Class Notes

Lesson plan for today:

(1) Quiz 2 (Focus is on chapter 1. Continue reading chapter 2 of the textbook.)
(2) Due to many students in class and due to shortage of time in lectures we might need few students to post their five-minute presentations on YouTube and to give us the links to watch via Piazza.
(3) Briefing about check0.
(4) DNS discussion
    a. What is it, why we need it (telephone directory analogy. Well-known hosts)
    b. Primary and secondary functions of the DNS system
    c. Two ways to fully understand DNS (logical view & deployment view)
    d. Role of ISP provided local DNS server
    e. Recursive and iterative DNS queries (walking the DNS tree)
    f. Demo for www.nu.edu.pk and someone@lhr.nu.edu.pk using dig
    g. Resource record details
    h. DNS packet structure
    i. DNS as a "crude" load-balancer
    j. PTR queries in DNS
(5) If time permits, we will discuss TCP sockets (we discussed UDP sockets earlier)

Programming Assignment:

(1) There are 8 parts of the programming assignment.
(2) Check0 is out. It is a warm-up part. Next checks will gradually become challenging.
(3) You will not be able to complete these assignments if you start them late or try to do them in one sitting.
(4) Each next check depends on the previous one. That means if you don't do a part, it will impact you in the next check.
(5) Instead of stressing out about these assignments, try to approach them with a positive attitude. With some struggle you will be able to complete them.

Section 2.4: Domain Name System (DNS)--- The Internet's Directory Service

The global Internet is a packet-switched network. To router and deliver IP packets in this network, a network address is required. We call it the **IP address**. As an analogy from the telephone network, you need your intended receiver's phone number.

Example IP addresses:

www.google.com has IPv4 (version 4 of length 32 bits) 172.217.19.196

www.google.com has IPv6 (version 6 of length 128 bits) 2a00:1450:4019:80e::2004 (Each number is a hex digit, means 4 bits called nibble. So, there can be 8 such groups separated by ":")

Remembering human-friendly names (like www.google.com) is much easier than remembering IP addresses! DNS provides this mapping.

(Actually, Google has many IPv4 addresses. Different regions might get a different IP address from DNS for load balancing purposes.)

```
C:\Users\abdul>ping www.google.com

Pinging www.google.com [2a00:1450:4019:80e::2004] with 32 bytes of data:
Reply from 2a00:1450:4019:80e::2004: time=88ms
Reply from 2a00:1450:4019:80e::2004: time=60ms
Reply from 2a00:1450:4019:80e::2004: time=76ms
Reply from 2a00:1450:4019:80e::2004: time=82ms

Ping statistics for 2a00:1450:4019:80e::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 88ms, Average = 76ms
```

```
C:\Users\abdul>ping -4 www.google.com

Pinging www.google.com [172.217.19.196] with 32 bytes of data:
Reply from 172.217.19.196: bytes=32 time=80ms TTL=54
Reply from 172.217.19.196: bytes=32 time=71ms TTL=54
Reply from 172.217.19.196: bytes=32 time=71ms TTL=54
Reply from 172.217.19.196: bytes=32 time=70ms TTL=54

Ping statistics for 172.217.19.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 80ms, Average = 73ms
```

Some organizations try to be creative with their IPv6 addresses:

```
C:\Users\abdul>ping -6 www.facebook.com

Pinging star-mini.c10r.facebook.com [2a03:2880:f167:81:face:b00c:0:25de] with 32 bytes of data:
Reply from 2a03:2880:f167:81:face:b00c:0:25de: time=219ms
Reply from 2a03:2880:f167:81:face:b00c:0:25de: time=80ms
Reply from 2a03:2880:f167:81:face:b00c:0:25de: time=69ms
Reply from 2a03:2880:f167:81:face:b00c:0:25de: time=79ms

Ping statistics for 2a03:2880:f167:81:face:b00c:0:25de:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 219ms, Average = 111ms
```

Same goes for the email. If you need to send an email to somone@lhr.nu.edu.pk, the client side of Simple Main Transfer Protocol (SMTP) needs to know where is the SMTP mail server that is responsible for receiving "someone's" emails. Again, DNS provides that mapping.

DNS is **a critical infrastructure application** on the Internet. If DNS is not available to you, you might not visit any website, or could not send any email, and most of your workflow will be disrupted. DNS's availability is critical. That is why special engineering effort is devoted to the DNS, with thousands of servers, spread across the globe to make sure DNS is always available. **Sharding** and **replication** (two key concepts in distributed systems) is heavily used for DNS engineering.

One machine will not be enough to server DNS queries, that could be trillions of queries per day. One machine is a single-point-of-failure. If that server crashes, the whole DNS goes away.

In the early days of the Arpa net, there was this **hosts file** that maintained host name to IP address mapping. Different folks will download that file after a while (say every week).

What is DNS:

(1) DNS is a distributed database implemented in a hierarchy of DNS servers
(2) An application layer protocol that allows hosts to query the distributed database

DNS resolution delay:

DNS resolution can add **substantial delays** for the end user (for example when we type www.nu.edu.pk and the browser needs the IP address of the host nu.edu.pk). We will see later that DNS responses can be cached locally or "near-by" so that future requests for the same name could be fast.

Other auxiliary services of DNS:

(1) Host aliasing.
    a. Canonical name could be: relay1.west-coast.enterprise.com
    b. Alias could be: www.enterpirse.com
    c. DNS can give the canonical name and IP of the host given the alias.
(2) Mail server aliasing.

a. Canonical name of the mail server could be relay1.west-coast.yahoo.com
b. Alias could be yahoo.com
c. Using a special DNS record type (called MX record), both host names and mail server name could be the same (aliases).

(3) Load distribution

a. Large sites (such as cnn.com or google.com) have excessive user load (for example billions of search queries coming to the web server at Google.) Such sites therefore have many replicated services on many servers, each server having a different IP address. DNS might rotate available IPs for a name for different queries, say in round-robin fashion.
b. At times DNS server return multiple IP addresses to the client. Other times, server picks one IP of its choice and provides that one. DNS might provide an IP address that is "near" to the client. What constitutes "near" varies. It could be geographical distance or network distance (say in terms of number of hops from the client to the service.)

