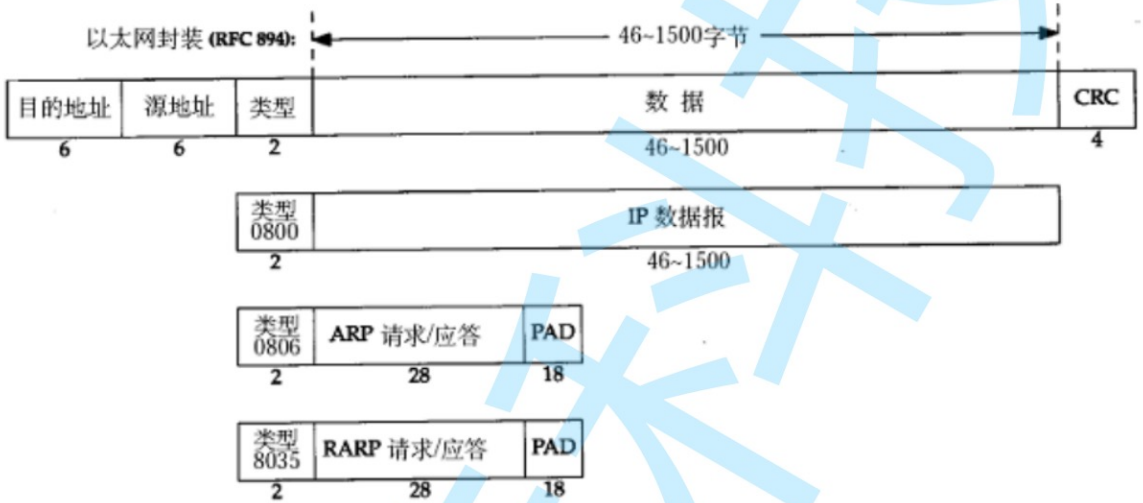
0321_arp_代理服务器

以太网的帧格式如下所示：

以太网的帧格式如下所示：




```
(base) [yufc@ALiCentos7:~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.31.69  netmask 255.255.240.0  broadcast 172.31.31.255
        inet6 fe80::216:3eff:fe01:c36e  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:01:c3:6e  txqueuelen 1000  (Ethernet)
        RX packets 4153884  bytes 3713806026 (3.4 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2479435  bytes 586105318 (558.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
MAC地址
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 809159  bytes 2190683685 (2.0 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 809159  bytes 2190683685 (2.0 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) [yufc@ALiCentos7:~]$
```

- 源地址和目的地址是指网卡的硬件地址(也叫MAC地址), 长度是48位,是在网卡出厂时固
- 帧协议类型字段有三种值,分别对应IP、ARP、RARP;
- 帧末尾是CRC校验码。

