# NAT-PT czyli współistnienie sieci IPv4 i IPv6



Piotr Wojciechowski (CCIE #25543)
Starszy konsultant ds. sieci
PLNOG #4 Warszawa

# Agenda

- Wprowadzenie do adresacji IPv6
- Współistnienie sieci IPv4 i IPv6
- NAT-PT w teorii
- NAT-PT w praktyce na Cisco
- Ograniczenia
- Podsumowanie (Q&A)

# Kilka faktów o IPv6?

- IPv6 już działa – zacznijmy go używać
- Zacznijmy już migrować – uczmy się gdy jest na to czas, rozkładajmy koszty w czasie
- NAT44 nie jest lekarstwem na kończącą się adresację
- NAT64 jest możliwy, ale to tylko etap
- NAT46 potrafi dać w kość

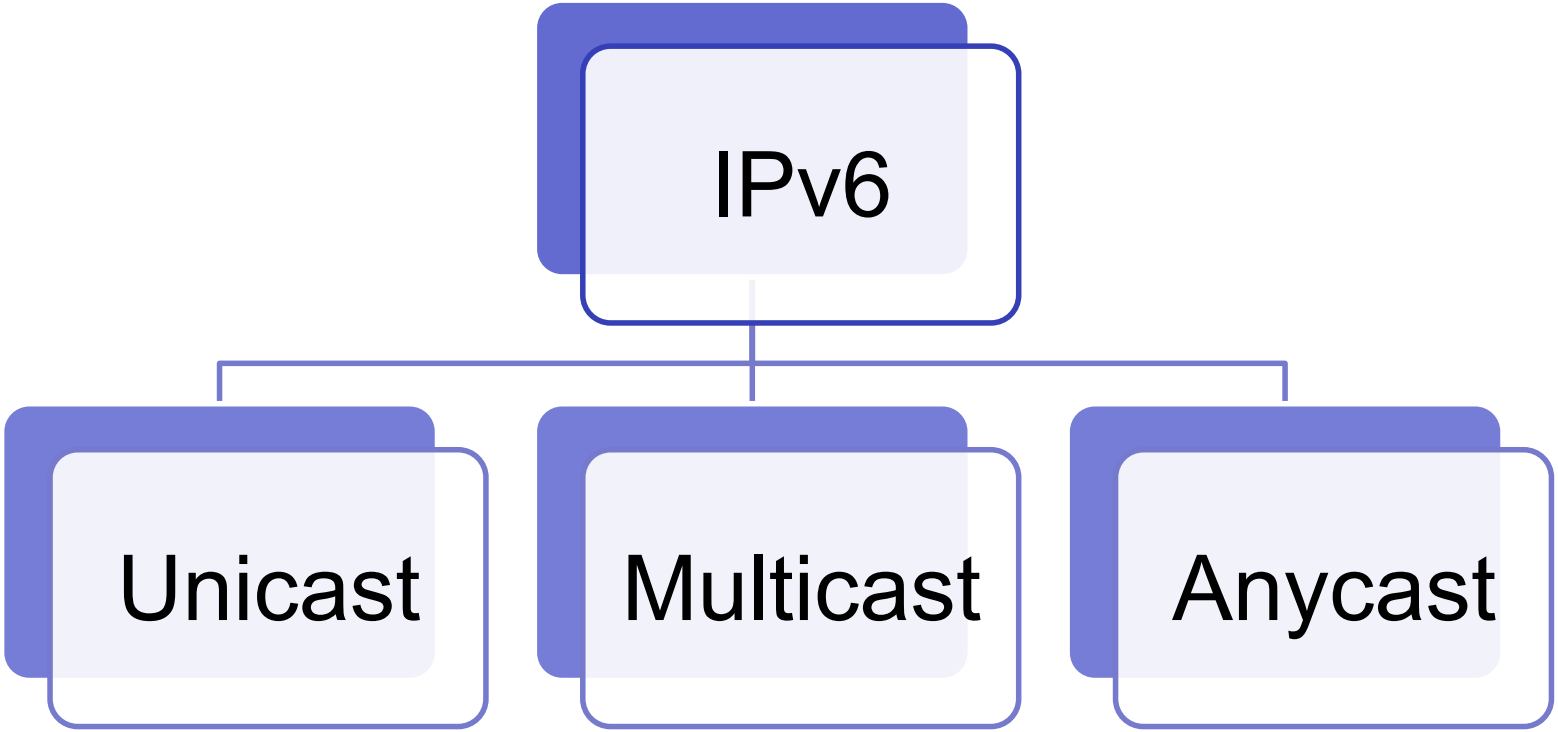
# Migracja do IPv6 - fakty

- Płynne przejście z IPv4 do IPv6 zapewni nam współpraca trzech mechanizmów:
  - Dual Stack
  - Tunneling
  - Translating
- Natywni klienci IPv6 wcześniej czy później się pojawią – trzeba zapewnić im łączność z siecią IPv4, NAT64 więc Twoim przyjacielem
- Z czasem pojawią się usługi dostępne tylko w IPv6 – jeżeli nie wdrożymy IPv6 szybko będziemy musieli zaprzyjaźnić się z NAT46

