Network Services Introduction

Domain Name System (DNS) with ISC BIND

Dr. Horia V. Corcalciuc
Horia Hulubei National Institute for R&D in Physics and Nuclear Engineering (IFIN-HH)

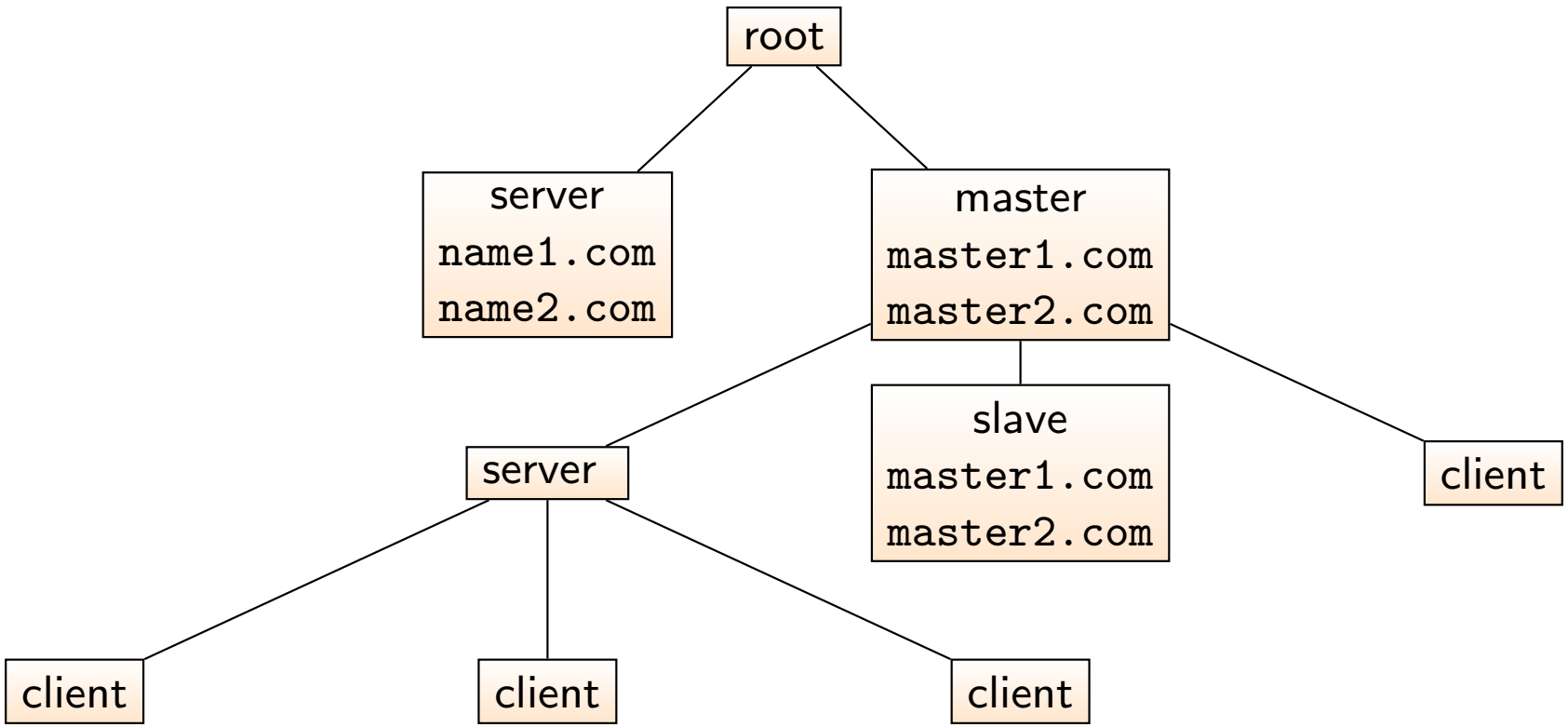
April 13, 2016

Introduction

- **Domain name servers** are responsible for **resolving** IP addresses to names (**reverse**) or domain names to IP addresses (**forward**).
- The resolution occurs on the **application layer** where domain name servers commonly bind to **UDP** port **53** and wait for requests - the related Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) work on the **network layer**.
- The domain name or reverse IP address block for which a domain name server is responsible is often called a **zone**.

