Website: http://www.allimagetool.com

攻击技术与防御

10.黑客攻击技术—网络欺骗技术

张晓炜

zhangxw@lzu.edu.cn

兰州大学 Lanzhou University

兰州大学信息科学与工程学院

网络欺骗技术

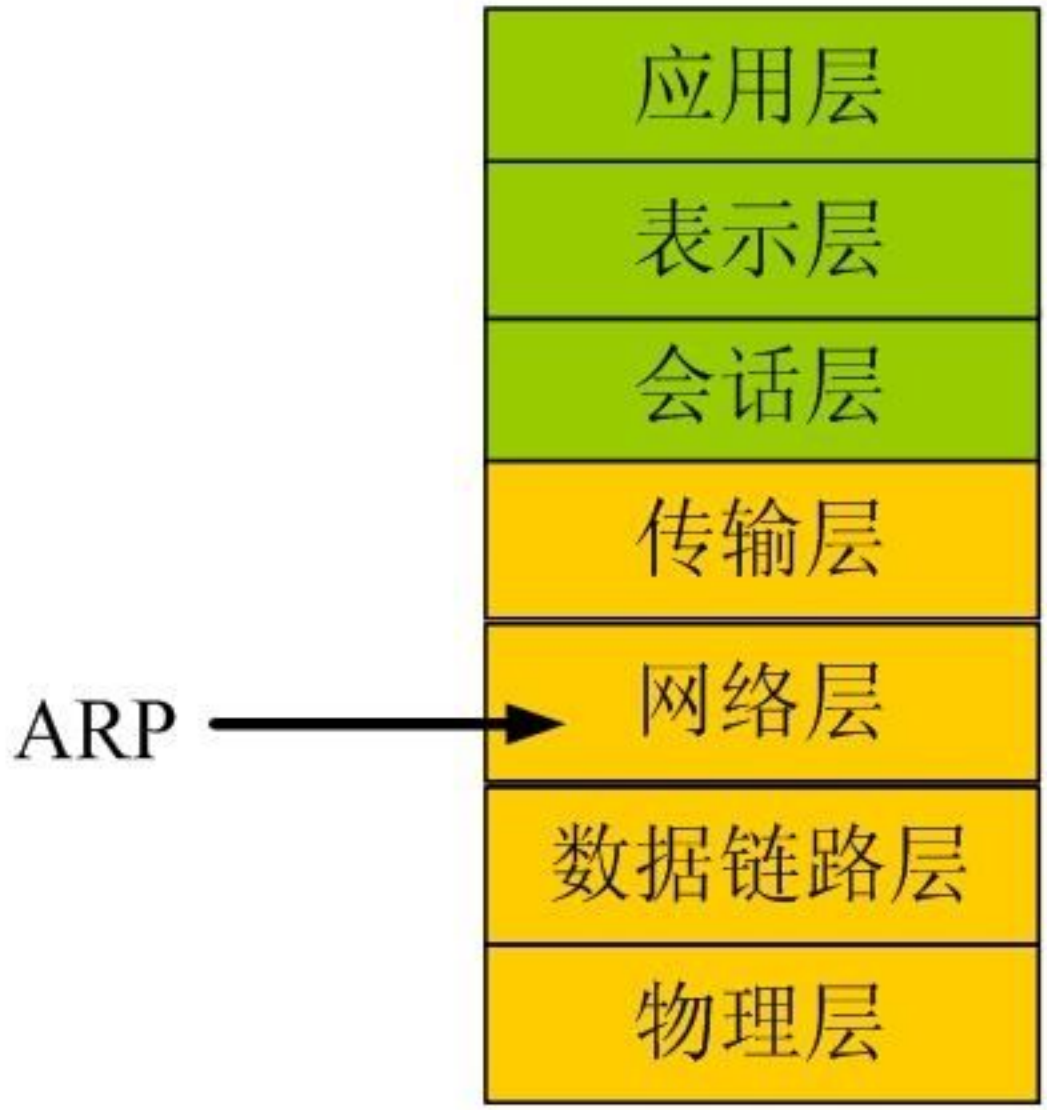
- 欺骗（**Spoofing**）：攻击者通过伪造一个网络数据包，从而得到目标主机的许可，以访问目标主机上的资源。
- 原因：**TCP/IP** 协议本身存在一些不安全隐患
- 欺骗通常作为一种进攻手段，用于获得目标主机的信任关系之后，再利用这种信任关系对目标主机进行攻击。

内容

1. ARP欺骗
2. IP欺骗
3. 路由欺骗攻击
4. 电子邮件欺骗
5. Web欺骗
6. 非技术类欺骗

ARP欺骗

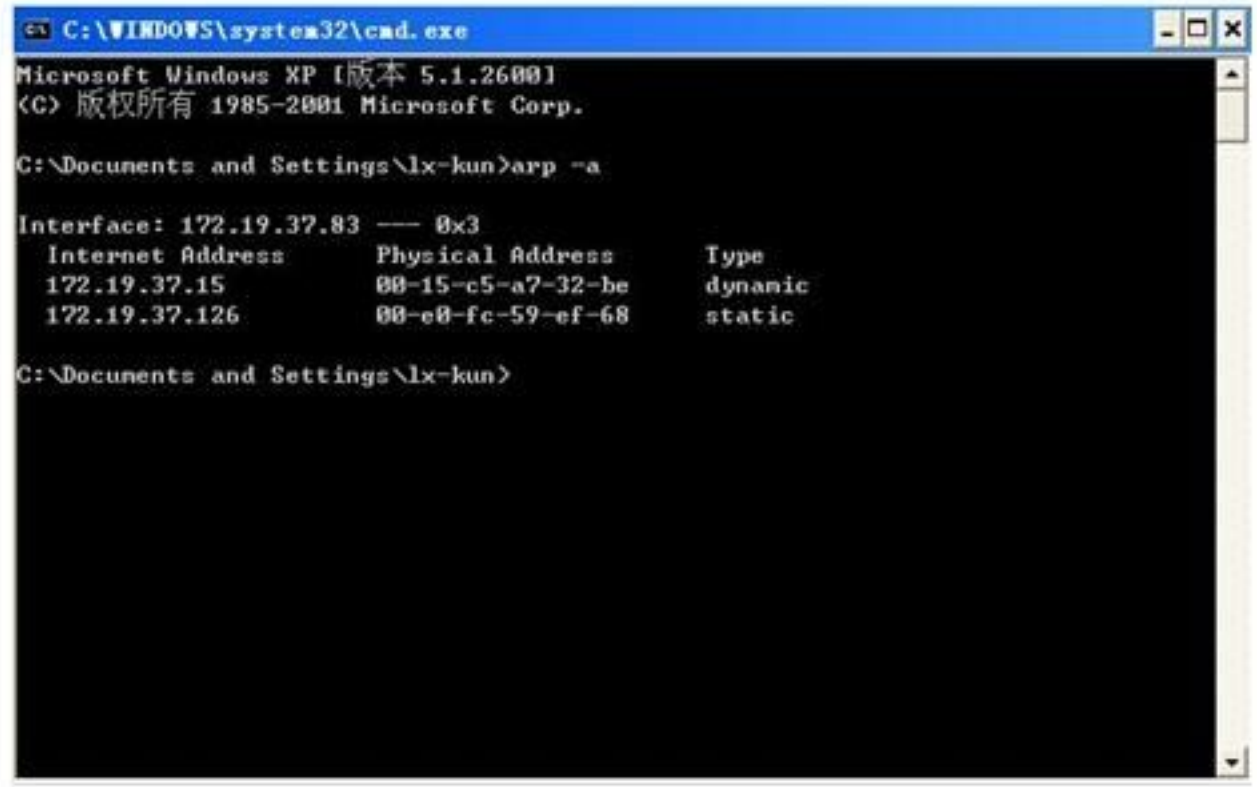
- ARP(Address Resolve Protocol)地址请求解析协议，用于寻找和IP 地址相对应的MAC地址。
- 在RFC 826中定义了ARP协议的数据格式和类型。
- ARP协议属于在网络层的下部，可看作为网络层和数据链路层的接口，主要用于IPv4以太网。
- ARP工作在同一网段，不能路由。



ARP Table

■ ARP Table

- 高速缓存区中保存最近获得的ARP表项
- 高速缓冲区中ARP表项新鲜性的保持：计时器



■ ARP Table的更新

- 静态绑定(static)
- 动态更新(dynamic)

arp –s 172.19.37.126 00-e0-fc-59-ef-68

ARP Table

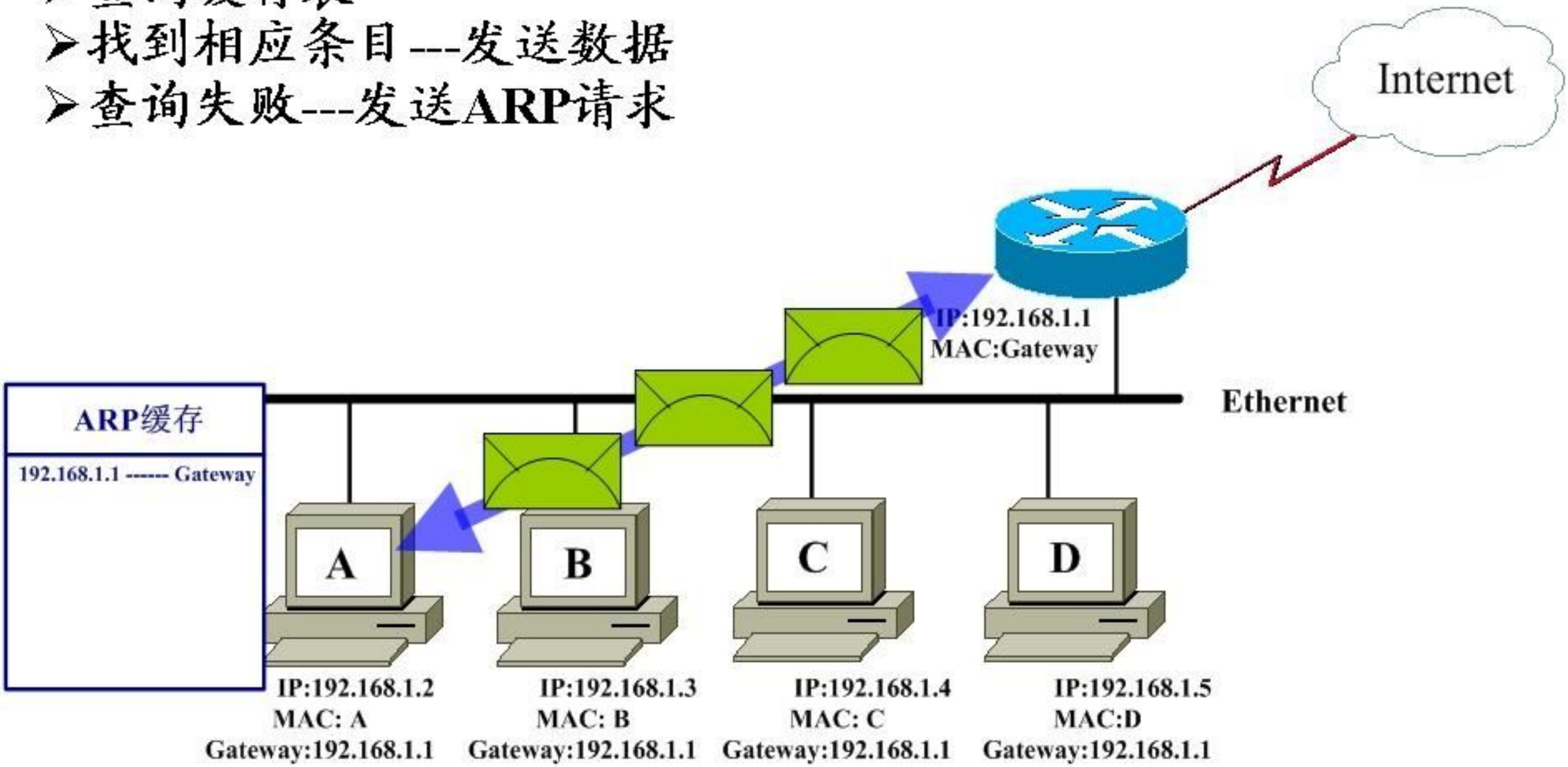
- **ARP Table 动态更新规则**
  - 源主机在发出ARP请求，接收到ARP应答后将目的主机的IP地址与物理地址映射关系存入自己的高速缓冲区。
  - 目的主机接收到ARP请求后将源主机的IP地址与物理地址映射关系存入自己的高速缓冲区。
  - ARP请求是广播发送的，网络中的所有主机接收到ARP请求后都可以将源主机的IP地址与物理地址映射关系存入自己的高速缓冲区。

ARP Table

- **ARP Table 计时器TTL（windows）**
  - 新表项加入时定时器开始计时
  - 表项添加后2分钟内没有被再次使用：删除
  - 表项被再次使用：增加2 分钟的生命周期
  - 表项始终在使用：最长生命周期为10 分钟

