# CSC 4350 – Computer Networks

Fall 2024 Semester

Lecture 4 – Delay, Loss, Throughput, Protocols, Attacks

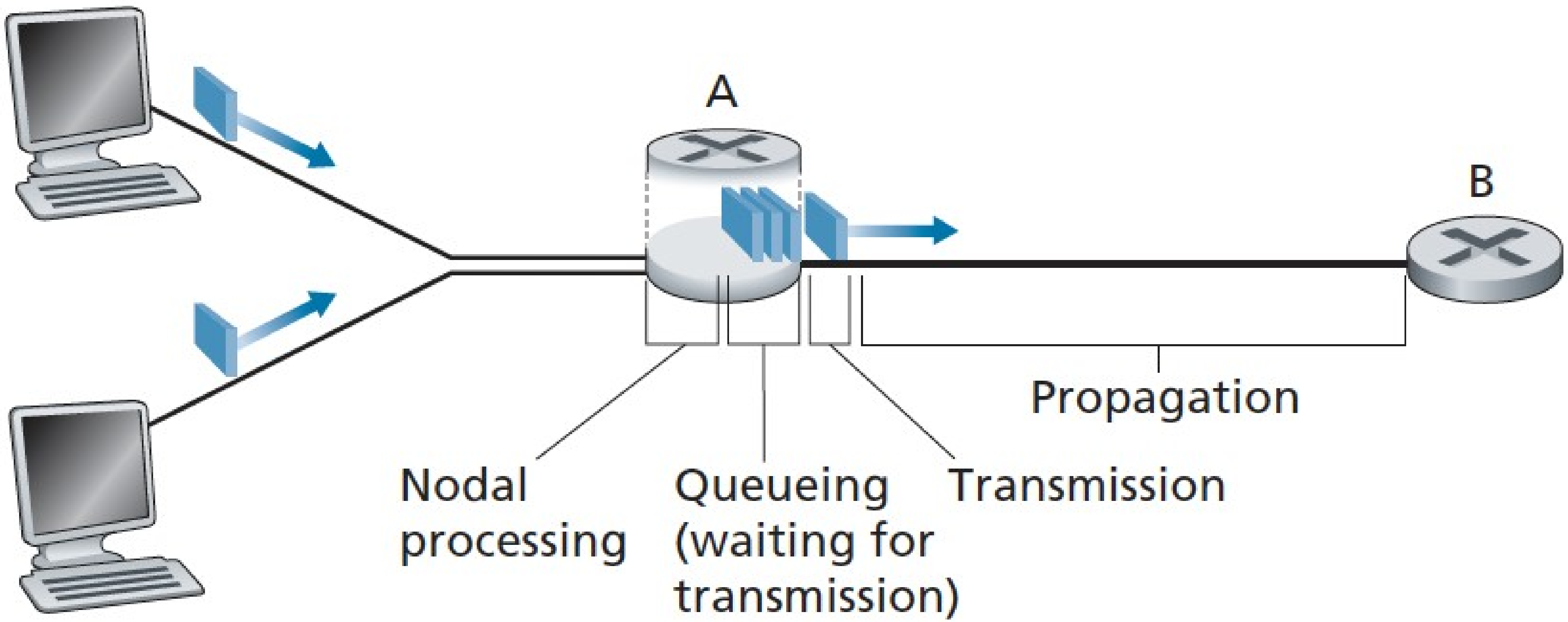
# Note

- Material used in this lecture is heavily borrowed from Kurose & Ross' "Computer Networking: A Top Down Approach, 8th Edition"
- Also:  assuming no prior knowledge of networks

# Packet-Switched Networks – Delay, Loss, and Throughput

- Delays – Types
  - Processing Delay – time required to examine the packet’s header and determine where to direct the packet
    - Can also include other factors
      - Time needed to check for bit-level errors in the packet in transmission from upstream node router A
      - After processing, router directs the packet to the queue that precedes the link to router B
  - Queuing Delay
    - Packet waits to be transmitted onto the link
    - Length of delay will depend on number of earlier-arriving packets that are queued and waiting for transmission

