Chapter 3
Transport Layer

A note on the use of these Powerpoint slides:
We’re making these slides freely available to all (faculty, students, readers). They’re in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a lot of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we’d like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2016
© J.F Kurose and K.W. Ross, All Rights Reserved
Chapter 3 outline

3.1 transport-layer services
3.2 multiplexing and demultiplexing
3.3 connectionless transport: UDP
3.4 principles of reliable data transfer
3.5 connection-oriented transport: TCP
  • segment structure
  • reliable data transfer
  • flow control
  • connection management
3.6 principles of congestion control
3.7 TCP congestion control
TCP: Overview  RFCs: 793, 1122, 1323, 2018, 2581

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

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

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

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

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

- **flow controlled:**
  - sender will not overwhelm receiver
TCP segment structure

- **Source port #**
- **Destination port #**
- **Sequence number**
- **Acknowledgement number**
- **Receive window**
- **Checksum**
- **Urg data pointer**
- **Options (variable length)**
- **Application data (variable length)**

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

**ACK**: ACK # valid

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

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

**Internet checksum** (as in UDP)

- Counting by bytes of data (not segments!)
- "# bytes rcvr willing to accept"
TCP seq. numbers, ACKs

sequence numbers:
- byte stream “number” of first byte in segment’s data

acknowledgements:
- 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
TCP seq. numbers, ACKs

Host A

User types ‘C’

seq=42, ACK=79, data = ‘C’

host ACKs receipt of echoed ‘C’

seq=79, ACK=43, data = ‘C’

Host B

host ACKs receipt of ‘C’, echoes back ‘C’

seq=43, ACK=80

simple telnet scenario
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?
- \textit{SampleRTT}: measured time from segment transmission until ACK receipt
  - ignore retransmissions
- \textit{SampleRTT} will vary, want estimated RTT “smoother”
  - average several recent measurements, not just current \textit{SampleRTT}
TCP round trip time, timeout

EstimatedRTT = (1− α)*EstimatedRTT + α*SampleRTT

- exponential weighted moving average
- influence of past sample decreases exponentially fast
- typical value: $\alpha = 0.125$

![Graph showing RTT](image-url)
TCP round trip time, timeout

- **timeout interval**: EstimatedRTT plus “safety margin”
  - large variation in EstimatedRTT → larger safety margin
- estimate SampleRTT deviation from EstimatedRTT:
  \[
  \text{DevRTT} = (1-\beta) \ast \text{DevRTT} + \\
  \beta \ast |\text{SampleRTT} - \text{EstimatedRTT}|
  \]

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

\[
\text{TimeoutInterval} = \text{EstimatedRTT} + 4 \ast \text{DevRTT}
\]

* Check out the online interactive exercises for more examples: [http://gaia.cs.umass.edu/kurose_ross/interactive/](http://gaia.cs.umass.edu/kurose_ross/interactive/)
Chapter 3 outline

3.1 transport-layer services
3.2 multiplexing and demultiplexing
3.3 connectionless transport: UDP
3.4 principles of reliable data transfer

3.5 connection-oriented transport: TCP
- segment structure
- reliable data transfer
- flow control
- connection management

3.6 principles of congestion control
3.7 TCP congestion control
TCP reliable data transfer

- TCP creates rdt service on top of IP’s unreliable service
  - pipelined segments
  - cumulative acks
  - single retransmission timer

- retransmissions triggered by:
  - timeout events
  - duplicate acks

Let’s initially consider simplified TCP sender:
- ignore duplicate acks
- ignore flow control, congestion control
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 ack acknowledges previously unacked segments
  - update what is known to be ACKed
  - start timer if there are still unacked segments
TCP sender (simplified)

Transport

Layer 3

TCP sender (simplified)

data received from application above
create segment, seq. #: NextSeqNum
pass segment to IP (i.e., “send”)
NextSeqNum = NextSeqNum + length(data)
if (timer currently not running)
    start timer

NextSeqNum = InitialSeqNum
SendBase = InitialSeqNum

wait for event

timeout
retransmit not-yet-acked segment
    with smallest seq. #
    start timer

ACK received, with ACK field value y

if (y > SendBase) {
    SendBase = y
    /* SendBase–1: last cumulatively ACKed byte */
    if (there are currently not-yet-acked segments)
        start timer
    else stop timer
}

TCP: retransmission scenarios

lost ACK scenario

Host A
Seq=92, 8 bytes of data
ACK=100

Host B
Seq=92, 8 bytes of data

timeout
X

premature timeout

SendBase=92

Host A
Seq=92, 8 bytes of data
ACK=100

Host B
Seq=100, 20 bytes of data
ACK=100
ACK=120

SendBase=120
SendBase=100
SendBase=120
SendBase=92

SendBase=120

ACK=120

SendBase=120

ACK=120

SendBase=120

ACK=120

SendBase=120
TCP: retransmission scenarios

Host A

Seq=92, 8 bytes of data
Seq=100, 20 bytes of data

timeout

Host B

ACK=100

ACK=120

Seq=120, 15 bytes of data

cumulative ACK
## 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>immediate send ACK, provided that segment starts at lower end of gap</td>
</tr>
</tbody>
</table>
TCP 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.

