

Politechnika Łódzka
Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki
Katedra Informatyki Stosowanej

PRACA DYPLOMOWA MAGISTERSKA

Tytuł pracy:

Zarządzanie ruchem pakietów w sieciach komputerowych opartych na protokole IP.

Management of packets traffic in computer networks based on IP protocol.

Autor: Sławomir Kozik

Numer albumu: 131503

Opiekun: dr inż. Łukasz Sturgulewski

Opiekun pomocniczy: dr inż. Artur Sierszeń

Łódź, wrzesień 2011

Spis treści:

Streszczenie	4
Abstract	4
Cel i zakres pracy	5
1. Wprowadzenie do sieci komputerowych opartych na protokole IP.....	8
1.1. Krótki rys historyczny	8
1.2. Porównanie modelu TCP/IP z modelem ISO/OSI	10
1.3. Warstwa trzecia jako podstawa funkcjonowania sieci LAN/WAN	11
1.4. Redundancja w sieciach komputerowych na poziomie warstwy 3	12
2. Mechanizmy warstwy sieci wykorzystywane w sieciach IP	15
2.1. Protokół IP	15
2.2. Protokół ICMP	22
2.3. Sieci IP	23
2.4. Modyfikacja datagramów w trakcie podróży	25
3. Metody sterowania ruchem wykorzystywane w sieciach opartych na protokole IP.....	31
3.1. Kształtowanie ruchu pakietów z wykorzystaniem routingu	31
3.1.1. Protokół RIPv2	36
3.1.2. Protokół OSPF (ang. Open Shortest Path First)	38
3.1.3. Protokół BGP	47
3.2. Jakość usług w sieciach IP	52
3.2.1. Podstawowe informacje o QoS	52
3.3. Przesyłanie datagramów w sieciach IP wykorzystując MPLS.....	62
3.3.1. Funkcjonowanie MPLS	62
3.3.2. Dystrybucja etykiet w sieci MPLS	66
3.3.3. Inżynieria ruchu w MPLS	70
3.4. Zarządzanie ruchem w sieciach IP z wykorzystaniem list dostępu	72
3.5. Metody sterowania ruchem pakietów w sieciach z nadmiarowością.....	75
3.5.1. Sterowanie ruchem w sieciach z redundancją bramy domyślnej	75
4. Zarządzanie ruchem pakietów z wykorzystaniem Systemów Zapobiegania Włamań	79
5. Urządzenia sieciowe odpowiedzialne za sterowanie ruchem pakietów w warstwie 3 modelu ISO/OSI.....	83
5.1. Routery segmentu Small Office/Home Office	84
5.2. Routery segmentu Small and Medium Business	84

5.3.	Routerzy oraz przełączniki warstwy 3 w segmencie dużych firm	87
5.4.	Routerzy oraz przełączniki warstwy 3 w segmencie ISP	90
6.	Projekt sieci implementującej mechanizmy zarządzania ruchem pakietów w sieciach opartych na protokole IP	93
6.1.	Założenia projektowe	93
6.2.	Opis realizowanych topologii.....	93
6.3.	Adresacja urządzeń w sieci	97
6.4.	Konfiguracja urządzeń	100
7.	Wdrożenie oraz testy akceptacyjne zaprojektowanej sieci	127
7.1.	Wdrożenie projektu	127
7.2.	Testy akceptacyjne	130
7.2.1.	Specyfikacja testów akceptacyjnych	130
7.3.	Wyniki testów akceptacyjnych.....	133
7.3.1.	Test protokołów trasowania bramy wewnętrznej.....	133
7.3.2.	Test protokołu BGP	138
7.3.3.	Test nadmiarowości łącz ISP	141
7.3.4.	Test protokołu HSRP	144
7.3.5.	Test funkcjonowania tunelu IPsec VPN.....	147
7.3.6.	Test zarządzania ruchem z wykorzystaniem map routingu (PBR)	150
7.3.7.	Test protokołu MPLS oraz protokołu LDP	152
7.3.8.	Test tuneli LSP	156
7.3.9.	Test mechanizmów QoS.....	161
8.	Podsumowanie i wnioski.....	171
	Wykaz rysunków	175
	Wykaz tabel.....	178
	Spis literatury	180

Streszczenie

Niniejsza praca przedstawia temat sterowania ruchem w sieciach opartych na protokole IP i podzielona została na dwie części. W pierwszej, opisowej części pracy wykazana została konieczność stosowania różnych mechanizmów sterujących ruchem we współczesnych sieciach komputerowych. Opisane zostały podstawy funkcjonowania sieci komputerowych oraz najczęściej stosowany protokół komunikacyjny IP. Przedstawiono także jego wady oraz zalety. W kolejnych rozdziałach omówiono zaawansowane mechanizmy sterowania ruchem pakietów w sieciach komputerowych i uzasadniono konieczność ich wdrażania we współczesnych sieciach. Uwzględniono m.in. protokoły trasowania dynamicznego, mechanizmy zapewniania jakości usług oraz nadmiarowość urządzeń w sieci oraz połączeń sieciowych. Druga, praktyczna część pracy obejmuje implementację oraz wdrożenie omówionych rozwiązań w symulowanej sieci komputerowej. Przedstawiono w tej części topologię wykorzystanej sieci, adresację urządzeń oraz sposób ich konfiguracji. Zbudowaną sieć poddano testom pod kątem działania zaimplementowanych mechanizmów, a uzyskane w ten sposób wyniki zostały szczegółowo opisane oraz podsumowane. Na końcu pracy podzielono omawiane mechanizmy ze względu na miejsce ich zastosowania w sieciach komputerowych.

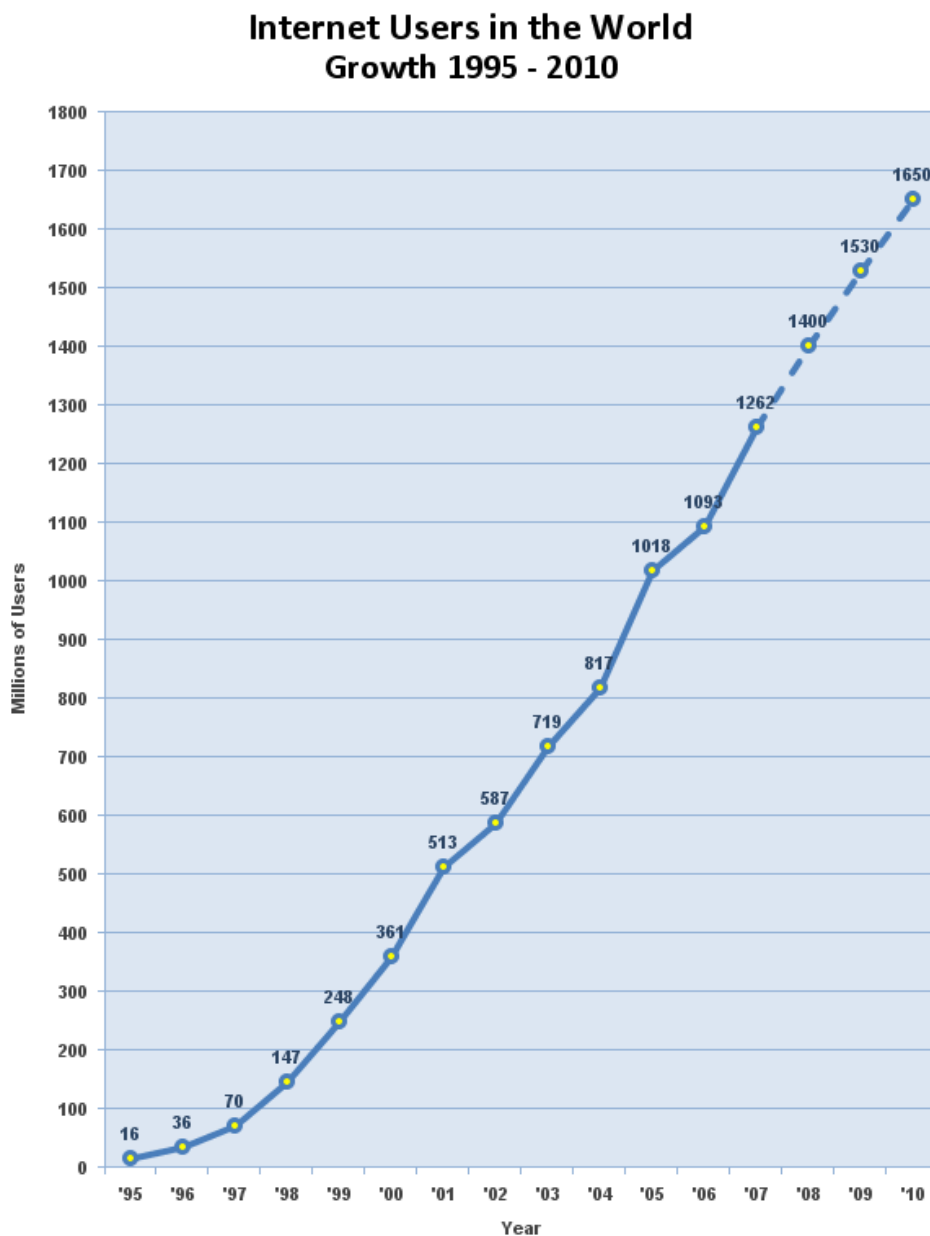
Abstract

The MA thesis, divided into two sections, deals with the topic of traffic control in IP protocol based networks. In the first descriptive section the necessity of using various traffic control mechanisms in contemporary computer networks has been proved. The basic network functions and IP communications protocol with its advantages and disadvantages have been described. The subsequent chapters discuss advanced packet traffic control mechanisms in computer networks and justify the need of introducing them in contemporary networks. Factors such as dynamic routing protocols, mechanisms ensuring the quality of service as well as device and networking redundancy have been taken into consideration

The practical section of the thesis involves implementation and introduction of the described solutions in a simulated network. The topology of the network used, device addressing and their configuration have been presented. The network has been tested for activity of implemented mechanisms, and the results have been described in detail and recapitulated. In the end, the mechanisms have been divided according to the place of application in networks.

Cel i zakres pracy

Zapotrzebowanie na informacje oraz ich obieg w dzisiejszych czasach wymusza szybki wzrost znaczenia sieci a zarazem ich rozwój, co obrazowo przedstawia Rysunek 1. pokazujący wzrost liczby użytkowników Internetu w latach 1995-2008 (lata 2009-2010 są danymi szacowanymi na podstawie lat poprzednich).



Source: www.internetworldstats.com - January, 2008
Copyright © 2008, Miniwatts Marketing Group

Rys. 1. Statystyczny wzrost liczby użytkowników internetu w latach 1995-2010 [27i].

Zgodnie z danymi na wykresie liczba użytkowników rosła eksponentalnie i dane szacowane na lata 2009 i 2010 zakładają dalszy wzrost. Dane zakładają liczbę użytkowników w roku 2010 na poziomie 1650 milionów, jednak z innych źródeł wynika, iż liczba ta pod koniec roku 2010 zbliżyła się do 2 miliardów (dane uzyskane od netcraft). Tak szybki rozwój

doprowadził w bieżącym roku do wyczerpania puli adresów IP przeznaczonych dla użytkowników Internetu. Oczywiście liczby te nie są do końca prawdziwe ponieważ powstało do tej pory wiele mechanizmów pozwalających na korzystanie z Internetu wielu użytkownikom stosując jeden adres IP (ang. *Internet Protocol*). Oznacza to, że rzeczywista liczba użytkowników oraz urządzeń końcowych wielokrotnie przekracza podane wyżej liczby. Taki rozwój sieci wymaga od ich operatorów korzystania z coraz bardziej wyrafinowanych metod sterowania ruchem w sieciach, aby mógł być dostarczany bez żadnych przeszkód. Mechanizmami takimi są protokoły trasowania bramy zewnętrznej (wymiana informacji o trasach między systemami autonomicznymi) oraz protokoły trasowania bramy wewnętrznej (umożliwiające trasowanie wewnątrz dużych sieci LAN (ang. *Local Area Network*) oraz między sieciami LAN i WAN (ang. *Wide Area Network*)). Innymi rozwiązaniami stosowanymi także w tym celu są: trasowanie na podstawie polityk (administratorzy sami decydują, jaką trasą mają zostać przesłane określone dane), mechanizm NAT (ang. *Network Address Translation*) (umożliwiający korzystanie z sieci globalnej wielu użytkownikom stosując jeden adres zewnętrzny) oraz stosunkowo nowe rozwiązanie nazwane MPLS (ang. *Multiprotocol Label Switching*) stosowane głównie w sieciach WAN (przesyłanie pakietów z zastosowaniem mechanizmu przełączania etykiet między warstwą drugą oraz trzecią modelu ISO/OSI, co pozwalana znacznie szybsze przenoszenie informacji niż przy zastosowaniu tradycyjnego protokołu trasowania).

Rozwój obecnych sieci wiąże się nie tylko ze wzrostem liczby użytkowników, ale także i może w głównej mierze z powstawaniem nowych usług udostępnianych użytkownikom. Wszystkie z nich mają specyficzne wymagania co do funkcjonowania sieci oraz traktowania pakietów przenoszących ich informacje np. serwery FTP (ang. *File Transfer Protocol*) lub usługi P2P (ang. *peer-to-peer*) wymagają dużych transferów, aby jak najszybciej pobrać duże pliki, ale nie ważne dla nich jest opóźnienie, z kolei dla usług związanych z telefonią internetową czy telekonferencjami przez Internet wymagane jest zarówno odpowiednie pasmo (aby przesłać wymaganą ilość danych) oraz małe opóźnienia (duże opóźnienia powodowałyby np. zatrzymywanie obrazu podczas konferencji czy zakłócenia podczas rozmowy telefonicznej). Rozwój nowych technologii wymusił na administratorach zaimplementowania w sieciach rozwiązań zapewniających odpowiedni poziom obsługi pakietów. Do mechanizmów takich należą między innymi: Quality of Service, technologia MPLS TE, czy wspomniany wcześniej routing z zastosowaniem polityk.

Ważnym aspektem zarządzania ruchem jest także zapewnienie bezpieczeństwa danym podczas ich transportu i do tego celu wykorzystywane są np. tunele IPsec VPN.

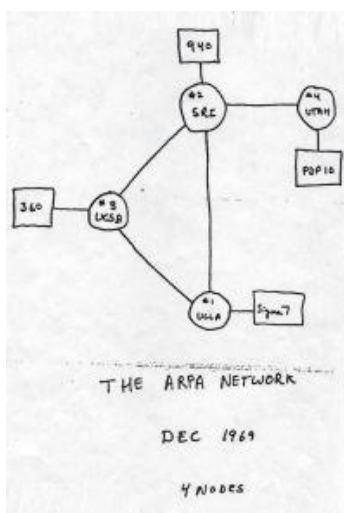
Celem niniejszej pracy jest przedstawienie metod oraz mechanizmów pozwalających na zarządzanie ruchem pakietów w sieciach IP oraz w części praktycznej pokazanie implementacji oraz funkcjonowania ich na wybranych przykładach (<http://royal.pingdom.com/>, <http://worldnarrowweb.wordpress.com/>).

Na pracę składa się 8 rozdziałów. Pierwszy rozdział opisuje historię sieci komputerowych oraz dwa podstawowe modele wykorzystywane w zagadnieniach związanych z sieciami komputerowymi. Częścią tego rozdziału jest także podrozdział opisujący działanie warstwy trzeciej modelu ISO/OSI, w której to działa większość mechanizmów związanych z ruchem pakietów IP. Kolejny rozdział poświęcony jest w całości warstwie trzeciej modelu ISO/OSI. Zawiera on informacje o protokołach działających w tej warstwie oraz o mechanizmach wprowadzających zmiany w przesyłanych datagramach. Rozdział 3 zadedykowany jest zaawansowanym mechanizmom funkcjonującym głównie w warstwie trzeciej modelu ISO/OSI zarządzania ruchem w sieciach LAN oraz WAN. Opisuje on mechanizmy trasowania w sieciach oraz między nimi, a także mechanizmy zapewniania jakości usług. Zawarte tu są także opisy działania mechanizmu MPLS, list dostępu oraz sposobów zapewnienia nadmiarowości w sieciach, co również należy rozpatrywać pod kątem zarządzania ruchem w sieciach. Rozdział 4 poświęcony jest sterowaniu ruchem sieciowym z wykorzystaniem Systemu Zapobieganiu Włamaniom. Rozdział 5 przedstawia oraz porównuje urządzenia sieciowe wykorzystywane w warstwie 3. do sterowania ruchem. Urządzenia podzielone są na kategorie ze względu na przeznaczenie (małe biura, małe firmy itp.) i w każdej kategorii wybrane zostały 3 modele różnych producentów (liczących się obecnie na rynku) i porównane pod względem funkcjonalności. Dwa kolejne rozdziały zostały poświęcone części projektowej. Pierwszy z nich obejmuje swoim zakresem założenia projektowe, topologię sieci, adresację oraz konfigurację urządzeń pracujących w infrastrukturze. Następny natomiast zawiera wdrożenie sieci przedstawionej we wcześniejszym rozdziale oraz testy akceptacyjne mające na celu potwierdzenie zgodności z założeniami oraz przedstawionymi wcześniej konfiguracjami. Rozdział 8 to wnioski oraz uwagi podsumowujące wykonaną pracę.

1. Wprowadzenie do sieci komputerowych opartych na protokole IP

1.1. Krótki rys historyczny

Szybki wzrost znaczenia komputerów uzmysłowił konieczność ich połączenia w celu wymiany danych między ich użytkownikami. Pierwsze kroki w tworzeniu sieci komputerowych poczyniono już w latach 60, gdy jeszcze w komunikacji dominowały sieci teleinformatyczne. Pierwszym tego typu rozwiązaniem było połączenie komputerów pomiędzy uczelniami Massachusetts (MIT) oraz w Santa Monica w 1965 r. W tym samym okresie czasu trwały prace badawcze na temat metod przełączania pakietów, które wykorzystał w 1964 roku Paul Baran z Rand Institute do bezpiecznej transmisji głosu w sieciach wojskowych. Powyższe prace leżą u podstaw późniejszych rozwiązań wykorzystywanych w sieciach komputerowych. Dużym krokiem w dziedzinie sieci było zbudowanie w roku 1969 w agencji ARPA (ang. *Advanced Research Projects Agency*) funkcjonującej sieci składającej się z 4 hostów nazwanej ARPAnet (Rys. 2.) (Kurose, Ross, 2006).



Rys. 2. Topologia pierwszej sieci komputerowej ARPAnet [29i]

Kolejne lata przynosiły coraz szybszy rozwój sieci ARPAnet, która w 1973 liczyła już 35 hostów (wtedy powstały pierwsze połączenia z jednostkami zagranicznymi) (<http://www.scientist.pl/>). W 1972 r. powstał protokół NCP (ang. *Network-Control Protocol*) pozwalający na komunikację między systemami końcowymi sieci. W połowie lat siedemdziesiątych oprócz rozwoju ARPAnet'u, powstało wiele sieci niezależnych. Szybki rozwój doprowadził do konieczności opracowania architektury pozwalającej na komunikację się hostów różnego rodzaju. Prace nad nową technologią zostały zapoczątkowane przez organizację DARPA (ang. *Defense Advanced Research Projects Agency*), których wynikiem

było powstanie idei trzech współcześnie stosowanych protokołów (IP, TCP oraz UDP). Dużymi osiągnięciami lat siedemdziesiątych w dziedzinie sieci komputerowych było powstanie protokołu FTP (pozwalającego na wymianę plików), pierwszej poczty elektronicznej oraz protokołu UUCP (ang. *Unix to Unix CoPy*) (umożliwiał komunikację między komputerami działającym pod nadzorem systemu UNIX). Ogromne znaczenie w historii sieci komputerowych było utworzenie pierwszego protokołu wielodostępowego a mianowicie ALOHA wykorzystywanego w sieci ALOHAnet. Protokół stał ten stał się pierwowzorem dla opracowania obecnie stosowanego Ethernetu (Kurose, Ross, 2006).

Lata osiemdziesiąte w historii Internetu to dalszy rozwój sieci łączących ośrodki uniwersyteckie. Powstają wtedy m.in. sieci BITNET, CSNET oraz NSFNET udostępniające połączenia z centrami superkomputerowymi. Rozwój szkieletu sieci NSFNET pozwolił mu pod koniec dekady pełnić rolę szkieletu łączącego sieci regionalne. Niewątpliwie najważniejszym wydarzeniem tego okresu jest wyparcie w sieci ARPAnet protokołu NCP przez grupę protokołów TCP/IP. Zmiana ta nastąpiła pierwszego stycznia 1983 r. Równolegle utworzono system DNS odpowiadający za translację adresów IP wykorzystywanych w sieciach do komunikacji na nazwy składające się ze znaków alfanumerycznych ułatwiając w ten sposób korzystanie z zasobów sieci (Kurose, Ross, 2006; Comer, 1998).

Wraz z popularyzacją komputerów osobistych w latach dziewięćdziesiątych nastąpił rozwój sieci na ogromną skalę. Zaczęto wykorzystywać sieć Internet do celów zarówno komercyjnych jak i rozrywkowych. Sieć ARPAnet, jako pierwowzór Internetu, zakończyła funkcjonowanie w roku 1991, natomiast NSFNET jako szkielet sieci funkcjonowała do 1995. Następnie jej rolę przejęli komercyjni dostawcy usług internetowych. Rewolucją tego okresu okazało się jednak wprowadzenie technologii WWW (ang. *World Wide Web*), umożliwiającej w prosty sposób zamieszczanie treści w Internecie, a także wdrażanie nowych rozwiązań pozwalających na szersze zastosowanie sieci. Na ten okres przypada również powstawanie sieci lokalnych w wyniku rozwoju routingu. Rosnące wykorzystanie sieci oraz Internetu do celów komercyjnych jak i rozrywkowych wymusiło w tym okresie także prace nad rozwojem mechanizmów zapewniających bezpieczeństwo użytkowników oraz umożliwiających świadczenie usług na odpowiednim poziomie (szczególnie dla celów przesyłu głosu i wideo, a także umożliwiających płynne uczestniczenie w rozgrywkach gier on-line). Najważniejszymi osiągnięciami ostatnich czasów jest niewątpliwie rozwój technologii DSL oraz ADSL umożliwiających dostęp do Internetu użytkownikom prywatnym z dużymi prędkościami. Do rewolucji w dziedzinie sieci należy także dodać rozwój sieci bezprzewodowych czy technologii P2P (Kurose, Ross, 2006; <http://www.scientist.pl/>).

1.2. Porównanie modelu TCP/IP z modelem ISO/OSI

Powstanie modeli TCP/IP oraz ISO/OSI wiązało się z szybkim rozwojem sieci w latach 80. Dostrzeżono wtedy konieczność ujednolicenia protokołów, w celu łatwego podłączania hostów a nawet całych sieci do już istniejących struktur. Do tego czasu każda istniejąca sieć stosowała najczęściej własne zamknięte protokoły, które uniemożliwiały komunikacje między ówczesnie istniejącymi strukturami sieciowymi oraz dalszy ich rozwój. Omawiane rozwiązania są modelami warstwowymi, czyli takimi, w których transmisja danych odbywa się w kilku etapach. Przedstawiane modele (Rys. 3.) posiadają cechy wspólne jak i zauważalne różnice w budowie (funkcjonowaniu) (Kurose, 2006; Krysiak, 2005).



Rys. 3. Porównanie modelu ISO/OSI z TCP/IP.

Podobieństwa:

- Obydwa modele mają budowę warstwową (prezentacja na rysunku powyżej);
- omawiane modele posiadają warstwę aplikacji, choć zestaw wykorzystywanych protokołów różni się;
- warstwy transportowe obydwu modeli oraz warstwa sieciowa modelu ISO/OSI i warstwa Internetowa modelu TCP/IP spełniają podobne funkcje.

Różnice:

- Pomimo budowy warstwowej liczba warstw w omawianych rozwiązaniach różni się;
- warstwa aplikacji modelu TCP/IP obejmuje funkcjonalnie warstwy aplikacji, prezentacji oraz sesji z modelu ISO/OSI;
- warstwa dostępu do sieci modelu TCP/IP obejmuje warstwy łącza danych oraz fizyczną.

Ważnymi z punktu widzenia funkcjonalności różnicami są także:

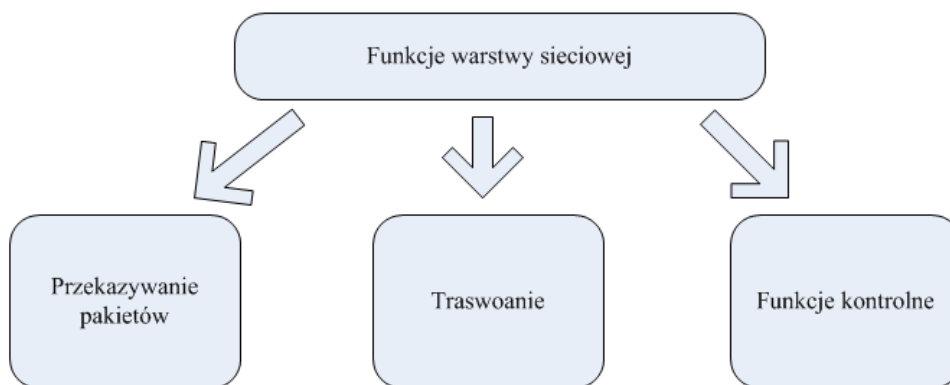
- łatwość implementacji modelu TCP/IP wynikająca z mniejszej ilości warstw;
- większa liczba warstw modelu ISO/OSI pozwala na łatwiejsze rozwiązywanie problemów z sieciami. (Krysiak, 2005; <http://www.ccnatut.info>; <http://www.rogaski.org>)

Model TCP/IP określany jest często mianem standardu Internetu, ponieważ został on wykorzystany do budowy sieci Internet. Wykorzystanie to uwarunkowane jest zdarzeniami historycznymi i wiąże się z tym, iż prace nad modelem ISO/OSI przedłużały się, natomiast w międzyczasie zestaw protokołów TCP/IP został wdrożony w sieci ARPAnet i zyskał dużą popularność. Obecnie praktycznie wszystkie sieci oparte są na modelu odniesienia TCP/IP, natomiast modelem OSI posługują się głównie producenci sprzętu sieciowego (<http://nss.et.put.poznan.pl>).

1.3. Warstwa trzecia jako podstawa funkcjonowania sieci LAN/WAN

Najważniejszym aspektem działania sieci komputerowych jest wymiana danych między jej użytkownikami (hostami) w obrębie sieci LAN oraz WAN, pozwala na to warstwa sieciowa modelu ISO/OSI. Dodatkowo umożliwia ona administratorom na sterowanie ruchem w sieciach komputerowych. Najważniejsze funkcje spełniane przez warstwę trzecią to (Rys. 4.):

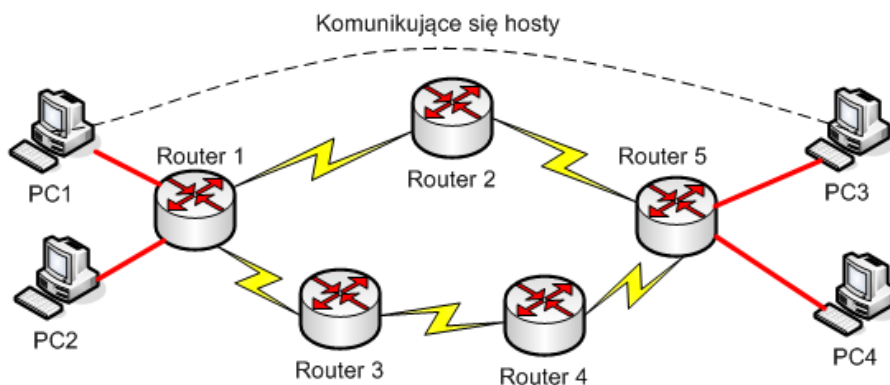
- Przekazywanie pakietów - przesyłanie pakietów od nadawcy do odbiorcy;
- Trasowanie – wyznaczanie tras dla pakietów przemierzających sieci WAN;
- Funkcje kontrolne – przesyłanie informacji o błędach.



Rys. 4. Funkcje warstwy trzeciej.

Warstwa sieciowa w celu przesyłania pakietów między hostami wykorzystuje różne protokoły. Najważniejszymi z nich są między innymi: IP, IPX, AppleTalk. W mojej pracy skupię się głównie na protokole IP w wersji 4. oraz 6. ze względu na dominującą pozycję

w obecnie wykorzystywanych sieciach komputerowych. Trasowanie natomiast pozwala na znalezienie jak najlepszej ścieżki do celu dla przesyłanego pakietu w sieciach nie połączonych bezpośrednio ze sobą. W takim wypadku trafia on do routera nazywanego bramą domyślną i tam, na podstawie zawartych informacji, przesyłany jest do kolejnego węzła w sieci (Rys. 4.) (Kurose, 2006; Hassan, Jain, 2004).



Rys. 5. Wymiana pakietów między sieciami nie posiadającymi bezpośredniego połączenia.

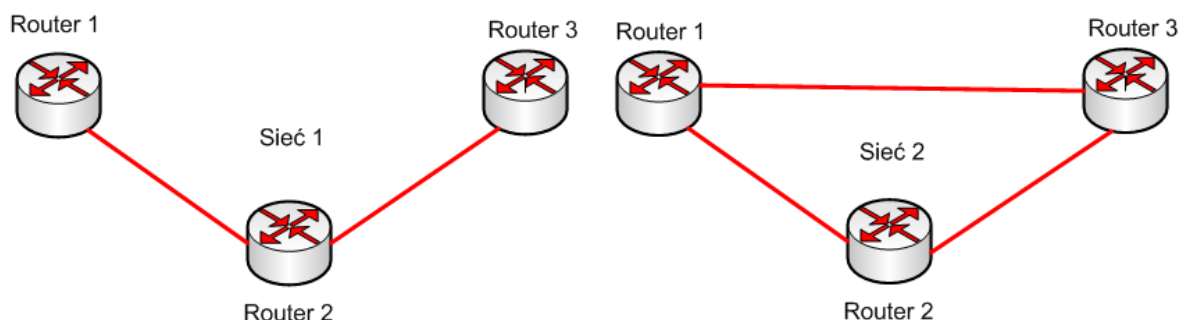
Przykład na Rys. 5. pokazuje, że podróż pakietu z jednego hosta do drugiego nie musi być wcale taka prosta. Komunikujące się komputery PC1 oraz PC3 znajdują się w różnych sieciach, które nie mają ze sobą bezpośredniego połączenia, w takim wypadku pakiet z PC1 trafia do routera, który następnie kieruje go do kolejnego węzła w sieci, aż do momentu gdy trafi on do celu. Schemat tego działania jest prosty w przypadku, gdy istnieje tylko jedna droga do sieci docelowej, w sytuacji przedstawionej na Rys. 5 (gdzie do hosta docelowego można dotrzeć korzystając z tras utworzonych przez Router 2 lub przez Routery 3 i 4) do sieci docelowej dotrzeć można korzystając z różnych tras i router musi wybrać odpowiednią z nich na podstawie posiadających informacji. Zbieranie informacji oraz ustalania najlepszej trasy do celu to zadanie routingu a dokładniej algorytmu trasowania. Bliżej funkcje trasowania przedstawię w dalszej części swojej pracy.

1.4. Redundancja w sieciach komputerowych na poziomie warstwy 3

Sieci komputerowe pełnią bardzo ważną rolę w dzisiejszym świecie, dlatego ich administratorzy muszą zapewnić ich prawidłowe funkcjonowanie. Jedną z wielu metod zapewniających prawidłowe działanie sieci jest nadmiarowość. Zapewnienie jej polega na powielaniu punktów newralgicznych na uszkodzenia np. większa liczba routerów czy połączeń między nimi, więcej połączeń między siecią LAN a WAN.

Metody stosowane dla uzyskania nadmiarowości zależne są od rodzaju sieci, w której ją stosujemy. W sieciach WAN czy dużych sieciach korporacyjnych gdzie występuje duża liczba węzłów sieciowych dąży się do zapewnienia ciągłości przesyłanych danych. Efekt

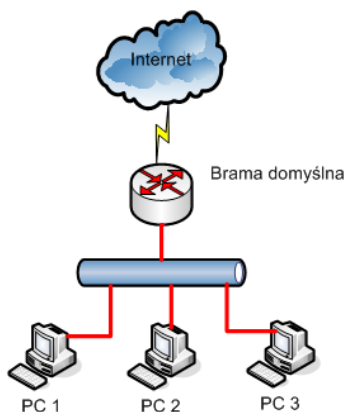
ten uzyskuje się przez dodawanie między węzłami połączeń nadmiarowych, które w wyniku awarii sprzętu czy połączenia głównego zezwolą na dalsze przenoszenie informacji (Oppenheimer, 2004).



Rys. 6. Nadmiarowość połączeń w sieciach.

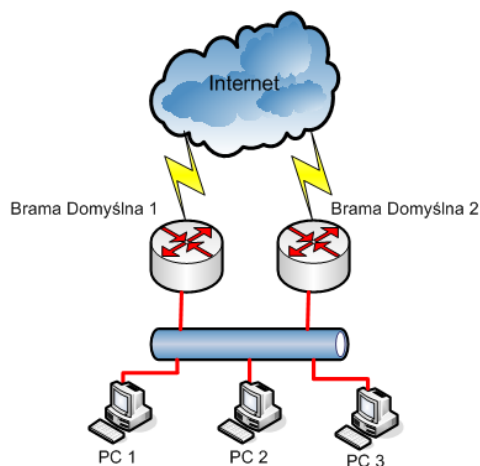
Sieć oznaczona numerem jeden na rysunku 6. nie zawiera połączeń nadmiarowych, dlatego w wypadku uszkodzenia któregośkolwiek z istniejących łącz bądź Routera 2 (ponieważ jest routerem pośredniczącym) nastąpią problemy z wymianą informacji między routerami np. gdy awarii ulegnie połączenie między Routerem 1 i 2, dane wysyłane do routera 2 i 3 nie dotrą do celu. Sytuację taką rozwiązuje się stosując trasę nadmiarową Rys. 6 Sieć 2. Dodatkowo pojawia się tu jeszcze połączenie nadmiarowe między Routerem 1 i 3, w sytuacji przedstawionej wcześniej to tą trasą będą przesyłane dane podczas awarii.

Komputery w sieciach LAN często komunikują się z urządzeniami znajdującymi się w innych sieciach, chociażby z serwerami w Internecie. Do tego typu komunikacji wykorzystywane jest urządzenie zwane bramą domyślną, jest to router, który otrzymuje dane od hostów w sieci wewnętrznej a następnie wysyła je dalej w kierunku celu. Brama domyślna jest najbardziej niewralgicznym punktem w sieci, ponieważ podczas jej awarii zaburzeniu ulega transmisja danych (Rys. 7).



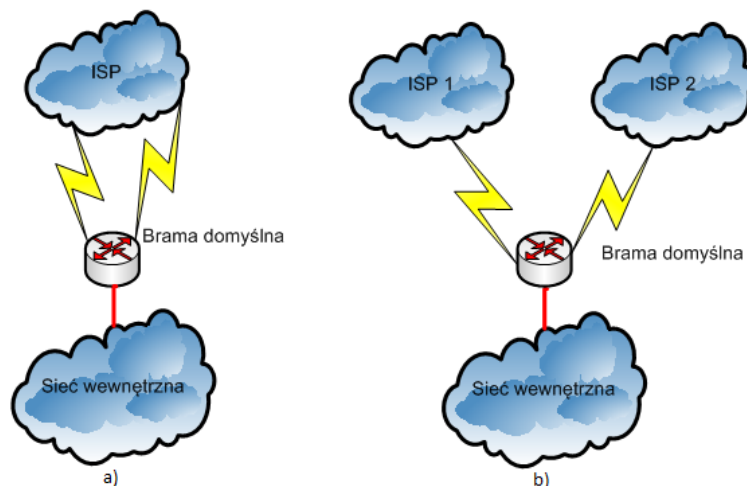
Rys. 7. Sieć bez redundancji bramy domyślnej.

Zagrożenia spowodowane awarią bramy domyślnej niweluje się stosując nadmiarowość bramy domyślnej. W takiej sytuacji, w razie awarii routera pełniącego tą rolę, jego zadanie przejmuje router zapasowy (Rys. 8). Nadmiarowość implementuje się przez podłączenie dodatkowych urządzeń i uruchomieniu na nich odpowiednich protokołów (Oppenheimer, 2004; <http://www.dell.com/>).



Rys. 8. Nadmiarowość bramy domyślnej.

Ważnym aspektem dobrze działającej sieci komputerowej jest bezawaryjne utrzymanie dostępu do sieci Internet. Sieci LAN uzyskują dostęp do Internetu wykorzystując dostawców usług internetowych (ISP – ang. *Internet Service Provider*). Administratorzy unikają przerw w dostępie do sieci globalnej wymykających ze strony ISP stosując dodatkowe łącza z jednym bądź wieloma usługodawcami. Dostęp do wielu ISP pozwala zachować połączenie w razie awarii występującej u jednego z dostawców. Najczęściej stosowane rozwiązania przedstawia Rysunek 9. (Oppenheimer, 2004).



Rys. 9. Nadmiarowość połączeń z dostawcą usług internetowych a) jeden ISP b) dwóch ISP.

2. Mechanizmy warstwy sieci wykorzystywane w sieciach IP

2.1. Protokół IP

Protokół IP jest mechanizmem warstwy sieci modelu ISO/OSI i jego głównym zadaniem jest zapewnienie możliwości komunikacji między odległymi od siebie systemami końcowymi. Przesyła on dane otrzymane od protokołów warstw wyższych (takich jak TCP (ang. *Transmission Control Protocol*) czy UDP (ang. *User Datagram Protocol*)) w postaci pakietów zwanych datagramami. Cechami charakterystycznymi tego protokołu są:

- bezpołączeniowość – nie tworzy połączeń podczas przesyłania datagramów;
- datagramowość – jak już wspomniałem wszystkie dane przesyłane są w postaci datagramów;
- działa na zasadzie „Najlepiej jak się da” (ang. *Best Effort*) – brak mechanizmów zapewniających niezawodność pozwalający na szybsze przesyłanie danych.

Innymi zadaniami spełnianymi przez protokół IP są:

- zapewnia jednolity sposób adresowania w całej sieci;
- wykonuje podział datagramu, jeżeli sieć do której trafił nie obsługuje danej jego wielkości (Krysiak, 2005; Hassan, 2004).

Współcześnie w użyciu są dwie wersje protokołu IP (wersja 4 oraz wersja 6). IPv4 jest protokołem starszym, który jest wypierany, ze względu na swoje ograniczenia, przez standard IPv6. Najważniejszymi zmianami, które przynosi nowy protokół są:

- zwiększenie puli adresowej z 32 do 128 bitów co rozszerzyło pulę adresową, dodatkowo zmiana ta ułatwia hierarchizację adresowania;
- uproszczenie struktury nagłówka przyspieszając przetwarzanie w węzłach sieci;
- wprowadzono ułatwienia w dodawaniu nowych opcji;
- zwiększono możliwości zapewnienia jakości usług (QoS - ang. *Quality of Service*);
- dodano opcje zapewniające bezpieczeństwo przesyłanych danych (<http://www.tech-portal.pl/>).

Nagłówek IPv4

W celu przesyłania danych przez sieć protokół IP wykorzystuje specjalny nagłówek (Rys. 10). Poniżej przedstawione są jego najważniejsze elementy:

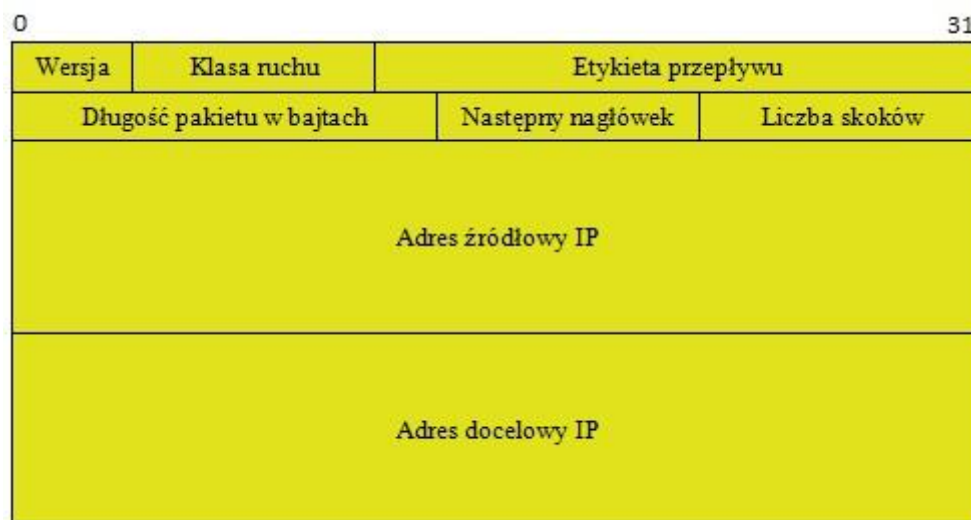
0				31	
Wersja	Długość nagłówka	Typ usługi	Całkowita długość		
Numer identyfikacyjny			Flagi	Kontrola przesunięcia	
TTL		Protokół warstwy wyższej	Suma kontrolna nagłówka		
Adres źródłowy IP					
Adres docelowy IP					
Opcje IP				Uzupełnienie	

Rys. 10. Nagłówek protokołu IPv4.

- Wersja – pole określające wersję wykorzystywanego protokołu;
- Długość nagłówka – określa rozmiar nagłówka, ponieważ pole Opcje IP może różnić się w zależności od wysyłanych danych;
- Typ usługi – pole umożliwiające ustawienie priorytetu dla pakietu, najczęściej stosowane przy mechanizmach zapewniania jakości usług czy routingu;
- Numer identyfikacyjny – identyfikuje datagram;
- Dwa kolejne pola wykorzystywane są przez system odbierający;
- TTL (ang. *Time To Live*) – określa liczbę skoków po których pakiet zostaje usuwany z sieci (zabezpieczenie przed powstawaniem pętli routingu);
- Suma kontrolna nagłówka – pozwala routerowi na sprawdzenie poprawności dostarczonego datagramu, w razie błędu pakiet jest odrzucany;
- Adres źródłowy oraz docelowy IP – określają odbiorcę oraz nadawcę na podstawie adresu docelowego routery znajdują odpowiednią trasę dla datagramów;
- Pole opcje – pole nieobowiązkowe, wykorzystywane głównie dla zapewnienia bezpieczeństwa czy odpowiedniego rodzaju routingu (RFC 791).

Nagłówek IPv6

Protokół IPv6 jako następca IPv4, który powstał prawie 30 lat temu, doczekał się wielu zmian i poprawek błędów swojego poprzednika. Wiele nowości i zmian można zauważyć już w budowie samego nagłówka (Rys. 11).



Rys. 11. Nagłówek protokołu IPv6.

Porównując nagłówki datagramu IPv4 oraz IPv6 zauważalne jest, że w nowszej wersji część pól nie zmieniła się np. pola: wersja, adres źródłowy IP czy adres docelowy IP (w dwóch ostatnich jedyna zmiana dotyczy długości pola, która została zwiększona). Łatwo także dojść do wniosku, iż część pól została po prostu usunięta. Resztę natomiast dodano albo zmieniono ich nazwy, a funkcje przedstawione są poniżej:

- Klasa ruchu – pole odpowiadające w nagłówku IPv4 polu Typ usługi;
- Etykieta przepływu – nowe pole pozwalające na określenie strumienia datagramów umożliwiające routerom na odpowiednie ich traktowanie (na poziomie warstwy sieciowej). Funkcja ta umożliwia np. odpowiednie traktowanie ruchu szyfrowanego bez potrzeby wglądu w jego zawartość;
- Rozmiar ładunku – określa ilość danych przesyłanych w pakiecie w bajtach bez rozmiaru nagłówka;
- Następny nagłówek – pełni podobne funkcje jak pole protokół warstwy wyższej w IPv4, dodatkowo tutaj również znajdować się mogą różne rodzaje nagłówków opcjonalnych;
- Liczba skoków – te same funkcje co TTL.

Poniżej znajdować się mogą nagłówki dodatkowe oraz przesyłane dane.

Nagłówki dodatkowe w przypadku protokołu IPv6 spełniają podobne funkcje jak pole opcji w IPv4. Liczba ich nie jest określona i układane są w odpowiedniej kolejności. Każdy kolejny nagłówek dodatkowy wyznaczany jest przez wartość *Następny nagłówek*. Mogą być w nich umieszczane takie informacje jak: nadmiarowość datagramu, dane potrzebne dla protokołu RSVP (ang. *Resource Reservation Protocol*) czy trasa nadana przez nadawcę dla protokołów trasowania (Kurose, 2006; <http://itpedia.pl/>; RFC 2460).

Adresowanie w sieciach IPv4

W sieciach IP wymagane jest, aby każde urządzenie końcowe było jednoznacznie określone. Umożliwia to mechanizm adresacji hostów zaprezentowany przez protokół IP. Wszystkie urządzenia podłączone czy to do sieci globalnej, czy też sieci lokalnej posiadają swój unikalny adres. W wersji 4 składa się on, jak już wspominałem, z 32 bitów i w postaci dziesiętnej przedstawiany jest za pomocą 4 liczb z zakresu od 1-255 rozdzielonych kropkami, natomiast wszystkie urządzenia korzystają z reprezentacji bitowej, która składa się z 4 oktetów bitów (Tab. 1).

Tab. 1. Adresy IPv4

Adres IP w postaci dziesiętnej	168.25.0.1
Adres IP w postaci binarnej	10101000 00011001 00000000 00000001

Każdy adres IP składa się z dwóch części:

- część sieci – fragment adresu określający sieć w Internecie;
- część hosta – fragment określający komputer w danej sieci.

Adresy w sieci Internet przydzielane są klientom przez odpowiednie organizacje prawidłowe dla danej lokalizacji geograficznej.

Typy adresów:

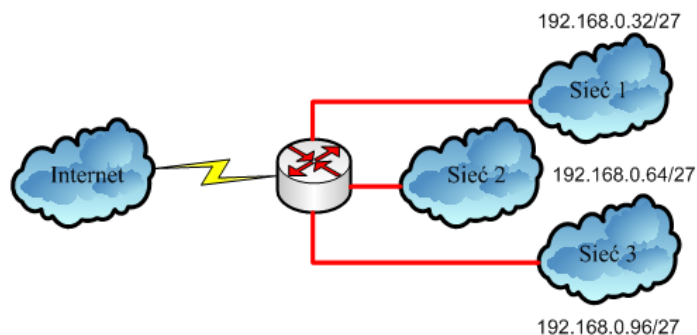
- adres unicastowy – charakteryzuje jeden określony system końcowy w sieci;
- adres multicastowy – adres tzw. „rozgłaszania grupowego” pozwala na rozsyłanie pakietów do hostów bezpośrednio zapisanych do grupy multicastowej. Do tego celu wykorzystywane są adresy z klasy D;
- adres broadcastowy – umożliwia dostarczenie pakietu do wszystkich hostów w sieci.

Początkowo adresy w Internecie określone były za pomocą klas (Tab. 2) rozróżnianych na podstawie kilku pierwszych bitów adresu. Do dyspozycji było 5 klas zawierających następujące zakresy adresów (Kurose, 2006; <http://www.staff.amu.edu.pl/>):

Tab. 2. Klasy adresów IPv4.

Klasa A	Przeznaczone dla dużych firm. Pozwala na wydzielenie 127 sieci, z których każda może zawierać 16 mln. hostów	1.0.0.1 – 127.255.255.254 127.x.x.x – służą do celów diagnostycznych
Klasa B	Przygotowane z przeznaczeniem dla średnich firm z liczbą urządzeń końcowych na poziomie 65535	128.0.0.1 - 191.255.255.254
Klasa C	Wykorzystywane w małych sieciach lokalnych z liczbą hostów nie przekraczającą 256	192.0.0.1 - 223.255.255.254
Klasa D	Dla celów specjalnych	224.0.0.1 – 239.255.255.254
Klasa E		240.0.0.1 – 247.255.255.254

Niestety podział na klasy w miarę ekspansji sieci komputerowych nie sprawdził się ze względu na zbyt dużą niegospodarność adresami. Przykładem może być sieć, w której znajduje się 400 hostów. W erze adresowania klasowego sieć taka musiałaby otrzymać adres z klasy B, w takim wypadku niewykorzystane adresy pozostają bezużyteczne. Problem ten rozwiązano stosując adresowanie z uwzględnieniem podsieci lub potocznie adresowaniem bezklasowym. Mechanizm ten polegał na podziale adresu IP na część sieci oraz hosta, których długość określa maska podsieci. Przykładem może tu być router posiadający kilka sieci fizycznych (Rys. 12), do ich adresowania wykorzystana zostaje jedna pula adresów klasy C (192.168.0.0/24). Adresowanie z podziałem na podsieci wykorzystuje część bitów z części hosta jako dodatkowe bity dodawane do części sieci. Pozwala to na wykorzystanie jednej puli adresów na zaadresowanie wielu podsieci. Należy zauważyć fakt, iż o sieciach wewnętrznych wiedzą jedynie routery wewnątrz niej, natomiast routery zewnętrzne traktują wnętrze sieci jako jedną sieć fizyczną i przesyłają datagramy do routera brzegowego, który dalej kieruje je do odpowiedniej podsieci (Comer, 1998; CCNA Exploration: Network Fundamentals).



Rys. 12. Adresowanie sieci z podsieciami.

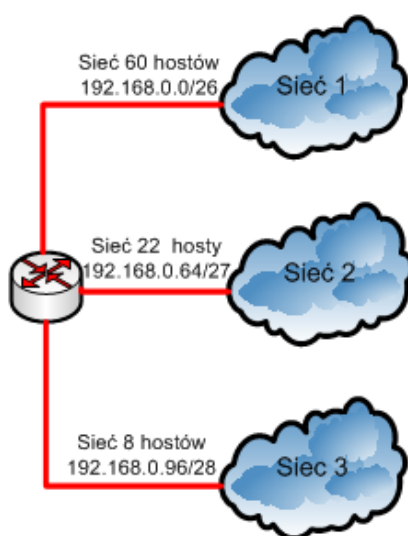
Maska podsieci podobnie jak adres IP składa się z 32 bitów reprezentowanych dziesiętnie przez 4 liczby oddzielone kropkami (można ją także przedstawić w postaci prefiksu np. /24 lub równoznacznie 255.255.255.0). Wykorzystywana jest ona do rozdzielania adresu sieci oraz adresu hosta, umożliwia to routerom przesłanie pakietu do odpowiedniej sieci fizycznej oraz hosta. Załóżmy, że mamy urządzenie o adresie IP 212.194.40.2 i maską podsieci 255.255.240.0, aby odczytać w jakiej sieci znajduje się system końcowy obie liczby należy zapisać w postaci binarnej i wykonać między nimi logiczną operację AND (Tab. 3).

Tab. 3. Zastosowanie maski podsieci.

Adres urządzenia	11010100 11000010 00101000 00000010
Maska sieci	11111111 11111111 11110000 00000000
Sieć w której znajduje się urządzenie	11010100 11000010 00100000 00000000

Adres sieci reprezentowany dziesiętnie: 212.194.32.0.

Kolejnym udoskonaleniem mechanizmu adresowania jest wykorzystanie maski podsieci o zmiennej długości VLSM (ang. *Variable Length Subnet Mask*) co pozwala na elastyczne wykorzystanie dostępnych adresów IP. Adresacja tą metodą polega na zastosowaniu różnych długości masek podsieci w obrębie jednej sieci (Rys. 13).



Rys. 13. Zastosowanie technologii VLSM.

Przedstawiając adresowanie w protokole IPv4 należy także wspomnieć o adresach nierutowalnych tzw. prywatnych, czyli takich, które mogą zostać użyte wyłącznie w sieciach lokalnych. Należą do nich 3 grupy adresów: (Kurose, 2006; CCNA Exploration: Network Fundamentals):

10.0.0.0 – 10.255.255.255 (10.0.0.0 /8)
172.16.0.0 – 172.31.255.255 (172.16.0.0 /12)
192.168.0.0 – 192.168.255.255 (192.168.0.0 /16)

Obecnie do globalnej sieci zaczyna się wprowadzać już wersje 6 protokołu IP a wraz z tym odpowiadające mu adresowanie, które zdecydowanie różni się od starego modelu.

Architektura adresacji w protokole IPv6

Wraz z wprowadzeniem do użycia najnowszej wersji protokołu IP zmianie uległ sposób adresowania systemów końcowych. Zmiany te wynikały z powiększenia adresu z 32 do 128 bitów oraz dodatkowych funkcjonalności jakie przynosiła wersja 6 tego protokołu.

Adres IPv6 składa się 8 liczb zapisanych w systemie szesnastkowym, każda z nich oddzielona jest dwukropkiem. Adres taki wygląda następująco:

FF01:0:0:0:456:FEDC:0:88

Ewentualnie w postaci skróconej zastępując zera w adresie kombinacją :: (wykorzystywane tylko raz w danym adresie), można ten sam adres zapisać jako:

FF01::456:FEDC:0:88

Protokół IPv6, podobnie jak jego poprzednik, również rozróżnia 3 kategorie adresów IP tylko z jedną różnicą: zamiast adresu rozgłoszeniowego do dyspozycji mamy adres rejonowy (grupowy). Dane dostarczane na taki adres trafiają do grupy (hosty pracujące w jednej sieci fizycznej, czyli mające ten sam prefiks sieci), następnie w jej obrębie rozsyłane są do urządzenia docelowego. Pozostałe dwie kategorie adresów pokrywają się z tymi poznanymi wcześniej (Krysiak, 2005).

W architekturze adresów IPv6 rozróżniamy także kilka typów adresów unicastowych:

- adres globalny (ang. *Global Address*) – jest on równoznaczny z adresem publicznym IPv4, Link-Local Address – typ adresu wykorzystywany do automatycznej adresacji hostów lub odkrywania sąsiadów. Funkcjonujący podobnie jak system automatycznej adresacji w protokole IPv4;
- Site-Local Address – adres wycofany z użycia;
- unikalne adresy lokalne (ang. *Unique Local Address*) – funkcjonalnie porównywalne do adresów prywatnych w IPv4; podobnie ruch w tych sieciach nie podlega trasowaniu do sieci globalnej;
- Adresy IPv6 zawierające IPv4 – ich zadaniem jest ułatwienie komunikacji między sieciami IPv6 i starszymi;

- adresy specjalne, takie jak: adres pętli zwrotnej oraz adres nieokreślony (<http://www.tech-portal.pl>).

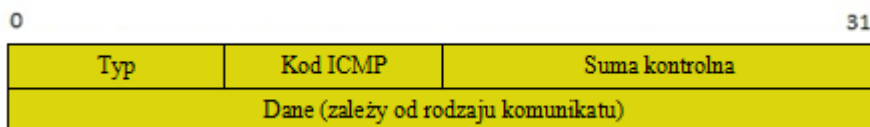
Wady protokołu IP

Protokół IP dzięki swojemu modelowi komunikacji do dnia dzisiejszego wykorzystywany jest w sieciach komputerowych do transmisji danych, niestety to z nim wiąże się wiele jego wad. Protokół nie zapewnia niezawodności co z jednej strony pozwala na szybsze dostarczanie datagramów, ale wiąże się z ich gubieniem i odrzucaniem w węzłach. Utracone w ten sposób dane muszą zostać retransmitowane przez mechanizmy warstw wyższych. Zapewnić muszą one także, obsługę datagramów, które nie są dostarczane w kolejności, ponieważ protokół komunikacyjny nie ma wpływu na kolejność ich dostarczania, ze względu na losowość tras, po których dostarczane są do celu (Hassan, 2004). Z punktu widzenia protokołu IP nieznana jest także szybkość jak i opóźnienia powstałe podczas przesyłania datagramów do celu, chyba że wykorzystane zostaną techniki QoS umożliwiające kontrolowanie tych parametrów. Niestety sam protokół IP nie wykorzystuje technik zapewniania jakości usług i konieczne jest stosowanie mechanizmów zewnętrznych co wiąże się z dodatkowymi kosztami.

Największymi mankamentami protokołu IP są: brak wbudowanych mechanizmów zabezpieczania przesyłanych przez sieci danych oraz ograniczona pula adresów IPv4 (obecnie pula ta się już wyczerpała a wdrażanie IPv6 postępuje bardzo wolno). Zabezpieczenie przesyłanych datagramów realizowane jest przez zbiór protokołów określony mianem IPsec (ang. *IP Security*) (Kurose, 2006, <http://twojepc.pl/>).

2.2. Protokół ICMP

Protokół ICMP (ang. *Internet Control Message Protocol*) podobnie jak protokół IP jest częścią warstwy sieciowej modelu ISO/OSI, nazywany jest często protokołem kontrolnym Internetu. Komunikat ICMP (Rys. 14) przenoszony jest bezpośrednio w datagramie IP.



Rys. 14. Pakiet ICMP.

- Pola Typ oraz Kod ICMP określają rodzaj wysyłanego komunikatu;
- Suma kontrolna – wykorzystywana do kontroli błędów.

