Nhập môn mạng máy tính

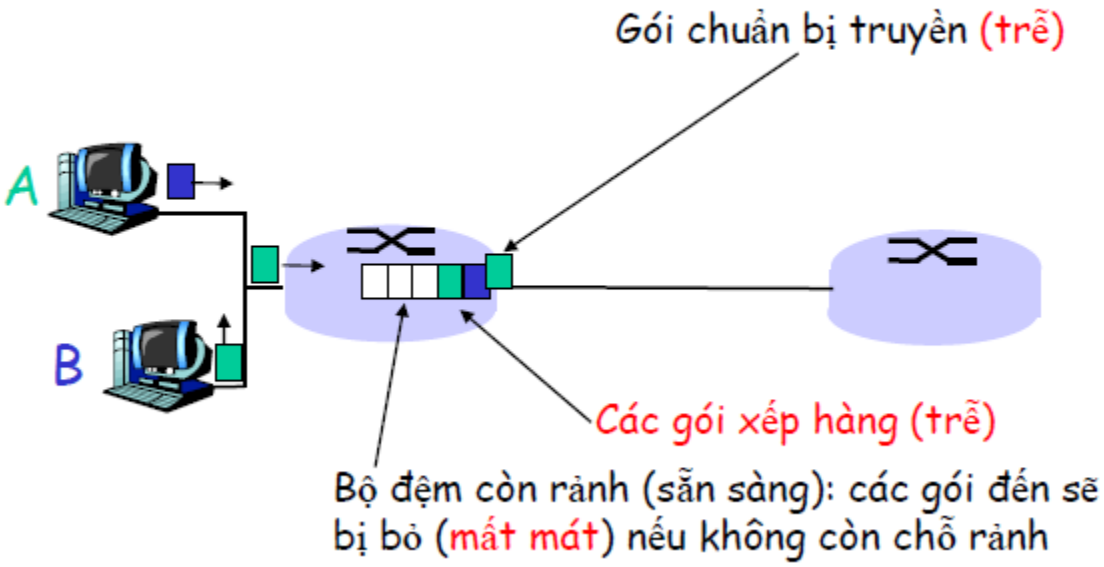
Chương 1: Giới thiệu (tiếp theo)

6. Việc trễ, mất mát dữ liệu và thông lượng

Các gói xếp hàng trong bộ nhớ đệm của router:

+ Các gói được chuyển đến router nhiều hơn khả năng xuất đi thì các gói sẽ xếp hàng đợi đến lượt được chuyển đi

+ Nếu buffers (bộ nhớ đệm) hết thì các gói tin đến sau sẽ bị mất



a) 4 nguyên nhân gây delay (trễ)

- Trễ do xử lý tại nút (nodal processing, $\mathbf{d_{proc}}$)

+ Kiểm tra lỗi

+ Xác định đường dẫn đích

+ Thời gian thường là vài mili giây hoặc ít hơn

- Trễ do xếp hàng (queueing delay, $\mathbf{d_{queue}}$)

+ Thời gian đợi để được truyền đi

+ Phụ thuộc vào mức độ tắc nghẽn của router

- Trễ khi truyền gói từ router vào đường dẫn (transmission delay, $\mathbf{d_{trans}}$)

+ L: kích thước gói (bits)

+ R: băng thông đường liên kết (bps)

=> $d_{trans} = L/R$

- Trễ khi lan truyền gói trong đường dẫn đến router tiếp theo (propagation delay, $\mathbf{d_{prop}}$)

