BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 30, 2011

Badanie porównawcze mechanizmów transportowania pakietów IPv6 przez środowisko IPv4

Tomasz MALINOWSKI, Janusz FURTAK, Kamil RENCZEWSKI

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

STRESZCZENIE: W artykule przedstawiono wyniki badań porównawczych mechanizmów transportowania pakietów IPv6 poprzez środowisko IPv4. Wyniki te, w połączeniu z subiektywną oceną ekspercką danego mechanizmu, pozwalają wskazać preferowany tryb transportowania pakietów.

SŁOWA KLUCZOWE: IPv4, IPv6, translacja NAT-PT, tunelowanie

1. Wprowadzenie

Od wielu lat, od momentu opracowania protokołu IPv6 (nowego protokołu warstwy sieciowej), rozważane są techniki łączenia sieci bazujących na protokole IPv4 z sieciami wykorzystującymi protokół IPv6. Protokół IPv6 jest coraz częściej używany z uwagi na wyczerpanie pul adresowych IPv4 i niedogodności wynikające ze stosowania translacji NAT. Można domniemywać, że proces wprowadzania w sieciach prywatnych i korporacyjnych rozwiązań z protokołem IPv6 będzie w najbliższych latach przyspieszał. Niestety nie jest możliwe natychmiastowe zastąpienie protokołu IPv4 protokołem IPv6 w skali globalnej. W związku z tym koniecznym jest zastosowanie mechanizmów przejściowych, jako rozwiązań tymczasowych, które umożliwią transmisję pakietów pomiędzy sieciami IPv6 przez infrastrukturę sieci Internet, w której najczęściej używany jest protokół IPv4 [1], [3] i [6].

Opracowane do tej pory sposoby łączenia sieci IPv6 klasyfikowane są jako techniki tunelowania (*transition technology*), techniki tworzenia sieci z węzłami posiadającymi implementację zarówno protokołu IPv4, jak i nowego protokołu IPv6 (tzw. mechanizm podwójnego stosu – ang. *dual stack*) oraz techniki dwukierunkowej translacji protokołów (*translation technology*) [1], [5] i [14].

Zasady funkcjonowania mechanizmów integracji sieci IPv4 i IPv6 zostały opisane w [9], a metodyka oceny mechanizmów integracji takich sieci została przedstawiona w [11]. Metodykę tę wykorzystano w badaniach porównawczych wybranych mechanizmów integracji sieci IPv6 i IPv4, którym poświęcono niniejszy artykuł. W badaniach uwzględniono techniki tunelowania uznane za najłatwiejszy w realizacji sposób łączenia sieci z różnymi wersjami protokołu IP oraz mechanizm NAT-PT, który powinien być stosowany jedynie wtedy, gdy nie istnieje możliwość skonfigurowania tunelu lub wtedy, gdy trzeba zapewnić komunikację pomiędzy hostem używającym jedynie IPv6 a węzłem lub aplikacją IPv4.

Techniki tunelowania i mechanizm NAT-PT mogą być również wykorzystane do łączenia sieci IPv4 przez środowisko IPv6. Szczegółowe dane na temat badań tych przypadków można znaleźć w [12].

Celem badań porównawczych było wskazanie sposobu integracji sieci IPv4 i IPv6, który powinien być użyty w wojskowym systemie łączności integrującym sieci IPv6. Na ocenę końcową (uogólnioną) danego sposobu integracji składały się:

- uzyskana przepustowość kanału transmisyjnego;
- obciążenie procesora urządzenia tunelującego;
- liczba utraconych pakietów;
- opóźnienie i fluktuacja opóźnienia;
- ocena ekspercka obejmująca takie cechy konfigurowanego mechanizmu jak: łatwość konfiguracji, łatwość diagnozowania, możliwość zautomatyzowania czynności konfiguracyjnych, czy łatwość szybkiego zaadoptowania mechanizmu do nowych warunków rozumianych jako stan sieci po zmianie jej konfiguracji.

Niektóre cechy tuneli, stanowiące zaletę w przypadku wielu innych rozwiązań, ocenione zostały jako ich wady dyskwalifikujące użycie tunelu w wojskowym systemie łączności. Na przykład dynamiczne tunelowanie, uproszczające zarządzanie i utrzymanie tuneli, wprowadza równocześnie utrudnienia w nadzorowaniu ruchu przekazywanego przez dynamicznie podnoszony tunel z nieokreślonym *a priori* adresem końcowym tunelu. Ponadto w zastosowaniach wojskowych tunel powinien być terminowany na urządzeniach o zweryfikowanej tożsamości [9].

Spośród szeregu opracowanych technik tunelowania do badań wybrane zostały te, w których tunele terminowane są na urządzeniach granicznych (routerach) sieci IPv6.

Wykaz przeprowadzonych badań jest pokazany w tab. 1.

Tab. 1. Wykaz badań wybranych mechanizmów integracji systemów IPv4 i IPv6

oznaczenie	opis
A.1	Brak tunelowania – jednorodne środowisko IPv6
A.2	Tunelowanie GRE
A.3	Tunelowanie w trybie *Manual Mode*
A.4	Tunelowanie w trybie *Automatic IPv4 Compatible Mode*
A.5	Tunelowanie w trybie *Automatic Mode*
A.6	NAT-PT statyczny (dwukrotna translacja)

W tab. 2 jest przedstawiona ocena ekspercka badanych mechanizmów integracji, wyznaczona zgodnie z metodyką omówioną w [11].