# Nodal Delay at Router A – Figure 1.16



# Delay, Loss, and Throughput

- Delays
  - Transmission Delay
    - Assume:  packets transmitted in first-come-first-served manner
    - Denote length of packets by L bits and denote the transmission rate of the link from router A to router B by R bits/sec
    - Transmission delay is L/R
      - Amount of time required to transmit all of the packet's links into the link
  - Propagation Delay
    - Time required to propagate from the beginning of the link to router B
    - Bit moves at the speed of the link
    - Speeds are dependent on the medium of the link
    - Distance between two routers divided by the propagation speed – d/s
    - WANs – equates to milliseconds

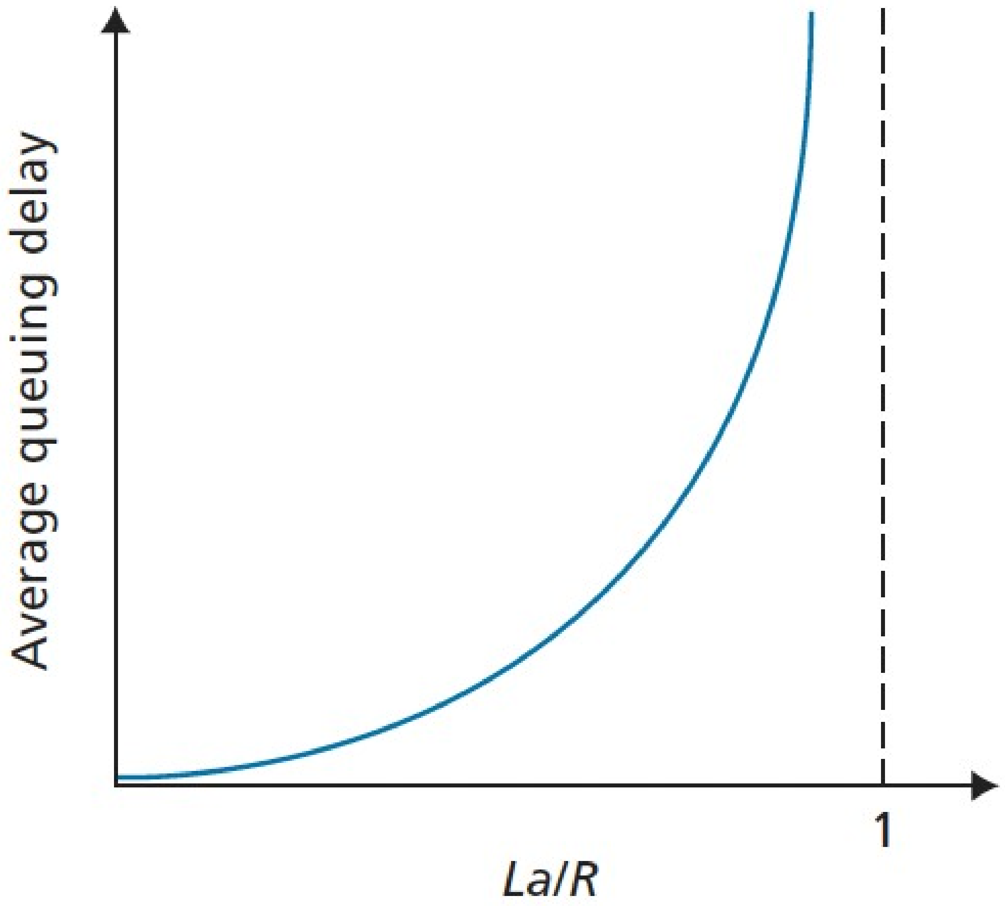
# Transmission v. Propagation Delay

- Transmission delay – amount of time required for the router to push out the packet
  - Function of the packet’s length and the transmission rate of the link
  - Distance between two routers isn’t factored in
- Propagation delay – time it takes a bit to propagate one bit from one router to the next
  - Function of distance between the two routers; has nothing to do with packet’s length or transmission rate
- Caravan Analogy

# Queuing Delay and Packet Loss

- Queuing delay can vary from packet to packet
  - 10 packets arrive to an empty queue
    - 1st – no delay
    - 10th – significant delay
- Need statistical measures for queuing delay
  - Average queuing delay
  - Variance of queuing delay
  - Probability that the queuing delay exceeds some specified value
- When is queuing delay large vs. insignificant?
  - Depends on the rate at which traffic arrives to the queue
  - R – transmission rate
  - a – average rate at which packets arrive at the queue
  - All packets consist of L bits
  - Average rate: La bits/sec
  - Queue is large, holding (essentially) an infinite number of bits
  - Traffic intensity – La/R
    - >1 – average rate at which bits arrive at queue exceeds transmission rate
  - Need to remember, therefore, that the system's traffic intensity is <=1
- Actual arrival time is random

