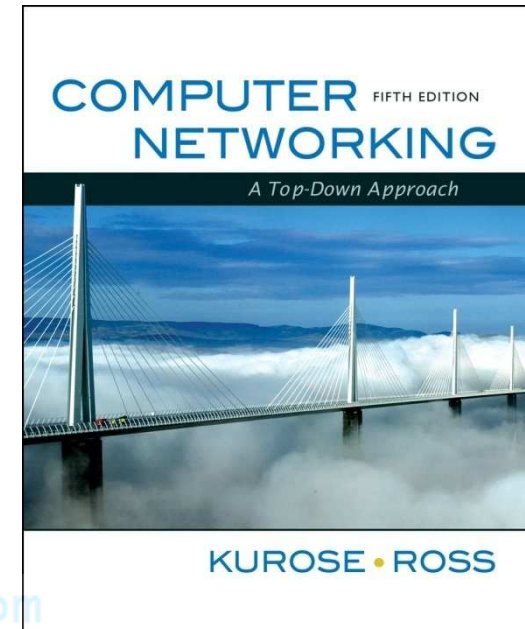


# Chapter 1

## Introduction



### A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- ❑ If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- ❑ If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2009  
J.F Kurose and K.W. Ross, All Rights Reserved

*Computer Networking:  
A Top Down Approach ,  
5<sup>th</sup> edition.*

*Jim Kurose, Keith Ross  
Addison-Wesley, April  
2009.*

# 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

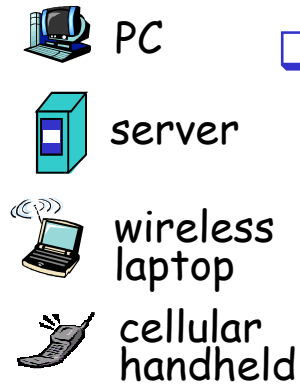
## 1.4 Delay, loss and throughput in packet-switched networks

## 1.5 Protocol layers, service models

## 1.6 Networks under attack: security

## 1.7 History

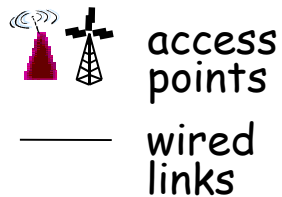
# What's the Internet: “nuts and bolts” view



- Hàng triệu thiết bị tính toán được nối mạng:  
*hosts = end systems*

- ❖ chạy các *ứng dụng mạng*

- *communication links*

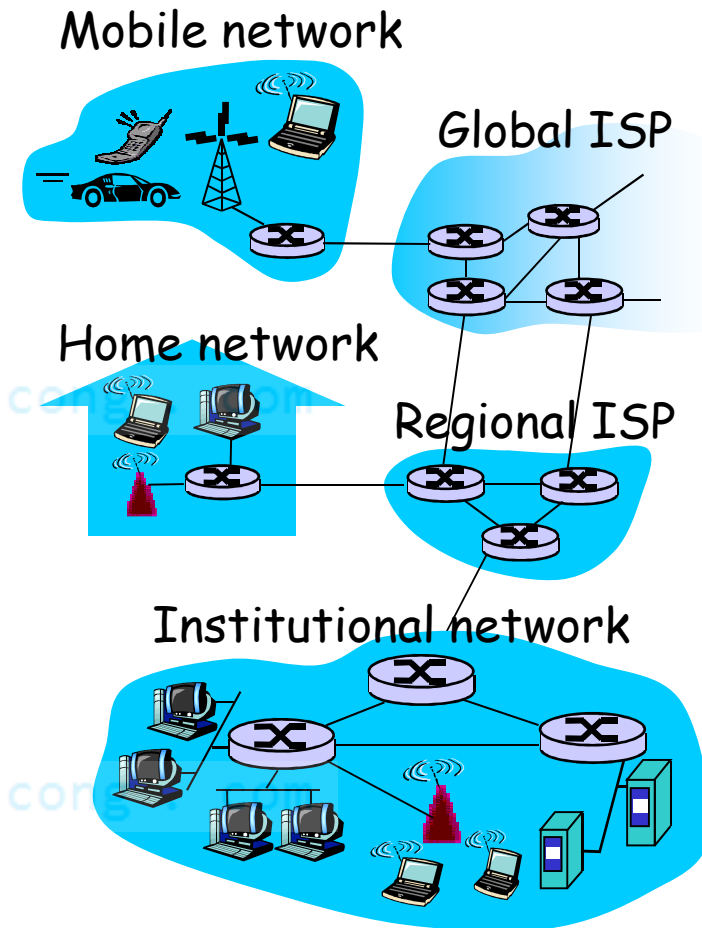


- ❖ fiber, copper, radio, satellite

- ❖ transmission rate = *bandwidth*



- *routers*: Chuyển các packets (gói tin)



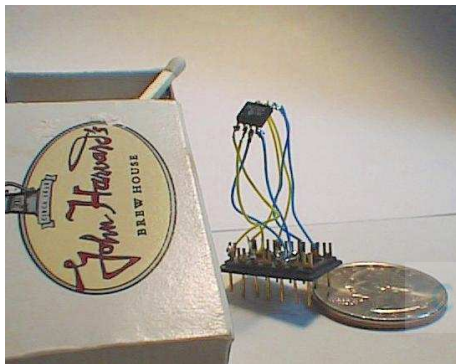
# “Cool” internet appliances



IP picture frame  
<http://www.ceiva.com/>



Web-enabled toaster +  
weather forecaster



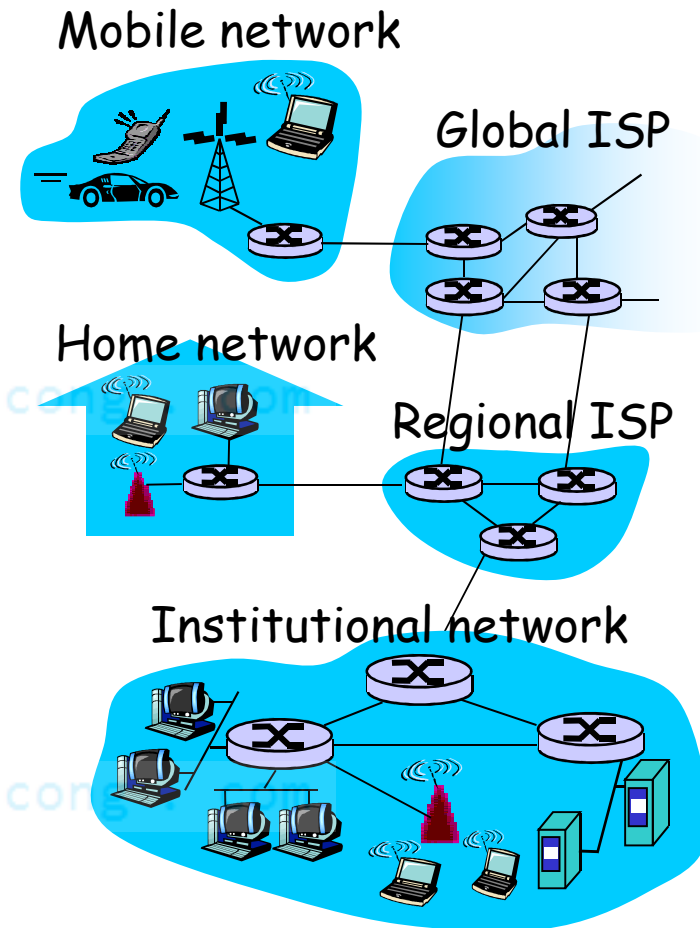
World's smallest web server  
<http://www-ccs.cs.umass.edu/~shri/iPic.html>



Internet phones

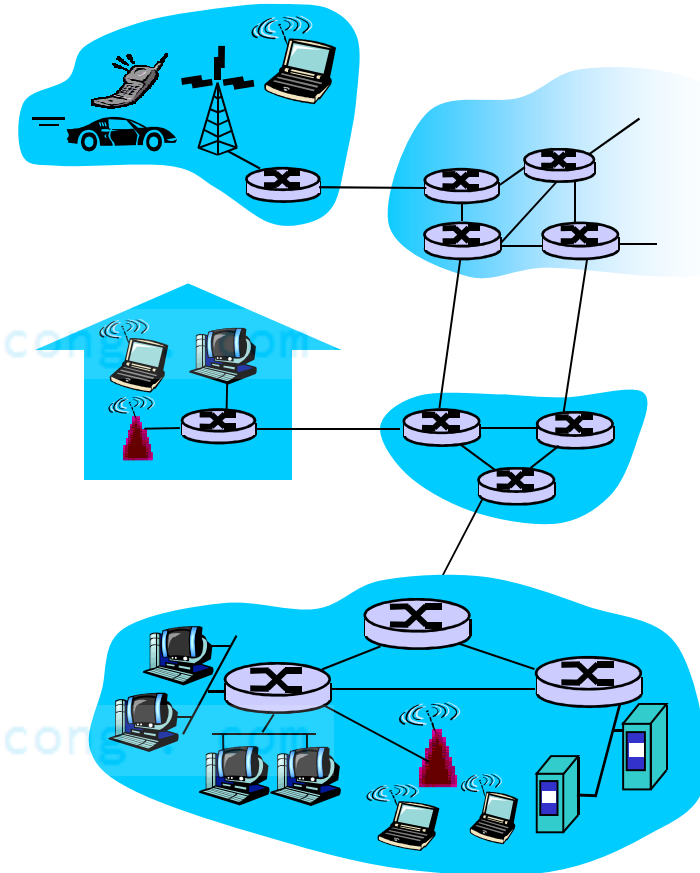
# What's the Internet: “nuts and bolts” view

- ❑ *protocols (giao thức)* điều khiển việc gửi/nhận các msg
  - ❖ e.g., TCP, IP, HTTP, Skype, Ethernet
- ❑ *Internet: “mạng của các mạng”*
  - ❖ loosely hierarchical
  - ❖ public Internet versus private intranet
- ❑ Các tiêu chuẩn Internet
  - ❖ RFC: Request for comments
  - ❖ IETF: Internet Engineering Task Force



# What's the Internet: a service view

- ❑ Hạ tầng truyền thông (communication *infrastructure*) cho phép các ứng dụng phân bố:
  - ❖ Web, VoIP, email, games, e-commerce, file sharing
- ❑ Các ứng dụng sử dụng các dịch vụ truyền thông (communication services)
  - ❖ Truyền dữ liệu bảo đảm từ máy nguồn đến máy đích
  - ❖ Truyền dữ liệu thường (không bảo đảm)



# What's a protocol?

## human protocols:

- ❑ “Mấy giờ rồi?”
  - ❑ “Cho tôi hỏi”
  - ❑ giới thiệu
- ... gửi đi một thông điệp nhất định
- ... một hành động nhất định được thực hiện khi nhận được thông điệp, hoặc khi có 1 sự kiện khác

## network protocols:

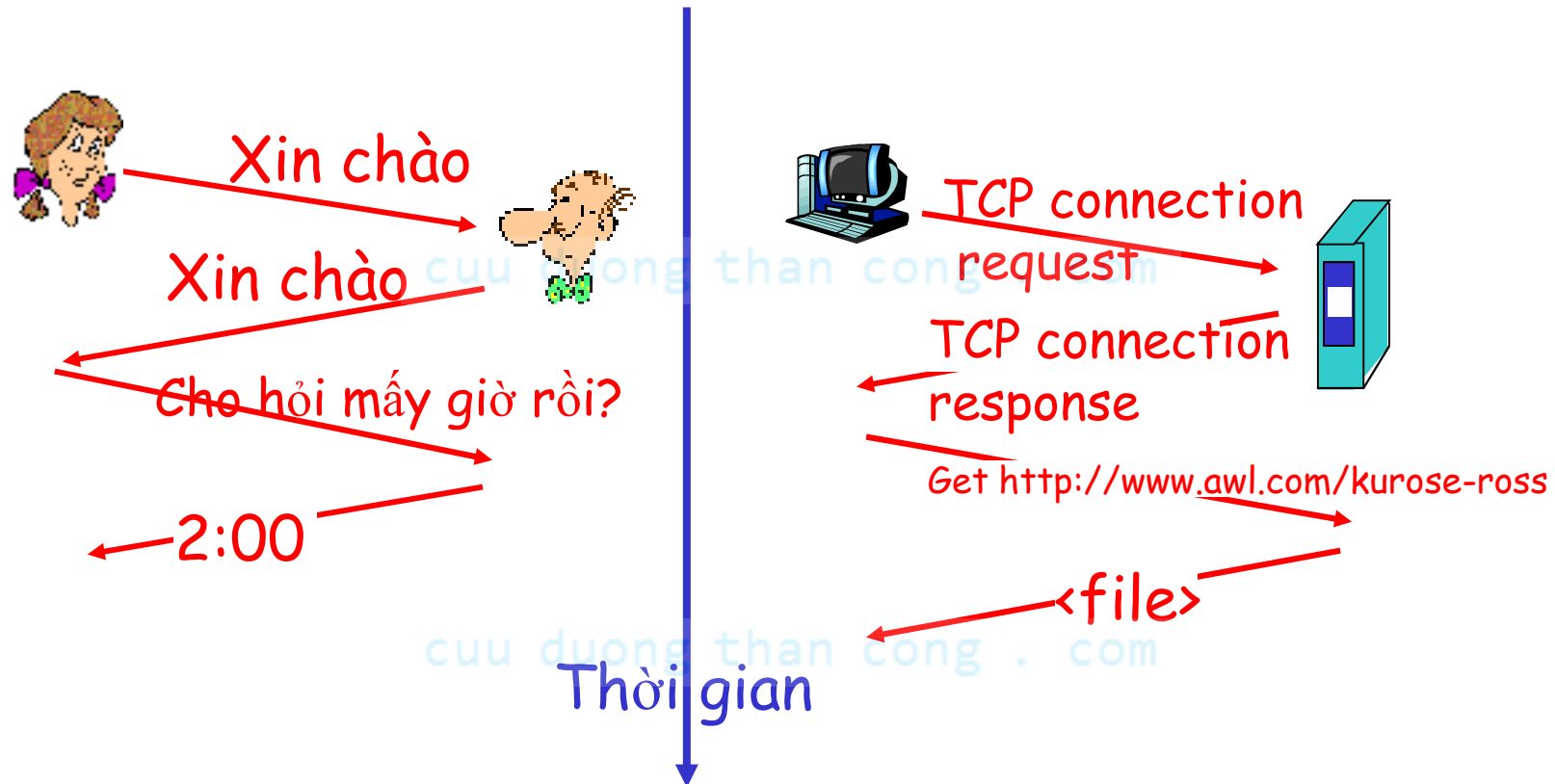
- ❑ Máy tính, ko phải người
- ❑ Tất cả các hoạt động truyền thông trên Internet phải tuân thủ các protocols

*protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt*



# What's a protocol?

a human protocol and a computer network protocol:



Q: Other human protocols?

# 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

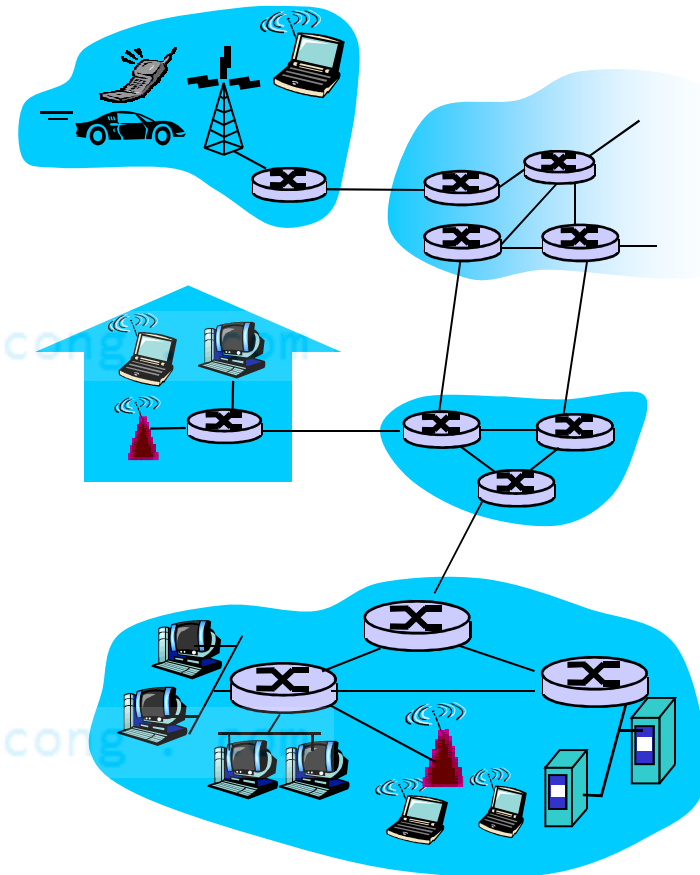
1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

# A closer look at network structure:

- ❑ **network edge:** ứng dụng và các máy tính (hosts)
- ❑ **access networks, physical media:** wired, wireless communication links
- ❑ **network core:**
  - ❖ interconnected routers
  - ❖ network of networks



