|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验5 | **实验名称** | ARP |
| **姓名** | 李彦浩 | **学号** | 202100300063 |
| **班级** | 工业软件班 | **成绩** | （空着） |
| 1. **实验目的**   探究ARP(地址解析协议)是如何工作的。ARP是一种基本的胶水协议，用于  加入以太网和IP。 | | | |
| 1. **实验要求**   wireshark：使用wireshark软件工具用于捕获和检查数据包跟踪。  arp：检查和清除计算机上ARP协议使用的缓存。  ipconfig：查看计算机网络接口状态。  netstat/route：查看计算机使用的路由。  Browser：寻找并抓取网页资源。 | | | |
| 1. **实验内容** 2. Network Setup 3. Capture a Trace 4. Inspect the Trace 5. ARP request and reply 6. Details of ARP over Ethernet 7. Explore on your own | | | |
| 1. **实验过程**  Network Setup ARP是用来根据你的计算机想要发包的目标IP地址找到目标机器的MAC地址的。（Address Resolution Protocol，地址解析协议）  一个典型的例子是这个目标IP地址就是将你的计算机连接到互联网的本地路由器或默认网关的。计算机会缓存这些结果，因此ARP并不是时时刻刻都在调用的。  1 Step 1:Capture a Trace(链路追踪) 捕获思路：   1. 诱发计算机向并不知道MAC地址的本地路由器发包 2. 用ARP来获取MAC地址 3. 抓ARP   首先获取一下本机的MAC地址。  ipconfig /all  2  MAC地址：48-89-E7-82-05-FA。  获取计算机访问网络时途径的路由器或者网关。  netstat -r  //或者  route print  3  默认网关：10.27.255.254。  打开wireshark，过滤器：  Arp  4  回到CMD，用  arp -a  展示ARP缓存内容。  arp -d  清除缓存内容。  但这样其实是清不干净的，因为计算机在清除ARP缓存后会立刻重发ARP报文来获取MAC地址，这已经是背景流量级的频率了。  5  随后就可以打开浏览器去访问网页资源了，这样获取默认网关的ARP报文将会被捕获。 Step 2:Inspect the Trace(追踪分析) 先只看直接和本地计算机有关联的ARP报文。  过滤器:  eth.addr == 48:89:E7:82:05:FA  6  找到和默认网关有关的ARP报文。有两种类型：   1. request 2. reply   逐一查看，request中的Info字段应该是“Who has…”开头的。”Who has xx:xx:xx…”中的”xx:xx:xx:…”就是默认网关的IP。  7  查看字段：   1. Hardware/Protocol type：常量，告诉我们硬件是以太网，协议是IP。代表IP向MAC的映射。 2. Hardware/Protocol size：常量。分别设置为6和4。代表MAC地址6个字节，IPV4四个字节。 3. opcode：操作码字段，告诉我们这是个请求帧。 4. Sender MAC/IP && Target MAC/IP：对于请求而言，发送方当然知道自己的MAC和IP地址。但是只知道目标的IP，不知道目标的MAC（不然还要ARP干啥）。它尽量把自己知道的信息天上，不知道的就填全0。（比如目标MAC地址）   8  而对于一个reply帧。在Info字段中就会有诸如“xx.xx.xx.xx is at yy:yy:yy:yy:yy:yy”的信息。这回复了request帧的问题，告知了网关的MAC地址。而对于Sender/Target 的MAC/IP来说，响应方当然都知道，因此全填上。  9 Step 3:ARP request and reply(ARP请求/响应帧) 画出ARP交换报文的过程。  10  请求响应的发送方都用红圈标识出来了。 Step 4:Details of ARP over Ehternet(以太网ARP协议的细节) 查看ARP请求/响应帧，回答以下问题。 Q1:opcode是怎样标识这是一个请求帧还是一个响应帧的？ opcode占两个字节。0x01表示request，0x02表示reply。  11  12 Q2:ARP帧头在request/reply帧中各多大？ request:28B  13  reply:28B  14 Q3:对于未知的目标MAC地址，request中的值为多少？ 00:00:00:00:00:00  15  ARP request是怎么发送给目标计算机的？答案是ARP request本质上是个局域网广播。展开Ethernet帧头，其中的Destination为全FF，意味着广播。因此附近所有计算机都接收到了ARP request报文，但除了目标主机的其他主机在检查目标IP后发现与自己的IP不吻合，因此只有目标主机会对此作出回应。 Q4:说明ARP是上层协议的Ethernet Type值是多少? 0x0806  16 Q5:ARP响应帧是广播帧吗？ 不是。  17  请求帧是广播帧是不知道目标MAC地址，所以广播去找目标主机。但响应帧都知道请求帧是哪个MAC地址发过来的了，直接单播就行了。 Explore on your ownQ1:捕获从其他计算机广播来的ARP请求帧。 这里就需要其他计算机来辅助实验了。我叫我室友一起做的。  因为校园网有端口隔离，因此无论怎样我俩也到不了同一个局域网下，我就开了个热点，然后我们同时加入。  18  再让他把防火墙关了。(当然自己的也要关)  19  这样我ARP设备里就由他电脑了。54是局域网（的默认网关）IP，242是他  20  随后让他arp -d。重新激活一次ARP广播。抓到了他的帧。  21  看一下，确实是广播，然后发送的是242，目标是54。  22 Q2:捕获从自己计算机响应其他计算机的ARP响应帧。 我和室友的两台电脑arp -a后都有对方的设备。  23  24  然后我ping他一下，诱发他发出ARP。  25  这样就捕获他向我发的ARP以及我向他的回复。  26  Q3:免费ARP(Gratuitous ARP)是本机发送并回复给自己的。当连接开启时用来保证自己的IP没有其他主机使用。最大的特点是发送方和目标主机有相同的IP地址，并且在info列中有信息标识这是一帧gratuitous帧。  27  抓到一个。  其中ARP Probe是探查帧，用来探查是否有相同IP的主机。随后的Announcement帧就是确认帧，也就是具有这个IP的主机进行确认。  28  29  Sender和Target的IP一致。 | | | |
| **四．实验心得**  本次我完成ARP实验，这次实验让我对ARP协议有了更深入的理解和认识。  ARP实验让我更清晰地理解了ARP协议的工作原理。ARP（Address Resolution Protocol）是一种用于将网络层IP地址解析为数据链路层MAC地址的协议。在局域网中，ARP协议通过发送广播请求来获取目标主机的MAC地址。通过这次实验，我对ARP协议的工作流程有了更直观的认识，包括如何发送ARP请求、如何接收ARP回复等。  在实验中，我通过抓包工具Wireshark捕获了ARP包，并分析了其中的内容。通过这种方式，我更好地理解了ARP协议的细节和实现方式。  在自主探究中，我尝试和同一局域网的设备交互，我和室友连接到同一个热点下，然后通过Ping和清除缓存的方式找到了对方的设备，并成功捕获到了不同类型的ARP帧，比如他的电脑向我的电脑广播的帧，以及我的电脑对请求的回复。  本次实验为我之后的计算机网络学习打下了坚实的基础。 | | | |