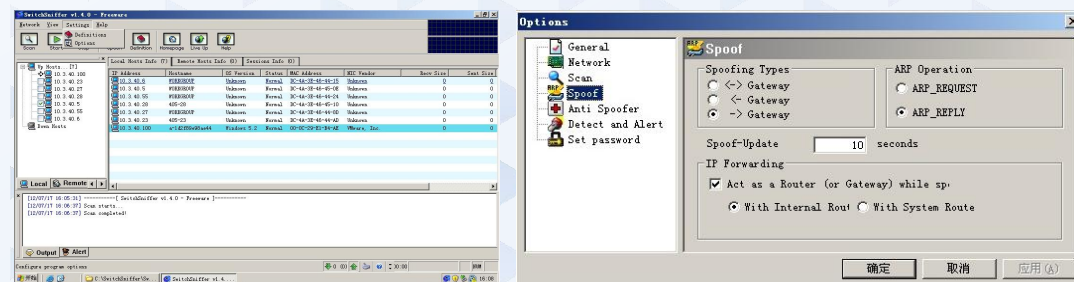


SwitchSniffer设置

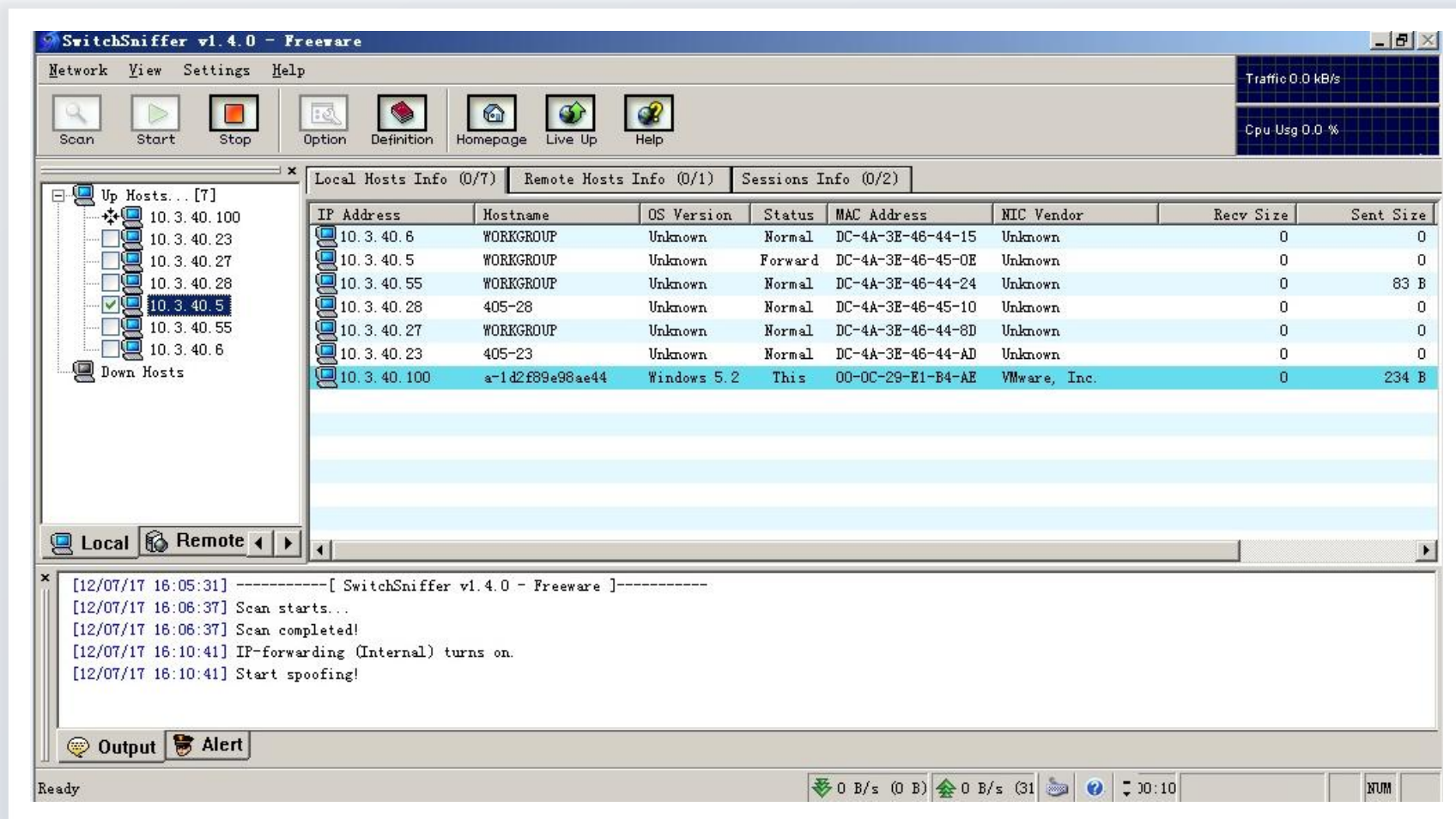
## 2.7 ARP协议简介



## 2.7 ARP协议简介



## 2.7 ARP协议简介

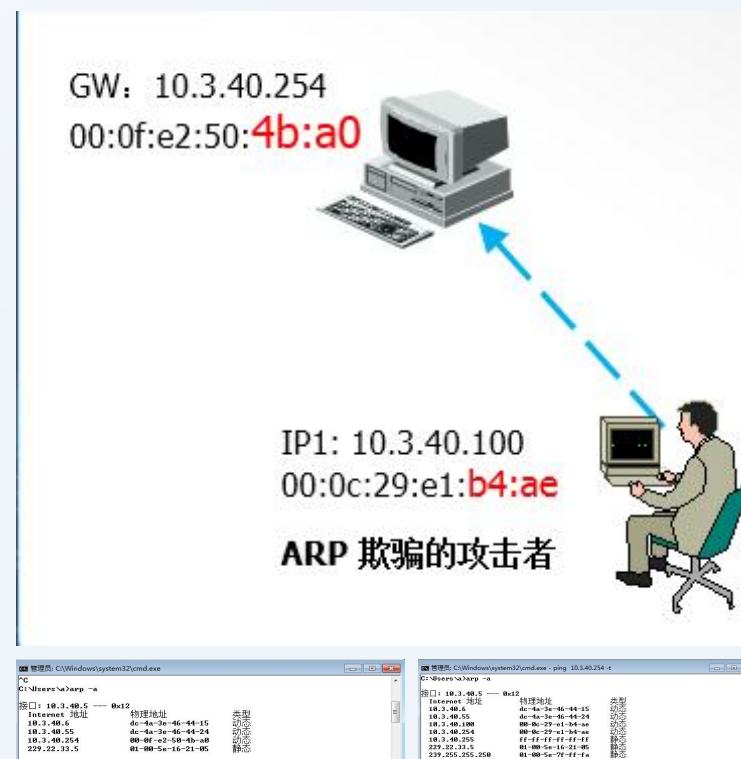




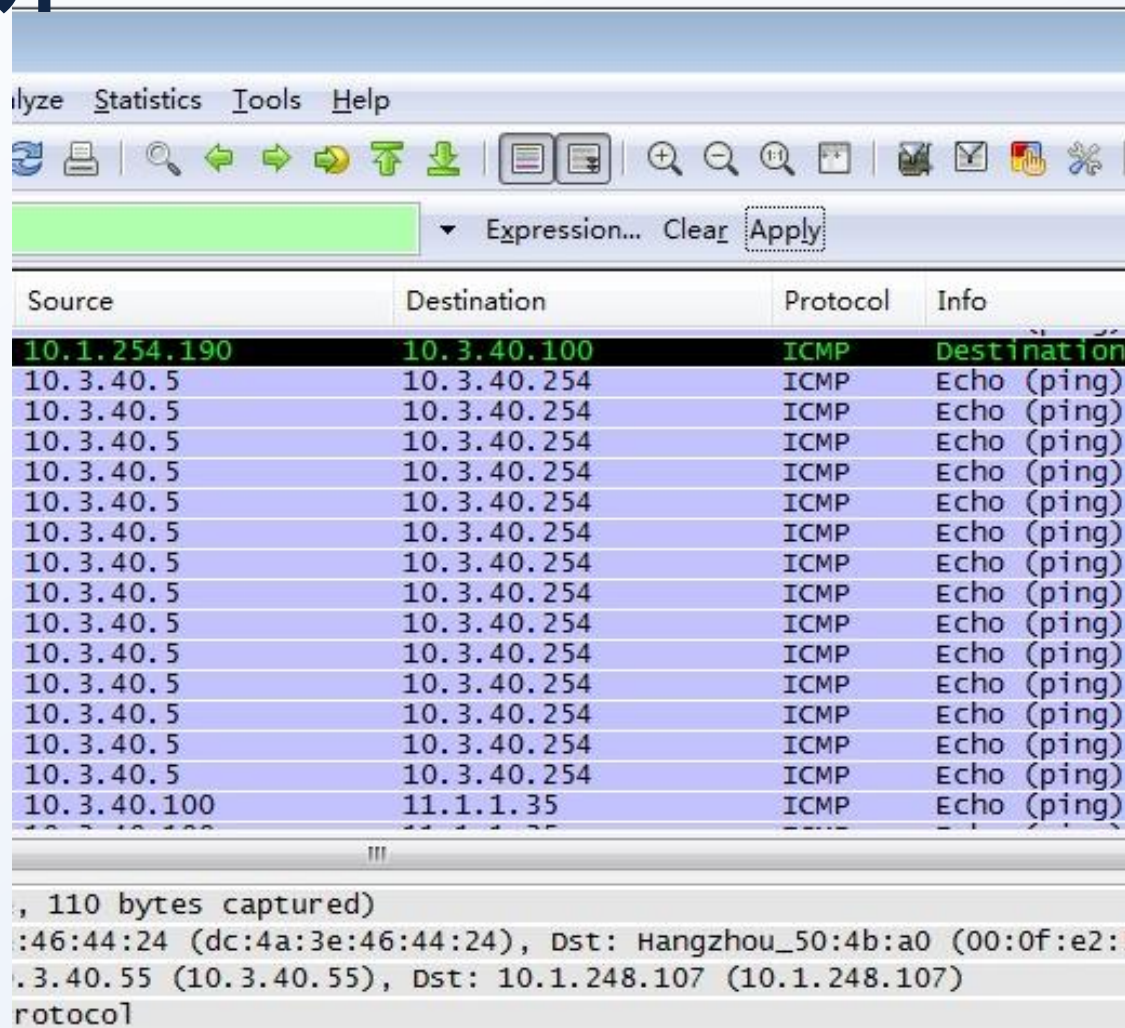
## 2.7 ARP协议简介



欺骗后PC2的arp  
缓存  
后  
前



## 2.7 ARP协议简介



The image shows a Wireshark packet capture window. The top menu bar includes 'Analyze', 'Statistics', 'Tools', and 'Help'. Below the menu is a toolbar with various icons for packet manipulation. A filter bar shows 'Expression...' with 'Clear' and 'Apply' buttons. The main packet list table is as follows:

Source	Destination	Protocol	Info
10.1.254.190	10.3.40.100	ICMP	Destination
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.5	10.3.40.254	ICMP	Echo (ping)
10.3.40.100	11.1.1.35	ICMP	Echo (ping)

Below the packet list, the packet details pane shows the following information:

- , 110 bytes captured)
- :46:44:24 (dc:4a:3e:46:44:24), Dst: Hangzhou\_50:4b:a0 (00:0f:e2:)
- .3.40.55 (10.3.40.55), Dst: 10.1.248.107 (10.1.248.107)
- rotocol

