SPOŁECZNA WYŻSZA SZKOŁA
PRZEDSIĘBIORCZOŚCI I ZARZĄDZANIA W ŁODZI

KIERUNEK STUDIÓW: INFORMATYKA

Krzysztof Gajdzicki
Nr albumu 50028

PROTOKOŁY ROUTINGU W SIECI PRZEDSIĘBIORSTWA Z WYKORZYSTANIEM URZĄDZEŃ CISCO

Praca inżynierska napisana
w Instytucie Technologii
Informatycznych pod kierunkiem
dr hab. inż. Marka Orzyłowskiego

Przyjmuję pracę do obrony: ……
Termin obrony: ……
Recenzent: ……....

Łódź 2011

Wstęp

Sieci komputerowe w wielu przedsiębiorstwach ulegają poważnym zmianom. Koniecznym krokiem stało się zapewnienie dostępu do dużej ilości danych. Sieć przedsiębiorstwa musi zapewnić dostęp do informacji i usług wielu użytkownikom. Pracownicy potrzebują dostępu do danych dotyczących sprzedaży, marketingu, procesów produkcyjnych, niezależnie od tego, czy dane przechowywane są na lokalnych serwerach, czy w środowiskach rozproszonych. Współczesny model sieci komputerowej musi spełniać cel biznesowy – korzystanie z sieci musi zapewnić przedsiębiorstwu zwiększenie swoich dochodów, podnieść wydajność pracowników oraz zapewnić bezpieczeństwo danych. W ostatnim czasie ważnym elementem w działaniu przedsiębiorstwa stały się aplikacje sieciowe umożliwiające pracę zarówno pracownikom wewnątrz przedsiębiorstwa jak i pracownikom mobilnym. Usprawniono procesy komunikacyjne z wykorzystaniem telefonii internetowej i wideokonferencji. Nie byłoby to możliwe gdyby nie rozwój technologii przesyłania danych. Do niedawna sieci telekomunikacyjne i sieci transmisji danych działały jako oddzielne sieci, jednakże rozwój nowych protokołów komunikacyjnych wpłynął na to, iż współczesne sieci stają się sieciami konwergentnymi. Od współczesnej sieci komputerowej wymaga się, aby była niezawodna. Są przedsiębiorstwa, dla których niedopuszczalna jest choćby krótkotrwała awaria i niedostępność sieci. Jeżeli już w sieci dojdzie do awarii, współczesna sieć w przedsiębiorstwie powinna charakteryzować się możliwością szybkiego powrotu do stanu normalnej pracy, szczególnie wymaga się od sprzętu sieciowego i protokołów odporności na uszkodzenia i wysokiej dostępności. Bardzo ważną cechą jest dla wielu przedsiębiorstw możliwość kontynuowania pracy po wystąpieniu klęsk żywiołowych. Utrata części sprzętu infrastruktury sieciowej nie powoduje całkowitego braku możliwości korzystania z usług sieciowych.

Spełnienie powyższych wymagań i osiągnięcie wymienionych celów możliwe jest między innymi dzięki zastosowaniu we współczesnych sieciach przedsiębiorstwa protokołów routingu dynamicznego, oraz odpowiedniej konfiguracji urządzeń, na których te protokoły będą mogły działać i realizować stawiane przed nimi wymagania.

Cel i zakres pracy

Celem pracy jest przedstawienie wybranych protokołów routingu dynamicznego i możliwości zastosowania ich we współczesnej sieci przedsiębiorstwa. Przedstawione zostaną możliwości poszczególnych protokołów routingu w zależności od typu sieci i stawianych wymagań. Protokoły te zostaną zaimplementowane na routerach firmy Cisco. Ze względu na fakt, iż tematyka protokołów routingu dynamicznego jest rozległa, zawartość merytoryczna pracy została ograniczona do takich protokołów routingu dynamicznego jak: RIP, EIGRP, OSPF, IS-IS. Zostanie przedstawiony routing statyczny, który również jest wykorzystywany w sieciach, w których funkcjonują protokoły routingu dynamicznego. Zostaną przedstawione sposoby redystrybucji tras pomiędzy różnymi protokołami routingu.

Część praktyczna pracy zawiera konfigurację sieci komputerowej wykonaną z wykorzystaniem symulatora sieci Packet Tracer firmy Cisco. W sieci skonfigurowano i uruchomiono następujące protokoły routingu: RIP, EIGRP, OSPF, topologia została tak zaprojektowana, aby mogła odwzorować rzeczywiste problemy występujące w sieciach produkcyjnych przedsiębiorstw. Wiele sieci przedsiębiorstw budowanych było stopniowo, przedsiębiorstwa przekształcały się, następowały połączenia różnych przedsiębiorstw na skutek zmieniających się warunków rynkowych. Sytuacje takie stawały się wyzwaniem dla działów IT, które miały za zadanie szybkie połączenie różnych sieci w jedną wspólną sieć przedsiębiorstwa. Takie czynniki zostały uwzględnione w przedstawianej przykładowej sieci przedsiębiorstwa.. W części praktycznej są zamieszczone i omówione tablice routingu poszczególnych routerów, pokazane drogi przemieszczania się pakietów do sieci docelowych, w zależności od zmian zachodzących w topologii sieci. Dokonano analizy działania wybranych protokołów, zamieszczono listingi wyników działania wybranych poleceń konfiguracyjnych systemu Cisco IOS.

Rozdział 1. Routery i routing – podstawy

Routery to urządzenia, których zadaniem jest przesyłanie pakietów do sieci zarówno lokalnych jak i odległych poprzez określenie najlepszej trasy do wysłania pakietów oraz przekazanie tych pakietów w kierunku celu [2]. Aby pakiety zostały prawidłowo przesłane router musi posiadać informacje o trasie do miejsca przeznaczenia. Router wybiera najlepszą trasę do przekazania pakietu na podstawie danych zgromadzonych w tablicy routingu [1]. Na przekazywanie przez router pakietów składają się dwie czynności [1]:

- proces wyznaczania trasy
- proces przełączania

Router odbierając pakiet na swoim interfejsie sprawdza docelowy adres IP i przeszukuje swoją tablicę routingu w celu odnalezienia adresu sieciowego najbardziej zbliżonego do adresu docelowego. Wpis w tablicy routingu zawiera również informację o interfejsie sieciowym, poprzez który należy wysłać pakiet. Router decyduje o przekazaniu pakietu w kierunku celu w warstwie 3 modelu OSI, jednakże uczestniczy również w procesach warstwy 1 i 2 modelu OSI. Router odbiera na swym interfejsie strumień bitów, które są dekodowane i następnie przesyłane do warstwy 2 gdzie następuje proces dekapsulacji ramki. Następuje porównanie przez router adresu docelowego ramki łącza danych, czy zgadza się z adresami – w tym również grupowym i rozgłoszeniowym interfejsu odbierającego routera. Jeżeli adresy są zgodne część informacji zawartej w ramce przekazywana jest do warstwy trzeciej, gdzie router decyduje o routingu. Następuje proces odwrotny, router enkapsuluje pakiet w nową ramkę warstwy 2 i wysyła ją poprzez interfejs wyjściowy, jako strumień bitów [1].

1.1 Tablica routingu

Tablica routingu to struktura danych znajdujący się w pamięci operacyjnej routera, w którym przechowywane są informacje o drogach do sieci połączonych bezpośrednio oraz sieci zdalnych [2]. Głównym celem tablicy routingu jest dostarczenie routerowi tras do różnych sieci docelowych. Tablica routingu składa się z adresów sieci połączonych bezpośrednio, adresów sieci zdalnych, skonfigurowanych statycznie i znalezionych

dynamicznie. W tablicy routingu jeden wpis odpowiada grupie urządzeń, które współdzielą tę samą sieć lub przestrzeń adresową [1].

Sieci połączone bezpośrednio – to sieci, w których docelowy adres IP pakietu należy do sieci, która jest bezpośrednio połączona z interfejsem routera – pakiet jest bezpośrednio przekazywany do celu.

Sieci zdalne – to sieci, w których pakiet, aby dotrzeć do celu jest przekazywany do innych routerów. Docelowy adres IP nie należy do sieci podłączonej bezpośrednio.

Brak ustalonej trasy – to sytuacja, w której docelowy adres IP nie należy do sieci połączonej bezpośrednio i nie należy do sieci zdalnej a router nie ma trasy domyślnej. W takiej sytuacji pakiet jest odrzucany.

Poprawność tablicy routingu opiera się na trzech zasadach [1]:

- Router podejmuje decyzje niezależnie od innych routerów. Podstawą podjęcia decyzji są informacje zawarte w tablicy routingu
- Informacja zawarta w tablicy routingu jednego z routerów nie jest tożsama z informacjami zawartymi w tablicach routingu innych routerów.
- Znajomość trasy przez router z jednej sieci do drugiej nie jest informacją o trasie powrotnej.

Tworzenie i aktualizacja tablicy routingu możliwa jest poprzez statyczne tworzenie i usuwanie wpisów przez administratora - tzw. routing statyczny, lub w sposób automatyczny za pomocą protokołów routingu dynamicznego [2]. Trasa statyczna zawiera adres sieciowy i maskę podsieci sieci zdalnej oraz adres IP routera następnego skoku, bądź interfejsu wyjściowego. Kiedy w tablicy routingu znajduje się wpis trasy do sieci zdalnej, pojawiają się dodatkowe informacje - metryka oraz odległość administracyjna.

