Wstęp

DNS (Domain Name Server, system nazw domen) odpowiada za tłumaczenie nazw domenowych na adresy IP. Dzięki niemu zamiast pamiętać złożony adres IP *212.77.98.9* wystarczy, że zapamiętamy *wp.pl*. To właśnie on ułatwia nam życie online na każdym kroku.

Protokół ten wykonuje 3 typy operacji:
- tłumaczy domeny na adresy IP (DNS),
- tłumaczy adresy IP na domeny (RevDNS),
- tłumaczy domeny na domeny (CNAME).

Posiada on strukturę drzewiastą, inaczej zwaną hierarchiczną. Korzeń oznaczany jest przez kropkę. Poniżej znajdują się domeny najwyższego poziomu (top-level domains – TLDs), takie jak .pl, .eu, .com itp. Domeny najwyższego poziomu mogą zawierać domeny drugiego poziomu (second level domains) takie jak np. wojst.pl. Później domeny mogą być trzeciego poziomu jak np. mail.generatorkultury.eu.

Systematyzując:
1. root – kropka (.)
2. top-level domains (.pl .eu .com)
3. second level domains (zspbialarawska.pl wojst.pl)
4. third level domains (mail.generatorkultury.eu)

Na szczycie hierarchii DNS znajdują się root serwery, które są zarządzane przez różne organizacje autoryzowane przez ICANN. Aktualnie na świecie działa 13 root serwerów:

a.root-servers.net. 198.41.0.4
b.root-servers.net. 192.228.79.201
c.root-servers.net. 192.33.4.12
d.root-servers.net. 199.7.91.13
e.root-servers.net. 192.203.230.10
f.root-servers.net. 192.5.5.241
g.root-servers.net. 192.112.36.4
h.root-servers.net. 128.63.2.53
i.root-servers.net. 192.36.148.17
j.root-servers.net. 192.58.128.30
k.root-servers.net. 193.0.14.129
l.root-servers.net. 199.7.83.42
m.root-servers.net. 202.12.27.33

Root serwery obsługują zapytania tylko dla domen najwyższego poziomu i dostarczają klientom adresy IP serwerów odpowiedzialnych za dane domeny TLD.

Protokół DNS posługuje się komunikacją klient-serwer. Działa na porcie 53. Komunikacja pomiędzy serwerami odbywa się po protokole TCP, natomiast pomiędzy klientem a serwer na protokole UDP.

Przeanalizujmy następującą sytuację: użytkownik wpisuje w przeglądarkę internetową adres *wojst.pl*. Co się wtedy dzieje „pod maską”?

1. **Przeglądarka** komunikuje się z **serwerem DNS zdefiniowanym w systemie** i pyta „*Czy znasz adres IP serwera wojst.pl*”?

2. **Serwer DNS zdefiniowany w systemie** komunikuje się z **root serwerem** z tym samym zapytaniem.
3. **Root serwer,** z racji że posiada tylko informacje o serwerach TLDs, odsyła nas do **serwera domeny .pl**
4. **Serwer DNS zdefiniowany w systemie** wysyła zapytanie do **serwera domeny .pl** *czy zna adres serwera wojst.pl*. Ona niestety nie posiada takich informacji, ale wie że informacje o takiej domenie posiada serwer zdefiniowany w niej (podczas rejestracji domeny podajemy serwery gdzie będzie utrzymywana).
5. **Serwer DNS zdefiniowany w systemie** wysyła zapytanie do **serwera otrzymanego w poprzednim kroku** czy *zna adres IP dla strony wojst.pl*. Serwer ten posiada takie informacje i wysyła je do nas.
6. W tym momencie **serwer DNS zdefiniowany w systemie** zwraca adres IP do **przeglądarki** i wówczas wysyłane jest zapytanie HTTP pod wskazany adres.

Jak widzimy zawsze komunikacja jest dwustronna, pytanie – odpowiedź.

