Any problem of your lab?

- Due by this Sunday (Jan 29)
Homework questions

- Available on course website

- Please work on them, but do not submit your answers. The answers will be posted later.
Chapter 2: outline

2.1 principles of network applications
   - app architectures
   - app requirements
2.2 Web and HTTP
2.3 FTP
2.4 electronic mail
   - SMTP, POP3, IMAP
2.5 DNS
2.6 P2P applications
2.7 socket programming with UDP and TCP
DNS: domain name system

Internet hosts, routers:
- IP address (32 bit) - used for addressing datagrams
- “name”, e.g., www.yahoo.com - used by humans

Q: how to map between IP address and name, and vice versa?

Domain Name System:
- distributed database implemented in hierarchy of many name servers
- application-layer protocol: hosts, name servers communicate to resolve names (address/name translation)
**DNS: a distributed, hierarchical database**

Client wants IP for www.amazon.com; 1st approx:

- Client queries root server to find com DNS server
- Client queries .com DNS server to get amazon.com DNS server
- Client queries amazon.com DNS server to get IP address for www.amazon.com
DNS: services, structure

**DNS services**
- hostname to IP address translation
- load distribution
  - replicated Web servers: many IP addresses correspond to one name

**why not centralize DNS?**
- single point of failure
- traffic volume
- distant centralized database
- maintenance

A: *doesn’t scale!"
DNS: root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server

- Verisign, Los Angeles CA (5 other sites)
- USC-ISI Marina del Rey, CA
- ICANN Los Angeles, CA (41 other sites)
- NASA Mt View, CA
- Internet Software C. Palo Alto, CA (and 48 other sites)
- U Maryland College Park, MD
- ARL Aberdeen, MD
- Verisign, Dulles VA (69 other sites)
- Cogent, Herndon, VA (5 other sites)
- NASA DoD Columbus, OH (5 other sites)
- WIDE Tokyo (5 other sites)
- RIPE London (17 other sites)
- Netnod, Stockholm (37 other sites)

13 root name “servers” worldwide
TLD, authoritative servers

**top-level domain (TLD) servers:**
- responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
- Network Solutions maintains servers for .com TLD
- Educause for .edu TLD

**authoritative DNS servers:**
- organization’s own DNS server(s), providing authoritative hostname to IP mappings for organization’s named hosts
- can be maintained by organization or service provider
Local DNS name server

- each ISP (residential ISP, company, university) has one
  - also called “default name server”
- when host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy
DNS name resolution example

- host at cis.poly.edu wants IP address for gaia.cs.umass.edu

iterated query:
- contacted server replies with name of server to contact
- “I don’t know this name, but ask this server”
DNS name resolution example

recursive query:
- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?
DNS: caching, updating records

- once (any) name server learns mapping, it caches mapping
  - cache entries timeout (disappear) after some time (TTL)
  - TLD servers typically cached in local name servers
    - thus root name servers not often visited

- cached entries may be out-of-date (best effort name-to-address translation!)
  - if name host changes IP address, may not be known Internet-wide until all TTLs expire
Chapter 2: outline

2.1 principles of network applications
  • app architectures
  • app requirements

2.2 Web and HTTP

2.3 FTP

2.4 electronic mail
  • SMTP, POP3, IMAP

2.5 DNS

2.6 P2P applications

2.7 socket programming with UDP and TCP
P2P architecture

- no always-on server
- arbitrary end systems directly communicate
- peers are intermittently connected and change IP addresses

**examples:**
- file distribution (BitTorrent)
- Streaming (KanKan)
- VoIP (Skype)

- However, most of them requires a central server to manage the peers
**Question:** how much time to distribute file (size $F$) from one server to $N$ peers?

