Computer Networks
-Transport/Network layer III.-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W5 short test (1)

- What is the process of Store-and-Forward packet switching?
  - The host with a packet to send transmits it to the nearest router, where the packet is stored until it has fully arrived and the link has finished its processing. Then it is forwarded to the next router until it reaches the destination.
- What are the routing tables?
  - The routing algorithm is responsible for filling in and updating the routing tables; it tells where to send packets for each of the possible destinations. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination.
- Why congestion management is important?
  - Managing/mitigating congestion is important, because too many packets introduce packet delay and loss that degrades performance, that basically results in less traffic being successfully delivered.

W5 short test (2)

- What is the main difference between transparent and nontransparent packet fragmentation?
  - Unlike transparent fragmentation, the nontransparent strategy refrains from recombining fragments at the intermediate routers. Once a packet has been fragmented, each fragment is treated as it were an original packet.
- What the Total length field is referring to in the IPv4 header?
  - Length of both the header and data, maximum of 65,535 bytes.
- How many IPv4 addresses would be associated with a prefix of /25 (block size)?
  - $2^7 = 128$

W5 recap (1)

- Running out of IP addresses: assign each home or business a single IP for traffic, but within the customer network, every computer gets a unique IP
- Using NAT, before the packet exists the customer network and goes to the ISP, the address is translated from internal to a the shared public IP
- Even with efficiently using CIDR and NAT, running out of addresses is a problem
- IPv6 has longer addresses than IPv4, simplified header, better support for options, and generally better security
  - headers: differentiated services, flow, payload length, next header, hop limit, source and destination addresses
  - extension headers
- The ICMP is used by routers to send operational information and error messages to other addresses
- The ARP is used to identify data link layer addresses associated with an IP address

W5 recap (2)

- Inside its own network, organizations can use their own IGPs, but routing between independently operated networks must be done with the same exterior gateway protocol (BGP for the Internet)
- Using DHCP, the DHCP server automatically assigns an IP address per request
- The transport layer builds on the network layer to provide data transport with a desired level of reliability
- The goal is to provide reliable data-transmission service to users in the application layer, using the services from the network layer
- Segments exchanged by the transport layer are contained in packets which are exchanged by the network layer, while packets are contained in frames exchanged by the data link layer

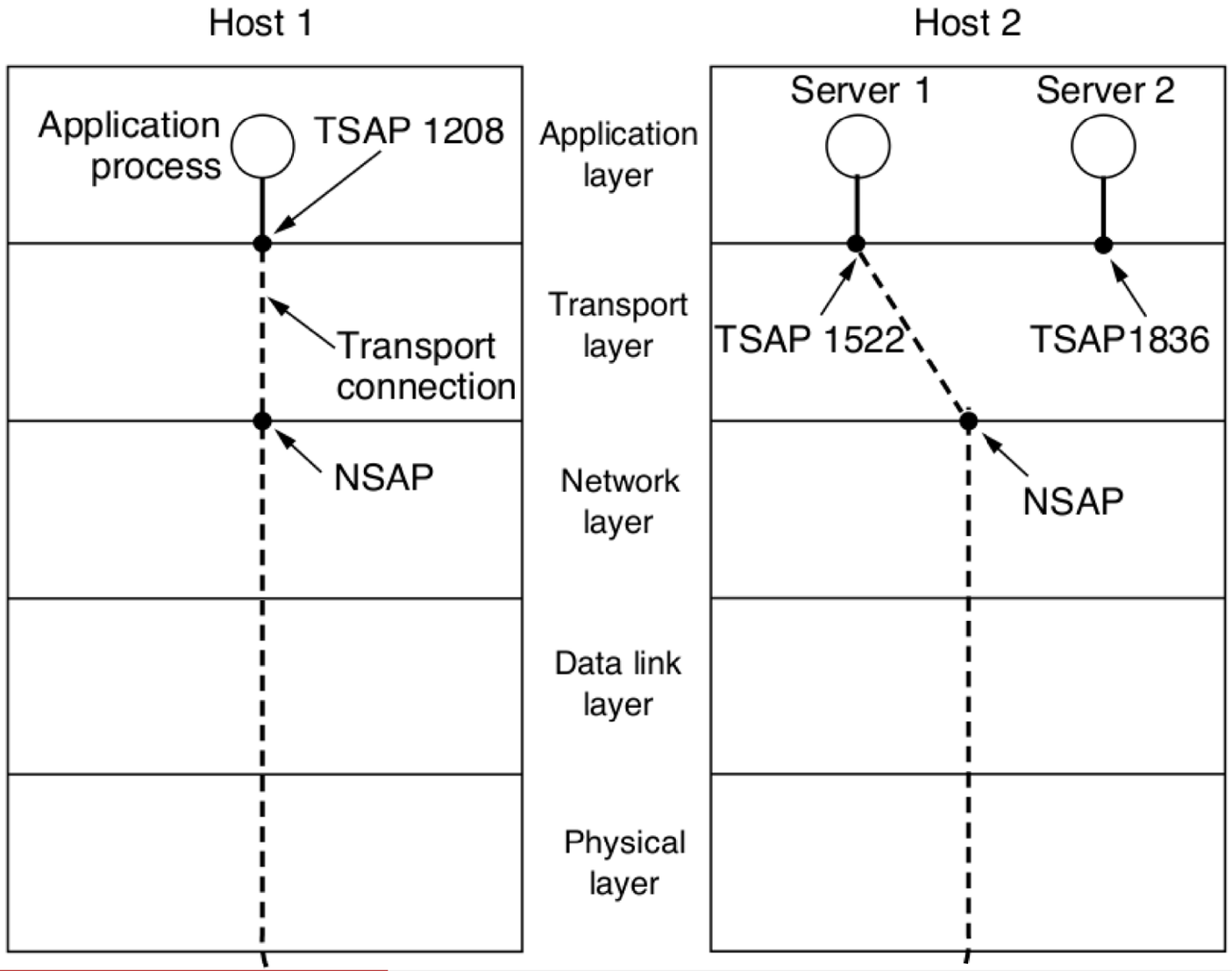
Agenda

- Transport protocol elements
- Connection establishment
- Internet transport protocols
- Summary

