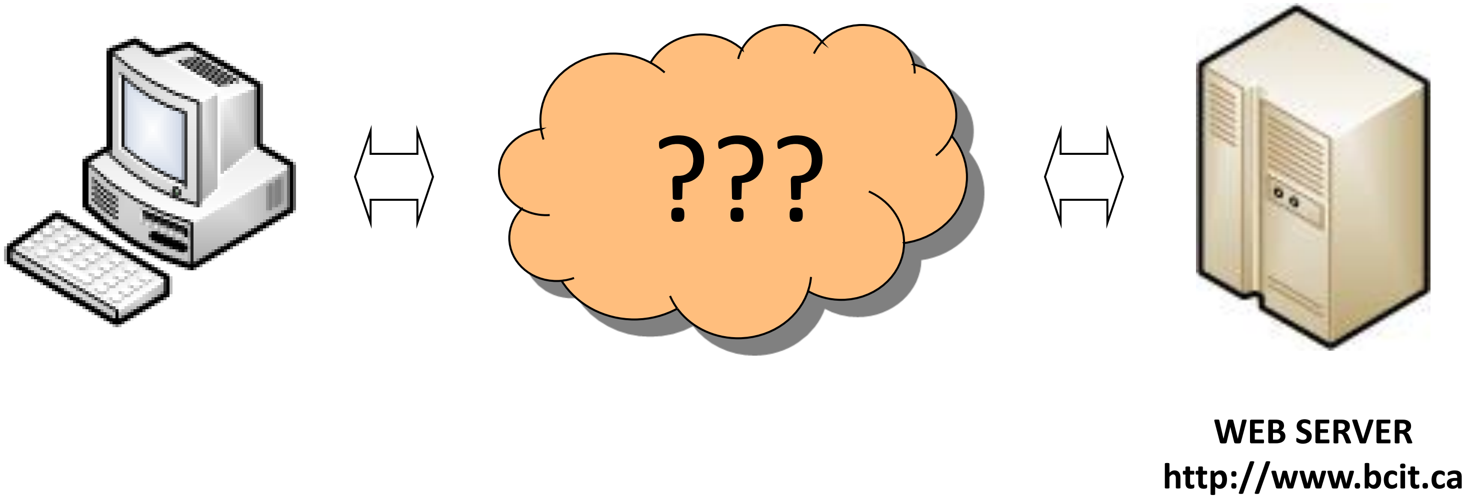
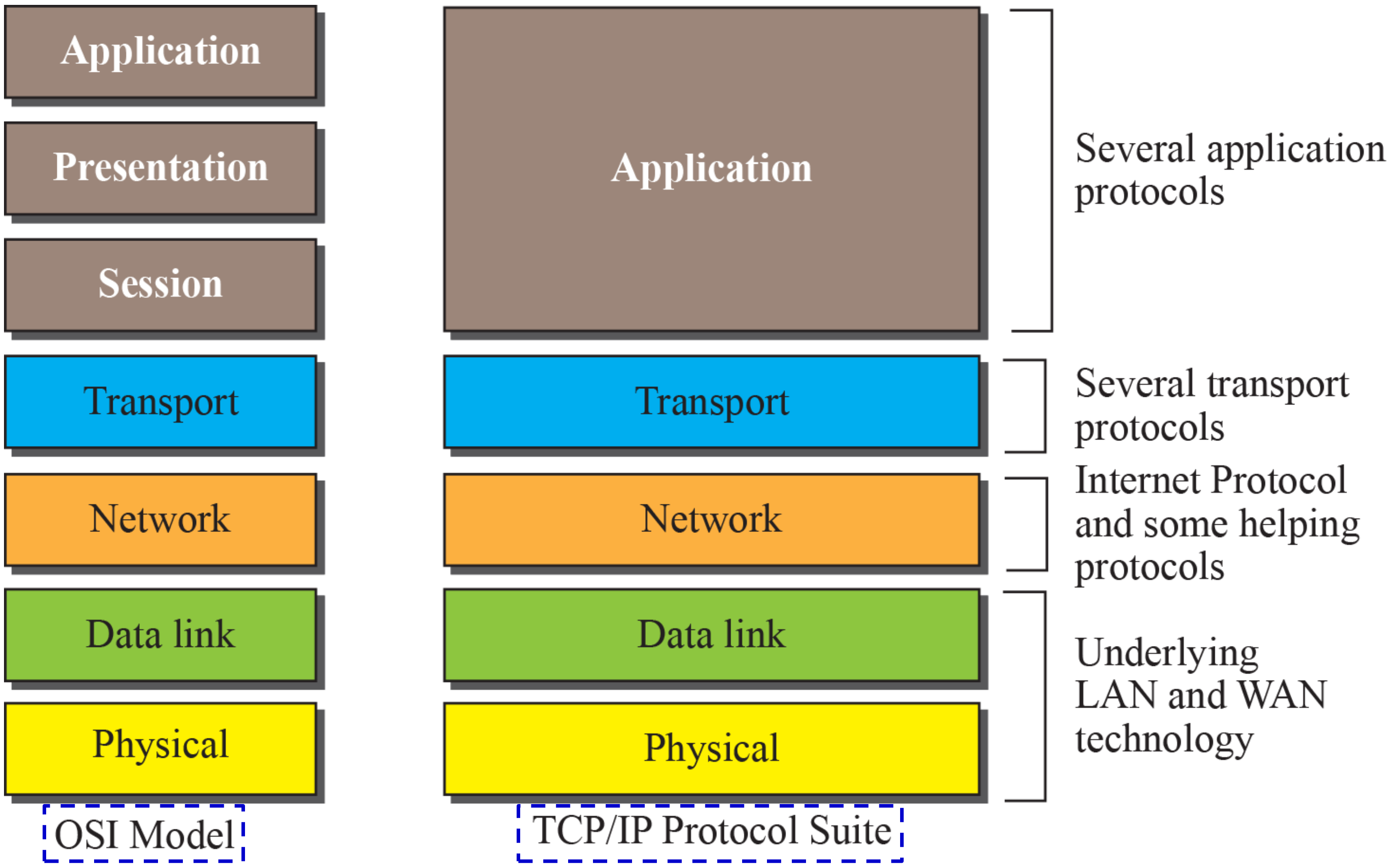
COMP 3725:
Data Communications for CST



