

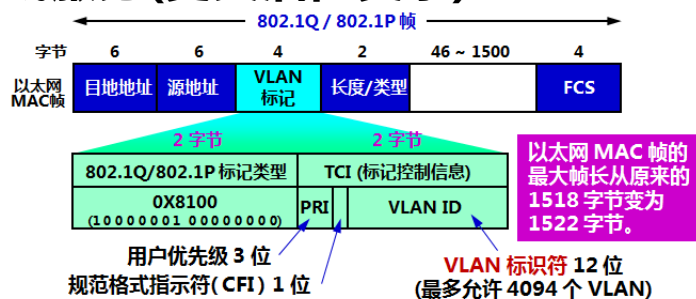
● 虚拟局域网 (VLAN)：用户和网络资源的逻辑组合

- 隔离广播域，控制广播风暴；防止机密信息泄漏；网络连接更加灵活性，节约了成本；简化了网络管理

● 虚拟局域网VLAN划分方法：

- 基于交换机端口(最简单、最常用、在第一层划分)
- 基于MAC地址(允许用户移动、在第二层划分)
- 基于协议类型(以太网帧“类型”字段、在第二层划分)
- 基于IP子网地址(“类型”字段+IP首部源IP地址字段、在第三层划分)
- 基于高层应用或服务(更灵活但复杂)

● VLAN帧格式

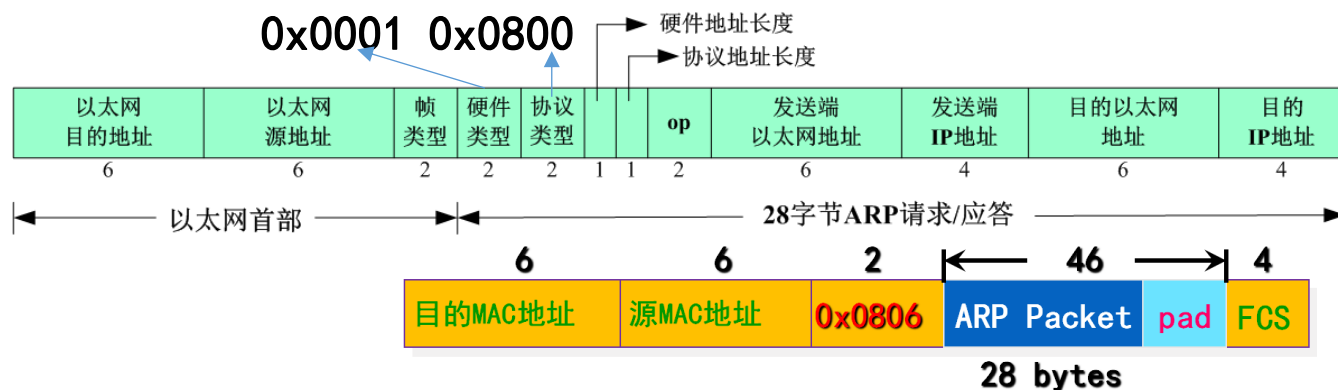


● 交换机端口类型

- Access端口(只属于一个VLAN，发送不带标签报文,一般与计算机连接)
- Trunk端口(可属于多个VLAN，通过标签区别，一般用于交换机之间连接)
- Hybrid端口(可允许不打标签发送，计算机与交换机连接均可)

- **互联网IP地址与物理网物理地址**：IP地址(全网统一编址，具有全局唯一性，通常用软件实现，用在网络层的分组中)；物理地址(由所属的物理网络来定义，具有本地唯一性不一定具有全局唯一性，通常写在硬件\网卡上，包含在数据链路层使用的帧中)；静态映射、动态映射。
- **为什么使用IP地址并调用ARP？**解决了异构网络之间复杂的硬件地址转换问题。

