**Czytaj lub słuchaj artykuł online**

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

**https://xo.pl/it-na-wesolo-net-dns**

SIECI KOMPUTEROWE

# DNS, czyli książka adresowa całego Internetu

Witamy ponownie na naszej Autostradzie Pakietów, zwanej potocznie Internetem!

Na osiedlu Spokojna Sieć życie toczy się swoim rytmem. Urząd **DHCP** rozdaje tablice rejestracyjne. **TCP** od dwóch godzin potwierdza odbiór korespondencji, **UDP** dostarczył paczkę do niewłaściwego miasta, a zarządca **NAT-u** zakupił nowy zeszyt.

Stary znalazł się w lodówce. Na drugiej półce. Pod mlekiem. Nikt nie potrafi wyjaśnić, jak się tam znalazł.

Tymczasem pewien kierowca postanowił odwiedzić znajomego. I odkrył, że **zna jego nazwisko, ale nie ma pojęcia, gdzie mieszka.**

## Dzień dobry, szukam Google

Kierowca podjeżdża do skrzyżowania.

— Dzień dobry, chciałbym pojechać do Google.

— Adres?

— Google.

— To nazwa.

— No właśnie!

— A ja pytam o adres.

— PRZECIEŻ PANU PODAŁEM!

— Nie. Podał pan nazwę.

— A CO ZA RÓŻNICA?!

— Na naszej autostradzie potrzebujemy adresu IP.

— A SKĄD JA MAM GO WZIĄĆ?!

— Z książki adresowej.

— A GDZIE JEST TA KSIĄŻKA?!

— W DNS.

— A CO TO JEST DNS?!

— Domain Name System.

— CZYLI?!

— System, który między innymi pozwala ustalić **adres IP** na podstawie nazwy domenowej.

— A NIE MOŻNA BYŁO OD RAZU TAK POWIEDZIEĆ?!

— Próbowałem. Pan krzyczał.

**DNS (Domain Name System)** to rozproszony system nazw. Dzięki niemu możemy wpisywać `www.google.com`, zamiast pamiętać **adresy IP**. Tylko że nasza książka adresowa ma pewną osobliwość: **nikt nie ma obowiązku przechowywać całej książki.**

## Pierwsze okienko, czyli lokalny informator

— Dzień dobry, jaki adres ma `www.example.com`?

— Chwileczkę.

Urzędnik kartkuje notes.

— Nie mam.

— JAK TO PAN NIE MA?!

— Nie pytał mnie jeszcze nikt o ten adres.

— TO JAKI Z PANA URZĘDNIK?!

— Rekurencyjny.

— JAKI?!

— **Resolver DNS**.

— A CO PAN ROZWIĄZUJE?!

— Nazwy.

— TO PROSZĘ ROZWIĄZAĆ MOJĄ!

— Właśnie zamierzam.

Resolver rekurencyjny przyjmuje pytania klientów i próbuje znaleźć odpowiedź. Zanim zacznie wydzwaniać po świecie, zagląda do pamięci podręcznej, czyli **cache**.

— A jeśli pan już zna adres?

— Odpowiem od razu.

— A jeśli nie?

— Muszę zapytać innych.

— ILU?!

— Tylu, ilu będzie trzeba.

— TO JA MOŻE SAM POJADĘ?!

— Bez adresu?

— ...

— Właśnie. Proszę usiąść.

### Urząd najwyższy, czyli kropka na końcu świata

Resolver zaczyna szukać. Najpierw kontaktuje się z jednym z serwerów głównych DNS, czyli **root DNS servers**.

— Dzień dobry. Szukam `www.example.com`.

— My zajmujemy się najwyższym poziomem.

— To może znacie adres?

— Nie podamy końcowego adresu, ale wskażemy, gdzie pytać o `.com`.

— Dziękuję.

— Następny!

Kierowca robi wielkie oczy.

