Internet Protocol Stack

- **Application**: supporting network applications
  - FTP, SMTP, HTTP
- **Transport**: host-host data transfer
  - TCP, UDP
- **Network**: routing of datagrams from source to destination
  - IP, routing protocols
- **Link**: data transfer between neighboring network elements
  - WiFi, Ethernet
- **Physical**: bits “on the wire”
  - Radios, coaxial cable, optical fibers
Transport Layer
Roadmap

- Overview transport layer
- Wireless TCP to address the challenges
  - Unreliable links
  - Node mobility
Transport services and protocols

- provide *logical communication* between app processes running on different hosts
- transport protocols run in end systems
  - send side: breaks app messages into *segments*, passes to network layer
  - rcv side: reassembles segments into messages, passes to app layer
- more than one transport protocol available to apps
  - Internet: TCP and UDP
Transport vs. network layer

- **network layer**: logical communication between hosts
- **transport layer**: logical communication between processes
  - relies on and enhances network layer services

**Household analogy:**
12 kids sending letters to 12 kids
- processes = kids
- app messages = letters in envelopes
- hosts = houses
- transport protocol = Ann and Bill
- network-layer protocol = postal service
Internet transport-layer protocols

- unreliable, unordered delivery: UDP
  - no-frills extension of “best-effort” IP
- reliable, in-order delivery (TCP)
  - congestion control
  - flow control
  - connection setup
- services not available:
  - delay guarantees
  - bandwidth guarantees
Multiplexing/demultiplexing

Demultiplexing at rcv host:
delivering received segments to correct socket

Multiplexing at send host:
gathering data from multiple sockets, enveloping data with header (later used for demultiplexing)

= socket  = process

<table>
<thead>
<tr>
<th>application</th>
<th>P3</th>
<th>transport</th>
<th>network</th>
<th>link</th>
<th>physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>host 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P1</th>
<th>application</th>
<th>P2</th>
<th>transport</th>
<th>network</th>
<th>link</th>
<th>physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>host 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P4</th>
<th>application</th>
<th>transport</th>
<th>network</th>
<th>link</th>
<th>physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>host 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How demultiplexing works

- host receives IP datagrams
  - each datagram has source IP address, destination IP address
  - each datagram carries 1 transport-layer segment
  - each segment has source, destination port number

- host uses IP addresses & port numbers to direct segment to appropriate socket

TCP/UDP segment format

<table>
<thead>
<tr>
<th>source port #</th>
<th>dest port #</th>
</tr>
</thead>
<tbody>
<tr>
<td>other header fields</td>
<td></td>
</tr>
</tbody>
</table>

application data (message)
Connectionless demultiplexing

- Create sockets with port numbers:
  
  ```java
  DatagramSocket mySocket1 = new DatagramSocket(12534);
  DatagramSocket mySocket2 = new DatagramSocket(12535);
  ```

- UDP socket identified by two-tuple:

  ```java
  (dest IP address, dest port number)
  ```

- When host receives UDP segment:
  
  - checks destination port number in segment
  - directs UDP segment to socket with that port number

- IP datagrams with different source IP addresses and/or source port numbers directed to same socket
Connectionless demux (cont)

DatagramSocket serverSocket = new DatagramSocket(6428);

SP provides “return address”
Connection-oriented demux

- TCP socket identified by 4-tuple:
  - source IP address
  - source port number
  - dest IP address
  - dest port number
- Receiving host uses all four values to direct segment to appropriate socket
- Server host may support many simultaneous TCP sockets:
  - each socket identified by its own 4-tuple
- Web servers have different sockets for each connecting client
  - non-persistent HTTP will have different socket for each request
Connection-oriented demux (cont)

Client IP: A

P1

SP: 9157
DP: 80
S-IP: A
D-IP: C

P2

SP: 9157
DP: 80
S-IP: B
D-IP: C

Server IP: C

P4

P5

P6

SP: 5775
DP: 80
S-IP: B
D-IP: C

Client IP: B
Connection-oriented demux: Threaded Web Server
Client side

- Create a socket with the socket() system call
- Connect the socket to the address of the server using the connect() system call
- Send and receive data. There are a number of ways to do this, but the simplest is to use the read() and write() system calls.
Server side

