

# 王道考研——计算机网络

WWW.CSKAOYAN.COM

## 第五章 传输层

64

公众号： 考研发条      一手课程！



Ch5.传输层

传输层概述

TCP协议

UDP协议

可靠传输

流量控制

拥塞控制

65

本节内容

传输层概述

王道考研/CSKAOYAN.COM

66

公众号： 考研发条      一手课程！

传输层

只有主机才有的层次

应用层

传输层

网络层

数据链路层

物理层

为应用层提供通信服务  
使用网络层的服务



传输层的功能：

1.传输层提供进程和进程之间的逻辑通信。

2.复用和分用

3.传输层对收到的报文进行差错检测。

4.传输层的两种协议。



网络层提供主机之间的逻辑通信。

王道考研/CSKAOYAN.COM

67

### 传输层的两个协议

传输层有两个好兄弟  
大哥TCP和二弟UDP  
大哥靠谱，二弟不靠谱

面向连接的传输控制协议TCP

传送数据之前必须建立连接，数据传送结束后要释放连接。不提供广播或多播服务。由于TCP要提供可靠的面向连接的传输服务，因此不可避免增加了许多开销：确认、流量控制、计时器及连接管理等。

**可靠，面向连接，时延大，适用于大文件。**

VS

无连接的用户数据报协议UDP

传送数据之前不需要建立连接，收到UDP报文后也不需要给出任何确认。

**不可靠，无连接，时延小，适用于小文件。**

王道考研/CSKAOYAN.COM

68

公众号： 考研发条      一手课程！

### 传输层的寻址与端口

复用：应用层所有的应用进程都可以通过传输层再传输到网络层。  
分用：传输层从网络层收到数据后交付指定的应用进程。

逻辑端口/软件端口 **端口** 是传输层的SAP，标识主机中的应用进程。

端口号只有本地意义，在因特网中不同计算机的相同端口是没有联系的。

端口号长度为16bit，能表示65536个不同的端口号。

端口号  
(按范围分)

服务端使用的端口号

熟知端口号：给TCP/IP最重要的一些应用程序，让所有用户都知道。  
0~1023

登记端口号：为没有熟知端口号的应用程序使用的。  
1024~49151

客户端使用：仅在客户进程运行时才动态选择的端口号  
49152~65535

王道考研/CSKAOYAN.COM

69

传输层的寻址与端口

应用程序	FTP	TELNET	SMTP	DNS	TFTP	HTTP	SNMP
熟知端口号	21	23	25	53	69	80	161

发现

FTP

谈恋爱

TELNET

删好友

SMTP

打电话

DNS

还要再见

HTTP

在网络中采用发送方和接收方的套接字组合来识别端点，套接字唯一标识了网络中的一个主机和它上面的一个进程。

套接字Socket=（主机IP地址，端口号）

王道考研/CSKAOYAN.COM

70

公众号： 考研发条      一手课程！

本节内容

UDP协议

王道考研/CSKAOYAN.COM

71

### 用户数据报协议UDP概述

UDP只在IP数据报服务之上增加了很少功能，即复用、分片和差错检测功能。

UDP的主要特点：

大哥TCP和二弟UDP

大哥靠谱，二弟不靠谱

- 1.UDP是**无连接**的，减少开销和发送数据之前的时延。
- 2.UDP使用最大努力交付，即**不保证可靠交付**。
- 3.UDP是**面向报文的**，适合一次性传输少量数据的网络应用。
- 4.UDP无拥塞控制，适合很多实时应用。
- 5.UDP首部开销小，8B，TCP20B。

