



Computer Networking: A revision

NT101 – NETWORK SECURITY

Giảng viên: Nghi Hoàng Khoa | khoanh@uit.edu.vn

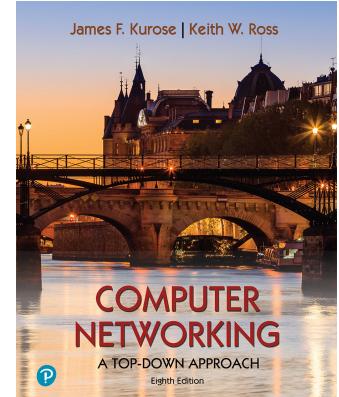


Outline



- **Mạng máy tính: xem lại**
 - Kiến trúc Internet
 - TCP/IP – Các tầng OSI
 - Tổng quan về bảo mật mạng

Slides are adapted from:
Computer Networking: A Top-Down Approach - 8th edition
Jim Kurose, Keith Ross
Pearson, 2020



Internet: xem nhanh



Internet: góc nhìn về “nuts and bolts”



Hàng tỷ thiết bị máy tính
được kết nối :

- **hosts** = end systems
- running network **apps** at Internet's “edge”



Packet switches: chuyển
tiếp gói tin (chunks of data)

- routers, switches



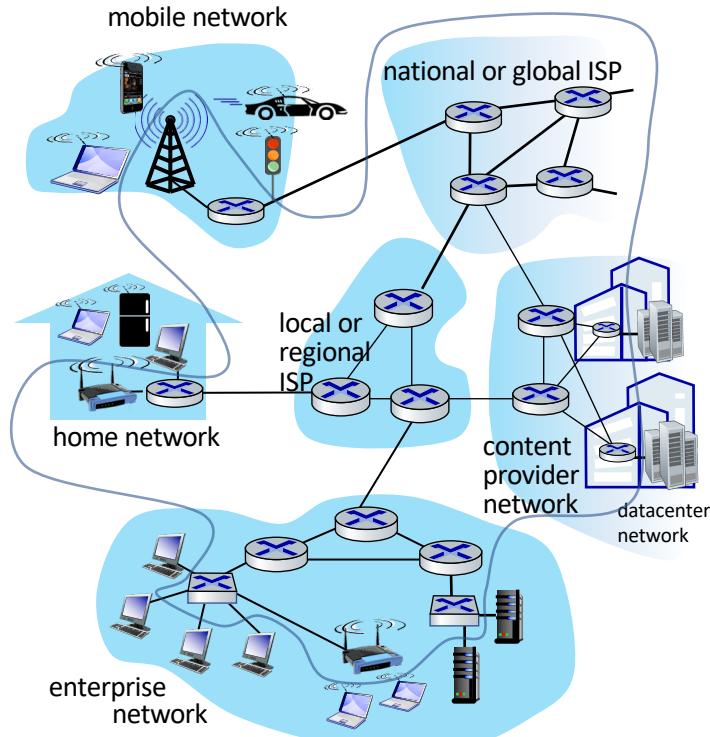
Communication links

- quang, đồng, radio, vệ tinh
- Tốc độ truyền tải: *bandwidth*



Networks

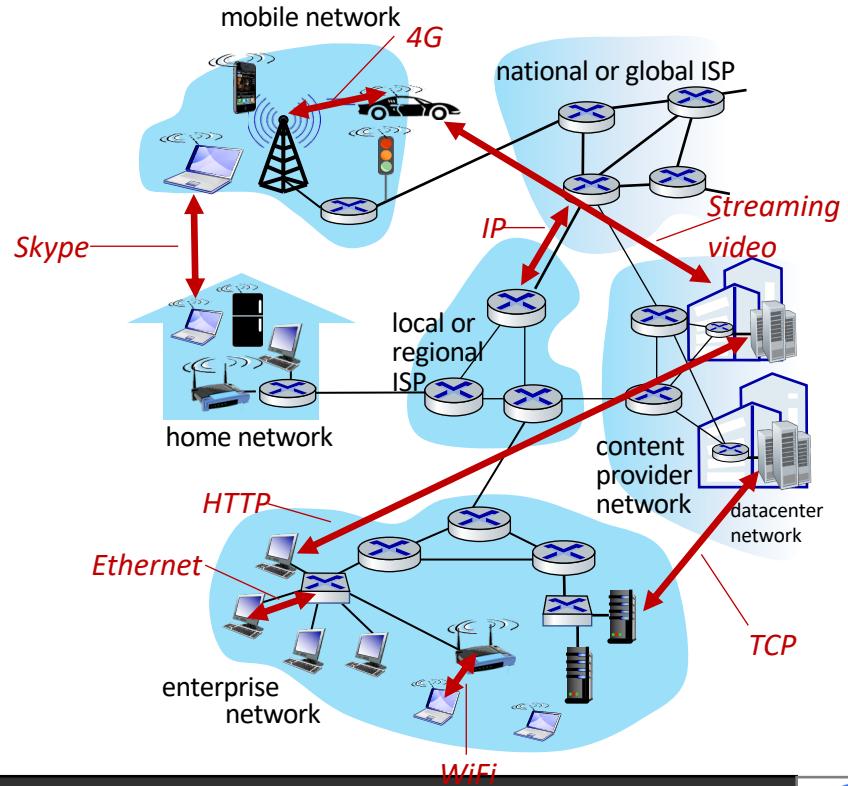
- Tập hợp các thiết bị, bộ định tuyến, liên kết : được quản lý bởi một tổ chức



Internet: góc nhìn về “nuts and bolts”

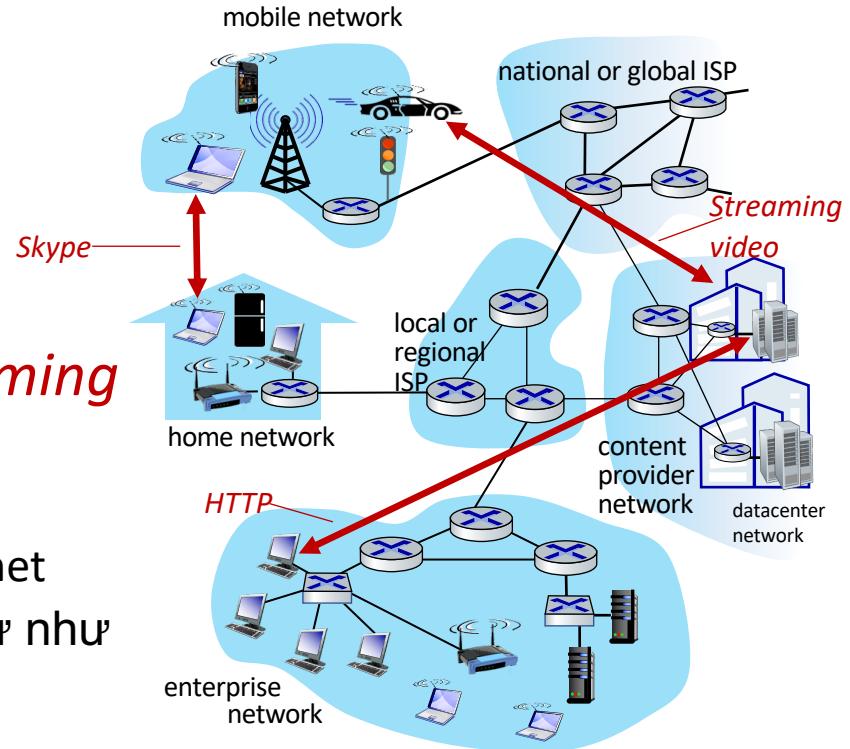


- *Internet: “network of networks”*
 - ISPs được kết nối với nhau
- *protocols ở khắp mọi nơi*
 - điều khiển gửi, nhận tin nhắn
 - e.g., HTTP (Web), streaming video, Skype, TCP, IP, WiFi, 4G, Ethernet
- *Tiêu chuẩn Internet*
 - RFC: Request for Comments
 - IETF: Internet Engineering Task Force



