Biuletyn WAT
Vol. LXI, Nr 1, 2012

Przydatność tunelowania GRE do integracji sieci IPv4 i IPv6

JANUSZ FURTAK, ZBIGNIEW ŚWIERCZYŃSKI

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Teleinformatyki i Automatyki, 00-908 Warszawa, ul. S. Kaliskiego 2, jfurtak@wat.edu.pl, z.swierczynski@ita.wat.edu.pl

Streszczenie. W artykule opisano tunelowanie GRE (*Generic Routing Encapsulation*), które jest używane jako jedna z metod integracji sieci IPv4 i IPv6. Przedstawiono zasady jego działania, konfiguracji oraz ocenę wydajności tego tunelowania w odniesieniu do innych alternatywnych metod integracji sieci IPv4 i IPv6. Przebadano dwa warianty wzajemnego ułożenia sieci IPv4 i IPv6. W pierwszym przypadku „wyspy IPv6" komunikowały się przez środowisko IPv4, a w drugim „wyspy IPv4" komunikowały się przez środowisko IPv6.
Słowa kluczowe: telekomunikacja, integracja sieci IPv4 i IPv6, sieci IPv6, tunelowanie protokołów

1. Wprowadzenie

Burzliwy rozwój sieci Internet w latach dziewięćdziesiątych XX w., stosowanie adresacji klasowej i nieodpowiednia dystrybucja grup adresów na poszczególne kontynenty (w konsekwencji do poszczególnych krajów) w powszechnie stosowanym protokole IP w wersji czwartej (IPv4) spowodowały szybkie wyczerpywanie puli adresów IPv4. Problem wyczerpywania się adresów IP próbowano rozwiązać wprowadzając różne rozwiązania mające na celu oszczędne gospodarowanie adresami, a równocześnie podjęto prace nad rozwiązaniami, które miały zwiększyć długość pola adresowego. Początkowo wykorzystywano maski sieciowe stałej długości[1], opisane w RFC 950 (1985 r.) [13], a później maski zmiennej długości

[1] Maski sieciowe stałej długości dawały możliwość wyznaczania identyfikatora sieci o długości większej niż 8, 16 lub 24 bity (zależnie od przynależności danego adresu do klasy sieci odpowiednio A, B lub C), to znaczy wyznaczania podsieci o rozmiarze dostosowanym do liczności węzłów w sieci,

(VLSM) (RFC 1009 — 1987 r.) i bezklasowy routing międzydomenowy (CIDR)[2] (RFC 1518 — 1993 r.), które są stosowane do dnia dzisiejszego. W lutym 1996 roku dokument RFC 1918 [15] wprowadził podział pełnego zakresu adresów IP na pulę tzw. adresów publicznych i prywatnych. W tym przypadku oszczędność polegała na możliwości wielokrotnego (w skali całej sieci Internet) wykorzystywania adresów prywatnych. Kosztem takiego rozwiązania jest konieczność stosowania serwerów NAT [1, 17], których zadaniem jest translacja adresów prywatnych na adresy publiczne i odwrotnie.

W połowie lat dziewięćdziesiątych rozpoczęto pracę nad nowym protokołem IP w wersji szóstej (IPv6). Nowy protokół oprócz zwiększenia długości pola adresowego zlikwidował szereg mankamentów protokołu IPv4, do których należy zaliczyć: często używany ruch rozgłoszeniowy (ang. *broadcast traffic*), konieczność przeliczania pól nagłówka każdej ramki na każdym routerze pośredniczącym w transmisji, brak wielopoziomowej hierarchii adresów. Ponadto protokół IPv6 wprowadził nowe rozwiązania, które są opisane w [3], na przykład: autokonfigurację adresu warstwy sieciowej niezauważalną dla użytkowników, mechanizm przenumerowywania adresów, obsługę mobilności i zintegrowane z protokołem IPv6 środowisko IPSec przeznaczone do zabezpieczania transmitowanych danych.

Przewidywano, że przejście z powszechnie używanego protokołu IPv4 do nowo projektowanego protokołu nie będzie zadaniem łatwym i krótkotrwałym. Równolegle z opracowywaniem rozwiązań dla IPv6 przygotowano szereg rozwiązań umożliwiających współistnienie sieci wykorzystujących protokół IPv4 i IPv6 [6]. Zasady ogólne stopniowego przejścia od sieci IPv4 do sieci IPv6 zostały określone w dokumentach RFC 3904 [12] i RFC 4213 [14]. Wśród rozwiązań można znaleźć tunelowanie pakietów jednego protokołu w pakietach drugiego protokołu z wykorzystaniem mechanizmu GRE (*Generic Routing Encapsulation*). W artykule przedstawiono sposób działania i zasady konfiguracji tunelowania GRE oraz wyniki badań wydajności tego rodzaju tunelowania.

