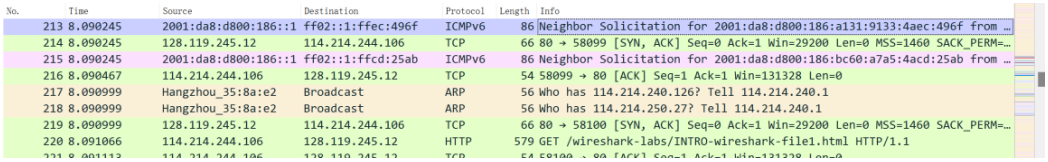
Getting Started 实验报告

PB20000296 郑滕飞

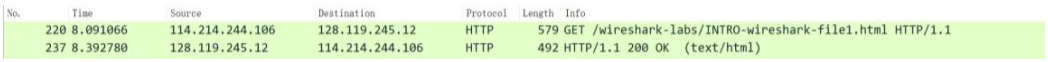
1、



No.	Time	Source	Destination	Protocol	Length	Info
213	8.090245	2001:da8:d800:186::1	ff02::1:ffec:496f	ICMPv6	86	Neighbor Solicitation for 2001:da8:d800:186:a131:9133:4aec:496f from …
214	8.090245	128.119.245.12	114.214.244.106	TCP	66	80 → 58099 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=…
215	8.090245	2001:da8:d800:186::1	ff02::1:ffcd:25ab	ICMPv6	86	Neighbor Solicitation for 2001:da8:d800:186:bc60:a7a5:4acd:25ab from …
216	8.090467	114.214.244.106	128.119.245.12	TCP	54	58099 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
217	8.090999	Hangzhou_35:8a:e2	Broadcast	ARP	56	Who has 114.214.240.126? Tell 114.214.240.1
218	8.090999	Hangzhou_35:8a:e2	Broadcast	ARP	56	Who has 114.214.250.27? Tell 114.214.240.1
219	8.090999	128.119.245.12	114.214.244.106	TCP	66	80 → 58100 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=…
220	8.091066	114.214.244.106	128.119.245.12	HTTP	579	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

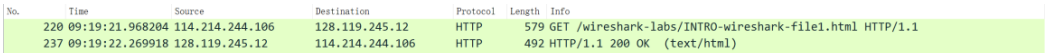
如图，ARP、TCP、HTTP、ICMPv6 等。

2、



No.	Time	Source	Destination	Protocol	Length	Info
220	8.091066	114.214.244.106	128.119.245.12	HTTP	579	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
237	8.392780	128.119.245.12	114.214.244.106	HTTP	492	HTTP/1.1 200 OK (text/html)

Time of day:



No.	Time	Source	Destination	Protocol	Length	Info
220	09:19:21.968204	114.214.244.106	128.119.245.12	HTTP	579	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
237	09:19:22.269918	128.119.245.12	114.214.244.106	HTTP	492	HTTP/1.1 200 OK (text/html)

如图，时间间隔为 0.30 秒左右。

3、

如上图, 目标网站 IP 地址为 128.119.245.12, 我的电脑的 IP 地址为 114.214.244.106。

4、

GET:

```
No.     Time              Source                Destination           Protocol Length Info
    220 09:19:21.968204   114.214.244.106       128.119.245.12        HTTP     579    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 220: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Chongqin_52:3d:90 (5c:3a:45:52:3d:90), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.244.106, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58099, Dst Port: 80, Seq: 1, Ack: 1, Len: 525
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/
537.36 Edg/105.0.1343.33\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 237]
    [Next request in frame: 244]
```

OK:

```
No.     Time              Source                Destination           Protocol Length Info
    237 09:19:22.269918   128.119.245.12        114.214.244.106       HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 237: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: Chongqin_52:3d:90 (5c:3a:45:52:3d:90)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.244.106
Transmission Control Protocol, Src Port: 80, Dst Port: 58099, Seq: 1, Ack: 526, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 12 Sep 2022 01:19:21 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 11 Sep 2022 05:59:01 GMT\r\n
    ETag: "51-5e86079cbdf11"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.301714000 seconds]
    [Request in frame: 220]
    [Next request in frame: 244]
    [Next response in frame: 266]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

HTTP 实验报告

PB20000296 郑滕飞

1、

```
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
```

```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
```

我的浏览器与服务器均是 1.1 版本的 HTTP 协议。

2、

```
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5\r\n
```

根据 GET 请求中的信息，接收简体中文、英文(英式、美式)、繁体中文。

3、

