What's the Internet: "nuts and bolts" view
- protocols control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, FTP, PPP
- Internet: "network of networks"
  - loosely hierarchical
  - public Internet versus private intranet
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force

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

What's a protocol?
- network protocols:
  - 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

What's the Internet: a service view
- communication infrastructure enables distributed applications:
  - Web, email, games, e-commerce, file sharing
- communication services provided to apps:
  - Connectionless unreliable
  - connection-oriented reliable

What's a protocol?
a human protocol and a computer network protocol:
A closer look at network structure:

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

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. Gnutella, KaZaA

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)

Circuit Switching: FDM and TDM

- **FDM**
  - dividing link bandwidth into “pieces”
  - frequency division
  - time division

- **TDM**
  - frequency division
  - time division

Example: 4 users
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

Packet Switching: Statistical Multiplexing

- A 10 Mb/s Ethernet
- B 1.5 Mb/s

queue of packets waiting for output link

Sequence of A & B packets does not have fixed pattern ➔ statistical multiplexing.
In TDM each host gets same slot in revolving TDM frame.

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 less than .0004

N users
1 Mbps link

Packet switching versus circuit switching

Is packet switching a "slam dunk 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 (chapter 6)

Packet-switching: store-and-forward

- Takes L/R seconds to transmit (push out) packet of L bits on to link or R bps
- Entire packet must arrive at router before it can be transmitted on next link: store and forward
- delay = 3L/R

Example:
- L = 7.5 Mbits
- R = 1.5 Mbps
- delay = 15 sec

Network Taxonomy

- Datagram network is not either connection-oriented or connectionless.
- Internet provides both connection-oriented (TCP) and connectionless services (UDP) to apps.
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?

Residential access: point to point access

- Dialup via modem
  - up to 56Kbps direct access to router (often less)
  - Can't surf and phone at same time: can't be "always on"
- ADSL: asymmetric digital subscriber line
  - up to 1 Mbps upstream (today typically < 256 kbps)
  - up to 8 Mbps downstream (today typically < 1 Mbps)
  - FDM: 50 kHz - 1 MHz for downstream
  - 4 kHz - 50 kHz for upstream
  - 0 kHz - 4 kHz for ordinary telephone

Residential access: cable modems

- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream, 2 Mbps upstream
- network of cable and fiber attaches homes to ISP router
  - homes share access to router
- deployment: available via cable TV companies

Cable Network Architecture: Overview

Typically 500 to 5,000 homes
Cable Network Architecture: Overview

Company access: local area networks
- company/univ local area network (LAN) connects end system to edge router
- Ethernet:
  - shared or dedicated link connects end system and router
  - 10 Mbs, 100Mbps, Gigabit Ethernet
- LANs: chapter 5

Wireless access networks
- shared wireless access network connects end system to router
  - via base station aka "access point"
- wireless LANs:
  - 802.11b (WiFi): 11 Mbps
  - wider-area wireless access
    - provided by telco operator
    - 3G ~ 384 kbps
- Will it happen??
- WAP/GPRS in Europe

Home networks
Typical home network components:
- ADSL or cable modem
- router/firewall/NAT
- Ethernet
- wireless access point
to/from cable headend
cable modem router/firewall
wireless access point

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
  - wireless access point
- unguided media:
  - signals propagate freely, e.g., radio

Twisted Pair (TP)
- two insulated copper wires
  - Category 3: traditional phone wires, 10 Mbps Ethernet
  - Category 5: 100Mbps Ethernet
### Physical Media: coax, fiber

**Coaxial cable:**
- two concentric copper conductors
- bidirectional
- baseband:
  - single channel on cable
  - legacy Ethernet
- broadband:
  - multiple channel on cable
  - HFC

**Fiber optic cable:**
- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 5 Gbps)
- low error rate: repeaters spaced far apart; immune to electromagnetic noise

