CS 410
Networks and Networking

Lecture 4

Quiz

- What is a shared guided medium?
- Name the most popular wireless Internet access technologies of today.
- What is routing?
- How is a home router different from a core router?
- When is a router said to be congested?
- What is the difference between bandwidth and throughput? Define each term.
- What are some categories of multiplexing?
- What is round trip time?
- List some advantages of packet switching. What are some of its criticisms?
- What reason of packet loss we observed during last lecture?

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

Protocol "Layers"

Networks are complex!

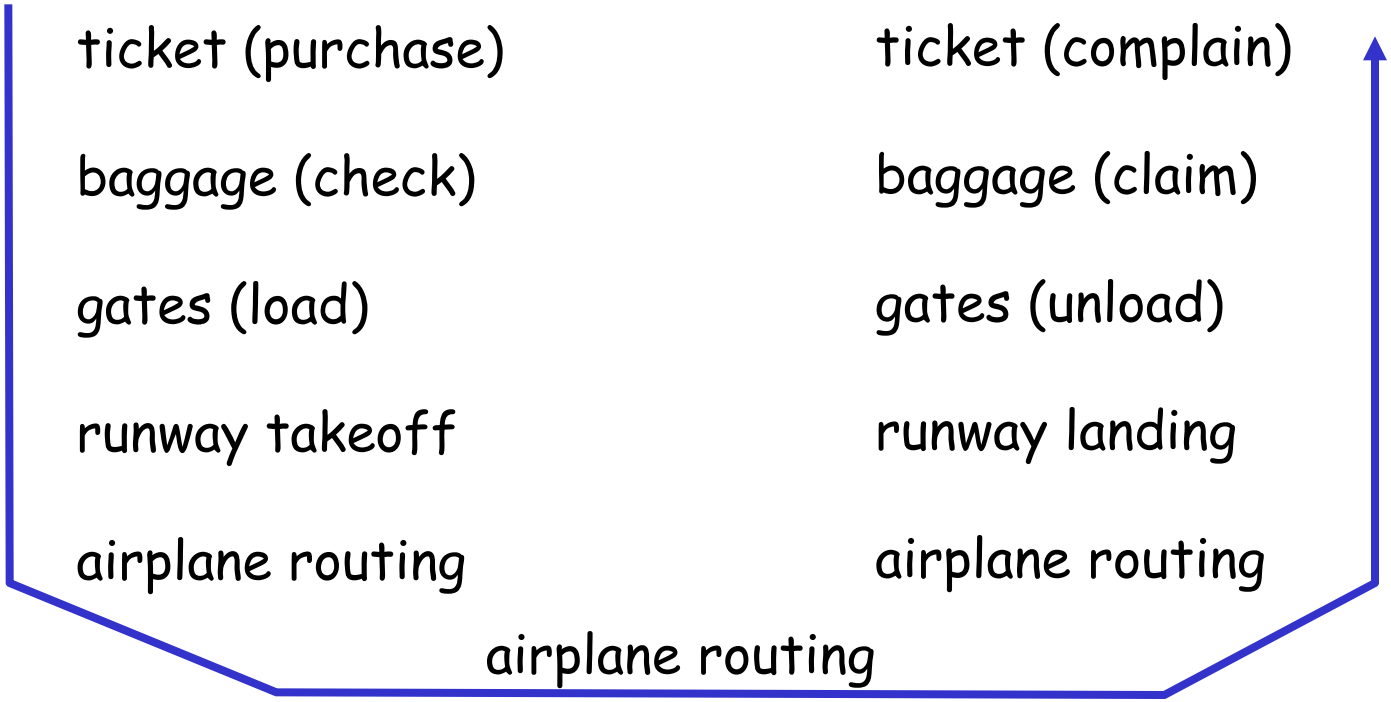
- many "pieces":
  - hosts
  - routers
  - links of various media
  - applications
  - protocols
  - hardware, software

Question:

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

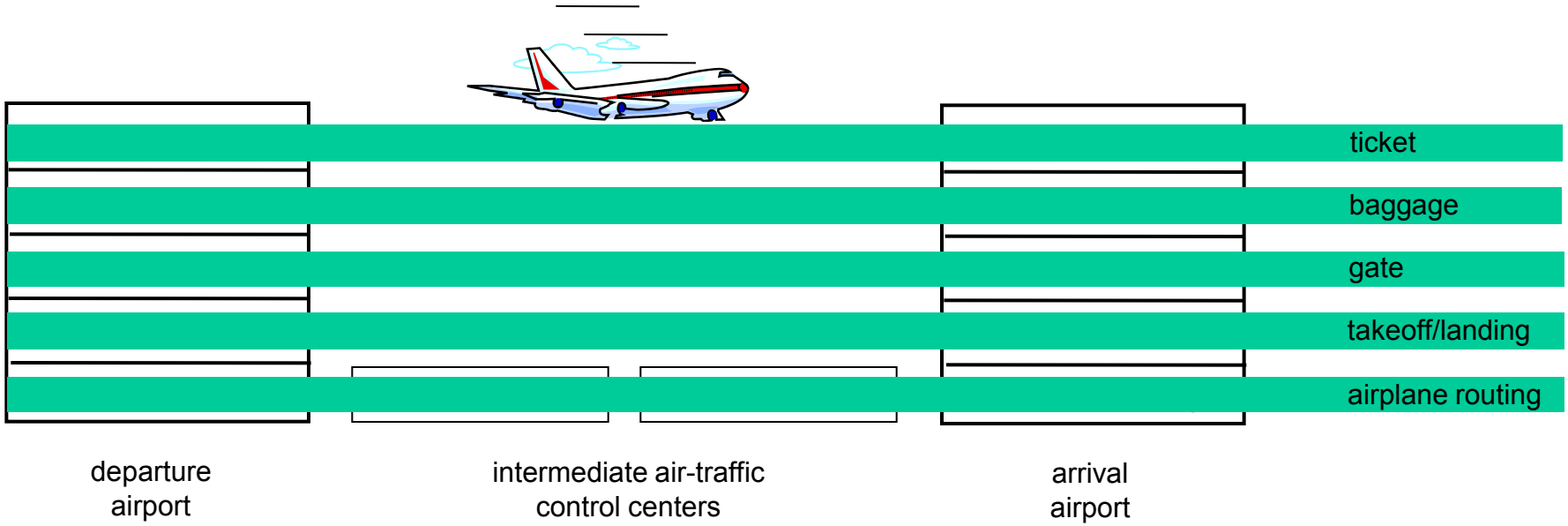
Or at least our discussion of networks?

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

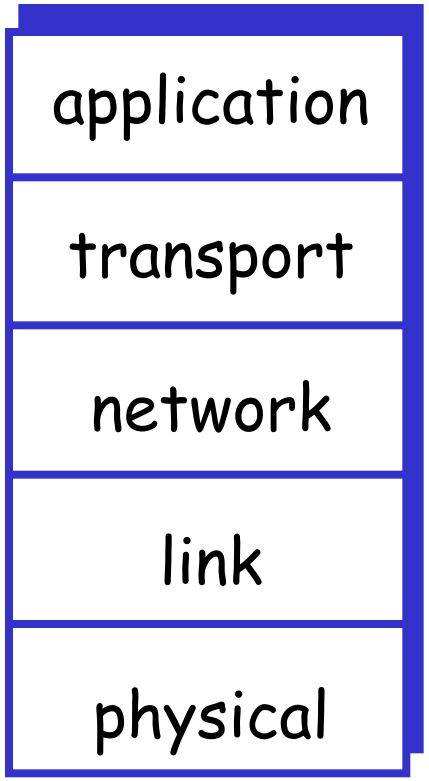
Why layering?

Dealing with complex systems:

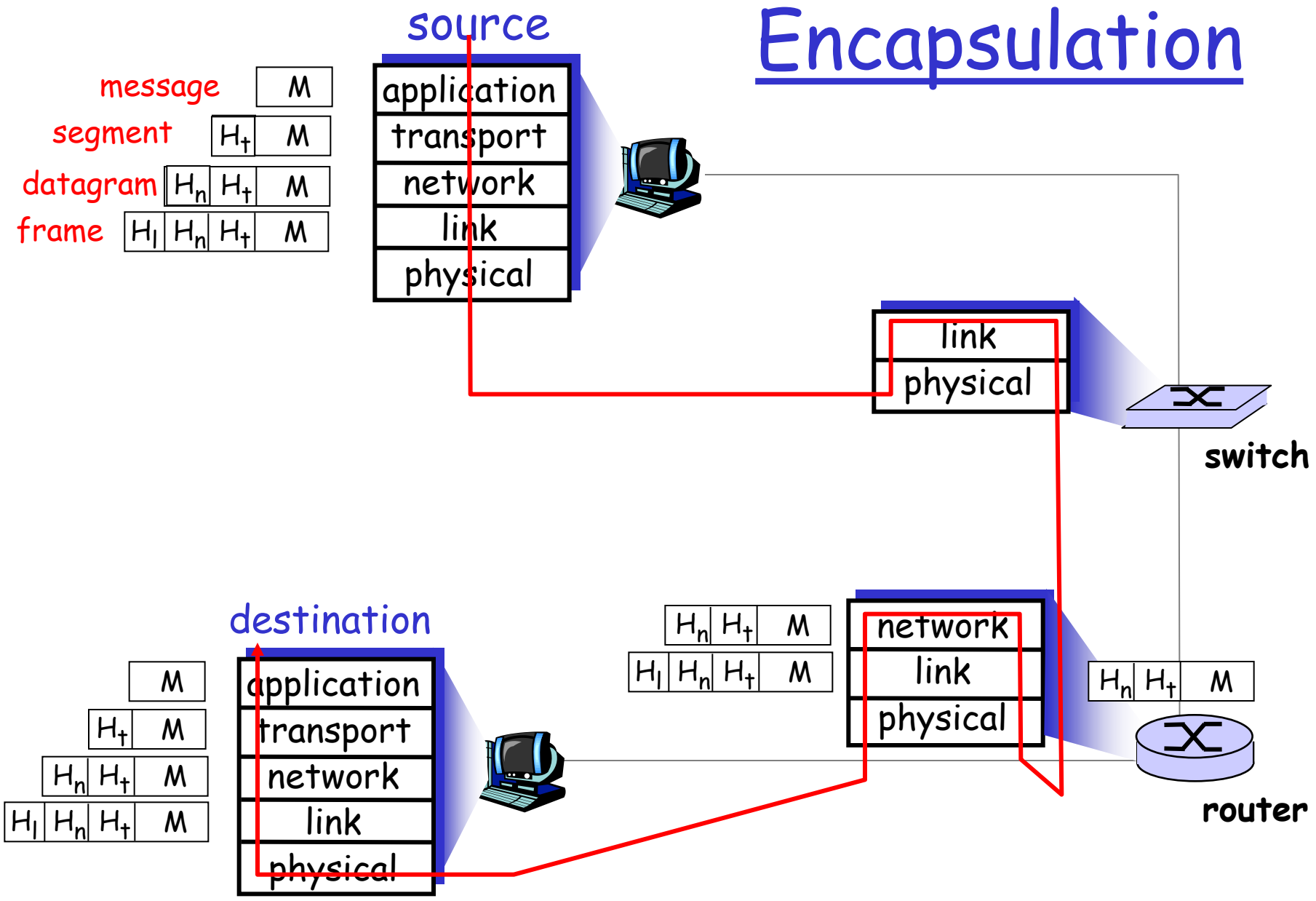
- explicit structure allows identification, relationship of complex system's pieces
  - layered reference model for discussion
- modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system
  - e.g., change in gate procedure doesn't affect rest of system
- Drawbacks of layering?

Internet protocol stack

- application: supporting network applications
  - FTP, SMTP, HTTP, DNS
- 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"

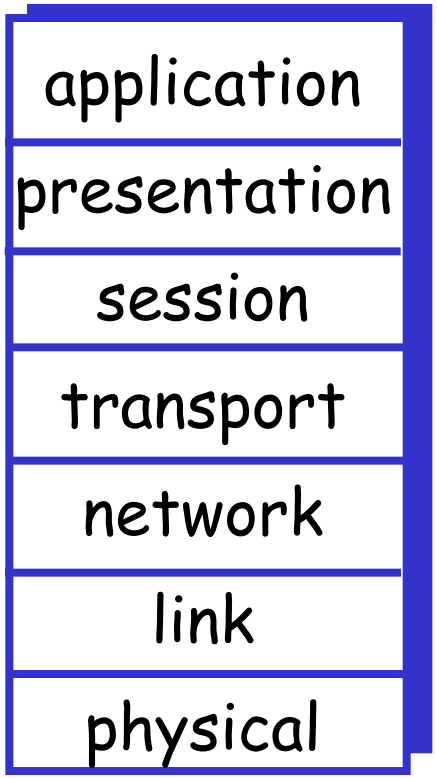


Encapsulation



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?



Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

Network Security

- The field of network security is about:
  - 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!

Questions in Network Security

- What can go wrong?
- How are computer networks vulnerable?
- What are some of the most prevalent types of attacks today?

