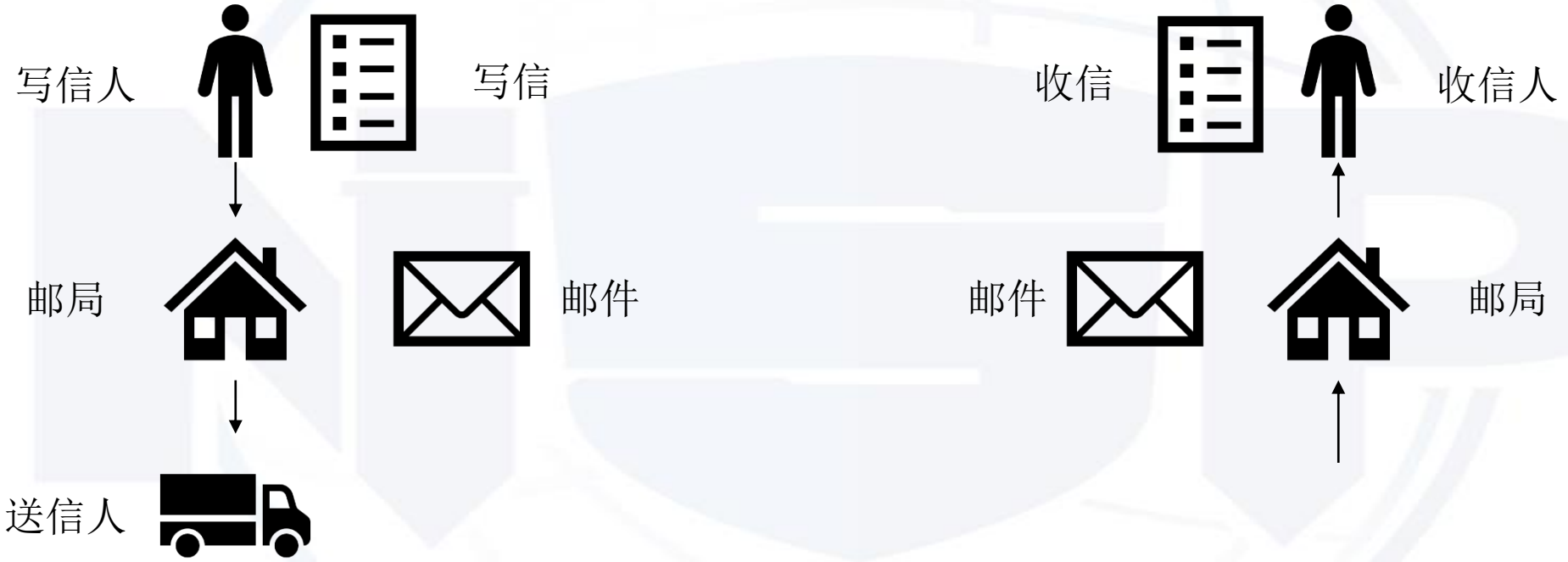
国家信息安全水平考试
NATIONAL INFORMATION SECURITY TEST PROGRAM

