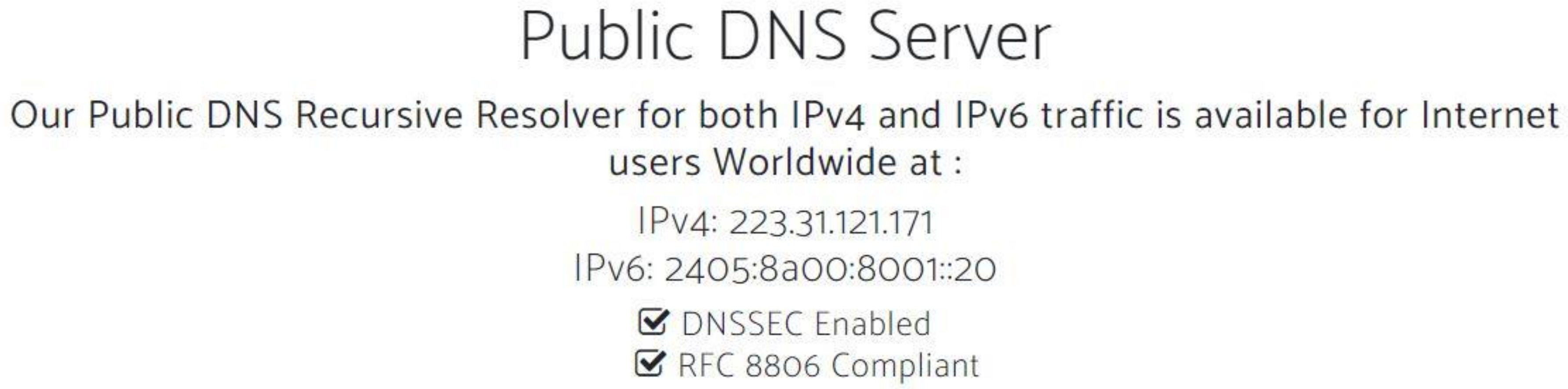
Centre of Excellence in DNS SECURITY

# Advanced DNS Security Training in association with ICANN

**24th November 2020 to 27th November 2020**

**03:00 PM - 05:00 PM**



## Public DNS Server

Our Public DNS Recursive Resolver for both IPv4 and IPv6 traffic is available for Internet users Worldwide at :

IPv4: 223.31.121.171

IPv6: 2405:8a00:8001::20

☑ DNSSEC Enabled

☑ RFC 8806 Compliant

Ministry of Electronics and
Information Technology
Government of India

ICANN nixi

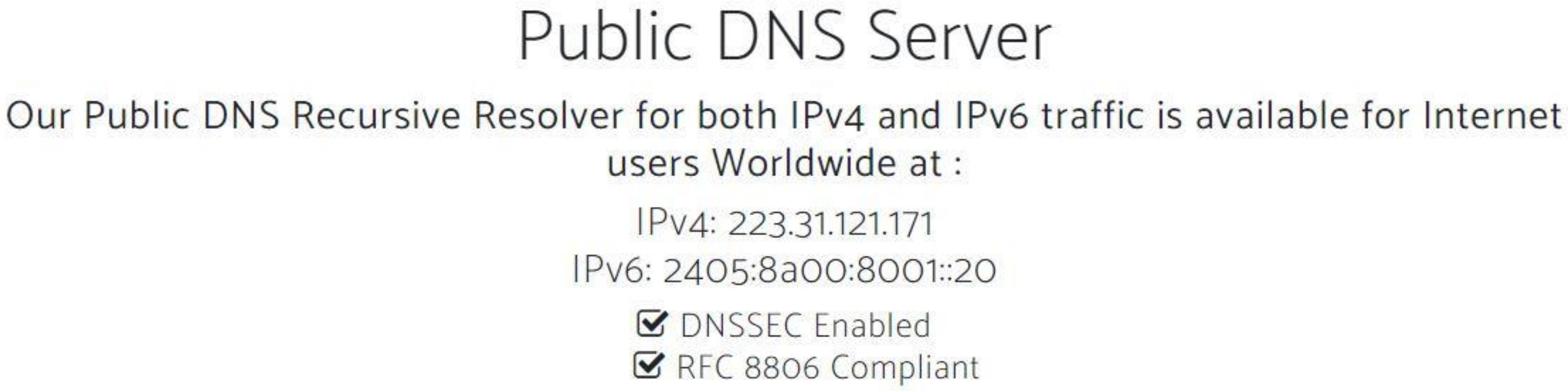
सी-डैक CDAC प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Centre of Excellence in DNS SECURITY

