Chapter 1: Introduction

**our goal:**
- get “feel” and terminology
- more depth, detail *later* in course
- approach:
  - use Internet as example

**overview:**
- what’s the Internet?
- what’s a protocol?
- network edge; hosts, access net, physical media
- network core: packet/circuit switching, Internet structure
- performance: loss, delay, throughput
- security
- protocol layers, service models
- history
Chapter 1: roadmap

1.1 what *is* the Internet?
1.2 network edge
   ▪ end systems, access networks, links
1.3 network core
   ▪ packet switching, circuit switching, network structure
1.4 delay, loss, throughput in networks
1.5 protocol layers, service models
1.6 networks under attack: security
1.7 history
What’s the Internet: “nuts and bolts” view

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

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

- **packet switches:**
  - *forward packets (chunks of data)*
  - *routers and switches*
“Fun” Internet-connected devices

- IP picture frame
  http://www.ceiva.com/

- Web-enabled toaster + weather forecaster

- Slingbox: watch, control cable TV remotely

- Tweet-a-watt: monitor energy use

- Sensorized, bed mattress

- Internet refrigerator

- Internet phones
What’s the Internet: “nuts and bolts” view

- **Internet**: “network of networks”
  - Interconnected ISPs
- **Protocols** control sending, receiving of messages
  - e.g., TCP, IP, HTTP, Skype, 802.11
- **Internet standards**
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force
What’s the Internet: a service view

- **infrastructure that provides services to applications:**
  - Web, VoIP, email, games, e-commerce, social nets, ...

- **provides programming interface to apps**
  - hooks that allow sending and receiving app programs to “connect” to Internet
  - provides service options, analogous to postal service
What’s a protocol?

**human protocols:**
- “what’s the time?”
- “I have a question”
- introductions

... specific messages sent

... specific actions taken when messages received, or other events

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

**protocols define format, order of messages sent and received among network entities, and actions taken on message transmission, receipt**
What’s a protocol?

A human protocol and a computer network protocol:

Q: other human protocols?
Chapter 1: roadmap

1.1 what is the Internet?
1.2 network edge
   ▪ end systems, access networks, links
1.3 network core
   ▪ packet switching, circuit switching, network structure
1.4 delay, loss, throughput in networks
1.5 protocol layers, service models
1.6 networks under attack: security
1.7 history
A closer look at network structure:

- **network edge:**
  - hosts: clients and servers
  - servers often in data centers

- **access networks, physical media:** wired, wireless communication links

- **network core:**
  - interconnected routers
  - network of networks
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?
Access network: digital subscriber line (DSL)

- use existing telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)
Access network: cable network

frequency division multiplexing: different channels transmitted in different frequency bands
Access network: cable network

- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

Data, TV transmitted at different frequencies over shared cable distribution network.
Access network: home network

- Wireless devices
- Often combined in single box
- Wireless access point (54 Mbps)
- To/from headend or central office
- Cable or DSL modem
- Router, firewall, NAT
- Wired Ethernet (1 Gbps)

Introduction 1-15
Enterprise access networks (Ethernet)

- typically used in companies, universities, etc.
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
- 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:**
- within building (100 ft.)
- 802.11b/g/n (WiFi): 11, 54, 450 Mbps transmission rate

**wide-area wireless access**
- provided by telco (cellular) operator, 10’s km
- between 1 and 10 Mbps
- 3G, 4G: LTE
Host: sends packets of data

host sending function:
• takes application message
• breaks into smaller chunks, known as packets, of length \( L \) bits
• transmits packet into access network at transmission rate \( R \)

- link transmission rate, aka link capacity, aka link bandwidth

| packet transmission delay | time needed to transmit \( L \)-bit packet into link | \( = \) \( \frac{L \text{ (bits)}}{R \text{ (bits/sec)}} \) |
Physical media

- **bit**: propagates between transmitter/receiver 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

**twisted pair (TP)**

- two insulated copper wires  
  - Category 5: 100 Mbps, 1 Gbps Ethernet  
  - Category 6: 10Gbps
**Physical media: coax, fiber**

**coaxial cable:**
- two concentric copper conductors
- bidirectional
- broadband:
  - multiple channels on cable

**fiber optic cable:**
- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10’s-100’s Gbps transmission rate)
- 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

