# 福昕PDF编辑器 个人版

**• 永久 • 轻巧 • 自由**

立即下载

购买会员

**永久使用**

无限制使用次数

**极速轻巧**

超低资源占用，告别卡顿慢

**自由编辑**

享受Word一样的编辑自由

扫一扫，关注公众号

http://edit.foxitreader.cn

# 福昕PDF编辑器 个人版

**• 永久 • 轻巧 • 自由**

立即下载

购买会员

**永久使用**

无限制使用次数

**极速轻巧**

超低资源占用，告别卡顿慢

**自由编辑**

享受Word一样的编辑自由

扫一扫，关注公众号

http://edit.foxitreader.cn

# 网络攻击--加密技术

梁宗文　西南石油大学

# 学习内容

- 网络安全问题
- 引发网络安全问题的原因
- 网络安全目标

# 网络安全问题

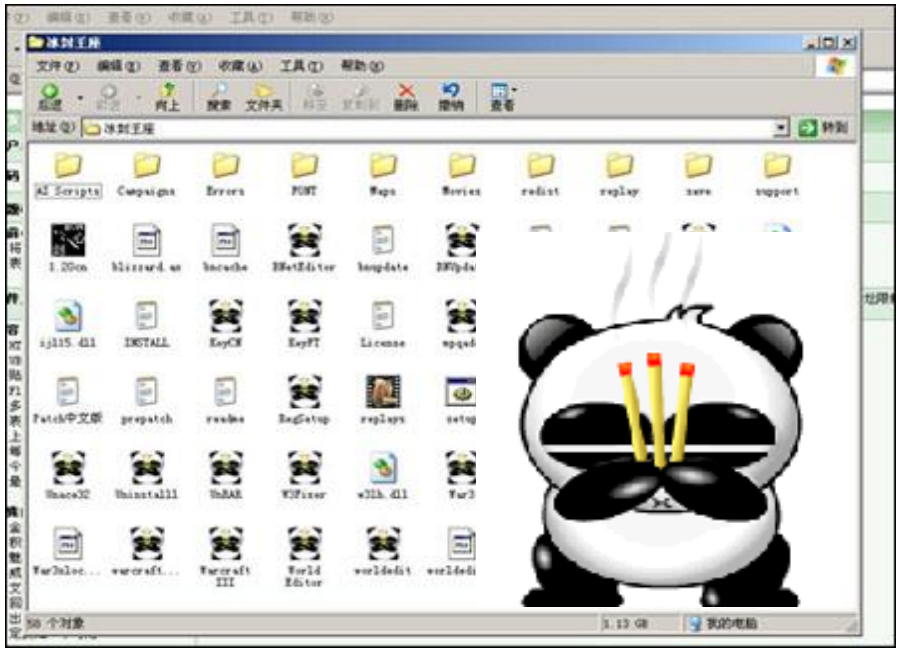
## 什么是网络安全？

- 网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。
- 网络安全从其本质上来讲就是网络上的信息安全。