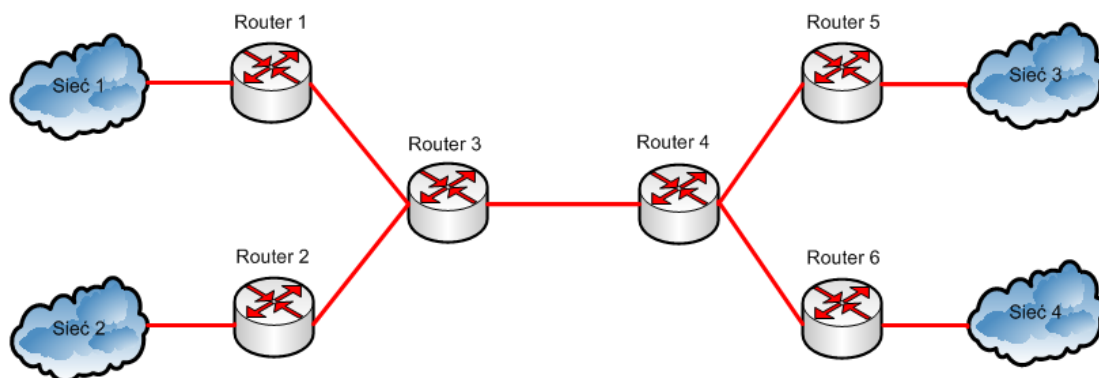
Do jego zadań należą m.in.

- Kontrolowanie przepływu danych; np. w przypadku gdy komputer odbierający nie nadąża z przetwarzaniem datagramów, wysyłany jest komunikat o chwilowym przerwaniu nadawania;
- Rozsyłanie komunikatów o braku możliwości dostarczenia datagramu (błędy typu: cel nieosiągalny, host nieosiągalny, sieć nieosiągalna itp.);
- Do przekierowywania tras przez routery; router odbierający datagram przy pomocy komunikatu ICMP wskazuje lepszego kandydata na bramkę w danej sieci;
- W przypadku wyzerowania wartości TTL, wysyłana jest informacja do źródła o przekroczeniu czasu.

Przygotowana także została wersja protokołu ICMP dla protokołu IPv6. Strukturalnie nagłówki dla obu wersji ICMP jest taki sam, różnice wynikają np. ze sposobu obliczania pola checksum, czy też innych rodzajów przesyłanych komunikatów. Inną zmianą w porównaniu do poprzedniej wersji ICMP, jest dodanie funkcjonalności IGMP (ang. *IPv4 Group Membership Protocol*) (Krysiak, 2005; www.winsocketdotnetworkprogramming.com).

2.3. Sieci IP

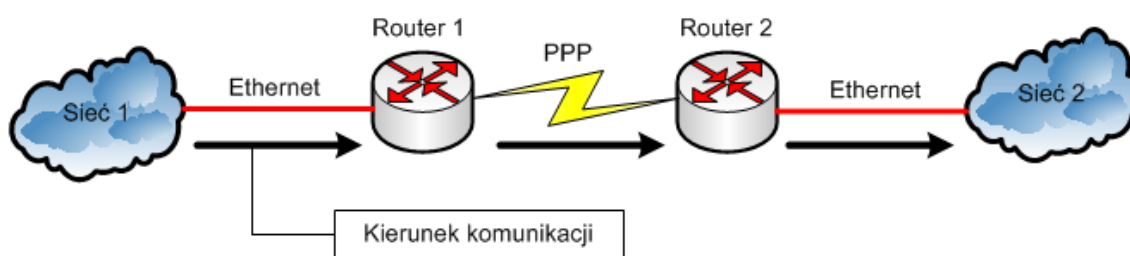
Zbiór niezależnych komputerów połączonych ze sobą za pomocą urządzeń sieciowych oraz mediów transmisyjnych określany jest mianem sieci komputerowych. Sieci IP są właśnie takimi sieciami wykorzystującymi do komunikacji między urządzeniami zbiór protokołów TCP/IP. Obecnie wyróżnia się sieci o różnym poziomie złożoności od jednosegmentowych (gdzie komunikacja zachodzi bezpośrednio między hostami bez wykorzystania routerów), po sieć typu Internet gdzie połączonych ze sobą jest wiele segmentów (Rys. 15) i w wymianie danych uczestniczą routery (Tanenbaum, 2004).



Rys. 15. Sieć wielosegmentowa.

Wymiana danych w sieciach IP

Celem połączenia urządzeń w sieci komputerowe jest wymiana danych między nimi. Sieci IP do wymiany danych wykorzystują zbiór protokołów TCP/IP, a dokładnie protokół komunikacyjny IP. Dane trafiające z warstwy wyższej do warstwy sieciowej enkapsulowane są w datagram IP przez dodanie nagłówka IP zawierającego informacje konieczne do jego przesłania. Tak przygotowany datagram trafia do warstwy łącza danych gdzie przez dodanie kolejnego nagłówka enkapsulowany jest w ramkę i to ona przesyłana jest do celu. W sieciach jednosegmentowych, gdzie wymiana informacji odbywa się bez pośrednictwa routerów, dane trafiają od razu do miejsca przeznaczenia i tam są odpowiednio przetwarzane. Niestety obecna złożoność sieci komputerowych i różnorodność stosowanych technologii transmisji nie pozwala na tak proste przesyłanie danych. Często zdarza się, że datagram przed dotarciem do miejsca docelowego przemierza wiele sieci komputerowych wykorzystujących różne technologie transmisji (Ethernet, PPP itp.) (Kurose, 2006; Tanenbaum, 2004).



Rys. 16. Przesyłanie datagramów przez sieć złożoną.

W sieci złożonej przedstawionej na Rysunku 16, informacje przesyłane z sieci 1 do sieci 2 muszą zostać przetransportowane przez sieci wykorzystujące różne technologie transmisji połączone routerami. Ramka podróżuje pierwotnie przez sieć Ethernet gdzie jej maksymalny rozmiar może wynosić 1500 bajtów tzw. MTU (ang. *Maximum Transfer Unit*), w kolejnym etapie dane trafiają do Routera 1 skąd muszą zostać przetransportowane do Routera 2. Urządzenia połączone są technologią punkt-punkt PPP (ang. *Point-to-Point Protocol*), w której maksymalny rozmiar ramki wynosi 296 bajtów. Sytuacja ta wymusza na Routerze 1 fragmentację otrzymanych w ramach datagramów i ponowne umieszczanie ich w odpowiedniej ramce w celu dalszego przesłania. Mechanizm fragmentacji udostępnia protokół IP. Każdy powstały w wyniku tego procesu fragment traktowany jest jako oddzielny datagram i może samodzielnie podróżować przez sieć. Dodatkowo podczas fragmentacji ustawiane są pola: Flagi oraz Kontrola przesunięcia w celu późniejszego scalenia. W Routerze 2 następuje składanie fragmentów i przesłanie ich w postaci ramek do celu.

Urządzenia wykorzystywane w sieciach IP

Nad dostarczaniem datagramów do celu w sieciach komputerowych pracuje wiele urządzeń. Rozróżnia się je ze względu na funkcjonalność:

- Urządzenia warstwy dostępu do sieci:
 - Przełącznik (ang. *Switch*) – łączy segmenty sieci i przesyła ramki między nimi;
 - Koncentrator (ang. *Hub*) – propagacja danych poprzez powielanie sygnału wejściowego na wszystkie interfejsy wyjściowe;
 - Bezprzewodowe punkty dostępu (ang. *Wireless Access point*) – zapewniają możliwość podłączania się systemów;
- Urządzenia warstwy sieciowej:
 - Routery – urządzenia odpowiedzialne za przesyłanie danych między sieciami;
 - Przełączniki warstwy 3 – Urządzenie podobne w działaniu do routera służy do przetwarzania pakietów, nie wykorzystuje jednak procesora a układy cyfrowe ASIC;
- Urządzenia warstwy aplikacji, czyli serwery oraz systemy końcowe (Ogletree, 2001).

Zgodnie z tematem pracy bliżej przedstawione zostaną urządzenia pracujące w warstwie sieciowej.

2.4. Modyfikacja datagramów w trakcie podróży

Datagramy w trakcie swojej podróży mogą ulegać różnym modyfikacjom. Zmian dokonują administratorzy stosując różne mechanizmy w celu sterowania ich ruchem w żądany przez nich sposób. Do najpopularniejszych tego typu mechanizmów należą:

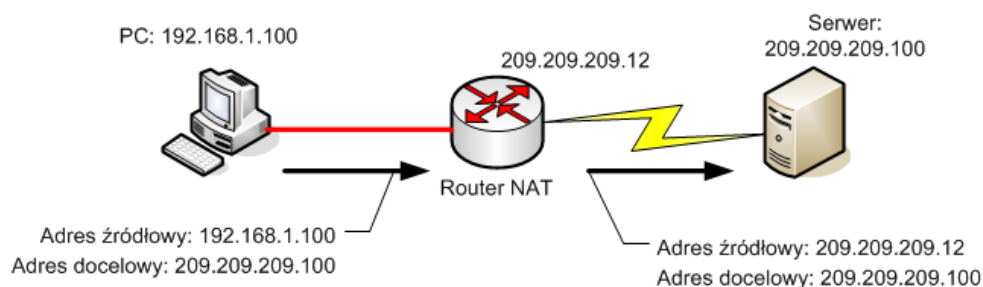
- Translacje adresów sieciowych NAT – zmianom ulegają adresy, źródła lub celu, ewentualnie na poziomie warstwy transportowej adresy portów;
- Wirtualne sieci prywatne VPN (ang. *Virtual Private Network*) – podczas przesyłania do datagramów dodawane są dodatkowe nagłówki.

Translacja adresów sieciowych

Operatorzy sieci komputerowych wykorzystują mechanizm NAT z dwóch głównych powodów: udostępnienie dostępu do Internetu komputerom wewnątrz sieci oraz zabezpieczenie pracujących w niej urządzeń. Hosty funkcjonujące wewnątrz sieci prywatnej, aby uzyskać dostęp do sieci globalnej, musiałyby posiadać własny publiczny adres IP. Współcześnie możliwość taka praktycznie nie istnieje ponieważ najpopularniejszym

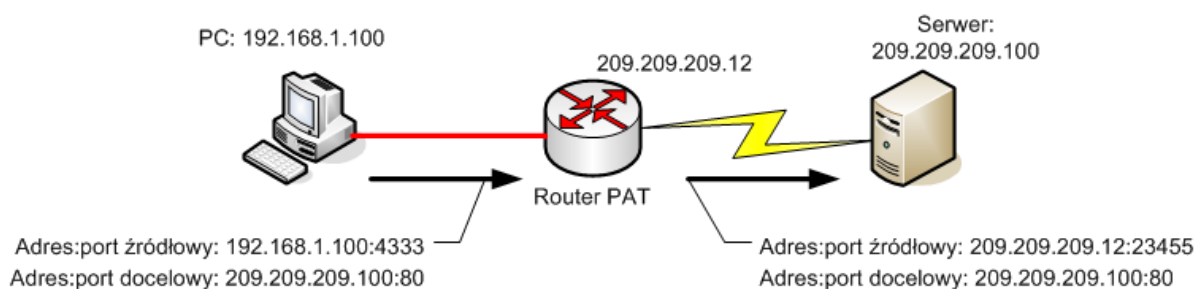
standardem adresowania nadal jest IPv4, którego pula adresowa jest ograniczona w porównaniu do liczby urządzeń uzyskujących dostęp do Internetu. Administratorzy wykorzystując mechanizm translacji adresów sieciowych modyfikują datagram w taki sposób aby hosty wewnątrz sieci mogły bez problemu korzystać z zasobów sieci globalnej. Translacja adresów może się odbywać na poziomie różnych warstw w zależności od zastosowanego mechanizmu.

- Translacja na poziomie warstwy sieciowej potocznie zwana NAT (Rys. 17) – zmianie ulega adres źródłowy datagramu IP. Komputer PC wysyła datagram ze swoim adresem źródłowym oraz adresem docelowym serwera, przechodząc przez Router NAT. Modyfikacji ulega adres źródłowy na adres interfejsu wyjściowego routera. W drodze powrotnej modyfikacji ulegają odpowiednio adres docelowy, tak aby datagram mógł wrócić do komputera PC. W tym wypadku, oprócz zmian adresów, translacji ulegają także pola sum kontrolnych nagłówka IP i TCP bądź UDP.



Rys. 17. Działanie NAT.

- Translacja na poziomie warstwy transportowej zwana potocznie PAT (ang. *Port Address Translatio*) (Rys. 18) – modyfikuje pola zarówno w nagłówku IP jak i nagłówku warstwy 4. Zmianom ulegają odpowiednio: adres IP oraz numer portu źródła a także sumy kontrolne nagłówka IP i TCP/UDP. Komputer PC wysyła datagram IP z własnym adresem źródłowym oraz numerem portu (192.168.1.100:4333). Podczas transportu Router PAT modyfikuje źródłowy adres IP oraz numer portu na 209.209.209.12:23455 i przesyła datagram do serwera. W drodze powrotnej modyfikacjom ulegają odpowiednio adresy celu, tak, aby trafił one z powrotem do komputera (Krysiak, 2005; RFC 2663; CCNA Exploration: Accessing the WAN; <http://www.tech-portal.pl>).



Rys. 18. Działanie PAT.

Administratorzy sieci wykorzystujący mechanizm NAT mają do swojej dyspozycji dodatkowo dwa jego warianty zależne od potrzeb danej sieci. Statyczna translacja adresów Static NAT (ang. *Static Network Address Translation*) polega na ręcznym mapowaniu adresów prywatnych na publiczne przez użytkownika. W wariancie tym adresy mapowane są 1-do-1 co oznacza, że ten sam adres prywatny zawsze będzie tłumaczony na ten sam adres publiczny. Drugim wariantem NAT jest dynamiczna translacja adresów sieciowych Dynamic NAT (ang. *Dynamic Network Address Translation*), gdzie administrator ustawia pulę adresów, które mogą zostać użyte do translacji i przy każdej nowej sesji adres zewnętrzny jest przydzielany dynamicznie, i nie musi być to zawsze ten sam adres (Krysiak, 2005; <http://www.tech-portal.pl>).

Wirtualne sieci prywatne

Technologią, w której administratorzy ingerują w przepływ datagramów przez sieć są wirtualne sieci prywatne. Służą one do bezpiecznego łączenia sieci między oddziałami firmy porozerzucanymi po całym świecie, bądź dla zapewnienia bezpiecznego łącza między pracownikiem pracującym w domu lub w podróży a centralą firmy. Rozwiązanie to jest stosowane ze względu na duże bezpieczeństwo i zarazem stosunkowo niski koszt utrzymania w odróżnieniu od dedykowanych połączeń kablowych. Wirtualne sieci prywatne w celu spełnienia swojego przeznaczenia muszą zapewniać różne parametry (Tab. 4.).

Tab. 4. Cechy Wirtualnych sieci prywatnych.

Parametr	Powód wykorzystania
Integralność danych	Ochrona przed manipulowaniem i modyfikowaniem danych
Poufność danych	Zabezpieczenie danych przed podsłuchiowaniem
Uwierzytelnianie	Zapewnia, że dane pochodzą od pewnego źródła i trafiają do właściwego celu

Zasada działania wirtualnych sieci prywatnych polega na przesyłaniu danych przez ogólnie dostępną sieć prywatną w postaci bezpiecznej, często przesyłanie takie nazywa się tunelowaniem, ponieważ dane są szyfrowane i umieszczane w nowym datagramie, i tak

są transportowane przez sieć publiczną do celu (Rys. 19). Prawidłowe funkcjonowanie VPN opiera się o różne mechanizmy umożliwiające szyfrowanie i tunelowanie informacji przez sieć. Do pracujących w warstwie sieci należą m.in.: protokół GRE (ang. *Generic routing encapsulation*) oraz bardziej popularny IPSec ze względu na to, że jest to cały szablon składający się z wielu otwartych standardów dających mu dużą elastyczność i to właśnie z tego powodu przedstawię go w swojej pracy (Krysiak, 2005; CCNA: Accessing the WAN).



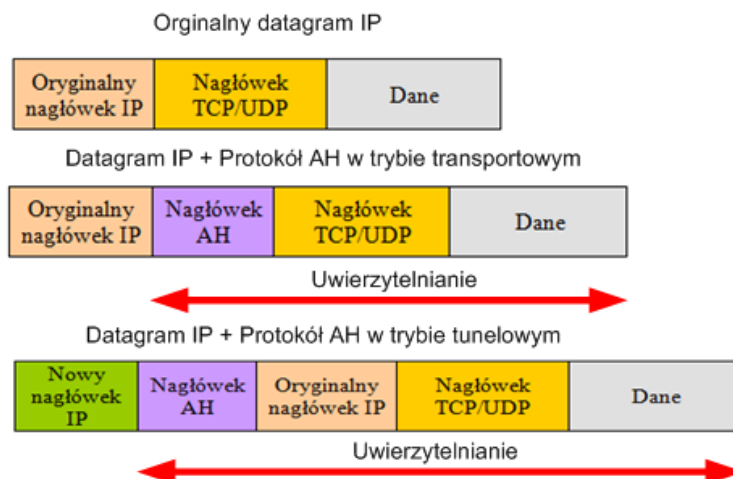
Rys. 19. Działanie Wirtualnej Sieci Prywatnej.

IP Security

IPSec jest zbiorem protokołów opracowanych przez IETF (ang. *The Internet Engineering Task Force*) w celu zapewnienia bezpiecznej transmisji pakietów przez sieć. Funkcjonowanie IPSec opierać się może na dwóch różnych protokołach bezpieczeństwa, z których oba pracować mogą w trybie transportowym oraz tunelowym.

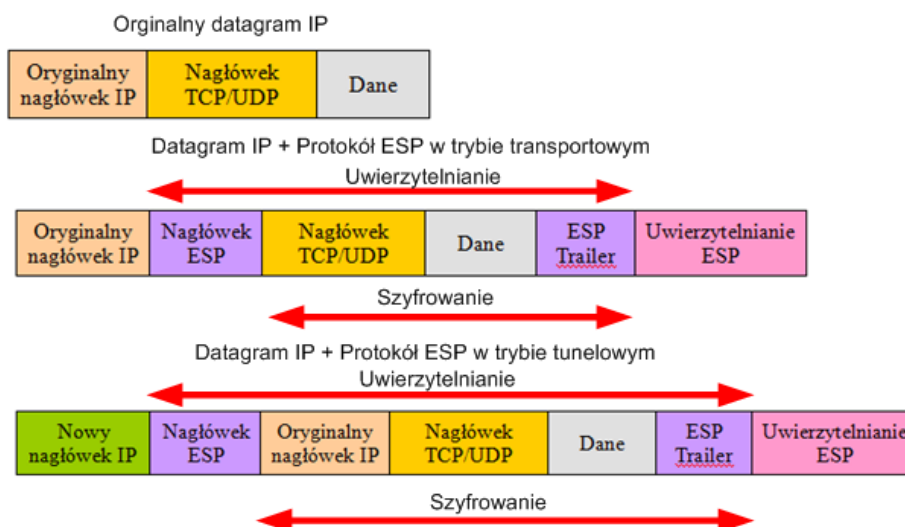
- Tryb transportowy - zabezpieczeniu ulegają jedynie dane warstw powyżej warstwy sieciowej;
- Tryb tunelowy zapewnia zabezpieczenie dla całego datagramu IP i w celu dalszego przesłania enkapsuluje go w nowym datagramie IP.

Protokół AH (ang. *Authentication Header*) zabezpiecza dane zawarte w datagramie przed modyfikacją oraz przed odebraniem pakietu przez nieupoważnionego hosta. Żadne informacje w nim zawarte nie zostają zaszyfrowane. Protokół AH do zapewnienia integralności i uwierzytelniania wykorzystuje m.in. algorytmy mieszające SHA1, MD5 oraz klucze RSA i PSK. Budowę datagramu IP przy wykorzystaniu protokołu AH przedstawia Rysunek 20.



Rys. 20. Umieszczenie nagłówka protokołu AH w datagramie.

Drugim wykorzystywanym przez IPSec protokołem bezpieczeństwa jest protokół ESP (ang. *Encapsulation Security Payload*). Dzięki możliwości szyfrowania danych zawartych w datagramie zyskuje zdecydowaną przewagę nad protokołem AH, ponieważ lepiej zabezpiecza przesyłane dane. Szyfrowanie ich przebiegać może z wykorzystaniem jednego z kilku algorytmów (np. DES, 3DES czy Rijndael/AES). Budowę datagramu przy wykorzystaniu protokołu AH przedstawia Rysunek 21 (Krysiak, 2005; CCNA: Security).

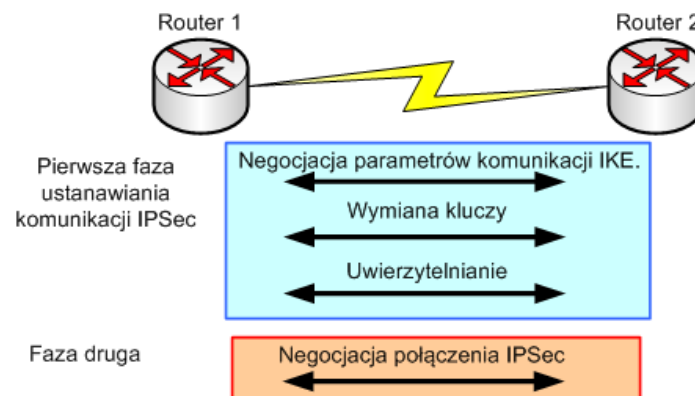


Rys. 21. Umieszczenie elementów nagłówka ESP w datagramie.

Funkcjonowanie IPSec opiera się na ustanowieniu połączenia między węzłami sieci uczestniczącymi w zabezpieczonej wymianie danych. Działanie połączeniowe IPSec wydaje się nietypowe ze względu na jego mechanizmy pracujące na poziomie warstwy sieciowej współpracujące z bezpołączeniowym protokołem IP. Twórcy doszli jednak do wniosku, iż zapewnienie bezpieczeństwa wymaga ustanowienia szyfrowanego połączenia (w sensie logicznym, ponieważ polega ono na utrzymaniu jednego klucza szyfrującego przez pewien

okres komunikacji) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Sesje IPSec są jednokierunkowe, więc w celu uzyskania w pełni dwustronnego bezpiecznego połączenia konieczne jest utworzenie dwóch oddzielnych sesji. Połączenia takie nazywane są skojarzeniem bezpieczeństwa SA (ang. *Security Association*), aby zostały utworzone urządzenia muszą posiadać te same parametry. Zestawianie sesji w przypadku IPsec odbywa się wykorzystując protokół IKE (ang. *Internet Key Exchange*) w 2 fazach (Rys. 22):

- Ustawianie kanału komunikacji dla IKE;
- Negocjowanie połączenia IPSec (CCNA: Security; Tanenbaum, 2004) .

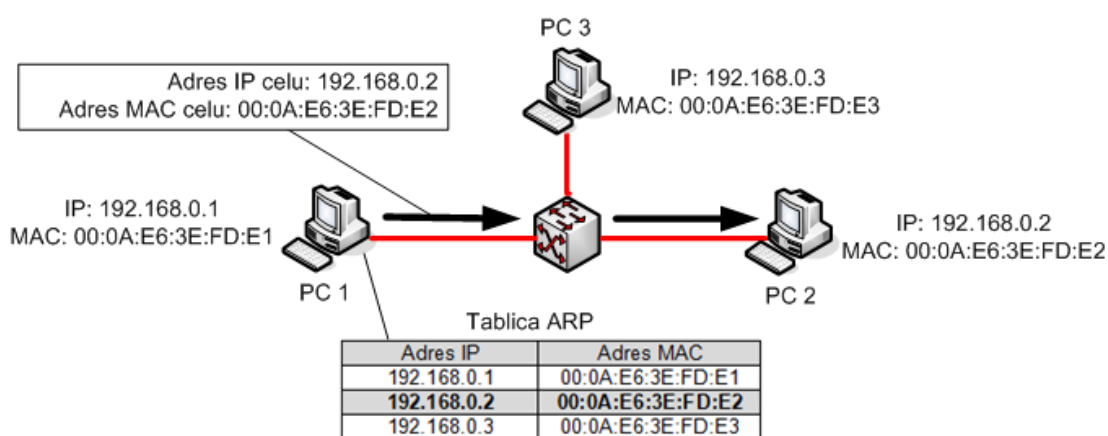


Rys. 22. Zestawianie bezpiecznego połączenia IPSec.

3. Metody sterowania ruchem wykorzystywane w sieciach opartych na protokole IP

3.1. Kształtowanie ruchu pakietów z wykorzystaniem routingu

Warstwa sieciowa modelu ISO/OSI odpowiada za transmisję danych między nadawcą a odbiorcą. Służą do tego dwa mechanizmy wykorzystywane w zależności czy urządzenia znajdują się w jednej sieci czy nie. W przypadku komputerów znajdujących się w jednej sieci proces ten jest stosunkowo prosty. Host źródłowy wykorzystując tablice ARP (ang. *Address Resolution Protocol*) uzyskuje adres Ethernetowy urządzenia docelowego i wysyła do niego datagramy (Rys. 23).



Rys. 23. Przesyłanie pakietów w obrębie jednej sieci.

Mechanizm przesyłania komplikuje się w dużych sieciach składających się z wielu segmentów połączonych za pomocą routerów. Zadaniem ich jest przesyłanie datagramów między dwoma różnymi sieciami fizycznymi (segmentami), tak aby trafiły do celu jak najszybciej oraz z najmniejszym możliwym opóźnieniem. Proces ten określany jest mianem trasowania. Wszystkie routery na drodze od źródła do celu tworzą tzw. ścieżkę (trasę) czyli inaczej logiczną drogę między odbiorcą a nadawcą. Każdy router w sieci jest urządzeniem autonomicznym i sam na podstawie informacji które posiada, kieruje pakiet IP do kolejnego miejsca w sieci (Kurose, 2006; Krysiak, 2005). Idealnym przykładem sieci wielosegmentowej jest Internet, składający się z wielu tzw. Systemów Autonomicznych.

Systemy Autonomiczne

Terminem systemu autonomicznego określany jest zbiór routerów pracujących pod nadzorem jednej organizacji, wykorzystujących wspólną politykę trasowania w obrębie systemu (może korzystać z kilku protokołów trasowania w obrębie AS – ang. *Autonomous*

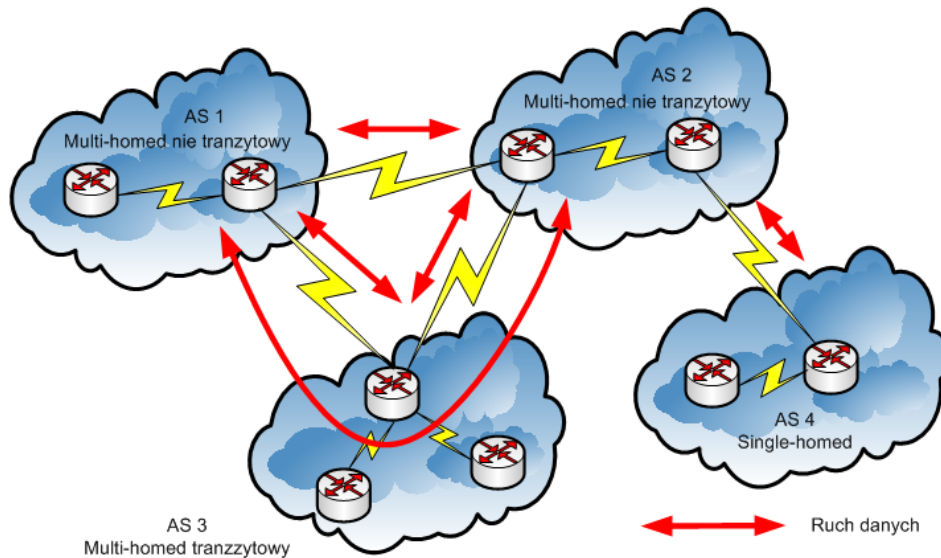
System). Powstanie systemów autonomicznych wymuszone było przez wzrost złożoności obecnych sieci komputerowych, chociażby sieci globalnej Internet. Podział taki sieci Internet wymuszony był z dwóch powodów:

- Wymiana informacji o trasach w tak dużej sieci generowałaby ogromny ruch;
- Problemy administracyjne – każda organizacja (najczęściej dostawcy usług internetowych, bądź duże korporacje) musi mieć możliwość zastosowania własnych koncepcji działania sieci (ukrycie informacji o sieci wewnętrznej, zastosowanie wybranego algorytmu trasowania)

Podział taki zapewnia autonomię w zarządzaniu siecią przez organizacje a jednocześnie optymalną komunikację między systemami autonomicznymi (szybsze trasowanie itd.). (Kurose, 2006; Halbi, 2000; RFC 1930).

Systemy autonomiczne mogą być połączone z resztą sieci w różny sposób (Rys. 24):

- Single-homed – ruch z systemu autonomicznego kierowany jest do reszty sieci przez dokładnie jeden inny system autonomiczny. W przypadku tego typu komunikacji, w razie awarii połączenia następuje brak dostępu do sieci globalnej;
- Multi-homed – System autonomiczny uzyskuje dostęp do sieci wykorzystując dwa bądź więcej pośredniczących systemów autonomicznych (np. ISP). Dzięki alternatywnym połączeniom zmniejsza się ryzyko utracenia dostępu do sieci w wyniku awarii. Dodatkowo połączenia te pozwalają administratorom na kierowanie danej klasy ruchu przez wybrane łącze. Tego typu połączenia dzielimy na dwie grupy:
 - Nie tranzytowe – system autonomiczny nie może być pośrednikiem w wymianie informacji między innymi systemami autonomicznymi;
 - Tranzytowy - umożliwia pośredniczenie w wymianie danych między systemami autonomicznymi. (<http://fatcat.ftj.agh.edu.pl>, Kurose, 2006).



Rys. 24. Systemy autonomiczne oraz połączenia między nimi.

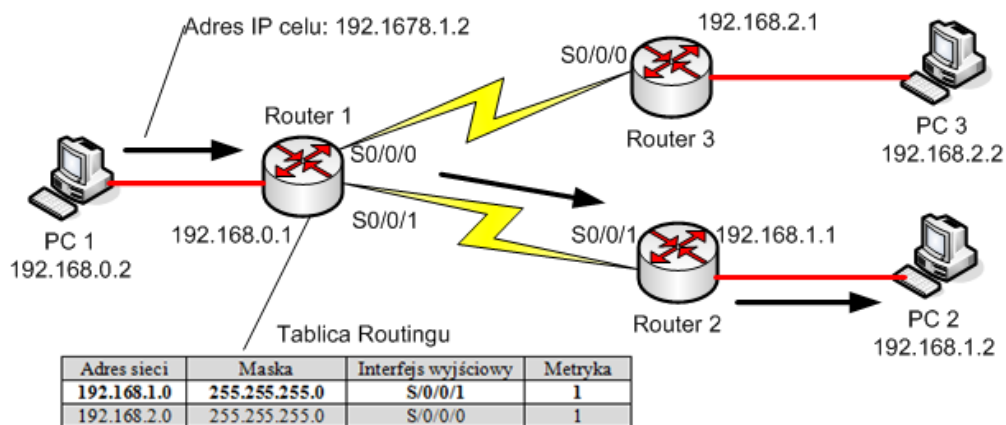
Systemy autonomiczne, podobnie jak komputery w sieci, muszą być rozróżnialne, z tego powodu do ich oznaczania stosuje się numery określone mianem ASN (ang. *Autonomous System Number*). Numery ASN to 16 bitowe pola pozwalające na wykorzystanie numerów z zakresu 0-65536, przy czym pierwszy i ostatni adres są zarezerwowane. Podobnie zarejestrowane są numery 64512-65534 do użytku prywatnego wewnątrz systemów autonomicznych przez dostawców. Pozostałe numery przydzielane są przez organizację IANA (ang. *Internet Assigned Numbers Authority*) w postaci bloków dla RIR (ang. *Regional Internet Registries*), z których swoje adresy uzyskują klienci (cisco.com; <http://fatcat.ftj.agh.edu.pl>).

Trasowanie w sieciach IP

Za trasowanie w sieciach komputerowych odpowiedzialne są urządzenia zwane routerami. Aby routery mogły spełniać prawidłowo swoje funkcje muszą posiadać informacje na temat sieci podłączonych bezpośrednio do niego jak i sieci zdalnych czyli takich, do których istnieje dostęp przez inny węzeł w sieci. Dane takie zawarte są w strukturze zwanej tablicą routingu, którą określić można mianem bazy danych zawierającej następujące informacje :

- adres sieci;
- maska sieci;
- informacje o interfejsie, przez który router ma dostęp do danej sieci lub kolejnego węzła; ewentualnie adres IP kolejnego skoku;
- metryka – koszt osiągnięcia sieci docelowej.

Proces trasowania polega na porównaniu adresu IP hosta docelowego znajdującego się w nagłówku IP a adresami w sieci znajdującymi się w tablicy routingu. Wpisy przeglądane są po kolei do momentu najlepszego dopasowania a następnie datagramy przesyłane są do celu lub kolejnego Routera (Rys. 25). W przypadku braku odpowiadającej trasy router wysyła je do innego punktu wykorzystując trasę domyślną (Kurose, 2006, CCNA Exploration: Routing Protocols and Concepts).



Rys. 25. Trasowanie w sieci.

Ważna funkcja pełniona przez tablicę trasowania wymaga od administratorów sieci jej prawidłowego utrzymania w celu jak najlepszego przesyłania danych. Uzupełnianie oraz aktualizowanie tras w tablicy może odbywać się na dwa sposoby różniące się mechanizmem:

- routing statyczny – administratorzy sieci ręcznie wpisują trasy do tablicy routingu; Umożliwia to administratorom na elastyczne zarządzanie trasami;
- routing dynamiczny – do uzupełniania tablicy wykorzystywane są odpowiednie protokoły pozwalające na wyznaczanie najlepszych tras oraz automatyczną reakcję na zmiany występujące w topologii sieci.

Obecnie najczęściej wykorzystywane jest w sieciach komputerowych trasowanie dynamiczne ze względu na szybsze konfigurowanie tablicy routingu oraz większą elastyczność topologii sieci. Trasy w tablicach zawsze są najlepszymi z możliwych. (Doyle, 2005; Kurose, 2006; Krysiak, 2005)

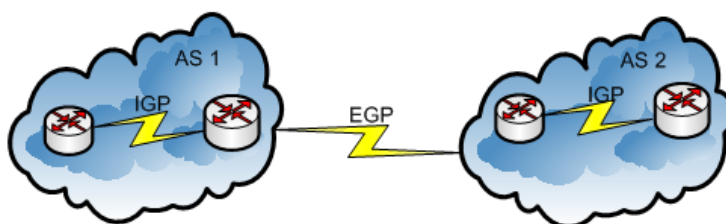
Protokoły trasowania dynamicznego można dzielić ze względu na wiele parametrów. Głównym z nich jest zasada działania tych algorytmów:

- Protokoły trasowania na podstawie wektora odległości – wyróżniamy m.in. RIP (ang. *Routing Information Protocol*), IGRP (ang. *Interior Gateway Protocol*), EIGRP (ang. *Enhanced Interior Gateway Protocol*), BGP (ang. *Border Gateway Protocol*);

- Protokoły trasowania na podstawie stanu łącza – są to OSPF (ang. *Open Shortest Path First*) oraz IS-IS (ang. *Intermediate System-Intermediate System*).

Innym kryterium dzielącym protokoły routingu są zależności między routerami (Rys. 26):

- Wewnętrzne protokoły trasowania - IGP (ang. *Interior Gateway Protocol*) – wykorzystywany przez routery wymieniające informacje w obrębie jednego systemu autonomicznego. Zaliczamy do nich m.in. RIP, IGRP, EIGRP, OSPF, IS-IS.
- Zewnętrzne protokoły trasowania – EGP (ang. *Exterior Gateway Protocol*) – wykorzystywany do wymiany informacji o trasach między różnymi systemami autonomicznymi. Do tego typu protokołów należy np. BGP (Krysiak, 2005; Doyle, 2005).



Rys. 26: Podział algorytmów trasowania ze względu na zależności między routerami.

Każdy z przedstawionych protokołów routingu ma swoje cechy charakterystyczne, które umożliwiają mu pracę w określonych warunkach (Tab. 5) (Krysiak, 2005; CCNP Building Scalable Internetworks v5.0):

Tab. 5. Porównanie protokołów routingu.

Cechy	RIP	RIPv2	IGRP	EIGRP	OSPF	IS-IS	BGP
Algorytm wektora odległości	+	+	+	+	-	-	+
Algorytm stanu łącza	-	-	-	-	+	+	-
Obsługa VLSM	-	+	-	+	+	+	+
Standard otwarty	+	+	-	-	+	+	+
Obsługa sumaryzacji tras	-	+	-	+	+	+	-
Obsługa AS	-	-	+	+	+	+	+
Obsługa uwierzytelniania	-	+	-	+	+	+	+

W mojej pracy przedstawię działanie trzech najczęściej wykorzystywanych protokołów trasowania. Będzie to OSPF umożliwiający dużą elastyczność konfiguracji oraz trasowanie nawet w dużych sieciach komputerowych w odróżnieniu do pozostałych wspomnianych

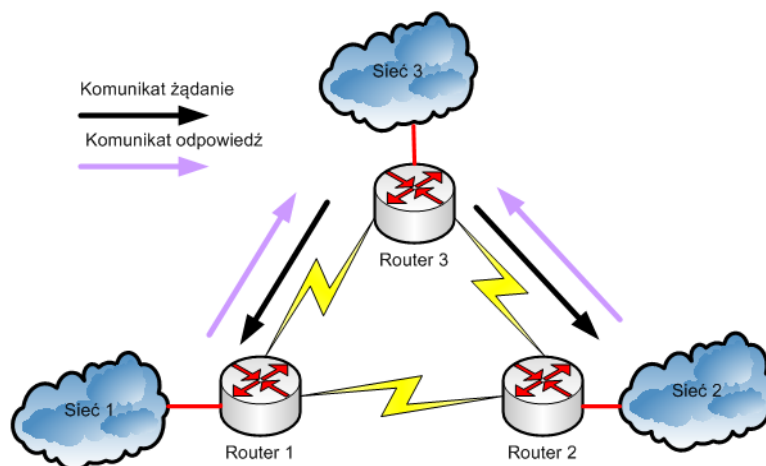
protokołów. Drugim omawianym protokołem jest RIPv2, ze względu na łatwość konfiguracji i ciągłe wykorzystanie w małych sieciach, oraz protokół BGP, ponieważ jako jedyny jest obecnie przedstawicielem protokołów bramy zewnętrznej.

3.1.1. Protokół RIPv2

RIPv2 nie jest nowym protokołem, a jedynie aktualizacją protokołu RIP wprowadzającą kilka poprawek do jego funkcjonowania. Został on opisany w dokumencie RFC 2453. Podobnie jak poprzednik zaliczany jest do grupy protokołów wektora odległości i jego działanie opiera się na algorytmie Bellmana-Forda. Mimo istnienia wielu potężnych konkurentów (OSPF, IS-IS czy EIGRP) protokół ten ze względu na swoją prostotę konfiguracji oraz małe obciążenie sieci podczas działania jest nadal wykorzystywany w wielu małych sieciach komputerowych. Metryką dla tego protokołu jest liczba skoków (czyli liczba węzłów od źródła do celu), jej maksymalna wartość wynosi 15, z tego powodu RIPv2 działać może tylko w stosunkowo małych sieciach. Sieć oznaczona metryką 16 jest nieosiągalna (RFC 2453).

Działanie protokołu RIPv2

RIPv2 podobnie jak jego poprzednik rozsyła aktualizacje stosując protokół UDP, różnica polega na tym iż datagramy wysyłane są z wykorzystaniem adresu grupowego 224.0.0.9 zamiast adresu rozgłaszania, co zmniejsza obciążenie urządzeń nie mających włączonego protokołu RIP.

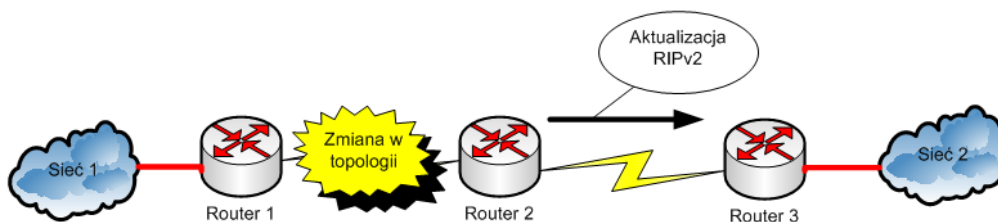


Rys. 27. Proces uzyskiwania informacji o trasach przez nowy router.

Routery korzystające z protokołu RIPv2 po włączeniu do sieci muszą zbudować własną tablicę trasowania. Rysunek 27 przedstawia sieć wykorzystującą RIPv2 do trasowania w sieci. Router 3 jest urządzeniem nowo podłączonym do infrastruktury i nie posiada wszystkich informacji na temat sieci zdalnych i tras. Rozsyła on zaraz po uruchomieniu

komunikat *Żądanie* na wszystkich interfejsach, na których operuje protokół RIP. Następnie przełącza się w stan oczekiwania na komunikaty *Odpowiedź* oraz *Żądanie* od innych routerów z sieci. Routery 1 oraz 2 po otrzymaniu komunikatu *Żądanie* wysyłają od razu swoją tablicę trasowania do Routera 3, on odbiera je i przetwarza umieszczając potrzebne dane we własnej tablicy.

Podczas normalnego działania sieci (brak awarii itp.) routery rozsyłają aktualizacje co 30 sekund. Wykorzystywane są do tego celu komunikaty *Odpowiedź* i w nich przesyłane są całe tablice routingu. W odróżnieniu do pierwszej wersji protokołu RIP, RIPv2 oprócz adresu IP sieci oraz metryki zawiera informacje na temat maski sieci, wykorzystywanie jej pozwala protokołowi RIPv2 na prawidłowe funkcjonowanie w sieciach nieciągłych stosujących model adresowania VLSM, czyniąc go protokołem bezklasowym. Oprócz aktualizacji okresowych routery rozsyłają aktualizacje wymuszone zmianami zaistniałymi w topologii sieci bądź w samej tablicy trasowania np. zmiana metryki trasy lub dodanie nowej sieci (Rys. 28).



Rys. 28. Aktualizacja wymuszone w sieci z trasowaniem RIPv2.

W przykładzie na Rysunku 28 uszkodzeniu ulega połączenie między Routerami 1 oraz 2, zmianie ulega tablica routingu ponieważ sieć 1 oznaczona zostaje jako nieosiągalna. Zmiany w tablicy wymuszają na Routerze 1 rozesłanie aktualizacji na wszystkie interfejsy z uruchomionym protokołem RIPv2. Aktualizacja dociera do Routera 3, który w swojej bazie oznacza Sieć 1 jako nieosiągalną.

Aktualizacje mają za zadanie utrzymywanie spójnej tablicy trasowania, oprócz nich do tego celu służą także specjalne liczniki odpowiedzialne za usuwanie tras z tablicy w przypadku braku jej aktualizacji:

- Licznik uznania trasy za nieistniejącą – ustawia metrykę trasy na 16 w przypadku braku jej aktualizacji w ciągu 180 sekund od poprzedniej;
- Licznik oczyszczania – usuwa trasę uznaną jako nieistniejącą po 240 sekundach od jej aktualizacji (czyli 60 sekund po oznaczeniu jej jako nieistniejąca);
- Licznik wstrzymania – ustawiony na 180 sekund, jego zadaniem jest zapobieganie pętlom trasowania podczas zmian w topologii (Doyle, 2005; CCNA Exploration: Routing Protocols and Concepts, RFC 2453).

Dużym zagrożeniem dla sieci składających się z kilku routerów są pętle routingu odpowiedzialne za obniżenie jakości funkcjonowania sieci czy wręcz za utratę danych. Powstawanie ich jest ściśle związane z błędami w ustawieniach tablicy trasowania lub redystrybucji tras. RIPv2 posiada kilka mechanizmów odpowiedzialnych za unikanie powstawania pętli trasowania:

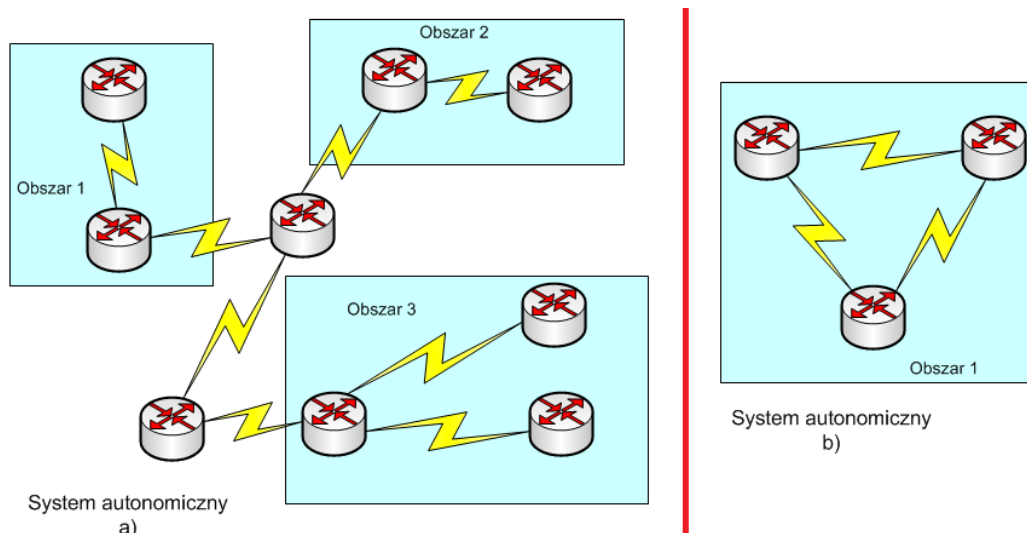
- Metryka – niepoprawne aktualizacje (poruszające się w pętli pomiędzy routerami) mogą doprowadzić do ciągłego zwiększania metryki. Dlatego ustalono maksymalną wartość skoków i w protokole RIP wynosi ona 15, metryka 16 oznacza nieskończoność;
- Licznik wstrzymania – zatrzymuje możliwość aktualizacji podczas niestabilności w sieci unikając powstawania pętli;
- Podzielony horyzont z zatruciem trasy – aktualizacje nie są wysyłane na interfejsy przez które zostały dostarczone; zatrucie tras powoduje oznaczanie tras nieosiągalnych od razu metryką 16, co przyspiesza zbieżność sieci (Doyle, 2005; CCNA Exploration: Routing Protocols and Concepts; RFC 2453).

3.1.2. Protokół OSPF (ang. Open Shortest Path First)

OSPF jest protokołem stanu łącza. Opracowany został ze względu na niedostateczną wydajność protokołu RIP w coraz większych sieciach komputerowych. Obecnie wykorzystywana jest druga wersja OSPF opisana w dokumencie RFC 2328. Na potrzeby sieci wykorzystujących protokół IPv6 utworzona została wersja 3 tego protokołu routingu. OSPF jest protokołem trasowania bramy wewnętrznej wykorzystywanym do obsługi trasowania wewnątrz systemów autonomicznych. Jak każdy protokół stanu łącza OSPF, wymaga znajomości całej topologii sieci w celu wyznaczenia najlepszej trasy do sieci docelowej. Do obliczania najlepszych ścieżek w sieci wykorzystywany jest algorytm SPF (ang. *Shortest Path First*).

Zaletą OSPF jest możliwość podziału systemu autonomicznego na obszary. Pozwala to administratorom dużych sieci na zwiększenie elastyczności oraz zastosowanie oddzielnych reguł trasowania w każdym obszarze, wyróżniamy dwa rodzaje protokołu OSPF (Rys. 29):

- OSPF jednoobszarowy – system autonomiczny nie jest podzielony na obszary; wszystkie routery komunikują się ze sobą;
- OSPF wieloobszarowy – system autonomiczny podzielony jest na obszary; każdy z obszarów jest od siebie niezależny i posiada własny algorytm routingu z użyciem stanu łącz (Kurose, 2006; Doyle, 2005).



Rys. 29. OSPF a) wieloobszarowy b) jednoobszarowy

Innymi niewątpliwie ważnymi cechami protokołu OSPF są:

- Otwarta specyfikacja umożliwia producentom na implementację protokołu w swoich urządzeniach bez opłacania licencji.
- Wykorzystuje różne mechanizmy uwierzytelniania, zwiększając bezpieczeństwo wymiany tras; każdy obszar może korzystać z innego mechanizmu.
- Pozwala administratorom na konfigurowanie łączy wirtualnych między routerami oddzielonymi siecią pośrednią. Takie połączenie jest przedstawiane na grafie jako bezpośrednie połączenie routerów.
- Umożliwia rozsyłanie we własnym obszarze informacji uzyskanych ze źródeł zewnętrznych.

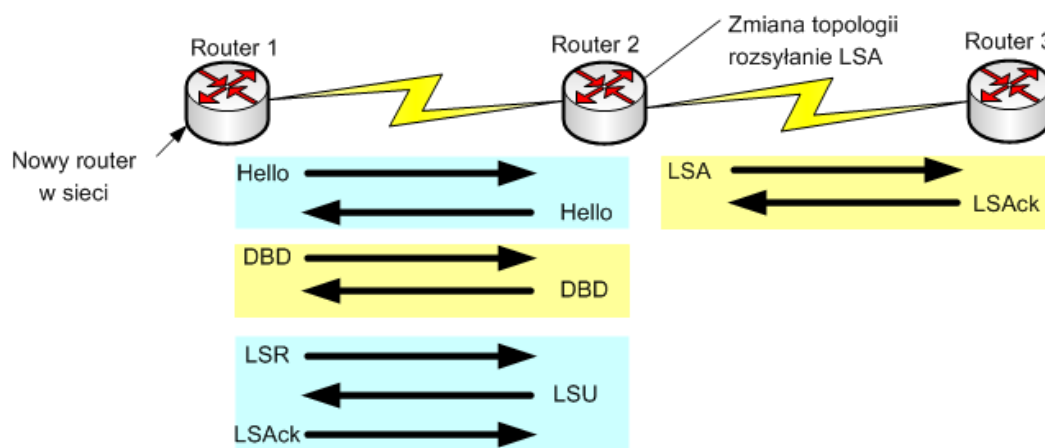
Protokół OSPF jest w pełni bezklasowym protokołem trasowania, oznacza to, że podczas wyznaczania tras nie uwzględnia związku między adresami IP a odpowiadającymi im domyślnymi maskami sieci (Kurose, 2006; CCNA Exploration: Routing Protocols and Concepts).

Komunikacja routerów wykorzystujących protokół OSPF

Złożoność działania protokołu OSPF wymusza odpowiedni rodzaj komunikacji między współdziałającymi routerami (Rys. 30). Komunikacja przebiega przy wykorzystaniu pakietów OSPF *LSP* (ang. *Link State Packet*). Wyróżnia się pięć rodzajów komunikatów (Tab. 6) (RFC 2328, Doyle 2005).

Tab. 6. Typy komunikatów LSP.

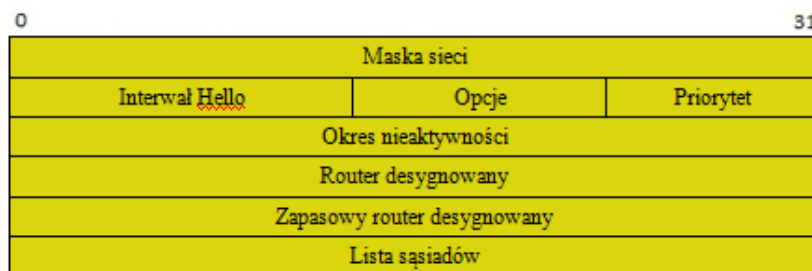
Typ pakietu	Wykonywane zadanie
<i>Hello</i>	Służy do wykrywania sąsiadujących routerów, oraz w elekcji DR i BDR
<i>Database Description (DBD)</i>	Wykorzystywane podczas początkowej synchronizacji bazy danych topologii.
<i>Link-state Request (LSR)</i>	Pakiet zgłaszający prośbę przesłania konkretnego stanu łącza z bazy danych
<i>Link-state Update (LSU)</i>	Pakiet ten wykorzystywany jest przy odpowiedzi na pakiet <i>LSR</i> oraz do rozsyłania nowych informacji o stanie łącz. Może przenosić kilka pakietów <i>LSA</i> (ang. <i>Link-state Advertisements</i>)
<i>Link-State Acknowledgement (LSAck)</i>	Komunikat potwierdzający otrzymanie pakietów <i>LSA</i> . Jeden komunikat <i>LSAck</i> może potwierdzić kilka <i>LSA</i> .



Rys. 30. Komunikacja routerów OSPF.

Pakiet „Hello”

Najważniejszym komunikatem rozsyłanym przez routery korzystające z protokołu OSPF jest komunikat *Hello*, służy do wykrywania sąsiadujących routerów oraz ustanawiania sąsiedztwa z nimi. W sieciach wielodostępowych komunikatów tego typu wykorzystywane są także do wyboru routera desygnowanego oraz zapasowego routera desygnowanego. Pakiet *Hello* składa się z nagłówka OSPF zawierającego m.in. pola Wersja, Typ=1, Długość pakietu, ID routera, Numer obszaru, Suma kontrolna oraz nagłówka pakietu *Hello* przedstawionego na Rysunku 31.



Rys. 31. Nagłówek pakietu Hello.

- **Maska sieci** – zawiera maskę sieci interfejsu, z którego pochodzi pakiet. Niezgodność masek uniemożliwi nawiązanie sąsiedztwa;
- **Interwał Hello** – określa okres czasu po jakim router wysyła ponownie komunikat *Hello*. Wartość ta musi być wspólna dla routerów próbujących nawiązać komunikację dwukierunkową;
- **Priorytet** – priorytet routera wykorzystywany podczas wyborów DR oraz BDR. Wartość zero oznacza wyłączenie urządzenia z elekcji;
- **Okres nieaktywności** – czas, po którym router oznaczany jest jako nieosiągalny. Routery nawiązujące komunikację dwukierunkową muszą używać tej samej wartości;
- **Router desygnowany** – pole wskazujące adres IP routera desygnowanego w sieci, wartość 0.0.0.0 oznacza jego brak;
- **Zastępczy router desygnowany** – określa adres IP zapasowego routera desygnowanego, wartość 0.0.0.0 oznacza brak zapasowego routera desygnowanego;
- **Lista sąsiadów** – lista ID sąsiednich routerów.

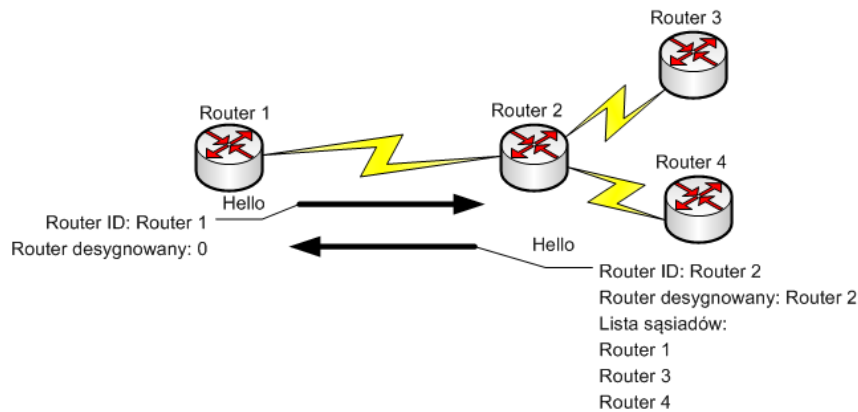
W celu zapewnienia spójności bazy danych stanu łączy routery okresowo rozsyłają pakiety Hello. W przypadku braku odpowiedzi na któryś z nich, nie odpowiadający sąsiad zostaje usunięty z bazy danych i router rozsyła *LSU* w celu poinformowania wszystkich węzłów sieci o zmianie w topologii (RFC 2328, CCNA Exploration: Routing Protocols and Concepts).

Funkcjonowanie protokołu OSPF

Działanie protokołu OSPF, podobnie jak każdego protokołu stanu łączy, można przedstawić w kilku etapach.

- **Ustanawianie sąsiedztwa** – każdy router po uruchomieniu musi poznać swoich sąsiadów i umieścić informacje o nich w tablicy sąsiadów, w przeciwnym razie wysyłanie pakietów *LSU* będzie niemożliwe. Do tego celu wykorzystywane są pakiety *Hello*, wysyłane przez wszystkie interfejsy OSPF, każdy z nich zawiera ID sąsiadów

znanych przez router wysyłający oraz parametry konieczne do ustanowienia sąsiedztwa. Router otrzymujący pakiet *Hello* przegląda go, jeżeli znajdzie tam ustanowioną komunikację dwukierunkową (Rys 32). W przypadku sieci rozgłoszeniowych oraz nie rozgłoszeniowymi sieciami wielodostępowymi ten rodzaj komunikacji nie występuje między wszystkimi routerami, jedynie między routerem desygnowanym a pozostałymi routerami.



Rys. 32. Ustanawianie komunikacji dwustronnej.

