计算机网络

实验报告

（2022学年秋季学期）

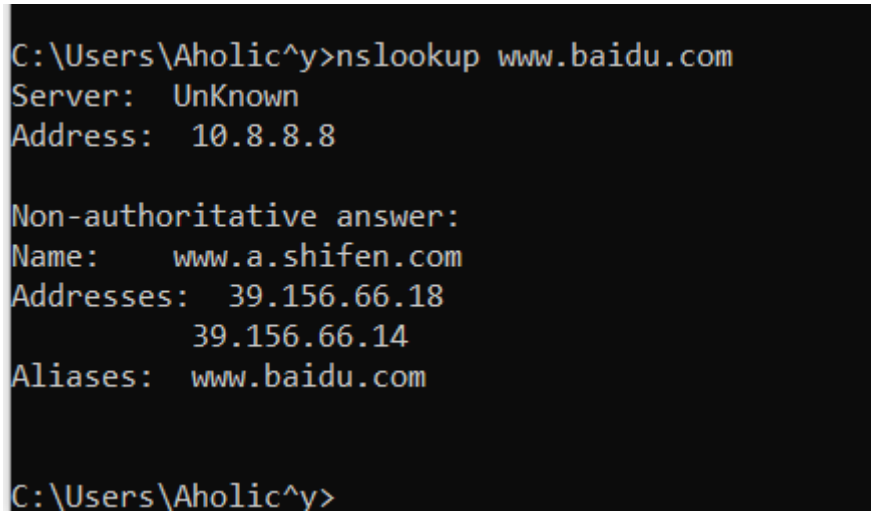
教学班级	计科二班	专业（方向）	计算机科学与技术
学号	20337263	姓名	俞泽斌

一、 实验题目

1、学会在客户端使用nslookup命令进行域名解析

2、通过协议分析软件掌握DNS协议的报文格式

二、 实验内容



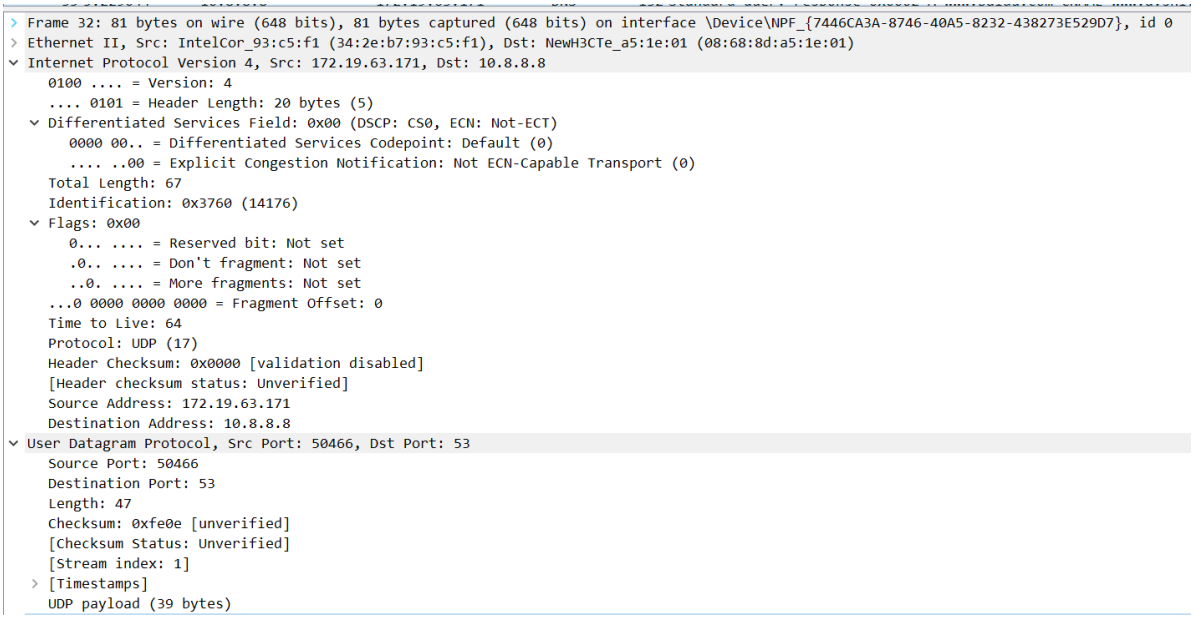
首先是打开wireshark开始抓包，然后在命令行中输入nslookup www.baidu.com的命令，得到如上反馈

