

# The Network Stack (2)

Lecture 6, Part 1: TCP

Prof. Robert N. M. Watson

2021-2022

# The Network Stack (2)

- The Transmission Control Protocol (TCP)
  - The TCP state machine
  - TCP congestion control
  - TCP implementations and performance
  - The evolving TCP stack
  - Lab 3 on TCP
- Wrapping up the Advanced Operating Systems lecture series

Lecture 6, Part 1

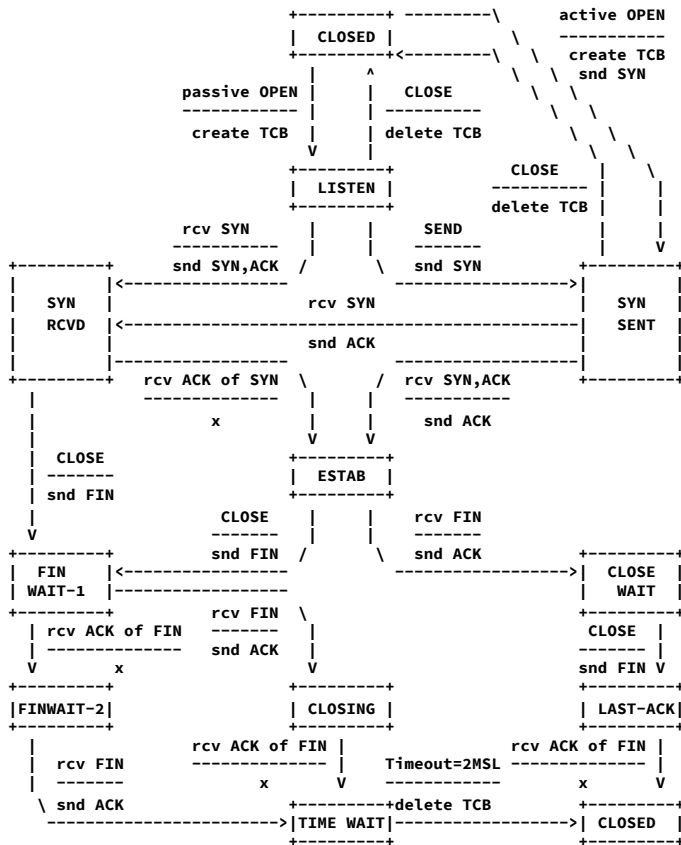
Lecture 6, Part 2

Lecture 6, Part 3

# The Transmission Control Protocol (TCP)

September 1981

Transmission Control Protocol  
Functional Specification

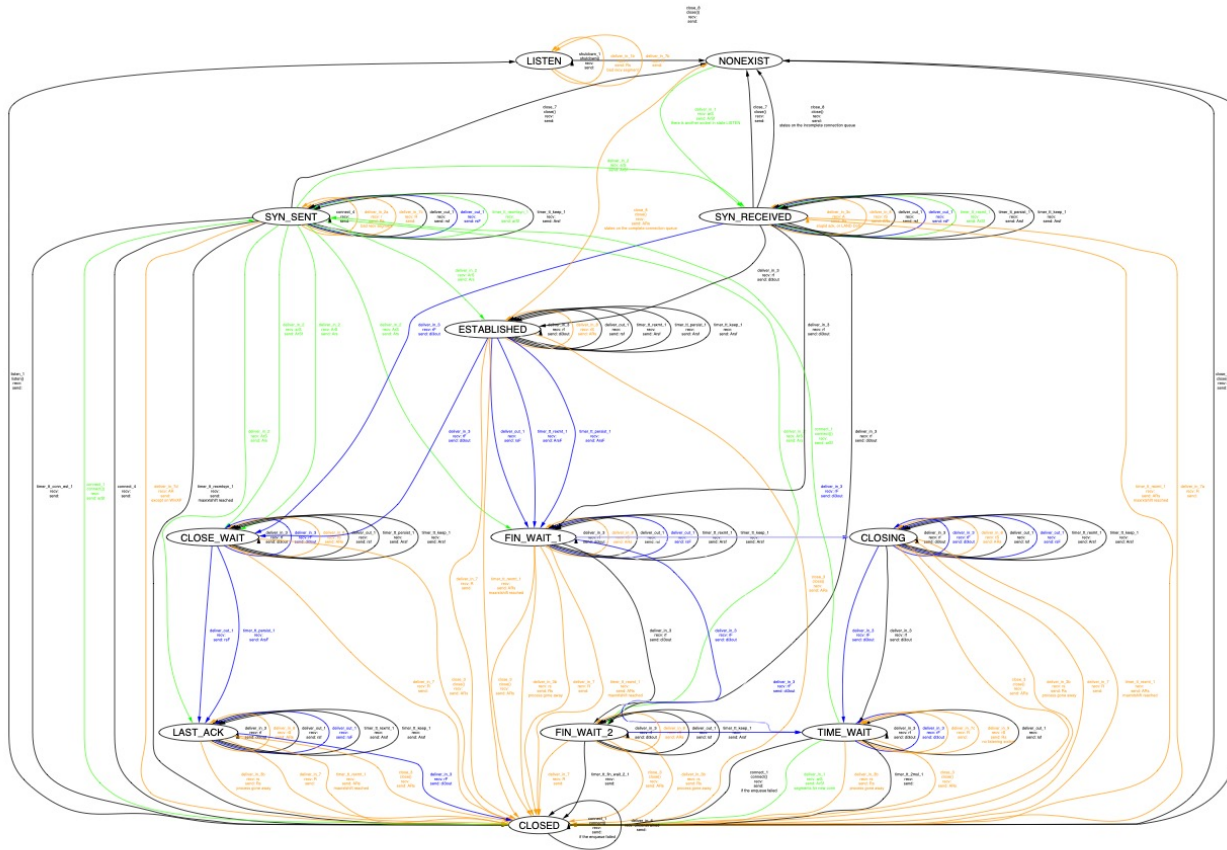


TCP Connection State Diagram  
Figure 6.

- V. Cerf, K. Dalal, and C. Sunshine, ***Transmission Control Protocol (version 1)***, INWG General Note #72, December 1974.
- In practice: J. Postel, Ed., ***Transmission Control Protocol: Protocol Specification***, RFC 793, September, 1981.

# Compare to Bishop, et al (2005)

## TCP: an approximation to the real state diagram



<http://www.cl.cam.ac.uk/users/pes20/Netsem>  
March 18, 2005

### What Is This?

This graph shows an approximation to the Host Transition System of the TCP specification.

TCP, UDP and Sockets: rigorous and experimentally-validated behavioural specification. Volume 1: Overview. Volume 2: The Specification. Steven Bishop, Matthew Fairbairn, Michael Norrish, Peter Sewell, Michael Smith, and Keith Wansbrough. 2005.

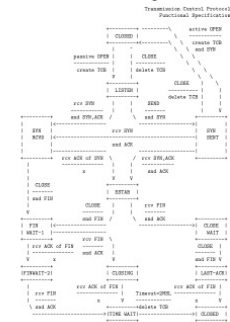
The states are the classic 'TCP states', though note that these are only a tiny part of the protocol endpoint state, in the specification or in implementations. The transitions are an over-approximation to the set of all the transitions in the model which (1) affect the TCP state of a socket, and/or (2) involve processing segments from the host's input queue or adding them to its output queue, except that transitions involving ICMPv4 are omitted, as are transitions arising from the pathological BSD behaviour in which arbitrary sockets can be moved to LISTEN states. Transitions are labelled by their Host LTS rule name (e.g. socket.L, deliver.m.2, etc.), any socket call involved (e.g. close()), and constraints on the flags of any TCP segment received and sent, with e.g. R indicating that RST is set and r indicating RST is clear. Transitions involving segments (either inbound or outbound) with RST set are coloured orange; others that have SYN set are coloured green; others that have FIN set are coloured blue; others are coloured black. The FIN indication includes the case of FINs that are constructed by reassembly rather than appearing in a literal segment.

