A Basic Introduction to DNS

Introduction to Domain Name Server basics with enlightment on MiNET DNS infrastructure and bind9 DNS server.

PIPEREAU Yohan

Introduction

Mind Map DNS

Question :

-What is DNS ?
-Why do we use DNS ?
-What is a domain name ?
-What are root nameservers ?
-Who is AFNIC in France ?
-What is a name space ?
-What is a DNS zone ?
-Is it a client-server protocol ?
-Is it Layer 2, 3, 4 ? TCP, UDP ? Port number ?
-Is there an open source solution ?
-Can I query any DNS ? What is 8.8.8.8 ?
-What is unicast ? broadcast ? Multicast ? Anycast ?
-What is the difference between www.example.org and example.org ?

-What is DNS ? Domain Name Server is 1. a protocol ; 2. a server :S. Like a database

-Why do we use DNS ?

What is Facebook IP ? Would you like to have a file indexing every domain name/IP ?

-What is a domain name ?

., .net, minet.net., www-user.minet.net., google.fr, yahoo.jp

-What are root nameservers ?

ROOT(.) > TLD (.net) > SOA (minet.net) > Hosting (www-user.minet.net)

-Who is AFNIC in France ?

.fr <3 Organisation. Association française pour le nommage Internet en coopération

-What is a name space ? Concept for a set of DNS zone

-What is a DNS zone ? Concept for a set of DNS entry

Zone1 ~ {ns1.minet.net – 157.159.40.54 , www.minet.net - 157.159.0.103}

Zone2 ~ {ns1.minet.net – 192.168.102.55 , www.minet.net - 192.168.102.103}

-Is it a client-server protocol ? Yes

-Is it Layer 1, 2, 3, 4, 5, 6, 7 ? 111b

-TCP, UDP ? Both but default is UDP

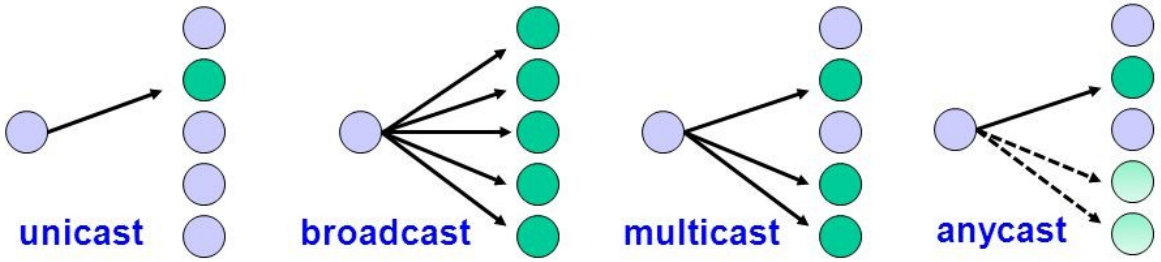
-Port number ? 53

-Is there an open source solution ? So Many :p

-Can I query any DNS ? No + depends on type of query (AXFR, Recursion, Zone info,...)

