IPv4 Mroczne Widmo czyli IPv6 DS-lite w Neostradzie

Orange Polska

Monika Antoniak-Lewandowska

Krzysztof Kwiecień

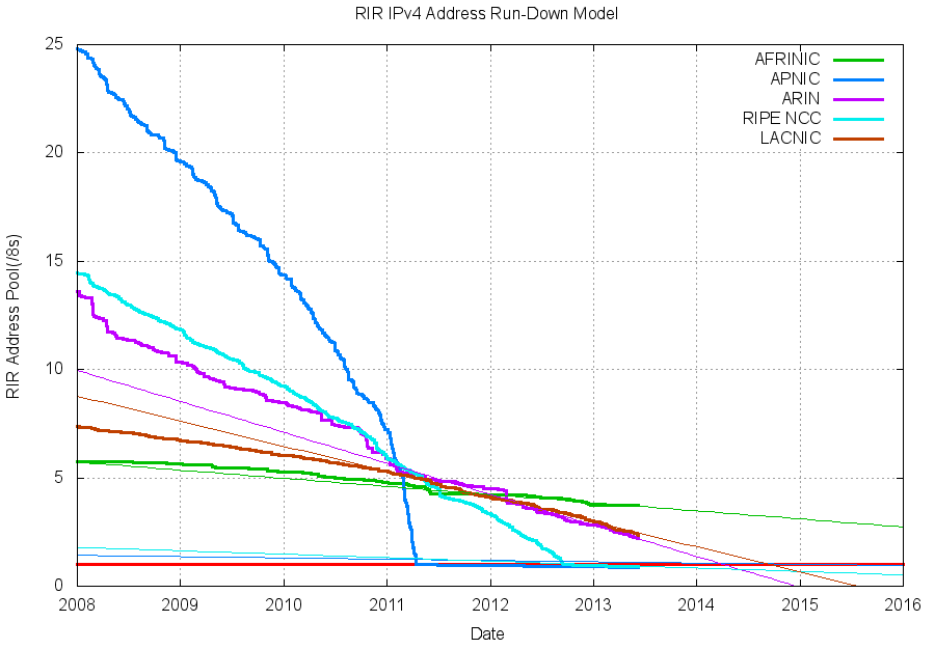
PLNOG, 3-4 marca 2014, Warszawa

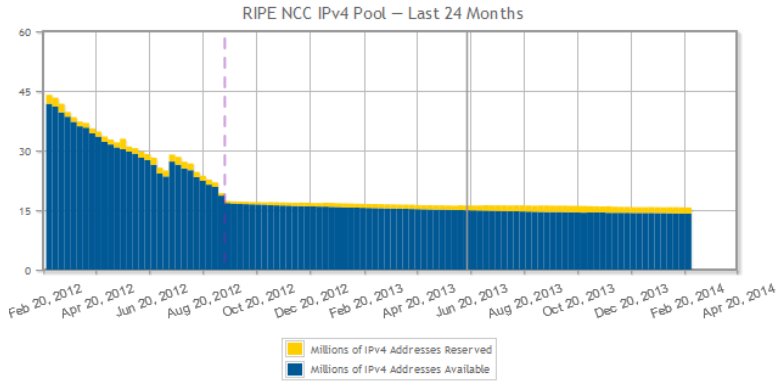
orange™

Agenda

- **Powody rozpoczęcia projektu**
- **Za i przeciw: Dual-Stack, NAT444, NAT64, DS-lite**
- **Inne wymagania i ograniczenia**
- **Architektura rozwiązania**
- **Obszary, których projekt dotyczył**
- **Topologia CGN**
- **Wybór urządzenia na platformę CGN**
- **Wyzwania**
  - wytyczne
  - wymiarowania – makieta testowa
  - BRAS
  - bezpieczeństwo
  - redundancja
  - ustawienia konfiguracyjne, timeout'y
  - CPE
- Rozwiązanie z punktu widzenia użytkownika
- Podsumowanie

Powody rozpoczęcia projektu





- Kończenie się pul adresowych IPv4 oraz ciągły wzrost zapotrzebowania na adresy przez usługi Orange
  - IPv4 skończyły się w IANA - 31 stycznia 2011
  - IPv4 skończyły się w RIPE - 14 września 2012
- Stanowisko prezesa UKE W sprawie IPv6 z sierpnia 2011

