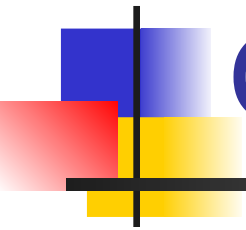
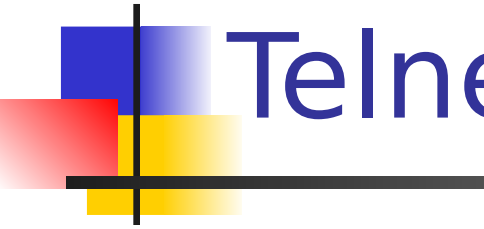
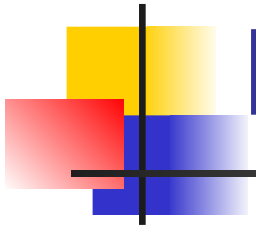


CS684 – Network Protocols

Session 8

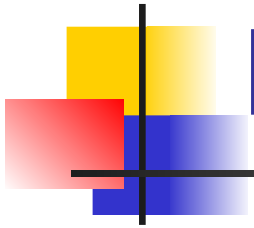


Telnet Protocol



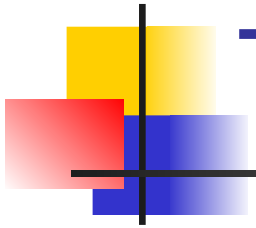
Network Virtual Terminal

- Defined in RFC 854 – May ‘83
- Protocol designers envisioned the possibility of working on a terminal without actually being at that terminal
- Entirely text based
- Left open for **some** expandability



NVT (cont.)

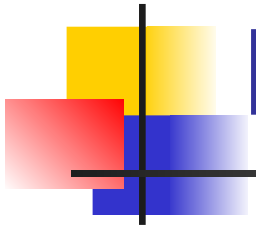
- Can operate in multiple modes
  - Half-duplex
  - Character at a time
  - Line at a time
  - Linemode
- Can be used for printing to an NVT Printer



Telnet program

- Primarily used for connecting to a network virtual terminal server
- Can also be used for network diagnostics
- Does not require that we connect to an NVT server!

File Transfer Protocl

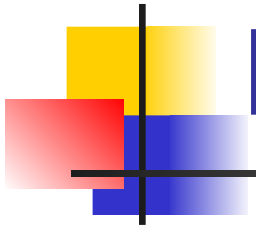


FTP

- Defined in RFC 959, Oct. 1985
- Still in use today for moving files across a network
- Uses a control connection and one or more data connections

FTP Procedure

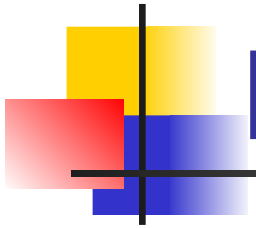
- When client connects to port 21 on server they are presented with a welcome message in the form “220 ID”
- Client issues the command “USER <username>”
- Server acknowledges “331 password required”
- Client responds with “pass <PASSWORD>”
- If username/password pair is correct, server responds with “230 Welcome”



FTP Procedure (cont)

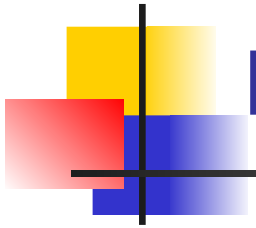
- After authentication, user can issue a multitude of commands including:
  - LIST
  - CD
  - TYPE
  - RETR
  - STOR
  - SYST
  - PORT
  - PASV

FTP data transfer procedure (normal mode)

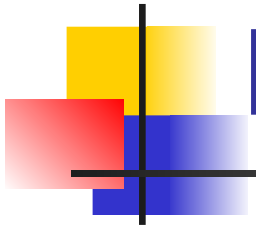


1. Client issues command “TYPE #” where # is I for binary and A is for ASCII. Server responds with 200 code
2. Client issues command “PORT I1,I2,I3,I4,P1,P2” and creates and listens for connections on that port
3. Client issues command “RETR <filename>”
4. Server establishes connection to client on data port, and sends data to client
5. When port is closed, transfer is complete.

