DNS & IPV6

Francisco J. Obispo
fobispo@gmail.com

Director de Operaciones y Red Académica
Fundación Centro Nacional de Innovación Tecnológica
http://www.cenit.gob.ve
Caracas - Venezuela

Topics

* Importance of DNS in IPv6

* Server configuration

* Client Configuration

* Resource Records

IMPORTANCE OF DNS

Importance of DNS

Ease of use

www.nic.ve

⬇

150.188.229.4
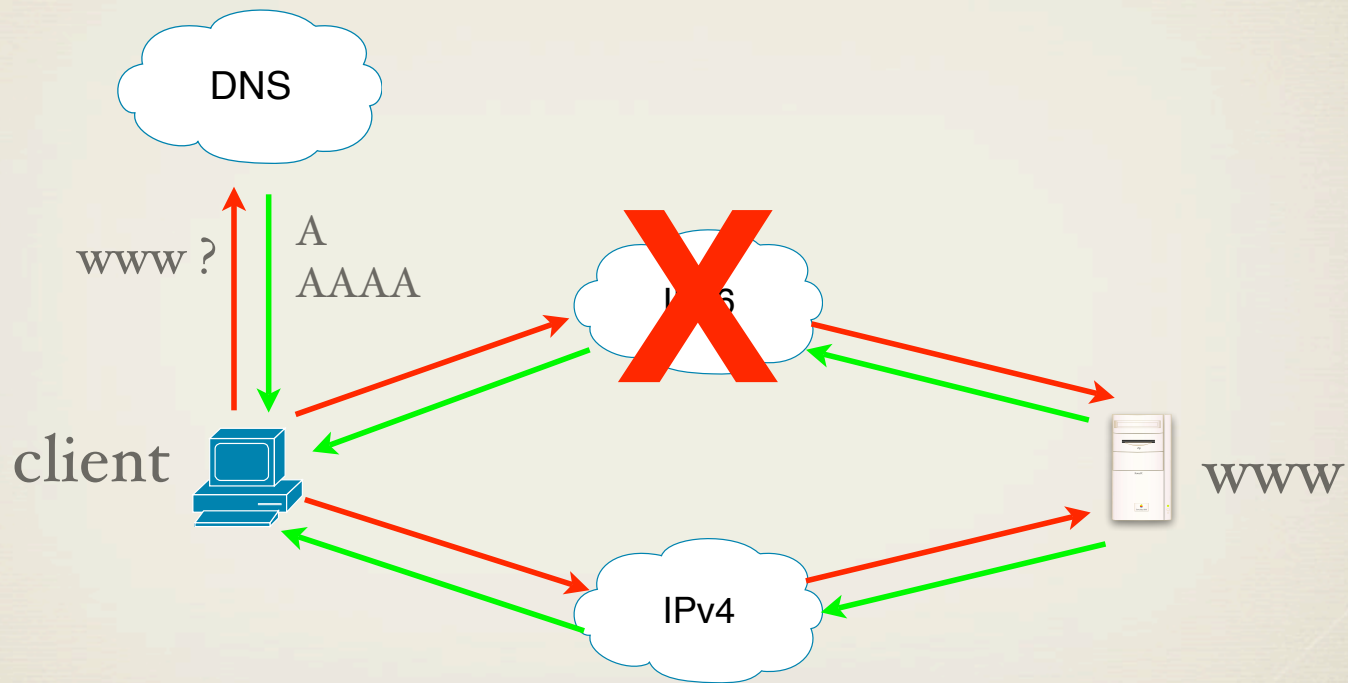
2001:1338::1:20d:56ff:febb:2865

Importance of DNS

Transparency

* Host will ask for both A and AAA RRs and will try IPv6 first

* If its unable to connect using IPv6, will fallback to IPv4

Importance of DNS

Transparency

Importance of DNS

Transparency... not perfection

✳ What happens if there is bad connectivity to the IPv6 Internet ?

