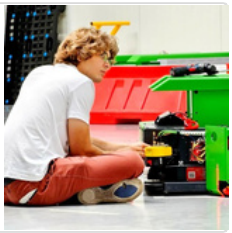
DNS Bind9: The Biggest Phonebook Ever Created

Check GitHub for helpful DevOps tools:

Michael Robotics
Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats information overload by adhering to the set of principles: simplify, prioritize, and execute.

https://github.com/MichaelRobotics



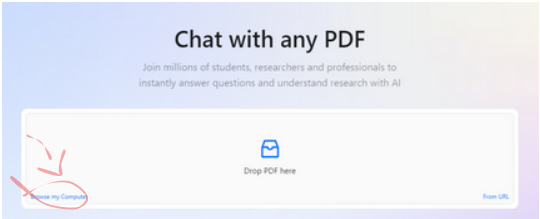
Ask Personal AI Document assistant to learn interactively (FASTER)!

1. Download PDF
2. Go to website
3. Browse file
4. Chat with Document

1 https://github.com/MichaelRobotics/DevOpsTools/blob/main/DNS.pdf

Click there to go to ChatPdf website 2

3



Ask questions about document! 4

Complety new to Linux and Networking?

Essential for this PDF is a thorough knowledge of networking. I highly recommend the HTB platform's networking module, which offers extensive information to help build a comprehensive understanding.

HTB - Your Cyber Performance Center

We provide a human-first platform creating and maintaining high performing cybersecurity individuals and organizations.

https://www.hackthebox.com/

What DNS?

DNS (Domain Name System) is the system that translates human-readable domain names (like example.com) into machine-friendly IP addresses, allowing web browsers to locate and load websites. It acts as the Internet's "phonebook," eliminating the need to remember complex IP addresses for every online resource.

How DNS work?

The process of converting human-readable domain names, like "example.com," into machine-readable IP addresses involves several DNS servers working in sequence. These include recursive resolvers, root servers, TLD (top-level domain) servers, and authoritative servers, which collaborate to efficiently locate and return the correct IP address for a requested domain.

DNS: Why and When

DNS is essential because it translates human-readable domain names, like "example.com," into machine-readable IP addresses. Since it's impractical for people to remember complex numeric IP addresses, DNS simplifies the process of accessing websites, allowing users to use easy-to-remember names instead of having to recall intricate strings of numbers.

DNS performs this translation whenever a user enters a domain name into their web browser. For example, when you type "nytimes.com" into your browser, DNS translates this name into the corresponding IP address to load the New York Times website.

System Requirements

- 1 GB RAM (minimum, 2 GB recommended for better performance)
- 10 GB free storage (more may be required depending on the size of the DNS zone files and logs)
- Ubuntu 22.04

If you want to install it on a different Linux distro, ask in the comments and I will write an Ansible playbook or bash script.

DNS: Main components & packages

- bind9 – The BIND DNS server itself, providing the DNS service.
- dnsutils – A package containing command-line tools like dig, nslookup, and host for DNS troubleshooting and queries.

DNS Server: How to setup on Linux

1) Install bind9

```
sudo apt-get update && sudo apt-get install -y bind9 dnsutils
```

2) configure forwarders

In this stage of BIND9 setup, you specify external DNS servers (like your ISP's or public DNS servers) that your BIND9 server will forward queries to if it doesn't have the answer. This helps reduce query resolution time and improves reliability by using upstream DNS servers such as Google's (8.8.8.8 and 8.8.4.4) for recursive queries.

named.conf.options

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

     forwarders {
        8.8.8.8;
        8.8.4.4;
     };

    //========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //========================================================================
    dnssec-validation auto;
```

3) Configure zones

Define specific DNS zones for which your server will provide authoritative answers. The provided named.conf.local configuration specifies the master zones, including the domain class.home with its corresponding database file (/etc/bind/db.example.com) and the reverse lookup zone for the IP range 192.168 with the database file (/etc/bind/db.10).

named.conf.local

```
//
// Do any local configuration here
//
zone "class.home" {
    type master;
    file "/etc/bind/db.example.com";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10";
};
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

4) Configure forward DNS zone

Create a DNS zone file that defines how domain names are resolved to IP addresses within your specified domain. The provided BIND data file for class.home includes key records such as the Start of Authority (SOA), Name Server (NS), and Address (A) records, mapping the domain and its associated resources to the appropriate IP addresses (192.168.1.21 and ::1).

db.example.com

```
;
; BIND data file for class.home
;
$TTL  604800
@       IN      SOA     class.home. root.class.home. (
                                3     ; Serial
                           604800     ; Refresh
                            86400     ; Retry
                          2419200     ; Expire
                           604800 )   ; Negative Cache TTL
;
@       IN      NS      ad1.class.home.
@       IN      A       192.168.1.21
@       IN      AAAA    ::1
ad1     IN      a       192.168.1.21
```

5) Configure reverse DNS zone

Create a reverse zone file that maps IP addresses back to their corresponding domain names, allowing for reverse DNS lookups. The provided BIND reverse data file includes the Start of Authority (SOA) record and a Pointer (PTR) record, linking the IP address 1.0.0 to the domain ad1.class.home, thus enabling reverse resolution for that address.