# The network edge:

## □ end systems (hosts):

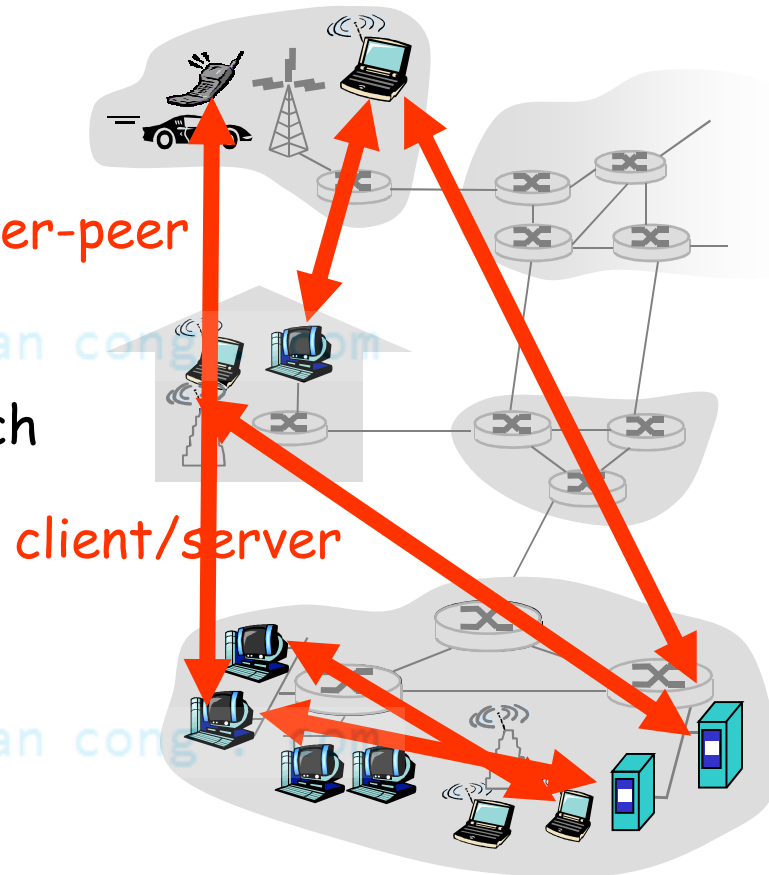
- ❖ Chạy các C trình ứng dụng
- ❖ e.g. Web, email
- ❖ ở “đường biên của mạng” **peer-peer**

## □ client/server model

- ❖ Client yêu cầu và nhận các dịch vụ từ các server
- ❖ e.g. Web browser/server; email client/server

## □ peer-peer model:

- ❖ Dùng ít hoặc ko dùng các server dành riêng
- ❖ e.g. Skype, BitTorrent



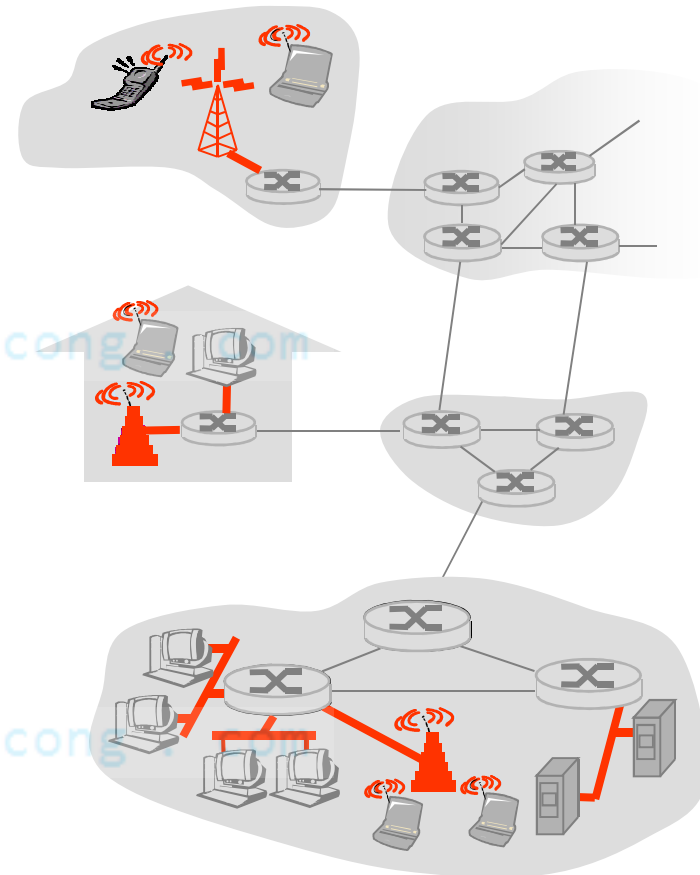
# Access networks and physical media

*Q: Kết nối các host vào các edge router ra sao?*

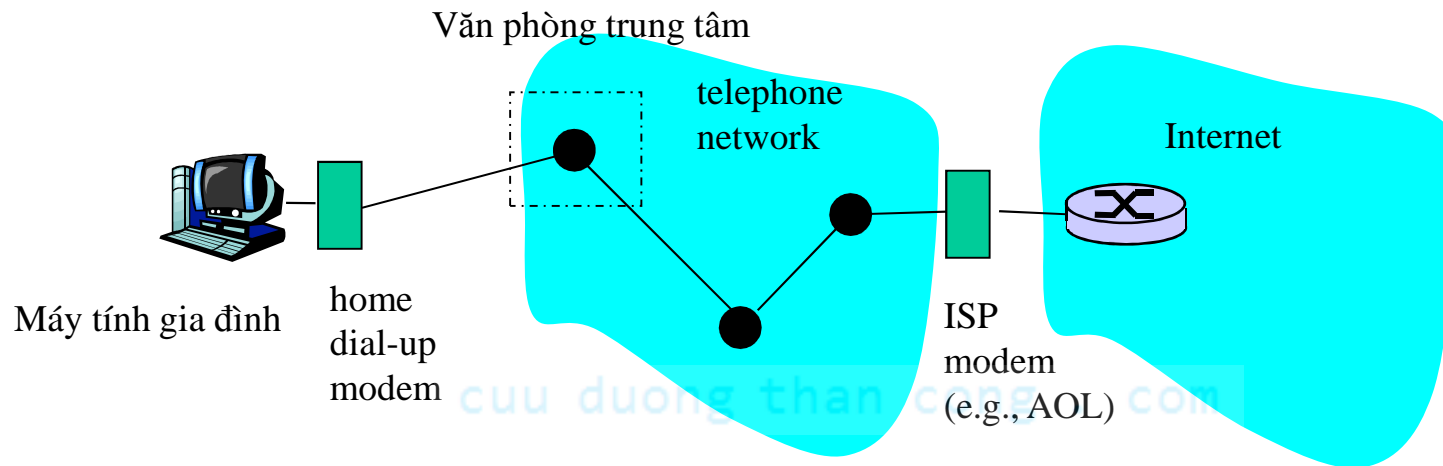
- ❑ Qua mạng truy cập thường trực
- ❑ Mạng truy cập của tổ chức (trường học, cty)
- ❑ Mạng truy cập không dây

*Nhớ :*

- ❑ Khả năng truyền (bandwidth, bits per second) của mạng truy cập?
- ❑ Dùng chung hay dành riêng?

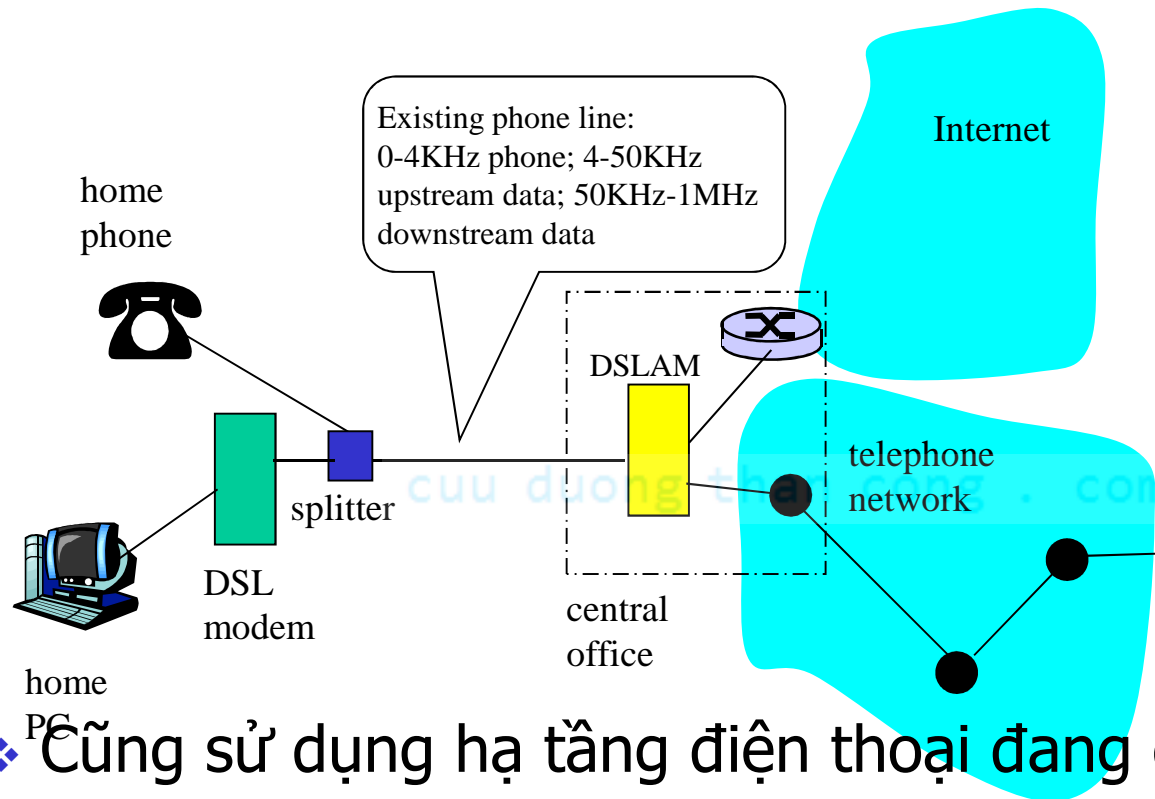


# Dial-up Modem



- ❖ Sử dụng hạ tầng mạng điện thoại đang có
  - ❖ Máy tính gia đình được kết nối vào **văn phòng trung tâm**
- ❖ Tốc độ truy cập trực tiếp đến các router lên tới 56Kbps
- ❖ Không thể vừa lướt web, vừa nghe điện thoại cùng lúc

# Digital Subscriber Line (DSL)



- ❖ Cũng sử dụng hạ tầng điện thoại đang có
- ❖ Tốc độ upstream lên tới 1Mbps (hiện giờ < 256 Kbps)
- ❖ Tốc độ downstream lên tới 8Mbps (hiện giờ < 1 Mbps)
- ❖ Sử dụng đường truyền vật lý dành riêng nối đến văn phòng trung tâm.

## Residential access: cable modems

- ❑ Không sử dụng hạ tầng điện thoại
  - ❖ Sử dụng hạ tầng mạng truyền hình cáp
- ❑ **HFC: hybrid fiber coax**
  - ❖ Bất đối xứng: 30Mbps downstream, 2 Mbps upstream
- ❑ **Mạng lưới** cáp đồng và cáp quang nối từng hộ gia đình đến router của ISP
  - ❖ Các hộ gia đình chia sẻ truy cập (**share access**) tới router
  - ❖ Không như DSL, kỹ thuật **dedicated access**



# Residential access: cable modems

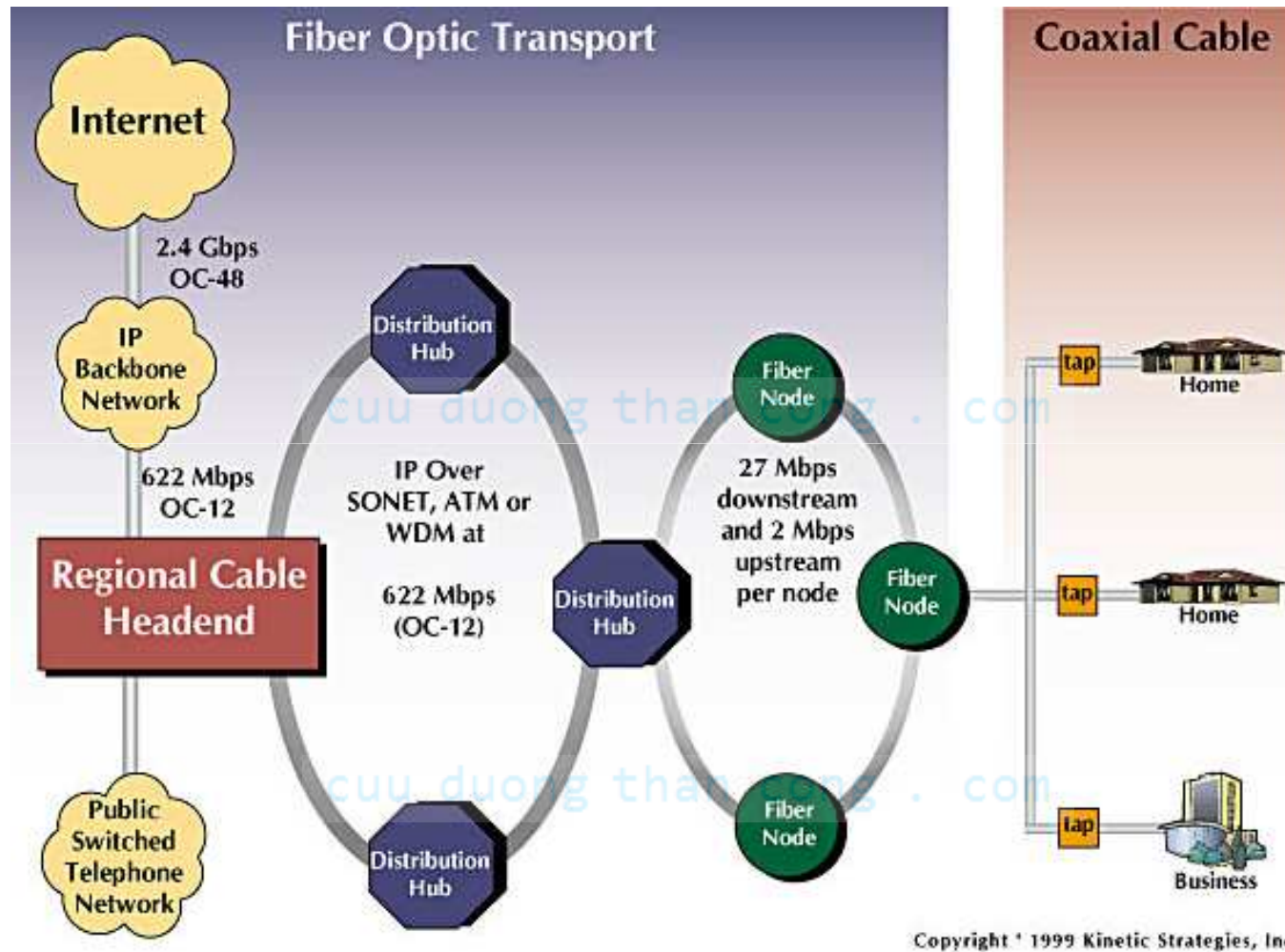
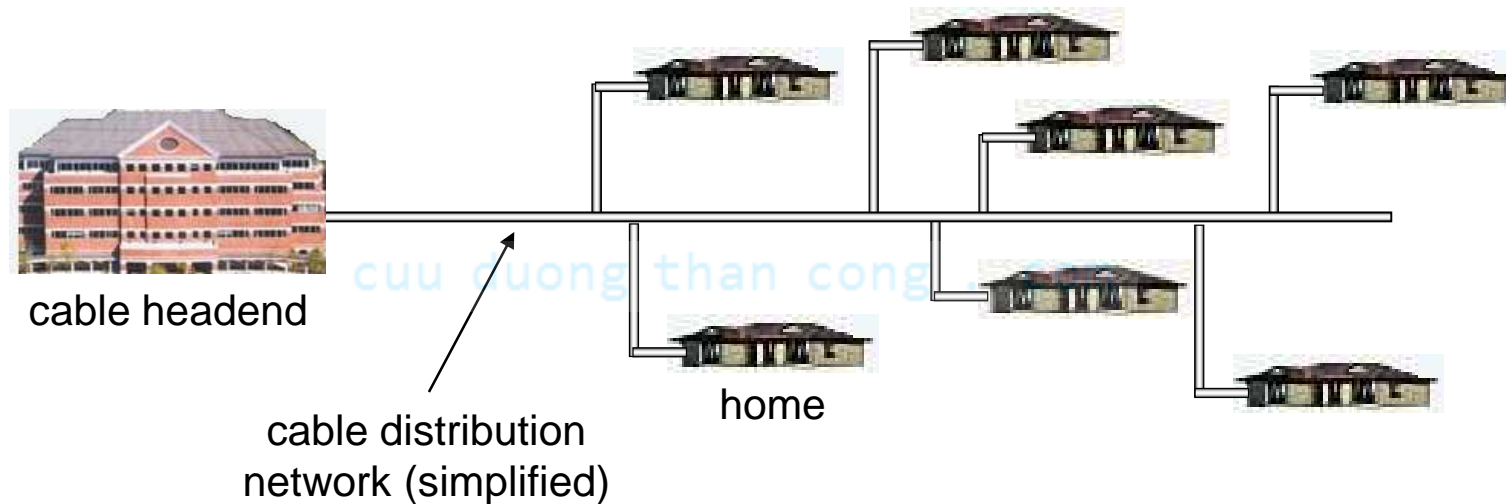