打开wireshark的过滤器，使用DNS作为过滤条件，得到下面几帧

No.	Time	Source	Destination	Protocol	Length	Info
32	5.166055	172.19.63.171	10.8.8.8	DNS	81	Standard query 0x0001 PTR 8.8.8.10.in-addr.arpa
33	5.198218	10.8.8.8	172.19.63.171	DNS	140	Standard query response 0x0001 No such name PTR 8.8.8.10.in-addr.arpa SOA localhost
34	5.199755	172.19.63.171	10.8.8.8	DNS	73	Standard query 0x0002 A www.baidu.com
35	5.229044	10.8.8.8	172.19.63.171	DNS	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 39.156.66.18 A 39.156.66.14
36	5.229670	172.19.63.171	10.8.8.8	DNS	73	Standard query 0x0003 AAAA www.baidu.com
37	5.263350	10.8.8.8	172.19.63.171	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com

前两帧是通过反向查询获得本地DNS服务器的地址，之后的两帧是通过正向查询获得查询域名对应的IP地址，接下来的两帧也是一样的操作，不过对应的是ipv6的地址，接下来对报文进行具体分析

第一帧是172.19.63.171发送给本地DNS服务器10.8.8.8来反向查询取得报文



直接看应用层的报文，

首部字段名	字段值	含义
version	4	代表ip的规格版本为4
header length	20	标头长度
total length	67	总共的长度
identification	0x3760	识别码

然后可以看到source Address 和Destination Address分别为172.19.63.171和10.8.8.8，代表请求从网络开始传到本地的DNS服务器

同时Source port 和Destination Port为50466和53,53是DNS服务器的标准服务端口

最后一行看到使用协议为UDP

第二帧其实本地DNS服务器并没有返回具体的域名，但并不影响

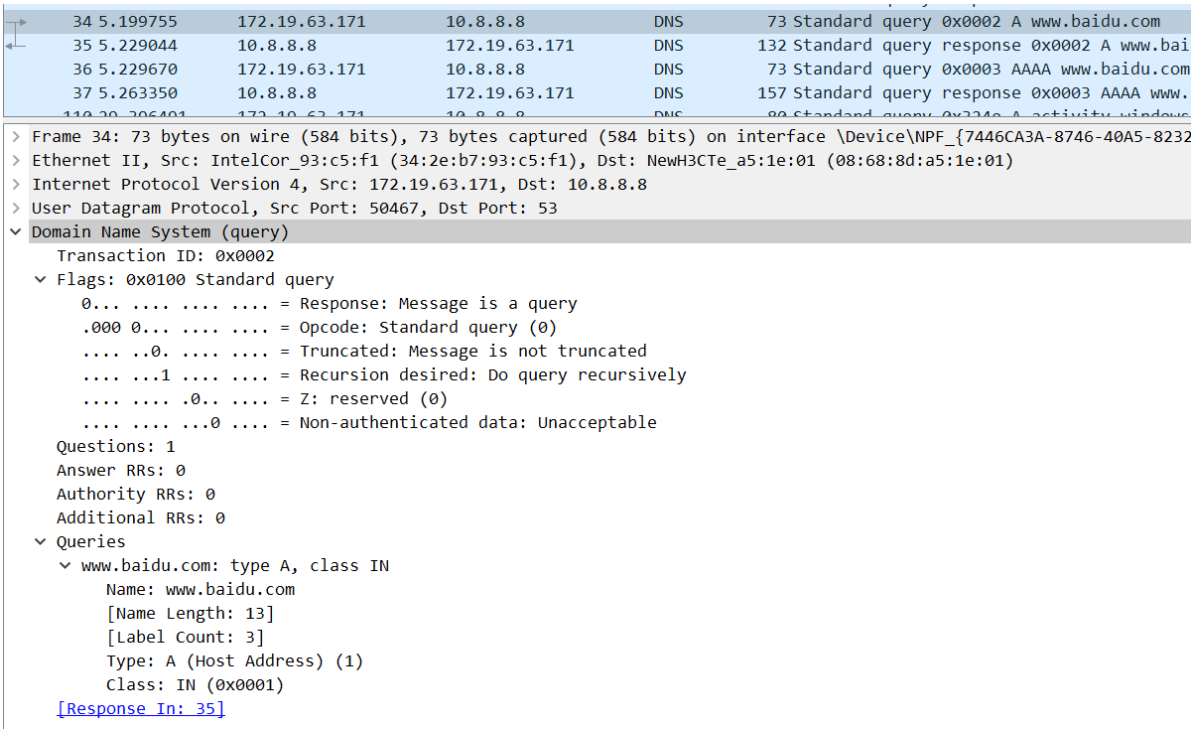
```
> Internet Protocol Version 4, Src: 10.8.8.8, Dst: 172.19.63.171
> User Datagram Protocol, Src Port: 53, Dst Port: 50466
v Domain Name System (response)
    Transaction ID: 0x0001
  v Flags: 0x8583 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v 8.8.8.10.in-addr.arpa: type PTR, class IN
        Name: 8.8.8.10.in-addr.arpa
        [Name Length: 21]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
  v Authoritative nameservers
    > 10.in-addr.arpa: type SOA, class IN, mname localhost
    [Request In: 32]
    [Time: 0.032163000 seconds]
```