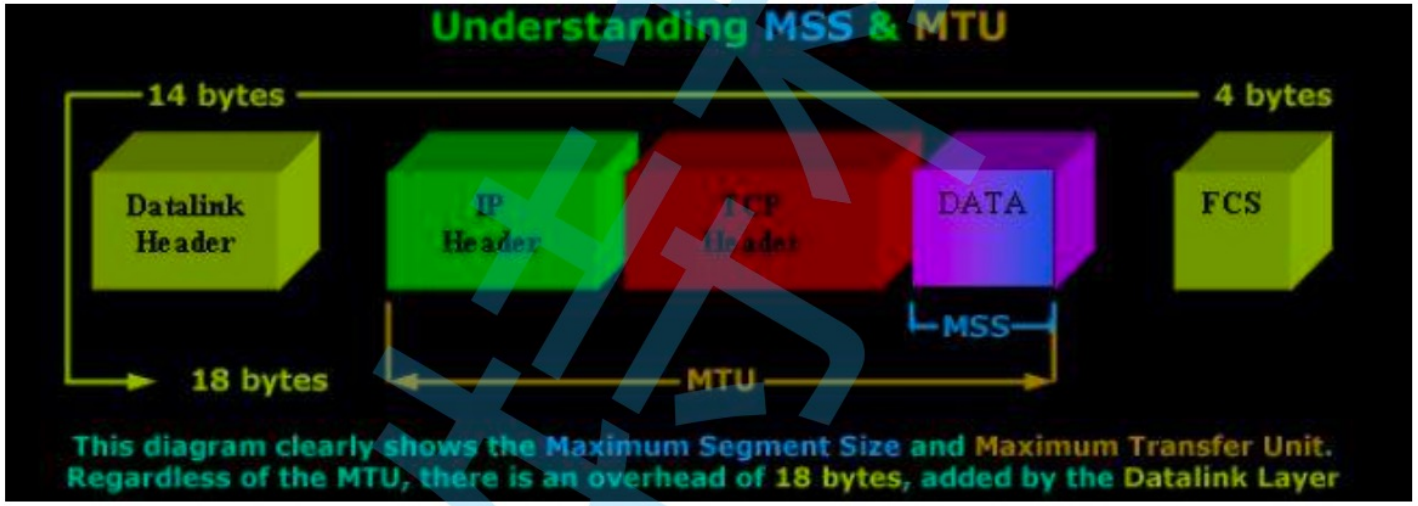
MTU=1500 = IP

IP有效载荷 = 1500-20 = TCP+数据 = 1480

数据 = 1480-TCP报头的长度（20） = 1460

MSS 不能大于 1460

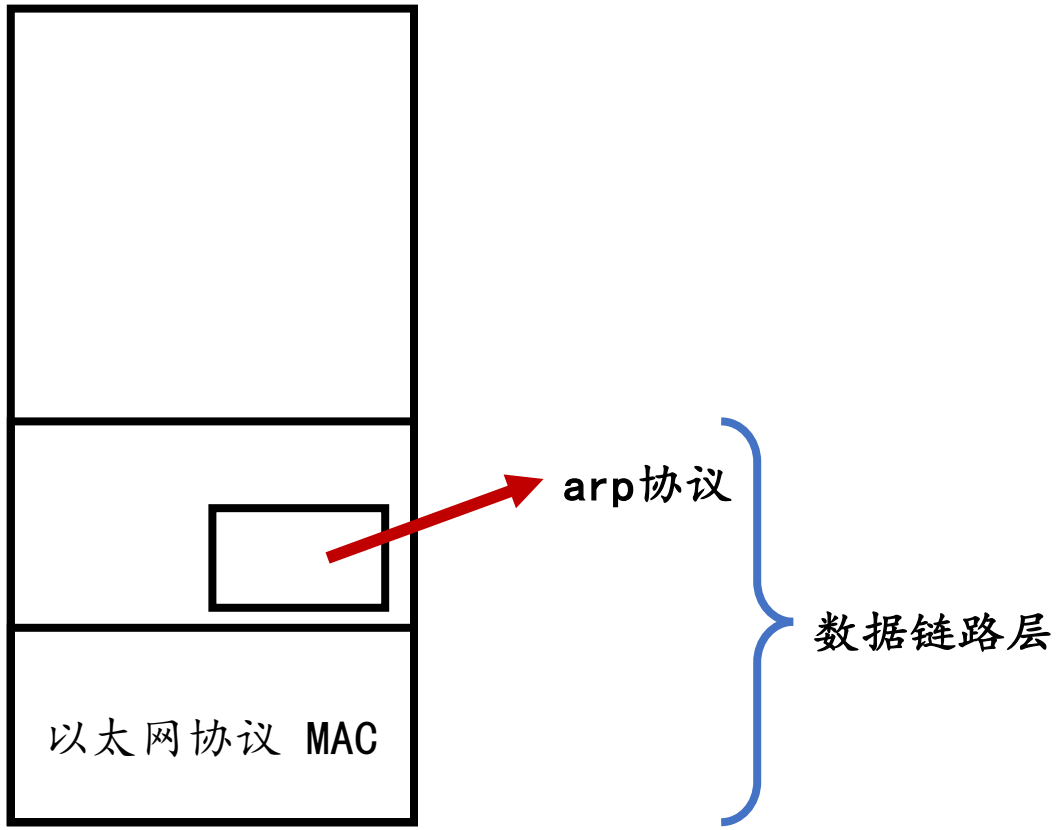
MSS和MTU的关系



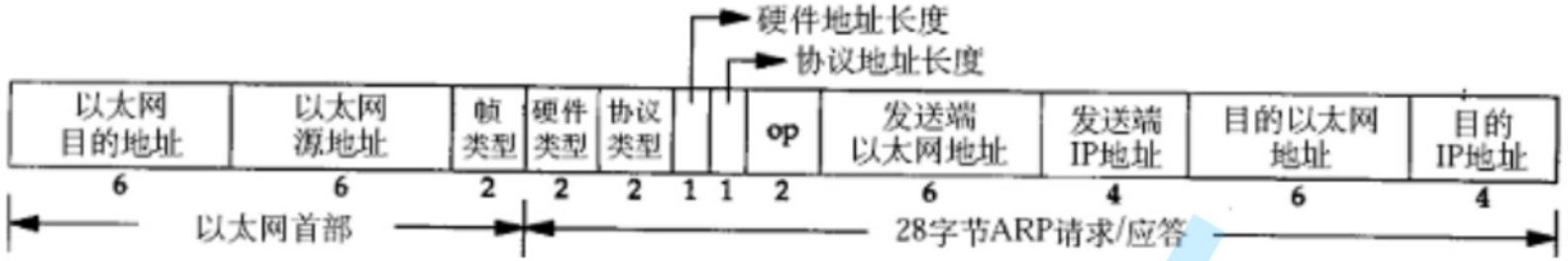
ARP协议

现在的问题是：
我们只知道目标主机的IP地址，但是不知道目标主机的MAC地址
所以在同一个网段，需要一个东西，通过对方的IP地址，得到对方的MAC地址 --- ARP协议（地址解析协议）
这直接决定了，ARP协议是一个局域网协议

mac帧和arp之间的关系



arp的工作过程



1. 先广播 2. 再1v1进行发送 -- mac在局域网中完成
身份证是1234的同学，请告诉我你的名字（广播）
我是1234号，我的名字是张三 -- 这个消息定向发回给我

arp协议

如果是发送arp请求的时候
这里是不知道的
此时填成**全F**

- 硬件类型指链路层网络类型,1为以太网;
- 协议类型指要转换的地址类型,0x0800为IP地址;
- 硬件地址长度对于以太网地址为6字节;
- 协议地址长度对于和IP地址为4字节;
- op字段为1表示ARP请求,op字段为2表示ARP应答。

理解op字段：

1. 任何主机可能之前向目标主机发起过arp请求，注定了，未来会收到对应的arp应答
2. 任何一台主机，也可能被别人发起arp请求
3. 因此，我们收到的arp请求有可能是一个应答也可能是一个请求，所以才会有op字段

1. arp看起来至少需要一个请求和一个应答，那是不是每一次发送数据都要这么干呢？
   不需要！arp请求成功之后，请求方会暂时将MAC和IP的映射关系保存下来，这个是有时间的。