---

### Figure 5-7 NIC Interface Card

---

### Figure 5-8 Unshielded Twisted Pair (UTP) Cable

---

### Figure 5-9 Optical Fiber Cable

---

### Physical media: radio

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

**Radio link types:**
- terrestrial microwave
  - e.g., up to 45 Mbps channels
- LAN (e.g., Wi-Fi)
  - 2 Mbps, 11 Mbps
- wide-area (e.g., cellular)
  - e.g., 3G: hundreds of Mbps
- satellite
  - up to 50 Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - geosynchronous versus low altitude

---

### Internet structure: network of networks

- roughly hierarchical
- at center: "tier-1" ISPs (e.g., UUNet, BBN/Genuity, Sprint, AT&T), national/international coverage
  - treat each other as equals

- Tier-1 providers interconnect (peer) privately
- Tier-1 providers also interconnect at public network access points (NAPs)
Tier-1 ISP: e.g., Sprint
Sprint US backbone network

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

- "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

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. queuing
   - time waiting at output link for transmission
   - depends on congestion level of router
Delay in packet-switched networks

3. Transmission delay:
   \[ R \text{ (link bandwidth, bps)} \times \frac{L \text{ (packet length, bits)}}{R} \]

4. Propagation delay:
   \[ d \text{ (length of physical link)} \times \frac{s \text{ (propagation speed in medium, m/sec)}}{s} \]

Note: \( s \) and \( R \) are very different quantities!

An Example: Caravan analogy

Cars "propagate" at 100 km/hr
Toll booth takes 12 sec to service a car (transmission time)
car~bit; caravan ~ packet
Q: How long until caravan is lined up before 2nd toll booth?

Toll booth takes 12 sec to service a car (transmission time)
car~bit; caravan ~ packet
Q: How long until caravan is lined up before 2nd toll booth?

Packet loss

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

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

- ticket (purchase)
- baggage (check)
- gate (load)
- runway (takeoff)
- airplane routing
- 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?

**Internet protocol stack**

- application: supporting network applications
  - FTP, SMTP, STTP
- transport: host-host 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**

**IP Addressing: introduction**

- IP address: 32-bit identifier for host, router interface
- interface: connection between host/router and physical link
  - router's typically have multiple interfaces
  - host may have multiple interfaces
  - IP addresses associated with each interface

**IPv6**

- Initial motivation: 32-bit address space soon to be completely allocated.
- Additional motivation:
  - header format helps speed processing/forwarding
  - header changes to facilitate QoS

**MAC Addresses and ARP**

- 32-bit IP address:
  - network-layer address
  - used to get datagram to destination IP subnet
- MAC (or LAN or physical or Ethernet) address:
  - 48 bit MAC address (for most LANs) burned in the adapter ROM
**LAN Address (more)**

- MAC address allocation administered by IEEE
- Manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  1. MAC address: like Social Security Number
  2. IP address: like postal address
- MAC flat address → portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on IP subnet to which node is attached

**Elements of a wireless network**

- **Base station**
  - Typically connected to wired network
  - Relay - responsible for sending packets between wired network and wireless host(s) in its “area”
    - e.g., cell towers / 802.11 access points

- **Network infrastructure**

- **Wireless link**
  - Typically used to connect mobile(s) to base station
  - Also used as backbone link
  - Multiple access protocol coordinates link access
  - Various data rates, transmission distance

**Multimedia, Quality of Service: What is it?**

- Multimedia applications: network audio and video ("continuous media")
- **QoS**
  - Network provides level of performance needed for application to function.

**MM Networking Applications**

- Classes of MM applications:
  1. Streaming stored audio and video
  2. Streaming live audio and video
  3. Real-time interactive audio and video
- **Fundamental characteristics:**
  - Typically delay sensitive
  - End-to-end delay
  - Delay jitter
  - But loss tolerant:
    - Infrequent losses cause minor glitches
    - Antithesis of data, which are loss intolerant but delay tolerant.