```
Internet Protocol Version 4, Src: 114.214.244.106, Dst: 128.119.245.12
```

根据 GET 请求中的信息，我的电脑的 IP 地址为 114.214.244.106，目标网站 IP 地址为 128.119.245.12。

4、

```
HTTP/1.1 200 OK\r\n
```

接收的状态码为 200，即 OK。

5、

```
    HTTP/1.1 200 OK\r\n
    Date: Fri, 16 Sep 2022 07:24:12 GMT\r\n
```

根据回复中的信息，最后一次修改是在 9 月 16 日。

6、

```
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
```

根据回复中的信息，内容的字节数为 81。

7、

```
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/
537.36 Edg/105.0.1343.33\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5\r\n
    \r\n
```

如客户端可识别的数据编码类型。

8、

```
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/
537.36 Edg/105.0.1343.33\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,zh-TW;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 541]
    [Next request in frame: 860]
```

如图，第一次请求时并没有 If-Modified-Since。

9、

```
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
```

从文件长度可以看出，第一次请求时服务器回复了文件内容。

10、

```
   If-None-Match: "173-5e8c50f0c0eb2"\r\n
   If-Modified-Since: Fri, 16 Sep 2022 05:59:02 GMT\r\n
```

第二次请求时出现了 If-Modified-Since，后面跟着的时间是服务器上一次回复时 Last-Modified 的时间。

11、

```
pertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Fri, 16 Sep 2022 08:24:33 GM
```

第二次回复的状态码是 304，Not Modified，并没有回复文件内容。这是由于在短期第二次请求时，浏览器已经有了缓存，只需知道没有被修改就可以直接展示缓存的文件。

12、

```
No.     Time              Source                Destination           Protocol Length Info
   1038 18:24:48.973488    114.214.220.115       128.119.245.12        HTTP     578    GET /wireshark-labs/HTTP-wireshark-
file3.html HTTP/1.1
Frame 1038: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
```

发送了一个 HTTP GET 请求，分组号是 1038。

13、

```
No.     Time              Source                Destination           Protocol Length Info
   1054 18:24:49.229080    128.119.245.12        114.214.220.115       HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 1054: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
```

分组号为 1054。

14、

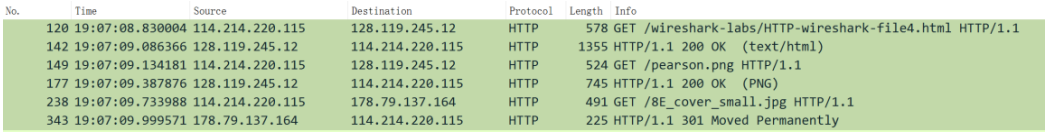
如上图，回复状态码仍然是 200，OK。

15、

```
Transmission Control Protocol, Src Port: 80, Dst Port: 63123, Seq: 4381, Ack: 525, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #1051(1460), #1052(1460), #1053(1460), #1054(481)]
Hypertext Transfer Protocol
```

需要 4 个 TCP 段。

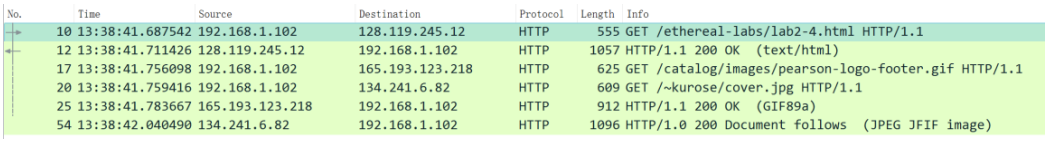
16、



No.	Time	Source	Destination	Protocol	Length	Info
120	19:07:08.830004	114.214.220.115	128.119.245.12	HTTP	578	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
142	19:07:09.086366	128.119.245.12	114.214.220.115	HTTP	1355	HTTP/1.1 200 OK (text/html)
149	19:07:09.134181	114.214.220.115	128.119.245.12	HTTP	524	GET /pearson.png HTTP/1.1
177	19:07:09.387876	128.119.245.12	114.214.220.115	HTTP	745	HTTP/1.1 200 OK (PNG)
238	19:07:09.733988	114.214.220.115	178.79.137.164	HTTP	491	GET /8E_cover_small.jpg HTTP/1.1
343	19:07:09.999571	178.79.137.164	114.214.220.115	HTTP	225	HTTP/1.1 301 Moved Permanently

发送了三次请求，分别对 128.119.245.12 与 178.79.137.164。

17、



No.	Time	Source	Destination	Protocol	Length	Info
10	13:38:41.687542	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1
12	13:38:41.711426	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)
17	13:38:41.756098	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
20	13:38:41.759416	192.168.1.102	134.241.6.82	HTTP	609	GET /~kurose/cover.jpg HTTP/1.1
25	13:38:41.783667	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)
54	13:38:42.040490	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)

上方所展示的图片是无法在现实网络连接中运行 wireshark 时实验设计者准备的现成结果，从中根据 GET 的先后顺序可以看出对两个图片的加载是并行进行的。
(然而自己做了几次，情况都如 16 题的图，收到了 301 且看不出串并)

18、

