**实验七 传输控制协议TCP仿真实验**

**【实验目的】**

1. 掌握TCP协议的报文格式。

2. 理解TCP连接过程。

**【实验学时】**

2学时

**【实验性质】**

验证性实验

**【实验环境】**

Cisco Packet Tracer 7.2模拟器

**【实验报告】**

1. 什么是TCP协议？(20分)

传输控制协议（Transmission Control Protocol，简称TCP）是一种面向连接的、可靠的、基于字节流的通信协议。它主要应用于互联网中的数据传输，是互联网协议套件（Internet Protocol Suite）的一部分，通常与IP协议（Internet Protocol）一起使用，被称为TCP/IP协议栈。

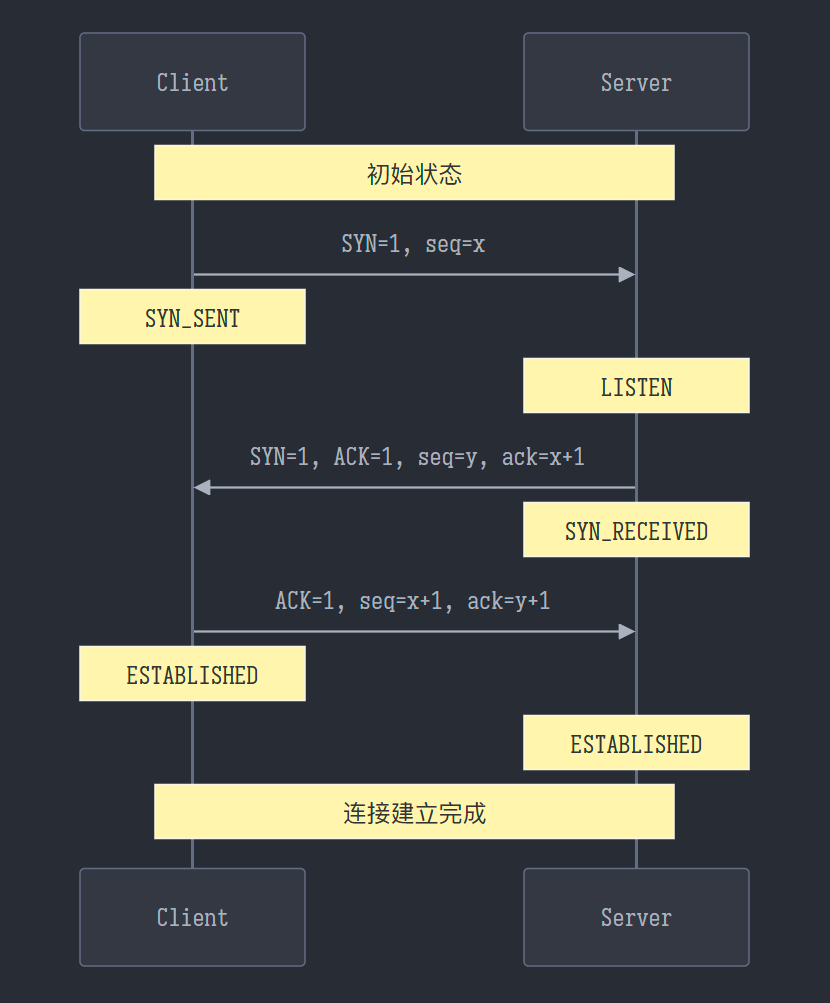
#### 主要特点：

* **面向连接**：在数据传输前需要建立连接，确保双方都已准备好接收或发送数据。这种连接机制类似于电话系统，在通话开始之前先拨号建立连接。
* **可靠性**：通过确认机制、重传机制、错误检测等技术保证数据能够准确无误地从发送端传输到接收端。如果发送的数据包丢失或损坏，TCP会自动请求重新发送。
* **流量控制**：通过滑动窗口机制来避免发送方发送的数据量超过接收方处理能力，从而导致数据溢出或丢失。
* **拥塞控制**：当网络出现拥塞时，TCP协议能够减少数据发送速率以缓解网络拥堵情况，防止网络性能进一步恶化。
* **有序性**：即使数据在网络中乱序到达，TCP也能将它们按照正确的顺序重组后交给应用程序。
* **数据校验**：使用校验和机制来检查数据完整性，确保接收到的数据没有发生错误。

#### 应用场景：

TCP适用于那些要求高可靠性和完整性的应用场合，例如文件传输、电子邮件、网页浏览等服务。这些应用需要确保所有数据都能正确无误地到达目的地，因此选择使用TCP协议。

1. 画出TCP三次握手状态图，并简述TCP三次握手的过程。(40分)



让我详细解释TCP三次握手的过程：

1. 第一次握手（客户端发起）：
   * 客户端处于CLOSED状态，服务器处于LISTEN状态
   * 客户端发送SYN报文（SYN=1，seq=x）
   * 客户端进入SYN\_SENT状态
2. 第二次握手（服务器响应）：
   * 服务器收到SYN报文
   * 服务器发送SYN+ACK报文（SYN=1，ACK=1，seq=y，ack=x+1）
   * 服务器进入SYN\_RECEIVED状态
3. 第三次握手（客户端确认）：
   * 客户端收到SYN+ACK报文
   * 客户端发送ACK报文（ACK=1，seq=x+1，ack=y+1）
   * 客户端进入ESTABLISHED状态
   * 服务器收到ACK后也进入ESTABLISHED状态
   * 连接建立完成