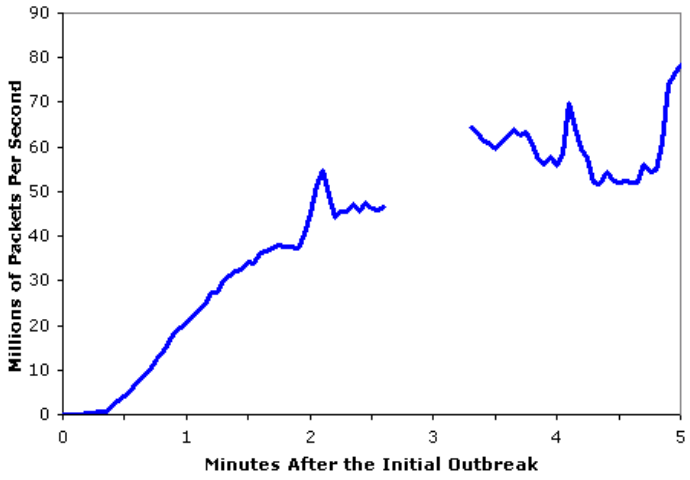
Bad guys can put malware into hosts via Internet

- Malware can get in host from a virus, worm, or Trojan horse.
- Spyware malware can record password, keystrokes, web sites visited and send all this info to collection site. Can also change computer settings resulting in slower speed
- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.
- Malware is often self-replicating: from an infected host, seeks entry into other hosts

Bad guys can put malware into hosts via Internet

- Trojan horse
  - Hidden part of some otherwise useful software
  - Today often on a Web page (Active-X, plugin)
- 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

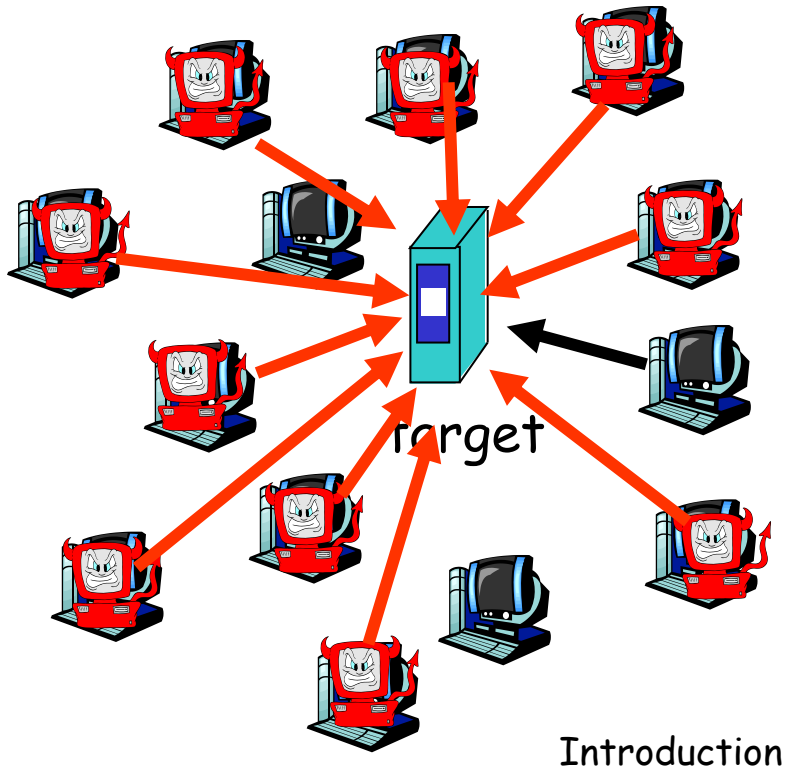
Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)