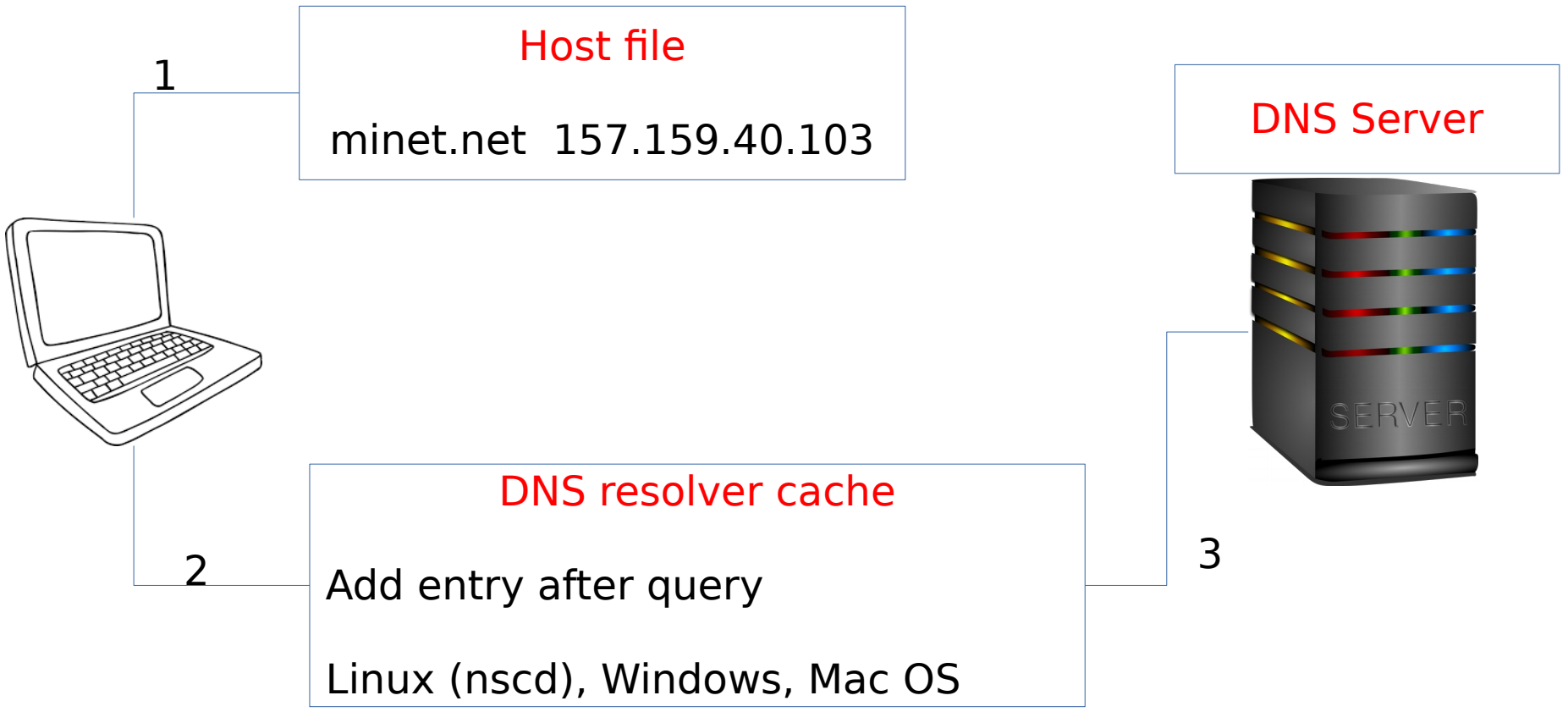
-What is 8.8.8.8 ? dig -x 8.8.8.8 +short

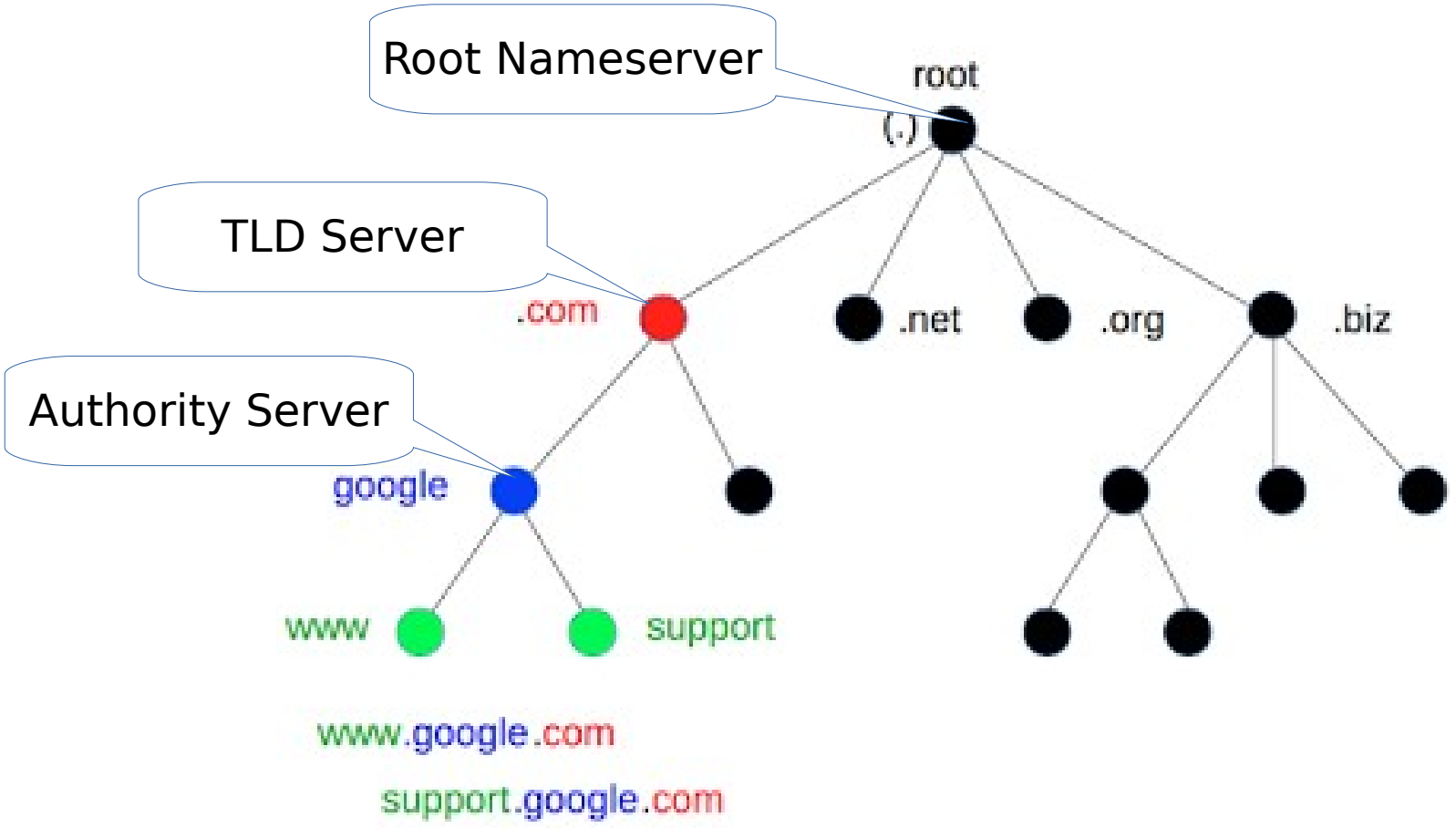
-What is unicast ? broadcast ? Multicast ? Anycast ?



