

## Konfiguracja serwera DNS na Ubuntu 20

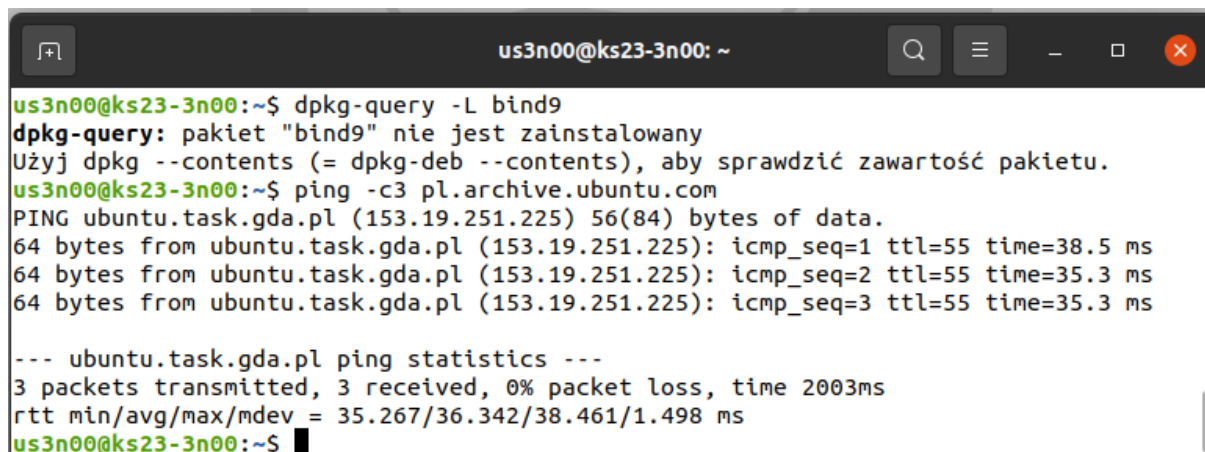
Usługa nazw domen (DNS) to usługa internetowa, która mapuje nawzajem adresy IP i w pełni kwalifikowane nazwy domen (FQDN). W ten sposób DNS łagodzi potrzebę zapamiętywania adresów IP. Komputery z systemem DNS nazywane są *serwerami nazw*. Ubuntu jest dostarczany z BIND (Berkley Internet Naming Daemon), najpopularniejszym programem używanym do utrzymywania serwera nazw w systemie Linux.

Autorytatywny serwer DNS jest używany przez właścicieli nazw domen do przechowywania rekordów DNS. Zapewnia autorytatywne odpowiedzi dla resolverów DNS (takich jak 8.8.8.8 czy 1.1.1.1), które wyszukują rekordy DNS w imieniu użytkowników końcowych.

### Instalacja

Przed przystąpieniem do instalacji odpowiedniego oprogramowania, należy:

- sprawdzić czy pakiet nie jest zainstalowany `dpkg-query -L bind9`
- sprawdzić dostęp do Internetu np. `ping -c3 pl.archive.ubuntu.com`



```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ dpkg-query -L bind9
dpkg-query: pakiet "bind9" nie jest zainstalowany
Użyj dpkg --contents (= dpkg-deb --contents), aby sprawdzić zawartość pakietu.
us3n00@ks23-3n00:~$ ping -c3 pl.archive.ubuntu.com
PING ubuntu.task.gda.pl (153.19.251.225) 56(84) bytes of data.
64 bytes from ubuntu.task.gda.pl (153.19.251.225): icmp_seq=1 ttl=55 time=38.5 ms
64 bytes from ubuntu.task.gda.pl (153.19.251.225): icmp_seq=2 ttl=55 time=35.3 ms
64 bytes from ubuntu.task.gda.pl (153.19.251.225): icmp_seq=3 ttl=55 time=35.3 ms

--- ubuntu.task.gda.pl ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 35.267/36.342/38.461/1.498 ms
us3n00@ks23-3n00:~$

```

- Zaktualizować system i jego komponenty  
`sudo apt update`

Aby zainstalować BIND 9, narzędzia, dokumentację na Ubuntu 20.04 z domyślnego repozytorium, trzeba uruchomić następujące polecenie: (BIND 9 to aktualna wersja)

```
sudo apt-get install bind9 bind9utils bind9-doc bind9-host
```

Po instalacji można sprawdzić wersję.

```
named -v
```

Aby sprawdzić numer wersji i opcje kompilacji, uruchomiamy:

```
named -V
```

```

us3n00@ks23-3n00: ~$ named -v
BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
us3n00@ks23-3n00: ~$ named -V
BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
running on Linux x86_64 5.4.0-96-generic #109-Ubuntu SMP Wed Jan 12 16:49:16 UTC 2022
built by make with '--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=/usr/include' '--mandir=/usr/s
hare/man' '--infodir=/usr/share/info' '--sysconfdir=/etc' '--localstatedir=/var' '--disable-silent-rules'
 '--libdir=/usr/lib/x86_64-linux-gnu' '--runstatedir=/run' '--disable-maintainer-mode' '--disable-dependenc
y-tracking' '--libdir=/usr/lib/x86_64-linux-gnu' '--sysconfdir=/etc/bind' '--with-python=python3' '--local
statedir=/ ' '--enable-threads' '--enable-largefile' '--with-libtool' '--enable-shared' '--enable-static' '
--with-gost=no' '--with-openssl=/usr' '--with-gssapi=/usr' '--with-libidn2' '--with-json-c' '--with-lmdb=/
usr' '--with-gnu-ld' '--with-maxminddb' '--with-atf=no' '--enable-ipv6' '--enable-rrl' '--enable-filter-aa
aa' '--disable-native-pkcs11' '--disable-isc-spnego' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-g -O2 -fdebug
-prefix-map=/build/bind9-e4rzcc/bind9-9.16.1=. -fstack-protector-strong -Wformat -Werror=format-security -
fno-strict-aliasing -fno-delete-null-pointer-checks -DNO_VERSION_DATE -DDIG_SIGCHASE' 'LDFLAGS=-Wl,-Bsymbo
lic-functions -Wl,-z,relro -Wl,-z,now' 'CPPFLAGS=-Wdate-time -D_FORTIFY_SOURCE=2'
compiled by GCC 9.3.0
compiled with OpenSSL version: OpenSSL 1.1.1f 31 Mar 2020
linked to OpenSSL version: OpenSSL 1.1.1f 31 Mar 2020
compiled with libxml2 version: 2.9.10
linked to libxml2 version: 20910
compiled with json-c version: 0.13.1
linked to json-c version: 0.13.1
compiled with zlib version: 1.2.11
linked to zlib version: 1.2.11
linked to maxminddb version: 1.4.2
threads support is enabled

default paths:
  named configuration: /etc/bind/named.conf
  rndc configuration: /etc/bind/rndc.conf
  DNSSEC root key: /etc/bind/bind.keys
  nsupdate session key: //run/named/session.key
  named PID file: //run/named/named.pid
  named lock file: //run/named/named.lock
  geoip-directory: /usr/share/GeoIP
us3n00@ks23-3n00: ~$

```

Domyślnie BIND uruchamia się automatycznie po instalacji.

Jeśli jednak chcemy go uruchomić, wpisujemy:

**sudo systemctl start named**

Aby sprawdzić jego status wpisujemy polecenie:

**sudo systemctl status named**

```

us3n00@ks23-3n00: ~$ sudo systemctl start named
[sudo] hasło użytkownika us3n00:
us3n00@ks23-3n00: ~$ sudo systemctl status named
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-02-24 08:33:19 UTC; 1h 0min ago
     Docs: man:named(8)
    Main PID: 4216 (named)
      Tasks: 5 (limit: 2268)
     Memory: 15.5M
    CGroup: /system.slice/named.service
            └─4216 /usr/sbin/named -f -u bind

lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './NS/IN': 2001:7fe::53#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
lut 24 08:33:20 ks23-3n00 named[4216]: network unreachable resolving './NS/IN': 2001:dc3::35#53
lut 24 08:33:20 ks23-3n00 named[4216]: managed-keys-zone: Initializing automatic trust anchor management
lut 24 08:33:20 ks23-3n00 named[4216]: resolver priming query complete
us3n00@ks23-3n00: ~$

```

Automatyczne uruchamianie w czasie rozruchu włącza polecenie:

**sudo systemctl enable named**

```

us3n00@ks23-3n00: ~$ sudo systemctl enable named
Synchronizing state of named.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable named
us3n00@ks23-3n00: ~$

```

Serwer BIND będzie działał jako bind. System utworzony podczas instalacji nasłuchuje na porcie 53TCP i UDP, co można zobaczyć, uruchamiając następujące polecenia:

**sudo apt install net-tools** – instaluje narzędzia sieciowe

**sudo netstat -lnptu | grep named**

```

us3n00@ks23-3n00: ~$ sudo netstat -lnptu | grep named
tcp        0      0 10.0.2.15:53          0.0.0.0:*               LISTEN      842/named
tcp        0      0 172.22.0.11:53        0.0.0.0:*               LISTEN      842/named
tcp        0      0 172.22.0.2:53         0.0.0.0:*               LISTEN      842/named
tcp        0      0 172.22.0.1:53         0.0.0.0:*               LISTEN      842/named
tcp        0      0 127.0.0.1:53          0.0.0.0:*               LISTEN      842/named
tcp        0      0 127.0.0.1:953         0.0.0.0:*               LISTEN      842/named
tcp6       0      0 fe80::a00:27ff:fe52::53 :::*                   LISTEN      842/named
tcp6       0      0 fe80::a00:27ff:fe52::53 :::*                   LISTEN      842/named
tcp6       0      0 ::1:53                :::*                   LISTEN      842/named
tcp6       0      0 ::1:953                :::*                   LISTEN      842/named
udp        0      0 10.0.2.15:53          0.0.0.0:*               842/named
udp        0      0 172.22.0.11:53        0.0.0.0:*               842/named
udp        0      0 172.22.0.2:53         0.0.0.0:*               842/named
udp        0      0 172.22.0.1:53         0.0.0.0:*               842/named
udp        0      0 127.0.0.1:53          0.0.0.0:*               842/named
udp6       0      0 ::1:53                :::*                   842/named
udp6       0      0 fe80::a00:27ff:fe52::53 :::*                   842/named
udp6       0      0 fe80::a00:27ff:fe52::53 :::*                   842/named
us3n00@ks23-3n00: ~$

```

Zwykle zapytania DNS są wysyłane do portu UDP 53. Port TCP 53 jest przeznaczony dla odpowiedzi większych niż 512 bajtów.

Demon BIND nazywa się named. (Demon to oprogramowanie działające w tle). Plik binarny named jest instalowany przez pakiet bind9. Jest jeszcze jeden ważny plik binarny: rndc - zdalny kontroler demona nazw, który jest instalowany przez pakiet bind9utils. Plik binarny rndc służy do przeładowywania / zatrzymywania i kontrolowania innych aspektów demona BIND. Komunikacja odbywa się przez port TCP 953.

Status zdalnego kontrolera demona nazw, możemy sprawdzić poleceniem:

**sudo rndc status**

```

us3n00@ks23-3n00: ~$ sudo rndc status
version: BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
running on ks23-3n00: Linux x86_64 5.4.0-97-generic #110-Ubuntu SMP Thu Jan 13 18:22:13 UTC 2022
boot time: Fri, 04 Feb 2022 19:39:53 GMT
last configured: Fri, 04 Feb 2022 19:39:53 GMT
configuration file: /etc/bind/named.conf
CPUs found: 1
worker threads: 1
UDP listeners per interface: 1
number of zones: 102 (97 automatic)
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/900/1000
tcp clients: 0/150
TCP high-water: 0
server is up and running
us3n00@ks23-3n00: ~$

```

## Konfiguracja

Istnieje wiele sposobów konfiguracji BIND9. Niektóre z najczęstszych konfiguracji to buforujący serwer nazw, serwer główny i serwer pomocniczy.

- Po skonfigurowaniu jako buforujący serwer nazw BIND9 znajdzie odpowiedź na zapytania o nazwy i zapamięta odpowiedź, gdy domena zostanie ponownie zapytana.
- Jako serwer główny, BIND9 odczytuje dane strefy z pliku na swoim hoście i jest autorytatywny dla tej strefy.
- Jako serwer pomocniczy BIND9 pobiera dane strefy z innego serwera nazw, który jest autorytatywny dla strefy.

## Przegląd

Pliki konfiguracyjne DNS są przechowywane w katalogu `/etc/bind`. Podstawowym plikiem konfiguracyjnym jest `/etc/bind/named.conf`, który w układzie dostarczonym przez pakiet zawiera tylko te pliki.

- `/etc/bind/named.conf.options`: globalne opcje DNS
- `/etc/bind/named.conf.local`: dla twoich stref
- `/etc/bind/named.conf.default-zones`: domyślne strefy, takie jak localhost, jego rewers i wskazówki dotyczące roota

Główne serwery nazw były kiedyś opisane w pliku `/etc/bind/db.root`. Jest to teraz dostarczane w pliku `/usr/share/dns/root.hints` dostarczonym z `dns-root-datat` pakietem i jest wymienione w powyższym pliku konfiguracyjnym `named.conf.default-zones`

Możliwe jest skonfigurowanie tego samego serwera jako buforującego serwera nazw, podstawowego i pomocniczego: wszystko zależy od obsługiwanych stref. Serwer może być początkiem autorytetu (SOA) dla jednej strefy, zapewniając jednocześnie usługę dodatkową dla innej strefy. Cały czas świadczymy usługi buforowania dla hostów w lokalnej sieci LAN.

## Ustawianie domyślnego serwera rozpoznawania nazw DNS na serwerze Ubuntu 20

**Systemd-resolved** zapewnia narzędzie do rozpoznawania skrótów w systemie Ubuntu 20. Za pomocą tego polecenia można zobaczyć domyślny program rozpoznawania nazw rekurencyjnych.

```
systemd-resolve --status
```



```
us3n00@ks23-3n00: ~$ systemd-resolve --status
Global
    LLMNR setting: no
MulticastDNS setting: no
    DNSOverTLS setting: no
    DNSSEC setting: no
    DNSSEC supported: no
        DNSSEC NTA: 10.in-addr.arpa
                    16.172.in-addr.arpa
                    168.192.in-addr.arpa
                    17.172.in-addr.arpa
```

**Wskazówka:** jeśli powyższe polecenie nie zakończy się natychmiast, możesz je zakończyć, naciskając klawisz Q.

Jak widać, BIND nie jest wartością domyślną.

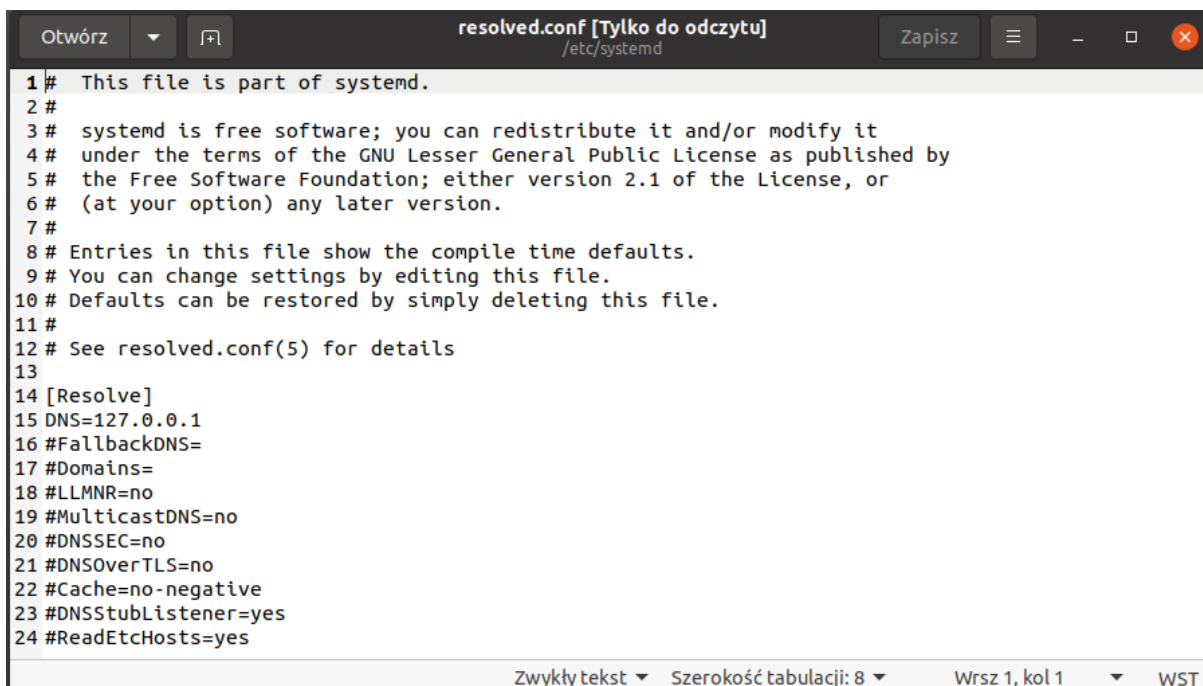
Aby ustawić BIND jako domyślny program rozpoznawania nazw, otwórz plik konfiguracyjny rozpoznawany przez systemd.

```
sudo nano /etc/systemd/resolved.conf
```

w sekcji [Resolve] , dodaj następujący wiersz.

```
DNS=127.0.0.1
```

Spowoduje to ustawienie globalnego serwera DNS dla twojego serwera. Zapisz i zamknij plik.



```
Otwórz ▼ resolved.conf [Tylko do odczytu] /etc/systemd
Zapisz
1 # This file is part of systemd.
2 #
3 # systemd is free software; you can redistribute it and/or modify it
4 # under the terms of the GNU Lesser General Public License as published by
5 # the Free Software Foundation; either version 2.1 of the License, or
6 # (at your option) any later version.
7 #
8 # Entries in this file show the compile time defaults.
9 # You can change settings by editing this file.
10 # Defaults can be restored by simply deleting this file.
11 #
12 # See resolved.conf(5) for details
13
14 [Resolve]
15 DNS=127.0.0.1
16 #FallbackDNS=
17 #Domains=
18 #LLMNR=no
19 #MulticastDNS=no
20 #DNSSEC=no
21 #DNSOverTLS=no
22 #Cache=no-negative
23 #DNSStubListener=yes
24 #ReadEtcHosts=yes
Zwyczajny tekst Szerokość tabulacji: 8 Wrsz 1, kol 1 WST
```