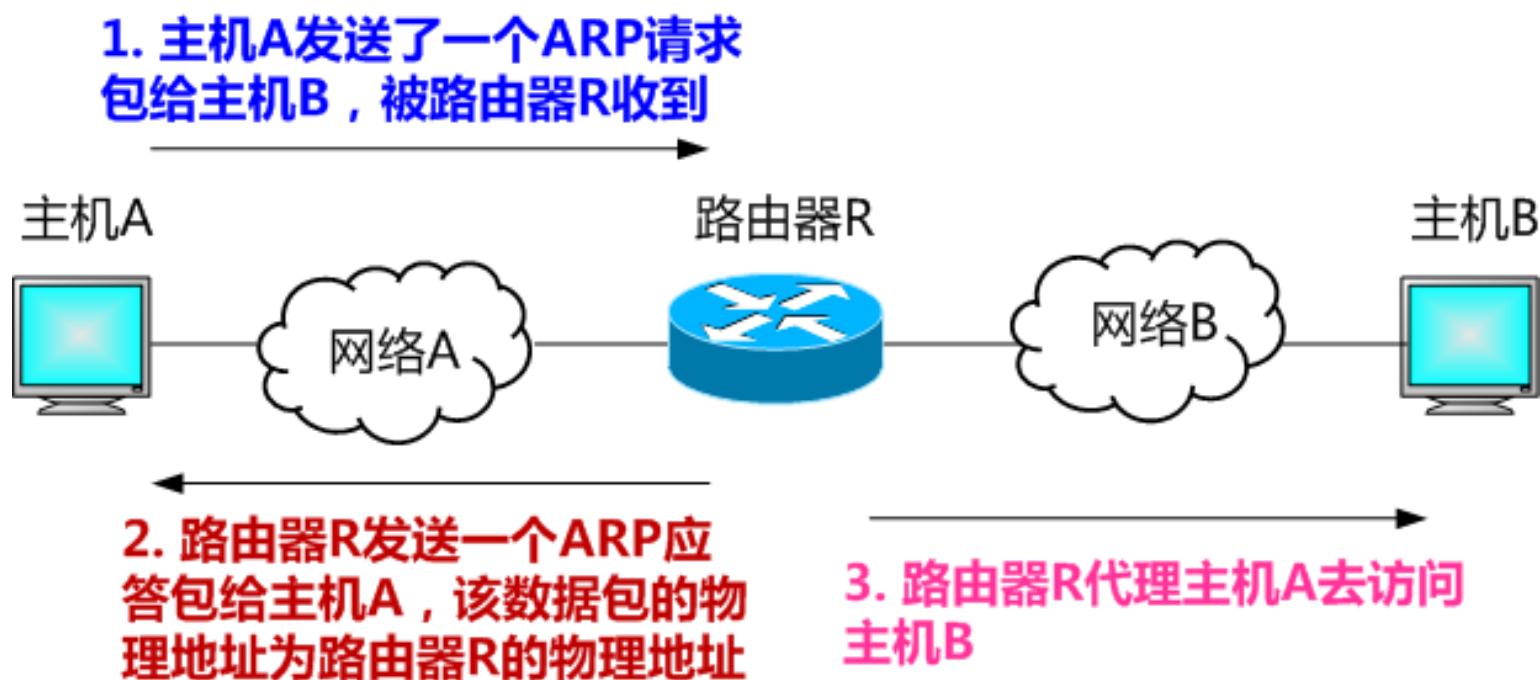
● ARP分组格式：



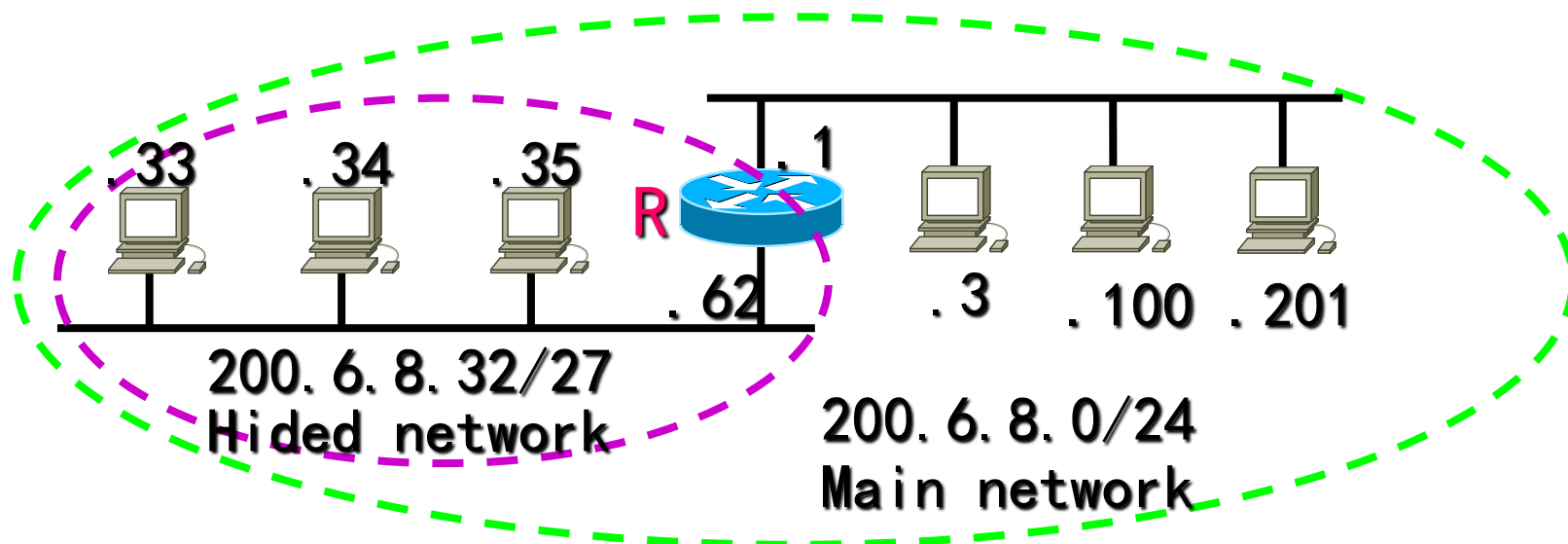
- **ARP高速缓存**：IP地址到硬件地址的映射表 < IP address ; MAC address ; TTL >
- **ARP命令**：-a/g(显示ARP高速缓存中的所有内容); -d inet_addr(删除ARP高速缓存中的某一项内容); -s inet_addr eth_addr(用于静态绑定IP和MAC)。
- **代理ARP**

