Network Basics

Outline

- Introduction to network protocols
- TCP/IP & OSI
- Some network threats

Introduction

- A network protocol is used for communication between entities in different systems

- For two entities to communicate successfully, they must "speak the same language."
  - What is communicated, how it is communicated, and when it is communicated

- When communication is not simple, we may divide the complex task of communication into several **layers**. In this case, we may need several protocols, one for each layer.

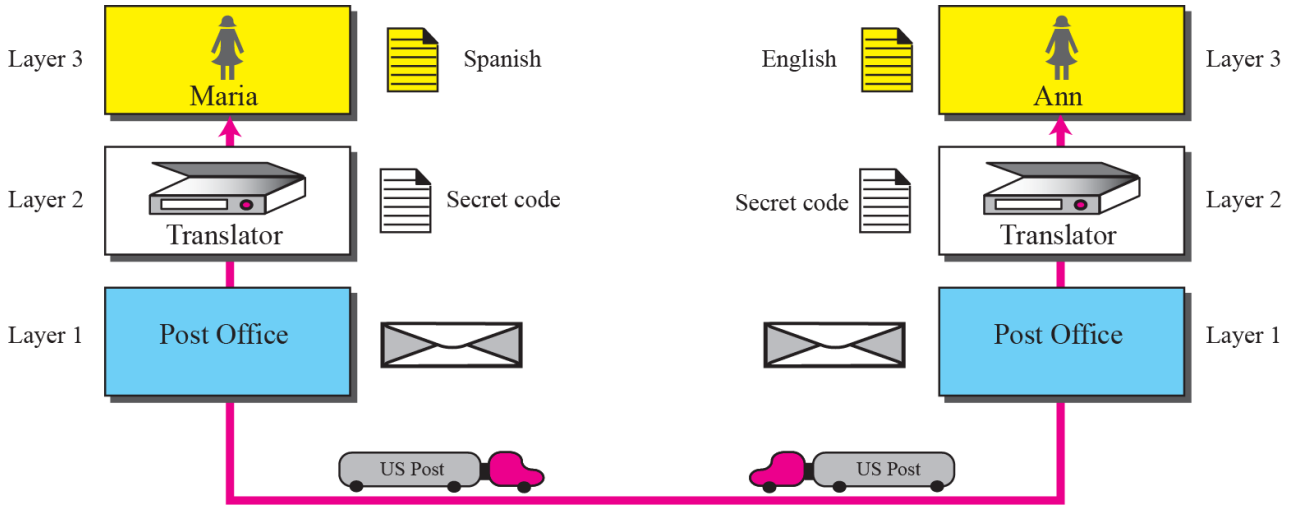
Example

- Assume Maria and Ann are neighbors with a lot of common ideas. However, Maria speaks only Spanish, and Ann speaks only English. Since both have learned the sign language in their childhood, they enjoy meeting in a cafe a couple of days per week and exchange their ideas using signs. Communication is face to face and happens in one layer.

Source: Behrouz A. Forouzan, TCP/IP Protocol Suite

Example

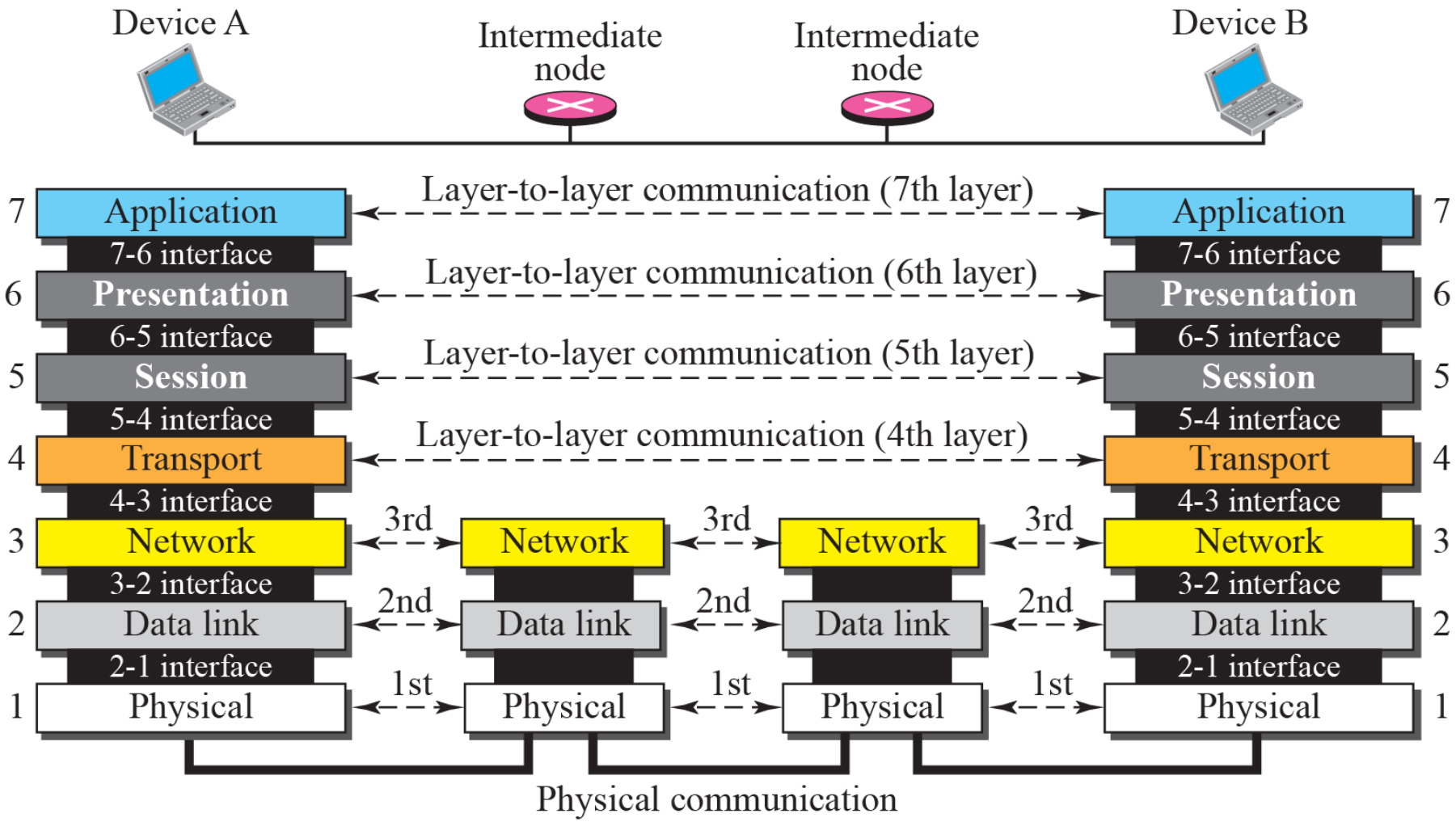
- Now assume that Ann has to move to another town because of her job. Before she moves, the two meet for the last time in the same cafe. Although both are sad, Maria surprises Ann when she opens a packet that contains two small machines. The first machine can scan and transform a letter in English to a secret code or vice versa. The other machine can scan and translate a letter in Spanish to the same secret code or vice versa. Ann takes the first machine; Maria keeps the second one. The two friends can still communicate using the secret code.



