Internet

Technology and Applications

- EITF25 -

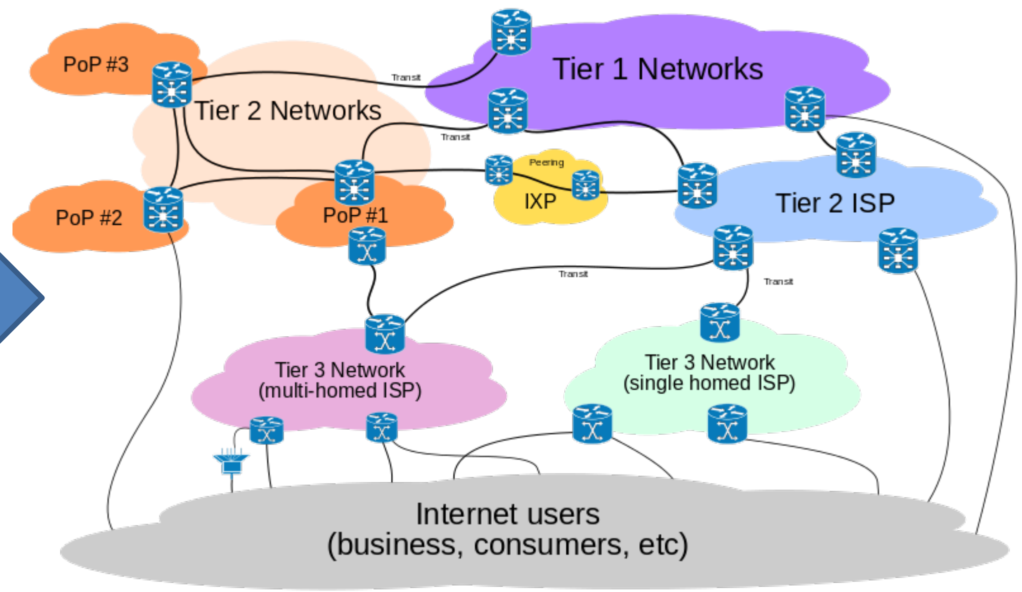
Summary Lecture

Kaan Bür, 2015

kaan.bur@eit.lth.se

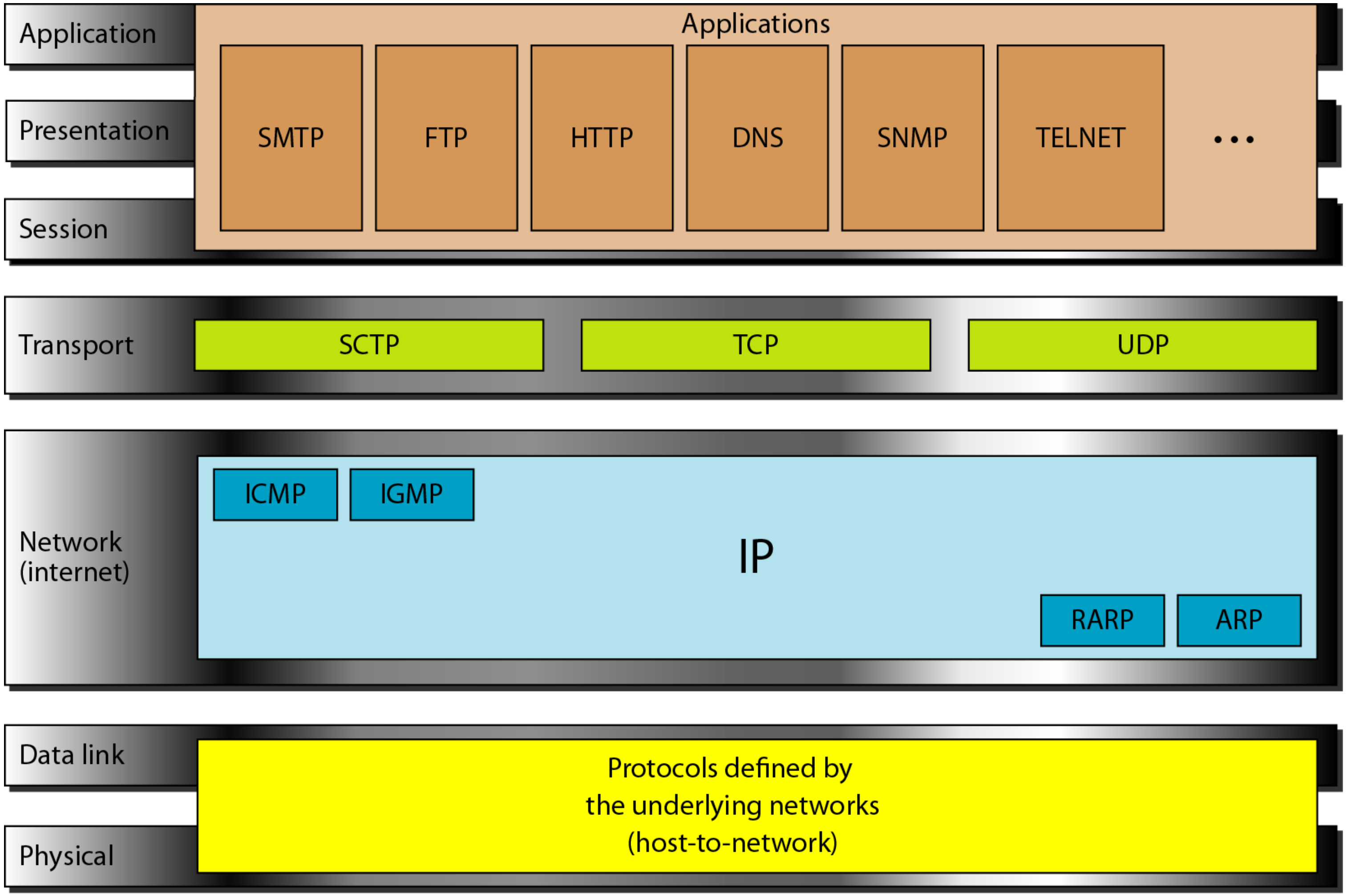
Room E:3130 (Monday, Friday)

What is Internet?



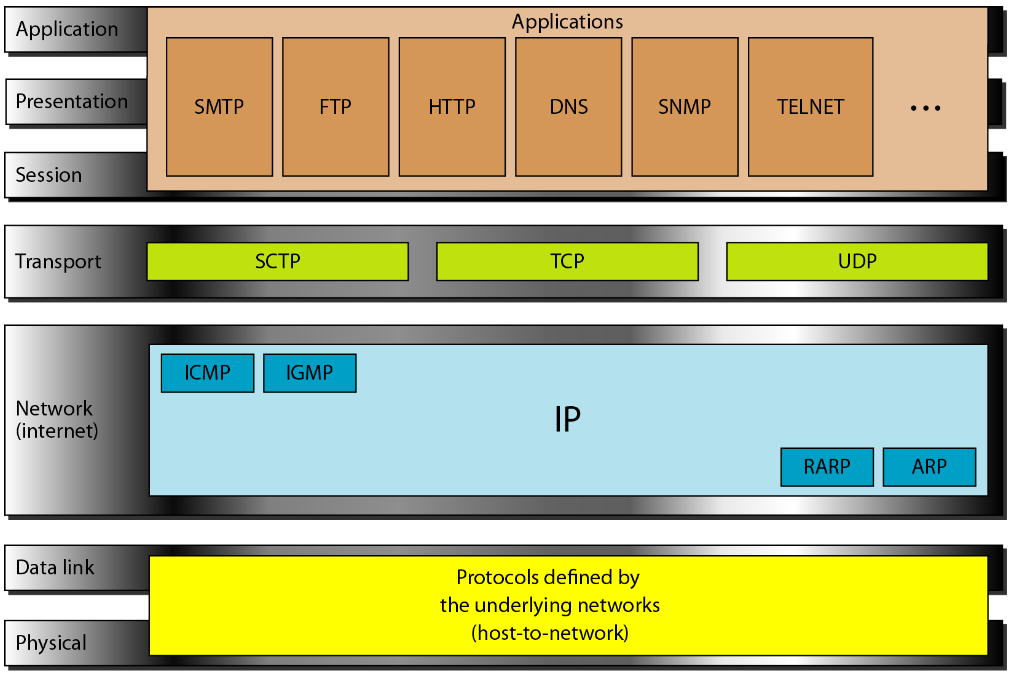
TCP/IP model

- Developed by DARPA, 1970~

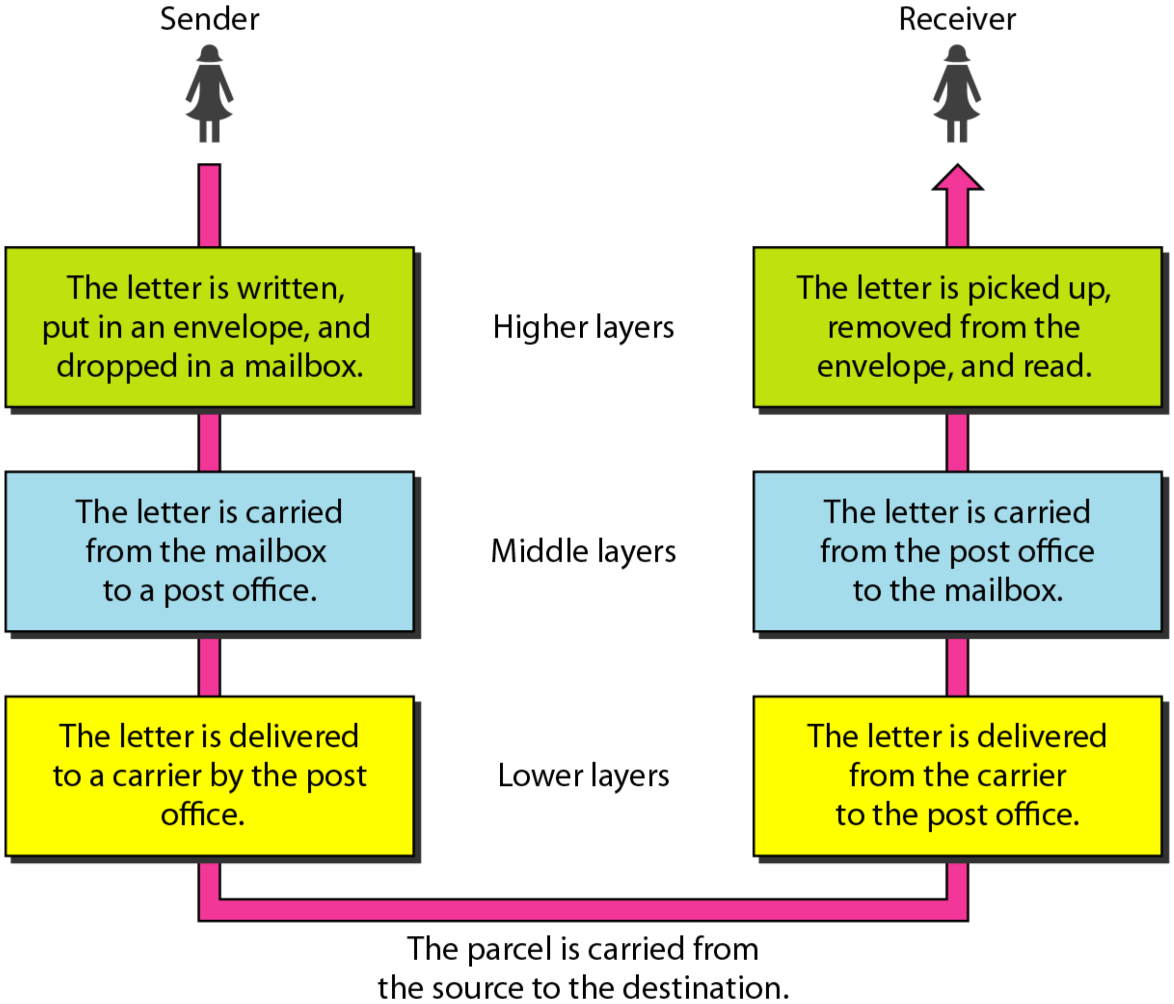


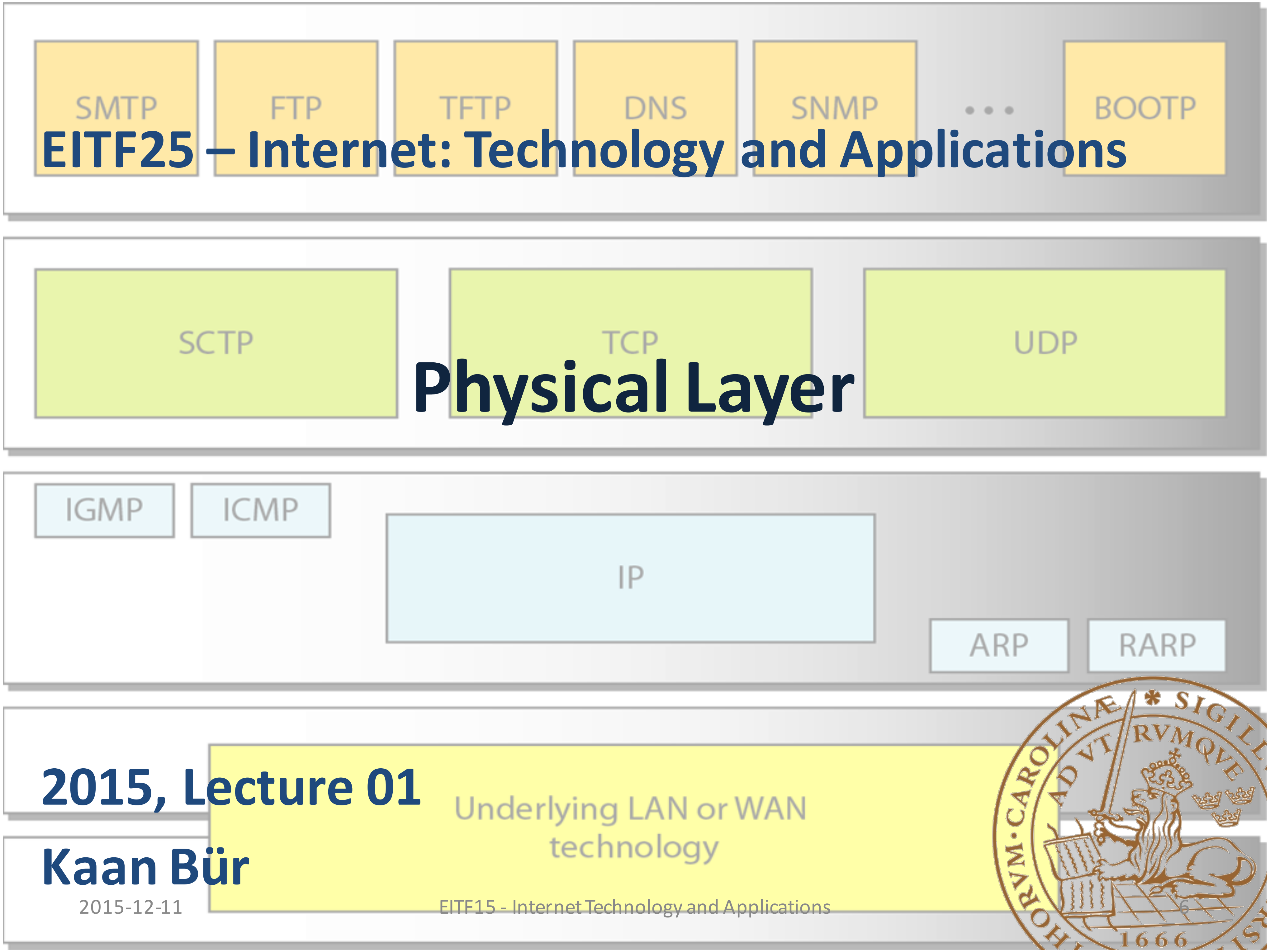
A bottom-up approach

- Principles of digital communications
  - From electrical signals to bits to packets
- Using the physical infrastructure
  - Network access
- Finding your way
  - Addressing, routing
- Making use of it all
  - Applications



Layer concept





EITF25 – Internet: Technology and Applications

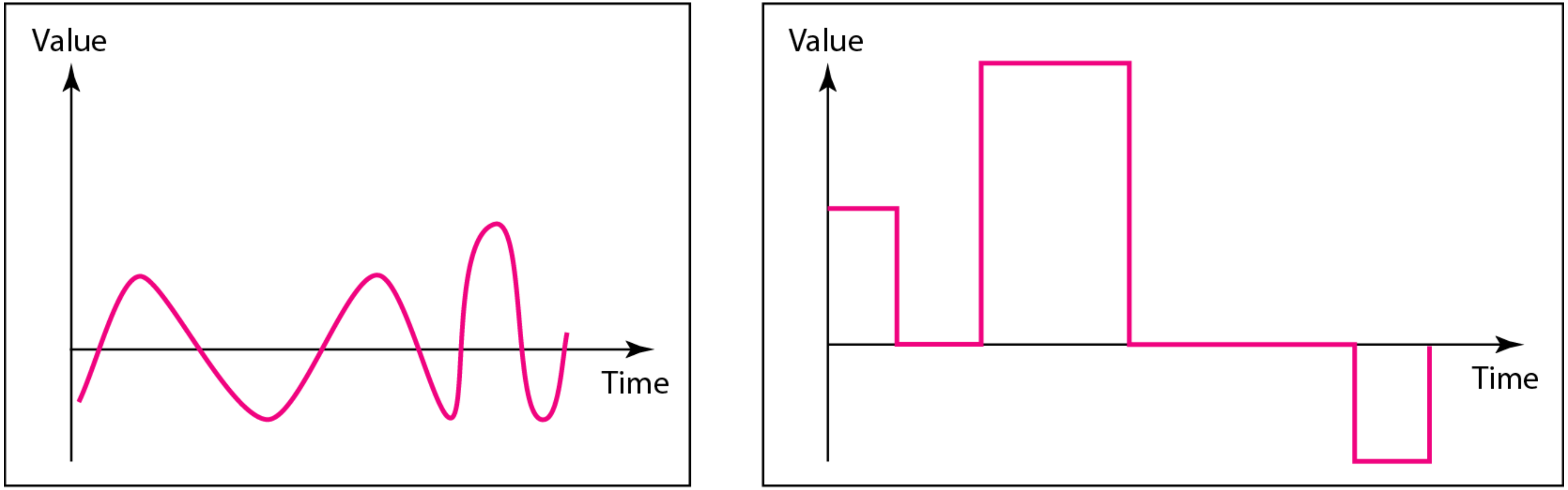
Physical Layer

2015, Lecture 01

Kaan Bür

Analog vs Digital

- Analog → continuous
- Digital → discrete



a. Analog signal

b. Digital signal

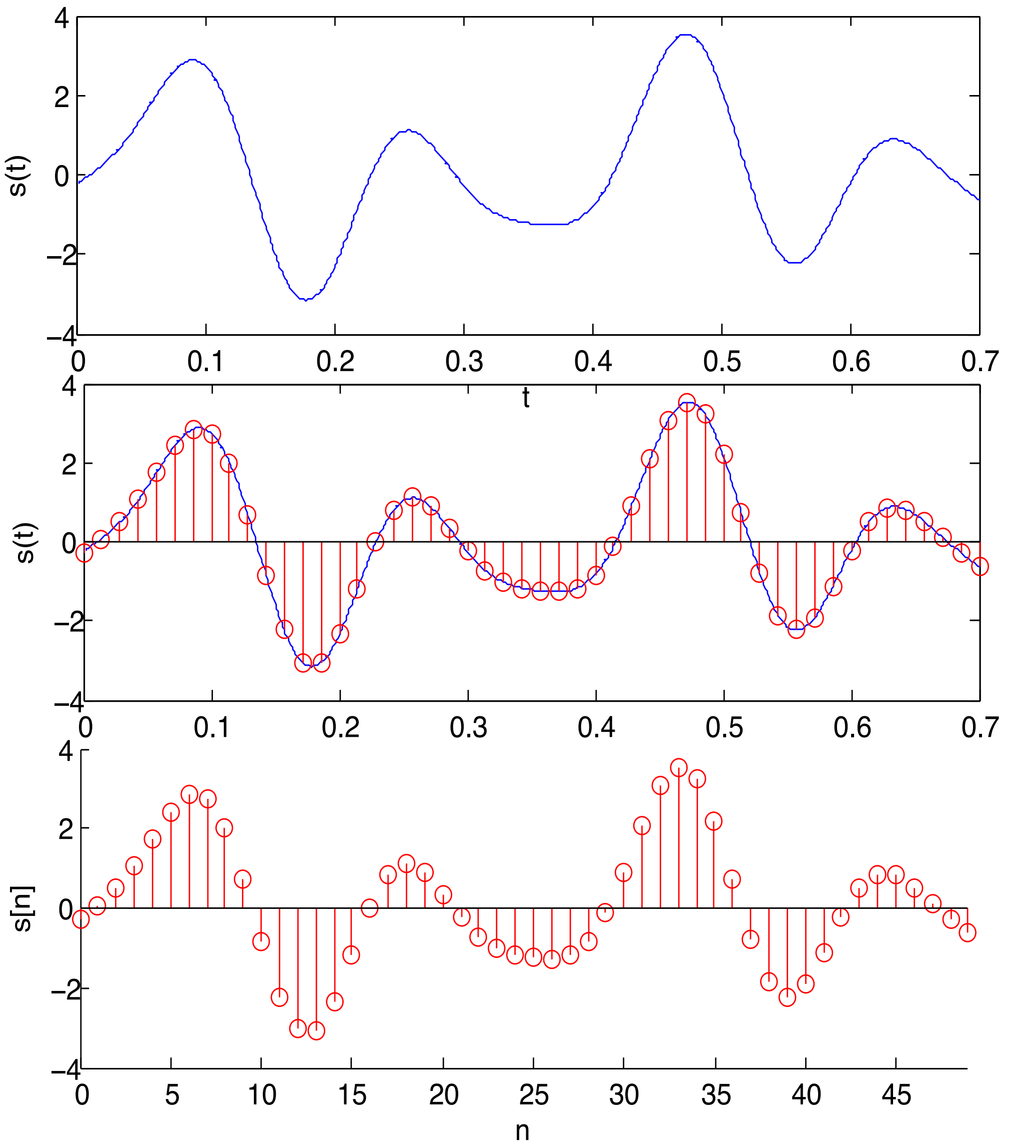
Digitalization of analog signals

- Performed in three steps:

1. Sampling
   - Discretization in time
2. Quantization
   - Discretization in amplitude
3. Encoding
   - Binary representation of amplitude levels

Sampling

- The process of discretizing the time of a continuous function.



Nyquist Sampling Theorem

- If *s(t)* is a band limited signal with highest frequency component F_{max}, then *s(t)* is uniquely determined by the samples $s_n = s(nT)$ if and only if

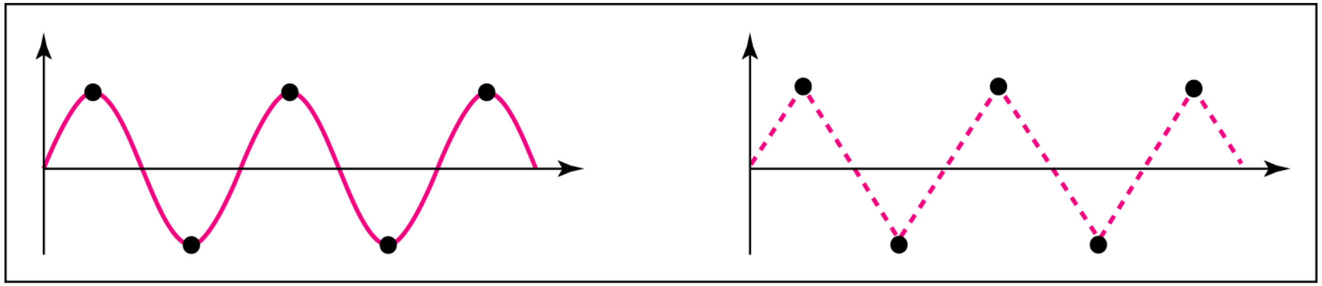
$$F_s = \frac{1}{T} \geq 2F_{\max}$$

- The signal can be reconstructed with

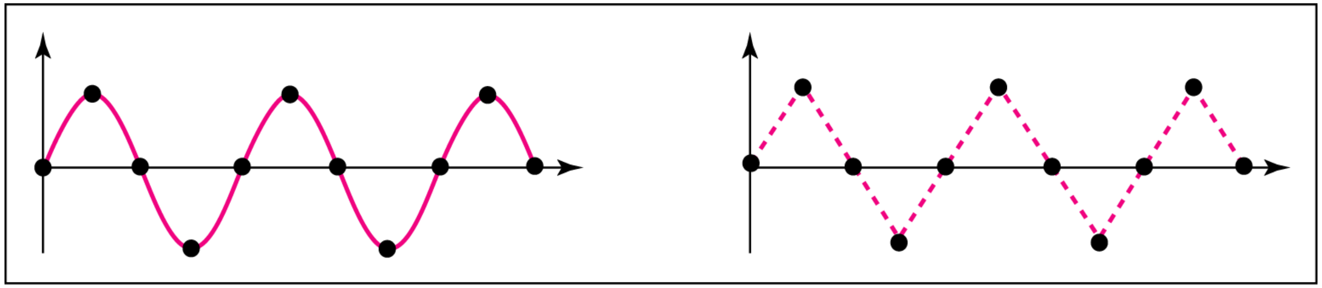
$$s(t) = \sum_n s_n \operatorname{sin}c\left(\frac{t - nT}{T}\right)$$

- F_{max} is the Nyquist frequency and F_s the Nyquist rate

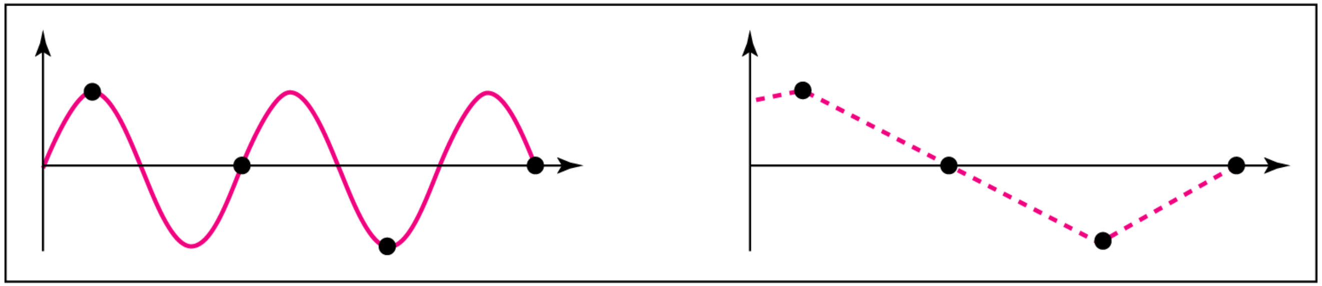
How sampling rate affects the result



a. Nyquist rate sampling: $f_s = 2f$



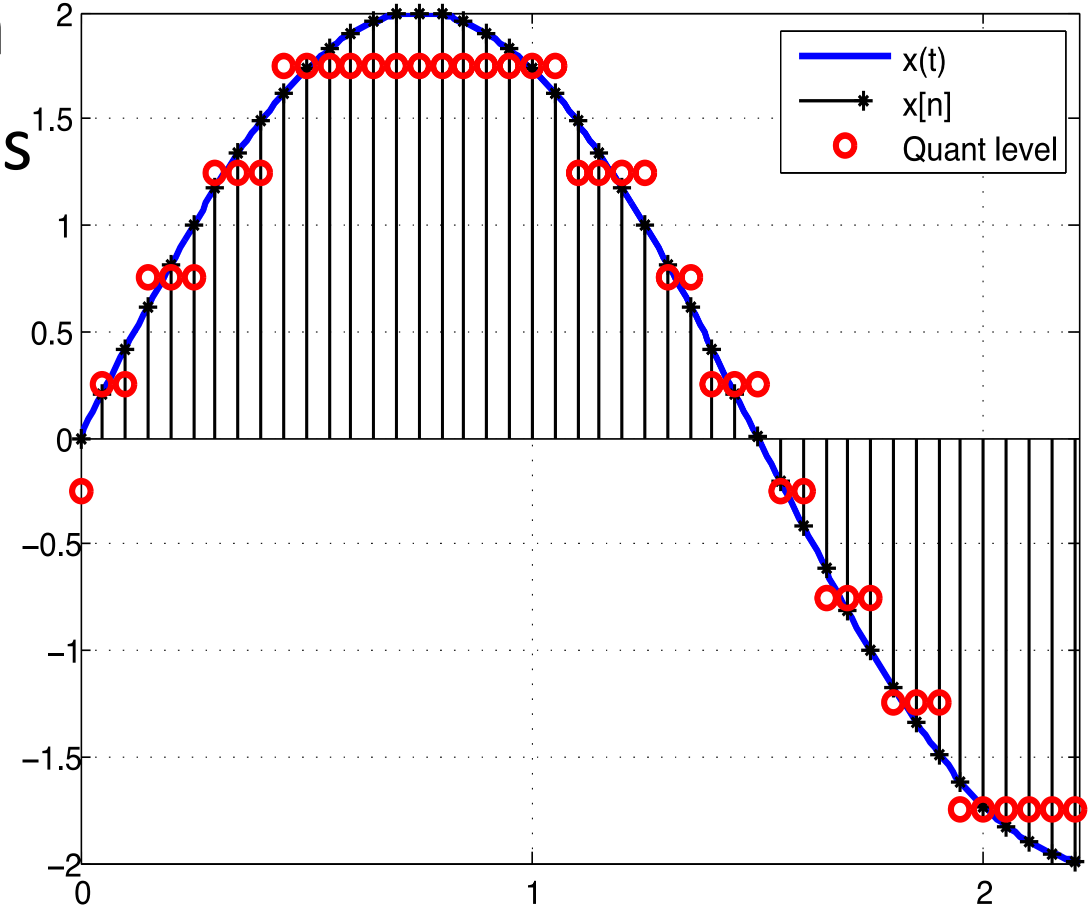
b. Oversampling: $f_s = 4f$



c. Undersampling: $f_s = f$

Quantization

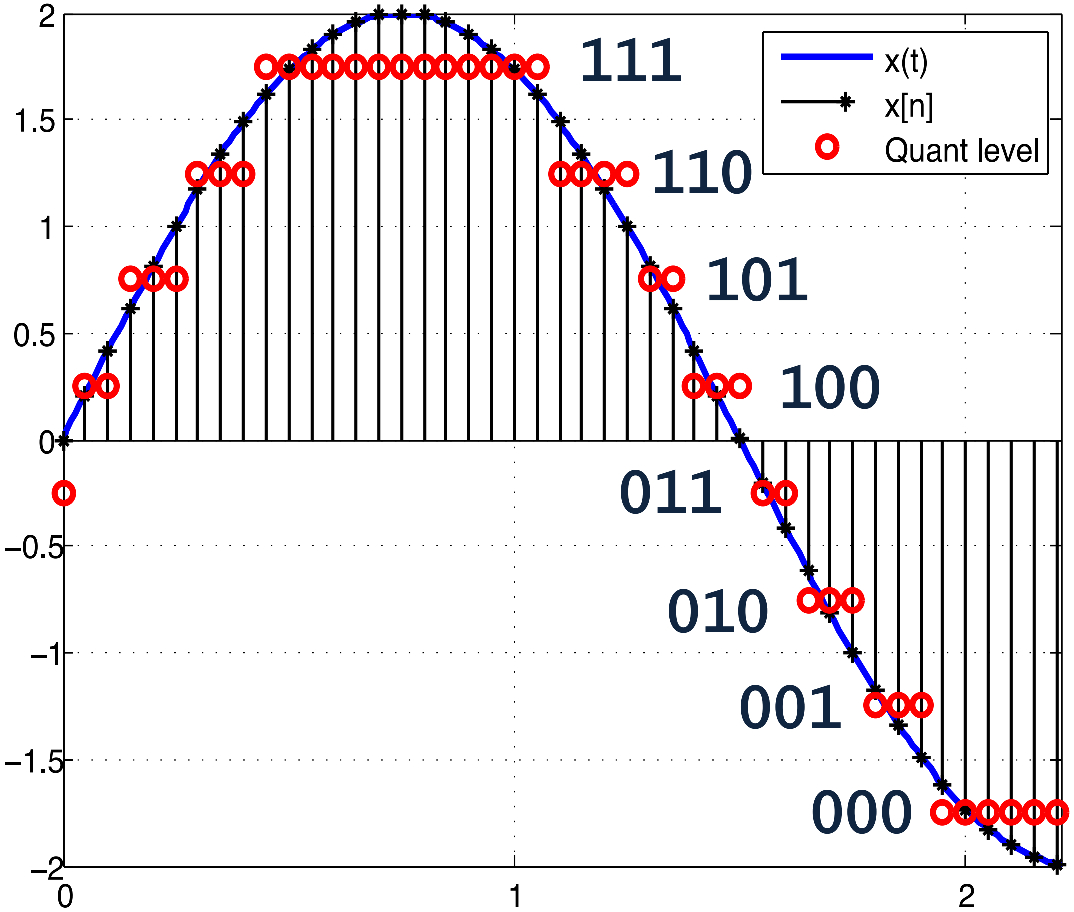
- Linear Quantization
  - 2^N equidistant levels
  - Represent sample with N bits



- Telephony
  - N=8 → 256 levels
- CD
  - N=16 → 65 536 levels

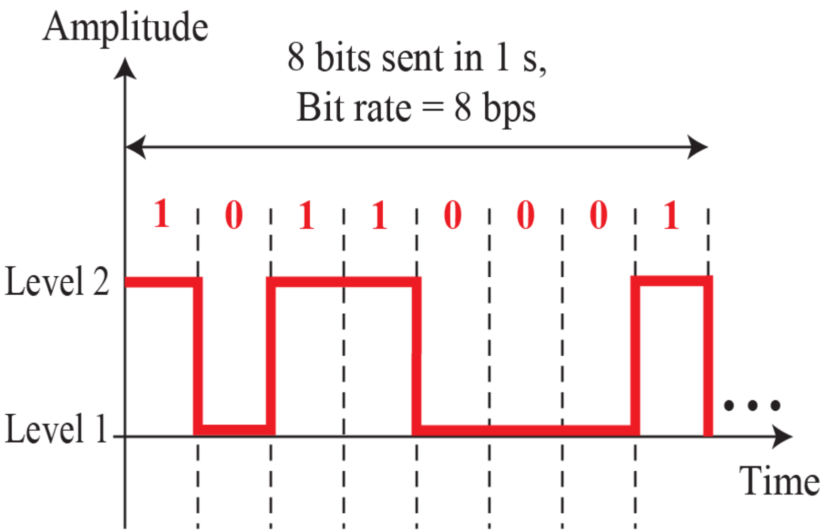
Encoding

- Representation of quantized samples in bits

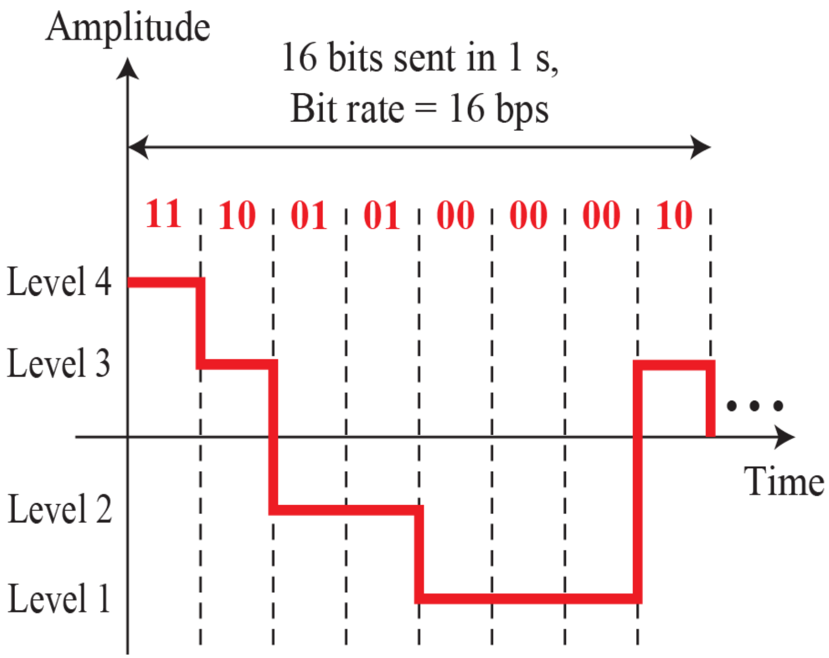


Digital signal transmission

- Signals coded by changes in voltage amplitude



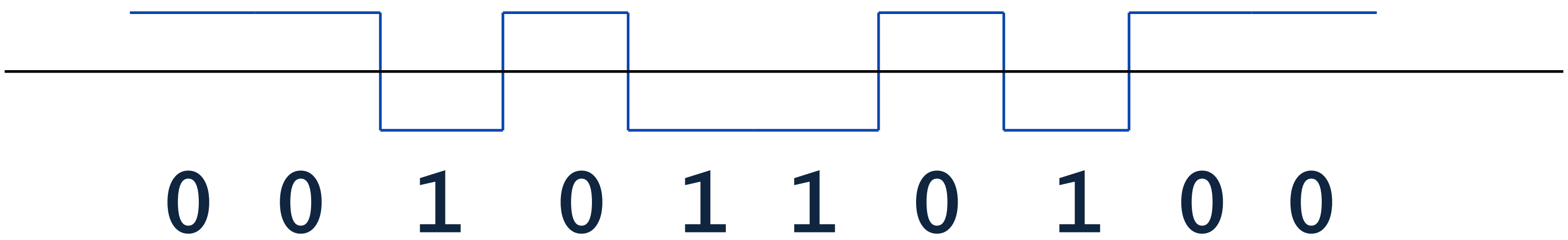
a. A digital signal with two levels



b. A digital signal with four levels

Non-Return-to-Zero (NRZ-L)

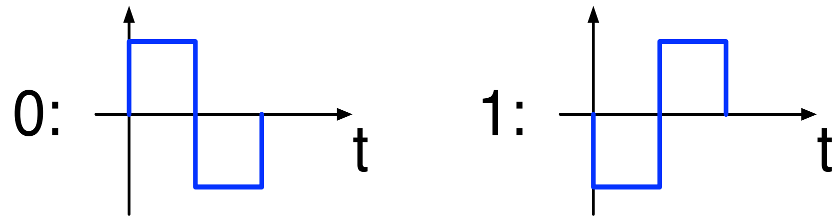
- 0 = high voltage amplitude
- 1 = low voltage amplitude

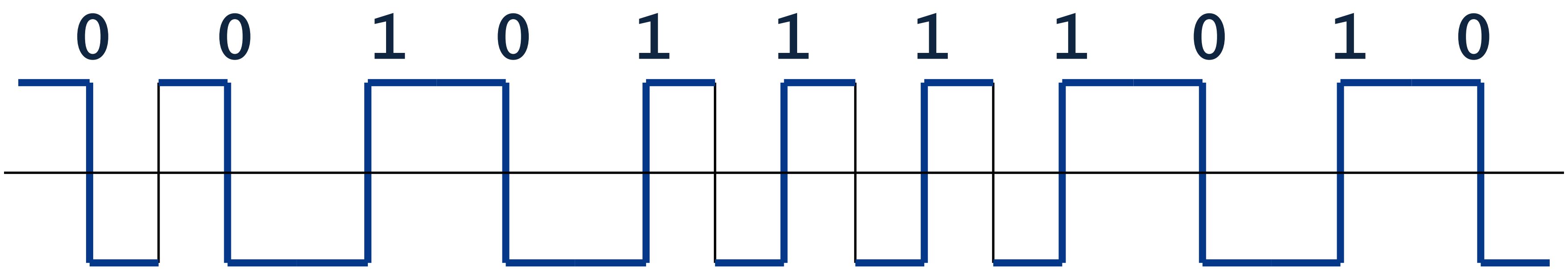


- Twice as bandwith-efficient than RZ
- Synchronisation problem

Manchester Coding

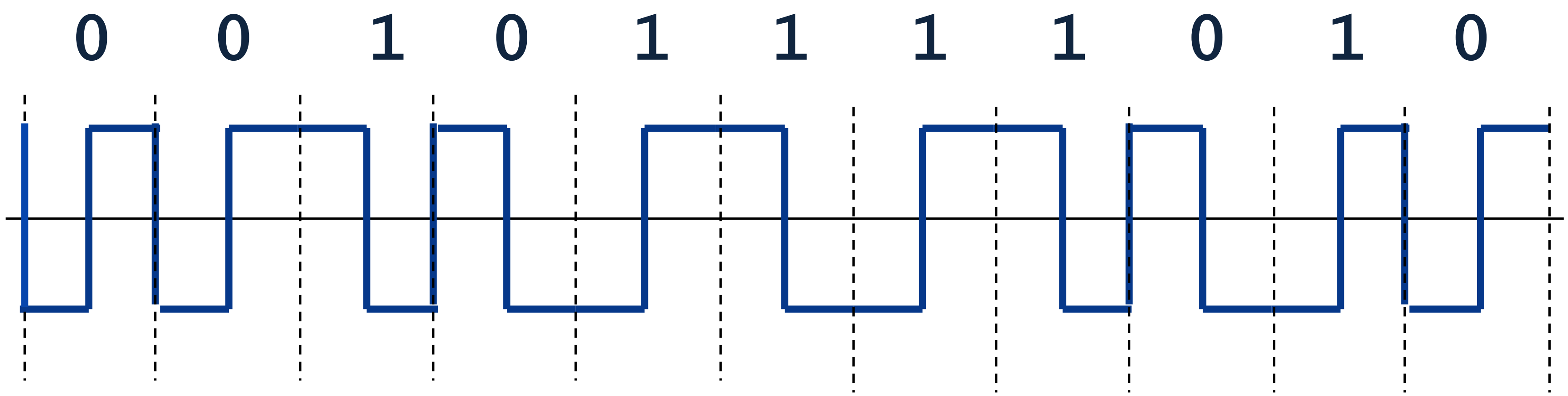
- Combines NRZ with a clock pulse





Differential Manchester

- 0 = Inversion at the beginning of the bit
- 1 = No inversion at the beginning of the bit



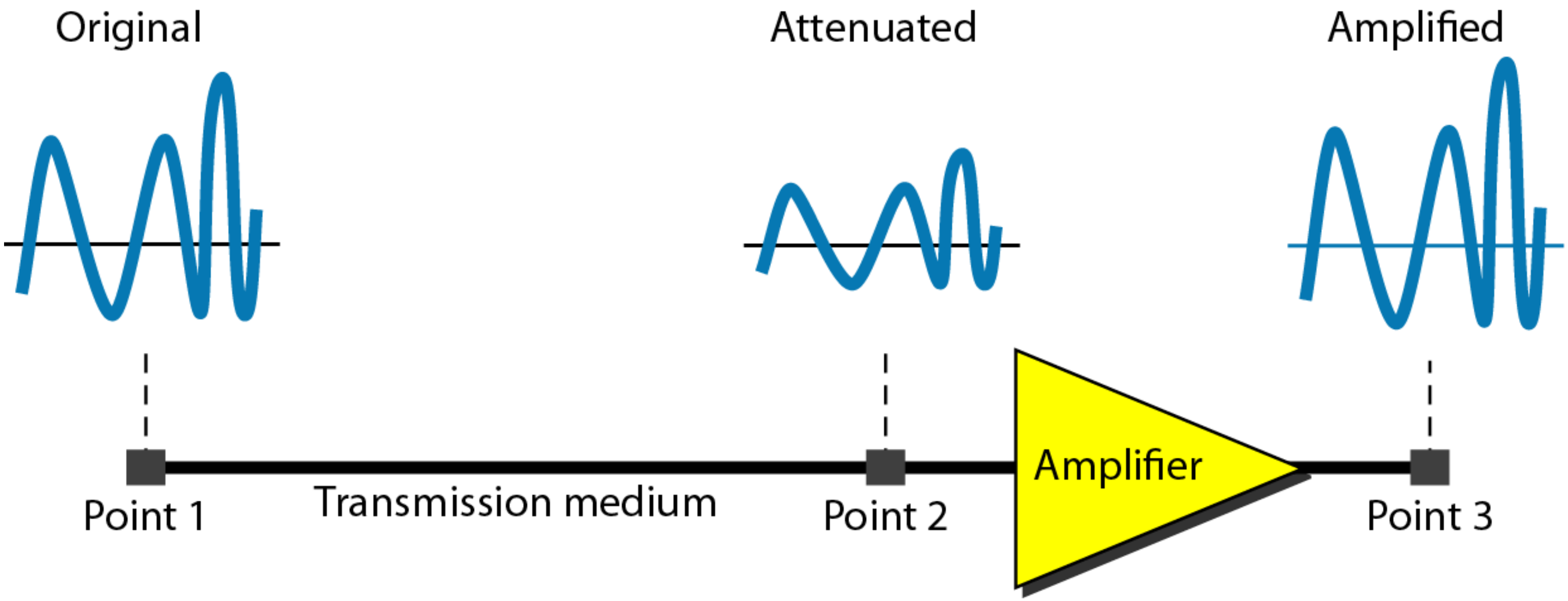
Transmission impairment

- When a signal travels on a link, it deteriorates due to transmission impairment.
  - Attenuation
  - Distortion
  - Noise
- Digital: repeaters vs. Analog: amplifiers

$$\text{Signal-to-noise ratio (SNR)} = \frac{\text{Average signal power}}{\text{Average noise power}}$$

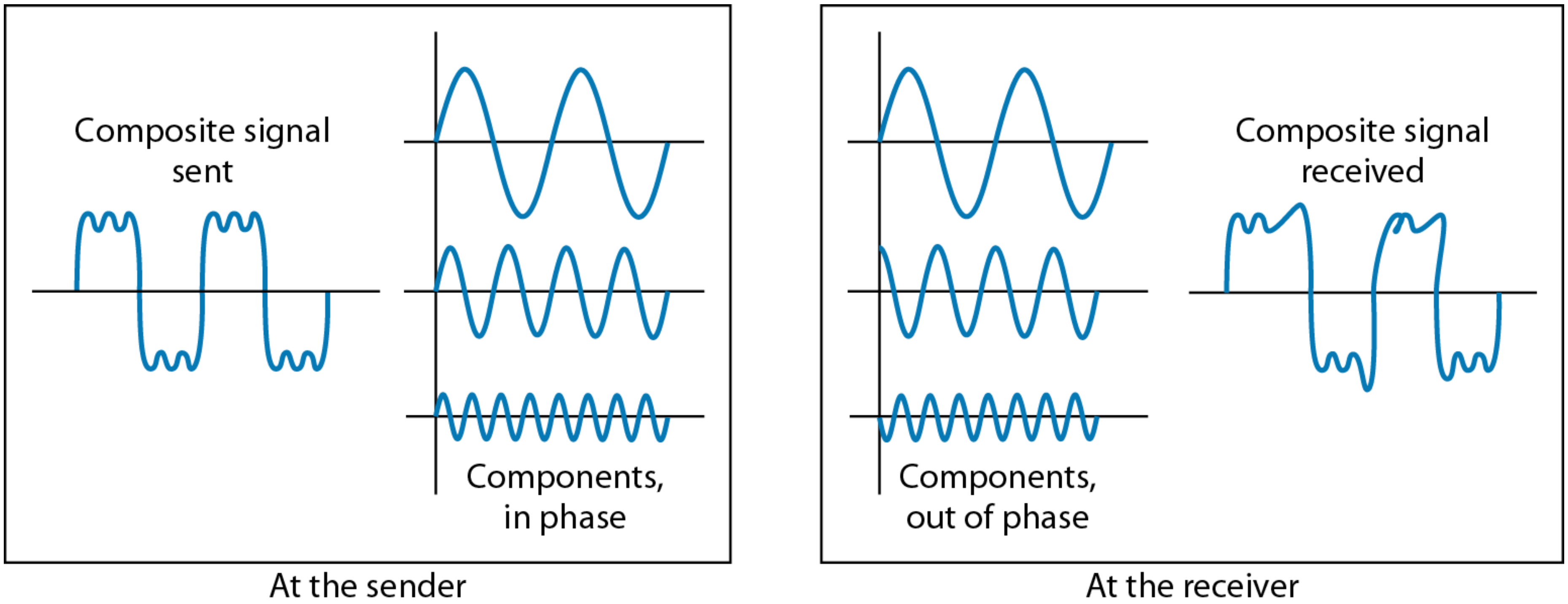
Attenuation

- Loss of energy



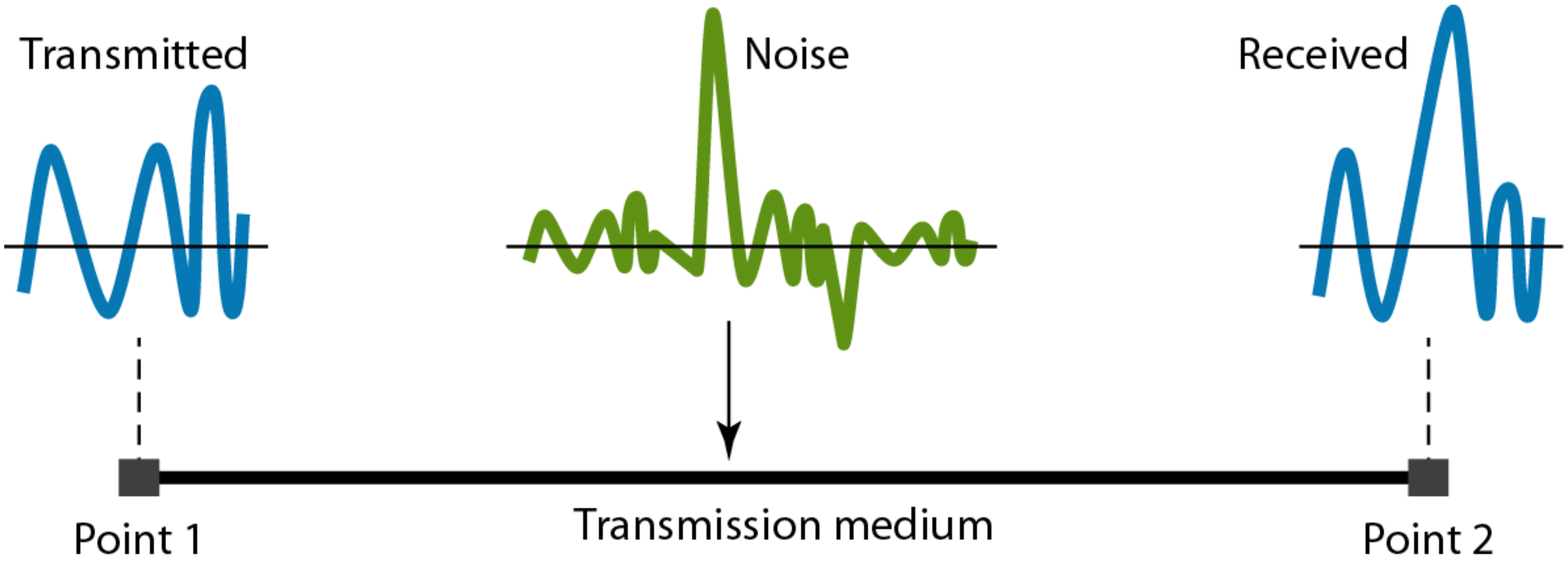
Distortion

- Change in signal shape due to differences in propagation delay



Noise

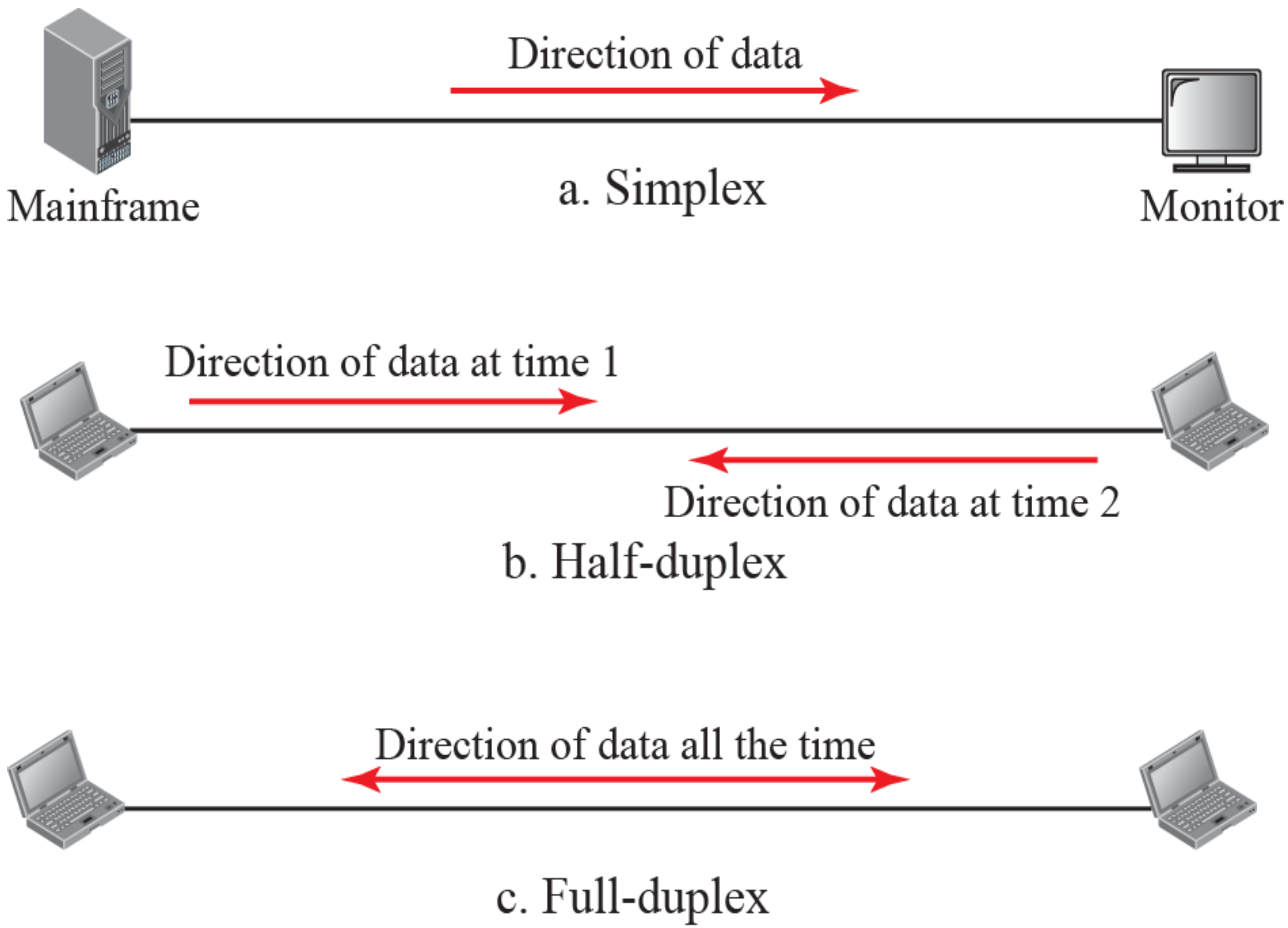
- Corruption due to e.g. thermal noise (a.k.a. white noise) or crosstalk



Digital transmission

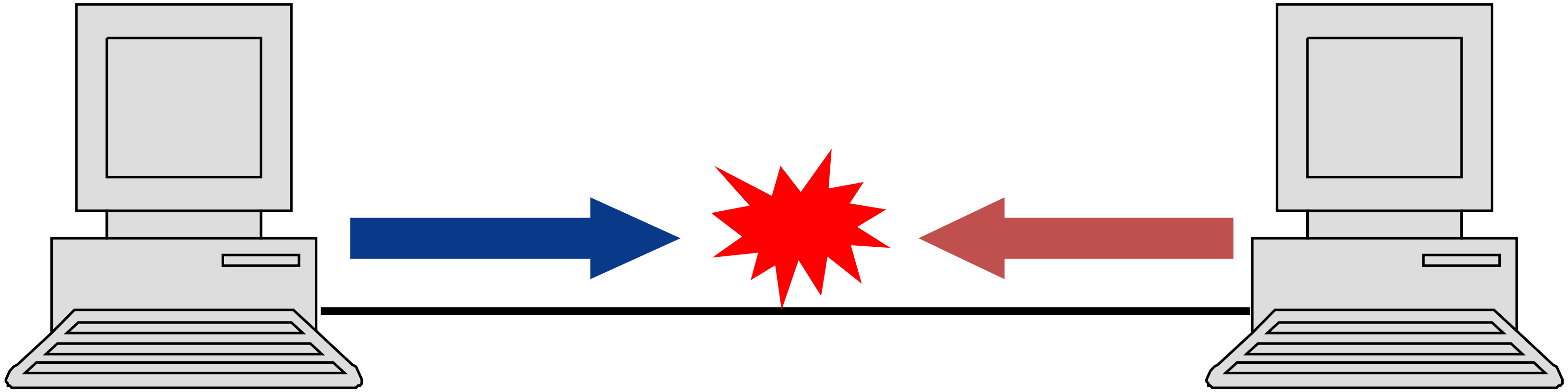
- Preferred method today
  - Data mostly digital
  - Repeaters better than amplifiers
  - Digital multiplexing easier than analog
  - Security implementations easier

Data flow concepts



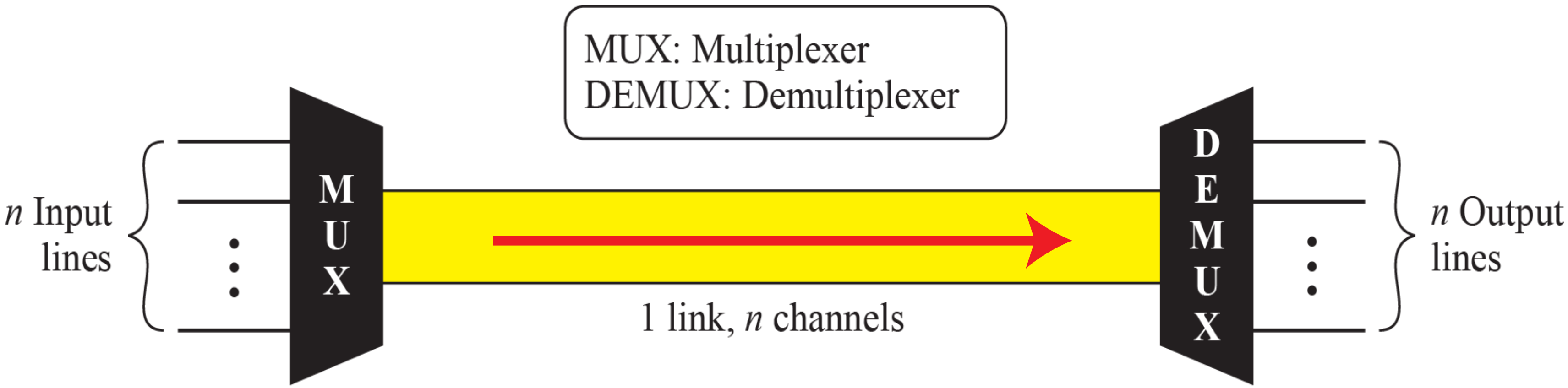
Multiplexing

- Why?
  - Two computers transmitting data on a link cannot do this simultaneously on the same frequencies with the same coding scheme.