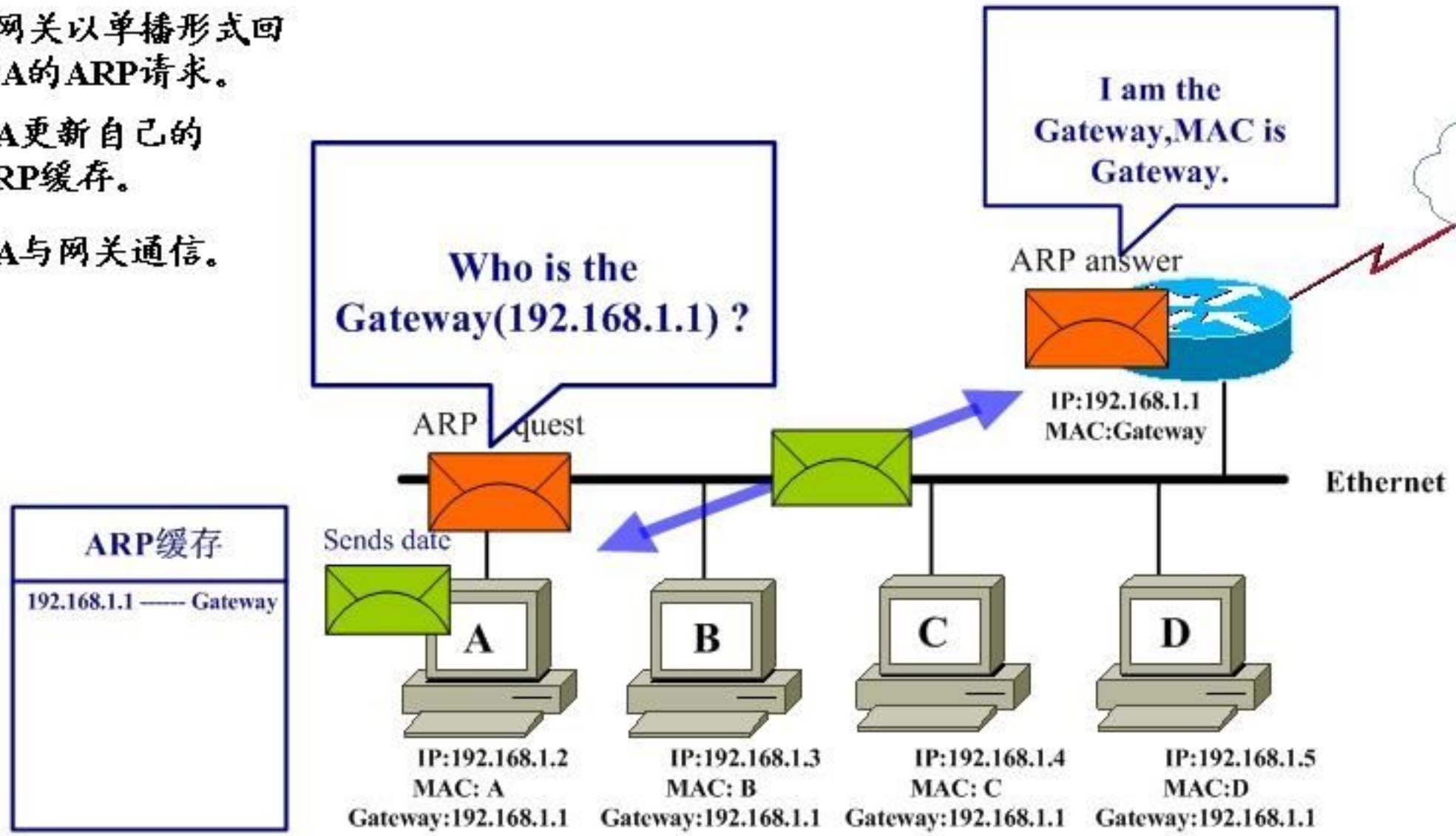
ARP例子

- 查询缓存表
- 找到相应条目---发送数据
- 查询失败---发送ARP请求



ARP例子

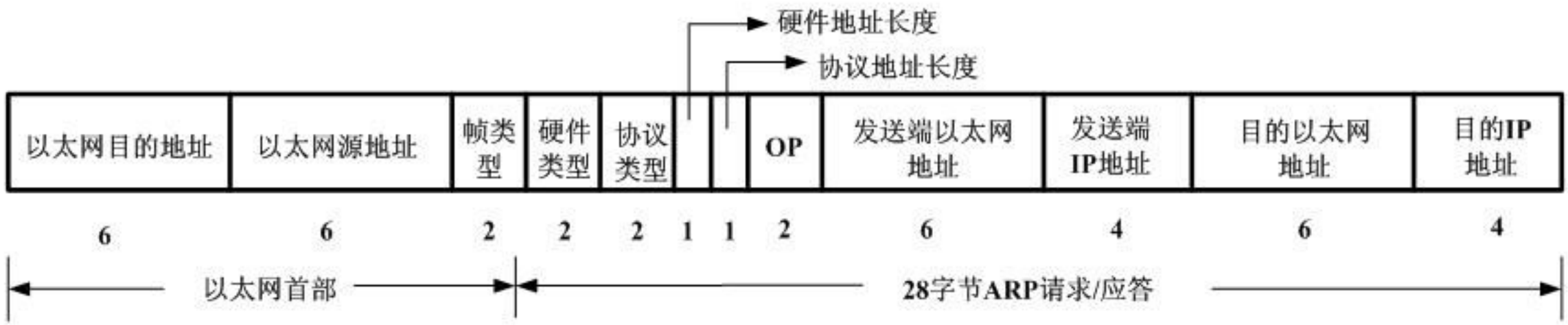
- 1.PCA以广播形式发送ARP请求,请求网关的MAC地址。
- 2.网关以单播形式回应A的ARP请求。
- 3.A更新自己的ARP缓存。
- 4.A与网关通信。



ARP分组格式

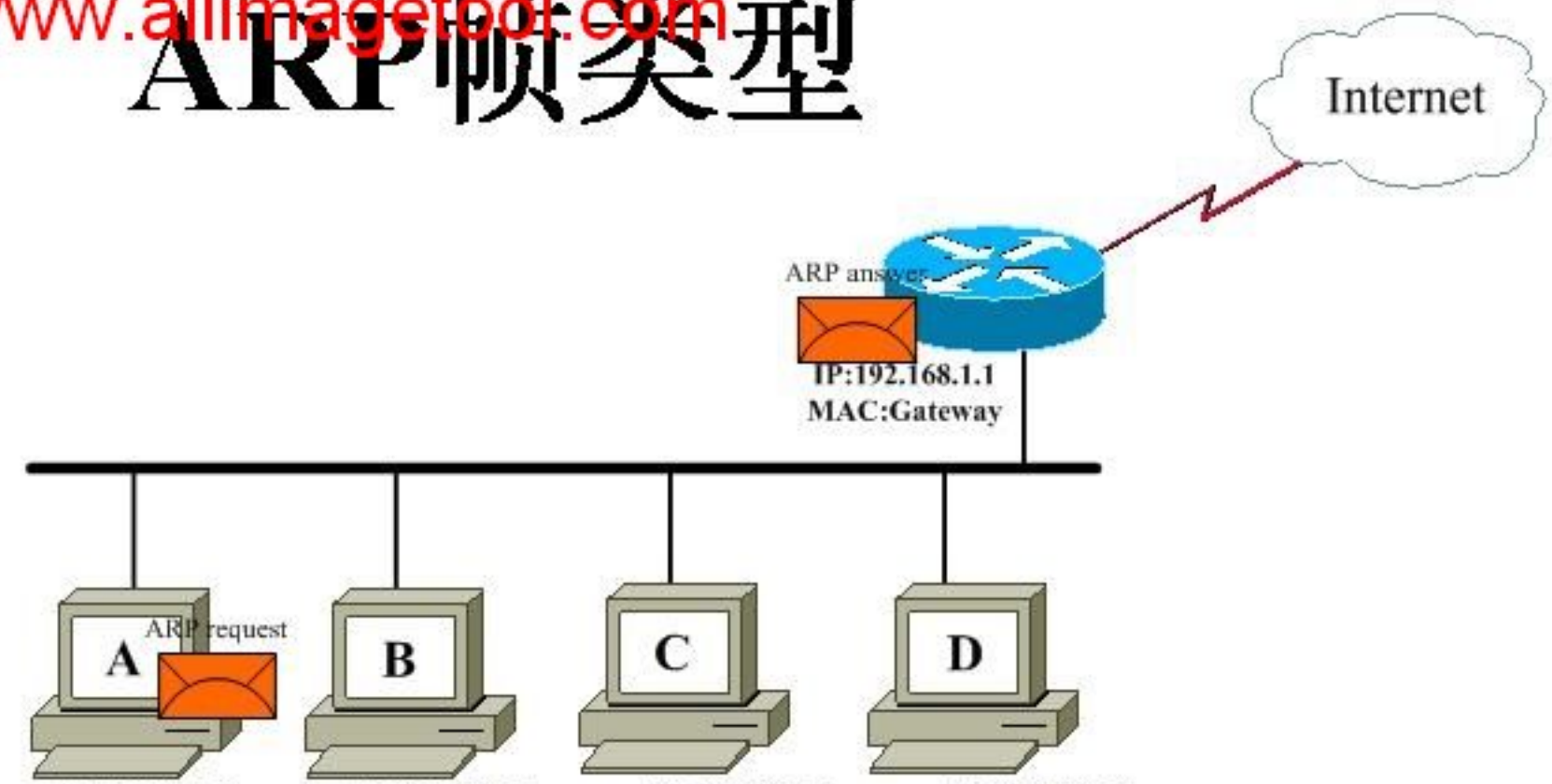
OP=1 ARP请求

OP=2 ARP应答



ARP帧类型

- ARP请求帧
- ARP应答帧



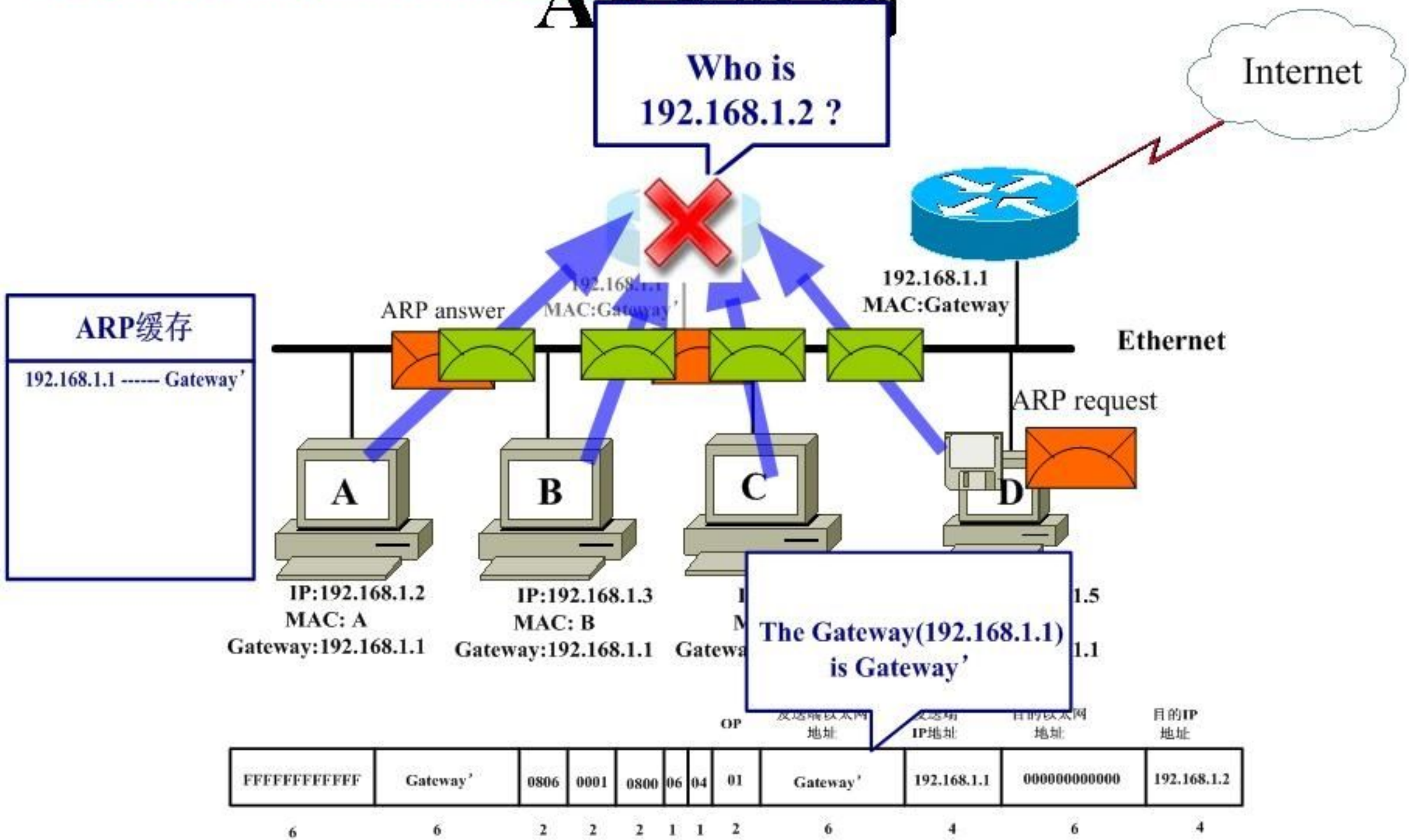
ARP请求帧

							OP	发送端以太网地址	发送端IP地址	目的以太网地址	目的IP地址
FFFFFFFFFFFF	MAC: A	0806	0001	0800	06	04	01	MAC: A	192.168.1.2	000000000000	192.168.1.1
6	6	2	2	2	1	1	2	6	4	6	4

ARP应答帧

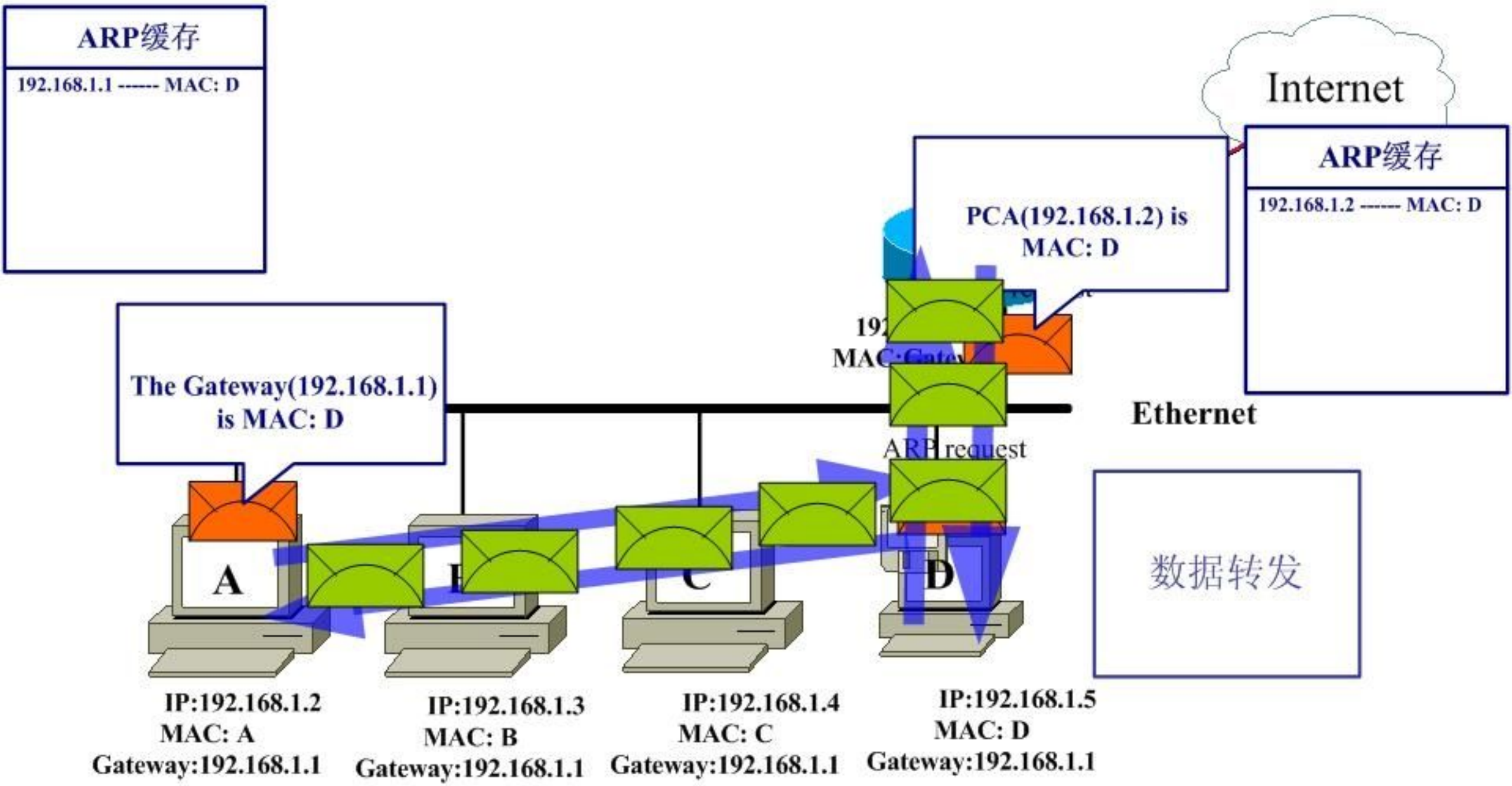
							OP	发送端以太网地址	发送端IP地址	目的以太网地址	目的IP地址
MAC:A	MAC:Gateway	0806	0001	0800	06	04	02	MAC:Gateway	192.168.1.1	MAC:A	192.168.1.2
6	6	2	2	2	1	1	2	6	4	6	4

