实验 24：TCP 数据分析实验

姓名	学号	合作学生	指导教师	实验地点	实验时间
林继申	2250758	无	陈伟超	济事楼 330	2024/05/16

【实验目的】

1. 理解 TCP 报文结构：学生将学习 TCP 报文段的各个字段，包括端口号、序号、确认号、数据偏移、控制位（如 SYN, ACK, FIN 等）、窗口大小、校验和、紧急指针等的作用和意义。
2. 掌握 TCP 的三次握手和四次挥手过程：通过实验，学生将详细了解 TCP 连接的建立和终止过程，即所谓的“三次握手”和“四次挥手”。这些知识对于理解网络通信的可靠性和效率至关重要。
3. 分析 TCP 的流量控制和拥塞控制机制：实验中，学生将观察和分析 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：学生将使用如 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，学生可以更好地理解理论知识在实际网络通信中的应用。
5. 诊断网络问题：通过分析 TCP 数据段，学生能学习如何诊断网络中的问题，例如乱序数据包、丢包、重复确认等，并理解这些问题对网络性能的影响。
6. 实践和加深网络协议栈的理解：此实验不仅帮助学生加深对 TCP 协议的理解，还能够帮助他们了解更多关于网络层到应用层之间如何交互和协作的知识。

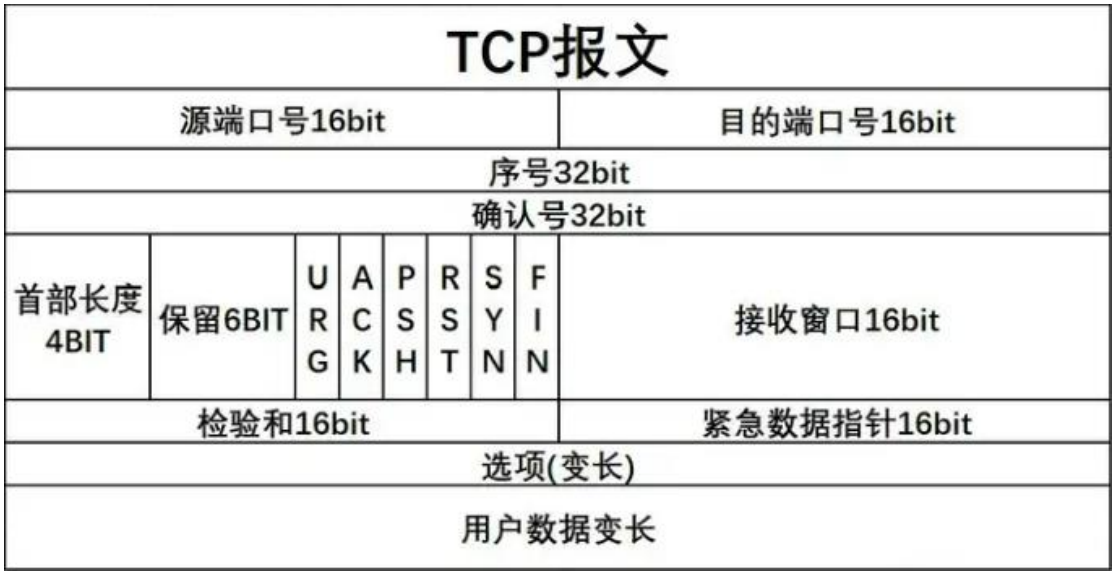
【实验原理】

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（确认）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】