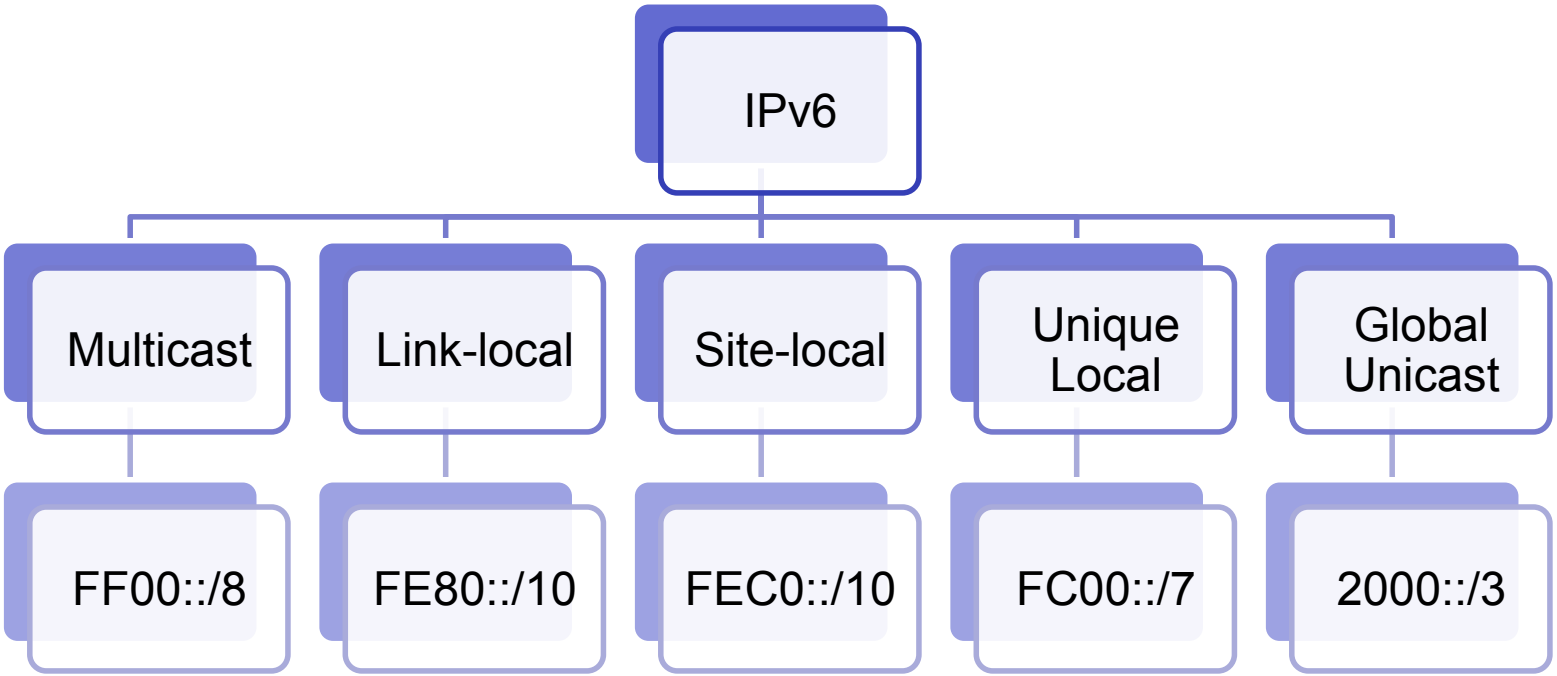
# Agenda

- **Wprowadzenie do adresacji IPv6**
- Współistnienie sieci IPv4 i IPv6
- NAT-PT w teorii
- NAT-PT w praktyce na Cisco
- Ograniczenia
- Podsumowanie (Q&A)

# IPv6
## *Typy adresów*



# IPv6
## *Pule adresów*



# Metody konfiguracji adresów IPv6
## *Manual Assignment*

- Adres konfigurowany statycznie przez administratora
- Pole do wielu „literówek” potencjalnie trudnych do wyłapania
- Idealne i pożądane rozwiązanie dla urządzeń sieciowych i niezmiennych elementów sieci (serwery SMTP, WWW)

# Metody konfiguracji adresów IPv6
## *Stateless Address Autoconfiguration (RFC2462)*

- Akronim - SLAAC
- Najprostsza metoda konfiguracji – nie wymaga od administratora dotykania się do urządzenia końcowego
- Stacja robocza na podstawie adresu MAC interfejsu sieciowego tworzy identyfikator EUI-64
- Stacje końcowe konfigurują swój adres IP i adres link-local routera będącego domylną bramą dla segmentu sieci

# Metody konfiguracji adresów IPv6
## *Stateless Address Autoconfiguration (RFC2462)*

1

```
Router Solicitation (RS) – ICMPv6 133
Src: link-local
Dst: FF02::2 (All routers)
```

2

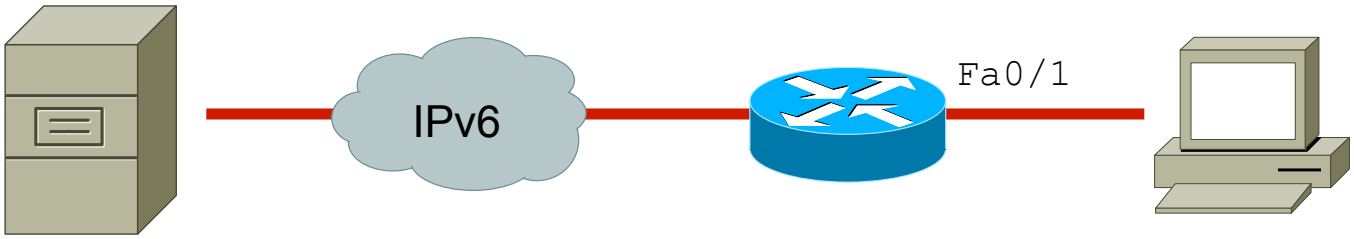
```
Router Advertisement (RA) – ICMPv6 134
Src: link-local
Dst: FF02::1 (All hosts)
```

*Prefix = 2001::/64*
*Lifetime (valid and preferred)*
*Default router = link-local address*
*O and M bits*

# Metody konfiguracji adresów IPv6
## *Stateful DHCPv6 (RFC3315)*

- Idea działania jak w DHCP dla IPv4
- Brak możliości konfiguracji statycznego powiązania między MAC klienta a adresem IPv6
- Pełna kontrola nad przydziałem adresów kosztem większego nakładu pracy
- Wymaga wyłączenia SLAAC

# Metody konfiguracji adresów IPv6
## *Stateful DHCPv6 (RFC3315)*




2001:10::1

```
interface FastEthernet0/1
 ipv6 address 2001:1::1/64
 ipv6 nd prefix 2001:1::1/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:10::1
```

Wyłącz rozgłaszanie za pomocą ND

Włącz flagi M (adres z serwera DHCP) oraz O (pozostałe dane z serwera DHCP)

Przekieruj zapytania do serwera DHCPv6

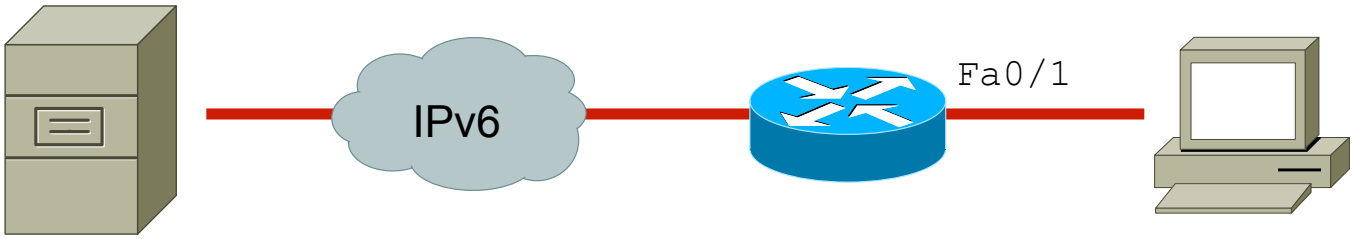
# Metody konfiguracji adresów IPv6
## *DHCPv6-PD (RFC3633)*

- DHCPv6 Prefix Delegation
- Rozszerzenie do DHCPv6 pozwalające na przydział nie tylko pojedynczego adresu lecz całej podsieci
- Klient może następnie dokonać dalszej segmentacji i przydziału dla poszczególnych stacji roboczych
- Najczęściej stosowane na routerach PE (DHCP server) dla przydziału adresacji dla routerów CE (DHCP client)

# Metody konfiguracji adresów IPv6
## *Stateless DHCPv6 (RFC3736)*

- Kombinacja DHCPv6 i SLAAC, zwana też DHCPv6-Lite
- Komputer końcowy używa SLAAC do pozyskania adresacji IPv6 oraz informacji dotyczących domyślnej bramy
- DHCPv6 stosowane do pobrania informacji, których nie da się przekazać za pomocą SLAAC, np. informacje o serwerach DNS
- DHCPv6-Lite wygodnie konfiguruje się na routerach

