



EDNS Compliance Status of Resolvers



Jeisson Sanchez
jeisson@niclabs.cl

What is EDNS?

Extension mechanisms for DNS: RFC 6891 in 2013

Defines a backward-compatible mechanisms to deploy new DNS features

- Extra data space for additional flags
- DNS messages larger than 512 bytes
- Extended response codes
- Among others...

Problem – Solution with EDNS

But there are some operational workarounds with EDNS...

- Poorly firewall rules blocking valid traffic
- Obsolete DNS software

Summary: Bad implementations of DNS not following standards





CONTRIBUTION

What is EDNS status resolvers before and after DNS Flagday?

TEST

- 19061 Resolvers
- VMs: Ubuntu 16.04
- Dig and Pydig [1]: DNS query tool written in Python
- Each test was performed 5 times
- Tests 1 & 2 are based on I-D “A Common Operational Problem in DNS Servers - Failure To Respond”

1

Basic Test

Normal operation of resolvers and basic information

2

Edns and DNSSEC

Edns version , negotiation and complete chain of validation

3

Some extensions

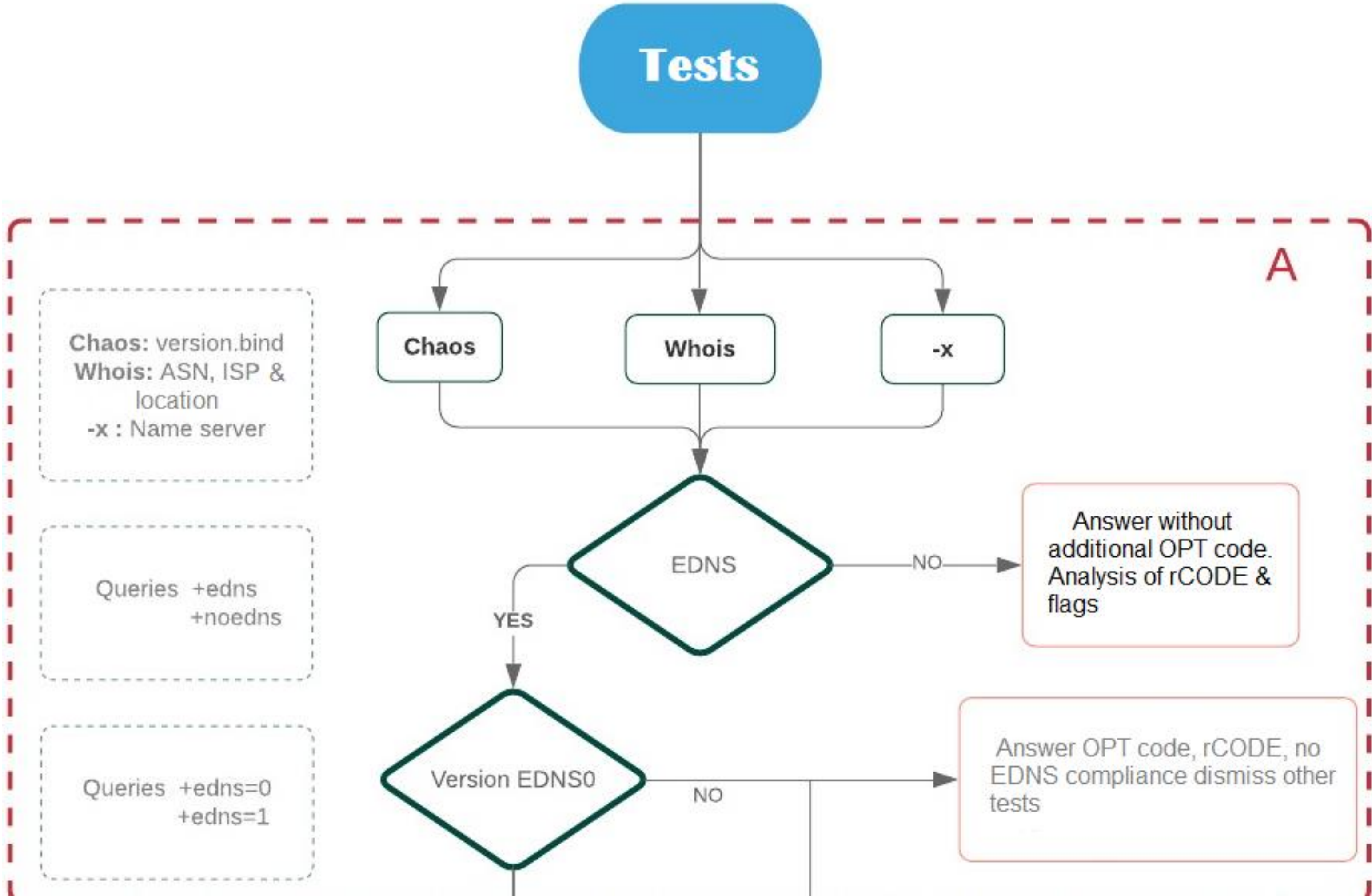
Client Subnet, Chain query, EDNS TCP Keepalive, among others