Addressing (1)

- The transport service is implemented by a **transport protocol**
- When an application process wishes to set up a connection to a remote application process, it must specify which process on the remote endpoint to connect to
  - in the Internet, endpoints are called **ports**
  - **TSAP** (Transport Service Access Point) is a specific endpoint in the transport layer, such as a port
  - network layer addresses are called **NSAP** (Network Service Access Point), such as IP addresses
- Application processes can attach themselves to a local TSAP to establish a connection to a remote TSAP
- The connections run through NSAPs on each host

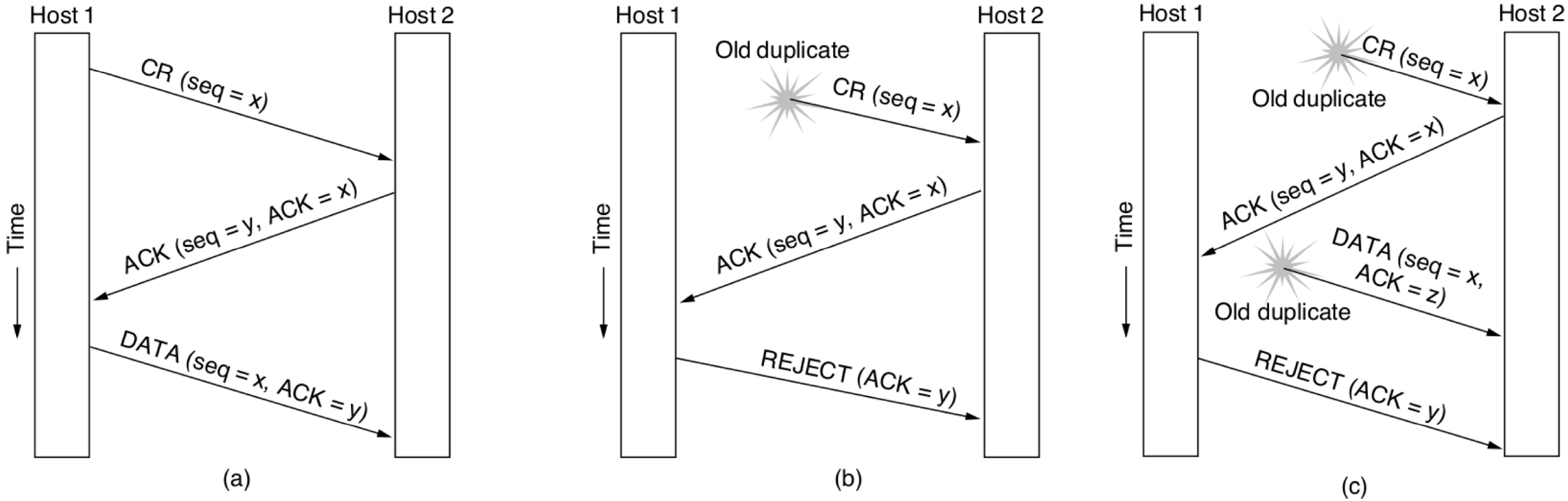
Addressing (2)



The three-way handshake (1)