DNS Data sharded into zones:

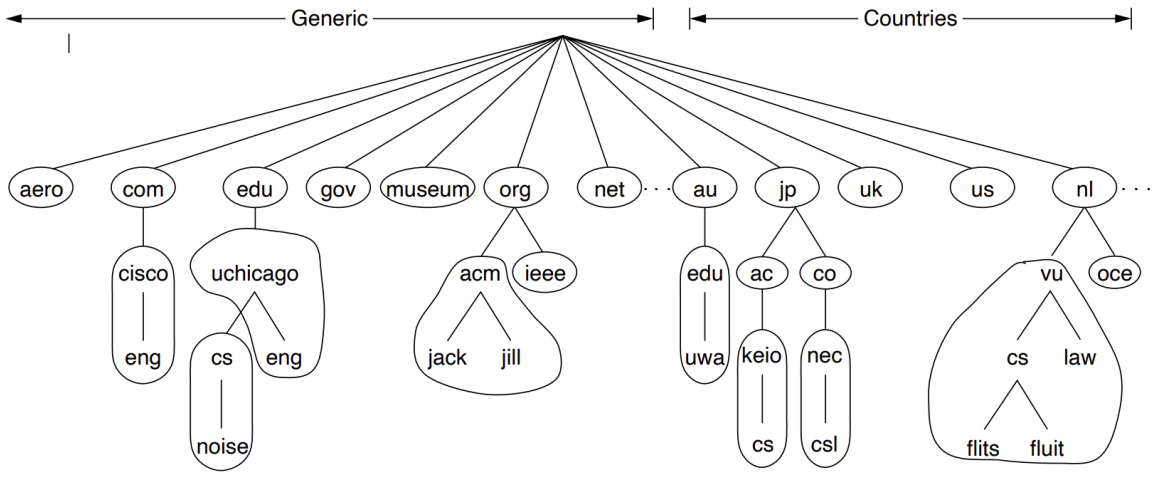
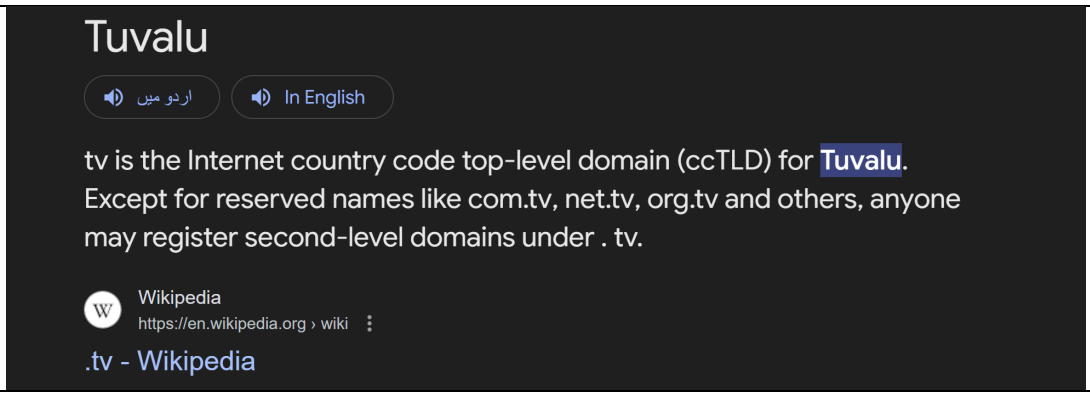


Figure 7-6. Part of the DNS name space divided into zones (which are circled).

Tuvalu (Pronounced as: Too-Vuh-Loo) is located in south Pacific Ocean, near Australia.



The Top 10 Most Expensive Domains Ever Reported

When it comes to memorable domain names that are short, to the point and can describe their intent in a matter of seconds, businesses and large corporations are willing to spend big bucks to secure their space on the Internet.

Here are some of the most valuable domain names ever reported:

1. Cars.com – $872 million
2. CarINsurance.com – $49.7 million
3. Insurance.com – $35.6 million
4. VacationRentals.com – $35 million
5. PrivateJet.com – $30.18 million
6. Voice.com – $30 million
7. Internet.com – $18 million
8. 360.com – $17 million
9. Insure.com – $16 million
10. Fund.com – $9.95 million

Source: https://www.name.com/blog/the-top-10-most-expensive-domains-ever-sold

Whois:

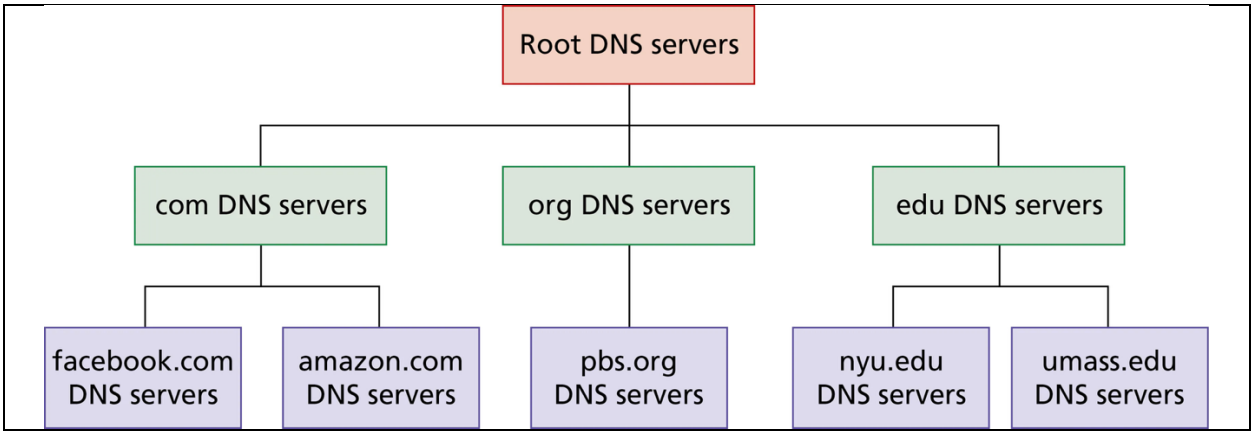
The **`whois`** command-line tool is a client program that queries the **WHOIS database,** which stores registration details about Internet resources such as **domain names, IP address blocks,** or **autonomous system numbers (ASNs).**

```
$whois 1.1.1.1
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.apnic.net

inetnum:      1.0.0.0 - 1.255.255.255
organisation: APNIC
```

```
status:       ALLOCATED

whois:        whois.apnic.net

changed:      2010-01
source:       IANA

# whois.apnic.net

% [whois.apnic.net]
% Whois data copyright terms
http://www.apnic.net/db/dbcopyright.html

% Information related to '1.1.1.0 - 1.1.1.255'

% Abuse contact for '1.1.1.0 - 1.1.1.255' is 'helpdesk@apnic.net'

inetnum:        1.1.1.0 - 1.1.1.255
netname:        APNIC-LABS
descr:          APNIC and Cloudflare DNS Resolver project
descr:          Routed globally by AS13335/Cloudflare
descr:          Research prefix for APNIC Labs
country:        AU
org:            ORG-ARAD1-AP
admin-c:        AIC3-AP
tech-c:         AIC3-AP
abuse-c:        AA1412-AP
status:         ASSIGNED PORTABLE
remarks:        ---------------
remarks:        All Cloudflare abuse reporting can be done via
remarks:        resolver-abuse@cloudflare.com
remarks:        ---------------
mnt-by:         APNIC-HM
mnt-routes:     MAINT-APNICRANDNET
mnt-irt:        IRT-APNICRANDNET-AU
last-modified:  2023-04-26T22:57:58Z
mnt-lower:      MAINT-APNICRANDNET
source:         APNIC

irt:            IRT-APNICRANDNET-AU
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
e-mail:         helpdesk@apnic.net
abuse-mailbox:  helpdesk@apnic.net
admin-c:        AR302-AP
tech-c:         AR302-AP
auth:           # Filtered
remarks:        helpdesk@apnic.net was validated on 2021-02-09
mnt-by:         MAINT-APNICRANDNET
```