Diagram: <http://www.cabledatacomnews.com/cmhc/diagram.html>

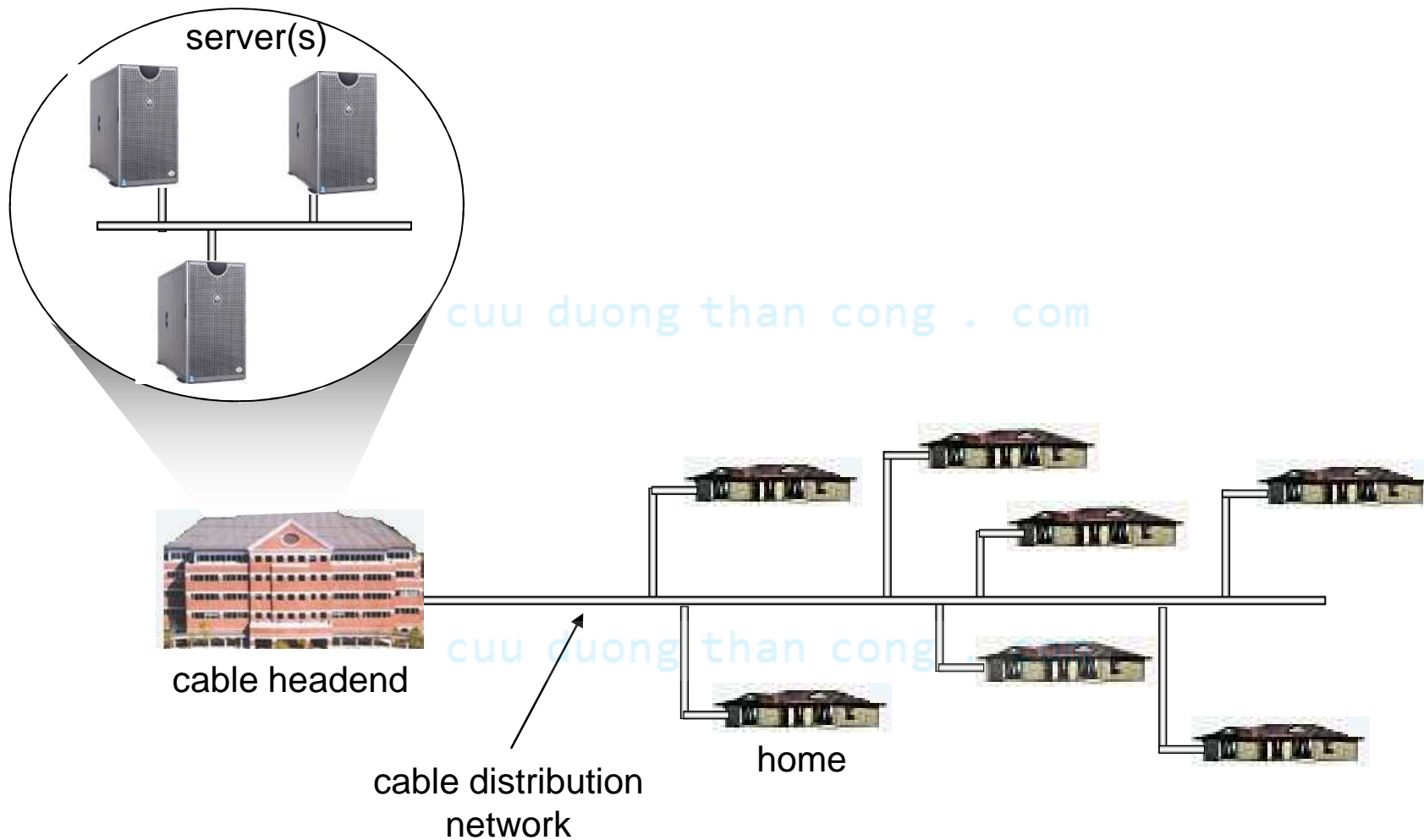
Introduction 1-17

# Cable Network Architecture: Overview

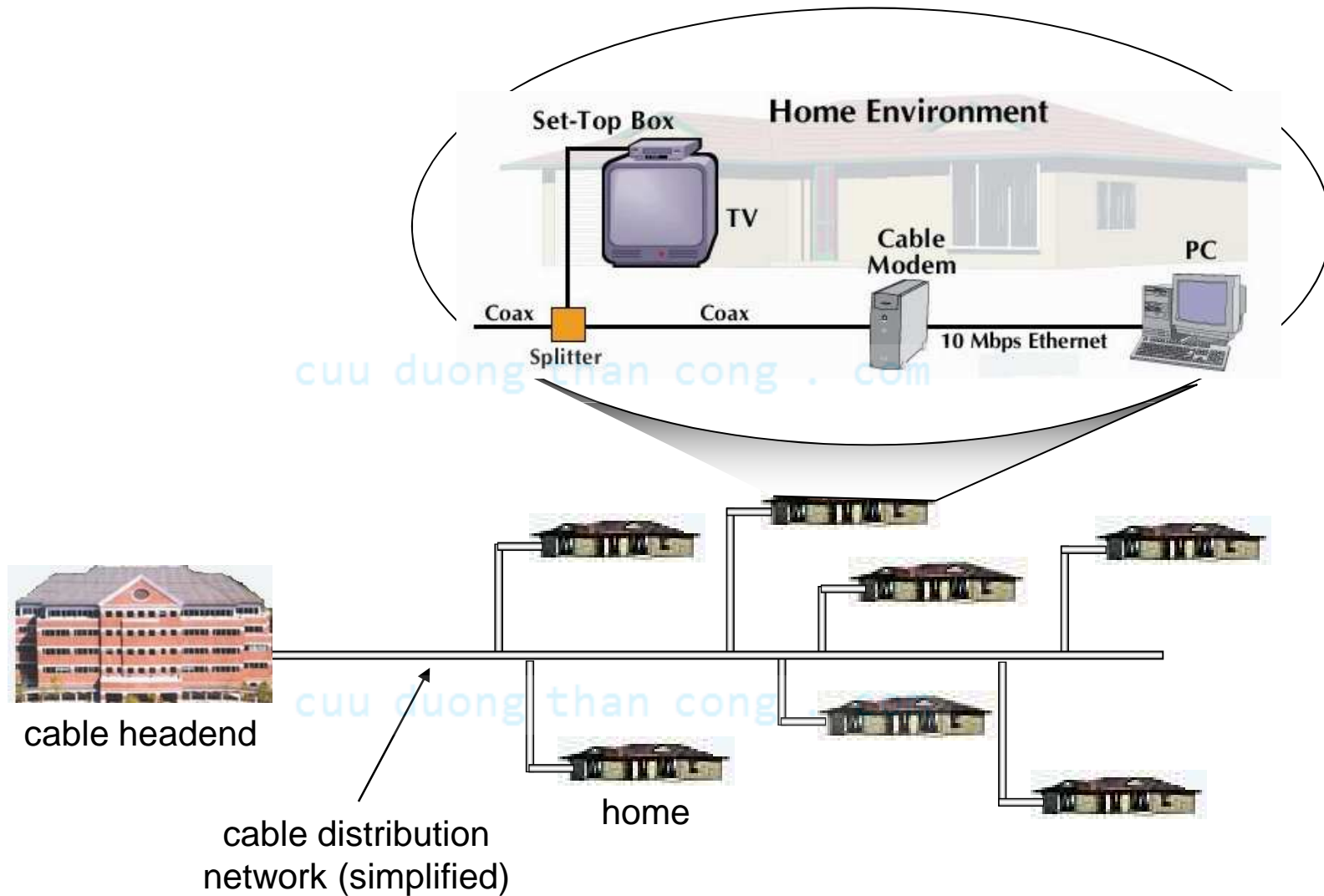
Typically 500 to 5,000 homes



# Cable Network Architecture: Overview

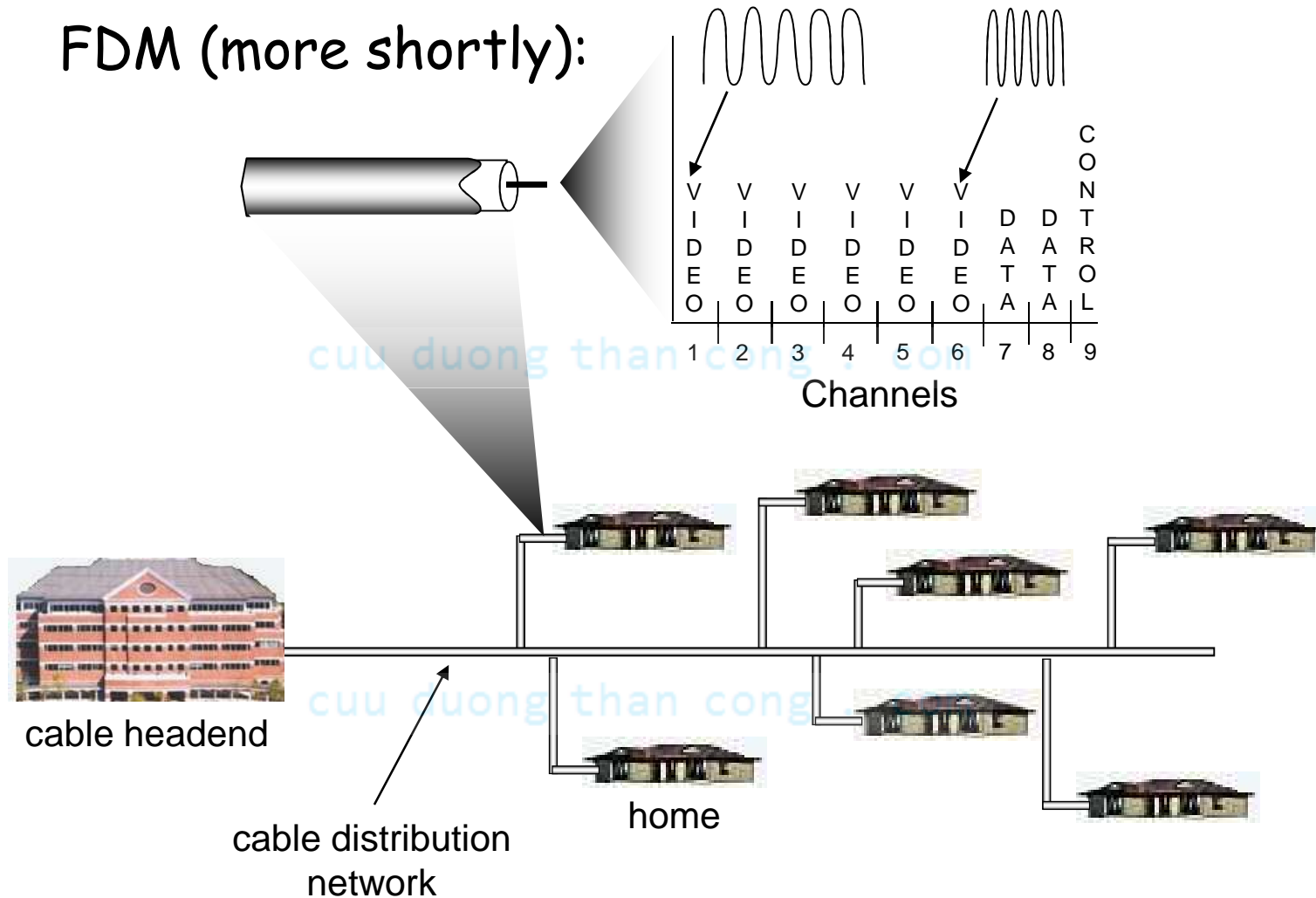


# Cable Network Architecture: Overview

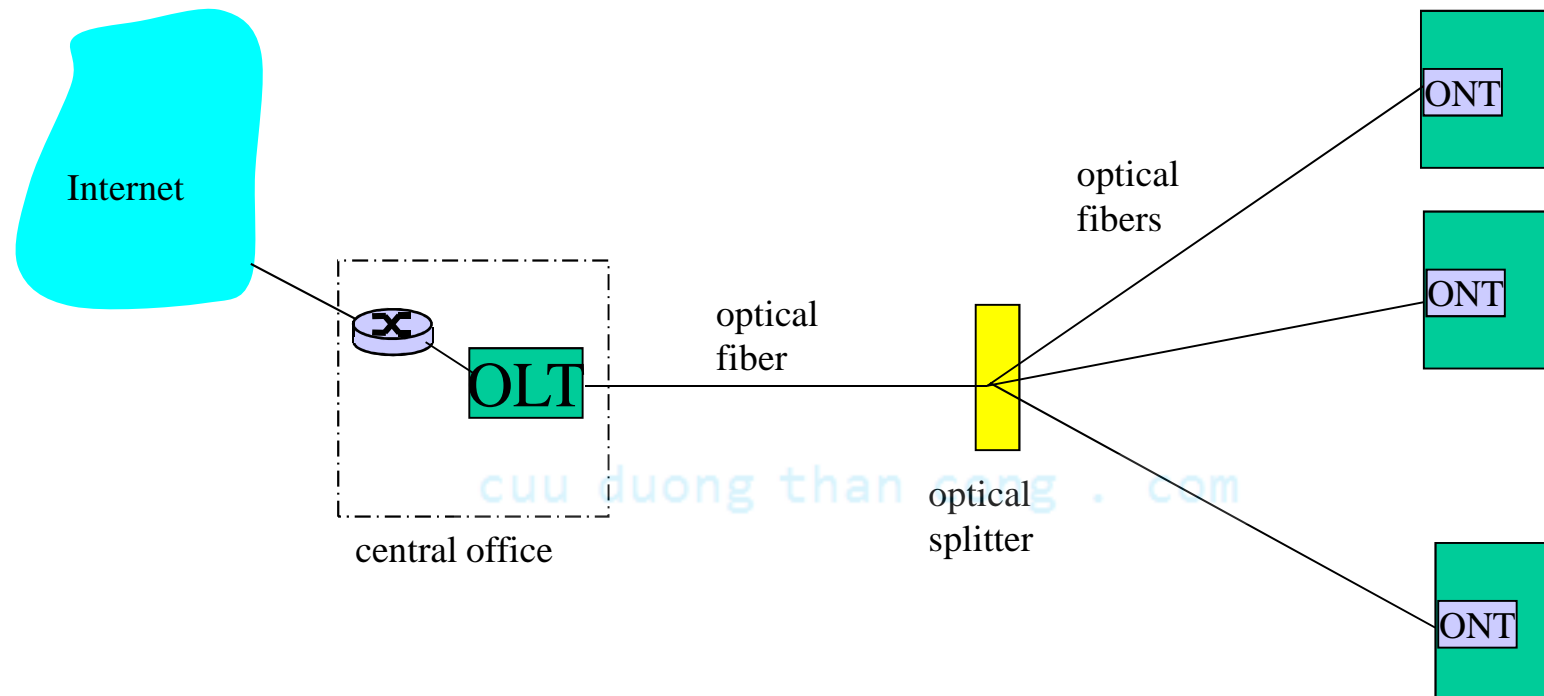


# Cable Network Architecture: Overview

FDM (more shortly):

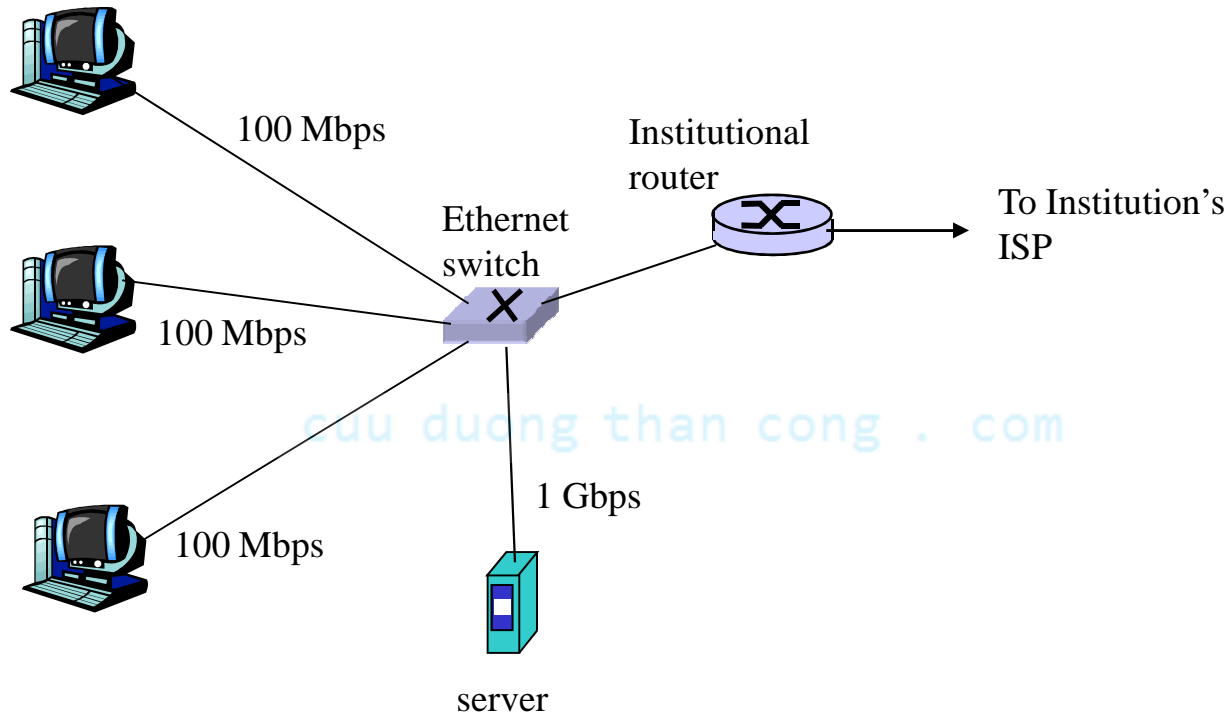


# Fiber to the Home



- ❑ Sử dụng đường cáp quang nối đến nhà
- ❑ Sử dụng 2 kỹ thuật cáp quang cạnh tranh:
  - ❖ Passive Optical network (PON)
  - ❖ Active Optical Network (PAN)
- ❑ Tốc độ truy cập Internet cao hơn, cho phép TV và điện thoại.