Następnie uruchom ponownie usługę rozwiązana przez systemd.



```
sudo systemctl restart systemd-resolved
```

i sprawdź domyślny program rozpoznawania nazw DNS.

```
systemd-resolve --status
```



```
us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ systemd-resolve --status
Global
    LLNMR setting: no
    MulticastDNS setting: no
    DNSOverTLS setting: no
    DNSSEC setting: no
    DNSSEC supported: no
    DNS Servers: 127.0.0.1
    DNSSEC NTA: 10.in-addr.arpa
```

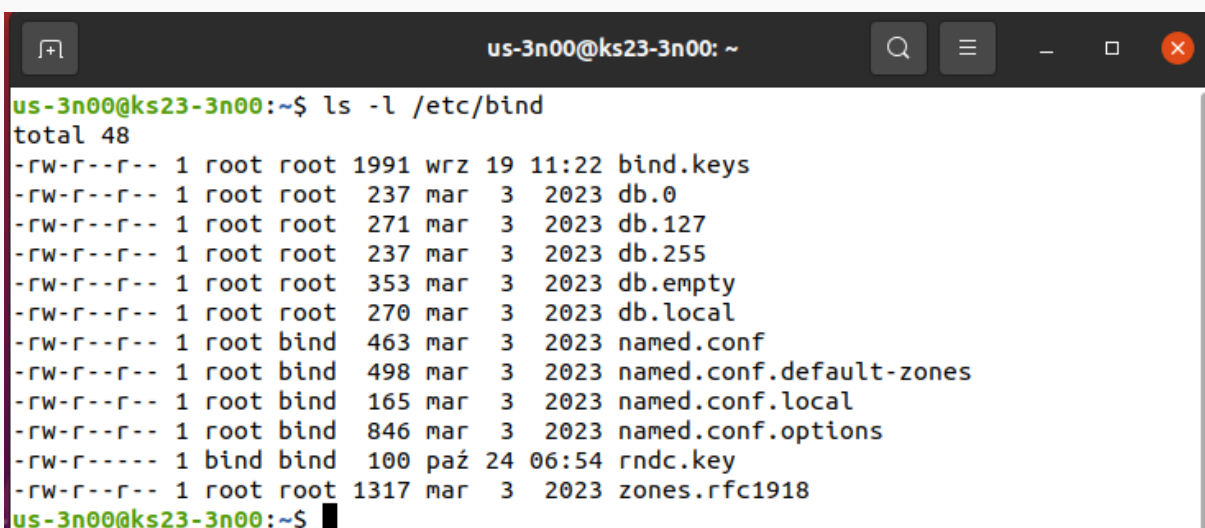
## Konfiguracja serwera głównego (autorytatywnego)

Naszym autorytatywnym serwerem DNS będzie nasz serwer **ks23-xyyy** z lokalnymi adresami IP: 172.22.y.1/24, 172.22.y.2/24 oraz 172.22.y.11.

Naszą podstawową domeną będzie **szkola.lokalna** powiązana z adresem 172.22.y.1.

Główny serwer DNS przechowuje główną kopię pliku strefy. Zmiany rekordów DNS są wprowadzane na tym serwerze. Domena może mieć jedną lub więcej stref DNS. Każda strefa DNS ma plik strefy, który zawiera rekordy DNS w tej strefie. Dla uproszczenia w tym materiale założono, że chcemy używać jednej strefy DNS do zarządzania wszystkimi rekordami DNS dla nazwy domeny.

Domyślnie, pliki konfiguracyjne znajdują się w **katalogu /etc/bind/**



```
us-3n00@ks23-3n00: ~
us-3n00@ks23-3n00:~$ ls -l /etc/bind
total 48
-rw-r--r-- 1 root root 1991 wrz 19 11:22 bind.keys
-rw-r--r-- 1 root root 237 mar 3 2023 db.0
-rw-r--r-- 1 root root 271 mar 3 2023 db.127
-rw-r--r-- 1 root root 237 mar 3 2023 db.255
-rw-r--r-- 1 root root 353 mar 3 2023 db.empty
-rw-r--r-- 1 root root 270 mar 3 2023 db.local
-rw-r--r-- 1 root bind 463 mar 3 2023 named.conf
-rw-r--r-- 1 root bind 498 mar 3 2023 named.conf.default-zones
-rw-r--r-- 1 root bind 165 mar 3 2023 named.conf.local
-rw-r--r-- 1 root bind 846 mar 3 2023 named.conf.options
-rw-r----- 1 bind bind 100 paź 24 06:54 rndc.key
-rw-r--r-- 1 root root 1317 mar 3 2023 zones.rfc1918
us-3n00@ks23-3n00:~$
```

W pliku **/etc/bind/named.conf.default-zones** są predefiniowane:

- ukryta strefa serwerów głównych, (root.hints)
- strefa localhost, (db.local)
- oraz lokalne strefy wyszukiwania wstecznego, (db.0, db.127, db.255)

```

1 // prime the server with knowledge of the root servers
2 zone "." {
3     type hint;
4     file "/usr/share/dns/root.hints";
5 };
6
7 // be authoritative for the localhost forward and reverse zones, and for
8 // broadcast zones as per RFC 1912
9
10 zone "localhost" {
11     type master;
12     file "/etc/bind/db.localhost";
13 };
14
15 zone "127.in-addr.arpa" {
16     type master;
17     file "/etc/bind/db.127";
18 };
19
20 zone "0.in-addr.arpa" {
21     type master;
22     file "/etc/bind/db.0";
23 };
24
25 zone "255.in-addr.arpa" {
26     type master;
27     file "/etc/bind/db.255";
28 };
29
30

```

**Dla nas tylko wartość informacyjna, nie edytujemy.**

Plik `/etc/bind/named.conf.options`, już znamy, zawiera podstawowe opcje konfiguracyjne.

Dyrektywa RFC 1918 wprowadza prywatną przestrzeń adresową.

Plik `zones.rfc1918` zawiera strefy wyszukiwania wstecznego tej prywatnej przestrzeni adresowej. **Dla nas tylko wartość informacyjna, nie edytujemy.**

Plik `/etc/bind/named.conf` jest podstawowym plikiem konfiguracyjnym serwera BIND DNS. Zawiera informacje, które pliki konfiguracyjne dołączamy.

```

1 // This is the primary configuration file for the BIND DNS server named.
2 //
3 // Please read /usr/share/doc/bind9/README.Debian.gz for information on the
4 // structure of BIND configuration files in Debian, *BEFORE* you customize
5 // this configuration file.
6 //
7 // If you are just adding zones, please do that in /etc/bind/named.conf.local
8
9 include "/etc/bind/named.conf.options";
10 include "/etc/bind/named.conf.local";
11 include "/etc/bind/named.conf.default-zones";

```

Aby zmienić BIND w serwer podstawowy należy dodać strefę DNS do BIND, edytując plik `/etc/bind/named.conf.local`

Aby skonfigurować strefę `szkola.lokalna` dodajemy wiersze np.:

```

zone "szkola.lokalna" {
    type master;
    file "/etc/bind/db.szkola.lokalna";
};

```

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ sudo nano /etc/bind/named.conf.local
us3n00@ks23-3n00:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "szkola.lokalna" {
    type master;
    file "/etc/bind/db.szkola.lokalna";
}

us3n00@ks23-3n00:~$

```

Powyższy wpis:

- utworzy nową strefę - klauzula **zone**,
- określa, że jest to strefa główna –type master
- plik strefy to **/etc/bind/db.szkola.lokalna**, w którym utworzymy rekordy DNS.

**Uwaga! W tej konfiguracji nie przewidujemy serwera pomocniczego, stąd brak transferu strefy, do podrzędnego serwera DNS.**

Gdybyśmy mieli serwer podrzędny, należałoby dopisać wiersz:

```
allow-transfer { xxx.xxx.xxx.xxx; };
```

gdzie xxx.xxx.xxx.xxx byłby adresem IP serwera podrzędnego

Aby nie tworzyć pliku strefy od początku, możemy użyć szablonu strefy np pliku **db.local**. Wystarczy skopiować zawartość **db.local** lub **db.empty** do nowego pliku.