Slower connections, compared to the IPv4 alternative

✳ What happens if there is "NO" connectivity to the IPv6 Internet ?

User has to wait for a timeout, which is worst than connecting without trying for IPv6

SERVER CONFIGURATION

* focused on ISC's BIND 9

Server Configuration

Issues regarding the server

✳ IPv6 Transport

   The server does not need IPv6 transport in order to serve IPv6 Resource Records. This is only needed to serve IPv6 Requests

✳ Support to IPv6 Resource Records

Server Configuration

Objectives

✳ Configure a BIND9 based DNS server

✳ Run the server in a chroot() jail

✳ Support IPv6 transport

✳ Manage IPv6 Resource Records

Server Configuration

Ingredients...

✳ Linux Debian or any other UNIX like OS

✳ Latest copy of ISC's BIND 9
http://ftp.isc.org/isc/bind9/9.4.2/bind-9.4.2.tar.gz

✳ C compiler with heather libraries

✳ IPv6 support on the server

Server Configuration

First... Checking the configuration

```
# aptitude update

# aptitude install gcc make libc6-dev
  wget ipv6calc

# modprobe ipv6 && echo "ipv6" >>/etc/
  modules

# ifconfig -a
```

Server Configuration

Mixing the ingredients...

```
# tar -zxf bind-9.4.2.tar.gz

# cd bind-9.4.2

# CFLAGS='-O2' ./configure --prefix=/var/
  named --enable-ipv6

# make && make install
```

Server Configuration

A note on CFLAGS='-O2'...

✳ Usually CFLAGS is configured: '-g -O2'

✳ -g enables debugging symbols in the executable

✳ If you are not a developer and do not need to debug named, then "turn it off"

✳ named executable is 5 MBs with debugging symbols vs 2 MB without

Server Configuration

Finishing up...

```
#  cd /var/named ; mkdir db ; mkdir etc ; mkdir dev

#  cd var ; ln -s .. named ; cd ..

#  cd dev;
   mknod null c 1 3 ;
   mknod zero 1 5;
   mknod random c 1 8;

#  cd ..

#  useradd -c "BIND9 User" -s /bin/false -d /var/named named
```

Server Configuration

Setting up the nameserver (named.conf)

✳ Create /var/named/etc/named.conf

```
acl myTestNetwork {
        127.0.0.1/32;
        10.0.0.0/8;
        2001:1338::/32;
} ;

options {
        allow-recursion {myTestNetwork;};
        directory /var/named/db;
        version "MyDNS Test Server";
        listen-on-v6 { any; };
};
```

Server Configuration

Setting up the nameserver (hints)

✳ Download the latest named.cache from INTERNIC and place it in the /var/named/db directory:

```
cd /var/named/db
wget ftp://anonymous:guest@internic.net/domain/named.cache
```

✳ Add the "hints" or root zone to the named.conf file:

```
zone "." {
        type hint;
        file "named.cache";
};
```

Server Configuration

Setting up the nameserver (hints)

✓ Add the following zones for local resolution:

➡ `localhost`

➡ `1.0.0.127.in-addr.arpa`

➡ `1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa`

✓ Include the following text in the zone file

```
localhost.                      IN AAAA ::1
                                IN A    127.0.0.1
1.0.0.127.in-addr.arpa. IN PTR  localhost.

$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN PTR    localhost.
```

Server Configuration

Setting up the nameserver (hints)

✳ Check permissions:

`/var/named/var/run` should be owned by named

✳ Configure rndc (Remote Named Daemon Controller)

```
/var/named/sbin/rndc-confgen -a
chmod named /var/named/etc/rndc.key
vi /var/named/etc/named.conf  (include "/etc/rndc.key";)
```

Server Configuration

Setting up the nameserver

✴ Specific IPv6 configuration parameters

- transfer-source-v6 (ipv6_address | *) [port (integer | *)];

- listen-on-v6 [port integer] { address_match_element; ... };

- query-source-v6 ((ipv6_address | *) |
  [address (ipv6_address | *)]) [port (integer | *)];

- notify-source-v6 (ipv6_address | *) [port (integer | *)];

- alt-transfer-source-v6 (ipv6_address | *)
  [port (integer | *)];

Server Configuration

Taking a test bite...