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@   IN  SOA ad1.class.home. root.class.home. (
                3     ; Serial
           604800     ; Refresh
            86400     ; Retry
          2419200     ; Expire
           604800 )   ; Negative Cache TTL
;
@   IN  NS  ad1.
1.0.0   IN  PTR ad1.class.home
```

6) Test DNS server

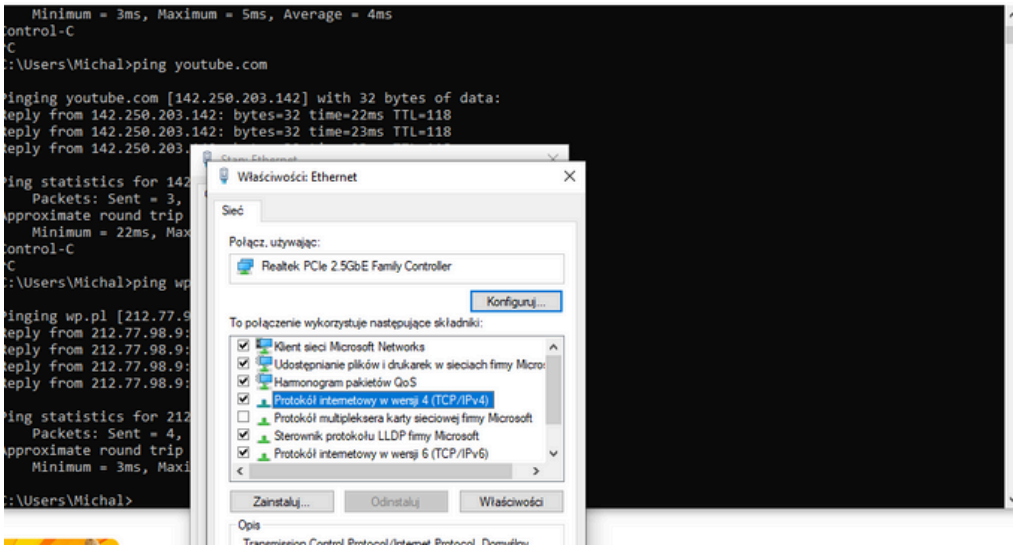
Ping on your local machine, to test DNS server availability

