The Transport Layer:
TCP and UDP

Jean-Yves Le Boudec

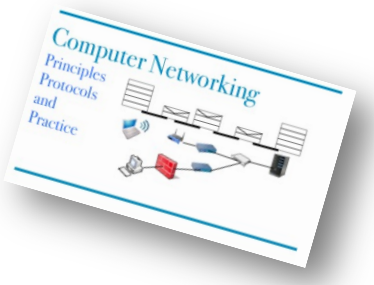
2022

Contents

1. The transport layer, UDP
2. TCP Basics: Sliding Window and Flow Control
3. TCP Connections and Sockets
4. More TCP Bells and Whistles
5. Secure Transport
6. Where should packet losses be repaired ?

Textbook

Chapter 4: The Transport Layer



1. The Transport Layer

Reminder:

network + link + phy carry packets end-to-end

transport layer makes network services available to programs

is in end-systems only, not in routers

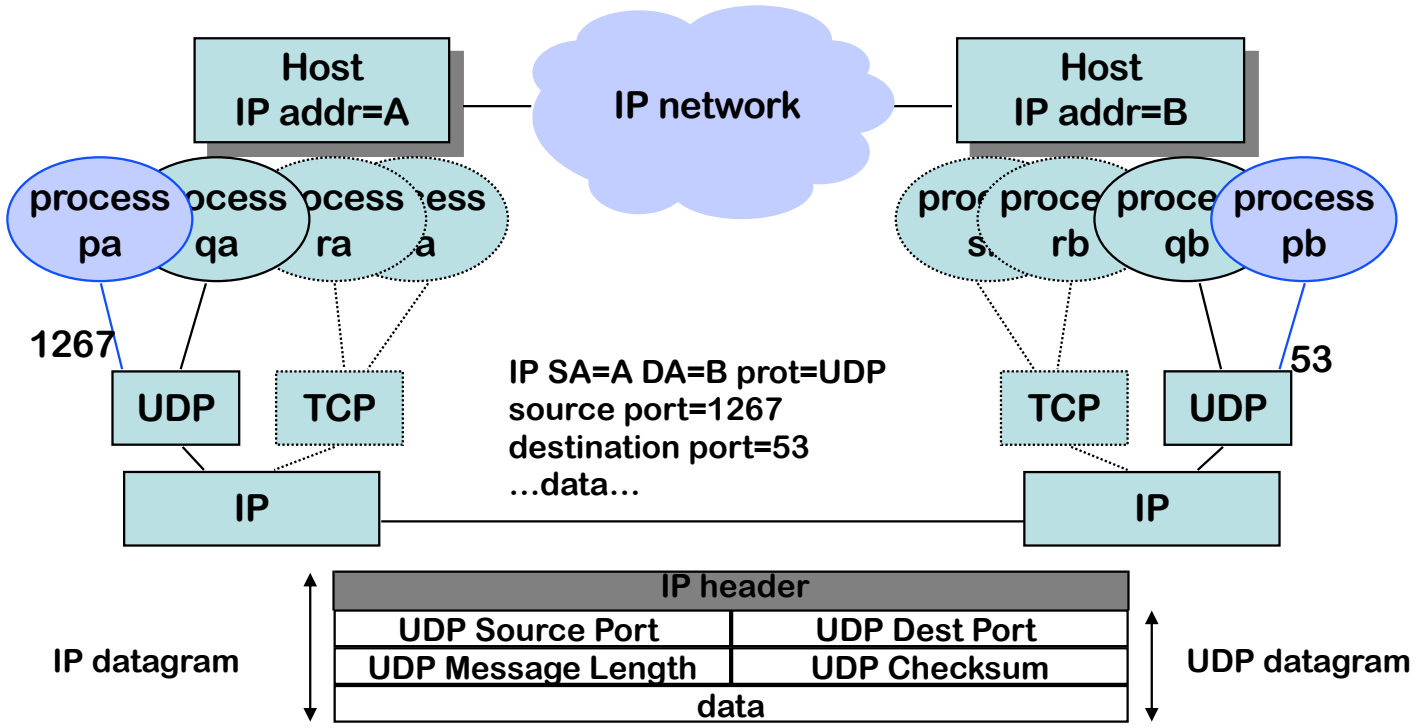
In TCP/IP there are mainly two transport layers

UDP (User Datagram Protocol):

TCP (Transmission Control Protocol): error recovery + flow control

There is no TCPv6 nor UDPv6, the same TCP and UDP are used over IPv4 and IPv6

UDP Uses Port Numbers



The picture shows two processes (= application programs) pa, and pb, are communicating. Each of them is associated locally with a port, as shown in the figure.

The example shows a packet sent by the name resolver process at host A, to the name server process at host B. The UDP header contains the source and destination ports. The destination port number is used to contact the name server process at B; the source port is not used directly; it will be used in the response from B to A.

The UDP header also contains a checksum the protect the UDP data plus the IP addresses and packet length. Checksum computation is not performed by all systems. Ports are 16 bits unsigned integers. They are defined statically or dynamically. Typically, a server uses a port number defined statically.

Standard services use well-known ports; for example, all DNS servers use port 53 (look at /etc/services). Ports that are allocated dynamically are called ephemeral. They are usually above 1024. If you write your own client server application on a multiprogramming machine, you need to define your own server port number and code it into your application.

What is the definition of a «server» ?

A. A machine that hosts resources used in the web
B. A computer with high CPU performance
C. A computer with large data storage
D. The role of a program that waits for requests to come
E. The role of a program that allows users to access large amounts of resources
F. None of the above
G. I don’t know

The UDP service is message oriented

UDP service interface

- one message, up to 65,535 bytes
- destination address, destination port, source address, source port
- destination address can be unicast or multicast

UDP service is message oriented

- UDP delivers exactly the message (called “Datagram”) or nothing
- consecutive messages may arrive in disorder
- message may be lost -- application must handle

If a UDP message is larger than the possible maximum size for the IP layer, MTU, then fragmentation occurs at the IP layer – this is not visible to the application program

UDP is used via a Socket Library

The socket library provides a programming interface to TCP and UDP

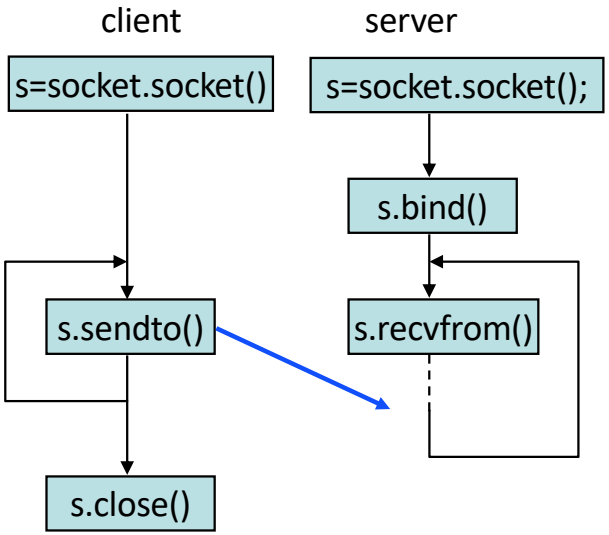
The figure shows toy client and server UDP programs. The client sends one string of chars to the server, which simply receives (and displays) it.

socket(socket.AF_INET,…) creates an IPv4 socket and returns a number (=file descriptor) if successful; socket(socket.AF_INET6,…) creates an IPv6 socket

bind() associates the local IP address and port number with the socket – can be skipped for a client socket. Port 0 means any available port
IP address can be 0 (0.0.0.0 or ::), it means all addresses of this host

sendto() gives the destination IP address, port number and the message to send

recvfrom() blocks until one message is received for this port number. It returns the source IP address and port number and the message.




```
% ./udpClient <destAddr> bonjour les amis
%
```

```
% ./udpServ &
%
```

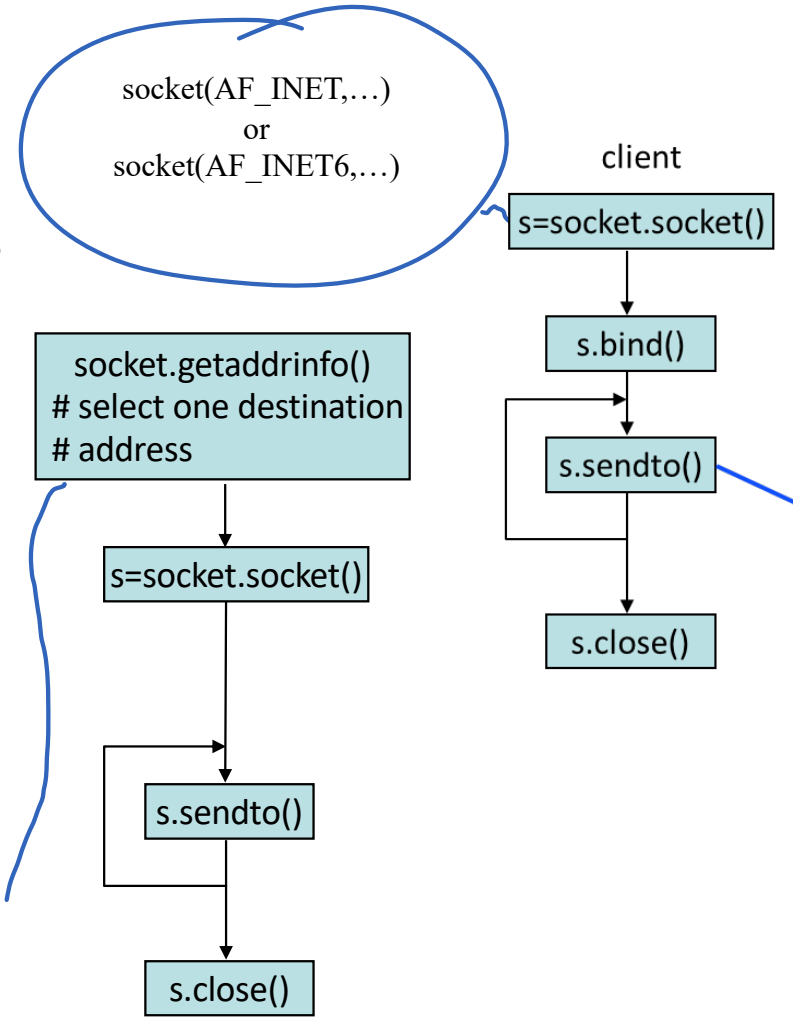
Is there a UDPv6 ?

There is no UDPv6 (nor TCPv6), UDP and TCP protocols are not affected by the choice of IPv4 or IPv6

However, there are UDPv4 sockets and UDPv6 sockets.
An application program has to choose IPv4 or IPv6, or, better, to support both.

This can be done using DNS (with eg. socket.getaddrinfo()) to know what is available.

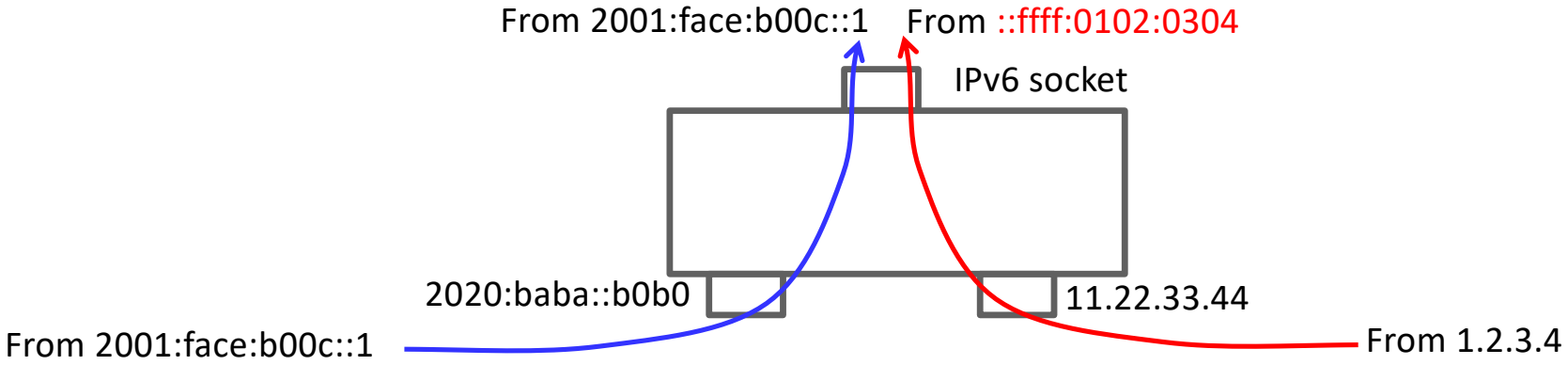
```
C:\Users\joe> python
>>> import socket
>>> socket.getaddrinfo("lca.epfl.ch",None)
[(<AddressFamily.AF_INET6: 23>, 0, 0, '',
('2001:620:618:521:1:80b3:2127:1', 0, 0, 0)),
(<AddressFamily.AF_INET: 2>, 0, 0, '', ('128.179.33.39',
0))]
```



An IPv6 socket can be dual-stack

On some dual-stack machine (= IPv4 and IPv6) an IPv6 socket can be bound to both IPv6 and IPv4 addresses of the local host.