```

sudo cp /etc/bind/db.local /etc/bind/db.szkola.lokalna
ls /etc/bind

```

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ sudo cp /etc/bind/db.local /etc/bind/db.szkola.lokalna
us3n00@ks23-3n00:~$ ls /etc/bind
bind.keys  db.empty      named.conf.default-zones  zones.rfc1918
db.0       db.local      named.conf.local
db.127     db.szkola.lokalna  named.conf.options
db.255     named.conf    rndc.key
us3n00@ks23-3n00:~$

```

Otrzymamy strukturę pliku do konfiguracji.



```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ cat /etc/bind/db.szkoła.lokalna
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
us3n00@ks23-3n00:~$

```

Plik strefy może zawierać 3 typy wpisów:

- **Comments - Komentarze:** zaczyna się od średnika (;)
- **Directives - Dyrektywy:** zaczyna się znaku dolara (\$)
- **Resource Records - Rekordy zasobów:** (@)

Plik strefy zazwyczaj składa się z następujących typów rekordów DNS.

- **Rekord SOA (Start of Authority)** : definiuje kluczowe cechy strefy. Jest to pierwszy rekord DNS w pliku strefy i jest obowiązkowy.
- **Rekord NS (serwer nazw)** : określa, które serwery są używane do przechowywania rekordów DNS i odpowiadania na zapytania DNS dotyczące nazwy domeny. W pliku strefy musi znajdować się co najmniej jeden rekord NS.
- **Rekord A (adresowy)** : Konwertuje nazwy DNS na adresy IPv4.
- **Rekord AAAA (Quad A)** : Konwertuje nazwy DNS na adresy IPv6.
- **Rekord CNAME (nazwa kanoniczna)** : służy do tworzenia aliasu dla nazwy DNS.
- **Rekord MX (Mail Exchanger)** : określa, które hosty są odpowiedzialne za dostarczanie wiadomości e-mail dla nazwy domeny.
- **Rekord TXT** : SPF, DKIM, DMARC itp.

Edytujemy plik strefy db.szkoła.lokalna.

Zmieniamy zawartość, na zgodną z poniższą treścią:

gdzie           xx       - to klasa  
                   a y lub yy   - to nr z dziennika  
 (u mnie to 3n00)

```

;
; Plik strefy szkola.lokalna
;
$TTL      604800      ; domyslny czas zycia strefy w [s]
$ORIGIN    szkola.lokalna.      ;definiowana domena - mozna pominac
;
;bazowe rekordy strefy okreslajace kluczowe cechy strefy
@          IN          SOA      ks23-xyy.szkola.lokalna root.szkola.lokalna. (
                                2022020901      ; Serial
                                604800           ; Refresh
                                86400            ; Retry
                                2419200         ; Expire
                                604800 )        ; Negative Cache TTL
;
;serwer nazw domeny szkola.lokalna
          IN          NS      ks23-xyy.szkola.lokalna.
;
;rekordy A
@          IN          A        172.22.y.1
ks23-xyy   IN          A        172.22.y.2
;
;rekordy CNAME - aliasy domeny
www        IN          CNAME    @
ftp        IN          CNAME    szkola.lokalna.

```

## Gdzie

- **\$TTL** Dyrektywa definiuje domyślny czas życia dla strefy. Niniejsza dyrektywa jest obowiązkowa. Czas jest określony w sekundach.
- **\$ORIGIN** Dyrektywa określa definiowaną domenę. Można ją pominąć.
- Nazwy domen muszą kończyć się kropką (.), są wówczas domeną główną. Gdy nazwa domeny kończy się kropką, jest to w pełni kwalifikowana nazwa domeny (FQDN).
- Symbol @ odwołuje się do domeny definiowanej.
- **IN** to klasa DNS. To oznacza Internet. Istnieją inne klasy DNS, ale są rzadko używane.

Pierwszym rekordem w pliku strefy jest rekord SOA (Start of Authority). Ten rekord zawiera następujące informacje:

- **ks23-3n00.szkola.lokalna. - The master DNS server – Główny serwer DNS .**
- **root.szkola.lokalna. - Email address of the zone administrator. - Adres e-mail administratora strefy.** RFC 2142 zaleca adres e-mail *hostmaster@example.com* . W pliku strefy ten adres e-mail ma następującą postać: *root.szkola.lokalna*, ponieważ symbol @ ma specjalne znaczenie w pliku strefy.

- **2022020901- Zone serial numer.** Numer seryjny ułatwia śledzenia zmian w strefie, przez podrzędny serwer DNS. Należy aktualizować numer seryjny po każdym wprowadzeniu zmian w pliku strefy. Mogą to być kolejne liczby, jednak zgodnie z konwencją numer seryjny przyjmuje format daty: `yyyymmddss` gdzie `rrrr` to czterocyfrowy numer roku, `mm` to miesiąc, `dd` to dzień, a `ss` to numer kolejny w danym dniu, co ułatwi identyfikację terminu zmiany.
- **604800 - Refresh value.** Po osiągnięciu wartości odświeżania podrzędny serwer DNS spróbuje odczytać rekord SOA z głównego serwera DNS. Jeśli numer seryjny jest wyższy, inicjowany jest transfer strefy.
- **86400 - Retry value.** Definiuje interwał ponownych prób w sekundach, jeśli podrzędny serwer DNS nie połączy się z głównym serwerem DNS.
- **2419200 - Expiry Wygaśnięcie :** jeśli podrzędny serwer DNS nie nawiązał kontaktu z głównym serwerem DNS przez ten czas, urządzenie podrzędne przestanie odpowiadać na zapytania DNS dotyczące tej strefy.
- **604800- Negative cache TTL:** określa czas odpowiedzi DNS dla nieistniejących nazw DNS (NXDOMAIN).

Rekordy TXT są zwykle ujęte w podwójne cudzysłowy. Jeśli dodasz rekord DKIM, musisz również dołączyć wartość w nawiasach.

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ cat /etc/bind/db.szkoła.lokalna
;
; Plik strefy szkoła.lokalna
;
$TTL      604800      ; domyslny czas zycia strefy w [s]
$ORIGIN   szkoła.lokalna.      ;definiowana domena - mozna pominac
;
;bazowe rekordy strefy okreslajace kluczowe cechy strefy
@         IN         SOA      ks23-3n00.szkoła.lokalna. root.szkoła.lokalna. (
                                2022020901      ; Serial
                                604800           ; Refresh
                                86400            ; Retry
                                2419200          ; Expire
                                604800 )         ; Negative Cache TTL
;
;serwer nazw domen szkoła.lokalna
IN        NS         ks23-3n00.szkoła.lokalna.
;
;rekordy A
@         IN         A        172.22.0.1
ks23-3n00 IN         A        172.22.0.1
;
;rekordy CNAME - aliasy domen
www       IN         CNAME    @
ftp       IN         CNAME    szkoła.lokalna.
us3n00@ks23-3n00:~$

```

Po zapisaniu i zamknięciu pliku, należy sprawdzić, czy w głównym pliku konfiguracyjnym występują błędy składniowe:

```
sudo named-checkconf
```

Ciche wyjście wskazuje, że nie znaleziono błędów.

Następnie sprawdzamy składnię plików strefy.

```
sudo named-checkzone szkola.lokalna /etc/bind/db.szkola.lokalna
```

Jeśli w pliku strefy występują błędy składniowe, należy to naprawić, w przeciwnym razie strefa nie zostanie załadowana. Poniższy komunikat wskazuje, że nie ma błędów składniowych.

```
us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ sudo named-checkzone szkola.lokalna /etc/bind/db.szkola.lokalna
zone szkola.lokalna/IN: loaded serial 2022020901
OK
us3n00@ks23-3n00:~$
```

Następnie ponownie uruchomiamy BIND9.

```
sudo systemctl restart bind9
```

Jeśli używamy nieskomplikowanej zapory ogniowej (UFW), otwieramy port TCP i UDP 53:

```
sudo ufw allow 53/tcp
sudo ufw allow 53/udp
```

Jeśli bezpośrednio używamy zapory iptables, wpisujemy polecenia.