```
771 HTTP/1.1 401 Unauthorized  (text/html)
```

第一次的回复是 401 Unauthorized。

19、

```
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTMl
```

增加了 Authorization 的字段。

DNS 实验报告

PB20000296 郑滕飞

1、

```
PS D:\Desktop> nslookup ustc.edu.cn
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

名称:    ustc.edu.cn
Addresses:  2001:da8:d800:642::248
          202.38.64.246
```

如图，科大服务器的 IP 地址为 202.38.64.246。

2、

```
PS D:\Desktop> nslookup uni-goettingen.de
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    uni-goettingen.de
Address:  134.76.18.234
```

上图中非权威应答即为哥廷根大学的服务器。

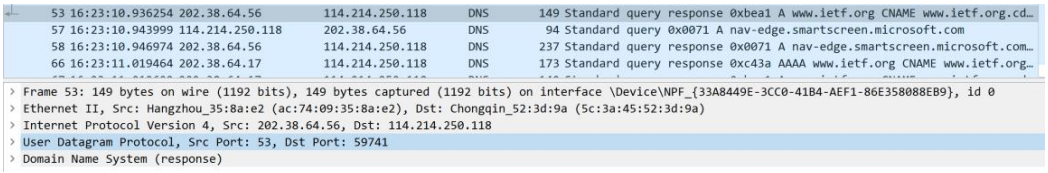
3、

```
PS D:\Desktop> nslookup mail.yahoo.com mx.ustc.edu.cn
服务器:  UnKnown
Address:  2001:da8:d800::56

非权威应答:
名称:    edge.gycpi.b.yahoodns.net
Addresses:  2001:4998:18:800::4003
          2001:4998:18:800::4002
          69.147.88.8
          69.147.88.7
Aliases:  mail.yahoo.com
```

由于外网问题，此处使用科大的服务器，可发现雅虎邮箱的 IPv4 与 IPv6 地址。

4、



由选中的部分可发现其通过 UDP 进行传输。

5、

```
Source                Destination           Protocol Length Info
114.214.250.118       202.38.64.56          DNS      72     Standard query 0xbea1 A www.ietf.org
```

```
Source                Destination           Protocol Length Info
202.38.64.56          114.214.250.118       DNS      149    Standard query response 0xbea1 A
```

请求的目标与响应的来源均为 202.38.64.56，具体见下题。

6、

```
   DNS 服务器  . . . . . . . . . . . . : 202.38.64.56
                                         202.38.64.17
```

利用 ipconfig 可发现，此 IP 即为本地 DNS 服务器。

7、

```
Info
Standard query 0xbea1 A www.ietf.org
```

```
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
```

它的 Type 是 A，且不包含答复。

8、

```
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

包含三个答复，先获取了对应的主名称，再找到了主名称的两个 IP 地址。

9、

```
55 16:23:10.937744 2001:da8:d800:186:c… 2606:4700::6810:2c63 TCP   86 52585 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
56 16:23:10.938534 2001:da8:d800:186:c… 2606:4700::6810:2c63 TCP   86 52586 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
```

此处目标地址的 IPv6 形式后 8 位是 6810:2c63，转换为 IPv4 形式即为 104.16.44.99，也即之前 DNS 答复的 IP 地址。

10、

```
No.  Time            Source                Destination           Protocol Length Info
 63  16:23:11.002465 2001:da8:d800:186:c… 2606:4700::6810:2c63 HTTP      553 GET / HTTP/1.1
 75  16:23:11.077094 2606:4700::6810:2c63 2001:da8:d800:186:c… HTTP      377 HTTP/1.1 301 Moved Permanently
```

```
     66 16:23:11.019464 202.38.64.17    114.214.250.118  DNS   173 Standard query response 0xc43a AAAA www.ietf.org CNAME www.ietf.org…
     67 16:23:11.019692 202.38.64.17    114.214.250.118  DNS   149 Standard query response 0xbea1 A www.ietf.org CNAME www.ietf.org.cd…
    206 16:23:11.445986 114.214.250.118 202.38.64.56     DNS    78 Standard query 0xc0ac A analytics.ietf.org
    207 16:23:11.446222 114.214.250.118 202.38.64.56     DNS    78 Standard query 0x7c23 AAAA analytics.ietf.org
```

