COMPUTER NETWORKS
CHAP 1 : INTRODUCTION

ESIEE PARIS

IN411

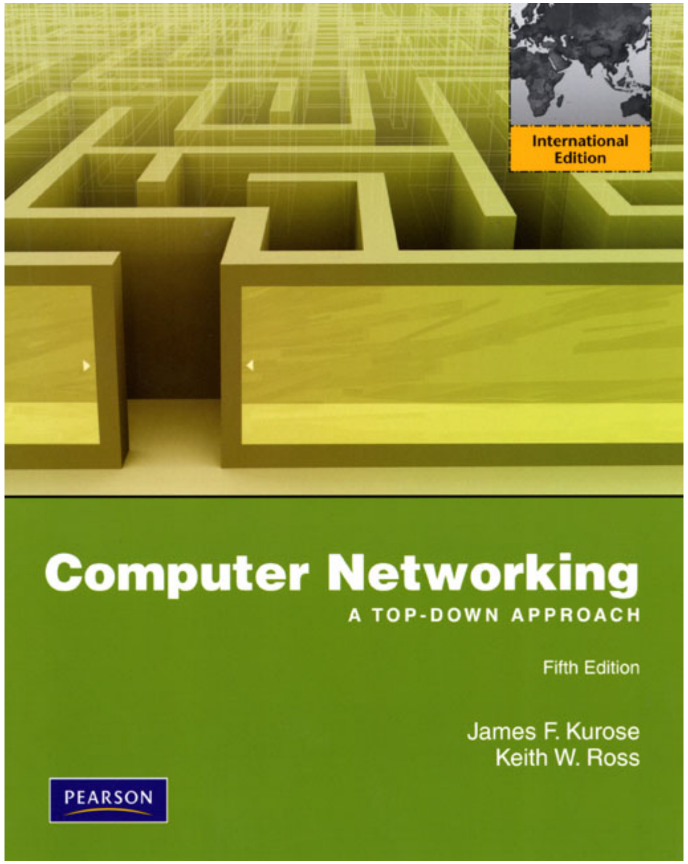
15 h – 18 h

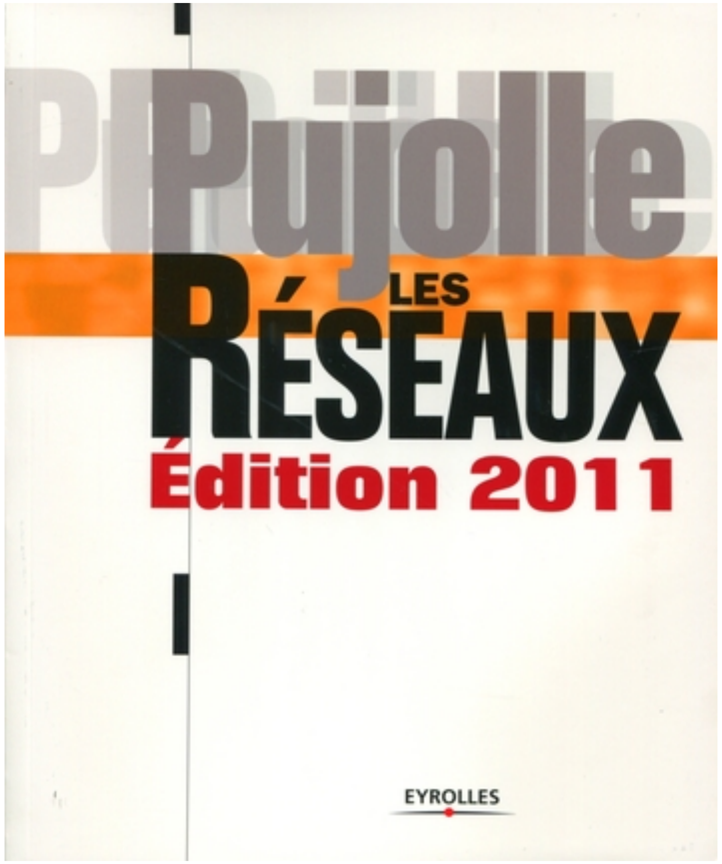
Short CV

- Samer Ammoun
  - samer.ammoun@mines-paris.org
  - 33 years old
- Innovation engineer at « Modulowatt ingénierie »
  - www.modulowatt.com
- Expert Engineer in cooperative ITS at Inria Rocqencourt
  - www.imara.inria.fr
- Phd in mobile robotics « Innovative application in vehicular network for safety enhancement» at Ecole des Mines de Paris
  - caor.ensmp.fr
- Telecommunication and computer science engineer at lebanese university

ESIEE ENGINEERING

References


International Edition
Computer Networking
A TOP-DOWN APPROACH
Fifth Edition
James F. Kurose
Keith W. Ross
PEARSON


Pujolle
LES RÉSEAUX
Édition 2011
EYROLLES

Computer networks

- Goal
  - What are looking from this course ?
- Prerequisites

Dates and contents

mar. 13/09/2011	15h	18h	0160
jeu. 22/09/2011	08h	12h	0210
sam. 24/09/2011	10h	12h	0110
jeu. 29/09/2011	08h	12h	0160
sam. 08/10/2011	08h	12h	0160
lun. 10/10/2011	13h	17h	0110
mar. 11/10/2011	08h	09h	0160

Introduction

Application layer

Transport layer

Network layer

Link and physical layers

Security

Mobile and wireless networks

Network management

….

Computer Networks

- Computer
- Networks

Chapter 1: Introduction

Our goal:

- get "feel" and terminology
- more depth, detail *later* in course
- approach:
  - use Internet as example

Overview:

- 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
- security
- protocol layers, service models
- history

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

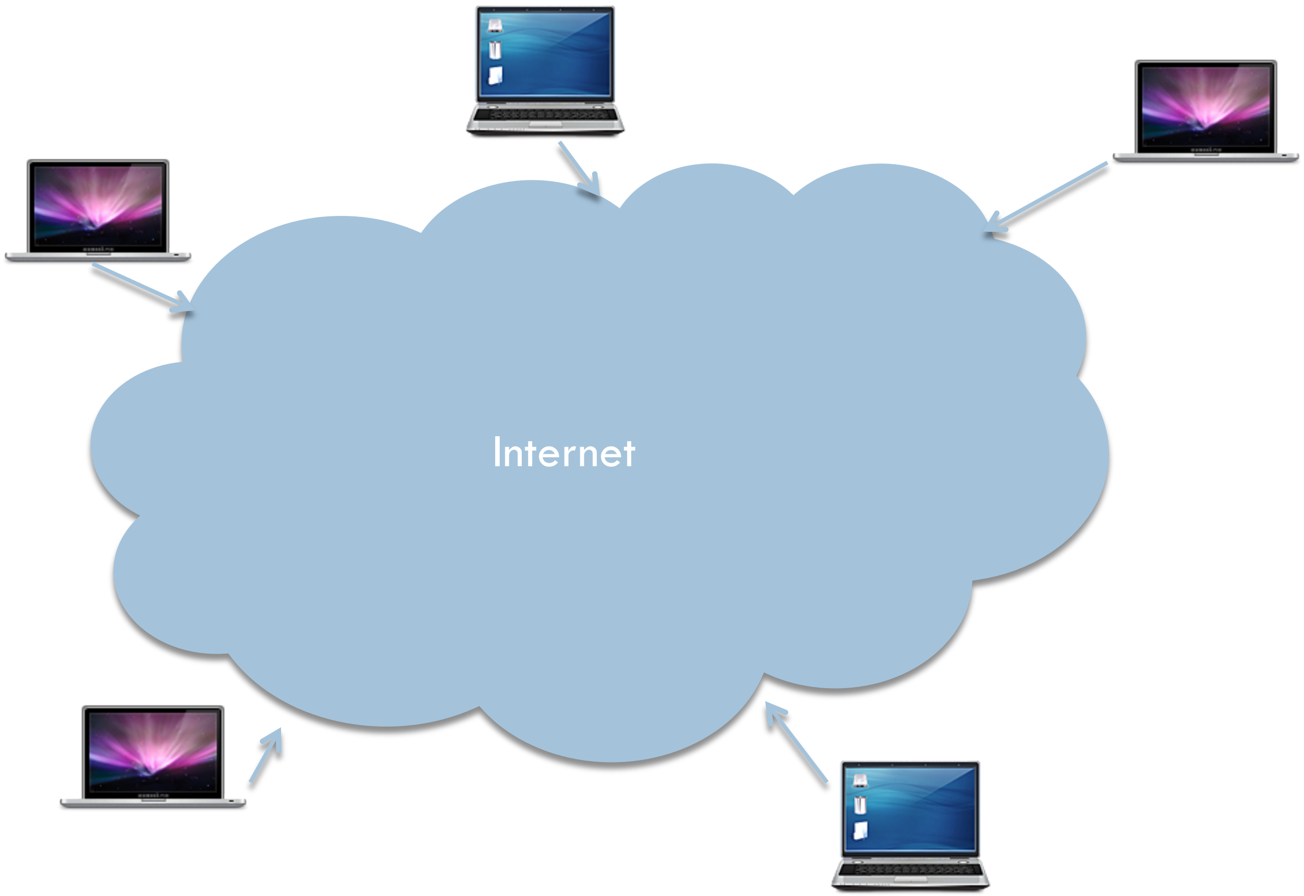
1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