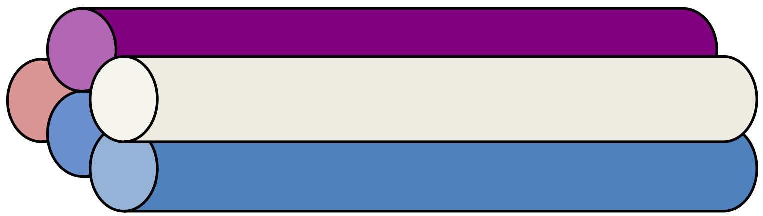
Multiplexing of links

- Physical links need to be shared.
- They are divided into several channels.



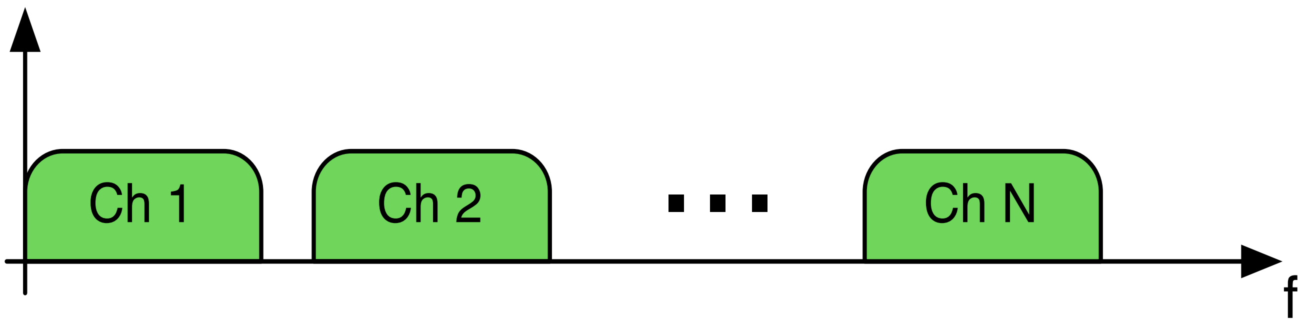
Space-Division Multiplexing (SDM)

- Used in fibre-optic cables
- Each channel uses one optical fibre.



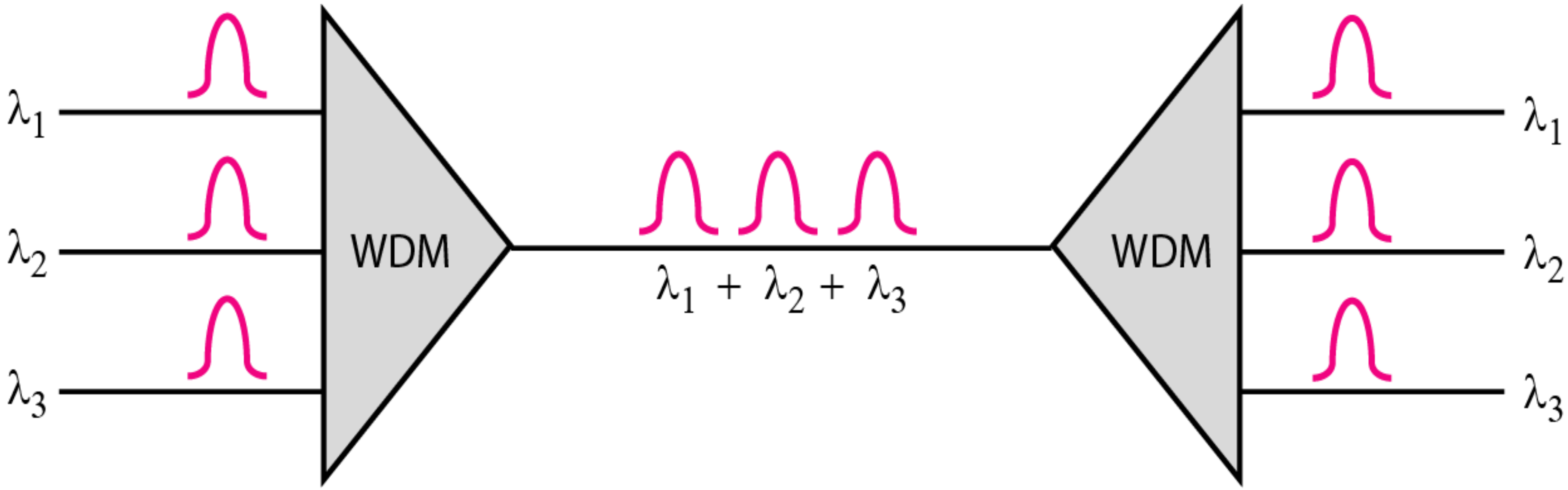
Frequency-Division Multiplexing (FDM)

- Analog multiplexing technique
- Physical link divided into frequency bands
- Each channel uses a unique carrier frequency.



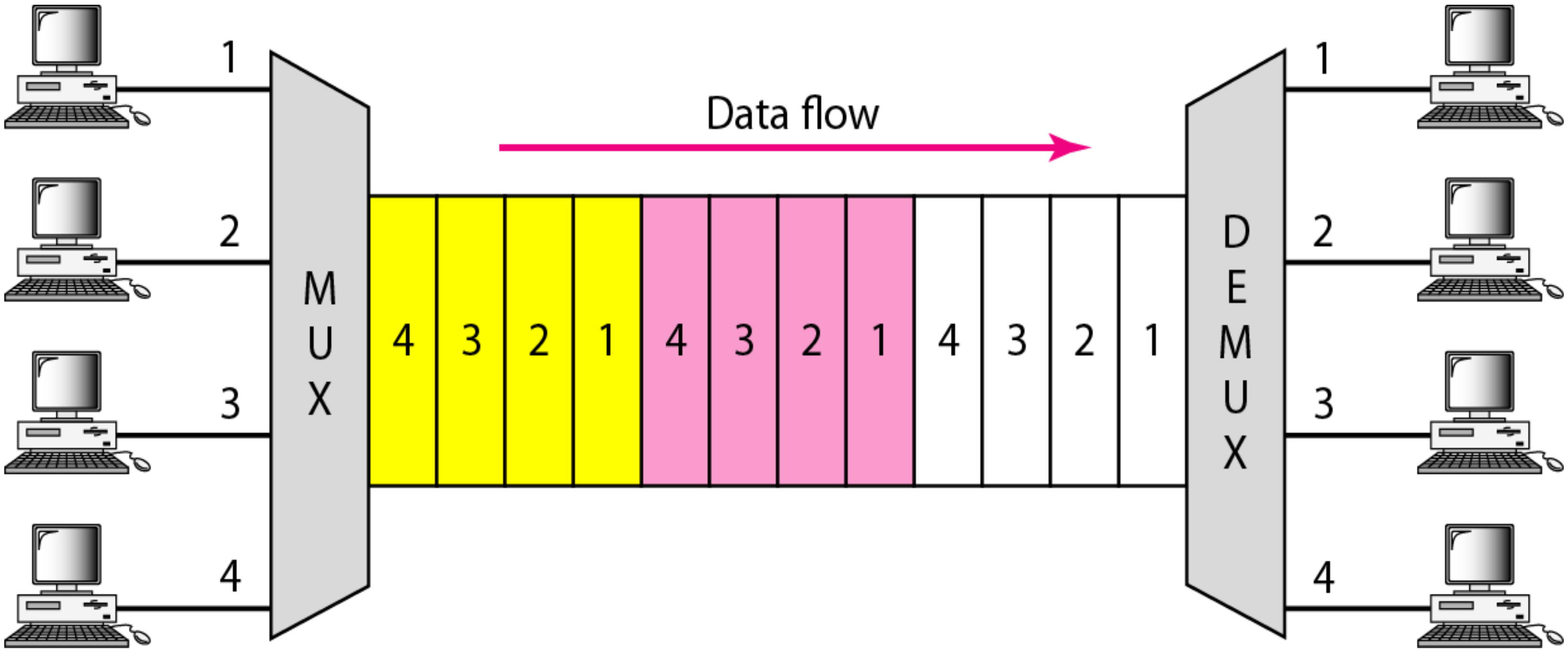
Wavelength-Division Multiplexing (WDM)

- Analog multiplexing technique
- Combines optical signals



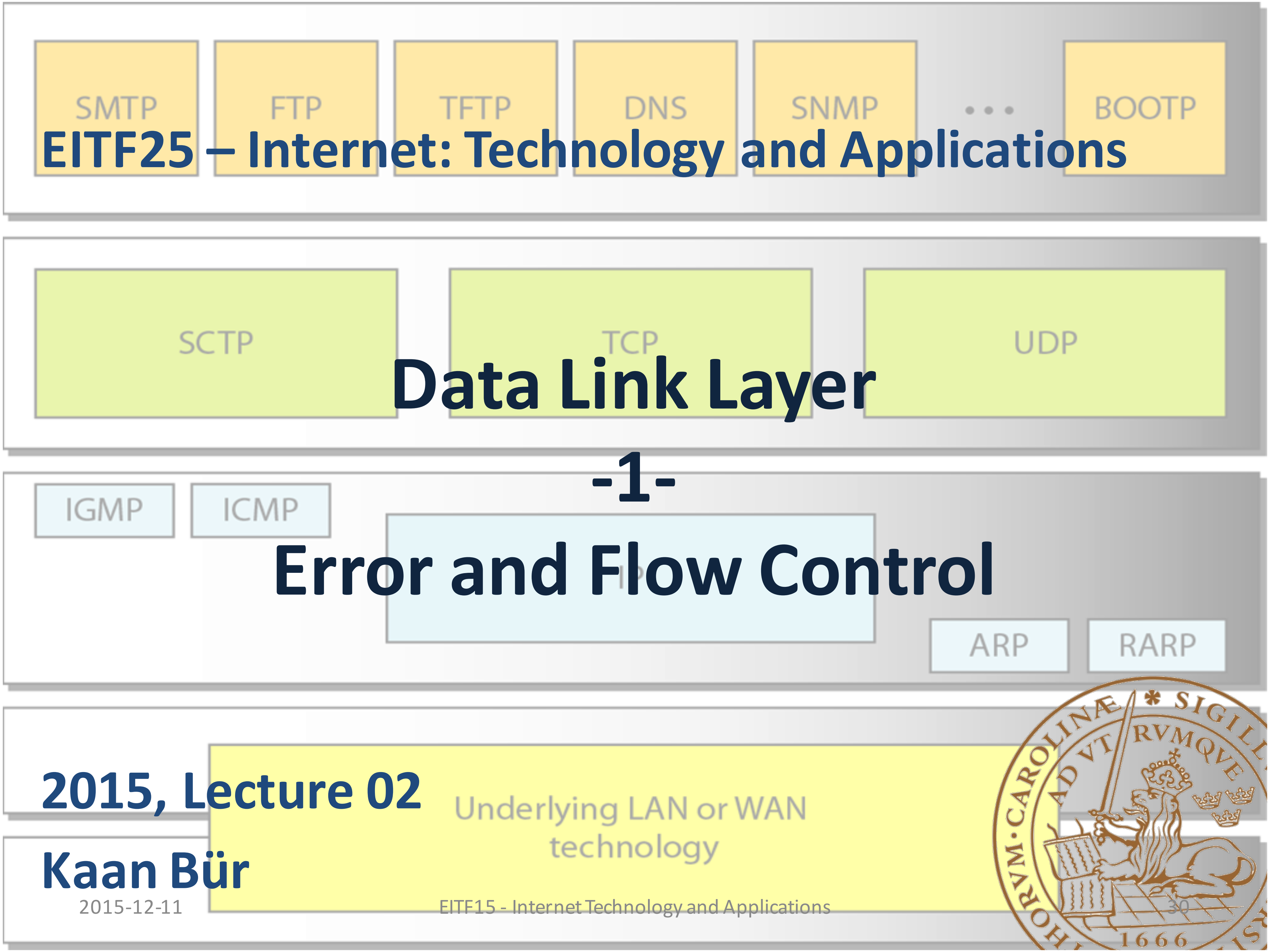
Time-Division Multiplexing (TDM)

- Digital multiplexing technique
- Each channel occupies a time slot on the link.



EITF25 – Internet: Technology and Applications

Data Link Layer
-1-
Error and Flow Control



2015, Lecture 02

Kaan Bür

Data Link Layer

- Medium Access Control
  - Access to network
- Logical Link Control
  - Node-to-node error and flow control

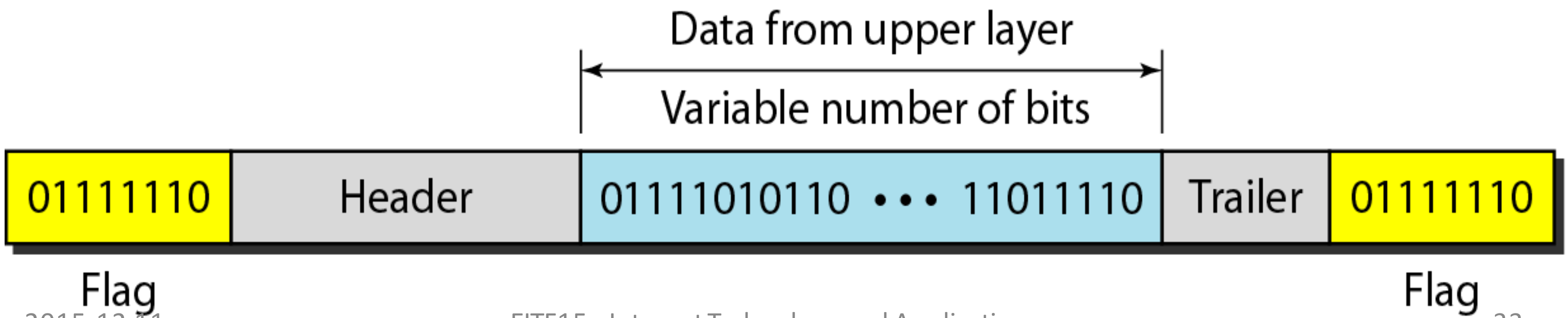
Link layer protocols

Link layer protocols

- Error detection
  – All errors must be detected
- Error correction
  – Receiver must get correct data
- Flow control
  – Receiver must not be overloaded

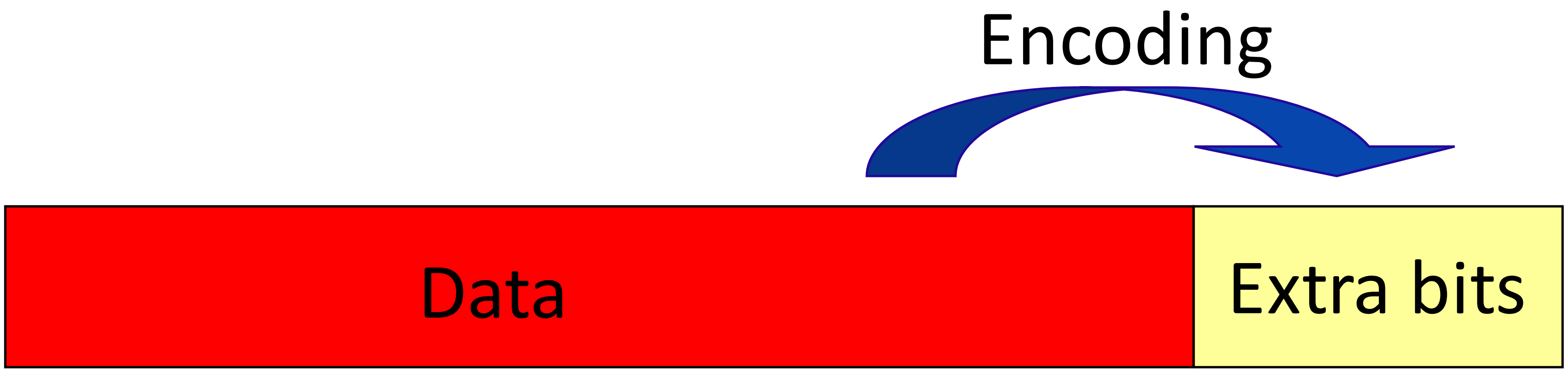
Framing

- Physical layer → bitstream
- Link layer → frames
- We need logical transmission units
  - Synchronisation points
  - Switching between users
  - Error handling



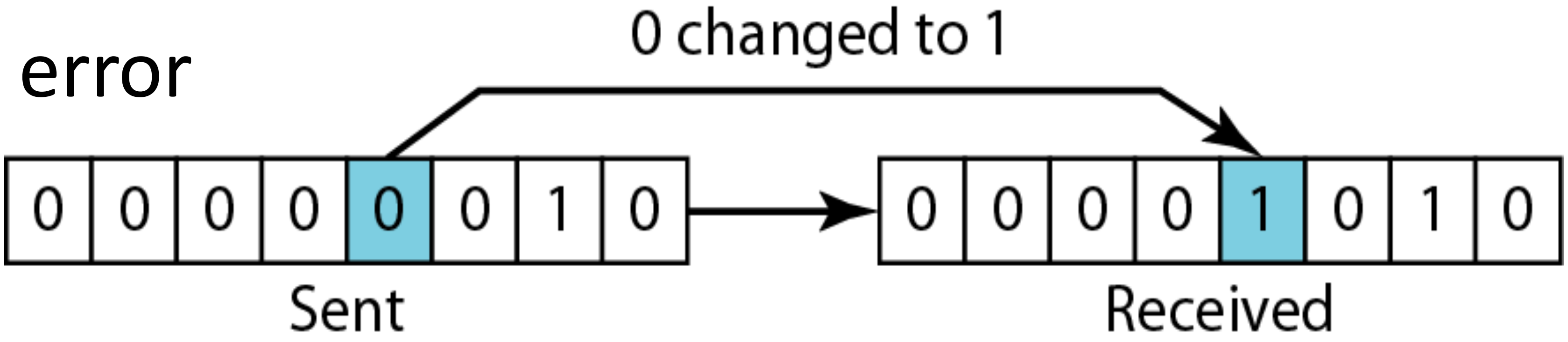
Error control

- Data assumed error-free by higher layers
  - Errors occur at lower layers (physical)
  - Job for LLC layer
- Extra (redundant) bits added to data
  - Generated by an encoding scheme from data

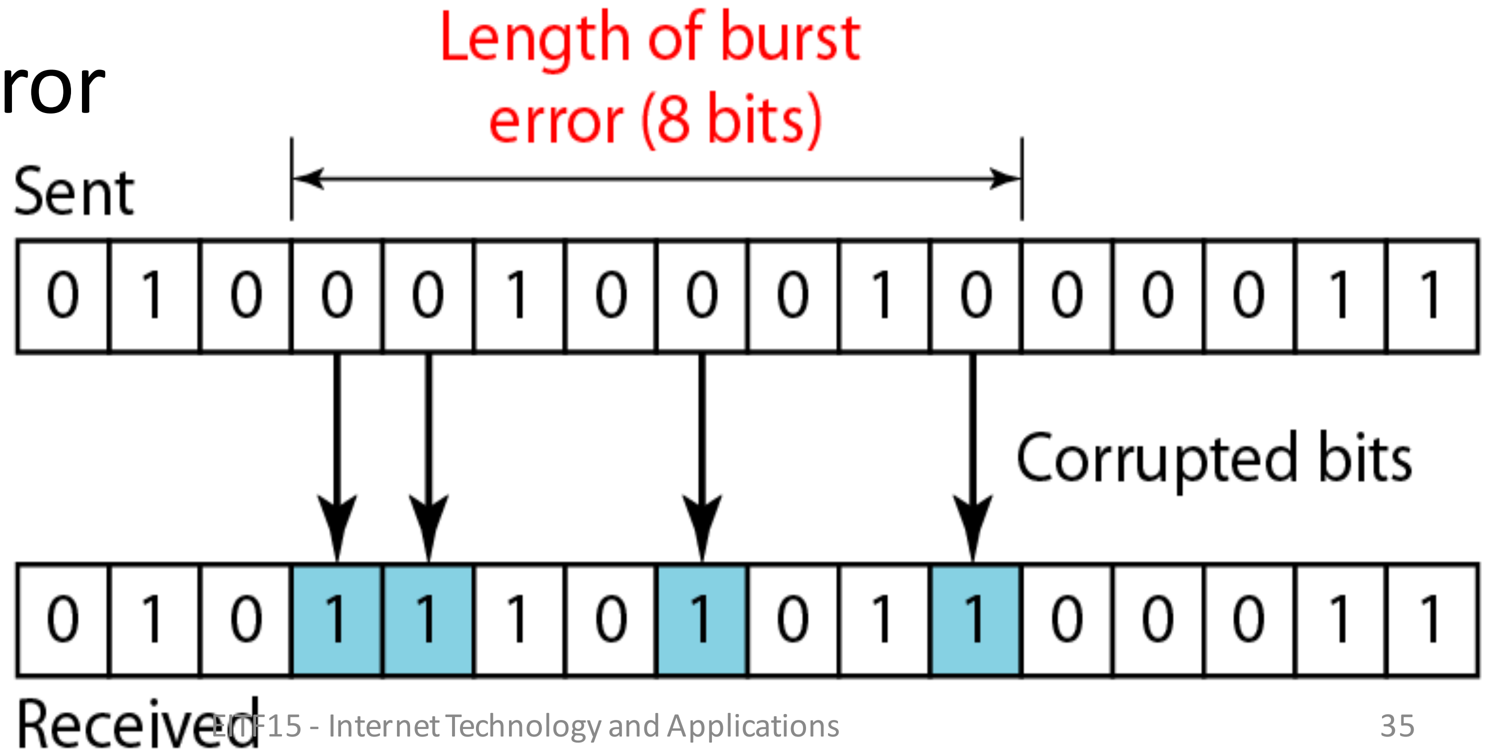


Error types

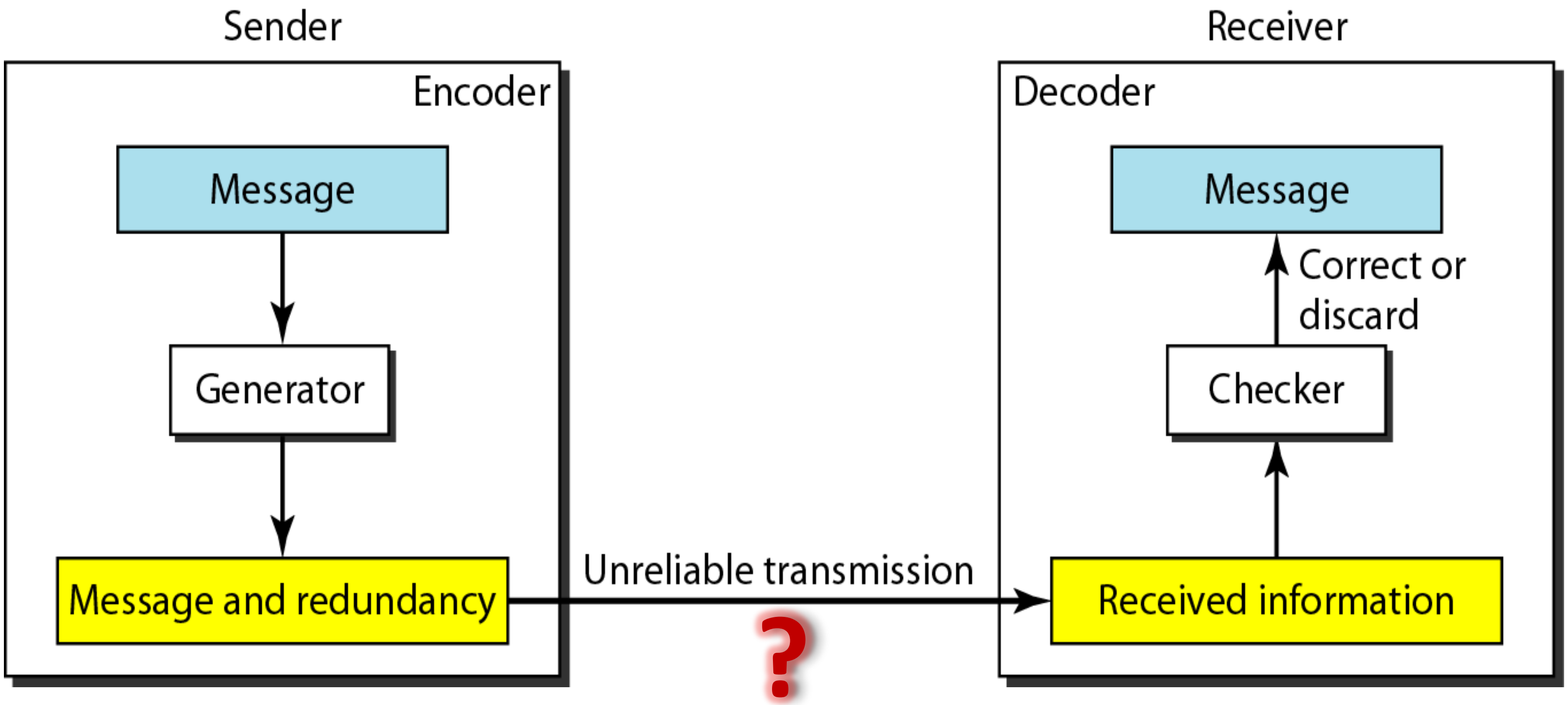
- Bit error



- Burst error



Error detection process



Error detection schemes

- Simple parity-check code
- Cyclic Redundancy Check (CRC)
- Checksum

Simple Parity-Check Code

- Extra bit added to make the total number of 1s in the codeword
  - Even → even parity
  - Odd → odd parity

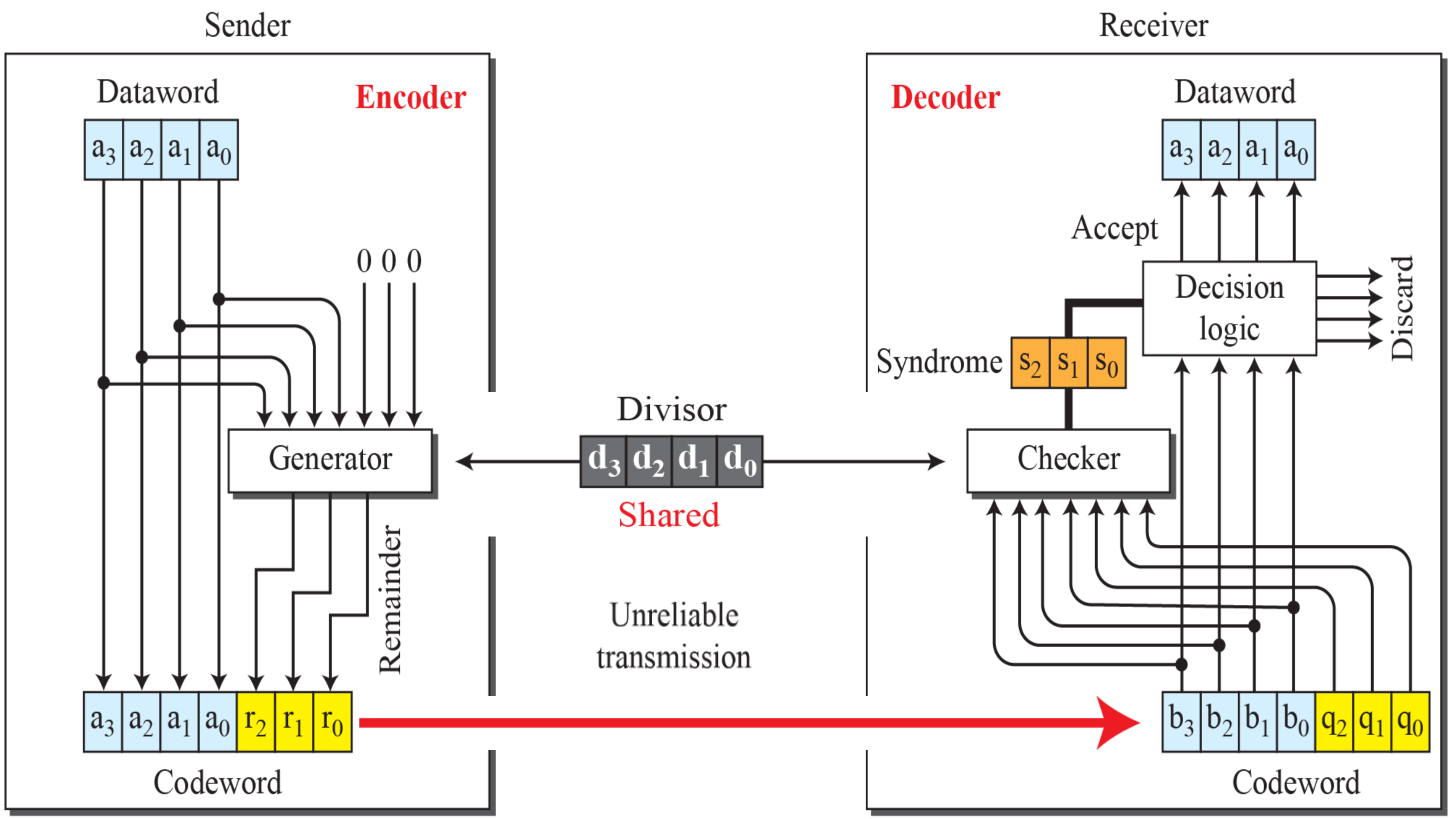
dataword **codeword**

10011100 + 0 = 100111000

- Problem?
  - Can detect an odd number of errors

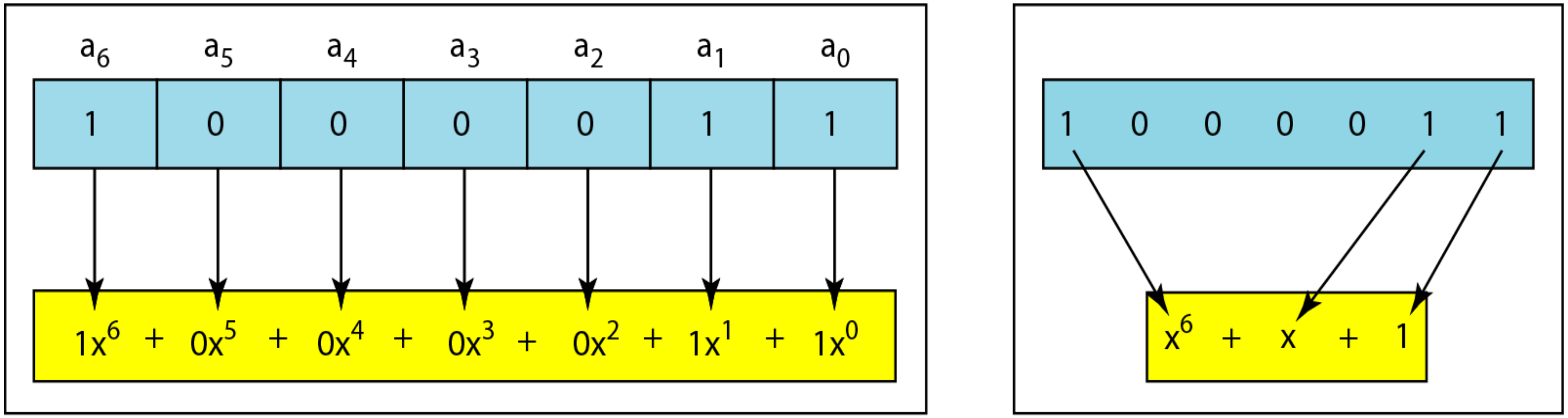
Cyclic Redundancy Check (CRC)

- Predefined shared *divisor* to calculate codeword



CRC: Polynomial representation

- The dataword of *k* bits is represented by a polynomial, *d(x)*.
- The degree of the polynomial is *k*-1.



a. Binary pattern and polynomial

b. Short form

CRC: The principle

- **Objective**: Send a dataword ***d(x)*** of k bits represented by a polynomial of degree ***k*-1**.
- **Given**: Generator polynomial ***g(x)*** of degree ***m***.
- **Find**: Remainder polynomial ***r(x)*** such that:

  $$c(x) = d(x) \cdot x^m + r(x)$$

  can be divided by g(x) without remainder.
- Codeword ***c(x)*** will then be sent to the receiver.
- ***r(x)*** has degree ***m*-1** or less, and CRC has ***m*** bits.

CRC: How it works

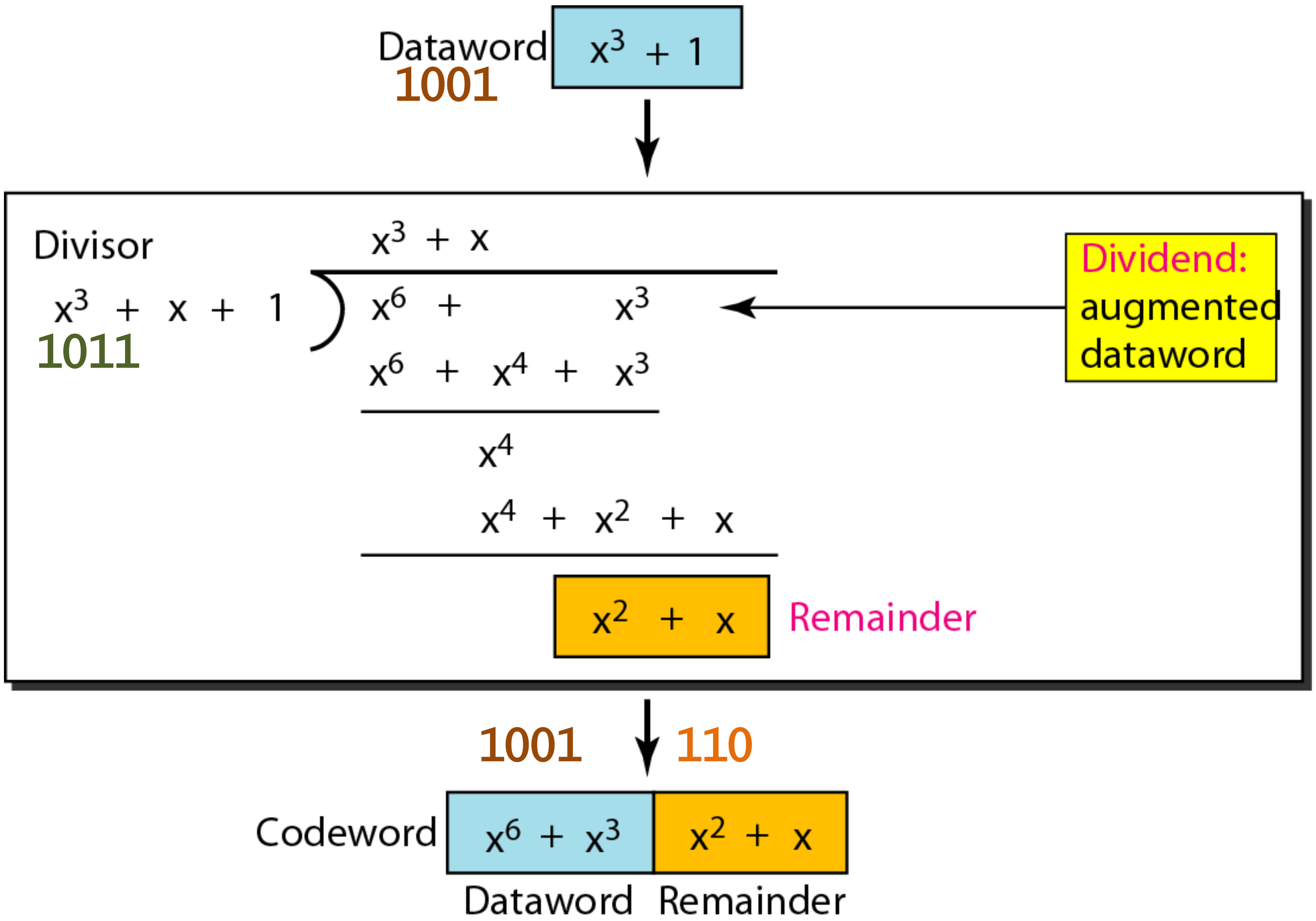
- Sender:
  1. Generate $b(x) = d(x) \cdot x^m$
  2. Divide $b(x)$ by $g(x)$ to find $r(x)$
  3. Send $c(x) = b(x) + r(x)$
- Receiver:
  1. Divide $c'(x) = c(x) + e(x)$ by $g(x)$
  2. Check remainder $r'(x)$ → if 0 data correct, $c(x) = c'(x)$
  3. Remove CRC bits from codeword to get dataword

Example: CRC derivation

- For dataword **1001**, derive CRC using generator **1011**.

- Data polynomial: $d(x) = x^3+1$
- Generator polynomial: $g(x) = x^3+x+1$
- Dividend: $b(x) = d(x) \cdot x^3 = x^6+x^3$
- Codeword polynomial: $c(x) = d(x) \cdot x^3 + r(x)$
- CRC polynomial: $r(x) = ?$

Example: CRC derivation

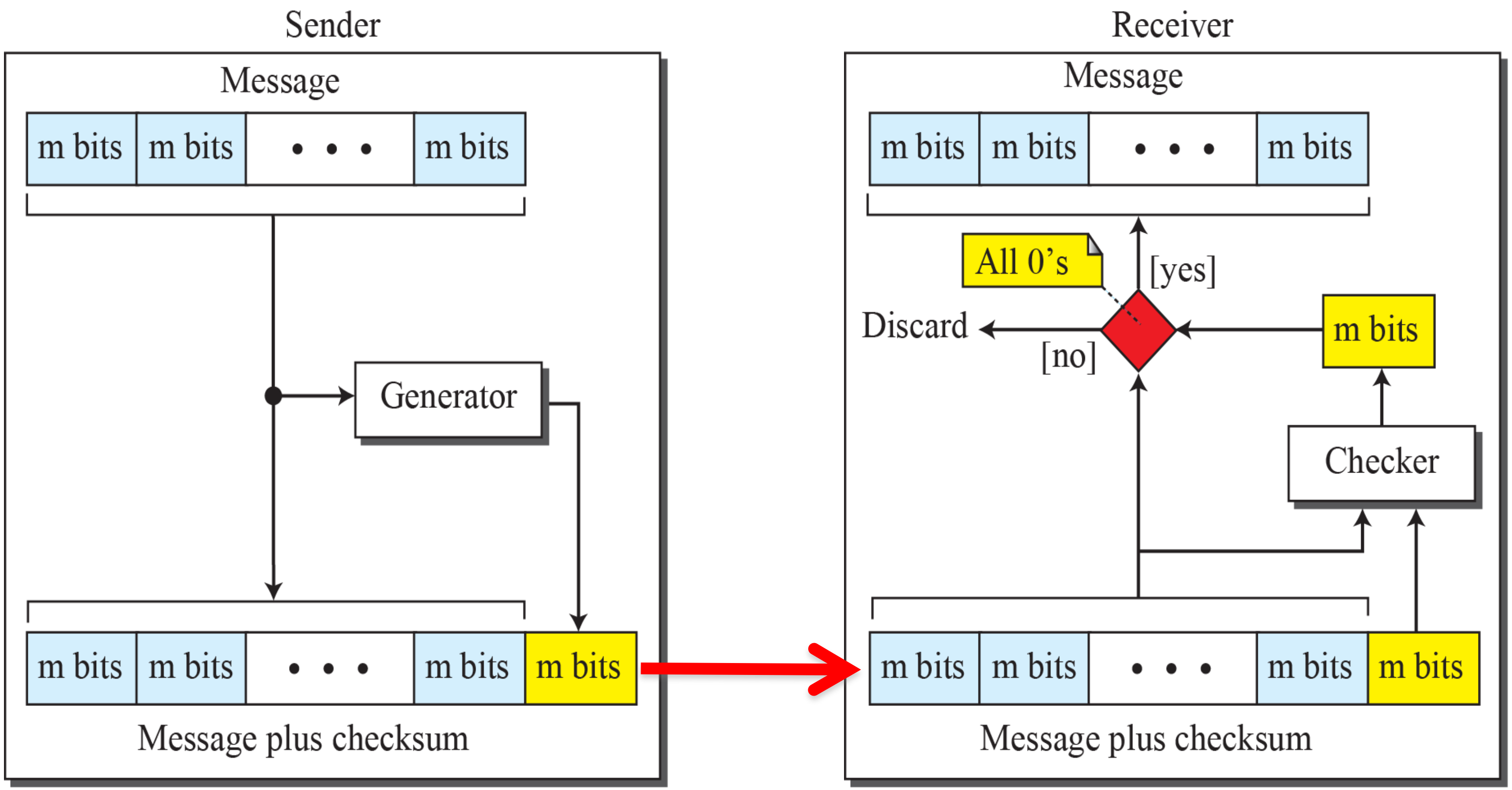


Checksum

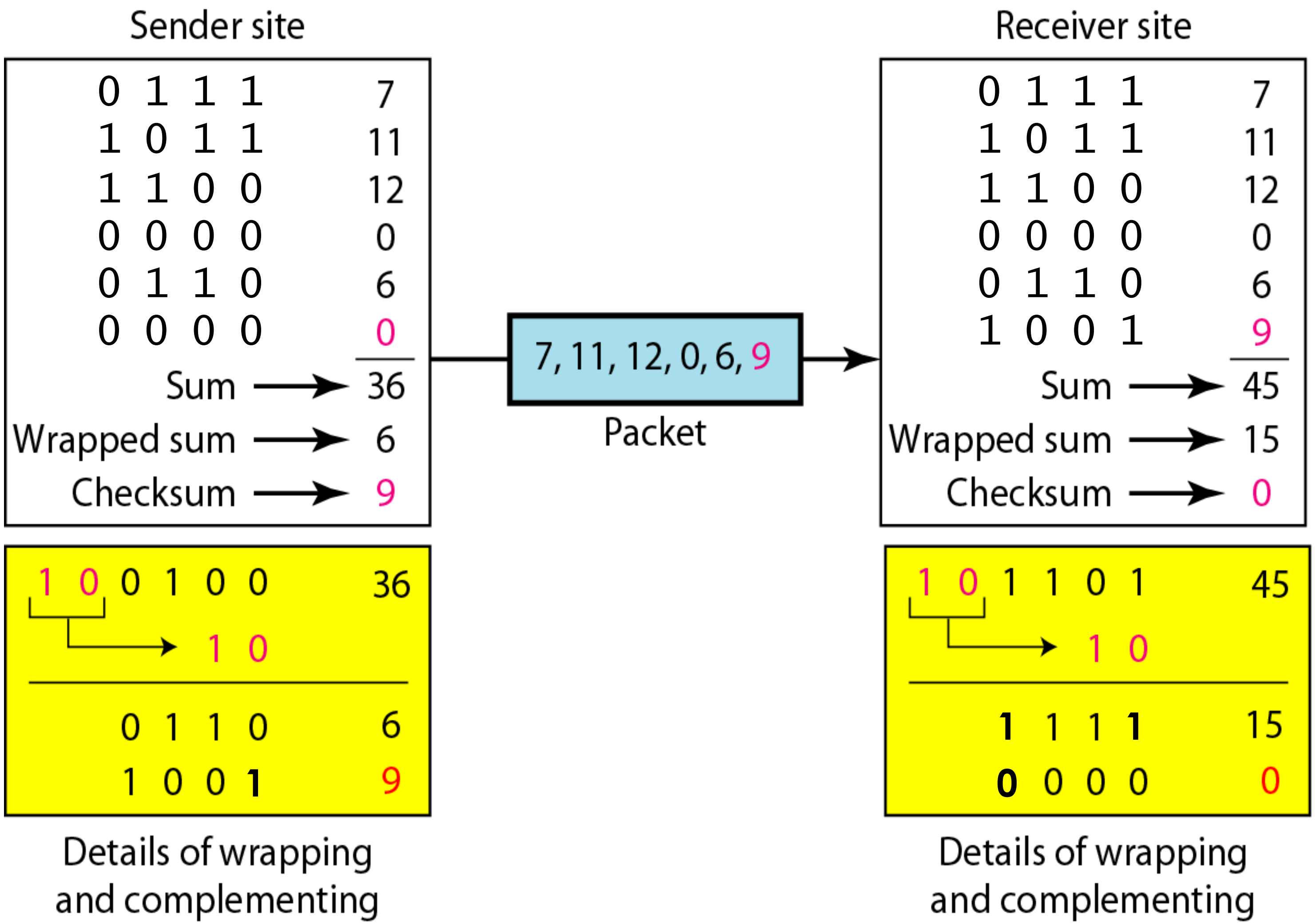
- The checksum is used in the Internet by several protocols although not at the data link layer.

- The main principle is to divide the data into segments of n bits. Then add the segments and use the sum as redundant bits.

Checksum process



Example: Checksum

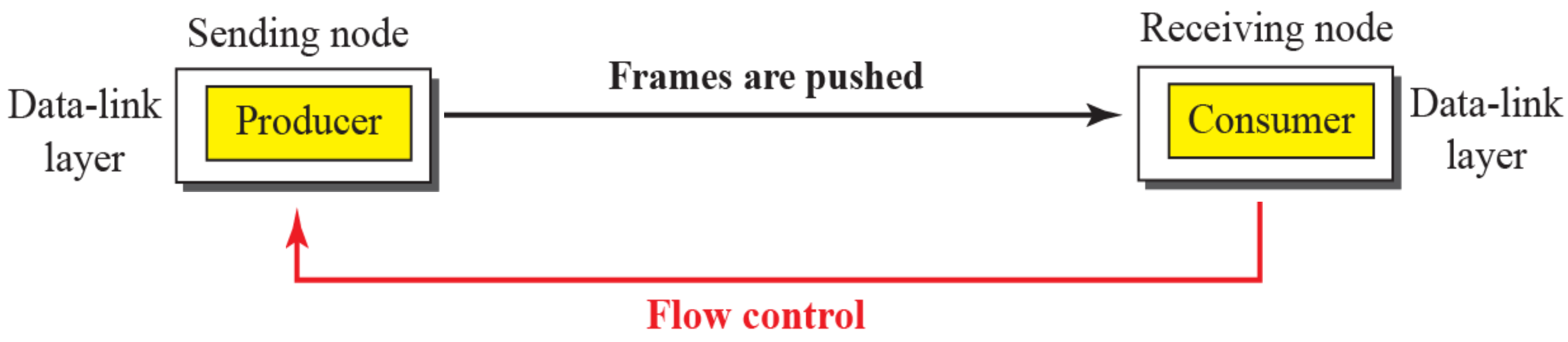


Error and flow control

- The basic principle in error and flow control is that the receiver **acknowledges** all correctly received packets.

The need for flow control

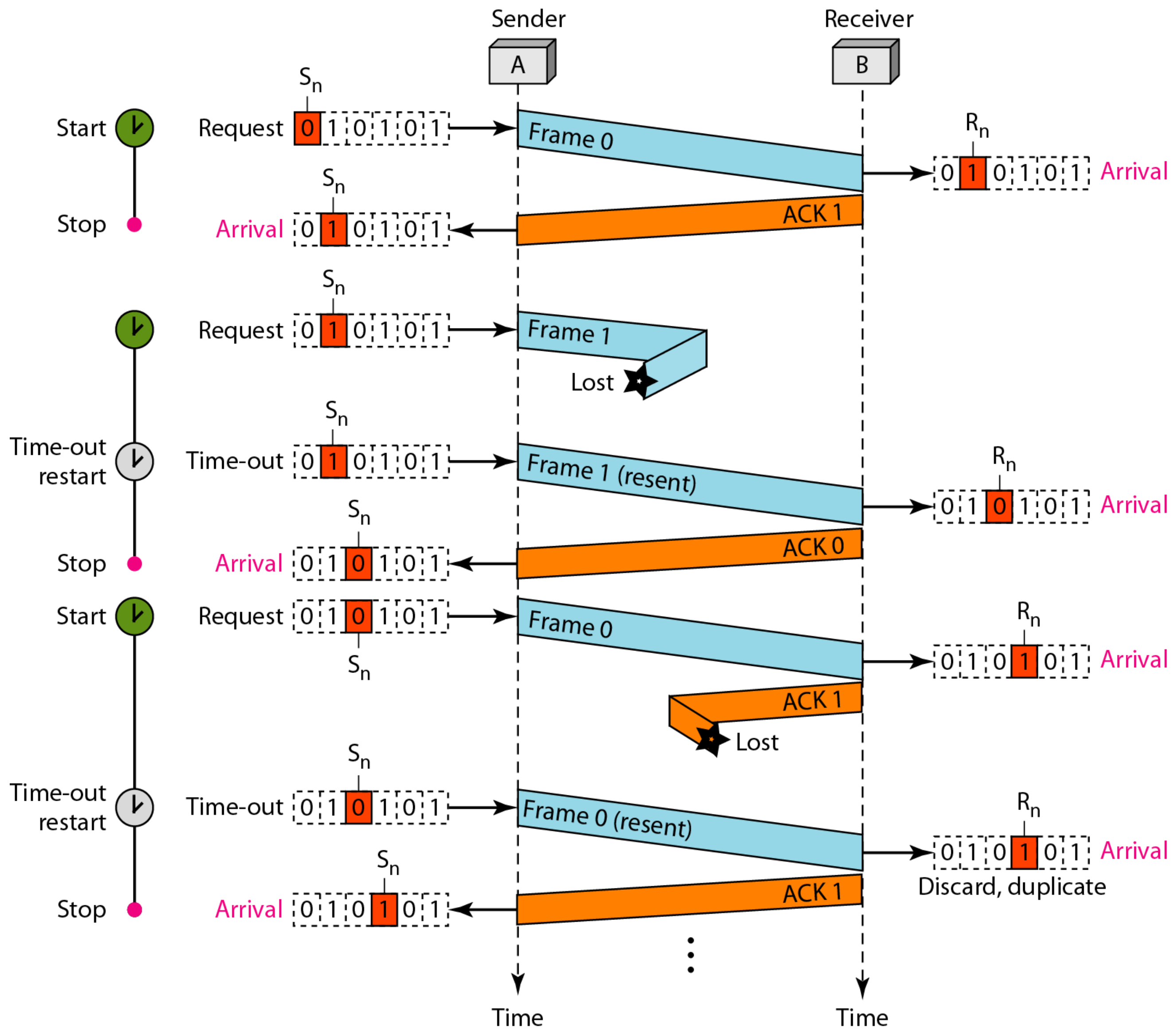
- The receiver must be able to handle all recieved frames. If the transmission rate is too high, the receiver may become overloaded and drop frames due to full buffers.



