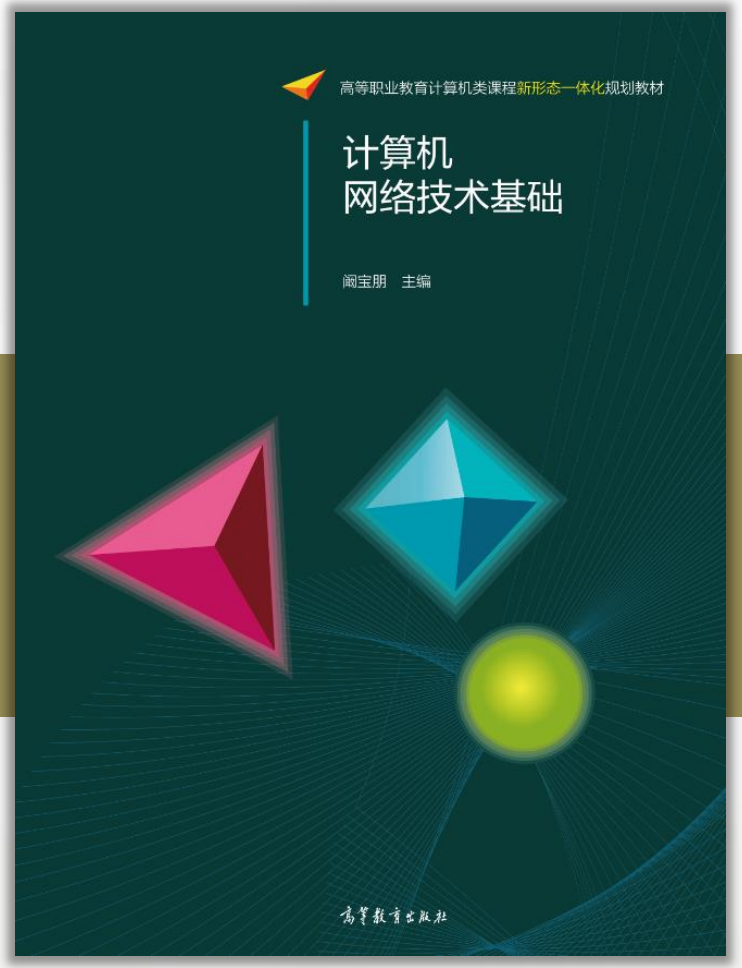


新形态一体化教材 配套MOOC课程

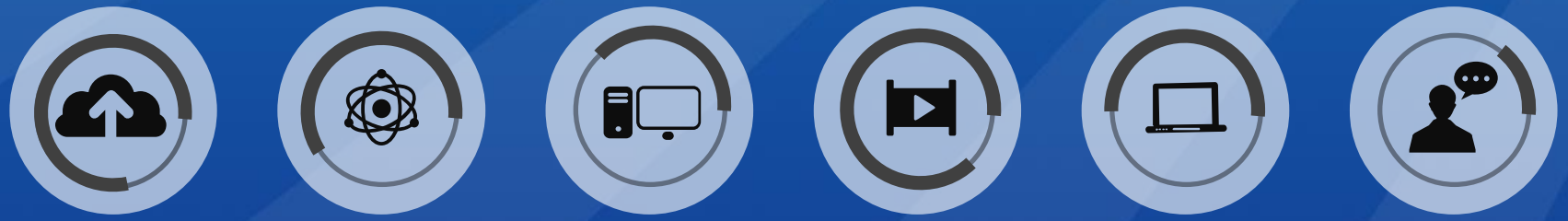
计算机网络技术基础

主编 阚宝朋 高等教育出版社
书号：978-7-04-043546-7

扫描教材上二维码 实现随扫随学

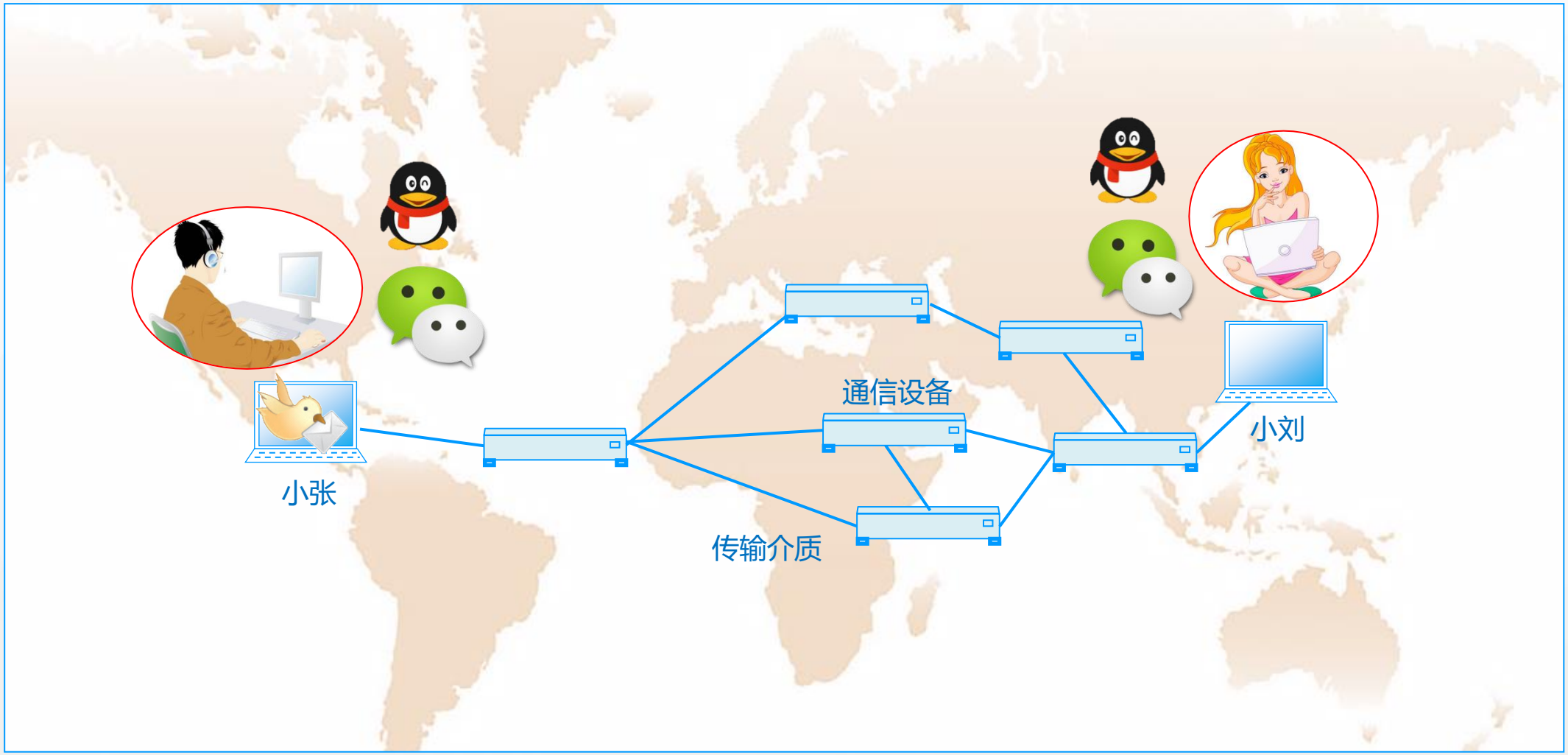
高等教育出版社
HIGHER EDUCATION PRESS

传输层的主要功能



高等教育出版社
HIGHER EDUCATION PRESS

传输层的主要功能



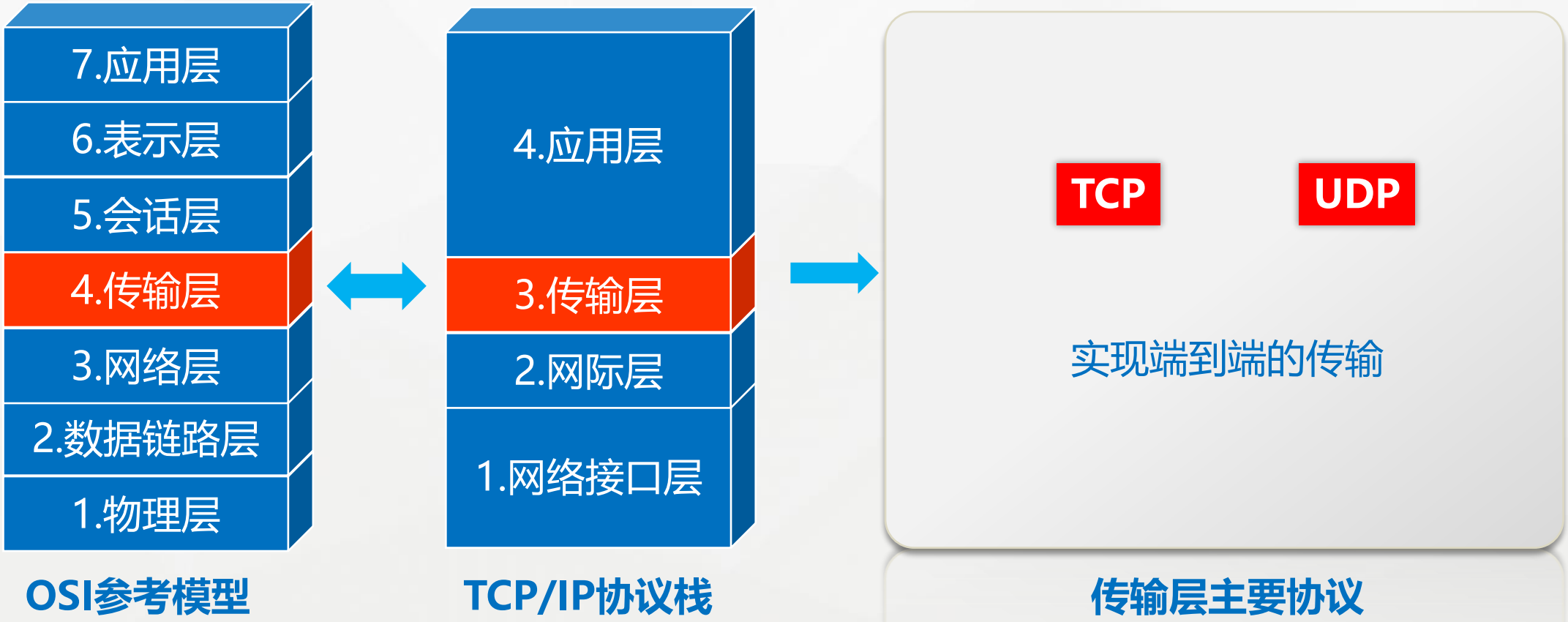
传输层关注的是：数据包在通信双方的终端上是如何知道将数据发送给哪个应用程序的呢

目录
Contents

学习目标

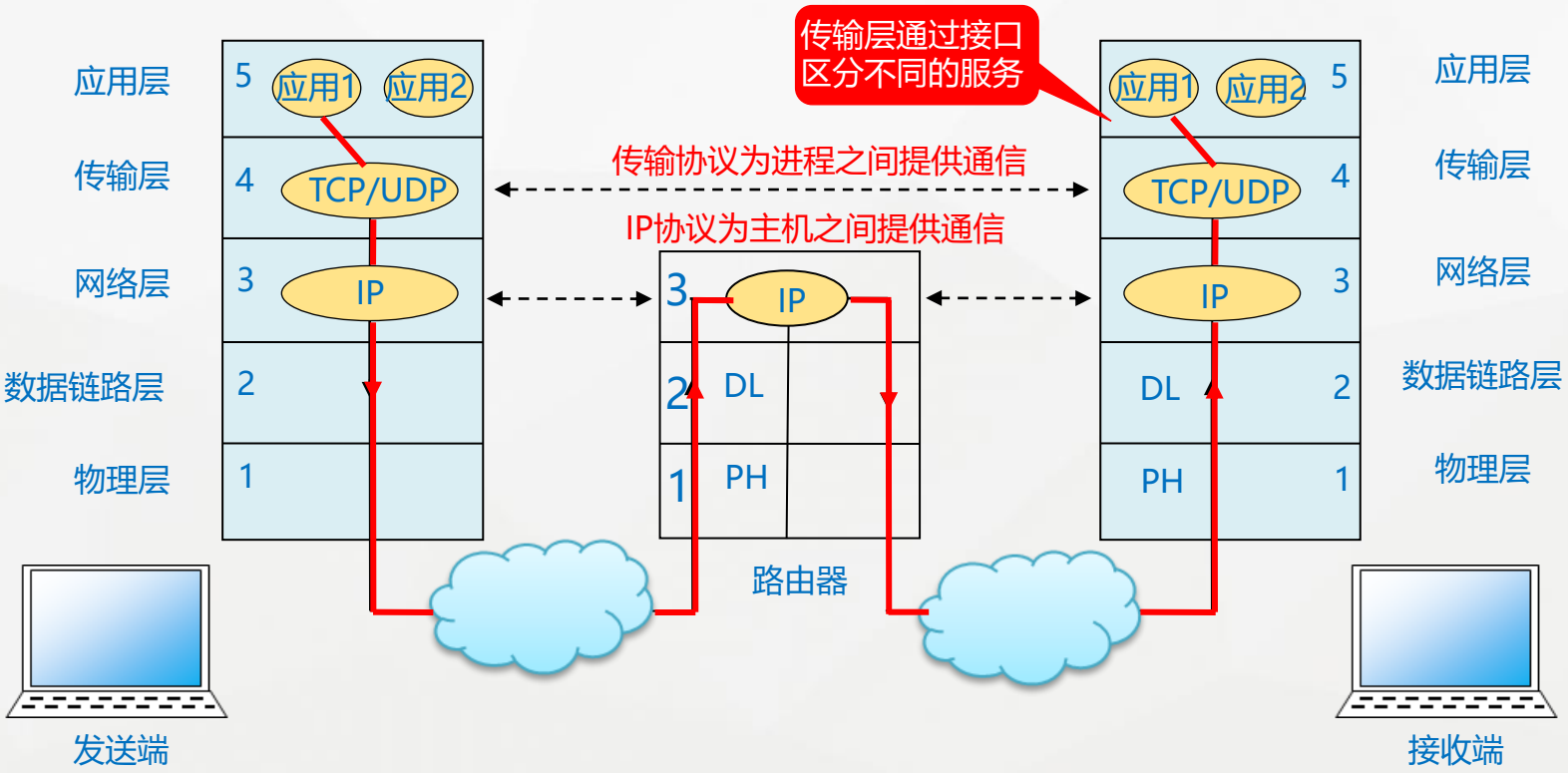
- 了解传输层功能
- 了解传输层与网络层关系
- 理解传输层通信方式

1.传输层概述

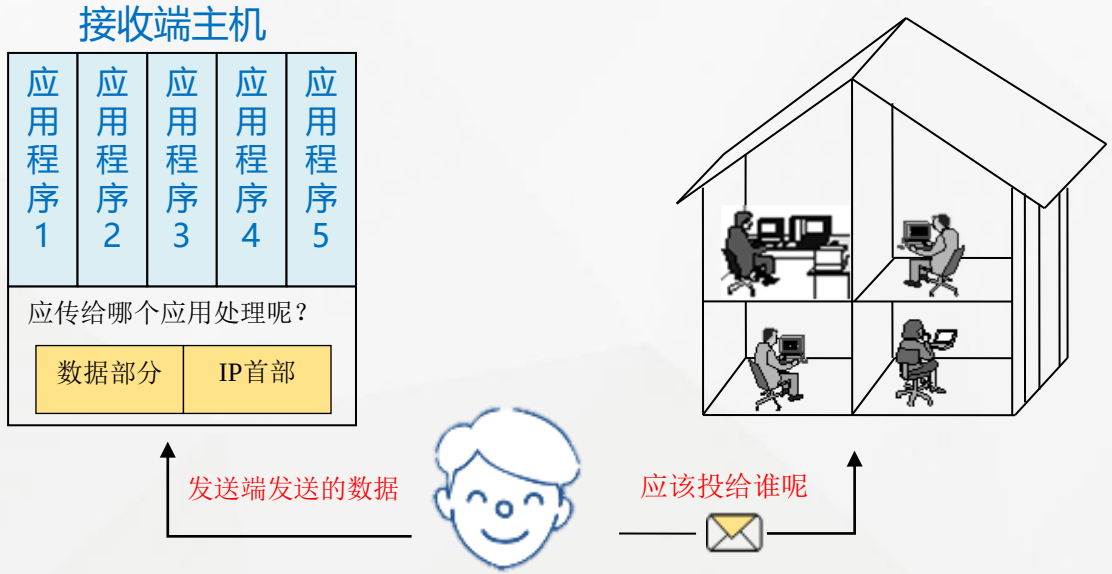

7.应用层
6.表示层
5.会话层
4.传输层
3.网络层
2.数据链路层
1.物理层
OSI参考模型
4.应用层
3.传输层
2.网际层
1.网络接口层
TCP/IP协议栈
TCP
UDP
实现端到端的传输
传输层主要协议

