Computer Networks
@CS.NYCU

Lecture 1: Introduction

Instructor: Kate Ching-Ju Lin (林靖茹)

Slides modified from
"Computer Networking: A Top-Down Approach" 7th Edition

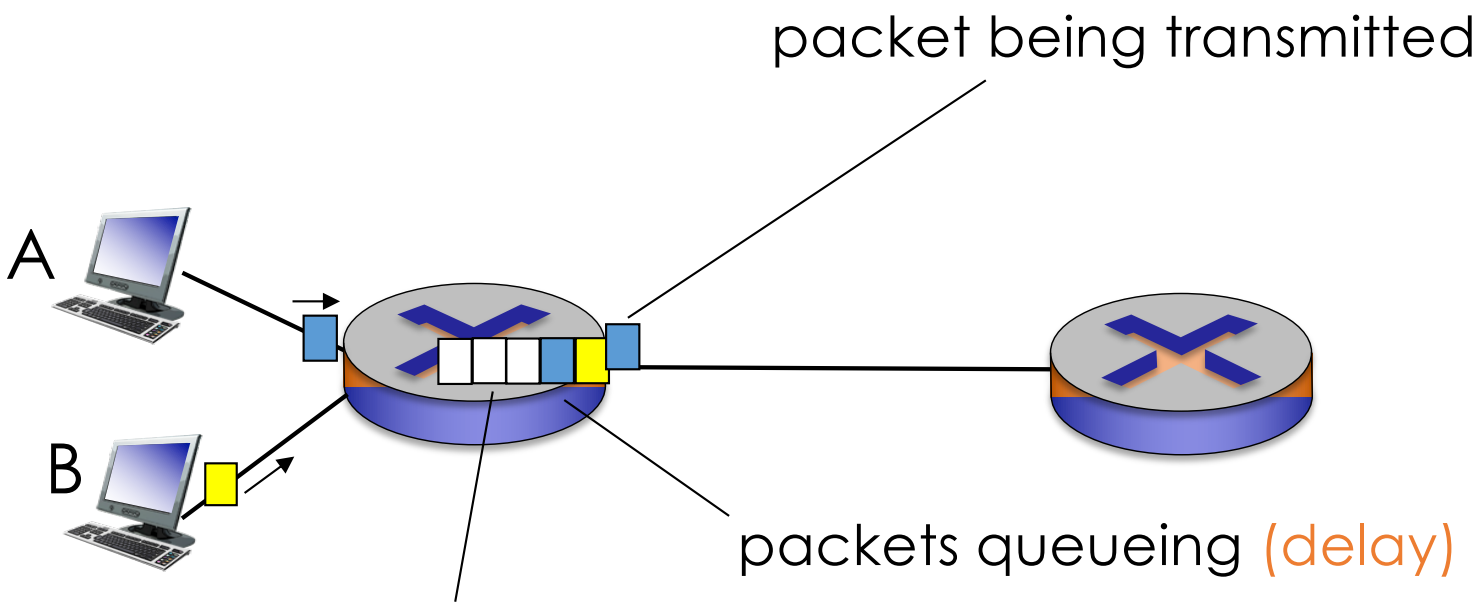
Outline

- What's the Internet?
- What's a protocol?
- Network edge
  - hosts, access network, physical links
- Network core
  - packet/circuit switching, Internet structure
- **Performance**
  - loss, delay, throughput
- Protocol layers, service models
- Network Security
- History

How do loss and delay occur?

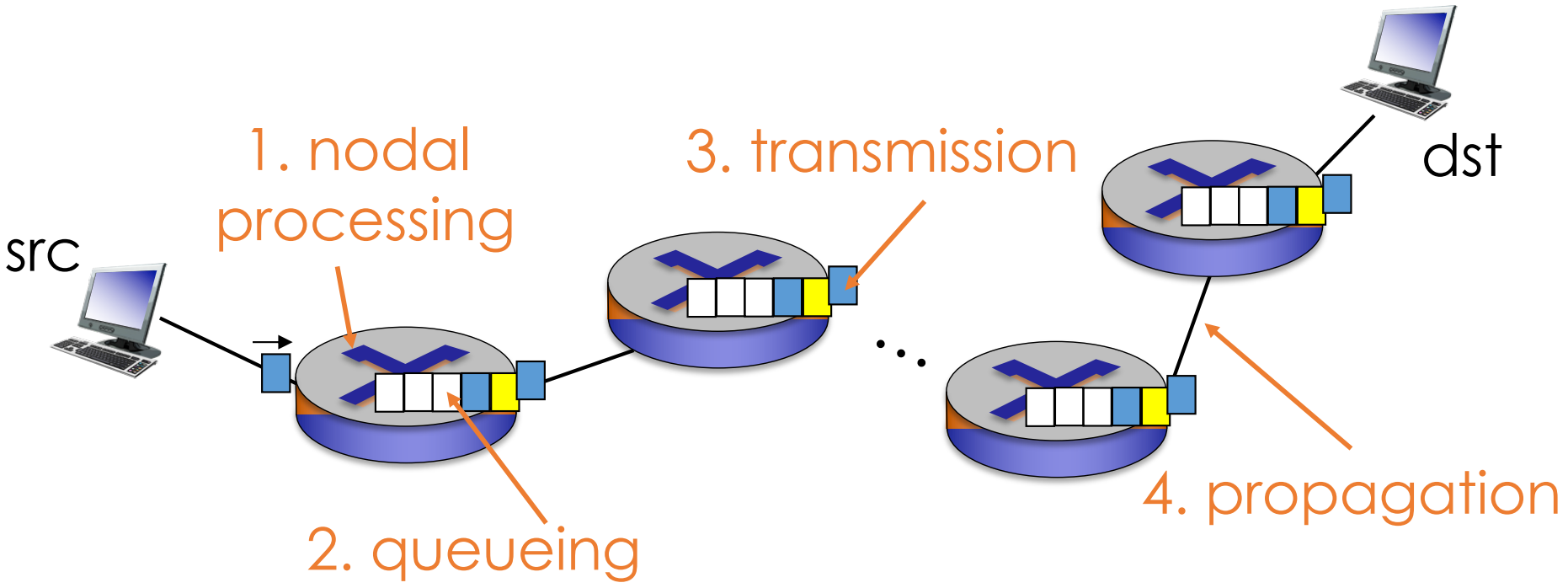
packets queue in router buffers

- packet arrival rate to link (temporarily) exceeds output link capacity
- packets queue, wait for turn



What is End-To-End Delay?

