T: Instalacja i konfiguracja serwera DNS.

Cel ogólny lekcji to nauczenie się instalacji i konfiguracji serwera DNS oraz konfiguracji strefy przeszukiwania do przodu i wstecz oraz zrozumienie sposobu tworzenia rekordów jak korzystać z DNS oraz jak testować działanie uruchomionego serwera DNS oraz innych serwerów DNS.

Cele szczegółowe:

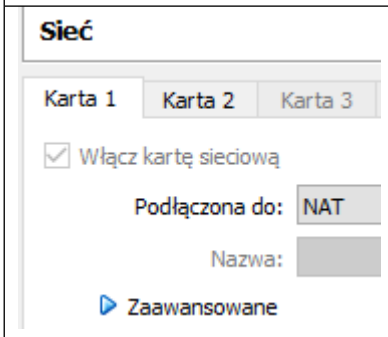
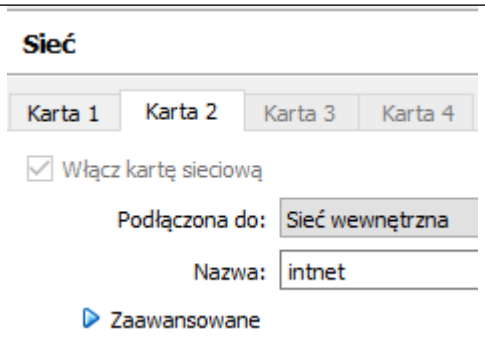
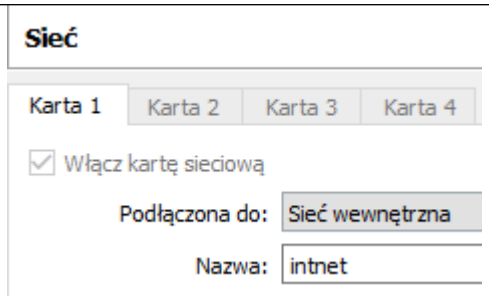
1. Wyjaśnienie pojęć związanych z DNS.
2. Instalacja serwera DNS BIND w wersji 9.
3. Konfiguracja serwera DNS wraz z ustawieniem stałego adresu IP oraz nazwy hosta.
4. Testowanie uruchomionego serwera DNS.
5. Testowanie innych serwerów DNS.
6. Zapisanie w zeszycie wszystkich poleceń konfiguracyjnych z wyjaśnieniem ich działania.
7. Skopiowanie przykładowego pliku konfiguracyjnego i nadanie mu odpowiedniej nazwy
8. Zmiana nazw labhost i root.labhost na nazwę domenową naszego serwera
9. Zmiana numeru seryjnego pliku o 1 po każdej zmianie
10. Dodanie interesujących nas rekordów, takich jak A, NS, CNAME, MX, AAAA, TXT, i zrozumienie ich składni
11. Utworzenie kopii pliku /etc/bind/db.127 i zmiana jego nazwy
12. Dodanie rekordów PTR używanych przy RevDNS, tyle ile zdefiniowanych jest subdomen w strefie przeszukiwania do przodu
13. Sprawdzenie i zaakceptowanie konfiguracji serwera DNS oraz poprawność konfiguracji strefy przeszukiwania do przodu dla naszej domeny.

Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu

1. podaj i wyjaśnij polecenia, które użyjesz, aby:
   - wyjaśnić pojęcia związane z dns,
   - zainstalować serwer dns,
   - uruchomić lub zatrzymać usługi sieciowe,
   - konfigurować serwer dns,
   - korzystać z dns.
2. podaj odpowiedzi na pytania zadane w treści zadań.

Przywróć migawkę „Migawka 1” zawierającą przygotowane do ćwiczeń maszyny Ubuntu serwer i desktop (klient). Przed przystąpieniem do ćwiczenia sprawdź czy ustawienie maszyny wirtualnej

pozwala na dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu serwer i klienty zgodnie z wymaganiami w instrukcji.

Ubuntu serwer Adapter 1	Ubuntu serwer Adapter 2
	
	Ubuntu desktop Adapter 1
	

login: ubuntu **password**: ubuntu zalogowanie do ubuntu

```
Ubuntu 24.04 LTS ubuntu2204 tty1

ubuntu2204 login: ubuntu
Password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-31-generic x86_64)
```

sudo -s **password**: ubuntu - logowanie z podniesionymi uprawnieniami

exit - zamknięcie

```
ubuntu@ubuntu2204:~$ sudo -s
root@ubuntu2204:/home/ubuntu# exit
exit
ubuntu@ubuntu2204:~$
```

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Za pomocą polecenia ip a ustal dostępne interfejsy sieciowe.