- **Jitter** is the variability of packet delays within the same packet stream
Streaming Stored Multimedia

Streaming:
- Media stored at source
- Transmitted to client
- Streaming: client playout begins before all data has arrived
- Timing constraint for still-to-be transmitted data: in time for playout

Streaming Multimedia: Client Buffering

Client-side buffering, playout delay compensates for network-added delay, delay jitter

Streaming Multimedia: Client rate(s)

1.5 Mbps encoding

28.8 Kbps encoding

Q: How to handle different client receive rate capabilities?
- 28.8 Kbps dialup
- 100 Mbps Ethernet
A: Server stores, transmits multiple copies of video, encoded at different rates

What is network security?

Confidentiality: Only sender, intended receiver should "understand" message contents
- Sender encrypts message
- Receiver decrypts message

Authentication: Sender, receiver want to confirm identity of each other

Message Integrity: Sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and Availability: Services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- Well-known in network security world
- Bob, Alice (lovers) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages

There are bad guys (and girls) out there!

Q: What can a "bad guy" do?
A: A lot!
- Eavesdrop: Intercept messages
- Actively insert messages into connection
- Impersonation: Can fake (spoof) source address in packet (or any field in packet)
- Hijacking: "Take over" ongoing connection by removing sender or receiver, inserting himself in place
- Denial of service: Prevent service from being used by others (e.g., by overloading resources)

More on this later …
Firewalls

- A firewall isolates an organization's internal network from the larger Internet, allowing some packets to pass, blocking others.

Firewalls: Why

- Prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections.
- Prevent illegal modification/access of internal data:
  - e.g., attacker replaces CIA's homepage with something else
- Allow only authorized access to inside network (set of authenticated users/hosts)
- Two types of firewalls:
  - Application-level
  - Packet-filtering

Virtual Private Network

- Virtual private network (VPN) is the fourth WAN alternative.
- A VPN uses the Internet or a private internet to create the appearance of private point-to-point connections.
- A VPN uses the public Internet to create the appearance of a private connection.
- A connection called a tunnel, is a virtual pathway over a public or shared network from the VPN client to the VPN server.

Virtual Private Network (Continued)

- VPN communications are secure:
  - The VPN client software encrypts or codes, the original messages so that its contents are hidden.
- Virtual private networks offer the benefit of point-to-point leased lines, and they enable remote access, both by employees and by any others who have been registered with the VPN server.

Figure 5-18 Remote Access Using VPN: Actual Connections

Figure 5-19 Remote Access Using VPN: Apparent Connection
**Criteria for Comparing Network Alternatives**

- Many different computer networking alternatives are available, each with different characteristics.
- There are three types of costs that need to be considered.
  - **Setup costs** include the costs of acquiring transmission lines and necessary equipment, such as switches, routers, and access devices.
  - **Operational costs** include lease fees for lines and equipment, charges of the ISP, the cost of ongoing training, etc.
  - **Maintenance costs** include those for periodic maintenance, problem diagnosis and repair, and mandatory upgrades.

**Criteria for Comparing Network Alternatives (Continued)**

- There are six considerations with regard to performance:
  - Speed
  - Latency
  - Availability
  - Loss rate
  - Transparency
  - Performance guarantees

- Other criteria to consider when comparing network alternatives include the growth potential (greater capacity) and the length of contract commitment.

**Domain Name System**

- IP addresses are useful for computer-to-computer communication, but they are not well suited for human use.
- The purpose of the domain name system (DNS) is to convert user-friendly names into their IP addresses.
- Any registered, valid name is called a domain name.
- The process of changing a name into its IP address is called resolving the domain name.
- Every domain name must be unique, worldwide.
- To ensure duplicate domain names do not occur, an agency registers names and records the corresponding IP addresses in a global directory.

**Domain Name Registration**

- ICANN is a nonprofit organization that is responsible for administering the registration of domain names.
- ICANN does not register domain names itself; instead it licenses other organizations to register names.
- ICANN is also responsible for managing the domain name resolution system.
- The last letter in any domain name is referred to as the top-level-domain (TLD).
  - In the domain www.icann.org, the top level domain is .org.
Domain Name Resolution (Continued)

- A uniform resource locator (URL) is a document’s address on the Web.
- URLs begin with a domain and then are followed by optional data that locates a document with that domain.
  - Thus, in the URL www.prenhall.com/kroenke, the domain name is www.prenhall.com, and /kroenke is a directory within that domain.