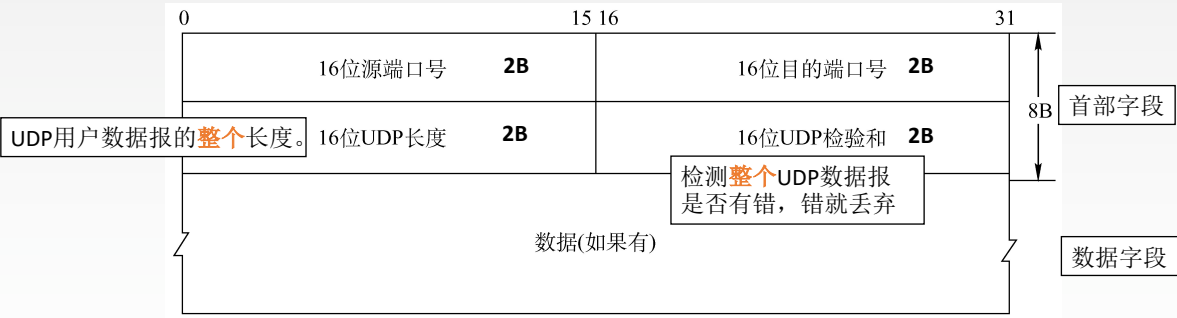


王道考研/CSKAOYAN.COM

72

公众号： 考研发条      一手课程！

### UDP首部格式



分用时，找不到对应的目的端口号，就丢弃报文，并给发送方发送ICMP“端口不可达”差错报告报文。

王道考研/CSKAOYAN.COM

73

### UDP校验

字节 4 4 1 1 2

源IP地址 目的IP地址 0 17 UDP长度

字节 12 2 2 2 2

伪首部 源端口 目的端口 长度 校验和

伪IP首部

UDP用户数据报 首部 数据

发送在前

首部 数据

IP数据报

伪首部只有在计算校验和时才出现，不向下传送也不向上递交。

17：封装UDP报文的IP数据报首部协议字段是17。

UDP长度：UDP首部8B+数据部分长度（不包括伪首部）。

王道考研/CSKAOYAN.COM

74

公众号： 考研发条      一手课程！

### UDP校验

12B 伪首部

8B UDP首部

7B 数据

153.19.8.104

171.3.14.11

全0 17 15

1087 13

15 全0

数据 数据 数据 数据

数据 数据 数据 全0

填充

使用16bit段反码运算

填充部分仅参加计算

按二进制反码运算求和

将得出的结果求反码

10011001 00010011 → 153.19

00001000 01101000 → 8.104

10101011 00000011 → 171.3

00001110 00001011 → 14.11

00000000 00010001 → 0和17

00000000 00001111 → 15

00000100 00111111 → 1087

00000000 00001101 → 13

00000000 00001111 → 15

00000000 00000000 → 0(校验和)

01010100 01000101 → 数据

01010011 01010100 → 数据

01001001 01001110 → 数据

01000111 00000000 → 数据和0(填充)

10010110 11101101 → 求和得出的结果

01101001 00010010 → 校验和

**在发送端：**

1. 填上伪首部
2. 全0填充校验和字段
3. 全0填充数据部分（UDP数据报要看成许多4B的字串接起来）
4. 伪首部+首部+数据部分采用二进制反码求和
5. 把和求反码填入校验和字段
6. 去掉伪首部，发送

**在接收端：**

1. 填上伪首部
2. 伪首部+首部+数据部分采用二进制反码求和
3. 结果全为1则无差错，否则丢弃数据报/交给应用层附上出差错的警告。

王道考研/CSKAOYAN.COM

75

### 本节内容

## TCP协议特点和TCP报文段

王道考研/CSKAOYAN.COM

76

公众号： 考研发条      一手课程！

### TCP协议的特点

- 1.TCP是面向连接（虚连接）的传输层协议。**打call**
- 2.每一条TCP连接只能有两个端点，每一条TCP连接只能是点对点的。
- 3.TCP提供可靠交付的服务，无差错、不丢失、不重复、按序到达。**可靠有序，不丢不重**
- 4.TCP提供全双工通信。
 

➡ 发送缓存	准备发送的数据&已发送但尚未收到确认的数据
接收缓存	按序到达但尚未被接受应用程序读取的数据&不按序到达的数据
- 5.TCP面向字节流 ➡ TCP把应用程序交下来的数据看成仅仅是一连串的**无结构的字节流**。