4

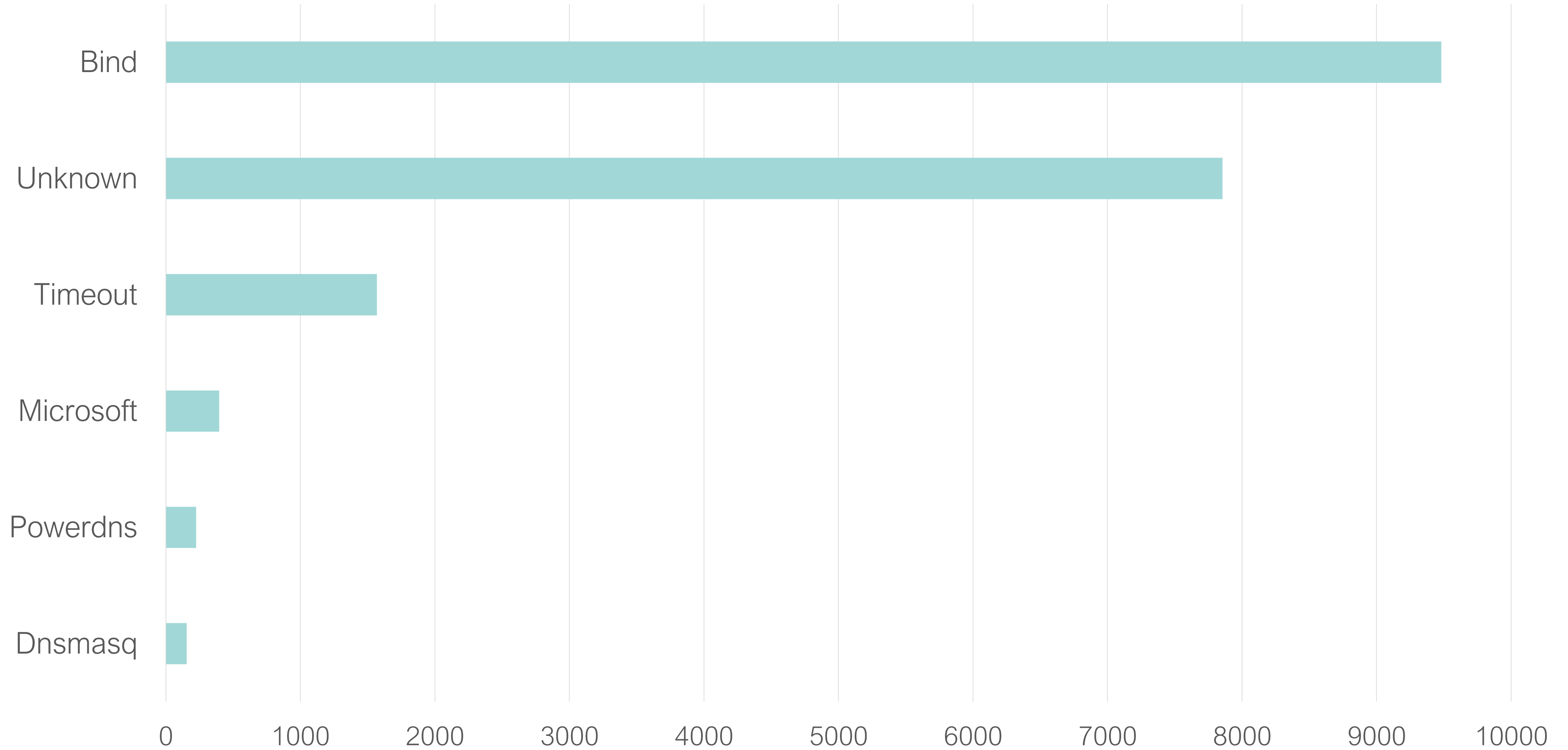
DNSFlag Day



Basic Test



Server's version



fcfm

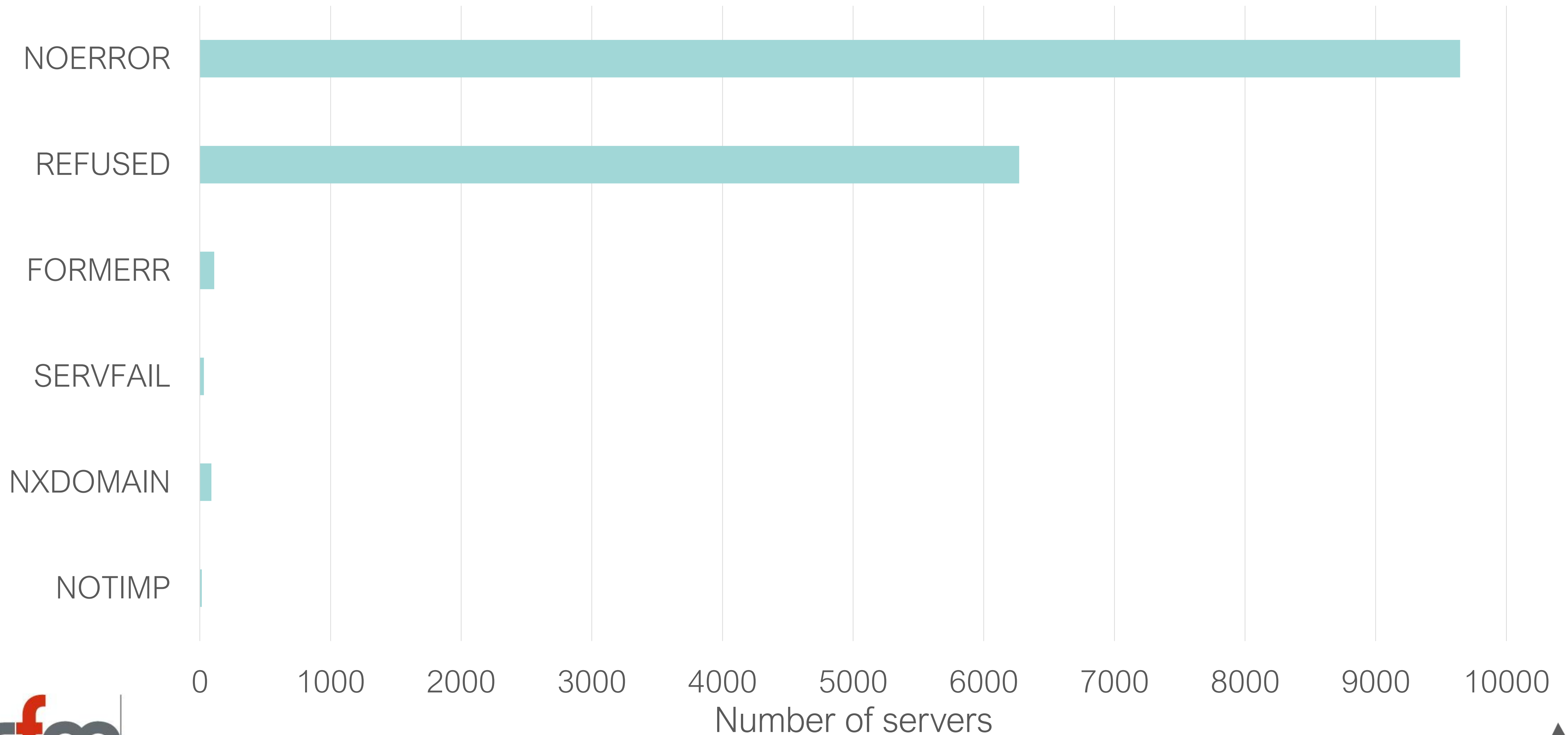
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