Tab. 2. Ocena ekspercka wybranych mechanizmów współdziałania IPv6 i IPv4

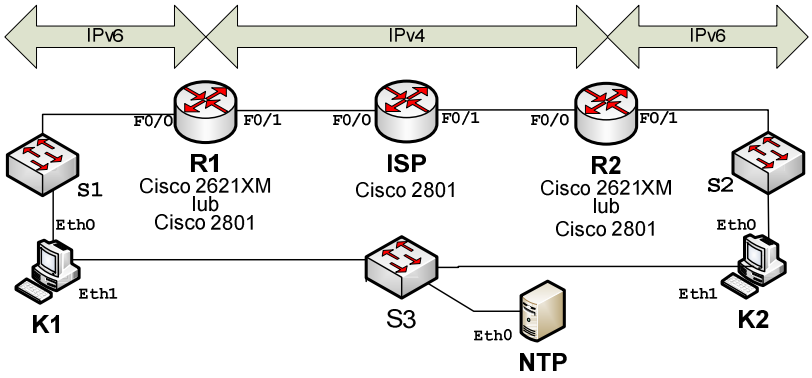
Nr badania	Łatwość Konfiguracji <0;10>	Liczba elementów konfiguracyjnych 10/Lel	Łatwość diagnozowania <0;10>	Automatyzacja czynności konfiguracyjnych <0;5>	Automatyczna adaptacja do zmian <0;5>	Ograniczenia przy stosowaniu <0;10>	Wynik/ ocena max
A.1	X	X	X	X	X	X	X
A.2	10	10	10	X[1]	X	10	**40/40**
A.3	10	5	10	X[2]	X	10	**35/40**
A.4	10	10	10	5[3]	5	10	**50/50**
A.5	10	10	10	5[4]	5	5[5]	**45/50**
A.6	4	5[6]	7[7]	X	X	5[8]	**21/40**

[1] Konfiguracja ogranicza się do wydania trzech poleceń – automatyzacja jest zbędna
[2] j.w.
[3] Punkt końcowy tunelu nie jest jawnie definiowany, a jego adres jest automatycznie wyznaczany z adresu IPv4 interfejsu stanowiącego zakończenie tunelu
[4] Punkt końcowy tunelu nie jest jawnie definiowany, a jego adres jest automatycznie wyznaczany z adresu IPv4 interfejsu stanowiącego zakończenie tunelu
[5] Wymagane jest użycie dla określenia tunelu adresów z prefiksem 2002::/16
[6] Jest proporcjonalna do liczby urządzeń, między którymi ma być nawiązany kanał wymiany danych.
[7] Nawet w dużych sieciach, pomimo licznych wpisów w tablicy translacji, za kanał komunikacyjny pomiędzy konkretnymi hostami odpowiadają dwa wpisy translacyjne.

W podsumowaniu odniesiono się do uzyskanych wyników oraz wskazano rekomendowane rozwiązanie do łączenia środowisk IPv6 przez sieć IPv4.

2. Stanowisko laboratoryjne

W celu realizacji badań przygotowano odpowiednie stanowisko laboratoryjne, którego topologia została przedstawiona na rys. 1. 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. 3 przedstawione są szczegółowe parametry elementów sprzętowych stanowiska.



Rys. 1. Topologia sieci użyta w badaniach tunelowania pakietów IPv6 przez sieć IPv4

Tab. 3. Wykaz wykorzystywanego sprzętu

Nazwa urządzenia	Model	Oprogramowanie
R1, ISP, R2	Cisco 2801 lub Cisco 2621XM[9]	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 wysyłaniu 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

[8] Mało przydatny dla dużych sieci, w których często zmieniają się adresy na hostach, których transmisje trzeba translować.

[9] Routery Cisco 2621XM były używane przy badaniu mechanizmu NAT-PT z tego powodu, że w systemach IOS routerów Cisco 2801 nie było możliwości prawidłowego skonfigurowania NAT-PT

elementem badania była identyfikacja wysłanych/odbieranych pakietów i dokładna synchronizacja czasowa generatora/analizatora ruchu. Do tego celu użyto serwer czasu[10] wykorzystujący protokół NTP (*Network Time Protocol*) Serwer ten na rys. 1 jest zaznaczony jako **NTP**.

W konfiguracji przedstawionej na rys. 1 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.

Jako podstawę wszystkich pomiarów wykorzystano topologię bazową (rys. 1), która była modyfikowana w celu dostosowania do potrzeb poszczególnych badań. Tunele terminowane były na interfejsach routerów **R1** i **R2**, łączących te routery z routerem o nazwie **ISP**. Badania kolejnych mechanizmów integracji sieci IPv4 i IPv6 wymagały modyfikacji konfiguracji stanowiska. Istotne elementy konfiguracji stanowiska właściwe dla każdego badania są przedstawione w opisie poszczególnych eksperymentów.

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

Kolejne podpunkty zawierają szczegółowe dane dotyczące konfiguracji środowiska badawczego dla wymienionych w tab. 1 mechanizmów transportowania pakietów IPv6 przez sieć z protokołem IPv4.

Opracowana metodyka oceny mechanizmów integracji środowisk wykorzystujących protokoły IPv4 i IPv6[11] przewiduje uwzględnienie przy porównywaniu następujących elementów:

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

Założono, że pomiary wymienionych parametrów najpierw będą wykonane w środowisku tylko-IPv6. Wyniki uzyskane w tym badaniu będą przyjęte jako bazowe, z którymi będą porównywane wyniki uzyskane przy badaniu poszczególnych rozwiązań.

[10] http://www.zti-telecom.com

[11] Szczegółowy opis metodyki oceny mechanizmów integracji sieci IPv4 i IPv6 (dalej zwaną metodyką) można znaleźć w [11].

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.

