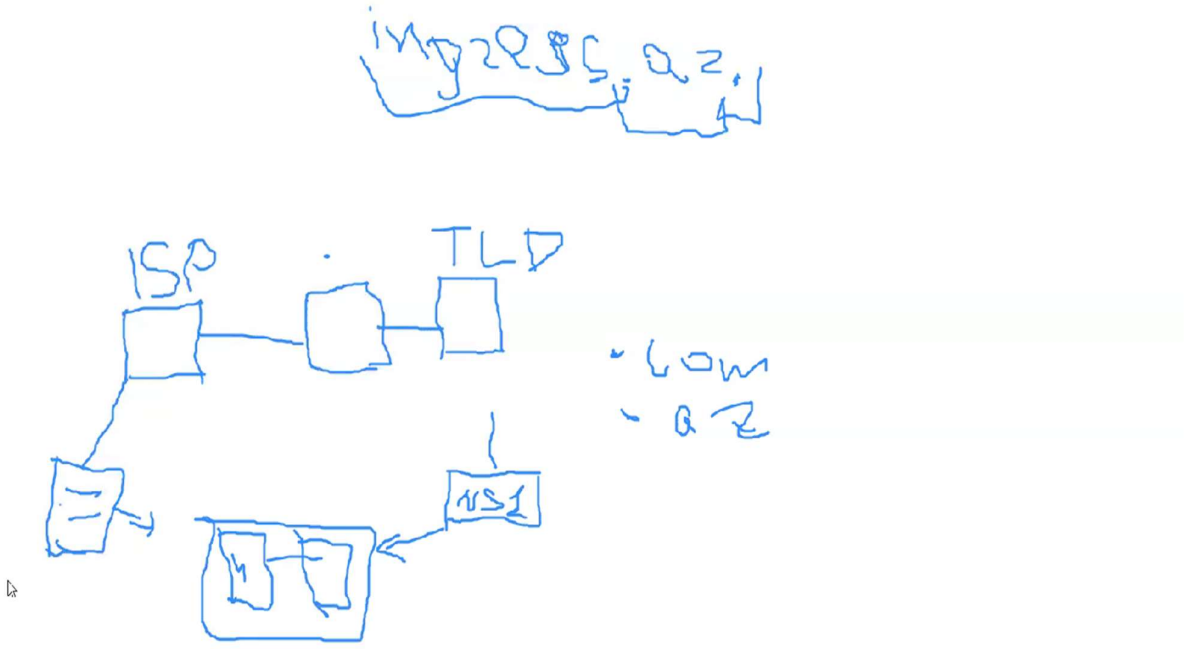
DNS

DNS nə üçündür?
Biz browserdə saytlara girmək üçün İP yazmalıyıq. Amma IP çox uzun olduğu üçün onu yadda saxlamaq olmur. Çünki rəqəmlər yadda saxlamaq çətindir. Buna görədə biz DNS istifadə edirik. DNS IP-ni ada, adıda IP-yə resolv edir.

DNS necə işləyir?
1. İlk olaraq browser-in cache-nə baxır. (TTL vaxtı qədər cache-də qalır.)
2. Daha sonra local host faylına baxır.
3. OS səviyyəsində cache baxır.
4. DNS server varsa ona baxır.
5. Daha sonra ISP-yə baxır.
6. 13 root DNS server-ə baxır. (Burada Top-Level-Domain məlumatlarını öyrənir.)
7. Name Server-ə yönləndirilir.



Biz burada Name Server-in Public IP-sini Domain aldığımız sayta qeyd edirik.

Təhlükəsizlik üçün master Name Server qurulur. Və bu global-a çıxarılmır. Bunun yerinə Slave Name Server qurulur, və global-a çıxarılır.