Number of servers

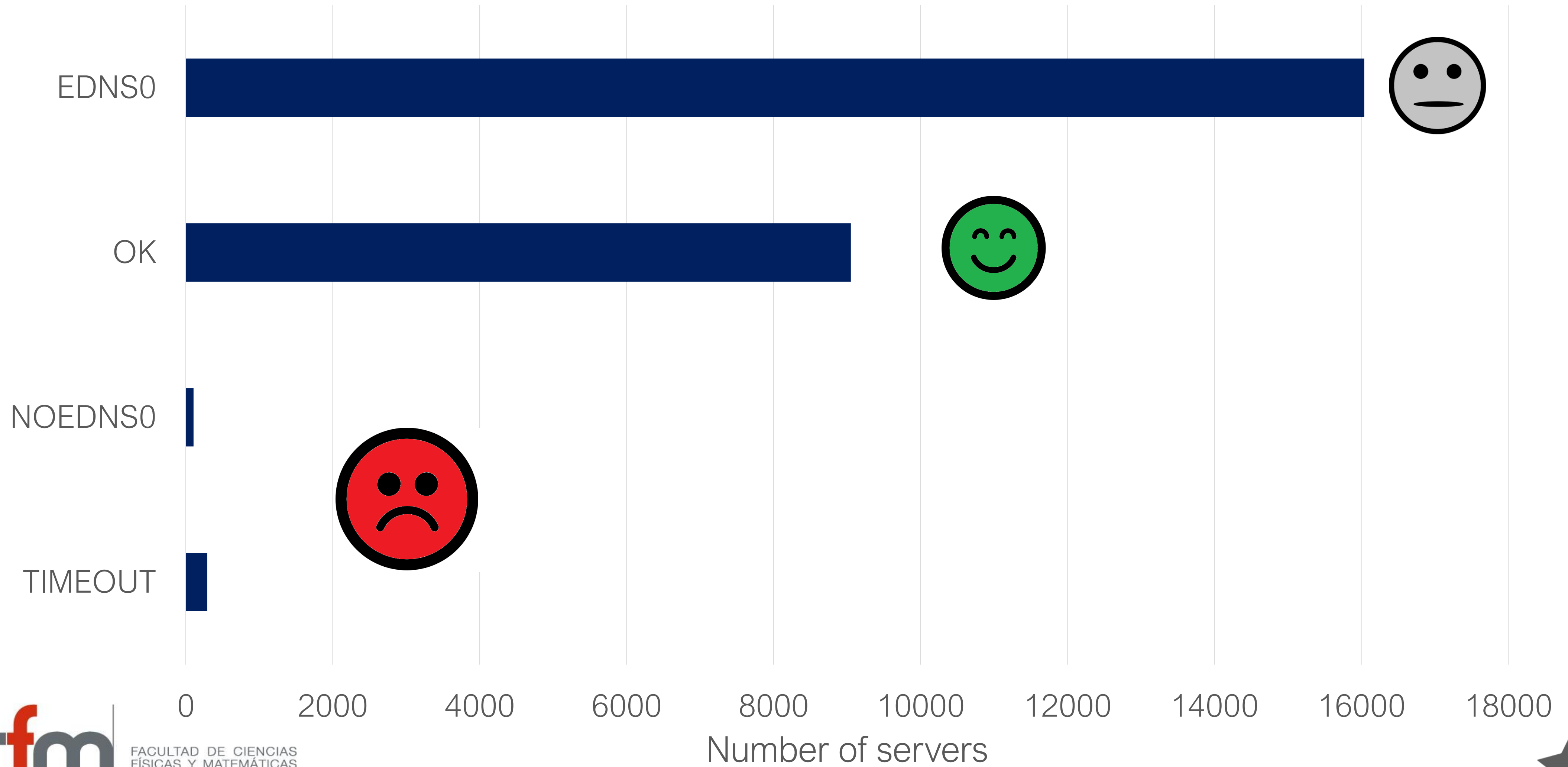


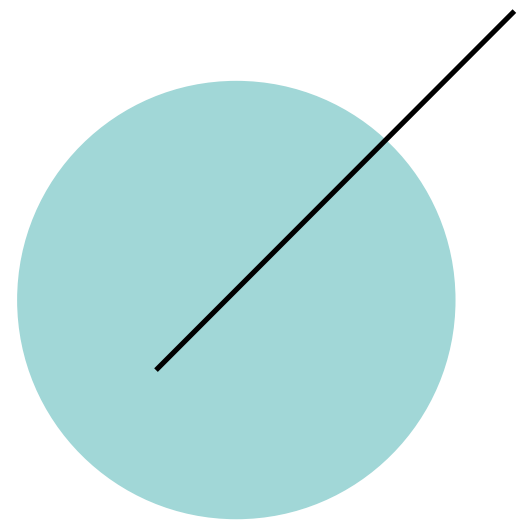
Edns aware

dig +nocookie +edns=0 +noad +nored soa \$zone @\$server



Algorithm EDNS classification





1

Basic Test

Normal operation of
resolvers and basic
information

2

Edns and DNSSEC

Edns version and
