Dariusz ŻELASKO[1]

Politechnika Krakowska, Instytut Teleinformatyki (1)

Policy-Based Routing na przykładzie systemu Vyatta

Streszczenie. *W artykule tym przedstawiona została technika, która umożliwia administratorowi sieci definiowanie reguł routingu opierających się na informacjach zawartych w nagłówku pakietu. W odróżnieniu od klasycznych technik routing decyzje nie są podejmowane wyłącznie na podstawie adresu docelowego. Dzięki tej technice administrator ma możliwość samodzielnego kierowania ruchu sieciowego w oparciu o pewne samodzielnie zdefiniowane zasady. W artykule omówione zostały również inne techniki, które często mylone są z Policy-Based Routing (PBR). Przykład wykorzystania techniki PBR przedstawiony został z wykorzystaniem programowego routera Vyatta. Również oprogramowaniu Vyatta został poświęcony fragment artykułu tak aby możliwym było zrozumienie zaprezentowanego przykładu.*

Abstract. *In this article technique which provides to administrator ability of defining different routing rules based on information from packet header was presented. In contrast to the classical routing techniques decisions are not based only on the destination address. With this technique administrator has ability to self-manage network traffic routing on the basis of self-established rules. In this article also some other techniques were presented which are often mistaken with Policy-Based Routing technique (PBR). An example of use of PBR technique was presented on Vyatta software router. To make it easier to understand the example Vyatta router was also described in this article.* ***(Policy-Based Routing on the example of Vyatta system)***

Słowa kluczowe: Vyatta, Policy-Based Routing, Source-Based Routing, Source Routing, Dynamic Source Routing
Keywords: Vyatta, Policy-Based Routing, Source-Based Routing, Source Routing, Dynamic Source Routing

doi:10.12915/pe.2014.08.11

Wstęp

W przypadku tradycyjnych protokołów routingu decyzje dotyczące przekazania pakietu podejmowane są na podstawie adresu docelowego znajdującego się w nagłówku pakietu. Tego typu rozwiązanie oznacza, iż wszystkie pakiety mające ten sam cel będę podróżowały tą samą trasą. W artykule tym zaprezentowana została technika Policy-Based Routing (PBR), która umożliwia podejmowanie decyzji dotyczących przekazywania pakietów nie tylko na podstawie adresu docelowego ale również na podstawie innych informacji zawartych w nagłówku pakietu. Podejście takie pozwala administratorowi samodzielnie definiować trasy, którymi przesyłane będą pakiety. Dzięki temu możliwym jest kształtowanie ruchu i regulacja obciążenia na poszczególnych łączach. PBR jest bardzo przydatne w momencie gdy w sieci występuje kilka połączeń do sieci WAN. Wówczas administrator może samodzielnie zdefiniować, którymi łączami przekazane zostaną pakiety pochodzące z różnych źródeł. Tego typu podejście może posłużyć do uzależnienia wysokości wnoszonych przez użytkowników opłat od trasy, którą podróżują ich pakiety. Kolejnym przypadkiem w którym można wykorzystać PBR jest równoważenie obciążenia z wykorzystaniem połączeń zestawianych na żądanie. W momencie gdy w sieci znacząco podnosi się natężenie ruchu możliwym jest zestawienie dodatkowego połączenia (np. ISDN), którym może zostać przekazana część ruchu. W takim wypadku PBR wykorzystane zostanie do zrównoważenia obciążenia - część pakietów przesłana zostanie dodatkowym łączem. Jeśli tego typu skok natężenia jest okresowy i można przewidzieć kiedy nastąpi reguły PBR można tak skonfigurować aby działały wyłącznie w określonym czasie. Podejście takie pozwoli zaoszczędzić pieniądze ponieważ dodatkowe połączenie zestawiane jest okresowo i nie ma konieczności stałego utrzymywania go.