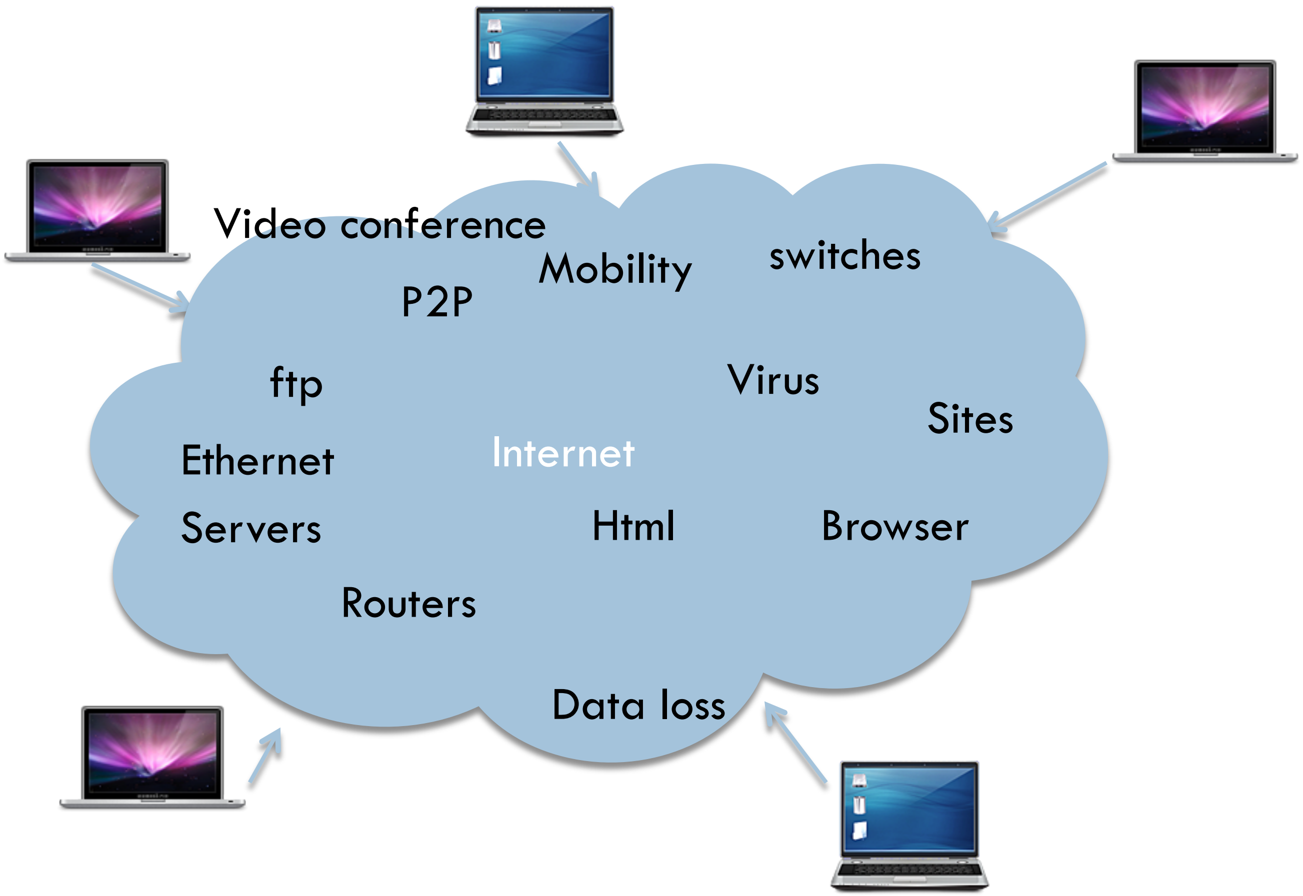
1.6 Networks under attack: security

1.7 History

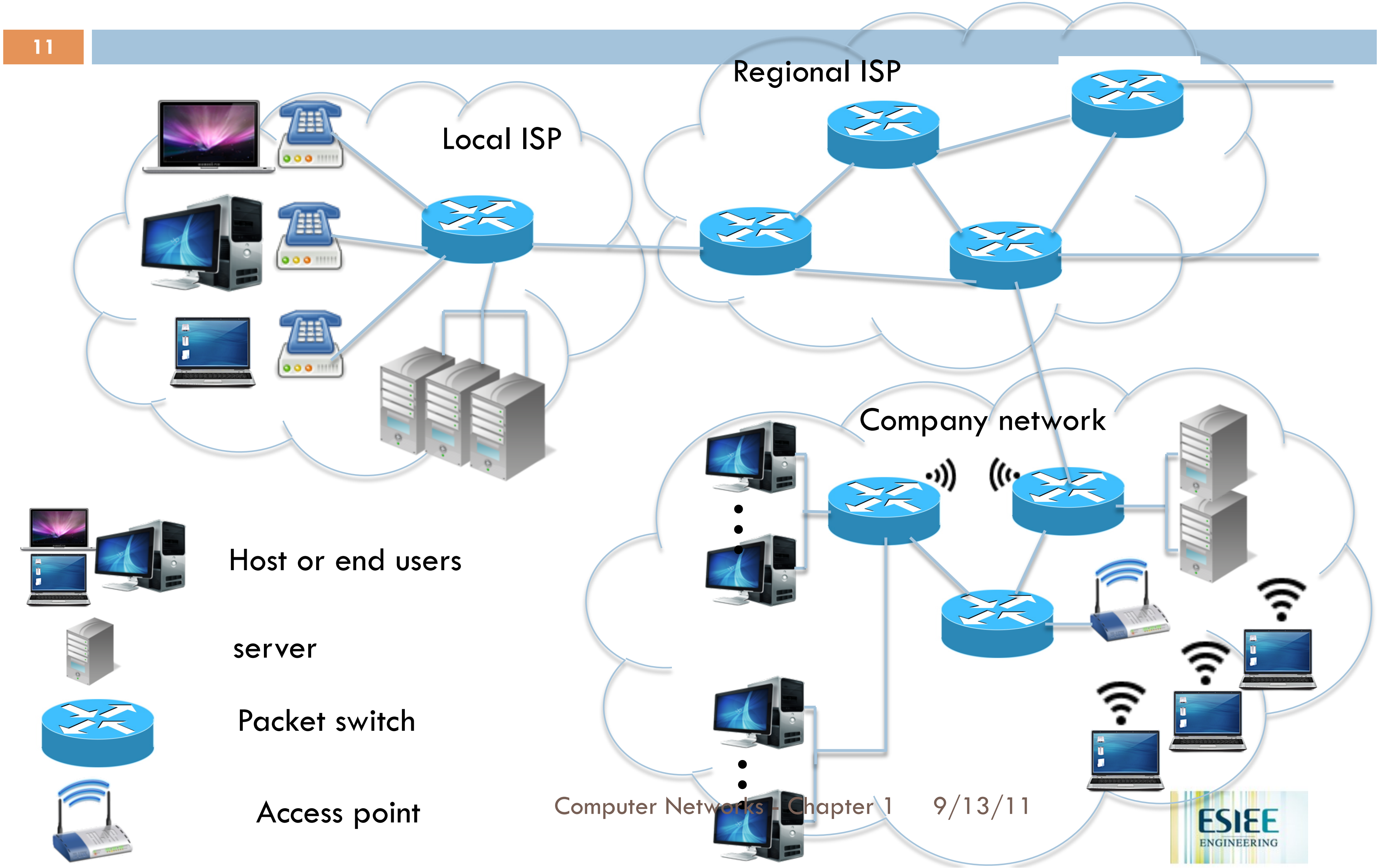
What's the Internet: General view



What's the Internet: General view



What's the Internet: General view



What's the Internet ?

- Millions of connected « computers » : 600 millions of end-users (July 2008)
- Running Network applications
- Links :
  - copper, Fiber optics, radio, etc.
- packet switches:
  - router, link layer switch, etc.
- Protocols :
  - http, TCP/IP, UDP, SMTP
- Architecture:
  - loosely hierarchical
  - public Internet versus private intranet
- Standards :
  - RFC Request for Comments,
  - IETF Internet Engineering Task Force

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

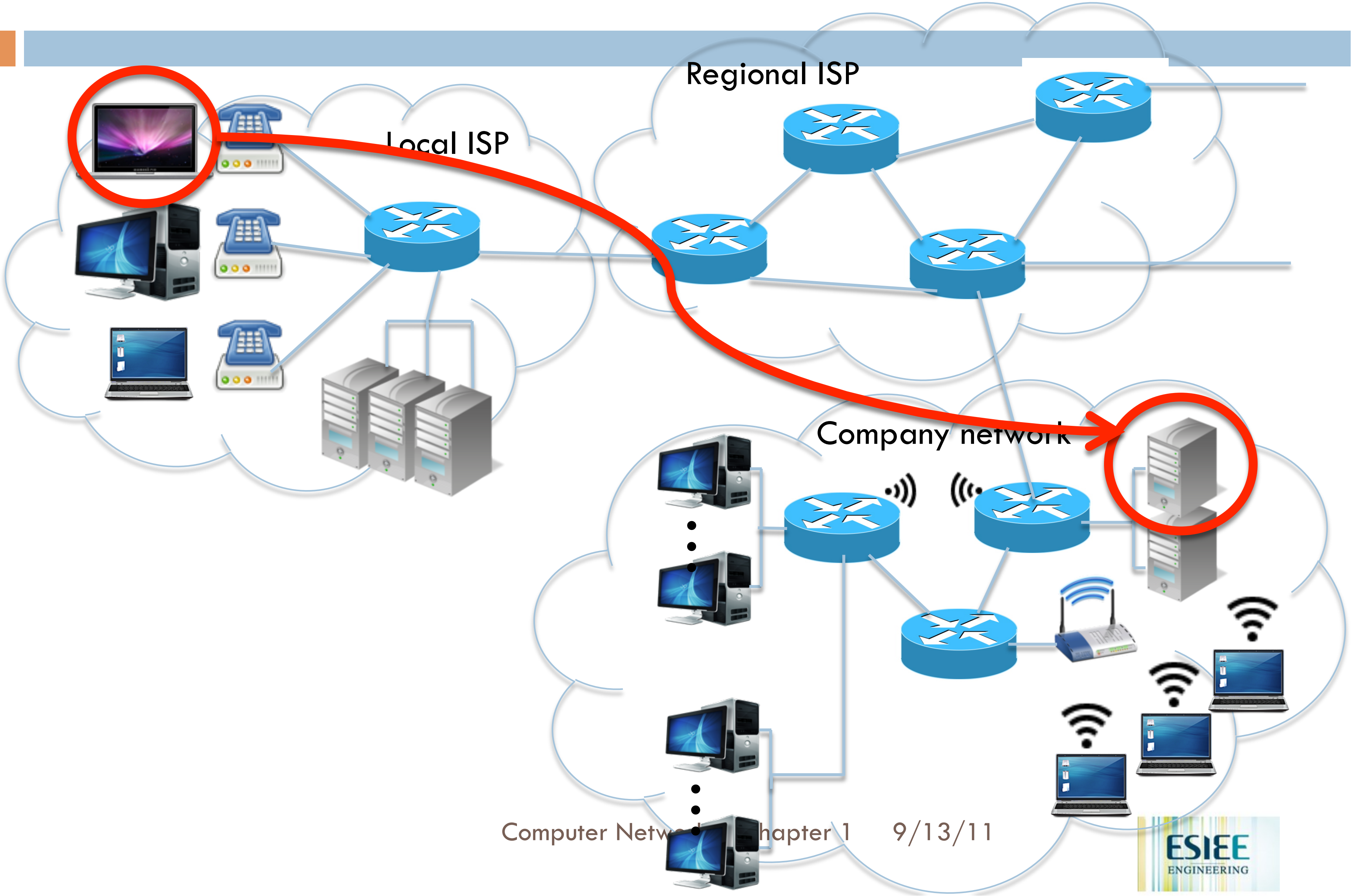
1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

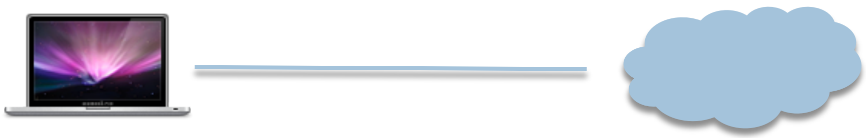
1.7 History

Network Edge



What is Protocol ?

- Internet as a shared infrastructure



- Software in the end users that knows how to communicate with « networks »
- Example of Alice mail

Network Edge

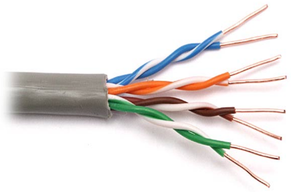
- Client server program
  - End system requests a service from a server
  - Ex : ?
- Peer to Peer program
  - End system to end system (not 100%)
  - Client and server on each side
  - Ex : ?

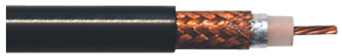
Physical Media

- Bit: propagates between transmitter/rcvr pairs
- physical link: what lies between transmitter & receiver
- guided media:
  - signals propagate in solid media: copper, fiber, coax
- unguided media:
  - signals propagate freely, e.g., radio

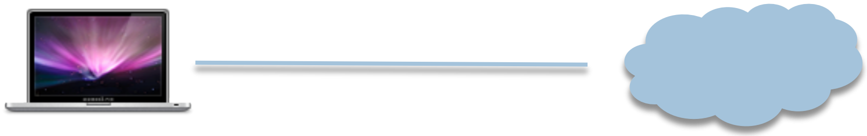
Physical Media

- Twisted pair
- Coaxial Cable
- Fiber optics
- Terrestrial radio channel
- Satellite radio channel



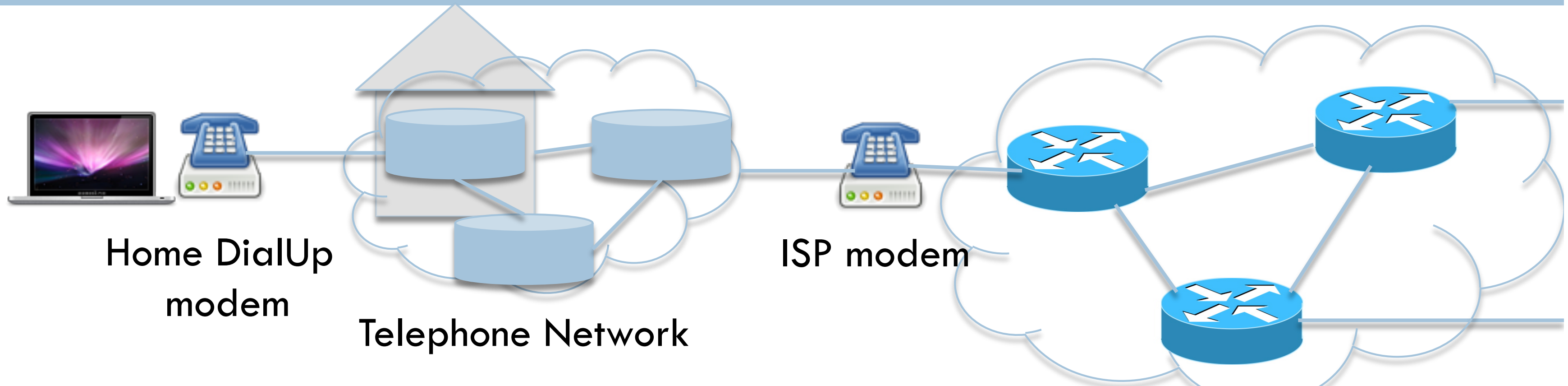


Access Networks and physical media



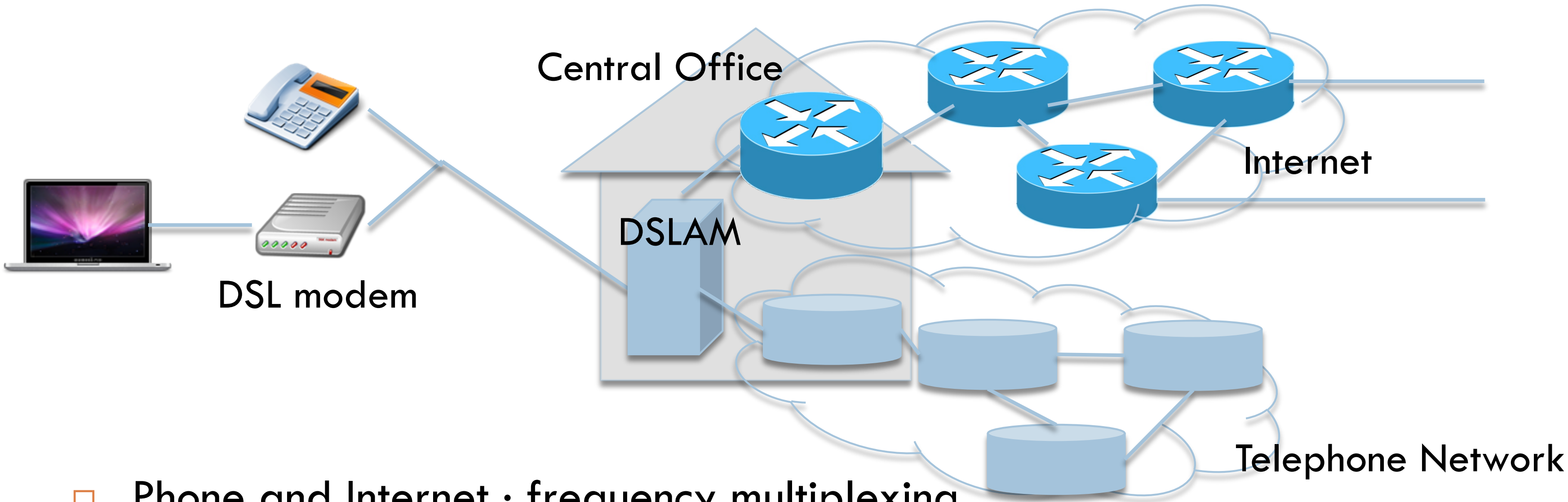
- Dial up
- DSL
- Cable
- FTTH (Fiber To The Home)
- Ethernet
- WiFi
- Wide Area Access Network
- Wimax

