STUDIA INFORMATICA 2002
Volume 23 Number 4 (51)

Jacek KOSIŃSKI
Akademia Górniczo-Hutnicza, Katedra Informatyki

METODY I ASPEKTY MIGRACJI ŚRODOWISK IPv4 DO TECHNOLOGII IPv6

Streszczenie. Protokół IPv6 zyskuje coraz większą popularność. Większość administratorów sieci podłączonych do Internetu stanie niedługo przed koniecznością zapewnienia komunikacji z serwisami IPv6. Pojawią się też nowe wersje systemów operacyjnych wspierających protokół IPv6. Artykuł ten pokazuje,jak aplikacjom IPv6 umożliwić komunikację w istniejącym świecie IPv4 wykorzystując odpowiednie, stworzone do tego celu rozwiązania.

METHODS AND ASPECTS OF IPv4 ENVIRONMENTS MIGRATION TO IPv6 TECHNOLOGY

Summary. IPv6 protocol is being more and more popular. Most of network administrators will have to meet the requirements of enabling the communication with IPv6 services. There will also appear new versions of operating systems that support IPv6 protocol. This paper presents the possibilities of communication with IPv6 application in the existing IPv4 network.

1. Wstęp

Technologii leżącej u podstaw wszechobecnej sieci Internet używamy już od 20 lat. Oryginalnie zaprojektowany do obsługi wydzielonych sieci wojskowych w USA protokół TCP/IP bez większych modyfikacji został użyty w o wiele większej infrastrukturze. Dlaczego więc czas zmieniać technologię pracującą poprawnie bez większych zmian od tak długiego czasu? Niestety, nikt nie przewidział tak ogromnego rozwoju Internetu, a co za tym idzie – zapotrzebowania na adresy dla coraz to nowych urządzeń. Przestrzeń użyta do adresacji

węzłów w Internecie ma rozmiar 32 bitów, co pozwala na teoretyczne wykorzystanie 2^32 różnych adresów. Jednak po odliczeniu adresów na klasy adresowe i wzięcie pod uwagę nieefektywne wykorzystanie początkowo przydzielonych ogromnych klas A i B oraz dużą dynamikę rozwoju powstaje problem wyczerpywania się przestrzeni adresowej. Szacuje się, iż z wszystkich 4 bilionów praktycznie wykorzystuje się jedynie 250 milionów adresów, pozostała pula zawiera adresy niewykorzystane ze względu na podział na klasy, sieci, rezerwacje czy używane do dystrybucji multicastu.

Stosowane obecnie metody konserwacji przestrzeni adresowej, opierające się na technologii NAT [RFC 3022], dają pewne oszczędności wynikające z możliwości konfiguracji w sieciach lokalnych adresacji niepublicznej [RFC1918] i stosowania jedynie kilku lub nawet jednego adresu publicznego do obsługi całych sieci. Mechanizmy te powodują oszczędności, lecz wprowadzają równocześnie zwiększenie stopnia komplikacji konfiguracji sieci, spada wydajność rutingu, a co najważniejsze, pewne usługi takie jak VoIP czy inne o podobnym charakterze peer-to-peer, wymagające, aby każda ze stron posiadała własny adres, przestają poprawnie działać. Warto jeszcze wspomnieć o dynamicznym przydziale adresów stosowanym przy użyciu protokołów DHCP i BOOTP. Obie te metody działają poprawnie, jednak wymagają stosowania serwerów implementujących ten protokół, ponadto zwiększa się stopień komplikacji sieci. Również początkowa metoda rozdziału adresów i tworzenia tablic rutingu na podstawie klas adresowych została zastąpiona metodą CIDR (ang. ClassLess Interdomain Routing). Wielkie przestrzenie adresowe zostały przydzielone dla ISP (ang. Internet Service Provider), którzy to z kolei rozdzielają je na mniejsze sieci swoim klientom. W rezultacie globalny ruting wymaga jedynie tras do wielkich operatorów i obsługi sieci szkieletowej, co owocuje zmniejszeniem ilości wpisów w tablicy rutingu oraz bardziej efektywnym wykorzystaniem przestrzeni adresowej.

Protokół TCP/IP, jak wspomniano na początku, był projektowany dla wydzielonych sieci wojskowych o ściśle ograniczonym fizycznym dostępie, więc kwestie zapewnienia bezpieczeństwa i poufności przekazywanych nim danych zostały pominięte. Istnieją co prawda pewne nowe rozwiązania, takie jak IPsec czy HTTPS, jednak mają one bardziej charakter nakładki niż bycia obowiązującym standardem. Między innymi dlatego nie można zakładać, iż druga strona, z którą będziemy chcieli utworzyć bezpieczny kanał transmisji, implementuje któreś z istniejących rozwiązań, zazwyczaj nie implementuje żadnego.

