Domain Name System (DNS)

Md. Mahedi Hasan
Technology Specialist (Innovation), BdREN, UGC
mahedi@bdren.net.bd

Index

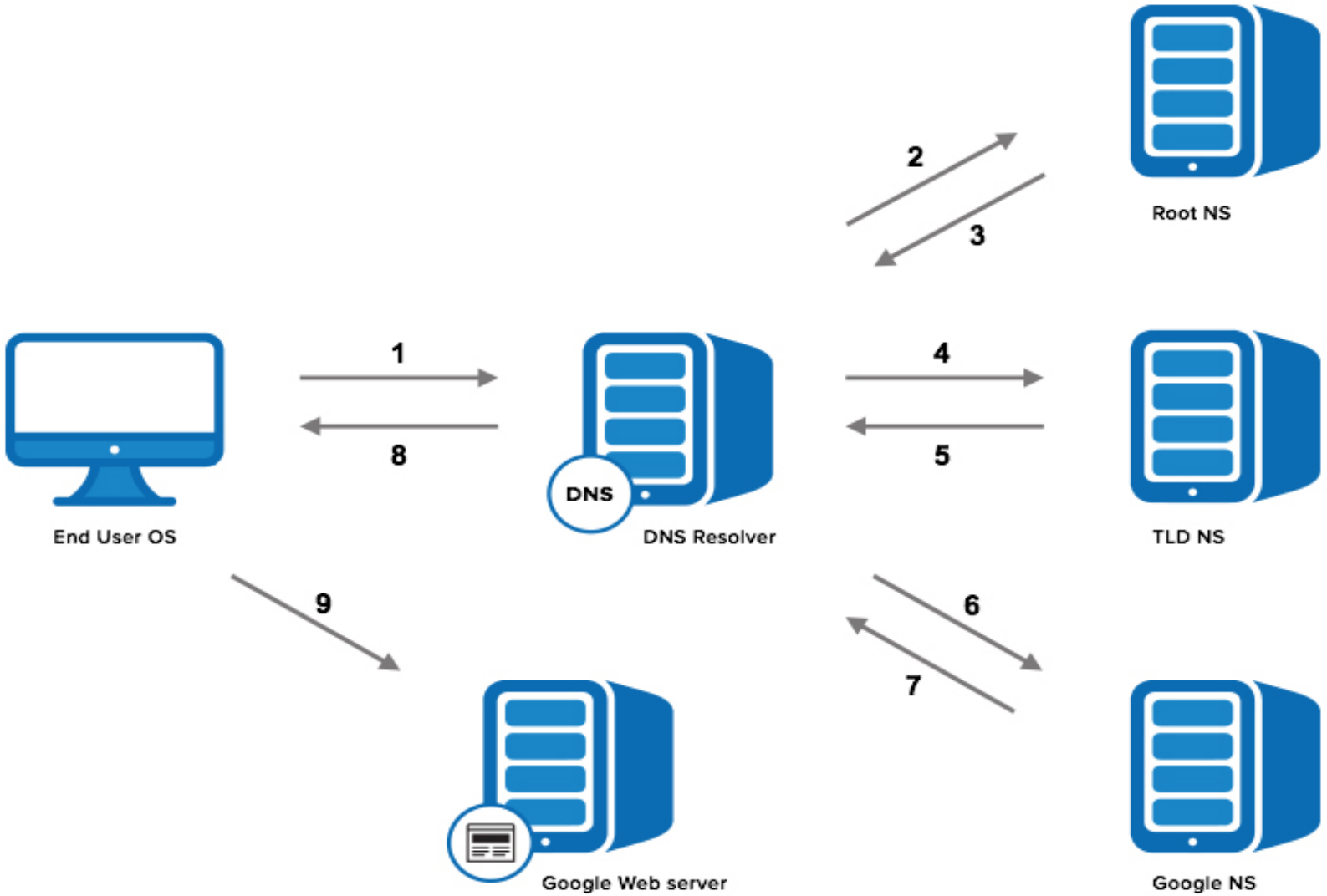
Overview of DNS

- A Domain Name System (DNS) is a distributed hierarchical system.
- It’s maintain a directory of domain names and translate them to Internet Protocol (IP) addresses.
- Inform which are the official Name Servers for a particular Domain.
- The DNS is divided into sections called zones.
- Each zone has name servers that respond to the queries belonging to their zones.
- Inform mail servers which mail servers will accept and process for a particular Domain.