✳ Launch the named daemon:

```
cd /var/named ;
./sbin/named -t /var/named -u named -c etc/named.conf
```

✳ Check for the named process and fix any mistakes:

```
ps aux | grep named ;
tail -f /var/log/daemon.log
```

Server Configuration

Congratulations !!!

You now have a Cache-Only enabled server with IPv6 Support

CLIENT CONFIGURATION

Client Behavior

* Depending on the Operating System, client resolver libraries will behave differently in an IPv6 environment

  ✓ Windows Vista

  ‣ If it has a Teredo or Local Link Address only, will only query for A records

  ‣ If it has a global address, will first ask for A resource records, if the query time outs or returns an error (other than nxdomain), it will not try AAAA addresses

  ‣ In any other case, will prefer IPv6 transport over IPv4

Client Behavior

✓ Other Unix Based.. (Mac OS, etc.)

▸ Will prefer IPv6 transport, but will not distinguish between types of addresses

Client Configuration

✳ Currently there are four(4) ways to configure the DNS servers on the client [1]

  ✓ Static configuration

  ✓ RA Option

  ✓ DHCPv6

  ✓ Well Known Anycast DNS Servers

Client Configuration

Static Configuration

✳ Requires to hard-code the DNS servers in each of the clients connected to the network

✳ In a unix-like OS, usually involves adding the DNS Servers to the /etc/resolv.conf file

```
echo "nameserver 2001:1338:3::4" > /etc/resolv.conf
```

Back to this later...

Client Configuration

RA Option

✳ Because the RA support is usually built in into the kernel, its IPv6 support needs to be modified[2] and a daemon written in order to notify the OS about the Recursive DNS Servers (i.e. write /etc/resolv.conf file)

✳ Currently RADVD (Router Advertisement Daemon) supports the RDNSS Option, but it is using an ad-hoc opt code (25). Waiting for IANA to provide the resource.

Client Configuration

DHCPv6

✳ DHCPv6 provides mechanisms to configure Recursive DNS Servers on the client, as well as other configuration parameters (NTP servers, SIP, etc.)

✳ The main advantage is the possibility to manage all the configurations from a main control center

✳ One disadvantage is that the client will receive at least two packages, a RA and one for the DNS Server

Client Configuration

DHCPv6

✳ Configure Recursive DNS Severs

```
option domain-name-servers 2001:1338::2 2001:1338::3;
```