计算机网络分层模型及wireshark抓包

目录

分层思想

- 邮局寄信件

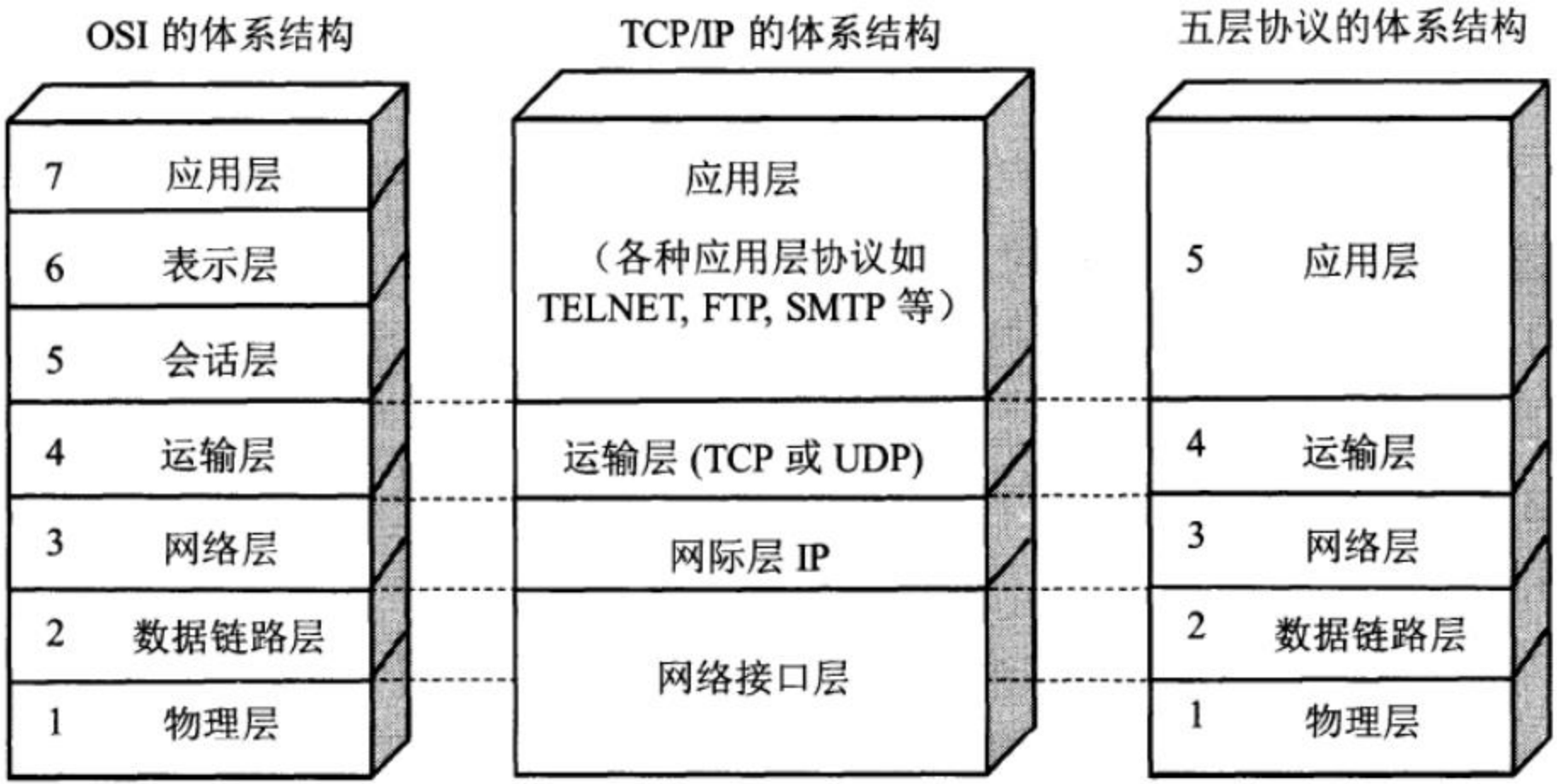


分层思想

- 1974年，ISO组织发布了OSI七层参考模型
- ISO/OSI七层参考模型
- 国际标准化组织（ISO，International Organization for Standardization）
- 开放式系统互联通信参考模型（OSI，Open System Interconnection Reference Model）