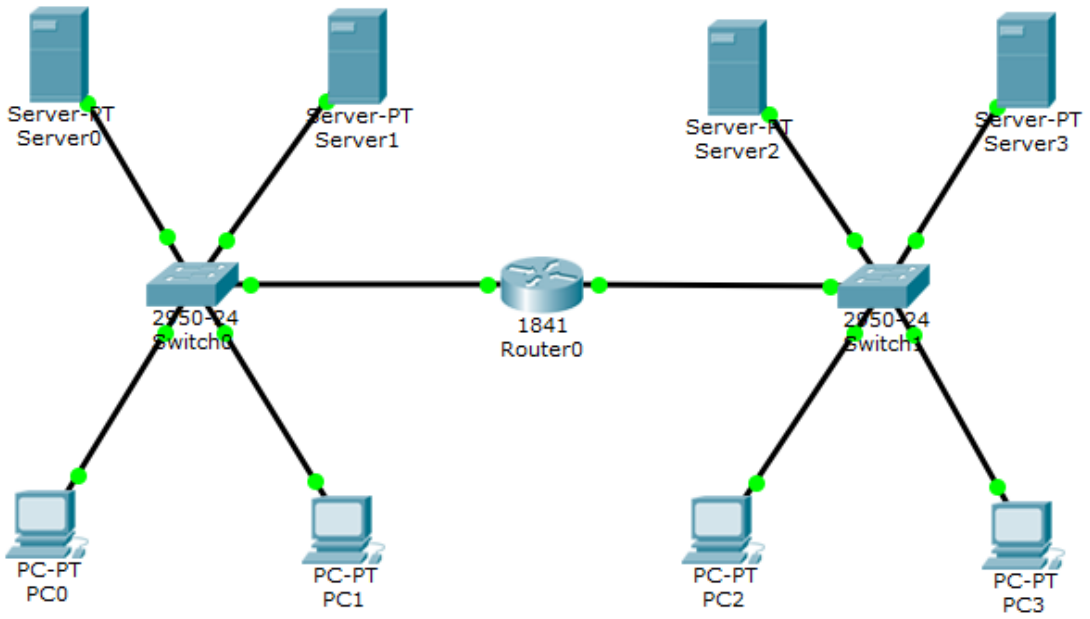
1. 操作系统：Windows 10

2. 网络环境：局域网

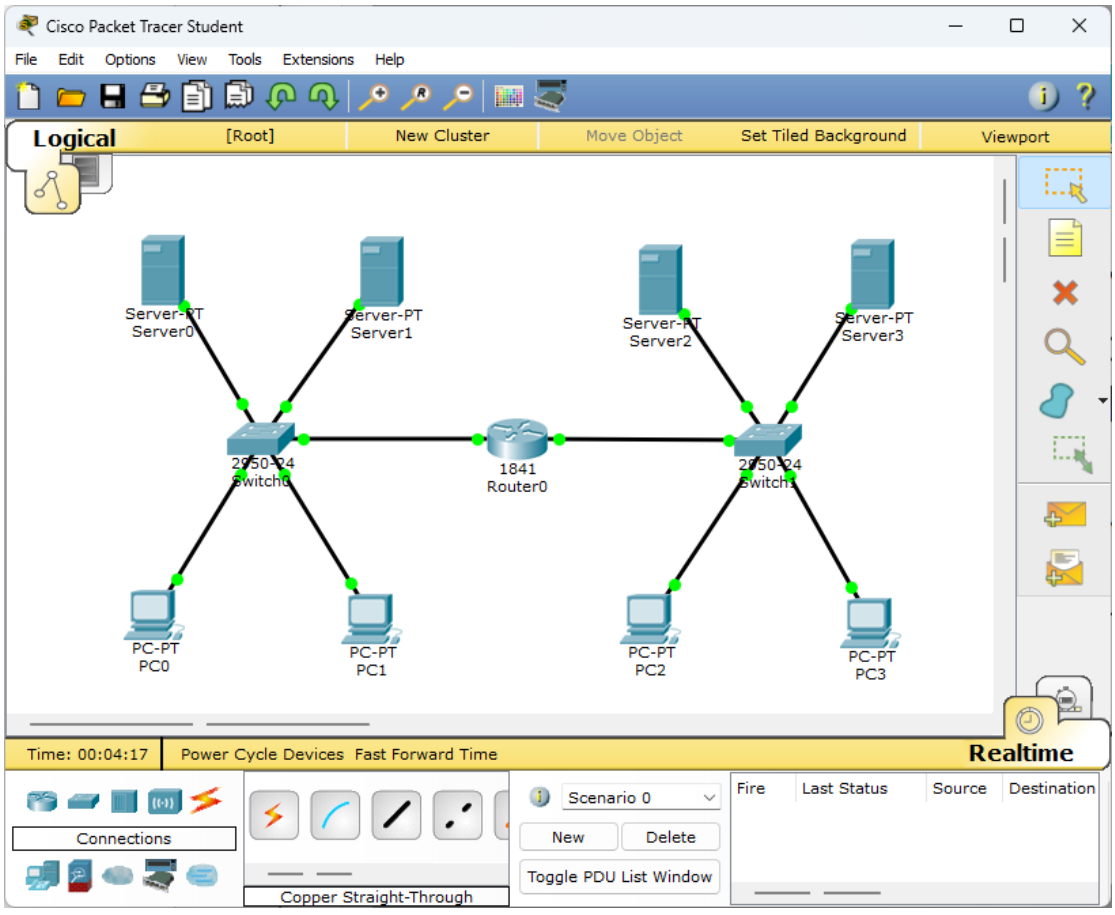
3. 应用程序：Cisco Packet Tracer 6.0

【实验步骤】

1. 规划网络地址及拓扑图。

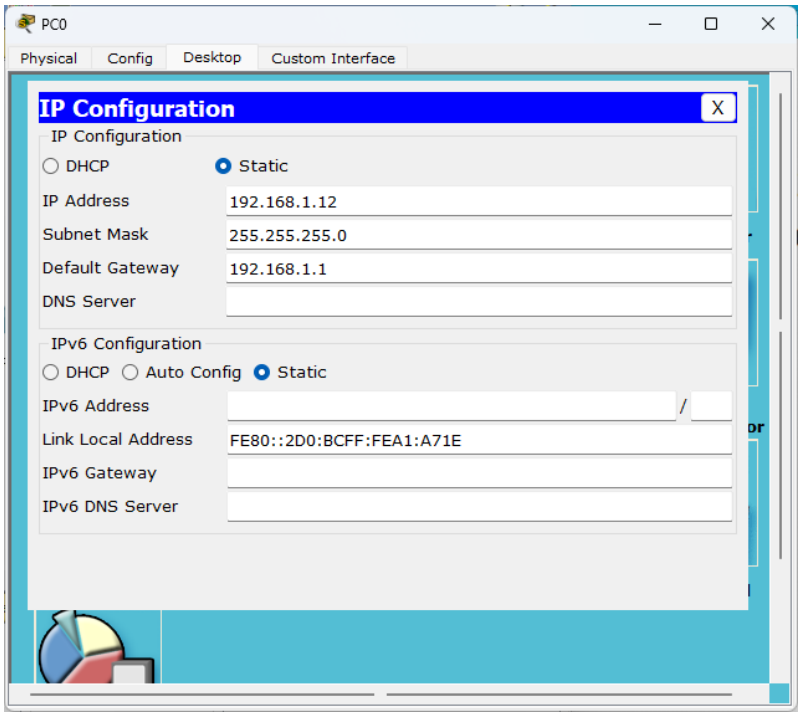


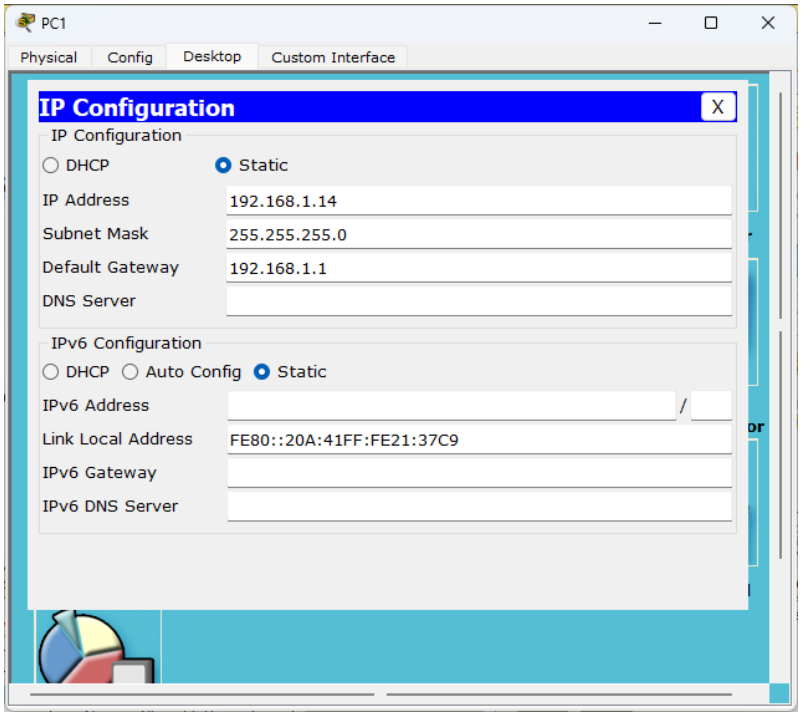
2. 启动 Cisco Packet Tracer，按照上图连接网络。

