Protocol & Layered Service Models

A/PROF. DUY NGO

Learning Objectives

1.5 protocol layers

service models

1.6 networks under attack: security

1.7 internet development history

Protocol “Layers”

Networks are complex,

with many “pieces”:

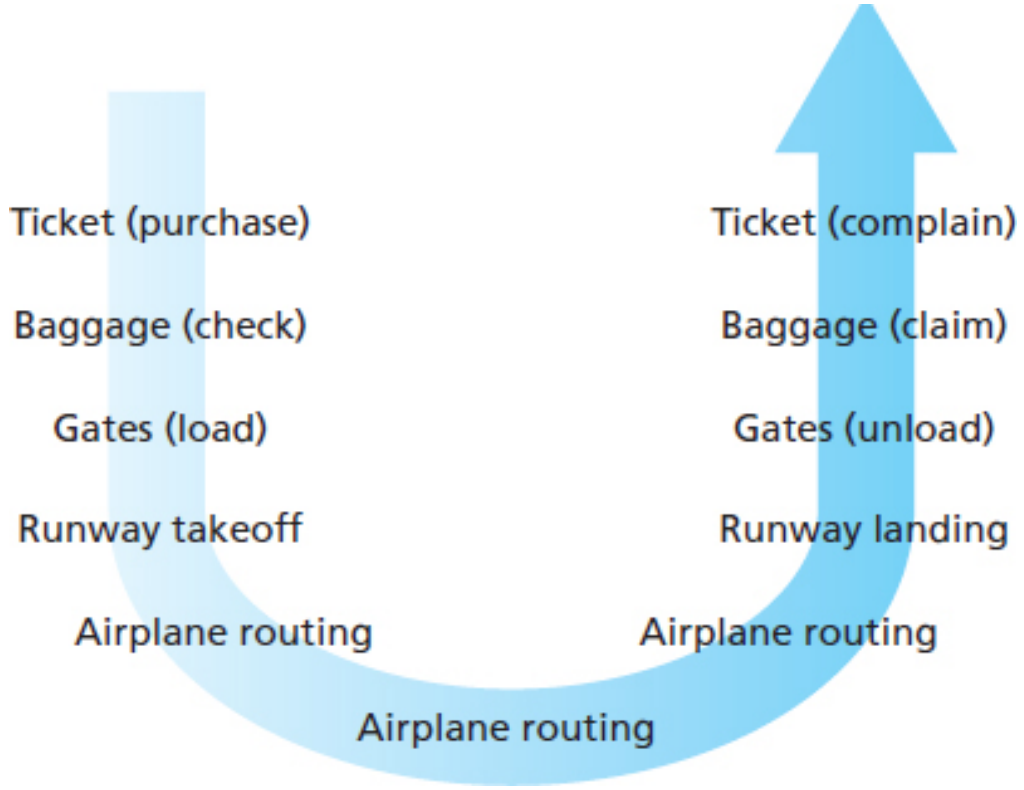
- Hosts
- Routers
- Links of various media
- Applications
- Protocols
- Hardware, software

Question:

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

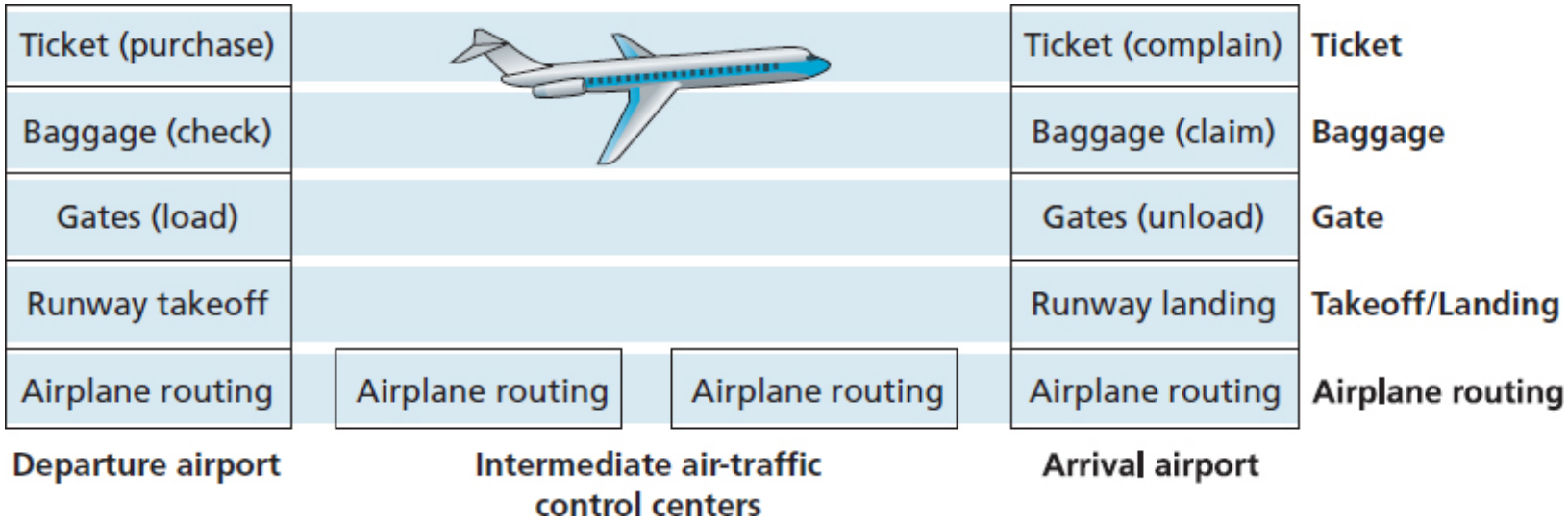
…. or at least our discussion of networks?

Organization of Air Travel



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

layering considered harmful?

Networking Protocols

- Communication protocols define the intelligent procedures used to support end to end communication needs
- Protocols are used to control flow of packets across a network, protocols are generally organised in multilayer models
- Two main communication models are used in current day networks:
  - OSI (Open System Interconnection): a seven layer model
  - TCP/IP (Transmission Control Protocol/Internet Protocol)
- OSI model:
  - Describes a seven-layer abstract reference model for a network architecture
  - Purpose of the reference model was to provide a framework for the development of protocols
  - OSI also provided a unified view of layers, protocols, and services which is still in use in the development of new protocols
  - Detailed standards were developed for each layer, but most of these are not in use
  - TCP/IP protocols preempted deployment of OSI protocols

Internet Protocol Stack (TCP/IP)

application: supporting network applications

- FTP, SMTP, HTTP

transport: process-process data transfer

- TCP, UDP

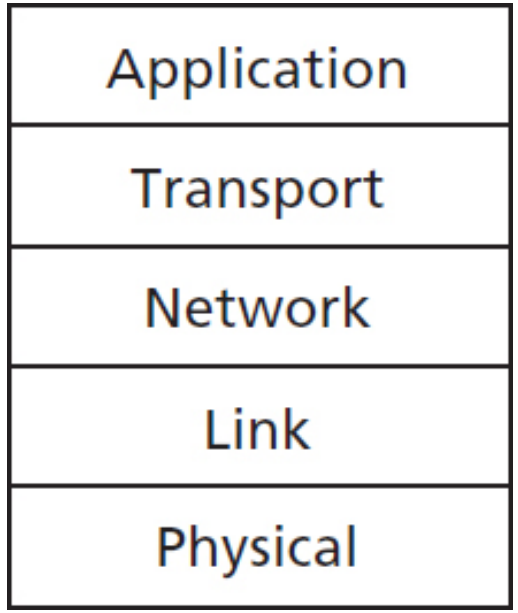
network: routing of datagrams from source to destination