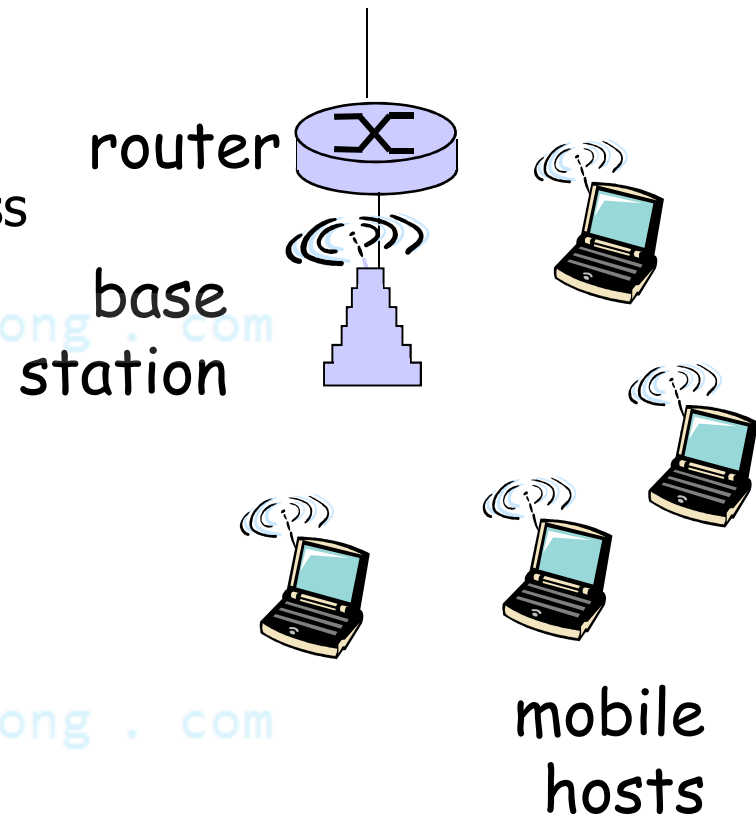
# Ethernet Internet access



- ❑ Được dùng phổ biến trong các Cty, trường học, ...
- ❑ 10 Mbs, 100Mbps, 1Gbps, 10Gbps Ethernet
- ❑ Hiện thời, các host được nối trực tiếp đến các Ethernet switch

# Wireless access networks

- ❑ Kết nối host đến router qua các mạng truy cập không dây (wireless) dùng chung
  - ❖ Qua các base station (hoặc “access point”)
- ❑ **wireless LANs:**
  - ❖ 802.11b/g (WiFi): 11 or 54 Mbps
- ❑ **wider-area wireless access**
  - ❖ provided by telco operator
  - ❖ ~1Mbps over cellular system (EVDO, HSDPA)
  - ❖ next up (?): WiMAX (10's Mbps) over wide area

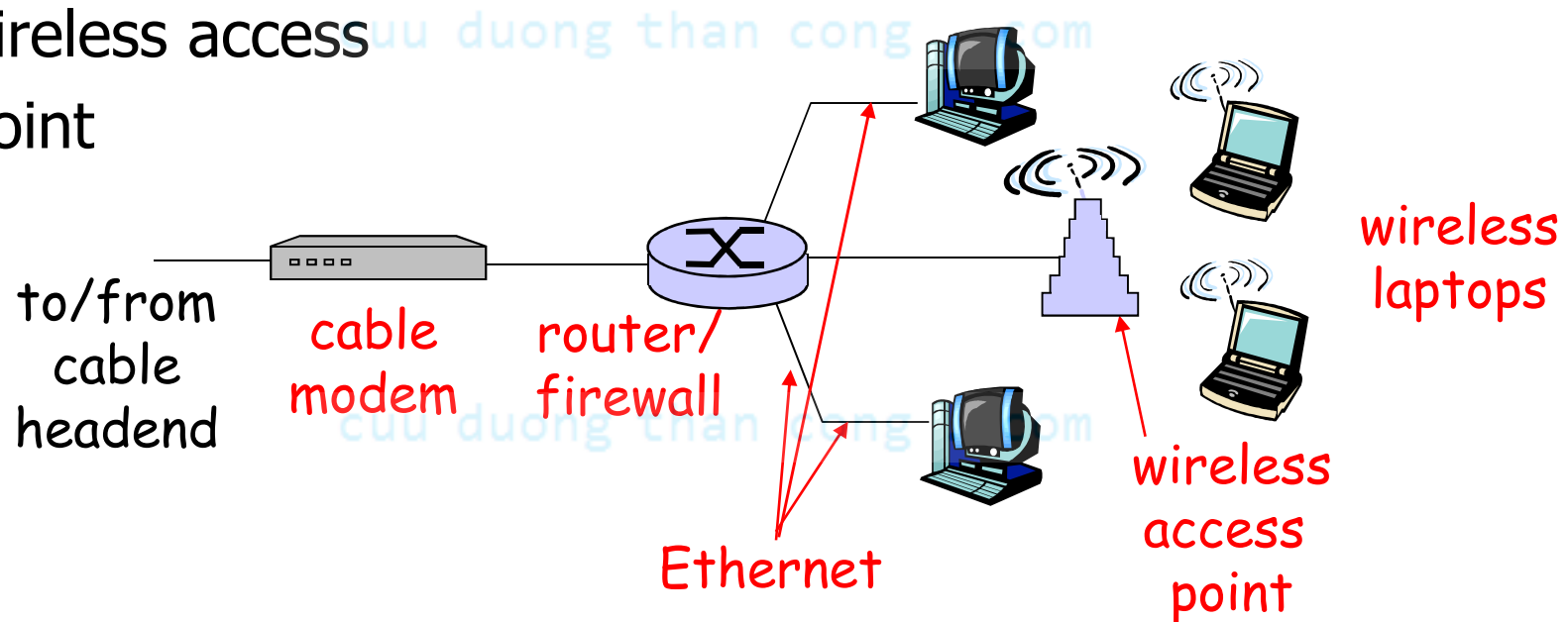




# Home networks

## Các thành phần tiêu biểu của home network

- ❑ DSL or cable modem
- ❑ router/firewall/NAT
- ❑ Ethernet
- ❑ wireless access point



# Physical Media

- ❑ **Bit:** propagates between transmitter/rcvr pairs
- ❑ **physical link:** what lies between transmitter & receiver
- ❑ **Phương tiện truyền dẫn (guided media):**
  - ❖ signals propagate in solid media: copper, fiber, coax
- ❑ **unguided media:**
  - ❖ signals propagate freely, e.g., radio

## Twisted Pair (TP)

- ❑ two insulated copper wires
  - ❖ Category 3: traditional phone wires, 10 Mbps Ethernet
  - ❖ Category 5: 100Mbps Ethernet



# Physical Media: coax, fiber

## Coaxial cable:

- ❑ Hai dây dẫn đồng trục
- ❑ Hai hướng
- ❑ baseband:
  - ❖ Một kênh truyền trên cáp
  - ❖ legacy Ethernet
- ❑ broadband:
  - ❖ Nhiều kênh truyền trên cáp
  - ❖ HFC



## Fiber optic cable:

- ❑ Sợi quang mang xung ánh sáng, mỗi xung biểu diễn 1 bit
- ❑ Làm việc ở tốc độ cao:
  - ❖ high-speed point-to-point transmission (e.g., 10's-100's Gps)
- ❑ Ít lỗi, miễn nhiễu điện từ



# Physical media: radio

- ❑ signal carried in electromagnetic spectrum
- ❑ no physical “wire”
- ❑ bidirectional
- ❑ propagation environment effects:
  - ❖ reflection
  - ❖ obstruction by objects
  - ❖ interference

## Radio link types:

- ❑ **terrestrial microwave**
  - ❖ e.g. up to 45 Mbps channels
- ❑ **LAN** (e.g., Wifi)
  - ❖ 11Mbps, 54 Mbps
- ❑ **wide-area** (e.g., cellular)
  - ❖ 3G cellular: ~ 1 Mbps
- ❑ **satellite**
  - ❖ Kbps to 45Mbps channel (or multiple smaller channels)
  - ❖ 270 msec end-end delay
  - ❖ geosynchronous versus low altitude

# 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

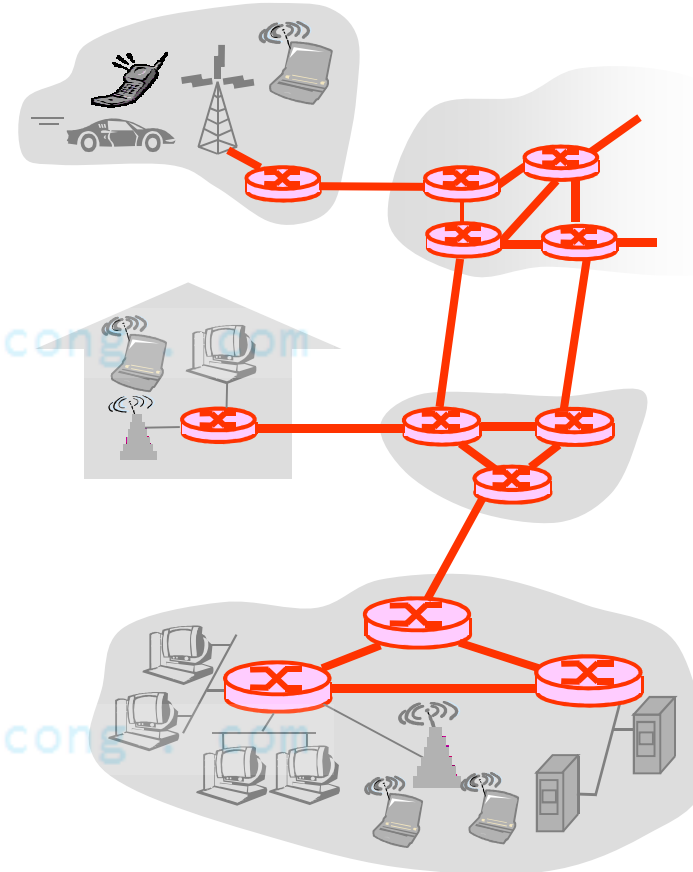
1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

# The Network Core

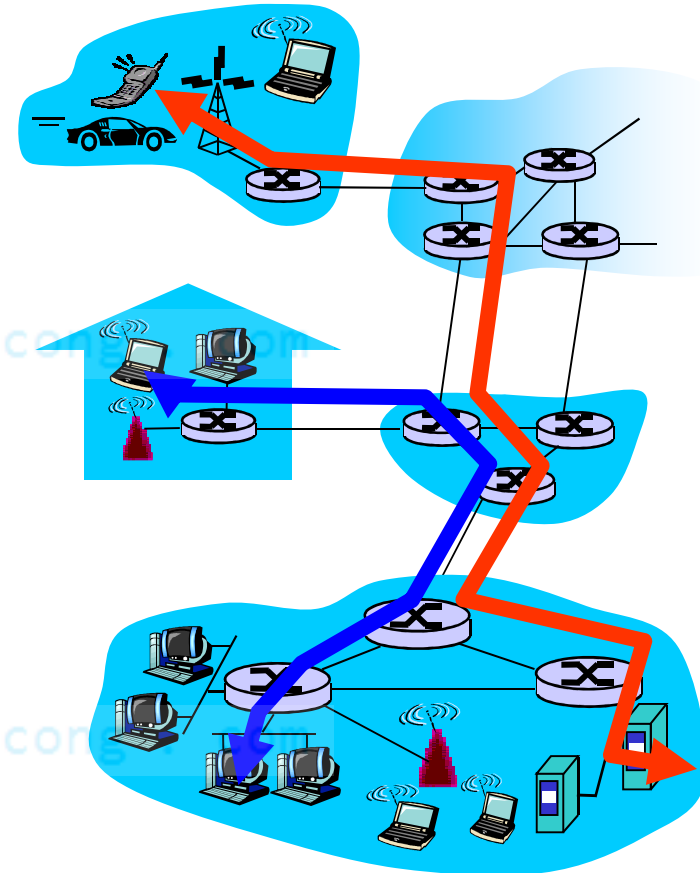
- ❑ Mạng lưới các router được nối kết nhau
- ❑ Câu hỏi căn bản: dữ liệu được truyền dẫn qua mạng này như thế nào?
  - ❖ **circuit switching**: dedicated circuit per call: telephone net
  - ❖ **packet-switching**: data sent thru net in discrete "chunks"



# Network Core: Circuit Switching

End-end resources reserved for "call"

- ❑ link bandwidth, switch capacity
- ❑ dedicated resources: no sharing
- ❑ circuit-like (guaranteed) performance
- ❑ call setup required



# Network Core: Circuit Switching

- network resources (e.g., bandwidth) **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

cuu duong than cong . com

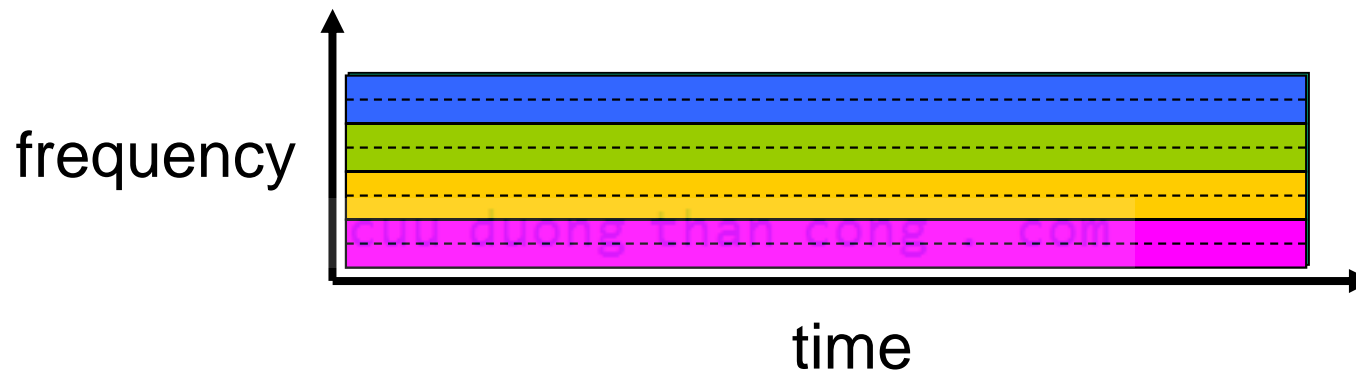


# Circuit Switching: FDM and TDM

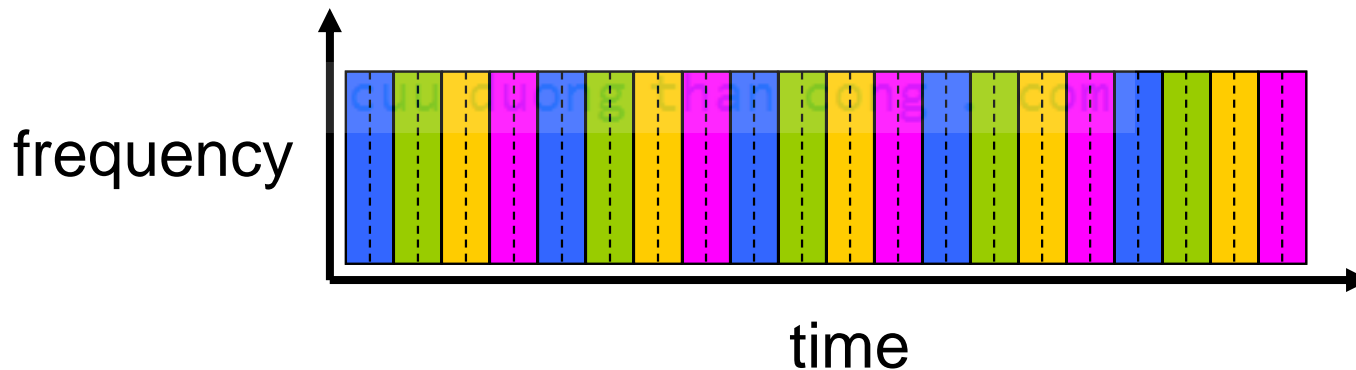
FDM

Example:

4 users



TDM



# Numerical example

- ❑ Gửi 1 file 640,000 bits, từ host A đến host B qua mạng circuit-switched mất bao lâu?
  - ❖ Tốc độ đường truyền 1.536 Mbps
  - ❖ Mỗi đường truyền sử dụng TDM với 24 slots/sec
  - ❖ Cần 500 msec để thiết lập mạch nối 2 điểm


cuu duong than cong . com

# Network Core: Packet Switching

Dòng dữ liệu được chia thành các gói tin (*packets*)

- ❑ user A, B packets *share* network resources
- ❑ each packet uses full link bandwidth
- ❑ resources used *as needed*

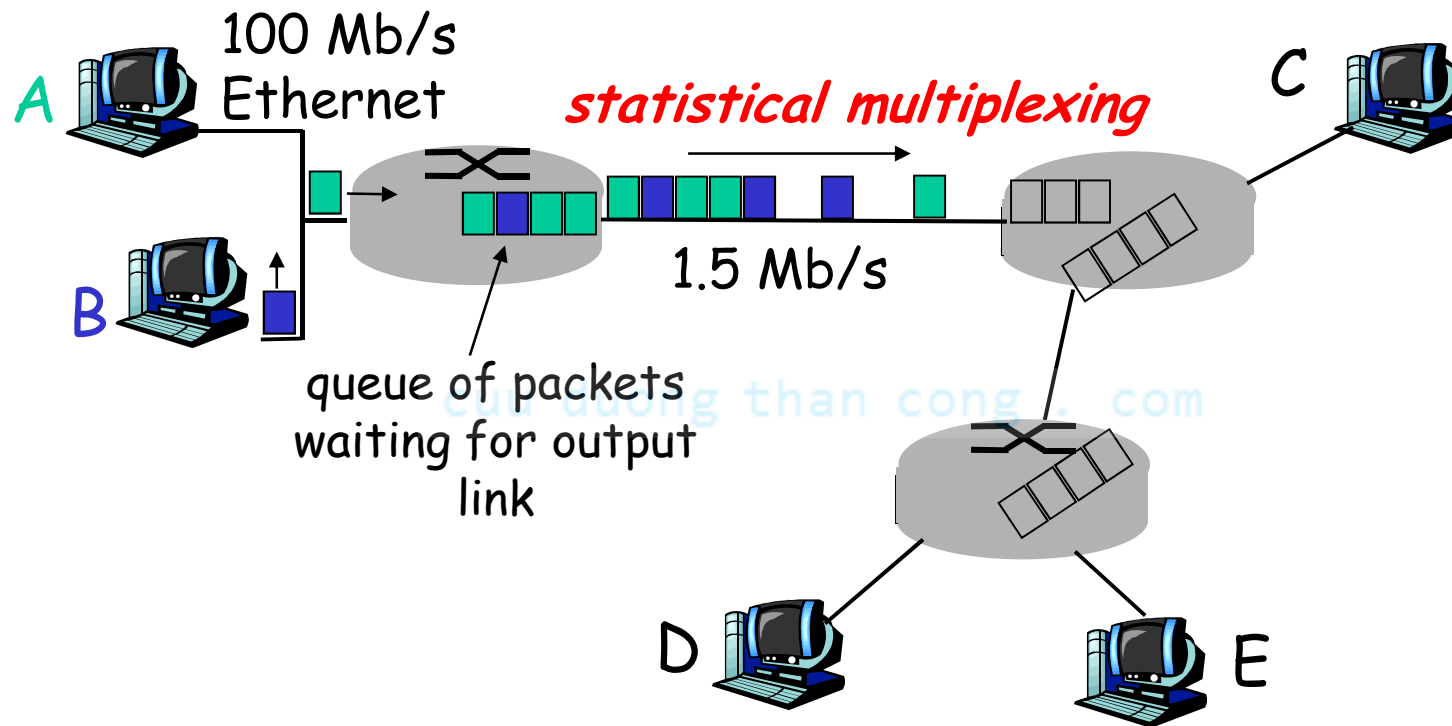
Bandwidth division into "pieces"  
Dedicated allocation  
Resource reservation



Tranh chấp tài nguyên:

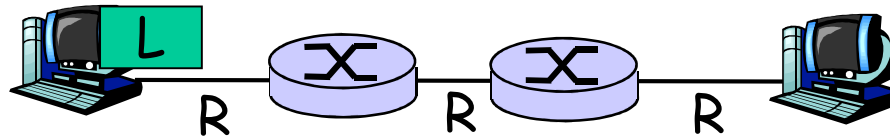
- ❑ Tổng nhu cầu tài nguyên yêu cầu có thể vượt quá khả năng tài nguyên đang có
- ❑ Tắc nghẽn: hàng đợi gói tin, chờ sử dụng đường truyền
- ❑ store and forward: packets move one hop at a time
  - ❖ Node receives complete packet before forwarding

# Packet Switching: Statistical Multiplexing



Sequence of A & B packets does not have fixed pattern,  
bandwidth shared on demand → **statistical multiplexing**.  
TDM: each host gets same slot in revolving TDM frame.

