

STOSOWANIE QOS WRAZ Z PCQ W LABORATORIACH UCZELNIANYCH W CELU NADZOROWANEGO WSPÓLDZIELENIA DOSTĘPU DO LABORATORYJNYCH SERWERÓW PRZEZ STUDENTÓW

Tomasz MUCHOWSKI¹, Adam MUC², Adam SZELEZIŃSKI³

1. Student kierunku Informatyka, Uniwersytet Morski w Gdyni, Wydział Elektryczny
tel.: 535-427-765 e-mail: e.44349@student.amg.edu.pl
2. Uniwersytet Morski w Gdyni, Wydział Elektryczny, Katedra Automatyki Okrętowej
tel.: 504-449-932 e-mail: a.muc@we.umg.edu.pl
3. Uniwersytet Morski w Gdyni, Wydział Mechaniczny, Katedra Podstaw Techniki
tel.: 516-513-666 e-mail: a.szelezinski@wm.umg.edu.pl

Streszczenie: W pracy przedstawiono metodę konfiguracji sieci lokalnej na potrzeby laboratoriów komputerowych. Zastosowano QoS (ang. Quality of Service) z PCQ (ang. Per Connection Queuing) w celu zapewnienia studentom dostępu o równej przepustowości do serwerów laboratoryjnych. Metoda ta umożliwia zarówno priorytetyzację konkretnego ruchu sieciowego, ograniczanie przepustowości do konkretnych, z góry ustalonych wartości, jak i gwarantowanie prędkości transferu na poziomie przepływności pozostałych użytkowników. Metoda ta jest skalowalna i możliwa do zastosowania w większości routerów programowalnych.

Słowa kluczowe: QoS, PCQ, sieć, laboratorium, priorytetyzacja, współdzielenie zasobów

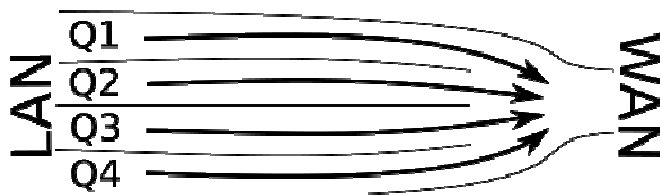
1. WSTĘP

QoS to narzędzie routera pozwalające na priorytetyzowanie ruchu sieciowego według określonych kryteriów, np. ruchu konkretnego użytkownika lub wybranego typu ruchu sieciowego tj. strumieniowanie wideo [1, 2]. QoS posiada także mechanizmy kontrolowanej rezerwacji zasobów. Mechanizmy te pozwalają na zagwarantowanie użytkownikom ustalonej prędkości transferu. Zapobiega to zawłaszczaniu ruchu sieciowego przez pojedynczych użytkowników [3, 4]. Jest to niekorzystne zjawisko, ponieważ znacznie obniża komfort lub wręcz uniemożliwia korzystanie z internetu, usług i zasobów sieciowych.

QoS pozwala na ograniczanie prędkości transferów konkretnym adresom IP (więc konkretnym użytkownikom) i całym podsieciami. Ograniczenia mogą być także nakładane na protokoły, porty i inne identyfikowalne parametry ruchu sieciowego (np. pakiety oznaczone poprzez zapórę sieciową).

W QoS ruch sieciowy opiera się na zapytaniach (ang. queue). Osobne zapytania obejmują ruch różnego typu, zdefiniowany przy tworzeniu zapytania. Wszystkie zapytania obsługiwane są jednocześnie, lecz istnieje opcja nadawania priorytetu poszczególnym zapytaniom i różnych ograniczeń. Oznacza to, że jeśli zdefiniujemy zapytanie, w którym znajdować będzie się ruch sieciowy konkretnego

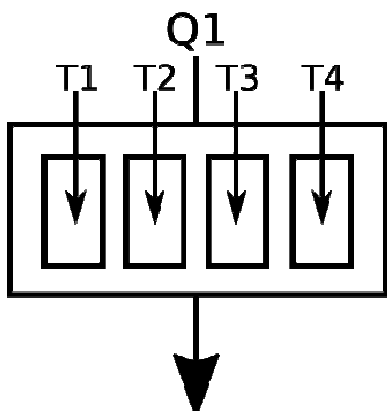
użytkownika i nadamy mu priorytet, to żądania sieciowe tego użytkownika wykonywane będą w pierwszej kolejności. Jeśli nadamy także inne ograniczenie, to użytkownik ten może posługiwać się np. większą przepustowością niż pozostali użytkownicy. Analogiczne działanie ma priorytet w przypadku zapytań zdefiniowanych dla portu, protokołu, itp. W takim przypadku żądania sieciowe na określonym porcie lub wykorzystujące określony protokół wykonywane będą w pierwszej kolejności. Na rysunku 1 przedstawiono schematyczne działanie QoS.



Rys. 1. Graficzna reprezentacja ruchu sieciowego, gdzie Q1, Q2, Q3 i Q4 to zapytania obejmujące ruch sieciowy różnego typu