Access Networks and physical media Dial-up



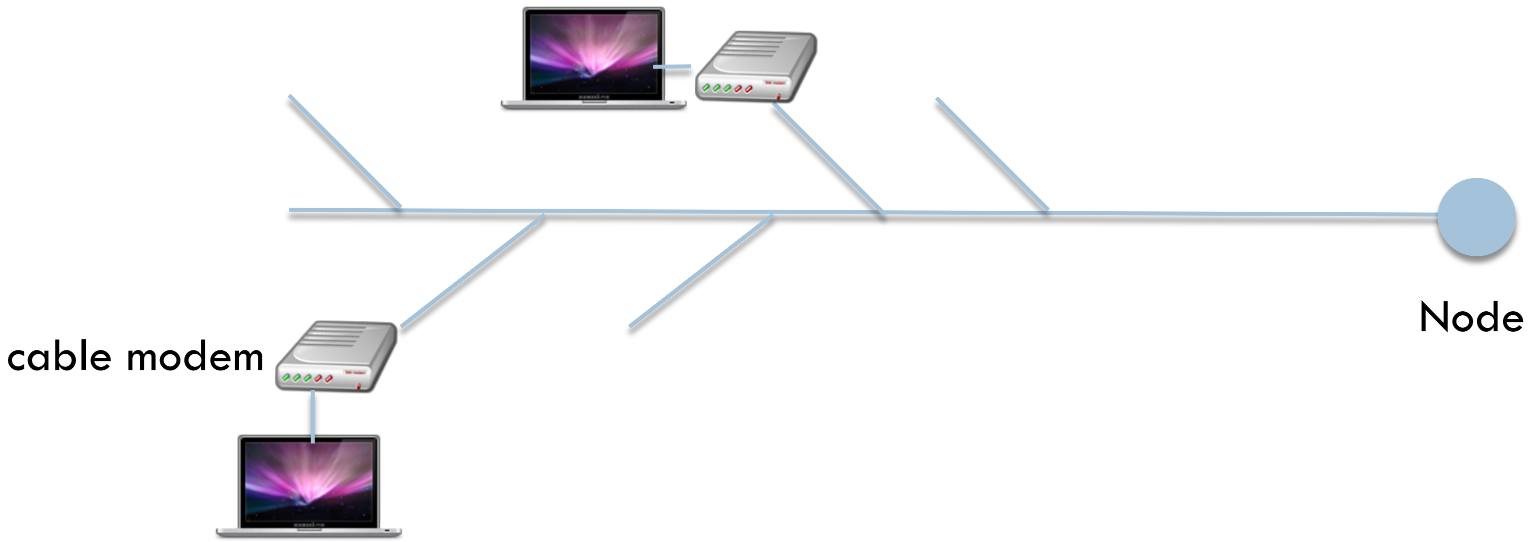
- Dial-up ISP phone number
- 10% residential users in US in 2008
- 56 Kbps

Access Networks and physical media
DSL : Digital subscriber line



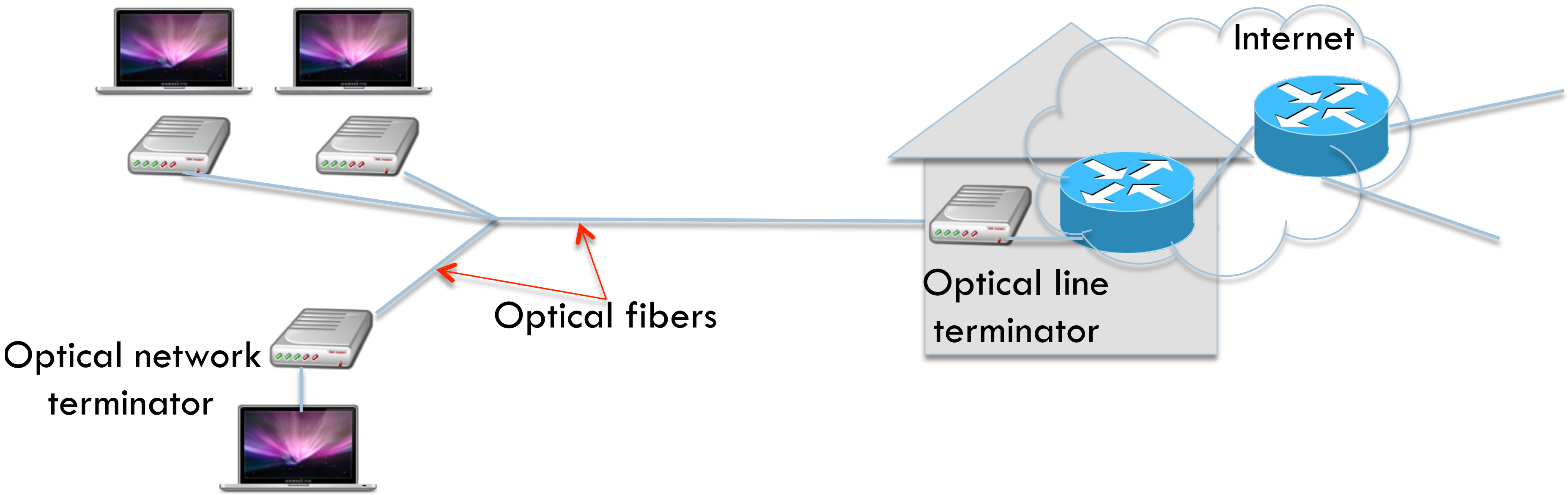
- Phone and Internet : frequency multiplexing
- Asymetric ADSL
- Rate :
  - upstream 1.6 to 20 Mbps
  - Downstream 12 to 55 Mbps
- Function of the distance between the home and the DSLAM

Access Networks and physical media Cable



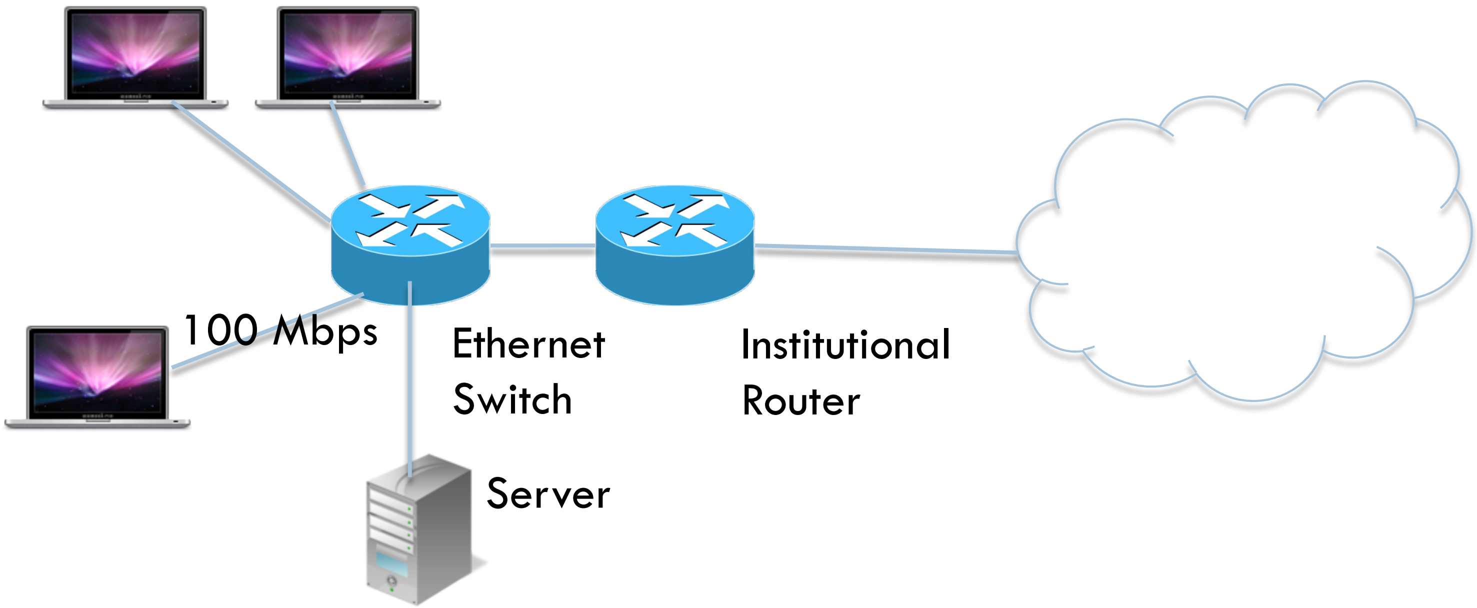
- Shared boradcast medium : variable rate
- Node rate ; Internet provider : satellite, fiber, etc
- Usage rate : number of active users
- Usage type : Download, surfing

Access Networks and physical media FTTH



- Higher transmission rate
- Direct or shared fiber
- Active or passive optical networks

Access Networks and physical media Ethernet



- 100 Mbps up to 10 Gbps

Access Networks and physical media WiFi

- IEEE 802.11 a,b,d,g,e,p
- Up to 54 Mbps
- 2.4, 5.9 GHz
- Access point

ESIEE ENGINEERING

Access Networks and physical media Wide Area Wireless access

- Cellular phone infrastructure
- Up to 1 Mbps
- GPRS -> Edge -> 3G -> LTE

Access Networks and physical media
Wimax

- Killer technology or Killed technology
- IEEE 802.16
- Tens of kilometers
- 5 to 10 Mbps

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

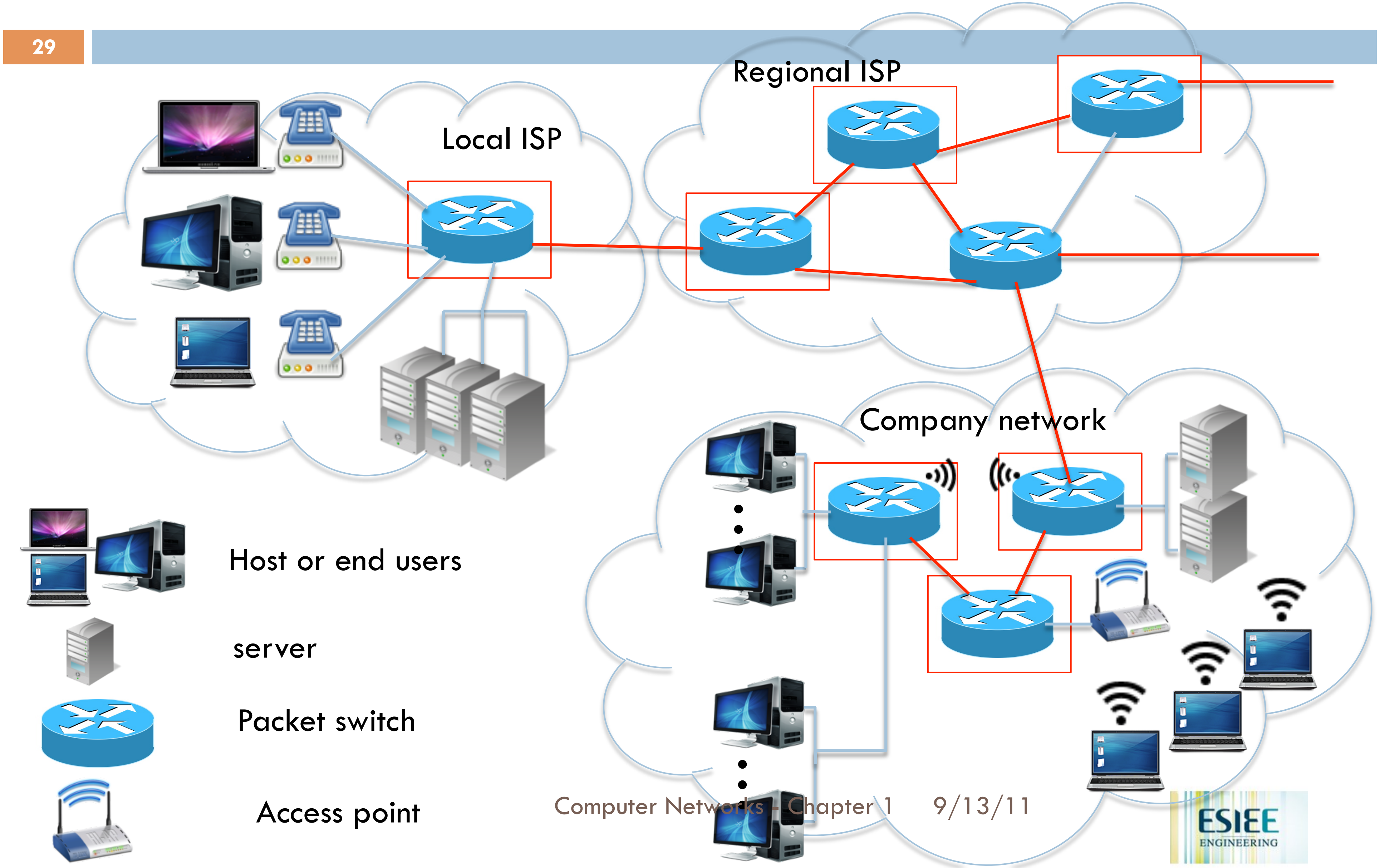
1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