Za i przeciw: Dual-Stack, NAT444, NAT64, DS-lite

NAT444

Za	Przeciw
• Wdrożenie oparte tylko o IPv4 • Brak zmian po stronie CPE	• Wielokrotna translacja adresów • Konieczność zarządzania adresacją prywatną. • Brak wdrożenia IPv6 • Brak perspektywy ograniczenia kosztów NAT'a

Dual-Stack

Za	Przeciw
• Prosta implementacja na CPE • Wdrożenie IPv6 • Perspektywa zmniejszenia kosztów NAT wraz z migracją ruchu do IPv6	• Konieczne wdrożenie łącznie z NAT444 w celu ograniczenia wykorzystania adresów. • Dwa protokoły na łączu WAN - podwójne wykorzystanie zasobów BNG

Za i przeciw: Dual-Stack, NAT444, NAT64, DS-lite

NAT64/DNS64

Za	Przeciw
• Jeden protokół na łączu WAN. • Wdrożenie IPv6 • Perspektywa zmniejszenia kosztów NAT wraz z migracją ruchu do IPv6	• Wielokrotna translacja adresów i protokołów • Problem w realizacji usług wykorzystujących czyste IP (bez DNSów) • Dwa urządzenia brzegowe (CGN i BNG) • Problemy w implementacji w CPE

DS-Lite

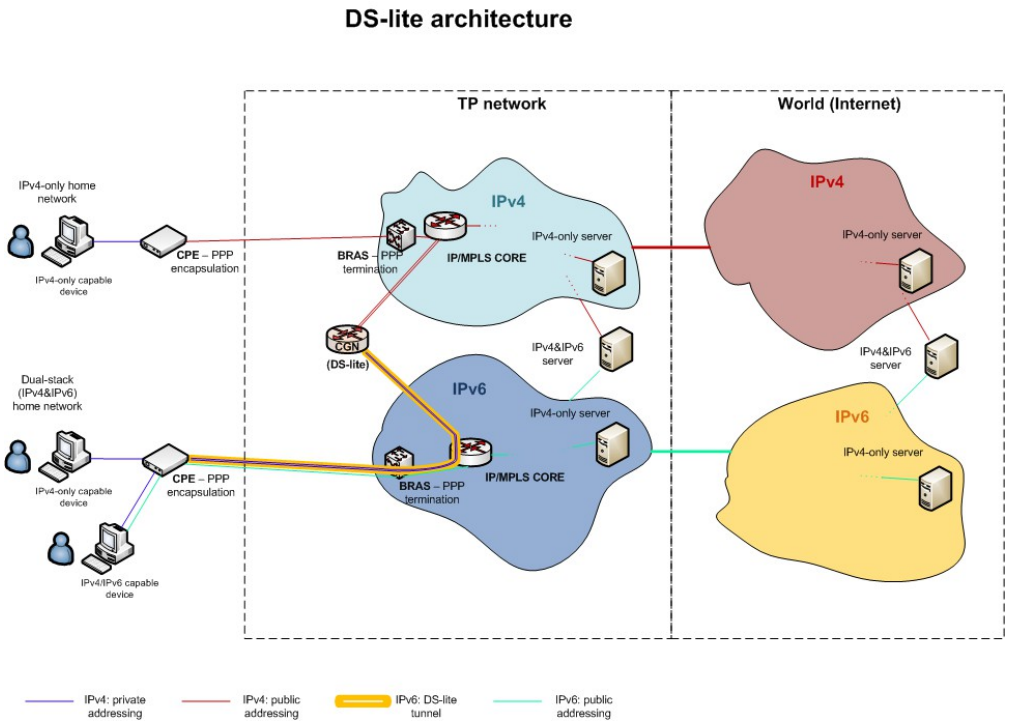
Za	Przeciw
• Relatywnie prosta implementacja na CPE • Wdrożenie IPv6 • Perspektywa zmniejszenia kosztów NAT wraz z migracją ruchu do IPv6 • Jeden protokół na łączu WAN • Zgodność ze strategią Grupy Orange	• Konieczność dostosowania CPE • Dodatkowy narzut nagłówków • Dwa urządzenia brzegowe (CGN i BNG)