1.2 Metryka

Metryka – jest to wartość używana przez protokołu routingu w celu ustalenia kosztu dotarcia do sieci docelowych. Metryka jest sposobem porównywania lub mierzenia i służy do wyznaczenia potencjalnej drogi wtedy, gdy do sieci docelowej wiedzie wiele różnych dróg [1]. Każdy z protokołów routingu dynamicznego inaczej oblicza swoją metrykę. Metryka stosowana przez jeden protokół routingu nie jest porównywalna z metryką

stosowaną przez inny protokół routingu. Protokół RIP jako metrykę wykorzystuje liczbę skoków, protokół EIGRP wykorzystuje szerokość pasma i opóźnienie a OSPF wykorzystuje koszt interfejsu [3]. Dwa różne protokoły routingu, które używają różnych metryk mogą na ich podstawie wybrać inną drogę do tej samej sieci docelowej [1].

Metryki używane w protokołach routingu zawierają niżej wymienione wartości [1]:

- Liczba skoków – wartość metryki, która zawiera liczbę routerów, poprzez które musi przejść pakiet, aby dotrzeć do sieci docelowej.
- Szerokość pasma – droga do sieci docelowej wybierana jest poprzez łącza z największą przepustowością.
- Obciążenie – wartość metryki, w której uwzględniane jest natężenie ruchu w danym łączu
- Opóźnienie – wartość metryki, w której uwzględniany jest czas, w jakim pakiet dotrze do sieci docelowej
- Niezawodność – wartość metryki, w której szacowane jest prawdopodobieństwo wystąpienia awarii łącza obliczane na podstawie licznika błędów interfejsu lub awarii łącza, które wystąpiły w przeszłości.
- Koszt – wartość metryki ustalana przez system operacyjny routera lub przez administratora sieci, która wskazuje preferencje dla danej trasy. Koszt może przedstawiać metrykę, połączenie metryk lub regułę.

Protokoły ustalając najlepszą trasę, wybierają trasę z najniższą metryką [1].

1.3 Odległość administracyjna

Odległość administracyjna – to liczba całkowita z przedziału od 0 do 255 określająca pierwszeństwo routingu. Im niższa wartość, tym wyższy jest priorytet źródła routingu. Odległość administracyjna 0 posiada sieć połączona bezpośrednio, natomiast wartość odległości administracyjnej 255 oznacza, iż trasa jest niewiarygodna i router nie zainstaluje jej w swojej tablicy routingu [1]. Każde źródło routingu, czyli trasy statyczne i trasy połączone bezpośrednio mają swój priorytet. Jeżeli router zna drogę do sieci docelowej z dwóch lub więcej źródeł routingu to wybiera tą z niższą wartością administracyjną.

Źródło trasy	Odległość administracyjna
Połączona bezpośrednio	**0**
Statyczna	**1**
Trasa sumaryczna EIGRP	**5**
Zewnętrzna BGP	**20**
Wewnętrzna EIGRP	**90**
IGRP	**100**
OSPF	**110**
IS-IS	**115**
RIP	**120**
Zewnętrzna EIGRP	**170**
Wewnętrzna BGP	**200**

Tabela 1. Domyślne odległości administracyjne.

Opracowanie własne na podstawie [1]

W tabeli 1 zawarte są domyślne odległości administracyjne dla wybranych protokołów routingu.

Z tabeli 1 wynika że trasa statyczna posiada wartość administracyjną 1 i ma pierwszeństwo routingu na d protokołami routingu dynamicznego.

Rozdział 2. Routing statyczny

W sytuacji, kiedy trasa do sieci zdalnej zostaje umieszczona w tablicy routingu poprzez wydanie polecenia konfiguracyjnego przez administratora, nazywa się routingiem statycznym [2]. Po skonfigurowaniu takiej trasy system operacyjny routera umieszcza w tablicy routingu informacje na temat maski podsieci, interfejsu wyjściowego oraz adresu IP routera następnego skoku. Routing statyczny można konfigurować za pomocą adresu IP interfejsu routera następnego skoku, w tym przypadku proces tablicy routingu musi przyporządkować ten adres IP do interfejsu wyjściowego routera. Jeżeli routing statyczny konfigurowany jest na szeregowych łączach punkt – punkt, korzystniejszym rozwiązaniem jest wprowadzenie do tablicy routingu zamiast adresu IP następnego skoku, tylko interfejsu wyjściowego [1]. Proces przeszukiwania tablicy routingu jest bardziej efektywny, gdy trasy statyczne mają zdefiniowane tylko interfejsy wyjściowe [1]. Różnica pomiędzy siecią punkt – punk a siecią wielodostępowią np. Ethernet jest taka, że w łączu punkt – punkt po drugiej stronie łącza znajduje się tylko jedno urządzenie [6]. W przypadku sieci wielodostępowych wiele różnych urządzeń może wspólnie wykorzystywać tę samą sieć wielodostępową [5]. W związku z tym tylko informacja o ethernetowym interfejsie wyjściowym dla trasy statycznej jest niewystarczająca do tego, aby router mógł ustalić, które urządzenie jest następnym skokiem. Sieci punkt – punkt, które używają protokołów takich jak PPP lub HDLC w procesie przekazywania pakietów nie stosują adresu IP następnego skoku [4]. Przekazywany pakiet IP jest inkapsulowany w ramkę PPP warstwy 2 z adresem rozgłoszeniowym docelowym warstwy 2. W sieciach wielodostępowych, np. Ethernet dla routingu statycznego należy podać adres IP i interfejs wyjściowy [1].

W tablicy routingu może zostać umieszczony wpis dotyczący konkretnej sieci docelowej, może również znajdować się wpis bardziej ogólny - trasa sumaryczna lub domyślna. Dzięki temu następuje zmniejszenie rozmiaru tablicy routingu i proces przeszukiwania tablicy routingu jest wydajniejszy. Zamiast wielu można użyć jednej trasy sumarycznej [2]. Trasa domyślna reprezentuje wszystkie trasy – jeżeli nie istnieją w tablicy routingu z lepszym dopasowaniem, zostanie wybrana trasa domyślna. Składnia domyślnej trasy statycznej zawiera jako adres sieciowy 0.0.0.0 z maską 0.0.0.0. Wartość odległości administracyjnej dla tras tworzonych statycznie równa jest 1 (Tabela 1).

Jeżeli zajdzie potrzeba modyfikacji wcześniej skonfigurowanej trasy statycznej należy w pierwszej kolejności usunąć istniejącą trasę statyczną a następnie skonfigurować nową trasę statyczną.

Routing statyczny znajduje zastosowanie w niewielkich sieciach, co do których rozbudowa nie jest przewidywana. Zaletami są: niewielkie zapotrzebowanie na zasoby sprzętowe routera, stosunkowa łatwość konfiguracji, jest bezpieczniejszy od protokołów routingu dynamicznego, jest przewidywalny tzn. trasa do celu jest zawsze taka sama.

Wadą routingu statycznego jest to, iż nie jest skalowalny, złożoność konfiguracji rośnie wraz z rozmiarem sieci. Każda zmiana topologii sieci wymaga interwencji administratora. Prawidłowe wdrożenie routingu statycznego wymaga pełnej wiedzy o topologii sieci [1].

Rozdział 3. Protokoły routingu dynamicznego – podstawy

Protokół routingu dynamicznego to zestaw komunikatów, procesów i algorytmów, które służą do komunikacji między routerami, pozwalają na wymianę informacji o sieciach między routerami oraz umożliwiają budowanie tablicy routingu routerów [1]. Protokoły routingu dynamicznego umożliwiają wymianę informacji o dostępności i stanie sieci zdalnych. Protokoły routingu dynamicznego nie tylko wyznaczają najlepszą drogę do celu, ale ustalają nową drogę, jeżeli zmieni się topologia, w związku, z czym mogą na bieżąco reagować na zachodzące zmiany w sieci co daje im przewagę nad routingiem statycznym [1].

Do głównych zadań protokołów routingu dynamicznego należy:

- Wykrywanie sieci
- Utrzymywanie aktualnej informacji o trasach do danych sieci
- Wybór najlepszej drogi do docelowej sieci
- Znalezienie nowej drogi do docelowej sieci w przypadku, kiedy droga bieżąca przestanie działać.

Algorytm protokołu routingu wyznacza najlepszą drogę do sieci docelowej na podstawie metryki. Metryka ta jest różnie obliczana dla różnych protokołów routingu. Metryką może być liczba skoków – dla protokołu RIP, lub szerokość pasma - dla protokołu OSPF [1].

Ważnym parametrem protokołów routingu jest tzw. czas zbieżności, czyli czas, w jakim wszystkie tablice routingu routerów zostaną doprowadzone do stanu spójności. Będzie to miało miejsce wtedy, gdy wszystkie routery w tej samej domenie routingu będą miały pełną informację o sieci [1].