Network Core



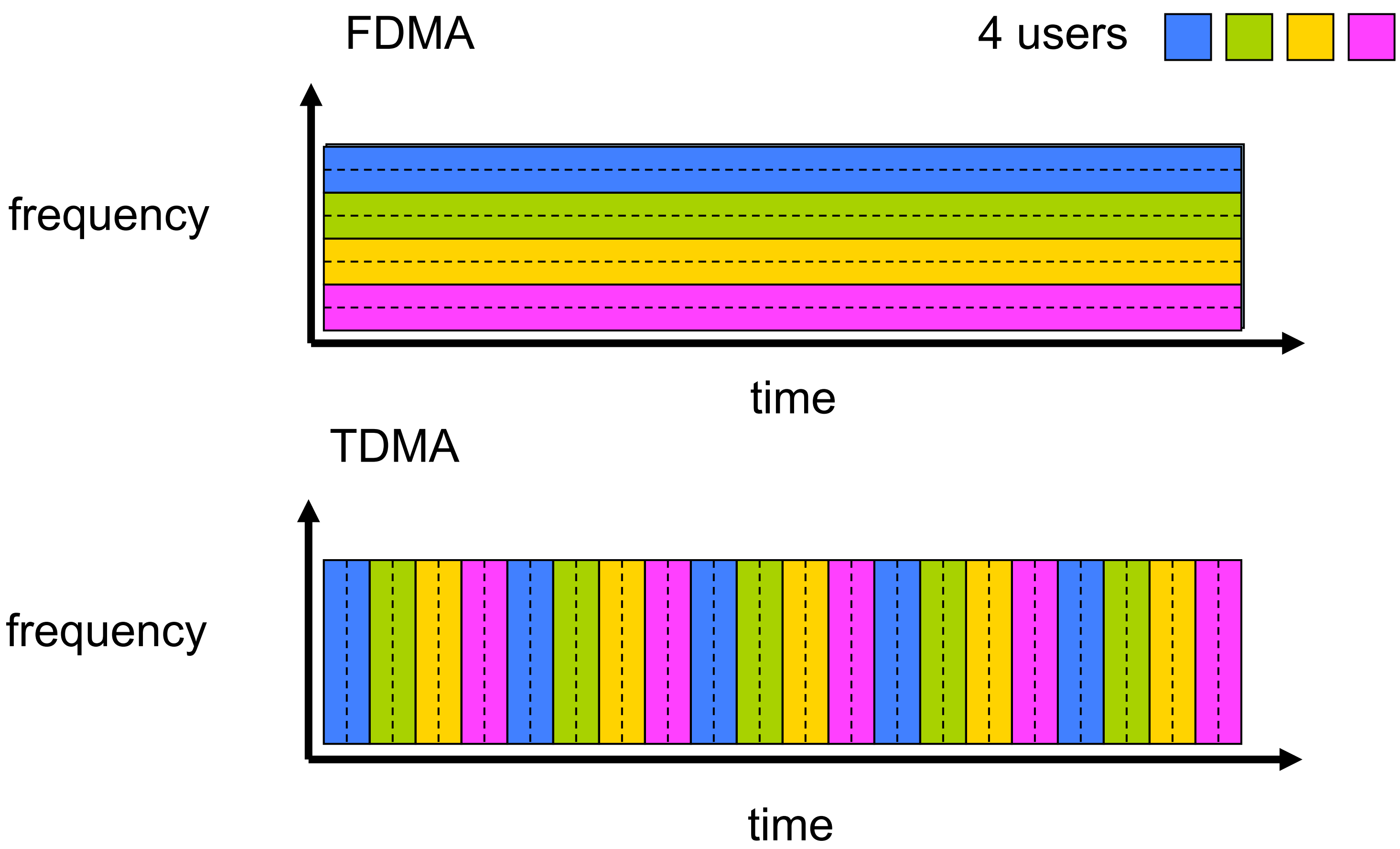
Network Core

- Circuit switching
  - Reserve «ressource»: setup required
  - Link transmission rate : guaranteed performance
  - e.g. telephony, fax, radio, tv
- Packet switching
  - Do not reserve
  - Use the ressource on demand
  - Queue, delay, best effort
  - e.g. Today's internet

Network Core: Circuit Switching

- network resources (e.g., bandwidth or time) divided into "pieces"
  - pieces allocated to calls
  - resource piece idle if not used by owning call (no sharing)
- dividing link bandwidth into "pieces"
  - Frequency division
  - Time division
- Silent Slots

Network Core: TDMA, FDMA



Example

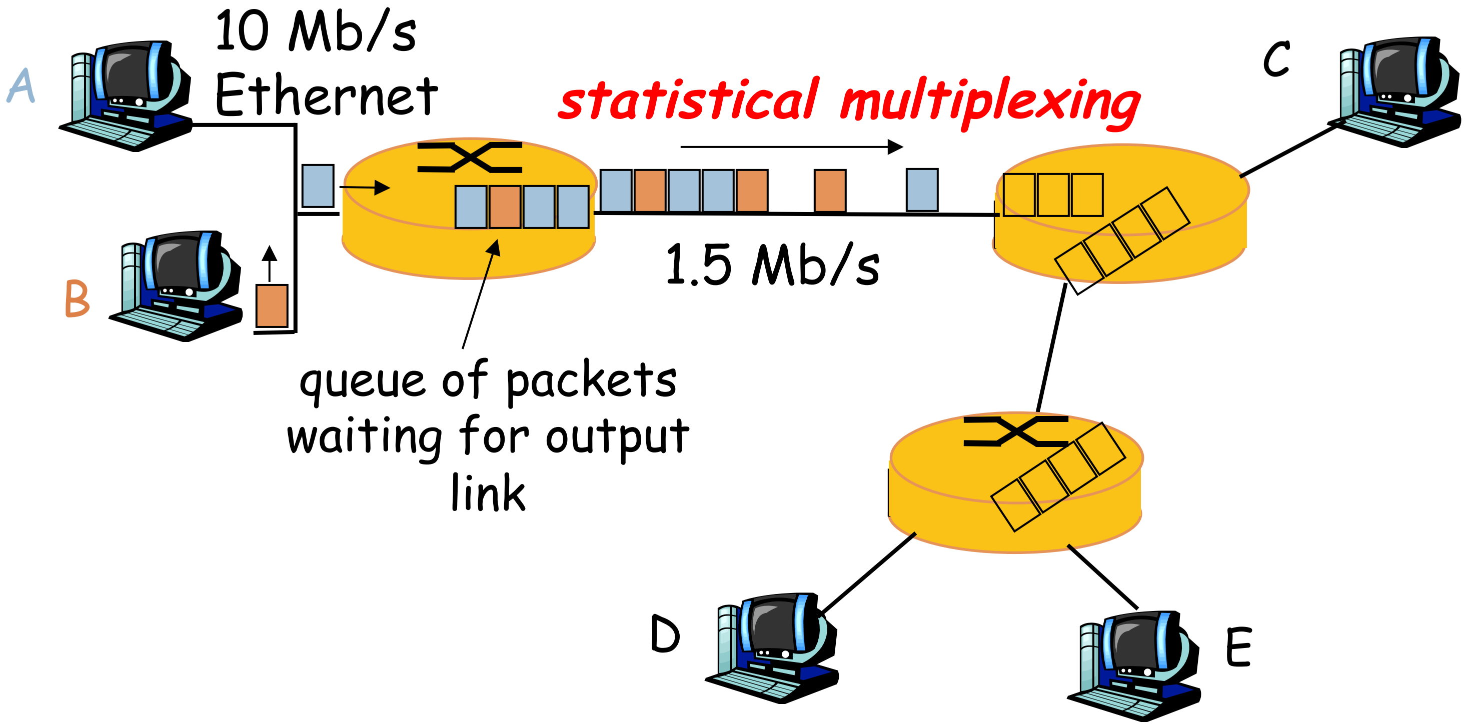
- How long does it take to send a file of 640,000 bits from host A to host B over a circuit-switched network?
  - All links are 1.536 Mbps
  - Each link uses TDMA with 24 slots
  - 500 msec to establish end-to-end circuit

Work it out!

Network Core: Packet switching

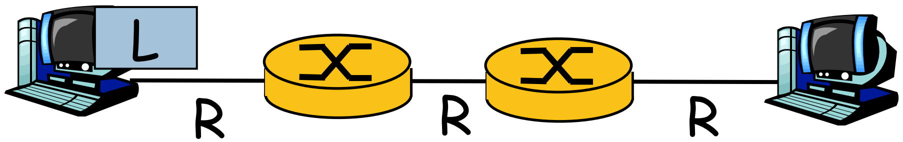
- each end-end data stream divided into packets
- user A, B packets share network resources
- each packet uses full link bandwidth
- resources used as needed
- congestion: packets queue, wait for link use
- store and forward: packets move one hop at a time
  - Node receives complete packet before forwarding

Packet Switching: Statistical Multiplexing



Sequence of A & B packets does not have fixed pattern ➡ ***statistical multiplexing***.

Packet-switching: store-and-forward



- takes L/R seconds to transmit (push out) packet of L bits on to link at R bps
- *store and forward:* entire packet must arrive at router before it can be transmitted on next link
- delay = 3L/R (assuming zero propagation delay)

Example:

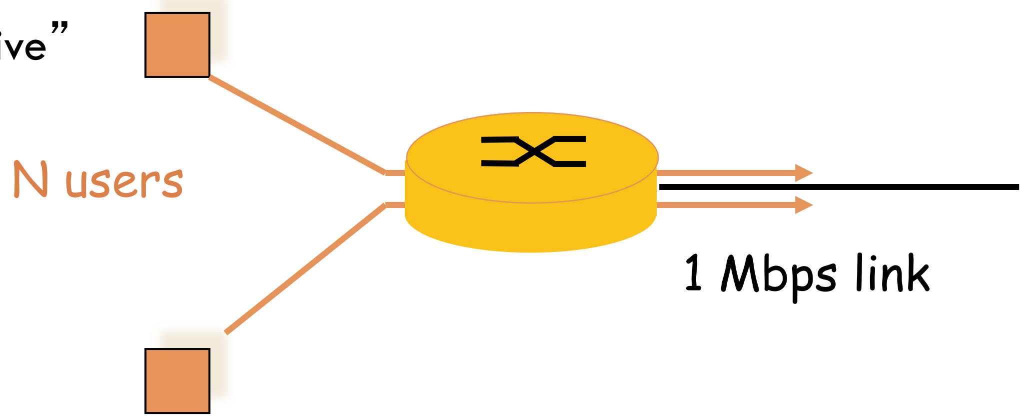
- L = 7.5 Mbits
- R = 1.5 Mbps
- transmission delay = 15 sec

more on delay shortly …

Packet switching versus circuit switching

Packet switching allows more users to use network!

- 1 Mb/s link
- each user:
  - 100 kb/s when "active"
  - active 10% of time



- circuit-switching:
  - 10 users
- packet switching:
  - with 35 users, probability > 10 active at same time is less than .0004

Packet switching versus circuit switching

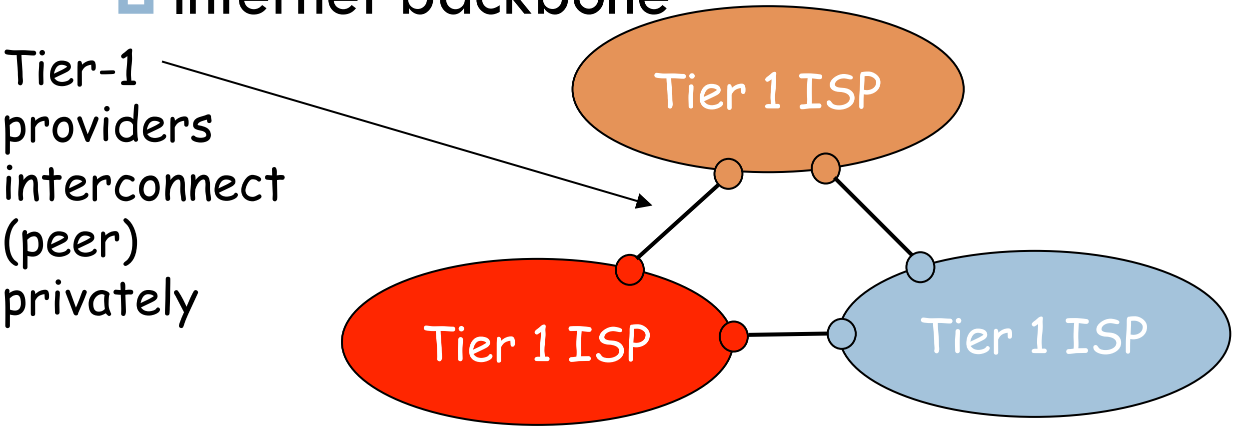
- Great for bursty data
  - resource sharing
  - simpler, no call setup
- Excessive congestion: packet delay and loss
  - protocols needed for reliable data transfer, congestion control

Packet switching: how packet knows its way ?