# Dependence of Average Queuing Delay on Traffic Intensity – Figure 1.18



# Figure 1.18

- As traffic intensity approaches 1, average queuing delay increases rapidly
- Small percentage increase in the intensity will result in a much larger percentage-wise increase in delay

# Packet Loss

- A queue preceding a link has finite capacity
  - Capacity does depend on the router design and cost
- Packet delays do not approach infinity as the traffic intensity approaches 1
- Packet can arrive to find a full queue; no place to store in the router – it’s dropped
- Fraction of lost packets increases as traffic intensity increases

# End-To-End Delay

- Assumptions
  - N-1 routers between the source host and destination host
  - Network is uncongested
  - Processing delay at each router at the source is dproc
  - Transmission rate out of each router and out of the source host: R bits/sec
  - Propagation on each link is dprop
  - Nodal delays accumulate to give an end-to-end delay of:

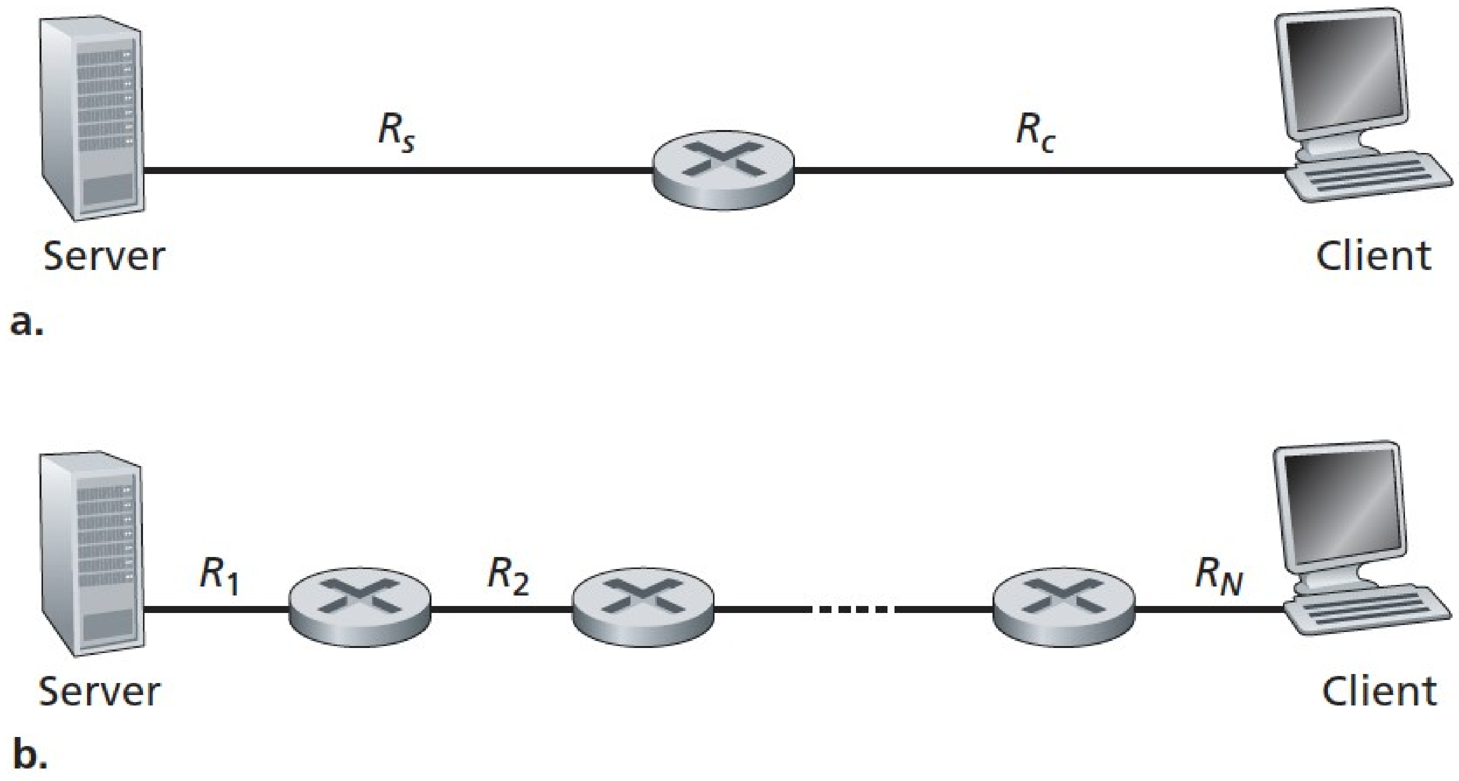
$$d_{\text{end-end}} = N\left(d_{\text{proc}} + d_{\text{trans}} + d_{\text{prop}}\right)$$