A Brief History of Name Servers

- The Open Systems Interconnect (OSI) Model, developed by the International Organization for Standardization (ISO—www.iso.org), defined Address/Name Translation services at the Transport Layer (Layer 4) when initially published in 1978.
- NetBIOS provided the NetBIOS Name Server (NBNS) when originally defined in 1984, which later transformed into Microsoft's Windows Internet Naming Service (WINS).
- The first ARPANET (the network that adapted into the Internet) RFC, the quaintly named Request For Comments that document and standardize the Internet, on the concept of domain names dates from 1981 (RFC 799),
- And the definitive specifications for the Internet's Domain Name System as we know it today were published in 1987 (RFC 1034 and RFC 1035).

How DNS Works



DNS Components

- **DNS resolver —** Resides on the client side of the DNS. When a user sends a hostname request, the resolver sends a DNS query request to the name servers to request the hostname's IP address.
- **Name servers —** Processes the DNS query requests received from the DNS resolver and returns the IP address to the resolver.
- **Resource records —** Data elements that define the basic structure and content of the DNS.

Categories of DNS Server

- Based on Functionality
  - Authoritative-Only DNS Servers
  - Caching DNS Server
  - Forwarding DNS Server
- Relational Differences
  - Primary and Slave Servers
  - Public vs. Private Servers

Authoritative-Only DNS Servers

- An authoritative-only DNS server is a server that only concerns itself with answering the queries for the zones that it is responsible for.
- Since it does not help resolve queries for outside zones, it is generally very fast and can handle many requests efficiently.
- Authoritative-only servers have the following properties:
  - Very fast at responding to queries for zones it controls
  - Will not respond to recursive queries
  - Does not cache query results.

Caching DNS Server

- A caching DNS server is a server that handles recursive requests from clients.
- Almost every DNS server that the operating system's stub resolver will contact will be a caching DNS server.
- A caching DNS server has the following properties:
  - Access to the entire range of public DNS data
  - Ability to spoon-feed data to dumb clients
  - Maintains a cache of recently requested data.

Forwarding DNS Server

- A alternative way to developing a cache for client machines is through the use of a forwarding DNS server.
- It's simply passes all requests to another DNS server with recursive capabilities (such as a caching DNS server).
- A forwarding DNS server has the following properties:
  - The ability to handle recursive requests without performing recursion itself
  - Provide a local cache at a closer network location
  - Increases flexibility in defining local domain space

Primary and Slave Servers

- Both master and slave servers are authoritative for the zones they handle.
- The master does not have any more power over the zones than the slave. The only differentiating factor between a master and a slave server is where they read their zone files from.
- A master server reads its zone files from files on the system's disk.
- The slave server receives the zones through a zone transfer from one of the master servers for the zone.
- DNS zones usually have at least two name servers.
- Any zone responsible for an internet routable zone must have at least two name servers.

Public vs. Private Servers

- An organization might maintain an externally available authoritative-only DNS server to handle public DNS queries for the domains and zones that it handles.
- For its internal users, the organization might use a separate DNS server that contains the authoritative information that the public DNS provides, as well as additional information about internal hosts and services.
- It might also provide additional features, such as recursion and caching for its internal clients.

Scenario

- Primary DNS Server:
  - Hostname : **ns1**
  - Domain Name: **bdren.net.bd**
  - IP Address : **192.168.1.5**
- Secondary DNS Server:
  - Hostname : **ns2**
  - Domain Name: **bdren.net.bd**
  - IP Address : **192.168.1.10**

Configure Firewall

```
# vim /etc/selinux/config
```

Set SELINUX=disabled and restart

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


:x
# reboot
```

Configure Hostname

- To see current hostname:

```
[root@localhost ~]# hostname
localhost.localdomain
```

- To changed hostname:
  - Step-1:

```
[root@localhost ~]# vim /etc/hostname
ns1.bdren.net.bd

:x


[root@localhost ~]# logout  [to see effect logout and login your system]
 Login:  [give your credential and login the system]
[root@ns1 ~]#
```

! Note: “ns1” yellow marked will be replaced with as your scenario

Configure Hostname Cont.

- Step-2: [Changed `/ete/hosts` file like following]