- Routing mechanism
- Forwarding tables
- …

Internet structure: network of networks

- roughly hierarchical
- at center: "tier-1" ISPs (e.g., Verizon, Sprint, AT&T, Cable and Wireless), national/international coverage
  - treat each other as equals
  - Internet backbone

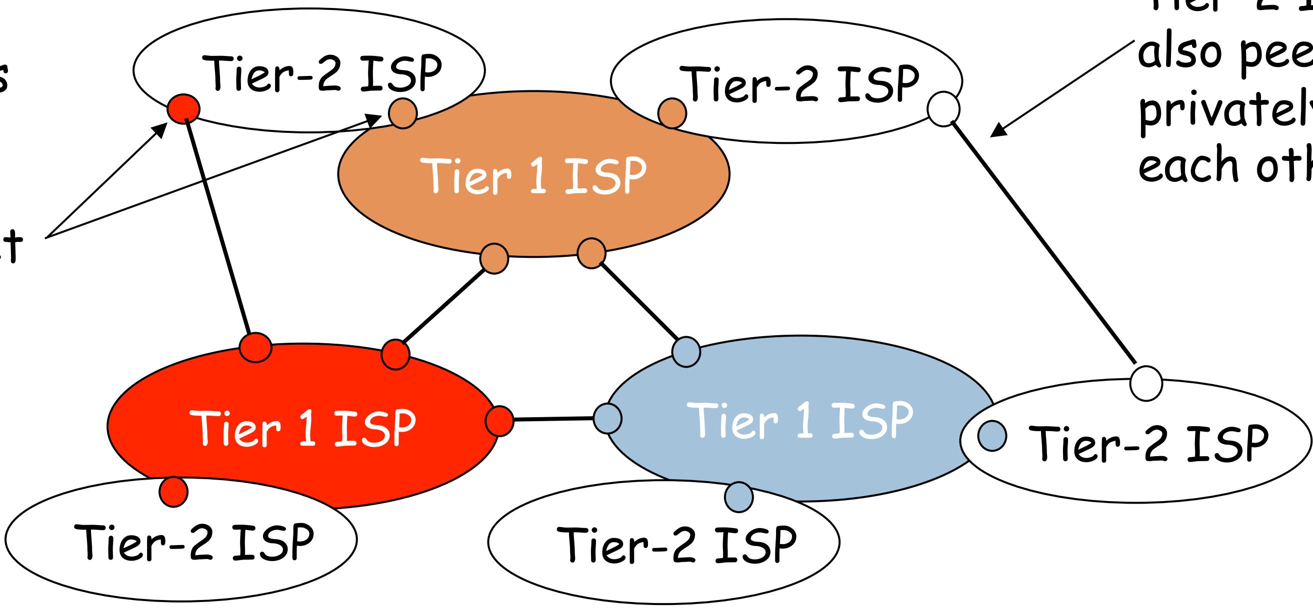


Internet structure: network of networks

- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

Tier-2 ISP pays tier-1 ISP for connectivity to rest of Internet

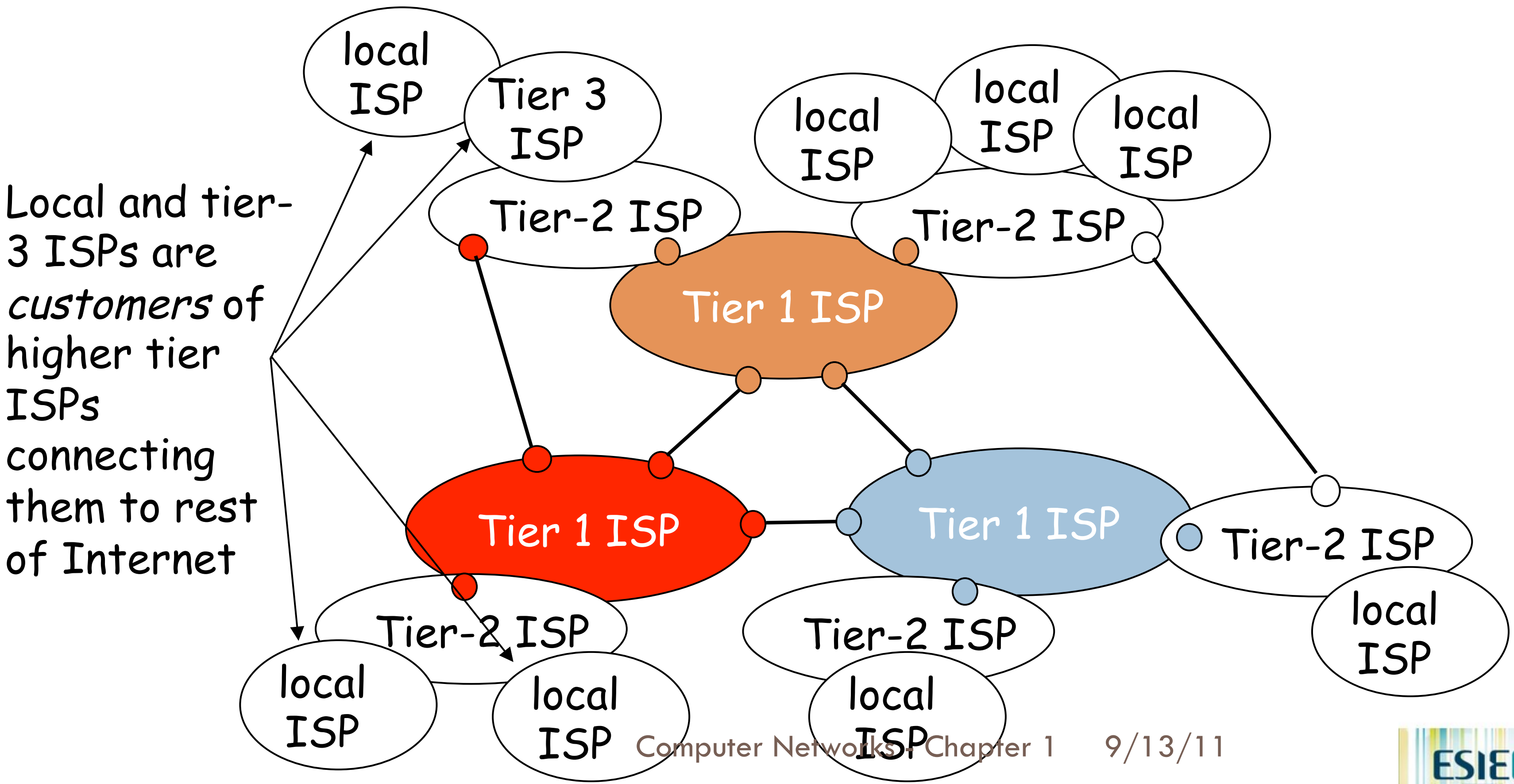
- tier-2 ISP is *customer* of tier-1 provider



Tier-2 ISPs also peer privately with each other.

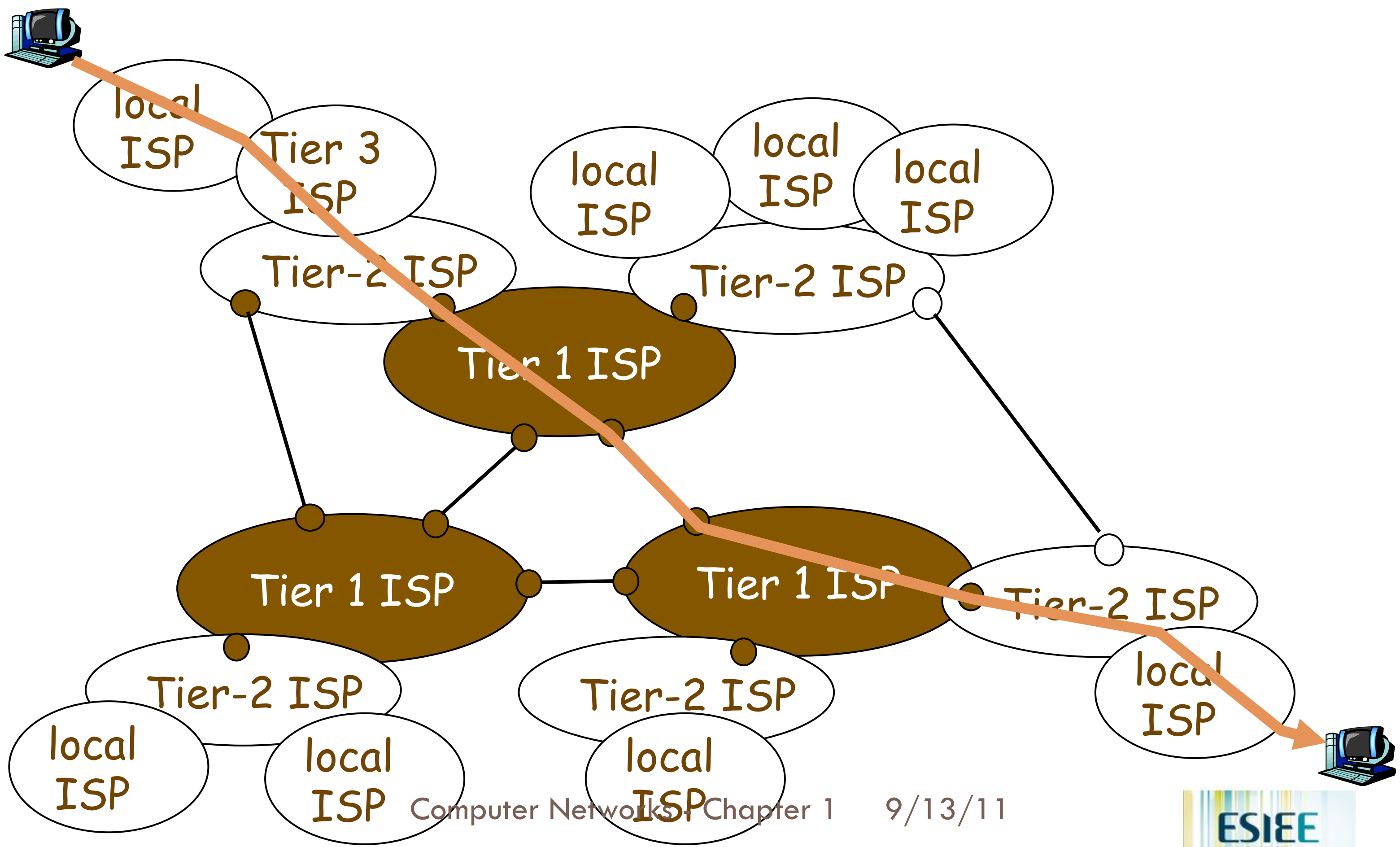
Internet structure: network of networks

- "Tier-3" ISPs and local ISPs
  - last hop ("access") network (closest to end systems)



Internet structure: network of networks

- a packet passes through many networks!



Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

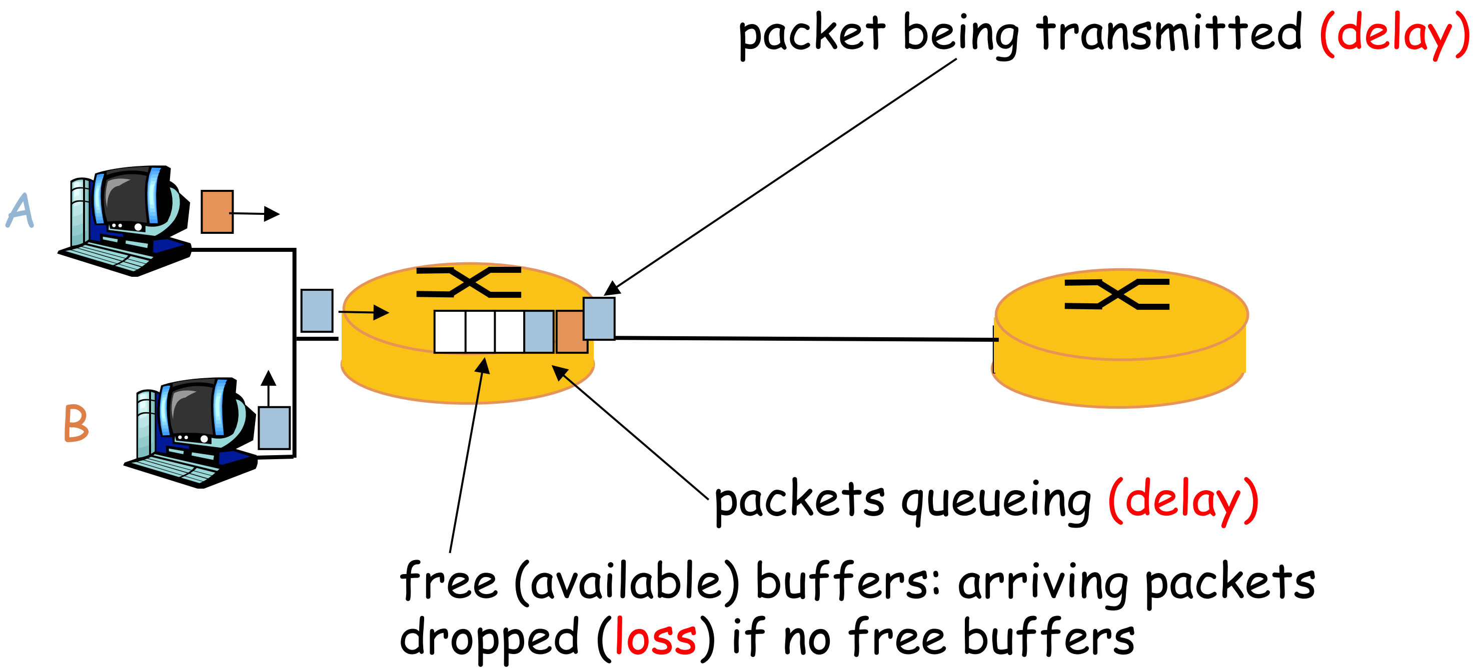
1.6 Networks under attack: security

1.7 History

How do loss and delay occur?