特殊的ARP — 代理ARP

● 工作原理

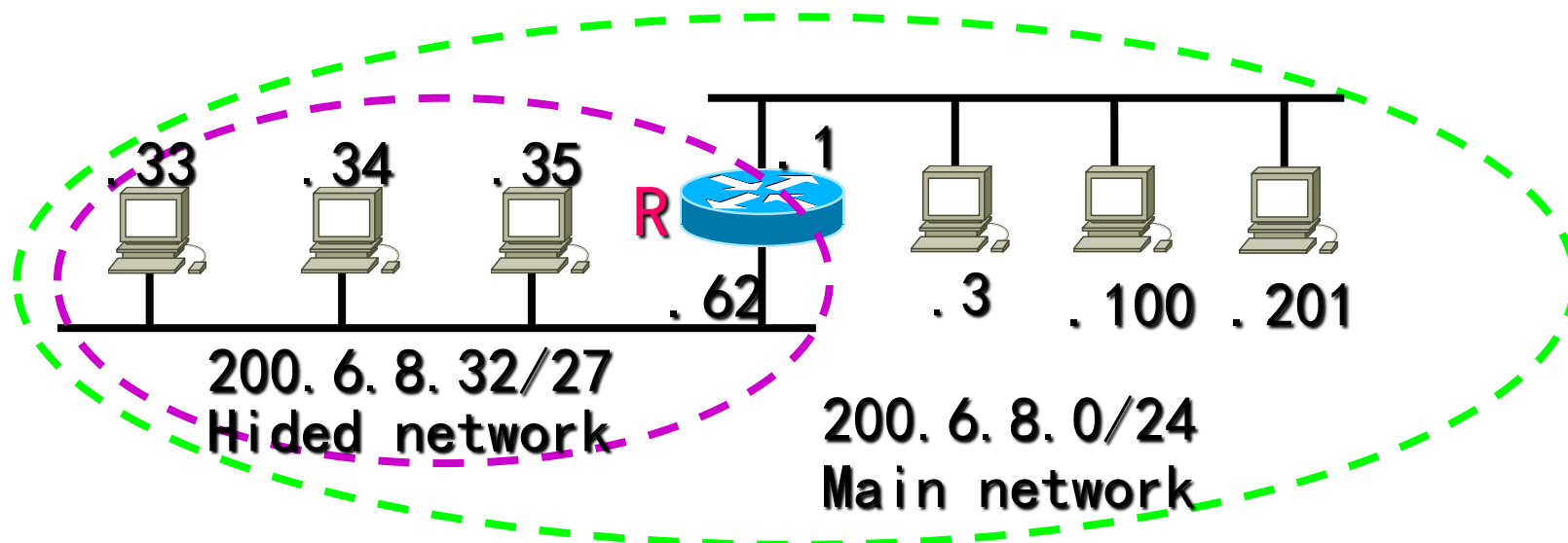


特殊的ARP — 代理ARP



- .35向.3发送IP分组 → IP分组发送成功
 - .35广播请求.62的ARP分组 → ARP成功
- .3向.35发送IP分组 → IP分组发送失败
 - .3广播请求.35的ARP分组, R不转发广播 → ARP失败

特殊的ARP — 代理ARP

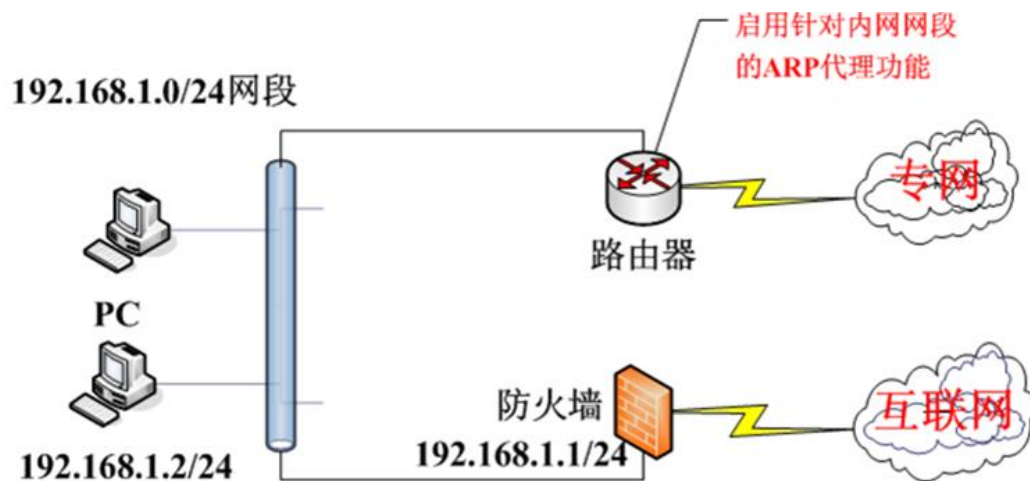


特点：

- 针对具体的网络接口实现
 - 如：R在.62接口上可不启用代理ARP
- 多个IP地址与一个MAC地址的映射关系
 - 如：.3中，.33、.34、.35都映射于R的.1接口的MAC地址
- 保留网络外部特性，隐藏了内部网络的结构

特殊的ARP — 代理ARP

存在的问题：开启代理ARP功能后，可能会导致地址冲突等类似故障，产生一系列不稳定的故障现象。

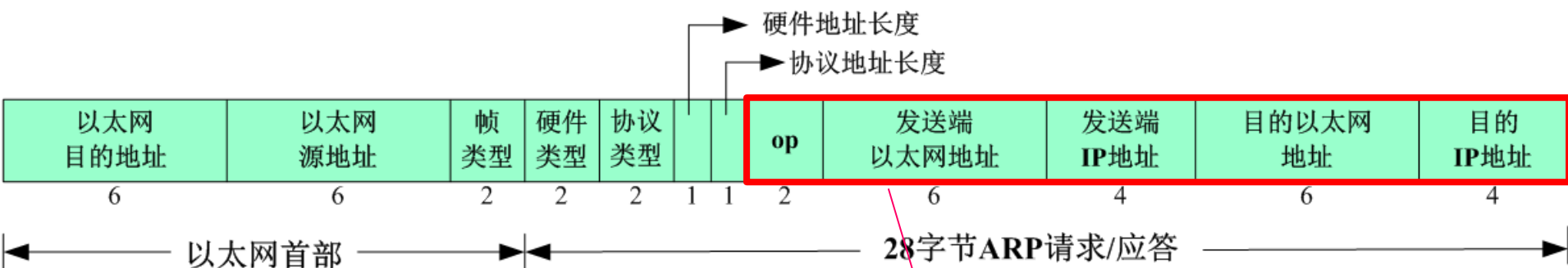


环境描述:

- 1、PC访问互联网时，会向全网发送ARP广播，请求1.1的MAC
- 2、1.1防火墙先收到会响应，PC会将其加入ARP表项
- 3、路由启用了ARP代理，也会响应PC的ARP请求
- 4、路由的ARP响应包后到，导致PC的ARP表项更新