FTP Passive Data transfer mode (PASV)



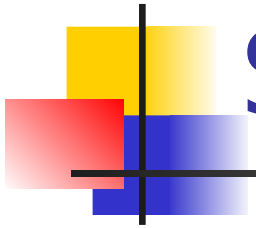
1. Client issues a “TYPE #” command
2. Client issues a “PASV” command; server responds with IP and PORT it will listen on
3. Client connects to port (this is the data connection)
4. On Control connection client issues “RETR <filename>” command
5. Server sends requested file on data connection



FTP Notes

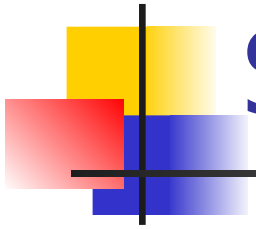
- LIST requires that a data connection be established
- Passive mode is common today because it is much simpler and more reliable due to firewalls
- Anonymous user accounts exist on most servers for minimal access to public files

Simple Mail Transport Protocol



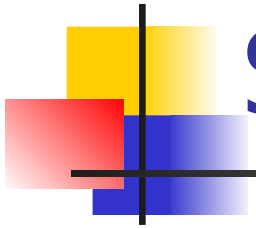
SMTP

- Defined in RFC 821; Aug 1982
- The primary method of transferring email on the Internet today. In 1991, about 50% of the TCP connections established were SMTP connections



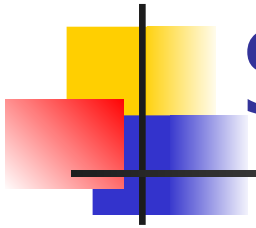
SMTP steps

- User creates a message in a MUA (Mail User Agent) and delivers it to the MTA (Message Transfer Agent)
- The local MTA determines which host should receive this message and opens a TCP (port 25) connection to the remote MTA



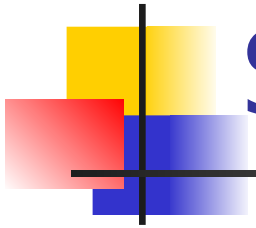
SMTP Steps (cont)

1. Remote MTA introduces itself (i.e. “220 Hello this is …”)
2. Local MTA introduces itself by announcing “HELO <servername>”; remote replies with 250 code
3. Local MTA issues “MAIL FROM: <<email address>>”; remote MTA replies with 250 code
4. Local MTA issues one or more “RCPT TO:<<email address>>” commands; server replies with 250 code for each or error if it will not relay or if user does not exist
5. Local MTA issues “DATA” command; server replies with 250 code
6. Local MTA sends message, headers and body are separated by “<crlf><crlf>”. When finished local MTA sends “<crlf>.<crlf>” (period on a line by itself); remote replies with 250 code or error



SMTP Steps (cont)

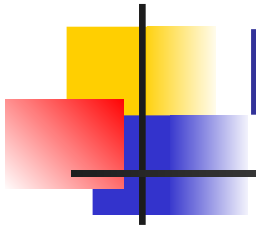
- Message is passed from MTA to MTA until it reaches the MTA of the end user. This MTA delivers through whatever method has been programmed.
- How message is received by end user is not the concern of SMTP!



SMTP Notes

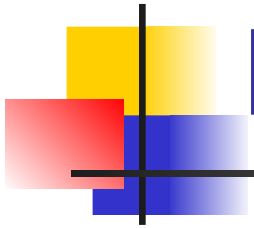
- VRFY is used to verify if an address is valid
- EXPN command should be disabled; but is defined to expand the membership of a mailing list
- Relaying should not be allowed from a client offsite to an MTA offsite!

Post Office Protocol v3



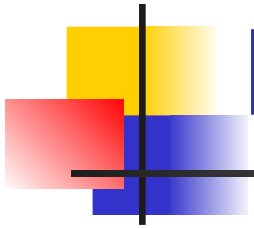
POP3

- Defined in RFC 1725; Nov. ’94
- POP3 is the most common method of recovering mail from a remote server
- Three modes exist: Authorization, Transaction, and update.
- Positive status result is indicated by “+OK”; negative result by “-ERR”



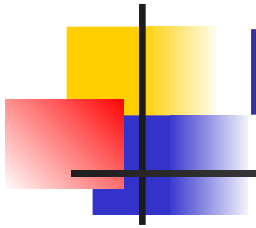
POP3 Steps

1. Client connects to server on TCP port 110; Server responds “+OK”
2. Client issues command “USER <username>”; server responds “+OK”
3. Client issues command “PASS <password>”; server responds “+OK” or “-ERR”; if “+OK” was issued connection is now in the Transaction state



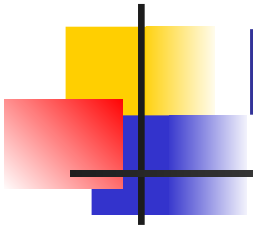
POP3 Steps (cont.)