2. IPv4 vs IPv6

Konieczność zaprojektowania nowego protokołu wynikała głównie z wyczerpywania się przestrzeni adresowej obecnego standardu, jednak nowy protokół modyfikuje również inne cechy IPv4, takie jak:

a) rozszerzenie przestrzeni adresowej,
b) uproszczenie formatu nagłówka,
c) wprowadzenie nowego mechanizmu opcji i rozszerzeń,
d) umieszczenie pola FlowLabel,
e) wsparcie dla autentykacji i enkrypcji.

Podstawowym rozszerzeniem IPv6 w stosunku do swojego poprzednika jest ogromne poszerzenie przestrzeni adresowej z 32 do 128 bitów. Wszystkich możliwych adresów jest teraz 3.4e+36, co jest niewyczerpalną przestrzenią w przewidywanej przyszłości. Nagłówek IPv4 posiada 13 pól i ma rozmiar 20 oktetów, dodatkowo rozmiar ten z dodanym polem opcji może się zwiększać, a to komplikuje i spowalnia przetwarzanie ruchu w węzłach. Nagłówek IPv6 ma stałą długość i znacznie mniej, bo tylko 8 pól (i stałą długość 40 bajtów); tylko niezbędne pola znajdują się w części podstawowej nagłówka, wszystkie pozostałe zostały umieszczone w tzw. nagłówkach dodatkowych, które są umieszczane w pakiecie tylko wówczas, gdy istnieje taka potrzeba. Ułatwia to obsługę pakietów np. przez rutery, gdyż każdy węzeł musi przetwarzać tylko nagłówek podstawowy i ewentualnie nagłówek rutingu, reszta jest pomijana i przetwarzana dopiero w hostach docelowych pakietu. Mechanizm ten jest ważny przy ewentualnych rozszerzeniach protokołu w przyszłości, które to sprowadziłyby się do dodania nowego formatu subnagłówka. Zdefiniowane zostały również w standardzie nagłówki umożliwiające stosowanie różnych metod autentykacji lub enkrypcji danych przenoszonych przez pakiet.

3. Możliwe warianty przejścia na IPv6

Po podjęciu decyzji o zmianie istniejącego rozwiązania na nowe warto też pomyśleć o odpowiednim zaplanowaniu całej operacji. Konieczność zmiany może stanowić nie lada problem dla dużych organizacji, a w skali światowej problem dotyka każdego systemu używającego IP, czyli około 100 milionów urządzeń rozsianych po całym świecie. Jeśli do tego wszystkiego doliczymy niezliczone wersje stosów TCP/IP, systemów operacyjnych czy platform sprzętowych, to okaże się, że stoimy przed bardzo poważnym wyzwaniem. Przejście na IPv6 będzie się zatem odbywać stopniowo. Przez pewien okres czasu zarówno urządzenia

używające starego protokołu IPv4, jak i nowego IPv6 będą koegzystować w Internecie. W miarę pojawiania się coraz większej liczby węzłów IPv6 będzie pojawiać się konieczność zapewnienia możliwości współpracy z istniejącym światem IPv4, w którym po pierwsze nie wszystkie serwery obsługują ruch IPv6, jak i nie wszystkie rutery umieją taki ruch przetwarzać. Współpraca ta może być osiągnięta na kilka sposobów.

3.1. Tunelowanie

Tunelowanie zapewnia możliwość komunikacji sieci IPv6 poprzez istniejącą infrastrukturę IPv4. Jest to mechanizm często stosowany obecnie, w czasie gdy większość ruterów rdzeniowych Internetu (ang. core routers) nie wspiera jeszcze rutingu ruchu IPv6 i istnieje potrzeba połączenia ze sobą coraz to nowych sieci IPv6 LAN w globalną infrastrukturę. Eksperymentalna, globalna sieć 6BONE powstała dzięki połączeniu siatką tuneli, enkapsulujących w ruchu IPv4 datagramów IPv6, dużej liczby rozproszonych sieci, w których jest stosowany protokół IPv6.