complete chain of validation

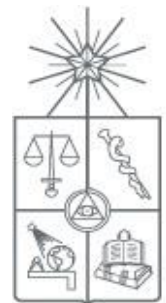
3

Some extensions

Client Subnet, Chain query,
EDNS TCP Keepalive, among others

4

DNSFlag Day



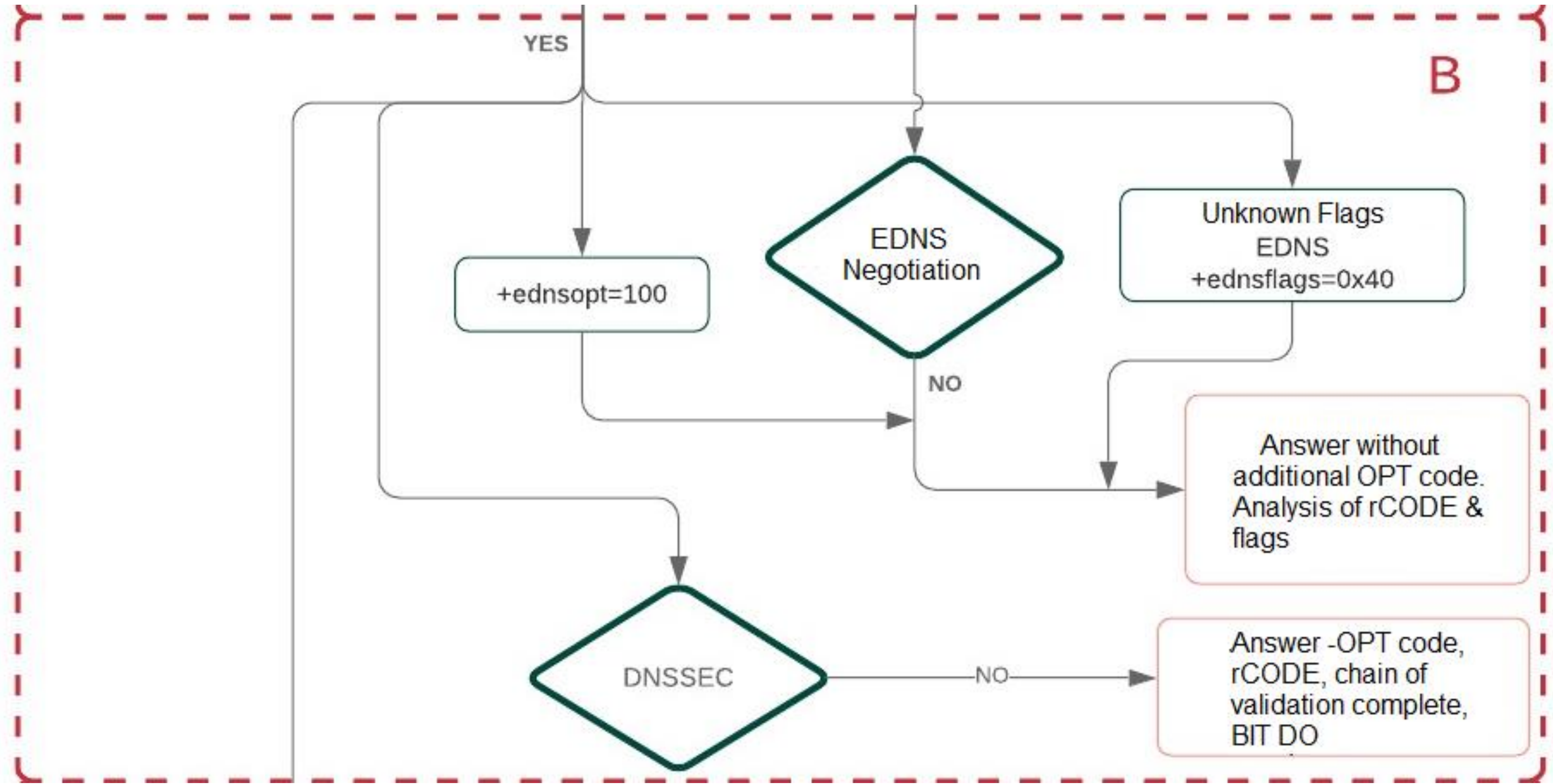
fcfm

FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

NIC
CHILE
RESEARCH LABS

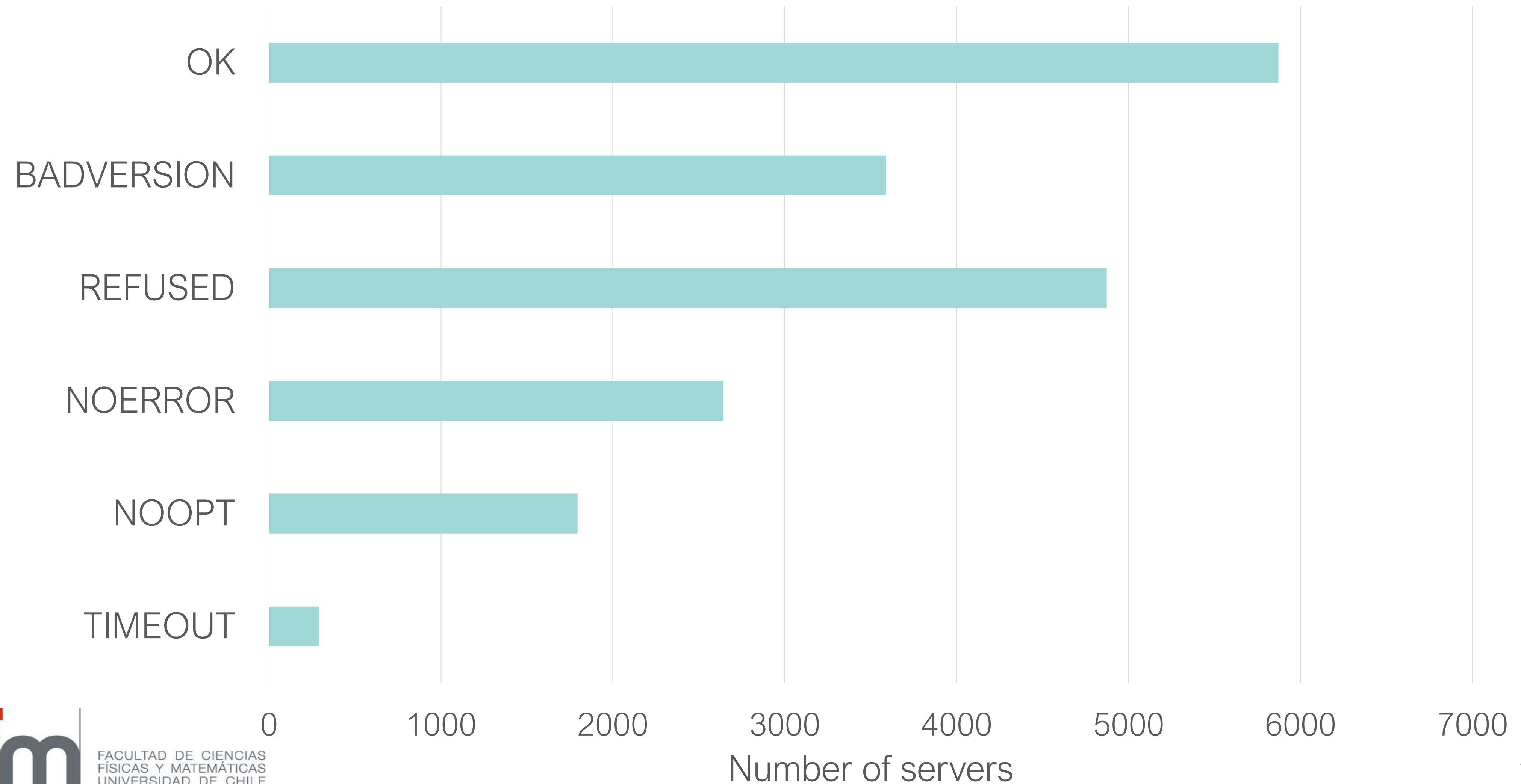