2.传输层与上下层关系

传输层主要是在网络层在通信两端已经建立连接的基础上实现端到端的传输



2.传输层与上下层关系



主机（终端系统）=A/B单位

网络层协议=邮寄服务（包括邮递员）

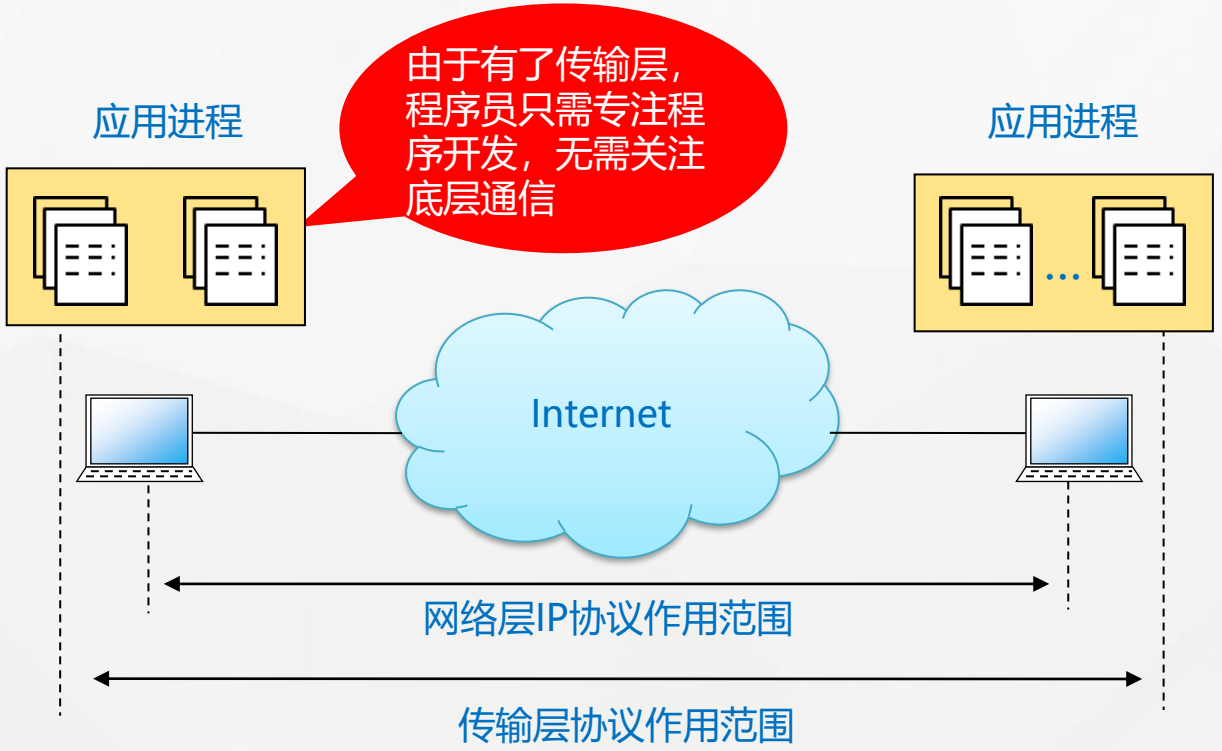
传输层协议=单位收发员

进程=单位员工

端口=单位员工的姓名

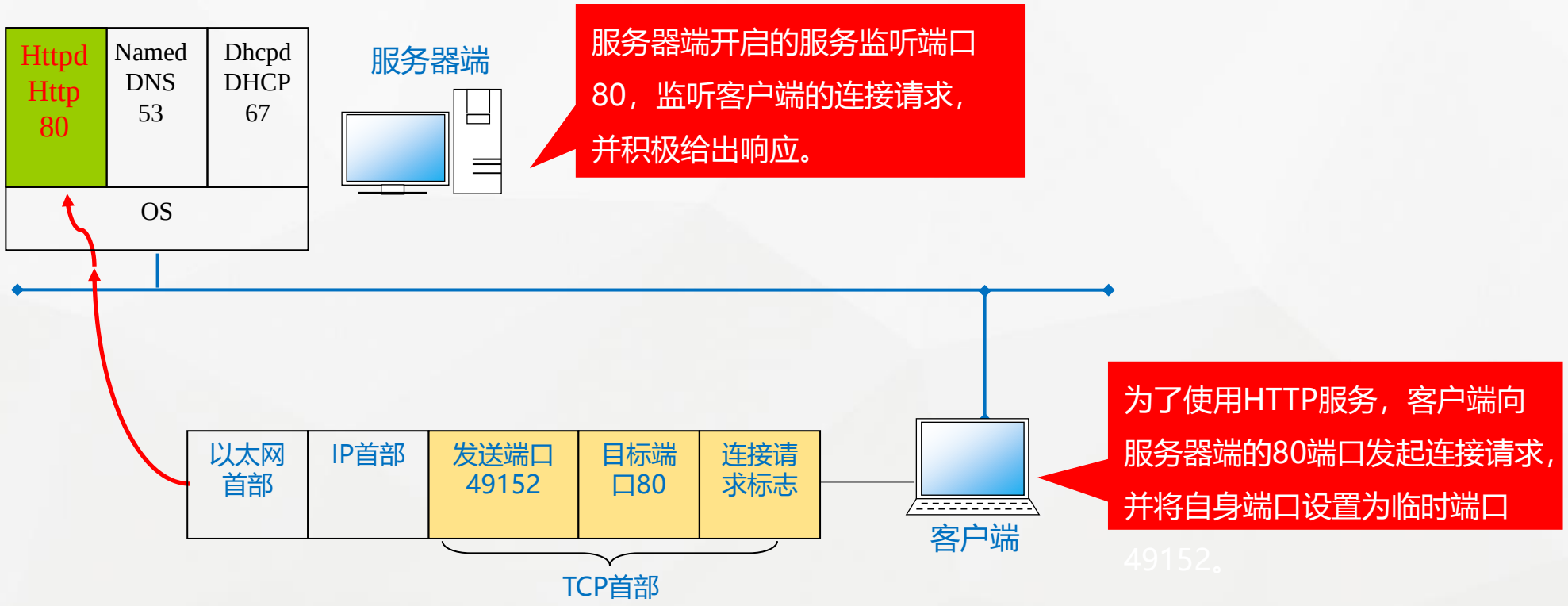
应用程序消息=信封里的信

2.传输层与上下层关系



1. 差错控制
2. 流量控制
3. 拥塞控制

3.传输层通信过程举例


Httpd
Http
80
Named
DNS
53
Dhcpd
DHCP
67
OS
服务器端
服务器端开启的服务监听端口80，监听客户端的连接请求，并积极给出响应。
以太网首部
IP首部
发送端口49152
目标端口80
连接请求标志
TCP首部
客户端
为了使用HTTP服务，客户端向服务器端的80端口发起连接请求，并将自身端口设置为临时端口49152。

传输层协议特点

高等教育出版社
HIGHER EDUCATION PRESS

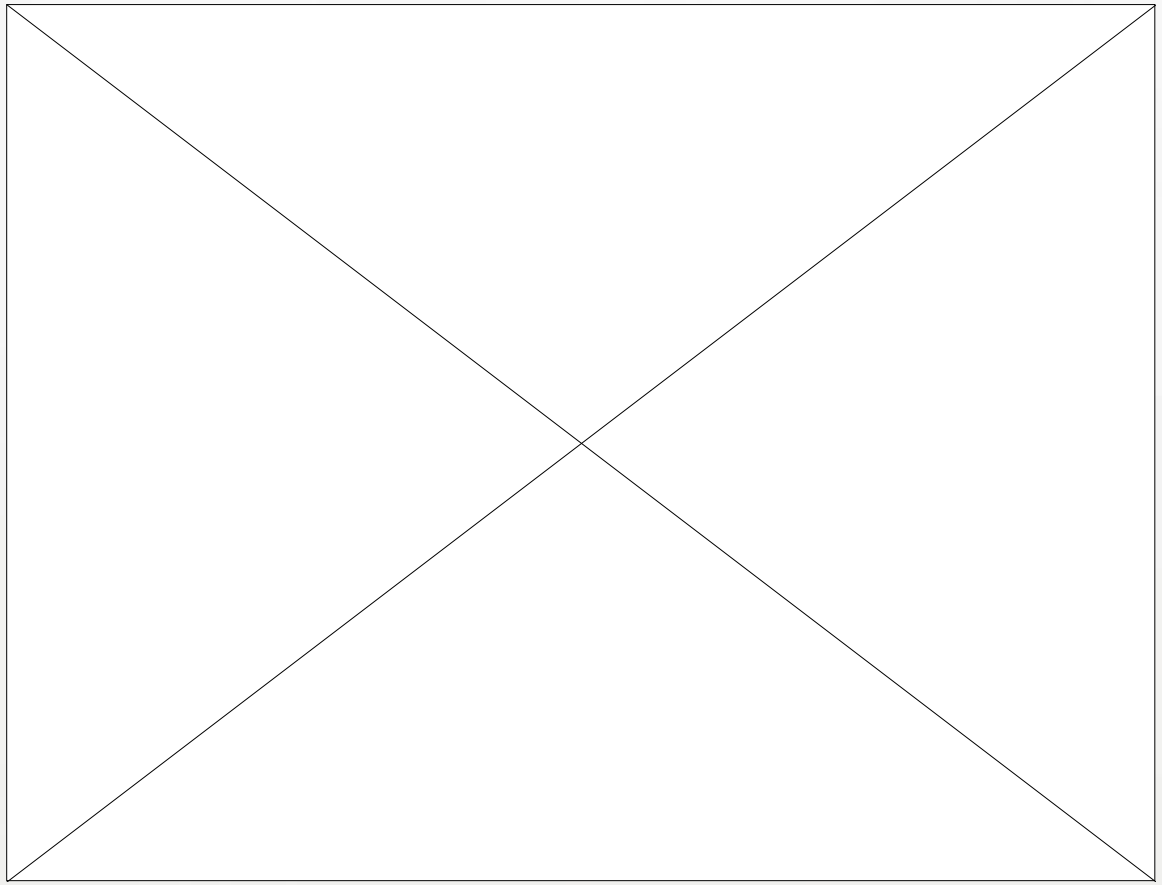
目录
Contents

学习目标

- 了解面向连接的含义
- 了解面向无连接的含义

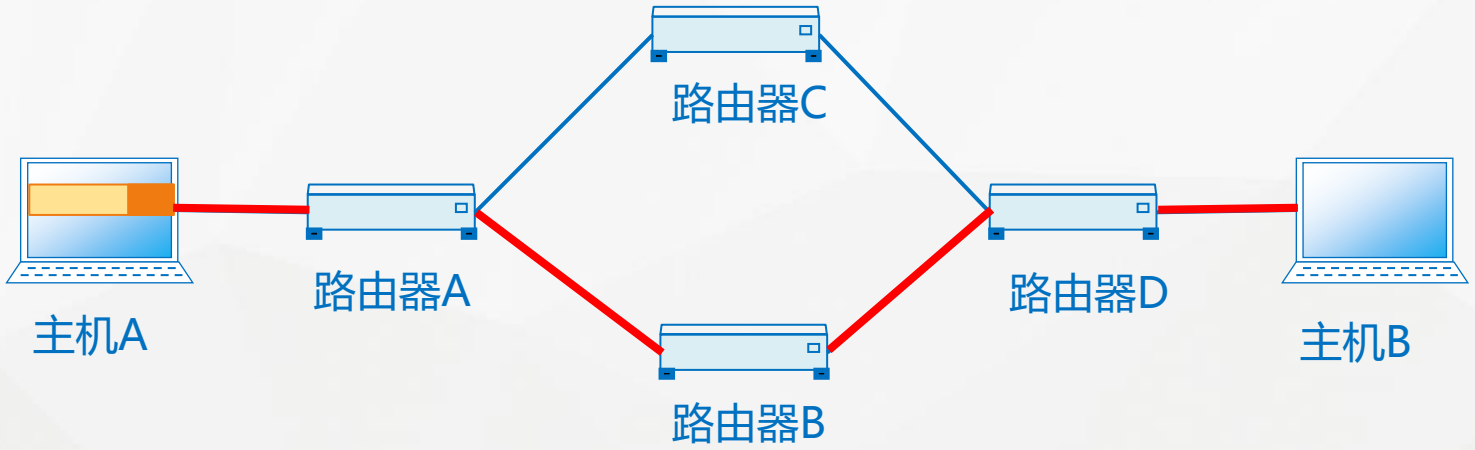
1.面向连接的TCP

面向连接的会话建立的通信信道是一条逻辑链路，TCP协议属于面向连接的协议。



1.面向连接的TCP

面向连接的会话建立的通信信道是一条逻辑链路



1.源应用程序向目的端请求一个面向连接的通信会话

2.两端建立会话

3.在逻辑连接上开始数据传输

4.传输结束时，信道解除连接

TCP:

- 使用顺序控制或重发机制保证数据传输的可靠性
- 流控（流量控制）、拥塞控制、差错控制

2.面向无连接的UDP

面向无连接的服务中，发送方和接收方之间没有建立连接，每个分组含有源地址和目的地址，自行寻址

UDP是不具有可靠性的数据包协议

如视频、咨询、股票等，用的几乎全都是UDP协议

3.两种协议比较

TCP	比较方面	UDP
面向连接	协议类型	面向无连接
提供可靠传输	可靠性	提供不可靠传输
流控、拥塞控制、差错控制	控制机制	无
尽量按序到达	发送顺序	不一定按序到达
不会丢失数据，适合大数据量交换	分组顺序	高速传输和实时性有较高要求的通信

端口号的作用

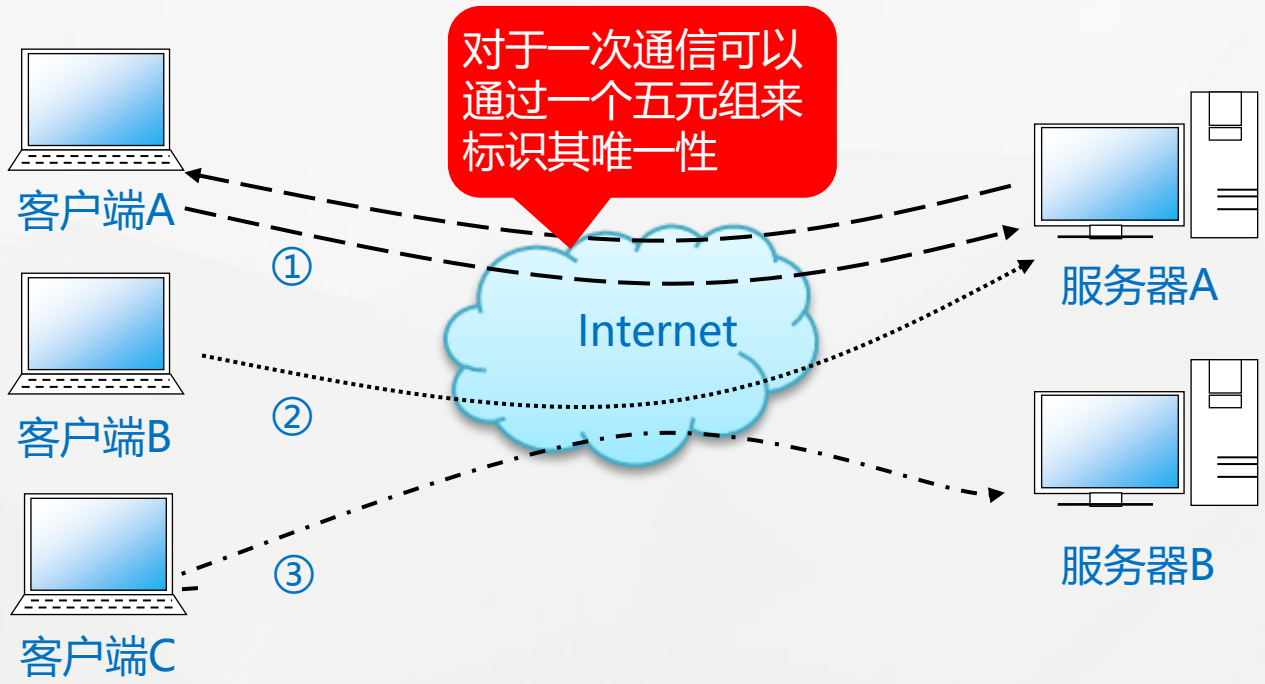
高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