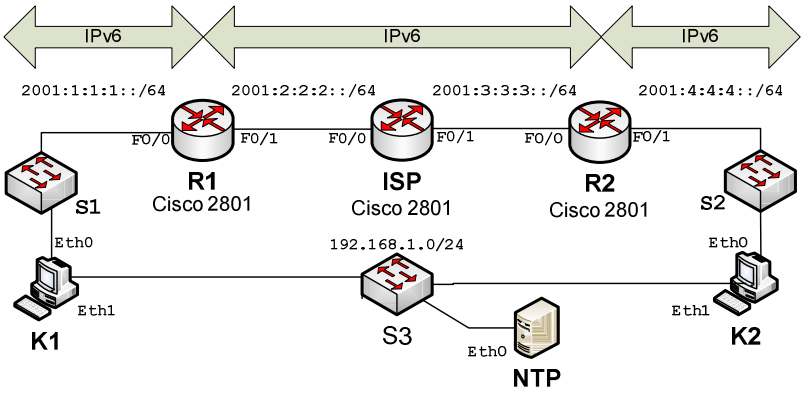
Pierwszy przypadek charakteryzuje się koniecznością obsługi dużej liczby małych pakietów, co jest zbliżone do działania sieci komputerowej wykorzystywanej do transmisji strumieni audio-video. Drugi przypadek jest adekwatny do sytuacji, jaka ma miejsce w sieciach obsługujących różnego typu transmisje, czyli dotyczy on większości standardowych sieci komputerowych. Trzeci przypadek jest szczególnym o tyle, że rzadko spotyka się sieci, w których rozmiar wszystkich pakietów oscyluje na pograniczu progu fragmentacji. Z drugiej strony przypadek ten jest ciekawy, bo pokazuje reakcję sieci komputerowej, a w zasadzie urządzeń, które dokonują fragmentacji w sytuacji, kiedy należy często przeprowadzać tego typu działania. 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.

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, za wyjątkiem badania tunelowania w trybie Automatic IPv4 Compatible Mode.

Uzyskane wyniki badań są przedstawione w tab. 4.

3.1. Badanie A.1 - Brak tunelowania w środowisku tylko-IPv6

Badanie wykonano z wykorzystaniem programowego generatora ruchu *IP Traffic* w sieci tylko-IPv6 oraz topologii sieci przedstawionej na rys. 2.



Rys. 2. Topologia bazowa użyta w badaniach porównawczych

Istotne elementy konfiguracji routerów **ISP**, **R1** i **R2** zostały przedstawione na rysunkach 3, 4 i 5.

```
hostname ISP
ipv6 unicast-routing
interface FastEthernet0/0
 ipv6 address 2001:2:2:2::2/64
!
interface FastEthernet0/1
 ipv6 address 2001:3:3:3::1/64
!
ipv6 route 2001:1:1:1::/64 FastEthernet0/0 2001:2:2:2::1
ipv6 route 2001:4:4:4::/64 FastEthernet0/1 2001:3:3:3::2
```

Rys. 3. Konfiguracja routera ISP

```
hostname R1
ipv6 unicast-routing
interface FastEthernet0/0
 ipv6 address 2001:1:1:1::2/64
!
interface FastEthernet0/1
 ipv6 address 2001:2:2:2::1/64
!
ipv6 route ::/0 FastEthernet0/1 2001:2:2:2::2
```

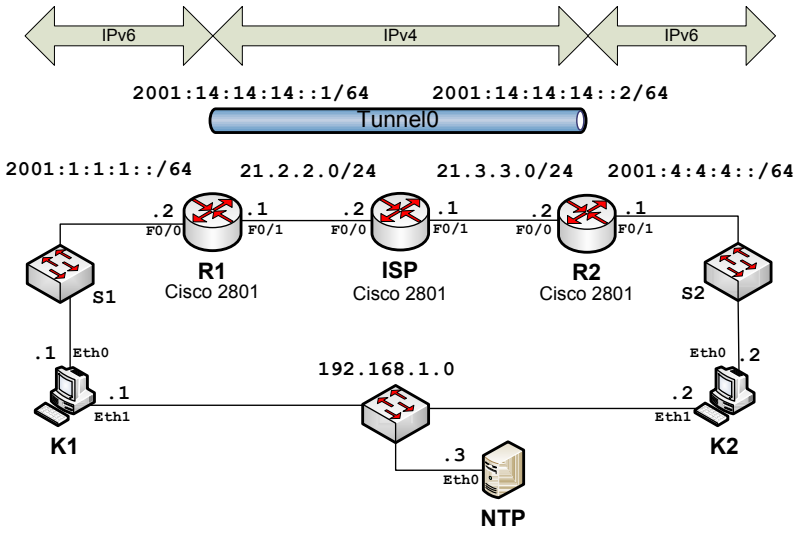
Rys. 4. Konfiguracja routera R1

```
hostname R2
ipv6 unicast-routing
interface FastEthernet0/0
 ipv6 address 2001:3:3:3::2/64
!
interface FastEthernet0/1
 ipv6 address 2001:4:4:4::1/64
ipv6 route ::/0 FastEthernet0/0 2001:3:3:3::1
```

Rys. 5. Konfiguracja routera R2

3.2. Badanie A.2 - Tunelowanie GRE

Pierwszym z rozważanych sposobów tunelowania jest tunelowanie z wykorzystaniem „ręcznie" budowanego tunelu GRE (*Generic Encapsulation Protocol*) [4], [7], [8] pomiędzy routerami granicznymi środowisk IPv6. Podstawową zaletą tunelowania GRE jest możliwość przenoszenia przez logiczny interfejs tunelowy ruchu pojedynczego (ang. *unicast*), grupowego (ang. *multicast*) i rozgłoszeniowego (ang. *broadcast*) tunelowanego protokołu. Routery graniczne, stanowiące końcowe punkty tunelu, muszą obsługiwać podwójny stos IP.



Rys. 6. Topologia dla badania tunelowania GRE

Badanie wykonano z wykorzystaniem programowego generatora ruchu *IP Traffic* oraz topologii jak na rys. 6. Rolę routerów **R1**, **ISP** i **R2** pełniły routery Cisco 2801.