2

EDNS and DNSSEC test



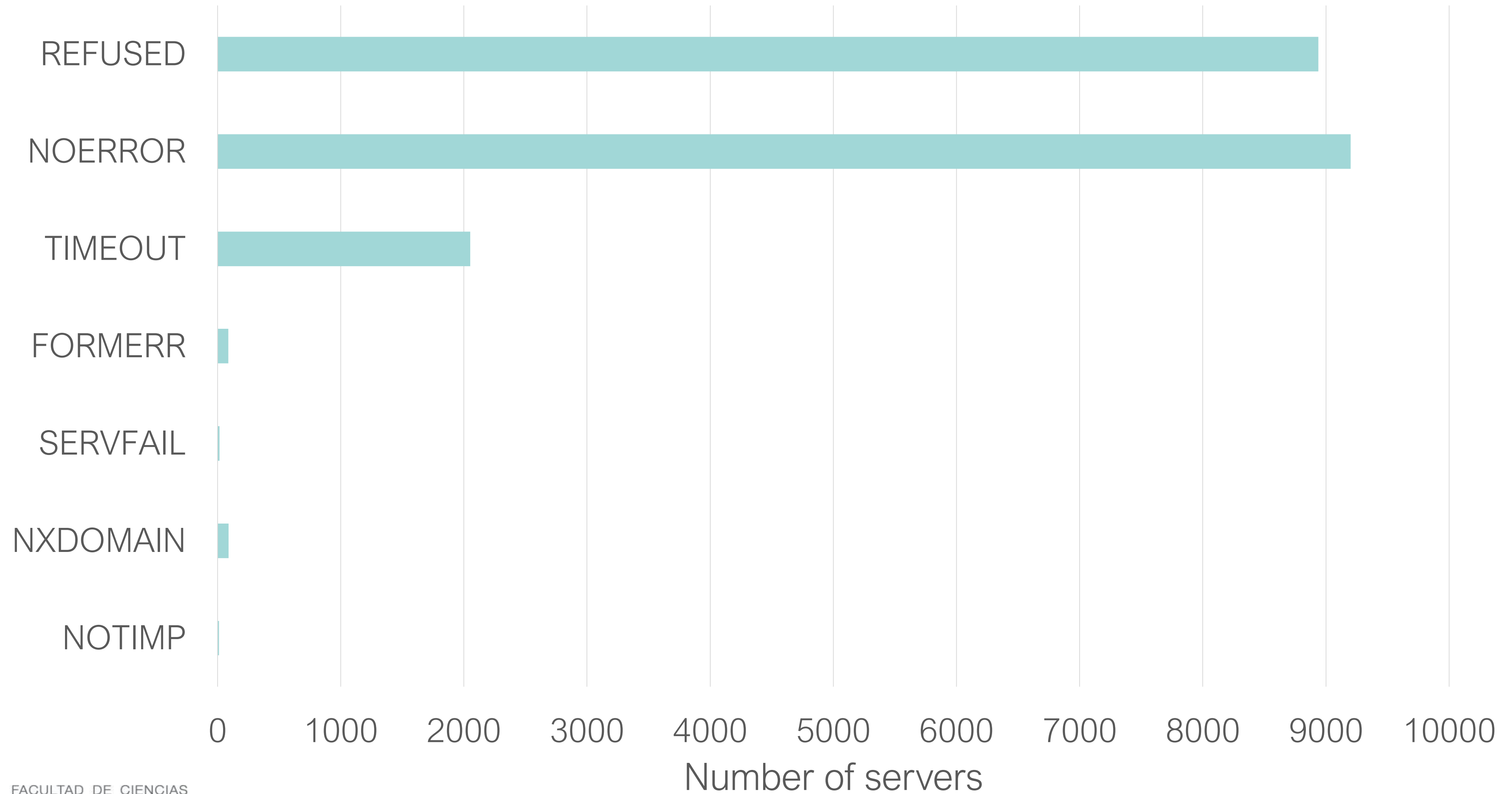
Testing Edns1

dig +nocookie +edns=1 +noednsneg +noad +nored soa \$zone @\$server

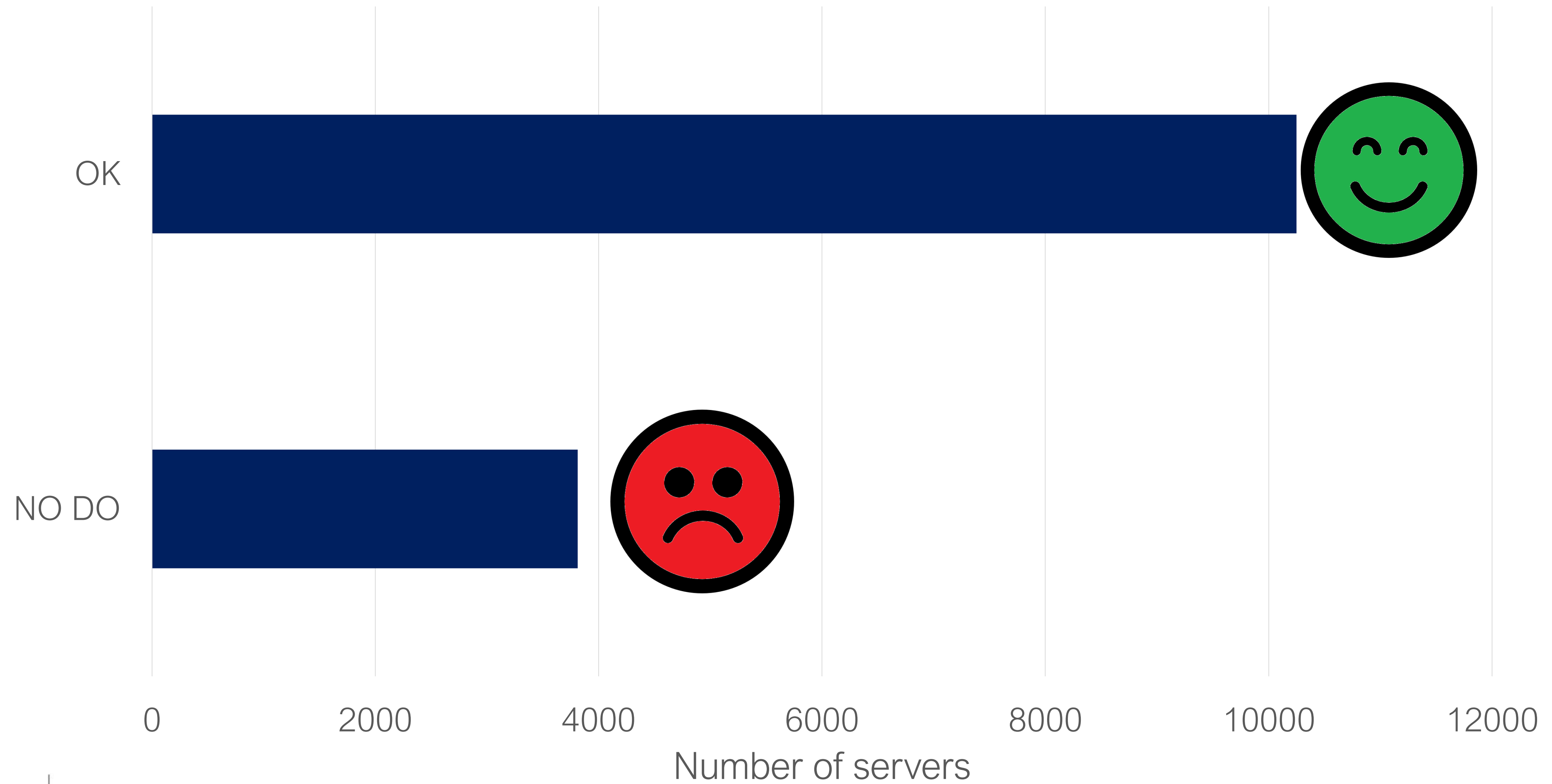


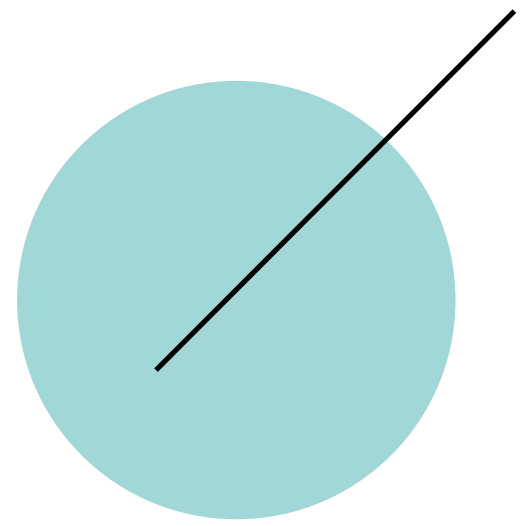
Testing DNSSEC

```
dig +nocookie +edns=0 +noad +nored +dnssec soa $zone @$server
```