- 了解端口号的作用

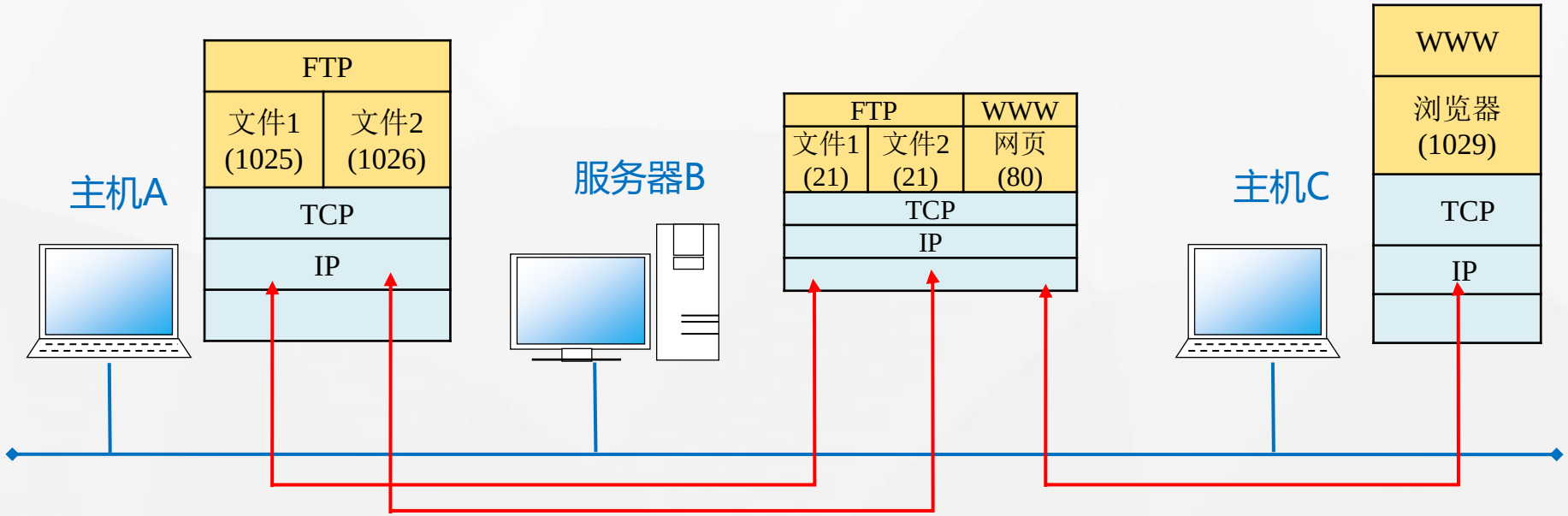
1.网络通信的五元组



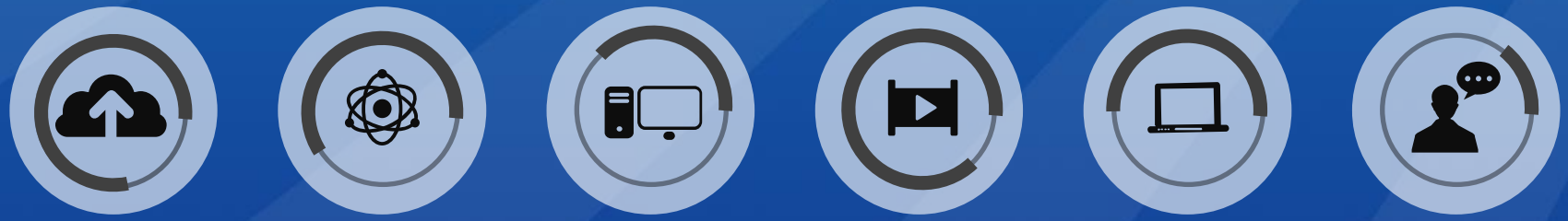
- 源IP地址
- 目的IP地址
- 协议
- 源端口号
- 目的端口号

2.端口号的使用

端口号主要是区分服务类别和在同一时间进行多个会话



端口号的分类



高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

- 理解端口号的分类
- 掌握常用知名端口的分配

1.端口号的分类

端口号是由16位二进制数组成，最大为65535

系统端口号

又称知名端口号

范围是0到1023

每个端口号对应固定应用

FTP→20、21

HTTP→80

对于应用程序，也可自行设定：

HTTP→8080

用户端口号

又称注册端口号

范围是1024到49151

没有明确的定义服务对象

动态端口号

又称临时端口号

范围是49152到65535

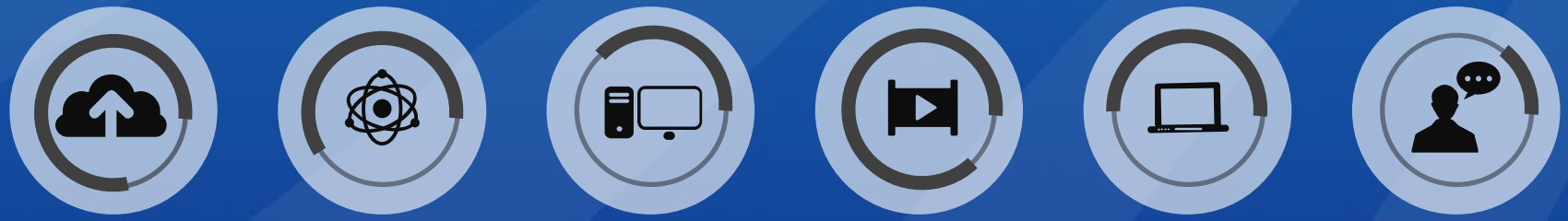
系统分配给应用程序使用

使用完成后释放这个端口

2.端口号与协议的对应关系

服务类型	端口号	传输层协议	内 容
ftp-data	20	tcp/udp	文件传输协议
ftp	21	tcp	文件传输协议
ssh	22	tcp/udp	SSH远程登录协议
telnet	23	tcp/udp	远程登录协议
smtp	25	tcp	简单邮件传输协议
dns	53	tcp/udp	域名系统
tftp	69	udp	小型文件传输协议
http	80	tcp	超文本传输协议
pop3	110	tcp	邮局协议
snmp	161	udp	简单网络管理协议
https	443	tcp	超文本传输安全协议

TCP协议



高等教育出版社
HIGHER EDUCATION PRESS

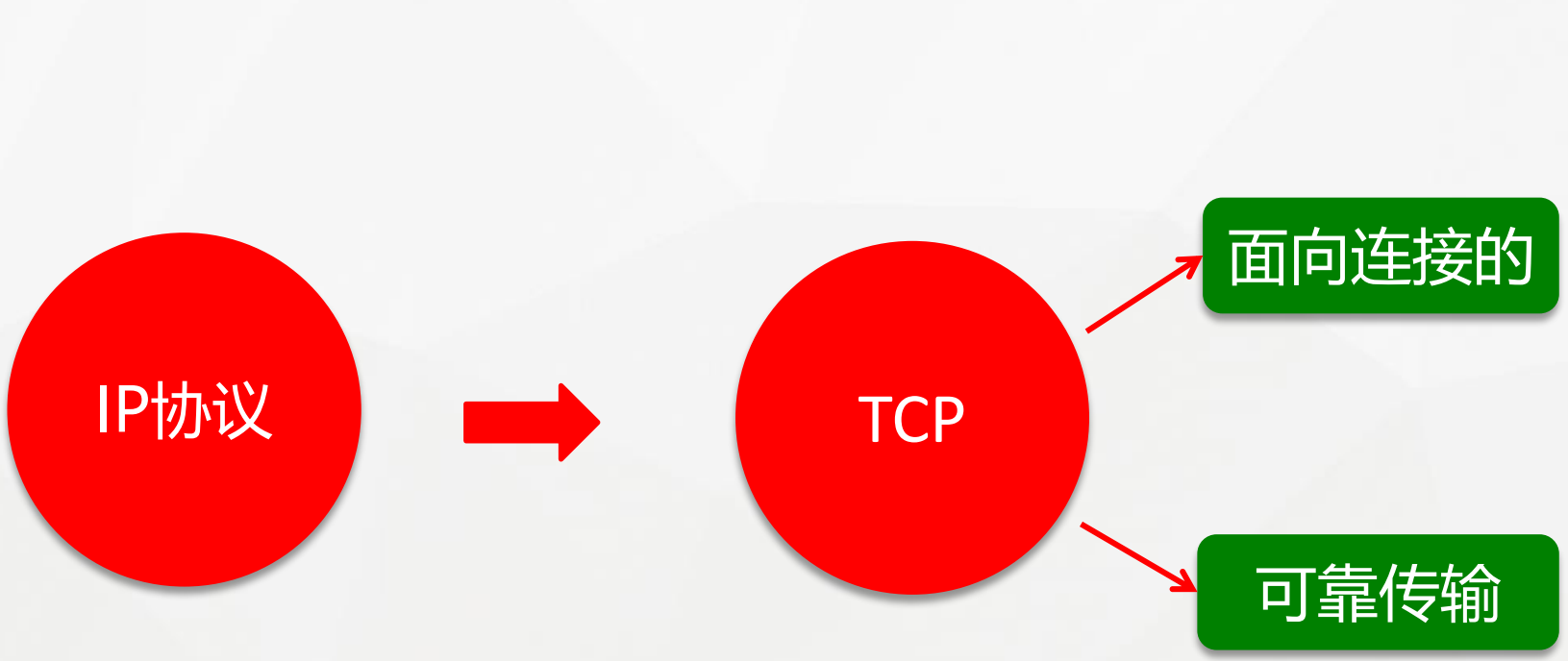
目录
Contents

学习目标

- 掌握TCP协议特点
- 理解TCP协议格式

1. TCP协议特点

TCP:传输控制协议，为了在主机间实现高可靠性数据交换的传输协议



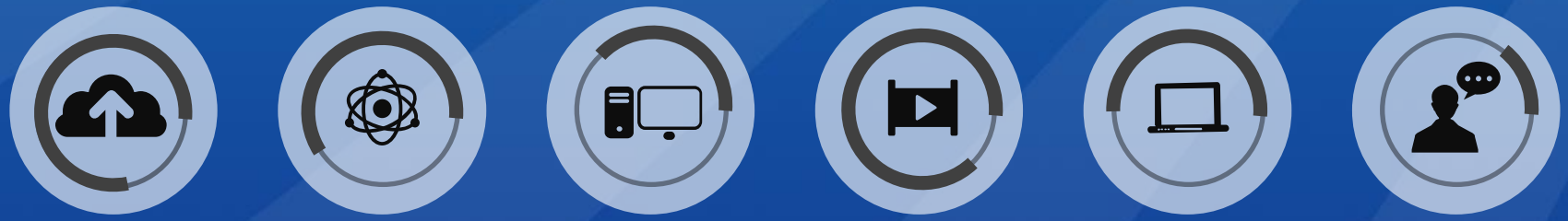
面向无连接的

不可靠的协议

2.TCP协议应用场景

主要用于对网络传输可靠性高的环境

TCP协议报文格式



高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

- 掌握TCP协议特点
- 理解TCP协议格式

1. TCP报文格式

bit0 bit31

源端口（16）	目标端口（16）
序列号（Sequence Number，32）	
确认号（Acknowledgement Number，32）	
数据偏移 / 保留字段 / URG ACK PSH RST SYN FIN	窗口大小（16位）
校验和（16）	紧急指针（16）
可选项	填充
数据	