Internet : góc nhìn về “services”

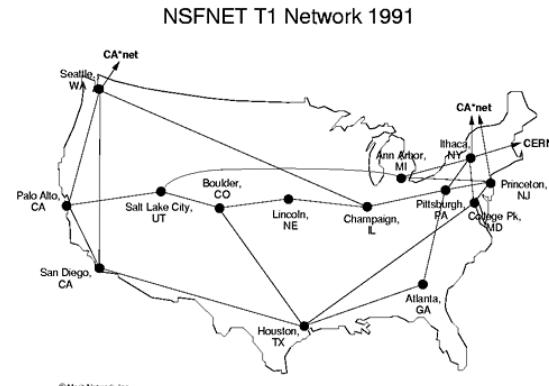
- **Cơ sở hạ tầng (Infrastructure)** cung cấp dịch vụ cho các ứng dụng:
 - Web, streaming video, multimedia teleconferencing, email, games, e-commerce, social media, interconnected appliances, ...
- Cung cấp giao diện lập trình (**programming interface**) cho các ứng dụng phân tán
 - “hooks” cho phép gửi / nhận ứng dụng để “connect”, sử dụng dịch vụ truyền tải Internet
 - cung cấp các tùy chọn dịch vụ, tương tự như dịch vụ bưu chính



Lịch sử Internet



- 1980-1990: các giao thức mới, sự gia tăng của các mạng lưới
 - 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
- Mạng quốc gia mới : CSnet, BITnet, NSFnet, Minitel
- 100.000 hosts được kết nối với liên hiệp các mạng



Lịch sử Internet



- 2005 - đến nay: *scale, SDN, mobility, cloud*
 - Triển khai điểm truy băng thông rộng cho các hộ gia đình (10-100Mbps)
 - 2008: software-defined networking (SDN)
 - Sự phô biến ngày càng tăng của truy cập không dây tốc độ cao (4G/5G, WiFi)
 - Các nhà cung cấp dịch vụ (Google, FB, Microsoft) tạo mạng của riêng họ
 - bỏ qua Internet thương mại để kết nối “close” với người dùng cuối, cung cấp quyền truy cập “instantaneous” vào mạng xã hội, tìm kiếm, nội dung video,...
 - Doanh nghiệp triển khai dịch vụ trên “cloud” (ví dụ Amazon Web Services, Microsoft Azure)
 - Sự gia tăng của điện thoại thông minh: di động nhiều hơn thiết bị cố định trên Internet (2017)
 - ~ 18B thiết bị được kết nối với Internet (2017)

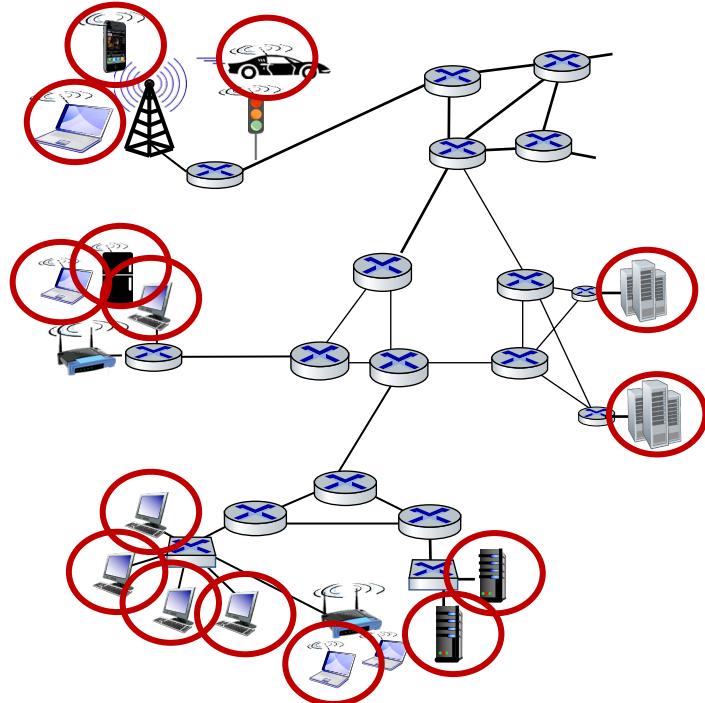


Một cái nhìn sâu hơn về cấu trúc Internet



Network edge (mạng biên):

- hosts: clients và servers
- máy chủ thường ở trung tâm dữ liệu



Một cái nhìn sâu hơn về cấu trúc Internet

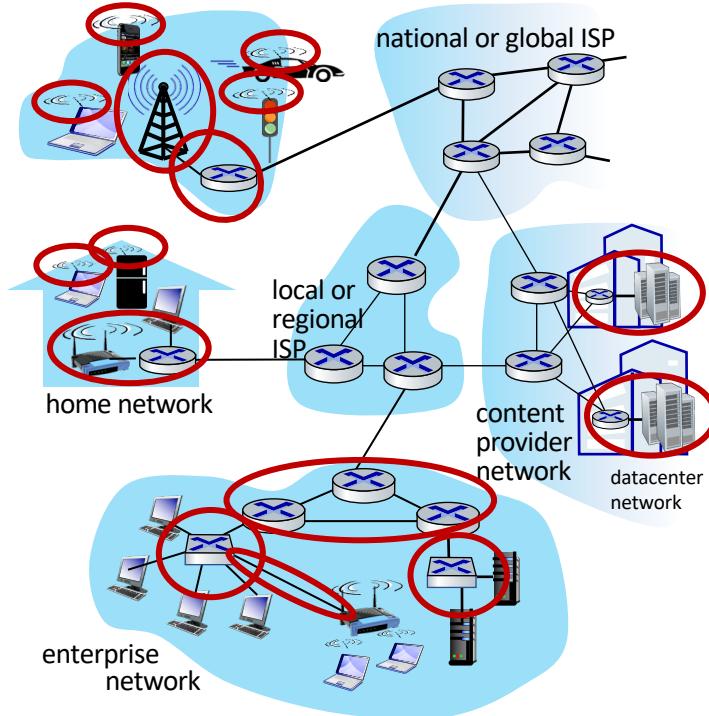


Network edge:

- hosts: clients and servers
- servers often in data centers

Access networks, physical media (truy cập mạng, phương tiện vật lý):

- Wired (dây), wireless (không dây) communication links



Một cái nhìn sâu hơn về cấu trúc Internet



Network edge:

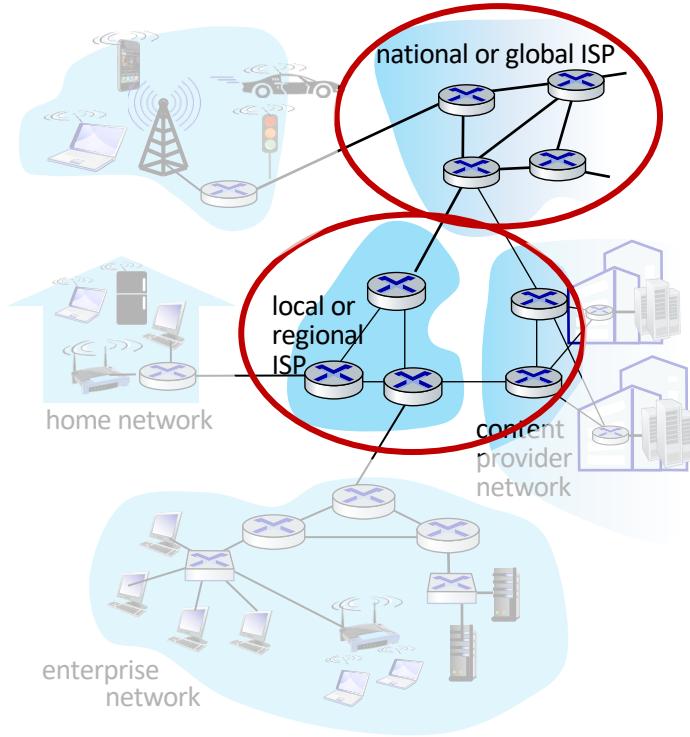
- hosts: clients and servers
- servers often in data centers

Access networks, physical media:

- wired, wireless communication links

Network core:

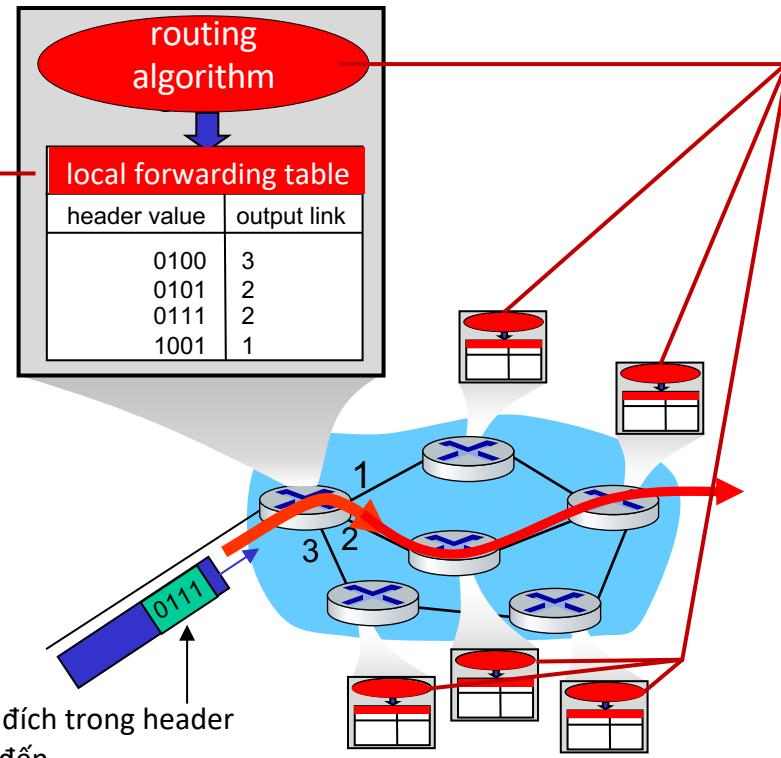
- bộ định tuyến được kết nối với nhau (routers)
- mạng lưới (network of networks)



Hai chức năng lõi của mạng

Forwarding:

- aka “switching”
- Hành động *local* : di chuyển các packet đến từ liên kết đầu vào của bộ định tuyến đến liên kết đầu ra bộ định tuyến thích hợp



Routing:

- Hành động *global* : xác định đường dẫn nguồn-đích được thực hiện bởi các packet
- các giải thuật định tuyến

Hai chức năng lõi của mạng



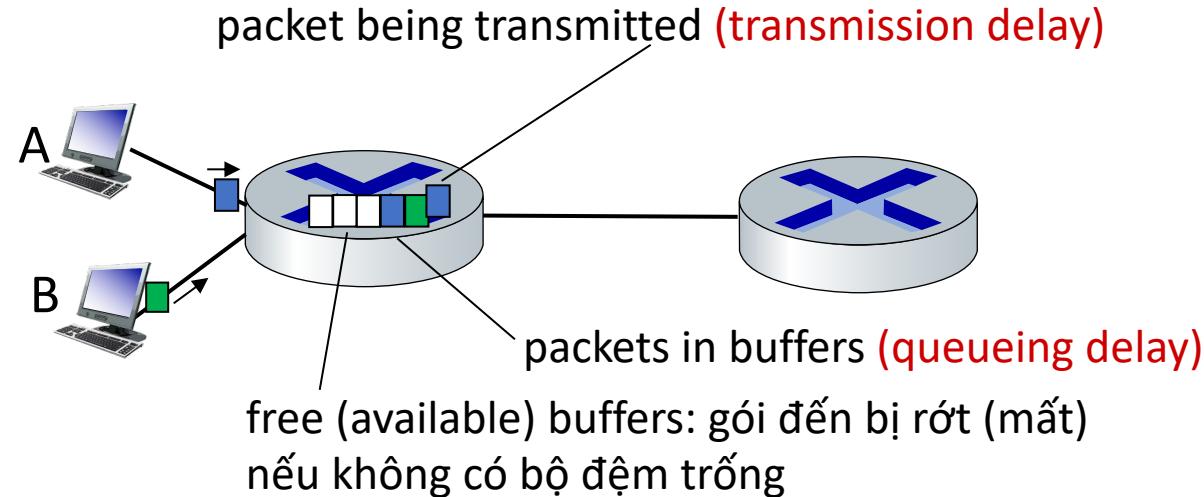
Hai chức năng lõi của mạng



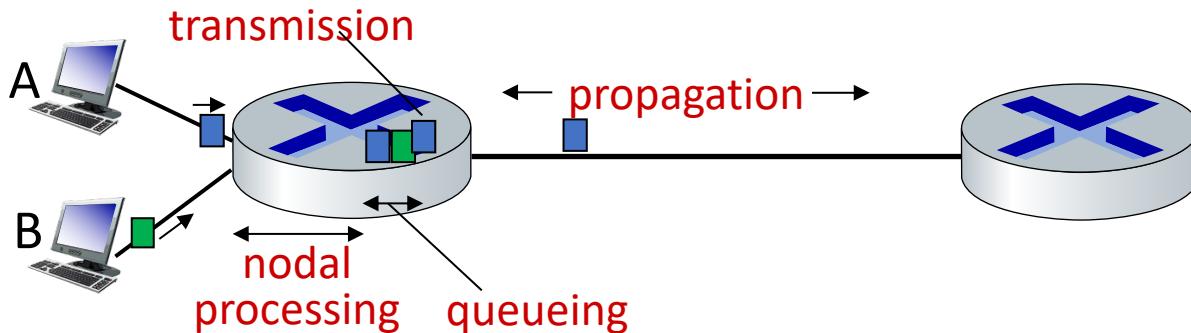
Bằng cách nào để xảy ra hiện tượng trễ và mất gói tin?