nslookup google.com

```
[root@localhost ~]# nslookup google.com
Server:         192.168.149.2
Address:        192.168.149.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.140.14
Name:   google.com
Address: 2a00:1450:4017:813::200e
```

dig yandex.ru

```
[root@localhost ~]# dig yandex.ru

; <<>> DiG 9.16.23-RH <<>> yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41581
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;yandex.ru.                     IN      A

;; ANSWER SECTION:
yandex.ru.              5       IN      A       5.255.255.70
yandex.ru.              5       IN      A       5.255.255.77
yandex.ru.              5       IN      A       77.88.55.88
yandex.ru.              5       IN      A       77.88.55.60

;; Query time: 8 msec
;; SERVER: 192.168.149.2#53(192.168.149.2)
;; WHEN: Wed Jan 17 20:36:29 +04 2024
;; MSG SIZE  rcvd: 102
```

dig +trace yandex.ru

```
[root@localhost ~]# dig +trace yandex.ru

; <<>> DiG 9.16.23-RH <<>> +trace yandex.ru
;; global options: +cmd
.                       5       IN      NS      j.root-servers.net.
.                       5       IN      NS      k.root-servers.net.
.                       5       IN      NS      l.root-servers.net.
.                       5       IN      NS      m.root-servers.net.
.                       5       IN      NS      a.root-servers.net.
.                       5       IN      NS      b.root-servers.net.
.                       5       IN      NS      c.root-servers.net.
.                       5       IN      NS      d.root-servers.net.
.                       5       IN      NS      e.root-servers.net.
.                       5       IN      NS      f.root-servers.net.
.                       5       IN      NS      g.root-servers.net.
.                       5       IN      NS      h.root-servers.net.
.                       5       IN      NS      i.root-servers.net.
.                       5       IN      RRSIG   NS 8 0 518400 20240130050000 20240117040000 309
```

```
ru.                     172800  IN      NS      a.dns.ripn.net.
ru.                     172800  IN      NS      f.dns.ripn.net.
ru.                     172800  IN      NS      b.dns.ripn.net.
ru.                     172800  IN      NS      d.dns.ripn.net.
ru.                     172800  IN      NS      e.dns.ripn.net.
ru.                     86400   IN      DS      18274 8 2 AB35D17D3F39EB42CEE14C6273247938D33EEEAA9F5CAA70B3858DBF 4B
D3E87B
ru.                     86400   IN      RRSIG   DS 8 1 86400 20240130050000 20240117040000 30903 . 3cdreVVXGcD3coCwbY
```

```
YANDEX.RU.              345600  IN      NS      ns1.yandex.RU.
YANDEX.RU.              345600  IN      NS      ns2.yandex.RU.
J20C0QKDHUA3CUMNKST289FF06U2SQ91.ru. 3600 IN NSEC3 1 1 0 - J21C11SHOOTMOEQKPRM91C8AGL4886M6 NS SOA RRSIG DNSKEY NSEC3
PARAM
J20C0QKDHUA3CUMNKST289FF06U2SQ91.ru. 3600 IN RRSIG NSEC3 8 2 3600 20240127131355 20231215181945 44301 ru. LCkuUEjOZa6
VmLNRplmlyS8dPoQ95vLWZZKXTAclGhnpkYVcvZeJMuiI JGkF92VYfAJTZ/i9vAj86qZAqRur6SdjtzjrKLiAqqJbcmp7vk5wsovd V6LoFcgyu3NlF/
otqVMScVZCeNVSZtRk4TmZYC828qfPrX0j+LTy3tP5 rwE=
VJH3PPLST1U7RJRUM4A0TH2P9E83M9P8.ru. 3600 IN NSEC3 1 1 0 - VJOEGEO1PD6MC6EJ56UVD2GD4HB9Q7DR NS DS RRSIG
VJH3PPLST1U7RJRUM4A0TH2P9E83M9P8.ru. 3600 IN RRSIG NSEC3 8 2 3600 20240215192320 20240116182007 44301 ru. tFEyAs1YXW/
FTjjwZ5COmj5rXIaG27EMrfyfU+nw9eyFytv1TiGmAGLg Tm+jw72neb2izriq335Zvn3Hek0Am5kaPdJo5nAuduKeIr8GCXa/beRz GuKTpHZXdq7OKO
VXaxPJjb0jDpjO3oovYHN+U1TiHdO+KNUrh/F0V9NN 0VI=
;; Received 669 bytes from 193.232.142.17#53(e.dns.ripn.net) in 112 ms

yandex.ru.              300     IN      A       5.255.255.70
yandex.ru.              300     IN      A       77.88.55.60
yandex.ru.              300     IN      A       5.255.255.77
yandex.ru.              300     IN      A       77.88.55.88
yandex.ru.              604800  IN      NS      ns2.yandex.ru.
yandex.ru.              604800  IN      NS      ns1.yandex.ru.
;; Received 254 bytes from 213.180.193.1#53(ns1.yandex.RU) in 68 ms
```