-What is the difference between www.example.org and example.org ?
Depends on the entries in your zone.

-Who handles root zone ?
Until 2014, USA gov through NTIA for root zone
After 2014, ICANN & IANA for root zone


Host file
minet.net 157.159.40.103
1
DNS Server
SERVER
DNS resolver cache
Add entry after query
Linux (nscd), Windows, Mac OS
2
3


Root Nameserver
root
(.)
TLD Server
.com
.net
.org
.biz
Authority Server
google
www
support
www.google.com
support.google.com

Graphique Bind9, OpenDNS, Windows

-Bind9 : Most used DNS server (libre)

-PowerDNS : stable, fully featured as bind but only CLI (libre)

-NSD : implement new features. Run 3/13 root DNS server (libre)

-Knot DNS : claim more security, stability (opensource)

-Microsoft DNS : Integrated with Active Directory. CLI, GUI, Powershell

-Erl-DNS : very fast query response (30 µs)

-Dnsmasq : lightweigth DNS forwarder (opensource)

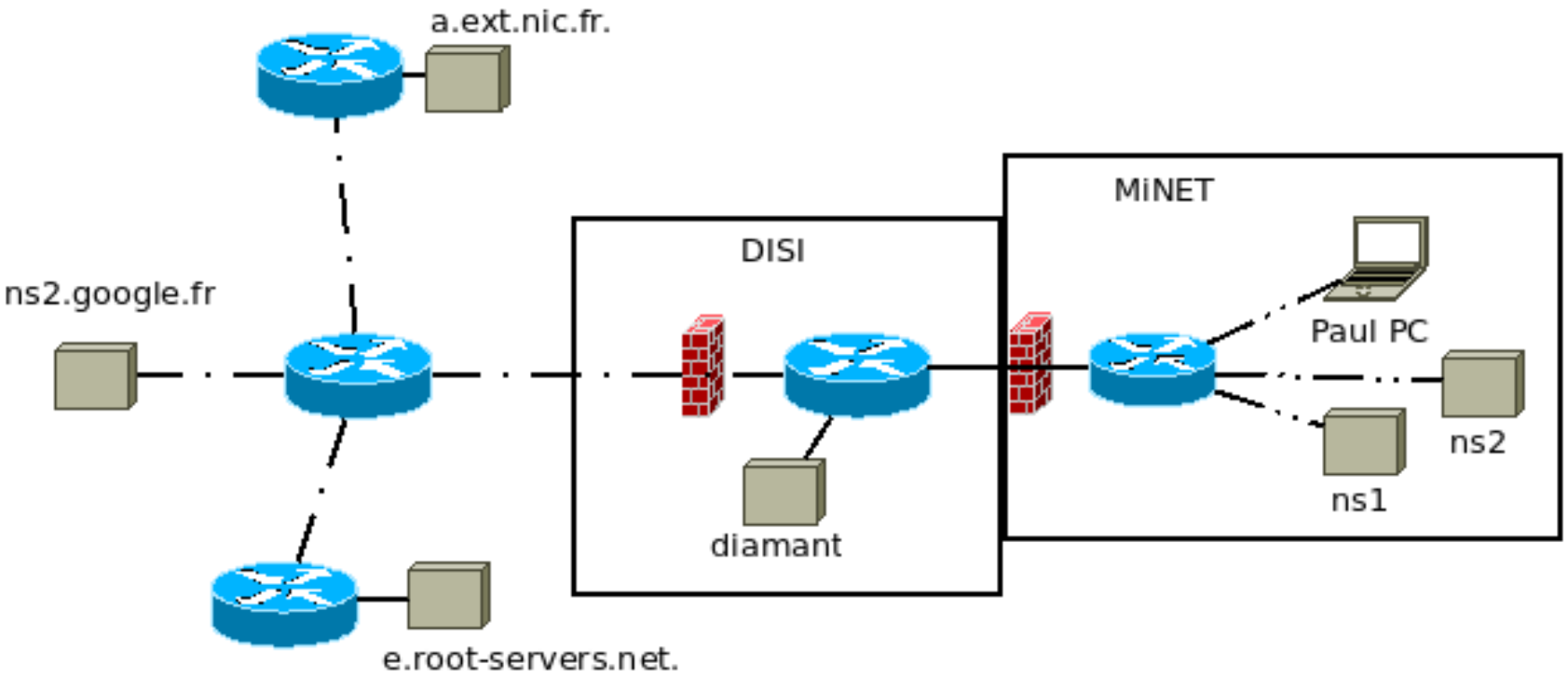
Question :