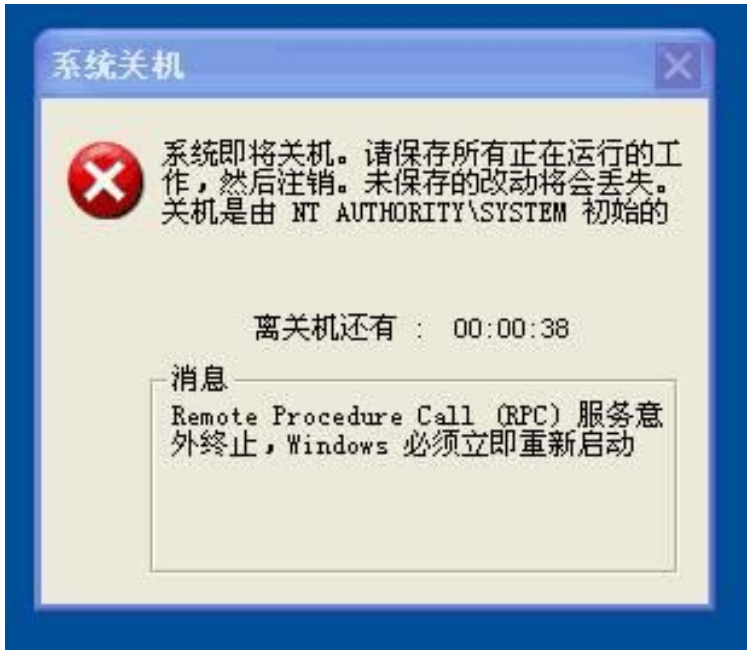
# 网络安全问题

## 常见的网络威胁：

### 1．病毒侵害



熊猫烧香




冲击波病毒

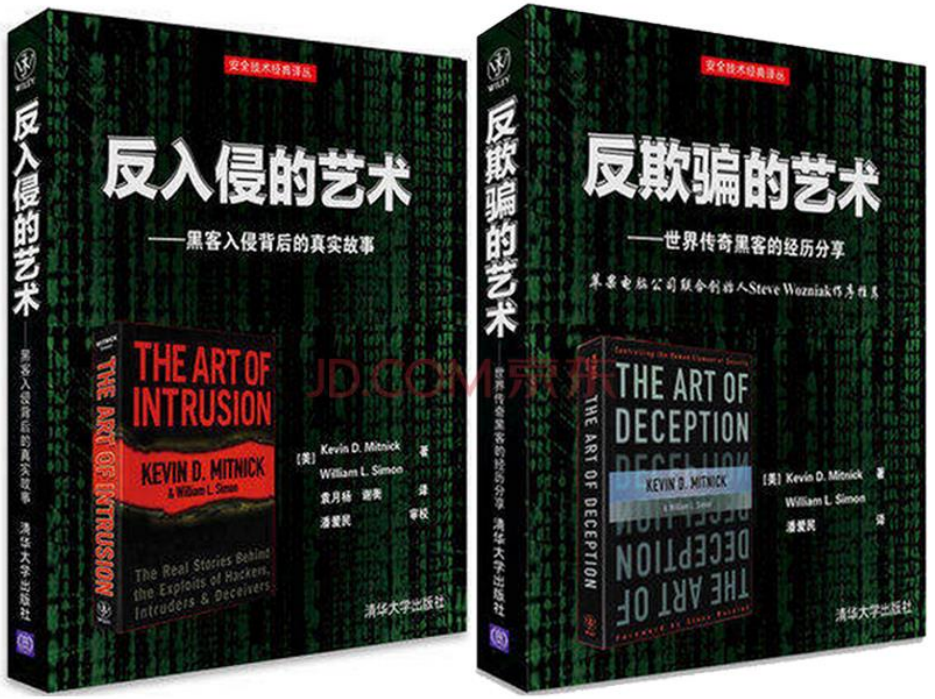
# 网络安全问题

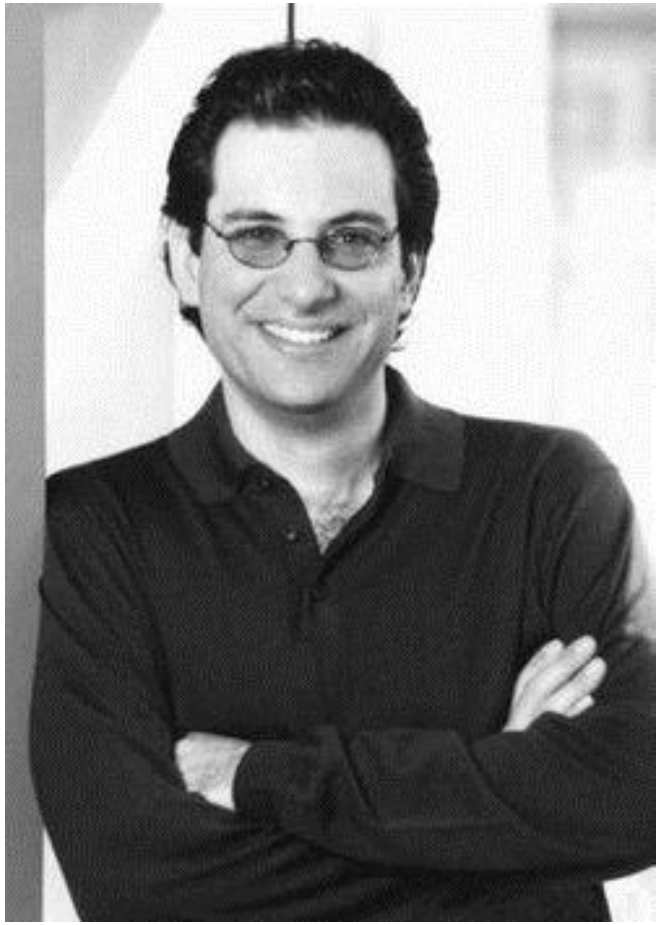
## 常见的网络威胁：

### 2．黑客攻击

黑客是指具有以下行为

- 一是侵入他人计算机
  系统中的信息，或者
  提供服务；
- 二是使网络无法正常



凯文·米特尼克
“世界头号黑客”

# 网络安全问题

## 常见的网络威胁：

### 3．拒绝服务攻击

**拒绝服务攻击**是一种使网络丧失服务功能的攻击行为，

比如电子邮件无法发送、网站无法登陆。

# 网络安全问题

## 常见的网络威胁：

### 4．网络欺骗

中国移动通信的网站域名是

www.10086.cn

- 提供近似域名的链接

www.l0086.com

- 域名映射到错误的IP地址上

# 引发网络安全问题的原因

## 1．网络和网络中信息资源的重要性

- 个人私密信息
- 公司单位秘密信息
- 国家机密信息

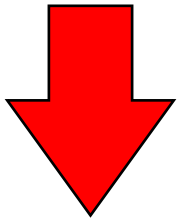
**太多的利益诱惑**

# 引发网络安全问题的原因

## 2．技术与管理缺陷

### （1）通信协议固有缺陷

- 网络协议的原旨是实现终端间的通信过程
- 设计TCP/IP协议族时更多考虑的是开放性和包容性
- 对安全因素考虑不够



**Internet安全方面的先天不足**

# 引发网络安全问题的原因

## 2．技术与管理缺陷

### （2）硬件、系统软件和应用软件固有缺陷

- 系统漏洞：Windows、浏览器
- 漏洞很难免：
  - Windows2000操作系统约4000万行代码，30915个文件
  - 系统开发过程：内部测试版、公开测试版、候选版、正式版等，但还有Bug，然后数以百计的补丁，月补丁最多达21个。

# 引发网络安全问题的原因

## 2．技术与管理缺陷

### （3）不当使用和管理不善

- 如用姓名、生日；常见数字串，如12345678；常用单词，如admin等作为口令
- 网络硬件设施管理不严，黑客可以轻而易举地接近交换机等网络接入设备
- 杀毒软件不及时更新
- 不及时下载补丁软件来弥补已经发现的系统软件和应用软件的漏洞
- 下载并运行来历不明的软件
- 访问没有经过安全认证的网站

# 网络安全目标

## 网络安全目标：

- **可用性**：始终保证授权用户能用，非授权用户不能用。
  身份鉴别
- **保密性**：始终保证非授权用户无法看到网络信息。 数据加密
- **完整性**：始终保证网络信息不被篡改。 消息摘要
- **不可抵赖性**：不能否认曾经完成的操作或承诺 数据签名
- **可控制性**：对网络信息传播方式和内容进行控制

# 网络攻击举例

- SYN泛洪攻击
- Smurf攻击
- DHCP欺骗攻击
- ARP欺骗攻击
- 路由项欺骗攻击

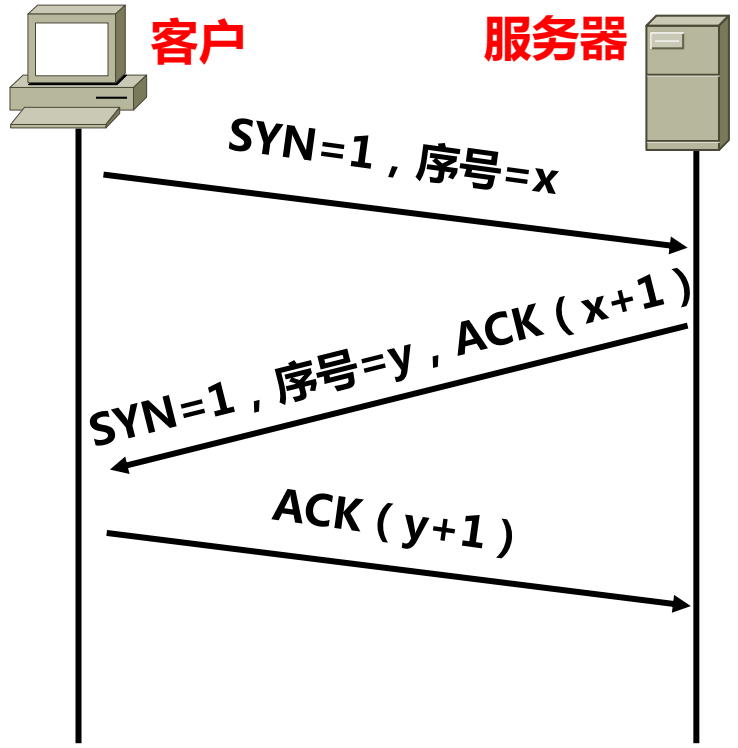
# SYN泛洪攻击

TCP首部控制信息

| 源 端 口 | | | | | | | | 目 的 端 口 |
|---|---|---|---|---|---|---|---|---|
| 序 号 | | | | | | | | |
| 确认序号 | | | | | | | | |
| TCP 首部长度 | 保留 | | URG | ACK | PSH | RST | SYN | FIN | 窗 口 |
| 检 验 和 | | | | | | | | 紧 急 指 针 |
| 可选项 | | | | | | | | |