Często zdarza się, iż PBR jest mylona z innymi technikami. W związku z tym w artykule, poza PBR, zaprezentowane zostały również dwie inne techniki - Source Routing (SR) i Dynamic-Source Routing (DSR). Konfiguracja PBR zaprezentowana została z wykorzystaniem programowego routera Vyatta. Główną zaletą oprogramowania Vyatta jest to, iż w podstawowej wersji jest ono darmowe. Ma to bardzo duże znaczenie ponieważ dzięki temu stanowi ono alternatywę dla rozwiązań komercyjnych. Rozwiązania płatne takie jak np. Cisco są zazwyczaj dość drogie co często uniemożliwia zastosowanie ich. Wynika to głównie z faktu, iż środki przeznaczone na budowę sieci nie pozwolą na zakup rozwiązań komercyjnych. Dodatkowo rozwiązania komercyjne zazwyczaj posiadają wiele innych funkcjonalności, które niekoniecznie będą wykorzystywane, a są elementem za który musimy zapłacić. W artykule tym opisane zostały również główne funkcjonalności systemu Vyatta tak aby przybliżyć jego możliwości i zastosowania. W przypadku tego artykułu techniki routingu rozważane są pod kątem IPv4. Zaprezentowany został również przykład konfiguracji PBR na routerze Vyatta. Przykład ten umożliwia stosowanie różnych tras w zależności od źródła i celu transmisji.

Source Routing

Source Routing (SR) jest techniką wykorzystywaną głównie w sieciach Token Ring. Opiera się na zasadzie, iż źródło transmisji samo określa trasę po jakiej transmisja ma się odbyć wraz z wyszczególnieniem wszystkich węzłów pośredniczących. Głównym założeniem było umożliwienie diagnozowania problemów w sieci właśnie poprzez wysyłanie pakietów określonymi ścieżkami - dzięki temu możliwym było stwierdzenie w którym miejscu sieci pojawiają się problemy z transmisją.

W przypadku source routing wykorzystywane są dwie opcje:

- SSRR (ang. strict source and record route) - zdefiniowanie ścieżki, którą ma iść pakiet,
- LSRR (ang. loose source route and record route) - zdefiniowanie węzłów przez które ma przejść pakiet.

SR pozwala także na wyszukiwanie optymalnych tras. Przykładowo jeśli istnieje kilka tras dotarcia do danego miejsca w sieci możliwym jest wysłanie kilku pakietów w których zdefiniowane zostaną różne trasy. Następnie na podstawie czasu transmisji ze źródła do celu można ocenić poszczególne trasy i wybrać tę najbardziej optymalną dla danego zastosowania.

Dynamic Source Routing

DSR jest protokołem routingu stworzonym dla rozproszonych sieci bezprzewodowych. Protokół może również funkcjonować w sieciach komórkowych. Ścieżka tworzona jest na żądanie w momencie gdy jest potrzebna. Sieć wykorzystująca DSR może skonfigurować się samodzielnie. W tej technice na podstawie źródła definiowana jest ścieżka która powinna zostać wykorzystana w trakcie transmisji. W

pierwszej kolejności uzyskiwana jest informacja o wszystkich ścieżkach. Następnie ścieżki te wykorzystywane są w transmisji.

Policy-Based Routing

Policy-Based Routing jest techniką umożliwiającą podejmowanie decyzji dotyczących routingu na podstawie reguł definiowanych przez administratora. Dzięki temu administrator ma możliwość samodzielnego kierowania ruchem w sieci. W klasycznym routingu w momencie gdy router odbierze pakiet sprawdzany jest adres docelowy w pakiecie IP. Następnie w oparciu o ten adres przeszukiwana jest tablica routingu routera w poszukiwaniu wpisu odpowiadającego sieci docelowej. Gdy odpowiedni wpis zostanie znaleziony pakiet zostaje przekazany do routera następnego skoku lub sieci docelowej. W przypadku PBR decyzje dotyczące przekazania pakietu mogą bazować nie tylko na adresie docelowym ale również na adresie źródłowym, rozmiarze pakietu, porcie źródłowym i docelowym oraz innych informacjach, które dostępne są w nagłówku pakietu.