-Why do we use different DNS server software for the root DNS server ?

More details :

https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software

MiNET Infrastructure



Questions :

What does cutting down DNS servers implie ?

How critical is this service for our production ? For subscribers ?

DNS Theory

- **Resource Records (RRs)**
- **DNS zones**
- **DNS protocol**
- **Recursive/fowarding/iterative mode**
- **Query/reverse-lookup**

Resource Records (RRs)

RR = (owner/name, type, class, TTL)
owner : points to the domain, depends on the type
    * A, CNAME : hostname
    * PTR : IP
Type (16 bits) : Specify the type of data
Class :
    * In (01) Internet
    * Cs (02) Csnet : network extending ARPANET
    * Ch (03) Chaos : chaosnet, extends ARPANET, former network
    * Hs (04) Hesiod : distribute info on name databases
TTL : how long a RR can be cached

RFC 1034

Resource Records (RRs)

Type	Description
NS	Authoritative DNS for domain
A	Host address
AAA	Ipv6 Host address
SOA	Start of a zone of authority
MX	Mail Exchange
CNAME	Canonical name of an alias
TXT	Descriptive Data. Used for SPF
AXFR	Zone Transfer
IXFR	
PTR	Pointer to another part of DN space. RevDNS
AFSDB	Points to AFS database

Used ++

Used --

RFC 1034

DNS Zone

Types of zone :

- **Primary zone, Master Zone**
- **Secondary zone, Slave Zone**
- **Active Directory Integrated Zone**
- **Stub Zone, Stub Zone**
- **Forward Zone**

Microsoft Name, Bind Name

DNS Zone : Primary/Master Zone

Primary Zone, Master Zone :

- **RW zone**
- **ONE AND ONLY ONE primary zone for a zone**

Bind9 :

```
zone "minet.net" {
        type master;
        file "/etc/bind/zones/minet/db/minet.net.db.INT";
};
```

DNS Zone : Secondary/Slave Zone

Secondary Zone, Slave Zone :

- **RO copy of Primary/Secondary/AD**

Bind9 :

```
zone "minet.net" {
        type slave;
        masters { 172.16.0.55; };
        file "/etc/bind/zones/minet/db/minet.net.db.INT";
};
```

DNS Zone : Active Directory Integrated Zone

Active Directory Integrated Zone :

- **Microsoft Software using LDAP protocol.**
- **RW zone**
- **Zones stored in Active Directory controllers**
- **High Availability+Redundancy, you can change zone even if one controller is down**
- **Not a text file → hard restoration**
- **Secure Updates between Windows Environment only → Not Unix compliant**

DNS Zone : Stub Zone

Stub Zone, Stub Zone :

Stub zones are DNS zones that contain only the SOA, NS, and A glue records for a domain. A stub zone doesn’t store any other records.

Ex : stub zone on NS1 redirecting to google.fr zone authority server.