Istotne elementy konfiguracji routerów **R1**, **R2** i **ISP** zostały przedstawione na rysunkach 7, 8 i 9.

```
hostname R1
ipv6 unicast-routing
interface Tunnel0
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. 7. Konfiguracja routera R1

```
hostname R2
ipv6 unicast-routing
interface Tunnel0
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. 8. 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. 9. Konfiguracja routera ISP

3.3. Badanie A3 – tunelowanie w trybie Manual Mode

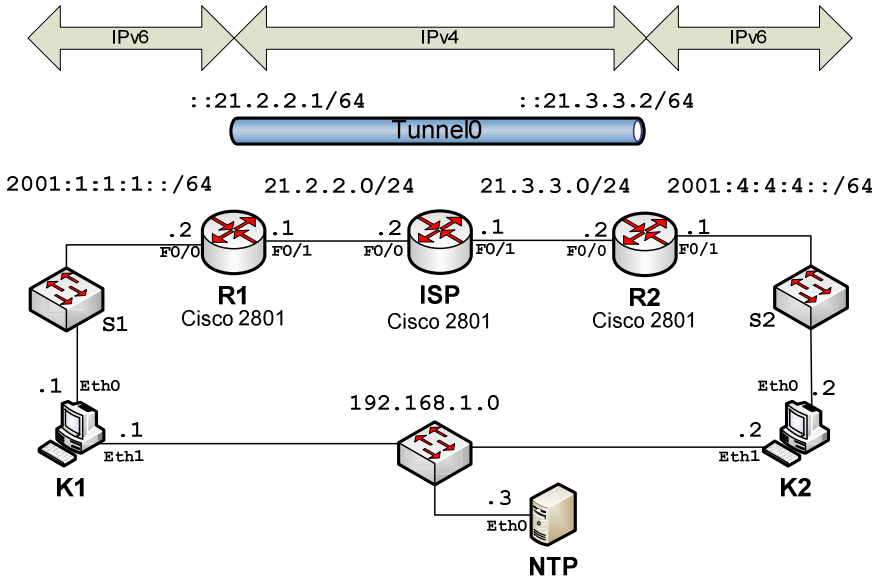
W przypadku tunelowania w tybie *Manual Mode* [14] zmianie ulega tryb pracy interfejsu Tunnel0 z ***mode gre ip*** na ***mode ipv6ip***, co zostało pokazane na rys. 10 zawierającym istotne elementy pliku konfiguracyjnego routera **R1**. Zmianie nie uległa adresacja urządzeń sieciowych,

```
hostname R1
ipv6 unicast-routing
interface Tunnel0
ipv6 address 2001:14:14:14::1/64
 tunnel source FastEthernet0/1
 tunnel destination 21.3.3.2
 tunnel mode ipv6ip
!
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. 9. Konfiguracja routera R1

3.4. Badanie A.4 - Tunelowanie w trybie *Automatic IPv4 Compatible Mode*

Automatyczny tunel 6to4 w odróżnieniu od tunelu konfigurowanego ręcznie jest tunelem typu *point-to-multipoint*. W przypadku konfigurowania tunelu tego typu, końcowy punkt tunelu nie jest jawnie definiowany, a jego adres jest automatycznie wyznaczany z adresu IPv4 interfejsu stanowiącego zakończenie tunelu i konwertowany na adres IPv6 [2] i [14]. Topologia sieci wykorzystana w badaniu jest pokazana na rys. 10.



Rys. 10. Topologia dla badania tunelowania w trybie *Automatic IPv4 Compatible Mode*

Istotne elementy konfiguracji routerów **R1**, **R2** i **ISP** zostały przedstawione na rys. 11, 12 i 13.

Do informowania o dostępności sieci IPv6 zastosowany został protokół BGP działający na routerach **R1** i **R2** (BGP peers). Omawiany tryb tunelowania wymaga zastosowania protokołu routingu z jawnym podaniem adresów IPv6 routerów-sąsiadów. W tym przypadku są to adresy IPv6 wyznaczone na podstawie adresów IPv4 interfejsów Ethernetowych routerów granicznych (odpowiednio ::21.2.2.1 dla routera **R1** i ::21.3.3.2 dla routera **R2**).

```
hostname R1
!
interface Tunnel0
 tunnel source FastEthernet0/1
 tunnel mode ipv6ip auto-tunnel
interface FastEthernet0/0
 ipv6 address 2001:1:1:1::1/64
interface FastEthernet0/1
 ip address 21.2.2.1 255.255.255.0
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor ::21.3.3.2 remote-as 100
 address-family ipv6
 neighbor ::21.3.3.2 activate
 neighbor ::21.3.3.2 next-hop-self
 bgp redistribute-internal
 network 2001:1:1:1::/64
 exit-address-family
!
ip route 0.0.0.0 0.0.0.0 21.2.2.2
```

Rys. 11. Konfiguracja routera R1

```
hostname R2
interface Tunnel0
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip auto-tunnel
!
interface FastEthernet0/1
 ipv6 address 2001:4:4:4::1/64
!
interface FastEthernet0/0
 ip address 21.3.3.2 255.255.255.0
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor ::21.2.2.1 remote-as 100
 address-family ipv6
 neighbor ::21.2.2.1 activate
 neighbor ::21.2.2.1 next-hop-self
 bgp redistribute-internal
 network 2001:4:4:4::/64
 exit-address-family
!
ip route 0.0.0.0 0.0.0.0 21.3.3.1
```

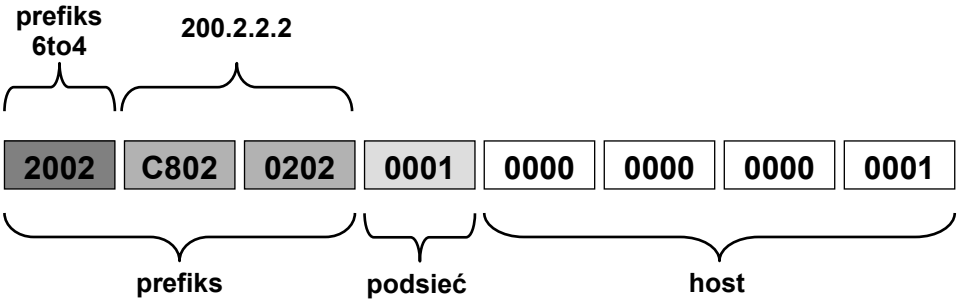
Rys. 12. Konfiguracja routera R2