1. Zapisz plik static.yaml z katalogu /usr/share/doc/netplan/examples/ plik jako /etc/netplan/00-installer-config.yaml plik z niższym numerem, ma wyższy priorytet.

```
cp /usr/share/doc/netplan/examples/static.yaml /etc/netplan/00-installer-config.yaml
```

2. Ustaw adres IP dla Ubuntu (na Adapter 2 na statyczny).

Otwórz plik, który opisuje interfejsy sieciowe nano /etc/netplan/0 tabulator - nazwa pliku zostanie uzupełniona do postaci *.yaml

Pozostaw zalecane wpisy w tym pliku jak poniżej, pamiętając, że możesz mieć inny interfejs nie enp0s8

Plik *.yaml posiada dość wybredną składnię. Należy uważać, aby WSZYSTKO było wpisane poprawnie. W przeciwnym wypadku interfejs NIE ZADZIAŁA. Proszę się pilnować, aby NIE POMIJAĆ znaków ani NIE PRZEPISYWAĆ WSZYSTKIEGO NA ŚLEPO, ma być dokładnie literka pod literką, znak pod znakiem, spacja pod spacją.

Poprawna wersja (Server – renderer: networkd)

Jeśli zostawiasz DHCP na NAT (enp0s3), usuń trasę z enp0s8:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:          # NAT – wyjście do Internetu (DHCP ustawia gateway)
      dhcp4: true
    enp0s8:          # Sieć wewnętrzna – tylko adres statyczny
      dhcp4: false
      addresses:
        - 10.0.0.3/24
      nameservers:
        addresses:
          - 8.8.8.8
```

- 1.1.1.1

2. Zastosuj ustawienia

sudo netplan apply

ip a

3. Zmień nazwę hosta na stałe

hostnamectl set-hostname dlp

init 6

Opisz w zeszycie:

- procedurę instalacji i konfiguracji oraz uruchomienia serwera DNS,
- testowania uruchomionego serwera DNS,
- testowania innych serwerów DNS.

Wszystkie polecenia konfiguracyjne zapisz w zeszycie z wyjaśnieniem ich działania.

Ćwiczenie Instalacja i konfiguracja serwera DNS – bind

DNS to skrót od Domain Name System i jest to hierarchiczny, rozproszony system nazw sieciowych, odpowiadający na zapytania o nazwy domen. Stwierdzenie "jest to usługa zamieniająca domenę na nazwę IP" jest dość powierzchownym stwierdzeniem i nadaje się na lekcje Informatyki w szkole podstawowej. DNS nie tylko tłumaczy domeny na adresy IP, ale może np. tłumaczyć adresy IP na domeny (tzw. RevDNS), a nawet domeny na domeny (CNAME). Hierarchiczny oznacza, że opiera się na jakiejś hierarchii, w tym przypadku będziemy mieć 13 głównym serwerów zwanych root-servers, do których są podłączone mniejsze serwery w różnych krajach. Do tych serwerów mogą być podłączone inne serwery np. operatorów domen, operatorów internetowych itd. Z kolei do tych serwerów często podłączone są serwery mniejsze - firmowe, domowe. Rozproszony oznacza, że nie skupia się w jednym miejscu. Serwery DNS rozproszone są po krajach, kontynentach, miastach itd.
Znając to, możemy przejść do instalacji naszego serwera DNS. Użyjemy do tego implementacji o nazwie BIND w wersji 9. Jest to serwer stworzony przez Internet Systems Consortium. BIND to skrót od Berkley Internet Name Domain. Wpierw jednak warto zaktualizować repozytoria i pakiety na serwerze.

Zainstaluj BIND, aby skonfigurować serwer DNS, który rozpoznaje nazwę domeny lub adres IP.
DNS używa 53 / TCP, UDP.

1. Instalacja BIND 9 i czynności po instalacyjne.

A. Wykonaj aktualizację apt update - aktualizowanie listy pakietów i repozytoriów

B. Instalacja pakietów serwera DNS

```
apt install -y bind9 bind9utils bind9-doc
```

bind9 pakiet bind9; bind9utils pakiet diagnozujący; bind9-doc pakiet z dokumentacją

Jeśli pojawi się `'apt list --upgradable'.` można instalować powyższe pakiety.

Jeśli nie jest możliwe należy zapytać prowadzącego czy można wykonać apt-get upgrade - aktualizacja systemu.

C. Czynności po instalacyjne

Nie zamykaj konsoli z poleceniami

Po zakończeniu procesu instalacji sprawdź:

a) Sprawdzenie działania usługi:

```
systemctl status bind9
```

Test lokalny:

```
nslookup google.com 127.0.0.1
```

Odpowiedź będzie mniej więcej taka:

```
root@dlp:/home/ubuntu# nslookup google.com 127.0.0.1
;; Got SERVFAIL reply from 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53

** server can't find google.com: SERVFAIL
```

b) Skonfiguruj plik /etc/hosts

```
nano /etc/hosts
```

ZMIEŃ NA

```
10.0.0.3  dlp.srv.lab dlp
```

c) Skonfiguruj plik /etc/hostname

```
nano /etc/hostname
```

dlp

d) Otwórz także plik /etc/cloud/cloud.cfg i ustaw preserve_hostname: true

e) Konfiguracja resolvera

Sprawdzenie stanu: resolvectl status

Poprawne podejście (ZALECANE)

Adres DNS ustawiamy w Netplanie

Nie edytujemy ręcznie /etc/resolv.conf.

(Alternatywa dydaktyczna – tylko jeśli wymagane):

ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf

f) Za pomocą narzędzia DIG sprawdź, czy serwer DNS działa prawidłowo

```
root@dlp:/home/ubuntu# dig -x 127.0.0.1

; <<>> DiG 9.18.39-0ubuntu0.24.04.3-Ubuntu <<>> -x 127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6465
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 0       IN      PTR     localhost.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 13 19:04:03 UTC 2026
;; MSG SIZE  rcvd: 74
```

Serwer DNS odpowie prawidłowo, jeśli zwróci nazwę hosta pętli zwrotnej: labhost

g) Po zakończeniu instalacji i przygotowań wstępnych wyświetl zawartość katalogu /etc/bind.

```
ubuntu@dlp:~$ ls -l /etc/bind
razem 48
-rw-r--r-- 1 root root 2928 mar 24 15:25 bind.keys
-rw-r--r-- 1 root root  255 sie 21  2025 db.0
-rw-r--r-- 1 root root  271 sie 18  2025 db.127
-rw-r--r-- 1 root root  237 sie 18  2025 db.255
-rw-r--r-- 1 root root  353 sie 18  2025 db.empty
-rw-r--r-- 1 root root  270 sie 18  2025 db.local
-rw-r--r-- 1 root bind  458 sie 21  2025 named.conf
-rw-r--r-- 1 root bind  498 sie 18  2025 named.conf.default-zones
-rw-r--r-- 1 root bind  165 sie 18  2025 named.conf.local
-rw-r--r-- 1 root bind  846 sie 18  2025 named.conf.options
-rw-r----- 1 bind bind  100 kwi 13 16:16 rndc.key
-rw-r--r-- 1 root root 1317 sie 18  2025 zones.rfc1918
```

Zapisz w zeszycie

- db.127 - przykładowa konfiguracja strefy przeszukiwania wstecznego

- db.lab - przykładowa konfiguracja strefy przeszukiwania do przodu
- named.conf - globalna konfiguracja DNS
- named.conf.default-zones - domyślne strefy przeszukiwania
- named.conf.lab - lokalna konfiguracja DNS
- named.conf.options - konfiguracja serwera DNS

h) Wykonaj kopię named.conf.

```
root@dlp:~# cp /etc/bind/named.conf /etc/bind/named.confbackup
```

Przygotuj: zeszyt z notatką i niezamkniętą konsolę z wydanymi poleceniami

Zgłoszenie 1

UWAGA! ACHTUNG! ATTENTION!

Serwer BIND9 posiada dość wybredną składnię plików konfiguracyjnych. Należy uważać, aby WSZYSTKO było wpisane poprawnie. W przeciwnym wypadku serwer NIE ZADZIAŁA. Proszę się pilnować, aby NIE POMIJAĆ znaków ani NIE PRZEPISYWAĆ WSZYSTKIEGO NA ŚLEPO.

2. Skonfiguruj BIND 9.

Najważniejsze informacje:
- Adres IP serwera: 10.0.0.3
- Docelowa domena: srv.lab
- Nazwa domenowa serwera: dlp.srv.lab
- Nazwa domenowa klienta: klient1.srv.lab

Każdy może sobie wybrać inną domenę. Ważne jest, aby nie była to domena publiczna, taka jak .com, .pl, .edu itd.
Do ćwiczeń zaleca się stosowanie niepublicznych domen testowych, np. .lab, .test, .labnet lub domeny własnej szkoły (np. .zsl).
Nie zaleca się używania domeny .lab, ponieważ jest ona zarezerwowana dla usługi mDNS i może powodować problemy z klasycznym serwerem DNS (BIND9).

Domeny .lab nie zaleca się używać w klasycznym DNS, ponieważ jest obsługiwana przez Multicast DNS (mDNS). Jej użycie wymaga dodatkowej konfiguracji systemd-resolved lub bezpośredniego odpytywania serwera DNS.

a. Edytuj pliku /etc/bind/named.conf.options (forwarders) stosując polecenie:

```
nano /etc/bind/named.conf.options
```

Musisz sobie odnaleźć w nim zakomentowaną opcję nazwaną forwarders. Odkomentujemy całą opcję, a następnie w miejsce 0.0.0.0 wpisujemy adres IP jakiegoś serwera DNS. Ja w swojej sieci domowej posiadam własny serwer DNS, więc tego też używam. Wy możecie, a nawet musicie, wpisać inny serwer. Zapisujemy plik i opuszczamy edytor.

```
forwarders {
    8.8.8.8;
    1.1.1.1;
};
```

Zgłoszenie 2

b. Skonfiguruj plik /etc/bind/named.conf.lab

Strefa DNS to część systemu DNS, za którą odpowiada jeden serwer DNS.
Jeden serwer DNS może obsługiwać wiele stref.
W ćwiczeniu zostaną utworzone dwie strefy:
strefa przeszukiwania naprzód (Forward Lookup Zone) – mapuje nazwę hosta na adres IP,
strefa przeszukiwania wstecz (Reverse Lookup Zone) – mapuje adres IP na nazwę hosta (Reverse DNS).
Przykład definicji stref w BIND9

```
zone "srv.lab" IN {                 // strefa przeszukiwania naprzód
        type master;                // serwer główny (master)
        file "/etc/bind/for.srv.lab.db";
};

zone "0.0.0.10.in-addr.arpa" IN {   // strefa przeszukiwania wstecz
        type master;
        file "/etc/bind/rev.srv.lab.db";
};
```

Opis użytych parametrów
zone – definiuje nową strefę DNS,
"srv.lab" – nazwa domeny obsługiwanej przez strefę,
IN – klasa Internet DNS,

type master; – serwer jest głównym serwerem DNS dla tej strefy,

file – plik zawierający rekordy DNS danej strefy.

Strefa przeszukiwania wstecznego (Reverse DNS)

Dla strefy wstecznej nazwa ma postać:

X.in-addr.arpa

gdzie X to odwrócony adres sieci, bez części hosta.

Przykłady:

192.168.10.10/24 → 10.168.192.in-addr.arpa

10.0.0.1/24 → 0.0.10.in-addr.arpa

10.0.0.1/8 → 10.in-addr.arpa

c. Edycja pliku konfiguracyjnego

Plik edytujemy poleceniem:

```
nano /etc/bind/named.conf.lab
```

Po zapisaniu pliku strefy DNS są gotowe do dalszej konfiguracji (tworzenia plików stref i rekordów).

Zgłoszenie 3

d. Konfiguracja strefy przeszukiwania do przodu. Skopiuj przykładowy plik konfiguracyjny (/etc/bind/db.lab) i nadaj mu taką nazwę jaką podaliśmy w poprzednim pliku przy opcji file. Komenda:

```
cp /etc/bind/db.lab /etc/bind/for.srv.lab.db
```

e. Edytuj plik /etc/bind/for.srv.lab.db poleceniem:

```
nano /etc/bind/for.srv.lab.db
```

Widzimy oryginalną zawartość tego pliku, którą za chwilę zmienimy. Pierwsze co musimy zrobić to zmienić labhost. oraz root.labhost. na nazwę domenową jaką wybrałeś dla naszego serwera dlp.srv.lab.

PROSZĘ PAMIĘTAĆ O KROPCE NA KOŃCU KAŻDEJ NAZWY DOMENOWEJ.

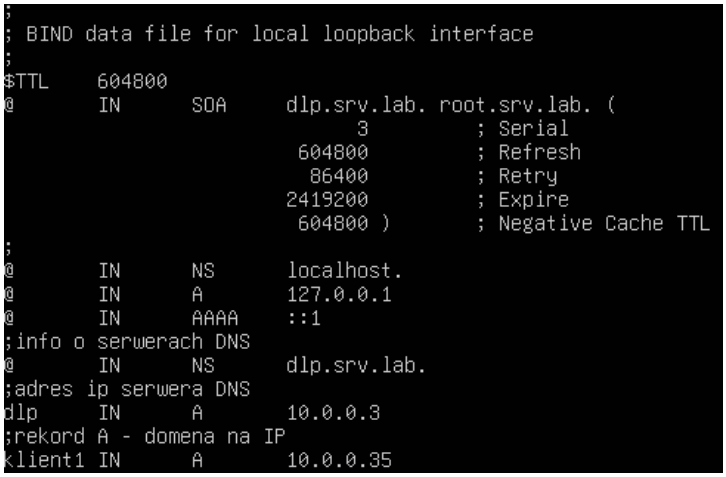
Później zmieniamy numer seryjny (Serial) pliku o 1. DOKONUJEMY TEGO ZAWSZE PO KAŻDORAZOWEJ ZMIANIE TEGO PLIKU. Jest to istotne, gdyż wtedy informujemy serwer DNS, że strefa uległa zmianie. Na samym końcu dodajemy już interesujące nas rekordy. Ich składnia wygląda następująco:

nazwa_domenowa IN typ_rekordu wartość

serwer IN A 10.0.0.3

Znak @ oznacza tutaj sam serwer.

@ IN SOA dlp.srv.lab. root.srv.lab. (



```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dlp.srv.lab. root.srv.lab. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
;info o serwerach DNS
@       IN      NS      dlp.srv.lab.
;adres ip serwera DNS
dlp     IN      A       10.0.0.3
;rekord A - domena na IP
klient1 IN      A       10.0.0.35
```

Zapisz w zeszycie:

Rekordy to są poszczególne wpisy w strefie, które mapują odpowiednie informacje. Typów rekordów jest wiele jednak takimi najpopularniejszymi są:

- A - mapuje nazwę domenową na adres IP

- NS - informuje o serwerach DNS

- CNAME - mapuje nazwę domenową na nazwę domenową

- MX - informuje o serwerze poczty

- AAAA - mapuje nazwę domenową na adres IPv6

- TXT - przechowuje czysty tekst. Używany przez chociażby przez Google do autoryzacji właściciela

Zgłoszenie 4

f. Strefa przeszukiwania wstecznego. Utwórz kopię pliku /etc/bind/db.127 Nadaj mu taką nazwę jaką podana wcześniej przy opcji file. Komenda będzie wyglądać następująco:

cp /etc/bind/db.127 /etc/bind/rev.srv.lab.db

g. Kiedy to już zrobiliśmy to możemy przejść do edycji tego pliku znanym już poleceniem:

nano /etc/bind/rev.srv.lab.db

Widzimy oryginalną zawartość tego pliku i postępujemy tak samo jak w poprzednim przypadku (zmiana labhost i numeru seryjnego). Aż do momentu dodawania rekordów. Najpierw tak jak poprzednio dodajemy dwa rekordy - NS i A informujące o serwerze DNS. Na samym końcu dodajemy interesujące nas rekordy, a ich składnia wygląda następująco:

część_hosta_ip IN PTR adres_domenowy

np. 10 IN PTR dlp.srv.lab.

PAMIĘTAJMY O KROPCE NA KOŃCU.

10 IN PTR dlp.srv.lab.

35 IN PTR klient1.srv.lab.

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dlp.srv.lab. root.srv.lab. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
;info o serwerach DNS
@       IN      NS      dlp.srv.lab.
dlp     IN      A       10.0.0.3
;przeszukiwanie wsteczne dla serwera DNS
10      IN      PTR     dlp.srv.lab.
;rekordy PTR - adres ip na domene
35      IN      PTR     klient1.srv.lab.
```

Dodajemy tyle rekordów PTR, używanych przy RevDNS ile mamy zdefiniowanych subdomen w strefie przeszukiwania do przodu. Mam dwa - serwer oraz klienta, więc dodaję dwa rekordy.

Jeżeli nasz plik wygląda jak powyżej to zapisujemy w nim zmiany

Zgłoszenie 5

i zamykamy go.

h. Sprawdź i zaakceptuj konfigurację serwera DNS i poprawność konfiguracji stref:

named-checkconf

Powyższa komenda sprawdzi nam konfigurację serwera DNS.

named-checkzone srv.lab /etc/bind/for.srv.lab.db

Ta komenda sprawdzi nam poprawność konfiguracji strefy przeszukiwania do przodu dla naszej domeny.

named-checkzone 0.0.0.10.in-addr.arpa /etc/bind/rev.srv.lab.db

Ostatnia komenda sprawdzi nam poprawność konfiguracji strefy przeszukiwania wstecznego dla naszej domeny.

