Tomasz MALINOWSKI[1]

MECHANIZMY QOS W KONTEKŚCIE INTEGROWANIA SIECI IPV4 I IPV6

Streszczenie

Artykuł przedstawia metody klasyfikowania pakietów w kontekście integrowania sieci z protokołem IPv6 i IPv4. IPv6 wprowadza pewne dodatkowe udogodnienia, jak pole flow label w nagłówku pakietu IP, ale realizacja systemu QoS w sieci IPv6 oparta jest na zasadach stosowanych w sieciach IPv4. Szczególnie istotnym staje się wybór miejsca klasyfikowania pakietów i mechanizmu integracji sieci IPv4 z siecią IPv6. Rozważania zawarte w artykule dotyczą realizacji QoS przy zastosowaniu podwójnego stosu, tunelowania i translacji protokołów.

Abstract

The article presents methods of classifying packets in the context of integrating the net with IPv6 and IPv4 protocols. IPv6 introduces some additional features (like flow label field in the packet header) and the current support for QoS mechanisms in IPv6 implementations approaches the corresponding QoS support in IPv4. The choice of the place of classifying packets and the mechanism of integrating the IPv4 and IPv6 networks are particularly important. QoS implementations with the use of dual-stack, tunneling and translation protocols are discussed.

1. KLASYFIKOWANIE PAKIETÓW I REALIZACJA SYSTEMU QOS W SIECIACH IPV4 I IPV6

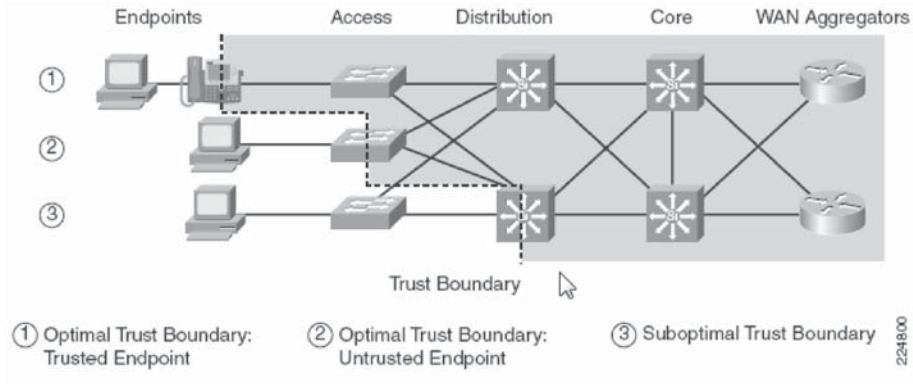
Podstawą realizacji systemów QoS jest oznaczanie lub jawne informowanie węzłów sieciowych o ważności strumienia pakietów. Oznaczanie pakietów (także ramek warstwy łącza danych) jest ściśle związane z modelem DiffServ systemu QoS. Producenci sprzętu sieciowego, w tym firma Cisco Systems, wyposażają swoje urządzenia sieciowe w mechanizmy umożliwiające identyfikowanie określonych strumieni danych (z dokładnością do pojedynczych ramek i pakietów), klasyfikowanie tych strumieni zgodnie z przyjętą polityką zapewniania pożądanego poziomu usług

[1] Dr inż. Tomasz Malinowski jest wykładowcą Warszawskiej Wyższej Szkoły Informatyki, a jednocześnie pracownikiem Instytutu Teleinformatyki i Automatyki Wojskowej Akademii Technicznej.

i realizację systemu QoS z wykorzystaniem kolejkowania pakietów, „przycinania" dostępnego pasma przepustowości, algorytmów zarządzania zatorami i unikania przeciążeń.

Klasyfikowanie i oznaczanie pakietów jest procesem służącym identyfikowaniu strumieni danych związanych z konkretnym źródłem lub aplikacją, które są istotne z punktu widzenia realizacji systemu QoS.

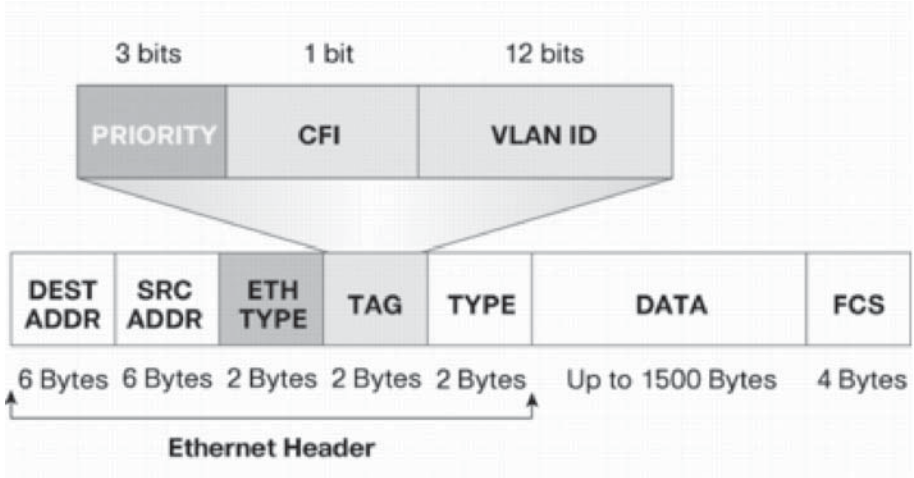
Oznaczanie ważności strumienia danych może odbywać się już w systemie końcowym (np. hoście, telefonie IP), który jest źródłem ruchu sieciowego, w przełączniku warstwy II lub III i routerze. Miejsce oznaczania ramek (pakietów) wskazane zostało na rysunku 1.



Rys. 1. Granice klasyfikowania i oznaczania pakietów na potrzeby systemu QoS

Oczywiście w gestii administratora sieci pozostaje podjęcie decyzji gdzie oznaczać pakiety. Biorąc pod uwagę łatwość samodzielnego ustalenia priorytetu na stacji roboczej raczej rzadko oznaczanie to realizowane jest w systemie końcowym. Częściej granicą systemu oznaczania i klasyfikowania pakietów jest przełącznik warstwy dostępu, warstwy jądra lub router.

Sklasyfikowany ruch otrzymuje ustalony znacznik QoS (zmiana wartości pola CoS, ToS). Najczęściej podstawą klasyfikowania są informacje zawarte w nagłówkach ramek warstwy II (MAC adres, identyfikator sieci VLAN), nagłówku warstwy III (adres IP, wejściowy interfejs) i nagłówku warstwy IV (port TCP lub UDP). Zaznaczyć należy, że nagłówek warstwy II nie posiada pola, które mogłoby zawierać znacznik QoS i konieczna jest zastosowanie enkapsulacji 802.1q. Nagłówek ramki 802.1q zawiera 3 bitowe pole o nazwie PRI (User Priority), nazywane potocznie CoS (Class of Service) – rysunek 2.



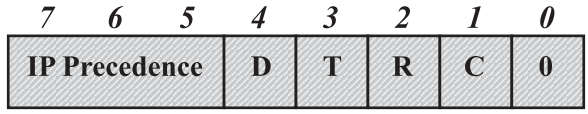
Rys. 2. Struktura ramki 802.1q

Struktura nagłówka pakietu IPv4 z wyróżnionym polem ToS (interpretowanym jako pole IP Precedence lub DSCP – Differentiated Services Code Point) przedstawiona została rysunku 3.

Rys. 3. Struktura nagłówka pakietu IPv4

Wymienione pola mogą być mapowane na siebie na przykład przez proste przepisanie przez urządzenie sieciowe wartości pola CoS w pole ToS pakietu IP. Z kolei pole ToS może być przepisane przykładowo w pole EXP (Experimental) pakietu MPLS, jeśli pakiet skierowany zostanie do domeny MPLS.