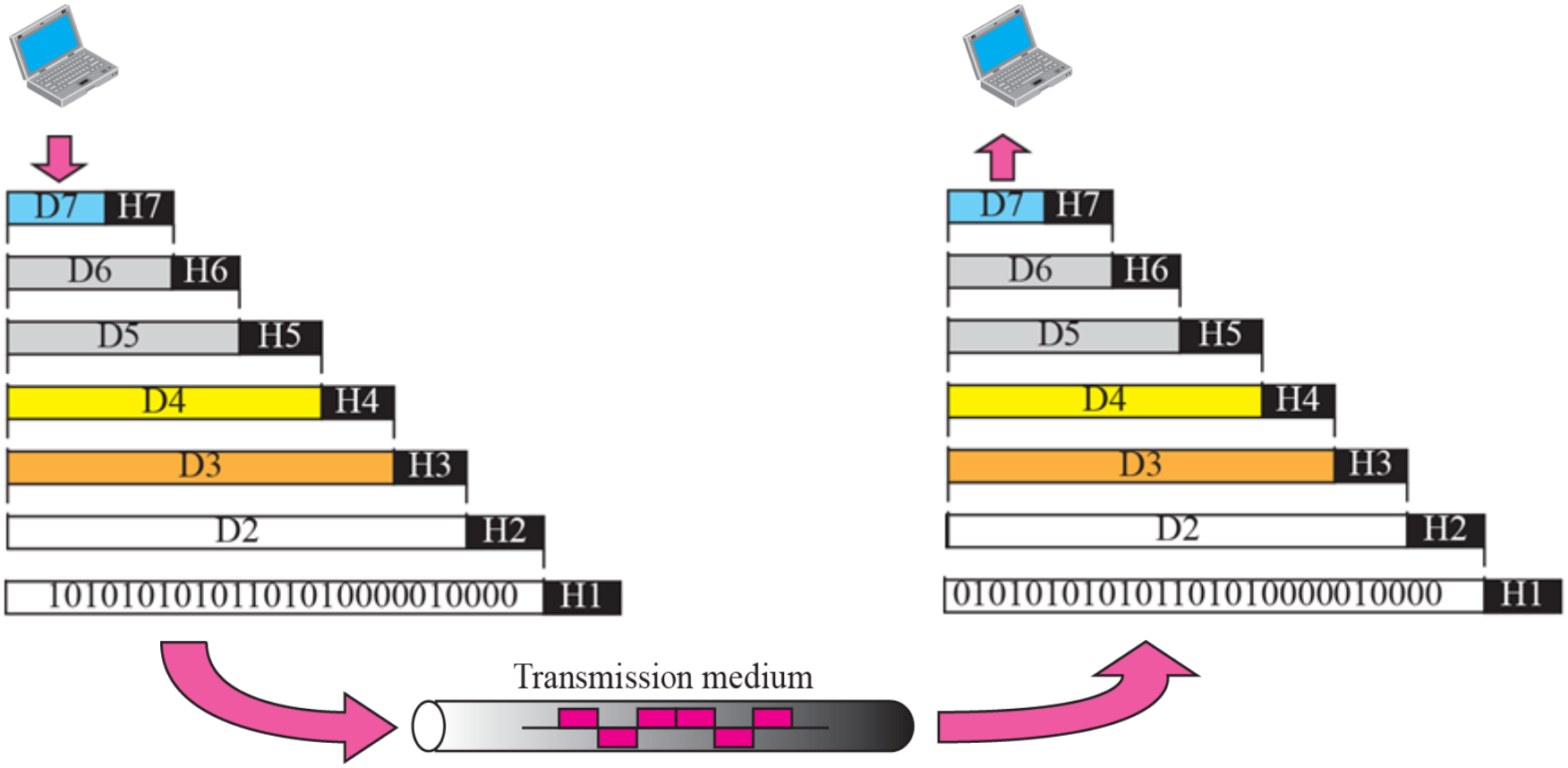
OSI: the Seven-Layer Model

- …dates back to 1983 and was released by ISO.
- The OSI is an abbreviation of Open Systems Interconnection.
- Generally we distinguish between the upper layers, the top three, and the lower layers, the bottom four.
  - Effectively the upper layers are local and associated with the “end-user”, while the lower layers relate to the actual network and communication services.
- http://en.wikipedia.org/wiki/OSI_model

OSI Layers


Device A
Intermediate node
Intermediate node
Device B
Layer-to-layer communication (7th layer)
Layer-to-layer communication (6th layer)
Layer-to-layer communication (5th layer)
Layer-to-layer communication (4th layer)
7
Application
7-6 interface
6
Presentation
6-5 interface
5
Session
5-4 interface
4
Transport
4-3 interface
3
Network
3-2 interface
2
Data link
2-1 interface
1
Physical
3rd
2nd
1st
Physical communication

OSI Layers

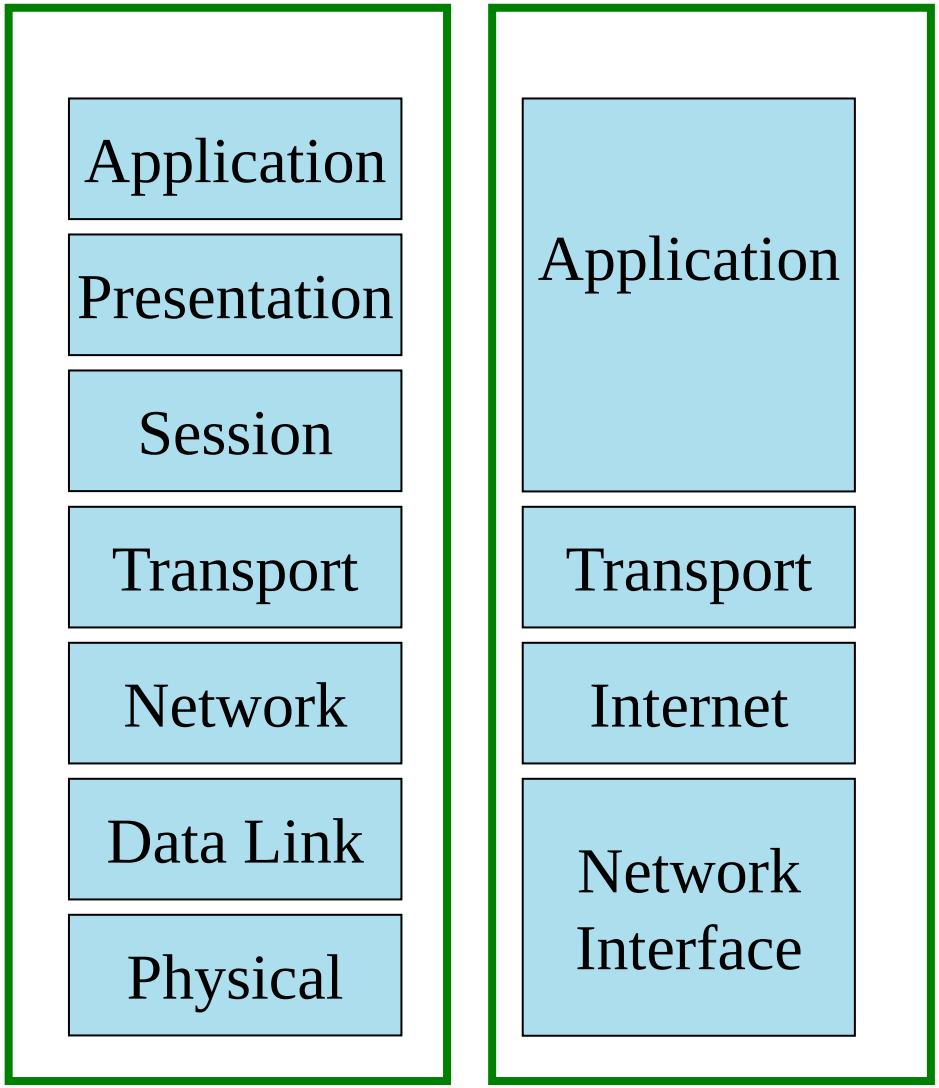

D7
H7
D6
H6
D5
H5
D4
H4
D3
H3
D2
H2
1010101010110101000010000
H1
Transmission medium
D7
H7
D6
H6
D5
H5
D4
H4
D3
H3
D2
H2
0101010101011010000010000
H1

TCP/IP Suite

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model.
- The original TCP/IP protocol suite was defined as four software layers built upon the hardware.
- Today, however, TCP/IP is thought of as a five-layer model with the layers named similarly to the ones in the OSI model.