- IP, routing protocols

link: data transfer between neighboring network elements

- Ethernet, 802.11 (WiFi), PPP

physical: bits “on the wire”



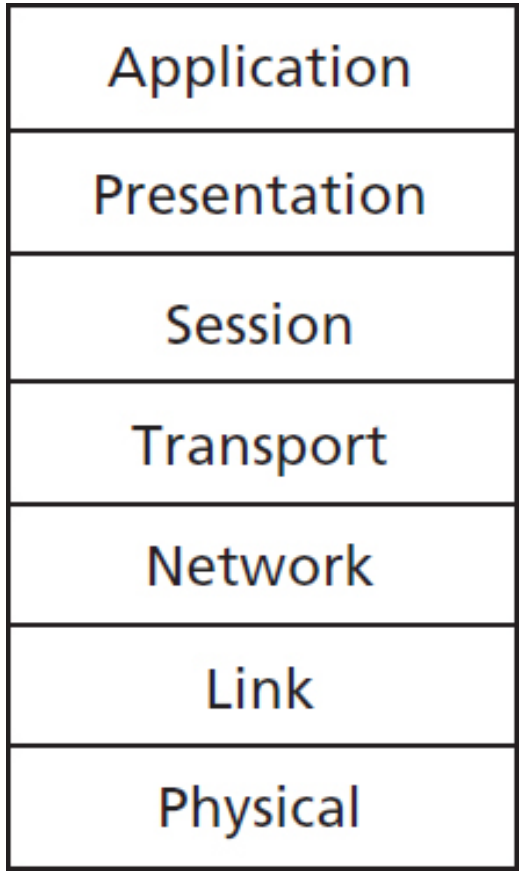
ISO/OSI Reference Model

presentation: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions

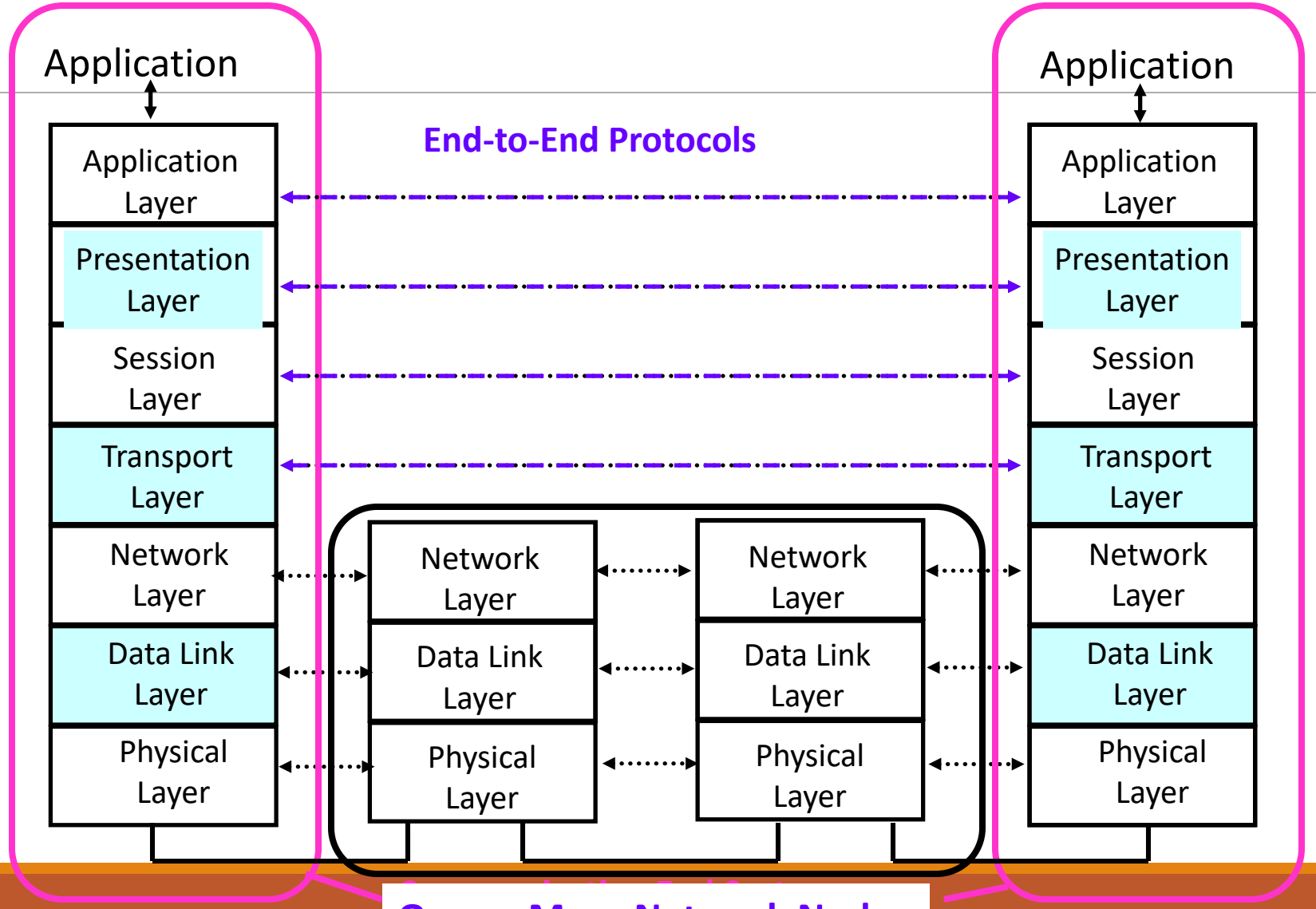
session: synchronization, checkpointing, recovery of data exchange