三次握手的主要目的：

1. 确认双方的发送和接收能力都正常
2. 同步双方的序列号（seq）和确认号（ack）
3. 协商一些连接参数

通过这三次握手，TCP连接正式建立，双方可以开始可靠的数据传输。

1. 为什么在TCP连接过程中要使用三次握手？如不这样做可能会出现什么情况。(30分)

TCP协议在建立连接时采用三次握手（Three-Way Handshake）的方式，主要是为了确保连接的可靠性和防止错误连接的发生。三次握手的过程包括以下几个步骤：

1. **第一次握手**：客户端向服务器发送一个SYN（同步序列编号 Synchronize Sequence Numbers）报文段，并进入SYN\_SEND状态，等待服务器确认。
2. **第二次握手**：服务器收到客户端的SYN报文段后，会回复一个SYN+ACK（同步确认 Synchronize Acknowledgment）报文段，表示接受客户端的连接请求，并进入SYN\_RECV状态。
3. **第三次握手**：客户端收到服务器的SYN+ACK报文段后，再发送一个ACK（确认 Acknowledgment）报文段给服务器，确认连接建立成功，此时客户端和服务器都进入ESTABLISHED状态，可以开始进行数据传输。

**使用三次握手的原因：**

1. **确保双方都准备好**：三次握手确保了客户端和服务器双方都已经准备好进行数据交换。只有当双方都确认对方的存在并准备好接收数据时，连接才真正建立起来。
2. **防止已失效的连接请求**：三次握手可以防止由于网络延迟或其他原因导致的旧连接请求报文段再次到达服务器，从而引起错误连接。例如，假设客户端发送了一个连接请求但未收到响应，客户端可能会重新发送请求。如果不采用三次握手，服务器可能会因为收到了重复的请求而误以为新的连接请求到来，从而创建不必要的连接。
3. **同步序列号**：三次握手过程还允许双方同步初始序列号（ISN, Initial Sequence Number），这对于后续的数据传输非常重要，可以确保数据包按顺序到达。

**如果不使用三次握手可能出现的情况：**

1. **连接失败**：如果没有三次握手，客户端和服务器可能无法确认对方是否已经准备好接收数据，导致连接建立失败。
2. **错误连接**：旧的连接请求报文段可能会因为网络延迟等原因再次到达服务器，如果不经过三次握手验证，服务器可能会误认为这是一个新的连接请求，从而创建不必要的连接，浪费资源。
3. **数据混乱**：如果缺少三次握手，客户端和服务器之间的序列号可能不同步，导致数据包乱序或丢失，影响数据传输的可靠性。
4. **安全风险**：三次握手还可以作为一种简单的安全措施，防止恶意攻击者通过伪造连接请求来消耗服务器资源。

综上所述，三次握手是TCP协议中一个非常重要的机制，它不仅确保了连接的可靠性，还有效防止了错误连接和资源浪费等问题。希望这部分内容能帮助你更好地理解TCP连接过程中的三次握手机制及其重要性。

1. 实验总结。(10分)

通过本次精心设计的实验，我们不仅系统地掌握了TCP（传输控制协议）的报文格式这一核心技术细节，而且深刻领悟到了TCP连接建立过程中三次握手机制的精妙与必要性。三次握手，作为TCP协议确保连接可靠性的基石，其通过一系列严谨的信息交换步骤——即客户端发送SYN请求、服务器响应SYN-ACK、客户端再确认ACK——来确认双方均具备通信能力，且网络路径畅通无阻，从而为后续的数据传输奠定了坚实的基础，保障了数据传输的准确性、顺序性和完整性。

在实验过程中，我们充分利用了Wireshark这一强大的网络协议分析工具，它如同一扇透视网络流量的窗口，使我们能够细致入微地观察和分析TCP报文段。从TCP报文的头部结构，包括源端口、目的端口、序列号、确认号、标志位（如SYN、ACK等）到选项字段，每一项数据都被清晰地呈现出来。通过对这些报文段的逐一剖析，我们不仅直观地见证了三次握手的全过程，还深入理解了TCP如何通过序列号、确认号以及窗口大小等机制来实现流量控制、拥塞控制和错误恢复等高级功能。

此外，实验中的实践操作环节极大地锻炼了我们的动手能力。面对实际网络环境中复杂多变的数据包，我们学会了如何高效地过滤、搜索和分析特定类型的TCP报文，以及如何根据报文内容诊断网络连接问题。例如，通过分析TCP重传现象，我们理解了网络延迟和丢包对传输性能的影响；通过观察TCP窗口更新，我们体会到了流量控制的动态调整过程。这些实践经验不仅加深了我们对TCP协议内在工作机制的理解，也提高了我们解决实际网络问题的能力。

更重要的是，本次实验促进了理论知识与实践技能的深度融合。原本抽象的TCP协议概念，在亲手操作Wireshark分析真实数据包的过程中变得生动具体。我们学会了如何将课本上的理论知识应用于实际场景，如何在遇到问题时运用所学知识进行分析和推理，这种“学以致用”的过程极大地增强了我们的学习兴趣和自信心，同时也为我们的专业成长和未来职业发展奠定了坚实的基础。

实验成绩：

批改时间：

评阅教师：