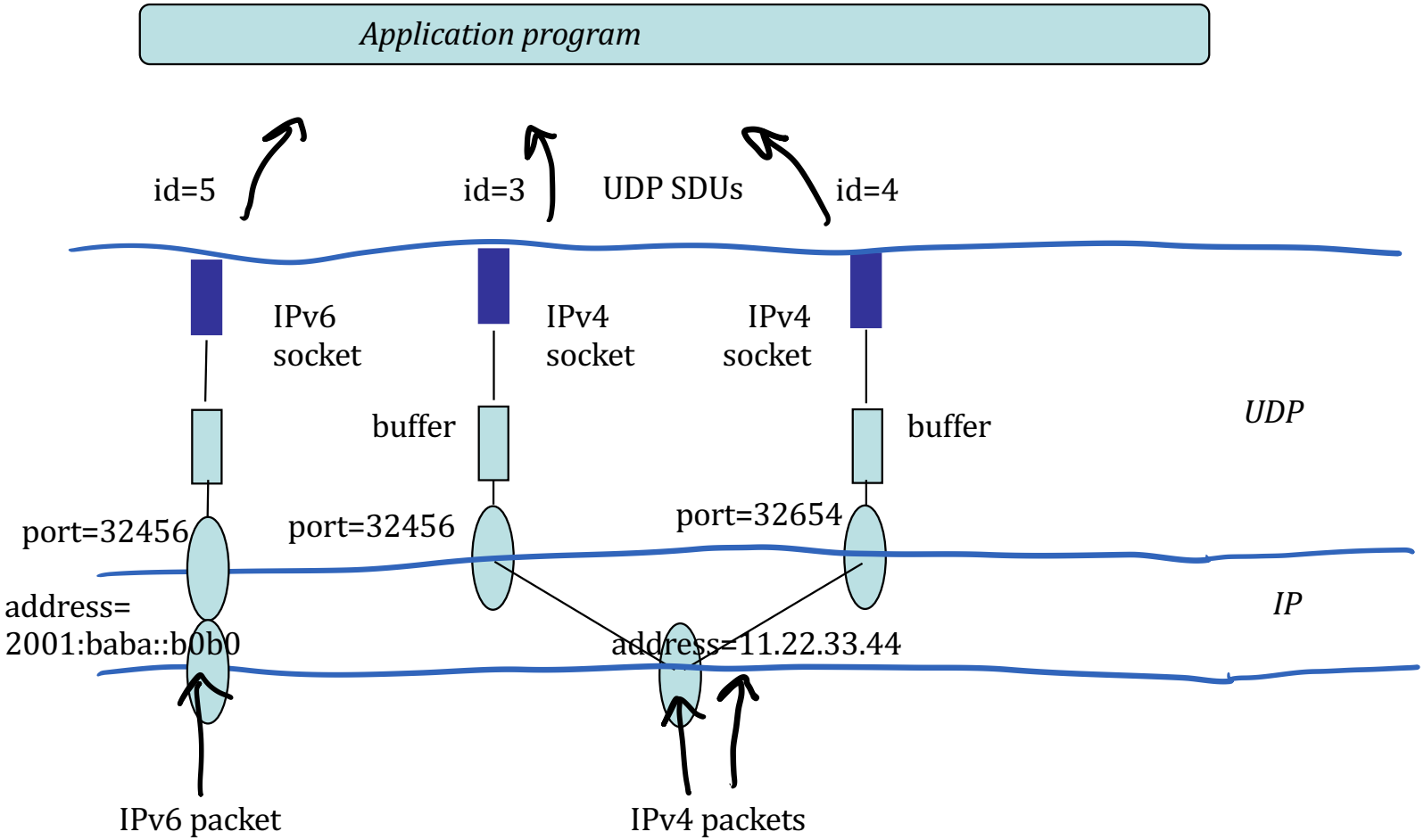
It then receives packets from IPv6 and from IPv4 correspondents.
IPv4 addresses of correspondents are mapped to IPv6 addresses using the IPv4-mapped IPv6 address format, i.e. an address in the block ::ffff:0:0/96



Default on Linux, must be enabled for every socket (with setsockopt) on Windows.

An IPv4 socket cannot be dual-stack. Why ?

How the Operating System views UDP

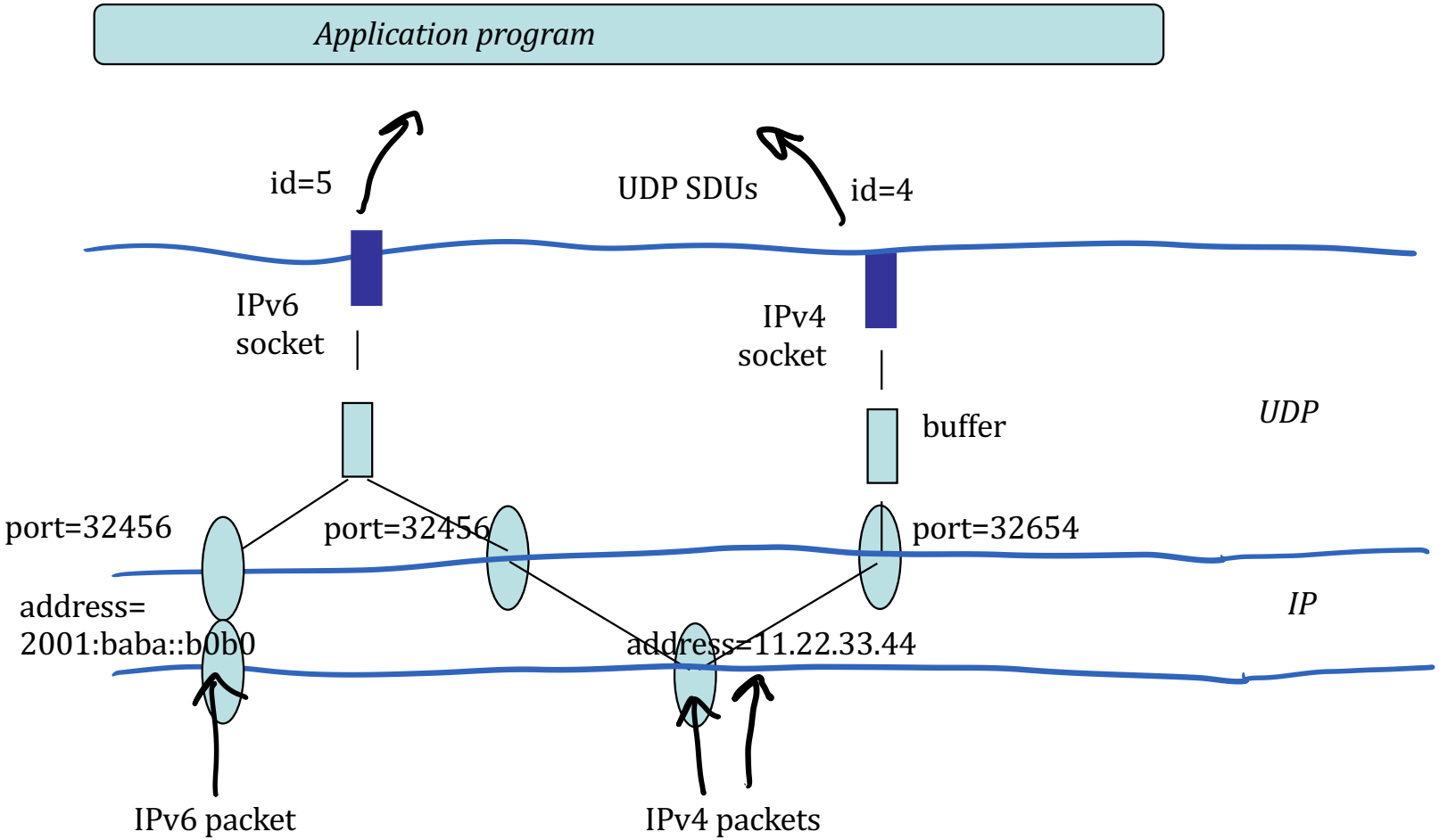


Socket 5 is bound to local address 2001:baba::b0b0 and port 32456; receives all data to 2001:baba::b0b0 udp port 32456

Socket 3 is bound to local address 11.22.33.44 and port 32456; receives all data to 11.22.33.44 udp port 32456

Socket 4 is bound to local address 11.22.33.44 and port 32654; receives all data to 11.22.33.44 udp port 32654

With a dual-stack IPv6 socket



Socket 5 is non connected and is bound to any local address, which includes IPv6 and IPv4 addresses, and to port 32456. Receives all packets to 2001:baba::b0b0, udp port 32456 and to 11.22.33.44 udp port 32456

Socket 4 is non connected and is bound to local address 11.22.33.44 and port 32654. Receives all packets to 11.22.33.44 udp port 32654

How the Operating System views UDP

On the sending side: Operating System sends the UDP datagram as soon as possible

On the receiving side: Operating System re-assembles IP fragments of UDP datagram (if required) and keeps it in buffer ready to be read. Packet is removed from buffer when application reads.

A socket is bound to one port; it is also bound to one or multiple IP addresses of the local machine.

Lisa's browser sends DNS query to DNS server, over UDP. What happens if query or answer is lost ?

A. Name resolver in browser waits for timeout, if no answer received before timeout, sends again
B. Messages cannot be lost because UDP assures message integrity
C. UDP detects the loss and retransmits
D. Je ne sais pas

2. TCP Basics: Sliding Window and Flow Control

In the Internet, packets may be lost

- buffer overflow
- physical layer errors

UDP application must handle loss

TCP solves the problem once for all

TCP offers in-sequence, lossless delivery

What does TCP do ?

TCP guarantees that all data is delivered *in sequence* and without loss, unless the connection is broken;

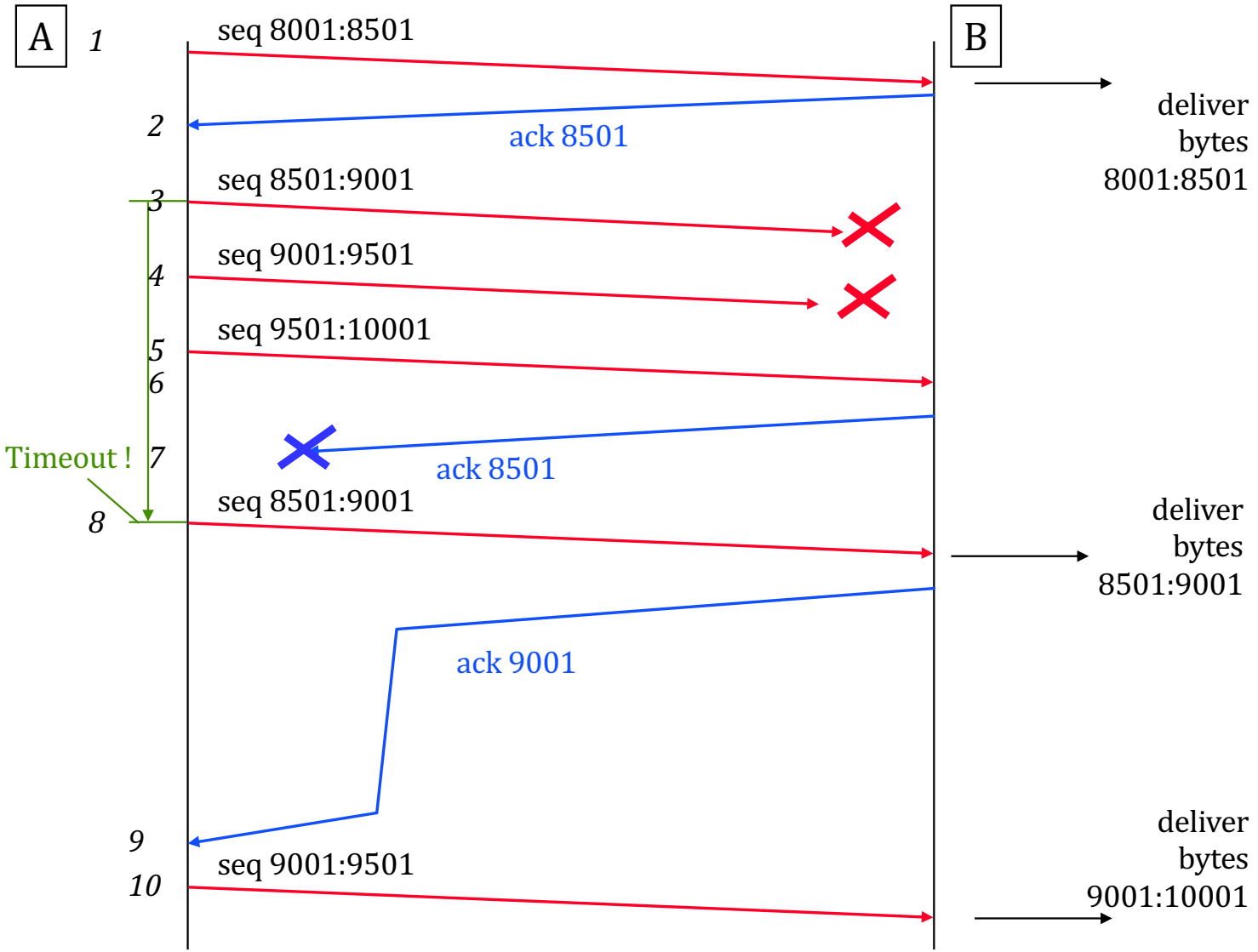
How does TCP work ?

data is numbered (per-byte sequence numbers)

a connection (=synchronization of sequence numbers) is opened between sender and receiver

TCP waits for acknowledgements; if missing data is detected, TCP re-transmits

TCP Basic Operation 1: showing SEQ and ACK



The previous slide shows A in the role of sender and B of receiver. The application at A sends data in blocks of 500 bytes. The maximum segment size is 1000 bytes. Ranges such as 8001:8501 mean bytes numbers 8001 to 8500.

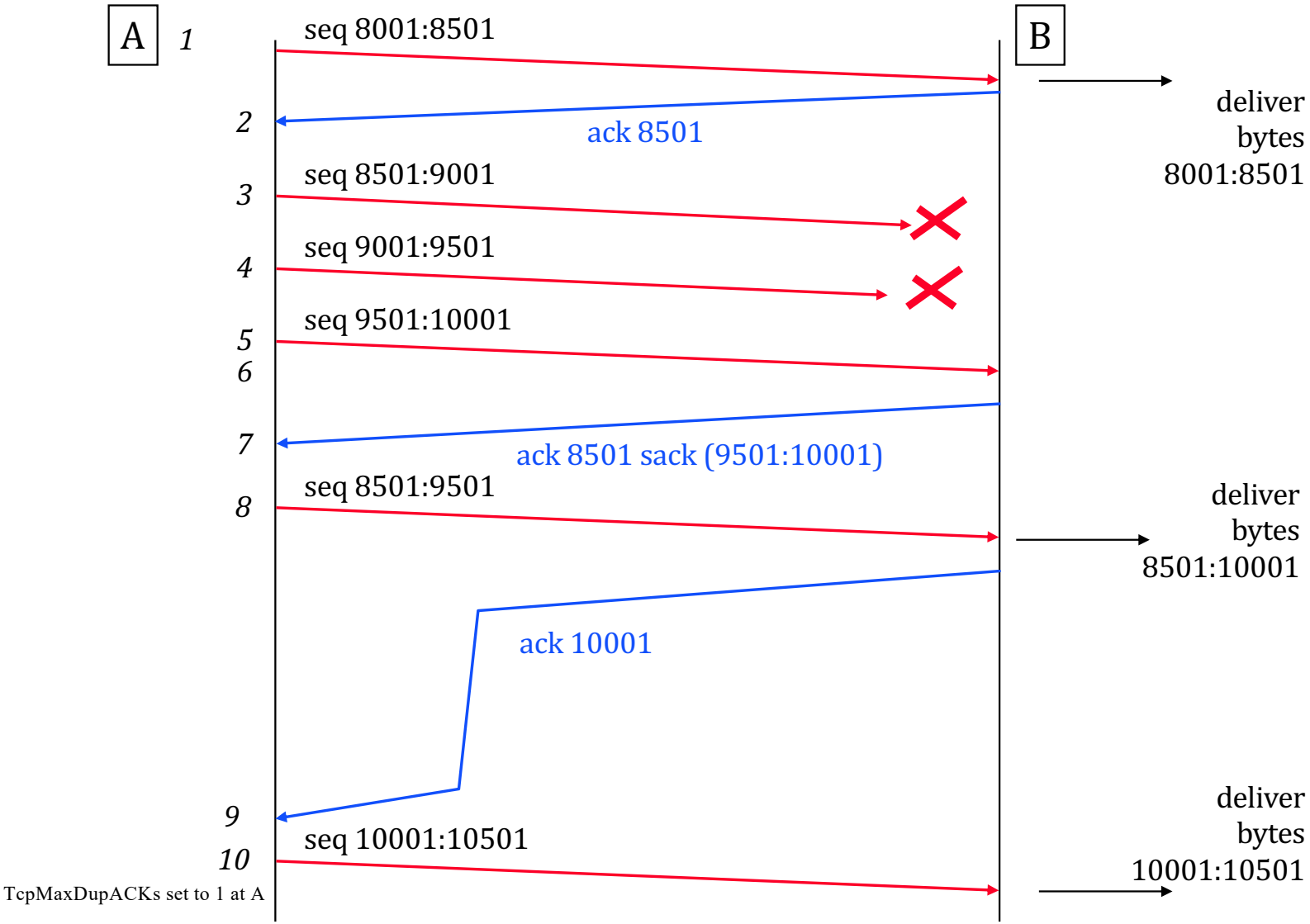
Packets 3, 4 and 7 are lost.