IFIN-HH

Zones Managed by Domain Name Servers



IFIN-HH

Questions and Statements

- *What's the DNS of [...]?* - this ambiguous question most likely ask what the **domain name** is supposed to be. I always ask the follow-up question: *You mean the* **domain name** *or the* **DNS server's IP address***?*
- *What are the DNS for [...]?* - this ambiguous question probably asks what the IP addresses of the **domain name server** are.
- *The DNS is not set for [...]* - most likely similar to the former and refers to the IP addresses of the **domain name server** not being set on a computer.

Software

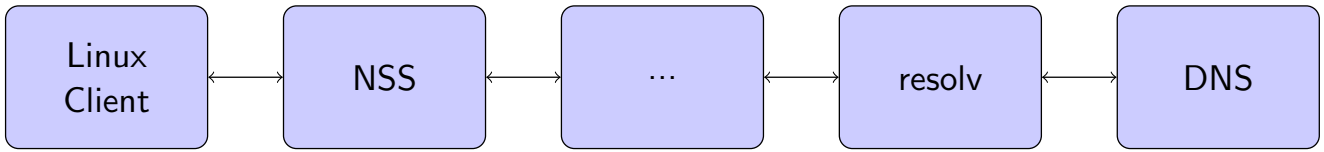
The most common domain name servers are:

- ISC BIND - covers most Unix systems (Linux, BSD, etc...) and is ported to Windows as well.
- Microsoft Domain Name Server - is included in Windows Server variants.

along with some hybrids such as:

- pdnsd - a caching DNS **forwarder**.
- dnsmasq - a **forwarding** DNS server and a DHCP server bundled together in the same package.

Linux



In order to resolve a hostname to an IP address on a Linux / BSD system, the following rough procedure takes place:

1. The `nsswitch.conf` file is queried in order to determine the order of the resolution:

nsswitch.conf

```
hosts:          files dns mdns4
```

2. The `/etc/hosts` file is queried in order to check if the hostname resolves to an IP address.
3. The `/etc/resolv.conf` file is read in order to determine the IP address of the name server:

resolv.conf

```
nameserver 194.102.58.3
```

FIN-HH

The Hosts File

/etc/hosts

```
127.0.0.1       localhost
127.0.1.1       tandem.nipne.ro
```

- The hosts file is located at:
  - On Linux at `/etc/` and called `hosts`.
  - On Windows at `%windir%` called `lmhosts`.
- The hosts file contain IP addresses separated by a space and the hostname that the IP address resolves to.
- The hosts file can sometimes be used to optimise very frequently accessed servers in order to offload some work from the domain name server.
- Some low-level API calls will bypass the hosts file entirely so it should not be relied upon.

The Resolv File

/etc/resolv.conf

```
domain nipne.ro
search nipne.ro.
nameserver 194.102.58.3
nameserver 8.8.8.8
```

- The **nameserver** option specifies the IP address of a domain name server to be queried.
- All configured **nameserver** entires will be queried in turn depending on whether a connection could be established.
- The **domain** option specifies that queries for names within the domain can use short names instead of Fully Qualified Domain Names (FQDN).
- The **search** list contains the domain names to search.

IFIN-HH

Introduction

- ISC BIND is the standard fully-featured domain name server software for Unix operating systems that can perform both forward and reverse domain resolutions.
- ISC BIND uses files in order to configure the domain name server itself as well as **zone files** for each configured domain name.
- Compared to other hybrid domain names, ISC BIND can act as a caching domain name server but its cache is dispelled once the daemon restarts.

