

# **Badanie porównawcze mechanizmów transportowania pakietów IPv4 przez środowisko IPv6**

**Janusz FURTAK, Zbigniew ŚWIERCZYŃSKI,  
Kamil RENCZEWSKI**

Institut Teleinformatyki i Automatyki WAT,  
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: W artykule przedstawiono wyniki badań porównawczych mechanizmów transportowania pakietów IPv4 poprzez środowisko IPv6, a także sugestie dotyczące zastosowania poszczególnych rozwiązań w środowiskach produkcyjnych (w tym dedykowanych do konkretnych zadań).

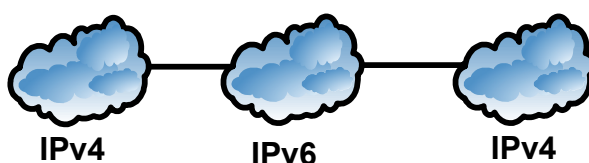
SŁOWA KLUCZOWE: IPv4, IPv6, tunelowanie, mechanizmy integracji

## **1. Wprowadzenie**

Wraz z rozwojem sieci Internet, sieci mobilnych oraz wzrostem liczby urządzeń wykorzystujących do komunikacji stos protokołów TCP/IP koniecznym zadaniem staje się wprowadzanie nowych rozwiązań, które zapewnią wystarczającą pulę adresów IP. Preferowanym rozwiązaniem jest nowa, szósta wersja protokołu IP. Jednakże ze względu na skalę i zastosowania obecnie wykorzystywanych technologii sieciowych, nie w każdym przypadku możliwe jest wprowadzenie nowych rozwiązań. W związku z powyższym konieczne było opracowanie metod integracji środowisk wykorzystujących protokoły IP w wersjach 4 i 6. Zagadnienie to zostało poruszone między innymi w następujących dokumentach RFC: [2], [3], [4], [5], [6]. Dokładne omówienie metod oraz mechanizmów integracji IPv4 i IPv6 wykracza poza ramy tego artykułu, ale szczegółowe informacje dotyczące tej tematyki są dostępne w opracowaniu [8].

Ze względu na mnogość rozwiązań zapewniających komunikację pomiędzy środowiskami sieciowymi wykorzystującymi różne wersje protokołu IP występuje konieczność opracowania metodyki umożliwiającej ocenę wybranych rozwiązań względem ściśle określonych kryteriów. Należy zauważyć, że różne środowiska produkcyjne (np. sieć korporacyjna, sieć mobilna, sieć realizująca VoIP) mają odmienne charakterystyki transmisji i dlatego wymagają zastosowania innych kryteriów oceny. Metodyka uwzględniająca poruszone kwestie została przedstawiona w [10] i stanowi podstawę badań, których wyniki zostaną zaprezentowane w kolejnych częściach artykułu.

W części drugiej dokładnie opisane zostało stanowisko laboratoryjne, które wykorzystywane było podczas przeprowadzania badań. Przedstawiona została topologia badanej sieci oraz specyfikacja wykorzystanego sprzętu i oprogramowania. Część trzecia poświęcona została badaniom wybranych mechanizmów transportowania pakietów IPv4 przez środowisko IPv6 – sytuacja poglądowo została zobrazowana na rys. 1.



Rys. 1. Integracja sieci IPv4 poprzez środowisko IPv6

Analizie poddane zostały następujące mechanizmy transportowania pakietów:

- tunelowanie GRE (*Generic Routing Encapsulation*)<sup>1</sup>;
- tunelowanie GPT (*Generic Packet Tunneling in IPv6*);
- NAT-PT – statyczny (podwójna translacja).

Należy zaznaczyć, że do transportowania pakietów IPv6 przez środowisko IPv4 można również wykorzystać „dynamiczny NAT-PT” bazujący na translacji adresów wykonywanej przy udziale serwerów DNS obsługujących IPv4 i IPv6. Rozwiązanie to nie zostało jednak uwzględnione w badaniach ze względu na złożoność konfiguracji oraz niską wydajność wynikającą z konieczności kilkukrotnego pobierania adresów z serwerów DNS. Szczegóły badań potwierdzających powyższe stwierdzenia można znaleźć w [9], [10] i [11].

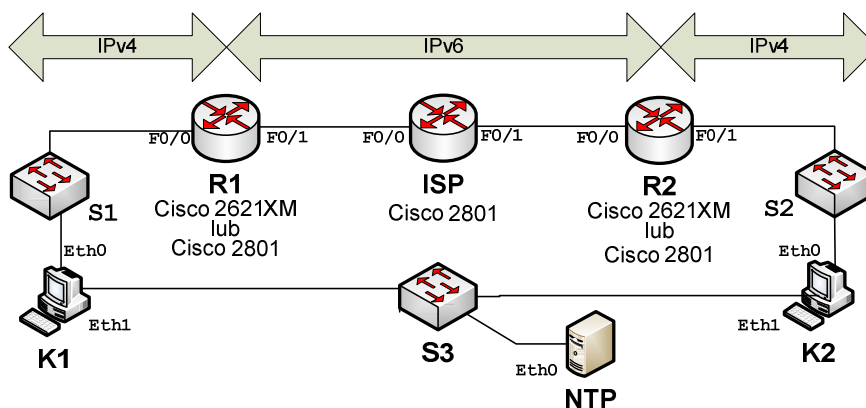
Na podstawie wyników badań sformułowano zalecenia dotyczące wdrażania poszczególnych mechanizmów integracji w określonych środowiskach produkcyjnych. Szczególną uwagę zwrócono na możliwość i efektywność wykorzystania poszczególnych rozwiązań do konkretnych zadań.