根据 HTTP 请求与 DNS 请求的序号可以推断之后获取图片并不需要新的 DNS 请求(通过实验文档中的示例包也能看出)。

11-12、

```
No.     Time               Source              Destination         Protocol Length Info
     80 17:19:46.469640    114.214.250.118     202.38.64.56        DNS      71     Standard query 0x0003 AAAA www.mit.edu
```

```
No.     Time               Source              Destination         Protocol Length Info
     81 17:19:46.472487    202.38.64.56        114.214.250.118     DNS      203    Standard query response 0x0003 AAAA
```

请求的目标与响应的来源均为本地 DNS 服务器。

13、

```
Info
Standard query 0x0003 AAAA www.mit.edu
```

```
Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
```

它的 Type 是 AAAA，不包含答复。

14、

```
Answers
    www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:140e:6:a83::255e
    e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:140e:6:ab3::255e
```

四个答复，两个为主名称，两个为 IP 地址。

15、

```
No.     Time               Source              Destination         Protocol Length Info
     37 16:23:09.427545    114.214.250.118     202.38.64.56        DNS      72     Standard query 0xbea1 A www.ietf.org
Frame 37: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Chongqin_52:3d:9a (5c:3a:45:52:3d:9a), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.250.118, Dst: 202.38.64.56
User Datagram Protocol, Src Port: 59741, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xbea1
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 53]
No.     Time               Source              Destination         Protocol Length Info
     53 16:23:10.936254    202.38.64.56        114.214.250.118     DNS      149    Standard query response 0xbea1 A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
Frame 53: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: Chongqin_52:3d:9a (5c:3a:45:52:3d:9a)
Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.250.118
User Datagram Protocol, Src Port: 53, Dst Port: 59741
Domain Name System (response)
    Transaction ID: 0xbea1
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
        www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 37]
    [Time: 1.508709000 seconds]
```

16、

```
No.     Time               Source               Destination          Protocol Length Info
     77 17:23:00.834136    114.214.250.118      202.38.64.56         DNS      71     Standard query 0x0002 NS www.mit.edu
```

```
No.     Time               Source               Destination          Protocol Length Info
     78 17:23:00.899423    202.38.64.56         114.214.250.118      DNS      225    Standard query response 0x0002 NS
```

请求的目标仍为本地 DNS 服务器。

17、

```
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
    www.mit.edu: type NS, class IN
```

它的 Type 是 NS，且不包含答复。

18、

```
Answers
    www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
```

答复包含了两个名字服务器，且并没有包含 IP。

19、

```
No.     Time               Source               Destination          Protocol Length Info
     37 16:23:09.427545    114.214.250.118      202.38.64.56         DNS      72     Standard query 0xbea1 A www.ietf.org
Frame 37: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Chongqin_52:3d:9a (5c:3a:45:52:3d:9a), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.250.118, Dst: 202.38.64.56
User Datagram Protocol, Src Port: 59741, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xbea1
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 53]
No.     Time               Source               Destination          Protocol Length Info
     53 16:23:10.936254    202.38.64.56         114.214.250.118      DNS      149    Standard query response 0xbea1 A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
Frame 53: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: Chongqin_52:3d:9a (5c:3a:45:52:3d:9a)
Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.250.118
User Datagram Protocol, Src Port: 53, Dst Port: 59741
Domain Name System (response)
    Transaction ID: 0xbea1
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
        www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 37]
    [Time: 1.508709000 seconds]
```

20、

```
PS D:\Desktop\3上-计算机网络\实验\3> nslookup www.aiit.or.kr dns.opendns.com
服务器:  dns.opendns.com
Address:  208.67.220.220

非权威应答:
名称:    www.aiit.or.kr
Address:  58.229.6.225
```

由于外网问题，此处使用了查到的开放 DNS 服务器，可发现请求的目标不再是本地 DNS 服务器。

21、

```
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
    www.aiit.or.kr: type A, class IN
[Response In: 51]
```