- Create a socket with the socket() system call
- Bind the socket to an address using the bind() system call. For a server socket on the Internet, an address consists of a port number on the host machine.
- Listen for connections with the listen() system call
- Accept a connection with the accept() system call. This call typically blocks until a client connects with the server.
- Send and receive data
UDP: User Datagram Protocol [RFC 768]

- “no frills,” “bare bones” Internet transport protocol
- “best effort” service, UDP segments may be:
  - lost
  - delivered out of order to app
- connectionless:
  - no handshaking between UDP sender, receiver
  - each UDP segment handled independently of others

Why is there a UDP?
UDP: User Datagram Protocol [RFC 768]

- "no frills," "bare bones" Internet transport protocol
- "best effort" service, UDP segments may be:
  - lost
  - delivered out of order to app
- connectionless:
  - no handshaking between UDP sender, receiver
  - each UDP segment handled independently of others

Why is there a UDP?
- no connection establishment (which can add delay)
- simple: no connection state at sender, receiver
- small segment header
- no congestion control: UDP can blast away as fast as desired
UDP: more

- often used for streaming multimedia apps
  - loss tolerant
  - rate sensitive
- other UDP uses
  - DNS
  - SNMP
- reliable transfer over UDP:
  add reliability at application layer
  - application-specific error recovery!

UDP segment format:

<table>
<thead>
<tr>
<th>source port #</th>
<th>dest port #</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>checksum</td>
</tr>
</tbody>
</table>

Application data (message)
UDP checksum

Goal: detect “errors” (e.g., flipped bits) in transmitted segment

Sender:
- treat segment content as sequence of 16-bit integers
- checksum: addition (1’s complement sum) of segment contents
- sender puts checksum value into UDP checksum field

Receiver:
- compute checksum of received segment
- check if computed checksum equals checksum field value:
  - NO - error detected
  - YES - no error detected. *But maybe errors nonetheless? More later* ...

Internet Checksum Example

- **Note**
  - When adding numbers, a carryout from the most significant bit needs to be added to the result

- **Example: add two 16-bit integers**
  - Take one’s complement
  - Add them
  - Take one’s complement
Internet Checksum Example (Cont.)

- **Note**
  - When adding numbers, a carryout from the most significant bit needs to be added to the result.

- **Example: add two 16-bit integers**

  \[
  \begin{array}{cccccccccccccccc}
  1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
  1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
  \hline
  1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1
  \end{array}
  \]

  - **wraparound**
    \[
    1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1
    \]

  - **sum**
    \[
    1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0
    \]

  - **checksum**
    \[
    0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1
    \]

  **Benefits:** easy to compute; can do incremental update; endian-independent.
Principles of Reliable data transfer

- important in app., transport, link layers
- top-10 list of important networking topics!

(a) provided service

- characteristics of unreliable channel will determine complexity of reliable data transfer protocol (rdt)
Principles of Reliable data transfer

- important in app., transport, link layers
- top-10 list of important networking topics!

- characteristics of unreliable channel will determine complexity of reliable data transfer protocol (rdt)
Reliable Data Transfer

Reliable data transfer over a reliable channel
☑ over a reliable channel
Reliable Data Transfer

Reliable data transfer over a reliable channel
☑ over a reliable channel
☑ over a channel with error
Reliable Data Transfer

Reliable data transfer over a reliable channel
☑ over a reliable channel
☑ over a channel with error
   ☑ Checksum + NACK or ACK
☑ over a channel with error and loss
Reliable Data Transfer

Reliable data transfer over a reliable channel
- over a reliable channel
- over a channel with error
  - Checksum + NACK or ACK
- over a channel with error and loss
  - Checksum + ACK + sequence no. + timeout
Reliable transfer in action

(a) operation with no loss

(b) lost packet
Reliable transfer in action

(c) lost ACK

(d) premature timeout
Any problem with the above protocol?
Performance

- It works, but performance stinks
- example: 1 Gbps link, 15 ms e-e prop. delay, 1KB packet:
Performance