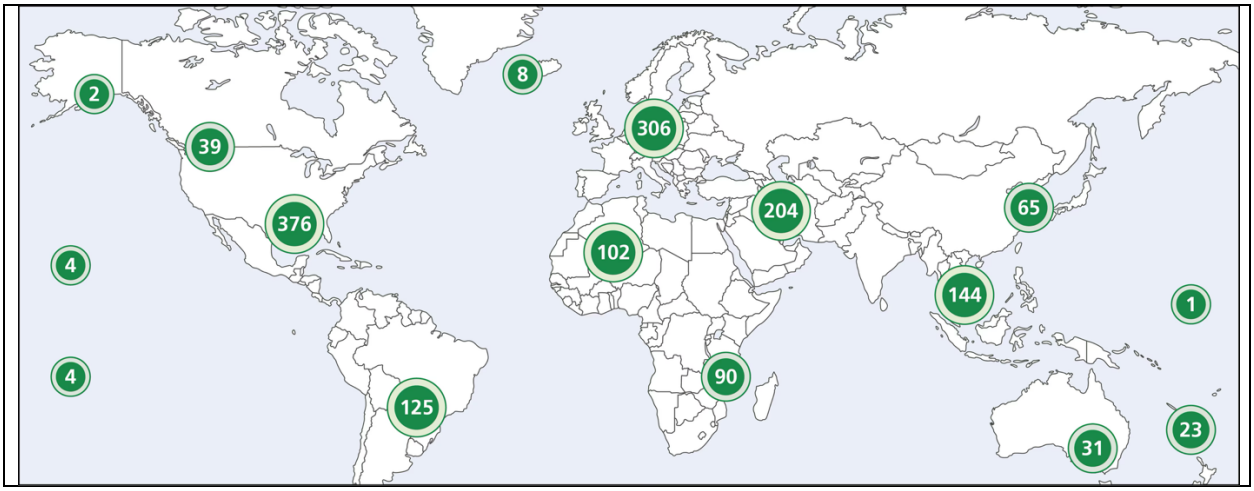
```
last-modified:  2025-09-03T02:28:14Z
source:         APNIC

organisation:   ORG-ARAD1-AP
org-name:       APNIC Research and Development
org-type:       LIR
country:        AU
address:        6 Cordelia St
phone:          +61-7-38583100
fax-no:         +61-7-38583199
e-mail:         helpdesk@apnic.net
mnt-ref:        APNIC-HM
mnt-by:         APNIC-HM
last-modified:  2023-09-05T02:15:19Z
source:         APNIC

role:           ABUSE APNICRANDNETAU
country:        ZZ
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
phone:          +000000000
e-mail:         helpdesk@apnic.net
admin-c:        AR302-AP
tech-c:         AR302-AP
nic-hdl:        AA1412-AP
remarks:        Generated from irt object IRT-APNICRANDNET-AU
remarks:        helpdesk@apnic.net was validated on 2021-02-09
abuse-mailbox:  helpdesk@apnic.net
mnt-by:         APNIC-ABUSE
last-modified:  2025-05-28T03:31:35Z
source:         APNIC

role:           APNICRANDNET Infrastructure Contact
address:        6 Cordelia St
                South Brisbane
                QLD 4101
country:        AU
phone:          +61 7 3858 3100
e-mail:         research@apnic.net
admin-c:        AIC3-AP
tech-c:         AIC3-AP
nic-hdl:        AIC3-AP
mnt-by:         MAINT-APNICRANDNET
last-modified:  2024-07-18T04:37:37Z
source:         APNIC

% Information related to '1.1.1.0/24AS13335'

route:          1.1.1.0/24
```

```
origin:          AS13335
descr:           APNIC Research and Development
                 6 Cordelia St
mnt-by:          MAINT-APNICRANDNET
last-modified:   2023-04-26T02:42:44Z
source:          APNIC

% This query was served by the APNIC Whois Service version 1.88.34
(WHOIS-JP1)


 $
```

