**Czytaj lub słuchaj artykuł online**

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

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

SIECI KOMPUTEROWE

# NAT, czyli wymiana tablic rejestracyjnych na bramkach

Wyobraź sobie autostradę, na której pewien zarządca postanowił, że wszystkie samochody wyjeżdżające z osiedla będą miały **te same tablice rejestracyjne**.

Co mogło pójść nie tak? 🤣

## Osiedle Spokojna Sieć

Na niewielkim osiedlu stoją cztery domy. Pod pierwszym zaparkował komputer `192.168.1.10`, pod drugim laptop `192.168.1.11`, pod trzecim telefon `192.168.1.12`, a pod czwartym inteligentna lodówka `192.168.1.13`, która właśnie poinformowała właściciela, że skończyło się mleko.

Właściciel poinformował lodówkę, że mleko stoi na drugiej półce. Lodówka odpowiedziała, że nie ma uprawnień do przeszukiwania drugiej półki. Sprawa trafiła do administracji osiedla.

Wszystkie pojazdy mają własne numery i bez problemu poruszają się po osiedlowych uliczkach. Ale pewnego dnia komputer postanawia wyjechać na wielką autostradę.

Dojeżdża do bramki.

— Dzień dobry! Chciałbym pojechać do serwera z filmami.

— Dokumenty pojazdu.

— Proszę.

— Tablice `192.168.1.10`?

— Zgadza się.

— Z takimi pan nie wyjedzie.

— DLACZEGO?!

— Bo to tablice osiedlowe. Na autostradzie ich nie uznajemy.

— To co mam zrobić?!

— Wymienimy.

— Na jakie?

— Na nasze.

Zarządca wyciąga śrubokręt, odkręca tablice i przykręca nowe:

**193.24.14.111**

— Gotowe. Szerokiej drogi!

— Ale to nie jest mój numer!

— Już jest.

— A jak wrócę?!

— To pana rozpoznam.

— PO CZYM?!

— Spokojnie. Zapisuję wszystko w zeszycie.

I tak poznajemy **NAT — Network Address Translation**, czyli translację adresów sieciowych.

Adres osiedlowy to adres prywatny. Adres na autostradzie jest publiczny. A zarządca bramki właśnie zamienił jeden na drugi.

## Jeden numer dla wszystkich

Pięć minut później do bramki podjeżdża laptop.

— Dzień dobry, jadę sprawdzić pocztę.

— Proszę bardzo. Zmieniamy tablice.

— Na jakie?

— `193.24.14.111`.

— Zaraz! Przecież taki numer miał samochód przede mną!

— Zgadza się.

— TO PAN MA DRUGI TAKI SAM?!

— Mam jeden.

— TO JAK MAMY OBAJ NA NIM JEŹDZIĆ?!

— Normalnie.

— ALE TO JEST NIELEGALNE!

— Na zwykłej autostradzie owszem. Na naszej administracja ustala własne przepisy.

Po chwili przyjeżdża telefon.

— Ja też poproszę na autostradę.

— `193.24.14.111`. Następny!

Przyjeżdża lodówka.

— Ja w sprawie mleka.

— `193.24.14.111`.

— Ale ja mam ważną reklamację!

— Proszę nie blokować bramki.

I oto cztery różne urządzenia wyjeżdżają na Internet, występując pod jednym publicznym adresem.

**To typowa sytuacja w domowej sieci z maskaradą, czyli masquerade — odmianą źródłowego NAT-u (SNAT).**

Ale oczywiście pojawia się problem. Bo jak odróżnić cztery samochody, które mają ten sam numer?

## Zeszyt, bez którego autostrada przestaje mieć sens

Komputer dojechał do serwera, poprosił o film i czeka na odpowiedź. Serwer przygotował dane i wysłał je pod adres `193.24.14.111`.

Odpowiedź dociera do bramki osiedla.

— Dzień dobry! Mam przesyłkę dla samochodu `193.24.14.111`.

— Świetnie.

— Komu ją dać?

— Chwileczkę...

Zarządca otwiera zeszyt.

— Był komputer, laptop, telefon i lodówka.

— Któremu przekazać przesyłkę?

— Już patrzę.

— PAN NIE WIE?!

— WIEM! TYLKO MUSZĘ ZNALEŹĆ ODPOWIEDNI WPIS!

— A CO JEST W TYM ZESZYCIE?!

— Numery portów!

— JAKICH PORTÓW?!

— NIE MORSKICH! PROSZĘ SIĘ USPOKOIĆ!

I właśnie tutaj robi się ciekawie.