```
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. 13. Konfiguracja routera ISP

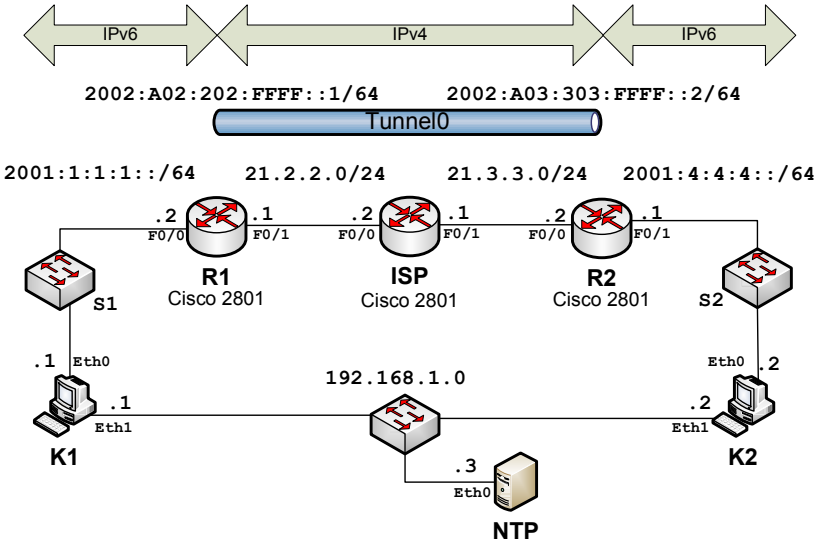
2.5. Badanie A.5 – Tunelowanie w trybie *Automatic Mode*

Tryb tunelowania *Automatic Mode* stosowany jest w przypadkach organizowania dostępu do publicznej sieci IPv6 [3] i [14]. Podobnie jak w przypadku tunelowania *Automatic IPv4 Compatible Mode* interfejs tunelowy dziedziczy adres IPv6 z interfejsu IPv4 routera. Adres ten charakteryzuje się jednak specyficznym prefiksem 2002::/16. Zasada „wplatania" adresu IPv4 w adres IPv6 interfejsu tunelowego zobrazowana została na rys. 14.



Rys. 14. Adres IPv6 z „wplecionym" adresem IPv4

Topologia sieci wykorzystana w badaniu jest pokazana na rys. 15. Istotne elementy konfiguracji routerów: **R1**, **R2** i **ISP** zostały przedstawione na rys. 16, 17 i 18.



Rys. 15. Topologia dla badania tunelowania w trybie *Automatic Mode*

```
hostname R1
interface Tunnel0
 ipv6 address 2002:A02:202:FFFF::1/64
 tunnel source Loopback0
 tunnel mode ipv6ip 6to4
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.0
 ipv6 address 2002:A02:202::1/64
!
interface FastEthernet0/0
 ipv6 address 2001:1:1:1::1/64
!
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 2001:4:4:4::/64 2002:A03:303:FFFF::2
```

Rys. 16. Konfiguracja routera R1

```
hostname R2
interface Tunnel0
 ipv6 address 2002:A03:303:FFFF::2/64
 tunnel source Loopback0
 tunnel mode ipv6ip 6to4
!
interface Loopback0
 ip address 10.3.3.3 255.255.255.0
 ipv6 address 2002:A03:303::2/64
!
interface FastEthernet0/0
 ip address 21.3.3.2 255.255.255.0
!
interface FastEthernet0/1
 ipv6 address 2001:4:4:4::1/64
!
ip route 0.0.0.0 0.0.0.0 21.3.3.1
ipv6 route 2001:1:1:1::/64 2002:A02:202:FFFF::1
ipv6 route 2002::/16 Tunnel0
```

Rys. 17. Konfiguracja routera R2

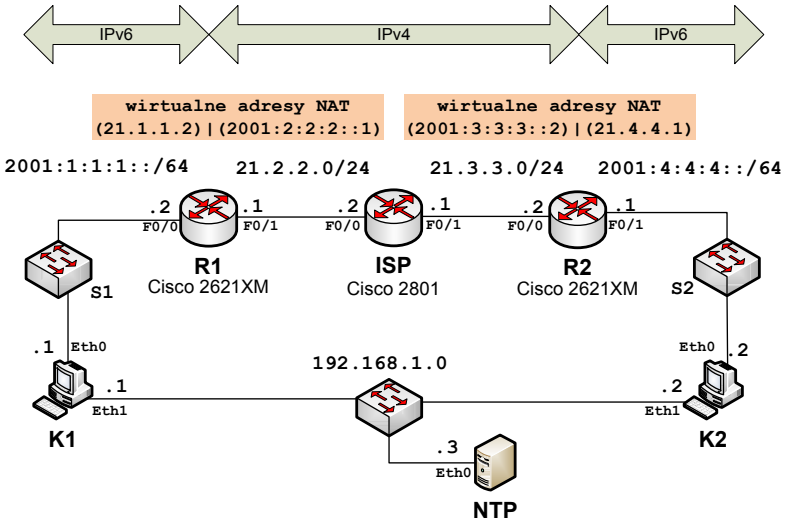
```
hostname ISP
!
interface FastEthernet0/0
 ip address 21.2.2.2 255.255.255.0
!
interface FastEthernet0/1
 ip address 21.3.3.1 255.255.255.0

ip route 10.2.2.0 255.255.255.0 21.2.2.1
ip route 10.3.3.0 255.255.255.0 21.3.3.2
```

Rys. 18. Konfiguracja routera ISP

3.6. Badanie A.6 – NAT-PT statyczny (dwukrotna translacja pomiędzy stacjami K1 i K2)

Badanie mechanizmu NAT-PT [15] wykonano w środowisku sieciowym pokazanym na rys. 19. Translacja adresów IPv6 na IPv4 i na odwrót była translacją statyczną, przeprowadzaną na routerach **R1** i **R2**.