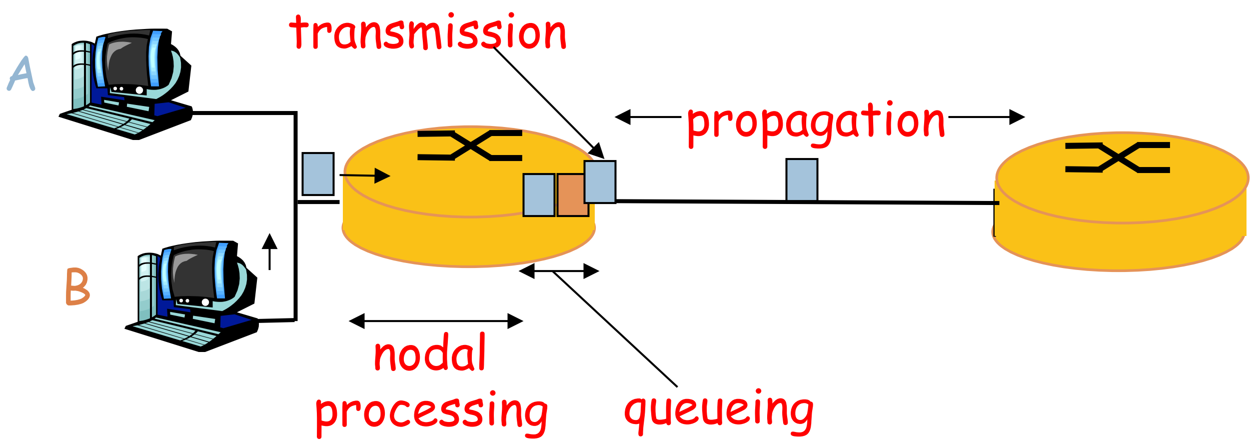
packets *queue* in router buffers

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



Four sources of packet delay

- 1. nodal processing:
  - check bit errors
  - determine output link
- 2. queueing
  - time waiting at output link for transmission
  - depends on congestion level of router



Delay in packet-switched networks

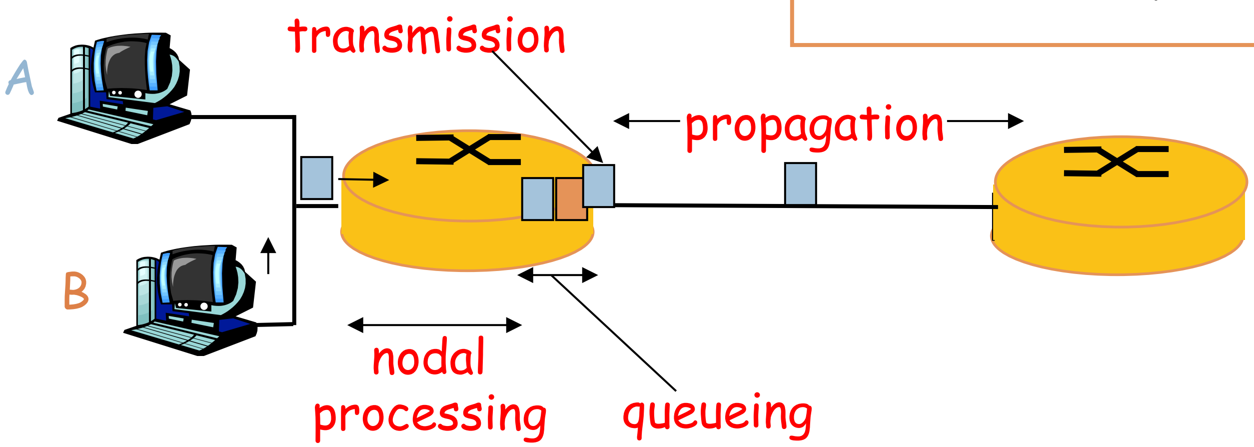
3. Transmission delay:

- R=link bandwidth (bps)
- L=packet length (bits)
- time to send bits into link = L/R

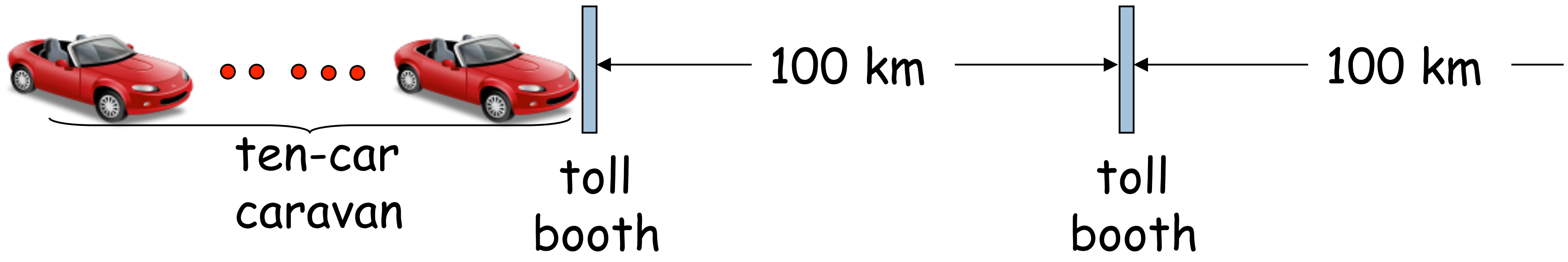
4. Propagation delay:

- d = length of physical link
- s = propagation speed in medium (~$2x10^8$ m/sec)
- propagation delay = d/s

Note: s and R are *very* different quantities!

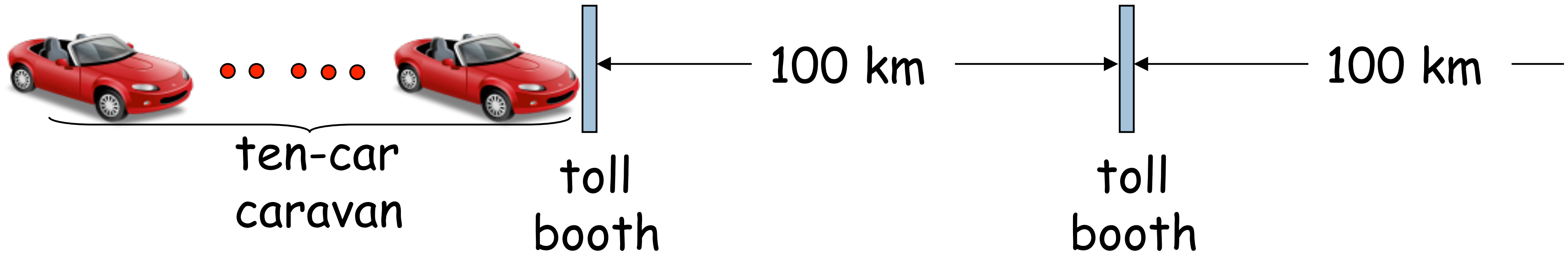


Caravan analogy



- Cars "propagate" at 100 km/hr
- Toll booth takes 12 sec to service a car (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

Caravan analogy (more)



- Cars now "propagate" at 1000 km/hr
- Toll booth now takes 1 min to service a car
- Q: Will cars arrive to 2nd booth before all cars serviced at 1st booth?
- Yes! After 7 min, 1st car at 2nd booth and 3 cars still at 1st booth.
- 1st bit of packet can arrive at 2nd router before packet is fully transmitted at 1st router!

Nodal delay

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

- d_{proc} = processing delay
  - typically a few microsecs or less
- d_{queue} = queuing delay
  - depends on congestion
- d_{trans} = transmission delay
  - = L/R, significant for low-speed links
- d_{prop} = propagation delay
  - a few microsecs to hundreds of msecs

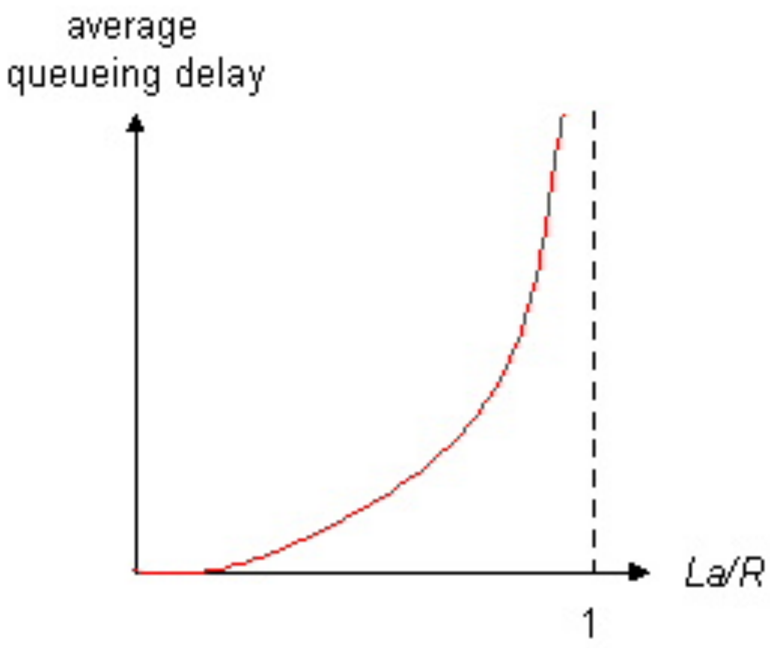
Packet loss

- queue (buffer) preceding link in buffer has finite capacity
- when packet arrives to full queue, packet is dropped (lost)
- lost packet may be retransmitted by previous node, by source end system, or not retransmitted at all

Queueing delay (revisited)

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

traffic intensity = La/R

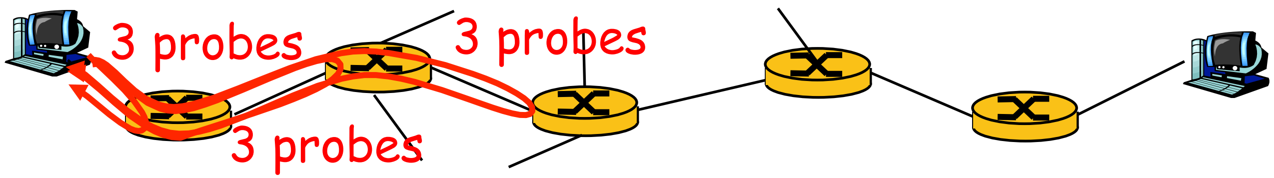


- La/R ~ 0: average queueing delay small
- La/R -> 1: delays become large
- La/R > 1: more "work" arriving than can be serviced, average delay infinite!

ESIEE ENGINEERING

"Real" Internet delays and routes

- What do "real" Internet delay & loss look like?
- **Traceroute** program: provides delay measurement from source to router along end-end Internet path towards destination. For all *i:*
  - sends three packets that will reach router *i* on path towards destination
  - router *i* will return packets to sender
  - sender times interval between transmission and reply.
  - "Tracert" in a windows environment



ESIEE ENGINEERING

"Real" Internet delays and routes

traceroute: gaia.cs.umass.edu to www.eurecom.fr

Three delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

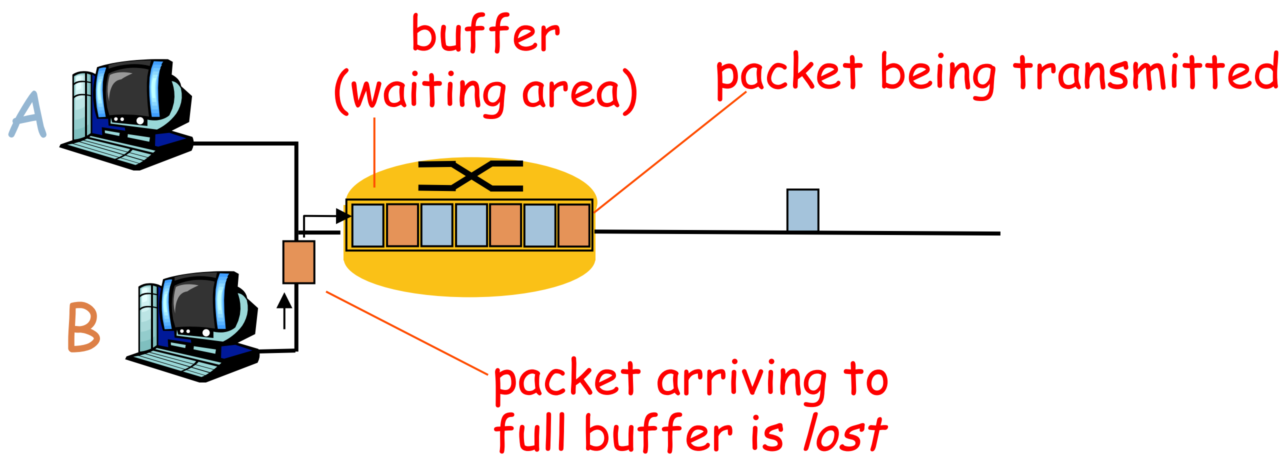
1 cs-gw (128.119.240.254) 1 ms 1 ms 2 ms
2 border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145) 1 ms 1 ms 2 ms
3 cht-vbns.gw.umass.edu (128.119.3.130) 6 ms 5 ms 5 ms
4 jn1-at1-0-0-19.wor.vbns.net (204.147.132.129) 16 ms 11 ms 13 ms
5 jn1-so7-0-0-0.wae.vbns.net (204.147.136.136) 21 ms 18 ms 18 ms
6 abilene-vbns.abilene.ucaid.edu (198.32.11.9) 22 ms 18 ms 22 ms
7 nycm-wash.abilene.ucaid.edu (198.32.8.46) 22 ms 22 ms 22 ms
8 62.40.103.253 (62.40.103.253) 104 ms 109 ms 106 ms
9 de2-1.de1.de.geant.net (62.40.96.129) 109 ms 102 ms 104 ms
10 de.fr1.fr.geant.net (62.40.96.50) 113 ms 121 ms 114 ms
11 renater-gw.fr1.fr.geant.net (62.40.103.54) 112 ms 114 ms 112 ms
12 nio-n2.cssi.renater.fr (193.51.206.13) 111 ms 114 ms 116 ms
13 nice.cssi.renater.fr (195.220.98.102) 123 ms 125 ms 124 ms
14 r3t2-nice.cssi.renater.fr (195.220.98.110) 126 ms 126 ms 124 ms
15 eurecom-valbonne.r3t2.ft.net (193.48.50.54) 135 ms 128 ms 133 ms
16 194.214.211.25 (194.214.211.25) 126 ms 128 ms 126 ms
17 * * *
18 * * *
19 fantasia.eurecom.fr (193.55.113.142) 132 ms 128 ms 136 ms

trans-oceanic link

* means no response (probe lost, router not replying)