ARP报文

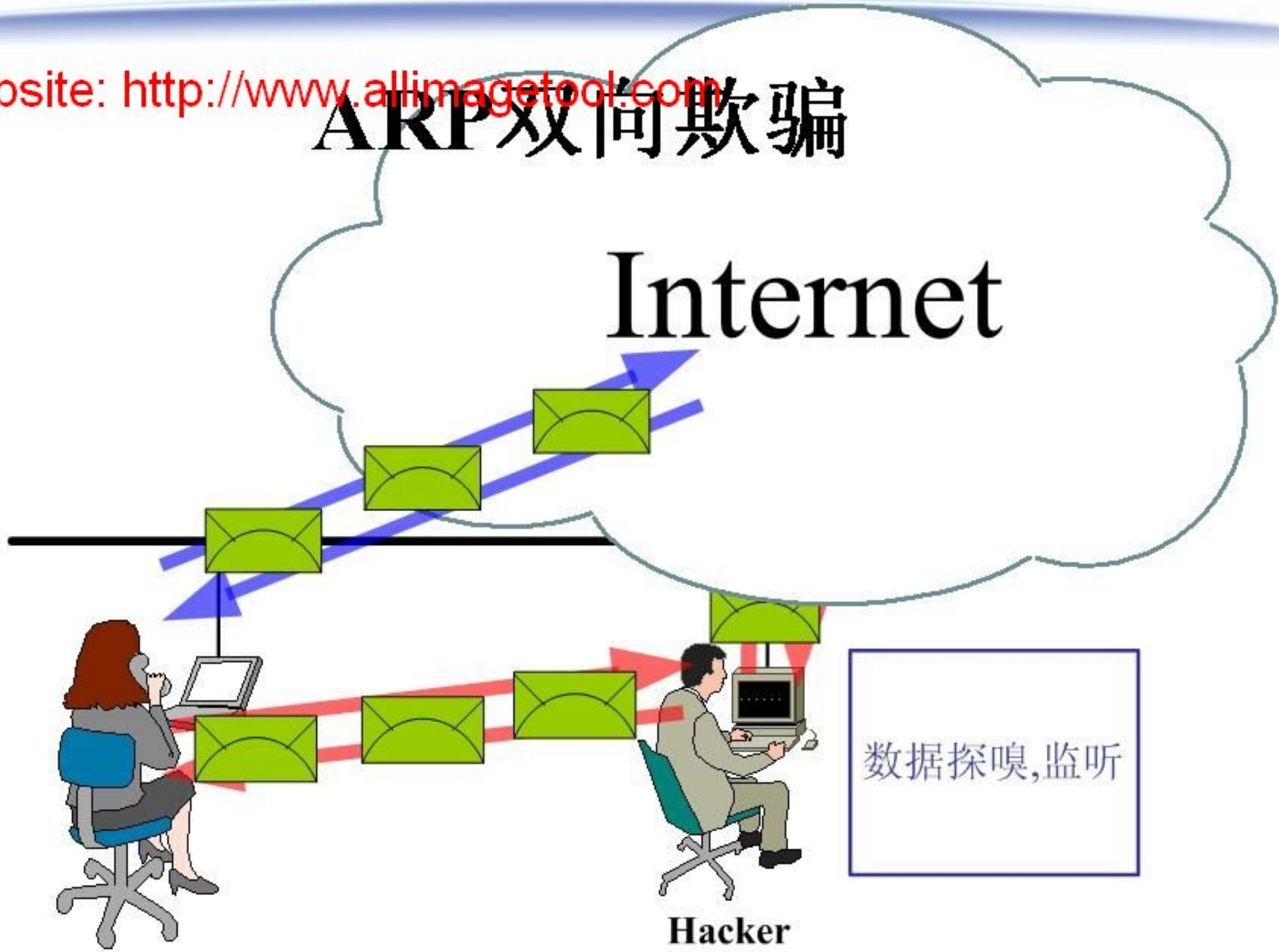


	OP	发送端以太网地址	发送端IP地址	目的以太网地址	目的IP地址
FFFFFFFFFFFF	0806 0001 0800 06 04 01	Gateway'	192.168.1.1	000000000000	192.168.1.2
6	2 2 2 1 1 2	6	4	6	4

ARP双向欺骗

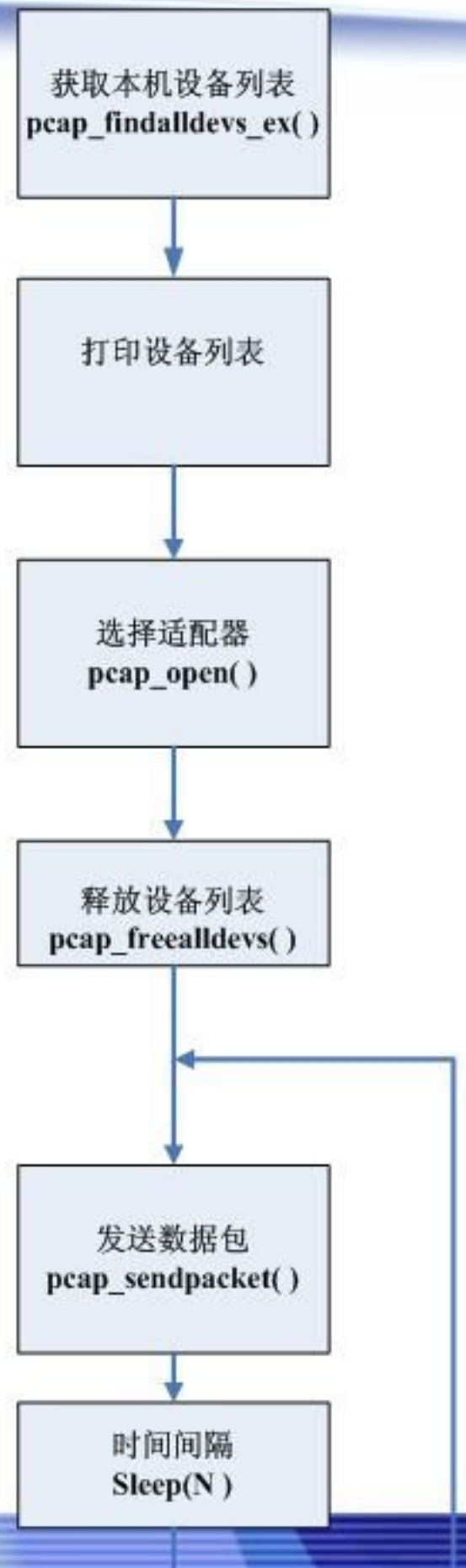


ARP双向欺骗



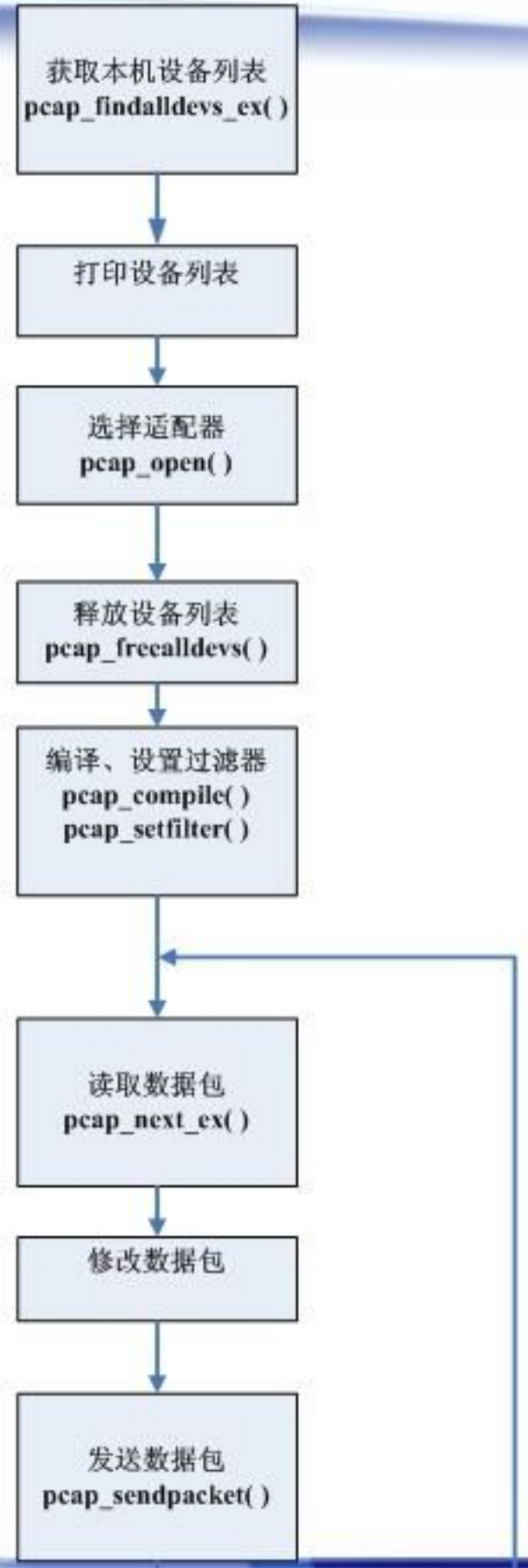
ARP欺骗实现（WinPcap）

- ARP欺骗进程
  - 获取设备列表
  - 打开选中的网卡
  - 发送ARP欺骗数据包

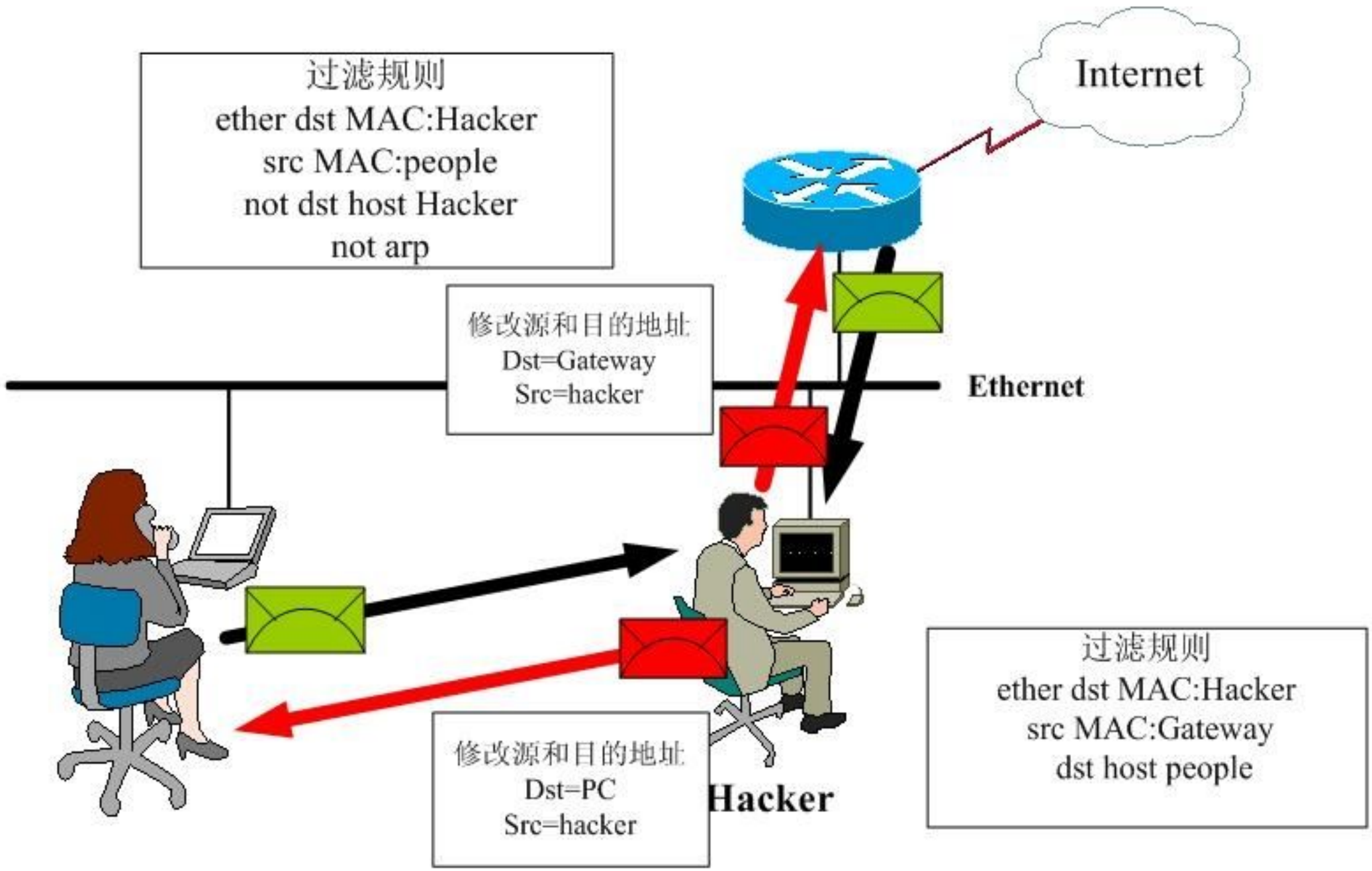


ARP欺骗实现（WinPcap）

- 转发进程
  - 获取设备列表
  - 打开选中的网卡
  - 设置过滤规则
  - 读取数据包
  - 修改源MAC和目的MAC
  - 转发数据包



修改数据包



防范ARP欺骗

- 客户端：
  - 静态绑定地址：
    - **arp –s 192.168.1.1 00-aa-bb-cc-dd-ee**
  - 安装个人防火墙

防范ARP欺骗

- 交换机：
  - DAI(Dynamic ARP inspection，动态ARP检测)是一种能检测ARP数据包的安全特性。通过DAI网络管理员能够拦截、记录和丢弃具有无效MAC地址/IP地址绑定的ARP数据包。

内容

1. ARP欺骗
2. IP欺骗
3. 路由欺骗攻击
4. 电子邮件欺骗
5. Web欺骗
6. 非技术类欺骗

IP欺骗

- 用虚假的IP地址来达到欺骗目的。
- IP欺骗的动机
  - 隐藏自己的IP地址，防止被追踪
  - 以IP为授权依据
  - 穿越防火墙
- IP欺骗的三种基本形式：
  - 基本地址变化：伪装成他人机器的IP地址。（单向IP欺骗）
  - 使用源路由选项截取数据包：源路由允许指定一条数据包必须经过的路径，使用源路由可以保证数据包经过攻击者的机器。（双向IP欺骗）
  - 利用UNIX机器上的信任关系：信任关系允许一台主机上的用户不需口令访问另外的主机。（TCP会话劫持）

单向IP欺骗

- 简单欺骗
  - 改变自己的IP地址
- 问题
  - 只能发送数据包
  - 无法收到回送的数据包
  - 防火墙可能阻挡
- 实现手段
  - 发送IP包，包头填写上虚假的源IP地址
  - 在Unix平台上，直接用socket就可以
  - 在Windows平台上，可以使用winpcap等工具

单向IP欺骗

可以输入任何源地址！

原始套接字构造IP欺骗攻击包

```
sock=socket(AF_INET,SOCK_RAW,255));     //创建原始套接字
bzero(&buffer,sizeof(struct iphdr)+sizeof(struct tcphdr));
//清空缓冲区
ipheader->version=4;                                  //IP版本4
ipheader->ihl=sizeof(struct iphdr)/4;                 //IP包头部长
ipheader->tot_len=htons(sizeof(struct iphdr)+sizeof(struct tcphdr));
//IP包总长
ipheader->id=htons(0xF1C);                            //IP包的id号
ipheader->ttl=255;                                    //IP包中的TTL域
ipheader->protocol=IPPROTO_TCP;                       //IP包中的协议类型域
ipheader->saddr=inet_addr("192.168.1.1");  //IP包中的源IP地址域
```