- Packet xếp vào hàng đợi trong bộ đệm bộ định tuyến, chờ đến lượt truyền
 - độ dài hàng đợi tăng lên khi tỷ lệ đến để liên kết (tạm thời) vượt quá khả năng liên kết đầu ra
 - mất packet xảy ra khi bộ nhớ để giữ các packet được xếp hàng chờ đầy



Packet delay: four sources



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

d_{proc} : nodal processing

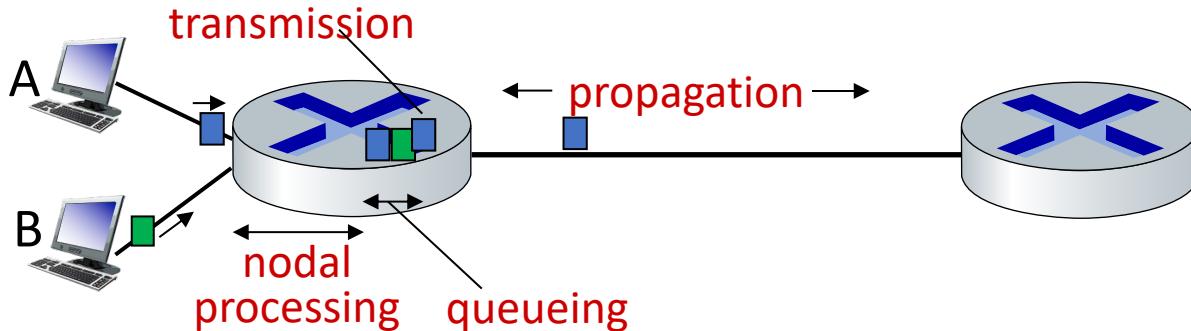
- Kiểm tra bit lỗi
- Xác định đầu ra liên kết
- typically < microsecs

d_{queue} : queueing delay

- Thời gian chờ đợi liên kết đầu ra để truyền
- Phụ thuộc vào mức độ nghẽn của bộ định tuyến



Packet delay: four sources



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

d_{trans} : transmission delay:

- L : packet length (bits)
- R : link transmission rate (bps)
- $d_{\text{trans}} = L/R$

d_{trans} and d_{prop}
very different

d_{prop} : propagation delay:

- d : length of physical link
- s : propagation speed ($\sim 2 \times 10^8$ m/sec)
- $d_{\text{prop}} = d/s$

Protocol stack: xem lại



Tại sao phân lớp?

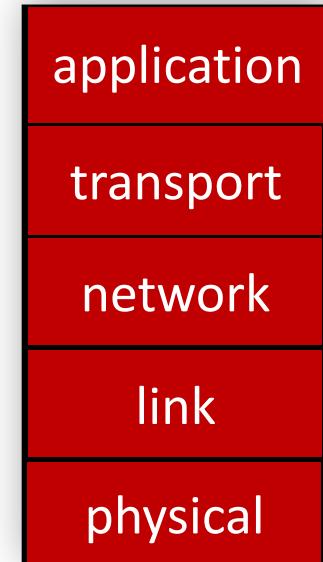
- Phương pháp tiếp cận để thiết kế / thảo luận các hệ thống phức tạp:
 - Cấu trúc rõ ràng cho phép xác định, mối quan hệ của các phần của hệ thống
 - layered **reference model** for discussion
 - Mô-đun hóa giúp dễ dàng bảo trì, cập nhật hệ thống
 - change in layer's service implementation: transparent to rest of system
 - ví dụ: thay đổi trong thủ tục cổng không ảnh hưởng đến phần còn lại của hệ thống



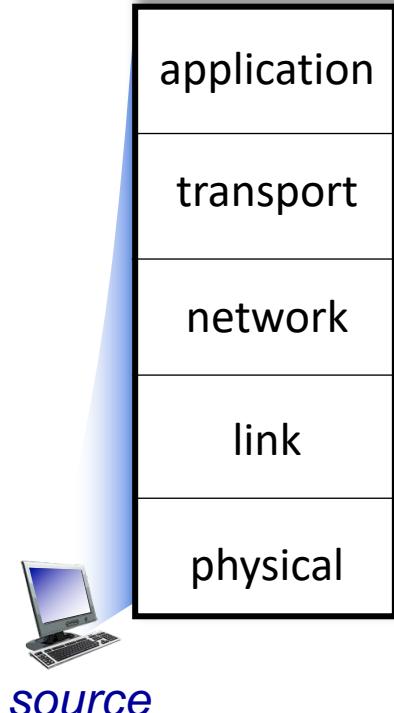
Layered Internet protocol stack



- **application:** hỗ trợ các ứng dụng mạng
 - HTTP, IMAP, SMTP, DNS
- **transport:** quá trình xử lý chuyển dữ liệu
 - TCP, UDP
- **network:** định tuyến các diagram dữ liệu từ nguồn đến đích
 - IP, routing protocols
- **link:** dữ liệu giữa các thành phần mạng lân cận
 - Ethernet, 802.11 (WiFi), PPP
- **physical:** bits “on the wire”



