BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 29, 2010

Metodyka oceny mechanizmów integracji sieci IPv4 i IPv6[1]

Janusz FURTAK, Zbigniew ŚWIERCZYŃSKI, Tomasz MALINOWSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
jfurtak@wat.edu.pl, zswierczynski@ita.wat.edu.pl, tmalinowski@ita.wat.edu.pl

STRESZCZENIE: W artykule przedstawiono metodykę oceny mechanizmów integracji sieci IPv4 i IPv6 dla przypadków: „wyspy IPv6" podłączone przez środowisko IPv4 i „wyspy IPv4" podłączone przez środowisko IPv6. Ocena poszczególnych mechanizmów jest oceną względną w stosunku do rozwiązania bazowego (odpowiednio środowisko tylko-IPv6 i tylko-IPv4) i obejmuje: ocenę wydajności mechanizmu integracji uwzględniającą przepustowość, utracone pakiety, opóźnienie i fluktuacje opóźnienia oraz parametry niemierzalne takie jak: łatwość konfiguracji i diagnozowania mechanizmu, możliwość automatyzacji konfigurowania, adaptacji do zmian i ograniczenia stosowania mechanizmu.

SŁOWA KLUCZOWE: sieci IPv6, integracja sieci IPv4 i IPv6, wydajność sieci

1. Wprowadzenie

Od początku lat dziewięćdziesiątych XX w. trwają prace nad opracowaniem zasad funkcjonowania i implementacji protokołu IPv6 [5], [7]. Przy projektowaniu rozwiązań dla tego protokołu umożliwiających integrację użytkowanego od kilkudziesięciu lat protokołu IPv4 z protokołem IPv6 zakładano, że protokół IPv6 zachowa wsteczną kompatybilność z IPv4, konwersja z IPv4 do IPv6 będzie trwała długo oraz będzie występowała

[1] Metodykę opracowano na potrzeby badań realizowanych w ramach projektu PBR-MNiSW-O R00 0024 06 pt. *Metoda gwarantowania jakości usług w taktycznym systemie łączności wykorzystującym technikę sieciową IPv6 i integracji systemów bazujących na IPv4* [10], [12].

konieczność współistnienia sieci wykorzystujących IPv4 i sieci wykorzystujących IPv6 [5], [14]. Do tej pory stworzono szereg opracowań normujących poszczególne aspekty działania protokołu IPv6 w postaci licznych dokumentów RFC (obecnie jest dostępnych ponad sto dokumentów tego typu).

Ze względu na to, że aktualnie istniejąca sieć Internet w znakomitej większości przypadków wykorzystuje protokół IPv4, opracowanie mechanizmów umożliwiających integrację „wysp IPv6" poprzez infrastrukturę sieciową wykorzystującą protokół IPv4 wydawało się naturalnym podejściem. Za potwierdzenie tego faktu można uznać opracowanie dosyć licznych mechanizmów umożliwiających integrację sieci IPv6 poprzez infrastrukturę IPv4. Należą do nich:

- tunelowanie w trybie *Manual Mode* [13], [17];
- tunelowanie GRE [8],[9];
- tunelowanie w trybie *Automatic IPv4 Compatible Mode* [13], [17];
- tunelowanie w trybie *Automatic Mode* [2];
- tunelowanie *Teredo* [15], [20];
- tunelowanie ISATAP [19];
- NAT-PT statyczny i dynamiczny [1], [21].

Natomiast rozwiązania mające na celu integrację „wysp IPv4" poprzez środowisko IPv6 są mniej liczne. Należą do nich:

- tunelowanie GRE;
- tunelowanie w trybie *Generic Packet Tunneling* [4];
- NAT-PT statyczny i dynamiczny.

Pozornie wydaje się, że integracja „wysp IPv4" poprzez środowisko IPv6 będzie wykorzystywana dużo rzadziej, ale na przykład w zastosowaniach wojskowych zwykle buduje się niezależną od sieci Internet infrastrukturę sieciową coraz częściej z wykorzystaniem urządzeń oferujących protokół IPv6. Ta infrastruktura wykorzystywana jest przez systemy dowodzenia użytkujące tylko protokół IPv4. Tego typu scenariusz może spowodować, że mechanizmy integracji „wysp IPv4" poprzez infrastrukturę IPv6 będą bardzo często stosowane.