流：流入到进程或从进程流出的字节序列。

王道考研/CSKAOYAN.COM

77



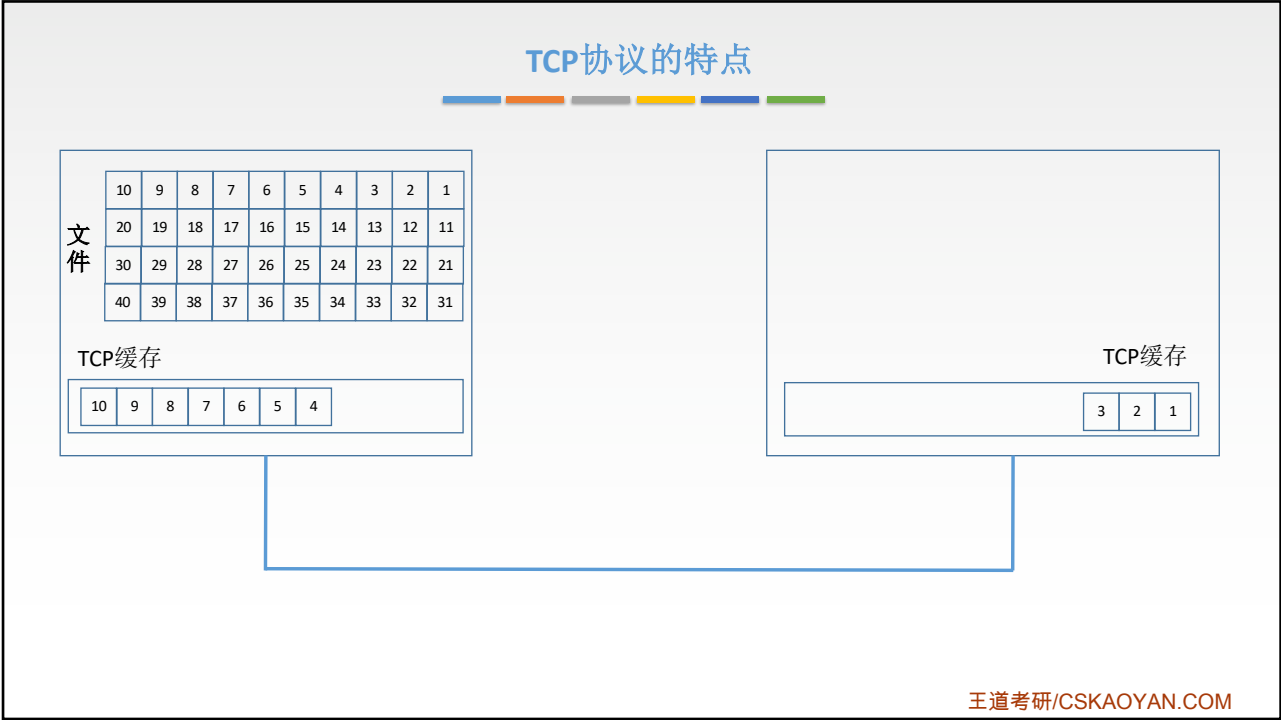
78

公众号： 考研发条      一手课程！



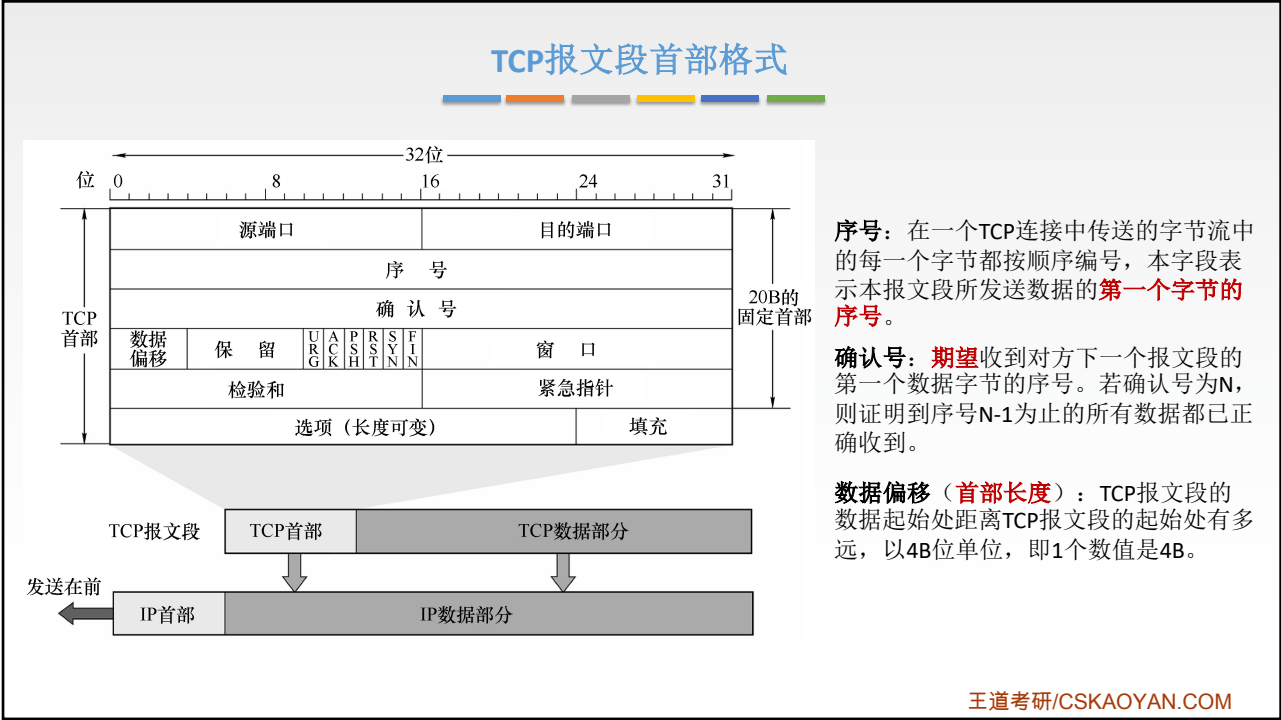
79





80

公众号： 考研发条      一手课程！

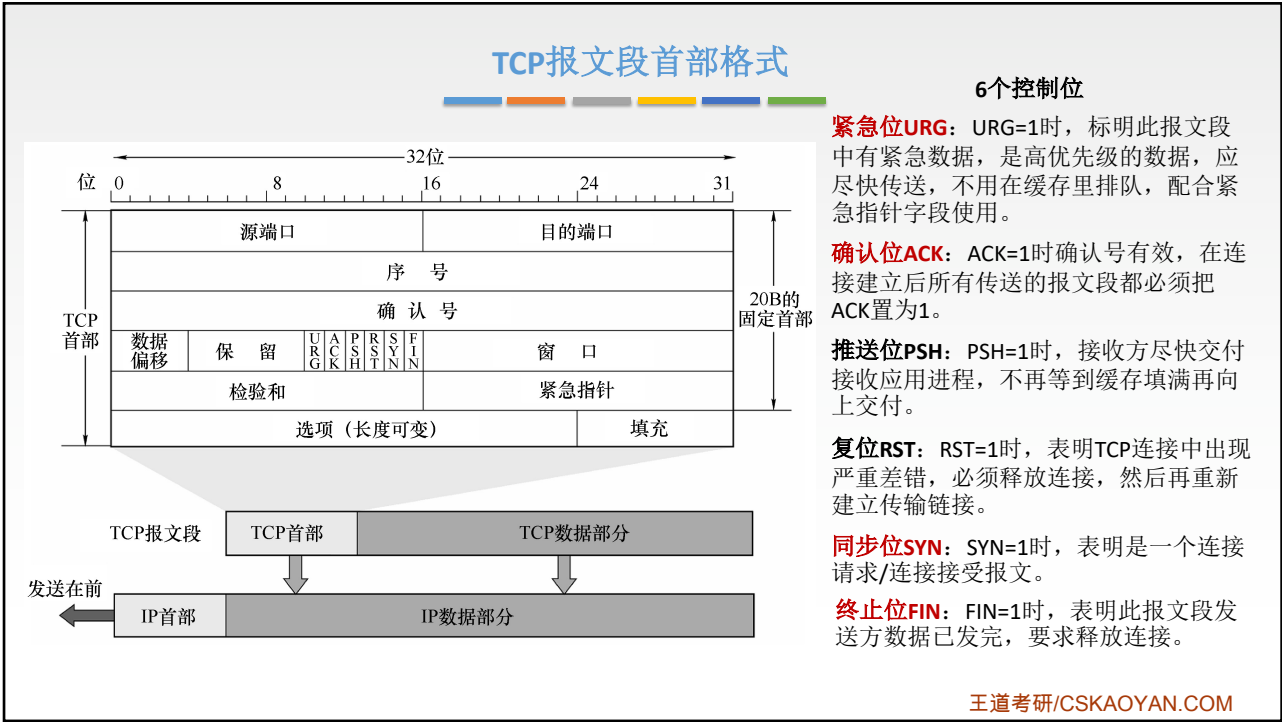