*TCP fast retransmit*

if sender receives 3 ACKs for same data ("triple duplicate ACKs"), resend unacked segment with smallest seq #
- likely that unacked segment lost, so don’t wait for timeout
TCP fast retransmit

Host A
Seq=92, 8 bytes of data
Seq=100, 20 bytes of data
timeout
ACK=100
ACK=100
ACK=100
ACK=100
Seq=100, 20 bytes of data

Host B

fast retransmit after sender receipt of triple duplicate ACK
Chapter 3 outline

3.1 transport-layer services
3.2 multiplexing and demultiplexing
3.3 connectionless transport: UDP
3.4 principles of reliable data transfer

3.5 connection-oriented transport: TCP
   • segment structure
   • reliable data transfer
   • flow control
   • connection management

3.6 principles of congestion control
3.7 TCP congestion control
TCP flow control

receiver controls sender, so sender won’t overflow receiver’s buffer by transmitting too much, too fast

flow control
TCP flow control

- receiver “advertises” free buffer space by including `rwnd` value in TCP header of receiver-to-sender segments
  - `RcvBuffer` size set via socket options (typical default is 4096 bytes)
  - many operating systems autoadjust `RcvBuffer`
- sender limits amount of unacked (“in-flight”) data to receiver’s `rwnd` value
- guarantees receive buffer will not overflow

![Diagram of TCP flow control](image)
Chapter 3 outline

3.1 transport-layer services
3.2 multiplexing and demultiplexing
3.3 connectionless transport: UDP
3.4 principles of reliable data transfer

3.5 connection-oriented transport: TCP
- segment structure
- reliable data transfer
- flow control
- connection management

3.6 principles of congestion control
3.7 TCP congestion control
Connection Management

before exchanging data, sender/receiver “handshake”:

- agree to establish connection (each knowing the other willing to establish connection)
- agree on connection parameters

```
Socket clientSocket = newSocket("hostname","port number");
Socket connectionSocket = welcomeSocket.accept();
```
Agreeing to establish a connection

2-way handshake:

Q: will 2-way handshake always work in network?
- variable delays
- retransmitted messages (e.g. req_conn(x)) due to message loss
- message reordering
- can’t “see” other side
Agreeing to establish a connection

2-way handshake failure scenarios:

- **choose x**
- **req_conn(x)**
- **ESTAB**
- **acc_conn(x)**
- **req_conn(x)**
- **ESTAB**
- **data(x+1)**
- **accept data(x+1)**
- **ESTAB**
- **data(x+1)**
- **accept data(x+1)**

1. **half open connection! (no client!)**
2. **client terminates**
3. **server forgets x**
4. **connection x completes**

Transport Layer 3-25
TCP 3-way handshake

**client state**

1. **LISTEN**
   - Choose init seq num, x
   - Send TCP SYN msg

2. **SYNSENT**
   - Received SYNACK(x)
   - Indicates server is live
   - Send ACK for SYNACK
   - This segment may contain client-to-server data

3. **ESTAB**
   - SYN bit=1, Seq=x
   - SYN bit=1, Seq=y
   - ACK bit=1; ACK num=x+1
   - ACK bit=1, ACK num=y+1

**server state**

1. **LISTEN**
   - Choose init seq num, y
   - Send TCP SYNACK msg, acking SYN

2. **SYN RCVD**
   - SYN bit=1, Seq=y
   - ACK bit=1; ACK num=x+1

3. **ESTAB**
   - Received ACK(y)
   - Indicates client is live
TCP 3-way handshake: FSM

Socket connectionSocket =
welcomeSocket.accept();

SYN(x)
SYNACK(seq=y,ACKnum=x+1)
create new socket for communication back to client

ACK(ACKnum=y+1)

SYN rcvd

SYN sent

SYN(seq=x)

SYNACK(seq=y,ACKnum=x+1)

ACK(ACKnum=y+1)
TCP: closing a connection

- client, server each close their side of connection
  - send TCP segment with FIN bit = 1
- respond to received FIN with ACK
  - on receiving FIN, ACK can be combined with own FIN
- simultaneous FIN exchanges can be handled
TCP: closing a connection

**client state**

- **ESTAB**
  - `clientSocket.close()`

- **FIN_WAIT_1**
  - can no longer send but can receive data

- **FIN_WAIT_2**
  - wait for server close

- **TIMED_WAIT**
  - timed wait for 2*max segment lifetime

- **CLOSED**

**server state**

- **ESTAB**

- **CLOSE_WAIT**
  - can still send data

- **LAST_ACK**
  - can no longer send data

- **CLOSED**

- **FINbit=1, seq=x**
- **ACKbit=1; ACKnum=x+1**

- **FINbit=1, seq=y**
- **ACKbit=1; ACKnum=y+1**