



# 网络安全

## 第四章 网络监听

黄 玮



- 代理模型中的嗅探问题
  - 所有通信数据都会经过代理服务器
- 网络数据包嗅探工具
  - Wireshark工具的高级使用
    - 协议分析 / 网络故障诊断



- 交换式网络环境依然可以网络监听
- 网络监听是通信内容机密性的大敌
- 如何抓出局域网中的嗅探者
- 如何防范网络监听



## 本章内容提要

- 网络监听原理
- 网络监听工具
- 网络监听的检测与防范
- 实验讲解



# 网络监听原理

---

- 被动监听
  - 共享式网络环境
  - 交换式网络环境
- 主动监听
  - 数据链路层的漏洞利用
  - ARP欺骗



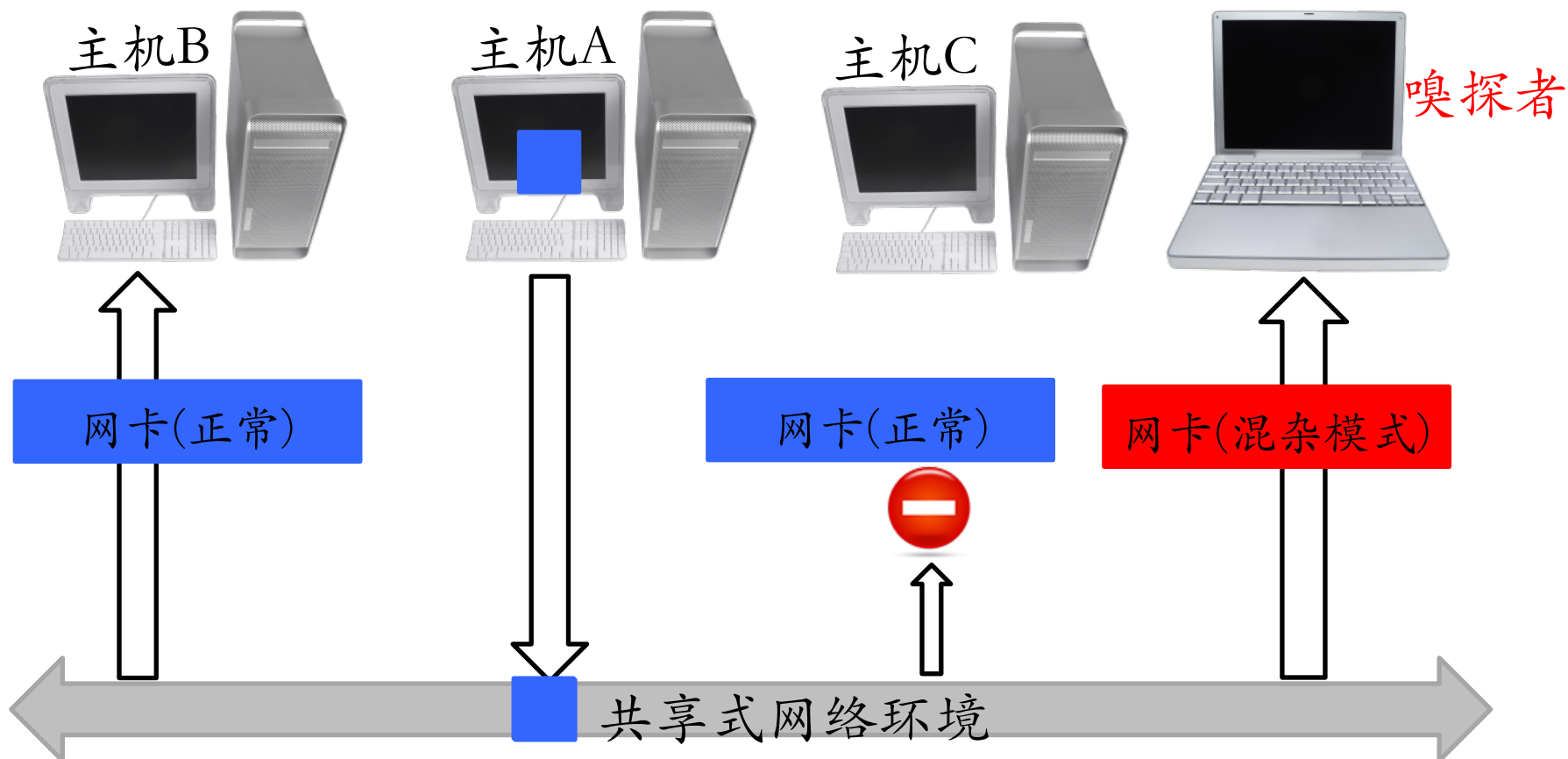
## 共享式网络环境

- IEEE 802.3以太局域网采用广播机制
  - 局域网上的所有主机共享相同的通信链路
  - 单个主机的标识
    - MAC (Media Access Control) 地址
- 网卡检查接收到的数据包的目的地址
  - 正常状态下的网卡操作
    - 只接收目的MAC地址是自己的数据包
    - 其他数据包丢弃
  - 混杂模式 完全被动的嗅探，很难发现嗅探者
    - 不检查目的MAC地址，来者不拒



# 共享式网络环境的被动监听原理

主机A发送数据包给主机B



广播模式：数据包被广播(传送)之局域网内所有在线主机



# 交换式网络环境

- 交换机的CAM表

- Content Addressable Memory

- 存储局域网中每台计算机的MAC地址

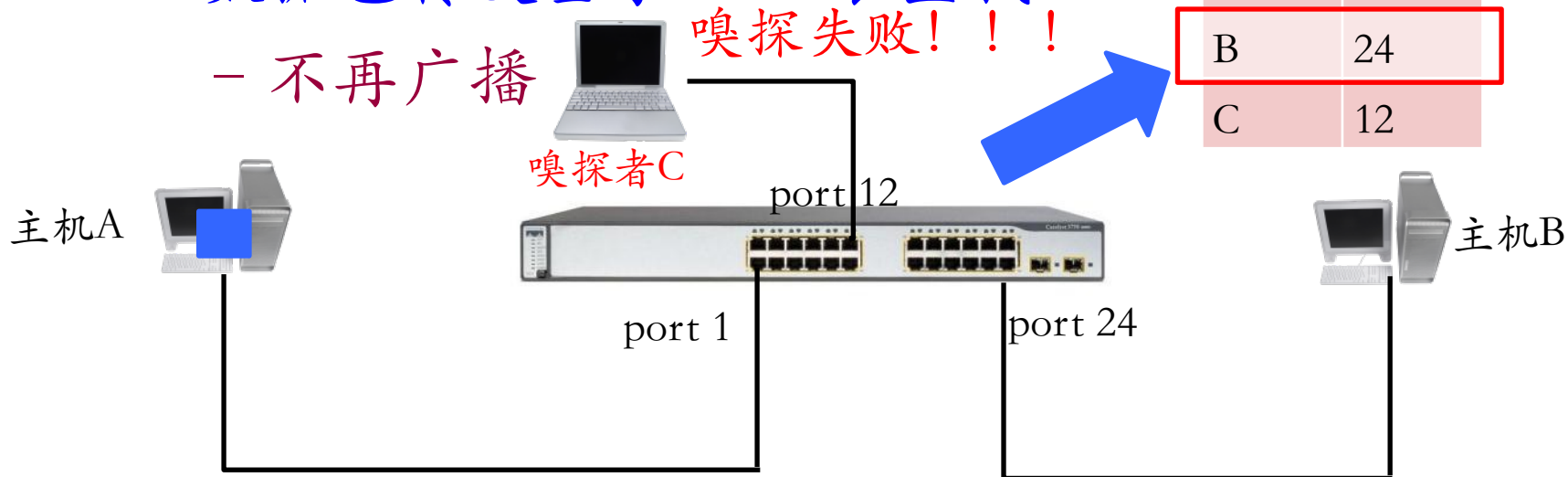
- MAC地址所连接的交换机端口号

- 数据包转发基于CAM表查找

- 不再广播

嗅探失败!!!

嗅探者C







交换式网络环境就没有被嗅探的可能了吗？

主动监听！



## 主动监听的原理

- 数据链路层的漏洞利用
  - ARP欺骗的三种模式
    - 终端ARP缓存投毒
      - 主动嗅探/中间人攻击
    - 交换机DoS
      - 强制交换机进入Hub模式：广播
    - 交换机投毒
      - 主动“污染”交换机的MAC-Port转发表
- Content Addressable Memory (CAM)



## 温故：ARP

- ARP: Address Resolution Protocol

- 地址解析协议

- 主机在发送帧前将目标IP地址转换成目标MAC地址的过程

- 局域网中的主机间通信依赖于ARP找到目标主机

- 局域网中的主机访问外网依赖于ARP找到网关

- ARP表

- 动态学习

- 静态配置

```
C:\Users\huangwei>arp -a
```

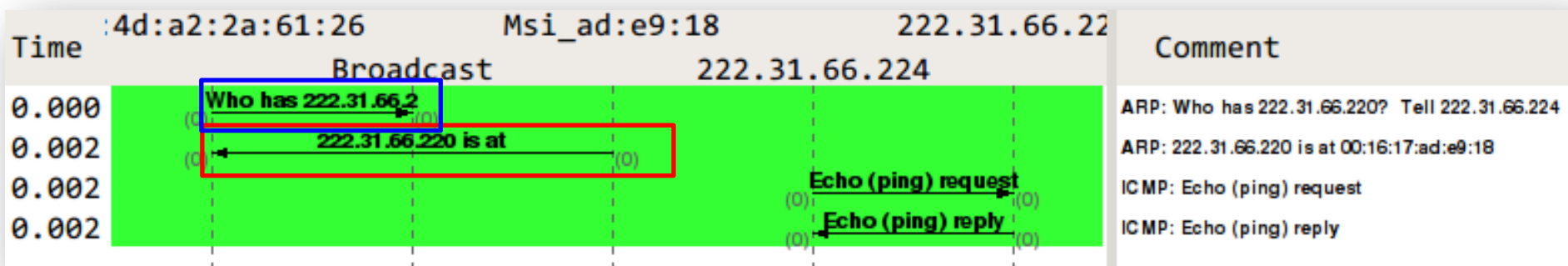
```
接口: 10.0.2.15 --- 0xb
```

Internet 地址	物理地址	类型
10.0.2.2	52-54-00-12-35-02	动态
10.0.2.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态