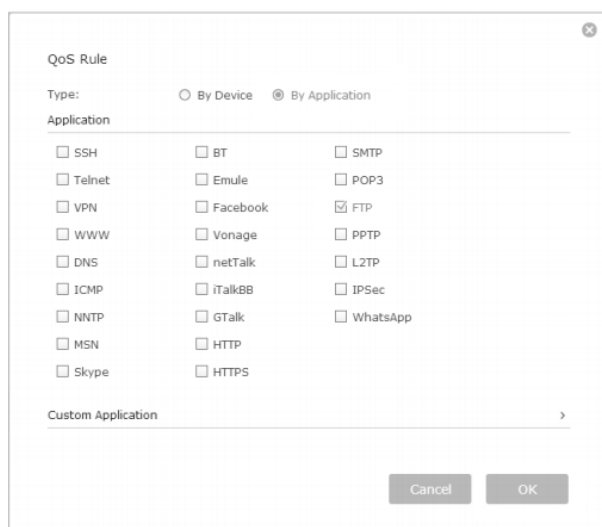
PCQ to mechanizm umieszczający ruch sieciowy wszystkich użytkowników w jednym zapytaniu, gdzie ruch sieciowy każdego z użytkowników stanowi osobne transmisje (zapytania zawarte w transmisjach określane są mianem pod-zapytań). W połączeniu z QoS mechanizm ten pozwala na lepsze zarządzanie ruchem sieciowym. Dzięki zastosowaniu PCQ te same ograniczenia i zasady nakładane możemy na każdą transmisję, nawet jeśli sama stanowi zapytanie. Pozwala to stworzyć konfigurację, w której możemy nakładać na pod-zapytanie zasady odnoszące się do poszczególnych użytkowników. Przykładowo, jeśli istnieje zapytanie, w którym QoS priorytetyzuje żądania na konkretnym porcie, a chciałoby się aby poszczególni użytkownicy posiadali inne ograniczenia, to należałoby utworzyć osobne zapytania. Zastosowanie PCQ ogranicza ilość tworzonych definicji zapytań i ułatwia konfigurację. Sama konfiguracja staje się znacznie bardziej skalowalna, ponieważ stworzone definicje zapytań można stosować do

nowo podłączonych do sieci komputerów - wystarczy jedynie nałożyć na przydzielone im adresy IP te same zasady PCQ. Na rysunku 2 zilustrowano działanie PCQ.



Rys. 2. Graficzna reprezentacja zapytania Q1 z zastosowanym PCQ dzielącym przepustowość pomiędzy transmisje T1, T2, T3 i T4

Istnieje wiele zastosowań dla QoS z PCQ. Implementacja zapytań zależy od wymagań postawionych przez stworzony koncept sieciowej warstwy logicznej [5]. W zależności od potrzeb stworzyć można wiele zapytań QoS z wykorzystaniem PCQ do tworzenia pod-zapytań. Jednak należy mieć na uwadze to, że nie wszystkie routery w pełni wspierają QoS. Proste routery sprzętowe (w cenie do 200 zł) zazwyczaj nie posiadają mechanizmów zarządzania ruchem sieciowym. Routery te pozwalają na tworzenie jednej lokalnej podsieci i zarządzanie przydzielonymi adresami IP poprzez DHCP. Są to routery przeznaczone do użytku domowego, lecz stosowane są także na uczelniach wyższych. Celem tego działania jest redukcja kosztów, która w ostatecznym rozrachunku jest pozorna. Routery sprzętowe ze średniej półki tj. TP-Link Archer C9 (w cenie około 400 zł) oferują tworzenie zapytań według narzuconych reguł. W przypadku routera Archer C9 rysunek 3 możliwa jest konfiguracja typu priorytetyzowanej usługi (np. FTP) oraz protokołu (TCP, UDP) i portu tej usługi (np. 21). Możliwa jest także priorytetyzacja konkretnego urządzenia. Nie został w nim jednak zaimplementowany mechanizm PCQ.



Rys. 3. Tworzenie zapytania QoS w routerze marki TP-Link

wspierają tworzenie własnych zapytań. Jednak nie wszystkie oferują wsparcie dla PCQ - w takim przypadku administrator sieci zmuszony jest do tworzenia oddzielnych zapytań dla każdego użytkownika jeśli chce zarządzać poszczególnymi użytkownikami.

Dominującym na rynku producentem routerów programowalnych jest Cisco. Routery Cisco stosowane są w największych przedsiębiorstwach [6] tj. Netflix, Nvidia oraz Pinterest. Routery Cisco pozwalają na tworzenie własnych zapytań QoS. Umożliwia to na dopasowanie zapytań do potrzeb obiektu. Routery tej marki nie posiadają jednak wsparcia dla mechanizmu PCQ. Administrator sieci zmuszony jest więc do własnoręcznego zaimplementowania zapytania spełniającego rolę PCQ. Autorzy skupili się na routerach z natywnym wsparciem dla mechanizmu PCQ.

Przykładem routerów wspierających QoS wraz z PCQ są routery marki Mikrotik stosujące oprogramowanie RouterOS. W przeciwieństwie do wyżej wymienionych marek routerów te są znacznie łatwiejsze w konfiguracji i obsłudze. Jest to o tyle ważne, że na uczelniach bardzo często administratorami sieci na poziomie danego laboratorium komputerowego stają się wykładowcy prowadzący w nim zajęcia.

Oprogramowanie RouterOS, oparte jest na Linuksie. Stworzone zostało przez Mikrotik i stosowane jest w routerach tego producenta. RouterOS dostępny jest do pobrania także w wersji na architekturę x86, więc można zainstalować go na serwerze, który pełni usługę routingu. Wspierana jest także architektura ARM, więc możliwa jest instalacja na Raspberry Pi. RouterOS może być administrowany z użyciem terminala lub oprogramowania Winbox. Winbox jest graficznym interfejsem, upraszczającym tworzenie konfiguracji sieciowych [7]. Mikrotik oferuje także oprogramowanie CHR (ang. *Cloud Hosted Router*) - jest to obraz dysku wirtualnej maszyny, na której zainstalowano RouterOS. Instalacja CHR w środowisku wirtualnym pozwala na łatwe przygotowanie i przetestowanie zamierzonej konfiguracji.