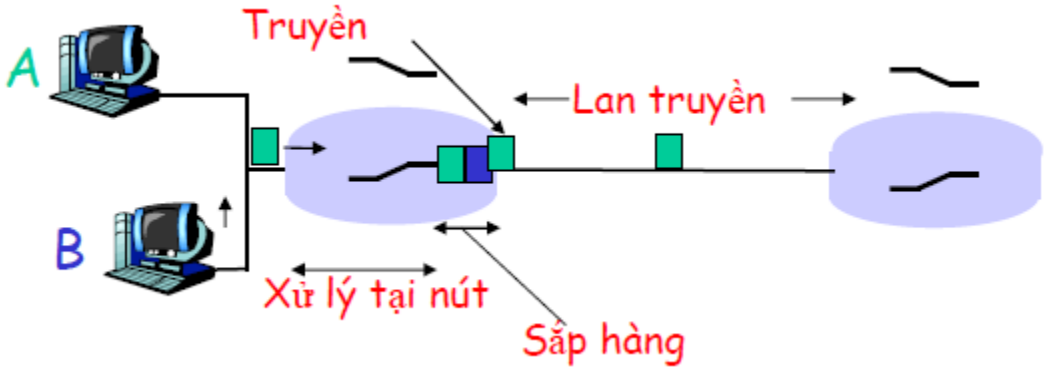
+ d: chiều dài đường dẫn vật lý

+ s: tốc độ lan truyền đến router tiếp theo (~2.10^8 m/s)

=> $d_{prop} = d/s$

+ Thời gian thường tầm vài micro giây hoặc vài trăm mili giây

*** $\mathbf{d_{trans}}$ và $\mathbf{d_{prop}}$ khác nhau**



d_{nodal} (trễ tại nút) = d_{proc} + d_{queue} + d_{trans} + d_{prop}

*** Trễ do xếp hàng:**

a: tốc độ gói tin đến trung bình

L.a/R ~ 0: trễ ít

L.a/R -> 1: trễ nhiều

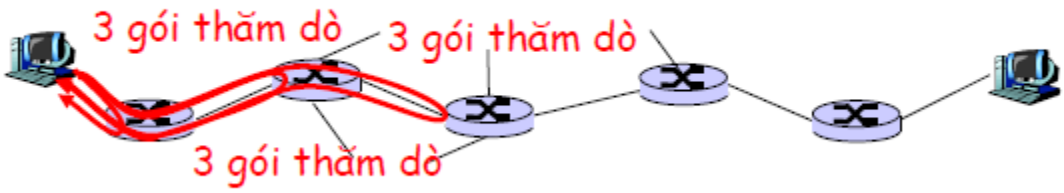
L.a/R > 1: trễ vô hạn

*** Chương trình Traceroute:** Tính độ trễ từ nguồn đến bộ định tuyến (router) thứ i trên quãng đường đến điểm đích. Với mọi i:

+ Gửi 3 gói tin đến router I trên đường tới đích

+ Router I sẽ trả về các gói cho người gửi

+ Tính thời gian giữa lúc gửi và nhận



b) Mất gói:

- Hàng đợi (bộ nhớ đệm) có khả năng xử lý hữu hạn (giới hạn dung lượng)

=> Những gói được đưa đến hàng đợi đã đầy sẽ bị mất

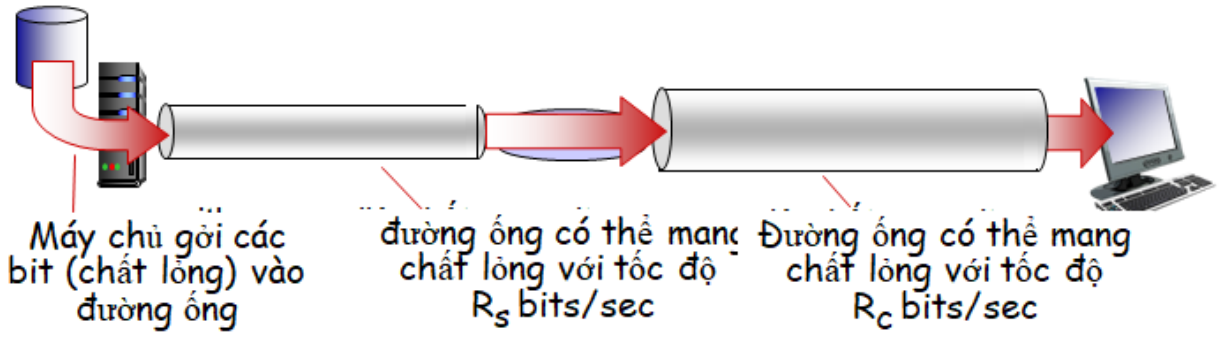
- Gói bị mất có thể được truyền lại từ router trước, hoặc hệ thống đầu cuối nguồn hoặc không được truyền lại

c) Thông lượng (Throughput)