- It works, but performance stinks
- example: 1 Gbps link, 15 ms e-e prop. delay, 1KB packet:

\[ T_{\text{transmit}} = \frac{L \text{ (packet length in bits)}}{R \text{ (transmission rate, bps)}} = \frac{8\text{kb/pkt}}{10^9 \text{ b/sec}} = 8 \text{ microsec} \]

- \( U_{\text{sender}} \): utilization - fraction of time sender busy sending

\[ U_{\text{sender}} = \frac{L / R}{\text{RTT} + L / R} = \frac{.008}{30.008} = 0.00027 \]

- 1KB pkt every 30 msec \( \rightarrow \) 33kB/sec thruput over 1 Gbps link
- network protocol limits use of physical resources!
Stop-and-wait operation

- First packet bit transmitted, $t = 0$
- Last packet bit transmitted, $t = \frac{L}{R}$
- First packet bit arrives
- Last packet bit arrives, send ACK
- ACK arrives, send next packet, $t = RTT + \frac{L}{R}$

\[ U_{\text{sender}} = \frac{L}{R} \frac{RTT + L}{R} = \frac{.008}{30.008} = 0.00027 \]
How to fix the problem?
Pipelined protocols

Pipelining: sender allows multiple, “in-flight”, yet-to-be-acknowledged pkts

- range of sequence numbers must be increased
- buffering at sender and/or receiver

Two generic forms of pipelined protocols: go-Back-N, selective repeat
Pipelining: increased utilization

\[ U_{\text{sender}} = \frac{3 \times L / R}{\text{RTT} + L / R} = \frac{.024}{30.008} = 0.0008 \]

Increase utilization by a factor of 3!
Go-Back-N

Sender:
- k-bit seq # in pkt header
- “window” of up to N, consecutive unack’ed pkts allowed

ACK(n): ACKs all pkts up to, including seq # n - “cumulative ACK”
  - may receive duplicate ACKs (see receiver)
- timer for each in-flight pkt
- timeout(n): retransmit pkt n and all higher seq # pkts in window
GBN in action

sender
send pkt0
send pkt1
send pkt2
send pkt3 (wait)
rcv ACK0
send pkt4
rcv ACK1
send pkt5
pkt2 timeout
send pkt2
send pkt3
send pkt4
send pkt5

receiver
rcv pkt0
send ACK0
rcv pkt1
send ACK1
rcv pkt3, discard
send ACK1
rcv pkt4, discard
send ACK1
rcv pkt5, discard
send ACK1
rcv pkt2, deliver
send ACK2
rcv pkt3, deliver
send ACK3
What is the drawback of GBN?
How to eliminate that?
Selective Repeat

- receiver *individually* acknowledges all correctly received pkts
  - buffers pkts, as needed, for eventual in-order delivery to upper layer
- sender only resends pkts for which ACK not received
  - sender timer for each unACKed pkt
- sender window
  - N consecutive seq #'s
  - again limits seq #s of sent, unACKed pkts
Selective repeat: sender, receiver windows

(a) sender view of sequence numbers

(b) receiver view of sequence numbers
Selective repeat

**Sender**

- Data from above:
  - If next available seq # in window, send pkt
- **Timeout(n):**
  - Resend pkt n, restart timer
- **ACK(n) in [sendbase, sendbase+N]:**
  - Mark pkt n as received
  - If n is smallest unACKed pkt, advance window base to next unACKed seq #

**Receiver**

- **Packet n in [rcvbase, rcvbase+N-1]:**
  - Send ACK(n)
  - Out-of-order: buffer
  - In-order: deliver (also deliver buffered, in-order pkts), advance window to next not-yet-received pkt
- **Packet n in [rcvbase-N, rcvbase-1]:**
  - ACK(n)
- Otherwise:
  - Ignore
Selective repeat in action
# Reliable Data Transfer Mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum</td>
<td>Detect bit errors</td>
</tr>
<tr>
<td>Timer</td>
<td>Detect packet loss at sender</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Detect packet loss and duplicates at receiver</td>
</tr>
<tr>
<td>ACK</td>
<td>Inform sender that pkt has been received</td>
</tr>
<tr>
<td>NACK</td>
<td>Inform sender that pkt has not been received correctly</td>
</tr>
<tr>
<td>Window, pipelining</td>
<td>Increase throughput, and adapt to receiver buffer size and network congestion</td>
</tr>
</tbody>
</table>
TCP: Overview