The graph is based on data extracted manually from the HOL specification. The data does not capture all the invariants of the model, so some disjunct transitions may not be reachable in the model (or in practice). Similarly, the constraints on flags shown may be overly weak.

### Transition Rules

- listen\_0 Successfully creates a new socket
- listen\_1 Successfully closes the host's behaviour to enable the CLOSED state
- listen\_2 SYN\_RECV → SYN\_RECEIVED state
- listen\_3 Successfully closes the host's behaviour for a listening TCP socket
- listen\_4
- listen\_5
- listen\_6
- listen\_7
- listen\_8
- listen\_9
- listen\_10
- listen\_11
- listen\_12
- listen\_13
- listen\_14
- listen\_15
- listen\_16
- listen\_17
- listen\_18
- listen\_19
- listen\_20
- listen\_21
- listen\_22
- listen\_23
- listen\_24
- listen\_25
- listen\_26
- listen\_27
- listen\_28
- listen\_29
- listen\_30
- listen\_31
- listen\_32
- listen\_33
- listen\_34
- listen\_35
- listen\_36
- listen\_37
- listen\_38
- listen\_39
- listen\_40
- listen\_41
- listen\_42
- listen\_43
- listen\_44
- listen\_45
- listen\_46
- listen\_47
- listen\_48
- listen\_49
- listen\_50
- listen\_51
- listen\_52
- listen\_53
- listen\_54
- listen\_55
- listen\_56
- listen\_57
- listen\_58
- listen\_59
- listen\_60
- listen\_61
- listen\_62
- listen\_63
- listen\_64
- listen\_65
- listen\_66
- listen\_67
- listen\_68
- listen\_69
- listen\_70
- listen\_71
- listen\_72
- listen\_73
- listen\_74
- listen\_75
- listen\_76
- listen\_77
- listen\_78
- listen\_79
- listen\_80
- listen\_81
- listen\_82
- listen\_83
- listen\_84
- listen\_85
- listen\_86
- listen\_87
- listen\_88
- listen\_89
- listen\_90
- listen\_91
- listen\_92
- listen\_93
- listen\_94
- listen\_95
- listen\_96
- listen\_97
- listen\_98
- listen\_99