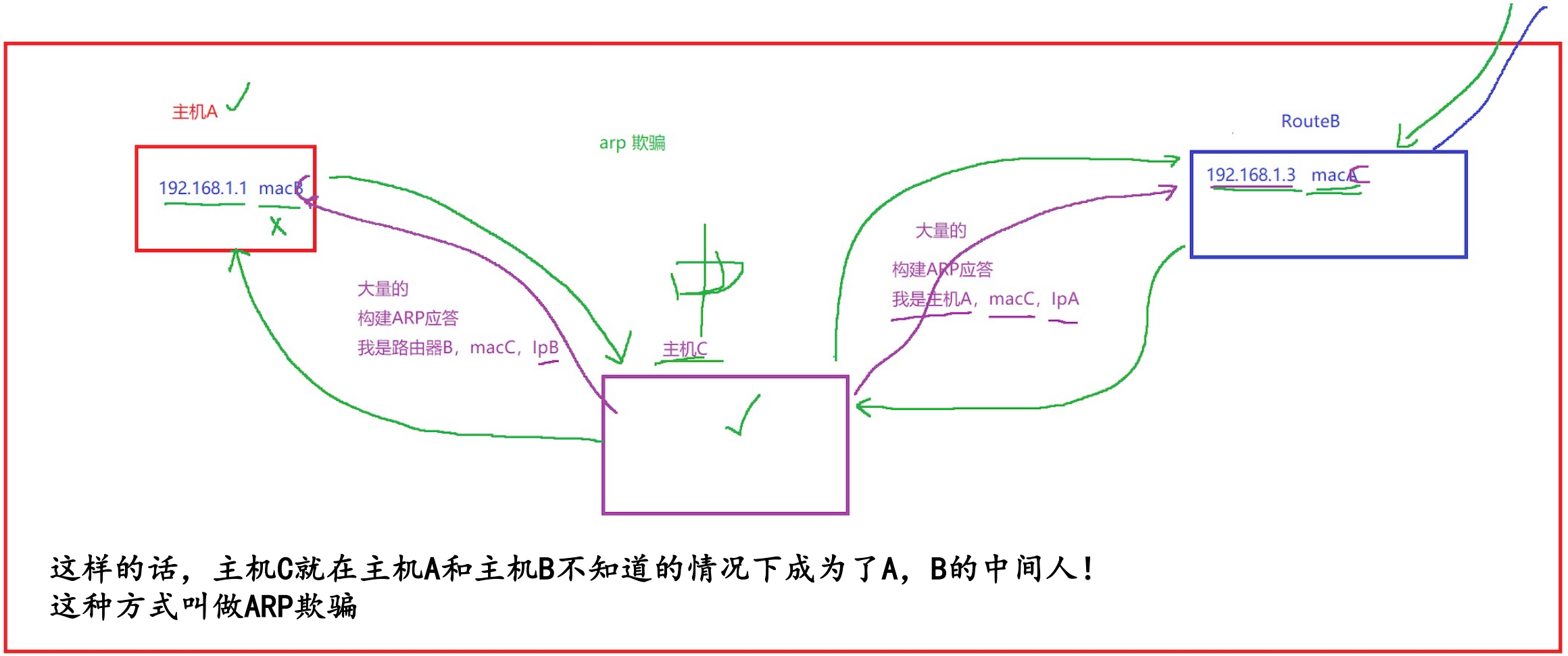
2. 是不是只会在目标最终的子网中进行arp，其他地方会不会也发生arp呢？

3. arp伪装，arp攻击，让自己成为中间人？

如何查看自己本机的arp缓存？

```
(base) [yufc@ALiCentos7:~]$ arp -a
gateway (172.31.31.253) at ee:ff:ff:ff:ff:ff [ether] on eth0
? (169.254.169.254) at <incomplete> on eth0
(base) [yufc@ALiCentos7:~]$
```