# ARP 实例

No.	Time	Source	Destination	Protocol	Info
1	0.000000	f0:4d:a2:2a:61:26	Broadcast	ARP	Who has 222.31.66.220? Tell 222.31.66.224
2	0.001709	Msi_ad:e9:18	f0:4d:a2:2a:61:26	ARP	222.31.66.220 is at 00:16:17:ad:e9:18
3	0.001717	222.31.66.224	222.31.66.220	ICMP	Echo (ping) request
4	0.001875	222.31.66.220	222.31.66.224	ICMP	Echo (ping) reply



ARP请求： 可以看作是提问

ARP响应： 可以看作是举手



- Gratuitous ARP (GARP)

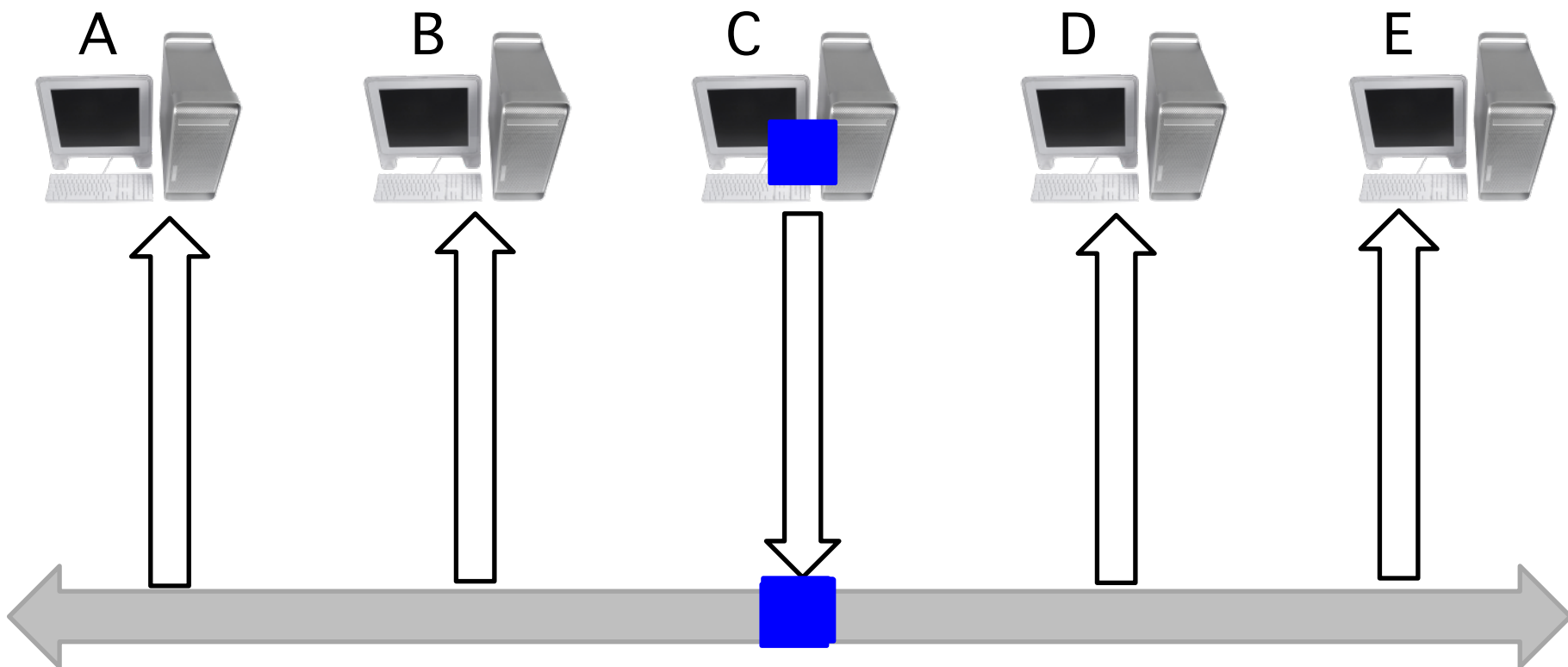
- 无故ARP

- 检查重复地址或IP地址冲突（如果收到ARP响应则表明存在重复地址或IP地址冲突）
    - 用于通告一个新的数据链路标识

当一个设备收到一个arp请求时，发现arp缓冲区中已有发送者的IP地址，则更新此IP地址的MAC地址条目。



# GARP演示



Hey, everyone! I'm C, my IP address is  $ip_c$  and my MAC address is  $mac_c$

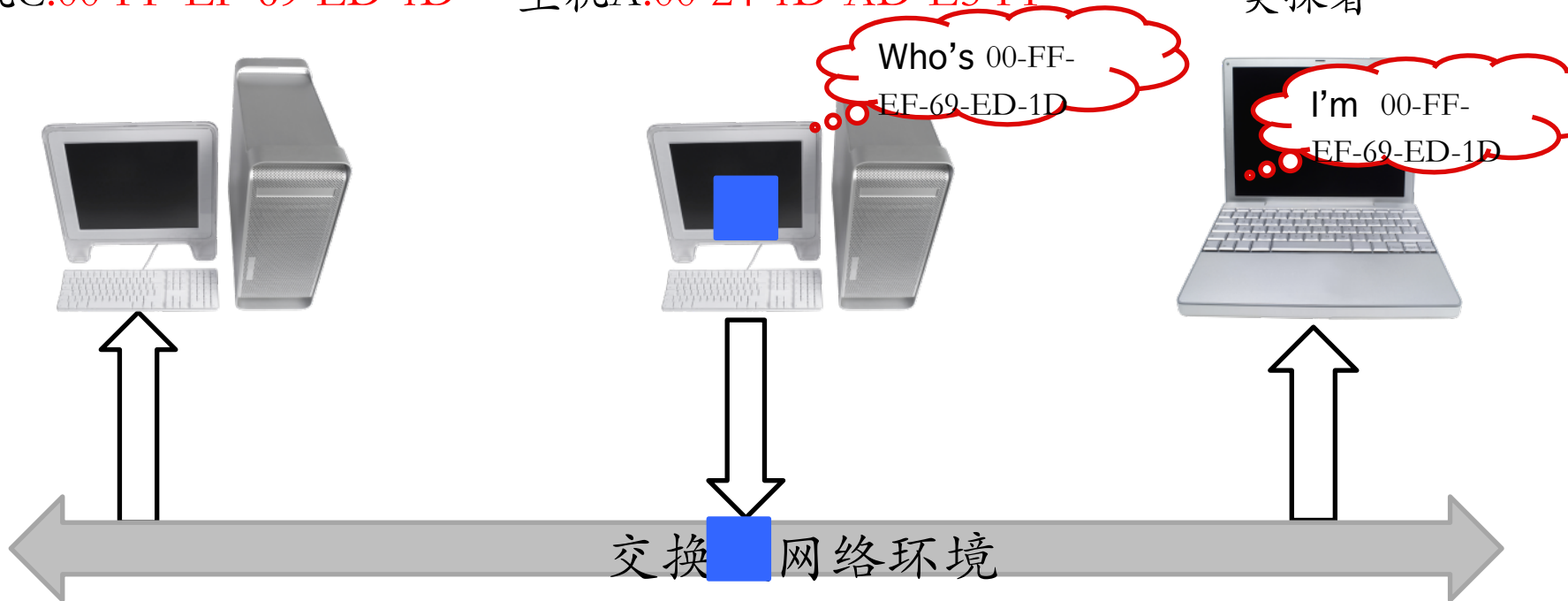


# 终端ARP缓存投毒——向发送方投毒

主机C:00-FF-EF-69-ED-1D

主机A:00-24-1D-AD-E5-FF

嗅探者



主机A

嗅探成功!!!