2. Tunelowanie GRE

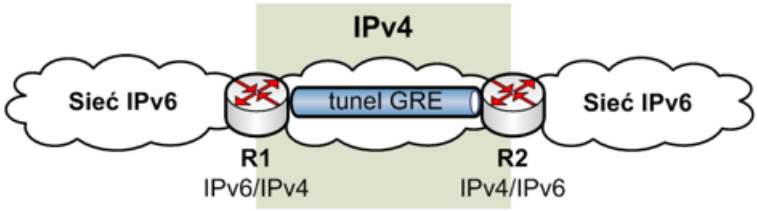
Tunelowanie polega na tym, że cały pakiet jednego protokołu IP jest traktowany jako ładunek (to znaczy, że cały pakiet jest umieszczany w polu danych) pakietu innego protokołu. Czynność ta nosi nazwę kapsułkowania lub enkapsulacji

co w konsekwencji prowadziło do zmniejszenia marnotrawienia adresów IP. Ograniczeniem tego rozwiązania była konieczność stosowania takiej samej maski sieciowej we wszystkich podsieciach danej sieci.

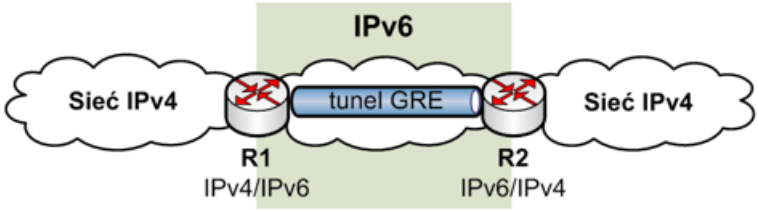
[2] Mechanizmy VLSM (*Variable Length Subnet Mask*) [2] i CIDR (*Classless Interdomain Routing*) [9, 16] umożliwiają efektywne gospodarowanie adresami IP i istotne zmniejszenie rozmiarów tablic routingu poprzez agregowanie tras.

(ang. *encapsulation*). Czynność odwrotna polegająca na odpakowaniu pakietu nosi nazwę dekapsulacji (ang. *decapsulation*). Jednym ze sposobów tunelowania jest tunelowanie z użyciem mechanizmu GRE. W szczególnym przypadku tunelowanie GRE może być wykorzystane do integracji sieci IPv4 i IPv6 poprzez transferowanie pakietów jednej wersji protokołu IP przez infrastrukturę drugiej wersji protokołu IP. Istnieje możliwość kapsułkowania pakietów protokołu IPv6 w pakietach protokołu IPv4 i odwrotnie. Tunelowanie pakietów może być zastosowane w dwóch różnych sytuacjach:

— sieci IPv6 (tzw. wyspy IPv6) wymieniają dane poprzez infrastrukturę IPv4 (rys. 1);
— sieci IPv4 (tzw. wyspy IPv4) wymieniają dane poprzez infrastrukturę IPv6 (rys. 2).



Rys. 1. Wyspy IPv6 wymieniają dane poprzez infrastrukturę IPv4



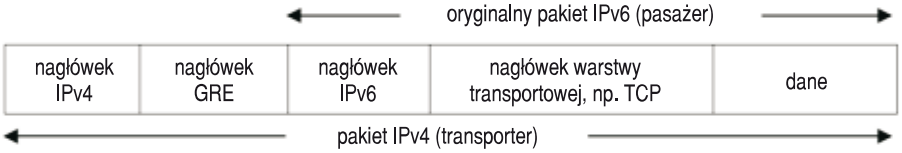
Rys. 2. Wyspy IPv4 wymieniają dane poprzez infrastrukturę IPv6

Pierwszy przypadek występuje częściej i jest odzwierciedleniem aktualnej sytuacji na świecie, w której pojawiające się sieci IPv6 wymieniają dane poprzez sieć Internet, gdzie powszechnie używanym protokołem jest IPv4. Drugi przypadek występuje w sytuacjach sieci zamkniętych (np. sieci wojskowych), w których infrastruktura jest zbudowana z urządzeń obsługujących nowy protokół IPv6, a użytkowane systemy mogą funkcjonować tylko w środowisku IPv4. W obu przypadkach routery **R1** i **R2** pełnią rolę końców tuneli i muszą obsługiwać podwójny stos.

Tunele mogą być konstruowane pomiędzy dwoma hostami, pomiędzy hostem a routerem i pomiędzy routerami. Mechanizmy tunelowania można pogrupować ze względu na sposób konfiguracji tuneli (tunele manualne i automatyczne), ich

zastosowania oraz sposób pakowania pakietu kapsułkowanego (pakietu pasażera) w pakiecie transportowym.

