Communication Protocols
and Internet Architectures

Harvard University

Lecture #9

Instructor: Len Evenchik
cs40@evenchik.com or evenchik@fas.harvard.edu

ALIGHLSOD1701

Lecture Agenda

- Course Logistics
- Q&A and Topics from Last Week
- Suggestions for Studying for the Exam
- Domain Name System (DNS)
- Application Layer Protocols
- Email Protocols (SMTP) and Architecture (part 1)
- One Minute Wrap-Up

Course Logistics

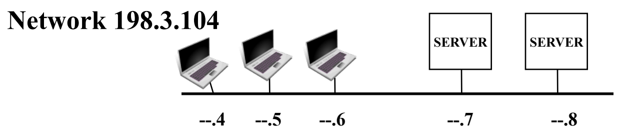
Course Logistics

- The solutions to homework #3 have been posted. Please make sure to review them before the midterm.
- MIDTERM EXAM – Please make sure to read all of the logistics and administrative information about the midterm that is in the weekly course information sheet. Please contact a TA or the instructor if you have any questions.
- The section meetings held right before the midterm will include a review for the exam.
- **Please submit a one minute wrap-up each week. Thank You!**

Q&A
Topics from Last Week

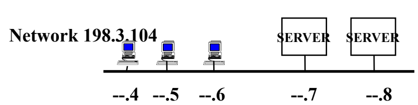
Connection Management

Application Layer Connection Management



- How does a system keep track of all of its application layer connections?
- Can we see the details of these connections?

Connection Management Table



Connection ID #	Protocol (TCP/UDP)	Local IP	Remote IP	Local Port	Remote Port

netstat -an

tcp	140.247.30.107.80	24.60.123.123.1518	ESTABLISHED
tcp	140.247.30.107.23	24.60.234.234.2055	ESTABLISHED
tcp	140.247.30.107.25	24.60.222.221.2006	ESTABLISHED
tcp	140.247.30.107.110	134.174.111.222.1186	FIN_WAIT_2
tcp	140.247.30.107.143	134.174.123.213.1682	ESTABLISHED
tcp	140.247.30.107.80	134.174.212.121.1683	ESTABLISHED
tcp	140.247.30.107.22	24.60.33.22.1516	TIME_WAIT
tcp	*.80	*.*	LISTEN
tcp	*.443	*.*	LISTEN
tcp	*.22	*.*	LISTEN
tcp…..			

Network Address Translation (NAT)

Network Address Translation (NAT)

- NAT functionality maps between private addresses and public addresses using various mechanisms. Remember that private means a non-routable address within the Internet.
- NAT breaks the Internet's end-to-end model.
- NAT functionality can be standalone or implemented in routers, proxies, application layer gateways (ALG), firewalls, SBC, etc.
- Operational details vary by the type of protocol (ICMP, UDP, TCP) as well as type of application layer protocol (email, HTTP, FTP, peer-to-peer, SIP, H.323, mapping, voice and video)
- How do you create and manage the table in the NAT that keeps track of connections? This is what we need to understand.

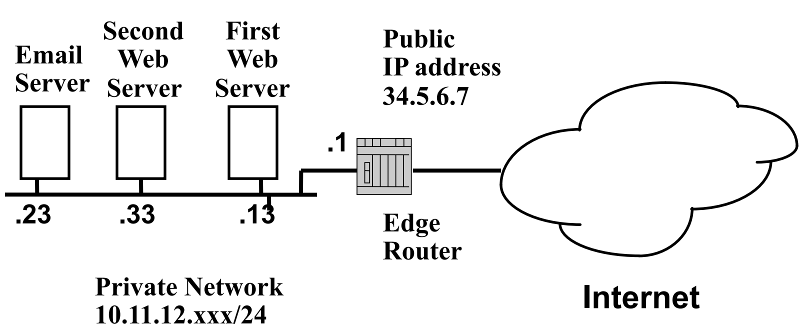
Network Address Translation (NAT)

- 1-to-1 address mapping
- Many-to-many address mapping
- Network Address and Port mapping, called NAPT or PAT

Simplified NAPT/PAT Table in Firewall

Protocol	Private Source IP Address	Private Source Port	Mapped Source IP Address	Mapped Source Port	Foreign IP Address	Foreign Port #

Handling Incoming Connections with NAT (Multiple Web Servers in DMZ)



NAT - Outstanding Issues (1 of 2)

- NAT breaks the Internet' s end-to-end connection model. How and why this happened and its importance is still discussed and debated. The same questions are now being asked about IPv6.
- As we will learn later in the term there is a significant problem with embedded addresses at the application layer as used in SIP and VoIP. Note though that this is not a new problem since it was an issue with FTP, which is over 40 years old.)
- There are issues with IPSec and other end-to-end security mechanisms.
- There is a problem of managing incoming connections of any type as well as long term UDP connections. Lets think about this.

NAT - Outstanding Issues (2 of 2)

- Network management and debugging is much more difficult with NAT (as you would expect.)
- NAT is NOT a solution to network security! It just provides some address obscurity.
- Regardless, NAT is as common as the home router.
- NAT is also being used as part of the transition to IPv6.

Some Questions related to NAT

- What behavior do your users see if the edge router crashes? How does it depend on the protocol, HTTP versus SSH for example?
- What happens if UDP or TCP is not used, such as with ICMP?
- What about protocols such as VoIP (SIP) that open multiple connections, or require an inbound connection?
- How should we support inbound connections to systems such as a web server? What happens if you want to support more than one web server?
- What happens when there are two levels of NAT? This is now very common with wireless networks.

STUN, TURN and ICE

Quick Definition of STUN, TURN and ICE

- STUN – protocol used by a client to determine the presence and type of NAT
- TURN – protocol for working with a media relay which is typically located on the public Internet. (We'll cover this later when we talk about SIP and VoIP.)
- ICE – protocol and technique for dealing with and managing NAT traversal in protocols such as SIP (for VoIP) that use the offer/answer model. We'll cover this later when we talk about SIP and VoIP.

Suggestions for Studying for the Exam

Suggestions for Studying for the Exam (1)
(Applies to both the midterm and final.)

- Concentrate on the theories, framework, building blocks, tools, design tradeoffs, etc. that are needed to understand the course material.
- It is important to be able to apply what you have learned to a protocol design, a question on network architecture or a debugging situation.
- Your approach to answering a question is important. Make sure to state any important assumptions that you make that are not obvious.
- If the topic was discussed in lecture or on the homework then it means that we believe it very important and something you should understand.

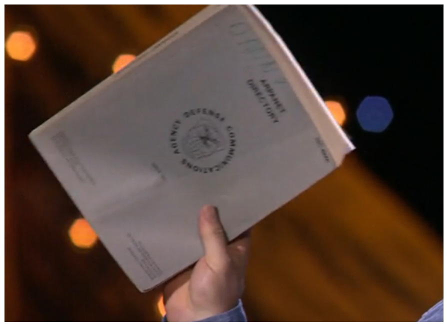
Suggestions for Studying for the Exam (2)
(Applies to both the midterm and final.)

- The assigned readings (textbook, RFCs and articles) provide the needed background for the topics we have discussed, but provide more detail than needed for the exam.
- You should understand ethernet, IP, UDP and TCP very well, including the various header field and what they do. However, except for ethernet, the detailed layout of the header is less important.
- Do I need to know the hex value for …. *probably not.*
- A good way to study is to review each lecture and write down the most important topics that were discussed that week. Do the same for articles. RFCs, and the homework.

Studying for the Exam (3)

- Basic theories, technology and definitions
  - Protocol layering, encapsulation, muxing, packet switching, packet loss, etc.
- Tools
  - Time sequence diagrams, State diagrams, 5-tuple, etc.
- Protocol Framework
  - SP3 framework, protocol functionality such as error detection versus error correction, etc.
- Architectures and topology
  - Bus, pt2pt, ring, star, mesh, etc.
- Building blocks
  - Switches, routers, NAT, etc.
- Protocols
- Design tradeoffs and performance issues

Domain Name System (DNS)



1982 Network Directory

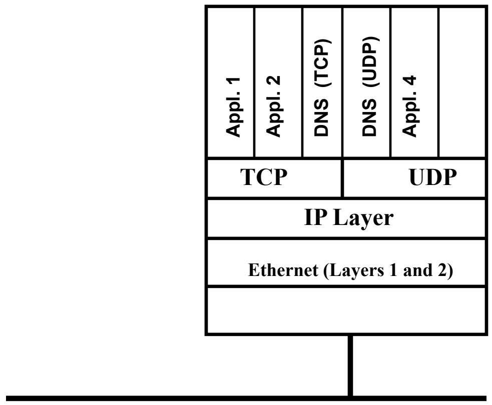
A few pages of this Directory are posted on the course website. This was before DNS so an email address has the form evenchik@bbn-unix

Understanding the Domain Name System

- DNS is an approach to naming things (for example hosts, computers, all types of network devices, IoT devices, or other resources) such that there are no naming conflicts; in other words, all names are unique.
- DNS uses a decentralized database approach to mapping these unique names to IP addresses via the use of distributed but coordinated database servers.
- DNS uses a hierarchical name space to assign and manage this name space.