Stop-and-wait ARQ

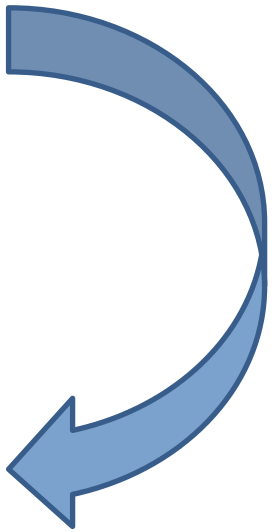
- Send and wait
  - Keep time
  - Wait for ACK
  - Retransmit
- Automatic repeat request
  - Frames (SEQ++)
  - Acknowledgements (SEQ+1)
  - Mismatch = problem!

Stop-and-wait ARQ flow diagram



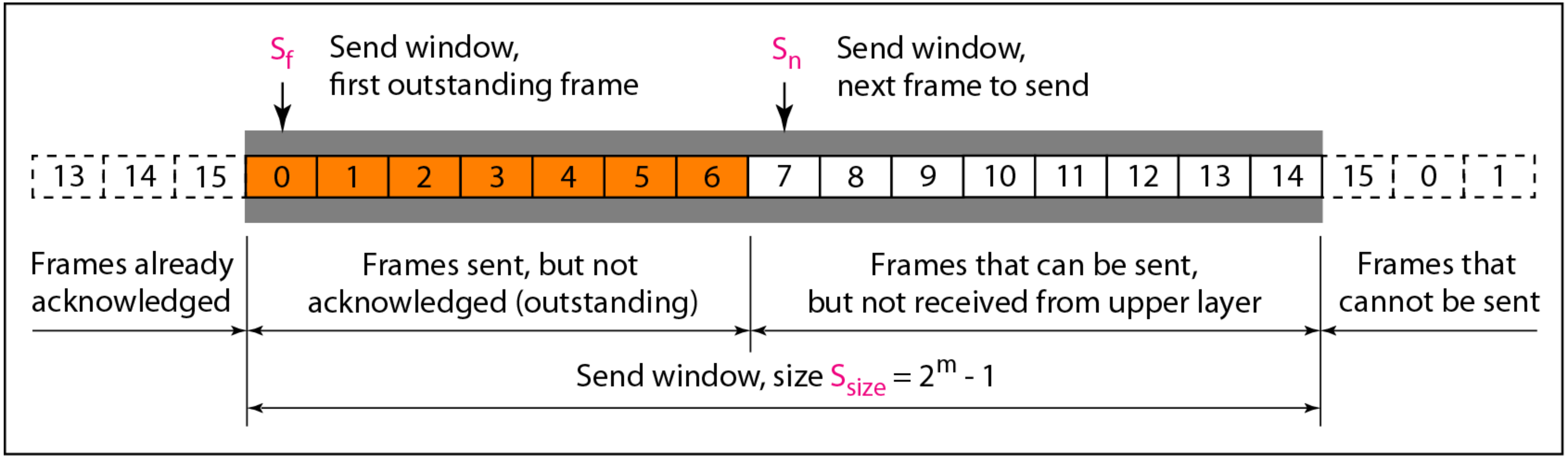
Stop-and-wait ARQ inefficiency

- Too much waiting
- Solution
  - Keep the pipe full
  - But not too full

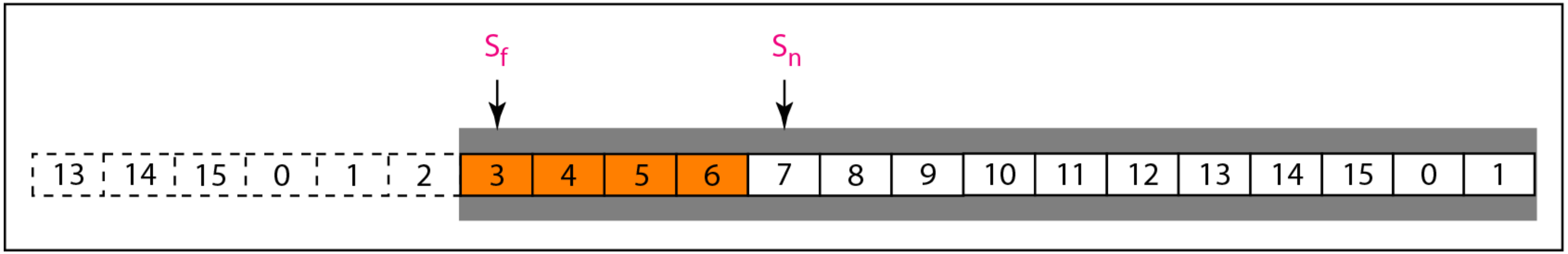


- Sliding window
  - Size matters
  - Window size < 2^m

Sliding window

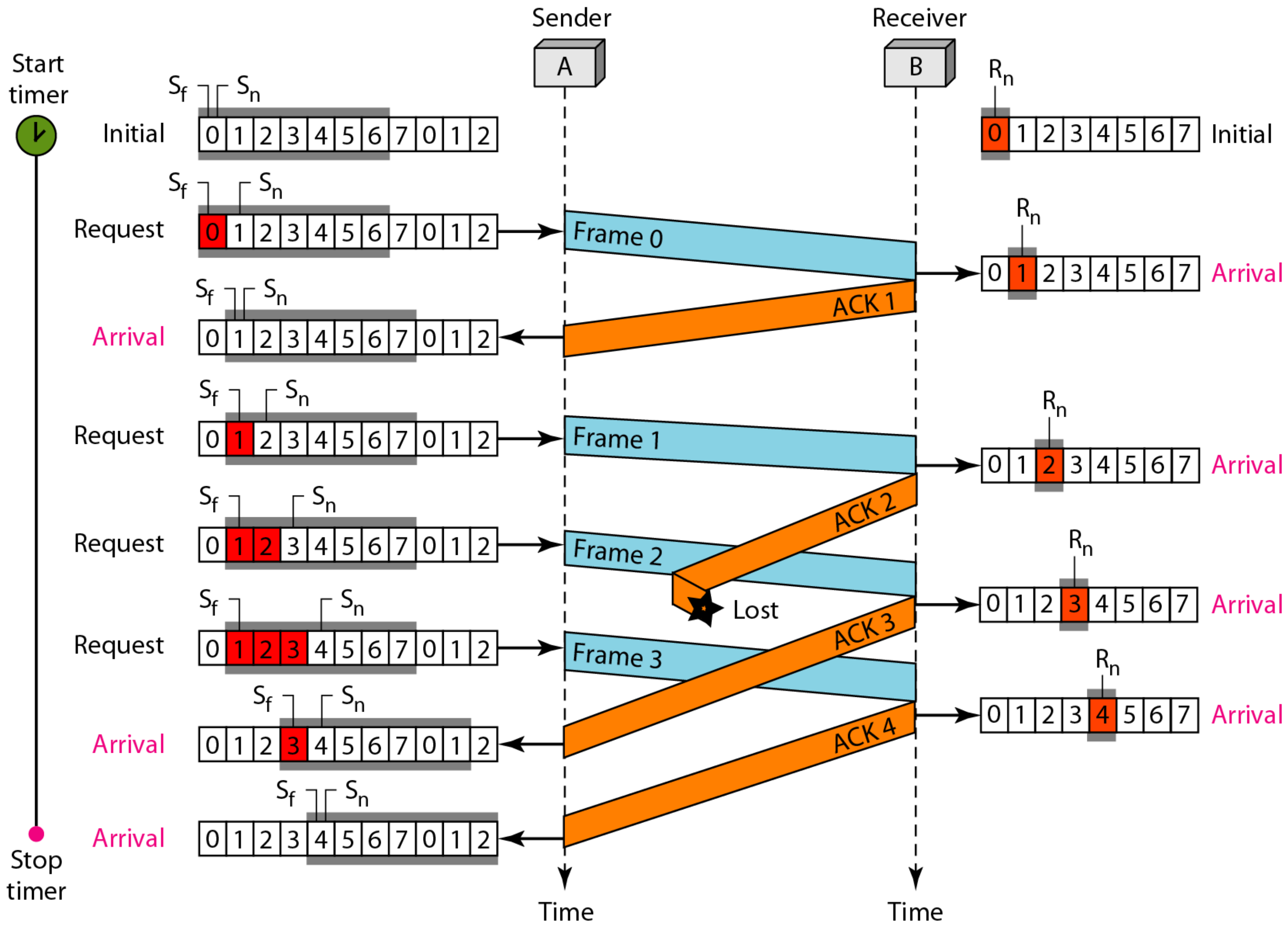


a. Send window before sliding

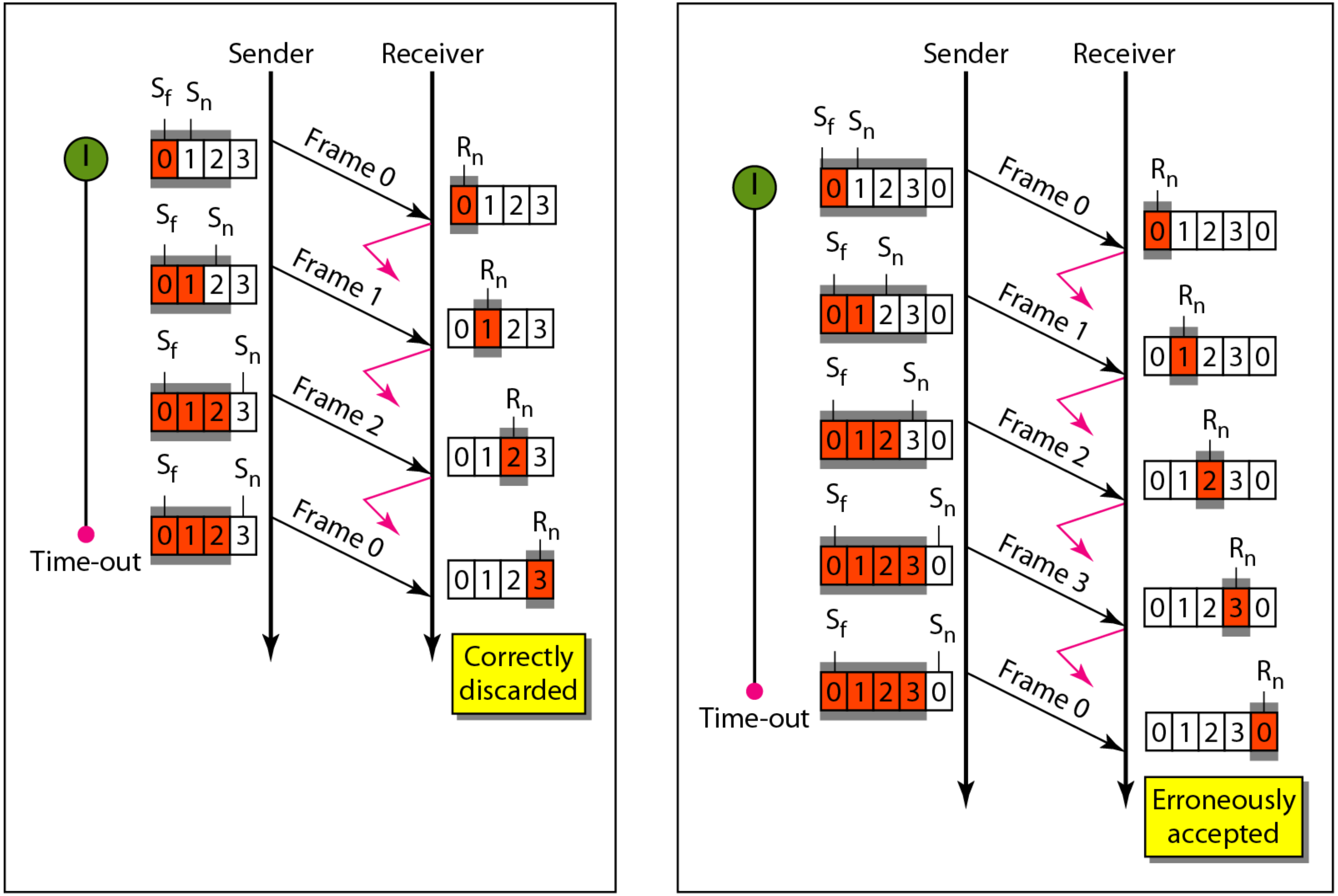


b. Send window after sliding

Go-back-N ARQ flow diagram



Go-back-N ARQ window size

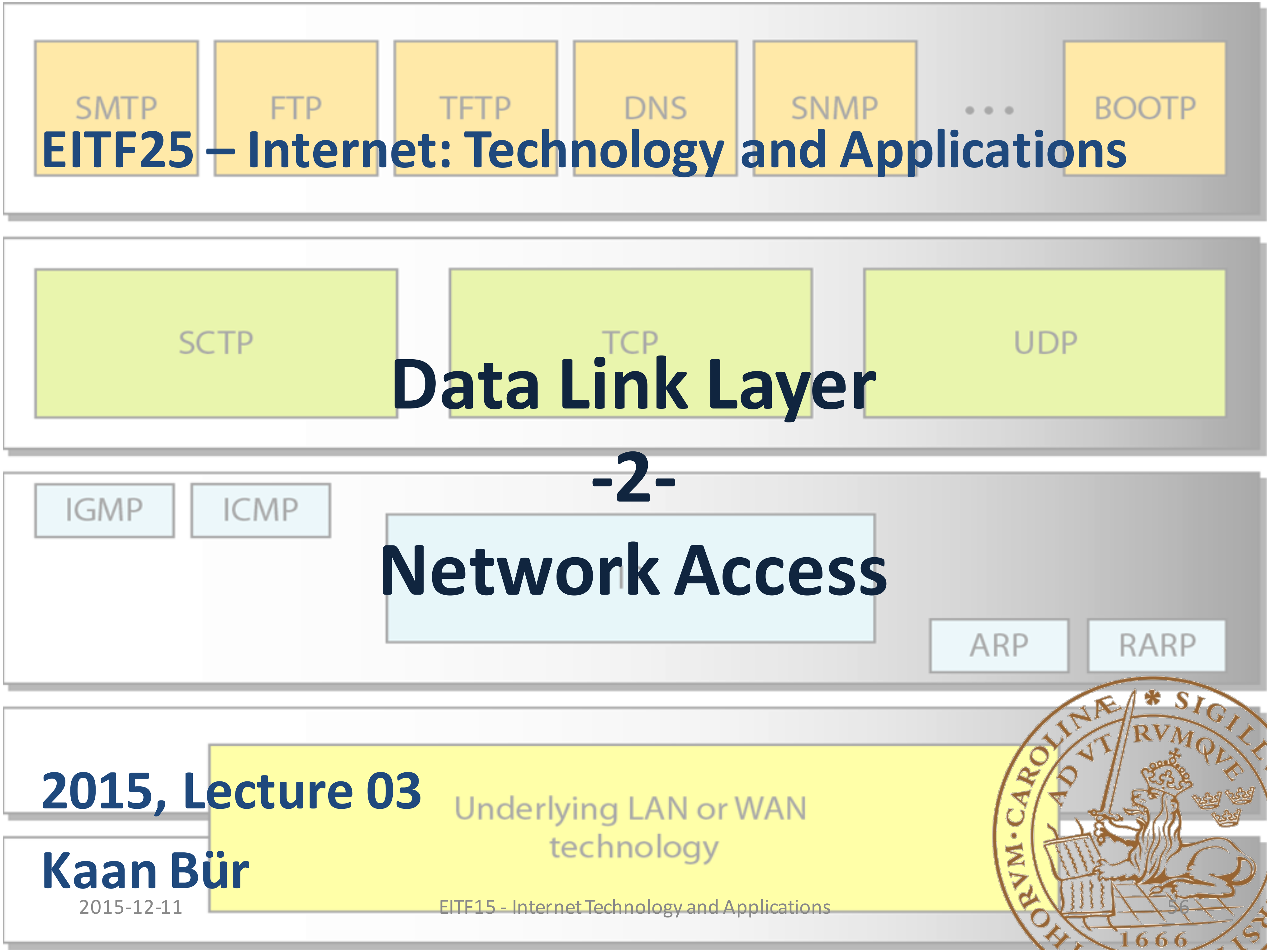


a. Window size < 2^m

b. Window size = 2^m

EITF25 – Internet: Technology and Applications

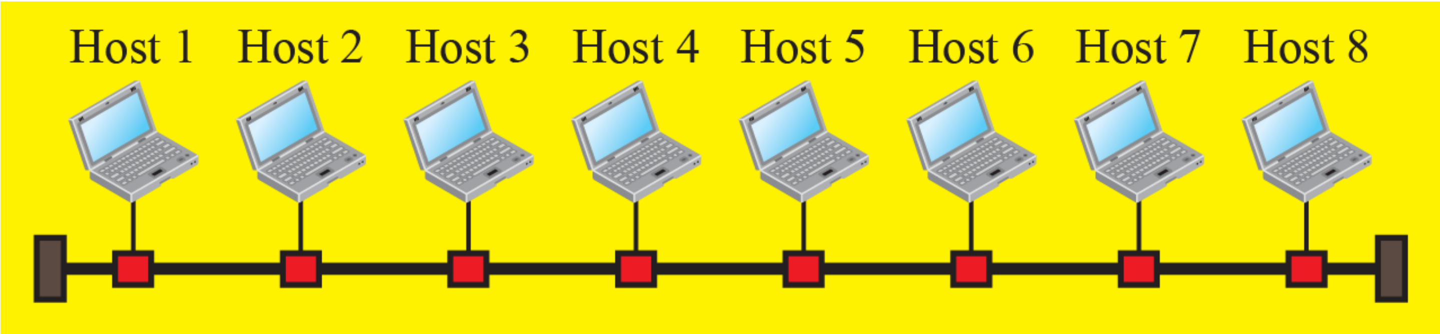
Data Link Layer
-2-
Network Access



2015, Lecture 03

Kaan Bür

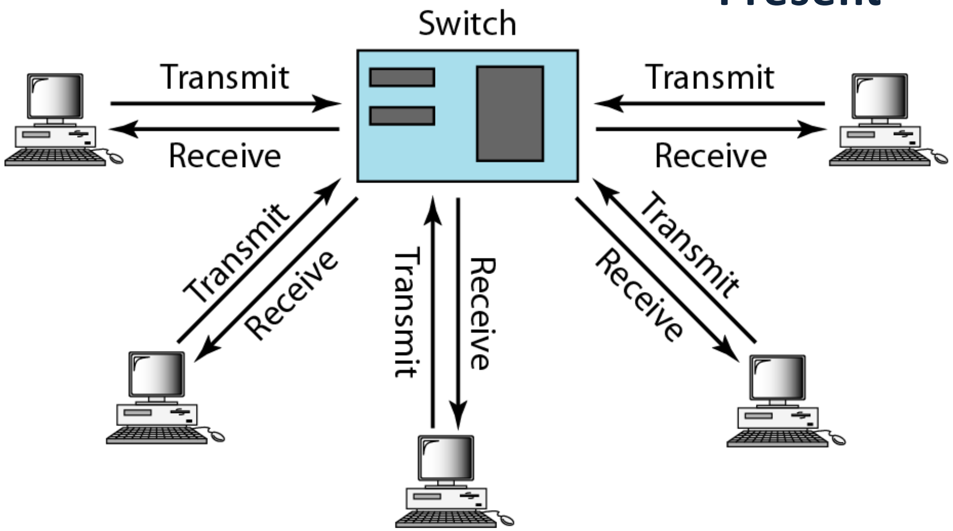
Concept of shared medium



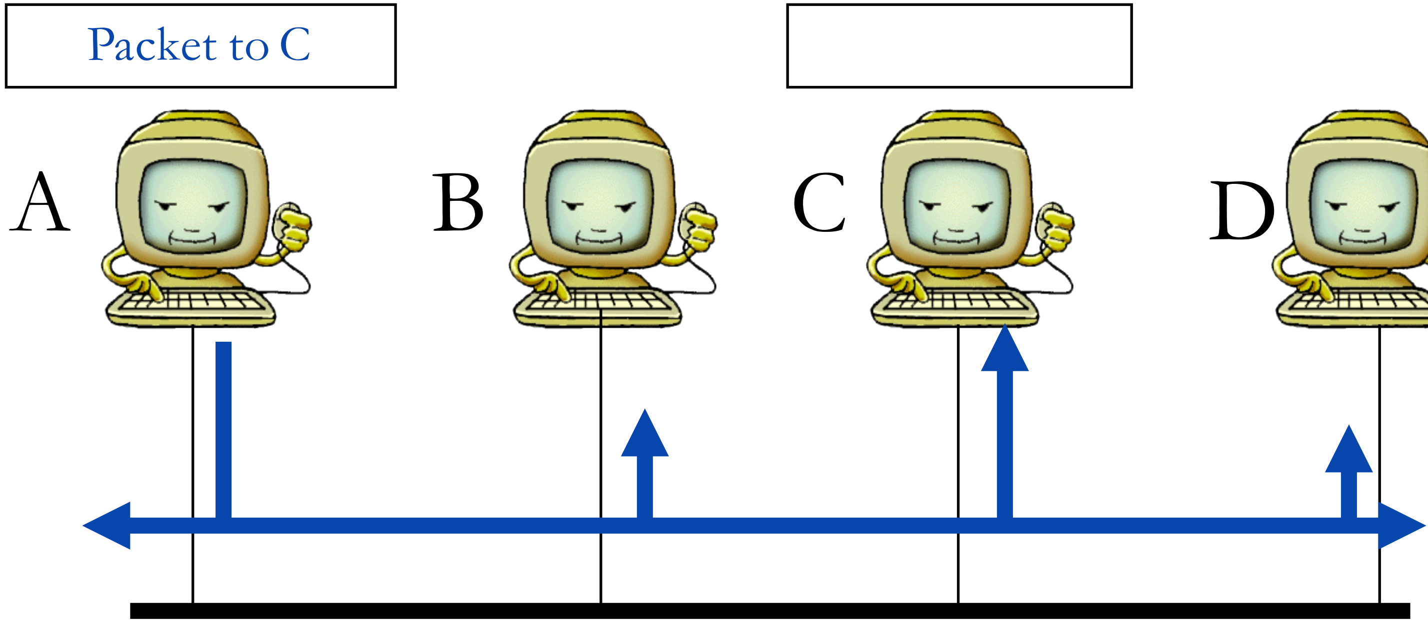
Past

- Not for wired media any longer
- Wireless LAN (WLAN) share wireless medium.

Present



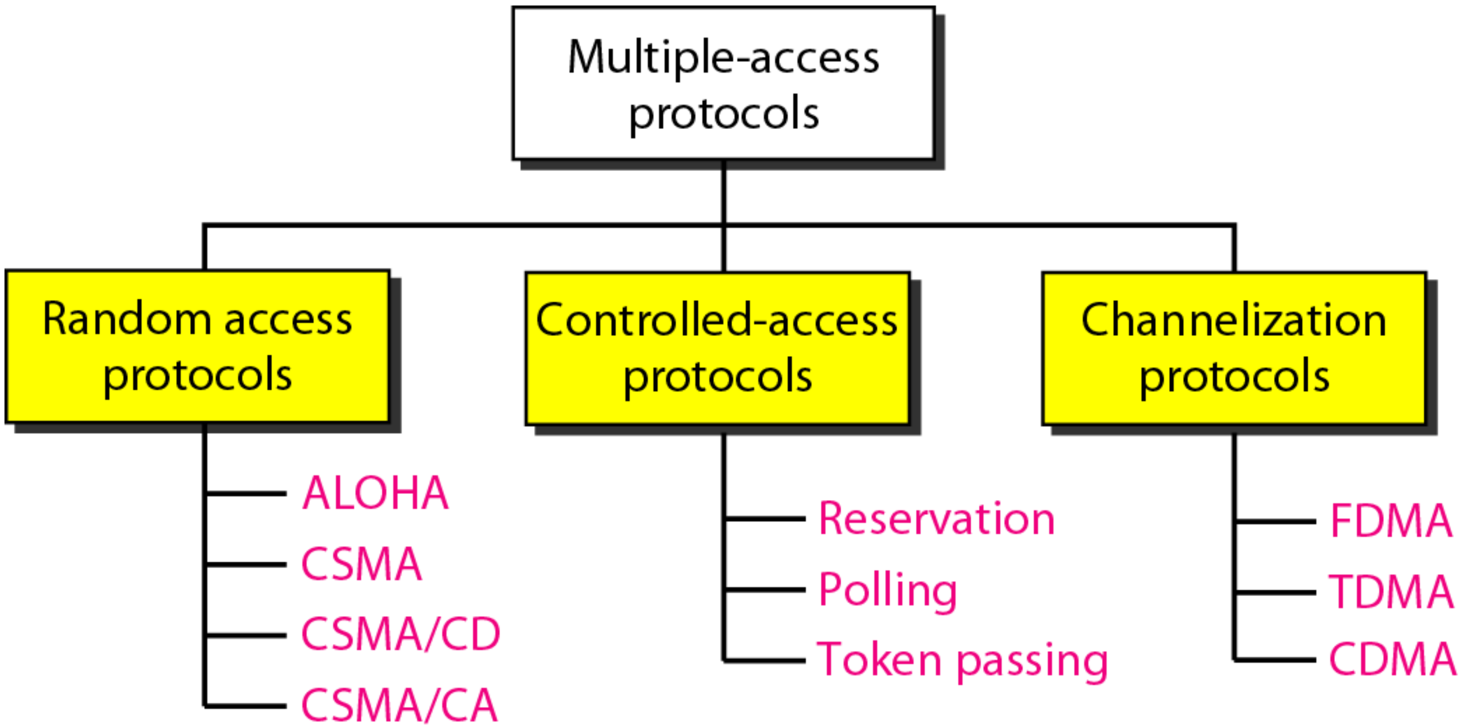
Data transfer on a shared medium



The computer with the right destination address copies the packet and delivers it to the application.

Medium Access Control (MAC)

- Set of rules for sending (and receiving) data in a multiple access network



Controlled access protocols

- Stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.

- Used in different parts of the mobile networks.

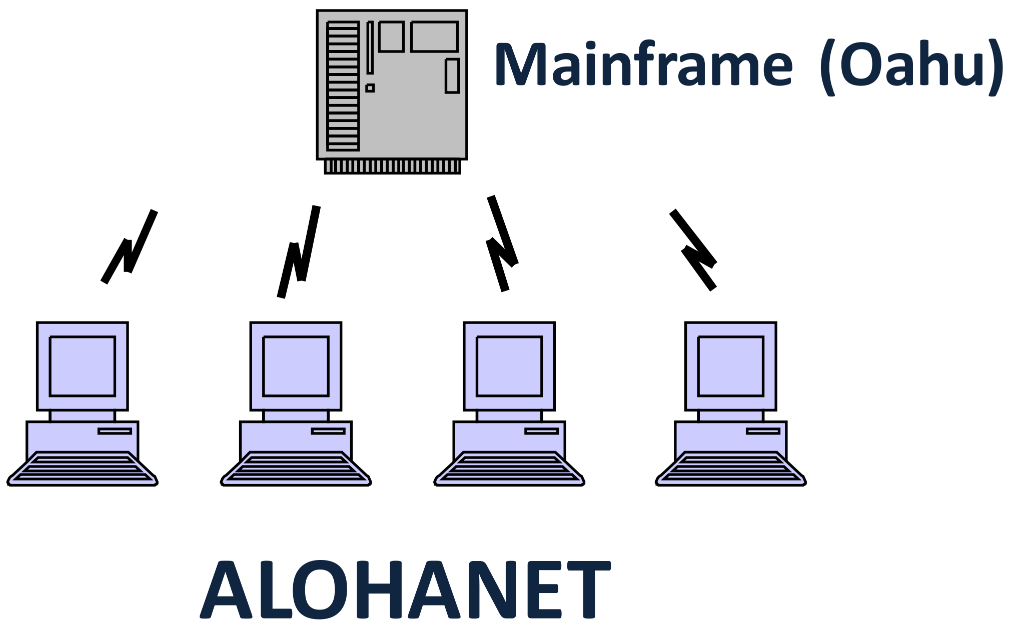
Random access protocols

- No station superior to another
- No station in control of another

- A station with data to send uses a procedure to decide whether or not to send

Random access: ALOHA

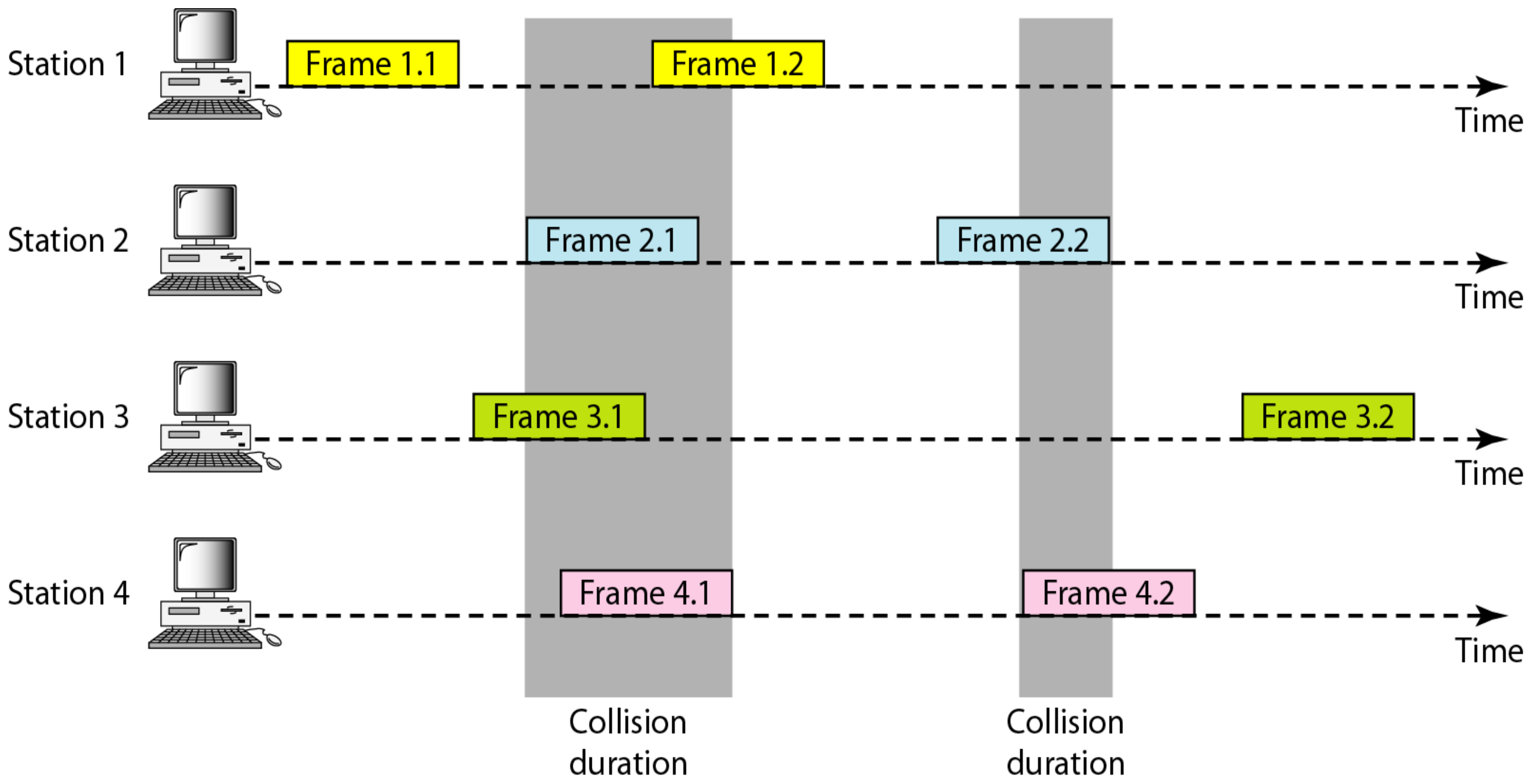
- Multiple-access method of ALOHANET
  - One of the first WLAN in the world
  - Devloped by the University of Hawaii (1970)



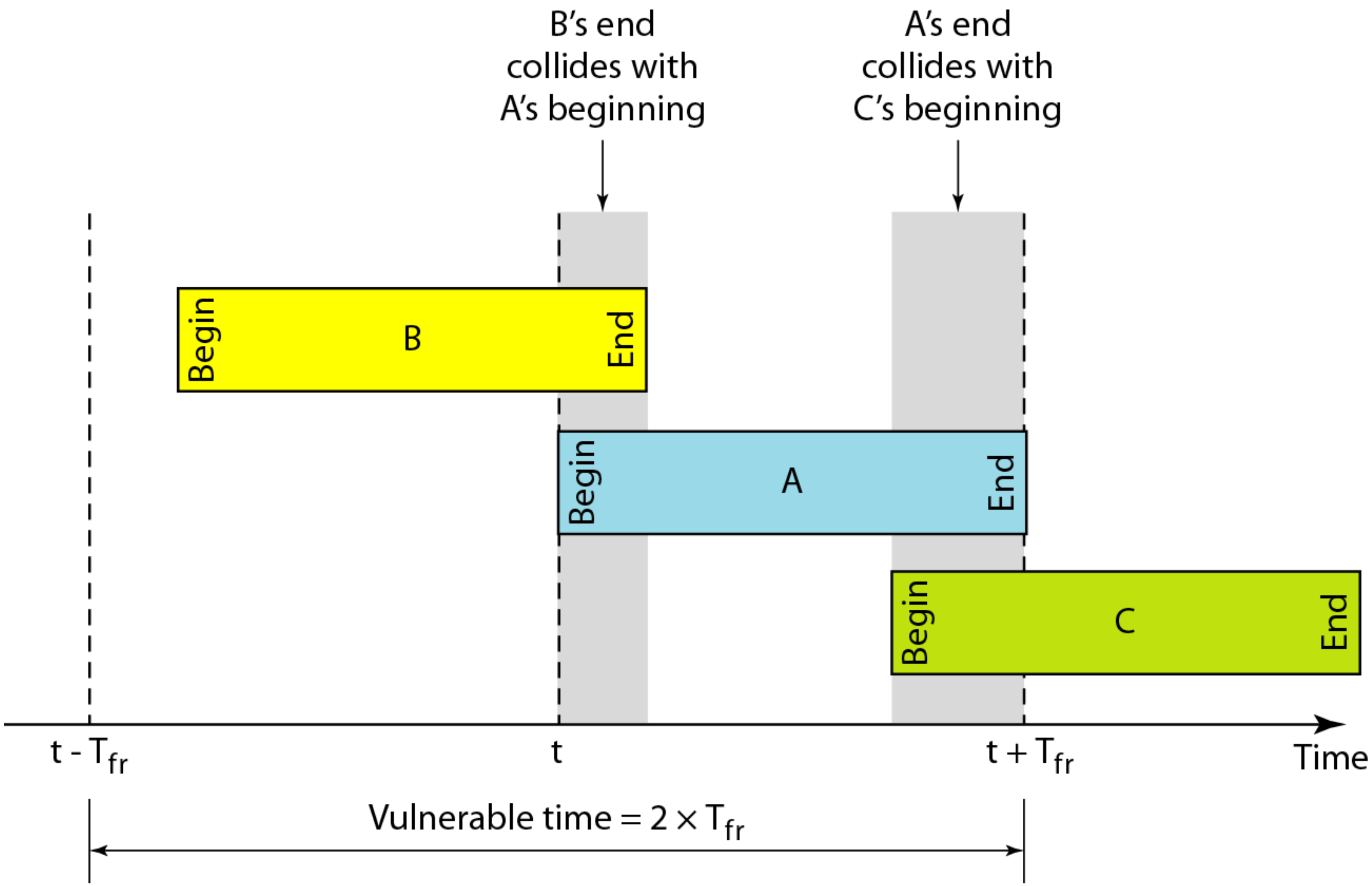
Pure ALOHA

- Stations share one frequency band
- Mainframe sends data on another frequency (broadcast channel)
- A station sends a frame whenever it has a frame to send.
- If the station receives an ACK from the mainframe on the broadcast channel, the transmission is successful.
- If not, the frame needs to be retransmitted.

Pure ALOHA: Frames



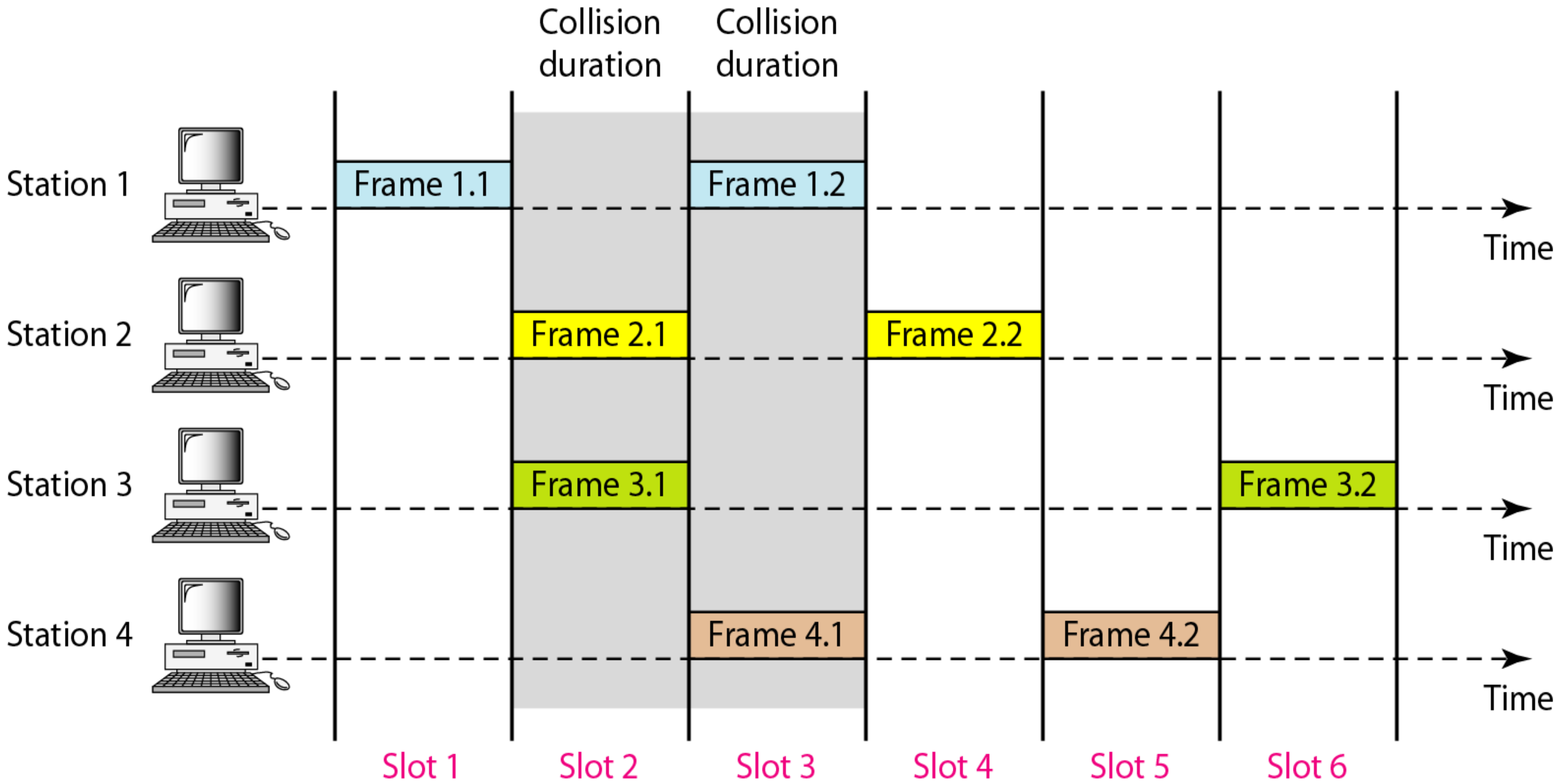
Pure ALOHA: Collisions



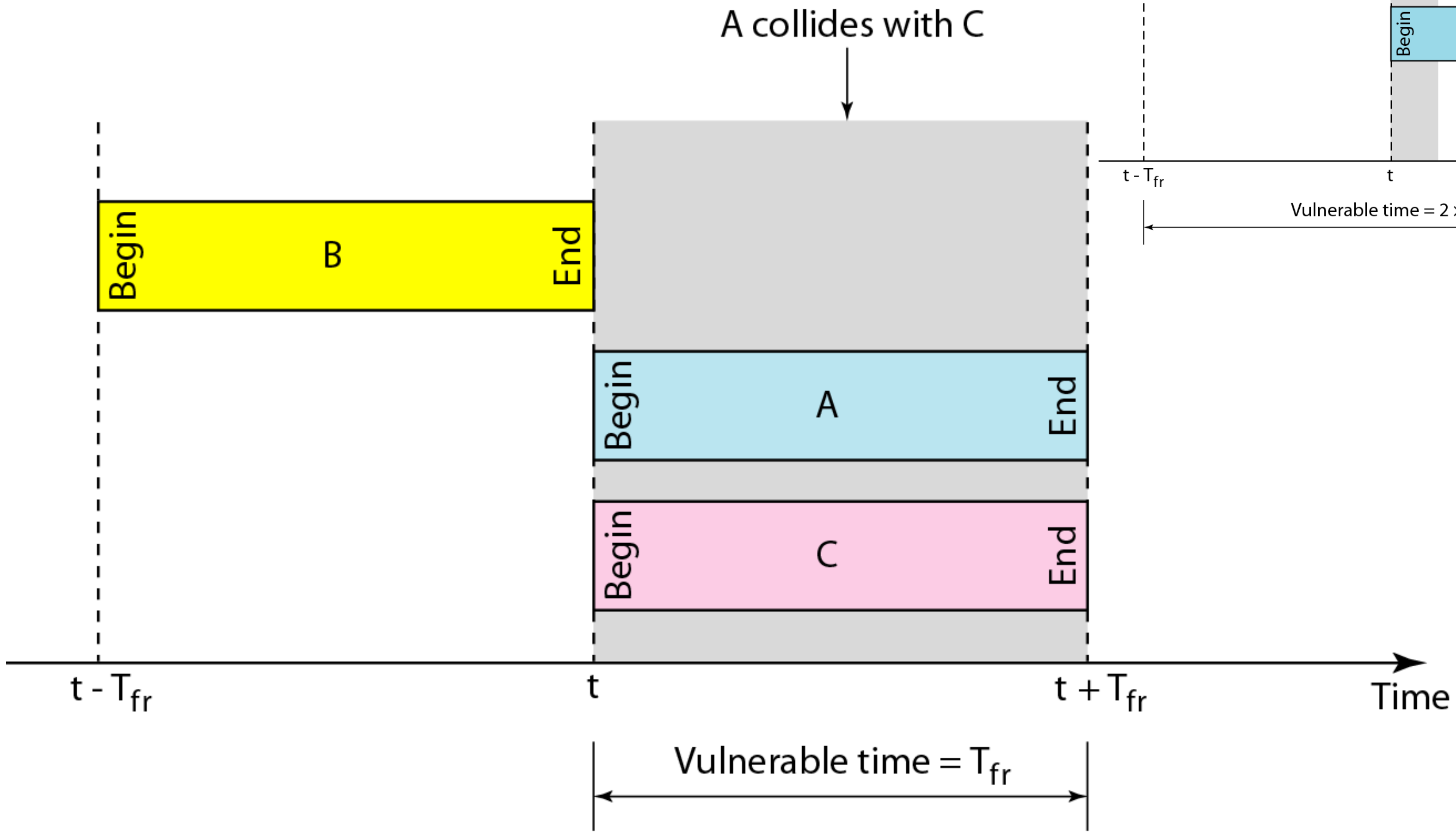
Slotted ALOHA

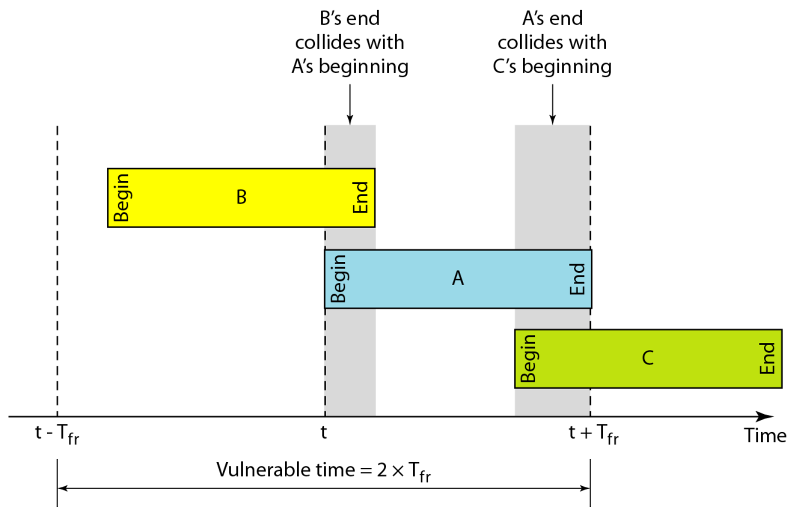
- Time divided into slots
- Each slot contains one frame in time
- A station can only send at the beginning of a slot.

Slotted ALOHA: Frames



Slotted ALOHA: Colllisions

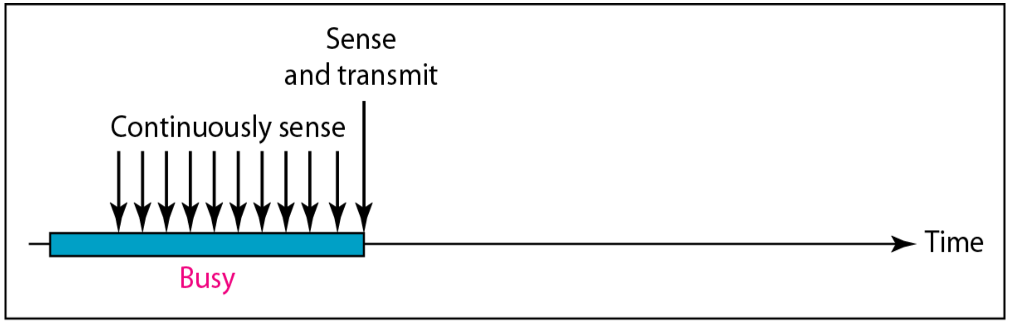




Carrier Sense Multiple Access (CSMA)

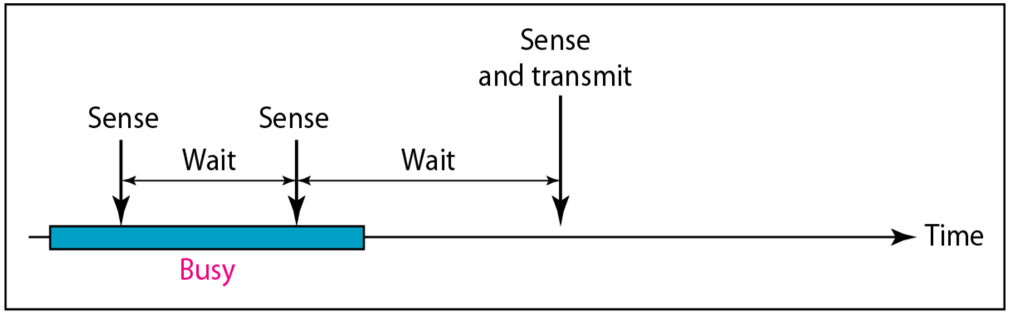
- Listen to (sense) medium before sending
- If medium occupied (busy), wait
  - 1-persistent
  - Non-persistent
  - P-persistent

Persistence methods



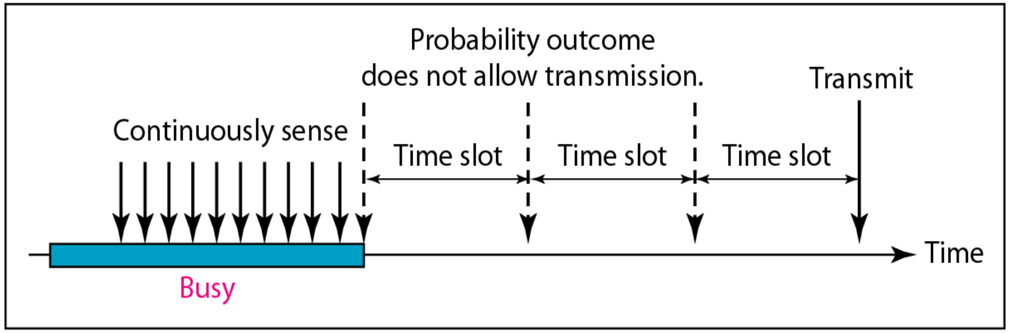
a. 1-persistent

Keep sensing and send as soon as channel idle



b. Nonpersistent

Wait random, sense again, send if idle

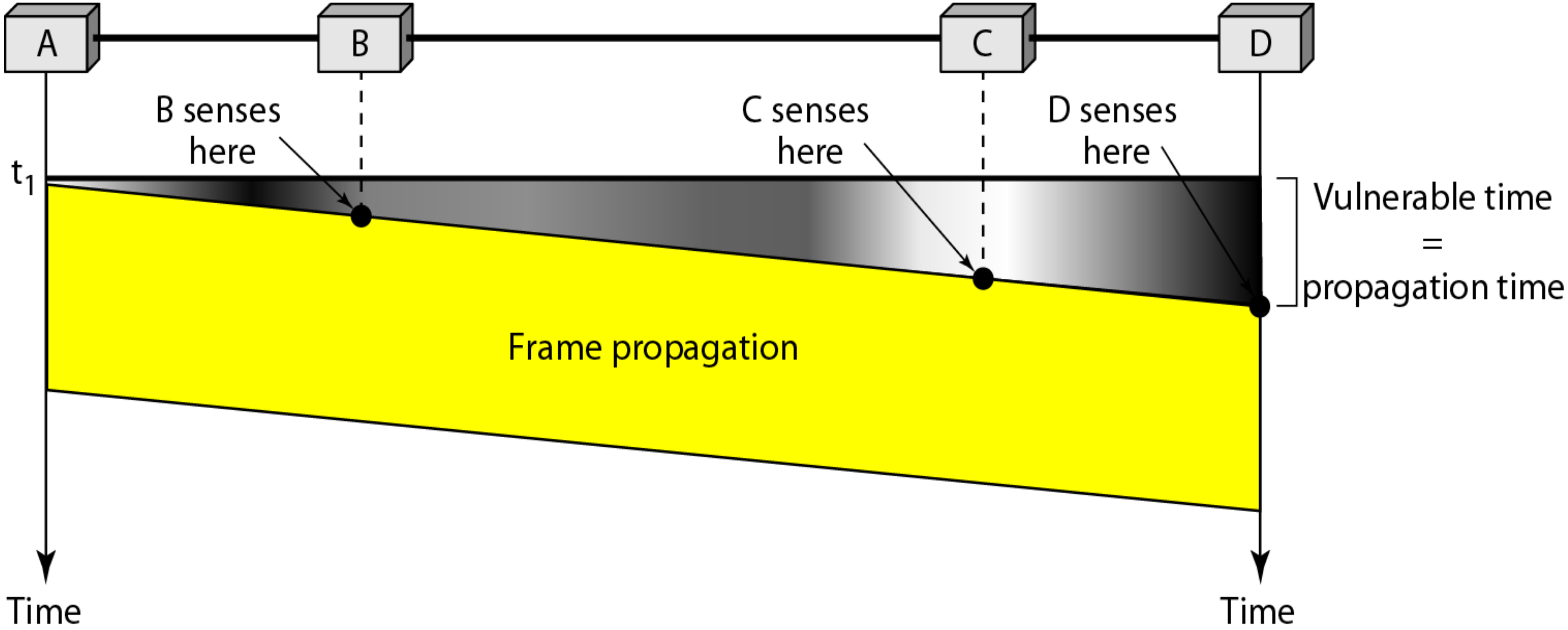


c. p-persistent

Transmit with probability p, sense with 1-p, wait if busy

CSMA: Vulnerable time

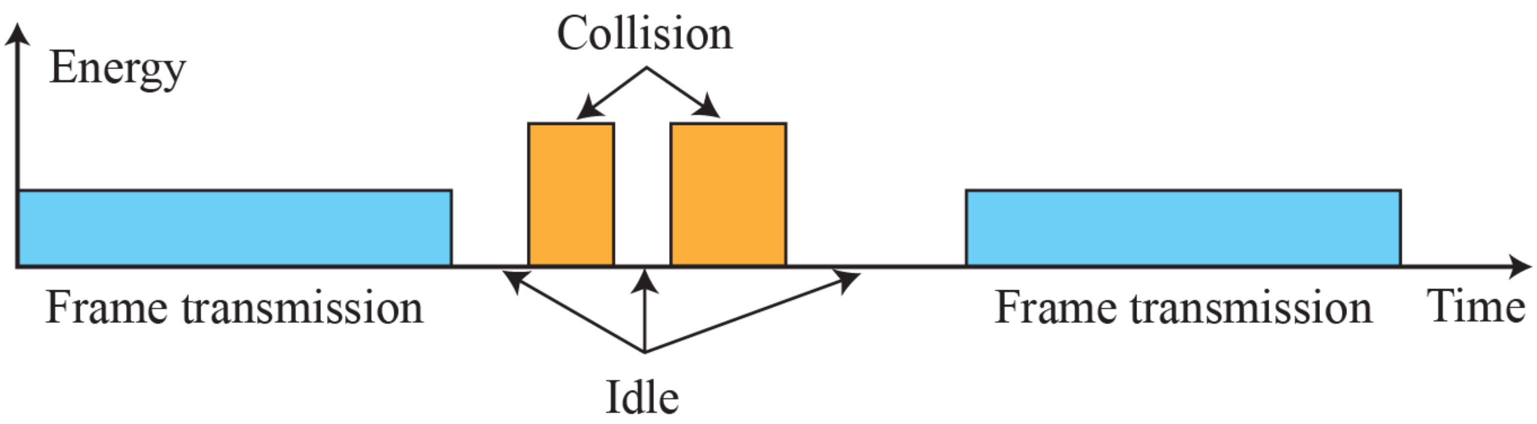
- Propagation time



- Collisions?

