桂林电子科技大学

数学与计算科学学院实验报告（验证性）

**实验室：06205 实验日期：2021年10月16日**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 院（系） | 数学与计算科学学院 | 学号 | 1900710106 | 姓名 | 欧安怡 | 成绩 |  |
| 课程  名称 | 计算机网络C实验 | 实验项目  名 称 | **网络协议分析** | | | 指导  教师 |  |
| 1. **实验目的**   1、熟练Wireshark的使用；  2、分析TCP三次握手的工作原理；分析UDP协议；  3、研究Ping操作与ARP协议的关系；  4、分析DHCP与DNS协议的工作原理。   1. **实验原理**   **1、UDP协议**  UDP协议在IP协议上增加了复用、分用和差错检测功能。UDP的特点：    无连接的。相比于TCP协议，UDP协议在传送数据前不需要建立连接，当然也就没有释放连接。尽最大努力交付的。也就是说UDP协议无法保证数据能够准确的交付到目的主机。也不需要对接收到的UDP报文进行确认。是面向报文的。也就是说UDP协议将应用层传输下来的数据封装在一个UDP包中，不进行拆分或合并。因此，运输层在收到对方的UDP包后，会去掉首部后，将数据原封不动的交给应用进程。没有拥塞控制。因此UDP协议的发送速率不受网络的拥塞度影响。  **2、ARP协议**  IP数据包常通过以太网发送，以太网设备并不识别32位IP地址，它们是以48位以太网地址（MAC地址）传输以太网数据包，设备驱动程序从不检查IP数据报中的目的IP地址。因此，必须把IP目的地址转换成以太网目的地址。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？它就是通过地址解析协议获得的。ARP协议用于将网络中的IP地址解析为目的硬件地址（MAC地址），以保证通信的顺利进行。ARP的工作原理如下：  每台主机都会在自己的ARP高速缓冲区 (ARP Cache)中建立一个 ARP列表，以表示IP地址和MAC地址的对应关系。  当源主机需要将一个数据包发送到目的主机时，会首先检查自己 ARP列表中是否存在该IP地址对应的MAC地址，如果有﹐就直接使用此MAC地址；如果没有，主机就先将目标主机的IP地址与自己的子网掩码进行"与"操作，以判定目标主机与自己是否位于同一网段内。假如目标主机与自己在同一网段内，就向本地网段发起一个ARP请求的广播包，查询此目的主机对应的MAC地址；如果目的主机在一个远程网络上，那么就通过路由器等路由设备转发此ARP请求到远程网络中广播。此ARP请求数据包里包括源主机的IP地址、硬件地址、以及目的主机的IP地址。  源主机和目的主机在一个网络内的情况下：网络中所有的主机收到这个ARP请求后，会检查数据包中的目的IP和自己的IP地址是否一致。如果不相同就不回应，但是该主机仍然会检查自己的ARP高速缓存，如果此请求的源IP地址已经在高速缓存中，那么就用ARP请求帧中的发送端硬件地址对高速缓存中相应的内容进行更新；如果相同，该主机首先将发送端的MAC地址和IP地址添加到自己的ARP列表中，如果ARP表中已经存在该IP的信息，则将其覆盖，然后给源主机发送一个 ARP响应数据包，告诉它需要查找的MAC地址；    **3、DHCP协议**  DHCP，全称是 Dynamic Host Configuration Protocol﹐中文名为动态主机配置协议，它的前身是 BOOTP**(在wireshark中过滤DHCP报文用bootp)** ，它工作在应用层，是一种帮助计算机从指定的DHCP服务器获取它们的配置信息的自举协议。  DHCP使用客户端/服务器模式，请求配置信息的计算机叫做DHCP客户端，而提供信息的叫做DHCP的服务器。DHCP为客户端分配地址的方法有三种：手工配置、自动配置、动态配置。  DHCP最重要的功能就是动态分配。除了IP地址，DHCP分组还为客户端提供其他的配置信息，比如子网掩码。这使得客户端无需用户动手就能自动配置连接网络。  **4、DNS协议**  DNS是域名系统(Domain Name System)的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。域名是由圆点分开一串单词或缩写组成的，每一个域名都对应一个惟一的IP地址，在Internet上域名与IP地址之间是一一对应的，DNS就是进行域名解析的服务器  DNS协议报文结构  DNS协议分成包头和数据两部分。如图1所示，该报文由12字节的首部和4个长度可变的字段组成。      以下会详细介绍个字段：  1. 标识  标识字段由客户程序设置并有服务器返回结果，16位，在对应的query和response报文中有着相同的ID，可以在抓到的包中配对请求和应答报文，提取相关信息，同时也可以根据他们的时间戳大致估计DNS的相应时间。  2. 