首先可以看到Flags下不断地在进行循环请求，然是最后的reply code为no such name，说明本地的DNS服务器并没有给请求来返回具体的域名地址。所以在最后返回的位置上可以看到Name为8.8.8.10.in-addr.arpa，然后具体展开Authoritative nameserver（权威DNS）

```
v Authoritative nameservers
  v 10.in-addr.arpa: type SOA, class IN, mname localhost
      Name: 10.in-addr.arpa
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 10800 (3 hours)
      Data length: 47
      Primary name server: localhost
      Responsible authority's mailbox: nobody.invalid
      Serial Number: 1
      Refresh Interval: 3600 (1 hour)
      Retry Interval: 1200 (20 minutes)
      Expire limit: 604800 (7 days)
      Minimum TTL: 10800 (3 hours)
  [Request In: 32]
  [Time: 0.032163000 seconds]
```

可以看到在primary name server 的页面也注明了localhost

第三帧是客户端发给本地DNS服务器的请求www.baidu.com的域名地址的请求报文

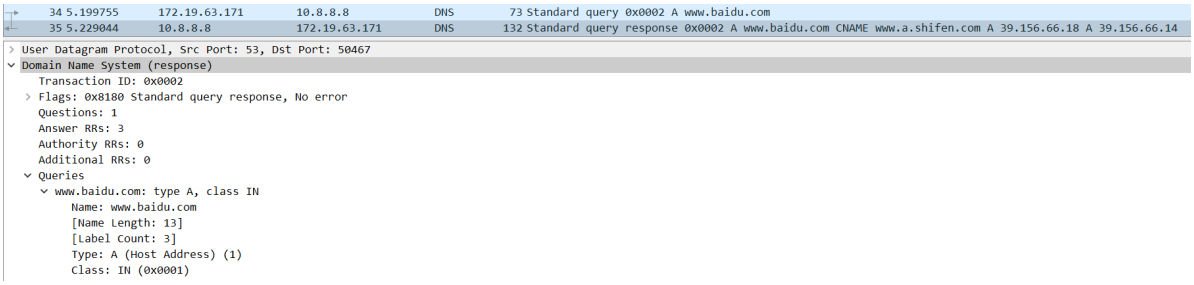


可以看到发出请求的是172.19.63.171，即本地客户端，接受请求的为10.8.8.8，为本地的DNS服务器

首部字段名	字段值	含义
Questions	1	代表查询的问题有多少个
Answer RRs（回答）	0	代表返回的回答
Authority RRs（授权）	0	代表返回的授权信息
Additional RRs（额外信息）	0	代表返回的额外信息

然后在报文的Queries下可以看到对于www.baidu.com的请求资源记录

第四帧是本地DNS服务器对客户端返回的www.baidu.com的域名和ip地址



```
Answers
  www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 163 (2 minutes, 43 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
  www.a.shifen.com: type A, class IN, addr 39.156.66.18
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 259 (4 minutes, 19 seconds)
      Data length: 4
      Address: 39.156.66.18
  www.a.shifen.com: type A, class IN, addr 39.156.66.14
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 259 (4 minutes, 19 seconds)
      Data length: 4
      Address: 39.156.66.14
  [Request In: 34]
  [Time: 0.029289000 seconds]
```

首部字段名	字段值	含义
Questions	1	代表查询的问题
Answer RRs（回答）	3	代表返回的回答信息
Authority RRs（授权）	0	代表返回的授权信息
Additional RRs（额外信息）	0	代表返回的额外信息

