【实验名称：TCP数据分析实验】

学生姓名：李雪菲 合作学生：无

实验地点：济事楼330 实验时间：2025-05-15

【实验目的】

1. 理解 TCP 报文结构，包括端口号、序号等的作用和意义。

2. 掌握 TCP 的三次握手和四次挥手过程，通过实验详细了解 TCP 连接的建立和终止过程。

3. 分析 TCP 的流量控制和拥塞控制机制，观察和分析 TCP 如何通过窗口调整机制来进行流量控制，以及如何通过拥塞控制算法来响应网络中的拥塞情况。

4. 使用网络分析工具，使用如 Wireshark 这类网络分析工具来捕获和分析 TCP 数据包。通过实际数据包的分析，更好地理解理论知识在实际网络通信中的应用。

【实验原理】

一、TCP 概述

TCP（传输控制协议）是传输层的基于连接的协议，提供可靠的全双工数据传输。它通过序号和确认号机制确保数据按序传递且无损坏，并利用窗口机制进行流量控制，以及采用拥塞控制算法防止网络拥堵。虽然 TCP 需要在端系统中维护连接状态，带来一定的时间和空间开销，但其可靠性和数据完整性使其广泛应用于需要稳定传输的场景。相比之下，UDP 不维护连接状态，开销较小，适用于

对传输速度要求高而对可靠性要求低的实时应用。

二、TCP 的报文格式



TCP 报文是 TCP 层传输的数据单元，也叫报文段。

三、TCP 的报文字段

TCP 报文段由多个字段组成，每个字段在 TCP 传输过程中扮演着不同的角色。

以下是这些字段的详细介绍：

1. 源端口：标识发送数据的应用进程，用于确定数据的返回地址。

2. 目的端口：标识接收数据的应用进程，指明接收方计算机上的应用程序接口。

3. 序号：表示报文段中的第一个字节的序号，确保数据按序到达。例如，如果报文段序号为 300，数据部分为 100 字节，则下一个报文段的序号为 400。

4. 确认号（ACK）：指示下一个期待收到的字节序号，表明之前的所有数据已正确接收。只有当 ACK 标志为 1 时才有效。

5. 数据偏移/首部长度：4 位字段，表示 TCP 报头的长度（以 32 位字为单位）。首部长度最大可为 60 字节。

6. 保留字段：为将来用途预留，一般置为 0。

7. 控制位：

URG：紧急指针标志，为 1 时表示紧急指针有效。

ACK：确认序号标志，为 1 时表示确认号有效。

PSH：Push 标志，为 1 表示接收方应尽快将报文段交给应用程序。

RST：重置连接标志，用于重置连接或拒绝非法的报文段。

SYN：同步序号标志，用于建立连接。

FIN：结束标志，用于释放连接。

8. 窗口：16 位字段，指示接收端的缓存大小，用于流量控制，最大值为 65535字节。

9. 校验和：用于校验整个 TCP 报文段（包括头部和数据部分），确保数据完整性。

10. 紧急指针：在 URG 标志为 1 时有效，指示紧急数据的最后一个字节的序号。

11. 选项和填充：包含可选字段，如最大报文段大小（MSS）。选项字段的长度不定，需填充到 32 位整数倍。

12. 数据部分：可选字段，包含实际传输的数据。在连接建立和终止时，报文段仅包含 TCP 首部。

四、TCP 连接过程

TCP 连接过程包括“建立连接的三次握手”和“断开连接的四次挥手”，这两个过程确保了连接的可靠性和有序性。

（一）三次握手（Three-way Handshake）

建立一个 TCP 连接时，需要客户端和服务器之间进行三次握手。其目的是建立 TCP 连接，并同步双方的序列号和确认号，同时交换窗口大小信息。

1. 第一次握手：

客户端发送一个 SYN（同步序号）标志位为 1 的报文段，指明要连接的

服务器端口和初始序列号 X。这个报文段表示客户端希望建立连接。服务器接收到这个报文段后，处于 SYN\_RECEIVED 状态。

2. 第二次握手：

服务器收到客户端的 SYN 报文后，回应一个 SYN 和 ACK（标志位均为 1 的报文段。确认号为 X+1，表示服务器已经收到并确认了客户端的请求。这个报文段的初始序列号为 Y。客户端接收到这个报文段后，处于 SYN\_ACK\_RECEIVED 状态。