Jeżeli komendy te zachowają się tak samo jak na screenie to gratuluję! Wszystko zostało skonfigurowane poprawnie. Jeżeli coś pójdzie nie tak to komendy te poinformują nas, gdzie jest błąd i co nim jest.

```
root@dlp:/home/ubuntu# named-checkconf
root@dlp:/home/ubuntu# named-checkzone srv.lab /etc/bind/for.srv.lab.db
zone srv.lab/IN: loaded serial 3
OK
root@dlp:/home/ubuntu# named-checkzone 0.0.0.10.in-add.arpa /etc/bind/rev.srv.lab.db
zone 0.0.0.10.in-add.arpa/IN: loaded serial 1
OK
```

Restart:

systemctl restart bind9

Wnioski:

- Jeśli wszystkie trzy komendy zwracają brak błędów, to oznacza, że konfiguracja serwera DNS oraz konfiguracja stref przeszukiwania do przodu i wstecznego są poprawne.
- W przypadku wystąpienia błędów, komendy te powinny dostarczyć informacji o konkretnej lokalizacji błędu, co ułatwia identyfikację i naprawę problemów z konfiguracją DNS.
- Po wykryciu i naprawieniu ewentualnych błędów można ponownie uruchomić te komendy, aby potwierdzić, że konfiguracja serwera DNS jest teraz poprawna.

Zgłoszenie 6

3. Konfiguracja serwera do świadczenia usług.

a. przygotowanie serwera do świadczenia usług DNS-owych. W tym celu musimy dodać w Netplanie do karty LAN adres IP serwera DNS, czyli samego siebie. Wpisujemy polecenie:

nano /etc/netplan/00-installer-config.yaml

Dla interfejsu LAN (np. enp0s8) dodaj serwer DNS i jego adres IP 10.0.0.3:

Sprawdzamy poprawność konfiguracji poleceniami:

```
netplan try
```

```
netplan apply
```

Jeśli uzyskamy powyższy efekt, to znaczy, że wszystko jest ok.

b. sprawdź stan systemd-resolved

```
ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
```

```
systemctl restart systemd-resolved
```

```
resolvectl status
```

c. Przetestuj działanie serwera DNS korzystając z dwóch poleceń. Pierwsze wchodzi w skład pakietu bind9utils, czyli dig wyświetla nam więcej informacji o danej domenie. Istotna dla nas jest sekcja ANSWER SECTION. Tutaj wyświetlana jest informacja o rekordzie. Prostszym poleceniem jest nslookup. Wyświetla ono tylko podstawowe informacje. Wpisujemy:

```
dig dlp.srv.lab
```

```
nslookup dlp.srv.lab
```

```
root@dlp:/home/ubuntu# dig dlp.srv.lab

; <<>> DiG 9.18.39-0ubuntu0.24.04.3-Ubuntu <<>> dlp.srv.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14954
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;dlp.srv.lab.                   IN      A

;; ANSWER SECTION:
dlp.srv.lab.            0       IN      A       10.0.0.3

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 13 19:32:56 UTC 2026
;; MSG SIZE  rcvd: 56

root@dlp:/home/ubuntu# nslookup dlp.srv.lab
Server:         127.0.0.53
Address:        127.0.0.53#53

Name:   dlp.srv.lab
Address: 10.0.0.3
```

Wnioski:

- Polecenie **dig** jest bardziej wszechstronne i pozwala na uzyskanie obszernych informacji o domenie, co jest przydatne w bardziej zaawansowanych przypadkach diagnozowania problemów z DNS.
- Polecenie **nslookup** jest bardziej uproszczone i nadaje się do szybkiego sprawdzenia podstawowych informacji o domenie.
- Wybór między tymi dwoma narzędziami zależy od konkretnego przypadku i poziomu szczegółowości potrzebnej do diagnozowania problemów z DNS.