Internet stack "missing" these layers!

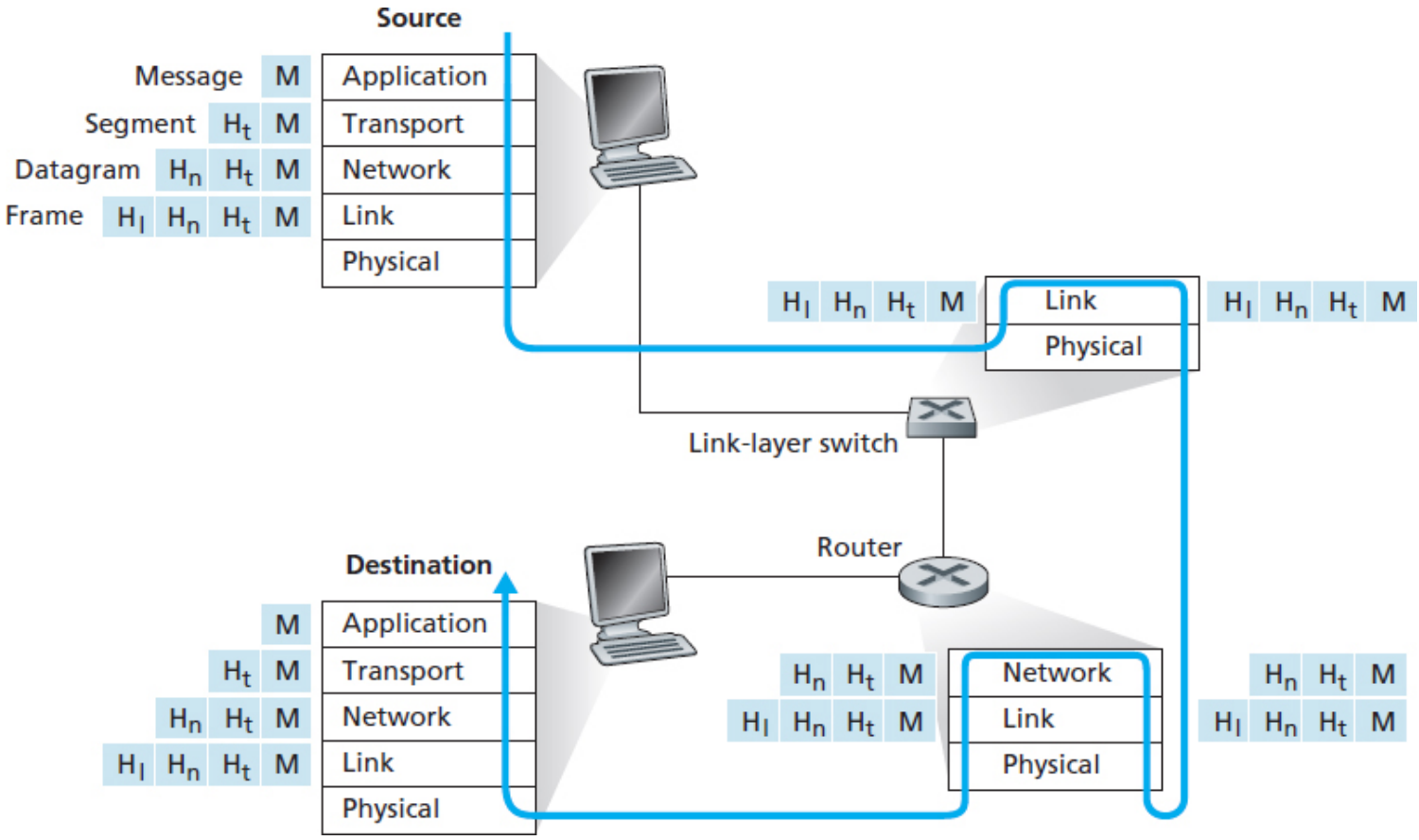
- these services, **if needed**, must be implemented in application
- needed?