The OSI Model and TCP/IP Protocol Suite



OSI: Open Systems Interconnection

TCP/IP: Transmission Control Protocol/Internet Protocol

Chapter 1: Introduction

Outline

1.1 Data Communications

1.2 Networks

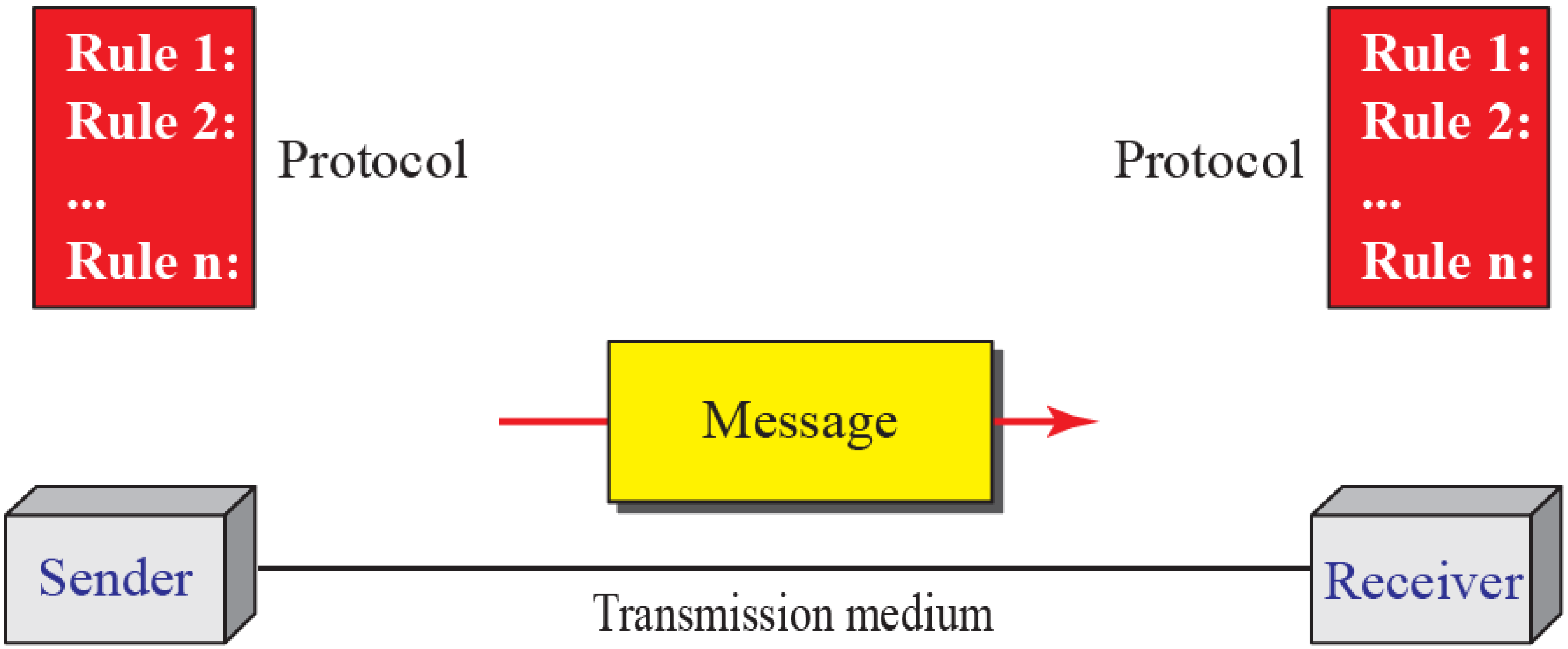
1-1 DATA COMMUNICATIONS

When we communicate, we are <u>sharing information</u>. This <u>sharing can be local or remote</u>. The term <u>telecommunication</u>, which includes telephony, telegraph, and television, <u>means communication at a distance</u>.

<u>Data communications is the exchange of data between two devices via some form of transmission media</u>.

1.1.1 Components

A data communications system has five components.



1.1.1 Components

Sender: **The sender is the device that sends the data message. It can be a computer, workstation, a telephone handset and so on.**

Receiver: **The receiver is the device that receives the message. It can be a computer, workstation, a telephone handset and so on.**

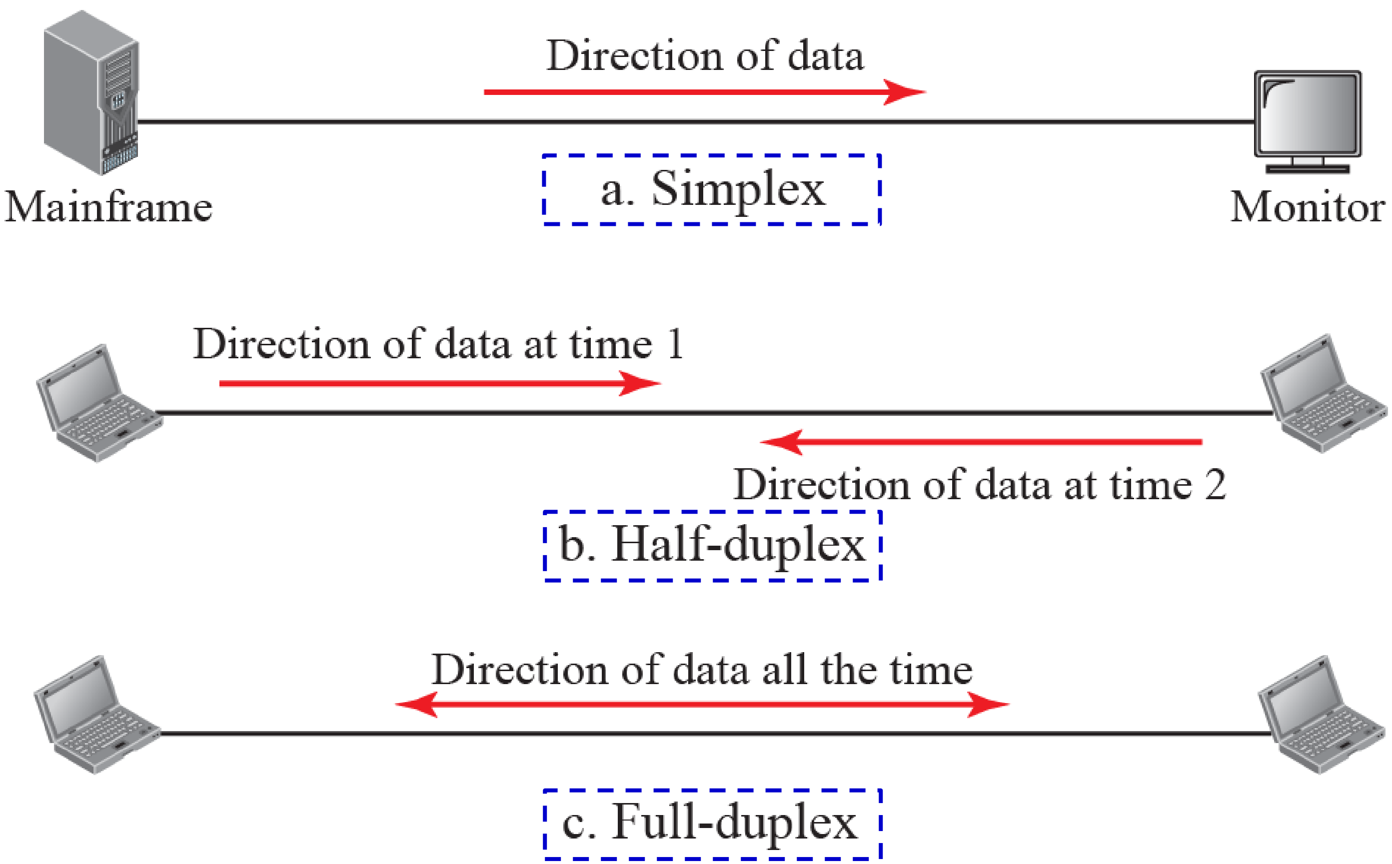
Message: **The message is the information (data) to be communicated. Forms of information include text, numbers, pictures, audio and video.**