Pomimo tego, że wymienione wyżej mechanizmy integracji są dosyć liczne, nie wyczerpują wszystkich możliwości integracji sieci IPv4 i IPv6[2]. Pojawia się pytanie, który mechanizm i w jakich okolicznościach należy wskazać jako najlepszy. Tak sformułowane zadanie nie jest proste. Do jego rozwiązania zaproponowano metodykę oceny mechanizmów integracji sieci IPv4 i IPv6 przedstawioną w kolejnym rozdziale.

[2] Metody integracji sieci IPv4 i IPv6 bardziej szczegółowo przedstawione są w [10].

2. Opis metodyki oceny mechanizmów integracji sieci IPv4 i IPv6

Do oceny poszczególnych rozwiązań przeznaczonych do integracji sieci IPv4 i IPv6 można wykorzystać miary, które będą określały przydatność badanych mechanizmów w konkretnych zastosowaniach [3], [17]. Przy określeniu miary przewidziano uwzględnienie następujących elementów:

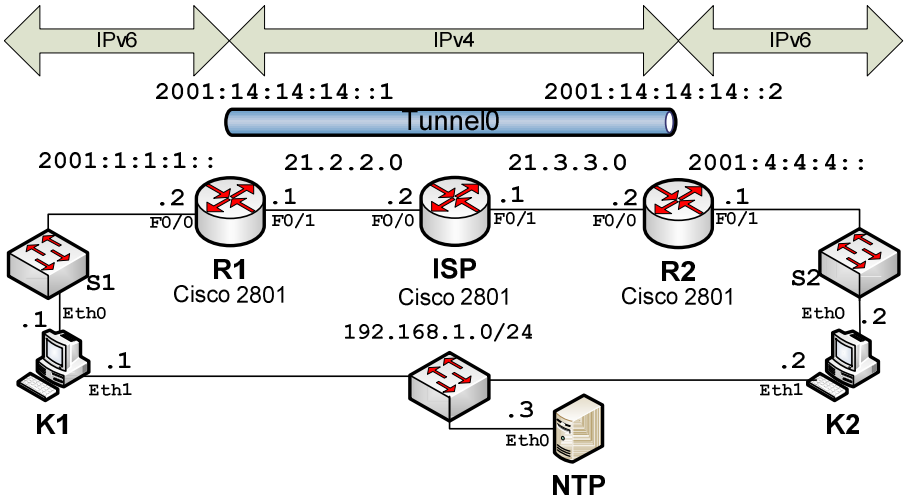
1. Wydajność sieci zestawionej z wykorzystaniem danego mechanizmu (parametry mierzalne przy pomocy generatora ruchu).
2. Inne właściwości mechanizmu:
   a) łatwość konfiguracji badanego mechanizmu;
   b) minimalna liczba elementów konfiguracyjnych niezbędnych do uruchomienia mechanizmu, np. routery z odpowiednim oprogramowaniem, dodatkowe serwery (np. DNS);
   c) łatwość diagnozowania danego mechanizmu;
   d) możliwość automatyzacji pewnych czynności związanych z uruchomieniem mechanizmu;
   e) możliwość automatycznej adaptacji skonfigurowanego mechanizmu do zmian konfiguracji sieci;
   f) ograniczenia przy stosowaniu danego rozwiązania.

2.1. Wydajność mechanizmu integracji sieci IPv4 i IPv6

Do wykonania pomiarów przygotowano stanowisko pomiarowe. Topologia sieci wykorzystywanej na stanowisku z przykładowymi parametrami konfiguracyjnymi jest pokazana na rys. 1. W pokazanej sieci źródłem danych jest komputer **K1**, a odbiorcą komputer **K2**. Badany mechanizm był skonfigurowany pomiędzy routerami **R1** i **R2**. Jako kanał transmisyjny traktowano trasę **K1→S1→R1→ISP→R2→S2→K2.**

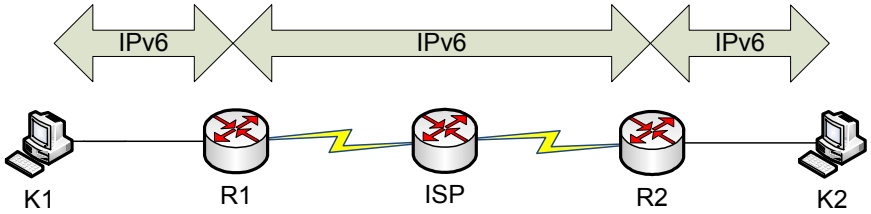
Wydajność mechanizmu integracji jest oceną złożoną, w której uwzględnione będą oceny następujących elementów:

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

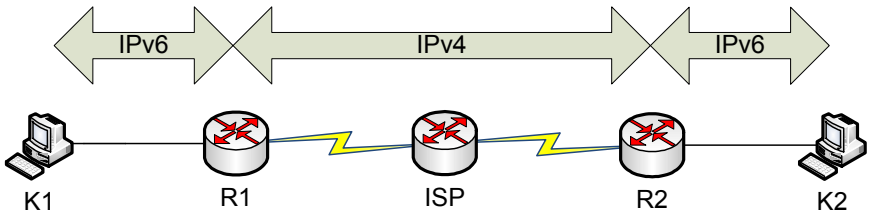


Rys. 1. Stanowisko do badania tunelowania pakietów IPv6 przez środowisko IPv4

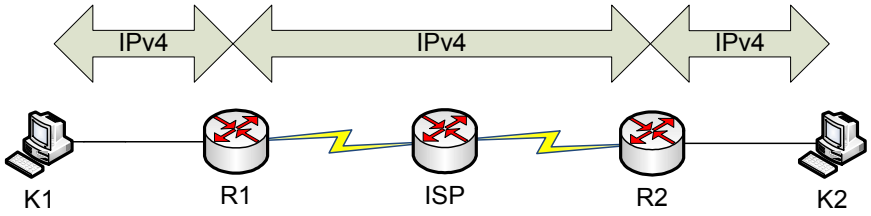
Ocena powyższych parametrów jest oceną względną w stosunku do rozwiązania bazowego. Założono, że pomiary wymienionych parametrów najpierw będą wykonane w środowisku tylko-IPv6 (rys. 2) i tylko-IPv4 (rys. 4). Pomiary uzyskane w tych badaniach będą przyjęte jako pomiary rozwiązania bazowego i w stosunku do niego będą porównywane te same parametry uzyskane przy badaniu poszczególnych rozwiązań. Rozwiązaniem bazowym dla badań przypadku „wysp IPv6" połączonych przez środowisko IPv4 (wariant A) jest środowisko tylko-IPv6 (rys. 3), a dla przypadku „wysp IPv4" połączonych przez środowisko IPv6 (wariant B) jest środowisko tylko-IPv4 (rys. 5). W efekcie uzyskana będzie ocena wydajności poszczególnych rozwiązań w stosunku do środowiska odpowiednio tylko-IPv6 i tylko-IPv4.



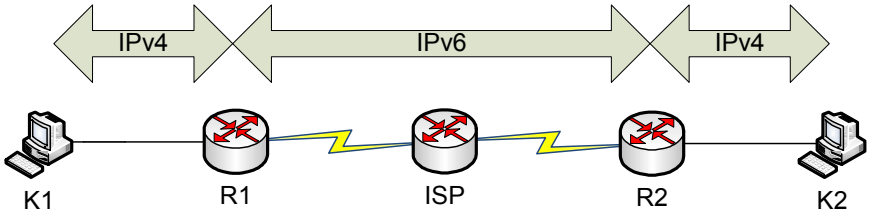
Rys. 2. Środowisko tylko-IPv6 (bazowe dla wariantu A)



Rys. 3. „Wyspy IPv6" połączone przez środowisko IPv4 (wariant A)



Rys. 4. Środowisko tylko-IPv4 (bazowe dla wariantu B)



Rys. 5. „Wyspy IPv4" połączone przez środowisko IPv6 (wariant B)

Wymienione pomiary zostaną przeprowadzone dla różnej wielkości pakietów w przypadku posiadania na wyłączność kanału transmisyjnego. Zdecydowano, że kolejne warianty z tym związane będą następujące:

- transmisja małych pakietów – rozmiar 100 bajtów z nagłówkiem;
- transmisja pakietów o rozmiarze[3] z zakresu <64;1400>;
- transmisja pakietów o rozmiarze nieco mniejszym od progu fragmentacji.

[3] W generowanym ruchu nie wymuszano transmisji pakietów o wielkości przekraczającej próg fragmentacji, z tego względu, że nawet gdy wymuszono taką długość pakietów u źródła, to mechanizmy protokołu TCP dostosowywały rozmiar pakietu do maksymalnej wartości MTU na łączu.

