Introduction to Computer Networks

Acknowledgements
These Slides have been adapted from the originals made available by J. Kurose and K. Ross

Introduction

Goals

- get "feel" and terminology
- more depth, detail *later* in course
- approach:
  - use Internet as example

Roadmap

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

What's the Internet: "nuts and bolts" view

PC
server
wireless laptop
cellular handheld

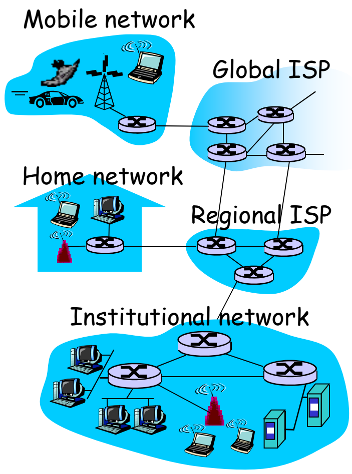
- millions of connected computing devices: *hosts = end systems*
  - running *network apps*

access points
wired links

- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = *bandwidth*

router

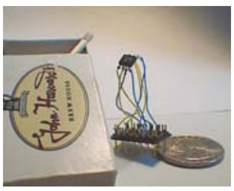
- *routers:* forward packets (chunks of data)



"Cool" internet appliances


IP picture frame


Web-enabled toaster + weather forecaster


World's smallest web server

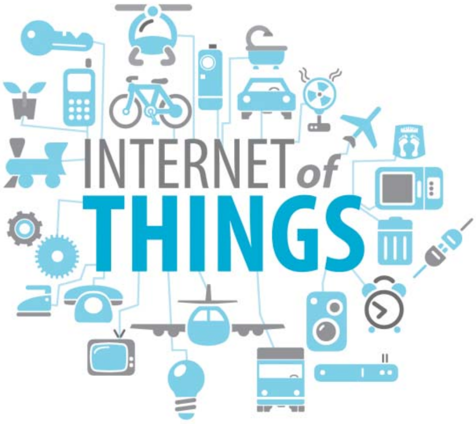

Internet phones

Internet of Things

"The next logical step in the technological revolution connecting people anytime, anywhere is to connect inanimate objects. This is the vision underlying the **Internet of things: anytime, anywhere, by anyone and anything"**
(ITU, Nov. 2005)

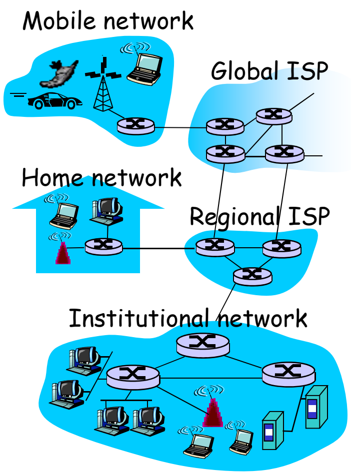
More than 26 billions devices will be wirelessly connected to the Internet of Things by 2020

- computers and communication devices
- cars, robots, machine tools
- persons, animals, and plants
- garments, food, drugs, etc.



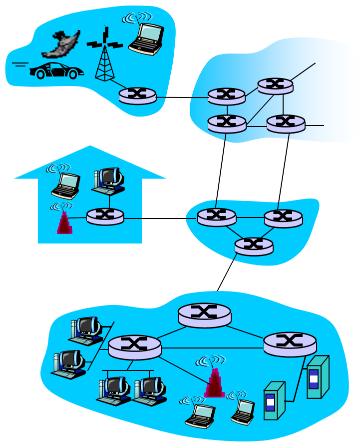
What's the Internet: "nuts and bolts" view

- *Internet:* "network of networks"
  - loosely hierarchical
  - public Internet versus private intranet
- *Protocols* control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, Skype, Ethernet
- Internet standards
  - IETF: Internet Engineering Task Force
  - RFC: Request for comments
  - Other Standard Bodies (e.g. IEEE)



What's the Internet: a service view

- communication *infrastructure* enables distributed applications:
  - Web, email, VoIP, P2P file sharing, Internet radio, Internet TV, e-commerce, games, …
  - Application Programming Interface (API)
- communication services provided to apps:
  - reliable data delivery from source to destination
  - "best effort" (unreliable) data delivery



Introduction 1-9

What's a protocol?

human protocols:

- "what's the time?"
- "I have a question"
- introductions

… specific msgs sent

… specific actions taken when msgs received, or other events

network protocols:

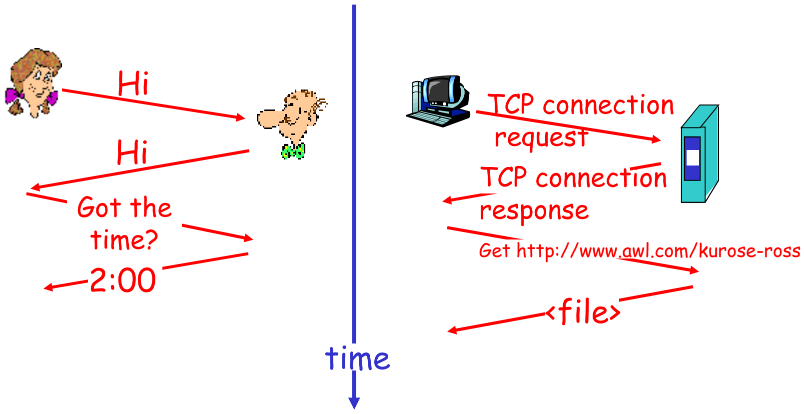
- machines rather than humans
- all communication activity in Internet governed by protocols

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

Introduction 1-10

What's a protocol?

a human protocol and a computer network protocol:



Q: Other human protocols?

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

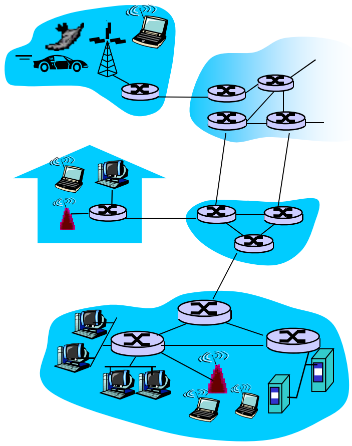
1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

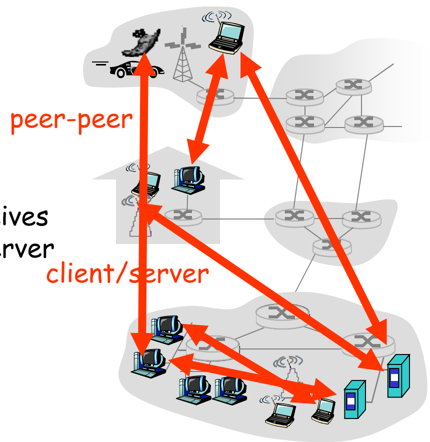
A closer look at network structure:

- network edge: applications and hosts
- access networks, physical media: wired, wireless communication links
- network core:
  - interconnected routers
  - network of networks



The network edge:

- end systems (hosts):
  - run application programs
  - e.g. Web, email
  - at "edge of network"
- client/server model
  - client host requests, receives service from always-on server
  - e.g. Web browser/server; email client/server
- peer-peer model:
  - minimal (or no) use of dedicated servers
  - e.g. Skype, BitTorrent



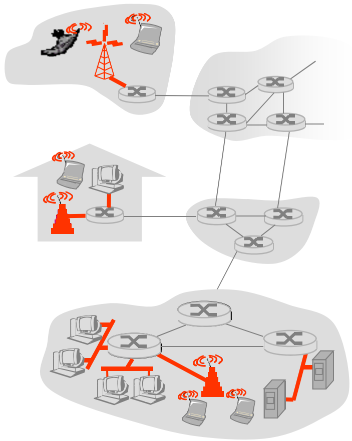
Access networks and physical media

Q: How to connect end systems to edge router?

- residential access nets
- institutional access networks (school, company)
- mobile access networks

Keep in mind:

- bandwidth (bits per second) of access network?
- shared or dedicated?



Physical Media

- Twisted Pairs
- Coaxial Cable
- Fiber Optics
- Radio Links
  - Terrestrial microwave
  - WLAN (e.g., WiFi)
  - Wide-Area (e.g., Cellular)
  - Satellite

Physical Media

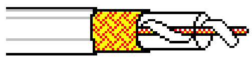
- Bit
  - propagates between transmitter/rcvr pairs
- Physical link
  - what lies between transmitter & receiver
- Guided media:
  - signals propagate in solid media: copper, fiber, coax
- Unguided media:
  - signals propagate freely, e.g., radio

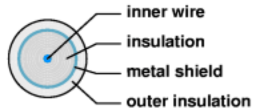
Physical Media: twisted pairs

- Two insulated copper wires
  - UTP: Unshielded Twisted Pairs
    - Category 3: traditional phone wires, 10 Mbps Ethernet
    - Category 5: 100Mbps Ethernet
  - ScTP: Screened Twisted Pairs
  - STP: Shielded Twisted Pairs

Physical Media: coaxial cable

- two concentric copper conductors
- bidirectional
- baseband:
  - single channel on cable
  - legacy Ethernet
- broadband:
  - multiple channels on cable
  - Hybrid Fiber Cable (HFC)





Physical Media: fiber optics

- glass fiber carrying light pulses
  - each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10's-100's Gps)
- low error rate
  - repeaters spaced far apart;
  - immune to electromagnetic noise

Physical Media: radio

- signal carried in electromagnetic spectrum
- no physical "wire"
- bidirectional
- propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

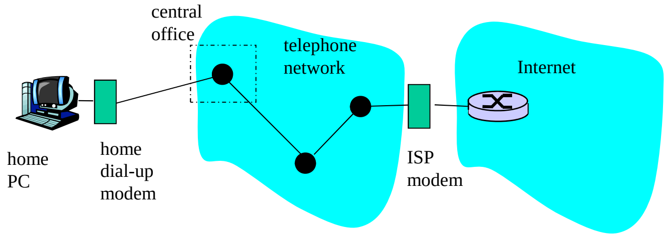
Physical Media: radio link types

- Terrestrial microwave
  - e.g. up to 45 Mbps channels
- LAN (e.g., Wifi)
  - 11Mbps, 54 Mbps, 108 Mbps, … 600 Mbps, …
- wide-area (e.g., cellular)
  - 3G cellular: ~ Mbps
- satellite
  - Kbps to 45Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - geosynchronous versus low altitude

Access Networks

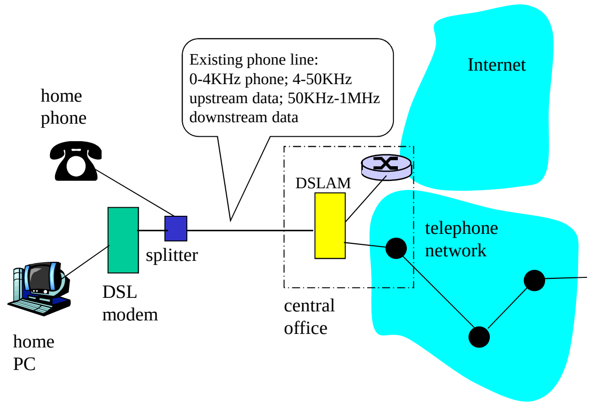
- Dial-up Modem
- Digital Subscriber Line (DSL)
- Cable Modem
- Fiber-To-The-Home (FTTH)
- Ethernet
- WiFi
- Wide-Area Wireless Access
- WiMax

Dial-up Modem



- Uses existing telephony infrastructure
  - Home is connected to central office
- up to 56Kbps direct access to router (often less)
- Can't surf and phone at same time: not "always on"

Digital Subscriber Line (DSL)



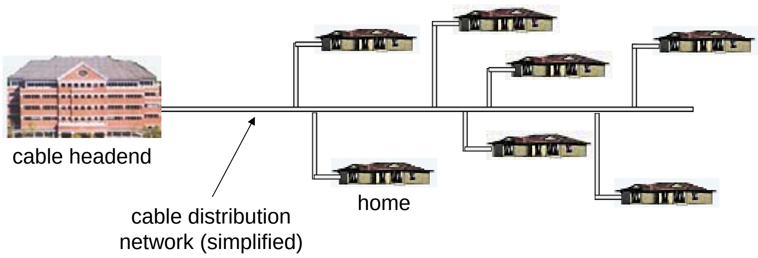
- Also uses existing telephone infrastructure
- up to 1.8-2.5 Mbps upstream
- up to 12-24 Mbps downstream
- dedicated physical line to telephone central office

