TCP协议培训系列

—— 第一讲 基本概念

作者：老高

RFC 列表

1. RFC 7414: A Roadmap of TCP ….
2. RFC 793: TRANSMISSION CONTROL PROTOCOL
3. RFC 813: Windows and Acknowledge Strategy …
4. RFC 879: The TCP Maximum Segment Size …
5. RFC 896: Congestion Control in IP/TCP …
6. RFC 1122: Requirements for Internet Hosts
7. RFC 1146: TCP Alternate Checksum Options
8. RFC 1323 TCP Extensions for High Performance
9. …… …..

爱快路由（全讯汇聚）

RFC 793 —— TCP的第一个RFC

1. TCP/IP的分层

2. 为什么要有TCP？

3. TCP的基本功能

TCP/IP分层

TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP			UDP	
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet		Token Ring	Other Link-Layer Protocols	

-- 服务

-- 端对端

-- 寻路

-- 数据包发送

爱快路由（全讯汇聚）

为什么要有TCP？解决什么问题

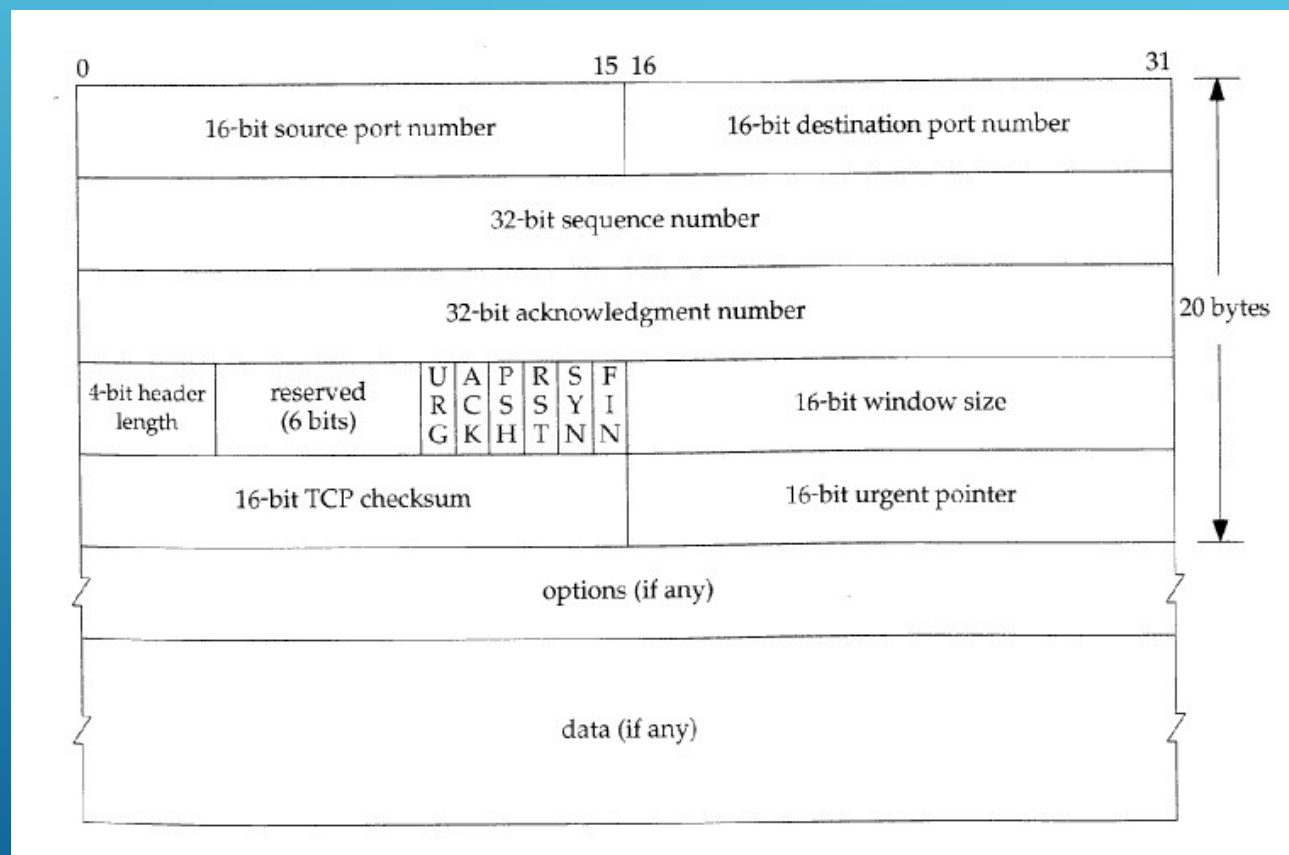## 端对端的、可靠连接！

不对底层协议做出任何假设

基本功能

1. Stream data transfer

2. Reliable

3. Flow Control

4. Multiplexing
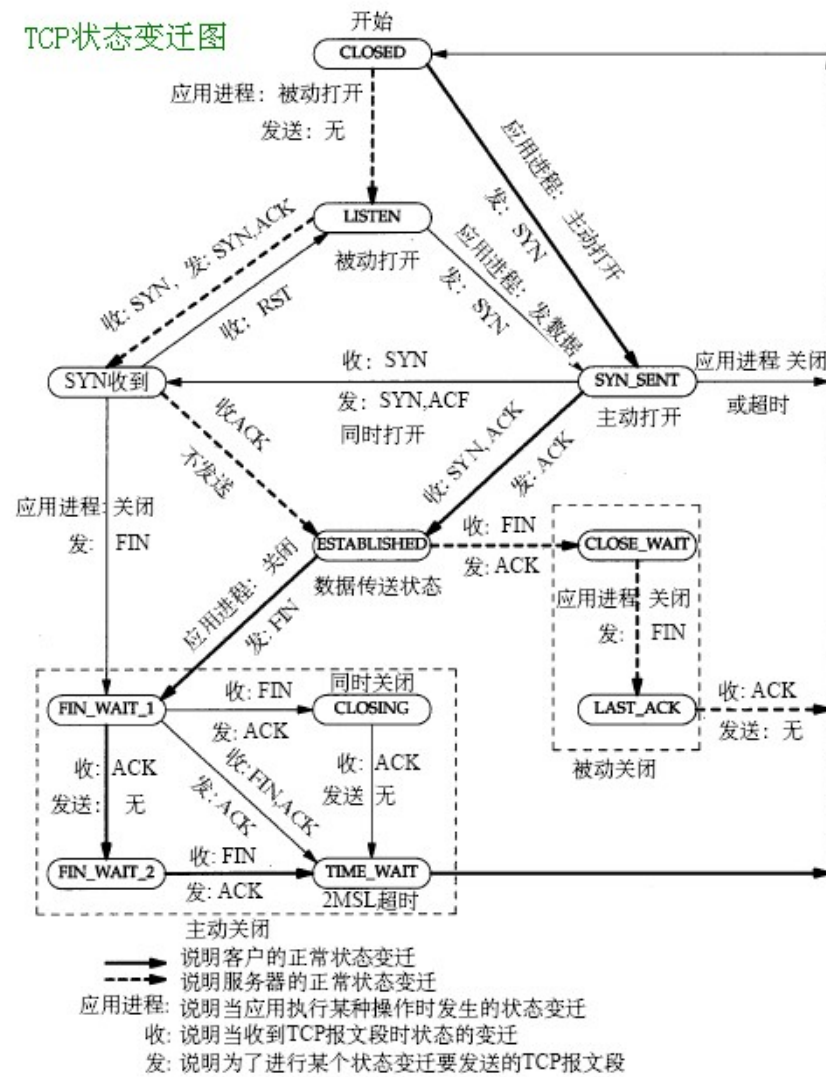
5. Connections

6. Precedence and Security —— 失败！

报文格式 —— 已过时
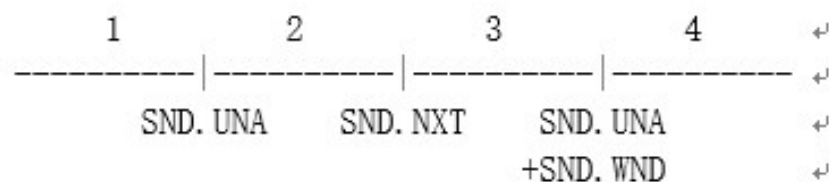
更多的控制位

1. NS：ECN-nonce concealment protection