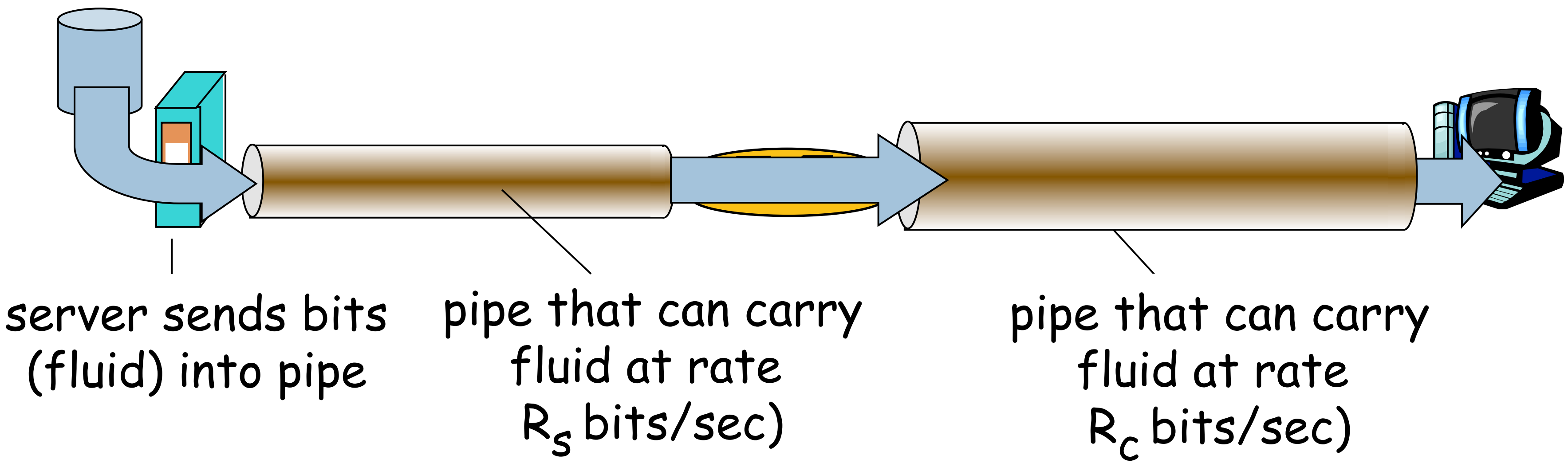
Packet loss

- Queue preceding link in buffer has finite capacity
- packet arriving to full queue dropped
- lost packet may be retransmitted by previous node, by source end system, or not at all



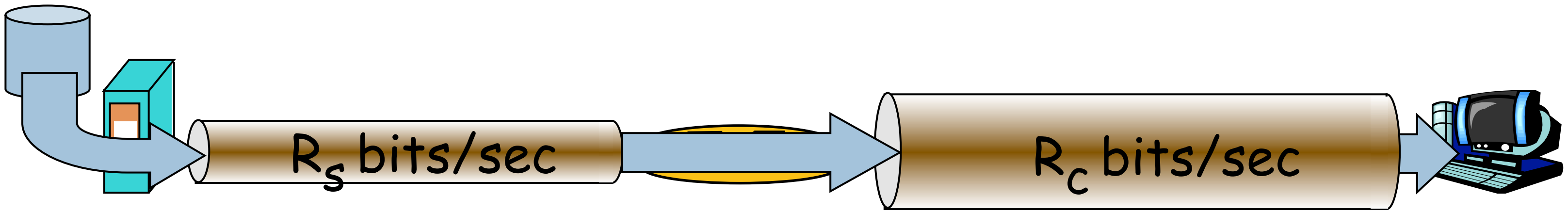
Throughput

- *throughput:* rate (bits/time unit) at which bits transferred between sender/receiver
  - *instantaneous:* rate at given point in time
  - *average:* rate over longer period of time

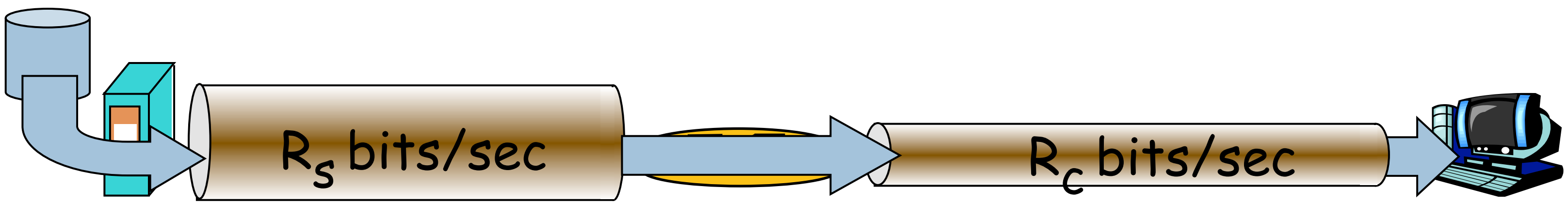


Throughput (more)

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



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

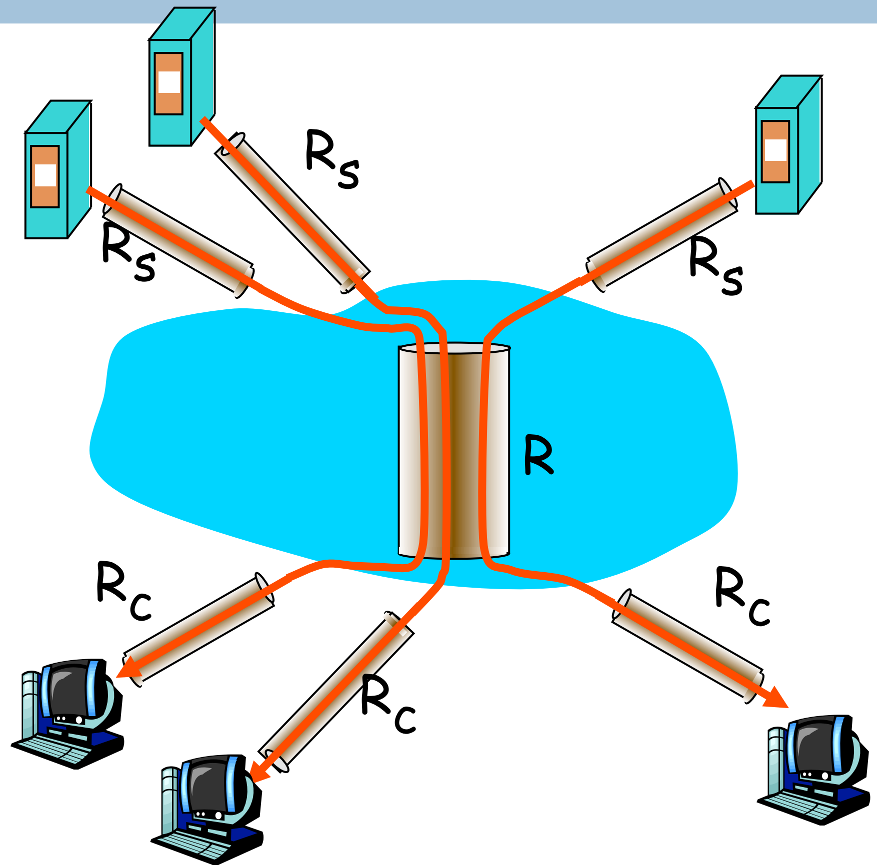


bottleneck link

link on end-end path that constrains end-end throughput

Throughput: Internet scenario

- per-connection end-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

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

Protocol "Layers"

Networks are complex!

- many "pieces":
  - hosts
  - routers
  - links of various media
  - applications
  - protocols
  - hardware, software

Question:

Is there any hope of *organizing* structure of network?

Or at least our discussion of networks?

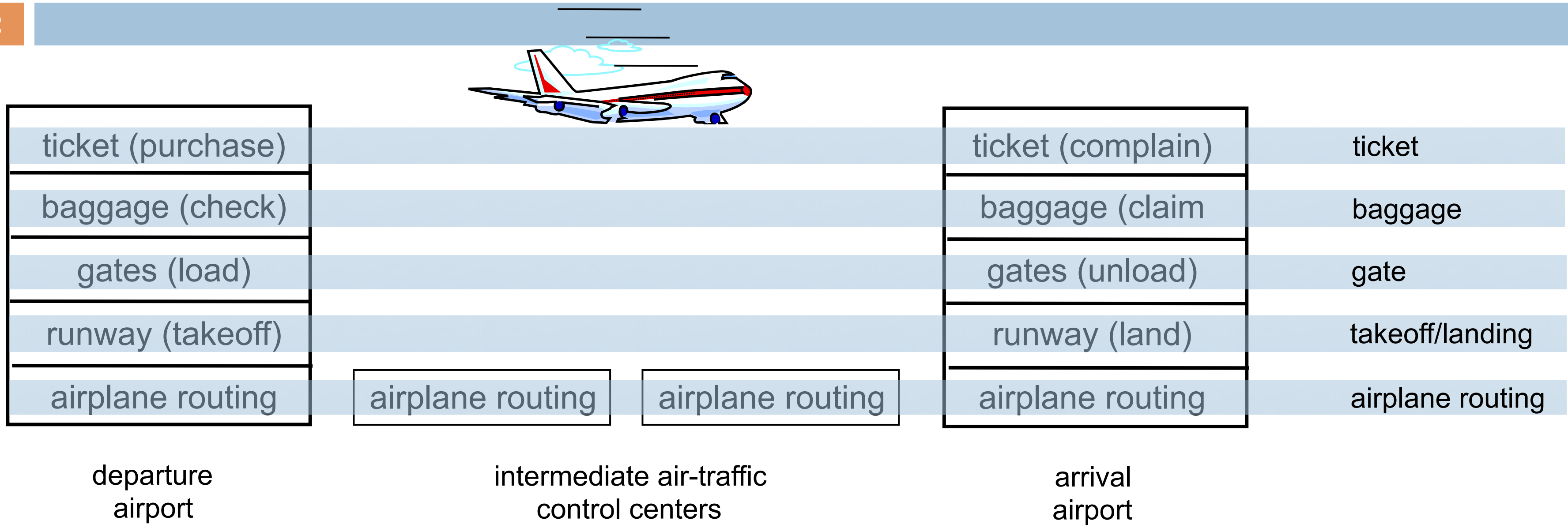
Organization of air travel

ticket (purchase)	ticket (complain)
baggage (check)	baggage (claim)
gates (load)	gates (unload)
runway takeoff	runway landing
airplane routing	airplane routing

airplane routing

- a series of steps

Layering of airline functionality



Layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

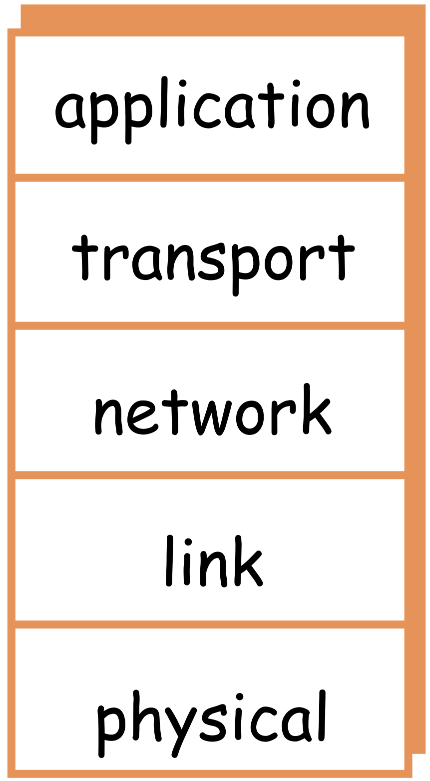
Why layering?

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., change in gate procedure doesn't affect rest of system

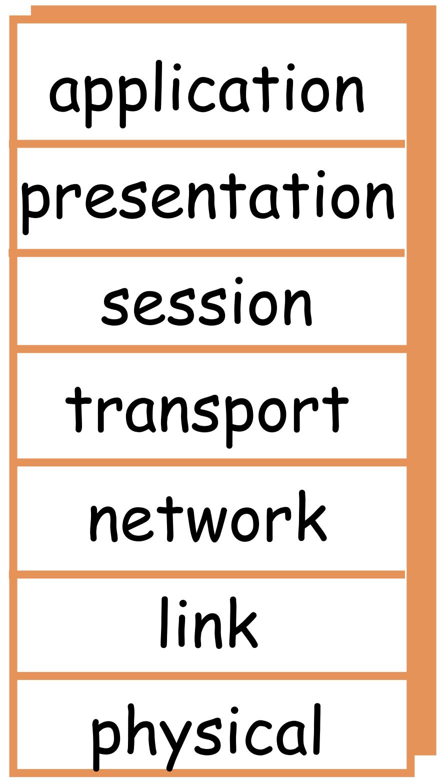
Internet protocol stack

- application: supporting network applications
  - FTP, SMTP, HTTP
- transport: process-process data transfer
  - TCP, UDP
- network: routing of datagrams from source to destination
  - IP, routing protocols
- link: data transfer between neighboring network elements
  - PPP, Ethernet
- physical: bits "on the wire"