Inne wymagania i ograniczenia

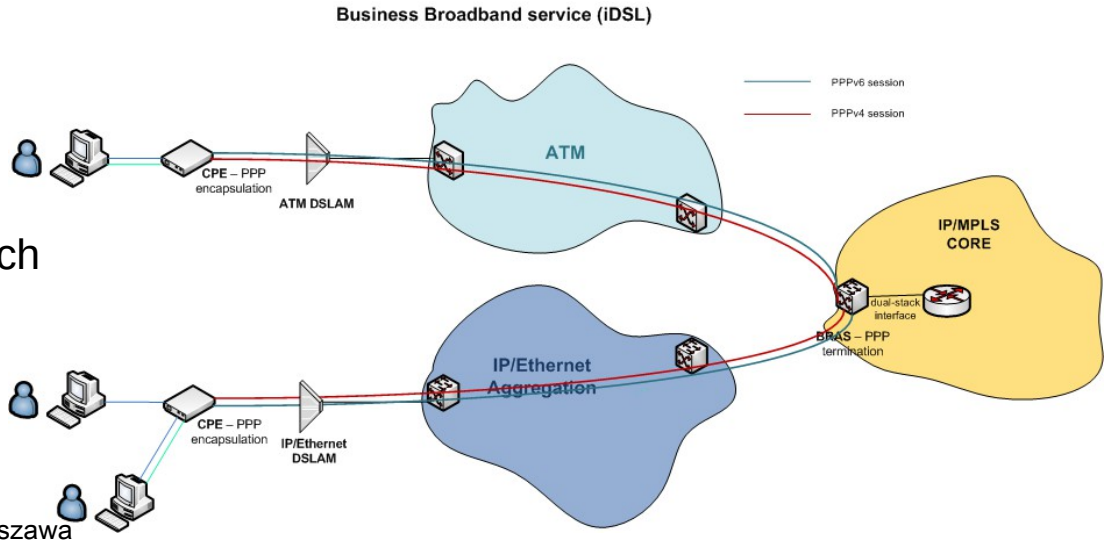
Inne wymagania, które należało uwzględnić w projekcie:

- maksymalnie dostępna transparentność usługi
- uniezależnienie dostępności IPv6 od rodzaju dostępu
- możliwość migracji pomiędzy IPv4 i DS-Lite
- skalowalność

Architektura rozwiązania



Architektura dla klientów indywidualnych (Neostrada)
-dostęp tylko przy użyciu protokołu IPv6
-brak publicznego adresu IPv4
-prefiks /56 dla użytkownika
-DS-Lite CGN dla dostępu do IPv4
-możliwość migracji do IPv4



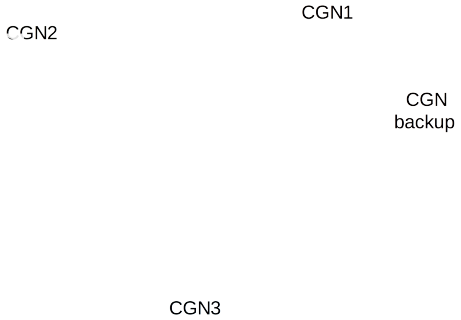
Architektura dla klientów biznesowych (IDSL)
-dostęp Dual-Stack.
-publiczny adres IPv4
-prefiks /56 dla abonenta

Obszary, których projekt dotyczył

Obszary, gdzie wprowadzenie IPv6 (DS-lite) wymaga dokonania zmian

- **Szkielet sieci**
  - w sieci Orange dual-stack od 2006 roku
  - zmiany nie były konieczne
- **BRAS**
  - AAA
  - PPPv6/DHCPv6
- **CGN**
  - nowy element sieci
- **CPE**
  - konieczność dostosowania do wymogów IPv6
  - konieczność zapewnienia kompatybilności wstecz

Topologia CGN



- 3 CGN (1 w strefie obsługi)
- Jeden węzeł zapasowy (redundancja N+1)
- Integracja z siecią szkieletową IP/MPLS Orange Polska
- Styki z IP Backbone = nx10Gbps