B returns an acknowledgement in the ACK field. The ACK field is *cumulative*, so ACK 8501 means: B is acknowledging all bytes up to (excluding) number 8501.

At line 8, the timer that was set at line 3 expires (A has not received any acknowledgement for the bytes in the packet sent at line 3). A re-sends data that is detected as lost, i.e. bytes 8501:9001. When receiving packet 8, B can deliver to the application all bytes 8501:9001.

When receiving packet 10, B can deliver bytes 9001:10001 because packet 5 was received and kept by B in the receive buffer.

TCP Basic Operation 1: showing SEQ, ACK and SACK



In addition to the ACK field, most TCP implementation also use the SACK field (Selective Acknowledgement). The previous slide shows the operation of TCP with SACK.

The application at A sends data in blocks of 500 bytes. The maximum segment size is 1000 bytes. Packets 3 and 4 are lost.

At line 6, B is acknowledges all bytes up to (excluding) number 8501.

At line 7, B acknowledges all bytes up to 8501 and in the range 9501:10001. Since the set of acknowledged bytes is not contiguous, the SACK option is used. It contains up to 3 blocks that are acknowledged in addition to the range described by the ACK field.

At line 8, A detects that the bytes 8501:9501 were lost and re-sends them. Since the maximum segment size is 1000 bytes, only one packet is sent.

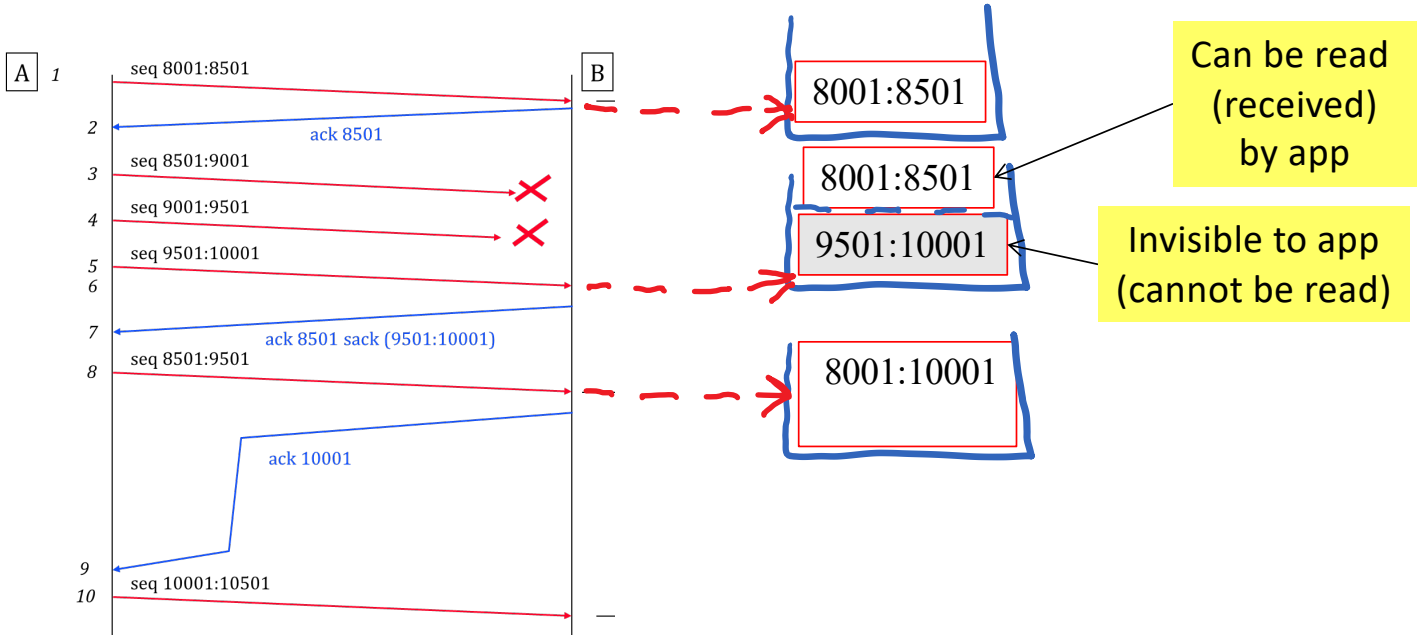
When receiving packet 8, B can deliver bytes 9001:10001 because packet 5 was received and kept in the receive buffer.

TCP receiver uses a *receive buffer = re-sequencing buffer* to store incoming packets before delivering them to application

Why invented ?

Application may not be ready to consume data

Packets may need re-sequencing; out-of-sequence data is stored but is not visible to application



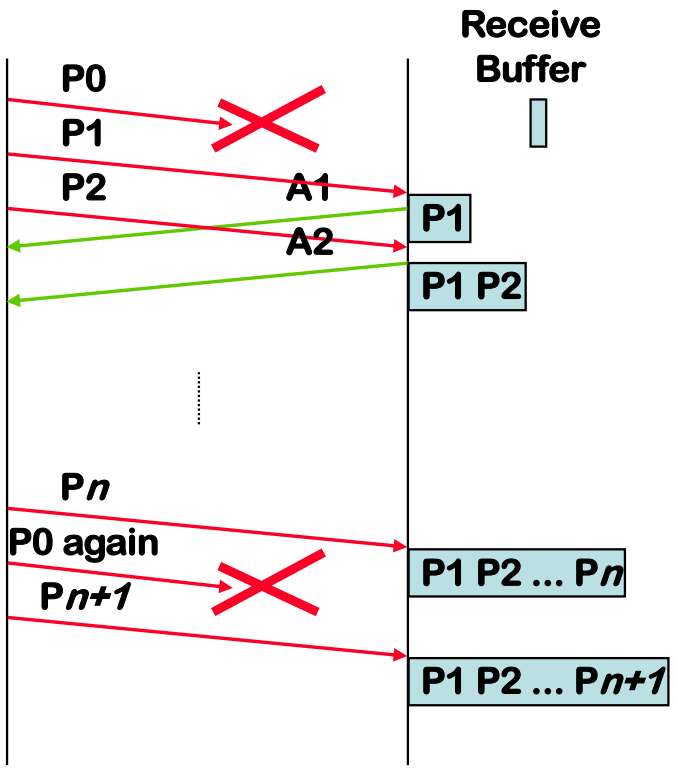
TCP uses a sliding window

The receive buffer may overflow if one piece of data “hangs”

- E.g. multiple losses affecting the same packet

This is why the sliding window was invented

- limits the number of data “on the fly”

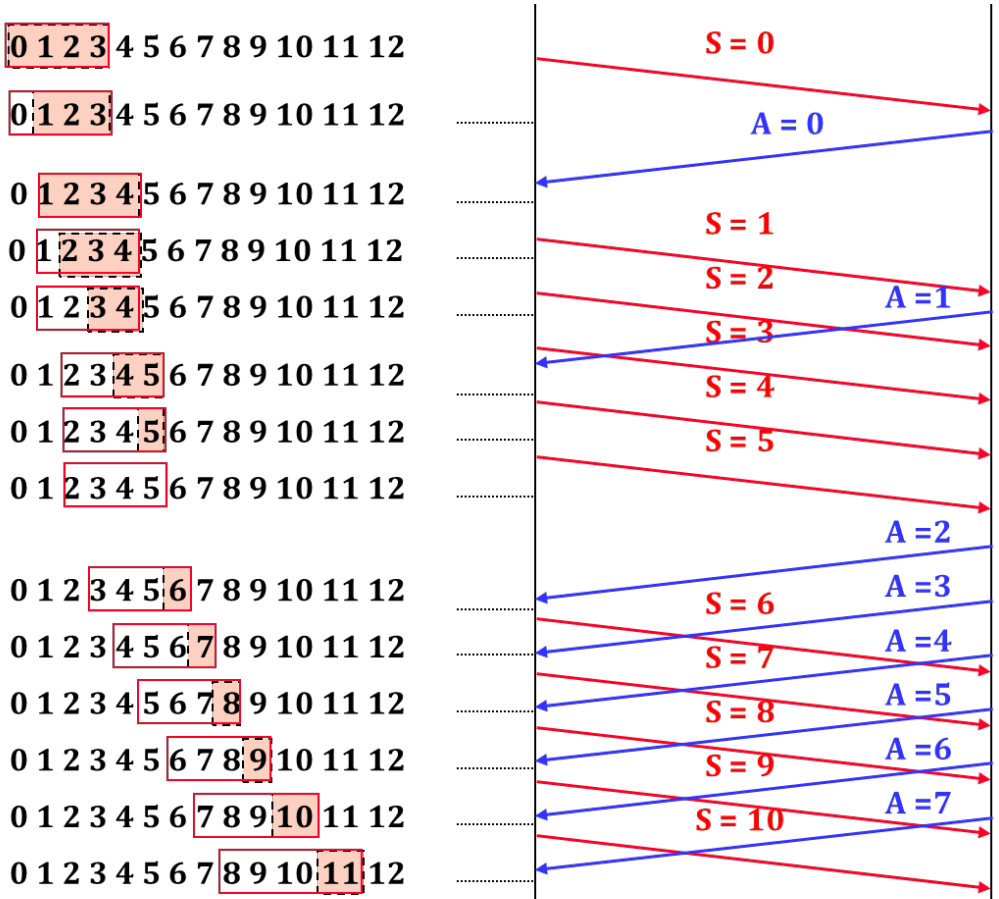


How the sliding window works

lower edge = smallest non acknowledged sequence number

upper edge = lower edge + window size

Only sequence numbers that are in the window may be sent

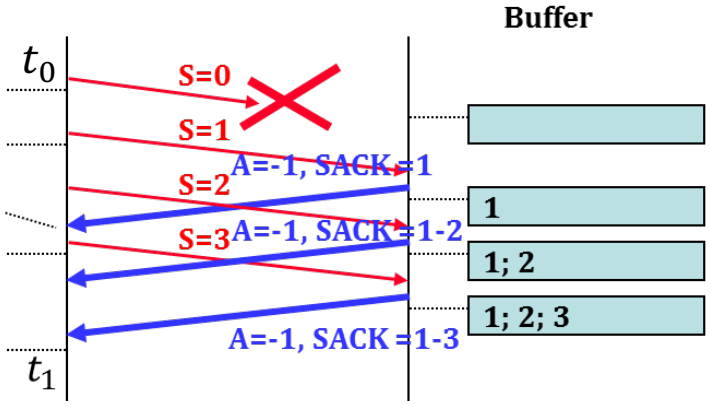


Window size = 4'000 bytes; one packet is 1'000 bytes

Window

Usable part of the window

At time t_1, sender…



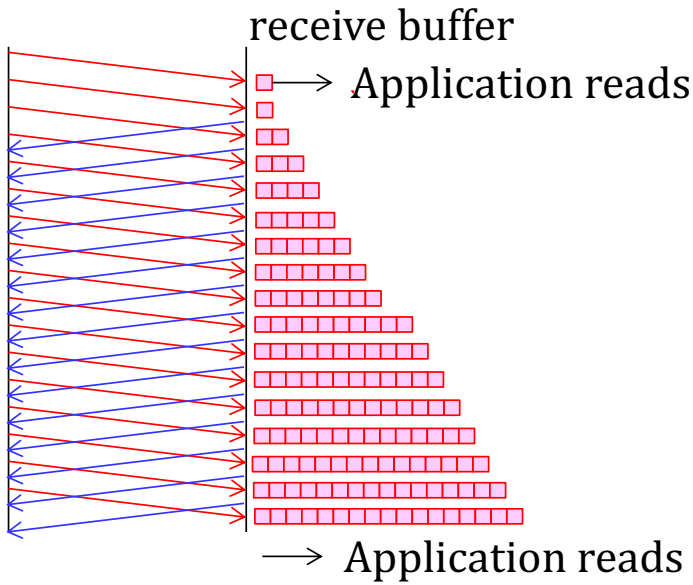
Window size = 4'000 bytes, one packet = 1'000 bytes
Sliding window was initialized at time t_0

A. … can send packet 4
B. … cannot send packet 4
C. It depends on whether data was consumed by application
D. Ich weiss nicht

Sliding Window is not sufficient to limit buffer size at receiver

Data that is received in-sequence remains in receive buffer until consumed by application (typically using a socket “read” or “receive”)

A slow application could cause buffer overflow



Window size = 4’000 bytes

One packet = = 1’000 bytes

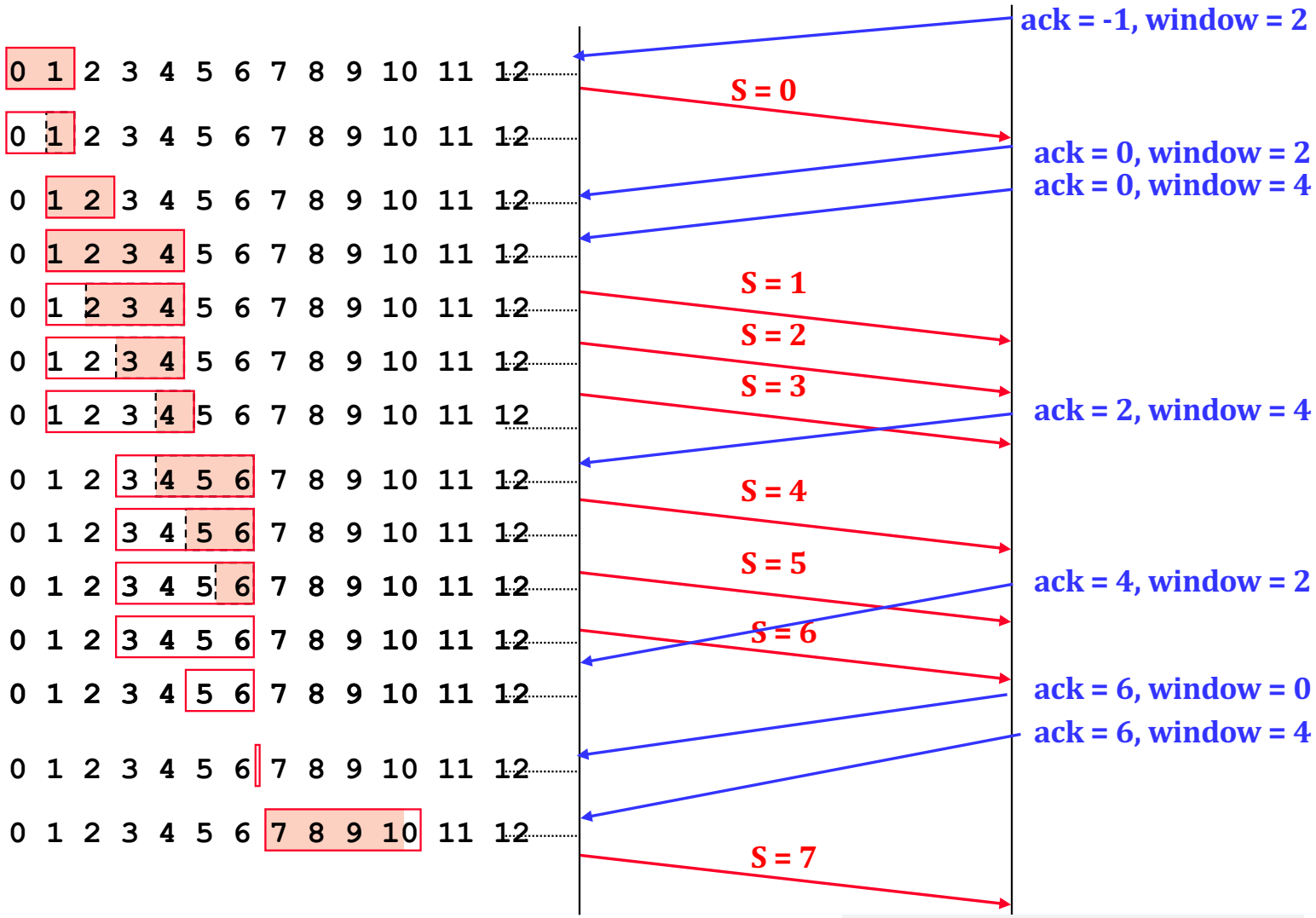
Window Flow Control is used to prevent receive-buffer overflow

TCP constantly adapts the size of the window by sending "window" advertisements back to the source.