- Wybór routera desygnowanego oraz zastępczego routera desygnowanego – w sieciach wielodostępowych rozplywowe rozsyłanie aktualizacji stosowane w sieciach punkt-punkt staje się nieefektywne, mogłoby ono prowadzić do dużego obciążenia łącz. Z tego względu w sieciach wielodostępowych stosuje się podział ról na DR (ang. *designated router*), BDR (ang. *backup designated router*) oraz pozostałe routery. Wszystkie routery w sieci wymieniają się aktualizacjami jedynie z routerem desygnowanym. Proces elekcji rozpoczyna się po ustanowieniu komunikacji dwukierunkowej. Do wyboru routera desygnowanego wykorzystuje się priorytet interfejsu, z którego wysłany został komunikat *Hello*. Router posiadający interfejs o najwyższym priorytecie zostaje routerem desygnowanym, natomiast drugi w kolejności zastępczym routerem desygnowanym. W przypadku równorzędności interfejsów przy wyborze brane jest pod uwagę ID routera, elekcje wygrywa router o najwyższej wartości ID. Zastępczy router desygnowany, podobnie jak DR, utrzymuje wszystkie aktualne informacje na temat topologii sieci i w przypadku awarii DR pełni jego funkcje w sieci.
- Synchronizacja baz danych – Po ukończeniu dwóch poprzednich etapów następuje synchronizacja baz danych topologii. Proces ten jest konieczny, ponieważ protokoły stanu łącza do wyznaczania tras wymagają znajomości pełnej topologii sieci.

Synchronizacja następuje przez wymianę komunikatów DBD między routerami, które nawiązały komunikację dwukierunkową. Pakiet ten zbudowany jest z nagłówka OSPF oraz komunikatów LSA. Proces synchronizacji przebiega między dwoma routerami w relacji master/slave. Router o większym ID zostaje master'em i przejmuje kontrolę nad całym procesem. Następnie rozpoczyna się wymiana komunikatów DBD między routerami, każdy z nich musi zostać potwierdzony, w innym wypadku router wysyłający będzie go retransmitował co pewien okres czasu. Po wymianie następuje porównywanie odebranych danych z zawartością własnej bazy danych, w ten sposób routery określają czy tablica topologii jest kompletna. W przypadku braków w tablicy router tworzy pakiet LSR z żądaniem konkretnych wpisów a następnie przesyła go do swojego sąsiada. Router odbierający żądanie ma za zadanie odesłać komunikat LSU zawierający żądane informacje. Po zakończeniu tego procesu obydwa routery stają się do siebie przyległe a ich bazy danych topologii są identyczne.

Po ukończeniu synchronizacji posiadają pełną topologię sieci. Po wyznaczeniu najlepszych tras za pomocą algorytmu SPF oraz umieszczeniu ich w tablicy trasowania mogą już w pełni spełniać swoje funkcje w sieci (RFC 2328, Doyle, 2005).

Wykorzystanie pakietów LSU i rozsyłanie aktualizacji

Najważniejszym elementem komunikacji między routerami OSPF jest rozsyłanie informacji o stanie łącz, służą do tego pakiety LSU. Wykorzystywane są zarówno podczas synchronizacji tablicy stanu łącz w trakcie pierwszego uruchomienia routera, oraz do okresowych aktualizacji informacji o stanach łącz. Standardowo aktualizacje rozsyłane są co 30 minut a konieczność ich wysyłania wynika z ograniczonej czasowo ważności LSA znajdujących się w bazie danych stanów łącz. W przypadku gdy router nie otrzyma aktualizacji przeterminowane informacje zostają usunięte z bazy. Routery wykorzystują pakiety LSA również w przypadku otrzymania żądania o konkretny stan łącza, wtedy pakiet LSU zawiera LSA z żądanymi informacjami.

Routery OSPF informują się nawzajem o każdej zmianie w topologii sieci w celu utrzymania spójnej topologii sieci, wykorzystując pakiety LSU zawierające informacje o zmienionych stanach łącz. Informacje są rozsyłane za pomocą mechanizmu zwanego „*Reliable flooding*” lub inaczej rozsyłania rozplywowego. Niezawodność tego procesu zapewnia mechanizm potwierdzania przez router otrzymanych komunikatów LSU, każdy z nich musi zostać potwierdzony. Router otrzymując aktualizację, wykorzystując mechanizmy zawarte w protokole OSPF sprawdza poprawność aktualizacji i w zależności od wyniku uaktualnia

tablice lub odrzuca aktualizacje. Następnie pakiety *LSU* przesyłane są do kolejnych węzłów w sieci. Wyróżniamy siedem typów pakietów *LSA*, są one przedstawione w Tabeli 7 (CCNP Building Scalable Internetworks v5.0; Doyle, 2005; www.enterprisenetworkingplanet.com) .

Tab. 7. Rodzaje komunikatów *LSA*.

Rodzaj <i>LSA</i>	Opis
1. Router <i>LSA</i>	Zawiera informacje o stanie łącz oraz ich koszcie dla danego routera. Rozsyłany jest wewnątrz danego obszaru
2. Network <i>LSA</i>	Rozsyłany przez router będącym DR do wszystkich routerów znajdujących się w obszarze i zawiera informacje o wszystkich routerach, z którymi nawiązał relacje przyległości.
3. Network Sumary <i>LSA</i>	Generowany przez ABR (ang. <i>Area Border Router</i>), zawiera informacje o podsieciach w obszarze. Wysyłany jest do obszaru backbone, (Pojęcia ABR oraz backbone omówione zostaną w dalszej części pracy).
4. AS External ASBR Summary <i>LSA</i>	Pakiet wysyłany z ABR do ASBR (ang. <i>Autonomous System Boundary Router</i>), zawierający informacje o koszcie połączeń między nimi.
5. External <i>LSA</i>	Generowany przez ASBR. Zawiera informacje o podsieciach na zewnątrz AS lub o domyślnej trasie prowadzącej poza AS.
6.	Podsumowanie grup stosowane w MOSPF.
7. NSSA External <i>LSA</i>	Generowane przez routery ASBR znajdujące się w obszarze NSSA (ang. <i>Not so stuby area</i>). Rozsyłane są tylko wewnątrz obszaru NSSA.

Metryki OSPF

Metryka trasowania jest wartością wykorzystywaną przez algorytmy trasowania do wyboru najlepszej trasy z możliwych (najkrótszej, najszybszej itd.). Najczęściej brany pod uwagę parametrami do jej obliczania są: szybkość łącza, opóźnienie, przeciążenie w sieci oraz rodzaj wykorzystywanego łącza. W przypadku OSPF metrykę określa się mianem kosztu, określa on koszt dostarczenia pakietu do sieci docelowej. Na wartość całkowitą metryki dla trasy składa się suma kosztów wzdłuż całej ścieżki, która przemierza datagram. Specyfikacja OSPF nie precyzuje wartości kosztów i najczęściej są one ustawiane przez administratora w zależności od warunków jakie panują w sieci. Dla routerów CISCO koszt domyślny obliczany jest na podstawie przepustowości danego interfejsu według wzoru: (CCNA Exploration: Routing Protocols and Concepts)

$$KOSZT = \frac{1000000}{PASMO} \quad (1)$$

gdzie:

KOSZT – Koszt połączenia,
PASMO – Szerokość pasma w bitach na sekundę.

Kształtowanie ruchu pakietów za pomocą OSPF

OSPF pozwala na określanie, w jaki sposób datagramy będą przesyłane od źródła do celu. Służą do tego mechanizmy takie jak: równoważenie obciążenia, obsługa pola TOS, czy przesyłanie w zależności od adresu celu.

Trasowanie wielościżkowe zwane inaczej równoważeniem obciążenia umożliwia routerom wykorzystanie wielu tras jednocześnie, aby dostarczyć datagramy do celu. OSPF charakteryzuje się automatyczną obsługą tego mechanizmu. Pozwala on na wykorzystanie wielu tras o takim samym koszcie do jednoczesnego przesyłania danych, dzięki temu rozwiązaniu łącza są obciążane równomiernie i dane przesyłane są szybciej.

Innym sposobem kształtowania ruchu w sieciach przy użyciu protokołu OSPF jest wykorzystanie pola TOS w nagłówku IP. Ten mechanizm pozwala administratorowi na ustalenie trasy dla datagramów w zależności od rodzaju przesyłanych danych np. strumień dźwiękowy powinien być przesyłany trasą o najmniejszym możliwym opóźnieniu

OSPF umożliwia także wybór trasy w zależności od adresu sieci docelowej czy nawet samego adresu celu (Comer, 1998; itepedia.pl; RFC 2328; CCNA Exploration: Routing Protocols and Concepts).

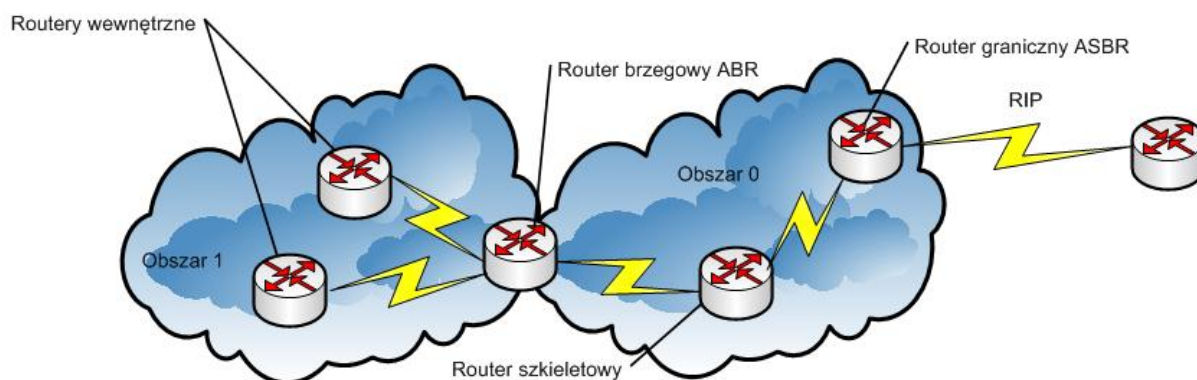
OSPF wieloobszarowy

OSPF charakteryzuje się możliwością podziału sieci na mniejsze fragmenty zwane obszarami. Zostało to wymuszone przez dynamiczny rozwój sieci, który doprowadził do pewnych trudności:

- Prawidłowe funkcjonowanie dużej sieci wymaga odpowiednio dużej ilości urządzeń. Stwarza to zwiększone ryzyko wystąpienia awarii, które wymuszają aktualizację tablic trasowania na pozostałych urządzeniach. Proces ten wymaga uruchomienia algorytmu SPF, co przy dużej tablicy topologii zwiększa obciążenie routera.
- Zwiększanie liczby routerów, zwiększa liczbę tras powiększając tablice trasowania. Duży rozmiar tablicy wydłuża jej przeszukiwanie oraz wymaga większych zasobów sprzętowych do jej utrzymania.

- Routery OSPF do funkcjonowania wymagają znajomości całej topologii, umieszczana jest ona w tablicy topologii. Rozmiar sieci wpływa na rozmiar tablicy, której zwiększanie wymaga coraz większej liczby zasobów udostępnianych przez router (głównie pamięć RAM - ang. *Random Access Memory*). (CCNP Building Scalable Internetworks v5.0; Kurose 2006; <http://dervish.wsisiz.edu.pl>)

Podział Systemów Autonomicznych wymusiła również podział urządzeń sterujących ruchem ze względu na spełniane funkcje (Rys 33). W sieciach hierarchicznych wyróżniamy 4 typy routerów odpowiadających za poprawne rozsyłanie tras w sieci z podziałem na obszary (Tab. 8):



Rys. 33. Rodzaje routerów OSPF.

Tab. 8. Typy routerów OSPF.

Typ routera	Funkcje
Wewnętrzny	Wszystkie jego interfejsy znajdują się w jednym obszarze i posiadają tablice topologii tylko własnego obszaru; odpowiedzialny jest za trasowanie w obrębie tego obszaru.
Szkieletowy	Wchodzi w skład grupy routerów szkieletowych sieci, połączone są do nich obszary.
Brzegowy - ABR (ang. <i>Area Border Router</i>)	Odpowiedzialne za komunikacje między obszarami. Posiadają tablice topologii dla każdego obszaru i rozsyłają trasy w postaci sumarycznej.
Graniczny - ASBR (ang. <i>Autonomous System Boundary Router</i>)	odpowiada za połączenia obszarów z innymi sieciami. Obsługuje zarówno protokoły IGP jak i EGP. Wymienia także informacje między OSPF a innymi protokołami trasowania. Najczęściej umieszczany jest w obszarze 0, co umożliwia do niego dostęp wszystkim obszarom znajdującym się w systemie autonomicznym.

Specyfikacja OSPF wyróżnia także kilka typów obszarów (Tab. 9):

Tab. 9. Typy obszarów w wielobszarowym OSPF.

Typ obszaru	Opis
Szkielet	Nazywany obszarem 0, zapewnia komunikację między pozostałymi obszarami.
Standardowy	Obszary podłączone bezpośrednio do szkieletu; każdy router posiada pełną tablicę topologii swojego obszaru, przyjmuje wszystkie typy aktualizacji.
Totally Stubby Area	Obszar, nie akceptuje tras zewnętrznych oraz tras sumarycznych z innych obszarów. Datagramy wysyłane są wykorzystując trasę domyślną. Nie może zawierać ASBR'a.
Stub Area	Obszar, w którym nie są akceptowane informacje przesyłane z innych protokołów routingu. Przesyłanie do sieci wykorzystujących inne protokoły odbywa się przy pomocy tras domyślnych. Dopuszczane są jednak trasy sumaryzacyjne z innych obszarów. Nie może zawierać ASBR'a.
No so stubby area	Obszar dający podobne możliwości jak Totally Stubby Area i Stub Area. Pozwala jednak na ogłaszanie tras zewnętrznych w systemie autonomicznym.

(CCNP Building Scalable Internetworks v5.0; Kurose, 2006; <http://dervish.wsisiz.edu.pl>).

3.1.3. Protokół BGP

Internet to zbiór systemów autonomicznych połączonych ze sobą. Aby mogły wymieniać dane między sobą, ich routery brzegowe muszą zawierać trasy do każdego z systemów. Protokoły IGP sprawdzają się wewnątrz systemów autonomicznych, jednak rozmiar sieci globalne powodowałby ich niepoprawne funkcjonowanie. Do obsługi routingu w sieci Internet utworzona została grupa protokołów EGP, obecnie jedynym wykorzystywanym jej przedstawicielem jest protokół BGP.

BGP jest protokołem wektora odległości opracowanym w 1989 roku. Aktualnie stosowana wersja 4, wniosła wiele usprawnień w porównaniu do poprzedników. Wspiera ona między innymi CIDR (ang. *Classless Inter-Domain Routing*), inkrementacyjne aktualizacje, lepsze filtrowanie oraz elastyczne polityki routingu w porównaniu do wersji poprzedniej. Działanie protokołu BGP opiera się na zestawianiu połączeń między routerami go obsługującymi. Do komunikacji wykorzystywany jest port 179 protokołu TCP, który zapewnia niezawodność przesyłania informacji między współpracującymi ze sobą urządzeniami. W celu poprawnego działania wymagane jest, aby każda para routerów miała

ustanowioną relację sąsiedztwa (sesję) między sobą w celu wymiany informacji o trasach. Zestawienie oraz utrzymanie sesji wiąże się z ustanowieniem połączenia TCP oraz wymianą odpowiednich komunikatów między sąsiadującymi routerami. Wyróżniamy kilka komunikatów pozwalających na utworzenie oraz zarządzanie sesją między urządzeniami (Tab. 10) (Kurose, 2006, cisco.com).

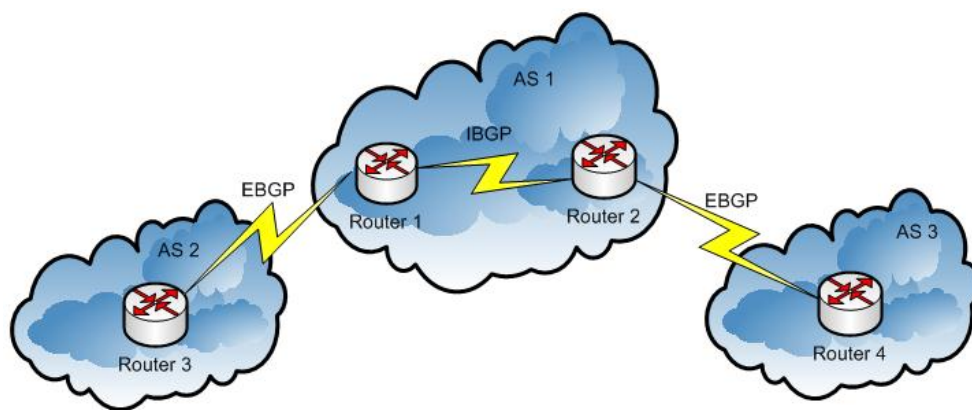
Tab. 10. Komunikaty wykorzystywane w tworzeniu sesji BGP.

Typ komunikatu	Opis
<i>Open</i>	Rozpoczyna sesję BGP; Zawiera wersję protokołu (obecnie wersja 4), numer systemu autonomicznego, parametr określający czas po jakim sesja BGP ma zostać zakończona; jeżeli nie nadejdzie wiadomość <i>KEEPALIVE</i> lub <i>UPDATE</i> , identyfikator routera, oraz dodatkowe parametry używane do zestawienia sesji BGP
<i>Update</i>	Przenosi informacje o trasach. Zawiera 3 rodzaje informacji: o trasach nieaktualnych, atrybutach ścieżki oraz o dostępnych sieciach
<i>Keepalive</i>	Wiadomość podtrzymująca połączenie BGP; jej zadaniem jest zerowanie licznika HOLD TIME w przypadku braku wiadomości <i>UPDATE</i> .
<i>Notification</i>	Wykorzystywana w przypadku jakichkolwiek błędów występujących podczas ustanawiania lub istnienia sesji. Wiadomość ta powoduje przerwanie tworzenia sesji lub zamknięcie istniejącego połączenia.

Routery obsługujące protokół BGP mogą ustanawiać dwa rodzaje sesji (Rys. 34) w zależności od usytuowania w sieci:

- Sesja zewnętrzna eBGP (ang. *External BGP*) – zestawiana między routerami BGP pracującymi w różnych systemach autonomicznych;
- Sesja wewnętrzna iBGP (ang. *Internal BGP*) - zestawiana między routerami BGP w obrębie jednego systemu autonomicznego posiadającego więcej niż jeden router z uruchomionym protokołem BGP. Sesja tego typu wymagana jest w przypadku sieci tranzytowych, gdzie każdy router brzegowy musi znać wszystkie trasy zewnętrzne.

EBGP wymaga bezpośredniego połączenia między routerami ustanawiającymi sesję, można to zmienić wykorzystując technologię ebgp-multi-hop. Pozwala ona na połączenia eBGP za pośrednictwem routera trzeciego. W przypadku iBGP musi istnieć połączenie pośrednie np. przez inny router w systemie autonomicznym. Rodzaj sesji między routerami brzegowymi ustalany jest już podczas jej nawiązywania automatycznie. (Halbi, 2000; www.cisco.com)



Rys. 34. Działanie eBGP oraz iBGP.

Rysunek 33 przedstawia 3 systemy autonomiczne, w których pary routerów: Router 1 – Router 3 oraz Router 2 – Router 4 posiadają między sobą sesję eBGP wykorzystywaną do wymiany informacji o trasach. AS 1 jest tranzytowym systemem autonomicznym posiadającym 2 routery brzegowe (Router 1 i Router 2) odpowiedzialne za komunikację między wszystkimi AS’ami. Routery te posiadają sesje iBGP w celu wymiany informacji o trasach zewnętrznych.

Przenoszenie aktualizacji w protokole BGP

Po zestawieniu sesji routery BGP wymieniają się między sobą częściami tablicami routingu, na których rozesłanie pozwala polityka organizacji zarządzających systemami autonomicznymi. Kolejne zmiany w tablicach trasowania przesyłane są za pomocą aktualizacji inkrementacyjnych, zmniejsza to obciążenie CPU (ang. *Central Processing Unit*) routera oraz pasma wykorzystwanego do wymiany informacji. Aktualizacje BGP przenoszone są za pomocą komunikatów *UPDATE* składających się z trzech części:

- Network Layer Reachability Information (NLRI) – parametr określający sieć docelową, o której router BGP chce poinformować inne routery. Składa się on z dwóch części: maski sieci w postaci liczby bitów oraz prefiksu IP rozgłaszanej sieci. Dzięki temu router informuje o sieciach jakie są dostępne przez niego a wyznaczanie trasy do celu zostawia routerom w obrębie systemu autonomicznego.
- Lista atrybutów – parametr pozwalający protokołowi BGP na eliminację pętli routingu oraz wykorzystywanie lokalnych i globalnych polityk trasowania. Najczęściej wykorzystywane atrybuty zostaną przedstawione w dalszej części pracy.
- Trasy nieaktualne – w tej części komunikatu aktualizacji przenoszone są informacje o trasach już nieaktualnych, do których nie ma dostępu.

- Komunikat zawiera dwa pola określające odpowiednio rozmiar listy atrybutów oraz listy tras nieaktualnych.

Tablice routingu BGP wykorzystują numerację wersji, aby zapewnić wykorzystywanie jak najbardziej aktualnych tablic przez routery. W przypadku dotarcia aktualizacji do routera i wprowadzenia jej do tablicy trasowania zostaje zwiększony jej numer wersji (Halbi, 2000; Doyle 2001).

Metryki BGP

BGP w odróżnieniu od innych protokołów routingu nie wykorzystuje jako metryk żadnych miar technicznych lecz stosuje parametry zwane atrybutami. Dzięki nim routery są w stanie unikać pętli routingu a także pozwalają administratorom na stosowanie polityk trasowania w zależności od potrzeby. Potocznie prefiksy IP wraz z ich atrybutami uznawane są jako trasy. BGP wykorzystuje szereg wielu atrybutów przy czym przedstawię tu trzy najważniejsze, które muszą znaleźć się w każdej aktualizacji:

- **AS_PATH** – atrybut zawierający numery ASN wszystkich systemów autonomicznych, którym został przesłany prefiks. Jeśli router otrzyma trasę i w atrybucie **AS_PATH** znajdzie swój identyfikator trasa zostanie odrzucona, pozwalając na uniknięcie pętli routingu. Dodatkowo parametr **AS_PATH** wykorzystywany jest podczas wyboru najbardziej optymalnej trasy.
- **NEXT_HOP** – gdy jedna z sieci może być dostępna z routera brzegowego za pomocą kilku tras, atrybut ten określa router, który ma być użyty do dalszego przesłania informacji.
- **ORIGIN** – informuje, skąd protokół BGP zna daną trasę. Może przyjąć trzy różne wartości: **IGP** – trasa została uzyskana przez protokoły bramy wewnętrznej, **EGP** – gdy trasa została uzyskana przez protokół bramy wewnętrznej, **Incomplete** – pochodzenie trasy jest nieznane. Parametr wykorzystywany przy wyborze najlepszej trasy.

Protokół BGP posiada także wiele atrybutów wpływających na stopień uprzywilejowania tras (docwiki.cisco.com; Doyle, 2001; Kurose, 2006).

Wybór trasy oraz uzupełnianie tablicy routingu

Routery BGP rozsyłają między sobą informacje o posiadanych trasach, często każdy router posiada kilka ścieżek do tego samego miejsca w sieci i musi wybrać tę najlepszą.

Z tego powodu każdy router BGP przechowuje tablicę informacji o routingu składającą się z:

- Adj-RIBs-In – tablica zawiera wszystkie informacje o trasach uzyskanych w wymianie pakietów aktualizacyjnych;
- Loc-RIB – tablica zawierająca wyłącznie wybrane przez router trasy; po spełnieniu kryteriów wymaganych przez administratora systemu autonomicznego trafiają one do tablicy trasowania;
- Adj-RIBs-Out – zawiera wszystkie trasy, które zostaną zawarte w kolejnych aktualizacjach BGP (Doyle, 2001).

BGP określa sposób wyboru najbardziej korzystnej trasy spośród dostępnych i umieszcza ją w tablicy trasowania. W tym celu do wyboru trasy wykorzystywane są atrybuty przypisane trasom w odpowiedniej kolejności:

- Najpierw pod uwagę brany jest atrybut określający wartość lokalnego uprzywilejowania trasy.
- Następnie w przypadku, gdy poprzedni parametr jest taki sam dla kilku tras, protokół wybiera trasę o najkrótszym atrybucie AS_PATH.
- W kolejnym etapie uwzględniania jest wartość NEXT_HOP, zostaje wybrana trasa, dla której koszt trasy do punktu kolejnego skoku jest najmniejszy.
- Jeżeli trasa nie zostanie wybrana protokół weźmie pod uwagę identyfikatory protokołu BGP.

Należy także pamiętać, iż nie każda trasa może zostać dodana do tablicy routingu. Z taką sytuacją spotykamy się na przykład gdy administrator nie chce przysyłać określonych danych przez dany system autonomiczny. W takim przypadku trasa, która w atrybucie posiada identyfikator takiego systemu autonomicznego zostaje odrzucona. Pozwala to jednostkom administracyjnym na regulowanie przepływu informacji między systemami autonomicznymi (np. Pewne dane nie mogą zostać wysłane poza obszar danego kraju) (Kurose, 2006; Doyle, 2001).

Kształtowanie ruchu w sieciach wykorzystujących BGP

Protokół BGP pozwala administratorom na manipulowanie ruchem datagramów w sieci. Umożliwia on manipulowanie atrybutami tras zwiększając lub zmniejszając prawdopodobieństwo umieszczenia ich w tablicy trasowania. Proces ten odbywa się w trzech etapach:

- Filtrowanie (identyfikacja) tras;
- Blokowanie lub dopuszczanie tras;
- Manipulacja atrybutami tras.

Inną metodą kierowania ruchem datagramów jest podział obciążenia między istniejące połączenia stosując listy dostępu (Halbi, 2000).

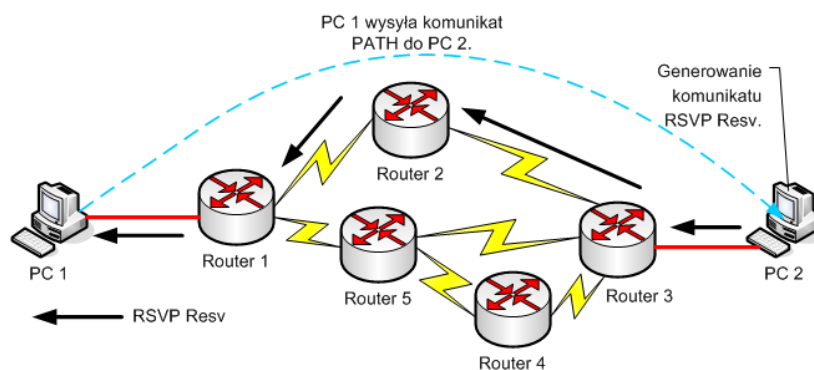
3.2. Jakość usług w sieciach IP

Szybko rozwijające się sieci IP często wymagają rozwiązań pozwalających na bezstratne oraz szybkie przesyłanie pakietów wzdłuż jej węzłów. Wymagania co do tych mechanizmów zależne są od typu przesyłanych danych i różnią się w zależności czy przesyłane są pliki czy rozmowa telefoniczna. Podczas transferu plików nie wymaga się od sieci małych opóźnień oraz strat, ponieważ dane i tak zostaną przesłane do celu a szybkość transmisji wpłynie jedynie na czas po jakim pobieranie się ukończy. Natomiast w przypadku transmisji rozmowy telefonicznej czy chociażby streamingu wideo wpływ wspomnianych wcześniej parametrów jest ogromny. Duże opóźnienia czy utraty pakietów mogą doprowadzić do zakłóceń głosu czy obrazu, podobnie dzieje się w przypadku małych szybkości transmisji. W takich wypadkach z pomocą administratorom przychodzą mechanizmy zebrane pod nazwą QoS. Są one wykorzystywane wszędzie tam, gdzie należy zapewnić odpowiedni przepływ danych wzdłuż sieci (Kurose, 2006; Flannagan, 2001).

3.2.1. Podstawowe informacje o QoS

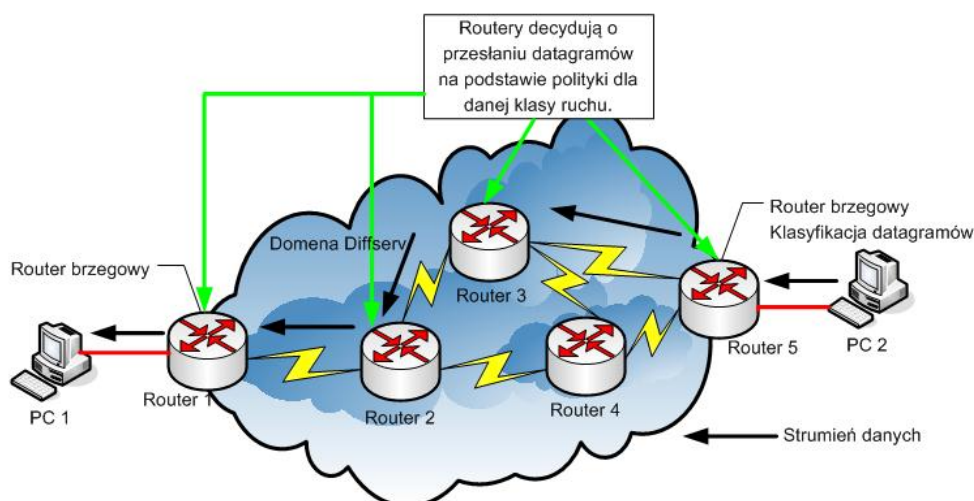
QoS to szereg mechanizmów umożliwiających administratorom wprowadzenie do sieci odpowiedniego poziomu jakości obsługi datagramów. Obecnie wyróżnia się dwa modele QoS:

- Model usług zintegrowanych Intserv (ang. *Integrated Services*) (Rys. 35) – charakteryzuje się rezerwacją zasobów dla przepływającego strumienia, odpowiadają za to mechanizmy sygnalizujące, które informują routery na trasie datagramu o wymaganiach stawianych przez aplikacje nadająca dane. Rezerwacja następuje tylko w przypadku, gdy router posiada odpowiednią ilość wymaganych zasobów. Po dokonaniu rezerwacji przez wszystkie węzły na trasie strumienia danych następuje zestawienie połączenia i przesłanie datagramów. Do sygnalizacji w sieci wykorzystywany jest protokół RSVP w celu sygnalizacji rezerwacji zasobów.



Rys. 35. Działanie modelu Intserv.

- Model usług zróżnicowanych Diffserv (ang. *Differentiated Services*) (Rys. 36) – charakteryzuje się dzieleniem przepływających datagramów na klasy i zapewnianie odpowiedniej obsługi w zależności od niej. Wszystkie routery w domenie Diffserv działają autonomicznie, opierając się na klasie przydzielonej strumieniowi danych i politykach ich obsługi tzw. PHB (ang. *Per Hop Behaviour*). Zaletą tego modelu jest duża skalowalność oraz elastyczność w porównaniu do modelu Intserv.



Rys. 36. Działanie modelu Diffserv.

Dodatkowo poza dwoma przedstawionymi modelami QoS wykorzystywany jest także mechanizm BE (ang. *Best effort*), którego zadaniem jest obsługa strumieni danych gdy nie są przewidziane inne sposoby traktowania. Traktowane w ten sposób są datagramy w wypadku braku mechanizmów zapewniania jakości usług. BE oznacza, że protokół próbuje dostarczyć datagramy tak, aby one dotarły do celu ale nie gwarantuje ich jakość obsługi.

Wszystkie przedstawione mechanizmy administratorzy mogą implementować wspólnie w sieci, wykorzystując zalety każdego z modeli. W swojej pracy bliżej przedstawię funkcjonowanie modelu usług zróżnicowanych ze względu na szersze zastosowanie

w dzisiejszych sieciach komputerowych spowodowane jego zaletami w porównaniu do modelu usług zintegrowanych (Kurose, 2006; Flannagan, 2001).

Działanie modelu usług zróżnicowanych

Celem wprowadzenia modelu Diffserv w sieciach komputerowych jest zapewnienie odpowiedniej obsługi strumieni danych umożliwiając łatwe jej skalowanie. Niezawodne dostarczanie jakości usług w sieciach umożliwia mu rozbudowana architektura składająca się z wielu komponentów wykonujących wyspecjalizowane funkcje. W skład modelu Diffserv wchodzi m.in. mechanizmy:

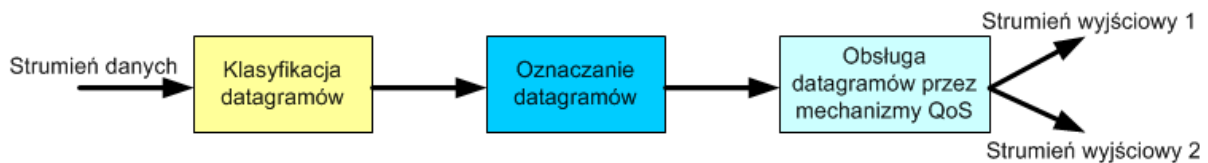
- Klasyfikacji pakietów;
- Oznaczania pakietów;
- Zarządzania zatorami;
- Unikania zatorów.

Obszar sieci, w której zaimplementowany jest model Diffserv określany jest mianem domeny Diffserv, składającej się z routerów brzegowych (odpowiedzialnych za klasyfikowanie strumieni danych) oraz routerów szkieletowych przesyłających pakiety zgodnie z własnymi politykami. Routery szkieletowe przesyłają strumień danych zgodnie z zasadami określonymi przez PHB, czyli model określający sposób traktowania danej klasy ruchu rozpoznawanej na podstawie odpowiedniego pola w nagłówku IP. Administratorzy do dyspozycji mają dwa rodzaje PHB:

- Przekazywanie przyśpieszone EF (ang. *Expedited Forwarding*) – określa, że dostarczony pakiet powinien zostać wysłany do kolejnego węzła z jak najmniejszym opóźnieniem. Dodatkowo klasa ruchu o skonfigurowanej prędkości musi zostać wysłana z taką samą lub wyższą prędkością. Głównym przeznaczeniem tego modelu przekazywania są sieci obsługujące transmisje wymagające małego opóźnienia.
- Przekazywanie gwarantowane AF (ang. *Assured Forwarding*) – model ten klasyfikuje każdy strumień do jednej z czterech klas ruchu, każda z nich uzyskuje część bufora oraz pasma. W obrębie klasy każdy pakiet otrzymuje jedną z trzech preferencji odrzucenia, określającą w jakiej kolejności router będzie odrzucał dane w przypadku wykorzystania zasobów przez daną klasę (Kurose, 2006; Flannagan, 2001; Flannagan, 2003).

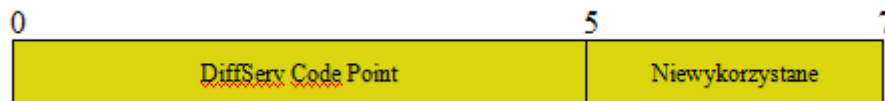
Klasyfikacja oraz oznaczanie pakietów

Klasyfikacja pakietów jest podstawą prawidłowego funkcjonowania modelu usług zróżnicowanych. Każdy strumień wchodzący do domeny DS przechodzi przez odpowiedni filtr klasyfikujący typ ruchu, następnie zostaje w odpowiedni sposób oznaczony (Rys 37). Każdy strumień oznaczony w ten sam sposób przydzielany jest do tej samej grupy oraz traktowany w ten sam sposób.



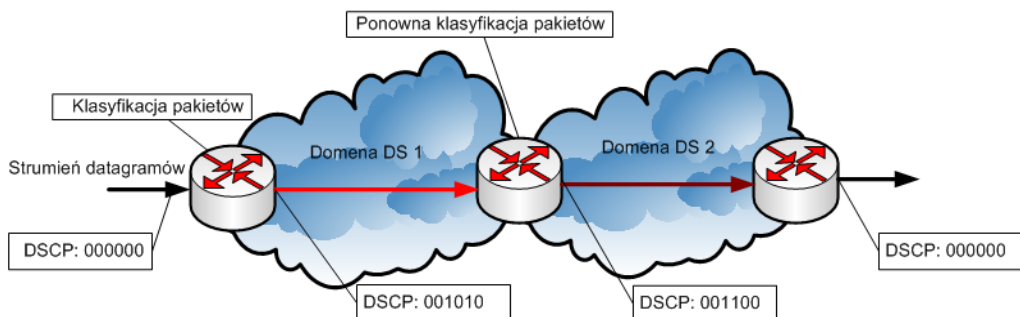
Rys. 37. Klasyfikacja oraz oznaczanie datagramów.

Kluczowym elementem oznaczania pakietów w architekturze Diffserv jest DSCP (ang. *Differentiated Services Code Point*) znajdujący się w polu DS (ang. *Differentiated Services*), zastępującym w nagłówku IP dotychczas używany znacznik TOS (Rys. 38).



Rys. 38. Pole DSCP.

Pole DS zbudowane jest z 6 bitowego pola DiffServ Code Point oraz 2 bitów nie wykorzystanych zarezerwowanych do późniejszego zastosowania. DSCP nie jest kompatybilne z dotychczas wykorzystywanym polem ToS, dlatego urządzenia wykorzystujące pole Typ usługi odczytują jedynie pierwsze 3 bity pola DS. DSCP ustawiane jest przez router brzegowy domeny i może ulegać zmianom podczas przekraczania granicy między domenami (Rys. 39) (Flannagan, 2001; Flannagan, 2003).



Rys. 39. Ponowna klasyfikacja pakietów na granicy domen DiffServ.

Zadanie klasyfikacji oraz oznaczania datagramów spełnia wiele mechanizmów. Najczęściej spotykanymi rozwiązaniami są (Tab. 11) :

- CAR (ang. *Comitted Access Rate*);
- PBR (ang. *Policy-based routing*);
- NBAR (ang. *Network-based application recognition*).

Tab. 11. Mechanizmy klasyfikacji oraz znakowania datagramów.

Mechanizm	Działanie
PBR	Mechanizm ten podejmuje decyzję na podstawie adresu lub portu źródłowego oraz zdefiniowanej przez administratora listy dostępu. Na początku przy wykorzystaniu ACL (ang. <i>Access Control List</i>) wybierane są strumienie danych, a następnie przesyłane przez odpowiednie interfejsy lub oznaczane .
CAR	Mechanizm ten klasyfikuje oraz oznacza datagramy na podstawie różnych informacji m.in.: portu fizycznego, adresu docelowego i źródłowego, adresu fizycznego czy rodzaju protokołu IP. Przeznaczony jedynie do filtrowania sieci opartych na protokole IP. Kontroluje on strumień wybrany na podstawie ACL, porównuje jego szybkość transmisji z ustawieniami administratora i podejmuje działanie w zależności od wyniku. Współpracuje wraz z mechanizmem „wiadra z żetonami”.
NBAR	Podobnie jak dwa powyższe mechanizmy służy do klasyfikacji oraz oznaczania datagramów w sieciach IP. Zaletą przemawiającą za jego wykorzystaniem jest dużo większa elastyczność, ponieważ do klasyfikacji wykorzystuje oprócz informacji zawartych w nagłówkach warstwy 2 i 3, także informacje w nagłówkach warstw wyższych. Umożliwia to na dokładniejsze sterowanie ruchem w dużych sieciach.

(docwiki.cisco.com; Flannagan, 2001).

Zarządzanie zatorami

Ważnym aspektem modelu usług zróżnicowanych jest zarządzanie zatorami w sieciach komputerowych. Mogą one doprowadzić do niekontrolowanego zmniejszenia efektywności jej działania a nawet uniemożliwić jej funkcjonowanie. Najpowszechniej stosowanym mechanizmem przeznaczonym do zarządzania zatorami wykorzystywanymi w QoS jest kolejkovanie datagramów w węzłach sieci. Algorytmy stosowane do tego celu różnią się w zależności od potrzeb konkretnej sieci komputerowej (zależy od rodzaju ruchu

obsługiwanego przez nią). Najczęściej stosowane mechanizmy kolejowania ich działania, zalety oraz wady przedstawione są Tabeli 12 (docwiki.cisco.com; Ferguson, 1998; Flannagan, 2001).

Tab. 12. Mechanizmy kolejkowania datagramów.

	FIFO (ang. First In First Out)	PQ (ang. Priority Queuing)
Opis mechanizmu kolejkowania	FIFO jest najprostszym z wykorzystywanych obecnie mechanizmów kolejkowania. Jego zadaniem jest przyjmowanie datagramów z interfejsu wejściowego a następnie umieszczanie ich w tej samej kolejności w buforze interfejsu wyjściowego i wysyłaniu ich z prędkością na jaką pozwala dany interfejs. Mechanizm ten nie wymaga żadnych dodatkowych mechanizmów klasyfikacji pakietów.	Działanie tego mechanizmu opiera się na klasyfikacji datagramów na różne priorytety. Urządzenia wykorzystujące Priority Queuing posiadają 4 kolejki o różnych priorytetach do których są przydzielane dane przychodzące. Następnie wysyłane są do interfejsu wyjściowego zgodnie z ich priorytetem (kolejki opróżniane są w kolejności od najwyższego priorytetu do najniższego).
Zalety	<ul style="list-style-type: none"> - w większości urządzeń wykorzystywany jako mechanizm domyślny, oznacza to dobrze opracowany algorytm działania; - w przypadku gdy sieć działa przy wystarczającym poziomie zasobów oraz poziomie możliwości przełączających opóźnienia są małe. 	<ul style="list-style-type: none"> - daje administratorom dużą kontrolę nad ruchem sieciowym; - duża elastyczność klasyfikacji oraz przypisywania datagramów do odpowiednich kolejek; - datagramy wymagające szybszej obsługi otrzymują wyższy priorytet i zostają obsłużone w pierwszej kolejności.
Wady	<ul style="list-style-type: none"> - duże opóźnienia datagramów przy dużych obciążeniach; - utrata danych w przypadku przepełnienia kolejki, co powoduje obniżenie poziomu jakości usług 	<ul style="list-style-type: none"> - duże natężenie ruchu wysoko priorytetowego może doprowadzić do zablokowania danych o niskim priorytecie; - duże obciążenie systemu spowodowane konieczności klasyfikacji oraz obsługi kolejek; - mała skalowalność mechanizmu.

	CBQ (ang. <i>Class-Based Queuing</i>)	FQ (ang. <i>Fair Queuing</i>)
Opis mechanizmu kolejkowania	<p>CBQ jest odmianą algorytmu PQ, istnieje możliwość utworzenia kilkunastu kolejek obsługujących przychodzący ruch. W kolejkowaniu CBQ do opróżniania kolejek wykorzystywany jest algorytm round-robin (opróżnianie kolejek następuje cyklicznie). Algorytm ten pozwala administratorowi na ustawienie ilości danych w kolejce, które zostaną obsłużone w danym cyklu.</p>	<p>FQ to grupa algorytmów zwana potocznie algorytmami sprawiedliwego kolejkowania. Ruch sieciowy dzielony jest zgodnie z ustawionymi przez administratora parametrami na strumienie, a następnie przypisywany do odpowiedniej kolejki. Obecnie istnieje kilka algorytmów z tej rodziny różniących się sposobem podziału na strumienie. Obecnie najczęściej wykorzystywanym algorytmem jest WFQ (ang. <i>Weighted Fair Queuing</i>) i jego odmiany, które oprócz podziału na strumienie przypisuje odpowiednie priorytety kolejkom.</p>
Zalety	<ul style="list-style-type: none"> - wyeliminowane ryzyko zatrzymania datagramów z niższym priorytetem; - większa elastyczność algorytmu w porównaniu do PQ ze względu na większą liczbę kolejek (do 16) oraz możliwość ustalenia ilości danych obsługiwanych w cyklu. 	<ul style="list-style-type: none"> - do obsługi kolejek wykorzystywany mechanizm round-robin, co zapobiega zatorom w kolejkach; - możliwość równego podziału łącza między użytkowników; - obsługa do 256 kolejek co zwiększa elastyczność algorytmu; - w niektórych przypadkach kolejki otrzymują priorytety, co umożliwia obsługę naważniejszego ruchu szybciej.
Wady	<ul style="list-style-type: none"> - mała skalowalność ze względu na duże zapotrzebowanie zasobów sprzętowych w przypadku dużych sieci; - niekorzystny wpływ routingu przemieszczanych pakietów i intensywnego zarządzania kolejkami. 	<ul style="list-style-type: none"> - podobnie jak w przypadku CBQ mała skalowalność; - nie można określić przepustowości dla konkretnych danych; - brak priorytetyzacji poza algorytmami ważonymi.

Zarządzanie zatorami w sieciach IP nie ogranicza się wyłącznie do kolejgowania przychodzących danych. Skutecznymi metodami ograniczającymi liczbę występujących zatorów są także mechanizmy profilowania ruchu:

- kształtowanie ruchu sieciowego (ang. *Traffic Shaping*) – zbiór mechanizmów odpowiedzialny za kontrolowanie ilości danych wchodzących do sieci oraz natężenia transmisji z niej.
- kontrola dostępu (ang. *Admission Control*) – odpowiada za kontrolowanie ruchu wchodzącego do sieci i odrzucanie ruchu blokowanego.

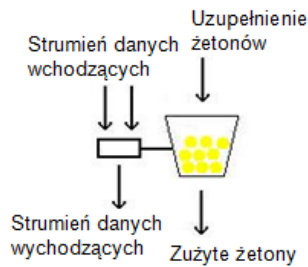
Podstawowymi mechanizmami pozwalającymi na kształtowanie ruchu w sieciach komputerowych są model „cieknącego wiadra” (ang. *Leaky Bucket*) oraz model „wiadra z żetonami” (ang. *Token Bucket*). W przypadku pierwszego modelu (Rys. 40) strumień danych trafiają do bufora (reprezentowanego przez wiadro) z różnymi prędkościami.

Natomiast z wiadra „wyciekają” z ustaloną prędkością porcje danych, w ten sposób kontrolowana jest prędkość danych wychodzących z sieci. W sytuacji szybszego napływania danych niż szybkość opróżniania wiadra może dojść do przepełnienia bufora oraz odrzucania nadmiaru datagramów.



Rys. 40. Model ciekącego wiadra.

Mechanizm „wiadra z żetonami” (Rys. 41) to metoda pozwalająca na kształtowanie ruchu w urządzeniach sieciowych. Działa podobnie do modelu pierwszego z tym, że transmisja danych przebiega tylko wtedy, gdy w wiadrze znajdują się żetony. W innym wypadku następuje oczekiwanie (pakiety są buforowane a w przypadku przepełnienia bufora są odrzucane) na uzupełnienie żetonów. Administrator ustala ilość danych, która może być przetransportowana przy użyciu jednego żetonu. W przypadku, gdy w wiadrze znajdzie się nadmiar żetonów nastąpi chwilowe przyśpieszenie transmisji pakietów. Obecnie oba modele wykorzystywane są najczęściej wspólnie (np. Jako pierwsze „wiadro z żetonami” z niego dane trafiają do „cieknącego wiadra” gdzie strumień zostaje wygładzony) (Ferguson, 1998; Flannagan, 2001).

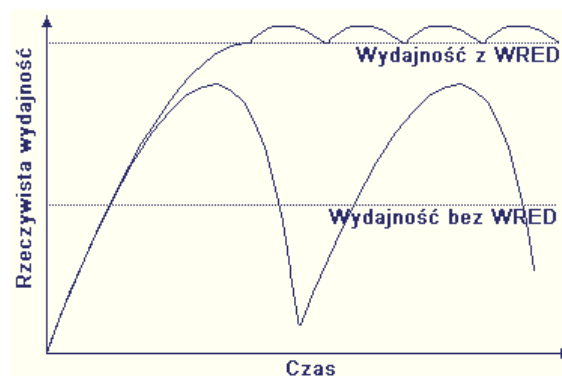


Rys. 41. Model wiadra z żetonami.

Mechanizmy zapobiegania zatorów

Do prawidłowego funkcjonowania sieci nie wystarczą jedynie mechanizmy zarządzania zatorami, najlepszą metodą zapewnienia jakości usług jest ich unikanie na co pozwalają algorytmy „losowego wczesnego wykrywania” (RED - ang. *Random Early Detection*) oraz „ważonego losowego wczesnego wykrywania” (WRED – ang. *Weighted Random Early Detection*). Mechanizmy te, w odróżnieniu do mechanizmów szeregowania datagramów, mają za zadanie nie dopuścić do powstawania zatorów.

Pierwszym z mechanizmów stosowanych do zapobiegania powstawaniu zatorów jest RED. Odrzuca on pakiety TCP zmniejszając tym sposobem wielkość okna TCP a zarazem ilość danych transmitowanych w późniejszym czasie. Działanie jego opiera się na dwóch granicznych wartościach długości bufora. Jeżeli bufor przekroczy pierwszą z wartości granicznych system RED rozpoczyna losowe odrzucanie pakietów przychodzących, od tego momentu im większa wielkość bufora, tym więcej pakietów zostanie odrzuconych. Przekroczenie wartości górnego progu przez długość kolejki spowoduje, że wszystkie przychodzące pakiety będą odrzucane do momentu zmniejszenia ilości pakietów w buforze. Odmianą algorytmu RED częściej stosowaną jest mechanizm WRED, który dodatkowo wprowadza podział przychodzącego strumienia danych na klasy, którym niezależnie przydzielane są odpowiednie progi, a jako pierwsze odrzucane są pakiety o najniższym priorytecie (cisco.com; Hassan, 2004; Flannagan, 2003).



Rys. 42. Wpływ zastosowania WRED na wydajność sieci [30i].

Wpływ działania mechanizmu WRED na funkcjonowanie sieci przedstawia Rysunek 42. Widoczne jest na nim znaczny wzrost wydajności sieci przy wykorzystaniu mechanizmów unikania zatorów.

3.3. Przesyłanie datagramów w sieciach IP wykorzystując MPLS

MPLS jest technologią opracowaną na potrzeby współczesnych, szybko rozwijających się sieci IP. Wzrost natężenia ruchu danych w istniejącej infrastrukturze (np. sieć szkieletowa ISP) wykorzystującej tradycyjne mechanizmy trasowania powoduje stopniowe zmniejszanie ich efektywności działania. Algorytmy trasowania korzystają z informacji o adresie, celu znajdującym się w nagłówku warstwy 3, co zmusza routery do dekapulacji każdego otrzymanego pakietu. Proces ten jest pracochłonny i przy dużym natężeniu ruchu danych może doprowadzić do poważnego obciążenia urządzenia, i dodatkowo powodować zatory w sieci (ze względu na czas uzyskiwania adresu celu). MPLS to protokół opracowany uwzględniając zalety protokołu IP jak i technologii ATM (ang. *Asynchronous Transfer Mode*). Wykorzystano w nim rozwiązania znane z sieci wirtualnych obwodów, czyli etykiety stałej długości pozwalające na przesyłanie datagramów od źródła do celu. Nie zrezygnowano jednak z wykorzystania adresów celu oraz protokołów trasowania, są one nadal wykorzystywane w sieciach bez zaimplementowanego protokołu MPLS. Zaletą takiego rozwiązania jest szybkość działania. Routery obsługujące MPLS nie muszą dekapulować pakietu do warstwy 3 aby odczytać adres celu, wystarczy jedynie odczytanie etykiety. Prowadzi to do zmniejszenia obciążenia infrastruktury oraz przyspieszenia przesyłania danych przez sieć. Dodatkową zaletą MPLS jest duży wgląd w charakterystykę sieci na poziomie warstwy drugiej umożliwiający zarządzanie ruchem pakietów wykorzystując rodzaj przenoszonych przez nie informacji, czyli pozwala na wykorzystanie QoS. Oprócz sterowania ruchem, wykorzystując mechanizmy jakości usług MPLS umożliwia także tworzenie wirtualnych sieci prywatnych (Alvayn, 2001; Kurose, 2006).

3.3.1. Funkcjonowanie MPLS

Działanie MPLS polega na dołączeniu do pakietu etykiety na podstawie, której routery MPLS wiedzą gdzie dalej mają przesłać dane, bez potrzeby jego dekapulacji. Etykieta dodawana jest do datagramu w zależności od technologii sieci, w której będzie przenoszony:

- W sieciach Ethernet etykieta dodawana jest pomiędzy nagłówkami warstwy 2 i 3 (Rys. 43), w tym wypadku protokół ten nazywany jest protokołem warstwy 2,5.



Rys. 43. Etykieta MPLS w ramce Ethernet.

- W przypadku sieci FR (ang. *Frame Relay*) oraz ATM informacje etykiety MPLS zawarte są odpowiednio w identyfikatorze ścieżek wirtualnych VPI (ang. *Virtual Path Identifier*) lub identyfikatory kanałów wirtualnych VCI (ang. *Virtual Chanel Identifier*) dla FR oraz w polu DLCI dla ATM.

Obecne zastosowania protokołu MPLS ograniczają się do przenoszenia datagramów protokołu IP, same etykiety MPLS mogą być przenoszone przez wszystkie technologie warstwy 2 (Ghein, 2006; Kurose, 2006, tech-portal.pl).

Etykieta MPLS jest 32 bitowym polem zbudowanym z 4 struktur (Rys. 44):



Rys. 44. Budowa etykiety MPLS.

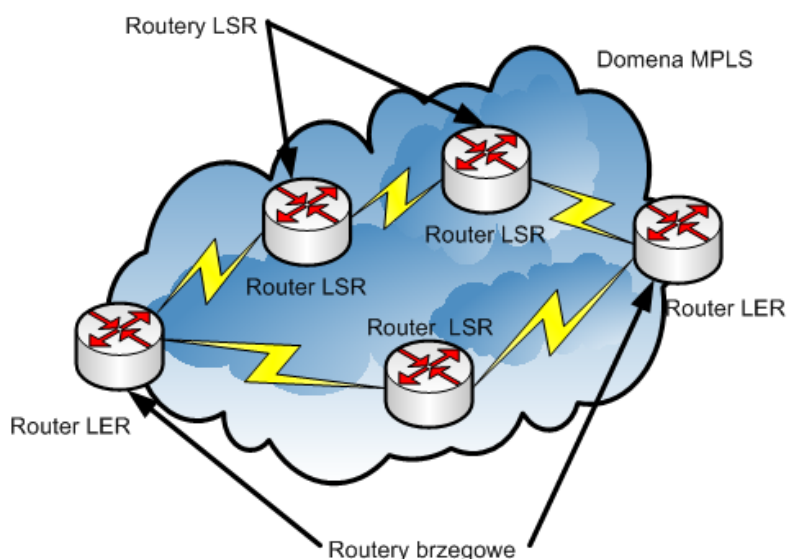
- Numer etykiety – 20 bitowe pole zawierające indeks wykorzystywany do określenia kolejnego punktu w sieci, do którego ma zostać przesłany pakiet;
- TC – 3 bitowe pole obecnie stosowane w technikach QoS do sterowania przepływem informacji w zależności od danych przenoszonych przez pakiet;
- S – pole 1 bitowe odpowiedzialne za sygnalizowanie końca stosu etykiet;
- TTL (ang. *Time to Live*) – ostatnie pole w etykiecie MPLS pozwalające na uniknięcie pętli podczas przenoszenia pakietu.

Zdarza się również, że w celu przesłania pakietu przez sieć wykorzystującą MPLS routery wymagają kilku etykiet. W takim wypadku etykiety łączone są w stos, a ostatnia etykieta nazywana jest dnem stosu i ma ustawiony odpowiednio bit S (Ghan, 2006; tech-portal.pl).

Przesyłanie pakietów z wykorzystaniem MPLS

Przesyłanie danych z wykorzystaniem MPLS opiera się o mechanizm przełączania pakietów wzdłuż trasy. Służą do tego specjalne routery obsługujące technologie MPLS nazwane LSR (ang. *Label Switched Router*). W domenie MPLS wyróżnić możemy 2 rodzaje takich urządzeń (Rys. 45):

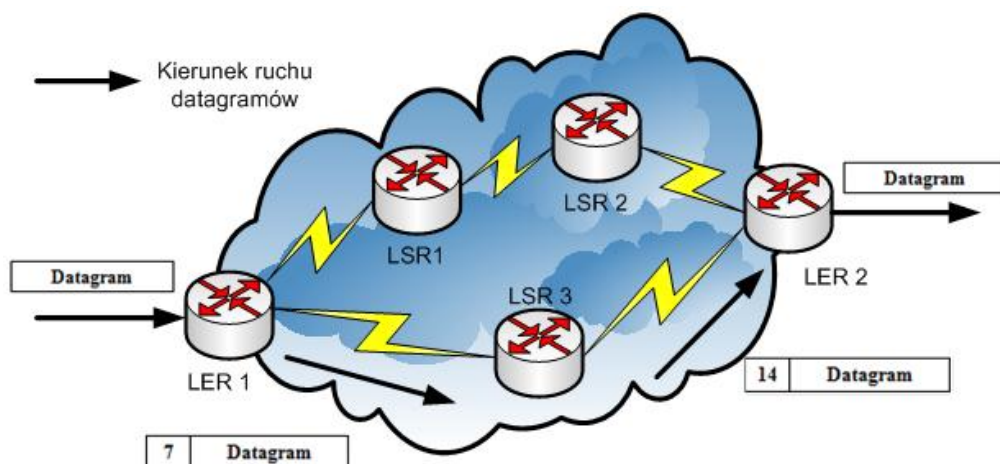
- Routery brzegowe LER (ang. *Label Edge Router*) – rodzaj routera LSR znajdującego się na wejściu oraz wyjściu domeny i jego zadaniem jest dodawanie oraz usuwanie etykiet
- Routery szkieletowe LSR – zwykły router LSR przełączający podróżujące pakiety wewnątrz domeny MPLS.