Wybór urządzenia na platformę CGN

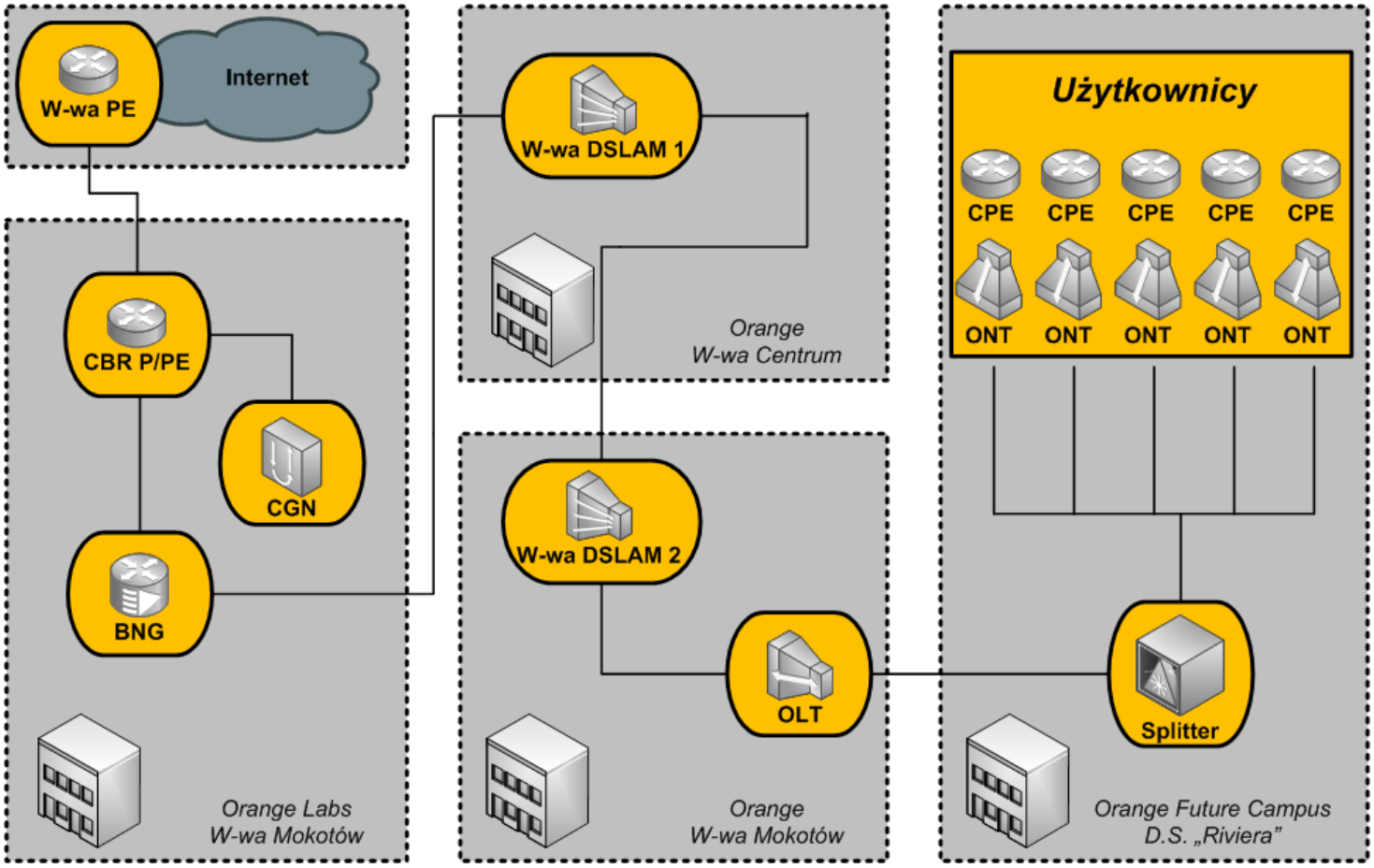
- Zostały przetestowane wszystkie platformy CGN dedykowane dla ISP dostępne w latach 2011/2012
  - Nie ma idealnego rozwiązania - każda platforma ma unikalne zalety i wady
  - Testy i wybór platformy trwały rok i obejmowały m.in. stworzenie środowiska E2E dla studentów akademika w Warszawie
  - Urządzenie musiało być wystarczająco elastyczne, aby obsłużyć także inne usługi
  - Przy dostosowaniu platformy do wymagań Orange oraz ze względu na wykryte podczas testów braki i błędy w implementacji konieczna, ale i bardzo pomocna była bezpośrednia współpraca z zespołem deweloperów producenta