Transmission medium: **The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable and radio waves.**

Protocol: **A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.**

1.1.3 Data Flow

Communication between two devices can be simplex, half-duplex or full-duplex as shown below:



- **Eg. Keyboard**
- **Entire Capacity in one direction**

- **Eg. Walkie-talkie**
- **Entire Capacity in one direction**

- **Eg. Telephone network**
- **Capacity is divided between the two directions**

1-2 NETWORKS

A network is the interconnection of a set of devices capable of communication.

In this definition, a device can be a host such as a large computer, desktop, laptop, workstation, cellular phone, or security system. A device in this definition can also be a connecting device such as a router, a switch, a modem that changes the form of data, and so on.

1.2.1 Network Criteria

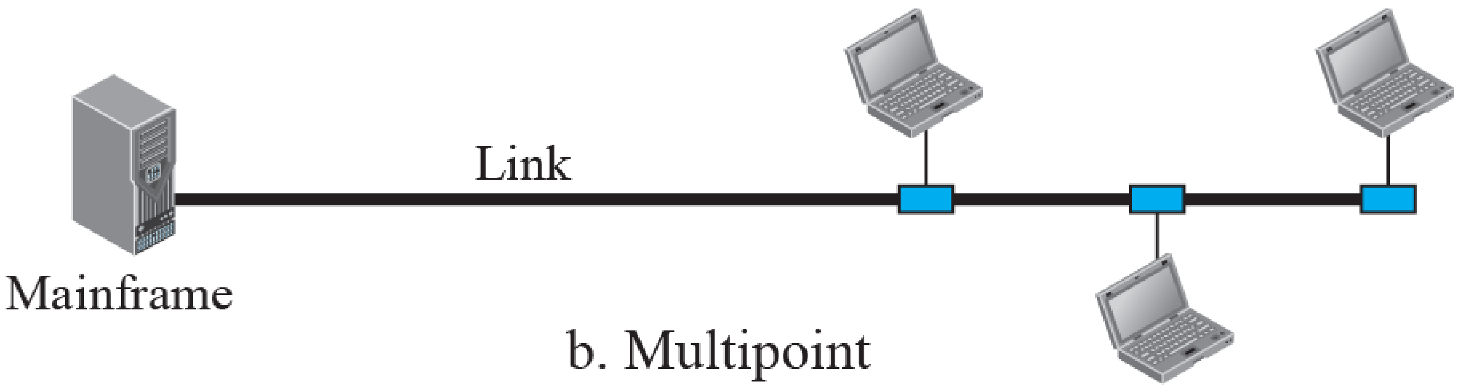
A network must be able to meet a certain number of criteria. The most important of these are performance, reliability and security.

- ***Performance*** **is often evaluated by i) throughput and ii) delay.**
- ***Reliability*** **is often measured by i) the frequency of failure, ii) the time it takes to recover from a failure and iii) the network's robustness in a catastrophe.**
- ***Security*** **include i) protecting data from unauthorized access and from damage and ii) implementing policies and procedures for recovery from breaches and data losses.**

Figure 1.3: Types of connection

a. Point-to-point

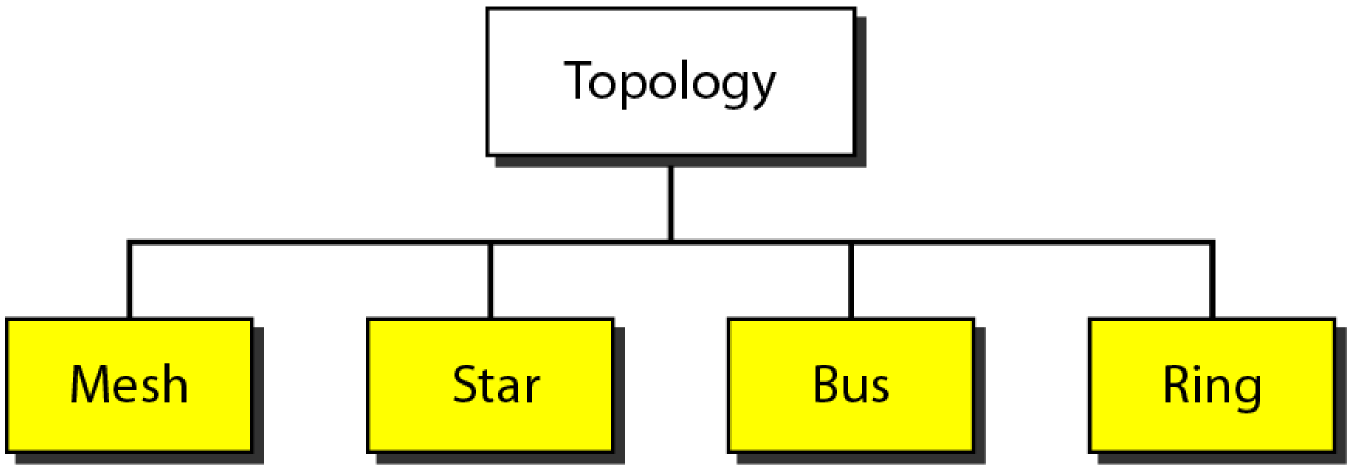
- Provides a dedicated link between two devices.
- Capacity of the link is used for transmission between these two devices.