DNS is an Application Layer Protocol

(but of course the implementation is not as simple as this makes it look)



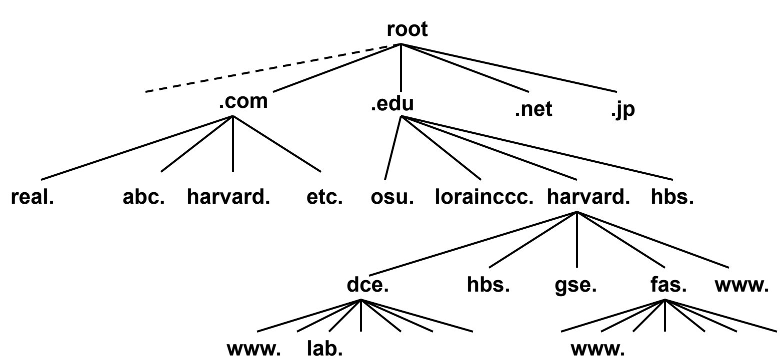
Internet Domain Name System (1)

- DNS is a hierarchical naming system, or name space.
- Authority for assigning and managing individual names are delegated to a particular partition (or zone) within this hierarchical name space.
- Original top-most level of the name space used a broad partition into categories (EDU, COM, GOV, MIL, NET, INT, ORG), plus two letter country code. The first new set of gTLDs were defined in Nov. 2000 and many others have been defined since then. There are over 1,000 gTLD today.
- Names are mapped to 32 bit IPv4 addresses and of course there is now support in DNS for IPv6 where names are to 128 bit IPv6 addresses.

Internet Domain Name System (2)

- Domain Name Servers map between names and addresses. DNS server are arranged in a tree structure and these servers answer requests for name/address mappings within a particular level, or zone, in the name space.
- Security was not a critical factor when DNS was designed so there are many security issues in the original design. DNSSEC is an upgrade with provides data integrity and authentication.
- IP addresses can also be mapped to names (reverse mapping)
  - *.*.*.*.in-addr.arpa
- Telephone numbers can also be mapped to IP addresses
  - *.*.*.*.e164.arpa

Partial DNS Name Space



DNS Forward and Reverse Query

The current Unix command to do this is dig, but this is not always available. The older command is nslookup. Note that the IP addresses below are not current.

```
fas% dig www.mit.edu
; <<>> DiG 9.3.2 <<>> www.mit.edu
;; QUESTION SECTION:
;www.mit.edu.             IN    A

;; ANSWER SECTION:
www.mit.edu.        30    IN    A     18.9.22.169

;; AUTHORITY SECTION:
mit.edu.          21570   IN    NS    BITSY.mit.edu.
mit.edu.          21570   IN    NS    W20NS.mit.edu.
mit.edu.          21570   IN    NS    STRAWB.mit.edu.
```


DNS Forward and Reverse Query

The current Unix command for this is dig, but this is not always available. The older command is nslookup.

```
Windows 7 % nslookup www.mit.edu

> www.mit.edu
Server:       140.247.233.195
Address:      140.247.233.195#53
Non-authoritative answer:
Name:   www.mit.edu
Address: 18.9.22.169
>
> 18.9.22.169
Server:       140.247.233.195
Address:      140.247.233.195#53

169.22.9.18.in-addr.arpa name = WWW.MIT.EDU.
>
```

DNS Resource Records (partial listing)

- A - specifies 32 bit IPv4 address
- AAAA – IPv6 address record
- MX - mail exchange record
- NS - specifies authoritative name server for a domain
- CNAME - canonical name, provides alias functionality
- HINFO - specifies limited host information
- SRV – identifies a specific service
- NAPTR

IPv6 DNS Query

```
fas% dig www.harvard.edu AAAA
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23697
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 9

;; QUESTION SECTION:
;www.harvard.edu.            IN     AAAA

;; ANSWER SECTION:
www.harvard.edu.      10800   IN     AAAA    2607:fb60:100:210::e6

;; AUTHORITY SECTION:
harvard.edu.          2318    IN     NS      internaldns-b6.fas.harvard.edu.
harvard.edu.          2318    IN     NS      internaldns-b1.harvard.edu.
… etc….
```

DNS Simplified Zone File (abridged)

DNS Related Files

networklandscape.com.forward
networklandscape.com.reverse.140.247.30
networklandscape.com.reverse.140.247.31

Printout of networklandscape.com.forward

```
@       IN      SOA   ns.networklandscape.com. root.ns.networklandscape.com. (
                      97021601        ; serial
                      7200    ; refresh 2 hours
                      3600    ; retry 1 hour
                      3600000 ; expire 1 week
                      604800 )        ; min 1 week

                      IN      NS      unix1.networklandscape.com.
networklandscape.com          IN      MX 0   mail.networklandscape.com.

unix1                 IN      A       140.247.30.37
unix1                 IN      HINFO           ops             unix
marketing             IN      A       140.247.31.34
marketing             IN      HINFO           marketing       nt
www                   IN      CNAME           marketing.networklandscape.com.
web                   IN      CNAME           marketing.networklandscape.com.
mail                  IN      CNAME           unix1.networklandscape.com.
```


Address Resolution – use of CNAME

```
dig www.yahoo.com
;; ANSWER SECTION:
www.yahoo.com.          239     IN      CNAME   fp.wg1.b.yahoo.com.
fp.wg1.b.yahoo.com.     2040    IN      CNAME   any-fp.wa1.b.yahoo.com.
any-fp.wa1.b.yahoo.com. 60      IN      A       67.195.160.76
any-fp.wa1.b.yahoo.com. 60      IN      A       69.147.125.65
any-fp.wa1.b.yahoo.com. 60      IN      A       209.191.122.70
```

Address Resolution – with very, very simple load sharing

```
dig www.yahoo.com
;; ANSWER SECTION:
www.yahoo.com.          239   IN    CNAME   fp.wg1.b.yahoo.com.
fp.wg1.b.yahoo.com.     2040  IN    CNAME   any-fp.wa1.b.yahoo.com.
any-fp.wa1.b.yahoo.com. 60    IN    A       67.195.160.76
any-fp.wa1.b.yahoo.com. 60    IN    A       69.147.125.65
any-fp.wa1.b.yahoo.com. 60    IN    A       209.191.122.70

dig www.yahoo.com
;; ANSWER SECTION:
www.yahoo.com.          151   IN    CNAME   fp.wg1.b.yahoo.com.
fp.wg1.b.yahoo.com.     1952  IN    CNAME   any-fp.wa1.b.yahoo.com.
any-fp.wa1.b.yahoo.com. 57    IN    A       209.191.122.70
any-fp.wa1.b.yahoo.com. 57    IN    A       67.195.160.76
any-fp.wa1.b.yahoo.com. 57    IN    A       69.147.125.65
```


DNS Address Resolution - simple load sharing *First Request*

```
fas% dig www.cbs.com
;; QUESTION SECTION:
;www.cbs.com.                 IN    A

;; ANSWER SECTION:
www.cbs.com.            5     IN    CNAME   www.cbs.com.edgesuite.net.
www.cbs.com.edgesuite.net. 27114 IN CNAME   a916.g.akamai.net.
a916.g.akamai.net.      9     IN    A       212.23.37.6
a916.g.akamai.net.      9     IN    A       212.23.37.30
```

DNS Address Resolution - load sharing

Second Request – just a few seconds later

```
fas% dig www.cbs.com
;; QUESTION SECTION:
;www.cbs.com.                IN    A

;; ANSWER SECTION:
www.cbs.com.          212    IN     CNAME   www.cbs.com.edgesuite.net.
www.cbs.com.edgesuite.net. 27016 IN    CNAME   a916.g.akamai.net.
a916.g.akamai.net.     11     IN     A      212.23.37.30
a916.g.akamai.net.     11     IN     A      212.23.37.6
```


Finding a Network Resource such as a Mail Server or VoIP Server via DNS

(This is different than finding an IP address for a name.)

- "A" records provide a mapping between names and addresses. This is what you would expect the DNS to handle. IPv6 uses AAAA.
- But how do you find a resource such a mail server for an organization when you don't know the specific name of the server?
- For example, email to webmaster@harvard.edu must be delivered to the mail server for Harvard, even though you do not know the name (or IP address) of the specific mail server that handles incoming mail.