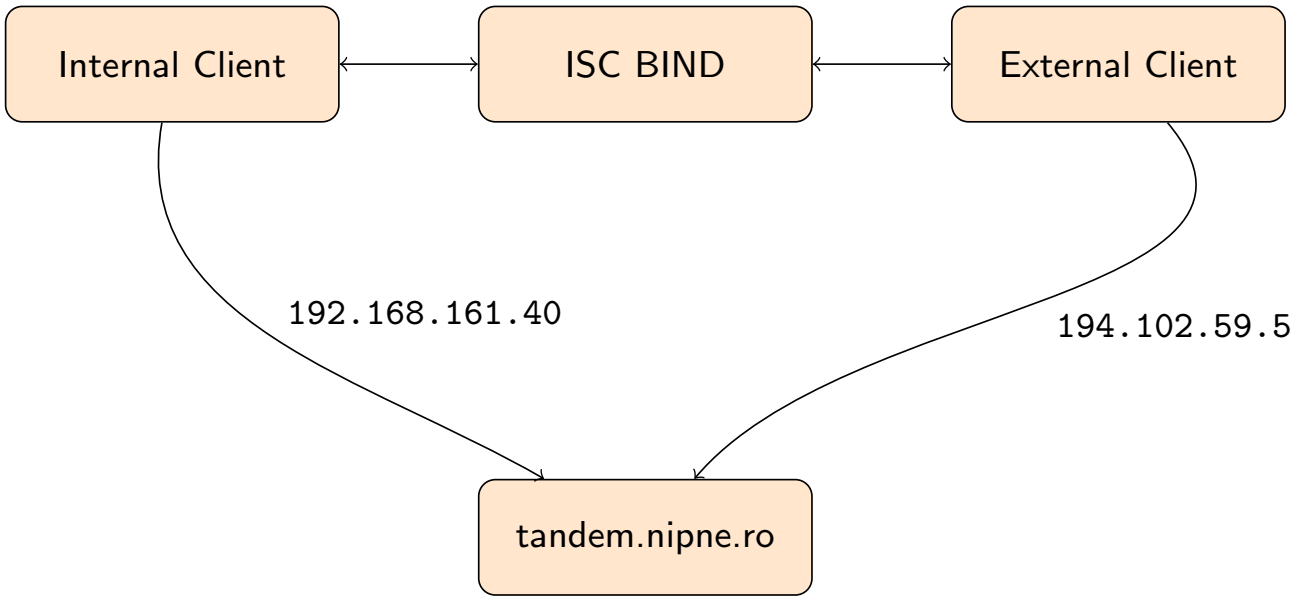
Configuring Views

Configuring Domain Name System Views

```
view "internal" {
    match-clients {
        192.168.1.0/24;
    };

    // internal view zones
};

view "external" {
    match-clients { any; };

    // external view zones
};
```

- The domain name system can be partitioned such that clients from a specified network will see only certain zone declarations.
- When the domain name server loads it will scan the views and create the partitions accordingly based on the `match-clients` directive.

Usefulness of Views



The IP address of the server `tandem.nipne.ro` can be resolved to two different IP addresses depending on whether the client is an internal view or an external view.

IFIN-HH

Declaring Zones

Zone Declarations

```
view "internal" {
    match-clients { 192.168.1.0/24; };

    // cache
    zone "." IN {
        type hint;
        file "db.cache";
    };
};

view "external" {
    match-clients { any; };

    // forward zone declaration
    zone "tandem.nipne.ro " IN {
        type master;
        file "zones/tandem.nipne.ro";
    };

    // reverse zone declaration
    zone "59.102.194.in-addr.arpa" {
        type master;
        file "zones/194.102.59";
    };
};
```

Forward Zones

Forward Zone Declaration

```
// forward zone declaration
zone "tandem.nipne.ro " IN {
    type master;
    file "zones/tandem.nipne.ro";
};
```

- The configuration in this example declares a zone `tandem.nipne.ro` for which sub-domains of `tandem.nipne.ro` will be managed.
- The zone file where the sub-domains will be declared will be stored at `zones/tandem.nipne.ro`.
- By adding `master` as the `type` declares the current domain name server to be the master for the `tandem.nipne.ro` zone.

Reverse Zones

Reverse Zone Declaration

```
// reverse zone declaration
zone "59.102.194.in-addr.arpa" {
    type master;
    file "zones/194.102.59";
};
```

- The configuration declares a reverse zone for `194.102.59` where all the IP addresses under `194.102.59` (`194.102.59.1`, `194.102.59.2`, ...) can be given a domain name.
- Note that the syntax is to write the IP address in reverse `59.102.194` and postfix the result with `.in-addr.arpa`.
- The zone file where the IP address to domain name mappings will be listed is declared to be at `zones/194.102.59`.

Reverse Zone File

Reverse Zone File

```
$ORIGIN .
$TTL 259200     ; 3 days
59.102.194.in-addr.arpa   IN SOA  tandem.nipne.ro. root.tandem.nipne.ro. (
                                  200517517  ; serial
                                  28800      ; refresh (8 hours)
                                  7200       ; retry (2 hours)
                                  2419200    ; expire (4 weeks)
                                  86400      ; minimum (1 day)
                                  )
                          NS      tandem.nipne.ro.
$ORIGIN 59.102.194.in-addr.arpa.
5                         PTR     tandem.nipne.ro.
10                        PTR     webmail.tandem.nipne.ro.
7                         PTR     support.tandem.nipne.ro.
```

- The **reverse zone file** for an ISC BIND DNS server hosted on `tandem.nipne.ro` maps IP addresses to domain names using `PTR` records.
- The `NS` record specifies **the DNS server** for this zone - in this case it is set to `tandem.nipne.ro` which will most likely resolve to `194.102.59.5` due to the first pointer.