# Metody konfiguracji adresów IPv6
## *Stateless DHCPv6 (RFC3736)*




```
interface FastEthernet0/1
 ipv6 address 2001:1::1/64
 ipv6 nd other-config-flag
!
ipv6 dhcp pool IPv6
 dns-server 2001:1a68::4d4f:eb66
```

Rozgłaszamy prefix za pomocą ND

Włącz flagę O (pozostałe dane z serwera DHCP)

Konfiguracja DHCPv6-Lite na routerze Cisco

# Wybór protokołu w systemach operacyjnych *Microsoft Windows Vista, Windows 7*

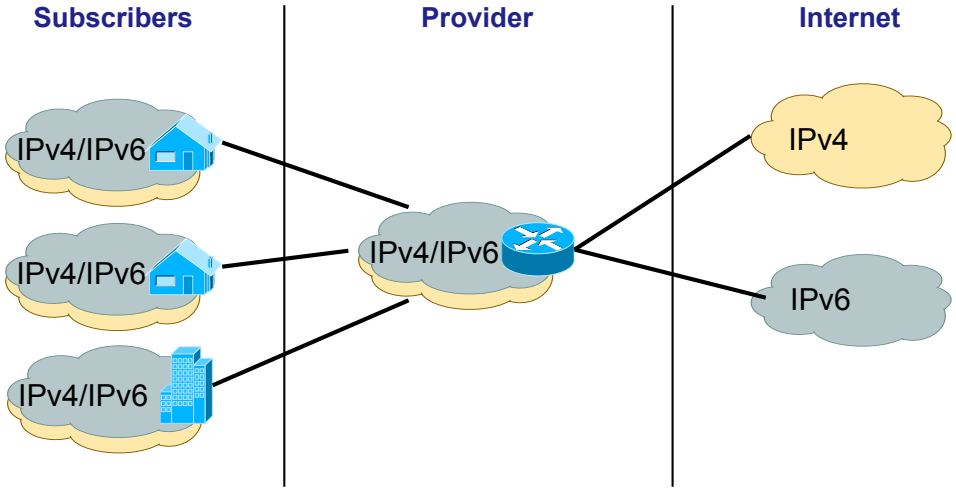
- Vista preferuje IPv6 przed IPv4
- Po podniesieniu łącza wysyłane jest IPv6 NA/NS/RS, wykonywana jest też próba pobrania informacji z DHCPv6
- Vista nasłuchuje na ICMP RA
- Jeżeli powyższe metody nie zadziałają próbuje użyć ISATAP
- Jeżeli ISATAP zawiedzie próbuje użyć Teredo
- A gdy się skończą możliwości użyje IPv4

# Agenda

- Wprowadzenie do adresacji IPv6
- **Współistnienie sieci IPv4 i IPv6**
- NAT-PT w teorii
- NAT-PT w praktyce na Cisco
- Ograniczenia
- Podsumowanie (Q&A)

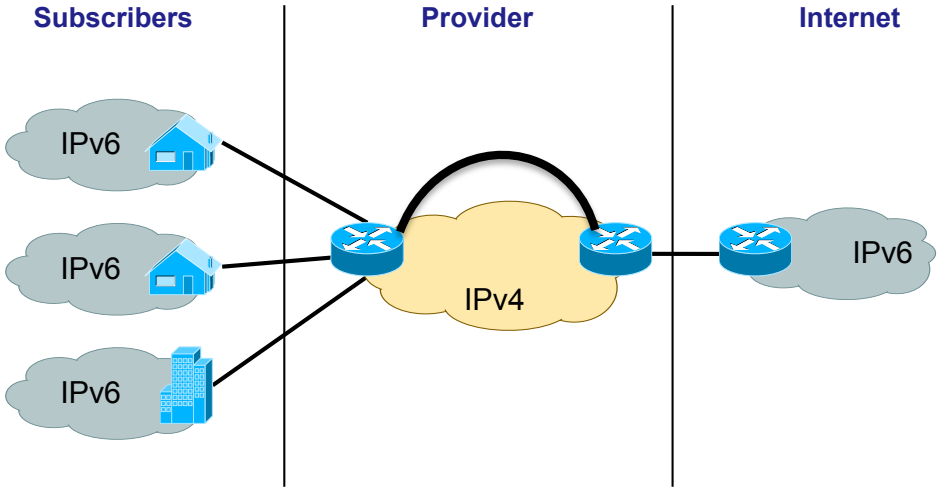
# Współistnienie sieci IPv4 i IPv6
# Dual Stack

- Preferujemy IPv6 przed IPv4
- Pozwalamy aplikacjom IPv4 na normalną pracę
- Dajemy komputerom możliwość natywnej komunikacji po IPv6



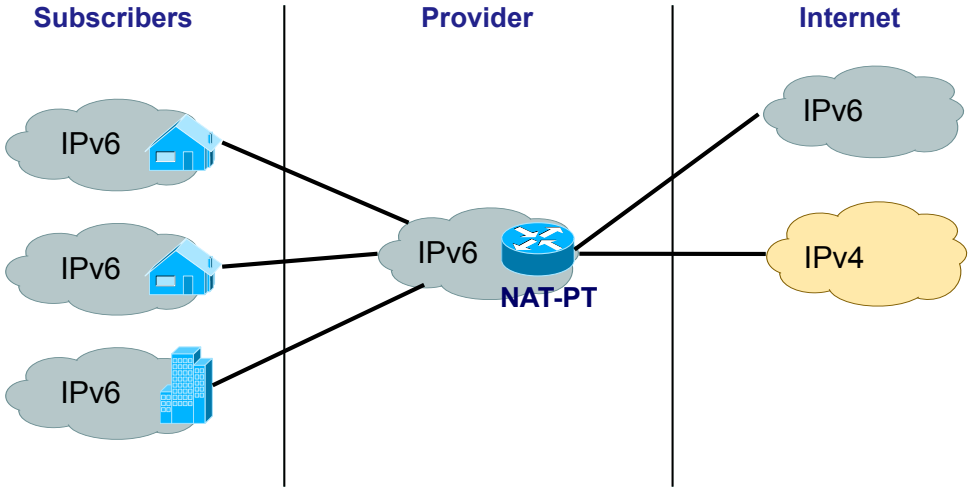
# Współistnienie sieci IPv4 i IPv6
# Tunelowanie

- Tunele IPv6 przenoszone poprzez sieć IPv4
- 6to4 dla zastosowań site-to-site, ISATAP dla pojedynczych urządzeń
- Trudne do diagnostyki w przypadku problemów, potencjalnie niebezpieczne dla naszej sieci, często trudne do uruchomienia dla użytkownika końcowego



# Współistnienie sieci IPv4 i IPv6
# NAT-PT

- Stacje końcowe otrzymują jedynie adresację i informacje o routingu w protokole IPv6
- Do natywnej sieci IPv6 ruch przepuszczamy bez zmian
- Na styku z siecią IPv4 wykonujemy translację między protokołami
- Ruch do sieci IPv6 gdy stosujemy adresację publiczną



# Agenda

- Wprowadzenie do adresacji IPv6
- Współistnienie sieci IPv4 i IPv6
- **NAT-PT w teorii**
- NAT-PT w praktyce na Cisco
- Ograniczenia
- Podsumowanie (Q&A)

# NAT-PT

- Pozwala aplikacjom korzystającym z IPv6 na komunikację z aplikacjami korzystającymi z IPv4 i vice versa
- Pozwala tworzyć segmenty działające tylko w oparciu o IPv6
- Urządzenia IPv6 myślą, że rozmawiają z innym urządzeniem IPv6, IPv4 z innym IPv4 – nie trzeba więc nic zmieniać na urządzeniach końcowych!