Sam **adres IP** nie wystarcza, żeby rozróżnić wiele równoczesnych rozmów. Pomagają w tym **numery portów**. Wyobraź sobie, że oprócz tablicy rejestracyjnej każdy samochód dostaje numer swojej sprawy.

Komputer wyjechał z numerem `192.168.1.10:51001`. Zarządca wypuścił go jako `193.24.14.111:40001`.

Laptop wyjechał z `192.168.1.11:51001` jako `193.24.14.111:40002`.

**Zeszyt zarządcy bramki — uproszczony przykład:**

| Na osiedlu | Na autostradzie |
|---|---|
| `192.168.1.10:51001` | `193.24.14.111:40001` |
| `192.168.1.11:51001` | `193.24.14.111:40002` |
| `192.168.1.12:52000` | `193.24.14.111:40003` |
| `192.168.1.13:53000` | `193.24.14.111:40004` |

*Adresy i porty są przykładowe. W rzeczywistości rejestr uwzględnia też inne informacje, między innymi protokół i parametry połączenia.*

Kiedy odpowiedź wraca na port `40001`, zarządca wie, że należy przekazać ją komputerowi. Kiedy na `40002` — laptopowi. A kiedy na `40004`...

— MAM WIADOMOŚĆ DLA LODÓWKI!

— W SPRAWIE MLEKA?!

— NIE WIEM, PRZECIEŻ NIE CZYTAM CUDZEJ KORESPONDENCJI!

— TO SKĄD PAN WIE, ŻE DLA LODÓWKI?!

— BO MAM ZESZYT!

Takie współdzielenie jednego adresu z wykorzystaniem portów nazywa się **PAT (Port Address Translation)**, a w bardziej formalnych opisach również **NAPT**.

## A co, jeśli zgubi się zeszyt?

Pewnego dnia zarządca robi porządki.

— Co to za stary zeszyt?

— Lista połączeń.

— A potrzebna?

— Nie wiem. Leży tutaj od rana.

— To wyrzucamy.

Pięć minut później...

— SZEFIE! PRZYSZŁA ODPOWIEDŹ DLA PORTU 40001!

— No to doręczyć!

— KOMU?!

— Jak to komu?!

— NIE MA ZESZYTU!

— TO SPRAWDŹCIE TABLICE!

— WSZYSCY MAJĄ TAKIE SAME!!!

**I właśnie dlatego urządzenie wykonujące NAT musi pamiętać aktywne translacje.**

W praktyce te informacje znajdują się w pamięci urządzenia, w tablicy stanów lub translacji, a nie w zeszycie oprawionym w skórę z napisem „TAJNE”.

Jeżeli taki stan zostanie utracony, odpowiedzi należące do istniejących połączeń mogą przestać trafiać do właściwych odbiorców.

— To może odtworzymy zeszyt?

— Z czego?

— Z pamięci!

— PANIE, TO JEST ROUTER, A NIE JASNOWIDZ!

## A teraz spróbuj zaprosić kogoś do domu

Do tej pory nasi mieszkańcy sami wyjeżdżali na autostradę. Zarządca ich rejestrował, więc wiedział, gdzie skierować odpowiedzi.

Ale pewnego dnia komputer postanawia uruchomić własny serwer.

— Będę organizował spotkania! Niech ludzie do mnie przyjeżdżają!

Wysyła zaproszenie znajomemu. Znajomy dojeżdża do osiedlowej bramki.

— Dzień dobry! Przyjechałem do serwera.

— Do którego?

— Pod adres `193.24.14.111`.

— To nasze osiedle.

— Zgadza się.

— A do którego domu?

— Nie wiem. Miałem podany ten adres.

— Numer sprawy?

— Port `8080`.

Zarządca zagląda do zeszytu.

— Nie ma.

— Jak to nie ma?!

— Nikt mi nie powiedział, że będzie pan przyjeżdżał.

— ALE JA MAM ZAPROSZENIE!

— A JA NIE MAM WPISU!

— TO PROSZĘ ZADZWONIĆ DO WŁAŚCICIELA!

— DO KTÓREGO?!

I tak wygląda jedna z typowych przeszkód przy próbie nawiązania połączenia z zewnątrz do urządzenia schowanego za NAT-em.

**Dla nieoczekiwanego ruchu przychodzącego brakuje reguły, która wskazywałaby odbiorcę.**

## Specjalne przepustki — przekierowanie portów

Następnego dnia komputer przychodzi do administracji.

— Chciałbym przyjmować gości.

— Bardzo dobrze. Proszę wypełnić formularz.