它的 Type 是 A，且不包含答复。

22、

```
Answers
    www.aiit.or.kr: type A, class IN, addr 58.229.6.225
```

包含了一个答复，直接给出了 IPv4 地址。

23、

```
No.     Time           Source                Destination           Protocol Length Info
     43 18:37:16.211298    114.214.208.54        208.67.220.220        DNS      74     Standard query 0x0002 A www.aiit.or.kr
Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Chongqin_52:3d:ff (5c:3a:45:52:3d:ff), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.208.54, Dst: 208.67.220.220
User Datagram Protocol, Src Port: 61092, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0002
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.aiit.or.kr: type A, class IN
    [Response In: 51]
No.     Time           Source                Destination           Protocol Length Info
     51 18:37:16.703997    208.67.220.220        114.214.208.54        DNS      90     Standard query response 0x0002 A
www.aiit.or.kr A 58.229.6.225
Frame 51: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{33A8449E-3CC0-41B4-
AEF1-86E358088EB9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: Chongqin_52:3d:ff (5c:3a:45:52:3d:ff)
Internet Protocol Version 4, Src: 208.67.220.220, Dst: 114.214.208.54
User Datagram Protocol, Src Port: 53, Dst Port: 61092
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.aiit.or.kr: type A, class IN
    Answers
        www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    [Request In: 43]
    [Time: 0.492699000 seconds]
```

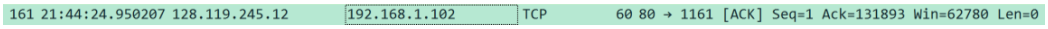
TCP 实验报告

PB20000296 郑滕飞

1、

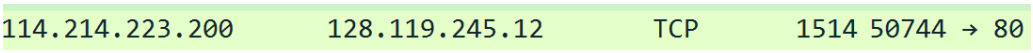
从 POST 中可以看出客服计算机 IP 地址 192.168.1.102，端口号 1161。

2、



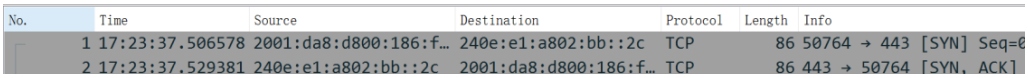
IP 地址为 128.119.245.12，端口号 80.

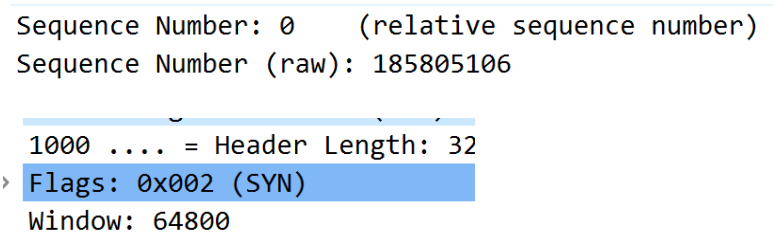
3、



我的电脑 IP 地址为 114.214.223.200，端口号 50744。

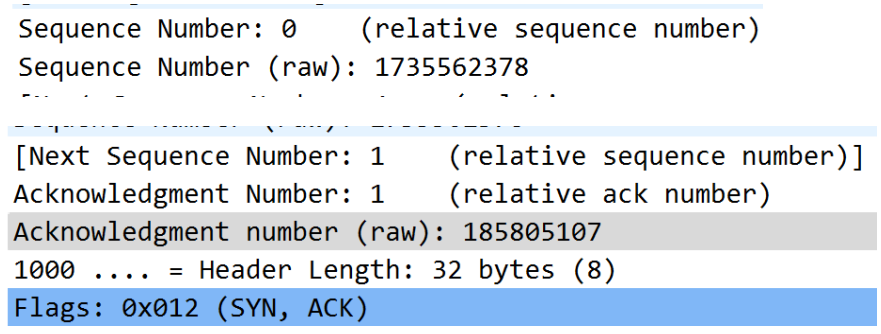
4、





序列号绝对值为 185805106，相对为 0，通过 Flags 字段确定为 SYN。

5、



序列号为 1735562378，相对为 0，其中确认编号绝对值为 185805107，相对为 1，即请求连接端发来的序列号增加 1，无论是相对值还是绝对值都是如此。依然通过 Flags 字段确认为 SYN ACK。

6、

```
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 2803700399
[Next Sequence Number: 760    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 3317517564
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 513]
```

```
20  f5 0c c6 38 00 50 a7 1d  12 af c5 bd 4c fc 50 18   ··8·P··  ····L·P·
30  02 01 eb c2 00 00 50 4f  53 54 20 2f 77 69 72 65   ····PO ST /wire
40  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
50  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
60  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
70  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
80  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
```