3.1 Podział protokołów routingu dynamicznego.

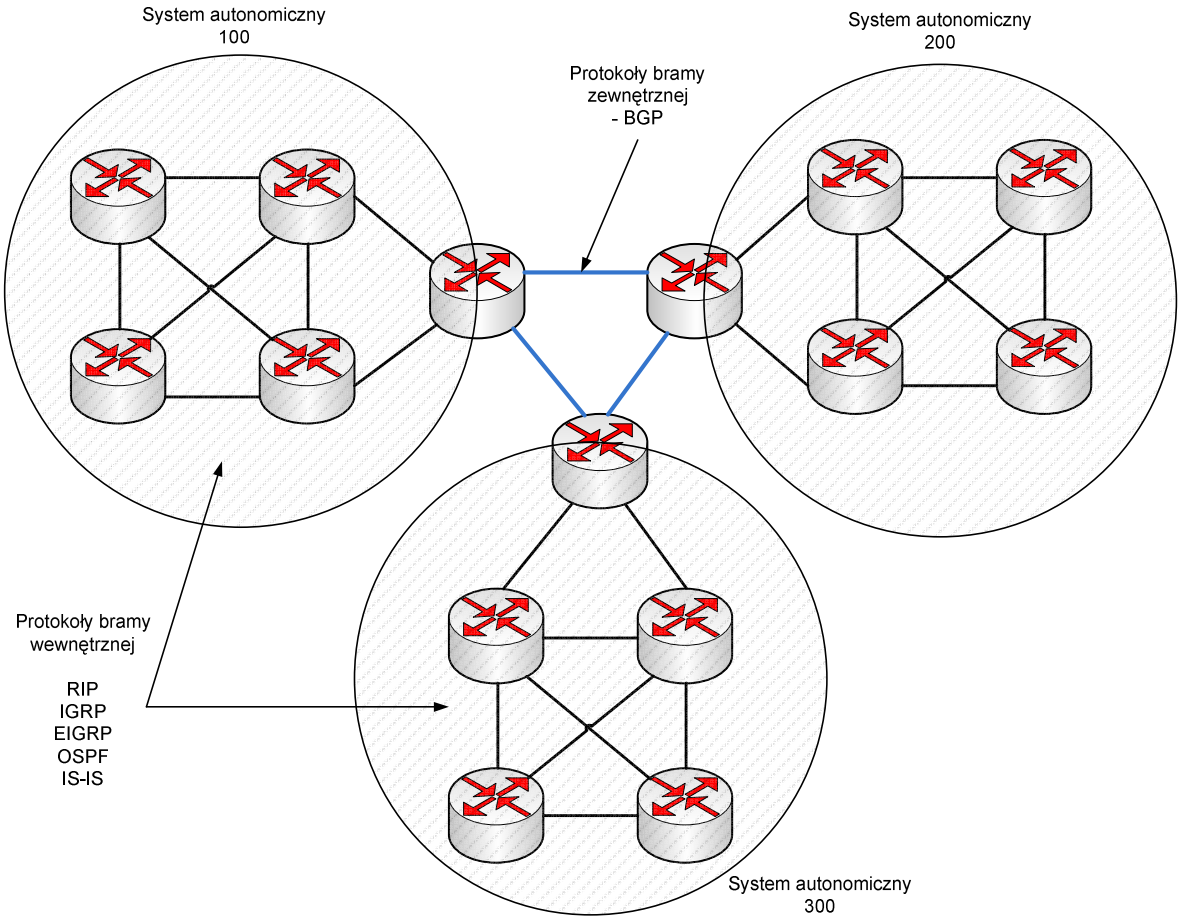
Protokoły routingu można podzielić na podstawie różnych ich właściwości. W zależności od miejsca w sieci, w którym działają, protokoły routingu dynamicznego dzielą się na:

3.1.1 Protokoły IGP i EGP

Protokoły bramy wewnętrznej – IGP – Interior Gateway Protocols – to zbiór protokołów routingu dynamicznego działających wewnątrz systemu autonomicznego – AS.

Protokoły bramy zewnętrznej – EGP – Exterior Gateway Protocols - to zbiór protokołów routingu dynamicznego działających pomiędzy systemami autonomicznymi

System autonomiczny - AS, to sieć pod kontrolą pojedynczej organizacji. System autonomiczny zwany jest również domeną routingu. System autonomiczny składa się z wielu sieci kontrolowanych przez jedną organizację.



Rys 1. Protokoły IGP i protokoły BGP

opracowanie własne na podstawie [1]

Rysunek 1 przedstawia schemat zastosowania protokołów IGP oraz EGP. Protokoły IGP stosowane są wewnątrz systemów autonomicznych. Przykładem protokołów IGP są: RIP, EIGRP, OSPF, IS-IS. Protokoły EGP stosowane są pomiędzy systemami autonomicznymi należącymi do różnych organizacji. Przykładem protokołu EGP jest protokół BGP, który obecnie jest jedynym protokołem EGP obecnie stosowanym [2].

3.1.2 Protokoły wektora odległości i stanu łącza.

Protokoły wektora odległości - to protokoły w których trasy do sieci docelowych określane są jako wektory odległości i kierunku. Odległość zdefiniowana jest za pomocą metryki, której wartością jest liczba skoków, czyli liczba routerów poprzez które musi przebyć pakiet danych aby dotrzeć do sieci docelowej, a kierunek to adres IP routera następnego skoku lub interfejs wyjściowy routera [1].

Protokoły stanu łącza – to protokoły, które wykorzystują informacje o stanie łączy routerów, na których są uruchomione. Informacja ta składa się z [1]:

- adresu IP i maski podsieci interfejsu,
- typu sieci – np. Ethernet, PPP,
- kosztu łącza,
- danych o sąsiednich routerach na tym samym łączu.

Protokoły wektora trasy – nie stosują metryk, lecz tzw. Atrybuty. Atrybuty są związane z konkretną siecią IP i są przesyłane razem z informacją o tej sieci. Protokołem wektora trasy jest protokół BGP [3].

3.1.3 Klasowe i bezklasowe protokoły routingu.

Klasowe protokoły routingu – to protokoły, które w aktualizacjach routingu nie wysyłają informacji o masce podsieci. Pierwsze protokoły routingu były protokołami klasowymi. Związane to było z faktem, iż adresy sieciowe były przyporządkowywane na podstawie klas. Maska podsieci była ustalana na podstawie pierwszego oktetu adresu sieciowego, w związku z czym protokół routingu w swoich aktualizacjach nie musiał umieszczać informacji o masce podsieci. Klasowe protokoły routingu nie obsługują masek

VLSM - Variable Length Subnet Mask – masek podsieci o zmiennej długości. Protokoły klasowe routingu nie obsługują również sieci nieciągłych. Sieci nieciągłe to sieci, w których adresowanie nie ma systemu hierarchicznego. Sieć nieciągła to taka sieć, która składa się z sieci klasowej przedzielonej inną siecią klasową [1].

Bezklasowe protokoły routingu – to protokoły, które w aktualizacjach routingu wraz z adresem IP zamieszczają maskę podsieci. Dzięki temu mogą być stosowane w sieciach wykorzystujących VLSM oraz w sieciach nieciągłych [1].

Ponadto protokoły routingu dynamicznego posiadają pewne cechy właściwe dla poszczególnych protokołów, co umożliwia ich porównywanie.

3.2 Właściwości protokołów routingu dynamicznego.

Protokoły routingu dynamicznego cechują się pewnymi właściwościami, które predysponują je do zastosowania w różnych sieciach, w zależności od topologii, wielkości sieci, zastosowanych urządzeń, oraz od stanu wiedzy administratorów, którzy będą dane protokoły wdrażać i rozwiązywać występujące problemy w ich działaniu.

Protokoły routingu dynamicznego posiadają następujące właściwości [1]:

- Skalowalność – określa rozmiar sieci, w jakiej dany protokół routingu może być stosowany.
- Zbieżność – czas, w jakim tablice routingu wszystkich routerów będących we wspólnej domenie routingu osiągną stan spójności.
- Klasowość lub bezklasowość – protokoły, które w wysyłanych aktualizacjach tablicy routingu zamieszczają bądź nie zamieszczają informacji o masce podsieci.
- Zapotrzebowanie na zasoby sprzętowe – protokoły routingu do poprawnego działania wymagają odpowiedniej ilości pamięci RAM oraz mocy obliczeniowej procesora.
- Wdrożenie i utrzymanie – poszczególne protokoły routingu wymagają odpowiedniego poziomu wiedzy od administratora w celu poprawnego ich skonfigurowania oraz rozwiązywania problemów z ich działaniem. W zależności od protokołu routingu wiedza potrzebna do skonfigurowania i wdrożenia może być mniej lub bardziej zaawansowana.

Protokoły różnią się skalowalnością i wydajnością . Niektóre z protokołów zaprojektowano dla małych sieci, niektóre dobrze pracują w sieciach, w których rzadko

następują zmiany w topologii i mają trudności ze zbieżnością w sytuacji kiedy nastąpi zmiana w topologii. W zależności od zastosowanego protokołu routingu należy zapewnić routery o odpowiednich zasobach sprzętowych, aby proces routingu realizowany był prawidłowo.

Rozdział 4. Protokoły routingu wektora odległości

W protokołach routingu wektora odległości informacja o trasach określana jest jako wektor odległości i kierunku [2]. Odległość reprezentowana jest jako metryka, czyli liczba skoków poprzez poszczególne routery aby dotrzeć do sieci docelowej, a kierunek to adres IP routera następnego skoku lub interfejs wyjściowy [1]. Routery z zaimplementowanym protokołem routingu wektora odległości nie znają całej topologii sieci [2]. Router ma tylko informację, w jakim kierunku należy wysłać pakiet, czyli adres IP lub interfejs wyjściowy i odległość do sieci docelowej. Protokoły routingu wektora odległości posiadają klika cech wspólnych. Aktualizacje okresowe wymieniane są między routerami w regularnych interwałach czasowych – 90 sekund dla protokołu IGRP, 30 sekund dla protokołu RIP [1]. Wyjątkiem jest protokół EIGPR, gdzie nie są wysyłane aktualizacje okresowe. Tylko zmiany informacji o trasach powodują wysłanie aktualizacji. Dla protokołu RIPv1 aktualizacje wysyłane są na adres rozgłoszeniowy - 255.255.255.255, a dla protokołu RIPv2 na adres multicast. Routery sąsiadujące, na których skonfigurowany jest ten sam protokół routingu analizują i przetwarzają te informacje. Inne urządzenia pracujące w sieci również otrzymują i analizują aktualizacje, aż do warstwy 3, po czym je odrzucają. Aktualizacje powodują obciążanie łącza, jeżeli topologia sieci nie zmienia się przez długie okresy czasu, aktualizacje okresowe są wysyłane powodując niepotrzebne przetwarzanie i marnotrawienie zasobów procesorów. Niektóre protokoły wektora odległości np. RIPv2 i EIGRP używają adresów multicast zamiast adresu brodacast [2].