Tunelowanie GRE [4, 5] należy do grupy tuneli manualnych, tzn. konfiguracja tunelu jest wykonywana przez administratora na urządzeniach, które są zakończeniami tunelu i ta konfiguracja obowiązuje do momentu jej zmiany przez administratora. Ten rodzaj tunelowania może być wykorzystany zarówno do transferowania pakietów IPv6 poprzez infrastrukturę IPv4 (przypadek «1») jak i do transferowania pakietów IPv4 poprzez infrastrukturę IPv6 (przypadek «2»). Sposób kapsułkowania pakietów IPv6 w pakietach IPv4 przy tunelowaniu GRE jest pokazany na rysunku 3.



Rys. 3. Kapsułkowanie pakietów IPv6 w pakietach IPv4 przy tunelowaniu GRE

W przypadku kapsułkowania pakietów IPv4 w pakietach IPv6 przy tunelowaniu GRE kapsułkowanie jest podobne (rolę pasażera pełni pakiet IPv4, a transportera pakiet IPv6).

W przypadku «1» w polu „protokół" nagłówka IPv4 wpisywana jest liczba 47 wskazująca, że ładunkiem tego pakietu jest protokół GRE, pole „adres nadawcy" określa adres interfejsu wyjściowego kapsułkującego węzła, a pole „adres odbiorcy" adres zdalnego końca tunelu. W nagłówku GRE w polu „typ protokołu" wpisana jest liczba 0 × 86DD wskazująca, że ładunkiem pakietu GRE jest pakiet IPv6.

W przypadku «2» w polu „następny nagłówek" nagłówka IPv6 wpisywana jest liczba 47, wskazująca, że ładunkiem tego pakietu jest protokół GRE, pole „adres nadawcy" określa adres interfejsu wyjściowego kapsułkującego węzła, a pole „adres odbiorcy" adres zdalnego końca tunelu. W nagłówku GRE w polu „typ protokołu" wpisana jest liczba 0 × 0800 wskazująca, że ładunkiem pakietu GRE jest pakiet IPv4.

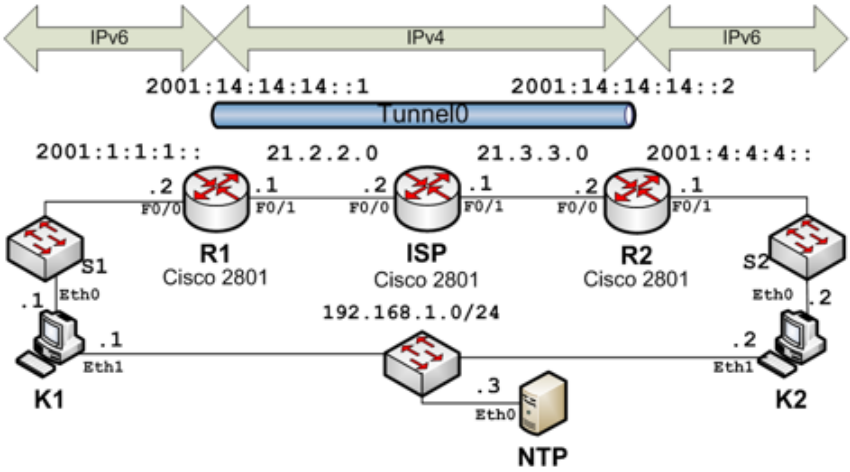
3. Badanie wydajności tunelowania GRE

Przy wprowadzaniu jakiegoś nowego rozwiązania najczęściej występuje konieczność zapewnienia tzw. „wstecznej zgodności" z poprzednimi rozwiązaniami. Tunelowanie GRE jest przykładem takiego mechanizmu umożliwiającego równoczesne użytkowanie w sieci „starego" protokołu IPv4 i „nowego" protokołu IPv6. W takich sytuacjach bardzo istotna jest odpowiedź na pytanie: jaki jest koszt zapewnienia wstecznej zgodności?

W celu znalezienia odpowiedzi na tak zadane pytanie przygotowano odpowiednie stanowisko badawcze, opracowano metodykę oceny i eksperymentalnie przebadano tunelowanie GRE dla dwóch wariantów: „wyspy IPv6" komunikują się przez środowisko IPv4 oraz „wyspy IPv4" komunikują się przez środowisko IPv6.

3.1. Metodyka oceny wydajności

Do wykonania pomiarów przygotowano stanowisko pomiarowe. Topologia wykorzystywanej sieci komputerowej z przykładowymi parametrami konfiguracyjnymi jest pokazana na rysunku 4. W pokazanej sieci źródłem danych jest komputer **K1**, a odbiorcą komputer **K2**. Tunel GRE był skonfigurowany pomiędzy routerami **R1** i **R2**. Jako kanał transmisyjny traktowano trasę **K1→S1→R1→ISP→R2→S2→K2.**