DNS Resource Records (partial listing)

- A - specifies 32 bit IPv4 address
- AAAA – IPv6 address record
- MX - mail exchange record
- NS - specifies authoritative name server for a domain
- CNAME - canonical name, provides alias functionality
- HINFO - specifies limited host information
- SRV – identifies a specific service
- NAPTR

Harvard DNS MX Query

```
fas% dig harvard.edu mx
;; QUESTION SECTION:
;harvard.edu.            IN    MX

;; ANSWER SECTION:
harvard.edu.         1018   IN    MX    20 mail.br.harvard.edu.
harvard.edu.         1018   IN    MX    0 ackroyd.harvard.edu.
harvard.edu.         1018   IN    MX    10 netopc.harvard.edu.

;; ADDITIONAL SECTION:
mail.br.harvard.edu.   10066  IN    A     128.119.3.169
netopc.harvard.edu.    10800  IN    A     128.103.1.37
netop3.harvard.edu.    10800  IN    A     128.103.208.29

ns1.harvard.edu.       10800  IN    A     128.103.200.101
ns.harvard.edu.        10800  IN    A     128.103.201.100
ns2.harvard.edu.       10800  IN    AAAA  2607:fb60:a:3::d
```

Harvard DNS MX Query for Harvard FAS (1)

```
fas% dig fas.harvard.edu mx
;; QUESTION SECTION:
;fas.harvard.edu.                IN     MX

;; ANSWER SECTION:
fas.harvard.edu.       615    IN     MX     0 smtp.fas.harvard.edu.
fas.harvard.edu.       615    IN     MX     10 mx1.fas.harvard.edu.

;; ADDITIONAL SECTION:
smtp.fas.harvard.edu.   618    IN     A      140.247.35.194
mx1.fas.harvard.edu.    963    IN     A      140.247.35.36
internaldns-b1.harvard.edu. 666 IN    A      128.103.201.105
internaldns-b2.harvard.edu. 666 IN    A      128.103.200.99
```


Harvard DNS MX Query for Harvard GSD (2)

```
fas% dig gsd.harvard.edu mx
;; QUESTION SECTION:
;gsd.harvard.edu.                IN     MX

;; ANSWER SECTION:
gsd.harvard.edu.       229    IN     MX     20 ext2.aliasing.harvard.edu.
gsd.harvard.edu.       229    IN     MX     10 ext1.aliasing.harvard.edu.

;; ADDITIONAL SECTION:
ext2.aliasing.harvard.edu. 1775 IN    A      128.103.1.38
internaldns-b1.harvard.edu. 366 IN    A      128.103.201.105
internaldns-b2.harvard.edu. 366 IN    A      128.103.200.99
```

MX Query for Harvard Divinity School (3)

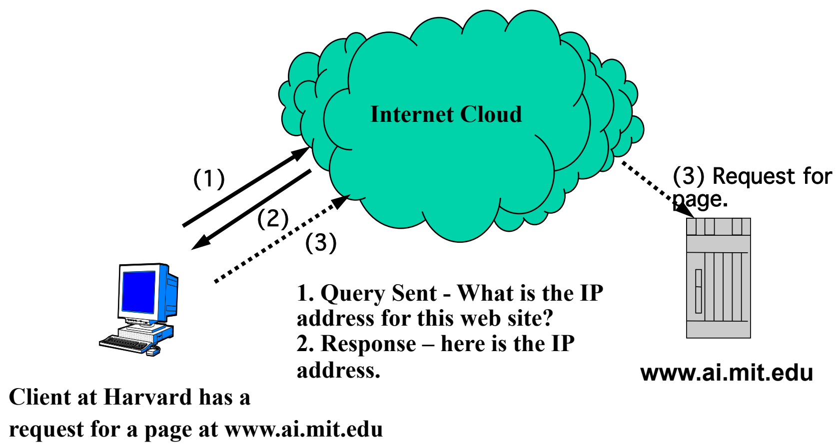
```
fas% dig hds.harvard.edu mx
;; QUESTION SECTION:
;hds.harvard.edu.                IN      MX

;; ANSWER SECTION:
hds.harvard.edu.       300     IN      MX      10 ext2.aliasing.harvard.edu.
hds.harvard.edu.       300     IN      MX      0 ext1.aliasing.harvard.edu.

;; ADDITIONAL SECTION:
ext2.aliasing.harvard.edu. 1685 IN      A       128.103.1.38
internaldns-b1.harvard.edu. 276 IN      A       128.103.201.105
internaldns-b2.harvard.edu. 276 IN      A       128.103.200.99
```


Harvard DNS MX Query (nslookup)

```
> set type=mx
>harvard.edu
Server:  ns3.fas.harvard.edu
Address:  140.247.30.30

harvard.edu     preference = 0, mail exchanger = netop3.harvard.edu
harvard.edu     preference = 10, mail exchanger = netopc.harvard.edu
harvard.edu     nameserver = ns.harvard.edu
harvard.edu     nameserver = ns1.harvard.edu
harvard.edu     nameserver = ns2.harvard.edu
netop3.harvard.edu      internet address = 128.103.205.103
netopc.harvard.edu      internet address = 128.103.201.112
ns.harvard.edu  internet address = 128.103.201.100
ns1.harvard.edu internet address = 128.103.200.101
ns2.harvard.edu internet address = 128.103.1.1
>
```

DNS Address Resolution

DNS Address Resolution: It looks this simple, but isn't.



DNS Architecture (part 1)

- A Zone is a separately administered sub-tree of the DNS. A zone can be subdivided further, i.e., into smaller Zones. This provide finer granularity for name resolution.
- DNS servers within a Zone have a database of name to address mappings for that specific Zone, but not other Zones.
- A Zone is managed by an administrator who is responsible for maintaining the database of name to address mappings.
- In order to use DNS, a client must first know the name and IP address of a DNS server which it can use. This initial information must be configured or assigned via DHCP.
- The client can only ask questions. It does not have its own database, although it can cache some DNS records.

DNS Simplified Zone File (abridged)

DNS Related Files

networklandscape.com.forward
networklandscape.com.reverse.140.247.30
networklandscape.com.reverse.140.247.31

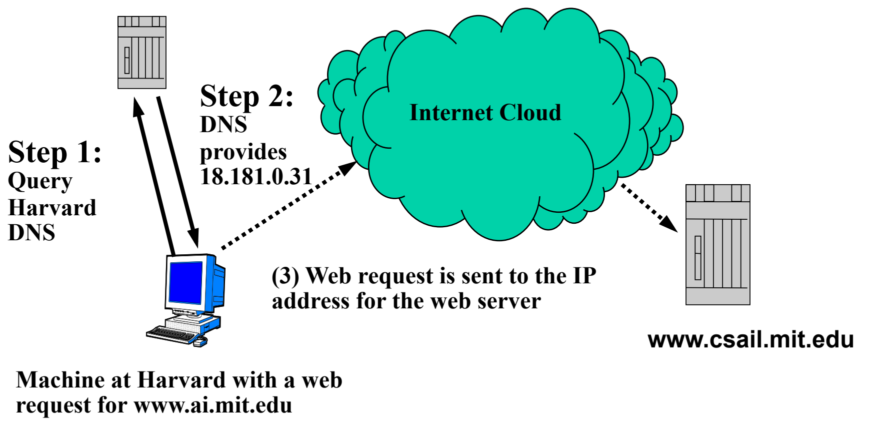
Printout of networklandscape.com.forward

```
@       IN      SOA   ns.networklandscape.com. root.ns.networklandscape.com. (
                      97021601        ; serial
                      7200    ; refresh 2 hours
                      3600    ; retry 1 hour
                      3600000 ; expire 1 week
                      604800 )        ; min 1 week

                      IN      NS      unix1.networklandscape.com.
networklandscape.com          IN      MX 0   mail.networklandscape.com.

unix1                 IN      A       140.247.30.37
unix1                 IN      HINFO           ops             unix
marketing             IN      A       140.247.31.34
marketing             IN      HINFO           marketing       nt
www                   IN      CNAME           marketing.networklandscape.com.
web                   IN      CNAME           marketing.networklandscape.com.
mail                  IN      CNAME           unix1.networklandscape.com.
```


DNS Architecture (part 2)

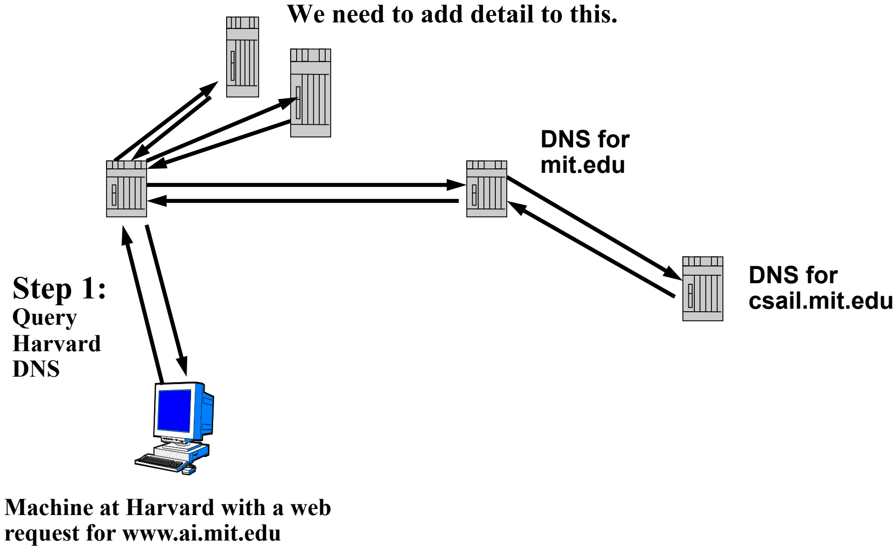
- The client queries the DNS server it is configured to use for the name to address mapping.
- The DNS server is typically called a Resolver. A recursive DNS Resolver is one that takes a query and handles all the necessary steps to provide the answer.
- Each Zone should have multiple DNS servers in order to minimize the problem from a server failure.
- DNS uses both TCP and UDP (but for different things.)
- In order to answer a query for a host outside of its own Zone, a DNS server must ask other DNS servers for that information.
- In simple terms, a DNS server starts at the root server when answering any query.

DNS Address Resolution: What is wrong with this?