Początkowo definicja IP Precedence ograniczała się jedynie do trzech najstarszych bitów pola ToS. Kolejne rozszerzenie standardu IP w postaci RFC 1349 opisuje znaczenie siedmiu bitów tego pola, co przedstawia rysunek 2.3.



Rys. 4. Pole IP Precedence

Trzy najstarsze bity pola ToS nadają odpowiedni priorytet danemu pakietowi i są bitami ustalającymi pierwszeństwo (ang. *Precedence*). W zależności od ich ustawienia pakiety obsługiwane są przez urządzenia sieciowe w odpowiedni sposób. Znaczenie poszczególnych wartości IP Precedence zawiera tabela 1.

Tabela 1. Definicje wartości IP Precedence

IP Precedence	Klasa	Definicja	Sposób obsługi
000	0	Routine	Rutynowa obsługa pakietu
001	1	Priority	Priorytetowa obsługa pakietu
010	2	Immediate	Natychmiastowa obsługa pakietu
011	3	Flash	Błyskawiczna obsługa pakietu
100	4	Flash-Override	Super-błyskawiczna obsługa pakietu
101	5	Critical	Krytyczna obsługa pakietu
110	6	Internetwork Control	Ruch kontrolny
111	7	Network Control	Ruch kontrolny

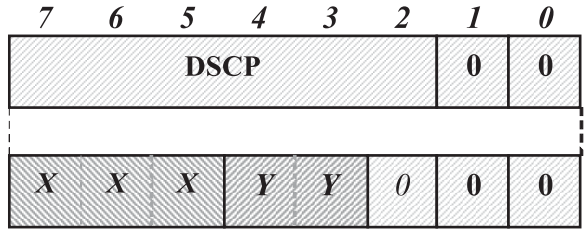
Wartości 6 i 7 są zarezerwowane na tzw. „ruch służbowy”, czyli np.: zarządzanie, protokoły routingu, itp. Cztery kolejne bity pełnią rolę flag, które określają sposób, w jaki odpowiednio sklasyfikowany pakiet ma być obsługiwany, co przedstawia Tabela 2. Odpowiednie ustawienie tych bitów ma wpływ na parametry transmisyjne przesyłanych pakietów.

Tabela 2. Flagi i znaczenie bitów pola ToS

Wartość	Bit	Definicja	Wpływ na parametr transmisji
1000	D=1	Delay	Minimalizacja opóźnienia transmisji
0100	T=1	Throughput	Maksymalizacja przepustowości transmisji
0010	R=1	Reliability	Maksymalizacja niezawodności transmisji
0001	C=1	Cost	Minimalizacja kosztu transmisji
0000	-	Normal	Normalna transmisja pakietu

Spośród czterech flag dany pakiet IP może mieć ustawiony tylko jedną z nich. Ostatni, najmłodszy bit jest niewykorzystywany i przyjmuje wartość zero.

Drugim sposobem znakowania pakietów jest DSCP. Definicja pola DSCP przedstawionego na rysunku 5 zawarta jest w dokumencie RFC 2474. Ten sposób kodowania pola ToS, w porównaniu do IP Precedence dostarcza możliwość zdefiniowania większej liczby poziomów usług sieciowych. Do oznaczania pakietów IP wykorzystywane jest tu sześć najbardziej znaczących bitów. Trzy najstarsze bity *XXX* klasyfikują dany pakiet przydzielając go do odpowiedniej klasy, informując tym samym urządzenia sieciowe o jego priorytecie. Kolejne dwa bity *YY* określają poziom obsługi tego pakietu w ramach danej klasy i prawdopodobieństwo usunięcia pakietu z kolejki. Najmłodszy z sześciu bitów DSCP oraz pozostałe dwa bity pola ToS przyjmują wartość zero. Rysunek 5 przedstawia podział bitowy pola ToS w znaczeniu DSCP.



Rys. 5. Format bajtu ToS w standardzie DSCP

Wartości bitów *YY* mają następujące znaczenie:

- 00 – wartość, która powoduje, że dany pakiet będzie klasyfikowany tylko na podstawie trzech najstarszych bitów *XXX*. Takie oznaczenie nosi nazwę selektora klas CS (ang. *Class Selector*). Ustawienie tej wartości dostarcza wsteczną kompatybilność z oznaczeniami IP Precedence.
- 01, 10, 11 – wartości te, w przypadku przeciążenia określają prawdopodobieństwo usunięcia danego pakietu z kolejki (ang. *drop probability*) przez mechanizmy QoS. Wartość maksymalna oznacza prawdopodobieństwo najmniejsze.

Ostatni bit pola DSCP oraz najmłodsze dwa bity pola ToS przyjmują wartość „0".

Wartości pola DSCP można przedstawiać w postaci binarnej, dziesiętnej lub w notacji PHB (ang. *Per Hop Behaviour*), która wprowadza nazwy dla poszczególnych klas. Tabela 3 przedstawia wartości oraz sposób oznaczania i interpretacji pola DSCP.

Tabela 3. Oznaczenie oraz klasy pola DSCP i IP Precedence

Wartość pola DSCP						Nazwa klasy
Binarnie		PHB		DSCP	IP Prec.	
XXX	YY					
000	00	BE		0	0 (routine)	Best Effort
000	01	---		2		---
	10			4		
	11			6		
001	00	CS1		8	1 (priority)	Class Selector
	01	AF1x	AF11	10		Assured Forwarding
	10		AF12	12		
	11		AF13	14		
010	00	CS2		16	2 (immediate)	Class Selector
	01	AF2x	AF21	18		Assured Forwarding
	10		AF22	20		
	11		AF23	22		
011	00	CS3		24	3 (flash)	Class Selector
	01	AF3x	AF31	26		Assured Forwarding
	10		AF32	28		
	11		AF33	30		
100	00	CS4		32	4 (flash-override)	Class Selector
	01	AF4x	AF41	34		Assured Forwarding
	10		AF42	36		
	11		AF43	38		
101	00	CS5		40	5 (critical)	Class Selector
	01	---		42		---
	10			44		
	11	EF		46		Expedited Forwarding
110	00	CS6		48	6 (Internet)	Class Selector
	01	---		50		---
	10			52		
	11			54		
111	00	CS7		56	7 (network)	Class Selector
	01	---		58		---
	10			60		
	11			62		

Projektanci protokołu IPv6 zadbali o wsteczną kompatybilność nowego protokołu w aspekcie realizacji systemu QoS, co oznacza, że pole Traffic Class w nagłówku pakietu IPv6 ma identyczne znaczenie i zastosowanie jak pole ToS w nagłówku pakietu IPv4. Przykładowo, Cisco System w swoich produktach oferuje dla IPv6

praktycznie te same mechanizmy realizacji systemu QoS co w przypadku protokołu IPv4. Są to:

1. Klasyfikowanie pakietów
2. Kolejkowanie pakietów (z wyłączeniem kolejkowania PQ i CQ)
3. Traffic shaping
4. WRED
5. Oznaczanie pakietów bazujące na zdefiniowanych klasach.

