Layered protocol (service) architecture

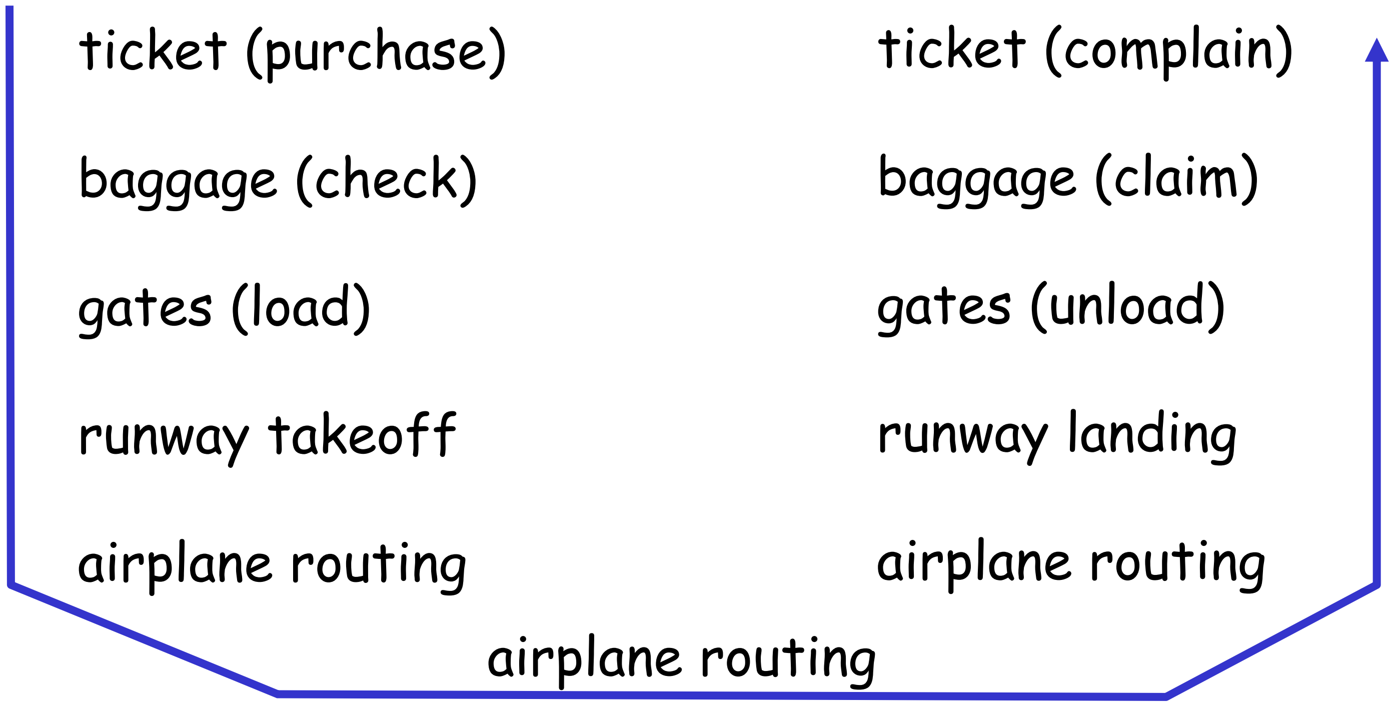
The Internet is complex!

- many “pieces”:
  - hosts
  - access network
  - routers
  - links of various media
  - applications
  - protocols

Question:

Is there any hope of *organizing* a structure of the Internet a so-called ***network (service) architecture***?

Analogy 1: Organization of air travel


ticket (purchase)

baggage (check)

gates (load)

runway takeoff

airplane routing

airplane routing

ticket (complain)

baggage (claim)