DNS Address Resolution

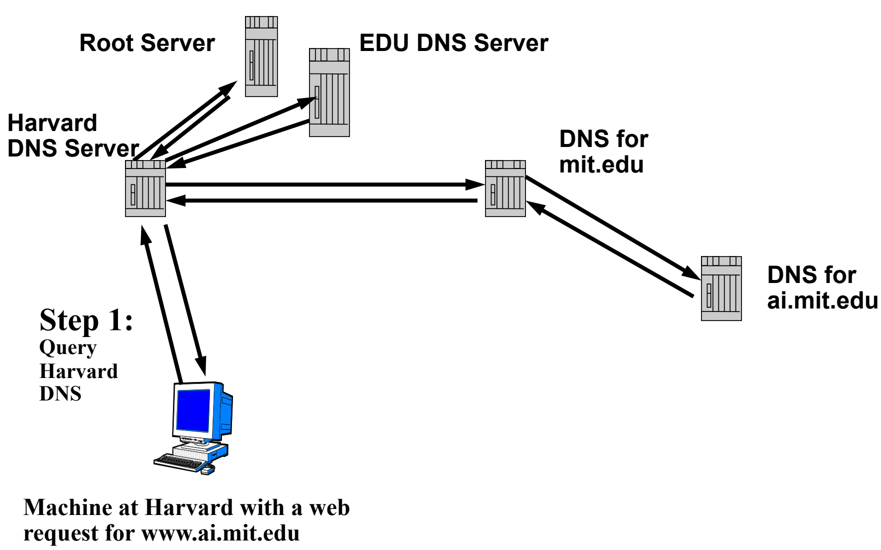
We need to add detail to this.



Domain Name System (DNS) Architecture (part 3)

- Root servers only know about the DNS servers for the TLDs.
- The DNS servers at the top of each gTLD only know about the next level down within their name space. This approach is used from level to level, walking down from the root to the leaf.
- The DNS servers at an organization must know the addresses of one of more root servers in order to start to use DNS.
- There are thirteen named root servers, but there are actually many more than 13 individual machines. (Why 13?)
- Caching is used to reduce network traffic. The TTL field in a DNS message provides the mechanism for ageing out the old, cached information.

DNS Address Resolution

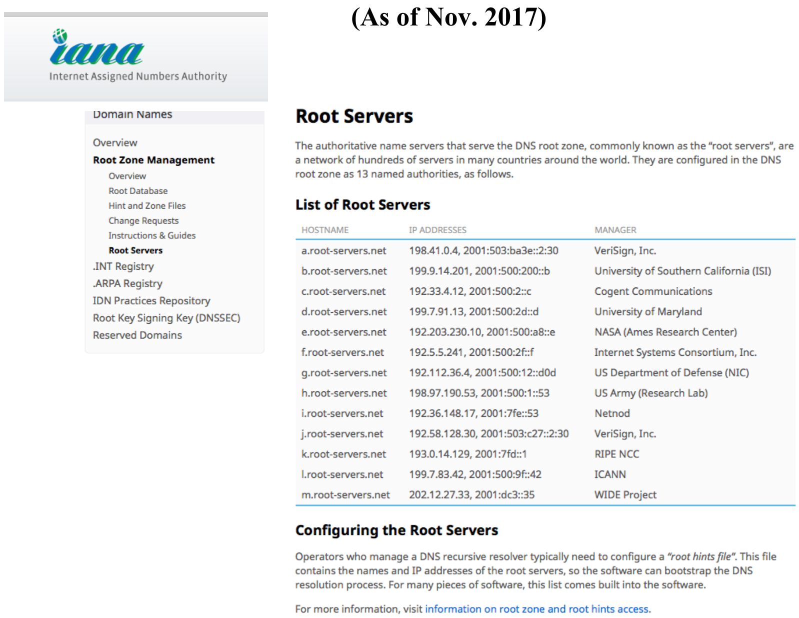


DNS Root Servers

- The root of the DNS hierarchy is anchored on 13 domain name servers scattered across the globe.
- The servers use diverse operating systems and hardware
- Anycast addressing is used for the root servers so that there are a large number of servers used for DNS. (It is not limited to 13 machines.)
- These servers are located in more than 50 countries (www.isoc.org)
- See http://www.root-servers.org/
- These DNS servers publish the root zone file.
- DNS Security (DNSSEC) provides authentication and integrity for responses and it is very important. It will be discussed in a later lecture.

List of Root Servers at IANA.ORG

(As of Nov. 2017)



iana
Internet Assigned Numbers Authority

Domain Names

Overview
Root Zone Management
Overview
Root Database
Hint and Zone Files
Change Requests
Instructions & Guides
Root Servers
.INT Registry
.ARPA Registry
IDN Practices Repository
Root Key Signing Key (DNSSEC)
Reserved Domains

Root Servers

The authoritative name servers that serve the DNS root zone, commonly known as the "root servers", are a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities, as follows.

List of Root Servers

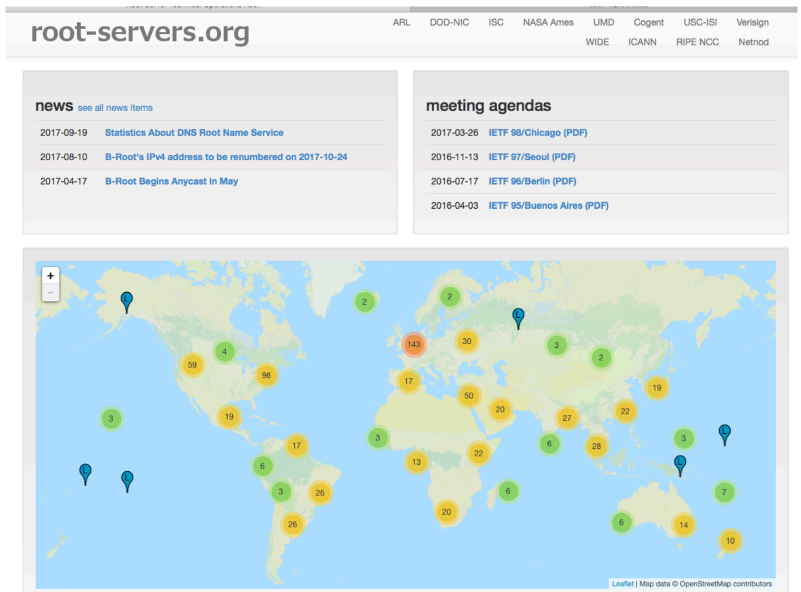
HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Configuring the Root Servers

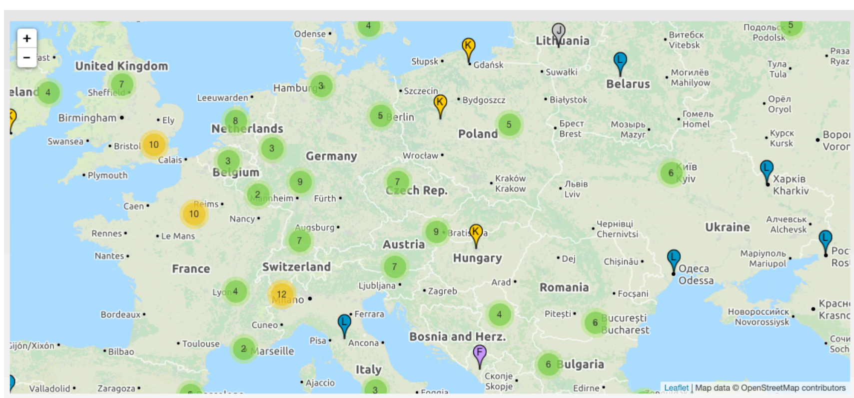
Operators who manage a DNS recursive resolver typically need to configure a *"root hints file"*. This file contains the names and IP addresses of the root servers, so the software can bootstrap the DNS resolution process. For many pieces of software, this list comes built into the software.

For more information, visit information on root zone and root hints access.