Residential access: cable modems

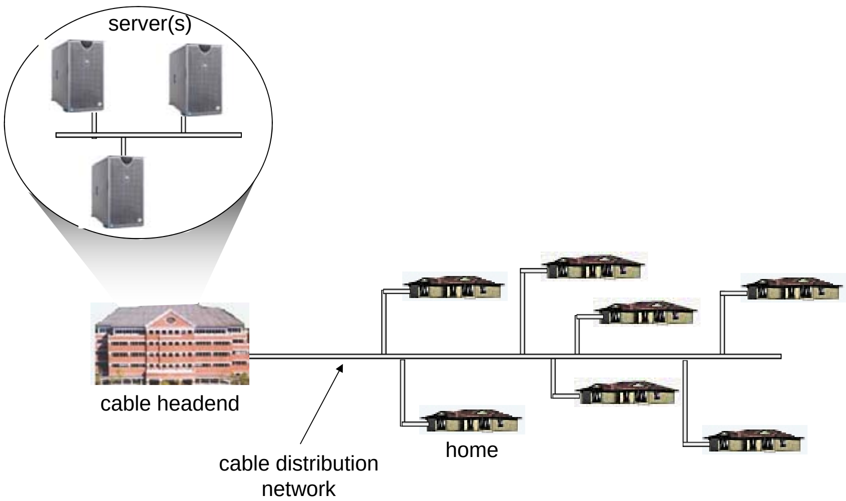
- Does not use telephone infrastructure
  - Instead uses cable TV infrastructure
- HFC: hybrid fiber coax
  - asymmetric: up to 42.8 Mbps downstream, up to 30.7 Mbps upstream
- network of cable and fiber attaches homes to ISP router
  - homes share access to router
  - unlike DSL, which has dedicated access

Cable Network Architecture: Overview

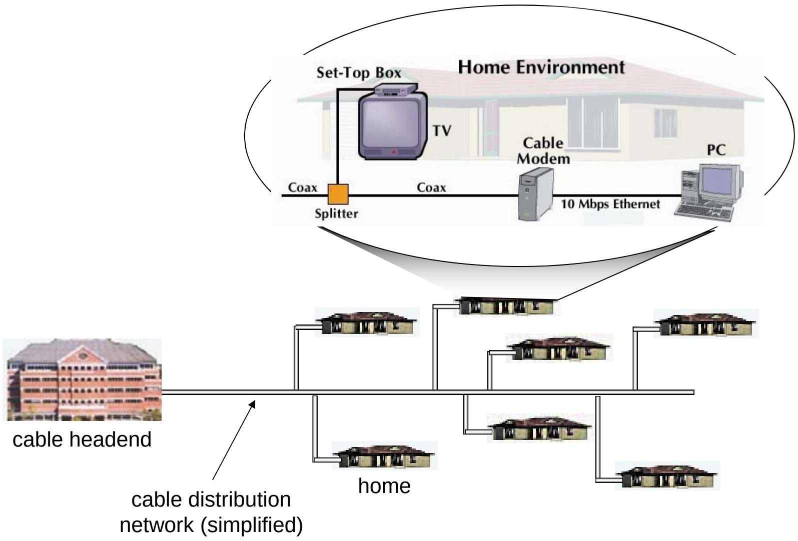
Typically 500 to 5,000 homes



Cable Network Architecture: Overview

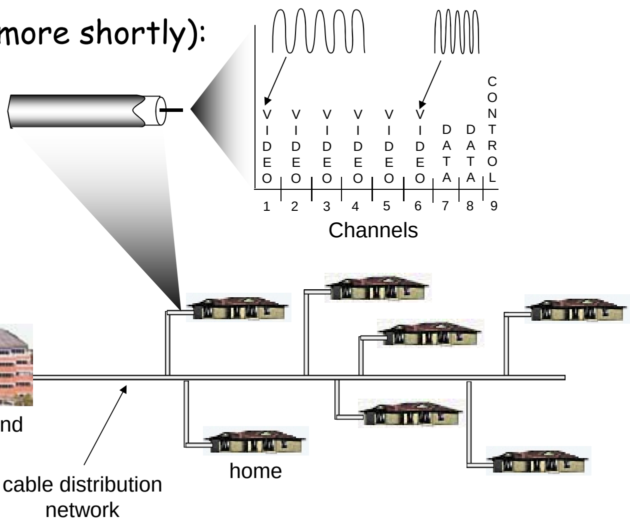


Cable Network Architecture: Overview

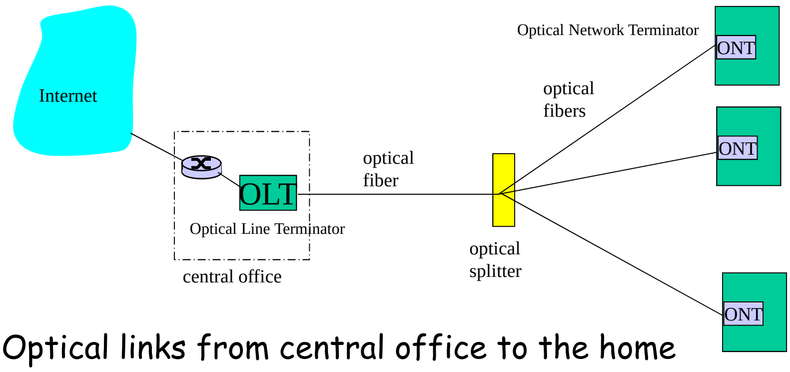


Cable Network Architecture: Overview

FDM (more shortly):

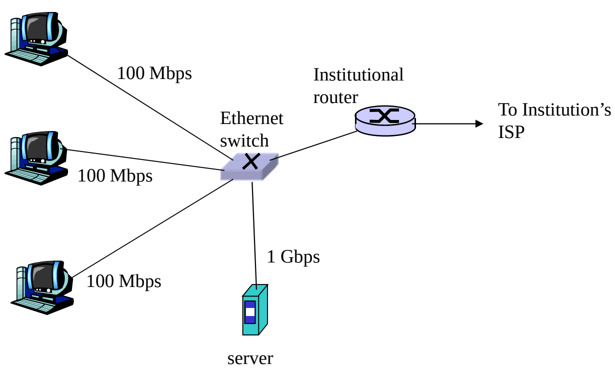


Fiber to the Home



- Optical links from central office to the home
  - Much higher Internet rates (up to Gbps, typically 20 Mbps)
  - Fiber also carries television and phone services
- Two competing optical technologies:
  - Passive Optical network (PON)
  - Active Optical Network (PAN)
    - Similar to switched Ethernet

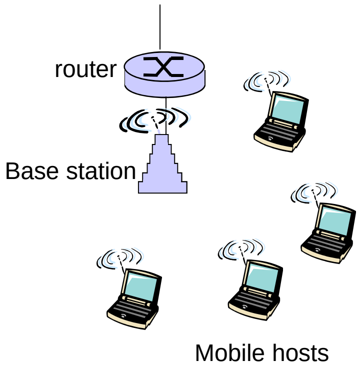
Ethernet Internet access



- Typically used in companies, universities, etc
- 10 Mbs, 100Mbps, 1Gbps, 10Gbps Ethernet
- Today, end systems typically connect into Ethernet switch

