CMPE 150/L : Introduction to Computer Networks

Chen Qian
Computer Engineering
UCSC Baskin Engineering
Lecture 6
Midterm room for overflow students

- The students who used my registration code to enroll will be seated in another room for exams. An Email will be sent to them.

- **Midterm:**
  - Thu Feb 15 2018
    - 1:30PM - 3:05PM
  - Space Assignment(s):
    - Crown 201
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**

![Diagram of DNS structure]

### 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

13 root name servers worldwide

- a. Verisign, Los Angeles CA (5 other sites)
- b. USC-ISI Marina del Rey, CA
- c. Cogent, Herndon, VA (5 other sites)
- d. U Maryland College Park, MD
- e. NASA Mt View, CA
- f. Internet Software C. Palo Alto, CA (and 48 other sites)
- g. US DoD Columbus, OH (5 other sites)
- h. ARL Aberdeen, MD
- i. Netnod, Stockholm (37 other sites)
- j. Verisign, Dulles VA (69 other sites)
- k. RIPE London (17 other sites)
- l. ICANN Los Angeles, CA (41 other sites)
- m. WIDE Tokyo (5 other sites)
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

$u_s$: server upload capacity

$u_i$: peer $i$ upload capacity

$d_i$: peer $i$ download capacity

$u_N$: peer upload capacity

$d_N$: peer download capacity

Network (with abundant bandwidth)
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
  - $d_{\text{min}} = \min$ client download rate
  - min client download time: $F/d_{\text{min}}$

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

(time to distribute $F$ to $N$ clients using client-server approach)

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 $u_s + \sum u_i$

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

- time to distribute $F$ to $N$ clients using P2P approach 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
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
Socket programming

**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

close
clientSocket
Example app: UDP client

Python UDPClient

- include Python’s socket library
- create UDP socket for server
- get user keyboard input
- Attach server name, port to message; send into socket
- read reply characters from socket into string
- print out received string and close socket

```python
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 *
s
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)
Client/server socket interaction: TCP

**server (running on hostid)**

- create socket, port=x, for incoming request:
  - serverSocket = socket()
- wait for incoming connection request
  - connectionSocket = serverSocket.accept()
  - read request from connectionSocket
  - write reply to connectionSocket
  - close connectionSocket

**client**

- create socket, connect to hostid, port=x
  - clientSocket = socket()
- send request using clientSocket
- read reply from clientSocket
- close clientSocket
Example app: TCP client

Python TCPClient

define TCP socket for server, remote port 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
  - 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