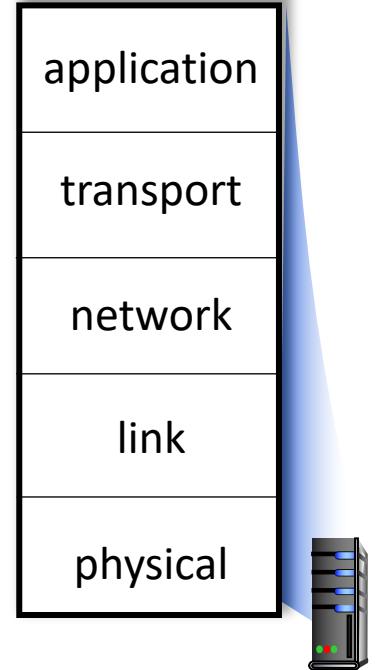
Services, Layering and Encapsulation



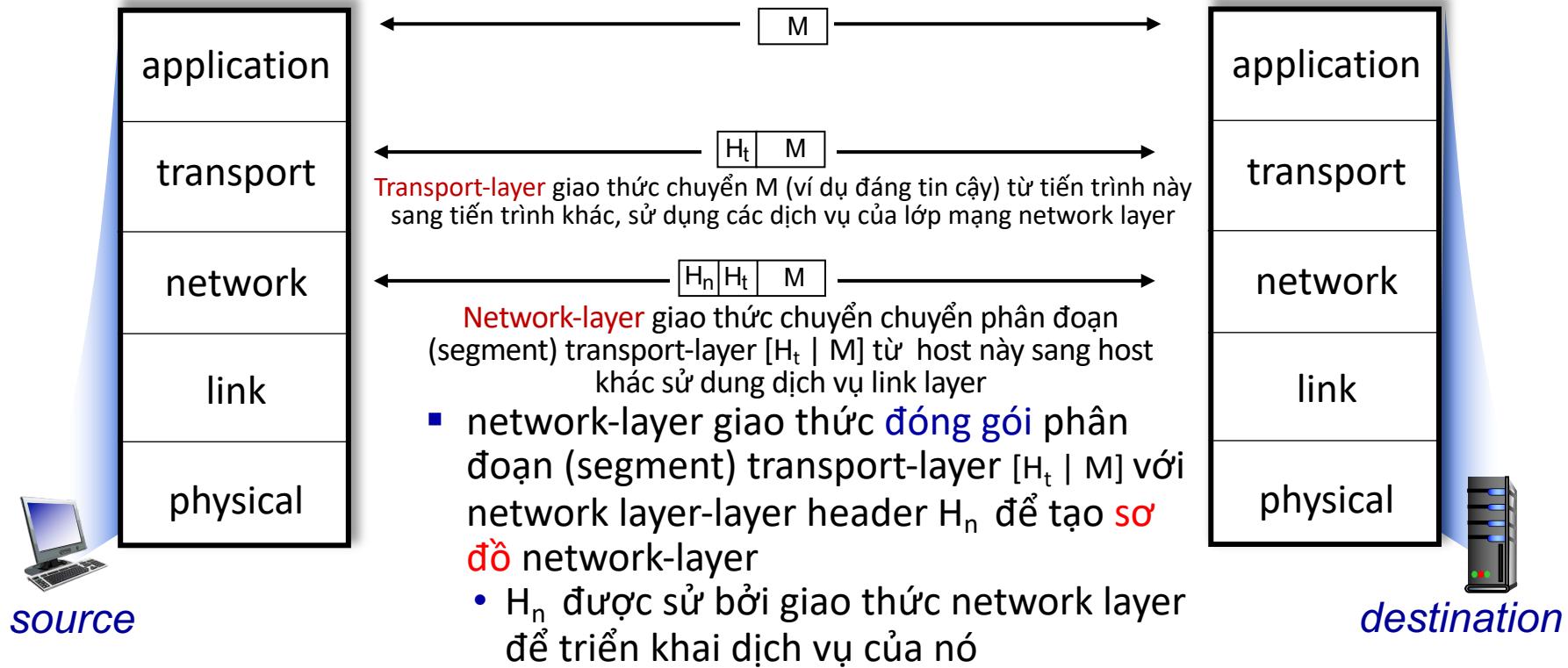
Application dùng trao đổi thông điệp để thực hiện một số dịch vụ ứng dụng bằng cách sử dụng các dịch vụ của transport layer

Transport-layer giao thức vận chuyển M (ví dụ đáng tin cậy) từ tiến trình này sang tiến trình khác, sử dụng các dịch vụ của network layer

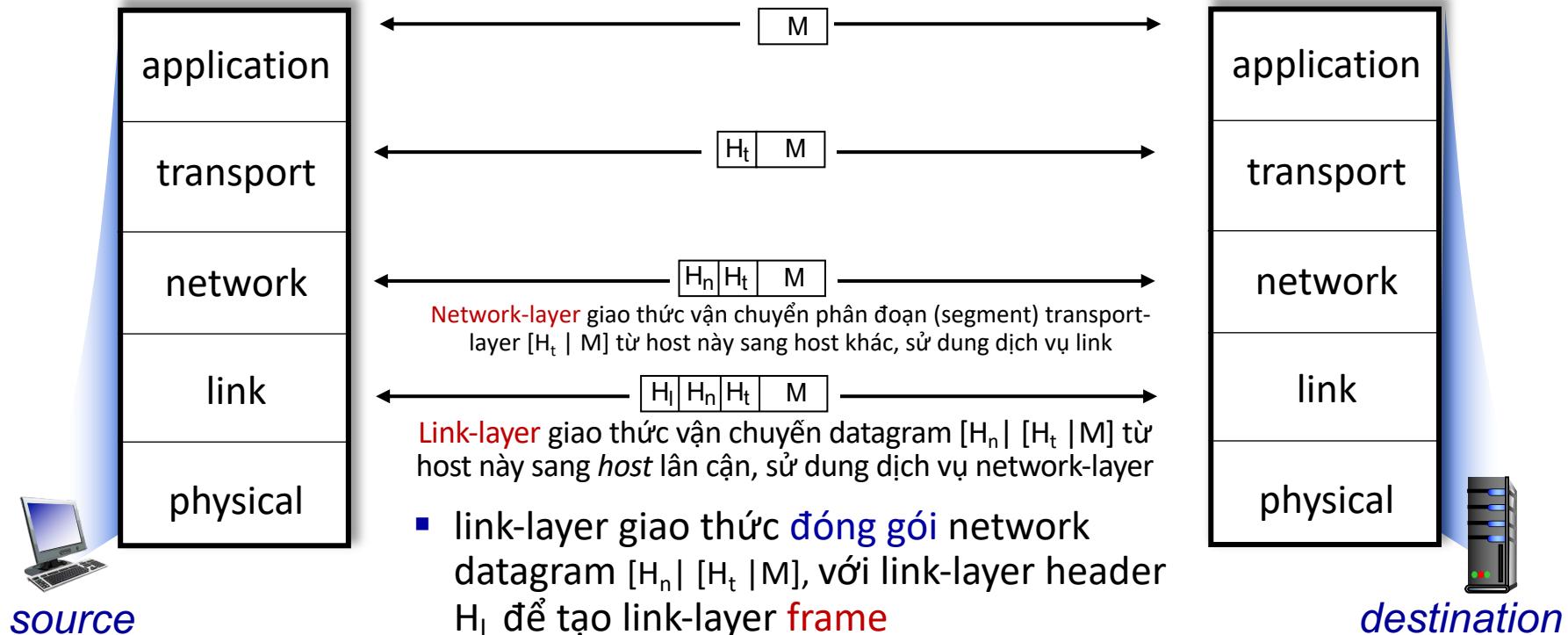
- Giao thức transport-layer **đóng gói** thông điệp application-layer, M, với *transport layer-layer header* H_t để tạo **transport-layer segment (phân đoạn)**
 - H_t được sử dụng bởi giao thức transport layer để triển khai dịch vụ của nó