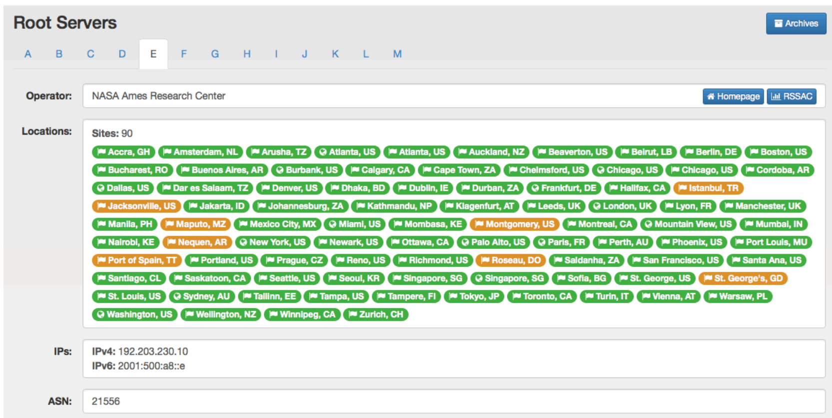
www.root-servers.org
(As of Nov. 2017)



www.root-servers.org
(As of Nov.2017)



www.root-servers.org
E Root Server (Nov.2017)



DNS Root Servers
(abridged display, via DIG on FAS host, *not current*)

a.root-servers.net.	362966	IN	A	198.41.0.4
a.root-servers.net.	362986	IN	AAAA	2001:503:ba3e::2:30
b.root-servers.net.	366987	IN	A	192.228.79.201
b.root-servers.net.	368849	IN	AAAA	2001:500:84::b
c.root-servers.net.	363771	IN	A	192.33.4.12
c.root-servers.net.	398977	IN	AAAA	2001:500:2::c
d.root-servers.net.	364616	IN	A	199.7.91.13
d.root-servers.net.	374986	IN	AAAA	2001:500:2d::d
e.root-servers.net.	363429	IN	A	192.203.230.10
f.root-servers.net.	365342	IN	A	192.5.5.241
f.root-servers.net.	396221	IN	AAAA	2001:500:2f::f
g.root-servers.net.	364102	IN	A	192.112.36.4
h.root-servers.net.	366456	IN	A	128.63.2.53

Root Name Server Information (abridged)

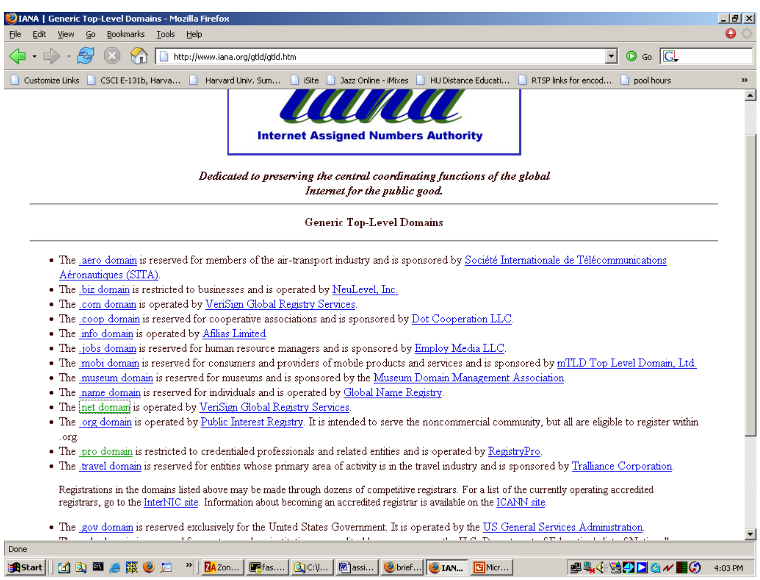
http://www.internic.net/zones/named.root

Configuration file for seeding a DNS.

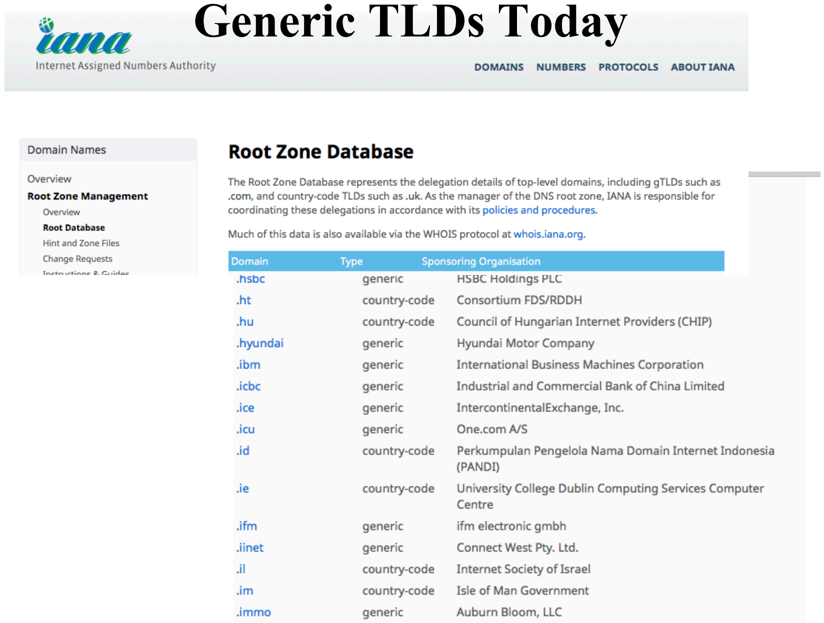
***** Always check for Updates)**

```
;       last update:     October 24, 2017
;       related version of root zone:     2017102400
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS     A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A      198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA   2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS     B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A      199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA   2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS     C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A      192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA   2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000      NS     D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A      199.7.91.13
D.ROOT-SERVERS.NET.      3600000      AAAA   2001:500:2d::d
```

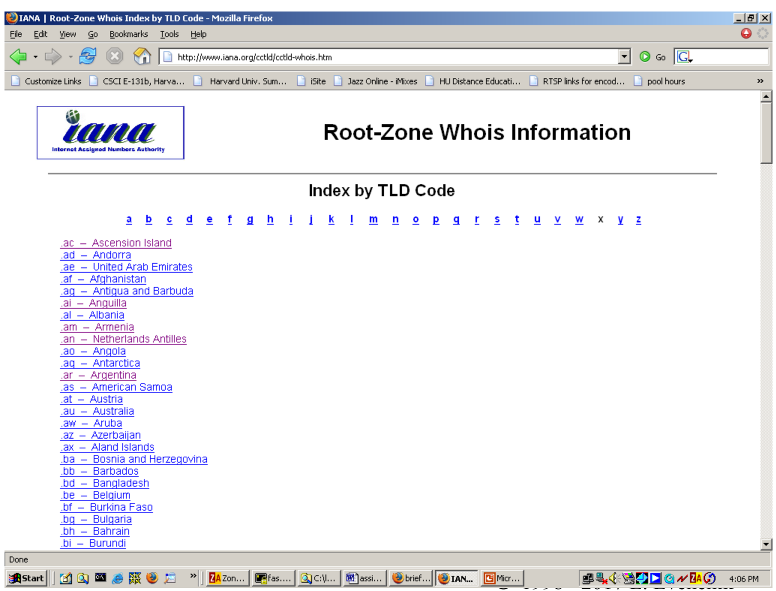

There was a relatively small number of Generic TLDs until a few years ago



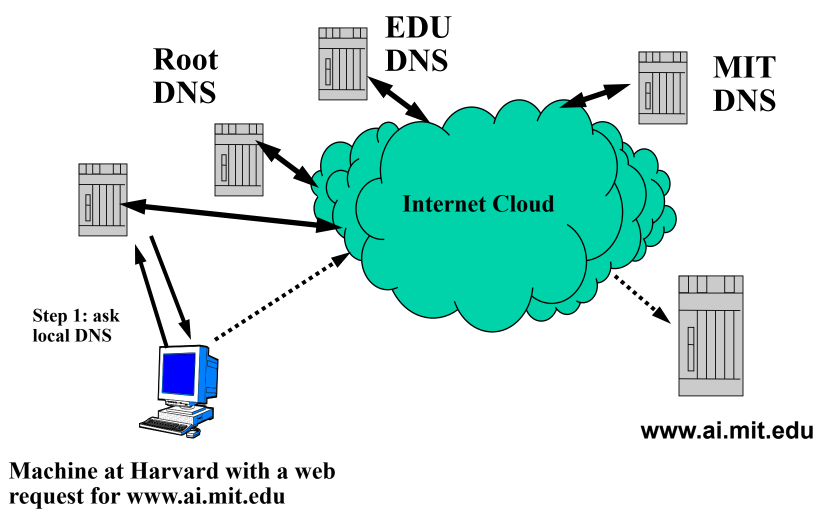
Much Larger Number of Generic TLDs Today



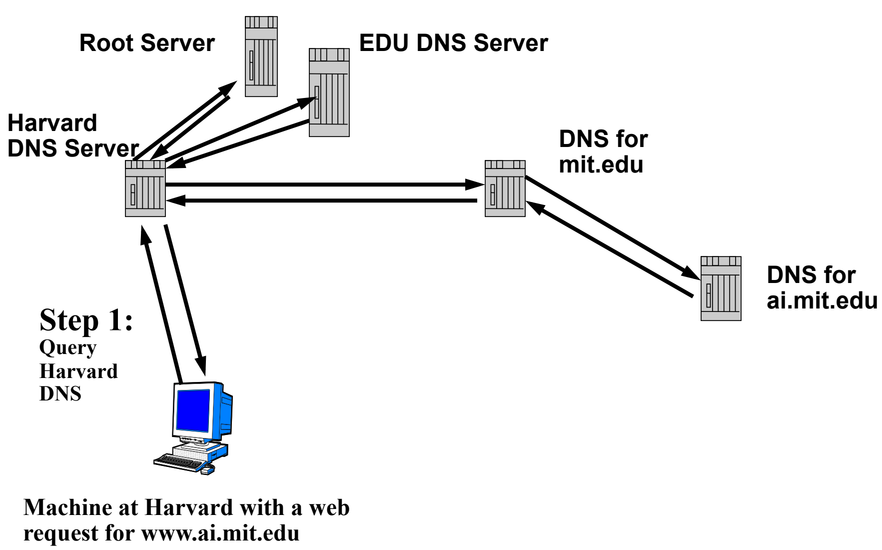
Country Code TLDs



DNS Address Resolution Process



DNS Address Resolution



Root Zone File (abridged listing without DNSSEC)