dig -x 8.8.8.8

```
[root@localhost ~]# dig -x 8.8.8.8

; <<>> DiG 9.16.23-RH <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   5       IN      PTR     dns.google.

;; Query time: 11 msec
;; SERVER: 192.168.149.2#53(192.168.149.2)
;; WHEN: Wed Jan 17 20:39:26 +04 2024
;; MSG SIZE  rcvd: 73
```

yum instal bind bind-utils
systemctl status named (distroya görə dəyişkənlik göstərir)
vim /etc/named.conf

```
        allow-query     { localhost; any;};
```

Allow-query kimlərdən gələcək olan requestləri resolve edəcəyini göstərir. Any yazıldığı üçün istənilən hostdan gələn request resolve ediləcək.

```
        recursion yes;
```

Recursion – Əgər no olarsa, "məndə əgər A recordu varsa cavab qaytar, əgər yoxdusa ilişib qalır".
Əgər yes olarsa DNS flow recursion sayılır.
Forwarder – Əgər məndə yoxdursa təyin olunmuş server-ə gedir. Məsələn 8.8.8.8 .

Forward

```
zone "ingress.local." IN {
        type master;
        file "ingress-forward.local.db";
        allow-update {none;};
};
```

Ingress.local. - domain
type - master
file – default olaraq /var/named altında olur
allow-update – none – dinamik olaraq heç bir yerdən update alma

```
[root@localhost ~]# named-checkconf
```

Servisin check olunması üçün istifadə edilir.

```
[root@localhost named]# named-checkzone ingress.local. ingress-forward.local.db
zone ingress.local/IN: loaded serial 0
OK
```

Ingress.local. domain-ə aid ingress-forward.local.db zone-sini kontrol elə.

chown named:named ingress-forward.local.db
getenforce
setenforce 0
firewall-cmd --add-service=dns –permanent
firewall-cmd –reload
nmcli connection modify ens160 ipv4.dns 192.168.149.129
systemctl restart NetworkManager

```
$TTL 3H
@       IN SOA  @ ingress.local. (
                                        00      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
master IN       A       192.168.149.129
slave IN        A       192.168.149.135
test IN         A       192.168.149.192
```

```
[root@localhost named]# nslookup test.ingress.local
Server:         192.168.149.129
Address:        192.168.149.129#53

Name:   test.ingress.local
Address: 192.168.149.192
```

Reverse

```
zone "149.168.192.in-addr.arpa." IN {
        type master;
        file "192.168.149.zone";
        forwarders {};
};
```

```
$TTL 3H
@       IN SOA  @ ingress.local. (
                002         ; serial
                1M          ; refresh
                1H          ; retry
                1W          ; expire
                3H )        ; minimum
;       owner   TTL     CL      type    RDATA
                600     IN      NS      ns1.ingress.local.

135     IN      PTR     slave
129     IN      PTR     master
```

```
[root@vm1]/var/named/zone# named-checkzone 1.168.192.in-addr.arpa 192.168.1.zone
zone 1.168.192.in-addr.arpa/IN: loaded serial 2
OK
[root@vm1]/var/named/zone#
```

systemctl restart named

dig -x 192.168.124.135

Slave

Add to Master Bind (slave-ip)

```
        allow-transfer {192.168.149.136; };
```

Forward

```
zone "ingress.local." IN {
        type slave;
        file "ingress.local.db";
        masters { 192.168.149.129; };
        masterfile-format text;
};
```

Reverse

```
zone "149.168.192.in-addr.arpa." IN {
        type slave;
        file "192.168.149.zone";
        masters {192.168.149.129; };
        masterfile-format text;
};
```

Automatic dəyişiklikləri qəbul etməsi üçün Master Bind-a bunları əlavə edirik. (slave-ip)

```
        notify yes;
        also-notify {192.168.149.136;};
```

Slave Bind-a bunu əlavə edirik. (master-ip)

```
    allow-notify {192.168.149.129;};
```