- Discussion of traceroute

# Throughput in Computer Networks

- Instantaneous throughput at any instant of time is the rate in which Host B is receiving the file/information
- If the file consists of F bits and the transfer takes T seconds for Host B to receive all bits, then the average throughput is F/T bits/sec

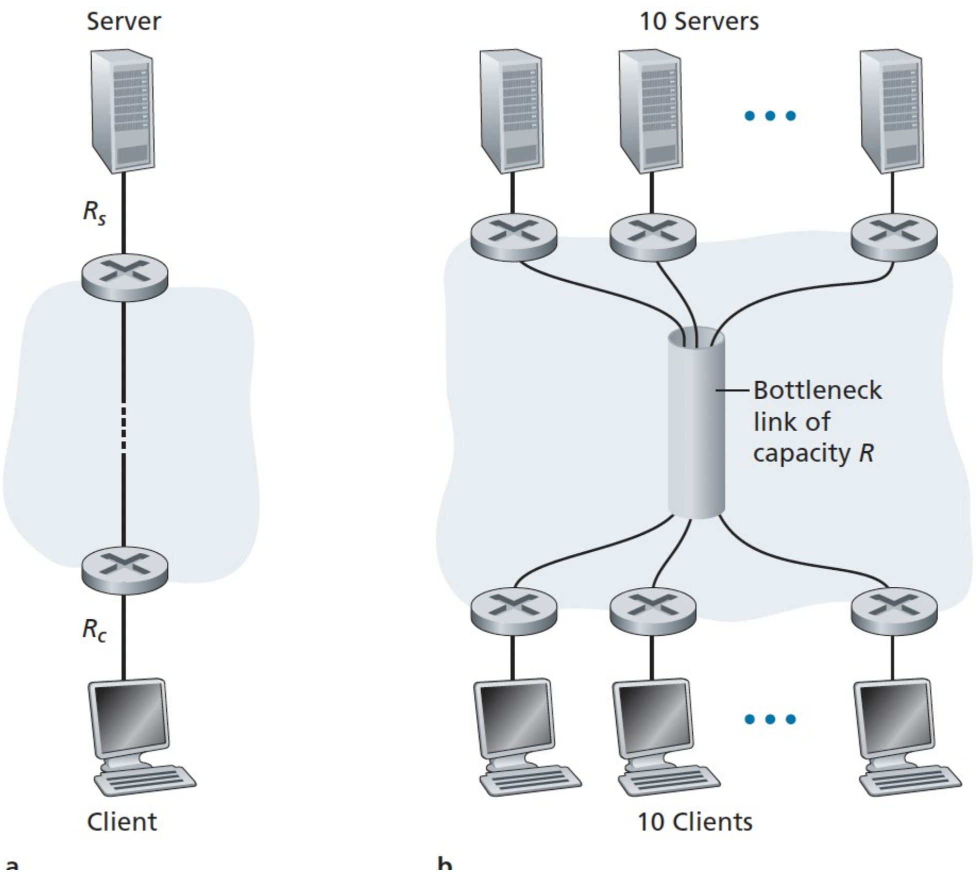
# Throughput for a File Transfer From Server To Client – Figure 1.19