81

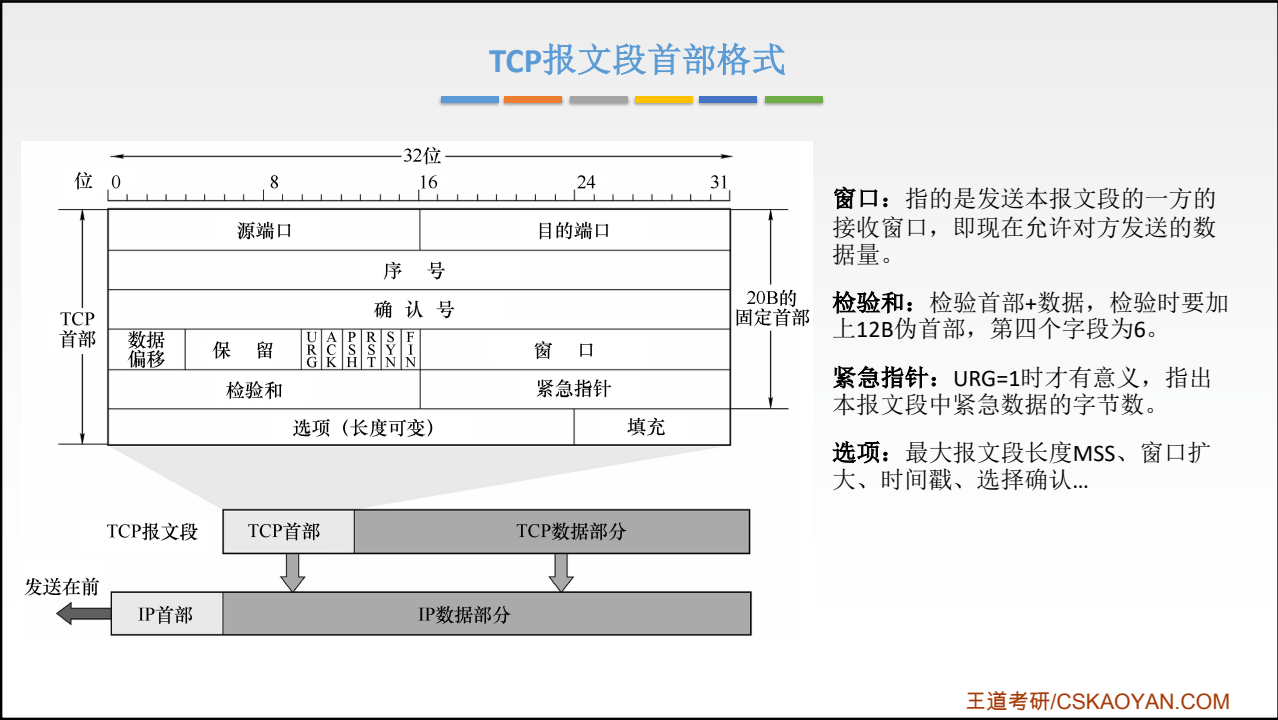


82

公众号： 考研发条      一手课程！



83



84

公众号： 考研发条      一手课程！

本节内容

TCP连接管理

王道考研/CSKAOYAN.COM

85

## TCP连接管理

TCP连接传输三个阶段：



TCP连接的建立采用**客户服务器方式**，主动发起连接建立的应用进程叫做客户，而被动等待连接建立的应用进程叫服务器。