标志  标志字段长16bit，结构如图2所示：   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | QR 1 | Opcode | AA 1 | TC 1 | RD 1 | RA 1 | Zero 3 | Rcode 4 |     QR：1bits字段，0表示查询报文，1表示响应报文  Opcode：4bits字段，通常值为0（标准查询），其他值为1（反向查询）和2（服务器状态请求）  AA：1bits标志表示授权回答（authoritive answer）,该名字服务器是授权于该领域的  TC：1bits字段，表示可截（truncated），使用UDP时，它表示当应答的总长度超过512字节时，只返回前512个字节  RD：1bits字段，表示期望递归，该比特能在一个查询中设置，并在一个响应中返回，这个标志告诉名字服务器必须处理这个查询，也称为一个递归查询，如果该位为0，且被请求的名字服务器没有一个授权回答，它就返回一个能解答该查询的其他名字服务器列表，这称为迭代查询（期望递归）  RA：1bits字段，表示可用递归，如果名字服务器支持递归查询，则在响应中将该bit置为1（可用递归）  zero：必须为0  rcode：是一个4bit的返回码字段，通常值为0（没有差错）和3（名字差错），名字差错只有从一个授权名字服务器上返回，它表示在查询中指定的域名不存在  随后的4个bit字段说明最后4个变长字段中包含的条目数，对于查询报文，问题数通常是1，其他三项为0，类似的，对于应答报文，回答数至少是1，剩余两项可以使0或非0  5. DNS查询报文中每个查询问题的格式   |  |  | | --- | --- | | 0 16 31查询名 | | | 查询类型 | 查询类 | |  |  |   查询名：要查找的名字  查询类：通常值为1，表示是互联网的地址，也就是IP协议族的地址  查询类型：有很多种查询类型，一般最常用的查询类型是A类型（表示查找域名对应的IP地址）和PTR类型（表示查找IP地址对应的域名）  查询名为要查找的名字，它由一个或者多个标示符序列组成，每个标示符已首字符字节数的计数值来说明该表示符长度，每个名字以0结束，计数字节数必须是0~63之间，该字段无需填充字节，如：gemine.tuc.noao.edu  6. DNS响应报文中的资源记录格式：    域名：记录中资源数据对应的名字，它的格式和查询名字段格式相同  类型：类型说明RR的类型码，类通常为1，指Internet数据  生存时间：客户程序保存该资源记录的秒数  资源数据长度：说明后面资源数据的数量，该数据的格式依赖于类型字段的值，对于类1（A记录）记录数据室4字节的IP地址  资源数据：服务器端返回给客户端的记录数据。   1. **使用仪器，材料**   计算机；接入网络。   1. **实验内容与步骤**   一、开启wireshark捕获数据，访问学校主页，停止捕获，以学校web服务器IP为过滤依据，检索出你的IE与学校服务器间的三次握手信息。  你用到的过滤条件是： ip.dst==202.193.64.75 。  IE客户端选择的ISN是 0 ；服务器端选择的ISN是 1 。  二、两位同学配合，A、B清空各种arp缓存（利用的命令是 arp -d ）。  1、开启wireshark捕获数据，A （172.16.86.107）ping B一次，再A ping B一次，停止捕获。检索出arp和icmp报文，是不是每次ping之前都会发出arp报文，为什么？  2、arp请求报文的目的MAC地址是什么？为什么是这个特殊的地址？  3、你认为arp协议安全吗？为什么？  三、利用ipconfig命令释放当前TCP/IP参数配置，开启wireshark，利用ipconfig命令重新获得TCP/IP参数，停止捕获。  1、DHCP报文在传输层用到什么协议？分析为什么利用该协议？  2、画出DHCP Discover/Offer/Request/ACK 时序图。  3、客户端、服务端用到的端口号分别是多少？Discover的源IP和目的IP是什么？分析为什么会取该值。  4、试分析Transaction-ID的作用。  5、在哪个DHCP报文中，DHCP服务器提供了你的IP地址？  6、你的DHCP服务器的IP地址是多少？  7、DHCP release报文的作用是什么？如果该报文丢失将会发生什么？   1. **实验过程原始记录（数据，图表，计算等）**       **删除前：**    **删除后：**    每次ping之前不一定都会发出arp报文，先在本地arp缓存表里查找目标主机ip地址和mac信息查找成功不发出arp请求，不成功则发出arp请求    MAC地址：**ff:ff:ff:ff:ff:ff,因为是广播地址。**  3. 不安全，ARP协议是建立在信任局域网内所有结点的基础上的，它很高效，但却不安全。它是无状态  的协议，不会检查自己是否发过请求包，也不管（其实也不知道）是否是合法的应答，只要收到目标MAC  是自己的ARP reply包或arp广播包（包括ARP request和ARP reply），都会接受并缓存。这就为ARP  欺骗提供了可能，恶意节点可以发布虚假的ARP报文从而影响网内结点的通信，甚至可以做“中间人”。  三·      1.udp协议  2.    3.  客户端、服务端用到的端口号67.68,获取ip的机器为客户端，dhcp服务器为服务端  4. Transaction ID 是随机产生的，DNS服务器返回dns应答信息时，使用的 Transaction ID 必须和  你询问时使用的一致，才会被你的机器接受。  **6.**  7. 作用是释放使用的地址，让 DHCP 服务器收回该地址，可以分配给其它设备使用。 该  报文使用已获取的地址作为源地址，以 255.255.255.255 为广播地址 进行发送。DHCP rel  ease消息的目的是释放租用的ip地址，DHCP服务器没有发出客户端DHCP请求的接收确认。  如果release消息丢失，那么会回收ip。  **四．**         1. **实验结果分析或总结**   本次实验学到了Wireshark的使用，TCP三次握手的工作原理，以及DHCP与DNS协议的工作  原理 | | | | | | | |
|  | | | | | | | |