— CHWILECZKĘ! JAKĄ KROPKĘ?!

— Główną.

— JEST JAKAŚ GŁÓWNA KROPKA?!

— Tak.

— A GDZIE?!

— Na końcu pełnej nazwy domenowej.

— PRZECIEŻ TAM NIC NIE MA!

— W zwykłym zapisie ją pomijamy.

— CZYLI ONA JEST, ALE JEJ NIE WIDAĆ?!

— Dokładnie.

— JA ZACZYNAM PODEJRZEWAĆ, ŻE WY SOBIE TE ZASADY WYMYŚLACIE!

Pełną nazwę można zapisać jako `www.example.com.`. Ostatnia kropka oznacza korzeń drzewa DNS. Serwery root nie przechowują wszystkich adresów; pomagają odnaleźć serwery odpowiedzialne za domeny najwyższego poziomu, takie jak `.com`, `.pl` czy `.org`.

— CZYLI TO CENTRALNY URZĄD CAŁEGO INTERNETU?!

— Raczej najwyższy poziom rozproszonego systemu.

— A JAK SIĘ ZEPSUJE?!

— Istnieje wiele serwerów i instancji tej infrastruktury.

— CZYLI NIE MA JEDNEGO PANA Z PIECZĄTKĄ?!

— Nie.

— TO JAK WY FUNKCJONUJECIE?!

— Zaskakująco dobrze.

### Dział .com odsyła do właściwego właściciela

Resolver dzwoni do serwera obsługującego `.com`.

— Dzień dobry. Szukam `www.example.com`.

— Aha. To nie u nas.

— JAK TO NIE U WAS?!

— My wiemy, kto odpowiada za `example.com`.

— To proszę podać.

— Oto odpowiednie serwery nazw.

Kierowca nie wytrzymuje.

— PAN JUŻ DZWONIŁ DWA RAZY!

— Zgadza się.

— I NADAL NIE MA ADRESU?!

— Jeszcze nie.

— TO CO PAN WŁAŚCIWIE USTALIŁ?!

— Kogo zapytać dalej.

— CZYLI ZADZWONIŁ PAN DO JEDNEGO URZĘDU, ŻEBY DOWIEDZIEĆ SIĘ, DO KTÓREGO URZĘDU ZADZWONIĆ?!

— Tak.

— A DRUGI URZĄD?!

— Wskazał trzeci.

— TO JEST PRZECIEŻ POLSKA ADMINISTRACJA!

— Nie, proszę pana. Globalny system DNS. 🤣

Serwery **TLD (Top-Level Domain)** udzielają informacji potrzebnych do znalezienia serwerów autorytatywnych.

### Właściciel posesji wreszcie odbiera telefon

Trzeci telefon.

— Dzień dobry. Czy rozmawiam z serwerem autorytatywnym dla `example.com`?

— Tak.

— Poszukuję adresu `www.example.com`.

— Już podaję.

— WRESZCIE! — krzyczy kierowca.

— `192.0.2.80`.

— HURRA!!!

Resolver przekazuje odpowiedź.

— TO TERAZ MOGĘ JECHAĆ?!

— Tak.

— A NIE MOŻNA BYŁO ZADZWONIĆ OD RAZU DO OSTATNIEGO URZĘDU?!

— Można, gdy wiemy, gdzie się znajduje.

— A NIE WIEDZIELIŚMY?!