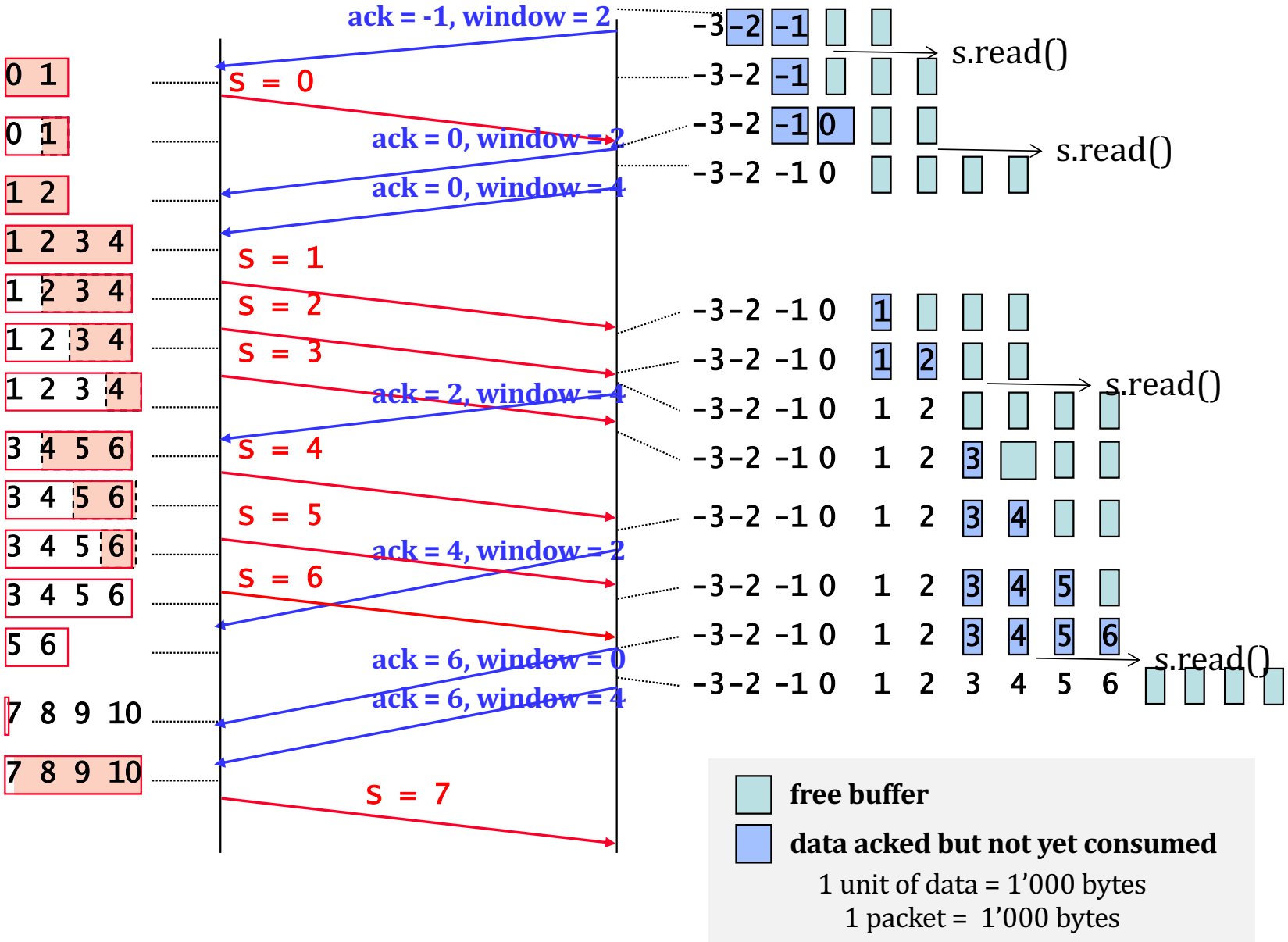
- Window size is set to available buffer size
- If no space in buffer, window size is set to 0

This is called "*Flow Control*" = adapt sending rate of source to speed of receiver

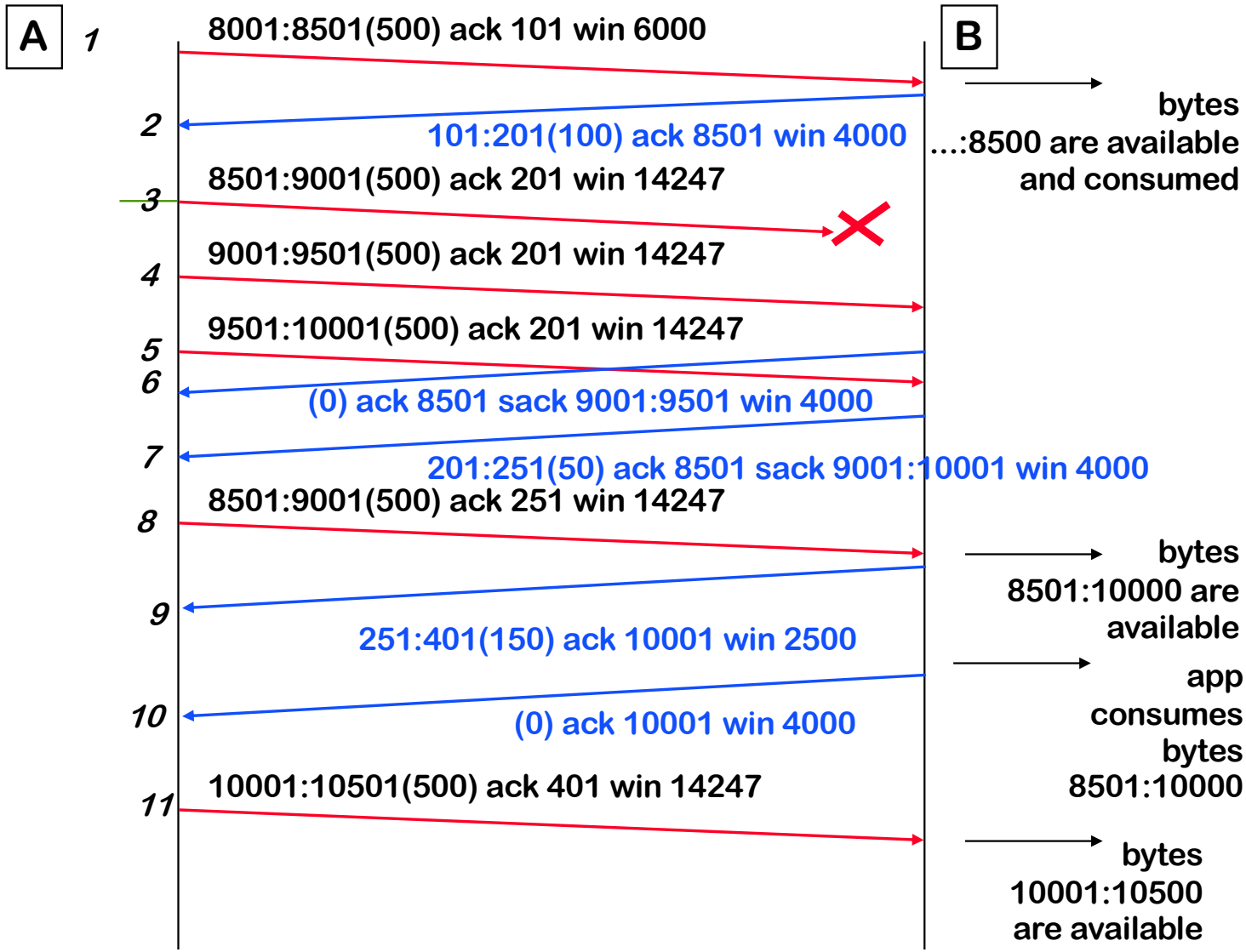
≠ Congestion Control (see later), which adapts rate of source to state of network



1 unit of data = 1’000 bytes
1 packet = 1’000 bytes


ack = -1, window = 2
S = 0
ack = 0, window = 2
ack = 0, window = 4
S = 1
S = 2
S = 3
ack = 2, window = 4
S = 4
S = 5
ack = 4, window = 2
S = 6
ack = 6, window = 0
ack = 6, window = 4
S = 7
s.read()
s.read()
s.read()
s.read()
free buffer
data acked but not yet consumed
1 unit of data = 1'000 bytes
1 packet = 1'000 bytes

TCP Basic Operation, Putting Things Together



The picture shows a sample exchange of messages. Every packet carries the sequence number for the bytes in the packet; in the reverse direction, packets contain the acknowledgements for the bytes already received in sequence. The connection is bidirectional, with acknowledgements and sequence numbers for each direction. So here A and B are both senders and receivers.

Acknowledgements are not sent in separate packets (“piggybacking”), but are in the TCP header. Every segment thus contains a sequence number (for itself), plus an ack number (for the reverse direction). The following notation is used:

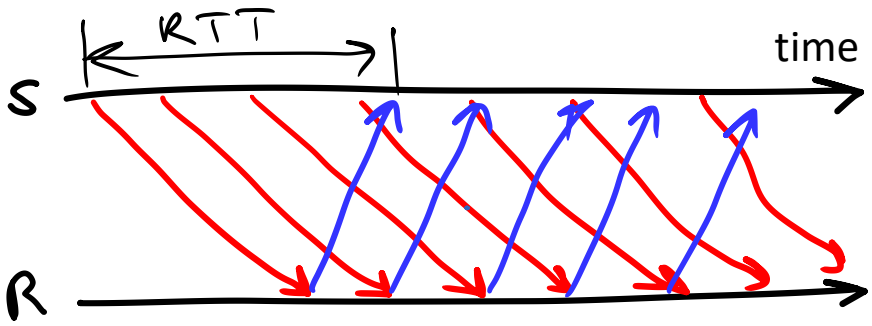
- firstByte”:”lastByte+1 “(“segmentDataLength”) ack” ackNumber+1 “win” offeredWindowSise. Note the +1 with ack and lastByte numbers.

At line 8, A retransmits the lost data. When packet 8 is received, the application is not yet ready to read the data.

Later, the application reads (and consumes) the data 8501:10001. This frees some buffer space on the receiving side of B; the window can now be increased to 4000. At line 10, B sends an empty TCP segment with the new value of the window.

Note that numbers on the figure are rounded for simplicity. In real examples we are more likely to see non-round numbers (between 0 and 232 -1). The initial sequence number is not 0, but is chosen at random.

In the absence of loss, and on a link with capacity c packets per second, the window size required for sending at the maximum possible rate is…



A. $W_{min} = RTT \times c$
B. $W_{min} = \frac{c}{RTT}$
C. $W_{min} = \frac{RTT}{c}$
D. None of the above
E. Non lo so

3. TCP Connections and Sockets

TCP requires that a connection (= synchronization) is opened before transmitting data

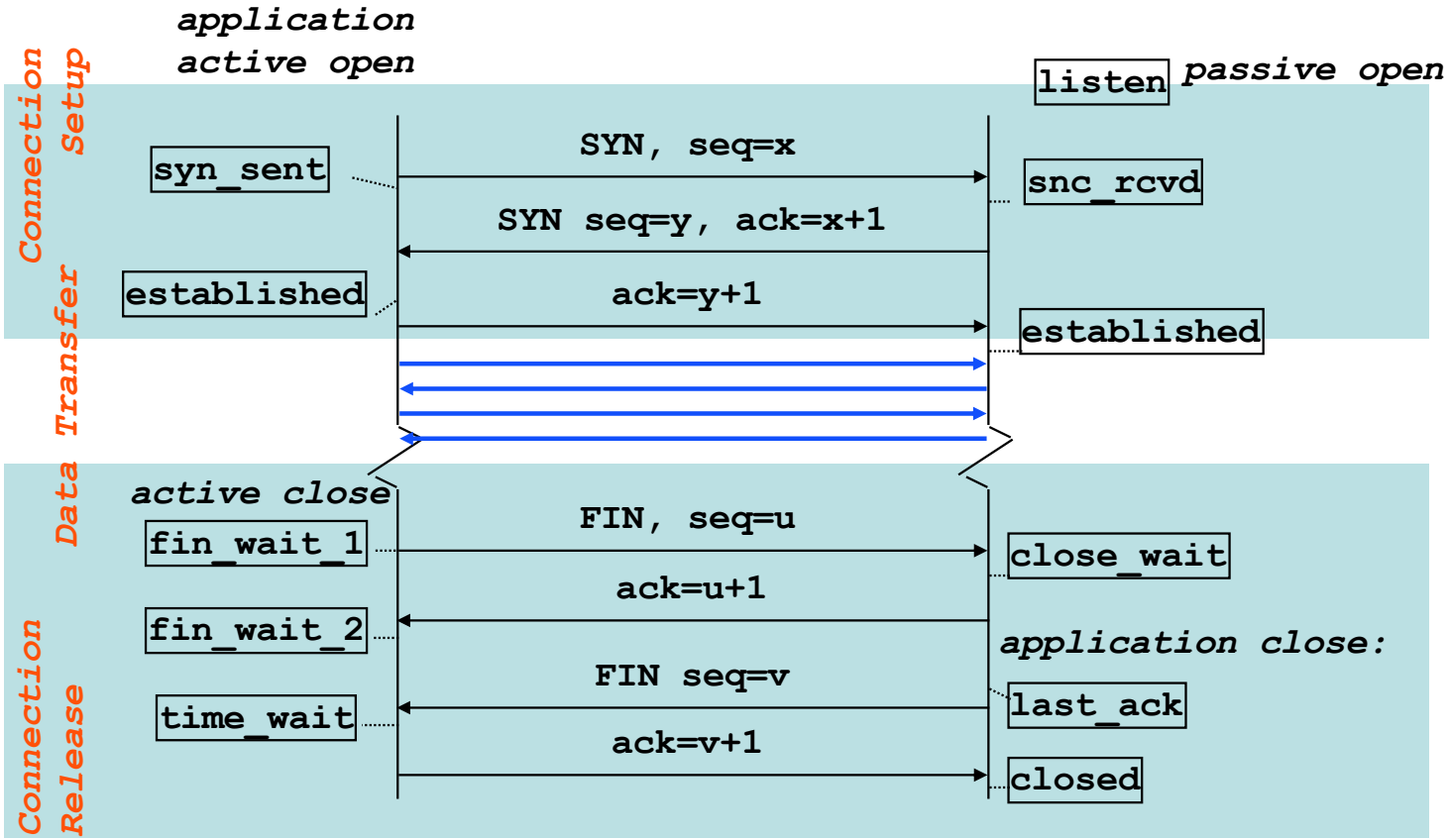
- Used to agree on sequence numbers and make sure buffers and window are initially empty