W podsumowaniu odniesiono się do uzyskanych wyników oraz wskazano rekomendowane rozwiązanie integracji środowisk korzystających z IPv4 i IPv6.

<sup>1</sup> W dalszej części artykułu będą używane skróty odpowiednio: GRE i GPT.

## 2. Stanowisko laboratoryjne

W celu realizacji badań przygotowano odpowiednie stanowisko laboratoryjne, którego topologia została przedstawiona na rys. 2. Do skompletowania stanowiska wykorzystano sprzęt sieciowy produkowany przez firmę Cisco oraz programowy generator/analizator ruchu *IP Traffic*, który zainstalowano na komputerach **K1** i **K2**. W tab.1 podane są szczegółowe parametry elementów sprzętowych stanowiska.



Rys. 2. Topologia stanowiska – obszary IPv4 komunikują się poprzez infrastrukturę IPv6

Tab. 1. Wykaz wykorzystywanego sprzętu

Nazwa urządzenia	Model	Oprogramowanie
R1, ISP, R2	Cisco 2621XM lub Cisco 2801	C2600-ADVIPSERVICESK9-M, Version 12.3 (11)T10 C2801-ENTSERVICESK9-M, Version 12.4 (22)T10
S1, S2, S3	Catalist 2960	C2960-LANBASEK9-M Version 12.2(44)SE6
NTP	z300-C(T101C) V2	-
K1, K2	Komputer klasy PC	MS Windows XP

Badania polegały na wysłaniu w ciągu około 30 sekund serii pakietów z komputera **K1** pełniącego rolę generatora ruchu do komputera **K2** pełniącego rolę analizatora ruchu. Po zakończeniu wysyłania serii pakietów porównywana była lista pakietów wysłanych z listą pakietów odebranych. Kluczowym elementem badania była identyfikacja wysłanych/odbieranych pakietów i dokładna synchronizacja czasowa generatora/analizatora ruchu. Do tego celu użyto serwer czasu wykorzystujący protokół NTP (*Network Time Protocol*). Serwer ten na rys. 2 jest zaznaczony jako **NTP**.

W konfiguracji przedstawionej na rys. 2 połączenie wykorzystujące przełącznik **S3** pomiędzy komputerami **K1**, **K2** oraz serwerem czasu **NTP** było wykorzystywane jedynie do synchronizacji czasu, a nie było wykorzystywane do realizacji transmisji, która była przedmiotem badania.

### 3. Badania wybranych mechanizmów integracji środowisk wykorzystujących protokoły IPv4 i IPv6

W badaniach używano metodyki oceny mechanizmów integracji środowisk wykorzystujących protokoły IPv4 i IPv6<sup>2</sup>, która szczegółowo została opisana w [13]. Zgodnie z tą metodyką ocena każdego mechanizmu była oceną względną w stosunku do tak zwanego rozwiązania bazowego. Takie podejście umożliwiło porównywanie ocen poszczególnych mechanizmów. W omawianych badaniach rolę rozwiązania bazowego pełniła sieć o topologii przedstawionej na rys. 2, w której był wykorzystywany tylko protokół IPv4.

Oceny badanych mechanizmów były ocenami złożonymi obejmującymi oceny wydajności mechanizmu i oceny właściwości użytkowych mechanizmów. W ocenie wydajności każdego mechanizmu uwzględniono:

- przepustowość;
- utracone pakiety;
- opóźnienie;
- fluktuacje transmisji;
- obciążenie procesora routera, który był początkiem tunelu.

Oceny właściwości użytkowych mechanizmów (dalej nazywane ocenami eksperckimi) wyznaczono na podstawie głosowania członków zespołu badawczego.

W ramach badań przeanalizowano trzy mechanizmy integracji sieci IPv4 i IPv6. W tab. 2 jest przedstawiony wykaz wykonanych badań.

Tab. 2. Wykaz badań mechanizmów integracji systemów IPv4 i IPv6

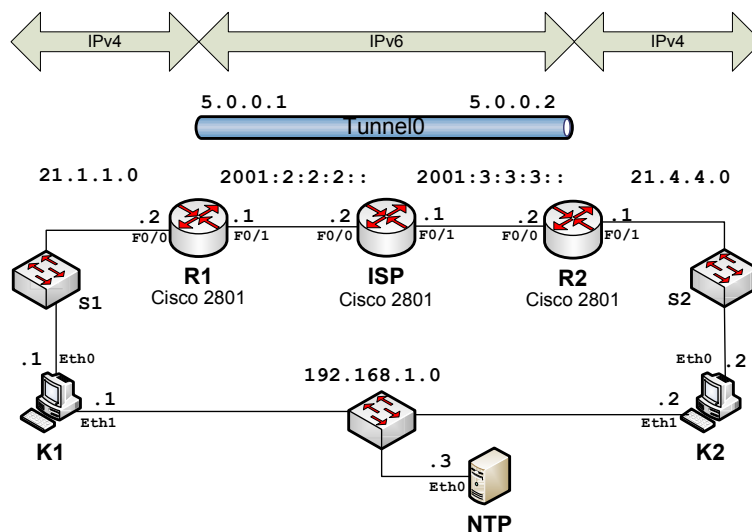
Oznaczenie	Opis
B.1	Brak tunelowania – jednorodne środowisko IPv4
B.2	Tunelowanie GRE
B.3	Tunelowanie GPT
B.4	NAT-PT statyczny – dwukrotna translacja

