Network Security

- 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!

- attacks on Internet infrastructure (putting malware into hosts via the Internet):
  - infecting/attacking hosts: spyware, virus,worms
  - denial of service: prevent access to servers

What can bad guys do: malware?

- Spyware:
  - infection by downloading e.g. web page with spyware
  - records passwords, 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 without explicit user interaction (e.g. using an e-mail program)
  - self- replicating

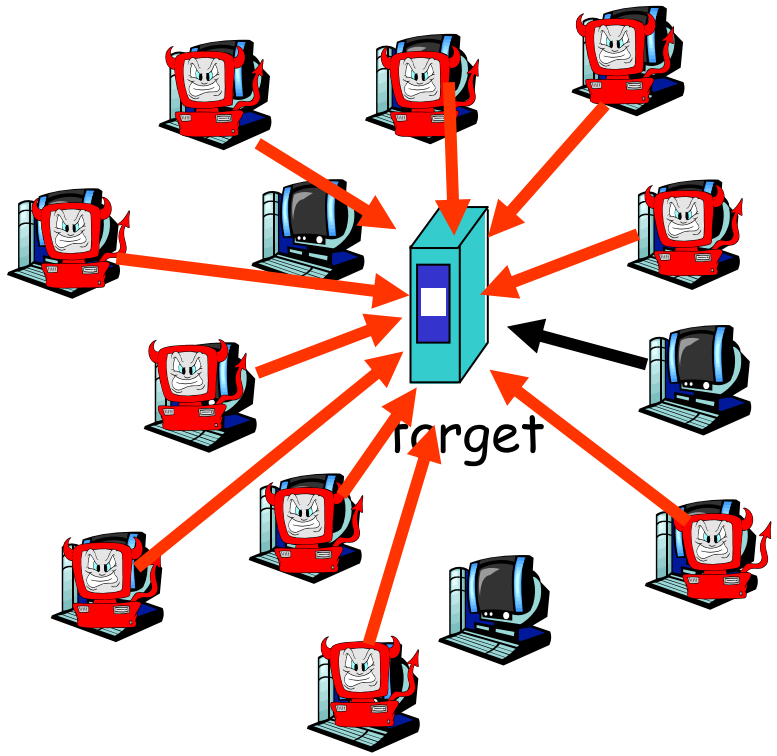
Example: Slammer worm:

- # hosts infected doubled every 8.5 secs in the first minutes after its outbreak
- 90% of the vulnerable hosts infected within 10 minutes

Denial of service attacks

- attackers make resources (e.g. servers) unavailable to legitimate traffic by overwhelming resource with bogus traffic (works very well in client/server applications)

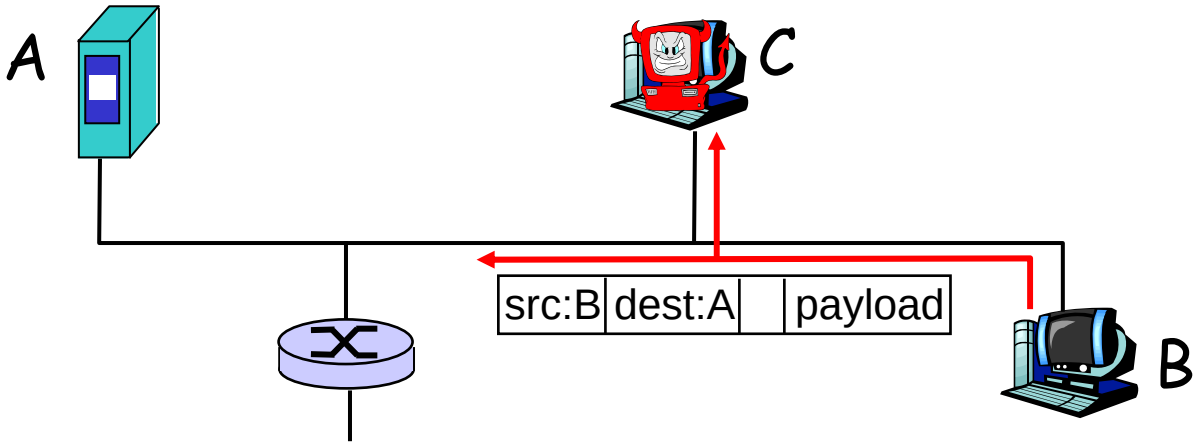
1. select target
2. break into hosts around the network (see malware)
3. send packets toward target from compromised hosts