7-layer OSI Reference Model

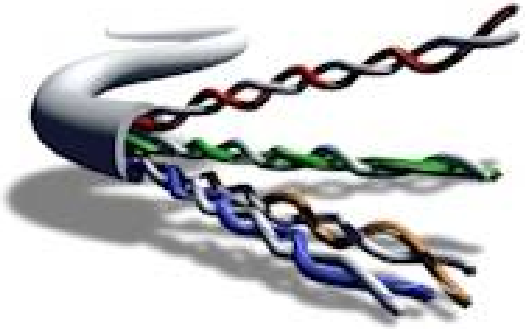


Encapsulation



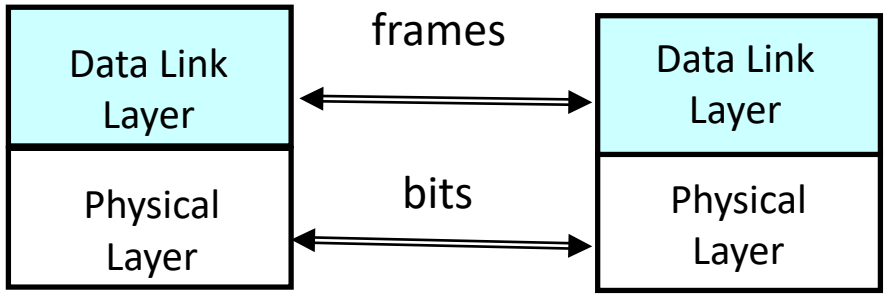
Physical Layer

- Transfers bits across link
- Definition & specification of the physical aspects of a communications link
  - Mechanical: cable, plugs, pins...
  - Electrical/optical: modulation, signal strength, voltage levels, bit times, …
  - Functional/procedural: how to activate, maintain, and deactivate physical links…
- Ethernet, DSL, cable modem, telephone modems…
- Twisted-pair cable, coaxial cable optical fiber, radio, infrared, …