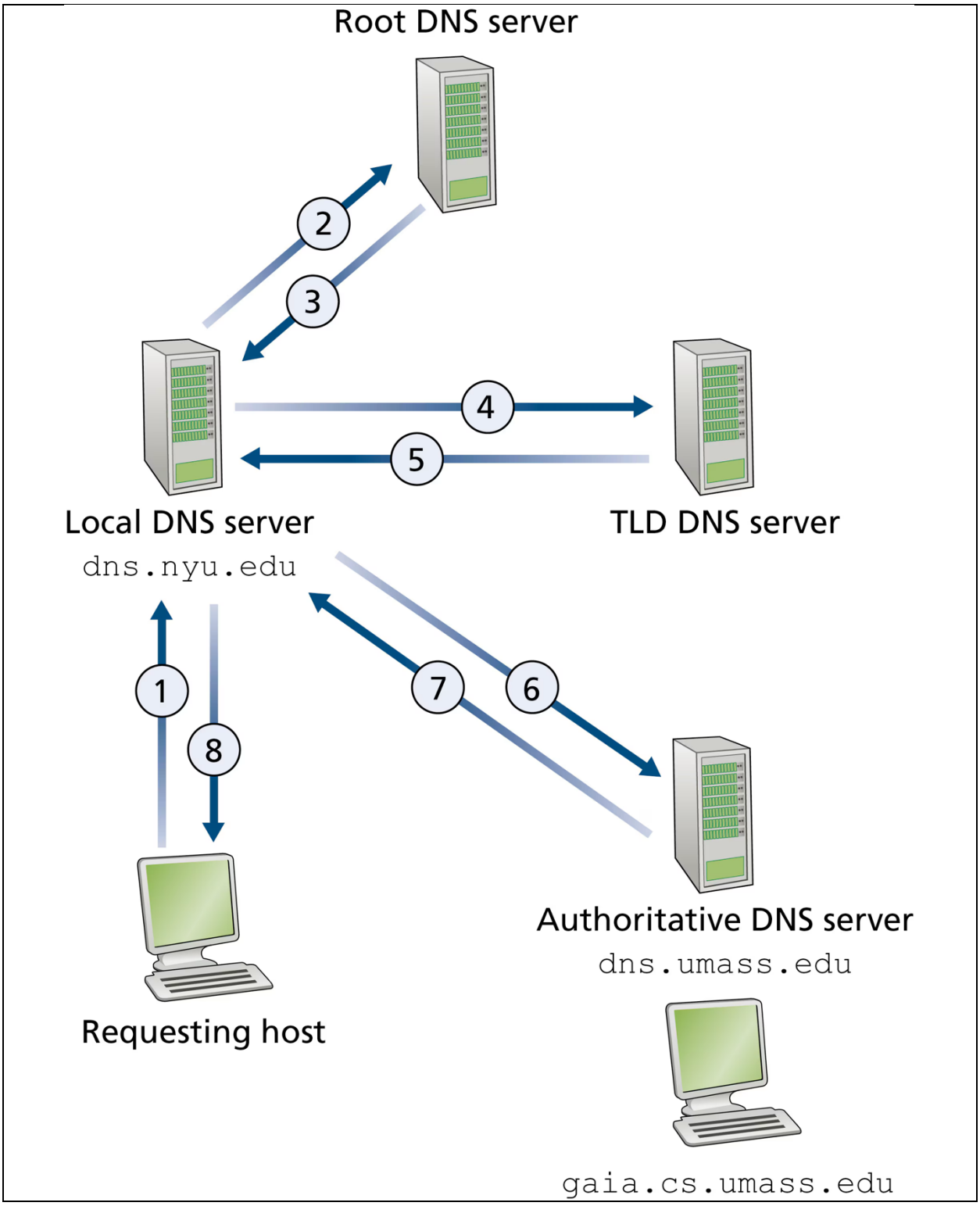


13 replicated root servers across the globe:

Logically 13, but physically many.



Typical DNS query resolution:



Two helpful program you should learn about:

(1) nslookup

(2) dig

Examples:

```
[aqadeer@AQWM ~]$ nslookup www.nu.edu.pk
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.nu.edu.pk   canonical name = nu.edu.pk.
Name:   nu.edu.pk
Address: 203.124.44.78

[aqadeer@AQWM ~]$ nslookup www.google.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.19.196
Name:   www.google.com
Address: 2a00:1450:4019:80e::2004
```

```
[aqadeer@AQWM ~]$ dig www.nu.edu.pk

; <<>> DiG 9.18.26 <<>> www.nu.edu.pk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42741
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.nu.edu.pk.                 IN      A

;; ANSWER SECTION:
www.nu.edu.pk.          9230    IN      CNAME   nu.edu.pk.
nu.edu.pk.              11014   IN      A       203.124.44.78

;; Query time: 6 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Sep 02 13:01:16 PKT 2024
;; MSG SIZE  rcvd: 81
```

```
[aqadeer@AQWM ~]$ dig -t AAAA www.google.com

; <<>> DiG 9.18.26 <<>> -t AAAA www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17344
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.google.com.                        IN      AAAA

;; ANSWER SECTION:
www.google.com.         74      IN      AAAA    2a00:1450:4019:80b::2004

;; Query time: 6 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Sep 02 13:06:18 PKT 2024
;; MSG SIZE  rcvd: 71
```

Lets do all the steps ourselves:

Step 1: List all the root servers

```
[aqadeer@AQWM ~]$ dig

; <<>> DiG 9.18.26 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53399
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: e9dd36b3e4fc123d1c42836866d5724be1e176bab9243c22 (good)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       50482   IN      NS      l.root-servers.net.
.                       50482   IN      NS      a.root-servers.net.
.                       50482   IN      NS      b.root-servers.net.
.                       50482   IN      NS      m.root-servers.net.
.                       50482   IN      NS      g.root-servers.net.
.                       50482   IN      NS      k.root-servers.net.
.                       50482   IN      NS      e.root-servers.net.
.                       50482   IN      NS      c.root-servers.net.
.                       50482   IN      NS      i.root-servers.net.
.                       50482   IN      NS      d.root-servers.net.
.                       50482   IN      NS      h.root-servers.net.
.                       50482   IN      NS      j.root-servers.net.
.                       50482   IN      NS      f.root-servers.net.

;; Query time: 69 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Sep 02 13:07:39 PKT 2024
;; MSG SIZE  rcvd: 267
```

Step 2: Lets pick any one of them to move forward in resolution.

```
[aqadeer@AQWM ~]$ dig www.nu.edu.pk @b.root-servers.net

; <<>> DiG 9.18.26 <<>> www.nu.edu.pk @b.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34243
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 7
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.nu.edu.pk.                 IN      A

;; AUTHORITY SECTION:
pk.                     172800  IN      NS      root-e.pknic.pk.
pk.                     172800  IN      NS      root-s.pknic.pk.
pk.                     172800  IN      NS      root-c1.pknic.pk.
pk.                     172800  IN      NS      root-c2.pknic.pk.

;; ADDITIONAL SECTION:
root-e.pknic.pk.        172800  IN      A       107.6.178.178
root-s.pknic.pk.        172800  IN      A       119.81.34.90
root-c1.pknic.pk.       172800  IN      A       185.159.197.160
root-c1.pknic.pk.       172800  IN      AAAA    2620:10a:80aa::160
root-c2.pknic.pk.       172800  IN      A       185.159.198.160
root-c2.pknic.pk.       172800  IN      AAAA    2620:10a:80ab::160

;; Query time: 213 msec
;; SERVER: 2801:1b8:10::b#53(b.root-servers.net) (UDP)
;; WHEN: Mon Sep 02 13:16:48 PKT 2024
;; MSG SIZE  rcvd: 254
```

Step 3:

```
[aqadeer@AQWM ~]$ dig www.nu.edu.pk @root-c1.pknic.pk.

; <<>> DiG 9.18.26 <<>> www.nu.edu.pk @root-c1.pknic.pk.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38778
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.nu.edu.pk.                 IN      A

;; AUTHORITY SECTION:
nu.edu.PK.              86400   IN      NS      n1.comsats.net.pk.
nu.edu.PK.              86400   IN      NS      n2.comsats.net.pk.

;; ADDITIONAL SECTION:
n2.comsats.net.PK.      86400   IN      A       203.124.45.92
n1.comsats.net.PK.      86400   IN      A       210.56.11.130

;; Query time: 180 msec
;; SERVER: 2620:10a:80aa::160#53(root-c1.pknic.pk.) (UDP)
;; WHEN: Mon Sep 02 13:19:35 PKT 2024
;; MSG SIZE  rcvd: 151
```