Mechanizm dynamicznego NAT-PT przy dwukrotnej dwukierunkowej translacji wymaga trzech serwerów DNS (tzn. dwóch DNS IPv4 i jednego IPv6). Ten mechanizm w początkowej fazie nawiązywania połączenia wymusza transmisję do odpowiednich serwerów DNS. Czas odpowiedzi tych serwerów w kolejnych takich samych eksperymentach jest różny i z tego względu uzyskiwane wyniki są trudne do porównywania. Z tego względu ten mechanizm nie został w badaniach sprawdzony. W dalszej części artykułu będą występowały odniesienia tylko do wersji statycznej NAT-PT.

<sup>2</sup> W dalszej części opracowania metodyka oceny mechanizmów integracji środowisk wykorzystujących protokoły IPv4 i IPv6 będzie nazywana *metodyką*.

### 3.1. Tunelowanie GRE

Badanie wykonano z wykorzystaniem programowego generatora ruchu *IP Traffic* oraz topologii pokazanej na rys. 3. Rolę routerów **R1**, **ISP** i **R2** pełniły routery Cisco 2801.



Rys. 3. Topologia dla badania tunelowania GRE

Badania zostały wykonane dla ruchu zawierającego różnej wielkości pakiety. Dla poszczególnych przypadków generowano pakiety:

- (s) o małej długości – 100 bajtów;
- (r) o losowej długości z przedziału <100;1400> bajtów;
- (bf) o długości 1400 bajtów;

Pierwszy przypadek charakteryzuje się koniecznością obsługi dużej liczby małych pakietów, co jest zbliżone do działania sieci komputerowej wykorzystywanej do transmisji strumieni audio-video. Drugi przypadek jest adekwatny do sytuacji, jaka ma miejsce w sieciach obsługujących różnego typu transmisje, czyli dotyczy on większości standardowych sieci komputerowych. Trzeci przypadek jest szczególnym z tego względu, że, co prawda, rzadko spotyka się sieci, w których rozmiar wszystkich pakietów oscyluje na pograniczu progu fragmentacji, ale pokazuje reakcję urządzeń sieci komputerowej, które są zmuszone do częstego fragmentowania pakietów. Uzyskane wyniki badań przy transmisji takich pakietów potwierdziły negatywny wpływ częstej fragmentacji na wydajność sieci.

Czas każdego badania: wynosił 30s. Wszystkie łącza Ethernetowe zostały skonfigurowane do pracy z prędkością transmisji 100Mb/s w trybie Full Duplex. W sieci wykorzystywany był routing statyczny. Istotne elementy konfiguracji

routerów **ISP**, **R1** i **R2** są przedstawione na rys. 4, 5 i 6, a wyniki badań dla poszczególnych przypadków zostały zestawione w tab. 3.

```
interface FastEthernet0/0
  no ip address
  ipv6 address 2001:2:2:2::2/64
  duplex full
  speed 100
interface FastEthernet0/1
  no ip address
  ipv6 address 2001:3:3:3::1/64
```

**Rys. 4. Konfiguracja routera ISP**

```
interface Tunnel0
  ip address 5.0.0.1 255.255.255.0
  tunnel source FastEthernet0/1
  tunnel destination 2001:3:3:3::2
  tunnel mode gre ipv6
!
interface FastEthernet0/0
  ip address 21.1.1.2 255.255.255.0
!
interface FastEthernet0/1
  no ip address
  ipv6 address 2001:2:2:2::1/64
!
ip route 0.0.0.0 0.0.0.0 Tunnel0
ipv6 route ::/0 FastEthernet0/1 2001:2:2:2::2
```

**Rys. 5. Konfiguracja routera R1 w badaniu tunelowania GRE**

```
interface Tunnel0
  ip address 5.0.0.2 255.255.255.0
  tunnel source FastEthernet0/0
  tunnel destination 2001:2:2:2::1
  tunnel mode gre ipv6
!
interface FastEthernet0/0
  no ip address
  ipv6 address 2001:3:3:3::2/64
!
interface FastEthernet0/1
  ip address 21.4.4.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 Tunnel0
ipv6 route ::/0 FastEthernet0/0 2001:3:3:3::1
```

**Rys. 6. Konfiguracja routera R2 w badaniu tunelowania GRE**

### 3.2. Tunelowanie GPT

Topologia sieci, sprzęt sieciowy, oprogramowanie oraz warunki wykonania badań tzn. rozmiar pakietów i czas trwania każdego eksperymentu nie uległy zmianie względem poprzedniego badania. Tryb pracy łączy Ethernetowych i konfiguracja routingu zostały skonfigurowane identycznie, jak w przypadku badania wydajności tuneli GRE. Badania różniły się tylko rodzajem skonfigurowanego tunelu na routerach **R1** i **R2**. Istotne elementy konfiguracji routerów **R1** i **R2** są przedstawione na rys. 7 i 8, a wyniki badań dla poszczególnych przypadków są pokazane w tab. 3.

```
interface Tunnel0
 ip address 5.0.0.1 255.0.0.0
 tunnel source FastEthernet0/1
 tunnel destination 2001:3:3:3::2
 tunnel mode ipv6
!
interface FastEthernet0/0
 ip address 21.1.1.2 255.0.0.0
!
interface FastEthernet0/1
 no ip address
 ipv6 address 2001:2:2:2::1/64
!
ip route 0.0.0.0 0.0.0.0 Tunnel0
ipv6 route ::/0 FastEthernet0/1 2001:2:2:2::2
```