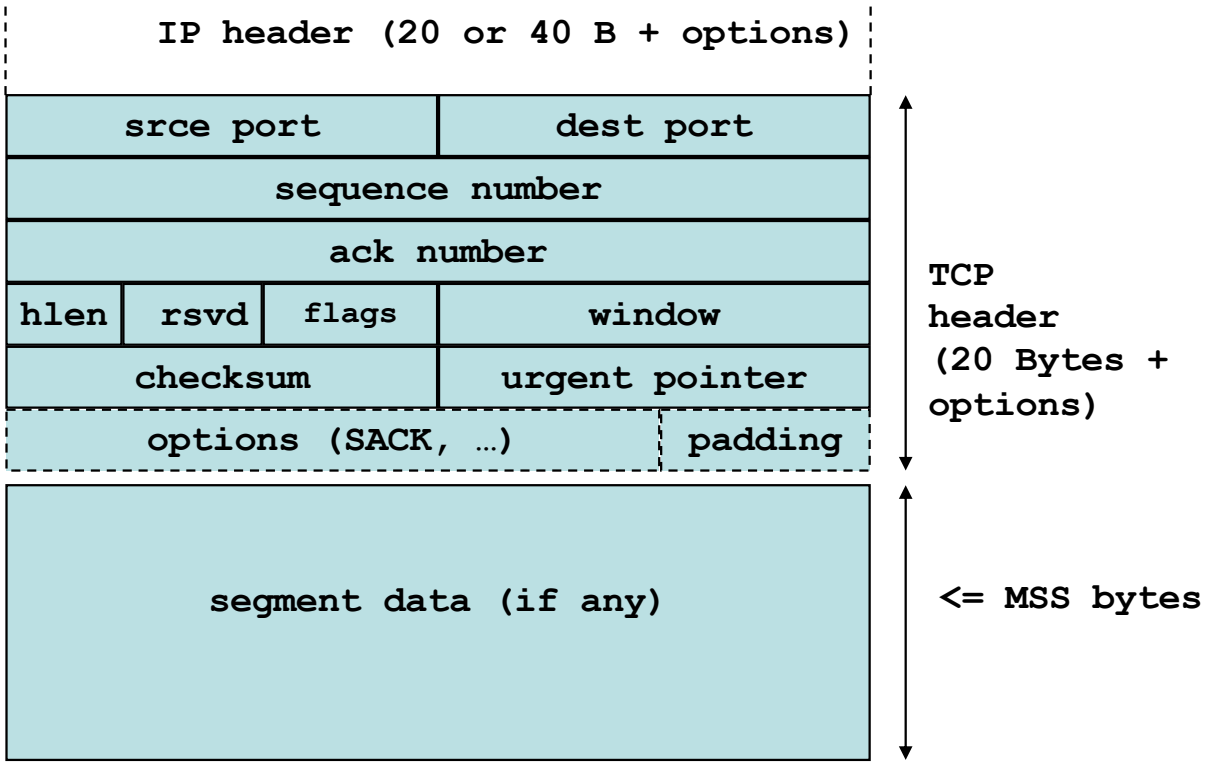
The next slide shows the states of a TCP connection:

- Before data transfer takes place, the TCP connection is opened using SYN packets. The effect is to synchronize the counters on both sides.
- The initial sequence number is a random number.
- The connection can be closed in a number of ways. The picture shows a graceful release where both sides of the connection are closed in turn.
- Remember that TCP connections involve only two hosts; routers in between are not involved.

There are many more subtleties (e.g. how to handle connection termination, lost or duplicated packets during connection setup, etc—see Textbook sections 4.3.1 and 4.3.2).

TCP Connection Phases





flags	meaning
NS	used for explicit congestion notification
CWR	used for explicit congestion notification
ECN	used for explicit congestion notification
urg	urgent ptr is valid
ack	ack field is valid
psh	this seg requests a push
rst	reset the connection
syn	connection setup
fin	sender has reached end of byte stream

TCP Segment Format

The previous slide shows the TCP segment format.

▪the push bit can be used by the upper layer using TCP; it forces TCP on the sending side to create a segment immediately. If it is not set, TCP may pack together several SDUs (=data passed to TCP by the upper layer) into one PDU (= segment). On the receiving side, the push bit forces TCP to deliver the data immediately. If it is not set, TCP may pack together several PDUs into one SDU. This is because of the stream orientation of TCP. TCP accepts and delivers contiguous sets of bytes, without any structure visible to TCP. The push bit used by Telnet after every end of line.

▪ the urgent bit indicates that there is urgent data, pointed to by the urgent pointer (the urgent data need not be in the segment). The receiving TCP must inform the application that there is urgent data. Otherwise, the segments do not receive any special treatment. This is used by Telnet to send interrupt type commands.

▪ RST is used to indicate a RESET command. Its reception causes the connection to be aborted.

▪ SYN and FIN are used to indicate connection setup and close. They each consume one sequence number.

▪ The sequence number is that of the first byte in the data. The ack number is the next expected sequence number.

▪ Options contain for example the Maximum Segment Size (MSS) normally in SYN segments (negotiation of the maximum size for the connection results in the smallest value to be selected) and SACK blocks.

▪The checksum is mandatory

▪The NS, CRW and ECN bits are used for congestion control (see congestion control module).

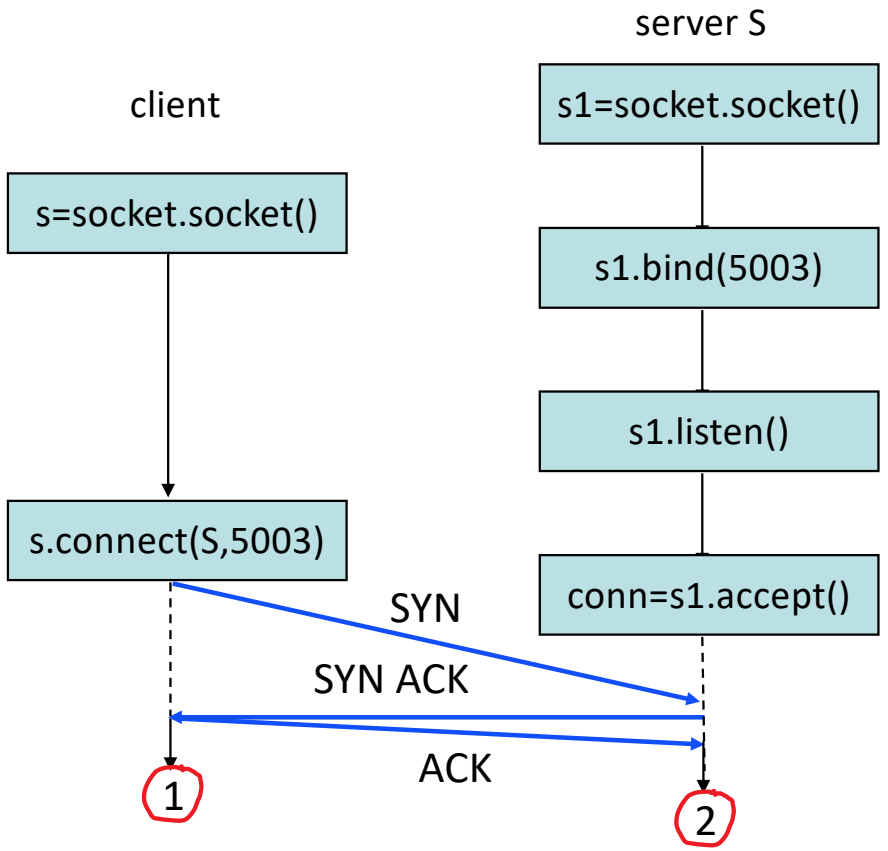
TCP Sockets

TCP is used by means of sockets, like UDP.

However, TCP sockets are more complicated because of the need to open/close a connection

Opening a TCP connection requires one side to listen (this side is called “server”) and one side to connect (called “client”)

At 1, client can use the connection to send or receive data on this socket



The figure shows toy client and servers. The client sends a string of chars to the server which reads and displays it.

socket(AF_INET,…) creates an IPv4 socket and returns a socket object if succesful
socket(AF_INET6,…) creates an IPv6 socket

bind(5003) associates the local port number 5003 with the socket; the server must bind, the client need not bind, a temporary port number is allocated by the OS

connect() associates the remote IP address and port number with the socket and sends a SYN packet

send() sends a block of data to the remote destination

listen() declares the size of the buffer used for storing incoming SYN packets;

accept() blocks until a SYN packet is received for this local port number. It creates a new socket (in pink) and returns the file descriptor to be used to interact with this new socket

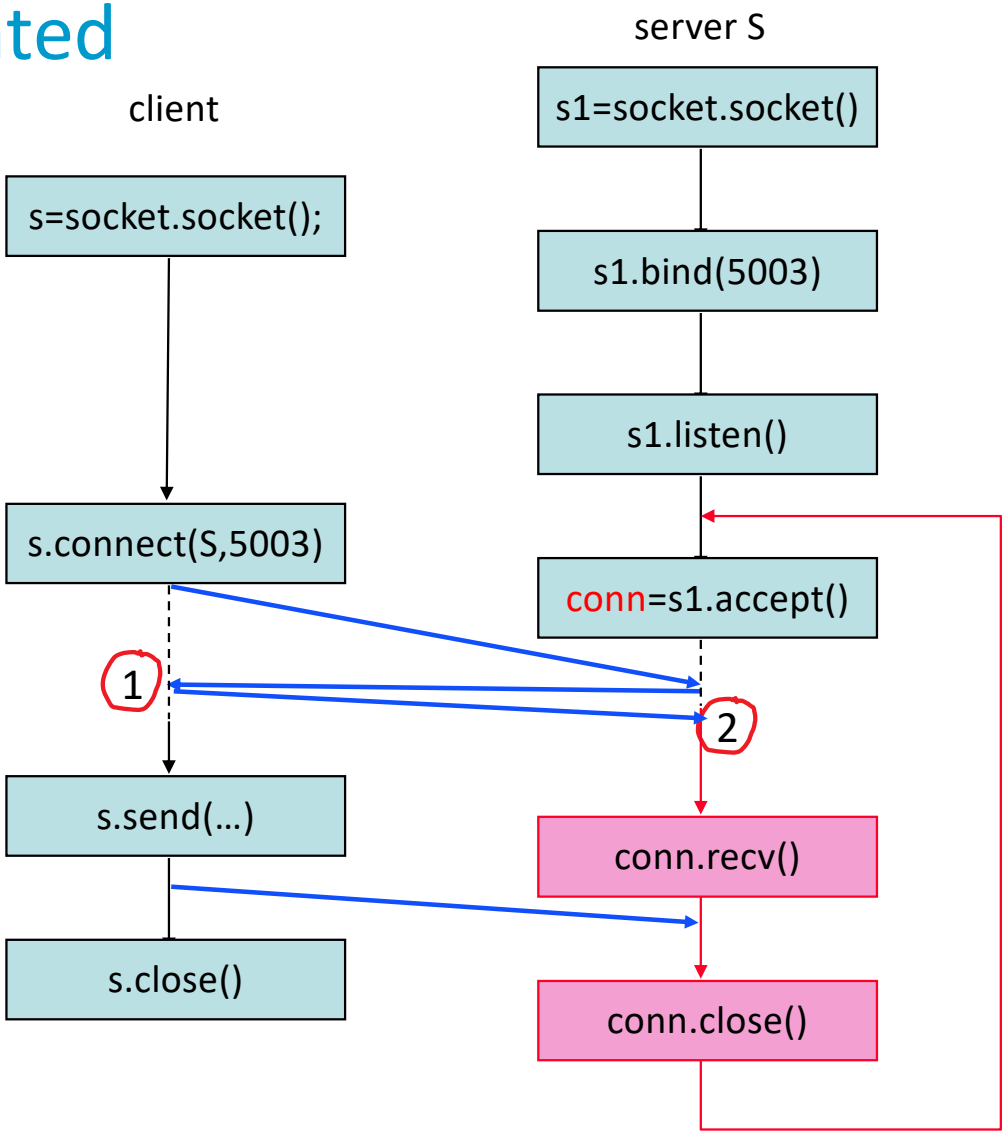
recv() blocks until one block of data is ready to be consumed on this port number. You must tell in the argument how many bytes at most you want to read. It returns a block of bytes with the bytes that are effectively returned. It raises an exception when the connection was closed by the other end.

A New Socket is Created by Accept()

At 2, on server side, a new socket (conn) is created – will be used by server to send or receive data.