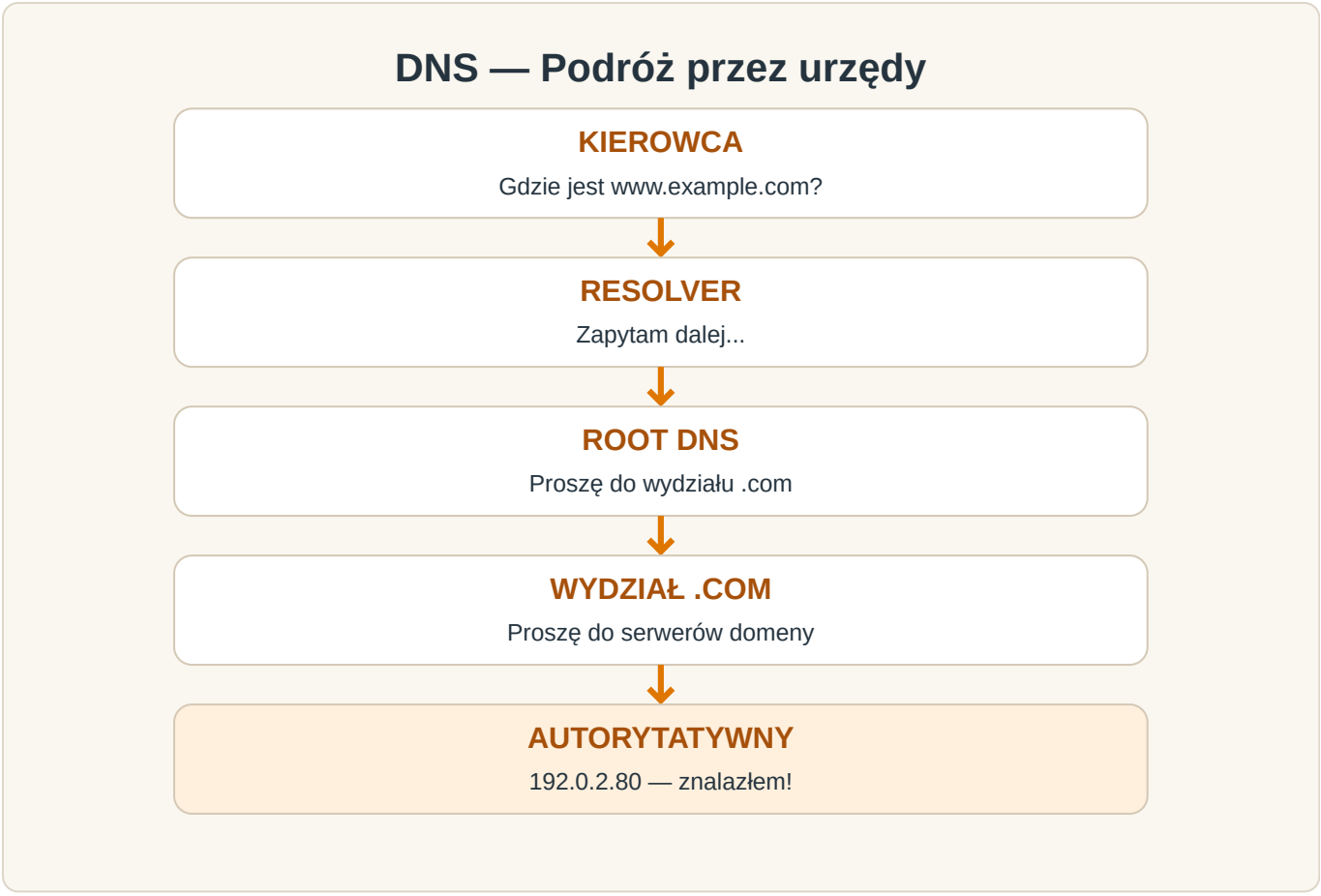
— Właśnie dlatego pytaliśmy poprzednie.

— ...

— Proszę pana?

— NIE. NIC. JADĘ.

Adres `192.0.2.80` jest przykładem z przestrzeni dokumentacyjnej. **Serwer autorytatywny** odpowiada na podstawie danych swojej strefy.




### Panie, ja mam ten numer zapisany od wczoraj!

Nazajutrz kierowca wraca.

— Znowu szukam `www.example.com`.

— `192.0.2.80`.

— JAK PAN TO TAK SZYBKO ZNALAZŁ?!