特点

- 根据**TCP/IP**协议，对这类数据包的所有应答都会回到被假冒的主机上，而不是攻击者的机器，因此这类欺骗又叫盲目飞行攻击，或者叫做单向攻击。
- 这种攻击的优点是难于找到攻击者的根源。而且对于某些拒绝服务攻击，需要的就是达到拒绝服务效果，而不需要从目标获得其他信息。

盲目飞行

攻击者

IP：192.168.1.5

假冒IP：172.16.1.1

发送信息

应答信息

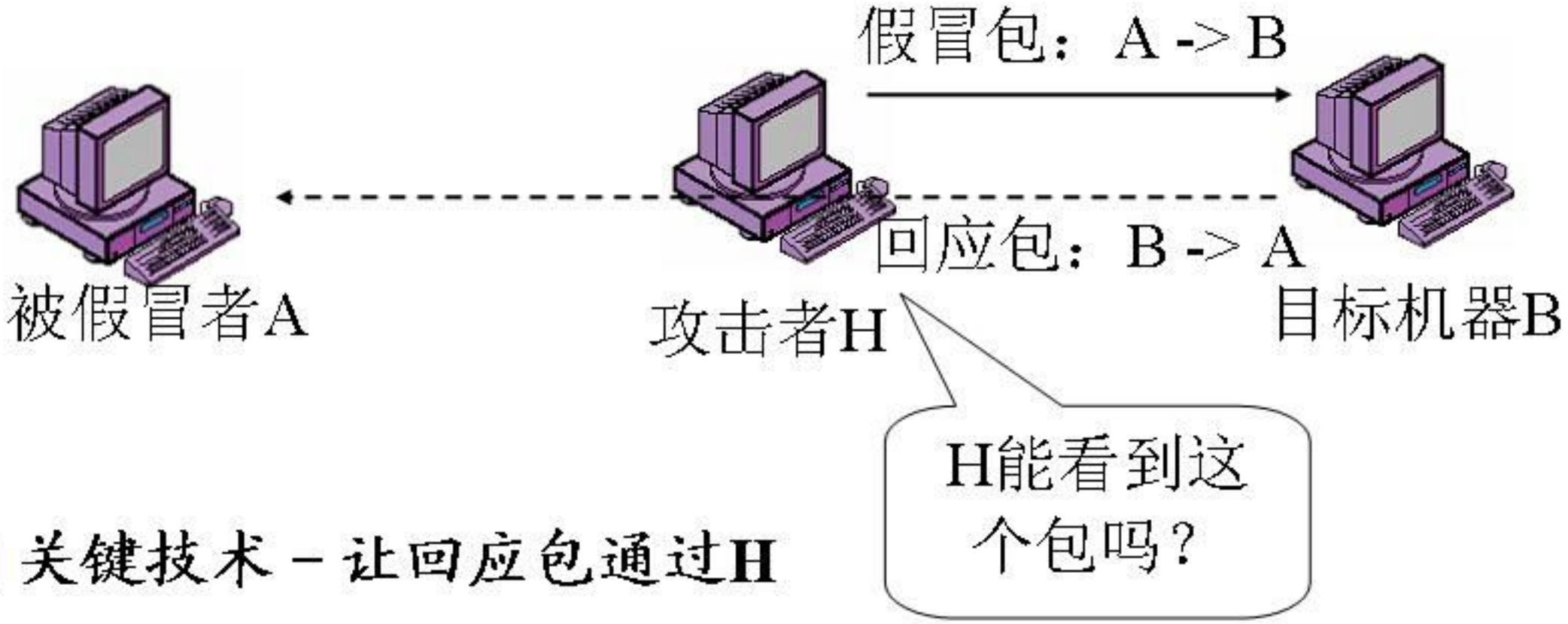
被假冒者

IP：172.168.1.1

攻击目标

- 在单向IP欺骗攻击中，目标的应答回到被假冒的地址上，攻击者不能得到应答。攻击者如果想了解会话情况，必须保证自己插入到应答经过的网络通路上。

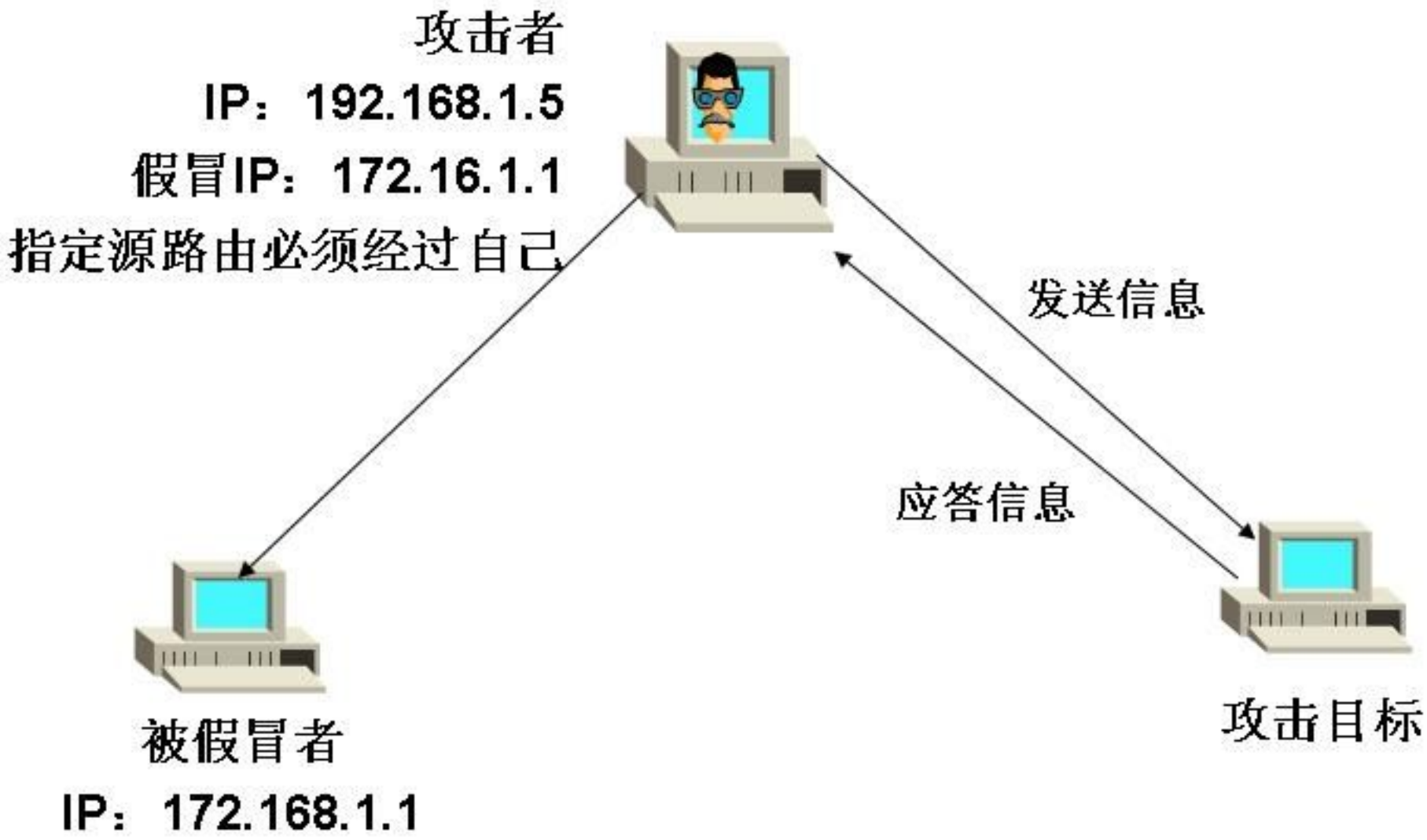
双向IP欺骗



- 关键技术－让回应包通过H
  - H和A在同一个子网内部
  - 使用源路由选项

设置源路由

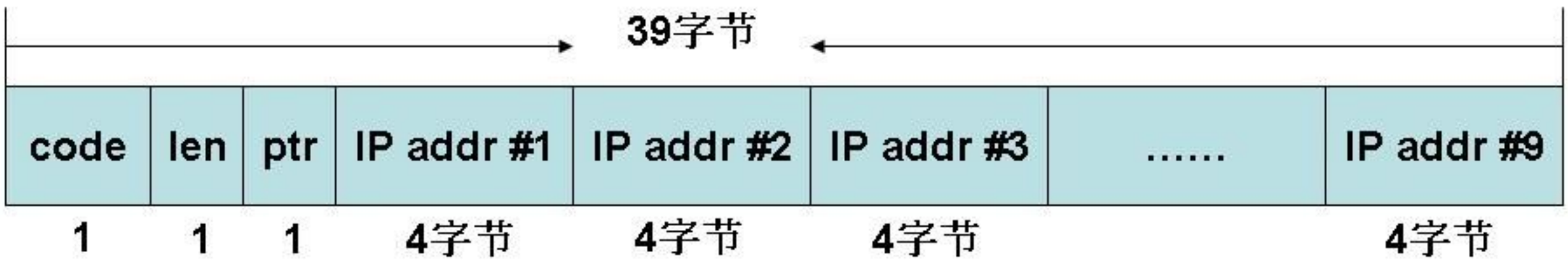
源路由允许指定一条数据包必须经过的路径，使用源路由可以保证数据包经过攻击者的机器。



IP首部的源路由选项

- 宽松的源路由选择（Loose Source Route-LSR）：发送端指明了一连串路由器接口的IP地址序列，报文必须沿着IP地址序列传送，但是数据包在清单上指明的任意两个地址之间可以通过其他路由器。换句话说，不用考虑数据包经过的确切地址，只要它经过这些指定的地址就可以。
- 严格的源路由选择（Strict Source Routing-SRS）：发送端指明一连串路由器接口的IP地址序列，报文必要严格按照路由转发，如果一个路由器发现源路由所指定的下一个路由器不在其直接连接的网络上，那么将会发生错误，数据包被丢弃，并返回一个ICMP差错报文。换句话说，必须考虑数据包经过的确切路径，而且如果由于某种原因没有经过这条路径，这个数据包就不能被送达。

IP首部源路由选项的通用格式

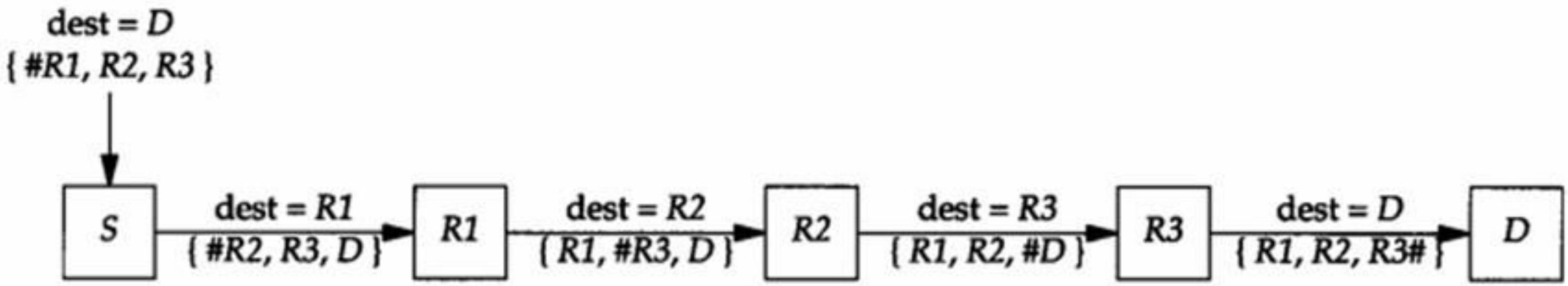


- 对于宽松的源路由选择来说，code字段的值是0x83；而对于严格的源路由选择，其值为0x89。len是选项总字节长度，最大为39。ptr为指针字段，指向存放下一个IP地址的位置。它的最小值为4，指向存放第一个IP地址的位置。随着每个IP地址存入序列，ptr的值逐步增大，分别为8、12、16。当记录下9个IP地址后，ptr的值为40，表示序列已满。

- 在TCP/IP协议规范中，源路由选项的实际称呼为“源站及记录路由”（Source and Record Route，对于宽松的源路由和严格的源路由，分别用LSRR和SSRR表示），这是因为在数据包沿路由发送过程中，对IP地址序列进行了更新。
- 主机和路由器对选项的处理过程如下：

1. 发送主机从应用程序接收源路由序列，将第1个表项去掉，将其设置为数据包的IP地址，剩余的项前移1个项，并将原来的目的地址（数据包真正的目标）作为序列清单的最后一项。指针仍然指向序列清单的第1项（即ptr的值为4）。
2. 处理数据包的每个中间路由器检查其是否为数据包的目的地址。如果不是，则正常转发数据包（在这种情况下，必须指明是宽松源路由选项，否则就不能接收到该数据包）。如果该路由器是目标地址，且指针不大于路径的长度，那么：
   ① 由ptr所指定的序列清单中的下一个地址设为数据包的目的地址。
   ② 由外出接口（outgoing interface）相对应的IP地址取代刚才使用的源地址。
   ③ ptr指针加4。
3. 如果指针ptr大于路径的长度，此次发送结束。

假设主机S上的发送应用程序发送一份数据报给D，指定源路由为R1，R2和R3。



在上图中，#表示指针字段，其值分别是4、8、12和16。长度字段恒为15（三个IP地址加上三个字节首部）。可以看出，每一跳IP数据报中的目的地址都发生改变。

数据包的应答

- 当一个应用程序接收到由信源指定路由的数据包，在发送应答时，应该读出接收到的路由值，并提供反向路由。所以，源路由选项可以保证欺骗者得到目标的应答。
- 攻击者使用假冒的地址向目的地发送数据包，如果指定了源路由选项，并把他的**IP**地址填入到地址清单中。那么，当目标端回应时，数据包返回到假冒的**IP**地址处，但它会经过攻击者的机器。攻击者没有盲目飞行，因为他能看到对话双方。

TCP会话劫持

- 在Unix系统中，用户为方便同时使用多个主机，经常在主机之间建立信任(Trust)关系。
- 假如用户在主机A和B上各有一个独立账号x。在使用过程中，在使用主机A时需要输入在A上的相应账号x和相应口令，在使用主机B时必须输入B上的帐号x和相应口令，两个账号在主机A和B上互不相关。
- 可以在主机A和主机B中建立起两个账号的相互信任关系。建立信任关系后，在任何一个主机上都可使用以r开头的远程调用命令（如rlogin、rcall、rsh 等），远程登录对方主机而不需要口令验证。