Step 4:

```
[aqadeer@AQWM ~]$ dig www.nu.edu.pk @n1.comsats.net.pk.

; <<>> DiG 9.18.26 <<>> www.nu.edu.pk @n1.comsats.net.pk.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61437
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d8a4a46233579285aaa2587566d57498a382807b126c310d (good)
;; QUESTION SECTION:
;www.nu.edu.pk.                 IN      A

;; ANSWER SECTION:
www.nu.edu.pk.          14400   IN      CNAME   nu.edu.pk.
nu.edu.pk.              14400   IN      A       203.124.44.78

;; AUTHORITY SECTION:
nu.edu.pk.              86400   IN      NS      n2.comsats.net.pk.
nu.edu.pk.              86400   IN      NS      n1.comsats.net.pk.

;; Query time: 55 msec
;; SERVER: 210.56.11.130#53(n1.comsats.net.pk.) (UDP)
;; WHEN: Mon Sep 02 13:20:43 PKT 2024
;; MSG SIZE  rcvd: 146
```

Similar for the email:

```
[aqadeer@AQWM ~]$ dig lhr.nu.edu.pk MX

; <<>> DiG 9.18.26 <<>> lhr.nu.edu.pk MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42030
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 497453a70c42c56dd89b7b4466d57749af7a0748547db1bb (good)
;; QUESTION SECTION:
;lhr.nu.edu.pk.                 IN      MX

;; ANSWER SECTION:
lhr.nu.edu.pk.          3484    IN      MX      1 ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.          3484    IN      MX      10 ALT4.ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.          3484    IN      MX      10 ALT3.ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.          3484    IN      MX      5 ALT1.ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.          3484    IN      MX      5 ALT2.ASPMX.L.GOOGLE.COM.

;; Query time: 48 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon Sep 02 13:28:57 PKT 2024
;; MSG SIZE  rcvd: 188
```