主机C



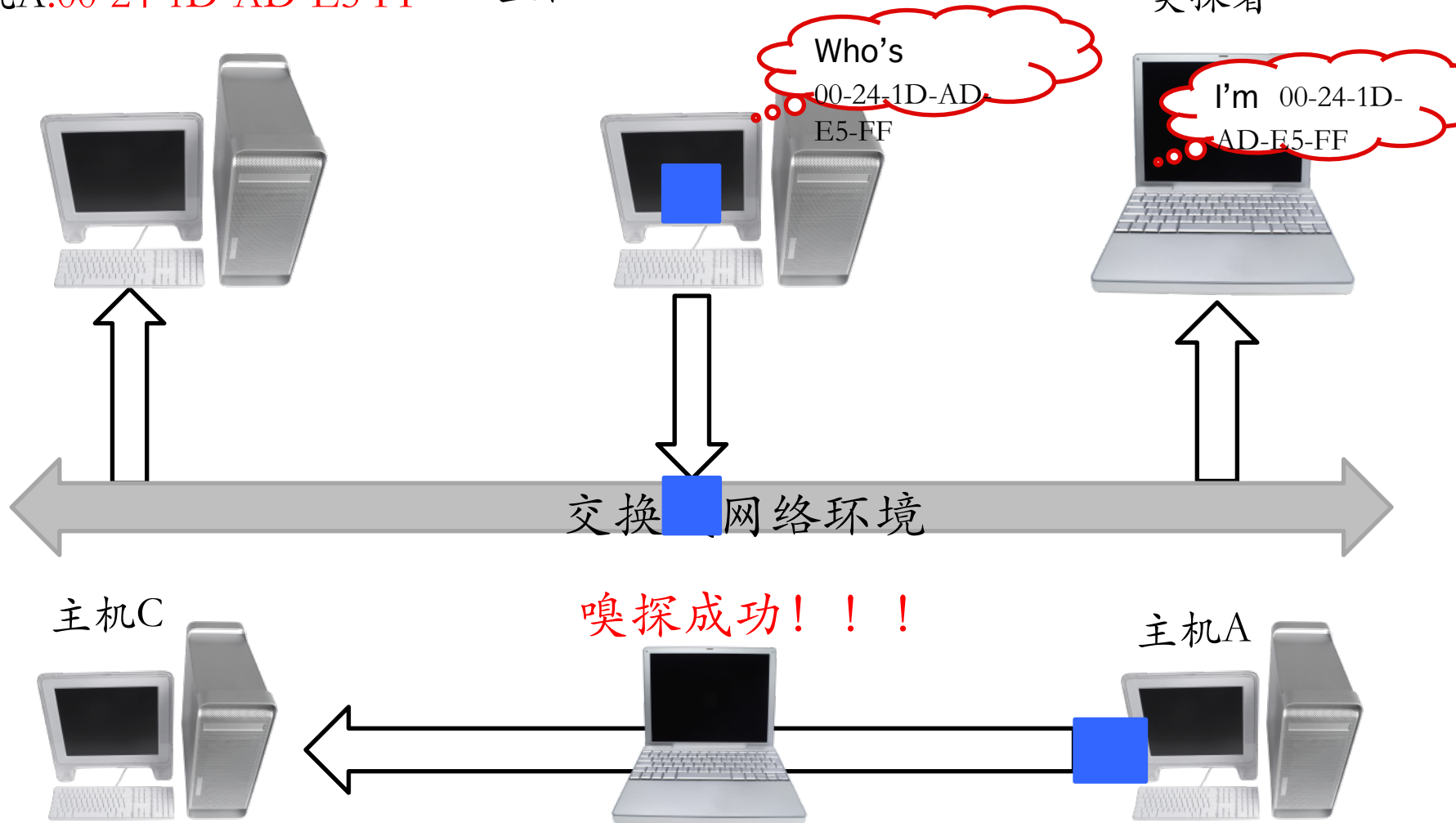


# 终端ARP缓存投毒——向接收方投毒

主机A:00-24-1D-AD-E5-FF

主机C:00-FF-EF-69-ED-1D

嗅探者

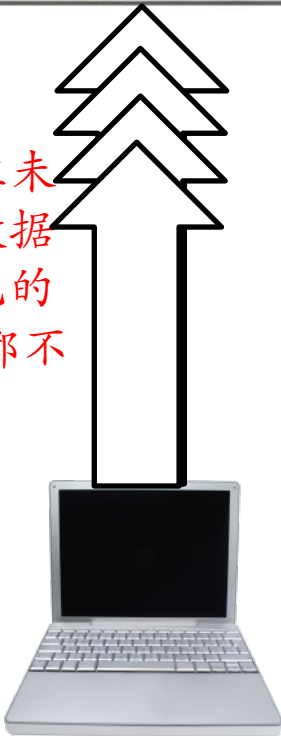






# 交换机DoS

不断发送去往未知目的地的数据帧，且每个包的源MAC地址都不同



CAM表满

MAC	端口
A	1
B	24
C	12

该表是MAC地址与交换机物理端口的对应关系，存储容量有限



迫使交换机退化为HUB，进入广播状态

还记得之前的共享式网络被动监听原理吗？

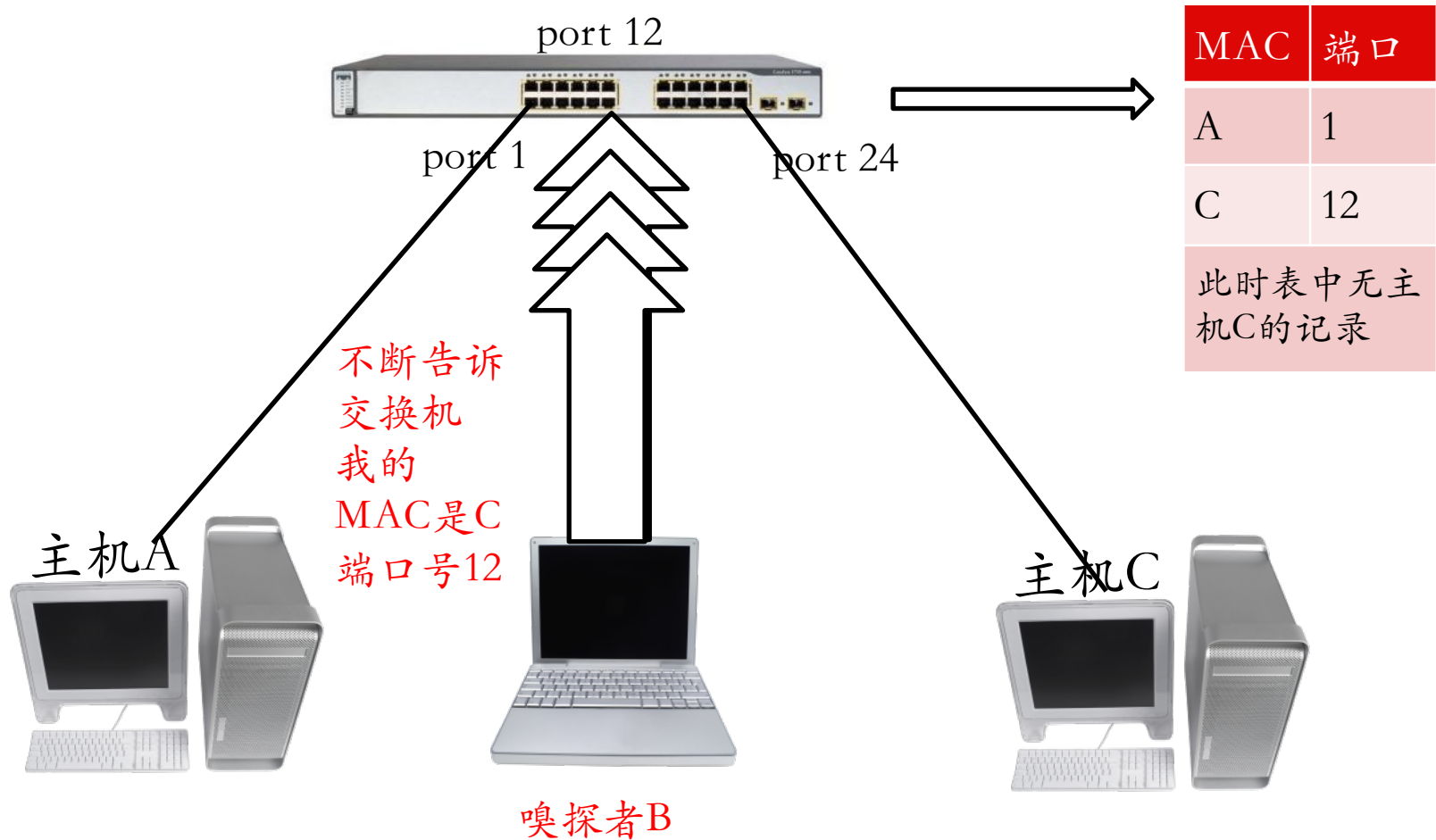
bingo!

We get it works!