- **point-to-point:**
  - one sender, one receiver

- **reliable, in-order byte steam:**
  - no “message boundaries”

- **pipelined:**
  - TCP congestion and flow control set window size

- **send & receive buffers**

- **full duplex data:**
  - bi-directional data flow in same connection
  - MSS: maximum segment size

- **connection-oriented:**
  - handshaking (exchange of control msgs) init’s sender, receiver state before data exchange

- **flow controlled:**
  - sender will not overwhelm receiver

RFCs: 793, 1122, 1323, 2018, 2581
# TCP segment structure

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source port #</td>
<td>Source port number</td>
</tr>
<tr>
<td>dest port #</td>
<td>Destination port number</td>
</tr>
<tr>
<td>sequence number</td>
<td>Sequence number</td>
</tr>
<tr>
<td>acknowledgement number</td>
<td>Acknowledgement number</td>
</tr>
<tr>
<td>head len</td>
<td>Length of TCP header</td>
</tr>
<tr>
<td>not used</td>
<td>Not used</td>
</tr>
<tr>
<td>UAP</td>
<td>Urgent data available pointer</td>
</tr>
<tr>
<td>RSF</td>
<td>Reserve flag</td>
</tr>
<tr>
<td>Receive window</td>
<td>Receive window</td>
</tr>
<tr>
<td>checksum</td>
<td>Checksum</td>
</tr>
<tr>
<td>Urg data pnter</td>
<td>Urgent data pointer</td>
</tr>
<tr>
<td>Options</td>
<td>Variable length options</td>
</tr>
<tr>
<td>application data</td>
<td>Application data (variable length)</td>
</tr>
</tbody>
</table>

**Internet checksum (as in UDP)**

**URG: urgent data (generally not used)**

**ACK: ACK # valid**

**PSH: push data now (generally not used)**

**RST, SYN, FIN: connection estab (setup, teardown commands)**

**counting by bytes of data (not segments!)**

**# bytes rcvr willing to accept**

**32 bits**
TCP Connection Management

Recall: TCP sender, receiver establish “connection” before exchanging data segments

- initialize TCP variables:
  - seq. #s
  - buffers, flow control info (e.g. RcvWindow)

- client: connection initiator
  ```java
  Socket clientSocket = new Socket("hostname","port number");
  ```

- server: contacted by client
  ```java
  Socket connectionSocket = welcomeSocket.accept();
  ```

Three way handshake:

- **Step 1**: client host sends TCP SYN segment to server
  - specifies initial seq #
  - no data

- **Step 2**: server host receives SYN, replies with SYNACK segment
  - server allocates buffers
  - specifies server initial seq. #

- **Step 3**: client receives SYNACK, replies with ACK segment, which may contain data
TCP Connection Management (cont.)

Closing a connection:

client closes socket:
   clientSocket.close();

Step 1: client end system
         sends TCP FIN control
         segment to server

Step 2: server receives
        FIN, replies with ACK.
        Closes connection, sends
        FIN.
TCP Connection Management (cont.)

**Step 3:** client receives FIN, replies with ACK.

- Enters “timed wait” - will respond with ACK to received FINs

**Step 4:** server, receives ACK. Connection closed.

**Note:** with small modification, can handle simultaneous FINs.
# TCP: Reliable Data Transfer Mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum</td>
<td>Detect bit errors</td>
</tr>
<tr>
<td>Timer</td>
<td>Detect packet loss at sender</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Detect packet loss and duplicates at receiver</td>
</tr>
<tr>
<td>ACK</td>
<td>Inform sender that pkt has been received</td>
</tr>
<tr>
<td>Window, pipelining</td>
<td>Increase throughput, and adapt to receiver buffer size and network congestion</td>
</tr>
</tbody>
</table>
**TCP seq. #'s and ACKs**

**Seq. #'s:**
- byte stream “number” of first byte in segment’s data

**ACKs:**
- seq # of next byte expected from other side
- cumulative ACK

Q: how receiver handles out-of-order segments
- A: TCP spec doesn’t say, - up to implementor