We can use:
Dig +trace www.nu.edu.pk
to see how resolution happens from root to the leaves:

```
$dig +trace www.nu.edu.pk

; <<>> DiG 9.10.6 <<>> +trace www.nu.edu.pk
;; global options: +cmd
.            403350   IN   NS   k.root-servers.net.
.            403350   IN   NS   d.root-servers.net.
.            403350   IN   NS   c.root-servers.net.
.            403350   IN   NS   l.root-servers.net.
.            403350   IN   NS   g.root-servers.net.
.            403350   IN   NS   b.root-servers.net.
.            403350   IN   NS   m.root-servers.net.
.            403350   IN   NS   j.root-servers.net.
.            403350   IN   NS   f.root-servers.net.
.            403350   IN   NS   i.root-servers.net.
.            403350   IN   NS   e.root-servers.net.
.            403350   IN   NS   h.root-servers.net.
.            403350   IN   NS   a.root-servers.net.
.            403350   IN   RRSIG   NS 8 0 518400 20250914170000
20250901160000 46441 .
a1IJsEURaxosjYZ49mO4br0JiOjCMGPfSyC/up+wi27LcJxGQ/3/5mKY
uVOYgtgu38pYt8pUapnRGhJa6UHN1LR8onpndygtQoeVHrQecKOKh/Yv
PiWQyB4MzfnbXeMjt1nNCkzrwZkbyjYKq7wDmj0+WZXqFnHJFSLkTEQZ
0YnZl7ZgBde4QQReCmIMbv8Khwp4dfo/4x7mIrsW0EhDgLC0mmxElVfe
P6jeM4ezVXXk1tiNehZ/ztSTpGocliH8PoFGNSgl4vmtYKQowLRKmxMI
MysATIHv70CAZ9Dsqy5mYDIX32qusaWffJNDaj3iD1zpliB5yO20PpHm S+BUjg==
```

```
;; Received 1109 bytes from
fe80::b00a:d50b:c1e7:1%14#53(fe80::b00a:d50b:c1e7:1%14) in 87 ms

pk.          172800   IN  NS   root-e.pknic.pk.
pk.          172800   IN  NS   root-s.pknic.pk.
pk.          172800   IN  NS   root-c1.pknic.pk.
pk.          172800   IN  NS   root-c2.pknic.pk.
pk.          86400    IN  NSEC pl. NS RRSIG NSEC
pk.          86400    IN  RRSIG   NSEC 8 1 86400 20250915170000
20250902160000 46441 .
FnW/6zL96Qm8fK3suGIIxW0nxI6vBECVdsCEaDrJ0vlIADZIvtdjeuyb
3uL6wJ76fcr/3YLedJ56arAQcQtUopDVnIRfuHpJP0hfuL9igwDxBTID
7MpvWjxAtjgn18TLNFLu/IiaM/aYDVN9nDkg7xDOEpLD0ReAE6bHMfbn
sw9cre1gcV4yltLzr+yAvvThLeOdnlCOSoXiA0BJsj7DanGf4tGB9caV
0m8iGkSMGSO8RcK6BIGJLHGye10MvDoEy2YVyTodTGUUfTcahG6i1FkI
N70wZhlxcJKwXBtP4r4az9v7VkUbUKrAUXYjLwTYxom//lsuHv962U0A xMe3iQ==
;; Received 565 bytes from 192.203.230.10#53(e.root-servers.net) in
152 ms

nu.edu.PK.       86400    IN  NS   n1.comsats.net.pk.
nu.edu.PK.       86400    IN  NS   n2.comsats.net.pk.
;; Received 147 bytes from 119.81.34.90#53(root-s.pknic.pk) in 140
ms

www.nu.edu.pk.       14400    IN   CNAME    nu.edu.pk.
nu.edu.pk.       14400    IN   A    203.124.44.78
nu.edu.pk.       86400    IN   NS   n2.comsats.net.pk.
nu.edu.pk.       86400    IN   NS   n1.comsats.net.pk.
;; Received 118 bytes from 210.56.11.130#53(n1.comsats.net.pk) in 51
ms

 $


$dig +trace nu.edu.pk MX

; <<>> DiG 9.10.6 <<>> +trace nu.edu.pk MX
;; global options: +cmd
.            403236   IN  NS   f.root-servers.net.
.            403236   IN  NS   k.root-servers.net.
.            403236   IN  NS   e.root-servers.net.
.            403236   IN  NS   g.root-servers.net.
.            403236   IN  NS   h.root-servers.net.
.            403236   IN  NS   b.root-servers.net.
.            403236   IN  NS   c.root-servers.net.
.            403236   IN  NS   a.root-servers.net.
.            403236   IN  NS   l.root-servers.net.
.            403236   IN  NS   d.root-servers.net.
.            403236   IN  NS   j.root-servers.net.
.            403236   IN  NS   m.root-servers.net.
```

```
.           403236   IN  NS  i.root-servers.net.
.           403236   IN  RRSIG   NS 8 0 518400 20250914170000
20250901160000 46441 .
a1IJsEURaxosjYZ49mO4br0JiOjCMGPfSyC/up+wi27LcJxGQ/3/5mKY
uVOYgtgu38pYt8pUapnRGhJa6UHN1LR8onpndygtQoeVHrQecKOKh/Yv
PiWQyB4MzfnbXeMjt1nNCkzrwZkbyjYKq7wDmj0+WZXqFnHJFSLkTEQZ
0YnZl7ZgBde4QQReCmIMbv8Khwp4dfo/4x7mIrsW0EhDgLC0mmxElVfe
P6jeM4ezVXXk1tiNehZ/ztSTpGocliH8PoFGNSgl4vmtYKQowLRKmxMI
MysATIHv70CAZ9Dsqy5mYDIX32qusaWffJNDaj3iD1zpliB5yO20PpHm S+BUjg==
;; Received 1109 bytes from
fe80::b00a:d50b:c1e7:1%14#53(fe80::b00a:d50b:c1e7:1%14) in 79 ms

pk.         172800   IN  NS  root-s.pknic.pk.
pk.         172800   IN  NS  root-e.pknic.pk.
pk.         172800   IN  NS  root-c2.pknic.pk.
pk.         172800   IN  NS  root-c1.pknic.pk.
pk.         86400    IN  NSEC pl. NS RRSIG NSEC
pk.         86400    IN  RRSIG   NSEC 8 1 86400 20250915170000
20250902160000 46441 .
FnW/6zL96Qm8fK3suGIIxW0nxI6vBECVdsCEaDrJ0vlIADZIvtdjeuyb
3uL6wJ76fcr/3YLedJ56arAQcQtUopDVnIRfuHpJP0hfuL9igwDxBTID
7MpvWjxAtjgn18TLNFLu/IiaM/aYDVN9nDkg7xDOEpLD0ReAE6bHMfbn
sw9cre1gcV4yltLzr+yAvvThLeOdnlCOSoXiA0BJsj7DanGf4tGB9caV
0m8iGkSMGSO8RcK6BIGJLHGye10MvDoEy2YVyTodTGUUfTcahG6i1FkI
N70wZhlxcJKwXBtP4r4az9v7VkUbUKrAUXYjLwTYxom//lsuHv962U0A xMe3iQ==
;; Received 565 bytes from 202.12.27.33#53(m.root-servers.net) in
357 ms

nu.edu.PK.       86400    IN  NS  n1.comsats.net.pk.
nu.edu.PK.       86400    IN  NS  n2.comsats.net.pk.
;; Received 143 bytes from 2620:10a:80ab::160#53(root-c2.pknic.pk)
in 205 ms

nu.edu.pk.       14400    IN  MX  10 aspmx4.googlemail.com.
nu.edu.pk.       14400    IN  MX  0 aspmx.l.google.com.
nu.edu.pk.       14400    IN  MX  10 aspmx2.googlemail.com.
nu.edu.pk.       14400    IN  MX  10 aspmx3.googlemail.com.
nu.edu.pk.       14400    IN  MX  10 aspmx5.googlemail.com.
nu.edu.pk.       14400    IN  MX  5 alt2.aspmx.l.google.com.
nu.edu.pk.       14400    IN  MX  5 alt1.aspmx.l.google.com.
nu.edu.pk.       86400    IN  NS  n2.comsats.net.pk.
nu.edu.pk.       86400    IN  NS  n1.comsats.net.pk.
;; Received 263 bytes from 210.56.11.130#53(n1.comsats.net.pk) in 65
ms

 $


$dig  +trace lhr.nu.edu.pk MX
```

```
; <<>> DiG 9.10.6 <<>> +trace lhr.nu.edu.pk MX
;; global options: +cmd
.            403150   IN   NS   e.root-servers.net.
.            403150   IN   NS   g.root-servers.net.
.            403150   IN   NS   d.root-servers.net.
.            403150   IN   NS   b.root-servers.net.
.            403150   IN   NS   m.root-servers.net.
.            403150   IN   NS   k.root-servers.net.
.            403150   IN   NS   j.root-servers.net.
.            403150   IN   NS   a.root-servers.net.
.            403150   IN   NS   l.root-servers.net.
.            403150   IN   NS   f.root-servers.net.
.            403150   IN   NS   h.root-servers.net.
.            403150   IN   NS   c.root-servers.net.
.            403150   IN   NS   i.root-servers.net.
.            403150   IN   RRSIG   NS 8 0 518400 20250914170000
20250901160000 46441 .
a1IJsEURaxosjYZ49mO4br0JiOjCMGPfSyC/up+wi27LcJxGQ/3/5mKY
uVOYgtgu38pYt8pUapnRGhJa6UHN1LR8onpndygtQoeVHrQecKOKh/Yv
PiWQyB4MzfnbXeMjt1nNCkzrwZkbyjYKq7wDmj0+WZXqFnHJFSLkTEQZ
0YnZl7ZgBde4QQReCmIMbv8Khwp4dfo/4x7mIrsW0EhDgLC0mmxElVfe
P6jeM4ezVXXk1tiNehZ/ztSTpGocliH8PoFGNSgl4vmtYKQowLRKmxMI
MysATIHv70CAZ9Dsqy5mYDIX32qusaWffJNDaj3iD1zpliB5yO20PpHm S+BUjg==
;; Received 1109 bytes from
fe80::b00a:d50b:c1e7:1%14#53(fe80::b00a:d50b:c1e7:1%14) in 71 ms

pk.          172800   IN   NS   root-e.pknic.pk.
pk.          172800   IN   NS   root-s.pknic.pk.
pk.          172800   IN   NS   root-c1.pknic.pk.
pk.          172800   IN   NS   root-c2.pknic.pk.
pk.          86400    IN   NSEC pl. NS RRSIG NSEC
pk.          86400    IN   RRSIG   NSEC 8 1 86400 20250915170000
20250902160000 46441 .
FnW/6zL96Qm8fK3suGIIxW0nxI6vBECVdsCEaDrJ0vlIADZIvtdjeuyb
3uL6wJ76fcr/3YLedJ56arAQcQtUopDVnIRfuHpJP0hfuL9igwDxBTID
7MpvWjxAtjgn18TLNFLu/IiaM/aYDVN9nDkg7xDOEpLD0ReAE6bHMfbn
sw9cre1gcV4yltLzr+yAvvThLeOdnlCOSoXiA0BJsj7DanGf4tGB9caV
0m8iGkSMGSO8RcK6BIGJLHGye10MvDoEy2YVyTodTGUUfTcahG6i1FkI
N70wZhlxcJKwXBtP4r4az9v7VkUbUKrAUXYjLwTYxom//lsuHv962U0A xMe3iQ==
;; Received 565 bytes from 2001:500:2d::d#53(d.root-servers.net) in
147 ms

nu.edu.pk.       86400    IN   NS   n1.comsats.net.pk.
nu.edu.pk.       86400    IN   NS   n2.comsats.net.pk.
;; Received 120 bytes from 2620:10a:80ab::160#53(root-c2.pknic.pk)
in 371 ms

lhr.nu.edu.pk.       3600 IN   MX   5 ALT1.ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.       3600 IN   MX   10 ALT3.ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.       3600 IN   MX   1 ASPMX.L.GOOGLE.COM.
```

```
lhr.nu.edu.pk.        3600 IN  MX  10 ALT4.ASPMX.L.GOOGLE.COM.
lhr.nu.edu.pk.        3600 IN  MX  5 ALT2.ASPMX.L.GOOGLE.COM.
nu.edu.pk.       86400    IN  NS  n1.comsats.net.pk.
nu.edu.pk.       86400    IN  NS  n2.comsats.net.pk.
;; Received 206 bytes from 210.56.11.130#53(n1.comsats.net.pk) in 67
ms

 $
```

There used to be a hosts.txt file in very early days of the Internet, which ware less frequently updated and when updated it was shared, say few times a week.