## 交换机投毒 (1/4)

主机A发送数据包给主机C之前





## 交换机投毒 (2/4)

主机A发送数据包给主机C

port 12



port 1

port 24

MAC	端口
A	1
C	12
此时表中无主机C的记录	

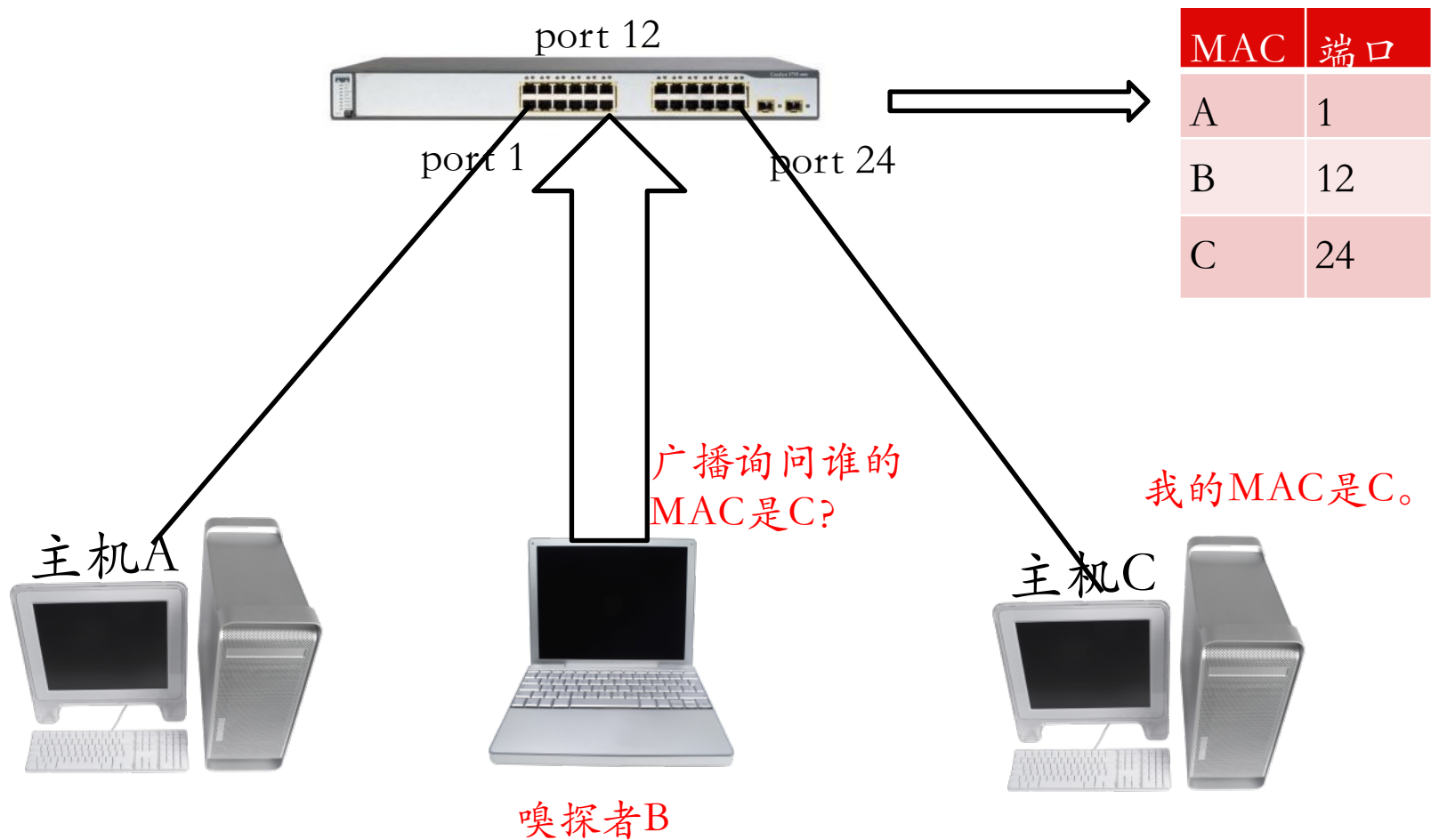


嗅探者B



## 交换机投毒 (3/4)

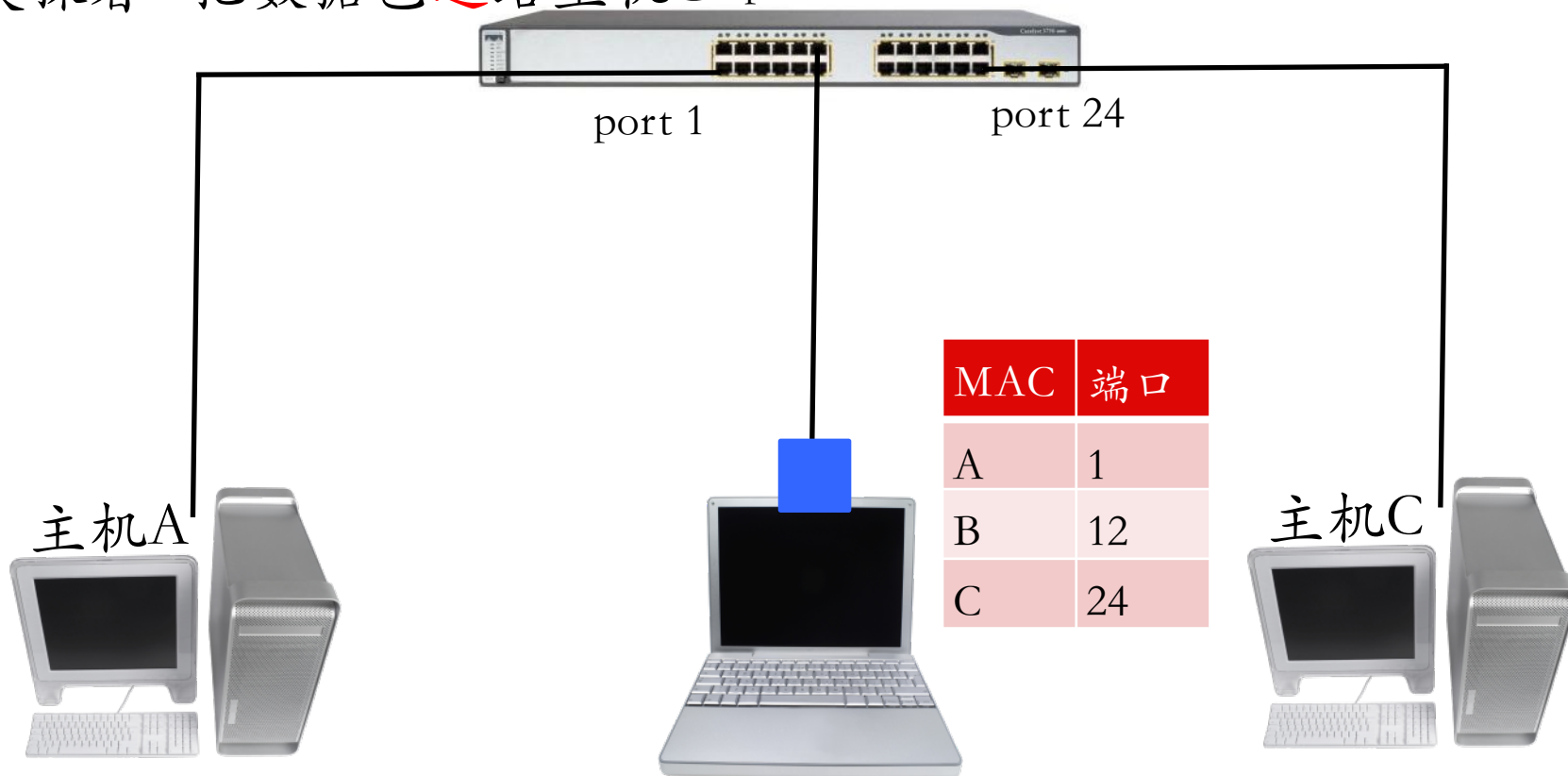
嗅探者B已完成对A->C的通信嗅探





## 交换机投毒 (4/4)

嗅探者B把数据包还给主机C port 12



嗅探者B



## 本章内容提要

---

- 网络监听原理
- 网络监听工具
- 网络监听的检测与防范
- 实验讲解



## 网络监听工具

---

- 被动监听
  - Wireshark
- 主动监听
  - dsniff
  - ettercap



## Wireshark 简介(1/2)

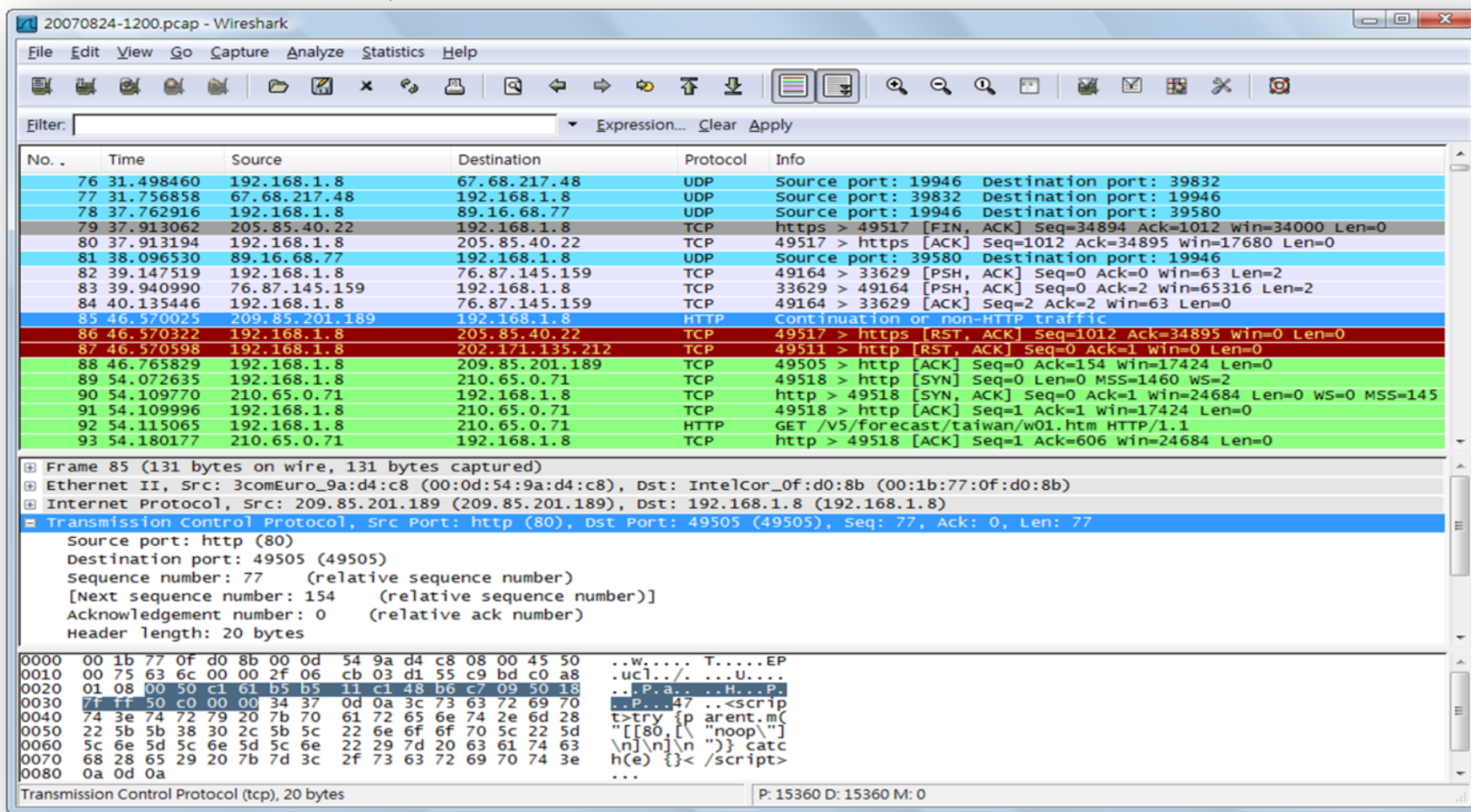
- Wireshark 是网络包分析工具，前身是Ethereal，主要用来捕获网络包，具有以下特性
  - 多平台支持：Win / Mac / \*nix
  - 实时捕获网络数据包
  - 详细显示数据包的协议信息
  - 读取/保存数据包
  - 支持基于规则的数据包/协议统计分析
  - 支持多种方式过滤捕获/显示网络数据包
  - 导入/导出其他网络嗅探程序支持的数据包格式
  - 多种方式查找包





# Wireshark 简介(2/2)

## • Wireshark 用户界面





## 命令行版wireshark的基本使用

- 捕获指定IP地址相关的数据包并保存到文件  
—`$sudo tshark -f "host <ip-address>" -w <output-file.pcap>`
- 获取当前系统上所有可捕获的网卡ID  
—`$sudo tshark -D`
- 指定数据包捕获所使用的网卡  
—`$sudo tshark -I <capture interface>`



## 不可思议的Wireshark功能(1/3)

- 大流量数据捕获优化
  - 非实时更新报文窗口
  - 文件切割保存
  - 禁用MAC地址/域名/协议类型反向解析
  - 自定义数据包捕获终结条件
    - 按报文个数 / 大小 / 捕获时间



## 不可思议的Wireshark功能(2/3)

- 自定义过滤规则
  - 数据包捕获时过滤规则——大流量数据捕获优化
  - 报文显示时过滤规则——协议分析辅助
- 网络状况分析
  - 网络质量参数分析
    - 按协议分类报文速率
    - 丢包率/重传报文数/畸形包数量
    - TCP QoS参数
  - RTT / 带宽 / 时序图
- 一键导出防火墙规则
  - Cisco IOS / iptables / windows firewall / IPFirewall



## 不可思议的Wireshark功能(3/3)

- 协议分析神器

- TCP/UDP会话跟踪

- Follow TCP/UDP Stream

- VoIP协议分析

- 信令 / 语音数据自动识别和提取

- 应用层负载数据关键词检索

- 二进制 / 十六进制 / 文本

- 一键导出保存应用层负载到

- 文本 / 二进制原始数据 / 十六进制 / C语言数组

- 报文统计规律

- 按报文长度 / 按协议分层会话 / 自定义报文显示过滤



## 常用报文**捕获**过滤规则举例

- 只捕获IP地址为**172.18.5.4**的相关报文  
—**host 172.18.5.4**
- 只捕获指定网段的相关报文  
—**net 192.168.0.0/24**
- 只捕获特定端口流量  
—**port 53 or port 80**
- 只捕获指定端口范围的TCP报文  
—**tcp portrange 1501-1549**