---

**Simple Telnet Scenario**

- User types 'C'
- Host A sends `Seq=42, ACK=79, data = 'C'`
- Host B receives `Seq=42, ACK=79, data = 'C'`
- Host B sends `Seq=79, ACK=43, data = 'C'`
- Host A receives `Seq=79, ACK=43, data = 'C'`
- Host A sends `Seq=43, ACK=80`
- Host B receives `Seq=43, ACK=80`
TCP Timeout

Q: how to set TCP timeout value?
TCP Round Trip Time and Timeout

Q: how to set TCP timeout value?
- longer than RTT
  - but RTT varies
- too short: premature timeout
  - unnecessary retransmissions
- too long: slow reaction to segment loss

Q: how to estimate RTT?
TCP Round Trip Time and Timeout

**Q:** how to set TCP timeout value?
- longer than RTT  
  - but RTT varies
- too short: premature timeout  
  - unnecessary retransmissions
- too long: slow reaction to segment loss

**Q:** how to estimate RTT?
- **SampleRTT:** measured time from segment transmission until ACK receipt  
  - ignore retransmissions
  - Why?
- **SampleRTT** will vary, want estimated RTT “smoother”  
  - average several recent measurements, not just current **SampleRTT**
TCP Round Trip Time and Timeout

EstimatedRTT = (1 - \(\alpha\)) \times \text{EstimatedRTT} + \alpha \times \text{SampleRTT}

- Exponential weighted moving average
- Influence of past sample decreases exponentially fast
- Typical value: \(\alpha = 0.125\)
Example RTT estimation:

RTT: gaia.cs.umass.edu to fantasia.eurecom.fr

![RTT graph]
TCP Round Trip Time and Timeout

Setting the timeout

- EstimatedRTT plus “safety margin”
  - large variation in EstimatedRTT -> larger safety margin
- first estimate of how much SampleRTT deviates from EstimatedRTT:

  \[
  \text{DevRTT} = (1-\beta) \times \text{DevRTT} + \\
  \beta \times |\text{SampleRTT} - \text{EstimatedRTT}|
  \]

(typically, \( \beta = 0.25 \))

Then set timeout interval:

\[
\text{TimeoutInterval} = \text{EstimatedRTT} + 4 \times \text{DevRTT}
\]
TCP sender events:

**data rcvd from app:**
- Create segment with seq #
- seq # is byte-stream number of first data byte in segment
- start timer if not already running (think of timer as for oldest unacked segment)
- expiration interval: TimeOutInterval

**timeout:**
- retransmit segment that caused timeout
- restart timer

**Ack rcvd:**
- If acknowledges previously unacked segments
  - update what is known to be acked
  - start timer if there are outstanding segments
TCP sender (simplified)

NextSeqNum = InitialSeqNum
SendBase = InitialSeqNum

loop (forever) {
    switch(event)

    event: data received from application above
        create TCP segment with sequence number NextSeqNum
        if (timer currently not running)
            start timer
        pass segment to IP
        NextSeqNum = NextSeqNum + length(data)

    event: timer timeout
        retransmit not-yet-acknowledged segment with
        smallest sequence number
        start timer

    event: ACK received, with ACK field value of y
        if (y > SendBase) {
            SendBase = y
            if (there are currently not-yet-acknowledged segments)
                start timer
        }

} /* end of loop forever */

Comment:
• SendBase-1: last cumulatively ack'ed byte
Example:
• SendBase-1 = 71; y= 73, so the rcvr wants 73+ ;
  y > SendBase, so that new data is acked
TCP: retransmission scenarios

TCP retransmission scenarios include:

1. Premature timeout:
   - Host A sends a segment with Seq=92.
   - Host B times out without receiving an ACK.
   - Host A resends the segment.

2. Lost ACK scenario:
   - Host A sends a segment with Seq=92, 8 bytes data.
   - Host B receives the segment but loses the ACK.
   - Host A retransmits the segment.

3. Sendbase update:
   - Host A sends a segment with Seq=92, 8 bytes data.
   - Host B sends an ACK with Seq=100, ACK=100.
   - Host A updates its SendBase to 100.
   - Host A retransmits the segment.