Linux and Unix based hosts still has something like that in /etc/hosts

"`/etc/hosts` is a simple text file on Unix-like systems that maps hostnames to IP addresses, acting like a small, local DNS.

History: In the early days of ARPANET (1970s–early 1980s), there was no DNS. Instead, a central file called *HOSTS.TXT* was maintained at SRI (Stanford Research Institute) and distributed to all networked computers. Each machine used that file to resolve hostnames to IPs. When the Internet grew too large for this system to scale, DNS was invented (1983), but the local `hosts` file remained for compatibility, overrides, and testing.

So `/etc/hosts` is essentially a leftover from the *pre-DNS era* that's still useful today.

" Credit: ChatGPT

```
$cat /etc/hosts
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1       localhost
255.255.255.255 broadcasthost
::1             localhost
 $
```

While we are at it, you can see well-known ports in Linux / Unix machines at: /etc/services:

```
#
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, most entries here have two entries
# even if the protocol doesn't support UDP operations.
#
# The latest IANA port assignments can be gotten from
#
#       http://www.iana.org/assignments/port-numbers
#
# The Well Known Ports are those from 0 through 1023.
# The Registered Ports are those from 1024 through 49151
# The Dynamic and/or Private Ports are those from 49152 through 65535
#
# $FreeBSD: src/etc/services,v 1.89 2002/12/17 23:59:10 eric Exp $
#       From: @(#)services      5.8 (Berkeley) 5/9/91
#
# WELL KNOWN PORT NUMBERS
#
rtmp            1/ddp    #Routing Table Maintenance Protocol
tcpmux          1/udp     # TCP Port Service Multiplexer
tcpmux          1/tcp     # TCP Port Service Multiplexer
#                        Mark Lottor <MKL@nisc.sri.com>
nbp             2/ddp    #Name Binding Protocol
compressnet     2/udp     # Management Utility
compressnet     2/tcp     # Management Utility
compressnet     3/udp     # Compression Process
compressnet     3/tcp     # Compression Process
#                        Bernie Volz <VOLZ@PROCESS.COM>
echo            4/ddp    #AppleTalk Echo Protocol
#               4/tcp    Unassigned
#               4/udp    Unassigned
rje             5/udp     # Remote Job Entry

finger          79/udp     # Finger
finger          79/tcp     # Finger
#                        David Zimmerman <dpz@RUTGERS.EDU>
http            80/udp     www www-http # World Wide Web HTTP
http            80/tcp     www www-http # World Wide Web HTTP
#                        Tim Berners-Lee <timbl@W3.org>
hosts2-ns       81/udp     # HOSTS2 Name Server
hosts2-ns       81/tcp     # HOSTS2 Name Server
```

ICANN, IANA, RIRs (So many acronyms: )

IANA (ICANN) → RIRs (ARIN, RIPE, APNIC, LACNIC, AFRINIC) → ISPs / organizations → end users

ICANN – *Internet Corporation for Assigned Names and Numbers*

- A **nonprofit organization** based in California (founded in 1998).
- Oversees the **global Domain Name System (DNS)**, including top-level domains (like `.com`, `.org`, `.pk`).
- Coordinates the **policies** and contracts for domain registries, registrars, and root name servers.
- In short: ICANN manages the **business and policy side** of the Internet's naming system.

IANA – *Internet Assigned Numbers Authority*

- A **function** performed under ICANN's umbrella.
- Handles the **technical coordination** of:
    1. **DNS root zone** (assigning TLDs, publishing root zone data).

2. **IP addresses** (allocating large IP blocks to Regional Internet Registries like APNIC, RIPE, ARIN).
3. **Protocol parameters** (port numbers, protocol numbers, values used in Internet standards).

- In short: IANA manages the **technical registries** that keep the Internet interoperable.

- **ICANN** = the organization setting policies and contracts for the "phone book of the Internet."

- **IANA** = the registry clerks maintaining the official lists of phone numbers, prefixes, and technical codes.

The 5 Regional Internet Registries (RIRs)

These are nonprofit organizations that allocate and manage IP address blocks **within their regions**:

1. **ARIN** – American Registry for Internet Numbers
   - Region: USA, Canada, parts of the Caribbean
2. **RIPE NCC** – Réseaux IP Européens Network Coordination Centre
   - Region: Europe, Middle East, Central Asia
3. **APNIC** – Asia-Pacific Network Information Centre
   - Region: Asia and Pacific (including Pakistan, India, China, Australia, etc.)
4. **LACNIC** – Latin America and Caribbean Network Information Centre
   - Region: Latin America, Caribbean (except parts covered by ARIN)
5. **AFRINIC** – African Network Information Centre
   - Region: Africa

DNS record types:

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

Figure 7-4. The principal DNS resource record types.

Source: Computer Networks by Tanenbaum et al.

Reverse DNS (Given an IP, tell a human readable name):

```
$dig -x 8.8.8.8

; <<>> DiG 9.10.6 <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN   PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.54805     IN   PTR dns.google.

;; Query time: 62 msec
;; SERVER: fe80::b00a:d50b:c1e7:1%14#53(fe80::b00a:d50b:c1e7:1%14)
;; WHEN: Wed Sep 03 10:41:12 PKT 2025
;; MSG SIZE  rcvd: 73
```

Top Level Domains:

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

Figure 7-2. The original generic TLDs, as of 2010. As of 2020, there are more than 1,200 gTLDs.

Source: Computer networks by Tanenbaum

ICANN and Others:

From Wikipedia: “The **Internet Corporation for Assigned Names and Numbers** (**ICANN** /ˈaɪkæn/ *EYE-kan*) is a global multistakeholder group and nonprofit organization headquartered in the United States responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the Internet's stable and secure operation.”

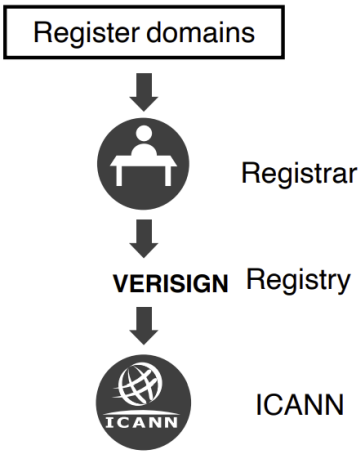


Figure 7-3. The relationship between registries and registrars.