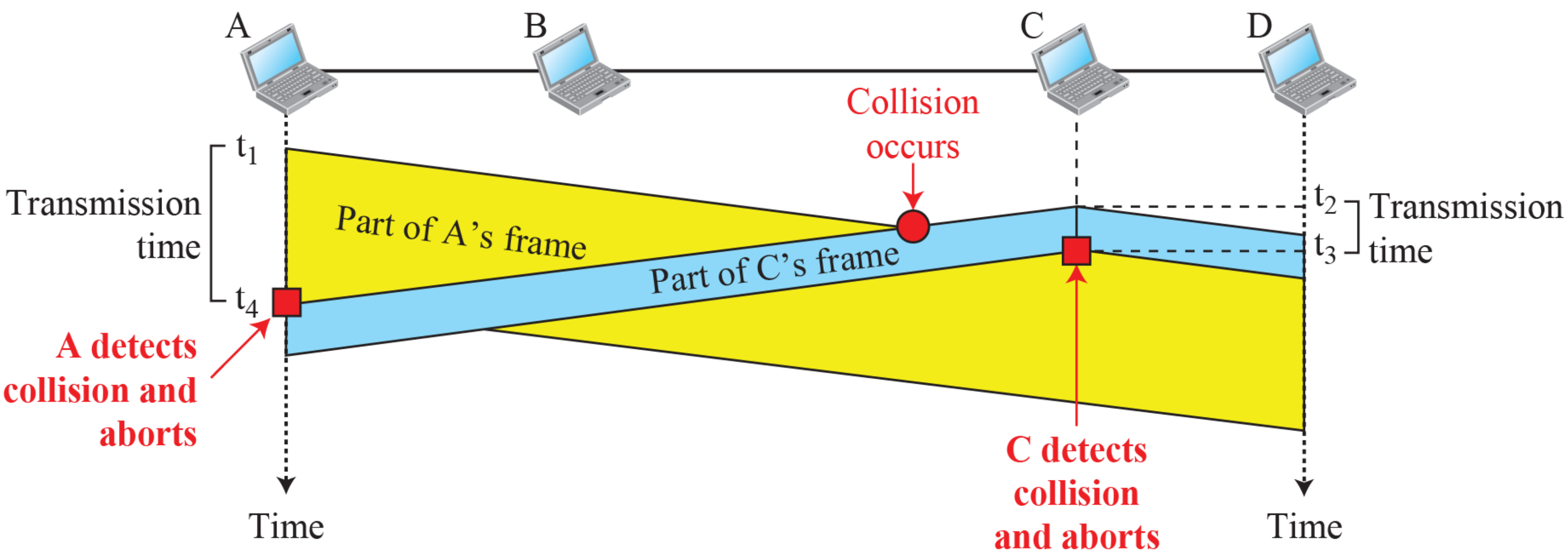
CSMA with Collision Detection (CSMA/CD)

- CSMA has no collision procedure
- CSMA/CD developed to handle collisions



CSMA/CD: Collision detection

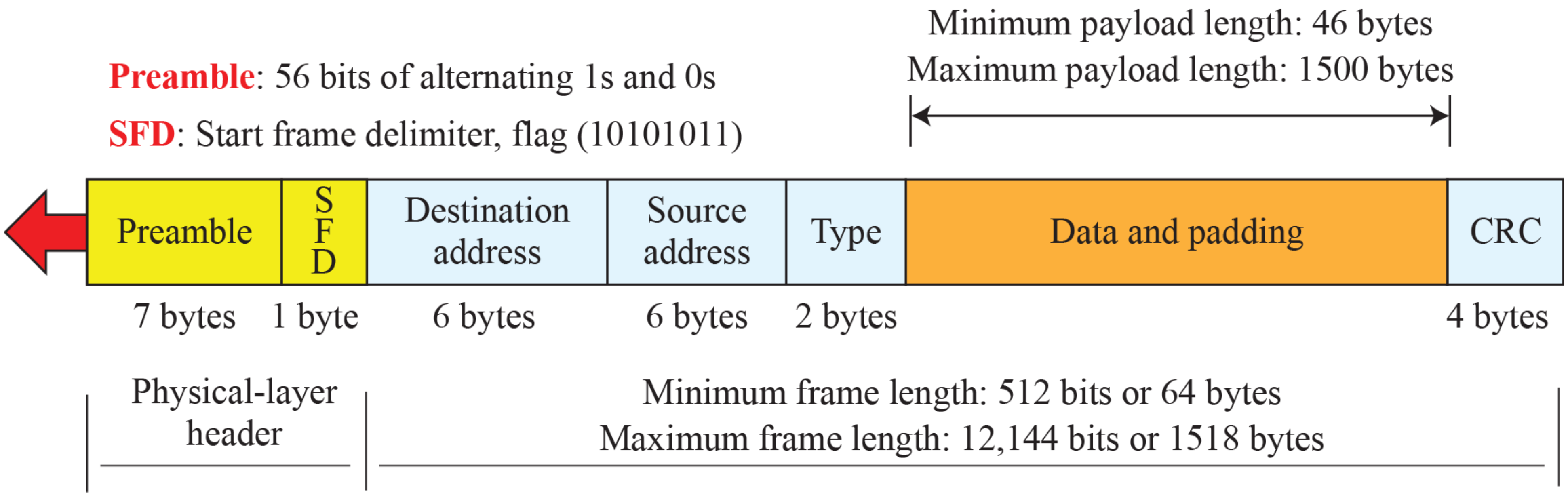
- Monitors medium after sending a frame
- Abort transmission and send a jamming signal if collision detected



CSMA/CD: Minimum frame size

- Sending station must be able to detect a collision *before* transmitting the frame's last bit
- Frame transmission time must be at least two times maximum propagation time
- Colliding signal can propagate to sending station before the last bit is transmitted.

Ethernet frame structure



Ethernet MAC address

06 : 01 : 02 : 01 : 2C : 4B

6 bytes = 12 hex digits = 48 bits

- ipconfig /all

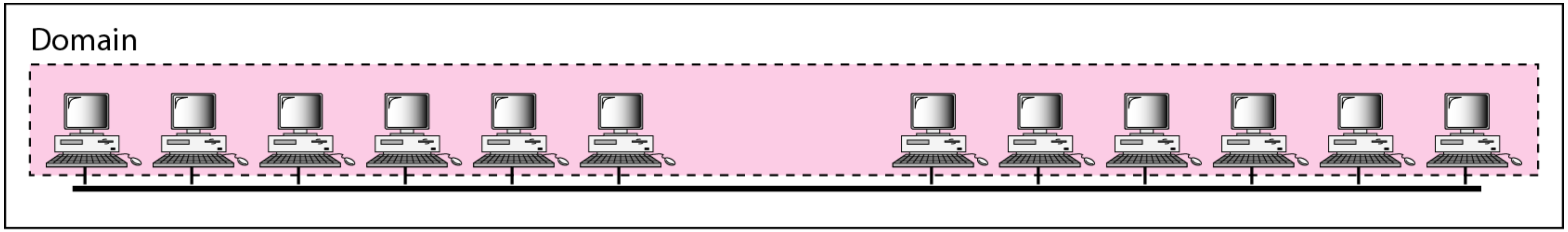
Network addresses

- In a network, all stations need an address so that the data can reach the right destination.
- All computers connected to a standard LAN have a unique physical address.

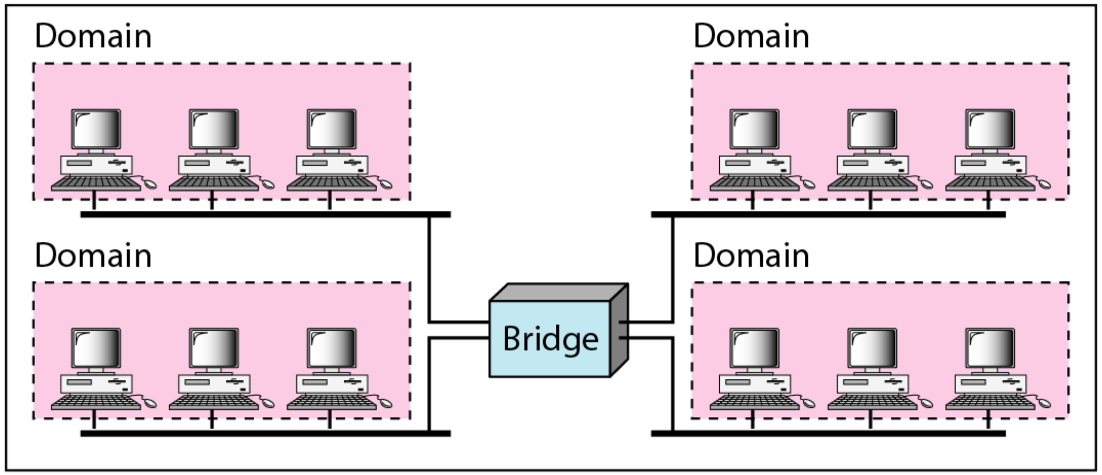
Evolution of Ethernet

CSMA/CD

- Collision domains



a. Without bridging



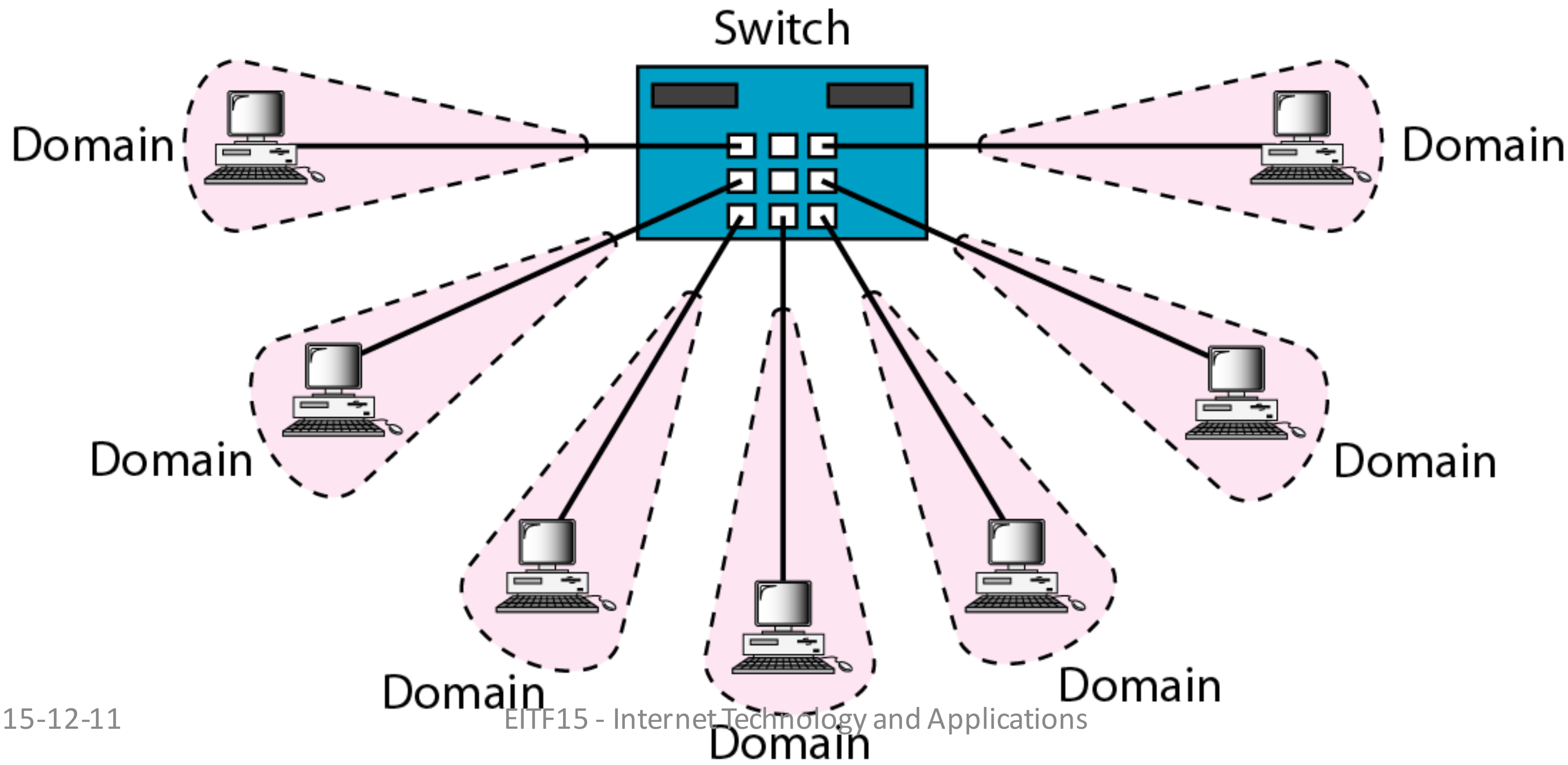
b. With bridging

Switched Ethernet

Switching table

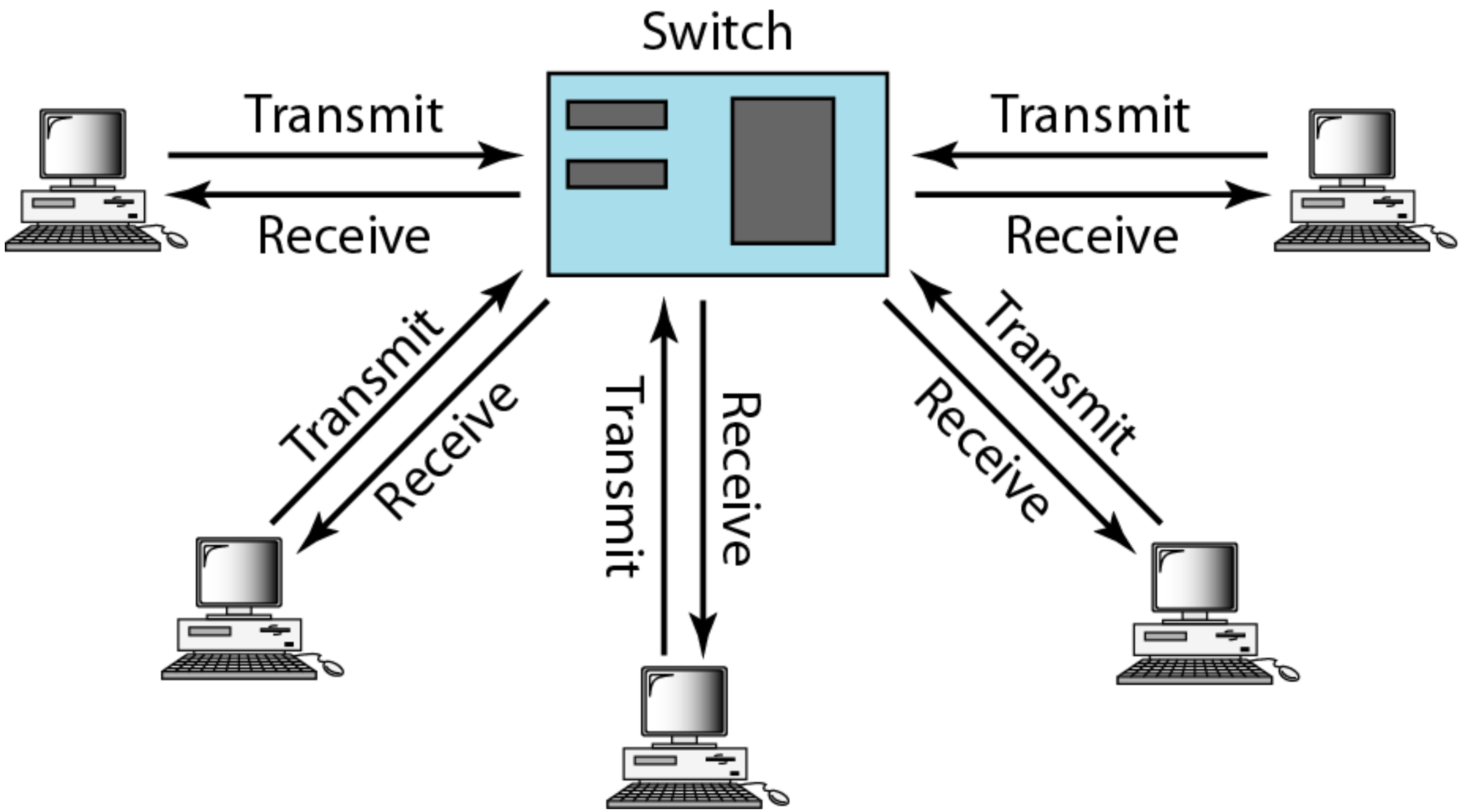
Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

CSMA/CD



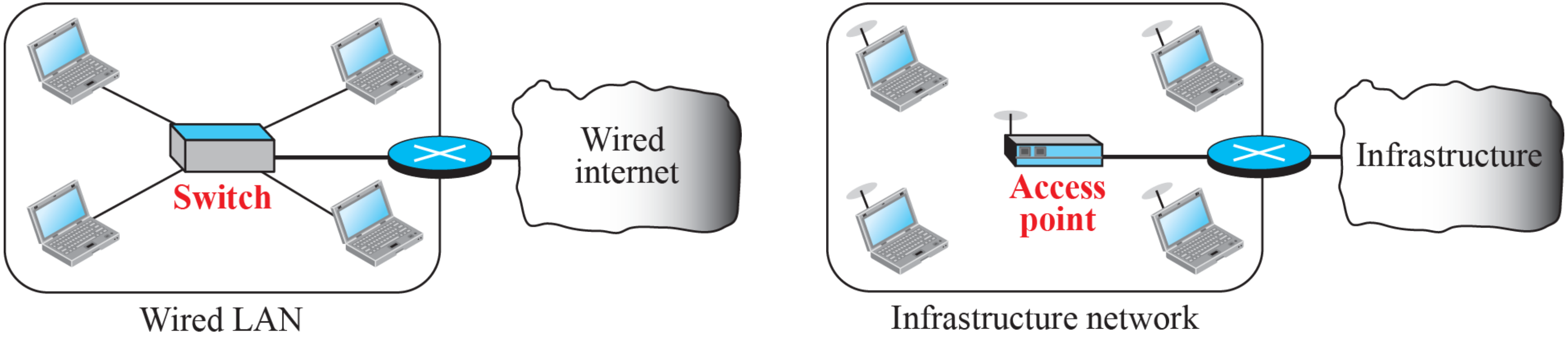
Full-duplex switched Ethernet

CSMA/CD



Wireless LAN

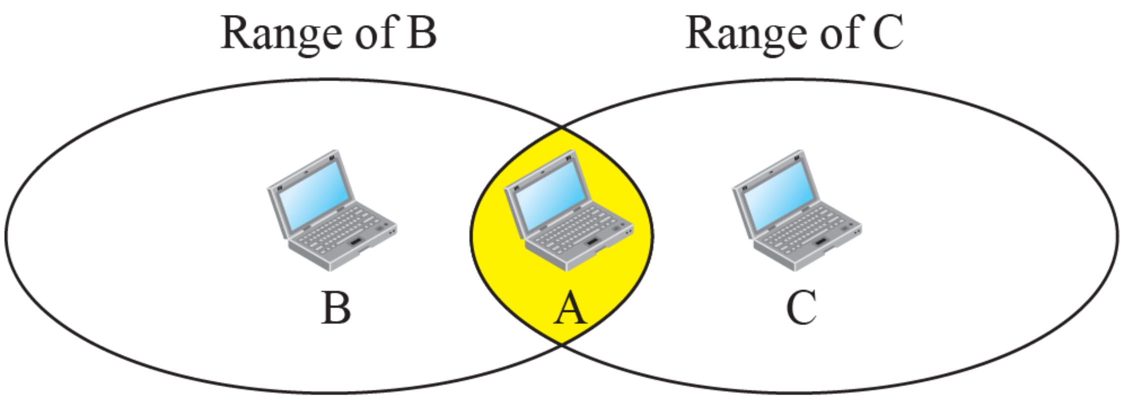
- Popularity of Internet ↑
- Popularity of mobility ↑



- **Basically: A change in medium**
- **Media access technology becomes important**

Hidden terminal problem

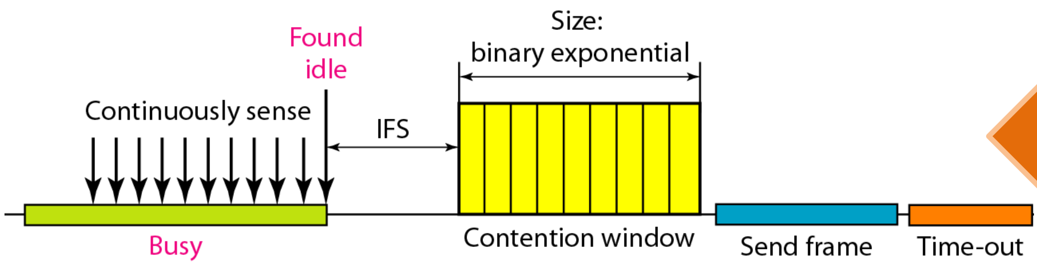
- Infamous in wireless networks
- Prevents collision detection



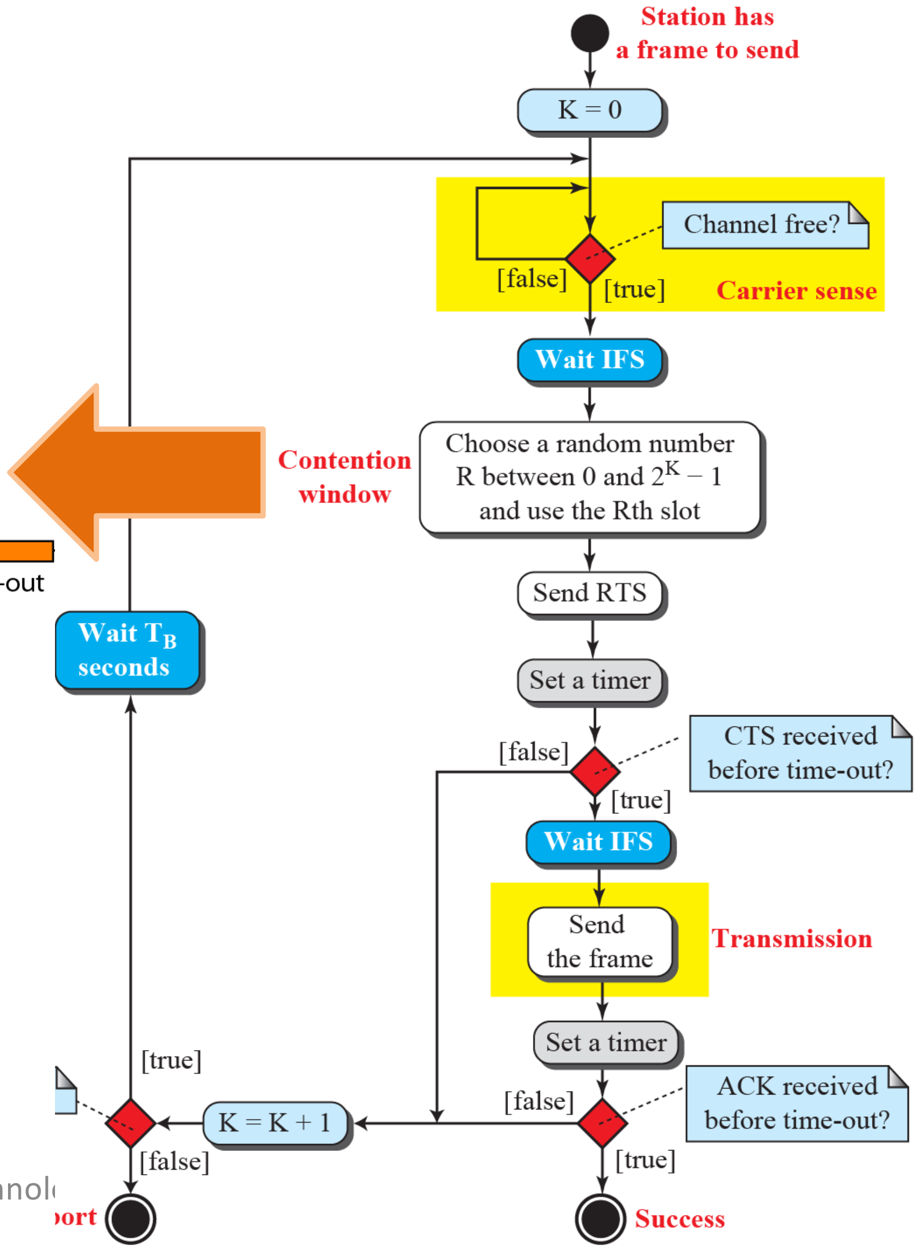
a. Stations B and C are not in each other's range.

CSMA with Collision Avoidance (CSMA/CA)

- Invented for wireless

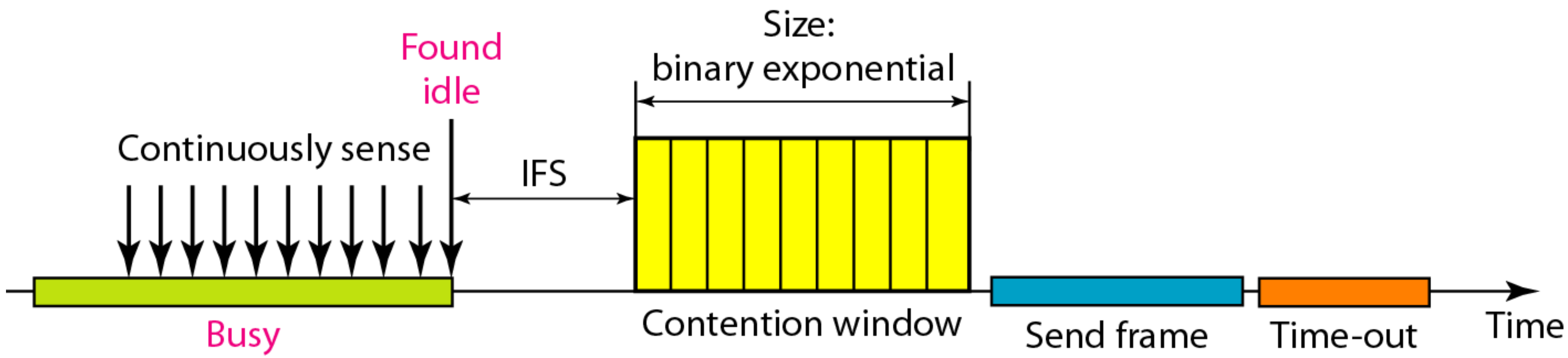


  - Interframe space
  - Contention window
  - RTS/CTS/ACK



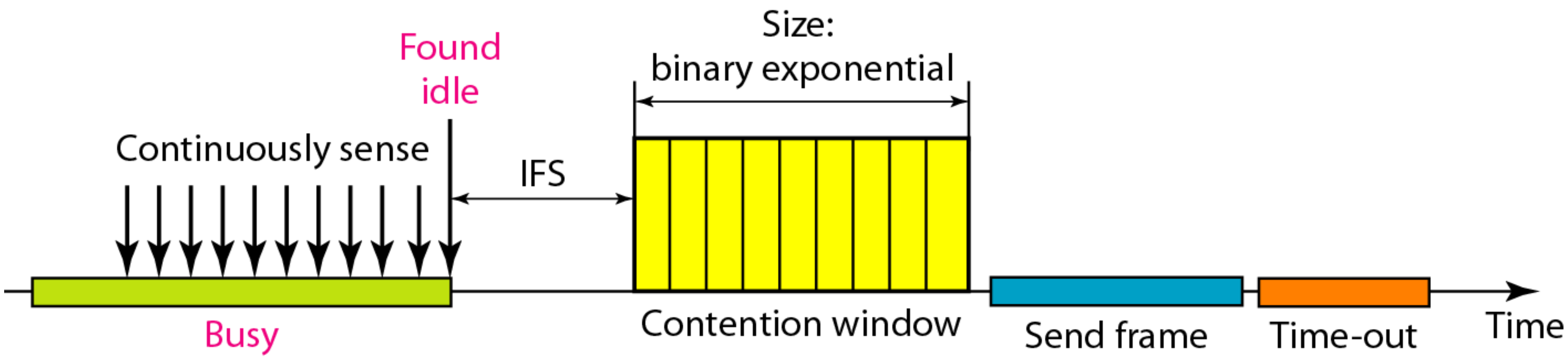
Interframe space

- Do not send immediately when medium idle
- Wait a period of time (interframe space, IFS)
  - A distant station may have already started transmitting
- If, after IFS time, channel still idle, send



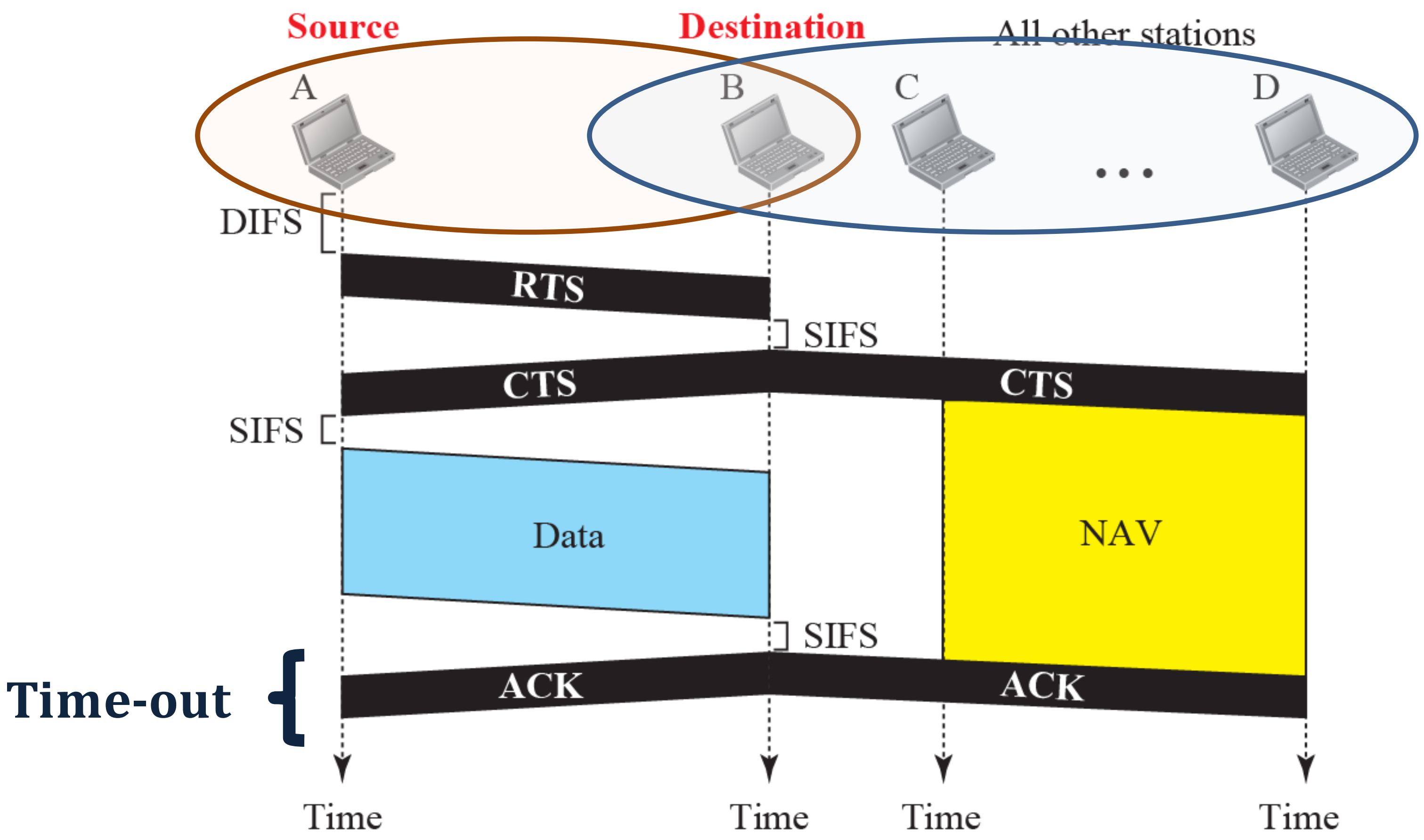
Contention window

- Amount of time divided into slots
- Pick a random number of slots as waiting time
- During waiting time, if channel becomes busy, defer transmission and restart timer when channel idle again



RTS/CTS/ACK

- Solution to hidden terminal problem



See you in 15’ :)

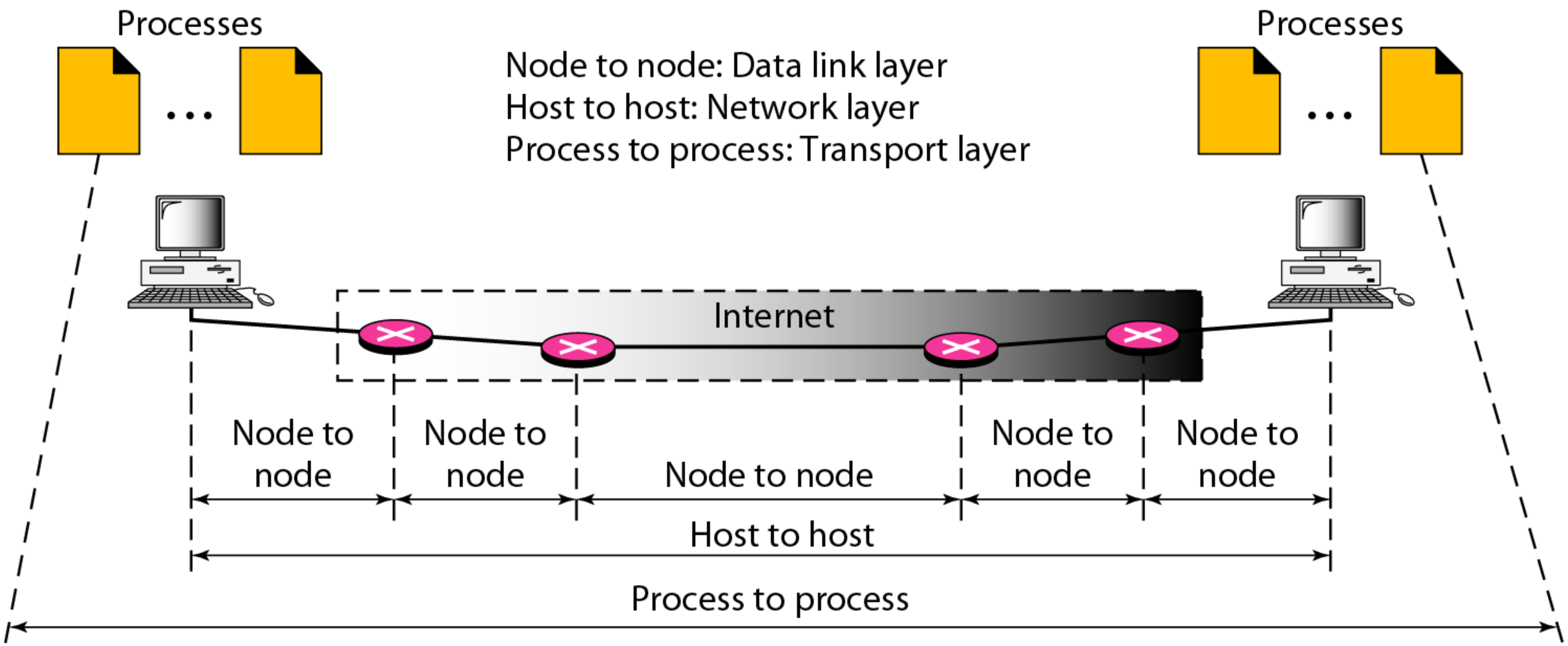
Internet Protocols
-1-
Network Layer

2015, Lecture 04

Kaan Bür

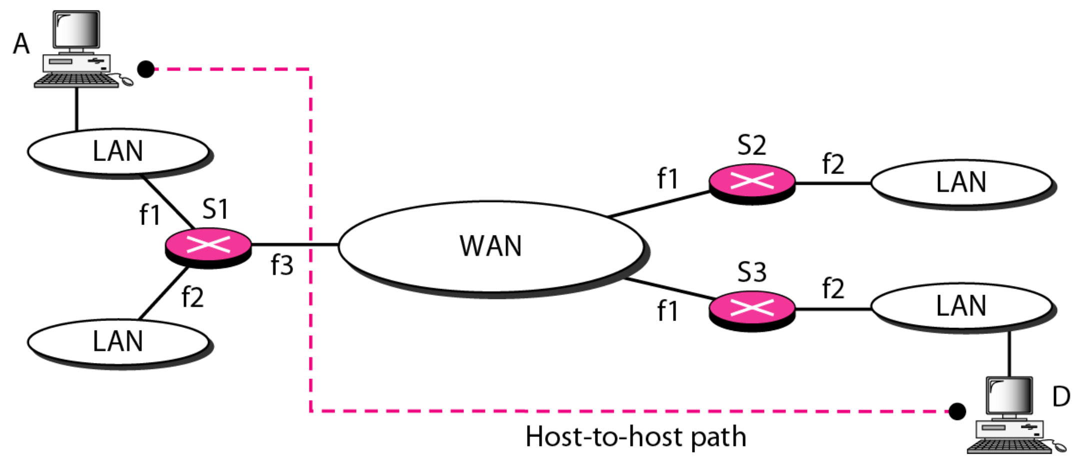
Host-to-host delivery

- Multiple applications even on the same host



Network layer

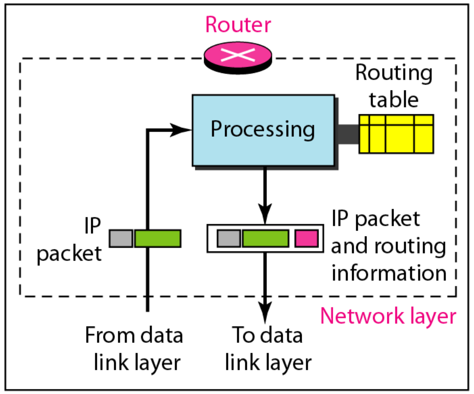
- L3
  - end-to-end



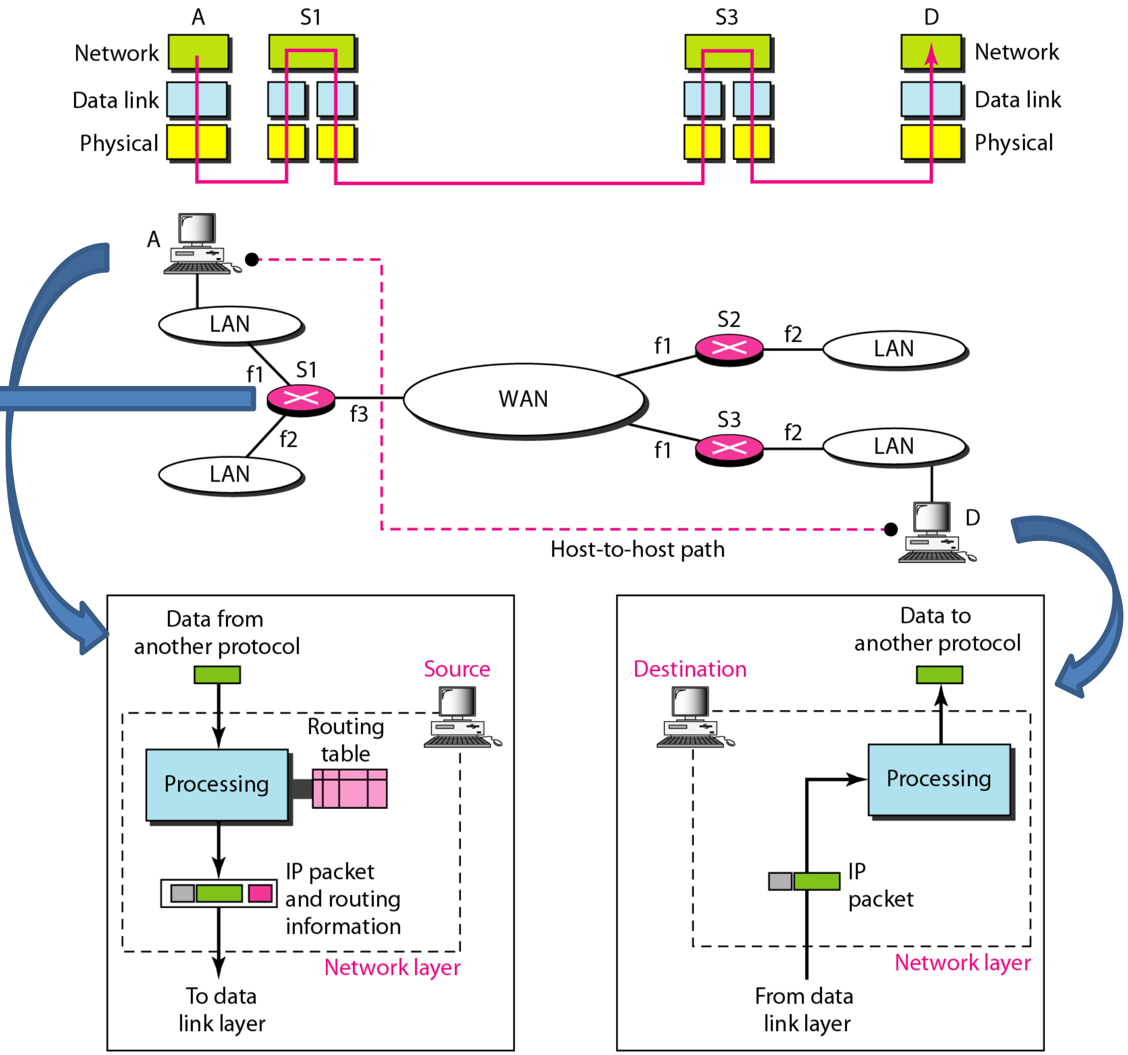
- L2
  - hop-by-hop

Network layer: Routing

- L3 is end-to-end



c. Network layer at a router



a. Network layer at source

b. Network layer at destination

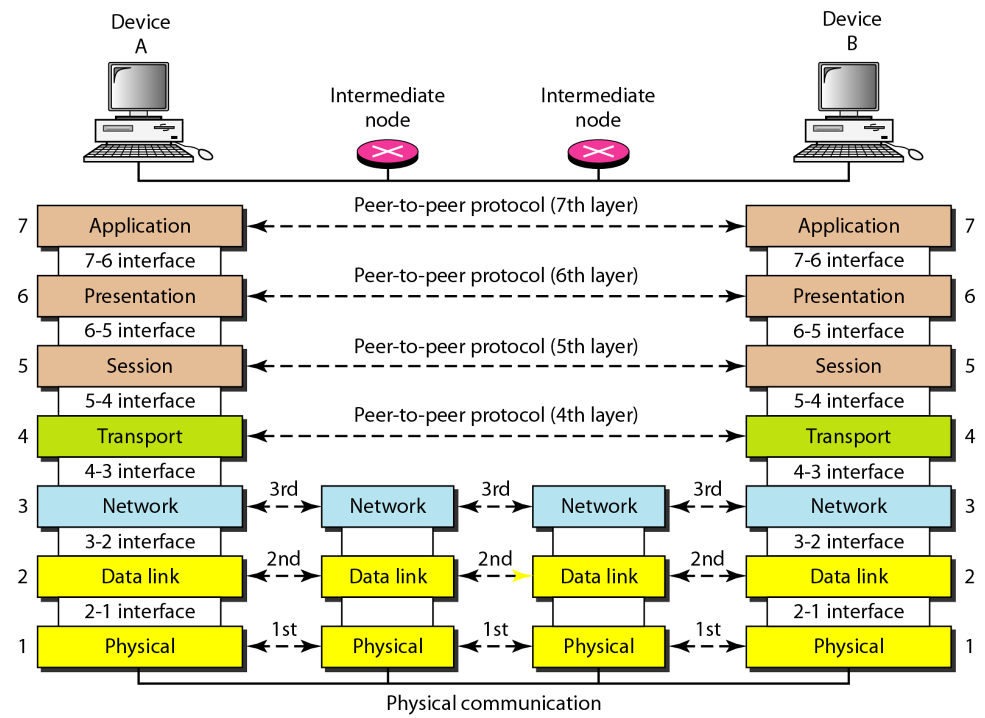
Two functions:

❶ Addressing

❷ Feedback

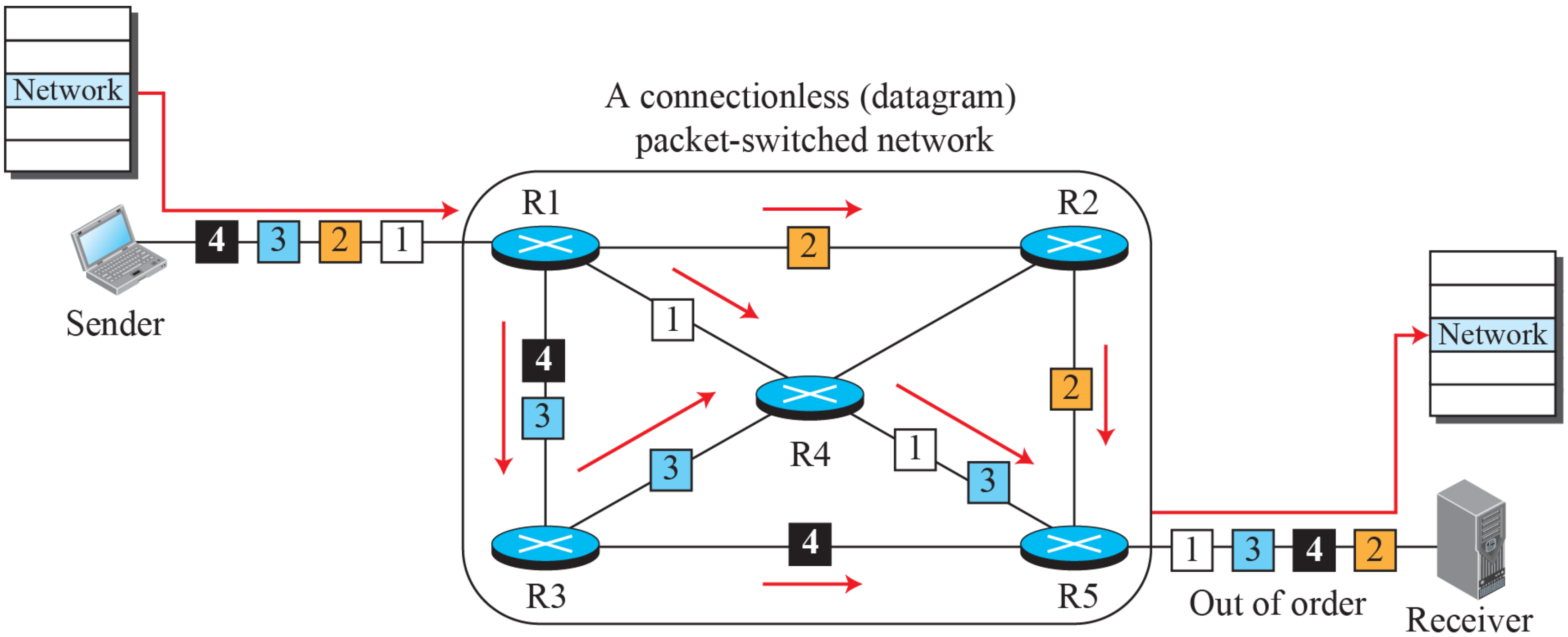
Routing

- Choosing the optimal path
  - Using a cost metric
- Sharing information
  - Central
  - Distributed
- Algorithms
  - Rules and procedures
  - Updates



Packet-switched routing

- Choosing the optimal path
  - Using a cost metric



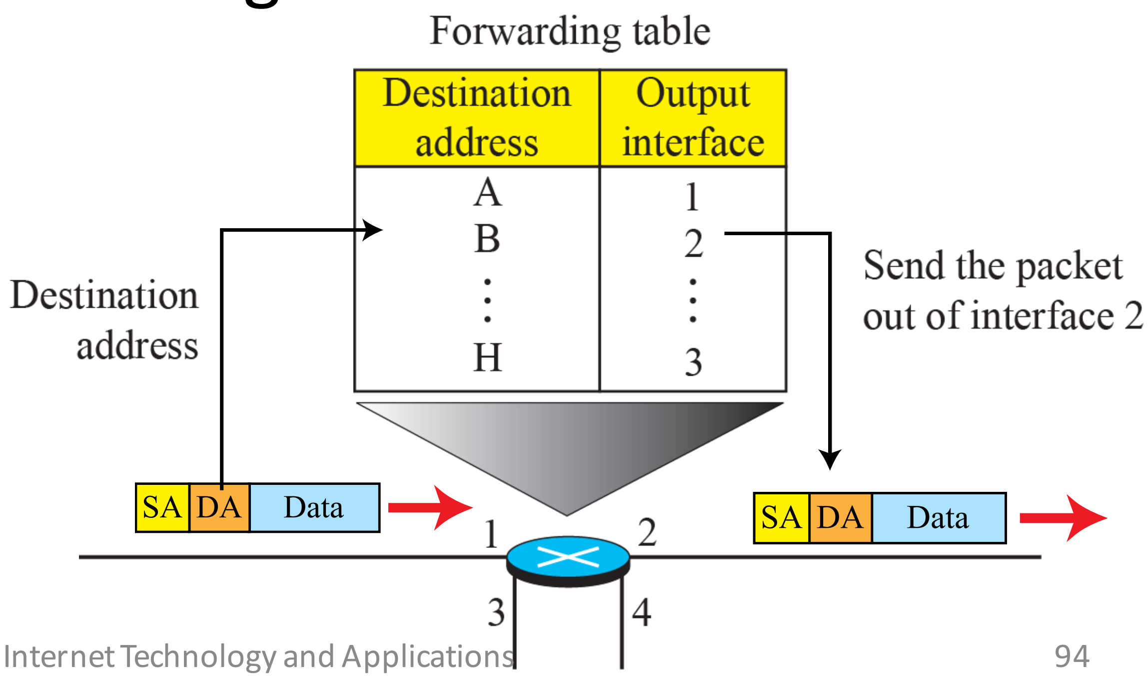
Router

- Internetworking device
  - Passes data packets between networks
  - Checks ***Network Layer*** addresses
  - Uses Routing/forwarding tables

Two functions:

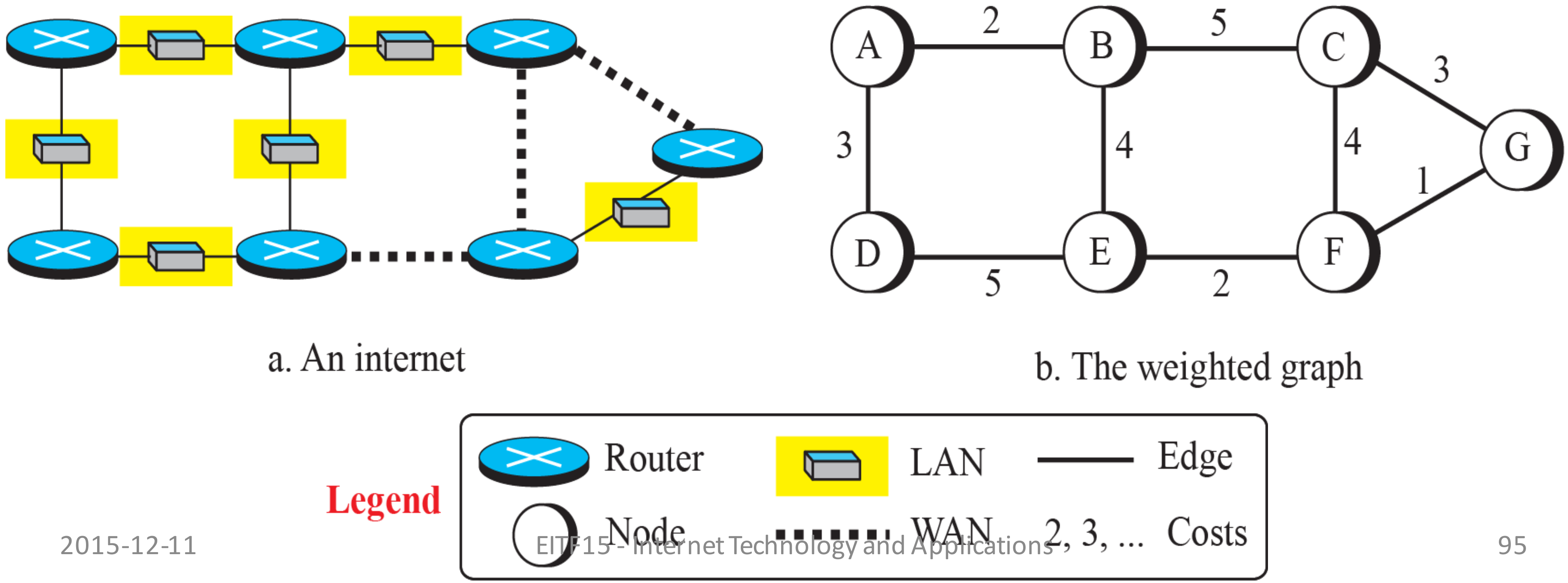
❶ Routing

❷ Forwarding



Routing algorithm

- Find route with least cost between source and destination.
- Update routing tables



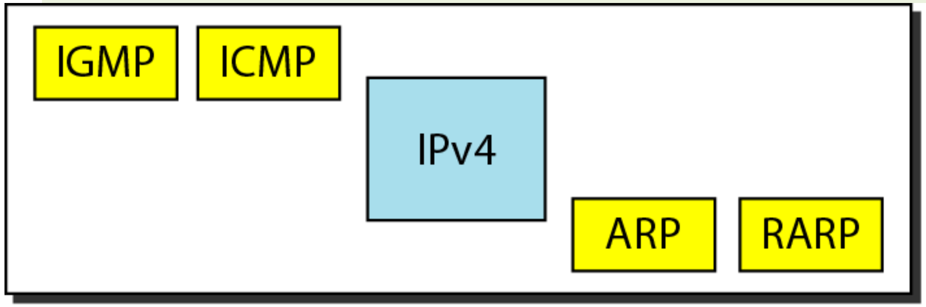
Network layer protocols

- We need a universal address system. This is called the *network address*.
- We need rules for data forwarding. This is called *routing*.
- We need entities connecting several networks together and forwarding data between them. These are called *routers*.