# Packet-switching: store-and-forward



- ❑ Cần  $L/R$  giây để truyền hết gói tin  $L$  bit lên đường truyền với tốc độ  $R$  bps

- ❑ *store and forward*: toàn bộ gói tin phải đến router trước khi có thể được truyền trên nhánh mạng kế tiếp.

- ❑ Độ trễ (delay) =  $3 L/R$  (giả sử ko có độ trễ trên đường truyền)

## Example:

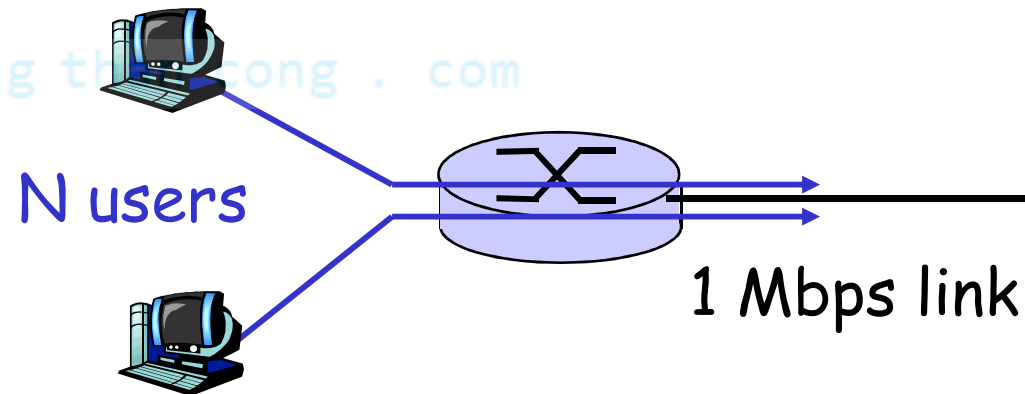
- ❑  $L = 7.5$  Mbits
- ❑  $R = 1.5$  Mbps
- ❑ transmission delay = 15 sec

} more on delay shortly ...

# Packet switching versus circuit switching\*

*Packet switching cho phép nhiều user hơn dùng mạng*

- ❑ 1 Mb/s link
- ❑ Mỗi user:
  - ❖ 100 kb/s khi “active”
  - ❖ active 10% of time
- ❑ *circuit-switching:*
  - ❖ 10 users
- ❑ *packet switching:*
  - ❖ Với 35 users, xác suất nhiều hơn 10 user “active” cùng lúc  $< .0004$



Q: Tính như thế nào để ra 0.0004?

# Packet switching versus circuit switching

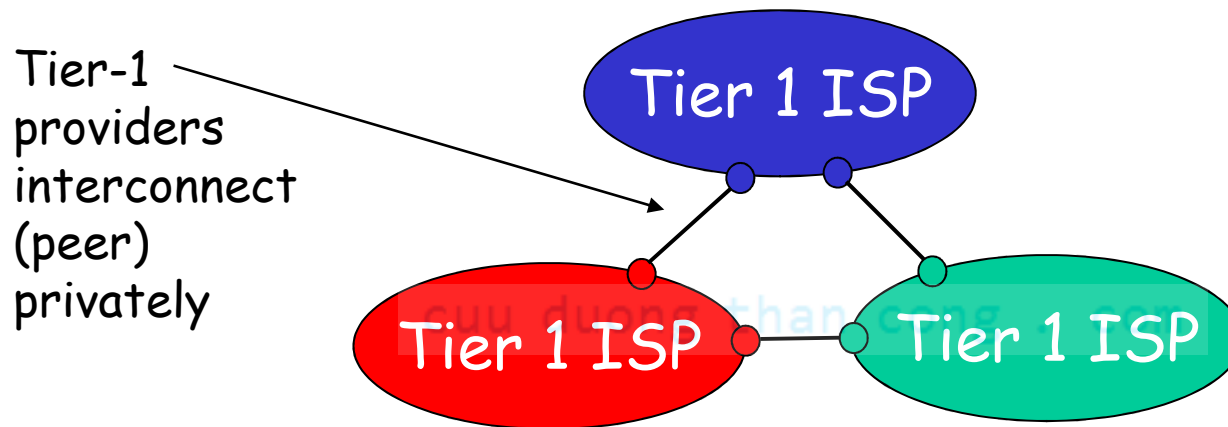
Is packet switching a “slam dunk winner?”

- ❑ Tốt cho trường hợp truyền dữ liệu hàng loạt
  - ❖ resource sharing
  - ❖ simpler, no call setup
- ❑ Sự ùn tắc quá mức: chậm trễ và mất gói tin
  - ❖ Cần có protocol để đảm bảo việc truyền dữ liệu, kiểm soát việc ùn tắc.
- ❑ Q: How to provide circuit-like behavior?
  - ❖ Cần có cơ chế đảm bảo tốc độ truyền tối thiểu cho các ứng dụng video/audio
  - ❖ Vẫn còn là vấn đề nan giải (chương 7)

Q: human analogies of reserved resources (circuit switching) versus on-demand allocation (packet-switching)?

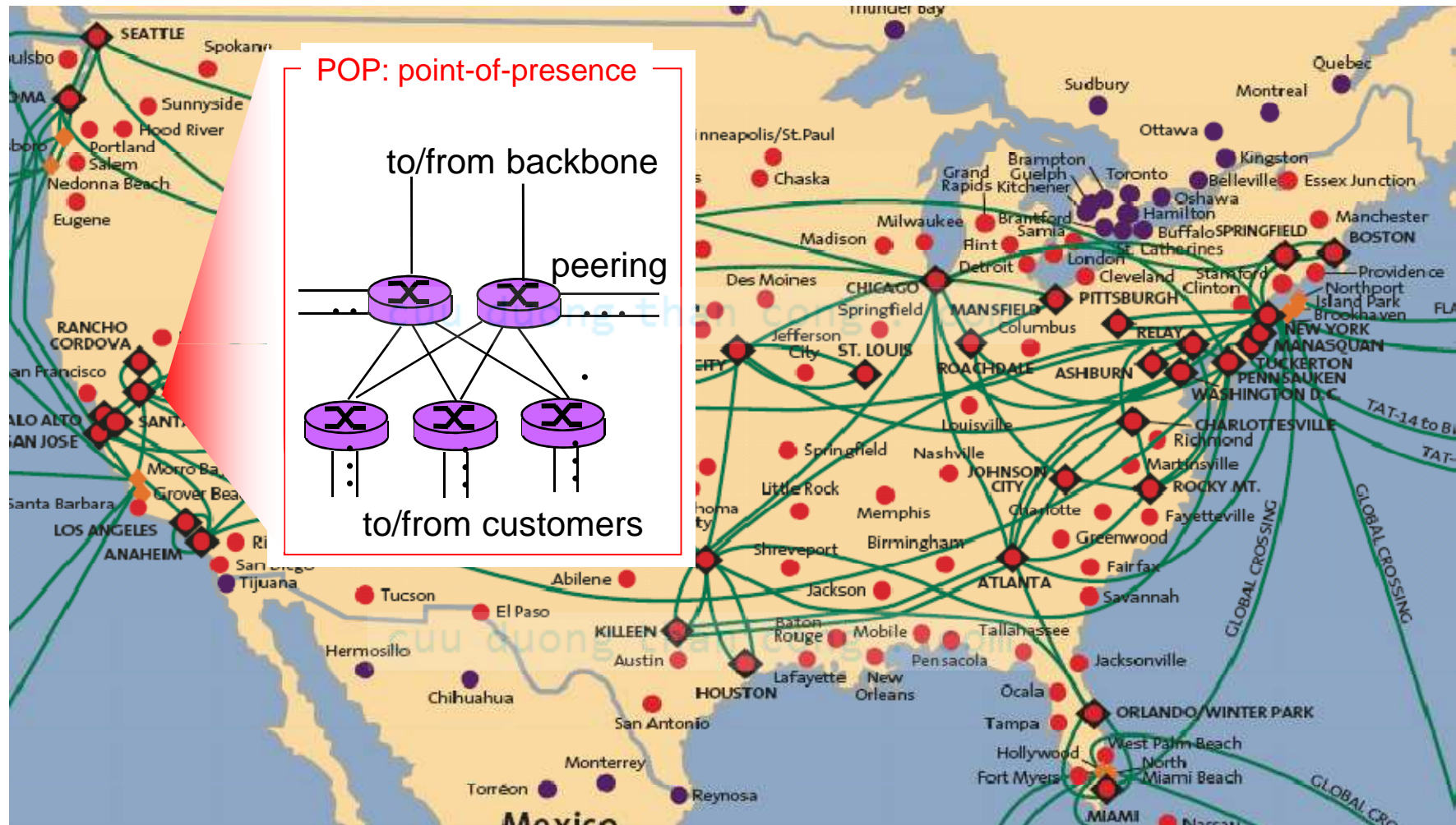
# Internet structure: network of networks

- ❑ Có cấu trúc phân cấp
- ❑ ở trung tâm: các nhà cung cấp dịch vụ Internet cấp 1 "tier-1" ISPs (e.g., Verizon, Sprint, AT&T, Cable and Wireless), có tầm bao phủ quốc gia/quốc tế
  - ❖ treat each other as equals





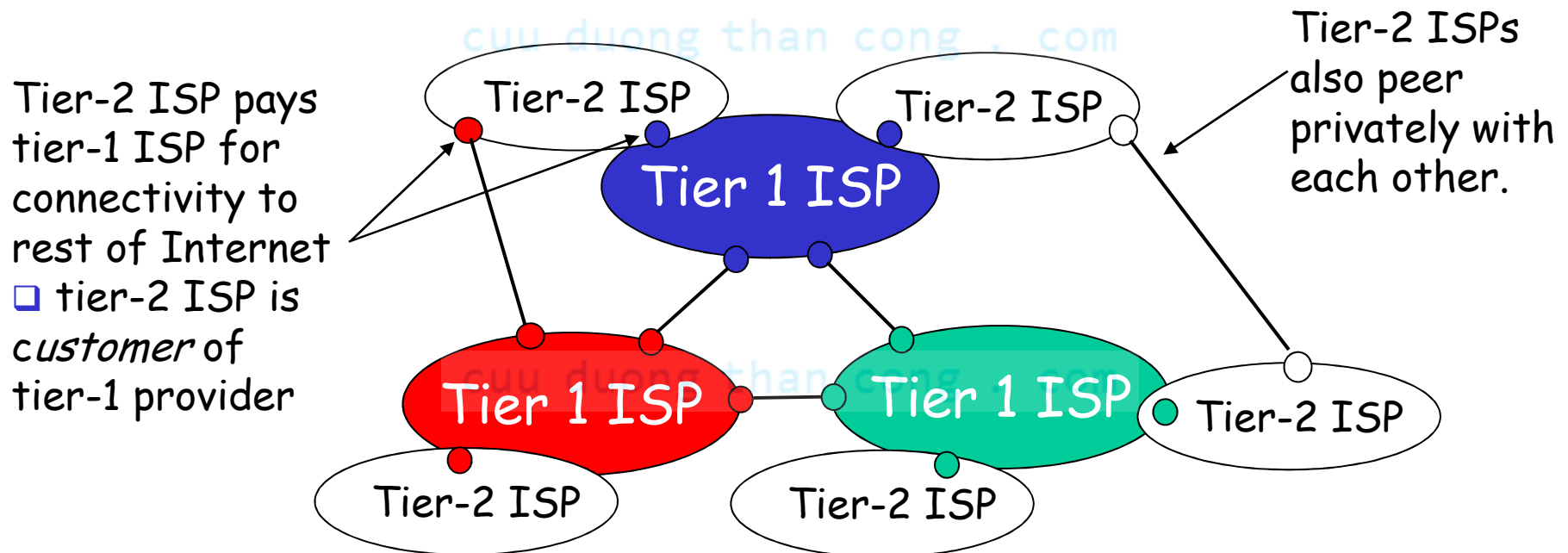
# Tier-1 ISP: e.g., Sprint



# Internet structure: network of networks

## ❑ Nhà cung cấp dịch vụ cấp 2 ("Tier-2" ISPs): nhỏ hơn, độ bao phủ cấp vùng

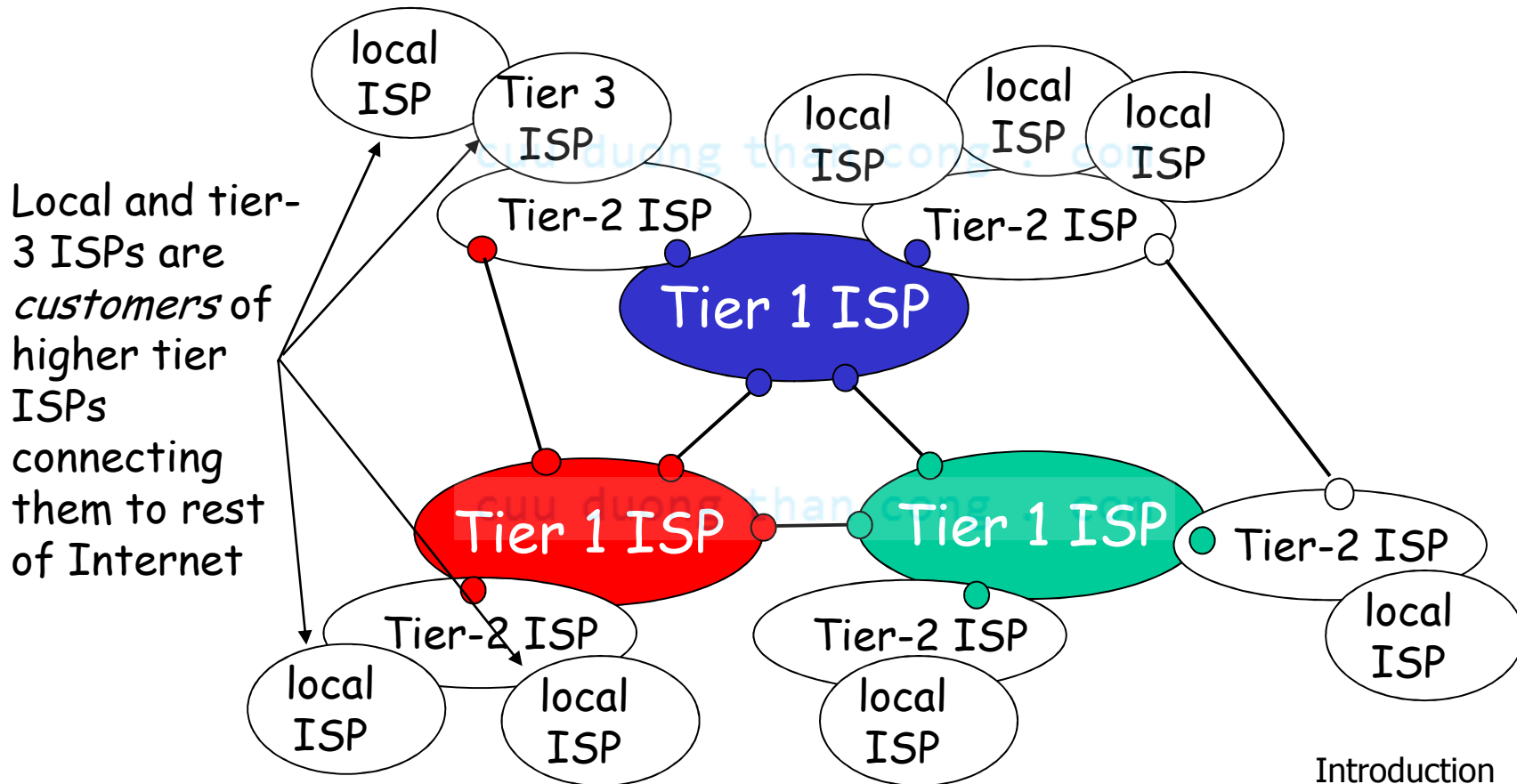
- ❖ Kết nối đến 1 hoặc nhiều ISP cấp 1, cũng có thể với các ISP cấp 2 khác