远程登录（rlogin）Linux系统

- 远程用户启动rlogin访问本地Linux主机，本地主机上的服务器进程rlogind负责对客户进行安全性检查，检查过程如下：
  - rlogind在本地/etc/passwd文件中寻找远程用户名，如果没有远程用户名则拒绝访问。
  - 如果在/etc/passwd中存在远程用户名，rlogind在/etc/hosts.equiv寻找远程主机名，找到远程主机名则允许访问。
  - 如果/etc/hosts.equiv中没有远程主机名，rlogind在$HOME/.rhosts寻找远程主机名，如果找到主机名且该主机名后无任何用户名则允许访问；若找到主机名且该项后有用户名，并且用户名中有x，则允许访问。注意，这里的变量$HOME表示与远程用户同名的本机用户的主目录。
  - 若通过了/etc/passwd的检查，但没有通过/etc/hosts.equiv或者$HOME/.rhosts的检查，远程用户需要输入相应的口令后才可以登录本机，但无法使用rcp、rsh等命令。
  - 文件/etc/hosts.equiv与文件$HOME/.rhosts的格式基本相同，格式如下：

```
hostname                  //表示允许主机hostname上的所有用户
hostname username         //表示允许主机hostname上的用户 username
+                         //允许任意主机
```

TCP会话劫持

- 假设B上的客户运行rlogin与A上的rlogind通信:

1. B发送带有SYN标志的数据段通知A需要建立TCP连接。并将TCP报头中的sequence number设置成自己本次连接的初始值ISN。
2. A回传给B一个带有SYS+ACK标志的数据段，告之自己的ISN，并确认B发送来的第一个数据段，将acknowledge number设置成B的ISN+1。
3. B确认收到的A的数据段，将acknowledge number设置成A的ISN+1。

B --- SYN ---> A
B <---- SYN+ACK ---- A
B --- ACK ---> A

(1)使被信任主机丧失工作能力

TCP SYN-Flood :

t1: Z(X) ---- SYN ----> B

Z(X) ---- SYN ----> B

Z(X) ---- SYN ----> B

Z(X) ---- SYN ----> B

Z(X) ---- SYN ----> B

t2: X <---- SYN+ACK ---- B

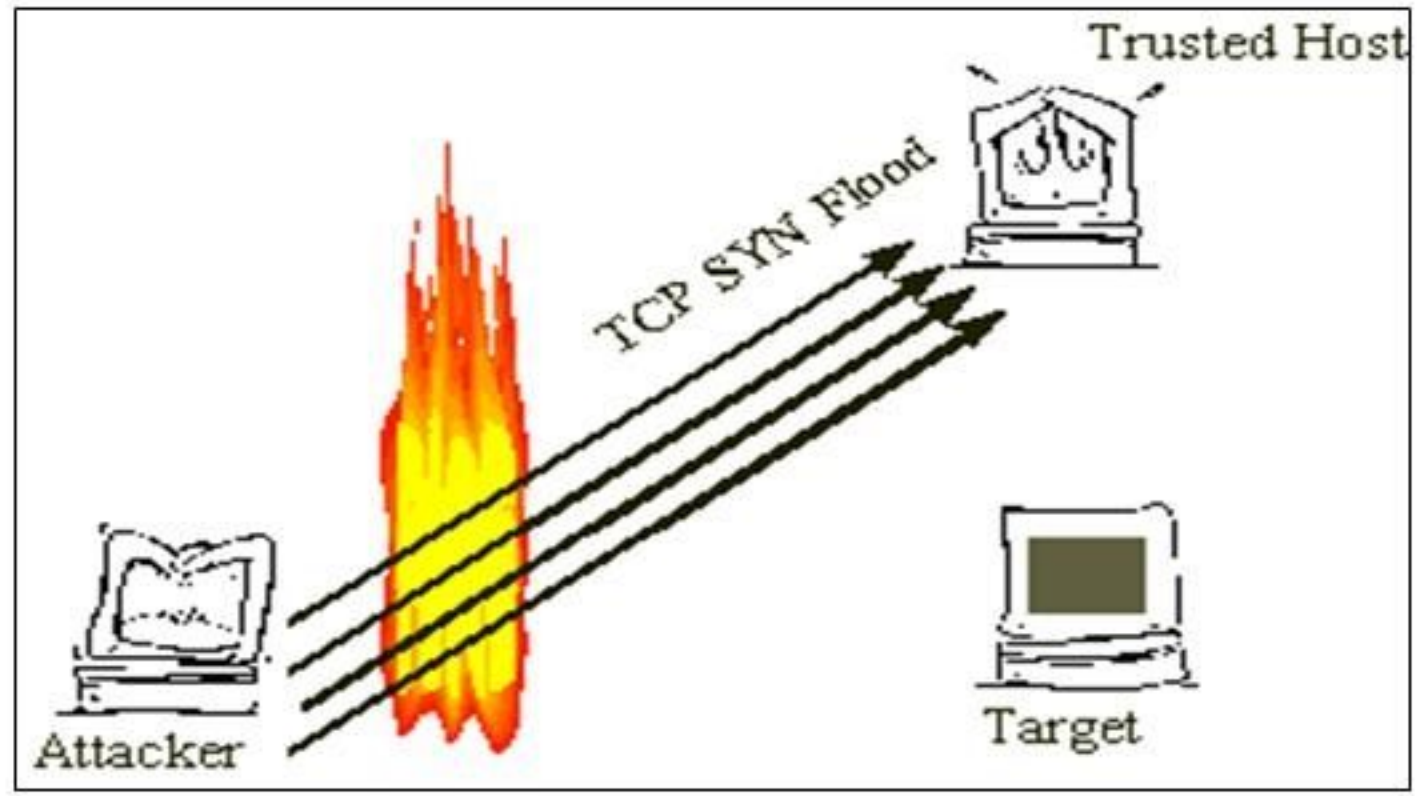
X <---- SYN+ACK ---- B

X <---- SYN+ACK ---- B

X <---- SYN+ACK ---- B

X <---- SYN+ACK ---- B

X <---- SYN+ACK ---- B



(2)序列号猜测

- Z必须确定A当前的ISN。
  - 首先连向25端口(SMTP是没有安全校验机制的)，记录A的ISN，以及Z到A的大致的RTT (round trip time)。这个步骤要重复多次以便求出RTT的平均值。现在Z知道了A的ISN基值和增加规律(比如每秒增加128000，每次连接增加64000)，也知道了从Z到A需要RTT/2 的时间。必须立即进入攻击，否则在这之间有其他主机与A连接， ISN将比预料的多出64000。