- Time taken for a packet to be transmitted from the source to the destination

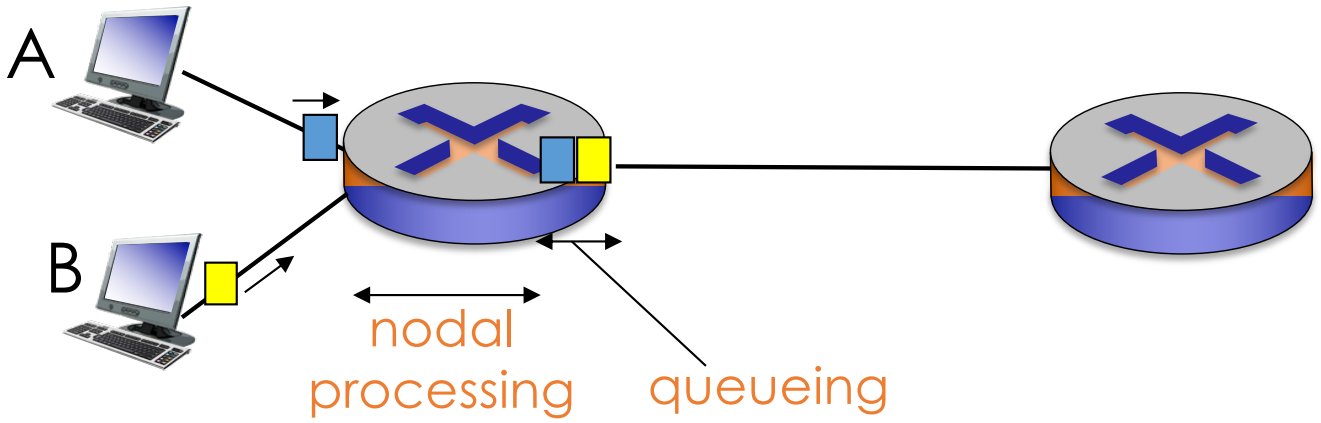


Four Sources of Packet Delay

1. **Nodal processing delay**
   - Time required to examine the packet's header and determine where to go
2. **Queueing delay**
   - Wait in the buffer for being transmitted onto the link
3. **Transmission delay**
   - Time required to push all the packet's bits into the link
4. **Propagation delay**
   - Time required to propagate from the beginning of the link to another end point

Four Sources of Packet Delay

- d_{proc}: nodal processing
  - check bit errors
  - determine output link
  - typically < msec
- d_{queue}: queueing delay
  - time waiting at output link for transmission
  - depends on congestion level of router

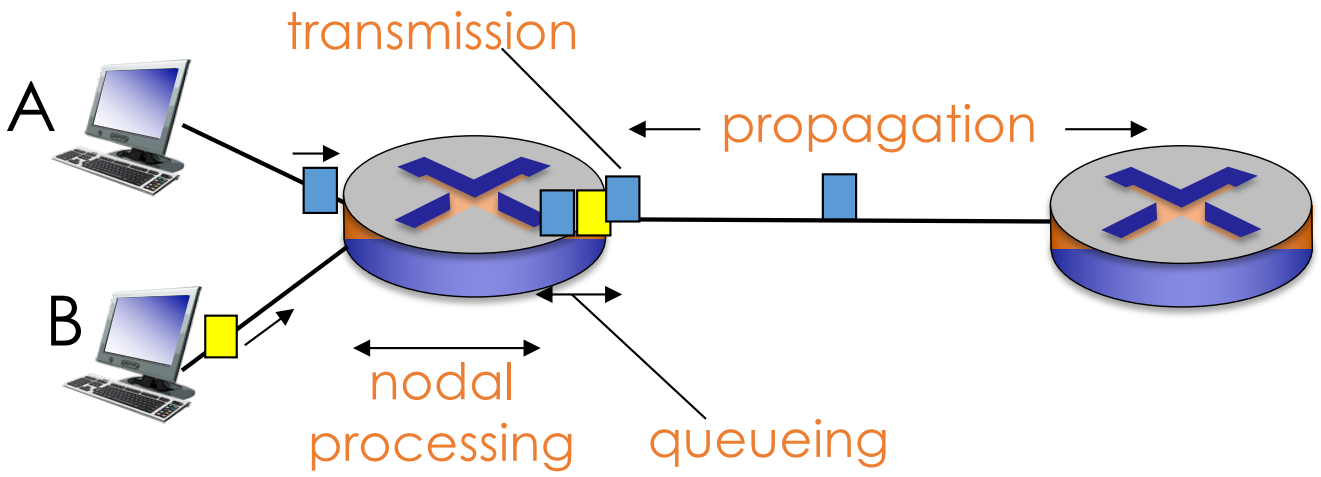


Four Sources of Packet Delay

- d_{trans}: transmission delay
  - L: packet length (bits)
  - R: link bandwidth (bps)
  - $d_{trans} = L/R$

d_{trans} and d_{prop} *very* different

- d_{prop}: propagation delay
  - d: length of physical link
  - s: propagation speed (e.g., light speed $3x10^8$ m/sec)
  - $d_{prop} = d/s$



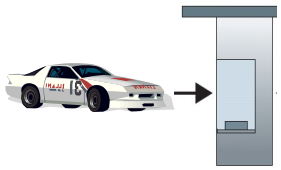
$$d_{e2e} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

Transmission vs. Propagation

- Analog to cars driving through a high way (e.g., Snow Mountain tunnel)

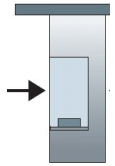
Transmission vs. Propagation

- Analog to cars driving through tollbooth
  - Transmission: time required to pass through a tollbooth (determined by the capacity of the tollbooth)
  - Propagation: time from one tollbooth to another (determined by the driving speed)