Bind9 :

```
zone example.com {
   type static-stub;
   server-addresses { 192.168.2.57; 2001:db8:0:1::17;};
};
```

DNS Zone : Forward Zone

Foward Zone :

- **Redirect to another DNS for resolution of a specific zone or all zones.**

Bind9 :

```
zone "example.com" {
    type forward;
    forward only;
    forwarders { 192.168.0.4; };
};
```

DNS Zone : Redirect Zone

Redirect Zone :

Used for DNS Hijacking (advertisement or FBI).

Bind9 :

```
zone "." {
        type redirect;
        file "db.redirect" ;
};
```

db.redirect :

```
$TTL 300
@ IN SOA ns.example.net hostmaster.example.net 0 0 0 0 0
@ IN NS ns.example.net
*.ES. IN A 10.100.100.3 //redirect all spanish names
```

What is the difference between Forwarding zone and Stub zone ?

What is the difference between Forwarding zone and Stub zone ?

-Same purpose

DNS fowarding : connect to these DNS servers to resolve IP addresses for domain whatever.com

Actually, Stub zone almost always used on Microsoft networks.

DNS protocol

Source Socket : **(192.168.1.2 , UDP, port 50679)**
Destination Socket: **(8.8.8.8 , UDP, port 53)**

Analysis of a DNS query to 8.8.8.8

```
Transaction ID: 0xc557
```

ID used in query and answer

```
▼ Flags: 0x0020 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...0 .... .... = Recursion desired: Don't do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..1. .... = AD bit: Set
    .... .... ...0 .... = Non-authenticated data: Unacceptable
```

Flag section is 2 Byte size :

Response : query (0), response (1)

Opcode : Query, Iquery, Status, Unassigned, Notify, Update, Unassgined

Truncated : not truncated (0), truncated (1) [only 512 bits]

RA, Recursion Available : no recursion (0), recursion (1)

Z : ??

AD, Authenticated Data : a

CD, Checking Disabled : Non-authenticated (0) ,

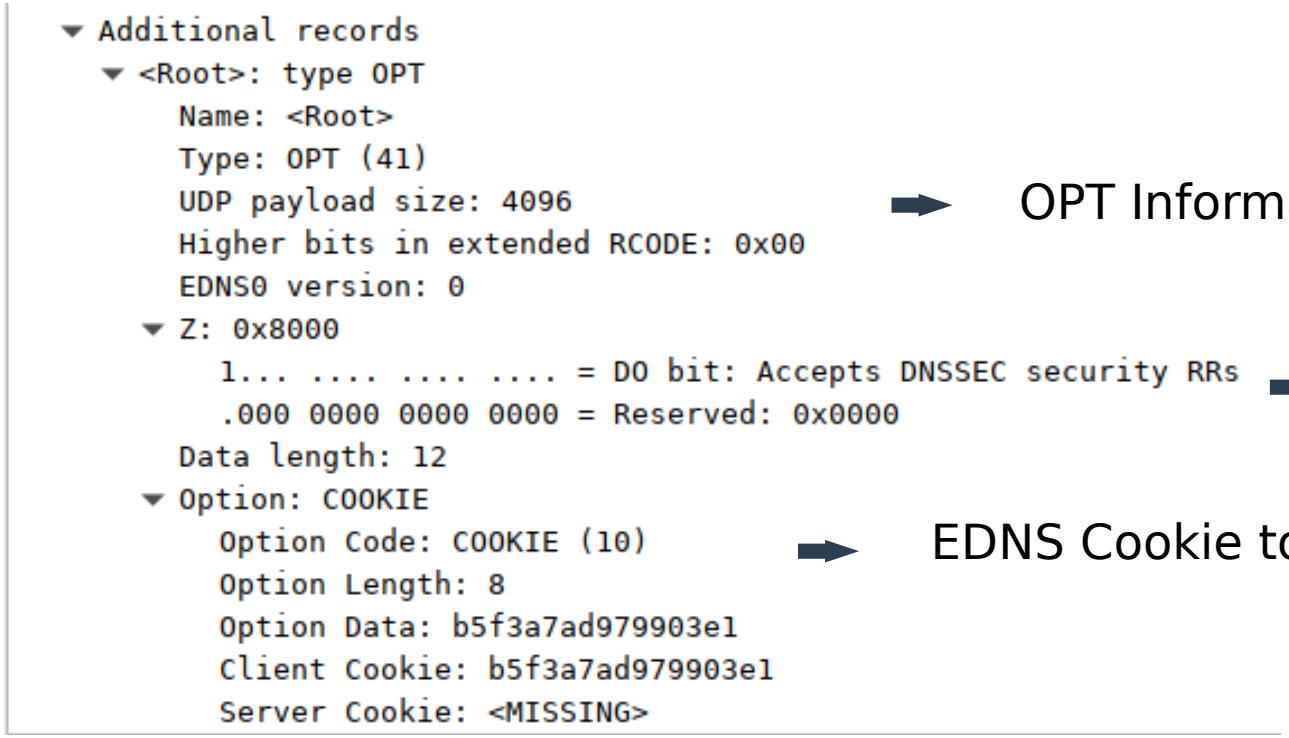
Rcode , Return Code : No error, Format error, Server Failure, Name error, Not Implemented, Refused, YXDomain, YXRRSET, NXRRSET, NotAuth., BADSIG, BADKEY, ...