王道考研/CSKAOYAN.COM

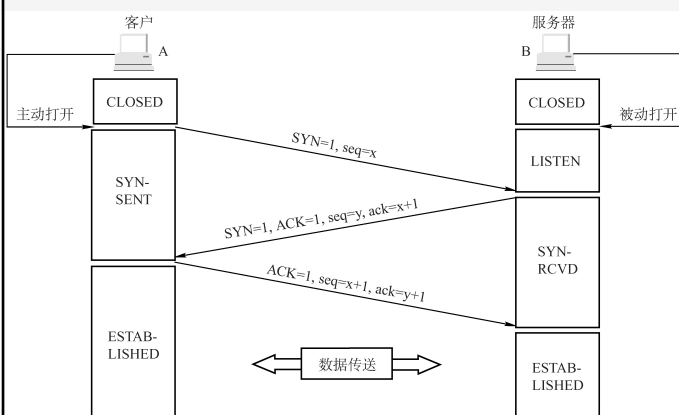
86

公众号： 考研发条

一手课程！

## TCP的连接建立

假设运行在一台主机（客户）上的一个进程想与另一台主机（服务器）上的一个进程建立一条连接，客户应用进程首先通知客户TCP，他想建立一个与服务器上某个进程之间的连接，客户中的TCP会用以下步骤与服务器中的TCP建立一条TCP连接：