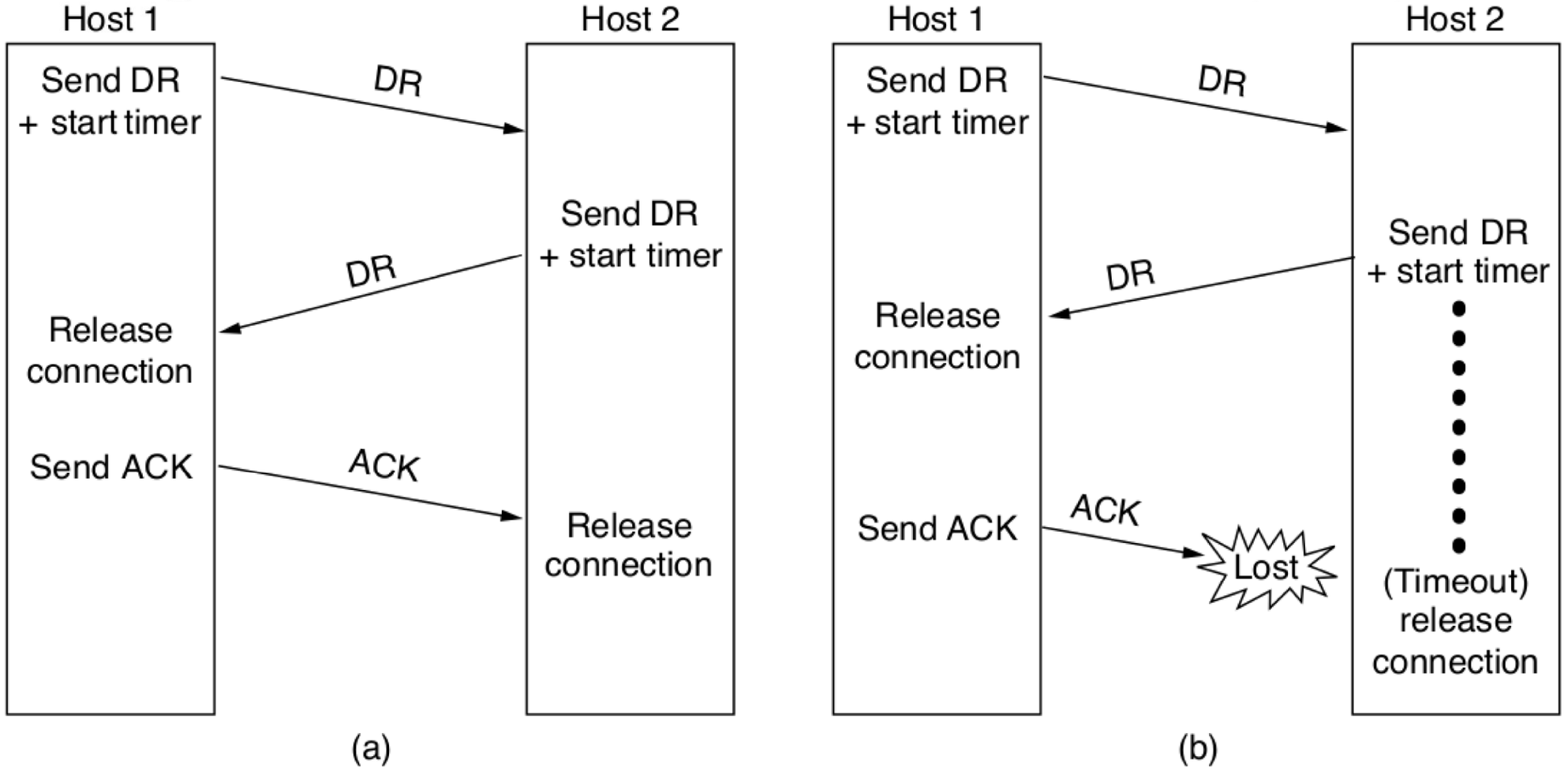
- To establish a connection, a transport entity would send a CONNECTION REQUEST segment to the destination and wait for a CONNECTION ACCEPTED reply
  - the problem is that a network can lose, delay, corrupt, and duplicate packets
- The **three-way handshake** involves one peer checking with the other that the connection request is indeed current
- TCP uses this method to establish connections

The three-way handshake (2)

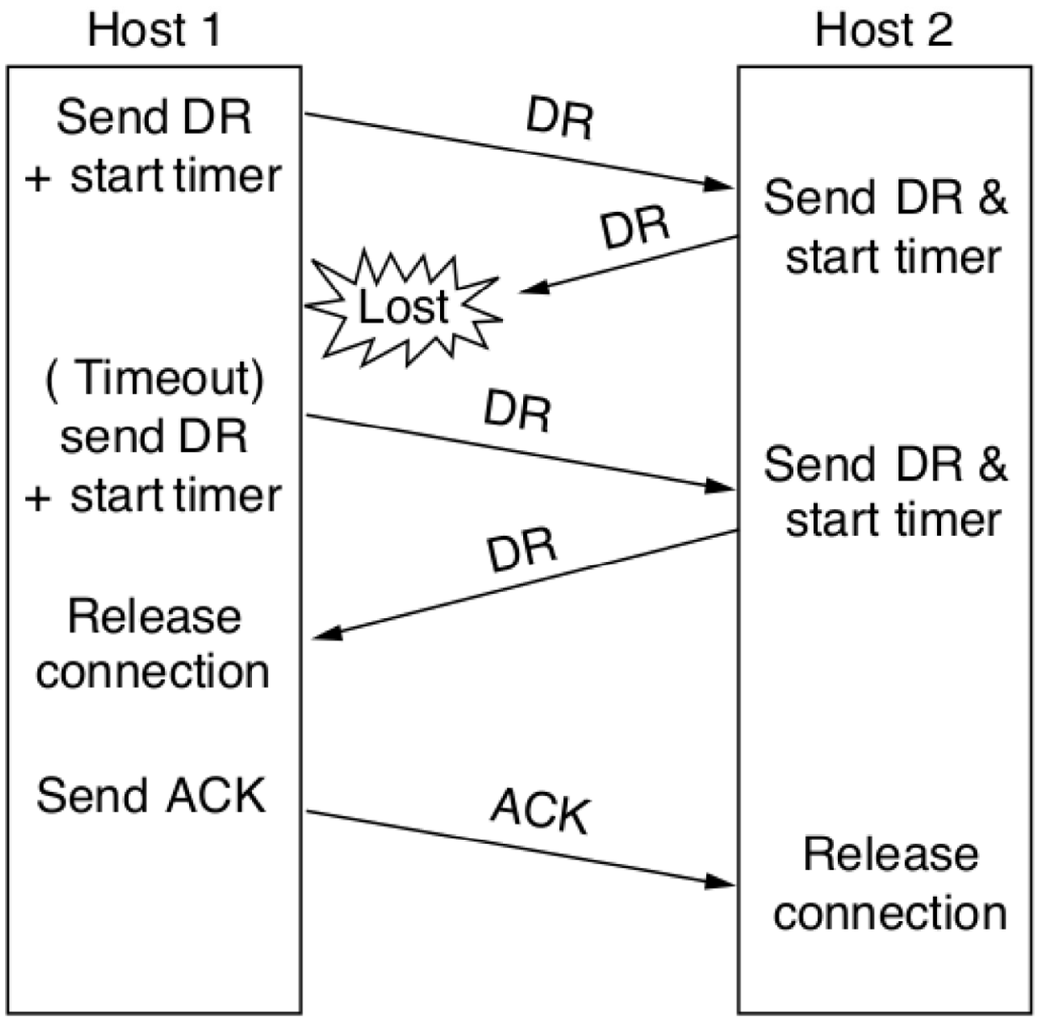


Releasing the connection (1)

