南 开 大 学

计算机网络

1811507 文静静

2020 年 11 月 12 日

Web 服务器配置，HTTP 报文捕获

一、实验要求

（1）搭建 Web 服务器（自由选择系统），并制作简单 Web 页面，包含简单文本信息（至少包含专业、学号、姓名）。

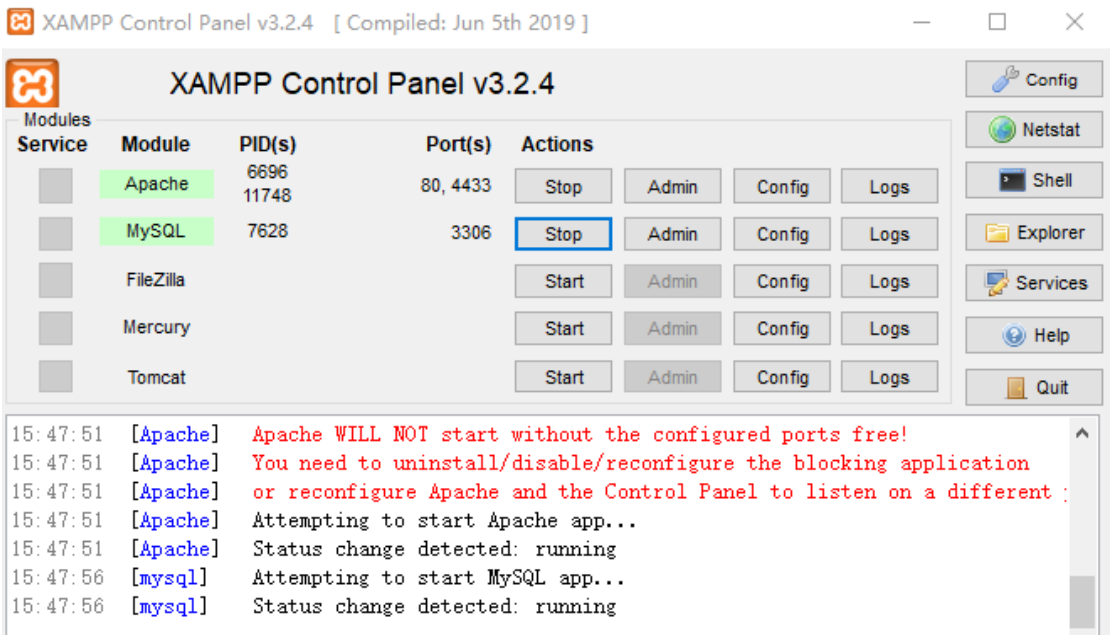
（2）通过浏览器获取自己编写的 Web 页面，使用 Wireshark 捕获与 Web 服务器的交互过程，并进行简单分析说明。

（3）提交实验报告。

二、实验内容以及结果

1．搭建 web 服务器

下载 xampp 并配置好 Apache 和 MySql，并开启 Apache 和 MySql 就搭建好了 web 服务器。



2．编写简单网页

网页如图：

专业：计算机科学与技术

学号：1811507

姓名：文静静

3．通过 wireshark 捕获与 web 服务器的交互过程

打开 xampp，通过服务器访问网页

打开 wireshark，捕获数据报

三次握手过程：

```
TCP        56 63601 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
TCP        56 80 → 63601 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
TCP        44 63601 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
```

第一次握手：客户端将 TCP 报文标志位 SYN 置为 1，随机产生一个序号值 seq=J（如图 J=0），保存在 TCP 首部的序列号字段里，指明客户端打算连接的服务器的端口，并将该数据包发送给服务器端，发送完毕后，客户端进入 SYN_SENT 状态，等待服务器端确认。

第二次握手：服务器端收到数据包后由标志位 SYN=1 知道客户端请求建立连接，服务器端将 TCP 报文标志位 SYN 和 ACK 都置为 1，ack=J+1，随机产生一个序号值 seq=K，并将该数据包发送给客户端以确认连接请求，服务器端进入 SYN_RCVD 状态。

第三次握手：客户端收到确认后，检查 ack 是否为 J+1，ACK 是否为 1，如果正确则将标志位 ACK 置为 1，ack=K+1，并将该数据包发送给服务器端，服务器端检查 ack 是否为 K+1，ACK 是否为 1，如果正确则连接建立成功，客户端和服务器端进入 ESTABLISHED 状态，完成三次握手，随后客户端与服务器端之间可以开始传输数据了。

四次挥手过程：

```
TCP        44 80 → 60223 [FIN, ACK] Seq=1 Ack=2 Win=2619648 Len=0
TCP        44 60223 → 80 [ACK] Seq=2 Ack=2 Win=327424 Len=0
TCP        44 60205 → 80 [FIN, ACK] Seq=1135 Ack=31415 Win=1156 Len=0
TCP        44 80 → 60205 [ACK] Seq=31415 Ack=1136 Win=10231 Len=0
```