Podstawą PBR jest możliwość definiowania wielu tablic routingu - wybierana jest tablica routingu na podstawie której następuje trasowanie pakietów spełniających określone reguły. W ten sposób można definiować inne tablice routingu dla różnych sieci źródłowych, a nawet poszczególnych użytkowników. Czasami Policy-Based Routing nazywane jest również Source-Based Routing czego nie należy mylić z techniką Source Routing, która opisana została we wcześniejszej części tego artykułu.

W artykule [3] przedstawione zostały najbardziej popularne techniki zapewniania jakości w sieciach. Metody te wymagają modyfikowania pakietów (ustawiania odpowiednich opcji) i stosowania urządzeń sieciowych, które są w stanie odpowiednio przetworzyć pakiety. Powoduje to znaczący wzrost kosztów wdrożenia tego typu rozwiązań. W stosunku do powyższych technik główną zaletą PBR jest to, iż nie wymaga ono modyfikowania pakietów (jest to możliwe ale nie konieczne). Wszystkie decyzje podejmowane są na podstawie informacji zawartych w pakietach pochodzących bezpośrednio od klientów bez jakichkolwiek modyfikacji i bez konieczności stosowania specjalizowanych urządzeń.

Vyatta

PBR stosowany jest w rozwiązaniach komercyjnych. Rozwiązania takie bywają dość kosztowne i w związku z tym nie każdy jest w stanie zakupić tego typu sprzęt. Od niedawna PBR dostępny jest również w rozwiązaniach darmowych routerów programowych, spośród których na szczególną uwagę zasługuje Vyatta - przede wszystkim ze względu na oferowane funkcjonalności. Vyatta to programowy router, firewall i VPN dla sieci IPv4 i IPv6. Pierwsza darmowa wersja systemu wydana została w 2006 roku. Vyatta zbudowana została na bazie darmowego oprogramowania (m.in. Quagga). System Vyatta może być obsługiwany zdalnie poprzez SSH, Telnet, SNMP i interfejs WWW. Do usług, które mogą być świadczone przez system zaliczyć można DHCP, DHCPv6, NAT. System obsługuje interfejsy takie jak Ethernet, łącza bezprzewodowe, łącza szeregowe, DSL. Pozwala również na pracę z wirtualnymi sieciami lokalnymi (VLAN). Możliwym jest wykorzystanie enkapsulacji HDLC, Frame Relay, PPP oraz PPPoA i PPPoE. Jednym z głównych zadań systemu Vyatta jest trasowanie pakietów.

W ramach Vyatta poza routingiem statycznym wykorzystać można następujące protokoły routingu:

- RIP (przy czym jest to protokół określany jako RIPv2),
- RIPng (RIP dla IPv6),
- OSPF (dla IPv4 i IPv6),
- BGP.