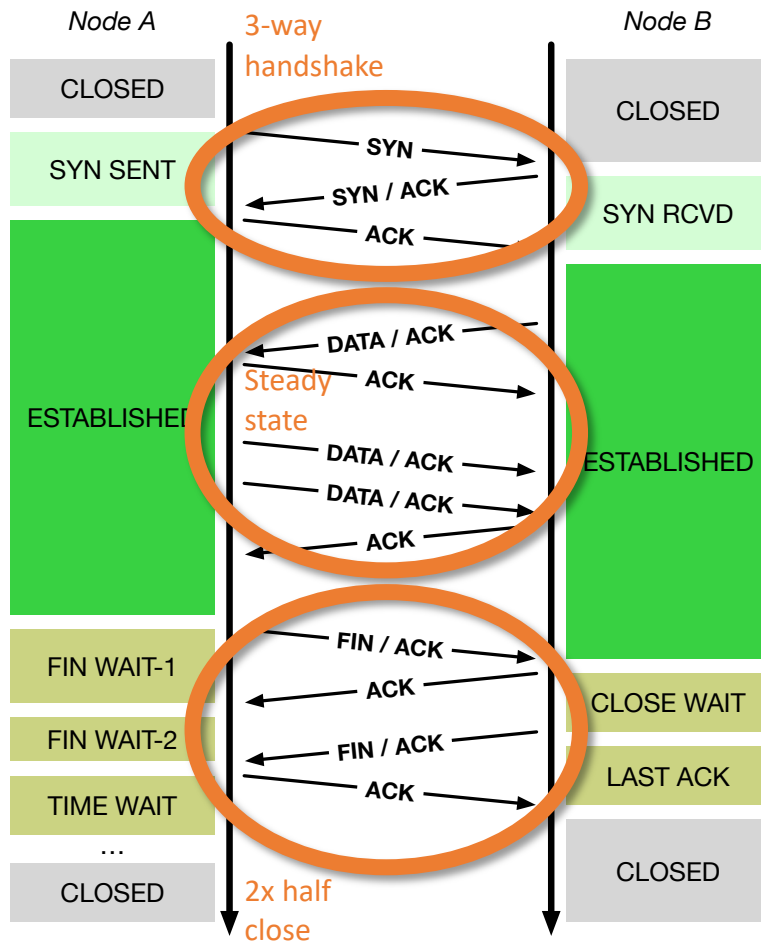
### The RFC793 Original



TCP Observation Diagram  
Page 6  
September 1981

Steve Bishop, Matthew Fairbairn, Michael Norrish, Peter Sewell, Michael Smith, and Keith Wansbrough. **Rigorous Specification and Conformance Testing Techniques for Network Protocols, as Applied to TCP, UDP, and Sockets.** Proceedings of SIGCOMM 2005, ACM, 2005.

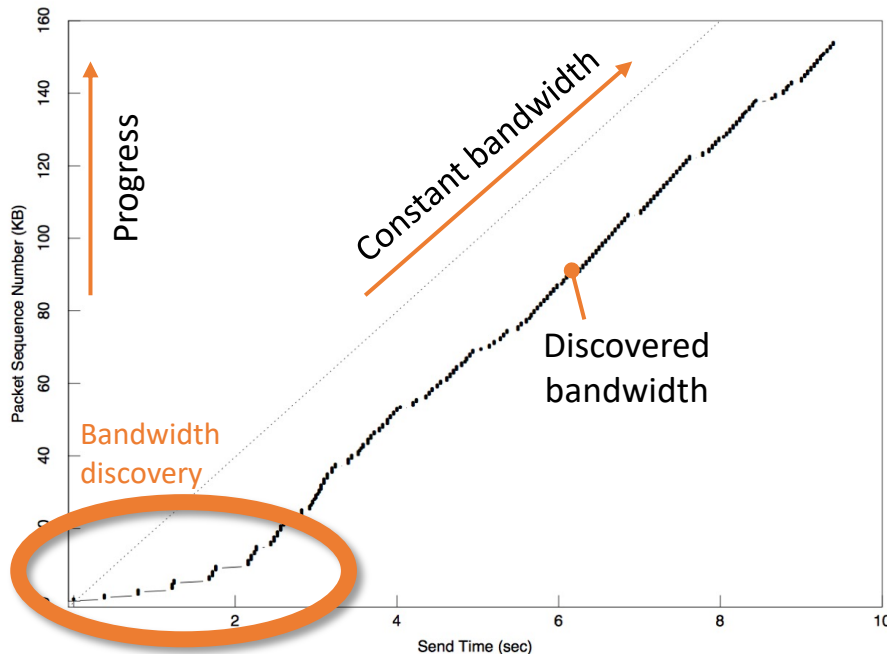
# TCP principles and properties



- Assumptions: Network may delay, (reorder), drop, corrupt IP packets
- TCP implements reliable, ordered, stream transport protocol over IP
- Three-way handshake: SYN / SYN-ACK / ACK (mostly!)
- Steady state
  - Sequence numbers ACK'd
  - Round-Trip Time (RTT) measured to time out loss
  - Data retransmitted on loss
  - Flow control via advertised window size in ACKs
  - Congestion control ("fairness") detects congestion via loss (and, recently, via delay: BBR)
- NB: "Half close" allows communications in one direction to end while the other continues