Internet Protocol

IPv4

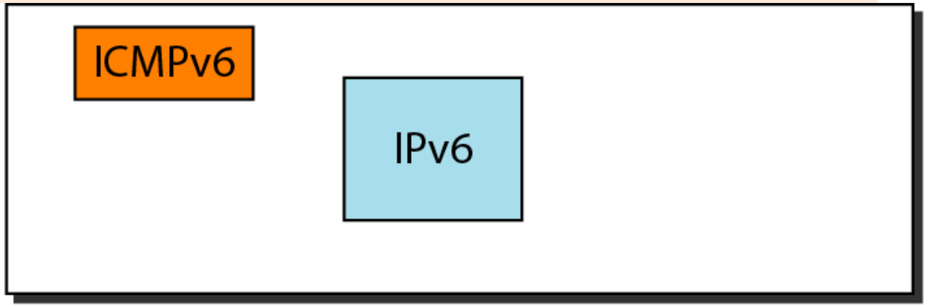
- Addressing scheme
  - Hierarchy
  - Configuration
  - Lookup
- Datagram format



Network layer in version 4

IPv6

- Larger address space
- Better header format
  - Extendible
  - More secure
- Support for QoS

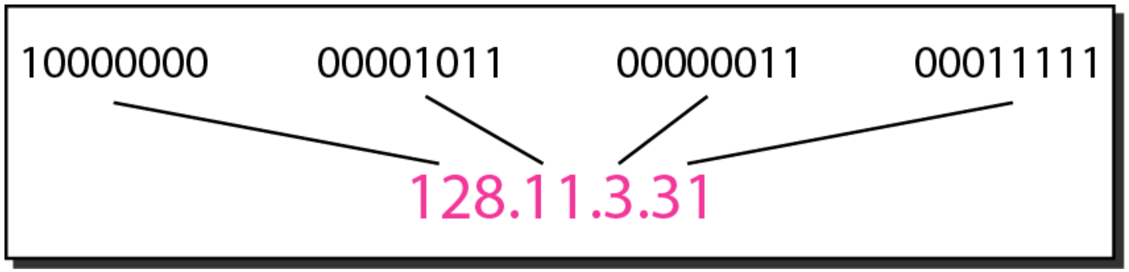


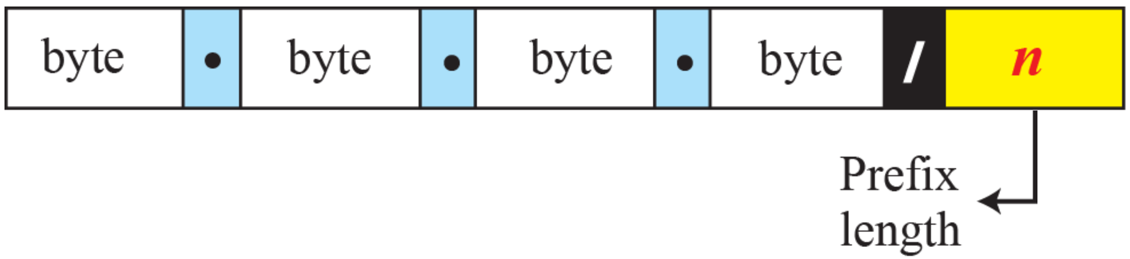
Network layer in version 6

IPv4 addresses

- 32 bits = 4 bytes
- $2^{32} = (2^8)^4 = 256^4 = 4\ 294\ 967\ 296$
- Classful vs. classless hierarchy

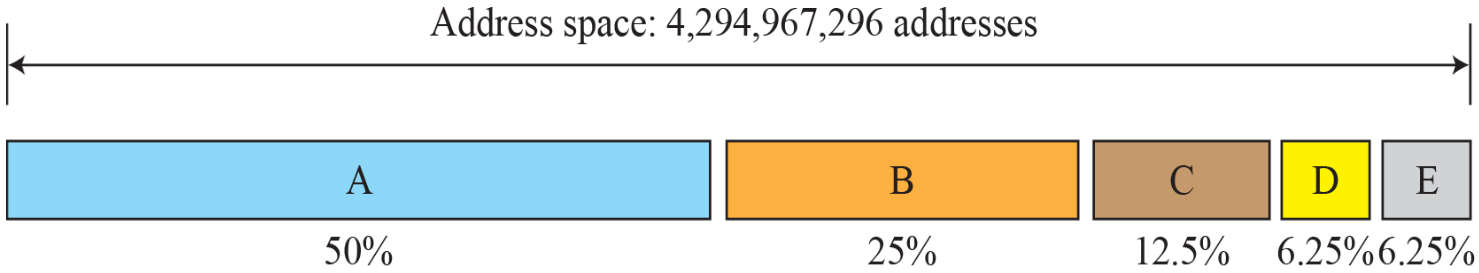
- Notations
  - Dotted decimal
  - Slash (CIDR)

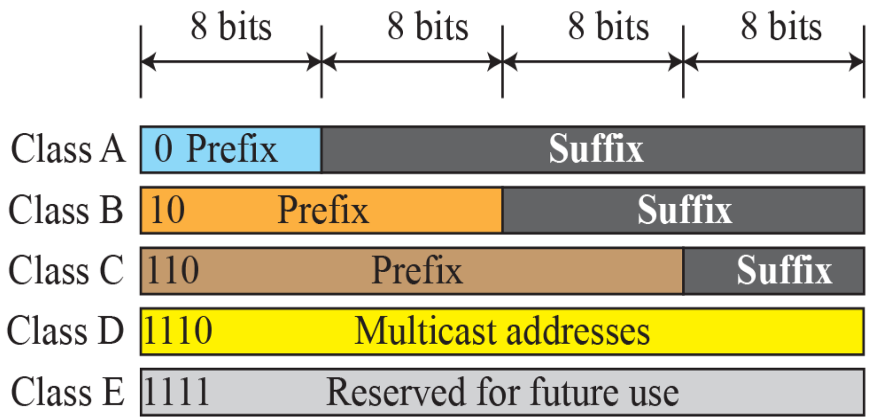




Classful addressing

- Five address classes defined: A, B, C, (D and E)





Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

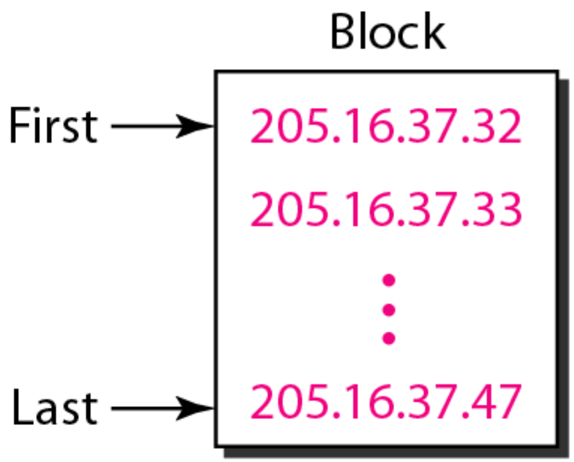
Classful addressing

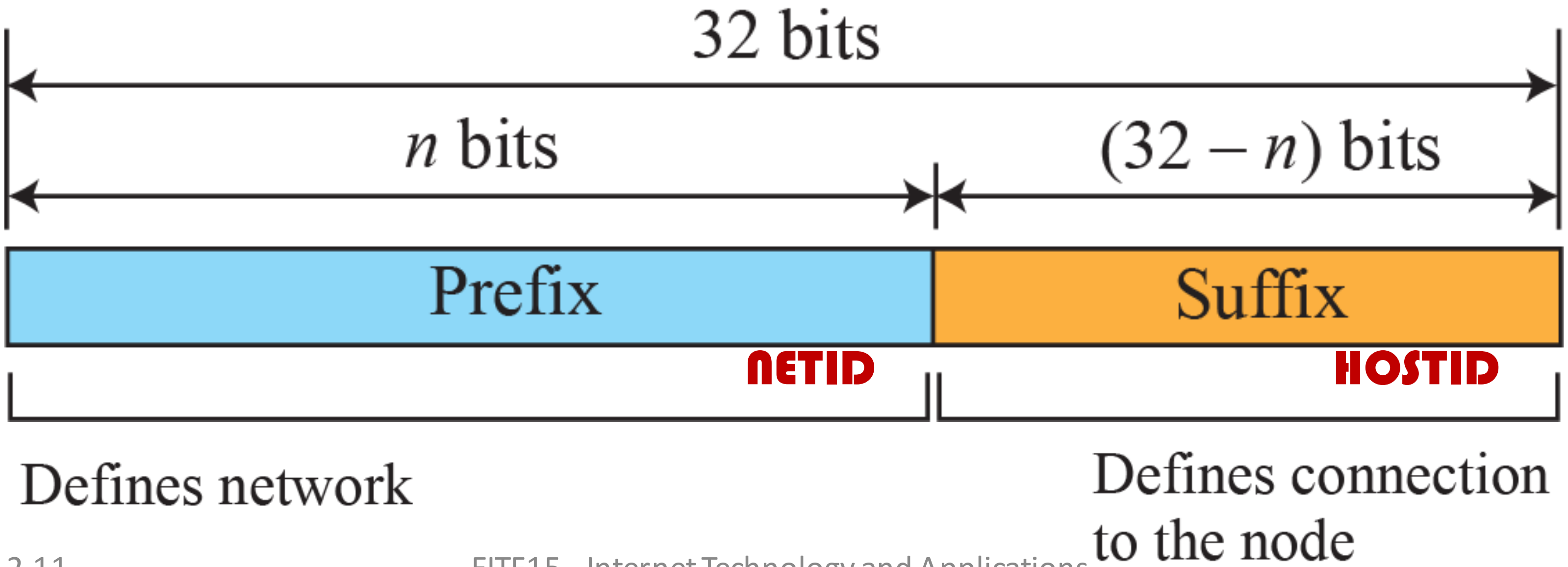
- Organizations can only get addresses in one of the predefined blocks.

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast

Classless addressing

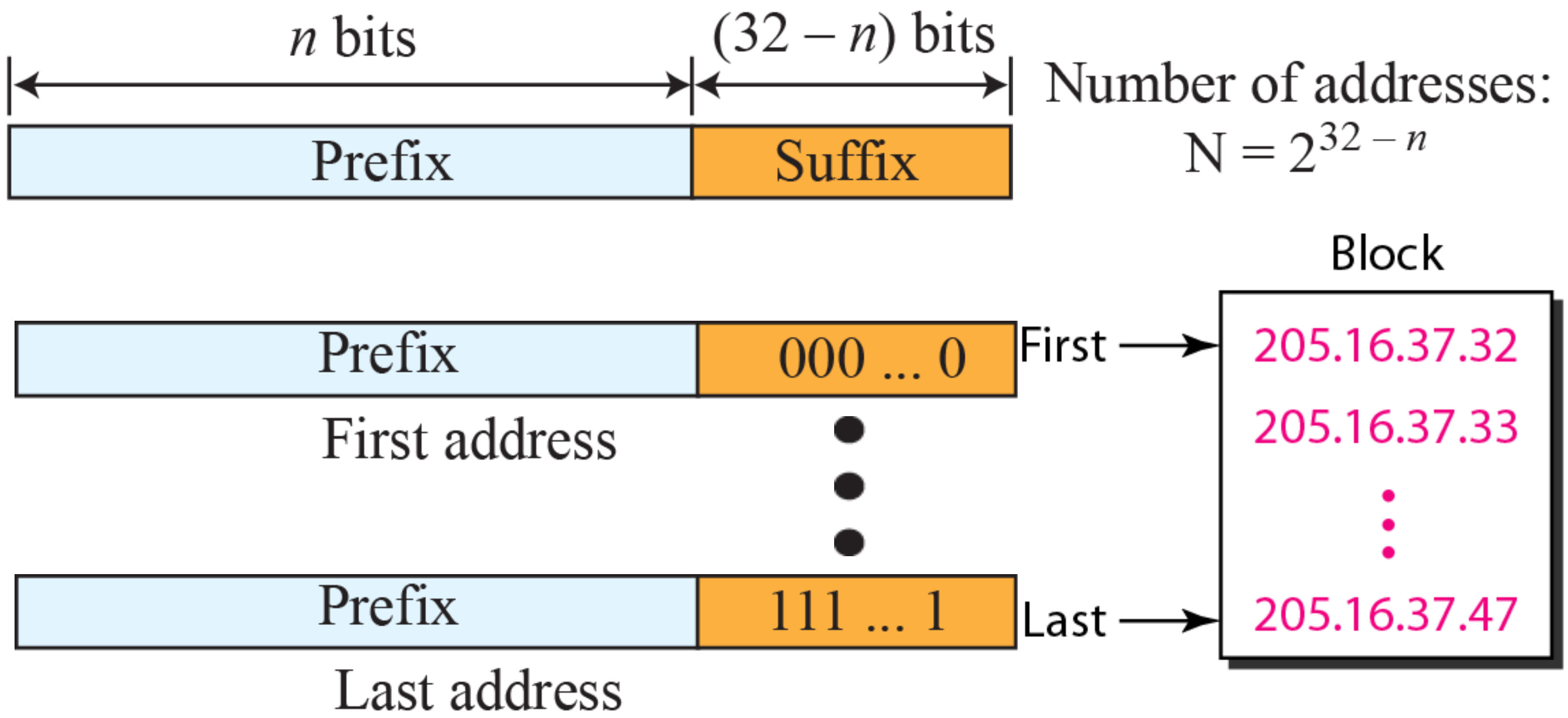
- Addresses in blocks
  - Block size power of 2
  - $N = 2^{32-n}$
  - First address divisible by N





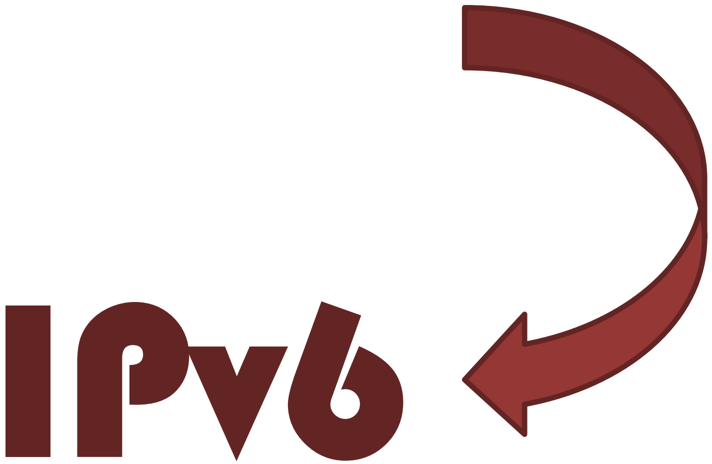
Exercise: Classless addressing

- CIDR = slash notation with mask ***/n***
- 205.16.37.39/28



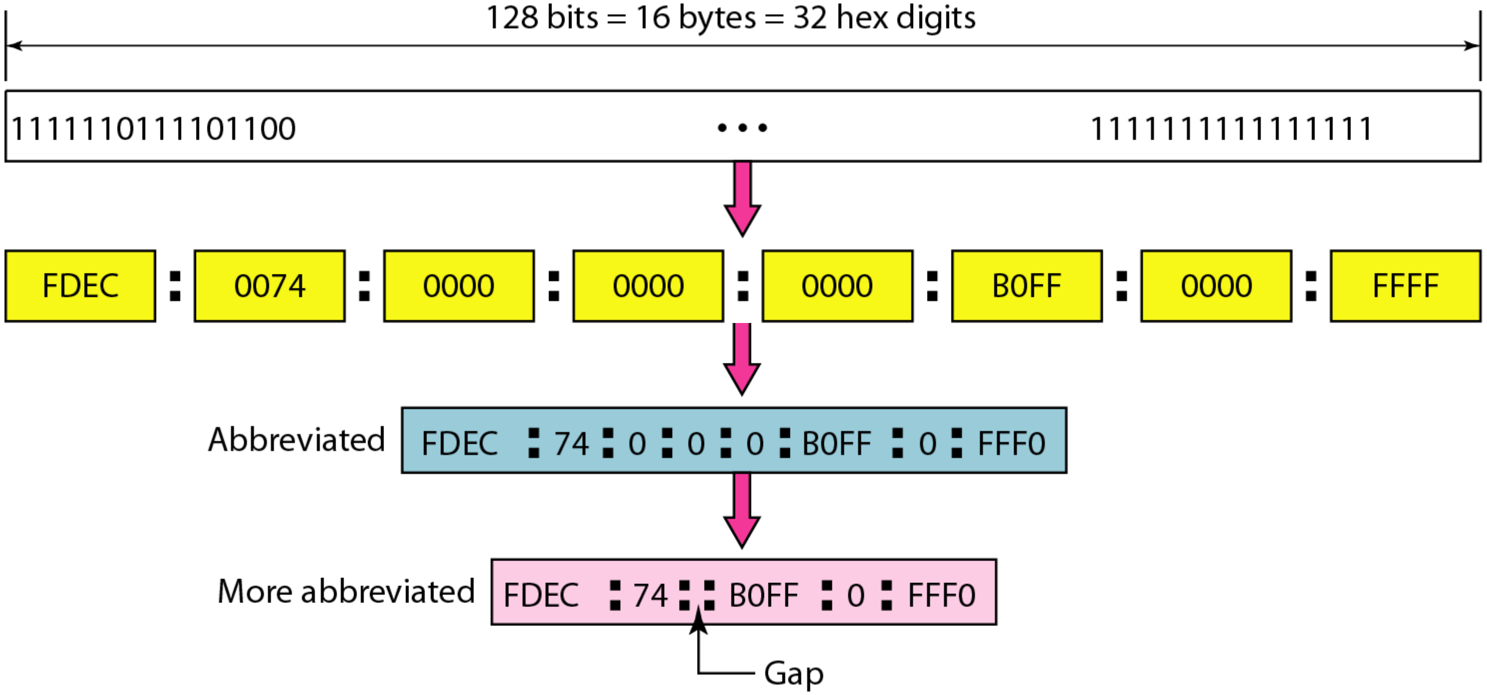
Problems with IPv4

- Address space too small
- Not designed for real-time applications
- No support for encryption and authentication



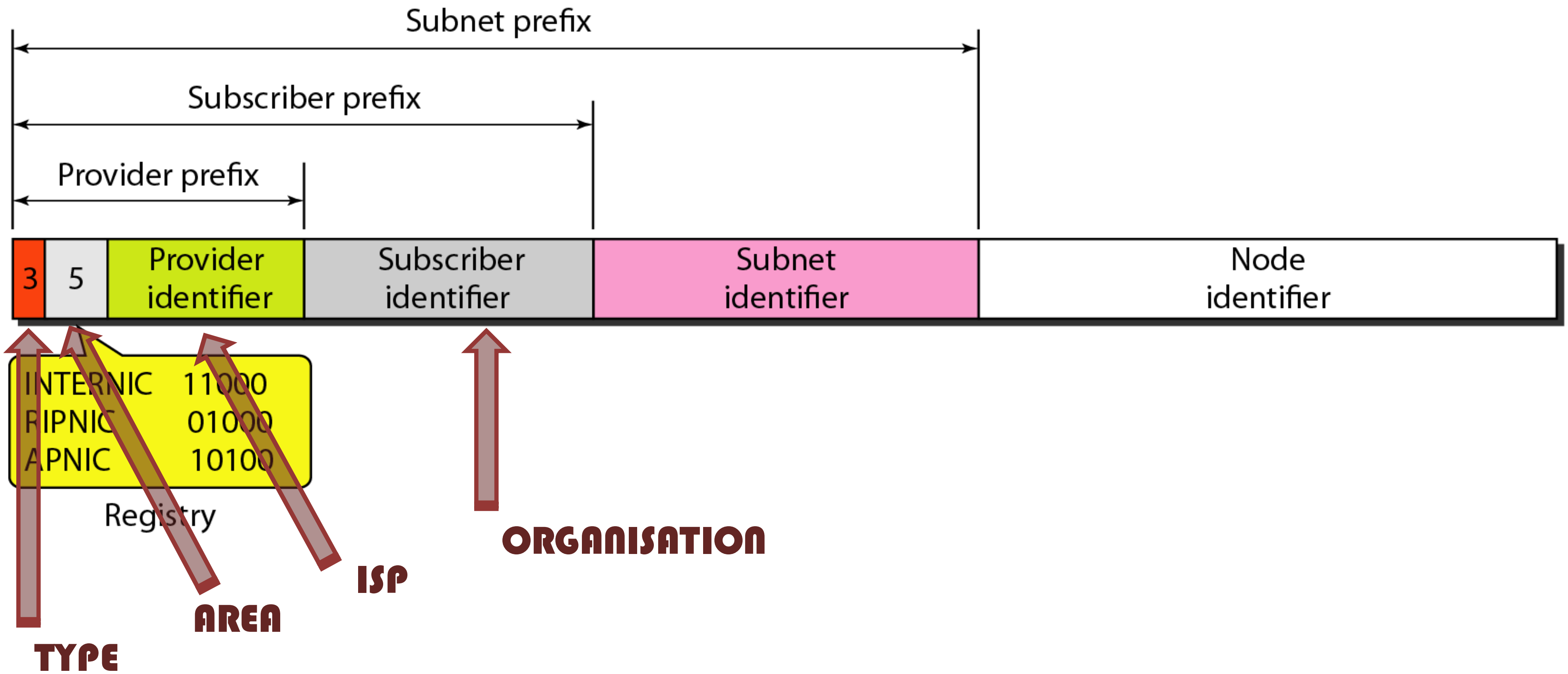
IPv6 addresses

- 128 bits = 16 bytes
- $2^{128} = 2^{32} \cdot 2^{96} > 3 \cdot 10^{35}$
- Notations



Global unicast addresses

- Identify individual computers



IPv6 and QoS

Flow label

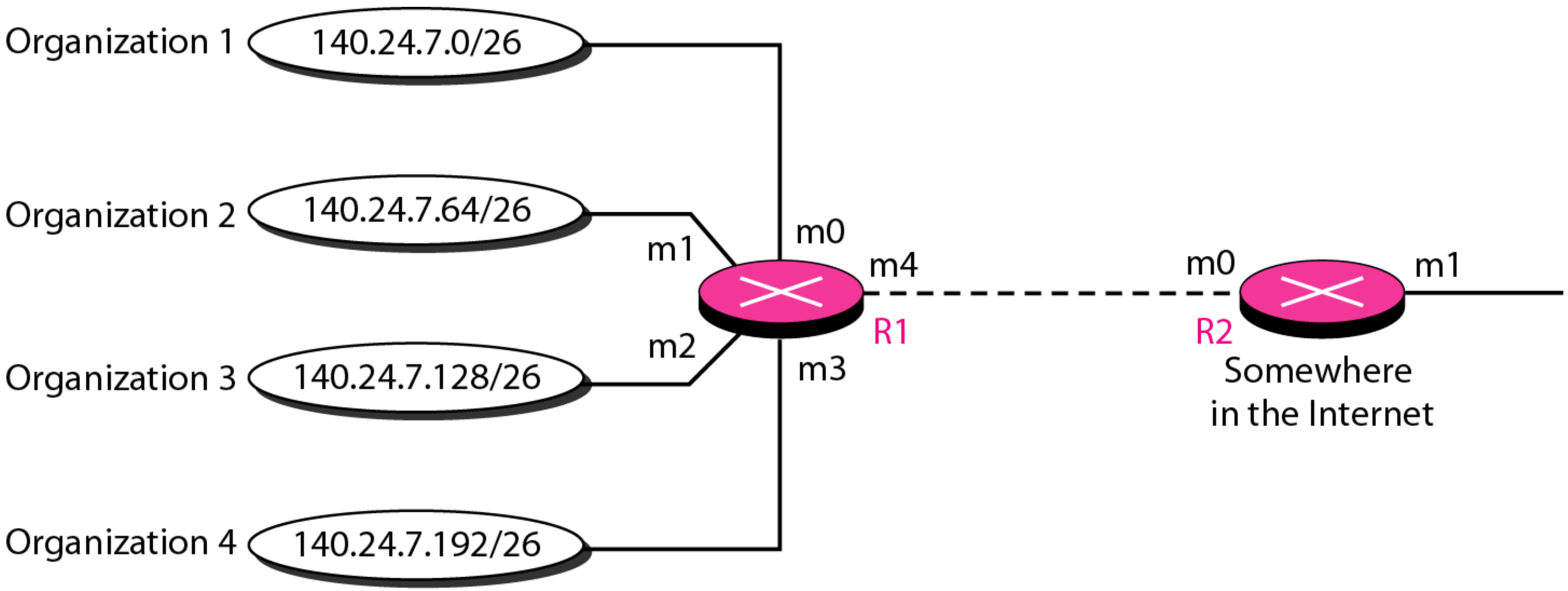
- Identification of a stream
  - TCP sessions
  - Virtual connections
- Processing
  - Flow label table
  - Forwarding table
- Routing
  - Algorithms still necessary
  - But not run for every packet!

CROSS-LAYER?

Traffic class

- Classification of packets
  - Queueing schemes
  - Relation to delay
- TCP vs. UDP
  - Congestion-controlled
  - Non-congestion-controlled
- Other protocols
  - RTP
  - RSVP

Forwarding: Address aggregation



Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/26	140.24.7.192	----------	m3
/0	0.0.0.0	Default	m4

Routing table for R1

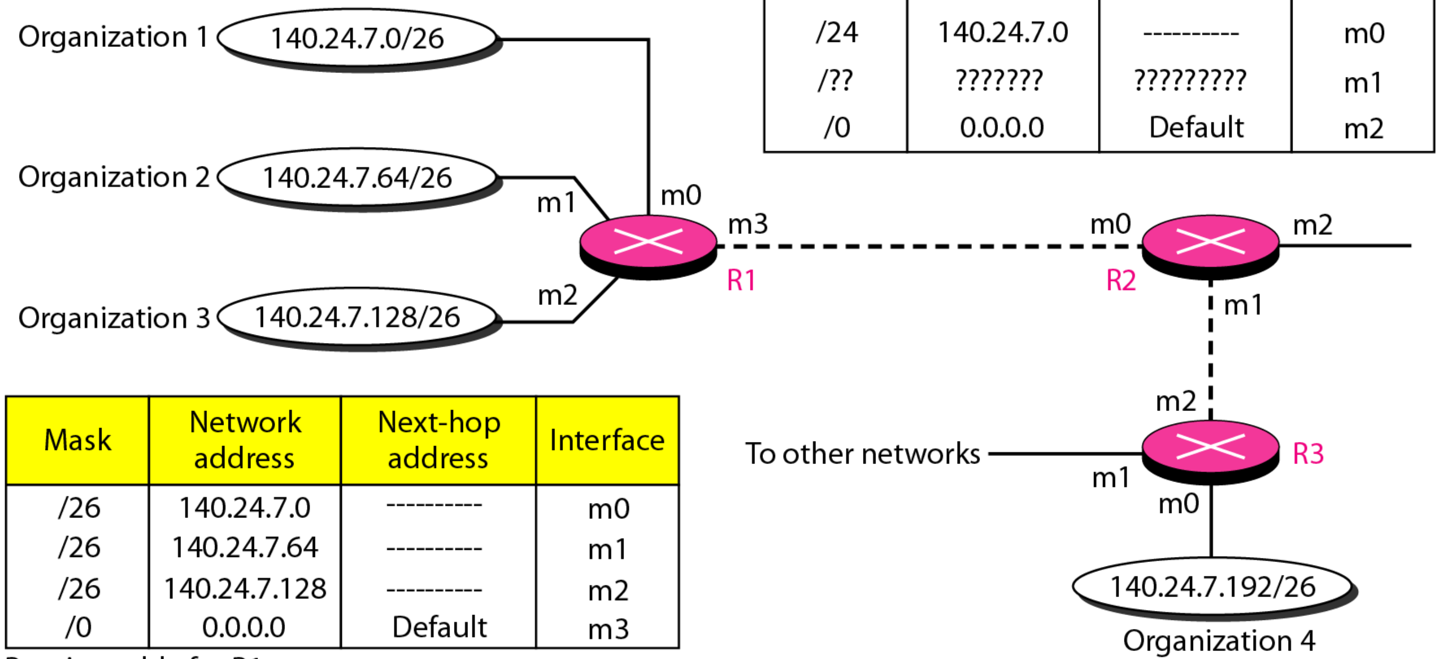
Mask	Network address	Next-hop address	Interface
/24	140.24.7.0	----------	m0
/0	0.0.0.0	Default	m1

Routing table for R2

Forwarding: Longest mask matching

Routing table for R2

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m1
/24	140.24.7.0	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2



Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/0	0.0.0.0	Default	m3

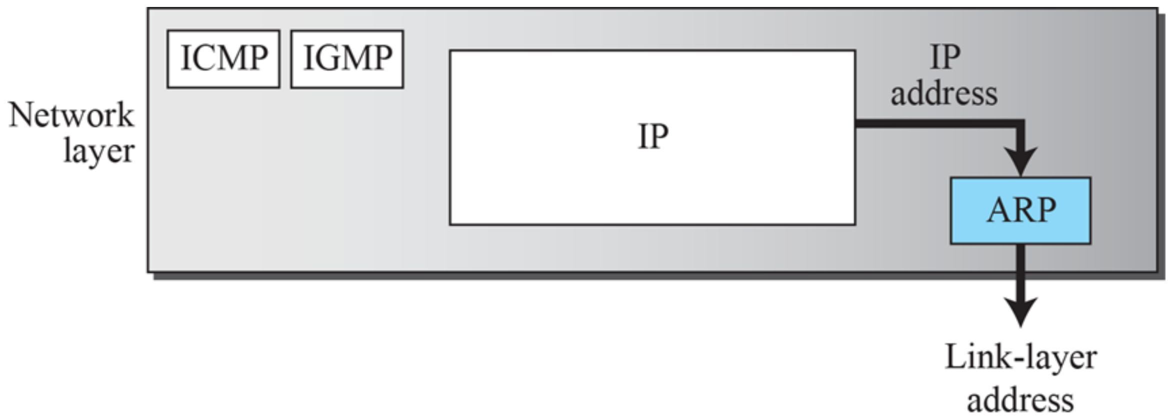
Routing table for R1

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

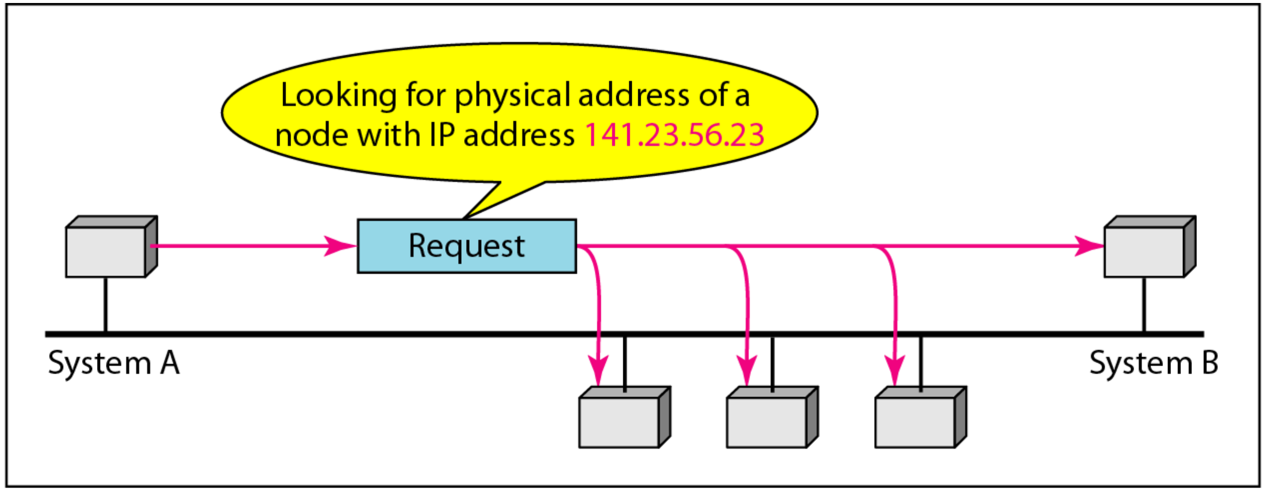
Routing table for R3

Address Resolution Protocol (ARP)

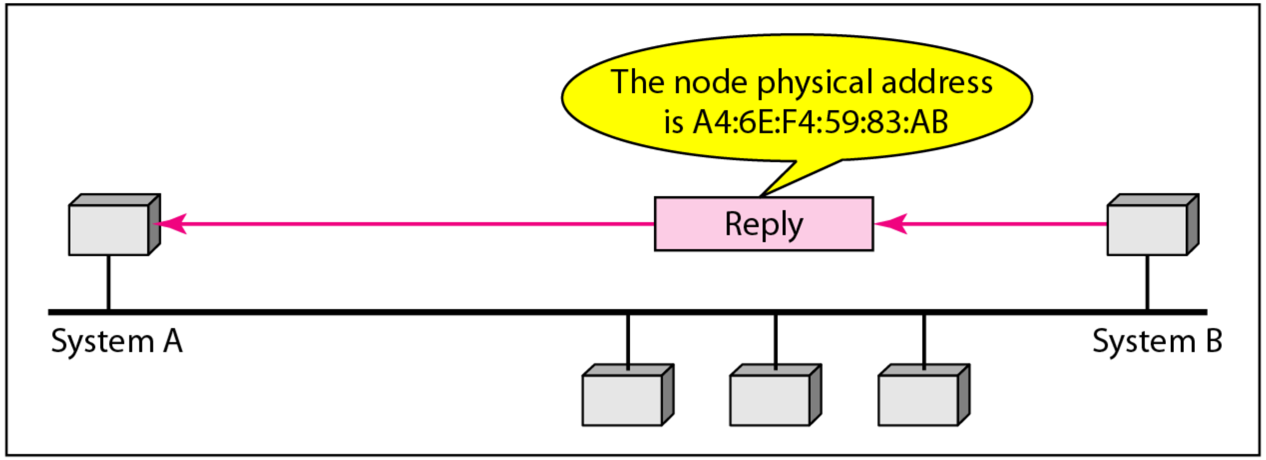
- Mapping of IP addresses to MAC addresses
- Internet
  - Network of networks connected by routers
- Routers/hosts need information
  - Logical (IP) → physical (MAC)



ARP request and reply

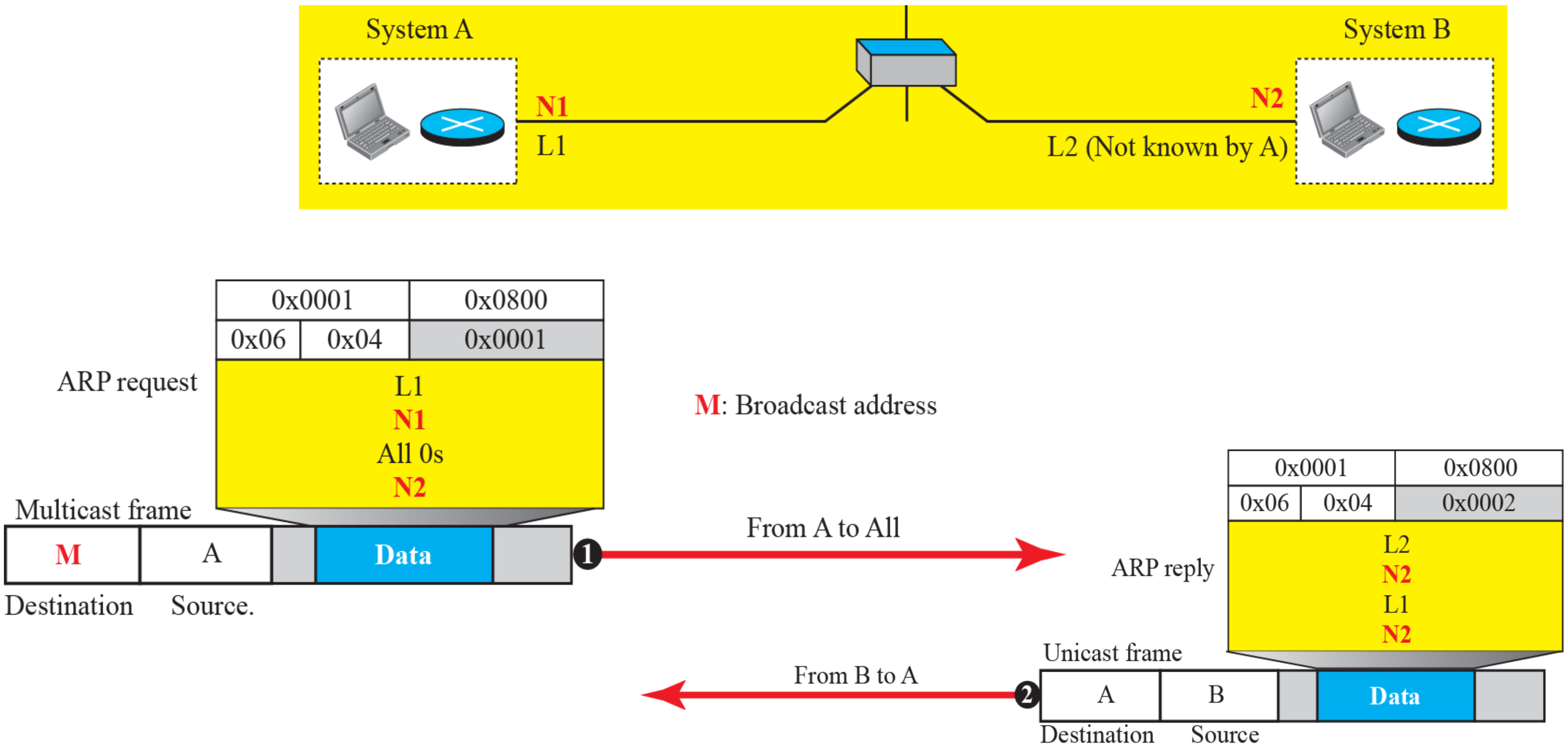


a. ARP request is broadcast



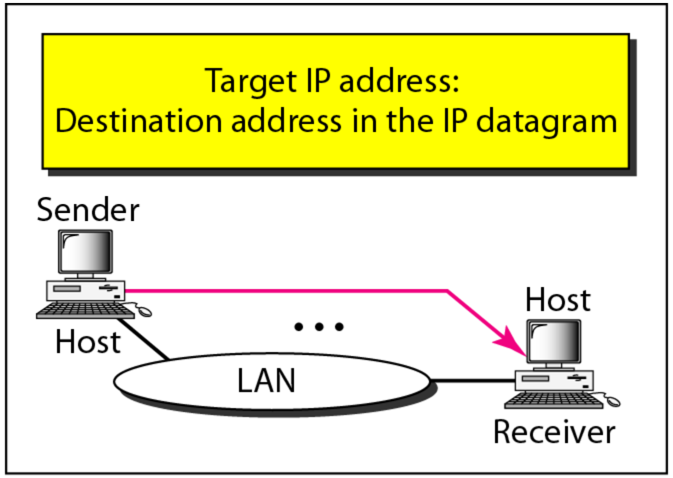
b. ARP reply is unicast

ARP example

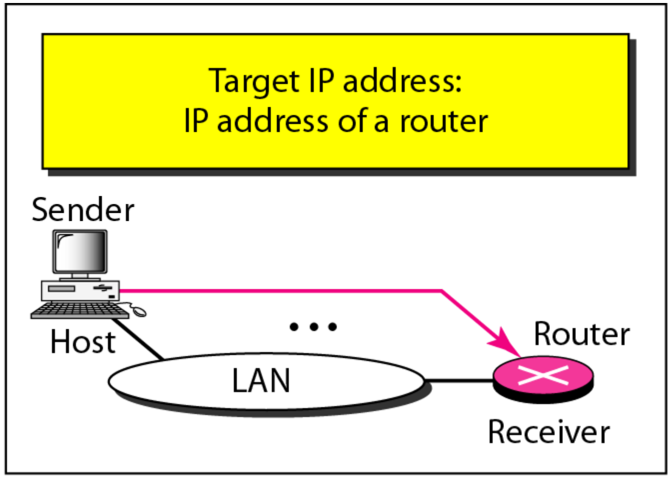


System A
System B
N1
L1
N2
L2 (Not known by A)
ARP request
0x0001
0x0800
0x06
0x04
0x0001
L1
N1
All 0s
N2
M: Broadcast address
Multicast frame
M
A
Data
Destination
Source.
From A to All
ARP reply
0x0001
0x0800
0x06
0x04
0x0002
L2
N2
L1
N2
Unicast frame
From B to A
A
B
Data
Destination
Source

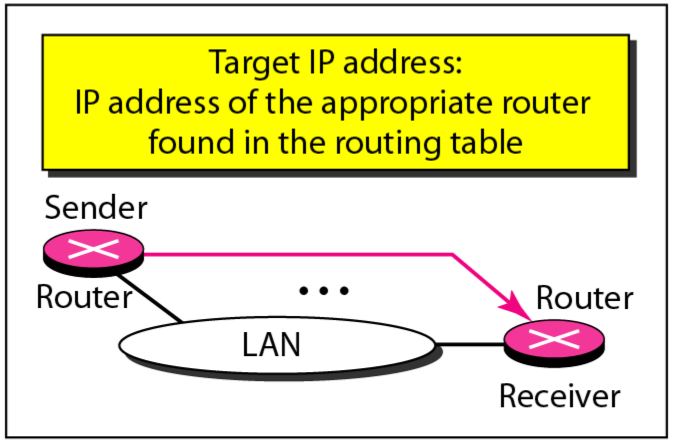
Four use cases for ARP



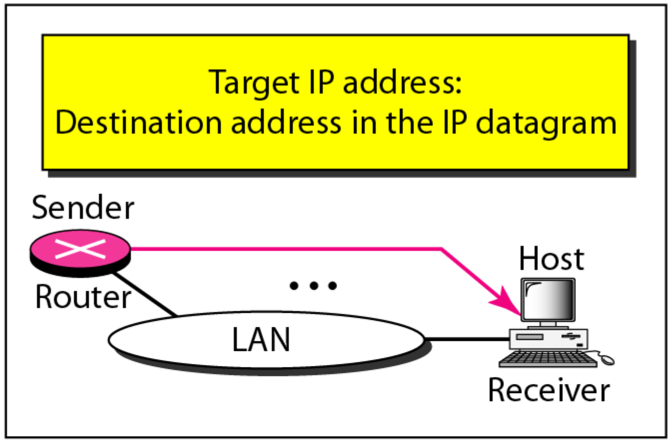
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.



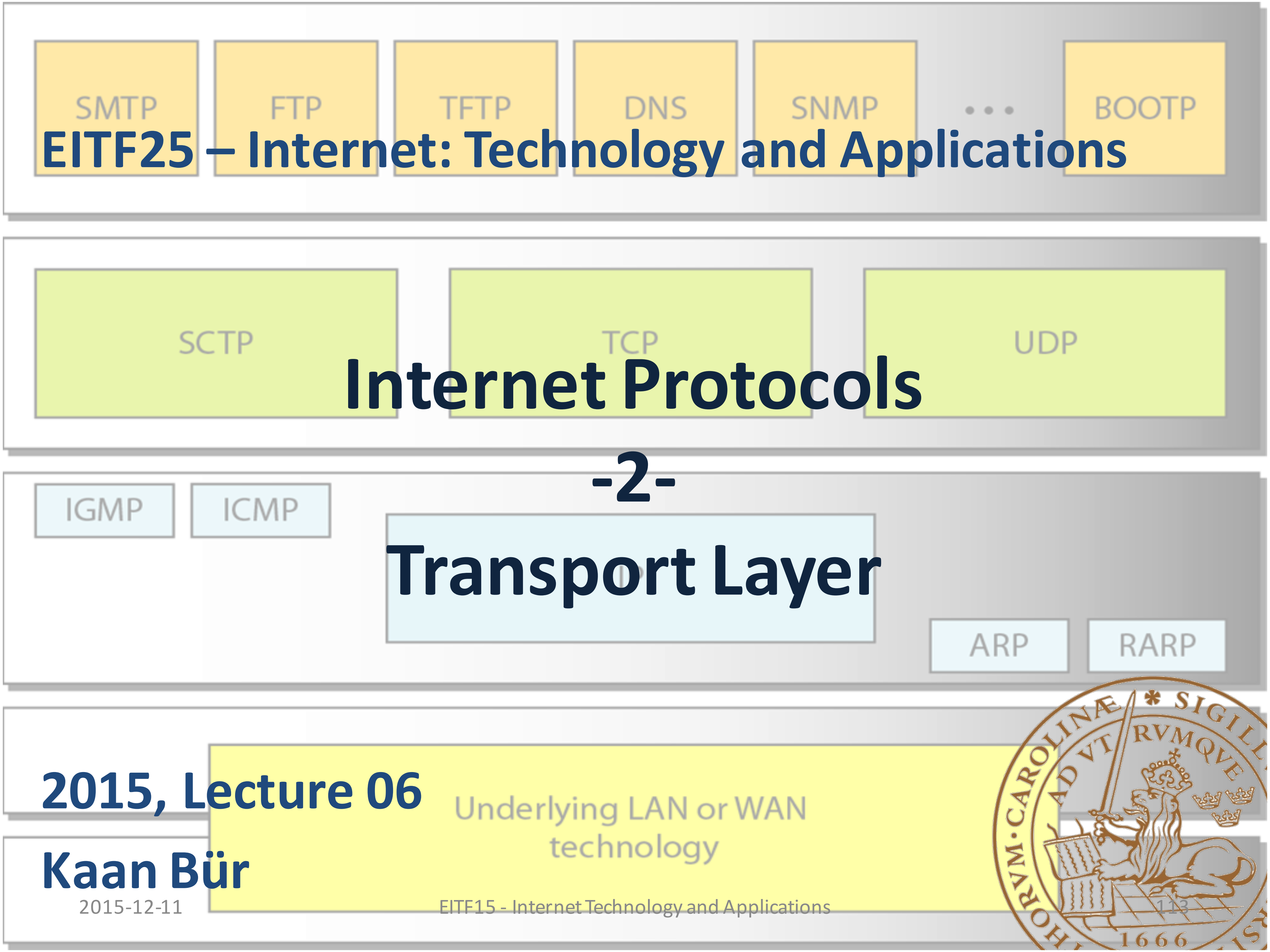
Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



Case 4. A router receives a packet to be sent to a host on the same network.

