**题目： 发送ARP请求**

**姓名:**

**学号：2015**

**班号：HC**

**时间：2017.11.26**

**计算机学院**

**时间:2017/11**

**目 录**

摘 要

[题目： 1](#_Toc499504141)

[1、 目的 1](#_Toc499504142)

[2、要求 1](#_Toc499504143)

[3、相关知识 1](#_Toc499504144)

[4、实现原理及流程图 2](#_Toc499504145)

[5、运行结果与分析 5](#_Toc499504146)

[6、参考文献 11](#_Toc499504147)

# 题目：

发送一个ARP请求报文

# 目的

ARP协议用于完成IP地址与MAC地址之间的转换。熟悉ARP协议对于IP数据包的传输过程具有重要意义。本project主要目的为通过封装和发送ARP帧，了解ARP协议的工作原理与ARP帧的结构。

# 2、要求

根据后面介绍的ARP包结构，编写程序封装并发送ARP包。

以命令行的形式运行: SendArp sourse\_ip source\_mac dest\_ip dest\_mac

其中，SendArp为程序名；sourse\_ip为源IP地址；source\_mac为源MAC地址；dest\_ip为目的IP地址；dest\_mac为目的MAC地址

输出内容：ARP帧的各字段值。包括源IP地址、源MAC地址、目的IP地址、源MAC地址等。

# 3、相关知识

**ARP协议的工作原理：**

（1）每台主机都会根据以往在网络中与其他节点的通信，在自己的ARP缓存区（ARP Cache）中建立一个ARP列表，以表示网络中节点IP地址和MAC地址的对应关系。

【说明】ARP缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用（Windows系统的这个时间为2分钟，而Cisco路由器的这个时间为5分钟），就会被删除，这样可以大大减少ARP缓存表的长度，加快查询速度。

（2）当源节点需要将一个数据包发送到目标节点时，会首先检查自己ARP列表中是否存在该包中所包含的目标节点IP地址对应的MAC地址。如果有，则直接将数据包发送到这个MAC地址节点上；如果没有，就向本地网段发起一个ARP请求的广播包，查询此IP地址目标节点对应的MAC地址。此ARP请求数据包里包括源节点的IP地址、硬件地址，以及目标节点的IP地址。

（3）网络中所有的节点在收到这个ARP请求后，会检查数据包中的目标IP地址是否和自己的IP地址一致。如果不相同就忽略此数据包；如果相同，该节点首先将源端的MAC地址和IP地址的对应表项添加到自己的ARP列表中。如果发现ARP表中已经存在该IP地址所对应的MAC地址表项信息，则将其覆盖，然后给源节点发送一个ARP响应数据包，告诉对方自己是它需要查找的MAC地址节点。

（4）源节点在收到这个ARP响应数据包后，将得到的目标节点的IP地址和MAC地址对应表项添加到自己的ARP列表中，并利用此信息开始数据的传输。如果源节点一直没有收到ARP响应数据包，则表示ARP查询失败。

**ARP协议的工作流程：**

第1步：根据主机A上的[路由表](http://baike.baidu.com/view/149989.htm)内容，IP确定用于访问主机B的转发IP地址是192.168.1.2。然后A主机在自己的本地ARP缓存中检查主机B的匹配MAC地址。

第2步：如果主机A在ARP缓存中没有找到映射，它将询问192.168.1.2的硬件地址，从而将ARP请求帧广播到本地网络上的所有主机。源主机A的IP地址和MAC地址都包括在ARP请求中。本地网络上的每台主机都接收到ARP请求并且检查是否与自己的IP地址匹配。如果主机发现请求的IP地址与自己的IP地址不匹配，它将丢弃ARP请求。

第3步：主机B确定ARP请求中的IP地址与自己的IP地址匹配，则将主机A的IP地址和MAC地址[映射](http://baike.baidu.com/view/21249.htm)添加到本地ARP缓存中。

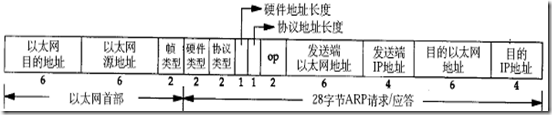
第4步：主机B将包含其MAC地址的ARP回复消息直接发送回主机A。

第5步：当主机A收到从主机B发来的ARP回复消息时，会用主机B的IP和MAC地址映射更新ARP缓存。本机缓存是有[生存期](http://baike.baidu.com/view/159877.htm)的，生存期结束后，将再次重复上面的过程。主机B的MAC地址一旦确定，主机A就能向主机B发送IP通信了。