Wyzwania: wytyczne

- Przyjęte założenia i wartości
  - Jeden klient może zaalokować jeden blok portów (8192 porty). Jeden blok portów uniemożliwia zaistnienie sytuacji gdy klient używa 2 publicznych adresów IPv4 do jednego serwera (SSL/banki)
  - Klient posiada dynamiczny prefiks IPv6, który może być zmieniony ze względu na zmianę topologii sieci. Powiązanie prefiksu IPv6 z publicznym adresem IPv4 jest zachowane przez 24 godziny
  - Jeden klient może nawiązać maksymalnie 3 tunele DS-lite do CGNa
- Wyzwania warstwy L4/7
  - Do czasu wdrożenia CGN urządzenia rdzeniowe pracowały tylko w trybie bezstanowym. Ich obciążenie urządzeń nie zależało od liczby sesji L4
  - Nie można zasymulować ruchu użytkownika za pomocą generatorów ruchu. Za to za pomocą ruchu syntetycznego można łatwo zdiagnozować ukryte/zaszyte limity CGNa (np. ilość sesji na Softwire)
  - Do oszacowań została wykorzystana makieta End-to-End

Wyzwania: wymiarowania – makieta testowa

Makieta testowa



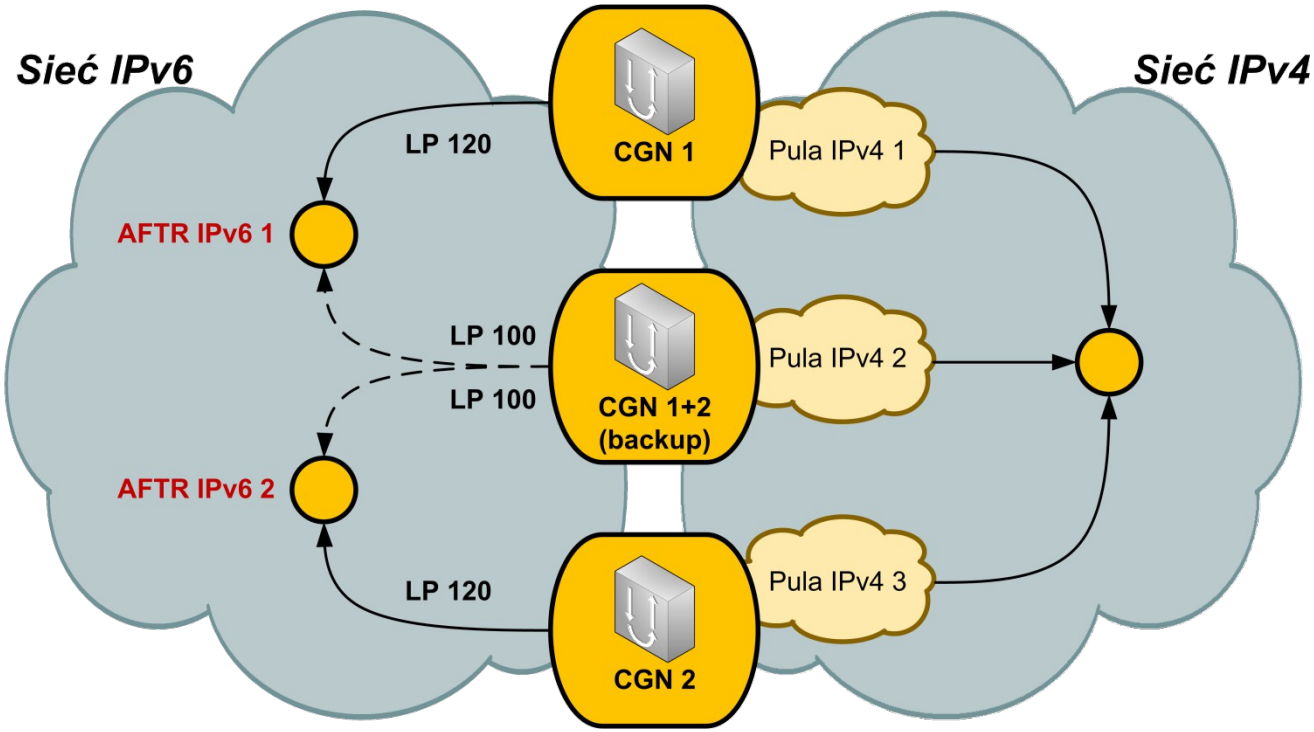
Wyzwania: BRAS

- model adresacji: unnumbered model (link-local + DHCPv6 PD)