b. Multipoint

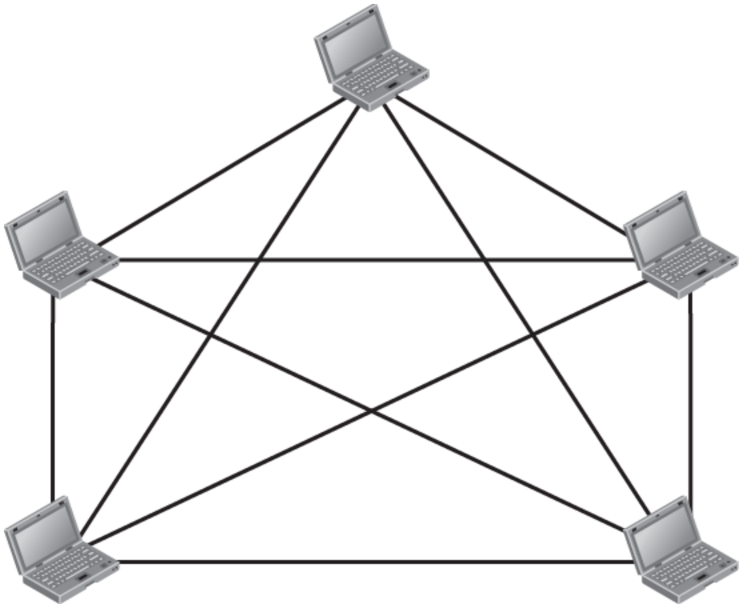
- More than two devices share a single link.
- Capacity of the link is shared among the devices.

1.2.2 Physical Topology



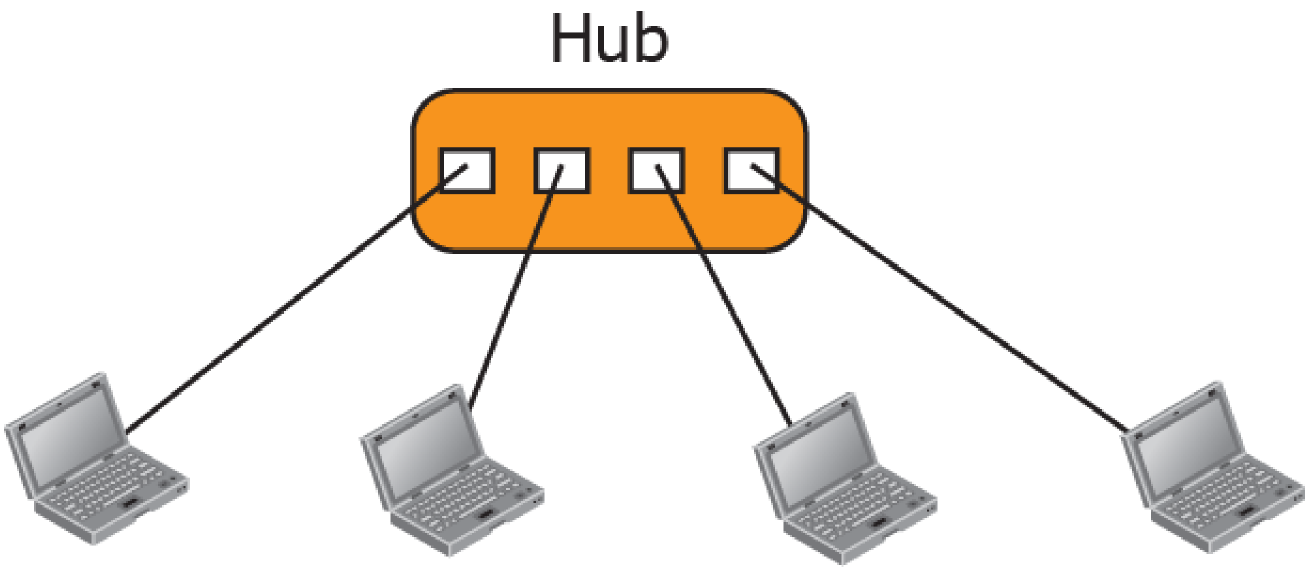
Which physical topology should one use?

Figure 1.4: A fully-connected mesh topology



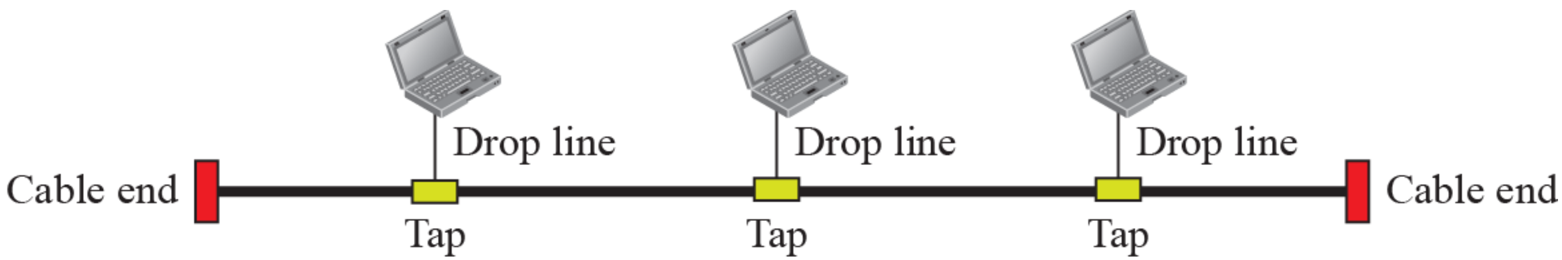
- Every device has a dedicated <u>point-to-point</u> link to every other device.
- A mesh topology with *n* nodes require *n(n-1)/2* full-duplex links.
- Advantages:
  - Dedicated links – Entire capacity of link is used for transmission between two devices.
  - Robust – Entire system not incapacitated due to one unusable link.
  - Privacy and security – Only intended recipient sees message on dedicated line.
  - Easy fault identification and isolation – Traffic can be routed to avoid problem links.
- Disadvantages:
  - Amount of cabling and number of I/O ports required ➔ Expensive.