2. ZASTOSOWANIE QOS WRAZ Z PCQ W LABORATORIUM KOMPUTEROWYM

Autorzy zajmują się administracją sieci na uczelniach wyższych oraz szkołach średnich w Trójmieście i Kościerzynie. W żadnym z tych obiektów nie był stosowany QoS. W przypadku jednej z administrowanych uczelni brak QoS uniemożliwił niektórym pracownikom użytkowanie serwera lokalnego. Problem rozwiązany został przez jednego z autorów dzięki zastosowaniu pojedynczego zapytania QoS wraz z PCQ. QoS z PCQ umożliwiło wszystkim pracownikom dzielenie łącza i uzyskiwanie równej przepustowości. Skuteczność i skalowalność tej konfiguracji wykazała sens stosowania QoS nawet przy niewielkiej ilości użytkowników, aby zagwarantować równy dostęp do zasobów sieciowych. Należy jednak zauważyć, że niektóre uczelnie posiadają także serwery udostępniane studentom. Ilość użytkowników tych serwerów jest znacznie większa i problem się nasila. W takim przypadku konieczna może okazać się również priorytetyzacja konkretnego typu ruchu, aby ograniczyć do minimum narzut sieciowy niepotrzebnego ruchu sieciowego. Oznacza to, że priorytetyzując jedynie ruch pożądaný (np. ruch sieciowy związany z wykonywanymi przez studentów zadaniami) możemy ograniczyć przepustowość łącza użytkowaną przez studentów nie wykonujących zadań i np. przeglądających

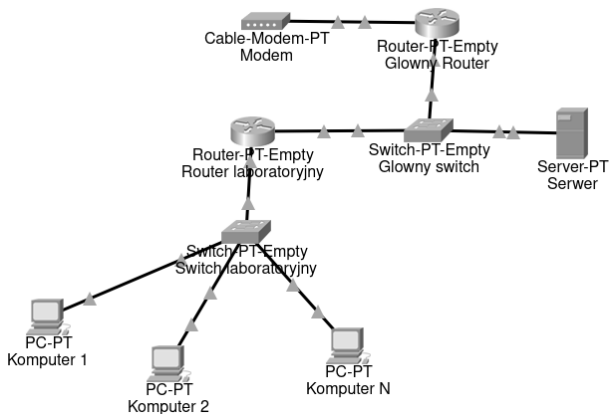
Routery programowalne zazwyczaj obsługują QoS oraz

strony internetowej.

2.1. Przygotowanie prostej konfiguracji QoS wraz z PCQ

Uniwersalnym zastosowaniem QoS z PCQ jest równy podział łącza bez priorytetyzacji w zapytaniu. Z doświadczenia autorów w stosowaniu QoS równy rozdzielacz poprawia jakość korzystania z sieci pod warunkiem, że każdy użytkownik powinien posiadać gwarancję równej przepustowości. Taka konfiguracja sprawdzi się w większości zastosowań, szczególnie zastosowań w laboratoriach uniwersyteckich, ponieważ każdy ze studentów powinien posiadać gwarancję dostępu np. do serwera laboratoryjnego z taką samą przepustowością jak inni studenci. Przygotowanie takiej konfiguracji wiąże się ze stworzeniem zapytania. Na zapytanie muszą być narzucone zasady. Jeśli tworzone jest zapytanie, które nie ma narzucać żadnych ograniczeń, a stanowi jedynie strukturę do której zastosowany ma być PCQ, to można na nie narzucić ograniczenie do pełnej przepustowości. Ograniczenie użytkowników do pełnej przepustowości nie wpłynie w żaden sposób na połączenie. Do tego zapytania można dodać pod-zapytania PCQ narzucające zasadę równej przepustowości.

W pierwszej kolejności należy przygotować projekt sieci, aby umożliwić sobie stworzenie prawidłowej konfiguracji [8]. Na rysunku 4 przedstawiono plan sieci komputerowej obiektu stworzony w programie Cisco Packet Tracer.

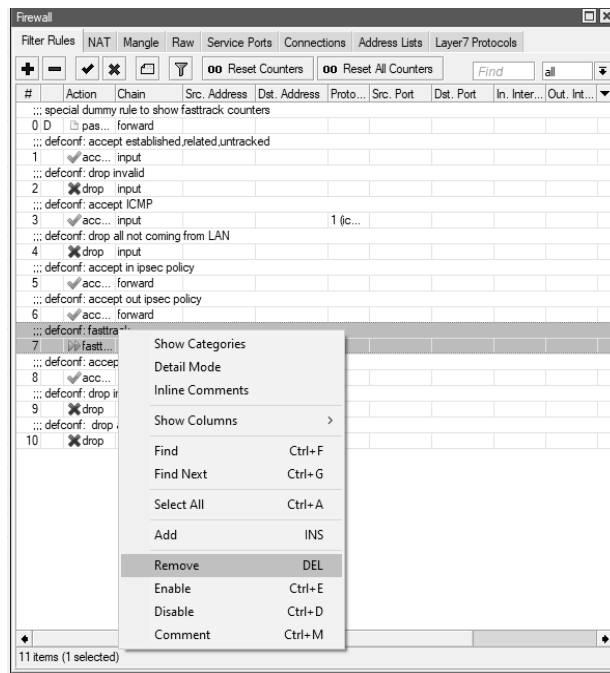


Rys. 4. Plan sieci komputerowej obiektu

Jak widać na rysunku 4 obiekt posiada dwa routery - router główny i router laboratoryjny. Router główny połączony jest z modemem poprzez port WAN (ang. Wide Area Network). Do portu LAN (ang. Local Area Network) głównego routera podłączony jest główny switch, do niego zaś podłączony serwer i port WAN routera laboratoryjnego (dokonywana jest translacja NAT pomiędzy podsiecią laboratoryjną, a siecią główną). Podsieć laboratoryjna składa się ze switcha laboratoryjnego, który podpięty jest do portu LAN routera laboratoryjnego. Do switcha laboratoryjnego podpięte są komputery. W tej konfiguracji istnieje tylko jedno laboratorium, więc łącze prowadzące do serwera nie musi być dzielone pomiędzy wieloma routerami. Oznacza to, że nie ma potrzeby tworzenia zapytania na routerze głównym. Należy jedynie stworzyć odpowiednie zapytanie na routerze laboratoryjnym.