- integracja z AAA, konieczność dostosowania systemów AAA
- konfiguracja jednocześnie dla trybu IPv4 i IPv6
- skalowalność
  - liczba klientów
  - ACLki
  - DHCPv6 local server (DHCPv6 serwer na BRAS)
- nowe funkcjonalności - nowy software
- brak wsparcia w sprzęcie testowym (na początku projektu)
- MTU – zalecane dodatkowe 40B

Wyzwania: bezpieczeństwo

- Potencjalne problemy
  - Klient w usłudze DS-lite otrzymuje prefiks /56. Może symulować miliardy unikalnych klientów doprowadzając CGN do wyczerpania zasobów
  - PCP – CGN interpretuje pakiety otrzymane bezpośrednio od użytkownika – należy być gotowym na niepoprawnie skonstruowane pakiety
  - Rozdzielenie funkcji brzegu sieci na dwa urządzenia: BRAS dla IPv6 i CGN dla IPv4
  - Retencja

Wyzwania: redundancja



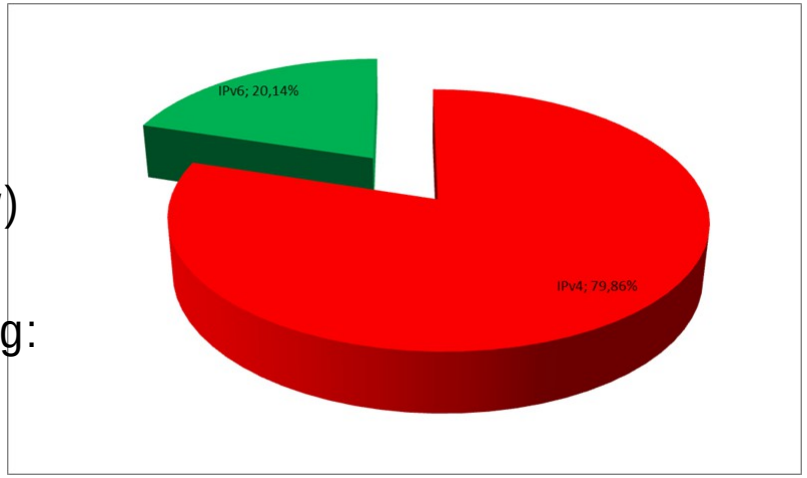
- Przyjęte rozwiązanie:
  - Zastosowana redundancja N+1
  - Adresy IPv6 AFTR są rozgłaszane za pomocą Anycast
  - Zapasowy CGN posiada jeden prefiks IPv4 niezależnie od tego, którego CGN'a zastępuje (prostsza konfiguracja ale brak PCP)

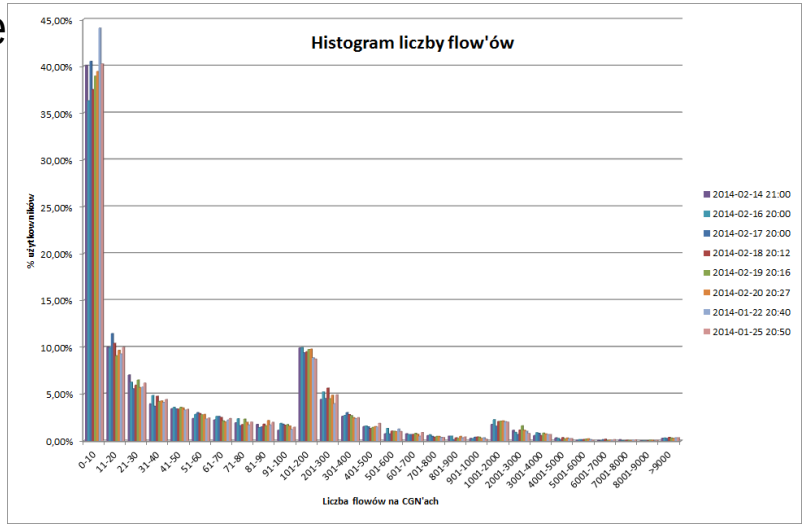
Wyzwania: ustawienia konfiguracyjne, timeout'y