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
```

-Number of questions
-Number of RR answer
-Number of authority RR
-Number of additionnal RR

```
▼ Queries
  ▼ <Root>: type NS, class IN
      Name: <Root>
      [Name Length: 6]
      [Label Count: 1]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

-Nu



OPT Information

EDNS Header

EDNS Cookie to detect spoofed answers

Diggy, diggy

-Simple query domain « A » record :	dig google.com
-Short query domain « A » record :	dig google.com +short
-Query domain NS record :	dig google.com NS
-Query domain MX record :	dig google.com MX
-Query all DNS records :	dig google.com ANY
-Reverse-DNS lookup :	dig -x 157.159.40.1
-Try AXFR zone transfer:	dig minet.net axfr
-Get DNS server version (sometimes):	dig -t txt -c chaos VERSION.BIND @<serv dns>
-Get DNS server hostname:	dig -t txt -c chaos HOSTNAME.BIND @<serv dns>
-Query domain A record from <IP> :	dig @<ip_dns_server> hackersgarage.com NS
-Test DNS SOA server serial answer :	dig minet.net +nssearch
-Registrar info about domain name :	whois minet.net
-Query nss hosts :	getent hosts

Question	**Query Name & Parameters**
Answer	**answer RRs for the query**
Authority	**answer RRs for other authoritative servers.**
Additional	**answer helpful RRs**

Dig Usage Moment

Observe DNS flags

(qr,rd,ra) : dig google.fr

Qr : query
Rd : Recursion Desired
Ra : Recursion Available

(qr,ra) : dig facebook.fr +norecurse

(qr,rd,ra,ad) : dig +dnssec d.nic.fr

Ad : authenticated data

(qr,aa,rd) : dig minet.net @ns1.minet.net

aa : Authoritive Answer

Reverse Lookup

-The zone .in-addr.arpa is for reverse-lookup.

Ex : "102.168.192.in-addr.arpa"

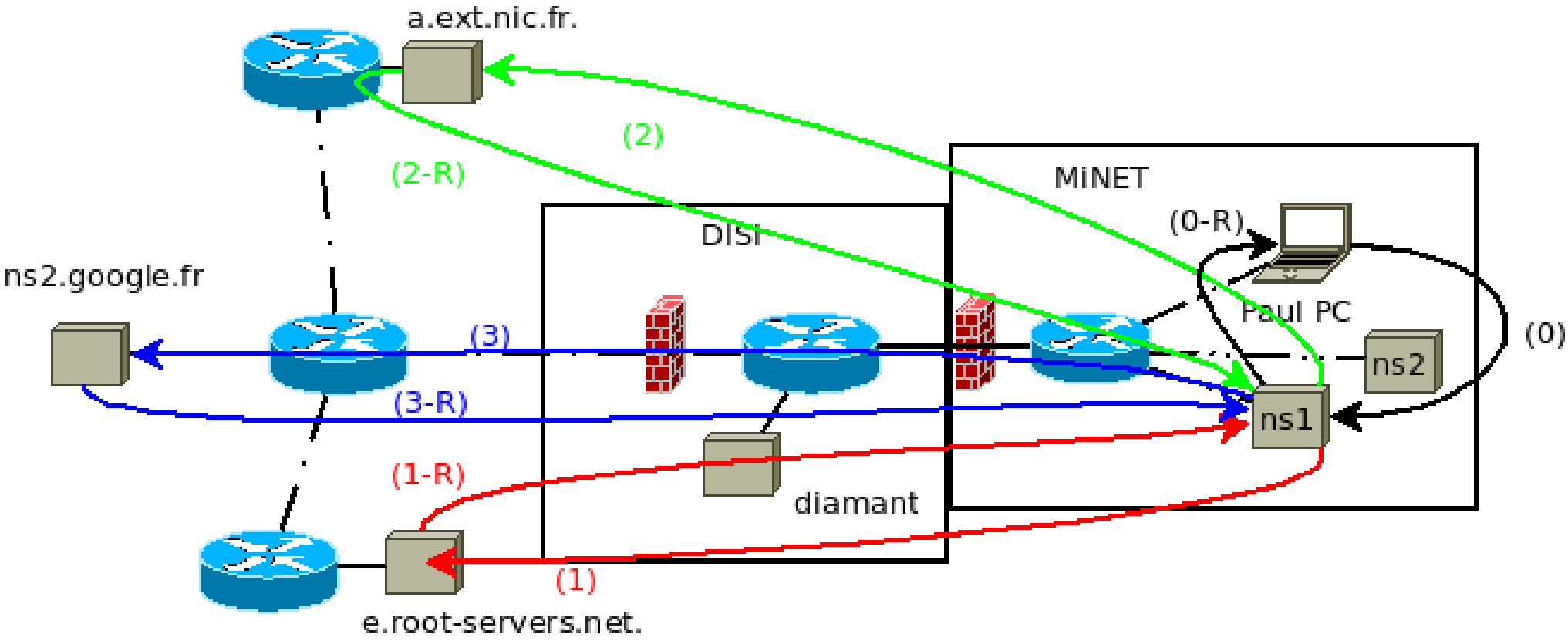
10 IN PTR dhcpv6.minet.net.