3. 第三次握手：

客户端收到服务器的 SYN-ACK 报文后，再次发送一个 ACK 标志位为 1 的报文段，确认号为 Y+1，表示客户端已经收到服务器的确认。这个报文段的序列号为 X+1。服务器接收到这个报文段后，连接进入 ESTABLISHED 状态，客户端也进入 ESTABLISHED 状态。

（二）四次挥手（Four-way Handshake）

断开一个 TCP 连接需要发送四个报文段，任何一方都可以主动发起断开连接

的请求。

1. 第一次挥手：

发起方（客户端或服务器）发送一个 FIN（结束）标志位为 1 的报文段，表示没有数据要发送了。对方接收到这个报文段后，处于 CLOSE\_WAIT 状态。

2. 第二次挥手：

接收方回应一个 ACK 标志位为 1 的报文段，确认号为发起方的序列号加1。 发起方接收到这个报文段后，处于 FIN\_WAIT\_2 状态。

3. 第三次挥手：

接收方如果也没有数据要发送，发送一个 FIN 标志位为 1 的报文段，表示同意断开连接。发起方接收到这个报文段后，处于 TIME\_WAIT 状态。

4. 第四次挥手：

发起方回应一个 ACK 标志位为 1 的报文段，确认号为接收方的序列号加1。接收方接收到这个报文段后，进入 CLOSED 状态。发起方等待一段时间后也进入 CLOSED 状态，确保对方接收到 ACK 后才彻底断开连接。

（三）SYN 攻击

在三次握手过程中，攻击者伪造大量不存在的 IP 地址发送 SYN 报文，服务器回复 SYN-ACK 报文并等待确认。由于源地址不存在，服务器需要不断重发，导致未连接队列被占用，正常请求被拒绝，系统性能下降甚至瘫痪。

【实验设备】

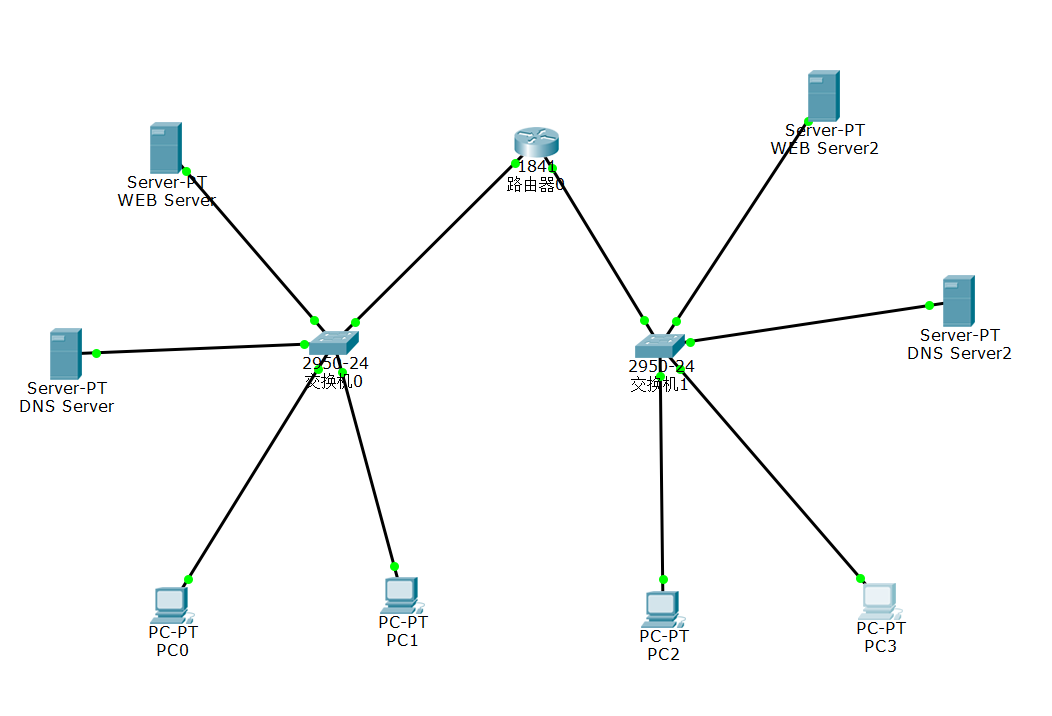
1. 一台电脑
2. Cisco packet tracer 仿真软件
3. Wireshark 仿真软件