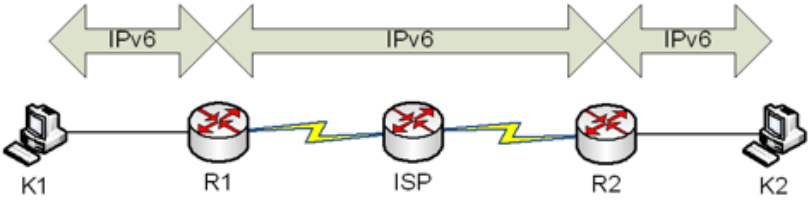
Rys. 4. Stanowisko do badania tunelowania pakietów IPv6 przez środowisko IPv4

Wydajność mechanizmu integracji jest oceną złożoną, w której uwzględniono oceny następujących elementów:

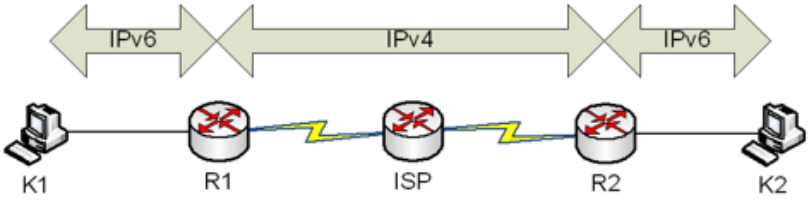
— przepustowość (ang. *throughput*) — przepływność kanału transmisyjnego liczona jako liczba bitów przesłana w jednostce czasu;
— utracone pakiety;
— opóźnienie;
— fluktuacja opóźnienia;
— obciążenie procesora routera.

Do wykonania pomiarów wykorzystano programowy generator ruchu „IP Traffic — Test & Measure" w wersji 2.5.8 firmy ZTI. W celu zwiększenia dokładności pomiarów stacja generująca ruch i stacja odbierająca ruch wykorzystywały serwer NTP.

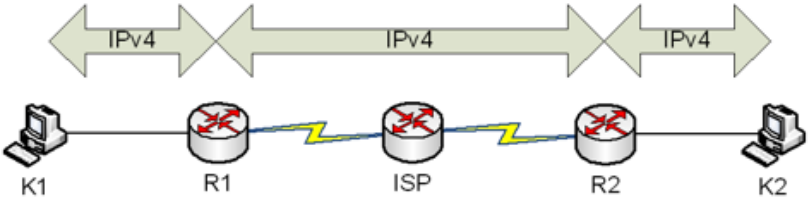
Wydajność każdego rozwiązania jest ściśle uzależniona od topologii sieci stanowiska badawczego i parametrów wykorzystywanego sprzętu sieciowego. W celu zminimalizowania wpływu tych dwóch elementów na ocenę badanego mechanizmu zaproponowano ocenę względną w stosunku do rozwiązania bazowego. Dla przypadku „wysp IPv6" połączonych tunelem GRE przez środowisko IPv4 (wariant A) środowiskiem bazowym była sieć tylko-IPv6 (rys. 5 i 6), a dla przypadku „wysp IPv4" połączonych tunelem GRE przez środowisko IPv4 (wariant B) środowiskiem bazowym była sieć tylko-IPv4 (rys. 7 i 8).



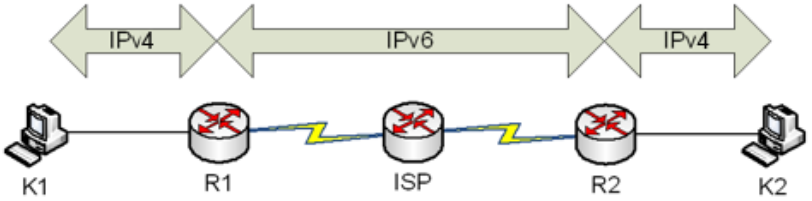
Rys. 5. Środowisko tylko-IPv6 (bazowe dla wariantu A)



Rys. 6. „Wyspy IPv6" połączone przez środowisko IPv4 (wariant A)



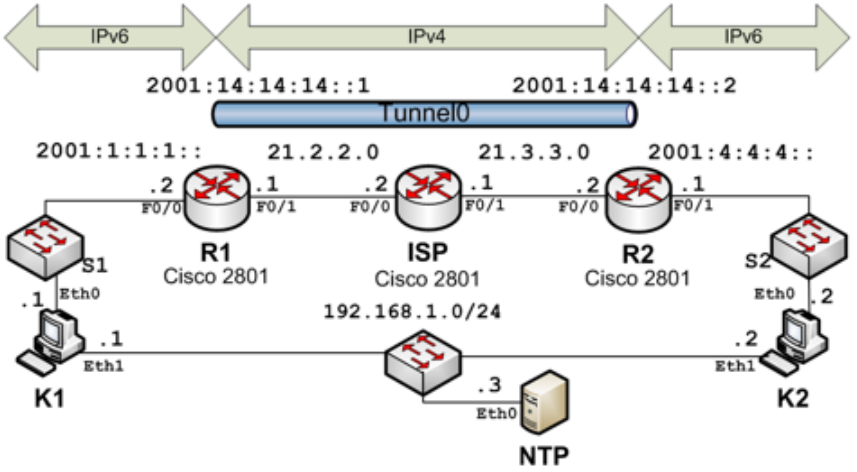
Rys. 7. Środowisko tylko-IPv4 (bazowe dla wariantu B)