W strukturze DNS wyróżniamy:
- primary server – główny serwer, który utrzymuje oryginalne dane domeny
- secondary serwer – zapasowy serwer, jego dane kopiowane są z serwera głównego, uruchamiany jest dla redundancji i odciążenia serwera głównego
- cache server – serwer cachujący, jego dane kopiowane są z serwera i przechowywane w pamięci
- forwarding dns server – przekazuje zapytania od klientów do innych serwerów DNS
- klient DNS – host korzystający z serwerów DNS w celu rozwiązania nazw domenowych

Przestrzeń adresowa, którą zarządza dany serwer DNS nazywana jest strefą, a pliki z danymi nazywane są plikami stref lub bazą danych strefy. Pliki stref zawierają dyrektywy i rekordy danej domeny.

Rekordy domeny umożliwiają konfigurowanie „ruchu w Twojej domenie”. Za każdym razem gdy użytkownik Internetu otwiera Twoją stronę WWW albo gdy Ty wysyłasz lub odbierasz e-maila z adresem Twojej domeny lub gdy korzystasz z innych usług, np. ftp czy ssh to wtedy generowany jest tzw. ruch w Twojej domenie. Rekordy domeny zapisane są w tzw. pliku strefy serwera DNS.

Główne typy rekordów DNS:
A – mapuje nazwę domenową na adres IPv4
AAAA – mapuje nazwę domenową na adres IPv6
MX – mapuje nazwę domenową na adres serwer pocztowego
CNAME – definiuje alias nazwy domenowej, subdomeny
NS – mapuje nazwę domenową na listę serwerów DNS dla tej domeny
definiuje on informację o serwerze, który należy odpytać aby otrzymać informacje o danej domenie
TXT - pozwala dołączyć dowolny tekst do rekordu DNS. Rekord ten może być użyty np. do weryfikacji własności domeny przykładowo w usługach firmy Google.

Przypisanie na kliencie serwera DNS

W systemach Linux serwery definiujemy albo w GUI poprzez *NetworkManager*, albo z poziomu CLI – znajdują się one w bliku */etc/resolv.conf*. Definiujemy je jako:
nameserver IP_serwera_DNS
Kolejne serwery definiujemy w następnych wersach w taki sam sposób.

W przypadku systemów z rodziny Windows: *Właściwości karty sieciowej -> Protokół internetowy w wersji 4 (TCP/IPv4) -> Użyj następujących adresów serwerów DNS*.

W tym miejscu wpisujemy adres IP naszego głównego i alternatywnego serwera DNS.
Po co wgl definiujemy alternatywny serwer DNS na kliencie? W przypadku, gdy pierwszy serwer przestanie odpowiadać wówczas jego rolę zastępuje serwer alternatywny.

Oczywiście powyższe kroki wykonujemy, gdy chcemy sami zdefiniować z jakich serwerów mamy korzystać. Podczas otrzymywania adresu IP z serwera DHCP otrzymujemy również adresy serwerów DNS zdefiniowanego przez administratora.

Narzędzia przydatne podczas administracji serwerem DNS

Pierwszym z narzędzi będzie *nslookup*, zwraca nam ono informację o adresie IP danego serwera oraz informację jaki serwer DNS obsłużył dane zapytanie. Przykład użycia:
nslookup wp.pl

Drugim z kolei będzie powszechnie znany *ping*. W czym on nam tutaj może pomóc? Możemy po prostu puścić pinga do danego serwera (np.: *ping wp.pl)*. Dowiemy się wówczas nie tylko czy serwer działa, ale również czy dobrze / w ogóle została rozwiązana nazwa domenowa na adres IP.