# NAT-PT w Cisco

- Wspierane platformy:
  - Routery ISR (870, 880, 1800, 2800, 3800)
  - Routery ISR G2 (1900, 2900, 3900)
  - Routery 7200, 7400, 7500
  - Access Servers 5350XM, 5400XM
  - Starsze modele – 2600XM, 3640, 3640A

# NAT-PT w Cisco

- Premiera w IOS 12.2(13)T wraz z DNS ALG
- W 12.3(2)T dodany tryb PAT, FTP ALG oraz obsługa fragmentacji
- W 12.3(14)T dodany tryb v4-mapped dla prefixu IPv6
- Implementacja zgodna ze standardami RFC 2765 oraz RFC 2766
- Co prawda RFC 4966 przenosi do archiwum NAT-PT jego stosowanie u wielu operatorów może okazać się koniecznością

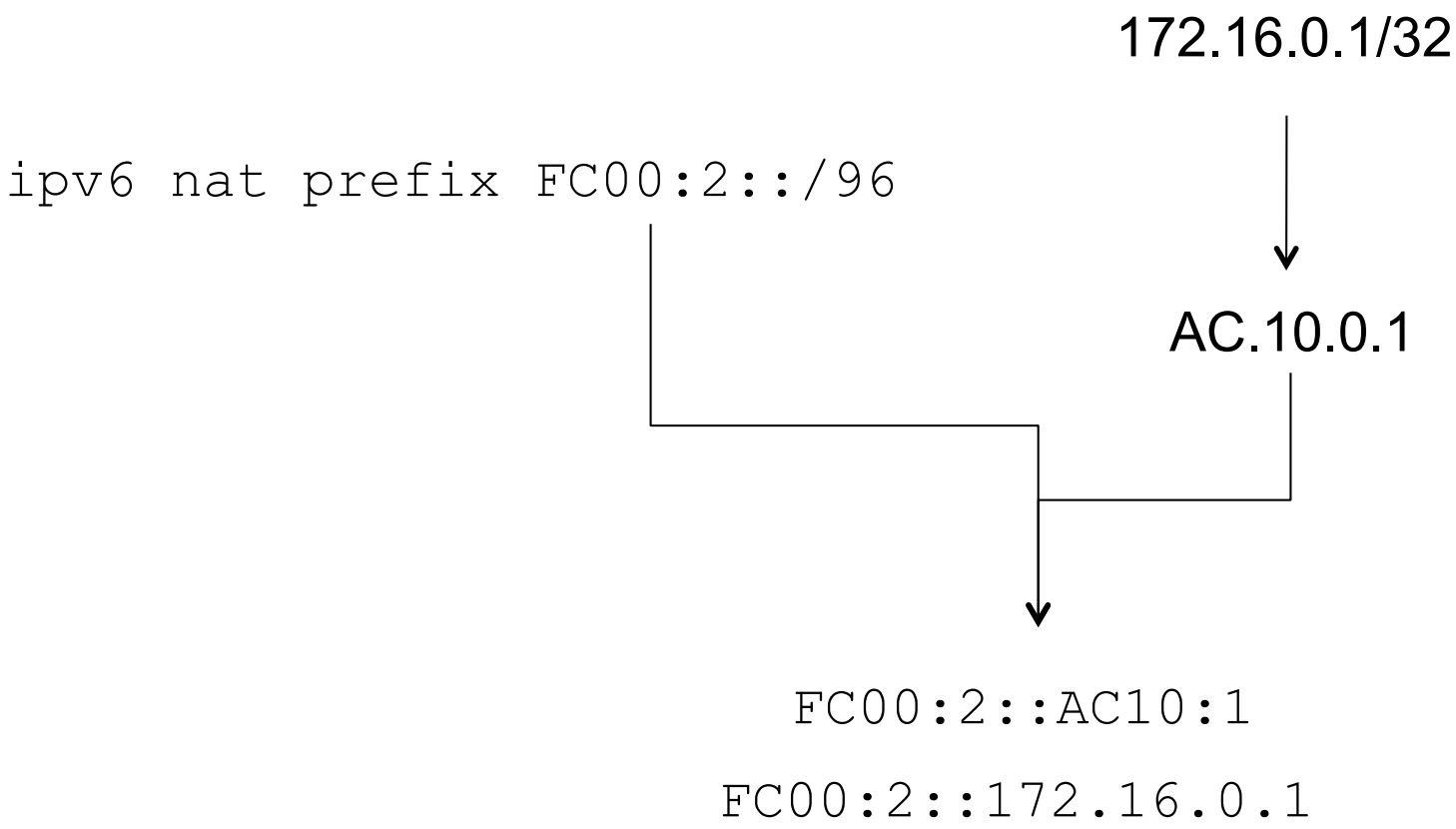
# NAT-PT

- NAT-PT to nie automatyczne tunele 6to4
- NAT-PT traktujmy jako doraźne rozwiązanie tymczasowe a nie permanentne rozwiązanie
- NAT-PT wymaga pamięci oraz zasobów CPU
  - NAT-PT nie działa w CEF
  - Do 12.4(20)T działał jako fast switching
  - Od 12.4(20)T fast switching jest usunięty – NAT64 działa jako process switching!
  - Cisco 2801 – 70% wysycenia CPU dla ruchu 4Mbit bez żadnych innych usług
- NAT-PT nie jest trudny w konfiguracji