OSI vs TCP/IP Model

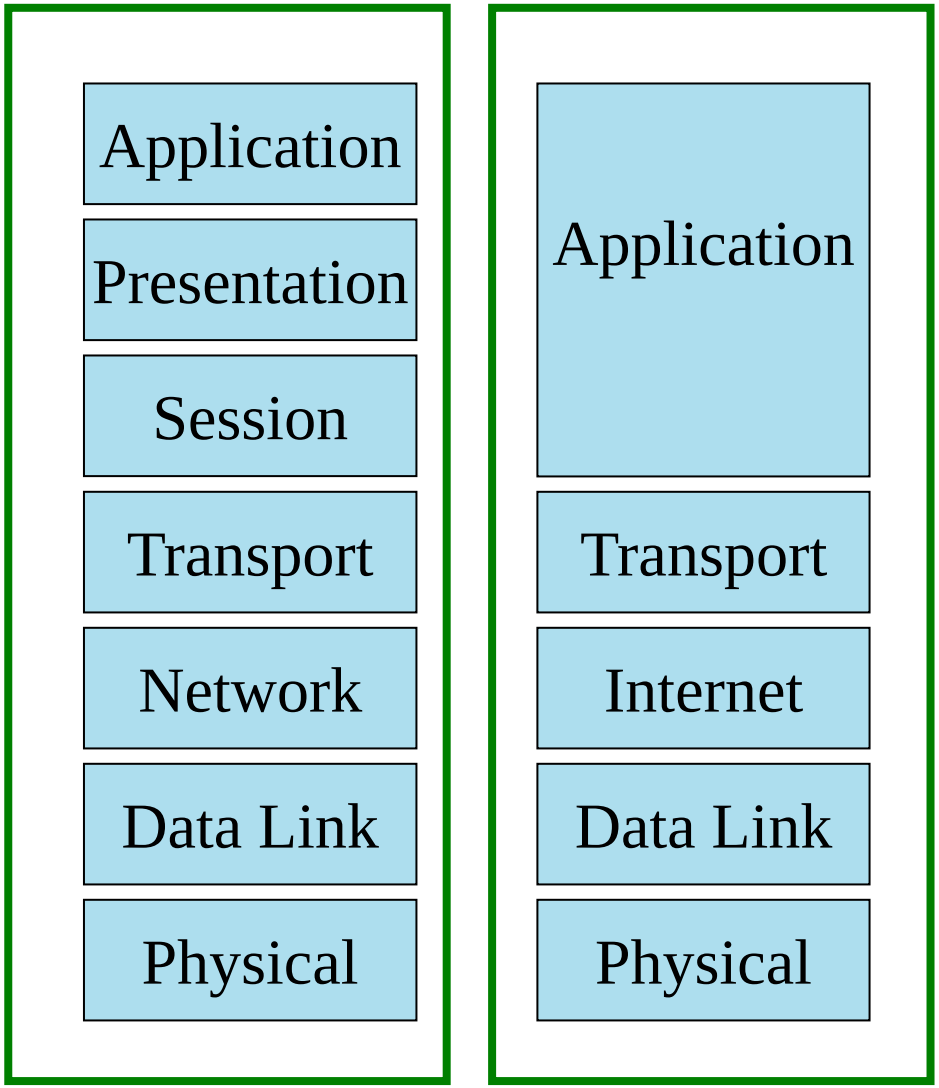
OSI Reference Model



TCP/IP Internet Model

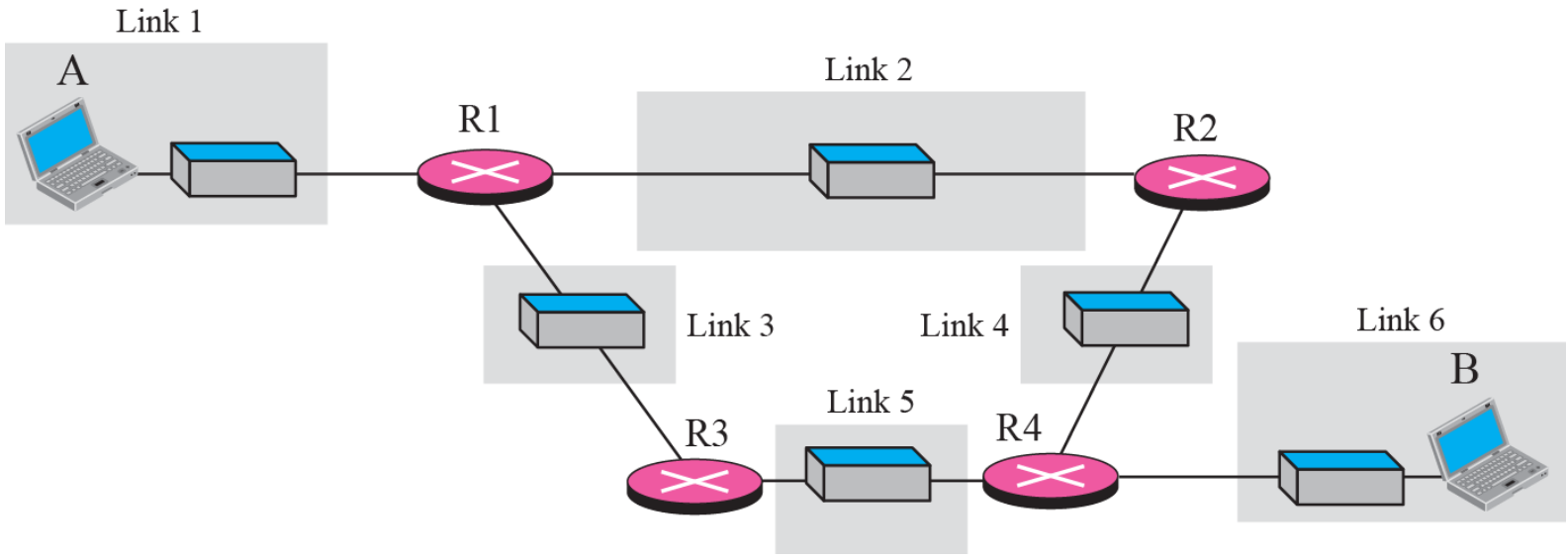
OSI vs TCP/IP Model

7-layer OSI Reference Model



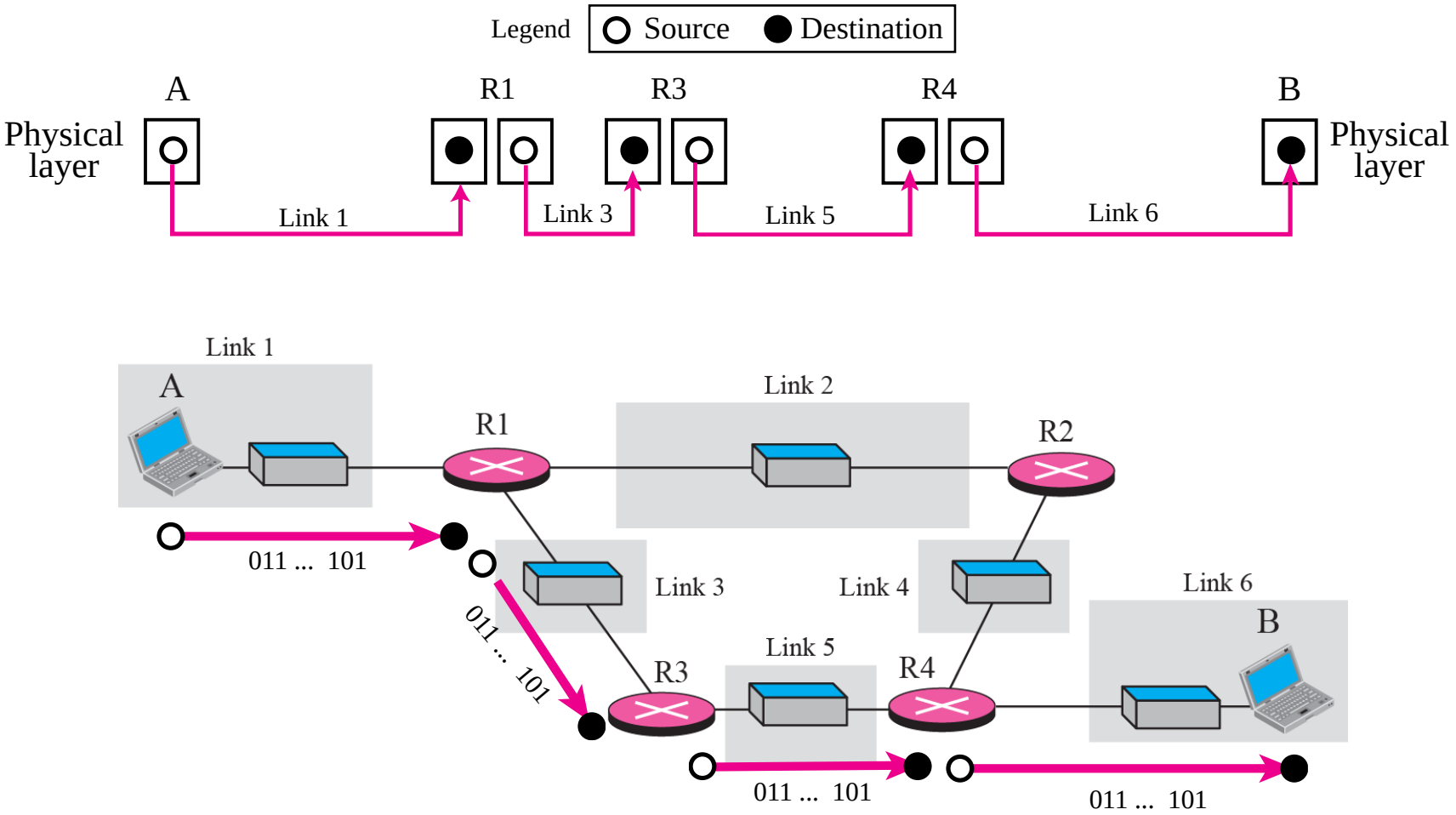
5-layer TCP/IP Internet Model

Example