## 1．SYN泛洪攻击原理

- 终端访问web服务器之前，必须建立与web服务器之间的TCP连接，建立TCP连接过程是三次握手过程。




建立TCP连接的三次握手过程

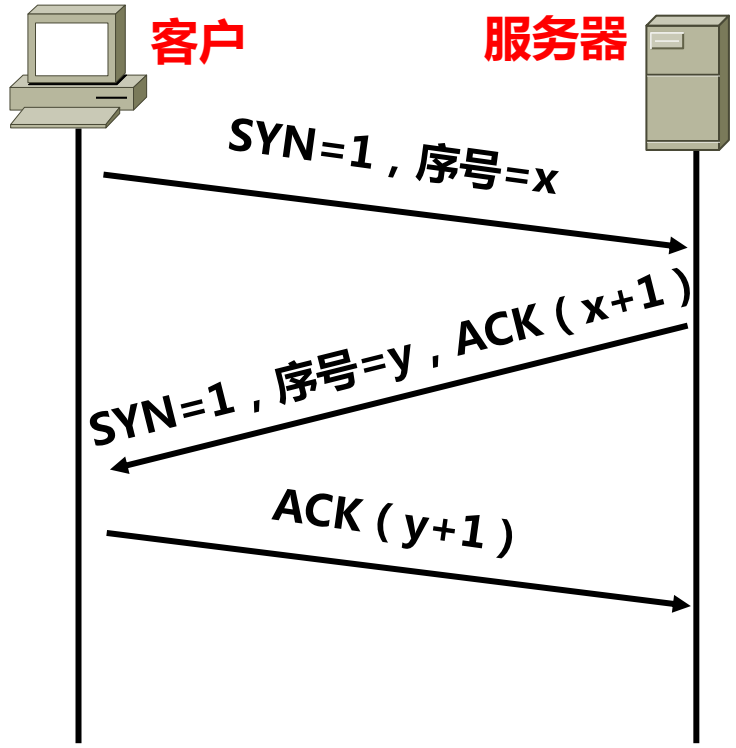
# SYN泛洪攻击

TCP会话表

| 序号 | 会话信息 |
| --- | --- |
| 1 | 会话1信息 |
| 2 | 会话2信息 |
| …… | …… |
| | |

## 1．SYN泛洪攻击原理

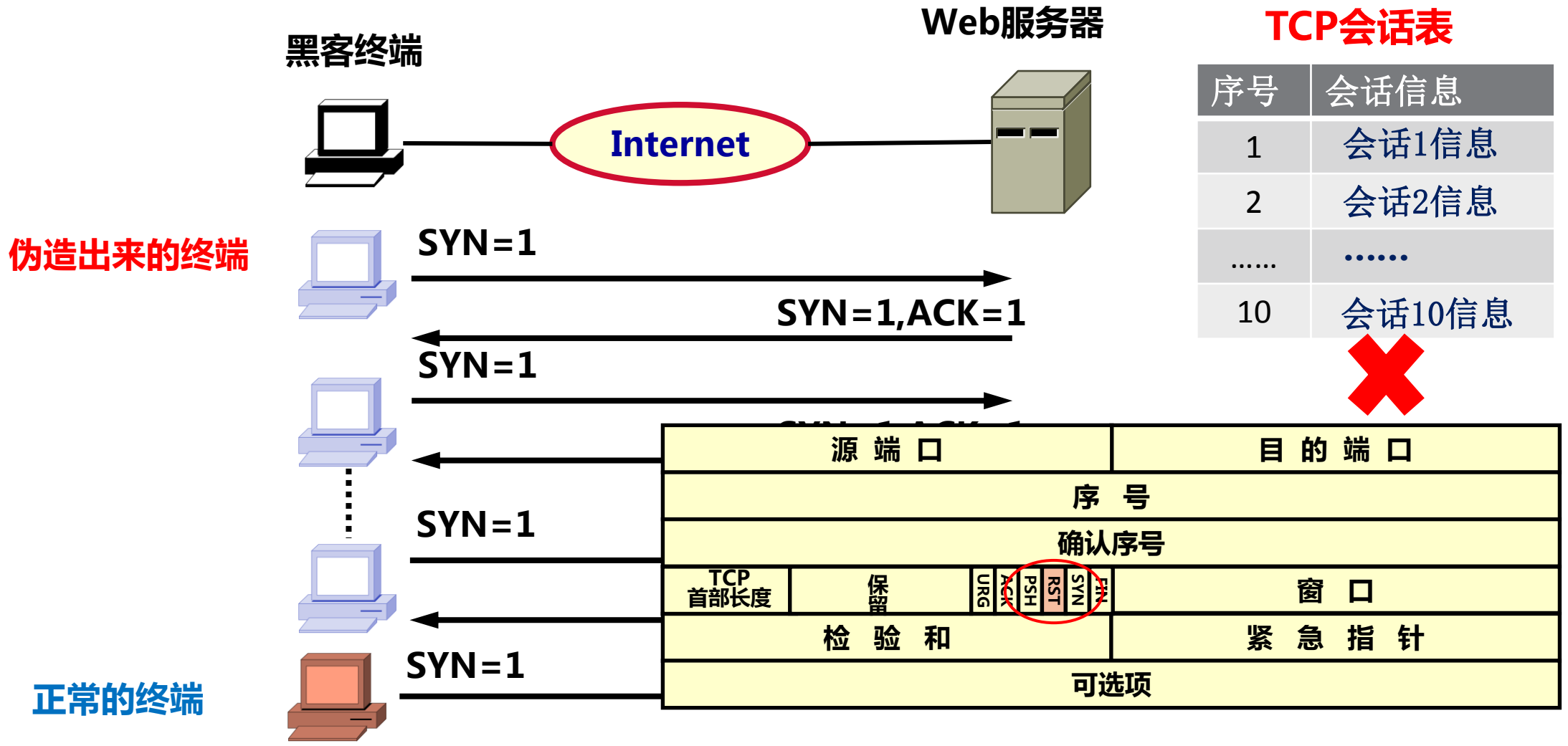
- 终端访问web服务器之前，必须建立与web服务器之间的TCP连接，建立TCP连接过程是三次握手过程。
- SYN泛洪攻击就是通过快速消耗掉web服务器TCP会话表中的连接项，使得正常的TCP连接建立过程无法正常进行的攻击行为。