— Zapisałem sobie wczoraj.

— CZYLI NIE MUSI PAN DZWONIĆ?!

— Dopóki zapis jest ważny.

— A JAK DŁUGO?!

— Zależy od **TTL**.

— CO?!

— **TTL**.

— NIE! MY JUŻ MIELIŚMY **TTL** NA AUTOSTRADZIE!

— To inny **TTL**.

— JAK TO INNY?!

— W pakiecie IP ogranicza liczbę węzłów. W DNS czas przechowywania w cache.

— TO WY MACIE DWA RÓŻNE **TTL**?!

— Tak.

— I NIKT NIE WPADŁ NA POMYSŁ, ŻEBY NAZWAĆ JE INACZEJ?!

— Najwyraźniej nie.

**DNS TTL (Time To Live)** wyznacza czas przechowywania odpowiedzi w pamięci podręcznej. **TTL** 3600 oznacza godzinę.

— Czyli jeśli właściciel zmieni adres, a pan ma stary zapis...

— Przez jakiś czas mogę zwracać starą odpowiedź.

— ALE TAM JUŻ NIKT NIE MIESZKA!

— Mój wpis jeszcze nie wygasł.

— TO NIECH PAN GO SKREŚLI!

— W standardowym działaniu cache czekamy na wygaśnięcie.

— PAN MA STARY NOTES I JESZCZE JEST Z TEGO DUMNY?!

### DNS Cache — Stary notes

**NOTES RESOLVERA**

192.0.2.80

TTL: pozostało 1800 s

**SERWER ŹRÓDŁOWY**

192.0.2.81

Nowy adres

**ALE JA JUŻ TAM NIE MIESZKAM!**

Dlatego zmiany DNS nie muszą być widoczne wszędzie natychmiast. Często to nie tajemnicza „propagacja”, lecz **stare, niewygasłe wpisy w cache**.

## Książka adresowa ma więcej niż jedną rubrykę

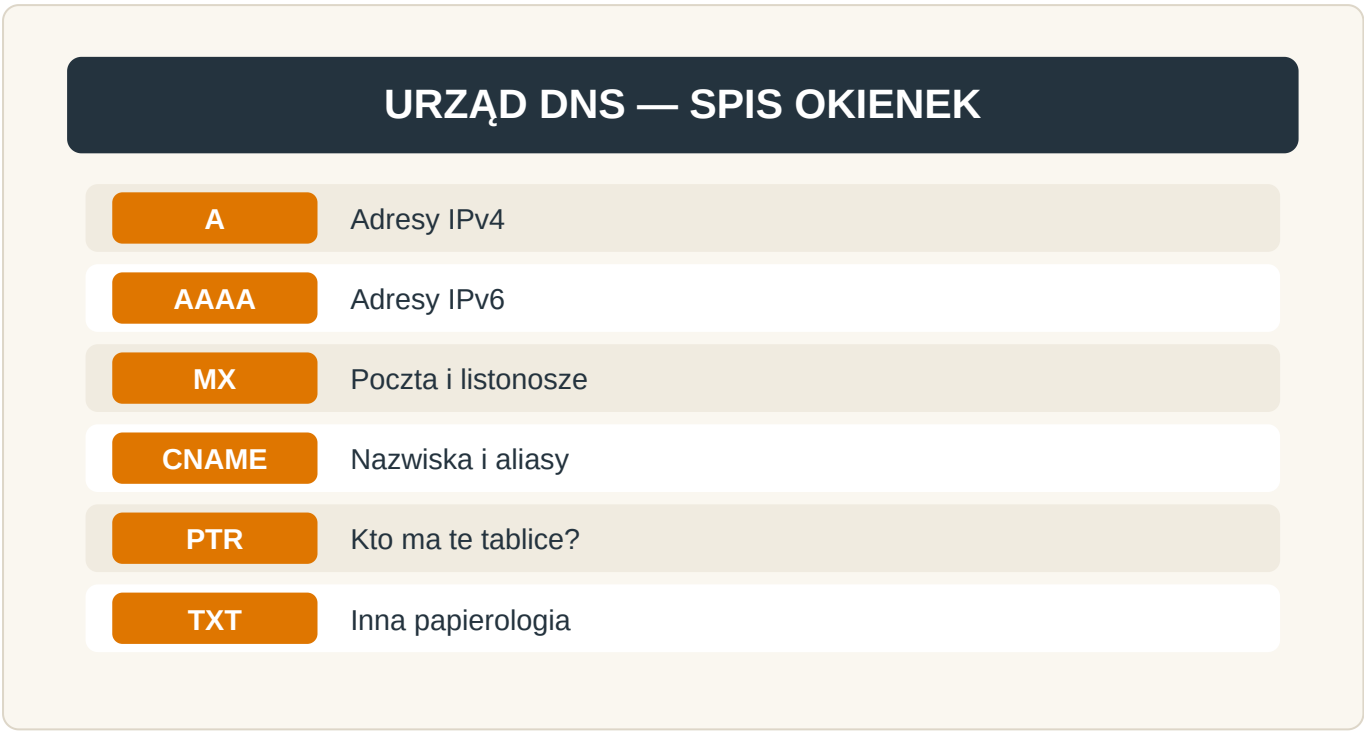
— Czyli pan przechowuje tylko **adresy IP**?