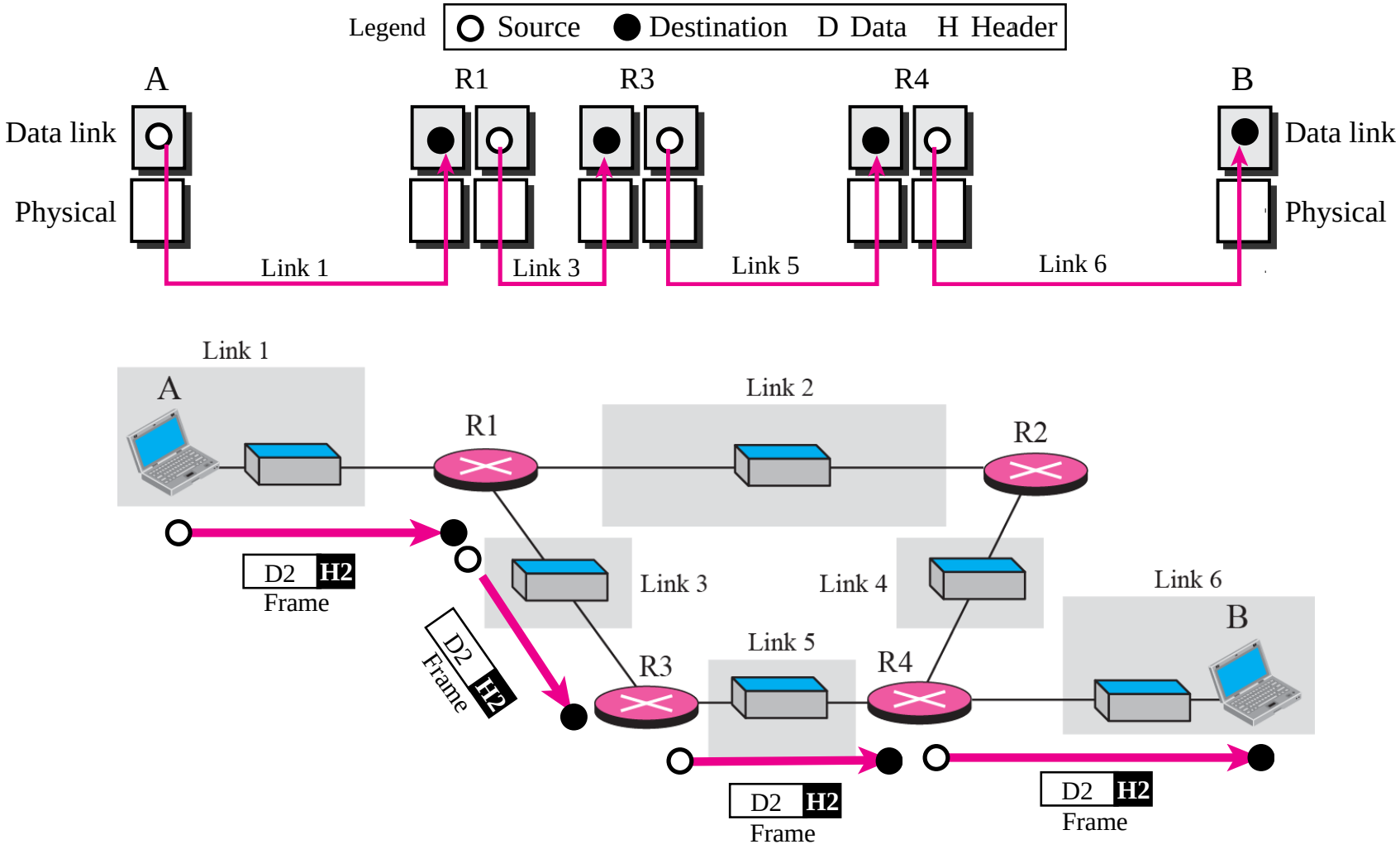


A Computer Network

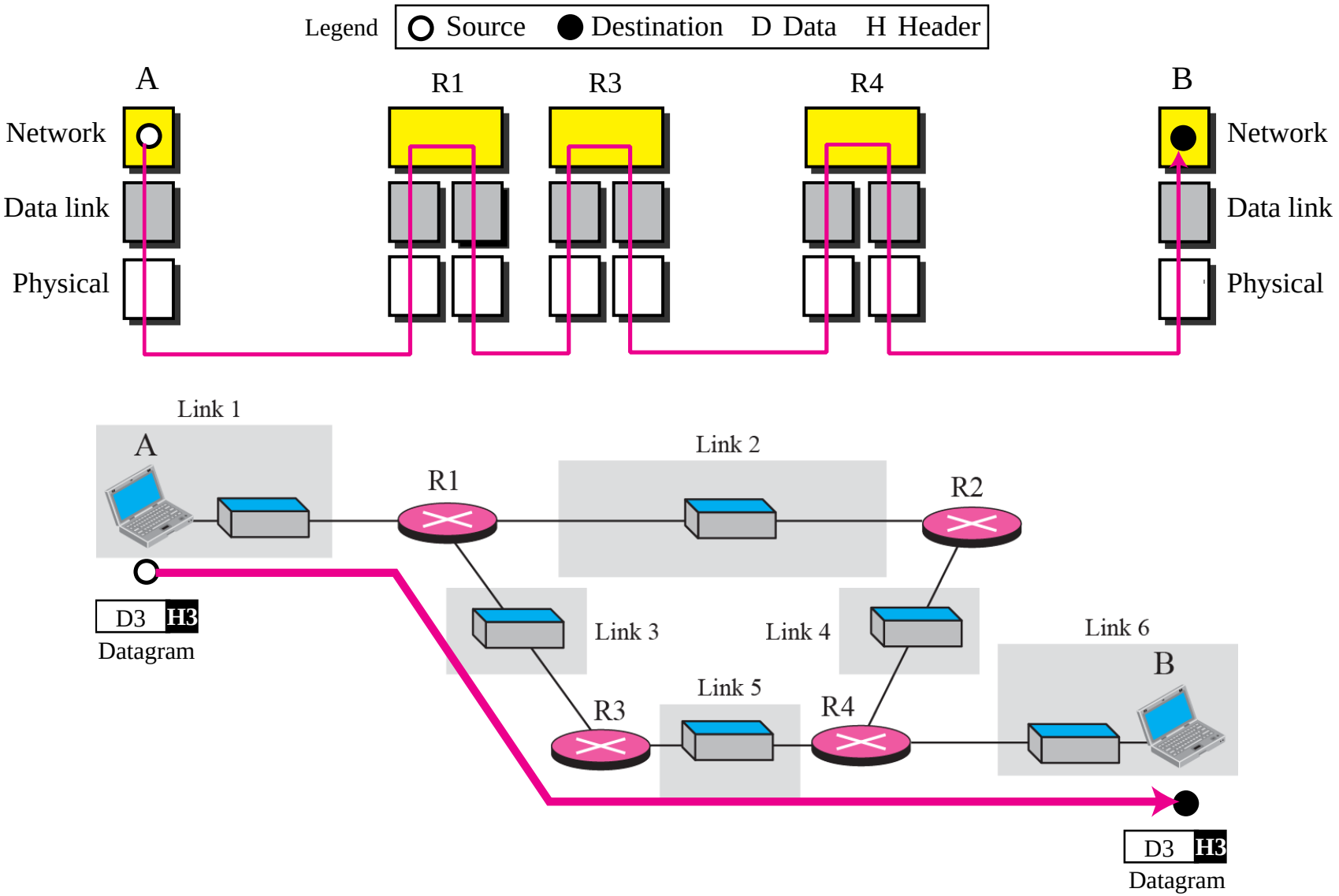
Communication at physical layer



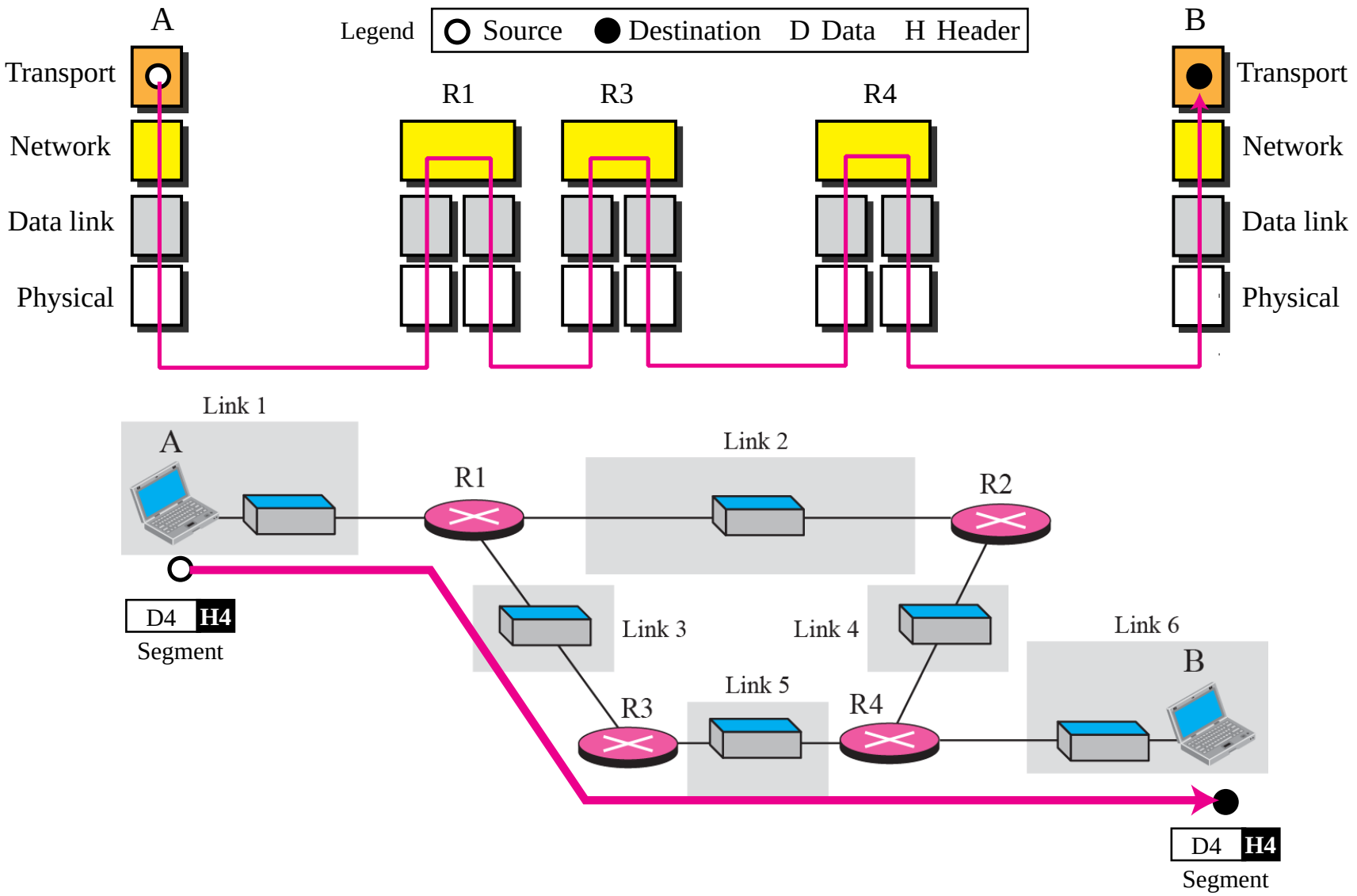
Communication at Data Link layer



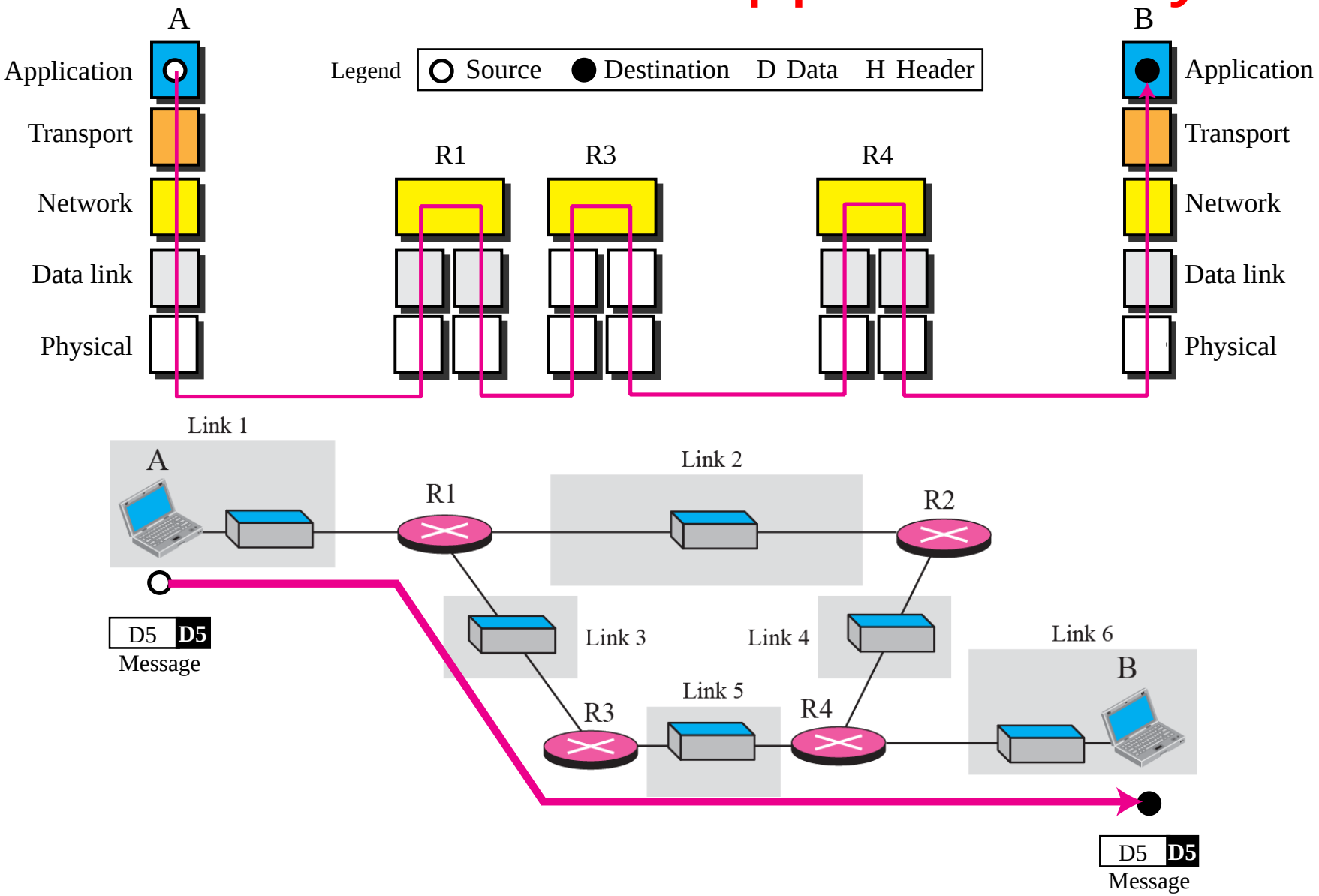
Communication at Network layer