Wireless access networks

- shared *wireless* access network connects end system to router
  - via base station aka "access point"
- wireless LANs (WiFi):
  - 802.11b/g: 11/54/Mbps
  - 802.11 a: up to 54 Mbps
  - 802.11n: up to 600 Mbps
  - 802.11ac: up to 3 Gbps
- wider-area wireless access
  - provided by telco operator
  - ~Mbps over cellular system (EVDO, HSDPA)
  - next:LTE



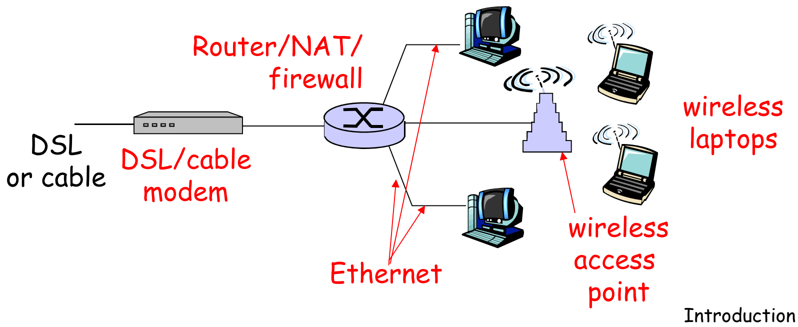
Access Networks

- Residential Access
  - Dial-up Modem
  - Digital Subscriber Line (DSL)
  - Cable Modem, Fiber-To-The-Home (FTTH)
  - Ethernet
  - WiFi
  - Cellular
- Univerity/Corporate Campuses
  - Ethernet
  - WiFi
- Mobile Access
  - WiFi hotspot
  - Cellular

Home networks

Typical home network components:

- DSL or cable modem
- router/firewall/NAT
- Ethernet
- wireless access point



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

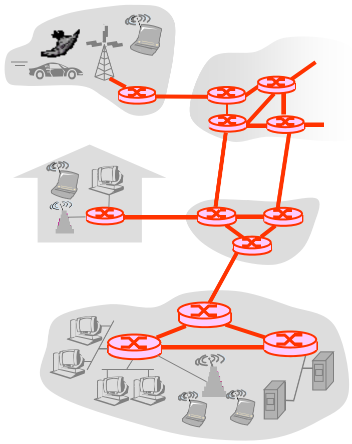
1.5 Protocol layers, service models

1.6 Networks under attack: security

1.7 History

The Network Core

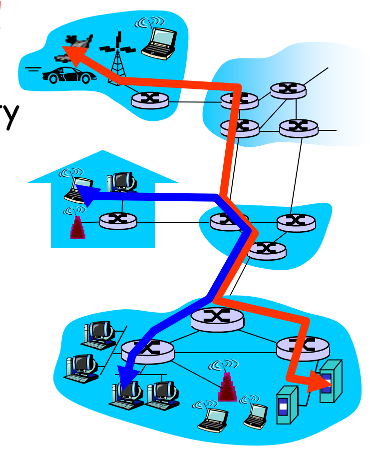
- mesh of interconnected routers
- *the* fundamental question: how is data transferred through net?
  - circuit switching: dedicated circuit per call: telephone net
  - packet-switching: data sent thru net in discrete "chunks"



Network Core: Circuit Switching

End-end resources reserved for "call"

- link bandwidth, switch capacity
- dedicated resources
  - no sharing
- circuit-like
  - guaranteed performance
- call setup required



Network Core: Circuit Switching

network resources (e.g., bandwidth) divided into "pieces"

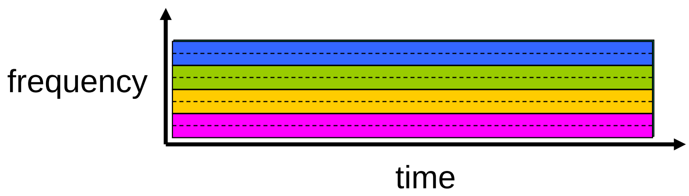
- pieces allocated to calls
- resource piece *idle* if not used by owning call *(no sharing)*
- dividing link bandwidth into "pieces"
  - frequency division
  - time division

Circuit Switching: FDM and TDM

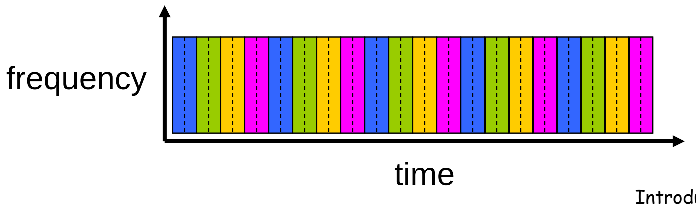
Example:

4 users

FDM



TDM



Network Core: Packet Switching

each end-end data stream divided into *packets*

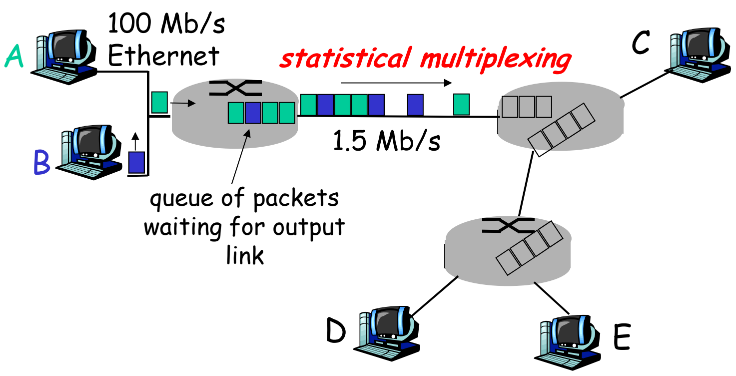
- user A, B packets *share* network resources
- each packet uses full link bandwidth
- resources used *as needed*

Bandwidth division into "pieces"
Dedicated allocation
Resource reservation

resource contention:

- aggregate resource demand can exceed amount available
- congestion: packets queue, wait for link use
- store and forward: packets move one hop at a time
  - Node receives complete packet before forwarding

Packet Switching: Statistical Multiplexing

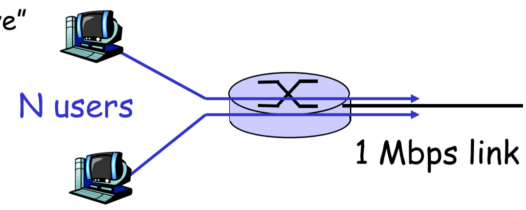


Sequence of A & B packets does not have fixed pattern, bandwidth shared on demand ➔ ***statistical multiplexing***

Packet switching versus circuit switching

Packet switching allows more users to use network!