Rys. 45. Typy routerów w domenie MPLS.

Routery LSR wykonują szereg operacji związanych z przełączaniem etykiet (Rys. 46):

- Dodawanie nowych etykiet do datagramów, które jeszcze ich nie posiadają;
- Usuwanie etykiet od datagramu oraz wysłanie go do sieci docelowej (lub sieci, w której MPLS nie funkcjonuje);
- Zamianę etykiet w przypadku, gdy pakiet przesyłany jest przez pośredni router LSR. (Na wejściu do routera etykieta jest zdejmowana, następnie dodawana jest nowa i pakiet przekazywany jest do kolejnego punktu).



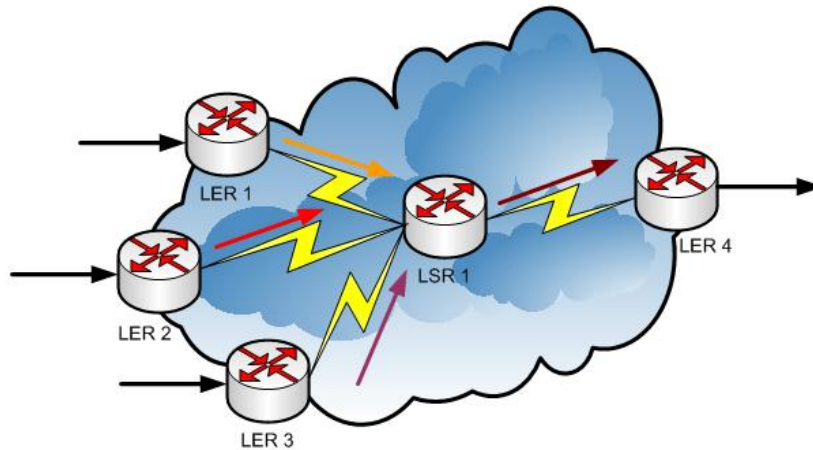
Rys. 46. Funkcje routerów w domenie MPLS.

Datagramy trafiają do domeny MPLS przez router brzegowy LER 1, który przydziela im odpowiednią etykietę i wysyła korzystając z odpowiedniego interfejsu. Dane trafiają do interfejsu wejściowego LSR 3 gdzie etykieta jest usuwana. Router przeszukuje tablicę LFIB (ang. *Lobel Forwarding Informtion Base*) i na podstawie jej zawartości wybiera nową etykietę. Następnie datagramy wysyłane są w kierunku routera LER 2, który usuwa etykiety i wysyła dane do celu.

Zbiór wszystkich routerów LSR na drodze od wejścia do domeny do jej wyjścia, przez które transportowane są datagramy, nazywany jest LSP (ang. *Label Switched Path*). Ścieżki rozpoczynają routery wejściowe LER (dodają etykiety), a kończą routery wyjściowe LER (usuwiają etykiety), wzdłuż ścieżki znajdują się routery LSR przełączające etykiety (Alvayn, 2001; tech-portal.pl, itpedia.pl).

Protokół MPLS pozwala także na wykorzystanie wielu istniejących połączeń o takim samym koszcie w celu zrównoważenia obciążenia. Przesyłane dalej datagramy mogą mieć te same bądź różne etykiety, w zależności od relacji między routerami. W przypadku, gdy routery, do których mają trafić dane należą do tej samej przestrzeni etykiet datagramy otrzymują te same etykiety niezależnie od trasy, w innym wypadku natomiast etykiety są różne.

W MPLS wspierane jest również agregowanie ruchu w domenie MPLS trafiającego do niej wykorzystując różne routery LER (Rys. 47).



Rys. 47. Agregacja ruchu w domenie MPLS.

Strumienie danych trafiają do domeny MPLS korzystając z routerów LER 1, LER 2 oraz LER 3, wszystkie strumienie mają opuścić domenę korzystając z routera brzegowego LER 4. Dane z różnymi etykietami trafiają z wejściowych routerów do routera LSR 1, gdzie otrzymują nowe etykiety i są wysyłane dalej. Wszystkie strumienie poruszają się do routera LER 4 tą samą trasą, z tego względu router LSR 1 wszystkim datagramom przydzielił tą samą etykietę. Praktyka taka umożliwia na zmniejszenie wykorzystania puli etykiet, co przydatne jest w rozbudowanych sieciach MPLS (Ghein, 2006; itpedia.pl).

Przydzielanie etykiet datagramom wchodzącym do domeny MPLS odbywa się na podstawie klasyfikacji strumieni przy pomocy klas FEC (ang. *Forwarding Equivalence Class*). Klasy te ustalane są przez administratorów na podstawie wielu parametrów co nadaje całemu procesowi elastyczności (Ghein, 2006).

3.3.2. Dystrybucja etykiet w sieci MPLS

Routery MPLS podejmują decyzję dotyczącą przesyłania datagramu na podstawie etykiet, które są do niego dołączone, następnie zmieniają etykietę tak, aby kolejny LSR wiedział gdzie wysłać dalej dane. Etykiety dodawane są wyłącznie przez routery brzegowe, następnie ulegają tylko zamianom wzdłuż trasy. Routery MPLS muszą posiadać pewne informacje, aby mogły poprawnie przysyłać dane dalej i zamieniać etykiety. Służą do tego dwie struktury danych:

- LIB (ang. *Label Information Base*) – tablica zawierająca wszystkie etykiety lokalne wraz z skojarzonymi z nimi etykietami otrzymanymi od innych routerów LSR;
- LFIB (ang. *Local Forwarding Information Base*) - posiada jedynie obecnie używane wpisy pochodzące z tablicy LIB.

Routery do utrzymania spójności tych tablic muszą rozsyłać informacje o odwzorowaniach etykieta/FEC do swoich sąsiadów, wykorzystuje się do tego dwa mechanizmy:

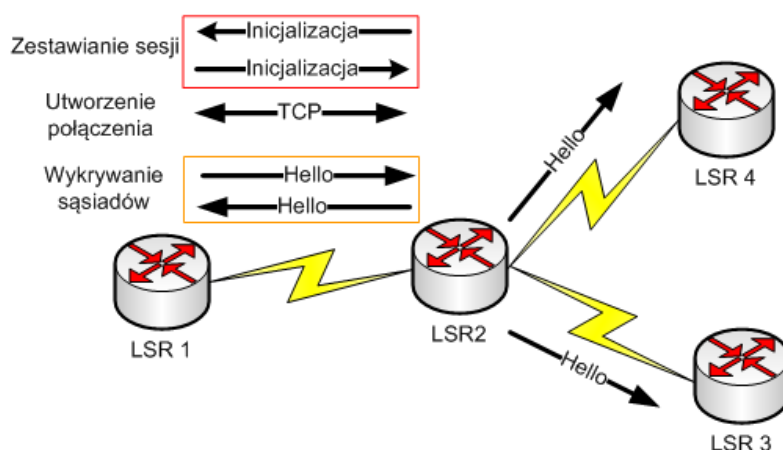
- Mapowania etykiet można rozsyłać korzystając z istniejących protokołów trasowania, co niestety niesie ze sobą konieczność opracowania odpowiednich mechanizmów. Wyjątek stanowi protokół BGP, w którym łatwo można zaimplementować możliwość przenoszenia etykiet wraz z prefiksami IP;
- Najczęściej stosowanymi obecnie mechanizmami służącymi do rozsyłania odwzorowań etykiet na klasy FEC są specjalne protokoły, m.in: LDP (ang. *Label Distribution Protocol*), TDP (ang. *Tag Distribution Protocol*) oraz RSVP.

Liczącymi się obecnie rozwiązaniami są protokoły LDP oraz RSVP. LDP ze względu na otwartość standardu, która pozwala na implementacje w urządzeniach wszystkich producentów, natomiast RSVP jest jedynym protokołem wykorzystywanym w inżynierii ruchu MPLS (Alvayn,2001; Ghein, 2006; Kummar, 2004).

Funkcjonowanie protokołu LDP

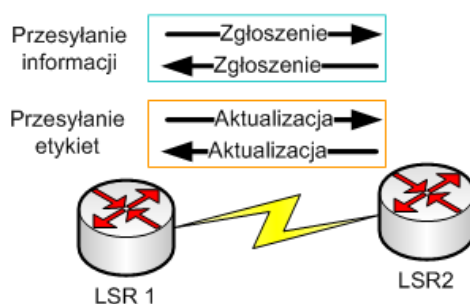
Protokół LDP służy do rozsyłania skojarzeń etykiet z klasami FEC, aby pakiety mogły zostać przesyłane wzdłuż LSP. Działanie protokołu opiera się na połączeniu między sąsiadującymi LSR. Wyszukiwanie sąsiadów odbywa się przez rozsyłanie komunikatów „Hello” na adres 224.0.0.2 wykorzystując port UDP 646. Po wykryciu sąsiadów routery LSR przystępują do ustanowienia połączenia między sobą w celu zestawienia sesji LDP i wymiany informacji o etykietach. Połączenie zestawiane jest z wykorzystaniem protokołu TCP oraz portu 646, i jest ono dwukierunkowe. Następnie zestawiana zostaje sesja (Rys. 48) z określonymi parametrami, do ich negocjacji wykorzystywane są komunikaty inicjalizujące. Ustaleniu podlegają takie parametry jak:

- Wartości liczników;
- Metoda dystrybucji etykiet;
- W przypadku implementacji MPLS w środowisku ATM dodatkowymi parametrami są identyfikator drogi wirtualnej - VPI oraz identyfikator kanału wirtualnego – VCI;
- Natomiast w przypadku sieci wykorzystujących technologię Frame Relay dodatkowym parametrem jest zakres identyfikatorów łącza danych (DLCI – ang. *Data-link connection identifier*) (tech-portal.pl; Alvayn,2001; Ghein, 2006).



Rys. 48. Etapy zestawiania sesji LDP.

Zestawienie sesji umożliwia wymianę aktualizacji LDP, zawierających aktualne mapowania etykiet na klasy FEC. Sesje LDP (Rys. 49) utrzymywane są do momentu wystąpienia błędów bądź usunięcia routera z sieci. Podtrzymywanie sesji odbywa się wykorzystując komunikaty informacyjne (przesyłają standardowe informacje o sesji LDP oraz informacje o błędach). W przypadku nieobecności któregoś z tych komunikatów sesja zostaje zakończona po określonym czasie (Ghein, 2006).

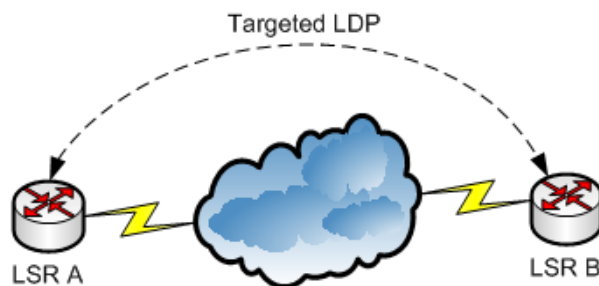


Rys. 49. Komunikaty wymienianie podczas sesji LDP.

Opisany powyżej mechanizm ustanawiania sąsiedztwa dotyczy jedynie przypadku, w którym routery LSR są ze sobą połączone bezpośrednio i nazywany jest podstawowym mechanizmem wykrywania. Technologia MPLS pozwala także na ustanawianie relacji sąsiedztwa pomiędzy routerami, którymi nie istnieje połączenie bezpośrednie, ten mechanizm nazywany jest rozszerzonym mechanizmem wykrywania (Rys. 50) i charakteryzuje się:

- Komunikaty *Hello* wysyłane są na unicastowy adres IP.
- Mechanizm rozszerzony jest procesem asymetrycznym, w odróżnieniu do symetrycznego mechanizmu podstawowego. Oznacza to, że odbierający LSR może odebrać komunikat albo go zignorować. W przypadku odebrania komunikatu router

odbierający okresowo wysyła komunikaty *Hello* do urządzenia inicjalizującego (Ghein, 2006; cisco.com).



Rys. 50. Rozszerzony mechanizm wykrywania sąsiadów.

Routerzy LSR do oznaczania pakietów wykorzystują pulę etykiet. Wyróżniamy ich dwa rodzaje: pula etykiet dla całego urządzenia oraz pula etykiet wydzielana dla poszczególnych interfejsów. Zastosowanie ich jest zależne od zastosowanej technologii warstwy 2. W przypadku, gdy dwa routery mają więcej niż jedno połączenie bezpośrednie w technologii LC-ATM (ang. *Label-controlled ATM*), to dla każdego takiego połączenia musi istnieć oddzielna sesja i każdy interfejs musi posiadać własną pulę etykiet. W pozostałych przypadkach wykorzystywana jest pula etykiet dla całego urządzenia i tworzona jest tylko jedna sesja LDP. Po ustanowieniu sesji następuje wymiana informacji między routerami LSR (juniper.net; Ghein, 2006).

MPLS umożliwia dystrybucję skojarzeń etykieta/FEC w trzech trybach, z których każdy ma 2 algorytmy działania:

- Przydział etykiet (ang. *Label Distribution Modes*);
- Sterowanie LSP (ang. *LSP Control Modes*);
- Podtrzymywanie etykiet (ang. *Label Retention Modes*) (tech-portal.pl; Alvayn,2001).

Tab. 13. Tryby rozsyłania odwzorowań etykiet.

Przydział etykiet	
„na żądanie” (ang. <i>Downstream-on-Demand</i>)	LSR wysyła żądanie do routera następnego o odwzorowanie etykieta/FEC, router następny przygotowuje mapowanie i odsyła je do routera poprzedniego.
„niezapowiedzianej” (ang. <i>unsolicited downstream</i>)	Router LSR wysyła przyporządkowania etykiet do FEC bez uprzedniego żądania do wszystkich przyległych routerów LSR.

Sterowanie LSP	
„niezależny” (ang. <i>Independent LSP Control</i>)	Routery niezależnie tworzą odwzorowania etykiet i rozsyłają je do routerów sąsiednich w dowolnym czasie, co może doprowadzić do rozpoczęcia transmisji przed utworzeniem pełnej trasy LSP.
„uporządkowany” (ang. <i>Ordered LSP Control</i>)	LSR tworzy odwzorowanie wyłącznie, gdy jest routerem brzegowym dla danej klasy ruchu lub gdy otrzymał odwzorowanie etykiet od routera następnego. Podejście takie umożliwia zestawienie pełnej ścieżki przed rozpoczęciem przełączania pakietów.
Podtrzymywanie etykiet	
Liberal Label Retention	Routery LSR przechowują wszystkie otrzymane odwzorowania w tablicy LIB, jedno z nich umieszczane jest w LFIB i wykorzystywane do przełączania. Metoda ta pozwala na szybką reakcję w przypadku zmian topologii, niestety przechowywanie wszystkich odwzorowań powoduje zwiększenie zapotrzebowania na pamięć.
Conservative Label Retention	Urządzenia wykorzystujące ten algorytm przechowują jedynie odwzorowania powiązane z routerem, który jest punktem kolejnego skoku dla danego FEC. Algorytm ten prowadzi do zmniejszenia zapotrzebowania na pamięć, jednak w razie zmian w topologii router musi oczekiwać na odwzorowanie do nowego punktu skoku.

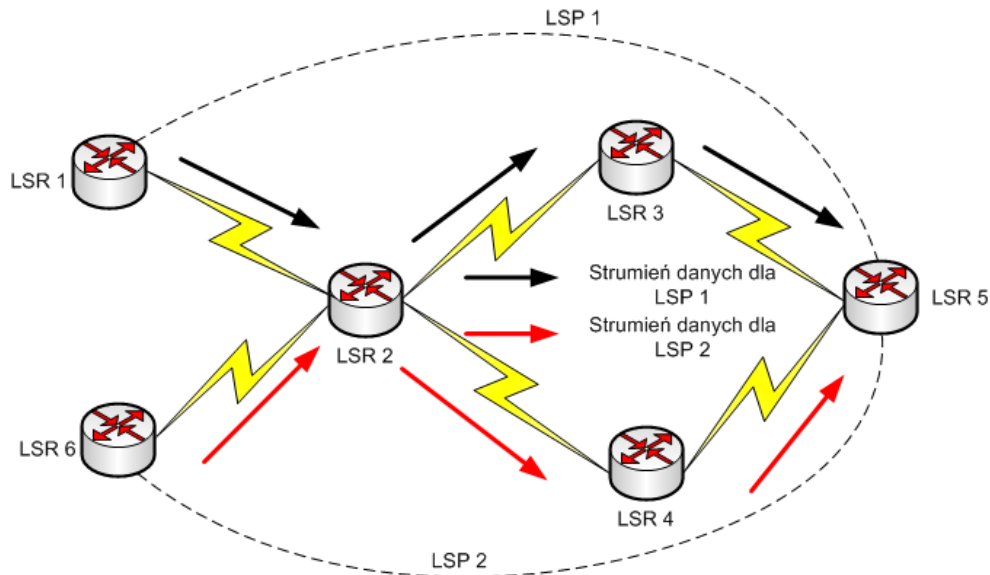
Usuwanie etykiet

Mapowania etykiet przechowywane są w routerach do momentu zakończenia sesji LDP lub otrzymania komunikatu wymuszającego ich usunięcie. Mapowanie może zostać usunięte w przypadku zmiany etykiety lokalnej (np. w wyniku gdy interfejs o danym prefiksie IP zostanie odłączony, ale inne urządzenie nadal rozsyła dany prefiks). Router LSR w takim wypadku wysyła komunikat *LDP Withdraw* do wszystkich urządzeń, z którymi ma zestawioną sesję. Następnie każdy router go otrzymujący musi potwierdzić przyjęcie wiadomości za pomocą komunikatu *LDP Release* (Gheini, 2006).

3.3.3. Inżynieria ruchu w MPLS

Podstawowe działanie routerów LSR polega na przełączaniu datagramów w oparciu o posiadane informacje. Oznacza to, że każdy router wzdłuż LSP jest niezależny, podobnie jak w przypadku standardowych protokołów trasowania. Podczas takiego sposobu przesyłania

wybierana jest najlepsza trasa z możliwych, co w dużych sieciach operatorskich doprowadzić może do przeciążenia jednej trasy przy jednoczesnym braku wykorzystania innych. W przypadku takim administratorzy wykorzystują techniki zebrane pod pojęciem Inżynieria ruchu do kierowania strumieni danych tak, aby równoważyć obciążenia w sieci. Protokół MPLS w tym celu pozwala na zestawianie ścieżek między źródłem a celem tak, aby różne strumienie danych przesyłane były różnymi trasami.



Rys. 51. Inżynieria ruchu w sieciach MPLS.

W sieci na rysunku 51 obydwa strumienie danych przeznaczone są dla LSR 5, jeżeli zastosowano by standardowe protokoły routingu obydwa strumienie od routera LSR 2 przesyłane by były tą samą najlepszą trasą. MPLS TE (ang. *MPLS Traffic Engineering*) pozwala administratorowi zestawić trasę LSP (tunel) dla każdego z tych strumieni. Zestawienie takich LSP ma na celu dzielenie obciążenia między istniejące połączenia. Każda z takich ścieżek posiada router początkowy oraz router końcowy, przy czym router początkowy zajmuje się obliczaniem najlepszej z możliwych tras na podstawie posiadanych informacji (niewykorzystane pasmo połączeń oraz muszą znać całą topologię sieci). Dane potrzebne do wyznaczania najlepszych tras zbierane są wykorzystując protokoły trasowania stanu łącza. Zestawienie ścieżki LSP wymaga także sygnalizacji lub inaczej rezerwacji zasobów w węzłach wzdłuż niej, wykorzystywany do tego jest protokół sygnalizujący RSVP. Utworzony w ten sposób tunel jest jednokierunkowy ponieważ LSP są jednokierunkowe. Prawidłowe jego funkcjonowanie wymaga także aby każdy LSR wewnątrz LSP znał etykiety obowiązujące w obrębie tunelu, do ich dystrybucji wykorzystywane są dwa protokoły RSVP

z rozszerzeniem TE oraz CR-LDP (ang. *Constraint-based LDP*) (Ghein, 2006; Alwayn, 2001; itportal.pl).

3.4. Zarządzanie ruchem w sieciach IP z wykorzystaniem list dostępu

Filtrowanie ruchu w węzłach sieciowych to jedna z podstawowych metod, jakie administratorzy mogą wykorzystać do zarządzania ruchem w sieci. Proces ten pozwala zarówno na blokowanie niechcianego ruchu przed wejściem do sieci oraz kierowanie specyficznego strumienia przez odpowiedni interfejs routera. Filtrowanie ruchu wykorzystywane jest w wielu zaawansowanych funkcjach routera takich jak:

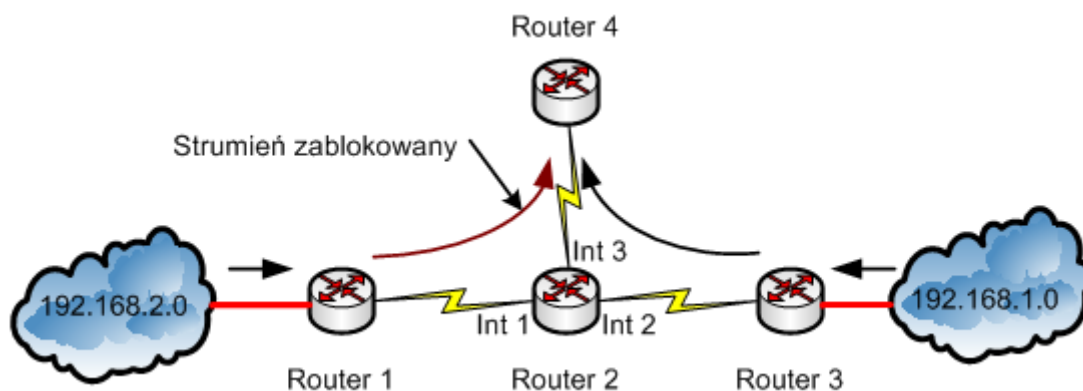
- Zapewnianie jakości usług – filtrowanie ruchu oraz jego kolejkovanie;
- Trasowanie – ograniczenie rozsyłania aktualizacji oszczędzając pasmo dostępne w sieci;
- Rozpoznawanie ruchu, który ma być poddany różnym procesom np. ruch przeznaczony dla szyfrowania;
- Zabezpieczanie routera – ograniczenie dostępu do sieci jak i samych urządzeń znajdujących się w niej (www.cisco.howto.pl; Flannagan, 2001; CCNA Exploration: Accessing the WAN).

Administratorzy wprowadzają funkcje filtrowania w routerach stosując listy dostępu ACL (ang. *Access Control List*). ACL składają się z reguł określających zachowanie routera wobec otrzymanych pakietów. Podzielić je można na 2 główne grupy:

- Standardowe listy dostępu;
- Rozszerzone listy dostępu.

Standardowe listy dostępu

Działanie standardowych list dostępu opiera się o adresy źródłowe datagramów. Każdy router odbierając strumień danych porównuje ich adres źródłowy i w zależności od posiadanych reguł kieruje ruch dalej, bądź odrzuca go. Głównym zastosowaniem standardowych list dostępu jest blokowanie ruchu wchodzącego do naszej sieci, bądź blokowanie ruchu z określonej sieci bądź hosta.



Rys. 52. Działanie standardowej listy dostępu.

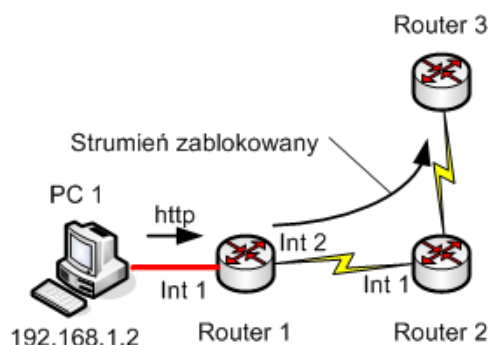
Rysunek 52 przedstawia zasadę działania standardowych list dostępu. Ruch pochodzący z sieci 192.168.2.0 nie zostaje przepuszczony do Routera 4, natomiast ruch pochodzący z sieci 192.168.1.0 przechodzi bez przeszkód. Związane jest to z umieszczoną w interfejsie 3 listą dostępu blokującą cały ruch pochodzący z sieci 192.168.2.0 oraz dopuszczający pozostały.

Najważniejszym aspektem działania jest konieczność umieszczenia standardowej listy dostępu jak najbliżej celu podróży datagramów. W innym wypadku ruch z sieci źródłowej zablokowany zostałby całkowicie lub nie miałby dostępu do części sieci, do której dostać się powinien normalnie. Rozwiązanie takie jest wadą standardowych ACL, ponieważ ruch zablokowany jest na końcu swojej podróży i zanim to się stanie przejdzie przez sieć marnując niepotrzebnie zasoby (CCNA Exploration: Accessing the WAN; Józefiak, 2009).

Standardowe listy dostępu stosowane są także wraz z protokołami trasowania dynamicznego. Router na podstawie reguł znajdujących się w ACL określa czy dane trasy mają zostać odebrane lub wysłane z wykorzystaniem aktualizacji protokołów routingu (Doyle, 2005).

Rozszerzone listy dostępu

Większe możliwości kontroli ruchu dają administratorom rozszerzone listy dostępu. Strumień ruchu rozpoznawane na podstawie nie tylko adresu źródłowego, ale także adresu celu, oraz protokołów i portów zamieszczonych w nagłówku warstwy 4. Taki sposób filtrowania sprawdza do sieci możliwości elastycznego kierowania ruchem. W odróżnieniu do standardowych list dostępu administrator dostaje możliwość szczegółowego rozpoznawania strumieni i ich manipulowania.



Rys. 53. Działanie rozszerzonej listy dostępu..

Administrator sieci, jak na Rysunku 53, chce zablokować dostęp do stron www komputerowi PC 1. Stosuje do tego celu rozszerzoną listę dostępu na interfejsie Int 1 Routera 1 blokującą ruch wejściowy www z komputer 192.168.1.2 skierowany do dowolnego innego hosta. Ruch innego typu będzie przepuszczany bez zatrzymywania.

Zaletą takiego rozwiązania jest możliwość zablokowania ruchu już na samym początku, odciążając w ten sposób sieć od niepotrzebnego obciążenia. Oprócz zastosowania przy sterowaniu ruchu w sieci, rozszerzone listy dostępu stosuje się także np.. przy rozpoznawaniu strumieni ruchu przeznaczonych do szyfrowania przez protokół IPsec (np. przy tworzeniu wirtualnych sieci prywatnych). Rozszerzone ACL pozwalają również administratorom na zabezpieczenie naszej sieci przed określonymi typami ataków, chociażby atakami typu DoS (ang. *Denial of Service*).

Zaawansowane listy dostępu

Poza standardowymi oraz rozszerzonymi listami dostępu administratorzy mają także do dyspozycji rozwiązania bardziej złożone, zaliczamy do nich np.:

- Dynamiczne listy dostępu – dostęp do danej sieci jest blokowany użytkownikom przez rozszerzoną listę dostępu znajdującą się na routerze do momentu, aż uwierzytlinią się wykorzystując telnet. Wykorzystywane często w przypadkach, gdy do sieci mają mieć dostęp użytkownicy zdalni korzystający z sieci globalnej do połączenia;
- Reflexive ACL – daje administratorom większą możliwość kontroli ruchu wchodzącego do sieci. W przypadku strumienia mającego początek na zewnątrz sieci zostaje on zablokowany przez router. Natomiast jeśli ruch zewnętrzny jest częścią sesji, której początek znajduje się wewnątrz sieci zostanie dopuszczony przez router;
- Czasowe listy dostępu – funkcjonują na podobnej zasadzie jak rozszerzone listy dostępu, z tą różnicą iż jest on przydzielany czasowo (np. w określonym dniu, o określonej godzinie itp.) (CCNA Exploration: Accessing the WAN).

3.5. Metody sterowania ruchem pakietów w sieciach z nadmiarowością

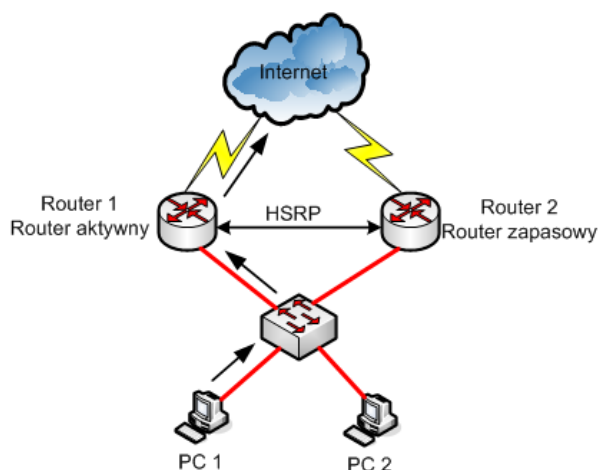
Nadmiarowość zapewnia sieciom prawidłowe działanie nawet w wyniku awarii jakie w niej mają miejsce. Wymusza ona także na administratorach odpowiednie sterowanie ruchem datagramów w sieciach. W przypadku redundancji bramy domyślnej administratorzy muszą zapewnić, że wszystkie urządzenia w sieci będą korzystać z odpowiedniej bramy domyślnej. Natomiast nadmiarowa liczba połączeń WAN pozwala na elastyczne sterowanie ruchem w zależności np. od adresu sieci docelowej wykorzystując do tego zmiany metryk tras w protokole BGP.

3.5.1. Sterowanie ruchem w sieciach z redundancją bramy domyślnej

Najczęstszą przyczyną braku dostępu do Internetu w sieciach komputerowych jest awaria routera pełniącego rolę bramy domyślnej. Operatorzy sieci chcąc uniknąć takich sytuacji korzystają z kilku routerów pełniących rolę bram domyślnych, jednak wymaga to uruchomienia w sieci specjalnych protokołów umożliwiających prawidłową współpracę wszystkich routerów. Należą do nich m.in. HSRP (ang. *Hot Standby Router Protocol*), VRRP (ang. *Virtual Router Redundancy Protocol*), GLBP (ang. *Gateway Load Balancing Protocol*) (Oppenheimer, 2004; cisco.com).

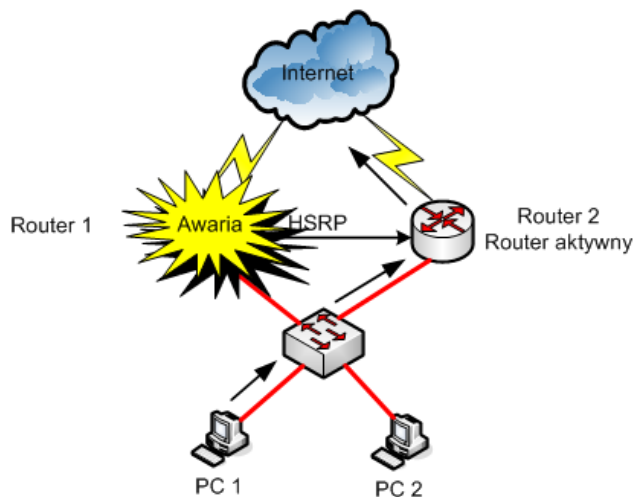
Protokół HSRP

Protokół HSRP opracowany został przez firmę Cisco jako protokół pozwalający na eliminację braku łączności w sieci wynikłej z awarii bramy domyślnej. Działanie protokołu opiera się na utworzeniu wirtualnej bramy domyślnej, która uczestniczy w wymianie danych. Wirtualny router posiada własny adres IP oraz MAC (ang. *Media Access Control*), który używany jest przez wszystkie hosty w sieci jako adres bramy domyślnej. W obrębie grupy routerów pracujących pod kontrolą HSRP za przesyłanie datagramów odpowiada w danym momencie tylko jeden router zwany także routerem aktywnym (Rys. 54).



Rys. 54. Przesyłanie datagramów w sieci wykorzystującej protokół HSRP.

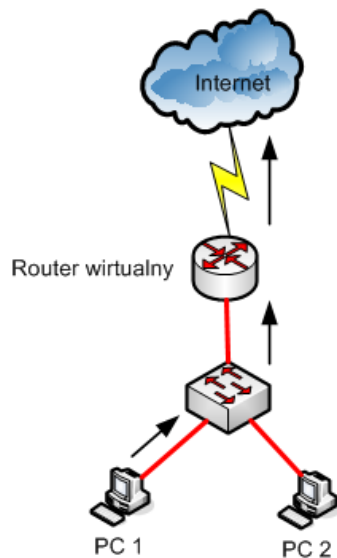
W przypadku jego awarii jego miejsce zajmuje router zapasowy i w ten sposób uzyskuje się ciągłość pracy sieci (Rys. 55) (Oppenheimer, 2004; cisco.com).



Rys. 55. Przesyłanie datagramów w sieci z protokołem HSRP. Awaria Router'a 1.

Funkcjonowanie HSRP

Wszystkie routery pracujące pod kontrolą protokołu HSRP mają swoje własne unikalne adresy IP. Spośród wszystkich tych routerów wybierany jest jeden pełniący rolę bramy domyślnej. Dla urządzeń w sieci routery te widoczne są jako jeden router wirtualny posiadający własny adres IP i to on wykorzystywany jest do komunikacji z bramą domyślną (Rys 56). Podczas awarii routera aktywnego jego funkcje przejmuje router zapasowy, urządzenia w sieci nadal korzystają z adresu IP routera wirtualnego więc zmiana ta dla nich jest niewidoczna (Oppenheimer, 2004).



Rys. 56. Topologia logiczna sieci z punktu widzenia znajdujących się w niej urządzeń.

Ważnym aspektem działania protokołu HSRP jest wybór routerów aktywnych oraz zapasowych. Wyłanianie są one w procesie elekcji, której podstawą są priorytety posiadane przez każdy router. Urządzenia z najwyższym priorytetem wybierane są na router aktywny, a drugi router pod tym względem jest routerem zapasowym. Niejednokrotnie ma miejsce sytuacja, iż routery mają ten sam priorytet, w takiej sytuacji protokół bierze pod uwagę adres IP urządzenia. W skrajnym przypadku routerem aktywnym staje się ten, który został uruchomiony jako pierwszy i pozostaje nim do momentu pojawienia się w sieci routera o wyższym priorytecie.

W dużych sieciach, gdzie wymagana jest niezawodność komunikacji między podsieciami grupa routerów HSRP liczy często więcej niż dwa urządzenia. W grupie takiej zawsze wybierane jest jedno urządzenie aktywne i jedno zastępcze, pozostałe są nieaktywne do momentu awarii routera głównego, i zmiany stanu routera zapasowego. W takiej sytuacji protokół wybiera nowy router zastępczy spośród routerów nieaktywnych. Działanie takie zapewnia mniejsze obciążenie sieci, ponieważ komunikaty okresowe wymieniane są jedynie między routerem aktywnym oraz zapasowym (Solie, 2001; cisco.howto.pl; cisco.com).

Prawidłowe działanie protokołu HSRP zapewnione jest przez jego mechanizm komunikacji, w skład którego wchodzi trzy typy komunikatów:

- *Hello* – zawiera priorytet routera oraz wszystkie dane potrzebne do elekcji routera aktywnego i zapasowego. Komunikat ten rozsyłany jest okresowo w celu informowania grupy o prawidłowym funkcjonowaniu routera;
- *Coup* – komunikat wysyłany przez router informujący router aktywny, że w sieci znajduje się router o wyższym priorytecie;

- *Resign* – komunikat wysyłany przez router aktywny podczas jego wyłączania, bądź otrzymania komunikatów Hello lub Coup od urządzenia o wyższym priorytecie.

Komunikaty HSRP rozsyłane są wykorzystując adres rozsyłania grupowego i wykorzystują nagłówek protokołu HSRP (Rys. 57).

0	7	15	23	31
Wersja	Kod	Stan	Hello time	
Hold time	Priorytet	Grupa	Zarezerwowane	
Dane uwierzytelniania				
Adres IP routera wirtualnego				

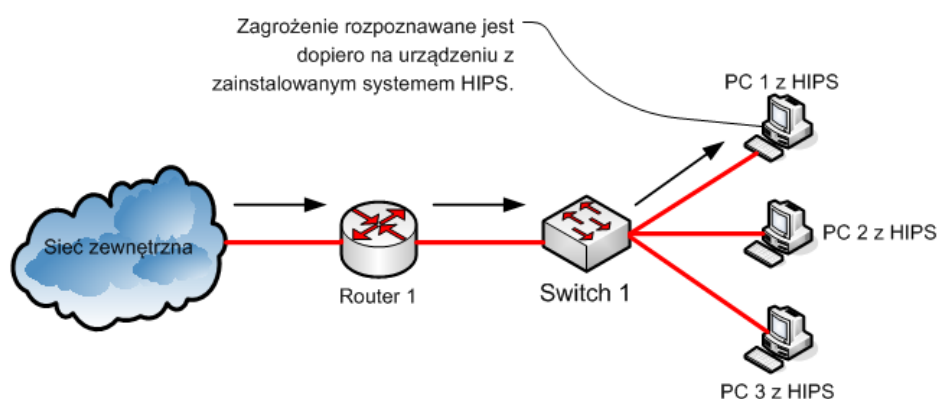
Rys. 57. Nagłówek komunikatu HSRP.

- Wersja – wersja wykorzystywanego protokołu HSRP;
- Kod – określa typ przesyłanego w pakiecie komunikatu;
- Stan – określa stan, w którym obecnie znajduje się router wysyłający komunikat;
- Hello time – zawiera okres czasu, po którym rozsyłany jest ponownie komunikat Hello, w przypadku, gdy nie jest on ustawiony router otrzymuje go w komunikacie od routera aktywnego;
- Hold time – określa czas, przez jaki obecny komunikat Hello ma być ważny;
- Priorytet – zawiera priorytet routera wysyłającego i wykorzystywane jest do elekcji routera aktywnego oraz zapasowego;
- Grupa – identyfikuje grupę routerów HSRP;
- Dane uwierzytelniania – zawiera informacje potrzebne do uwierzytelniania routera HSRP;
- Adres IP routera wirtualnego – określa adres IP routera wirtualnego, z którego korzystają urządzenia w sieci do komunikacji z bramą domyślną (Solie, 2001, docwiki.cisco.com, javvin.com).

4. Zarządzanie ruchem pakietów z wykorzystaniem Systemów Zapobiegania Właman

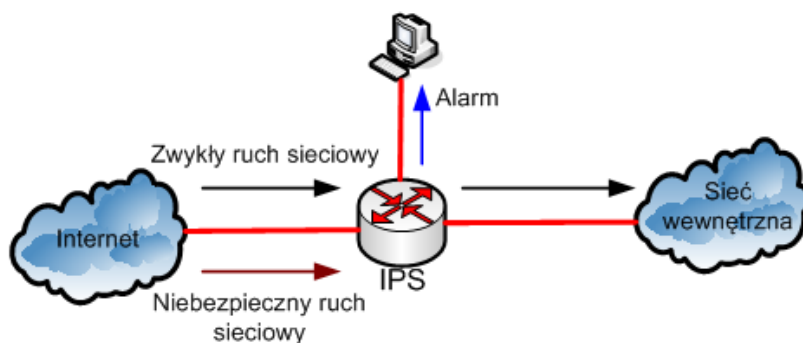
Przepływem pakietów w sieciach komputerowych sterują także systemy zapobiegania włamanom IPS (ang. *Intrusion Prevention System*). Zadaniem ich jest wykrywanie wszelkich niebezpieczeństw grożącym sieci oraz zapobieganie im. Systemy IPS mogą działać w dwóch następujących konfiguracjach:

- Systemy instalowane na hostach w sieci HIPS (ang. *Host-Based IPS*) (Rys. 58) – badają wyłącznie ruch wchodzący i wychodzący do hosta, na którym się znajdują zabezpieczając go przed zagrożeniami pochodzącymi z sieci.



Rys. 58. Działanie systemu HIPS.

- Systemy instalowane w sieci jako oddzielne urządzenia NIPS (ang. *Network-Based IPS*) (Rys. 59) – oddzielne urządzenia umieszczane w sieci np. na połączeniu sieci wewnętrznej i zewnętrznej, analizujące ruch wchodzący do sieci zabezpieczonej i reagujące w przypadku niebezpieczeństwa. (cisco.netacad.net).



Rys. 59. Działanie sieciowego systemu zapobiegania włamaniom.

Działanie systemów IPS

Podstawą działania systemów zapobiegania włamaniom jest wykrywanie zagrożeń w przesyłanych strumieniach danych. W systemach tych wykrywanie odbywa się w oparciu o trzy następujące mechanizmy:

- Wykrywanie w oparciu o sygnatury – cały ruch przechodzący przez urządzenie IPS podlega dokładnemu filtrowaniu. Dane zawarte w poszczególnych warstwach podlegają sprawdzeniu i porównaniu z wzorcami posiadanymi przez IPS. Gdy wykryte zostanie zagrożenie, IPS podejmuje akcje zgodnie z ustawieniami administratora;
- Wykrywanie w oparciu o anomalie – system IPS posiada profile ruchu dla określonych grup użytkowników, z którymi porównuje ruch obecny w sieci i w przypadku wystąpienia dużych różnic podejmuje odpowiednie akcje. Detekcja taka nie przebiega w oparciu o sygnatury, co daje jej większe możliwości wykrywania nowych typów ataku. Metoda ta także pozwala wykryć i zablokować np. ataki typu DoS (ang. *Denial of Service*), DDoS (ang. *Distributed Denial of Service*), które potrafią zagrażać sieciom. Wykrycie ich opiera się m.in. na liczbie połączeń w okresie czasu i w przypadku przekroczenia limitu ruch zostaje zablokowany. Ruch pochodzący z urządzenia atakującego jest blokowany natomiast pozostały bez problemu wpuszczany jest do wnętrza sieci (cisco.netacad.net, CNAP Network Security 2 v2.0).

Systemy IPS chronią sieci oraz użytkowników przed różnego rodzaju atakami przeprowadzanymi na poziomie różnych warstw modelu ISO/OSI i wyróżniamy m.in.:

- Ataki w warstwie aplikacji oraz prezentacji (ataki na protokoły takie jak http (ang. *Hypertext Transfer Protocol*), DNS (ang. *Domain Name System*), FTP, SMTP (ang. *Simple Mail Transfer Protocol*) i inne; ataki powodujące przepełnienie buforów; uruchamianie niechcianego oprogramowania np. skryptów, przenoszenie wirusów) oraz ataki rozpoznawcze w tej warstwie;
- Ataki w warstwie sesji m.in. ataki na protokół zdalnego wywoływania procedur (stosując np. wirusy komputerowe), ataki na tunele VPN, czy zabezpieczenia SSL (ang. *Secure Sockets Layer*);
- Ataki w warstwie transportowej – skanowanie portów (atak rozpoznawczy), ataki typu DoS, nienaturalna fragmentacja pakietów, wykorzystanie niedoskonałości protokołu TCP.

- Ataki w warstwie sieciowej – Nieprawidłowe dane w nagłówku datagramu IP (adresy, opcje itp.), wykorzystanie protokołu ICMP do ataków rozpoznawczych (www.checkpoint.com, csrc.nist.gov).

Przykłady ataków sieciowych występujących w warstwach od sieciowej do warstwy aplikacji

Cross Site Scripting – to ataki występujące w warstwach aplikacji oraz prezentacji. Głównym ich zadaniem jest umożliwienie atakującemu przejęcie kontroli nad atakowanym hostem. Wykorzystuje się do tego specjalny link prowadzący do strony z zawartym skryptem, który po otwarciu przez przeglądarkę atakowanego urządzenia wykonuje się i umożliwia uzyskanie dostępu do komputera ofiary. Przed tego typu atakami zabezpieczają sieci systemy zapobiegania włamaniom, filtrują one cały ruch wchodzący do sieci i porównują go z sygnaturami. Dzięki nim są one w stanie wykryć, iż zawartość strony jest potencjalnie niebezpieczna i informują o tym użytkownika, blokując także wyświetlenie zawartości takiej strony.

Kolejnym zagrożeniem dla systemów pracujących w sieciach komputerowych są ataki na protokół Zdalnego Wywoływania Procedur RPC (ang. *Remote Procedure Call*). Protokół ten odpowiedzialny jest za udostępnianie zasobów urządzeniom pracującym w sieci. Jednym z najbardziej popularnych ataków na tę usługę był wirus Blaster, atakujący usługę RPC i powodujący m.in. restart komputera oraz był odpowiedzialny za ataki DDoS na serwery Microsoftu. Głównym źródłem pochodzenia wirusa były załączniki w poczcie elektronicznej a także sieć lokalna. Współczesne systemy IPS posiadają sygnatury pozwalające wykryć robaka w strumieniu danych i blokują np. możliwość ściągnięcia zainfekowanego pliku z poczty, bądź blokują jego przeniesienie przez sieć lokalną.

Liczną grupę ataków tworzących niebezpieczeństwo sieci komputerowych są ataki występujące w warstwie 3, a do najpopularniejszych należą ataki rozpoznawcze oraz ataki typu DDoS mające na celu unieruchomienie serwera bądź całej sieci. Do pierwszego typu ataków zaliczamy np. „TCP Sweep” oraz „UDP Sweep”, służą głównie do zdobycia informacji o usługach działających w sieci, a zarazem uzyskanie informacji o słabościach systemu i wykorzystaniu ich do późniejszego ataku. Systemy zapobiegania włamaniom posiadają wzorce odpowiadające tego typu atakom i w przypadku wykrycia informują administratora o zagrożeniu. Drugi typ ataku wykorzystywany jest często do zatrzymania działania systemu informatycznego i wykorzystuje się do tego często mechanizm ustanawiania połączenia TCP. Atak ten polega na podmianie przez atakującego adresu źródła

i wysłaniu takiego pakietu z flagą SYN do komputera ofiary, on odpowiada pakietem SYN-ACK i oczekuje na odpowiedź. Odpowiedź jednak nie zostanie odesłana, ponieważ adresat nie istnieje. W tym przypadku połączenie TCP zostaje na półotwarte przez pewien czas i gdy liczba takich połączeń będzie duża, zapełnią się bufory, co nie pozwoli na otwarcie kolejnych połączeń oraz zablokuje cały ruch sieciowy na urządzeniu. Urządzenia IPS wykrywają tego typu ataki korzystając z mechanizmu wykrywania anomalii i blokują adres IP atakującego hosta.

W warstwie sieciowej często spotykanym typem ataków są ataki przez fragmentacje i polegają one na manipulowaniu przez atakującego fragmentami tak, aby host docelowy (bądź węzeł sieciowy) miał problemy z ich złożeniem w całość. Systemy IPS posiadają specjalne mechanizmy wirtualnego scalania fragmentów, które pozwalają na wykrycie anomalii występujących w fragmentach. Atutem takiego scalania jest to, iż nie jest wymagane scalenie całego datagramu a jedynie jego fragmentów, co zapobiega niepotrzebnemu zużyciu pamięci. Po wykryciu jakichś nieprawidłowości IPS natychmiast alarmuje operatora o występującym problemie (<http://www.cgisecurity.com>, www.cisco.com, CNAP: Network Security 2 v2.0, www.itpedia.pl).

5. Urządzenia sieciowe odpowiedzialne za sterowanie ruchem pakietów w warstwie 3 modelu ISO/OSI

Sieci komputerowe mogą spełniać swoje funkcje dzięki szeregowi urządzeń odpowiedzialnych za przesyłanie danych. Urządzenia te pozwalają na zarządzanie ruchem datagramów IP w sieciach korzystając z różnych mechanizmów. Najważniejszą grupę tych urządzeń stanowią pracujące w warstwie 3 routery oraz przełączniki warstwy 3.

Routery zapewniają między innymi komunikację pomiędzy różnymi sieciami, pozwalają na sterowanie przepływem danych przez mechanizmy takie jak: Translacja adresów NAT, protokoły routingu dynamicznego, zapewnienie jakości usług QoS czy listy dostępu pozwalające administratorom blokowanie określonego ruchu. Rozwiązania bardziej zaawansowane umożliwiają także wykorzystywanie systemów zapobiegania włamania w celu blokowania ruchu niebezpiecznego dla sieci wewnętrznej.

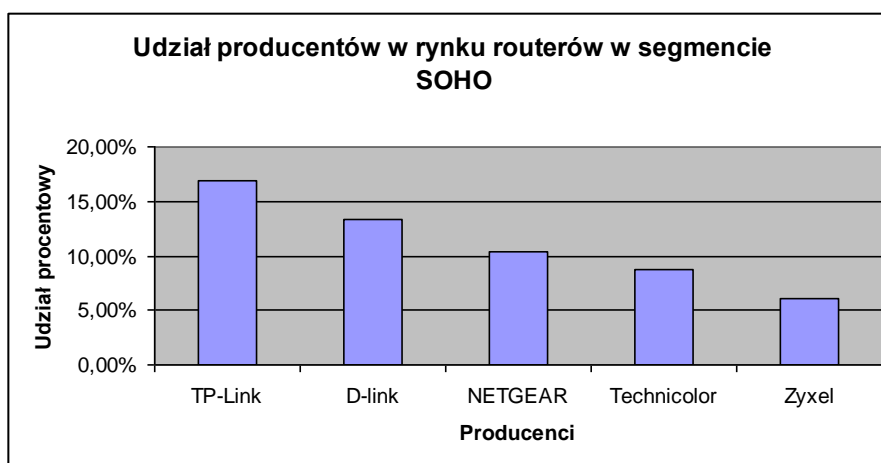
Przełączniki warstwy 3 w odróżnieniu do tych z warstwy 2 pozwalają na bardziej zaawansowane przesyłanie danych w sieci wykorzystując informacje zawarte w nagłówkach warstwy 3, podobnie jak routery pozwalają na trasowanie datagramów między sieciami, jednak wykonują to znacznie szybciej dzięki wyspecjalizowanej budowie. Jedną z ważnych cech odróżniających je od routerów jest brak typowych złącz WAN, które posiadają wszystkie routery (compnetworking.about.com, www.cisco.com).

Urządzenia sieciowe, podobnie jak wszystkie inne produkty, dzielone są na segmenty, które przeznaczone są dla różnych grup odbiorców w zależności od ich potrzeb oraz możliwości finansowych. I tak dzielimy urządzenia na 4 segmenty:

- Małe przedsiębiorstwa prowadzone najczęściej w małych biurach potocznie określane mianem SOHO (ang. *Small Office/Home Office*);
- Średnie i duże przedsiębiorstwa określane potocznie mianem SMB (ang. *Small and Medium Bussines*);
- Sektor dużych firm (*Enterprise*);
- Firmy udostępniające dostęp do sieci globalnej, potocznie nazywane ISP (wikipedia.org).

5.1. Routery segmentu Small Office/Home Office

W segmencie produktów przeznaczonych dla najmniejszych firm rzadko spotykane są routery takiego typu, jak te przeznaczone na najwyższe segmenty rynku; podobnie nie występują tutaj przełączniki warstwy 3. Najczęściej spotykanymi urządzeniami wykorzystywanymi w tym segmencie są stosunkowo tanie produkty łączące w sobie funkcje routerów, przełączników, modemów oraz punktów dostępowych. W tym segmencie rynku do najważniejszych dostawców, według zestawienia przedstawionego na rysunku 60, należą TP-Link, D-link oraz Netgear. Porównanie funkcjonalności w zakresie zarządzania ruchem pakietów urządzeń tych producentów znajduje się w tabeli 14 (www.tp-link.com, www.dlink.pl, www.netgear.pl).



Rys. 60. Udział w rynku producentów routerów w segmencie SOHO.

5.2. Routery segmentu Small and Medium Business

Zapotrzebowanie przedsiębiorstw segmentu małych i średnich firm na wydajne rozwiązania sieciowe są większe niż tych z segmentu SOHO. Wiąże się to bezpośrednio z liczbą użytkowników oraz urządzeń pracujących w sieci. Podobnie jak w przypadku rynku bardzo małych firm dostawcami sprzętu jest tu wielu producentów jednak najbardziej liczącymi graczami są: CISCO, TP-Link, D-Link i to ich produkty przedstawię w pracy. W tym segmencie rynku nadal mamy do czynienia z rozwiązaniami łączącymi wiele funkcji w jedno za stosunkowo małe pieniądze, jednak spotykane są także rozwiązania bardziej zaawansowane, chociażby urządzenia firmy CISCO z serii 2900, których funkcjonalność w dużej mierze zależna jest od wykupionych licencji (np. możliwość tworzenia tuneli VPN wymaga licencji), od wykorzystywanej wersji IOS, czy od zamontowanych dodatkowych modułów. Funkcjonalność wybranych modeli przedstawia tabela 15 (www.realwire.com, www.cisco.com, www.tp-link.com, www.dlink.pl).

Tab. 14. Porównanie wybranych urządzeń segmentu SOHO.

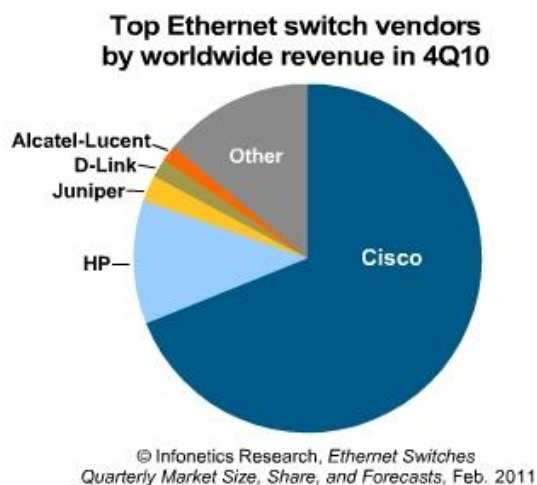
Nazwa urządzenia:	TP-Link TD8950ND	Netgear DGN-2200	D-Link DSL-2740B
Firewall:	NAT, SPI (ang. <i>Stateful Packet Inspection</i>), Filtrowanie ruchu sieciowego na podstawie adresów MAC, IP a także zawartości przesyłanych pakietów.	NAT, Filtrowanie ruchu sieciowego na podstawie adresu IP oraz zawartości przesyłanych pakietów, IDS.	NAT, SPI, Filtrowanie pakietów (MAC/IP/TCP/UDP), wbudowany IDS.
Quality of Service:	Kolejność obsługi w oparciu o pole ToS. Możliwość oznaczania pakietów stosując pole DSCP, urządzenie umożliwia tworzenie kolejek dla pakietów.	Automatyczne priorytety dla przesyłanego ruchu – działa wyłącznie dla sieci beprzewodowej.	Zarówno dla sieci LAN jak i WLAN, predefiniowane klasy ruchu, działanie w oparciu o pole ToS, Kształtowanie ruchu.
Wirtualne sieci Prywatne:	Możliwość tworzenia tuneli VPN stosując protokół IPsec. Obsługa funkcji VPN Pass-through.	Możliwość tworzenia tuneli VPN stosując protokół IPsec. Obsługa funkcji VPN Pass- through.	Obsługuje jedynie opcje VPN Pass-through
Inne funkcje zarządzania ruchem:	Serwer wirtualny: Pozwala na udostępnienie usługi publicznej poza NAT, korzystając z przekierowania portu. Strefa zdemilitaryzowana i przekierowywanie portów. Routing statyczny.	Przekierowywanie portów, strefa zdemilitaryzowana, routing statyczny, Serwer Wirtualny	Serwer wirtualny, przekierowywanie portów, DMZ, Routing statyczny oraz dynamiczny (RIP v1 oraz v2)

Tab. 15. Porównanie wybranych urządzeń segmentu SMB.