Zgłoszenie 7

4. Konfiguracja klienta.

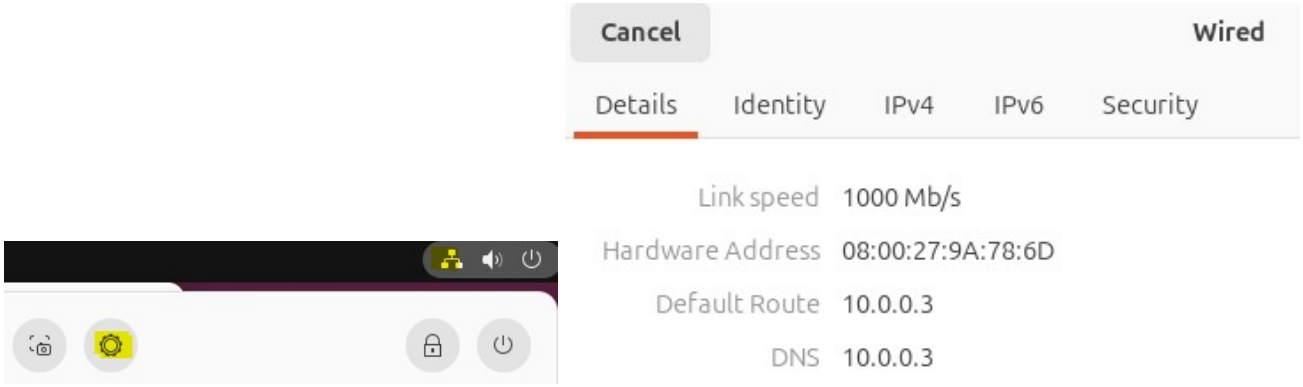
Przygotowanie do ćwiczenia.

Włącz klienta - Ubuntu desktop

Po uruchomieniu Ubuntu desktop podaj **login**: ubuntu **Password**: ubuntu

Jeśli zalogowałeś się do ubuntu wpisz sudo -s **Password**: ubuntu

Ustaw statyczny adresu IP 10.0.0.35/24 brama 10.0.0.3



a. Z sewera zpinguj naszego klienta. Najpierw na samą subdomenę (klient1) wpisujemy:

```
ping klient1
```

Sprawdzić, czy zadziała na pełną nazwę domenową:

```
ping klient1.srv.lab
```

ping → używa resolvera systemowego

```
root@dlp:/home/ubuntu# ping klient1
PING klient1.srv.lab (10.0.0.35) 56(84) bytes of data.
64 bytes from 10.0.0.35: icmp_seq=1 ttl=64 time=0.776 ms
64 bytes from 10.0.0.35: icmp_seq=2 ttl=64 time=0.999 ms
^C
--- klient1.srv.lab ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.776/0.887/0.999/0.111 ms
root@dlp:/home/ubuntu# ping klient1.srv.lab
PING klient1.srv.lab (10.0.0.35) 56(84) bytes of data.
64 bytes from 10.0.0.35: icmp_seq=1 ttl=64 time=0.758 ms
64 bytes from 10.0.0.35: icmp_seq=2 ttl=64 time=0.782 ms
^C
--- klient1.srv.lab ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.758/0.770/0.782/0.012 ms
```

b. Przetestuj działanie serwera DNS korzystając z dwóch poleceń. Pierwszym poleceniem jest nslookup. Wyświetla ono tylko podstawowe informacje. Drugie wchodzi w skład pakietu bind9utils, czyli dig wyświetla nam więcej informacji o danej domenie. Istotna dla nas jest sekcja ANSWER SECTION. Tutaj wyświetlana jest informacja o rekordzie. Wpisujemy:

```
nslookup klient1
```

```
dig klient1.srv.lab
```

dig → pyta konkretny DNS

```
root@dlp:/home/ubuntu# nslookup klient1
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   klient1.srv.lab
Address: 10.0.0.35

root@dlp:/home/ubuntu# dig klient1.srv.lab

; <<>> DiG 9.18.39-0ubuntu0.24.04.3-Ubuntu <<>> klient1.srv.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45474
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;klient1.srv.lab.               IN      A

;; ANSWER SECTION:
klient1.srv.lab.        6669    IN      A       10.0.0.35

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Apr 13 20:00:16 UTC 2026
;; MSG SIZE  rcvd: 60
```

Podaj wnioski:

- Jeśli klient był dostępny po nazwie hosta "klient1" i pełnej nazwie domenowej "klient1.srv.lab", to oznacza, że serwer DNS działa poprawnie i przekierowuje zapytania DNS do odpowiednich adresów IP.
- Polecenie **nslookup** jest przydatne do podstawowego testowania działania DNS, podczas gdy **dig** dostarcza bardziej szczegółowych informacji, w tym rekordy DNS.
- Ustawienie statycznego adresu IP jest przydatne w sytuacjach, gdy konkretny adres IP musi być przypisany do klienta, aby zapewnić stałą konfigurację sieciową.