TCP报文格式

1 源端口号

端口号占用16位

源端口是由发送方进程产生的一个随机数，一般使用临时端口。

1. TCP报文格式

TCP报文格式

2 目标端口号

端口号占用16位

目标端口 ➡ 接收端的进程

接收端收到数据段后，根据其来确定把数据送给哪个应用程序的进程。

1. TCP报文格式

TCP报文格式

3 序列号

占用32位

不同的数据段

按序列号把数据段重新排列

1. TCP报文格式

TCP报文格式

4 确认号

占用32位

下一个期望收到的段的序列号

如果是X　　代表前X-1各收到

1. TCP报文格式

TCP报文格式

5 数据偏移

占用4位

TCP所传输的数据应该从TCP包的哪个位开始计算

也表示首部长度

如： 0111 ➡ 7

报头区长度为：

7*32bits=224bits=28Bytes

1. TCP报文格式

TCP报文格式

6 保留字段

占用6位

部分保留位作为今后扩展功能用

1. TCP报文格式

TCP报文格式

7 标志位

占用6位

URG：紧急指针有效位

ACK：确认位

PSH：推送位

RST：重置位

SYN：同步序号位

FIN：结束位，

1. TCP报文格式

TCP报文格式

8 标志位

占用16位

说明本地可接收数据段的数目

流量控制机制

1. TCP报文格式

TCP报文格式

9 校验和

占用16位

差错控制

通过在发送端和接收端两次计算结果，看是否相同

1. TCP报文格式

TCP报文格式

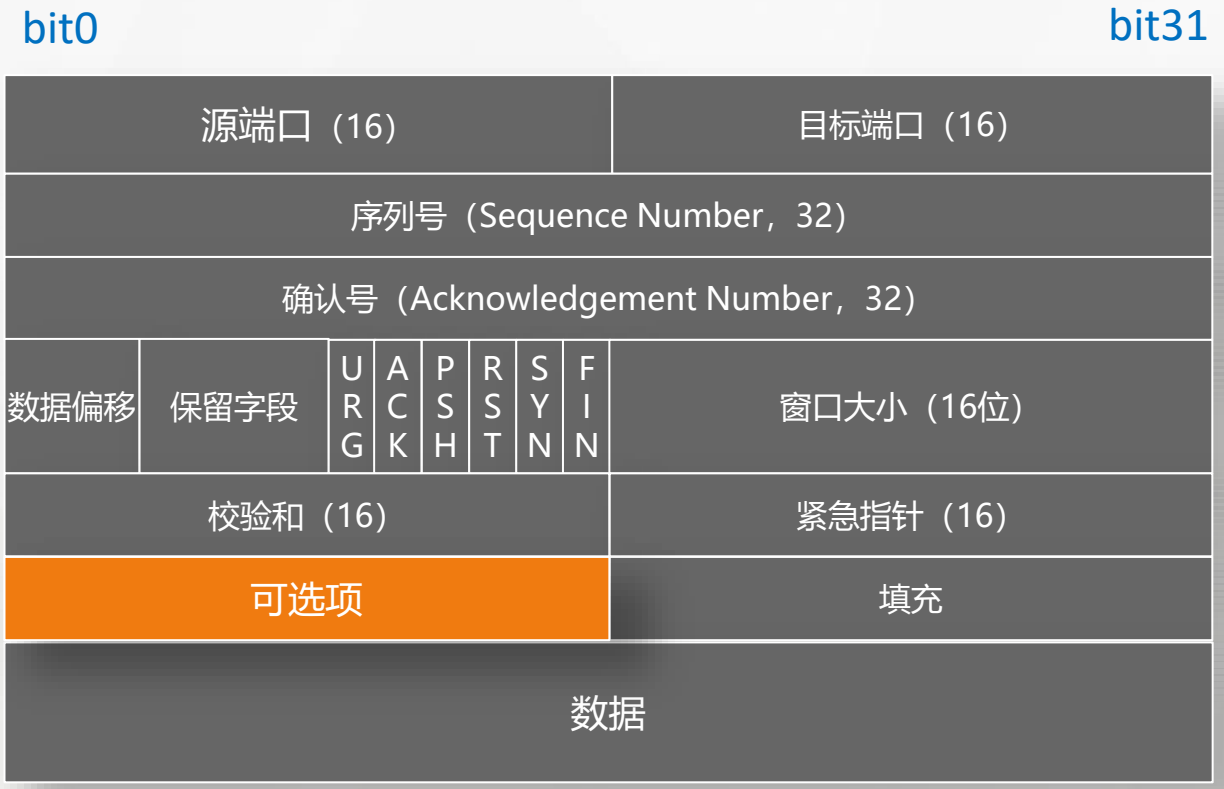
10 紧急指针

占用16位

用来确定紧急数据的最后一个字节的位置。

优先快速地获取紧急数据

1. TCP报文格式



TCP报文格式

11 可选项

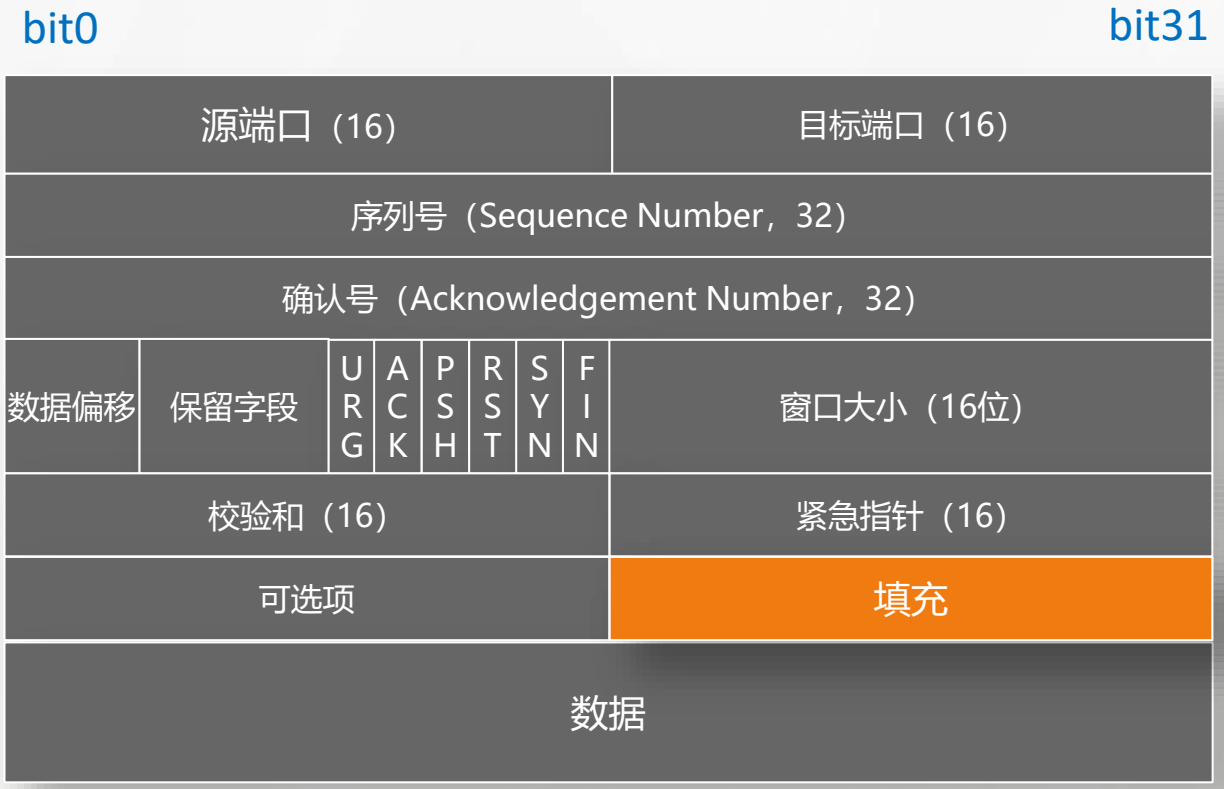
TCP首部中附加的一些信息，用于提高TCP传输性能

最大报文长度

时间戳选项

选择性确认选项

1. TCP报文格式



TCP报文格式

13 填充

填充0，用于保证首部的长度是32位的整数倍

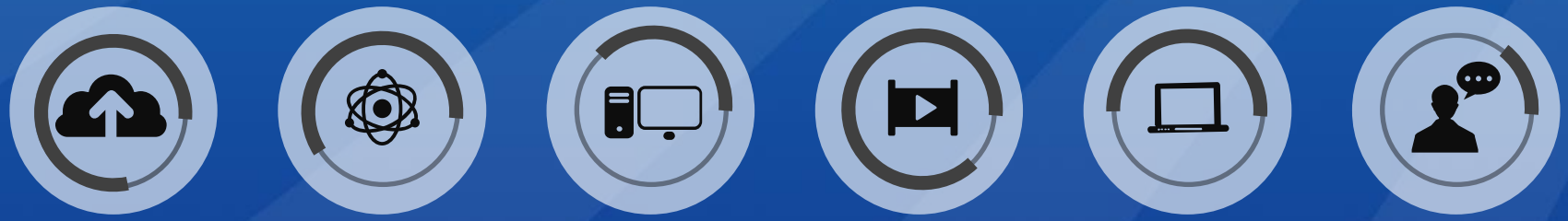
1. TCP报文格式

TCP报文格式

14 数据

数据字段内容是上层所封装的完整数据。

TCP连接建立与释放



高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

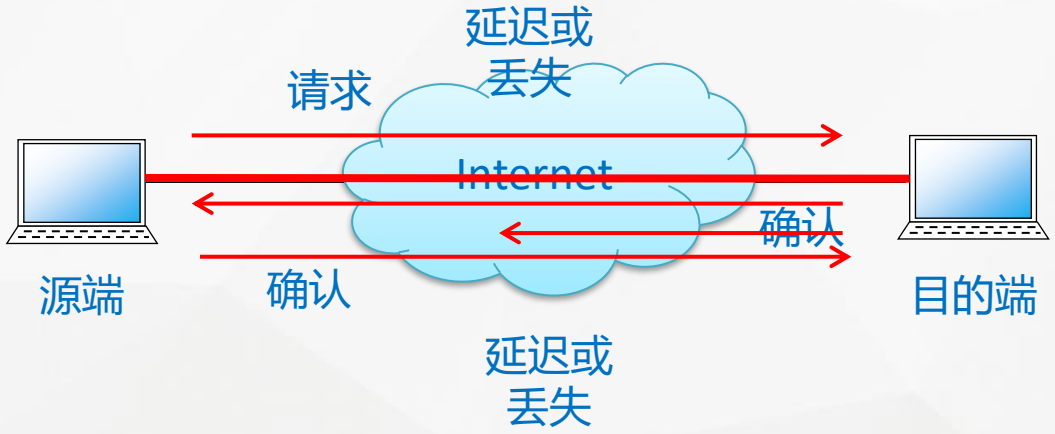
- 掌握TCP建立连接过程
- 掌握TCP断开连接过程

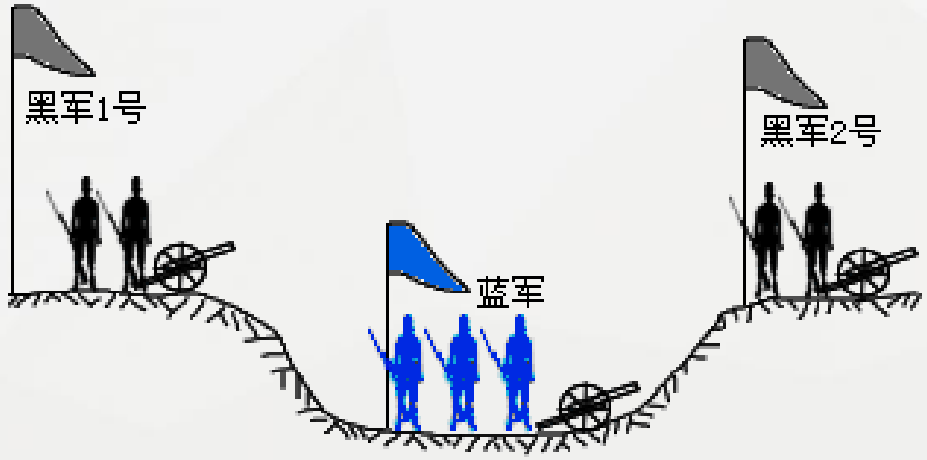
1. TCP连接建立过程

TCP：面向连接的协议

建立连接三次握手

释放连接四次挥手



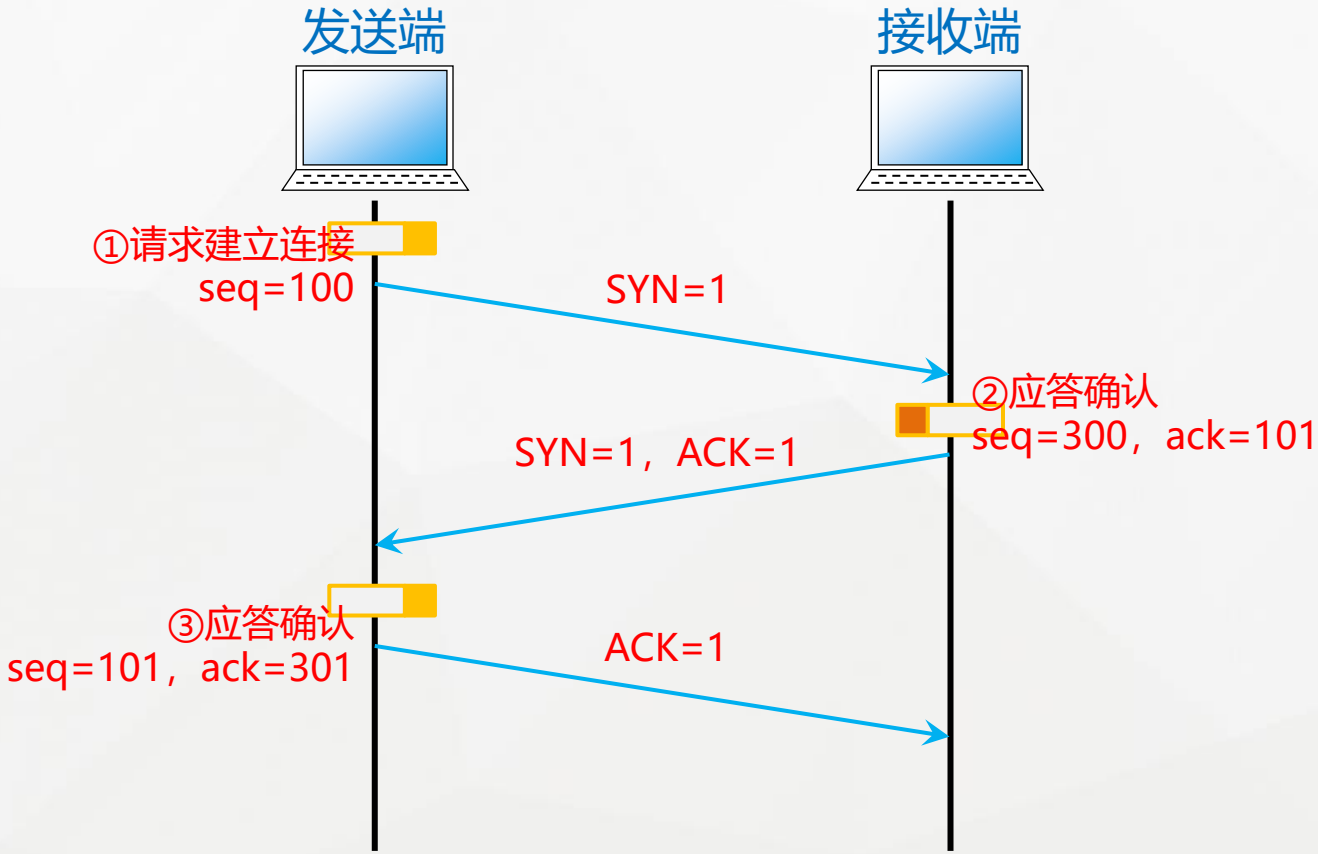


1. TCP连接建立过程

三次握手

源端口（16）	目标端口（16）
序列号（Sequence Number，32）	
确认号（Acknowledgement Number，32）	
数据偏移 / 保留字段 / URG ACK PSH RST SYN FIN	窗口大小（16位）
校验和（16）	紧急指针（16）
可选项	填充
数据	

TCP报文格式

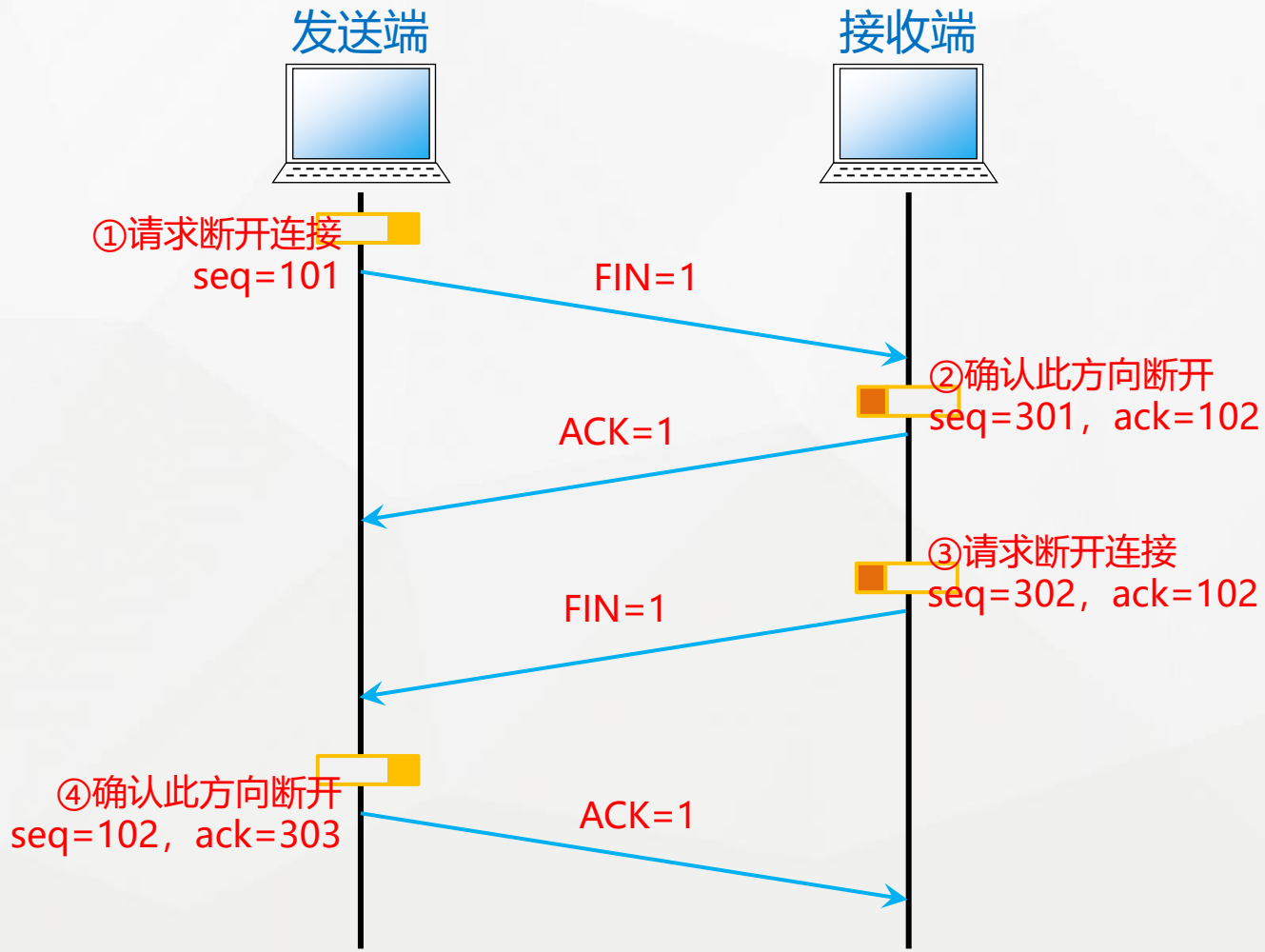


2. TCP连接断开过程

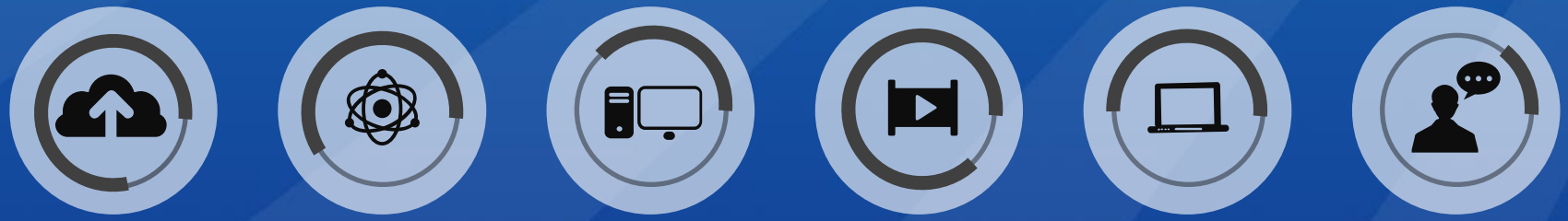
四次挥手

源端口（16）	目标端口（16）
序列号（Sequence Number，32）	
确认号（Acknowledgement Number，32）	
数据偏移 / 保留字段 / URG ACK PSH RST SYN FIN	窗口大小（16位）
校验和（16）	紧急指针（16）
可选项	填充
数据	