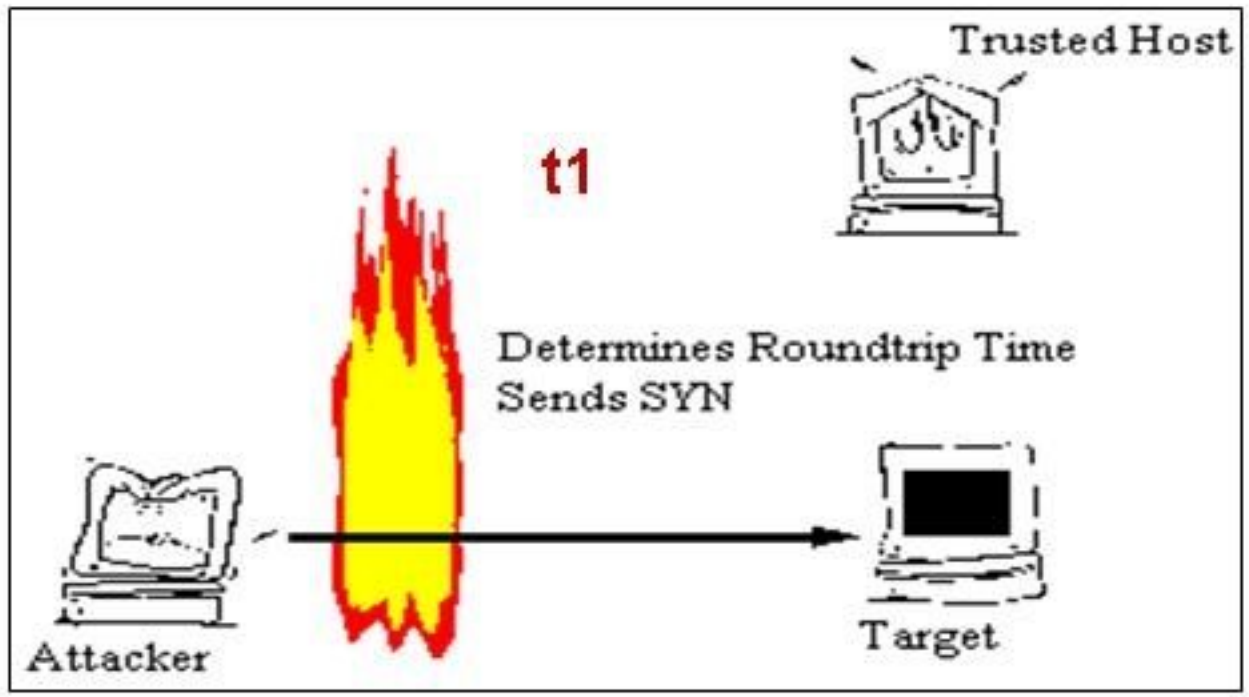
(3)实施欺骗

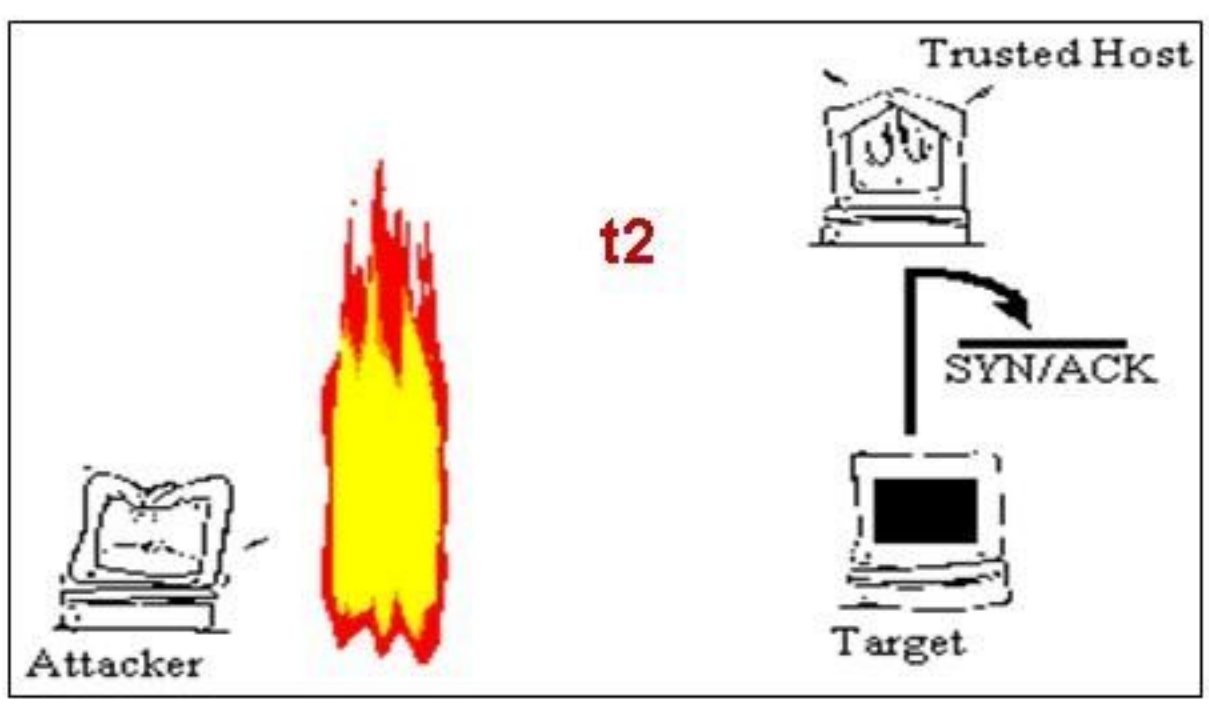
- Z伪装成A信任的主机B攻击目标A的过程如下：

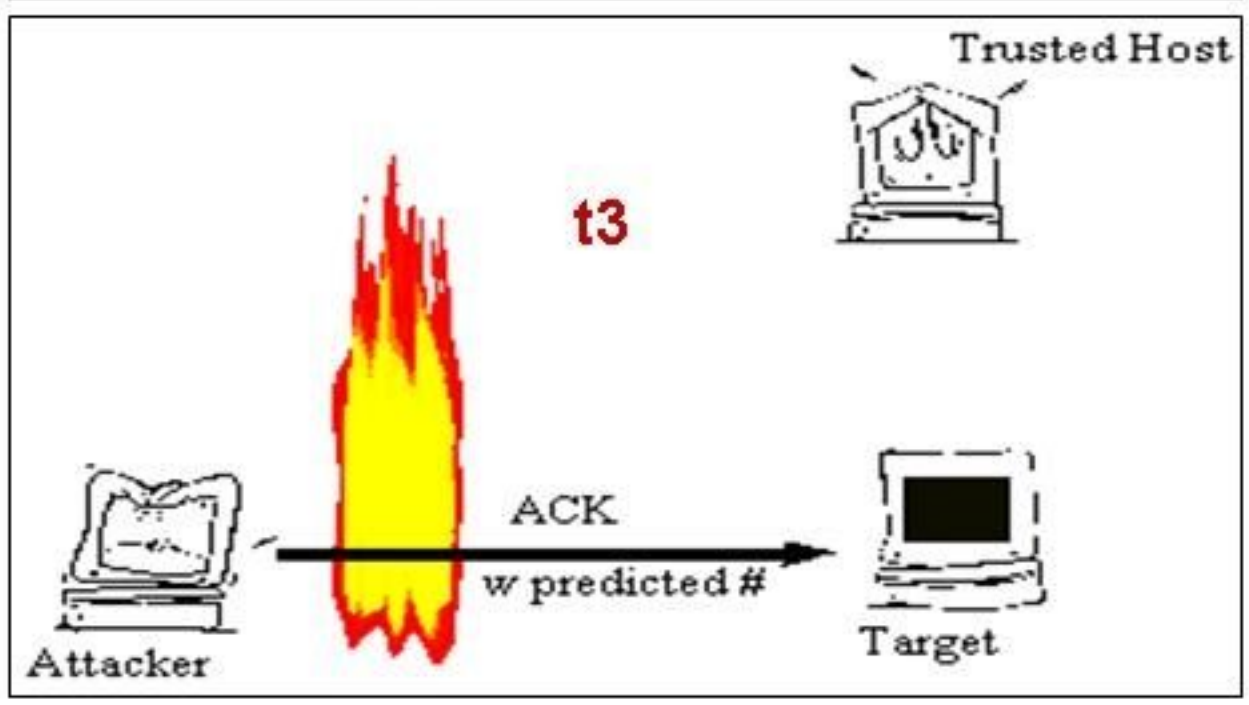
  t1: Z(B) - - - SYN - - > A

  t2: B < - - SYN/ACK - - A

  t3: Z(B) - - - ACK - - > A



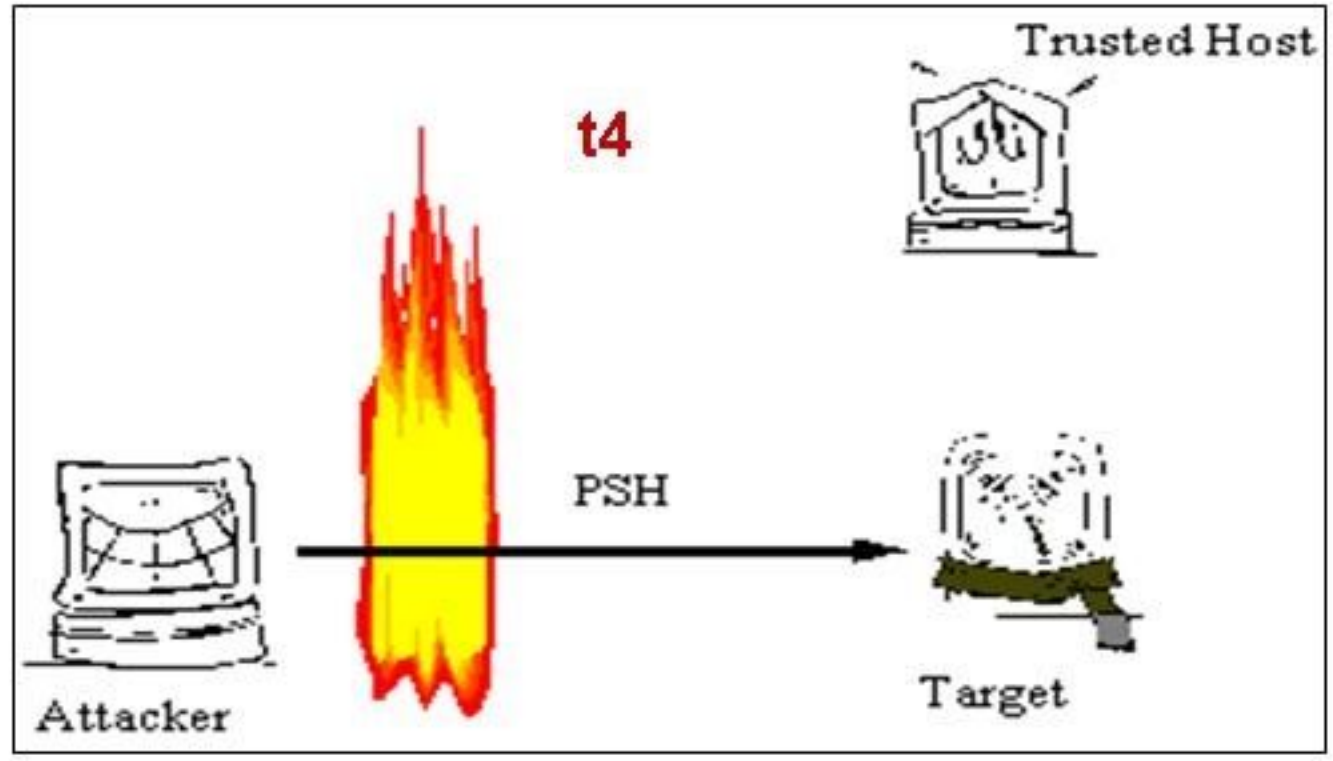




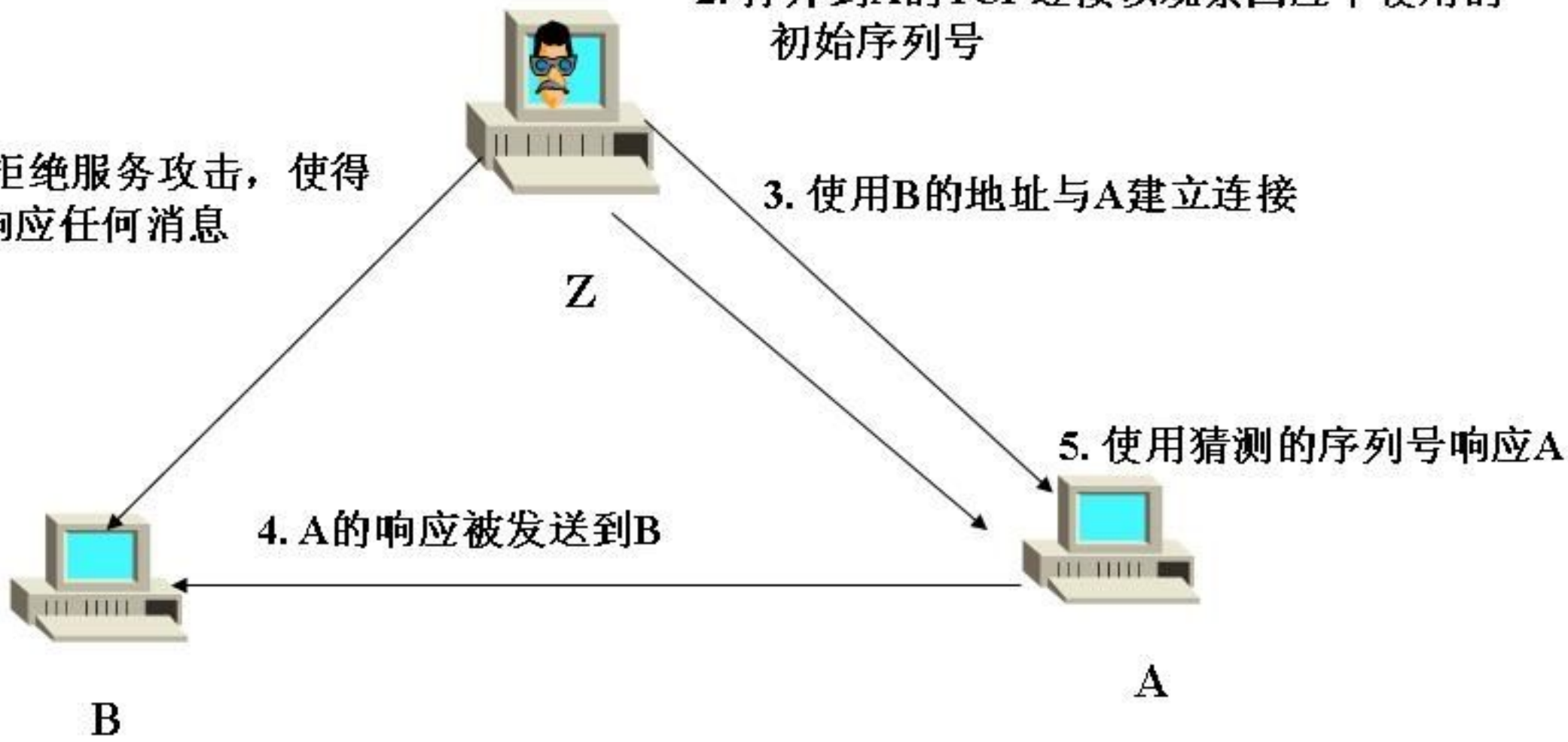
(4)建立后门

- 如果序列号猜测准确，连接建立，数据传送开始。问题在于即使连接建立，A仍然会向B发送数据，而不是Z，Z仍然无法看到A发往B的数据段，Z必须按照rlogin协议标准假冒B向A发送类似“cat＋＋>> ~/.rhosts”这样的命令，在系统中放置一个后门，以使下一次侵入。

t4: Z(B) ---PSH---> A



TCP会话劫持



难点：初始序列号猜测问题

- 目标主机的初始序列号（ISN）
- RTT（round-trip time）值
- 序列号的增加规律（128000/秒或者其它）

关于会话劫持的参考

- 三篇文章
  - **Simple Active Attack Against TCP,**

    http://www.insecure.org/stf/iphijack.txt
  - **A short overview of IP spoofing: PART I,**

    http://staff.washington.edu/dittrich/papers/IP-spoof-1.txt
  - **A short overview of IP spoofing: PART II ,**

    http://staff.washington.edu/dittrich/papers/IP-spoof-2.txt

IP欺骗+TCP会话劫持的防范

- 使用路由器或防火墙进行数据包过滤
  - 不允许源地址不是本网络的数据包流出
- 抛弃基于地址的信任策略
- 使用随机化的初始序列号

内容

1. ARP欺骗
2. IP欺骗
3. 路由欺骗攻击
4. 电子邮件欺骗
5. Web欺骗
6. 非技术类欺骗

攻击原理及攻击过程

- TCP/IP上有两种基本的路由方式：一种是使用预编程的静态路由，这种路由适用于网络拓扑相对稳定的网络；另一种是使用通过任何一种动态路由协议来动态计算路由。
- 静态路由或预编程路由是最简单的路由形式。它是由静态路由编程的路由器将报文转发至预定的端口。

- 静态路由只适用于小型网络，且到达任一目的地只有一条路径，因此它不消耗任何带宽来发现路由或与其它路由器进行通信。但是随着网络的增大，到达目的地冗余路径的出现，使用静态路由的工作量会变大，因此在广域网中必须采用动态路由。
- 在每一台路由器或承担部分路由功能的硬件设备中，都维护着一个动态路由表。路由表中主要的结构字段如下所示：

动态路由表

Destination	Gateway	Flags	Ref	Use	Interface

- 图中Flags域中可能包含的符号及其含义如下：
  1. U表示该路由可用；
  2. G表示该路由是一个网关(路由器)。如果没有，则表示与目的地直接相连；
  3. H该路由是一个主机，即目的地是一个完整的主机地址，没有此标志表示该路由是到一个网络，而且目的地址是一个网络地址；
  4. D该路由是由重定向报文创建的；
  5. M该路由已被重定向报文修改。
- 从上面的描述可以看出：重定向报文可以创建路由，也可以修改路由。ICMP重定向报文格式如下表所示。

ICMP重定向报文格式

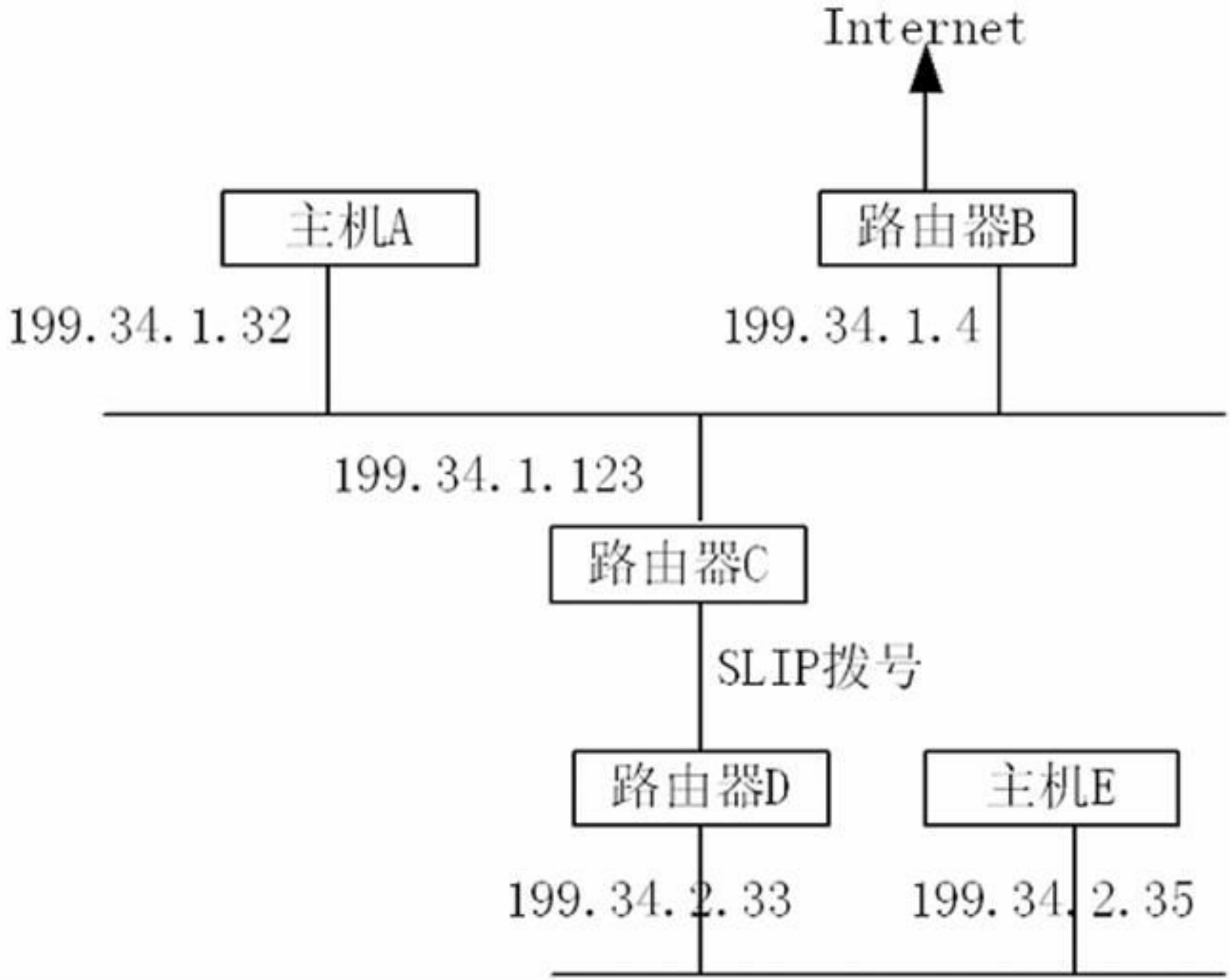
0 15	16 31
（5）类型 （0~3）代码	检验和
应该使用的路由器 IP 地址	
IP 首部（包括选项）+原始 IP 数据报中的数据前 8 字节	

四种不同的重定向报文的代码值

代码	描述
0	网络重定向
1	主机重定向
2	服务类型重定向
3	服务类型和主机重定向

- **ICMP重定向报文的接收者必须查看三个IP地址：**
  - **(1)导致重定向的IP地址（即ICMP重定向报文的数据中位于IP首部中的IP地址）；**
  - **(2)发送重定向报文的路由器的IP地址（包含重定向信息的IP数据报中的源地址）；**
  - **(3)应该采用的路由器IP地址（在ICMP报文中的4~7字节）。**

ICMP重定向报文创建一个路由的过程



- 路由器B接入Internet网，而路由器C与D是通过一个拔号的SLIP链路将上下两子网相连。在主机A上对主机E进行Ping 操作。在此操作之前，其路由表中的默认路由为199.34.1.4，且没有通往主机E的路由。发出Ping 操作命令后，报文先到达默认路由199.34.1.4，但由于路由器B不与199.34.2.0子网相连，因此它发送一个ICMP重定向报文给主机A，使其指向路由器C，此后主机A的路由表中增加了一条新的记录如下：

Destination	Gateway	Flags	Ref	Use	Interface
199.34.2.35	199.34.1.123	UGHD	0	2	

- 因此如果攻击者伪装成一个路由器节点，向攻击目标发送一个ICMP重定向报文，使目标主机的路由表中指向某些网段的路由变为指向攻击者的路由，这样，攻击者就可能截获目标主机向外发送的信息。这种攻击方法即称为路由重定向攻击。
- 如图中，如果主机A的默认路由是指向199.34.1.4，而攻击者仅能从路由器C中捕获数据。这样攻击者可以伪装成路由器B向主机A发送一个路由重定向数据包，使得主机A的路由表中的默认路由变为指向路由C（199.34.1.123）这样攻击者可以从路由器C中捕获目标系统A向外发送的一些信息，以此获得重要信息。

防御措施

- 出于系统安全性的考虑，在路由器中有八条配置命令，可以分别用来禁止或使能四种类型的ICMP报文的发送。
  - (1) ICMP echo enable，ICMP echo disable，利用上面两条命令可以使能或禁止ICMP的echo reply报文的发送。一旦禁止该类型的报文，从其他机器利用ping命令搜索该路由器时，路由器将不作出反应。
  - (2) ICMP mask enable，ICMP mask disable，利用上面两条命令可以使能或禁止ICMP的Mask Reply报文的发送。当在路由器上禁止该类型的报文时，路由器对于来自其他机器的mask request请求不作反应。