Zgłoszenie 8

c. Sprawdź poprawność działania serwera DNS z klienta. Dokonaj zmian w pliku /etc/resolv.conf

```
nameserver 10.0.0.3
options edns0 trust-ad
search srv.lab
```

```
ubuntu@ubuntu2204:~$ sudo -s nano /etc/resolv.conf
ubuntu@ubuntu2204:~$ nslookup dlp
Server:         10.0.0.3
Address:        10.0.0.3#53

Name:   dlp.srv.lab
Address: 10.0.0.3

ubuntu@ubuntu2204:~$ nslookup dlp.srv.lab
Server:         10.0.0.3
Address:        10.0.0.3#53

Name:   dlp.srv.lab
Address: 10.0.0.3
```

```
ubuntu@ubuntu2204:~$ ping dlp
PING dlp.srv.lab (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=1.76 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=1.26 ms
^C
--- dlp.srv.lab ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 1.263/1.509/1.755/0.246 ms
ubuntu@ubuntu2204:~$ ping dlp.srv.lab
PING dlp.srv.lab (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.925 ms
^C
--- dlp.srv.lab ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.925/0.978/1.032/0.053 ms
```

Jak widać serwer DNS poprawnie podaje adres IP dla pełnej domeny (dlp.srv.lab) oraz dla samej subdomeny (dlp). Poprawnie pinguje na serwer korzystając z subdomeny.

Zgłoszenie 9

d. Łączność z komputerem z internetem

```
ubuntu@ubuntu2204:~$ ping google.pl
PING google.pl (142.250.120.94) 56(84) bytes of data.
^C
--- google.pl ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11345ms
```

Nie działa pingowanie do google.pl, gdyż serwera DNS nie ma routingu.

Najszybszym sposobem na konfigurację dostępu do sieci Internet serwera DNS jest:

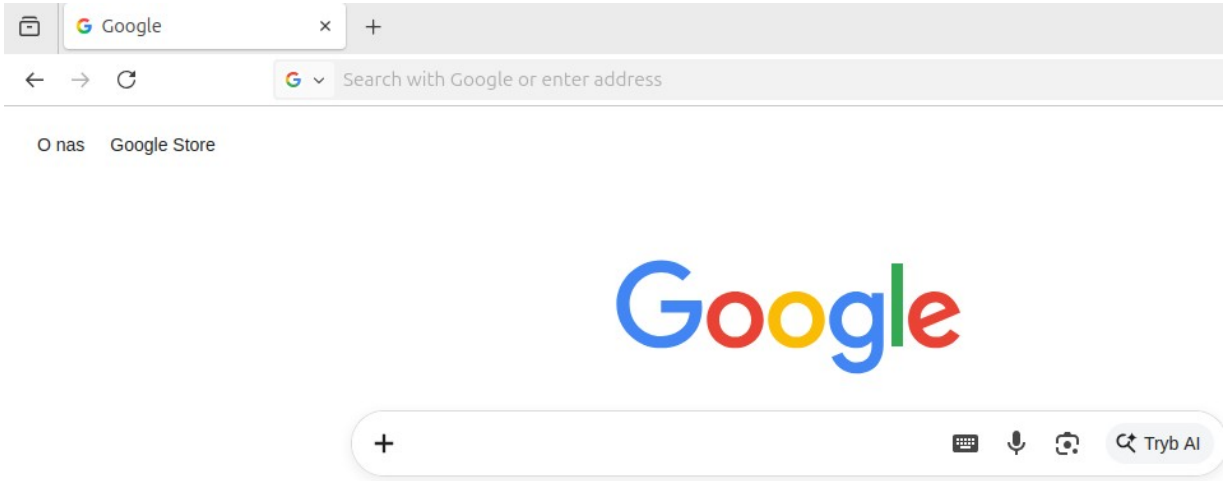
```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

```
root@dlp:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@dlp:~# iptables -t nat -A POSTROUTING -j MASQUERADE
```

Sprawdź

```
ubuntu@ubuntu2204:~$ ip a |grep enp0s3 |grep inet
    inet 10.0.0.35/24 brd 10.0.0.255 scope global noprefixroute enp0s3
ubuntu@ubuntu2204:~$ ping google.pl
PING google.pl (142.250.120.94) 56(84) bytes of data.
64 bytes from zo-in-f94.1e100.net (142.250.120.94): icmp_seq=1 ttl=254 time=21.4
 ms
64 bytes from zo-in-f94.1e100.net (142.250.120.94): icmp_seq=2 ttl=254 time=22.3
 ms
64 bytes from zo-in-f94.1e100.net (142.250.120.94): icmp_seq=3 ttl=254 time=21.6
 ms
^C
--- google.pl ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 21.404/21.762/22.301/0.387 ms
```



Zgłoszenie 10

Zgłoś zakończenie ćwiczenia w celu sprawdzenia.

Przywróć pierwszą migawkę

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.