## 常用报文显示过滤规则举例

- 只显示SMTP和ICMP相关报文  
—tcp.port eq 25 or icmp
- 只匹配显示UDP报文头部或负载的连续3字节值为0x81, 0x60, 0x03  
—udp contains 81:60:03
- 应用层正则式匹配查找  
—sip.To contains “^a1762\$”  
—http.request.uri matches “^id=[\d]\*”



---

# Show Time!





## 协议分析样本资源

---

- Wireshark官方的报文样本库  
—<http://wiki.wireshark.org/SampleCaptures>
- Web 2.0 Packet Samples  
—<http://pcapr.net>



## 被动监听小结

- 网络管理
  - 网络质量监视
  - 网络故障排查
- 网络协议分析
  - 已知协议的自动化分析辅助
  - 未知协议的逆向分析辅助
- 一般方法
  - 应用命令行版数据捕获工具完成报文捕获
  - 使用GUI工具深入分析捕获的报文



## • 网络安全审计和渗透测试工具集

1. **arp spoof** 指定目标的**arp**欺骗重定向
2. **dnsspoof** 伪造**DNS**响应消息
3. **dsniff** 口令嗅探
4. **filesnarf** **NFS**文件流截获**dump**
5. **macof** 泛洪攻击交换机
6. **mailsnarf** 截获**SMTP**和**POP**协议邮件正文并**dump**为**Berkeley mbox**格式
7. **msgsnarf** 即时通信消息截获
8. **sshmitm** 针对**Open SSH V1**的**SSH**中间人攻击
9. **sshow** **SSH**流量分析工具
10. **tcpkill** 强行终止局域网中的**TCP**连接
11. **tcpnice** 强行降速局域网中的**TCP**连接
12. **urlsnarf** 嗅探局域网中的所有**HTTP**连接请求
13. **webmitm** 针对**HTTP/HTTPS**的局域网中间人攻击
14. **webspy** 将嗅探到的**HTTP**流量发送到本地浏览器实时查看



## dsniff的基本使用(1/2)

- dsniff常用指令参数

- f

- 从文件中加载触发器(也就是口令嗅探的服务类型, 文件格式参考*/etc/services*)