DNS packet format:

1. **Header**: Contains metadata about the DNS query or response, including flags, operation codes, and counts of various sections.

2. **Question**: Specifies the domain name being queried, along with the type of query (e.g., A, MX) and the class (usually IN for internet).

3. **Answer**: Holds the resource records (RRs) that directly answer the question, containing the resolved data like IP addresses or mail server names.

4. **Authority**: Lists the resource records pointing to authoritative name servers for the domain, used to help resolve the query further if needed.

5. **Additional**: Provides extra information that may be useful for resolving the query, such as additional RRs not directly answering the question but related to the authority section.

And further details in the header:

DNS Header

Offsets	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
0	0	Transaction ID																Flags															
																		QR	OPCODE							AA	TC	RD	RA	Z		RCODE	
4	32	Number of questions																Number of answers															
8	64	Number of authority RRs																Number of additional RRs															

Source: Wikipedia

Field	Description
ID	A unique identifier for matching responses with queries.
QR (Query/Response)	Indicates if the packet is a query (0) or a response (1).
Opcode	Specifies the type of query (e.g., standard, inverse, or server status).
AA (Authoritative Answer)	Indicates if the response is from an authoritative name server.
TC (Truncation)	Indicates if the message was truncated due to size limits.
RD (Recursion Desired)	Requests that the server perform recursion to resolve the query.
RA (Recursion Available)	Indicates if the server supports recursion in the response.
Z	Reserved for future use, must be set to 0.
AD (Authenticated Data)	Indicates if the data has been authenticated by the server (DNSSEC).
CD (Checking Disabled)	Instructs the server to disable DNSSEC validation.
RCODE (Response Code)	Indicates the status of the response (e.g., no error, format error).
QDCOUNT (Question Count)	Number of entries in the Question section.
ANCOUNT (Answer Count)	Number of resource records in the Answer section.
NSCOUNT (Authority Count)	Number of resource records in the Authority section.
ARCOUNT (Additional Count)	Number of resource records in the Additional section.

Security aspects:

Any compromise to the DNS resolution system can badly impact security of the user. Example: If yourbank.com could be mapped to a malicious server, that impersonate your bank's usual look and feel, malicious actors might be able to deceive to give up your login and password. Which then they can use on the real bank website to transfer funds!

The DNS root server H-root is managed by U.S. Army Research Lab (ARL). Turns out naming can help us catch many illicit activities on the Internet.

DNS PTR records can help detecting malicious activity such as scanning and spams:

Detecting Malicious Activity with DNS Backscatter Over Time

Kensuke Fukuda John Heidemann Abdul Qadeer

***Abstract*—Network-wide activity is when one computer (the *originator*) touches many others (the *targets*). Motives for activity may be benign (mailing lists, CDNs, and research scanning), malicious (spammers and scanners for security vulnerabilities), or perhaps indeterminate (ad trackers). Knowledge of malicious activity may help anticipate attacks, and understanding benign activity may set a baseline or characterize growth. This paper identifies *DNS backscatter* as a new source of information about network-wide activity. Backscatter is the reverse DNS queries caused when targets or middleboxes automatically look up the domain name of the originator. Queries are visible to the authoritative DNS servers that handle reverse DNS. While the fraction of backscatter they see depends on the server's location in the DNS hierarchy, we show that activity that touches many targets appear even in sampled observations. We use information about the queriers to classify originator activity using machine-learning. Our algorithm has reasonable accuracy and precision (70–80%) as shown by data from three different organizations operating DNS servers at the root or country-level. Using this technique we examine nine months of activity from one authority to identify trends in scanning, identifying bursts corresponding to Heartbleed and broad and continuous scanning of ssh.**

does not generalize to network-wide activity. Darknets [38], [35], [56], [13], [14], [17] and honeypots (for example, [42]) are effective at understanding network-wide activity, but they miss targeted scans (scanning only Alexa top websites [17]), and new large darknets are unlikely given IPv4 full allocation and the huge IPv6 space. Search engines gather information about activity that appears in the public web, but information is unstructured and may be delayed by indexing [50]. (§ VII has detailed related work.)

This paper identifies a new source of information on network-wide activity: *DNS backscatter*, the reverse DNS queries triggered by such activity (see Figure 1 and § II). Activities of interest are those that touch many Internet devices, including malicious or potentially malicious activity such as spamming and scanning, as well as widespread services such as CDNs, software updates, and web crawling. These activities trigger *reverse DNS queries* as firewalls, middleboxes, and servers (*queriers*) resolve mapping of the IP address of the

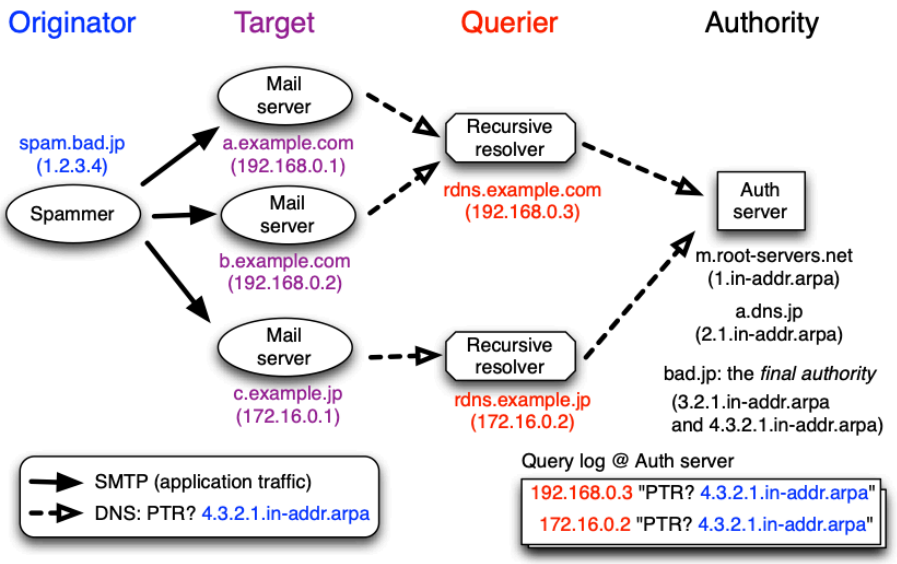


Fig. 1: The process behind a DNS backscatter sensor: an originator sends mail to targets, causing queries that are observed at the authority.

https://ant.isi.edu/~johnh/PAPERS/Fukuda17a.pdf

Homework (not graded):

(1) Do some DNS queries and capture their request and response packets using Wireshark. Match what you see in Wireshark to the output in nslookup/dig.

(2) Read section 2.4 on DNS from the book. There are many details we didn't get to in the class. For example, recursive and iterative query resolution.