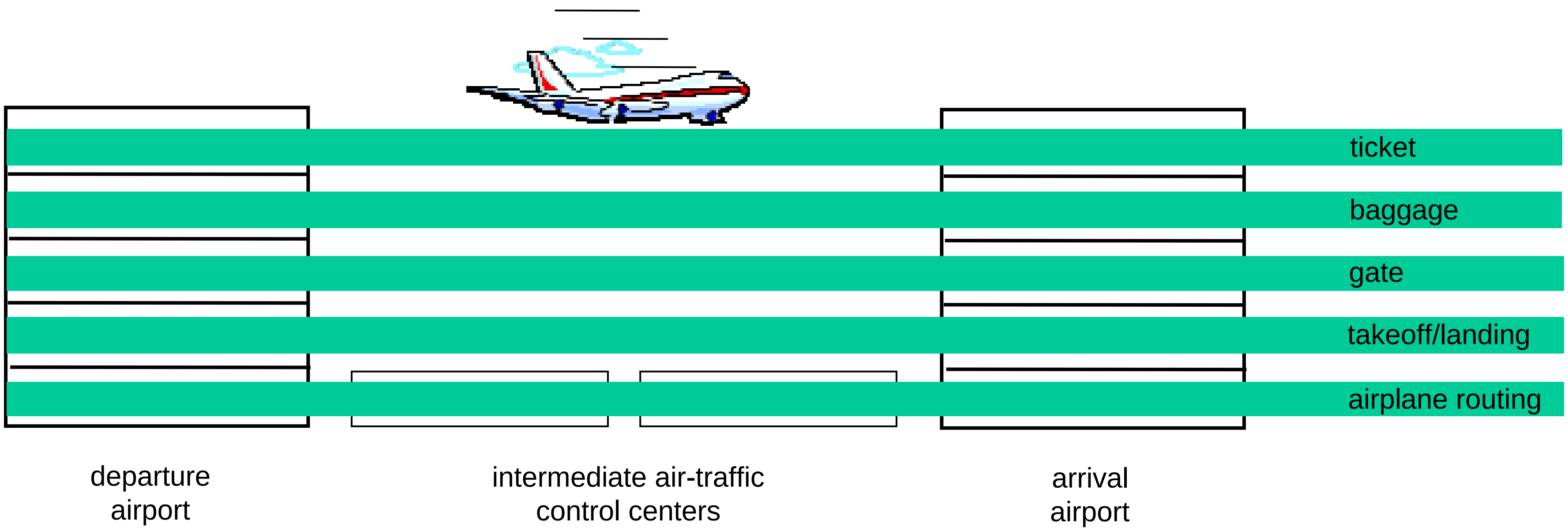
gates (unload)