### ROUND 1:

客户端发送**连接请求报文段**，无应用层数据。

$SYN=1, seq=x(\text{随机})$

### ROUND 2:

服务器端为该TCP连接**分配缓存和变量**，并向客户端返回**确认报文段**，允许连接，无应用层数据。

$SYN=1, ACK=1, seq=y(\text{随机}), ack=x+1$

### ROUND 3:

客户端为该TCP连接**分配缓存和变量**，并向服务器端返回确认的确认，可以携带数据。

$SYN=0, ACK=1, seq=x+1, ack=y+1$

王道考研/CSKAOYAN.COM

87

## SYN洪泛攻击

SYN洪泛攻击发生在OSI第四层，这种方式利用TCP协议的特性，就是三次握手。攻击者发送TCP SYN，SYN是TCP三次握手中的**第一个数据包**，而当服务器返回ACK后，该攻击者就不对其进行再确认，那这个TCP连接就处于挂起状态，也就是所谓的半连接状态，服务器收不到再确认的话，还会重复发送ACK给攻击者。这样更加会浪费服务器的资源。攻击者就对服务器发送非常大量的这种TCP连接，由于每一个都没法完成三次握手，所以在服务器上，这些TCP连接会因为挂起状态而消耗CPU和内存，最后服务器可能死机，就无法为正常用户提供服务了。