Niestety, w nowej wersji protokołu IP nie są oferowane:

1. Kompresja pakietów protokołu RTP
2. Mechanizm automatycznego rozpoznawania wykorzystywanych protokołów i aplikacji NBAR
3. Mechanizm CAR (Committed Access Rate)
4. Kolejkowanie PQ (Priority Queuing)
5. Kolejkowanie CQ (Custom Queuing)

Problemem pozostaje przepisanie wartości pola ToS do pola Traffic Class w trakcie integrowania sieci bazujących na IPv4 z sieciami IPv6. **W związku z tym szczególnego znaczenia nabiera zastosowany mechanizm translacji protokołu IPv4 na IPv6.**

1.1. Oznaczanie pakietów w warstwie dostępu i systemach końcowych

W modelu DiffServ (Differentiated Services) przyjmuje się, że oznaczanie pakietów na potrzeby systemu QoS odbywa się w momencie wejścia pakietu do sieci i może być realizowane przez ustawienie wartości pola IP Precedence, pola DSCP, pola Traffic Class (w przypadku pakietów IPv6), a więc w warstwie III lub przez ustawienie pola CoS enkapsulowanej ramki Ethernet (802.1q/p lub ISL), a więc w warstwie II, bezpośrednio w urządzeniu końcowym, które jest źródłem ruchu lub w przełączniku sieciowym. W przypadku oznaczania pakietów w warstwie II (ustalenie wartości 3 bitowego pola CoS przez przełącznik), zwykle urządzenie warstwy III przepisuje wartość CoS w pole ToS (Traffic Class w przypadku IPv6) nagłówka pakietu IP.

Współczesne systemy końcowe (systemy operacyjne hostów) mogą same oznaczać swoje pakiety odpowiednimi wartościami CoS, IP Precedence, DSCP, Traffic Class, aczkolwiek zadanie to może być scedowane na przełącznik warstwy dostępu.

W przypadku oznaczania ramek w urządzeniach końcowych (ustalenie wartości pola CoS) zadaniem przełącznika jest wymazanie (ustalenie nowej wartości CoS, zwykle na 0) dla urządzeń „niezaufanych" lub przepuszczenie ramki bez modyfikowania, jeśli urządzenie rozpoznawane jest jako „zaufane". Identyfikowanie jest konieczne, szczególnie w przypadkach jak na rysunku 6, gdzie pokazano stację roboczą przyłączoną do przełącznika sieciowego przez telefon IP. Przykładowo, telefon VoIP może być traktowany jako urządzenie uprzywilejowane i wymagające gwarantowanego określonego pasma, a stacja robocza nie.

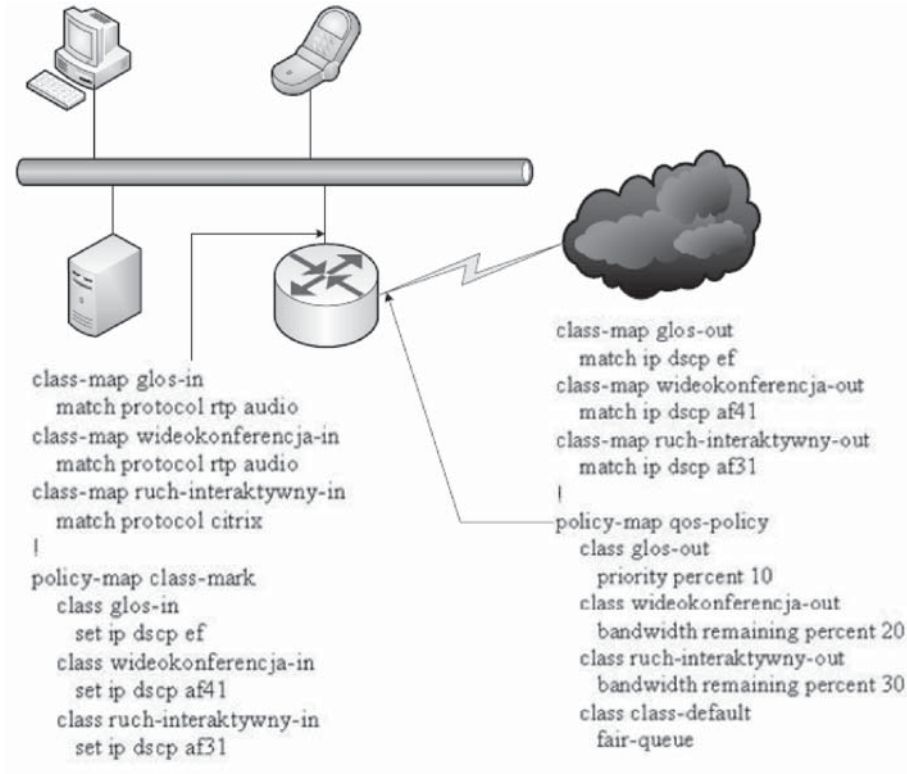
Rys. 6. Przyłączenie stacji roboczej do sieci przez telefon IP

W przypadku hostów czy np. drukarek, porty przełącznika, do których przyłączone są te urządzenia powinny być ustawione w tryb domyślnego zerowania pola CoS, gdyż rzadko urządzenia te są urządzeniami uprzywilejowanymi, czyli ważnymi z punktu widzenia realizacji systemu QoS.

Cechą szczególną wielu przełączników (zależnie od modelu i oprogramowania) jest możliwość ustalenia wartości pola DSCP w oparciu o pole CoS (mapowanie CoS na DSCP). Niestety, w wielu przypadkach, a w szczególności gdy przez pojedynczy port przełącznika przechodzi ruch pochodzący z różnych hostów, ustalanie wartości pola CoS dla ramek pochodzących od pojedynczego urządzenia nie jest możliwe. W takich przypadkach stosowane są listy kontroli dostępu identyfikujące źródło ruchu w oparciu o adres MAC i oznaczanie sklasyfikowanych w oparciu o adres fizyczny ramek przez modyfikowanie pola DSCP w nagłówku pakietu IP. Z kolei listy kontroli zwane IP ACL umożliwiają identyfikowanie i klasyfikowanie pakietów w oparciu o źródłowy i docelowy adres IP, czy też nr portu (TCP/UDP) źródłowego i docelowego.

2. REALIZACJA SYSTEMU QOS W URZĄDZENIACH WARSTWY III

Warstwa III sieci i urządzenia routujące, często będące urządzeniem granicznym systemu autonomicznego instytucji są najczęściej obieranym miejscem realizacji systemu gwarantowania odpowiedniej jakości usług. Typowy system przedstawiony został na rysunku 7.



Rys. 7. Przykład realizacji systemu QoS

Klasyfikowanie i oznaczanie pakietów może odbywać się na wejściu routera lub wcześniej, w systemie końcowym, przełączniku warstwy dostępu, warstwy dystrybucji lub przełączniku szkieletowym (warstwy jądra) sieci. W rozważanym przykładzie zarówno proces klasyfikowania jak i realizacji ustalonej polityki QoS przeprowadzany jest w routerze granicznym sieci. Klasyfikowanie pakietów związanych z ruchem VoIP, wideokonferencją i ruchem interaktywnym dokonywane jest na wejściu routera, natomiast konkretna polityka QoS aplikowana jest na interfejsie wyjściowym.

W przypadku protokołu IPv6 polecenia konfiguracyjne są w zasadzie identyczne, co przedstawia tabela 4.