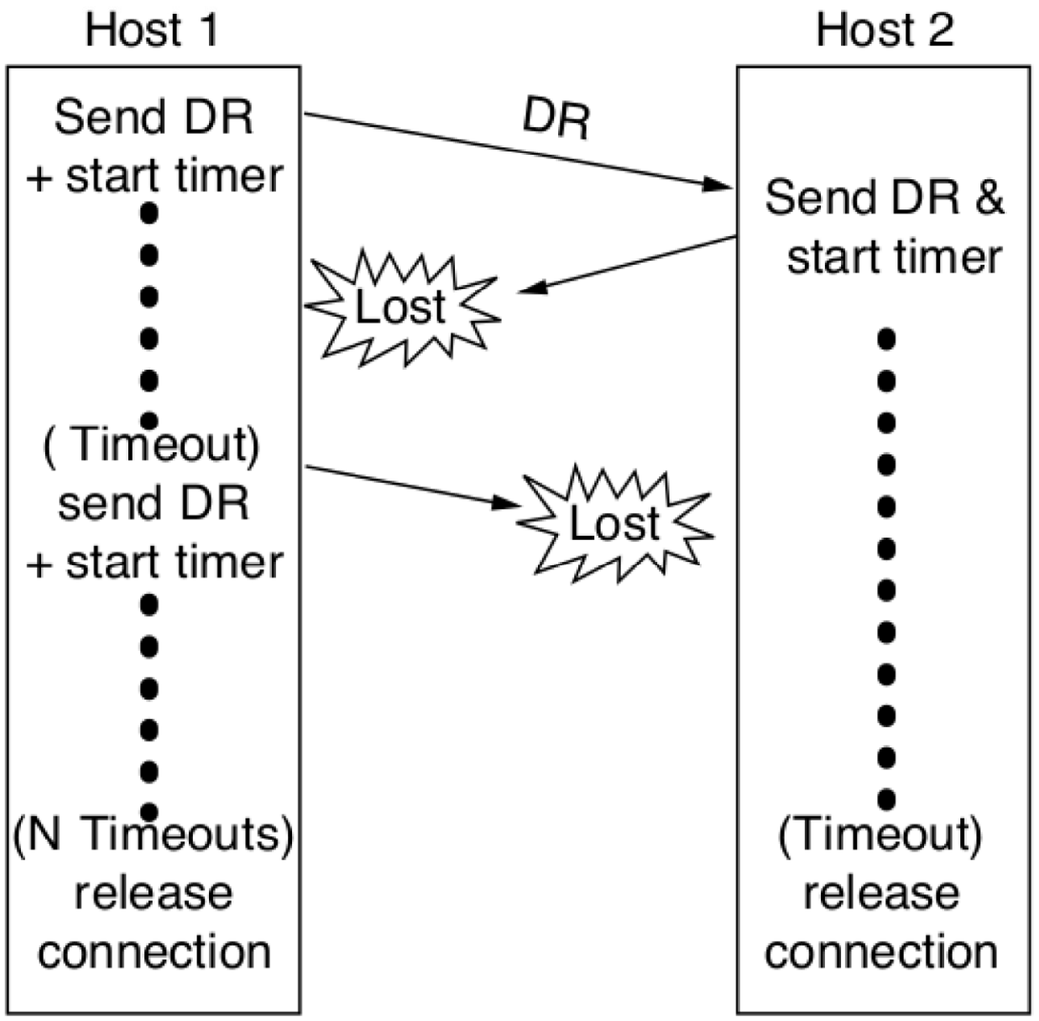
- Releasing a connection can be done asymmetrically or symmetrically



Releasing the connection (2)



(c)



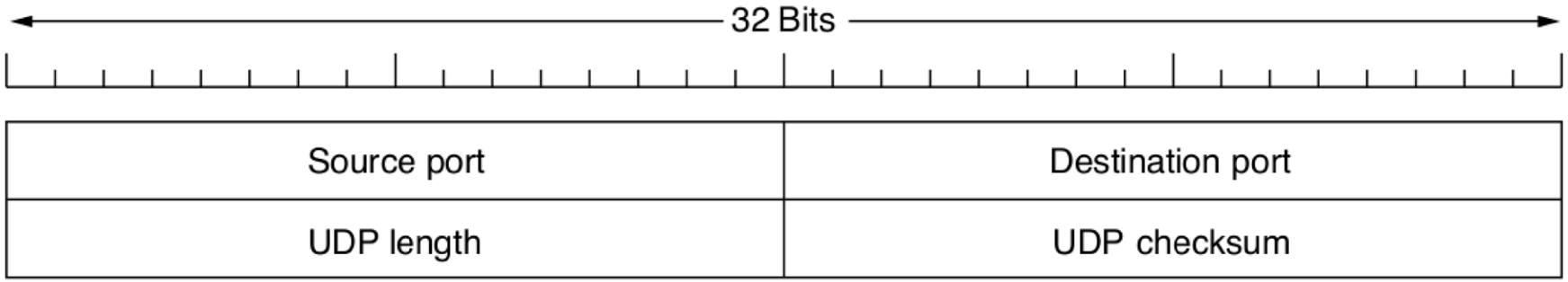
(d)

Other transport issues

- Error control ensures that the data is delivered with the desired level of reliability (all data is delivered without errors)
- Flow control is about keeping a fast transmitter from overrunning a slow receiver
- Multiplexing is about managing several conversations over connections, virtual circuits and physical links (e.g., only one network address is available on a host and all transport connections have to use it)
- Since host and routers can crash, recovery from crashes is an important issue
- Network congestion happens when the transport entities send too many packets into the network too quickly (e.g., degraded performance, lost and delayed packets, etc.)