Data Link Layer

- Transfers *frames* across *direct* connections
- Groups bits into frames
- Detection of bit errors; retransmission of frames
- Activation, maintenance, & deactivation of data link connections
- Medium access control for local area networks
- Flow control

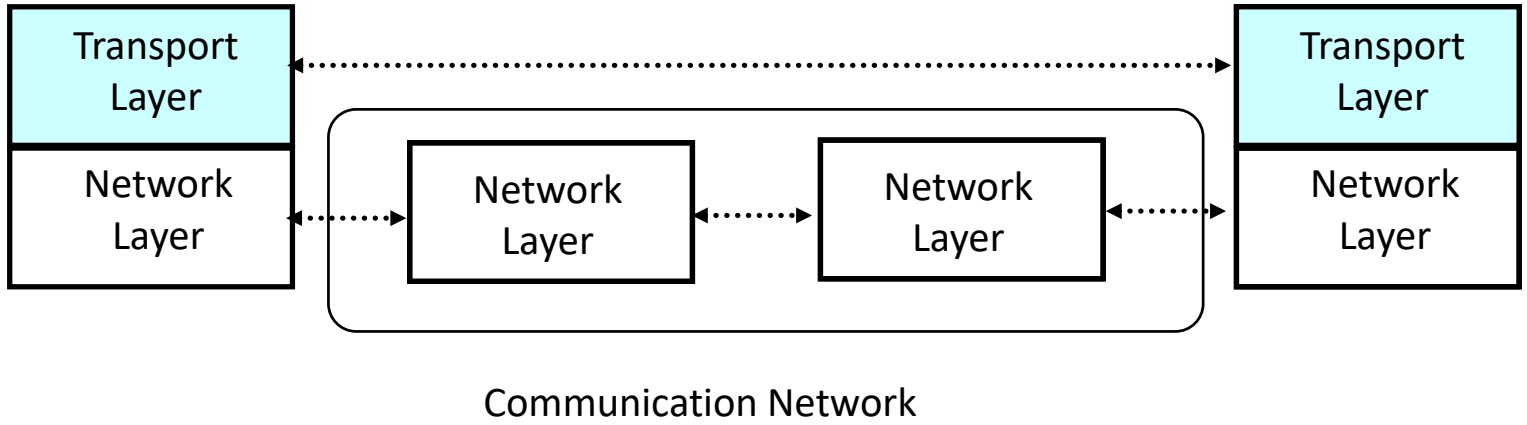


Network Layer

- Transfers *Packets* Across Multiple Links And/Or Multiple Networks
- Addressing Must Scale To Large Networks
- Nodes *Jointly* Execute Routing Algorithm To Determine Paths Across The Network
- Forwarding Transfers Packet Across A Node
- Congestion Control To Deal With Traffic Surges
- Connection Setup, Maintenance, And Teardown When Connection-based

Transport Layer

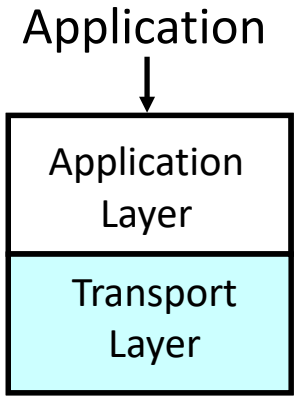
- Transfers Data End-to-end From Process In A Machine To Process In Another Machine
- Reliable Stream Transfer Or Quick-and-simple Single-block Transfer
- Port Numbers Enable Multiplexing
- Message Segmentation And Reassembly
- Connection Setup, Maintenance, And Release



Application & Upper Layers

- Application layer: provides services that are frequently required by applications: DNS, web access, file transfer, email…
- Presentation layer: machine-independent representation of data…
- Session layer: dialog management, recovery from errors, …

Incorporated into Application Layer



Network Security

field of network security:

- 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: Put Malware into Hosts via Internet

malware can get in host from:

- **virus:** self-replicating infection by receiving/executing object (e.g., e-mail attachment)
- **worm:** self-replicating infection by passively receiving object that gets itself executed

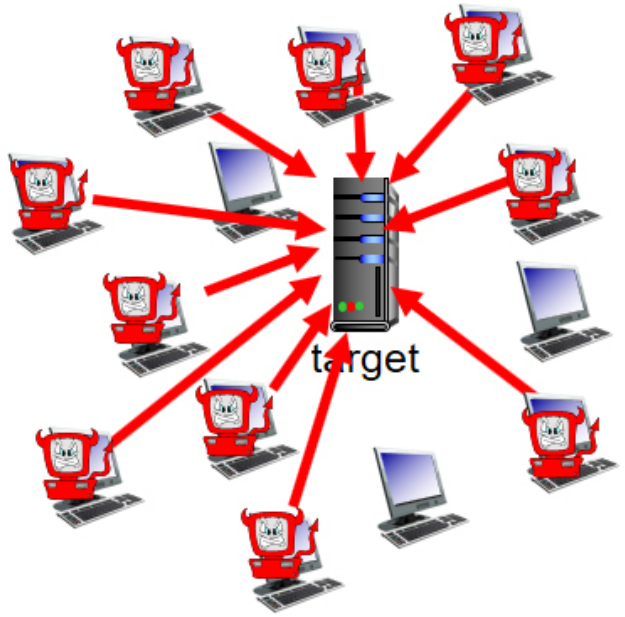
spyware malware can record keystrokes, web sites visited, upload info to collection site

infected host can be enrolled in **botnet,** used for spam. DDoS attacks

Bad Guys: Attack Server, 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 to target from compromised hosts

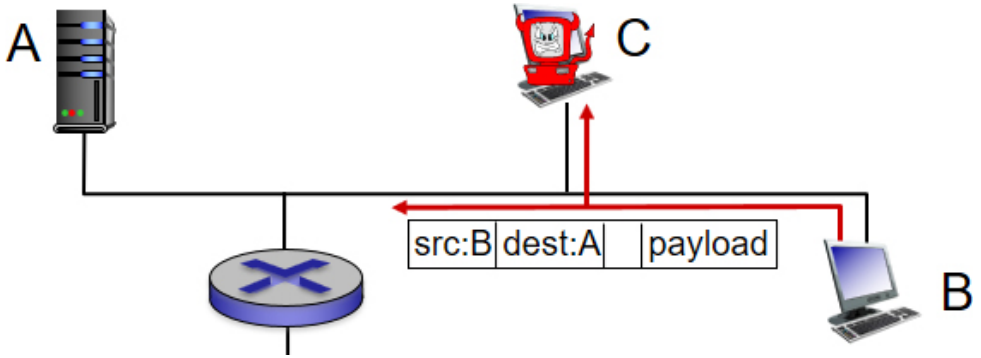


Bad Guys Can Sniff Packets

packet "sniffing":

broadcast media (shared Ethernet, wireless)