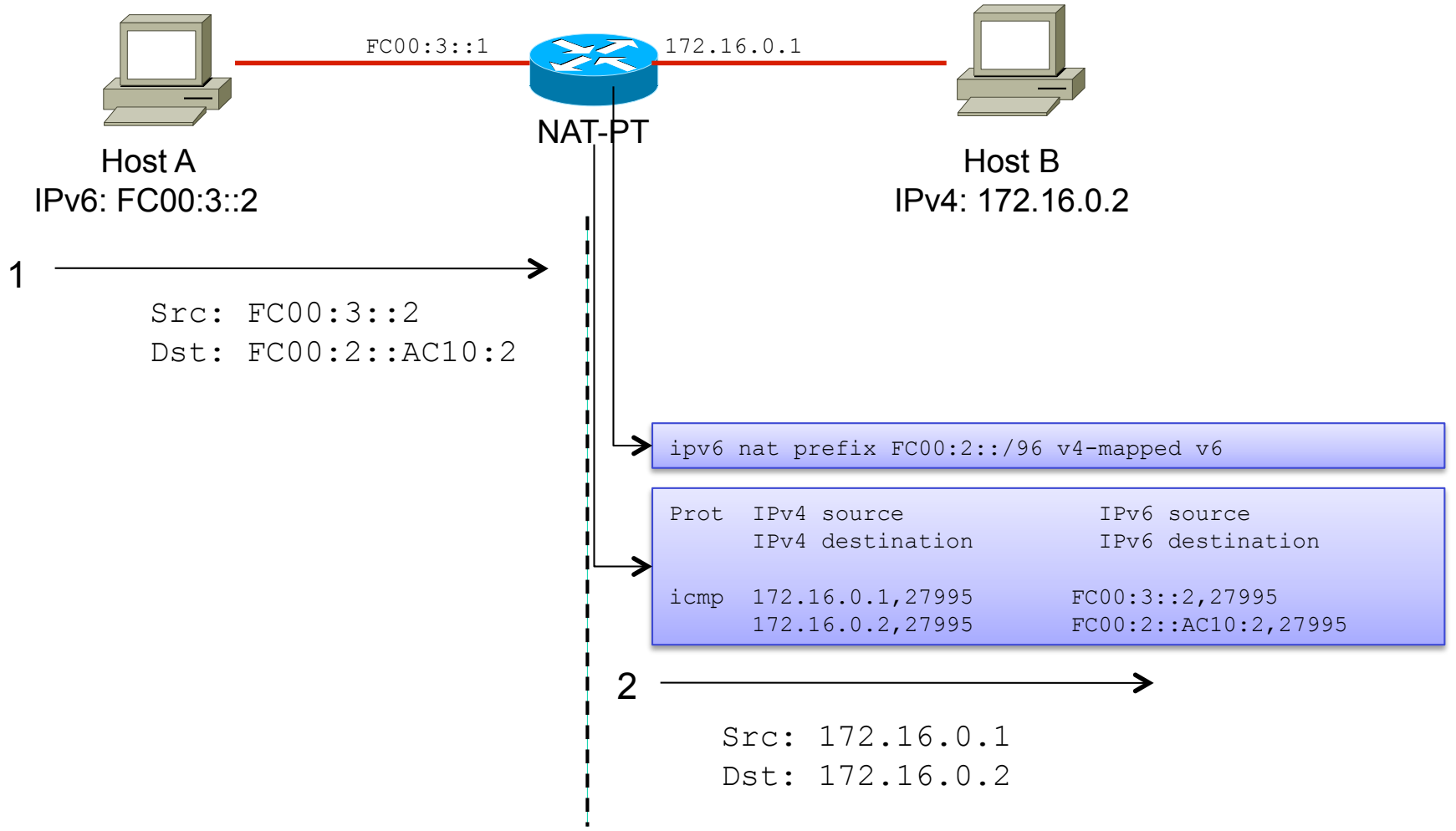
# NAT-PT
## *Konwersja adresu*

- Definiujemy prefix o długości /96 – adresy IPv4 będą konwertowane na adresy IPv6 z jego użyciem
- Prefix konfigurujemy globalnie lub na poziomie konkretnego interfejsu, jeżeli potrzebujemy wielu translacji
- `ipv6 nat prefix FC00:2::/96`