Algorithm DNSSEC classification





1

Basic Test

Normal operation of
resolvers and basic
information

2

Edns and DNSSEC

Edns version , negotiation and
chain of validation

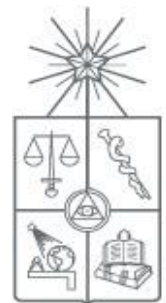
3

Some extensions

Client Subnet, Chain query, expire
option, among others

4

DNSFlag Day



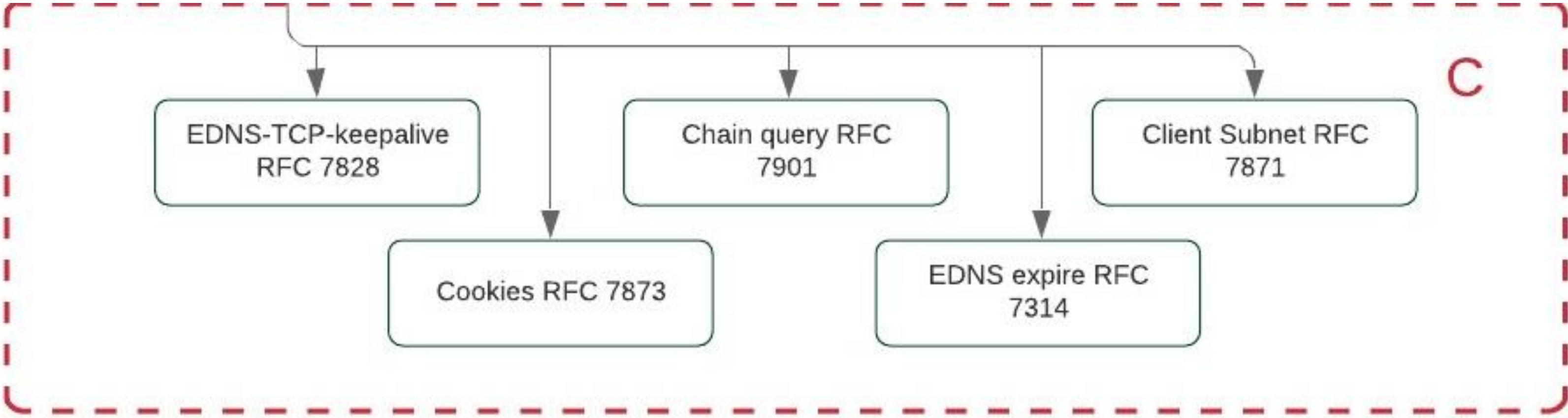
fcfm

FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

NIC
CHILE
RESEARCH LABS

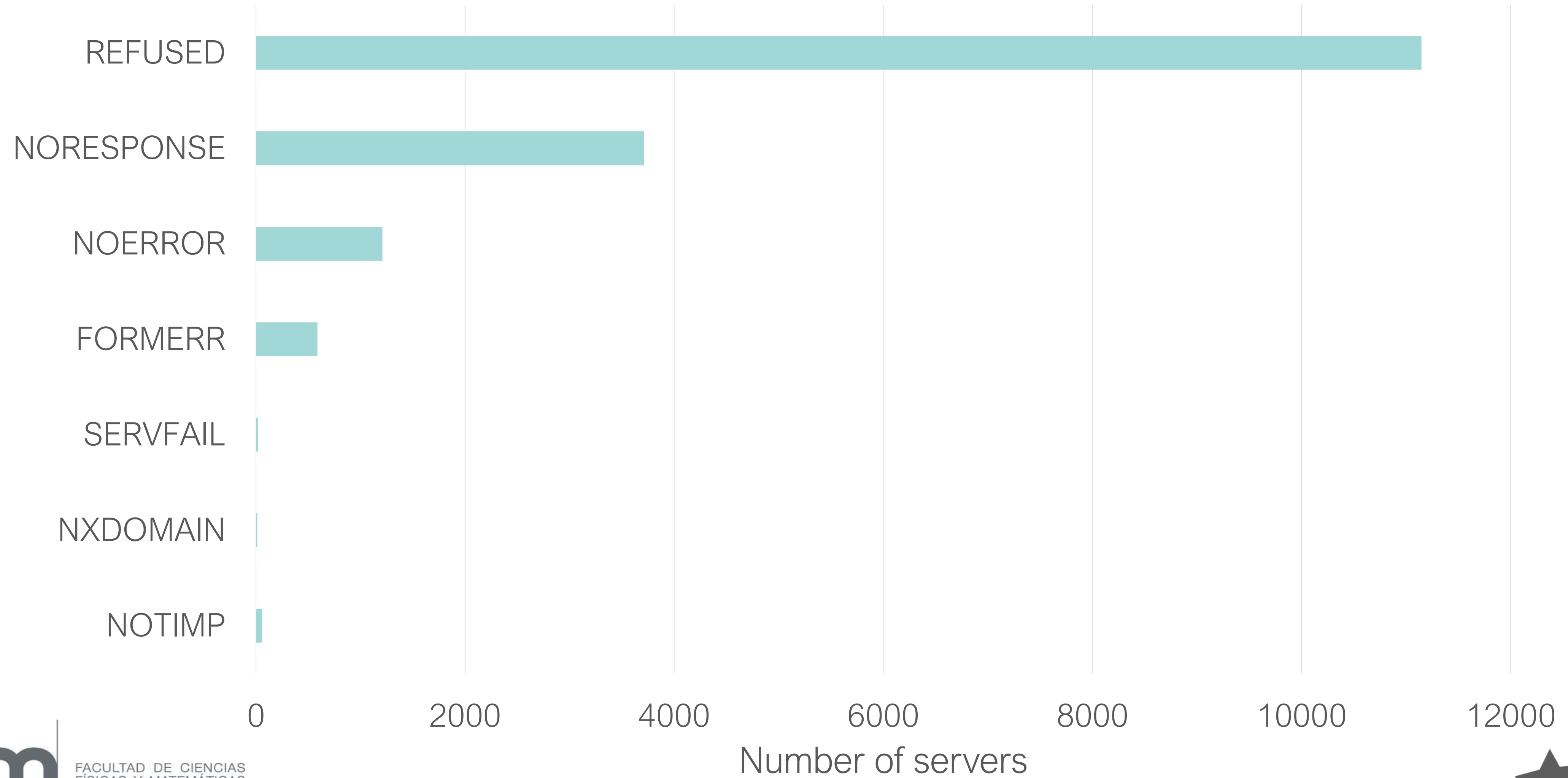
3

Extensions test



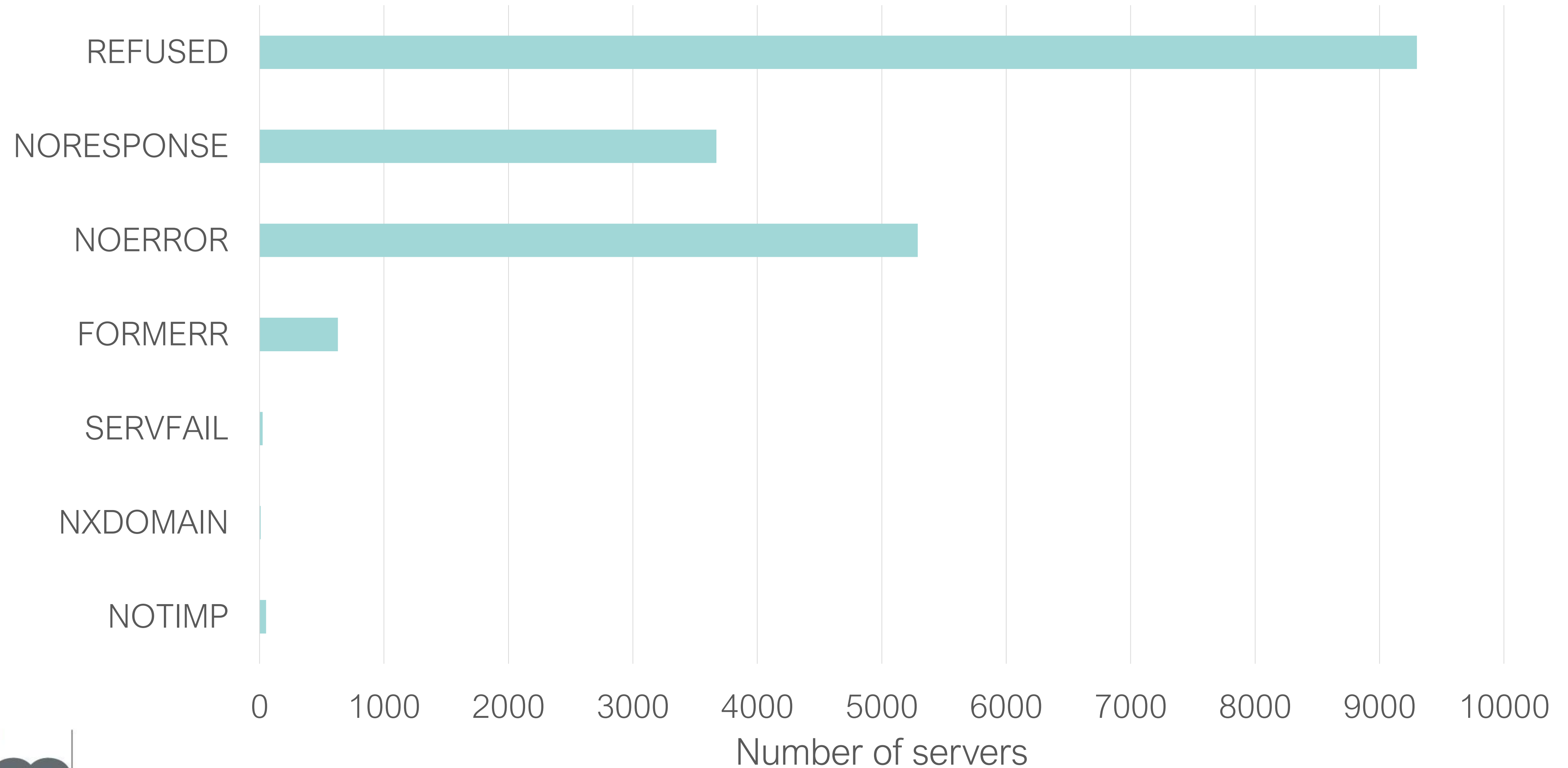
Chain query in DNS - RFC 7901

```
pydig +tcp +chainquery soa $zone @$server
```