Kolejnym z narzędzi zewnętrznych jest *dig*. Bez przełączników zwraca on takie informacje jak: rekord A domeny, serwer obsługujący dane zapytanie oraz czas odpowiedzi. To ostatnie przyda nam się w przypadku testowania działania cache servera. Przykład użycia to po prostu *dig wojst.pl*

Dwa ostatnie narzędzia dostarczane są z oprogramowaniem serwera bind.
named-checkconf służy do sprawdzenie konfiguracji serwera bind. Gdy znajdzie jakiś błąd w plikach konfiguracyjny (chociażby literówkę) wyświetli on nam informacje – gdy nic nie zwraca, znaczy że wszystko jest ok. Wywołujemy jest bez żadnych przełączników i argumentów.
Ostatnie z narzędzi (*named-checkzone)* służy do sprawdzenia konfiguracji strefy domeny. Wywołanie następuje z podaniem domeny oraz pliku zawierającego strefę: *named-checkzone wojst.pl db.wojst.pl*

Instalacja serwera DNS na systemie Linux

Na początku oczywiście warto pamiętać aby przypisać statyczny adres IP. W konfiguracji netplan w adresach serwerów DNS podajemy taki sam adres jaki przypisujemy dla karty sieciowej (bind będzie obsługiwał również zapytania naszego serwera).

Aby zainstalować serwer DNS należy zainstalować pakiety **bind9, bind9utils** oraz **dnsutils.** Po tym zostanie utworzona usługa *named*, która możemy zarządzać poprzez *systemctl*.

apt update
apt install bind9 bind9utils dnsutils
systemctl enable/disable/start/stop/restart named

Pliki konfiguracyjne usługi (w przypadku systemu Ubuntu) znajdują się w katalogu */etc/bind*. Przejrzyjmy jego zawartość:

- *db.127* - przykładowa konfiguracja strefy przeszukiwania wstecznego
- *db.local* - przykładowa konfiguracja strefy przeszukiwania do przodu
- *named.conf* - globalna konfiguracja DNS
- *named.conf.default-zones* - domyślne strefy przeszukiwania
- *named.conf.local* - lokalna konfiguracja DNS
- *named.conf.options* - konfiguracja serwera DNS

Na domyślnej konfiguracji serwer pełni funkcję cache serwera – odpytuje inne serwery i przechowuje odpowiedzi w pamięci cache.

Skonfigurujmy najpierw nasz serwer jako *forwarder*. W tej sytuacji wszystkie zapytania DNS będzie przekierowywał do zdefiniowanych przez nas serwerów, a odpowiedzi przechowywał w pamięci cache. Aby to osiągnąć w pliku *named.conf.options* musimy odkomentować sekcję *forwarders* (usunąć // na początku linii) i zmienić domyślne serwery złożone z zer na adresy IP preferowanych przez nas serwerów. Serwery wpisujemy w kolejnych wersach, każdy zakończony średnikiem. Finalnie sekcja powinna wyglądać następująco:

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

Poprawność konfiguracji możemy sprawdzić narzędziem *named-checkconf*.

W tym miejscu możemy także rozwinąć temat cachowania odpowiedzi. Aby sprawdzić zawartość cache naszego serwera musimy wykonać następujące kroki:

1. Wykonanie zrzutu bazy do pliku
rndc dumpdb
2. Przeglądanie pliku z bazą
Plik znajduje się w lokalizacji */var/cache/bind/named_dump.db*
Jest to zwykły plik tekstowy, więc możemy przeglądać go za pomocą narzędzi *cat, less, tail, head, nano* itp.

Konfiguracja strefy dla domeny

Przejdźmy teraz do głównej roli serwera DNS czyli przechowywania informacji o domenach. Takie informacje o poszczególnych domenach przechowywana są w plikach stref.

Strefa DNS to wszystkie informacje, które posiada serwer DNS o danej domenie.

Zajmijmy się najpierw wstępem teoretycznym do stref. Pliki ze strefami zawierają dyrektywy i rekordy.
Dyrektywy zaczynają się od znaku *$*. Możemy tutaj zdefiniować *TTL* (czyli czas życia przez ile sekund serwer podrzędny powinien trzymać strefę w pamięci podręcznej i nie musi odpytywać się ponownie, żeby nie generować niepotrzebnego ruchu i opóźnień) dla danej domeny oraz *ORIGIN*, czyli po prostu nazwę domenową.