序列号相对为 1。

7、

```
 76 17:23:39.752255 114.214.223.200  128.119.245.12   TCP    813 50744 → 80 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=759
 77 17:23:39.752708 114.214.223.200  128.119.245.12   TCP   1514 50744 → 80 [ACK] Seq=760 Ack=1 Win=513 Len=1460
 78 17:23:39.752708 114.214.223.200  128.119.245.12   TCP   1514 50744 → 80 [ACK] Seq=2220 Ack=1 Win=513 Len=1460
 79 17:23:39.752708 114.214.223.200  128.119.245.12   TCP   1514 50744 → 80 [ACK] Seq=3680 Ack=1 Win=513 Len=1460
 80 17:23:39.752708 114.214.223.200  128.119.245.12   TCP   1514 50744 → 80 [ACK] Seq=5140 Ack=1 Win=513 Len=1460
 81 17:23:39.752708 114.214.223.200  128.119.245.12   TCP   1514 50744 → 80 [ACK] Seq=6600 Ack=1 Win=513 Len=1460
```

```
 94 17:23:39.999970 128.119.245.12   114.214.223.200  TCP     60 80 → 50744 [ACK] Seq=1 Ack=760 Win=240 Len=0
 95 17:23:40.000083 114.214.223.200  128.119.245.12   TCP   1514 50744 → 80 [ACK] Seq=13900 Ack=1 Win=513 Len=1460
 96 17:23:40.000856 128.119.245.12   114.214.223.200  TCP     60 80 → 50744 [ACK] Seq=1 Ack=2220 Win=263 Len=0
 97 17:23:40.000856 128.119.245.12   114.214.223.200  TCP     60 80 → 50744 [ACK] Seq=1 Ack=3680 Win=286 Len=0
 98 17:23:40.000856 128.119.245.12   114.214.223.200  TCP     60 80 → 50744 [ACK] Seq=1 Ack=5140 Win=309 Len=0
 99 17:23:40.000856 128.119.245.12   114.214.223.200  TCP     60 80 → 50744 [ACK] Seq=1 Ack=6600 Win=332 Len=0
100 17:23:40.000856 128.119.245.12   114.214.223.200  TCP     60 80 → 50744 [ACK] Seq=1 Ack=8060 Win=355 Len=0
```

编号	序列号	发送时间	ACK 到达时间	Sample RTT	Estimated RTT
1	1	39.752255	39.999970	247.7ms	247.70ms
2	760	39.752708	40.000856	248.1ms	247.75ms
3	2220	39.752708	40.000856	248.1ms	247.79ms
4	3680	39.752708	40.000856	248.1ms	247.83ms
5	5140	39.752708	40.000856	248.1ms	247.87ms
6	6600	39.752708	40.000856	248.1ms	247.89ms

*由于在同一分钟，发送与接收只记录秒数

8、

如第 7 题图，长度除第一个为 759 外均为 1460。

9、

如第 7 题图，最小的 window size 为 240，传输不会因为缓冲区空间不足而终止。

10、

观察可发现序列号单调递增，因此不存在重传的分段。

11、

```
101 17:23:40.000856 128.119.245.12      114.214.223.200     TCP       60 80 → 50744 [ACK] Seq=1 Ack=9520 Win=377 Len=0

115 17:23:40.003041 128.119.245.12      114.214.223.200     TCP       60 80 → 50744 [ACK] Seq=1 Ack=10980 Win=400 Len=0
```

类似第 7 题图，通过 ACK 序号可发现，一般是确认的数据长度为 1460，而编号 102 与 115 的包中没有其他 ACK，可发现确认的长度为$4 \times 1460 = 5640$。

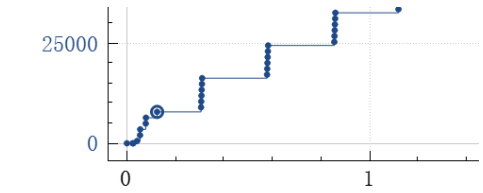
12、

```
76 17:23:39.752255 114.214.223.200     128.119.245.12      TCP       813 50744 → 80 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=759

310 17:23:40.774582 128.119.245.12      114.214.223.200     TCP       60 80 → 50744 [ACK] Seq=1 Ack=153081 Win=2066 Len=0
```