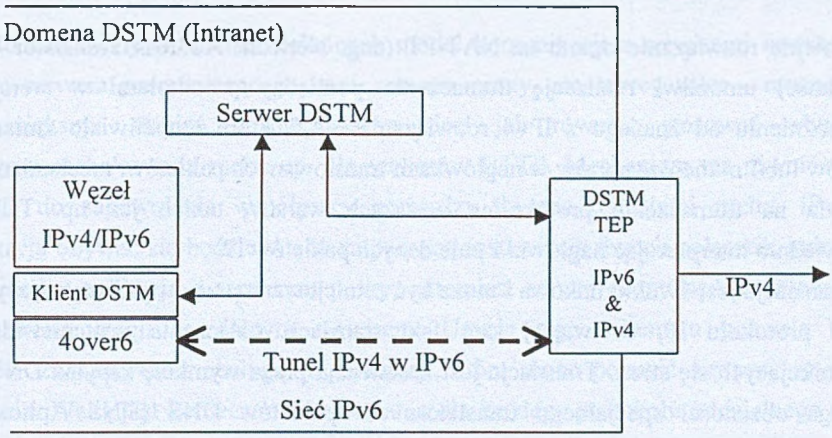
Rozróżniamy dwa podstawowe typy tuneli: statyczne – konfigurowane przez administratora pomiędzy dwoma ruterami IPv6 i dynamiczne - zestawiane automatycznie na żądanie aplikacji. Wszystkie obecne implementacje ruterów IPv6 (np. Cisco, Ericsson, 6WIND czy Telebit) pozwalają na konfigurację statycznych tuneli. Natomiast tunele dynamiczne pozwalają na automatyczną realizację połączeń pomiędzy węzłami IPv6. Istnieje kilka mechanizmów zestawiania dynamicznych tuneli zaproponowanych przez IETF. Do głównych możemy zaliczyć 6to4, 6over4 i tunell broker.

Problemem pojawiającym się przy stosowaniu enkapsulacji może okazać się zapewnienie pewnych właściwości ruchu przekazywanego przez tunel. Problem głównie dotyczy parametrów QoS, gdyż gwarantowanie jakości obsługi przy połączeniu IPv6 może nie być możliwe do zapewnienia, jeśli połączenie to będzie przekazywane wewnątrz strumienia IPv4, który nie pozwala wpływać na QoS. Warto zwrócić również uwagę na bezpieczeństwo sieci z skonfigurowanymi tunelami, które pozwalają na obejście naszych zapór ogniowych. Nie zawsze oprogramowanie firewalla pozwala na sprawdzanie i filtracje ruchu enkapsulowanego. Pojawia się też narzut na przenoszony ruch związany z koniecznością dodania drugiego nagłówka.

Większość z tych problemów można uniknąć zachowując podobną funkcjonalność przez zastosowanie technologii transportowej obsługującej koncepcje wirtualnych kanałów, takich jak ATM czy FrameRelay. Zestawianie takich kanałów pomiędzy odległymi lokalizacjami pozwoli na stosowanie native-ipv6.

3.2. Mechanizm Dual Stack

Kolejną metodą zapewnienia łączności jest stworzenie tzw. sieci dual stack, zawierających węzły posiadające zarówno implementacje protokołu IPv4, jak i nowego IPv6. Komputery i rutery mogą dzięki temu przetwarzać oba typy ruchu używając adresów IPv4 do komunikacji z serwerami IPv4 i adresów w wersji 6 do obsługi połączeń wychodzących do innych sieci IPv6. Istotną wadą tego rozwiązania jest to, iż sieci te nie skalują się w związku z zapotrzebowaniem na adresy IPv4, natomiast można ten mechanizm stosować w sieciach już posiadających infrastrukturę IPv4. Można zmniejszyć zapotrzebowanie na adresy IPv4 poprzez wprowadzenie modyfikacji pozwalającej na efektywniejsze użycie puli adresów IPv4 w oparciu o serwer DHCP, który dynamicznie przydziela adres IPv4 na czas trwania połączenia. Adres ten zwalniany jest po wykorzystaniu i może być przydzielony do innego połączenia. Mechanizm ten został nazwany DSTM (ang. Dual Stack Transition Mechanizm). Generowany ruch IPv4, aby mógł być przekazywany poprzez sieci IPv6, musi być tunelowany w datagramach IPv6, co w zasadzie eliminuje konieczność zapewnienia wsparcia dla DSTM w sieciach IPv6, by móc nawiązywać połączenia do sieci opartych tylko na IPv4.