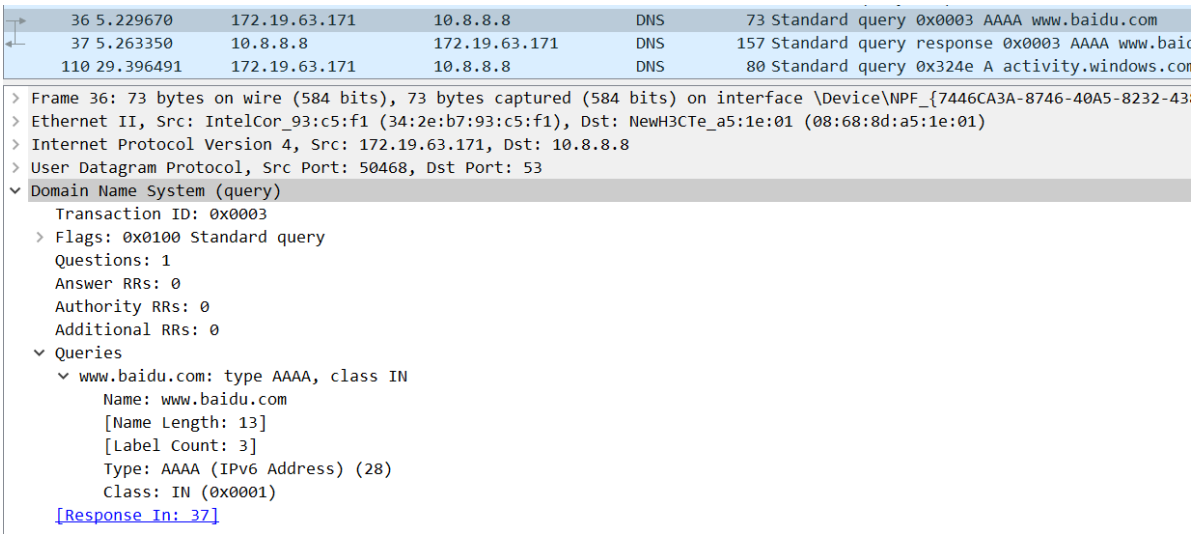
可以看到在Queries下还是那个问题，但是此时在下面的报文中出现了answer

answer分为了三个部分，分别是www.baidu.com和www.a.shifen.com(39.156.66.18)以及www.a.shifen.com(39.156.66.14)

后面两个都是www.baidu.com的初始名字，也是对应的真正域名，具体直接挑baidu.com来进行分析

首部字段名	字段值	含义
Name	www.baidu.com	网址
Type	A	查询类型，A代表IPv4地址
Class	IN	类域
Time to live	163	存活时间
Data length	15	数据长度
Address	39.156.66.14/39.156.66.18	IP地址
CNAME	www.a.shifen.com	对应真正域名

第5帧是ipv6条件下客户端发给本地DNS服务器的请求www.baidu.com的域名地址的请求报文



可以看到此时的Queries中type属性变成了AAAA，表示此时的为IPV6地址，其余没有大的变化

第6帧也是本地DNS服务器对客户端返回的www.baidu.com的域名和ip地址

```
Queries
  www.baidu.com: type AAAA, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
Answers
  www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 163 (2 minutes, 43 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
Authoritative nameservers
  a.shifen.com: type SOA, class IN, mname ns1.a.shifen.com
      Name: a.shifen.com
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 66 (1 minute, 6 seconds)
      Data length: 45
      Primary name server: ns1.a.shifen.com
      Responsible authority's mailbox: baidu_dns_master.baidu.com
      Serial Number: 2209160033
      Refresh Interval: 5 (5 seconds)
      Retry Interval: 5 (5 seconds)
      Expire limit: 2592000 (30 days)
      Minimum TTL: 3600 (1 hour)
  [Request In: 36]
  [Time: 0.033680000 seconds]
```

此时其实与第四帧相比区别不是很大，开始的Queries下只有Type的区别，之后的Answer下也一样，但ipv6多了个Authoritative nameservers，并且将a.shifen.com，也就是baidu.com的原始名字拿来做了具体的分析，具体的区别也就是type上的差别了

步骤4：再次访问www.baidu.com时，没有DNS请求

因为此时本地的DNS已经有了baidu.com的DNS缓存，所以不需要继续向本地DNS服务器来

步骤五：此时有DNS请求

```
2681 225.204679    172.26.49.213     10.8.8.8          DNS      78 Standard query 0x4bbd A portal.sysu.edu.cn
2682 225.221863    10.8.8.8          172.26.49.213     DNS     119 Standard query response 0x4bbd A portal.sysu.edu.cn CNAME portal.adc.sysu.edu.cn A 202.116.64.123
```