```
laptopdev@laptopdev2:/etc/bind$ ping ad1.example.home
ping: ad1.example.home: Name or service not known
laptopdev@laptopdev2:/etc/bind$ ping ad1.class.home
PING ad1.class.home (192.168.1.21) 56(84) bytes of data.
64 bytes from 192.168.1.21 (192.168.1.21): icmp_seq=1 ttl=64 time=0.130 ms
64 bytes from 192.168.1.21 (192.168.1.21): icmp_seq=2 ttl=64 time=0.072 ms
64 bytes from 192.168.1.21 (192.168.1.21): icmp_seq=3 ttl=64 time=0.080 ms
^C
--- ad1.class.home ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.072/0.094/0.130/0.025 ms
laptopdev@laptopdev2:/etc/bind$
```

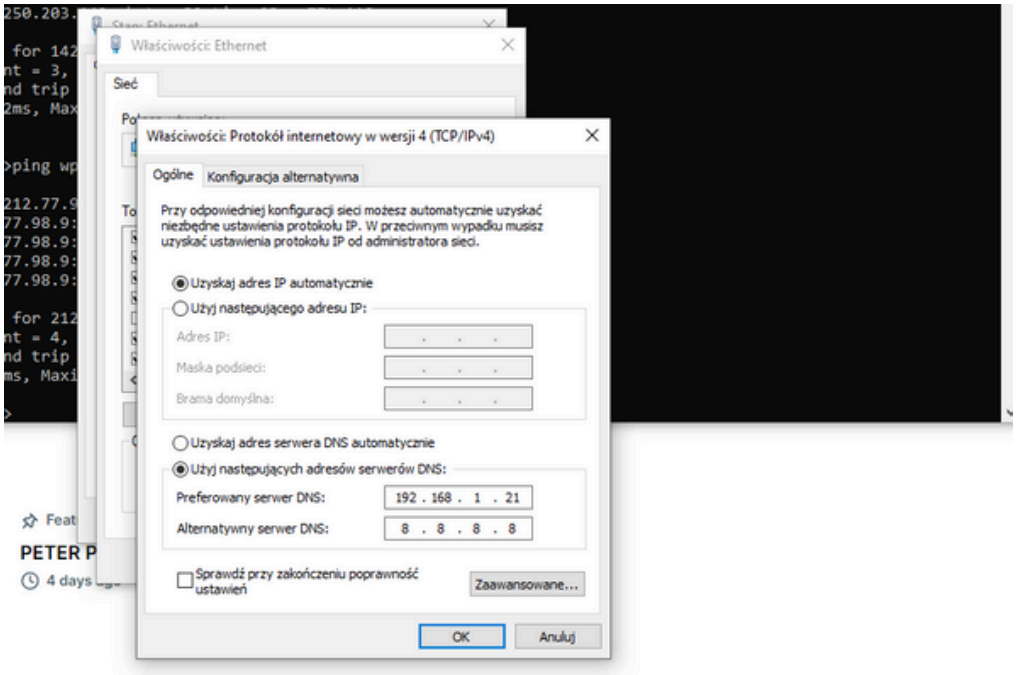
DNS server pings back: everything is setup correctly.

Next, set up the appropriate DNS server records on another host in the same network

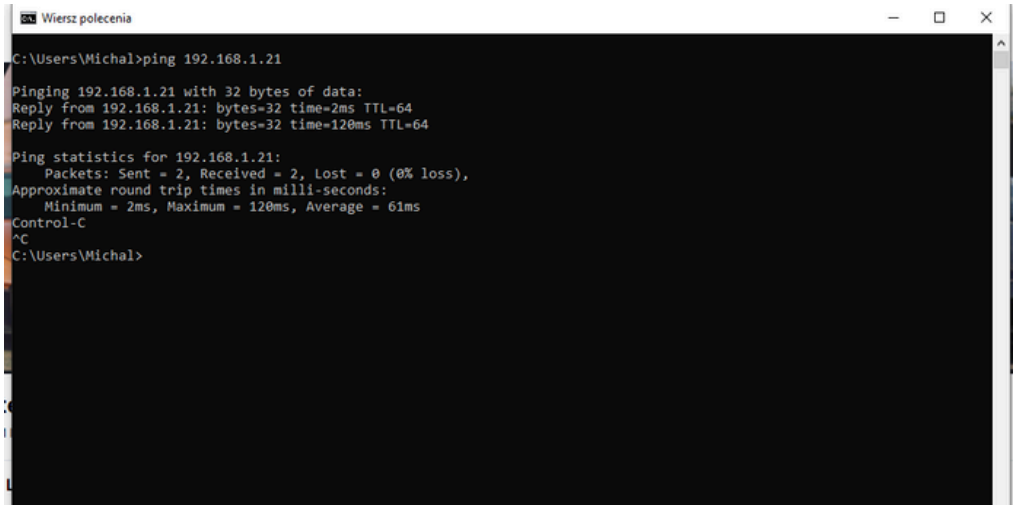
(in my case, the host is running Windows



Configure settings accordingly to your DNS server:



Ping any domain and ad1.class.home



Voilà! You have successfully set up your BIND9 DNS server!

Common troubleshooting

1) "SERVFAIL" Responses

Missing or misconfigured forwarders. Ensure the correct forwarders are defined if using forwarding

2) "REFUSED" Responses

Misconfigured ACLs (Access Control Lists) or allow-query directives, preventing certain clients from querying the server. Check ACLs and allow-query settings in named.conf to ensure the clients are permitted to make queries.

3) "NXDOMAIN" Responses

The DNS server returns a NXDOMAIN response, indicating that the queried domain name does not exist. Verify the correct spelling of the domain in the zone file.

4) **Check the bind9 man page**

5) **If everything is a complete mess**

Remove the bind9 and revert the configuration to its previous state.

DNS Server: How to remove

1) stop bind9 service

my was named "Wired connection 1"

```
$ sudo systemctl stop bind9
```

2) Uninstall bind9 and all of its configuration files

```
$ sudo apt-get purge bind9 -y
```

3) Uninstall dnsutils and all of its configuration files

```
$ sudo apt-get purge dnsutils -y
```

Learn more about DNS

Check BIND9, they have great docs

Why use BIND 9?

BIND 9 has evolved to be a very flexible, full-featured DNS system

https://www.isc.org/support/

Share, comment, DM and check GitHub for scripts & playbooks created to automate process.

Check my GitHub

Michael Robotics
Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats skill information overload by adhering to the set of principles: simplify, prioritize, and execute.

https://github.com/MichaelRobotics

PS.

If you need a playbook or bash script to manage KVM on a specific Linux distribution, feel free to ask me in the comments or send a direct message!