Rys. 1. Działanie mechanizmu DSTM
Fig. 1. Dual Stack Transition Mechanism (DSTM)

Aby więc móc używać mechanizmu DSTM, host musi być tak skonfigurowany, by zwracać się do serwera DHCP, kiedy istnieje potrzeba zestawienia połączenia IPv4. Schemat ten inaczej wygląda w zależności od kierunku przyjścia pakietu inicjalizującego połączenie. Aplikacja dual stack musi sprawdzić przez wysłanie zapytania do serwera DNS, czy zdalny host używa wyłącznie IPv4. Wtedy host DSTM żąda od serwera DHCP przydzielenia adresu, który jest używany do obsługi tunelowanego w datagramach IPv6 połączenia. Pakiety są tunelowane wyłącznie do rutera brzegowego sieci IPv6, gdzie następuje ich przesłanie

zwykłym ruchem IPv4 do odbiorcy. W przypadku gdy zdalny host IPv4 rozpoczyna połączenie, serwer DNS wspierający DSTM wykrywa fakt, iż host nie posiada adresu IPv4 i rozpoczyna procedurę przydziału adresu dla hosta DSTM z serwera DHCP.

Takie rozwiązanie może powodować szereg problemów związanych z podatnością na ataki typu "Denial of Service", gdyż każde zapytanie do serwera DNS powoduje akcje przydziału kolejnego adresu, więc ciągłe powtarzanie takich zapytań może spowodować wyczerpanie się całej puli adresów IPv4 i w rezultacie zablokowanie komunikacji z siecią opartą na DSTM. Drugim problemem jest precyzyjne określenie momentu zakończenia sesji potrzebne przy zwracaniu adresu do serwera DHCP. Moment ten może być szczególnie trudny do określenia w przypadku pewnych sesji protokołu UDP.

Główną zaletą tego rozwiązania jest fakt, iż pozwala ono na prostą obsługę połączeń IPv4 z sieci IPv6, z jednoczesnym efektywnym gospodarowaniem przestrzenią adresową IPv4. Metoda ta będzie raczej stosowana we wczesnej fazie wdrożenia technologii IPv6, gdzie w sieci IPv6 będzie istniała znikoma liczba hostów obsługujących wyłącznie ruch IPv4.

3.3. Translacja protokołów

Kolejne rozwiązanie oparte na NAT-PT (ang. Network Address Translator – Protocol Translator) umożliwi realizację tłumaczenia pomiędzy protokołami w wersji 4 i 6. W odróżnieniu od znanego z IPv4 rozwiązania NAT, które umożliwiało zmianę jedynie adresów lub/i numerów portów w nagłówkach translowanych pakietów, mechanizm NAT-PT pozwala na tłumaczenie protokołów wyższych warstw, takich jak np. TCP i UDP odpowiednio interpretując nagłówki i pole danych pakietów IP.

Translacja jest dwukierunkowa i może być zainicjowana przez węzeł używający dowolnej wersji protokołu IP, co więcej sam fakt translacji połączenia jest niewidoczny dla komunikujących się stron. Translacja jest zestawiana przez wymianę zapytań DNS; etap ten wymaga obecności specjalnego translatora dla pakietów DNS (DNS Aplication-Layer Gateway) w standardowym procesie translacji NAT-PT. Mechanizm ALG jest używany w przypadku konieczności stosowania translacji protokołów, które używają adresów w warstwie aplikacji modelu OSI-ISO RM. Stosowanie ALG wychodzi poza zakres normalnej pracy NAT-PT; większość pakietów IP wymaga prostego tłumaczenia adresów i nagłówków.

NAT-PT modyfikuje jedynie pakiety, które są przekazywane pomiędzy sieciami IPv4/IPv6 poprzez translację nagłówka do formatu sieci docelowej. Może również tymczasowo przydzielić adres IPv4 dla hosta IPv6, adresy te są przydzielane z posiadanej przez translator puli i zwracane podobnie jak w DSTM na zakończenie sesji. Schemat ten może zostać rozszerzony do mechanizmu zwanego NAPT-PT (ang. Network Address Port

Translator – Protocol Translator). NAPT-PT używa łącznie z adresami również numery portów, przez co może on adresować z wykorzystaniem pojedynczego adresu IPv4 kilka węzłów IPv6.

Problemem podczas stosowania NAT-PT jest tzw. pojedynczy punkt uszkodzenia. Wszystkie połączenia pomiędzy sieciami IPv6 i IPv4 muszą przechodzić przez pojedynczy węzeł, którego uszkodzenie powoduje odcięcie komunikacji. Można temu zapobiegać przez konfigurowanie wielu translatorów dla pojedynczej sieci, co zwiększy niezawodność połączeń, jak również umożliwi zastosowanie zrównoważenia obciążenia (ang. load-balance) poszczególnych translatorów. Używanie NAT-PT utrudnia również stosowanie technologii zapewniających autoryzację i poufność przenoszonych danych.