**Rys. 7. Konfiguracja routera R1 w badaniu tunelowania GPT**

```
interface Tunnel0
 ip address 5.0.0.2 255.0.0.0
 tunnel source FastEthernet0/0
 tunnel destination 2001:2:2:2::1
 tunnel mode ipv6
!
interface FastEthernet0/0
 no ip address
 ipv6 address 2001:3:3:3::2/64
!
interface FastEthernet0/1
 ip address 21.4.4.1 255.0.0.0
!
ip route 0.0.0.0 0.0.0.0 Tunnel0
ipv6 route ::/0 FastEthernet0/0 2001:3:3:3::1
```

**Rys. 8. Konfiguracja routera R2 w badaniu tunelowania GPT**

### 3.3. NAT-PT – statyczny

Topologia sieci, oprogramowanie oraz warunki wykonania badań tzn. rozmiar pakietów i czas trwania eksperymentu nie uległy zmianie względem poprzedniego badania. Tryb pracy łączy Ethernetowych i konfiguracja routingu zostały skonfigurowane identycznie, jak w przypadku badania wydajności tuneli GRE. Na routerach **R1** i **R2** skonfigurowano statyczny mechanizm NAT-PT. Istotne elementy konfiguracji routerów **R1** i **R2** są przedstawione na rys. 9 i 10, a wyniki badań dla poszczególnych rozwiązań są pokazane w tab. 3.

```
interface FastEthernet0/0
 ip address 21.1.1.2 255.255.255.0
 ipv6 nat
interface FastEthernet0/1
 ipv6 address 2001:2:2:2::1/64
 ipv6 nat prefix 2010::/96
 ipv6 nat
!
ip classless
ipv6 route ::/0 FastEthernet0/1 2001:2:2:2::2
ip http server
no ip http secure-server
!
ipv6 nat v6v4 source 2001:1:1:1::1 21.1.1.1
ipv6 nat v4v6 source 10.3.51.1 2010::2
```

Rys. 9. Konfiguracja routera R1 w badaniu statycznego mechanizmu NAT-PT

```
interface FastEthernet0/0
 ipv6 address 2001:3:3:3::2/64
 ipv6 nat prefix 2011::/96
 ipv6 nat
!
interface FastEthernet0/1
 ip address 21.4.4.1 255.255.255.0
 ipv6 nat
!
ip classless
ipv6 route ::/0 FastEthernet0/1 2001:3:3:3::1
!
ip http server
no ip http secure-server
!
ipv6 nat v6v4 source 2001:1:1:1::1 11.0.0.1
ipv6 nat v4v6 source 21.4.4.2 2010::2
```

Rys. 10. Konfiguracja routera R2 w badaniu statycznego mechanizmu NAT-PT



**Tab. 3. Wyniki badań mechanizmów transportowania pakietów IPv4 przez środowisko IPv6**

nazwa pomiaru	<i>p</i> [Mbps]	<i>up</i>		<i>op</i> [ms]	<i>fl</i>	<i>cpu</i> [%]	ocena wydajności $O_{wyd}$	
		liczba utraconych	liczba wysłanych					
wpółcz. wagowe	4	2		2	4	1	80	
<b>B.1</b> brak tunelowania	(s)	89,2	0	249112	26	0	28	13
	(r)	89,7	0	270618	26	0	29	13
	(bf)	90,1	0	244343	26	0	27	13
<b>B.2</b> GRE	(s)	15,6	53	39623	32	0	97	3,013
	(r)	15,3	143	38756	30	0	97	3,114
	(bf)	15,8	245	38118	31	0	97	3,057
<b>B.3</b> Generic Packet Tunneling in IPv6	(s)	15,9	203	39848	26	0	97	3,401
	(r)	16,2	230	32415	29	0	98	3,211
	(bf)	16,2	63	41776	29	0	97	3,190
<b>B.4</b> NAT-PT	(s)	3,68	0	14789	33	1	55	2,265
	(r)	3,22	0	15647	32	0	52	2,737
	(bf)	4,49	0	12978	36	1	56	2,140

W tab. 3 użyto następujących oznaczeń:

- p* – przepustowość;
- up* – utracone pakiety;
- op* – opóźnienie liczone w milisekundach;
- fl* – fluktuacje transmisji;
- CPU* – obciążenie procesora routera, który był początkiem tunelu;
- $O_{wyd}$  – uogólniona ocena wydajności.

#### 4. Analiza wyników przeprowadzonych badań

Oceny eksperckie właściwości badanych mechanizmów integracji sieci IPv4 i IPv6, które wyznaczono według zasad szczegółowo opisanych w metodyce, są przedstawione w tab. 4. Najwyższe oceny eksperckie uzyskało tunelowanie GRE (B.2) (100% możliwych punktów), niewiele niższe tunelowanie GPT (B.3), a mechanizm statyczny NAT-PT (B.4) zdobył około połowy możliwych punktów.