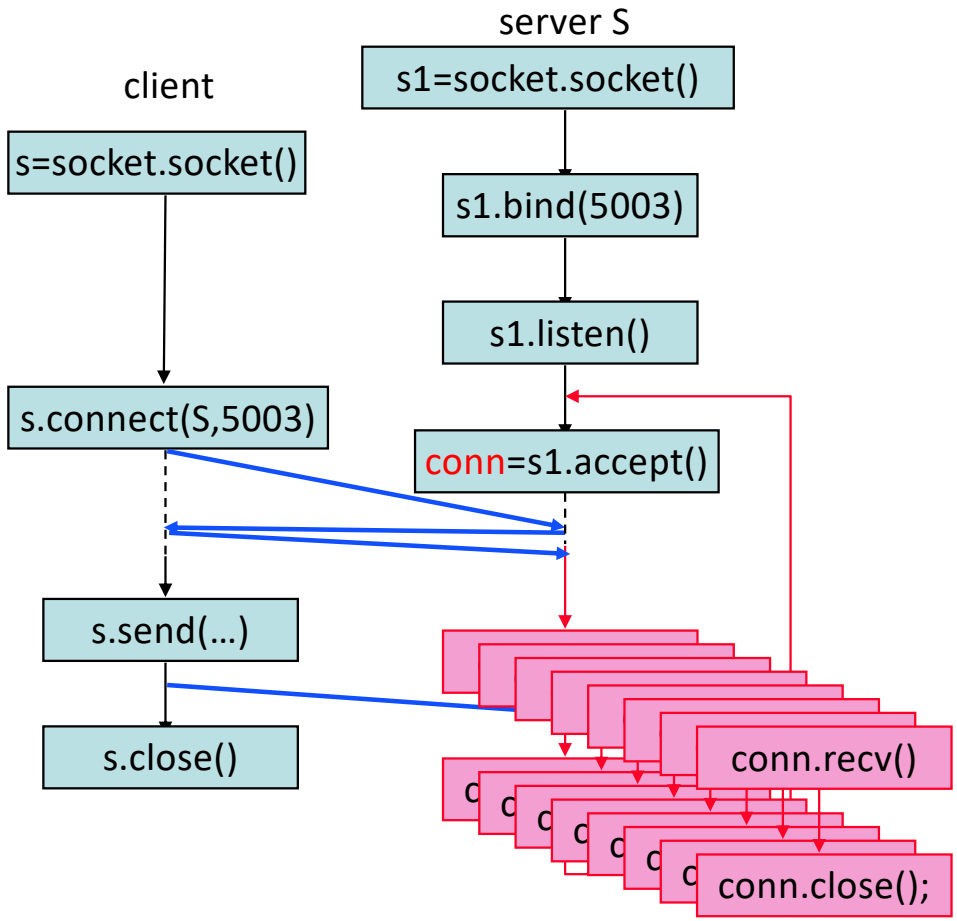
conn is a *connected* socket, s1 is a *non-connected* socket

This example shows a simplistic program: client sends one message to server and quits; server handles one client at a time.

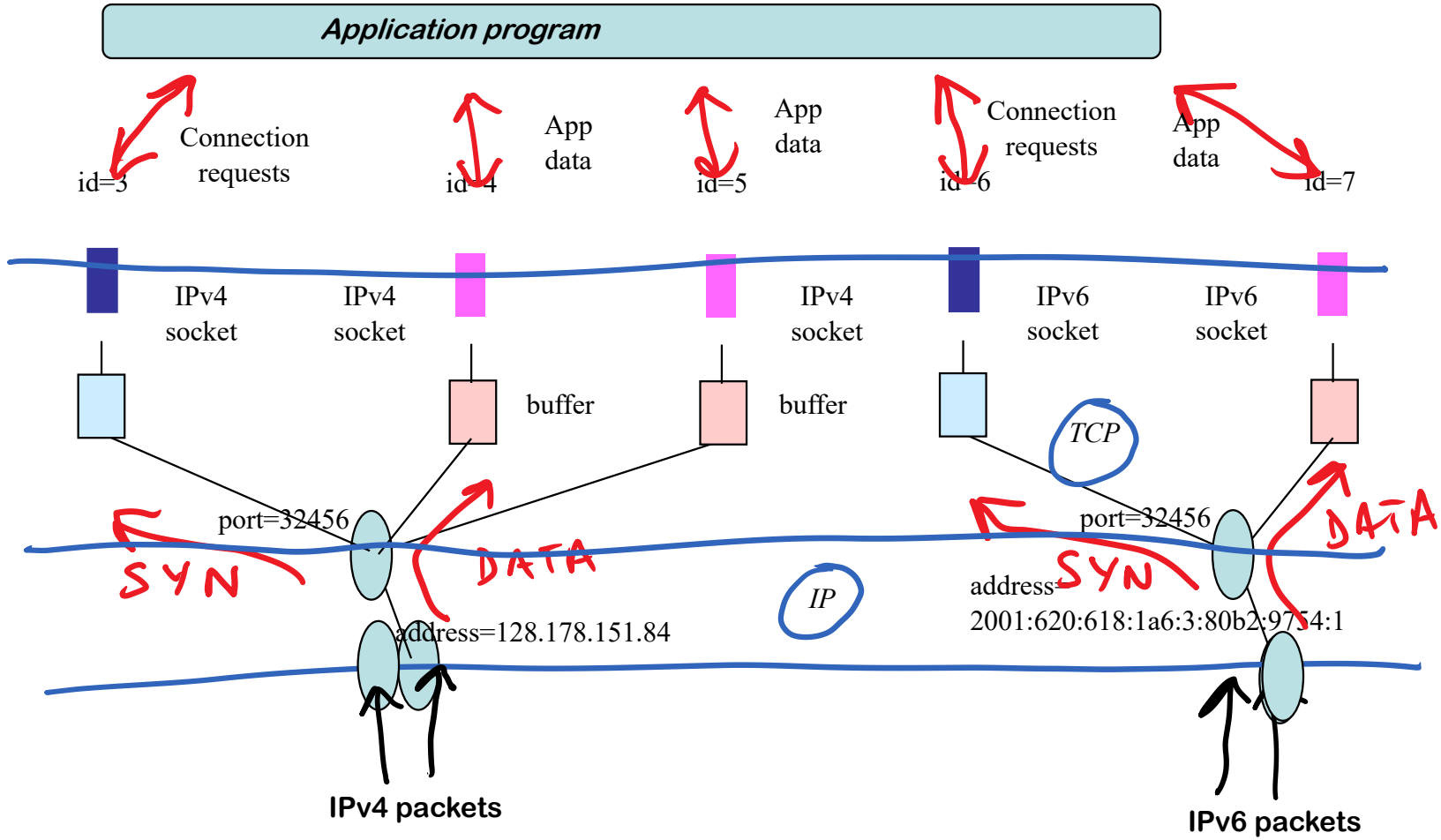


A More Typical Server

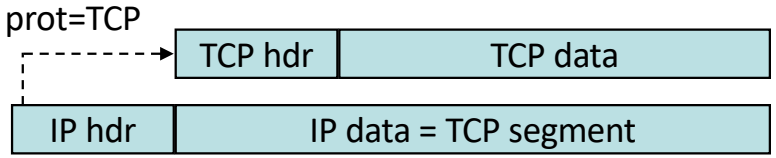
TCP Server typically uses parallel threads of execution to handle several TCP connections + to listen to incoming connections



How the Operating System views TCP Sockets



TCP Connections and Segments



TCP uses port numbers like UDP eg. TCP port 80 is used for web server. A TCP connection is identified by: **srce IP addr, srce port, dest IP addr, dest port.**

TCP-PDUs (called TCP segments) have a maximum size (called MSS). 536 bytes by default for IPv4 operation (576 bytes IPv4 packet), 1220 by default for IPv6 operation (1280 bytes IPv6 packets)

TCP, not the application, chooses how to segment data

TCP segments should not be fragmented at source

Modern OSs use TCP Segmentation Offloading (TSO) : the TCP code in the OS sends a possibly large block of data to the network interface card (NIC). Segmentation is performed in the NIC with hardware assistance (reduces CPU consumption of TCP).

TCP Offers a Streaming Service

Streaming Service: TCP accumulates bytes in send buffer until it decides to create a segment

independent of how application writes data

On receiver side, data accumulates in receive buffer until application reads it – data is not delineated, several small pieces of data sent by A may be received by B as a single block – and conversely, a single block sent by A may be received by B as multiple blocks.

A side effect is head of the line blocking : If one packet sent by A is lost, all data following this packet is delayed until the loss is repaired.

For which types of apps is the streaming service a drawback ?

A. an app using http/1 with one TCP connection per object
B. an app using http/2 with one TCP connection in total
C. a real time streaming application that sends one new packet every msec
D. A and B
E. A and C
F. B and C
G. All
H. None
I. No lo sé

A TCP server is, by definition…

A. … an application program that does listen( ) and accept( ) on a TCP socket

B. … an application program that does receive( ) on a TCP socket

C. … an application program that does send( ) on a TCP socket

D. $\Delta\varepsilon\nu\ \xi\varepsilon\rho\omega$

Why both TCP and UDP ?

Most applications use TCP rather than UDP, as this avoids re-inventing error recovery in every application

But some applications do not need error recovery in the way TCP does it (i.e. by packet retransmission)

For example: Voice applications / PMU streaming

Q. why ?

For example: an application that sends just one message, like name resolution (DNS).

Q. Why ?

For example: multicast (TCP does not support multicast IP addresses)

4. More TCP Bells and Whistles

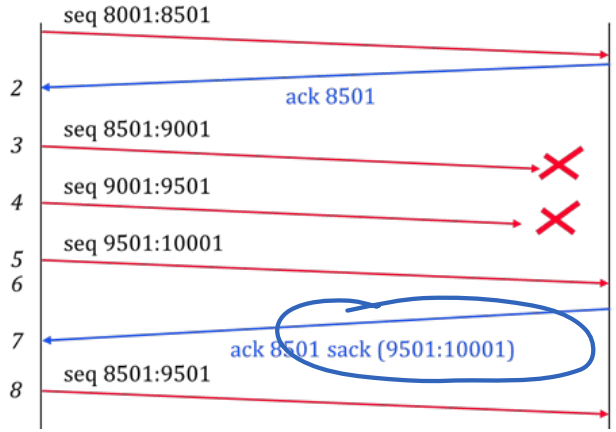
TCP has been constantly improved since its inception in 1974. For example, problems to be solved are

- When to send a packet (application may write 1 byte into the socket; should TCP make one packet ?) -> Nagle's algorithm prevents making many small packets.
- When to send an ACK when there is no data to send in return ?
- When to increase the window size (silly window syndrome avoidance)?
- How to detect packet loss
- How to choose initial sequence numbers (SYN cookies) to avoid denial of service attack by SYN flooding
- How to avoid three way handshake

We will see only the last three in detail; see textbook section 4.3.3 for the ones we don't see here.

We could say that TCP declares a packet lost when a duplicate ACK is received with a SACK field. Is it a good idea ?

A. Yes because it is likely that there is some missing data
B. No as it may cause superfluous retransmissions (some data could simply be late -- out of order)
C. No because an ACK also could be lost
D. N'ouzhon ket.



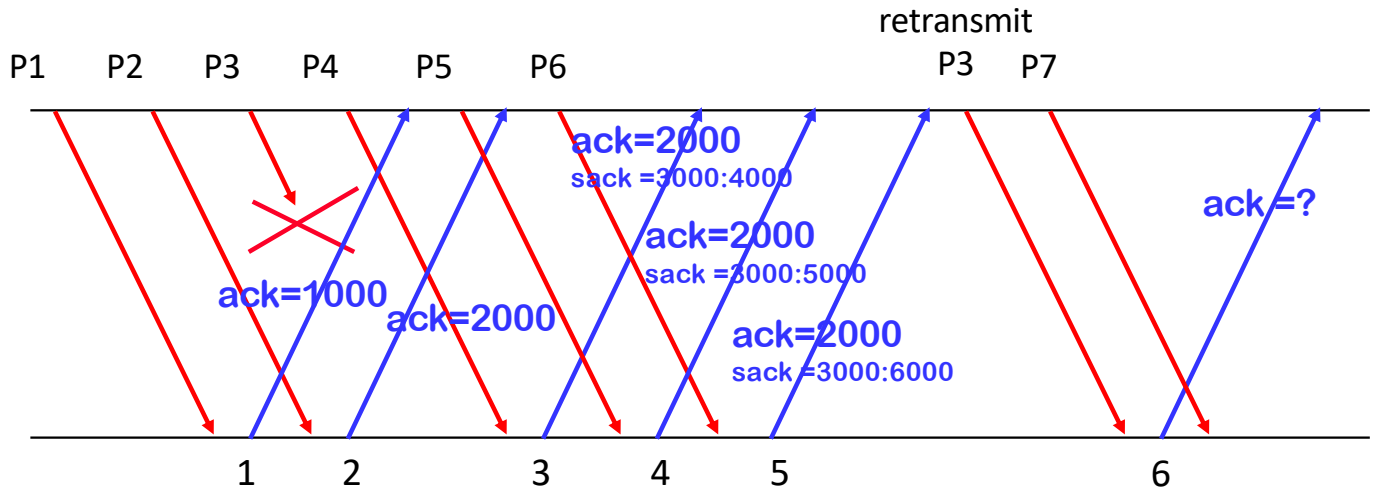
Fast Retransmit

Principle: when n duplicate ACKs are received, declare a loss

(Duplicate ACK = a TCP packet where the ACK value repeats a previously received ACK value)

The lost data is inferred from the SACK blocks

$n =$ *TcpMaxDupACKs* is set by the Operating System (typically or 3)



all segments are 1000 bytes; TcpMaxDupACKs = 3

Loss Detection in TCP also uses timers

"Fast retransmit" detects most losses but not all

- some bursts of losses are not detected
- last packets that are lost are not detected
- isolated packets that are lost are not detected

TCP also uses a retransmit timer, set for every packet transmission

- when one timer expires this is interpreted as a severe loss (loss of channel). All timers are reset and all data is marked as needing retransmission.

Round Trip Estimation

Why ? The retransmission timer must be set at a value larger than the round trip time, but not too much

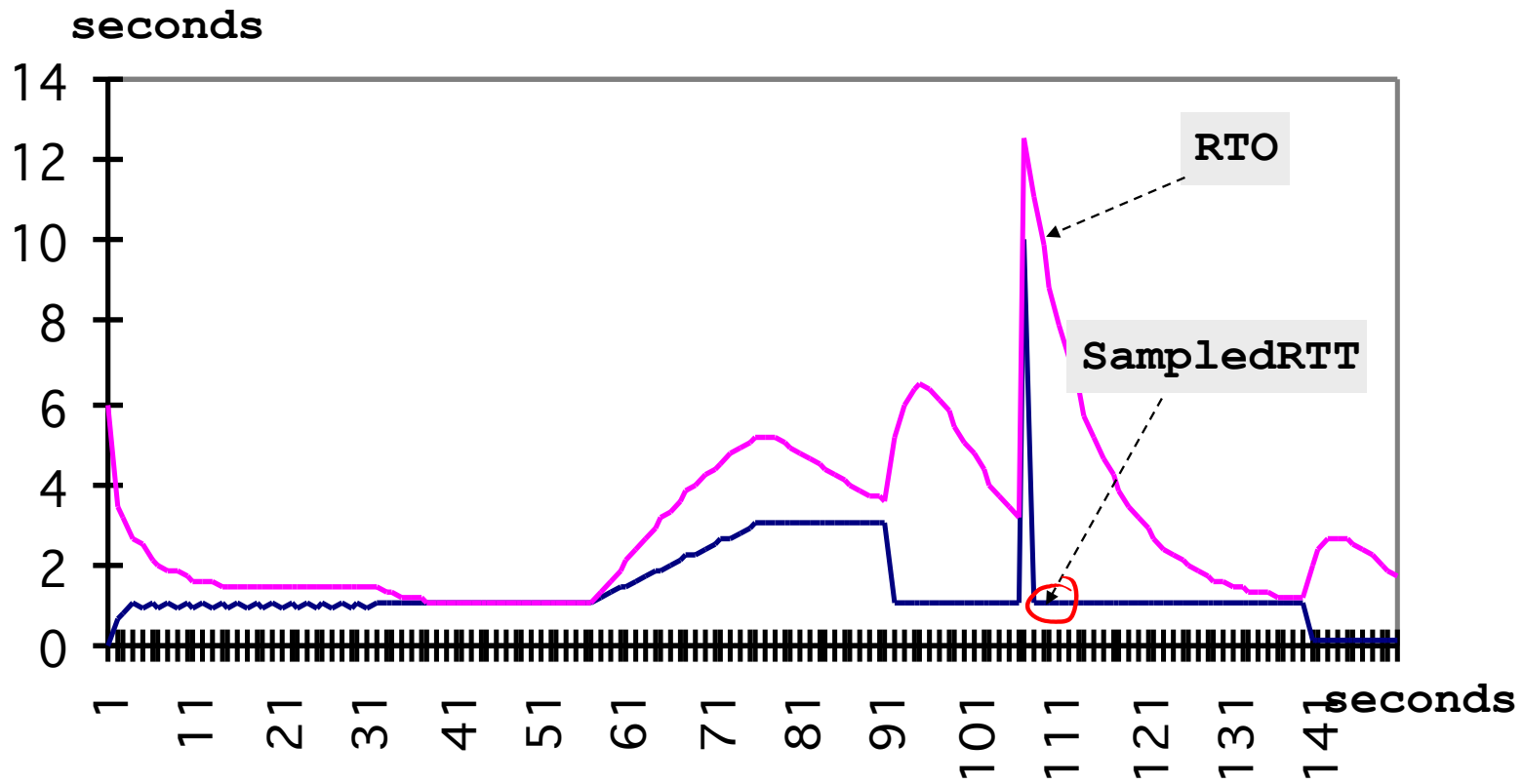
What ? RTT estimation computes an upper bound RTO on the round trip time

How ?

srtt : smoothed RTT
rtt: last measured RTT
rttvar: ℓ^1 error bound
$\alpha = \frac{1}{8}, \beta = \frac{1}{4}, \eta = 4$

rttvar $= (1 - \beta)$ rttvar $+ \beta$ |srtt – rtt|
srtt $= (1 - \alpha)$ srtt $+ \alpha$ rtt
rto $=$ srtt $+ \eta$ rttvar

Sample RTO


seconds
14
12
10
8
6
4
2
0
RTO
SampledRTT
1
11
21
31
41
51
61
71
81
91
101
111
121
131
141
seconds

When does Fast Retransmit Fail ?