Communication at Transport layer



Communication at Application layer



Addressing

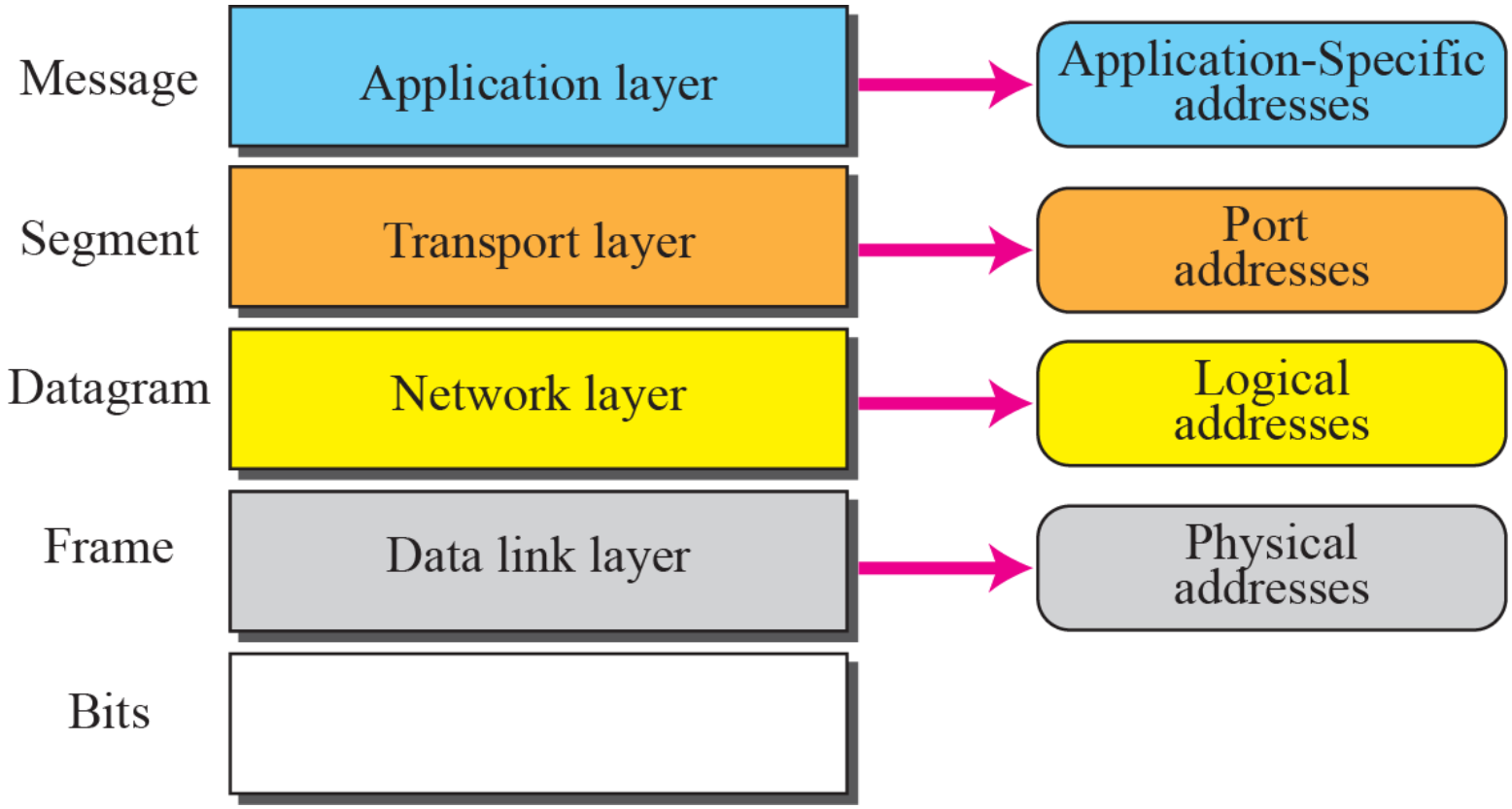
- Each computer on a network requires a unique address on that network
- Each application requires a unique address within the computer to allow support for multiple applications