— Jaki formularz?

— Przekierowanie portu.

— A po ludzku?!

— Każdy, kto przyjedzie na nasz publiczny adres przez bramkę numer 8080, ma zostać skierowany do pana domu.

— I tyle?

— I tyle.

— To dlaczego wczoraj nie mogłem?!

— BO WCZORAJ NIE BYŁO FORMULARZA!

Zarządca zapisuje:

**`193.24.14.111:8080 → 192.168.1.10:80`**

Od tej chwili ruch przychodzący na wskazany adres i port może zostać skierowany do komputera.

To **DNAT (Destination NAT)**, a taki przypadek często nazywamy **port forwarding**, czyli przekierowaniem portów.

— A mogę przekierować wszystkie bramki?

— Technicznie są różne sposoby, żeby to zrobić.

— To poproszę!

— A zna pan wszystkich, których tym sposobem wpuści pan na osiedle?

— ...

— Właśnie. Może zaczniemy od jednej bramki?

Bo NAT nie zastępuje dobrze skonfigurowanego firewalla, a wystawianie usług do Internetu wymaga rozsądnych zasad dostępu.

## Osiedle za osiedlem, czyli CGNAT

Wszystko działało znakomicie. Aż pewnego dnia operator autostrady ogłosił reorganizację.

— Od jutra państwa osiedle nie będzie miało własnego bezpośredniego wyjazdu na Internet.

— Jak to?!

— Wszystkie osiedla będą przejeżdżać przez naszą wspólną bramkę.

— Ale my już mamy bramkę!

— Doskonale. Teraz będą państwo mieli dwie.

I tak wygląda podróż:

**Komputer `192.168.1.10` → bramka domowa NAT `100.64.12.34` → bramka operatora CGNAT `193.24.14.72` → Internet**

— Dzień dobry, przyjechałem do komputera z osiedla Spokojna Sieć.

— To proszę do pierwszej bramki.

— Tam powiedzieli, że mam jechać do operatora.

— A operator?

— Powiedział, że bez przepustki nie wjedziemy.

— To niech pan załatwi przepustkę!

— ALE KTO MA JĄ WYSTAWIĆ?!

— Operator.

— A OPERATOR POWIEDZIAŁ, ŻE NIE WYSTAWIA!!!

Witamy w świecie **CGNAT (Carrier-Grade NAT)** — translacji adresów wykonywanej przez operatora dla wielu klientów.

CGNAT pomaga oszczędzać publiczne **adresy IPv4**, ale może utrudnić przyjmowanie bezpośrednich połączeń przychodzących.

Jeśli bramka operatora nie zapewnia odpowiedniego przekierowania, samo otwarcie portu na domowym routerze niczego nie załatwi.

— Czyli mam swój router, swoje porty, własny zeszyt i nadal nie mogę zaprosić gości?!

— Zgadza się.

— TO PO CO MI TEN ZESZYT?!

— Do wyjazdów. Z wyjazdami wszystko działa bardzo ładnie.

— A Z POWROTAMI?!

— Powroty z zarejestrowanych wyjazdów również.

— A GOŚCIE?!

— Gości proszę uzgadniać z administracją wyższego szczebla.

## UPnP, czyli kiedy samochód sam załatwia sobie przepustkę

Na naszym osiedlu mieszka także konsola do gier. Konsola nie lubi wypełniać formularzy. Konsola lubi grać.

Pewnego dnia podjeżdża do bramki.

— Poproszę otworzyć przejazd dla moich znajomych.

— Wniosek?

— Nie mam.

— Podpis administratora?

— Nie mam.

— To na jakiej podstawie?!

— Na podstawie tego, że bardzo chcę.

— ...

— Mam specjalny system automatycznego zgłaszania.

— Aha. No to proszę.

I zarządca sam dopisuje odpowiednią regułę.

Tak w dużym uproszczeniu działa **UPnP IGD**, dzięki któremu aplikacje i urządzenia w sieci lokalnej mogą automatycznie poprosić router o utworzenie przekierowania portu.

Wygodne? Bardzo.

Ale czy każde urządzenie na osiedlu powinno mieć prawo samodzielnego otwierania bramek na zewnątrz?

— Dzień dobry, jestem inteligentnym tosterem.

— Słucham?

— Chciałbym otworzyć osiemnaście portów.

— PO CO?!

— Aktualizacje.

— OSIEMNAŚCIE?!

— Producent zaleca.

— A KTO JEST PRODUCENTEM?!

— Nie mogę ujawnić. Tajemnica handlowa.