Figure 1.5: A star topology



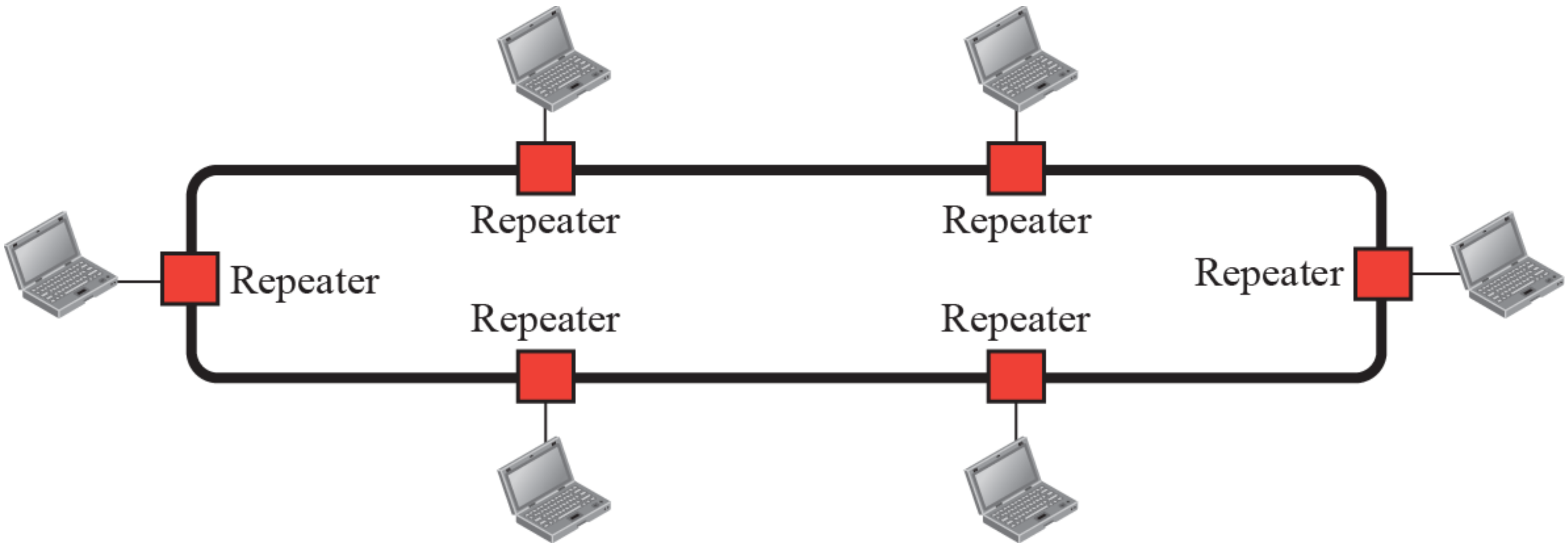
- Every device has a dedicated <u>point-to-point</u> link to a central controller (hub).
- Does not allow traffic between devices; the controller acts as an exchange.
- Advantages:
  - Cost – Less cabling and I/O ports (i.e., less expensive) than mesh topology.
  - Robust – Entire system not incapacitated due to one unusable link.
  - Easy fault identification and isolation – Central controller can monitor/avoid problem links.
- Disadvantages:
  - Single point of failure – Dependence of the whole network on a central controller.

Figure 1.6: A bus topology



- <u>Multipoint</u> **connection: One long cable acts as a backbone to link all the devices in a network. One of the first topologies used in the design of early local-area networks (less popular now).**
- **Advantages:**
  - **Ease of installation.**
  - **Less cabling than either mesh or star topologies.**
- **Disadvantages:**
  - **Single point of failure – backbone cable.**
  - **Difficult fault isolation.**

Figure 1.7: A ring topology



- Each device has a dedicated point-to-point connection with only two devices on either side of it.
- Advantages:
  - Easy to install and reconfigure – Each device is linked to only its immediate neighbors.
  - Simplified fault identification and isolation – A signal circulates at all times; if a device does not receive a signal within a specified period, an alarm is issued.
- Disadvantages:
  - Single point of failure – Break in ring can disable the entire network.