Tabela 4. Polecenia konfiguracyjne QoS dla wersji protokołu IPv4 i IPv6

IPv4-Only QoS Syntax	**IPv4/IPv6 QoS Syntax**
match ip dscp	match dscp
match ip precedence	match precedence
set ip dscp	set dscp
set ip precedence	set precedence

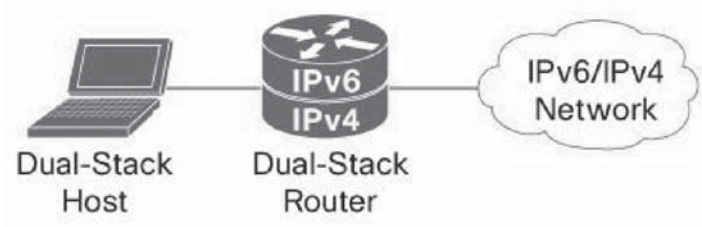
3. REALIZACJA SYSTEMU QOS NA TLE SPOSOBÓW INTEGROWANIA SIECI IPV4 I IPV6

W 1996 roku powołana została specjalna grupa IETF NGtrans, odpowiedzialna za opracowanie mechanizmów i procedur służących integrowaniu sieci bazujących na protokołach IPv4 i IPv6. W wyniku prac tej grupy opracowane zostały trzy strategie integrowania protokołów IPv4 i IPv6:

1. Podwójny stos IP
2. Tunelowanie
3. Translacja protokołu.

3.1. Podwójny stos IP

Realizacja podwójnego stosu IP jest preferowaną strategią integrowania sieci IPv4 i IPv6. Strategia nie jest niczym nowym i odkrywczym i była z powodzeniem wykorzystywana na przykład w trakcie wdrażania protokołu IPv4 w sieciach bazujących na protokole IPX. Zakłada się, że urządzenia sieciowe będą obsługiwały na swoich interfejsach sieciowych zarówno ruch pochodzący z sieci (aplikacji) bazujący na IPv4, jak i na IPv6. Konieczne jest zatem przywiązanie do interfejsu urządzenia sieciowego adresu IPv4 i adresu IPv6 (rysunek 8).

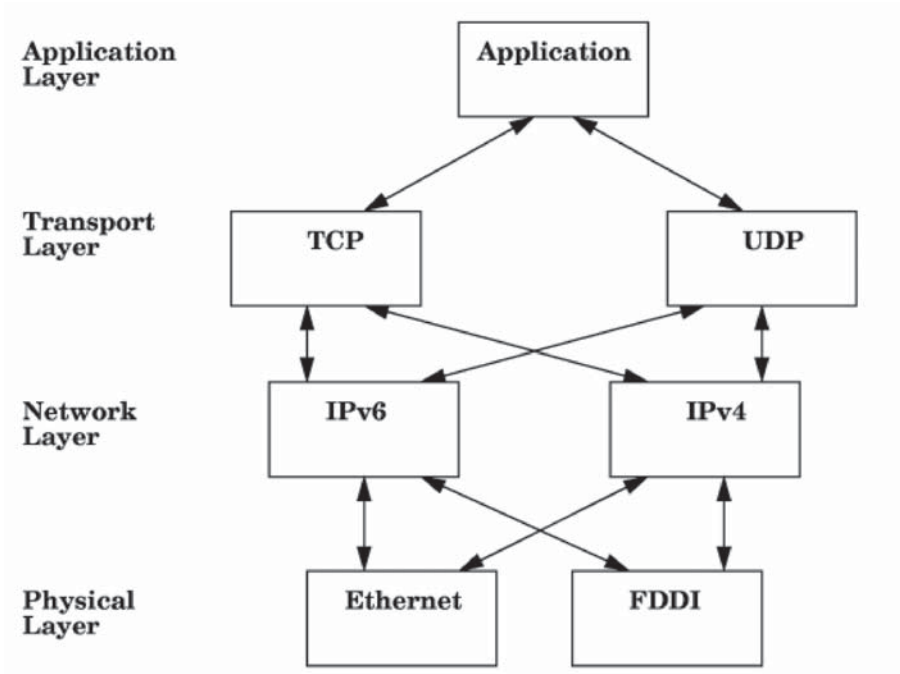


Rys. 8. Host z podwójnym stosem protokołów przyłączony do sieci IPv6/IPv4

Zakłada się, że w przypadku tej metody integracji na hoście w sieci IPv4/IPv6 będą współistniały aplikacje korzystające z IPv4 lub z IPv6. Należy przyjąć zasadę dążenia do wyboru stosu IPv6 tam, gdzie tylko jest to możliwe. To z jakiego protokołu sieciowego skorzysta dana aplikacja może zostać określone na drodze ręcznej konfiguracji lub wykorzystania odpowiednio skonfigurowanej usługi DNS.

Typowa aplikacja obsługująca tylko protokół IPv4 kierując zapytanie do serwera DNS dostaje z bazy Sewera DNS w odpowiedzi wartość rekordu A. Aplikacja obsługująca obydwa protokoły IP, kierując zapytanie do serwera DNS powinna odpytać o rekordy obydwu protokołów, czyli A dla protokołu IPv4 oraz AAAA dla protokołu

IPv6. Serwer DNS na takie zapytanie powinien w pierwszej kolejności w odpowiedzi zwrócić wartość rekordu AAAA. Dopiero gdy nie znajdzie w swojej bazie rekordu AAAA może zwrócić wartość rekordu A. Dzięki takiemu zabiegowi, gdy tylko będzie to możliwe, zostanie użyty protokół IPv6. Rysunek 9 przedstawia schemat podwójnego stosu IP.



Rys. 9. Podwójny stos IP

W przypadku urządzeń z implementowanym podwójnym stosem klasyfikowanie pakietów w oparciu o wartość pola ToS lub Traffic Class w nagłówku IPv6 nie stanowi problemu. Ustalenie wartości wymienionych pól może odbyć się już w urządzeniu stanowiącym źródło ruchu lub też na interfejsie wejściowym urządzenia z podwójnym stosem, oczywiście po wcześniejszym zidentyfikowaniu źródła (z wykorzystaniem np. list kontroli dostępu).

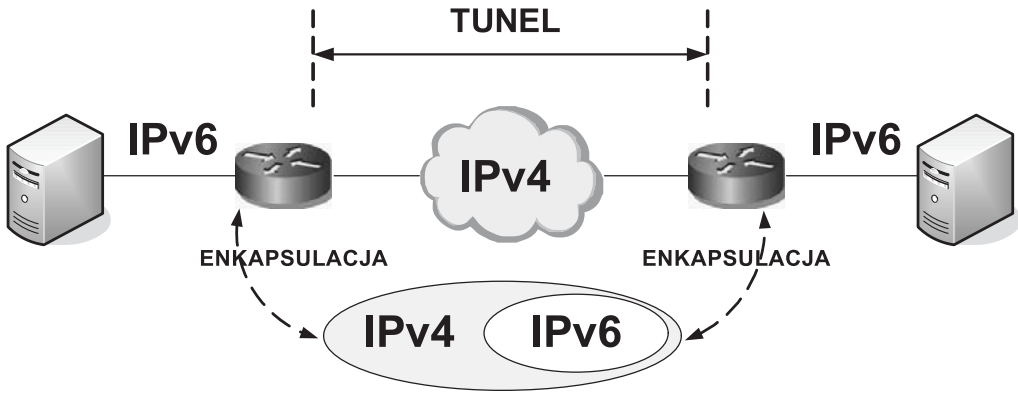
3.2. Tunelowanie protokołu

Tunelowanie jest techniką pozwalającą na przesyłanie jednego protokołu wewnątrz drugiego. Tunelowanie znajduje zastosowanie wszędzie tam, gdzie w sąsiedztwie znajdują się niekompatybilne protokoły. Taka właśnie sytuacja ma miejsce

przy protokołach IPv4 i IPv6. Mówi się o zjawisku oceanu IPv4, jakim jest Internet i wyspach IPv6, jakimi są obecne sieci bądź pojedyncze hosty pracujące w oparciu o protokół IPv6. Oczekuje się, że w ciągu kilku lat sytuacja się odwróci i protokół IPv4 pozostanie tym tworzącym wyspy.