Nazwa urządzenia:	TP-Link TL-R480T+	D-Link DSR-1000	CISCO Router 2911 ISR2
Firewall:	NAT, Filtrowanie adresów IP/MAC oraz filtrowanie domen, filtrowanie pakietów.	IPS, SPI, NAT, PAT, Filtrowanie zawartości stron WWW, filtrowanie na podstawie adresu IP oraz MAC.	NAT, PAT, filtrowanie wykorzystując ACL, jako opcja płatna IPS oraz filtrowanie zawartości datagramów.
Quality of Service:	Zarządzanie przepustowością dla portu lub adresu IP, limitowanie liczby aktywnych sesji oraz lista sesji.	Zarządzanie przepustowością dla portu w oparciu o 3 klasy ruchu.	Klasyfikowanie i obsługa datagramów przy pomocy PBR oraz NBAR, zaawansowane zarządzanie zatorami (kolejkowanie, mechanizmy kształtowania ruchu), zapobieganie zatorom WRED.
Wirtualne sieci Prywatne:	Obsługuje tylko VPN pass-through.	70 tuneli VPN (IPSec/PPTP/L2TP), 20 tuneli SSL VPN, VPN pass-through.	Tunele VPN IPSec (zależne od zakupionej licencji).
Inne funkcje zarządzania ruchem:	Routing statyczny, Serwer wirtualny, przekierowywanie portów, DMZ, równoważenie obciążenia, nadmiarowość połączenia WAN.	Routing statyczny, dynamiczny (RIPv1, v2, OSPF), DMZ, przekierowywanie portów, równoważenie obciążenia na portach WAN, Failover WAN.	Protokoły HSRP, VRRP, GLBP w celu nadmiarowości bramy domyślnej, routing statyczny, routing dynamiczny (OSPF, EIGRP, BGP, IS-IS), MPLS, sterowanie za pomocą list dostępu

5.3. Routery oraz przełączniki warstwy 3 w segmencie dużych firm

W przypadku dużych firm zatrudniających wielu pracowników i dbających o poprawne funkcjonowanie swoich dużych sieci, administratorzy wybierają do ich budowy bardzo wydajne urządzenia sieciowe mogące sprostać obecnym oraz przyszłym potrzebom sieci. Do zarządzania przepływem datagramów służą routery ale także przełączniki warstwy 3 charakteryzujące się mniejszą funkcjonalnością, ale często wystarczającą do sprostania zadaniom przed nimi postawionymi i przy okazji mniejszą ceną, niż typowe urządzenia trasujące. Według danych statystycznych pochodzących z 4 kwartału 2010 roku przygotowanych przez Infonetics Research liczącymi producentami routerów dla segmentu dużych przedsiębiorstw są Cisco (71,8% udziałów w rynku), Hewlett-Packard oraz Juniper (Rys. 61) (www.einnews.com, <http://www.networld.pl>). Porównanie routerów tych firm znajduje się w Tabeli 16. Firma Cisco jest również głównym dostawcą przełączników na rynek urządzeń sieciowych, pozostałymi liczącymi dystrybutorami są Hewlett-Packard oraz Juniper. Dlatego do porównania wybiorę urządzenie tej firmy oraz HP i Juniper (Tab. 17) (www.cisco.com, www.juniper.net, www8.hp.com).



Rys. 61. Udział producentów przełączników w rynku [31i].

Tab. 16. Porównanie routerów segmentu Enterprise.

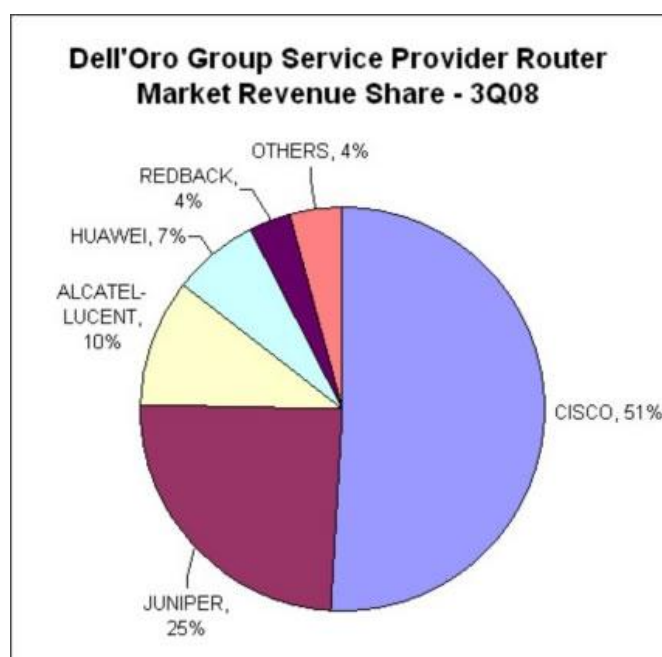
Nazwa urządzenia:	Cisco Router 7200 VXR Series	HP A-MSR-50 Series	Juniper J Series
Firewall:	Filtrowanie ruchu z wykorzystaniem ACL, NAT, PAT, CISCO Firewall, IPS (wymaga dodatkowego modułu), filtrowanie ruchu na podstawie zawartości.	SPI, filtrowanie przesyłanych danych, blokowanie ruchu z wykorzystaniem ACL.	SPI, NAT, PAT, filtrowanie z wykorzystaniem list dostępu, podział sieci na strefy, IPS (konieczny zakup dodatkowej licencji).
Quality of Service:	Klasyfikowanie i obsługa datagramów przy pomocy PBR oraz NBAR, Zaawansowane zarządzanie zatorami (kolejkowanie np. CBWFQ), unikanie zatorów (CBWRED, kształtowanie ruchu).	Kształtowanie ruchu i klasyfikacja datagramów przy pomocy mechanizmu CAR, zarządzanie zatorami (kolejkowanie FIFO, PQ, CQ itd.), unikanie zatorów (RED/WRED), Policy Routing.	Kształtowanie oraz klasyfikacja ruchu, zarządzanie zatorami (kolejkowanie np. CBWFQ), mechanizmy unikania zatorów WRED.
Wirtualne sieci Prywatne:	Z dodatkowym modulem do 5000 tuneli VPN (IPSec), obsługa MPLS VPN.	Tunele VPN (IPSec/MPLS).	Liczba tuneli IPSec VPN zależna od konkretnego modelu do 1024, obsługa MPLS VPN.
Inne funkcje zarządzania ruchem:	Protokoły HSRP, VRRP, GLBP w celu nadmiarowości bramy domyślnej, routing statyczny, routing dynamiczny (OSPF, EIGRP, BGP, IS-IS, RIP), MPLS, sterowanie za pomocą list dostępu.	Nadmiarowość bramy domyślnej (VRRP), routing statyczny, routing dynamiczny (RIP, OSPF IS-IS, BGP), MPLS, zarządzanie z wykorzystaniem ACL.	Nadmiarowość bramy domyślnej (VRRP, JSRP), routing statyczny, routing dynamiczny (RIPv2, OSPF, BGP, IS-IS), MPLS.

Tab. 17. Porównanie routerów segmentu Enterprise.

Nazwa urządzenia:	Cisco Router 7200 VXR Series	HP A-MSR-50 Series	Juniper J Series
Firewall:	Filtrowanie ruchu z wykorzystaniem ACL, NAT, PAT, CISCO Firewall, IPS (wymaga dodatkowego modułu), filtrowanie ruchu na podstawie zawartości.	SPI, filtrowanie przesyłanych danych, blokowanie ruchu z wykorzystaniem ACL.	SPI, NAT, PAT, filtrowanie z wykorzystaniem list dostępu, podział sieci na strefy, IPS (konieczny zakup dodatkowej licencji).
Quality of Service:	Klasyfikowanie i obsługa datagramów przy pomocy PBR oraz NBAR, Zaawansowane zarządzanie zatorami (kolejkowanie np. CBWFQ), unikanie zatorów (CBWRED, kształtowanie ruchu).	Kształtowanie ruchu i klasyfikacja datagramów przy pomocy mechanizmu CAR, zarządzanie zatorami (kolejkowanie FIFO, PQ, CQ itd.), unikanie zatorów (RED/WRED), Policy Routing.	Kształtowanie oraz klasyfikacja ruchu, zarządzanie zatorami (kolejkowanie np. CBWFQ), mechanizmy unikania zatorów WRED.
Wirtualne sieci Prywatne:	Z dodatkowym modulem do 5000 tuneli VPN (IPSec), obsługa MPLS VPN.	Tunele VPN (IPSec/MPLS).	Liczba tuneli IPSec VPN zależna od konkretnego modelu do 1024, obsługa MPLS VPN.
Inne funkcje zarządzania ruchem:	Protokoły HSRP, VRRP, GLBP w celu nadmiarowości bramy domyślnej, routing statyczny, routing dynamiczny (OSPF, EIGRP, BGP, IS-IS, RIP), MPLS, sterowanie za pomocą list dostępu.	Nadmiarowość bramy domyślnej (VRRP), routing statyczny, routing dynamiczny (RIP, OSPF IS-IS, BGP), MPLS, zarządzanie z wykorzystaniem ACL.	Nadmiarowość bramy domyślnej (VRRP, JSRP), routing statyczny, routing dynamiczny (RIPv2, OSPF, BGP, IS-IS), MPLS.

5.4. Routery oraz przełączniki warstwy 3 w segmencie ISP

Firmy tego segmentu zajmują się udostępnianiem usług internetowych, a także często odpowiadają za tranzytowe przysyłanie ruchu między sieciami innych operatorów. Funkcje te wymagają bardzo wydajnej infrastruktury i wydajnych urządzeń zapewniających odpowiedni poziom obsługi. Wymagania takie spełniają jedynie routery oraz przełączniki wielowarstwowe, szczególnie te o budowie modularnej pozwalającej na ciągły ich rozwój. Głównymi dostawcami routerów na ten segment rynku, według raportu Dell'Oro Group, są firmy Cisco, Juniper oraz Alcatel-Lucent co przedstawia wykres na Rysunku 62. (<http://www.networkworld.com>, www.alcatel-lucent.com, www.juniper.net, www.cisco.com)



Rys. 62. Udział producentów routerów w segmencie ISP [32i].

Sytuacja producentów przełączników w tym segmencie rynku jest praktycznie taka sama jak w segmencie dużych firm i według statystyk przedstawionych na rysunku 61 głównymi producentami są firmy: Cisco, Juniper oraz HP. Porównanie możliwości routerów z tego segmentu znajduje się w Tabeli 18, natomiast przełączników w Tabeli 19 (www.cisco.com, www.juniper.net, www8.hp.com).

Tab. 18. Wybrane modele routerów z segmentu dostawców usług internetowych.

Nazwa urządzenia:	Alcatel-Lucent 7750 Series	Cisco ASR-1000 Series	Juniper M Series
Firewall:	NAT, PAT (moduł MS-ISA), blokowanie ruchu przez ACL.	NAT, PAT, SPI, IPS, filtrowanie przesyłanych danych i szereg innych opcji (konieczne oprogramowanie CISCO Firewall).	NAT, PAT, SPI, IPS (wymagany moduł MS-PIC), zarządzanie ruchem z wykorzystaniem ACL.
Quality of Service:	Klasyfikowanie oraz oznaczanie pakietów z wykorzystaniem DSCP, zarządzanie zatorami (kolejkowanie, kształtowanie ruchu), unikanie zatorów (WRED), opcje QoS zależne od wykorzystywanych modułów.	Klasyfikowanie (np. NBAR) oraz oznaczanie pakietów z wykorzystaniem DSCP, zarządzanie zatorami (kolejkowanie, 128000 kolejek, kształtowanie ruchu), opcje zależne od modułu oraz wersji IOS), unikanie zatorów (WRED).	Klasyfikowanie oraz oznaczanie pakietów z wykorzystaniem DSCP, zarządzanie zatorami (kolejkowanie, kształtowanie ruchu), unikanie zatorów (WRED, RED).
Wirtualne sieci Prywatne:	IP VPN (oparte o protokół IPv6), IPSec VPN (konieczny dodatkowy moduł) 16000 tuneli na jeden moduł.	IPSec VPN liczba tuneli zależna od modułu, MPLS VPN, IP VPN (oparte o protokół IPv6).	MPLS VPN, IPv6 VPN, IPSec VPN (wymagane odpowiednie moduły).
Inne funkcje zarządzania ruchem:	Nadmiarowość bramy domyślnej (VRRP), routing statyczny, routing dynamiczny (RIP, OSPF IS-IS, BGP), MPLS oraz szereg opcji dodawanych przez dodatkowe moduły.	Nadmiarowość bramy domyślnej (HSRP, GLBP), routing statyczny, routing dynamiczny (RIP, OSPF, EIGRP, IS-IS, BGP), MPLS, DMZ.	Nadmiarowość bramy domyślnej (VRRP), routing statyczny, routing dynamiczny (RIP, OSPF IS-IS, BGP), MPLS.

Tab. 19. Wybrane przełączniki wielowarstwowe z segmentu ISP.

Nazwa urządzenia:	HP A12500 Series	Cisco Catalyst 6500 Series	Juniper EX8200 Series
Quality of Service:	Klasyfikacja pakietów w oparciu o informacje 2,3,4 warstwy ISO/OSI z wykorzystaniem ACL, wykorzystuje pola ToS, DSCP, CoS, zarządzanie zatorami (kolejkowanie, kształtowanie ruchu).	Ustawienia QoS dla portów, dla VLAN'ów, klasyfikacja w oparciu o informacje warstw 3 oraz 4, wykorzystuje pola ToS, DSCP, CoS zarządzania zatorami (kolejkowanie, kształtowanie ruchu), unikania zatorów WRED.	Klasyfikacja pakietów w oparciu o informacje 2,3,4 warstwy ISO/OSI, wykorzystuje pola ToS, DSCP, zarządzania zatorami (kolejkowanie 8 kolejek na port, kształtowanie ruchu), unikania zatorów WRED.
Trasowanie:	Routing statyczny, routing dynamiczny (RIP, OSPF, IS-IS i BGP), Policy-Based Routing	Routing statyczny, routing dynamiczny (RIP, OSPF, EIGRP, IS-IS i BGP).	Routing statyczny, routing dynamiczny (RIP, OSPF, IS-IS i BGP) (moduł XRE200).
Wirtualne sieci prywatne:	Obsługa MPLS VPN.	MPLS VPN, IPsec VPN (dodatkowy moduł).	MPLS VPN (dodatkowa licencja).
Inne funkcje zarządzania ruchem:	Protokół VRRP, sterowanie ruchem wykorzystując listy dostępu, ECMP – funkcja pozwalająca na wykorzystanie wielu tras o tym samym koszcie., MPLS TE.	Protokół HSRP, MPLS, MPLS-TE, wykrywanie anomalii w ruchu sieciowym (dodatkowy moduł), NAT, PAT (ACE Module).	Protokół VRRP, MPLS (dodatkowa licencja), filtrowanie ruchu z wykorzystaniem ACL.

6. Projekt sieci implementującej mechanizmy zarządzania ruchem pakietów w sieciach opartych na protokole IP

6.1. Założenia projektowe

Celem projektu jest zaprojektowanie oraz zbudowanie sieci komputerowej przedstawiającej funkcjonowanie mechanizmów umożliwiających administratorom na zarządzanie ruchem pakietów IP przez nią przesyłanych. Sieć taka powinna spełniać następujące założenia:

- Hierarchiczny model budowanej sieci;
- Podział projektowanej sieci na systemy autonomiczne;
- Implementacja protokołów trasowania dynamicznego w obrębie systemu autonomicznego (OSPF, RIPv2);
- Implementacja protokołów trasowania między systemami autonomicznymi (BGP);
- Implementacja protokołu MPLS oraz mechanizmu TE (ang. *Traffic Engineering*);
- Użycie w sieci mechanizmów umożliwiających sterowanie przepływającym ruchem HSRP, PBR (ang. *Policy Based Routin*), IPSec VPN (ang. *IPSec Virtual Private Network*).
- Uruchomienie w zbudowanej sieci usług takich jak WWW, FTP i innych.

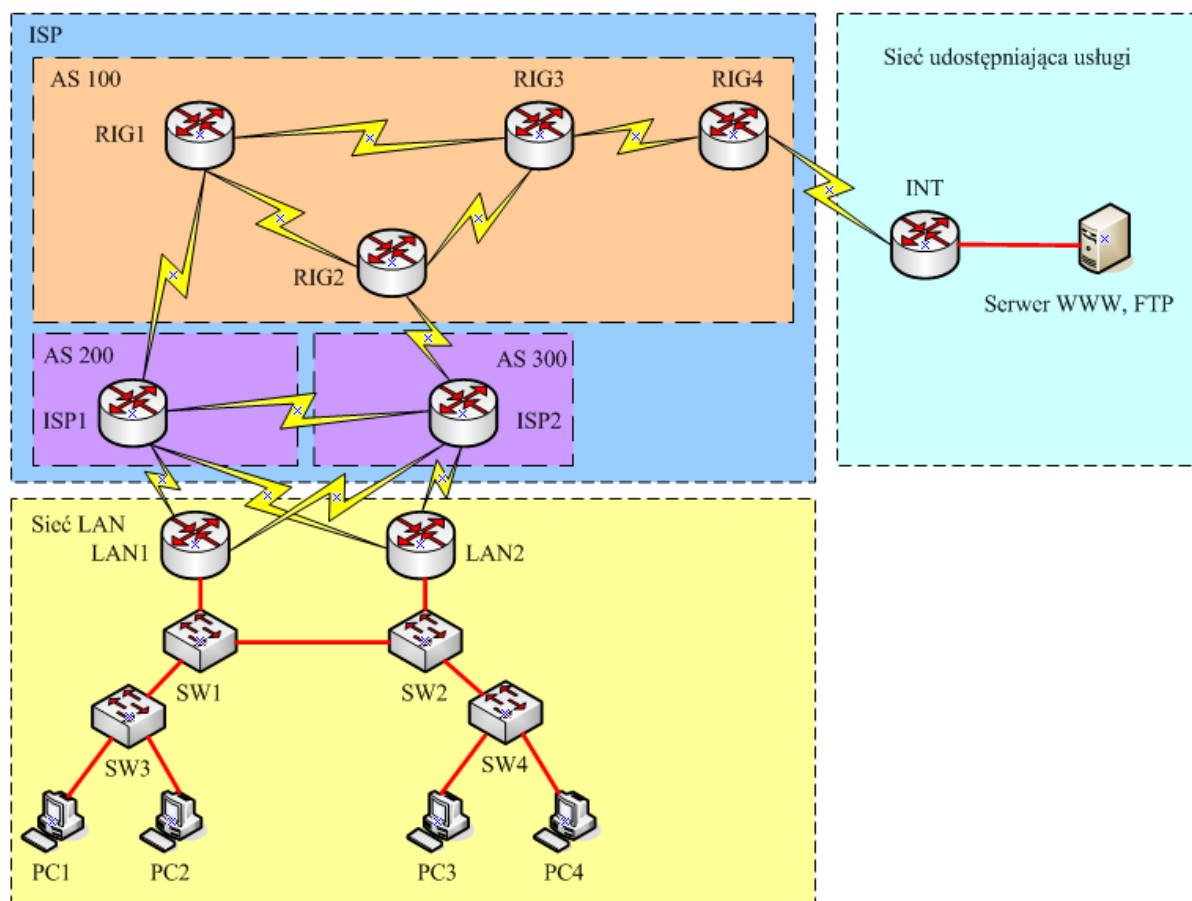
6.2. Opis realizowanych topologii

Największym problemem napotkanym podczas realizowania tego projektu jest rozmiar sieci koniecznej do przedstawienia pełni możliwości wykorzystywanych mechanizmów. Problem ten ograniczyłem realizując dwie oddzielne sieci implementujące różne mechanizmy sterowania ruchem, co pozwoliło na ich dokładniejsze przedstawienie.

Opis projektu pierwszej sieci

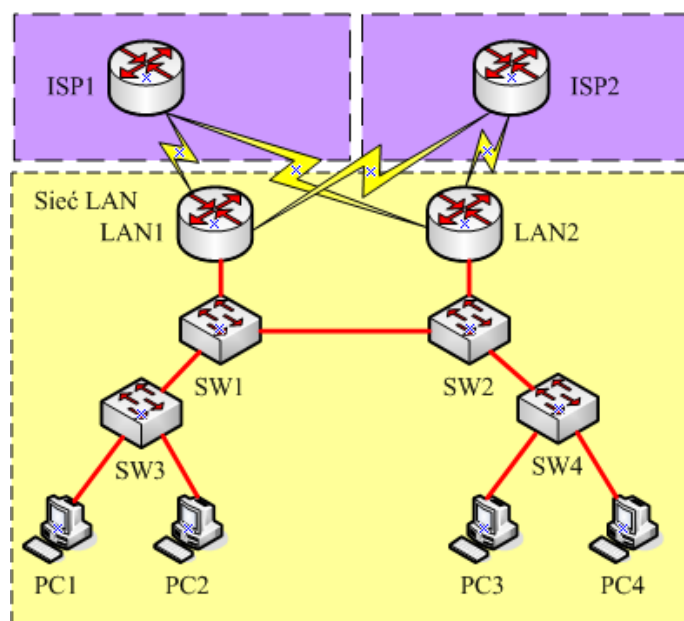
Topologię sieci przedstawia Rysunek 63, wyróżnić w niej można 3 główne elementy:

- Sieć LAN zapewniającą komunikację między jej użytkownikami oraz dostęp do sieci WAN;
- Sieć WAN zbudowaną z nadrzędnego usługodawcy usług internetowych oraz 2 podrzędnych ISP korzystających z jego usług;
- Sieć udostępniającą usługi WWW oraz FTP;



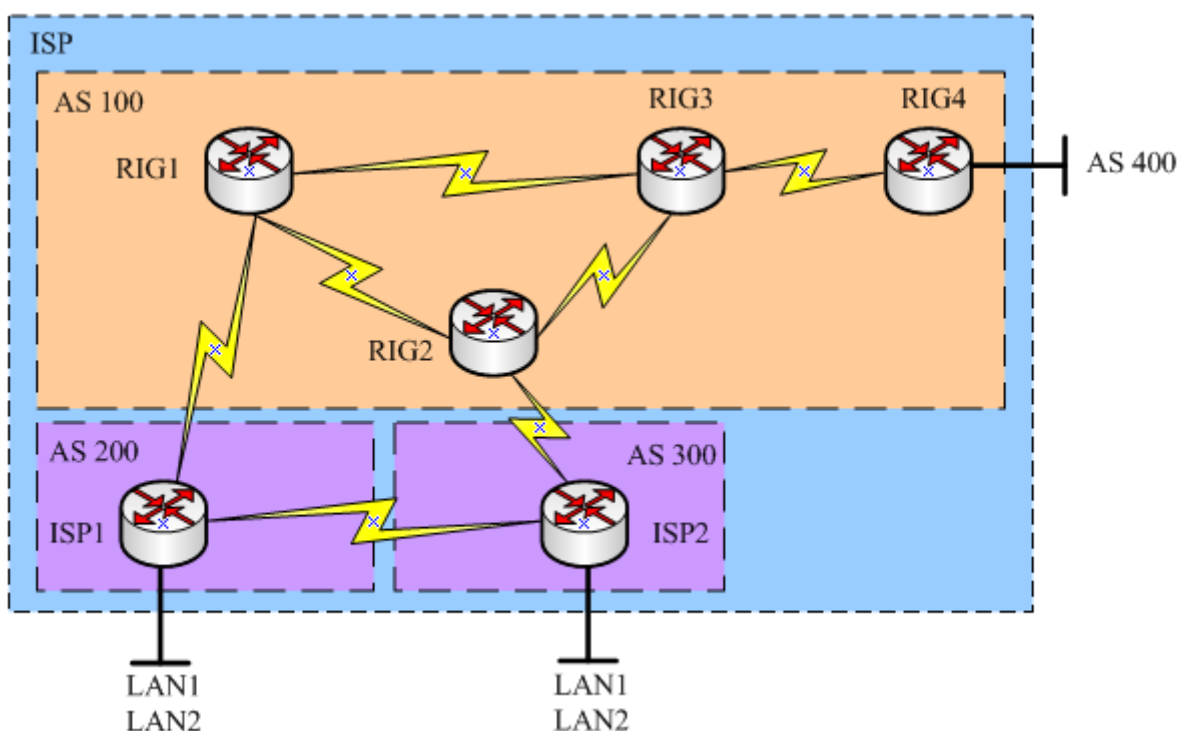
Rys. 63. Topologia pierwszej projektowanej sieci.

W sieci LAN (Rys. 64) skonfigurowane są wirtualne sieci lokalne (VLAN – ang. *Virtual Local Area Network*) zapewniające separację ruchu między różnymi sieciami bez konieczności stosowania dużej ilości urządzeń sieciowych.



Rys. 64. Sieć LAN pierwszej projektowanej sieci.

Sieć LAN zbudowana jest zgodnie z zasadami nadmiarowości umożliwiając jej pracę nawet podczas występowania awarii. Wykorzystane zostały dwa routery pełniące rolę bramy domyślnej pod kontrolą protokołu HSRP. Umożliwia on, w przypadku awarii routera pełniącego aktualnie rolę bramy domyślnej, przeniesienie jego funkcji na drugie urządzenie w grupie. W celu zabezpieczenia jak i rozdzielenia ruchu wychodzącego z sieci LAN wykorzystane zostały dwa łącza WAN. W trakcie normalnego funkcjonowania ruch transmitowany jest przez odpowiedniego providera zgodnie z politykami ustawionymi przez administratora na routerze, natomiast w razie awarii cały ruch kierowany jest przez łącze działające. Takie podejście umożliwia dostęp do sieci WAN nawet w wypadku awarii u któregoś z usługodawców.



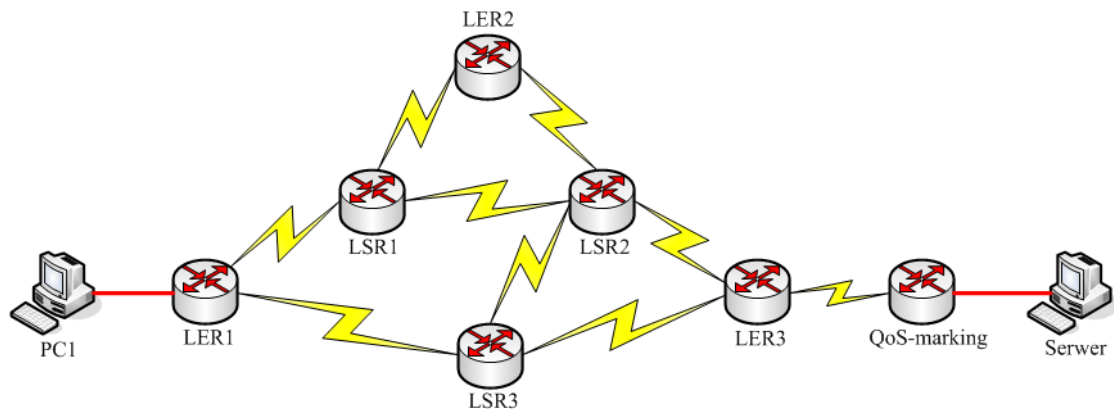
Rys. 65. Fragment pierwszej sieci obejmujący dostawców usług internetowych.

Drugim ważnym elementem realizowanej sieci jest sieć dostawców usług internetowych. Na Rysunku 65 przedstawiona jest sieć podzielona na 3 systemy autonomiczne, każdy z systemów odpowiada innemu operatorowi. Nadrzędny ISP oznaczony jako system autonomiczny 100 odpowiada za dostęp do sieci globalnej dwóm operatorom podrzędnym oznaczonym jako systemy autonomiczne 200 oraz 300, oni natomiast zapewniają dostęp do Internetu sieci LAN. W systemie autonomicznym 100 uruchomione zostały protokoły routingu dynamicznego bramy wewnętrznej OSPF oraz RIP, pomiędzy nimi występuje wymiana informacji o trasach. Natomiast między poszczególnymi systemami autonomicznymi w celu wymiany tras do sieci zewnętrznych działa protokół BGP.

Ostatnim elementem budowanego rozwiązania jest sieć oznaczona jako system autonomiczny o numerze 400. Router INT wymienia informacje o trasach z operatorem (AS 100) wykorzystując protokół BGP. Dodatkowo w celu bezpiecznej wymiany danych między siecią LAN a siecią za routerem INT utworzony został tunel VPN wykorzystując zestaw protokołów IPsec między routerem INT a routerem LAN2. Do routeru INT podłączony jest serwer udostępniający usługi WWW oraz FTP.

Opis projektu drugiej sieci

Druga sieć przedstawiona na Rysunku 66, podobnie jak pierwsza, składa się z 3 części: sieci LAN uzyskującej dostęp do serwera WWW oraz FTP z wykorzystaniem infrastruktury szkieletowej, serwera WWW i FTP oraz rdzenia sieci.



Rys. 66. Projekt drugiej sieci.

Głównym elementem tej sieci jest infrastruktura szkieletowa wykorzystująca do przesyłania danych między węzłami protokół MPLS. W tym celu w sieci uruchomiony jest protokół OSPF, aby routery miały aktualne informacje o stanach łącz. Kolejnym ważnym jej elementem jest router IP-QoS-Router, którego zadaniem jest odpowiednie oznaczanie pakietów z wykorzystaniem pola DSCP na podstawie polityk ustawionych przez administratora. Dzięki nim na wyjściu routera zapewniona jest odpowiednia ich obsługa. Poziom jakości usług zapewniany jest także w sieci szkieletowej. Pakiety trafiające do niej z routera IP-QoS-Router uzyskują odpowiednie ustawienia pola EXP na podstawie mapowań DSCP->EXP w routerze LER3. W kolejnych węzłach na podstawie tego pola pakiet jest odpowiednio traktowany. Wychodząc z sieci szkieletowej traci on ustawienia QoS przez oznaczenie pola DSCP jako 0. W realizowanej sieci wykorzystane zostały także elementy inżynierii ruchu dla MPLS (*MPLS-TE – ang. MPLS Traffic Engineering*), zapewniającej odpowiednie traktowanie określone przez operatora ruchu.

6.3. Adresacja urządzeń w sieci

Następnym etapem realizowanego projektu jest adresacja urządzeń końcowych pracujących w sieci oraz interfejsów routerów działających w sieci. Czynność tą rozpoczęto od przydzielenia odpowiednich adresów IP urządzeniom końcowym takim jak komputery oraz serwery; w następnej kolejności przydzielano adresy interfejsom routerów.

Adresacja w pierwszej realizowanej sieci komputerowej.

W sieci tej występuje 5 urządzeń końcowych 4 komputery klasy PC oznaczone odpowiednio PC1-PC4 oraz serwer usług WWW i FTP. Adresacja tych urządzeń przedstawiona jest w Tabeli 20:

Tab. 20. Adresacja urządzeń końcowych.

Oznaczenie urządzenia końcowego	Adres IP	Maska sieci	Brama domyślna
PC1	10.10.10.4	255.255.255.0	10.10.10.3
PC2	10.10.20.4	255.255.255.0	10.10.20.3
PC3	10.10.10.10	255.255.255.0	10.10.10.3
PC4	10.10.20.10	255.255.255.0	10.10.20.3
Serwer WWW i FTP	212.180.200.3	255.255.255.0	212.180.200.1

Następnie adresy IP przydzielane zostają interfejsom routerów nadrzędnego ISP oznaczonych odpowiednio RIG1-RIG4. Adresacja tych urządzeń znajduje się w Tabeli 21:

Tab. 21. Adresacja interfejsów urządzeń nadrzędnego ISP.

Oznaczenie urządzenia	Interfejs	Adres IP	Maska sieci
RIG1	Serial 0/0	170.200.101.2	255.255.255.252
	Serial 0/1	170.200.100.2	255.255.255.252
	Serial 0/2	200.200.100.1	255.255.255.252
	Loopback 0	192.168.1.1	255.255.255.255
RIG2	Serial 0/0	170.200.101.1	255.255.255.252
	Serial 0/1	170.200.102.2	255.255.255.252
	Serial 0/2	200.200.101.1	255.255.255.252
	Loopback 0	192.168.1.2	255.255.255.255

RIG3	Serial 0/0	170.200.103.2	255.255.255.252
	Serial 0/1	170.200.102.1	255.255.255.252
	Serial 0/2	170.200.100.1	255.255.255.252
	Loopback 0	192.168.1.4	255.255.255.255
RIG4	Serial 0/0	170.200.103.1	255.255.255.252
	Serial 0/1	200.200.104.1	255.255.255.252
	Loopback 0	192.168.1.3	255.255.255.255

W kolejnym etapie ustalana jest adresacja interfejsów routerów: ISP1 oraz ISP2 odpowiedzialnych za komunikację między siecią LAN a pozostałą częścią projektowanej sieci (Tab. 22).

Tab. 22. Adresacja interfejsów routerów ISP1 oraz ISP2.

Oznaczenie urządzenia	Interfejs	Adres IP	Maska sieci
ISP1	Serial 0/0	200.200.100.2	255.255.255.252
	Serial 0/1	200.200.102.1	255.255.255.252
	Serial 0/2	200.200.140.1	255.255.255.252
	Serial 0/3	200.200.140.5	255.255.255.252
ISP2	Serial 0/0	200.200.101.2	255.255.255.252
	Serial 0/1	200.200.102.2	255.255.255.252
	Serial 0/2	200.200.150.1	255.255.255.252
	Serial 0/3	200.200.150.5	255.255.255.252

Ostatnimi elementami wymagającymi przypisania adresów IP w pierwszej realizowanej sieci są interfejsy routerów LAN1, LAN2 oraz RD. Adresacja przedstawiona jest w Tabeli 23:

Tab. 23. Adresacja interfejsów routerów LAN1, LAN2 oraz RD.

Oznaczenie urządzenia	Interfejs	Adres IP	Maska sieci
LAN1	Serial 0/0	200.200.140.2	255.255.255.252
	Serial 0/1	200.200.150.6	255.255.255.252
	FastEthernet 0/0.10	10.10.10.1	255.255.255.0
	FastEthernet 0/0.20	10.10.20.1	255.255.255.0

LAN2	Serial 0/0	200.200.150.2	255.255.255.252
	Serial 0/1	200.200.140.6	255.255.255.252
	FastEthernet 0/0.10	10.10.10.2	255.255.255.0
	FastEthernet 0/0.20	10.10.20.2	255.255.255.0
INT	Serial 0/0	200.200.104.2	255.255.255.252
	Serial 0/1	212.180.200.1	255.255.255.0

Adresacja w drugiej realizowanej sieci komputerowej.

Projektowanie schematu adresacji w drugiej budowanej sieci komputerowej rozpoczyna się, podobnie jak w przypadku sieci pierwszej, od urządzeń końcowych (komputerów PC oraz Serwera WWW, FTP). Następnie ustalić należy adresy interfejsów routerów pracujących w sieci. Adresację urządzeń końcowych przedstawia Tabela 24:

Tab. 24. Adresacja urządzeń końcowych w drugiej sieci.

Oznaczenie urządzenia końcowego	Adres IP	Maska sieci	Brama domyślna
PC1	10.10.10.4	255.255.255.0	10.10.10.1
Serwer WWW, FTP	212.180.200.3	255.255.255.0	212.180.200.1

Natomiast w Tabeli 25 znajduje się adresacja dla interfejsów urządzeń pracujących w sieci.

Tab. 25. Adresacja interfejsów routerów pracujących w sieci.

Oznaczenie urządzenia	Interfejs	Adres IP	Maska sieci
LER1	Serial 0/0	200.200.100.1	255.255.255.252
	Serial 0/1	200.200.107.1	255.255.255.252
	FastEthernet 0/0	10.10.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.255
LER2	Serial 0/0	200.200.101.2	255.255.255.252
	Serial 0/1	200.200.102.1	255.255.255.252
	Loopback 0	10.10.1.2	255.255.255.255
LER3	Serial 0/0	200.200.105.1	255.255.255.252
	Serial 0/1	200.200.104.1	255.255.255.252
	Serial 0/2	200.200.108.2	255.255.255.252
	Loopback 0	10.10.1.6	255.255.255.255

LSR1	Serial 0/0	200.200.100.2	255.255.255.252
	Serial 0/1	200.200.101.1	255.255.255.252
	Serial 0/2	200.200.103.1	255.255.255.252
	Loopback 0	10.10.1.3	255.255.255.255
LSR2	Serial 0/0	200.200.102.2	255.255.255.252
	Serial 0/1	200.200.103.2	255.255.255.252
	Serial 0/2	200.200.106.1	255.255.255.252
	Serial 0/3	200.200.104.2	255.255.255.252
	Loopback 0	10.10.1.4	255.255.255.255
LSR3	Serial 0/0	200.200.107.2	255.255.255.252
	Serial 0/1	200.200.106.2	255.255.255.252
	Serial 0/2	200.200.105.2	255.255.255.252
	Loopback 0	10.10.1.5	255.255.255.255
QoS-marking	Serial 0/0	200.200.108.1	255.255.255.252
	FastEthernet 0/0	212.180.200.1	255.255.255.0

6.4. Konfiguracja urządzeń

Konfiguracja urządzeń w pierwszej realizowanej sieci

Etap ten rozpoczęto od podstawowych ustawień wszystkich routerów pracujących w sieci, czyli nazwę urządzenia oraz adresy IP zgodnie z tabelami 2, 3 oraz 4. Konfiguracja ta może zostać przeprowadzona korzystając z następujących komend:

```
Router>enable
Router#configure terminal
Router(config)#hostname RIG1
RIG1(config)#interface Serial 0/0
RIG1(config-if)#ip address 170.200.101.2 255.255.255.252
RIG1(config-if)#no shutdown
RIG1(config-if)#exit
RIG1(config)#interface Serial 0/1
RIG1(config-if)#ip address 170.200.100.2 255.255.255.252
RIG1(config-if)#no shutdown
RIG1(config-if)#exit
```

```
RIG1(config)#interface Serial 0/2
RIG1(config-if)#ip address 200.200.100.1 255.255.255.252
RIG1(config-if)#no shutdown
RIG1(config-if)#exit
```

Identycznie postąpić należy podczas konfiguracji pozostałych routerów w sieci z uwzględnieniem odpowiednich tabel. Dodatkowo wymagana jest konfiguracja interfejsu FastEthernet 0/0 na routerze INT oraz subinterfejsów w routerach LAN1 i LAN2 dla potrzeb sieci wirtualnych, polecenia do tego wymagane przedstawione są poniżej.

Konfiguracja interfejsu FastEthernet 0/0 na routerze INT:

```
INT(config)#interface FastEthernet 0/0
INT(config-if)#ip address 212.180.200.3 255.255.255.0
INT(config-if)#no shutdown
INT(config-if)#exit
```

Konfiguracja interfejsu FastEthernet 0/0 oraz subinterfejsów na routerze LAN1:

```
LAN1(config)#interface FastEthernet 0/0
LAN1(config-if)#no shutdown
LAN1(config-if)#exit
LAN1(config)#interface FastEthernet 0/0.10
LAN1(config-subif)encapsulation dot1Q 10
LAN1(config-subif)ip address 10.10.10.1 255.255.255.0
LAN1(config-subif)exit
LAN1(config)#interface FastEthernet 0/0.20
LAN1(config-subif)encapsulation dot1Q 20
LAN1(config-subif)ip address 10.10.10.1 255.255.255.0
LAN1(config-subif)exit
```

Konfiguracja analogiczna dla routera LAN2 zgodnie z Tabelą 23. Opis poleceń wykorzystanych podczas konfiguracji podstawowej znajduje się poniżej:

- enable – wejście w tryb uprzywilejowany;
- configure terminal – wejście w tryb konfiguracji globalnej;
- hostname – ustawienie nazwy urządzenia;
- interface <nazwa_int> <nr_int>/<nr_int>.<nr_subint> - wejście w tryb konfiguracji interfejsów oraz subinterfejsów;

- `ip address <IP> <maska>` - konfiguracja adresu IP oraz maski dla interfejsu;
- `no shutdown` – komenda pozwalająca na włączenie interfejsu;
- `encapsulation dot1Q <VLAN>` - uruchomienie enkapsulacji pakietów dla potrzeb obsługi sieci wirtualnych.

Kolejny etap konfigurowania urządzeń w pierwszej realizowanej sieci obejmuje ustawienie protokołów trasowania dynamicznego OSPF oraz RIP, aby umożliwić komunikację między urządzeniami RIG1-RIG4. Dodatkowo wymagana jest także możliwość redystrybucji tras uzyskanych z protokołu RIP do OSPF i w kierunku przeciwnym. Protokół OSPF odpowiada za wymianę trasa między routerami: RIG1, RIG2 i RIG3, natomiast protokół RIP między urządzeniami: RIG3 i RIG4. Poniżej przedstawione są przykładowe konfiguracje dla tych urządzeń.

Konfiguracja protokołu OSPF dla urządzeń RIG1 (analogicznie dla RIG2):

```
RIG1(config)#router ospf 1
RIG1(config-router)#network 170.200.100.0 0.0.0.3 area 0
RIG1(config-router)#network 170.200.101.0 0.0.0.3 area 0
RIG1(config-router)#passive-interface Serial 0/2
RIG1(config-router)#exit
```

Konfiguracja protokołu RIPv2 dla routera RIG4:

```
RIG4(config)#router rip
RIG4(config-router)#version 2
RIG4(config-router)#network 170.200.103.0
RIG4(config-router)#passive-interface Serial 0/1
RIG4(config-router)#exit
```

Konfiguracja protokołu RIPv2 oraz OSPF dla RIG3 przebiega podobnie jak przedstawiono powyżej z wyjątkiem jednej dodatkowej komendy:

```
RIG3(config)#router ospf 1
RIG3(config-router)#redistribute rip subnets
RIG3(config-router)#exit
RIG3(config)#router rip
RIG3(config-router)#redistribute ospf 1 metric 1
RIG3(config-router)#exit
```

Opis poleceń wykorzystanych do konfiguracji:

- `router ospf <numer_procesu>` - uruchamia proces protokołu OSPF;
- `network` – dodaje sieć której adres ma być rozsyłany w aktualizacjach;
- `passive-interface <interfejs>` - blokuje rozsyłanie aktualizacji na podany interfejs;
- `router rip` – uruchamia proces protokołu RIP;
- `version <1|2>` - ustala wersje uruchomionego protokołu RIP.

Następnie dla prawidłowego działania realizowanej sieci należy skonfigurować protokół BGP w celu wymiany informacji o trasach między routerami znajdującymi się w różnych systemach autonomicznych (eBGP) oraz routerami brzegowymi w obrębie jednego systemu autonomicznego (iBGP). W przypadku naszej sieci informacje o trasach zewnętrznych nie są redystrybuowane w obrębie AS100 przez protokoły IGP co wymusza zastosowanie modelu „full-mesh” iBGP aby prawidłowo funkcjonowało przesyłanie danych pomiędzy innymi systemami autonomicznymi wykorzystując AS100.

Konfiguracja protokołu BGP dla routera ISP1 (analogicznie dla ISP2 oraz INT):

```
ISP1(config)#router bgp 200
ISP1(config-router)#neighbor 200.200.100.1 remote-as 100
ISP1(config-router)#neighbor 200.200.102.2 remote-as 300
ISP1(config-router)#network 200.200.100.0 mask 255.255.255.252
ISP1(config-router)#network 200.200.102.0 mask 255.255.255.252
ISP1(config-router)#network 200.200.140.0 mask 255.255.255.252
ISP1(config-router)#network 200.200.140.4 mask 255.255.255.252
ISP1(config-router)#exit
```

Konfiguracja protokołu BGP dla routera RIG1 (analogicznie dla pozostałych urządzeń w AS100):

```
RIG1(config)#interface Loopback 0
RIG1(config)#ip address 192.168.1.1 255.255.255.255
RIG1(config)#exit
RIG1(config)#router ospf 1
RIG1(config-router)#network 192.168.1.1 0.0.0.0 area 0
RIG1(config-router)#exit
RIG1(config)#router bgp 100
RIG1(config-router)#neighbor 200.200.100.2 remote-as 200
```

```
RIG1(config-router)#neighbor 192.168.1.2 remote-as 100
RIG1(config-router)#neighbor 192.168.1.2 update-source
Loopback 0
RIG1(config-router)#neighbor 192.168.1.3 remote-as 100
RIG1(config-router)#neighbor 192.168.1.3 update-source
Loopback 0
RIG1(config-router)#neighbor 192.168.1.4 remote-as 100
RIG1(config-router)#neighbor 192.168.1.4 update-source
Loopback 0
RIG1(config-router)#exit
```

Jedyna różnica występuje w konfiguracji routera RIG4 gdzie zamiast OSPF działa RIPv2:

```
RIG4(config)#router rip
RIG4(config-router)#network 192.168.1.3 255.255.255.255
RIG4(config-router)#exit
```

Wszystkie routery w AS100 wymagają skonfigurowania adresu pętli zwrotnej oraz dodania go do aktualizacji rozsyłanych przez uruchomione protokoły trasowania dynamicznego bramy wewnętrznej. Pozwala to na utrzymanie sesji iBGP w przypadku, gdy jedno z połączeń między routerami sąsiadującymi ulegnie awarii. W takiej sytuacji zostanie wykorzystana inna ścieżka dostępna w danym momencie do zestawienia relacji sąsiedztwa.

Polecenia wykorzystane podczas konfiguracji routerów:

- `router bgp <nr_systemu_autonomicznego>` - uruchamia protokół trasowania BGP o ustalonym numerze systemu autonomicznego;
- `neighbor <adres_ip_sasiada> remote-as <nr_zdalnego_as>` - uruchamia wysyłanie pakietów Hello na podany adres w celu ustanowienia sesji BGP;
- `neighbor <adres_ip_sasiada> update-source <źródło>` - źródło aktualizacji dla danego sąsiada ustawione jest na wartość wpisaną w polu <źródło>;
- `network <adres_ip> mask <mask>` - określa sieci jakie mają być uwzględnione w aktualizacjach;

Ostatnim etapem konfiguracji urządzeń jest wprowadzenie ustawień w routerach sieci LAN oraz w systemie autonomicznym o numerze 400. Zgodnie z założeniami projektu w sieci

LAN skonfigurowana zostanie redundancją bramy domyślnej (protokół HSRP), obsługa nadmiarowych połączeń WAN, sterowanie ruchem przy pomocy map routingu (PBR) oraz tunel IPsec VPN między routerami LAN2 oraz INT.

W pierwszej kolejności konfigurujemy protokół HSRP zapewniający dostęp użytkownikom sieci do sieci globalnej. W konfiguracji uwzględniamy obecny stan połączeń WAN, w wyniku awarii któregoś z połączeń priorytet routera w grupie HSRP zmniejsza się; jeżeli w sieci istnieje router o wyższym priorytecie on zaczyna pełnić rolę bramy domyślnej.

W sytuacji, gdy awarii ulega ISP bramą domyślną pozostaje router o wyższym priorytecie (ponieważ w przypadku obydwu routerów następuje zmniejszenie priorytetu). Protokół HSRP tworzy wirtualną bramę domyślną, z której korzystają komputery w sieci, w wypadku realizowanej infrastruktury adresy te są następujące:

- VLAN 10 – wirtualna brama domyślna 10.10.10.3;
- VLAN 20 – wirtualna brama domyślna 10.10.20.3.

Konfiguracja HSRP na routerach poniżej:

```
LAN1(config)#interface FastEthernet 0/0.10
LAN1(config-if)#standby 1 ip 10.10.10.3
LAN1(config-if)#standby 1 preempt
LAN1(config-if)#standby 1 track Serial 0/0 20
LAN1(config-if)#standby 1 track Serial 0/1 20
LAN1(config-if)#exit
LAN1(config)#interface FastEthernet 0/0.20
LAN1(config-if)#standby 1 ip 10.10.20.3
LAN1(config-if)#standby 1 preempt
LAN1(config-if)#standby 1 track Serial 0/0 20
LAN1(config-if)#standby 1 track Serial 0/1 20
LAN1(config-if)#exit
```

Konfiguracja drugiego routera jest podobna z różnicą, iż należy dodatkowo zmienić priorytet routera korzystając z polecenia `standby 1 priority 110`.

Kolejnym krokiem w konfiguracji routerów LAN1 oraz LAN2 jest ustawienie mechanizmu NAT, aby użytkownicy w sieci LAN mieli dostęp do sieci zewnętrznej oraz ustawienia konieczne do prawidłowego funkcjonowania nadmiarowych połączeń WAN. ISP2 wybrany został jako główny operator i przez jego łącza domyślnie kierowany będzie ruch z sieci LAN. Drugie łącze w tym wypadku będzie pełniło funkcję łącza zapasowego i będzie uaktywniane

podczas awarii połączenia głównego lub gdy administrator skieruje ruch do niego z wykorzystaniem map trasowania. W tym celu ustawiono śledzenie dostępności połączenia głównego, wymagane polecenia konfiguracyjne przedstawione są poniżej.

```
LAN1(config)#track 3 rtr 1 reachability
LAN1(config-track)#exit
LAN1(config)#ip sla 1
LAN1(config-ip-sla)#icmp-echo 200.200.150.5 source-interface
Serial0/0
LAN1(config-ip-sla)#exit
LAN1(config)#ip sla schedule 1 life forever start-time now
```

Komenda `icmp-echo 200.200.150.5 source-interface Serial0/0` wymusza okresowe wysyłanie pakietu icmp-echo do portu zdalnego w przypadku routera LAN2 należy zmienić adres IP celu na 200.200.150.1.

Kolejne polecenia pokazują sposób konfiguracji tras domyślnych oraz mechanizmu NAT. W przypadku realizowanej sieci w tablicy trasowania na stałe znajduje się tylko jedna trasa domyślna, druga natomiast dodawana jest w wypadku uszkodzenia trasy domyślnej (istnieje możliwość współistnienia dwóch tras domyślnych w tablicy routingu co zapewniło by dzielenie obciążenia między dostępne trasy).

```
LAN1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0 10
LAN1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1 track 3
LAN1(config)#ip access-list standard 1
LAN1(config-std-nacl)#10 permit any
LAN1(config-std-nacl)#exit
LAN1(config)#route-map ISP1 permit 10
LAN1(config-route-map)#match ip address 1
LAN1(config-route-map)#match interface Serial0/0
LAN1(config-route-map)#exit
LAN1(config)#route-map ISP2 permit 10
LAN1(config-route-map)#match ip address 1
LAN1(config-route-map)#match interface Serial0/1
LAN1(config-route-map)#exit
LAN1(config)#ip nat inside source route-map ISP1 interface
```

```
Serial0/0 overload
LAN1(config)#ip nat inside source route-map ISP2 interface
Serial0/1 overload
LAN1(config)#interface Serial 0/0
LAN1(config-int)#nat outside
LAN1(config-int)#interface Serial 0/1
LAN1(config-int)#nat outside
LAN1(config-int)#interface FastEthernet0/0.10
LAN1(config-int)#nat inside
LAN1(config-int)#interface FastEthernet0/0.20
LAN1(config-int)#nat inside
LAN1(config-int)#exit
```

Konfiguracja translacji adresów z wykorzystaniem map trasowania pozwala na większą elastyczność i dokładne wydzielenie ruchu, który ma jej podlegać. Mapy routingu umożliwiają operatorom na zaawansowane sterowanie ruchem, np. przesyłanie określonego przez listę dostępu strumienia danych przez sprecyzowany punkt kolejnego skoku. Przykładowa konfiguracja zakładająca kierowanie całego ruchu z sieci 10.10.20.0 oraz ruchu http z sieci 10.10.10.0 przez ISP1 a resztę przez domyślne połączenie WAN (połączenie od ISP2), przedstawiona jest poniżej. Sterowanie ruchem przez określenie punktu kolejnego skoku stosując mapy routingu to PBR.

```
LAN1(config)#ip access-list extended RUCH_DO_ISP1
LAN1(config-ext-nacl)#permit tcp 10.10.10.0 0.0.0.255 any
eq www
LAN1(config-ext-nacl)#permit ip 10.10.20.0 0.0.0.255 any
LAN1(config-ext-nacl)#exit
LAN1(config)#route-map direct permit 9
LAN1(config-route-map)#match ip address RUCH_DO_ISP1
LAN1(config-route-map)#set ip next-hop 200.200.140.1
LAN1(config-route-map)#exit
LAN1(config)#interface FastEthernet0/0.10
LAN1(config-int)#ip policy route-map direct
LAN1(config-int)#exit
```

```
LAN1(config)#interface FastEthernet0/0.20
LAN1(config-int)#ip policy route-map direct
LAN1(config-int)#exit
```

Ostatnim punktem konfiguracji routerów w sieci LAN jest zrealizowanie połączenia VPN między routerem LAN2 i routerem INT. Pamiętać należy, że tunel ten działać będzie wyłącznie w przypadku, gdy router LAN2 jest w danej chwili urządzeniem aktywnym w grupie HSRP i on pełni funkcję bramy domyślnej.

```
LAN2(config)#crypto isakmp policy 5
LAN2(config-isakmp)#encryption 3des
LAN2(config-isakmp)#hash md5
LAN2(config-isakmp)#authentication pre-share
LAN2(config-isakmp)#group 2
LAN2(config-isakmp)#lifetime 28800
LAN2(config-isakmp)#exit
LAN2(config)#crypto isakmp key cisco123 address 200.200.104.2
LAN2(config)#crypto ipsec transform-set STRONG esp-3des esp-
sha-hmac
LAN2(config)#access-list 115 permit ip host 10.10.10.10 host
212.180.200.3
LAN2(config)#crypto map CISCO 10 ipsec-isakmp
LAN2(config-crypto-map)#set peer 200.200.104.2
LAN2(config-crypto-map)#set transform-set STRONG
LAN2(config-crypto-map)#set pfs group2
LAN2(config-crypto-map)#match address 115
LAN2(config-crypto-map)#exit
LAN2(config)#interface Serial 0/0
LAN2(config-int)#crypto map CISCO
LAN2(config-int)#exit
```

W celu poprawnego przepływu danych pomiędzy urządzeniem o adresie 10.10.10.10 a serwerem należy jeszcze wprowadzić dodatkową konfigurację: m.in. skierować ruch www przez interfejs Serial 0/0.

```
LAN2(config)# ip access-list extended 110
LAN2(config-ext-nacl)#permit ip host 10.10.10.10 host
212.180.200.3
LAN2(config-ext-nacl)#exit
LAN2(config)# route-map direct permit 8
LAN2(config-route-map)#match ip address 110
LAN2(config-route-map)#set interface Serial 0/0
LAN2(config-route-map)#exit
```

W następnej kolejności należy zapobiec translacji adresów w pakietach pochodzących z urządzenia o adresie 10.10.10.10. A także zapobiec przepływowi danych w postaci nie zaszyfrowanej przez router LAN1 w przypadku awarii urządzenia LAN2.

Ten wpis dotyczy urządzeń LAN1 oraz LAN2:

```
LAN2(config)#ip access-list standard 1
LAN2(config-std-nacl)#5 deny host 10.10.10.10
LAN2(config-std-nacl)#exit
```

Konfiguracja dodatkowa w urządzeniu LAN1:

```
LAN1(config)# ip access-list extended 110
LAN1(config-ext-nacl)#deny ip host 10.10.10.10 host
212.180.200.3
LAN1(config-ext-nacl)#permit ip any any
LAN1(config-ext-nacl)#exit
```

Utworzoną listę dostępu dodać należy do interfejsów Fa0/0.10 oraz Fa0/0.20

```
LAN1(config)#inteface FastEthernet0/0.10
LAN1(config-int)#ip access-group 110 in
LAN1(config-int)#exit
```

Opis poleceń wykorzystanych do konfiguracji routerów LAN1 oraz LAN2:

- `standby <nr_grupy_HSRP> ip <adres_IP>` - uruchamia protokół HSRP ustawia adres wirtualnej bramy domyślnej dla podanej grupy HSRP;
- `standby <nr_grupy_HSRP> preempt` – w przypadku gdy router ma wyższy priorytet staje się routerem aktywnym;
- `standby <nr_grupy_HSRP> priority` – ustawia priorytet routera;

- `standby <nr_grupy_HSRP> track <interfejs> <zmniejszenie_priorytetu>` - śledzenie czy interfejs jest włączony czy wyłączony; w przypadku gdy zostaje wyłączony, priorytet routera zmniejsza się o ustaloną wartość (domyślnie 10);
- `ip access-list <standard|extended> <numer ACL|nazwa>` - tworzy standardową lub rozszerzoną listę dostępu o podanym numerze lub nazwie;
- `access-list <numer ACL> ...` - podobnie jak wyżej, tyle że nie można użyć nazwy, jedynie numer;
- `route-map <nazwa> <permit|deny> <numer_wpisu>` - tworzy mapę trasowania o podanej nazwie;
 - `match ip address <ACL>` - określa dane, które mają podlegać mapie trasowania na podstawie ACL;
 - `match interface <interfejs>` - dane przeznaczone dla tego określenia mają podlegać mapie trasowania;
 - `set ip next-hop <adres_ip>` - ustala adres następnego skoku dla danych pasujących do mapy trasowania;

Ostatnim etapem jest skonfigurowanie routera INT tak, aby uzyskać dostęp do serwera podłączonego do tego routera. Należy także ustawić drugi koniec tunelu VPN.

```
INT(config)#crypto isakmp policy 5
INT(config-isakmp)#encryption 3des
INT(config-isakmp)#hash md5
INT(config-isakmp)#authentication pre-share
INT(config-isakmp)#group 2
INT(config-isakmp)#lifetime 28800
INT(config-isakmp)#exit
INT(config)#crypto isakmp key cisco123 address 200.200.150.2
INT(config)#crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
INT(config)#access-list 115 permit ip host 212.180.200.3 host 10.10.10.10
INT(config)#crypto map CISCO 10 ipsec-isakmp
INT(config-crypto-map)#set peer 200.200.150.2
INT(config-crypto-map)#set transform-set STRONG
```

```
INT(config-crypto-map)#set pfs group2
INT(config-crypto-map)#match address 115
INT(config-crypto-map)#exit
INT(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0
```

Konfiguracja w drugiej realizowanej sieci

Podobnie jak w przypadku pierwszej sieci konfigurację rozpoczęto od podstawowych ustawień wszystkich routerów pracujących w sieci. Ustawienia te obejmowały zmianę nazw urządzeń oraz ustawienie adresów IP wszystkich interfejsów.

```
Router>enable
Router#configure terminal
Router(config)#hostname LER1
LER1(config)#interface Serial 0/0
LER1(config-if)#ip address 200.200.100.1 255.255.255.252
LER1(config-if)#no shutdown
LER1(config-if)#exit
LER1(config)#interface Serial 0/1
LER1(config-if)#ip address 200.200.107.1 255.255.255.252
LER1(config-if)#no shutdown
LER1(config-if)#exit
LER1(config)#interface FastEthernet 0/0
LER1(config-if)#ip address 10.10.10.1 255.255.255.0
LER1(config-if)#no shutdown
LER1(config-if)#exit
```

Pozostałe urządzenia należy skonfigurować zgodnie z adresacją ustaloną w Tabeli 25. Kolejny krok obejmuje konfigurację interfejsów pętli zwrotnej wymaganego do prawidłowego funkcjonowania tuneli TE oraz protokołu trasowania dynamicznego opartego o mechanizm stanu łącza. Potrzebny on jest do prawidłowego funkcjonowania protokołu MPLS. W wypadku realizowanej sieci protokołem tym jest OSPF.

```
LER1(config)#interface Loopback 0
LER1(config-int)#ip address 10.10.1.1 255.255.255.0
LER1(config-int)#exit
LER1(config)#router ospf 1
LER1(config-router)#network 200.200.100.0 0.0.0.3 area 0
```

```
LER1(config-router)#network 200.200.107.0 0.0.0.3 area 0
LER1(config-router)#network 10.10.10.0 0.0.0.255 area 0
LER1(config-router)#network 10.10.1.1 0.0.0.0 area 0
LER1(config-router)#exit
```

Analogicznie konfiguracja przebiega na pozostałych routerach poza urządzeniem o nazwie QoS-marking. Drobne różnice występują także w routerze LER3 gdzie w celu dostępności sieci 212.1800.200.0 należy ustawić trasę domyślną i rozesłać ją do pozostałych urządzeń korzystając z protokołu OSPF.

```
LER3(config)#ip route 0.0.0.0 0.0.0.0 Serial0/2
LER3(config)#router ospf 1
LER3(config-router)#default-information originate
LER3(config-router)#exit
```

Jednym z wymagań dla drugiej realizowanej sieci jest zaimplementowanie protokołu MPLS w rdzeniu sieci i to kolejny etap jej ustawiania. Konfiguracji podlegają tylko urządzenia pracujące w szkieletcie mianowicie LER1-LER3 oraz LSR1-LSR3.

```
LER1(config)#ip cef
LER1(config)#interface Serial 0/0
LER1(config-int)#mpls ip
LER1(config-int)#mpls label protocol ldp
LER1(config-int)#exit
```

Identyczną konfigurację należy przeprowadzić na wszystkich interfejsach odpowiedzialnych za połączenia w sieci WAN. Po tym etapie konfiguracji protokół MPLS już działa. Kolejnym krokiem jest zestawienie tuneli TE pozwalających na przesyłanie danych zgodnie z parametrami jakie zażyczy sobie administrator.