```
sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
```

## Sprawdzamy działanie strefy

Na serwerze, aby sprawdzić poprawność rozpoznawania skonfigurowanych nazw wpisujemy kolejno:

```
dig szkola.lokalna
dig www.szkola.lokalna
dig ftp.szkola.lokalna
```

```
us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ dig szkola.lokalna

; <<>> DiG 9.16.1-Ubuntu <<>> szkola.lokalna
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63436
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;szkola.lokalna.                IN      A

;; ANSWER SECTION:
szkola.lokalna.                604800  IN      A      172.22.0.1

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 07:31:34 UTC 2022
;; MSG SIZE rcvd: 59

us3n00@ks23-3n00:~$
```

```

us3n00@ks23-3n00: ~$ dig www.szkoła.localna

; <<>> DiG 9.16.1-Ubuntu <<>> www.szkoła.localna
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9609
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.szkoła.localna.                IN      A

;; ANSWER SECTION:
www.szkoła.localna.        604800  IN      CNAME   szkoła.localna.
szkoła.localna.           604800  IN      A       172.22.0.1

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 07:32:34 UTC 2022
;; MSG SIZE rcvd: 77

us3n00@ks23-3n00: ~$

us3n00@ks23-3n00: ~$ dig ftp.szkoła.localna

; <<>> DiG 9.16.1-Ubuntu <<>> ftp.szkoła.localna
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32708
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ftp.szkoła.localna.                IN      A

;; ANSWER SECTION:
ftp.szkoła.localna.        604800  IN      CNAME   szkoła.localna.
szkoła.localna.           604800  IN      A       172.22.0.1

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 07:33:49 UTC 2022
;; MSG SIZE rcvd: 77

us3n00@ks23-3n00: ~$

```

Jak łatwo zauważyć, nasz serwer poprawnie rozpoznaje skonfigurowane nazwy.

Na desktopie, sprawdzamy czy mamy skonfigurowany nasz serwer DNS w konfiguracji interfejsu sieciowego.

Anuluj
Przewodowe
Zastosuj

Informacje
Tożsamość
IPv4
IPv6
Zabezpieczenia

Prędkość połączenia 1000 Mb/s

Adres IPv4 172.22.0.20

Adres IPv6 fe80::38da:d227:f721:fe2a

Adres sprzętowy 08:00:27:12:27:28

Domyślna trasa 172.22.0.1

DNS 172.22.0.1

☒ Łączenie automatyczne

☒ Dostępna dla innych użytkowników

☐ Mierzone połączenie: ma ograniczenia danych lub wiąże się z opłatami  
Aktualizacje oprogramowania i inne duże pobierania nie będą rozpoczynane automatycznie.

Usuń profil połączenia

Jeżeli nie jest jak powyżej. Adres DNS do celów testowych możemy wpisać w dig:  
dig szkola.lokalna @172.22.y.1

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ dig szkola.lokalna @172.22.0.1

; <<>> DiG 9.16.1-Ubuntu <<>> szkola.lokalna @172.22.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44414
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3ee2409f6defee3b01000000621c7c3bbbed7d5e74fb8f287 (good)
;; QUESTION SECTION:
;szkola.lokalna.                IN      A

;; ANSWER SECTION:
szkola.lokalna.                604800  IN      A      172.22.0.1

;; Query time: 0 msec
;; SERVER: 172.22.0.1#53(172.22.0.1)
;; WHEN: pon lut 28 08:39:39 CET 2022
;; MSG SIZE rcvd: 87

ud3n00@k1d23-3n00:~$

```



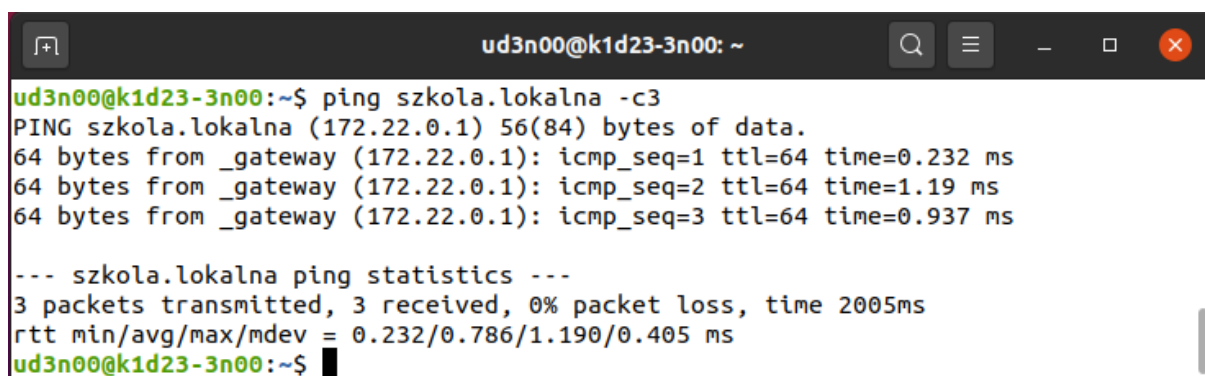
Docelowo powinniśmy jednak uzupełnić konfigurację interfejsu sieciowego, o poprawny DNS, ręcznie lub automatycznie, jeżeli mamy poprawnie skonfigurowany serwer DHCP.

W jednym i drugim przypadku, aby odświeżyć konfigurację karty sieciowej, rozłączmy istniejące połączenie, a po chwili, po pojawieniu się komunikatu Rozłączono..., wybieramy Połączenie przewodowe 1

Po pojawieniu się komunikatu Ustanowiono połączenie, sprawdzamy przypisany adres

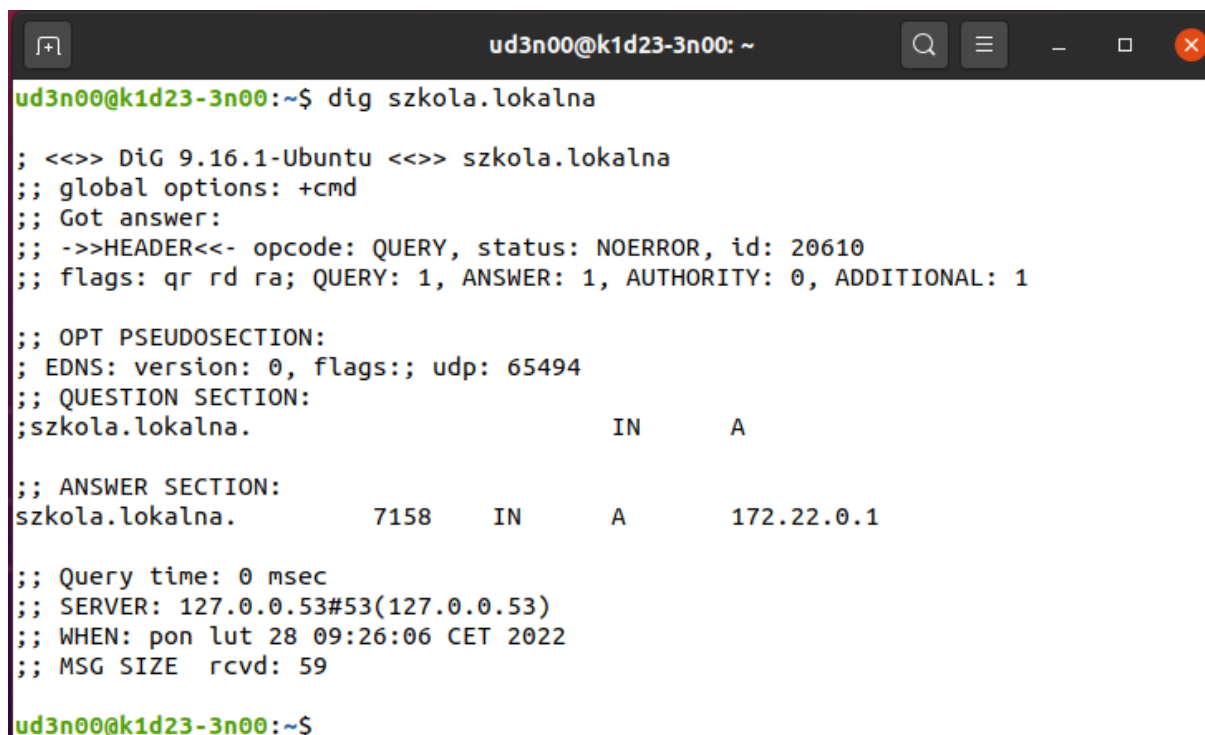
Po weryfikacji adresu DNS, sprawdzamy kolejno:

```
ping szkola.lokalna -c3
dig szkola.lokalna
dig www.szkola.lokalna
dig ftp.szkola.lokalna
```



```
ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ ping szkola.lokalna -c3
PING szkola.lokalna (172.22.0.1) 56(84) bytes of data.
64 bytes from _gateway (172.22.0.1): icmp_seq=1 ttl=64 time=0.232 ms
64 bytes from _gateway (172.22.0.1): icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from _gateway (172.22.0.1): icmp_seq=3 ttl=64 time=0.937 ms

--- szkola.lokalna ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.232/0.786/1.190/0.405 ms
ud3n00@k1d23-3n00:~$
```



```
ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ dig szkola.lokalna

; <<>> DiG 9.16.1-Ubuntu <<>> szkola.lokalna
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 20610
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 65494
;; QUESTION SECTION:
;szkola.lokalna.                IN      A

;; ANSWER SECTION:
szkola.lokalna.                7158    IN      A      172.22.0.1

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 09:26:06 CET 2022
;; MSG SIZE rcvd: 59

ud3n00@k1d23-3n00:~$
```