# Internet structure: network of networks

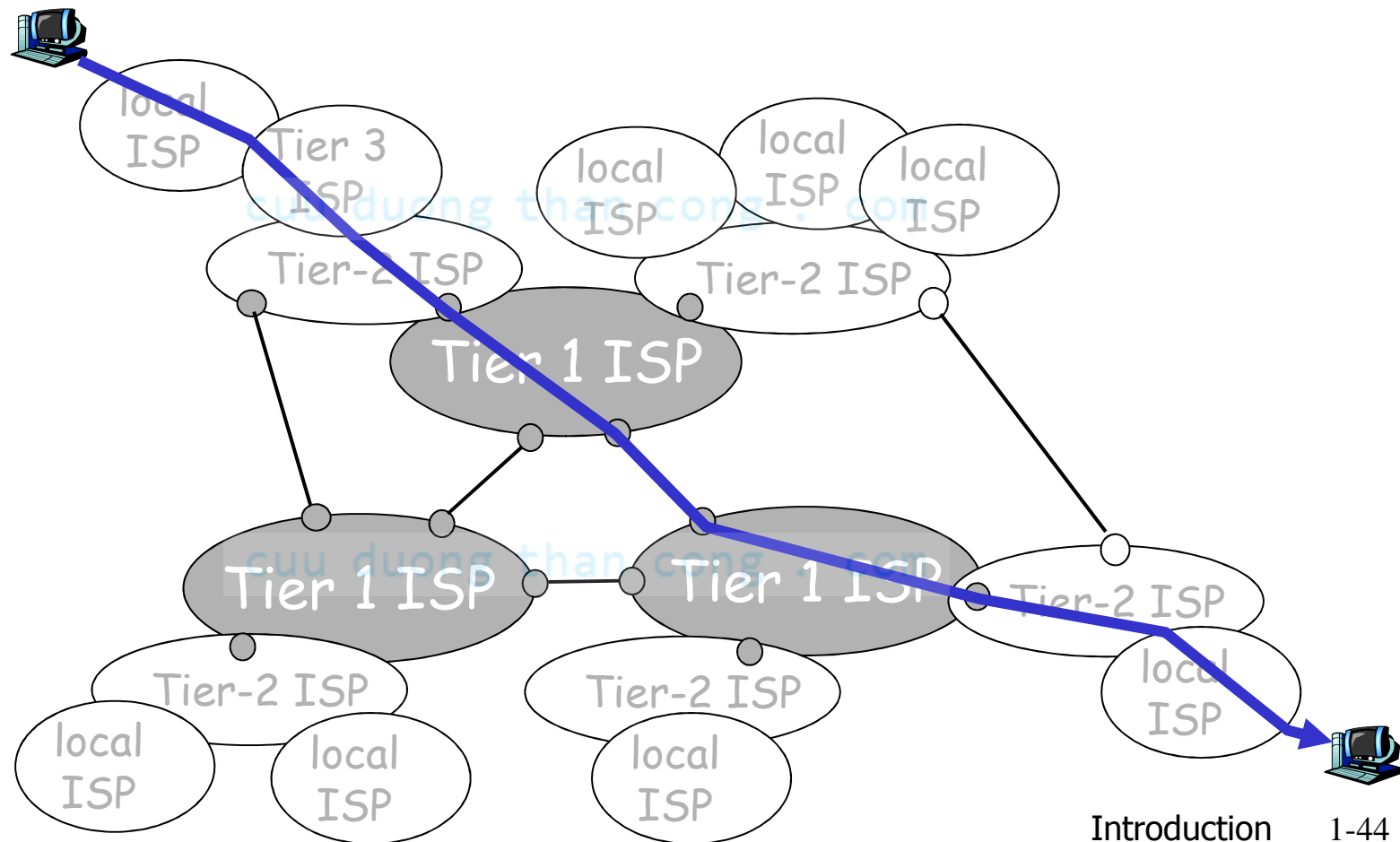
❑ ISP cấp 3 ("Tier-3" ISPs) và các ISP địa phương

- ❖ last hop ("access") network (closest to end systems)



# Internet structure: network of networks

- ❑ Một gói tin đi xuyên qua nhiều mạng!



# 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

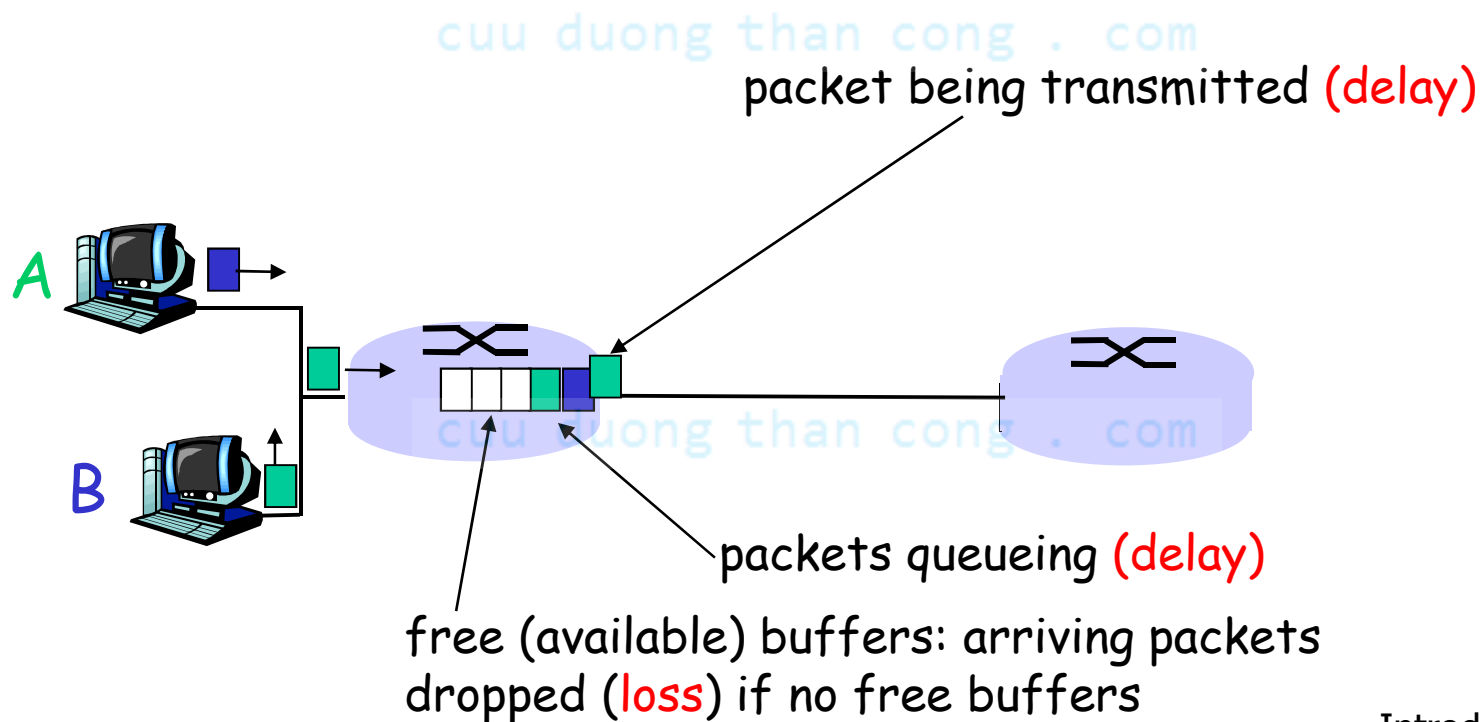
1.6 Networks under attack: security

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



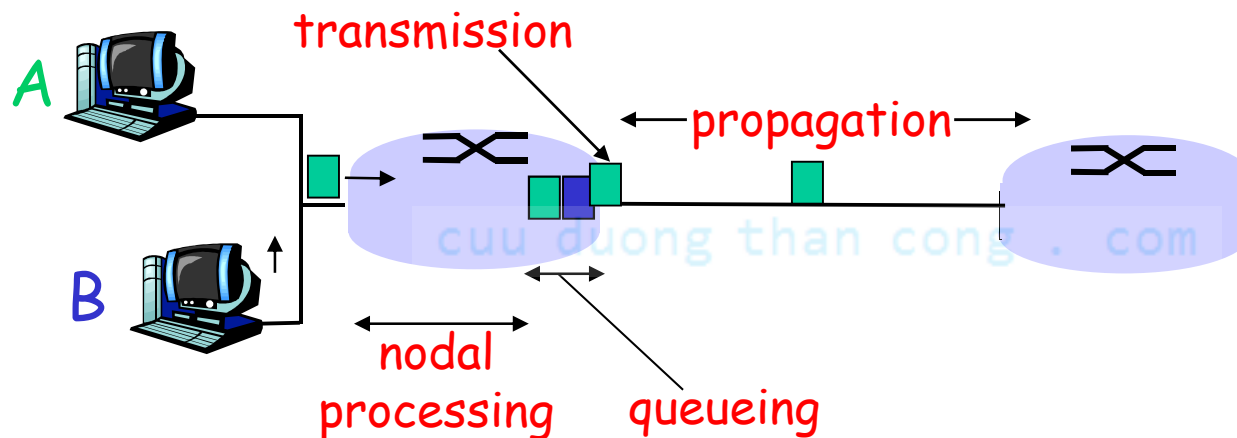
# Four sources of packet delay

## ❑ 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

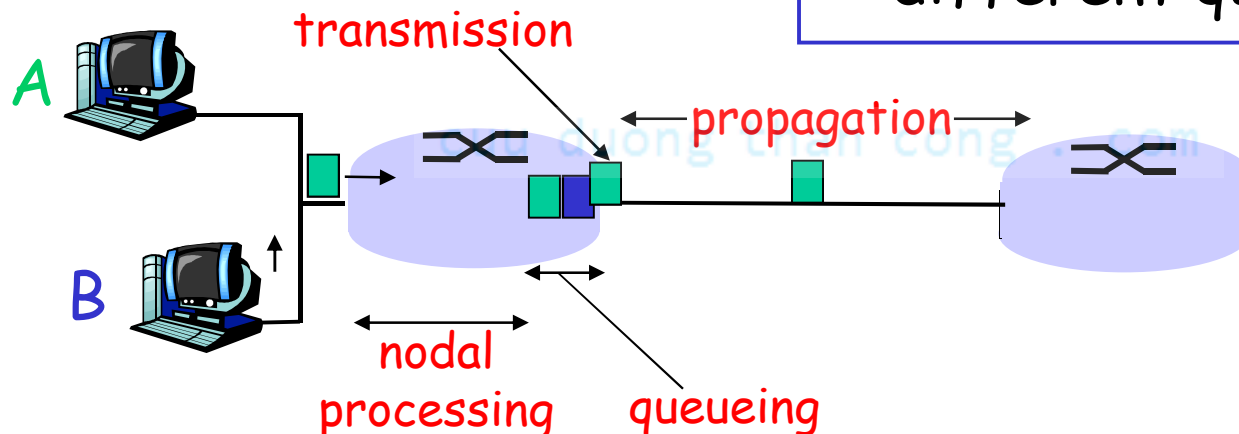
## 3. Transmission delay:

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

## 4. Propagation delay:

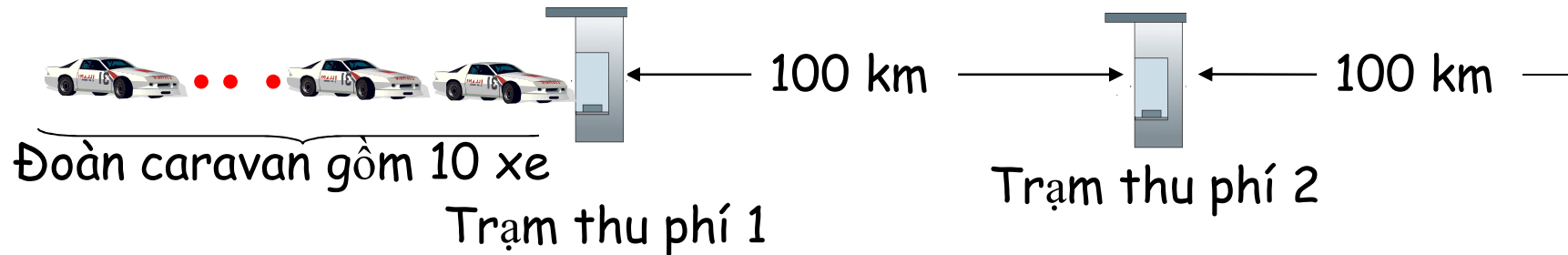
- ❑  $d$  = length of physical link
- ❑  $s$  = propagation speed in medium ( $\sim 2 \times 10^8$  m/sec)
- ❑ propagation delay =  $d/s$

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



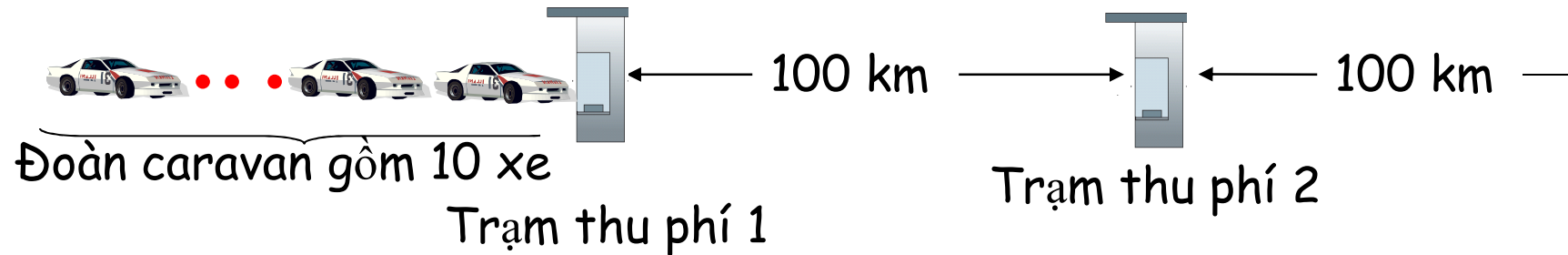


# Caravan analogy



- ❑ Các xe hơi “lan truyền” ở vận tốc 100 km/h
- ❑ Trạm thu phí phục vụ mỗi xe mất 12 giây (transmission time)
- ❑ Xe ô tô ~ bit; caravan ~ packet
- ❑ Q: Thời gian cần để đoàn caravan làm xong thủ tục ở trạm thu phí 1 và tập kết đến trạm thu phí thứ 2?
- ❑ Thời gian để trạm thu phí “đẩy” toàn đoàn caravan lên đường =  $12 \times 10 = 120$  giây
- ❑ Thời gian để chiếc xe sau cùng đi từ trạm 1 đến trạm 2:  
 $100 \text{ km} / (100 \text{ km/h}) = 1 \text{ h}$
- ❑ A: 62 phút

# Caravan analogy (more)



- ❑ Các xe “lan truyền” với tốc độ 1000km/h
- ❑ Trạm thu phí phục vụ 1 xe mất 1 phút
- ❑ Q: Các xe sẽ đến trạm thứ 2 trước khi tất cả các xe được phục vụ xong ở trạm 1?
- ❑ **Đúng vậy!** Sau 7 phút, xe thứ nhất đến trạm thu phí 2, và 3 xe vẫn còn ở trạm 1
- ❑ Bit đầu tiên của gói tin có thể đến router thứ 2 trước khi gói tin được truyền đi hết ở router thứ 1!
  - ❖ See Ethernet applet at AVL Web site

# Nodal delay

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

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

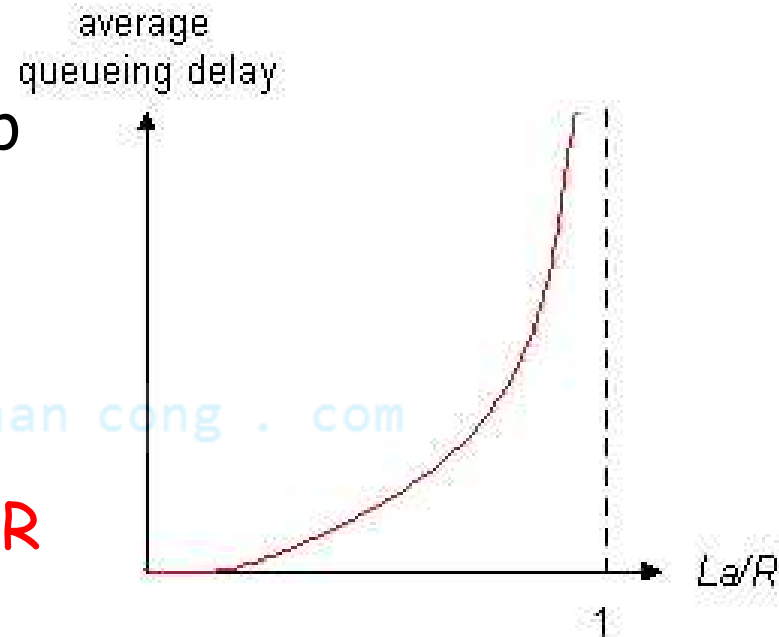
# Queueing delay (revisited)

- $R$  = tốc độ truyền cho phép của đường truyền (bps)
- $L$  = chiều dài gói tin (bits)
- $a$  = tốc độ trung bình của gói tin

$$\rho = \text{traffic intensity} = La/R$$

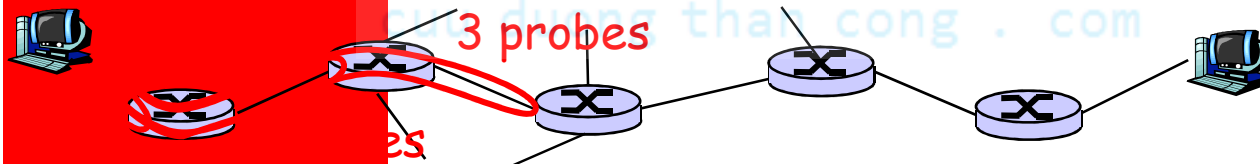
$$\text{Delay} = 1 / (1 - \rho)$$

- $La/R \sim 0$ : độ chờ (trung bình ở hàng đợi) nhỏ
- $La/R \rightarrow 1$ : độ chờ (trung bình ở hàng đợi) lớn
- $La/R > 1$ : độ chờ có thể rất lớn!