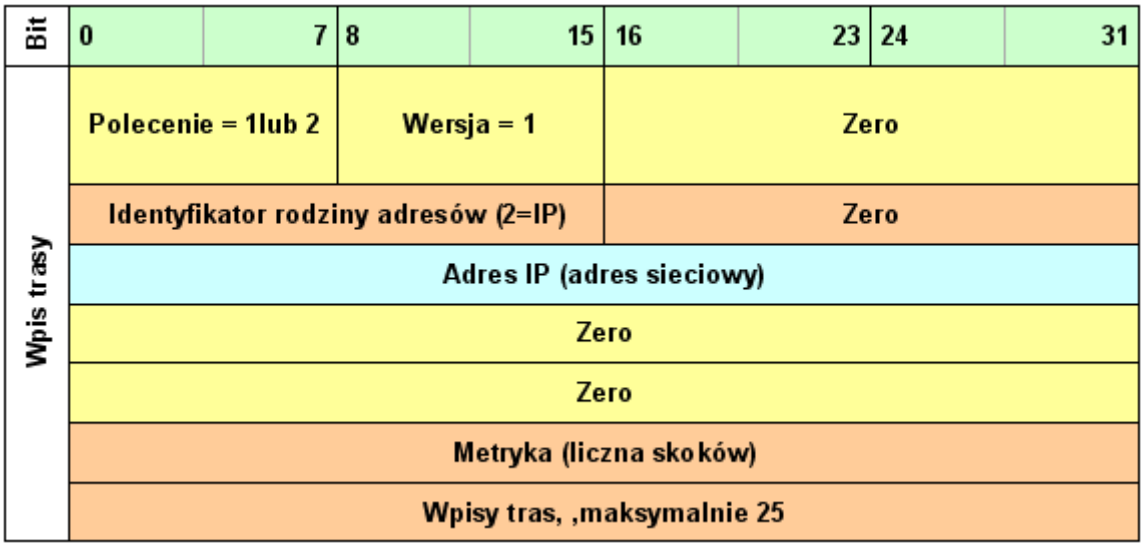
4.1 RIP – Routing Information Protocol.

RIP jest najstarszym protokołem routingu wektora odległości. Protokół RIP powstał na bazie protokołu GWINFO – Gateway Information Protocol firmy Xerox. Następnie RIP został wdrożony w systemie BSD. W 1988 roku protokół RIP został znormalizowany w dokumencie RFC 1058. W kolejnych latach powstały kolejne wersje protokołów RIP: RIP v2 w 1994r oraz RIPng w 1997r [1].

RIP jako metryki używa liczbę skoków, trasy z metryką powyżej 15 uznawane są za nieosiągalne. Aktualizacje tablicy routingu wysyłane są na adres broadcast 255.255.255.255 w segmencie UDP z numerem portu źródłowego i docelowego 520, z interwałem czasowym 30 sekund [2].

4.1.1 RIPv1

RIP jest znormalizowanym protokołem routingu wektora odległości, może być stosowany w sieciach, w których wykorzystywane są routery różnych producentów. RIPv1 jest klasowym protokołem wektora odległości dla IPv4 [1]. Na rysunku 2 przedstawiono format komunikatu RIPv1.



Rys 2. Format komunikatu RIPv1

Opracowanie własne na podstawie [1]

Opis pól komunikatu RIPv1:

Polecenie – wartość 1 dla żądania, wartość 2 dla odpowiedzi

Wersja – wartość 1 dla RIPv1, 2 dla RIPv2

Identyfikator – wartość 2 dla IP

Adres IP – adres docelowy, może być adresem sieci, podsieci lub hosta

Metryka – Liczba skoków, wartość z przedziału 1 – 16. Router wysyłający zwiększa metrykę przed wysłaniem komunikatu.

W komunikacie RIP (Rys.2) w polu „Polecenie” określony jest typ komunikatu, pole to może przyjmować wartość 1 dla żądania lub wartość 2 dla komunikatu odpowiedzi. Pole „Wersja” określa wersję protokołu RIP. Trzecie z pól pozostaje puste, zostało ono zarezerwowane na rozbudowę protokołu. Pola „Identyfikator”, „Adres IP” i „Metryka” zawierają informacje o trasie docelowej oraz skojarzoną z nią metryką. Pojedyncza aktualizacja RIP maksymalnie może zawierać do 25 wpisów tras. Maksymalny rozmiar komunikatu RIP to wartość 512 bajtów [1].

RIP stosuje dwa typy komunikatów: komunikat żądania i komunikat odpowiedzi. Każdy z interfejsów, na którym uruchomiony jest protokół RIP po uruchomieniu wysyła komunikat "żądanie” po to, aby wszystkie sąsiadujące routery wysłały pełne tablice routingu. Sąsiednie routery z protokołem RIP wysyłają komunikat „odpowiedź”. Router odbierający analizuje każdy wpis, jeżeli wpis jest nowy, router instaluje trasę w tablicy routingu. Po zaktualizowaniu tablicy routingu router wysyła aktualizację wyzwalaną z tablicą routingu do swoich sąsiadów [1].

RIPv1 w aktualizacjach nie umieszcza informacji o masce podsieci. Ze względu na to ograniczenie protokół RIPv1 nie może być stosowany w sieciach adresowanych z wykorzystaniem technologii VLSM [2]. Kiedy router odbiera aktualizację routingu musi ustalić maskę sieci docelowej. Jeżeli sieć docelowa należy do tej samej sieci ,co aktualizacja RIPv1 jako maskę podsieci wybiera maskę podsieci interfejsu odbierającego. Jeżeli adres sieci docelowej należy do innej sieci klasowej niż interfejs odbierający, zostaje zastosowana domyślna maska klasowa.

4.1.2 RIPv2

RIPv2 został opisany w dokumencie RFC 1723, RIPv2 jest enkapsulowany w segmencie UDP, do komunikacji wykorzystuje port 520. Podstawowy format komunikatu RIPv2 (Rys.3) jest podobny do komunikatu RIPv1, jednakże w formacie protokołu RIPv2 zostały zdefiniowane dotychczas niewykorzystane pola. Zostało zdefiniowane pole „Maska podsieci”, które zawiera 32 bitową maskę podsieci. Kolejnym rozszerzeniem jest pole „Następny skok”, które służy do zidentyfikowania lepszego adresu następnego skoku o ile taki istnieje. Jeżeli pole to zawiera adres IP 0.0.0.0 świadczy to o fakcie, że najlepszym adresem jest adres routera wysyłającego [1].

Rys.3 Format komunikatu RIPv2

Opracowanie własne na podstawie [1]

Routery z uruchomionym protokołem RIP regularnie wysyłają do swoich sąsiadów pełne tablice routingu w regularnych odstępach czasu [3]. Domyślnie protokół RIPv2 podobnie jak RIPv1 dokonuje automatycznego podsumowania sieci na granicach dużych sieci [1]. Automatyczne podsumowanie może zostać wyłączone przez administratora poprzez wydanie polecenia konfiguracyjnego „no auto-summary". Wyłączenie automatycznego podsumowania jest możliwe tylko dla protokołu RIPv2.[2]. Wyłącznie automatycznego podsumowania powoduje, iż protokół RIPv2 nie podsumowuje sieci do adresów klasowych na routerach brzegowych.. W aktualizacjach tablicy routingu umieszczone zostają wszystkie podsieci i maski podsieci.. Każda podsieć i maska mają własne wpisy, w których zawarte są interfejs wyjściowy i adres następnego skoku do sieci docelowej. Aktualizacje w przypadku protokołu RIPv2 wysyłane są na adres multicast 224.0.0.9, inaczej niż w przypadku protokołu RIPv1, w którym aktualizacje wysyłane są na adres rozgłoszeniowy 255.255.255.255. Zastosowanie adresu multicast umożliwiło zmniejszenie zajętości pasma sieciowego [1]. Urządzenia na których nie jest uruchomiony protokół RIPv2 odrzucają datagram w warstwie łącza danych, nie analizując jego zawartości. Protokół RIPv2 jest protokołem bezklasowym, czyli takim, który może przenosić informacje o masce podsieci. Sieć i maska podsieci są jawnie określone w każdej aktualizacji routingu. [1], czego potwierdzeniem jest format komunikatu RIPv2 (Rys.3).

Protokół RIPv2 może stosować uwierzytelnienie informacji o trasach, co wpływa na zwiększenie bezpieczeństwa. Routery przyjmują informacje o trasach tylko od routerów na których skonfigurowano te same parametry uwierzytelnienia [3].

4.1.3 Sposoby zapobiegania pętlom routingu w protokole RIP

Zagrożeniem w sieciach, w których uruchomione są protokoły routingu dynamicznego są pętle routingu [1]. Pętla routingu występuje wtedy, gdy pakiet krąży pomiędzy routerami nie docierając do sieci docelowej.