想获取一下我处局域网中所有主机的mac和ip地址？

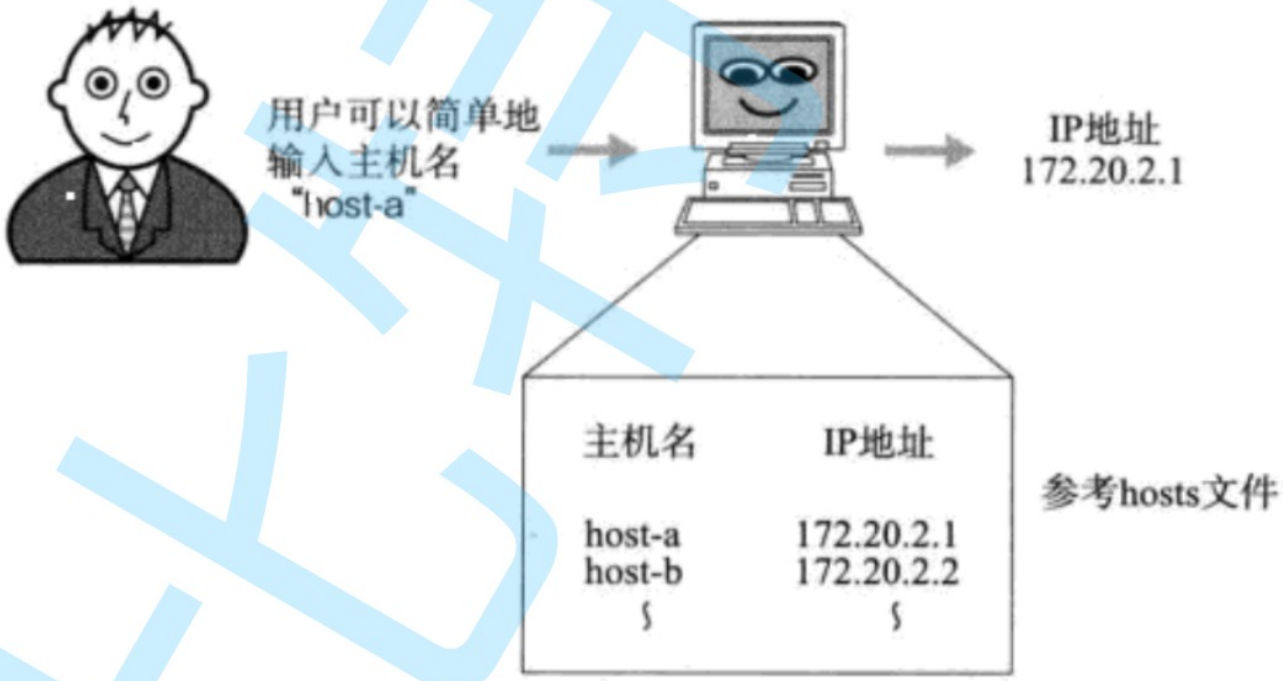


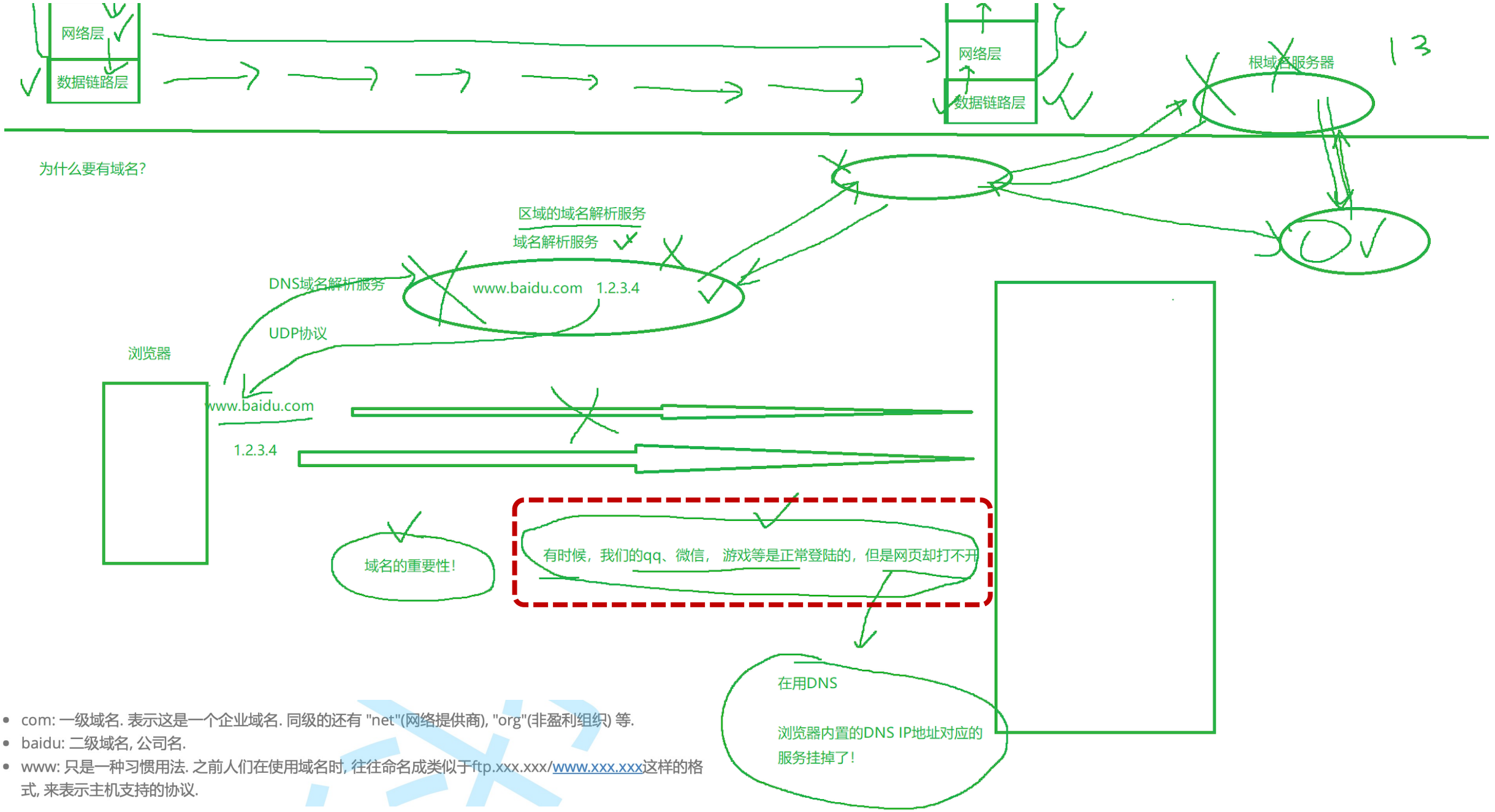
这样的话，主机C就在主机A和主机B不知道的情况下成为了A，B的中间人！
这种方式叫做ARP欺骗

DNS协议

域名和ip地址的映射

TCP/IP中使用IP地址和端口号来确定网络上的一台主机的一个程序. 但是IP地址不方便记忆.
于是人们发明了一种叫主机名的东西, 是一个字符串, 并且使用hosts文件来描述主机名和IP地址的关系.





- com: 一级域名. 表示这是一个企业域名. 同级的还有 "net"(网络提供商), "org"(非盈利组织) 等.
- baidu: 二级域名, 公司名.
- www: 只是一种习惯用法. 之前人们在使用域名时, 往往命名成类似于ftp.xxx.xxx/www.xxx.xxx这样的格式, 来表示主机支持的协议.