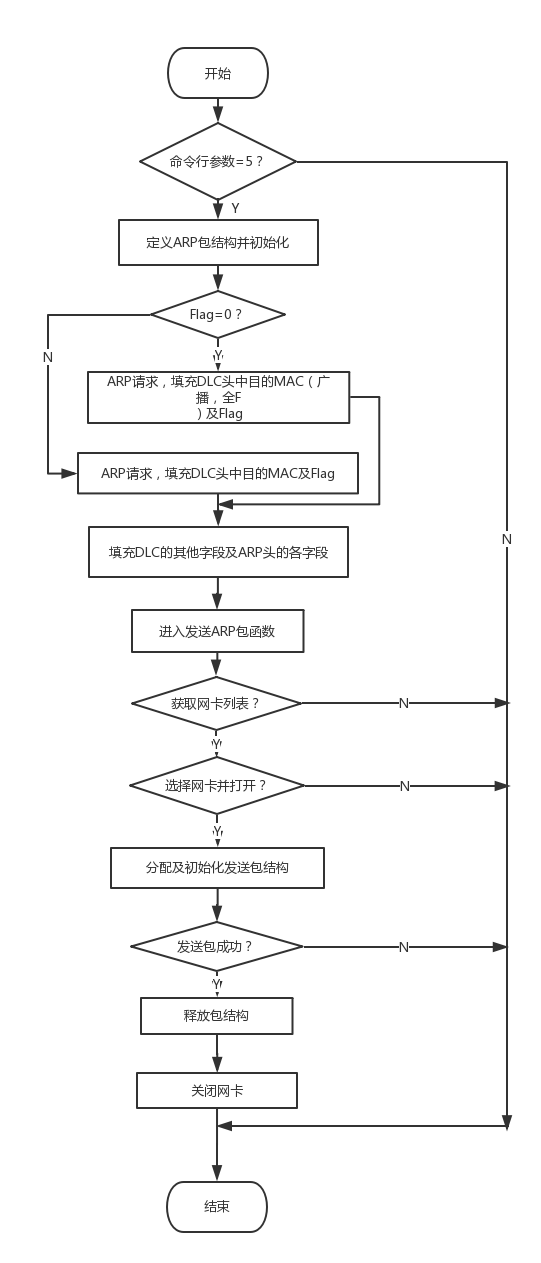
# 4、实现原理及流程图

**ARP的包格式：**

在网络通讯时，源主机的应用程序知道目的主机的IP地址和端口号，却不知道目的主机的硬件地址，而数据包首先是被网卡接收到再去处理上层协议的，如果接收到的数据包的硬件地址与本机不符，则直接丢弃。因此在通讯前必须获得目的主机的硬件地址。ARP协议就起到这个作用。源主机发出ARP请求，询问“IP地址是192.168.0.1的主机的硬件地址是多少”，并将这个请求广播到本地网段（以太网帧首部的硬件地址填FF:FF:FF:FF:FF:FF表示广播），目的主机接收到广播的ARP请求，发现其中的IP地址与本机相符，则发送一个ARP应答数据包给源主机，将自己的硬件地址填写在应答包中。

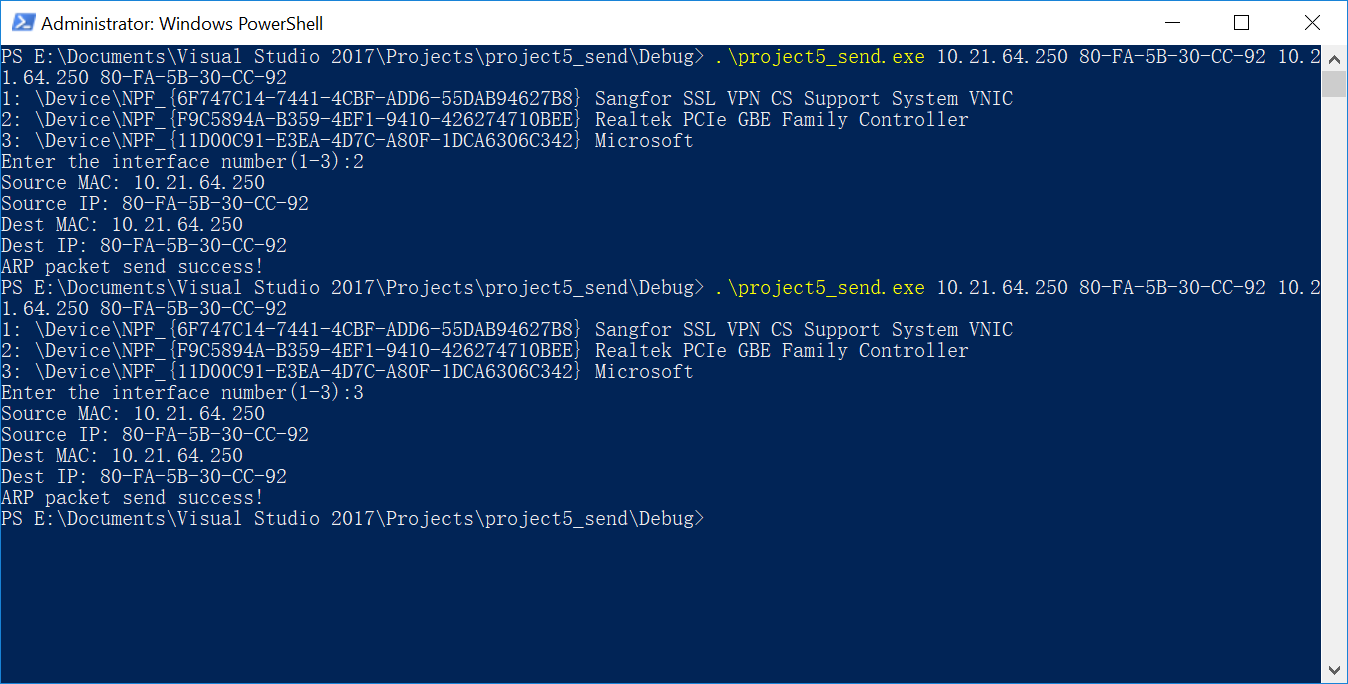
[](http://images.cnblogs.com/cnblogs_com/xmphoenix/201109/201109141550481792.png)

注意到源MAC地址、目的MAC地址在以太网首部和ARP请求中各出现一次，对于链路层为以太网的情况是多余的，但如果链路层是其它类型的网络则有可能是必要的。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，后面两个地址长度对于以太网地址和IP地址分别为6和4（字节），op字段为1表示ARP请求，op字段为2表示ARP应答。



# 5、程序代码(以附件形式,编程环境:VS017)

**运行结果：**

****

# 6、参考文献

老师所给资料与源码

CSDN博客