- (3) ICMP unreach enable，ICMP unreach disable，利用上面两条命令可以使能或禁Destination Unreachable报文的发送。当在路由器上禁止该类型的报文时，路由器对于其无法转发的ip报文将不再向其源地址发送Destination Unreachable的报文。利用show ICMP命令可以观察当前ICMP以上各项的设置。
- (4) ICMP redirect enable，ICMP redirect disable，利用上面两条命令可以使能或禁止ICMP的重定向(redirect)报文的发送。当在路由器上禁止该类型的报文时，路由器对于可能的路由错误不作反应。

配置主机—预防路由欺骗

- 避免ICMP重定向欺骗的最简单方法是将主机配置成不处理ICMP重定向消息，在Linux下可以利用firewall明确指定屏蔽ICMP重定向包。
- 另一种方法是验证ICMP的重定向消息。例如检查ICMP重定向消息是否来自当前正在使用的路由器。这要检查重定向消息发送者的IP地址并校验该IP地址与ARP高速缓存中保留的硬件地址是否匹配。

内容

1. ARP欺骗
2. IP欺骗
3. 路由欺骗攻击
4. 电子邮件欺骗
5. Web欺骗
6. 非技术类欺骗

电子邮件欺骗

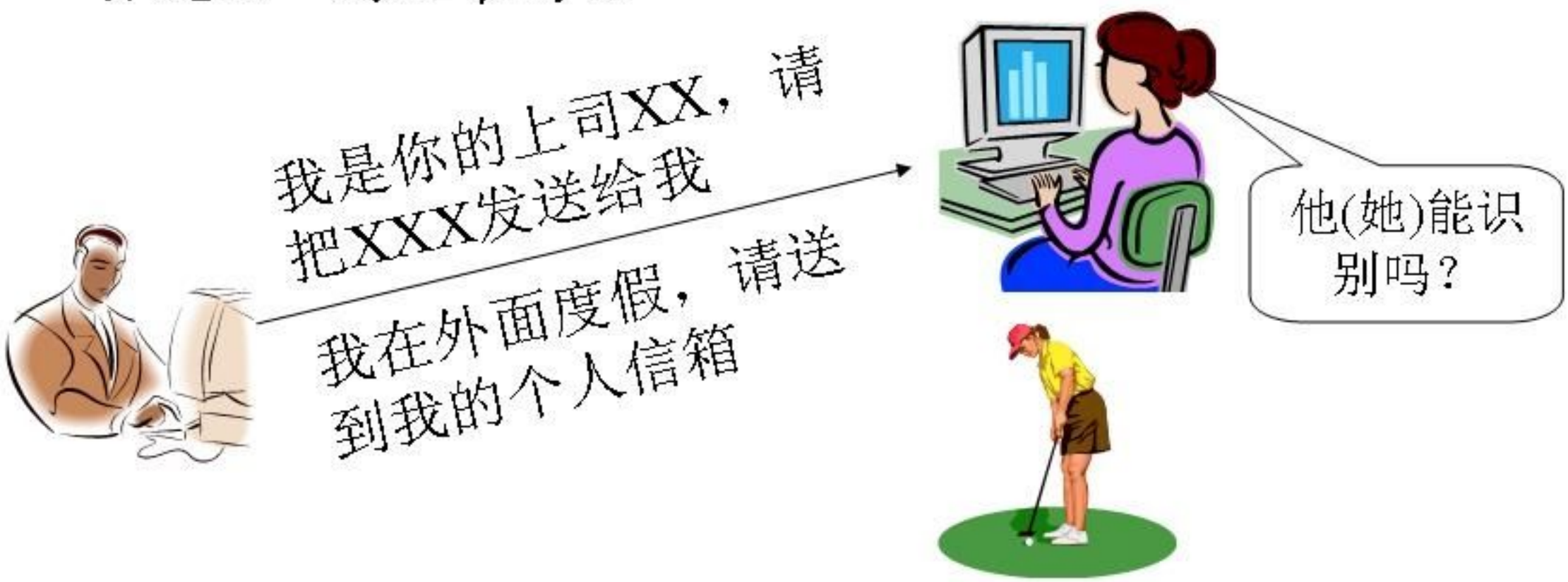
- 电子信件的发送方地址、发信内容的欺骗。
- 有三种目的：
  - 第一，隐藏自己的身份。
  - 第二，假冒他人的电子邮件。
  - 第三，电子邮件欺骗能被看作是社会工程的一种表现形式。

电子邮件欺骗的基本方法

- 相似的电子邮件地址
  - 假冒一个相似的邮件地址发送邮件，因为邮件地址似乎是正确的，所以收信人很可能会回复它，这样攻击者就会得到想要的信息。**liuhaiyan—1iuhaiyan**
- 修改邮件客户软件
  - 当发出电子邮件时，没有对发件人地址进行验证或者确认，因此他能够指定他希望出现在发件人中的任意地址。当用户回信时，答复回到真实的地址，而不是回到被盗用了地址的人那里。
- 远程登录到端口**25**，邮件转发
  - 邮件服务器使用**25**号端口在互联网上发送邮件。攻击者登录**25**号端口，直接发送邮件。

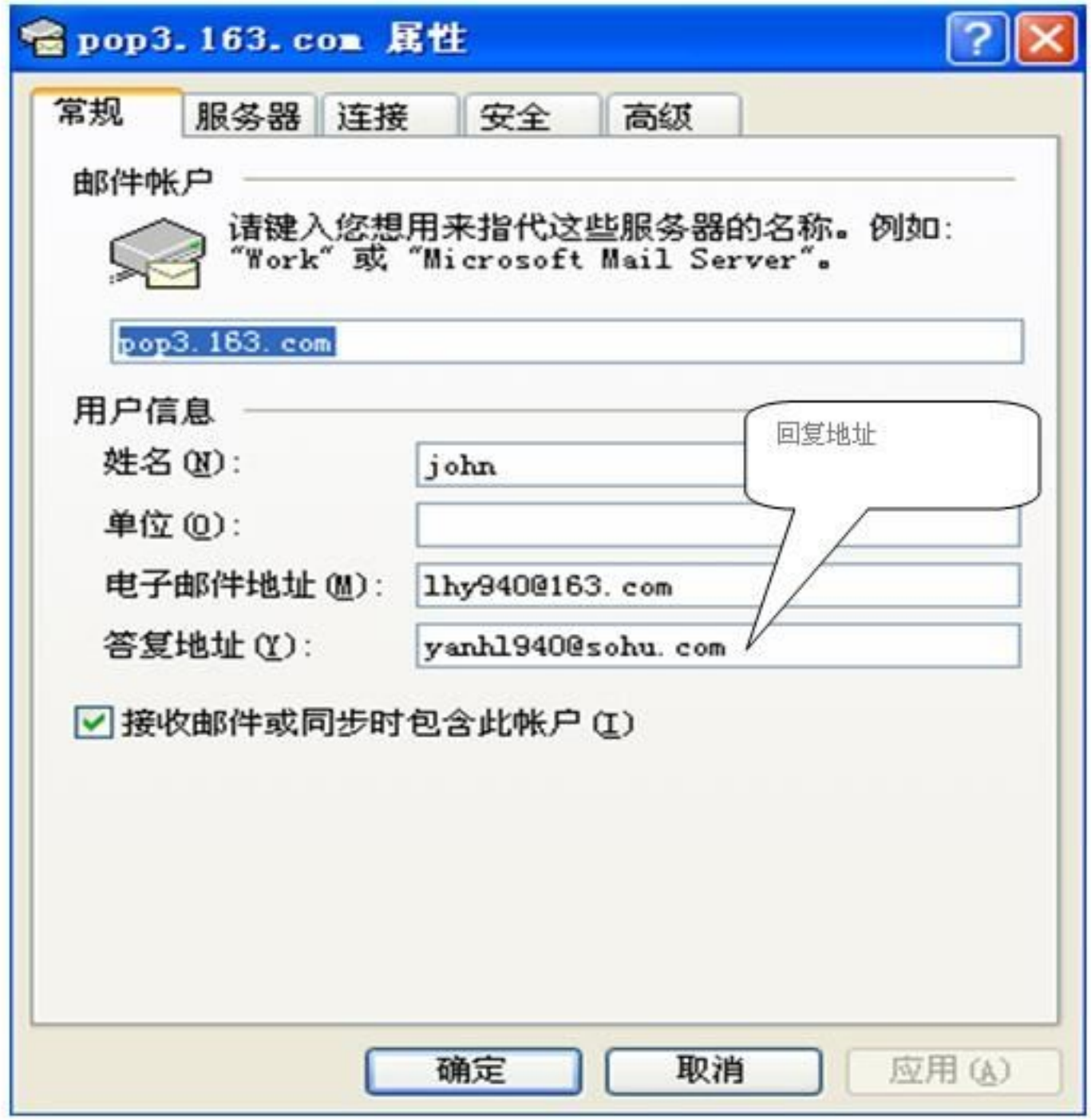
电子邮件欺骗(1)

- 使用类似的邮件地址
  - 发信人使用被假冒者的名字注册一个账号，然后给目标发送一封正常的信



电子邮件欺骗(2)

- 修改邮件客户端软件的账号设置



日　期:	2007-03-09 16:01:36
发件人:	john <lhy940@163.com> 拒收
收件人:	lhy940@163.com
主　题:	only a test [新窗口打开] [举报垃圾邮件]

aaa

Website: http://www.allimagetool.com

电子邮件欺骗(3)

- 直接连到SMTP服务器上发信
  - telnet连到SMTP服务器的25端口，然后发送命令，常用的命令为:
    - Helo、Mail from、Rcpt to、Data、Quit

telnet smtp.163.com 25　　//登陆 **smtp.163.com** 端口号为 **25**

Trying 202.108.44.205...

Connected to smtp.163.com (202.108.44.205).

Escape character is '^]'.

220 163.com Coremail SMTP(Anti Spam) System

HELO lhy　　//与服务器打招呼，并告知客户端的机器

250 OK

AUTH LOGIN　　//使用身份认证登陆指令

334 dXNlcm5hbWU6

cmVkc29zMw==　　//输入已经**base64_encode()**过的用户名

334 UGFzc3dvcmQ6

**********　　//输入已经**base64_encode()**过的密码

235 Authentication successful //通过认证

MAIL FROM:<redsos3@163.com> //告诉服务器发信人的地址

250 Mail OK

RCPT TO:<yourframe@21cn.com> //告诉服务器收信人的地址

250 Mail OK

DATA //开始传输信件的内容，且最后要以只含有“.”的特殊行结束

354 End data with <CR><LF>.<CR><LF>

To:yourframe@21cn.com

From:redsos3@163.com

Subject:test mail

From:redsos3@163.com

test body

. //结束信件内容

250 Mail OK queued as smtp14,F0CPBFsuzUOvoDwE.41582S2

QUIT //断开连接

221 Bye

Connection closed by foreign host.

电子邮件欺骗的防范

- 对于类似邮件地址的解决
  - 使用数字签名
- 保护用户免受修改邮件客户的攻击
  - 查看完整的电子邮件头部信息
    - 多数邮件系统允许用户查看邮件从源地址到目的地址经过的所有主机
- 防范直连SMTP服务器
  - 邮件服务器的验证
    - Smtp服务器验证发送者的身份，以及发送的邮件地址是否与邮件服务器属于相同的域
    - 验证接收方的域名与邮件服务器的域名是否相同
    - 有的也验证发送者的域名是否有效，通过反向DNS解析
  - 攻击者可以运行自己的smtp邮件服务器
  - 不能防止一个内部用户冒充另一个内部用户发送邮件

内容

1. ARP欺骗
2. IP欺骗
3. 路由欺骗攻击
4. 电子邮件欺骗
5. **Web欺骗**
6. 非技术类欺骗

Web欺骗

- 随着商务、政务领域信息化的发展，网站成为商务和政务活动的交流中心，也成为抱有各种目的攻击者的主要攻击目标，其中web欺骗是网站面临的一种主要攻击。
  - 基本的网站欺骗
  - 中间人攻击
  - URL重写

基本的网站欺骗

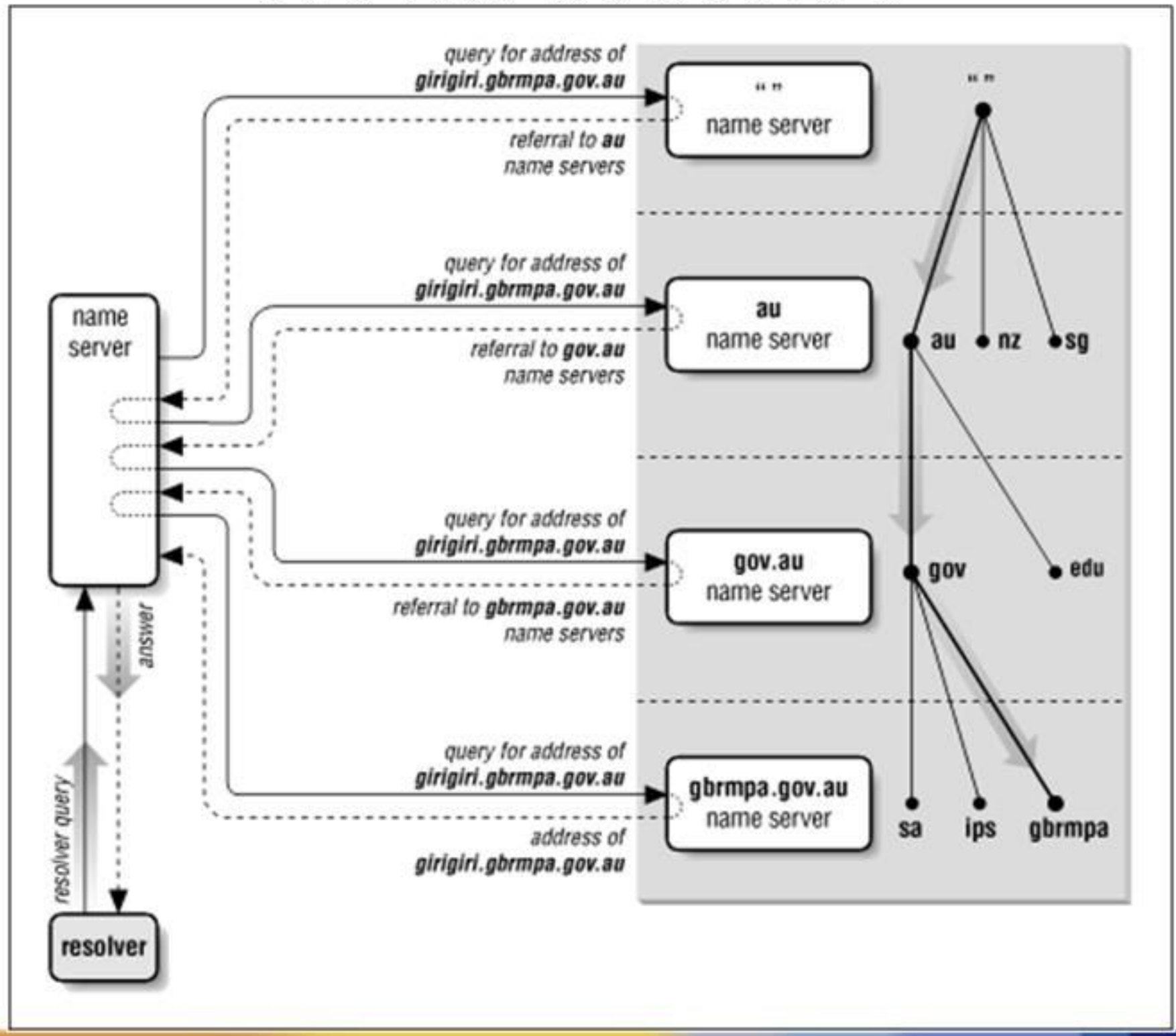
- 目前在互联网上注册一个域名没有严格的审查，攻击者可以抢先或特别设计注册一个非常类似的有欺骗性的站点。
- 当用户浏览了这个假冒地址,并与站点作了一些信息交流,如填写了一些表单之后，站点会给出一些响应式的提示和回答，同时记录下用户的信息。
- 典型的例子是假冒金融机构的网站，偷盗客户的信用卡、银行卡等信息。例如，中国工商银行网站为“**www.icbc.com.cn**”，有人注册了网站**www.lcbc.com.cn**。
- 这种欺骗方式被专家定义为网络陷井程序，也叫做网络钓鱼程序（**phishing**）,多以欺骗用户信用卡号、银行帐号、股票信息等获取经济利益为目的。