Istotnym parametrem badań jest czas obserwacji ruchu w sieci. Na potrzeby opisywanych badań przyjęto, że czas trwania pomiarów ***T*** do wyznaczenia miar oceny wydajności sieci będzie wynosił 30 sekund[4].

Do wykonania pomiarów zostanie wykorzystany 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. Przykładowa topologia sieci wykorzystanej w badaniach jest pokazana na rys. 5.

Przepustowość

Przepustowość (*ang. throughput*) jest tutaj rozumiana jako maksymalna przepływność kanału transmisyjnego i jest liczona jako liczba bitów przesłana przez łącze w jednostce czasu. Przy obliczaniu liczby bitów powinny być uwzględniane całe pakiety, to znaczy zawartość nagłówków i pól danych. Przepustowość p będzie obliczania według poniższej formuły:

$$p = \frac{1}{T}\sum_{i=1}^{n} M_i \,, \tag{1}$$

gdzie: n – liczba pakietów;

T – czas trwania eksperymentu;

M_i – rozmiar pakietu ze wszystkimi nagłówkami w bitach.

Utracone pakiety

W przypadku parametru „utracone pakiety" problemem jest ustalenie kryterium czasowego, po przekroczeniu którego pakiet jest traktowany jako utracony. Fakt utraty pakietów w transmisji z wykorzystaniem protokołów połączeniowych, np. TCP, nie jest istotny, gdyż takie protokoły wymuszają powtórzenie transmisji. Utrata pakietów istotna jest dla transmisji z wykorzystaniem protokołów bezpołączeniowych, np. UDP, a szczególnie transmisji danych multimedialnych. Kryterium utraty pakietu w takim przypadku jest uzależnione od rodzaju aplikacji wykorzystującej tę transmisję. Na przykład dla aplikacji multimedialnych według zalecenia ITU-T G.114 [16] jako graniczną akceptowalną wartość opóźnienia przyjmuje się 150 ms. Wartość opóźnienia 150-250 ms poważnie wpływa na jakość transmisji, 250-400 ms przeszkadza w odbiorze, a opóźnienie większe niż 400 ms jest nieakceptowane. W takim przypadku jako kryterium „utraty pakietu" można przyjąć 400 ms.

[4] W przyjętym czasie 30 sekund zależnie od rodzaju badanego mechanizmu generator ruchu był w stanie wysłać od 15000 do 270000 ramek.

W badaniach mechanizmów integracji IPv4 i IPv6 jednak nie brano pod uwagę wspomnianych zagadnień, a za utracony uznawano ten pakiet, który w oknie czasowym eksperymentu został wysłany przez nadawcę, a nie dotarł do odbiorcy. Jako miarę oceny utraty pakietów przyjęto następujący wskaźnik:

$$up = \frac{lup + \varepsilon_{up}}{n} \quad , \tag{2}$$

gdzie: *lup* – liczba utraconych pakietów;

ε_{up} – stała o wartości 0,01 dodana w celu uniknięcia dzielenia przez zero w końcowej formule w przypadku zerowej wartości *lup*;

n – liczba wysłanych pakietów.

Fakt utraty pakietu w trakcie transmisji uniemożliwia wyznaczenie innych miar oceny transmisji np. średniego opóźnienia pakietu. Z tego względu przy wyznaczaniu pozostałych miar brano pod uwagę parametry tych pakietów, które dotarły do celu.

Opóźnienie

Opóźnienie (ang. *latency*) to czas, jaki jest potrzebny pakietowi do osiągnięcia celu i jest obliczany jako różnica czasu pomiędzy chwilą wysłania pakietu a chwilą jego odebrania [6]. W ogólnym przypadku na czas opóźnienia składają się:

- opóźnienie propagacji związane z potrzebą pokonania przez sygnał dystansu od nadawcy do odbiorcy (jest zależne od rodzaju i długości medium);
- opóźnienie obsługi (przetwarzania) związane z przetwarzaniem pakietu na trasie pomiędzy nadawcą a odbiorcą (kapsułkowanie pakietów, routowanie pakietów, kolejkowanie pakietów itp.);
- opóźnienie serializacji określające ilość czasu potrzebną do umieszczenia bitów w łączu – jest zależne od rozmiaru pakietu.