2. CWR: Congestion Window Reduced

3. ECE: ECN-Echo

TCP状态变迁图

爱快路由（全讯汇聚）

发送序列

```
                1           2           3           4        ↵
        ----------|----------|----------|----------  ↵
              SND.UNA     SND.NXT     SND.UNA              ↵
                                      +SND.WND             ↵

1 - old sequence numbers which have been acknowledged  ↵
2 - sequence numbers of unacknowledged data            ↵
3 - sequence numbers allowed for new data transmission ↵
4 - future sequence numbers which are not yet allowed  ↵
```
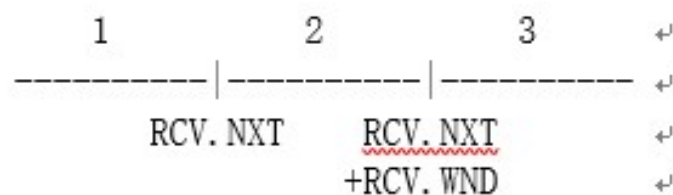
接收序列


```
     1              2            3       ↵
 ----------|----------|----------      ↵
    RCV. NXT      RCV. NXT             ↵
                  +RCV. WND            ↵

1 - old sequence numbers which have been acknowledged  ↵
2 - sequence numbers allowed for new reception          ↵
3 - future sequence numbers which are not yet allowed    ↵
```

什么样的ACK会被接受？

SND.UNA < SEG.ACK =< SND.NXT

什么样的SEQ会被接受？

RCV.NXT =< SEG.SEQ < RCV.NXT+RCV.WND

or