Addresses in the TCP/IP

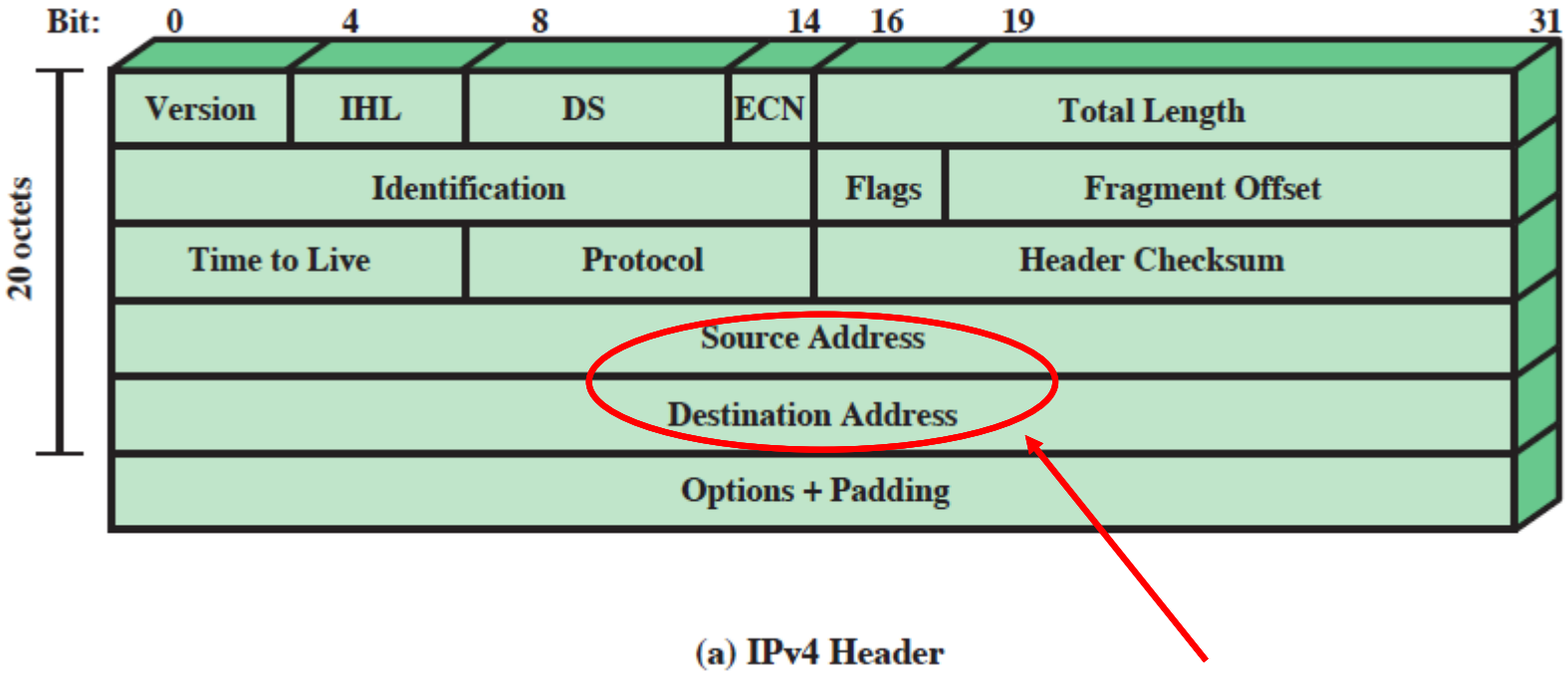
- Four levels of addresses are used in a network employing the TCP/IP protocols:
  - physical address, e.g., **07:01:02:01:2C:4B**
  - logical address, e.g., **130.130.215.2**
  - port address, e.g., **80**
  - application-specific address, e.g.,

    www.uow.edu.au
- Each address is related to a one layer in the TCP/IP architecture