Dlatego z automatycznym przekierowywaniem portów warto postępować świadomie, szczególnie gdy sieć pełna jest urządzeń, którym niekoniecznie chcemy bezgranicznie ufać.

## A może po prostu dać wszystkim własne tablice?

Pewnego dnia na osiedlu pojawia się nowy zarządca. Przywozi ogromne pudło tablic rejestracyjnych.

— Koniec tego szaleństwa! Każdy samochód dostanie własny, globalnie unikalny numer!

— Naprawdę?!

— Tak.

— A zeszyt?

— Do niektórych celów nie będzie potrzebny.

— A wymiana tablic przy wyjeździe?

— Też nie musi być potrzebna.

— A skąd pan ma tyle numerów?!

— **IPv6**.

Nagle okazuje się, że dla każdego samochodu można przydzielić własny, globalny adres, bez konieczności współdzielenia jednego **IPv4** przez całe osiedle.

**IPv6 nie wymaga NAT-u do oszczędzania adresów w taki sposób, jak robimy to w IPv4.**

Ale to nie oznacza, że każdy może sobie wjechać do dowolnego domu.

— To teraz wszyscy mogą do mnie przyjechać?!

— Nie.

— DLACZEGO?!

— Bo mamy jeszcze ochronę osiedla.

— JAKĄ OCHRONĘ?!

— Firewall.

— ALE PRZECIEŻ MAM WŁASNE TABLICE!

— Tablice rejestracyjne nie są przepustką do domu, proszę pana.

I to jest bardzo ważna różnica: **adresowanie i translacja adresów to jedno, a kontrola dostępu to drugie.**

Nie trzeba zmieniać numerów wszystkim samochodom, żeby zdecydować, kogo wpuszczamy na własny teren.

## Co się naprawdę dzieje na naszej bramce?

W rzeczywistym Internecie NAT nie odkręca tablic rejestracyjnych. Zmienia określone pola adresowe pakietów IP, a w popularnych odmianach wykorzystujących porty również numery portów **TCP** lub **UDP**.

W zależności od rodzaju translacji może zmieniać adres źródłowy, docelowy albo oba — według odpowiednich reguł.

**Najważniejsze pojęcia z naszej wycieczki:**

| Pojęcie | Co oznacza na autostradzie? |
|---|---|
| **NAT** | Wymiana tablic rejestracyjnych |
| **SNAT** | Zmiana tablic przy wyjeździe |
| **Masquerade** | SNAT korzystający z adresu interfejsu wyjściowego |
| **PAT / NAPT** | Dodatkowe numery spraw, żeby rozróżnić samochody |
| **DNAT** | Wskazanie domu, do którego skierować przyjezdnego |
| **Port forwarding** | Stała przepustka na wybranej bramce |
| **CGNAT** | Jeszcze jedna bramka, tym razem u operatora |
| **UPnP IGD** | Automatyczne załatwianie przepustek |
| **IPv6** | Wystarczająco dużo numerów, by nie trzeba było ich współdzielić |

A największa zaleta NAT-u w świecie **IPv4**? Wiele urządzeń może korzystać z Internetu, współdzieląc jeden publiczny adres.

Największa niedogodność? Kiedy ktoś z zewnątrz chce rozpocząć rozmowę z konkretnym urządzeniem, trzeba zapewnić mu odpowiednią drogę do środka.

**I pamiętajmy: NAT to mechanizm translacji, a nie magiczna ochrona przed wszystkimi zagrożeniami Internetu.**

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

## Tymczasem w administracji osiedla...

— Szefie! Mamy problem!

— Znowu?!

— Lodówka chce wyjechać na autostradę.

— To niech jedzie.

— Ale ona żąda własnego publicznego adresu!

— PO CO LODÓWCE PUBLICZNY ADRES?!

— Powiedziała, że nie życzy sobie dzielić tablic z tosterem.

— A TOSTER?!

— Toster już wyjechał.

— Dokąd?!

— NIE WIEMY!

— A ZESZYT?!

— ...

— GDZIE JEST ZESZYT?!

— Lodówka twierdzi, że leży na drugiej półce.

**— TO NIECH GO WYJMIE!!!**

**— NIE MA UPRAWNIEŃ.** 🤣

---

*Na kolejnej wycieczce możemy odwiedzić przewoźników **TCP** i **UDP**. Jeden żąda pokwitowania każdej dostawy, a drugi zostawia przesyłkę pod drzwiami i odjeżdża, zanim ktokolwiek zdąży zapytać o numer zamówienia.*

*Zarządca autostrady odmówił komentarza. Nadal szuka zeszytu.*