- i

- 使用特定的网络接口

- t

- 使用格式 *port /proto=service* 来加载一个以逗号为分隔符的触发器集

**dsniff -t 21/tcp=ftp,23/tcp=telnet**



## dsniff的基本使用(2/2)

- **sshmitm** 常用指令

- 拦截某主机的**ssh**连接密钥

- **sshmitm -p local\_port <remote\_ipaddress> [remote\_port]**

- **filesnarf** 常用指令

- 嗅探**NFS**流量中的文件

- 例如，只嗅探**mp3**文件

- **filesnarf \*.mp3**



## 本章内容提要

---

- 网络监听原理
- 网络监听工具
- 网络监听的检测与防范
- 实验讲解



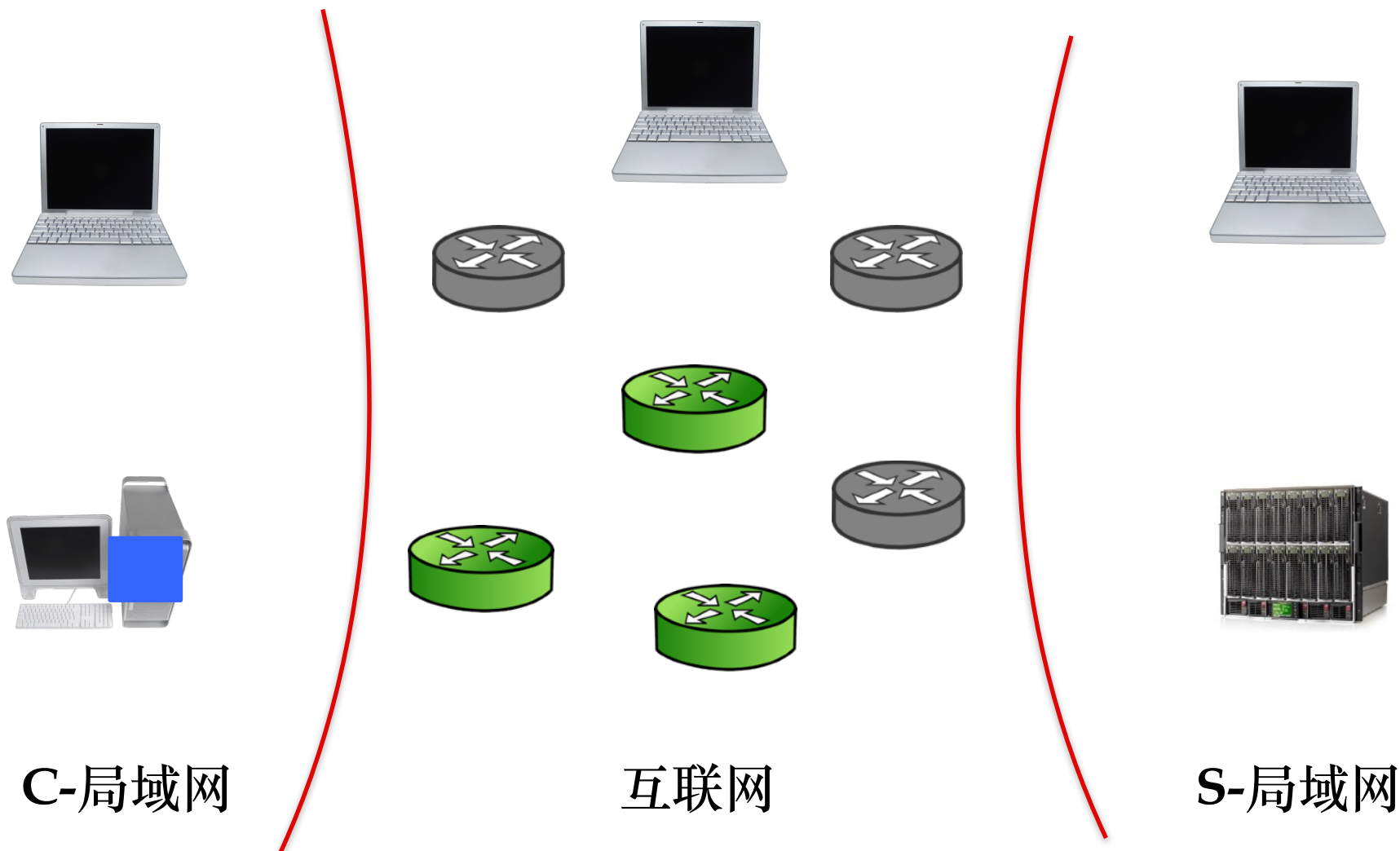
## 回顾：网络监听的方法

---

- 被动监听
  - 共享式网络环境
  - 交换式网络环境
- 主动监听
  - 终端ARP缓存投毒
  - 交换机DoS
  - 交换机投毒



# 扩展：任意网络拓扑主动监听的基本原理



C-局域网

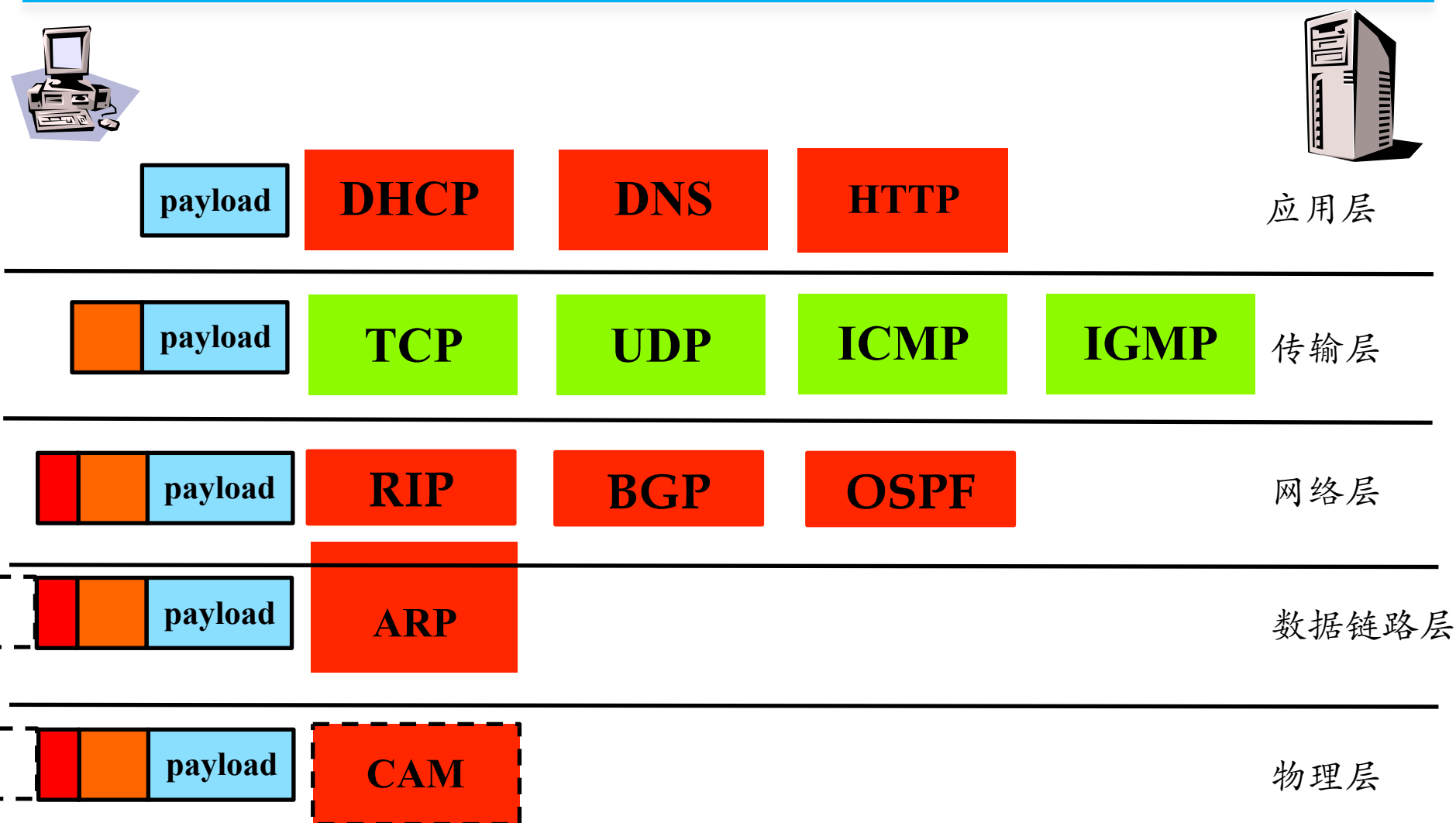
互联网

S-局域网





# 扩展：任意网络拓扑主动监听的基本原理





# 扩展：任意网络拓扑主动监听的基本原理



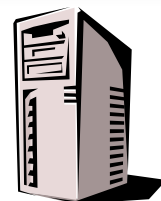
客户端



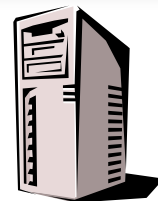
交换机



路由器



DNS



服务器端

DNS  
本机缓存

路由表

ARP表

CAM表

路由表

DNS  
局部缓存 /  
全局解析记录

DNS  
本机缓存

路由表

ARP表



## 扩展：任意网络拓扑主动监听的基本原理

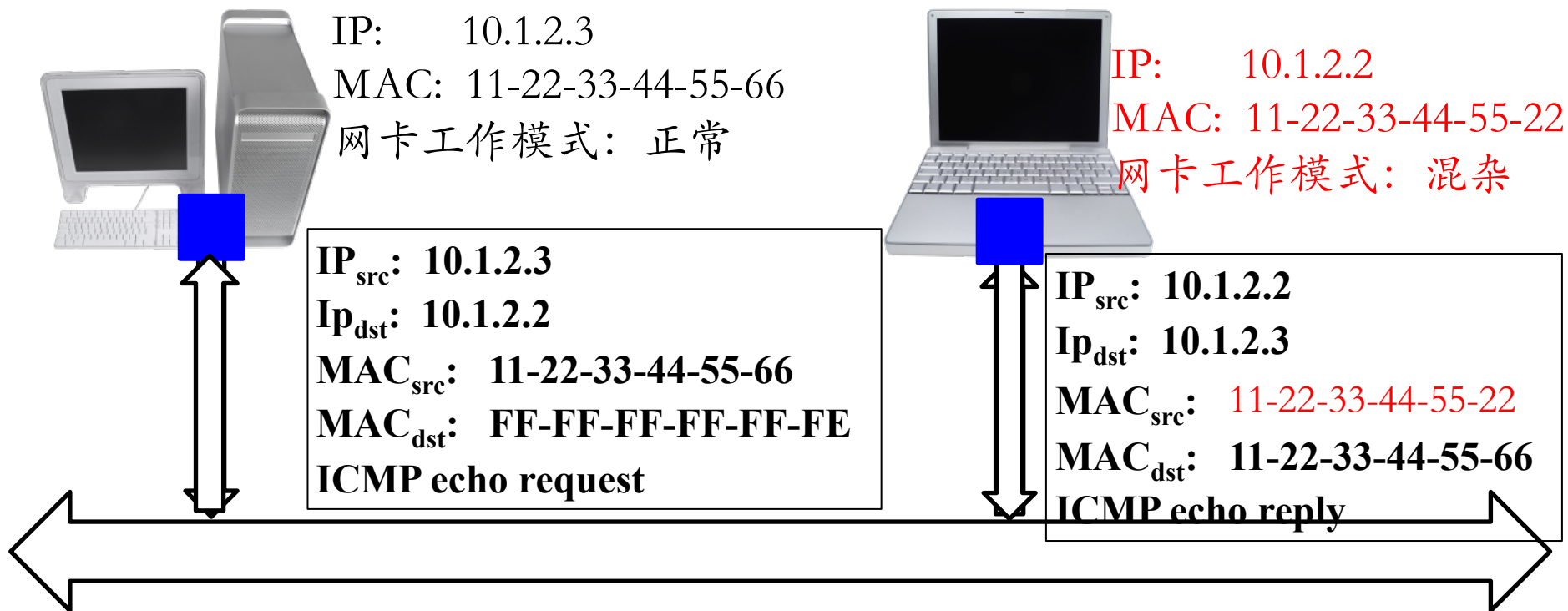
---

- 寻址机制是主动监听的攻击重点
  - 查找：CAM / ARP / 路由 / DNS
- 引流是主动监听的核心手段
  - 让通信流量（双向）通过监听者控制的设备、系统
- 获取通信负载是主动监听的核心目标



# 检测共享式网络环境中的监听者

- 检测混杂模式网卡



Bingo! 抓到混杂模式网卡了!!



## 检测交换式网络环境中的监听者

---

- 检测主动监听者  
——且看下文分解



## 检测终端ARP缓存投毒者

- 检测终端用户的ARP缓存表  
—发现异常ARP缓存记录

> arp -a

Internet 地址	物理地址	类型
10.0.2.2	52-54-00-12-35-02	动态

正常状态

> arp -a

Internet 地址	物理地址	类型
10.0.2.2	25-35-FE-12-35-12	动态

被投毒状态

桌面ARP防火墙可以有效检测、发现和防护



## 检测终端ARP缓存投毒者

- 发送ARP请求包
  - 正确的IP地址
  - 错误目的MAC地址
- 只有工作于混杂模式的网卡会响应该ARP请求数据包
- 工作于混杂模式网卡的操作系统内核会自动回应该ARP请求数据包



## 针对操作系统的检测

- 不同操作系统对ARP广播包的处理方式有差异

—例如:

– 虚假广播消息:

FF:FF:FF:FF:FF:FF:FF:FE (Br47):

Last bit missing

FF:FF:00:00:00:00:00:00 (BR16)

Only first 16 bits are the same as for broadcast.

FF:00:00:00:00:00:00:00 (BR8)

F0:00:00:00:00:00:00:00 (BR4)





## 针对操作系统的检测

- 不同操作系统的内核过滤机制有差异.

—例如:

— 虚假组播消息:

01:00:00:00:00:00:00:00 (Gr)

Only group-bit set.

01:00:5E:00:00:00:00:00 (M0)

Multicast address zero is usually not used

01:00:5E:00:00:00:00:01 (M1)(assigned to all)

Multicast address one should be received by all in the test system

01:00:5E:00:00:00:00:02 (M2)(assigned to different set of nodes)

Multicast address two should not be received by systems in the test group.

01:00:5E:00:00:00:00:03 (M3)(not registered)



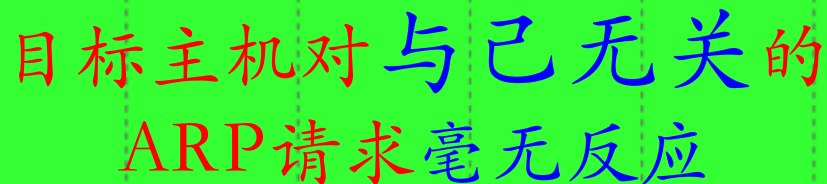
## 针对操作系统的检测

	Windows XP		WinME / 9x		Win2K/NT		Linux 2.4.x		Free BSD 5.0	
B47	--	X	--	X	--	X	--	X	--	X
B16	--	X	--	X	X	X	--	X	--	X
B8	--	--	--	X	--	--	--	X	--	X
Gr	--	--	--	--	--	--	--	X	--	X
M0	--	--	--	--	--	--	--	X	--	X
M1	O	O	O	O	O	O	O	O	O	O
M2	--	--	--	--	--	--	--	X	--	X
M3	--	--	--	--	--	--	--	X	--	X

不同ARP请求包的响应模式.

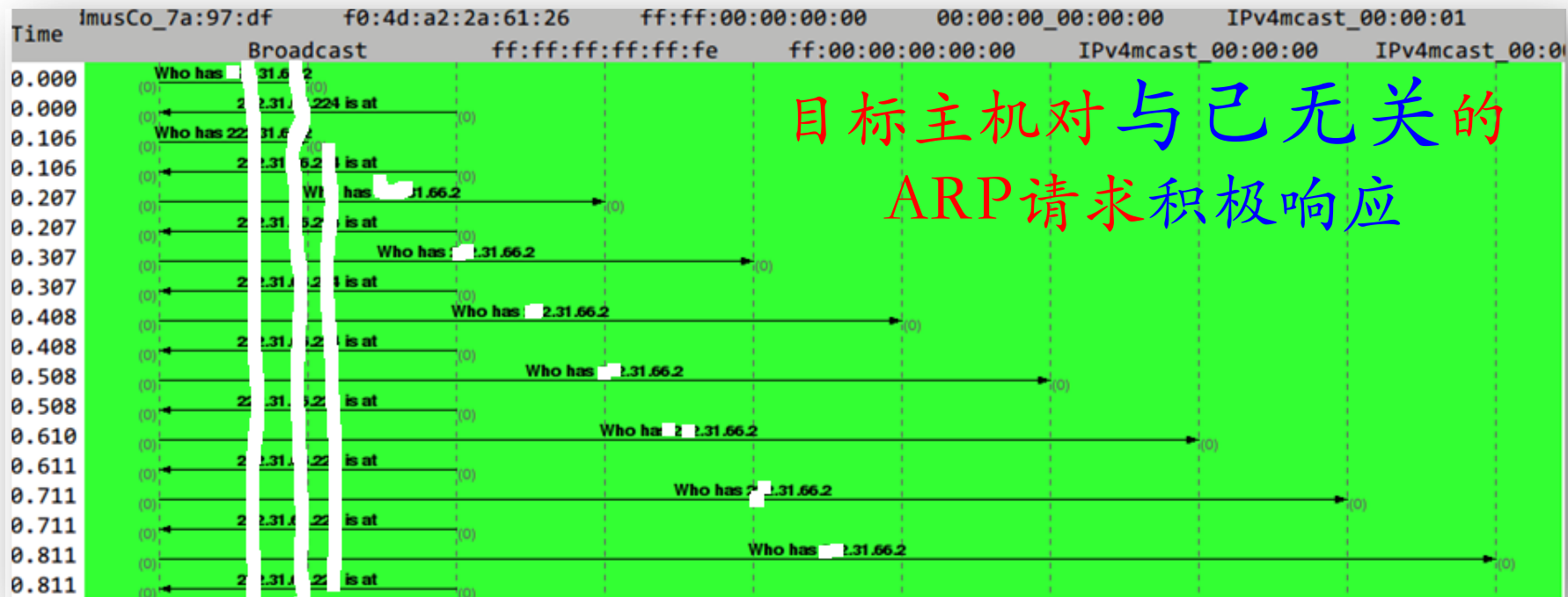
正常模式: 左侧 混杂模式: 右侧

O 合法响应, X 非法响应, -- 无响应





## 混杂模式网卡对ARP请求的响应实例





## 检测交换机DoS攻击

- 网络抓包分析
  - 启用交换机的端口镜像
  - 重点关注
    - 链路通信质量参数：丢包率/重传率
    - 未知MAC地址



## 检测交换机投毒者

---

- 交换机CAM表中的异常更新记录  
——同一个MAC地址反复被映射到不同物理端口



## 终端用户如何防范网络嗅探攻击

- 安装桌面型ARP防火墙  
— 防护终端ARP投毒
- 配置静态ARP地址表  
— 绑定网关IP与MAC地址
  - `arp -s <网关IP> <网关MAC>`
- 敏感数据加密后再传输并使用加密通信协议
  - 应用层（负载）加密
  - 遵循“纵深防御”原则