runway landing

airplane routing

- Structured into a series of steps on both ends

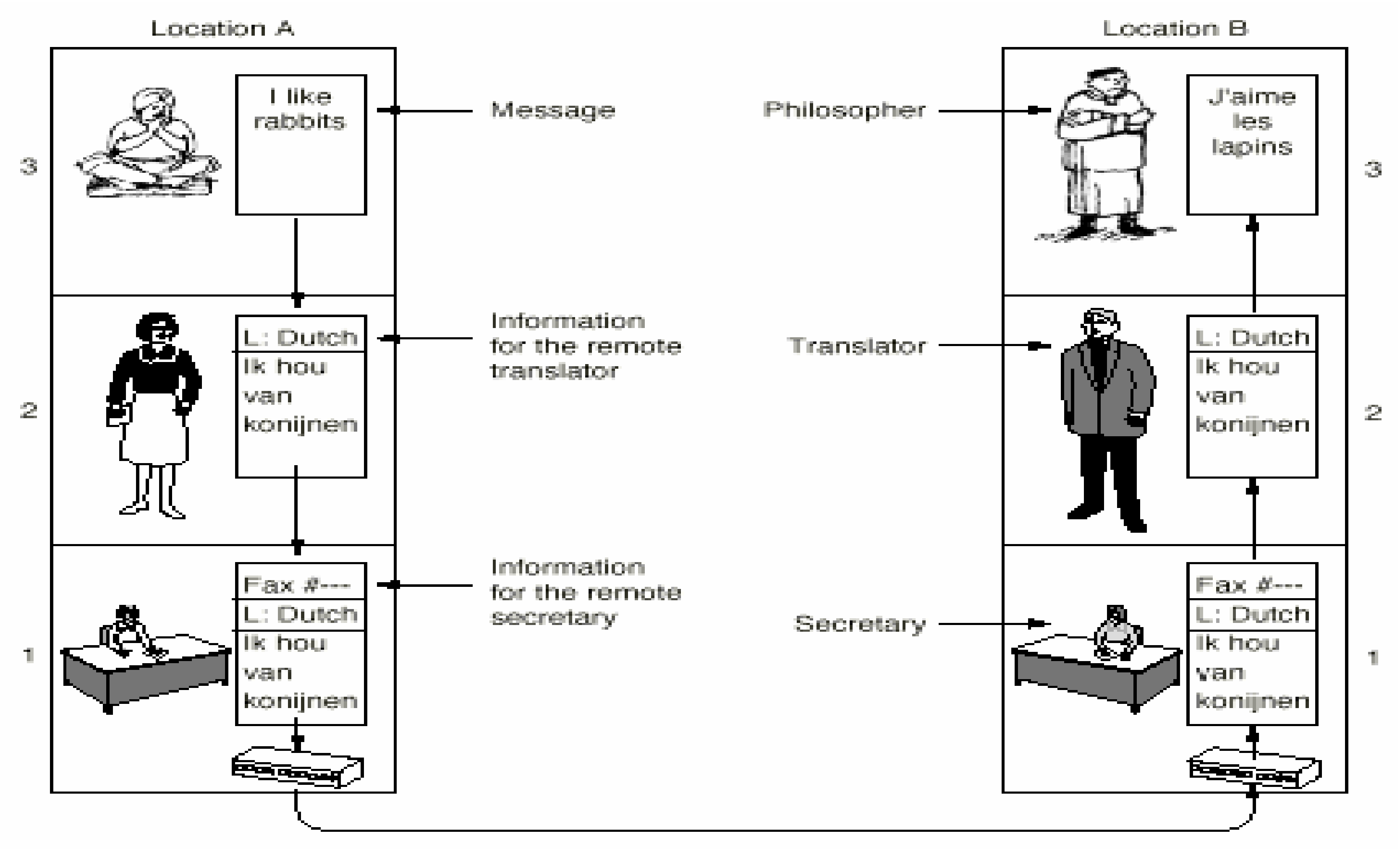
Layering of airline functionality



Layers: each layer implements a service

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

Analogy 2: The philosopher-translator-secretary architecture

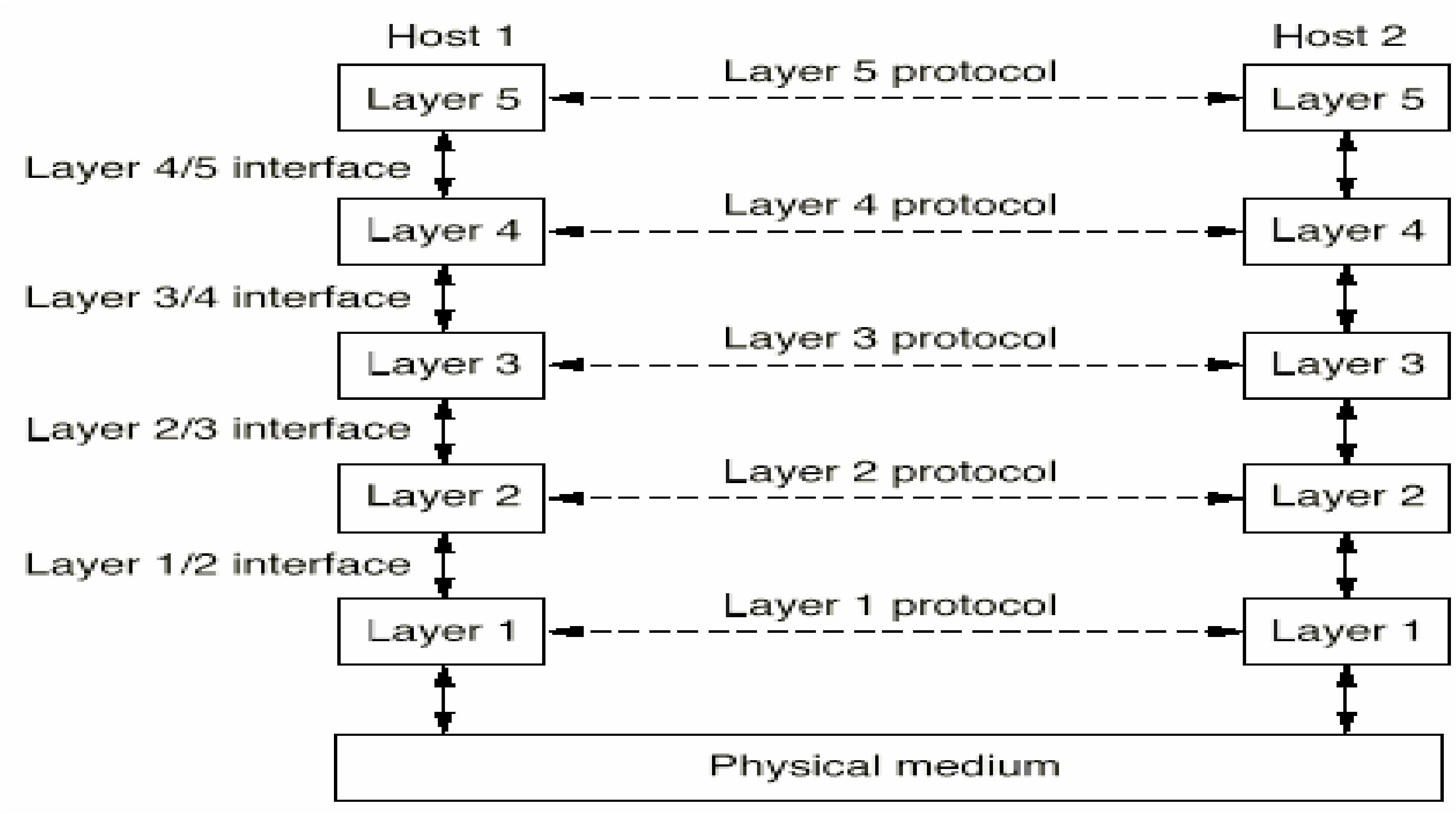


Why layering?

Dealing with complex systems:

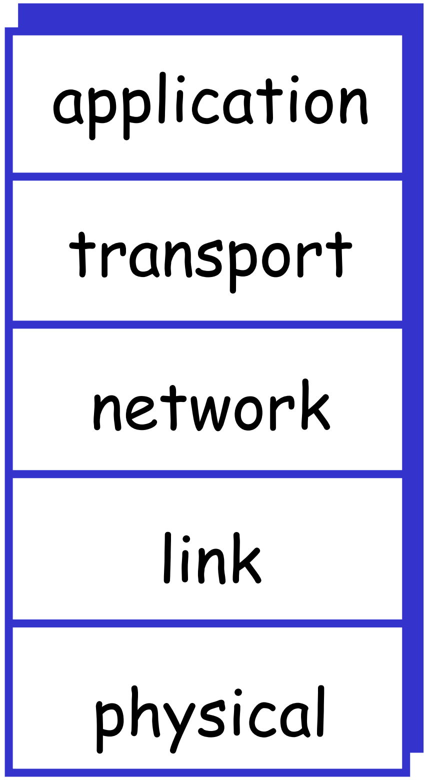
- explicit structure allows identification and relationship of complex system’s pieces
  - layered reference model
- modularization eases maintenance and updating of system
  - change of implementation of layer’s service transparent to rest of system

Network Architecture: A set of layers and protocols



Internet (TCP/IP) 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”