# TCP congestion control and avoidance

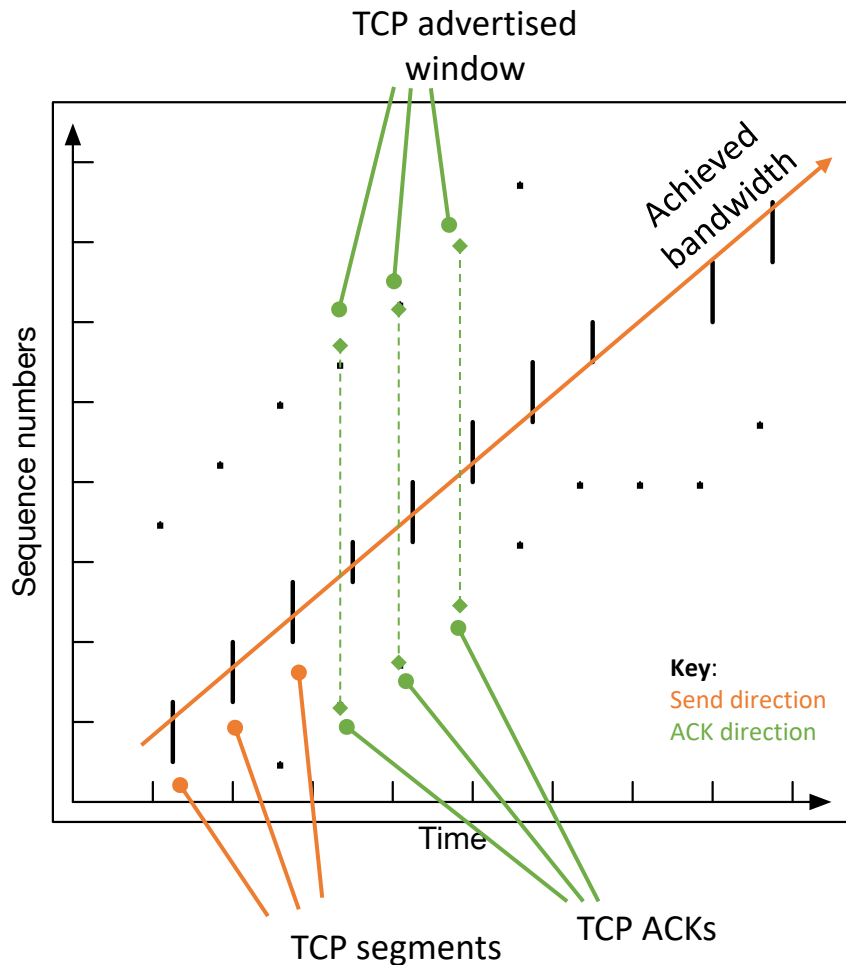
Figure 4: Startup behavior of TCP with Slow-start



Same conditions as the previous figure (same time of day, same Suns, same network path, same buffer and window sizes), except the machines were running the 4.3<sup>+</sup> TCP with slow-start. No bandwidth is wasted on retransmits but two seconds is spent on the slow-start so the effective bandwidth of this part of the trace is 16 KBps — two times better than figure 3. (This is slightly misleading: Unlike the previous figure, the slope of the trace is 20 KBps and the effect of the 2 second offset decreases as the trace lengthens. E.g., if this trace had run a minute, the effective bandwidth would have been 19 KBps. The effective bandwidth without slow-start stays at 7 KBps no matter how long the trace.)

- 1986 Internet CC collapse
  - 32Kbps → **40bps**
- Van Jacobson, SIGCOMM 1988
  - Don't send more data than the network can handle!
  - **Conservation of packets** via ACK clocking
  - Exponential retransmit timer, slow start, aggressive receiver ACK, dynamic window sizing on congestion, and (later) ABC
- ECN (RFC 3168), ABC (RFC 3465), Compound (Tan, et al, INFOCOM 2006), Cubic (Rhee and Xu, ACM OSR 2008), BBR (Cardwell, ACM Queue 2016)

# TCP time/sequence graphs (Van Jacobson)



- Extracted from TCP packet traces (e.g., via tcpdump)
- Visualize windows, congestion response, buffering, RTT, etc:
  - X: Time
  - Y: Sequence number
- We can extract this data from the network stack directly using DTrace
  - Allows correlation/plotting with respect to other variables / events
  - E.g., TCP and socket-buffer state
- TCP time/sequence diagrams have since been extended to represent additional information
  - E.g., SACK (selective acknowledgement) blocks