Rys. 8. „Wyspy IPv4" połączone przez środowisko IPv6 (wariant B)

3.1. Tunelowanie GRE w wariancie IPv6-IPv4-IPv6

Badanie wykonano z wykorzystaniem programowego generatora ruchu *IP Traffic* oraz topologii pokazanej na rysunku 9. Rolę routerów **R1**, **ISP** i **R2** pełniły routery Cisco 2801.



Rys. 9. Topologia dla badania tunelowania GRE (IPv6-IPv4-IPv6)

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>;
— (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 szczególny o tyle, że rzadko spotyka się sieci, w których rozmiar wszystkich pakietów oscyluje na pograniczu progu fragmentacji. Wyniki badań przy transmisji pakietów, które na skutek zwiększenia rozmiaru w trakcie tunelowania (dodatkowa enkapsulacja) musiały zostać fragmentowane, dobitnie pokazały negatywny wpływ tego działania na wydajność sieci. Wybór długości pakietu 1400 bajtów przy wykonywaniu wszystkich opisanych eksperymentów w podanych topologiach gwarantował uniknięcie procedury fragmentacji, a równocześnie dawał możliwość obserwacji zachowania sieci, w której transmitowane były pakiety o prawie maksymalnej długości.

Czas każdego badania wynosił 30 s. Wszystkie łącza ethernetowe zostały skonfigurowane do pracy z prędkością transmisji 100 Mb/s w trybie Full Duplex. W sieci wykorzystywany był routing statyczny. Istotne elementy konfiguracji routerów **ISP**, **R1** i **R2** zostały przedstawione na rysunkach 10, 11 i 12, a uzyskane wyniki badań dla poszczególnych przypadków przedstawiono w tabeli 1.

```
hostname R1
!
ipv6 unicast-routing
!
interface Tunnel0
 no ip address
 ipv6 address 2001:14:14:14::1/64
 tunnel source FastEthernet0/1
 tunnel destination 21.3.3.2
 tunnel mode gre ip
!
interface FastEthernet0/0
 ipv6 address 2001:1:1:1::2/64
!
interface FastEthernet0/1
 ip address 21.2.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 21.2.2.2
!
ipv6 route ::/0 Tunnel0
```

Rys. 10. Konfiguracja routera R1

```
hostname R2
!
ipv6 unicast-routing
!
interface Tunnel0
 no ip address
 ipv6 address 2001:14:14:14::2/64
 tunnel source FastEthernet0/0
 tunnel destination 21.2.2.1
tunnel mode gre ip
!
interface FastEthernet0/1
 ipv6 address 2001:4:4:4::1/64
!
interface FastEthernet0/0
 ip address 21.3.3.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 23.3.3.1
!
ipv6 route ::/0 Tunnel0
```

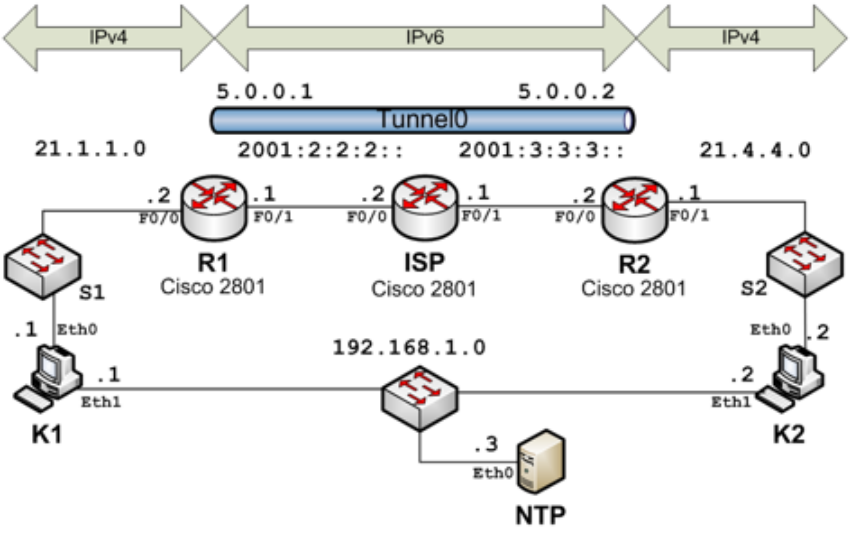
Rys. 11. Konfiguracja routera R2

```
hostname ISP
!
ipv6 unicast-routing
!
!
interface FastEthernet0/0
 ip address 21.2.2.2 255.255.255.0
!
interface FastEthernet0/1
 ip address 21.3.3.1 255.255.255.0
```

Rys. 12. Konfiguracja routera ISP

3.1. Tunelowanie GRE w wariancie IPv4-IPv6-IPv4

Badanie dla tego wariantu konfiguracyjnego wykonano w topologii pokazanej na rysunku 13. Wykorzystano ten sam sprzęt sieciowy, topologię oraz generator ruchu, co w wariancie IPv6-IPv4-IPv6. Takie same były również warunki wykonania badań.