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ dig www.szkoła.lokalna

; <<>> DiG 9.16.1-Ubuntu <<>> www.szkoła.lokalna
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56222
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.szkoła.lokalna.                IN      A

;; ANSWER SECTION:
www.szkoła.lokalna.        604800  IN      CNAME   szkoła.lokalna.
szkoła.lokalna.           7199   IN      A       172.22.0.1

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 09:26:45 CET 2022
;; MSG SIZE rcvd: 77

ud3n00@k1d23-3n00:~$

```

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ dig ftp.szkoła.lokalna

; <<>> DiG 9.16.1-Ubuntu <<>> ftp.szkoła.lokalna
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44355
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ftp.szkoła.lokalna.                IN      A

;; ANSWER SECTION:
ftp.szkoła.lokalna.        604800  IN      CNAME   szkoła.lokalna.
szkoła.lokalna.           7199   IN      A       172.22.0.1

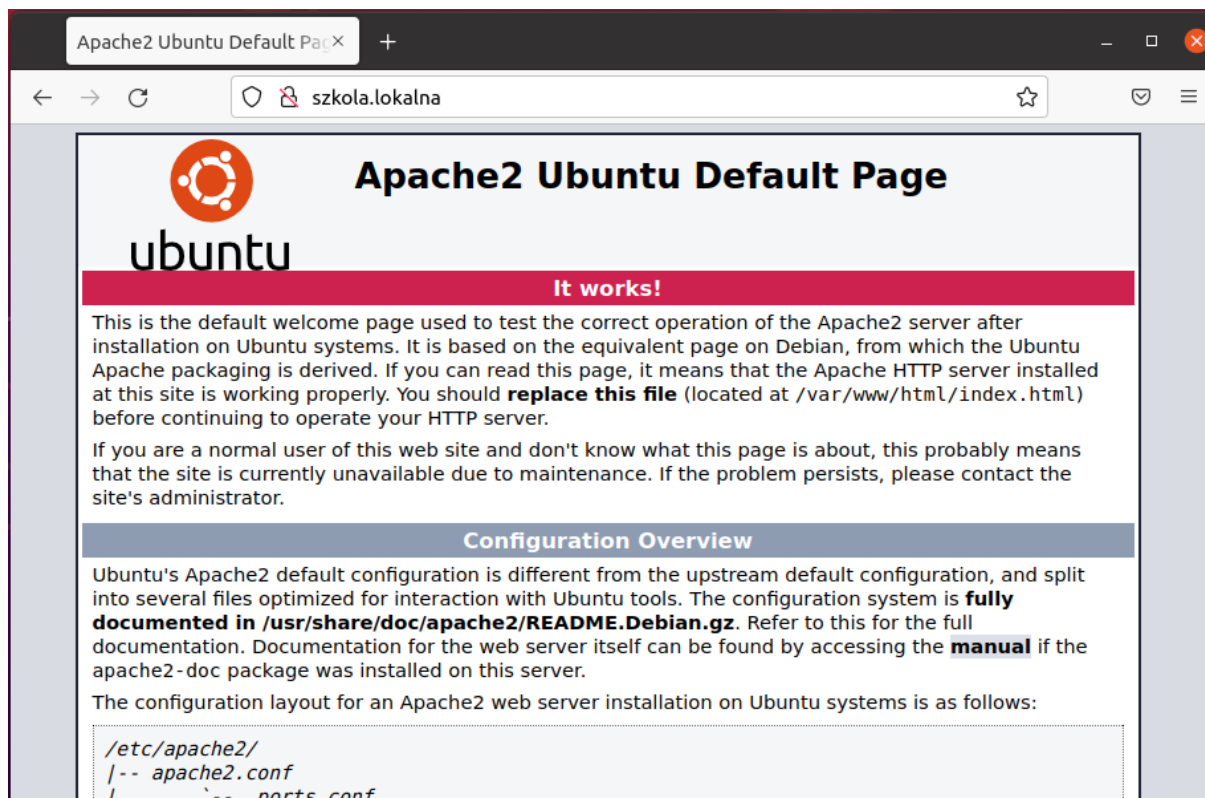
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 09:27:19 CET 2022
;; MSG SIZE rcvd: 77

ud3n00@k1d23-3n00:~$

```

Jak widać ping po nazwie działa poprawnie a wszystkie nazwy są rozpoznawane poprawnie przez nasz serwer.

Jeżeli mamy skonfigurowany serwer www, możemy otworzyć stronę powiązaną z adresem 172.22.0.1 na domyślnym porcie 80, po wpisaniu w oknie przeglądarki szkoła.lokalna, lub aliasu [www.szkoła.lokalna](http://www.szkoła.lokalna)



Jak widać nasz serwer DNS działa poprawnie.

### Rzeczy, które warto wiedzieć

- Termin **master DNS server** wskazuje, że ten serwer przechowuje główną kopię pliku strefy. Nie ma wyższego priorytetu, jeśli chodzi o rozpoznawanie DNS.
- Zawsze aktualizuj numer seryjny SOA podczas wprowadzania zmian w pliku strefy.

### Konfiguracja strefy wyszukiwania wstecznego

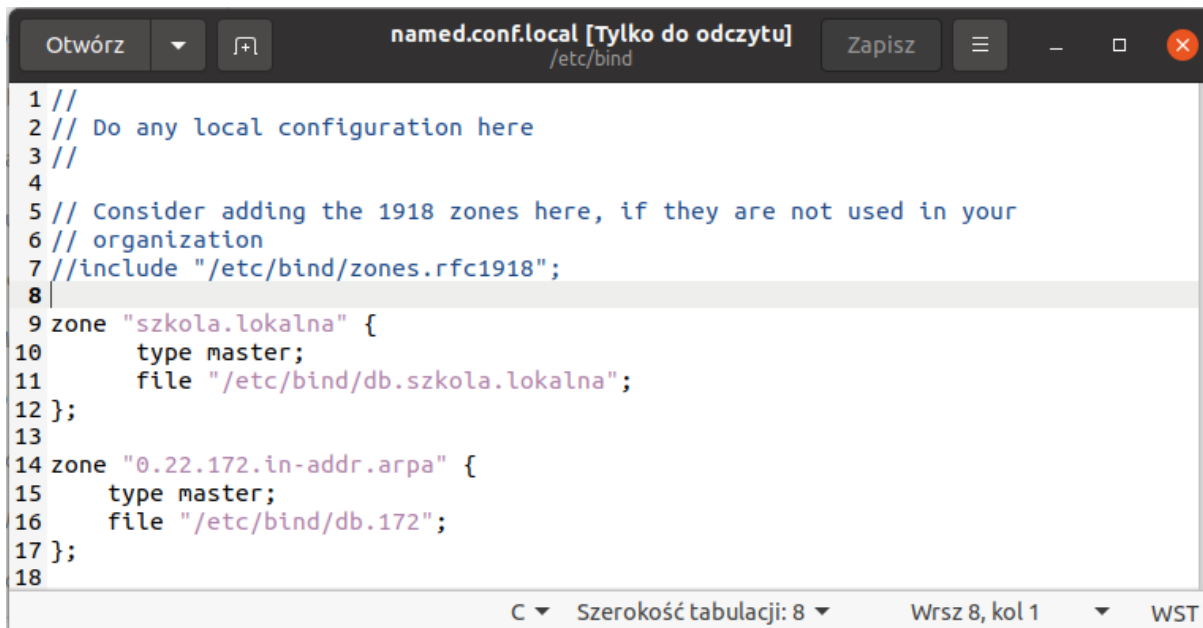
Teraz, gdy strefa wyszukiwania do przodu jest skonfigurowana i rozwiązuje nazwy na adresy IP, należy dodać **strefę odwrotną** **strefę wyszukiwania wstecznego**, aby umożliwić systemowi DNS przetłumaczenie adresu na nazwę.

Edytuj `/etc/bind/named.conf.local` i dodaj następujące elementy:

```
zone "y.22.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172";
};
```

### Uwaga

**y.22.172** to pierwsze trzy oktety naszej sieci, (**172.22.y.0** – y to nr z dziennika). Nadając nazwę plikowi strefy odwrotnej, wykorzystujemy najczęściej pierwszy oktet naszej sieci. `/etc/bind/db.172`



```


1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8
9 zone "szkola.lokalna" {
10     type master;
11     file "/etc/bind/db.szkola.lokalna";
12 };
13
14 zone "0.22.172.in-addr.arpa" {
15     type master;
16     file "/etc/bind/db.172";
17 };
18

```

Plik `/etc/bind/db.172` tworzymy przez skopiowanie pliku `/etc/bind/db.127`

```
sudo cp /etc/bind/db.127 /etc/bind/db.172
```

Następnie edytując plik `/etc/bind/db.172` zmieniamy na opcje zgodne z:  
`/etc/bind/db.szkola.lokalna`



```

1 ;
2 ; BIND      strefa wyszukiwania wstecznego dla sieci 172.22.y.0
3 ;                      gdzie y to nr z dziennika
4 ;
5 $TTL      604800
6 @         IN      SOA      ks23-3n00.szkola.lokalna. root.szkola.lokalna. (
7                               2022020801          ; Serial
8                               604800              ; Refresh
9                               86400               ; Retry
10                              2419200             ; Expire
11                              604800 )           ; Negative Cache TTL
12 ;
13 @         IN      NS       ks23-3n00.szkola.lokalna.
14 1         IN      PTR      szkoła.lokalna.