A. Extremely rarely, it is quasi-optimal
B. It fails to detect the loss extremely rarely, but it may often take a long time to detect.
C. When one of the last segments of an application layer block is lost, fast retransmit does not detect it.
D. It may often fail due to packet re-ordering
E. لا أعرف

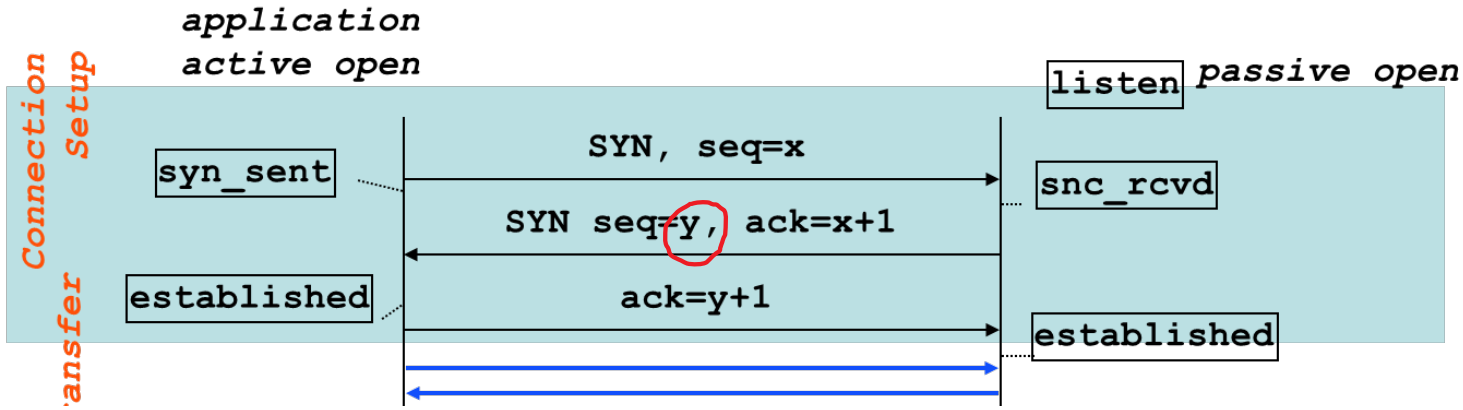
SYN Cookies

Why ? mitigate impact of SYN flood attack: lots of bogus SYN packets from invalid source addresses sent to a server.

When a TCP server receives a SYN packet, it should remember the details of the connection (source IP address, port, seq number) and store them in kernel space. If SYNs are bogus, they remain stored until timeout occurs. The listen queue is full and legitimate SYN packets are dropped. Server is out !

What ? with SYN cookies, TCP server does not keep state information after receiving a SYN packet. State is encoded in the Seq Number field, using a cryptographic function and returned to client (the “cookie”). If SYN is valid, 3rd ack contains the state in the ACK.

SYN Cookies Encode State in Seq of SYN ACK



State (called *SYN cookie*) is written in y

y = (5 bit) t mod 32 ||(3 bits) MSS encoded in SYN ||(24 bits) cryptographic hash of secret server key, of t (timestamp) and client IP address and port number, the server IP address and port number.

Server drops state and sends SYN cookie=y in SYN ACK. Client sends ack=y+1. Server verifies that hash is valid; if so creates socket, using the MSS recovered from the cookie.

If SYN was bogus, no ack follows and damage is reduced to loss of computation but no loss of listen queue availability.

Server does *not* implement SYN cookies. If the ACK (3) is never sent, server will

1) retransmit SYN ACK

2) keep state information until timeout occurs

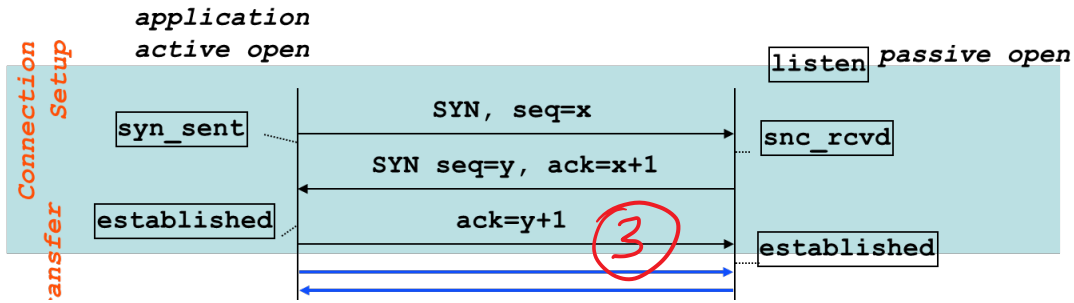
A. 1

B. 2

C. 1 and 2

D. None

E. 我不知道



With SYN cookies, the response time of SYN-ACK is…

A. Larger than without SYN cookies
B. Smaller than without SYN cookies
C. The same
D. I weiss nid

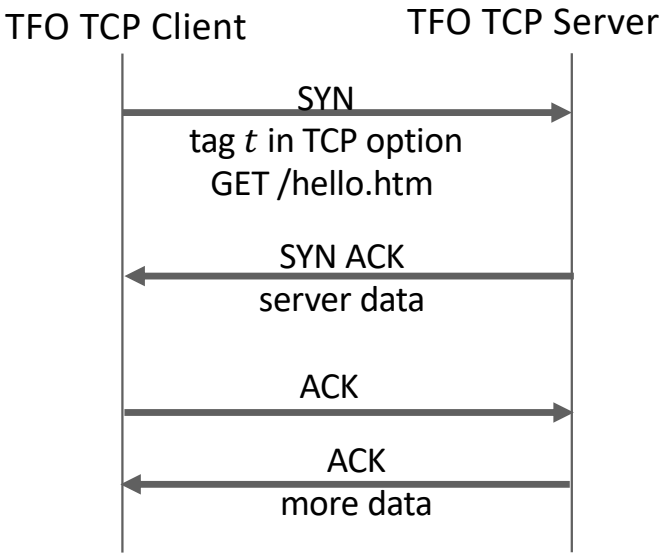
TCP Fast Open (TFO)

Why ? Avoid latency of 3-way handshake when opening repeated connections.

How? In first SYN_ACK, TCP client receives and caches a cookie that contains authentication tag $t = MAC(k, c)$ computed by server with secret key k (unknown to client) and client IP address c.

Client can send data in SYN packet.

When receiving SYN and tag t, server knows that this client is a real one and not spoofed. Server can send data already in SYN-ACK.



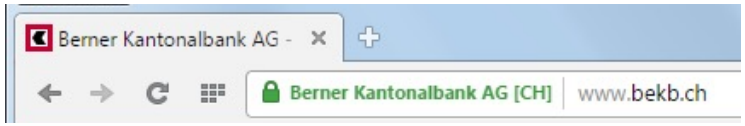
MAC= Message Authentication Code

5. Secure Transport

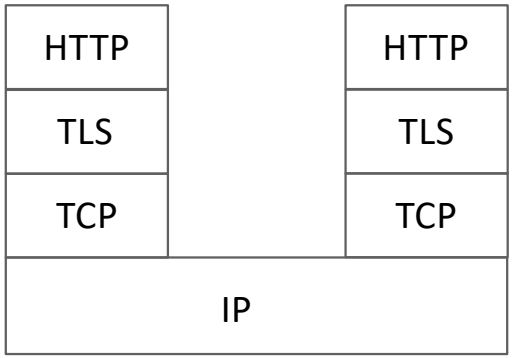
TCP has no security.
Needs to be complemented
with a security layer such as
Transport Layer Security (TLS)
(TLS is in application layer).

TLS adds to TCP:

- Confidentiality: data is encrypted
  with symmetric encryption; using
  secret keys created on the fly for this session
- Authentication: data is protected against forgery
  + identity of end-system is authenticated



http used over TLS and port 443 = https



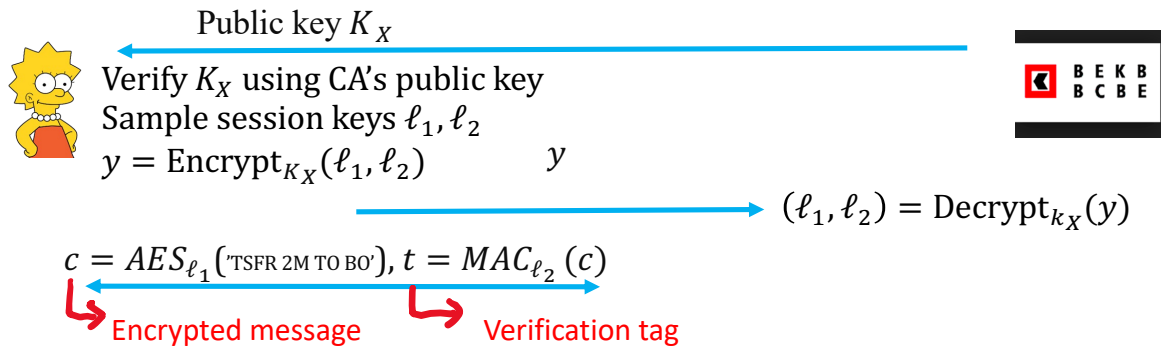
Crypto Background

Symmetric cryptography (e.g. AES) uses a secret key, known only by sender and receiver. Messages are encrypted using the secret key and can (only) be decrypted using the same secret key; this provides confidentiality. Can also be used to authenticate a message by adding a verification tag computed with the secret key, which can be verified using the same secret key. It is very fast but has the problem of key distribution.

Asymmetric cryptography (e.g. RSA) uses two different keys: one can be used for encryption, the other for decryption. One of the keys must be secret (private), the other one is public. The private key cannot be computed from the public key other than by brute-force (in principle). This eases the problem of key distribution but encryption/decryption is computationally intensive.

In all cases, keys must be long enough to resist brute-force attacks today (e.g. 256 bits for AES, 2000 bits for RSA).

TLS uses private/public key pairs + certificate

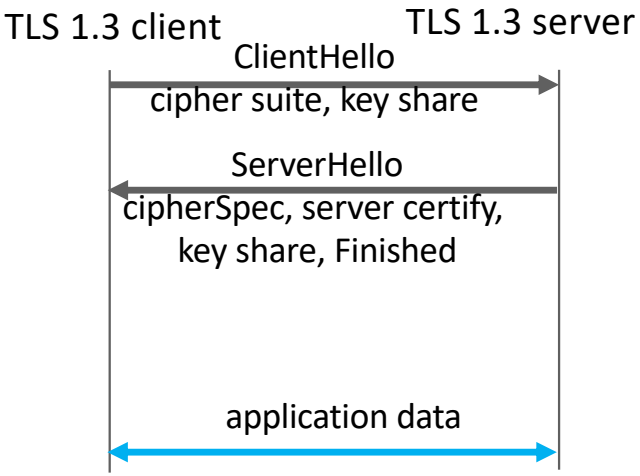


1. Lisa verifies that K_X is indeed the key of bank by using a certificate, which contains public key of bank signed by Certification Authority (CA). Lisa verifies signature of certificate by using CA's public key, pre-installed in Lisa's web browser.
2. Lisa uses public-key of bank to share secret session keys used to encrypt and authenticate the e-banking transaction.
3. Two-way communication uses secret keys

TLS 1.3

Typically uses one handshake before sending data.