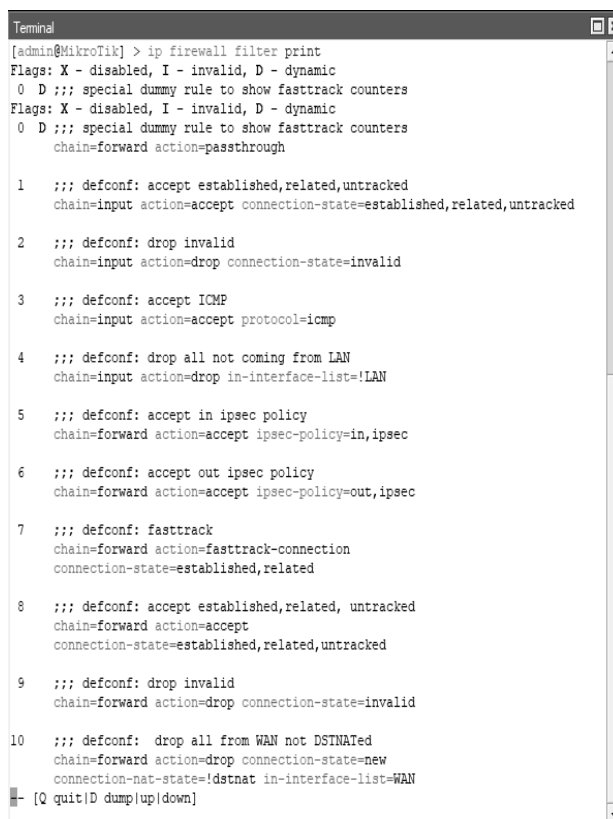
W przypadku RouterOS przygotowanie takiej konfiguracji jest nieskomplikowane. Należy pamiętać jednak, aby wpiery wyłączyć regułę Fasttrack w zaporze sieciowej routera laboratoryjnego. Reguła Fasttrack pomija wszystkie zapytania oraz zaporę sieciową i bezpośrednio

łączy klientów. W tym przypadku jest to zjawisko niekorzystne, więc reguła Fasttrack musi zostać z zapory usunięta. Na rysunku 5 przedstawiono procedurę usuwania Fasttrack za pomocą interfejsu graficznego WinBox. Po usunięciu reguły Fasttrack należy wyłączyć i włączyć router.



Rys. 5. Usuwanie reguły Fasttrack z zapory sieciowej

Alternatywnie regułę można wyłączyć za pomocą odpowiedniego polecenia. Na początku należy wyświetlić wszystkie reguły filtrujące zapory sieciowej. Można tego dokonać następującym poleceniem: `ip firewall filter print`. Przykładowe wyniki przedstawiono na rysunku 6.



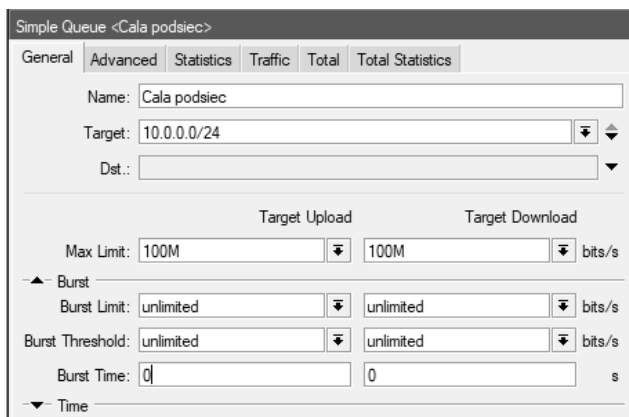
Rys. 6 Wynik polecenia wyświetlającego reguły zapory sieciowej. Następnie należy wyłączyć regułę, której akcja to *fasttrack-connection*. Jako, że w tym przypadku jest to reguła nr 7, *fasttrack* wyłączyć można następującym poleceniem:

```
ip firewall filter remove numbers=7
```

Numer należy dostosować do otrzymanej listy reguł poleceniem *print*. Po usunięciu reguły należy wyłączyć i włączyć router. Można tego dokonać poleceniem: *system reboot*.

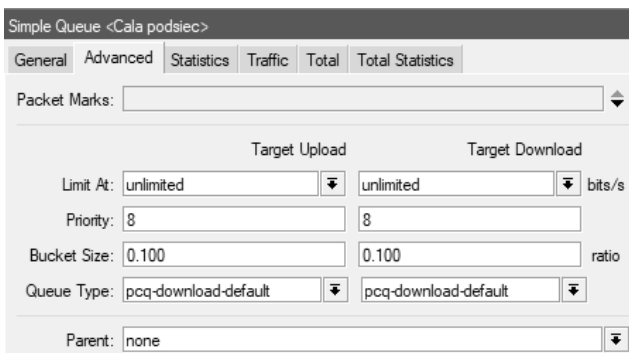
Po wyłączeniu i włączeniu routera *Fasttrack* zostanie usunięty. Aby sprawdzić zmiany można ponownie wyświetlić reguły filtrujące.

Po wyłączeniu *Fasttrack* można przejść do tworzenia zapytania. W pierwszej kolejności należy stworzyć zapytanie (zakładka *Simple Queue*), które ogranicza użytkowników do pełnej przepustowości. W zakładce *General* jako cel zapytania należy obrać całą podsieć, ponieważ zapytanie obsługiwać ma wszystkich użytkowników [9]. Należy także ustawić maksymalny limit pobierania i wysyłania (pole *Max Limit*). Ponieważ zapytanie to ogranicza przepustowość do pełnej, należy wpisać maksymalną obsługiwaną przepustowość przez router. Ten router zawiera gniazda *Fast Ethernet*, więc przepustowość wynosi 100 Mb/s, i taki powinien zostać ustawiony limit (w pole wpisywać należy jedynie 100M, końcówkę b/s należy pominąć). Konfigurację dla podsieci 10.0.0.0/24 przedstawiono na rysunku 7.