# Bottleneck Link

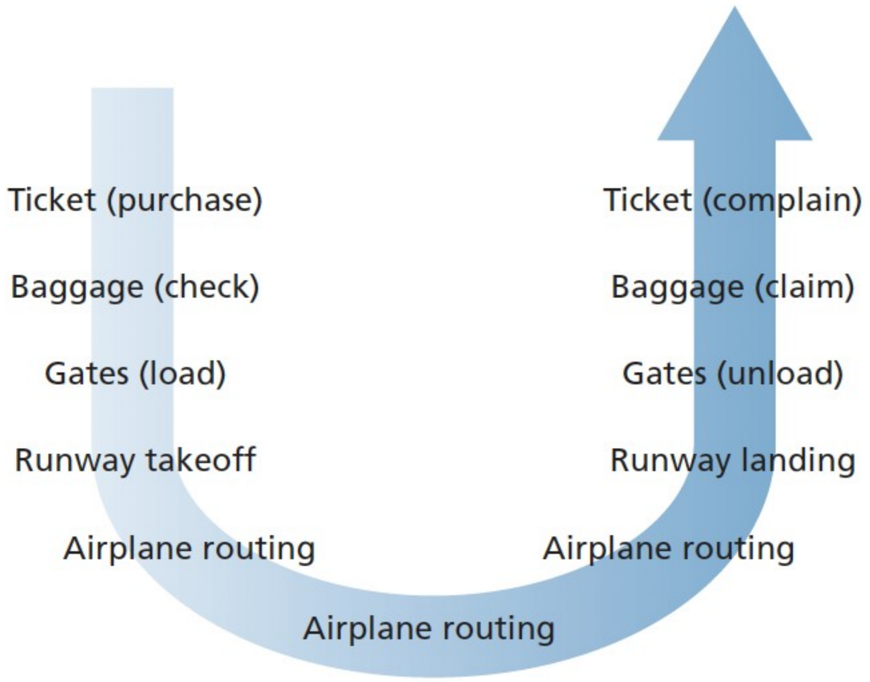
- Transmission rate: min{Rc, Rs} – throughput
  - For 1.19 a, this would be the slower link between Rc and Rs
  - For 1.19 b, this would be the slowest of all links

# End-To-End Throughput – Figure 1.20



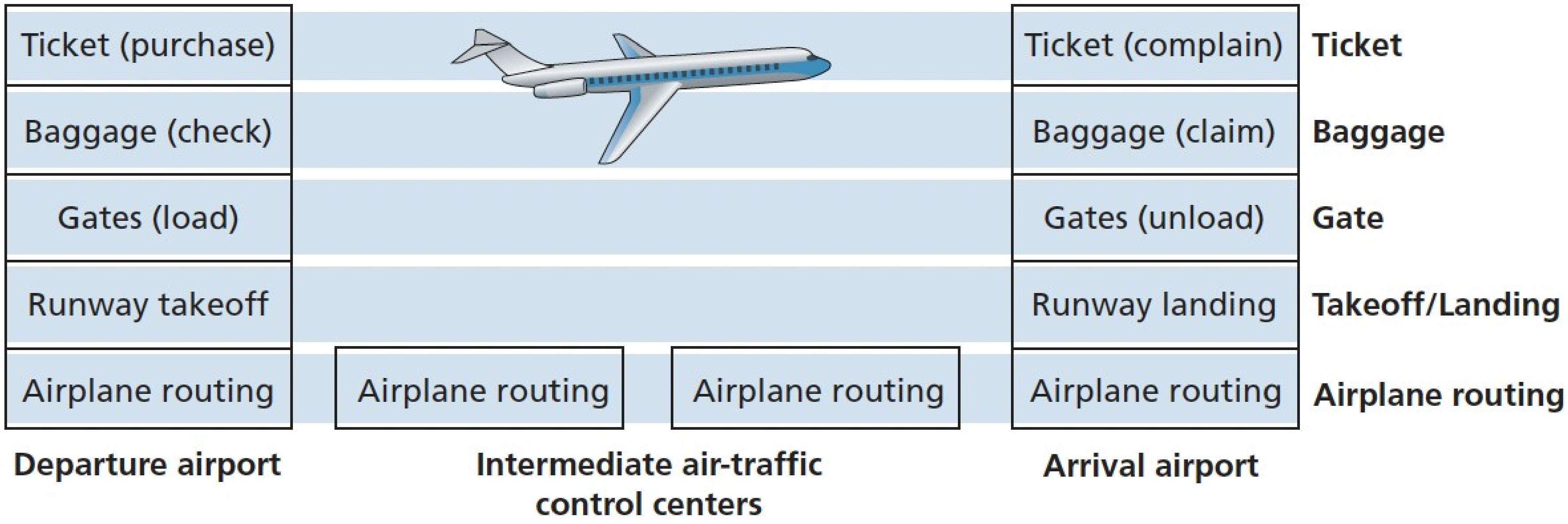
# Protocol Layers and Their Service Models