```

Numer *seryjny* w strefie odwrotnej należy również zwiększać przy każdej zmianie. Dla każdego *rekordu A* skonfigurowanego w `/etc/bind/db.szkola.lokalna`, czyli dla każdego adresu, musisz utworzyć *rekord PTR* w `/etc/bind/db.172`.

Po utworzeniu pliku strefy wyszukiwania wstecznego zrestartuj BIND9:

```
sudo systemctl restart bind9.service
```

## Sprawdź status

```
sudo systemctl status bind9.service
```

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ sudo systemctl restart bind9.service
us3n00@ks23-3n00:~$ sudo systemctl status bind9.service
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-03-01 07:56:17 UTC; 3s ago
     Docs: man:named(8)
    Main PID: 38731 (named)
      Tasks: 5 (limit: 2268)
     Memory: 13.9M
    CGroup: /system.slice/named.service
            └─38731 /usr/sbin/named -f -u bind

mar 01 07:56:17 ks23-3n00 named[38731]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
mar 01 07:56:17 ks23-3n00 named[38731]: network unreachable resolving './NS/IN': 2001:500:200::b#53
us3n00@ks23-3n00:~$

```

## Zweryfikuj działanie strefy odwrotnej na serwerze i kliencie

```
dig -x 172.22.y.1
```

```
nslookup 172.22.y.1
```

gdzie y to nr z dziennika

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ dig -x 172.22.0.1

; <<>> DiG 9.16.1-Ubuntu <<>> -x 172.22.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62930
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;1.0.22.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.0.22.172.in-addr.arpa. 604800 IN      PTR      szkoła.lokalna.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: wto mar 01 08:01:14 UTC 2022
;; MSG SIZE rcvd: 80

us3n00@ks23-3n00:~$

```

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ dig -x 172.22.0.1

; <<>> DiG 9.16.1-Ubuntu <<>> -x 172.22.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27966
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;1.0.22.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.0.22.172.in-addr.arpa. 604800 IN      PTR      szkola.lokalna.

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: wto mar 01 09:02:41 CET 2022
;; MSG SIZE rcvd: 80

ud3n00@k1d23-3n00:~$

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ nslookup 172.22.0.1
1.0.22.172.in-addr.arpa name = szkola.lokalna.

Authoritative answers can be found from:

us3n00@ks23-3n00:~$

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ nslookup 172.22.0.1
1.0.22.172.in-addr.arpa name = szkola.lokalna.

Authoritative answers can be found from:

ud3n00@k1d23-3n00:~$

```

## Konfiguracja dodatkowych domen,

do rozwiązania których, nasz serwer (szkola.lokalna.) będzie autorytatywny.

### Zadanie

Utworzyć i skonfigurować, na serwerze głównym z domeną podstawową szkola.lokalna, strefę wyszukiwania do przodu

- o **ferie.info.** - wskazującą na adres IP 172.22.y.2 gdzie y to nr z dziennika
- o alias domeny ferie.info. – [www.ferie.info](http://www.ferie.info)
- o alias domeny ferie.info. – [ftp.ferie.info](http://ftp.ferie.info)

### Rozwiązanie

Aby dodać nową strefę (domenę), należy edytować plik: /etc/bind/named.conf.local. Dodać do tego pliku wiersze definiujące nową strefę wyszukiwania do przodu, (bez transferu strefy do podrzędnego serwera DNS).

```

zone "ferie.info" {
    type master;

```



```
file "/etc/bind/db.ferie.info";
};
```

W powyższej konfiguracji tworzymy nową strefę klauzulą zone, określamy typ strefy -master, (strefa główna), lokalizację pliku strefy, w którym utworzymy wymagane rekordy DNS.



```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8
9 zone "szkola.lokalna" {
10     type master;
11     file "/etc/bind/db.szkola.lokalna";
12 };
13
14 zone "0.22.172.in-addr.arpa" {
15     type master;
16     file "/etc/bind/db.172";
17 };
18
19 zone "ferie.info." {
20     type master;
21     file "/etc/bind/db.ferie.info";
22 };
23
```

Po zapisaniu pliku, należy przystąpić do utworzenia i konfiguracji pliku definiującego nową strefę. Możemy to zrobić wykorzystując plik definiujący strefę podstawową, db.szkola.lokalna, ponieważ rekordy SOA oraz NS pozostają bez zmian – definiują one serwer, na którym tworzymy strefy. Kopiujemy zawartość pliku /etc/bind/db.szkola.lokalna do pliku /etc/bind/db.ferie.inf

```
sudo cp /etc/bind/db.szkola.lokalna /etc/bind/db.ferie.info
```

Mamy już zdefiniowany

- adres startowy - rekord SOA
- oraz serwer nazw - rekord NS.

Te dwa rekordy się nie zmieniają na naszym serwerze DNS.

```

us3n00@ks23-3n00: /$ cat /etc/bind/db.ferie.info
;
; Plik strefy ferie.info
;
$TTL      604800; domyslny czas zycia strefy w [s]
$ORIGIN   ferie.info.      ;definiowana strefa
;
;bazowe rekordy strefy - kluczowe cechy
@         IN      SOA      ks23-3n00.szkola.lokalna. root.szkola.lokalna. (
                                2022022801      ; Serial
                                604800           ; Refresh
                                86400            ; Retry
                                2419200          ; Expire
                                604800 )         ; Negative Cache TTL
;
;serwer nazw
@         IN      NS       ks23-3n00.szkola.lokalna.
;rekordy A
@         IN      A        172.22.0.2
;
;rekordy CNAME - aliasy
ftp       IN      CNAME    @
www       IN      CNAME    ferie.info.
us3n00@ks23-3n00: /$

```

Wystarczy:

- uaktualnić Zone serial numer. Numer seryjny ułatwia śledzenia zmian w strefie, przez podrzędny serwer DNS. Zgodnie z konwencją numer seryjny przyjmuje format daty: yyyyymmddss gdzie rrrr to czterocyfrowy numer roku, mm to miesiąc, dd to dzień a ss to numer kolejny w danym dniu. Musimy aktualizować numer seryjny po wprowadzeniu zmian w pliku strefy.
- zdefiniować rekordy hosta nowych stref - rekordy A
- zdefiniować aliasy nowych stref - rekordy CNAME

W pliku db.ferie.info :

- w opisie strefy zmieniamy nazwę szkola.lokalna na ferie.info
- w dyrektywie \$ORIGIN zmieniamy nazwę szkola.lokalna na ferie.info
- w definicji rekordu SOA zmieniamy serial, zgodnie z konwencją opisaną powyżej
- w sekcji rekordy A zmieniamy adres powiązany z domeną ferie.info na 172.22.y.2 (y to nr z dziennika)
- w sekcji rekordy CNAME definiujemy aliasy domeny ferie.info. Pamiętajmy że, jeżeli używamy pełnej nazwy domeny, na końcu musi być kropka. Możemy również wykorzystać symbol @ określający również domenę ferie.info - dyrektywa \$ORIGIN ferie.info

Po zapisaniu zmodyfikowanego pliku, sprawdzamy jego poprawność poleceniem:

```
sudo named-checkzone ferie.info /etc/bind/db.ferie.info
```

```

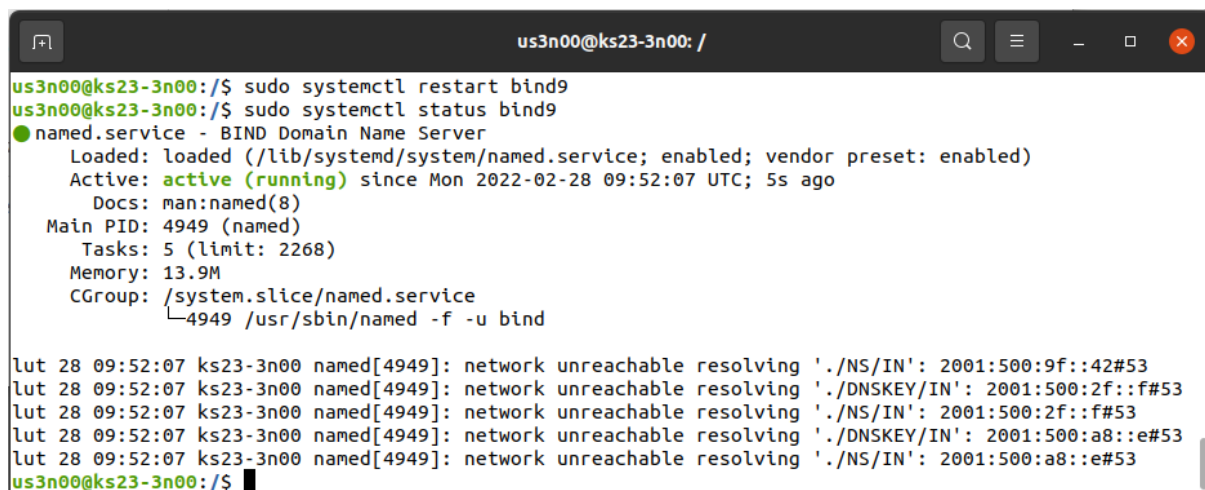
us3n00@ks23-3n00: ~$ sudo named-checkzone ferie.info /etc/bind/db.ferie.info
zone ferie.info/IN: loaded serial 2022022801
OK
us3n00@ks23-3n00: ~$

```

Możemy teraz restartować usługę bind9 oraz sprawdzić jej status, czy nie ma błędów przy jej uruchamianiu.