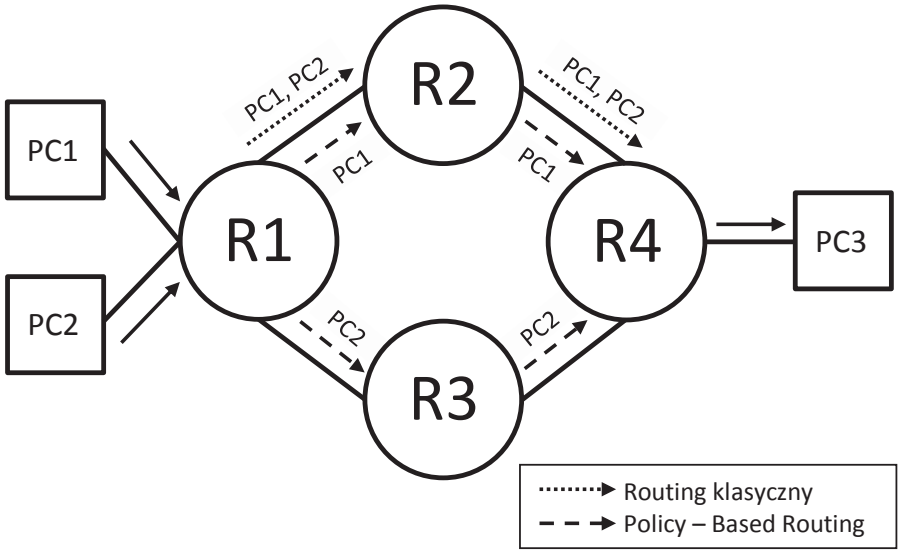
Kolejną istotną funkcjonalnością systemu Vyatta jest możliwość konfigurowania PBR. Funkcja ta pojawiła się pierwszy raz w wersji 6.5. Ważnym aspektem tego systemu jest również bezpieczeństwo. System Vyatta można wykorzystać jako Firewall (zarówno dla IPv4 jak i IPv6), do filtrowania stron WWW oraz do VPN. Vyatta wspiera również QoS poprzez możliwość kształtowania ruchu. algorytmy kolejkowania oraz unikanie przeciążeń sieci. Dodatkowo dostępnych jest kilka mechanizmów zapewniających niezawodną pracę systemu i wszystkich usług.

Vyatta w dużej mierze zależy od sprzętu na jakim zostanie uruchomiona. Problemem może okazać się dostępność interfejsów. W przypadku zwykłego Ethernetu nie ma większych przeszkód ponieważ każdy komputer można wyposażyć bez problemów w kilka interfejsów Ethernet. Natomiast w przypadku interfejsów typowych dla WAN (np. G.703, V.35, STM1) pojawia się pewna komplikacja. Należy stosować specjalizowane karty rozszerzeń lub konwertery pomiędzy różnymi standardami. Niedogodnością może okazać się instalacja tego typu kart w systemie. Jeśli chodzi o główną zaletę systemu Vyatta to należy tu wymienić bardzo niski koszt uruchomienia - oprogramowanie w podstawowej wersji jest darmowe. Główną rzeczą, którą należy przemyśleć jest konfiguracja techniczna komputera na którym system ma zostać uruchomiony. Konfiguracja zależy od natężenia ruchu w sieci, który ma zostać obsłużony. Sam system można uruchomić na stosunkowo prostych maszynach.

PBR i Vyatta

W systemie Vyatta PBR dostarcza dwie główne funkcjonalności - przesyłanie pakietów różnymi ścieżkami (alternatywny routing) oraz oznaczanie lub modyfikowanie pakietów przed przekazaniem. Bardzo istotną rzeczą jest to, iż w systemie Vyatta filtrowanie oparte o PBR działa dla ruchu przychodzącego. W momencie gdy w systemie nie zdefiniowano reguł PBR wszystkie decyzje dotyczące routingu podejmowane są na podstawie podstawowej tablicy routingu. Przy czym przez pojęcie tablica routingu należy rozumieć tablicę utworzoną przez wszystkie wykorzystywane protokoły routingu. Gdy wykorzystywany jest PBR to cały przychodzący ruch sieciowy jest w pierwszej kolejności filtrowany w oparciu o zdefiniowane reguły, a następnie jest przetwarzany zgodnie z wybranymi regułami.