Utworzone zostały 3 różne typy tuneli:

- 2 dynamiczne tunele TE; pierwszy podczas tworzenia bierze pod uwagę zarezerwowane pasmo, drugi metryki TE;
- Tunel statyczny – administrator ustala węzły tworzące tunel.

Metryki TE oraz wielkość pasma przeznaczonego do rezerwacji przedstawia Tabela 26 dla realizowanej sieci komputerowej.

Tab. 26. Wartości metryki TE oraz rezerwowanego pasma dla poszczególnych interfejsów..

Nazwa urządzenia	Interfejs	Metryka TE	Pasmo przeznaczone do rezerwacji (kbps)
LER1	Serial 0/0	10	1000
	Serial 0/1	40	500
LER2	Serial 0/0	15	1000
	Serial 0/1	15	1000
LER3	Serial 0/0	30	1000
	Serial 0/1	5	500
LSR1	Serial 0/0	10	1000
	Serial 0/1	15	1000
	Serial 0/2	5	500
LSR2	Serial 0/0	15	1000
	Serial 0/1	5	500
	Serial 0/2	5	1000
LSR3	Serial 0/0	40	500
	Serial 0/1	5	1000
	Serial 0/2	5	500

Następnie należy przeprowadzić konfigurację przy pomocy poniższych poleceń na wszystkich urządzeniach zgodnie z parametrami w Tabeli 26.

```
LER1(config)#interface Serial 0/0
LER1(config-int)#ip rsvp bandwidth 1000
LER1(config-int)#mpls traffic-eng administrative-weight 10
LER1(config-int)#exit
LER1(config)#interface Serial 0/1
LER1(config-int)#ip rsvp bandwidth 500
LER1(config-int)#mpls traffic-eng administrative-weight 40
LER1(config-int)#exit
```

Pamiętać należy także o włączeniu możliwości tworzenia tuneli na urządzeniach pracujących w sieci. Wszystkie routery i ich interfejsy konfigurowane są dokładnie w ten sam sposób.

```
LER1(config)#mpls traffic-eng tunnels
LER1(config)#interface Serial 0/0
LER1(config-int)#mpls traffic-eng tunnels
LER1(config-int)#exit
LER1(config)#interface Serial 0/1
LER1(config-int)#mpls traffic-eng tunnels
LER1(config-int)#exit
```

Poza obsługą tuneli TE należy wprowadzić także zmiany w konfiguracji protokołu trasowania stanu łącza, aby uaktywnić rozszerzenie TE do przenoszenia wszystkich danych wymaganych przez tunele.

```
LER1(config)#router ospf 1
LER1(config-router)#mpls traffic-eng router-id Loopback0
LER1(config-router)#mpls traffic-eng area 0
LER1(config-router)#exit
```

W pierwszej kolejności skonfigurowane zostały 2 tunele dynamiczne, których początkiem jest router LER1 a końcem LER3. Wymogiem pierwszego z nich jest możliwość zapewnienia pasma na poziomie 1000 kbps, drugi tunel natomiast zestawiany jest na podstawie metryk TE.

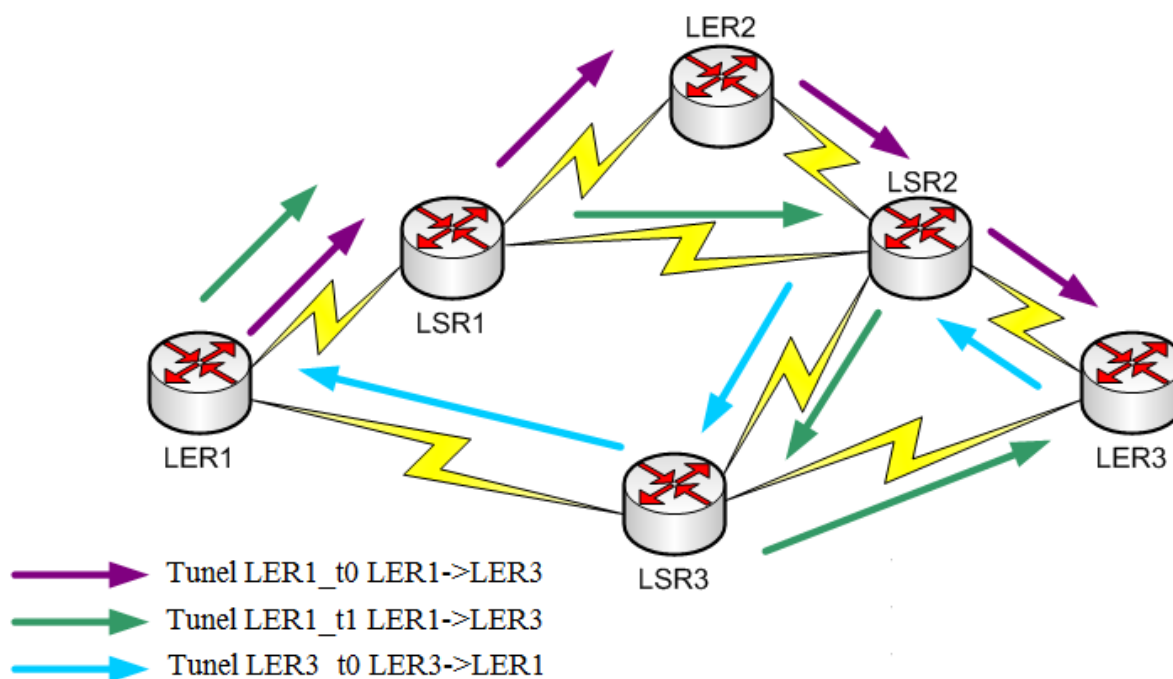
```
LER1(config)#interface Tunnel 0
LER1(config-int)#ip unnumbered Loopback0
LER1(config-int)#tunnel destination 10.10.1.6
LER1(config-int)#tunnel mode mpls traffic-eng
LER1(config-int)#tunnel mpls traffic-eng priority 1 1
LER1(config-int)#tunnel mpls traffic-eng bandwidth 1000
LER1(config-int)#tunnel mpls traffic-eng path-option 1 dynamic
LER1(config-int)#exit
LER1(config)#interface Tunnel 1
LER1(config-int)#ip unnumbered Loopback0
LER1(config-int)#tunnel destination 10.10.1.6
LER1(config-int)#tunnel mode mpls traffic-eng
LER1(config-int)#tunnel mpls traffic-eng priority 1 1
LER1(config-int)#tunnel mpls traffic-eng path-option 1 dynamic
```

```
LER1(config-int)#tunnel mpls traffic-eng path-selection metric  
te  
LER1(config-int)#exit
```

Ostatni tunel zestawiony został między routerami LER3 i LER1. Węzły, przez które kierowane są pakiety ustalane są przez administratora. W wypadku awarii któregoś z nich wykorzystywana jest funkcja dynamicznego tworzenia tunelu w oparciu o metryki protokołu trasowania bramy wewnętrznej.

```
LER3(config)#ip explicit-path  
LER3(cfg-ip-expl-path)#next-address 200.200.104.2  
LER3(cfg-ip-expl-path)#next-address 200.200.106.2  
LER3(cfg-ip-expl-path)#next-address 200.200.107.1  
LER3(cfg-ip-expl-path)#exit  
LER3(config)#interface Tunnel 0  
LER3(config-int)#ip unnumbered Loopback0  
LER3(config-int)#tunnel destination 10.10.1.1  
LER3(config-int)#tunnel mode mpls traffic-eng  
LER3(config-int)#tunnel mpls traffic-eng path-option 10  
explicit name trasa  
LER3(config-int)#tunnel mpls traffic-eng path-option 20  
dynamic  
LER3(config-int)#tunnel mpls traffic-eng path-selection metric  
igp  
LER3(config-int)#exit
```

Rysunek 67 przedstawia diagram sieci z zaznaczonymi trasami pakietów, które przemierzają określone tunele TE.



Rys. 67. Diagram przedstawiający trasę pakietów pokonującą utworzone tunele.

Ostatnim etapem konfiguracji jest skierowanie ruchu do utworzonych tuneli. Można zrobić to na kilka sposobów:

- Trasowanie statyczne - ręczne dodanie trasy korzystającej z tunelu do tablicy routingu;
- Trasowanie z wykorzystaniem polityk (PBR) – pozwala na elastyczne sterowanie ruchem, który ma trafić do określonego tunelu;
- Automatyczne rozgłaszanie tunelu z wykorzystaniem protokołów trasowania bramy wewnętrznej.

W przypadku realizowanej sieci wykorzystane zostały mapy trasowania do określenia strumieni danych, które mają zostać przesłane przez utworzone tunele LSP. Polecenia konfiguracyjne wykorzystane do tego celu umieszczone są poniżej.

```
LER1(config)# access-list 101 permit ip any host 212.180.200.1
LER1(config)# access-list 102 permit ip any host 212.180.200.3
LER1(config)# route-map pbr1 permit 10
LER1(config-route-map)# match ip address 101
LER1(config-route-map)# set interface Tunnel0
LER1(config-route-map)# exit
LER1(config)# route-map pbr1 permit 9
LER1(config-route-map)# match ip address 102
LER1(config-route-map)# set interface Tunnel1
LER1(config-route-map)# exit
LER1(config)# interface FastEthernet 0/0
LER1(config-int)# ip policy route-map pbr1
LER1(config-int)# exit

LER3(config)# access-list 101 permit ip any host 10.10.10.4
LER3(config)# access-list 101 permit ip any host 10.10.1.1
LER1(config)# route-map pbr1 permit 10
LER3(config-route-map)# match ip address 101
LER3(config-route-map)# set interface Tunnel0
LER3(config-route-map)# exit
LER3(config)# interface FastEthernet 0/0
LER3(config-int)# ip policy route-map pbr1
LER3(config-int)# exit
```

- `ip rsvp bandwidth` – włączenie protokołu RSVP, zadeklarowanie szerokości pasma, które może zostać zarezerwowane;
- `mpls traffic-eng administrative-weight` – ręczna zmianaa metryk TE;
- `mpls traffic-eng tunnels` – uruchamia obsługę inżynierii ruchu na routerze lub interfejsach;
- `mpls traffic-eng router-id <interfejs>` - określa identyfikator routera korzystającego z mechanizmu inżynierii ruchu;
- `mpls traffic-eng area <numer_obszaru>` - uruchamia mechanizmy MPLS TE dla obszaru OSPF o podanym numerze;

- `ip unnumbered` - przypisanie adresu określonego interfejsu do innego interfejsu;
- `tunnel destination <adres_IP>` - określa adres IP końca tunelu;
- `tunnel mode mpls traffic-eng` - ustawia tryb tunelu na tunel MPLS TE;
- `tunnel mpls traffic-eng priority` - ustawia priorytet dla tunelu;
- `tunnel mpls traffic-eng bandwidth <pasmo (kbps)>` - określa minimalną ilość pasma jaką protokół RSVP musi zarezerwować dla określonego tunelu
- `tunnel mpls traffic-eng path-option <priorytet> dynamic <dodatkowe_atrybuty>` - wymusza dynamiczne tworzenie trasy LSP. Do tunelu mogą zostać przydzielone priorytety oraz atrybuty;
- `tunnel mpls traffic-eng path-option <priorytet> explicit name <nazwa>` - tworzy trasę LSP na podstawie listy kolejnych węzłów o podanej nazwie;
- `tunnel mpls traffic-eng path-selection metric <metryka>` - określa na podstawie których metryk ma być wybierana ścieżka LSP;
- `ip explicit-path <nazwa>` - pozwala administratorowi na utworzenie listy o podanej nazwie zawierającej węzły, z których ma się składać ścieżka LSP;
- `next-address <adres_IP>` - określa adres IP kolejnego węzła na liście.

Kolejnym zadaniem postawionym przed drugą projektowaną siecią było zapewnienie jakości usług dla określonych strumieni danych, w tym celu zastosowany został model usług zróżnicowanych mechanizmu QoS. Rozwiązanie to jest obecnie najczęściej spotykane w sieciach komputerowych ze względu na swoją elastyczność, która osiągnięta jest przez zastosowanie mechanizmu obsługi pakietów zwanych PHB (ang. *Per-Hop Behaviour*) pozwalającego na autonomiczną obsługę pakietów w każdym węźle sieci.

Podczas konfiguracji sieci do prawidłowego spełniania przedstawionego zadania można wydzielić cztery etapy obejmujące:

- klasyfikowanie oraz oznaczanie pakietów wchodzących do sieci stosując pole DSCP. Ustalenie polityk dla sklasyfikowanych danych;
- mapowanie oznaczeń DSCP na odpowiadające pole EXP w sieci MPLS oraz ustawienia polityk do obsługi pakietów;
- ustawienie odpowiedniego traktowania pakietów w węzłach;
- zamiana oznaczeń MPLS na DSCP w miejscu usunięcia etykiet.

Konfiguracja mechanizmu QoS uwzględnia także fakt, że wartość pola DSCP nie zmienia się w sieci MPLS wraz ze zmianami pola EXP. Oznacza to, że informacje Diffserv tunelowane są przez rdzeń MPLS. Istnieją trzy modele tuneli, w realizowanej sieci skonfigurowany jest tunel typu „Pipe Model”. Pole EXP w etykiecie MPLS ustawianie jest zgodnie z ustawieniami administratora na wejściu do sieci MPLS, pole DSCP nie ulega zmianie. Na wyjściu z sieci MPLS do zapewnienia jakości usług brana jest także wartość pola EXP.

Zgodnie z przedstawionym podziałem konfigurację rozpoczynamy od klasyfikacji oraz oznaczania pakietów na wejściu do routera oraz ustawienie wstępnego traktowania ich na wyjściu z routera. Cała konfiguracja odbywa się na routerze QoS-marking, ponieważ jakość usług zapewniana ma być danym płynącym od serwera do PC1 (Rysunek 67). Klasyfikacja odbywa się z wykorzystaniem list dostępu.

```
IP-QoS-marking(config)#ip access-list extended Radio
IP-QoS-marking(config-ext-nacl)#permit tcp any eq 8000 any
IP-QoS-marking(config-ext-nacl)#permit tcp any eq 8888 any
IP-QoS-marking(config-ext-nacl)#exit
IP-QoS-marking(config)#ip access-list extended VOIP
IP-QoS-marking(config-ext-nacl)#tcp any range 16384 32768 any
IP-QoS-marking(config-ext-nacl)#permit icmp any host
10.10.10.3 echo
IP-QoS-marking(config-ext-nacl)#exit
IP-QoS-marking(config)#ip access-list extended ftp
IP-QoS-marking(config-ext-nacl)#permit tcp any eq ftp any
IP-QoS-marking(config-ext-nacl)#permit tcp any eq ftp-data any
IP-QoS-marking(config-ext-nacl)#permit tcp any range 2048 2148
any
IP-QoS-marking(config-ext-nacl)#exit
IP-QoS-marking(config)#ip access-list extended smtp
IP-QoS-marking(config-ext-nacl)#permit tcp any eq smtp any
IP-QoS-marking(config-ext-nacl)#exit
IP-QoS-marking(config)#ip access-list extended www
IP-QoS-marking(config-ext-nacl)# permit tcp any eq www any
IP-QoS-marking(config-ext-nacl)#exit
```

Następnie należy każdy ze sklasyfikowany strumieni przydzielić do odpowiedniej klasy i stosując Policy-map oznaczyć odpowiednio pakiety na interfejsie wejściowym routera.

```
IP-QoS-marking(config)#class-map match-all EF
IP-QoS-marking(config-cmap)#match access-group name VOIP
IP-QoS-marking(config-cmap)#exit
IP-QoS-marking(config)#class-map match-all AF21
IP-QoS-marking(config-cmap)#match access-group name ftp
IP-QoS-marking(config-cmap)#exit
IP-QoS-marking(config)#class-map match-all BF
IP-QoS-marking(config-cmap)#match access-group 101
IP-QoS-marking(config-cmap)#exit
IP-QoS-marking(config)#class-map match-all AF31
IP-QoS-marking(config-cmap)#match access-group name www
IP-QoS-marking(config-cmap)#exit
IP-QoS-marking(config)#class-map match-all AF11
IP-QoS-marking(config-cmap)#match access-group name Radio
IP-QoS-marking(config-cmap)#exit
IP-QoS-marking(config)# class-map match-all AF22
IP-QoS-marking(config-cmap)# match access-group name smtp
IP-QoS-marking(config-cmap)#exit
IP-QoS-marking(config)#policy-map SETDSCP
IP-QoS-marking(config-pmap)#class EF
IP-QoS-marking(config-pmap-c)#set dscp ef
IP-QoS-marking(config-pmap-c)#exit
IP-QoS-marking(config-pmap)#class AF11
IP-QoS-marking(config-pmap-c)#set dscp af11
IP-QoS-marking(config-pmap-c)#exit
IP-QoS-marking(config-pmap)#class AF21
IP-QoS-marking(config-pmap-c)#set dscp af21
IP-QoS-marking(config-pmap-c)#exit
IP-QoS-marking(config-pmap)#class AF22
IP-QoS-marking(config-pmap-c)#set dscp af22
IP-QoS-marking(config-pmap-c)#exit
IP-QoS-marking(config-pmap)#class AF31
```



```
IP-QoS-marking(config-pmap-c)#set dscp af31
IP-QoS-marking(config-pmap-c)#exit
IP-QoS-marking(config-pmap)#exit
```

W podobny sposób, jak w powyższym przykładzie, tworzy się klasy ruchu dla danych wychodzących (klasy tworzy się zgodnie z Tabelą 27), różnice natomiast występują podczas deklarowania polityki, ponieważ należy tam już ustawić parametry wymagane dla określonej klasy.

Tab. 27. Określenie klas ruchu dla pakietów wychodzących.

Klasa	Znacznik DSCP
Platinum	EF
Gold	AF11 AF12 AF13
Silver	AF21 AF22 AF23
Bronze	AF31 AF32 AF23

```
IP-QoS-marking(config)#policy-map RUCH
IP-QoS-marking(config-pmap)#class platinum
IP-QoS-marking(config-pmap-c)#priority 230
IP-QoS-marking(config-pmap)#class gold
IP-QoS-marking(config-pmap-c)#bandwidth percent 30
IP-QoS-marking(config-pmap-c)#random-detect
IP-QoS-marking(config-pmap-c)#shape average 512000
IP-QoS-marking(config-pmap-c)#class silver
IP-QoS-marking(config-pmap-c)#shape average 512000
IP-QoS-marking(config-pmap-c)#bandwidth percent 20
IP-QoS-marking(config-pmap-c)#random-detect
IP-QoS-marking(config-pmap-c)#class bronze
IP-QoS-marking(config-pmap-c)# bandwidth percent 10
IP-QoS-marking(config-pmap-c)# random-detect
IP-QoS-marking(config-pmap-c)# class BF
IP-QoS-marking(config-pmap-c)# police 56000 1750 1750 conform-
action set-dscp-transmit 0 exceed-action drop violate-action
drop
IP-QoS-marking(config-pmap-c)#exit
```

Po przygotowaniu polityk ruchu dla danych wchodzących i wychodzących należy dopisać je do odpowiednich interfejsów routera tak, aby pakiety były klasyfikowane, oznaczane oraz traktowane zgodnie z wymaganiami. Jako wejście danych traktowany jest port FastEthernet 0/0 routera, natomiast wyjściowy Serial 0/0.

```
IP-QoS-marking(config)#interface FastEthernet 0/0
IP-QoS-marking(config-int)#service-policy input SETDSCP
IP-QoS-marking(config-int)#exit
IP-QoS-marking(config)#interface Serial 0/0
IP-QoS-marking(config-int)#service-policy output RUCH
IP-QoS-marking(config-int)#exit
```

Dzięki takim ustawieniom pakiety wchodzące do sieci uzyskują oznaczenia DSCP i są traktowane zgodnie z ustawionymi przez administratora politykami (mają zapewnioną jakość usług na wymaganym dla nich poziomie).

W sieciach MPLS do oznaczania pakietów wykorzystywane jest odpowiednie pole zawarte w etykiecie zwane EXP. Wymagane jest więc odpowiednie rzutowanie wartości pola DSCP na pole EXP i takie zadanie wykonuje router LER3. Rzutowanie to odbywa się zgodnie z koncepcją podana w Tabeli 28.

Tab. 28. Mapowanie pola DSCP na EXP wraz z nazwami odpowiadających im klas.

DSCP	Klasa ruchu na wejściu	EXP	Klasa ruchu na wyjściu
EF	IP-EF	5	MPLS-EXP5
AF11 AF12 AF13	IP-AF1	4	MPLS-EXP4
AF21 AF22	IP-AF21-22	3	MPLS-EXP3
AF23	IP-AF23	2	MPLS-EXP2
AF31 AF32 AF33	IP-AF3	1	MPLS-EXP1
BE	IP-BE	0	MPLS-EXP0

Tworzenie klas dla ruchu wejściowego (analogicznie dla wszystkich pozycji w tabeli):

```
LER3(config)#class-map match-all IP-EF
LER3(config-cmap)#match dscp EF
```

Tworzenie klas dla ruchu wyjściowego (analogicznie dla wszystkich pozycji w tabeli):

```
LER3(config)#class-map match-all MPLS-EXP5
LER3(config-cmap)#match mpls experimental topmost 5
```

Polityka wejściowa o nazwie `traffic-in` tworzona jest w sposób podobny jak polityka `SETDSCP` na routerze `IP-QoS-marking`. Stosowane są następujące polecenia konfiguracyjne:

```
LER3(config)#policy-map traffic-in
LER3(config-pmap)#class IP-EF
LER3(config-pmap-c)#set mpls experimental imposition 5
```

Konfiguracje taką należy przeprowadzić dla każdej utworzonej klasy. Natomiast polityka dla ruchu wyjściowego o nazwie `traffic-out` tworzona jest tak samo jak w routerze `QoS-marking`. Parametry wymagane dla określonych klas ruchu przedstawione są w Tabeli 29.

Tab. 29. Parametry, które należy zapewnić danym wychodzącym.

Klasa	Opcje
MPLS-EXP5	priority 230
MPLS-EXP4	bandwidth percent 30 random-detect
MPLS-EXP3	bandwidth percent 15 random-detect
MPLS-EXP2	bandwidth percent 10 random-detect
MPLS-EXP1	bandwidth percent 5 random-detect

Pozostały ruch nie zawierający się w ustawionych politykach traktowany jest zgodnie z zasadą „best effort” i przesyłany jest dalej w miarę możliwości. Po zakończonej konfiguracji zasad należy je dodać jeszcze do interfejsów:

- polityka `traffic-in` dopisywana jest na wejściu interfejsu Serial 0/2 routera LER3;
- polityka `traffic-out` dopisywana jest na wyjściu interfejsu Serial 0/0 oraz Serial 0/1 routera LER3.

Kolejny etap obejmuje konfiguracje routerów LSR2 oraz LER2 (one odpowiedzialne są za przełączanie etykiet na trasie między urządzeniami LER3 oraz LER1). Podczas przełączania etykiet (czyli zamianie jednej na drugą) pole `EXP` ulega skopiowaniu ze starej etykiety do nowej, z tego względu należy jedynie skonfigurować obsługę pakietu na podstawie tego pola (nie ma konieczności ponownej klasyfikacji). Konfiguracja klas ruchu

oraz polityki ruchu dla danych wychodzących jest dokładnie taka sama jak w przypadku routera LER3. Zastosować można inne parametry obsługi pakietów zgodnie z zasadą mechanizmu PHB. Różnica dotyczy jedynie miejsca umieszczenia polityki ruchu, musi ona zostać dodana do wszystkich interfejsów (nie wiadomo jaką trasą przesłany zostanie pakiet). Istnieje także możliwość skonfigurowania oddzielnych polityk dla każdego istniejącego połączenia, ale w wypadku budowanej sieci wystarczy jedna.

Przedostatnim etapem konfiguracji QoS jest ustawienie routerów odpowiedzialnych za usuwanie etykiet na trasie LER3-LER1, są to urządzenia LSR1 i LSR3. Etykiety są usuwane na tych urządzeniach ze względu na działanie mechanizmu PHP (ang. *penultimate pop hopping*), czyli router LSR1 otrzyma już pakiet bez etykiety. Dla tunelu typu „Pipe Model” zakłada się obsługę pakietów na podstawie pola EXP, niestety jeżeli etykieta zostanie usunięta, pole to przestaje istnieć. W takim wypadku wykorzystana jest specjalna wartość qos-group do której zapisywane są, na wejściu do takiego routera, wartości pola EXP. Polecenia konfiguracyjne dla klas oraz polityki wejściowej znajdują się poniżej.

```
LSR1(config)# class-map match-all MPLS-EXP5
LSR1(config-cmap)# match mpls experimental topmost 5
LSR1(config)# class-map match-all MPLS-EXP4
LSR1(config-cmap)# match mpls experimental topmost 4
LSR1(config)# class-map match-all MPLS-EXP3
LSR1(config-cmap)# match mpls experimental topmost 3
LSR1(config)# class-map match-all MPLS-EXP2
LSR1(config-cmap)# match mpls experimental topmost 2
LSR1(config)# class-map match-all MPLS-EXP1
LSR1(config-cmap)# match mpls experimental topmost 1
```

Następnie skonfigurować należy politykę ruchu wejściowego na podstawie Tabeli 30. Poniżej wpis dla jednej klasy resztę konfiguruje się analogicznie.

```
LSR1(config)#policy-map traffic-in
LSR1(config-pmap)#class MPLS-EXP5
LSR1(config-pmap-c)#set qos-group 1
```

Tab. 30. Mapowanie pola EXP na wartości qos-group

Klasa ruchu	Ustawienia qos-group	Klasa wyjściowa
MPLS-EXP5	qos-group 1	IP-EF
MPLS-EXP4	qos-group 2	IP-AF1
MPLS-EXP3	qos-group 3 discard-class 2	IP-AF2
MPLS-EXP2	qos-group 3 discard-class 1	
MPLS-EXP1	qos-group 4	IP-AF3

Następnie należy skonfigurować przydzielanie pakietów do odpowiednich klas na interfejsie wyjściowym oraz przeprowadzić konfigurację polityki wyjściowej analogicznie jak w poprzednich przykładach zgodnie z parametrami przedstawionymi w Tabeli 31.

```
LSR1(config)# class-map match-all IP-AF1
LSR1(config-cmap)#match qos-group 2
```

Tab. 31. Poziom obsługi dla poszczególnych klas ruchu wyjściowego.

Klasa ruchu	Poziom obsługi
IP-EF	Priority 230
IP-AF1	bandwidth percent 30 random-detect
IP-AF2	bandwidth percent 25 random-detect discard-class-based
IP-AF3	bandwidth percent 5 random-detect

Na koniec dodać należy odpowiednie polityki do interfejsów routera:

- polityka ruchu wejściowego na interfejsach s0/1 oraz s0/2;
- polityka ruchu wyjściowego na interfejsie s0/0;

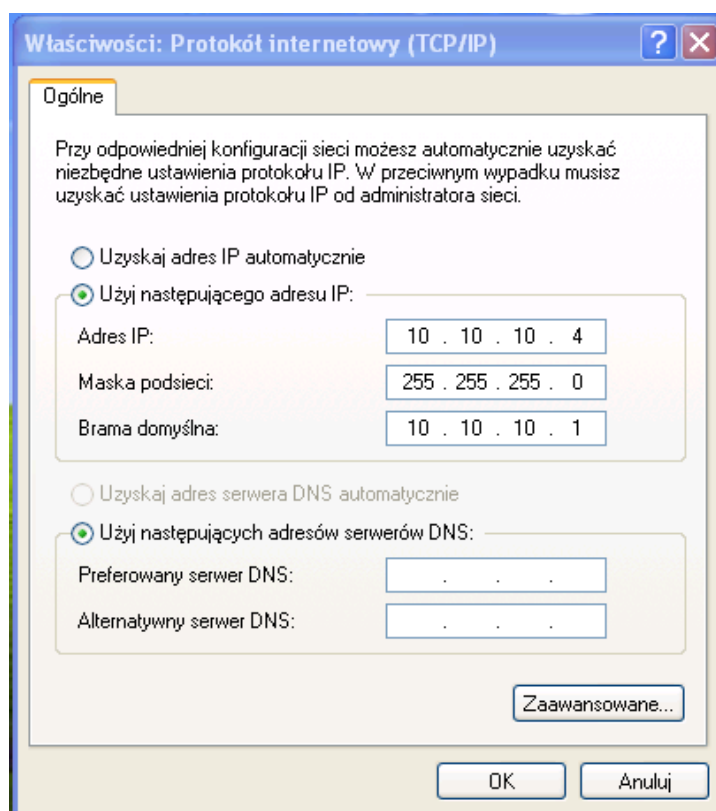
Ostatnim etapem konfiguracji w realizowanej sieci jest ustawianie routera LER1. Dostarczane tutaj pakiety nie posiadają już etykiety co oznacza, że widoczne jest w nim pole DSCP w nagłówku IP. Pole to podczas podróży w sieci MPLS nie zostało zmienione więc nie istnieje konieczność ponownej klasyfikacji oraz oznaczania pakietów. Należy jedynie podzielić pakiety na klasy ruchu wyjściowego i obsłużyć zgodnie z założeniami danej klasy.

Konfiguracja klas oraz polityki ruchu wyjściowego routera LER1 jest identyczna jak w przypadku routera QoS-marking, dlatego nie będą tu powtarzane polecenia konfiguracyjne.

Konfiguracja urządzeń końcowych

Ostatnim etapem konfiguracji urządzeń w przypadku obydwu sieci jest ustawienie adresów IP dla urządzeń końcowych. Serwery oraz część hostów działa pod kontrolą systemu Windows XP. Aby uzyskać dostęp do konfiguracji adresu IP w systemie Windows XP należy wykonać następujące akcje:

- Wybrać właściwości Mojego Otoczenia Sieciowego;
- Wybrać właściwości Połączenia lokalnego;
- W otwartym oknie wybrać Protokół internetowy (TCP/IP).
- W otwartym oknie wpisać wymagane dane (Rys. 68)



Rys. 68. Konfiguracja adresu IP w systemie Windows.

W systemie Linuks adres IP ustawiamy w trybie root'a korzystając z komendy:

```
ifconfig eth0 10.10.20.4 netmask 255.255.255.0  
ip route add default via 10.10.20.1
```

7. Wdrożenie oraz testy akceptacyjne zaprojektowanej sieci

7.1. Wdrożenie projektu

Do wykonania projektu wykorzystano środowisko symulacyjne GNS3 w wersji 0.7.4, pozwalające na wykorzystanie części routerów CISCO. GNS umożliwia także na korzystanie z systemu operacyjnego IOS, który używany jest w środowiskach rzeczywistych. Projektowana sieć zrealizowana została z wykorzystaniem urządzeń serii 3700 co wymuszone zostało małą ilością błędów w implementacji tych urządzeń w emulatorze. Wszystkie routery pracowały pod kontrolą IOS'a przeznaczonego dla Routera c3725 w wersji 1.24-17 advipservicesk9-mz pozwalającej na skonfigurowanie zaawansowanych usług IP oraz zaimplementowanie w sieci protokołu MPLS oraz IOS również dla tego routera w wersji 1.24-15.T12 advecurityk9-mz, na którym poprawnie działa mechanizm HSRP.

Każdy z routerów pracujących w sieci wyposażony został w karty rozszerzające WIC posiadające po 2 synchroniczne/asynchroniczne porty szeregowo umożliwiające łączenie urządzeń. Wszystkim urządzeniom przydzielono także 128 MB pamięci RAM i odpowiednie wartości Idle PC tak aby nie obciążały procesora w trakcie bezczynności.

Do budowy projektowanej sieci wykorzystane zostały przełączniki standardowe warstwy drugiej umożliwiające skonfigurowanie wirtualnych sieci prywatnych oraz portów trunk'owych z poziomu okien (bez korzystania z poleceń tekstowych).

Rolę urządzeń końcowych spełniały wirtualne maszyny pracujące pod kontrolą systemu Windows XP SP3 oraz Ubuntu w wersji 10.04 LTS. Do uruchomienia maszyn wirtualnych wykorzystane zostało oprogramowanie ORACLE VirtualBox 4.0.8.

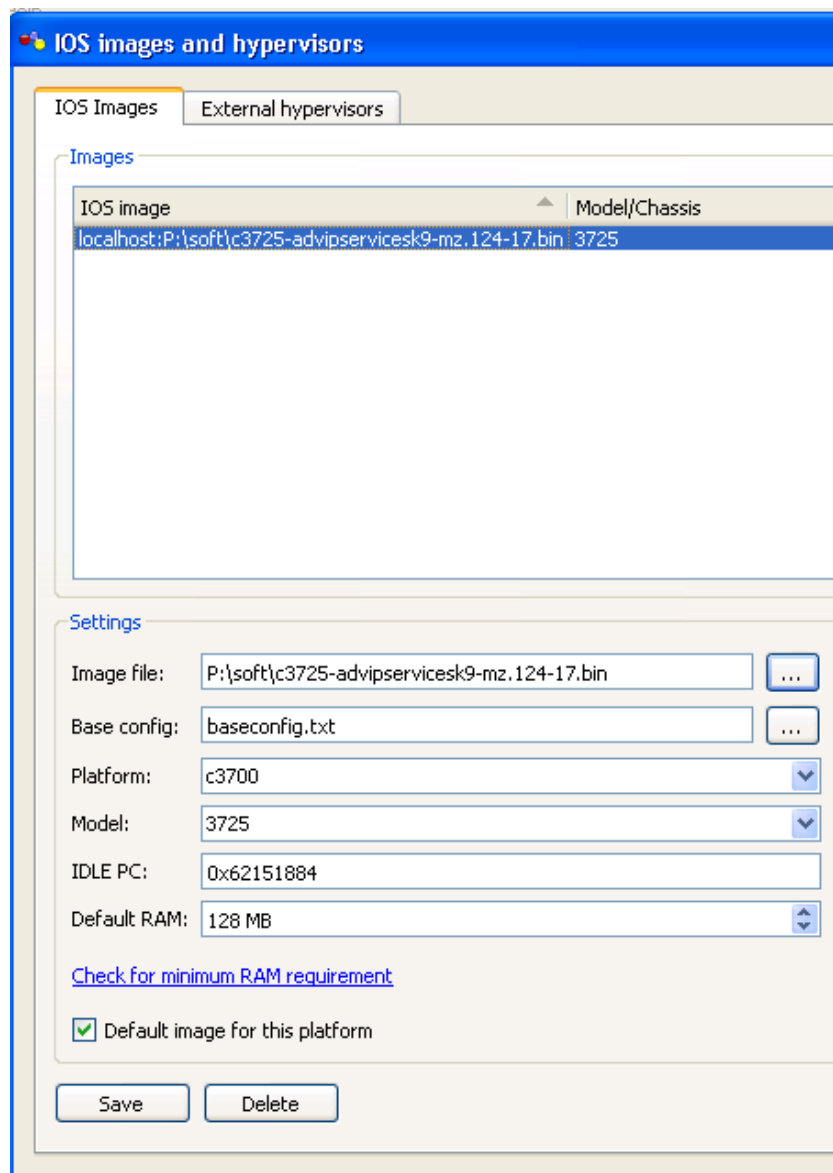
Całość uruchomiona została na komputerze stacjonarnym klasy PC wyposażonym w procesor dwurdzeniowy Core 2 Duo E4400 o częstotliwości rdzenia 2200 Mhz oraz 2 GB pamięci RAM. Konfiguracja taka umożliwiła mi uruchomienie bez problemów jednocześnie wszystkich urządzeń pracujących w realizowanych sieciach.

Podczas prac nad realizowaną siecią wykorzystano również oprogramowanie dodatkowe:

- IxChariot 6.70 – oprogramowanie symulacyjne pozwalające na podstawie określonych skryptów generować określony ruch między urządzeniami końcowymi;
- KrasnalServ – serwer WWW;
- CesarFTp – serwer FTP;
- DU Meter – oprogramowanie pozwalające na monitorowanie transferu.

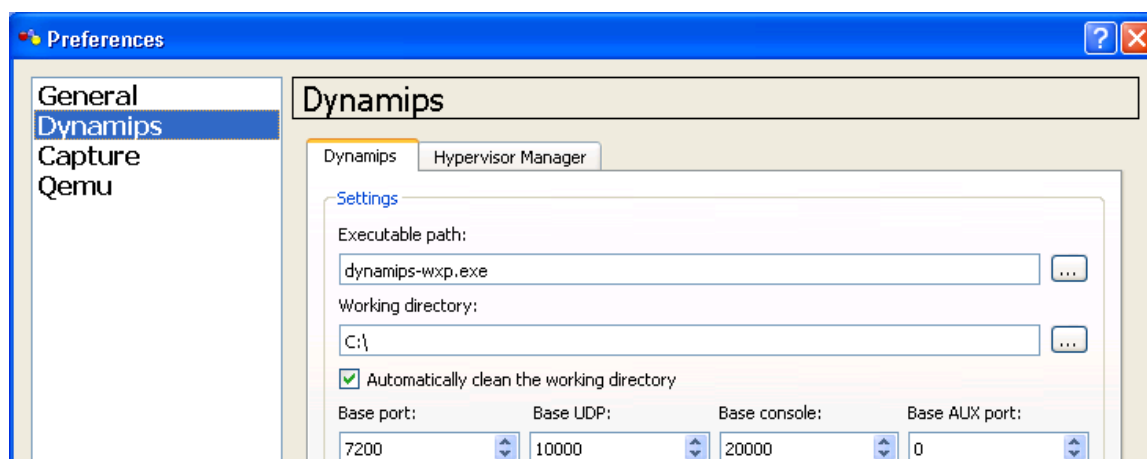
Konfiguracja GNS3 oraz routerów CISCO z serii 3725

Konfigurację GNS3 rozpocząć należy od dodania obrazów IOS, aby to zrobić wejść należy odpowiednio w Edit -> IOS Images and hypervisors. Pokaże nam się wtedy okno (Rysunek 69):



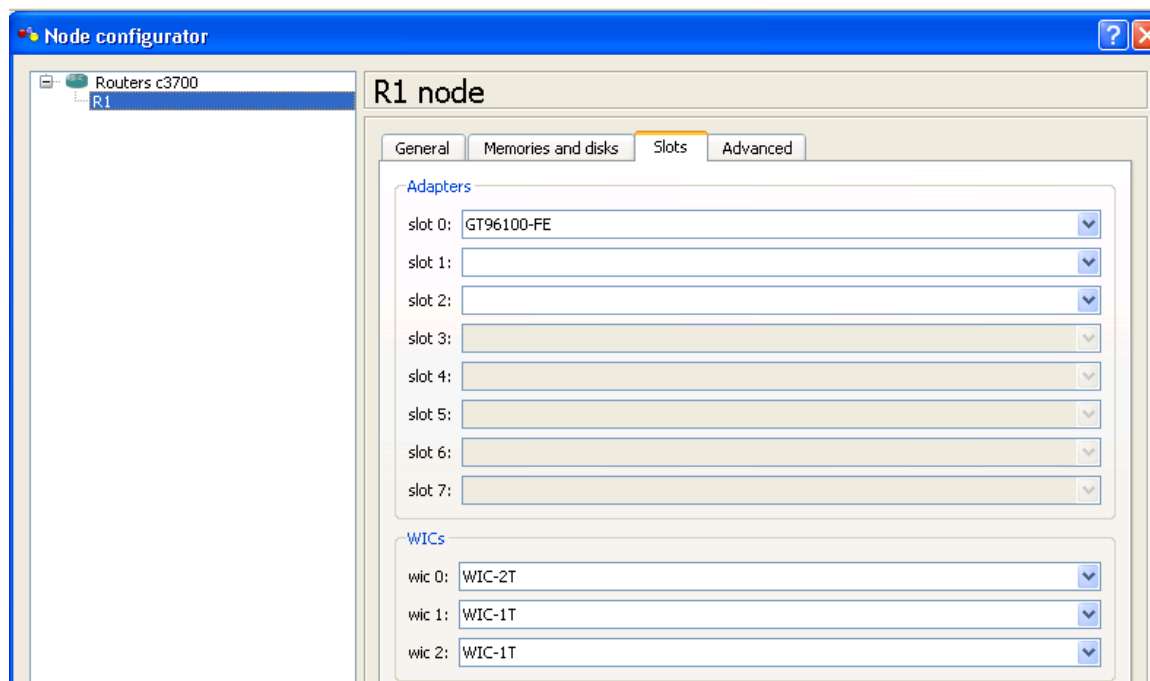
Rys. 69. Okno zarządzania obrazami IOS.

Obraz dodaje się przez wprowadzenie ścieżki w polu `Image file`, lub klikając na ikonę obok i wybierając plik z dysku. Należy również skonfigurować domyślną ilość pamięci RAM; w przypadku realizowanej sieci wynosi ona 128 MB. Następnie zmienić trzeba ustawienia zakresu portów wykorzystywanych do komunikacji z konsolą urządzeń (Rysunek 70) Edit -> Preferences zakładka Dynamips.



Rys. 70. Konfiguracja emulatora Dynamips.

Standardowe ustawienia przewidują porty od 2000 przy czym wielokrotnie zdarza się, że wykorzystywane są one w systemie, co powoduje problemy w komunikacji z urządzeniem, dlatego należy wartość `Base console` zmienić na 20000 unikając problemów. Ostatnim etapem jest tworzenie topologii w programie GNS3. Polega to na przeciągnięciu nazwy odpowiedniego modelu do środkowej części okna. Dla realizowanej sieci w routerach należy dodać dodatkowe porty Serial umożliwiając swobodne ich łączenie ze sobą. W tym celu należy prawym przyciskiem myszy kliknąć na router wybrać `Configure` i dostać się do zakładki `Slots` (Rysunek 71). Następnie w polach WIC wybrać odpowiednie rozszerzenie.



Rys. 71. Konfiguracja rozszerzeń w routerach.

W tak skonfigurowanym środowisku można budować realizowane sieci.

7.2. Testy akceptacyjne

Celem testów akceptacyjnych jest zbadanie poprawności działania wszystkich usług oraz protokołów działających w realizowanej sieci. Poprawne ich funkcjonowanie prowadzi do stwierdzenia, że sieć została zaprojektowana poprawnie oraz spełnia wszystkie postawione jej założenia.

7.2.1. Specyfikacja testów akceptacyjnych

Test protokołów trasowania bramy wewnętrznej – dotyczy obydwu realizowanych sieci komputerowych (OSPF, RIPv2 w pierwszej sieci, oraz OSPF w drugiej sieci). W pierwszej kolejności sprawdzić należy komunikację między routerami w stanie normalnego działania sieci a następnie w przypadku symulowanej awarii łącza między urządzeniami. Funkcjonowanie protokołów trasowania skontrolować można korzystając z polecenia `show ip route` przedstawiającego tablice routingu i oznaczenia z jakiego procesu pochodzą dane trasy co jednoznacznie potwierdzi działanie trasowania. Test protokołu OSPF polegać będzie także na wykazaniu sąsiedztwa między routerami korzystającymi z OSPF używając polecenia `show ip ospf neighbor`.

Test protokołu HSRP – test polegający na wykazaniu, iż w wyniku symulowanej awarii urządzenia pełniącego funkcję bramy domyślnej jego funkcje przejmie inne urządzenie w grupie. Dodatkowe testy wykazać mają, iż zmiana bramy domyślnej nastąpi także w wyniku awarii jednego z dostępnych połączeń WAN. Do przeprowadzenia tego testu użyte zostanie polecenie `traceroute (tracert)`.

Test protokołu BGP - podobnie jak w przypadku protokołów bramy wewnętrznej wykorzystać należy polecenie `show ip route` w warunkach normalnych oraz po symulowanej awarii (zmiany w tablicy routingu). Przeprowadzić należy także test komunikacji między urządzeniami znajdującymi się w dwóch różnych sieciach odległych wykorzystując polecenie `traceroute (tracert)`. Dodatkowo użyć należy poleceń diagnostycznych `show ip bgp Summary` oraz `show ip bgp neighbors`.

Test nadmiarowości łącz ISP – wykorzystując polecenie `tracert` skontrolować trasę pakietu przy symulowaniu awarii jednego z połączeń WAN. Test polegać będzie na wyłączeniu jednego z routerów (LAN1 lub LAN2), aby działanie mechanizmu HSRP nie przeszkodziło w testach. Domyślnie w przypadku awarii jednego dostawcy pakiet powinien zostać przesłany z wykorzystaniem innego łącza. Działanie nadmiarowości należy badać dla trzech różnych przypadków.

Test zarządzania ruchem z wykorzystanie map routingu (PBR) – przeprowadzony zostanie, podobnie jak pozostałe testy, z wykorzystaniem polecenia `tracert`. Dodatkowo możliwość sterowania ruchem w zależności od postawionych przez administratora wymagań wykaże korzystając z usług zawartych na serwerze. Przykładowy test będzie miał następujący przebieg: PC1 do serwera WWW łączyć będzie się z wykorzystaniem ISP1 natomiast do serwera FTP z wykorzystaniem ISP2.

Pozostałe testy dotyczyć będą wyłącznie drugiej realizowanej sieci i ich zadaniem będzie zweryfikowanie działania między innymi protokołu MPLS, tuneli LSP oraz oznaczania pakietów przez mechanizmy QoS.

Test protokołu MPLS oraz protokołu LDP - Test przeprowadzony będzie z wykorzystaniem narzędzi dostarczonych przez firmę CISCO w oprogramowaniu routera oraz dodatkowego oprogramowania dla systemu Ubuntu pod nazwą `paris-traceroute`, który oprócz standardowych informacji takich jak adres kolejnego skoku oraz opóźnienie wyświetla etykiety MPLS.

Narzędziami CISCO wykorzystanymi w teście będą:

- `show ip cef <adres_IP> detail` – testuje, czy przełączanie etykiet przez mechanizm CEF działa prawidłowo;
- `show mpls forwarding-table` – wyświetla odpowiednik tablicy routingu dla MPLS czyli tablicę LFIB);
- `show mpls ldp bindings <adres_IP>` - wyświetla powiązania etykiet do adresu docelowego;
- `show mpls ldp neighbor` – wyświetla informacje o routerach sąsiadujących w procesie LDP.

Test tuneli TE – Powinien zostać przeprowadzony z wykorzystaniem polecenia `tracert` (pozwoli pokazać jaką trasę pokonują pakiety w tunelu). Wykorzystane zostanie także polecenie udostępnione przez CISCO w systemie iOS – `show mpls traffic-te tunnels brief` – wyświetlające tunele przechodzące przez dany router oraz ich obecny stan. Kolejnym użytym poleceniem będzie `show mpls traffic-te tunnels Tunel <nr_Tunelu>` - szczegółowe informacje o tunelu.

Test ustawień mechanizmów QoS – ostatni test przeprowadzany w realizowanych sieciach komputerowych. Do wykonania pomiarów wykorzystane zostanie oprogramowanie IxChariot pozwalające na generowanie ruchu sieciowego. Dzięki skryptom, które można modyfikować program pozwala na symulacje praktycznie każdego typu danych, co idealnie

pasuje do testowania mechanizmów QoS. Wykorzystane zostaną także polecenia dostarczone przez CISCO w systemie operacyjnym routerów: `show policy-map interface <nr_interfejsu>` - pozwala na sprawdzenie, czy pakiety trafiają do odpowiednich klas w obrębie polityki dla danego interfejsu; drugim poleceniem wykorzystanym będzie `show ip access-list` - pokazuje, czy pakiety są poprawnie identyfikowane. Niestety, ze względu na środowisko emulowane nie mam możliwości zweryfikowania działania większości mechanizmów ograniczania pasma oraz działania kolejkowania, powodem jest obciążenie generowane podczas przesyłania danych i ograniczona do 80 kilobajtów/s prędkość (wahająca się w zależności od użycia CPU).

7.3. Wyniki testów akceptacyjnych.

7.3.1. Test protokołów trasowania bramy wewnętrznej

Testy rozpoczęto w pierwszej realizowanej sieci od kontroli funkcjonowania protokołu OSPF. W pierwszej kolejności wykonane zostało polecenie `show ip route` na routerze RIG3, którego efekt widoczny jest poniżej:

```
RIG3#sh ip route
...
Gateway of last resort is not set

    170.200.0.0/30 is subnetted, 4 subnets
C       170.200.102.0 is directly connected, Serial0/1
C       170.200.103.0 is directly connected, Serial0/0
C       170.200.100.0 is directly connected, Serial0/2
O       170.200.101.0 [110/128] via 170.200.102.2, 00:10:08, Serial0/1
        [110/128] via 170.200.100.2, 00:10:08, Serial0/2
    192.168.1.0/24 is variably subnetted, 4 `subnets, 2 masks
O       192.168.1.1/32 [110/65] via 170.200.100.2, 00:10:08, Serial0/2
R       192.168.1.0/24 [120/1] via 170.200.103.1, 00:00:13, Serial0/0
O       192.168.1.2/32 [110/65] via 170.200.102.2, 00:10:10, Serial0/1
C       192.168.1.4/32 is directly connected, Loopback0
```

Wszystkie trasy zdalne oznaczone literą O uzyskane zostały w wyniku wymiany informacji między routerami wykorzystującymi protokół OSPF. Kontrola protokołu OSPF polegać będzie na sprawdzeniu czy tablicach routingu routerów znajdują się wpisy dotyczące tras do sieci dostępnych za pośrednictwem innych routerów. Do tego testu wybrana została sieć 192.168.1.4/32 podłączona bezpośrednio do routera RIG3.

```
RIG2#show ip route
...
    192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
O       192.168.1.1/32 [110/65] via 170.200.101.2, 00:03:00, Serial0/0
O E2    192.168.1.0/24 [110/20] via 170.200.102.1, 00:03:02, Serial0/1
C       192.168.1.2/32 is directly connected, Loopback0
O       192.168.1.4/32 [110/65] via 170.200.102.1, 00:03:02, Serial0/1

RIG1#sh ip route
...
    192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.1/32 is directly connected, Loopback0
O E2    192.168.1.0/24 [110/20] via 170.200.100.1, 00:12:49, Serial0/1
O       192.168.1.2/32 [110/65] via 170.200.101.1, 00:12:49, Serial0/0
O       192.168.1.4/32 [110/65] via 170.200.100.1, 00:12:49, Serial0/1
```

W obu przypadkach trasa do sieci 192.168.1.4/32 znajduje się w tablicy trasowania i została uzyskana przez proces OSPF. Należy zauważyć, iż w przypadku normalnej pracy sieci

routerzy RIG1 oraz RIG2 korzystają z innego węzła w dotarciu do celu. Protokoły dynamiczne muszą także umożliwić aktualizację tablicy tras po zmianach w sieci. W trakcie testu zasymulować należy awarię połączenia między urządzeniami RIG1 oraz RIG3 a następnie wyświetlić tablice routingu w pierwszym urządzeniu.

```
RIG1#sh ip route
...
  192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C    192.168.1.1/32 is directly connected, Loopback0
O E2 192.168.1.0/24 [110/20] via 170.200.101.1, 00:00:04, Serial0/0
O    192.168.1.2/32 [110/65] via 170.200.101.1, 00:00:06, Serial0/0
O    192.168.1.4/32 [110/129] via 170.200.101.1, 00:00:06, Serial0/0
```

Zmianie uległa trasa dla badanej sieci; w sytuacji gdy niedostępny staje się adres IP 170.200.100.1 protokół OSPF wykorzystuje posiadane informacje i wstawia do tablicy tras nową ścieżkę do sieci 192.168.1.4.

Dodatkowym poleceniem weryfikującym działanie protokołu OSPF jest polecenie wyświetlające routery sąsiadujące i stan, w którym się znajdują.

```
RIG3#sh ip ospf neighbor

Neighbor ID  Pri  State  Dead Time  Address        Interface
192.168.1.2    0  FULL/-  00:00:36  170.200.102.2  Serial0/1
192.168.1.1    0  FULL/-  00:00:34  170.200.100.2  Serial0/2

RIG1#sh ip ospf neighbor

Neighbor ID  Pri  State  Dead Time  Address        Interface
192.168.1.2    0  FULL/-  00:00:34  170.200.101.1  Serial0/0
192.168.1.4    0  FULL/-  00:00:36  170.200.100.1  Serial0/1

RIG2#sh ip ospf neighbor

Neighbor ID  Pri  State  Dead Time  Address        Interface
192.168.1.4    0  FULL/-  00:00:30  170.200.102.1  Serial0/1
192.168.1.1    0  FULL/-  00:00:32  170.200.101.2  Serial0/0
```

W tablicach sąsiedztwa znajdują się wszystkie urządzenia, z którymi router ma ustanowione relacje. Stan FULL oznacza, że relacja sąsiedztwa jest ustanowiona i informacje o trasach zostały wymienione.

Test protokołu RIPv2 wyglądać będzie podobnie i wiąże się z wyświetleniem na urządzeniu RIG4 tablicy tras.

```
RIG4#sh ip route
...
 170.200.0.0/30 is subnetted, 4 subnets
R    170.200.102.0 [120/1] via 170.200.103.2, 00:00:07, Serial0/0
C    170.200.103.0 is directly connected, Serial0/0
R    170.200.100.0 [120/1] via 170.200.103.2, 00:00:07, Serial0/0
R    170.200.101.0 [120/1] via 170.200.103.2, 00:00:07, Serial0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.1.0/24 [120/1] via 170.200.103.2, 00:00:07, Serial0/0
C    192.168.1.3/32 is directly connected, Loopback0
```

Wszystkie trasy z oznaczeniem R zostały uzyskane przez router wykorzystując proces RIP co weryfikuje jego prawidłowe funkcjonowanie. Należy także skontrolować, czy wykorzystywana jest 2 wersja tego protokołu.

```
RIG4#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 13 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface          Send  Recv  Triggered RIP  Key-chain
    Serial0/0           2     2
    Loopback0           2     2
...
```

Ostatnim przeprowadzonym testem będzie zweryfikowanie komunikacji między urządzeniami. Do testu wykorzystane zostaną polecenia ping oraz traceroute między routerami RIG1 i RIG4 (z urządzenia RIG4 sprawdzać będziemy osiągalność sieci 192.168.1.1 podłączonej do RIG1). Test przeprowadzony zostanie podczas normalnego funkcjonowania sieci oraz symulowanej awarii łącza między urządzeniami RIG1 i RIG3.

```
RIG4#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/19/40
ms

RIG4#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

 0 170.200.103.2 16 msec 44 msec 8 msec
 1 170.200.100.2 8 msec * 52 msec
```

Wyniki tych samych operacji po wyłączeniu połączenia między RIG1 i RIG2.

```
RIG4#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/30/52
ms

RIG4#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

  0  170.200.103.2  36 msec  8 msec  4 msec
  1  170.200.102.2  12 msec  8 msec  8 msec
  2  170.200.101.2  24 msec *    40 msec
```

Wyniki powyższego testu pozwalają stwierdzić prawidłowe funkcjonowanie zarówno protokołu OSPF oraz RIPv2, ale także na prawidłową redystrybucję tras między tymi protokołami, co zapewnia poprawną komunikację. Na dostępność sieci nie wpłynęła także symulowana awaria łącza RIG1-RIG2, ponieważ dzięki działaniu protokołu trasowania pakiety wykorzystały inną trasę do celu. Niestety, w przypadku awarii łącza RIG3-RIG4 osiągalność routerów RIG1 i RIG2 z urządzenia RIG4 zostanie utracona, ponieważ brak jest połączenia zapasowego.