-RR type is PTR (Reverse-Lookup Pointer Records)

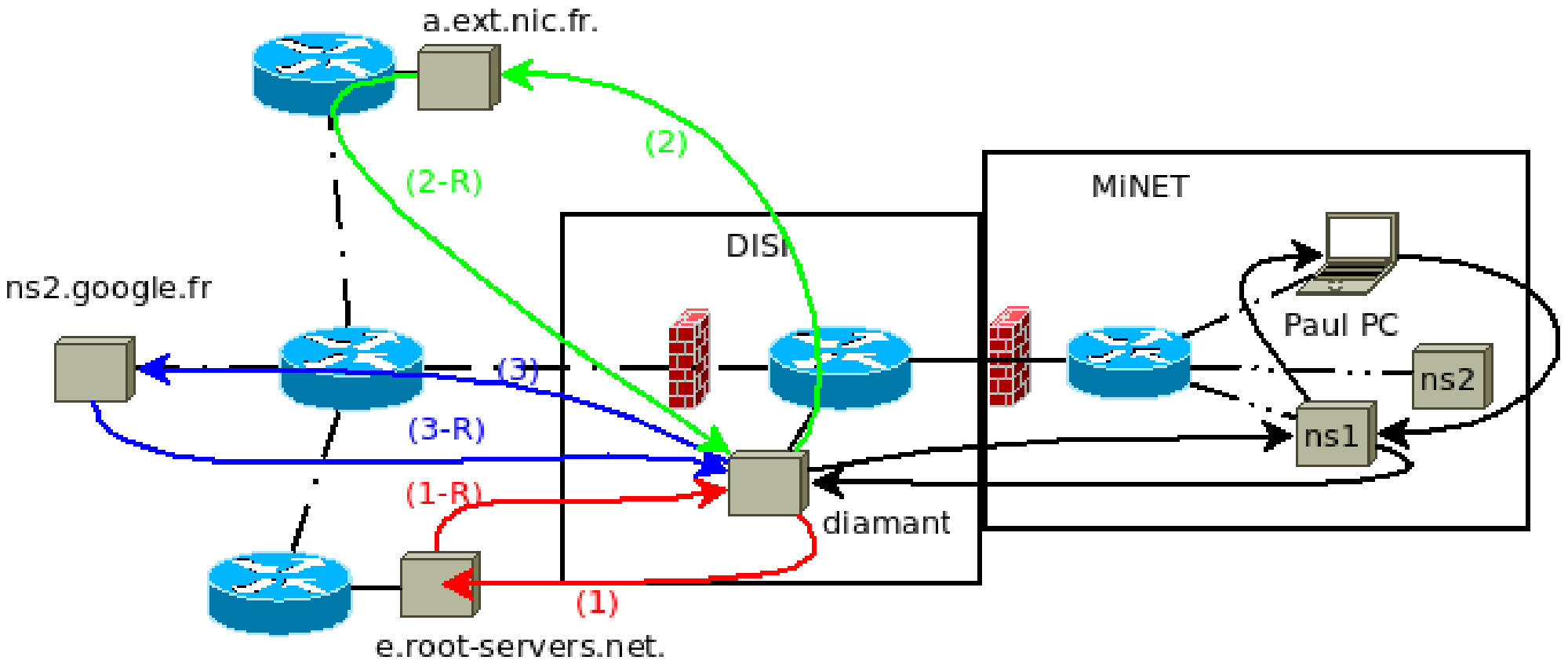
-No cache for inverse queries because improper TTL