Addresses in the TCP/IP



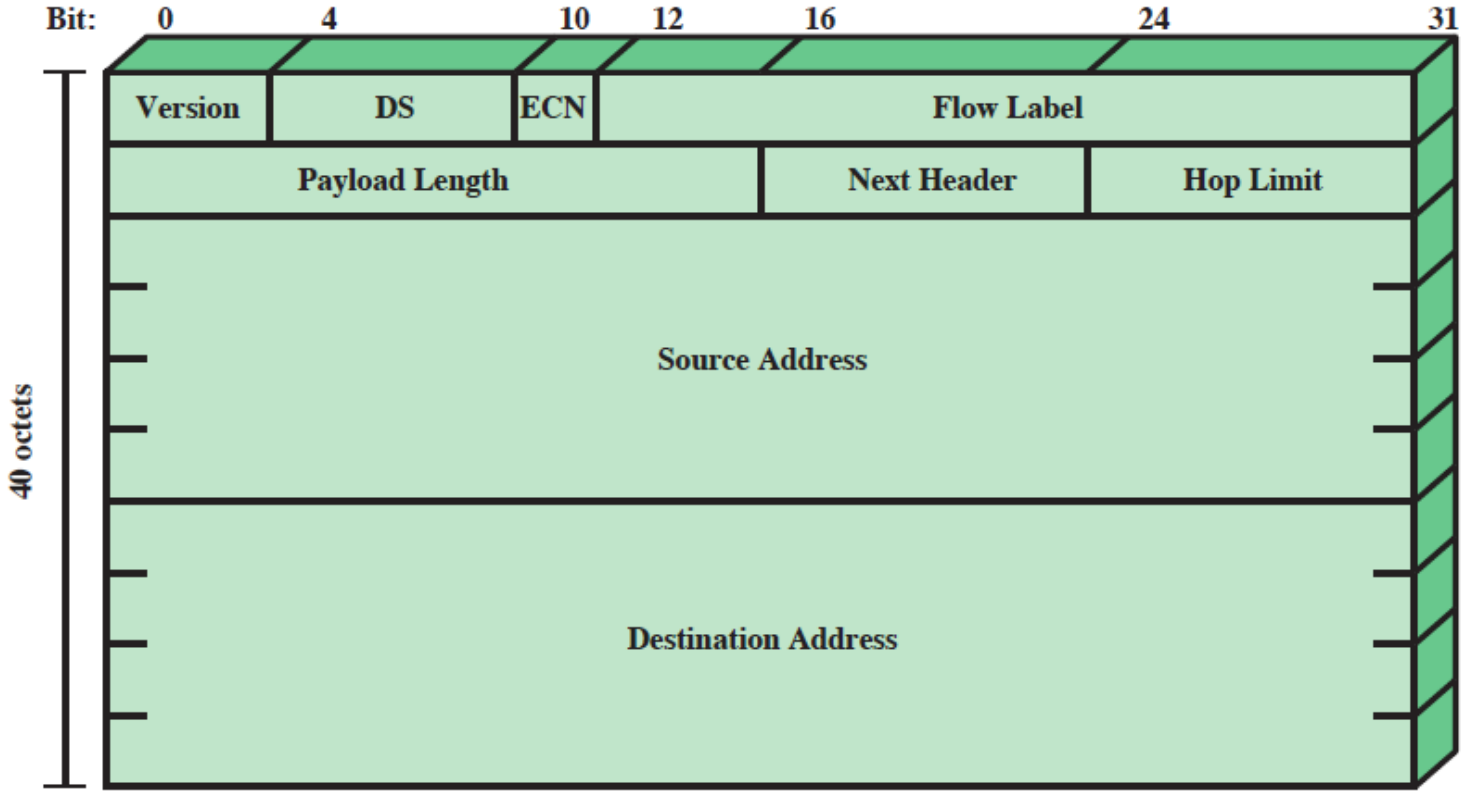
IPv4 Header



(a) IPv4 Header

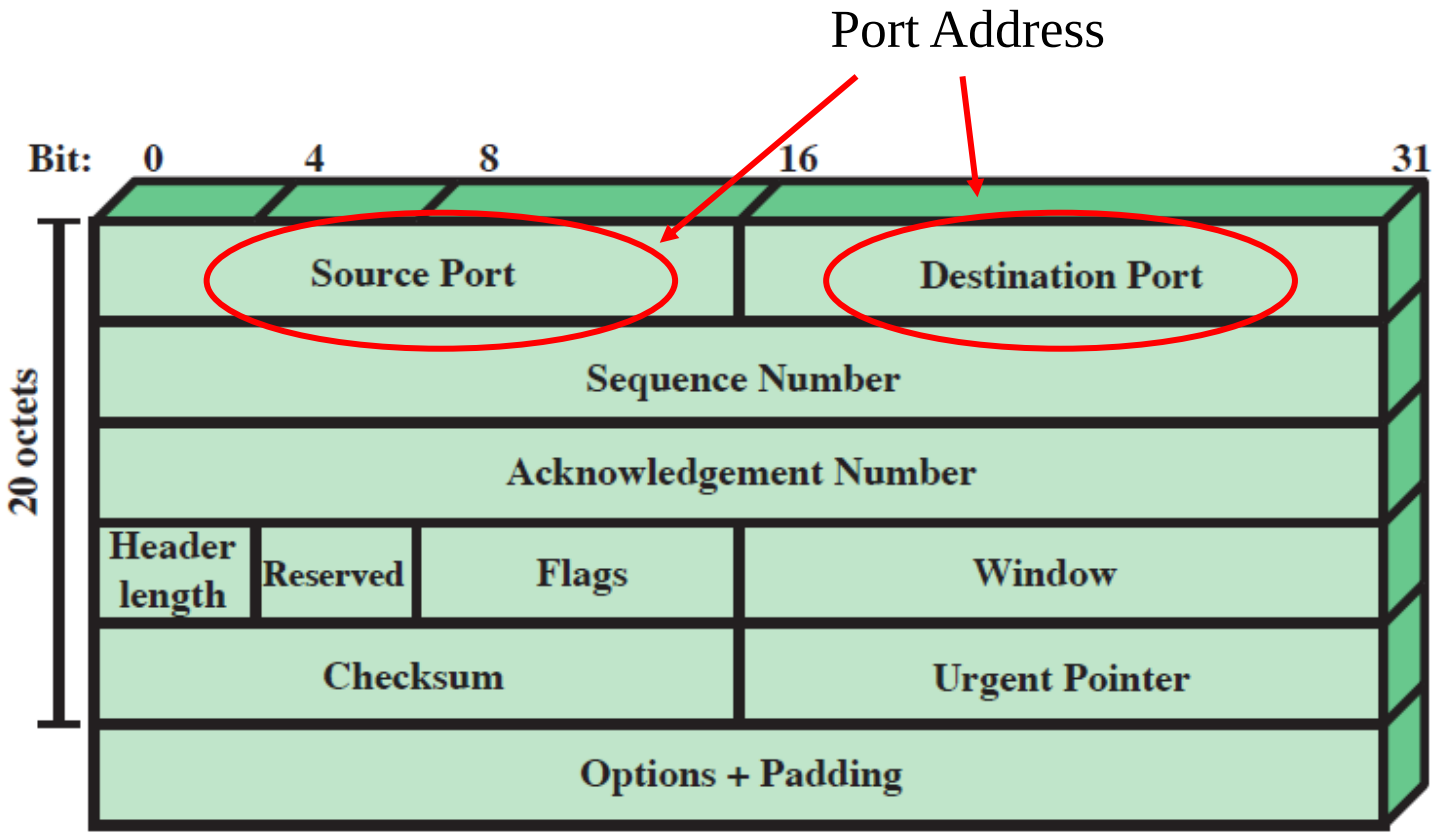
Logical/IP Address

IPv6 Header



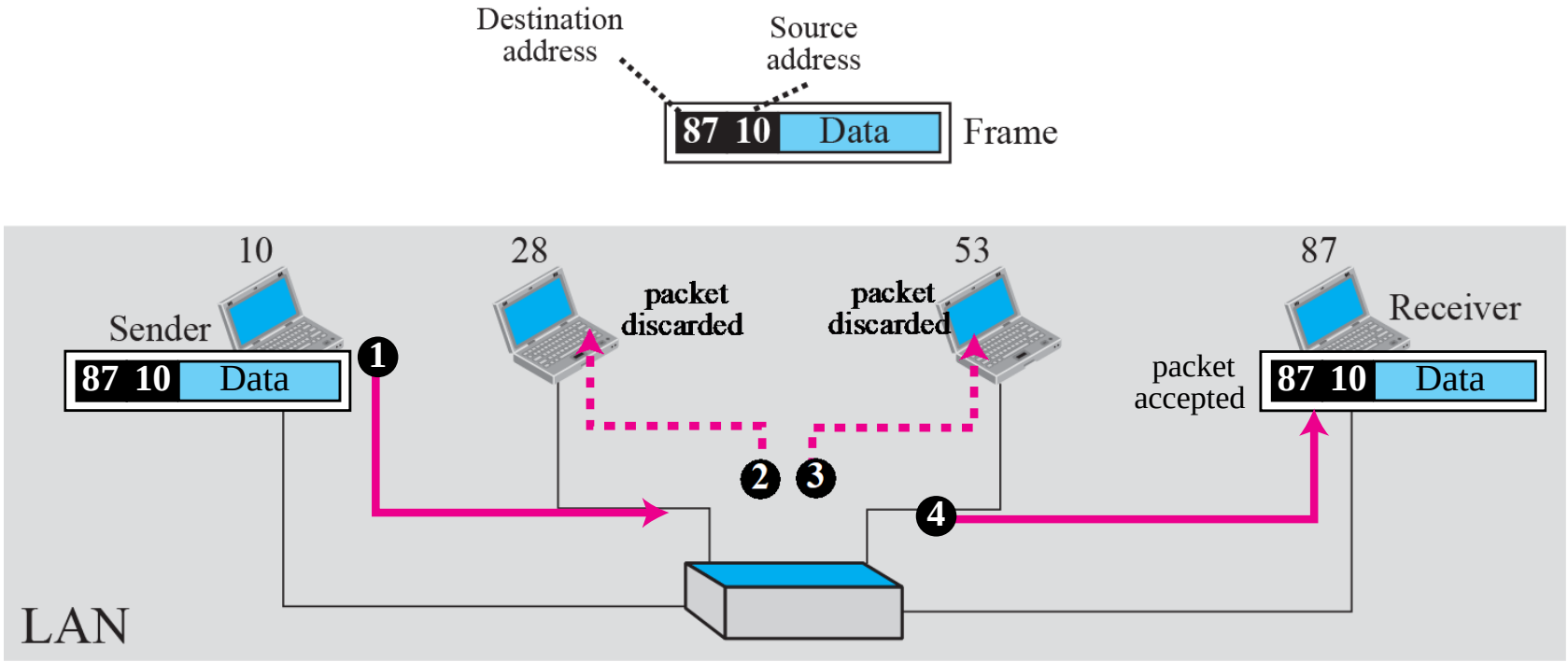
(b) IPv6 Header

TCP Header



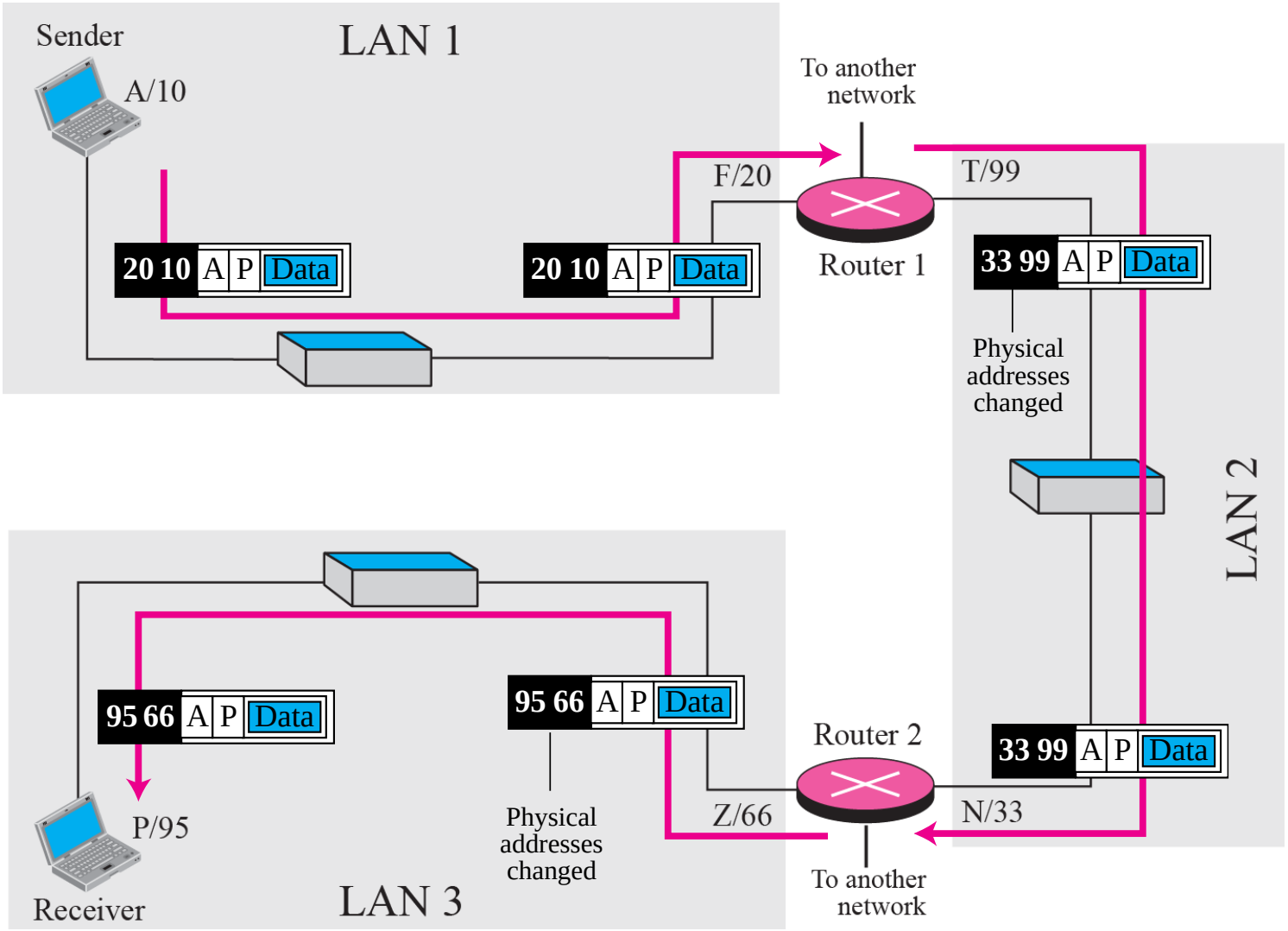
TCP ports: FTP(20 & 21), SSH(22), TELNET(23), SMTP(25), HTTP(80)