- Poszukiwanie złotego środka
  - zbyt niskie wartości – zrywanie sesji/protokołów
  - zbyt wysokie wartości – gwałtowny przyrost ilości równoległych sesji (P2P), klient alokuje wszystkie dostępne dla siebie porty i traci dostęp do sieci
  - brak jakichkolwiek pkt. odniesienia, dostępnych danych (jedna z przyczyn uruchomienia testowej usługi w miasteczku testowym)
  - proces ciągły – wraz z nowymi danymi możliwa jest adaptacja obecnej konfiguracji

Wyzwania: ustawienia konfiguracyjne, timeout'y (c.d)

- Przykładowe wartości
  - Przypisanie adresu IPv4 (8192 portów) do klienta: 24 godziny
  - Endpoint independent mapping/filtering: 300 sek.
  - Opcja: dedykowany timeout dla dedykowanych portów (np. DNS może mieć przypisaną niższą wartość, ze względu na specyfikę protokołu)





Wyzwania: CPE

Brak wsparcia dla DS-lite

- Na początku projektu żaden z producentów nie wspierał usługi DS-lite/PCP w swoim CPE
- Początkowo wszelkie testy były wykonywane na zmodyfikowanym Open-WRT
- Współpracy z dostawcami i konieczność wykonania wielokrotnych testów walidacyjnych
- Brak wsparcia PCP przez producentów (CPE + CGN), w momencie wdrożenia PCP nie posiadał jeszcze finalnego RFC
- Migracja do PPPoE
- Firewall dla IPv6
- Wydajność i MTU

Docelowo wszystkie urządzenia w ofercie Orange w usłudze Neostrada będą wspierać IPv6.

Rozwiązanie z punktu widzenia użytkownika oraz jak wrócić do IPv4

IPv6 dla odbiorcy końcowego

- **Dla większości użytkowników rodzaj użytego protokołu nie ma znaczenia**
  - Z uwagi na brak świadomości o istnieniu dwóch różnych typów
  - CGN zastępuje NAT na CPE (z dokładnością do UPnP/PCP)
- **Kluczowe jest, aby dotychczas działające usługi działały tak samo po zastosowaniu nowej technologii**

Co zrobić, żeby w Neostradzie wrócić do IPv4?

- **Z domyślnego loginu user@neostrada.pl/ipv6 należy usunąć sufiks „/ipv6”**
  - Klient podłączy się „starym” sposobem, otrzymując adres IPv4
  - Żadna inna rekonfiguracja nie jest konieczna (na wszystkich modemach dostarczanych przez Orange)

Podsumowanie

Problem pioniera

- **Projekt długotrwały, czasochłonny i skomplikowany**
  - Wymagający współpracy wielu jednostek wewnętrznych
  - Zależny od czynników zewnętrznych: CGN, CPE
- **Brak opisanych zasad „dobrych praktyk” i doświadczeń operacyjnych**
- **Łatwiejsza implementacja z uwagi na obecny w sieci szkieletowej Dual-Stack**
- **Wymagający nakładów**
- **Dla zaawansowanych użytkowników może wprowadzać niepożądane ograniczenia**

ale…

jest rozwiązaniem problemu kończących się pul adresowych IPv4 przy jednoczesnym wdrażaniu w sieci protokołu IPv6 i daje nowe możliwości

Dziękujemy

Kontakt:

Monika Antoniak-Lewandowska

Krzysztof Kwiecień

Adam Kułagowski

Paweł Włodawiec

Zbigniew Suchojad