http://www.internic.net/zones/root.zone

(Always check for updates.)

```
CM.  NS  LOM.CAMNET.CM.
CM.  NS  KIM.CAMNET.CM.
CN.  NS  B.DNS.CN.
CN.  NS  C.DNS.CN.
CO.  NS  SAELL.CC.COLUMBIA.EDU.
CO.  NS  KENSHIN.UNIANDES.EDU.CO.
COM. NS  A.GTLD-SERVERS.NET.
COM. NS  G.GTLD-SERVERS.NET.
MUSEUM. NS  NIC.MUSEUM
NET. NS  A.GTLD-SERVERS.NET.
NET. NS  G.GTLD-SERVERS.NET.
……
SANAGA.CAMNET.CM.   A  195.24.192.17
LOM.CAMNET.CM.      A  195.24.192.34
NIC.MUSEUM.         A  130.242.24.5
B.DNS.CN.           A  203.119.26.1
C.DNS.CN.           A  203.119.27.1
A.GTLD-SERVERS.NET. A  192.5.6.30
A.GTLD-SERVERS.NET. AAAA 2001:503:A83E:0:0:0:2:30
```

```
Country Codes:
.CM   Cameroon
.CN    China
.CO   Colombia
```


dig +norec www.csail.mit.edu +trace

Part 1 of 2

Cs40mac:$ dig +norec www.csail.mit.edu +trace | more

```
; <<>> DiG 9.8.3-P1 <<>> +norec www.csail.mit.edu +trace
;; global options: +cmd
.              497572  IN     NS     a.root-servers.net.
.              497572  IN     NS     b.root-servers.net.
.              497572  skipped some lines
.              497572  IN     NS     d.root-servers.net.
;; Received 508 bytes from 75.75.75.75#53(75.75.75.75) in 41 ms

edu.           172800  IN     NS     a.edu-servers.net.
edu.           172800  skipped some lines
edu.           172800  IN     NS     l.edu-servers.net.
;; Received 270 bytes from 192.203.230.10#53 in 40 ms

mit.edu.       172800  IN     NS     usw2.akam.net.
mit.edu.       172800  skipped some lines
mit.edu.       172800  IN     NS     use5.akam.net.
;; Received 414 bytes from 192.5.6.30#53in 15 ms
```

dig +norec www.csail.mit.edu +trace
Part 1 of 2

SEE previous page for initial steps
cs40mac: dig +norec www.csail.mit.edu +trace | more

```
csail.mit.edu.        1800   IN    NS    auth-ns3.csail.mit.edu.
csail.mit.edu.        1800   skipped some lines
csail.mit.edu.        1800   IN    NS    auth-ns0.csail.mit.edu.
;; Received 191 bytes from 95.100.175.64#53(95.100.175.64) in 87 ms

www.csail.mit.edu.     1800   IN    A     128.30.2.155
;; Received 51 bytes from 18.24.0.120#53(18.24.0.120) in 10 ms
```

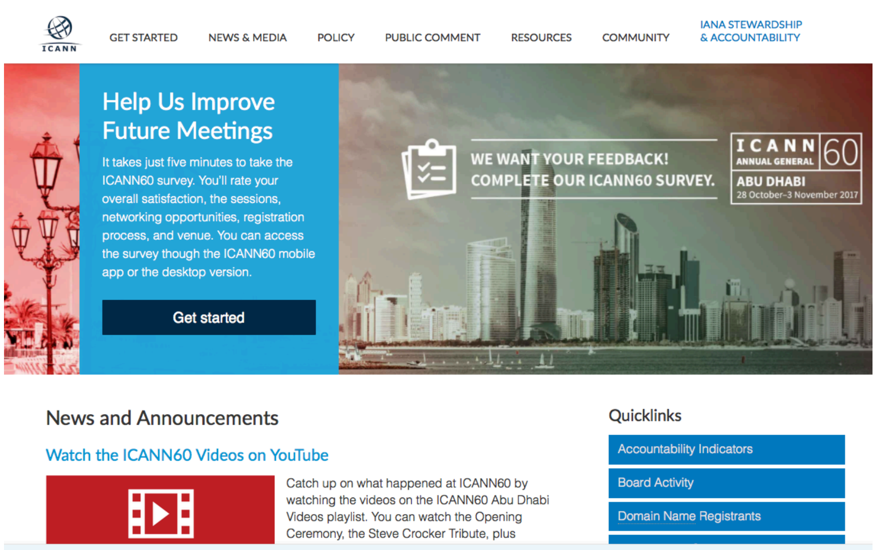

dig +norec www.oxford.edu +trace

```
cs40ac$ dig +norec www.oxford.edu +trace

; <<>> DiG 9.6-ESV-R4-P3 <<>> +norec www.oxford.edu
.                      252830 IN      NS     a.root-servers.net.
.                      252830 IN   skipped some lines
.                      252830 IN      NS     l.root-servers.net.
;; Received 228 bytes from 140.247.233.163#53 in 18 ms

edu.                   172800 IN      NS     a.edu-servers.net.
edu.                   172800 IN   skipped some lines
edu.                   172800 IN      NS     l.edu-servers.net.
;; Received 267 bytes from 128.63.2.53#53(h.root-servers.net)

oxford.edu.            172800 IN      NS     dns0.ox.ac.uk.
oxford.edu.            172800 IN      NS     dns2.ox.ac.uk.
;; Received 78 bytes from 192.5.6.30#53(a.edu-servers.net) in 39 ms

www.oxford.edu.               3600    IN      A       163.1.0.90
oxford.edu.            86400  IN      NS     dns0.ox.ac.uk.
;; Received 126 bytes from 163.1.2.190#53(dns2.ox.ac.uk) in 88 ms
```

IANA.org and ICANN.org

- IANA's online databases keep track of important names and numbers from A to Z. These values are necessary for operation and growth of the Internet. (Of course, in the beginning, this used to be done via printed RFCs.)
- For example, IANA keeps track of protocol numbers (within IP) and port numbers (within TCP and UDP.)
- IANA originally managed and kept track of IP addresses and domain names, but this function was transitioned to ICANN. Other functions and the management of IANA is also being revisited. (See IANA website for details.)
- Always check the ICANN website for current status of new domain names.

ICANN.ORG

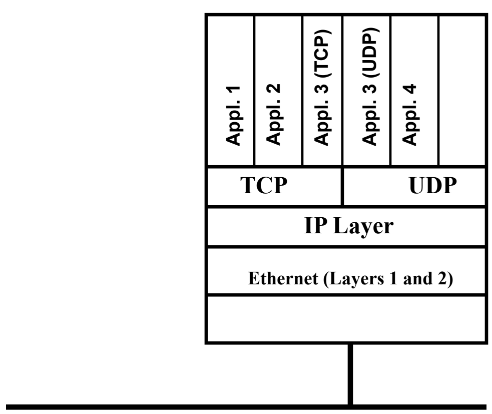


Increasing the Number of TLDs (Top-Level Domains)

- In Nov. 2000 the ICANN board decided on seven additional TLDs. The .biz and .info became operational in the fall of 2001. This was the first significant change in many years.
- In 2005-6 four new additional sponsored TLDs (.cat, .jobs, .mobi, and .travel) were created
- In 2008 ICANN started work on adding generic TLD (gTLD).
- Today there are about 1,500 assigned gTLD. Check ICANN for the current status.

Application Layer Protocols

Application Layer Software Schematic



Email Protocols

SMTP Electronic Mail (1)

- Email and its derivative applications drove the growth of the original ARPAnet and the Internet, and most corporate networks.
- Mail systems provide for the delayed delivery of messages and mail forwarding. Mail is not real time.
- There is a difference between the format of the email message and the protocol that is used to deliver the message.
- Mail is comprised of three parts: the envelope, the headers and the body. **The headers and the body together make up the email message.** All three originally used simple ASCII characters.

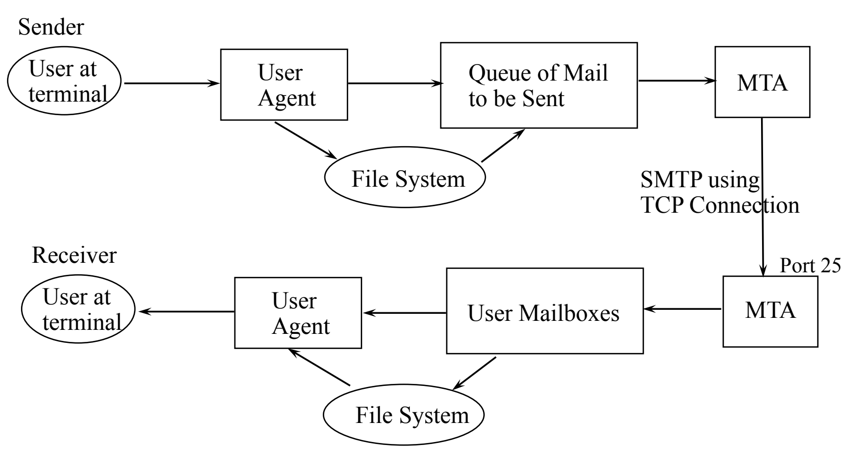
SMTP Electronic Mail (2)

- RFC 5321 (October 2008) describes the Simple Mail Transfer Protocol. This obsoletes RFC 2821 which updated the original RFC 821.
- SMTP uses a TCP connection for email transport.
- RFC 5322 describes the format of mail messages. This obsoletes RFC 2822 which updated the original RFC 822
- SMTP mail servers are found via MX records in DNS.