- 1 Mb/s link
- each user:
  - 100 kb/s when "active"
  - active 10% of time
- *circuit-switching:*
  - 10 users
- *packet switching:*
  - with 35 users, probability > 10 active at same time is less than .0004

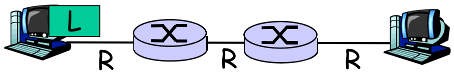


Packet switching versus circuit switching

Is packet switching the winner?

- great for bursty data
  - resource sharing
  - simpler, no call setup
- excessive congestion: packet delay and loss
  - protocols needed for reliable data transfer, congestion control
- Q: How to provide circuit-like behavior?
  - bandwidth guarantees needed for audio/video apps
  - still an unsolved problem

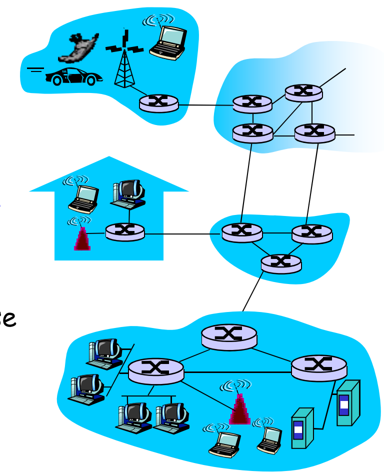
Packet-switching: store-and-forward



- Transmission delay
  - The sender takes L/R seconds to transmit (push out) packet of L bits on to link at R bps
- *store and forward:*
  - entire packet must arrive at router before it can be transmitted on next link
  - Store-and-forward delay (3L/R)
    - assuming zero propagation delay
  - Possible Queuing Delay (Output Buffer)
  - Possible Packet Loss

Packet forwarding in packet-switched nets

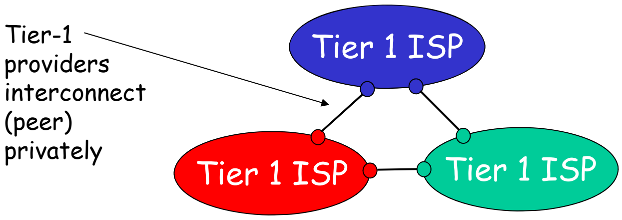
Reference: Internet



- Each packet (datagram) includes a dest address
- An intermediate router
  - Looks at the destination address
  - Uses it (or part of it) to index a forwarding table
  - And derives the output link to use
- How is forwarding table generated?
  - Routing protocols

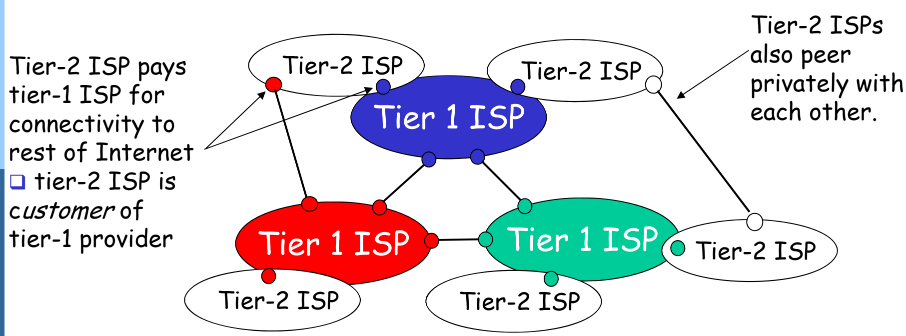
Internet structure: network of networks

- roughly hierarchical
- at center: "tier-1" ISPs (Internet backbone)
  - national/international coverage
  - treat each other as equals



Internet structure: network of networks

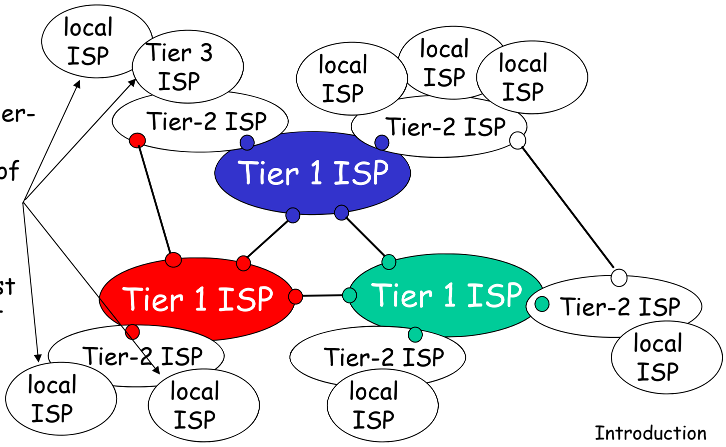
- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs



Internet structure: network of networks

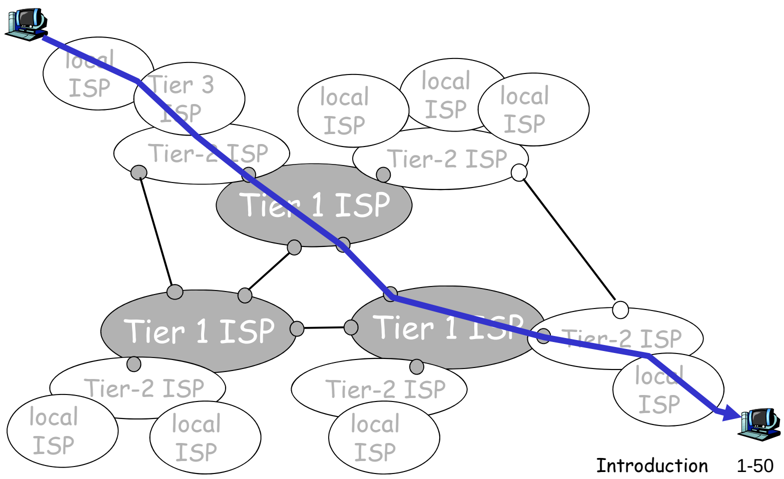
- "Tier-3" ISPs and local ISPs
  - last hop ("access") network (closest to end systems)

Local and tier-3 ISPs are *customers* of higher tier ISPs connecting them to rest of Internet



Internet structure: network of networks

- a packet passes through many networks!