TCP报文格式



TCP通信抓包体验



高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

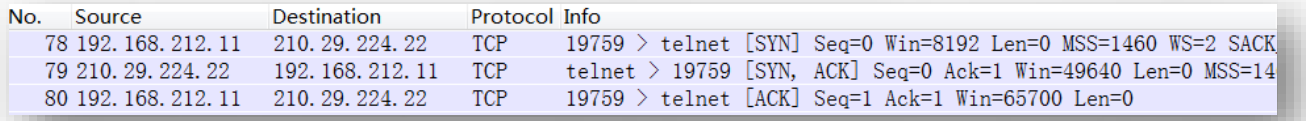
学习目标

- 掌握数据包抓包方法
- 理解TCP通信过程

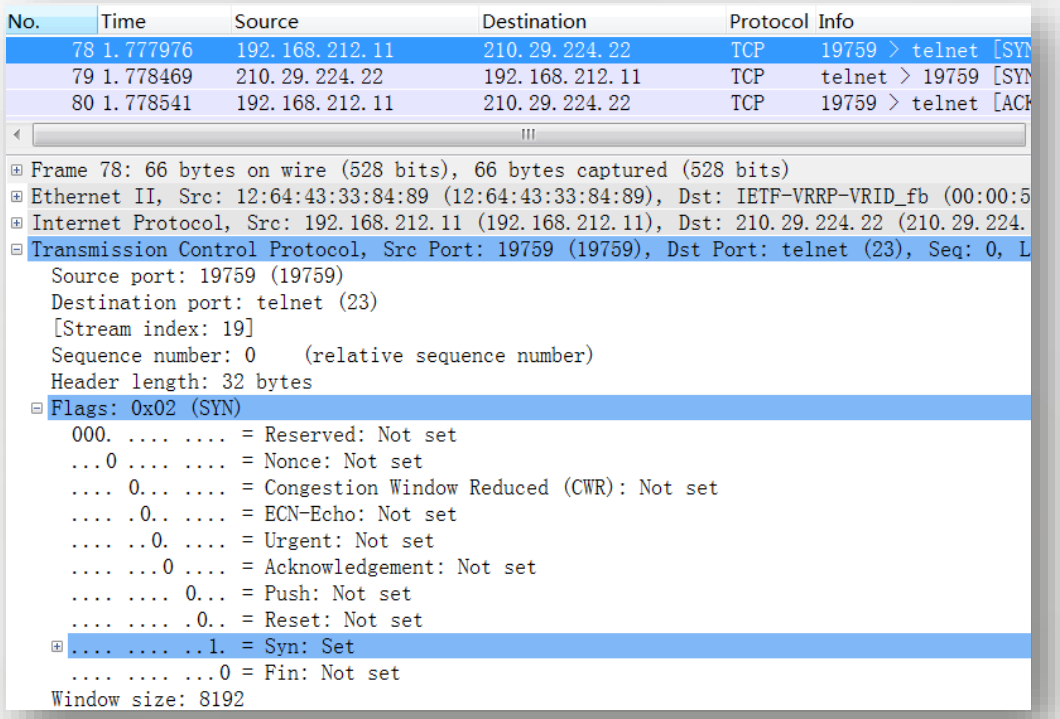
1. TCP抓包方法及过程

抓包操作过程：

1. 启动Wireshark抓包功能
2. 在浏览器中输入网址
3. 停止抓包
4. 对抓取的数据包进行过滤



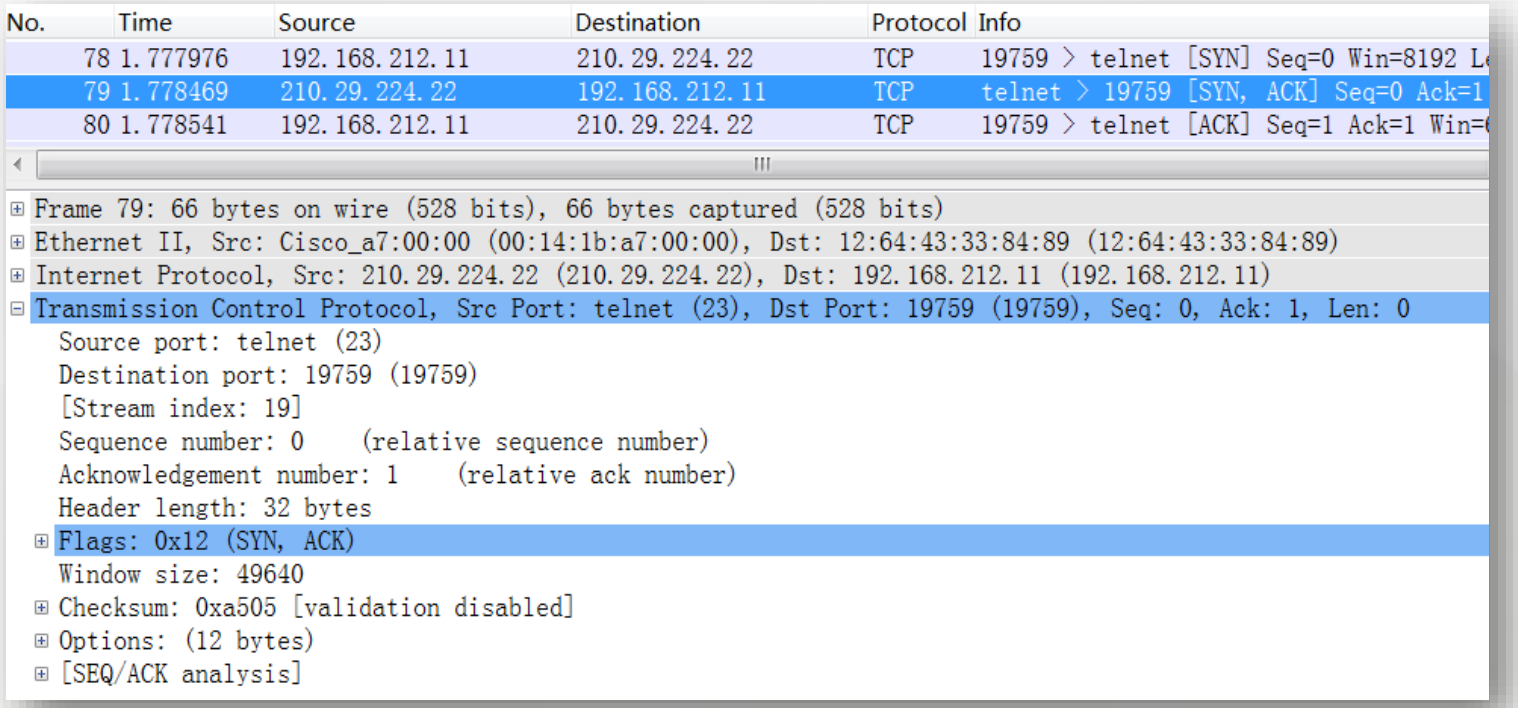
No.	Source	Destination	Protocol	Info
78	192.168.212.11	210.29.224.22	TCP	19759 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK
79	210.29.224.22	192.168.212.11	TCP	telnet > 19759 [SYN, ACK] Seq=0 Ack=1 Win=49640 Len=0 MSS=14
80	192.168.212.11	210.29.224.22	TCP	19759 > telnet [ACK] Seq=1 Ack=1 Win=65700 Len=0



No.	Time	Source	Destination	Protocol	Info
78	1.777976	192.168.212.11	210.29.224.22	TCP	19759 > telnet [SYN
79	1.778469	210.29.224.22	192.168.212.11	TCP	telnet > 19759 [SYN
80	1.778541	192.168.212.11	210.29.224.22	TCP	19759 > telnet [ACK

```
⊞ Frame 78: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: 12:64:43:33:84:89 (12:64:43:33:84:89), Dst: IETF-VRRP-VRID_fb (00:00:5
⊞ Internet Protocol, Src: 192.168.212.11 (192.168.212.11), Dst: 210.29.224.22 (210.29.224.
⊟ Transmission Control Protocol, Src Port: 19759 (19759), Dst Port: telnet (23), Seq: 0, L
    Source port: 19759 (19759)
    Destination port: telnet (23)
    [Stream index: 19]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊟ Flags: 0x02 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgement: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ⊞ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size: 8192
```

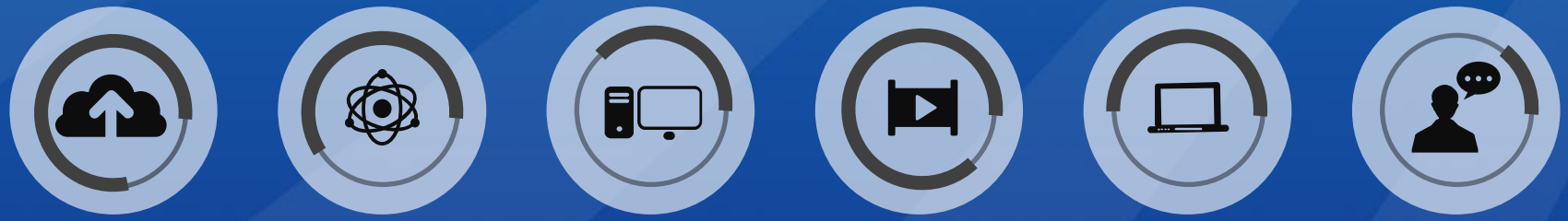
2. TCP连接过程分析



No.	Time	Source	Destination	Protocol	Info
78	1.777976	192.168.212.11	210.29.224.22	TCP	19759 > telnet [SYN] Seq=0 Win=8192 L
79	1.778469	210.29.224.22	192.168.212.11	TCP	telnet > 19759 [SYN, ACK] Seq=0 Ack=1
80	1.778541	192.168.212.11	210.29.224.22	TCP	19759 > telnet [ACK] Seq=1 Ack=1 Win=

```
⊞ Frame 79: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: Cisco_a7:00:00 (00:14:1b:a7:00:00), Dst: 12:64:43:33:84:89 (12:64:43:33:84:89)
⊞ Internet Protocol, Src: 210.29.224.22 (210.29.224.22), Dst: 192.168.212.11 (192.168.212.11)
⊟ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 19759 (19759), Seq: 0, Ack: 1, Len: 0
    Source port: telnet (23)
    Destination port: 19759 (19759)
    [Stream index: 19]
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
  ⊞ Flags: 0x12 (SYN, ACK)
    Window size: 49640
  ⊞ Checksum: 0xa505 [validation disabled]
  ⊞ Options: (12 bytes)
  ⊞ [SEQ/ACK analysis]
```

TCP可靠性传输机制



高等教育出版社
HIGHER EDUCATION PRESS

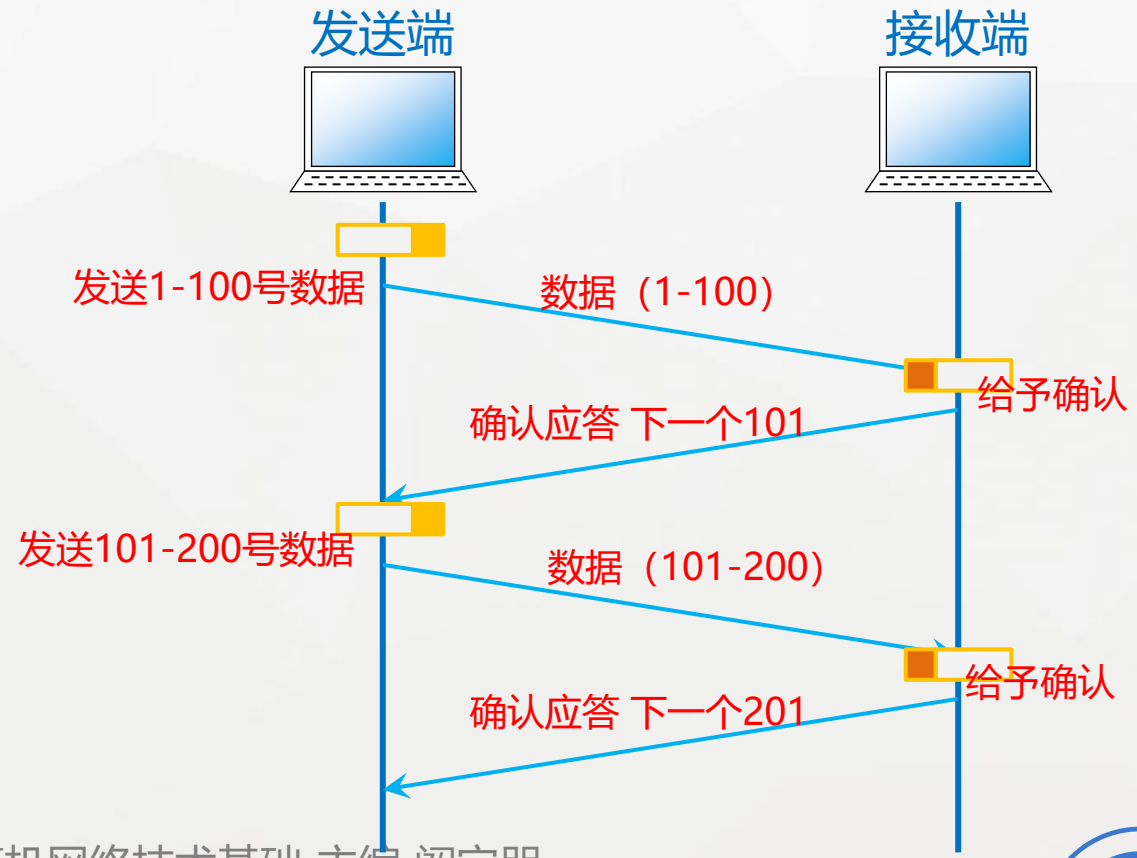
目录
Contents

学习目标

- 了解TCP可靠性传输机制
- 了解TCP未被确认的几种情况

确认应答

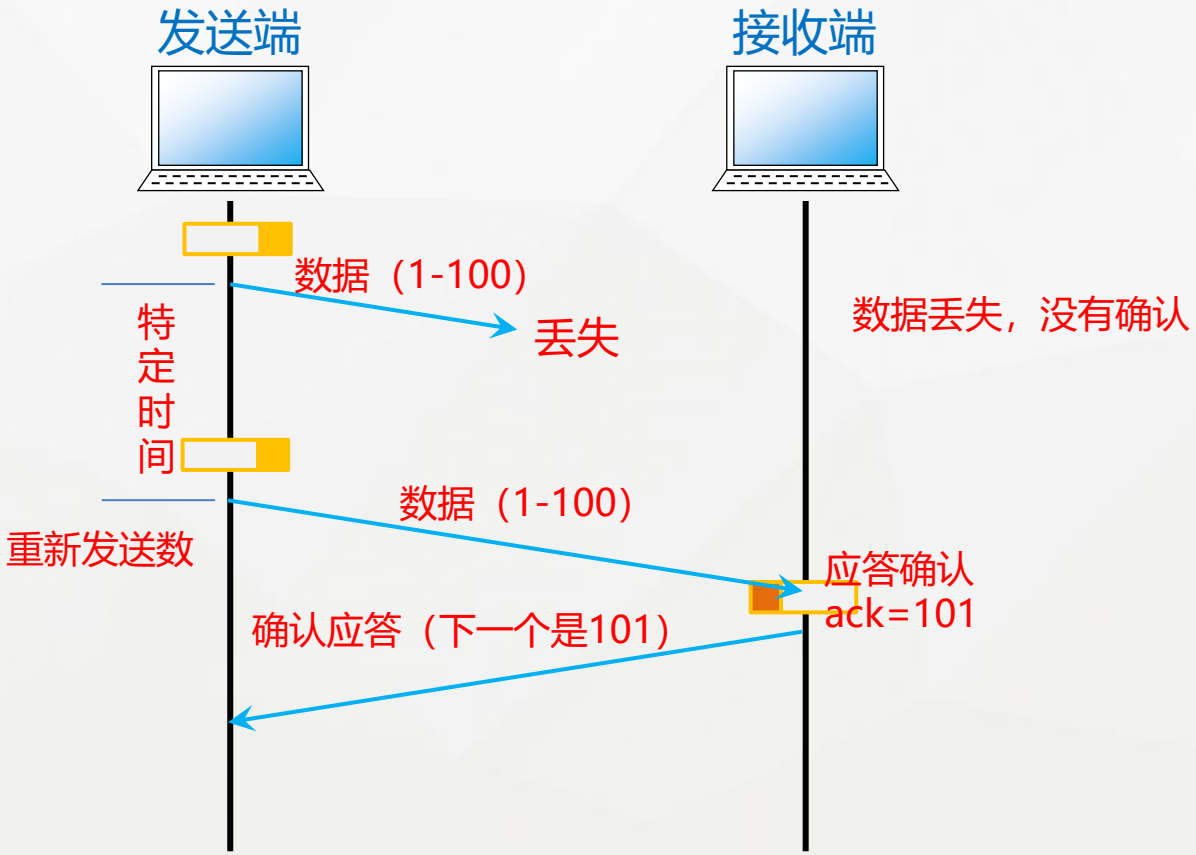
在TCP中，当发送端的数据到达接收端时，接收端会返回一个已收到消息的通知，这个消息叫做确认应答（ACK）