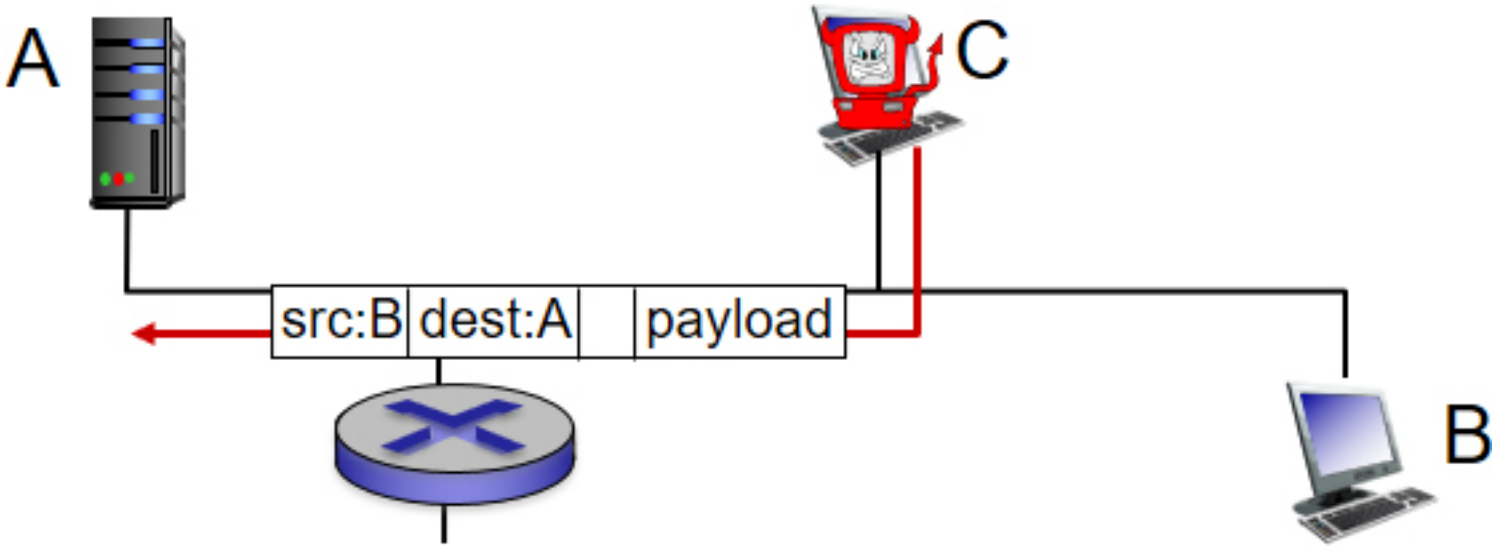
promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



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

Bad Guys Can Use Fake Addresses

IP spoofing: send packet with false source address



… lots more on security (throughout, Chapter 8)

Internet History (1 of 9)

1961-1972: Early packet-switching principles

1961: Kleinrock - queueing theory shows effectiveness of packet-switching

1964: Baran - packet-switching in military nets

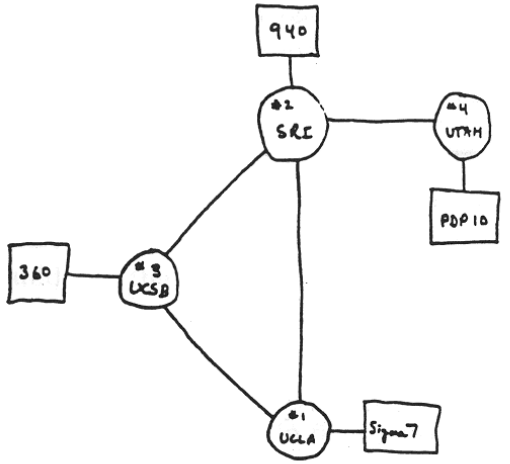
1967: ARPAnet conceived by Advanced Research Projects Agency

1969: first ARPAnet node operational

Internet History (2 of 9)

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 (3 of 9)

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 (Palo Alto Research Centre)

Late70's: proprietary architectures: DECnet, SNA (Systems Network Architecture, XNA

late 70's: switching fixed length packets (ATM precursor); ATM: Asynchronous Transmission mode

1979: ARPAnet has 200 nodes

Internet History (4 of 9)

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 (5 of 9)

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 (6 of 9)

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

early 1990's: ARPAnet decommissioned

1991: NSF (National Science Foundation) 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

Internet History (7 of 9)

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 (8 of 9)

2005-present

~5B devices attached to Internet (2016)

- smartphones and tablets

aggressive deployment of broadband access

increasing ubiquity of high-speed wireless access

By 2020 10 billions IoT (Internet of Things) devices will be connected

Internet History (9 of 9)

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)