UDP

- Two main protocols in the transport layer: a connectionless (UDP) and a connection-oriented (TCP)
- **UDP** (User Datagram Protocol) provides a way for applications to send encapsulated IP datagrams without having to establish a connection
- It transmits segments of a header and a payload
- Does not do flow and congestion control, or retransmission upon receipt of bad segment
- Useful in client-server situations, when the client sends a short request to the server and expects a short reply back (e.g., DNS, multimedia, broadcasting)



TCP basics

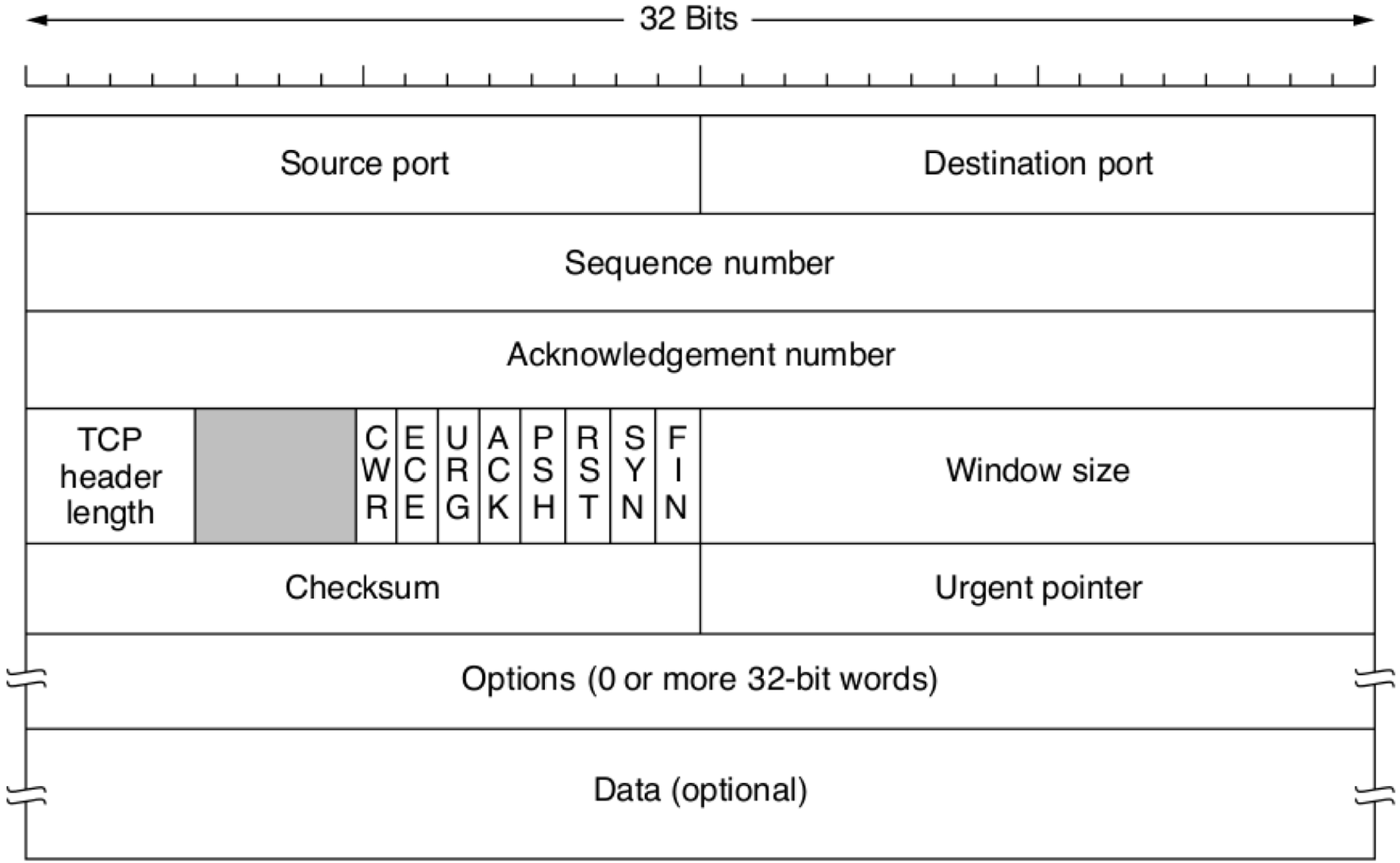
- Most Internet applications require a reliable, sequenced delivery: **TCP**(Transmission Control Protocol)
- The TCP service is obtained by both the sender and the receiver creating endpoints called sockets
- Each socket has a socket number/address consisting of the IP address of the host and a 16-bit number local to the host called a port (TCP name for a TSAP)
  - it is a connection between sockets of different machines
- TCP connections are full duplex and point-to-point: traffic can go in both directions at the same time, and each connection has exactly two end points