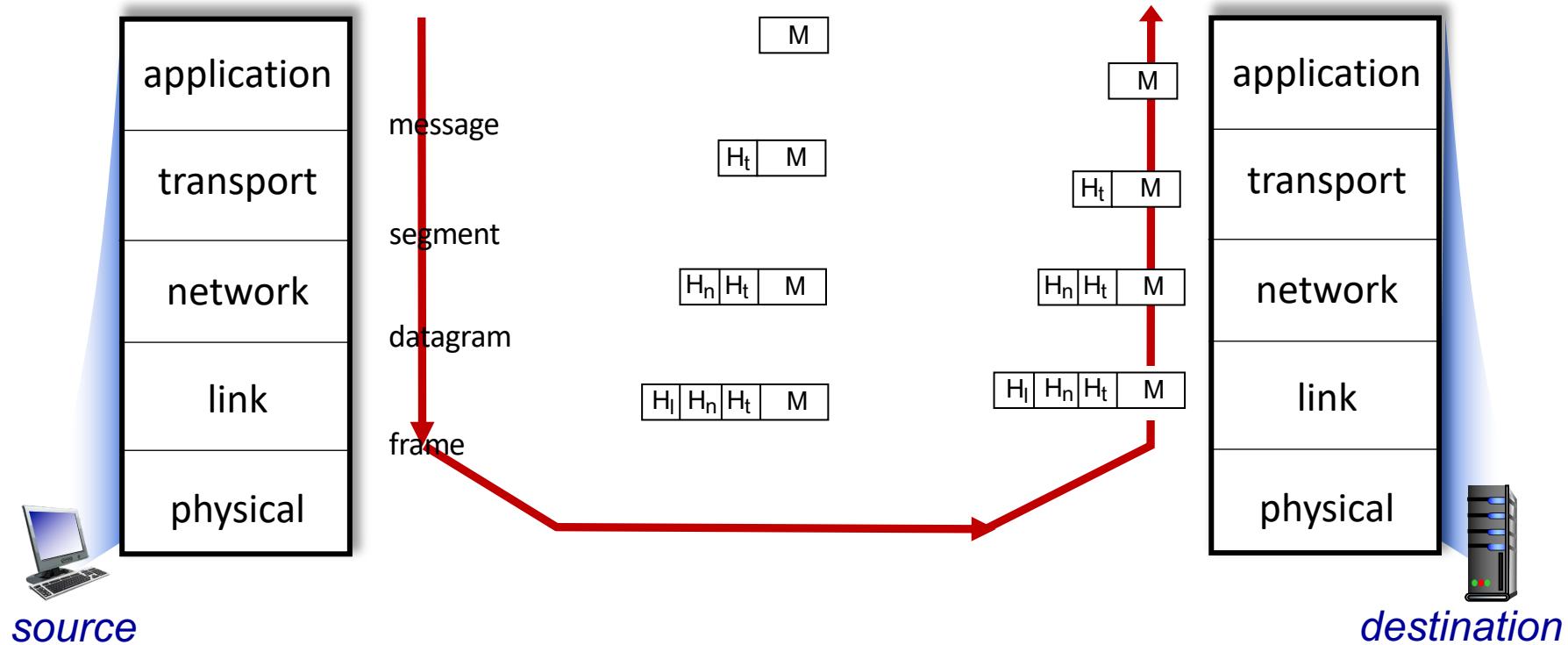
Services, Layering and Encapsulation



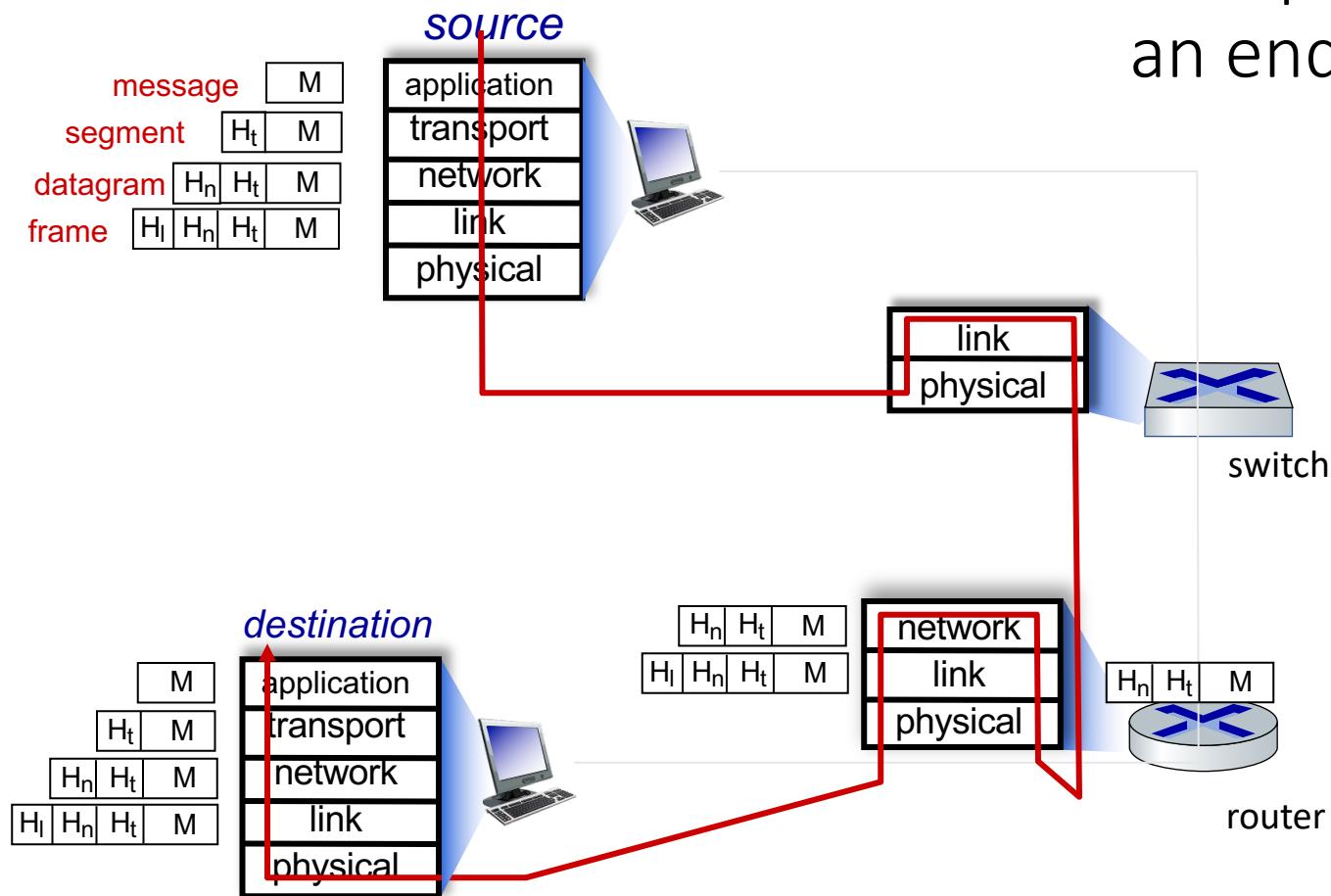
Services, Layering and Encapsulation



Services, Layering and Encapsulation



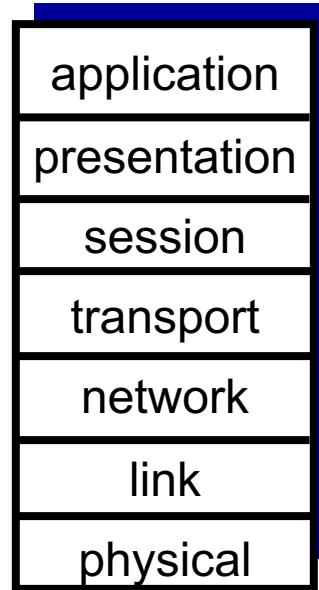
Encapsulation: an end-end view



ISO/OSI reference model

Không tìm thấy 2 layer trong Internet protocol stack!