**Tab. 4. Ocena ekspercka mechanizmów współdziałania IPv4 i IPv6**

Nr badania	Łatwość konfiguracji <0,10>	Liczba elementów konfiguracyjnych 10/L <sub>el</sub>	Łatwość diagnozowania <0,10>	Automatyzacja czynności konfiguracyjnych <0,5>	Automatyczna adaptacja do zmian <0,5>	Ograniczenia przy stosowaniu <0,10>	Wynik/ocena max
B.1	X	X	X	X	X	X	X
B.2	10	10	10	X <sup>3</sup>	X	10	40/40
B.3	10	10	10	X <sup>4</sup>	X	7 <sup>5</sup>	37/40
B.4	4	5 <sup>6</sup>	7 <sup>7</sup>	X	X	5 <sup>8</sup>	21/40

<sup>3</sup> Konfiguracja ogranicza się do czterech poleceń, więc trudno jest oceniać możliwość automatyzacji czynności konfiguracyjnych.

<sup>4</sup> j.w.

<sup>5</sup> Nie obsługuje ruchu *multicastowego*, nie obsługuje tunelowania pakietów IPv6 przez środowisko IPv4.

Pełne zestawienie wyników przeprowadzonych badań i ocen badanych mechanizmów jest przedstawione w tab. 5. Ocena końcowa podana w tab. 5 była obliczana zgodnie z metodyką według następującej formuły:

$$O_{kon} = w \cdot \frac{O_{wyd}}{O_{baz}} + (100 - w) \cdot \frac{O_{exp}}{O_{max}} \quad (1)$$

gdzie:  $w$  – współczynnik wagowy oceny wydajności  $O_{wyd}$  badanego mechanizmu równy 80;

$O_{wyd}$  – ocena wydajności badanego mechanizmu;

$O_{baz}$  – ocena wydajności bazowego mechanizmu;

$O_{exp}$  – ocena ekspercka mechanizmu;

$O_{max}$  – maksymalna ocena ekspercka możliwa do uzyskania.

**Tab. 5. Zestawienie otrzymanych wyników i ocen badanych mechanizmów**

nazwa pomiaru	$p$ [Mbps]	$up$		$op$ [ms]	$fl$	$cpu$ [%]	ocena wydajności i $O_{wyd}$	ocena ekspercka		ocena końcowa	
		liczba utraconych	liczba wysłanych					ocena	max		
wpółcz. wagowe	4	2		2	4	1	80	20		X	
<b>B.1</b> brak tunelowania	(s)	89,2	0	249112	26	0	28	13	X	X	X
	(r)	89,7	0	270618	26	0	29	13	X	X	X
	(bf)	90,1	0	244343	26	0	27	13	X	X	X
<b>B.2</b> GRE	(s)	15,6	53	39623	32	0	97	3,013	40	40	<b>38,5</b>
	(r)	15,3	143	38756	30	0	97	3,114	40	40	<b>39,2</b>
	(bf)	15,8	245	38118	31	0	97	3,057	40	40	<b>38,8</b>
<b>B.3</b> Generic Packet Tunneling in IPv6	(s)	15,9	203	39848	26	0	97	3,401	37	40	<b>39,4</b>
	(r)	16,2	230	32415	29	0	98	3,211	37	40	<b>38,3</b>
	(bf)	16,2	63	41776	29	0	97	3,190	37	40	<b>38,1</b>
<b>B.4</b> NAT-PT	(s)	3,68	0	14789	33	1	55	2,265	21	40	<b>24,4</b>
	(r)	3,22	0	15647	32	0	52	2,737	21	40	<b>27,3</b>
	(bf)	4,49	0	12978	36	1	56	2,140	21	40	<b>23,7</b>

Na podstawie uzyskanych wyników przeprowadzono analizę przydatności badanych mechanizmów do integracji środowisk IPv4 i IPv6 w przypadku, gdy pakiety IPv4 są transportowane przez środowisko IPv6. Mechanizmy integracji porównano biorąc pod uwagę następujące elementy:

- ocenę końcową uwzględniającą ocenę wydajności  $O_{wyd}$  i ocenę ekspercką;
- ocenę wydajności  $O_{wyd}$ ;
- ocenę uzyskiwanej przepustowości;
- ocenę fluktuacji czasów opóźnienia transmisji pakietów;
- obciążenie routerów wyrażone przez obciążenie procesora routera.

<sup>6</sup> Jest proporcjonalna do liczby urządzeń, między którymi ma być realizowana wymiana danych.

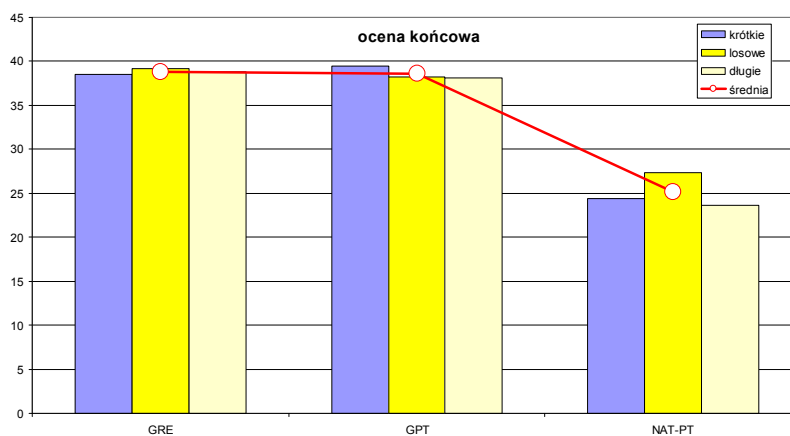
<sup>7</sup> Nawet w dużych sieciach, pomimo licznych wpisów w tablicy translacji, za kanał komunikacyjny pomiędzy konkretnymi hostami odpowiadają dwa wpisy translacyjne.