肯定的确认应答是返回一个下次接收时期望的TCP数据包的序列号（Acknowledgement Number）。

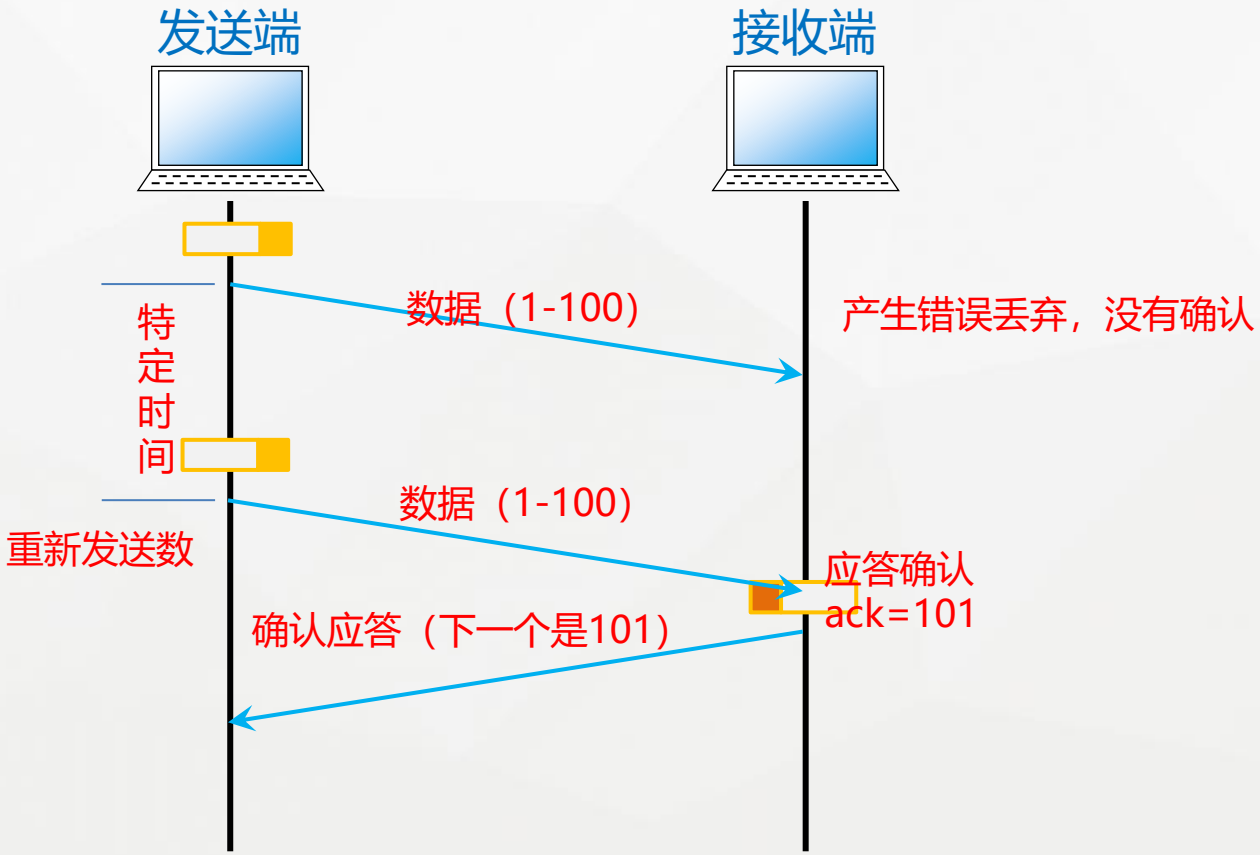
2.未被确认的几种情况

(1)数据丢失重新发送



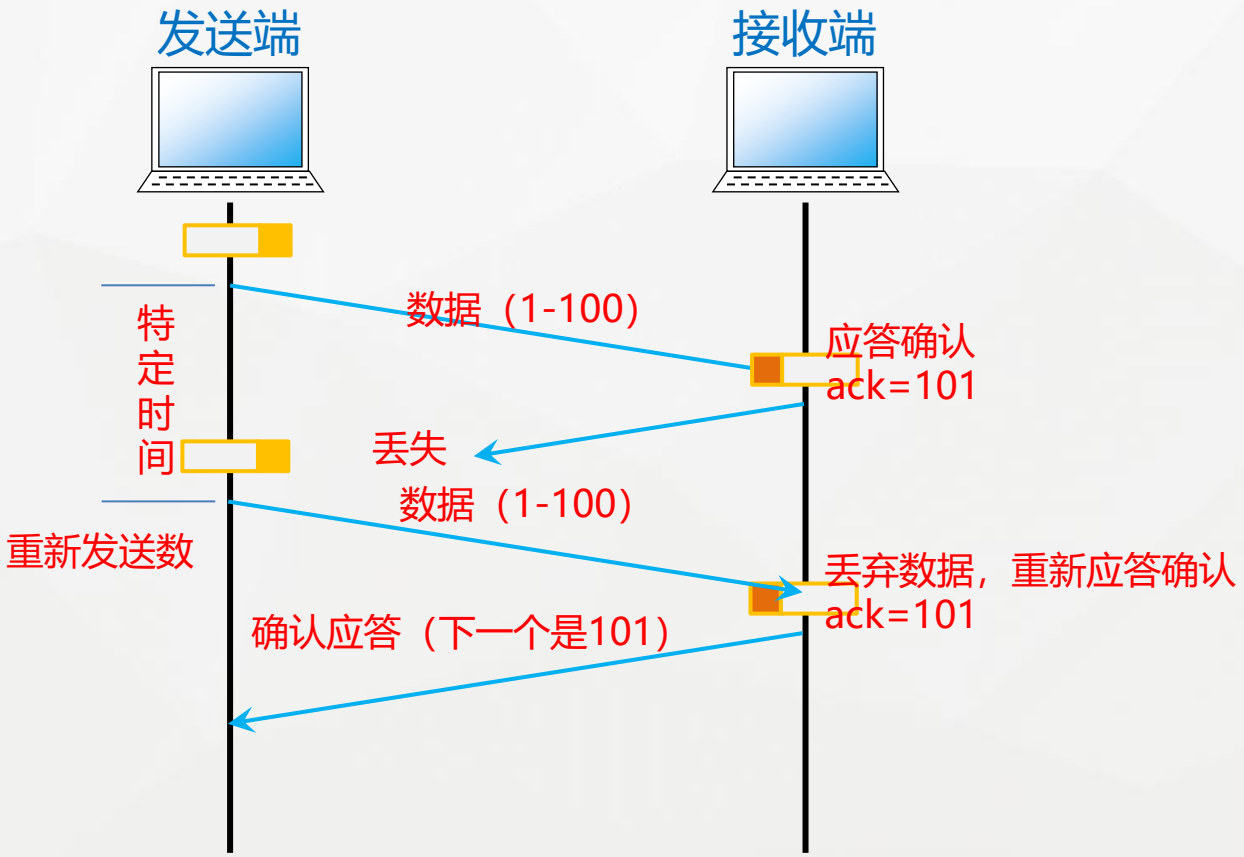
2.未被确认的几种情况

(2)数据传输错误重新发送



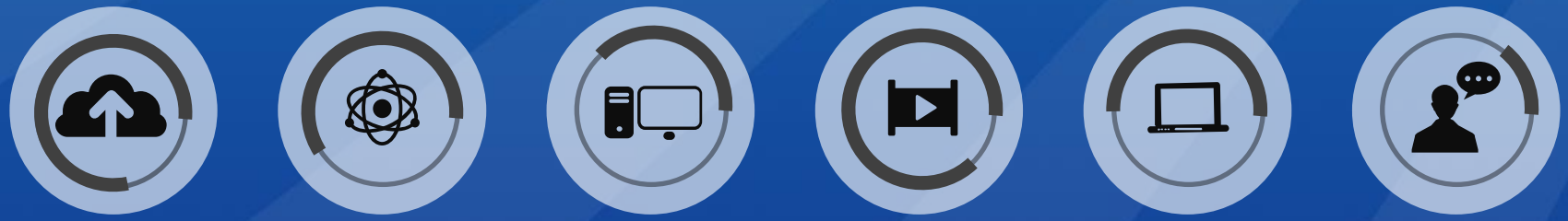
2.未被确认的几种情况

(3) 确认应答丢失重新发送



达到一定重发次数之后，如果仍没有任何确认应答返回，就会判断为网络或对端主机发生了异常，强制关闭连接

TCP滑动窗口及流控



高等教育出版社
HIGHER EDUCATION PRESS

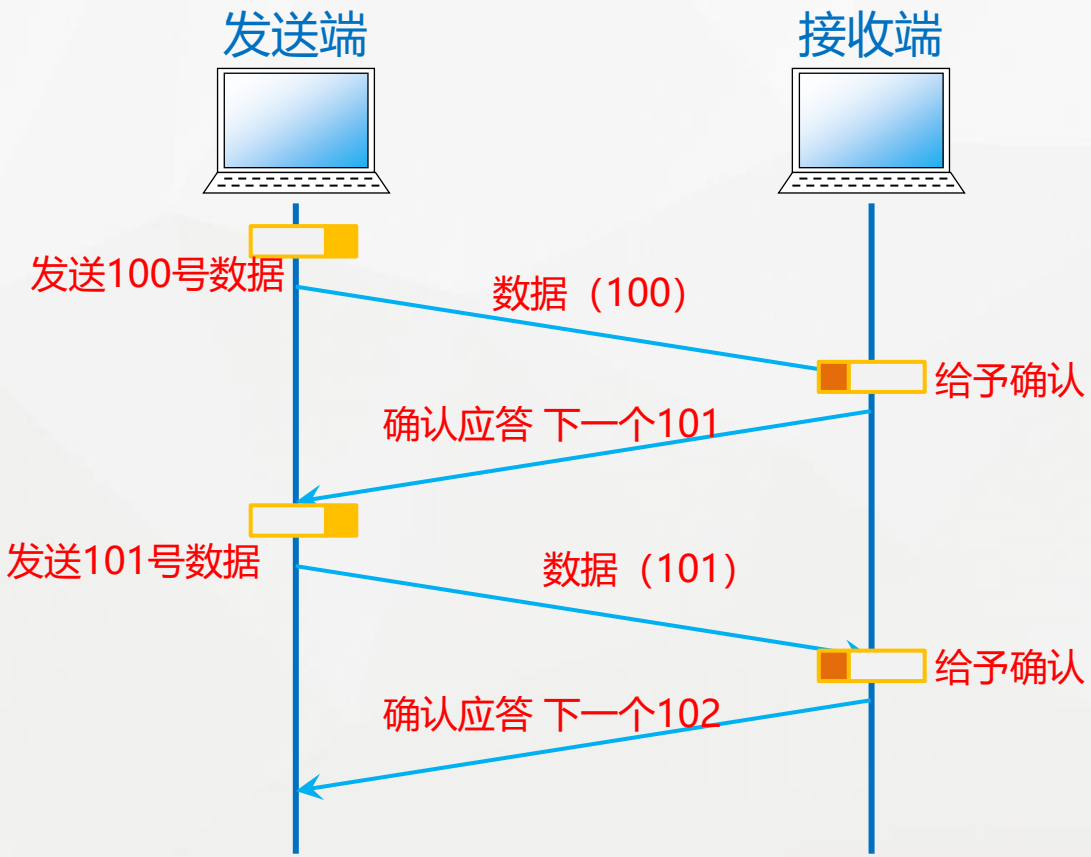
目录
Contents

学习目标

- 了解滑动窗口作用
- 了解滑动窗口确认机制
- 理解流量控制原理

1.滑动窗口工作方式

滑动窗口 是指无需等待确认应答而可以继续发送数据的最大值。



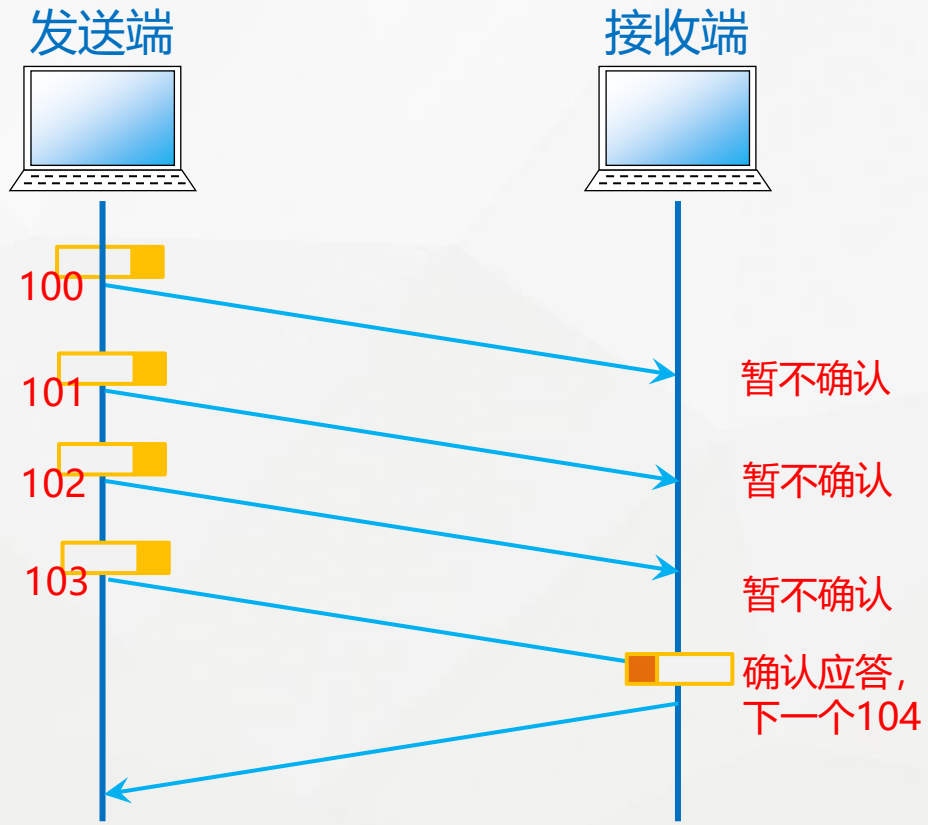
TCP发送数据是以段为单位的

最大消息长度 （MSS）

最大消息长度正好是IP中不会被分片处理的最大数据长度

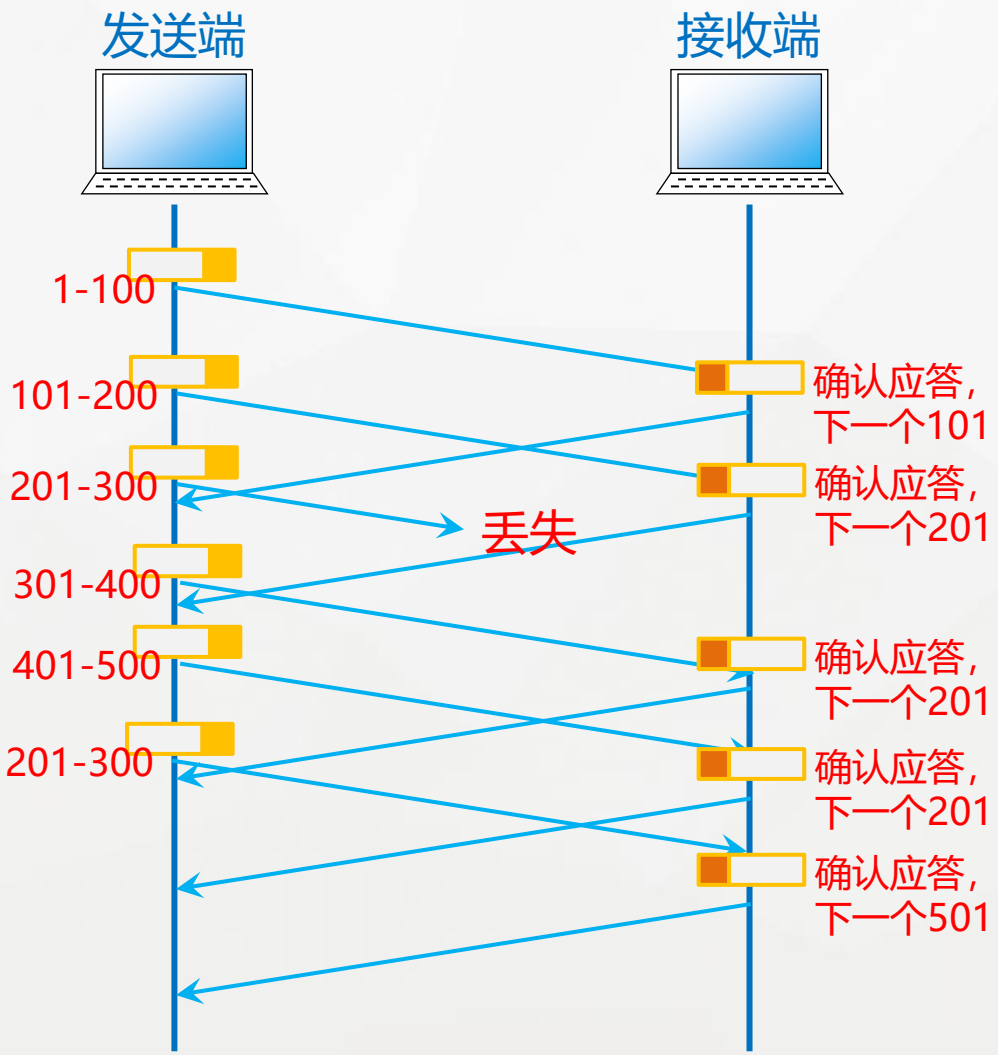
1.滑动窗口工作方式

使用滑动窗口：



这个机制实现了使用大量的缓冲区，通过对多个段同时进行确认应答的功能

2.滑动窗口确认机制



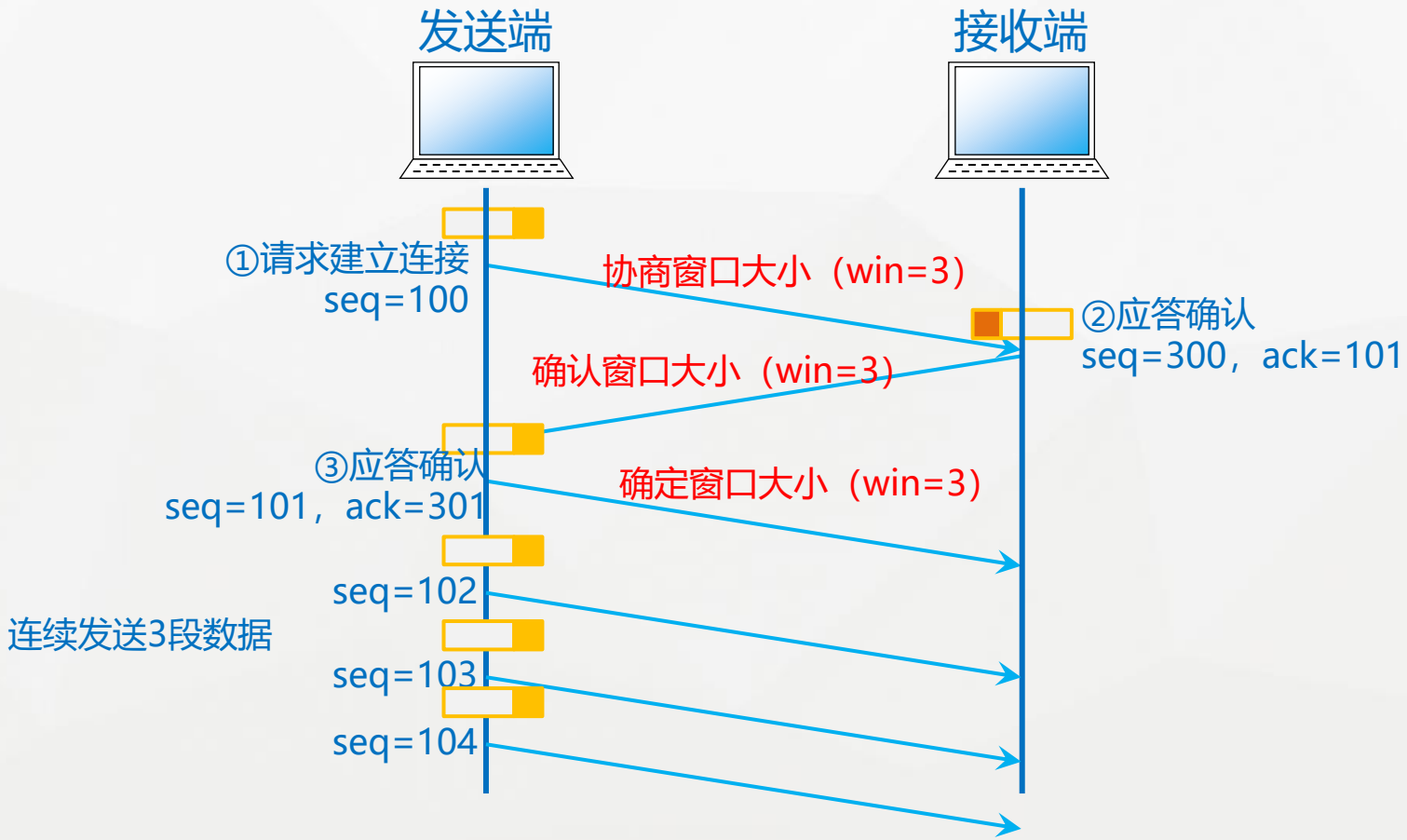
在没有使用窗口控制的时候，没有收到确认应答的数据都会被重发。而使用了窗口控制，某些确认应答即便丢失也无需重发，可以通过下一个应答进行确认