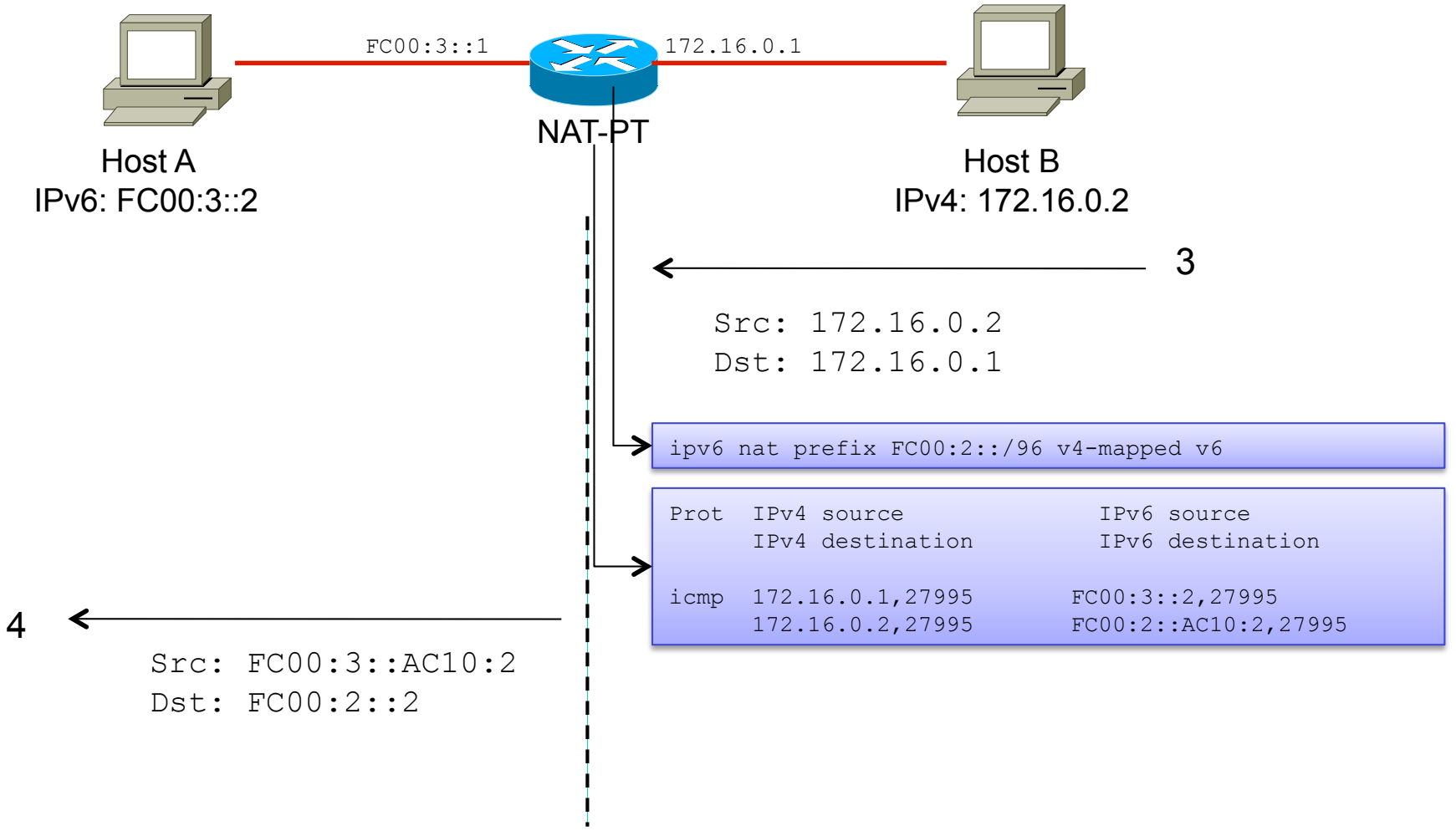
# NAT-PT
## *Konwersja adresu*



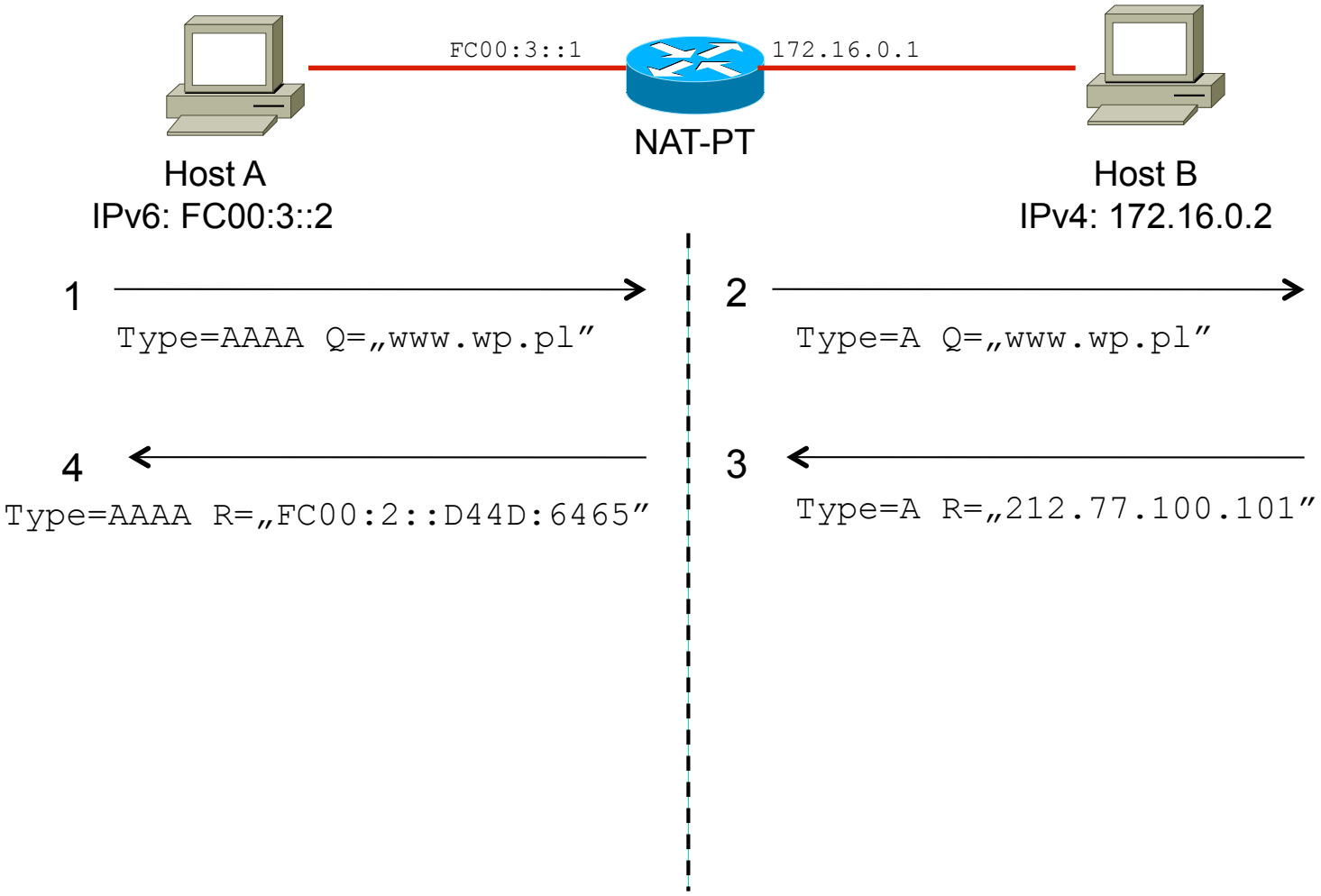
# NAT-PT
## *Proces translacji*



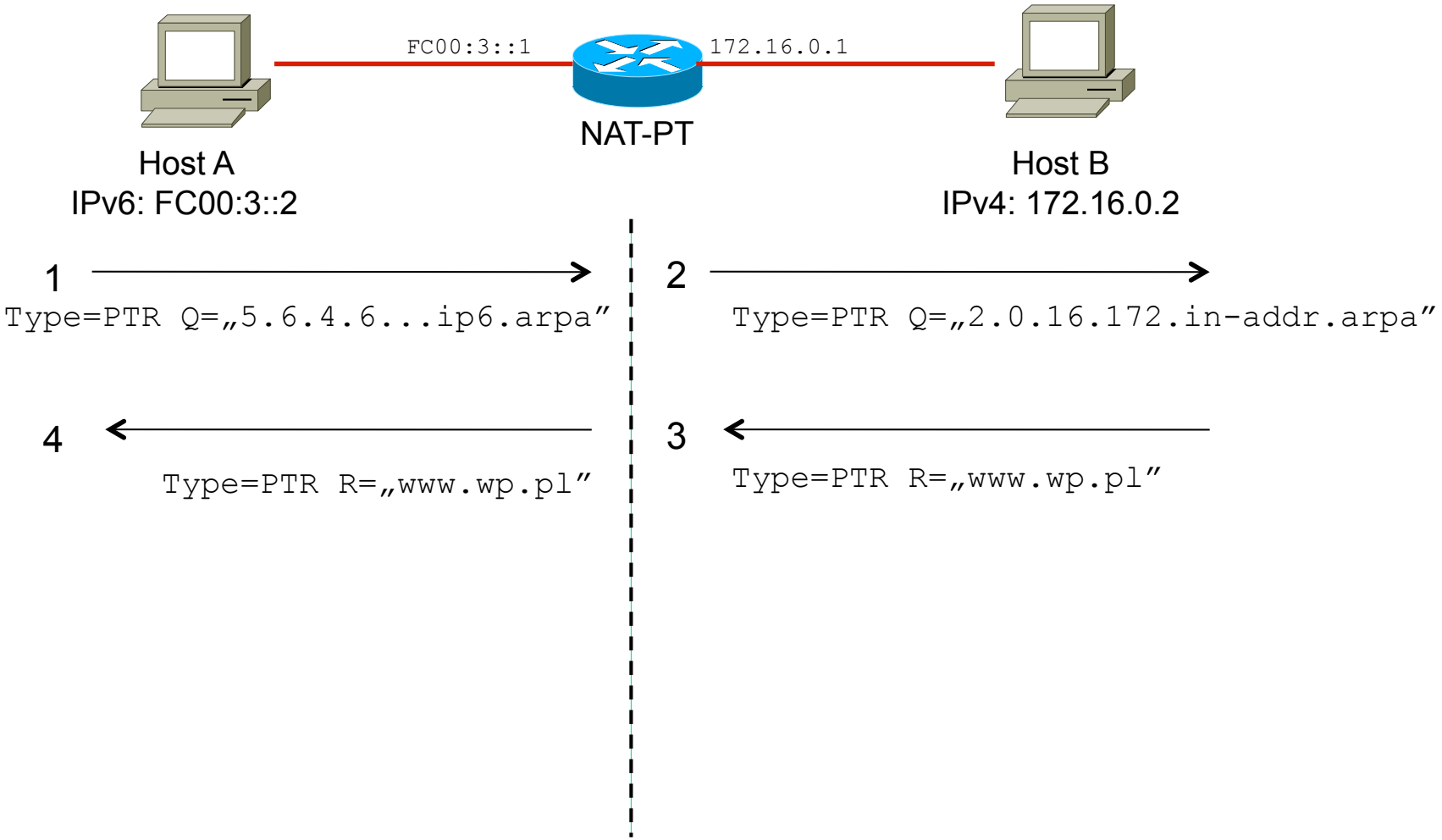
# NAT-PT
## *Proces translacji*



# NAT-PT
## *DNS ALG*



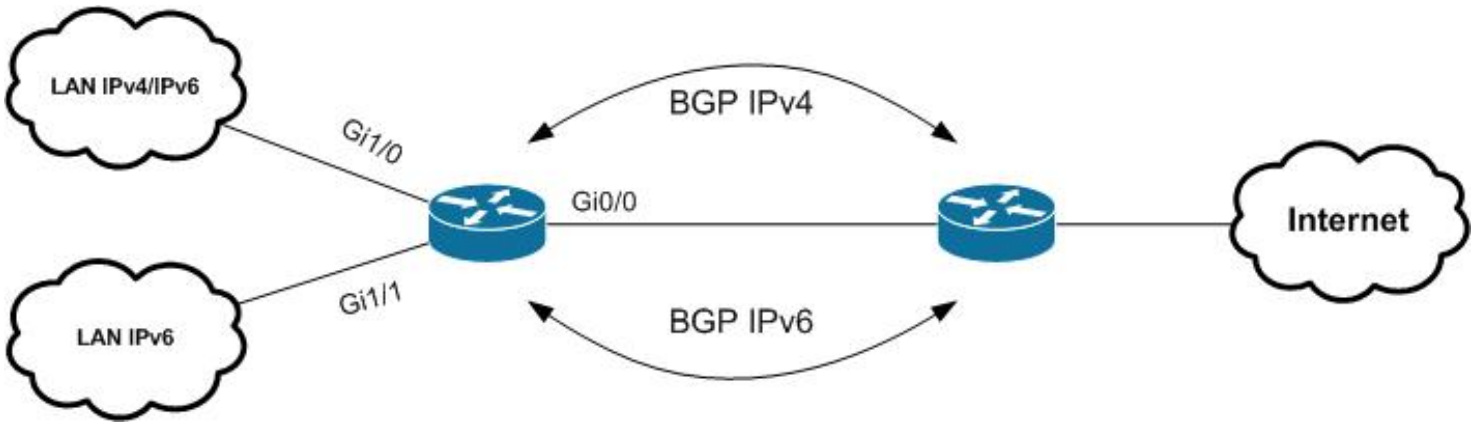
# NAT-PT
## *DNS ALG (RevDNS)*



# Agenda

- Wprowadzenie do adresacji IPv6
- Współistnienie sieci IPv4 i IPv6
- NAT-PT w teorii
- **NAT-PT w praktyce na Cisco**
- Ograniczenia
- Podsumowanie (Q&A)

# Konfiguracja NAT64 i DualStack w praktyce
## *Schemat*

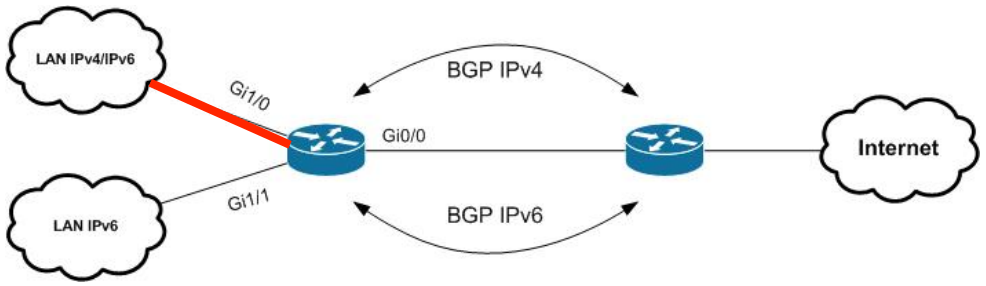