“Real” Internet routes

Traceroute/tracert: from an host at UniTS to www.unipi.it

```
Microsoft Windows 2000 [Versione 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>tracert www.unipi.it

Rilevazione instradamento verso www.unipi.it [131.114.190.24]
su un massimo di 30 punti di passaggio:

  1   <10 ms   <10 ms   <10 ms  rt50.univ.trieste.it [140.105.50.254]
  2   <10 ms   <10 ms   <10 ms  140.105.150.13
  3   <10 ms   <10 ms   <10 ms  utsgw48.univ.trieste.it [140.105.48.231]
  4    31 ms    31 ms    47 ms  rc-units2.ts.garr.net [193.206.132.29]
  5    31 ms    62 ms    47 ms  mi-ts-2.garr.net [193.206.134.53]
  6    47 ms    47 ms    47 ms  bo-mi-2.garr.net [193.206.134.6]
  7   125 ms   125 ms   125 ms  pi-bo-1.garr.net [193.206.134.82]
  8      *     204 ms   281 ms  unipi-rc.pi.garr.net [193.206.136.18]
  9   219 ms   312 ms   250 ms  eth03-gw.unipi.it [131.114.188.61]
 10   219 ms   187 ms   204 ms  131.114.186.1
 11   250 ms   266 ms   266 ms  solaria.adm.unipi.it [131.114.190.24]

Rilevazione completata.

C:\>
```


Roadmap

1.1 What *is* the Internet?
1.2 Network edge
- end systems, access networks, links

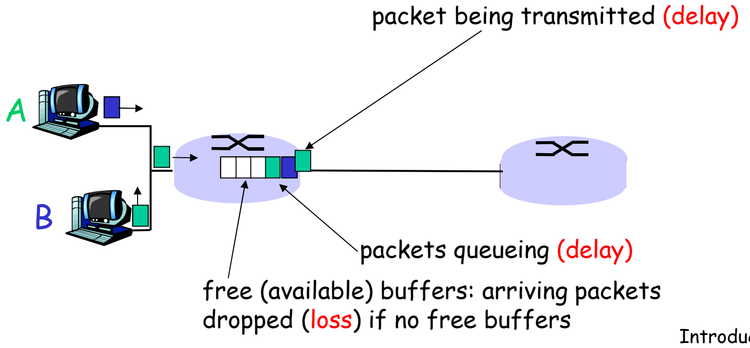
1.3 Network core
- circuit switching, packet switching, network structure

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

How do loss and delay occur?

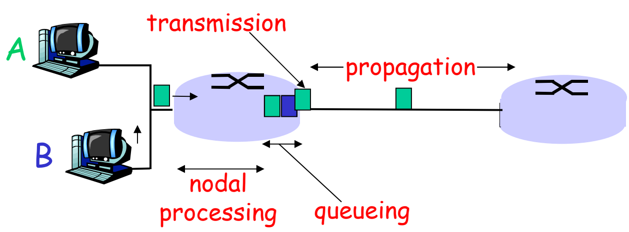
packets *queue* in router buffers

- packet arrival rate to link exceeds output link capacity
- packets queue, wait for turn



Four sources of packet delay

- 1. nodal processing:
  - check bit errors
  - determine output link
- 2. queueing
  - time waiting at output link for transmission
  - depends on congestion level of router

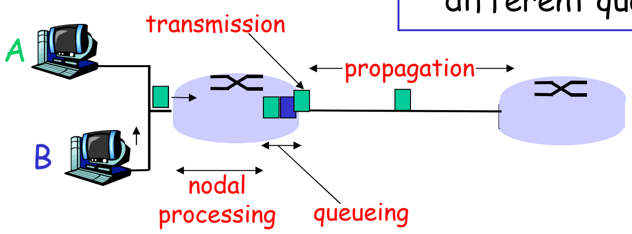


Delay in packet-switched networks

3. Transmission delay:
- R=link bandwidth (bps)
- L=packet length (bits)
- time to send bits into link = L/R

4. Propagation delay:
- d = length of physical link
- s = propagation speed in medium (~2×10^8 m/sec)
- propagation delay = d/s

Note: s and R are *very* different quantities!



Total Nodal (Hop) Delay

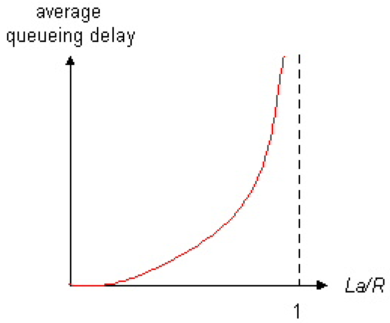
$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

- d_{proc} = processing delay
  - typically a few microsecs or less
- d_{queue} = queuing delay
  - depends on congestion
- d_{trans} = transmission delay
  - = L/R, significant for low-speed links
- d_{prop} = propagation delay
  - a few microsecs to hundreds of msecs

Queueing delay (revisited)

- R=link bandwidth (bps)
- L=packet length (bits)
- a=average packet arrival rate

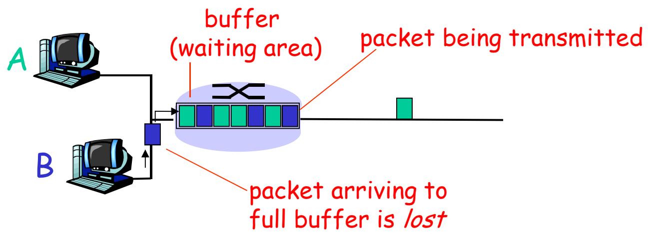
traffic intensity = La/R



- La/R ~ 0: average queueing delay small
- La/R -> 1: delays become large
- La/R > 1: more "work" arriving than can be serviced, average delay infinite!

Packet loss

- queue (aka buffer) preceding link in buffer has finite capacity
- packet arriving to full queue dropped (aka lost)
- lost packet may be retransmitted by previous node, by source end system, or not at all



“Real” Internet delays and routes

Traceroute/tracert: to www.unipi.it

Three delay measurements from source to www.unipi.it

```
Microsoft Windows 2000 [Versione 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>tracert www.unipi.it

Rilevazione instradamento verso www.unipi.it [131.114.190.24]
su un massimo di 30 punti di passaggio:

  1   <10 ms   <10 ms   <10 ms  rt50.univ.trieste.it [140.105.50.254]
  2   <10 ms   <10 ms   <10 ms  140.105.150.13
  3   <10 ms   <10 ms   <10 ms  utsgw48.univ.trieste.it [140.105.48.231]
  4    31 ms    31 ms    47 ms  rc-units2.ts.garr.net [193.206.132.29]
  5    31 ms    62 ms    47 ms  mi-ts-2.garr.net [193.206.134.53]
  6    47 ms    47 ms    47 ms  bo-mi-2.garr.net [193.206.134.6]
  7   125 ms   125 ms   125 ms  pi-bo-1.garr.net [193.206.134.82]
  8      *     204 ms   281 ms  unipi-rc.pi.garr.net [193.206.136.18]
  9   219 ms   312 ms   250 ms  eth03-gw.unipi.it [131.114.188.61]
 10   219 ms   187 ms   204 ms  131.114.186.1
 11   250 ms   266 ms   266 ms  solaria.adm.unipi.it [131.114.190.24]

Rilevazione completata.

C:\>
```