Na rysunku 1 przedstawiono przykładową sieć, która posłuży do wyjaśnienia sposobu działania PBR. W przypadku klasycznego routingu niezależnie od źródła transmisji pakiety podróżują tą samą trasą - trasa ta może zostać zdefiniowana ręcznie przez administratora (routing statyczny) lub wybrana przez protokół routingu dynamicznego. W odniesieniu do omawianego schematu w przypadku routingu statycznego w momencie, gdy PC1 rozpocznie transmisję do PC3 pakiety będą podróżowały poprzez router R1 - R2 - R4 aż do osiągnięcia celu. Gdy w systemie nie jest wykorzystywany PBR w przypadku, gdy PC2 rozpocznie transmisję danych do PC3 to pakiety zostaną przesłane dokładnie tą samą trasą (R1 - R2 - R4). Z kolei gdy w systemie wykorzystywany jest PBR możliwym jest zdefiniowanie różnych tras w zależności od źródła transmisji. Przykładowo administrator może zdefiniować takie reguły, iż transmisja między PC1 a PC3 odbywać się będzie trasą R1 - R2 - R4. Z kolei transmisja między PC2 a PC3 odbywać się będzie za pośrednictwem routerów R1 - R3 - R4. Tego typu rozdzie-



Rys. 1: Przykładowa sieć

lenie transmisji pozwala definiować trasy w zależności np. od potrzeb konkretnych użytkowników lub od ról poszczególnych urządzeń w sieci - przykładem takiego urządzenia, które powinno działać na specjalnych zasadach może być serwer świadczący różnego rodzaju usługi. PBR umożliwia administratorowi dość swobodnie kształtować ruch i sterować obciążeniem poszczególnych łączy.

W systemie Vyatta pakiety mogą być filtrowane na podstawie typu protokołu, źródłowego i docelowego adresu IP lub portu, fragmentacji, typu ICMP lub ICMPv6, stanu łącza, flag TCP i informacji czy pakiet jest pakietem IPSec. Vyatta umożliwia również definiowanie grup adresów, portów lub sieci do których mogą odwoływać się reguły. Tak jak już to zostało wspomniane wcześniej Vyatta dostarcza dwie funkcjonalności: alternatywny routing i oznaczanie/modyfikowanie pakietów. W przypadku alternatywnego routingu w momencie gdy pakiet jest zgodny z regułą następuje jego przesłanie w oparciu o alternatywną (inną niż główna) tablicę routingu. Oznaczanie pakietów lub ich modyfikacja polega na tym, iż pakiety zgodne z regułą mogą mieć np. ustawione pole DSCP lub zmodyfikowane pole TCP MSS. Reguły ustawiane są na konkretnych interfejsach - tych na których filtrowanie pakietów przychodzących jest niezbędne.

Najbardziej istotnym poleceniem z punktu widzenia PBR w systemie Vyatta jest:

set policy route NAZWA rule NUMER

Nazwa reguły oraz numer będą wykorzystywane w całym procesie konfiguracji. Numer reguły może być z przedziału 1-9999. Przedstawiona komenda nie jest kompletna i wymaga uzupełnienia. Skorzystać można z następujących opcji:

- destination - odpowiada za ustawienie reguł dla adresu docelowego pakietu
  - address - należy podać adres IP w formacie IP, IP/maska lub IP-początkowe - IP-końcowe dla zakresu. Możliwa jest również negacja adresu. Wówczas adres należy poprzedzić ***!***. Tego typu zapis oznaczać będzie, że reguła ta ma być stosowana dla wszystkich adresów z wyjątkiem tego wyszczególnionego
  - port - należy podać port lub porty w formacie port1, port2, port3, ... Grupę zanegować można dodając ***!*** na początek. Należy pamiętać, iż jest to negacja całej grupy portów
- icmp - dla reguł dotyczących ICMP
  - code - kod ICMP, zakres od 0 do 255
  - type - typ ICMP, zakres od 0 do 255
  - type-name - nazwa typu ICMP. Przykładowo echo-reply, echo-request
- log
  - enable - uruchomienie rejestrowania informacji o pakietach zgodnych z regułą
  - disable - wyłączenie
- set - służy do modyfikowania pakietów
  - dscp - ustawienie pola DSCP. Wartość 0-63
  - mark - znakowanie pakietu (1-2147483647)
  - table - tablica routingu, która ma zostać wykorzystana do przekazania pakietu. Możliwe wartości to 1-200 lub main co oznacza główną tablicę routingu
- source - odpowiada za ustawienie reguł zależnych od adresu źródłowego pakietu
  - address - adres źródłowy, format taki jak opcja destination address
  - port - port źródłowy, format taki jak opcja destination port
  - mac-address - źródłowy adres MAC. Adres należy podać w postaci aa:bb:cc:dd:ee:ff. Możliwym jest również zanegowanie adresu poprzez podanie znaku ***!*** przed adresem. Wówczas reguła zostanie zastosowana dla wszystkich adresów z wyjątkiem tego wyszczególnionego
- tcp
  - flags - filtrowanie w zależności od flag TCP. Możliwe flagi to SYN, ACK, FIN, RST, URG, PSH, ALL. Ustawienie więcej niż jednej flagi możliwe jest w następującym formacie: flaga1, flaga2, flaga3, ... Możliwym jest również negowanie poszczególnych flag poprzez ustawienie ***!*** przed nazwą. Przykładowo zapis !flaga1, flaga2, !flaga3 oznacza, że pakiet spełni daną regułę gdy nie będzie miał ustawionej flagi 1 i flagi 3 oraz będzie miał ustawioną flagę 2
- time - służy do definiowania kiedy dana reguła ma być stosowana