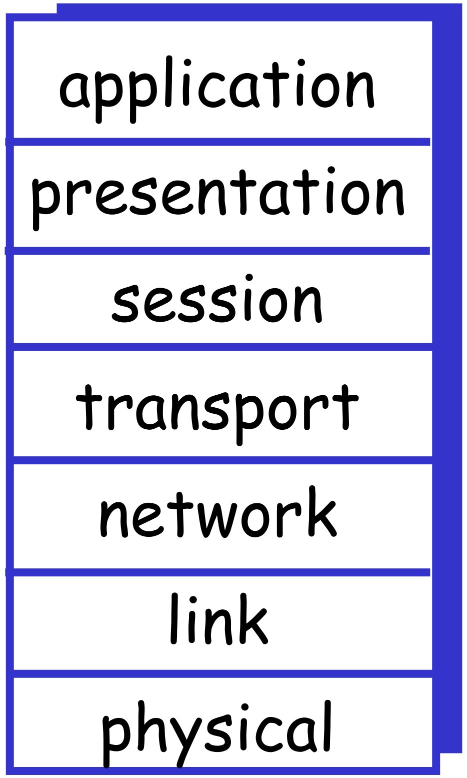


ISO/OSI reference model

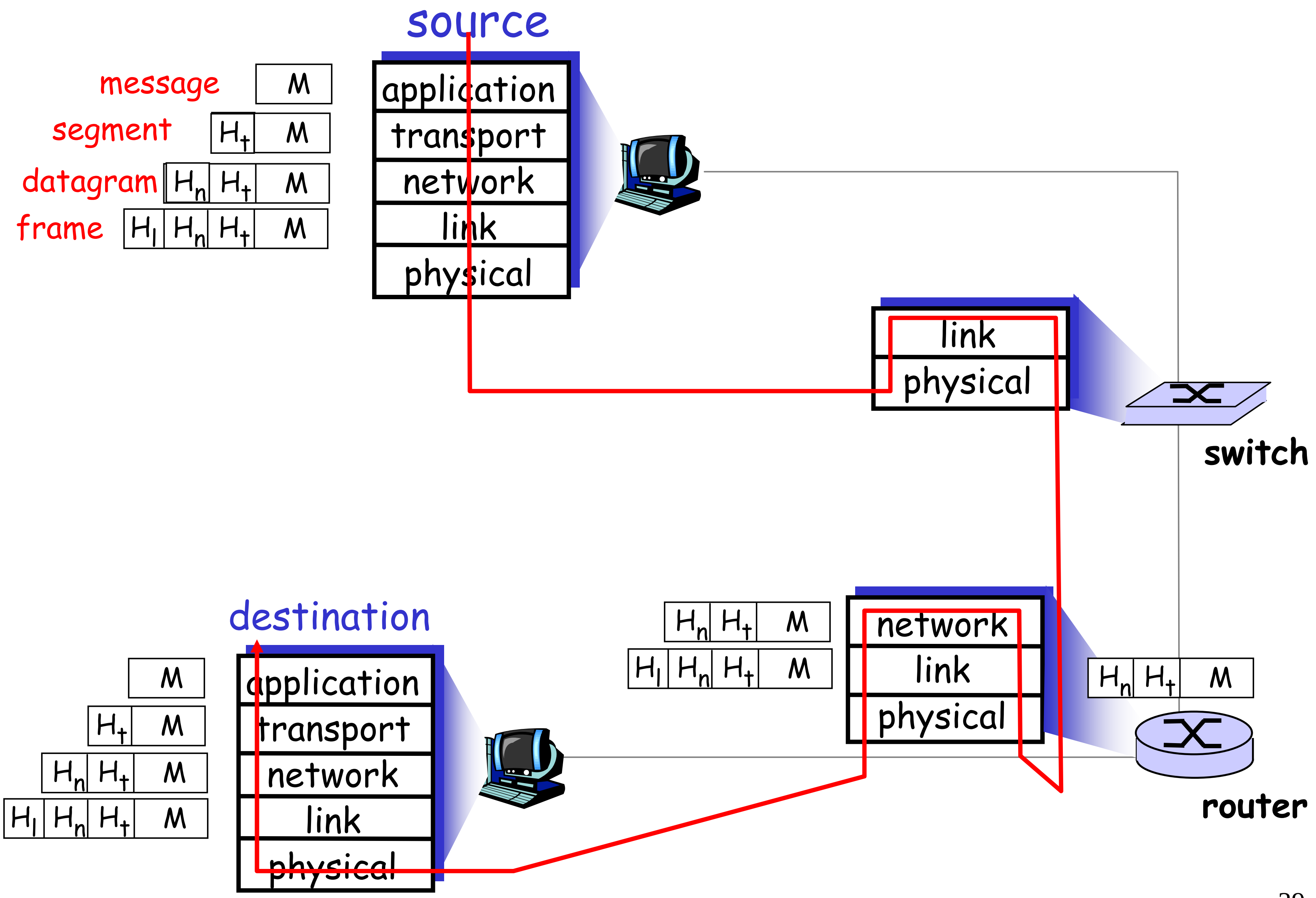
- presentation: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions

- *session:* synchronization, checkpointing, recovery of data exchange

- Internet stack "missing" these layers!
  - these services, *if needed*, must be implemented in application
  - needed?