特殊的ARP — 代理ARP

● 存在的安全问题——ARP 欺骗

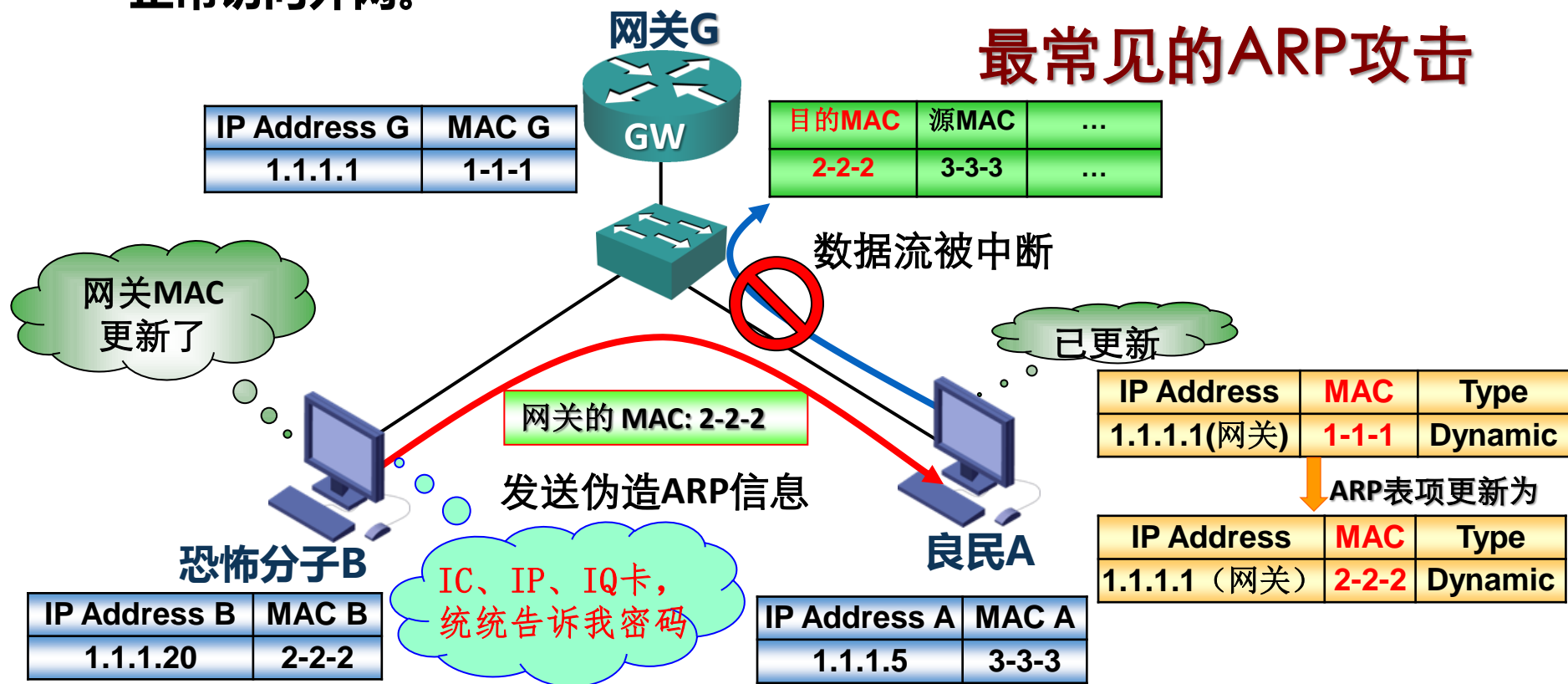


用于以太网的ARP请求或应答分

ARP欺骗都是通过填写错误的IP-MAC对应关系来实现的

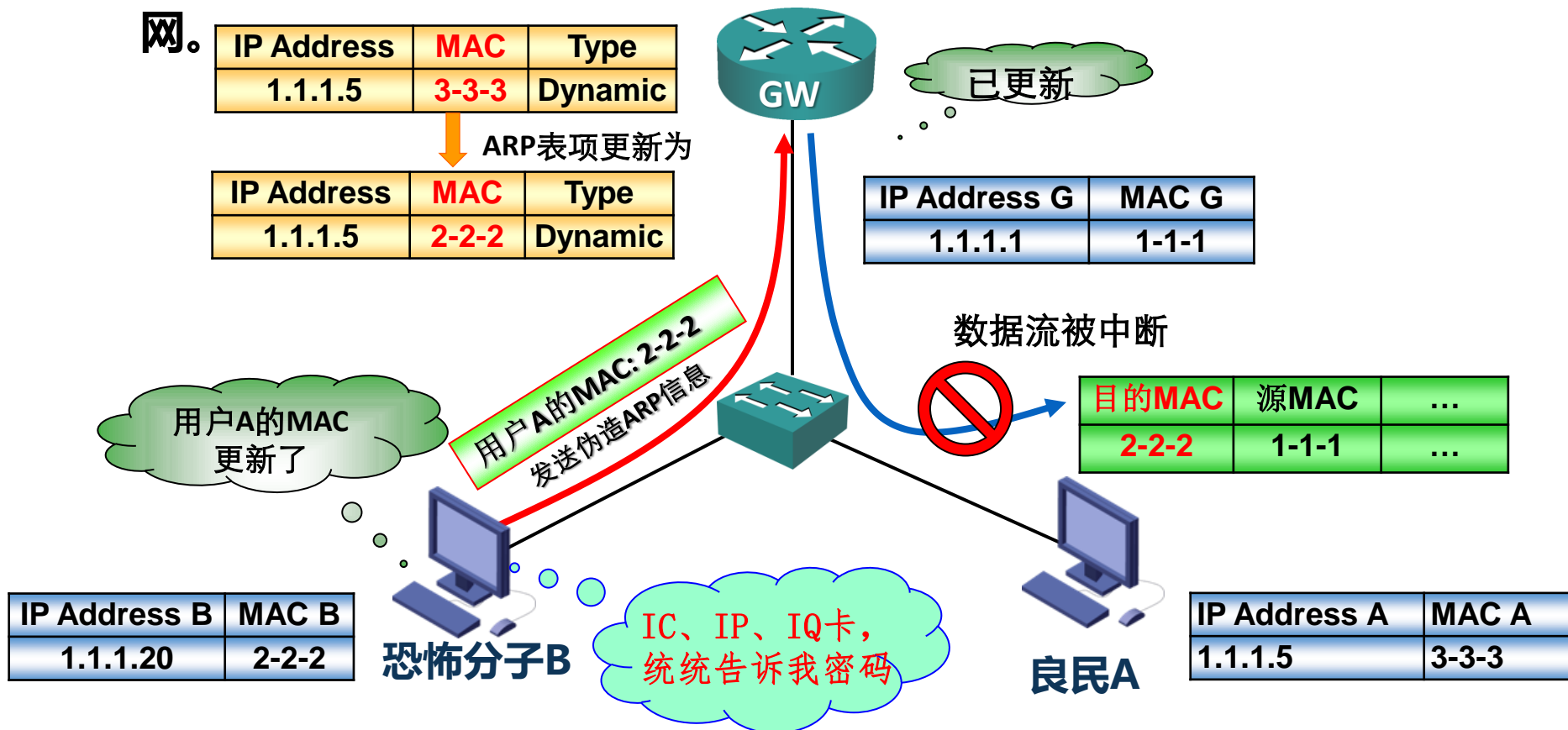
ARP 欺骗攻击--仿冒网关

- 攻击者发送伪造的网关ARP报文，欺骗同网段内的其它主机。主机访问网关的流量，被重定向到一个错误的MAC地址导致该用户无法正常访问外网。



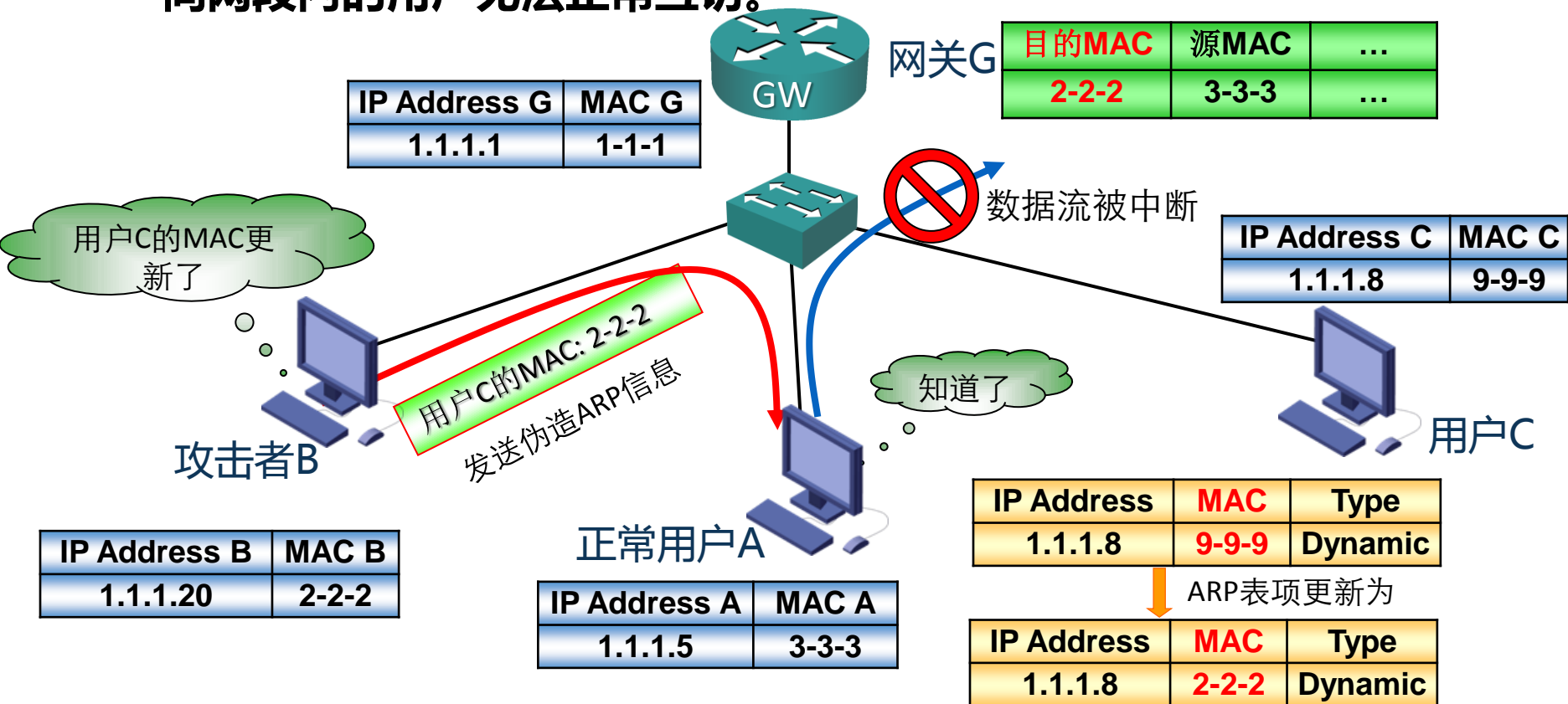
ARP 欺骗攻击--欺骗网关

- 攻击者伪造虚假的ARP报文，欺骗网关。网关发给该用户的所有数据全部重定向到一个错误的MAC地址，导致该用户无法正常访问外网。



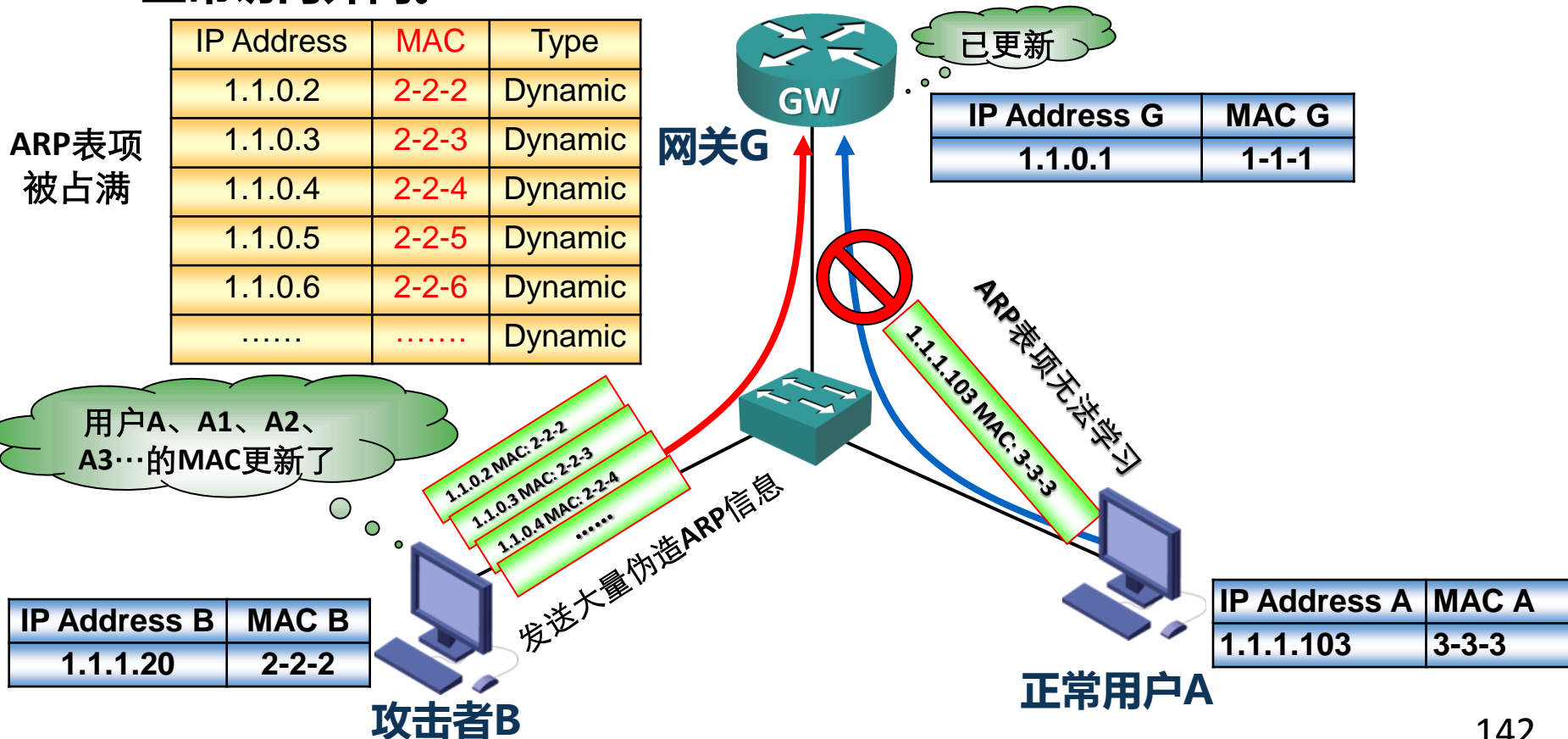
ARP 欺骗攻击--欺骗终端用户