Przyczyny powstawania pętli routingu [1]:

- niewłaściwa konfiguracja tras statycznych
- niewłaściwa konfiguracja redystrybucji tras
- niespójne tablice routingu z powodu wolnej zbieżności w zmieniającej się topologii sieci.

Skutkiem powstałej w sieci pętli routingu jest spadek wydajności sieci a nawet przerwa w działaniu sieci. Pętle routingu zdarzają się znacznie częściej w sieciach z protokołami wektora odległości niż w sieciach opartych o protokoły stanu łącza [3]. Aby zapobiegać powstawaniu pętli routingu należy przyspieszyć osiąganie stanu zbieżności sieci po zmianie w topologii. Mechanizmy, które zapobiegają powstawaniu pętli routingu to [1]:

- ustawienie maksymalnej metryki
- liczniki wstrzymania
- podzielony horyzont
- zatrucie trasy
- wyzwalane aktualizacje

Ustawienie maksymalnej metryki polega na zwiększenie wartości metryki do nieskończoności. Dla protokołu RIP będzie to wartość 16 skoków [3].

Liczniki wstrzymania uniemożliwiają zwykłym komunikatom aktualizacji ponownie zainstalować trasę, która mogła ulec awarii. Liczniki wstrzymania powodują, iż routery powstrzymują się przez określony czas z wprowadzeniem zmian [1].

Metoda podzielonego horyzontu polega na tym, że router powinien ogłaszać sieci z interfejsu, na którym odebrał aktualizacje. Podzielony horyzont może zostać wyłączony przez administratora sieci [1].

Zatrucie trasy polega na oznakowaniu trasy jako nieosiągalnej w aktualizacjach routingu wysłanych do innych routerów za pomocą maksymalnej wartości metryki. Dla protokołu RIP jest to wartość 16 [1].

Aktualizacje wyzwalane to aktualizacje, które zostają wysyłane do innych routerów natychmiast, gdy router wykryje zmiany w topologii sieci [1].

4.2 IGRP - Interior Gateway Routing Protocol

Protokół IGRP – Interior Gateway Routing Protocol – jest to protokołem bramy wewnętrznej. Obecnie nie jest wykorzystywany, jednakże stanowił on podstawę do stworzenia protokółu EIGRP. Protokół jest protokołem własnościowym firmy Cisco, został wprowadzony do użycia w 1985 roku. Jako metryki używał szerokości pasma, opóźnienia, niezawodności i obciążenia. Algorytm zastosowany w tym protokole to algorytm Belmana – Forda i opierał się podobnie jak RIP na wysyłaniu aktualizacji okresowych. Znajdował zastosowanie w sieciach gdzie liczba skoków była większa niż 15 routerów. IGRP umożliwiał wyrównywanie obciążenia pomiędzy trasami o jednakowych i niejednakowych metrykach [3].

Protokół IGRP nie jest wykorzystywany od wersji 12.2 systemu Cisco IOS [1].

4.3 EIGRP - Enhanced Interior Gateway Routing Protocol

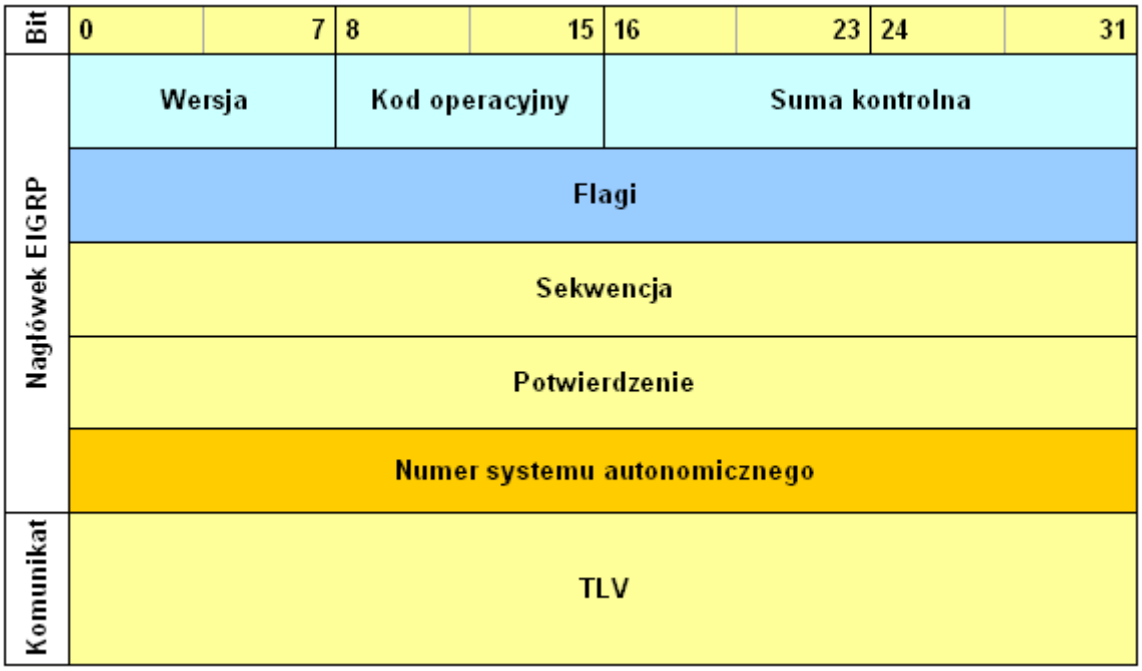
Protokół EIGRP – Enhanced Interior Gateway Routing Protocol jest bezklasowym protokołem routingu dynamicznego powstałym na podstawie klasowego protokołu IGRP. Jest protokołem własnościowym firmy Cisco, w związku z czym działa tylko na urządzeniach Cisco. Protokół został wprowadzony do użytku w 1992 roku wraz z wersją 9.21 systemu Cisco IOS [1].

Protokół EIGRP wykorzystuje protokół RTP – Reliable Transport Protocol, który może zapewnić niezawodne lub zawodne dostarczanie pakietów. Protokół EIGRP wykorzystuje do działania algorytm DUAL – Diffusing Update Algorithm, który zapewnia trasy wolne od pętli i trasy zapasowe. EIGRP tworzy z innymi routerami połączonymi bezpośrednio relacje sąsiedzkie, może działać jako protokół klasowy lub bezklasowy [4]. Pomimo, iż pozostaje protokołem wektora odległości, dzięki wykorzystaniu algorytmu

DUAL, protokół posiada pewne właściwości, których nie maja pozostałe protokoły wektora odległości [1]. Protokół EIGRP nie wysyła aktualizacji okresowych, do monitorowania połączeń z innymi routerami używa protokołu Hello. Aktualizacje wysyłane są wtedy, kiedy w sieci zajdzie zmiana topologii [4].

4.3.1 Format pakietu EIGRP

Na rysunku 4 przedstawiony jest format pakietu EIGRP



Rys. 4 Format pakietu EIGRP.

Opracowanie własne na podstawie [1]

Opis ważniejszych pól występujących w formacie pakietu EIGRP:

Kod operacyjny – wartość określająca typ pakietu EIGRP:

- Aktualizacja – wartość 1
- Zapytanie – wartość 3
- Odpowiedź – wartość 4
- Hello – wartość 5
- Acknowledge – wartość 8

Numer systemu autonomicznego – na jednym routerze Cisco może być uruchomionych wiele instancji protokołu EIGRP, w związku z czym numer systemu autonomicznego służy do identyfikacji poszczególnych instancji [1].

Pakiet EIGRP składa się z nagłówka EIGRP oraz komunikatu EIGRP – pole TLV – „Type/Length/Value". Nagłówek EIGRP i TLV są enkapsulowane w pakiecie IP. Nagłówek pakietu IP zawiera pole protokołu z ustawioną wartością 88 , co informuje że wewnątrz pakietu przenoszony jest EIGRP. Docelowym adresem IP jest adres grupowy 224.0.0.10. W sytuacji, kiedy pakiet EIGRP jest enkapsulowany w ramce ethernetowej adresem docelowym jest grupowy adres MAC 01-00-5E-00-00-0A [4].

Na rysunku 5 przedstawiono parametry TLV pakietu EIGRP:

Rys 5. Parametry TLV w pakiecie EIGRP

Opracowanie własne na podstawie [1]

Pola parametrów TLV (Rys.5) zawierają wagi, które służą do obliczania metryki. Domyślnie w protokole EIGRP metryka obliczana jest na podstawie dwóch wag: K1 – szerokość pasma, oraz K3 – opóźnienia. Pola te ustawione są na wartość 1. Pozostałe pola wag mają wartość 0 [1], i nie są brane pod uwagę podczas obliczania metryki EIGRP.

Czas wstrzymania jest czasem, przez jaki sąsiedni router z działającym protokołem EIGRP, który odbiera komunikat EIGRP będzie oczekiwał, zanim uzna router rozgłaszający ten pakiet za niedostępny. Domyślnie czas wstrzymania jest to trzykrotna wartość interwału hello, czyli 15 sekund w sieciach wielodostępowych i 180 sekund w sieciach NBMA [4]. Jeżeli czas wstrzymania się skończy EIGRP uznaje, że trasa jest nieczynna, a algorytm DUAL szuka nowej drogi.