SMTP Electronic Mail (3)

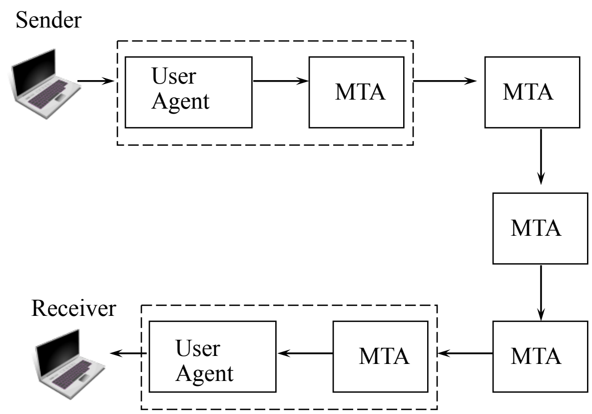
- SMTP is a very simple protocol.
- In the beginning, email was (not surprisingly) text based but MIME extended the functionality to images, audio, video, etc., etc. However, many of the details of current email systems can be better understood if you remember the text based nature of the original protocol.
- In the beginning, email was not typically encrypted (except for military applications.) A lot of work is being done today on secure email but we will not have time to discuss it.
- We will discuss the basic SMTP protocol. Extended SMTP (ESMTP) is now commonly used and it offers more flexibility and additional functionality

Mail System Architecture from the 1980s



Source and date: unknown, but circa 1980s

Simplified Mail System Architecture

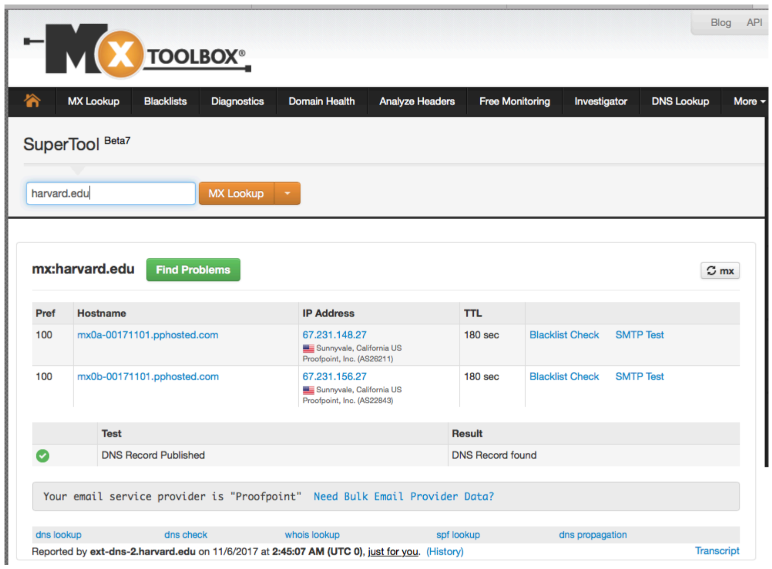


Finding a Network Resource such as a Mail Server or VoIP Server via DNS

(This is different than finding an IP address for a name.)

- "A" records provide a mapping between names and addresses. This is what you would expect the DNS to handle. IPv6 uses AAAA.
- But how do you find a resource such a mail server for an organization when you don't know the specific name of the server?
- For example, email to webmaster@harvard.edu must be delivered to the mail server for Harvard, even though you do not know the name (or IP address) of the specific mail server that handles incoming mail.
- **The answer, as previously discussed, is the MX record.**

MX Lookup at https://mxtoolbox.com
(Of course this can also be done via DIG)



Simplified SMTP Procedure

>>> HELO Alpha.EDU
250 Beta.COM Hello Alpha.EDU, pleased to meet you
>>> MAIL FROM:<Smith@Alpha.EDU>
250 OK
>>> RCPT TO:<Jones@Beta.COM>
250 OK
>>> RCPT TO:<Green@Beta.COM>
550 No such user here
>>> DATA
354 Start mail input; end with <CRLF>**.**<CRLF>
>>> headers go here
>>>
>>> blah, blah, message body goes here
>>> blah, blah, more message
>>> <CRLF>**.**<CRLF>
250 OK
>>> QUIT
221 Beta.COM delivering mail for you

Example: Comer Textbook

Reply Code Meanings

Code	Description
1yz	Positive preliminary reply, another reply to be sent
2yz	Positive completion reply, a new command can be sent
3yz	Positive intermediate reply, the command has been accepted but another command must be sent
4yz	Transient negative completion reply
5yz	Permanent negative completion reply
x0z	Syntax error
x1z	Information
x2z	Replies referring to the control or data connections
x3z	Authentication and accounting
x4z	Unspecified
x5z	Filesystem status

Typical Reply Codes with Possible Message String

125 - Data connection already open, transfer starting

250 – OK

331 - Username OK, password required

452 - Error writing file

500 - Syntax error, unrecognized command

501 - Syntax error, invalid arguments

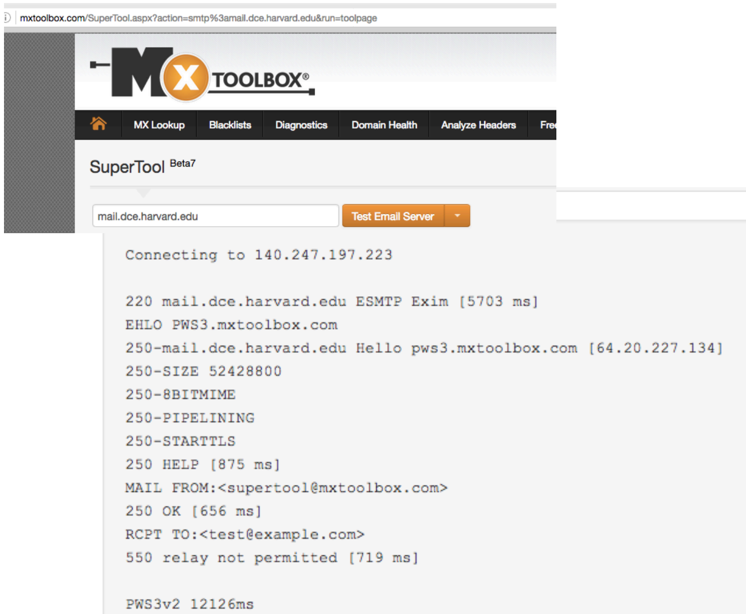
Sending Email (a)
(Simple example using Telnet connection)

```
ls03:~ % telnet mail.dce.harvard.edu 25
Trying 140.247.197.xxx...

Connected to mail.dce.harvard.edu (140.247.197.xxx).
Escape character is '^]'.
220 mail.dce.harvard.edu ESMTP Exim Mon,
        24 Oct 2016 18:25:54 -0500
```


Sending Email (b)
(Simple example using Telnet connection)

```
ls03:~ %
ls03:~ % telnet mail.dce.harvard.edu 25
Trying 140.247.197.235...
Connected to mail.dce.harvard.edu (140.247.197.235).
Escape character is '^]'.
220 mail.dce.harvard.edu ESMTP
        Exim Mon, 24 Oct 2016 18:25:54 -0500

HELO somemachine.edu
250
MAIL FROM:<le@harvard.edu>
250 <le@harvard.edu> is syntactically correct

RCPT TO:<cscie40@mail.dce.harvard.edu>
250 <cscie40@mail.dce.harvard.edu> verified

DATA
```

Email Test Tool at http://mxtoolbox.com/



Sending Email (c)

220 mail.dce.harvard.edu ESMTP Exim Mon, 24 Oct 2016 18:25:54 -0500
MAIL FROM:<le@harvard.edu>
250 <le@harvard.edu> is syntactically correct
RCPT TO:<csci-40@mail.dce.harvard.edu>
250 <csci-40@mail.dce.harvard.edu> verified
DATA
354 Enter message, ending with "." on a line by itself
From: Len at Lectern
To: The TAs in the course
Date: Wed, Dec 1, 1901
Re: Planning for the midterm

Dear TAs,

Should we include anything on the exam on this
new thing called a telephone?

... Len
.
250 OK id=1AOQ7C-0000CR-00

Sending Email (d)
Mail as Delivered (headers off)

Date: Wed, Dec 1, 1901 18:29:29 -0500
From: Len at Lectern
To: The TAs in the course

Dear TAs,

Should we include anything on the midterm on this new thing called a telephone?

.. Len

Sending Email (e)
Mail as Delivered (headers on)

Return-path: <le@harvard.edu>
Envelope-to: csci-40@mail.dce.harvard.edu
Delivery-date: Mon, 24 Oct 2016 18:31:09 -0500
Received: from ls03.fas.harvard.edu [140.247.34.xxx] (evenchik)
by mail.dce.harvard.edu with smtp (Exim)
for csci-40@mail.dce.harvard.edu
id 1AOQ7C-0000CR-00; Mon, 24 Oct 2016 18:29:29 -0500
From: Len at Lectern
To: The TAs in the course
Date: Wed, Dec 1, 1901
Re: Planning for the midterm
Message-Id: <E1AOQ7C-0000CR-00@barkley.dce.harvard.edu>
Date: Mon, 24 Oct 2016 18:29:29 -0500

Dear TAs,
Should we include anything on the midterm on this new thing called a telephone?
.. Len

Email Delivery Problems

What can happen when the destination mail system is not available?