# Konfiguracja NAT64 i DualStack w praktyce
## *Założenia*

- W naszej sieci DualStack używamy publicznej adresacji `220.0.0.0/24` oraz `2001:1A68:FFFF:FFFB::/64`
- W sieci IPv6 stosujemy adresację ULA `FC00:1::/64`
- Mamy działające mechanizmy przyznawania adresów
- Prefix do NAT64 to `FC00:2::/96`

# Konfiguracja NAT64 i DualStack w praktyce
## *Interfejs LAN DualStack*

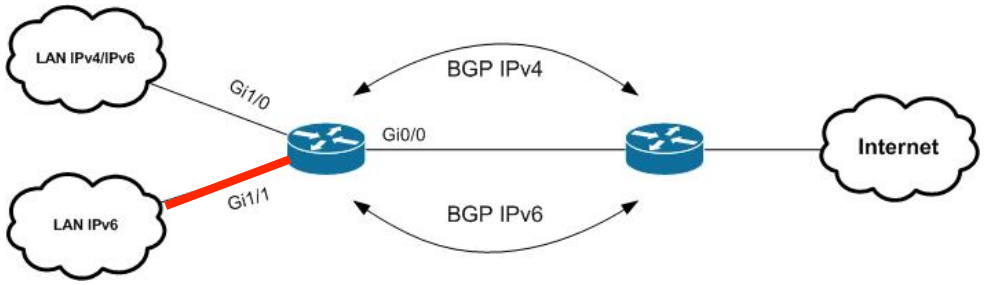
```
ipv6 unicast-routing
!
interface GigabitEthernet1/0
 ip address 220.0.0.1 255.255.255.0
 ip virtual-reassembly
 ipv6 address 2001:1A68:FFFF:FFFB::1/64
 ipv6 enable
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 nd ra lifetime 60
 ipv6 nd ra interval 10
```