- Thông lượng: Tốc độ (bits/đơn vị thời gian) mà bit được truyền giữa người gửi và người nhận, gồm:

+ Tốc độ tức thời: tốc độ tại một điểm thời gian nhất định

+ Tốc độ trung bình: Tốc độ trung bình trong một khoảng thời gian

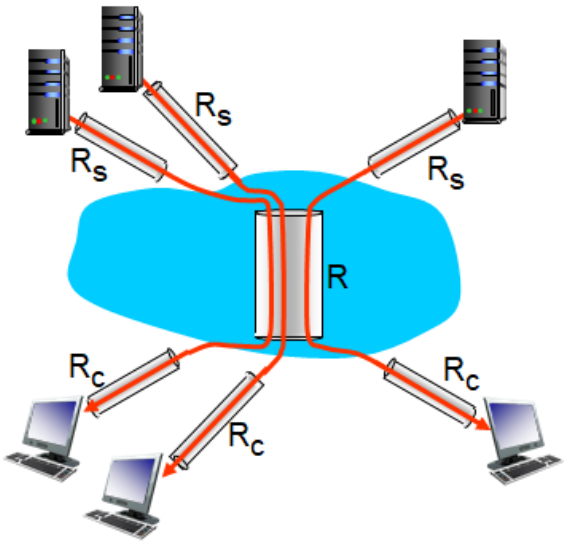


+ Nếu $R_s < R_c$, thông lượng trung bình giữa 2 đầu cuối là R_s (bottleneck link)

+ Ngược lại nếu $R_s > R_c$, thông lượng trung bình sẽ là R_c (bottleneck link)

* Liên kết nút cổ chai: Tốc độ truyền tin của liên kết nút cổ chai sẽ ảnh hưởng đến thông lượng của liên kết tổng từ đầu đến đích => thông lượng trung bình sẽ bằng thông lượng đoạn liên kết nút cổ chai.

* Trong mạng Internet:



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

+ Thông lượng cho mỗi kết nối sẽ bằng min{R_s,R_c,R/10}.

+ Trên thực tế R_s, R_c (access network) sẽ là bottleneck link.

7. Các lớp giao thức, mô hình dịch vụ

- Mục đích phân lớp giao thức:

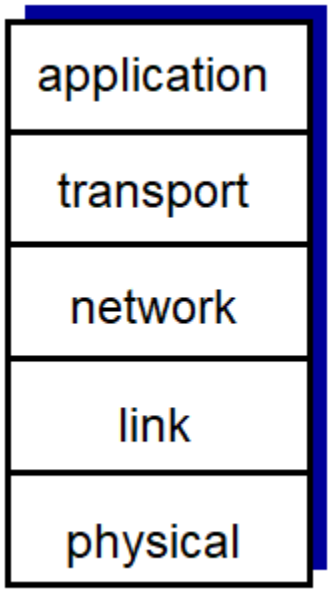
+ Các lớp được phân rõ ràng cho phép nhận dạng, biết được mối quan hệ giữa các phần trong mạng với nhau

+ Modun hóa giúp dễ dàng bảo trì, cập nhật phần mềm

Vd: Bảo trì một lớp sẽ không ảnh hưởng đến các lớp khác

- Các lớp giao thức của Internet:

*** Lớp trên sẽ sử dụng dịch vụ của các lớp dưới**



+ Application Layer: Hỗ trợ các ứng dụng mạng. Vd: FTP (hỗ trợ chuyển file), SMTP (hỗ trợ gửi email), HTTP (hỗ trợ duyệt web)