Istnieje wiele technik tunelowania protokołu IPv6 w IPv4. Warto zaznaczyć, że warunkiem koniecznym zestawienia tunelu jest obsługa podwójnego stosu IP przez oba węzły sieciowe, stanowiące krańce tunelu.

Przykładem szczególnie praktycznego protokołu tunelowania jest GRE (Generic Routing Encapsulation). W przypadku enkapsulowania pakietów IPv4 w pakietach IPv6, urządzenie graniczne realizujące tunelowanie przepisuje wartość pola Traffic Class enkapsulowanego pakietu IPv6 do pola ToS nowego nagłówka IPv4. Umożliwia to realizację np. procedury ograniczania pasma przepustowości w oparciu o wartość tego pola na interfejsie typu tunel urządzenia enkapsulującego. Technikę tunelowania przedstawia rysunek 10.



Rys. 10. Zasada tunelowania IPv6 w protokole IPv4

GRE jest przykładem jednej z wielu technik tunelowania, które znajdują zastosowanie przy integrowaniu systemów bazujących na IPv4 i IPv6. Inne zostały wymienione w tabeli poniżej. Każda z nich powinna być rozważana indywidualnie, pod kątem możliwości realizacji systemu QoS.

Tabela 5. Mechanizmy integracji IPv4 z IPv6. ES oznacza system końcowy (End System), ND– węzeł sieciowy (Node)

Name	Connectivity	Type	Location
Dual stack	4-to-4 over 4, 6-to-6 ocer 6	Dual stack	In single ES or ND
SIIT	6-to-4, 4-to-6	Translator	In single ES or ND
Bump-in-Stack (BIS)	4-to-6	Translator	In single ES
Bump-in-API (BIS)	4-to-6	Translator	In single ES

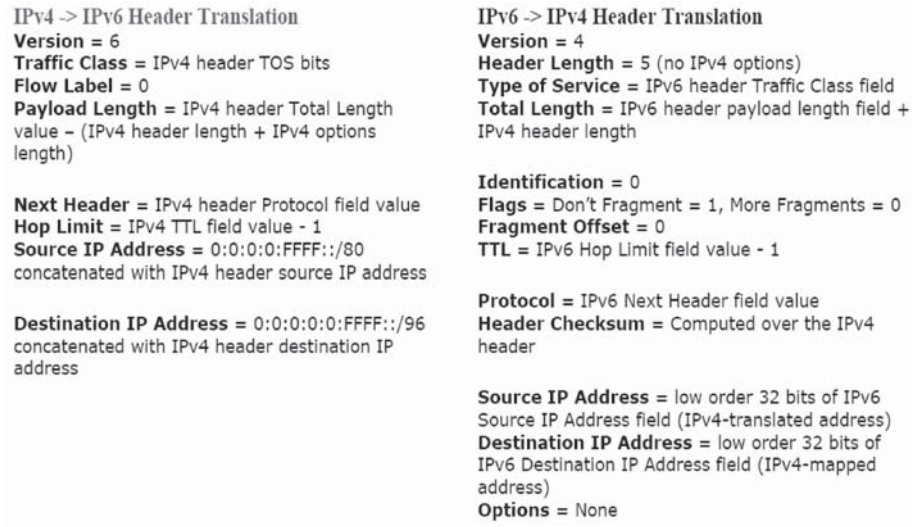
NAT-PT	6-to-4, 4-to-6	Translator	In single ES
MTP	4-to-6, 4-to-6 (multicast)	Translator	In single ES
TRT	6-to-4	Translator	In single ES
SOCKS64	4-to-6, 4-to-6	Translator	Between ES and ND
6over4	6-to-6 over 4	Tunnel	Between ES and ND
ISATAP	6-to-6 over 4	Tunnel	Between ES and ND
DSTM	4-to-4 over 6	Tunnel	Between ES and ND
Configured IP-in-IP	6-to-6 over 4, 4-to-4 over 6	Tunnel	Between ES and ND, two NDs or two ESs
6to4	6-to-6 over 4	Tunnel	Between two NDs

3.3. Translacja protokołu

Trzecim sposobem integrowania protokołów IPv4 i IPv6 jest użycie translatora protokołów. Translacja jest rozwiązaniem koniecznym w przypadku łączenia sieci zawierających urządzenia tylko-IPv4 (gdzie nie jest możliwa implementacja podwójnego stosu) z sieciami z urządzeniami tylko-IPv6. W przypadku realizacji systemu QoS w zintegrowanym środowisku urządzeń IPv4 i IPv6, właściwy wybór techniki translacji nabiera szczególnego znaczenia wtedy, gdy oznaczanie pakietów odbywa się w systemie (domenie) IPv4, natomiast klasyfikowanie w oparciu o wartość pola ToS (a właściwie pola Traffic Class) i poddanie pakietów odpowiednim regułom QoS w systemie IPv6. Rozważany zatem powinien być wybór takiego translatora, który umożliwia przepisanie wartości ToS do pola Traffic Class, a przy tym bezproblemowe komunikowanie się urządzeń sieciowych w warstwie aplikacji. Tabela 1 zawiera wykaz rekomendowanych i stosowanych obecnie technik translacji. Poniżej omówione zostały dwie pokrewne techniki translacji, SIIT i NAT-PT.

SIIT – Stateless IP/ICMP Translation algorithm

SIIT zapewnia tłumaczenie nagłówków pakietu IP pomiędzy IPv4 a IPv6. Translator uruchomiony jest na hoście obsługującym protokół IPv6 i dokonuje konwersji nagłówków wychodzących pakietów IPv6 na nagłówki IPv4 oraz konwersji nagłówków przychodzących pakietów IPv4 na nagłówki IPv6. Procedura wymaga ustalenia dla hosta IPv6 tymczasowego adresu IPv4, jednakże RFC 2765 opisujące SIIT nie określa sposobu pozyskiwania tego adresu ani też sposobu rejestrowania adresu na serwerze DNS czy mechanizmu routingu dla adresów IPv4 odpowiadających mapowanym adresom IPv6. Proces translacji odbywa się zgodnie z zamieszczonym poniżej zasadami.



IPv4 -> IPv6 Header Translation

Version = 6
Traffic Class = IPv4 header TOS bits
Flow Label = 0
Payload Length = IPv4 header Total Length value – (IPv4 header length + IPv4 options length)

Next Header = IPv4 header Protocol field value
Hop Limit = IPv4 TTL field value - 1
Source IP Address = 0:0:0:0:FFFF::/80 concatenated with IPv4 header source IP address

Destination IP Address = 0:0:0:0:0:FFFF::/96 concatenated with IPv4 header destination IP address

IPv6 -> IPv4 Header Translation

Version = 4
Header Length = 5 (no IPv4 options)
Type of Service = IPv6 header Traffic Class field
Total Length = IPv6 header payload length field + IPv4 header length

Identification = 0
Flags = Don't Fragment = 1, More Fragments = 0
Fragment Offset = 0
TTL = IPv6 Hop Limit field value - 1

Protocol = IPv6 Next Header field value
Header Checksum = Computed over the IPv4 header

Source IP Address = low order 32 bits of IPv6 Source IP Address field (IPv4-translated address)
Destination IP Address = low order 32 bits of IPv6 Destination IP Address field (IPv4-mapped address)
Options = None

Jak widać translator SIIT dokonuje przepisania wartości ToS nagłówka IPv4 w pole Traffic Class nagłówka IPv6 (IPv4->IPv6 Header Translation) i wartości Traffic Class w pole ToS przy translacji IPv6 na IPv4 (IPv6->IPv4 Header Translation).