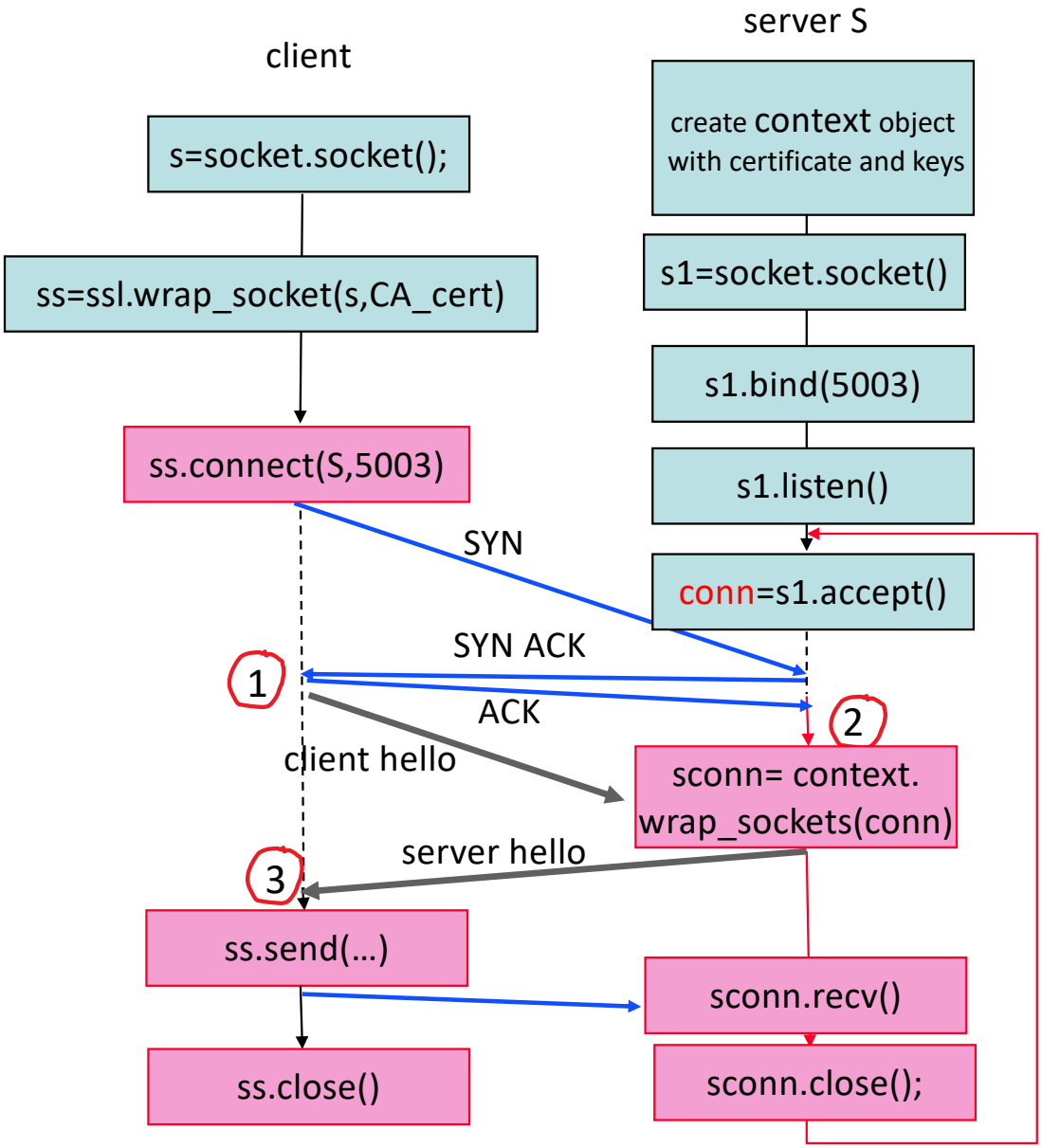
agree on cryptographic suites to be used



Many old cipher suites are no longer secure – important to be sure that TLS software is up-to-date.

TLS Sockets

TLS sockets (also called SSL sockets) are transformed "wrapped" from sockets.



On the client side, the socket s is transformed into a TLS socket using ssl.wrap_socket. This transformation requires the client to give the CA certificate. The connect() method does two things at a time: open the TCP connection and start the TLS handshake.

On the server side, things are different as the TCP socket used for communication is created only after accept().

At point 1, the client has opened the TCP connection and sent the TLS client hello but not yet received the TLS server hello.

At point 2, the server has accepted the TCP connection but not yet started the TLS handshake. It can continue with the TLS handshake only after wrapping the new socket conn into a TLS socket sconn. This requires the server to provide its pair of keys and its certificate.

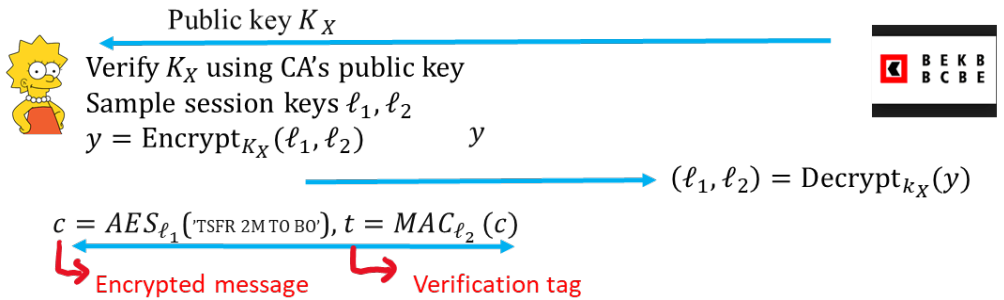
The client can send data only when the handshake is completed (point 3).

With https/TLS1.3, how many RTTs are required before data transfer can occur?

A. 1
B. 2
C. 3
D. 4
E. 0
F. من نمی دانم

A Digital Certificate for BEKB Contains…

A. The public key of BEKB
B. The identity of BEKB (official name as of Registre du Commerce)
C. The public key of the issueing CA
D. A and B
E. A and C
F. B and C
G. All
H. None
I. Nu știu



6. Error Recovery

We have seen *how* TCP repairs losses

We now discuss *why* this is so, and sometimes why it is not so

The Layered Model Transforms Errors into Packet Losses

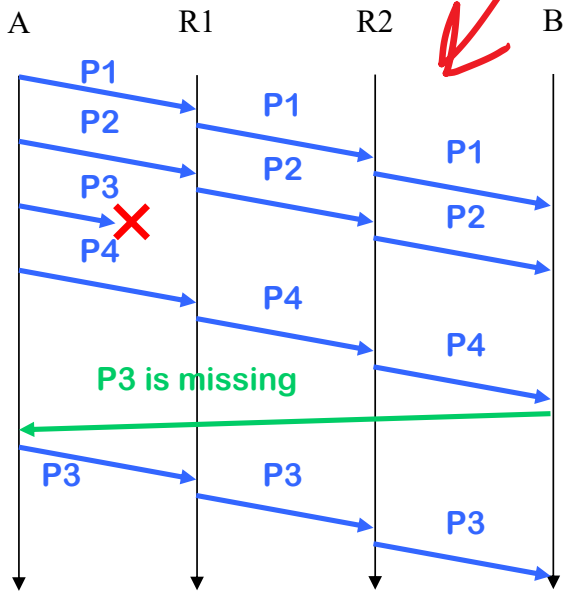
Packet losses occur due to

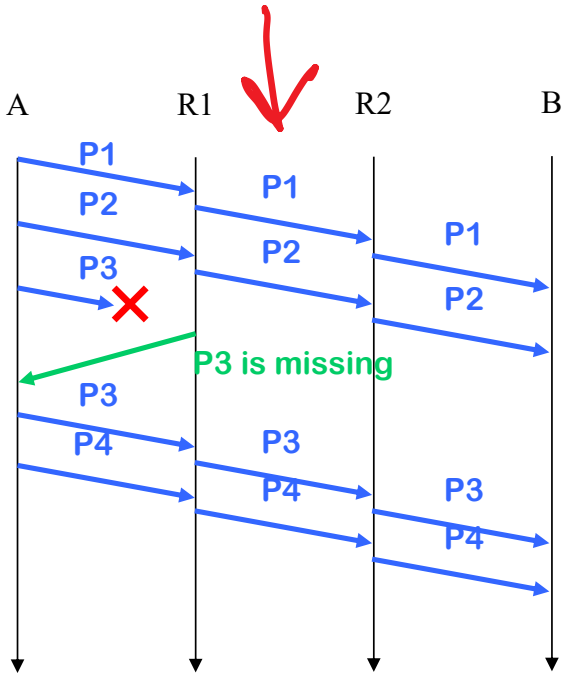
- error detection by MAC
- *buffer* overflow in bridges and routers
- Other exceptional errors may occur too

Therefore, packet losses must be repaired.

This can be done either

- *end to end* : host A sends 10 packets to host B. B verifies if all packets are received and asks for A to send again the missing ones.
- or hop by hop



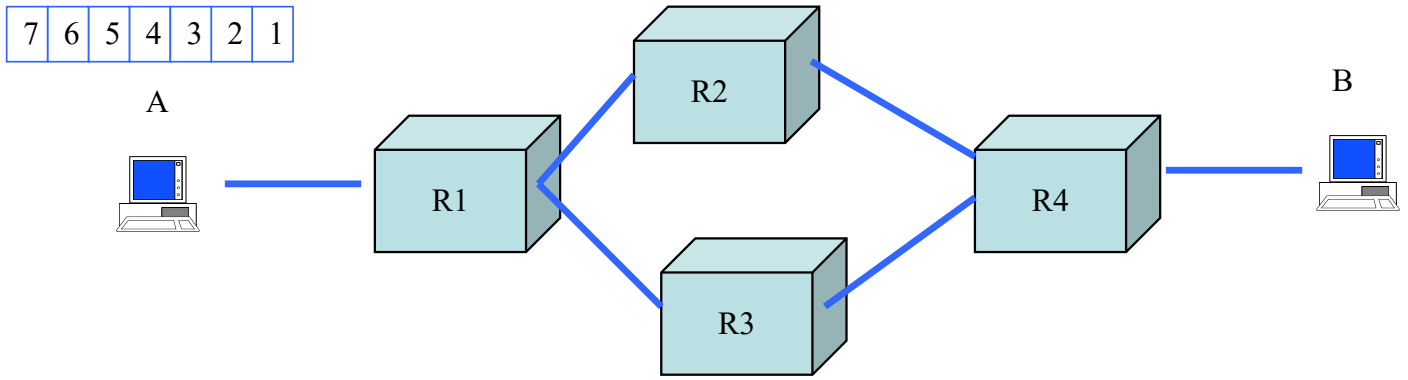


The Case for End-to-end Error Recovery

The end-to-end philosophy of the internet says: keep intermediate systems as simple as possible

IP packets may follow parallel paths, this is incompatible with hop-by-hop recovery.

- R2 sees only 3 out of 7 packets but should not ask R1 for re-transmisison



The Case for Hop-By-Hop Error Recovery

There are also arguments in favour of hop-by-hop strategy. To understand them, we will use the following result.

Capacity of erasure channel: consider a channel with bit rate R that either delivers correct packets or loses them. Assume the loss process is stationary, such that the packet loss rate is $p \in [0\,;1]$. The capacity is $R(1-p)$ packets/sec.

This means in practice that, for example, over a link at 10Mb/s that has a packet loss rate of 10% we can transmit up to 9 Mb/s of useful data.

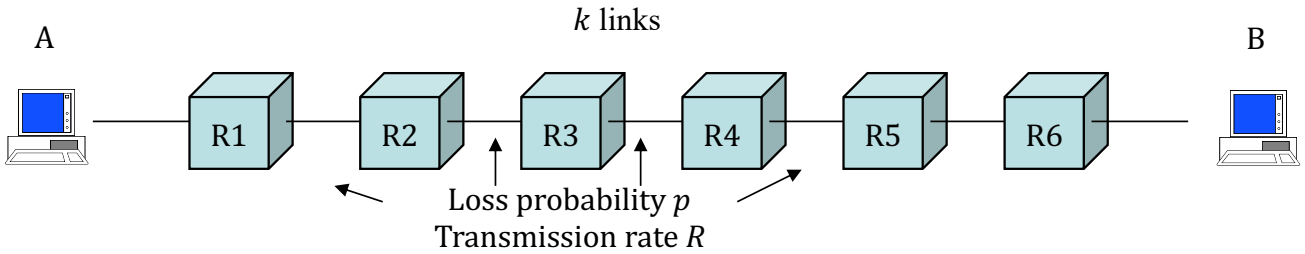
Furthermore, this capacity is obtained by a scheme (such as TCP) which retransmits lost packets.

The Capacity of the End-to-End Path

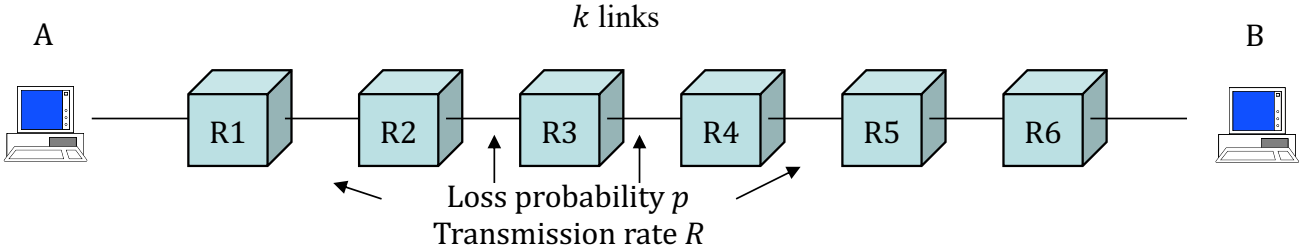
We can now compute the capacity of an end-to-end path with both error recovery strategies.

Assumptions: same packet loss rate p on k links; same nominal bit rate R. Losses are independent.

Q. compute the capacity with end-to-end and with hop by hop error recovery.



The capacity C_1 with hop-by-hop error recovery is …



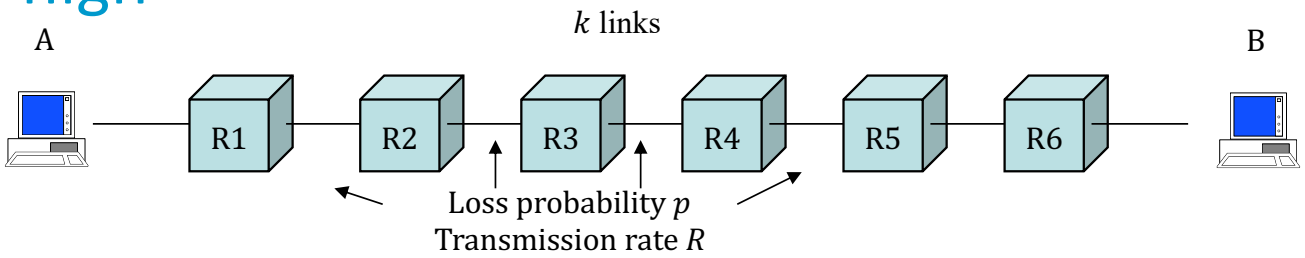
A. $C_1 = R(1-p)^k$

B. $C_1 = R(1-p)$

C. $C_1 = R(1-kp)$

D. Não sei

End-to-end Error Recovery is Inefficient when Packet Error Rate is high



k	Packet loss rate	C_1 (end-to-end)	C_2 (hop-by-hop)
10	0.05	0.6 R	0.95 R
10	0.0001	0.9990 R	0.9999 R

Q. How can the conflicting arguments for and against hop-by-hop error recovery be reconciled ?

Where is Error Recovery located in the TCP/IP architecture ?

The TCP/IP architecture assumes that

1. The MAC layer provides error—free packets to the network layer
2. The packet loss rate at the MAC layer (between two routers, or between a router and a host) must be made very small. It is the job of the MAC layer to achieve this.
3. Error recovery must also be implemented end-to-end.

Thus, packet losses are repaired:

At the MAC layer on lossy channels (wireless)
WiFi repairs losses with a repetition mechanism similar to TCP but simpler, window = 1 packet

In the end systems (transport layer by TCP or application layer if UDP is used).

Conclusion

The transport layer in TCP/IP exists in two flavours

- reliable and stream oriented : TCP
- unreliable and message based: UDP

TCP uses : sliding window and selective repeat; window flow control; congestion control – see later

TCP offers a strict streaming service and requires 3 way handshake

Other transport layer protocols exist but their use is marginal: e.g. SCTP (reliable + message based)

Some application layer frameworks are a substitute to TCP for some applications: e.g. QUIC (reliable and “message” based – see Appli), websockets (see lab).