EITF25 – Internet: Technology and Applications

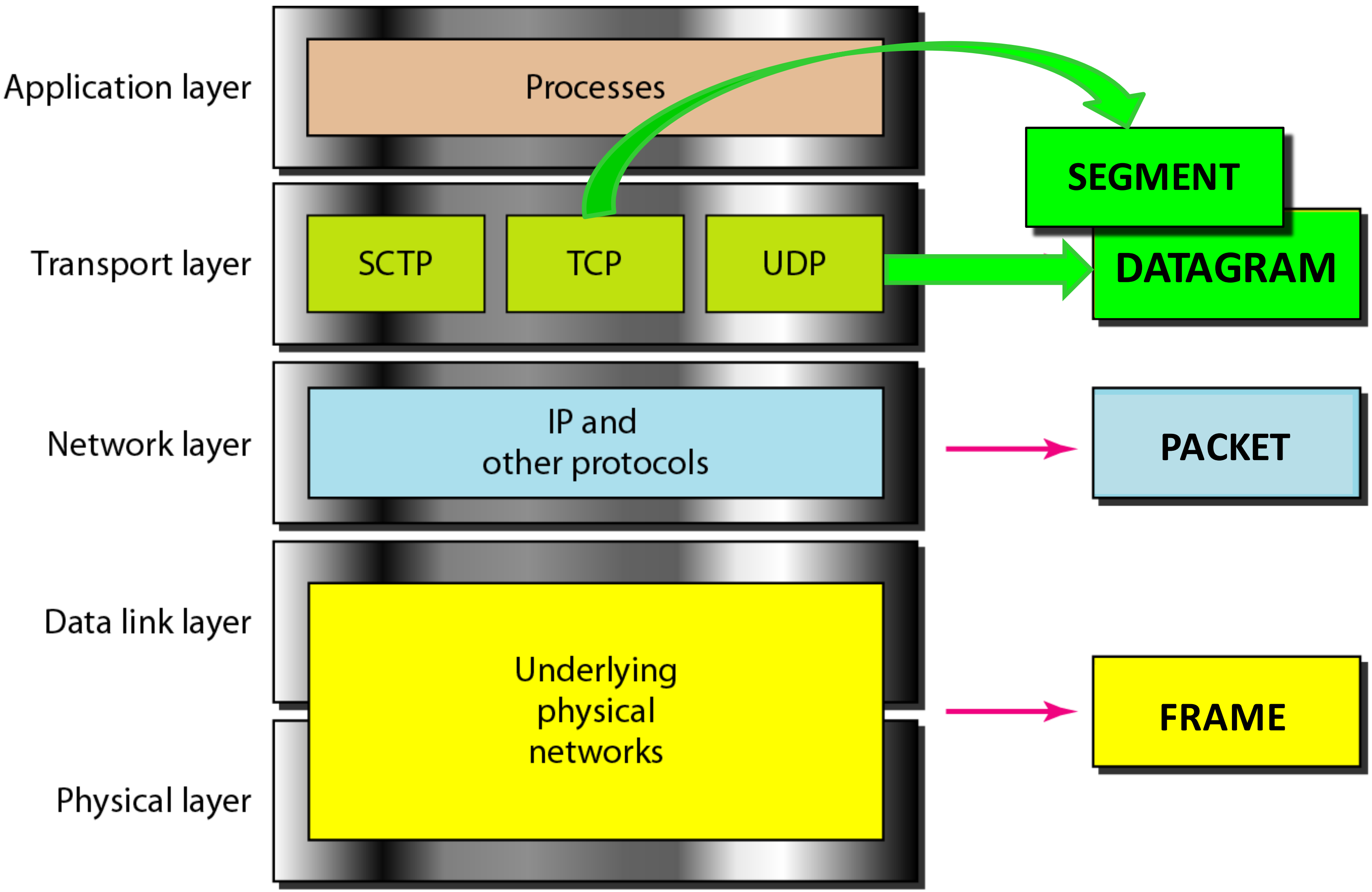
Internet Protocols
-2-
Transport Layer



2015, Lecture 06

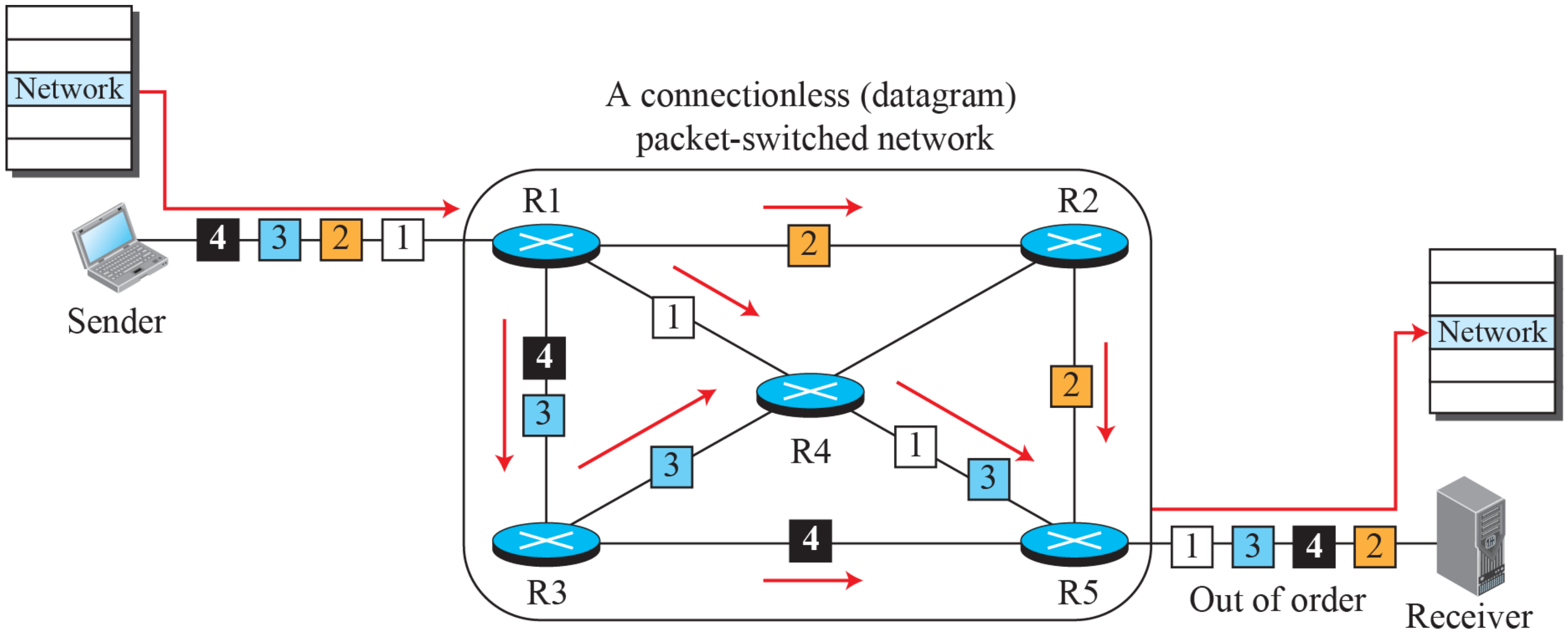
Kaan Bür

TCP/IP model and data units CORRECTION

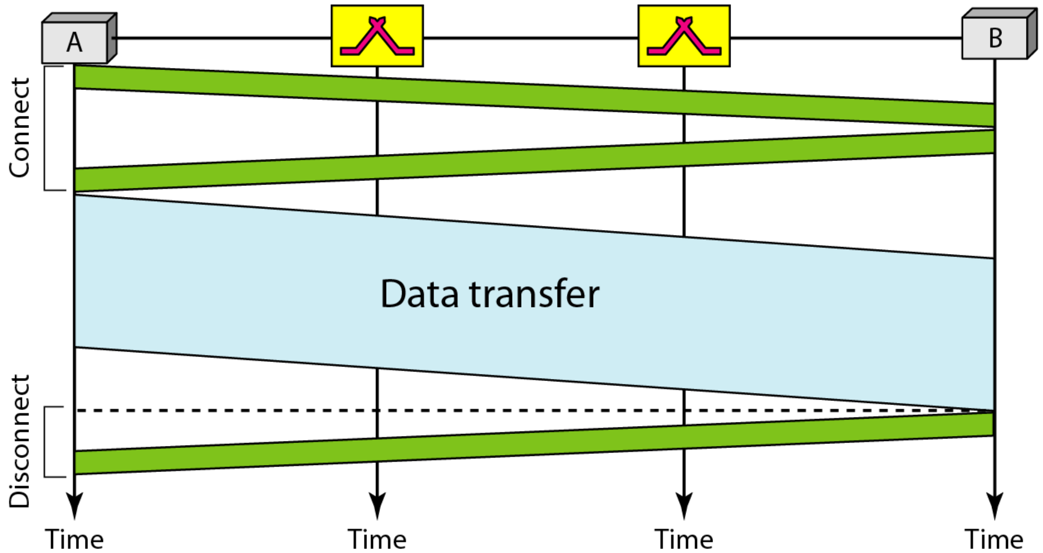


Network vs. Transport Layer

- L3



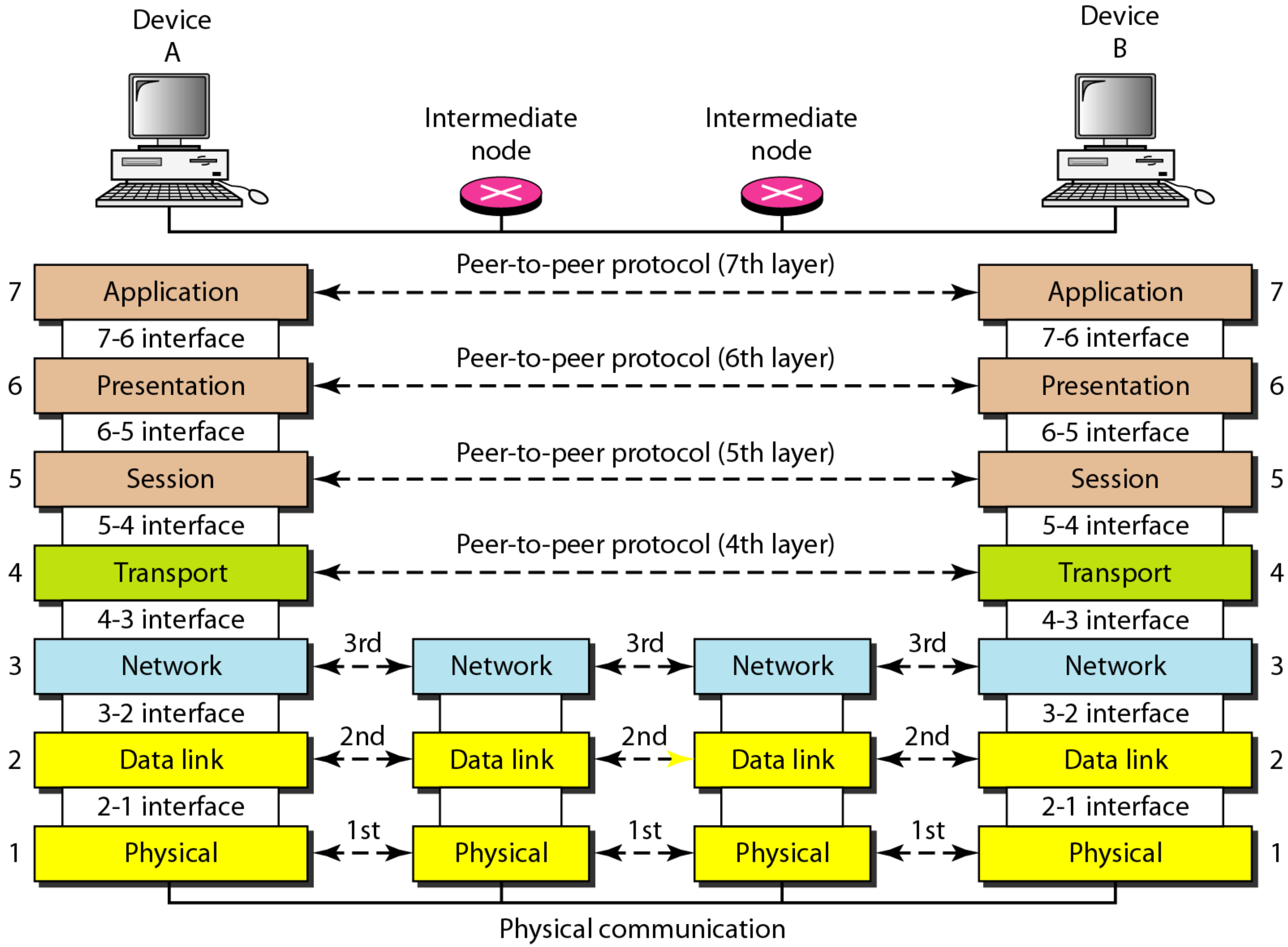
- L4?



Transport Layer

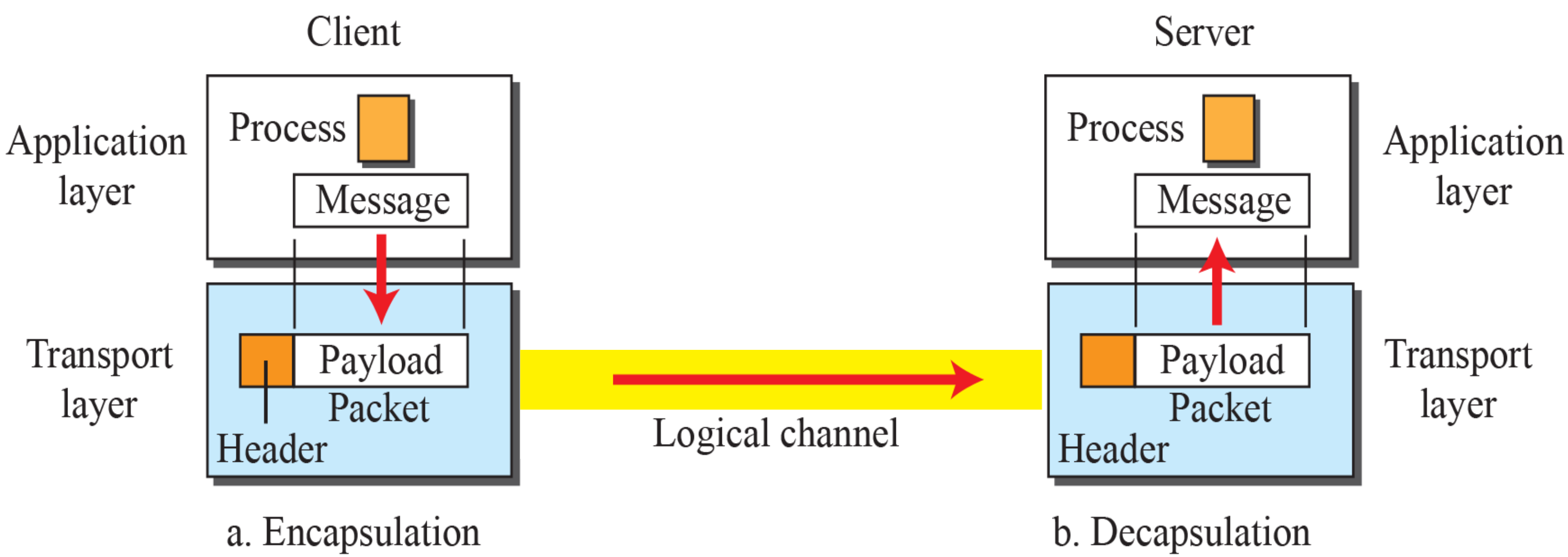
- Communication between applications
- Process-to-process delivery
- Client/server concept
  - Local host
  - Remote host
- Transport Protocol
  - Even more end-to-end

Transport Layer



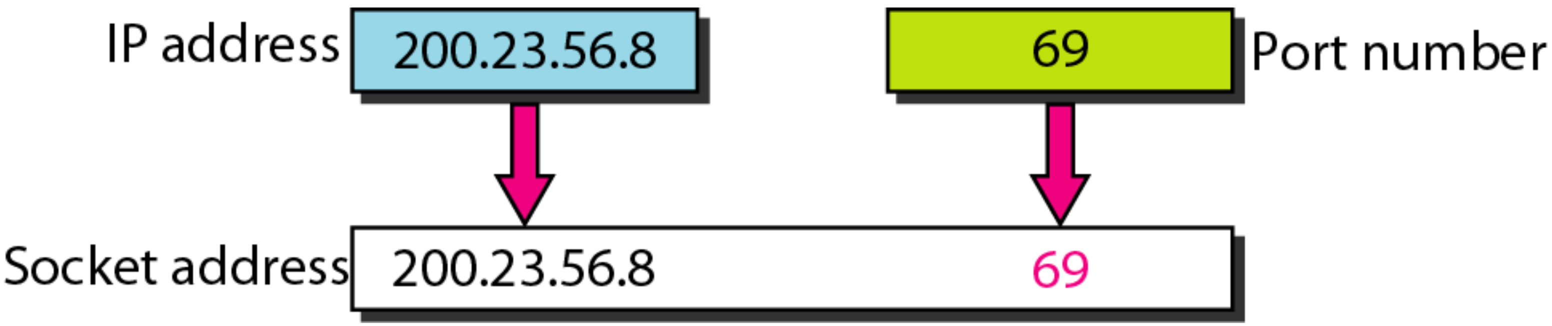
Transport protocol

- Encapsulates application data and ensures that it is sent to the correct receiving application to be decapsulated and used

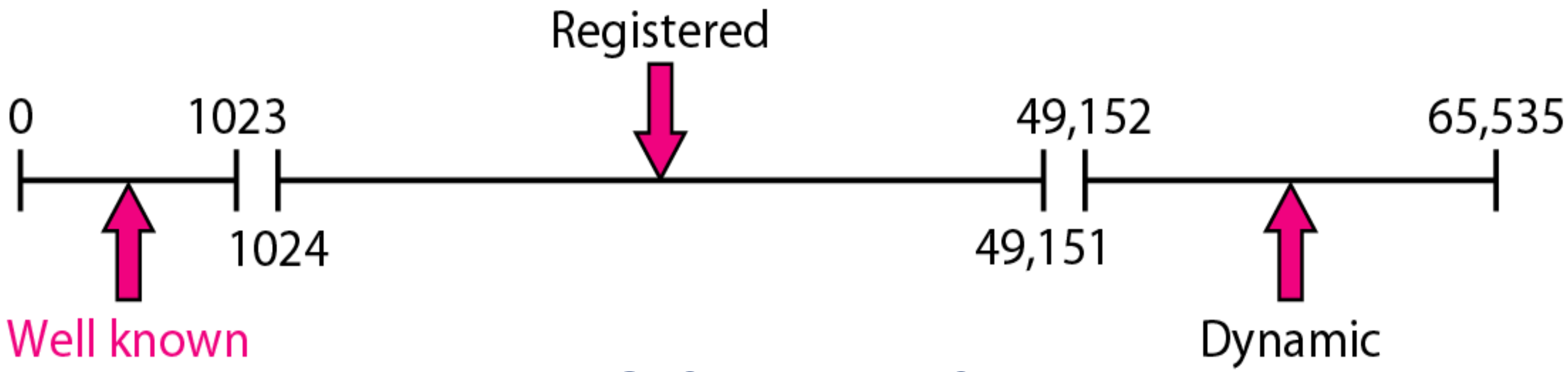


Socket addresses

- Combination of IP address & port number
  - Unique for each process on the host



Port number ranges



TCP

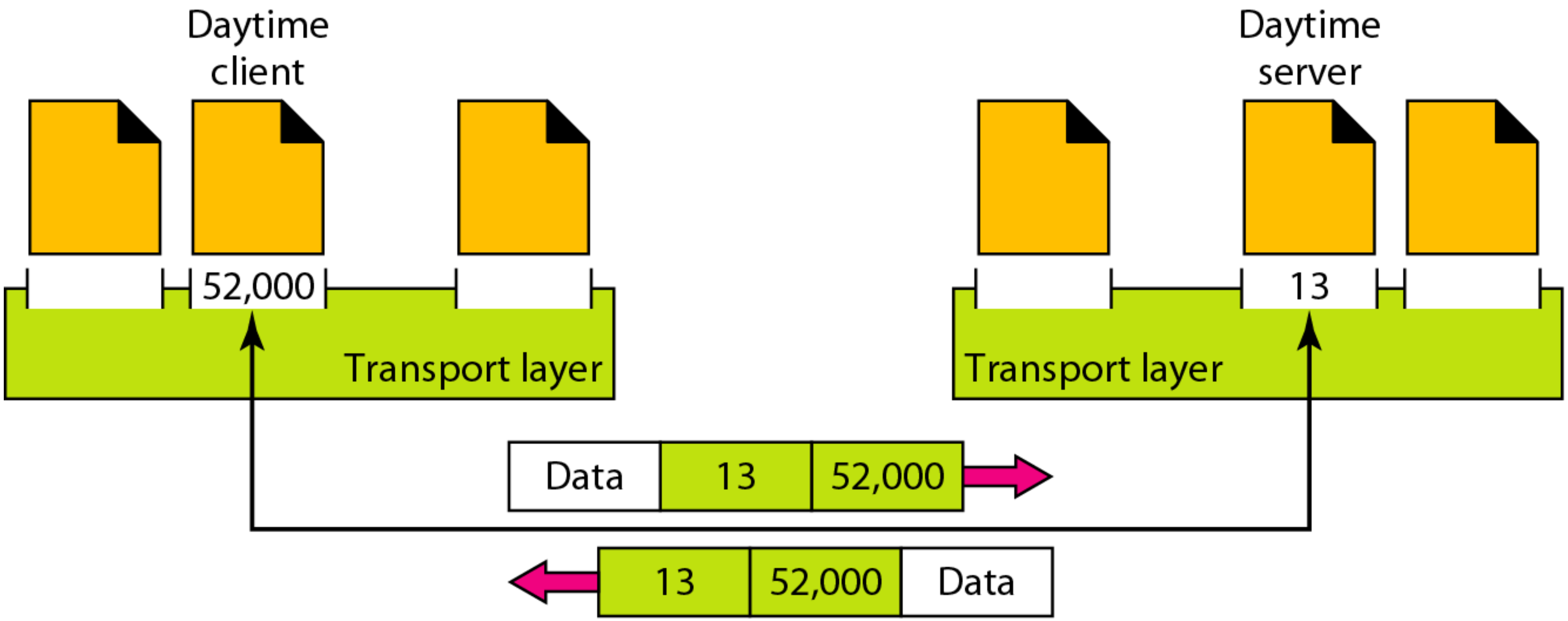
Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

UDP

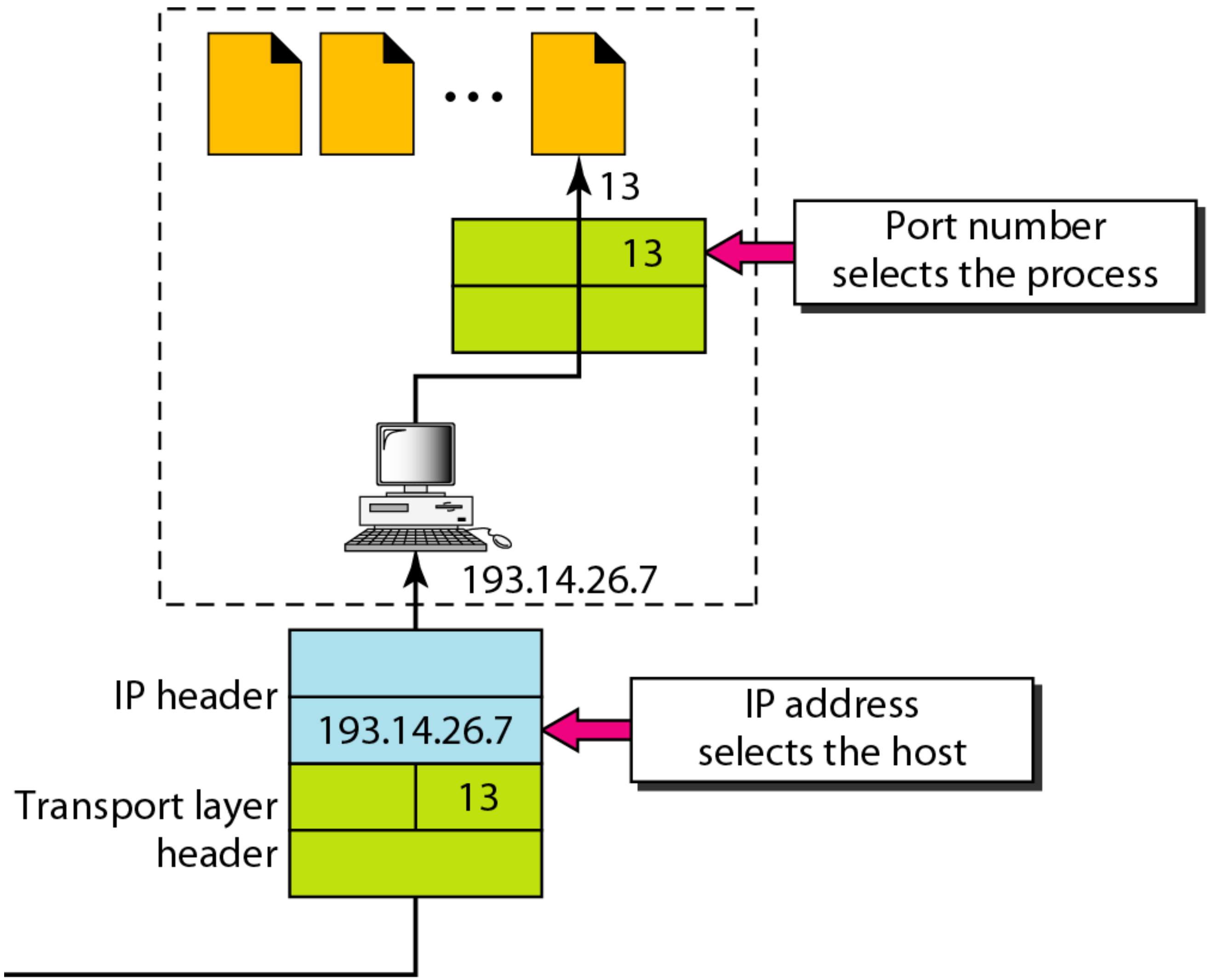
Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

Addressing the processes

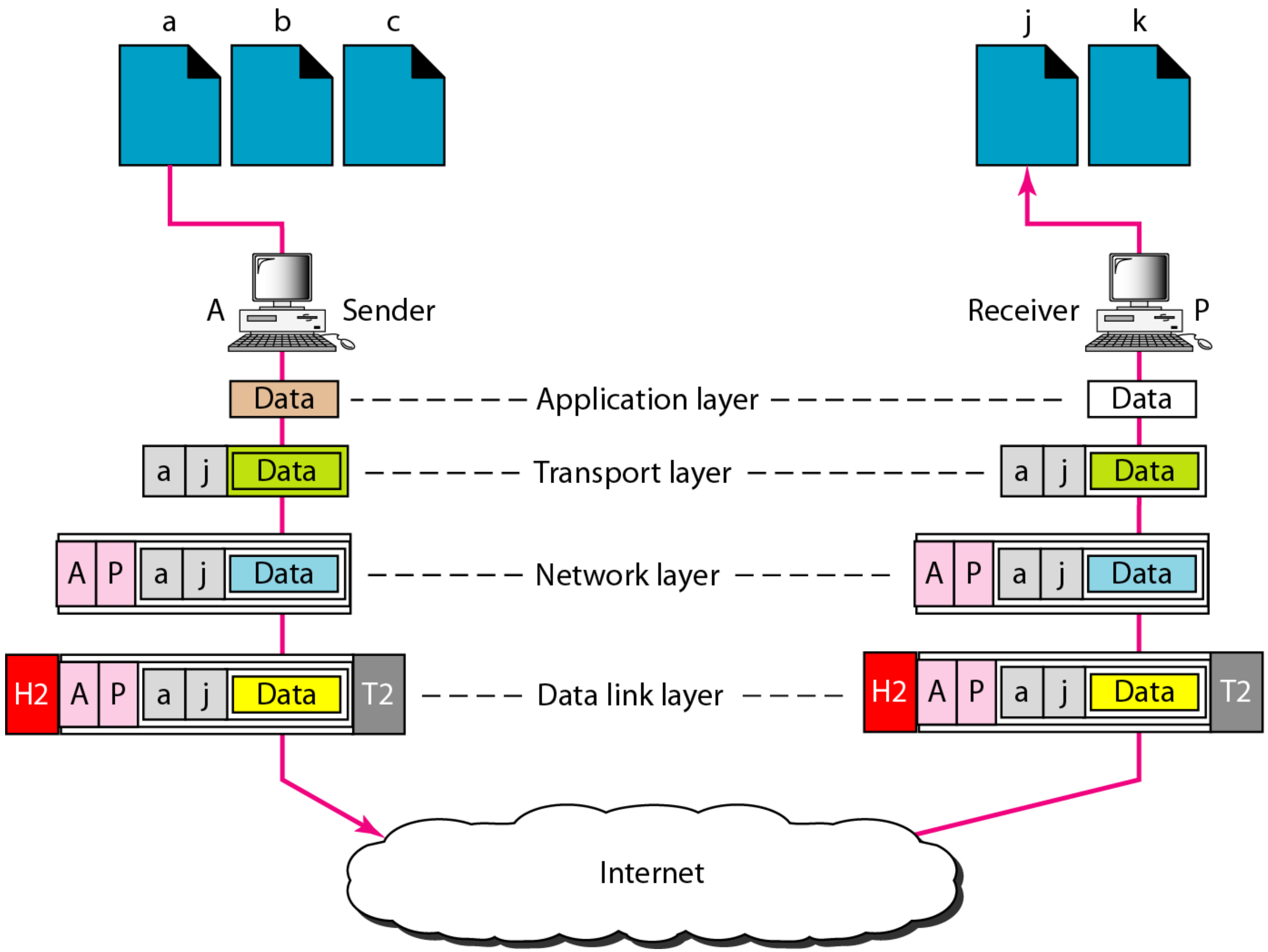
- Port numbers
  - Organised by IANA



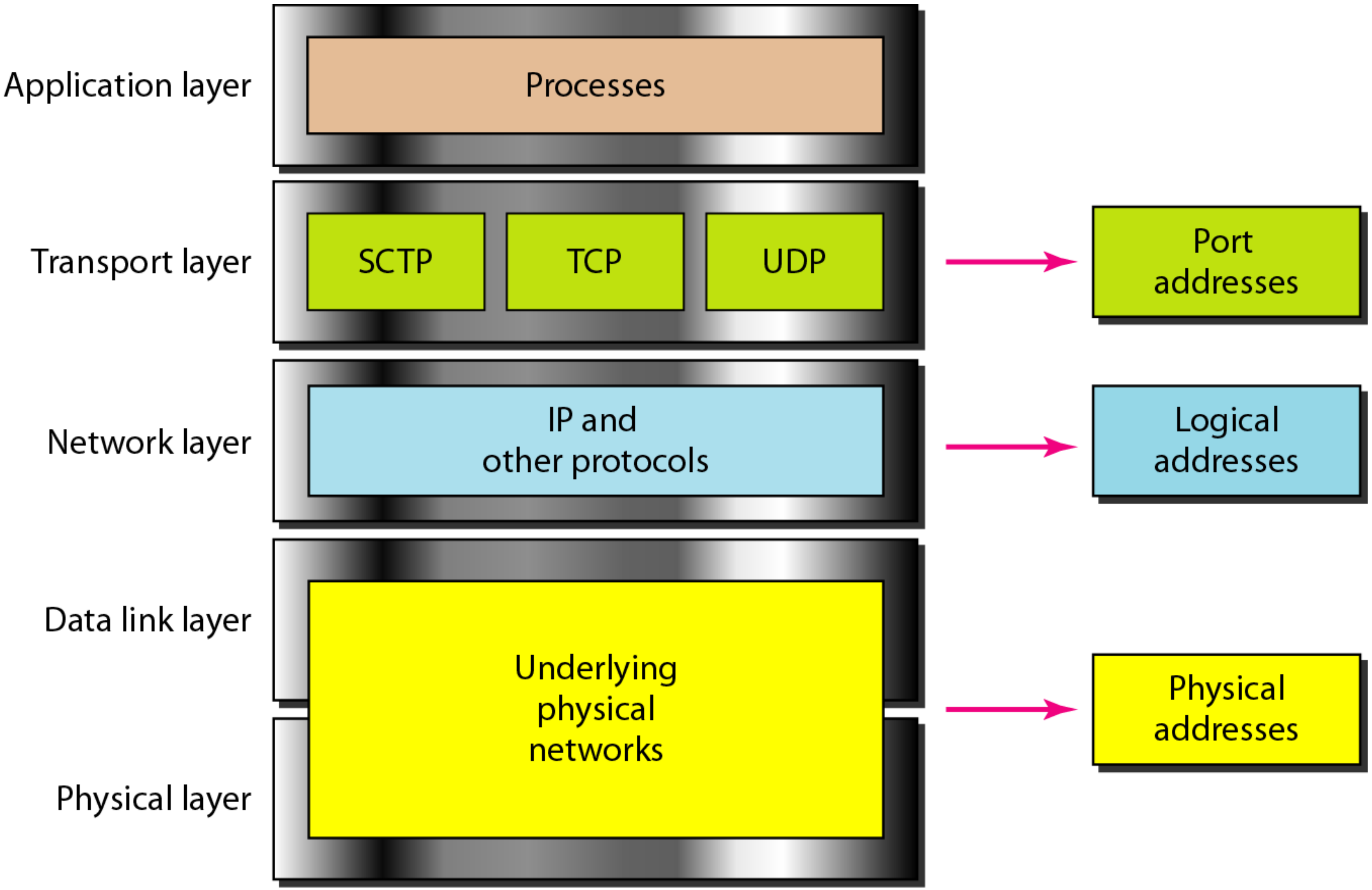
IP addresses and port numbers



Logical and port addresses

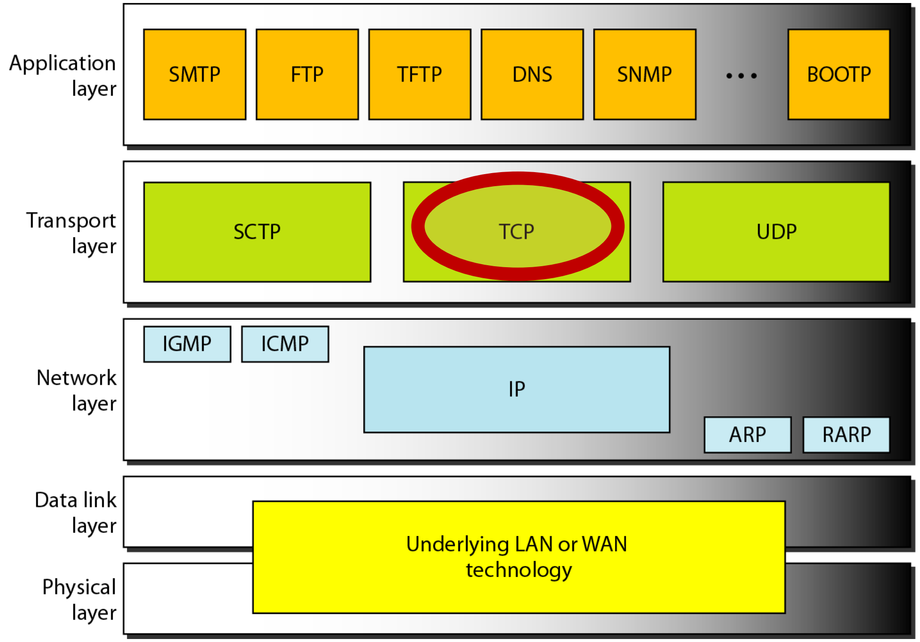


Addressing in TCP/IP

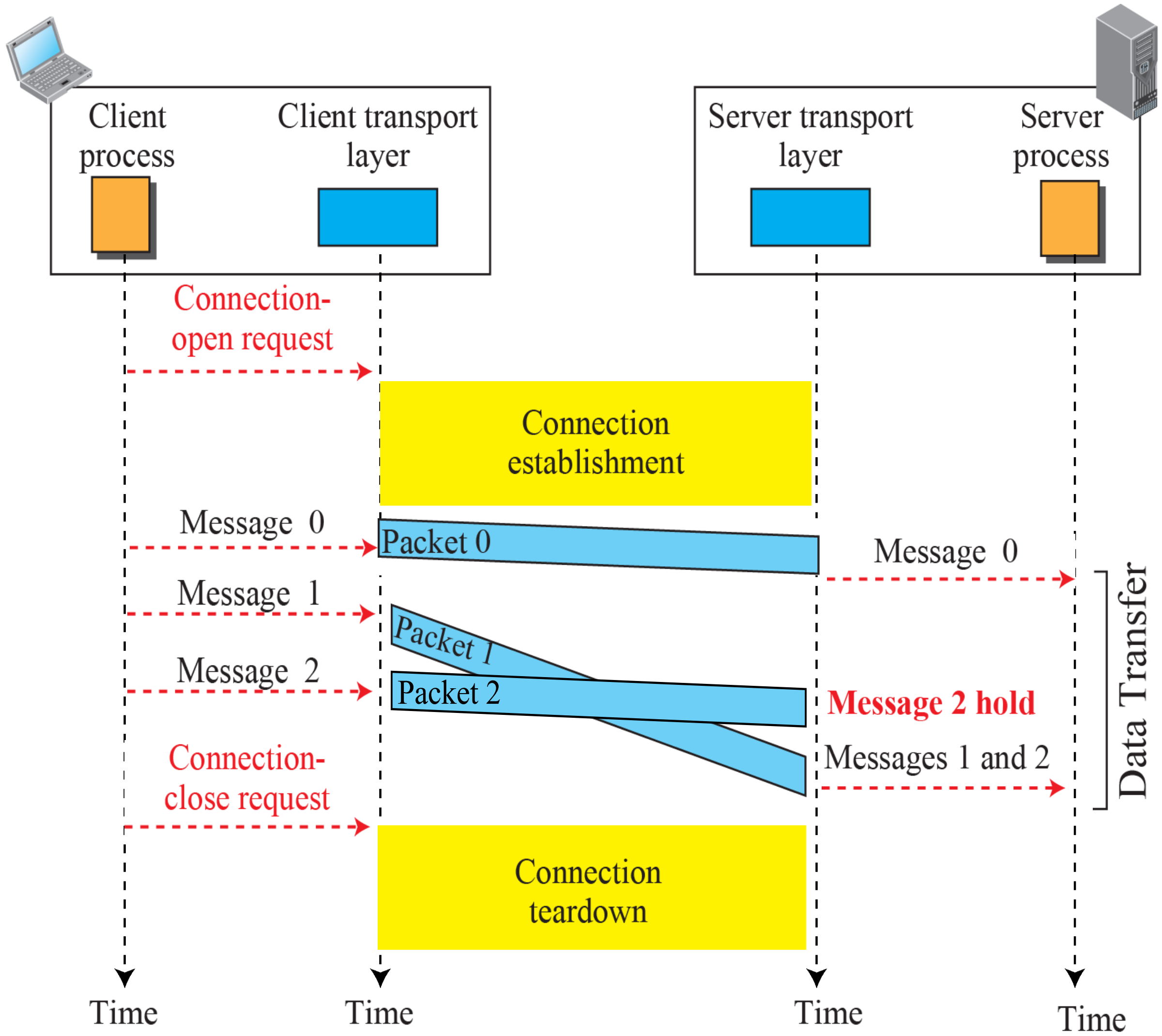


Transmission Control Protocol (TCP)

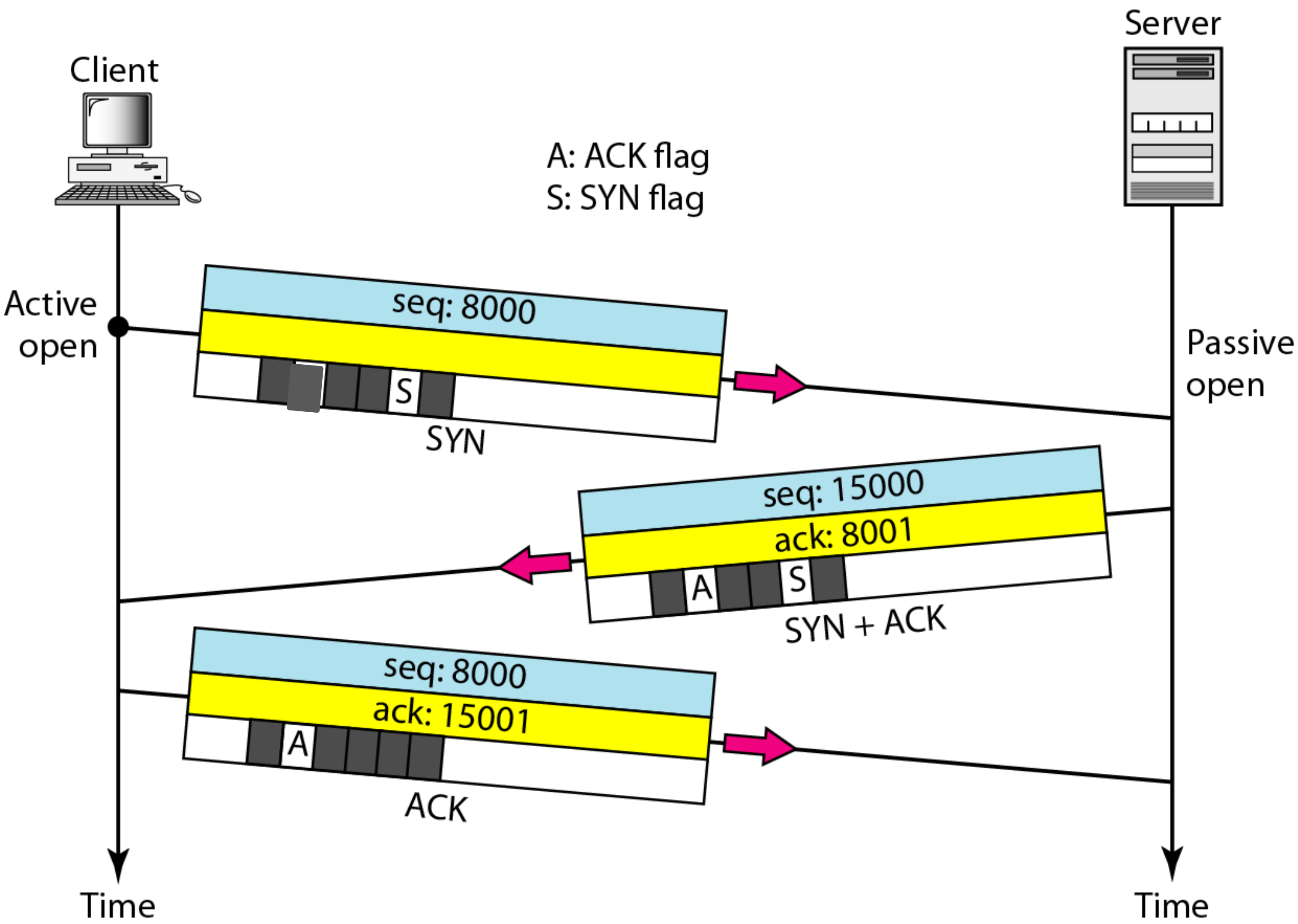
- Connection-oriented
  - Sessions
  - Byte stream service
    - Sequence numbers
- Reliable
  - Flow control
  - Error control
    - Retransmissions
  - Congestion control



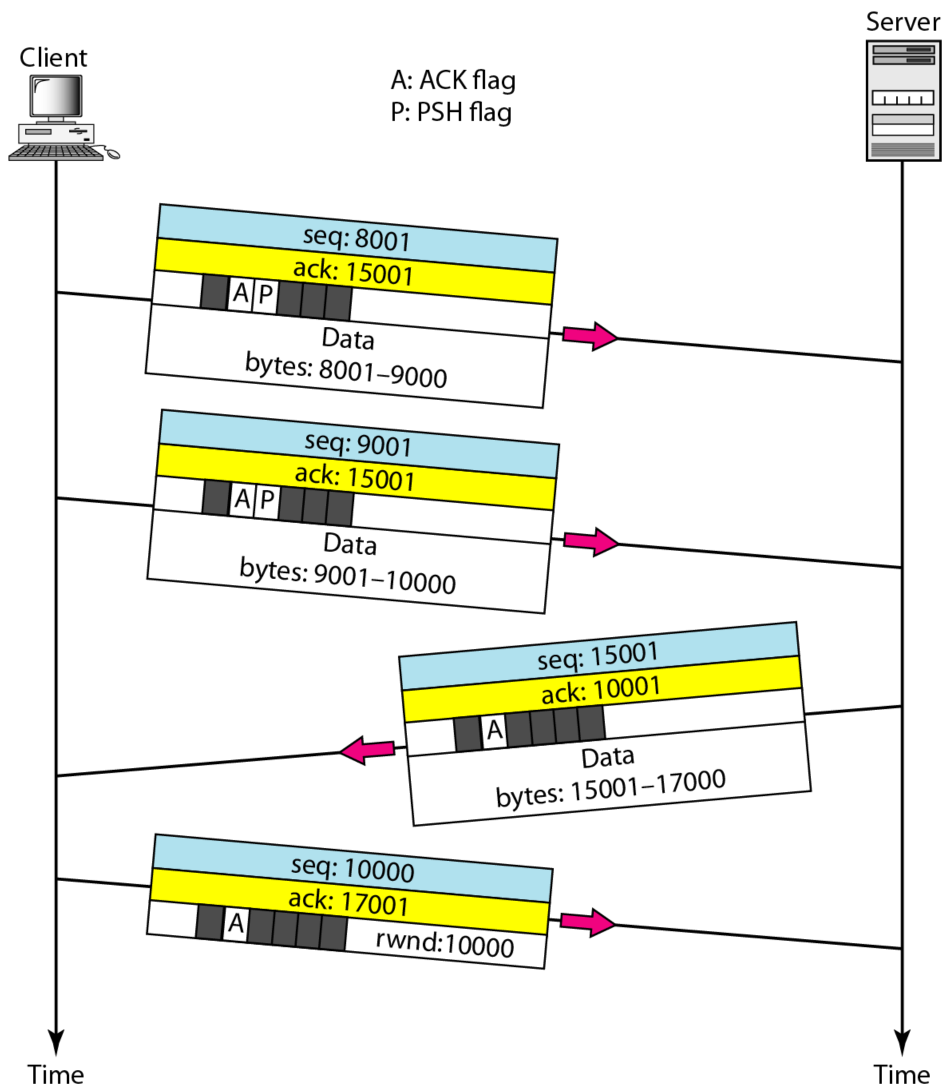
Connection-oriented service



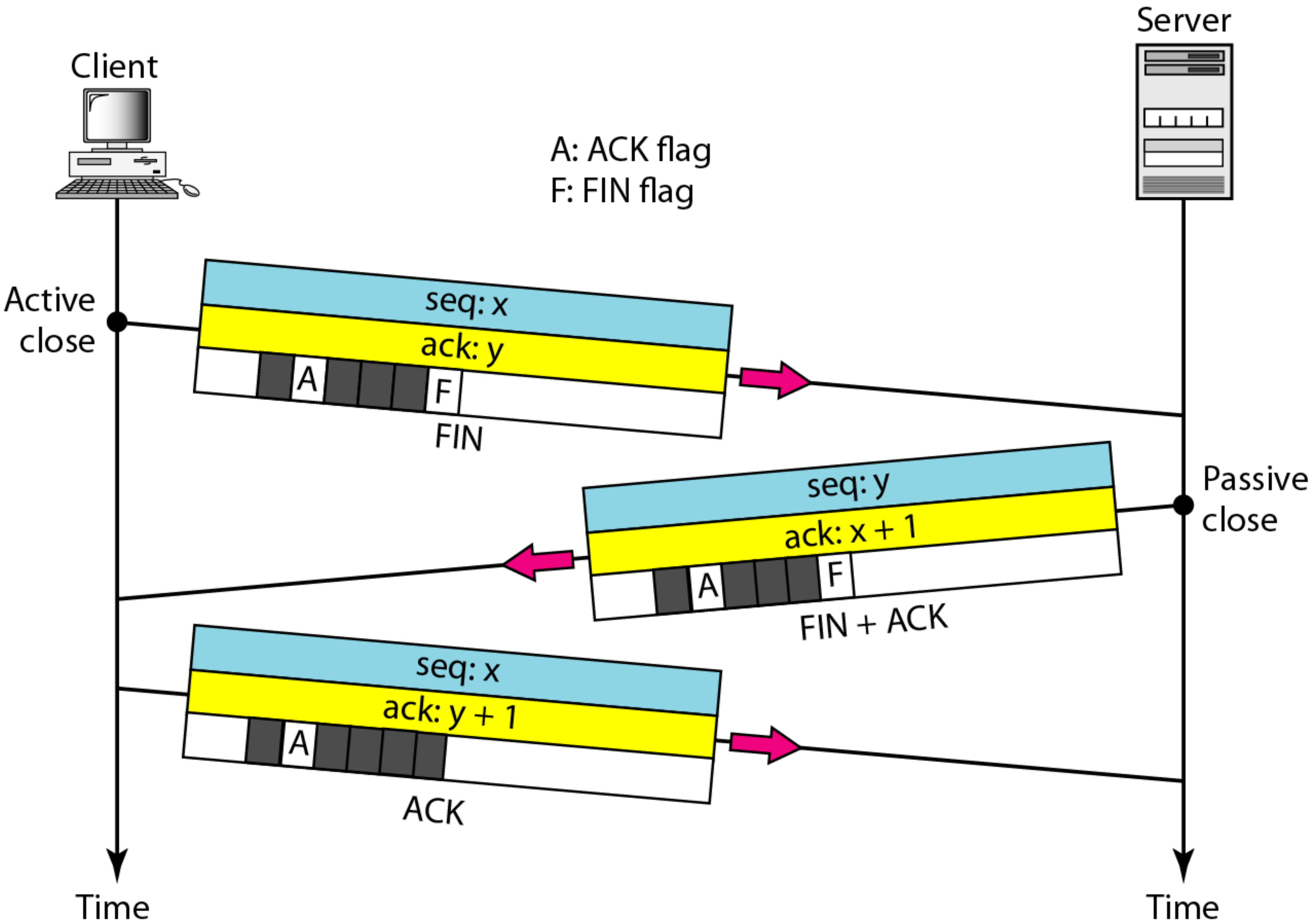
Connection establishment



Data transfer

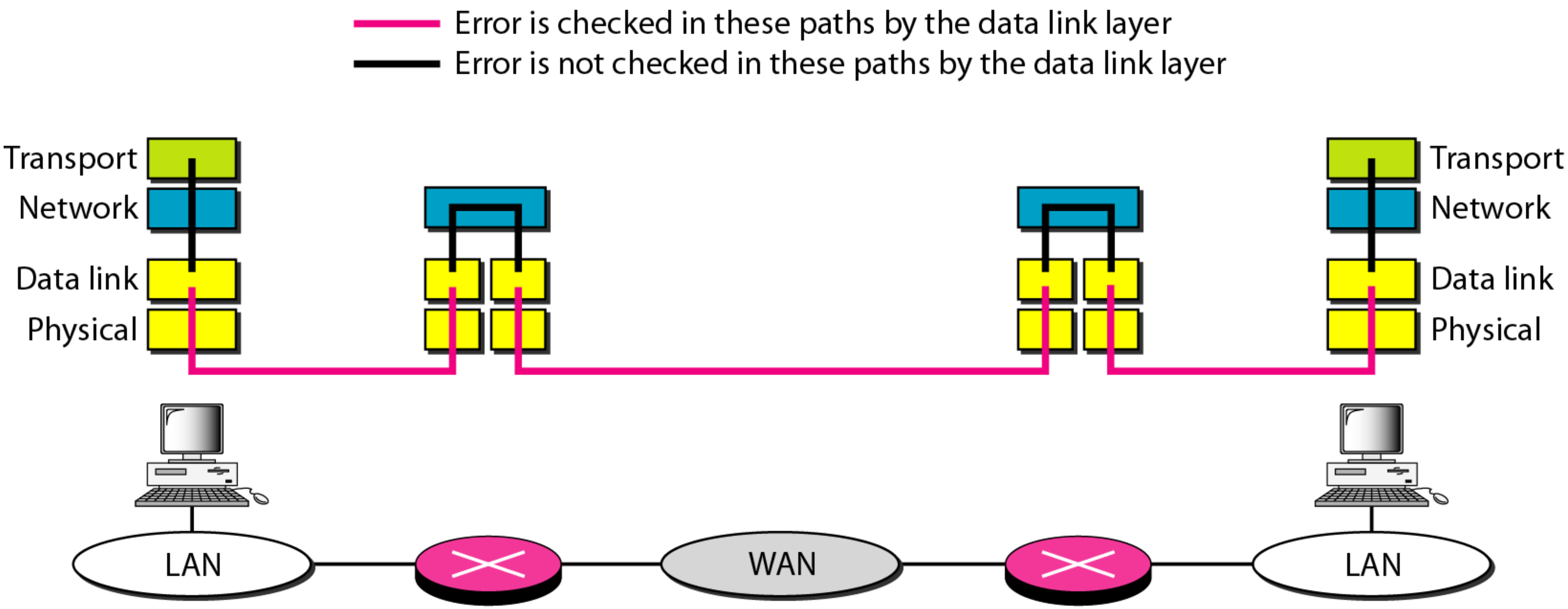


Connection termination



Error control

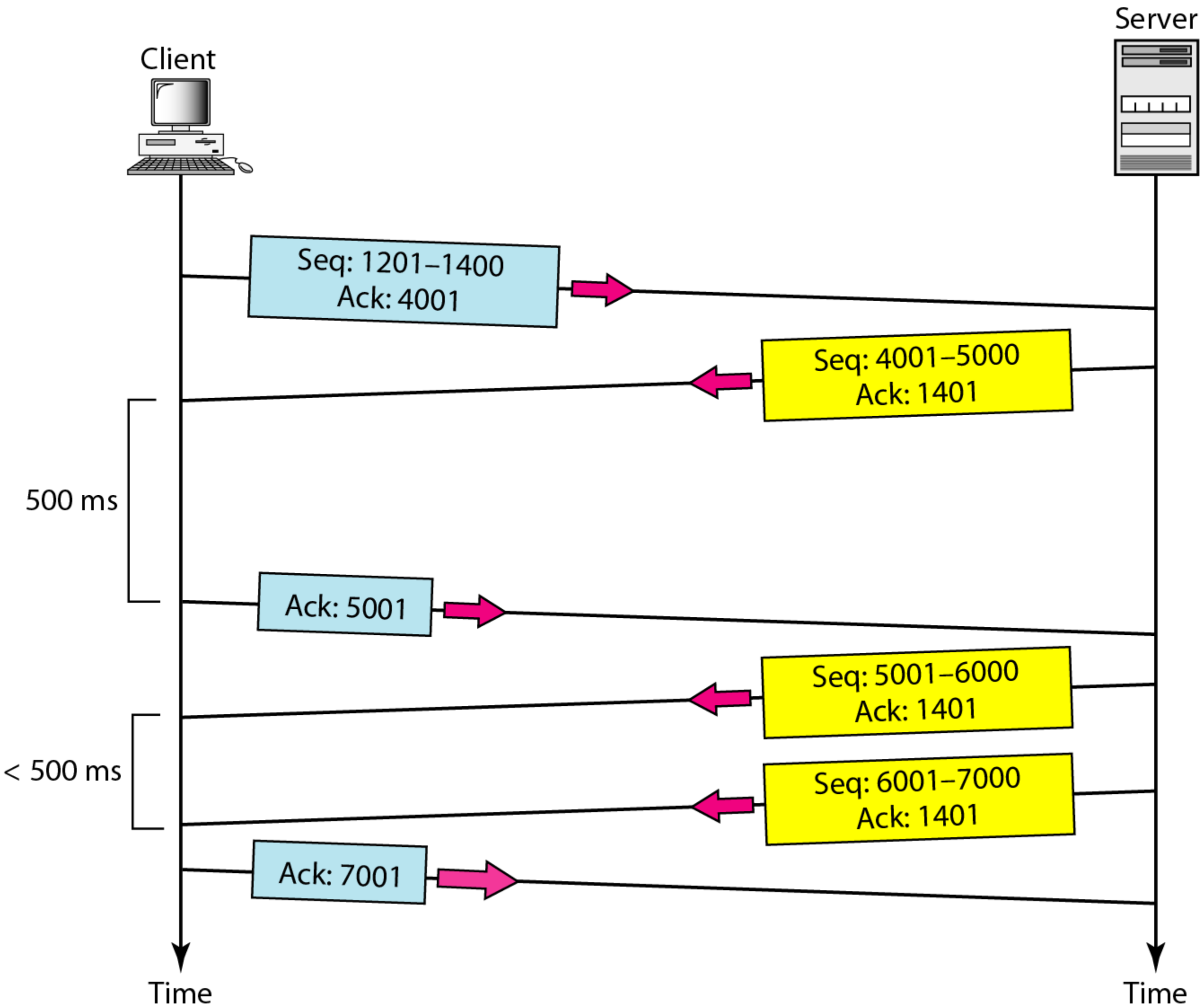
- Reliable transport layer service: TCP
- Unreliable network layer service: IP



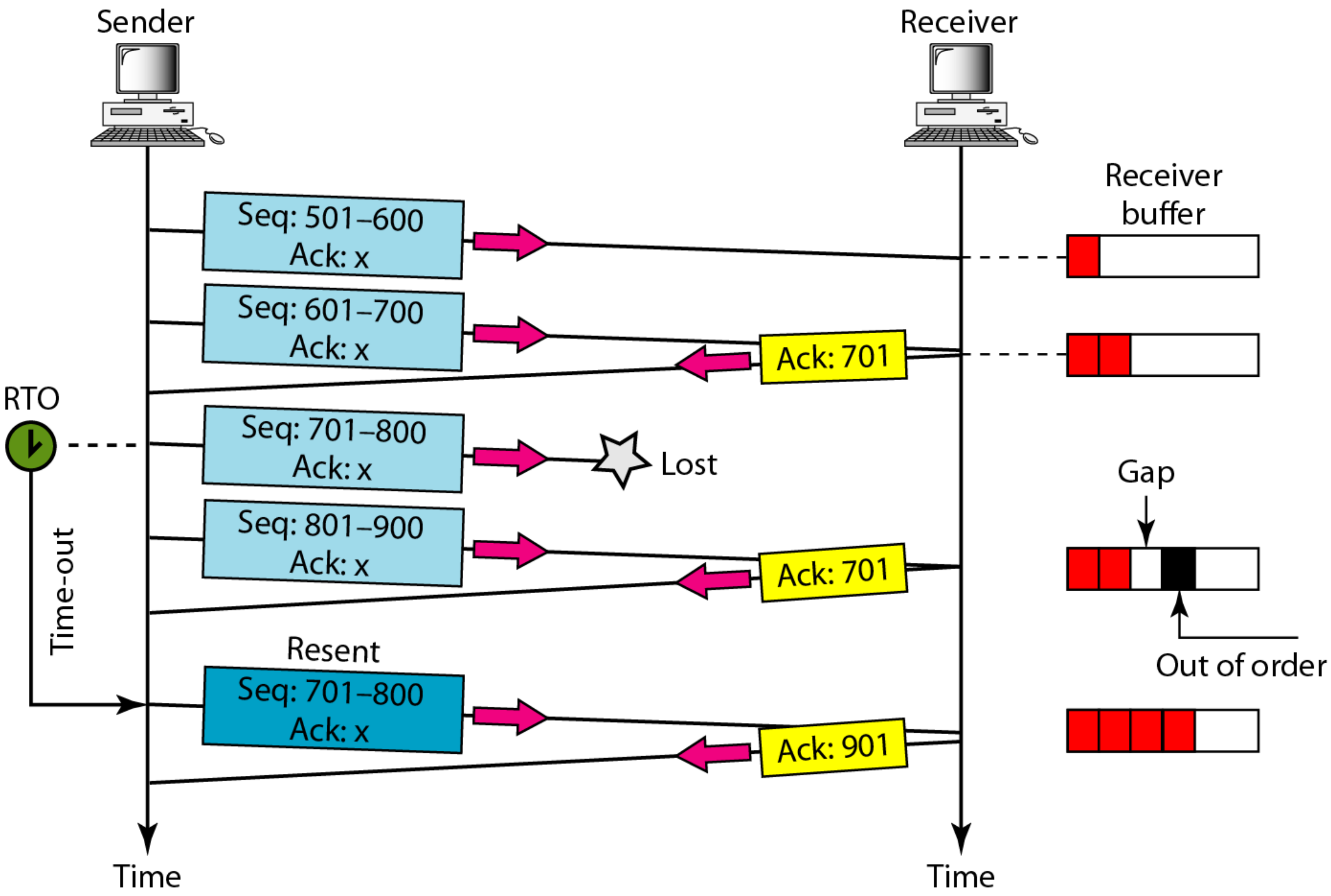
Error control in TCP

- Checksum
- Acknowledgement
  - ACK recieved data
- Retransmission
  - After time-out
  - After 3 duplicate ACK

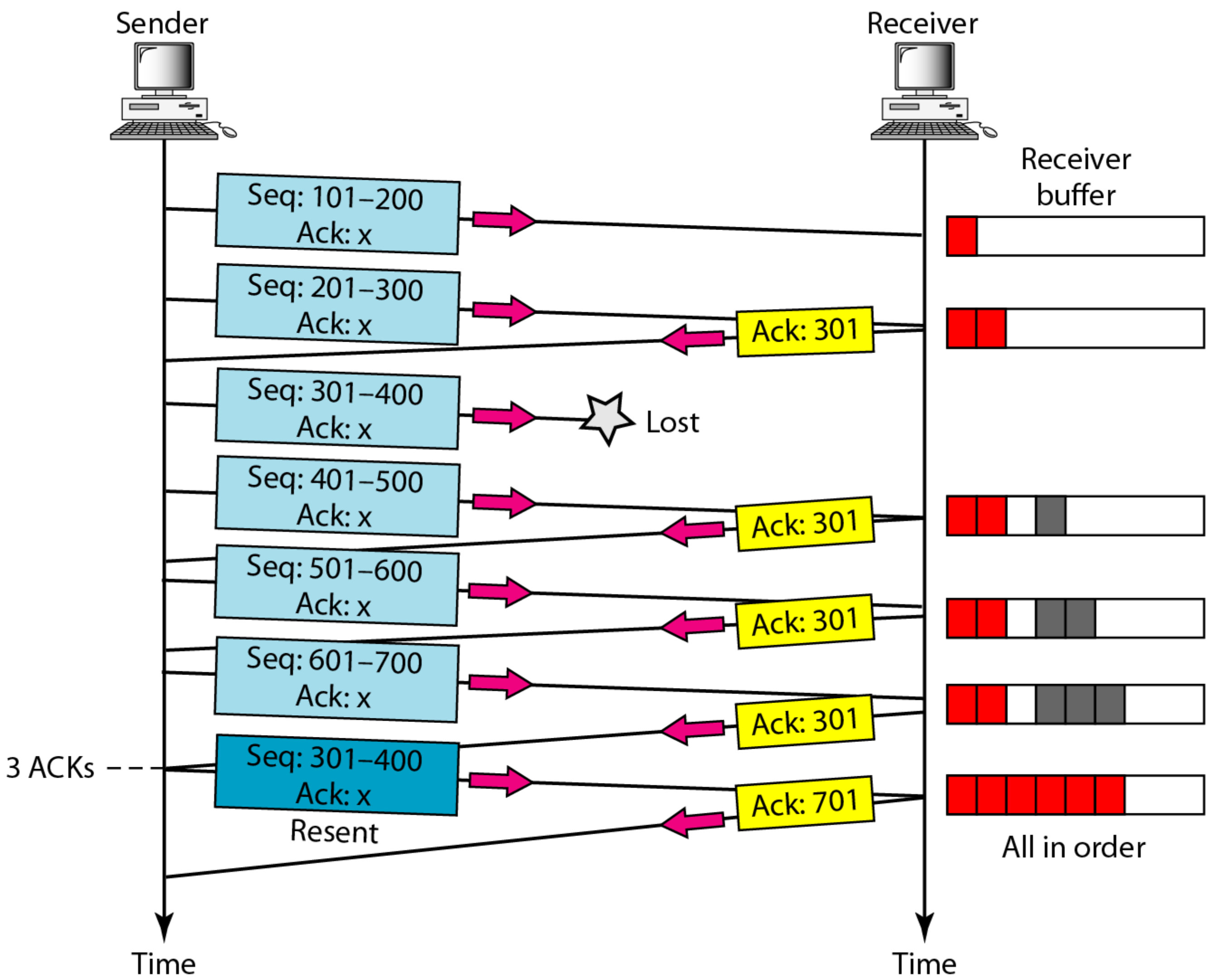
Normal operation



Lost segment



Fast retransmission



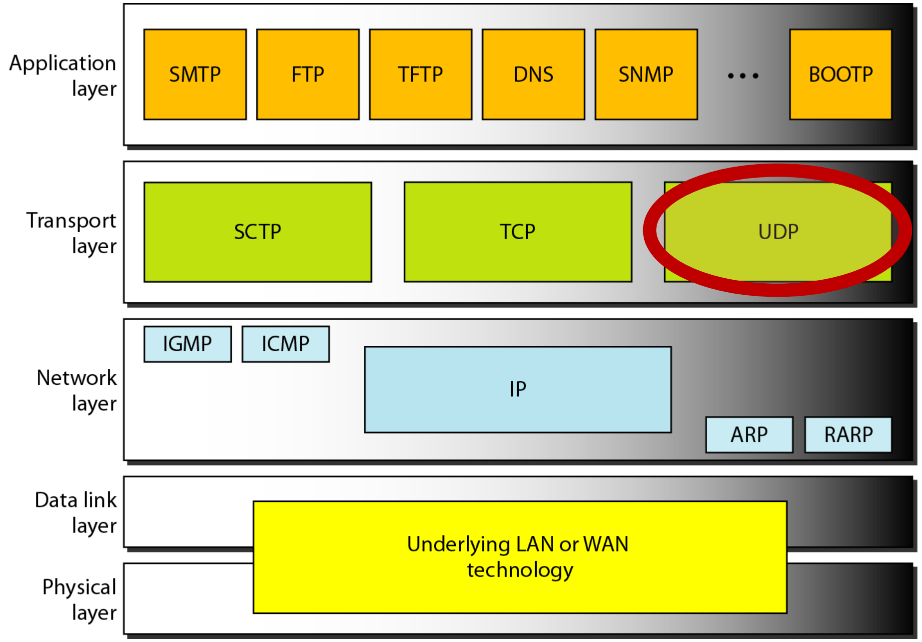
Summary and comparison: QoS

Multimedia Performance Requirements	*vs. Characteristics of TCP*
• Sensitive to: – Delay – Jitter • Not so sensitive to: – Packet loss – Corrupted packets	• Sensitive to: – Lost or corrupted packets • Not so sensitive to: – Delay • No multicasting!