建立TCP连接的三次握手过程

# SYN泛洪攻击

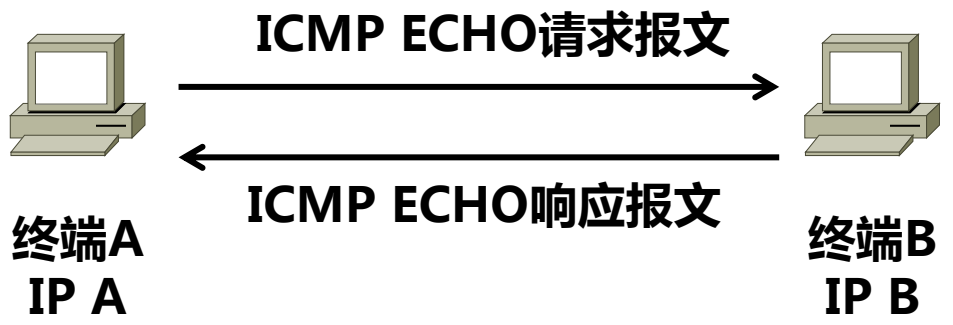
## 2．SYN泛洪攻击过程

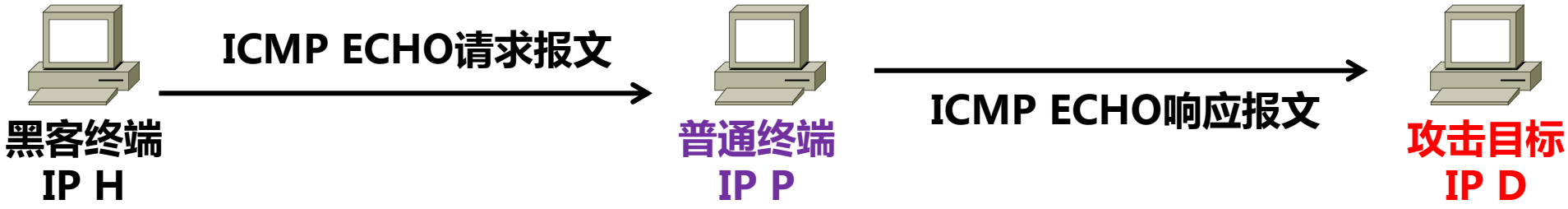


# Smurf攻击

## 1．Smurf攻击原理

- ping过程
- 间接攻击过程




**黑客终端以攻击目标的IP地址为源地址发送ICMP报文**

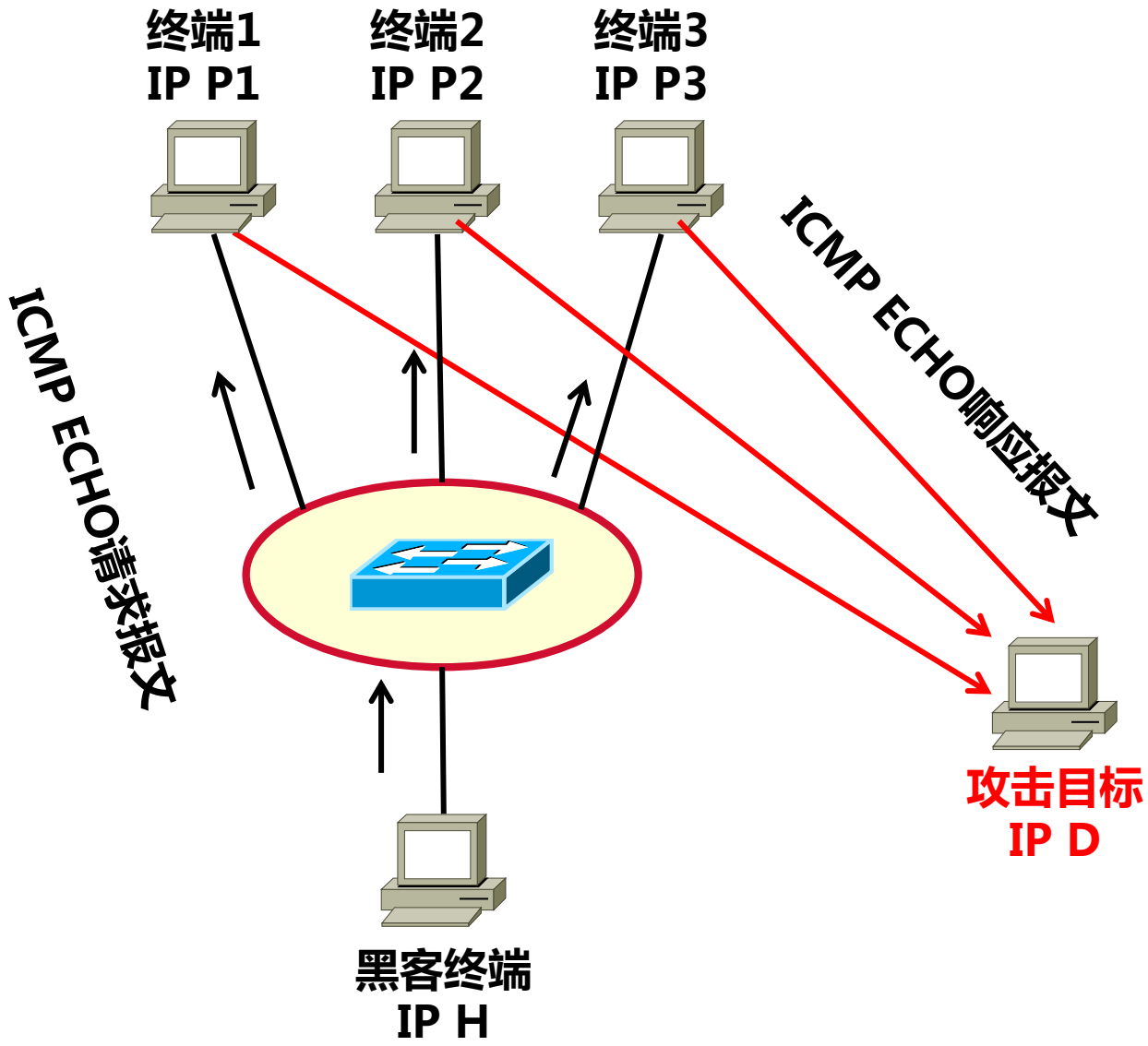
# Smurf攻击

## 1．Smurf攻击原理

- ping过程
- 间接攻击过程
- 放大攻击效果

**黑客终端发送的请求报文：**

- **以攻击目标地址为源地址**
- **以广播地址为目的地址**

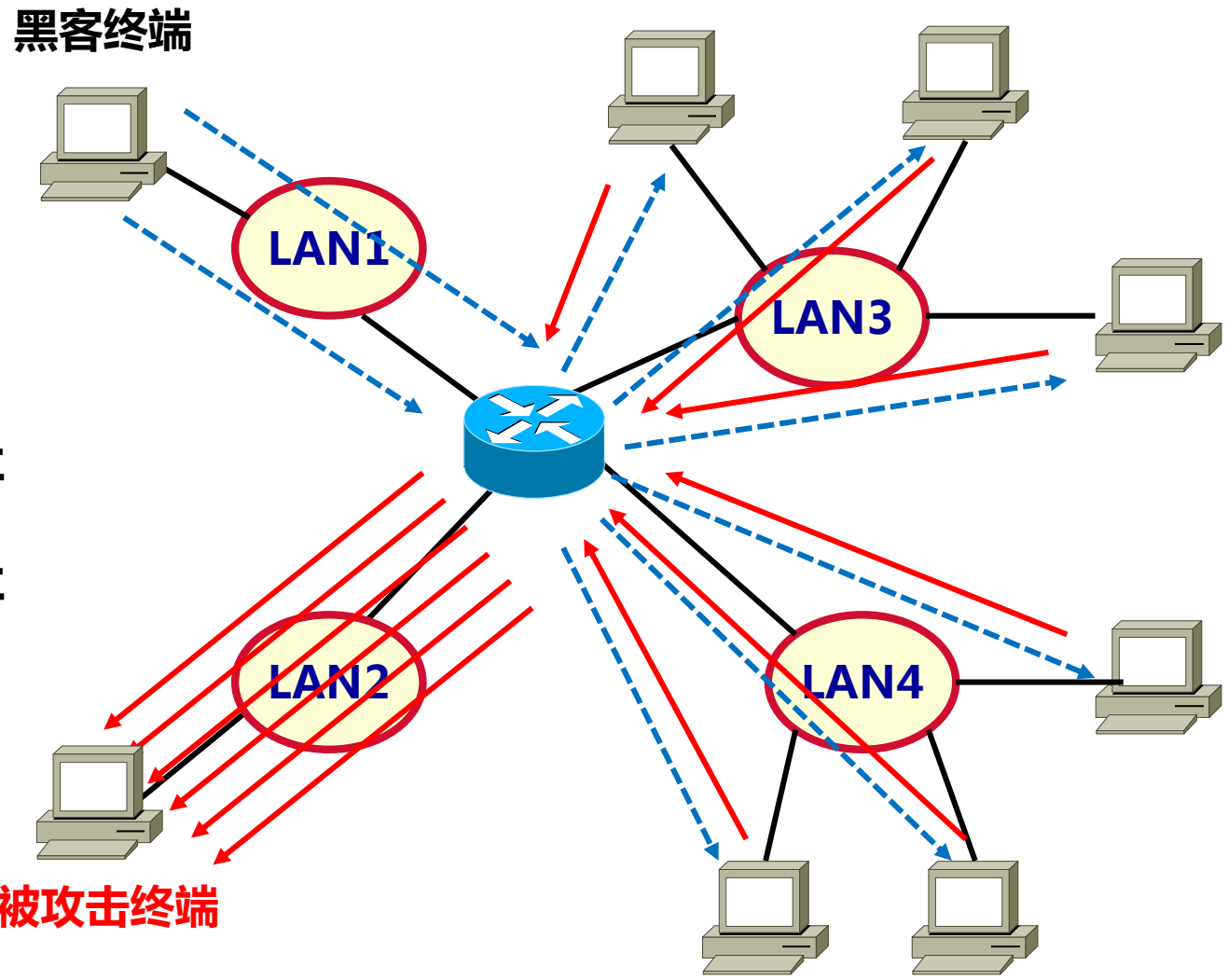