```
[root@ns1 ~]# vim /etc/hosts
127.0.0.1       localhost.localdomain           localhost
192.168.1.5     ns1.bdren.net.bd                ns1

:x
```

- Give following command for testing correctness:

```
root@ns1 ~]# hostname
Ns1.bdren.net.bd
root@ns1 ~]# hostname -d
bdren.net.bd
root@ns1 ~]# hostname -f
ns1.bdren.net.bd
```

! Note: “ns1” yellow marked will be replaced with as your scenario

Installing Required Software

To checked installed bind software

```
root@ns1 ~]# rpm -qa|grep bind
bind-9.8.2-0.17.rc1.el6_4.6.x86_64
bind-libs-9.8.2-0.17.rc1.el6_4.6.x86_64
bind-utils-9.8.2-0.17.rc1.el6_4.6.x86_64
```

If not installed, installing them using following command:

```
[root@ns1 ~]# yum install -y bind bind-utils
```

- Create a backup for original file

```
[root@ns1 ~]# cd /etc/
[root@ns1 etc]# cp named.conf named.conf.ori
```

Configuration of Primary DNS

- Step-1: Create a backup for original file and changed in `/etc/named.conf` file like following:

```
[root@ns1 ~]# vim /etc/named.conf
options {
        listen-on port 53 { 192.168.1.5; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 192.168.1.0/24; };
         recursion yes;

         dnssec-enable yes;
        dnssec-validation yes;
        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
        managed-keys-directory "/var/named/dynamic";
        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};
```

Configuration of Primary DNS Cont.

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

// Adding forward zone
zone “bdren.net.bd" IN {
        type master;
        file “db.bdren.net.bd";
        allow-update { none; };
};
```

Configuration of Primary DNS Cont.

```
// Adding Reverse zone

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "db.1.168.192.in-addr.arpa";
        allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

! Note: Here yellow marked texts are add or replace with default text

Configuration of Primary DNS Cont.

- Zone files are contained in `/var/named/` directory

```
[root@ns1 ~]# cd /var/named/
[root@ns1 named]# ls -la
drwxr-x---.  5 root  named 4096 Jul 24 17:04 .
drwxr-xr-x. 23 root  root  4096 Jul 24 17:04 ..
drwxrwx---.  2 named named    6 Jul  5 06:15 data
drwxrwx---.  2 named named    6 Jul  5 06:15 dynamic
-rw-r-----.  1 root  named 2281 May 22 05:51 named.ca
-rw-r-----.  1 root  named  152 Dec 15  2009 named.empty
-rw-r-----.  1 root  named  152 Jun 21  2007 named.localhost
-rw-r-----.  1 root  named  168 Dec 15  2009 named.loopback
drwxrwx---.  2 named named    6 Jul  5 06:15 slaves
```

- Copy existing zone file for sample configuration with your given name in named.conf file like following:

```
[root@ns1 named]# cp named.localhost db.bdren.net.bd
[root@ns1 named]# cp named.loopback db.1.168.192.in-addr.arpa
```

Configure Forward Zone file

- Now open your forward zone file changed the options like following:

```
[root@ns1 named]# vim db.bdren.net.bd
$TTL 1D
@       IN SOA  ns1.bdren.net.bd. root.bdren.net.bd. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns1.bdren.net.bd.
        A       192.168.1.5
        AAAA    ::1
ns1                 IN      A               192.168.1.5
mail                IN      A               192.168.1.5
bdren.net.bd.       IN      MX      10      mail.bdren.net.bd
www                 IN      CNAME           ns1.bdren.net.bd.
ftp                 IN      A               192.168.1.50
smtp                IN      A               210.20.30.5
```

Configure Reverse Zone file

- Now open your Reverse zone file changed the options like following:

```
[root@ns1 named]# vim db.1.168.192.in-addr.arpa
$TTL 1D
@       IN SOA  ns1.bdren.net.bd. root.bdren.net.bd. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns1.bdren.net.bd.
        A       192.168.1.5
        AAAA    ::1
5       IN      PTR     ns1.bdren.net.bd.
50      IN      PTR     ftp.bdren.net.bd.
```

Starting service and test from clients

- At first checked your configuration and zone file like following:

```
[root@ns1 named]# named-checkconf -z /etc/named.conf
zone localhost.localdomain/IN: loaded serial 0
zone localhost/IN: loaded serial 0