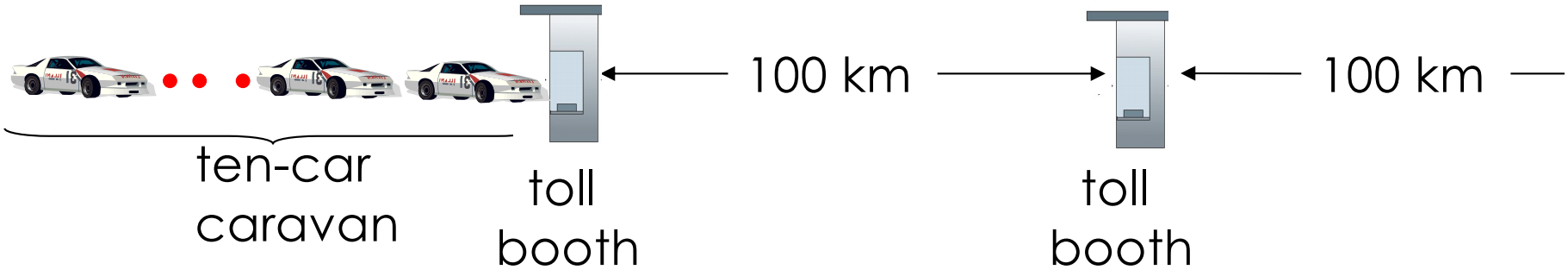
transmission

propagation



transmission

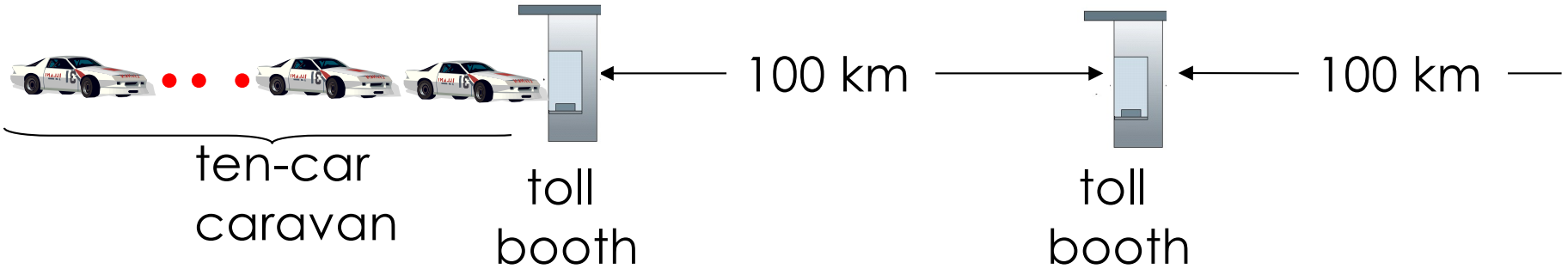
Example



- Cars "propagate" at 100 km/hr
- Toll booth takes 12 sec to service car (bit transmission time)
- car ~ bit; caravan ~ packet
- Q: How long until caravan is lined up before 2nd toll booth?

- Time to "push" entire caravan through toll booth onto highway = 12*10 = 120 sec
- Time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr
- A: 62 minutes

Example

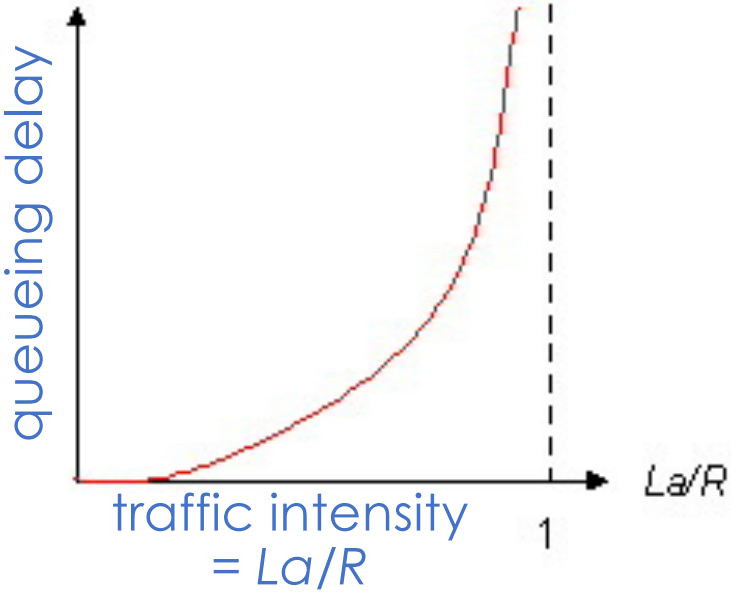


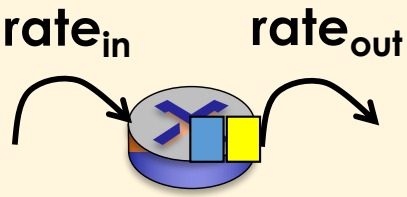
- Suppose cars now "propagate" at 1000 km/hr, and suppose toll booth now takes one min to service a car
- Q: Will cars arrive to 2nd booth before all cars serviced at first booth?

A: Yes! after 7 min, first car arrives at second booth; three cars still at first booth

Queueing Delay (revisited)

- R: link bandwidth (bps)
- L: packet length (bits)
- a: average packet arrival rate





traffic intensity:
$rate_{in}$ / $rate_{out}$ = La/R

- La/R ~ 0: avg. queueing delay small
- La/R →1: avg. queueing delay large
- La/R > 1: more "work" arriving than can be serviced, average delay **infinite**!

La/R ~ 0

La/R →1

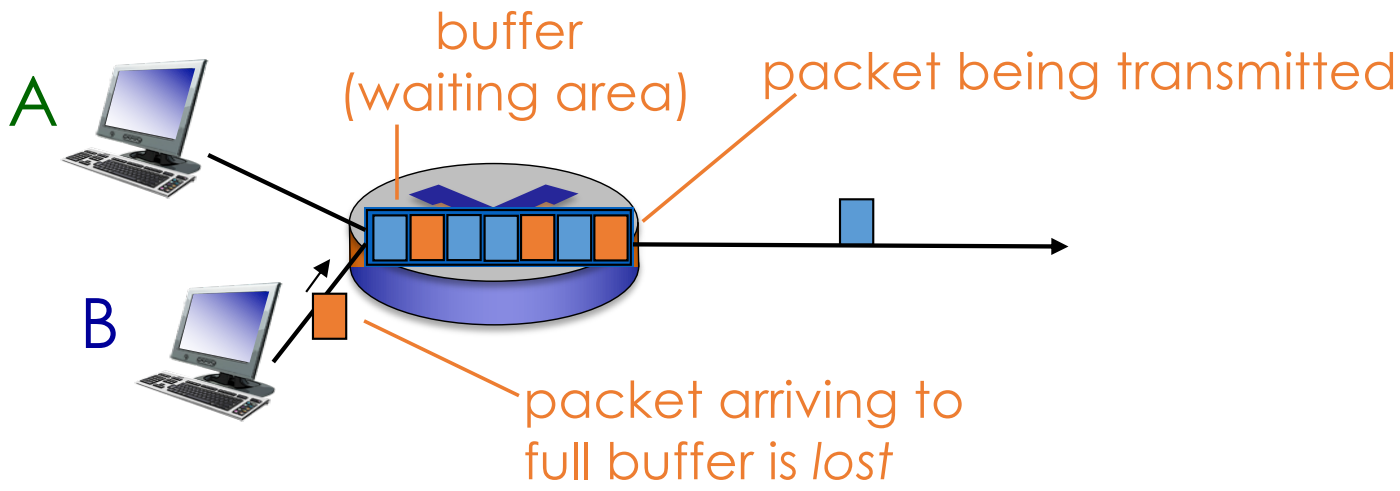
Try "traceroute"

- traceroute from linux6.cs.nctu.edu.tw (or your local machine) to www.csail.mit.edu and answer the following questions

1. Copy and paste your results
2. How many hops are there from the sources to the destination?
3. What is the hop with the longest delay?
4. Why sometimes a later router responds faster than earlier routers? (Why sometimes the response latency is decreasing?)