**radio link types:**

- **terrestrial microwave**
  - e.g. up to 45 Mbps channels
- **LAN** (e.g., WiFi)
  - 54 Mbps
- **wide-area** (e.g., cellular)
  - 4G cellular: ~ 10 Mbps
- **satellite**
  - Kbps to 45Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - geosynchronous versus low altitude
Chapter 1: roadmap

1.1 what *is* the Internet?
1.2 network edge
  - end systems, access networks, links
1.3 network core
  - packet switching, circuit switching, network structure
1.4 delay, loss, throughput in networks
1.5 protocol layers, service models
1.6 networks under attack: security
1.7 history
The network core

- mesh of interconnected routers
- packet-switching: hosts break application-layer messages into *packets*
  - forward packets from one router to the next, across links on path from source to destination
  - each packet transmitted at full link capacity
Packet-switching: store-and-forward

- Takes $L/R$ seconds to transmit (push out) $L$-bit packet into link at $R$ bps
- *Store and forward*: entire packet must arrive at router before it can be transmitted on next link

**One-hop numerical example:**
- $L = 7.5$ Mbits
- $R = 1.5$ Mbps
- One-hop transmission delay = 5 sec
- End-end delay = $2L/R$ (assuming zero propagation delay)
Packet Switching: queueing delay, loss

**queuing and loss:**

- If arrival rate (in bits) to link exceeds transmission rate of link for a period of time:
  - Packets will queue, wait to be transmitted on link
  - Packets can be dropped (lost) if memory (buffer) fills up
Two key network-core functions

*Routing:* determines source-destination route taken by packets
- *Routing algorithms*

*Forwarding:* move packets from router’s input to appropriate router output

<table>
<thead>
<tr>
<th>Header Value</th>
<th>Output Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>0100</td>
<td>3</td>
</tr>
<tr>
<td>0101</td>
<td>2</td>
</tr>
<tr>
<td>0111</td>
<td>2</td>
</tr>
<tr>
<td>1001</td>
<td>1</td>
</tr>
</tbody>
</table>

Destination address in arriving packet's header
Alternative core: circuit switching

end-end resources allocated to, reserved for “call” between source & dest:

- in diagram, each link has four circuits.
  - call gets 2\textsuperscript{nd} circuit in top link and 1\textsuperscript{st} circuit in right link.
- dedicated resources: no sharing
  - circuit-like (guaranteed) performance
- circuit segment idle if not used by call \((\textit{no sharing})\)
- commonly used in traditional telephone networks
Circuit switching: FDM versus TDM

FDM

TDM

Example:
4 users
Packet switching versus circuit switching

_packet switching allows more users to use network_

example:
- 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 *

Q: how did we get value 0.0004?
Q: what happens if > 35 users?

* Check out the online interactive exercises for more examples: [http://gaia.cs.umass.edu/kurose_ross/interactive/](http://gaia.cs.umass.edu/kurose_ross/interactive/)
Packet switching versus circuit switching

is packet switching a “slam dunk winner?”

- great for bursty data
  - resource sharing
  - simpler, no call setup
- excessive congestion possible: 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 7)

**Q**: human analogies of reserved resources (circuit switching) versus on-demand allocation (packet-switching)?
Internet structure: network of networks

- End systems connect to Internet via access ISPs (Internet Service Providers)
  - residential, company and university ISPs
- Access ISPs in turn must be interconnected.
  - so that any two hosts can send packets to each other
- Resulting network of networks is very complex
  - evolution was driven by economics and national policies
- Let’s take a stepwise approach to describe current Internet structure
Internet structure: network of networks

**Question:** given millions of access ISPs, how to connect them together?
Internet structure: network of networks

Option: connect each access ISP to every other access ISP?

connecting each access ISP to each other directly doesn't scale: $O(N^2)$ connections.
Internet structure: network of networks

**Option:** connect each access ISP to one global transit ISP?

*Customer and provider* ISPs have economic agreement.