第一次挥手：客户端先向服务端 TCP 发出连接释放报文段（FIN=1，序号 seq=u），并停止再发送数据，主动关闭 TCP 连接，进入 FIN-WAIT-1（终止等待 1）状态，等待服务端的确认。

第二次挥手：服务端收到连接释放报文段后即发出确认报文段（ACK=1，确认号 ack=u+1，序号 seq=v），服务端进入 CLOSE-WAIT（关闭等待）状态，此时的 TCP 处于半关闭状态。客户端收到服务端的确认后，进入 FIN-WAIT-2（终止等待 2）状态，等待服务端发出的连接释放报文段。

第三次挥手：服务端将最后的数据发送完毕后，发出连接释放报文段

（FIN=1，ACK=1，序号 seq=w，确认号 ack=u+1），服务端进入 LAST-ACK（最后确认）状态，等待客户端的确认。

第四次挥手：客户端收到服务端的连接释放报文段后，对此发出确认报文段（ACK=1，seq=u+1，ack=w+1），进入 TIME-WAIT（时间等待）状态。此时 TCP 未释放掉，需要经过时间等待计时器设置的时间 2MSL 后，客户端才进入 CLOSED 状态。服务器只要收到了客户端发出的确认，立即进入 CLOSED 状态。

TCP 报文分析：

```
Frame 2: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 80, Dst Port: 63601, Seq: 0, Ack: 1, Len: 0
```

第一行，帧 Frame 2 指的是要发送的数据块，其中，所抓帧的序号为 2，捕获字节数等于传送字节数：56 字节；

```
Frame 2: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_Loopback, id 0
> Interface id: 0 (\Device\NPF_Loopback)
  Encapsulation type: NULL/Loopback (15)
  Arrival Time: Nov 13, 2020 16:43:00.922464000 中国标准时间
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1605256980.922464000 seconds
  [Time delta from previous captured frame: 0.000114000 seconds]
  [Time delta from previous displayed frame: 0.000114000 seconds]
  [Time since reference or first frame: 0.000114000 seconds]
  Frame Number: 2
  Frame Length: 56 bytes (448 bits)
  Capture Length: 56 bytes (448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: null:ip:tcp]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

第二行，以太网，有线局域网技术，是数据链路层。

第三行，IPV4 协议，也称网际协议，是网络层；源 IP 地址为 127.0.0.1；目标 IP 地址为 127.0.0.1；

```
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x1ea6 (7846)
> Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 127.0.0.1
  Destination Address: 127.0.0.1
```

第四行，TCP 协议，也称传输控制协议，是传输层；源端口(80)；目标端口

(63601)；ACK 是 TCP 数据包首部中的确认标志，对已接收到的 TCP 报文进行确认，值为 1 表示确认号有效。

```
Transmission Control Protocol, Src Port: 80, Dst Port: 63601, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 63601
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1668549604
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 962222649
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x7b2c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [SEQ/ACK analysis]
  > [Timestamps]
```

获取网页：（GET 请求报文，HTTP 响应报文）

```
HTTP      692 GET /hello.html HTTP/1.1
TCP        44 80 → 63601 [ACK] Seq=1 Ack=649 Win=2619648 Len=0
HTTP      249 HTTP/1.1 304 Not Modified
TCP        44 63601 → 80 [ACK] Seq=649 Ack=206 Win=2619392 Len=0
HTTP      530 GET /favicon.ico HTTP/1.1
TCP        44 80 → 63601 [ACK] Seq=206 Ack=1135 Win=2619136 Len=0
HTTP    31252 HTTP/1.1 200 OK  (image/x-icon)
TCP        44 63601 → 80 [ACK] Seq=1135 Ack=31414 Win=2588160 Len=0
```

HTTP 报文分析：