- 攻击者伪造虚假的ARP报文，欺骗相同网段内的其他主机。网段内的其他主机发给该用户的所有数据都被重定向到错误的MAC地址，同网段内的用户无法正常互访。



ARP 欺骗攻击--洪泛攻击

- 攻击者伪造大量不同ARP报文在同网段内进行广播，导致网关ARP表项被占满，合法用户的ARP表项无法正常学习导致合法用户无法正常访问外网。



ARP 欺骗攻击

如何发现正在进行ARP攻击的主机呢？

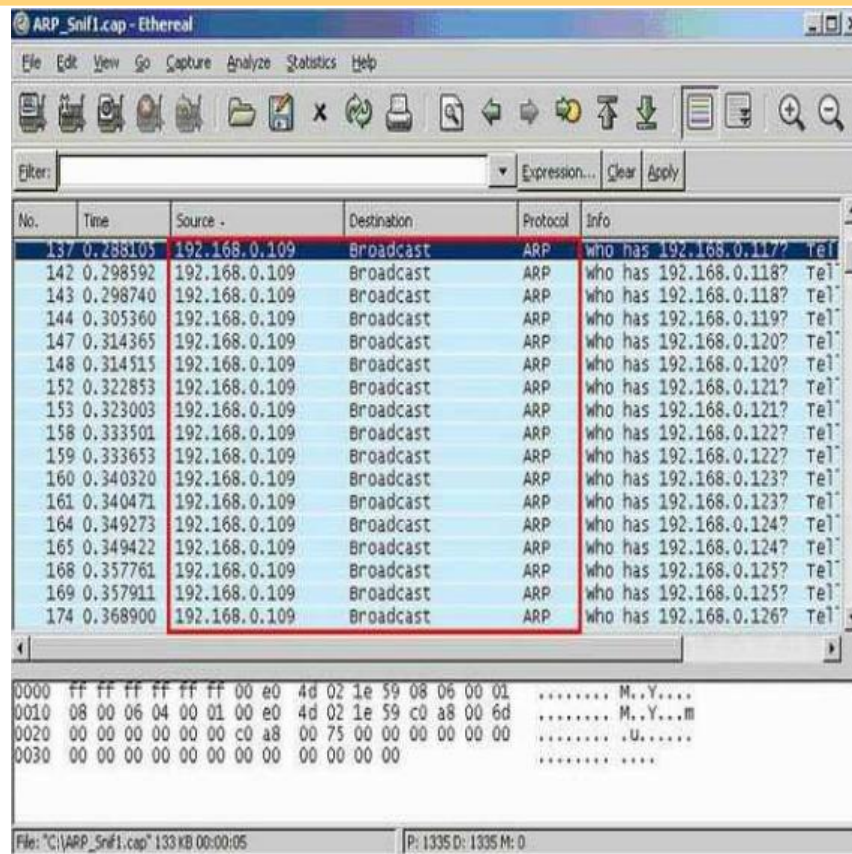
在知道正确的网关MAC地址的情况下，通过arp -a命令看到的另一个网关MAC地址就是攻击主机的MAC地址。再根据网络正常时全网的IP-MAC地址映射表，可以找到攻击主机的IP地址，确定攻击主机。

Internet Address	Physical Address	Type
192.168.0.1	00-50-56-e6-49-56	dynamic

ARP 欺骗攻击

如何发现正在进行ARP攻击的主机呢？

使用软件抓包，发现大量的以同一个IP地址发送的ARP响应包，包中指定的MAC地址就是攻击主机的MAC地址。拥有该IP地址的主机或设备就是攻击主机。



The screenshot shows a Wireshark packet capture titled 'ARP_Sniff1.cap - Ethereal'. The packet list pane displays a series of ARP responses from source IP 192.168.0.109 to various broadcast destinations. The 'Info' column for these packets shows 'who has 192.168.0.117? Tel' and similar queries for other IP addresses. The packet details pane at the bottom shows the raw packet data in hexadecimal and ASCII.