4. Premature timeout:
   - Host A sends a segment with Seq=92, 8 bytes data.
   - Host B times out without receiving an ACK.
   - Host A resends the segment.

Diagram illustrate the sequence of events for each scenario.
TCP retransmission scenarios (more)

Host A

SendBase = 120

Timeout

Host B

Cumulative ACK scenario

Seq=92, 8 bytes data

ACK=100

Seq=100, 20 bytes data

ACK=120

loss

X
Sending ACKs is an overhead. How to reduce the overhead?
### TCP ACK generation [RFC 1122, RFC 2581]

<table>
<thead>
<tr>
<th>Event at Receiver</th>
<th>TCP Receiver action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arrival of in-order segment with expected seq #. All data up to expected seq # already ACKed</td>
<td>Delayed ACK. Wait up to 500ms for next segment. If no next segment, send ACK</td>
</tr>
<tr>
<td>Arrival of in-order segment with expected seq #. One other segment has ACK pending</td>
<td>Immediately send single cumulative ACK, ACKing both in-order segments</td>
</tr>
<tr>
<td>Arrival of out-of-order segment higher-than-expect seq. #. Gap detected</td>
<td>Immediately send <em>duplicate ACK</em>, indicating seq. # of next expected byte</td>
</tr>
<tr>
<td>Arrival of segment that partially or completely fills gap</td>
<td>Immediately send ACK, provided that segment starts at lower end of gap</td>
</tr>
</tbody>
</table>
Retransmission upon timeout incurs significant delay. Can we retransmit sooner?
Fast Retransmit

- time-out period often relatively long:
  - long delay before resending lost packet
- detect lost segments via duplicate ACKs.
  - sender often sends many segments back-to-back
  - if segment is lost, there will likely be many duplicate ACKs for that segment
- If sender receives 3 ACKs for same data, it assumes that segment after ACKed data was lost:
  - fast retransmit: resend segment before timer expires
  - Why 3 dup acks?
Transport Layer

Host A

seq # x1
seq # x2
seq # x3
seq # x4
seq # x5

timeout

time

Host B

ACK x1
ACK x1
ACK x1
ACK x1

triple
duplicate
ACKs

resend seq X2

ACK x1

duplicate ACKs
Fast retransmit algorithm:

event: ACK received, with ACK field value of y
   if (y > SendBase) {
      SendBase = y
      if (there are currently not-yet-acknowledged segments)
         start timer
   }
   else {
      increment count of dup ACKs received for y
      if (count of dup ACKs received for y = 3) {
         resend segment with sequence number y
      }
   }

a duplicate ACK for already ACKed segment

fast retransmit
TCP Flow Control

- Receive side of TCP connection has a receive buffer:

  - RcvWindow
  - RcvBuffer
  - TCP data in buffer
  - Application process

- App process may be slow at reading from buffer

- Flow control:
  - Sender won't overflow receiver's buffer by transmitting too much, too fast
  - Speed-matching service: matching the sending rate to the receiving app's drain rate
  - Rcvr advertises spare room by including value of RcvWindow in segments
  - Sender limits unACKed data to RcvWindow
    - Guarantees receive buffer doesn't overflow
Principles of Congestion Control

Congestion:

- informally: “too many sources sending too much data too fast for network to handle”
- different from flow control
- manifestations:
  - lost packets (buffer overflow at routers)
  - long delays (queueing in router buffers)
- a top-10 problem!
Causes/costs of congestion: scenario 1

- two senders, two receivers
- one router, infinite buffers
- no retransmission

- large delays when congested
- maximum achievable throughput
Causes/costs of congestion: scenario 2

- one router, finite buffers
- sender retransmission of lost packet

\[ \lambda_{in} : \text{original data} \]
\[ \lambda'_{in} : \text{original data, plus retransmitted data} \]
Causes/costs of congestion: scenario 2

- always: $\lambda_{in} = \lambda_{out}$ (goodput)
- "perfect" retransmission only when loss: $\lambda'_{in} > \lambda_{out}$
- retransmission of delayed (not lost) packet makes $\lambda_{in}$ larger (than perfect case) for same $\lambda_{out}$