收到3个以上同样的应答，将会重发

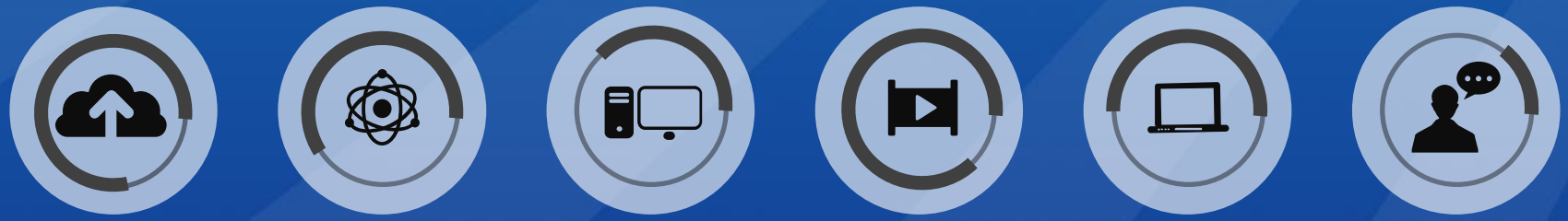
将301-500的数据放入缓冲区，等到201-300到达后交给应用程序

3.滑动窗口流控工作原理

流量控制 在两端发送数据前协商滑动窗口的大小，然后按照滑动窗口限定的缓冲区大小进行发送数据



TCP拥塞控制



高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

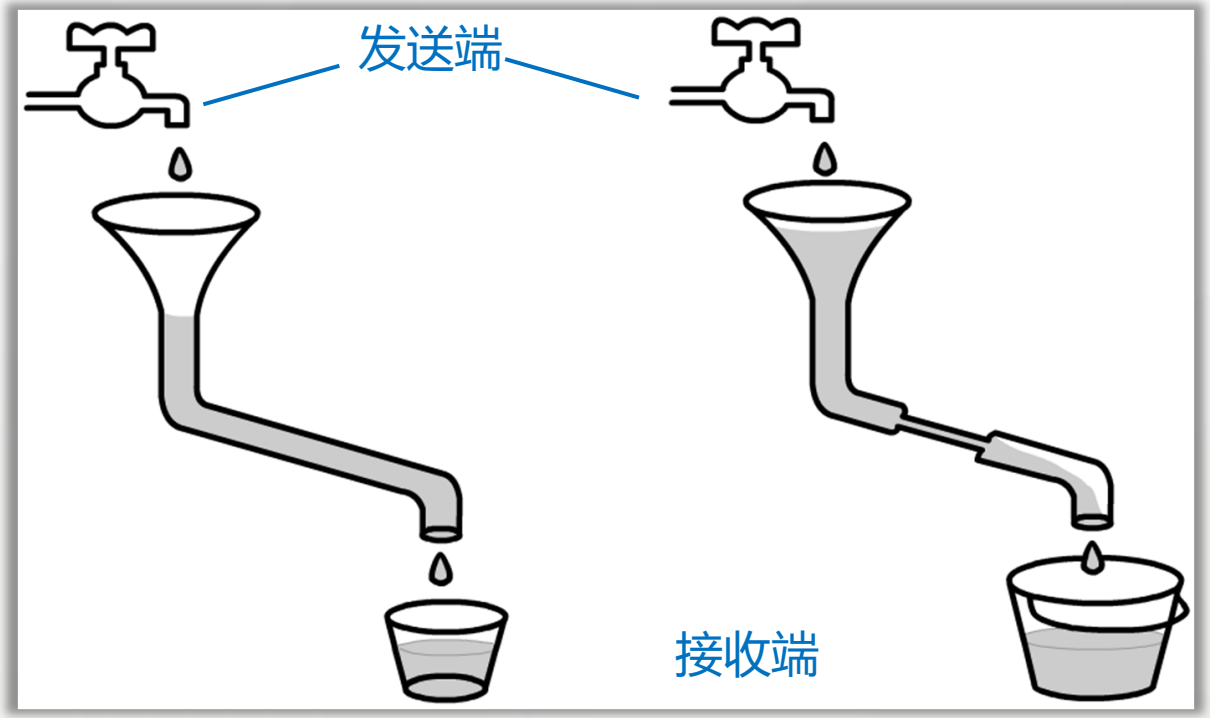
- 了解拥塞窗口作用
- 了解拥塞窗口的设置方法

1.拥塞窗口的作用

拥塞窗口 是发送端根据网络拥塞情况得出的窗口值，是来自发送端的流量控制

如果发送量过大，
水桶可能会溢出

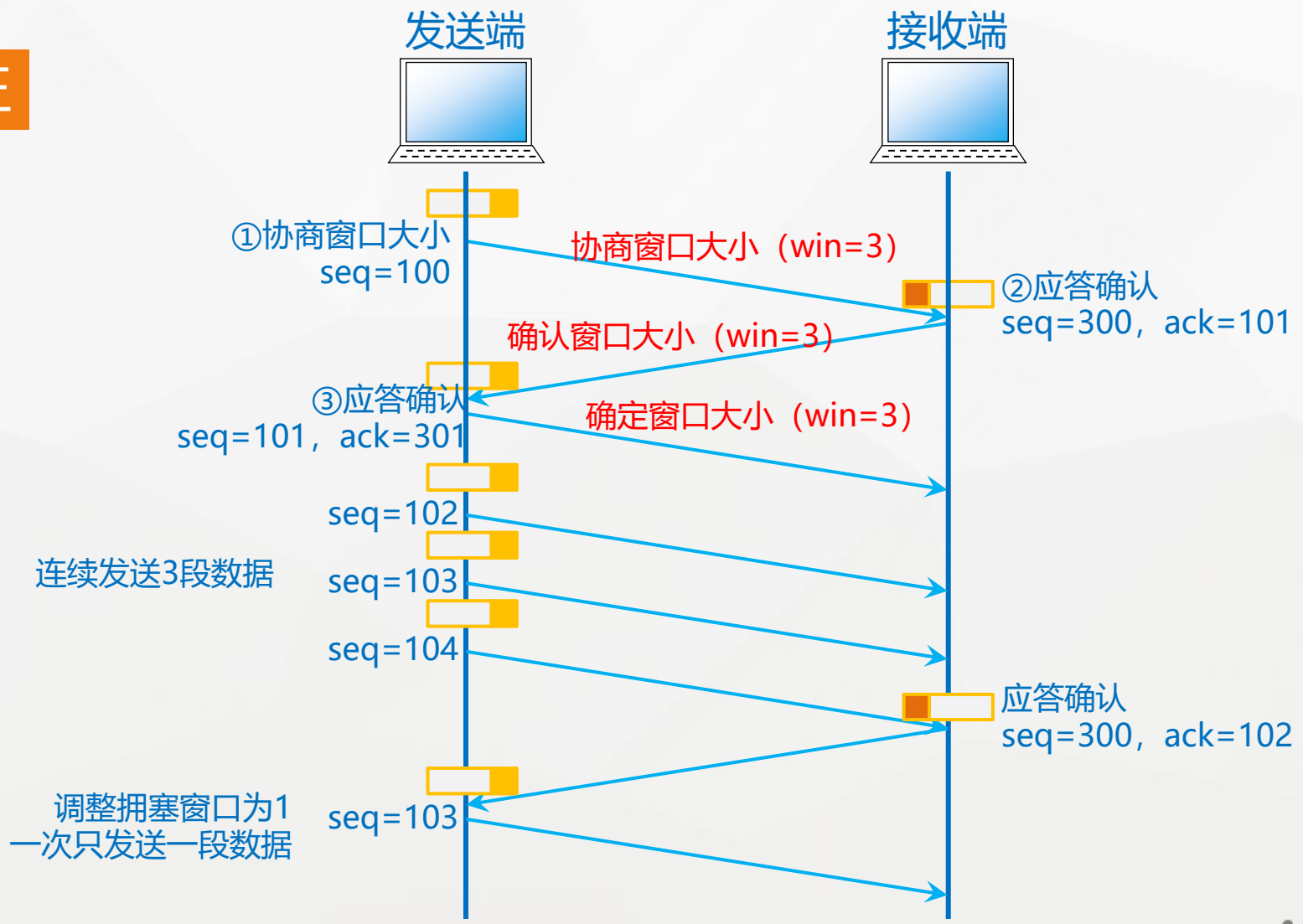
接收窗口来控制



如果产生拥塞，
漏斗可能会溢出

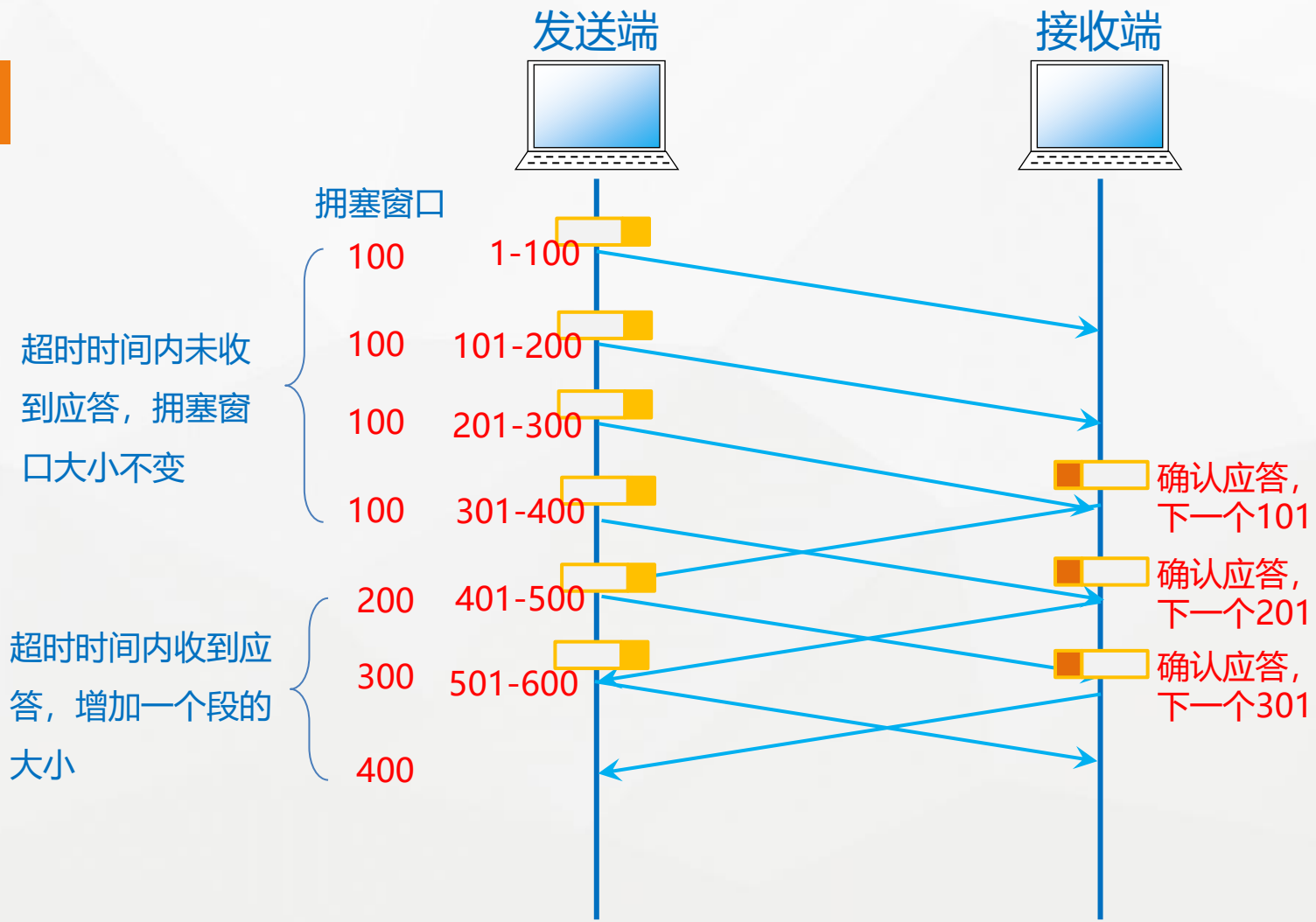
拥塞窗口来控制

拥塞窗口的修正

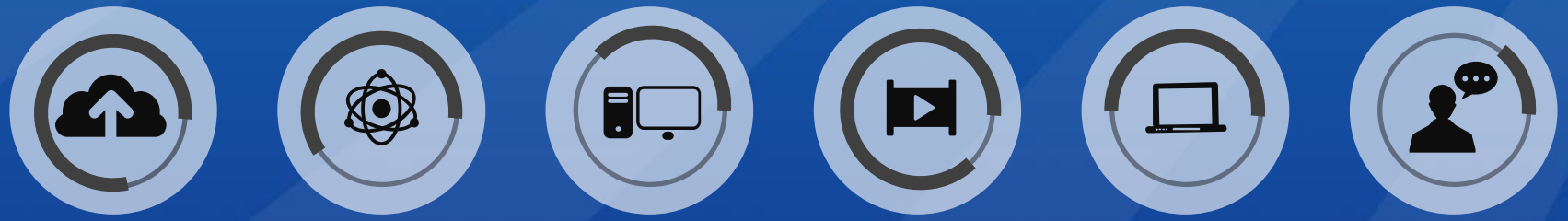

发送端
接收端
①协商窗口大小
seq=100
协商窗口大小（win=3）
②应答确认
seq=300，ack=101
确认窗口大小（win=3）
③应答确认
seq=101，ack=301
确定窗口大小（win=3）
seq=102
连续发送3段数据
seq=103
seq=104
应答确认
seq=300，ack=102
调整拥塞窗口为1
一次只发送一段数据
seq=103

2.拥塞窗口的设置方法

拥塞窗口的设置



TCP差错控制



高等教育出版社
HIGHER EDUCATION PRESS

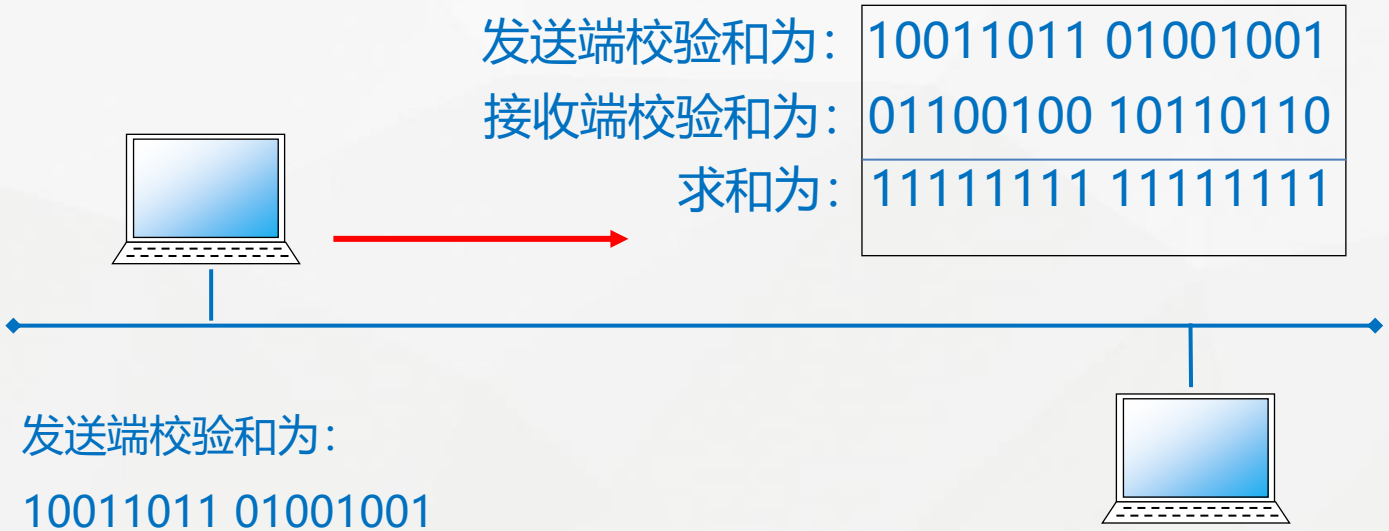
目录
Contents

学习目标

- 了解常用差错控制方法
- 理解校验和校验过程

1.校验和（Checksum）

校验　每一个数据段都包含校验和字段，用来检测受损数据段。



2.确认应答

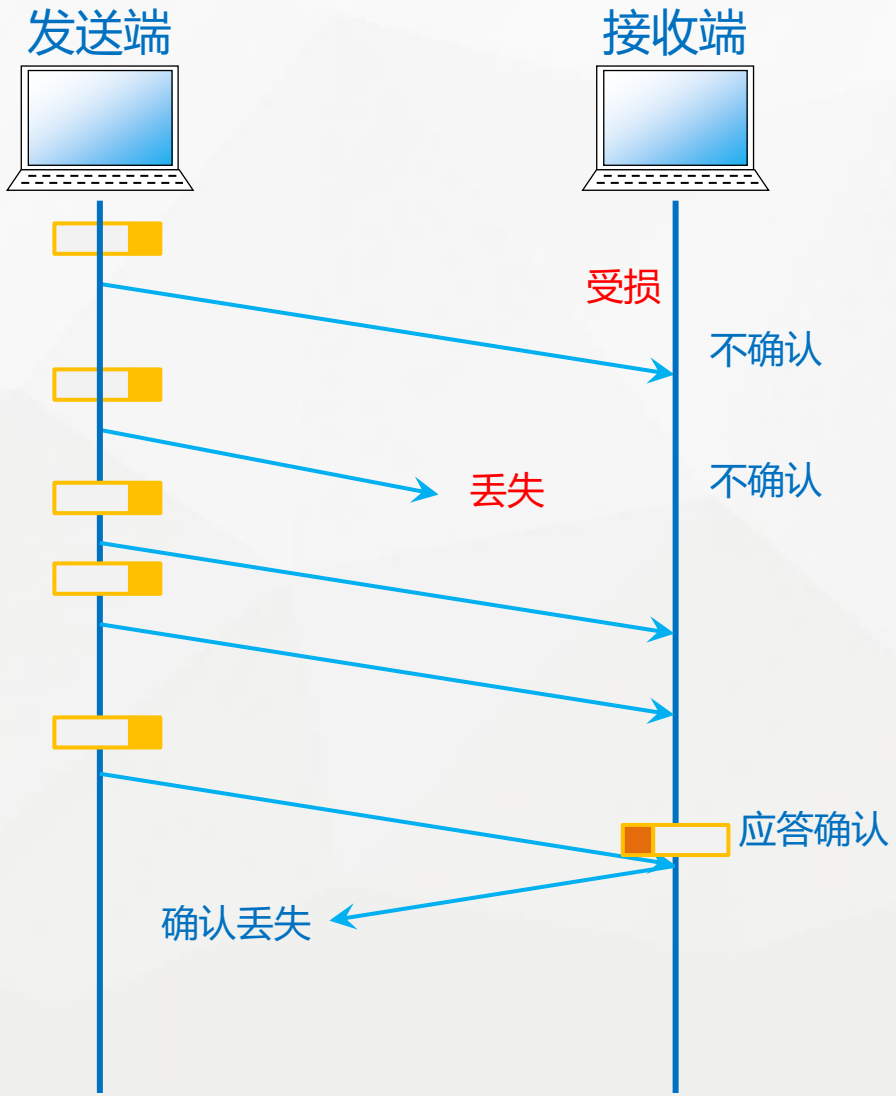
选择确认应答 它可以只对某一个数据段进行确认应答

延迟确认应答 可以对一组数据段进行确认

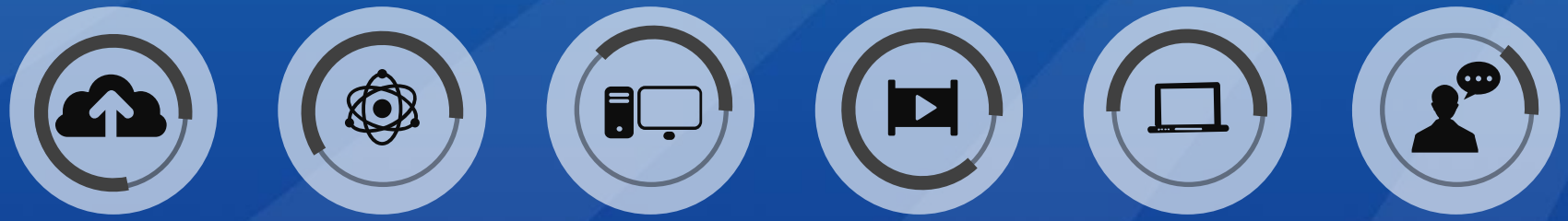
捎带应答 指TCP的确认应答可以和回执数据通过一个包发送，这种机制可以使收发的数据量减少。

3.超时


受损数据段
丢失的数据段
重复的数据段
失序的数据段
丢失的确认


发送端
接收端
受损
不确认
丢失
不确认
应答确认
确认丢失

UDP协议格式及应用



高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

- 了解UDP协议作用
- 理解UDP协议格式
- 了解UDP协议的应用

1. UDP协议特点及格式

- UDP全称是用户数据报协议，它是一种面向非连接的协议。
- UDP不提供数据包分组、组装和不能对数据包进行排序的缺点。
- 分组传输顺序的检查与排序由应用层完成。

实时流多媒体、实时多媒体播放器和游戏、IP电话（VoIP）

↓

TCP

需要建立连接、需要确认、需要添加20字节的首部