- 防止基本的网站欺骗的最好办法是使用站点服务器认证。
- 服务器认证是服务器向客户提供的一个有效证书，它能证明谁是谁，可以把证书看作服务器的一张身份证。
- 服务器认证不容易被欺骗而且提供了较高级别的保护，确保正在连接的站点是真正属于用户所期待的站点。

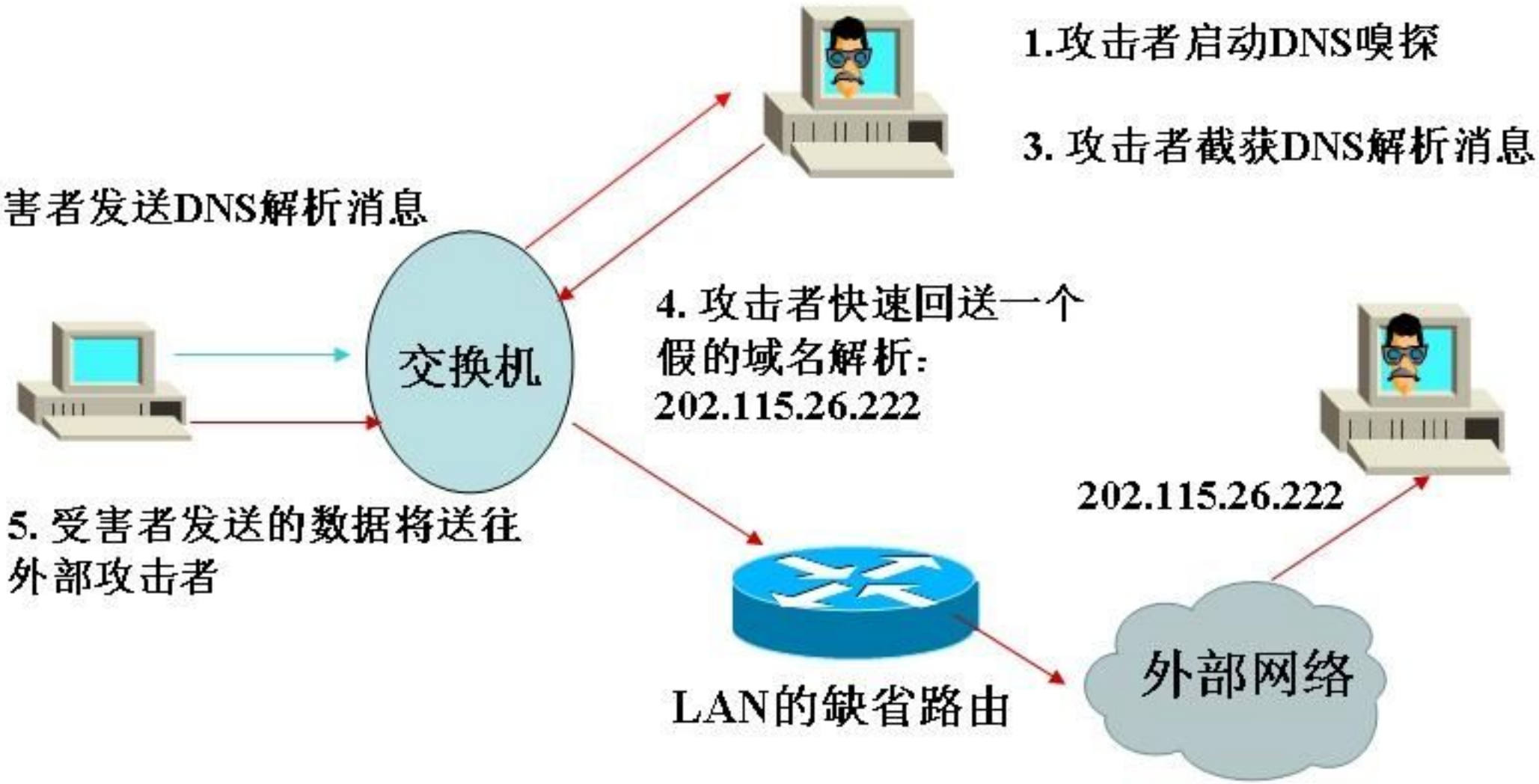
中间人攻击

- 所有不同类型的攻击都能使用中间人攻击，不止是Web欺骗。
- 在中间人攻击中，攻击者找到一个位置，使进出受害方的所有流量都经过他。
- 攻击者通过某种方法把目标机器的域名对应的IP更改为攻击者所控制的机器，这样所有外界对目标机器的请求将涌向攻击者的机器，这时攻击者可以转发所有的请求到目标机器，让目标机器进行处理，再把处理结果发回到发出请求的客户机。

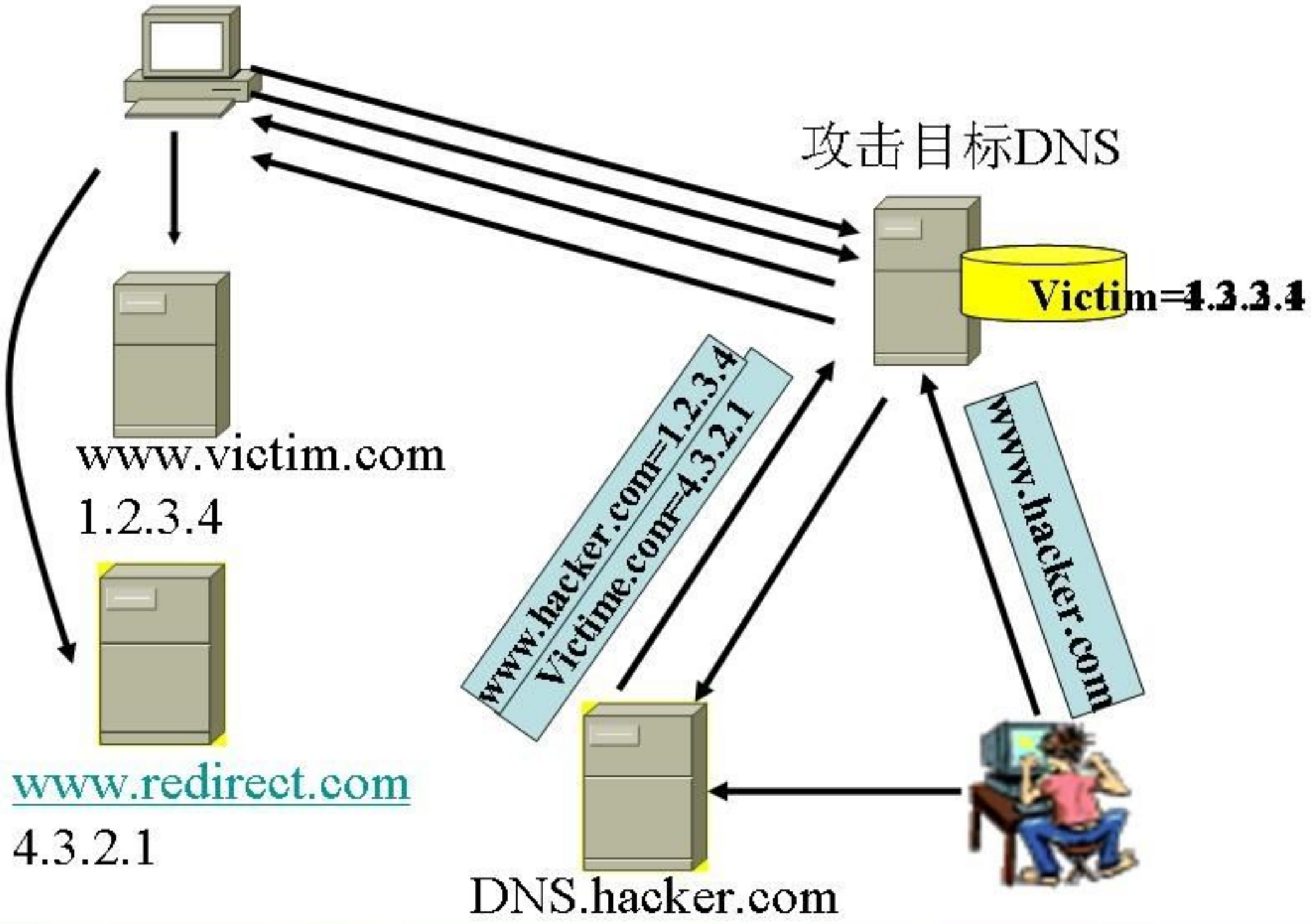
域名解析的过程



嗅探和欺骗DNS



DNS Cache Pollution



新浪首页 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 收藏夹

地址(D) http://www.sina.com.cn/ 转到

-_-o

注册 通行证 登录名 密码 免费邮箱 登录 忘记密码 免费邮箱 VIP邮箱 企业邮箱 设为首页 网站地图

新浪网 sina.com.cn

-_-o

首页 | 新闻 | 财经 | 娱乐 | 视频 | 女性 | 房产 | 旅游 | 游戏 | 军事 | 论 坛 | 企业 | 短信 | 商 城
爱问 | 体育 | 科技 | 音乐 | TV | 育儿 | 家居 | 法治 | 星座 | 上海 | 圈 子 | 城市 | 彩铃 | 图 铃
邮箱 | 博客 | 手机 | 乐库 | 理财 | 美食 | 汽车 | 尚品 | 教育 | 广东 | 高尔夫 | 黄页 | 彩信 | 音悦汇
天气 | 播客 | 数码 | 读书 | 家电 | 交友 | F1 | 健康 | UC | 搜索 | 公 益 | 分类 | 聊天 | 电 台

热销 上海 广东 加盟

金融大家西派国际 亦庄北岸 火爆热销 潘石屹的私密公馆 纳丹堡II 诚意启动 华瀚国际盛大开盘 望京阳光板楼一居
我的手机我做主 亚北臻稀 湾流独栋 国展精装 酒店公寓 世华水岸贺岁开盘 雍景二期 即将开盘 中庭开盘 抢购优惠
天洋城 首付3万 企业独栋·生态办公
宽频影视大讲堂 月亮河二期小户型
视频征婚现场直播 三元桥全现房三居
08年新浪冠军项目 东三环精装大宅
圣世一品.深巷名 CBD金地精装公寓
临湖海宅 即将上 二环60-388m²公寓 国信京西看山阁板 纳帕尔湾 精装独栋 合生国际精装公寓 爱答随行有问必答
美利山 现开始预 玫瑰园IV期大别墅 中海城II即将公开 燕西台 西山别墅 天恒别墅山居别墅 鼠年男人更幸福(图)

教育 培训 招生 出国

45天，突破英语听说！
北京外国语大学·寒假班
如何打造卓越班组模式

爱问搜索 网页 新闻 视频 音乐 图片 地图 知识人 博客 汽车 >>

请输入关键词 搜 索 Google谷歌 热搜 足球先生 集结号 出口退税 旷难

博客·播客 圈子 排行 图片 明星 草根 公益圈

新 闻 奥运站 我的2008 北京时间:2007.12.19

URL重写

- 与中间人攻击类似，在URL重写中攻击者也是将自己插入到通信流中。唯一不同的是，在中间人攻击中，当流量通过互联网时，攻击者必须在物理上能够截取它。如果攻击者在相同的局域网上或者能够攻击一台路由器，这容易做到。但是在其他情况下，则非常难实现。这时，可以使用URL重写技术。

URL重写

- 在URL重写中，攻击者重写网页上的URL链接，把用户指向或者重定向到攻击者控制的机器。
  - 一个正常的链接看上去如下所示：
  - <A href="http://www.sohu.com/news1.htm">Write for us</A>
  - 当用户单击"Write for us"时，可以打开网页http://www.sohu.com/news1.htm
  - 攻击者把链接修改为：
  - <A href="http://attacker.site.comhttp://www.sohu.com/news1.htm">Write for us</A>
  - 当用户单击"Write for us"时，也能浏览网页http://www.sohu.com/news1.htm，在浏览器上看不出什么不同。事实上当用户单击这些被修改的链接时，数据包首先到达攻击者的网站，然后再重定向到正确的站点。从用户的角度看，一切正常。但是攻击者参考了所有通信，而且他能截取或者修改任何信息。

URL重写

- 浏览器的地址栏和状态栏可以显示连接中的Web站点地址及其相关的传输信息，用户可以由此发现URL重写的问题，
- 攻击者往往在URL地址重写的同时，利用其它方法，如使用JavaScript程序来重写地址栏和状态栏，以达到其掩盖欺骗的目的。

Web欺骗的防范

- 注意观察URL地址栏的变化
- 不要信任不可靠的URL信息
- 对服务器和客户端的身份进行鉴别
  - SSL协议

内容

1. ARP欺骗
2. IP欺骗
3. 路由欺骗攻击
4. 电子邮件欺骗
5. Web欺骗
6. 非技术类欺骗

非技术类欺骗

- 把基于非计算机的技术叫做社会工程（也叫社交工程）。在社会工程中，攻击者设法让人相信他是其他人。
- 社交工程的核心是，攻击者设法伪装自己的身份并设计让受害人泄密私人信息，比如通过欺骗某人使之泄露口令或者在系统中建立个新帐号。
- 其目标是搜集信息来侵入计算机系统，其他目标包括侦察环境，找出安装了什么硬件和软件、服务器上装载了什么补丁等信息。
- 通过社会工程得到的信息是无限的。

社会工程的例子

- 攻击者打电话给帮助台要求建立一个新帐号。例如，攻击者假装是一名新员工，要求尽快建立一个新帐号。
- 攻击者打电话给IT部门，假装成一个查询公司正在运行何种软件的卖主。
- 攻击者假冒经理让员工给他发建议书。

- 社会工程相当简单，但又相当有效。
- 他利用了人类的弱点。象防火墙、入侵检测系统这样的技术对这种攻击不起作用。
- 这种攻击能够从根部入侵，从信息安全体系的角度看，人是信息安全体系中最容易成为薄弱环节的要素。

倒转的社会工程

- 在这种类型的攻击中，角色是反过来的，不是攻击者寻求帮助，而是用户向他寻求帮助。
- 为了执行倒转社会工程，攻击者必须将自己插入到正常情况下用户要求帮助的流中。攻击者这么做是使公司意识到他能为用户提供支持或者帮助.

防范社会工程

- 制定合理的制度和规范
- 加强对相关人员的教育和培训，使其时刻保持安全意识

Website: http://www.allimagetool.com

Q & A

轻用其芒，动即有伤，是为凶器；

深若藏拙，临机取决，是为利器。

--《古剑铭》