```
sudo systemctl restart bind9
```

```
sudo systemctl status bind9
```



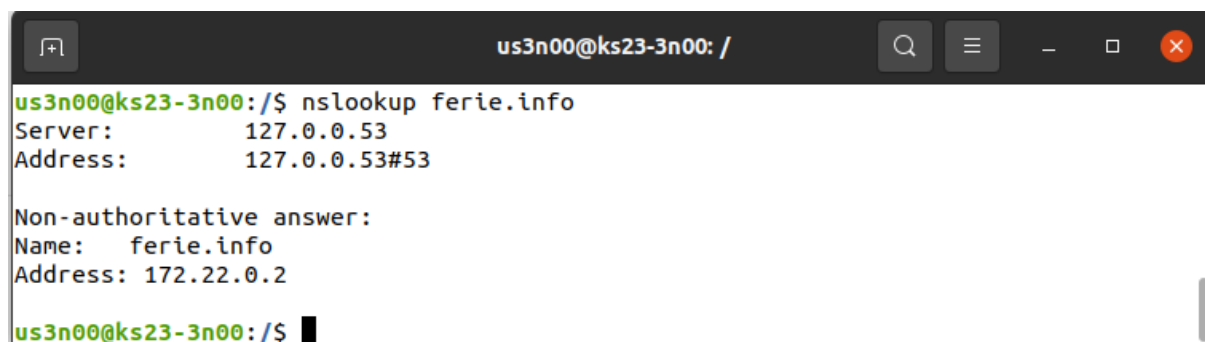
```
us3n00@ks23-3n00: /
us3n00@ks23-3n00:/$ sudo systemctl restart bind9
us3n00@ks23-3n00:/$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-02-28 09:52:07 UTC; 5s ago
     Docs: man:named(8)
    Main PID: 4949 (named)
      Tasks: 5 (limit: 2268)
     Memory: 13.9M
    CGroup: /system.slice/named.service
            └─4949 /usr/sbin/named -f -u bind

lut 28 09:52:07 ks23-3n00 named[4949]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
lut 28 09:52:07 ks23-3n00 named[4949]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
lut 28 09:52:07 ks23-3n00 named[4949]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
lut 28 09:52:07 ks23-3n00 named[4949]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
lut 28 09:52:07 ks23-3n00 named[4949]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
us3n00@ks23-3n00:/$
```

Jak widać, wszystkie strefy są załadowane, serwer uruchomiony i nie widać informacji o błędach.

Możemy przetestować działanie serwera. Mamy do tego polecenia **nslookup** (stare działające również w systemach Windows) oraz znane już, dające więcej informacji **dig**. Np.:

```
nslookup ferie.info
```



```
us3n00@ks23-3n00:/$ nslookup ferie.info
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   ferie.info
Address: 172.22.0.2

us3n00@ks23-3n00:/$
```

lub `dig ferie.info`

```

us3n00@ks23-3n00: /
us3n00@ks23-3n00:/$ dig www.ferie.info

; <<> DiG 9.16.1-Ubuntu <<> www.ferie.info
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32865
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.ferie.info.                IN      A

;; ANSWER SECTION:
www.ferie.info.        604800  IN      CNAME   ferie.info.
ferie.info.            604800  IN      A       172.22.0.2

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 09:56:25 UTC 2022
;; MSG SIZE rcvd: 73

us3n00@ks23-3n00:/$

```

Sprawdzamy ping po nazwie www.ferie.info

```

us3n00@ks23-3n00: /
us3n00@ks23-3n00:/$ ping ftp.ferie.info -c3
PING ferie.info (172.22.0.2) 56(84) bytes of data.
64 bytes from ks23-3n00 (172.22.0.2): icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from ks23-3n00 (172.22.0.2): icmp_seq=2 ttl=64 time=0.103 ms
64 bytes from ks23-3n00 (172.22.0.2): icmp_seq=3 ttl=64 time=0.104 ms

--- ferie.info ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.023/0.076/0.104/0.037 ms
us3n00@ks23-3n00:/$

```

Jeżeli mamy w sieci, skonfigurowanego klienta, możemy wszystkie powyższe testy wykonać na nim. Np.: ping ftp.ferie.info

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ ping ferie.info -c3
PING ferie.info (172.22.0.2) 56(84) bytes of data.
64 bytes from 172.22.0.2 (172.22.0.2): icmp_seq=1 ttl=64 time=0.485 ms
64 bytes from 172.22.0.2 (172.22.0.2): icmp_seq=2 ttl=64 time=0.936 ms
64 bytes from 172.22.0.2 (172.22.0.2): icmp_seq=3 ttl=64 time=1.01 ms

--- ferie.info ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.485/0.811/1.012/0.232 ms
ud3n00@k1d23-3n00:~$

```

nslookup ftp.ferie.info

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ nslookup ftp.ferie.info
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
ftp.ferie.info canonical name = ferie.info.
Name:   ferie.info
Address: 172.22.0.2

ud3n00@k1d23-3n00:~$

```

dig www.ferie.info

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ dig www.ferie.info

; <<>> DiG 9.16.1-Ubuntu <<>> www.ferie.info
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7142
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.ferie.info.                IN      A

;; ANSWER SECTION:
www.ferie.info.                604800  IN      CNAME   ferie.info.
ferie.info.                    7199   IN      A       172.22.0.2

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: pon lut 28 11:00:53 CET 2022
;; MSG SIZE rcvd: 73

ud3n00@k1d23-3n00:~$

```

Aby skonfigurować wyszukiwanie wsteczne dla innej strefy w tej samej sieci 172.22.y.0/24, wystarczy zmodyfikować plik **/etc/bind/db.172** dodając na końcu wiersz wiążący adres 172.22.y.2 z domeną **ferie.info**

IN PTR ferie.info.

```

Otwórz  db.172 [Tylko do odczytu]  Zapisz
/etc/bind

1 ;
2 ; BIND    strefa wyszukiwania wstecznego dla sieci 172.22.y.0
3 ;
4 ;
5 $TTL     604800
6 @        IN      SOA     ks23-3n00.szkoła.lokalna. root.szkoła.lokalna. (
7          2022020802      ; Serial
8          604800          ; Refresh
9          86400           ; Retry
10         2419200         ; Expire
11         604800 )        ; Negative Cache TTL
12 ;
13 @        IN      NS      ks23-3n00.szkoła.lokalna.
14 1        IN      PTR     szkoła.lokalna.
15 2        IN      PTR     ferie.info.

```

Weryfikujemy skuteczność konfiguracji na serwerze

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ dig -x 172.22.0.2

; <<>> DiG 9.16.1-Ubuntu <<>> -x 172.22.0.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25928
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;2.0.22.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
2.0.22.172.in-addr.arpa. 604800 IN      PTR      ferie.info.

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: wto mar 01 08:41:53 UTC 2022
;; MSG SIZE rcvd: 76

us3n00@ks23-3n00:~$

```

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ nslookup 172.22.0.2
2.0.22.172.in-addr.arpa name = ferie.info.

Authoritative answers can be found from:

us3n00@ks23-3n00:~$

```

Na kliencie

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ nslookup 172.22.0.2
2.0.22.172.in-addr.arpa name = ferie.info.

Authoritative answers can be found from:

ud3n00@k1d23-3n00:~$

```



```
ud3n00@k1d23-3n00: ~  
ud3n00@k1d23-3n00:~$ dig -x 172.22.0.2  
  
;<>> DiG 9.16.1-Ubuntu <>> -x 172.22.0.2  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 48645  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 65494  
;; QUESTION SECTION:  
;2.0.22.172.in-addr.arpa.      IN      PTR  
  
;; ANSWER SECTION:  
2.0.22.172.in-addr.arpa. 6283    IN      PTR      ferie.info.  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: wto mar 01 09:57:23 CET 2022  
;; MSG SIZE rcvd: 76  
  
ud3n00@k1d23-3n00:~$
```