- peer upload/download capacity is limited resource

```
\textbf{Question:} \text{how much time to distribute file (size $F$) from one server to $N$ peers?}

- peer upload/download capacity is limited resource

```

- Peer upload/download capacity is limited resource

```
\textbf{Application Layer 2-16}

```

File distribution time: client-server

- **server transmission**: must sequentially send (upload) $N$ file copies:
  - time to send one copy: $F/u_s$
  - time to send $N$ copies: $NF/u_s$

- **client**: each client must download file copy
  - $d_{\text{min}} = \text{min client download rate}$
  - min client download time: $F/d_{\text{min}}$

\[ D_{\text{c-s}} \geq \max\{NF/u_s, F/d_{\text{min}}\} \]

- increases linearly in $N$
File distribution time: P2P

- **server transmission:** must upload at least one copy
  - time to send one copy: \(F/u_s\)
- **client:** each client must download file copy
  - min client download time: \(F/d_{\text{min}}\)
- **clients:** as aggregate must download \(NF\) bits
  - max upload rate (limiting max download rate) is \(u_s + \sum u_i\)

\[
D_{P2P} \geq \max\{F/u_s, F/d_{\text{min}}, NF/(u_s + \sum u_i)\}
\]

Increases linearly in \(N\) …
… but so does this, as each peer brings service capacity
Client-server vs. P2P: example

client upload rate = \( u \), \( F/u = 1 \) hour, \( u_s = 10u \), \( d_{min} \geq u_s \)
P2P file distribution: BitTorrent

- file divided into 256Kb chunks
- peers in torrent send/receive file chunks

*tracker*: tracks peers participating in torrent

*torrent*: group of peers exchanging chunks of a file

Alice arrives ...
... obtains list of peers from tracker
... and begins exchanging file chunks with peers in torrent
P2P file distribution: BitTorrent

- peer joining torrent:
  - has no chunks, but will accumulate them over time from other peers
  - registers with tracker to get list of peers, connects to subset of peers ("neighbors")

- while downloading, peer uploads chunks to other peers
- peer may change peers with whom it exchanges chunks
- **churn**: peers may come and go
- once peer has entire file, it may (selfishly) leave or (altruistically) remain in torrent
BitTorrent: requesting, sending file chunks

**requesting chunks:**
- at any given time, different peers have different subsets of file chunks
- periodically, Alice asks each peer for list of chunks that they have
- Alice requests missing chunks from peers, rarest first

**sending chunks: tit-for-tat**
- Alice sends chunks to those four peers currently sending her chunks *at highest rate*
  - other peers are choked by Alice (do not receive chunks from her)
  - re-evaluate top 4 every 10 secs
- every 30 secs: randomly select another peer, starts sending chunks
  - “optimistically unchoke” this peer
  - newly chosen peer may join top 4
BitTorrent: tit-for-tat

(1) Alice “optimistically unchokes” Bob
(2) Alice becomes one of Bob’s top-four providers; Bob reciprocates
(3) Bob becomes one of Alice’s top-four providers

higher upload rate: find better trading partners, get file faster!
Lecture by Ion Stoica

https://www.youtube.com/watch?v=AVtRwriSqiE&t=2819s

2:30- 8:57

Ion Stoica is a Romanian-American computer scientist specializing in distributed systems, cloud computing and computer networking. He is currently a professor of computer science at the University of California Berkeley, co-director of AMPLab. Wikipedia
Chapter 2: outline

2.1 principles of network applications
   - app architectures
   - app requirements

2.2 Web and HTTP

2.3 FTP

2.4 electronic mail
   - SMTP, POP3, IMAP

2.5 DNS

2.6 P2P applications

2.7 socket programming with UDP and TCP
goal: learn how to build client/server applications that communicate using sockets

socket: door between application process and end-end-transport protocol
Socket programming

Two socket types for two transport services:

- **UDP**: unreliable datagram
- **TCP**: reliable, byte stream-oriented
Socket programming with UDP

UDP: no “connection” between client & server

- no handshaking before sending data
- sender explicitly attaches IP destination address and port # to each packet
- rcvr extracts sender IP address and port# from received packet