【实验步骤】

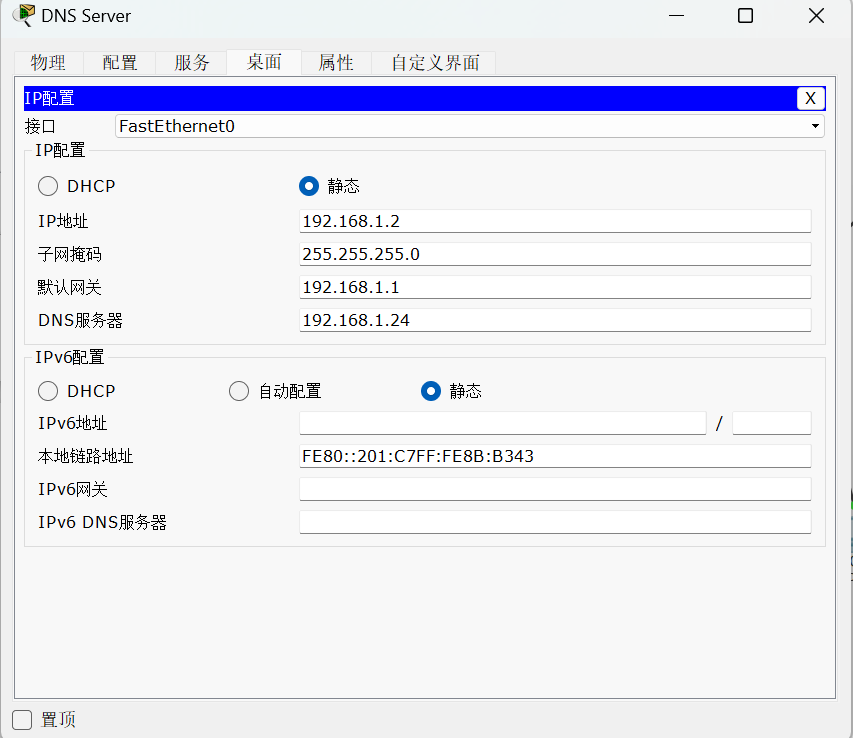
1. 搭建网络结构图
2. 设置WEB服务器和简单的DNS服务器
3. 打开PC0浏览器，输入配置Web服务器的 Web 地址，如www.tongji.edu.cn或 www.test.com，产生TCP数据报文
4. 分析在 Packet Tracer 中 TCP 报文情况。
5. 用 WireShark 抓取 TCP 数据包，查看 TCP 报文字段内容，并解读。