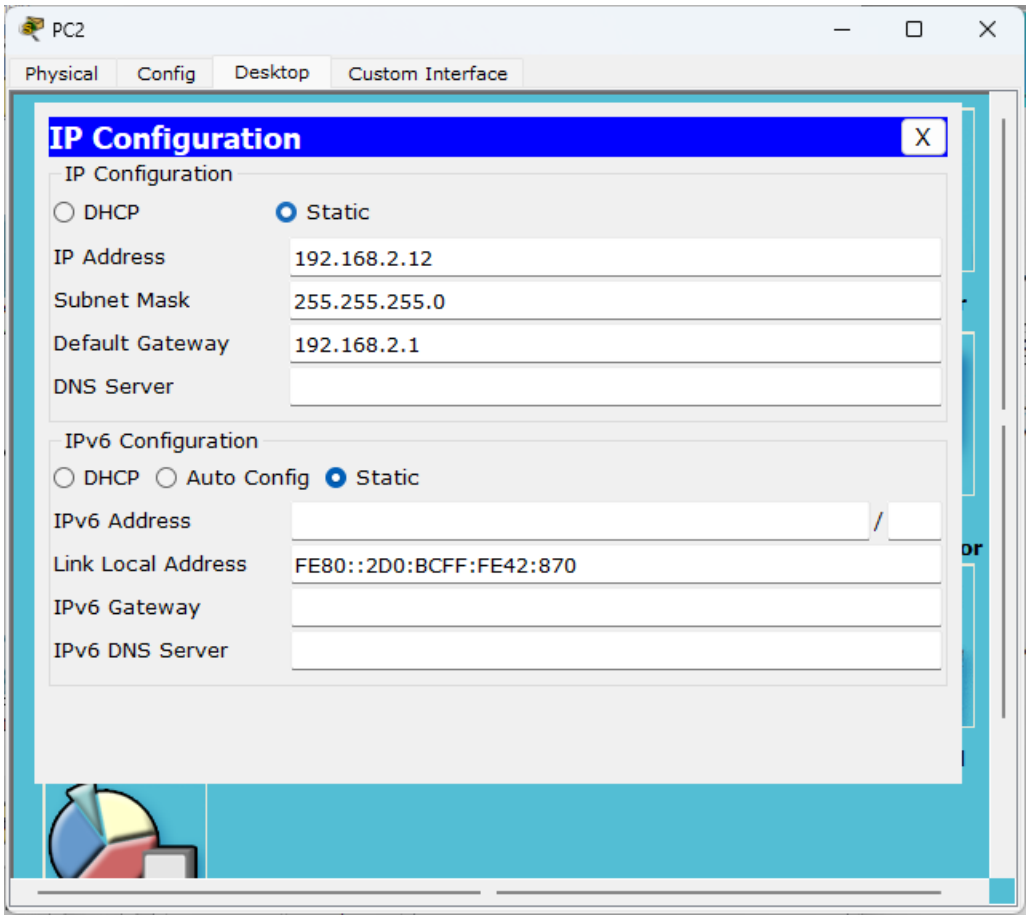


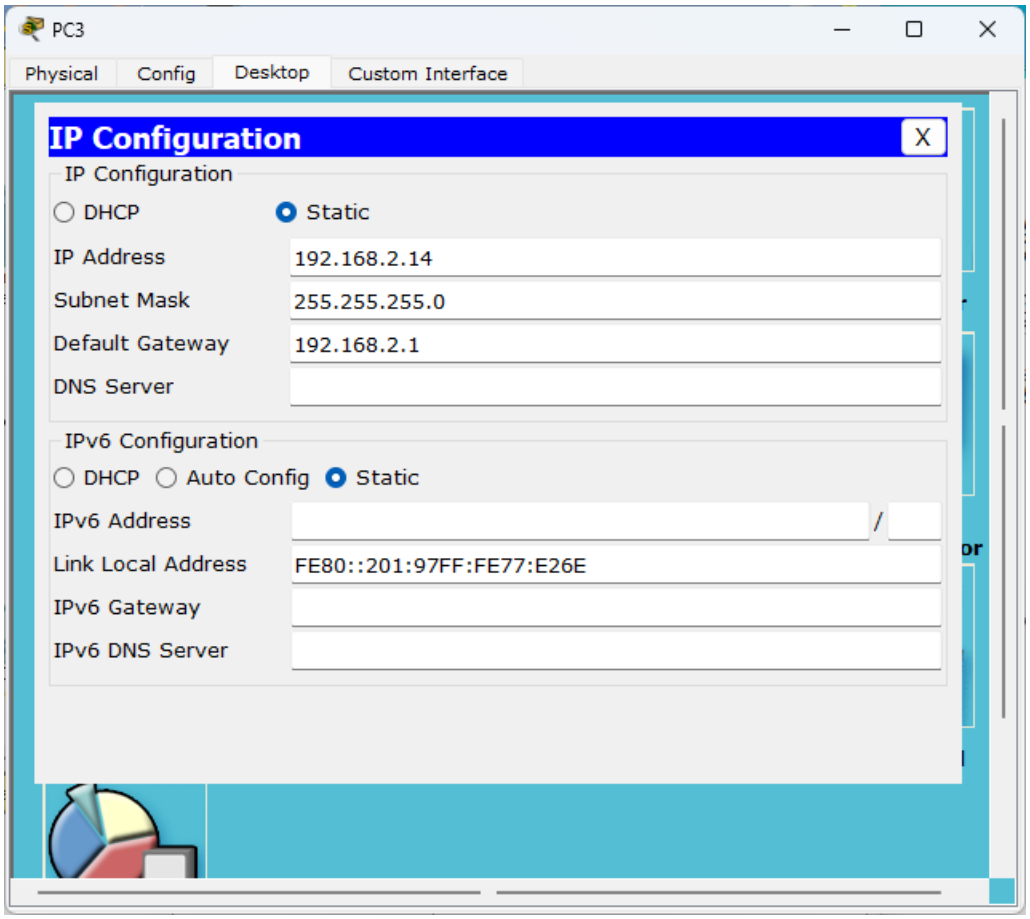
3. 为每台 PC 机配置如下静态 IP 地址、子网掩码和默认网关。

PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.12	255.255.255.0	192.168.1.1
PC1	192.168.1.14	255.255.255.0	192.168.1.1
PC2	192.168.2.12	255.255.255.0	192.168.2.1
PC3	192.168.2.14	255.255.255.0	192.168.2.1