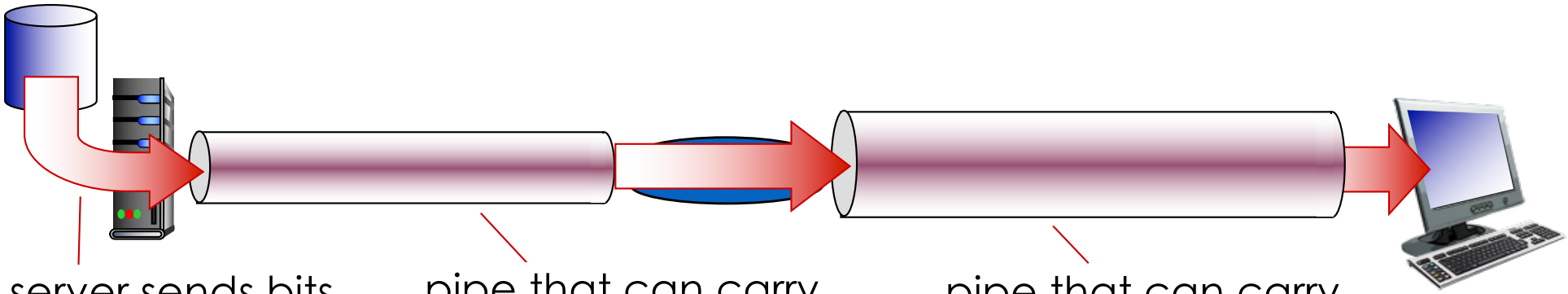
Packet Loss

- Queue (aka buffer) preceding a link has finite capacity
- Packets arriving to a full queue are dropped
- Lost packet may be retransmitted by previous node, by source end system, or not at all



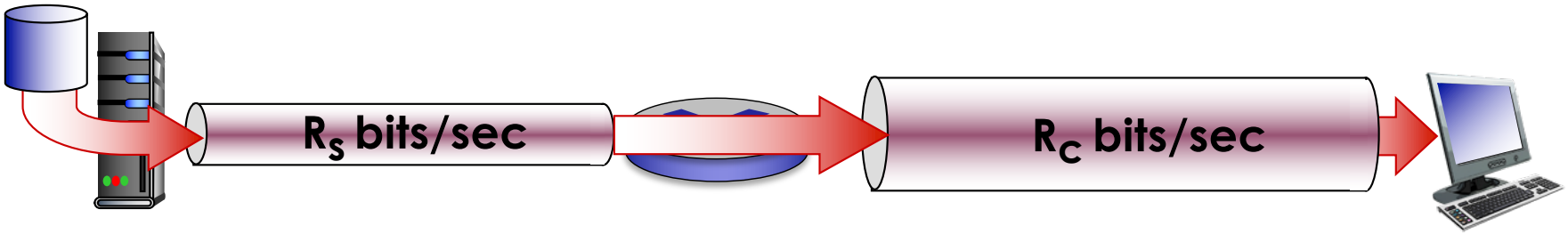
Throughput

- Throughput: rate (bits/time) at which bits transferred between sender/receiver
  - instantaneous: rate at a given point in time (how many bits sent in one second)
  - average: rate over longer period of time (how many time required to send a batch of bits)

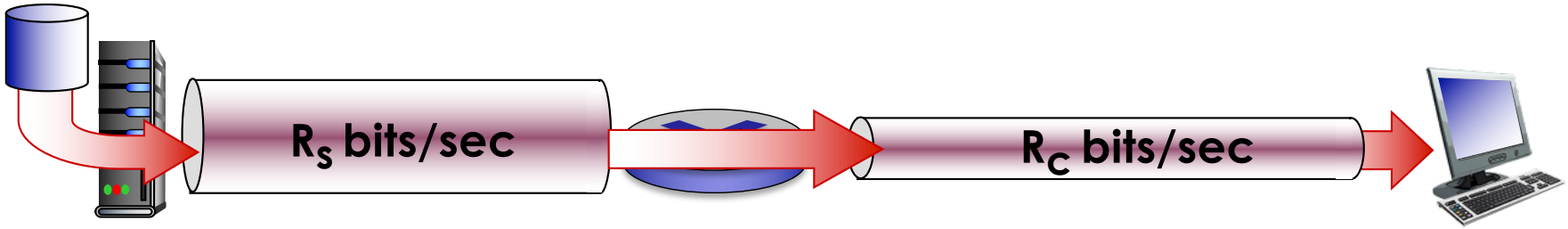


Throughput

- $R_s < R_c$ What is average end-end throughput?



- $R_s > R_c$ What is average end-end throughput?