【实验现象】

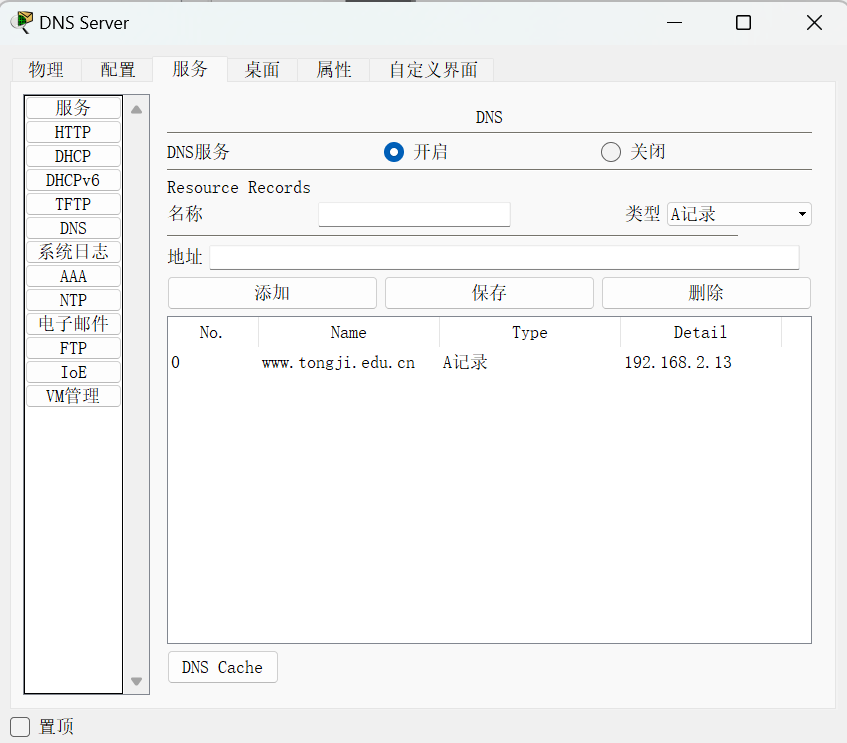
1. 搭建网络结构图

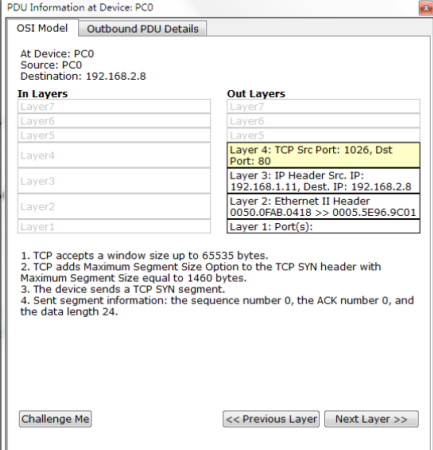


1. 设置WEB服务器和简单的DNS服务器

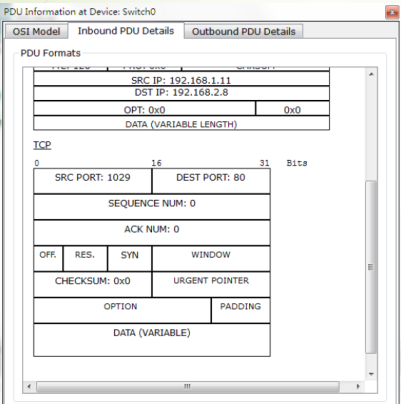


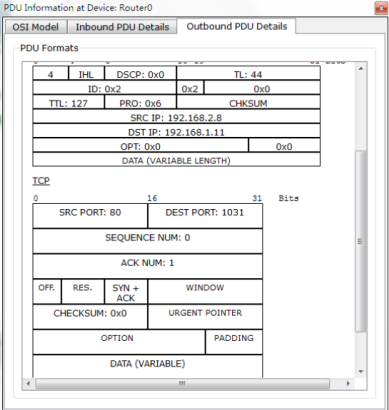
1. 打开PC0浏览器，输入配置DNS服务器的 Web 地址，如www.tongji.edu.cn或 www.test.com，产生TCP数据报文



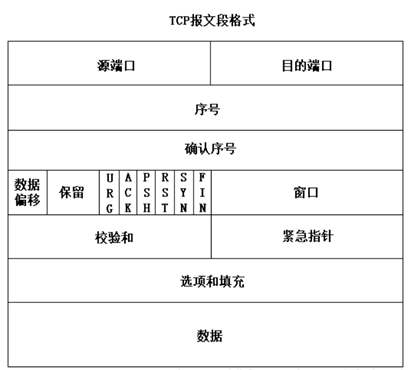


1. 分析在 Packet Tracer 中 TCP 报文情况。





综上，TCP报文格式：



源端口：占2个字节，源端口和IP的作用是标记报文的返回地址。  
目的端口：占2个字节，指明接收方计算机上的应用程序接口。

序号：占4个字节，是TCP可靠传输的关键部分。

确认序号：即ack，占4个字节，指明下一个期待收到的字节序号，表明该序号之前的所有数据已经正确无误的收到。

数据偏移：占4位，它指出TCP报文的数据距离TCP报文段的起始处有多远。

保留:为将来定义新的用途保留，一般置为0。

控制位：

　　URG：紧急指针标志。1：紧急指针有效；0：忽略紧急指针。  
  ACK：确认序号标志。1：确认号有效；0：忽略确认号段。  
  PSH：push标志。1：带有push标志的数据，表示接收方在接收到该报文后应尽快将这个报文段交给应用程序，而不是缓冲区排队。  
  RST：重置连接标志。用于重置由于主机崩溃或其他原因而出现错误的连接。或者用于拒绝非法的报文段和拒绝连接请求。  
  SYN：同步序号，用于建立连接过程，在连接请求中，SYN=1和ACK=0表示该数据段没有使用捎带的确认域，而连接应答捎带一个确认，即SYN=1和ACK=1。  
  FIN：结束标志，用于释放连接，为1时表示发送方已经没有数据发送了，即关闭本方数据流。  
窗口：滑动窗口大小，用来告知发送端接收端的缓存大小，以此控制发送端发送数据的速率，从而达到流量控制。