— Nie.

— A CO JESZCZE?!

— Różne rodzaje rekordów.

— JAKIE?!




| Rekord | Co mówi kierowcy? |
|---|---|
| **A** | Adres **IPv4** |
| **AAAA** | Adres **IPv6** |
| **CNAME** | Alias innej nazwy |
| **MX** | Dokąd kierować pocztę |
| **NS** | Serwery nazw |
| **TXT** | Informacje tekstowe |
| **PTR** | Nazwa powiązana z adresem przy zapytaniu odwrotnym |
| **SOA** | Informacje administracyjne strefy |
| **CAA** | Które urzędy certyfikacji mogą wydawać **certyfikaty** |

— Chciałbym **IPv4**.

— Rekord A.

— A **IPv6**?

— AAAA.

— CZTERY RAZY A?!

— Zgadza się.

— NIE MOGLIŚCIE NAZWAĆ GO B?!

— Nie.

— A CNAME?!

— Alias.

— A MX?!

— Poczta.

— A PTR?!

— Wyszukiwanie odwrotne.

— A TXT?!

— Tekst.

— A CO JEST W TEKŚCIE?!

— To zależy.

— ZNOWU „TO ZALEŻY”?!

## Cztery litery A i wielka panika IPv6

Do okienka podjeżdża przedstawiciel **IPv6**.

— Poproszę rekord AAAA.

— Oczywiście.

— PRZEPRASZAM, ILE A?! — pyta stary kierowca.

— Cztery.

— A DLACZEGO AŻ CZTERY?!

— Rekord A wskazuje **IPv4**, AAAA wskazuje **IPv6**.

— CZYLI NIE DOŚĆ, ŻE MACIE ADRESY Z DWUKROPKAMI, TO JESZCZE CZTERY LITERY A?!

— Tak.

— A CO BĘDZIE PRZY IPv8?!

— Nie mamy takich planów w tym znaczeniu.

— PEWNIE OSIEM LITER A!

— Proszę nie podpowiadać. 🤣

Jedna nazwa może mieć rekordy A i AAAA, a wybór połączenia zależy od systemu i dostępności trasy. DNS sam nie decyduje, którą drogą jedzie pojazd.

## CNAME, czyli proszę jechać pod inne nazwisko

— Gdzie mieszka `sklep.example.com`?

— Pod nazwą `serwer.example.net`.

— ALE JA SZUKAM SKLEPU!

— To alias.

— CZYLI NIE MA PAN ADRESU?!