Rys. 13. Topologia do badania tunelowania GRE

Istotne elementy konfiguracji routerów **ISP**, **R1** i **R2** zostały przedstawione na rysunkach 14, 15 i 16, a uzyskane wyniki badań dla poszczególnych przypadków zestawiono w tabeli 1.

```
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. 14. 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. 15. Konfiguracja routera R1

```
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. 16. Konfiguracja routera R2

3.2. Wyniki badań tunelowania GRE

Pełne zestawienie wyników przeprowadzonych badań i ocen badanych mechanizmów zostało przedstawione w tabeli 1.

Tabela 1

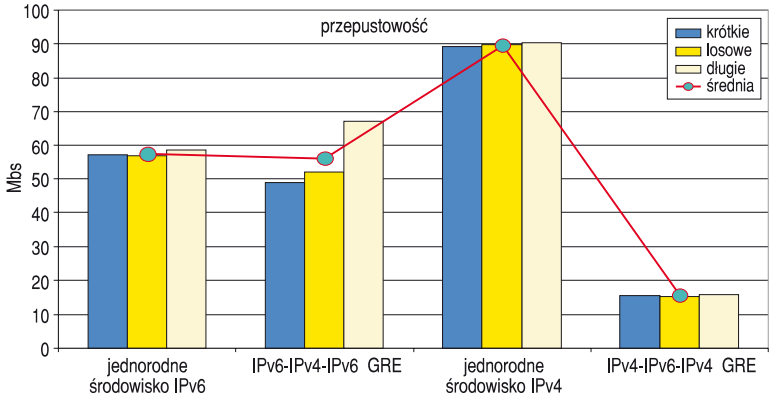
Wyniki badania wydajności tunelu GRE

Nazwa pomiaru		*p* [Mbps]	*up*		*op* [ms]	*fl*	*cpu* [%]
			liczba utraconych	liczba wysłanych			
współcz. wagowe		4	2	0	2	4	1
A.1	(s)	57,1	0	581578	0	0	56
jednorodne środowisko IPv6	(r)	56,7	0	243026	0	0	27
	(bf)	58,5	0	163922	0	0	20
A.2	(s)	49,1	2	274061	0	0	43
IPv6-IPv4--IPv6 GRE	(r)	52,0	0	229393	0	0	39,4
	(bf)	67,1	0	358922	0	0	59,6
B.1	(s)	89,2	0	249112	26	0	28
jednorodne środowisko IPv4	(r)	89,7	0	270618	26	0	29
	(bf)	90,1	0	244343	26	0	27
B.2	(s)	15,6	53	39623	32	0	97
IPv4-IPv6--IPv4 GRE	(r)	15,3	143	38756	30	0	97
	(bf)	15,8	245	38118	31	0	97

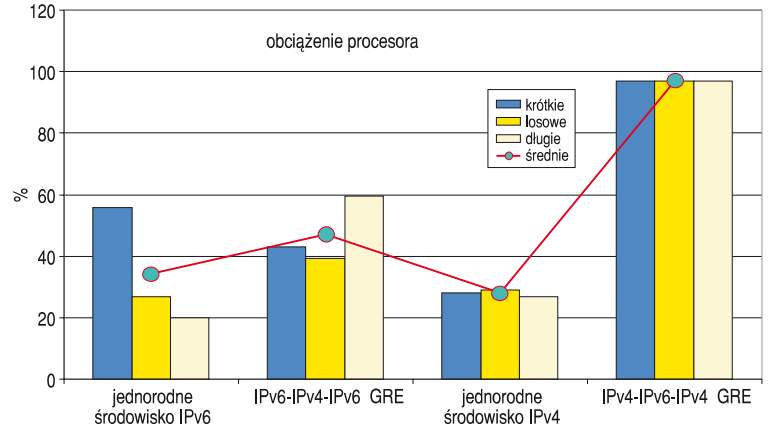
W tabeli 1 zostały zastosowane następujące oznaczenia:
p — przepustowość,
up — utracone pakiety,
op — opóźnienie liczone w milisekundach,
fl — fluktuacje transmisji,
CPU — obciążenie procesora routera, który był początkiem tunelu.

Uzyskane wyniki badania przepustowości i obciążenia procesora routera terminującego tunel są pokazane na rysunkach 17 i 18.