# Recursive/Caching Authoritative DNS Server Configuration

**24th November 2020 to 27th November 2020**

**03:00 PM - 05:00 PM**



## Public DNS Server

Our Public DNS Recursive Resolver for both IPv4 and IPv6 traffic is available for Internet users Worldwide at :

IPv4: 223.31.121.171

IPv6: 2405:8a00:8001::20

☑ DNSSEC Enabled

☑ RFC 8806 Compliant

Ministry of Electronics and
Information Technology
Government of India

nixi

सी डैक CDAC प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

# Agenda

- Recursive/Caching Server configuration
  - Introduction
  - Bind Components
  - DIG – Domain Information Groper
  - Methodology for setting up DNS server using BIND
- Authoritative DNS Server Configuration
  - Zone file and its details
- References
- Q & A

# Introduction

- BIND is the most popular Domain Name System (DNS) server.
- It is FOSS (Free & Open Source Software)
- BIND means Berkeley Internet Name Domain.
- It was developed in the 1980s at the University of Berkeley.
- It can be used both as a Caching Server as well as an Authoritative Server.
- The demonstrations are based on Bind 9.16.6

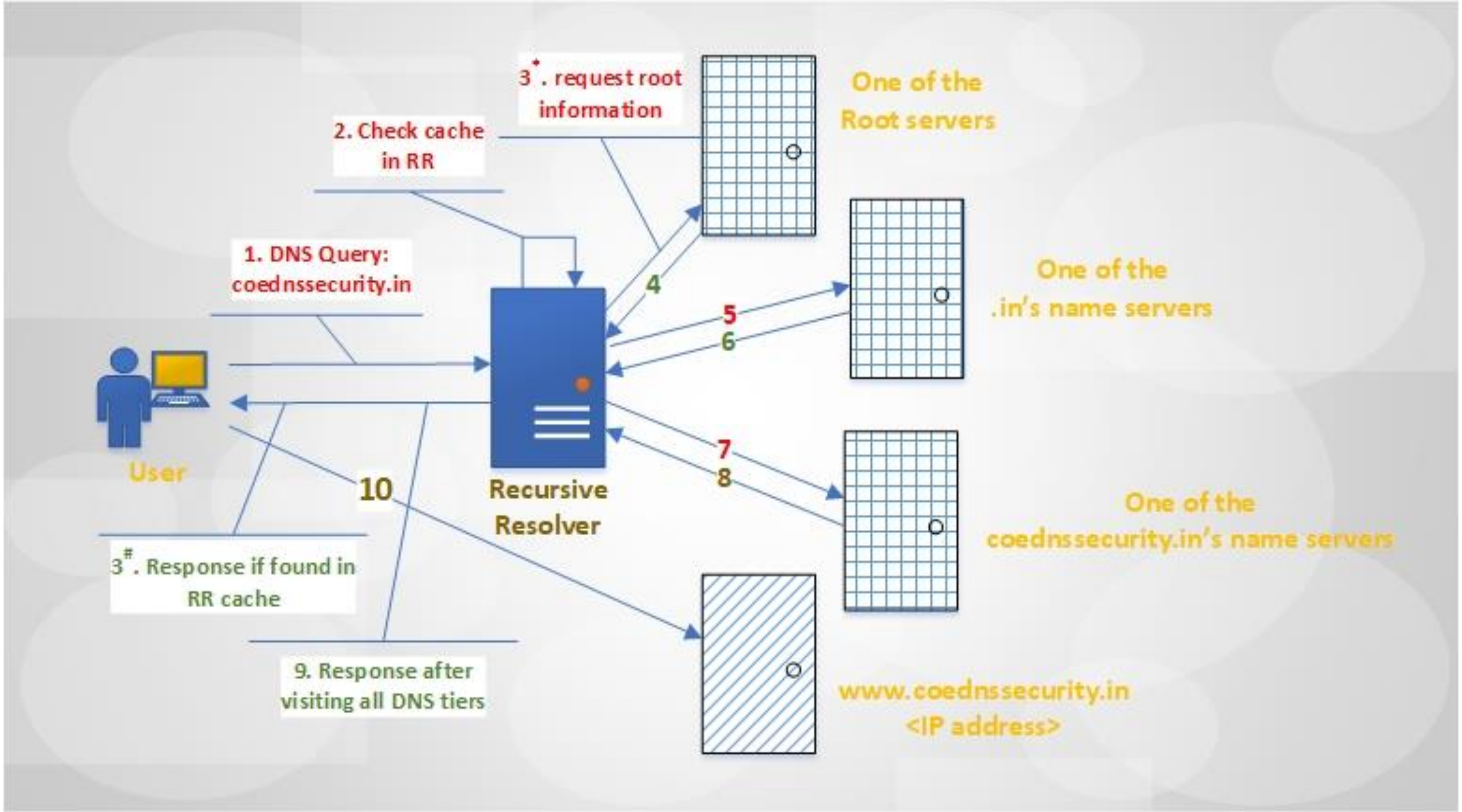
# BIND Components

- *Name Server.*
  - Maintains a DNS Zone file and responds to DNS Requests
  - Acts either as a Caching only Name Server (Recursive Resolver) or Authoritative Name Server.
- *Lightweight Resolver.*
  - It contains a lightweight resolver library that can be run on DNS clients like host Operating System and routers
  - It also contains resolver daemon process which can run on a local host.
- *Name Server Tools.*
  - **dig** - allows users to resolve DNS queries
  - **host** - converts hostnames to IP addresses
  - **nslookup** - queries DNS servers for information about hosts and domains
  - **named-checkconf :** This tool checks the syntax of *named.conf* file
  - **Remote Name Daemon Control (rndc)**