— Musimy ustalić adres wskazanej nazwy.

— A JEŚLI ONA WSKAZUJE JESZCZE INNĄ?!

— Wtedy szukamy dalej.

— CZYLI MOGĘ JEŹDZIĆ OD URZĘDU DO URZĘDU?!

— Przy błędnej konfiguracji może powstać problem.

— JA JUŻ WIEM, ŻE POWSTANIE!

**CNAME (Canonical Name)** tworzy alias nazwy, nie odrębny **adres IP**.

— Czyli sklep może zmienić siedzibę, ale jego nazwa zostanie?

— O ile odpowiednio utrzymamy wpisy DNS.

— TO WRESZCIE COŚ PRAKTYCZNEGO!

— Dziękuję.

— ALE DLACZEGO TAK DŁUGO PAN TO TŁUMACZYŁ?!

— Bo pan pytał o nazwisko.

## MX, czyli poczta nie musi mieszkać tam, gdzie sklep

Listonosz **TCP** wiezie list do `biuro@example.com`.

— Mam pocztę!

— To nie tutaj.

— ALE DOMENA TA SAMA!

— Proszę sprawdzić MX.

— A CO TO JEST?!

— Mail Exchanger.

Rekord **MX** wskazuje serwery pocztowe i ich preferencje.

— Czyli jeśli pierwszy urząd pocztowy nie odpowiada?

— Nadawca może spróbować kolejnego.

— A JEŚLI ŻADEN?!

— **TCP** będzie miało kolejny powód do formularzy.

— O NIE, TYLKO NIE ONI!

## PTR, czyli znam tablice, ale czyj to samochód?

— Dzień dobry. Znam numer `193.24.14.111`, ale nie znam nazwy.

— Zapytanie odwrotne. Już sprawdzam PTR.

— I CO?!

— `mail.msw.gov.pl`.

— ...

— Coś nie tak?

— NIC. JA TYLKO PYTAŁEM.

— WPISAĆ SPRAWĘ DO REJESTRU?!

— NIE! ABSOLUTNIE NIE! 🤣

**Reverse DNS** wykorzystuje rekordy **PTR**. Dla **IPv4** działa w przestrzeni `in-addr.arpa`, a dla **IPv6** w `ip6.arpa`. Sam PTR nie dowodzi właścicielstwa maszyny ani zgodności z rekordami A lub AAAA.

— CZYLI TO NIE JEST DOWÓD TOŻSAMOŚCI?!

— Nie.

— TO PO CO NAM TO?!

— Do diagnostyki i między innymi poczty.

— AHA. ZNOWU LISTONOSZ!

## Nie ma takiej ulicy! NXDOMAIN!

— Gdzie jest `nieistniejacy-serwer.example.com`?

— Nie ma.

— JAK TO NIE MA?!

— Nie istnieje taka nazwa.

— ALE MAM JĄ ZAPISANĄ!

— Proszę sprawdzić pisownię.

— A ZA PIĘĆ MINUT?!

— Nadal może nie być.

— TO CO PAN MI WYSTAWI?!

— NXDOMAIN.

— A MOGĘ SIĘ ODWOŁAĆ?!

— Do właściciela strefy.

— TO PROSZĘ PODAĆ JEGO ADRES!

— Chce pan go znaleźć przez DNS?

— NIECH PAN NIE ZACZYNA!!!

**NXDOMAIN** oznacza brak wskazanej nazwy. To co innego niż istniejąca nazwa bez rekordu określonego typu. Odpowiedzi negatywne również mogą być cache'owane.

— CZYLI POTRAFI PAN ZAPAMIĘTAĆ, ŻE CZEGOŚ NIE MA?!

— Tak.

— PANOWIE MAJĄ NIESAMOWITĄ PAMIĘĆ DO RZECZY, KTÓRE NIE ISTNIEJĄ!