RCV.NXT =< SEG.SEQ+SEG.LEN-1 < RCV.NXT+RCV.WND

初始化序列号与序号回绕

1. ISN generator: 4 ms递增；4.55小时回绕；

2. 序号回绕

```
Network        B*8          B            Twrap
               bits/sec     bytes/sec    secs
               --------     ---------    -----

ARPANET        56kbps       7KBps        3*10**5 (~3.6 days)

DS1            1.5Mbps      190KBps      10**4 (~3 hours)

Ethernet       10Mbps       1.25MBps     1700 (~30 mins)

DS3            45Mbps       5.6MBps      380

FDDI           100Mbps      12.5MBps     170

Gigabit        1Gbps        125MBps      17
```

序号回绕—— 如何破？！

RFC1323: TCP Exensions for High Performance

PAWS: Protect Against Wrapped Sequence Numbers

RESET的发送和处理

1. Close状态；

2. Non-synchronized状态；

3. 其它情况——一般会由防火墙，网关设备发出；

4. 校验Reset包 —— Reset攻击

爱快路由（全讯汇聚）

FIN的含义是什么？关闭连接？

1. "我不要再发数据了"
2. 可以读，不能写
3. Socket操作为shutdown，而不是close

爱快路由（全讯汇聚）

问题

1. 同时发syn会怎么样？

2. Zero-Window问题：如何处理？可以接收什么数据包？

3. Syn和fin是否占用sequence？为什么

本节结束
下集预告：RFC 813, ...

求贤若渴
欢迎Linux C/C++开发一起学习进步
内核、应用、服务端、嵌入式我们都要☺
fgao@ikuai8.com

爱快路由（全讯汇聚）