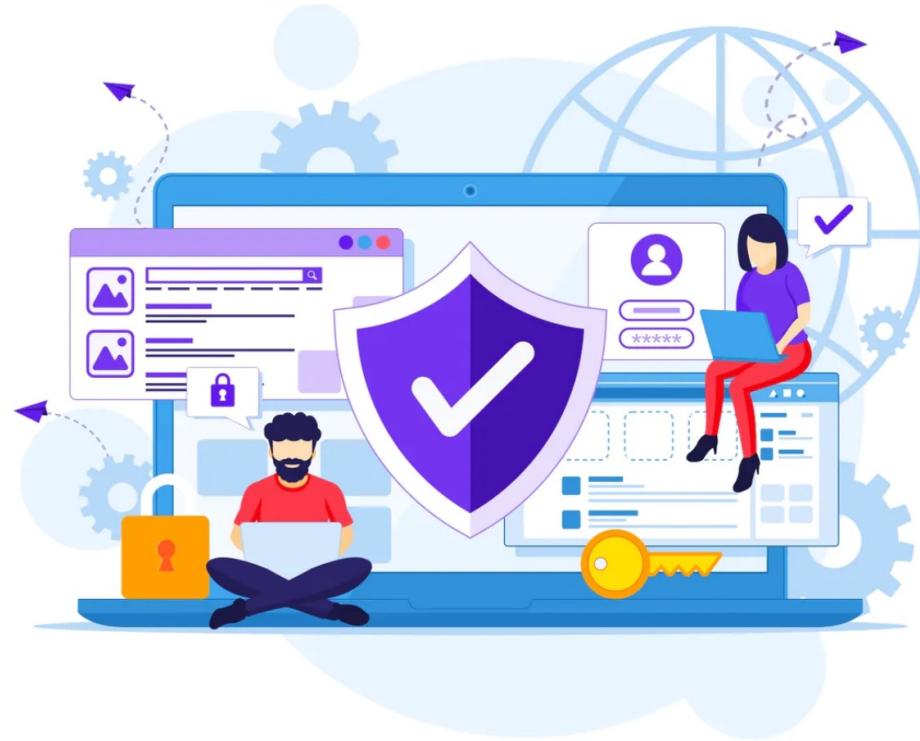
- ***presentation:*** cho phép các ứng dụng diễn giải ý nghĩa của dữ liệu, ví dụ: mã hóa, nén, các quy ước dành riêng cho máy
- ***session:*** đồng bộ hóa, kiểm tra, phục hồi trao đổi dữ liệu
- Internet stack “missing” these layers!
 - các dịch vụ này, nếu cần, phải được triển khai trong ứng dụng
 - needed?



The seven layer OSI/ISO reference model



Bảo mật mạng: sơ lược



Bảo mật mạng



- Internet ban đầu không được thiết kế với (nhiều) tính bảo mật
 - *original vision:* “a group of mutually trusting users attached to a transparent network” 😊
 - Các nhà thiết kế giao thức Internet chơi trò “catch-up”
 - Cân nhắc bảo mật trong tất cả các lớp!
- Nay giờ chúng ta cần nghĩ về:
 - làm thế nào kẻ xấu có thể tấn công mạng máy tính
 - làm thế nào chúng ta có thể bảo vệ các mạng chống lại các cuộc tấn công
 - làm thế nào để thiết kế các kiến trúc miễn nhiễm với các cuộc tấn công





Bảo mật mạng là gì?

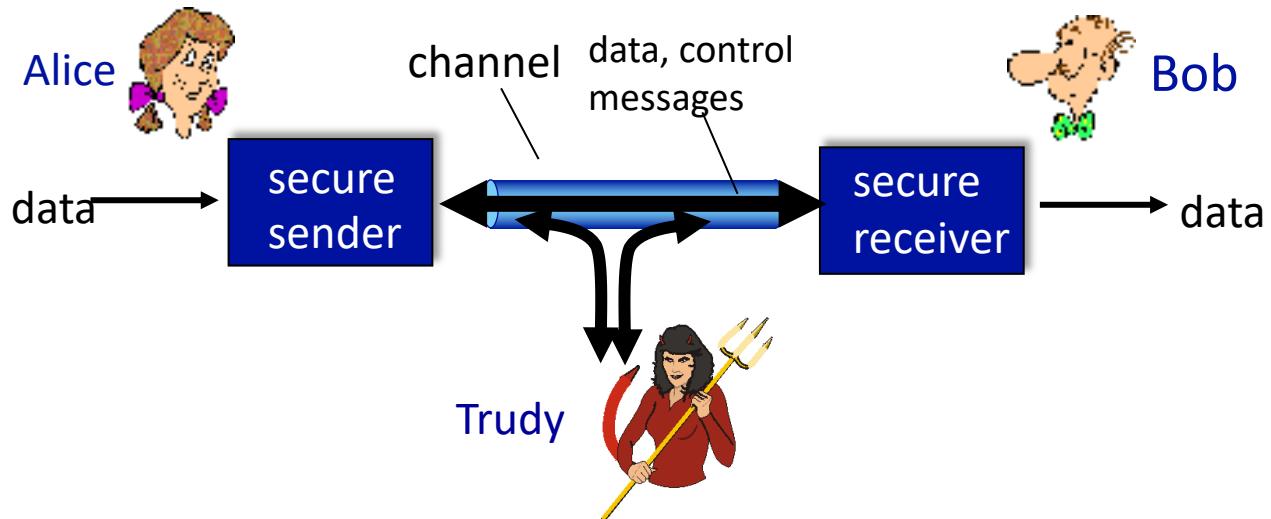
- **confidentiality**: chỉ người gửi và người nhận mới “understand” nội dung thông điệp
 - Người gửi mã hoá thông điệp
 - Người nhận giải mã thông điệp
- **authentication**: người gửi, người nhận muốn xác nhận danh tính của nhau
- **message integrity**: người gửi, người nhận muốn đảm bảo tin nhắn không bị thay đổi (đang chuyển tiếp hoặc sau đó) mà không bị phát hiện
- **access and availability**: dịch vụ phải có thể truy cập và khả dụng cho người dùng



Friends and enemies: Alice, Bob, Trudy



- well-known trong thế giới bảo mật mạng
- Bob, Alice (lovers!) muốn giao tiếp “an toàn”
- Trudy (intruder) có thể chặn, xóa, thêm tin nhắn



Friends and enemies: Alice, Bob, Trudy



- Bob và Alice có thể là ai?
 - ... well, *real-life* Bobs and Alices!
 - Trình duyệt web / máy chủ cho các giao dịch điện tử (ví dụ: mua hàng trực tuyến)
 - Máy khách / máy chủ ngân hàng trực tuyến
 - DNS servers
 - Router BGP trao đổi cập nhật bảng định tuyến
 - Những ví dụ khác?