## Dwa urzędy, dwie różne odpowiedzi

Jeden informator mówi `192.0.2.80`, drugi `192.0.2.81`.

— KTÓRY Z PANÓW KŁAMIE?!

— Niekoniecznie którykolwiek.

— TO JAK MAM DWA ADRESY?!

— Nazwa może wskazywać wiele adresów, a odpowiedzi różnić się w czasie i zależnie od miejsca.

— KTÓRY JEST PRAWDZIWY?!

— Oba mogą być poprawne.

— A MOŻE JEDEN Z PANÓW NIE UMIE CZYTAĆ?!

— Tej możliwości nie obejmuje specyfikacja DNS. 🤣

Wiele adresów dla jednej nazwy może być zamierzone, np. przy dostarczaniu treści z różnych lokalizacji.

## DNSSEC, czyli pieczątka, której nie da się łatwo podrobić

Na osiedlu pojawia się oszust.

— Od dziś adres banku jest u mnie.

— Na jakiej podstawie?

— Bo tak mówię.

— To nie wystarczy.

— A JAK PRZYBIJĘ PIECZĄTKĘ?!

— Kto ją wydał?

— Sam sobie zrobiłem.

— TO NIECH PAN SOBIE JESZCZE ZROBI KONTO W BANKU I TAM JE ZATRZYMA!

**DNSSEC** umożliwia kryptograficzną weryfikację autentyczności i integralności odpowiednich danych DNS w łańcuchu zaufania.

— CZYLI NIKT MNIE NIE OSZUKA?!

— Nie powiedziałem tego.

— JAK TO?!

— DNSSEC nie szyfruje zapytań ani nie dowodzi, że strona jest uczciwa.

— A ZESZYT OD **NAT**-U?!

— TEGO NIE OCHRONI JUŻ NIC!

## DNS przez szyfrowany tunel

Do urzędu wchodzi człowiek w ciemnych okularach.

— Chcę zapytać o adres, ale nie chcę, żeby ktoś podsłuchiwał.

— Może pan skorzystać z **szyfrowanego** połączenia.

— TAJNY KANAŁ!

— W pewnym sensie.

— I NIKT NIE WIE, O CO PYTAM?!

— Osoby postronne nie powinny odczytać zapytania na chronionym odcinku.

— A PAN WIE?!

— Muszę wiedzieć, żeby odpowiedzieć.

— TO CO TO ZA TAJEMNICA?!

— Przed osobami postronnymi, nie przede mną.

**DoT (DNS over TLS)** oraz **DoH (DNS over HTTPS)** szyfrują komunikację DNS na odpowiednim odcinku. **DNSSEC** realizuje inny cel: weryfikację danych.

— CZYLI MOGĘ MIEĆ **SZYFROWANIE** I PODPISY?!

— Tak.

— I CO JESZCZE?!

— Cały dział dokumentacji.

— NIE, DZIĘKUJĘ!

## A jeśli cały urząd DNS przestanie odpowiadać?

Kierowca wpisuje nazwę w przeglądarce. Cisza. Połączenie do znanego mu adresu IP działa.

— AUTOSTRADA DZIAŁA!

— Tak.

— SAMOCHODY JEŻDŻĄ!

— Tak.

— TO DLACZEGO NIE MOGĘ NIGDZIE POJECHAĆ?!

— Nie udaje się ustalić adresu z nazwy.

— CZYLI MAM SPRAWNY SAMOCHÓD I AUTOSTRADĘ, ALE KSIĄŻKA TELEFONICZNA JEST ZAMKNIĘTA?!

— W uproszczeniu.

— JA JUŻ NAPRAWDĘ WOLĘ POCZTÓWKI!

Awaria DNS potrafi sprawiać wrażenie awarii całego Internetu, choć komunikacja do znanych **adresów IP** nadal może działać.