- Domain name resolution is the process of converting a domain name into a public IP address.
- The process starts from the TLD and works to the left across the URL.
- As of 2005, ICANN manages 13 special computers called root servers that are distributed around the world.
- Each root server maintains a list of IP addresses of servers that each resolve each type of TLD.

Domain Name Resolution (Continued)

- Domain name resolution proceeds quickly because there are thousands of computers called domain name resolvers that store the correspondence of domain names and IP addresses.
  - These resolvers reside at ISPs, academic institutions, large companies, government organizations, etc.
  - For example, if a domain name resolver is on your campus and whenever anyone on your campus needs to resolve a domain name, that resolver will store, or cache, the domain name and IP address on a local file.
  - When someone else on the campus needs to resolve the same domain name, the resolver can supply the IP address from the local file.

Internet History

1961-1972: Early packet-switching principles

- 1963: 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 demonstrated publicly
  - NCP (Network Control Protocol) first host-host protocol
  - First e-mail program
  - ARPAnet has 15 nodes

1972-1980: Internetworking, new and proprietary nets

- 1970: ALOHAnet satellite network in Hawaii
- 1973: Metcalf’s PhD thesis proposes Ethernet
- 1974: Cerf and Kahn - architecture for interconnecting networks
  - late 70’s: proprietary architectures: DEChet, SNA, XNA
  - late 70’s: switching fixed length packets (ATM precursor)
- 1979: ARPAnet has 200 nodes
Internet History
1990, 2000s: commercialization, the Web, new apps
- Early 1990s: ARPAnet decommissioned
- Early 1990s: Web
  - hypertext [Bush 1945, Nelson 1960s]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, later Netscape
- Late 1990s: commercialization of the Web

Late 1990s – 2000s:
- More killer apps: instant messaging, P2P file sharing
- Network security to forefront
- 1990, 2000s: commercialization, the Web

Introduction: Summary
Covered a "ton" of material!
- Internet overview
- What's a protocol?
- Network edge, core, access network
  - Packet-switching versus circuit-switching
- Internet/ISP structure
- Performance: loss, delay
- Layering and service models
- History

Problem-Solving Guide—Thinking Exponentially Is Not Possible, but…
- Nathan Myhrvold, the chief scientist at Microsoft Corporation during the 1990s, once said that humans are incapable of thinking exponentially.
  - Instead, when something changes exponentially, we think of the fastest linear change we can imagine and extrapolate from there.
  - His point was that no one could then imagine how much growth there would be in magnetic storage and what we would do with it.
  - We have all witnessed exponential growth in a number of areas: Internet connection, Web pages, and the amount of data accessible on the Internet.

Problem Solving Guide—Thinking Exponentially Is Not Possible, but… (Continued)
- Every business, every organization, needs to be thinking about ubiquitous and cheap connectivity that is growing exponentially.
  - What are the new opportunities?
  - What are the new threats?
  - How will our competition react?
  - How should we position ourselves?
  - How should we respond?
- Understand that technology does not drive people to do things they’re never done before, no matter how much the technologists suggest it might.

Reflection Guide—Human Networks Matter More
- The Hungarian writer, Frigyes Karinthy, came up with the idea that everyone on earth is connected to everyone else by five or six people.
  - Today, in fact with the Internet, the number may be closer to three people than five or six.
- Suppose you want to meet your university's president.
  - The president has a secretary who acts as a gatekeeper.
  - If you walk up to that secretary and say, "I'd like a half hour with President Jones," you're likely to be pointed off to some other university administrator.
  - What else can you do?

Reflection Guide—Human Networks Matter More (Continued)
- The problem with the six-degree theory, is that even though those six people do exist, we don't know who they are.
  - Even worse, we often don't know who the person is with whom we want to connect.
- Most successful professionals consistently build personal human networks.
  - They keep building them because they know that somewhere there is someone whom they need to know or will need to know.
  - They meet people at professional and social situations, collect and pass out cards, and engage in pleasant conversation (all part of a social protocol) to expand their networks.