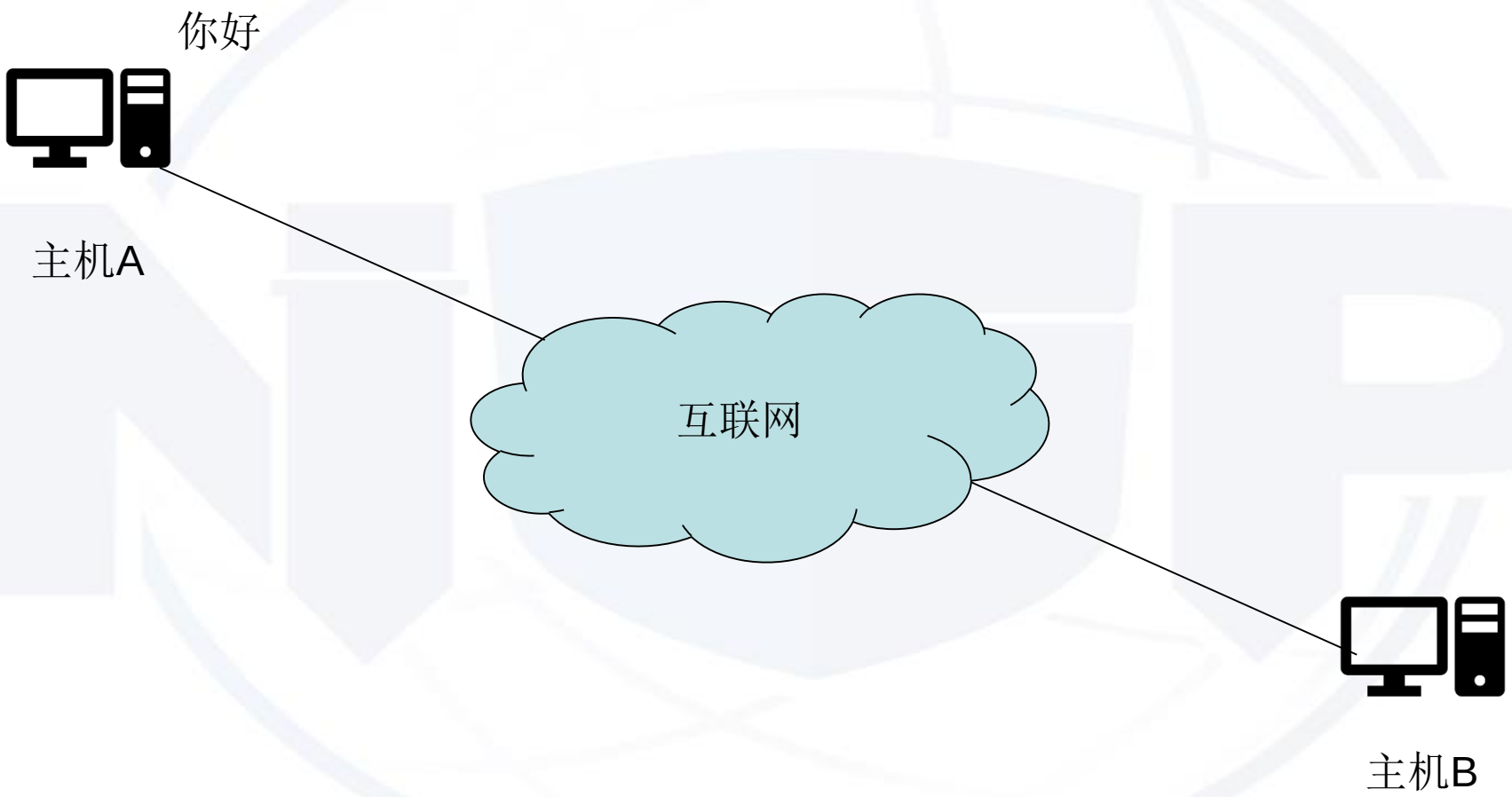
OSI模型特点

TCP/IP协议结构



目录

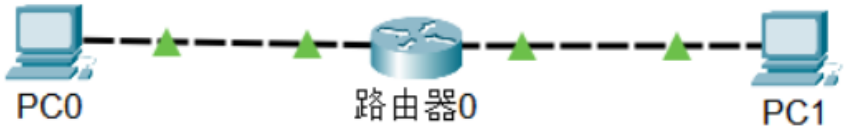
数据传输过程

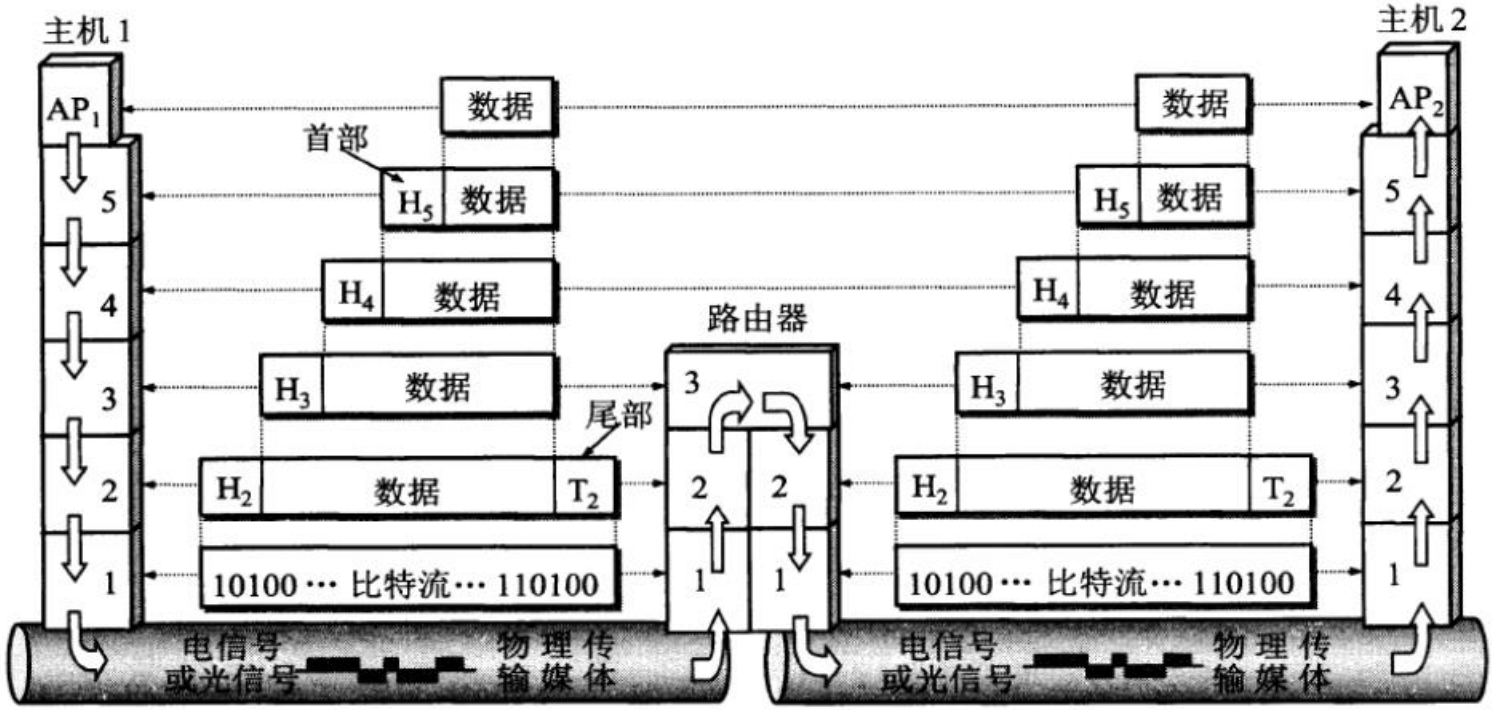


数据传输过程

数据传输过程

- 数据封装与分用（解封装）





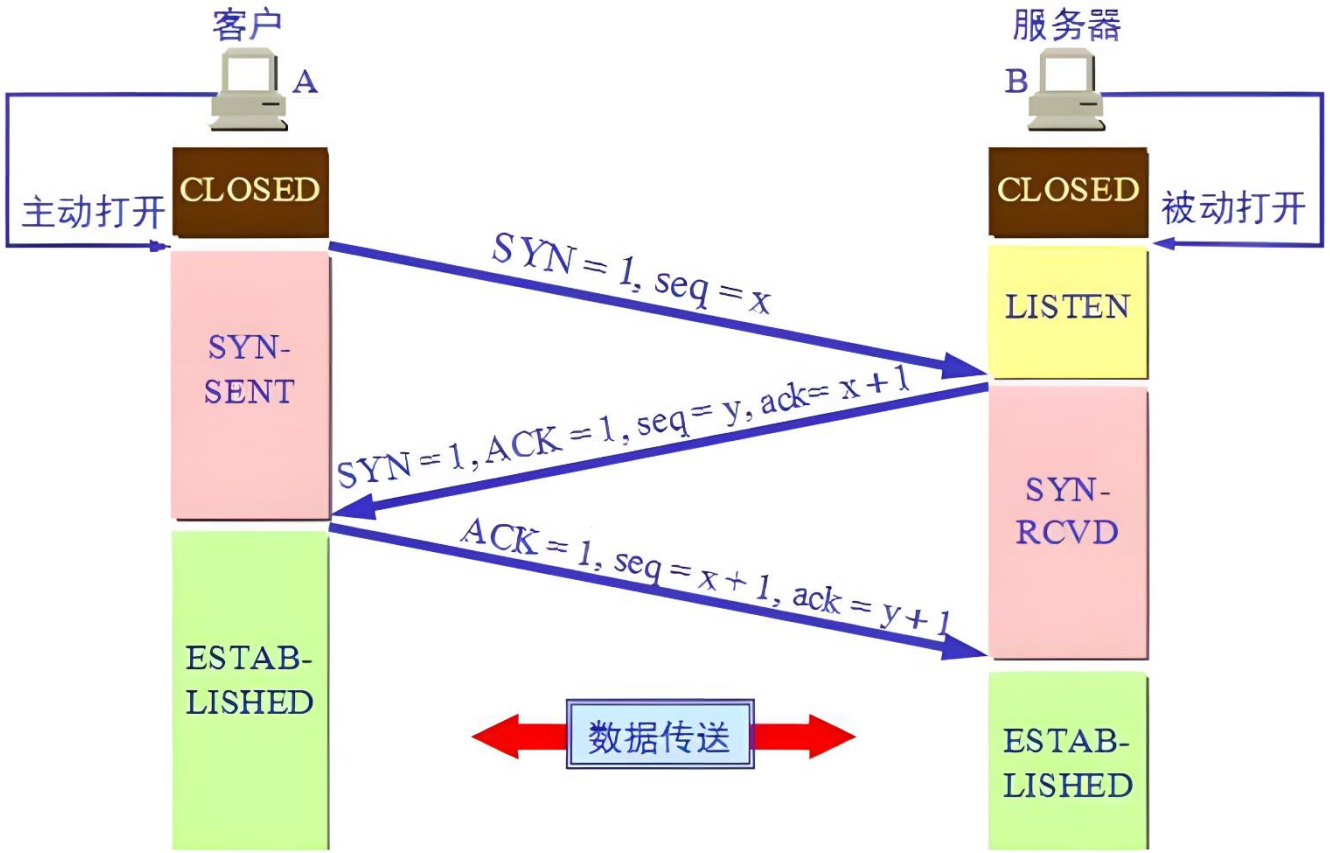
传输层协议-TCP（传输控制协议）

- 提供面向连接的、可靠的数据通信服务
- 提供可靠性服务
  - 数据包分块、发送接收确认、超时重发、数据校验、数据包排序、控制流量

<table>
<tr><td colspan="8">16位源端口号</td><td colspan="2">16位目的端口号</td></tr>
<tr><td colspan="10">32位序号</td></tr>
<tr><td colspan="10">32位确认序号</td></tr>
<tr><td>偏移量</td><td>保留位</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td colspan="2">16位窗口指针</td></tr>
<tr><td colspan="8">16位校验和</td><td colspan="2">16位紧急指针</td></tr>
<tr><td colspan="10">数据</td></tr>
</table>