## Co naprawdę robi nasza książka adresowa?

DNS jest **rozproszonym, hierarchicznym systemem nazw**, a różne serwery pełnią w nim różne role.

| Pojęcie | Na naszej autostradzie |
|---|---|
| **DNS** | Książka adresowa Internetu |
| **Resolver** | Informator szukający odpowiedzi |
| **Root DNS** | Najwyższy urząd wskazujący właściwy dział |
| **TLD** | Wydział odpowiedzialny za .pl, .com itd. |
| **Serwer autorytatywny** | Urząd prowadzący właściwą kartotekę |
| **A / AAAA** | Adres **IPv4** / **IPv6** |
| **CNAME** | Alias nazwy |
| **MX** | Poczta |
| **PTR** | Wyszukiwanie nazwy po adresie |
| **TTL DNS** | Ważność wpisu w notesie |
| **NXDOMAIN** | Takiej nazwy nie ma |
| **DNSSEC** | Kryptograficzna weryfikacja danych |
| **DoH / DoT** | **Szyfrowane** zapytania DNS |

DNS nie zastępuje **adresów IP** ani **routingu**. Kiedy znajdziemy numer, samochód nadal musi dojechać do celu.

Jeśli chcesz przejechać dalej po naszej Autostradzie Pakietów, zajrzyj także do tematów: **DHCP**, **TCP i UDP**, **NAT**.

## Tymczasem na osiedlu Spokojna Sieć...

Do okienka DNS podjeżdża lodówka.

— Szukam mleka.

— A ma pani nazwę domenową?

— `mleko`.

— To nie wystarczy.

— `www.mleko.pl`?

— Musiałbym sprawdzić.

Urzędnik zaczyna szukać. Root... .pl... serwery autorytatywne...

— PANIE, JA TYLKO CHCIAŁAM ZNALEŹĆ MLEKO!

— Proszę poczekać.

— ALE ONO JEST W MOJEJ LODÓWCE!

— To dlaczego pyta pani DNS?!

— BO MI NIKT NIE CHCE POWIEDZIEĆ, GDZIE LEŻY!

Wychodzi urzędnik **DHCP**.

— MÓWIŁEM, ŻE NA DRUGIEJ PÓŁCE!

— NIE MAM UPRAWNIEŃ DO DRUGIEJ PÓŁKI!

— TO PROSZĘ ZGŁOSIĆ DO WŁAŚCICIELA!

— WŁAŚCICIEL NIEDOSTĘPNY!

— A DNS CO MÓWI?!

Urzędnik DNS podnosi głowę.

— NXDOMAIN.

— JAKI NXDOMAIN?!

— Nie znalazłem takiej nazwy.

— PRZECIEŻ MLEKO ISTNIEJE!

— W DNS nie musi.

— ALE JA JE WIDZĘ PRZEZ SZYBĘ!

— To proszę użyć innego protokołu.

— JAKIEGO?!

— **OTWORZYĆ DRZWI.**

— Nie mogę.

— DLACZEGO?!

— Brak uprawnień.

Z tyłu odzywa się toster:

— A MOŻE ZROBIMY CNAME Z „MLEKO” NA „DRUGA PÓŁKA”?!

Administrator **DHCP** zdejmuje okulary.

— PANOWIE... JA JUŻ NAPRAWDĘ IDĘ ROZWIESZAĆ PRANIE.

Wchodzi zarządca **NAT-u**.

— Czy ktoś widział mój zeszyt?

— Druga półka — odpowiada lodówka.

— A MOGĘ GO ODEBRAĆ?!

— Nie.

— DLACZEGO?!

— **BRAK UPRAWNIEŃ.** 🤣🤣🤣

---

*Na następnej wycieczce odwiedzimy **HTTPS** i urząd certyfikacji, gdzie każdy twierdzi, że jest tym, za kogo się podaje. Nie każdy jednak ma dokumenty.*

*Urząd DNS zakończył poszukiwania mleka. Zwrócono NXDOMAIN. Lodówka złożyła odwołanie.*