Chapter 2: Network Models

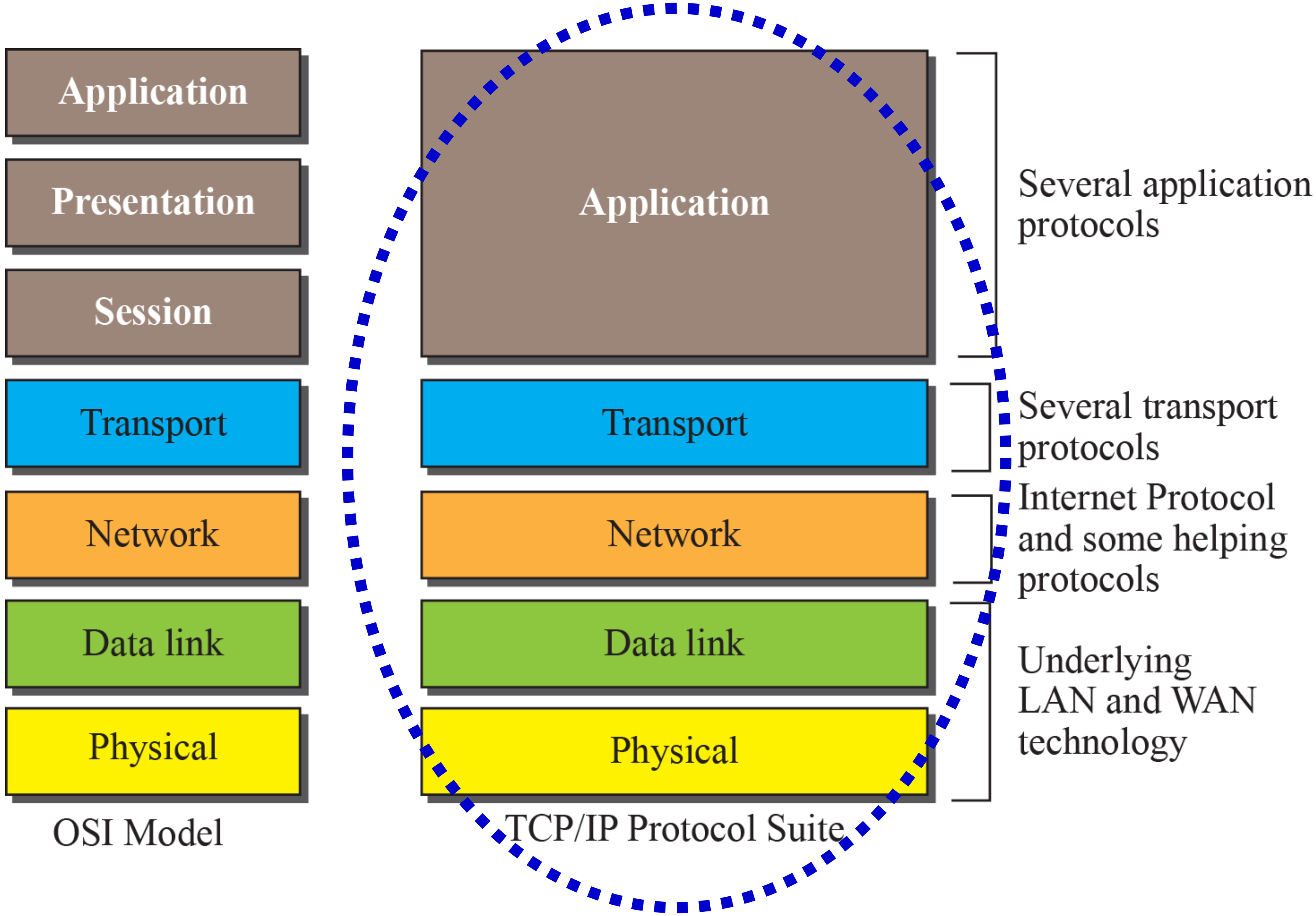
Outline

2.1 Protocol Layering

2.2 More on TCP/IP Protocol Suite

The OSI model and TCP/IP Protocol Suite

OSI: Open Systems Interconnection
TCP/IP: Transmission Control Protocol/Internet Protocol



TCP/IP Protocol Suite Layers
(Brief Functional Summary)

Application: enables the users to access the network: <u>HTTP, FTP, SMTP, Telnet, etc</u>.

Transport: responsible for the process-to-process delivery of the entire message: <u>process-to-process communication - User Datagram Protocol / Transmission Control Protocol</u>. <u>UDP: Best effort delivery of user datagrams</u>. <u>TCP: flow, error (retransmission/reordering) and congestion control of segments</u>.

Network: responsible for the host-to-host (source-to-destination) delivery of a **packet / datagram** across multiple network links: <u>host-to-host communication, routing</u>.

Data link: responsible for delivering **frames** from one station to the next without errors: <u>Data Link Control (DLC) sublayer: framing, error detection and correction of frames/bits; Medium Access Control (MAC) sublayer: physical hardware address, medium access control</u>.

Physical: coordinates the functions required to transmit a **bit** over a transmission medium: <u>bit representation, type of encoding</u>. Not the physical transmission mediums (twisted pair, coaxial, radio wave).

2-1 PROTOCOL LAYERING

***A protocol defines the rules** that **both the sender and receiver** and all intermediate devices **need to follow to be able to communicate effectively**.*

When communication is simple, we may need only one simple protocol; when the communication is complex, we need a protocol at each layer, or protocol layering (referred to as modularity).

2.2.1 Layered Architecture

To show how the layers in the TCP/IP protocol suite are involved in <u>communication between two hosts</u>, we use the <u>TCP/IP protocol suite</u> in a small internet made up of <u>three LANs</u> (links), each with a <u>link-layer switch</u>. We also assume that the <u>links are connected by one router</u>.

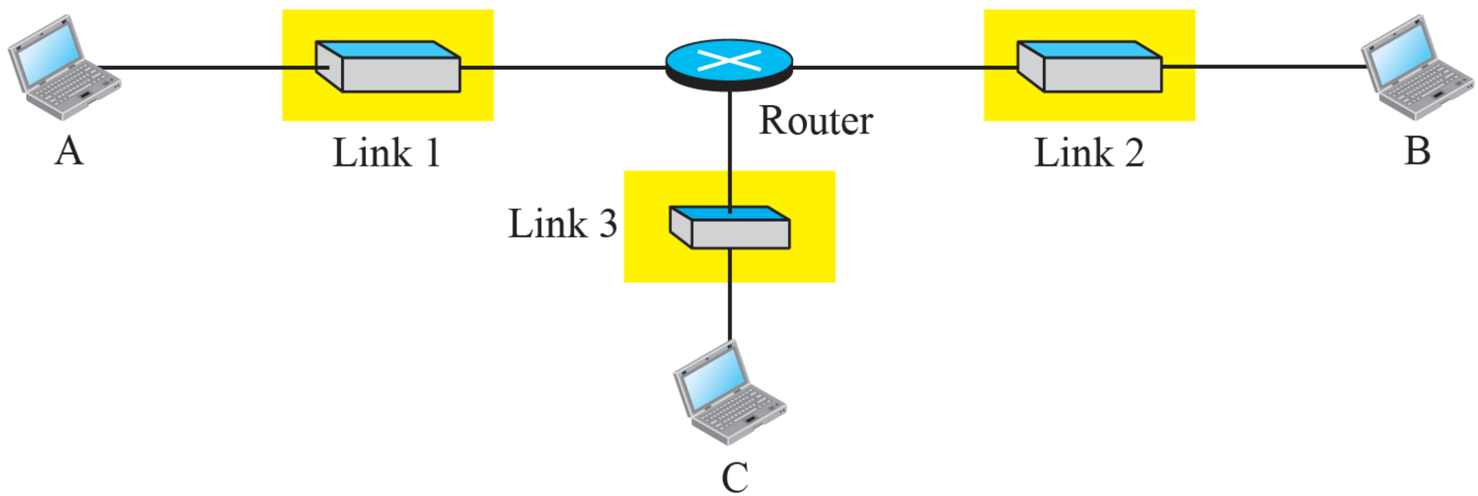
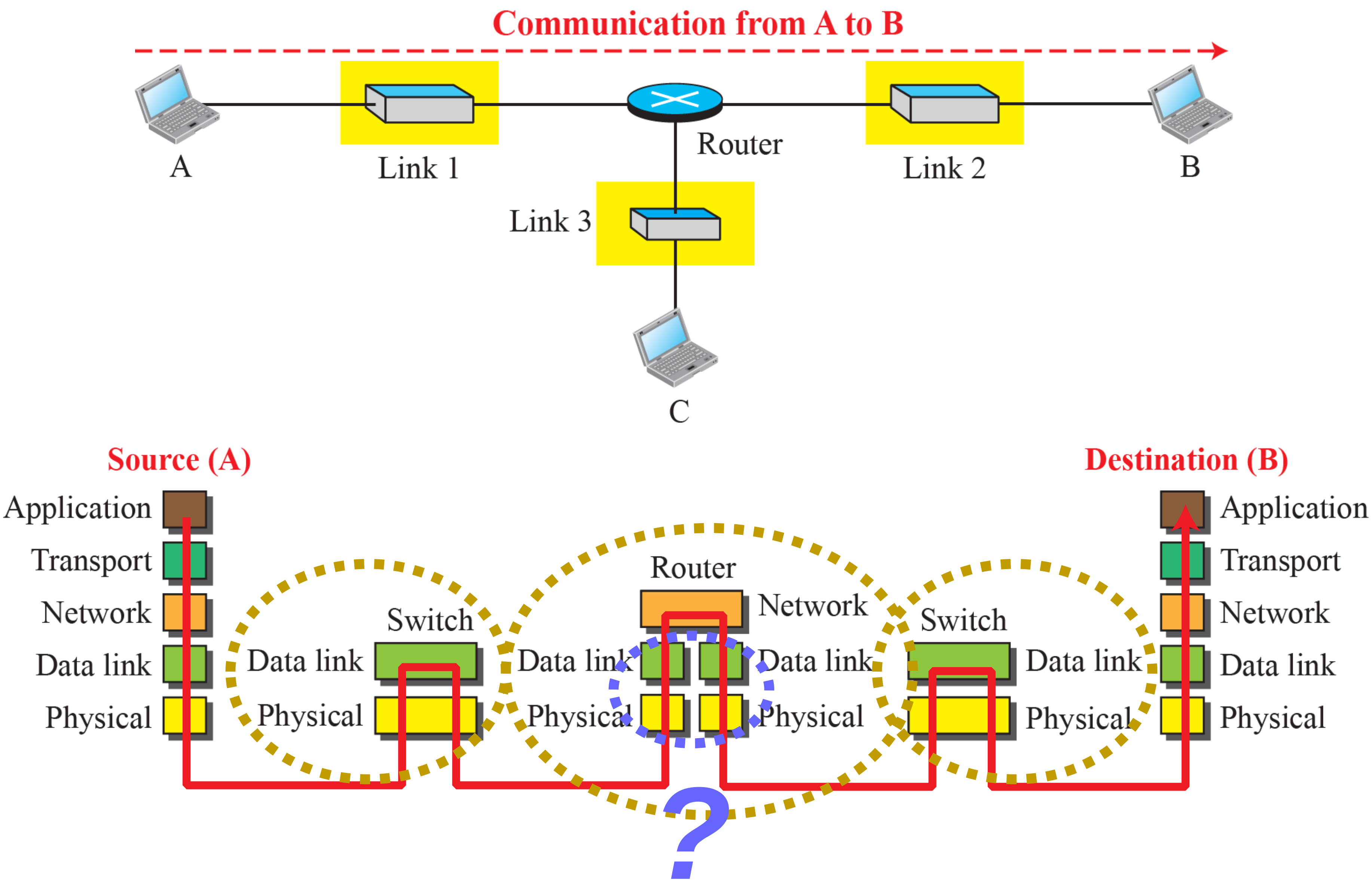