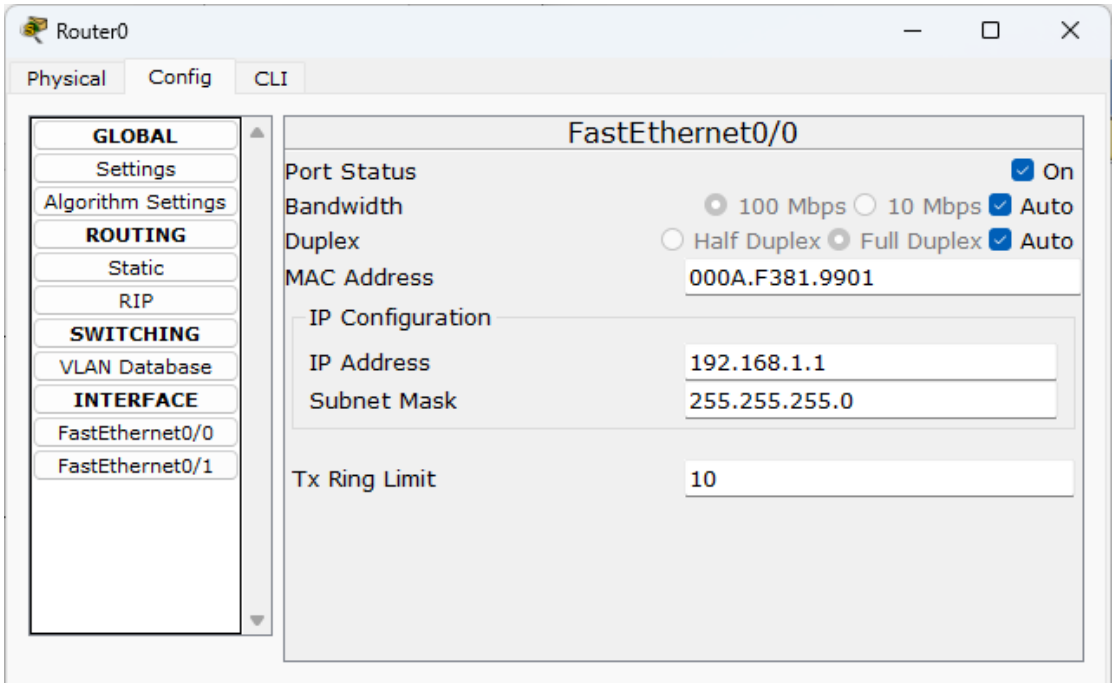


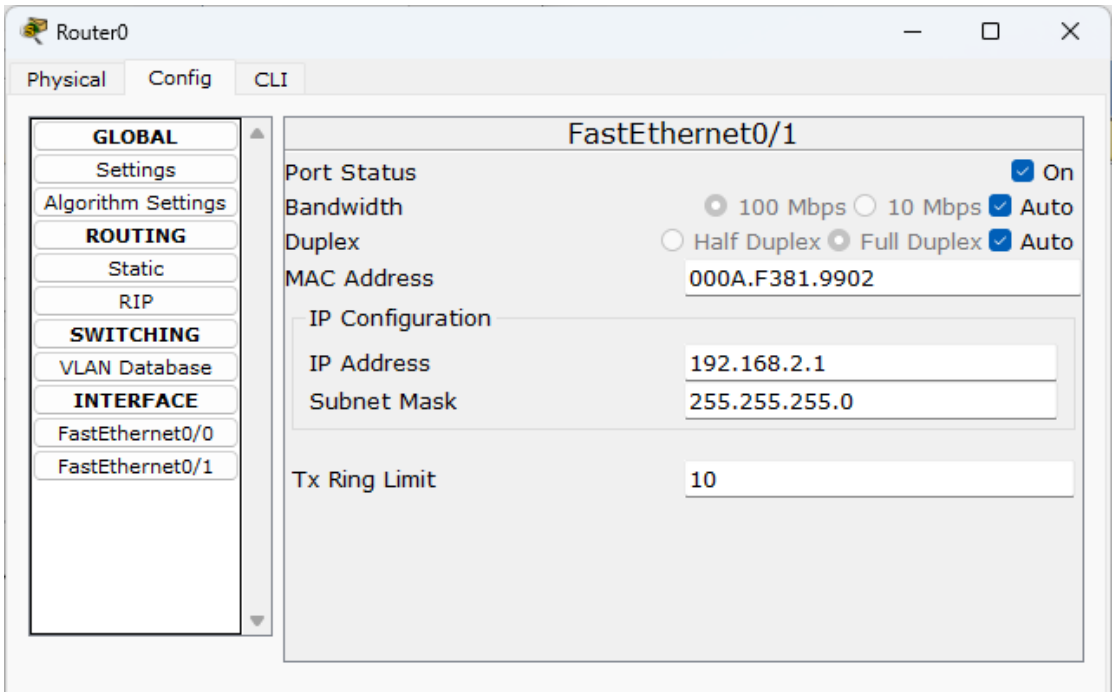

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE42:870
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE77:E26E
IPv6 Gateway
IPv6 DNS Server

4. 参照先前实验（实验 18：动态 IP 地址分配 DHCP 实验）配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```