Physical path data takes and the concept of Encapsulation



Network Security

- attacks on Internet infrastructure:
  - infecting/attacking hosts: malware, spyware, worms, unauthorized access (data stealing, user accounts)
  - denial of service: deny access to resources (servers, link bandwidth)

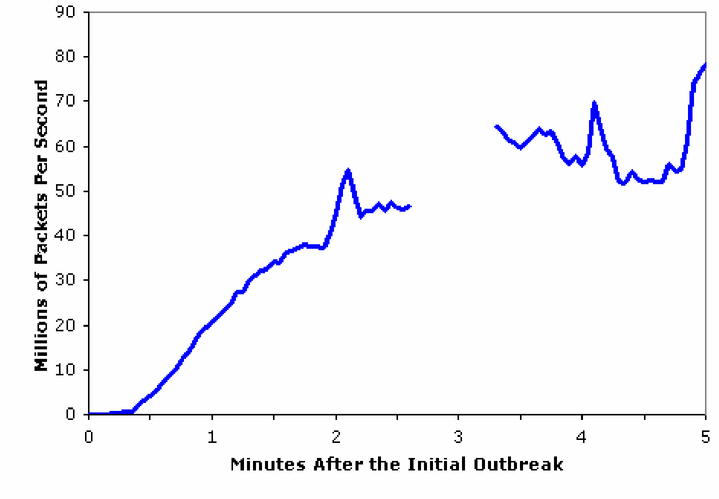
- Internet not originally designed with (much) security in mind
  - *original vision:* “a group of mutually trusting users attached to a transparent network” ☺
  - Security considerations in all layers!

What can bad guys do: malware?

- Spyware:
  - infection by downloading web page with spyware
  - records keystrokes, web sites visited, upload info to collection site
- 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

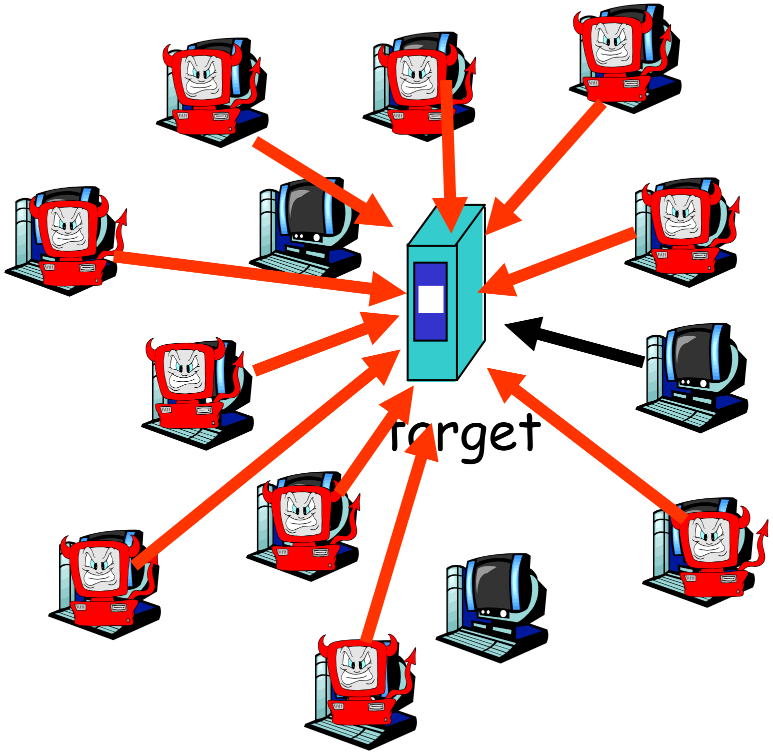
Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)