<sup>8</sup> Mało przydatny dla dużych sieci, w których często zmieniają się adresy na hostach, których transmisje trzeba translować, nie obsługuje ruchu *multicastowego*.

#### 4.1. Ocena końcowa uwzględniająca oceny eksperckie

Najważniejszym uogólnieniem (oceną końcową) w prowadzonym w ramach analizy wyników było powiązanie wyniku  $O_{wyd}$  z ocenami eksperckimi, które uzyskały poszczególne mechanizmy integracji. Oceny eksperckie miały wpływ na uogólniony wynik w stosunku 1:4, gdzie 1 to waga ocen eksperckich, a 4 to waga parametru  $O_{wyd}$ . W przypadku badanych mechanizmów integracji tunelowanie GRE uzyskało średnią ocenę końcową 38,84, która była minimalnie wyższa od średniej oceny 38,61 tunelowania GPT, pomimo tego, że GRE uzyskało nieco gorszy wynik w kategorii wydajności. Mechanizm NAT-PT uzyskał ocenę końcową najniższą (średnia ocena 25,15). Porównanie ocen końcowych jest przedstawione na rys. 11.

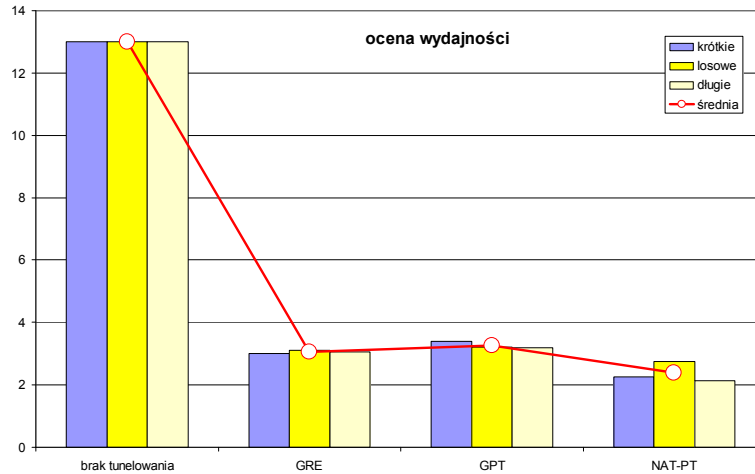
Kolejne płaszczyzny porównawcze odnoszą się do pojedynczych parametrów lub określonych podzbiorów parametrów, które przy wzajemnej korelacji mogą być przydatne podczas formułowania odpowiedzi na pytanie, z jakich mechanizmów należy skorzystać w przypadku przewagi określonych typów transmisji, np. VoIP.



Rys. 11. Ocena końcowa mechanizmów transportu pakietów

#### 4.2. Porównanie wydajności $O_{wyd}$

Porównanie ocen wydajności łącza w zależności od wykorzystywanego mechanizmu integracji jest przedstawione na rys. 12. W tym przypadku najlepszą ocenę 3,27 uzyskał tunel GPT, a nieznacznie gorszą ocenę 3,06 otrzymał tunel GRE. Warto zaznaczyć, że poziomem bazowym w tym eksperymencie była ocena wydajności transmisji bez tunelowania, która miała wartość 13,0. Mechanizm NAT-PT jest zdecydowanie najmniej wydajny, a uzyskana średnia wartość wydajności dla tego wariantu wyniosła 2,38.