Client Subnet in DNS- RFC 7871

pydig +subnet=addr \$zone @\$server





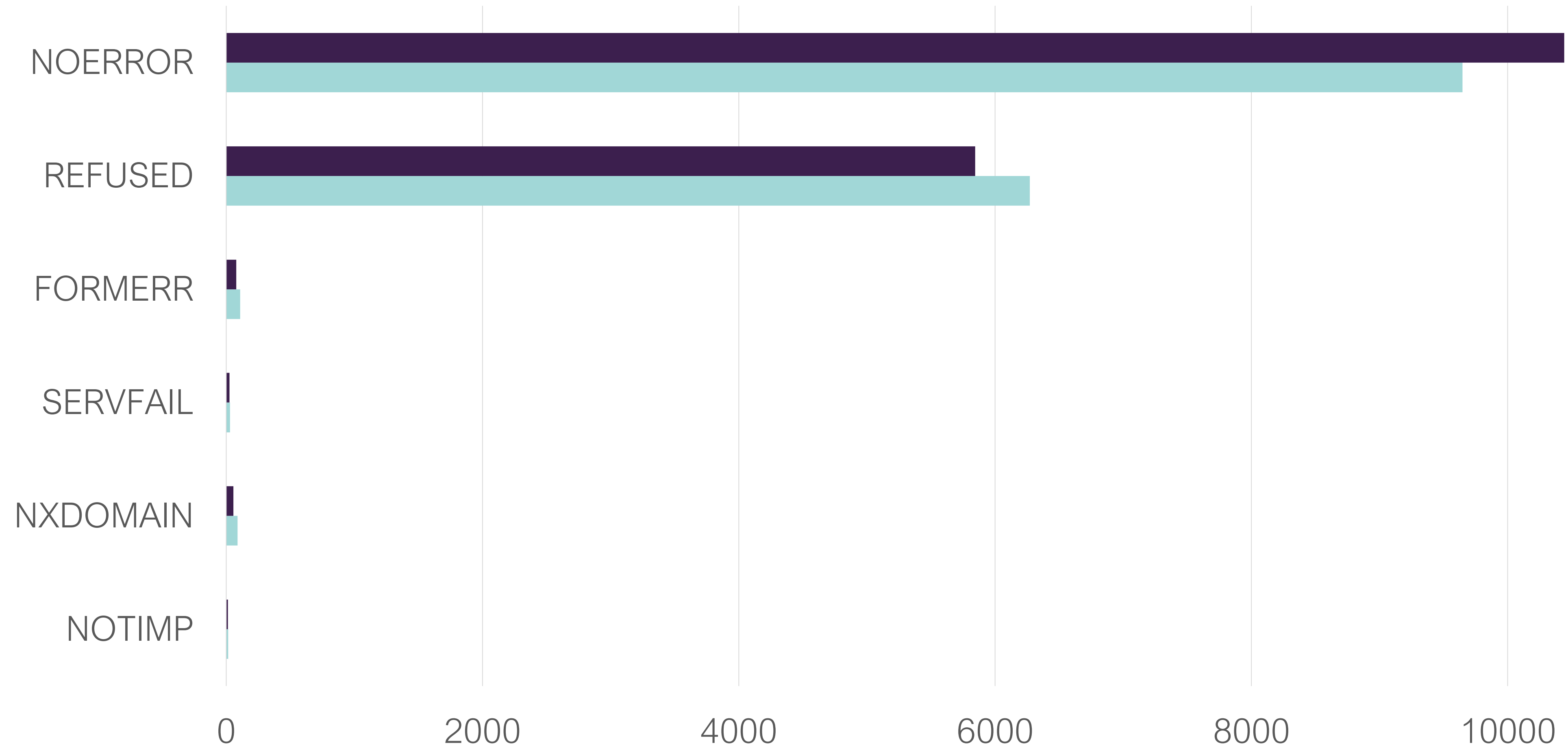
DNS FLAG DAY



FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE



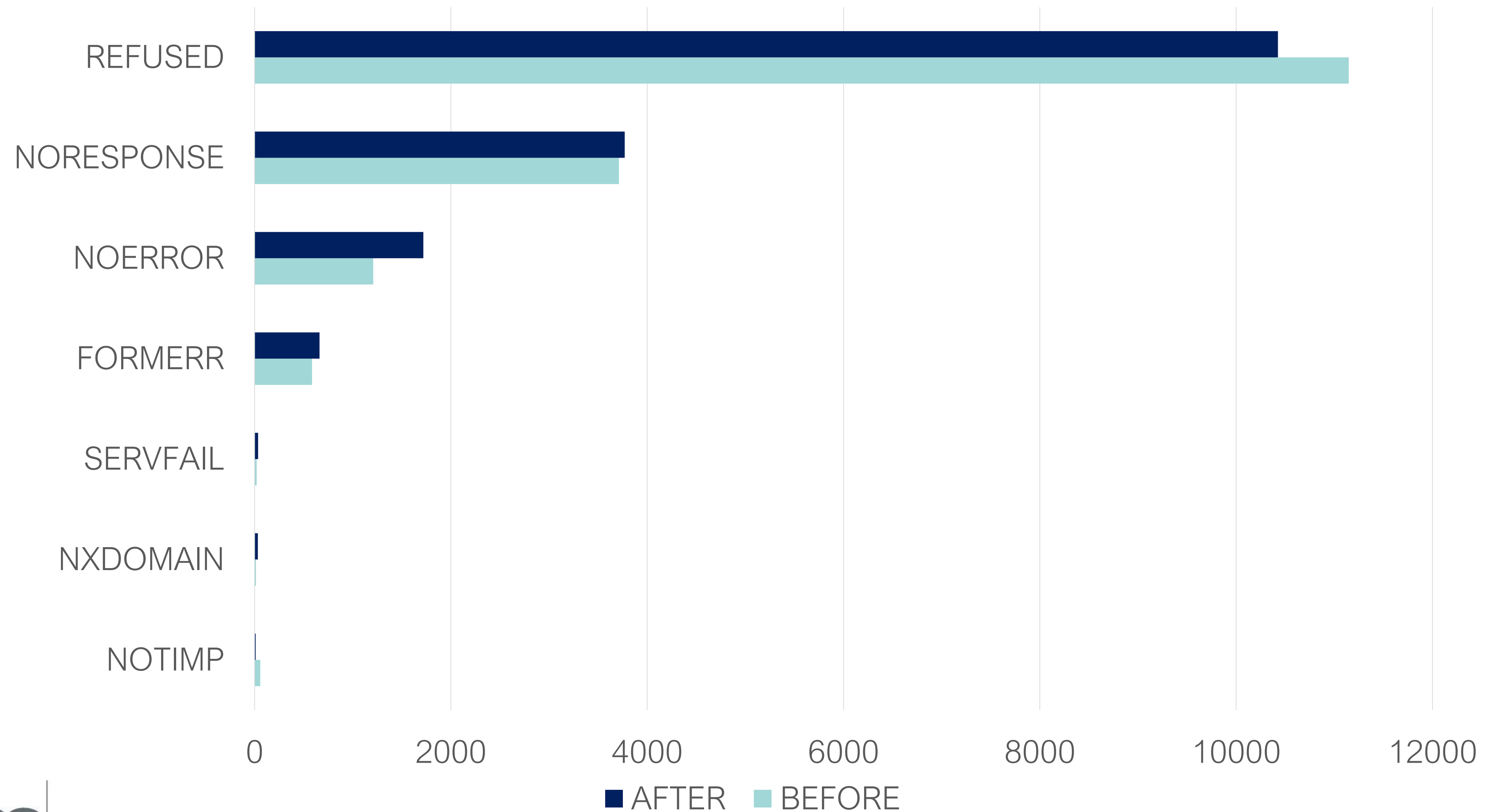
Comparison Minimal Edns



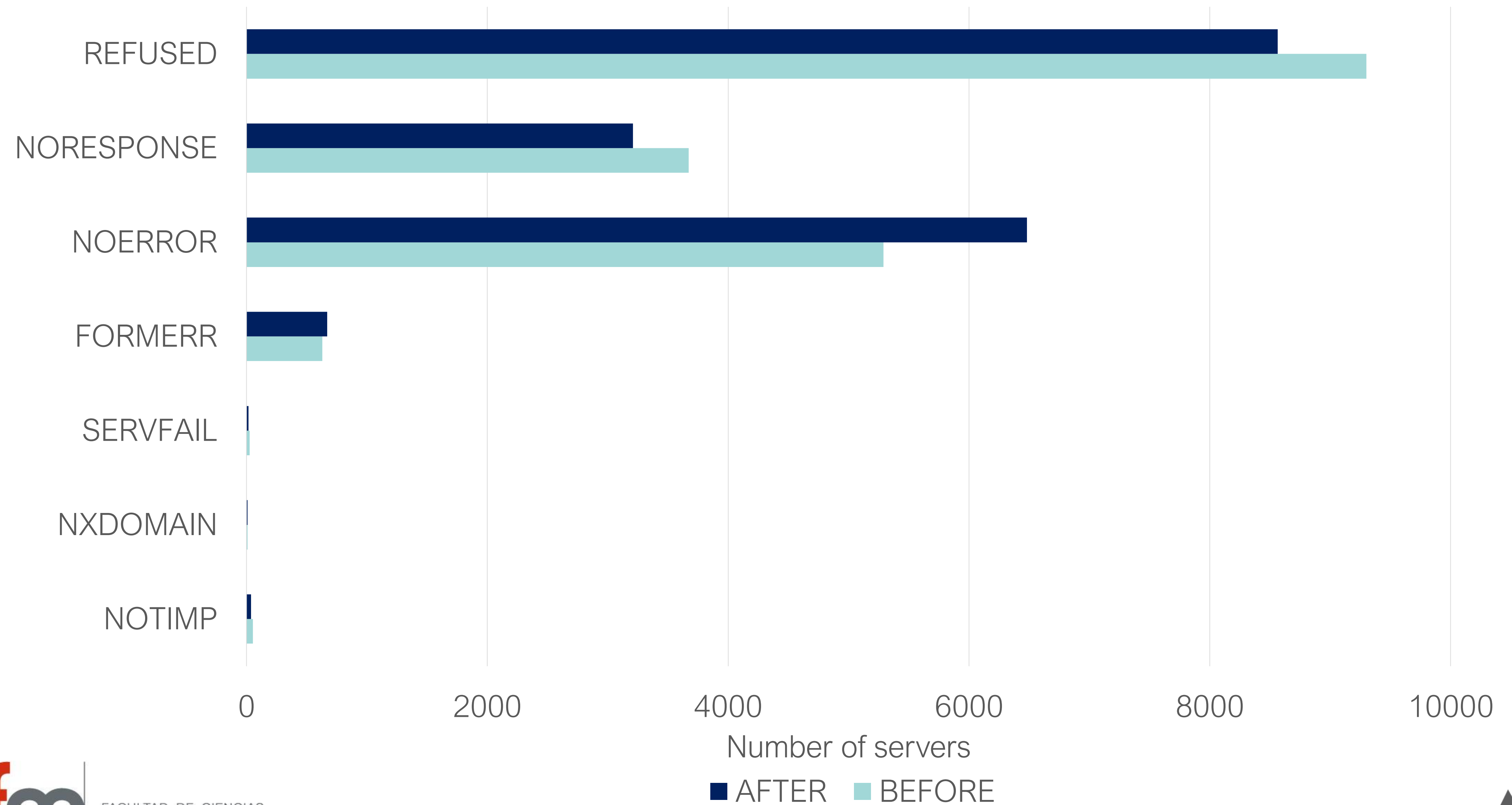
Number of Servers

■ AFTER ■ BEFORE

Chain query in DNS - RFC 7901






Client Subnet in DNS- RFC 7871



OPTcodes comparison

	Before	After
OPTcode 13	170 serv	413 serv
OPTcode 8	265 serv	631 serv
OPTcode 12	478 serv	792 serv

Summary Algorithm classification

	Before	After
 OK	714 serv	1084 serv
 Warnings	15813 serv	16518 serv
 Not EDNS	2534 serv	1459 serv



Thanks!

Questions?



<https://github.com/niclabs/testResolvers/tree/edns/resolvertests>



jeisson@niclabs.cl



fcfm

FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

NIC
CHILE
RESEARCH LABS