# Smurf攻击

## 2．Smurf攻击过程

黑客终端发送两个ECHO请求报文

- 都以被攻击终端的IP地址为源IP地址
- 以LAN3对应的直接广播地址为目的地址
- 以LAN4对应的直接广播地址为目的地址
- LAN3和LAN4所有终端向被攻击终端回送ECHO响应报文




：ICMP回送请求报文

：ICMP回送响应报文

导致被攻击终端和LAN 3、4之间的数据传输通路发生拥塞

# DHCP欺骗攻击

## 1．DHCP欺骗攻击原理

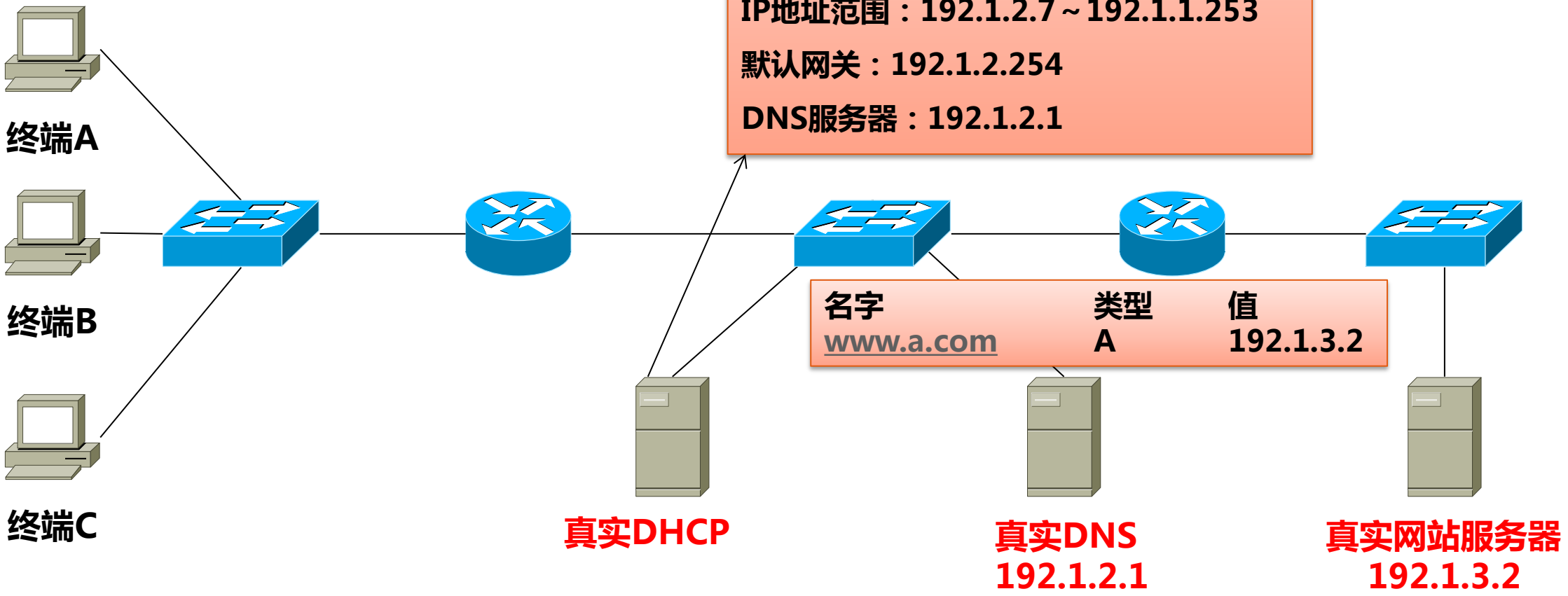
- 终端自动获取的网络信息来自DHCP服务器
- 黑客可以伪造一个DHCP服务器，并将其接入网络中
- 当终端从伪造的DHCP服务器获取错误的默认网关地址或是错误的本地域名服务器地址时，后续访问网络资源的行为将被黑客所控制