[root@ns1 named]# named-checkzone zone db.bdren.net.bd
zone zone/IN: loaded serial 0
OK

[root@ns1 named]# named-checkzone zone db.110.168.192.in-addr.arpa
zone zone/IN: loaded serial 0
OK
```

- If shown not OK then you need to checked your zone file, it has something wrong in syntax, correct and check again.
- Changed group ownership:

```
[root@ns1 named]# chgrp named db.bdren.net.bd
[root@ns1 named]# chgrp named db.1.168.192.in-addr.arpa
```

Starting service and test from clients cont.

- To start service and ensure start this service at startup run following command:

```
[root@ns1 named]# systemctl restart  named.service

[root@ns1 named]# systemctl enable named.service
ln -s '/usr/lib/systemd/system/named.service' '/etc/systemd/system/multi-user.target.wants/named.service'
```

- Test from Linux clients you need to add name server address in `/ete/reslov.conf` file:

```
[root@ns1 named]# vim /ete/reslov.conf
search bdren.net.bd
nameserver 192.168.1.5

:x
[root@ns1 named]#
```

Starting service and test from clients cont.

```
[root@ns1 named]# nslookup
> bdren.net.bd
Server:             192.168.1.5
Address:     192.168.1.5#53

Name:  bdren.net.bd
Address: 192.168.1.5
> www
Server:             192.168.1.5
Address:     192.168.1.5#53

www.bdren.net.bd    canonical name = ns1.bdren.net.bd.

Name:  ns1.bdren.net.bd
Address: 192.168.1.5
>
```

Configuration of Secondary DNS

- At first you have to install software, configure firewall, hostname and FQDN like same as primary DNS server by following previous slide
- Step-1: Changed in Primary DNS servers /etc/named.conf file in only zone section like following:

```
// Adding forward zone
zone “bdnog.org" IN {
        type master;
        file “db.bdren.net.bd";
        allow-update {192.168.1.10; };
};

// Adding Reverse zone

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file “db.110.168.192.in-addr.arpa";
        allow-update {192.168.1.10; };
};
```

Configuration of Secondary DNS Cont.

- Step-2: Changed `/etc/named.conf` in ns2 like following:

```
[root@ns2 ~]# vim /etc/named.conf
options {
        listen-on port 53 { 192.168.1.10; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 192.168.1.0/24;};
        recursion yes;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
        managed-keys-directory "/var/named/dynamic";
};
```

Configuration of Secondary DNS Cont.

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

// Adding forward zone
zone “bdren.net.bd" IN {
       type slave;
       master { 192.168.1.5; };
       file "slaves/db.bdren.net.bd";
};
```

Configuration of Secondary DNS Cont.

```
// Adding Reverse zone

zone "1.168.192.in-addr.arpa" IN {
        type slave;
       master { 192.168.1.5; };
        file "slaves/db.1.168.192.in-addr.arpa";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

:x
```

Starting service and test from clients

- To start service and ensure start this service at startup run following command:

```
[root@ns1 named]# systemctl restart  named.service

[root@ns1 named]# systemctl enable named.service
ln -s '/usr/lib/systemd/system/named.service' '/etc/systemd/system/multi-user.target.wants/named.service'
[root@ns2 ~]# cd /var/named/slaves/
[root@ns2 ~]# ls -la
-rw-r-----   1 root  named  421 May 27 21:37 db.bdren.net.bd
-rw-r-----.  1 root  named  292 May 13 13:58 db.110.168.192.in-addr.arpa
```

- Test from Linux clients you need to add name server address in `/ete/reslov.conf` file:

```
[root@ns2 named]# vim /ete/reslov.conf
search example.com
nameserver 192.168.1.10

:x
[root@ns2 named]#
```

Starting service and test from clients

```
[root@ns2 named]# nslookup
> bdren.net.bd
Server:             192.168.1.10
Address:     192.168.1.10#53

Name:  bdren.net.bd
Address: 192.168.1.5
> www
Server:             192.168.1.10
Address:     192.168.1.10#53

www.bdren.net.bd    canonical name = ns1.bdren.net.bd.

Name:  ns1.bdren.net.bd
Address: 192.168.1.5
> 192.168.1.5
Server:             192.168.1.10
Address:     192.168.1.10#53

5.1.168.192.in-addr.arpa   name = ns1.bdren.net.bd.
```

Thank You

?