Protokół EIGRP umożliwia routing nie tylko protokołu IP, lecz również IPX i AppleTalk. Możliwe jest to dzięki modułom PDM – Protocol Dependent Modules [3]. Aby możliwy był routing innych protokołów niż IP, EIGRP korzysta z protokołu RTP – Reliable Transport Protocol. Użycie tego protokołu jest koniecznie, ponieważ IPX i AppleTalk nie używają TCP/IP [7]. Protokół RTP może działać jako protokół dostarczający pakiety w sposób zawodny lub niezawodny [3]. Działanie niezawodne polega na tym, aby odbiorca wysyłał potwierdzenia otrzymanych pakietów. Pakiety mogą być wysyłane jako komunikaty typu unicast lub multicast na adres 224.0.0.10

Protokół EIGRP używa pięciu typów pakietów. Pakiety hello służą do wykrywania sąsiednich routerów i do tworzenia między nimi relacji sąsiedzkich. Pakiety te wysyłane są jako zawodne komunikaty multicast. Pakiety wysyłane są co pięć sekund. Pakiety aktualizacji EIGRP wysyłane są w sposób niezawodny, jako komunikaty multicast w sieciach wielodostępowych, lub jako komunikaty unicast w sieciach typu punkt-punkt [1].

Protokół EIGRP nie wysyła aktualizacji w stałych interwałach czasowych, lecz tylko w sytuacji, gdy zmieni się metryka dla trasy [4]. EIGRP nie wysyła całej tablicy routingu lecz aktualizacje przyrostowe o zmianach w trasie - są to aktualizacje częściowe. Aktualizacje te są ograniczone, ponieważ dotyczą tylko tych routerów, dla których te zmiany mają znaczenie. Dzięki temu zostaje zminimalizowane wykorzystanie pasma do wysyłania pakietów EIGRP [1].

4.3.2 Metryka protokołu EIGRP

Do obliczania metryki protokołu EIGRP mogą być wykorzystane: przepustowość pasma, opóźnienie, niezawodność, obciążenie łącza. W przypadku kiedy do obliczania metryki zostają wykorzystane wszystkie wartości K1 do K5 równanie na obliczenie metryki EIGRP ma postać (1):

$$\text{Metryka EIGRP} = [K1 * Bw + \frac{K2 * Bw}{256 - load} + K3 * delay] * [\frac{K5}{reliability + K4}] \quad (1)$$

Opracowanie na podstawie [8]

Opis symboli użytych we wzorze:

K1-K5 – wagi metryki EIGRP
Bw – przepustowość pasma
load – obciążenie
delay – opóźnienie
reliability – niezawodność

Bw = (10000000/Bw(i))*256 – gdzie Bw(i) jest najmniejszą przepustowością pasma interfejsów na drodze do sieci docelowej w kilobitach na sekundę [kb/s] [8]

delay = (delay(i)/10)*256 – gdzie delay(i) jest sumą opóźnień wszystkich interfejsów na drodze do sieci docelowej w mikrosekundach [8]

Przepustowość pasma to wartość wyrażona w kb/s.[1] Wartość przepustowości pasma niekoniecznie musi odzwierciedlać wartości rzeczywistej przepustowości pasma interfejsu. Zmiana tej wartości przez administratora nie zmienia faktycznej przepustowości pasma interfejsu. Opóźnienie, to czas, w jakim pakiet przebywa drogę wyrażony w mikrosekundach [1] Domyślne wartości opóźnienia dla różnych interfejsów przedstawione są w tabeli 2. Opóźnienie jest wartością statyczną, którą może zmienić administrator sieci. Niezawodność to wskaźnik częstości występowania awarii na danym łączu [1]. Jest to wartość mierzona dynamicznie na podstawie średniej ważonej z pięciominutowego pomiaru. Niezawodność wyrażana jest jako ułamek 255. Im wartość wyższa, tym łącze jest bardziej niezawodne. Obciążenie to wartość, która informuje o ilości ruchu w danym łączu, wyrażone jest jako ułamek liczby 255. Obciążenie uwzględnia dwie wartości – wartość wychodzącą – txload, oraz wartość wchodzącą – rxload [1]. Obciążenie mierzone jest na podstawie średniej ważonej z pięciominutowego okresu pomiaru.

Domyślnie do obliczenia metryki używane są tylko szerokość pasma i opóźnienie – wartość wag K1 i K3 ustawione na 1, . Pozostałe pola wag mają wartość 0 [1], i nie są brane pod uwagę podczas obliczania metryki EIGRP. W związku z powyższym, w równaniu (1)

ma metrykę EIGRP członów: $\frac{K2 * Bw}{256 - load}$ oraz $\frac{K5}{reliability + K4}$ nie bierze się pod uwagę [1] a równanie posiada następującą postać (2):

$$\boxed{\text{Metryka} \quad \text{EIGRP} \quad = Bw + delay} \quad (2)\ [8]$$

Przykład obliczenia metryki EIGRP znajduje się na stronie 51 w części praktycznej pracy.

W tabeli 2 przedstawiono domyślne wartości opóźnienia dla różnych interfejsów.

Nośnik	Opóźnienie w mikrosekundach
100M ATM	100
Fast Ethernet	100
FDDI	100
HSSI	20000
16M Token Ring	630
Ethernet	1000
T1 (domyślne szeregowe)	20000
512K	20000
DS0	20000
56K	20000

Tabela 2. Domyślne wartości opóźnienia dla różnych interfejsów.
Opracowanie własne na podstawie [1]

4.3.3 Algorytm protokołu EIGRP

Algorytmem używanym przez protokół EIGRP jest algorytm DUAL – Diffusing Update Algorithm. Zadaniem algorytmu DUAL jest to, aby w każdej chwili sieć była wolna od pętli. Obliczanie tras wykonywane jest przez DUAL Finite State Machine. FSM to model zachowań złożony z pewnej skończonej liczby stanów, przejść między tymi stanami i działań, które powodują te przejścia [1].

Algorytm DUAL zapewnia [4]:

- trasy wolne od pętli,
- trasy zapasowe wolne od pętli,
- szybką zbieżność,
- minimalną zajętość pasma dzięki aktualizacjom ograniczonym.

Algorytm DUAL odpowiedzialny jest za wybór sukcesora oraz dopuszczalnego sukcesora [1]. Sukcesor to router, który jest używany do przesyłania pakietów do sieci docelowej trasą o najniższym koszcie[1]. Dopuszczalny sukcesor to sąsiedni router, który posiada wolną od pętli trasę zapasową do tej samej co sukcesor sieci docelowej i spełnia warunek dopuszczalności [1]. Warunek dopuszczalności spełniony jest wtedy, gdy ogłaszana odległość do sieci sąsiedniego routera jest mniejsza niż dopuszczalna odległość lokalnego routera do tej samej sieci docelowej. Ogłaszana odległość to metryka, którą router przekazuje swojemu sąsiadowi informując o koszcie do sieci docelowej [1]. Kiedy sukcesor przestaje być dostępny i nie ma dopuszczalnego sukcesora, algorytm DUAL zmienia stan trasy na aktywny, wysyła zapytania EIGRP o drogę do tej sieci. Routery odpowiadają nadawcy czy mają drogę do żądanej sieci. Jeżeli żadna odpowiedź EIGRP nie zawiera informacja o drodze do tej sieci, nadawca nie otrzyma trasy do tej sieci. Jeżeli zaś odbierze odpowiedź z informacją o drodze do żądanej sieci, preferowana trasa zostanie uznana za nowy sukcesor i dodana do tablicy routingu [4]

Rozdział 5. Protokoły routingu stanu łącza

Protokoły routingu stanu łącza opierają się na innych zasadach niż protokoły wektora odległości, Protokoły stanu łącza tworzą topologiczną mapę sieci a każdy z routerów na podstawie tej mapy ustala najkrótszą trasę do sieci docelowej. Routery z zaimplementowanym protokołem routingu stanu łącza wysyłają innym routerom informacje o stanie swych łączy [4]. Protokoły routingu stanu łącza wykorzystują do działania algorytm SPF – (ang. shortest path first) Edsgera Dijkstry [1]. Algorytm sumuje koszty na drodze od źródła do celu. Każdy router do każdego celu w topologii ustala własny koszt. Najkrótszą drogą wcale nie musi być droga z najmniejszą liczbą skoków [4].

5.1 Proces routingu stanu łącza

Na proces routingu protokołu stanu łącza składa się pięć etapów [1]:

1. Wykrywanie sieci połączonych bezpośrednio – router wykrywa sieci podłączone bezpośrednio w chwili, kiedy zostanie skonfigurowany i aktywowany na routerze interfejs sieciowy. Jeżeli interfejs zostanie aktywowany, router zbiera następujące informacje o stanie tego łącza:
   - adres IP i maska podsieci interfejsu,
   - typ sieci – np. Ethernet, PPP,
   - koszt łącza,
   - informacje o sąsiednich routerach na tych łączach.
2. Rozsyłanie pakietów hello do sąsiednich routerów – do wykrywania sąsiednich routerów na łączu używany jest protokół hello. Za sąsiada uznawany jest router, który ma skonfigurowany protokół stanu łącza. Routery, do których dotrze pakiet hello odpowiadają nadawcy również pakietem hello. Pakiety hello wymianie są okresowo między routerami co powoduje monitorowanie stanu łącza. Jeżeli router przestanie odpowiadać na pakiet hello, uznawany jest za nieosiągalny.
3. Generowanie pakietu stanu łącza – routery generują pakiety LSP (ang. link-state packet), w którym jest informacja na temat każdego bezpośrednio połączonego łącza. Pakiety te są wysyłane tylko na łączach, na których są ustanowione przyległości z innymi routerami.