Przepustowość łącza w jednorodnym środowisku IPv6 wyniosła około 57 Mbs, a w jednorodnym środowisku IPv4 około 90 Mbs. Zastosowanie tunelowania GRE do połączenia wysp IPv6 przez środowisko IPv4 nieznacznie zmniejszyło przepustowość łącza do wartości około 56 Mbs w stosunku do środowiska jednorodnego tylko-IPv6. Istotną różnicę należy zauważyć w przypadku tunelowania GRE wykorzystanego do połączenia wysp IPv4 przez środowisko IPv6. Tu przepustowość wyniosła około 15 Mbs i była około sześciokrotnie niższa w stosunku do środowiska tylko IPv4.



Rys. 17. Porównanie przepustowości łącza z wykorzystaniem tunelowania GRE dla wariantu IPv6-IPv4-IPv6 i IPv4-IPv6-IPv4



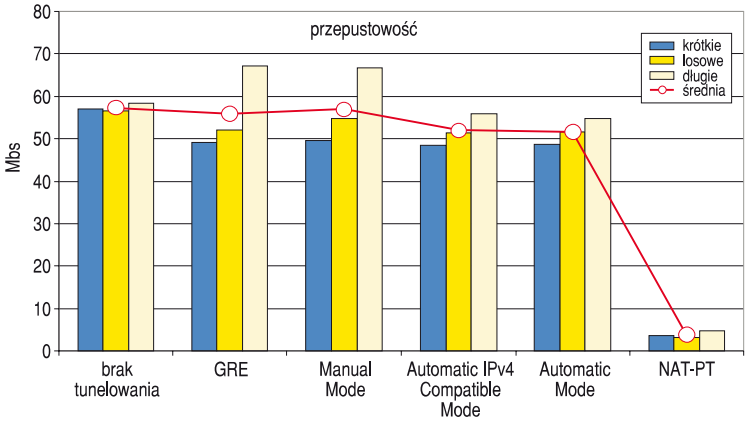
Rys. 18. Obciążenie procesorów routerów, które były początkiem tunelu GRE dla wariantu IPv6-IPv4-IPv6 i IPv4-IPv6-IPv4

Obciążenie procesora w przypadku środowisk jednorodnych i w przypadku tunelowania GRE w wariancie IPv6-IPv4-IPv6 kształtowało się na poziomie 30-50%, natomiast tunelowanie GRE w wariancie IPv4-IPv6-IPv4 obciążało procesor prawie w 100%.

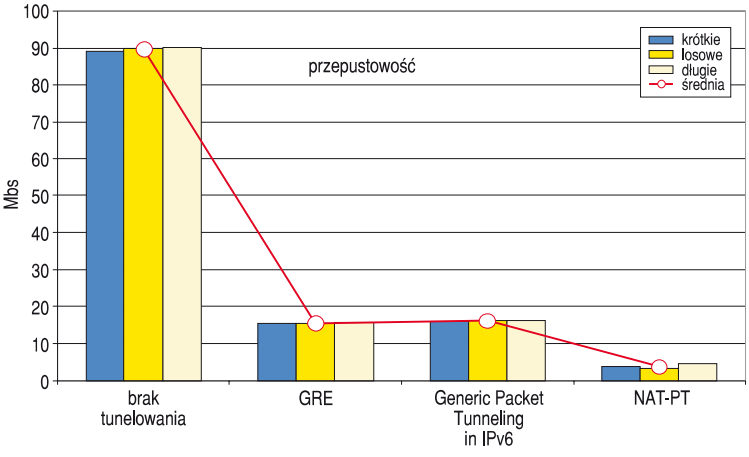
W przypadku obsługi pakietów, których rozmiar przekroczył próg fragmentacji, przepustowość sieci komputerowej drastycznie maleje. W przypadku tunelowania GRE w wariancie IPv6-IPv4-IPv6 rozmiar pierwotnego pakietu, aby nie był on fragmentowany, nie może przekroczyć 1476 bajtów. Wynika to z konieczności dodania do pakietu pierwotnego, w ramach wymaganej enkapsulacji, 20 bajtów nagłówka IPv4 oraz 4 bajtów nagłówka GRE. Daje to w sumie 1500 bajtów, co stanowi maksymalny rozmiar pakietu dla technologii Ethernet. W przeprowadzonych

doświadczeniach przepustowość sieci komputerowej w wariancie IPv6-IPv4-IPv6 dla pakietów przekraczających próg fragmentacji wynosiła średnio ok. 5,5 Mbs.

W ramach badań mechanizmów integracji sieci IPv4 i IPv6, oprócz badań tunelowania GRE, przebadano również inne mechanizmy umożliwiające współpracę sieci IPv4 i IPv6, stosując tę samą metodykę [7]. Porównanie przepustowości badanych mechanizmów jest pokazane na rysunkach 19 i 20[3]. Tunelowanie GRE jest jedynym mechanizmem, który występuje w obu wariantach integracji sieci IPv4 i IPv6. Dodatkowo, w porównaniu z innymi mechanizmami integracji sieci IPv4 i IPv6, charakteryzuje się dobrą wydajnością.