Następnie strefa powinna zawierać sekcję *SOA – Start Of Authority*. Zawiera ona podstawowe informacje o domenie przeznaczone dla serwerów,
- główny serwer nazw dla domeny (autoryzowany dla danej domeny)
- adres email administratora domeny (znak @ zamieniamy na kropkę)
- numer seryjny (serial), który powinien być zwiększany wraz z każdą edycją strefy
przyjmuje się, że jego składnia wygląda następująco: RRRRMMDDnn – Rok, miesiąc, dzień, numer modyfikacji w danym dniu
- refresh - czas w sekundach co ile strefa powinna być odświeżana przez serwery podrzędne
- retry - czas ponownej próby kontaktu z serwerem w przypadku braku odpowiedzi
- expire - po jakim czasie serwer ma odrzucić wcześniej pobraną strefę, jeśli w międzyczasie nie można było się skontaktować z serwerem master i nie doszło do aktualizacji sesji

- TTL, czyli czas życia przez ile sekund serwer podrzędny powinien trzymać strefę w pamięci podręcznej i nie musi odpytywać się ponownie, żeby nie generować niepotrzebnego ruchu i opóźnień

Ostatnim elementem strefy są rekordy. Zostały one wyjaśnione wyżej.

Przejdźmy do części praktycznej. Najpierw utwórzmy plik ze strefą dla danej domeny. Na potrzeby tego artykułu będziemy operować na domenie *wojst.local*

W tym celu w katalogu */etc/bind* utwórzmy plik *db.wojst.local*
Dobrą praktyką jest stosowanie odpowiedniego nazewnictwa pliku. db (database) oznacza strefę, a po niej podajemy pełną domenę.

Utwórzmy strefę według przykładu:

```
$TTL 3H
wojst.local.    IN SOA  dns-server.wojst.local. root.wojst.local. (
                        2022123001
                        1D
                        1H
                        1W
                        3H )

wojst.local.    IN      NS      dns-server.wojst.local.
dns-server      IN      A       192.168.1.147
wojst.local.    IN      A       192.168.1.147
```

!! NALEŻY PAMIĘTAĆ, ABY NA KOŃCU DOMENY ZAWSZE WSTAWIAĆ KROPKĘ !!
dns-server to hostname mojego serwera, należy go odpowiednio zamienić na wykorzystywany przez Ciebie

Przeanalizujmy utworzony plik:
- definiujemy TTL dla domeny
- określamy, że informacje dla domeny wojst.local są przechowywane w strefie SOA na serwerze dns-server, a adres mailowy administratora to root@wojst.local
- zdefiniowaliśmy trzy rekordy: informacje, że domena jest przechowywana na danym serwerze, serwer ma dany adres IP oraz wskazaliśmy adres IP dla danej domeny

Za pomocą narzędzia *named-checkzone* sprawdźmy konfigurację strefy.
named-checkzone wojst.local db.wojst.local

Na sam koniec pozostało nam jedynie uruchomienie obsługi domeny na danym serwerze. W tym celu do pliku *named.conf.local* dopiszemy następujące informacje:

```
zone "wojst.local" IN {
type  master;
file "/etc/bind/db.wojst.local";
allow-update { none; };
};
```

Tłumacząc wprowadzone zmiany:
- strefa danej domeny (w tym miejscu definiujemy już strefę bez kropki na końcu)

- typ serwera master/slave – informacja dla serwera jakim typem będzie (w przypadku serwera slave pobiera on dane o domenie z serwera głównego)
- lokalizacja pliku ze strefą (należy zwrócić uwagę, aby podać pełną ścieżkę)
- brak określenie adresu IP serwera głównego, z którego miałby pobierać dane o domenie

Poprawność konfiguracji serwera możemy sprawdzić z wykorzystaniem narzędzi *dig* oraz *nslookup* dla domeny *wojst.local*