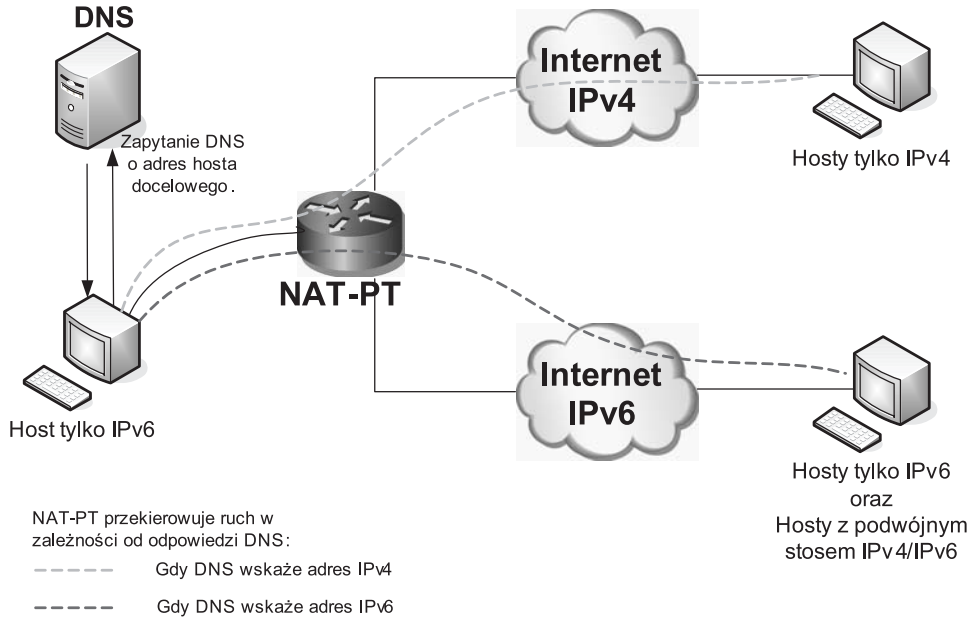
SIIT jest rekomendowany dla małych sieci i prawdopodobnie z powodu zastosowanego sposobu mapowania adresów IPv4 na IPv6 stanie się bezużyteczny, gdy Internet zacznie bazować na protokole IPv6 i łączyć nieliczne sieci z protokołem IPv4.

NAT-PT

Jako przykład szczególnie przydatnego, a zarazem przejrzystego rozwiązania translatora IPv4/IPv6, wymienić można NAT-PT (Network Address Translation – Protocol Translation). Protokół zdefiniowany został w dokumencie RFC 2766 („Network Address Translation – Protocol Translation"). Działanie NAT-PT wzorowane jest na rozwiązaniu NAT dla sieci IPv4. W porównaniu z SIIT, NAT-PT umożliwia komunikowanie się wielu węzłów IPv6 z węzłami IPv4 z wykorzystaniem pojedynczego, wspólnego adresu IPv4.

Translacja protokołów przy posługiwaniu się adresami w postaci mnemonicznej odbywa się z użyciem zapytań kierowanych do serwera DNS ALG (Application Level Gateway). Dla hostów nawiązujących połączenie translacja jest zupełnie niewidoczna. Host z adresem IPv6 odpytuje serwer DNS ALG o adres drugiego hosta. Jeśli adresem docelowym jest również adres IPv6, nawiązywana jest bezpośrednia komunikacja. Jeżeli natomiast okaże się, że host docelowy znajduje się w sieci IPv4,

wówczas transmisja kierowana jest automatycznie do niego poprzez NAT-PT, który w odpowiedni sposób podmienia nagłówki pakietów. Również NAT-PT powinien być postrzegany jako rozwiązanie przejściowe. Dopóki jednak Internet będzie zdominowany przez IPv4, NAT-PT wydaje się być dobrym narzędziem translacji. Rysunek 11 ilustruje sieć z NAT-PT.



Rys. 11. Integrowanie sieci IPv4 z IPv6 z użyciem protokołu NAT-PT

Translacja z wykorzystaniem NAT-PT jest dwukierunkowa i może być zainicjowana przez węzeł używający IPv4 lub IPv6, a translator, co istotne z punktu widzenia realizacji systemu QoS, transluje nagłówek zawierający pole określające priorytet pakietu do formatu nagłówka stosowanego w sieci docelowej, tak jak translator SIIT.

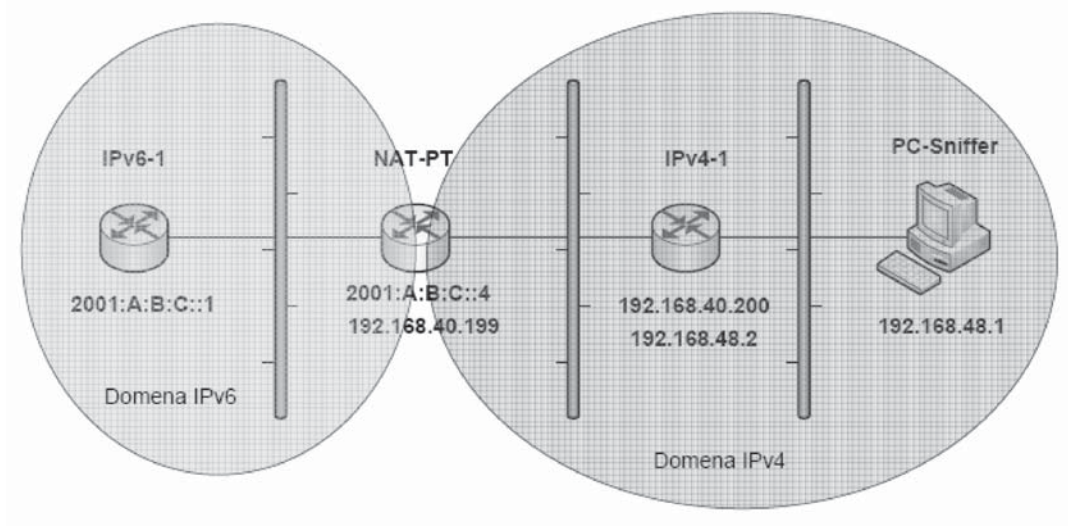
4. BADANIE SYSTEMU KLASYFIKOWANIA PAKIETÓW Z WYKORZYSTANIEM NAT-PT

W niniejszym rozdziale przedstawione zostały wyniki badania systemu klasyfikowania pakietów w sieci wykorzystującej translator NAT-PT. Działanie klasyfikatora zweryfikowane zostało dla przypadku statycznej translacji NAT-PT i translacji dynamicznej IPv4-to-IPv6. Dla prostej sieci LAN poddano klasyfikowaniu pakiety związane z protokołem telnet i WWW. Pakiety przenoszone były z systemu bazującego na protokole IPv4 i translowane przez NAT-PT do formatu pakietów IPv6.

Klasyfikowanie pakietów i przypisywanie im wybranych wartości pola DSCP ma charakter czysto poglądowy i miało posłużyć weryfikowaniu przepisywania przez translator NAT-PT wartości tego pola do pola Traffic Class pakietów IPv6.

Topologia badanej sieci i konfiguracja NAT-PT

Topologia badanej sieci przedstawiona została na rysunku 12.