4. Rozsyłanie pakietów LSP – pakiety LSP rozsyłane są lawinowo do wszystkich pozostałych routerów na obszarze routingu. Router, który odbierze pakiet LSP wysyła ten pakiet LSP na wszystkich swoich interfejsach oprócz tego, na którym odebrał pakiet. Pakiety LSP nie są wysyłane regularnie, pakiety wysyłane są podczas pierwszego uruchomienia routera, oraz kiedy zmieni się topologia. Skutkiem tego jest szybsza zbieżność, niż w przypadku protokołów wektora odległości.
5. Tworzenie bazy danych stanu łącza – po odebraniu pakietów LSP, pakiety te są gromadzone w bazie danych stanu łącza. Router używa algorytmu SPF do stworzenia drzewa SPF na podstawie którego można poznać drogi o najniższym koszcie. Drogi te następnie dodawane są do tablicy routingu.

Protokoły routingu stanu łącza wymagają większej mocy obliczeniowej procesora i zasobów pamięci RAM niż protokoły wektora odległości [4]. Zalewanie sieci pakietami LSP może również spowodować znaczne wykorzystanie szerokości pasma.

Do protokołów stanu łącza zalicza się protokół OSPF i IS-IS

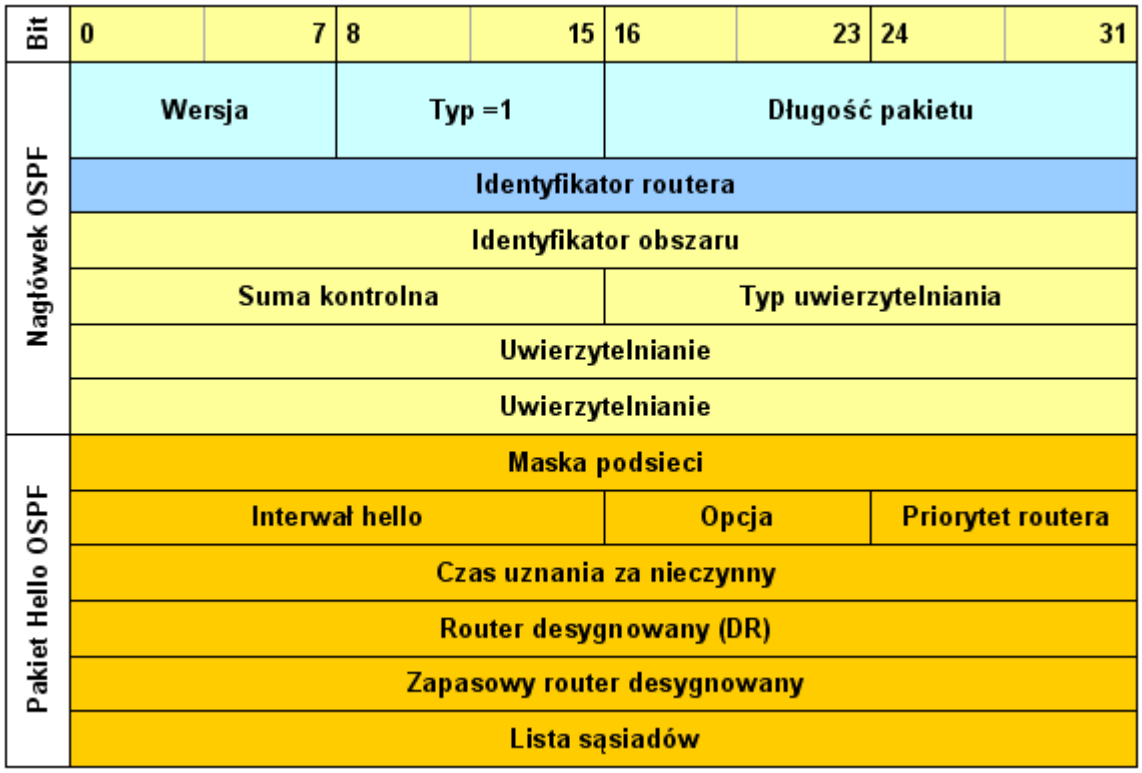
5.2 OSPF – Open Shortest Path First

Specyfikację protokołu OSPFv1 opublikowano w dokumencie RFC1131 w 1989 roku, OSPFv1 był eksperymentalnym protokołem, który nigdy nie został wdrożony w sieciach produkcyjnych. W 1991 roku został opublikowany protokół OSPFv2 w dokumencie RFC 1247. Ostateczna specyfikacja protokołu OSPFv2 ukazała się w 1998 roku i jest obowiązującą do dzisiaj. Istnieje również wersja protokołu OSPFv3 zaprojektowana dla sieci IPv6 [1].

Pakiet OSPF enkapsulowany jest pakiecie IP. W nagłówku IP pole Protokół ma wartość 89 – protokół OSPF a adresem docelowym jest adres multicast 224.0.0.5 lub 224.0.0.6 . Jeżeli pakiet OSPF enkapsulowany jest w ramce ethernetowej to docelowym adresem MAC jest adres multicast 01-00-5E-00-00-05 lub 01-00-5E-00-00-06 [1]

5.2.1 Format pakietu OSPF

Na rysunku 6 przedstawiono format nagłówka OSPF i pakiet hello.



Rys. 6 Nagłówek pakietu OSPF i pakiet hello

Opracowanie własne na podstawie [1]

Ważniejsze pola nagłówka OSPF

- Typ – typ pakietu OSPF: 1 – Hello, 2 – DBD, 3 – LSR, 4 – LSU, 5 – LSAck.
- Identyfikator routera - numer routera wysyłającego pakiet.
- Identyfikator obszaru początkowego – obszar początkowy, z którego jest wysyłany pakiet.
- Maska podsieci – maska podsieci skonfigurowana dla interfejsu wysyłającego.
- Interwał hello – czas w sekundach pomiędzy pakietami hello.
- Priorytet routera – służy do wybierania routera desygnowanego.
- Router desygnowany – nr id routera desygnowanego o ile istnieje.
- Zapasowy router desygnowany - nr id zapasowego routera desygnowanego o ile istnieje.
- Lista sąsiadów – lista nr id routerów sąsiednich z uruchomionym protokołem OSPF.

Występuje pięć typów pakietów OSPF:

- Hello – pakiety, które tworzą przyległości z innymi routerami.
- DBD – (ang. database description) – pakiety zawierający skróconą listę bazy danych stanu łącza.
- LSR – pakiet żądania dodatkowych informacji o dowolnym wpisie z opisu DBD.
- LSU – pakiet aktualizacji, który zawiera informacje żądane w pakiecie LSR.
- LSAck – pakiet potwierdzający odebranie pakietu LSU.

Aby router z uruchomionym protokołem OSPF mógł rozesłać swoje stany łącza do innych routerów, musi poznać swoich sąsiadów OSPF [4]. W informacjach wysyłanych w pakiecie hello znajduje się identyfikator routera OSPF wysyłającego pakiet. Odebranie pakietu hello jest dla routera potwierdzeniem, że na tym samym łączu znajduje się inny router OSPF. Routery tworzą przyległość, pełna przyległość ma miejsce wtedy, gdy zostaną uzgodnione trzy wartości: interwał pakietów hello, czas uznania za nieczynny i typ sieci. Domyślnie pakiety hello wysyłane są w odstępach 10 sekundowych w sieciach wielodostępowych i punk – punkt, oraz w odstępach 30 sekundowych w sieciach NMBA. [3]

5.2.2 Metryka protokołu OSPF

Metryką stosowaną przez protokół OSPF jest koszt. System Cisco IOS jako kosztu używa łącznej szerokości pasma sieciowych interfejsów wyjściowych z routera do sieci docelowej [1] zgodnie z poniższym równaniem (3):

$$Koszt\_OSPF = \frac{10^8}{przepustowosc\_pasma}[bps] \quad (3)\ [1]$$

10^8 - referencyjna szerokość pasma

Interfejsy z większą szerokością pasma mają niższy koszt. Koszt trasy OSPF to łączna wartość kosztów do sieci docelowej.

Typ interfejsu	Koszt
Fast Ethernet i szybsze	1
Ethernet	10
E1	48
T1	64
128 kb/s	781
64 kb/s	1562
56 kb/s	1785

Tabela 3. Wartość kosztów w protokole OSPF w zależności od typu interfejsu w systemie Cisco IOS.
Opracowanie własne na podstawie [1]

Istnieje możliwość modyfikacji kosztu łącza przez administratora. Do tego celu służy polecenie „ip ospf cost" [4]. Polecenie to jest przydatne wtedy, kiedy w sieci przedsiębiorstwa znajdują się routery innych producentów niż Cisco i do obliczania kosztu używają innej metryki niż szerokość pasma.

5.2.3 Router desygnowany i zapasowy router desygnowany.

W celu redukcji ilości ruchu w sieciach wielodostępowych wybierany jest router desygnowany DR i zapasowy router desygnowany BDR. Zadaniem routera desygnowanego jest aktualizowanie pozostałych routerów tzw. DROtherów [1]. Jeżeli zmieni się topologia sieci i router desygnowany stanie się nieosiągalny, zapasowy router desygnowany przejmuje zadania routera desygnowanego. W sieciach typu punkt-punkt nie jest wybierany router desygnowany ani zapasowy router desygnowany [4].

Identyfikator routera umożliwia jednoznaczną identyfikację routera w domenie routingu OSPF. Identyfikatorem jest adres IP. Routery Cisco tworzą identyfikator zgodnie z poniższą regułą [1]:

- Identyfikatorem staje się adres IP podany przez administratora poprzez wydanie komendy „router-id".