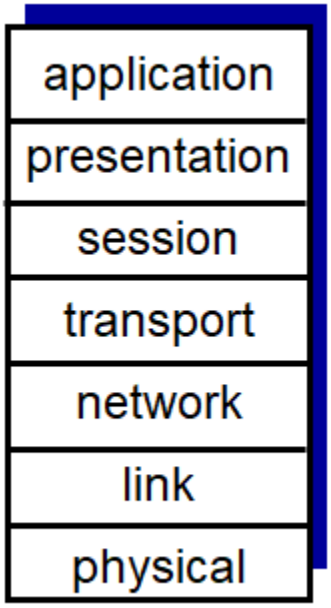
+ Transport Layer: Chuyển dữ liệu từ tiến trình này đến tiến trình kia. Vd: TCP, UDP

+ Network Layer: Định tuyến để các gói dữ liệu từ nguồn đến được đích. Vd: IP, các giao thức định tuyến

+ Link Layer: Chuyển dữ liệu giữa các thành phần mạng lân cận với nhau. Vd: Ethernet, Wifi, PPP

+ Physical Layer: Các bit được vận chuyển trên đường dây. Vd: cáp quang, cáp đồng trục…

- Mô hình tham chiếu ISO/OSI



+ Presentation: cho phép ứng dụng giải thích ý nghĩa của dữ liệu. Vd: nén, mã hóa và những quy trình riêng biệt

+ Session: Đồng bộ hóa, chịu lỗi, phục hồi việc trao đổi dữ liệu

8. An toàn mạng

- Gửi **Malware** (phần mềm độc hại) đến thiết bị người dùng qua Internet

Malware có thể xâm nhập qua:

+ virus: truyền nhiễm tự nhân đôi thông qua thực thi/mở một đối tượng nào đó (vd: tệp đính kèm trong email)

+ worm: truyền nhiễm tự nhân đôi thông qua một đối tượng được thiết bị người dùng tiếp nhận thụ động (không phải chủ động tải/ mở file)

Spyware Malware có khả năng ghi lại các phím người dùng đã nhập, biết các website đã truy cập và gửi thông tin về trang thu thập

Hệ thống đầu cuối bị nhiễm malware có thể bị đưa vào botnet (mạng các máy tính bị chiếm quyền điều khiển) dùng để spam, DdoS.

- **Tấn công máy chủ, hạ tầng mạng**:

Denial of Services (DoS): kẻ xấu làm tài nguyên (sever, băng thông) bị quá tải và không hoạt động được bằng lưu lượng truy cập giả

1. Chọn mục tiêu

2. Chiếm quyền các thiết bị lân cận (Botnet)

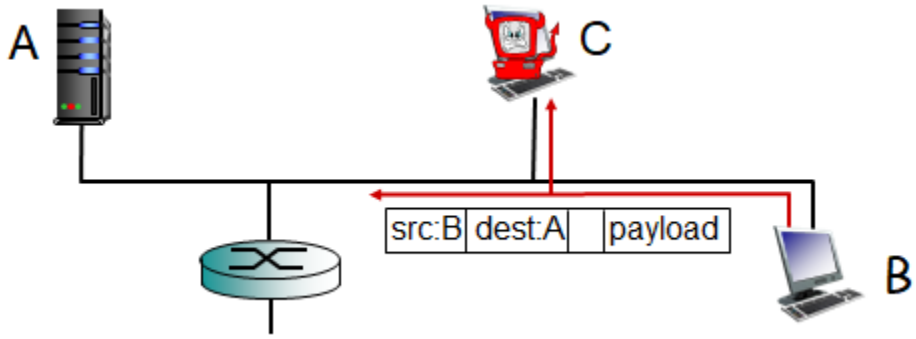
3. Gởi các gói tin đến mục tiêu từ Botnet

* xem wire shark

- **Packet "sniffing"** (đánh hơi gói tin):

+ Thông qua Ethernet, mạng không dây

+ Kẻ xấu ghi lại tất cả các gói tin được truyền qua đường mạng (password, tin nhắn…)



* xem wire shark

- **IP spoofing:** gửi gói tin với địa chỉ nguồn giả