Figure 2.5: Communication through an internet

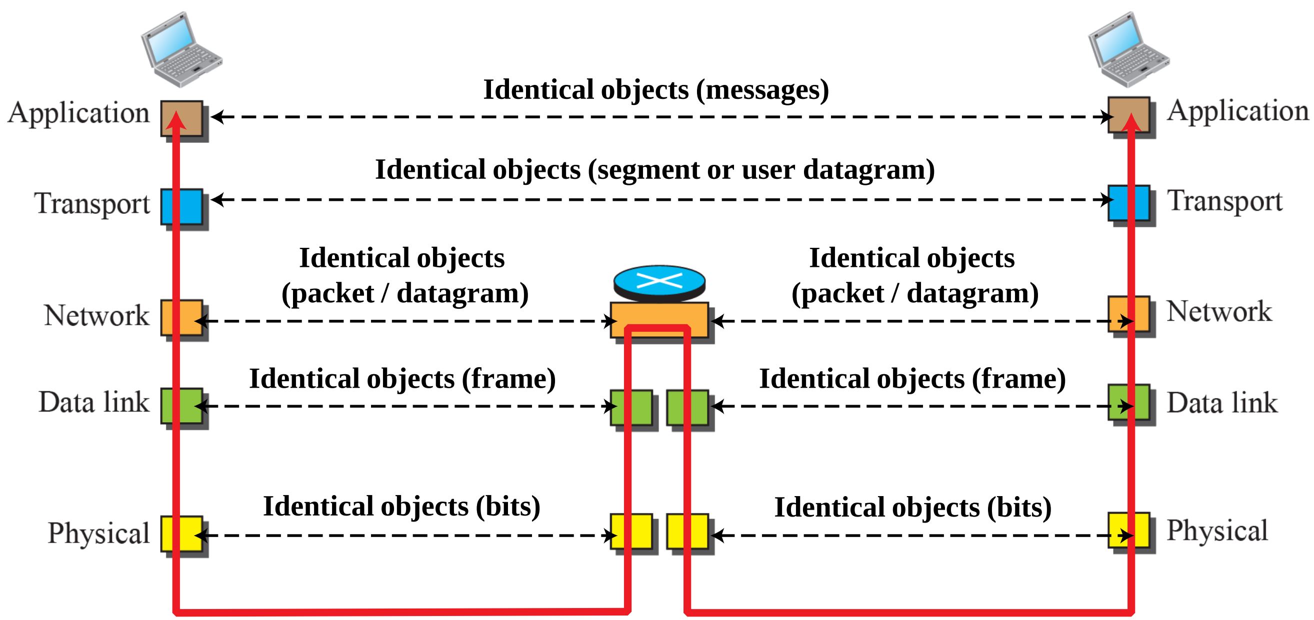


2.1.2 Principles of Protocol Layering

Two principles ***of protocol layering:***

The first principle dictates that if we want bidirectional communication, we need to make each layer such that it is able to perform two opposite tasks, one in each direction (i.e., send/receive, encrypt/decrypt, etc.).