---

**Introduction 1-34**
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors ....
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors … which must be interconnected
Internet structure: network of networks

... and regional networks may arise to connect access nets to ISPs
Internet structure: network of networks

... and content provider networks (e.g., Google, Microsoft, Akamai) may run their own network, to bring services, content close to end users.
Internet structure: network of networks

- at center: small # of well-connected large networks
  - “tier-1” commercial ISPs (e.g., Level 3, Sprint, AT&T, NTT), national & international coverage
  - content provider network (e.g., Google): private network that connects its data centers to Internet, often bypassing tier-1, regional ISPs
Tier-1 ISP: e.g., Sprint

POP: point-of-presence

to/from backbone

peering

to/from customers
Chapter 1: roadmap

1.1 what *is* the Internet?
1.2 network edge
   - end systems, access networks, links
1.3 network core
   - packet switching, circuit switching, network structure
1.4 delay, loss, throughput in 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 (temporarily) exceeds output link capacity
- packets queue, wait for turn

*packet being transmitted* (delay)

*packets queueing* (delay)

free (available) buffers: arriving packets dropped *(loss)* if no free buffers
Four sources of packet delay

- **$d_{\text{proc}}$: nodal processing**
  - check bit errors
  - determine output link
  - typically < msec

- **$d_{\text{queue}}$: queueing delay**
  - time waiting at output link for transmission
  - depends on congestion level of router

- **$d_{\text{trans}}$: transmission delay**

- **$d_{\text{prop}}$: propagation delay**

\[
d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}
\]
**Four sources of packet delay**

- **Transmission delay ($d_{trans}$):**
  - $L$: packet length (bits)
  - $R$: link bandwidth (bps)
  - $d_{trans} = L/R$

- **Propagation delay ($d_{prop}$):**
  - $d$: length of physical link
  - $s$: propagation speed ($\sim 2 \times 10^8$ m/sec)
  - $d_{prop} = d/s$

*Check out the online interactive exercises for more examples: [http://gaia.cs.umass.edu/kurose_ross/interactive/](http://gaia.cs.umass.edu/kurose_ross/interactive/)*

*Check out the Java applet for an interactive animation on trans vs. prop delay*
Caravan analogy

- cars “propagate” at 100 km/hr
- toll booth takes 12 sec to service car (bit transmission time)
- car ~ bit; caravan ~ packet
- Q: How long until caravan is lined up before 2nd toll booth?
- time to “push” entire caravan through toll booth onto highway = 12*10 = 120 sec
- time for last car to propagate from 1st to 2nd toll booth: 100km/(100km/hr) = 1 hr
- A: 62 minutes
Caravan analogy (more)

- Suppose cars now “propagate” at 1000 km/hr
- And suppose toll booth now takes one min to service a car
- **Q:** Will cars arrive to 2nd booth before all cars serviced at first booth?
  - **A:** Yes! after 7 min, first car arrives at second booth; three cars still at first booth
Queueing delay (revisited)

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

\[ \text{traffic intensity} = \frac{La}{R} \]

- \( \frac{La}{R} \sim 0 \): avg. queueing delay small
- \( \frac{La}{R} \to 1 \): avg. queueing delay large
- \( \frac{La}{R} > 1 \): more “work” arriving than can be serviced, average delay infinite!

* Check online interactive animation on queuing and loss
“Real” Internet delays and routes

- what do “real” Internet delay & loss look like?
- **traceroute** program: provides delay measurement from source to router along end-end Internet path towards destination. For all $i$:
  - sends three packets that will reach router $i$ on path towards destination
  - router $i$ will return $ith$ packets to sender
  - sender times interval between transmission and reply.
“Real” Internet delays, routes

traceroute: gaia.cs.umass.edu to www.eurecom.fr

1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms  5 ms  5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms  11 ms  13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms  18 ms  18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms  109 ms  106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms  102 ms  104 ms
10 de.fr1.fr.geant.net (62.40.96.50)  113 ms  121 ms  114 ms
11 renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12 nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13 nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14 r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15 eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16 194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17 ***
18 ***  * means no response (probe lost, router not replying)
19 fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms

* Do some traceroutes from exotic countries at wwwtraceroute.org
Packet loss

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

* Check out the Java applet for an interactive animation on queuing and loss
**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

![Diagram of server sending bits (fluid) into pipe, pipe that can carry fluid at rate $R_s$ bits/sec, and pipe that can carry fluid at rate $R_c$ bits/sec.](image)
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
Throughput: Internet scenario

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

* Check out the online interactive exercises for more examples: [http://gaia.cs.umass.edu/kurose_ross/interactive/](http://gaia.cs.umass.edu/kurose_ross/interactive/)
Chapter 1: roadmap

1.1 what is the Internet?