Common ports

- Port numbers below 1024 are reserved for standard services

Port	Protocol	Use
20, 21	FTP	File transfer
22	SSH	Remote login, replacement for Telnet
25	SMTP	Email
80	HTTP	World Wide Web
110	POP-3	Remote email access
143	IMAP	Remote email access
443	HTTPS	Secure Web (HTTP over SSL/TLS)
543	RTSP	Media player control
631	IPP	Printer sharing

The TCP header (1)



The TCP header (2)

- The **source port** and **destination port** field identify the local end points of the connection (to identify a connection: protocol, source IP and port, destination IP and port)
- The **sequence number** is the byte number of the first byte of data in the TCP packet sent
- The **acknowledgement number** is the sequence number of the next byte the receiver expects to receive
- The **TCP header length** tells how many 32-bit words are contained in the TCP header

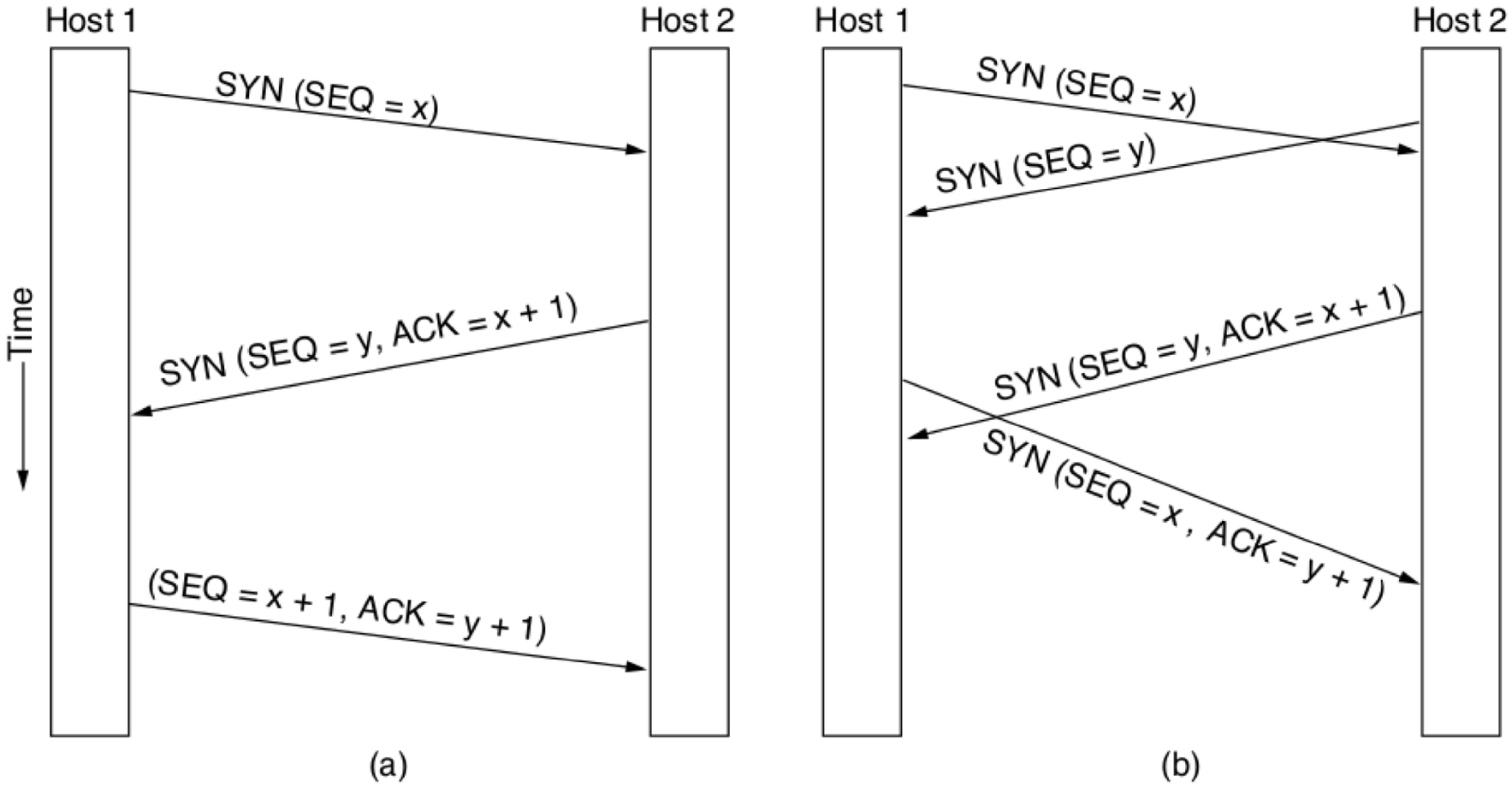
The TCP header (3)

- CWR and ECE are used to signal congestion when Explicit Congestion Notification (ECN) is used: ECE echos to a TCP sender to tell it to slow down if there is congestion, and CWR signals the TCP receiver so that it knows the sender has slowed down, and can stop sending ECN-echo
- URG is 1 if Urgent pointer is used, indicating a byte offset from the current sequence number at which urgent data are to be found (no queue for processing)
- When ACK is 1, it indicates that the Acknowledgement number is valid (if 0, the segment does not contain an acknowledgement)
- PSH indicates pushed data: the receiver is requested to deliver the data to the application upon arrival (no buffering until a full buffer has been received)
- The RST bit is used to reset a connection if there is a host crash, etc., or refuse an attempt to open a connection