Rys. 7. Zakładka General zapytania głównego

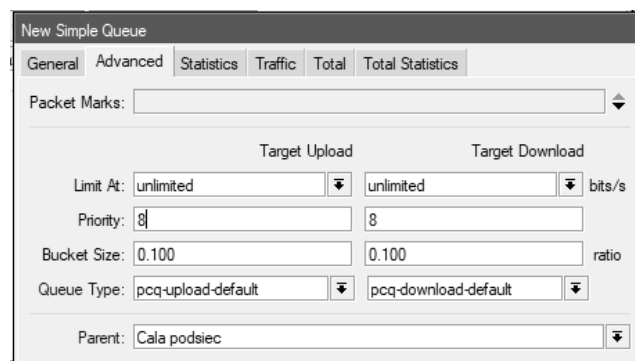
W zakładce *Advanced*, należy wybrać typ zapytania. Dla wysyłania należy wybrać *pcq-upload-default*, zaś dla pobierania *pcq-download-default*. Jako, że jest to główne zapytanie pole *Parent* pozostawić należy jako *none*. Konfigurację typu zapytania przedstawiono na rysunku 8.



Rys. 8. Zakładka Advanced kolejki głównej

W dalszej kolejności stworzyć należy

pod-zapytania dla każdego z użytkowników. W tym przypadku przy tworzeniu pod-zapytania, w zakładce jako cel wpisać adres IP komputera użytkownika. Istotne jest aby adres IP zarezerwowany był dla komputera, który jest celem ograniczenia, w przeciwnym wypadku komputer ten może (dzięki usługom DHCP routera) otrzymać inny adres przy ponownym połączeniu z siecią. W przypadku pod-zapytań pole *Max Limit* pełni funkcję ograniczania prędkości transferów konkretnego użytkownika. Jako, że pod-zapytanie nie ma na celu ograniczać maksymalnej prędkości, a jedynie zapewniać równą prędkość, jeśli łącze wykorzystywane jest przez kilku użytkowników jednocześnie, pole to można pozostawić na opcji *unlimited* lub wpisać pełną prędkość łącza (w tym przypadku 100 Mb/s). Ograniczanie prędkości konkretnego użytkownika ma sens nie tylko, jeśli planowane jest zmniejszenie prędkości dostępnej dla użytkownika. Ograniczyć można także użytkownika jeśli transfery użytkownika wykonywane będą z priorytetem - w takim przypadku ograniczenie przepustowości tego użytkownika zagwarantuje mu ustaloną prędkość (np. 80 Mb/s), lecz nie dopuści do zawłaszczenia łącza. W tej konfiguracji nie stosowana jest priorytyzacja, więc opcja ta może zostać pominięta. W zakładce *Advanced* należy zmienić typ zapytania (analogicznie do zapytania głównego). W tym celu należy w polu *Parent* zmienić ustawienie *none* na zapytanie nadrzędne. W ten sposób stworzone zapytanie dla użytkownika stanie się pod-zapytaniem zapytania głównego. Konfigurację zapytania stworzonego dla komputera użytkownika przedstawiono na rysunku 9.



Rys. 9. Konfiguracja pod-kolejki dla pierwszego użytkownika

Takie same zapytania należy stworzyć dla pozostałych użytkowników. Dzięki temu utworzona zostanie struktura (rys. 10), która zapewni sprawiedliwe dzielenie łącza pomiędzy użytkowników [10, 11].

#	Name	Target	Upload Max Limit	Download Max Limit	Upload	Download
0	Cala po...	10.0.0.0/24	100M	100M	633.4 kbps	100.1 Mbps
4	Komp4	10.0.0.250	unlimited	unlimited	251.8 kbps	33.0 Mbps
3	Komp3	10.0.0.251	unlimited	unlimited	203.5 kbps	34.9 Mbps
1	Komp2	10.0.0.253	unlimited	unlimited	178.0 kbps	32.3 Mbps
2	Komp1	10.0.0.254	unlimited	unlimited	0 bps	0 bps

Rys. 10. Struktura utworzonej struktury QoS wraz z PCQ

Jak widać na powyższym rysunku trzy z czterech urządzeń pobierały dane z serwera i przepustowość została pomiędzy nie sprawiedliwie podzielona. W przypadku zaprzestania pobierania poprzez jedno z urządzeń, przepustowość zostanie podzielona tylko pomiędzy dwa urządzenia

rysunku 11.

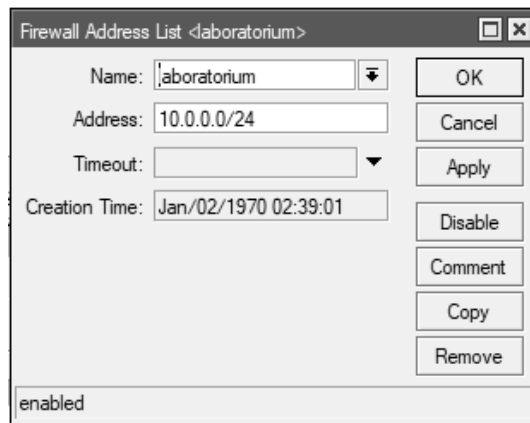
Queue List						
Simple Queues		Interface Queues		Queue Tree		Queue Types
#	Name	Target	Upload Max Limit	Download Max Limit	Upload	Download
0	Cala po...	10.0.0.0/24	100M	100M	806.0 kbps	98.0 Mbps
4	Komp4	10.0.0.250	unlimited	unlimited	0 bps	0 bps
3	Komp3	10.0.0.251	unlimited	unlimited	367.1 kbps	48.6 Mbps
1	Komp2	10.0.0.253	unlimited	unlimited	438.8 kbps	49.1 Mbps
2	Komp1	10.0.0.254	unlimited	unlimited	0 bps	0 bps

Rys. 11. Podział przepustowości pomiędzy dwa urządzenia

Dodanie kolejnych urządzeń wiąże się z koniecznością tworzenia kolejnych pod-zapytań. Oprogramowanie routera pozwala jednak na ich kopiowanie - w skopiowanym zapytaniu należy tylko zmienić nazwę oraz adres IP.