Rys. 12. Domeny IPv4 i IPv6 połączone przez NAT-PT

Konfiguracja interfejsów translatora adresów przedstawia się następująco:

```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:A:B:C::4/64
 ipv6 nat
 service-policy input QoS_Policy
!
interface FastEthernet0/1
 ip address 192.168.40.199 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
!
ip route 192.168.48.0 255.255.255.0 192.168.40.200
no ip http server
no ip http secure-server
!
```

Kolejny zrzut ekranu obrazuje w jaki sposób dokonywana jest przez translator NAT-PT statyczna translacja adresów.

```
NAT-PT#show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.40.200           2001::C0A8:28C8

---   ---                      ---
      192.168.48.1             2001::C0A8:28C9

---   ---                      ---
      192.168.48.2             2001::C0A8:28CA

---   192.168.50.1             2001:A:B:C::1
      192.168.48.1             2001::C0A8:28C9

---   192.168.50.1             2001:A:B:C::1
      ---                      ---
```

Polecenia konfiguracyjne użyte w trakcie konfigurowania translatora, znajdujące odzwierciedlenie w pliku konfiguracyjnym routera o nazwie NAT-PT to:

```
!
ipv6 nat v4v6 source 192.168.40.200 2001::C0A8:28C8
ipv6 nat v4v6 source 192.168.48.1 2001::C0A8:28C9
ipv6 nat v4v6 source 192.168.48.2 2001::C0A8:28CA
ipv6 nat v6v4 source 2001:A:B:C::1 192.168.50.1
ipv6 nat prefix 2001::/96
!
!
!
!
ipv6 access-list telnet
 permit tcp host 2001:A:B:C::1 eq telnet any
!
ipv6 access-list www
 permit tcp host 2001:A:B:C::1 eq www any
!
ipv6 access-list icmp
 permit icmp host 2001:A:B:C::1 any echo-reply
!
```

Jak widać, wyciąg z pliku konfiguracyjnego przedstawia zapisy w trzech lista kontroli dostępu dla protokołu IPv6 o nazwach: telnet, www i icmp. Listy te zostały użyte do wskazania jakie pakiety będą identyfikowane i oznaczane przez NAT-PT. Klasyfikowaniu będą podlegały pakiety płynące z routera IPv6 do sieci IPv4 (any). Pakiety te będą stanowiły odpowiedź na ruch zainicjowany z hosta o nazwie PC,

z domeny IPv4. Identyfikowanie pakietów i ich oznaczanie będzie realizowane po stronie domeny IPv6, na wejściu interfejsu Fa0/0 routera NAT-PT.

Poniżej przedstawiona została przykładowa konfiguracja class-map dla ruchu IPv6 związanego z protokołami telnet, www i icmp oraz konfiguracja zasad oznaczania pakietów, tzw. policy-mapa, aplikowana na wejściu interfejsu Fa0/0 NAT-PT.

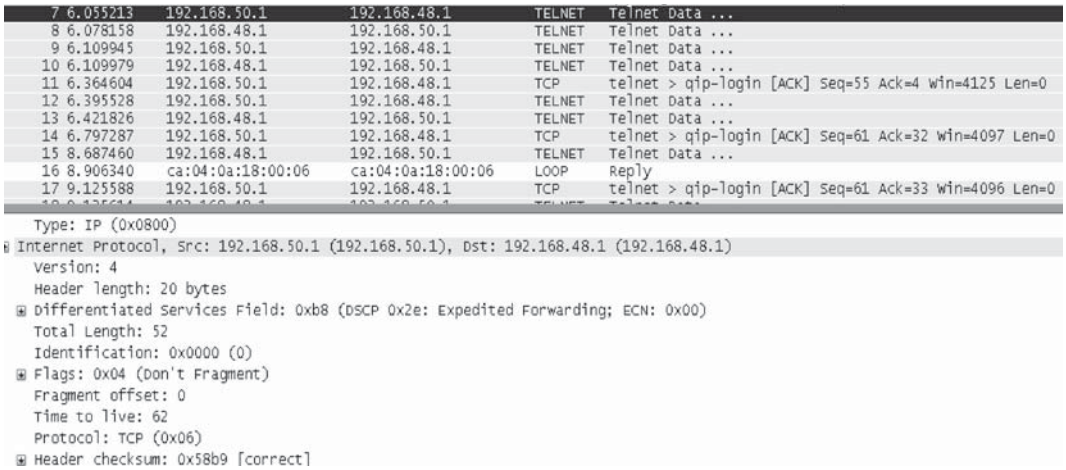
```
class-map match-all MatchWWW
 match protocol ipv6
 match access-group name www
class-map match-all MatchICMP
 match protocol ipv6
 match access-group name icmp
class-map match-all MatchTelnet
 match protocol ipv6
 match access-group name telnet
!
!
policy-map QoS_Policy
 class MatchTelnet
  set dscp ef
 class MatchWWW
  set dscp af41
 class MatchICMP
  set dscp af43
 class class-default
  set dscp default
!
```

Poprawność działania translatora potwierdzona została na drodze debugowania pakietów przesyłanych pomiędzy domenami IPv6 i IPv4. Wynik debugowania przedstawiony został poniżej.

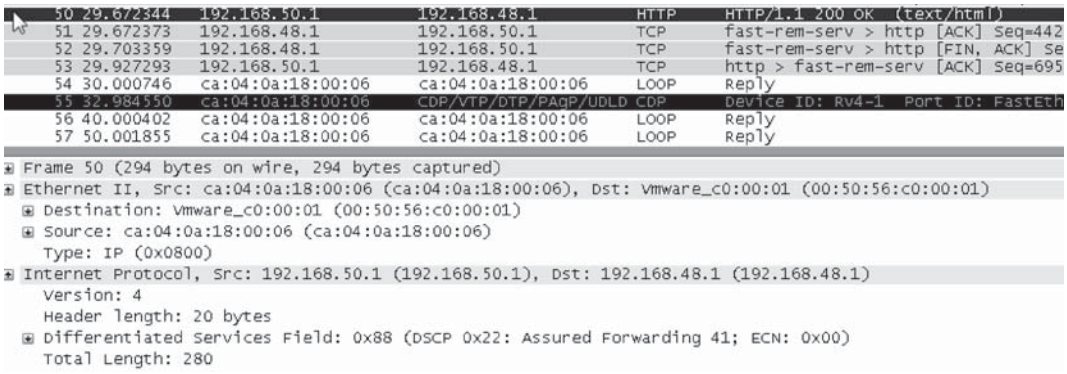
```
NAT-PT#debug ipv6 nat
IPv6 NAT-PT debugging is on
NAT-PT#
*Mar 30 14:29:01.011: IPv6 NAT:  src (192.168.48.1) -> (2001::C0A8:28C9), dst (1
92.168.50.1) -> (2001:A:B:C::1)
*Mar 30 14:29:01.135: IPv6 NAT: icmp src (2001:A:B:C::1) -> (192.168.50.1), dst
(2001::C0A8:28C9) -> (192.168.48.1)
NAT-PT#
*Mar 30 14:29:02.555: IPv6 NAT:  src (192.168.48.1) -> (2001::C0A8:28C9), dst (1
92.168.50.1) -> (2001:A:B:C::1)
*Mar 30 14:29:02.855: IPv6 NAT: icmp src (2001:A:B:C::1) -> (192.168.50.1), dst
(2001::C0A8:28C9) -> (192.168.48.1)
*Mar 30 14:29:03.515: IPv6 NAT:  src (192.168.48.1) -> (2001::C0A8:28C9), dst (1
92.168.50.1) -> (2001:A:B:C::1)
NAT-PT#
*Mar 30 14:29:03.587: IPv6 NAT: icmp src (2001:A:B:C::1) -> (192.168.50.1), dst
(2001::C0A8:28C9) -> (192.168.48.1)
*Mar 30 14:29:04.259: IPv6 NAT:  src (192.168.48.1) -> (2001::C0A8:28C9), dst (1
92.168.50.1) -> (2001:A:B:C::1)
*Mar 30 14:29:04.383: IPv6 NAT: icmp src (2001:A:B:C::1) -> (192.168.50.1), dst
(2001::C0A8:28C9) -> (192.168.48.1)
NAT-PT#_
```

Kolejny zrzut ekranu przedstawia zawartość pakietu IPv4 odebranego przez host o nazwie PC, a będącego odpowiedzią na zainicjowaną na hoście sesję telnet

z routerem o nazwie Rv6-1. Jak widać, odebrany pakiet został sygnowany wartością 0x2e pola DSCP (Expedited Forwarding), co potwierdza prawidłowe działanie klasyfikatora pakietów i mechanizmu translacji nagłówka pakietu IPv6 na nagłówek pakietu IPv4.