考虑第一个发送的分段与最后一个 ACK，大小可发现为 153080 字节，而总时间为 1.022 秒，于是大约每秒 149785 字节。

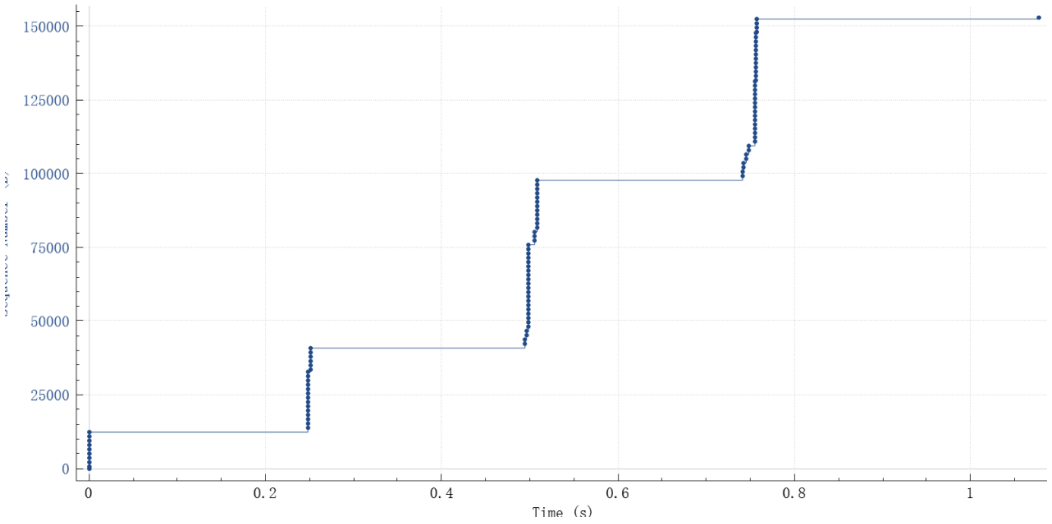
13、



击选取分组 13 (0.1242s len 1147 seq 7866 ack 1 win

可以看出慢启动阶段从开始到 0.1242 秒左右，此后开始拥塞避免。此处拥塞避免的机制不是如书上一样每个 RTT 增加一个 MSS，而是隔一段时间发送/接收六个包，直到最后也没有再增加。

14、



从自己捕获的包中看不出慢启动(或许开始部分已经是慢启动的过程)，而之后进入拥塞控制阶段，可以明显看到 MSS 分几次增长，直到传输结束。

IP 实验报告

PB20000296 郑滕飞

1、

```
> Frame 151: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Chongqin_52:3d:82 (5c:3a:45:52:3d:82), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
v Internet Protocol Version 4, Src: 210.45.118.132, Dst: 121.194.11.73
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x23de (9182)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
```

我的电脑的 IP 地址是 210.45.118.132

2.

```
Protocol: ICMP (1)
```

高层协议字段为 1。

3.

```
    .... 0101 = Header Length: 20 bytes (5)
>   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
```

头部 20 字节，总长度 56 字节，有效载荷 36 字节。

4.

```
> Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
```

此报文没有被分片。

5.

```
Identification: 0x23de (9182)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xca29 [validation disabled]
```

```
Identification: 0x23df (9183)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0xc829 [validation disabled]
```

一直在改变的有 Identification 字段、Time to live 字段与 Header Checksum 字段。

6.

上方的三个字段必须变化，而包相同时的 flag，源与目的地址、总长度等不变。

7.

Identification 每次增加 1。

8.

```
Identification: 0x23e0 (9184)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 254
```

Identification 为 9184，Time to Live 为 254。

9.

```
Identification: 0x23ef (9199)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 254
```

Identification 变化，唯一标识。
Time to Live 不变，经过第一跳比初始减少 1。

10.

```
> Flags: 0x20, More fragments
...0 0000 0000 0000 = Fragment Offset: 0
```

138	12:51:35.686	210.45.118.132	121.194.11.73	IPv4	1506 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2421) [Reassembled
139	12:51:35.686	210.45.118.132	121.194.11.73	ICMP	526 Echo (ping) request id=0x0001, seq=5226/27156, ttl=255 (reply in 1

被分为了两片。

11.

```
v Flags: 0x20, More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
```

Total Length: 1500

Flags 看出分片，更多分片看出该片为第一片，长度 1500 字节。

12.

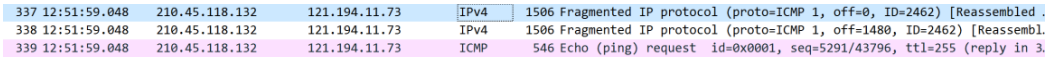
```
v Flags: 0x00
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0101 1100 1000 = Fragment Offset: 1480
```

Fragment Offset 看出不为第一片，更多分片看出没有其他分片。

13.

总长度、Flags 中的字段、Fragment Offset 与 Header Checksum 均改变了(Identification 相同)。

14.



337	12:51:59.048	210.45.118.132	121.194.11.73	IPv4	1506 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2462) [Reassembled
338	12:51:59.048	210.45.118.132	121.194.11.73	IPv4	1506 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2462) [Reassembl
339	12:51:59.048	210.45.118.132	121.194.11.73	ICMP	546 Echo (ping) request id=0x0001, seq=5291/43796, ttl=255 (reply in 3

分为了三片。

15.