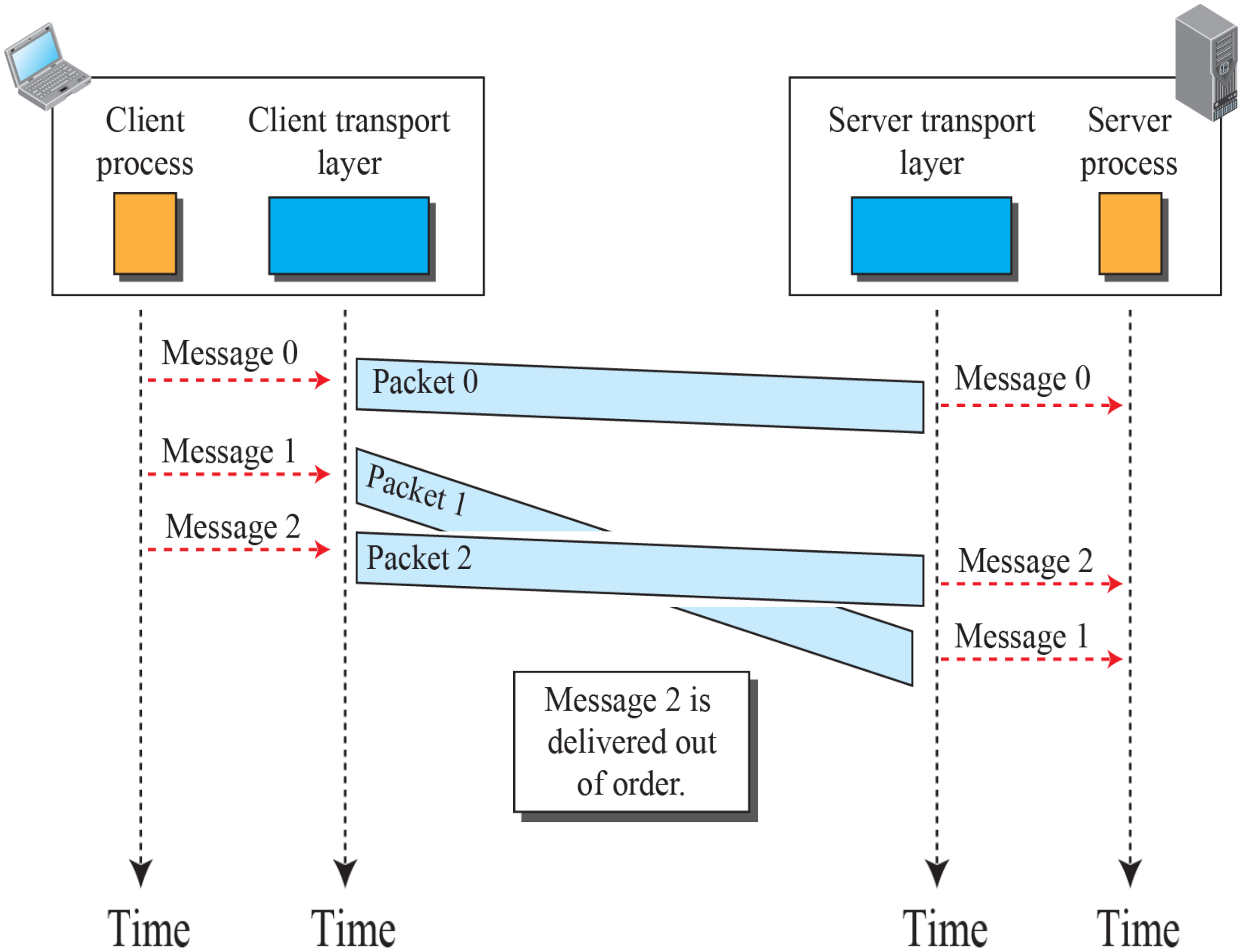
So, what about UDP?

User Datagram Protocol (UDP)

- Connectionless
  - Independent datagrams
  - No sessions
- Unreliable
  - No error control
  - No flow control
- Process-to-process

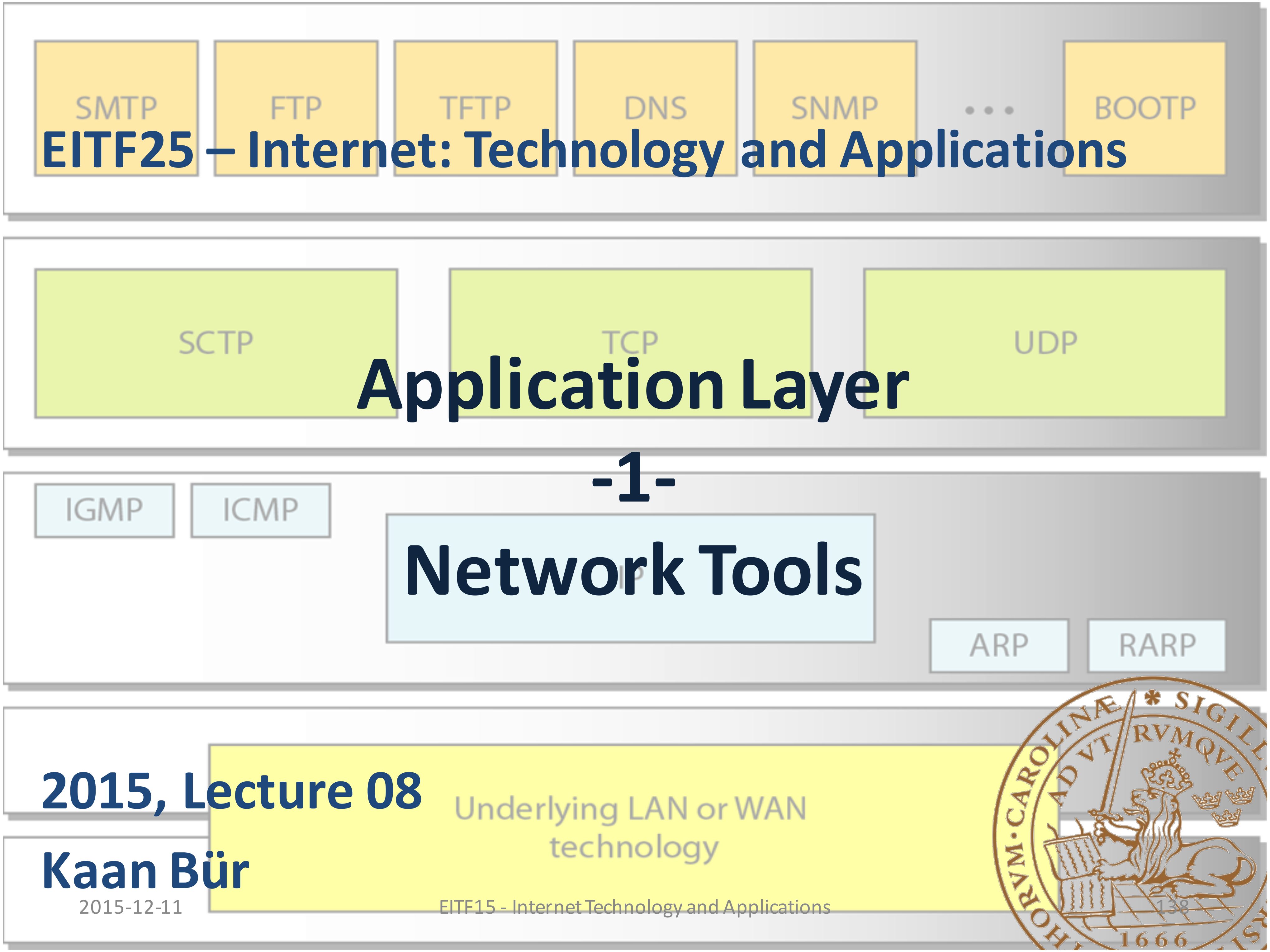


Connectionless service



EITF25 – Internet: Technology and Applications

Application Layer
-1-
Network Tools



2015, Lecture 08

Kaan Bür

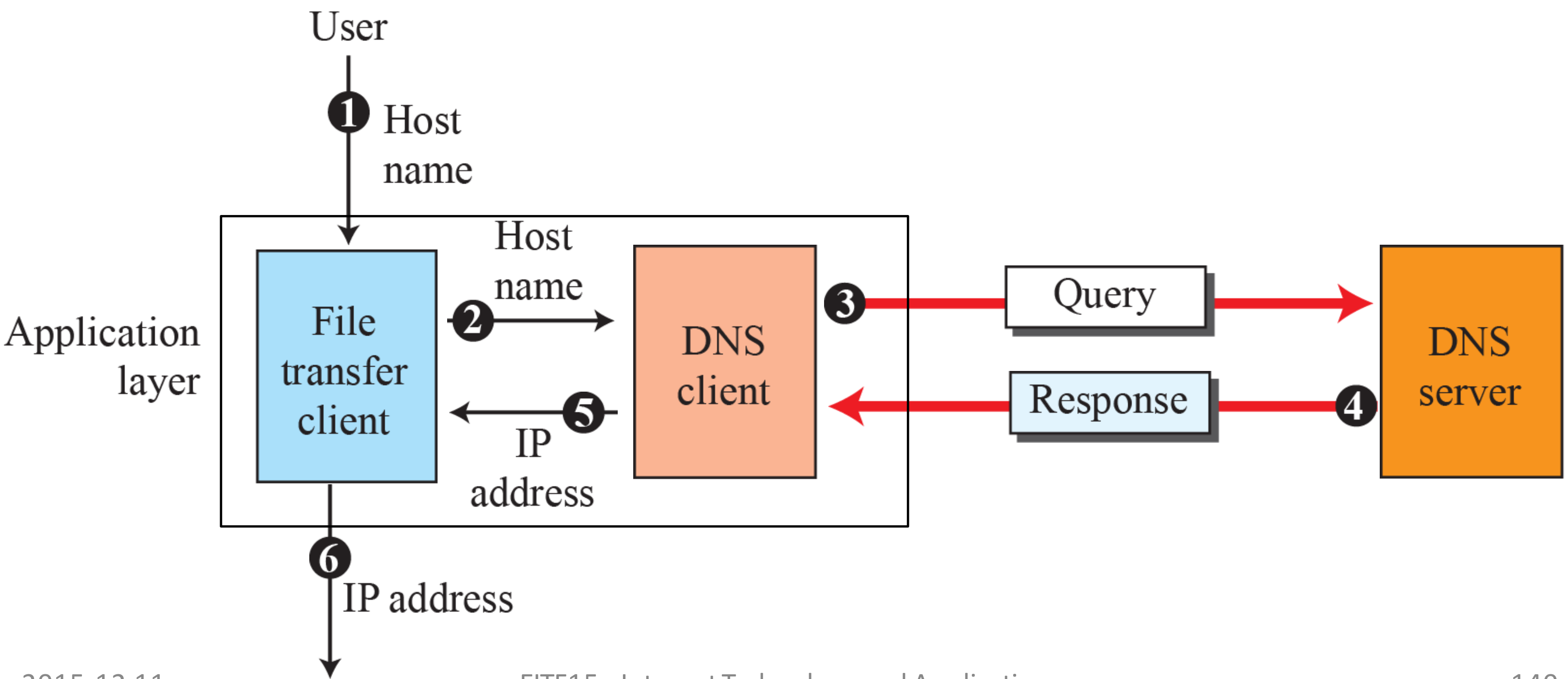
Mapping host name to IP address

- Application protocols use host names
- TCP/IP protocol suite uses IP addresses
- Mapping from host name to IP addresses

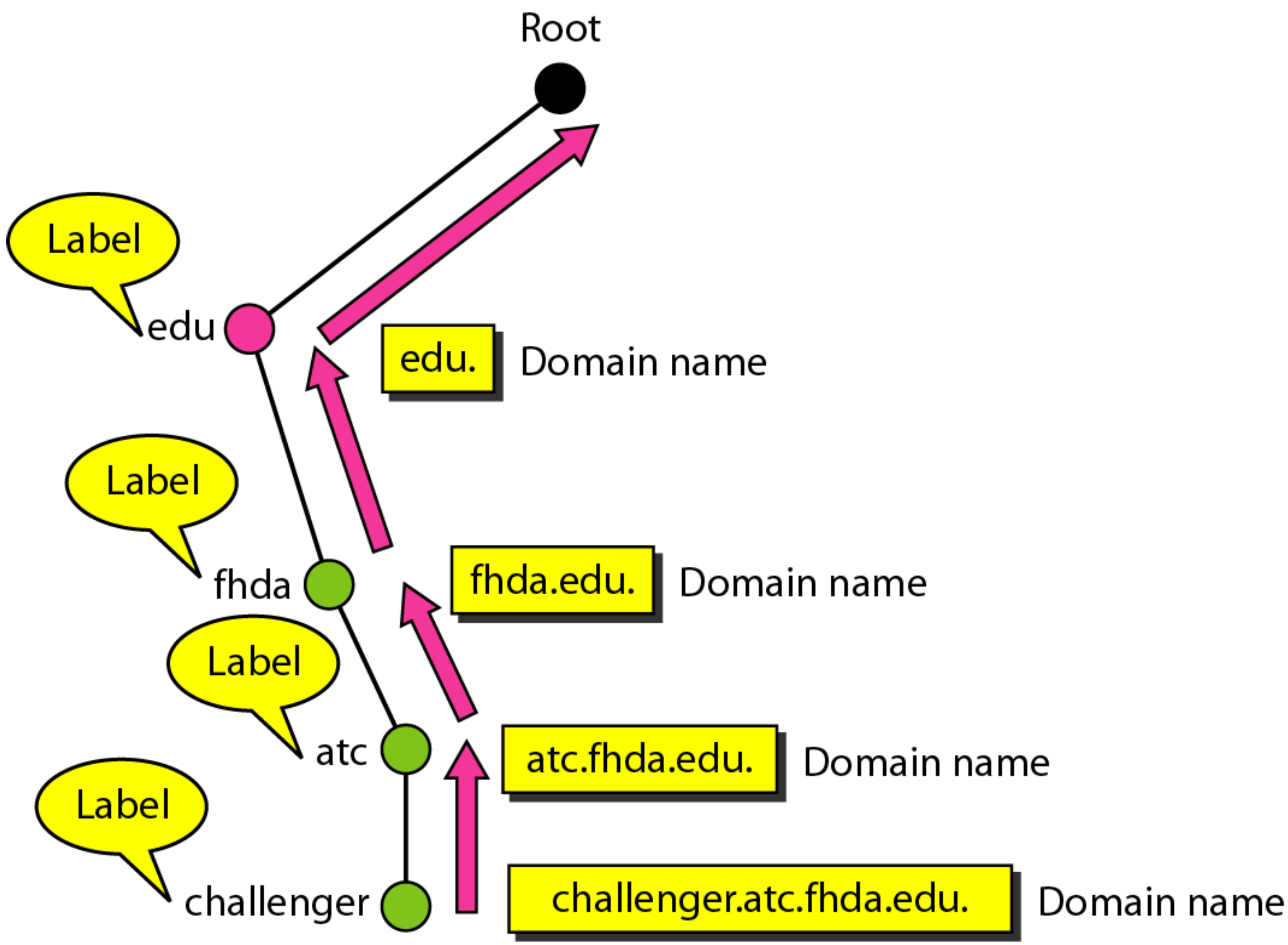
- Domain Name System (DNS)
  - Domain name space
  - Domain name resolution
- www.lth.se ≡ 130.235.209.220

Domain Name System (DNS)

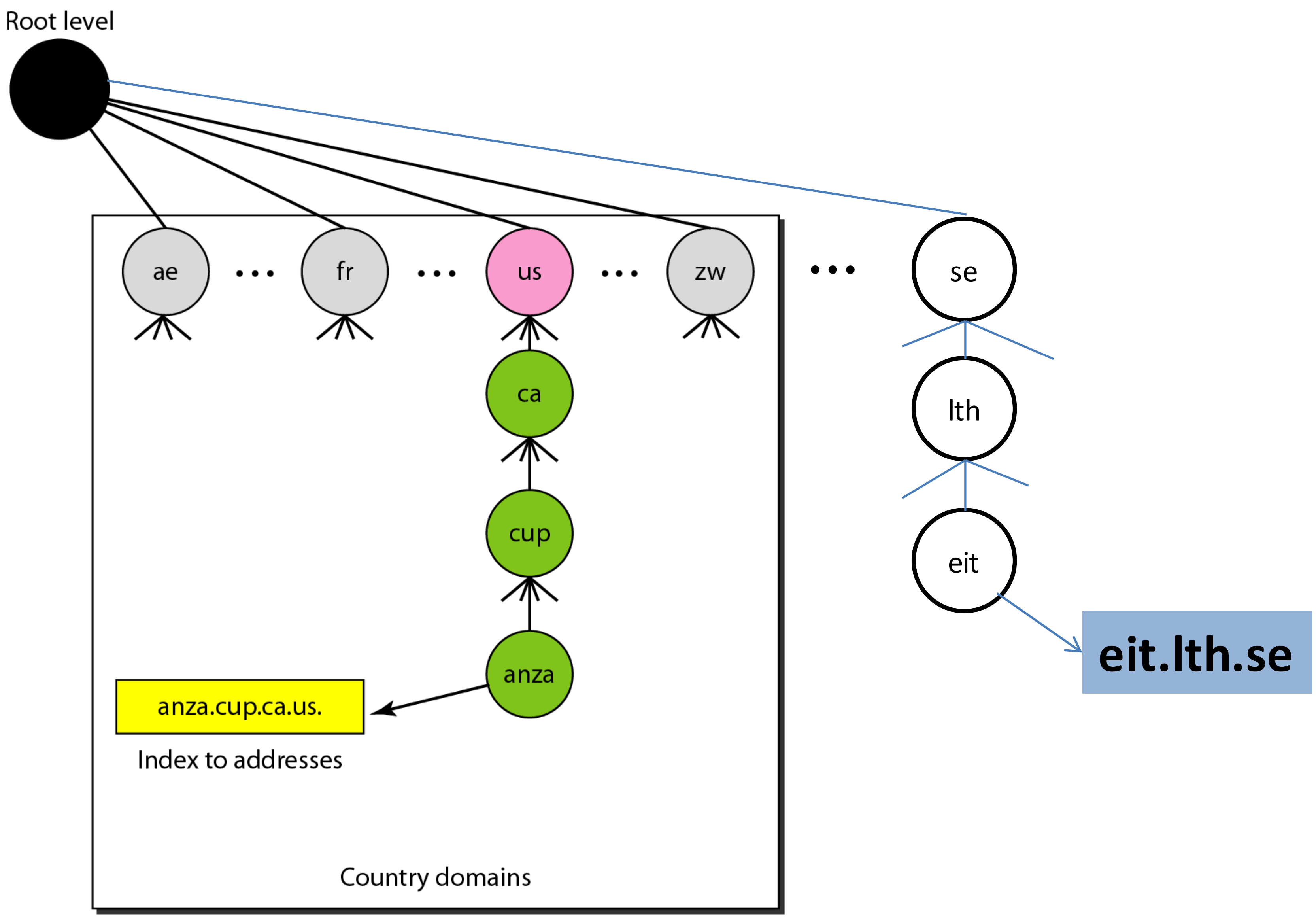
- Internet’s telephone book: Address ↔ name
  - One of the most important systems on the Internet



Domain names and labels

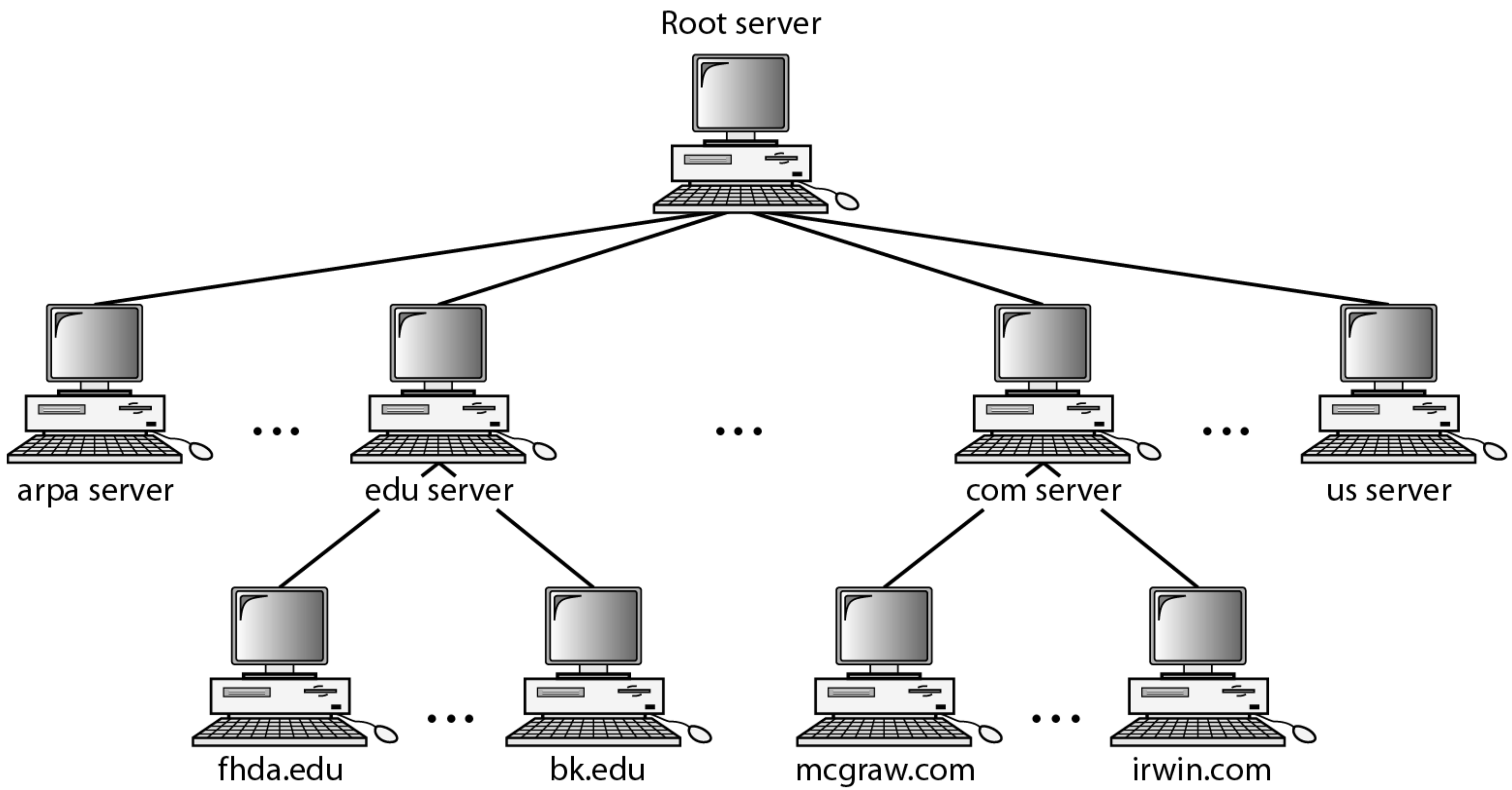


Country domains



Hierarchy of domain name servers

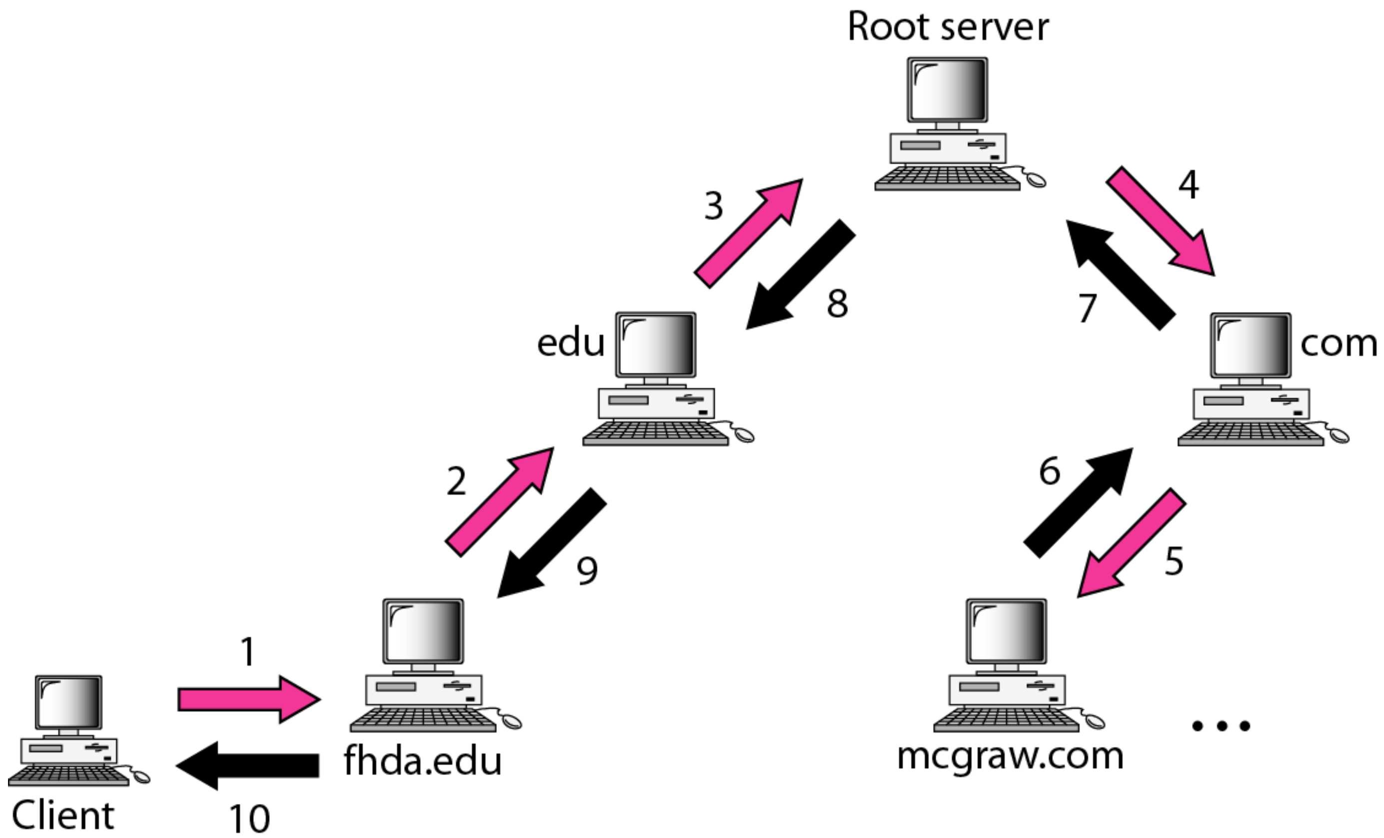
- 13 logical root name servers
  - implemented by 376 physical servers



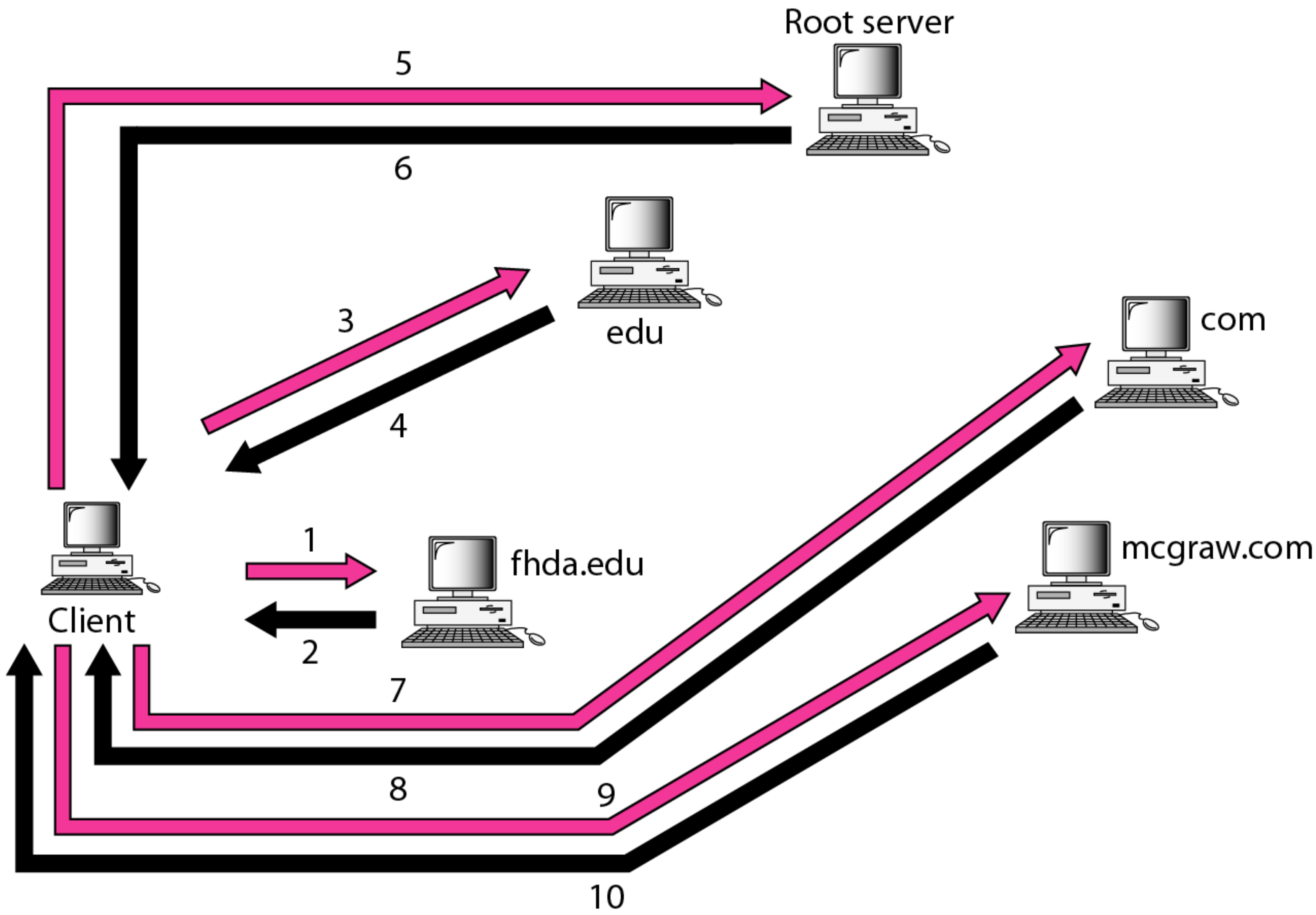
Domain name resolution

- Action of address mapping
  - Client = resolver
  - Server = DNS
- One server cannot have all the answers!
  - How to ask others?
  - What to do with the answer?
- Caching
  - Remember what you've learned!

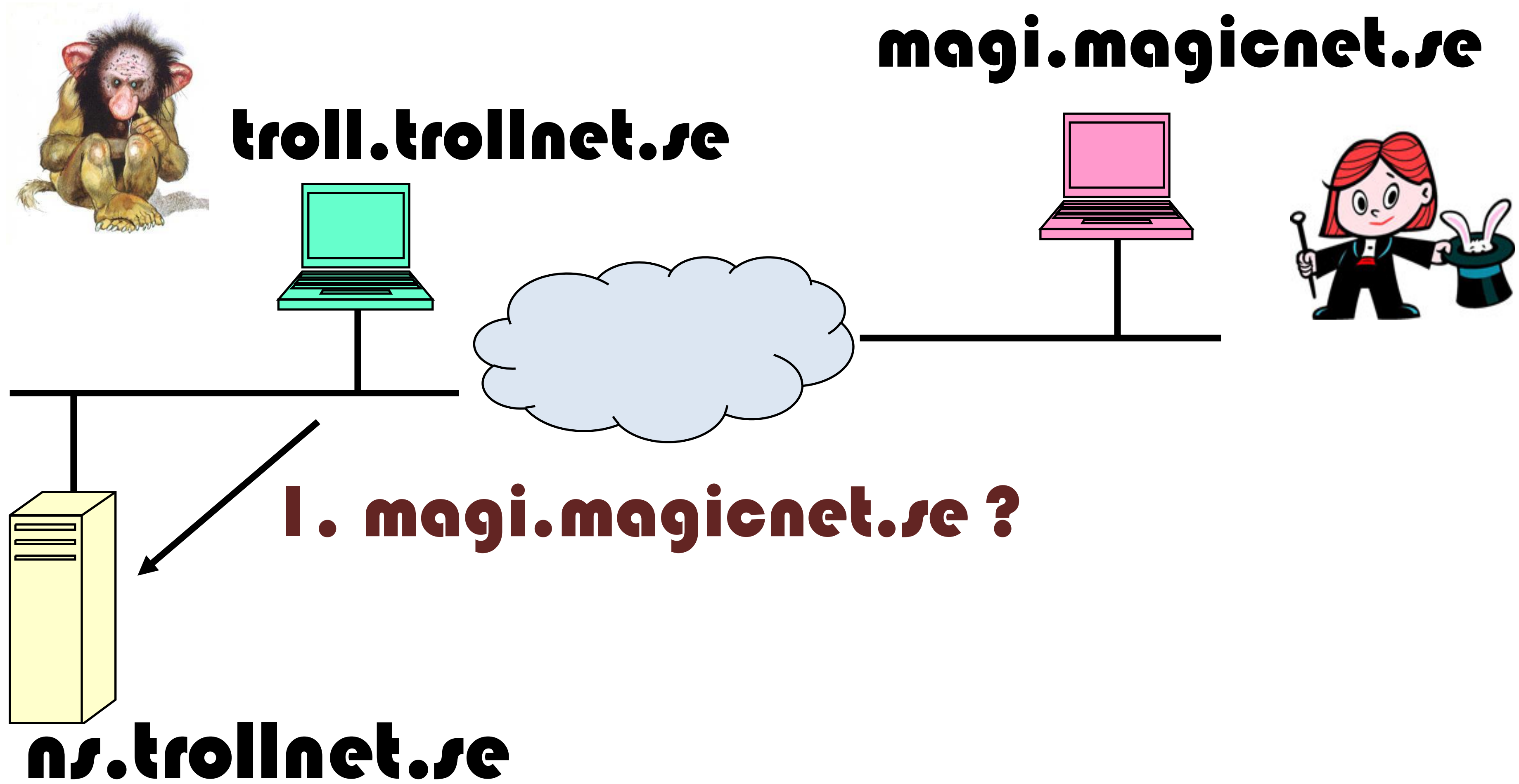
Recursive resolution



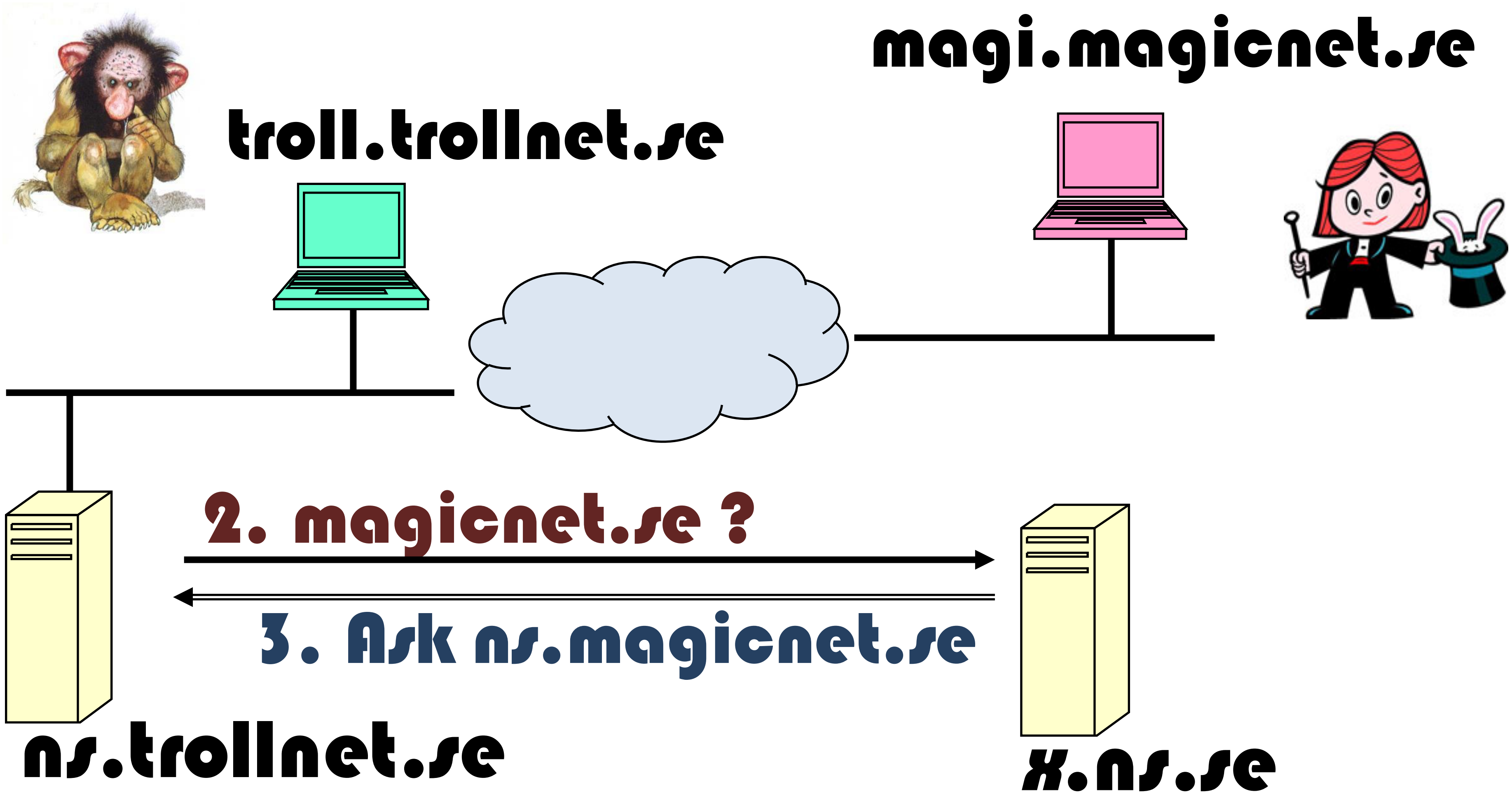
Iterative resolution



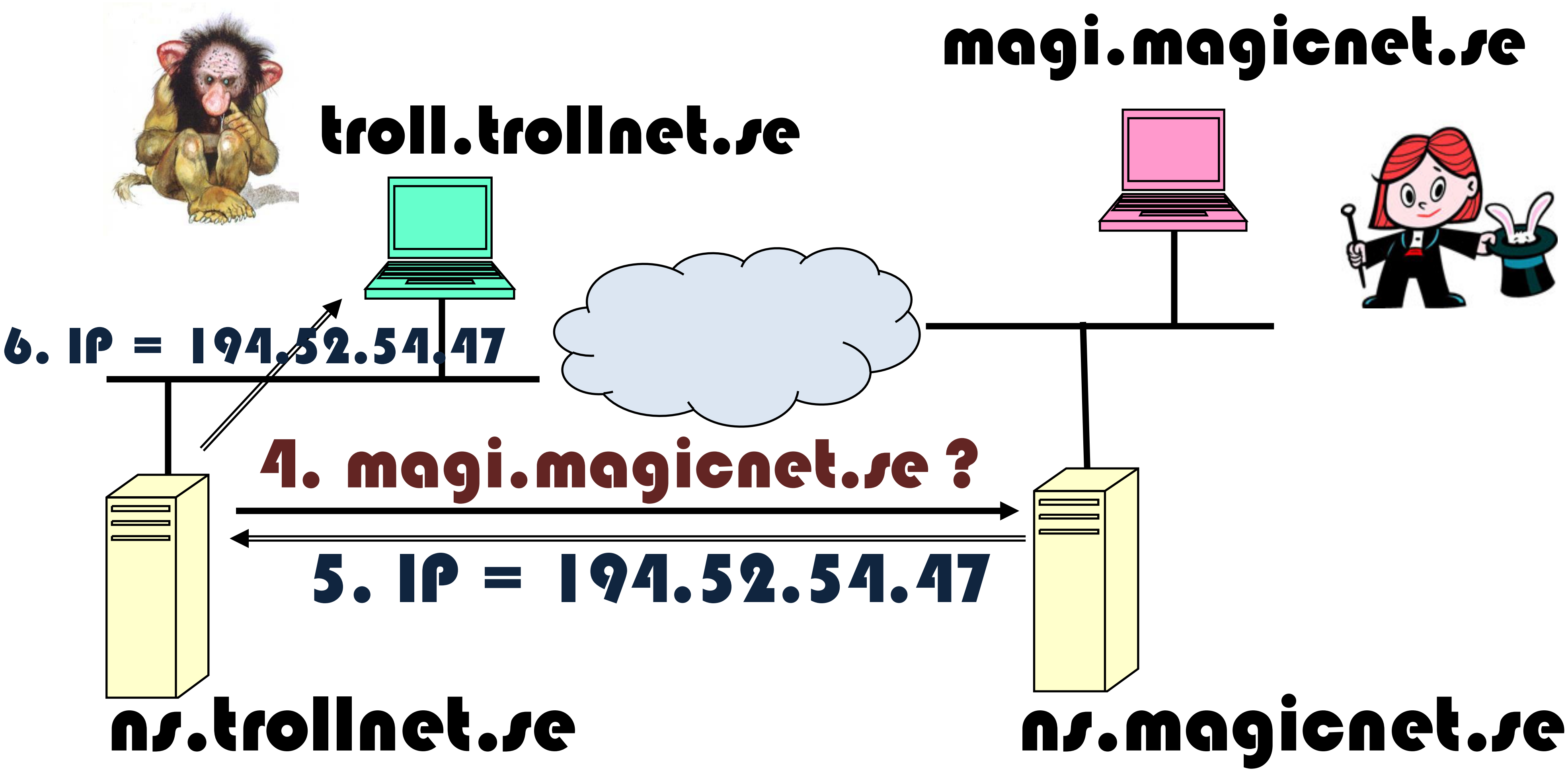
Domain name to IP address (1)



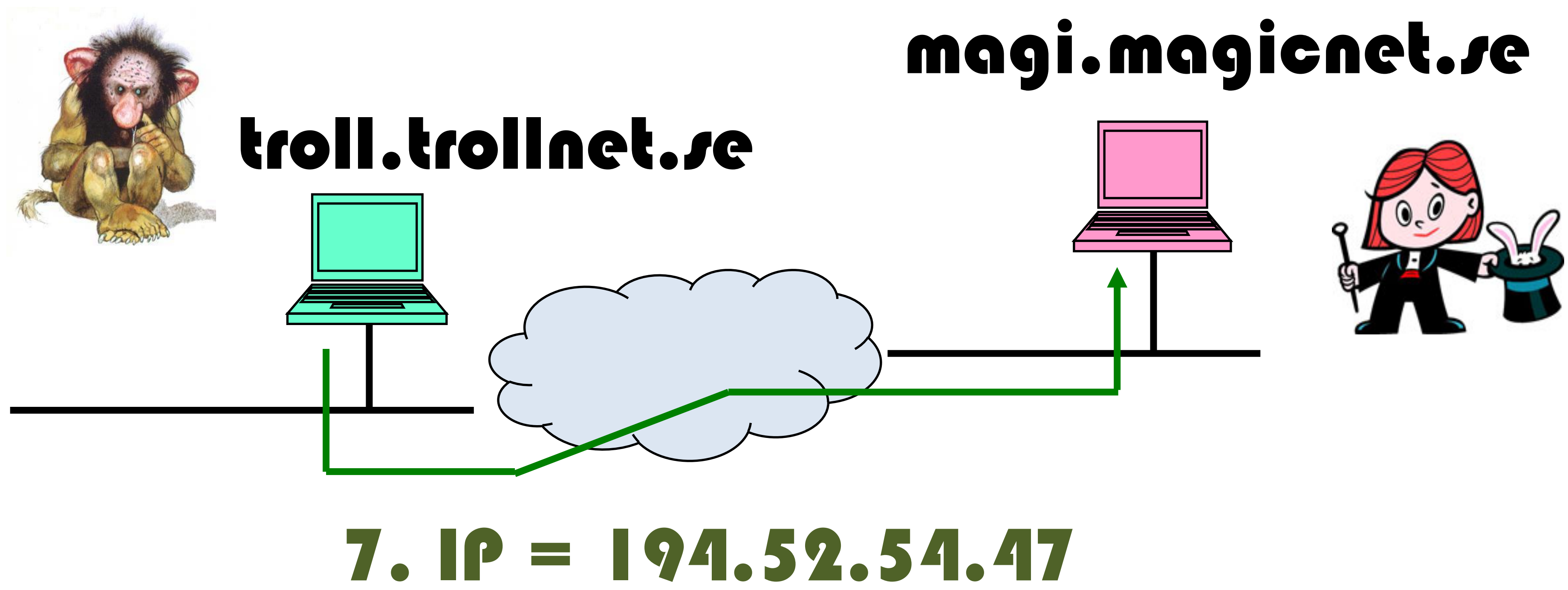
Domain name to IP address (2)



Domain name to IP address (3)



Domain name to IP address (4)