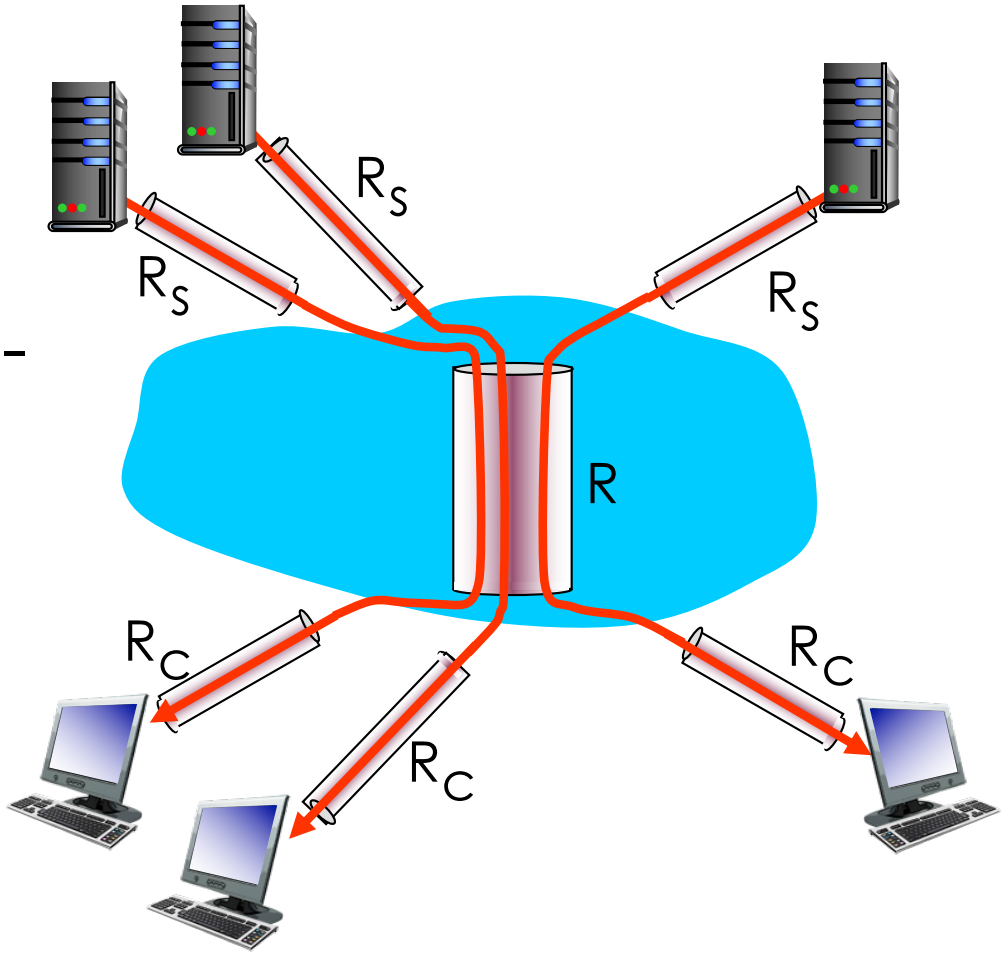


bottleneck link

- The link along a path with the minimum capacity
- The bottleneck link limits the end-end throughput

Throughput: Internet Scenario

- per-connection end-to-end throughput: *min(R_c,R_s,R/10)*
- In practice: R_c or R_s is often bottleneck



10 connections (fairly) share backbone bottleneck link R bits/sec

Outline

- What's the Internet?
- What's a protocol?
- Network edge
  - hosts, access net, physical media
- Network core
  - packet/circuit switching, Internet structure
- Performance
  - loss, delay, throughput
- **Protocol layers, service models**
- Network Security
- History

Protocol "Layers"

- Networks are complex, with many "pieces"
  - hosts
  - routers
  - links of various media
  - applications
  - protocols
  - hardware, software

- How to simplify the organization of a network?
  → **Layering!**
  - Build a structure: divide tasks based on their functionality and assign each task to a proper layer

Why Layering?

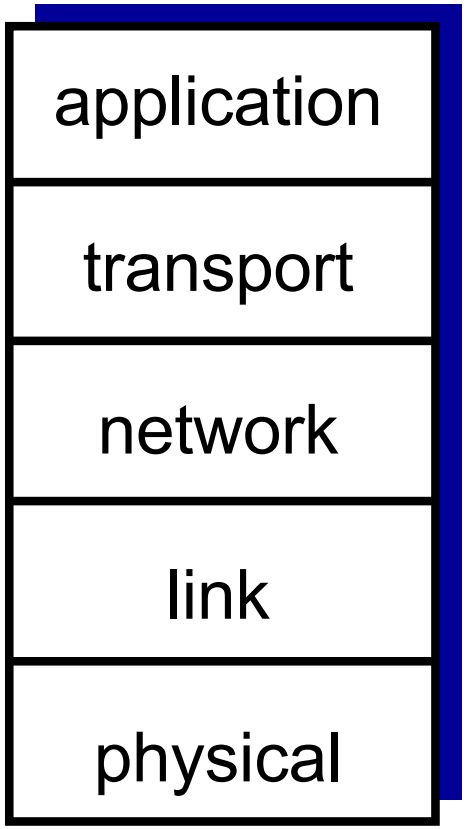
Dealing with complex systems:

- Explicit structure allows identification, relationship of complex system's pieces
  - Layered *reference model* for discussion
- Modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system
  - e.g., changing your home access from DSL to fiber doesn't affect the rest of a system
- Layering considered harmful?
  - May exist dependency between layers
  - If so, cross-layer designs might be preferable

Internet Protocol Stack

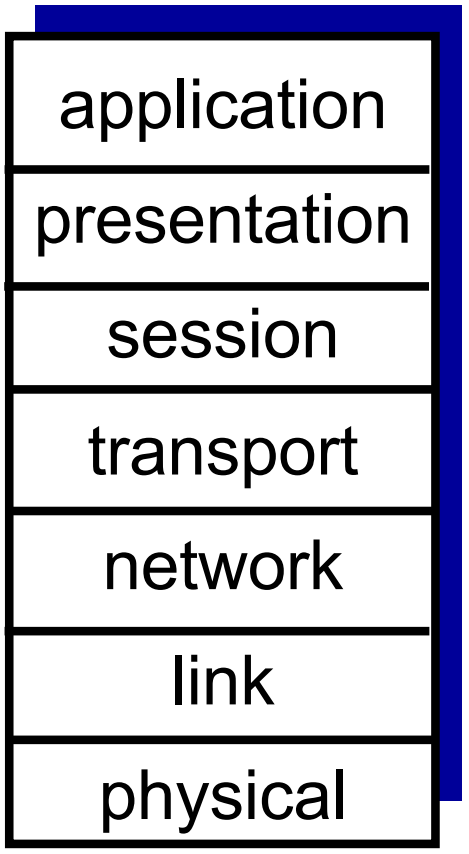
- ***Application:***
  - supporting network services
  - FTP, SMTP, HTTP, DNS (message)
- ***Transport:***
  - process-to-process data transfer
  - TCP, UDP (segment)
- ***Network (aka IP):***
  - end-to-end routing from source to destination (along a path)
  - IP, routing protocols (packet)
- ***Link:***
  - data transfer between neighboring network elements (host-to-host)
  - Ethernet, 802.11, PPP (frame)
- ***Physical:***
  - bits on the communication channels, i.e., "wire" or "air" (symbol)