UDP: transmitted data may be lost or received out-of-order

Application viewpoint:
- UDP provides unreliable transfer of groups of bytes (“datagrams”) between client and server
Client/server socket interaction: UDP

server (running on serverIP)

create socket, port = x:
serverSocket = socket(AF_INET,SOCK_DGRAM)

read datagram from serverSocket

write reply to serverSocket specifying client address, port number

client

create socket:
clientSocket = socket(AF_INET,SOCK_DGRAM)

Create datagram with server IP and port=x; send datagram via clientSocket

read datagram from clientSocket specifying client address, port number

close clientSocket
Example app: UDP client

Python UDPClient

from socket import *
serverName = 'hostname'
serverPort = 12000
clientSocket = socket(socket.AF_INET,
    socket.SOCK_DGRAM)
message = raw_input('Input lowercase sentence: ')
clientSocket.sendto(message,(serverName, serverPort))
modifiedMessage, serverAddress = 
    clientSocket.recvfrom(2048)
print modifiedMessage
clientSocket.close()
Example app: UDP server

**Python UDPServer**

```python
from socket import *
serverPort = 12000
serverSocket = socket(AF_INET, SOCK_DGRAM)
serverSocket.bind(('', serverPort))
print "The server is ready to receive"
while 1:
    message, clientAddress = serverSocket.recvfrom(2048)
    modifiedMessage = message.upper()
    serverSocket.sendto(modifiedMessage, clientAddress)
```

create UDP socket
bind socket to local port number 12000
loop forever
Read from UDP socket into message, getting client’s address (client IP and port)
send upper case string back to this client
Socket programming with TCP

client must contact server
- server process must first be running
- server must have created socket (door) that welcomes client’s contact

client contacts server by:
- Creating TCP socket, specifying IP address, port number of server process
- when client creates socket: client TCP establishes connection to server TCP

- when contacted by client, server TCP creates new socket for server process to communicate with that particular client
  - allows server to talk with multiple clients
  - source port numbers used to distinguish clients (more in Chap 3)
Server (running on hostid)

- Create socket, port=x, for incoming request:
  \[\text{serverSocket = socket()}\]

- Wait for incoming connection request:
  \[\text{connectionSocket = serverSocket.accept()}\]

- Read request from connectionSocket

- Write reply to connectionSocket

- Close connectionSocket

Client

- Create socket, connect to hostid, port=x
  \[\text{clientSocket = socket()}\]

- Send request using clientSocket

- Read reply from clientSocket

- Close clientSocket
Python TCPClient

from socket import *
serverName = 'servername'
serverPort = 12000
clientSocket = socket(AF_INET, SOCK_STREAM)
clientSocket.connect((serverName,serverPort))
sentence = raw_input('Input lowercase sentence:')
clientSocket.send(sentence)
modifiedSentence = clientSocket.recv(1024)
print 'From Server:', modifiedSentence
clientSocket.close()
**Example app: TCP server**

**Python TCPServer**

```python
from socket import *
serverPort = 12000
serverSocket = socket(AF_INET, SOCK_STREAM)
serverSocket.bind(('', serverPort))
serverSocket.listen(1)
print 'The server is ready to receive'
while 1:
    connectionSocket, addr = serverSocket.accept()
    sentence = connectionSocket.recv(1024)
capitalizedSentence = sentence.upper()
    connectionSocket.send(capitalizedSentence)
    connectionSocket.close()
```

create TCP welcoming socket

server begins listening for incoming TCP requests

loop forever

server waits on accept() for incoming requests, new socket created on return

read bytes from socket (but not address as in UDP)

close connection to this client (but *not* welcoming socket)
Chapter 2: summary

our study of network apps now complete!

- application architectures
  - client-server
  - P2P
- application service requirements:
  - reliability, bandwidth, delay
- Internet transport service model
  - connection-oriented, reliable: TCP
  - unreliable, datagrams: UDP
- specific protocols:
  - HTTP
  - FTP
  - SMTP, POP, IMAP
  - DNS
  - P2P: BitTorrent, DHT
- socket programming: TCP, UDP sockets
Next class

- Lab assignment due by this Sunday!

- Please read Chapter 3.1-3.3 of your textbook BEFORE Class