Denial of service attacks

- attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

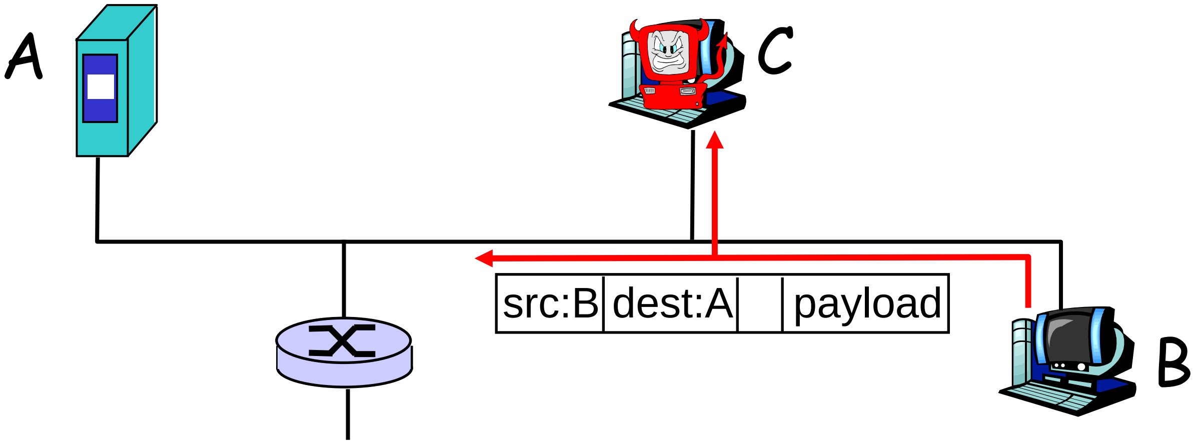
1. select target
2. break into hosts around the network (see malware)
3. send packets toward target from compromised hosts



Sniff, modify, delete your packets

Packet sniffing:

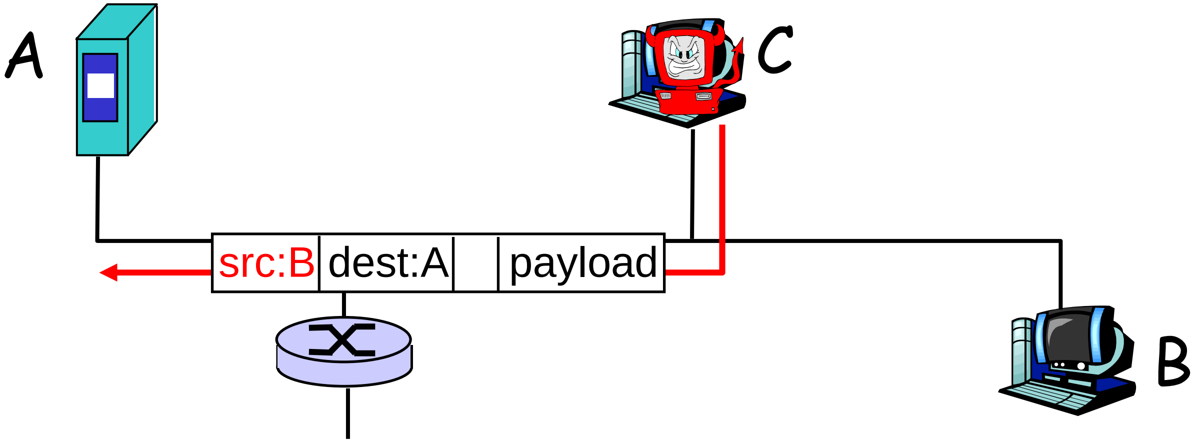
- broadcast media (shared Ethernet, wireless)
- network interface reads/records all packets (e.g., including passwords!) passing by



- needs confidentiality measures

Masquerade as you

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



- needs authentication measures

Internet History (1)

- 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
- 100,000 hosts connected to confederation of networks

Internet History (2)

Internet Explosion: commercialization, the Web, new apps

- early 1990s: Web
  - hypertext [Bush 1945, Nelson 1960’s]
  - HTML, HTTP: Berners-Lee
  - browsers: pioneered by Mosaic (1994), later Netscape
  - late 1990’s: commercialization of the Web (Internet commerce)

Late 1990’s – 2000’s:

- more killer apps: instant messaging (pioneered by ICQ), P2P MP3 file sharing (pioneered by Napster)
- network security to forefront
- est. 50 million hosts, 100 million+ users
- backbone links running at Gbps

Internet History (3)

2007:

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

Introduction: Summary

Covered a “ton” of material!