Top-down approach

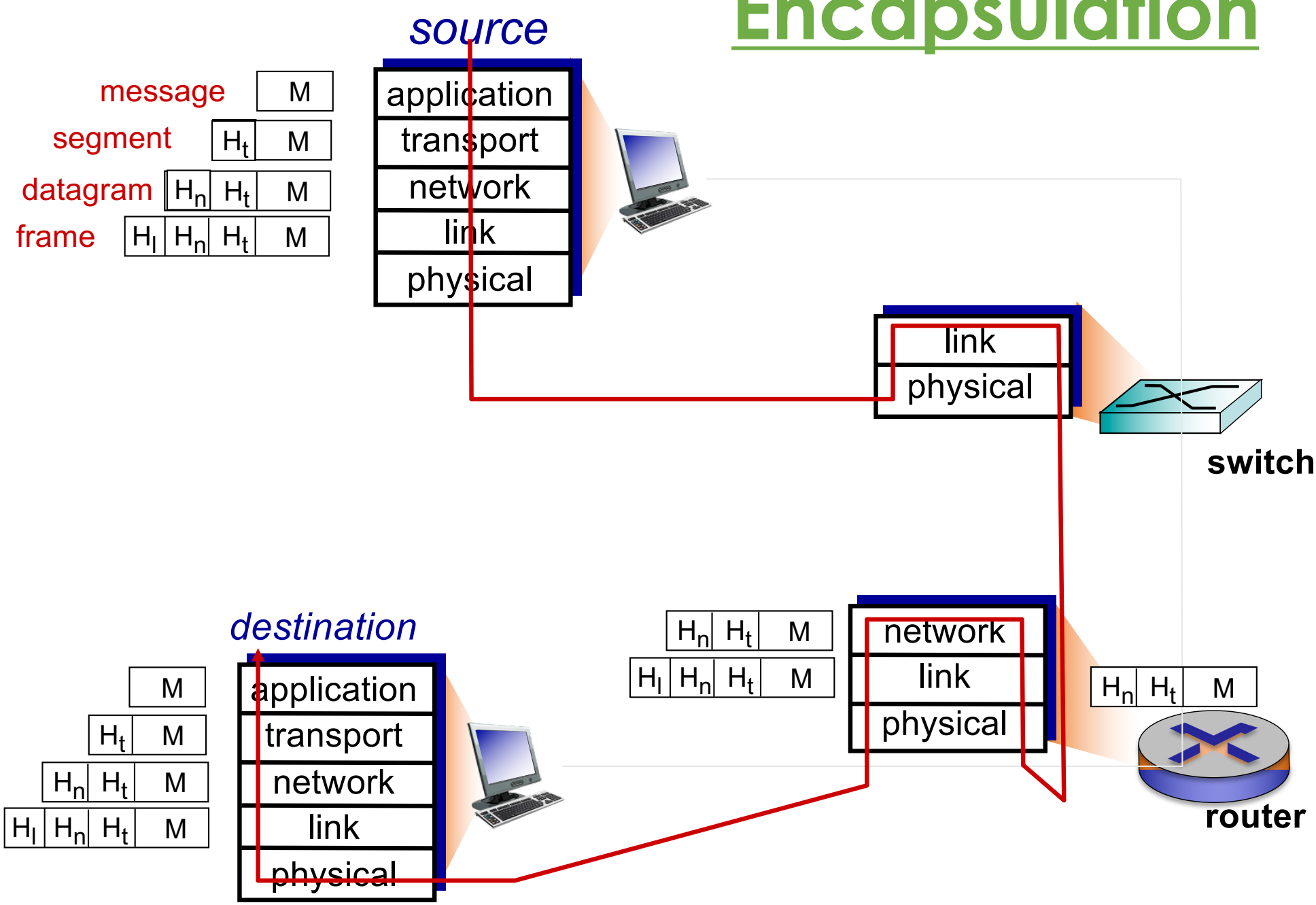


ISO/OSI Reference model

- ***presentation:***
  - allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- ***session:***
  - synchronization, check-pointing, recovery of data exchange
- Internet stack "missing" these layers!
  - optional
  - these services, if needed, must be implemented in application



Encapsulation



Outline

- What's the Internet?
- What's a protocol?
- Network edge
  - hosts, access net, physical media
- Network core
  - packet/circuit switching, Internet structure
- Performance
  - loss, delay, throughput
- Protocol layers, service models
- **Network Security**
- History

Network Attacks

- Malware
- Packet sniffing
- Man-in-the-middle attack
- DDoS (Distributed Denial-of-Service)
- IP Spoofing

Malware

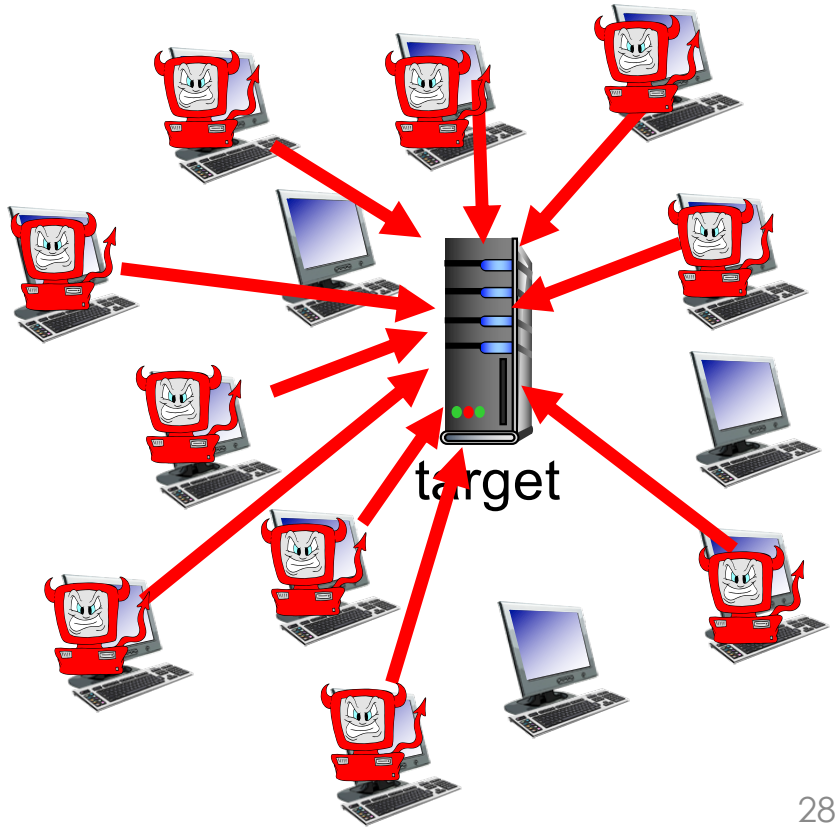
- Malicious stuffs that infect our devices
  - Deleting files
  - Installing **spyware** (steal private info.)
  - …
- **Botnet**: malware can be self-replicating
  - Infected host could become one of the attackers
  - Spread exponentially
- How malware spreads?
  - **Virus:** require user interaction (e.g., opening e-mail attachment)
  - **Worm:** passively take actions without user interaction

Denial-of-Service (DoS)

- Make resources (server, bandwidth) unavailable to legitimate users
- Three categories
  - **Vulnerability attack**: crash the system
  - **Bandwidth flooding**: exhaust all available bandwidth and prevent legitimate packet from reaching the server
  - **Connection flooding**: occupy all possible TCP connections on a server