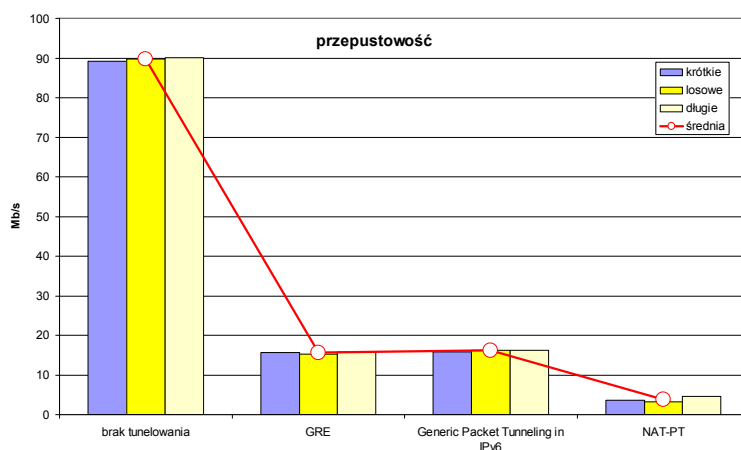


Rys. 12. Ocena wydajności łącza

### 4.3. Przepustowość łącza

Decyzję o szczególnym potraktowaniu tego parametru podjęto na podstawie obserwacji działania rzeczywistych sieci komputerowych, protokołów w nich wykorzystywanych oraz najczęściej zgłaszanych przez użytkowników wymagań. Można powiedzieć, że często potwierdza się reguła mówiąca o tym, że w nieprzeciążonych sieciach rzadko występuje utrata pakietów, znaczne fluktuacje, czy też duże opóźnienia. Dodatkowo, dysponując nieprzeciążonym łączem transmisyjnym protokoły połączeniowe (np. TCP) są w stanie przy wielu rodzajach transmisji (z wyłączeniem transmisji strumieniowych np. VoIP) zniwelować większość problemów związanych ze zdarzającymi się błędami poprzez retransmisje. To czy dana transmisja wysyci (przeciąży) łącze zależy w głównej mierze właśnie od przepustowości, co tłumaczy indywidualne potraktowanie tego parametru i sporządzenie dla niego oddzielnego porównania.

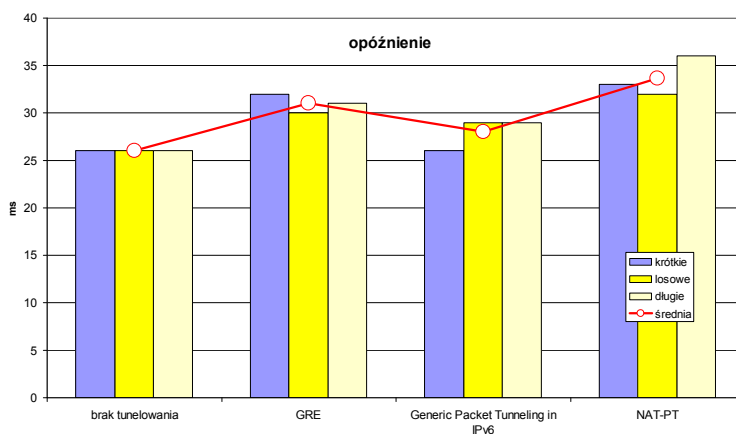
Uzyskane wyniki wskazują na to, że tunelowanie przy tych samych warunkach sprzętowych ograniczyło przepustowość, w porównaniu do poziomu bazowego, blisko sześciokrotnie. Oba typy tunelowania uzyskały bardzo podobne wyniki tzn. GRE - 15,57 Mb/s, a GPT - 16,1 Mb/s. Dużo słabiej w tym porównaniu wypadł statyczny NAT-PT. Mechanizm NAT-PT jest uważany za mało wydajny, a dodatkowo w tym przypadku konieczne jest dwukrotne tłumaczenie pakietów, najpierw z IPv4 do IPv6, a następnie znowu z IPv6 do IPv4. Przepustowość dla tego wariantu wyniosła 3,80 Mb/s. Dokładne porównanie przepustowości dla różnych wielkości pakietów zostało zaprezentowane na rys. 13.



Rys. 13. Ocena przepustowości badanych mechanizmów integracji

#### 4.4. Porównanie fluktuacji czasów opóźnienia transmisji pakietów i utraconych pakietów

Powiązanie wymienionych parametrów i porównanie tak uogólnionego wyniku może wskazać najlepsze rozwiązanie integracji środowisk IPv4 i IPv6 w przypadku transmisji wrażliwych na rozrzut opóźnień i straty pakietów, co jest bardzo istotnym na przykład przy transmisjach VoIP i video. Niestety trudno jednoznacznie ocenić wskazane cechy badanych mechanizmów, szczególnie porównując tunele z NAT-PT. Przy NAT-PT występują fluktuacje, przy tunelach ich nie ma, jednakże przy tunelach wychwycono fakt zagubienia pakietów, czego nie stwierdzono przy NAT-PT. Z tego powodu możliwe jest tylko wzajemne porównanie dwóch badanych tuneli, co graficznie zilustrowano na rys. 14.

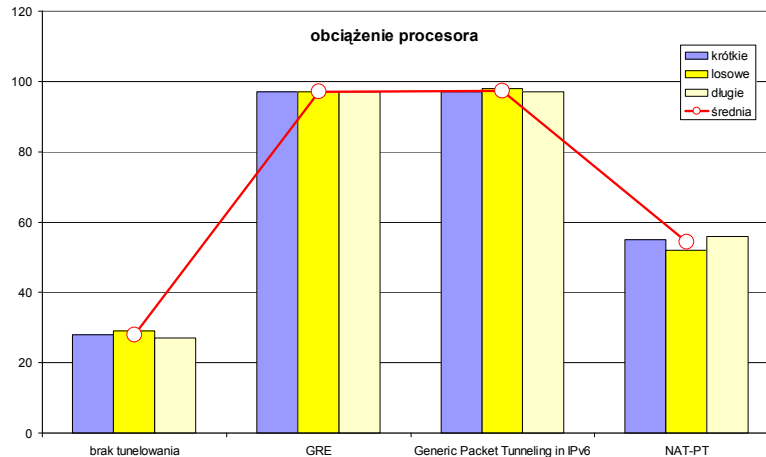


Rys. 14. Porównanie opóźnień dla badanych mechanizmów integracji

#### 4.5. Porównanie obciążenia procesorów routerów

Kolejną płaszczyzną do porównań jest obciążenie procesorów. Warto się skupić na porównaniu tego parametru tylko dla tuneli, ponieważ, jak wykazały badania, za małą wydajność mechanizmów NAT-PT nie odpowiada duże obciążenie procesora, który w tym przypadku był mniej angażowany niż przy zestawianiu tuneli.