Bad guys can attack servers and network infrastructure

- Denial of service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

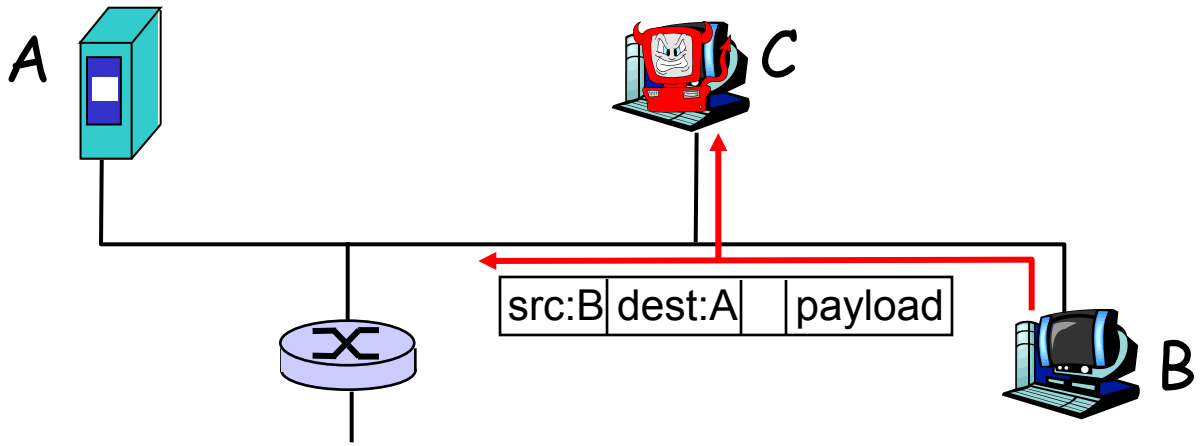
1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts



The bad guys can sniff packets

Packet sniffing:

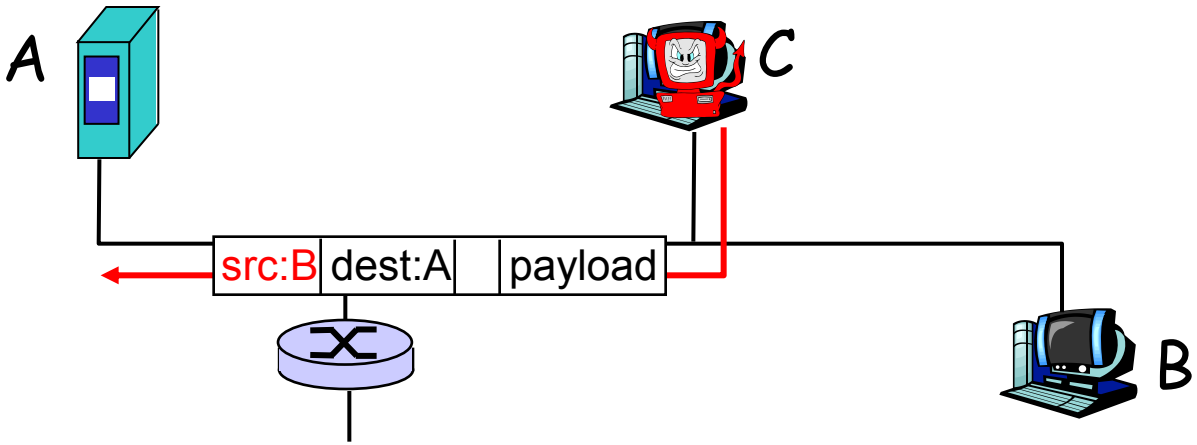
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



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

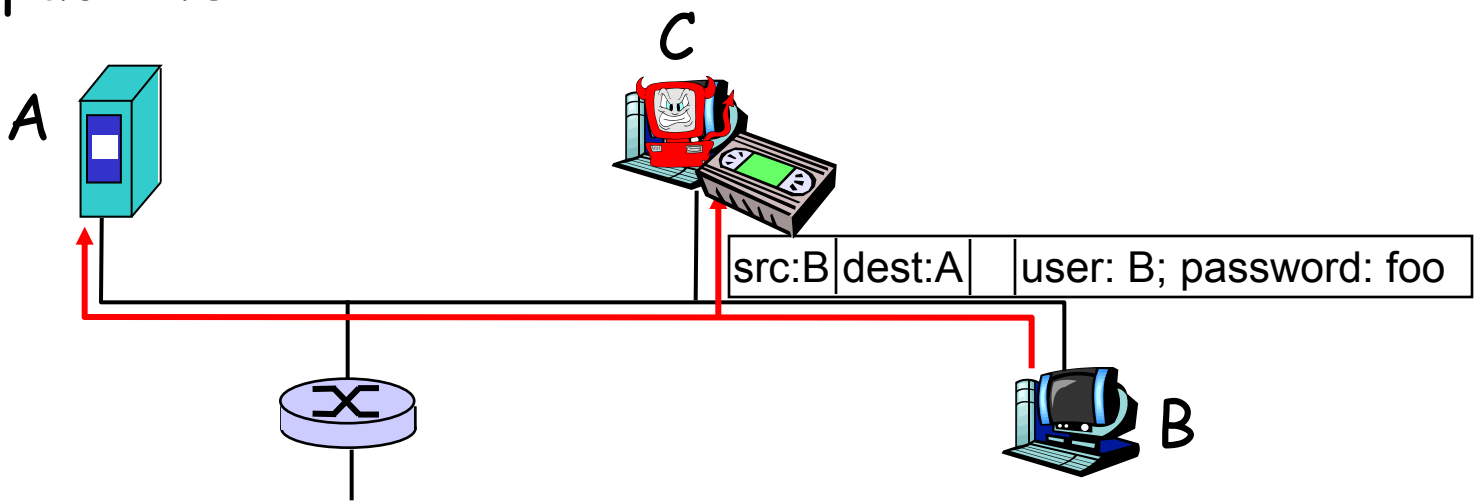
The bad guys can use false source addresses