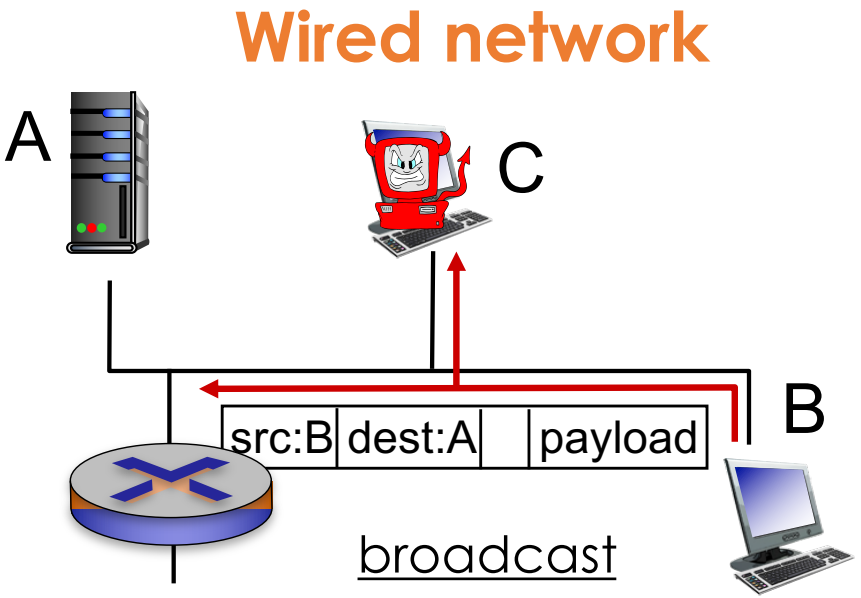
Distributed Denial-of-Service (DDoS)

- A single attacker may no be capable of generate enough traffic to harm the server
- Control multiple distributed devices to attack the target
  - How? **Botnet**



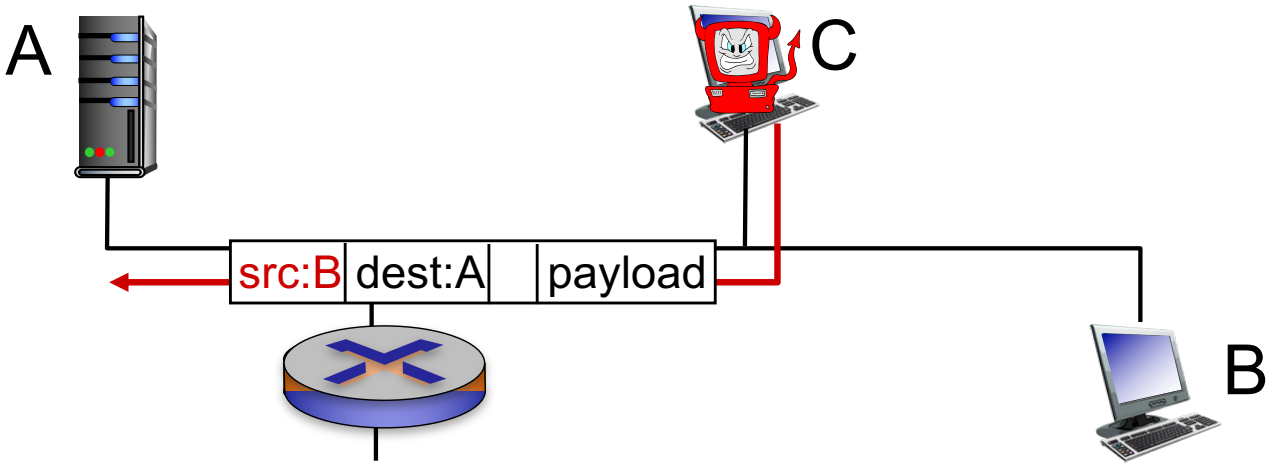
Packet Sniffing

- Promiscuous network interface hears all packets passing by
- Not always bad. Can be used to monitor/diagnose network performance
- Sniffer: sniffing software, e.g., Wireshark