"costs" of congestion:
- more work (retrans) for given "goodput"
- unneeded retransmissions: link carries multiple copies of pkt
Causes/costs of congestion: scenario 3

- four senders
- multihop paths
- timeout/retransmit

Q: what happens as $\lambda_{in}$ and $\lambda'_{in}$ increase?
Causes/costs of congestion: scenario 3

another “cost” of congestion:

- when packet dropped, any “upstream transmission capacity used for that packet was wasted!
How to avoid network congestion?
Approaches towards congestion control

Two broad approaches towards congestion control:

**End-end congestion control:**
- no explicit feedback from network
- congestion inferred from end-system observed loss, delay
- approach taken by TCP

**Network-assisted congestion control:**
- routers provide feedback to end systems
  - single bit indicating congestion (SNA, DECbit, TCP/IP ECN, ATM)
  - explicit rate sender should send at (XCP)
TCP congestion control:

- **goal:** TCP sender should transmit as fast as possible, but without congesting network
  - **Q:** how to find rate just below congestion level
- decentralized: each TCP sender sets its own rate, based on *implicit* feedback:
  - **ACK:** segment received (a good thing!), network not congested, so increase sending rate
  - **lost segment:** assume loss due to congested network, so decrease sending rate
TCP congestion control: bandwidth probing

- “probing for bandwidth”: increase transmission rate on receipt of ACK, until eventually loss occurs, then decrease transmission rate
  - continue to increase on ACK, decrease on loss (since available bandwidth is changing, depending on other connections in network)

Q: how fast to increase/decrease?
  - details to follow

TCP’s “sawtooth” behavior
TCP Congestion Control: details

- sender limits rate by limiting number of unACKed bytes “in pipeline”:
  \[ \text{LastByteSent} - \text{LastByteAcked} \leq \text{cwnd} \]
  - cwnd: differs from rwnd (how, why?)
  - sender limited by \( \min(cwnd, rwnd) \)

- roughly,
  \[ \text{rate} = \frac{\text{cwnd}}{\text{RTT}} \text{ bytes/sec} \]

- cwnd is dynamic, function of perceived network congestion
TCP Congestion Control: more details

**segment loss event:** reducing cwnd
- timeout: no response from receiver
  - cut cwnd to 1
- 3 duplicate ACKs: at least some segments getting through (recall fast retransmit)
  - cut cwnd in half, less aggressively than on timeout

**ACK received:** increase cwnd
- Slow start phase:
  - increase exponentially fast (despite name) at connection start, or following timeout
- congestion avoidance:
  - increase linearly
TCP Slow Start

- when connection begins, \( cwnd = 1 \) MSS
  - example: MSS = 500 bytes & RTT = 200 msec
  - initial rate = 20 kbps
- available bandwidth may be >> MSS/RTT
  - desirable to quickly ramp up to respectable rate
- increase rate exponentially until first loss event or when threshold reached
  - double \( cwnd \) every RTT
  - done by incrementing \( cwnd \) by 1 for every ACK received
TCP: congestion avoidance

- when $cwnd > ssthresh$
  - grow $cwnd$ linearly
  - increase $cwnd$ by 1 MSS per RTT
  - approach possible congestion slower than in slowstart
  - implementation: $cwnd = cwnd + \frac{MSS}{cwnd}$ for each ACK received

AIMD

- **ACKs**: increase $cwnd$ by 1 MSS per RTT: additive increase
- **loss**: cut $cwnd$ in half (non-timeout-detected loss): multiplicative decrease

AIMD: Additive Increase Multiplicative Decrease
Popular “flavors” of TCP

![Graph showing TCP Tahoe and TCP Reno](image)
Summary: TCP Congestion Control

- When \texttt{CongWin} is below \texttt{Threshold}, sender is in slow-start phase, window grows exponentially.

- When \texttt{CongWin} is above \texttt{Threshold}, sender is in congestion-avoidance phase, window grows linearly.

- When a triple duplicate ACK occurs, \texttt{Threshold} set to \texttt{CongWin}/2 and \texttt{CongWin} set to \texttt{Threshold}.

- When timeout occurs, \texttt{Threshold} set to \texttt{CongWin}/2 and \texttt{CongWin} is set to 1 MSS.