Istotne elementy konfiguracji routerów: **R1**, **R2** i **ISP** zostały przedstawione na rysunkach 20, 21 i 22 (na szarym tle zaznaczono wirtualne adresy wykorzystywane przez mechanizm NAT-PT).



Rys. 19. Topologia dla badania mechanizmu NAT-PT

```
hostname R1
interface FastEthernet0/0
 ipv6 address 2001:1:1:1::2/64
 ipv6 nat
!
interface FastEthernet0/1
 ip address 21.2.2.1 255.255.255.0
 ipv6 nat prefix 2001:2:2:2::/96
 ipv6 nat
!
ip classless
ip route 0.0.0.0 0.0.0.0 21.2.2.2
ipv6 nat v4v6 source 21.4.4.1 2001:2:2:2::1
ipv6 nat v6v4 source 2001:1:1:1::1 21.1.1.2
```

Rys. 20. Konfiguracja routera R1

```
hostname R2
interface FastEthernet0/0
 ip address 21.3.3.2 255.255.255.0
 ipv6 nat prefix 2001:3:3:3::/96
 ipv6 nat
!
interface FastEthernet0/1
 no ip address
 ipv6 address 2001:4:4:4::1/64
 ipv6 nat
!
ip classless
ip route 0.0.0.0 0.0.0.0 21.3.3.1
ipv6 nat v4v6 source 21.1.1.2 2001:3:3:3::2
ipv6 nat v6v4 source 2001:4:4:4::2 21.4.4.1
```

Rys. 21. Konfiguracja routera R2

```
hostname ISP
!
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

ip route 21.1.1.0 255.255.255.0 21.2.2.1
ip route 21.4.4.0 255.255.255.0 21.3.3.2
```

Rys. 22. Konfiguracja routera ISP

4. Analiza wyników przeprowadzonych badań

Zestawienie wyników przeprowadzonych badań zostało przedstawione w tab. 4.

Tab. 4. Wyniki badań mechanizmów transportowania pakietów IPv6 przez środowisko IPv4 z uwzględnieniem ocen eksperckich

nazwa pomiaru		p [Mbps]	up		op [ms]	fl	cpu [%]	ocena wydajności O_{wyd}	ocena ekspercka		ocena końcowa
			liczba utraconych	liczba wysłanych					ocena	max	
współczynniki wagowe		4	2		2	4	1	80	20		X
A.1	(s)	57,1	0	581578	0	0	56	13	X	X	X
brak tunelowania	(r)	56,7	0	243026	0	0	27	13	X	X	X
	(bf)	58,5	0	163922	0	0	20	13	X	X	X
A.2	(s)	49,1	2	274061	0	0	43	5,342	40	40	52,9
GRE	(r)	52	0	229393	0	0	39	5,142	40	40	51,6
	(bf)	67,1	0	358922	0	0	60	5,962	40	40	56,7
A.3	(s)	49,6	2	279320	0	0	42	5,408	35	40	50,8
Manual Mode	(r)	54,8	0	235853	0	0	40	5,344	35	40	50,4
	(bf)	66,8	0	364172	0	0	58	5,960	35	40	54,2
A.4	(s)	48,5	0	600431	0	0	73	4,971	50	50	50,6
Automatic IPv4 Compatible Mode	(r)	51,4	0	238552	0	0	39	5,115	50	50	51,5
	(bf)	56,1	0	157151	0	0	28	5,342	50	50	52,9
A.5	(s)	48,8	0	265279	0	0	40	5,510	45	50	51,9
Automatic Mode	(r)	51,5	0	238271	0	0	36	5,179	45	50	49,9
	(bf)	54,9	0	154823	0	0	28	5,257	45	50	50,4
A.6	(s)	3,72	0	15955	7	1	63	1,159	21	40	17,6
NAT-PT	(r)	3,27	0	17287	8	0	63	1,074	21	40	17,1
	(bf)	4,74	0	13316	5	1	59	0,684	21	40	14,7

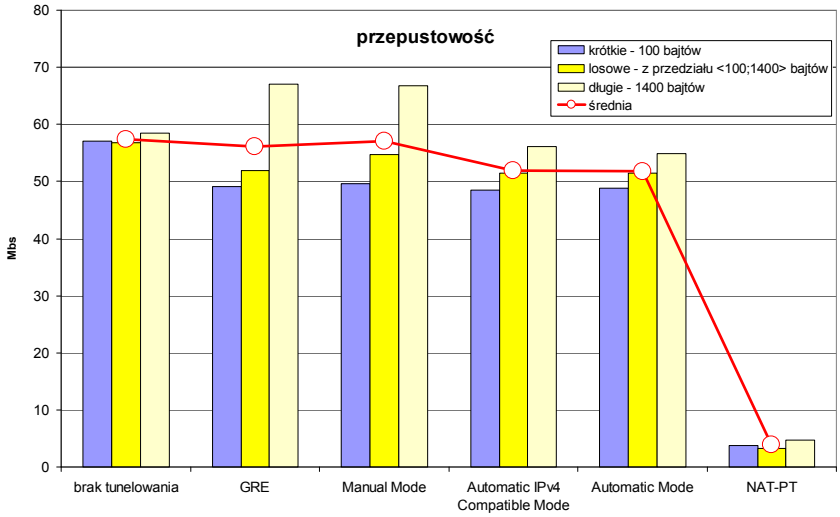
W tab. 4 zostały zastosowane następujące oznaczenia:

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

W trakcie prowadzonych badań mechanizmów przejściowych nie odnotowano drastycznych spadków (w stosunku do poziomu bazowego) przepustowości sieci, w której wykorzystywane są mechanizmy przejściowe. Odstępstwo od reguły stanowi przypadek NAT-PT, co związane jest z długim czasem przełączania pakietów przy zastosowaniu tej formy translacji.

Wykres ilustrujący uzyskane w badaniach wyniki przepustowości sieci przedstawiony został na rys. 23.