# DHCP欺骗攻击

## 2．DHCP欺骗攻击过程

- 钓鱼网站欺骗

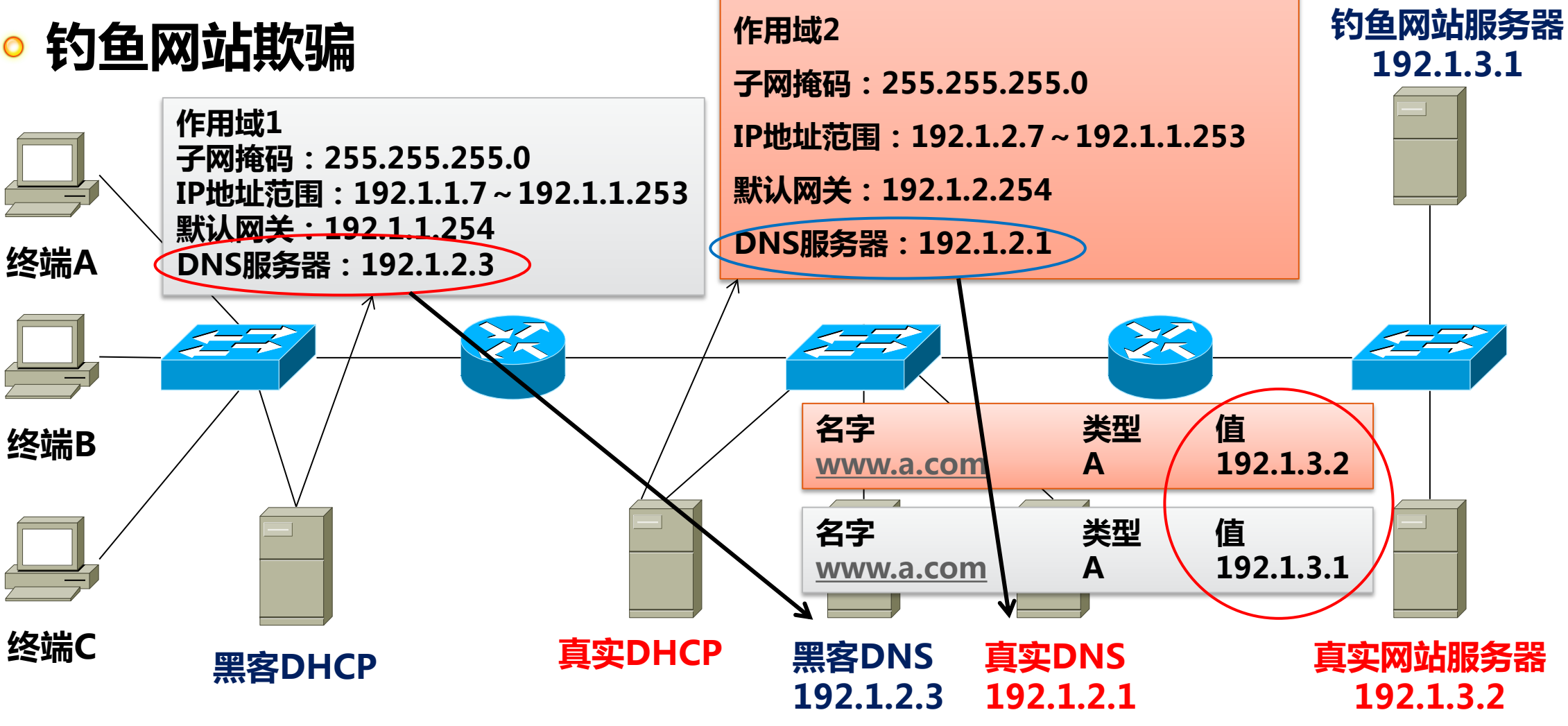
作用域1
子网掩码：255.255.255.0
IP地址范围：192.1.1.7～192.1.1.253
默认网关：192.1.1.254
DNS服务器：192.1.2.1
作用域2
子网掩码：255.255.255.0
IP地址范围：192.1.2.7～192.1.1.253
默认网关：192.1.2.254
DNS服务器：192.1.2.1