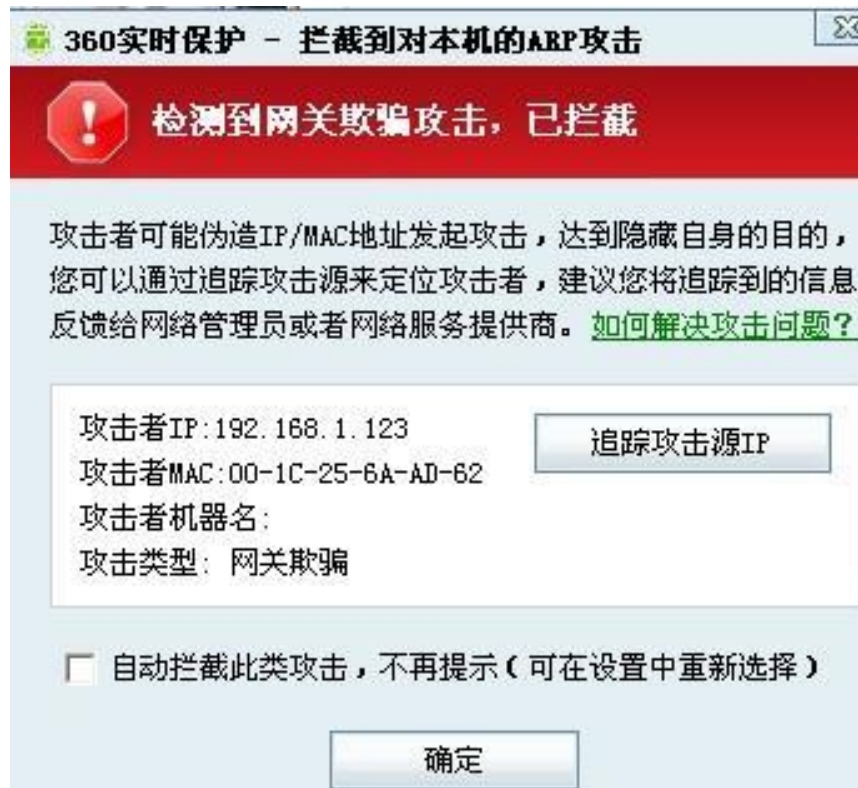
No.	Time	Source	Destination	Protocol	Info
137	0.288105	192.168.0.109	Broadcast	ARP	who has 192.168.0.117? Tel
142	0.298592	192.168.0.109	Broadcast	ARP	who has 192.168.0.118? Tel
143	0.298740	192.168.0.109	Broadcast	ARP	who has 192.168.0.118? Tel
144	0.305360	192.168.0.109	Broadcast	ARP	who has 192.168.0.119? Tel
147	0.314365	192.168.0.109	Broadcast	ARP	who has 192.168.0.120? Tel
148	0.314515	192.168.0.109	Broadcast	ARP	who has 192.168.0.120? Tel
152	0.322853	192.168.0.109	Broadcast	ARP	who has 192.168.0.121? Tel
153	0.323003	192.168.0.109	Broadcast	ARP	who has 192.168.0.121? Tel
158	0.333501	192.168.0.109	Broadcast	ARP	who has 192.168.0.122? Tel
159	0.333653	192.168.0.109	Broadcast	ARP	who has 192.168.0.122? Tel
160	0.340320	192.168.0.109	Broadcast	ARP	who has 192.168.0.123? Tel
161	0.340471	192.168.0.109	Broadcast	ARP	who has 192.168.0.123? Tel
164	0.349273	192.168.0.109	Broadcast	ARP	who has 192.168.0.124? Tel
165	0.349422	192.168.0.109	Broadcast	ARP	who has 192.168.0.124? Tel
168	0.357761	192.168.0.109	Broadcast	ARP	who has 192.168.0.125? Tel
169	0.357911	192.168.0.109	Broadcast	ARP	who has 192.168.0.125? Tel
174	0.368900	192.168.0.109	Broadcast	ARP	who has 192.168.0.126? Tel