Wszystkie powyższe testy zweryfikowały prawidłowe funkcjonowanie protokołów trasowania bramy wewnętrznej w pierwszej budowanej sieci, czyli uzyskany został pożądany efekt.

Testy protokołu OSPF w drugiej realizowanej będą przebiegać identycznie jak w przypadku sieci pierwszej. Wstępnie wykorzystane zostanie polecenie `show ip route` wykonane na routerze LSR2, obecność tras otrzymanych z procesu OSPF będzie oznaczać prawidłowe działanie protokołu.

```
LSR2#show ip route
...
    200.200.102.0/30 is subnetted, 1 subnets
C       200.200.102.0 is directly connected, Serial0/0
    200.200.103.0/30 is subnetted, 1 subnets
C       200.200.103.0 is directly connected, Serial0/1
    200.200.100.0/30 is subnetted, 1 subnets
O       200.200.100.0 [110/100] via 200.200.103.1, 02:14:42,
Serial0/1
    200.200.101.0/30 is subnetted, 1 subnets
O       200.200.101.0 [110/100] via 200.200.103.1, 02:14:42,
Serial0/1
    200.200.106.0/30 is subnetted, 1 subnets
```



```
C      200.200.106.0 is directly connected, Serial0/2
      200.200.107.0/30 is subnetted, 1 subnets
O      200.200.107.0 [110/100] via 200.200.106.2, 02:14:44,
Serial0/2
      10.0.0.0/32 is subnetted, 6 subnets
O      10.10.1.1 [110/101] via 200.200.106.2, 02:14:45, Serial0/2
      [110/101] via 200.200.103.1, 02:14:45, Serial0/1
O      10.10.1.3 [110/51] via 200.200.103.1, 02:14:45, Serial0/1
O      10.10.1.2 [110/51] via 200.200.102.1, 02:14:45, Serial0/0
O      10.10.1.5 [110/51] via 200.200.106.2, 02:14:45, Serial0/2
C      10.10.1.4 is directly connected, Loopback0
O      10.10.1.6 [110/51] via 200.200.104.1, 02:14:45, Serial0/3
      200.200.104.0/30 is subnetted, 1 subnets
C      200.200.104.0 is directly connected, Serial0/3
      200.200.105.0/30 is subnetted, 1 subnets
O      200.200.105.0 [110/100] via 200.200.106.2, 02:14:45,
Serial0/2
      [110/100] via 200.200.104.1, 02:14:45,
Serial0/3
O      212.180.200.0/24 [110/110] via 200.200.106.2, 02:14:45,
Serial0/2
      [110/110] via 200.200.103.1, 02:14:45,
Serial0/1
O      200.200.108.0/24 [110/100] via 200.200.104.1, 02:14:45,
Serial0/3
O*E2 0.0.0.0/0 [110/1] via 200.200.104.1, 02:14:46, Serial0/3
```

Przedstawiona tablica tras posiada wszystkie trasy rozpowszechniane za pomocą OSPF co weryfikuje poprawne działanie protokołu routingu. Działanie przetestować można także korzystając z polecenia `show ip ospf neighbors` oraz `tracert` z komputera PC1 do serwera.

```
LER1#show ip ospf neighbor
Neighbor ID  Pri  State  Dead Time  Address      Interface
10.10.1.5    0   FULL/-  00:00:32   200.200.107.2  Serial0/1
10.10.1.3    0   FULL/-  00:00:36   200.200.100.2  Serial0/0

LSR2#show ip ospf neighbor
Neighbor ID  Pri  State  Dead Time  Address      Interface
10.10.1.5    0   FULL/-  00:00:34   200.200.106.2  Serial0/2
10.10.1.6    0   FULL/-  00:00:37   200.200.104.1  Serial0/3
10.10.1.3    0   FULL/-  00:00:30   200.200.103.1  Serial0/1
10.10.1.2    0   FULL/-  00:00:34   200.200.102.1  Serial0/0

C:\Documents and Settings\sk1>tracert 212.180.200.1
...
 1    33 ms    11 ms    26 ms    10.10.10.1
 2    92 ms    54 ms    16 ms    200.200.108.2
 3   192 ms   151 ms   120 ms    200.200.105.2
 4   325 ms   227 ms   110 ms    212.180.200.1
...
```

Routery LER1 oraz LSR2 posiadają sąsiadów OSPF i stan ustawiony jest na FULL co oznacza, że proces OSPF funkcjonuje prawidłowo i wszystkie informacje zostały wymienione. Dodatkowo polecenie tracert potwierdziło komunikację między hostem PC1 oraz serwerem. Sprawdzić należy także komunikację między PC1 a serwerem podczas symulowanej awarii połączenia LER3 ->LSR3. Wyniki poniżej.

```
C:\Documents and Settings\sk1>tracert 212.180.200.1
...
 1      17 ms      16 ms      14 ms    10.10.10.1
 2      48 ms      17 ms      15 ms    200.200.108.2
 3      65 ms      79 ms      89 ms    200.200.104.2
 4      71 ms      67 ms      73 ms    200.200.106.2
 5     135 ms      48 ms      37 ms    212.180.200.1
...
```

Efekty testów są zgodne z założeniami, dowodzą poprawności funkcjonowania protokołu OSPF w drugiej realizowanej sieci. Udowodniono także, że protokoły trasowania pozwalają na zachowanie komunikacji między odległymi hostami nawet w wypadku awarii pojedynczego połączenia (oczywiście w przypadku, gdy może zostać znaleziona trasa zapasowa), w takim przypadku pakiety są kierowane innymi trasami.

7.3.2. Test protokołu BGP

Działanie protokołu BGP opiera się na wymianie informacji między routerami, które mają ustanowione sąsiedztwo między sobą; z tego powodu początkowa weryfikacja oparta jest o polecenie `show ip bgp summary`, które wyświetla informacje o identyfikatorze routera, numerze systemu autonomicznego, wersji tablicy BGP, ilości dostępnych tras i inne. Polecenie to również pozwala na sprawdzenie ustanowionych połączeń między routerami BGP.

```
INT#show ip bgp summary
BGP router identifier 212.180.200.1, local AS number 400
BGP table version is 17, main routing table version 17
9 network entries using 1053 bytes of memory
9 path entries using 468 bytes of memory
6/5 BGP path/bestpath attribute entries using 744 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2337 total bytes of memory
BGP activity 11/2 prefixes, 11/2 paths, scan interval 60 secs

Neighbor      V  AS   MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
200.200.104.1  4  100    39      27     17    0    0  00:23:43      8
```

```
RIG4#show ip bgp summary
```

```
...
Neighbor      V  AS    MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.1.1    4  100      30      26      17    0     0 00:20:07         4
192.168.1.2    4  100      33      28      17    0     0 00:22:03         4
192.168.1.4    4  100      26      28      17    0     0 00:22:50         0
200.200.104.2  4  400      28      40      17    0     0 00:24:31         1
```

```
RIG3#show ip bgp summary
```

```
...
Neighbor      V  AS    MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.1.1    4  100      31      25      17    0     0 00:21:20         4
192.168.1.2    4  100      34      27      17    0     0 00:23:01         4
192.168.1.3    4  100      30      28      17    0     0 00:24:03         2
```

```
RIG2#show ip bgp summary
```

```
...
Neighbor      V  AS    MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.1.1    4  100      31      33      15    0     0 00:22:00         4
192.168.1.3    4  100      29      34      15    0     0 00:23:49         2
192.168.1.4    4  100      27      34      15    0     0 00:23:34         0
200.200.101.2  4  300      36      32      15    0     0 00:20:38         6
```

```
RIG1#show ip bgp summary
```

```
...
Neighbor      V  AS    MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.1.2    4  100      33      31      18    0     0 00:22:29         4
192.168.1.3    4  100      28      32      18    0     0 00:22:21         2
192.168.1.4    4  100      26      32      18    0     0 00:22:22         0
200.200.100.2  4  200      34      31      18    0     0 00:18:11         6
```

```
ISP2#show ip bgp summary
```

```
...
Neighbor      V  AS    MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
200.200.101.1  4  100      33      37      15    0     0 00:21:34         6
200.200.102.1  4  200      34      33      15    0     0 00:18:49         7
```

```
ISP1#show ip bgp summary
```

```
...
Neighbor      V  AS    MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
200.200.100.1  4  100      32      35      15    0     0 00:19:32         6
200.200.102.2  4  300      34      35      15    0     0 00:19:28         7
```

Kolejny sposobem weryfikacji jest wyświetlenie tablicy BGP oraz tablicy routingu. Dla przykładu przedstawione zostaną wyniki poleceń `show ip bgp` oraz `show ip route` na urządzeniu ISP1.

```
ISP1#show ip bgp
BGP table version is 15, local router ID is 200.200.140.5
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop        Metric LocPrf Weight Path
* 200.200.100.0/30        200.200.102.2          0           0 300 100 i
*                        200.200.100.1          0           0 100 i
*>                       0.0.0.0                0          32768 i
* 200.200.101.0/30        200.200.102.2          0           0 300 i
*>                       200.200.100.1          0           0 100 i
* 200.200.102.0/30        200.200.102.2          0           0 300 i
*>                       0.0.0.0                0          32768 i
* 200.200.104.0/30        200.200.102.2          0           0 300 100 i
*>                       200.200.100.1          0           0 100 i
*> 200.200.140.0/30        0.0.0.0                0          32768 i
*> 200.200.140.4/30        0.0.0.0                0          32768 i
* 200.200.150.0/30        200.200.100.1          0           0 100 300 i
*>                       200.200.102.2          0           0 300 i
* 200.200.150.4/30        200.200.100.1          0           0 100 300 i
*>                       200.200.102.2          0           0 300 i
* 212.180.200.0          200.200.102.2          0           0 300 100 400i
*>                       200.200.100.1          0           0 100 400 i

ISP1#show ip route
...
    200.200.140.0/30 is subnetted, 2 subnets
C      200.200.140.4 is directly connected, Serial0/3
C      200.200.140.0 is directly connected, Serial0/2
    200.200.102.0/30 is subnetted, 1 subnets
C      200.200.102.0 is directly connected, Serial0/1
    200.200.100.0/30 is subnetted, 1 subnets
C      200.200.100.0 is directly connected, Serial0/0
    200.200.101.0/30 is subnetted, 1 subnets
B      200.200.101.0 [20/0] via 200.200.100.1, 00:35:15
    200.200.104.0/30 is subnetted, 1 subnets
B      200.200.104.0 [20/0] via 200.200.100.1, 00:35:16
    200.200.150.0/30 is subnetted, 2 subnets
B      200.200.150.4 [20/0] via 200.200.102.2, 00:33:56
B      200.200.150.0 [20/0] via 200.200.102.2, 00:35:01
B      212.180.200.0/24 [20/0] via 200.200.100.1, 00:35:21
```

Wyniki przeprowadzonych testów prowadzą do wniosków, iż protokół BGP działa bez problemu. Zarówno tablica BGP jest uzupełniona w całości oraz najlepsze trasy z niej umieszczone zostały w tablicy trasowania routera ISP1. Na końcu należy jeszcze przetestować łączność między urządzeniami, w tym celu wykorzystane zostały polecenia ping oraz traceroute. Test przeprowadzony będzie między urządzeniem INT oraz interfejsem o adresie IP 200.200.150.2 routera LAN2.

```
INT>ping 200.200.150.2
...
Sending 5, 100-byte ICMP Echos to 200.200.150.2, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
40/80/108 ms

INT>tracert 200.200.150.2
...
 1 200.200.104.1 28 msec 12 msec 4 msec
 2 170.200.103.2 28 msec 12 msec 8 msec
 3 170.200.102.2 20 msec 16 msec 4 msec
 4 200.200.101.2 [AS 100] 36 msec 4 msec 24 msec
 5 200.200.150.2 [AS 300] 60 msec * 76 msec
```

Wyniki tych poleceń także wykazują działanie protokołu BGP. Dodatkowo polecenie `tracert` pokazuje, przez jakie systemy autonomiczne pakiet przechodzi. Prawidłowego działania protokołu routingu dowodzi powyższe polecenie po symulowanej awarii połączenia RIG2->ISP2 (wykorzystana została trasa zapasowa uzyskana z protokołu BGP).

```
INT>tracert 200.200.150.2
...
 1 200.200.104.1 64 msec 8 msec 8 msec
 2 170.200.103.2 4 msec 36 msec 28 msec
 3 170.200.100.2 16 msec 20 msec 16 msec
 4 200.200.100.2 [AS 100] 20 msec 16 msec 4 msec
 5 200.200.102.2 [AS 200] 36 msec 20 msec 16 msec
 6 200.200.150.2 [AS 300] 64 msec * 72 msec
```

7.3.3. Test nadmiarowości łącz ISP

Celem testu jest zweryfikowanie dostępu do serwera WWW (212.180.200.3) podczas normalnego funkcjonowania sieci oraz w przypadku awarii jednego z łącz WAN. Do testu wykorzystane zostaną narzędzia `ping` oraz `tracert`, a także po stronie serwera programu Wireshark przechwytyującego pakiety docierające do serwera. Logi z programu mają na celu pokazanie zmiany adresu hosta źródłowego. Pierwszy test przeprowadzony zostanie w sieci funkcjonującej normalnie bez awarii, w takim wypadku w logach programu Wireshark ujawnić powinien się adres źródła 200.200.150.2, następnie zasymulowana zostanie awaria routera ISP2. Tak działająca sieć ponownie poddana zostanie testowi i w tym wypadku adres źródła powinien być następujący 200.200.140.6. Testy przeprowadzane są z urządzenia końcowego PC1.

```
C:\Documents and Settings\sk1>ping 212.180.200.3 -n 7
```

Badanie 212.180.200.3 z użyciem 32 bajtów danych:

```
Odpowiedź z 212.180.200.3: bajtów=32 czas=141ms TTL=121
Odpowiedź z 212.180.200.3: bajtów=32 czas=80ms TTL=121
Odpowiedź z 212.180.200.3: bajtów=32 czas=58ms TTL=121
Odpowiedź z 212.180.200.3: bajtów=32 czas=51ms TTL=121
Odpowiedź z 212.180.200.3: bajtów=32 czas=48ms TTL=121
Odpowiedź z 212.180.200.3: bajtów=32 czas=78ms TTL=121
Odpowiedź z 212.180.200.3: bajtów=32 czas=49ms TTL=121
```

Statystyka badania ping dla 212.180.200.3:

```
Pakiety: Wysłane = 7, Odebrane = 7, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
Minimum = 48 ms, Maksimum = 141 ms, Czas średni = 72 ms
```

Rysunek 72 przedstawia fragment logu z programu Wireshark, wynika z niego, iż pakiety pochodzą z adresu 200.200.150.2 a nie z adresu hosta PC1 (10.10.10.4); dzieje się tak w wyniku działania translacji adresów na routerach LAN1 oraz LAN2.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request
3	0.960564	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request
5	1.941170	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request
7	2.948105	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request
9	3.958550	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request
11	4.993697	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request
13	5.982568	200.200.150.2	212.180.200.3	ICMP	74	Echo (ping) request

Rys. 72. Log z programu Wireshark.

Test z wykorzystaniem tracert również udowadnia, iż pakiety przesyłane są do celu z wykorzystaniem ISP2.

```
C:\Documents and Settings\sk1>tracert 212.180.200.3
```

Trasa śledzenia do 212.180.200.3 przewyższa maksymalną liczbę przeskoków 30

```
 1    94 ms    7 ms    10 ms    10.10.10.2
 2   107 ms   53 ms   21 ms   200.200.150.1
 3    75 ms   27 ms   20 ms   200.200.102.1
 4    83 ms   59 ms   55 ms   200.200.100.1
 5   104 ms   66 ms   22 ms   170.200.100.1
 6   107 ms   38 ms   30 ms   170.200.103.1
 7    87 ms   54 ms   35 ms   200.200.104.2
 8    81 ms   42 ms   32 ms   212.180.200.3
```

...

Następnie wyłączamy router ISP2 symulując jego awarię i ponawiamy wcześniej przeprowadzone testy.

```
C:\Documents and Settings\sk1>ping 212.180.200.3 -n 5

Badanie 212.180.200.3 z użyciem 32 bajtów danych:

Odpowiedź z 212.180.200.3: bajtów=32 czas=91ms TTL=122
Odpowiedź z 212.180.200.3: bajtów=32 czas=59ms TTL=122
Odpowiedź z 212.180.200.3: bajtów=32 czas=60ms TTL=122
Odpowiedź z 212.180.200.3: bajtów=32 czas=64ms TTL=122
Odpowiedź z 212.180.200.3: bajtów=32 czas=51ms TTL=122
...
```

Wyniki z programu Wireshark po symulowanej awarii przedstawia Rysunek 73.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.200.140.6	212.180.200.3	ICMP	74	Echo (ping) request
3	0.967778	200.200.140.6	212.180.200.3	ICMP	74	Echo (ping) request
5	1.962846	200.200.140.6	212.180.200.3	ICMP	74	Echo (ping) request
7	2.974730	200.200.140.6	212.180.200.3	ICMP	74	Echo (ping) request
9	3.973931	200.200.140.6	212.180.200.3	ICMP	74	Echo (ping) request

Rys. 73. Log z programu Wireshark po symulowanej awarii.

```
C:\Documents and Settings\sk1>tracert 212.180.200.3

...
 1    41 ms    17 ms    15 ms    10.10.10.2
 2   115 ms    31 ms     9 ms    200.200.140.5
 3    88 ms    29 ms    51 ms    200.200.100.1
 4    70 ms    45 ms    21 ms    170.200.100.1
 5   111 ms    49 ms    63 ms    170.200.103.1
 6   151 ms    48 ms    61 ms    200.200.104.2
 7    72 ms    58 ms    22 ms    212.180.200.3

Śledzenie zakończone.
```

Powyższe testy ukazują poprawne działanie łączy redundantnych podczas awarii. Pozwala to na zachowanie połączenia z siecią w przypadku awarii jednego z dostawców usług sieciowych. Test wznawiania ściągania pliku z serwera 212.180.200.3 nie powiódł się, ponieważ na routerach LAN1 oraz LAN2 funkcjonuje mechanizm translacji adresów.

Problemy pojawiły się także podczas wykonywania przedstawionych testów, gdyż po awarii urządzenia ISP2 należało poczekać na wyczyszczenie tablicy translacji i dopiero ponowić test.

7.3.4. Test protokołu HSRP

Podobnie jak test nadmiarowości ISP ten test polegać będzie na zweryfikowaniu możliwości komunikacji z serwerem o adresie 212.180.200.3 z urządzenia końcowego PC1. Konfiguracja mechanizmu HSRP powoduje, że routerem aktywnym w grupie jest router LAN2. Charakterystyka ustawień routerów w grupie wymusza konieczność przetestowania sieci w trzech następujących scenariuszach:

- Normalny stan pracy sieci; wszystkie urządzenia i połączenia działają;
- Awaria połączenia ISP1->LAN2;
- Awaria routera ISP1;

Do testów wykorzystałem polecenia `show standby brief`, `show track brief` oraz `tracert`.

Normalny stan pracy sieci

Podczas prawidłowego działania wszystkich elementów sieci routerem aktywnym w sieci LAN jest urządzenie opatrzone nazwą LAN2. Stan ten potwierdzają wyniki podanych powyżej poleceń.

```
LAN1#show standby brief
                P indicates configured to preempt.
                |
Interface    Grp  Pri P State    Active        Standby    Virtual IP
Fa0/0.10     1   100 P Standby  10.10.10.2    local      10.10.10.3
Fa0/0.20     1   100 P Standby  10.10.20.2    local      10.10.20.3

LAN2#show standby brief
                P indicates configured to preempt.
                |
Interface    Grp  Pri P State    Active        Standby    Virtual IP
Fa0/0.10     1   110 P Active   local         10.10.10.1  10.10.10.3
Fa0/0.20     1   110 P Active   local         10.10.20.1  10.10.20.3
```

Protokół HSRP funkcjonuje, brama domyślna jest osiągalna pod adresem bramy wirtualnej pod adresem IP 10.10.10.3 dla VLAN10 oraz 10.10.20.3 dla VLAN20. Router LAN2 jest routerem aktywnym natomiast LAN1 zapasowym. Protokół HSRP w obecnej konfiguracji uwzględnia także zmiany stanów łącz korzystając z mechanizmu śledzenia, które sprawdzić należy korzystając z `show track brief`.


```
LAN2#show track brief
      H indicates object created via HSRP.
      |
Track H Object          Parameter      Value Last Change
1     H interface      Serial0/0 line-protocol Up    00:27:39
2     H interface      Serial0/1 line-protocol Up    01:53:31
3     rtr               1          reachability Up    00:26:44
```

Podczas prawidłowego działania sieci parametry Value dla każdego wpisu powinny być ustawione na Up co świadczy o funkcjonowaniu wszystkich połączeń WAN. Wyniki polecenia jednoznacznie określają, że sieć pracuje bez żadnych problemów. Ostatecznie na potwierdzenie, że pakiety korzystają z router LAN2 (pierwszy skok przez adres 10.10.10.2) wykorzystujemy polecenie `tracert 212.180.200.3` na hoscie PC1.

```
C:\Documents and Settings\sk1>tracert 212.180.200.3
...
 1  131 ms    21 ms    10 ms    10.10.10.2
 2   78 ms    85 ms    31 ms    200.200.150.1
 3   78 ms    32 ms    16 ms    200.200.101.1
 4   84 ms    25 ms    20 ms    170.200.102.1
 5  133 ms    55 ms    36 ms    170.200.103.1
 6   96 ms    59 ms    60 ms    200.200.104.2
 7   74 ms    24 ms    40 ms    212.180.200.3
...
```

Awaria połączenia ISP1->LAN2

Podczas awarii łącza między urządzeniami ISP1->LAN1 priorytet routera LAN2 w grupie HSRP zgodnie z konfiguracją zostaje zmniejszony o 20 przez mechanizm śledzący i jest niższy niż priorytet routera LAN1.

```
LAN2#show track brief
      H indicates object created via HSRP.
      |
Track H Object          Parameter      Value Last Change
1     H interface      Serial0/0 line-protocol Up    00:32:01
2     H interface      Serial0/1 line-protocol Down  00:01:10
3     rtr               1          reachability Up    00:31:06
```

Przedstawione dane potwierdzają wykrycie awarii przez mechanizm śledzenia interfejsów. Następnie weryfikacji podlega zmiana routera aktywnego w grupie HSRP.

```
LAN2#show standby brief
      P indicates configured to preempt.
      |
Interface  Grp  Pri  P State  Active        Standby        Virtual IP
Fa0/0.10   1    90   P Standby 10.10.10.1 local         10.10.10.3
Fa0/0.20   1    90   P Standby 10.10.20.1 local         10.10.20.3
```

Wynik polecenia `show standby brief` wykazał, iż zmianie uległ router aktywny. W obecnej sytuacji rolę bramy domyślnej, z którą komunikują się urządzenia pracujące w VLAN10 oraz VLAN20 pełni urządzeni o adresie IP 10.10.10.1 i 10.10.20.1 czyli router LAN1. Potwierdza to także wynik polecenia `tracert` na hoście PC1.

```
C:\Documents and Settings\sk1>tracert 212.180.200.3
...
 1  104 ms    45 ms    17 ms   10.10.10.1
 2   98 ms    64 ms    46 ms   200.200.150.5
 3   79 ms    47 ms    34 ms   200.200.101.1
 4  101 ms    83 ms    55 ms   170.200.102.1
 5  102 ms    32 ms    18 ms   170.200.103.1
 6   96 ms   108 ms    81 ms   200.200.104.2
 7  116 ms    50 ms    63 ms   212.180.200.3

Śledzenie zakończone.
```

Awaria routera ISP1

Ostatni scenariusz zakłada awarię jednego z dostawców usług internetowych w naszym wypadku ISP1 (wyłączenie routera ISP1). Przeprowadzone testy są identyczne jak w przypadku dwóch poprzednich sytuacji.

```
LAN1#show track brief
      H indicates object created via HSRP.
      |
Track H Object          Parameter      Value Last Change
 1    H interface      Serial0/0 line-protocol Down  00:00:31
 2    H interface      Serial0/1 line-protocol Up    00:21:38
 3      rtr             1      reachability Up    00:20:35

LAN2#show track brief
      H indicates object created via HSRP.
      |
Track H Object          Parameter      Value Last Change
 1    H interface      Serial0/0 line-protocol Up    00:40:36
 2    H interface      Serial0/1 line-protocol Down  00:09:46
 3      rtr             1      reachability Up    00:39:42
```

Po wykonaniu polecenia `show track brief` uzyskano potwierdzenie awarii routera ISP1, następnie zweryfikować należy, który router jest aktywny w grupie HSRP.

```
LAN2#show standby brief
      P indicates configured to preempt.
      |
Interface Grp Pri P State Active Standby Virtual IP
Fa0/0.10  1  90 P Active local 10.10.10.1 10.10.10.3
Fa0/0.20  1  90 P Active local 10.10.20.1 10.10.20.3
```

Zgodnie z konfiguracją routerem aktywnym bez zmian pozostaje urządzenie o nazwie LAN2 i ono pełni rolę bramy domyślnej w sieci LAN. Potwierdza to wynik komendy `tracert` na komputerze PC1.

```
C:\Documents and Settings\sk1>tracert 212.180.200.3
```

```
...
```

1	78 ms	16 ms	21 ms	10.10.10.2
2	71 ms	60 ms	48 ms	200.200.150.1
3	113 ms	65 ms	31 ms	200.200.101.1
4	109 ms	35 ms	69 ms	170.200.102.1
5	114 ms	54 ms	35 ms	170.200.103.1
6	102 ms	55 ms	55 ms	200.200.104.2
7	87 ms	64 ms	32 ms	212.180.200.3

```
Śledzenie zakończone.
```

Wyniki wszystkich testów wykazują prawidłowe działanie mechanizmu HSRP. W wyniku awarii łącza, dostawcy usług internetowych czy nawet jednego z routerów grupy HSRP, sieć wewnętrzna bez problemów może komunikować się z siecią zewnętrzną. Niestety, w przypadku testów protokołu HSRP, podobnie jak w trakcie testów redundantnych połączeń WAN, nie powiodło się wznowienie pobierania pliku z serwera HTTP czy to FTP. Przyczyną, podobnie jak w pierwszym wypadku, był mechanizm translacji adresów i sposób dostępu sieci wewnętrznej do sieci zewnętrznej.

7.3.5. Test funkcjonowania tunelu IPsec VPN

Testy rozpocząć należy od zweryfikowania poprawności konfiguracji, czyli sprawdzić należy czy podczas połączenia z hosta 10.10.10.10 do serwera nastąpiło utworzenie tunelu.

Wykorzystane zostaną polecenia `show crypto ipsec sa` oraz `show crypto isakmp sa`.

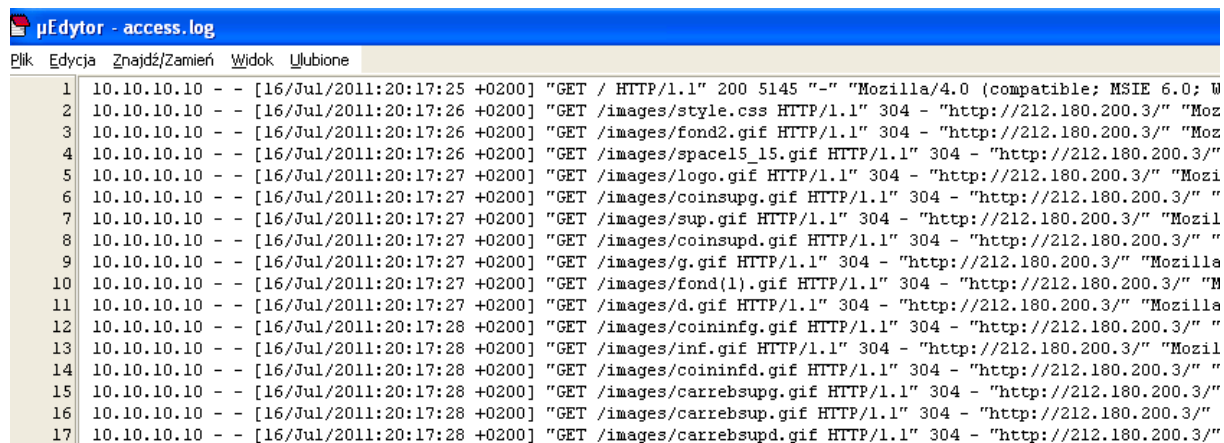
```
LAN2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
200.200.104.2 200.200.150.2 QM_IDLE    1001     0 ACTIVE

LAN2#show crypto ipsec sa
interface: Serial0/0
  Crypto map tag: CISCO, local addr 200.200.150.2
  protected vrf: (none)
  local ident (addr/mask/prot/port):
(10.10.10.10/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port):
(212.180.200.3/255.255.255.255/0/0)
  current_peer 200.200.104.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 108, #pkts encrypt: 108, #pkts digest: 108
    #pkts decaps: 104, #pkts decrypt: 104, #pkts verify: 104
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 200.200.150.2, remote crypto endpt.:
200.200.104.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0
    current outbound spi: 0x23994536(597247286)

    inbound esp sas:
      spi: 0x3793ADB2(932425138)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: 1, crypto map: CISCO
        sa timing: remaining key lifetime (k/sec):
(4400782/3126)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
    ...
    outbound esp sas:
      spi: 0x23994536(597247286)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: 2, crypto map: CISCO
        sa timing: remaining key lifetime (k/sec):
(4400781/3126)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
    ...
```

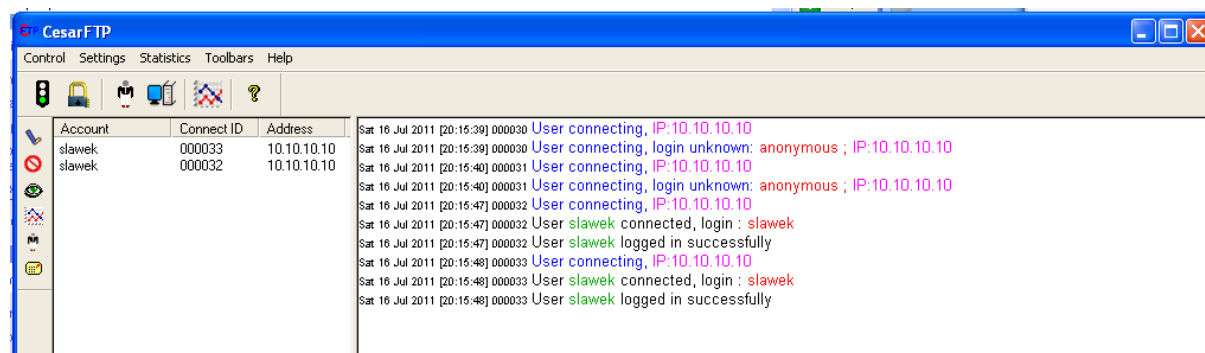
Wyniki powyższych poleceń pokazują, że tunel między routerem LAN2 oraz INT istnieje i przenoszone są przez niego informacje. Dodatkowo w celu pokazania, iż dane naprawdę wędrują przez tunel wykonano testy z wykorzystaniem serwera WWW, FTP oraz polecenia ping i programu Wireshark.



Linia	Adres IP	Metoda	Adres URL	Status	Informacje
1	10.10.10.10	GET	/ HTTP/1.1	200	5145 "-" "Mozilla/4.0 (compatible; MSIE 6.0; W
2	10.10.10.10	GET	/images/style.css HTTP/1.1	304	- "http://212.180.200.3/" "Moz
3	10.10.10.10	GET	/images/fond2.gif HTTP/1.1	304	- "http://212.180.200.3/" "Moz
4	10.10.10.10	GET	/images/spacel5_15.gif HTTP/1.1	304	- "http://212.180.200.3/"
5	10.10.10.10	GET	/images/logo.gif HTTP/1.1	304	- "http://212.180.200.3/" "Mozi
6	10.10.10.10	GET	/images/coinsupg.gif HTTP/1.1	304	- "http://212.180.200.3/" "
7	10.10.10.10	GET	/images/sup.gif HTTP/1.1	304	- "http://212.180.200.3/" "Mozil
8	10.10.10.10	GET	/images/coinsupd.gif HTTP/1.1	304	- "http://212.180.200.3/" "
9	10.10.10.10	GET	/images/g.gif HTTP/1.1	304	- "http://212.180.200.3/" "Mozilla
10	10.10.10.10	GET	/images/fond(1).gif HTTP/1.1	304	- "http://212.180.200.3/" "M
11	10.10.10.10	GET	/images/d.gif HTTP/1.1	304	- "http://212.180.200.3/" "Mozilla
12	10.10.10.10	GET	/images/coininf.gif HTTP/1.1	304	- "http://212.180.200.3/" "
13	10.10.10.10	GET	/images/inf.gif HTTP/1.1	304	- "http://212.180.200.3/" "Mozil
14	10.10.10.10	GET	/images/coininf.d.gif HTTP/1.1	304	- "http://212.180.200.3/" "
15	10.10.10.10	GET	/images/carrebsupg.gif HTTP/1.1	304	- "http://212.180.200.3/" "
16	10.10.10.10	GET	/images/carrebsup.gif HTTP/1.1	304	- "http://212.180.200.3/" "
17	10.10.10.10	GET	/images/carrebsupd.gif HTTP/1.1	304	- "http://212.180.200.3/" "

Rys. 74. Fragmenty logów z serwera WWW.

Rysunek 74 przedstawia fragment logów z serwera WWW (Krasnal Serv), pokazujące połączenia przychodzące. Dowodem na prawidłowe działanie tunelu VPN są adresy łączącego się komputera, gdyby tunel nie działał, adres IP źródła należałby do któregoś z interfejsów zewnętrznych routera LAN1 lub LAN2



Account	Connect ID	Address
slawek	000033	10.10.10.10
slawek	000032	10.10.10.10

Log entries:

- Sat 16 Jul 2011 [20:15:39] 000030 User connecting, IP: 10.10.10.10
- Sat 16 Jul 2011 [20:15:39] 000030 User connecting, login unknown: anonymous ; IP: 10.10.10.10
- Sat 16 Jul 2011 [20:15:40] 000031 User connecting, IP: 10.10.10.10
- Sat 16 Jul 2011 [20:15:40] 000031 User connecting, login unknown: anonymous ; IP: 10.10.10.10
- Sat 16 Jul 2011 [20:15:47] 000032 User connecting, IP: 10.10.10.10
- Sat 16 Jul 2011 [20:15:47] 000032 User slawek connected, login : slawek
- Sat 16 Jul 2011 [20:15:47] 000032 User slawek logged in successfully
- Sat 16 Jul 2011 [20:15:48] 000033 User connecting, IP: 10.10.10.10
- Sat 16 Jul 2011 [20:15:48] 000033 User slawek connected, login : slawek
- Sat 16 Jul 2011 [20:15:48] 000033 User slawek logged in successfully

Rys. 75. Logi z serwera FTP (CesarFTP).

Na Rysunku 75 pokazane jest okno programu CesarFTP pełniącego funkcje serwera FTP; podobnie jak w przypadku serwera WWW tu także hostem łączącym się do serwera jest urządzenie o adresie IP 10.10.10.10.

```
C:\Documents and Settings\sk1>ping 212.180.200.3
...
Odpowiedź z 212.180.200.3: bajtów=32 czas=97ms TTL=126
Odpowiedź z 212.180.200.3: bajtów=32 czas=117ms TTL=126
Odpowiedź z 212.180.200.3: bajtów=32 czas=100ms TTL=126
Odpowiedź z 212.180.200.3: bajtów=32 czas=86ms TTL=126
...
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.10.10	212.180.200.3	ICMP	74	Echo (ping) request
2	0.000064	212.180.200.3	10.10.10.10	ICMP	74	Echo (ping) reply
3	1.005762	10.10.10.10	212.180.200.3	ICMP	74	Echo (ping) request
4	1.005870	212.180.200.3	10.10.10.10	ICMP	74	Echo (ping) reply
5	4.754671	10.10.10.10	212.180.200.3	ICMP	74	Echo (ping) request
6	4.754715	212.180.200.3	10.10.10.10	ICMP	74	Echo (ping) reply
7	5.758981	10.10.10.10	212.180.200.3	ICMP	74	Echo (ping) request
8	5.759052	212.180.200.3	10.10.10.10	ICMP	74	Echo (ping) reply
9	6.757615	10.10.10.10	212.180.200.3	ICMP	74	Echo (ping) request
10	6.757714	212.180.200.3	10.10.10.10	ICMP	74	Echo (ping) reply
11	7.754353	10.10.10.10	212.180.200.3	ICMP	74	Echo (ping) request
12	7.754405	212.180.200.3	10.10.10.10	ICMP	74	Echo (ping) reply
13	241.536114	212.180.200.1	212.180.200.3	ICMP	70	Destination unreachable

Rys. 76. Fragment logów z programu Wireshak.

Efekt działania polecenia ping zgodny z założeniami a pozycje w logach programu Wireshark (Rysunek 76) potwierdzają wyniki poprzednich testów. Na podstawie uzyskanych wyników udowodnione zostało prawidłowe działanie tunelu IPsec. Podczas testów wystąpiły także błędy spowodowane małą wydajnością maszyny, na której funkcjonuje symulator. Brak mocy obliczeniowej podczas szyfrowania i deszyfrowania niejednokrotnie prowadził do nieosiągalności serwera. Ujawniły się także błędy emulatora, który w przypadkach dużego obciążenia procesora powodował utratę połączenia między routerami LAN1 oraz LAN2.

7.3.6. Test zarządzania ruchem z wykorzystanie map routingu (PBR)

Konfiguracja realizowanej sieci zakłada przepływ danych przez łącza różnych operatorów w zależności od wymagań administratora. Założenia konfiguracyjne są następujące:

- Ruch z sieci 10.10.10.0 255.255.255.0, oprócz danych www kierowany jest przez łącze udostępnione przez ISP2 (adresy IP 200.200.150.0/30 oraz 200.200.150.4/30);
- Pakiety z zawartością WWW kierowane są przez łącze od ISP1 (adresy IP 200.200.140.0/30 i 200.200.140.4/30);
- Cały ruch z sieci 10.10.20.0 255.255.255.0 kierowany jest przez łącze ISP1.

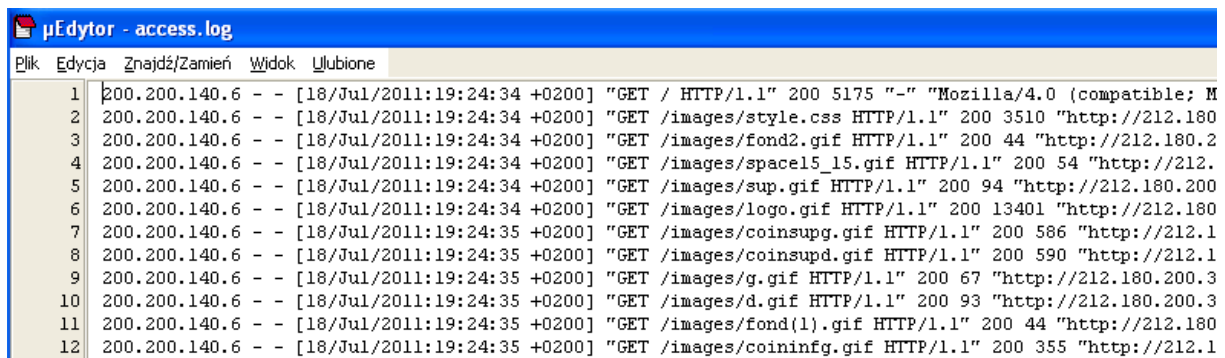
Testy polegać będą na sprawdzeniu, które łącza WAN wykorzystują pakiety w drodze do serwera. Weryfikacja przeprowadzona zostanie z urządzenia PC1 oraz PC2. Pamiętać należy, iż sieć LAN do komunikacji z siecią zewnętrzną korzysta z mechanizmu NAT, dlatego adresy

źródła w logach programów na serwerze wskazywać będą interfejs, którym pakiety opuściły sieć i jednocześnie zweryfikują, czy obrały drogę zgodną z konfiguracją.

Pierwszy test wykonany będzie z wykorzystaniem polecenia `tracert` z hostów PC1 oraz PC2 do serwera o adresie 212.180.200.3 wyniki poniżej:

```
C:\Documents and Settings\sk1>tracert 212.180.200.3
...
 1      87 ms      17 ms      16 ms    10.10.10.2
 2      85 ms      63 ms      20 ms    200.200.150.1
 3      91 ms      44 ms      14 ms    200.200.101.1
 4      97 ms      90 ms      58 ms    170.200.102.1
 5      69 ms      38 ms      33 ms    170.200.103.1
 6      94 ms      84 ms      40 ms    200.200.104.2
 7     114 ms      64 ms      33 ms    212.180.200.3
...
C:\Documents and Settings\sk2>tracert 212.180.200.3
...
 1      90 ms      13 ms      18 ms    10.10.20.2
 2     120 ms      36 ms      14 ms    200.200.140.5
 3      51 ms      56 ms      20 ms    200.200.100.1
 4      69 ms      51 ms      46 ms    170.200.100.1
 5      80 ms      33 ms      33 ms    170.200.103.1
 6     115 ms      47 ms      32 ms    200.200.104.2
 7      87 ms      68 ms      72 ms    212.180.200.3
...
```

Wyniki polecenia `tracert` wskazują, że ruch z sieci 10.10.10.0/24 korzysta z ISP2 a ruch z sieci 10.10.20.0/24 przechodzi przez ISP1. Sprawdzić należy jeszcze, czy ruch WWW z sieci 10.10.10.0 przechodzi przez łącze ISP1. Do przeprowadzenia tego testu wykorzystany zostanie serwer WWW KrasnaServ oraz przeglądarka internetowa. Wykonanie testu polegać będzie na wpisaniu adresu 212.180.200.3 w przeglądarce na urządzeniach PC1 (10.10.10.4) oraz PC2 (10.10.20.4) i odczytaniu logów z serwera WWW (Rysunek 77 oraz Rysunek 78).



Plik		Edycja	Znajdź/Zamień	Widok	Ulubione
1	200.200.140.6	-	-	[18/Jul/2011:19:24:34 +0200]	"GET / HTTP/1.1" 200 5175 "-" "Mozilla/4.0 (compatible; M
2	200.200.140.6	-	-	[18/Jul/2011:19:24:34 +0200]	"GET /images/style.css HTTP/1.1" 200 3510 "http://212.180
3	200.200.140.6	-	-	[18/Jul/2011:19:24:34 +0200]	"GET /images/fond2.gif HTTP/1.1" 200 44 "http://212.180.2
4	200.200.140.6	-	-	[18/Jul/2011:19:24:34 +0200]	"GET /images/spacel5_15.gif HTTP/1.1" 200 54 "http://212.
5	200.200.140.6	-	-	[18/Jul/2011:19:24:34 +0200]	"GET /images/sup.gif HTTP/1.1" 200 94 "http://212.180.200
6	200.200.140.6	-	-	[18/Jul/2011:19:24:34 +0200]	"GET /images/logo.gif HTTP/1.1" 200 13401 "http://212.180
7	200.200.140.6	-	-	[18/Jul/2011:19:24:35 +0200]	"GET /images/coinsupg.gif HTTP/1.1" 200 586 "http://212.1
8	200.200.140.6	-	-	[18/Jul/2011:19:24:35 +0200]	"GET /images/coinsupd.gif HTTP/1.1" 200 590 "http://212.1
9	200.200.140.6	-	-	[18/Jul/2011:19:24:35 +0200]	"GET /images/g.gif HTTP/1.1" 200 67 "http://212.180.200.3
10	200.200.140.6	-	-	[18/Jul/2011:19:24:35 +0200]	"GET /images/d.gif HTTP/1.1" 200 93 "http://212.180.200.3
11	200.200.140.6	-	-	[18/Jul/2011:19:24:35 +0200]	"GET /images/fond(1).gif HTTP/1.1" 200 44 "http://212.180
12	200.200.140.6	-	-	[18/Jul/2011:19:24:35 +0200]	"GET /images/coininfg.gif HTTP/1.1" 200 355 "http://212.1

Rys. 77. Logi z serwera WWW po połączeniu z PC1.

Przedstawione wyniki wskazują, że pakiety do serwera WWW wysłane zostały z sieci LAN z wykorzystaniem ISP1.

1	200.200.140.6	-	-	[18/Jul/2011:21:26:38 +0200]	"GET / HTTP/1.1"	200	5179	"-"	"Mozilla/4.0 (compatible; MSIE 6.0; "
2	200.200.140.6	-	-	[18/Jul/2011:21:26:39 +0200]	"GET /images/fond2.gif HTTP/1.1"	200	44	"http://212.180.200.3/"	"M
3	200.200.140.6	-	-	[18/Jul/2011:21:26:39 +0200]	"GET /images/spacel5_15.gif HTTP/1.1"	200	54	"http://212.180.200.3	
4	200.200.140.6	-	-	[18/Jul/2011:21:26:39 +0200]	"GET /images/style.css HTTP/1.1"	200	3510	"http://212.180.200.3/"	
5	200.200.140.6	-	-	[18/Jul/2011:21:26:39 +0200]	"GET /images/logo.gif HTTP/1.1"	200	13401	"http://212.180.200.3/"	
6	200.200.140.6	-	-	[18/Jul/2011:21:26:39 +0200]	"GET /images/sup.gif HTTP/1.1"	200	94	"http://212.180.200.3/"	"Moz
7	200.200.140.6	-	-	[18/Jul/2011:21:26:39 +0200]	"GET /images/coinsupg.gif HTTP/1.1"	200	586	"http://212.180.200.3/"	

Rys. 78. Logi z serwera WWW po połączeniu z PC2

Powyższe logi udowadniają także, iż zgodnie z założeniami ruch z sieci 10.10.20.0/24 kierowany jest przez połączenie z ISP1. Dodatkową weryfikację wykonać należy z wykorzystaniem np. programu CesarFTP zapisującego w logach adresy przychodzących połączeń; logi przedstawione są na rysunkach 79 (połączenie z PC1) oraz 80 (połączenie z PC2).

CesarFTP			
Control Settings Statistics Toolbars Help			
Account Connect ID Address			
slawek	000003	200.200.1...	Mon 18 Jul 2011 [19:24:47] 000001 User connecting, IP:200.200.150.2
			Mon 18 Jul 2011 [19:24:47] 000001 User connecting, login unknown: anonymous ; IP:200.200.150.2
			Mon 18 Jul 2011 [19:24:48] 000002 User connecting, IP:200.200.150.2
			Mon 18 Jul 2011 [19:24:48] 000002 User connecting, login unknown: anonymous ; IP:200.200.150.2
			Mon 18 Jul 2011 [19:24:51] 000003 User connecting, IP:200.200.150.2
			Mon 18 Jul 2011 [19:24:51] 000003 User slawek connected, login : slawek
			Mon 18 Jul 2011 [19:24:51] 000003 User slawek logged in successfully
			Mon 18 Jul 2011 [19:24:52] 000004 User connecting, IP:200.200.150.2

Rys. 79. Logi z serwera WWW po połączeniu PC1.

CesarFTP			
Control Settings Statistics Toolbars Help			
Account Connect ID Address			
slawek	000007	200.200.1...	Mon 18 Jul 2011 [21:24:14] 000006 User connecting, IP:200.200.140.6
slawek	000005	200.200.1...	Mon 18 Jul 2011 [21:24:14] 000006 User connecting, login unknown: anonymous ; IP:200.200.140.6
slawek	000003	200.200.1...	Mon 18 Jul 2011 [21:24:18] 000007 User connecting, IP:200.200.140.6
			Mon 18 Jul 2011 [21:24:18] 000007 User slawek connected, login : slawek
			Mon 18 Jul 2011 [21:24:18] 000007 User slawek logged in successfully

Rys. 80. Logi z serwera FTP po połączeniu z PC2.

Wszystkie przedstawione powyżej wyniki testów pokazują, że sieć funkcjonuje zgodnie z założeniami i routery LAN1 oraz LAN2 zostały skonfigurowane poprawnie.

7.3.7. Test protokołu MPLS oraz protokołu LDP

Pierwszy test w drugiej realizowanej sieci zakłada zweryfikowanie poprawności działania mechanizmów MPLS oraz protokołu LDP odpowiadającego za rozsyłanie etykiet. W tym celu wywołane zostaną na routerze LSR2 polecenia `show mpls forwarding-table` wyświetlające tablice LFIB oraz polecenie `show ip cef <adres_IP> detail` w celu przedstawienia funkcjonowania mechanizmu CEF.


```
LSR2#show mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	16	10.10.1.1/32	0	Se0/2	point2point
	16	10.10.1.1/32	0	Se0/1	point2point
17	Pop tag	10.10.1.2/32	0	Se0/0	point2point
18	Pop tag	10.10.1.3/32	0	Se0/1	point2point
19	Pop tag	10.10.1.5/32	1233	Se0/2	point2point
20	Pop tag	10.10.1.6/32	1140	Se0/3	point2point
21	17	10.10.10.0/24	0	Se0/2	point2point
	18	10.10.10.0/24	6524	Se0/1	point2point
22	Pop tag	200.200.100.0/30	0	Se0/1	point2point
23	Pop tag	200.200.101.0/30	0	Se0/1	point2point
25	Pop tag	200.200.107.0/30	0	Se0/2	point2point
26	Pop tag	200.200.108.0/24	0	Se0/3	point2point
27	Pop tag	10.10.1.1 1 [55]	102	Se0/3	point2point
28	Pop tag	10.10.1.1 0 [107]	0	Se0/3	point2point
29	30	10.10.1.6 0 [17]	0	Se0/2	point2point

Powyższy test przeprowadzony został przy wyłączonym interfejsie Serial 0/0 routera LER3, aby wykluczyć najkrótszą ścieżkę i dokładniej pokazać działanie mechanizmu MPLS. Przed wykonaniem powyższego polecenia przesłane zostały dane z serwera do urządzenia końcowego PC1, tak aby na przykładzie tablicy zweryfikować funkcjonowanie MPLS. Uzyskane wyniki jednoznacznie wskazują na prawidłowe działanie tego protokołu o czym świadczy liczba przelączonych bajtów (6524 bajtów) dla prefiksu 10.10.10.0/24.

```
LSR2#show ip cef 10.10.10.0 detail
10.10.10.0/24, version 33, epoch 0, per-destination sharing
0 packets, 0 bytes
  tag information set
    local tag: 21
  via 200.200.106.2, Serial0/2, 0 dependencies
    traffic share 1
    next hop 200.200.106.2, Serial0/2
    valid adjacency
    tag rewrite with Se0/2, point2point, tags imposed: {17}
  via 200.200.103.1, Serial0/1, 0 dependencies
    traffic share 1
    next hop 200.200.103.1, Serial0/1
    valid adjacency
    tag rewrite with Se0/1, point2point, tags imposed: {18}
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
         internal 0 packets, 0 bytes
```

Dane uzyskane po wykonaniu polecenia `show ip cef 10.10.10.0 detail` na routerze LSR2 pokazują, że istnieją 2 równoważne trasy do sieci 10.10.10.0, co jest zgodne z tablicą trasowania (zbudowana z wykorzystaniem protokołu OSPF) oraz topologią

i konfiguracją sieci. Każda ścieżka posiada własną etykietę, co również widoczne jest w przedstawionych wynikach:

- dla adresu kolejnego skoku 200.200.106.2 – etykieta 17;
- dla adresu kolejnego skoku 200.200.103.1 – etykieta 18.

W tablicy LFIB, podobnie jak w tablicy tras routera, znajdują się wyłącznie dane ścieżek o najniższym koszcie, jednak w przypadku ich uszkodzenia do tablic routingu dodawana jest inne ścieżka przez protokół OSPF (o ile taka istnieje), automatycznie również trasie tej przydzielana jest etykieta i router umieszcza ją w tablicy LFIB. Przypadek taki pokazuje kolejny test, w którym symulowanej awarii ulegają połączenia między LSR2 a LSR1 i LSR3.

```
LSR2#show ip cef 10.10.10.0 detail
10.10.10.0/24, version 69, epoch 0, cached adjacency to Serial0/0
0 packets, 0 bytes
  tag information set
    local tag: 21
    fast tag rewrite with Se0/0, point2point, tags imposed: {22}
  via 200.200.102.1, Serial0/0, 0 dependencies
  next hop 200.200.102.1, Serial0/0
  valid cached adjacency
  tag rewrite with Se0/0, point2point, tags imposed: {22}
```

Pakiet przesyłany do sieci 10.10.10.0 zostanie wysłany przez adres kolejnego skoku 200.200.102.1 i będzie tam opatrzony etykietą o numerze 22.

Następnie wykorzystany zostanie pakiet paris-traceroute w systemie Ubuntu do przeprowadzenia śledzenia tras. Program ten zwraca oprócz standardowych wyników takich jak komenda traceroute, numery etykiet MPLS.

```
root@skozik-desktop:/home/skozik# paris-traceroute -p icmp
10.10.10.4
traceroute [(212.180.200.3:33456) -> (10.10.10.4:33457)], protocol
icmp, algo hopbyhop, duration 60 s
 1  212.180.200.1 (212.180.200.1)  41.365 ms   20.707 ms   26.916 ms
 2  200.200.108.2 (200.200.108.2) 106.413 ms  * *
 3  200.200.104.2 (200.200.104.2)  71.095 ms  *  95.776 ms
    MPLS Label 21 TTL=1
 4  200.200.103.1 (200.200.103.1) 120.529 ms !T2  * *
    MPLS Label 18 TTL=1
 5  200.200.100.1 (200.200.100.1) 118.432 ms  * *
 6  10.10.10.4 (10.10.10.4) 173.381 ms  * *
```

Zgodnie z wynikami polecenia paris-traceroute 10.10.10.4 pakiet przechodząc do celu opatrywany jest odpowiednią etykietą, co oznacza prawidłowe funkcjonowanie protokołu MPLS. Na podstawie uzyskanych danych stwierdzić można, że pakiet przesłany został do celu z wykorzystaniem routera o adresie 200.200.103.1 i opatrzony został etykietą

o numerze 18, co weryfikuje informacje uzyskane dzięki poleceniu `show ip cef 10.10.10.0 detail` oraz `show mpls forwarding-table`.

Ostatnim z testów jest zweryfikowanie działania protokołu LDP odpowiedzialnego za wymiennę etykiet między routerami z uruchomionym protokołem MPLS. Do tego celu wykorzystać należy polecenie `show ip mpls ldp neighbor` na routerze LSR2.

```
LSR2#show mpls ldp neighbor
  Peer LDP Ident: 10.10.1.6:0; Local LDP Ident 10.10.1.4:0
    TCP connection: 10.10.1.6.21337 - 10.10.1.4.646
    State: Oper; Msgs sent/rcvd: 82/77; Downstream
    Up time: 00:28:44
    LDP discovery sources:
      Serial0/3, Src IP addr: 200.200.104.1
    Addresses bound to peer LDP Ident:
10.10.1.6      200.200.104.1    200.200.108.2    200.200.105.1
  Peer LDP Ident: 10.10.1.2:0; Local LDP Ident 10.10.1.4:0
    TCP connection: 10.10.1.2.646 - 10.10.1.4.53251
    State: Oper; Msgs sent/rcvd: 33/27; Downstream
    Up time: 00:04:08
    LDP discovery sources:
      Serial0/0, Src IP addr: 200.200.102.1
    Addresses bound to peer LDP Ident:
200.200.101.2  10.10.1.2      200.200.102.1
  Peer LDP Ident: 10.10.1.5:0; Local LDP Ident 10.10.1.4:0
    TCP connection: 10.10.1.5.15262 - 10.10.1.4.646
    State: Oper; Msgs sent/rcvd: 23/24; Downstream
    Up time: 00:02:36
    LDP discovery sources:
      Serial0/2, Src IP addr: 200.200.106.2
    Addresses bound to peer LDP Ident:
200.200.107.2  10.10.1.5      200.200.106.2    200.200.105.2
  Peer LDP Ident: 10.10.1.3:0; Local LDP Ident 10.10.1.4:0
    TCP connection: 10.10.1.3.646 - 10.10.1.4.28949
    State: Oper; Msgs sent/rcvd: 22/23; Downstream
    Up time: 00:02:33
    LDP discovery sources:
      Serial0/1, Src IP addr: 200.200.103.1
    Addresses bound to peer LDP Ident:
200.200.100.2  10.10.1.3      200.200.101.1    200.200.103.1

LSR2#show mpls ldp bindings 10.10.10.0 255.255.255.0
  tib entry: 10.10.10.0/24, rev 22
    local binding: tag: 21
    remote binding: tsr: 10.10.1.2:0, tag: 22
    remote binding: tsr: 10.10.1.6:0, tag: 20
    remote binding: tsr: 10.10.1.5:0, tag: 17
    remote binding: tsr: 10.10.1.3:0, tag: 18
```

Przeprowadzone testy oraz ich wyniki świadczą o poprawnym działaniu protokołu MPLS oraz LDP. Pakiety przechodząc przez węzły korzystające z MPLS otrzymują etykiety i w kolejnych węzłach są one zamieniane bądź usuwane. Poprawne funkcjonowanie MPLS zapewnione jest także podczas awarii pojedynczych połączeń między węzłami ze względu na funkcjonowanie protokołu trasowania OSPF. Działanie protokołu LDP wykazane zostało na przykładzie routera LSR2. Wykorzystane polecenia zweryfikowały obecność sąsiadów LDP oraz posiadanie przez router lokalnych a także zdalnych mapowań etykiet, co świadczy o prawidłowym funkcjonowaniu protokołu.