数据传输过程

TCP三次握手



1.在建立连接之前，B先创建TCB（传输控制块），准备接受客户进程的连接请求，处于LISTEN（监听）状态

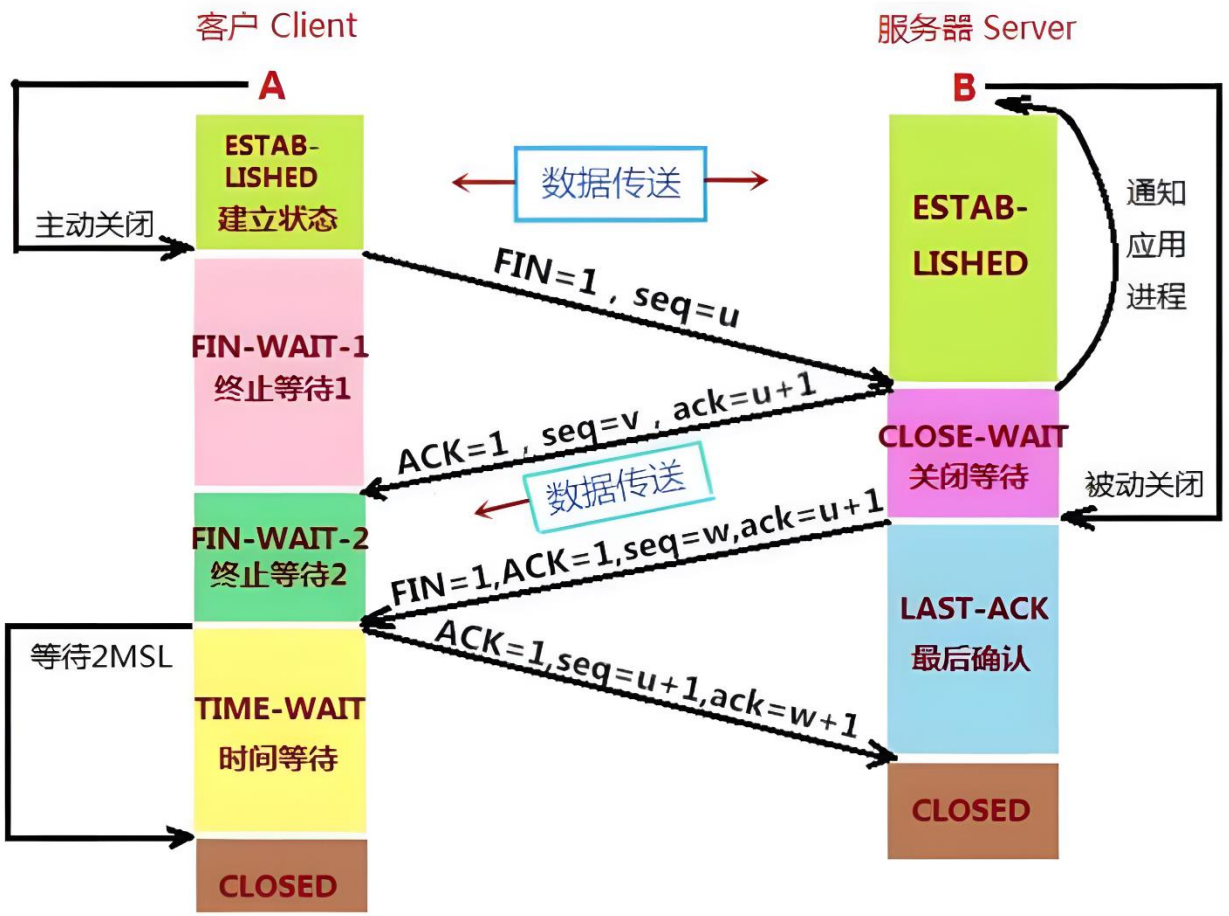
2.A首先创建TCB，然后向B发出连接请求，SYN置1，同时选择初始序号seq=x，进入SYN-SEND（同步已发送）状态

3.B收到连接请求后向A发送确认，SYN置1，ACK置1，同时产生一个确认序号ack=x+1。同时随机选择初始序号seq=y，进入SYN-RCVD（同步收到）状态

4.A收到确认连接请求后，ACK置1，确认号ack=y+1，seq=x+1，进入到ESTABLISHED（已建立连接）状态。向B发出确认连接，最后B也进入到ESTABLISHED（已建立连接）状态。

数据传输过程

TCP四次挥手



1.A发送一个FIN，用来关闭A到B的数据传送，A进入FIN_WAIT_1状态。

2.B收到FIN后，发送一个ACK给A，确认序号为收到序号+1（与SYN相同，一个FIN占用一个序号），B进入CLOSE_WAIT状态。

3.B发送一个FIN，用来关闭B到A的数据传送，B进入LAST_ACK状态。

4.A收到FIN后，A进入TIME_WAIT状态，接着发送一个ACK给B，确认
序号为收到序号+1，B进入CLOSED状态，完成四次挥手

传输层协议-TCP（传输控制协议)

为什么建立连接是三次握手，关闭连接确是四次挥手呢？

建立连接的时候， 服务器在LISTEN状态下，收到建立连接请求的SYN报文后，把ACK和SYN放在一个报文里发送给客户端。
而关闭连接时，服务器收到对方的FIN报文时，仅仅表示对方不再发送数据了但是还能接收数据，而自己也未必全部数据都发送给对方了，所以己方可以立即关闭，也可以发送一些数据给对方后，再发送FIN报文给对方来表示同意现在关闭连接，因此，己方ACK和FIN一般都会分开发送，从而导致多了一次。