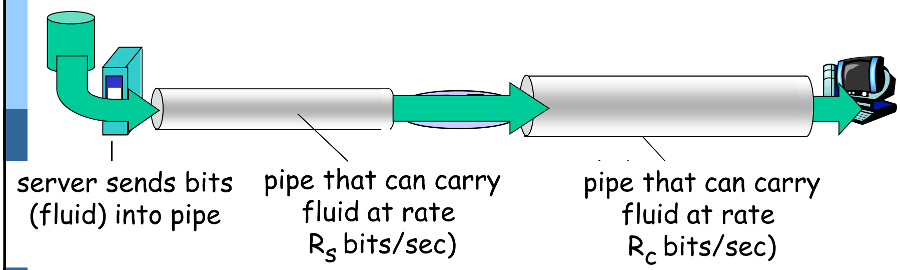

End-to-End Delay

- N-1 Routers between sender and destination
  - Each packet has to be transmitted N times

$$d_{e2e} = N(d_{proc} + d_{queue} + d_{trans} + d_{prop})$$

Throughput

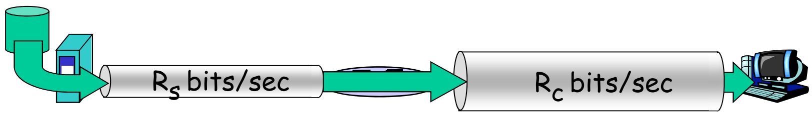
- *throughput:* rate (bits/time unit) at which bits transferred between sender/receiver
  - *instantaneous:* rate at given point in time
  - *average:* rate over longer period of time



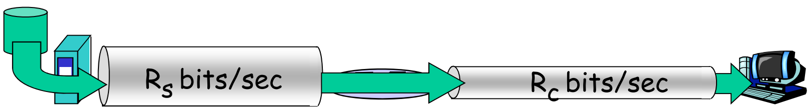
Introduction 1-61

Throughput (more)

- $R_s < R_c$ What is average end-end throughput?



- $R_s > R_c$ What is average end-end throughput?



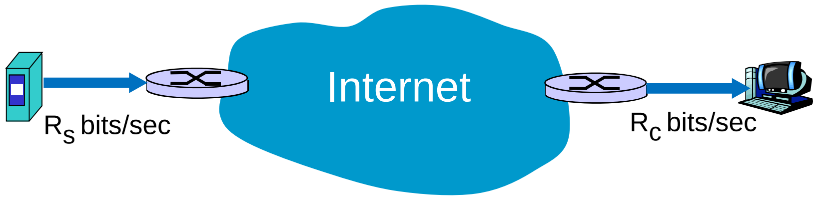
bottleneck link

link on end-end path that constrains end-end throughput

Introduction 1-62

Throughput (more)

- A client downloads a file from a server

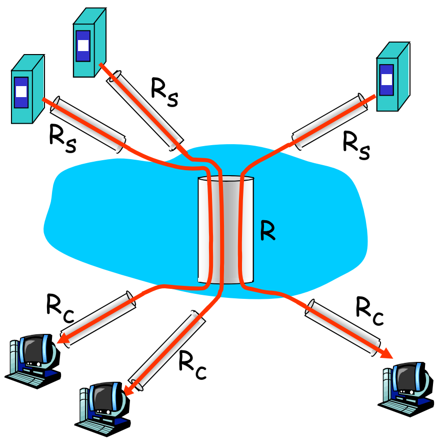


What is the average end-to-end throughput?

$\min(R_c, R_s)$

Throughput: Internet scenario

- per-connection end-to-end throughput: $\min(R_c, R_s, R/10)$
- in practice: R_c or R_s is often bottleneck



10 connections (fairly) share backbone bottleneck link R bits/sec

Roadmap

Protocol "Layers"

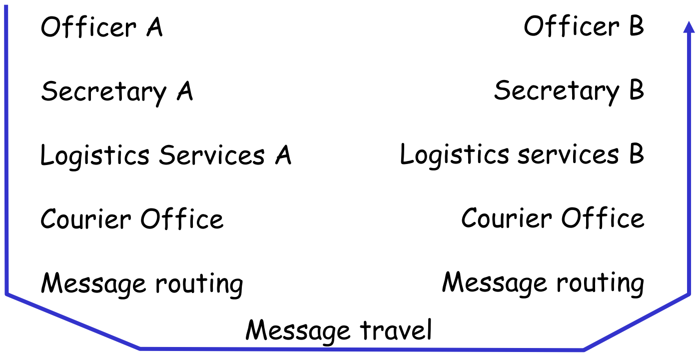
Networks are complex!

- 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 postal service



- a series of steps

Organization of postal service

Layers: each layer implements a service

- via its own internal-layer actions
- Following a specific protocol
- relying on services provided by layer below

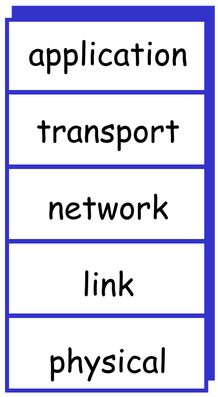
Why layering?

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?

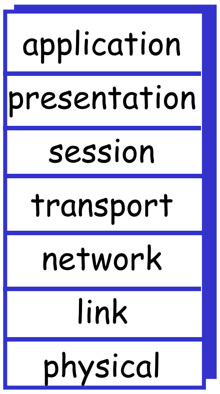
Internet protocol stack

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

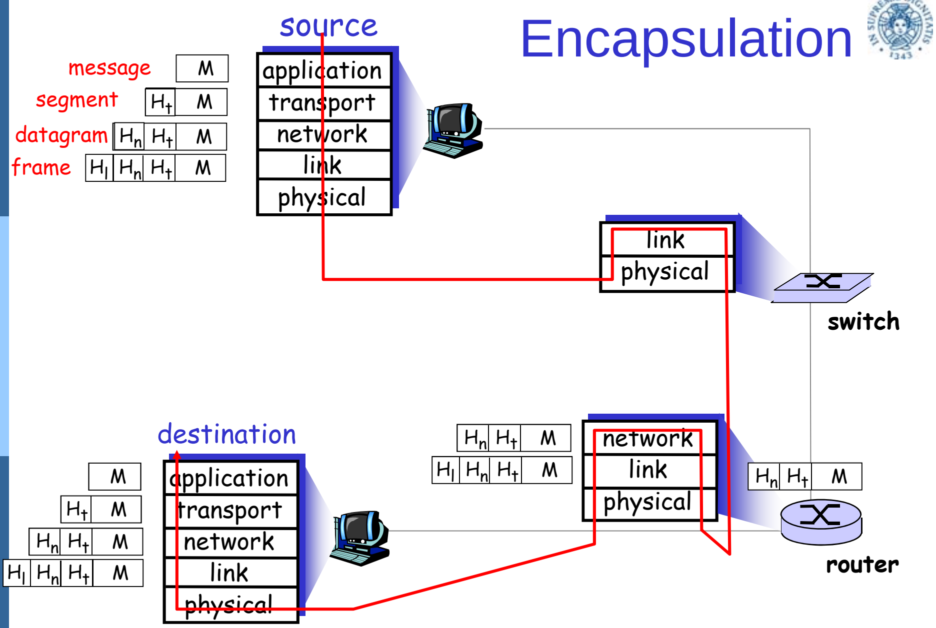


ISO/OSI reference model

- **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?