2.2. Tworzenie zapytań z priorytetyzacją ruchu SSH oraz hierarchiczną priorytetyzacją ruchu użytkowników.

Przy bardziej rozbudowanych sieciach, uniwersalne konfiguracje mogą nie być wystarczające. W laboratorium komputerowym często stosowane są serwery pełniące usługi (np. serwer PostgreSQL) lub serwery udostępniające zasoby sieciowe (np. serwer SAMBA). Odpowiednie zasady QoS pozwolą utworzyć zapytania, które priorytetyzować będą ruch sieciowy związany z zadaniami wykonywanymi przez studentów (np. ruch SSH na porcie 22), a pozostały ruch (np. przeglądanie internetu) będzie wykonywany z mniejszym priorytetem. Pozwoli to zapewnić studentom możliwość niezakłóconej pracy na serwerze poprzez SSH (ang. *Secure Shell*) np. do wykonywania kwerend na serwerze PostgreSQL [12, 13]. Nie rozwiązuje to jednak problemu nierównego dostępu do serwera SSH. Ruch SSH będzie priorytetyzowany, lecz jeden ze studentów, podczas pracy przez SSH, może uzyskać więcej przepustowości niż inni studenci. Ten problem rozwiązać można poprzez zastosowanie PCQ. Ruch każdego ze studentów zanim zostanie umieszczony w zapytaniu umieszczony zostanie w pod-zapytaniu, na które zostaną nałożone odpowiednie ograniczenia, tak aby studenci wspólnie dzielili łącze i mieli możliwość posługiwania się taką samą przepustowością. Jeśli nie zastosowano by PCQ trzeba byłoby wykonać dla każdego studenta zapytanie z zasadami QoS, które priorytetyzowało by ruch SSH oraz ograniczałyby przepustowość tak, aby każdy ze studentów posiadał równy dostęp. Rozwiązanie to oczywiście nie byłoby skalowalne, ponieważ dla każdego nowego studenta dodawano kolejne zapytanie, a w przypadku gdy przeniesiono by usługę SSH na inny port należało by zmienić port w każdym z zapytań. Byłoby to niewygodne, dlatego warto zastosować PCQ. Dzięki wykorzystaniu PCQ wystarczy stworzyć tylko jedno zapytanie, które można modyfikować według potrzeb. Natomiast jeśli nastąpi potrzeba dodania kolejnego użytkownika wystarczy stworzyć pod-zapytanie i wpiąć je do zapytania priorytetyzującego SSH. W wypadku konieczności priorytetyzacji konkretnego typu ruchu sieciowego należy posłużyć się zaporą sieciową. Stworzyć należy listę adresową, zawierającą adresy IP urządzeń lub adres całej podsieci, do której odwoływać mają się tworzone reguły. Stworzoną listę adresową przedstawiono na rysunku 12.



Rys. 12. Lista adresowa „laboratorium“

Zapora sieciowa posiada możliwość oznaczania połączeń jak i pakietów [14]. Do oznaczonych pakietów może odnosić się przez QoS i nadawać pakietom o różnym oznaczeniu, różny priorytet oraz wyznaczać różne zasady. Oznaczyć oddzielnie należy ruch wychodzący (wysyłanie) oraz ruch przychodzący (pobieranie), ponieważ ruch przychodzący pochodzi z interfejsu WAN (w tym przypadku *ether1*), zaś ruch wychodzący pochodzi z interfejsów LAN (w tym przypadku *bridge*, który jest mostkiem sieciowym łączącym wszystkie interfejsy LAN routera). Następnie rozróżniany jest konkretny typ ruchu. W tym przypadku oznaczono ruch na porcie 22 (ruch poprzez SSH) i oznaczono także pozostały ruch. Oznaczyć należy osobno rozróżniany ruch wychodzący, jak i rozróżniany ruch przychodzący. Aby oznaczyć połączenie lub pakiet należy przy tworzeniu reguły wybrać akcję *mark connection* lub *mark packet*. Łańcuchem reguły w przypadku połączeń i pakietów przychodzących będzie *forward*. Natomiast łańcuchem połączeń i pakietów wychodzących będzie *prerouting*, ponieważ QoS musi przetworzyć ruch sieciowy przed dokonaniem routingu. Dla ruchu przychodzącego należy wprowadzić docelową listę adresową, natomiast dla ruchu wychodzącego należy wprowadzić źródłową listę adresową. Należy nadać połączeniom nazwę oznaczenia (pole *New Connection Mark*) oraz wskazać interfejs wejściowy (dla połączenia przychodzącego będzie to interfejs WAN, zaś dla połączenia wychodzącego interfejs LAN lub mostek łączący interfejsy LAN). Następnie należy wskazać w regułach oznaczających pakiety oznaczenia połączeń do których nawiązują (pole *Connection Mark*). Stworzonym regułom oznaczającym należy także wskazać protokół (pole *Protocol*) i port (pole *Any Port*) na którym działają oraz nadać nazwę oznaczenia (pole *New Packet Mark*). Stworzone reguły zapory sieciowej (zakładka *Mangle*) przedstawiono na rysunku 13.