14

传输层协议-UDP(用户数据报协议)

- 提供面向事务的简单不可靠信息传送服务
- 特点
  - 无连接、不可靠
  - 协议简单、占用资源少，效率高

16位源端口号	16位目的端口号
16位UDP报文长度	16位校验和
数据	

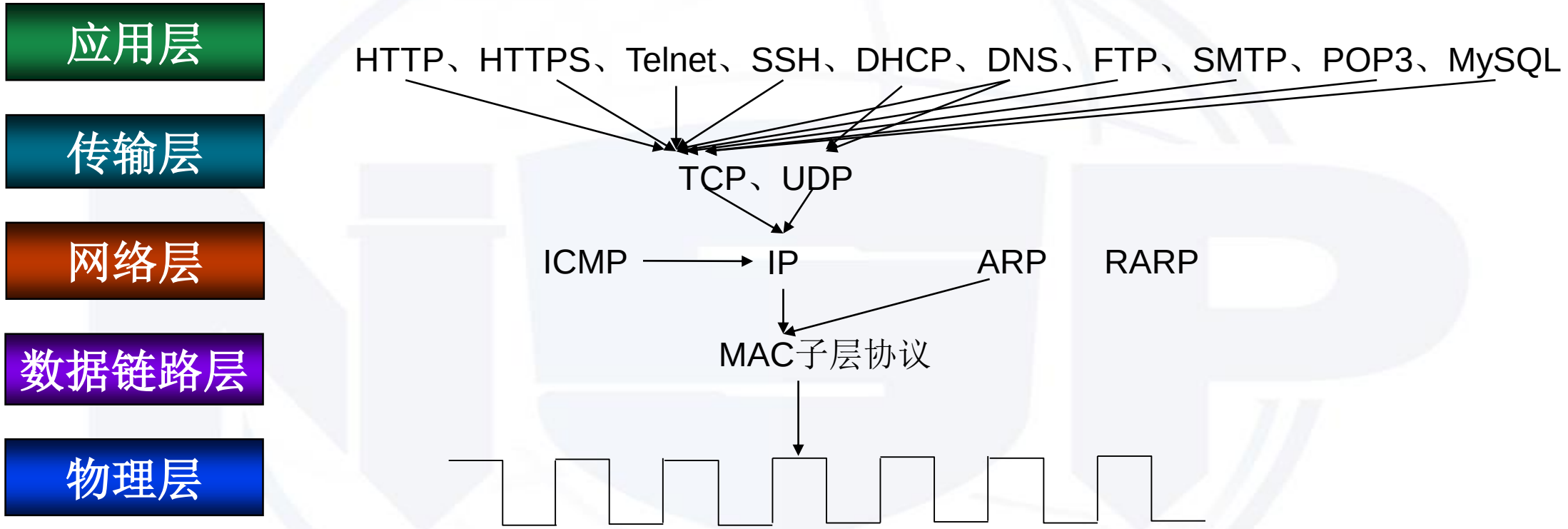
传输层安全问题

- 实验一：两台PC间tcp、udp通信
- 实验二：使用wireshark抓tcp三次握手包
- 实验三：使用wireshark抓tcp四次挥手包

目录

- 分层模型
  - ISO/OSI七层模型
  - TCP/IP协议
- 数据传输过程
  - 数据封装与分用（解封装）
- TCP/IP协议栈

TCP/IP协议



TCP/IP协议

协议	端口号
FTP（简单数据传输）	20/21
SSH（安全加密外壳）	22
Telnet（远程登陆）	23
SMTP（电子邮件传输协议）	25
DNS（域名系统）	53
DHCP（动态主机配置协议）	67/68
HTTP（超文本传输协议）	80
POP3（邮局协议的第三个版本）	110
HTTPS（超文本传输安全协议）	443
RDP（远程桌面协议）	3389
MySQL	3306
SQL server	1433
Oracle	1521

总结

- 分层模型
  - ISO/OSI七层模型
  - TCP/IP协议
- 数据传输过程
  - 数据封装与分用（解封装）
- TCP/IP协议栈

国家信息安全水平考试

NATIONAL INFORMATION SECURITY TEST PROGRAM

谢谢