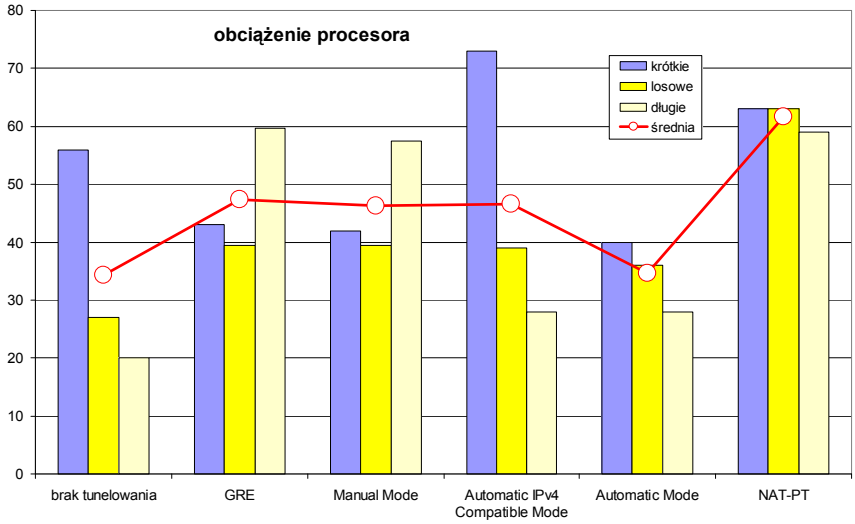
Badania wykazały również, że translacja NAT-PT w znacznie większym od pozostałych przypadków stopniu obciąża procesor urządzenia dokonującego translacji. Zestawianie tuneli nie stanowi znacznego obciążenia dla routera. Jedynie dla krótkich pakietów IP w przypadku tunelowania w trybie *Automatic IPv4 Compatible Mode* odnotowano znaczne obciążenie CPU, co może świadczyć o częstszej realizacji procedury wyznaczania adresu końcowego punktu tunelu.



Rys. 23. Przepustowość sieci w zależności od zastosowanego mechanizmu integracji[12]

Wartości obciążenia procesora routera tunelującego i dokonującego translacji NAT-PT przedstawione zostały na rys. 24.

[12] Badania wykonano dla ruchu pakietów: o małej długości 100 bajtów (krótkie), o losowej długości z przedziału <100;1400> bajtów (losowe), o dużej długości 1400 bajtów (długie)



Rys. 24. Obciążenie procesora routera w zależności od zastosowanego mechanizmu integracji

Ocena wydajności O_{wyd} jest oceną złożoną[13], wyznaczoną według następującej formuły:

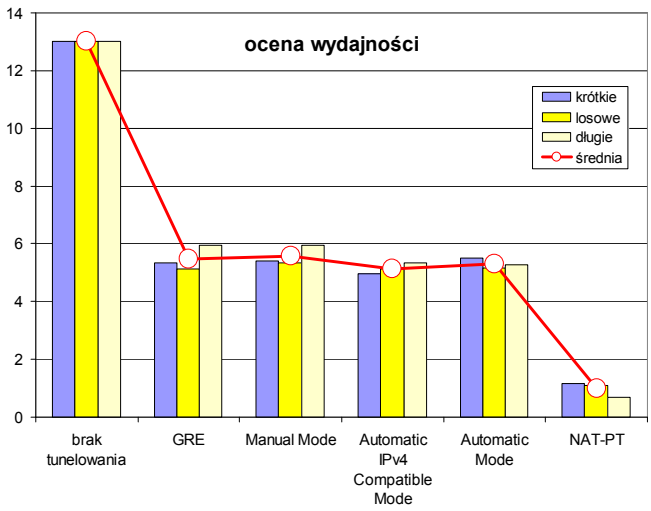
$$O_{wyd} = a\frac{p}{p_b} + b\frac{up_b}{up} + c\frac{op_b}{op} + d\frac{fl_b}{fl} + e\frac{cpu_b}{cpu} \tag{1}$$

gdzie: p_b, p – przepustowość bazowa i w badanym rozwiązaniu;
up_b, up – utrata pakietów bazowa i w badanym rozwiązaniu;
op_b, op – średnie opóźnienie pakietów bazowe i w badanym rozwiązaniu;
fl_b, fl – fluktuacja opóźnienia pakietów bazowa i w badanym rozwiązaniu;
cpu_b, cpu – obciążenie routerów bazowe i w badanym rozwiązaniu;
a,b,c,d,e – współczynniki wagowe poszczególnych miar.

Przyjęto założenie, że współczynniki wagowe będą miały następujące wartości: a=4, b=2, c=2, d=4, e=1.

Na rys. 25 przedstawiono wyliczoną dla każdego badanego mechanizmu ocenę wydajności O_{wyd}.

[13] Szczegółowe omówienie sposobu wyznaczania O_{wyd} można znaleźć w [11].



Rys. 25. Ocena wydajności łącza w zależności od zastosowanego mechanizmu integracji

Jak widać, najwyższe oceny wydajności uzyskało tunelowanie GRE i tunelowanie w trybie *Manual Mode*. O ile wszystkie sposoby tunelowania dla pakietów krótkich charakteryzują się podobną oceną wydajności, to dla pakietów o długości 1400 bajtów (pakiety długie) wyraźnie zaznacza się dominacja tunelowania GRE i tunelowania w trybie *Manual Mode*.

Wyniki uzyskane w eksperymentach ze statycznym mechanizmem NAT-PT kształtowały się na poziomie 10-12% przepustowości w stosunku do mechanizmów tunelowania.