- Layered Architecture – Fig. 1.21 – Airplane Trip



# Protocol Layers and Their Service Models

- Horizontal Layering of Airline Functionality – Figure 1.22



# Protocol Layering

- To provide structure to the design of network protocols, network designers organize protocols and hardware/software to implement protocols in layers
- Each protocol belongs to one of the layers
- Interested in the services that a layer offers to the layer above, a.k.a. service model of a layer
- Each layer provides its service by
  - Performing certain actions within that layer
  - Using the services of the layer directly below it
- Protocol layer can be implemented in hardware, software, or combo
  - Application, transport – software
  - Physical, data link layers – handle communications over a certain link – hardware
  - Network layer – mix of hardware, software

# Drawbacks

- One layer may duplicate lower-layer functionality
- Functionality at one layer may need information that is present in another layer
  - Timestamp value?
  - Violates goal of separation of layers

# Five-Layer Internet Protocol Stack

- Application (highest)
- Transport
- Network
- Link
- Physical (lowest)

# Protocol Stack

- Application Layer
  - Network applications and their application-layer protocols are located
  - Includes many protocols – HTTP, SMTP
  - Distributed over multiple end systems
    - Application in one end system using the protocol to exchange packets of information with the application in another end system
  - Packet of information – message
- Transport Layer
  - TCP or UDP
  - TCP – connection-oriented
  - UDP – connectionless-oriented
  - Transport layer packet - segment

# Protocol Stack

- Network Layer
  - Responsible for moving datagrams (network-layer packets) from one host to another
  - Transport-layer protocol in a source passes the transport-layer segment and a destination address
  - Provides the service of delivering segment to the transport layer in the destination
  - IP protocol – defines the fields in the datagram as well as how the end systems and routers act on these fields
    - Only one protocol
  - Routing protocols that determine the routes that datagrams take between sources and destinations

# Protocol Stack

- Network Layer
  - Moves network-layer packets – datagrams – from one host to another
  - Transport layer protocol (TCP or UDP) – host passes a transport-layer segment and destination address to the network layer
  - Provides the service of delivering the segment to the transport layer in the destination host
  - Also includes the IP protocol – defines fields in the datagram
  - Contains routing protocols
- Link Layer
  - Moves packet from one node to the next
  - Network layer passes datagram down to the link layer, which delivers the datagram to the next node along the route
  - Link layer protocols:  Ethernet, WiFi, DOCSIS protocol