Sniffing

Packet sniffing:

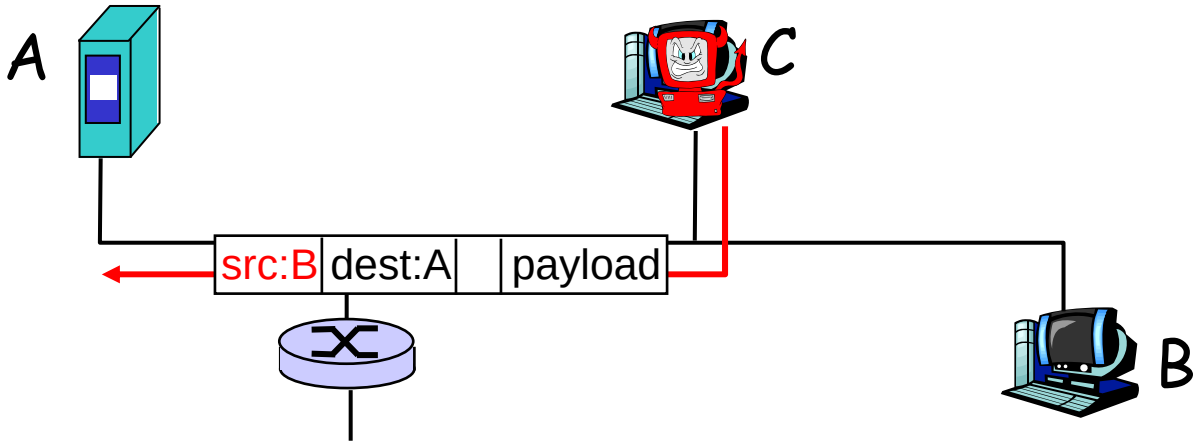
- broadcast media (shared Ethernet, wireless)
- network interface reads/records all packets (e.g., including passwords!) passing by



- 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), MP3 file sharing (pioneered by Napster),
- network security to forefront
- backbone links running at Gbps

Internet History (3)

Today:

- ~900 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

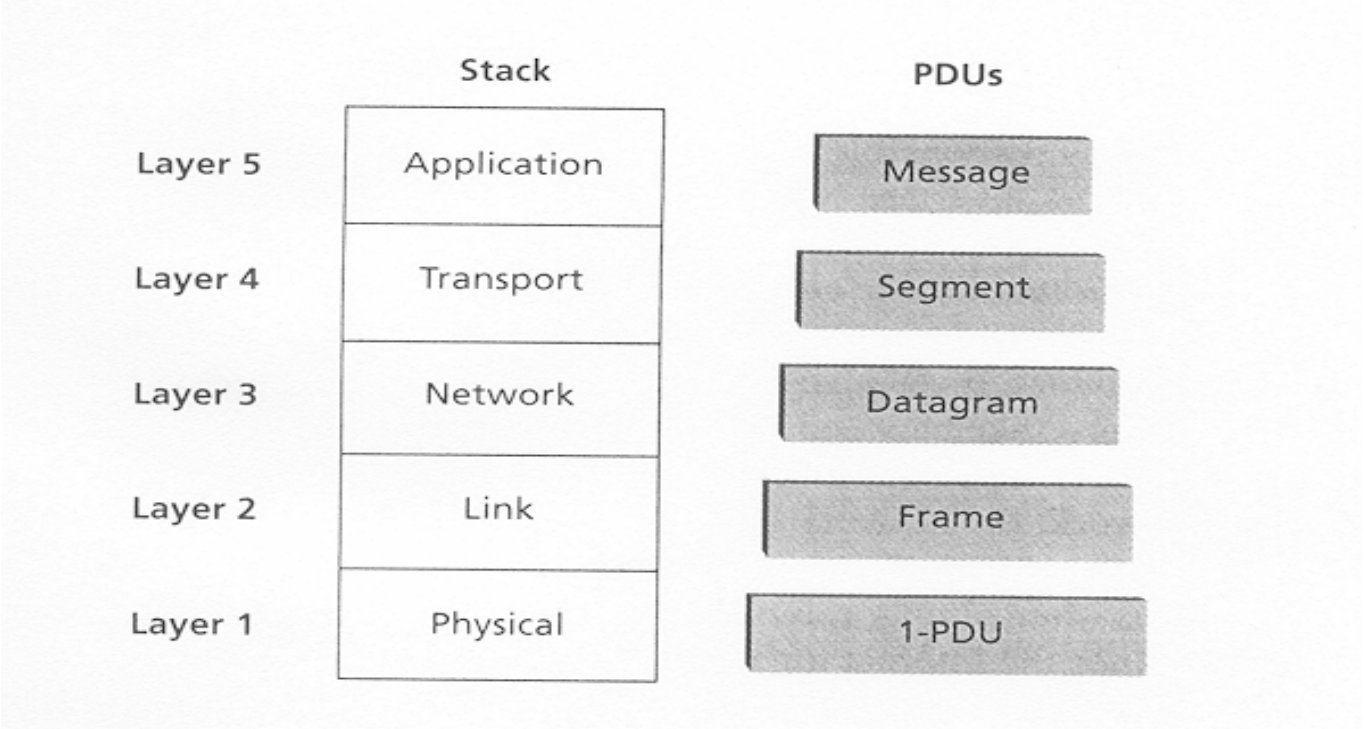
Brief history

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:

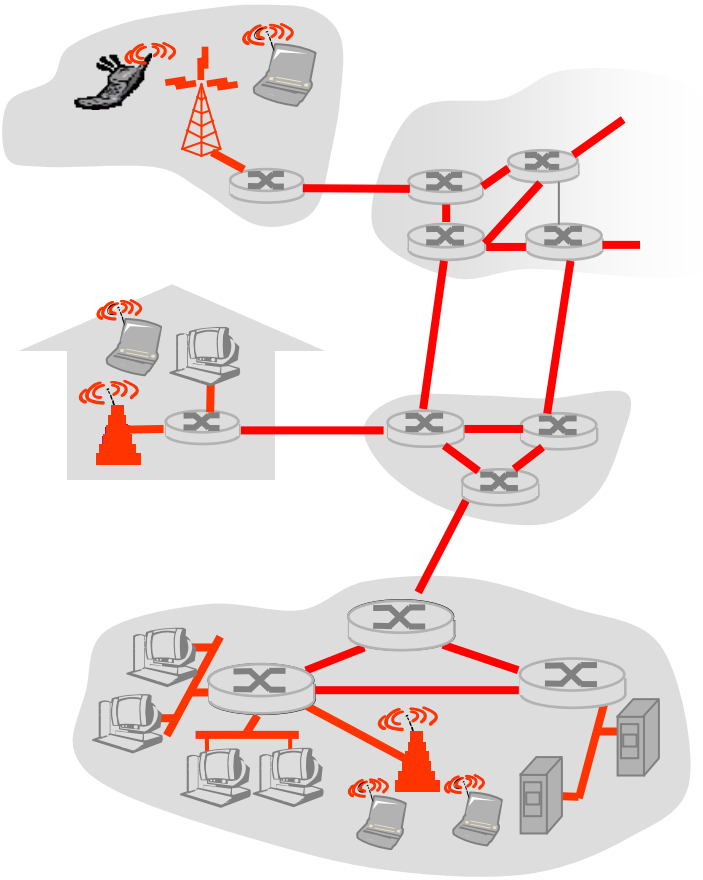
wired: magnetic media, twisted pair, coaxial cable, fiber optics

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

Data Link Layer(1a)

Some terminology:

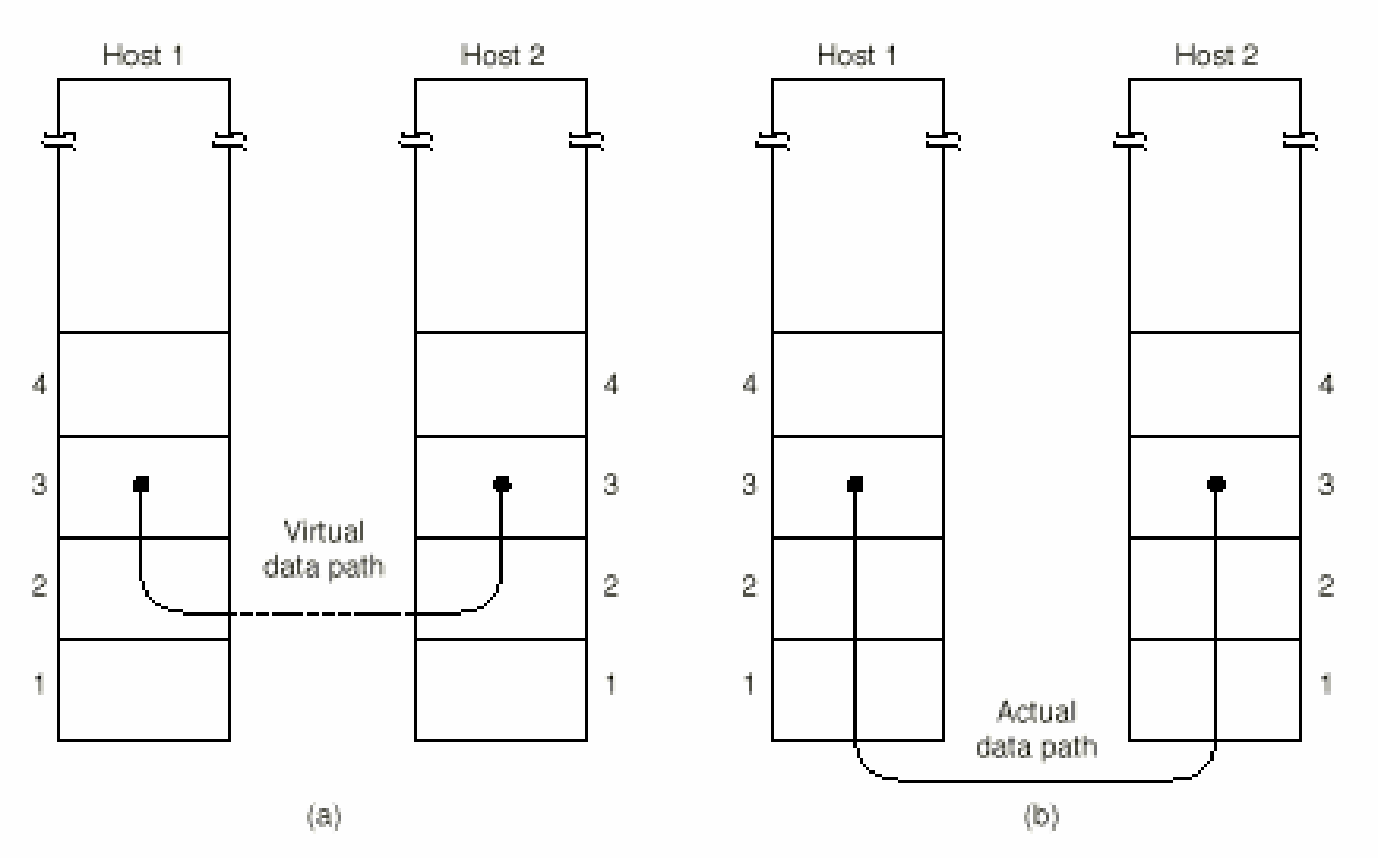
- hosts and routers are **nodes**
- communication channels that connect adjacent nodes along communication path are **links**
  - wired links
  - wireless links
  - LANs
- layer-2 packet is a **frame,** encapsulates datagram from the network layer



data-link layer has responsibility of transferring datagram from one node to adjacent node over a link encapsulated in a frame

Data Link Layer(1b)

Virtual communication versus actual communication:



Data Link Layer(1c)

- frames transferred by different link protocols over different links:
  - e.g., Ethernet on first link, PPP on an intermediate link, 802.11 on the last link
- each link protocol provides different services
  - e.g., may or may not provide rdt (reliable data transfer) over link

transportation analogy

- trip from Princeton to Lausanne
  - limo: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = frame
- transport segment = communication link
- transportation mode = link layer protocol
- travel agent = routing algorithm

Data Link Layer (1d)

Specific services to carry out:

- *framing*
  - determining how the bits of the physical layer are grouped into frames
- *dealing with transmission errors:*
  - *error detection*:
    - receiver detects presence of errors:
    - signals sender for retransmission and drops frame
  - *error correction:*
    - receiver identifies *and corrects* bit error(s) without resorting to retransmission
- *flow control:*
  - pacing between adjacent sending and receiving nodes
- *separate MAC sublayer*
  - controlling channel access if shared medium by so-called MAC protocols