IFIN-HH

Forward Zone File

Forward Zone File

```
$ORIGIN .
$TTL 259200     ; 3 days
tandem.nipne.ro.    IN SOA  tandem.nipne.ro. root.tandem.nipne.ro. (
                                200517518  ; serial
                                28800      ; refresh (8 hours)
                                7200       ; retry (2 hours)
                                2419200    ; expire (4 weeks)
                                86400      ; minimum (1 day)
                                )

                              NS      tandem.nipne.ro.
tandem.nipne.ro.              A     194.102.59.5

; A records with substitution for sub-domains not ending in dot
$ORIGIN tandem.nipne.ro.
webmail                       A     194.102.59.10
support                       A     194.102.59.7
```

- The **forward zone file** maps domain names (sub-domain names) to IP addresses using records - in this case `A` records and name server `NS` records.
- In case a sub-domain is not specified as a fully-qualified domain name (FQDN) then the `$ORIGIN` will be postfixed.

The PTR Record

Pointer Record

```
5                       PTR     tandem.nipne.ro.
```

- The pointer record PTR is mostly used for reverse domain name mapping and it makes the DNS server stop processing and return the name that the pointer points to.

The A and AAAA Records

IPv4 Address Record

```
webmail                         A       194.102.59.10
```

- The IPv4 address record A maps a domain name to an IPv4 address.

IPv6 Address Record

```
webmail                          AAAA   fdda:9ba5:12:8::2f
```

- The IPv6 address record AAAA maps a domain name to an IPv6 address.

IFIN-HH

The MX Record

Mail Exchange Record

```
tandem.nipne.ro.                MX 10     mail1.tandem.nipne.ro.
                                MX 20     mail2.tandem.nipne.ro.

$ORIGIN tandem.nipne.ro.
mail1                       A 194.102.59.80
mail2                       A 194.102.59.90
```

- The mail exchange record MX specifies the mail servers responsible for processing mail for the current domain.
- The MX record can be followed by a number (1 in this example) representing the priority of the mail server compared to other declared mail-servers.

IFIN-HH

The CNAME Record

Canonical Name Record

```
tandem2.nipne.ro.        CNAME   tandem.nipne.ro.
tandem.nipne.ro.         A       194.102.59.10
```

- The canonical name record CNAME creates an alias from a domain name to a different domain name. When a CNAME record is encountered, DNS resolution searches for the alias in the domain name system.
- CNAME records should always point to a domain name and not an IP Address.
- It is entirely possible to have an alias chain where one record points to another record that points to another record, and so on but this should be avoided due to the lack of efficiency.

The TXT Record

Text Record

```
tandem.nipne.ro.          TXT       "Serverul Grupului Tandem"
```

- The text record TXT was meant to store descriptive data about a domain name however it is recently used to store paramters for applications querying the domain.

Changing Records

- The procedure for changing zone files is as follows:
  1. Stop the name-server.
  2. Edit the zone file.
  3. Increment the serial in the zone file.
  4. Start the name-server.
- The reason for having to stop the domain name server temporarily is due to extra complications that may appear due to DDNS in case it is configured.
- The serial should be incremented every time the zone file is changed because it is used by other name servers to check how recent the zone is.

Tools

Unix systems come with administration tools that can be used to debug domain name servers:

- `nslookup` can be used on a Linux system in order to resolve a domain name to its IP address.
- `host` can be used on a Linux system in order to perform a reverse-lookup of an IP address.

However the most notable tool is `dig` that allows you to perform all the above an much more. You can consult the manual pages on any Unix system by typing:

Command-Line Manual

```
man dig
```

Extensions

There are many Domain Name System extensions that can be implemented using ISC BIND that were not covered:

- Dynamic DNS (DDNS) - combining ISC DHCP and ISC BIND together such that clients requesting IP addresses from the DHCP server will make the DHCP server create a hostname for that machine using ISC BIND.
- DNSSEC - secure DNS in order to work around spoofing and to ensure the legitimacy of domain name servers.
- SPF and DKIM - both are methods to further check the legitimacy of mail servers by tying together a domain name server and the mail-server.