Example



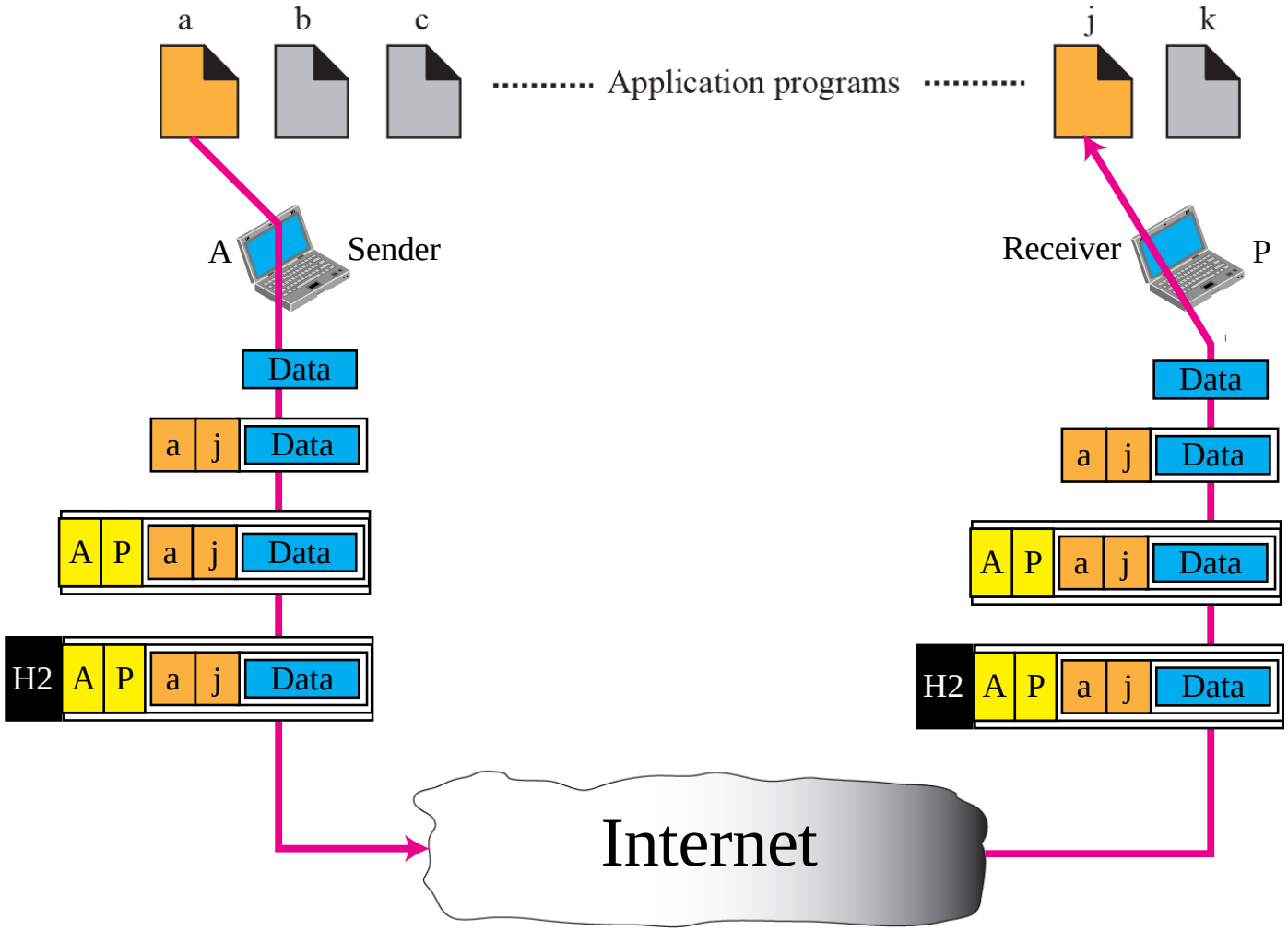
A node with physical address 10 sends a frame to a node with physical address 87.

Example



The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95.

Example

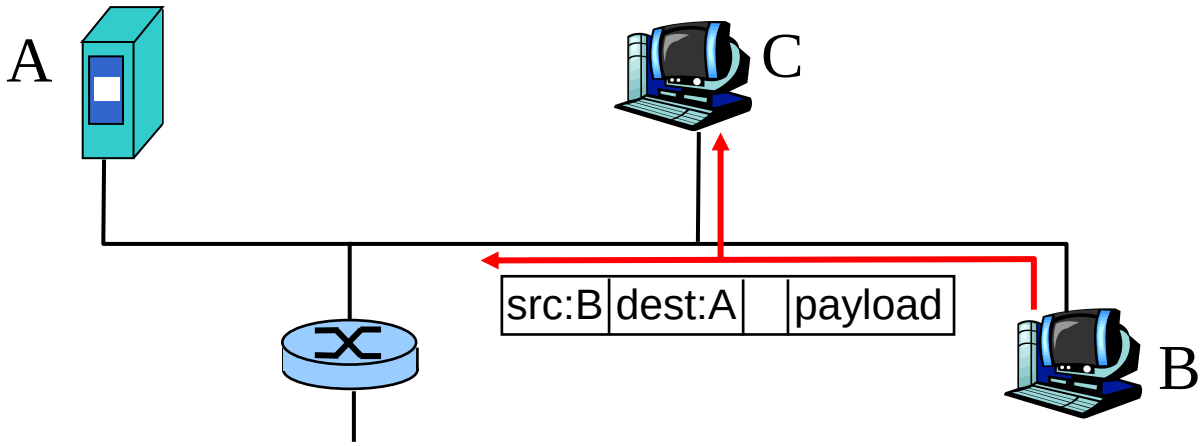


The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k.

Internet security threats

Packet sniffing:

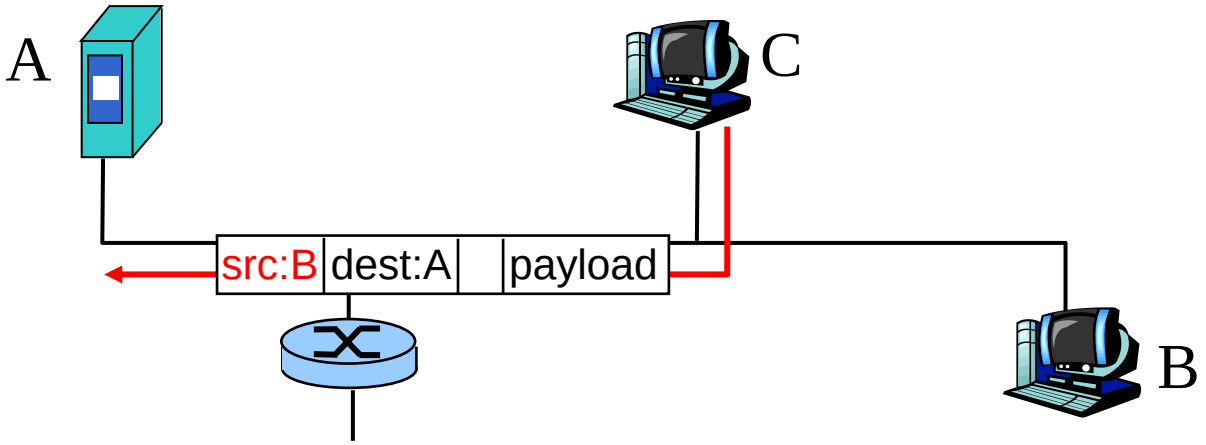
- the attacker reads all packets passing by
- can read all unencrypted data (e.g. passwords)
- e.g.: C sniffs B's packets



Internet security threats

IP Spoofing:

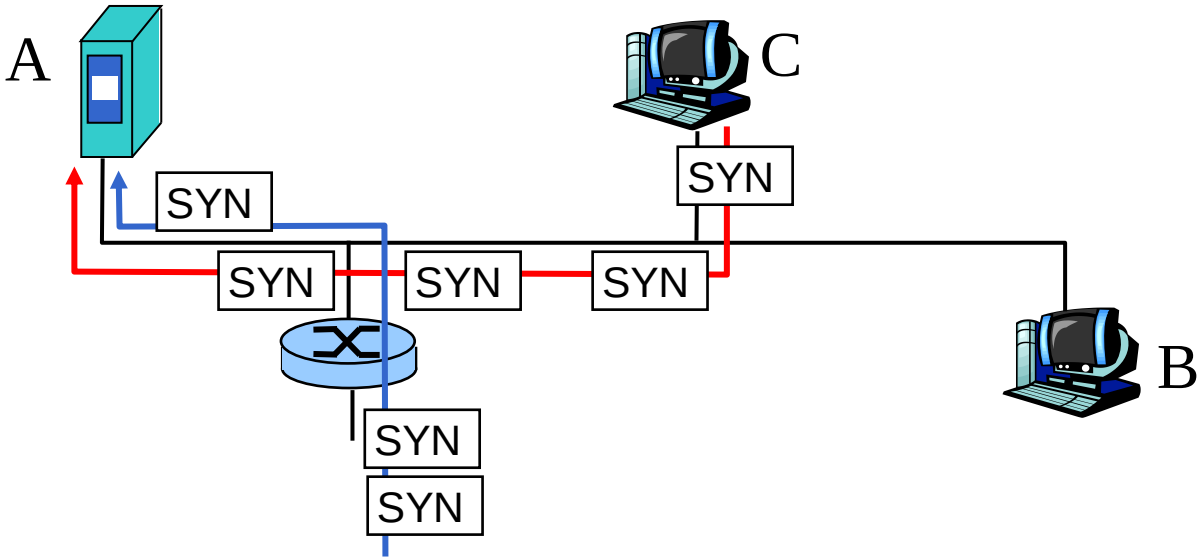
- can generate “raw” IP packets directly from application, putting any value into IP source address field
- receiver can’t tell if source is spoofed
- e.g.: C pretends to be B



Internet security threats

Denial of service (DoS):

- flood of maliciously generated packets “swamp” a receiver
- Distributed DOS (DDoS): multiple coordinated sources swamp a receiver
- e.g., C and remote hosts SYN-attack A



Movie of the Day

- Warriors of the Net

  http://www.youtube.com/watch?v=TBxZgOGjyZc

  A short and entertaining animated movie introducing basic concepts of TCP/IP networking