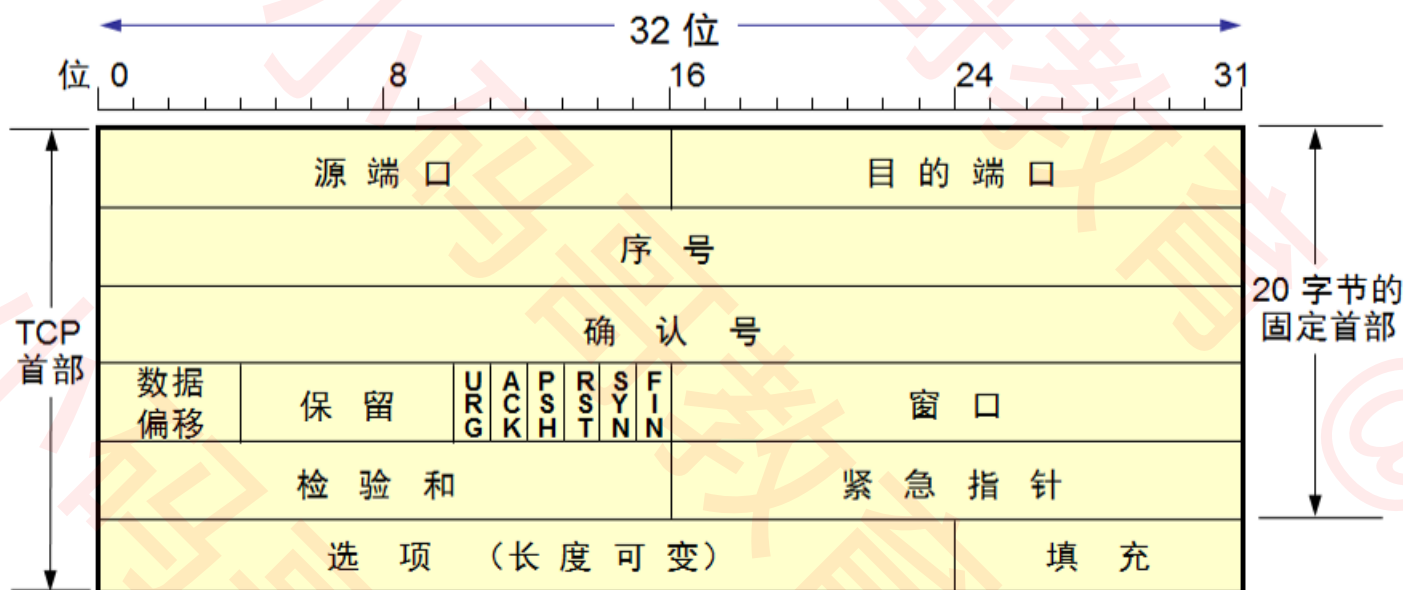


# TCP - 数据格式



## ■ 数据偏移

- 占4位，取值范围是0x0101~0x1111
- 乘以4：首部长度的 (Header Length)
- 首部长度的是20~60字节

## ■ 保留

- 占6位，目前全为0



# TCP – 小细节

## TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags			Window Size		
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

## UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

- 有些资料中，TCP首部的保留（Reserved）字段占3位，标志（Flags）字段占9位
- Wireshark中也是如此

# TCP — 一个细节

- UDP的首部中有个16位的字段记录了整个UDP报文段的长度（首部+数据）
- 但是，TCP的首部中仅仅有个4位的字段记录了TCP报文段的首部长度，并没有字段记录TCP报文段的数据长度
- 分析
  - UDP首部中占16位的长度字段是冗余的，纯粹是为了保证首部是32bit对齐
  - TCP\UDP的数据长度，完全可以由IP数据包的首部推测出来
  - ✓ 传输层的数据长度 = 网络层的总长度 - 网络层的首部长度 - 传输层的首部长度

# TCP – 检验和 (Checksum)

- 跟UDP一样，TCP检验和的计算内容：伪首部 + 首部 + 数据
- 伪首部：占用12字节，仅在计算检验和时起作用，并不会传递给网络层

TCP pseudo-header for checksum computation (IPv4)

Bit offset	0 - 3	4 - 7	8 - 15	16 - 31
0	Source address			
32	Destination address			
64	Zeros		Protocol	TCP length
96	Source port			Destination port
128	Sequence number			
160	Acknowledgement number			
192	Data offset	Reserved	Flags	Window
224	Checksum			Urgent pointer
256	Options (optional)			
256/288+	Data			

# TCP – 标志位 (Flags)

## ■ URG (Urgent)

□ 当URG=1时，紧急指针字段才有效。表明当前报文段中有紧急数据，应优先尽快传送

## ■ ACK (Acknowledgment)

□ 当ACK=1时，确认号字段才有效

## ■ PSH (Push)

## ■ RST (Reset)

□ 当RST=1时，表明连接中出现严重差错，必须释放连接，然后再重新建立连接

# TCP – 标志位 (Flags)

## ■ SYN (Synchronization)

- 当SYN=1、ACK=0时，表明这是一个建立连接的请求
- 若对方同意建立连接，则回复SYN=1、ACK=1

## ■ FIN (Finish)

- 当FIN=1时，表明数据已经发送完毕，要求释放连接

# TCP – 序号、确认号、窗口

## ■ 序号 (Sequence Number)

- 占4字节

- 首先，在传输过程的每一个字节都会有一个编号

- 在建立连接后，序号代表：这一次传给对方的TCP数据部分的第一个字节的编号

## ■ 确认号 (Acknowledgment Number)

- 占4字节

- 在建立连接后，确认号代表：期望对方下一次传过来的TCP数据部分的第一个字节的编号

## ■ 窗口 (Window)

- 占2字节

- 这个字段有流量控制功能，用以告知对方下一次允许发送的数据大小（字节为单位）

# TCP的几个要点

- 可靠传输

- 流量控制

- 拥塞控制

- 连接管理

- ☐ 建立连接

- ☐ 释放连接