Overview of Internet structure

- What are its main components?
- what’s a protocol?
- network edge, core, access network
- packet-switching versus circuit-switching

Topics central to the field of computer networking:

- performance: loss, delay, throughput
- layered reference models
- security

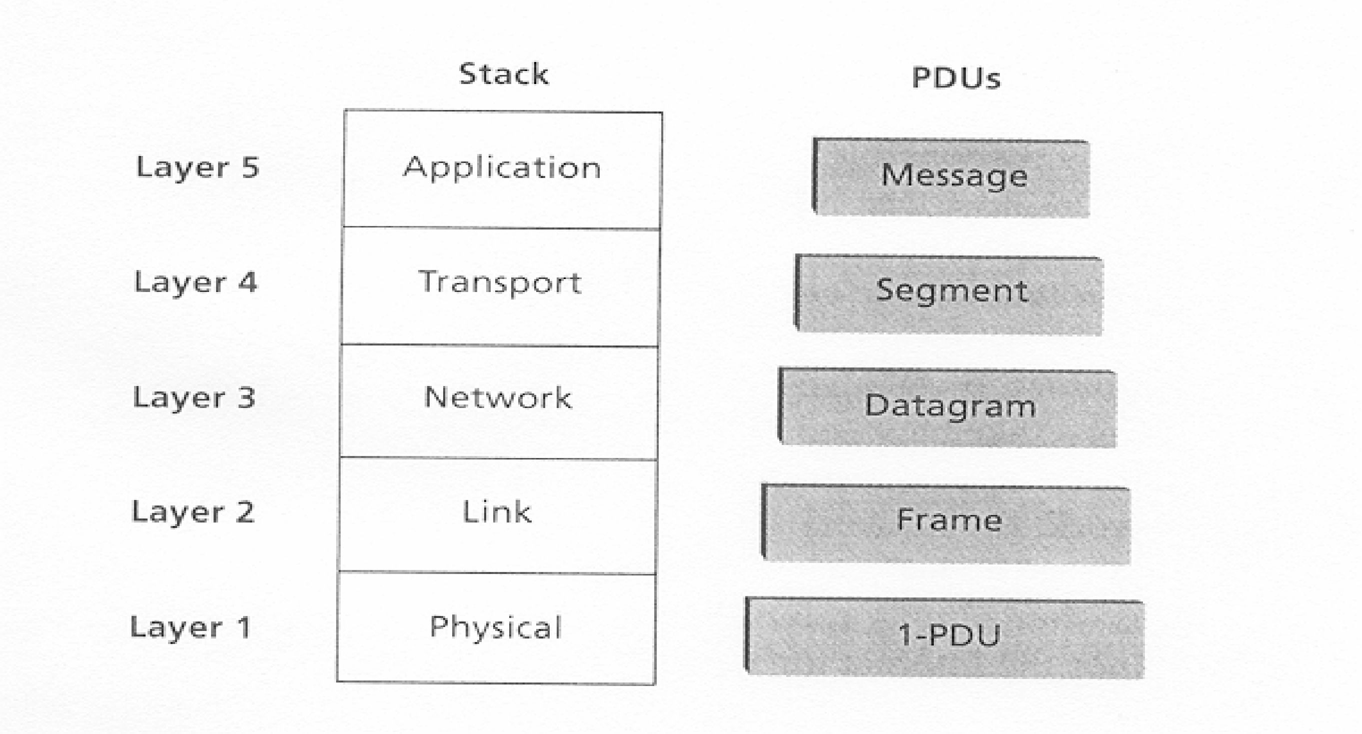
Brief history

You now have hopefully:

- context, overview, “feel” of networking

TCP/IP reference model (Internet architecture)

The Internet protocol stack and the respective protocol data units (PDUs):



The **physical layer** is not addressed further. It deals with transmitting raw bits over a physical transmission medium. The delivered service at the interface to the upper layer must ensure that sending a bit 1 at one side will result in receiving bit 1 at the other side. To do so, it must reflect the specific properties of the medium.

Examples for transmission media:

wired: magnetic media, twisted pair, coaxial cable, fiber optics

wireless: electromagnetic spectrum, radio- micro-, infrared waves