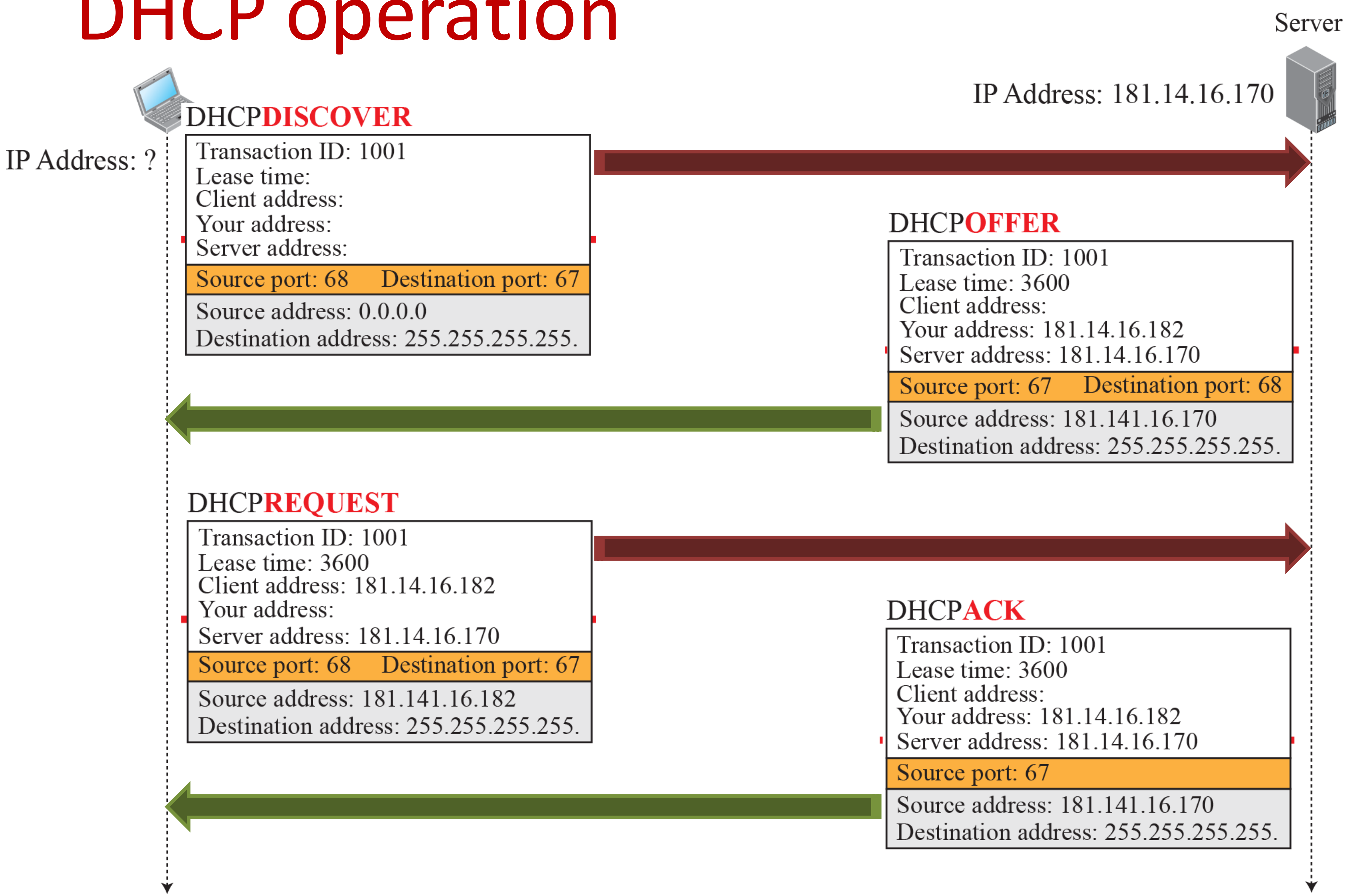


Obtaining an IP address

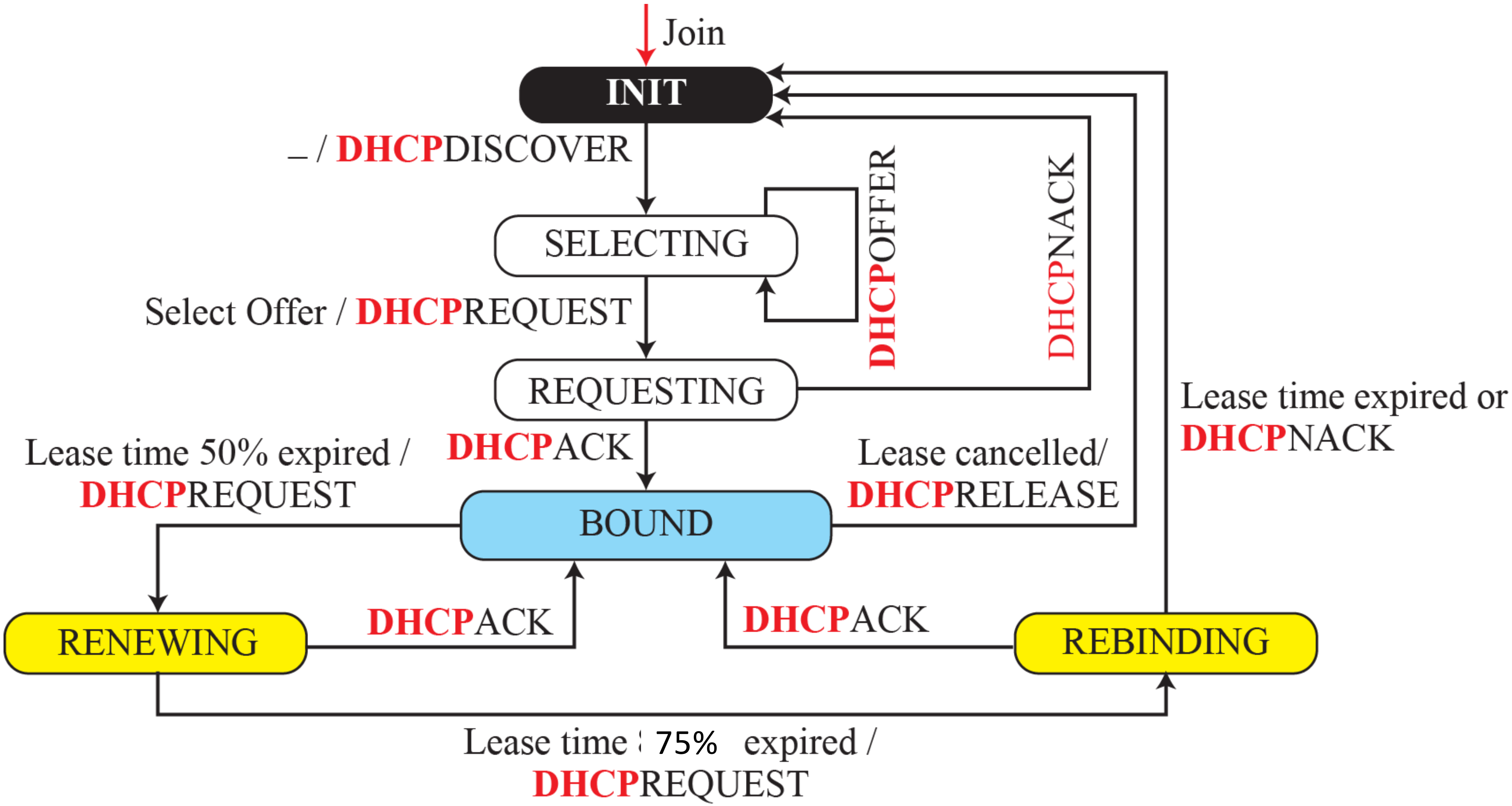
- Dynamic Host Configuration Protocol
  - Application layer

- DHCP
  - IP address
    - Allocation from pool or static
  - Network mask
  - Default gateway
  - DNS server(s)

DHCP operation



DHCP states



Join
INIT
_ / DHCPDISCOVER
SELECTING
DHCPOFFER
DHCPNACK
Select Offer / DHCPREQUEST
REQUESTING
Lease time expired or
DHCPNACK
Lease time 50% expired /
DHCPREQUEST
DHCPACK
Lease cancelled/
DHCPRELEASE
BOUND
RENEWING
DHCPACK
DHCPACK
REBINDING
Lease time 75% expired /
DHCPREQUEST

EITF25 – Internet: Technology and Applications

Application Layer
-2-
User Applications

2015, Lecture 10

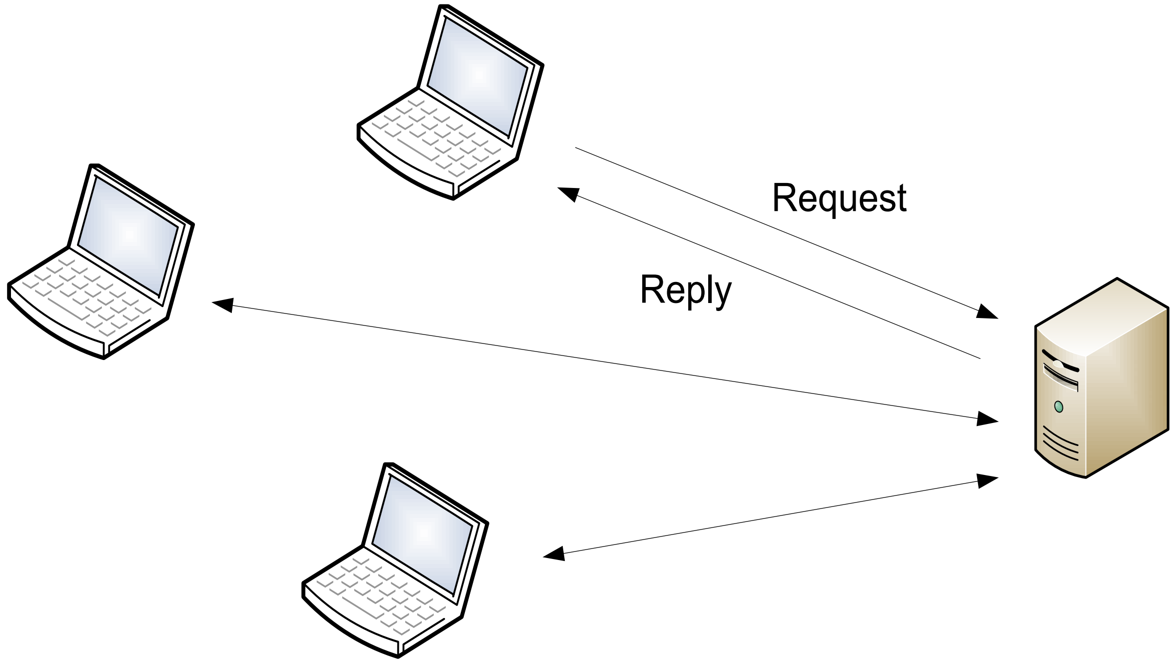
Kaan Bür

Application layer paradigms

- Client-server paradigm
  - WWW, Online games, Web TV, Facebook
- Peer-to-peer paradigm
  - BitTorrent, Voddler, Skype
- Some applications use both paradigms
  - Spotify

Client/server paradigm

- Most early applications were based on it
  - http
  - ftp
  - e-mail

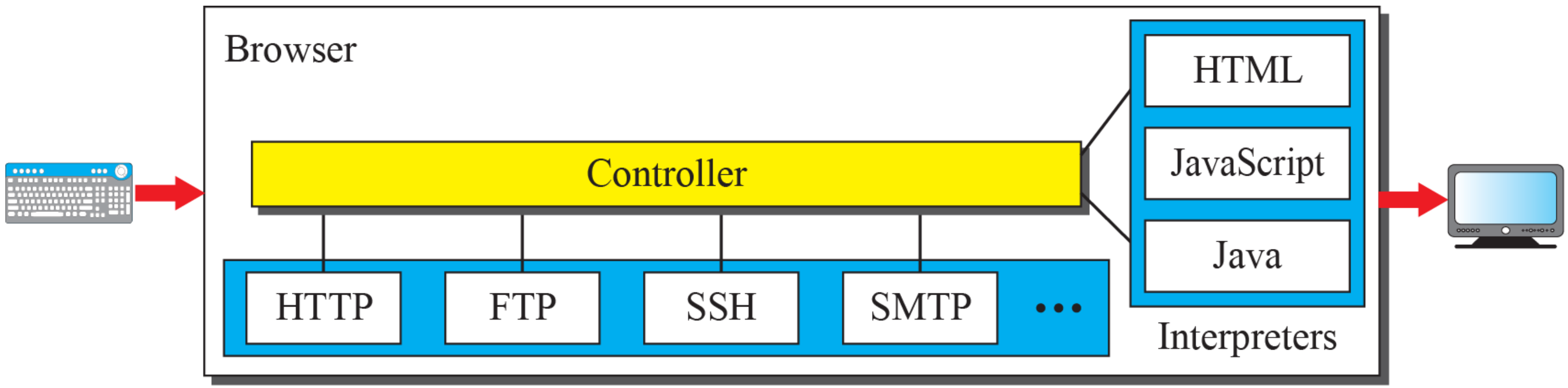


World Wide Web (WWW)

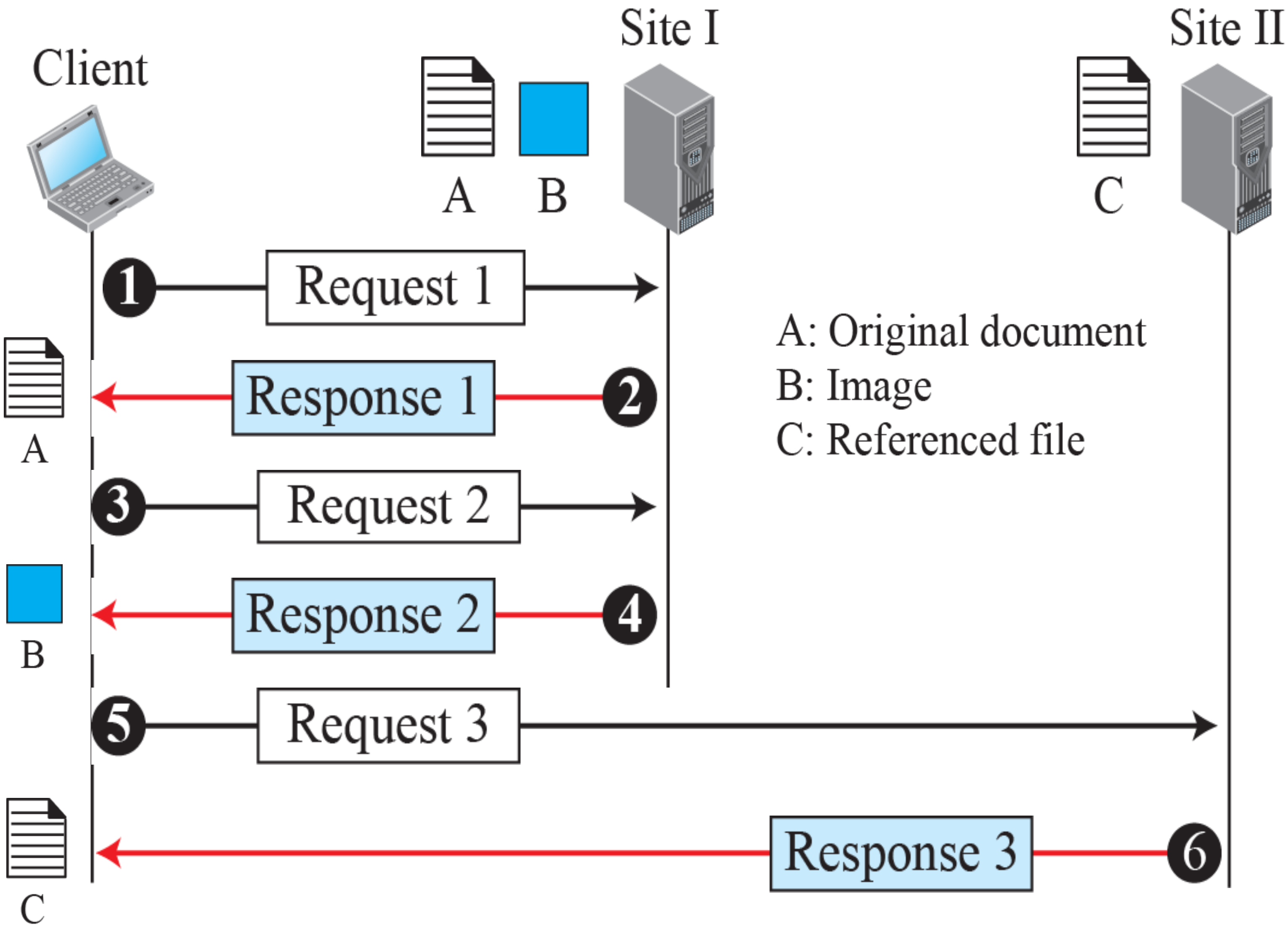
- Web documents (pages)
  - HyperTextMarkup Language (HTML) for static pages
  - Script languages (PHP, ASP, JSP, CGI etc.) for dynamic
- Universal Resource Locator (URL)
  - Standard way to identify location of web documents
  - **protocol://host:port/path**
- HyperText Transfer Protocol (HTTP)
  - Protocol to retrieve documents from a web server

Hypertext Transfer Protocol (HTTP)

- Text-based protocol
- Two basic types of messages
  - Requests and Responses
- Sets up and uses a TCP connection



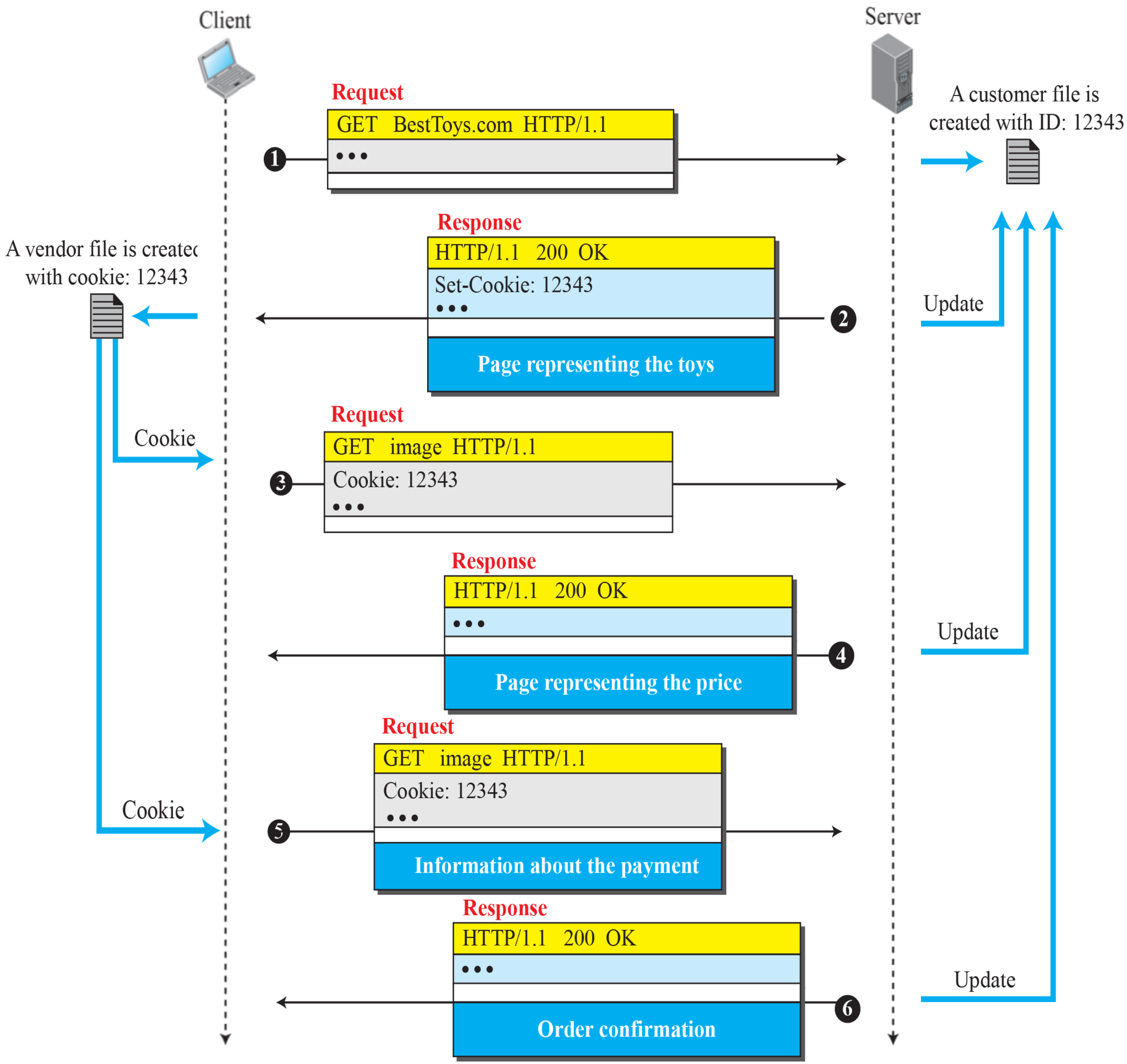
Document retrieval



Cookies

- Original WWW was stateless
  - Each request/response treated separately
  - No history of previous messages
- Cookies
  - store information about client
  - introduce concept of a user session
- Implementation (creation and storage) of cookies can be different, but same concept

Cookies



Client
Server
A customer file is created with ID: 12343
Request
GET BestToys.com HTTP/1.1
• • •
1
Response
HTTP/1.1 200 OK
Set-Cookie: 12343
• • •
Page representing the toys
2
A vendor file is createc with cookie: 12343
Update
Cookie
Request
GET image HTTP/1.1
Cookie: 12343
• • •
3
Response
HTTP/1.1 200 OK
• • •
Page representing the price
4
Update
Cookie
Request
GET image HTTP/1.1
Cookie: 12343
• • •
Information about the payment
5
Response
HTTP/1.1 200 OK
• • •
Order confirmation
6
Update

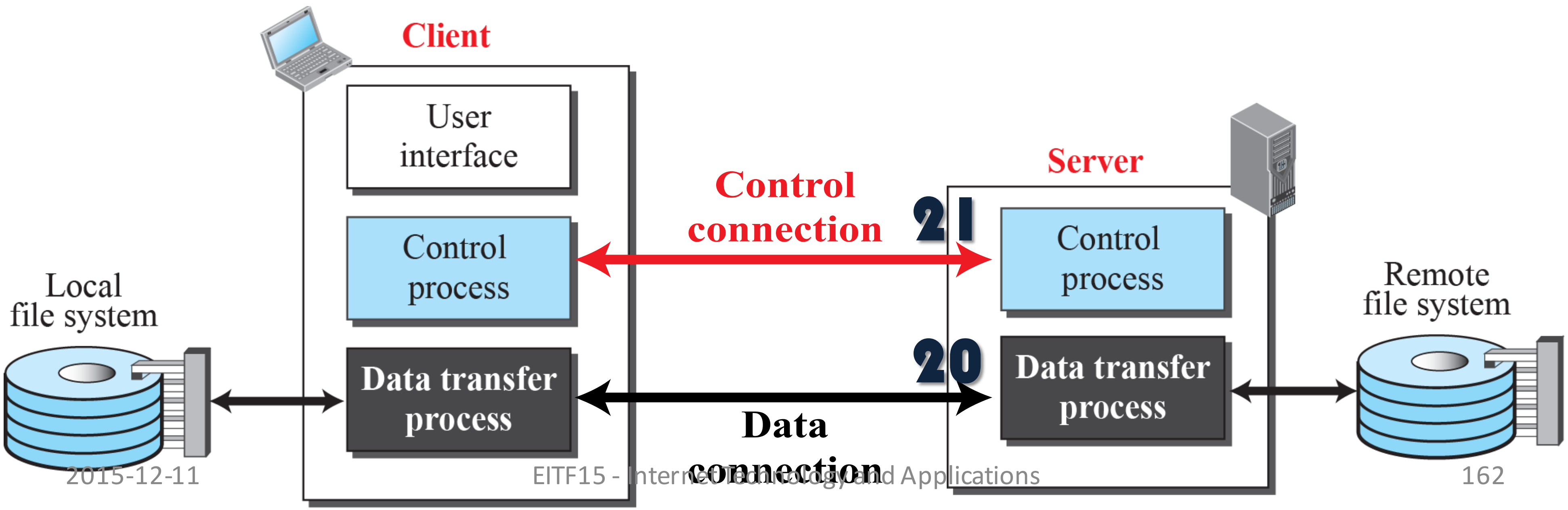
File Transfer Protocol (FTP) - 1971

Control connection

- Open for entire session
- Commands & responses
  - ASCII

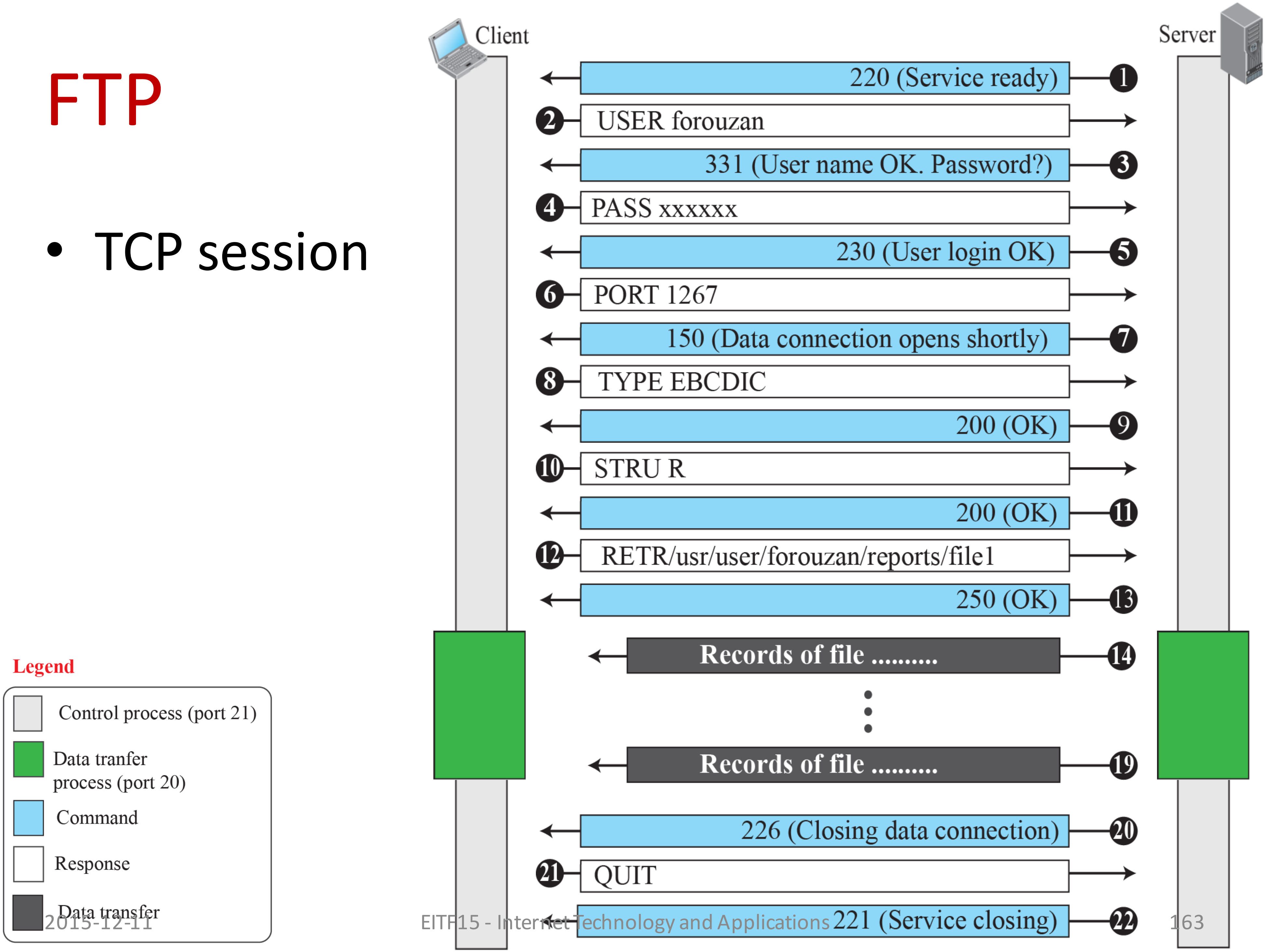
Data connection

- New one for each file

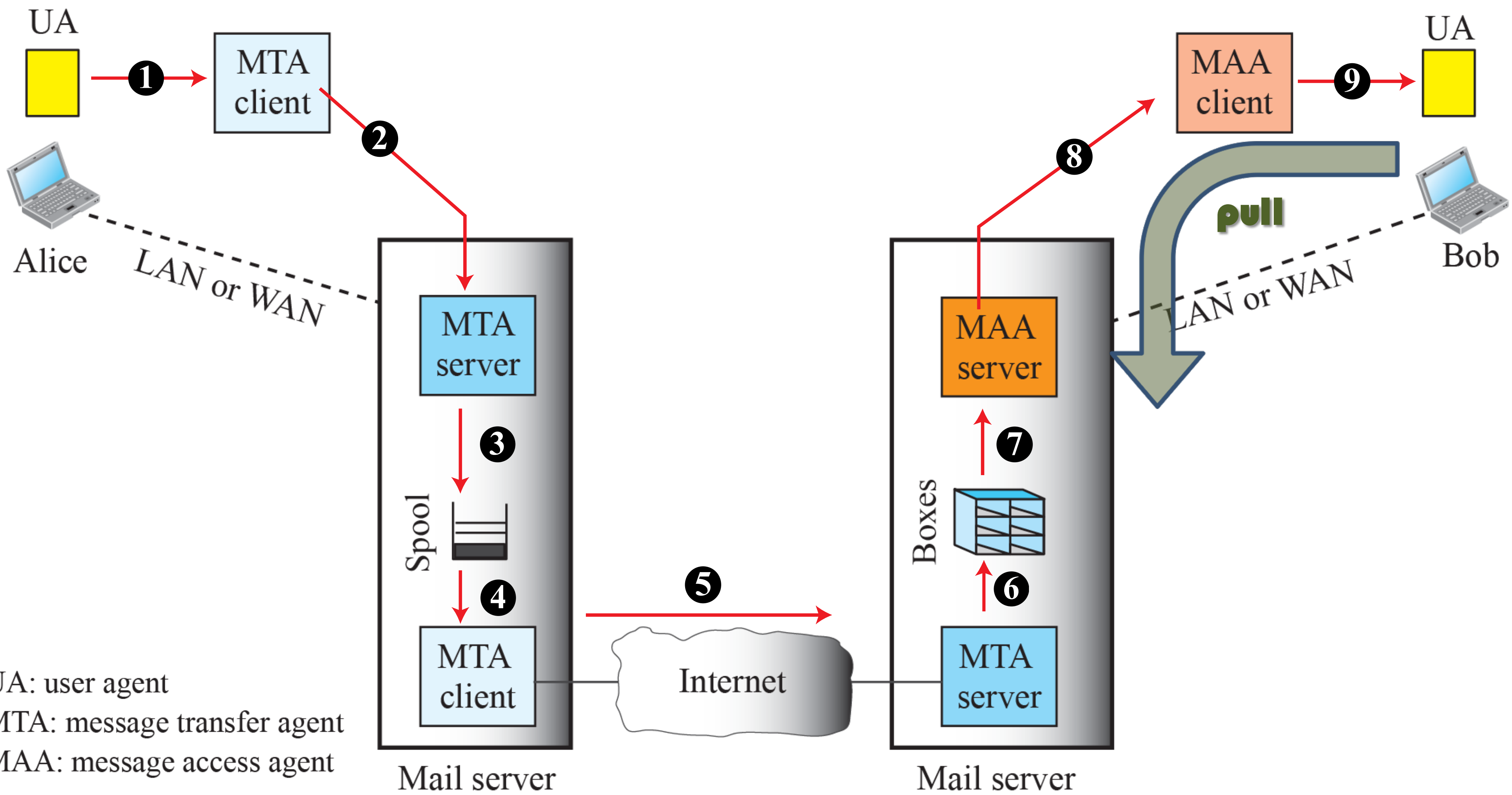


FTP

- TCP session



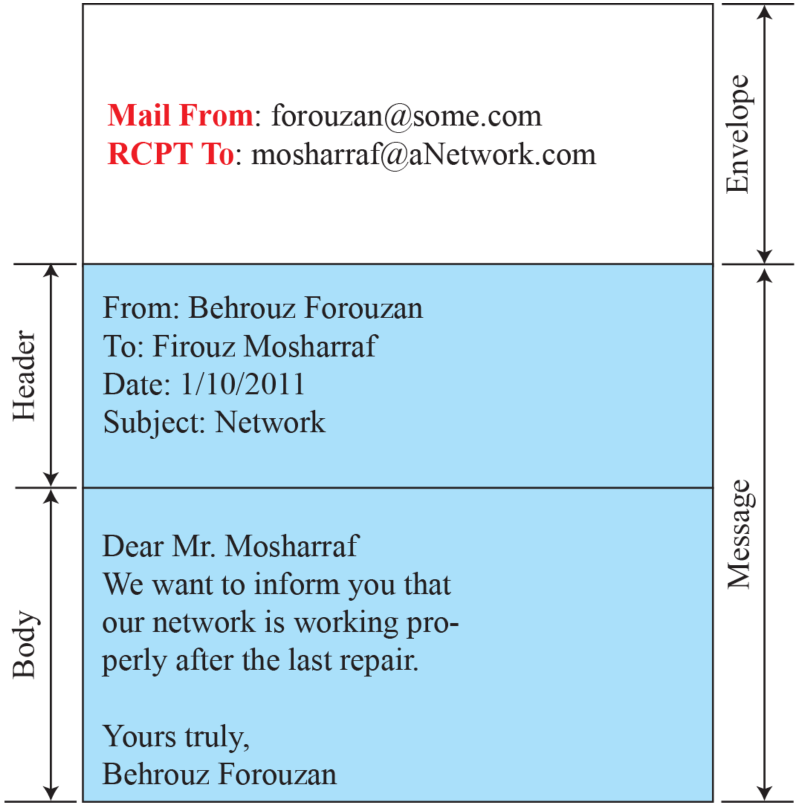
Electronic mail (e-mail) - 1971

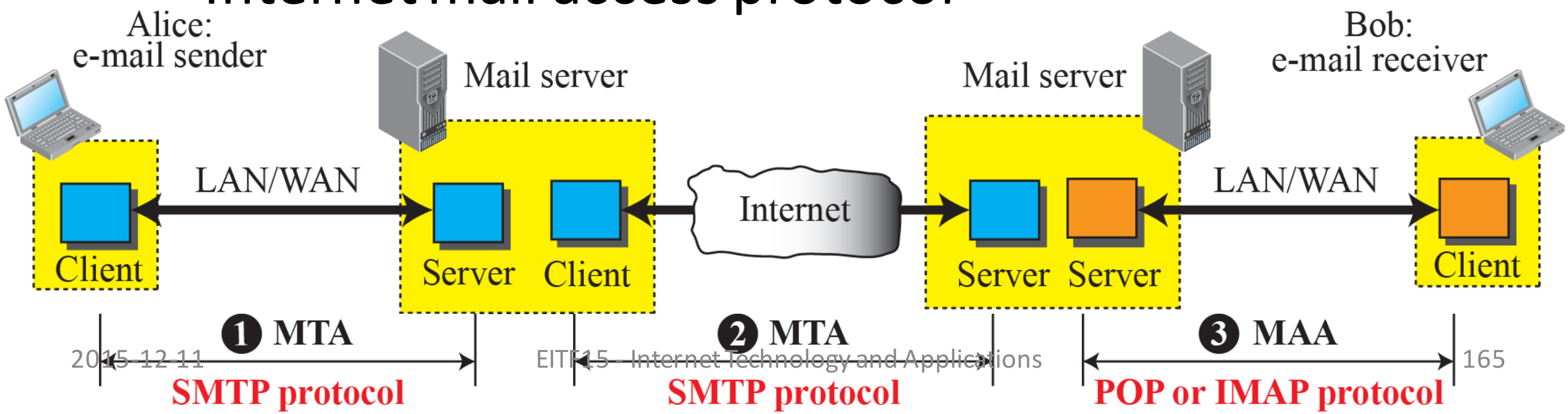


UA: user agent
MTA: message transfer agent
MAA: message access agent

E-mail: protocols used

- SMTP
  - Simple mail transfer protocol
- POP
  - Post office protocol
- IMAP
  - Internet mail access protocol

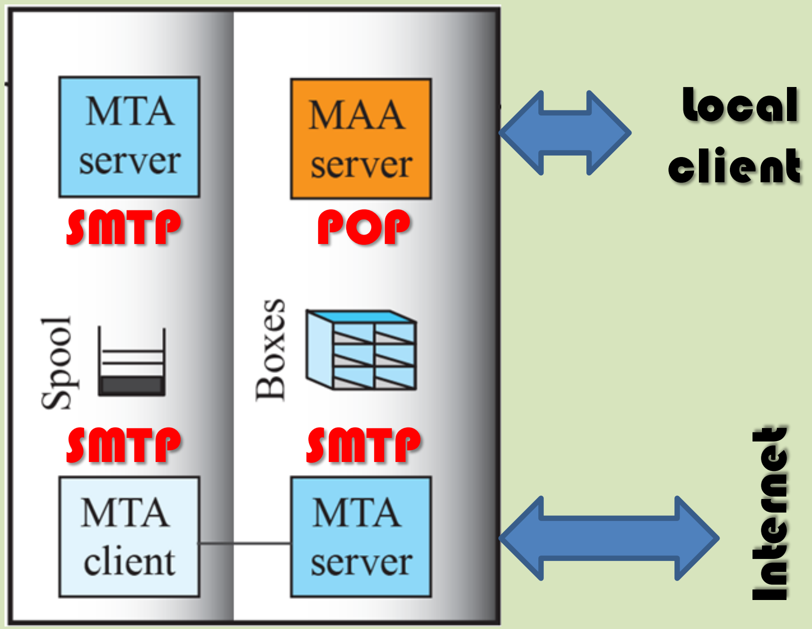




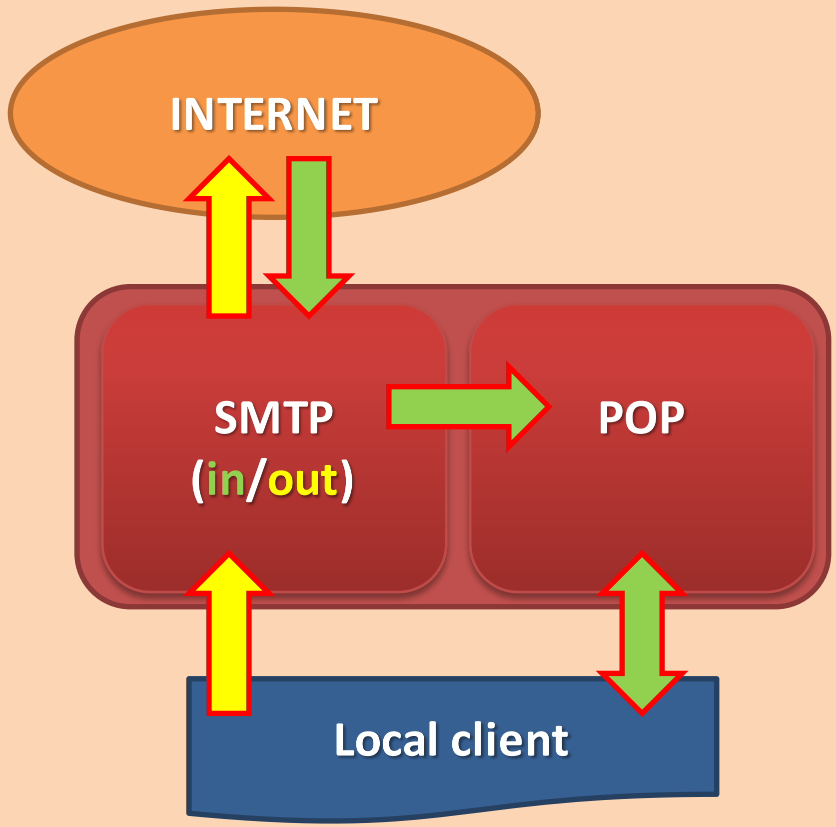
E-mail: server architecture

Sender & receiver in one

- Not a very good representation!



A holistic view



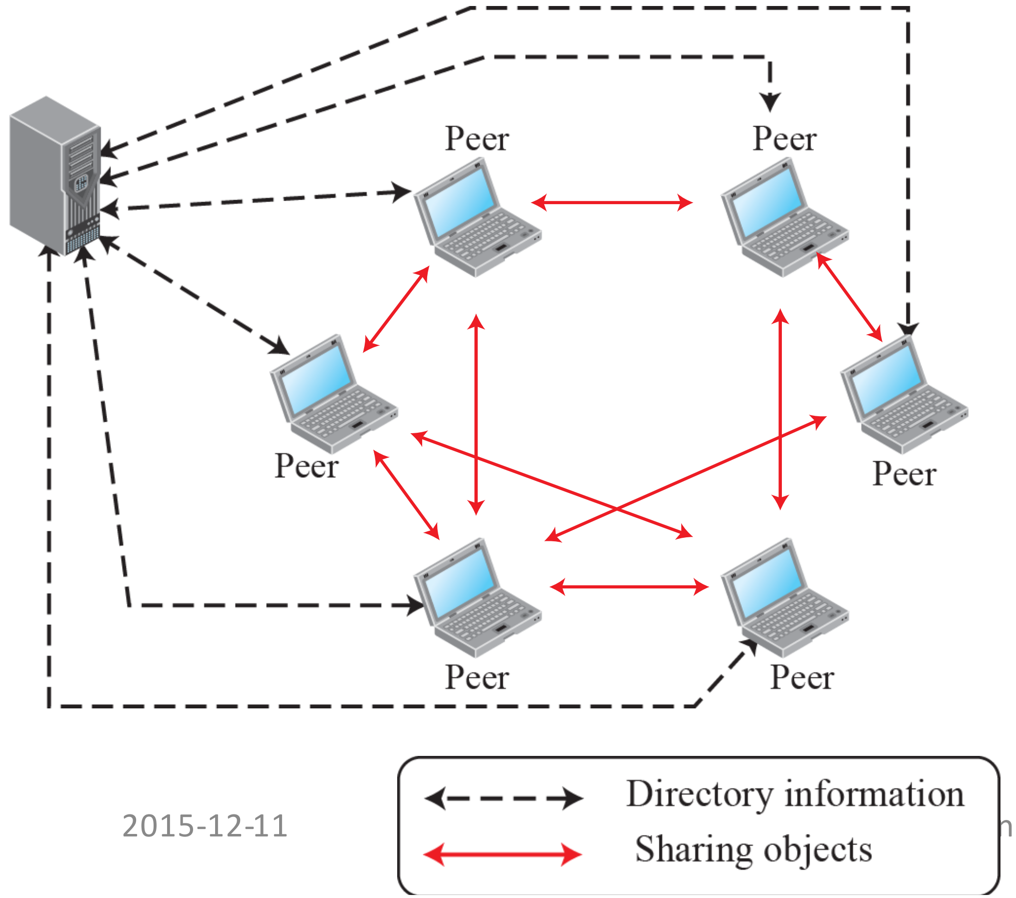
Performance challenges

- Client/server architectures
  - Standardized protocols like HTTP
  - Heavy traffic load on network infrastructure
  - Unicast transmission
  - Delays due to overloaded access networks
  - Single point of failure

Peer-to-peer (P2P) paradigm

Centralised

- Directory server



Decentralised

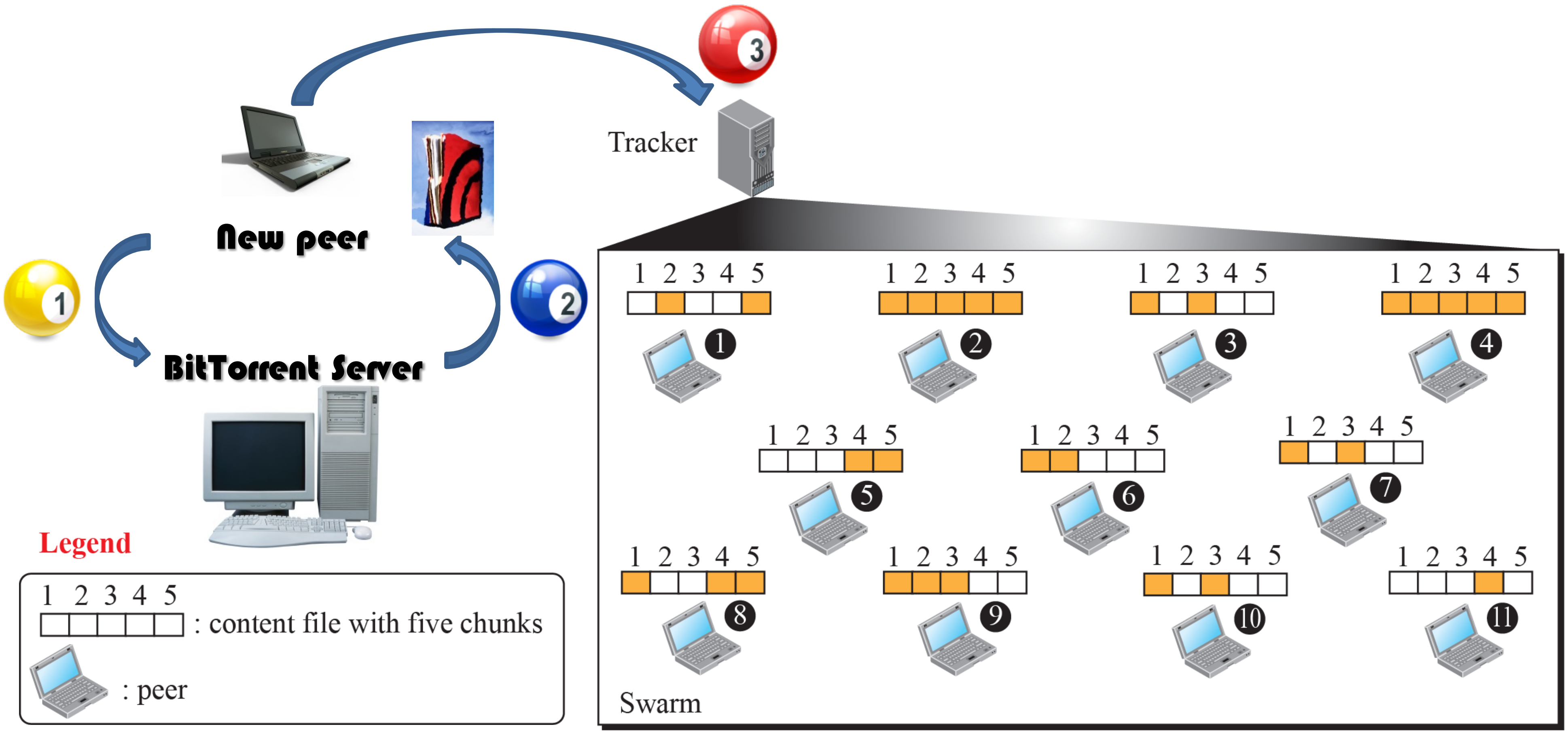
- Overlay network
  - Logical on top of physical
- A) unstructured
  - Nodes linked randomly
  - Queries flood network
- B) structured
  - Nodes linked with rules (DHT)
  - More efficient query resolving
- Initial list of nodes provided

P2P example: BitTorrent

- Group of peers work together to give all peers a copy of shared file.
  - Torrent (metadata about file and tracker)
  - Tracker (server with info on swarm)
  - Swarm (file-sharing group with seeds and leechers)
  - Seed (down- and uploader within swarm)
  - Leecher (downloader within swarm)
- No downloading whole file from one peer

Tracker

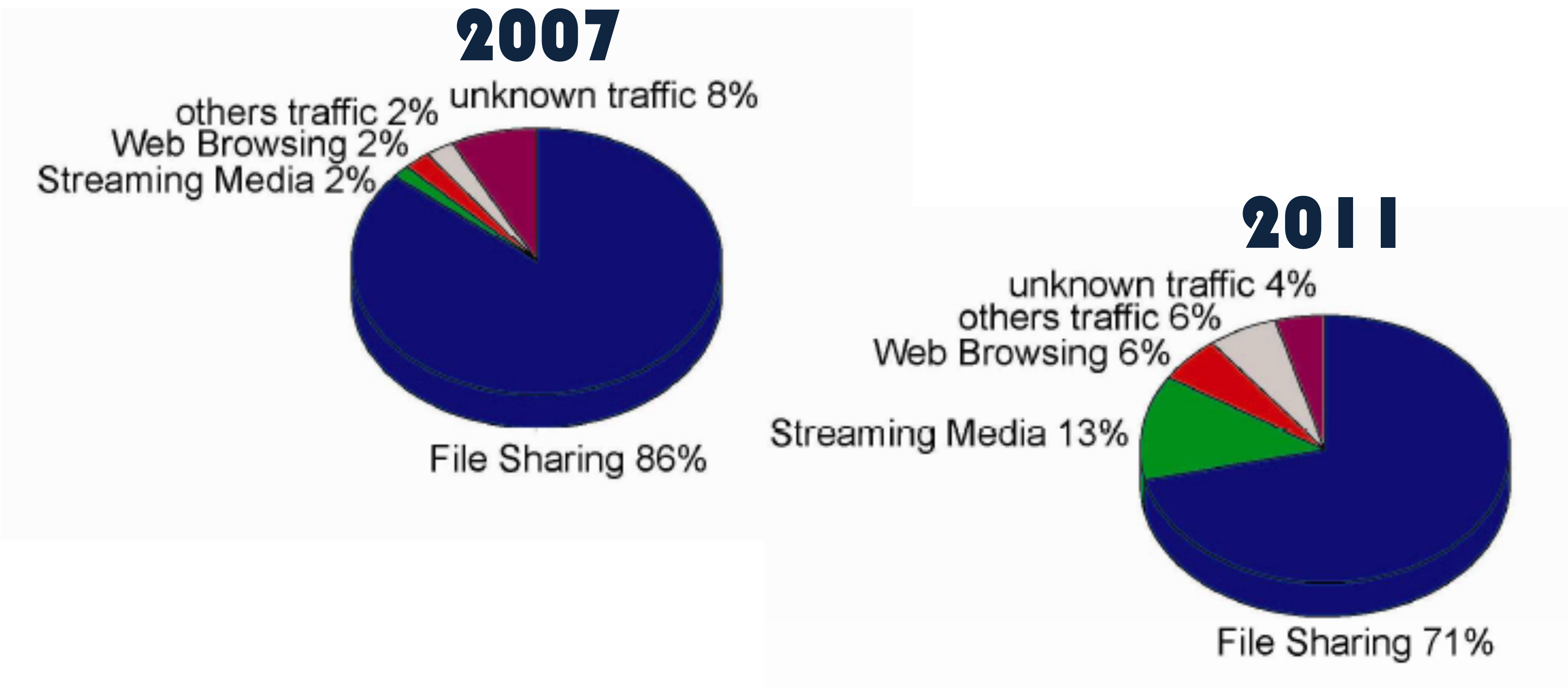
- Provides list of peers for given torrent



Note: Peers 2 and 4 are seeds; others are leeches.

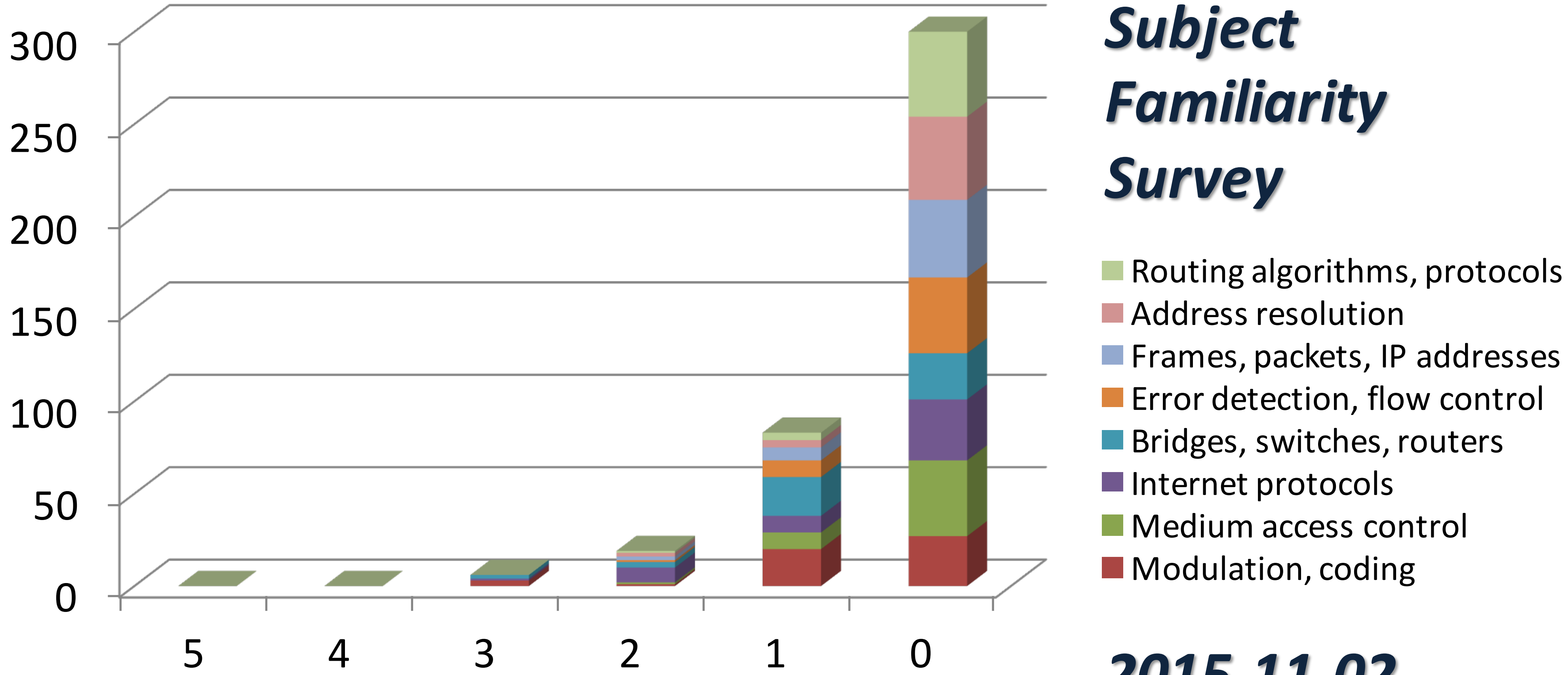
Evolution of Internet usage

- Traffic volumes generated by users



J. Li, A. Aurelius, V. Nordell, M. Du, Å. Arvidsson, M. Kihl:
A five year perspective of traffic pattern evolution in a residential broadband access network
Future Network & Mobile Summit 2012

This concludes our lectures. Thank you for your attendance.



Subject Familiarity Survey

2015-11-02

(5 = full familiarity; 0 = no familiarity at all)