5. 在路由器 Router0 配置 DHCP。

- 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

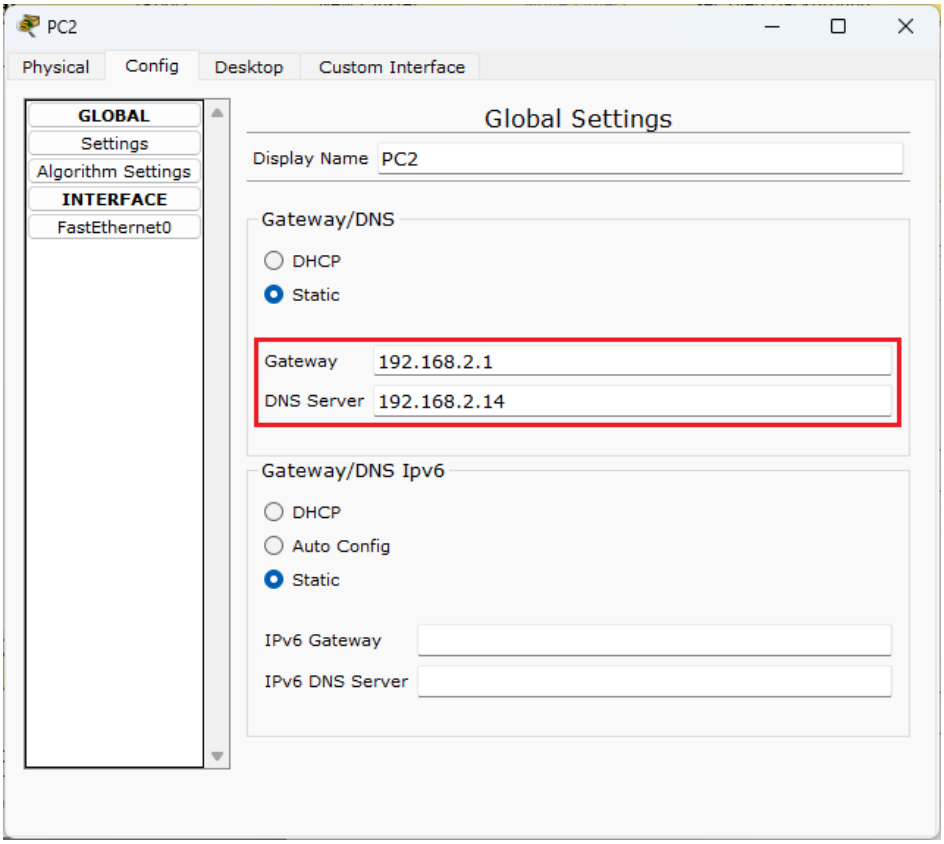
```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

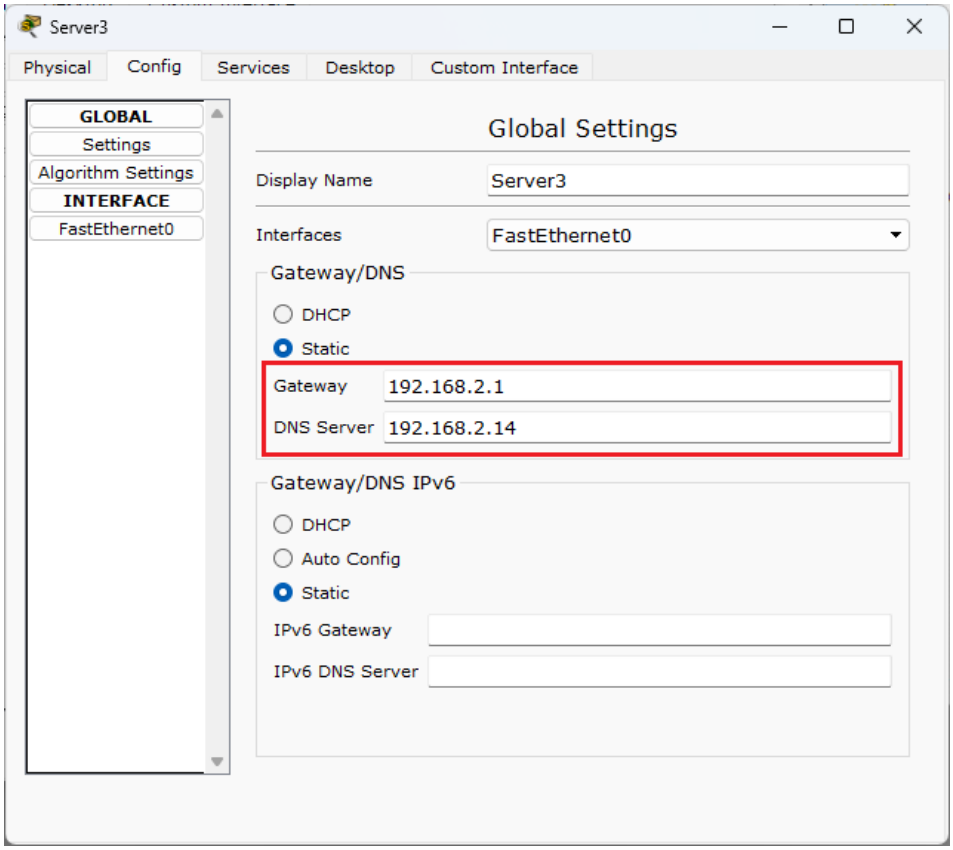
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

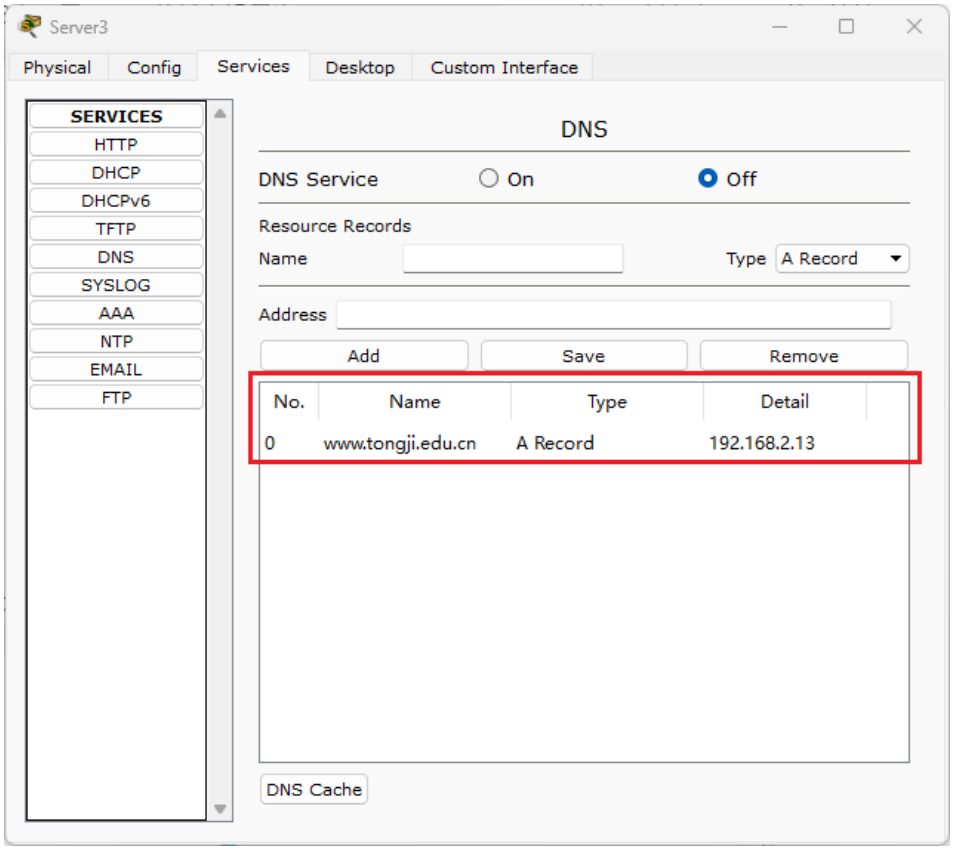
6. 配置 Server 的 Gateway 和 DNS Server。

7. 配置 PC2 的 DNS Server 为 192.168.2.14。设置 PC2 的 DNS Server 与 Server3 的 DNS Server 相同是为了能够通过 Server3 构建映射访问到 Server2。





8. 配置 Server3 的 Services，Name 设置为 www.tongji.edu.cn，Detail 设置为 Server2 的 IP 地址（192.168.2.13）。



9. 从 Realtime 模式切换至 Simulation 模式。

9.1 在 PC2 的 Web Browser 中输入 http://www.tongji.edu.cn，产生 TCP 数据报文。

9.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

9.3 在 Even List 中的 Info 栏可以查看相关信息。

10. 分析在 Packet Tracer 中 TCP 报文情况。

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

12. 仔细研读 TCP 连接建立过程数据报文。

13. 仔细研读 TCP 拆链过程数据报文。

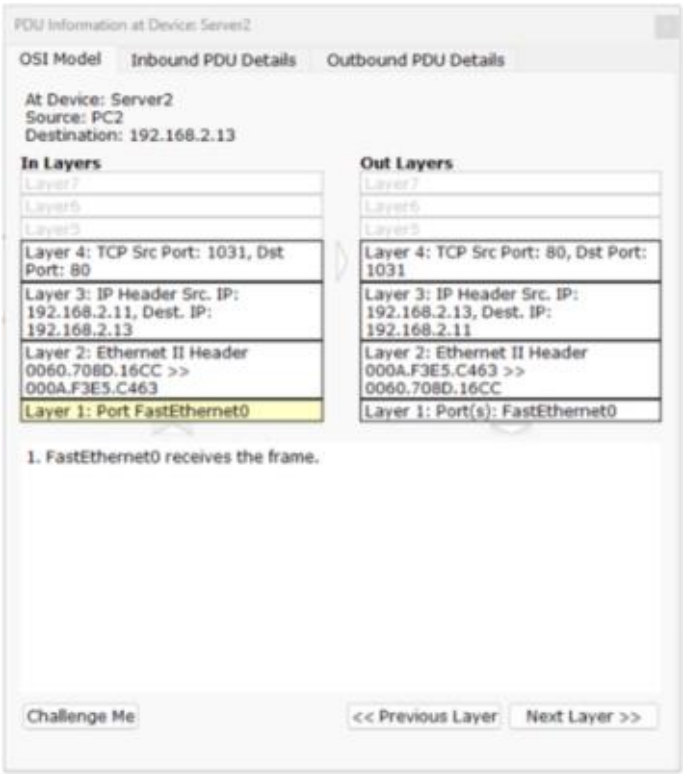
【实验现象】

1. 分析在 Packet Tracer 中 TCP 报文情况。

1.1 PDU Information at Device: Server2（OSI Model）

- 输入 PDU 详情（Switch2→Server2）
  - 源端口：1031
  - 目标端口：80（HTTP 服务）
  - 序列号：0
  - 确认号：0（此为建立连接时的 SYN 报文，序列号和确认号均为 0）
  - 源 IP 地址：192.168.2.11
  - 目的 IP 地址：192.168.2.13
  - 以太网 II 帧头：包含目标和源 MAC 地址（详细的 MAC 地址在描述中未提供）
  - TCP 控制位：SYN（由于是建立连接的 SYN 报文）
- 输出 PDU 详情（Server2→Switch2）
  - 源端口：80
  - 目标端口：1031
  - 序列号：0
  - 确认号：1（表示对第一阶段 SYN 请求的确认）
  - 源 IP 地址：192.168.2.13

- 目的 IP 地址：192.168.2.11
- TCP 控制位：SYN+ACK（表示对 SYN 的确认并请求对方也确认）



- 分析