The TCP header (4)

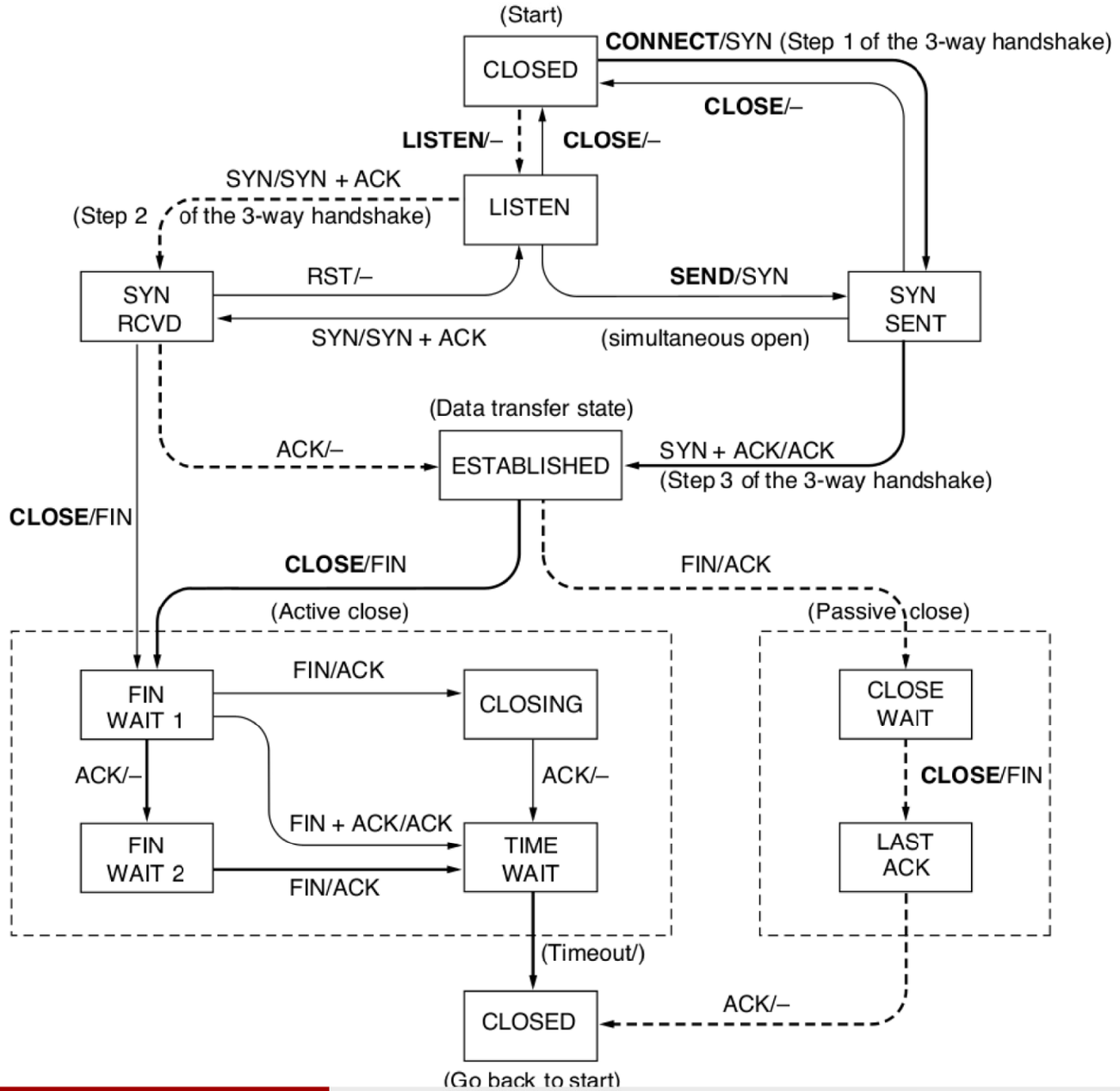
- SYN is used to establish connections: both connection request (SYN=1, ACK=0) and connection accepted (SYN=1, ACK=1)
- FIN is used to release a connection: it specifies that the sender has no more data to transmit (after closing, the process may continue to receive data indefinitely)
- Both SYN and FIN segments have sequence numbers so guaranteed to be processed in the correct order
- Flow control is handled using a variable-sized sliding window, where **window size** tells how many bytes may be sent starting at the byte acknowledged
- **Checksum** is the error detection mechanism to check the integrity of the data transmitted
- One of the widely used **options** is about specifying the MSS (Maximum Segment Size) each host is willing to accept