Ze względu na charakter i warunki badań opóźnienie propagacji w eksperymentach było stałe, bo rozległość badanych sieci była nieduża i stała. Opóźnienie serializacji nie miało istotnego wpływu na wyniki, ale fakt generowania w sieci w różnych eksperymentach ruchu obejmującego różną długość ramek pozwala ocenić wpływ tego elementu. Najistotniejszym elementem opóźnienia było opóźnienie obsługi, które było zależne od wybranej do badania metody integracji systemu IPv6 i IPv4. Do oceny opóźnienia w badaniach obliczano średnie opóźnienie na podstawie następującej formuły[5]:

[5] Jeżeli średnie opóźnienie przekroczy 400 ms, to zgodnie z zaleceniami ITU-T G.114 takie rozwiązanie można odrzucić (jako nienadające się do wykorzystania w sieciach przesyłających dane multimedialne).

$$op = \frac{1}{n}\sum_{i=1}^{n}\left(R_i - S_i\right), \tag{3}$$

gdzie: n – liczba pakietów;

S_i – czas wysłania i-tego pakietu;

R_i – czas odebrania i-tego pakietu.

Fluktuacja opóźnienia

Pojęcie fluktuacji opóźnienia jest bardzo obszerne [6], [17]. Na potrzeby badań przyjęto, że miarą fluktuacji opóźnienia będzie wartość średnia różnic czasów opóźnienia poszczególnych pakietów i opóźnienia średniego *op*. Miarę tę można wyznaczyć z poniższej formuły:

$$fl = \frac{1}{n}\sum_{i=1}^{n}\left(R_i - S_i - \left|op\right|\right), \tag{4}$$

gdzie: *op* – średnie opóźnienie pakietów;

n – liczba pakietów;

S_i – czas wysłania i-tego pakietu;

R_i – czas odebrania i-tego pakietu.

Obciążenie routera

Na wartość tego parametru wpływ ma obciążenie procesora w trakcie obsługi tuneli. Parametr ten będzie mierzony na routerach, które są początkiem tunelu. Obciążenie procesorów routerów, które były końcem tunelu, nigdy nie przekraczało obciążenia procesorów routerów, które były początkiem tunelu. Dlatego do oceny łącza uwzględniono tylko obciążenie procesora routera na początku tunelu.

Ocena wydajności

Na początku każdego eksperymentu wyznaczano wartości wyżej opisanych miar dla rozwiązania bazowego (dalej do oznaczenia tych miar będzie wykorzystany indeks „b"). Rozwiązaniem bazowym dla badań wariantu A (tzn. wyspy IPv6 połączone przez środowisko IPv4) było środowisko tylko-IPv6, a dla wariantu B (tzn. wyspy IPv4 połączone przez środowisko IPv6) było środowisko tylko-IPv4. Następnie wyznaczono wartości wyżej opisanych miar dla kolejnego badanego rozwiązania umożliwiającego integrację sieci IPv4 z siecią IPv6.

Jako ocenę badanego rozwiązania O_{wyd} przyjęto ocenę wypadkową opisanych wyżej wartości parametrów obliczaną według następującej formuły:

$$O_{wyd} = a\frac{p}{p_b} + b\frac{up_b}{up} + c\frac{op_b}{op} + d\frac{fl_b}{fl} + e\frac{cpu_b}{cpu}, \quad (5)$$

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: $a = 4$, $b = 2$, $c = 2$, $d = 4$, $e = 1$.

2.2. Ocena pozostałych właściwości mechanizmu integracji

Łatwość konfigurowania

W kwestii łatwości konfigurowania danego mechanizmu brano pod uwagę liczbę elementów, które należało skonfigurować, oraz czytelność (intuicyjność) tej konfiguracji. W przypadkach konfiguracji ograniczających się do routerów porównywana była liczba komend, które należało wprowadzić w celu uruchomienia mechanizmu integracji. Ten element oceny jest zdaniem autorów badań istotny ze względu na specyfikę warunków pracy administratorów w trakcie prowadzenia działań wojennych. Bardzo istotną rolę odgrywa wtedy stres zwiększający prawdopodobieństwo popełnienia błędów oraz częste potrzeby modyfikacji konfiguracji.

Ocenę rozwiązania $O_{latkonf}$ wyznaczano na podstawie wyniku głosowania członków zespołu badawczego przy założeniach:

- zakres przydzielanych punktów: <0; 10>;
- 0 pkt – ocena najgorsza;
- 10 pkt – ocena najlepsza.