# 网络管理员如何防范网络嗅探攻击

- 启用并正确配置交换机的安全机制
  - 交换机的端口安全机制
    - 交换机物理端口和MAC地址的静态绑定
    - 限制交换机单个物理端口可以动态绑定的MAC地址数量
  - 划分VLAN
- 部署内网安全监控设备
  - 监视异常网络状况
    - 丢包 / 重传 / 畸形包 / 广播风暴 …





## 本章内容提要

---

- 网络监听原理
- 网络监听工具
- 网络监听的检测与防范
- 实验讲解



## 实验案例

- 实验一：检测局域网中的异常终端
- 实验二：交换式局域网的口令嗅探
  - 实验目的
  - 实验工具
  - 实验步骤
  - 实验分析



# 实验一：检测局域网中的异常终端

- 使用前述方法

- 终端上查看ARP缓存表

- arp -an

- 检测网卡是否工作于混杂模式状态

- nmap -sP --script=sniffer-detect <remote\_ip>

- 使用scapy的promiscping和自己对照课件内容构造2层报文直接发送



# 实验一：检测局域网中的异常终端

```
In [3]: promiscping('192.168.56.101', iface='eth1')
Begin emission:
Finished to send 1 packets.

Received 0 packets, got 0 answers, remaining 1 packets
Out[3]:
(<PROMISCPing: TCP:0 UDP:0 ICMP:0 Other:0>,
 <Unanswered: TCP:0 UDP:0 ICMP:0 Other:1>)
```

```
In [4]: pkt = Ether(dst = 'FF:FF:FF:FF:FF:FE')/IP(dst='192.168.56.101')/ICMP()

In [5]: promiscping('192.168.56.101', iface='eth1')
Begin emission:
Finished to send 1 packets.

Received 0 packets, got 0 answers, remaining 1 packets
Out[5]:
(<PROMISCPing: TCP:0 UDP:0 ICMP:0 Other:0>,
 <Unanswered: TCP:0 UDP:0 ICMP:0 Other:1>)
```



# 实验一：检测局域网中的异常终端

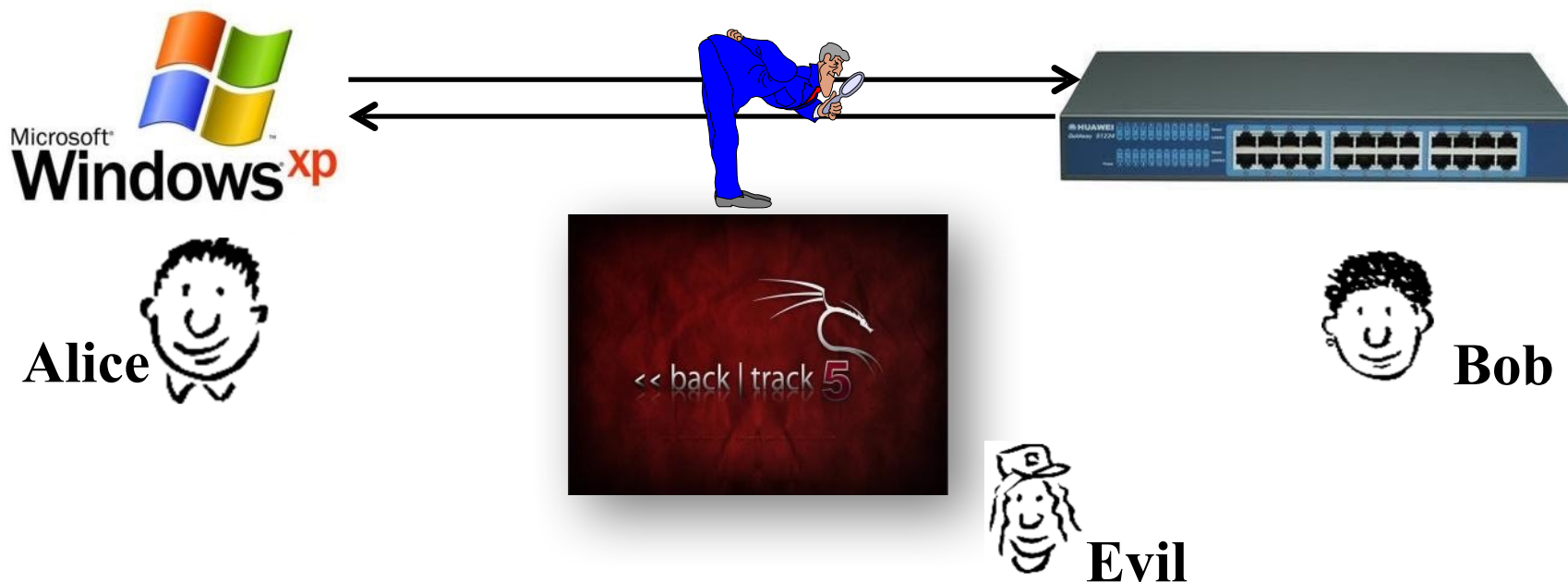
---

- 交换机状态查看（可网管的交换机）
  - CAM表变化情况
  - 是否受迫进入半双工模式
- 在发送者和接收者主机上分别抓包分析
  - 检测网卡是否处于混杂模式使用的数据包内容有什么区别



## 实验二：交换式局域网的口令嗅探

- 实验目的  
—通过Ettercap嗅探交换式局域网的口令
- 实验说明





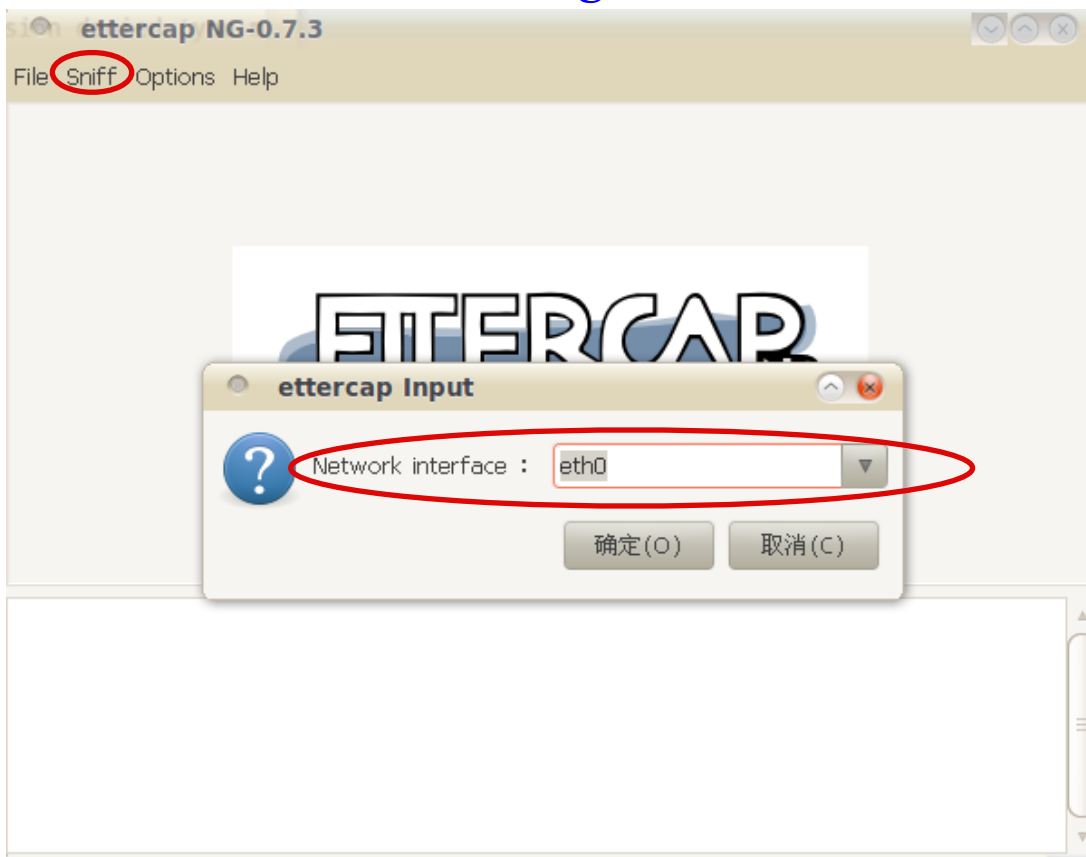
## 实验二：交换式局域网的口令嗅探

- Ettercap简介
  - Ettercap是一个多功能的中间人攻击（MITM）工具
- Ettercap两个主要的嗅探选项
  - UNIFIED
    - 一般我们选用这个，下面有演示
  - BTIDGED
    - 桥接模式，用于双网卡