1.2 network edge
   ▪ end systems, access networks, links

1.3 network core
   ▪ packet switching, circuit switching, network structure

1.4 delay, loss, throughput in networks

1.5 protocol layers, service models

1.6 networks under attack: security

1.7 history
Protocol “layers”

Networks are complex, with 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

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

- ticket (complain)
- baggage (claim)
- gates (unload)
- runway landing
- airplane routing
Layering of airline functionality

<table>
<thead>
<tr>
<th>Ticket (purchase)</th>
<th>Baggage (check)</th>
<th>Gates (load)</th>
<th>Runway (takeoff)</th>
<th>Airplane routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket (complain)</td>
<td>Baggage (claim)</td>
<td>Gates (unload)</td>
<td>Runway (land)</td>
<td>Airplane routing</td>
</tr>
</tbody>
</table>

**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, 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
  - Ethernet, 802.111 (WiFi), PPP
- **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

Introduction 1-61
## The OSI Model (Open Systems Interconnection)

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>TCP/IP Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION 7</td>
<td>FTP services</td>
</tr>
<tr>
<td>PROVIDES SERVICES/PROTOCOLS TO APPLICATIONS</td>
<td></td>
</tr>
<tr>
<td>PRESENTATION 6</td>
<td>ANSI</td>
</tr>
<tr>
<td>DATA FORMATTING, I.E. ANSI COMPRESSION/ENCRYPTION</td>
<td></td>
</tr>
<tr>
<td>SESSION 5</td>
<td>PORTS</td>
</tr>
<tr>
<td>CONTROLS CONVERSATIONS/SESSIONS (DIALOG, CONTROL) INTEGRITY AND RELIABILITY DESCRIPTIVE NAMING</td>
<td>DATA SERVICES SOME FIREWALLS</td>
</tr>
<tr>
<td>TRANSPORT 4</td>
<td>TRANSPARENT</td>
</tr>
<tr>
<td>FRAGMENTATION/SEQUENCING OF DATA RELIABLE DELIVERY ERROR RECOVERY FLOW CONTROL MUXING(PORTS)</td>
<td>DATA SERVICES SOME FIREWALLS</td>
</tr>
<tr>
<td>NETWORK 3</td>
<td>ROUTERS</td>
</tr>
<tr>
<td>END TO END DELIVERY LOGICAL ADDRESSING FRAGMENTATION/SEQUENCING FOR MTU ROUTING</td>
<td></td>
</tr>
<tr>
<td>DATA-LINK 2</td>
<td>BRIDGES OR SWITCHES</td>
</tr>
<tr>
<td>PHYSICAL 1</td>
<td>HUBS</td>
</tr>
<tr>
<td>PHYSICAL ADDRESSING ERROR DETECTION (FCS/CRC) ACKNOWLEDGMENTS PACKET/FRAME HEADER AND TRAILER BRIDGING</td>
<td>NETWORK INTERFACE</td>
</tr>
<tr>
<td>TRANSMISSION METHOD SIGNAL STRENGTH TOPOLOGY</td>
<td></td>
</tr>
</tbody>
</table>

© Copyright 2008 Steven Iveson
www.networkstuff.eu
I want to download a web page from this address: 192.168.1.102
Chapter 1: roadmap

1.1 what is the Internet?
1.2 network edge
   ▪ end systems, access networks, links
1.3 network core
   ▪ packet switching, circuit switching, network structure
1.4 delay, loss, throughput in networks
1.5 protocol layers, service models
1.6 networks under attack: security
1.7 history
Network security

- field of network security:
  - 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!
Bad guys: put malware into hosts via Internet

- malware can get in host from:
  - *virus*: self-replicating infection by receiving/executing object (e.g., e-mail attachment)
  - *worm*: self-replicating infection by passively receiving object that gets itself executed

- spyware malware can record keystrokes, web sites visited, upload info to collection site

- infected host can be enrolled in botnet, used for spam. DDoS attacks
Bad guys: attack server, 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 to target from compromised hosts
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
Bad guys can use fake addresses

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

... lots more on security (throughout, Chapter 8)
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!
Wireshark lab 0: getting started

- Packet capture (pcap)
- Packet analyzer
- Application (www browser, email client)
- Transport (TCP/UDP)
  - Network (IP)
  - Link (Ethernet)
  - Physical
- OS

Copy of all Ethernet frames sent/received