7.3.8. Test tuneli LSP

Kolejnym testem przeprowadzanym w drugiej realizowanej sieci jest weryfikacja poprawnej konfiguracji TE. Utworzone zostały trzy tunele:

- dwa mające początek w routerze LER1 i koniec w LER3 (LER1_t0 oraz LER1_t1);
- jeden rozpoczynający się w routerze LER3 i kończący w LER1 (LER3_t0).

Początkowo należy zweryfikować istnienie skonfigurowanych tuneli; w tym celu wykorzystane zostaną polecenia `show mpls traffic-eng tunnels brief` (użyte na routerze LER1, LER3 oraz LSR3) oraz `show mpls forwarding-table lsp-tunnels` (wprowadzone na routerze wewnętrznym tunelu LSP).

```
LER1>show mpls traffic-eng tunnels brief
Signalling Summary:
  LSP Tunnels Process:          running
  RSVP Process:                running
  Forwarding:                   enabled
  Periodic reoptimization:      every 3600 seconds, next
in 547 seconds
  Periodic auto-bw collection:  disabled
TUNNEL NAME    DESTINATION    UP IF    DOWN IF    STATE/PROT
LER1_t0        10.10.1.6      -        Se0/0      up/up
LER1_t1        10.10.1.6      -        Se0/0      up/up
LER3_t0        10.10.1.1      Se0/1    -          up/up
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 1 (of 1) tails

LER3>show mpls traffic-eng tunnels brief
...
TUNNEL NAME    DESTINATION    UP IF    DOWN IF    STATE/PROT
LER3_t0        10.10.1.1      -        Se0/1      up/up
LER1_t0        10.10.1.6      Se0/1    -          up/up
LER1_t1        10.10.1.6      Se0/0    -          up/up
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 2 (of 2) tails
```

Przedstawiane informacje wskazują na istnienie trzech tuneli; dwa z nich mają początek w routerze LER1 oraz jeden w routerze LER3, co jest zgodne z założeniami konfiguracyjnymi. Wszystkie tunele są w stanie „UP”, co oznacza prawidłowe funkcjonowanie oraz gotowość do przesyłania danych. Powyższe polecenie pozwoliło także na zweryfikowanie protokołu sygnalizującego RSVP odpowiedzialnego za rezerwowanie zasobów w węzłach wzdłuż tworzonej ścieżki LSP.

```
LSR3>show mpls forwarding-table lsp-tunnel
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
25 Pop tag 10.10.1.1 1 [58] 0 Se0/2 point2point
28 Pop tag 10.10.1.6 0 [20] 0 Se0/0 point2point

LSR3>show mpls traffic-eng tunnels brief
...
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
LER1_t1 10.10.1.6 Se0/1 Se0/2 up/up
LER3_t0 10.10.1.1 Se0/1 Se0/0 up/up
Displayed 0 (of 0) heads, 2 (of 2) midpoints, 0 (of 0) tails
```

Wyniki tych samych poleceń wykonane na węźle wzdłuż ścieżki LSP (w tym przypadku router LSR3), informują o przebiegających przez niego tunelach LSP potwierdzając ich działanie oraz poprawność konfiguracji urządzeń.

Następnym krokiem będzie weryfikacja parametrów, z którymi zostały utworzone tunele. Parametry te są następujące:

- LER1_t0 – możliwość zarezerwowania pasma w wysokości 1000 kbps w węzłach;
- LER1_t1 – tunel zestawiony dynamicznie z wykorzystaniem metryk TE;
- LER3_t0 – ścieżka LSP ustawiona przez administratora, w przypadku awarii któregoś węzła tunel zestawiany dynamicznie w oparciu o metryki IGP;

Do weryfikacji ustawień wykorzystać należy polecenie `mpls traffic-te tunnels Tunnel <nr_Tunelu>`.

```
LER1>show mpls traffic-eng tunnels Tunnel 0
Name: LER1_t0 (Tunnel0) Destination: 10.10.1.6
Status:
Admin: up Oper: up Path: valid Signalling: connected

path option 1, type dynamic (Basis for Setup, path weight 70)

Config Parameters:
Bandwidth: 1000 kbps (Global) Priority: 1 1 Affinity:
0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Loadshare: 1000
```

```
bw-based
  auto-bw: disabled
  InLabel   : -
  OutLabel  : Serial0/0, 24
  RSVP Signalling Info:
    Src 10.10.1.1, Dst 10.10.1.6, Tun_Id 0, Tun_Instance 120
  RSVP Path Info:
    My Address: 10.10.1.1
    Explicit Route: 200.200.100.2 200.200.101.2 200.200.102.2
200.200.104.1 10.10.1.6
    Record Route: NONE
    Tspec: ave rate=1000 kbits, burst=1000 bytes, peak rate=1000
kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=1000 kbits, burst=1000 bytes, peak rate=1000
kbits
  Shortest Unconstrained Path Info:
    Path Weight: 25 (TE)
    Explicit Route: 200.200.100.2 200.200.103.2 200.200.106.2
200.200.105.1 10.10.1.6
...

LER1#show mpls traffic-eng tunnels Tunnel 1
Name: LER1_t1                               (Tunnell) Destination: 10.10.1.6
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected

  path option 1, type dynamic (Basis for Setup, path weight 25)

Config Parameters:
  Bandwidth: 0 kbps (Global)  Priority: 1 1  Affinity:
0x0/0xFFFF
  Metric Type: TE (interface)
  AutoRoute: disabled LockDown: disabled Loadshare: 0
bw-based
  auto-bw: disabled
  InLabel   : -
  OutLabel  : Serial0/0, 30
  RSVP Signalling Info:
    Src 10.10.1.1, Dst 10.10.1.6, Tun_Id 1, Tun_Instance 58
  RSVP Path Info:
    My Address: 10.10.1.1
    Explicit Route: 200.200.100.2 200.200.103.2 200.200.106.2
200.200.105.1
                  10.10.1.6
    Record Route: NONE
    Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 25 (TE)
    Explicit Route: 200.200.100.2 200.200.103.2 200.200.106.2
200.200.105.1 10.10.1.6
...
```

```
Name: LER3_t0 (Tunnel0) Destination:
10.10.1.1
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected

  path option 10, type explicit cos (Basis for Setup, path weight
150)
  path option 20, type dynamic

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity:
0x0/0xFFFF
  Metric Type: IGP (interface)
  AutoRoute: disabled LockDown: disabled Loadshare: 0
bw-based
  auto-bw: disabled

InLabel : -
OutLabel : Serial0/1, 27
RSVP Signalling Info:
  Src 10.10.1.6, Dst 10.10.1.1, Tun_Id 0, Tun_Instance 20
RSVP Path Info:
  My Address: 10.10.1.6
  Explicit Route: 200.200.104.2 200.200.106.2 200.200.107.1
10.10.1.1
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 100 (IGP)
  Explicit Route: 200.200.105.2 200.200.107.1 10.10.1.1
....
```

Dane uzyskane w trakcie przeprowadzania testów pokrywają się z założeniami i również potwierdzają poprawną konfigurację. W przedstawionych powyżej wynikach zwrócić uwagę należy na parametr `Tun_Instance`, określający identyfikator tunelu. Numer ten pozwala na identyfikację tunelu w tablicy LFIB oraz sprawdzenie, czy dane są przesyłane z ich wykorzystaniem.

Kolejnym testem potwierdzającym prawidłową konfigurację oraz działanie tuneli TE będzie wykonanie polecenia `tracert` na urządzeniu końcowym PC1 oraz serwerze.

```
C:\Documents and Settings\sk1>tracert 212.180.200.3
```

```
...
 1    98 ms    21 ms    17 ms    10.10.10.1
 2    97 ms    43 ms    25 ms    200.200.100.2
 3    53 ms    63 ms    25 ms    200.200.103.2
 4    95 ms    59 ms    55 ms    200.200.106.2
 5   132 ms    60 ms    26 ms    200.200.105.1
 6   106 ms    77 ms    76 ms    200.200.108.1
 7   142 ms   129 ms    63 ms    212.180.200.3
```

```
...
C:\Documents and Settings\sk1>tracert 212.180.200.1
```

```
...
 1    38 ms    10 ms    16 ms    10.10.10.1
 2    61 ms    38 ms    99 ms    200.200.100.2
 3    95 ms    65 ms    32 ms    200.200.101.2
 4    91 ms    59 ms    35 ms    200.200.102.2
 5    82 ms    51 ms    44 ms    200.200.104.1
 6   105 ms    38 ms    42 ms    212.180.200.1
```

```
...
C:\Documents and Settings\slawek>tracert 10.10.10.4
```

```
...
 1    22 ms     9 ms    11 ms    212.180.200.1
 2    73 ms    46 ms    12 ms    200.200.108.2
 3    49 ms    88 ms    61 ms    200.200.104.2
 4    75 ms    82 ms    40 ms    200.200.106.2
 5    63 ms    67 ms    36 ms    200.200.107.1
 6    63 ms    50 ms    81 ms    10.10.10.4
```

Trasy pakietów uzyskane w trakcie powyższych testów pokrywają się ścieżkami tuneli LSP, które można odczytać w wynikach wcześniejszego testu, oznacza to, że pakiety przesyłane są przez tunele co dodatkowo potwierdzić można korzystając z `show mpls forwarding-table lsp-tunnels` na routerze LSR2.

```
LSR2#show mpls forwarding-table lsp-tunnel
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
24	25	10.10.1.1 1 [58]	1728	Se0/2	point2point
27	28	10.10.1.6 0 [20]	900	Se0/2	point2point
28	Pop tag	10.10.1.1 0 [120]	1608	Se0/3	point2point

Dane w kolumnie “Bytes tag switched” oznaczają ilość przełączonych danych, wartość większa od 0 potwierdza, iż dane rzeczywiście zostały przesłane przez tunele.

Ruch do tuneli LSP kierowany jest przez mapy trasowania czyli mechanizm PBR. Oznacza to, że tylko wybrane pakiety są przesyłane przez tunele. W celu sprawdzenia tego wykorzystać należy polecenie `tracert` np. z serwera z adresem celu 10.10.10.1.

```
C:\Documents and Settings\slawek>tracert 10.10.10.1
...
 1    61 ms    11 ms    12 ms    212.180.200.1
 2    78 ms    31 ms    10 ms    200.200.108.2
 3    62 ms    37 ms    24 ms    200.200.105.2
 4    77 ms    21 ms    39 ms    10.10.10.1
...
```

Ostatni test sprawdza poprawność działania tunelu z routera LER3 do LER1 podczas symulowanej awarii jednego z połączeń, które wykorzystywane jest podczas normalnej pracy tunelu LER3_t0.

```
C:\Documents and Settings\slawek>tracert 10.10.10.4
...
 1    50 ms    11 ms    10 ms    212.180.200.1
 2    45 ms    47 ms    15 ms    200.200.108.2
 3    57 ms    22 ms    34 ms    200.200.105.2
 4    74 ms    72 ms    26 ms    200.200.107.1
 5   110 ms    34 ms    37 ms    10.10.10.4
...
```

Zgodnie z konfiguracją utworzony został tunel dynamiczny i wykorzystana została trasa o najniższym koszcie OSPF.

Powyższe testy wykazały prawidłowe działanie wszystkich tuneli oraz prawidłową ich konfigurację. Ponadto zweryfikowaniu uległa konfiguracja map trasowania, które odpowiedzialne były za kierowanie wybranego ruchu do tuneli.

7.3.9. Test mechanizmów QoS.

Pierwszy test posłuży do zweryfikowania poprawności klasyfikowania ruchu oraz oznaczania go, odpowiednio w przypadku pakietów IP pole DSCP oraz dla pakietów z etykietą MPLS pole EXP. Badanie polegać będzie na wygenerowaniu ruchu WWW oraz FTP między Serwerem a komputerem PC1 symulującego ściąganie danych z serwera. Do wygenerowania ruchu użyć należy programu IxChariot wraz z odpowiednim skryptem; przykładowy kod skryptu przedstawiony jest na Rysunku 81. Skrypt ten dostarczony jest wraz z programem; do celów wykonywanego testu ustawić należy odpowiednio pole `port = source port(nr_portu)` oraz `count = number_of_timing_records(liczba powtórzeń)` na wartości:

- Dla wygenerowania ruchu http numer portu = 80 a liczba powtórzeń 1 (jeden ponieważ testowane jest tylko poprawność klasyfikacji pakietów);
- Dla ruchu ftp numer portu = 2049 i liczba powtórzeń także 1.

Line	Endpoint 1	Endpoint 2
1	SLEEP	
2	time = initial_delay (0)	
3	CONNECT_INITIATE	CONNECT_ACCEPT
4	port = source_port (80)	port = destination_port (AUTO)
5	send_buffer = DEFAULT	send_buffer = DEFAULT
6	receive_buffer = DEFAULT	receive_buffer = DEFAULT
7	LOOP	LOOP
8	count = number_of_timing_records (1)	count = number_of_timing_records (1)
9	START_TIMER	
10	LOOP	LOOP
11	count = transactions_per_record (1)	count = transactions_per_record (1)
12	SEND	RECEIVE
13	size = file_size (1000000)	size = file_size (1000000)
14	buffer = send_buffer_size (65535)	buffer = receive_buffer_size (65535)
15	type = send_datatype (NOCOMPRESS)	
16	rate = send_data_rate (UNLIMITED)	
17	CONFIRM_REQUEST	CONFIRM_ACKNOWLEDGE
18	INCREMENT_TRANSACTION	
19	END_LOOP	END_LOOP
20	END_TIMER	
21	SLEEP	
22	time = transaction_delay (0)	
23	END_LOOP	END_LOOP
24	DISCONNECT	DISCONNECT
25	type = close_type (Reset)	type = close_type (Reset)

Rys. 81. Przykładowy skrypt z programu IxChariot.

Po wygenerowaniu ruchu HTTP między serwerem a komputerem PC1 zweryfikować należy na kolejnych routerach, czy pakiety zostały sklasyfikowane i oznaczone prawidłowo. W tym celu wykorzystane zostanie polecenie `show policy-map interface <interfejs numer_interfejsu> <input|output>`. Przedstawione zostaną dane z trzech routerów, aby pokazać także działanie mechanizmu zmiany wartości DSCP na EXP i odwrotnie oraz obsługi pakietów na ich podstawie.

```
QoS-marking>show policy-map interface fa0/0 input class AF31
FastEthernet0/0

Service-policy input: SETDSCP

Class-map: AF31 (match-all)
  703 packets, 1053632 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name www
QoS Set
  dscp af31
  Packets marked 703
```

Pakiety trafiając do routera QoS-marking podlegają na interfejsie wejściowym klasyfikacji na podstawie list dostępu. Trafiają one do odpowiednich klas i ustawiona zostaje im wartość DSCP. Ruch HTTP trafia zgodnie z konfiguracją do klasy AF31 i zostaje mu ustawiana wartość DSCP na AF31 co potwierdza powyższy wynik. Następnie pakiety trafiają do interfejsu wyjściowego, tam na podstawie pola DSCP trafiają do klasy brzoze i otrzymują odpowiednie traktowanie zgodnie z ustawionymi politykami.

```
QoS-marking>show policy-map interface s0/0 output class brzoze
...
  Class-map: brzoze (match-all)
    703 packets, 1046596 bytes
    1 minute offered rate 0 bps, drop rate 0 bps
    Match:  dscp af31 (26) af32 (28) af33 (30)
    Queueing
      Output Queue: Conversation 267
      Bandwidth 10 (%)
      Bandwidth 154 (kbps)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0
      exponential weight: 9
      mean queue depth: 0
```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Maximum thresh	Mark prob
0	0/0	0/0	0/0	20	40	1/10
1	0/0	0/0	0/0	22	40	1/10
2	0/0	0/0	0/0	24	40	1/10
3	703/1046596	0/0	0/0	26	40	1/10
4	0/0	0/0	0/0	28	40	1/10
5	0/0	0/0	0/0	30	40	1/10
6	0/0	0/0	0/0	32	40	1/10
7	0/0	0/0	0/0	34	40	1/10
rsvp	0/0	0/0	0/0	36	40	1/10

Zgodnie z konfiguracją pakiety WWW trafiły do klasy ruchu brzoze i zapewnione zostało im 10% całości pasma. W następnym routerze sprawdzić należy poprawność rozpoznawania pakietów na interfejsie wejściowym oraz mapowanie wartości DSCP na wartości EXP.

```
LER3>show policy-map interface s0/2 input class IP-AF3
...
  Class-map: IP-AF3 (match-all)
    703 packets, 1046596 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:  dscp af31 (26) af32 (28) af33 (30)
    QoS Set
      mpls experimental imposition 1
      Packets marked 703
```

Pakiet został rozpoznany i przydzielony do klasy IP-AF3 i zgodnie z Tabelą 28 ustawiona została wartość pola EXP na 1.

```
LER3>show policy-map interface s0/1 output class MPLS-EXP1
...
  Class-map: MPLS-EXP1 (match-all)
    697 packets, 1041820 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: mpls experimental topmost 1
    Queueing
      Output Queue: Conversation 268
      Bandwidth 5 (%)
      Bandwidth 77 (kbps)
      (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0
      exponential weight: 9
      mean queue depth: 0
```

Ruch HTTP trafił do klasy MPLS-EXP1 (zgodnie z Tabelą 28) i zostało mu zapewnione przewidziane przez konfigurację minimalne pasmo transferu 5%. Następnie pakiet trafia do routera LSR2, gdzie wartość pola EXP nie ulega zmianie i ruch wychodząc z routera podlega polityką ustawionym przez administratora. Na routerze LSR1 usuwane są etykiety MPLS przez co usuwane jest także pole EXP, jednak obsługa pakietów nadal przebiega na podstawie wartości tego pola przeniesionej do lokalnej dla routera zmiennej qos-group.

```
LSR1>show policy-map interface s0/2 input class EXP1
...
  Class-map: EXP1 (match-all)
    697 packets, 1041820 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: mpls experimental topmost 1
    QoS Set
      qos-group 4
      Packets marked 697
```

Wynik polecenia potwierdził zgodne z konfiguracją oraz Tabelą 29 mapowanie wartości pola EXP na wartość qos-group. Kolejne wyniki pokazują, że ruch http przydzielony został do odpowiedniej grupy qos i zgodnie z jej wartością uzyskał odpowiedni poziom jakości usług.

```
LSR1>show policy-map interface s0/0 output class IP-AF3
...
Class-map: IP-AF3 (match-all)
  697 packets, 1039032 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: qos-group 4
Queueing
  Output Queue: Conversation 267
  Bandwidth 5 (%)
  Bandwidth 77 (kbps)
  (pkts matched/bytes matched) 1/1500
  (depth/total drops/no-buffer drops) 0/0/0
  exponential weight: 9
  mean queue depth: 0
```

Powyższe oraz kolejne wyniki potwierdzają poprawną konfigurację mechanizmu DiffServ oraz tunelu DiffServ typu „Pipe Model” (pozwala na przeniesienie wartości DSCP przez sieć MPLS). Zgodnie z założeniami modelu „Pipe Mode” wartości DSCP na wejściu do sieci MPLS oraz po wyjściu z niej zostały nie zmienione.

```
LSR1>show policy-map interface s0/0 output class IP-AF3
Serial0/0
...
Class-map: IP-AF3 (match-all)
  697 packets, 1039032 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: qos-group 4
Queueing
  Output Queue: Conversation 267
  Bandwidth 5 (%)
  Bandwidth 77 (kbps)
  (pkts matched/bytes matched) 1/1500
  (depth/total drops/no-buffer drops) 0/0/0
  exponential weight: 9
  mean queue depth: 0
```

Powyższe wyniki poleceń weryfikujących potwierdzają działanie mechanizmów klasyfikowania oraz oznaczania pakietów. Potwierdziły one także poprawną konfigurację modelu usług zróżnicowanych m.in. mechanizm Per-Hop-Behaviour, ponieważ pakiety klasyfikowane były w każdym węźle i również w każdym z nich autonomicznie ustalony był sposób ich obsługi. Powyższy test powtórzono dla wygenerowanego ruchu FTP na porcie 2049, aby wykazać prawidłową klasyfikację pakietów. (Ruch FTP otrzymuje DSCP AF21).

```
QoS-marking>show policy-map interface fa0/0 input class AF21
...
  Class-map: AF21 (match-all)
    699 packets, 1049036 bytes
    5 minute offered rate 15000 bps, drop rate 0 bps
    Match: access-group name ftp
    QoS Set
      dscp af21
      Packets marked 699

QoS-marking>show policy-map interface s0/0 output class silver
...
  Class-map: silver (match-all)
    699 packets, 1042040 bytes
    1 minute offered rate 11000 bps, drop rate 0 bps
    Match: dscp af21 (18) af22 (20) af23 (22)
    Queueing
      Output Queue: Conversation 266
      Bandwidth 20 (%)
      Bandwidth 308 (kbps)
      (pkts matched/bytes matched) 684/1025308
      (depth/total drops/no-buffer drops) 0/0/0
      exponential weight: 9
      mean queue depth: 0
```

Zgodnie z danymi uzyskanymi z routera QoS-marking pakiety FTP na wejściu są klasyfikowane i ustawiana jest im wartość DSCP na AF21. Na tej podstawie trafiają na wyjściu do klasy silver i otrzymują tam odpowiedni poziom obsługi, w tym wypadku jest to gwarancja minimum 20% pasma przesyłu.

```
LER3>show policy-map interface s0/2 input class IP-AF21-22
...
  Class-map: IP-AF21-22 (match-all)
    699 packets, 1042040 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: dscp af21 (18) af22 (20)
    QoS Set
      mpls experimental topmost 3
      Packets marked 0

LER3>show policy-map interface s0/1 output class MPLS-EXP3
...
  Class-map: MPLS-EXP3 (match-all)
    697 packets, 1041820 bytes
    5 minute offered rate 33000 bps, drop rate 0 bps
    Match: mpls experimental topmost 3
    Queueing
      Output Queue: Conversation 266
      Bandwidth 15 (%)
```

```
Bandwidth 231 (kbps)
(pkts matched/bytes matched) 1/1504
(depth/total drops/no-buffer drops) 0/0/0
exponential weight: 9
mean queue depth: 0
```

Na wejściu routera LER3 pakiety uzyskują etykietę MPLS i ustawiona zostaje wartość pola EXP na podstawie pola DSCP (mapowanie wartości pola DSCP na EXP znajduje się w Tabeli 28). Z uzyskanych wyników widać, że pakiety danych FTP otrzymują wartość 3 pola EXP. Na wyjściu z routera LER3 ruch FTP otrzymuje gwarancję 15% pasma przesyłu. Kolejnym węzłem na drodze pakietów jest router LSR2, gdzie zgodnie z mechanizmem PHB zapewniony zostaje im odpowiedni poziom usług. Router LSR1 odpowiada na tej trasie za usuwanie etykiet, a razem z nimi wartości EXP. Aby spełnione zostały założenia „Pipe Model” tunelu Diffserv wartość EXP musi zostać skopiowana w celu jej późniejszego wykorzystania.

```
LSR1>show policy-map interface s0/2 input class MPLS-EXP3
Serial0/2

Service-policy input: traffic-in

Class-map: MPLS-EXP3 (match-all)
  697 packets, 1041820 bytes
  5 minute offered rate 9000 bps, drop rate 0 bps
  Match: mpls experimental topmost 3
  QoS Set
    qos-group 3
      Packets marked 697
  discard-class 1
    Packets marked 697
```

Dane FTP trafiły do klasy MPLS-EXP3 przydzielona została im grupa qos o numerze trzy i klasa odrzucenia określająca prawdopodobieństwo odrzucenia pakietu podczas zatoru przez mechanizm WRED.

```
LSR1>show policy-map interface s0/0 output class IP-AF2
...
Class-map: IP-AF2 (match-all)
  697 packets, 1039032 bytes
  5 minute offered rate 5000 bps, drop rate 0 bps
  Match: qos-group 3
  Queueing
    Output Queue: Conversation 266
    Bandwidth 25 (%)
    Bandwidth 386 (kbps)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
    exponential weight: 9
    mean queue depth: 0
```

Fragment powyższych wyników potwierdził prawidłową konfigurację polityk ruchu na wyjściu routera LSR1. Pakietom FTP została zagwarantowana założona przez administratora jakość obsługi.

Wyniki uzyskane podczas testów ze strumieniami danych HTTP oraz FTP wskazują na prawidłową konfigurację mechanizmów QoS. Pakiety trafiają do odpowiednich klas i uzyskują założoną przez administratora jakość obsługi w każdym węźle sieci.

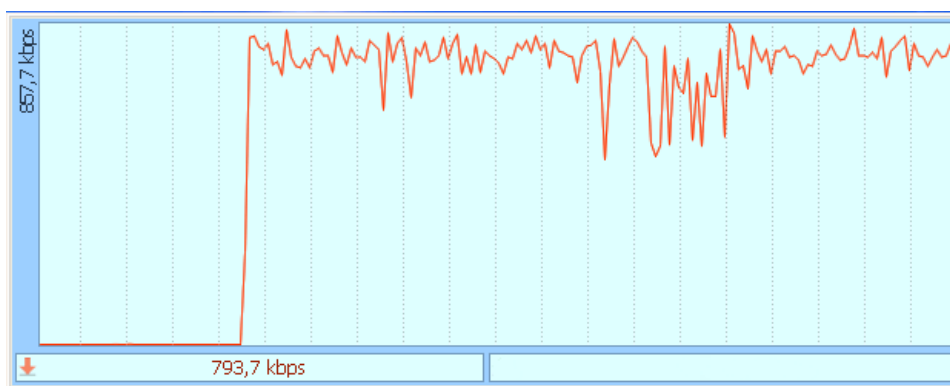
Kolejny test powinien polegać na obciążeniu sieci ruchem różnego typu, wykorzystując do tego celu program IxChariot. Pozwoliłoby to zweryfikować działanie mechanizmów QoS wykorzystanych w sieci (minimalne pasmo, mechanizm WRED itp.). Niestety ze względów uruchomienia całej sieci w środowisku symulacyjnym obciążenie CPU komputera, na którym znajduje się symulator powoduje ograniczenie transferu, który waha się w granicach 600 do 800 kbps (wartość ta w sieci wykorzystującej porty Serial do połączeń WAN wynosić powinna 1544 kbps). Oprócz obciążenia CPU problemem są także błędy symulatora dynamips wpływające na wysokość transferów.

Celem kolejnego etapu testu jest weryfikacja działania mechanizmu kształtującego ruch na przykładzie wygenerowanego strumienia danych HTTP oraz FTP. Pakiety FTP podlegają kształtowaniu i średnia prędkość transferu ustawiona w konfiguracji powinna wynosić około 512 kbps (1 kbps = 1000 bitów/s). Do testów wykorzystać należy program IxChariot generujący ruch HTTP oraz na komputerze PC1 oprogramowanie służące do pomiaru transferu np. DU Meter. Wynik z pomiaru uzyskany przy pomocy DU Meter przedstawiony jest na Rysunku 82.



Rys. 82. Wykres transferu uzyskany programem DU Meter podczas symulowanego ściągania danych z serwera FTP.

Wykres potwierdza poprawność konfiguracji kształtowania ruchu, transfer waha się w przedziale 500 kbps do 520 kbps (co jest zgodne z ustawioną wartością średnią 512 kbps w mechanizmie kształtującym) i jest płynny (brak dużych skoków oprócz widocznego na wykresie jednego punktu, który mógł być spowodowany niewydolnością CPU). Rysunek 83 przedstawia wartości uzyskane podczas takiego samego testu przy wygenerowanym ruchu HTTP, zauważyć można, że uzyskany transfer jest wyższy zgodnie z konfiguracją (brak ograniczenia transferu, jedynie dostępne pasmo na łączu) jednak brak mechanizmów kształtowania ruchu powoduje, że wielkość transferu waha się w dużym zakresie prędkości, co reprezentują spadki oraz wzrosty na wykresie.



Rys. 83. Wykres transferu uzyskany programem DU Meter podczas symulowanego ściągania danych z serwera HTTP.

W trakcie testów zweryfikować należy także działanie mechanizmu ograniczającego ruch nie pasujący do żadnej z przygotowanych klas. W tym celu wygenerowany został strumień danych z serwera do komputera PC1 na porcie 2500. W celu uzyskania odpowiedzi, czy mechanizm działa, należy wykonać polecenie `show policy-map interface s0/0 output class IP-BE` na routerze QoS-marking. Uzyskane wyniki znajdują się poniżej.

```
QoS-marking#show policy-map interface s0/0 output class BE
...
Class-map: BE (match-all)
  7059 packets, 10067453 bytes
  1 minute offered rate 46000 bps, drop rate 17000 bps
Match: access-group 101
police:
  cir 56000 bps, bc 1750 bytes, be 1750 bytes
  conformed 4115 packets, 5657217 bytes; actions:
    set-dscp-transmit default
  exceeded 1718 packets, 2571236 bytes; actions:
    drop
  violated 1226 packets, 1839000 bytes; actions:
    drop
  conformed 30000 bps, exceed 12000 bps, violate 6000
bps
```

Wyniki potwierdzają działanie mechanizmu kontrolującego szybkość przepływającego ruchu. Wszystkie przeprowadzone testy wykazują na poprawną konfigurację mechanizmów zapewniania usług w drugiej realizowanej sieci. Pakiety są klasyfikowane, oznaczane oraz podlegają zasadom ruchu ustalonym przez konfigurację. Część koniecznych testów musiała zostać pominięta ze względu na błędy symulatora lub duże obciążenie CPU, ograniczające transfer w sieci.

8. Podsumowanie i wnioski

W niniejszej pracy omówione zostały zagadnienia związane z zarządzaniem ruchem pakietów w sieciach opartych na protokole IP. Sieci komputerowe są najszybciej rozwijającym się medium udostępniającym różnego rodzaju dane oraz informacje, obecne są w codziennym życiu każdego człowieka. Tak duża rola wymusza na sieciach sprawne oraz szybkie ich działanie, co spowodowało szybki rozwój mechanizmów odpowiadających za poprawne przesyłanie datagramów w sieciach. Wszystkie omówione w pracy mechanizmy opierają swoje działanie na najpowszechniej obecnie stosowanym protokole komunikacyjnym IP.

Praca swoim zakresem obejmuje funkcjonowanie protokołu IP w wersji 4 oraz 6, który obecnie zaczyna funkcjonować w Internecie. Przedstawia sposób adresacji urządzeń w sieci oraz komunikacji urządzeń końcowych. Pokazany został także tzw. protokół kontrolny Internetu, czyli ICMP odpowiedzialny za informowanie się urządzeń o błędach oraz przeciążeniach występujących w sieci. Omówione zostały, na podstawie mechanizmów translacji adresów oraz tuneli VPN, sposoby modyfikowania zawartości datagramów. Pierwszy z mechanizmów pozwala na komunikację z siecią globalną urządzeń pracujących w sieci lokalnej nawet w przypadku braku odpowiedniej ilości publicznych adresów IP. Tunele VPN natomiast pozwalają na tworzenie bezpiecznych połączeń między urządzeniami końcowymi, a nawet całymi sieciami.

Dalsza część pracy przedstawia zaawansowane mechanizmy zarządzania ruchem działające w oparciu o protokół IP. Omówiony został protokół BGP służący do wymiany informacji o trasach między systemami autonomicznymi, a także routerami brzegowymi w obrębie jednego systemu. Obecnie jest on jedynym protokołem przystosowanym do tego celu i stosowana wersja BGP-4 obsługuje również protokół IPv6. Praca przedstawia także protokół OSPF służący do trasowania wewnątrz systemów autonomicznych. Z wykonanych w części praktycznej analiz wynika, że obydwa protokoły spełniają swoje zadanie. Dzięki ich działaniu urządzenia końcowe znajdujące w różnych sieciach mogą się ze sobą komunikować. Dbają również aby ścieżka, którą podróżują pakiety była najbardziej optymalna. Protokoły trasowania dynamicznego umożliwiają zachowanie łączności między sieciami odległymi nawet w przypadku awarii pojedynczych połączeń; zostaje zastosowana po prostu inna dostępna trasa. Oprócz protokołów trasowania pozwalających na przesyłanie pakietów między różnymi sieciami do tego celu służy także mechanizm MPLS (współpracuje on z protokołami stanu łącza). Zaletą jego, w odróżnieniu do tradycyjnych protokołów

trasowania, jest szybkość przesyłania pakietów IP przez sieć oraz mniejsze obciążenie węzłów (brak konieczności dekapulacji pakietów w celu uzyskania adresu IP).

Ważnym elementem zarządzania ruchem w sieciach IP jest także zapewnienie odpowiedniego poziomu obsługi pakietom w niej podróżującym. Każda usługa działająca w sieci ma własne wymagania odnośnie pasma, opóźnień oraz innych parametrów w sieci. Opisane w pracy mechanizmy zapewniania jakości usług pozwalają, aby pakiety obsługiwane były zgodnie z ich wymaganiami lub wymaganiami administratora sieci. Pozwalają one na priorytyzację ruchu w oparciu o założone parametry. W pracy przedstawiony został model usług zróżnicowanych umożliwiający różną obsługę pakietów w różnych węzłach sieci, co daje dużą elastyczność podczas konfiguracji.

Podczas omawiania problemu zarządzania ruchem pakietów pamiętać należy także o zapewnieniu możliwości ich przesyłania nawet podczas awarii. Nadmiarowość zapewniającą ciągłość pracy sieci komputerowych również należy dodać do kategorii zarządzania ruchem pakietów. Zwrócono zatem uwagę w pracy na problem jej zapewnienia w różnych częściach sieci. Omówiono zastosowanie większej liczby połączeń między węzłami sieci tworząc zapasowe trasy dla datagramów. Przedstawiono oraz omówiono zalety i wady dodatkowych połączeń WAN (w tym połączenia od kilku dostawców internetowych). Uwagę zwrócono także na zachowanie ciągłości dostępu użytkowników sieci LAN do sieci globalnej poprzez zastosowanie protokołu HSRP i nadmiarowość bramy domyślnej.

Praca obejmuje także sterowanie ruchem z wykorzystaniem list dostępu oraz Systemów Zapobiegania Włamaniom. Opisuje ona sposób tworzenia list dostępu oraz jak wpływają one na ruch przesyłany przez węzły w sieci. Pokazana jest możliwość blokowania określonego przez administratora ruchu.

W części praktycznej analizie podlega większość wyżej omówionych mechanizmów, przedstawiony jest sposób ich konfiguracji na urządzeniach firmy CISCO. Do tego celu zbudowane zostały dwie sieci. W pierwszej z nich zastosowano różne techniki nadmiarowości m.in. nadmiarowe połączenia między urządzeniami w sieci, dodatkowe połączenia ISP oraz radunacja bramy domyślnej w sieci LAN (protokół HSRP). Zaprojektowana sieć podzielona została także na systemy autonomiczne pomiędzy, którymi wykorzystano protokół BGP w celu wymiany tras. W obrębie jednego z systemów symulującego nadrzędnego dostawcę usług internetowych, składającego się z czterech routerów do rozsyłania informacji o trasach zastosowane zostały protokoły OSPF oraz RIPv2. W sieci LAN wykorzystano również mechanizm trasowania zgodnie z politykami ustalonymi przez administratora tzw. PBR. Ostatnim zaimplementowanym rozwiązaniem w tej sieci było utworzenie między routerem

LAN2 oraz INT tunelu VPN IPSec w celu przesyłania informacji w postaci zaszyfrowanej. W drugiej zbudowanej sieci wykorzystany został protokół MPLS w rdzeniu sieci (oraz protokół OSPF do poprawnego działania MPLS). Zastosowany został także mechanizm MPLS TE, czyli tunele LSP, do przesyłania danych z zapewnieniem odpowiedniego poziomu obsługi. Ostatnim wprowadzonym rozwiązaniem do tej sieci był mechanizm zapewniania obsługi pakietom zarówno w sieci IP jak i w sieci wykorzystującej techniki MPLS oraz pokazano działanie modelu usług zróżnicowanych.

Następnie zbudowane sieci oraz wykorzystane mechanizmy podległy różnym testom weryfikującym ich działanie. Otrzymane wyniki świadczą o poprawnym działaniu wszystkich zaimplementowanych mechanizmów. Podczas przeprowadzania testów pojawiły się błędy związane z tym, iż sieci zbudowane zostały w środowisku symulacyjnym. Nie udało się również przeprowadzić testów wydajnościowych dla mechanizmów zapewniania jakości usług z powodu zbyt małej wydajności komputera wykorzystanego do obsługi symulatora.

Informacje zawarte w części teoretycznej pracy oraz dane uzyskane podczas testów świadczą o zasadności wykorzystywania w sieciach komputerowych różnych metod sterowania ruchem. Pozwalają one bowiem na istnienie oraz działanie tak wielu usług w sieci z jakich obecnie można bez przeszkód korzystać. Jasne jest także, że istniejące sposoby zarządzania ruchem będą ewoluować oraz wraz z dalszym rozwojem sieci i usług w nich dostępnych pojawiać się będą nowe mechanizmy kierujące ruch jeszcze skuteczniej.

Przyglądając się topologii budowanych sieci oraz wykorzystanych w nim technikom zauważyć można również, że przeznaczone są do wykorzystania w różnych części sieci (Tabela 32).

Tab. 32. Mechanizmy zarządzania ruchem oraz miejsce ich występowania.

Mechanizm zarządzania ruchem	Miejsce wykorzystania w sieci
Protokół trasowania dynamicznego bramy wewnętrznej (OSPF, RIPv2)	Wykorzystywany w obrębie jednego systemu autonomicznego np. (Sieć LAN, połączenie między ISP a klientami).
Protokół trasowania dynamicznego bramy zewnętrznej (BGP)	Wykorzystywany do wymiany informacji o trasach między systemami autonomicznymi.
Translacja adresów	Połączenie sieci LAN z siecią globalną.
Nadmiarowość bramy domyślnej	Sieć LAN.
Nadmiarowość połączeń ISP	Połączenie sieci lokalnych z siecią globalną.
Nadmiarowość połączeń między urządzeniami	Stosowane zarówno w sieciach WAN oraz LAN.

PBR (ang. <i>Policy Based Routing</i>)	Rozwiązanie można to stosować praktycznie w każdej miejscu sieci.
MPLS	Stosowane w rdzeniach sieci.
Quality of Service	Stosowane zarówno w małych sieciach LAN (w ograniczonym zakresie) oraz w sieciach WAN.
Listy dostępu	Wykorzystywane praktycznie w każdym węźle sieci.

Po analizie przedstawionych danych nasuwa się wniosek, że w celu zapewnienia poprawnego działania sieci komputerowych konieczne jest wykorzystanie jednocześnie wielu mechanizmów zarządzania ruchem pakietów. Zastosowanie pojedynczych metod mogłoby doprowadzić do tego, że sieć nie spełniałaby postawionych jej wymogów, a wręcz uniemożliwiłoby jej prawidłowe działanie. Wykorzystanie wielu metod przeznaczonych dla różnych miejsc sieci pozwala na prawidłowe zarządzanie ruchem w całej sieci a nie tylko w jej fragmencie.

Wykaz rysunków

Rys. 1. Statystyczny wzrost liczby użytkowników internetu w latach 1995-2010 [27i].	5
Rys. 2. Topologia pierwszej sieci komputerowej ARPAnet [29i]	8
Rys. 3. Porównanie modelu ISO/OSI z TCP/IP.	10
Rys. 4. Funkcje warstwy trzeciej.	11
Rys. 5. Wymiana pakietów między sieciami nie posiadającymi bezpośredniego połączenia.	12
Rys. 6. Nadmiarowość połączeń w sieciach.	13
Rys. 7. Sieć bez redundancji bramy domyślnej.	13
Rys. 8. Nadmiarowość bramy domyślnej.	14
Rys. 9. Nadmiarowość połączeń z dostawcą usług internetowych a) jeden ISP b) dwóch ISP.	14
Rys. 10. Nagłówek protokołu IPv4.	16
Rys. 11. Nagłówek protokołu IPv6.	17
Rys. 12. Adresowanie sieci z podsieciami.	19
Rys. 13. Zastosowanie technologii VLSM.	20
Rys. 14. Pakiet ICMP.	22
Rys. 15. Sieć wielosegmentowa.	23
Rys. 16. Przesyłanie datagramów przez sieć złożoną.	24
Rys. 17. Działanie NAT.	26
Rys. 18. Działanie PAT.	27
Rys. 19. Działanie Wirtualnej Sieci Prywatnej.	28
Rys. 20. Umieszczenie nagłówka protokołu AH w datagramie.	29
Rys. 21. Umieszczenie elementów nagłówka ESP w datagramie.	29
Rys. 22. Zestawianie bezpiecznego połączenia IPsec.	30
Rys. 23. Przesyłanie pakietów w obrębie jednej sieci.	31
Rys. 24. Systemy autonomiczne oraz połączenia między nimi.	33
Rys. 25. Trasowanie w sieci.	34
Rys. 26: Podział algorytmów trasowania ze względu na zależności między routerami.	35
Rys. 27. Proces uzyskiwania informacji o trasach przez nowy router.	36
Rys. 28. Aktualizacja wymuszone w sieci z trasowaniem RIPv2.	37
Rys. 29. OSPF a) wieloobszarowy b) jednoobszarowy	39
Rys. 30. Komunikacja routerów OSPF.	40
Rys. 31. Nagłówek pakietu Hello.	41

Rys. 32. Ustanawianie komunikacji dwustronnej.	42
Rys. 33. Rodzaje routerów OSPF.....	46
Rys. 34. Działanie eBGP oraz iBGP.	49
Rys. 35. Działanie modelu Intserv.	53
Rys. 36. Działanie modelu Diffserv.	53
Rys. 37. Klasyfikacja oraz oznaczanie datagramów.	55
Rys. 38. Pole DSCP.....	55
Rys. 39. Ponowna klasyfikacja pakietów na granicy domen DiffServ.	55
Rys. 40. Model ciekącego wiadra.	60
Rys. 41. Model wiadra z żetonami.	61
Rys. 42. Wpływ zastosowania WRED na wydajność sieci [30i].	61
Rys. 43. Etykieta MPLS w ramce Ethernet.....	63
Rys. 44. Budowa etykiety MPLS.	63
Rys. 45. Typy routerów w domenie MPLS.....	64
Rys. 46. Funkcje routerów w domenie MPLS.	65
Rys. 47. Agregacja ruchu w domenie MPLS.	66
Rys. 48. Etapy zestawiania sesji LDP.	68
Rys. 49. Komunikaty wymienianie podczas sesji LDP.	68
Rys. 50. Rozszerzony mechanizm wykrywania sąsiadów.	69
Rys. 51. Inżynieria ruchu w sieciach MPLS.	71
Rys. 52. Działanie standardowej listy dostępu.....	73
Rys. 53. Działanie rozszerzonej listy dostępu.....	74
Rys. 54. Przesyłanie datagramów w sieci wykorzystującej protokół HSRP.	76
Rys. 55. Przesyłanie datagramów w sieci z protokołem HSRP. Awaria Router'a 1.	76
Rys. 56. Topologia logiczna sieci z punktu widzenia znajdujących się w niej urządzeń.	77
Rys. 57. Nagłówek komunikatu HSRP.	78
Rys. 58. Działanie systemu HIPS.....	79
Rys. 59. Działanie sieciowego systemu zapobiegania włamaniom.	79
Rys. 60. Udział w rynku producentów routerów w segmencie SOHO.....	84
Rys. 61. Udział producentów przełączników w rynku [31i].	87
Rys. 62. Udział producentów routerów w segmencie ISP [32i].	90
Rys. 63. Topologia pierwszej projektowanej sieci.....	94
Rys. 64. Sieć LAN pierwszej projektowanej sieci.	94
Rys. 65. Fragment pierwszej sieci obejmujący dostawców usług internetowych.	95

Rys. 66. Projekt drugiej sieci.	96
Rys. 67. Diagram przedstawiający trasę pakietów pokonujące utworzone tunele.....	116
Rys. 68. Konfiguracja adresu IP w systemie Windows.	126
Rys. 69. Okno zarządzania obrazami IOS.....	128
Rys. 70. Konfiguracja emulatora Dynamips.	129
Rys. 71. Konfiguracja rozszerzeń w routerach.	129
Rys. 72. Log z programu Wireshark.	142
Rys. 73. Log z programu Wireshark po symulowanej awarii.	143
Rys. 74. Fragmenty logów z serwera WWW.....	149
Rys. 75. Logi z serwera FTP (CesarFTP).	149
Rys. 76. Fragment logów z programu Wireshak.....	150
Rys. 77. Logi z serwera WWW po połączeniu z PC1.....	151
Rys. 78. Logi z serwera WWW po połączeniu z PC2.....	152
Rys. 79. Logi z serwera WWW po połączeniu PC1.	152
Rys. 80. Logi z serwera FTP po połączeniu z PC2.	152
Rys. 81. Przykładowy skrypt z programu IxChariot.	162
Rys. 82. Wykres transferu uzyskany programem DU Meter podczas symulowanego ściągania danych z serwera FTP.	169
Rys. 83. Wykres transferu uzyskany programem DU Meter podczas symulowanego ściągania danych z serwera HTTP.	169

Wykaz tabel

Tab. 1. Adresy IPv4.....	18
Tab. 2. Klasy adresów IPv4.	19
Tab. 3. Zastosowanie maski podsieci.....	20
Tab. 4. Cechy Wirtualnych sieci prywatnych.	27
Tab. 5. Porównanie protokołów routingu.....	35
Tab. 6. Typy komunikatów LSP.	40
Tab. 7. Rodzaje komunikatów LSA.	44
Tab. 8. Typy routerów OSPF.	46
Tab. 9. Typy obszarów w wieloobszarowym OSPF.	47
Tab. 10. Komunikaty wykorzystywane w tworzeniu sesji BGP.....	48
Tab. 11. Mechanizmy klasyfikacji oraz znakowania datagramów.	56
Tab. 12. Mechanizmy kolejkwania datagramów.	58
Tab. 13. Tryby rozsyłania odwozowań etykiet.	69
Tab. 14. Porównanie wybranych urządzeń segmentu SOHO.	85
Tab. 15. Porównanie wybranych urządzeń segmentu SMB.....	86
Tab. 16. Porównanie routerów segmentu Enterprise.	88
Tab. 17. Porównanie routerów segmentu Enterprise.	89
Tab. 18. Wybrane modele routerów z segmentu dostawców usług internetowych.	91
Tab. 19. Wybrane przełączniki wielowarstwowe z segmentu ISP.	92
Tab. 20. Adresacja urządzeń końcowych.....	97
Tab. 21. Adresacja interfejsów urządzeń nadrzędnego ISP.	97
Tab. 22. Adresacja interfejsów routerów ISP1 oraz ISP2.....	98
Tab. 23. Adresacja interfejsów routerów LAN1, LAN2 oraz RD.	98
Tab. 24. Adresacja urządzeń końcowych w drugiej sieci.	99
Tab. 25. Adresacja interfejsów routerów pracujących w sieci.....	99
Tab. 26. Wartości metryki TE oraz rezerwowanego pasma dla poszczególnych interfejsów..	113
Tab. 27. Określenie klas ruchu dla pakietów wychodzących.	121
Tab. 28. Mapowanie pola DSCP na EXP wraz z nazwami odpowiadających im klas.....	122
Tab. 29. Parametry, które należy zapewnić danym wychodzącym.	123
Tab. 30. Mapowanie pola EXP na wartości qos-group.....	125
Tab. 31. Poziom obsługi dla poszczególnych klas ruchu wyjściowego.....	125

Tab. 32. Mechanizmy zarządzania ruchem oraz miejsce ich występowania.	173
--	-----

Spis literatury

Źródła drukowane

- [1] Alvaayn V., *Advanced MPLS Design and Implementation (CCIE Professional Developmnet)*, Wydanie I, Cisco Press, 2001
- [2] Comer D.E., *Sieci komputerowe TCP/IP. Zasady, protokoły i architektury*, wydanie III, WNT, Warszawa 1998
- [3] Doyle J., Carroll J.D., *Routing TCP/IP, Volume I (CCIE Professional Development)*, Wydanie II, Cisco Press 2005
- [4] Doyle J., Carroll J.D., *Routing TCP/IP, Volume II (CCIE Professional Development)*, Wydanie I, Cisco Press 2001
- [5] Ferguson P., Huston G., *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*, Wydanie I, John Wiley & Sons, 1998
- [6] Flannagan M., *Administering CISCO QoS for IP Networks*, Wydanie I, Syngress 2001
- [7] Flannagan M., Froom R., Turek K., *Cisco Catalyst QoS: Quality of Service in Campus Networks*, Wydanie I, Cisco Press 2003
- [8] Ghein L.D., *MPLS Fundamentals*, Wydanie I, Cisco Press, 2006
- [9] Halbi S., McPherson D., *Internet Routing Architectures*, Wydanie II, Cisco Press 2000
- [10] Hassan M., Jain R., *Wysokowydajne sieci TCP/IP*, wydanie I, HELION, Gliwice 2004
- [11] Krysiak K., *Sieci komputerowe. Kompendium*, wydanie II, HELION, Gliwice 2005
- [12] Kummar R., *Building MPLS-Based Broadband Access VPN's*, Wydanie I, Cisco Press, 2004
- [13] Kurose J.F., Ross K.W., *Sieci komputerowe od ogółu do szczegółu z Internetem w tle*, wydanie III, HELION, Gliwice 2006
- [14] *Materiały szkoleniowe z kursu CCNP Building Scalable Internetworks v5.0*
- [15] *Materiały szkoleniowe z kursu CNAP Network Security 2 v2.0*
- [16] Ogletree T., *Rozbudowa i naprawa sieci*, Wydanie II, Helion, Gliwice 2001
- [17] Oppenheimer P., *Top-Down Network Design*, Wydanie II, Cisco Press, 2004
- [18] RFC 791 - INTERNET PROTOCOL
- [19] RFC 2328 – OSPF Version 2
- [20] RFC 2460 - Internet Protocol, Version 6 (IPv6)
- [21] RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations
- [22] Solie K., *CCIE Practical Studies, Volume I*, Wydanie I, Cisco Press 2001

[23] Tanenbaum A.S., *Sieci komputerowe*, wydanie IV, HELION, Gliwice 2004

Źródła internetowe

- [1i] <http://cisco.netacad.net>, *Materiały szkoleniowe z kursu CCNA Exploration: Network Fundamentals Wersja 4.0*, (sprawdzony 2011.03.19)
- [2i] <http://cisco.netacad.net>, *Materiały szkoleniowe z kursu CCNA Exploration: Routing Protocols and Concepts Wersja 4.0*, (sprawdzony 2011.03.19)
- [3i] <http://cisco.netacad.net>, *Materiały szkoleniowe z kursu CCNA Exploration: Accessing the WAN Wersja 4.0*, (sprawdzony 2011.03.19)
- [4i] <http://cisco.netacad.net>, *Materiały szkoleniowe z kursu CCNA Security Wersja 1.0*, (sprawdzony 2011.03.19)
- [5i] <http://www.cisco.com>, *Cisco Systems Inc. Strona Główna*, (sprawdzony 2011.05.19)
- [6i] <http://docwiki.cisco.com>, *Cisco DocWiki Strona Główna*, (sprawdzony 2011.05.19)
- [7i] <http://www.ccnatut.info/>, *Cisco Certified Network Associate Tutorials*, (sprawdzony 2011.03.19)
- [8i] <http://nss.et.put.poznan.pl/>, *Wydział Elektroniki i Telekomunikacji Politechniki Poznańskiej Strona Główna*, (sprawdzony 2011.03.19)
- [9i] <http://www.staff.amu.edu.pl/~psi/>, *Uniwersytet im. Adama Mickiewicza w Poznaniu Strona Mieczysława Cichonia*, (sprawdzony 17-01-2011)
- [10i] <http://www.dell.com/>, *Dell Strona Główna*, (sprawdzony 2011.04.04)
- [11i] <http://www.tech-portal.pl/>, *Tech-portal.pl – Technologie Sieciowe Strona Główna*, (sprawdzony 2011.01.17)
- [12i] <http://itpedia.pl/>, *ITpedia Strona Główna*, (sprawdzony 2011.04.05)
- [13i] <http://twojepc.pl/>, *Twoje PC Strona Główna*, (sprawdzony 2011.04.05)
- [14i] <http://www.scientist.pl/>, *Forum Naukowe scientist.pl*, (sprawdzony 2011.03.19)
- [15i] <http://www.rogaski.org/>, *Strona domowa Adriana Rogaskiego*, (sprawdzony 2011.03.19)
- [16i] <http://www.winsocketdotnetworkprogramming.com/winsock2programming/>, *Tutorials on 'Advanced' Winsock 2 Network Programming*, (sprawdzone 2011.04.07)
- [17i] <http://www.javvin.com>, *Javvin network managment & security Strona Główna*, (sprawdzony 2011.05.04)
- [18i] <http://www.networksorcery.com>, *Network Sortery Strona Główna*, (sprawdzony 2011.05.04)

- [19i] <http://www.checkpoint.com/>, *Check Point – Security Appliances, Security Gateways, Firewall, Security Managment, Endpoint Security & Software Blades Strona Główna*, (sprawdzony 2011.05.04)
- [20i] <http://csrc.nist.gov/>, *National Institute of Standard and Technology: Computer Security Resource Center Strona Główna*, (sprawdzony 2011.05.04)
- [21i] <http://www.clico.pl>, *Clio - autoryzowany dystrybutor nowoczesnych technologii IT Strona Główna*, (sprawdzony 2011.05.04)
- [22i] <http://www.cgisecurity.com>, *Web application news, and more. Strona Główna*, (sprawdzony 2011.05.19)
- [23i] <http://compnetworking.about.com>, *Networking – Computer and Wireless Networking Basics Strona Główna*, (sprawdzony 2011.05.19)
- [24i] <http://www.einnews.com>, *EIN News a digital news provider Strona Główna*, (sprawdzony 2011.05.19)
- [25i] <http://www.networkworld.com>, *Network World Strona Główna*, (sprawdzony 2011.05.19)
- [26i] <http://www.networld.pl>, *Networld Strona Główna*, (sprawdzony 2011.05.19)
- [27i] <http://worldnarrowweb.wordpress.com/category/the-narrow-web/>, *The World Narrow Web*, (sprawdzony 2011.08.24)
- [28i] <http://royal.pingdom.com/>, *Royal Pingdom: Ramblings and tech news from the Pingdom team Strona Główna*, (sprawdzony 2011.08.24)
- [29i] <http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html>, *An Atlas of Cyberspaces - Historical Maps*, (sprawdzony 2011.08.24)
- [30i] <http://szmarcin.w.interia.pl/text/QoS.html>, (sprawdzony 2011.08.24)
- [31i] <http://www.infonetics.com/newsletters/Enterprise-Networking-030211.html>, *Infonetics Research / telecommunications market research / telecom market analysis*, (sprawdzony 2011.08.24)
- [32i] <http://seekingalpha.com/article/109717-sector-overview-networking>, *Sector Overview: Networking - Seeking Alpha*, (sprawdzony 2011.08.24)

10 Załącznik Nr 2
do Regulaminu Studiów w PŁ
z dnia 29 marca 2006 roku

Łódź, dnia 25 sierpnia 2011 roku

Sławomir Kozik
(IMIĘ I NAZWISKO STUDENTA)

131503
(NR ALBUMU)

Informatyka
(KIERUNEK STUDIÓW)

jednolite magisterskie, dzienne
(RODZAJ I FORMA STUDIÓW)

OŚWIADCZENIE

Świadomy/a odpowiedzialności karnej za składanie fałszywych zeznań oświadczam, że przedkładana praca magisterska na temat:

Zarządzanie ruchem pakietów w sieciach komputerowych opartych na protokole IP.

została napisana przeze mnie samodzielnie.

Jednocześnie oświadczam, że ww. praca:

- nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. z 2000 r. Nr 80, poz. 904, z późniejszymi zmianami) oraz dóbr osobistych chronionych prawem cywilnym, a także nie zawiera danych i informacji, które uzyskałem/am w sposób niedozwolony,
- nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadawaniem dyplomów wyższej uczelni lub tytułów zawodowych.

Jestem także świadomy/a, że praca zawiera rezultaty stanowiące własność intelektualną Politechniki Łódzkiej, które nie mogą być udostępniane innym osobom i instytucjom bez zgody Uczelni.

.....
(PODPIS STUDENTA)