# “Real” Internet delays and routes


- ❑ What do “real” Internet delay & loss look like?
- ❑ program: đo độ trễ từ máy nguồn đến router, dọc theo đường đến máy đích. Với mọi  $i$ :
  - ❖ gửi 3 gói tin đến router thứ  $i$  nằm trên con đường đến đích
  - ❖ router  $i$  sẽ gửi các gói tin về máy nguồn
  - ❖ Máy nguồn sẽ tính được thời gian gói tin đi-về



# “Real” Internet delays and routes

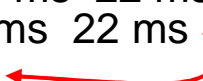
**traceroute:** gaia.cs.umass.edu to www.eurecom.fr

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

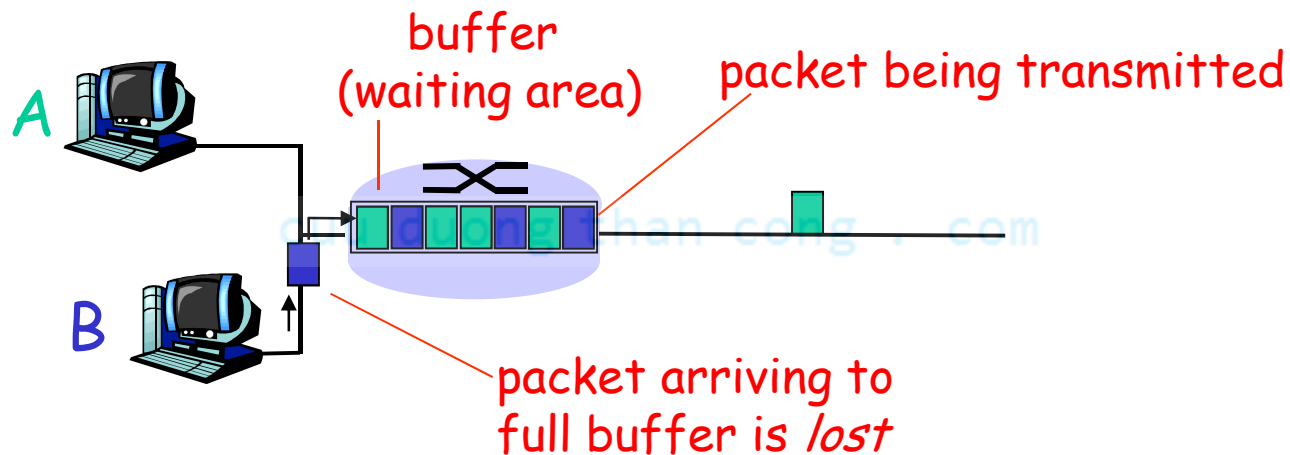


\* means no response (probe lost, router not replying)



# Packet loss

- ❑ Hàng đợi (queue) trước đường truyền có kích thước có hạn
- ❑ Các gói tin đến một hàng đợi đã đầy sẽ bị mất
- ❑ Các gói tin bị mất có thể được truyền lại, hoặc không

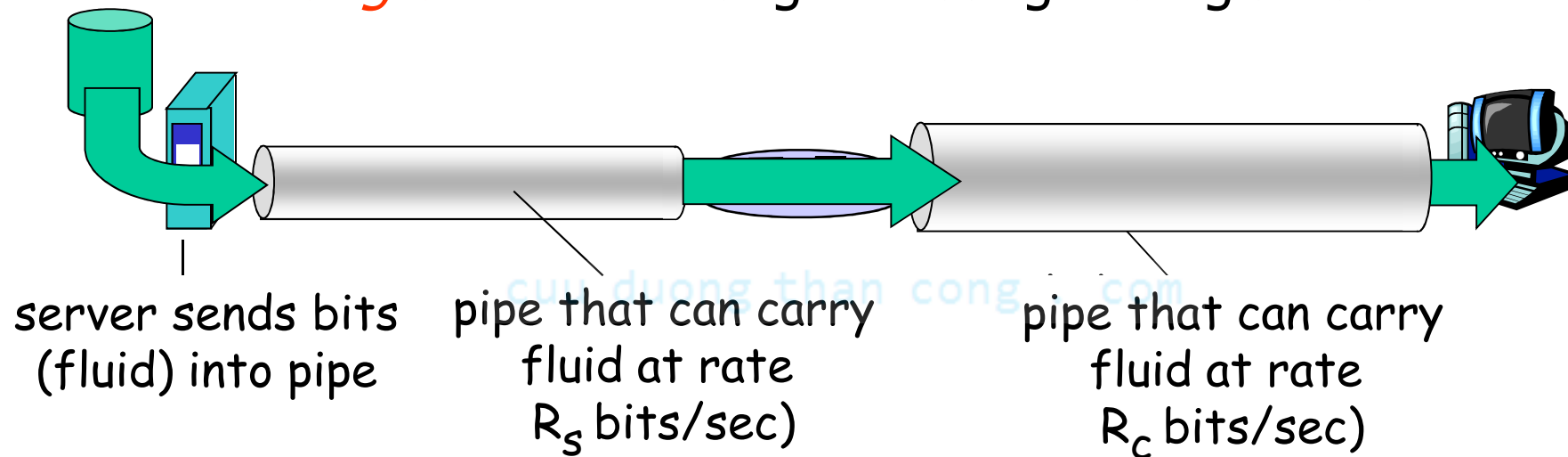


# Throughput

❑ *Thông lượng (throughput)* : số bit truyền giữa bên truyền và nhận trong một đơn vị thời gian

❖ *Tức thời*: tính ở một thời điểm.

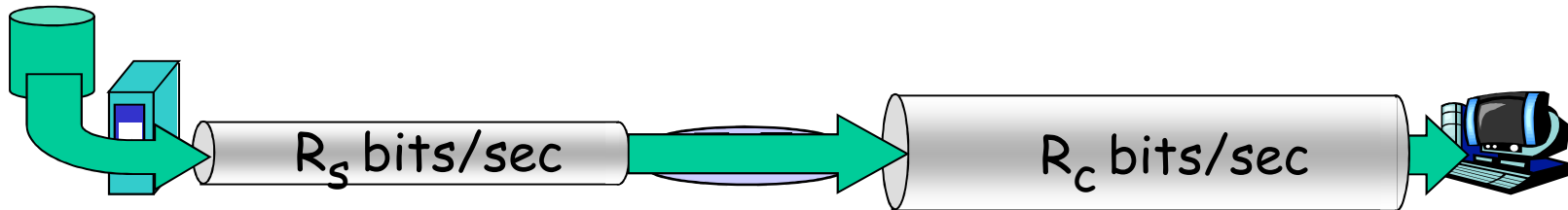
❖ *Trung bình*: tính trong 1 khoảng thời gian dài.





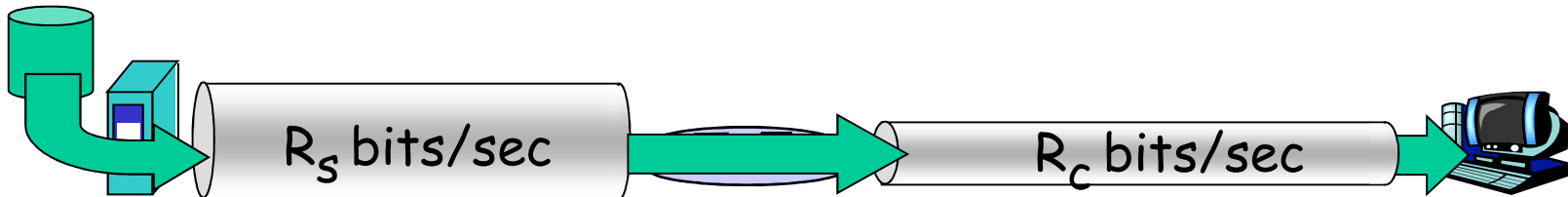
# Throughput (more)

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



cuu duong than cong . com

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



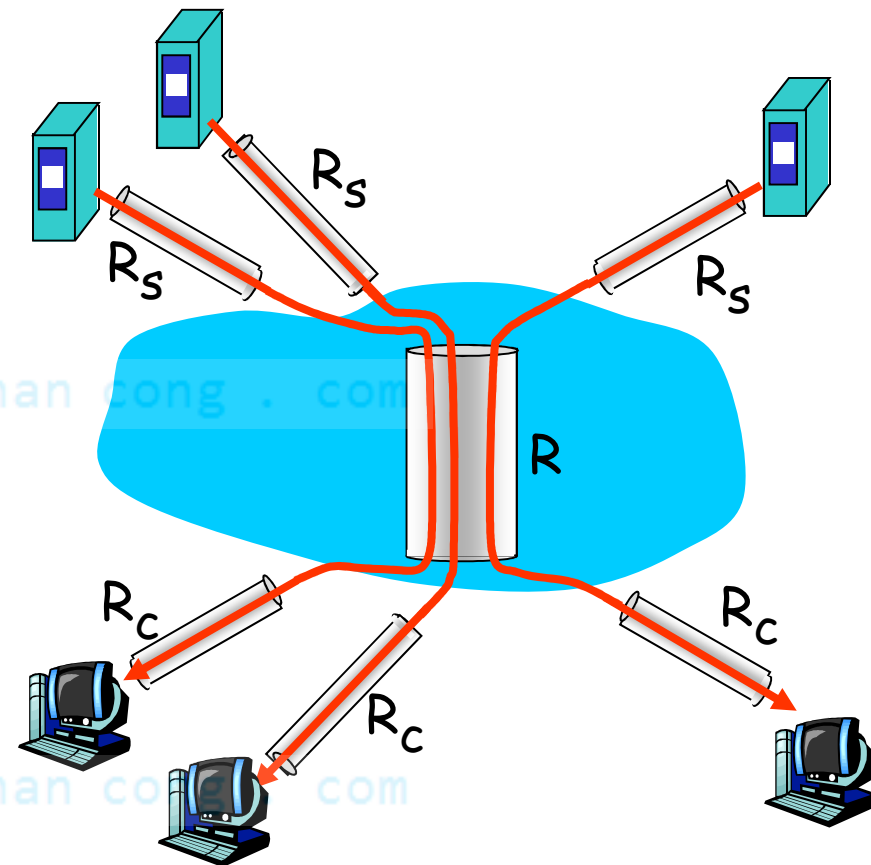
cuu duong than cong . com

*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”

## Mạng vốn phức tạp!

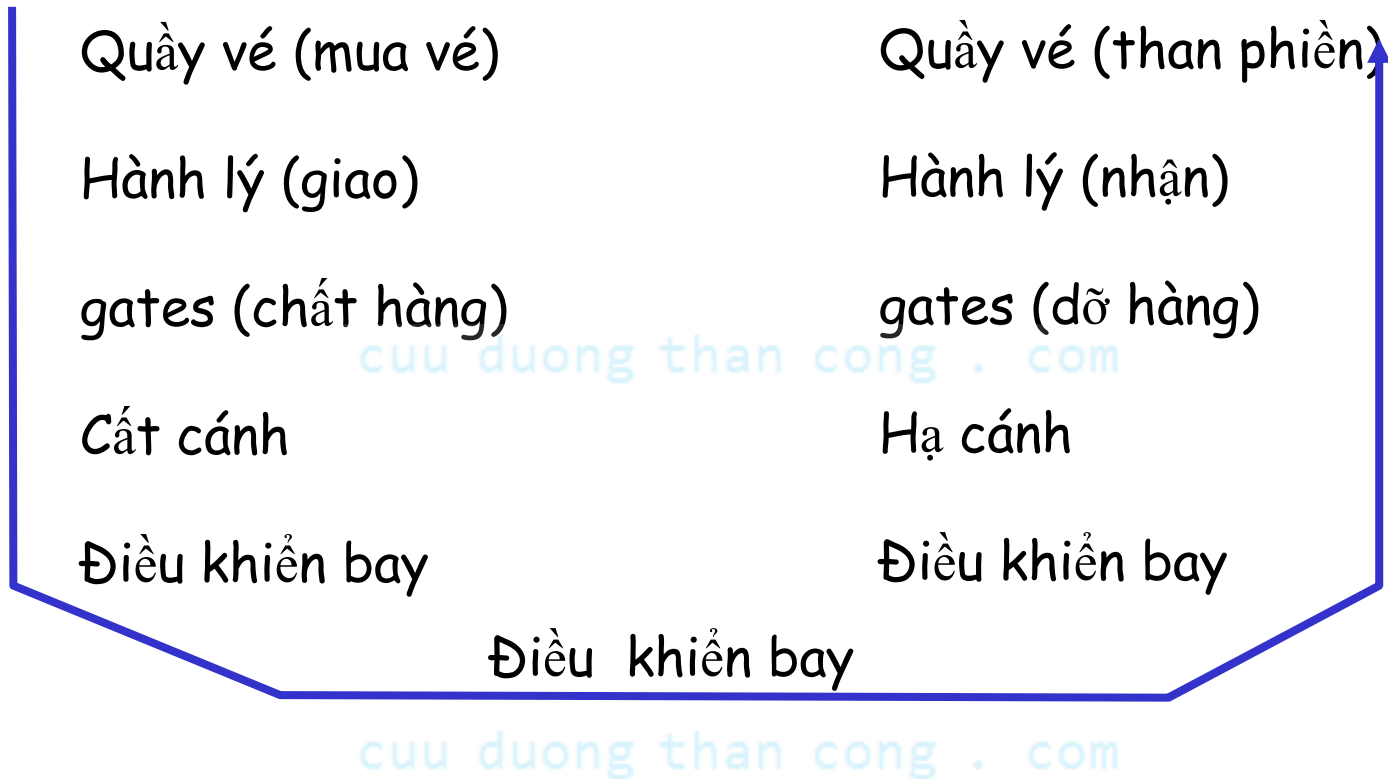
□ Gồm nhiều “thứ”:

- ❖ hosts
- ❖ routers
- ❖ links of various media
- ❖ applications
- ❖ protocols
- ❖ hardware, software

## Question:

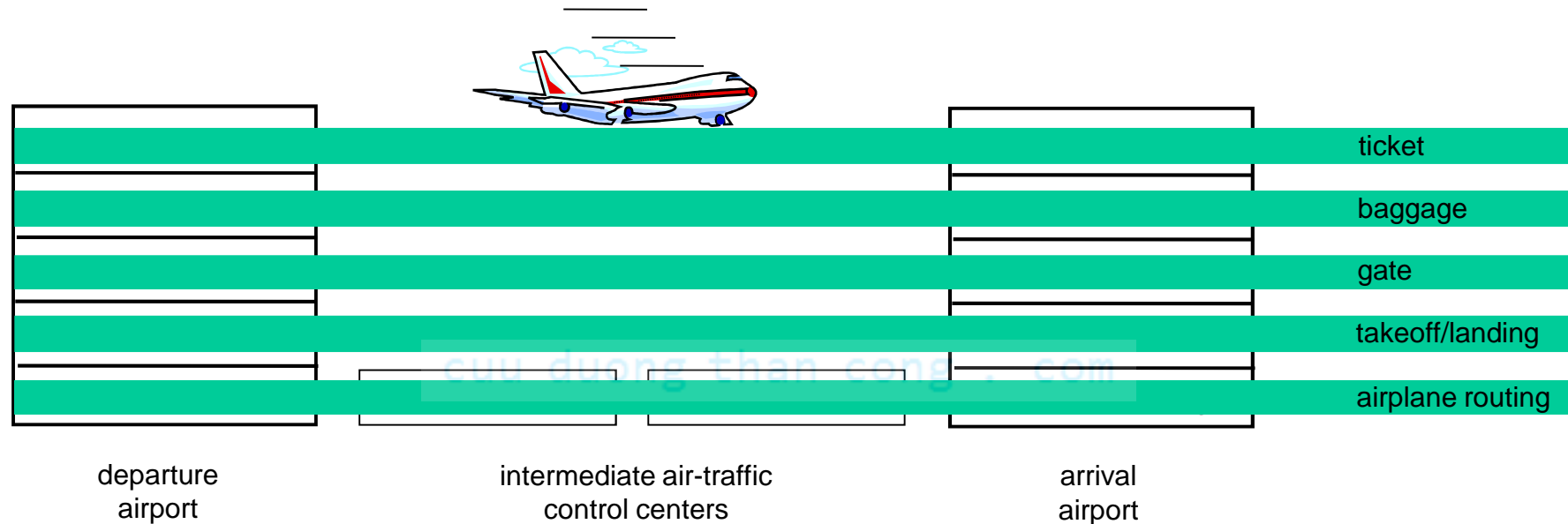
Có cách gì để *tổ chức* cấu trúc của mạng không?

# Organization of air travel



❑ Một chuỗi gồm nhiều bước

# Layering of airline functionality



**Layers:** mỗi tầng (layer) cài đặt một dịch vụ (service)

- ❖ Nhờ chính những hành động ngay tầng đó
- ❖ Nhờ những dịch vụ được cung cấp bởi các tầng bên dưới nó.