TCP connection establishment

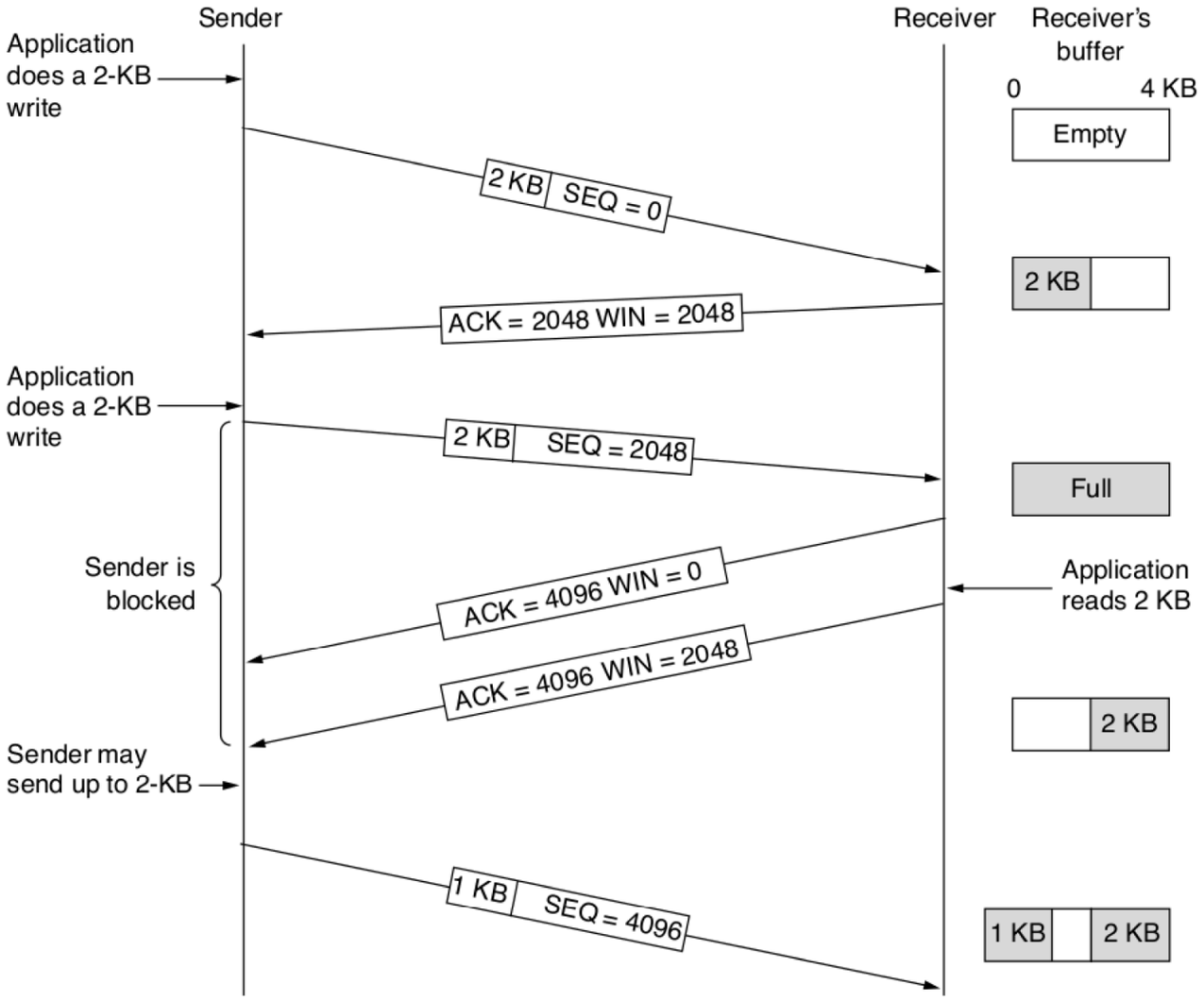


TCP connection management states

State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIME WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off


(Start)
CLOSED
CONNECT/SYN (Step 1 of the 3-way handshake)
CLOSE/–
LISTEN/–
CLOSE/–
SYN/SYN + ACK
(Step 2 of the 3-way handshake)
LISTEN
RST/–
SEND/SYN
SYN RCVD
SYN SENT
SYN/SYN + ACK
(simultaneous open)
(Data transfer state)
ACK/–
ESTABLISHED
SYN + ACK/ACK
(Step 3 of the 3-way handshake)
CLOSE/FIN
CLOSE/FIN
FIN/ACK
(Active close)
(Passive close)
FIN/ACK
FIN WAIT 1
CLOSING
CLOSE WAIT
ACK/–
ACK/–
CLOSE/FIN
FIN + ACK/ACK
FIN WAIT 2
TIME WAIT
LAST ACK
FIN/ACK
(Timeout/)
CLOSED
ACK/–
(Go back to start)

TCP sliding window management



TCP congestion control

- The network layer detects congestion when queues grow large at routers and tried to manage it
- It is up to the transport layer to receive congestion feedback from the network layer and slow down the rate of traffic that it is sending into the network
- In the Internet, TCP plays the main role in controlling congestion and ensuring reliable transport
- TCP maintains a **congestion window** whose size is the number of bytes the sender may have in the network at any time
    - **slow-start** is one of the algorithms used for congestion control: start using a small window, then gradually increase its size until packet loss is detected from a retransmission request (then decrease)

W6 Summary (1)

- The transport service is implemented by a transport protocol
- There are socket primitives that can be used to transfer data over a connection using TCP
- The three-way handshake used by TCP involves one peer checking with the other that the connection request is indeed current with a realiable way to release connections
- UDP is a connectionless protocol without flow or congestion control that is useful for many client-server situations (e.g., DNS, multimedia, broadcasting)

W6 Summary (2)

- The connection-oriented TCP service is obtained by both the sender and the receiver creating endpoints called sockets
- Sockets have socket addresses including the IP address of the host and a number local to the host called a port
  - common ports
- The TCP header includes source port and destination port, sequence number, acknowledgment number, TCP header length, eight 1-bit fields, window size, checksum, urgent pointer, options, and data
- Establishing a TCP connection involves multiple connection states and managing the TCP window for the receiver's buffer
- TCP plays the main role in controlling congestion and ensuring reliable transport using a congestion window and algorithms like slow-start