## 实验二：交换式局域网的口令嗅探

- 选择用于嗅探数据包的网络接口  
—Sniff->Unified sniffing->eth0

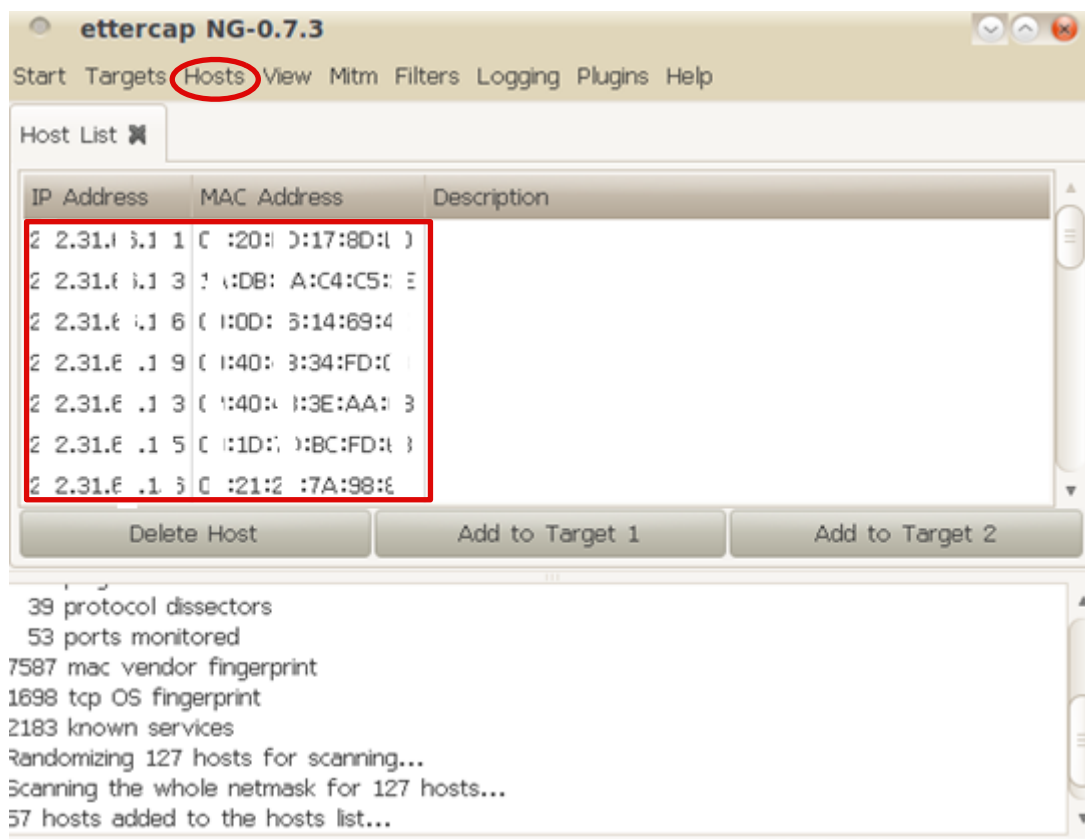






## 实验二：交换式局域网的口令嗅探

- 探测局域网内的主机列表  
—Hosts->Scan for hosts->Hosts list

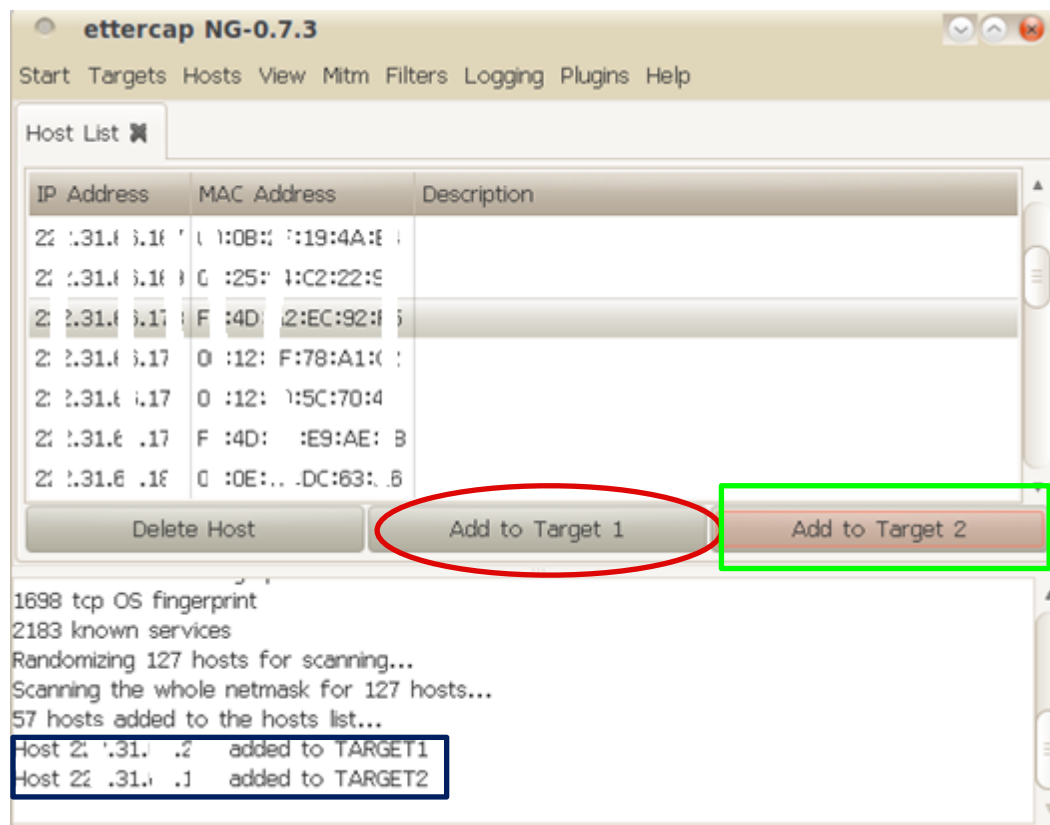




## 实验二：交换式局域网的口令嗅探

- 添加嗅探目标

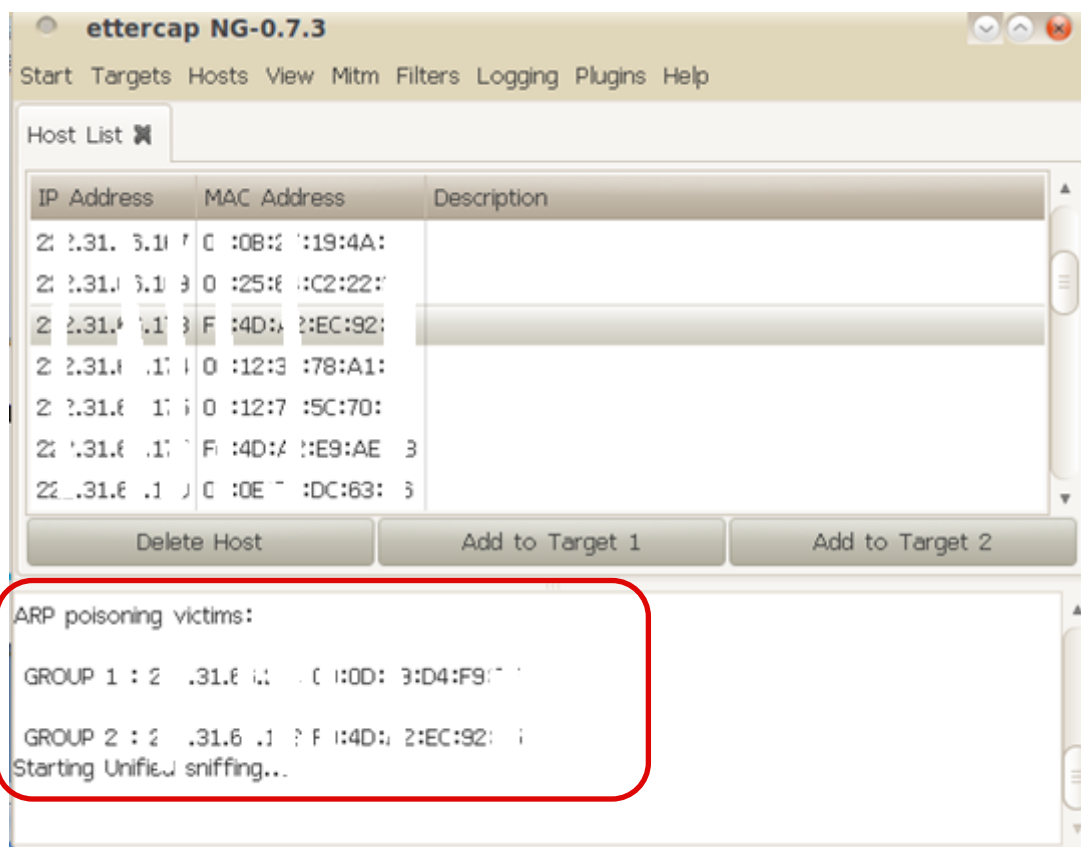
—网关->Add to Target1 被攻击者->Add to Target2





## 实验二：交换式局域网的口令嗅探

- 开始执行嗅探  
—start->start sniffing





## 实验二：交换式局域网的口令嗅探

- 重要提示

- Ettercap软件自身已具备数据包转发功能，请勿再次输入：`echo 1>/proc/sys/net/ipv4/ip_forward`,开启内核的数据包转发功能，以免同一数据包被转发两次

- 源主机和目标主机进行了数据通信，且涉及到了疑似用户名和密码的数据等，捕捉的信息将会显示

- 被攻击者的arp缓冲区的网关MAC地址被篡改  
为攻击者的MAC地址



## 本章小结

- 访问控制是（操作）系统安全的基础
  - 访问控制策略
    - 决策层安全：理论和模型安全
  - 访问控制机制
    - 实现机制安全
- 局域网的安全管理是网络安全的网络基础
  - 任何网络层加密数据在一个不安全的局域网中都有可能被嗅探
  - 攻击者一旦渗透进入内部网络，后果不堪设想
  - 内网安全先从管好ARP协议开始



## 参考文献

- ① S. Convery, Hacking Layer 2: Fun with Ethernet Switches. Blackhat [Online Document]. 2002. <http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf>
- ② 笑傲江湖之三层交换篇 [Online Document]. 2005. <http://t.cn/a01RFM>
- ③ dsniff官方网站: <http://monkey.org/~dugsong/dsniff/>
- ④ Wireshark官方wiki: <http://wiki.wireshark.org/>
- ⑤ 各种中间人攻击方法总结 <http://www.cnblogs.com/littlehann/p/3735602.html>



## 课后思考题

---

- 总结一下在交换式局域网环境中的网络攻防之术有哪些?
- 如何理解“仅仅使用VLAN划分的方法是无法彻底解决ARP欺骗与攻击”问题?