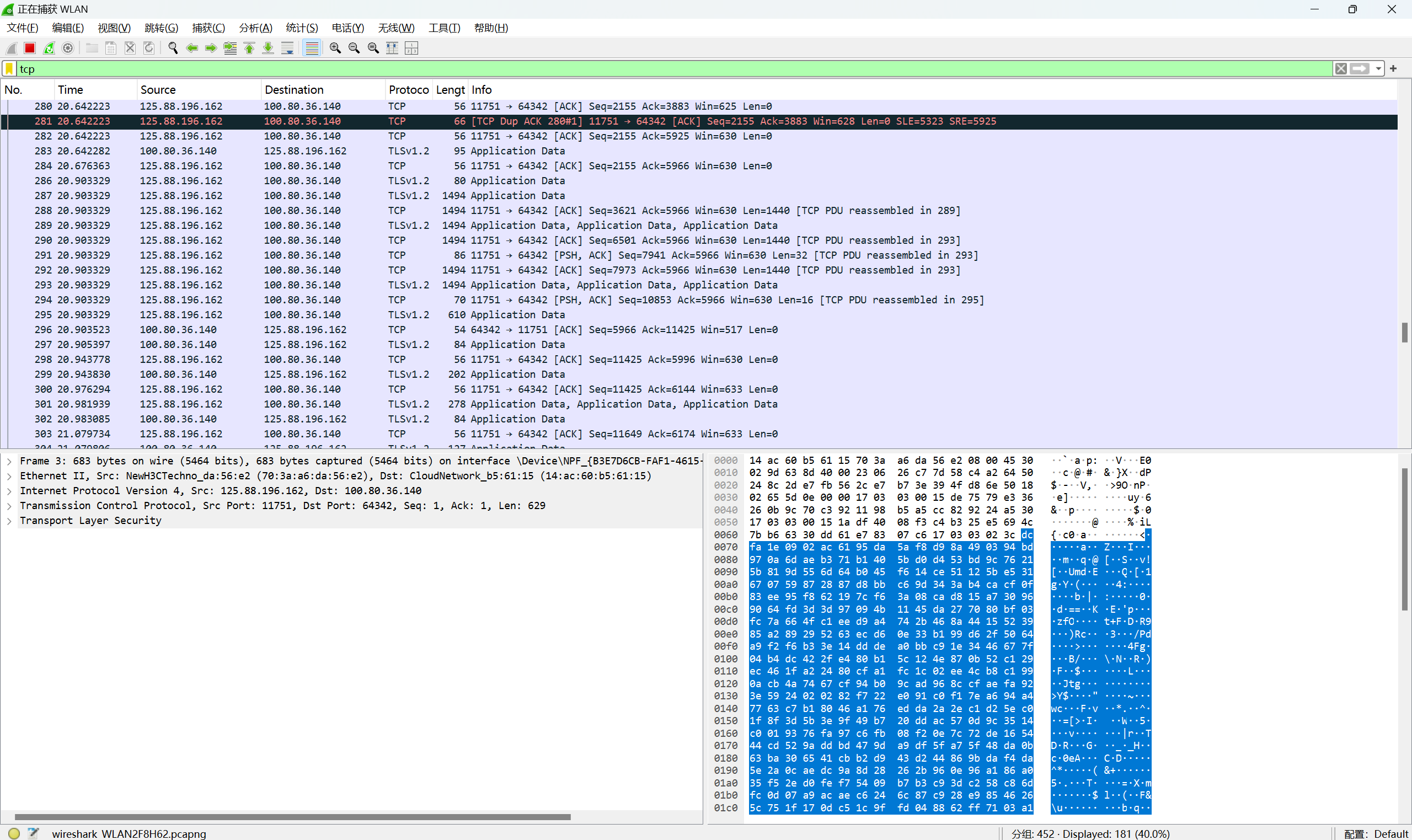
校验和：奇偶校验，此校验和是针对整个TCP报文段的，包括TCP报头和TCP报文数据段，以2个字节进行计算所得。