10.3.40.5  
ping 10.3.40.254

Wireshark 安装在  
10.3.40.100



## 2.7 ARP协议简介

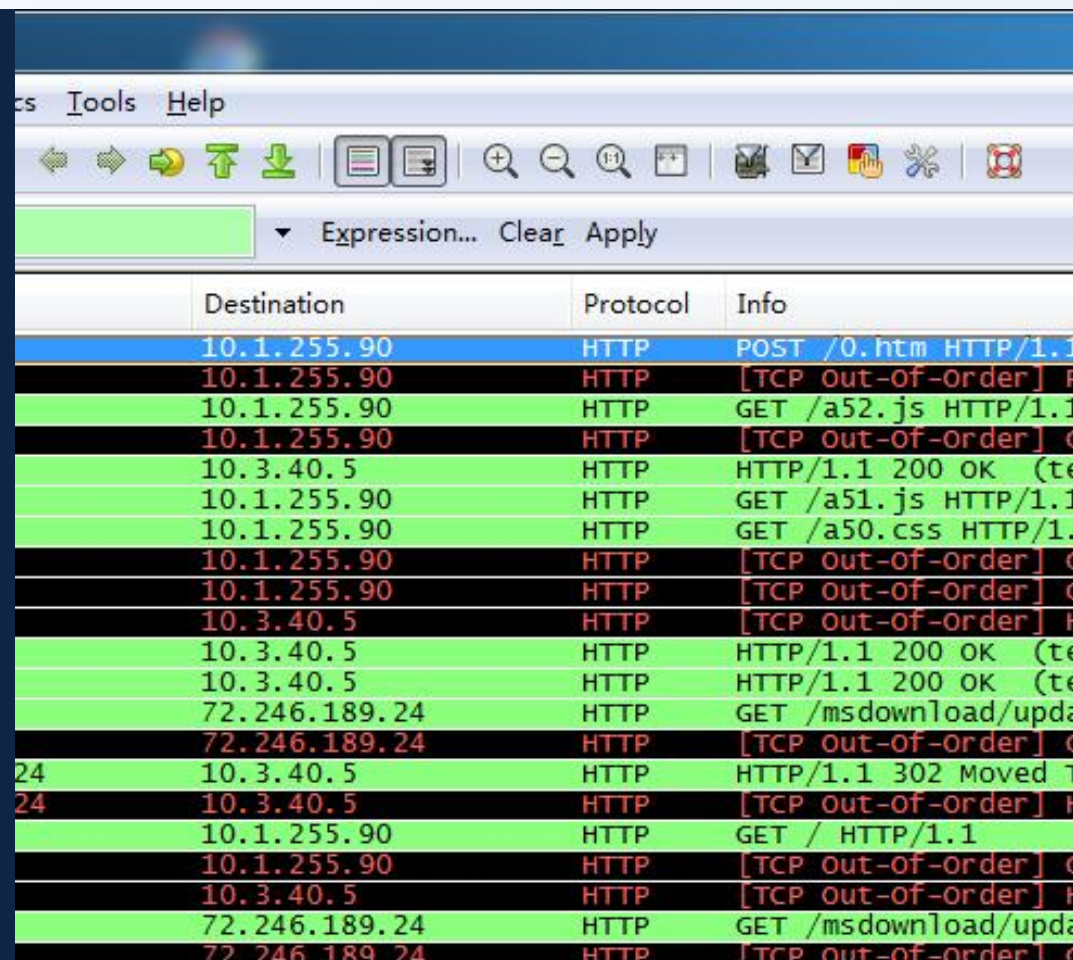
双向欺骗

logo



## 2.7 ARP协议简介

截获双向数据包

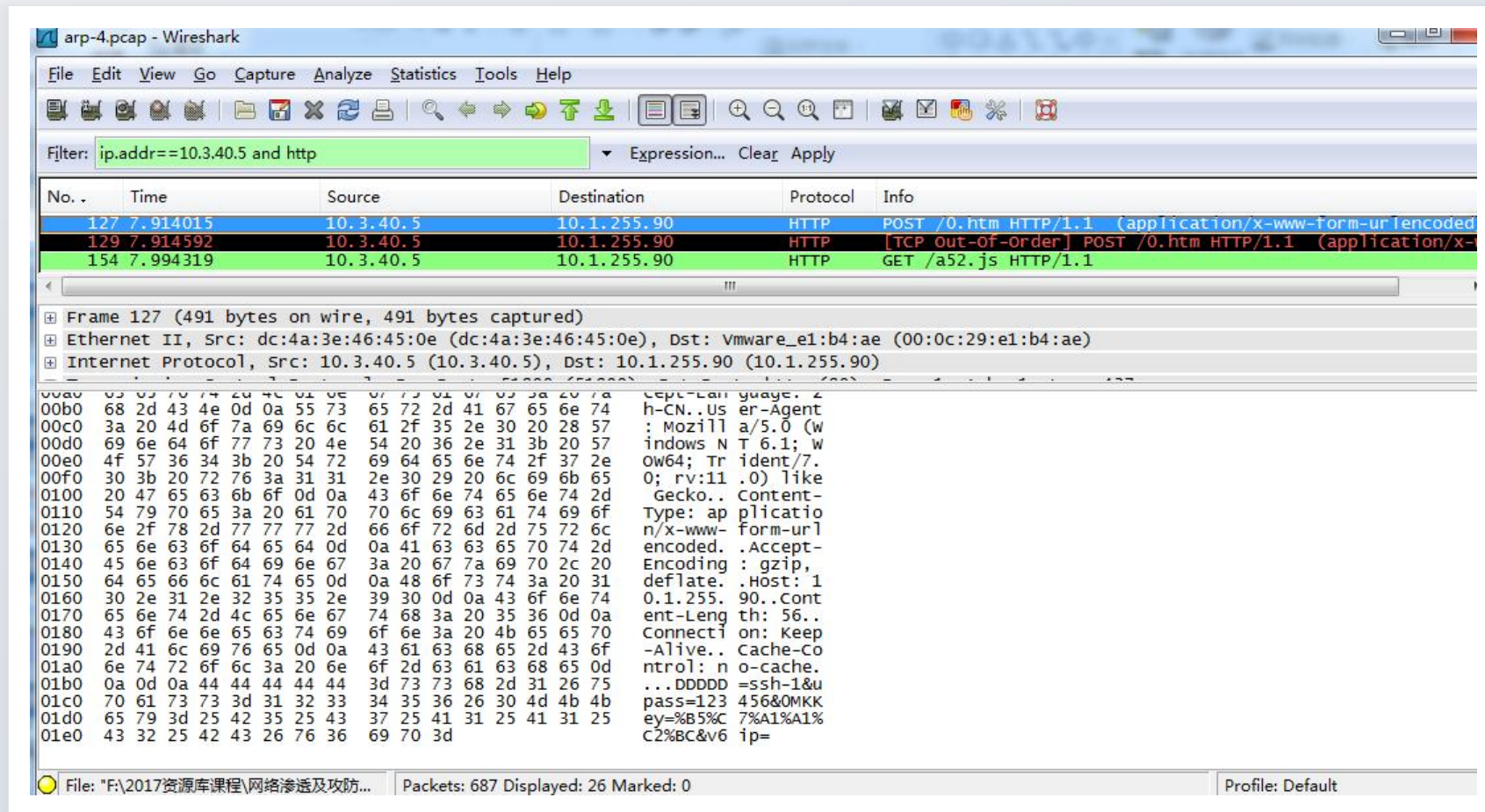


	Destination	Protocol	Info
	10.1.255.90	HTTP	POST /0.htm HTTP/1.1
	10.1.255.90	HTTP	[TCP out-Of-Order] P
	10.1.255.90	HTTP	GET /a52.js HTTP/1.1
	10.1.255.90	HTTP	[TCP out-Of-Order] c
	10.3.40.5	HTTP	HTTP/1.1 200 OK (te
	10.1.255.90	HTTP	GET /a51.js HTTP/1.1
	10.1.255.90	HTTP	GET /a50.css HTTP/1.1
	10.1.255.90	HTTP	[TCP out-Of-Order] c
	10.1.255.90	HTTP	[TCP out-Of-Order] c
	10.3.40.5	HTTP	[TCP out-Of-Order] H
	10.3.40.5	HTTP	HTTP/1.1 200 OK (te
	10.3.40.5	HTTP	HTTP/1.1 200 OK (te
	72.246.189.24	HTTP	GET /msdownload/upda
	72.246.189.24	HTTP	[TCP out-Of-Order] c
24	10.3.40.5	HTTP	HTTP/1.1 302 Moved T
24	10.3.40.5	HTTP	[TCP out-Of-Order] H
	10.1.255.90	HTTP	GET / HTTP/1.1
	10.1.255.90	HTTP	[TCP out-Of-Order] c
	10.3.40.5	HTTP	[TCP out-Of-Order] H
	72.246.189.24	HTTP	GET /msdownload/upda
	72.246.189.24	HTTP	[TCP out-Of-Order] c





## 2.7 ARP协议简介



## 2.7 ARP欺骗的防御



## 2.7 ARP欺骗的防御

防御方法1—MAC的静态绑定

在主机的ARP缓存表配置

静态记录: C:\>arp -s  
192.168.1.1 20-01-e6-  
b4-55-6c

防御方法2—第三方软件