Encapsulation



Roadmap

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" ☺
  - Security considerations in all layers!

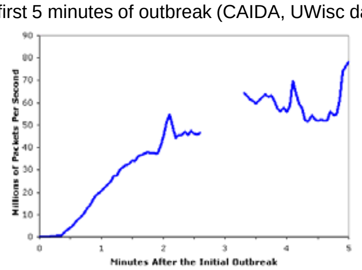
Bad guys can put malware into hosts via Internet

- Malware can get in host from a virus, worm, or trojan horse.
- Spyware malware can record keystrokes, web sites visited, upload info to collection site.
- 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

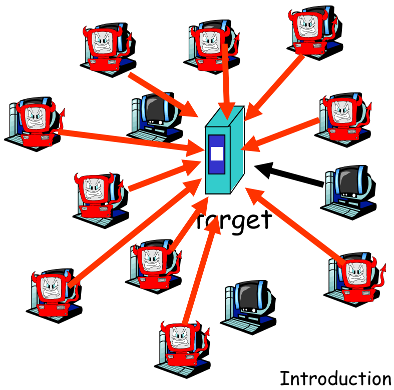
Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)



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

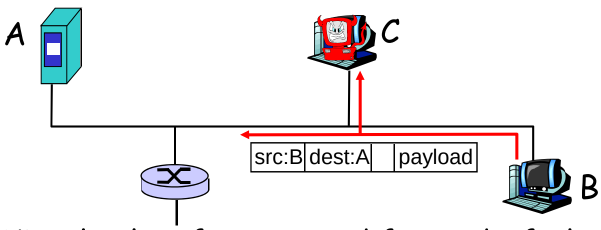
1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts



The bad guys can sniff packets

Packet sniffing:

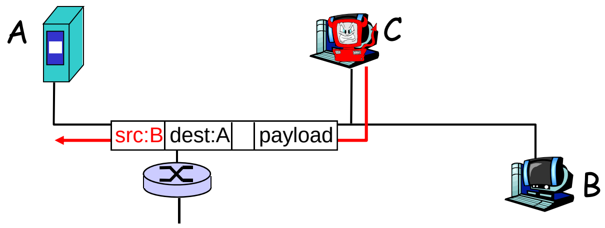
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



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

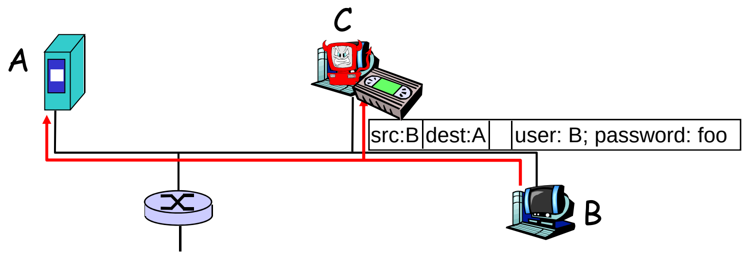
The bad guys can use false source addresses

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



The bad guys can record and playback

- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view



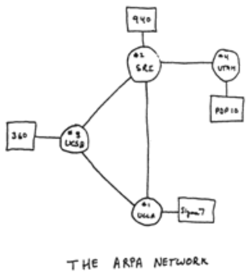
Roadmap

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
- late70'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
- 1986: first Italian node connected to the Internet (Pisa)
- 1988: TCP congestion control
- new national networks: Csnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks

Internet History

- First Italian node connected to the Internet
  - 30 Aprile 1986
  - Nodo CNUCE, Pisa


Consiglio Nazionale delle Ricerche
Istituto CNUCE

Pisa 12/5/86

Prot. n. 1922

Prof. L. Rossi Bernardi
Presidente del CNR

Prof. G. Biorci
Presidente CGI

Ing. S. Trumpy
Direttore CNUCE

Oggetto: Collegamento del CNUCE ad ARPANET.

Dal 30 Aprile scorso, il sistema di calcolo dell'Istituto CNUCE è stato collegato alla rete di elaboratori USA denominata ARPANET (Advanced Research Projects Agency NETwork). Tale rete, sponsorizzata dal Dipartimento della Difesa USA, collega ormai parecchie migliaia di elaboratori eterogenei per dimensione e per costruttore, operanti presso i più prestigiosi Centri di Ricerca, Università ed Istituzioni Militari prevalentemente USA.

Dopo la Norvegia, la Gran Bretagna e la Germania Ovest, l'Italia è la quarta nazione europea dotata di accesso ad ARPANET tramite la sottorete via satellite SATNET (SATellite NETwork) (Allegato 1).

A livello italiano tale collegamento è il risultato di una cooperazione tra CNR, TELESPAZIO ed ITALCABLE; cooperazione sancita dalla stipula di un comune contratto triennale che scadrà nell'Agosto del 1987.

Voluta dalla CGI per attuare la politica del calcolo scientifico dell'Ente, ARPANET consente adesso all'utente scientifico italiano collegato al CNUCE di accedere ai servizi disponibili presso gli altri elaboratori della rete e viceversa.

Data la riservatezza dei dati residenti presso gli elaboratori che operano soprattutto in ambito militare, e in conformità alle norme del suddetto contratto, l'accesso dell'utente CNUCE dovrà essere autorizzato, oltre che dal CNR, anche da TELESPAZIO, ITALCABLE e della DARPA (Defence Advanced Research Projects Agency).

Cordiali Saluti

Luciano Lenzini

PS: Allego copia della bozza del comunicato stampa il cui contenuto deve essere concordato con TELESPAZIO ed ITALCABLE.

CNUCE
36 VIA S. MARIA - 56100 - PISA
Telegrammi CNUCE - PISA

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

2009:

- ~1 billion hosts
- Voice, Video over IP
- P2P applications: BitTorrent (file sharing) Skype (VoIP), PPLive (video)
- Cloud Computing applications: YouTube, gaming, …
- wireless, mobility

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!*