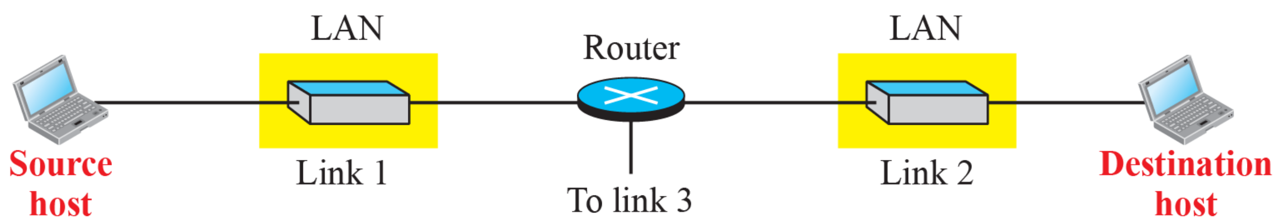
The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

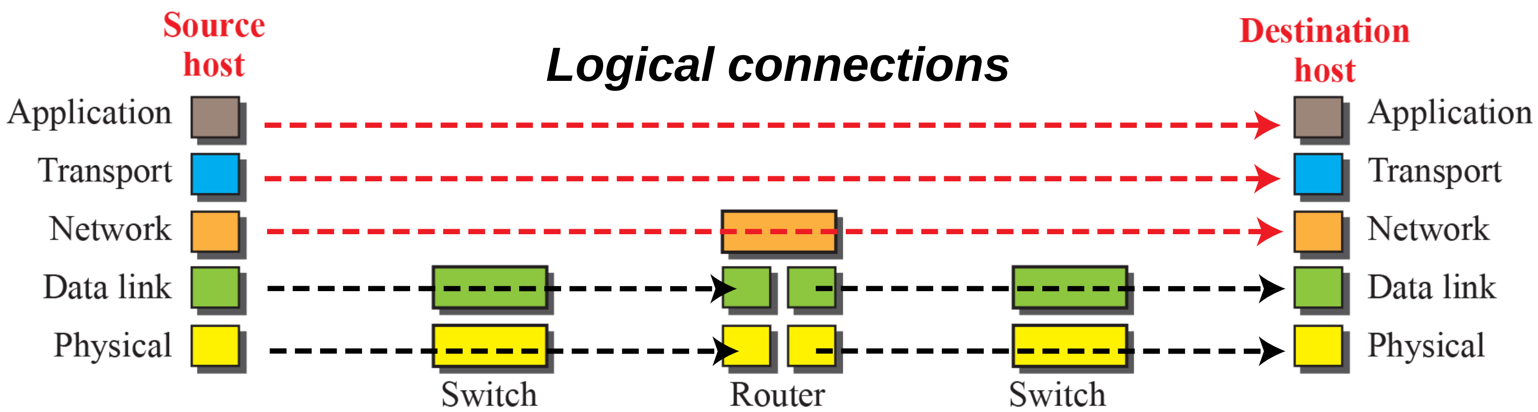


Notes: We have not shown switches because they don't change objects.

2.1.3 Logical Connections

Let's differentiate the <u>physical connection</u> vs. <u>logical connection (layer-to-layer communication) between each layer</u>:

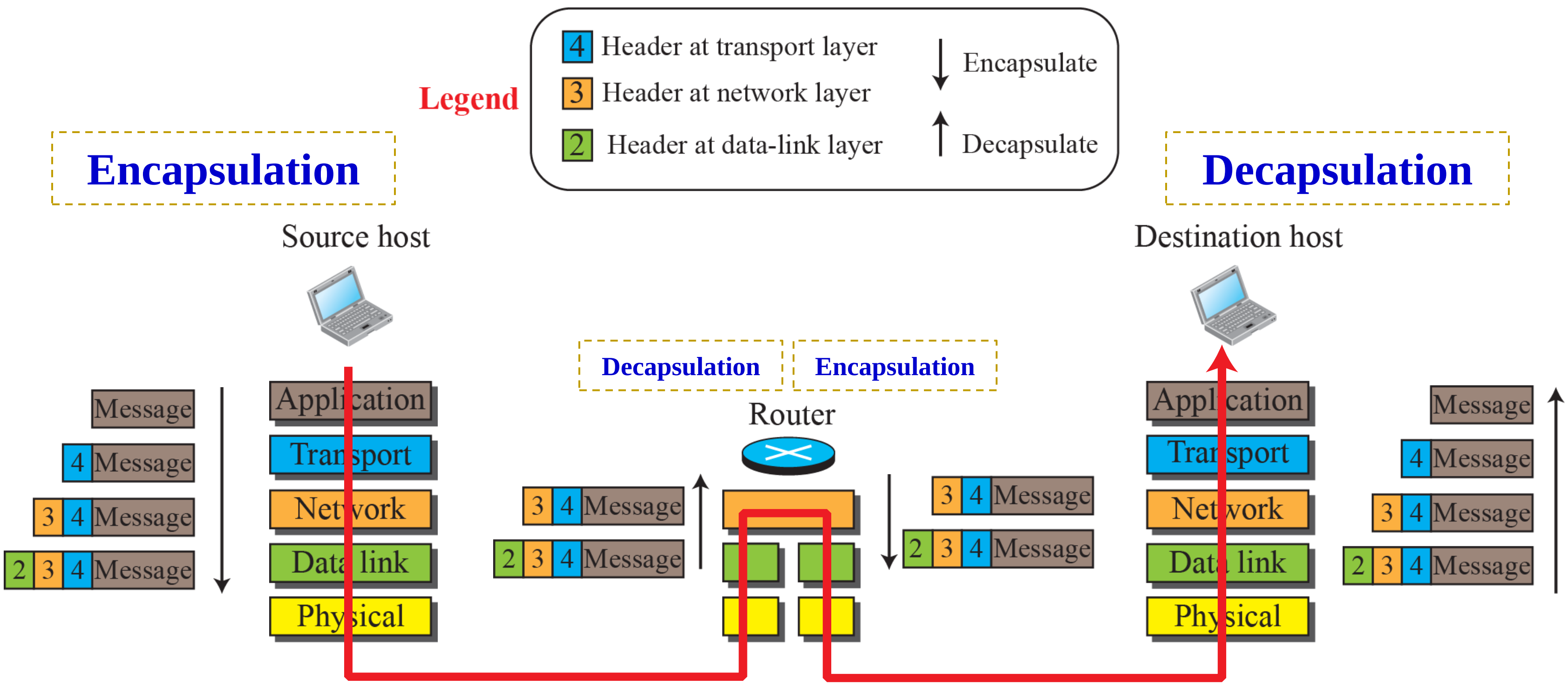




- **Duty of the <u>application, transport and network</u> layers is <u>end-to-end</u>.**
- **Duty of the <u>data link and physical</u> layers is <u>hop-to-hop</u>.**

2.2.4 Encapsulation and Decapsulation

An important concept in protocol layering is <u>encapsulation/decapsulation</u>.



2.2.5 Addressing

Another concept related to protocol layering is <u>addressing</u>.

Packet names	Layers	Addresses	
Message	Application layer	Names	▪ **Eg. www.bcit.ca**
Segment / User datagram	Transport layer	Port numbers	▪ **Eg. Port 80 (http)**
Packet / Datagram	Network layer	Logical addresses	**IP address**
Frame	Data-link layer	Link-layer addresses	**MAC ID**
Bits	Physical layer		