Podobnie przedstawia się sytuacja w przypadku wykorzystania protokołu http. Tutaj pakiet http odpowiedzi routera Rv6-1 oznaczony został wartością 0x22 (af41) pola DSCP.



Podobny eksperyment przeprowadzony został dla przypadku translacji dynamicznej i klasyfikowaniu pakietów płynących z domeny IPv4 do domeny IPv6.

Konfiguracja dynamicznej translacji NAT-PT (kierunek v4-to-v6) przedstawia się następująco:

```
!
ip access-list extended nat-list2
 permit ip any any
!
logging alarm informational
!
!
ipv6 nat v4v6 source list nat-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001::C0A8:28C8 2001::C0A8:28C9 prefix-length 128
ipv6 nat v6v4 source 2001:A:B:C::1 192.168.50.1
ipv6 nat prefix 2001::/96
!
!
```

Tak jak dla przypadku translacji statycznej, zaproponowane zostały dwie listy ACL, służące wskazaniu jaki ruch powinien być klasyfikowany. Listy te noszą nazwy telnet i www i określają strumień pakietów IPv4 przenoszący ruch związany z protokołami telnet i www, płynący z hosta PC do routera IPv6 (z adresem 192.168.50.1 po translacji).

```
ip access-list extended telnet
 permit tcp host 192.168.48.1 host 192.168.50.1 eq telnet
ip access-list extended www
 permit tcp host 192.168.48.1 host 192.168.50.1 eq www
!
```

Class-mapy oraz zasady oznaczania pakietów (policy-map o nazwie QoS_Policy) przedstawia wyciąg z pliku konfiguracyjnego routera NAT-PT zamieszczony poniżej.

```
!
class-map match-all MatchWWW
 match protocol ip
 match access-group name www
class-map match-all MatchTelnet
 match protocol ip
 match access-group name telnet
!
!
policy-map QoS_Policy
 class MatchTelnet
  set dscp ef
 class MatchWWW
  set dscp af41
 class class-default
  set dscp default
!
```

W tym przypadku polisa o nazwie QoS_Policy aplikowana jest na interfejsie fa0/1, po stronie domeny IPv4 i dotyczy ruchu wejściowego (z domeny IPv4).

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:A:B:C::4/64
 ipv6 nat
!
interface FastEthernet0/1
 ip address 192.168.40.199 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
 service-policy input QoS_Policy
!
```

Poniżej przedstawiony został wydruk potwierdzający zgodne z oczekiwaniami klasyfikowanie pakietów IPv4. Wynik użycia polecenia show policy-map interface pokazuje ile pakietów danego typ zostało sklasyfikowanych i jaką wartością pola DSCP oznaczonych.

```
NAT-PT#sh policy-map interface
 FastEthernet0/1

  Service-policy input: QoS_Policy

    Class-map: MatchTelnet (match-all)
      77 packets, 4296 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ip
      Match: access-group name telnet
      QoS Set
        dscp ef
          Packets marked 77

    Class-map: MatchWWW (match-all)
      224 packets, 13084 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ip
      Match: access-group name www
      QoS Set
        dscp af41
          Packets marked 224
```

Nieco inaczej przedstawiał się w tym przypadku sposób sprawdzania, że sklasyfikowane na wyjściu domeny IPv4 pakiety docierają do domeny IPv6 i charakteryzują się przypisaną przez klasyfikator wartością pola DSCP (Traffic Class w domenie IPv6). W domenie IPv6, na routerze Rv6-1 utworzona została lista ACL, a jej przeznaczeniem miało być zliczanie pakietów docierających do Rv6-1 charakteryzujących się wartością ef (dla ruchu telnet) i af41 (dla ruchu www) pola DSCP. Poniżej przedstawiony został wydruk potwierdzający poprawność działania klasyfikatora.

```
Rv6-1#clear access-list counters

Rv6-1#sh access-lists
IPv6 access list dscp
    permit ipv6 any host 2001:A:B:C::1 dscp ef log sequence 10
    permit ipv6 any host 2001:A:B:C::1 dscp af41 log sequence 20
    permit ipv6 any any sequence 30
Rv6-1#
*Mar 30 17:30:12.807: %IPV6-6-ACCESSLOGP: list dscp/10 permitted tcp 2001::C0A8:
28C8(2833) -> 2001:A:B:C::1(23), 1 packet
Rv6-1#
*Mar 30 17:30:40.215: %IPV6-6-ACCESSLOGP: list dscp/20 permitted tcp 2001::C0A8:
28C8(2850) -> 2001:A:B:C::1(80), 1 packet
Rv6-1#
*Mar 30 17:30:43.231: %IPV6-6-ACCESSLOGP: list dscp/20 permitted tcp 2001::C0A8:
28C8(2852) -> 2001:A:B:C::1(80), 1 packet
Rv6-1#
*Mar 30 17:30:47.043: %IPV6-6-ACCESSLOGP: list dscp/20 permitted tcp 2001::C0A8:
28C8(2853) -> 2001:A:B:C::1(80), 1 packet
Rv6-1#sh access-lists
IPv6 access list dscp
    permit ipv6 any host 2001:A:B:C::1 dscp ef log (44 matches) sequence 10
    permit ipv6 any host 2001:A:B:C::1 dscp af41 log (28 matches) sequence 20
    permit ipv6 any any (5 matches) sequence 30
Rv6-1#
```

5. PODSUMOWANIE

Wyniki przeprowadzonych w środowisku sieci laboratoryjnej badań dowodzą zgodnego z oczekiwaniem działania translatora NAT-PT. Badanie polegało na klasyfikowaniu pakietów IPv6/IPv4 przesyłanych do domeny IPv4/IPv6. Wykorzystany w pracy sniffer potwierdził, że pole TrafficClass/DSCP przepisywane jest poprawnie w pole DSCP/TrafficClass translowanego pakietu. Weryfikacja poprawności działania translatora pakietów jest istotna z punktu widzenia wstępnej klasyfikacji pakietów w systemie końcowym (domeny IPv6 lub IPv4), będącym źródłem ruchu podlegającego regułom ustalonym w zastosowanym systemie QoS.

Literatura

1. *Deploying IPv6 in Branch Networks* – dokumentacja techniczna Cisco
2. T. Rooney, *IPv4-to-IPv6 Transition Strategies*, BT Diamond IP Whitepaper, 2007
3. *Enterprise QoS Solution Reference Network Design Guide* – dokumentacja techniczna Cisco
4. R. Desmeules, *IPv6: Sieci oparte na protokole IP w wersji 6*, Wyd. Mikom, 2006
5. S. Hogg, E. Vyncke, *IPv6 Security*, Cisco Press, 2009