  - SYN 报文（输入）：第一步的 SYN 报文用于初始化 TCP 连接，它从源端口 1031 发出，请求与目的端口 80（通常用于 HTTP 服务）的设备建立连接。这是三次握手过程中的第一步。
  - SYN+ACK 报文（输出）：服务器收到 SYN 后，回复一个 SYN+ACK 报文，确认收到（通过 ACK 序号为 1），并同时发送自己的 SYN 请求。这是握手过程的第二步，用来确认客户端的 SYN 并要求客户端确认服务器的连接请求。

1.2 PDU Information at Device: Server2（Inbound PDU Details）

- IP 层信息
  - TTL（Time To Live）：128，这表示该数据包在网络上的最大跳数。
  - 协议（PRO）：0x6，表示传输层协议为 TCP。
  - 源 IP（SRC IP）：192.168.2.11，数据包的起始地址。
  - 目的 IP（DST IP）：192.168.2.13，数据包的目标地址。
  - 校验和(CHECKSUM)：0x0，虽然这里显示为 0，实际情况应有一个计算值。

- 选项（OPT）和数据：这两项在此图中未展示具体值，数据长度为可变。

- TCP 层信息
  - 源端口（SRC PORT）：1031，标识发送端的端口。
  - 目标端口（DEST PORT）：80，通常用于 HTTP 服务的端口。
  - 序列号（SEQUENCE NUM）：0，用于标识从 TCP 源端发送的数据字节流的顺序号。
  - 确认号（ACK NUM）：0，用于确认收到对方发送的数据。
  - 偏移（OFF.）和保留（RES.）：TCP 头部的长度和保留位，通常用于控制标志。
  - SYN（同步序列号）：设置此标志表示这是一个连接建立请求。
  - 窗口（WINDOW）：控制从对方接收的数据量，此处未显示具体值。
  - 校验和（CHECKSUM）：0x0，用于检测数据在传输过程中的任何错误。
  - 紧急指针（URGENT POINTER）：当 URG 标志被设置时，表示这个字段是有效的，此处显示为未设置。
  - 选项（OPTION）和填充（PADDING）：TCP 头部可能包含的选项和为了字节对齐而添加的填充字节。

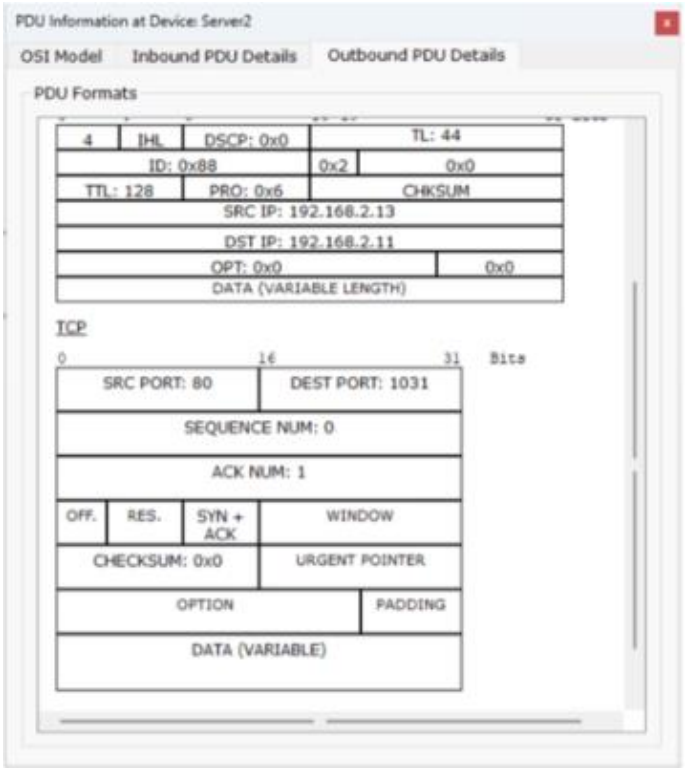
- 数据传输分析

- 这张图示例显示的是一个 TCP 初始化连接请求的 SYN 包。SYN 标志被设置表示请求建立连接。这是 TCP 三次握手过程中的第一步，用于同步序列号。接下来期待的是服务器响应一个 SYN-ACK 包，标志位 ACK 和 SYN 同时设置，表示确认并同意建立连接。

1.3 PDU Information at Device: Server2（Outbound PDU Details）

- IP 层信息
  - 版本号（Version）：4，表示这是 IPv4。
  - 首部长度（IHL - Internet Header Length）：表示 IP 头部的长度，单位为 32 位字（4 字节的倍数）。
  - 区分服务（DSCP）：0x0，表示没有特殊的区分服务。
  - 总长度（TL - Total Length）：44，表示整个 IP 数据包的长度（字节）。
  - 标识（ID）：0x88，一种标识，用于分片和重组。
  - 片偏移（Fragment Offset）：0x2，表示这个片段在原数据包中的位置。
  - 生存时间（TTL）：128，数据包在网络中的最大跳数。
  - 协议（PRO）：0x6，表示传输层协议为 TCP。