Uzyskane wyniki wskazują, że obciążenie procesora w przypadku NAT-PT przyjmuje wartości średnie, zaś dla obu tuneli duże i bardzo zbliżone do siebie, co zostało zobrazowane na rys. 15.



Rys. 15 Porównanie obciążenia CPU routerów

#### 4.6. Podsumowanie

Podsumowując wyniki przeprowadzonych badań należy zauważyć, że najwyższą ocenę końcową uzyskało tunelowanie w trybie GRE. Tunelowanie GPT ma ocenę nieco gorszą, a zdecydowanie odbiegającą ocenę uzyskało rozwiązanie wykorzystujące NAT-PT. Na podstawie uzyskanych wyników nie można jednoznacznie ocenić wpływu rozmiaru ramek na uzyskane wyniki.

Warto zaznaczyć, że tunele bazujące na protokole GRE posiadają istotną cechę przenoszenia ruchu *multicastowego*. Jest to bardzo cenna właściwość tego protokołu przy konieczności wykorzystania protokołu routingu dynamicznego przez interfejs tunelu. Dane przenoszone w takim tunelu mogą być zaszyfrowane na przykład z wykorzystaniem protokołu IPSec. Rozważając organizację systemu QoS w sieciach IPv4 i IPv6 użyteczną cechą tunelowania GRE jest również możliwość automatycznego przepisywania przez router (enkapsulujący

zgodnie z protokołem GRE) wartości pola *Type of Service* nagłówka pakietu IPv4 do pola *Traffic Class* nagłówka IPv6 pakietu GRE.

Biorąc pod uwagę wyniki przeprowadzonych badań, dodatkowe właściwości tunelowania GRE i fakt rekomendowania tego protokołu w tunelowaniu pakietów IPv6 w środowisku IPv4, o którym mowa w [14] można stwierdzić, że preferowanym rozwiązaniem przy transportowaniu pakietów IPv6 przez środowisko IPv4 powinno być **tunelowanie GRE**.

## Literatura

- [1] AOUN C., DAVIES E., *Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status*, RFC 4966, July 2007.
- [2] CARPENTER B., MOORE K., *Connection of IPv6 Domains via IPv4 Clouds*, RFC 3056, February 2001.
- [3] CONTA A., DEERING S., *Generic Packet Tunneling in IPv6 Specification*, RFC 2473, December 1998.
- [4] CRAWFORD M., *Transmission of IPv6 Packets over Ethernet Networks*, RFC 2464, 1998.
- [5] DEERING S., HINDEN R., *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.
- [6] DOMMETY G., *Key and Sequence Number Extensions to GRE*, RFC 2890, September 2000.
- [7] FARINACCI D., LI T., HANKS S., MEYER D., TRAINA P., *Generic Routing Encapsulation (GRE)*, RFC 2784, March 2000.
- [8] FURTAK J., *Metody integracji sieci IPv4 i IPv6*, Biuletyn IAIr, nr 29/2010, str. 39 – 58.
- [9] FURTAK J. i inni, *Program badań współpracy systemów IPv4 oraz IPv6 – etap III, Sprawozdanie z realizacji zadania badawczego nr 22 w projekcie PBR-MNiSW-0 R00 0024 06*, 2010.
- [10] FURTAK J. i inni, *Przeprowadzenie eksperymentów dotyczących sposobów integracji IPv4 z IPv6 – etap III, Sprawozdanie z realizacji zadania badawczego nr 23 w projekcie PBR-MNiSW-0 R00 0024 06*, 2010.
- [11] FURTAK J. i inni, *Analiza wyników oraz opracowanie wniosków dotyczących współpracy systemów IPv4 z IPv6 – etap III, Sprawozdanie z realizacji zadania badawczego nr 24 w projekcie PBR-MNiSW-0 R00 0024 06*, 2010.
- [12] FURTAK J. i inni, *Rekomendacje dla procesu integracji systemów IPv4 z IPv6 – etap III, Sprawozdanie z realizacji zadania badawczego nr 26 w projekcie PBR-MNiSW-0 R00 0024 06*, 2010.

- [13] FURTAK J., ŚWIERCZYŃSKI Z., MALINOWSKI T., *Metodyka oceny mechanizmów integracji sieci IPv4 i IPv6*, Biuletyn IAIiR, nr 29/2010, str. 59 – 72.
- [14] FURTAK J., MALINOWSKI T., RENCZEWSKI K., *Badania porównawcze mechanizmów transportowania pakietów IPv6 przez środowisko IPv4*, Biuletyn IAIiR, nr 30/2011, str. 33 – 54.
- [15] TSIRTIS G., SRISURESH P., *Network Address Translation - Protocol Translation (NAT-PT)*, RFC 2766, February 2000.

### **Comparative research of mechanisms for transmission of IPv4 packets over IPv6 infrastructure**

ABSTRACT: The paper presents results of comparison of mechanisms for transmission of IPv4 packets over IPv6 infrastructure, as well as suggestions concerning the use of individual solutions in productive environments (including those with specific tasks).

KEYWORDS: IPv4, IPv6, tunneling, transition mechanisms

*Praca wpłynęła do redakcji: 28.01.2011*