↓

UDP

不需要建立连接、不需要确认、不保证数据传送到对端

2.UDP报文格式

UDP报文格式

长度：指出UDP数据段中所包含数据的大小

校验和：用来完成对UDP数据的差错检验

3. UDP协议应用

流媒体

VOIP

游戏

实时交流工具

UDP协议没有流控、没有拥塞控制，除了校验和，没有差错控制

UDP协议抓包体验

高等教育出版社
HIGHER EDUCATION PRESS

目录
Contents

学习目标

- 掌握数据包抓包方法
- 理解UDP数据包格式

1. UDP抓包方法及过程

抓包操作过程：

1. 启动Wireshark抓包功能
2. 抓取QQ通信数据包
3. 停止抓包
4. 对抓取的数据包进行过滤

No.	Time	Source	Destination	Protocol	Info
107	1.088724	192.168.212.11	183.60.56.38	OICQ	OICQ Protocol
113	1.120124	183.60.56.38	192.168.212.11	OICQ	OICQ Protocol
116	1.142389	192.168.212.11	183.60.56.38	OICQ	OICQ Protocol
120	1.174022	183.60.56.38	192.168.212.11	OICQ	OICQ Protocol
124	1.195174	192.168.212.11	183.60.56.38	OICQ	OICQ Protocol
129	1.231248	183.60.56.38	192.168.212.11	OICQ	OICQ Protocol
130	1.242888	192.168.212.11	183.60.56.38	OICQ	OICQ Protocol
134	1.273992	183.60.56.38	192.168.212.11	OICQ	OICQ Protocol
137	1.286596	192.168.212.11	183.60.56.38	OICQ	OICQ Protocol

2. UDP协议格式分析

User Datagram Protocol, Src Port: terabase (4000), Dst Port: irdmi (8000)　//状态行

Source port: terabase (4000)　　//在源端使用端口号为4000

Destination port: irdmi (8000)　　//目的端端口号为8000

Length: 47　　//UDP数据包长度为47字节，由于头部长度为8字节，因此UDP数据区长度为39字节

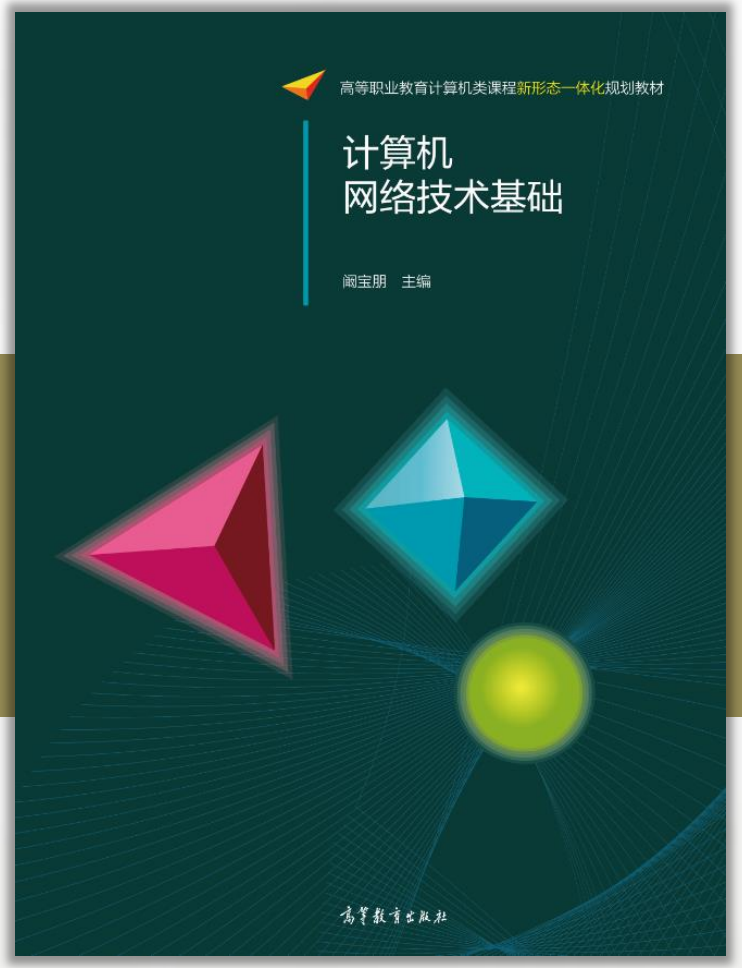
Checksum: 0x9deb [validation disabled]　//校验和。

Good Checksum: False

Bad Checksum: False

谢谢
Thanks!

高等教育出版社
HIGHER EDUCATION PRESS



新形态一体化教材 配套MOOC课程

计算机网络技术基础

主编 阚宝朋 高等教育出版社
书号：978-7-04-043546-7

扫描教材上二维码 实现随扫随学

高等教育出版社
HIGHER EDUCATION PRESS