  - 校验和（CHECKSUM）：未显示具体值，用于检验 IP 头部的完整性。
  - 源 IP（SRC IP）：192.168.2.13，数据包的起始地址。
  - 目的 IP（DST IP）：192.168.2.11，数据包的目标地址。
  - 选项（OPT）和 数据：没有特殊选项，数据长度可变。
- TCP 层信息
  - 源端口（SRC PORT）：80，标识响应方的端口（HTTP 服务）。
  - 目标端口（DEST PORT）：1031，标识请求方的端口。
  - 序列号（SEQUENCE NUM）：0，用于标识从 TCP 源端发送的数据字节流的顺序号。
  - 确认号（ACK NUM）：1，用于确认收到对方发送的数据，这里的 1 表示确认收到了包含序列号为 0 的 SYN 报文。
  - 偏移（OFF.）和 保留（RES.）：TCP 头部的长度和保留位，通常用于控制标志。
  - SYN+ACK：设置这两个标志位表示响应连接请求并要求确认。

- 窗口（WINDOW）：控制从对方接收的数据量，此处未显示具体值。
- 校验和（CHECKSUM）：0x0，用于检测数据在传输过程中的任何错误。
- 紧急指针（URGENT POINTER）：当 URG 标志被设置时，表示这个字段是有效的，此处显示为未设置。
- 选项（OPTION）和 填充（PADDING）：TCP 头部可能包含的选项和为了字节对齐而添加的填充字节。



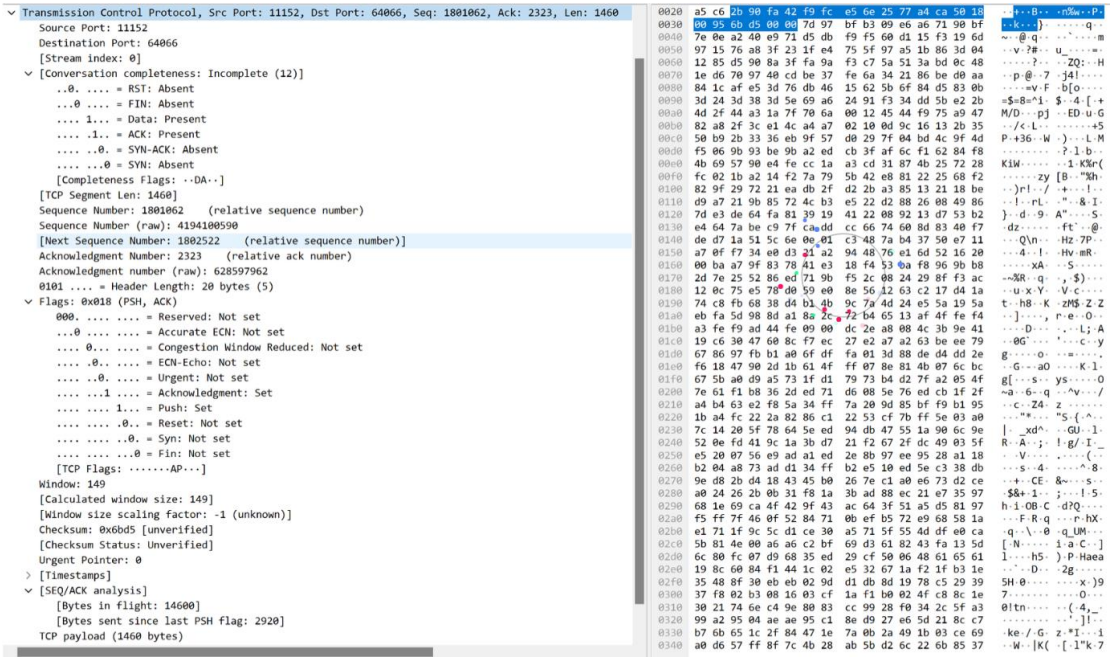
- 数据传输分析
  - 这个 SYN-ACK 报文是 TCP 三次握手过程中的第二步，用于确认之前收到的 SYN 请求，并要求对方确认本次连接的有效性。接下来期待的是客户端（源端口 1031）对此 SYN-ACK 的确认，发送一个仅设置 ACK 标志位的 TCP 报文，这将完成三次握手过程，建立 TCP 连接。

2. 仔细研读 TCP 连接建立过程数据报文。

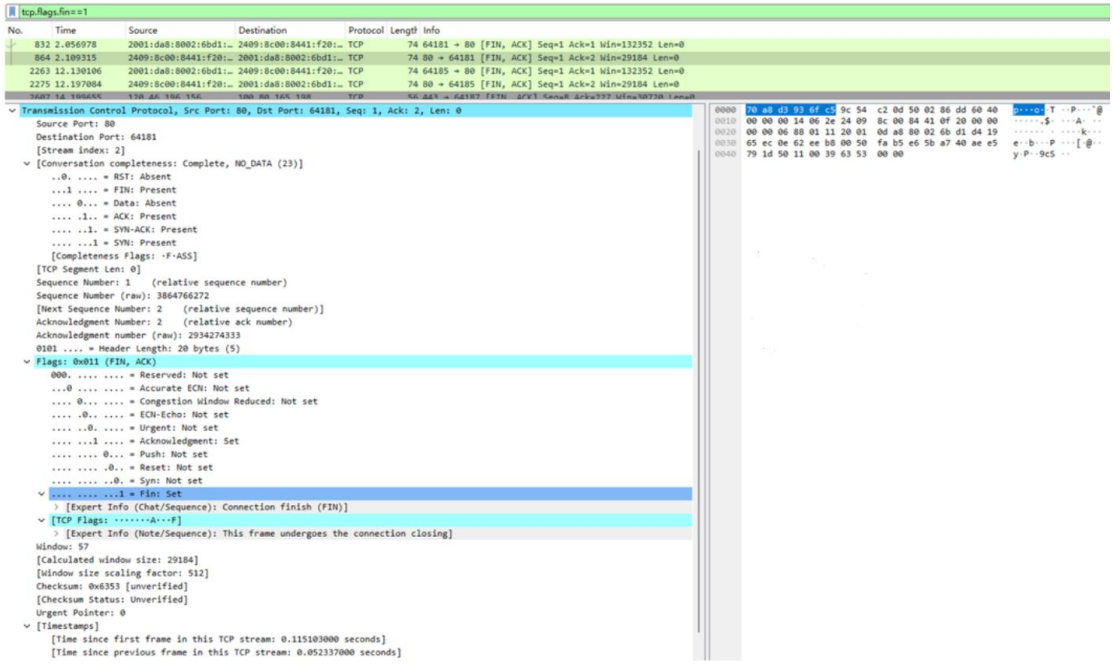
- 主要 TCP 字段解析
  - 源端口号（Source Port）：11152，标识发送方的应用层端口。
  - 目的端口号（Destination Port）：64066，标识接收方的应用层端口。
  - 序列号（Sequence Number）：4194102590，这是此 TCP 段发送的数据的第一个字节的序列号。

- 确认号（Acknowledgment Number）：2323，这表示接收方期待的下一个字节的序列号，确认了接收方已经成功接收的数据。
- 数据偏移（Header Length）：20 字节，指示 TCP 头部的长度，表明此 TCP 段没有包含额外的选项。
- 标志位（Flags）：PSH, ACK。PSH 标志位提示接收方应该立即将这些数据传递给应用层，而不是在缓冲区中等待更多的数据。ACK 标志位确认接收到的数据。
- 窗口大小（Window）：149，这表示接收方当前的接收窗口大小，告知发送方它还能接收多少字节的数据，用于流控制。
- 校验和（Checksum）：0x6bd5，用于验证接收到的数据在传输过程中是否出现错误。这个值是对整个 TCP 段（包括 TCP 伪头部，TCP 头部和数据）计算得出的。
- 紧急指针（Urgent Pointer）：0，由于 URG 标志没有设置，这个字段不被使用。

- 数据包分析