我这里访问的是portal.sysu.edu.cn，可以看到此时客户端也会向本地的DNS服务器来请求域名的解析，返回的报文中也展示了这个网址的具体ip地址。

步骤6 使用ipconfig/displaydns的命令来显示本机缓冲区所包含的DNS解析内容

这里因为太多，所以只截取部分

```
C:\Users\Aholic^y>ipconfig/displaydns

Windows IP Configuration

    optimizationguide-pa.googleapis.com
    ----------------------------------------
    Record Name . . . . . : optimizationguide-pa.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 40
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 172.217.163.42


    static-ecst.licdn.com
    ----------------------------------------
    Record Name . . . . . : static-ecst.licdn.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 876
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : cs1404.wpc.epsiloncdn.net
```

```
    sslvpn.sysu.edu.cn
    ----------------------------------------
    Record Name . . . . . : sslvpn.sysu.edu.cn
    Record Type . . . . . : 1
    Time To Live  . . . . : 288
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 202.116.81.14
```

步骤7，使用ipconfig/flushdns清楚本机的DNS缓存记录

```
C:\Users\Aholic^y>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Aholic^y>
```

成功清除缓存内容

步骤8，关闭浏览器再打开，访问刚才打开过的网站，观察是否有DNS请求

```
10894 1012.298228  172.26.49.213     10.8.8.8          DNS      78 Standard query 0x4b47 A portal.sysu.edu.cn
10895 1012.310341  10.8.8.8          172.26.49.213     DNS     119 Standard query response 0x4b47 A portal.sysu.edu.cn CNAME portal.adc.sysu.edu.cn A 202.116.64.123
```

发现确实有DNS请求，因为本地的DNS缓存被清除，此时需要客户端重新向本地的DNS服务器来请求域名的解析，才能访问具体的地址

三、实验思考

1、DNS协议中的资源记录RR包含哪些内容

回答字段、授权字段、附加信息字段使用RR的相同格式，RR包含

域名：记录资源数据对应的名字

类型：说明RR的类型码

类域：与问题记录的查询类型字段相同

生存时间：客户程序保留该资源记录的秒数

数据长度：说明资源数据的数量

数据

2、DNS处理返回需查找的域名还可能返回哪些内容

还可以如果查找到了具体的域名，还会返回查询类型，类域，生存时间，数据长度

如果没有查找到，就会在reply里输出no such name，并开启下一次握手

3、反复试验，判断一个域名是否可以对应多个ip地址？域名与IP地址之间是不是一一对应的关系？

并不是一一对应的关系，一个域名可以对应多个ip地址，比如我们访问baidu.com的时候，

```
Answers
  www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 163 (2 minutes, 43 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
  www.a.shifen.com: type A, class IN, addr 39.156.66.18
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 259 (4 minutes, 19 seconds)
      Data length: 4
      Address: 39.156.66.18
  www.a.shifen.com: type A, class IN, addr 39.156.66.14
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 259 (4 minutes, 19 seconds)
      Data length: 4
      Address: 39.156.66.14
  [Request In: 34]
  [Time: 0.029289000 seconds]
```

可以看到baidu.com的原名 www.a.shifen.com就有两个ip地址39.156.66.18和39.156.66.14，说明域名和ip不是一一对应的关系

4、若实验中无法进行DNS解析，请写出导致问题的原因以及解决办法

（1）网站故障，当发现打开某些网站会出现dns错误，但又有些大站打开一切正常，这种情况由于网站域名服务器故障。只需要换一个网站来进行实验即可

（2）网络故障，没网络打开网页，修复只需要修复网络问题即可

5、DNS协议何时用UDP？何时用TCP？

首先了解一下两者的概念

TCP：面向连接的协议，提供可靠的数据传输，一般服务质量要求比较高的情况，使用这个协议。

UDP：用户数据报协议，是一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。

但是虽然TCP协议中植入了各种安全保障功能，但是在实际执行的过程中会占用大量的系统开销，无疑使速度受到严重的影响。

反观UDP由于排除了信息可靠传递机制，将安全和排序等功能移交给上层应用来完成，极大降低了执行时间，使速度得到了保证。

所以DNS在进行区域传输（即辅助DNS服务器启动时，它需要与主DNS服务器通信，并加载数据信息）的时候使用TCP协议，其它时候则使用UDP协议。