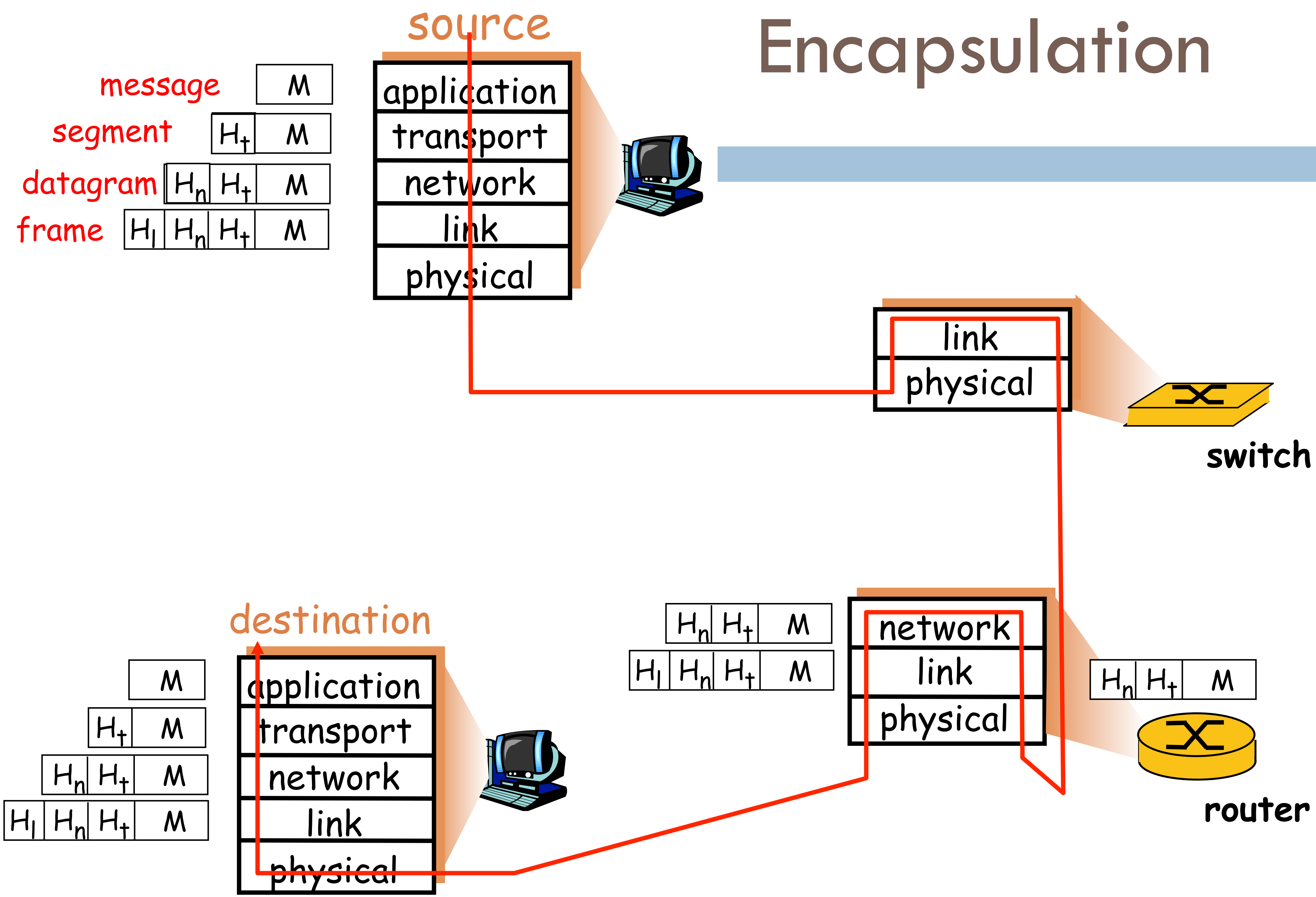


ISO/OSI reference model

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



Encapsulation



Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

Network Security

- The field of network security is about:
  - how bad guys can attack computer networks
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks
- Internet not originally designed with (much) security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network"
  - Internet protocol designers playing "catch-up"
  - Security considerations in all layers!

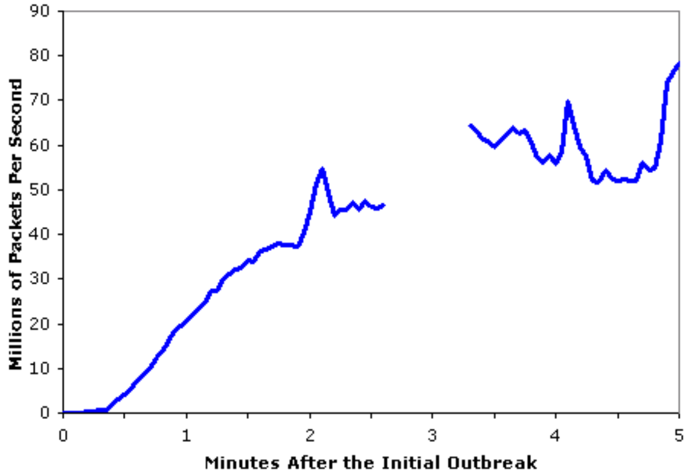
Bad guys can put malware into hosts via Internet

- Malware can get in host from a virus, worm, or trojan horse.
- Spyware malware can record keystrokes, web sites visited, upload info to collection site.
- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.
- Malware is often self-replicating: from an infected host, seeks entry into other hosts

Bad guys can put malware into hosts via Internet

- Trojan horse
  - Hidden part of some otherwise useful software
  - Today often on a Web page (Active-X, plugin)
- Virus
  - infection by receiving object (e.g., e-mail attachment), actively executing
  - self-replicating: propagate itself to other hosts, users
- Worm:
  - infection by passively receiving object that gets itself executed
  - self- replicating: propagates to other hosts, users

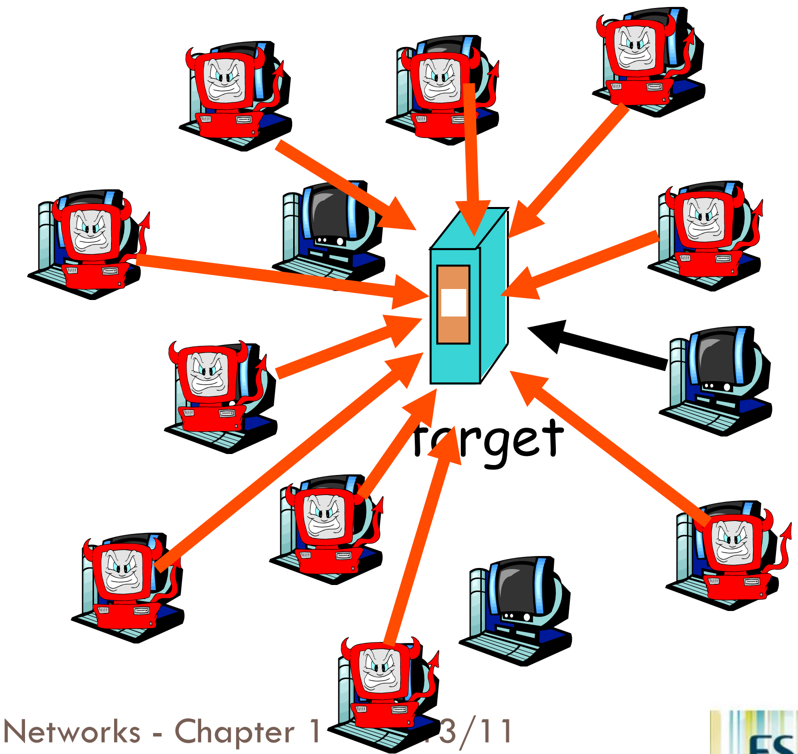
Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)



Bad guys can attack servers and network infrastructure

- Denial of service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts

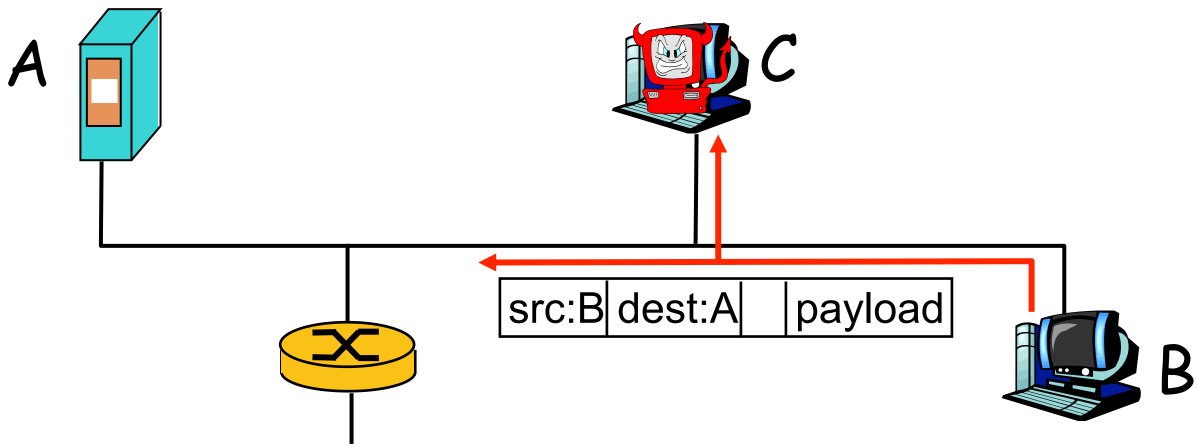


ESIEE ENGINEERING

The bad guys can sniff packets

Packet sniffing:

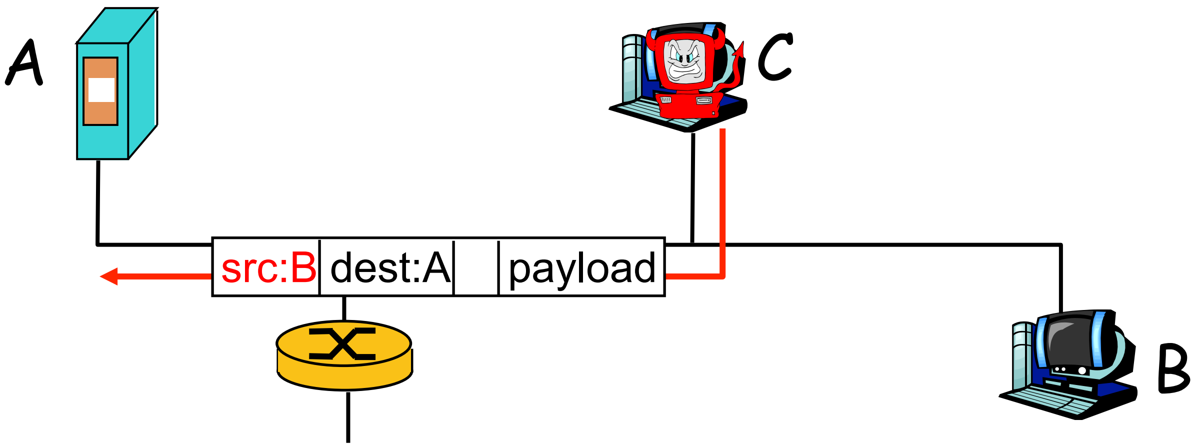
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- Wireshark software used for end-of-chapter labs is a (free) packet-sniffer

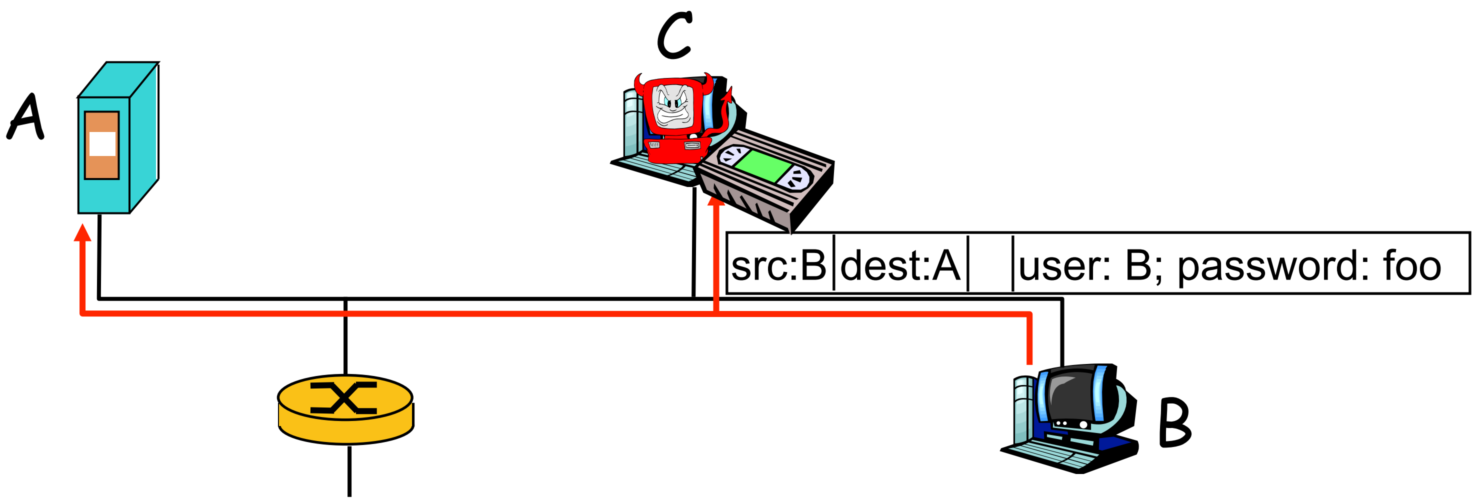
The bad guys can use false source addresses

- *IP spoofing:* send packet with false source address



The bad guys can record and playback

- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view



Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

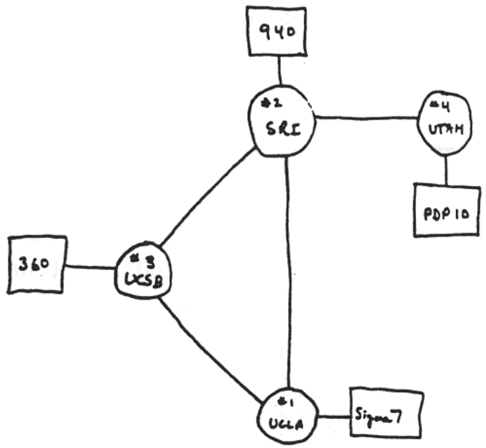
1.6 Networks under attack: security

1.7 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 demonstration
  - 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
- ate70'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

2007:

- ~500 million hosts
- Voice, Video over IP
- P2P applications: BitTorrent (file sharing) Skype (VoIP), PPLive (video)
- more applications: YouTube, gaming
- wireless, mobility

Introduction: Summary

<u>Covered a "ton" of material!</u>

- Internet overview
- what's a protocol?
- network edge, core, access network
  - packet-switching versus circuit-switching
  - Internet structure
- performance: loss, delay, throughput
- layering, service models
- security
- history

<u>You now have:</u>

- context, overview, "feel" of networking
- more depth, detail *to follow!*