  - monthdays - dzień miesiąca. Należy wymienić kolejne dni oddzielając je przecinkami. 5,10,23 oznacza, że reguła ma być stosowana wyłącznie piątego, dziesiątego i dwudziestego trzeciego dnia każdego miesiąca. Możliwym jest również zanegowanie pojedynczych dni. Uzyskać to można poprzedzając dany dzień znakiem ***!***
  - startdate - data od kiedy dana reguła ma być stosowana. Format to rrrr-mm-dd lub gdy jednocześnie chcemy określić konkretną godzinę rrrr-mm-ddTgg:mm:ss
  - startime - godzina rozpoczęcia stosowania reguły. Format gg:mm:ss
  - stopdate - data kiedy reguła ma przestać być stosowana. Format jest taki sam jak w przypadku startdate
  - stoptime - godzina zakończenia stosowania reguły. Format taki sam jak w przypadku starttime
  - weekdays - dni tygodnia kiedy reguła ma być stosowana. Format mon, thu, wed,... Można również zanegować poszczególne dni poprzedzając je symbolem ***!***
- action
  - drop - pakiet, który spełni daną regułę nie zostanie przesłany dalej
- disable - służy do wyłączenia danej reguły

Konfiguracja PBR w przypadku Vyatta sprowadza się do wydania poleceń będących kombinacją opcji przedstawionych powyżej. Poniższy przykład spowoduje ustawienie alternatywnego routingu (zależnego od adresu źródłowego i docelowego):

1. set policy route NAZWA - stworzenie polityki NAZWA.
2. set policy route NAZWA rule NUMER-REGUŁY destination address SIEĆ-DOCELOWA - utworzenie reguły o konkretnym numerze. Sieć docelowa pakietu musi być zgodna z tą, która została skonfigurowana aby dana reguła została zastosowana.
3. set policy route NAZWA rule NUMER-REGUŁY source address SIEĆ-ŹRÓDŁOWA - w ten sposób zdefiniowana zostanie sieć źródłowa dla której reguła ma zostać zastosowana. Ważne jest to, że nazwa i numer reguły muszą być zgodne z tymi skonfigurowanymi w poprzednich krokach.
4. set policy route NAZWA rule NUMER-REGUŁY set table NUMER-TABLICY - pakiety, które są zgodne z regułą zostaną przetworzone zgodnie z alternatywną tablicą routingu o zdefiniowanym numerze NUMER-TABLICY.
5. set protocols static table NUMER-TABLICY route SIEĆ-DOCELOWA nexthop NASTĘPNY-SKOK - spowoduje utworzenie wpisu w alternatywnej tablicy routingu, która wykorzystana zostanie w procesie trasowania pakietów.
6. set interfaces ethernet ethX address IP/maska - ustawienie adresu IP na konkretnym interfejsie sieciowym.
7. set interfaces ethernet ethX policy NAZWA - dzięki temu poleceniu stworzona polityka zostanie zastosowana na interfejsie ethX.