紧急指针：只有当URG标志置1时紧急指针才有效，TCP的紧急方式是发送端向另一端发送紧急数据的一种方式。

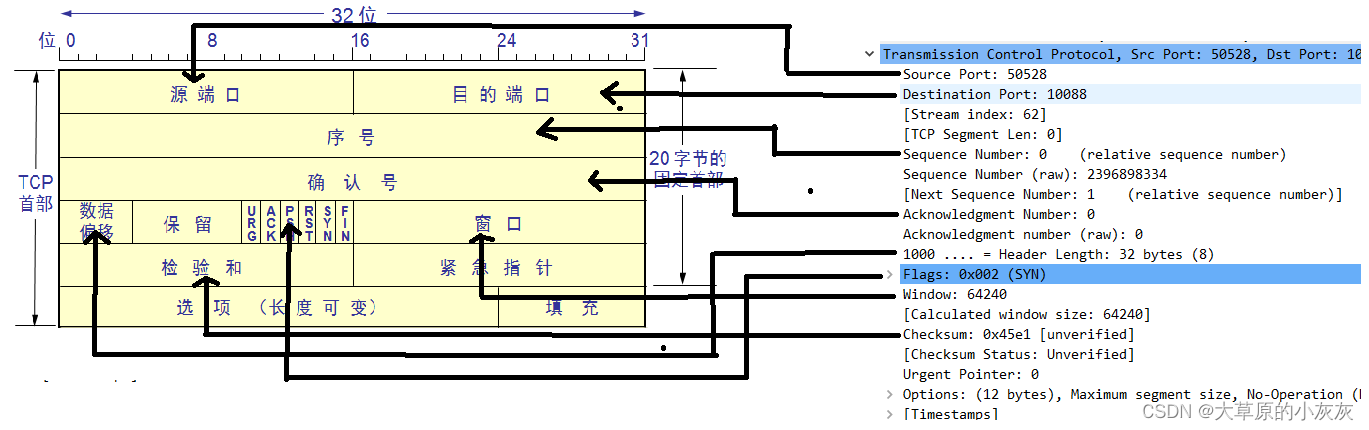
选项和填充：最常见的可选字段是最长报文大小，它表示本端所能接受的最大报文段的长度。

数据部分：TCP报文段中的数据部分是可选的。

1. 用 WireShark 抓取 TCP 数据包，查看 TCP 报文字段内容，并解读。



每个字段对应的TCP包头：



【分析讨论】

1. 查看TCP报文字段内容，并解读。

报文字段（从 Wireshark 中展开 TCP 协议部分可见）：

|  |  |
| --- | --- |
| 字段名称 | 含义说明 |
| SourcePort | 源端口号（客户端） |
| DestinationPort | 目的端口号（服务器） |
| SequenceNumber | 序列号，标识发送的数据位置 |
| AcknowledgmentNumber | 确认号，确认接收数据 |
| HeaderLength | TCP首部长度 |
| Flags（控制位） | 包括 SYN, ACK, FIN, PSH, URG 等 |
| WindowSize | 滑动窗口大小 |
| Checksum | 校验和 |
| UrgentPointer | 紧急数据指针（一般为0） |
| Options | 可选字段，如时间戳、窗口扩展等 |

1. 仔细研读TCP连接建立过程数据报文

（1）客户端 -> 服务器：SYN

SYN = 1，客户端发起连接请求，Seq=X

（2） 服务器 -> 客户端：SYN-ACK

SYN = 1，ACK = 1，Seq=Y，Ack=X+1

（3） 客户端 -> 服务器：ACK

ACK = 1，Seq=X+1，Ack=Y+1

1. 仔细研读TCP拆链过程数据报文

（1） 客户端 -> 服务器：FIN

表示客户端完成发送

（2） 服务器 -> 客户端：ACK

确认收到 FIN

（3） 服务器 -> 客户端：FIN

表示服务器也准备关闭

（4） 客户端 -> 服务器：ACK

最后确认关闭