# DHCP欺骗攻击

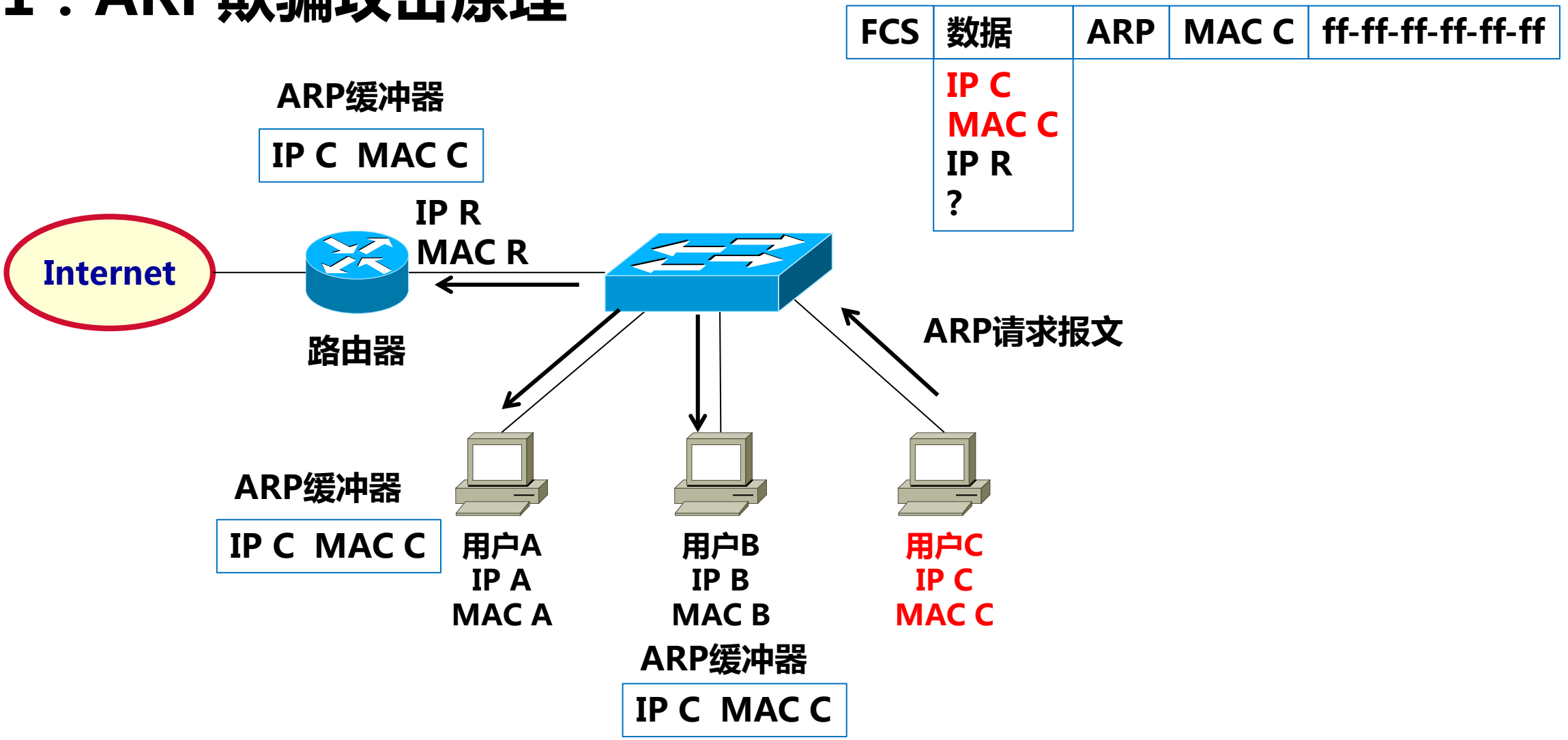
## 2．DHCP欺骗攻击过程

- 钓鱼网站欺骗



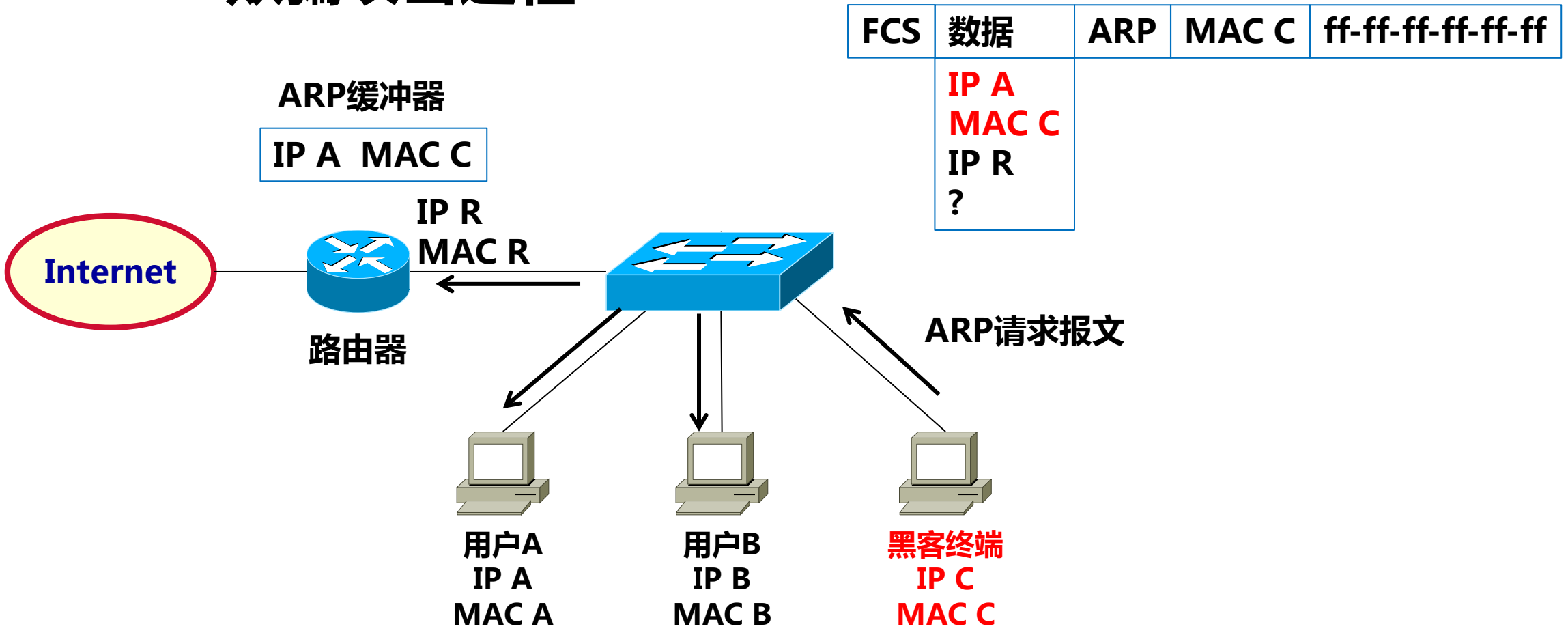
# ARP欺骗攻击

## 1．ARP欺骗攻击原理



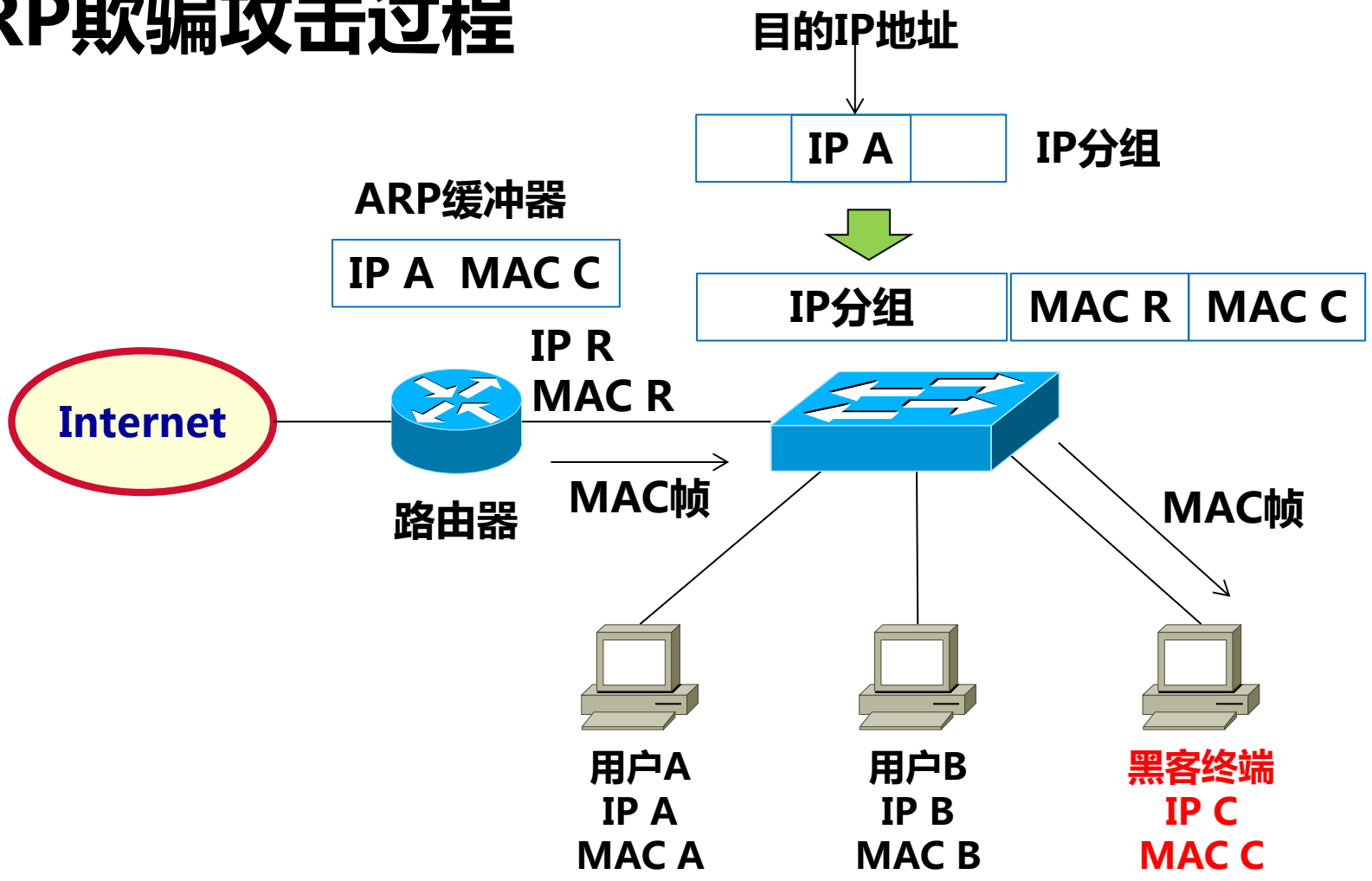