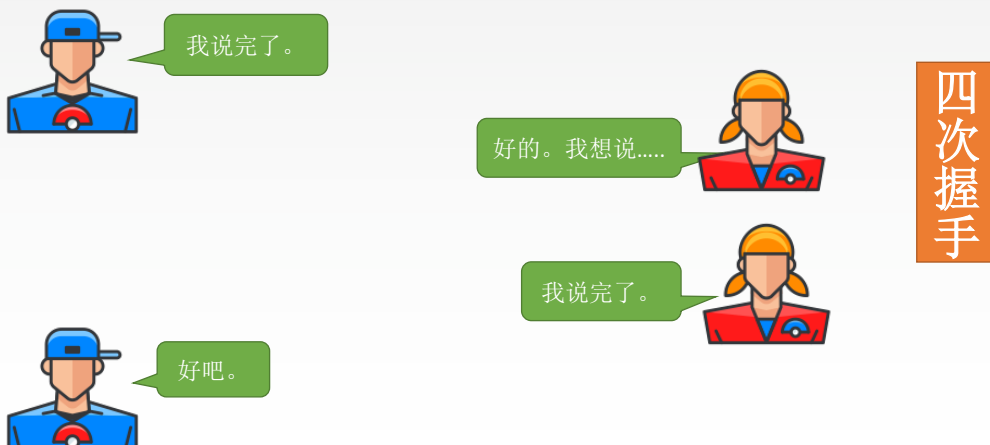
## SYN cookie

王道考研/CSKAOYAN.COM

88

公众号： 考研发条      一手课程！

## TCP的连接释放

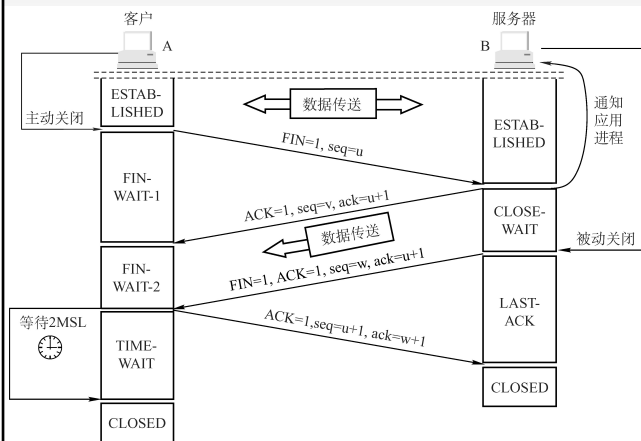


王道考研/CSKAOYAN.COM

89

## TCP的连接释放

参与一条TCP连接的两个进程中的任何一个都能终止该连接，连接结束后，主机中的“资源”（缓存和变量）将被释放。



### ROUND 1:

客户端发送**连接释放报文段**，停止发送数据，主动关闭TCP连接。

$FIN=1, seq=u$

### ROUND 2:

服务器端回送一个确认报文段，客户到服务器这个方向的连接就释放了——半关闭状态。

$ACK=1, seq=v, ack=u+1$

### ROUND 3:

服务器端发完数据，就发出连接释放报文段，主动关闭TCP连接。

$FIN=1, ACK=1, seq=w, ack=u+1$

### ROUND 4:

客户端回送一个确认报文段，再等到时间等待计时器设置的2MSL（最长报文段寿命）后，连接彻底关闭。

$ACK=1, seq=u+1, ack=w+1$

王道考研/CSKAOYAN.COM

90

公众号： 考研发条

一手课程！

本节内容

TCP可靠传输

王道考研/CSKAOYAN.COM

91

### TCP可靠传输

传输层

使用TCP实现可靠传输

网络层

提供尽最大努力交付，不可靠传输

可靠

保证接收方进程从缓存区读出的字节流与发送方发出的字节流是完全一样的。

TCP实现可靠传输的机制

1.校验

2.序号

3.确认

4.重传

与UDP校验一样，  
增加伪首部

王道考研/CSKAOYAN.COM

92

公众号： 考研发条      一手课程！

### 序号

文件

10	9	8	7	6	5	4	3	2	1
20	19	18	17	16	15	14	13	12	11
30	29	28	27	26	25	24	23	22	21
40	39	38	37	36	35	34	33	32	31

TCP缓存

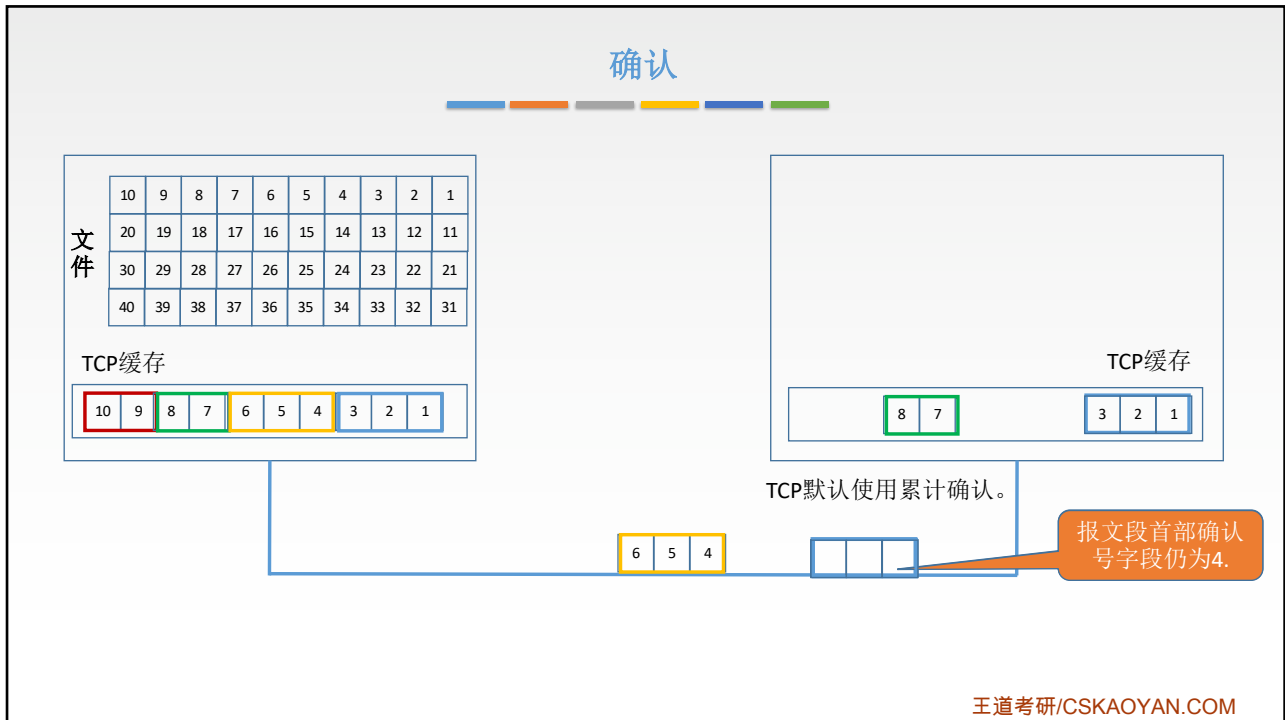
10	9	8	7	6	5	4	3	2	1
----	---	---	---	---	---	---	---	---	---