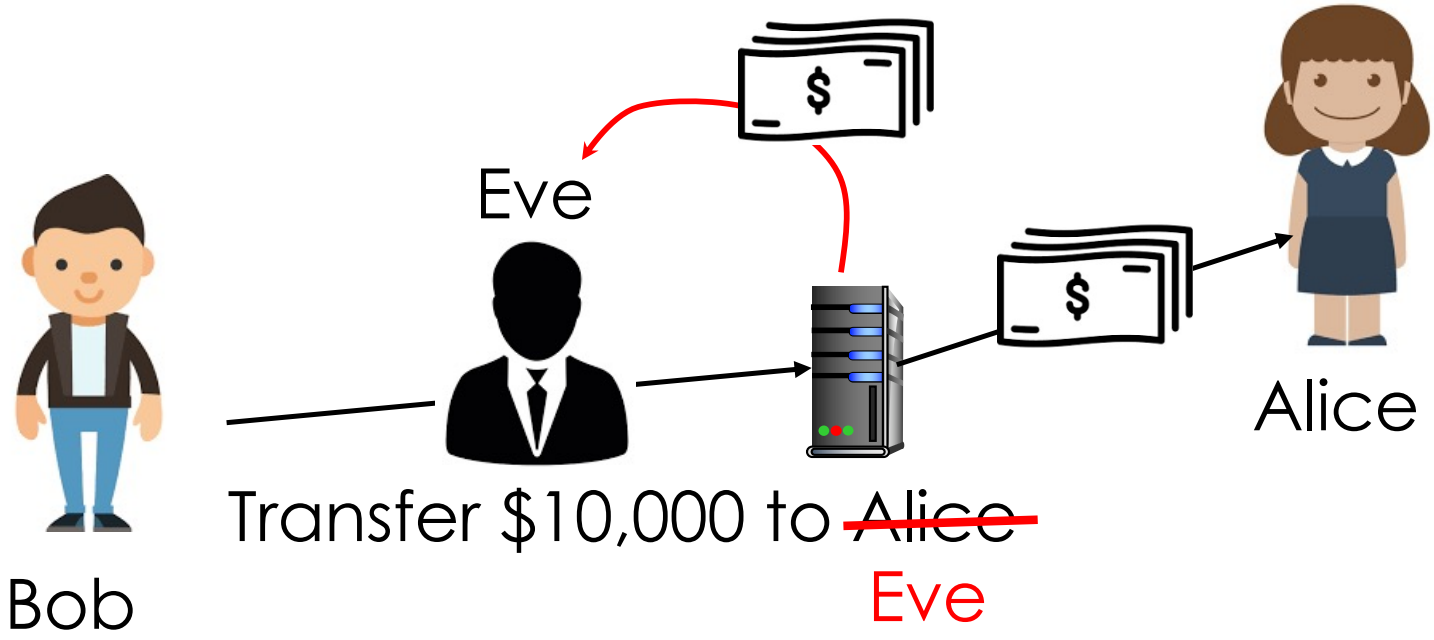
IP Spoofing

send packet with false source address



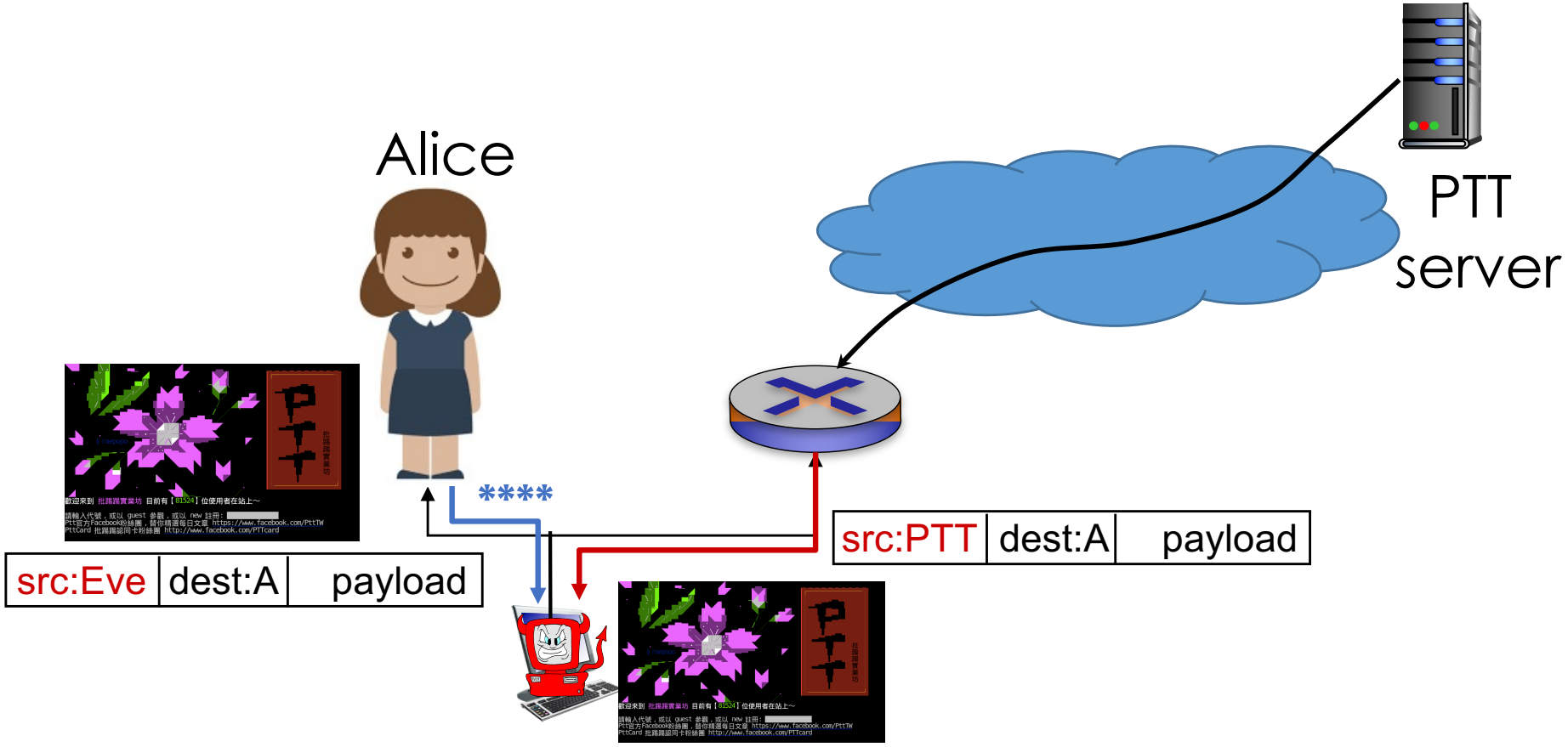
Man In The Middle (MITM)

- An attacker relays and alters the communications between two hosts



Overhear your PTT password!

- man-in-the-middle + IP spoofing



Outline

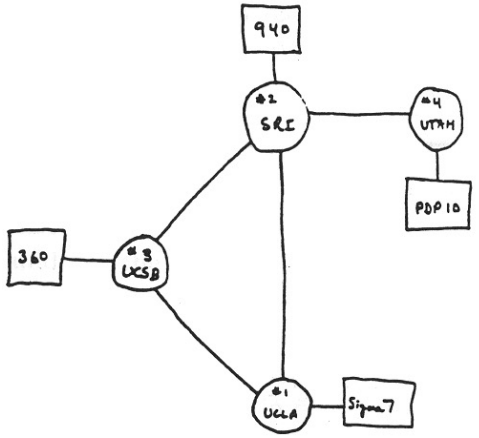
- What's the Internet?
- What's a protocol?
- Network edge
  - hosts, access net, physical media
- Network core
  - packet/circuit switching, Internet structure
- Performance
  - loss, delay, throughput
- Protocol layers, service models
- **History**

Internet History

1961-1972: Early packet-switching principles

- 1961: Kleinrock - queueing theory shows effectiveness of packet-switching
- 1964: Baran - packet-switching in military nets
- 1967: ARPAnet conceived by Advanced Research Projects Agency
- 1969: first ARPAnet node operational

- 1972:
  - ARPAnet public demo
  - NCP (Network Control Protocol) first host-host protocol
  - first e-mail program
  - ARPAnet has 15 nodes



THE ARPA NETWORK

Internet History

1972-1980: Internetworking, new and proprietary nets

- 1970: ALOHAnet satellite network in Hawaii
- 1974: Cerf and Kahn - architecture for interconnecting networks
- 1976: Ethernet at Xerox PARC
- late70's: proprietary architectures: DECnet, SNA, XNA
- late 70's: switching fixed length packets (ATM precursor)
- 1979: ARPAnet has 200 nodes

Cerf and Kahn's internetworking principles:

- minimalism, autonomy - no internal changes required to interconnect networks
- best effort service model
- stateless routers
- decentralized control

define today's Internet architecture

Internet History

1980-1990: new protocols, a proliferation of networks

- 1983: deployment of TCP/IP
- 1982: smtp e-mail protocol defined
- 1983: DNS defined for name-to-IP-address translation
- 1985: ftp protocol defined
- 1988: TCP congestion control

- new national networks: CSnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks

Internet History

1990, 2000's: commercialization, the Web, new apps

- early 1990's: ARPAnet decommissioned
- 1991: NSF lifts restrictions on commercial use of NSFnet (decommissioned, 1995)
- early 1990s: Web
  - hypertext [Bush 1945, Nelson 1960's]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, later Netscape
  - late 1990's: commercialization of the Web

late 1990's – 2000's:

- more killer apps: instant messaging, P2P file sharing
- network security to forefront
- est. 50 million host, 100 million+ users
- backbone links running at Gbps

Internet History

2005-present

- ~5B devices attached to Internet (2016)
  - smartphones and tablets
- aggressive deployment of broadband access
- increasing ubiquity of high-speed wireless access
- emergence of online social networks:
  - Facebook: ~ one billion users
- service providers (Google, Microsoft) create their own networks
  - bypass Internet, providing "instantaneous" access to search, video content, email, etc.
- e-commerce, universities, enterprises running their services in "cloud" (e.g., Amazon EC2)