NAT-PT powinien być używany jedynie wówczas, gdy nie istnieje możliwość zapewnienia natywnej lub tunelowanej komunikacji IPv6 pomiędzy węzłami, dodatkowo powinien być stosowany, gdy musimy zapewnić komunikację pomiędzy hostem używającym jedynie IPv6 a aplikacją lub węzłem IPv4.

3.4. Proxy aplikacyjne

Często stosowany w sieciach lokalnych model komunikacji z serwisami zewnętrznymi z użyciem serwera pośredniczącego, tzw. serwera proxy, ma szereg zalet – można dzięki niemu zwiększyć stopień bezpieczeństwa sieci jak również stosować wbudowane mechanizmy cache'owania ruchu np. dla serwerów HTTP. Mechanizm ten również dobrze nadaje się do zapewnienia współpracy pomiędzy dwoma rodzajami ruchu, IPv4/IPv6. Komunikacja obywać się będzie wtedy za pomocą zestawienia dwóch połączeń, jednego np. IPv4 pomiędzy aplikacją a serwerem proxy, natomiast serwer proxy będzie używał ruchu IPv6 do komunikacji z zdalnym serwisem. Użycie tego schematu pozwala uniknąć problemów związanych z obsługą fragmentacji, która może pojawić się przy stosowaniu tunelowania. Wadą jest konieczność stosowania dla każdego protokołu oddzielnego serwera proxy lub aplikacji realizującej tę funkcje.

4. Podsumowanie

Pytanie czy protokół IPv6 uzyska odpowiednio wysoką popularność, aby móc wyprzeć całkowicie używany obecnie standard, powinno raczej brzmieć: kiedy to tak naprawdę nastąpi. Wcześniej czy później znajdziemy się przed koniecznością zmiany. Ważne, aby operacja ta przebiegła możliwie jak najbardziej bezboleśnie dla użytkowników, oprogramowania oraz stosowanych systemów operacyjnych. O sukcesie może decydować

fakt znajomości rozwiązań i mechanizmów umożliwiających wspólną koegzystencję obu protokołów, a ich zastosowanie zagwarantuje ciągłość ewolucji sieci.

LITERATURA

1. Lutchansky N.: A Technical Introduction to IPv6. Internet Draft, 2001.
2. Dual Stack Transition Mechanism (DSTM). Internet Draft, 2002.
3. Carpenter B., Moore K.: Connection of IPv6 Domains via IPv4 Clouds. RFC3056.
4. Network Address Translation - Protocol Translation (NAT-PT). RFC2766.
5. Gilligan R., Nordmark E.: Transition Mechanisms for IPv6 Hosts and Routers. RFC 1933, 1996.

Recenzent: Dr inż. Mirosław Skrzewski

Wpłynęło do Redakcji 25 marca 2002 r.

Abstract

In the Internet the most popular protocol is IPv4, built for military networks and adapted to much bigger infrastructure in which its addressing possibilities have run low. This fact slows down the network expansion and may contribute to stopping its development. The case concerns not only addresses for new devices, but also reserving address space for innovative technologies as VoIP, UMTS or interactive services. The used methods of addresses management as NAT does not work properly with the above mentioned technologies, moreover they increase the complexity of network configuration and slow down the routing.

The solution to these problems might be IPv6 protocol introduced as a successor to currently used IPv4 protocol. It increases the address space, and improves some IPv4 disadvantages. The main differences are: FlowLabel, Security and usage of QoS. IPv6 besides the header format does not introduce changes in transporting TCP and UDP protocols, hence all services using fourth layer will impose little work while moving to new standard.

The issue will be deployment of new protocol. It is estimated that the operation enabling coexistence both of these protocols will last nearly 10 years. Just after this period every node will use IPv6. During this time it must be guaranteed that all nodes will be able to communicate nevertheless the network protocol. The main method of achieving this is

tunneling IPv6 inside IPv4 packets linking the IPv6 islands through routers that support only IPv4. The other solution is DSTM that enables usage of both IPv4 and IPv6 addresses in single node and transparent usage of both protocols by choosing appropriate on the basis of address configuration of target host. In some topologies it will be necessary to translate between IPv6 and IPv4 protocols. This would enable pure IPv6 communication between different nodes.