Liczba elementów do konfiguracji

Liczba elementów konfiguracyjnych potrzebnych do zaimplementowania mechanizmu odpowiada liczbie miejsc, w których może dojść do uszkodzenia mechanizmu: czy to fizycznego, czy konfiguracyjnego. Im więcej występuje elementów składowych, tym większe jest prawdopodobieństwo wystąpienia awarii. Jako pojedynczy element uważany jest np. router czy serwer DNS.

Ocenę rozwiązania obliczano według formuły:

$$O_{lel} = 10 / L_{el}, \tag{6}$$

gdzie: O_{lel} – ocena mechanizmu z punktu widzenia liczby konfigurowanych elementów;

L_{el} – liczba wymaganych elementów konfiguracji.

Łatwość diagnozowania

Łatwość diagnozowania mechanizmu integracji jest bardzo istotna w sieciach wojskowych z powodu wysokiego prawdopodobieństwa ich uszkodzenia, jak również sabotażu konfiguracyjnego. Dodatkowo czas usunięcia usterki jest nierzadko krytyczny dla działań wojskowych, a tym samym pokazuje przydatność danego mechanizmu dla tego typu zastosowań. Ten parametr jest najczęściej ściśle powiązany z poprzednim kryterium, ponieważ zależy od złożoności danego mechanizmu.

Ocenę rozwiązania $O_{latdiag}$ wyznaczano na podstawie wyniku głosowania członków zespołu badawczego przy założeniach:

- zakres przydzielanych punktów: <0; 10>;
- 0 pkt – ocena najgorsza;
- 10 pkt – ocena najlepsza.

Możliwość automatyzacji czynności konfiguracyjnych

Możliwość automatyzacji pewnych etapów konfiguracyjnych związanych z uruchomieniem mechanizmu jest istotna z punktu widzenia częstych rekonfiguracji sieci wojskowych, szczególnie na terenie działań wojennych. Automatyzacja pewnych etapów konfiguracyjnych powoduje przyspieszenie rekonfiguracji oraz minimalizuje prawdopodobieństwo popełnienia błędu przez administratorów systemów.

Ocenę rozwiązania O_{autom} wyznaczano na podstawie wyniku głosowania członków zespołu badawczego przy założeniach:

- zakres przydzielanych punktów: <0; 5>;
- 0 pkt – ocena najgorsza w przypadku braku możliwości automatyzacji czynności konfiguracyjnych;
- 5 pkt – ocena najlepsza.

Adaptacja do zmian konfiguracji sieci

Możliwość automatycznej adaptacji skonfigurowanego mechanizmu do zmian konfiguracji sieci pokazuje, na ile dany mechanizm jest odporny

na różnego typu zmiany w sieci teleinformatycznej. Zmiany te mogą być planowane lub nie i dotyczyć zarówno zmian konfiguracji programowej (np. zmiana adresu urządzenia, które terminuje koniec tunelu) lub topologii obsługiwanej sieci teleinformatycznej.

Ocenę rozwiązania O_{adapt} wyznaczano na podstawie wyniku głosowania członków zespołu badawczego przy założeniach:

- zakres przydzielanych punktów: <0; 5>;
- 0 pkt – ocena najgorsza w przypadku braku możliwości adaptacji;
- 5 pkt – ocena najlepsza.

Ograniczenia przy stosowaniu danego rozwiązania

Ostatnie kryterium dotyczyło ograniczeń, jakie są związane z wykorzystywaniem danej technologii integracji, np. konieczność posiadania rzadko spotykanej funkcji wymaganej do uruchomienia mechanizmu tunelowania czy narzucenie pewnego schematu adresacyjnego.

Ocenę rozwiązania O_{zast} wyznaczano na podstawie wyniku głosowania członków zespołu badawczego przy założeniach:

- zakres przydzielanych punktów: <0; 10>;
- 0 pkt – ocena najgorsza;
- 10 pkt – ocena najlepsza – brak ograniczeń.