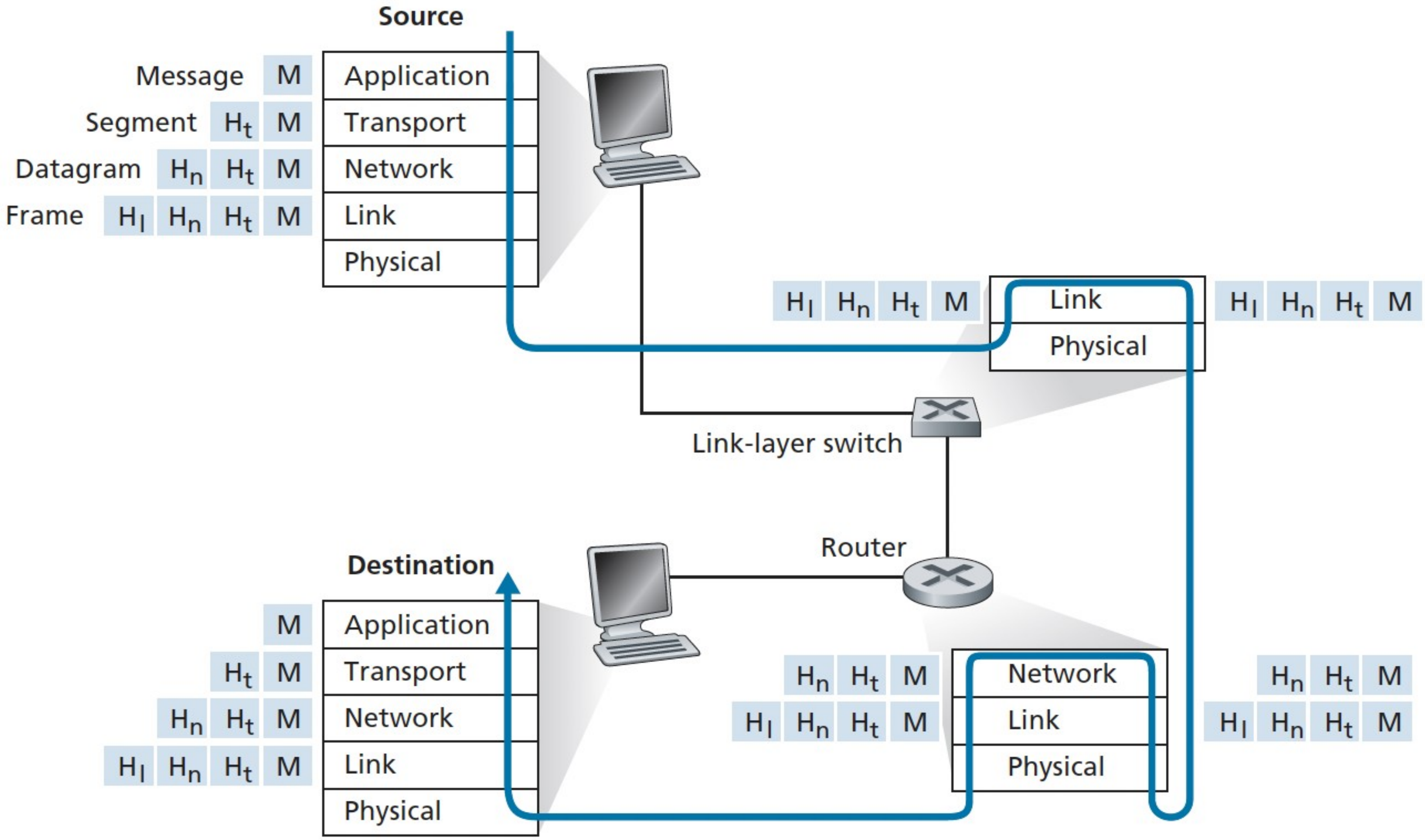
# Protocol Stack

- Physical Layer
  - Move the individual bits within the frame from one node to the next
  - Protocols in this layer are link dependent and depend on the transmission medium of the link
    - Twisted-pair copper wire
    - Coaxial cable
    - Fiber

# Encapsulation

- Routers and link-layer switches are both packet switches
  - Organize their networking hardware and software into layers
  - Do not necessarily implement all of the layers in the protocol stack
    - Usually only responsible for bottom layers
- Encapsulation
  - Sending host – an application-layer message is passed to the transport layer
  - Transport layer – takes message and appends additional information to be used by the receiver-side transport layer
  - Network layer – adds network-layer header information, such as source and destination end system addresses creating a network-layer datagram
  - Each layer – packet has two types of fields
    - Header field
    - Payload field – typically a packet from the layer above

# Hosts, Routers, and Link-Layer Switches, Each with a Different Set of Layers – Figure 1.24



# Networks Under Attack

- Malware via Internet
- Attack Servers and Network Infrastructure – DoS Attacks
  - Vulnerability – right sequence of packets can cause a system to crash
  - Bandwidth flooding – prevents legitimate packets from reaching the server
  - Connection flooding – attacker establishes a large number of half-open/fully-open TCP connections at the target host
    - Host can become so bogged down that it stops accepting legitimate connections
- DDoS Attack
  - Attacker controls multiple sources and has each source blast traffic at the target
  - Use botnets with thousands of compromised hosts
  - Difficult to detect/defend against
- Packet Sniffing – via passive receiver that records a copy of every packet that flies by
- IP Spoofing
  - Need:  end-point authentication – determine with certainty if a message originates from where we think it does

# End Chapter 1

- Homework – See Canvas
- Next Time – Chapter 2