# Konfiguracja NAT64 i DualStack w praktyce
## *Interfejs LAN IPv6*

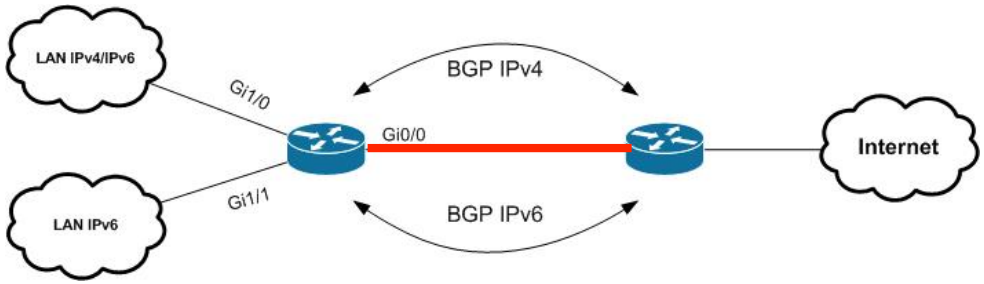
```
interface GigabitEthernet1/1
 ipv6 address FC00:1::1/64
 ipv6 enable
 ipv6 nd prefix FC00:1::/64
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 nd ra lifetime 60
 ipv6 nd ra interval 10
 ipv6 dhcp server IPv6
```

```
ipv6 dhcp pool IPv6
 dns-server FC00:2::D911:220A
```



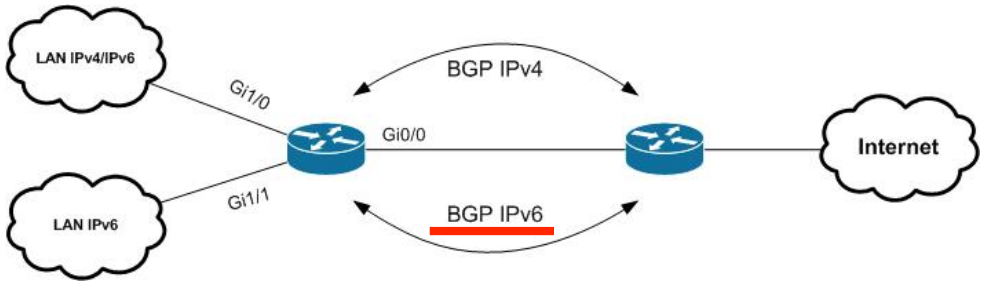
# Konfiguracja NAT64 i DualStack w praktyce
## *Styk z operatorem*

```
interface GigabitEthernet0/0
 ip address 217.17.0.2 255.255.255.252
 ipv6 address 2001:1A68:0:C::2/126
 ipv6 enable
 ipv6 nd ra suppress
```



# Konfiguracja NAT64 i DualStack w praktyce
## *Styk z operatorem – BGP*

```
router bgp 20000
 neighbor 2001:1A68:0:C::1 remote-as 15694
 neighbor 2001:1A68:0:C::1 ebgp-multihop 10
 !
 address-family ipv4
  no synchronization
  no neighbor 2001:1A68:0:C::1 activate
  no auto-summary
 exit-address-family
 !
 address-family ipv6
  network 2001:1A68:FFFF:FFFB::/64
  neighbor 2001:1A68:0:C::1 activate
  neighbor 2001:1A68:0:C::1 send-community both
  neighbor 2001:1A68:0:C::1 soft-reconfiguration inbound
 exit-address-family
```



# Konfiguracja NAT64 i DualStack w praktyce
## *NAT64*

```
ipv6 dhcp pool IPv6
 dns-server FC00:2::D911:220A
!
ipv6 nat v4v6 source 217.17.34.10 FC00:2::D911:220A
ipv6 nat v6v4 source list v6 interface GigabitEthernet0/0 overload
ipv6 nat prefix FC00:2::/96 v4-mapped v6
!
ipv6 access-list v6
 permit ipv6 FC00:1::/64 FC00:2::/96
```

# Konfiguracja NAT64 i DualStack w praktyce
## *NAT64*

```
interface GigabitEthernet0/0
 ipv6 nat
!
interface GigabitEthernet1/1
 ipv6 nat
```

# Konfiguracja NAT64 i DualStack w praktyce
## *NAT64*

```
c3925#sh ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
tcp   192.168.88.2,60695       FC00:1::2,60695
      192.168.88.1,5001        FC00:2::C0A8:5801,5001

tcp   192.168.88.2,60696       FC00:1::2,60696
      192.168.88.1,5001        FC00:2::C0A8:5801,5001
```

# Konfiguracja NAT64 i DualStack w praktyce
## *NAT64*

ATM SI

```
c3925#debug ipv6 nat ?
  <1-99>    Access list
  detailed  NAT-PT detailed events
  port      NAT-PT PORT events
  <cr>

*Feb 28 17:34:41.221: IPv6 NAT: IPv6->IPv4: icmp src (FC00:1::2) ->
(192.168.88.2), dst (FC00:2::C0A8:5801) -> (192.168.88.1)
*Feb 28 17:34:41.221: IPv6 NAT:  src (192.168.88.1) -> (FC00:2::C0A8:5801), dst
(192.168.88.2) -> (FC00:1::2)

*Feb 28 17:34:41.321: IPv6 NAT: IPv6->IPv4: icmp src (FC00:1::2) ->
(192.168.88.2), dst (FC00:2::C0A8:5801) -> (192.168.88.1)
*Feb 28 17:34:41.321: IPv6 NAT:  src (192.168.88.1) -> (FC00:2::C0A8:5801), dst
(192.168.88.2) -> (FC00:1::2)
```

# Agenda

- Wprowadzenie do adresacji IPv6
- Współistnienie sieci IPv4 i IPv6
- NAT-PT w teorii
- NAT-PT w praktyce na Cisco
- **Ograniczenia**
- Podsumowanie (Q&A)

# NAT64 na Cisco
## *Ciekawe obserwacje*

ATM SI

- DHCPv6 na routerach działa mimo wyłączonej usługi DHCP (no `service dhcp`) – przetestowane na routerach ISR z IOS 15.0
- Usunięcie NAT-PT z interfejsu „outside” powoduje wyłączenie NAT IPv4 – trzeba usunąć i ponownie dodać `ip nat outside` – przetestowane na routerach ISR z IOS 15.0
- Udało mi się wygenerować Traceback dla procesu „IPv6 Input” – stos IPv6 przestał działać.
- Ivan Pepelnjak na blogu „Cisco IOS hints and tricks” twierdzi, że trzeba wyłączyć CEF IPv4 i IPv6 do poprawnego działania NAT-PT z uwagi na brak fast switching – nie trzeba! (Przetestowane)
  - Jeżeli nie mamy w tablicy routingu trasy ::/0 – `no ipv6 cef`
  - Jeżeli mamy trasę ::/0 – oba CEFy mogą działać

# NAT64
## *Zalety*

- Przeźroczystość dla stacji końcowych
- Większość aplikacji wspierających IPv6 będzie działać bez problemu
- Możemy szybko stworzyć „wyspę” IPv6 z dostępem do zasobów Internetowych
- Wiemy jak działa i jak konfigurować NAT44 na Cisco – wiemy tak na prawdę jak skonfigurować NAT64

# NAT64
## *Wady*

- Zasobożerność CPU
- Problemy ze skalowaniem
- Konieczność zapewnienia symetrycznego ruchu poprzez ten sam router – wymusza niejednokrotnie brak redundantnej architektury
- Brak wsparcia dla multicastów, mało ALG

# PYTANIA?

# DZIĘKUJĘ ZA UWAGĘ