```
Frame 7: 692 bytes on wire (5536 bits), 692 bytes captured (5536 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 63601, Dst Port: 80, Seq: 1, Ack: 1, Len: 648
Hypertext Transfer Protocol
```

第一行，帧 Frame 7 指的是要发送的数据块，其中，所抓帧的序号为 7，捕获字节数等于传送字节数：692 字节；

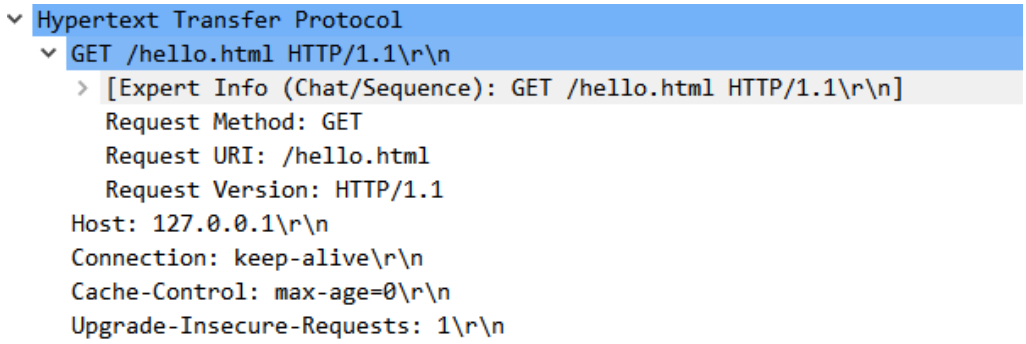
第二行，以太网，有线局域网技术，是数据链路层。

第三行，IPV4 协议，也称网际协议，是网络层；源 IP 地址为 127.0.0.1；目标 IP 地址为 127.0.0.1；

第四行，TCP 协议，也称传输控制协议，是传输层；源端口(63601)；目标端口(80)；ACK 是 TCP 数据包首部中的确认标志，对已接收到的 TCP 报文进行确认，值为 1 表示确认号有效；长度为 648；

第五行，Http 协议，也称超文本传输协议，是应用层。

GET 请求报文：



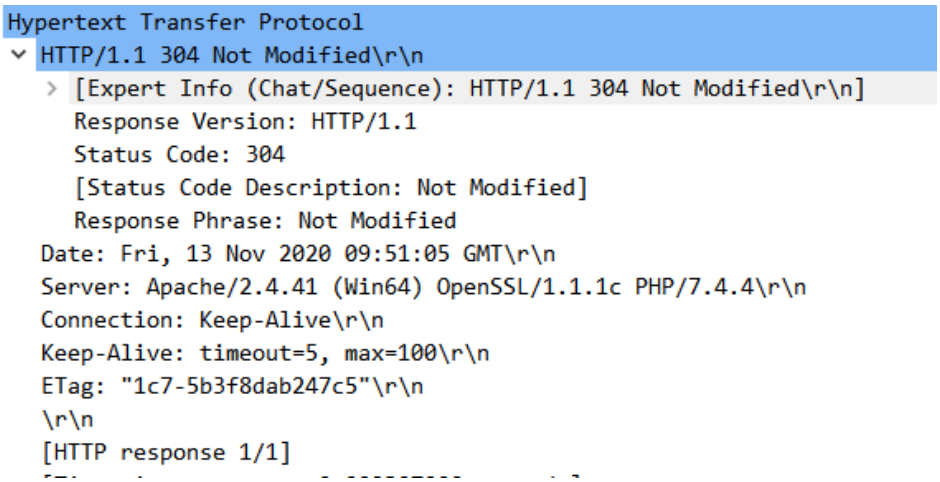
一个 HTTP 请求报文由请求行（request line）、请求头部（header）、空行和请求数据 4 个部分组成。

前三行为请求行，其余部分称为 request-header。请求行中的 method 表示这次请求使用的是 get 方法，URI，表示请求的页面地址。

Host：连接的目标主机，如果连接的服务器是非标准端口，在这里会出现使用的非标准端口。

Connection：对于 HTTP 连接的处理，keep-alive 表示保持连接，如果是在响应报文中发送页面完毕就会关闭连接，状态变为 close。

HTTP 响应报文：



HTTP 响应报文由状态行、响应头部、空行 和 响应包体 4 个部分组成。

状态行由 HTTP 协议版本字段、状态码和状态码的描述文本 3 个部分组成。

状态码以及描述文本有常见的如下几种：

200 OK：表示客户端请求成功；

304 Not Modified：表示此次请求为条件请求；

400 Bad Request：表示客户端请求有语法错误，不能被服务器所理解；

401 Unauthonzed：表示请求未经授权，该状态代码必须与 WWW-Authenticate 报头域一起使用；

403 Forbidden：表示服务器收到请求，但是拒绝提供服务，通常会在响应正文中给出不提供服务的原因；

404 Not Found：请求的资源不存在，例如，输入了错误的 URL；

500 Internal Server Error：表示服务器发生不可预期的错误，导致无法完成客户端的请求；

503 Service Unavailable：表示服务器当前不能够处理客户端的请求，在一段时间之后，服务器可能会恢复正常；

当一次访问网页的时候，显示的是 200 OK，当多次访问的时候，会显示 304 Not Modified，因为此时客户端已经换成了目标资源并且已经为最新版本，如果不是最新版本，将显示 200 OK，并缓存最新资源覆盖旧资源。

附录：网页代码

```
<!doctype html>
<html lang="en">
  <head>
    <title>computer network</title>
    <meta charset="utf-8">
  </head>
  <body>
    <img src="hero_1.jpg">
    <div class="container">
      <div style="text-align: center; line-height: 100px;">
        <h1>专业：计算机科学与技术
          <br>
          学号：1811507
          <br>
          姓名：文静静
        </h1>
      </div>
    </div>
  </body>
</html>
```