    - Remote Name Daemon Control
    - It allows the System Administrators to control the operation of a name server over a TCP connection

# DIG – Domain Information Groper

- DIG is an administrative tool for querying DNS Name Servers
- It is useful for performing DNS Lookups and displays the answers that are returned from the name server
- It is also useful for verifying and troubleshooting DNS Problems

# DNS Query Resolution


3*. request root information
2. Check cache in RR
1. DNS Query: coednssecurity.in
User
4
5
6
7
8
10
Recursive Resolver
One of the Root servers
One of the .in's name servers
One of the coednssecurity.in's name servers
3#. Response if found in RR cache
9. Response after visiting all DNS tiers
www.coednssecurity.in <IP address>

*"In the conventional approach, the RR server spends considerable time to reach out to the closest root server"*

# Methodology for setting up DNS server using BIND

- To install from Linux repository on CentOS:
  - *yum install –y bind bind-utils*
- To download the BIND package, and install:
  - Bind 9.16.6 Software: https://coednssecurity.in/pdf/bind-9.16.6.tar.xz
  - Bind 9.16.6 Manual: https://coednssecurity.in/pdf/DNS-Bind-Server-Installation-Configuration.pdf
- Setting up Recursive/Caching Server

# Authoritative DNS Server

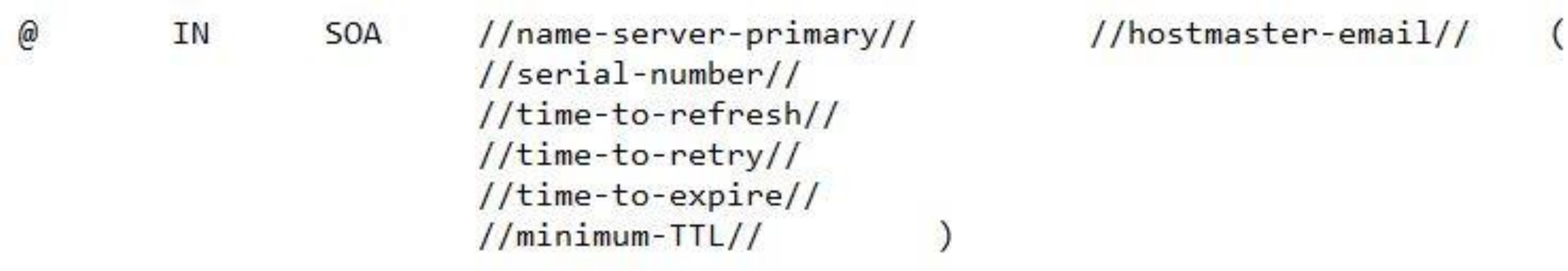
- An Authoritative DNS Server is the nameserver that provides an authoritative answer to the queries from Recursive DNS nameserver.
- Types:
  - Root Servers
  - Primary
  - Secondary

# Authoritative DNS Server: Zone file

- DNS Zone file is the text file containing all DNS zone information.
- Format: RFC 1035
- Parts of Zone file:
  - “$ORIGIN” – start of a DNS zone file, it appends to all labels to form FQDN, if the label doesn’t end with a period
  - “@” – indicates $ORIGIN should replace it
  - “SOA” – Start of Authority (SOA) record follows “$ORIGIN”