dig -x 157.159.40.103

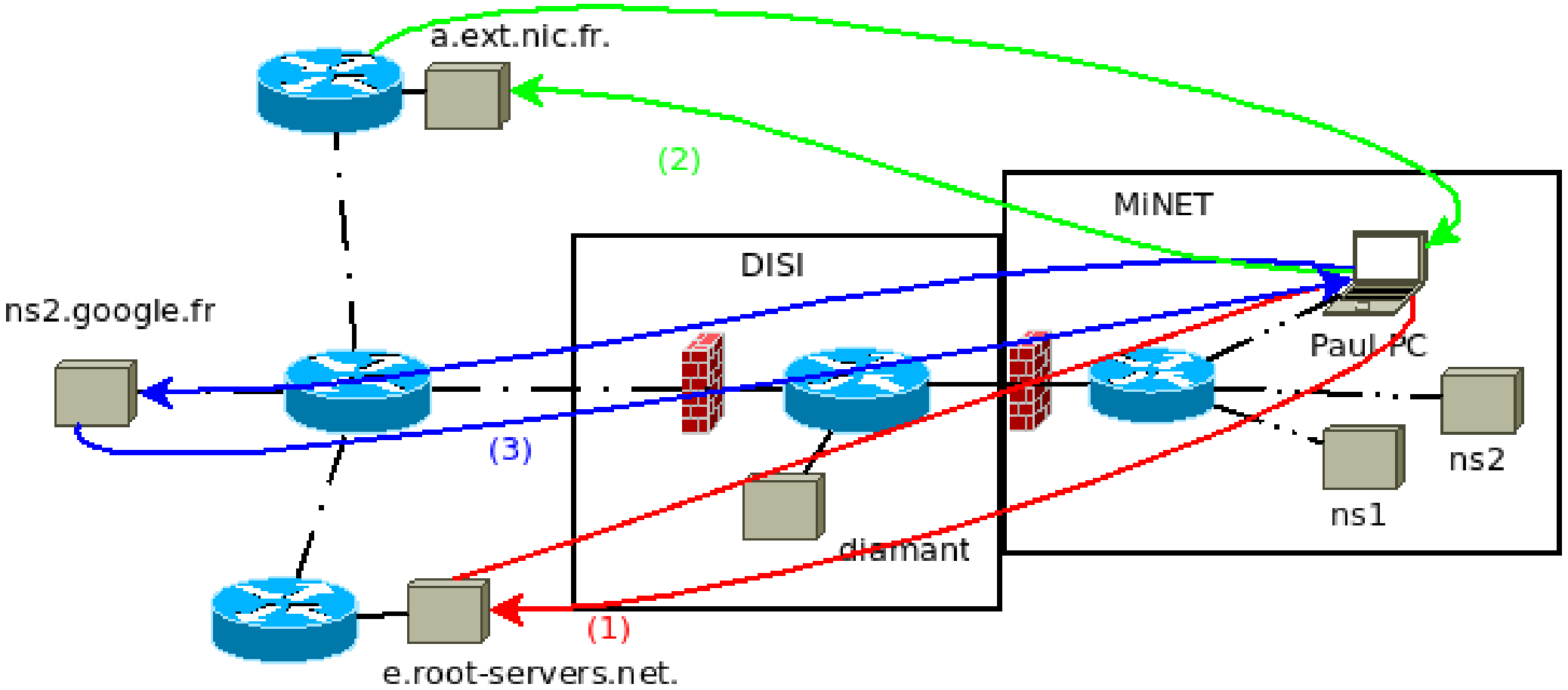
Recursive mode



Forwarding mode



Iterative mode



DNS cache server

How to Detect a DNS caching server ?

Dig minet.net → anwer in 30ms

Dig minet.net → answer in 0ms

How to look into the DNS cache ?

rndc dumpdb –cache

cat /var/cache/bind/named_dump.db

What happens if you ask a non forwarding dns server to do no recursion ?

dig facebook.fr +norecurse (output nothing)

Dig facebook.fr +recurse (output sthg and add to cache)

Dig facebook.fr +norecurse (output what is cached)

Is Bind caching data ?

You can not disable caching in bind.

What is a SOA record ?

Administrative information about the DNS Server

```
@   IN SOA master.example.com. hostmaster.example.com. (
    2017030300 ; serial
    3600       ; refresh
    1800       ; retry
    604800     ; expire
    600 )      ; ttl
```

You have to change manually the SOA value when you edit the master zone to update the changes on the slave zone as well !!!

TP Bind

https://imagine.minet.net/pad/p/dns