#	Action	Chain	Protocol	Any	Port	In	Interface	Connection Mark	Src. Address List	Dst. Address List	New Packet Mark	New Connection Mark
0	mark connection	forward					ether1			laboratorium		pobieranie
1	mark packet	forward	6 (tcp)	22					pobieranie	laboratorium	SSH	pobieranie
2	mark packet	forward							pobieranie	laboratorium	pozostalyruch	pobieranie
3	mark connection	prerouting					bridge			laboratorium		wysylanie
4	mark packet	prerouting	6 (tcp)	22				wysylanie	laboratorium		SSH	wysylanie
5	mark packet	prerouting						wysylanie	laboratorium		pozostalyruch	wysylanie

Rys. 13. Konfiguracja reguł oznaczających zapory sieciowej

Na rysunku 13 kolumny przedstawiają wartości wszystkich opcji, które zostały zmodyfikowane względem domyślnych ustawień nowej reguły. Następnym krokiem

jest stworzenie zapytań. Jako, że rozdzielany jest typ ruchu i dokonywana jest priorytetyzacja należy posłużyć się drzewami zapytań. Drzewa zapytań pozwalają na dzielenie ruchu sieciowego na różne zapytania w zależności od typu ruchu. Należy stworzyć zapytanie główne, które będzie zapytaniem nadrzędnym. Następnie stworzyć trzeba osobne zapytania do pobierania i wysyłania. W tych zapytaniach zostaną umieszczone zapytania z ruchem SSH i pozostałym ruchem. W zapytaniach SSH i zapytaniach dla pozostałego ruchu zastosować należy PCQ, tak aby sprawiedliwie rozdzielać łącze pomiędzy użytkowników. W zapytaniu głównym zmieniany jest jedynie maksymalny limit. W zapytaniach wysyłania (*Wysyłanie*) i pobierania (*Pobieranie*) wprowadzane jest zapytanie nadrzędne (pole *Parent*) i maksymalny limit. W zapytaniach dla ruchu SSH i pozostałego ruchu wprowadzono typ zapytania (pole *Queue Type*) jako PCQ, zapytanie nadrzędne (*Pobieranie* lub *Wysyłanie*), maksymalny limit oraz oznaczenie pakietu, do którego odwołuje się zapytanie. Zapytaniu SSH nadano także najwyższy priorytet. Stworzone drzewo zapytań przedstawiono na rysunku 14.

Name	Parent	Packet Marks	Queue Type	Priority	Max Limit	Avg. Rate	Bytes
Cala podsiec	global		default-small	8	100M	93.7 Mbps	3912.8...
Pobieranie	Cala podsiec		default-small	8	100M	92.2 Mbps	3860.2...
Pozostałe pob...	Pobieranie	pozostaly-ruch-pobi...	pcq-download-default	8	100M	14.4 Mbps	704.5...
SSH pobieranie	Pobieranie	SSH-pobieranie	pcq-download-default	1	100M	77.8 Mbps	3155.7...
Wysyłanie	Cala podsiec		default-small	8	100M	1538.6 kbps	52.6 MB
Pozostałe wys...	Wysyłanie	pozostaly-ruch-wysy...	pcq-upload-default	8	100M	175.3 kbps	6.0 MB
SSH wysyłanie	Wysyłanie	SSH-wysyłanie	pcq-upload-default	1	100M	1363.3 kbps	46.6 MB

Rys. 14. Widok drzewa zapytań

Na rysunku 14 kolumny przedstawiają wartości wszystkich opcji, które zostały zmodyfikowane względem domyślnych ustawień nowego zapytania. Jako, że zapytaniu SSH nadany został najwyższy priorytet (1 - najwyższy, 8 - najniższy), ruch na porcie 22 otrzymał znaczną część przepustowości łącza i żądania na tym porcie wykonywane zastawały w pierwszej kolejności. Jeśli priorytet zostanie zmieniony na taki sam jak priorytet pozostałego ruchu, przepustowość zostanie podzielona równo pomiędzy oba zapytania (rys. 15). Jako, że zastosowano PCQ, ruch na porcie SSH dzielony jest równo dla każdego połączenia na tym porcie (więc dla każdego użytkownika).

Name	Parent	Packet Marks	Queue Type	Priority	Max Limit	Avg. Rate	Bytes
Cala podsiec	global		default-small	8	100M	100.5 Mbps	4.0 GB
Pobieranie	Cala podsiec		default-small	8	100M	98.9 Mbps	4.7 GB
Pozostałe pob...	Pobieranie	pozostaly-ruch-pobi...	pcq-download-default	8	100M	49.6 Mbps	1029.1...
SSH pobieranie	Pobieranie	SSH-pobieranie	pcq-download-default	8	100M	49.3 Mbps	3790.1...
Wysyłanie	Cala podsiec		default-small	8	100M	1586.4 kbps	68.3 MB
Pozostałe wys...	Wysyłanie	pozostaly-ruch-wysy...	pcq-upload-default	8	100M	695.0 kbps	10.4 MB
SSH wysyłanie	Wysyłanie	SSH-wysyłanie	pcq-upload-default	1	100M	891.3 kbps	57.9 MB

Rys. 15. Widok drzewa zapytań z równym priorytetem pobierania poprzez port 22 i pozostałego ruchu sieciowego

Niewielkim wysiłkiem można stworzyć nowe zapytania, dotyczące innych typów ruchu i umieścić je w zapytaniach *Pobieranie* i *Wysyłanie*. Należy jednak pamiętać o oznaczaniu odpowiednich pakietów w zaporze sieciowej. Dostępność ośmiu różnych priorytetów pozwala na łatwe stworzenie drzewa priorytetyzacji.

3. PODSUMOWANIE

Optymalizacja ruchu sieciowego w sieci lokalnej jest istotna, ponieważ poprawia komfort korzystania z sieci.

Routery posiadają narzędzia, służące do zarządzania ruchem sieciowym. Jednym z tych narzędzi jest QoS wraz z mechanizmem PCQ. Niewłaściwe zarządzanie ruchem sieciowym powoduje niepoprawne rozdzielanie przepustowości pomiędzy podłączane urządzenia korzystające z sieci i w konsekwencji może taka sytuacja doprowadzić do zawłaszczenia łącza przez danego użytkownika.