  - 此数据包的 PSH 和 ACK 标志位被设置，表明这是一个在数据传输中间阶段的包，发送方不仅发送数据还确认之前接收的数据。ACK 标志常用于所有接收到数据的确认响应中，而 PSH 标志用于指示接收方应立即处理这些数据，这常见于需要快速响应的应用，如实时通信应用。



3. 仔细研读 TCP 拆链过程数据报文。



- 主要 TCP 字段解析
  - 源端口（Source Port）：80，通常用于 HTTP 服务的端口，表示发送方的端口。
  - 目的端口（Destination Port）：64181，表示接收方的端口。
  - 序列号（Sequence Number）：1，这是相对序列号，Wireshark 显示为 1，表示这是相对于 TCP 连接初始序列号的序列号。
  - 确认号（Acknowledgment Number）：293474333，这是相对确认号，表示接收方已经收到对方发送的数据直到这个序号。
  - 标志位（Flags）：FIN, ACK。FIN 标志用于通知接收方发送方已完成发送数据并希望建立终止连接，ACK 标志是对之前接收到的 TCP 段的确认。
  - 窗口大小（Window）：57，这指示接收方当前的接收窗口大小，告知发送方它还能接收多少字节的数据，这对于流量控制很重要。
  - 校验和（Checksum）：0x6353，用于验证接收到的数据在传输过程中的完整性和正确性。
  - 紧急指针（Urgent Pointer）：0，由于紧急标志(URG)未被设置，此字段不被使用。
- 连接拆除分析

  这个 TCP 段标志着一个 TCP 连接的结束阶段之一。当一个 TCP 连接准备关闭

时，一个端点会发送一个 FIN 标志位的段。这里，端口 80 发送了一个包含 FIN 和 ACK 标志的 TCP 段，目的是通知接收端（端口 64181），它已经完成了数据传输，并希望建立终止连接。

这种 FIN 和 ACK 的组合也是对接收端之前发送的任何未确认数据的确认。接下来的期待是接收端响应一个 ACK，确认这个 FIN 段，然后发送自己的 FIN 段，如果还有待发送的数据，则在此之后发送。最终，发送端将确认这个 FIN，从而完成四次挥手过程，彻底关闭连接。

【分析讨论】

一、在 Packet Tracer 中 TCP 报文情况

在 Packet Tracer 模拟环境中，TCP 报文被详细模拟，展现了从 TCP 三次握手到四次挥手的全过程。通过模拟，可以观察到报文的发送和接收，以及在不同 TCP 状态转换时各种控制位的变化。

二、TCP 报文字段内容

TCP 报文的字段结构包括源端口、目的端口、序列号、确认号、数据偏移、控制位、窗口、校验和、紧急指针等。这些字段合作确保了 TCP 的可靠传输，其中序列号和确认号为核心机制，支持数据的有序传送和重传机制。窗口大小字段则关系到流量控制，而控制位如 SYN、ACK、FIN 等则是连接管理的基础。

三、TCP 连接建立过程数据报文

TCP 连接的建立过程，即三次握手，涉及 SYN 和 ACK 报文的交换。首先，客户端发送 SYN 报文请求建立连接；接着，服务器回应 SYN-ACK 报文；最后，客户端再发送 ACK 报文确认，完成连接建立。这个过程确保了双方的序列号和确认号能被正确同步，是建立可靠通信的基石。

四、TCP 拆链过程数据报文

TCP 连接的终止过程，即四次挥手，涉及 FIN 和 ACK 报文的交换。这个过程开始于发送方发送一个 FIN 报文，请求关闭连接。接收方确认这个 FIN 报文，并可能继续发送数据直到也发送 FIN 报文。发送方确认这个 FIN 后，连接终止。这一过程确保了双方数据的完整传输，即使在关闭连接时。