# Authoritative DNS Server: Zone file

- Parts of Zone file:
  - “SOA” – Start of Authority (SOA) record follows “$ORIGIN”

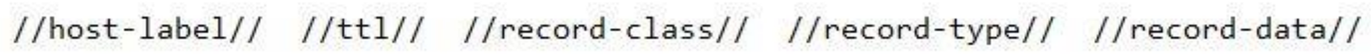


```
@       IN      SOA     //name-server-primary//         //hostmaster-email//    (
                        //serial-number//
                        //time-to-refresh//
                        //time-to-retry//
                        //time-to-expire//
                        //minimum-TTL//          )
```

  - *name-server-primary*: contains the original zone file
  - *serial-number*: version number
  - *time-to-refresh*: waiting time for secondary servers to check change in serial (seconds)
  - *time-to-retry*: waiting time for secondary servers after a failed attempt to update zone (seconds)
  - *time-to-expire*: time for *time-to-retry* to expire
  - *minimum-TTL*: caching time of negative response (seconds)

# Authoritative DNS Server: Resource Record

- Parts of Resource Record:
  - A zone file can contain many resource records.



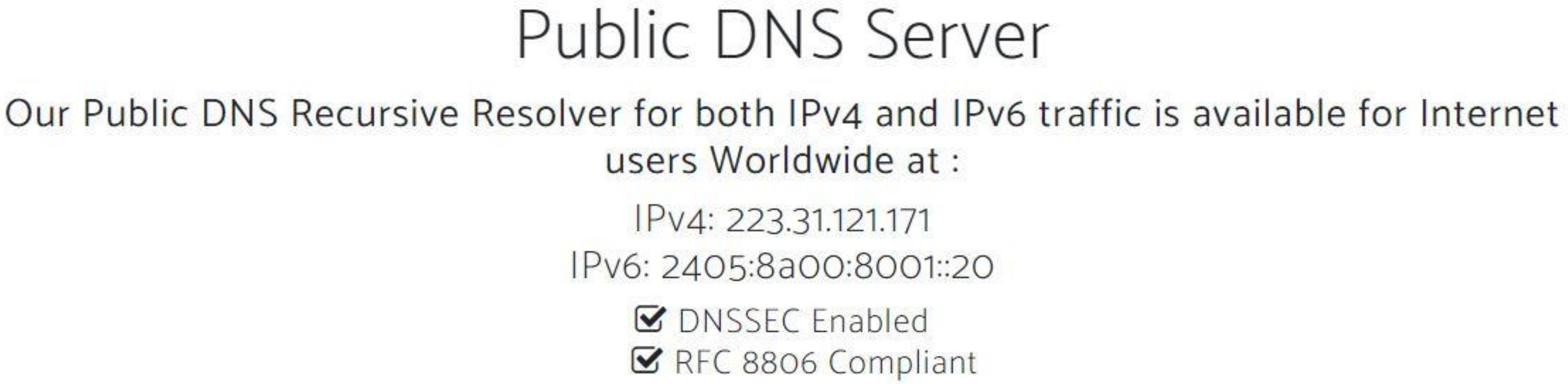
```
//host-label//  //ttl//  //record-class//  //record-type//  //record-data//
```

  - *host-label*: defines hostname of a record and “$ORIGIN” appends to it
  - *ttl*: caching time of the DNS record
  - *record-class*: usually “IN”
  - *record-type*: common types are- A, AAAA, NS, SOA, MX, CNAME
  - *record-data*: the data to returned as the answer/reply

# References

- Bind 9.16.6 Software: https://coednssecurity.in/pdf/bind-9.16.6.tar.xz
- Bind 9.16.6 Manual: https://coednssecurity.in/pdf/DNS-Bind-Server-Installation-Configuration.pdf
- Bind Administration Manual: https://bind9.readthedocs.io/en/v9_16_7/
- RFC 1035: https://tools.ietf.org/html/rfc1035

# Q & A



## Public DNS Server

Our Public DNS Recursive Resolver for both IPv4 and IPv6 traffic is available for Internet users Worldwide at :

IPv4: 223.31.121.171

IPv6: 2405:8a00:8001::20

☑ DNSSEC Enabled

☑ RFC 8806 Compliant

Please help us improve our email security solution by forwarding your spam emails to our SPAM BOX at:

**spam@coednssecurity.in**

*Thank you*