# ARP欺骗攻击

## 2．ARP欺骗攻击过程



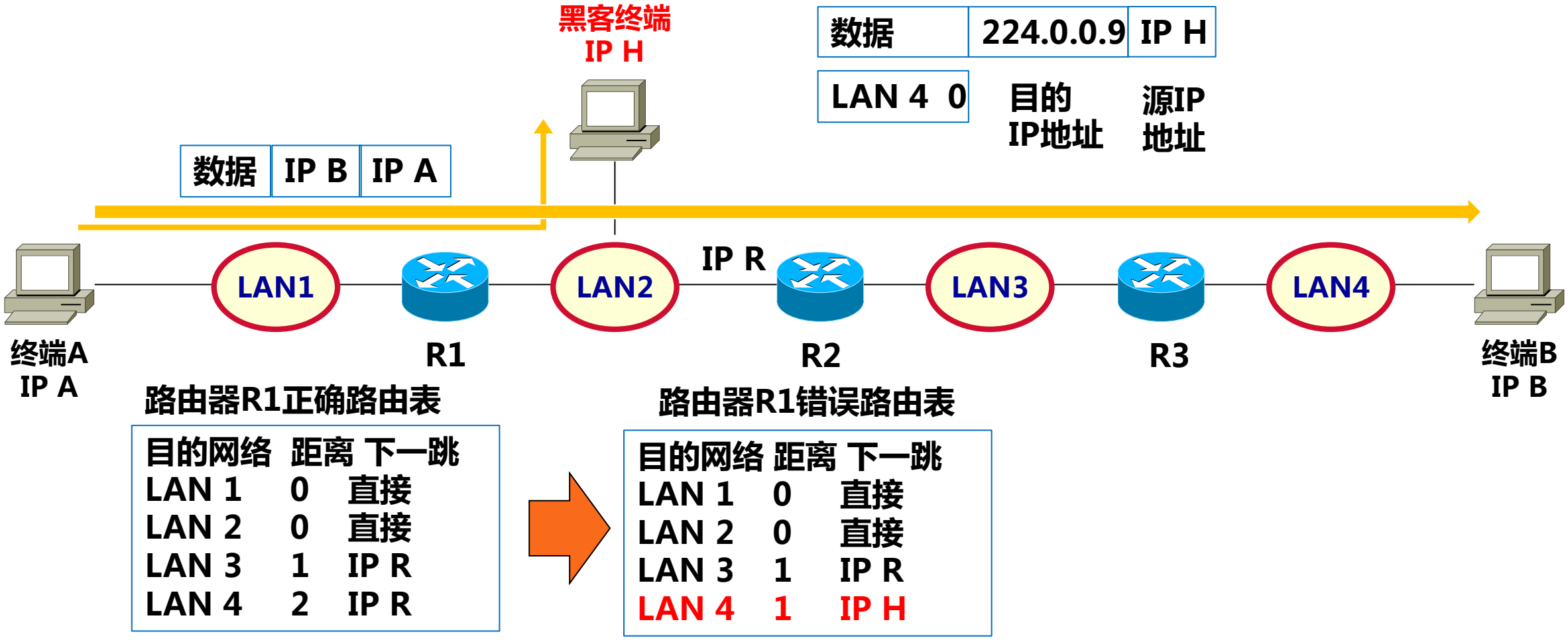
# ARP欺骗攻击

## 2．ARP欺骗攻击过程



# 路由项欺骗攻击

## 路由项欺骗攻击过程



# 小结

- 知己知彼，百战不殆
- 安全技术随着攻击手段的发展而发展
- 了解攻击过程能够更好地理解网络安全技术