----- The following addresses had transient non-fatal errors -----
<websupt@lab.dce.harvard.edu>

----- Transcript of session follows -----
451 4.4.1 <websupt@lab.dce.harvard.edu>... Deferred: Connection reset
Warning: message still undelivered after 4 hours
Will keep trying until message is 5 days old

Reporting-MTA: dns; smtp3.fas.harvard.edu
Arrival-Date: Thu, 25 Oct 2012 15:35:05 -0400 (EDT)
Action: delayed
Status: 4.4.2
Last-Attempt-Date: Thu, 25 Oct 2012 19:54:26 -0400 (EDT)
Will-Retry-Until: Tue, 30 Oct 2012 15:35:05 -0400 (EDT)
….. a copy of the original message followed….

Email Delivery Problems (Part 1a)

What can happen when the destination mail system is not available?

Return-Path: <MAILER-DAEMON@fas.harvard.edu>
Received: from localhost by smtp3.fas.harvard.edu
Date: Thu, 25 Oct 2012 19:54:27 -0400 (EDT)
From: Mail Delivery Subsystem <MAILER-DAEMON@fas.harvard.edu>
To: <evenchk@fas.harvard.edu>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;

Subject: Warning: could not send message for past 4 hours
Auto-Submitted: auto-generated (warning-timeout)

Email MTA Forwarding

Date: Sat, 1 Dec 2012 17:10:26 -0500 (EST)
From: csci-40@mail.dce.harvard.edu
To: len@alum.mit.edu
Subject: Message to test MTA forwarding

This is a test of forwarding by MTAs.

--

Email MTA Forwarding
(With header option turned on.)

Date: Sat, 1 Dec 2012 17:10:26 -0500 (EST)
From: csci-40@mail.dce.harvard.edu
To: len@alum.mit.edu
Subject: Message to test MTA forwarding
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII

This is a test of forwarding by MTAs.

--

Email MTA Forwarding

Forward 4	FORWARD 4 Received: from ALUM.MIT.EDU [18.7.21.81] by smtp3.fas.harvard.edu with ESMTP id... 1 Dec 2012 17:10:29 Return-Path: <csci-40@mail.dce.harvard.edu>
Forward 3	FORWARD 3 Received: from smtp2.fas.harvard.edu [140.247.34.52]) by alum.mit.edu with ESMTP for <len@alum.mit.edu>; 1 Dec 2012 17:10:28 -0500 (EST) From: csci-40@mail.dce.harvard.edu
Forward 2	FORWARD 2 Received: from mail.dce.harvard.edu {140.247.197.235]) by smtp2.fas.harvard.edu with ESMTP 1 Dec 2012 17:10:28 -0500 (EST)
Forward 1	FORWARD 1 Received: from csci-40 by mail.dce.harvard.edu with local-esmtp for len@alum.mit.edu id 16AIL4-0000PB-00; Sat, 01 Dec 2012 17:10:26 -0500
Email message	Date: Sat, 1 Dec 2012 17:10:26 -0500 (EST) To: len@alum.mit.edu Subject: Message to test MTA forwarding MIME-Version: 1.0 Content-Type: TEXT/PLAIN; charset=US-ASCII This is a test of forwarding by MTAs.

Email MTA Forwarding

FORWARD 4 - not shown (see next page)
FORWARD 3 - not shown (see next page)

FORWARD 2
Received: from mailaa.dce.harvard.edu {140.247.197.235]) by
smtp2.fas.harvard.edu with ESMTP 1 Dec 2012 17:10:28 -0500 (EST)

FORWARD 1
Received: from csci-40 by mailaa.dce.harvard.edu with local-esmtp for
len@alum.mit.edu
id 16AIL4-0000PB-00; Sat, 01 Dec 2012 17:10:26 -0500

actual email message….

Email MTA Forwarding

FORWARD 4
Received: from ALUM.MIT.EDU [18.7.21.81]
by smtp3.fas.harvard.edu with ESMTP id... 1 Dec 2001 17:10:29
Return-Path: <csci-40@mail.dce.harvard.edu>

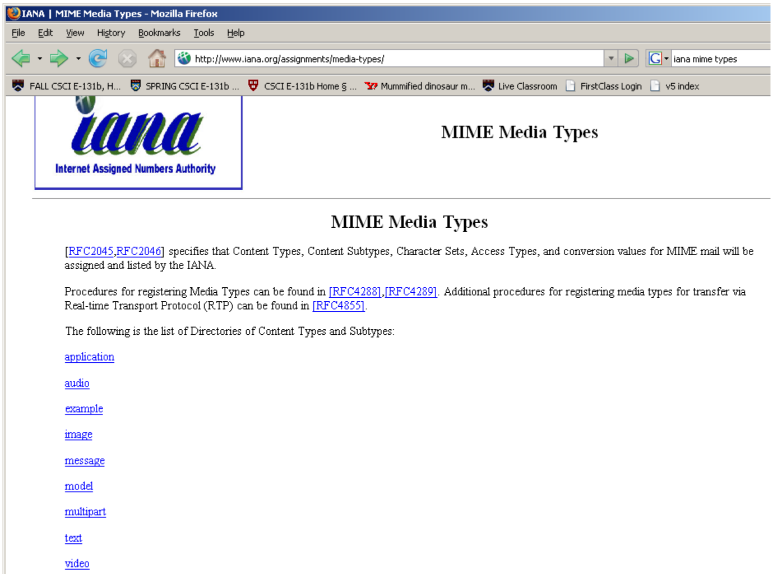
FORWARD 3
Received: from smtp2.fas.harvard.edu [140.247.34.52])
by alum.mit.edu with ESMTP for <len@alum.mit.edu>;
1 Dec 2012 17:10:28 -0500 (EST)
From: csci-40@mail.dce.harvard.edu

FORWARD 2 - not shown
FORWARD 1 - not shown

MIME
(Multipurpose Internet Mail Extensions)

- Defines encoding rules to allow for non-ASCII messages.
- RFCs 2045 through 2049, November 1996
- Defines additional message headers within email message.
- Content-Tansfer-Encoding defines how the body is wrapped for transmission. Schemes include: 7-bit ASCII, 8-bit characters, base64 encoding, quoted-printable, binary
- Content-Type describes the nature of the message. Types include: text, image, audio, video application, multipart
- Sub-types are present for each Content-Type
- Defined first for email, has been applied to HTTP, RTP and SIP. MIME listing available at IANA

WWW.IANA.ORG


IANA | MIME Media Types - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.iana.org/assignments/media-types/

iana mime types

FALL CSCI E-131b, H... SPRING CSCI E-131b ... CSCI E-131b Home § ... Mummified dinosaur m... Live Classroom FirstClass Login v5 index

iana

Internet Assigned Numbers Authority

MIME Media Types

MIME Media Types

[RFC2045,RFC2046] specifies that Content Types, Content Subtypes, Character Sets, Access Types, and conversion values for MIME mail will be assigned and listed by the IANA.

Procedures for registering Media Types can be found in [RFC4288],[RFC4289]. Additional procedures for registering media types for transfer via Real-time Transport Protocol (RTP) can be found in [RFC4855].

The following is the list of Directories of Content Types and Subtypes:

application

audio

example

image

message

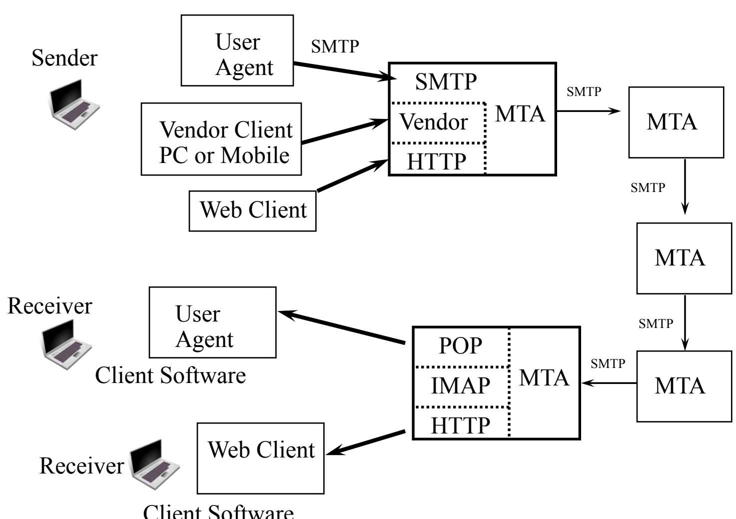
model

multipart

text

video

Mail System Architecture Protocols for Client to MTA



One Minute Wrap-Up

- Please do this Wrap-Up at the end of each lecture.
- Please fill out the form on the website.
- The form is anonymous (but you can include your name if you want.)
- Please answer three questions:
  – What is your grand "Aha" for today's class?
  – What concept did you find most confusing in today's class?
  – What questions should I address next time
- **Thank you!**