TCP缓存

一个字节占一个序号。  
序号字段指的是一个报文段第一个字节的序号。

王道考研/CSKAOYAN.COM

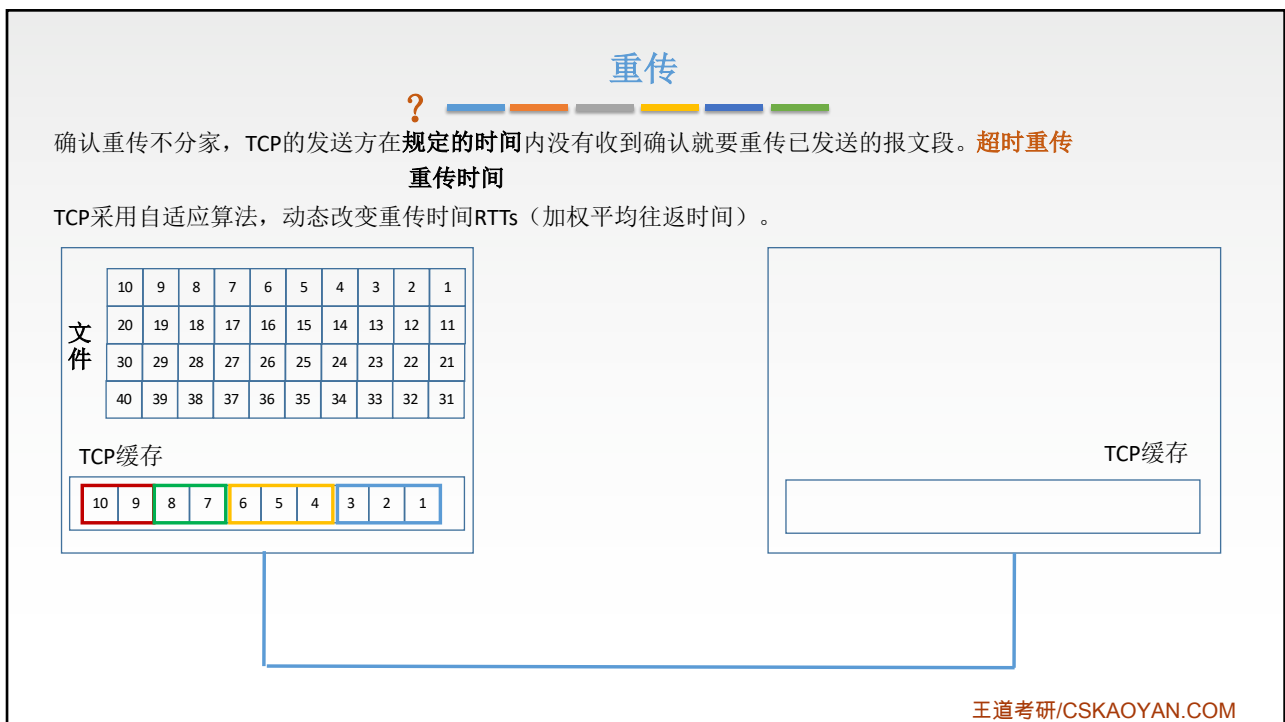
93



94

公众号： 考研发条

一手课程！



95



## 重传

?

确认重传不分家，TCP的发送方在**规定的时间内没有收到确认**就要重传已发送的报文段。**超时重传**  
**重传时间**

TCP采用自适应算法，动态改变重传时间RTTs（加权平均往返时间）。

等太久了!!!

### 冗余ACK（冗余确认）

每当比期望序号大的失序报文段到达时，发送一个**冗余ACK**，指明下一个期待字节的序号。

发送方已发送1, 2, 3, 4, 5报文段

接收方收到1，返回给1的确认（确认号为2的第一个字节）

接收方收到3，仍返回给1的确认（确认号为2的第一个字节）

接收方收到4，仍返回给1的确认（确认号为2的第一个字节）

接收方收到5，仍返回给1的确认（确认号为2的第一个字节）

发送方收到**3个对于报文段1的冗余ACK** ➡ 认为2报文段丢失，重传2号报文段 **快速重传**

王道考研/CSKAOYAN.COM

96

公众号： 考研发条

一手课程！