Autorzy podjęli próbę rozwiązania tego problemu. Dokonali konfiguracji routera korzystającego z RouterOS. Stworzyli dwie konfiguracje. Pierwsza konfiguracja równo rozdziela przepustowość pomiędzy wszystkie urządzenia korzystające aktywnie z sieci. Wykorzystane zostały proste zapytania. Druga stworzona przez autorów konfiguracja wykorzystywała drzewo zapytań. Stworzono reguły zapory sieciowej, które oznaczały ruch przychodzący i wychodzący, a następnie oznaczały pakiety ruchu przychodzącego i pakiety ruchu wychodzącego. Oddzielnie oznaczano pakiety wykorzystujące port 22 (w tym przypadku ruch poprzez SSH), a oddzielnie pozostałe pakiety. Następnie wykorzystując QoS wraz z PCQ stworzono drzewo zapytań, które nadawało ruchowi na porcie 22 najwyższy priorytet. Zapytania zostały skonfigurowane również tak, aby równo rozdzielały przepustowość pomiędzy urządzenia. Wykorzystano do tego celu PCQ.

Równe dzielenie łącza pomiędzy użytkowników jest szczególnie istotne w laboratoriach komputerowych na uczelniach wyższych. Na kierunkach informatycznych sporą ilość zadań wykonuje się na serwerze poprzez połączenie SSH. Na serwerze zazwyczaj zapisywane są także pliki użytkowników, ponieważ komputery w pracowni często podlegają czyszczeniu lub resetowaniu do konkretnej konfiguracji. Każdy ze studentów musi mieć dostęp do serwera z taką samą przepustowością. W ten sposób praca na serwerze nie jest dla nikogo spowolniona lub utrudniona. Ważna jest także priorytetyzacja odpowiedniego typu ruchu. Pozwala to wykluczyć sytuację, w których studenci spowalniają ruch innym wykonując czynności tj. przeglądanie Internetu lub pobieranie plików z Internetu. Zastosowanie QoS wraz z PCQ pozwala w odpowiedni sposób skonfigurować laboratoryjną lokalną sieć komputerową.

4. BIBLIOGRAFIA

1. Szigeti T., Hattingh C., Barton R., Briley K.: End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition. Cisco Press, 2013, s. 5 – 9
2. Grabiec P.: Routery z QoS – jak działają?. Poradniki Allegro, 2014. <https://allegro.pl/artukul/routery-z-qos-jak-dzialaja-113739> [dostęp na dzień 30.06.2019]
3. Burakowski W., Dąbrowski M.: Multi-service IP QoS network: architecture and practical experiments. Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, Tom 5. Warszawa 2002, s. 5 – 7
4. Malinowski T.: Mechanizmy QOS w kontekście integrowania sieci IPV4 i IPV6. Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, Tom 4. Warszawa 2010, s. 26 – 27
5. Cisco Systems.: Enterprise QoS Solution Reference Network Design Guide. Cisco Press, 2004, s. 41 – 43
6. Cisco Systems: Customer Stories, <https://umbrella.cisco.com/customers> [dostęp na dzień 08.07.2019]

7. Mikrotik: Winbox Manual, <https://wiki.mikrotik.com/wiki/Manual:Winbox> [dostęp na dzień 08.07.2019]
8. Muc A., Idzikowski T., Szeleziński A., Maj M.: System do zarządzania infrastrukturą komputerową uczelni wyższej wykorzystujący technologię Intel AMT. Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Tom 48. Gdańsk 2016, s. 76
9. Peuhkuri M.: IP Quality of Service. Helsinki University of Technology, Laboratory of Telecommunications Technology. Helsinki 1999, s. 8 – 9
10. Vassisa D., Kampourakia A., Belsis P., Skourlas C.: A Resource Reservation and Traffic Categorization Agent for QoS in Medical Ad Hoc Networks. Elsevier: Procedia - Social and Behavioral Sciences Vol 73. Budapest 2013, s. 461 – 462
11. Newton P. C., Arockiam L.: A novel prediction technique to improve quality of service (QoS) for heterogeneous data traffic. Journal of Intelligent Manufacturing, vol. 22. Switzerland 2011, s. 867 – 872
12. El-Gendy M. A., Bose A., Shin K. G.: Evolution of the Internet QoS and support for soft real-time applications. Proceedings of the IEEE, vol. 91, no. 7, July 2003, s. 1086-1104
13. Almofari N., Moustafa H. S., Zaki F.: (2012). Optimizing QoS for Voice and Video using DiffServ-MPLS. International Journal of Modern Computer Science & Engineering Vol 1. Manusora 2012, s. 22 – 23
14. Vegesna S.: IP Quality of Service. Cisco Press. Indianapolis 2001, s. 28 – 29

USING QOS WITH PCQ IN UNIVERSITY LABORATORIES IN ORDER TO ENHANCE STUDENTS ACCESS TO LABORATORY SERVERS

The paper presents a method of configuring the computers laboratories' local network. The QoS with PCQ was used in order to guarantee an equal bandwidth for students connecting to laboratories' servers. This method allows both prioritizing specific type of network traffic, limiting bandwidth to pre-established values and guaranteeing the same bandwidth for every user. This method is scalable and can be applied by using most of programmable routers. A basic configuration of QoS with PCQ that made clients get equal bandwidth was presented in the second chapter. This configuration consisted of one parent query that created a structure in which sub-queries configured with PCQ were placed. The third chapter showed a configuration that prioritized traffic on specific port (port 22) above other traffic. This configuration was also configured with PCQ to share the bandwidth equally for every client that made prioritized traffic. In order to create the configuration, firewall mangle rules were created to mark connections (upload and download) and to mark packets (packets sent or received on port 22 and packets not sent or received on this port). The marks were used to allow QoS to select the packets that were meant to be prioritized and give them the highest priority. In collaboration with PCQ the configuration prioritized port 22 traffic while splitting the bandwidth equally amongst clients.

Keywords: QoS, PCQ, networking, laboratory, prioritizing, sharing resources.