Na podstawie przeprowadzonych badań wydajności oraz oceny eksperckiej wyznaczona została zgodnie z metodyką ocena końcowa (O_{kon}) mechanizmów transportu pakietów IPv6 przez środowisko IPv4, według następującej formuły.

$$O_{kon} = w \cdot \frac{O_{wyd}}{O_{baz}} + (100 - w) \cdot O_{\exp} \tag{2}$$

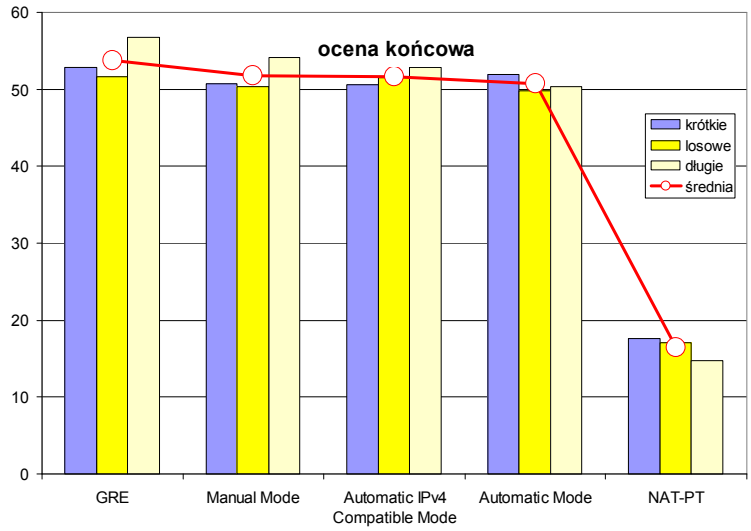
gdzie: w – współczynnik wagowy oceny wydajności O_{wyd} badanego mechanizmu równy 80;

O_{wyd} – ocena badanego mechanizmu z punktu widzenia wydajności sieci;

O_{baz} – ocena bazowego mechanizmu z punktu widzenia wydajności sieci;

O_{exp} – ocena ekspercka mechanizmu.

Wartości oceny końcowej dla badanych mechanizmów zobrazowane zostały na rys. 26.



Rys. 26. Ocena końcowa mechanizmów transportu pakietów IPv6 w środowisku IPv4

Najwyższą ocenę końcową uzyskało tunelowanie GRE. Pozostałe sposoby tunelowania mają ocenę nieco gorszą, ale porównywalną, a zdecydowanie odbiegającą ocenę uzyskało rozwiązanie wykorzystujące NAT-PT.

5. Podsumowanie

W artykule przedstawione zostały wyniki badań najczęściej wykorzystywanych metod transportowania pakietów IPv6 przez sieć z protokołem IPv4. Szczególnie interesujący przypadek użytecznego tunelowania *point-to-multipoint* (GRE w sieci Frame Relay) nie był szczegółowo badany ze względu na dynamiczny charakter tuneli oraz brak dostępu do systemu IOS z protokołem NHRP (*Next Hop Resolution Protocol*) [12].

Wyniki badań pozwalają przypuszczać, że stosowany od dawna protokół GRE (również przy tunelowaniu w jednorodnym środowisku IPv4 lub IPv6) znajdzie zastosowanie w sieciach heterogenicznych, gdzie łączone są ze sobą sieci IPv6 poprzez środowisko IPv4.

Tunele bazujące na protokole GRE posiadają istotną cechę przenoszenia ruchu multicastowego (bardzo cenna właściwość w przy konieczności wykorzystania protokołu routingu dynamicznego przez interfejs tunelu), który może być ponadto zaszyfrowany, 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 enkapsulujący router wartości pola *Type of Service* nagłówka pakietu IPv4 do pola *Traffic Class* nagłówka IPv6 pakietu GRE.

Uzyskane wyniki potwierdziły pogląd, że NAT-PT charakteryzuje się niską wydajnością w porównaniu z wydajnością technik tunelowania.

Wykonane eksperymenty potwierdziły przypuszczenie, że jednoznaczne wskazanie na najlepsze rozwiązanie będzie trudne. Różnice wartości oceny końcowej dla różnych form tunelowania są nieznaczne. Jednak biorąc pod uwagę opisane dodatkowe właściwości, rekomendowanym 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, 2007.

[2] BRISCOE B., *Tunneling of Explicit Congestion Notification*, RFC 6040, 2010.

[3] CARPENTER B., MOORE K., *Connection of IPv6 Domains via IPv4 Clouds*, RFC 3056, February 2001.

[4] CONTA A., DEERING S., *Generic Packet Tunneling in IPv6 Specification*, RFC 2473, December 1998.

[5] CRAWFORD M., *Transmission of IPv6 Packets over Ethernet Networks* RFC 2464, 1998.

[6] DEERING S., HINDEN R., *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

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

[8] FARINACCI D., LI T., HANKS S., MEYER D., TRAINA P., *Generic Routing Encapsulation (GRE)*, RFC 2784, March 2000.

[9] FURTAK J., *Metody integracji sieci IPv4 i IPv6*, Biuletyn IAiR, nr 29, Warszawa, 2010, str. 39 – 58.

[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., ŚWIERCZYŃSKI Z., MALINOWSKI T., *Metodyka oceny mechanizmów integracji sieci IPv4 i IPv6*, Biuletyn IAiR, nr 29, Warszawa, 2010, str. 59 – 72.

[12] FURTAK J., ŚWIERCZYŃSKI Z., RENCZEWSKI K., *Badania porównawcze mechanizmów transportowania pakietów IPv4 przez środowisko IPv6*, Biuletyn IAiR, nr 30/2011, str. 55 – 70.

[13] HANKS S., Li T., FARINACCI D., TRAINA P., *Generic Routing Encapsulation over IPv4 networks*, RFC 1702, 1994.

[14] NORDMARK E., GILLIGAN R., *Basic Transition Mechanisms for IPv6 Hosts and Routers*, RFC 4213, 2005.

[15] TSIRTSIS G., SRISURESH P., *Network Address Translation - Protocol Translation (NAT-PT)*, RFC 2766, 2000.

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

ABSTRACT: The paper presents results of comparison of mechanisms for transmission of IPv6 packets over IPv4 infrastructure. These results combined with a subjective expert assessment of the considered mechanism allow to indicate a preferred mode of transporting packets.

KEYWORDS: IPv4, IPv6, NAT-PT translation, tunneling

Praca wpłynęła do redakcji: 04.05.2011