File: "C:\ARP_Sniff1.cap" 133 KB 00:00:05 | P: 1335 D: 1335 M: 0

ARP 欺骗攻击

如何发现正在进行ARP攻击的主机呢？

使用工具软件，如360卫士等。



ARP 欺骗攻击防御

1 网关防御

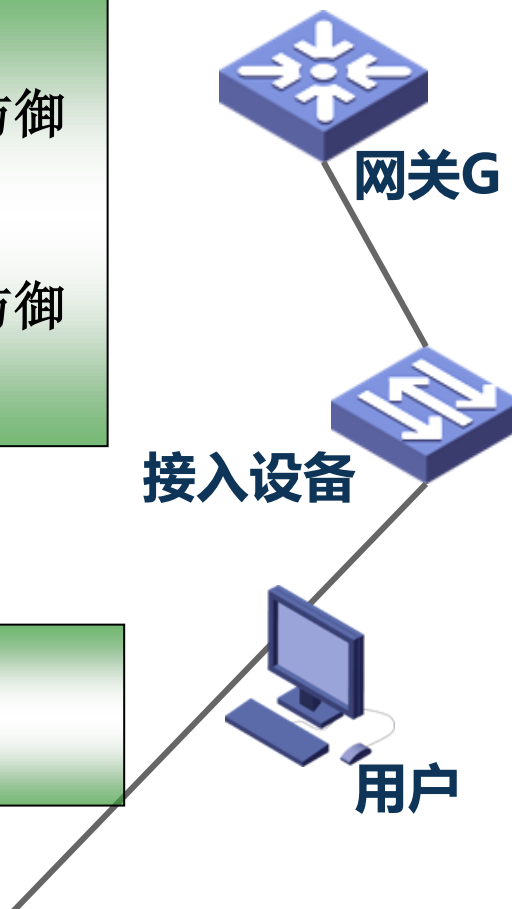
- 合法ARP绑定, 防御网关被欺骗
- ARP数量限制, 防御ARP洪泛攻击

3 客户端防御

- 绑定网关信息

2 接入设备防御

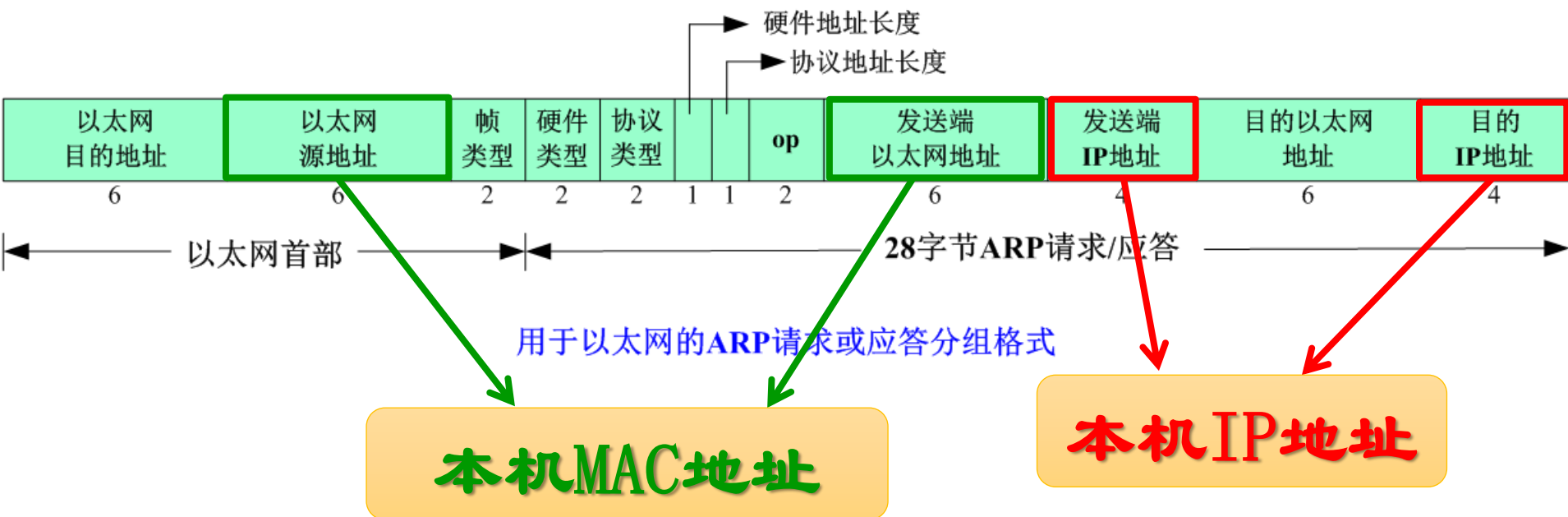
- 网关IP-MAC绑定, 过滤掉仿冒网关的报文
- 合法用户IP-MAC绑定, 过滤掉终端仿冒报文
- ARP限速



特殊的 ARP — 免费 ARP

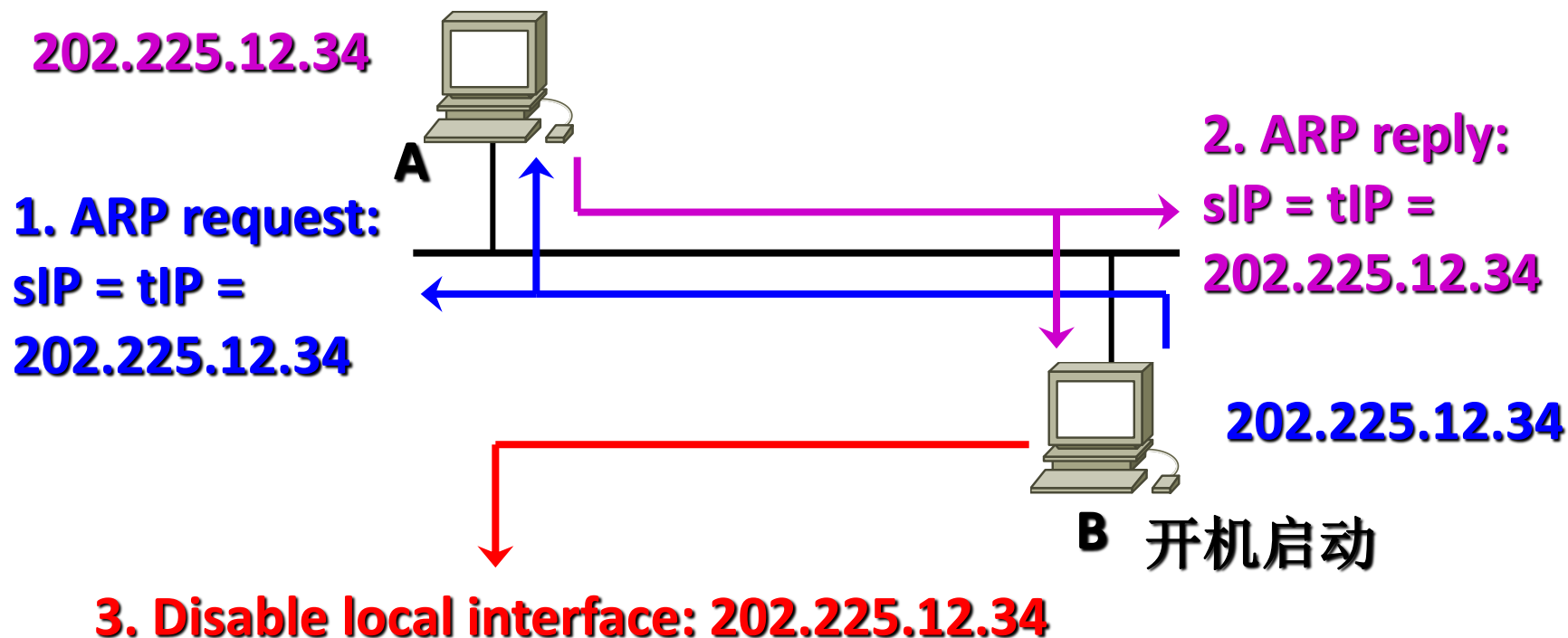
● 免费ARP

发给自己的ARP，一般发生在系统引导时，用来获得网络接口的MAC地址。



免费 ARP 的作用

- **检测IP地址冲突**。一台主机可以通过它来确定另一台主机是否设置了相同的IP地址。免费ARP报文发出去是不希望收到应答的，只希望起宣告作用。



免费 ARP 的作用

- **实现双机主备系统。** A、B两台服务器**互为备份**，主、备机内部使用**串口通信**，实现**心跳监听**。当前A为主机、B监听A，如果B监听不到A的心跳则认为**A发生故障**。B通过发送含有自己的硬件地址和故障服务器A的IP地址的**免费ARP请求**，使得所有目的IP地址为故障服务器A的IP地址的**报文都将被送到备机B**。**备机B顺利接管故障服务器A的工作**，而客户程序不用关心原来的服务器是否出现了故障。

4.1	数据链路层概述
4.2	数据链路层的三个基本问题
4.3	点对点信道的数据链路层协议
4.4	广播信道的数据链路层协议
4.5	扩展局域网
4.6	高速局域网
4.7	地址解析协议