Rys. 19. Porównanie przepustowości tunelowania GRE i innych metod integracji IPv4 i IPv6 dla wariantu IPv6-IPv4-IPv6



Rys. 20. Porównanie przepustowości tunelowania GRE i innych metod integracji IPv4 i IPv6 dla wariantu IPv4-IPv6-IPv4

[3] Pełne opisy wyników badań innych mechanizmów są przedstawione w [7] i [9].

4. Zakończenie

Przeprowadzone eksperymenty pozwoliły odpowiedzieć na pytanie dotyczące kosztu zapewnienia wstecznej zgodności protokołu IPv6. Zastosowanie protokołu GRE do integracji środowisk IPv4 i IPv6 powoduje (w różnym stopniu zależnie od tego, czy łączone są wyspy IPv6, czy wyspy IPv4) zmniejszenie wydajności kanału komunikacyjnego w stosunku do środowisk jednorodnych, ale pozwala na ewolucyjne wprowadzanie nowego protokołu IPv6. W badaniach znalazło potwierdzenie spostrzeżenie mówiące o tym, że integrowanie wysp IPv6 poprzez infrastrukturę sieci IPv4 będzie naturalnym procesem upowszechnienia protokołu IPv6 w sieci Internet. W uzyskanych wynikach badań daje się zauważyć mniejsze skutki stosowania tunelowania GRE dla przypadku łączenia wysp IPv6 przez infrastrukturę IPv4 niż w przypadku łączenia wysp IPv4 poprzez środowisko IPv6.

Artykuł wpłynął do redakcji 25.03.2011 r. Zweryfikowaną wersję po recenzji otrzymano w październiku 2011 r.

LITERATURA

[1] C. Aoun, E. Davies, *Reasons to Move the Network Address Translator — Protocol Translator (NAT-PT) to Historic Status*, RFC 4966, July 2007.

[2] R. Braden, J. Postel, *Requirements for Internet Gateways*, RFC 1009, June 1987.

[3] S. Deering, R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

[4] G. Dommety, *Key and Sequence Number Extensions to GRE, RFC 2890*, September 2000.

[5] D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, *Generic Routing Encapsulation (GRE)*, RFC 2784, March 2000.

[6] J. Furtak, *Metody integracji sieci IPv4 i IPv6*, Biul. IAiR, 29, 2010.

[7] J. Furtak, T. Malinowski, K. Renczewski, *Badania porównawcze mechanizmów transportowania pakietów IPv6 przez środowisko IPv4*, Biul. IAiR, 30, 2011.

[8] J. Furtak, Z. Świerczyński, T. Malinowski, *Metodyka oceny mechanizmów integracji sieci IPv4 i IPv6*, Biul. IAiR, 29, 2010.

[9] J. Furtak, Z. Świerczyński, K. Renczewski, *Badania porównawcze mechanizmów transportowania pakietów IPv4 przez środowisko IPv6*, Biul. IAiR, 30, 2011.

[10] R. Hinden, *Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR)*, RFC 1517, September 1993.

[11] R. Hinden, S. Deering, *IP Version 6 Addressing Architecture*, RFC 4291, February 2006.

[12] C. Huitema, R. Austein, S. Satapati, R. van der Pol, *Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks*, RFC 3904, September 2004.

[13] J. Mogul, J. Postel, *Internet Standard Subnetting Procedure*, RFC 950, August 1985.

[14] E. Nordmark, R. Gilligan, *Basic Transition Mechanisms for IPv6 Hosts and Routers*, RFC 4213, October 2005.

[15] Y. Rekhter i in., *Address Allocation for Private Internets*, RFC 1918, February 1996.

[16] Y. Rekhter, T. Li, *An Architecture for IP Address Allocation with CIDR,* RFC 1518, September 1993.

[17] P. Srisuresh, M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, RFC 2663, August 1999.

J. FURTAK, Z. ŚWIERCZYŃSKI

GRE tunneling usability for IPv4 and IPv6 networks integration

Abstract. This paper considers GRE (*Generic Routing Encapsulation*) tunneling used as one of the methods of IPv4 and IPv6 networks integration. GRE tunnel operating rules, GRE tunnel configuration methods and GRE tunneling performance estimation in comparison to other IPv4 and IPv6 networks integration methods are described. Two variants of network IPv4 and IPv6 localizations were get into consideration. In the fist case, the "IPv6 islands" was connected by IPv4 environment, and in other case the "IPv4 islands" was connected by IPv6 environment.

Keywords: telecommunication, IPv6 networks, IPv4 and IPv6 networks integration, protocol tunnelling