Powyższy przykład został opisany teoretycznie - bez podawania konkretnych wartości. Zaprezentowaną sekwencję komend należy zastosować na każdym routerze na którym ma działać PBR. Tego typu konfiguracja spowoduje, iż pakiety będą mogły podróżować różnymi trasami. Decyzje podejmowane będą na podstawie zdefiniowanych reguł, na podstawie których nastąpi wybór tablicy routingu.

Niestety dużym minusem PBR jest to, iż w przypadku awarii jakiegoś odcinka sieci trasy nie zostaną automatycznie zmodyfikowane - koniecznym będzie interwencja administratora i zdefiniowanie nowych reguł. Możliwym jest również zautomatyzowanie procesu przebudowywania reguł lecz wymaga to stworzenie wyspecjalizowanego oprogramowania, które mogłoby realizować tego typu zadanie.

Zakończenie

W artykule tym zaprezentowano PBR jako technikę stanowiącą alternatywę dla klasycznego routingu umożliwiającą w miarę swobodne kształtowanie ruchu w sieci. PBR przedstawiony został w oparciu o darmowy router programowy Vyatta. Technika ta stanowi alternatywę dla klasycznego routingu ponieważ to dzięki niej można uzależnić decyzje dotyczące kierowania pakietów od reguł bazujących na informacjach zawartych w nagłówku pakietu (adres źródłowy, adres docelowy, port). W związku z możliwością definiowania reguł administrator może samodzielnie sterować ruchem w sieci (trasowanie pakietów). W przypadku klasycznego routingu pakiety kierowane są wyłącznie w oparciu o adres docelowy pakietu. PBR może posłużyć do budowania sieci w których pakiety od źródeł takich jak klienci czy serwery posiadające ten sam cel transmisji będą podróżowały różnymi ścieżkami. Takie podejście umożliwi regulowanie natężenia ruchu na poszczególnych łączach i uzależnienie ścieżki od potrzeb danego źródła. W przypadku korzystania z PBR należy rozważyć możliwość zautomatyzowania procesu konfiguracji reguł. Niestety PBR w ramach systemu Vyatta nie posiada tego typu mechanizmów i w przypadku awarii któregoś fragmentu sieci reguły przestaną działać prawidłowo. Niezależnie od tego PBR jest bardzo użyteczną techniką z bardzo wieloma zastosowaniami.

LITERATURA

[1] Smith, B.R., Garcia-Luna-Aceves, J.J.: Efficient policy-based routing without virtual circuits, Quality of Service in Heterogeneous Wired/Wireless Networks, 2004. QSHINE 2004. First International Conference. Pages 242 - 251

[2] Nanda, P.: Supporting QoS Guarantees Using Traffic Engineering and Policy Based Routing, Computer Science and Software Engineering, 2008 International Conference. Pages 137 - 142

[3] Żelasko, D.: Współczesne technologie zapewniania jakości w sieciach komputerowych, Przegląd Elektrotechniczny, R.89 NR 8/2013. Strony 183 - 186.

[4] Boschi, E., Carle, G.: Active control architecture implementing policy-based routing, Telecommunications, 2003. ICT 2003. 10th International Conference. Pages 53 - 57 vol.1

[5] Chi-Kin Chau, Gibbens, R., Griffin, T.G.: Towards a Unified Theory of Policy-Based Routing INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Pages 1 - 12.

[6] `http://vyatta.org/` [Dostępne 26 stycznia 2014.].

***Autorzy**: Mgr inż. Dariusz Żelasko, Instytut Teleinformatyki, Wydział Fizyki, Matematyki i Informatyki, Politechnika Krakowska„ ul. Warszawska 24, 31-155 Kraków email: dzelasko@pk.edu.pl*