4. Client can now issue any of the following in any order:
   - STAT
   - LIST [#]
   - RETR #
   - DELE #
   - RSET
   - UIDL [#]
   - QUIT



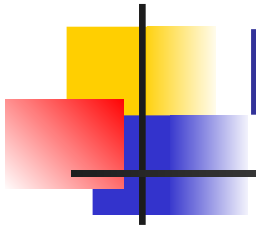
POP3 Notes

- The message store is locked when entering the transition state and opened in the update state.
- A very simple protocol but useful for it’s purpose.



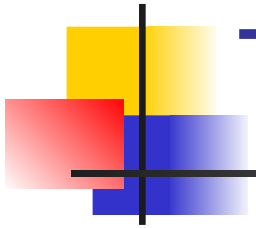
Domain Name System

- Defined in RFCs 2694, 2673, 2672, 2671, 2606, and others
- Used to convert a name to an IP address



DNS Basics

- The Domain Name System (DNS) runs on multiple Domain Name Servers (DNS) which server the domain names
- Designed to resolve names into addresses
- Designed to be a distributed hierarchical database.
- Different Types of records for different purposes



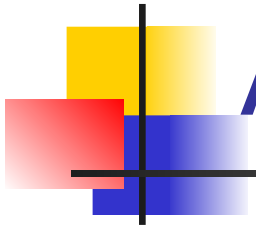
Types of Records

- A – a host address
- NS – Authoritative name Server address
- SOA – Start Of Authority
- MX – Mail Exchanger
- HINFO – Hardware info
- CNAME – Canonical name for an alias

Operation of DNS

0. User types in www.microsoft.com into Web Browser

- Client requests the address of www.microsoft.com (A) from local DNS
- Local DNS checks it's cache, if address is known it is immediately returned to client otherwise Local DNS requests microsoft.com (NS) from root-server
- Root-server responds to Local DNS with appropriate address for microsoft.com DNS
- Local DNS contacts Microsoft.com DNS to resolve www.microsoft.com (A)
- Microsoft.com DNS responds to Local DNS with address of www.microsoft.com (A)
- Local DNS Responds to client with address of www.microsoft.com (A)
- Client Initiates TCP session to IP address associated with www.microsoft.com (A)



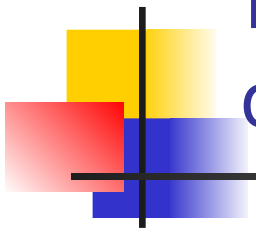
Authority

- When you “Own” a domain name, you are responsible for maintaining at least one authoritative name server
- This server NEVER checks a cache and is the authority for queries to your domain
- If this server goes down, so does your domain

Authoritative domain file

```
@       IN      SOA     dan.spacelab.net. dkatz.dan.spacelab.net. (
                        2001010801      ; serial number
                        86400           ; refresh:      24 hours
                        3600            ; retry:        1 hour
                        432000          ; expire:       5 days
                        86400   )       ; minimum:      1 week
                        IN      A       64.2.85.40
                        IN      NS      unix
                        IN      MX      0 unix
Localhost               IN      A       127.0.0.1
Unix                    IN      A       64.2.85.40
                        IN      HINFO   P100/48MB/4.0GB LINUX
www                     IN      CNAME   unix
ftp                     IN      CNAME   unix
login                   IN      CNAME   unix
irc                     IN      CNAME   unix
nt                      IN      A       209.14.148.179
                        IN      HINFO   K62-400/128MB/4.0GB     WIN95
me                      IN      CNAME   nt
www2                    IN      A       209.14.148.180
                        IN      HINFO   2xP90/100MB/4.0GB       WINNT
```

Diagnostic Tools (use with discretion)



- Dig
- Nslookup
- Whois (available at www.networksolutions.com)