2.3. Ocena końcowa

Ocenę końcową rozwiązania obliczano jako sumę ważoną ocen cząstkowych według podanej niżej formuły:

$$O_{kon} = w \cdot \frac{O_{wyd}}{O_{baz}} + (1-w) \cdot \frac{O_{latkonf} + O_{lel} + O_{latdiag} + O_{autom} + O_{adapt} + O_{zast}}{O_{\max}}, \quad (7)$$

gdzie: w – współczynnik wagowy oceny wydajności O_{wyd} badanego rozwiązania z przedziału <0;100>;

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

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

O_{latkon} – ocena badanego rozwiązania z punktu widzenia łatwości konfiguracji mechanizmu;

O_{lel} – ocena badanego rozwiązania z punktu widzenia liczby konfigurowanych elementów;

$O_{latdiag}$ – ocena badanego rozwiązania z punktu widzenia łatwości diagnozowania mechanizmu;

O_{autom} – ocena badanego rozwiązania z punktu widzenia możliwości automatyzacji czynności konfiguracyjnych;

O_{adpt} – ocena badanego rozwiązania z punktu widzenia możliwości adaptacyjnych mechanizmu do zmian konfiguracji;

O_{zast} – ocena badanego rozwiązania z punktu widzenia zastosowań mechanizmu;

O_{max} – ocena maksymalna możliwa do uzyskania z ocen $O_{latkonf}$, O_{lel}, $O_{latdiag}$, O_{autom}, O_{adpt}, O_{zast} (niektóre mechanizmy, ze względu na istotę ich działania, nie były oceniane według wszystkich wymienionych wyżej kryteriów).

3. Zakończenie

Liczba zagadnień, które można wziąć pod uwagę przy ocenie jakości rozwiązań teleinformatycznych, jest bardzo duża. W literaturze można znaleźć wiele opracowań na ten temat, na przykład dokumenty [3], [17]. Jednak opisane tam rozwiązania nie są przydatne do wyznaczenia oceny, którą można wykorzystać do wskazania najlepszego mechanizmu integracji sieci IPv4 i IPv6. Przedstawiona metodyka jest propozycją narzędzia do oceny mechanizmów integracji. Cechą charakterystyczną zaproponowanej metodyki jest uwzględnienie w ocenie parametrów mechanizmów trudno mierzalnych, które podlegały ocenie ekspertów. Stosując podaną metodykę, można również oceniać rozwiązania z pominięciem ocen ekspertów, bazując tylko na pomiarach.

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] CHADDA A., *Quality of Service Testing Methodology*, Master of Science Thesis, 2004.

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

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

[6] DEMICHELIS C., CHIMENTO P., *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*, RFC3393, 2002.

[7] DESMEULES R., *IPv6: Sieci oparte na protokole IP w wersji 6*, PWN, 2006.

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

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

[10] FURTAK J., *Metody integracji sieci IPv4 i IPv6*, Biuletyn IAiR, nr 29/2010.

[11] 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.

[12] 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.

[13] GILLIGAN R., NORDMARK E., *Transition Mechanisms for IPv6 Hosts and Routers*, RFC 2893, August 2000.

[14] HINDEN, R. DEERING S., *IP Version 6 Addressing Architecture*, RFC 4291, February 2006.

[15] HUITEMA C., *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*, RFC 4380, February 2006.

[16] *ITU-T Recommendation G.114. One-way transmission time*, INTERNATIONAL TELECOMMUNICATION UNION, Geneve 2003.

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

[18] PAXON V., ALMES G., MAHDAVI J., MATHIS M., *Framework for IP Performance Metrics*, RFC 2330, February 1998.

[19] TEMPLIN F., GLEESON T., THALER D., *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*, RFC 5214, March 2008.

[20] THALER D., KRISHNAN S., HOAGLAND J., *Teredo Security Updates*, RFC 5991, September 2010.

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

Praca naukowa finansowana ze środków na naukę w latach 2008-2010 jako projekt badawczy rozwojowy 0 R00 0024 02

An evaluation methodology for IPv4 and IPv6 networks integrated solutions

ABSTRACT: This paper considers an evaluation methodology for IPv4 and IPv6 networks integrated solutions in the following cases: IPv6 domains connected via an IPv4 environment and IPv4 domains connected via an IPv6 environment. The evaluation of a particular solution is relative to its base solution (i.e.: IPv6-only environment or IPv4-only environment) and includes: an evaluation of the integration solution performance and throughput, lost packets, latencies and fluctuations, as well as some immeasurable parameters (e.g.: configuration difficulties, diagnostics, auto-configuration possibilities, adaptation to changes, and limitations of the use).

KEYWORDS: IPv6 networks, IPv4 and IPv6 networks integration, network performance

Praca wpłynęła do redakcji: 18.12.2010