There are bad guys (and girls) out there!



- **Q:** “Kẻ xấu” có thể làm gì?
- **A:** Nhiều!
 - nghe lén: đánh chặn tin nhắn
 - tích cực chèn tin nhắn vào kết nối
 - mạo danh: có thể giả mạo (spoof) địa chỉ nguồn trong gói (hoặc bất kỳ trường nào trong gói)
 - Hijacking: chiếm quyền điều khiển - “tiếp quản” kết nối đang diễn ra bằng cách loại bỏ người gửi hoặc người nhận, tự chèn vị trí vào
 - Denial of service: từ chối dịch vụ - ngăn không cho người khác sử dụng dịch vụ (ví dụ: quá tải tài nguyên)

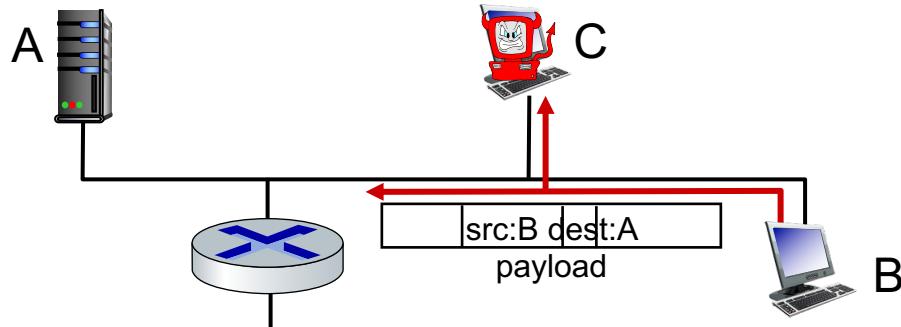


Bad guys: packet interception



- *packet “sniffing”:*

- broadcast media (shared Ethernet, wireless)
- giao diện mạng hổn tạp đọc / ghi lại tất cả các gói (ví dụ: bao gồm cả mật khẩu!) đi qua



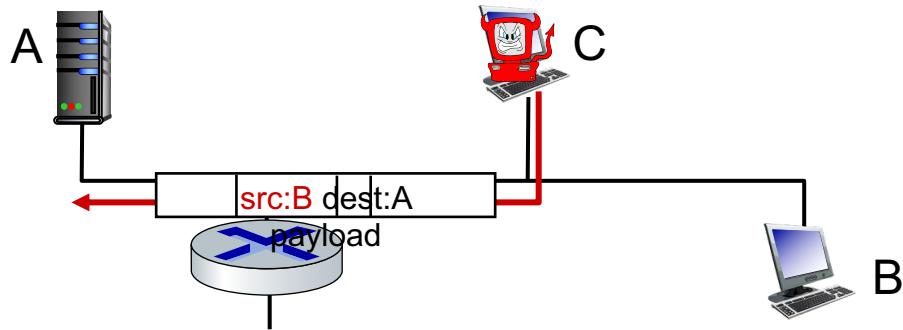
Wireshark software used for our end-of-chapter labs is a (free) packet-sniffer
Alternatives: tcpdump, scapy,...



Bad guys: fake identity



IP spoofing: đưa gói tin có địa chỉ nguồn sai



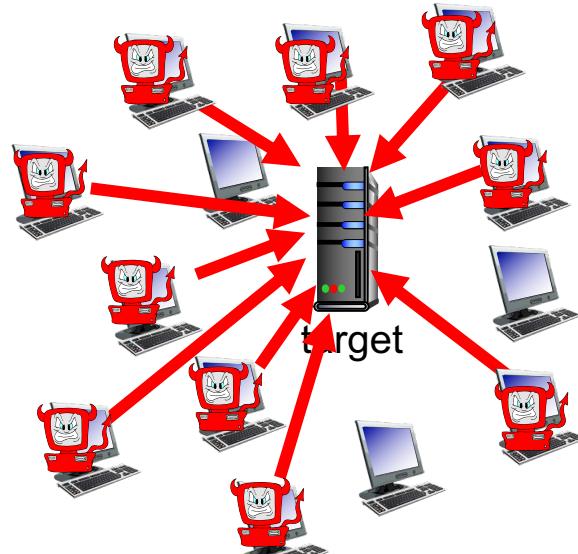
→ *Looking ahead: Phân tích sâu hơn về Sniffing và Spoofing trong buổi kế tiếp*



Bad guys: denial of service

Denial of Service (DoS): kẻ tấn công làm cho tài nguyên (máy chủ, băng thông) không có sẵn sàng cho lưu lượng truy cập hợp pháp bằng cách áp đảo tài nguyên với lưu lượng không có thật

1. Lựa chọn mục tiêu
2. Đột nhập vào các máy chủ trên mạng (xem botnet)
3. Gửi các gói đến mục tiêu từ các máy chủ bị xâm phạm



Các tuyến phòng thủ



- **authentication:** chứng minh bạn là con người bạn nói
 - cellular networks provides hardware identity via SIM card; no such hardware assist in traditional Internet
 - **confidentiality:** thông qua mã hóa
 - **integrity checks:** ký điện tử ngăn chặn / phát hiện giả mạo
 - **access restrictions:** VPN được bảo vệ bằng mật khẩu
 - **Firewalls** - “middleboxes” chuyên biệt trong truy cập và mạng lõi:
 - off-by-default: lọc các gói đến để hạn chế người gửi, người nhận, ứng dụng
 - phát hiện / phản ứng với các cuộc tấn công DOS
- **nhiều hơn nữa về bảo vệ mạng (trong suốt Bài giảng 10)**



Buổi kế tiếp



- Chuẩn bị
 - Chủ đề dự kiến: **Packet Sniffing and Spoofing**
 - Tài liệu:
 - SEED book, Chapter 15
 - Refs: <https://www.handsongsecurity.net/resources.html>
 - SEED Lab: **Packet Sniffing and Spoofing Lab**
 - Refs: https://seedsecuritylabs.org/Labs_16.04/Networking/Sniffing_Spoofing/



Hôm nay, kết thúc!

- Nghi Hoàng Khoa
- khoanh@uit.edu.vn
- www.inseclab.uit.edu.vn
- NT101 – An toàn Mạng máy tính