✳ Configure domain search path

```
option domain-name "lacnic.net";
option domain-name "workshop.lacnic.com.uy";
```
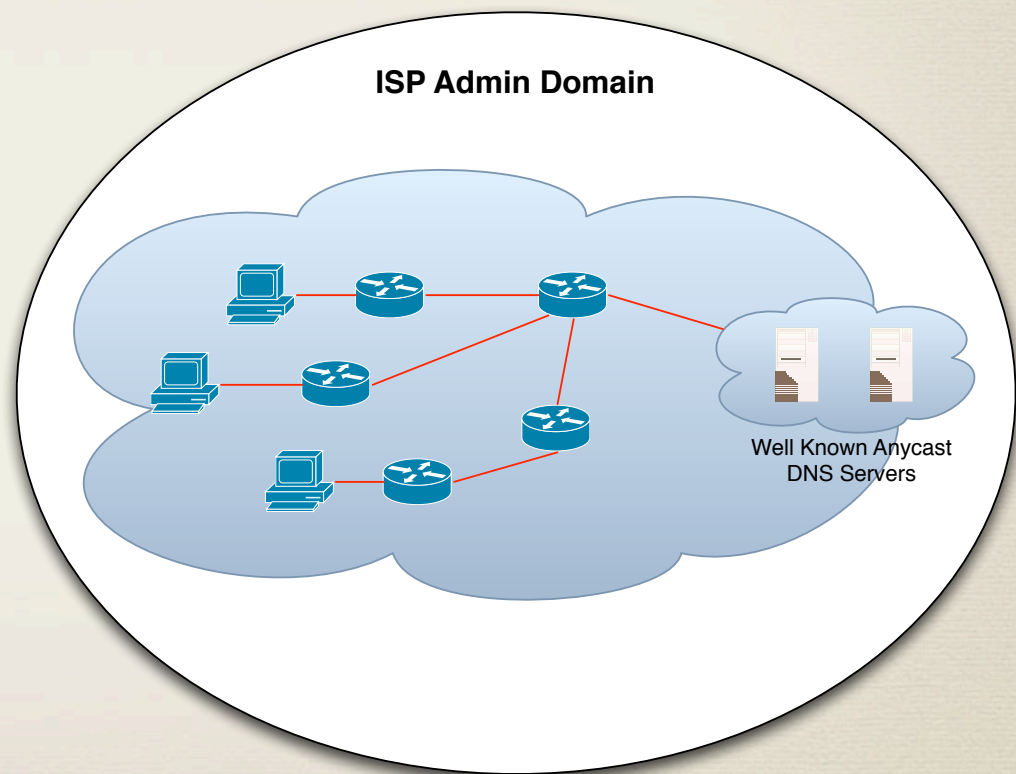
Client Configuration

Well Known Anycast Address

✓DNS servers have both WKA and global address space (global for external queries and responses)

✓WKA distributed via IGP

✓Not exported to external networks

ISP Admin Domain

Well Known Anycast
DNS Servers

Client Configuration

Well Known Anycast Address

✳ Support on all platforms, and can be combined with multiple configuration methods (RA, DHCP, static, etc.)

✳ Windows XP + Vista default behavior

✳ UNIX like OS, (MacOS, Linux, etc.) just add the WKA to the /etc/resolv.conf file and distribute at installation

✳ Main disadvantage: Requires additional networking configuration

DNS RESOURCE RECORDS

DNS Resource Records

Background...

✳ In order to maintain compatibility with existing applications and to provide an environment "similar" to the IPv4 space a new RR type has been created to identify hosts for forward resolution: AAAA

✳ For reverse resolution, PTR records have also been adopted

DNS Resource Records

Background...

✳ Other RR types were also proposed (A6, DNAME), but are currently marked as "experimental"

✳ Not covered since support has been removed from BIND9

DNS Resource Records

AAAA

✳ Structure

```
$ORIGIN domain.name.
NAME [TTL] IN AAAA   IPv6ADDR
```

✳ Example: RR for www.lacnic.net

```
$ORIGIN lacnic.net.
www     IN AAAA   2001:12ff:0:2::15
```

DNS Resource Records

PTR Records

✳ Structure

```
AddrNibbleFormat   [TTL]   IN PTR    fqdn.
```

✳ Example (using the prefix as origin)

```
$ORIGIN 2.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa.

5.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR lacnic.net.
```

DNS Resource Records

PTR Records

✳ Use IPv6Calc to convert IPv6 addresses to various formats:

```
$ ipv6calc --in ipv6addr --out revnibbles.arpa
2001:12ff:0:2::15

5.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.0.0.0.f.f.
2.1.1.0.0.2.ip6.arpa.
```

DNS Resource Records

Putting it all together

✳ Configure the following zones:

- `f.f.2.1.1.0.0.2.ip6.arpa.`

- `workshop.lacnic.net.`

Additional Resources

* [1] IPv6 Host Configuration of DNS Server
  http://tools.ietf.org/html/draft-ietf-dnsop-ipv6-dns-configuration-06

* [2] RADVD RDNSS Support
  http://lists.litech.org/pipermail/radvd-devel-l/2007-June/000276.html

* [3] DNS Configuration Options for DHCPv6
  http://www.ietf.org/rfc/rfc3646.txt