同 13，总长度、Flags 中的字段、Fragment Offset 与 Header Checksum 均有改变。

ARP 实验报告

PB20000296 郑滕飞

1、

```
Ethernet II, Src: Chongqin_52:3d:7b (5c:3a:45:52:3d:7b), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
```

以太网地址为 5c:3a:45:52:3d:7b。

2、

如上题图，地址 ac:74:09:35:8a:e2，是中转的交换机或路由器地址。

3、

```
Type: IPv4 (0x0800)
```

0x0800，为 IPv4。

4、

```
·t·5··\: ER={··E·
·7w·@···  ··r····w
···V·P··  ·····ZP·
·····GE T /wires
```

54 字节。

5、

```
32 12:26:56.133308 Hangzhou_59:13:41    Chongqin_52:3d:7b    0x0800    1514 IPv4
```

同第二题答案。

6、

同第一题答案，是我的计算机的 MAC 地址。

7、

```
Type: IPv4 (0x0800)
```

0x0800，为 IPv4。

8、

```
\:ER={·t ·Y·A··E·
····@·!· q··w··r·
···P·V··  ·Z····P·
··"k··HT TP/1.1 2
00 OK··D ate: Sun
```

66 字节。

9、

```
C:\Users\32575>arp -a

接口: 114.214.215.171 --- 0x8
  Internet 地址         物理地址              类型
  114.214.212.1         ac-74-09-35-8a-e2     动态
  114.214.215.255       ff-ff-ff-ff-ff-ff     静态
  114.214.240.1         ac-74-09-35-8a-e2     动态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.83.1 --- 0x9
  Internet 地址         物理地址              类型
  192.168.83.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.189.1 --- 0x10
  Internet 地址         物理地址              类型
  192.168.189.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

```
接口: 172.25.160.1 --- 0x38
  Internet 地址         物理地址              类型
  172.25.175.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

如图所示。

10、

```
> Ethernet II, Src: Chongqin_52:3d:a2 (5c:3a:45:52:3d:a2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

源同第一题，为我的计算机的以太网地址，目的地址为广播 ff:ff:ff:ff。、

11、

```
Type: ARP (0x0806)
```

类型 0x0806，为 ARP。

12、

```
Opcode: request (1)
Sender MAC address: Chongqin_52:3d:a2 (5c:3a:45:52:3d:a2)
Sender IP address: 114.214.215.171
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 114.214.212.1
```

```
ff ff ff ff ff ff 5c 3a  45 52 3d a2 08 06 00 01    ·····\: ER=·····
08 00 06 04 00 01 5c 3a  45 52 3d a2 72 d6 d7 ab    ······\: ER=·r···
00 00 00 00 00 00 72 d6  d4 01                      ·····r·  ··
```

a. 20 字节。

b. 0x0001

c. 包含。

d. 注意到 Who has 信息，问题即为目标 IP 地址。

13、

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
    Sender IP address: 114.214.212.1
    Target MAC address: Chongqin_52:3d:a2 (5c:3a:45:52:3d:a2)
    Target IP address: 114.214.215.171
```

```
0000  5c 3a 45 52 3d a2 ac 74  09 35 8a e2 08 06 00 01   \:ER=··t ·5·····
0010  08 00 06 04 00 02 ac 74  09 35 8a e2 72 d6 d4 01   ·······t ·5··r···
0020  5c 3a 45 52 3d a2 72 d6  d7 ab 00 00 00 00 00 00   \:ER=·r· ········
0030  00 00 00 00 00 00 00 00                           ········
```

a. 20 字节。

b. 0x0002。

c. 以太网地址在发送者的 MAC 地址中。

14、

```
> Destination: Chongqin_52:3d:a2 (5c:3a:45:52:3d:a2)
> Source: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
```

源地址为需要的 MAC 地址，目标地址为我的计算机的 MAC 地址。

15、

子网中不包含此 IP 地址。

EX 1、

会导致在 MAC 地址中无法获取到对应的 IP 地址。

[实际测试中使用-s 命令似乎会自动更正]

EX 2、

··· / SYSTEM / CurrentSet / Services / Tcpip / Parameters /

ArpCacheLife

Article • 09/10/2008 • 2 minutes to read

Note

This value does not affect ARP cache table entries that are added manually. TCP/IP does not remove manual entries.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

注册表中的此项有，但根据微软的信息现在已经没了，默认应为 120s。