# Why layering?

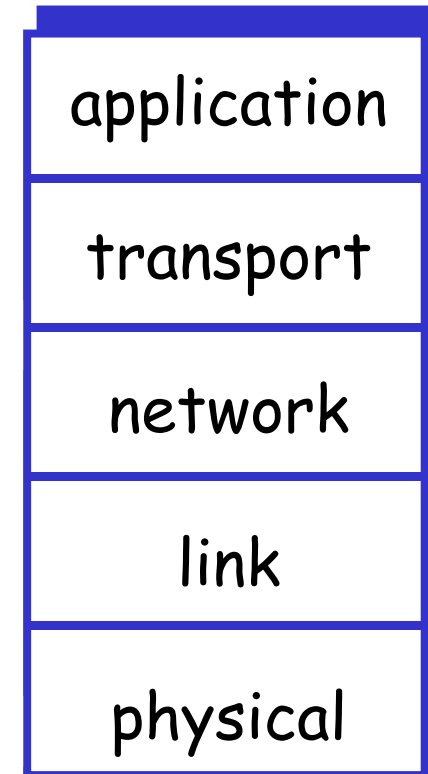
Đối phó với các hệ thống phức tạp:

- ❑ Cấu trúc rõ ràng cho phép định danh, mối quan hệ phức tạp giữa các thành phần hệ thống phức tạp
  - ❖ **Mô hình tham khảo** được phân tầng
- ❑ Module hóa giúp dễ bảo trì và cập nhật hệ thống
  - ❖ Việc thay đổi cách cài đặt dịch vụ của một tầng không ảnh hưởng đến phần còn lại của hệ thống

cuu duong than cong . com

# Internet protocol stack

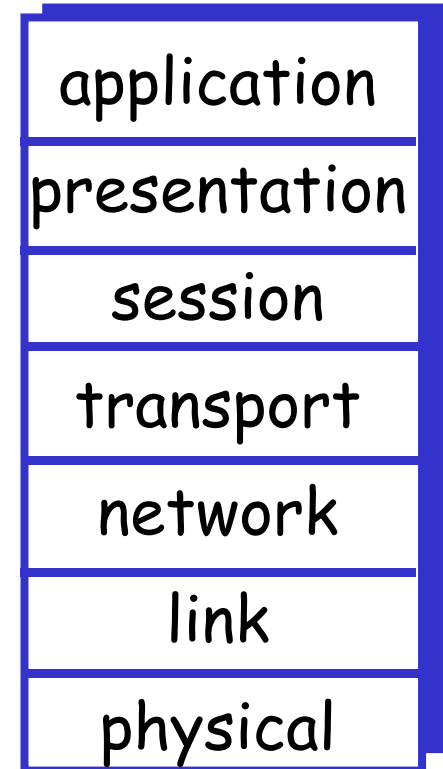
- ❑ **application:** cung cấp các ứng dụng mạng
  - ❖ FTP, SMTP, HTTP
- ❑ **transport:** truyền dữ liệu giữa các tiến trình (process)
  - ❖ TCP, UDP
- ❑ **network:** hướng (định tuyến) các datagrams đi từ nguồn đến đích
  - ❖ IP, routing protocols
- ❑ **link:** truyền dữ liệu giữa các phần tử mạng láng giềng nhau
  - ❖ PPP, Ethernet
- ❑ **physical:** truyền dòng bits “trên dây”



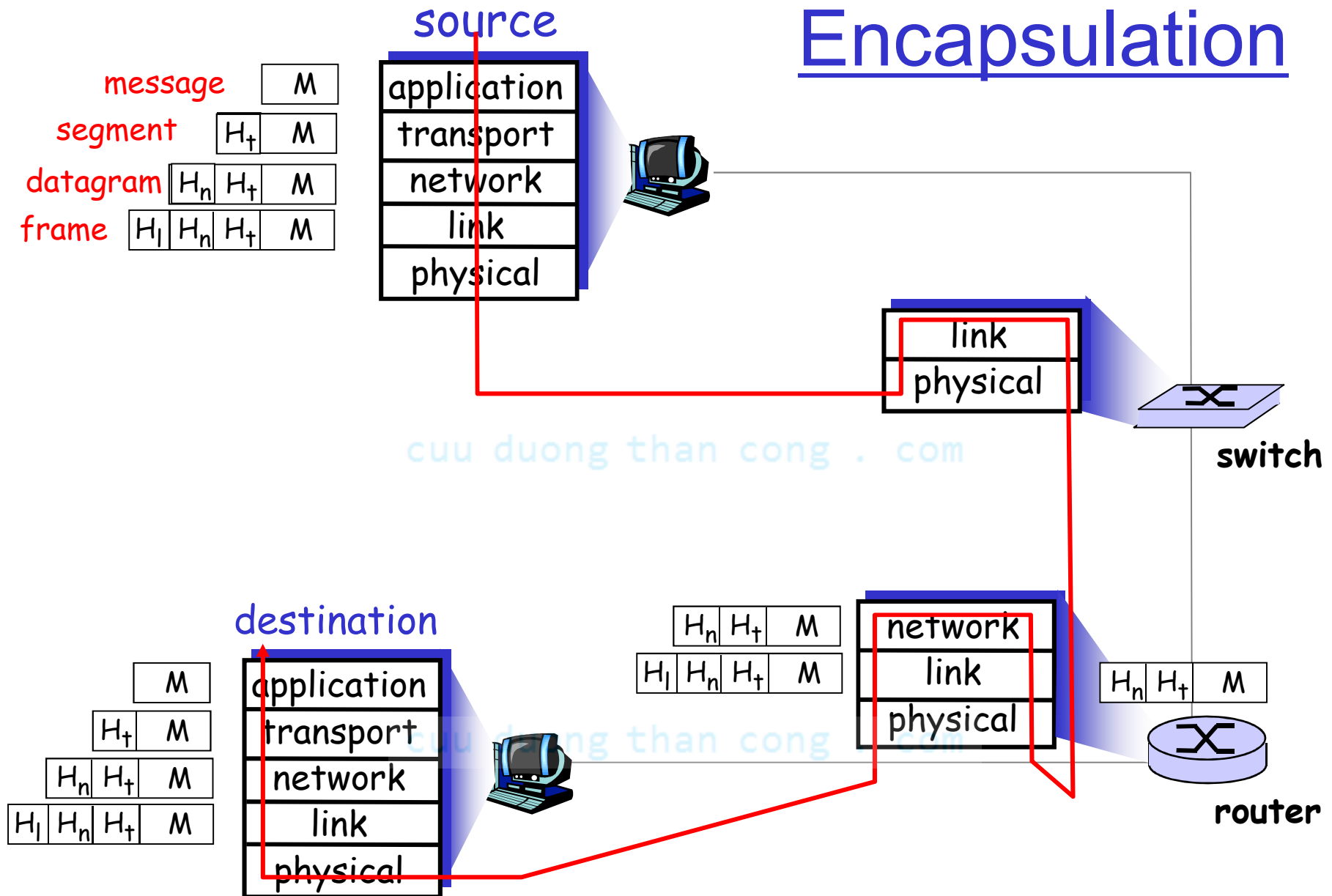


# ISO/OSI reference model

- ❑ **presentation:** cho phép các ứng dụng tạo ra các biểu diễn lại dữ liệu, e.g., mã hóa dữ liệu, nén dữ liệu, ...
- ❑ **session:** đồng bộ hóa, checkpointing, khôi phục các phiên trao đổi dữ liệu
- ❑ Chồng giao thức Internet “thiếu” các tầng này!
  - ❖ Các dịch vụ này, nếu cần, phải được cài đặt trong ứng dụng
  - ❖ Cần không?



# 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

- ❑ An ninh mạng nhằm nghiên cứu về:
  - ❖ Cách thức kẻ xấu tấn công vào MMT
  - ❖ Cách thức bảo vệ MMT khỏi các đợt tấn công
  - ❖ Cách thức thiết kế mạng để kháng với các đợt tấn công
- ❑ Ban đầu, Internet không được thiết kế với các ý định an ninh
  - ❖ *original vision*: “a group of mutually trusting users attacked to a transparent network” 😊
  - ❖ An ninh mạng cần được xem xét ở tất cả các tầng!

# Bad guys can put malware into hosts via Internet

- ❑ Malware có thể xâm nhập máy tính từ **virus**, **worm**, hoặc **trojan horse**
- ❑ **Spyware malware** có thể ghi nhận bàn phím, viếng thăm website, tải thông tin lên các site
- ❑ Các máy tính bị lây nhiễm có thể được kết nạp vào một botnet, được sử dụng cho các tấn công **spam** hoặc DDoS.
- ❑ Malware thường có khả năng tự nhân bản (**self-replicating**): từ một máy tính bị lây nhiễm, tìm kiếm các máy tính khác để lây nhiễm tiếp.

# Bad guys can put malware into hosts via Internet

## ❑ Trojan horse

- ❖ Phần ẩn của một vài phần mềm có ích.
- ❖ Hiện tại: dưới dạng các Active-X, plugin từ các trang Web

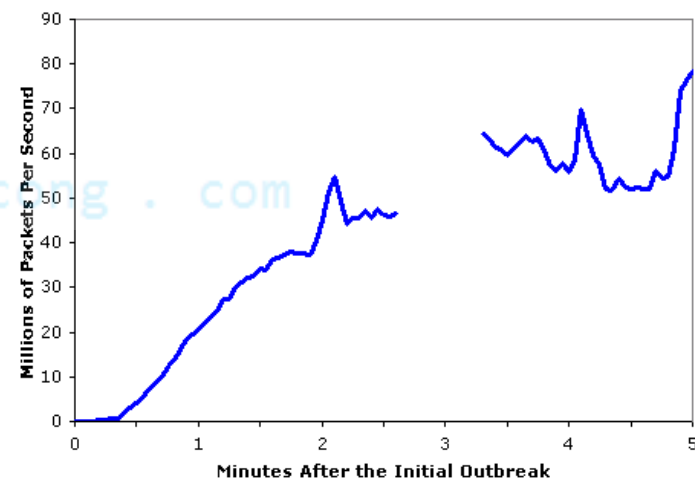
## ❑ Virus

- ❖ Gây lây nhiễm nhờ việc con người kích hoạt ứng dụng.
- ❖ Tự nhân bản: tự lây lan chính nó đến các file khác trong cùng máy

## ❑ Worm:

- ❖ Gây lây nhiễm bằng việc tấn công vào các lỗ hổng bảo mật, **ko cần người kích hoạt**
- ❖ Tự nhân bản: tự lây lan chính nó đến các máy tính khác

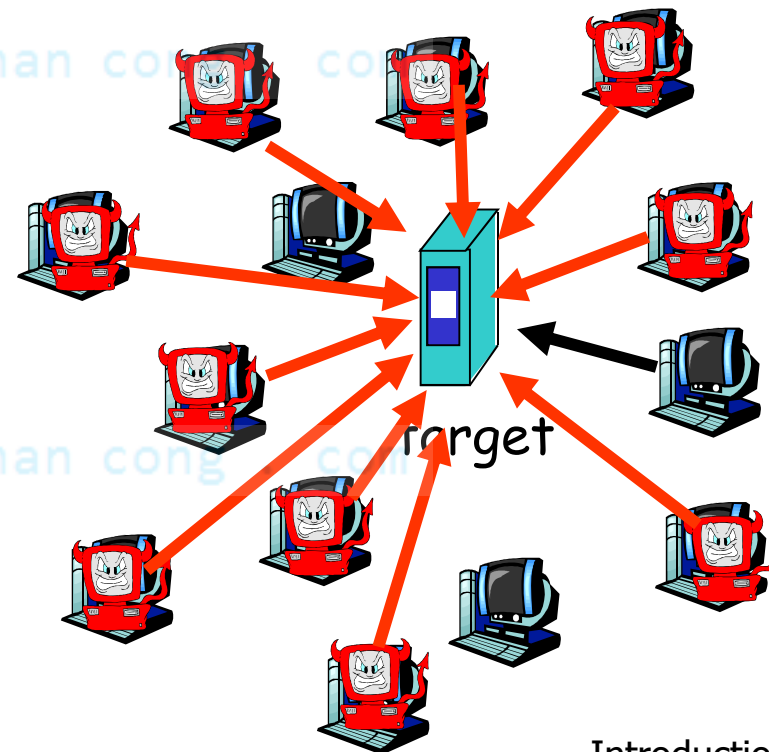
Sapphire Worm: aggregate scans/sec in first 5 minutes of outbreak (CAIDA, UWisc data)



# Bad guys can attack servers and network infrastructure

- ❑ Tấn công từ chối dịch vụ (Denial of service -DoS): kẻ tấn công sử dụng một số lượng lớn các truy cập hợp lệ làm cạn kiệt tài nguyên mạng (Server, băng thông)

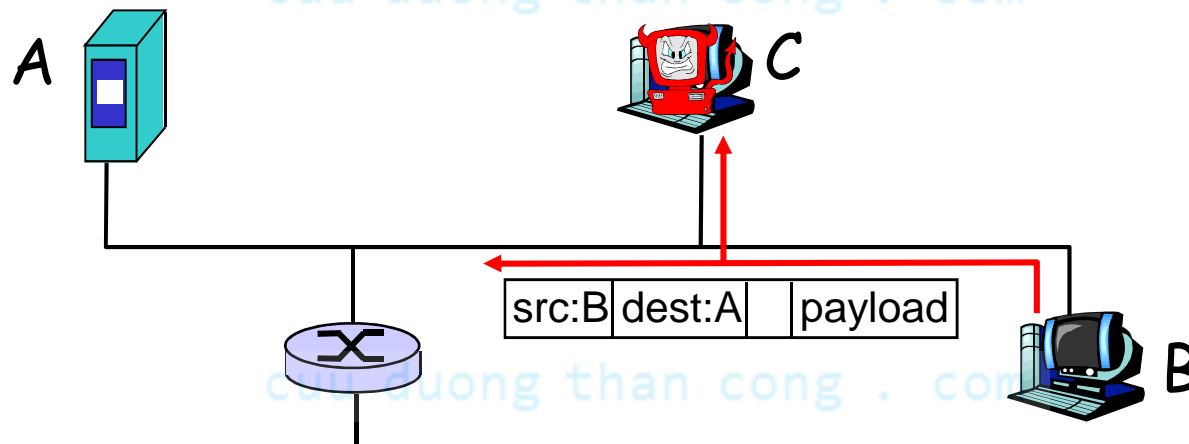
1. Chọn đích tấn công
2. Xâm nhập các máy tính khác từ mạng
3. Huy động các máy tính bị xâm nhập, đồng loạt gửi các gói tin đến máy bị tấn công



# 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

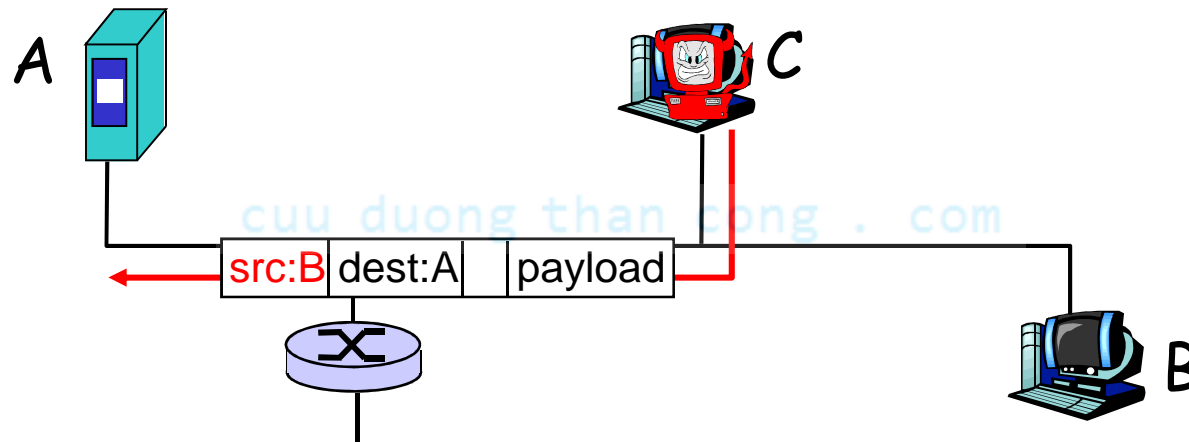


- ❖ Wireshark software used for end-of-chapter labs is a (free) packet-sniffer



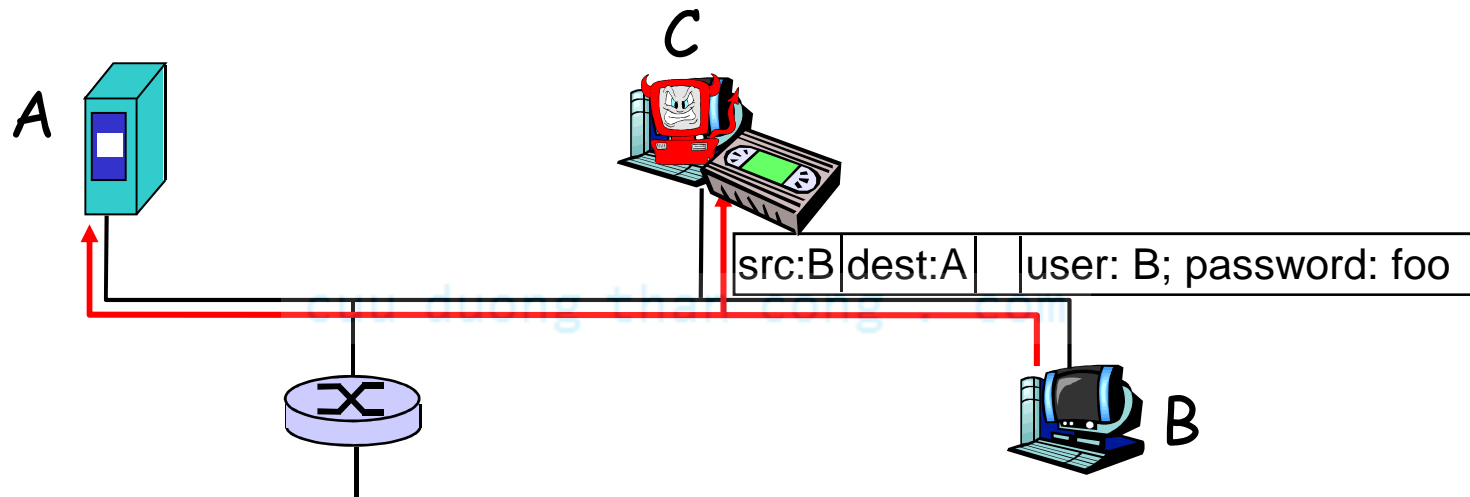
# The bad guys can use false source addresses

- ❑ *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



# Network Security

- ❑ more throughout this course
- ❑ chapter 8: focus on security
- ❑ cryptographic techniques: obvious uses and not so obvious uses

cuu duong than cong . com

cuu duong than cong . com

# 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

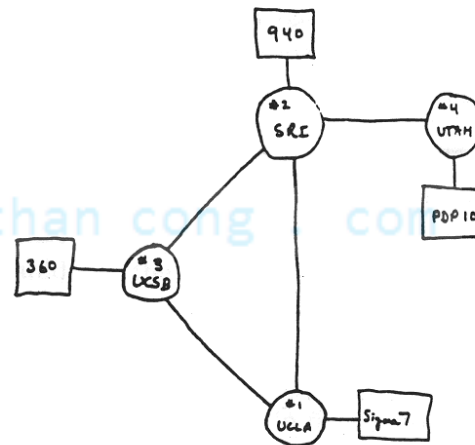
1.6 Networks under attack: security

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
- ❑ late 70'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: Cset, 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

## Covered a “ton” of material!

- ❑ 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

## You now have:

- ❑ context, overview, “feel” of networking
- ❑ more depth, detail *to follow!*