- *IP spoofing:* ability to inject packets into the internet with false source address



The bad guys can modify and delete messages

- *Man-in-the-middle attack*: bad guy is inserted into the communication path between two communicating entities
  - Not only sniffs but also injects and deletes packets



Network Security

- more throughout this course
- chapter 8: focus on security
- crypographic techniques: obvious uses and not so obvious uses

Network Monitoring Commands

- **Netstat** (Displays all TCP connections on your Windows operating system)
  - **Connection Establishment**
  - The client sends a SYN message which contains the server's port and the client's Initial Sequence Number (ISN) to the server (active open).
  - The server sends back its own SYN and ACK (which consists of the client's ISN + 1).
  - The Client sends an ACK (which consists of the server's ISN + 1).
  - **Connection Tear-down (modified three way handshake).**
  - The client sends a FIN (active close). This is a now a half-closed connection. The client no longer sends data, but is still able to receive data from the server. Upon receiving this FIN, the server enters a passive close state.
  - The server sends an ACK (which is the clients FIN sequence + 1)
  - The server sends its own FIN.
  - The client sends an ACK (which is server's FIN sequence + 1). Upon receiving this ACK, the server closes the connection

- SYN_SEND Indicates active open.
- SYN_RECEIVED Server just received SYN from the client.
- ESTABLISHED Client received server's SYN and session is established.
- LISTEN Server is ready to accept connection.
- NOTE: See documentation for listen() socket call. TCP sockets in listening state are not shown - this is a limitation of NETSTAT. For additional information, please see the following article in the Microsoft Knowledge Base:
- 134404 NETSTAT.EXE Does Not Show TCP Listen Sockets
- FIN_WAIT_1 Indicates active close.
- TIMED_WAIT Client enters this state after active close.
- CLOSE_WAIT Indicates passive close. Server just received first FIN from a client.
- FIN_WAIT_2 Client just received acknowledgment of its first FIN from the server.
- LAST_ACK Server is in this state when it sends its own FIN.
- CLOSED Server received ACK from client and connection is closed.

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

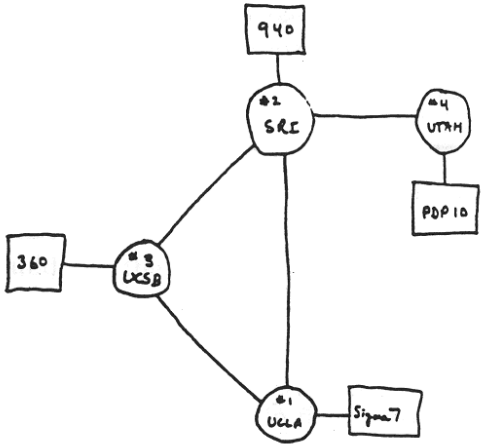
1.7 History

Internet History

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

- 1972:
  - ARPAnet public demonstration
  - NCP (Network Control Protocol) first host-host protocol
  - first e-mail program
  - ARPAnet has 15 nodes



THE ARPA NETWORK

Internet History

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
- ate70's: proprietary architectures: DECnet, SNA, XNA
- late 70's: switching fixed length packets (ATM precursor)
- 1979: ARPAnet has 200 nodes

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

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

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

- Early 1990's: ARPAnet decommissioned
- 1991: NSF 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

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

2007:

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

Introduction: Summary

Covered a "ton" of material!

- Internet overview
- what's a protocol?
- network edge, core, access network
  - packet-switching versus circuit-switching
  - Internet structure
- performance: loss, delay, throughput
- layering, service models
- security
- history

You now have:

- context, overview, "feel" of networking
- more depth, detail *to follow!*