- Jeżeli administrator nie skonfiguruje identyfikatora, identyfikatorem staje się najwyższy adres IP interfejsu loopback,
- Jeżeli interfejs pętli zwrotnej nie jest uruchomiony na routerze identyfikatorem staje się najwyższy adres IP interfejsu fizycznego – interfejs ten musi być podniesiony.

Zaletą używania interfejsu pętli zwrotnej w celu określenia identyfikatora routera jest fakt, iż interfejs pętli zwrotnej w przeciwieństwie do interfejsu fizycznego nie może ulec awarii, co zapewnia stabilność protokołu OSPF. Wybory routera desygnowanego i zapasowego routera desygnowanego mają miejsce wtedy, kiedy pierwszy router z włączonym protokołem OSPF stanie się aktywny w sieci. Problem jest to, że jeżeli w sieci jeszcze nie wszystkie routery zostały uruchomione, routerem desygnowanym może zostać router z niższym identyfikatorem, niekoniecznie router, który dysponuje odpowiednią mocą obliczeniową i odpowiednią pamięcią RAM [1].

5.3 IS-IS – Intermediate System to Intermediate System

IS-IS to protokół podobnie jak OSPF protokół stanu łącza opracowany do połączenia systemów otwartych OSI. IS-IS jest bezklasowym protokołem routingu bram wewnętrznych, którego działanie podobne jest do OSPF, ale charakteryzuje się lepszą wydajnością i skalowalnością. W protokole routingu IS-IS router może spełniać dwa różne zadania [3]:

- Jako routery poziomu pierwszego przekazują pakiety wewnątrz obszaru
- Jako routery poziomu drugiego przekazują pakiety między obszarami.
- Jako routery poziomu 1-2 przekazują pakiety wewnątrz obszaru pierwszego oraz pomiędzy obszarami poziomu drugiego.

W przypadku IS-IS granica między obszarami leży na łączu pomiędzy routerami. Router należy tylko do jednego obszaru, nie tak ja w przypadku protokolu OSPF gdzie interfejsy jednego routera mogły należeć do różnych obszarów. W związku z tym czyni to protokół IS-IS bardziej modularnym [3] .

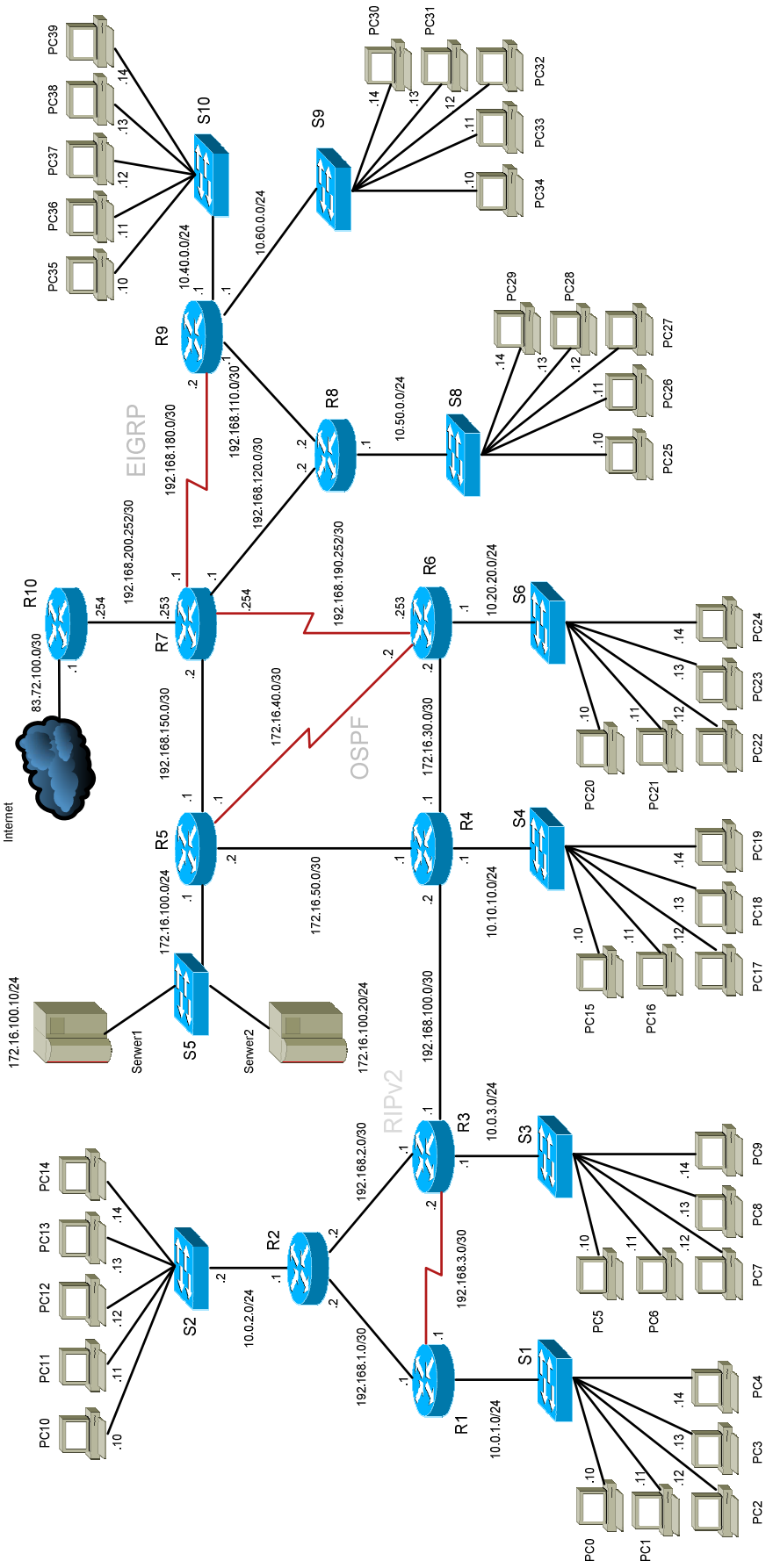
Routery poziomu pierwszego znajdujące się wewnątrz obszaru utrzymują identyczne bazy danych stanu łącza, które określają topologię obszaru. Routery poziomu drugiego również utrzymują osobne bazy danych stanu łącza dla topologii warstwy drugiej. Routery poziomu drugiego nie ogłaszają tras routerom poziomu pierwszego. Router poziomu pierwszego nie ma żadnej wiedzy, poza wiedzą o swoim obszarze. Powoduje to, że IS-IS jest bardziej wydajnym, charakteryzuje się mniejszym zapotrzebowaniem na moc obliczeniową procesora [3].

Rozdział 6. Część praktyczna - implementacja i analiza działania wybranych protokołów routingu w przykładowej sieci przedsiębiorstwa

Praktyczna część pracy inżynierskiej zawiera przykładową topologię sieci przedsiębiorstwa, wykonaną za pomocą symulatora sieci Cisco Packet Tracer. Schemat sieci przedstawia rysunek 7. Sieć zbudowana jest z dziesięciu routerów Cisco, na których zostały skonfigurowane wybrane protokoły routingu dynamicznego. Symulator Packet Tracer umożliwia symulację działania urządzeń firmy Cisco, ich konfigurację oraz możliwość śledzenia ich zachowań w zależności od zachodzących zmian w topologii sieci. Ze względu na ograniczenia wynikające z tematu pracy w przykładowej sieci nie implementowano vlanów, list kontroli dostępu ACL i innych technologii nie mających bezpośredniego związku z działaniem protokołów routingu dynamicznego.

6.1 Schemat sieci przedsiębiorstwa

Na rysunku 7 przedstawiony jest schemat zbudowanej sieci przedsiębiorstwa. W sieci znajduje się dziesięć routerów Cisco 2811, które umożliwiają routing pomiędzy poszczególnym podsieciami, w których znajdują się komputery pracowników oraz serwery firmowe. Sieć podzielona jest na obszary działania poszczególnych protokołów routingu: RIP, OSPF i EIGRP. Protokół RIP został skonfigurowany na routerach R1, R2, R3 i R4. Dokładną adresację IP routerów i informacje o skonfigurowanych protokołach routingu przedstawia tabela 4. Do routerów tych za pośrednictwem przełączników S1, S2, S3 i S4 podłączone są komputery pracowników, każda z grup komputerów należy do innej podsieci. Na routerach R4, R5, R6, R7 skonfigurowano protokół OSPF, do routera R5 podłączono za pośrednictwem przełącznika S5 dwa serwery firmowe. Na routerach R7, R8, R8 skonfigurowano protokół EIGRP, do routerów tych za pośrednictwem przełączników S8, S9, S10 przyłączono komputery pracowników, każda z grup komputerów należy do innej podsieci. Router R10 jest routerem brzegowym do sieci Internet. Pełna konfiguracja routerów zamieszczona jest w załączniku 1. Plik przykładowej sieci stworzonej w programie Pakiet Tracer znajduje się na dysku CD



Rys.7 Schemat sieci przedsiębiorstwa. Opracowanie własne

Router	Interfejs	Adres IP	Maska	Protokół routingu
R1	Fa0/0	10.0.1.1	/24	Interfejs pasywny
	Fa0/1	192.168.1.1	/30	RIPv2
	Se0/2/0	192.168.3.1	/30	RIPv2
R2	Fa0/0	192.168.1.2	/30	RIPv2
	Fa0/1	10.0.2.1	/24	Interfejs pasywny
	Fa1/0	192.168.2.2	/30	RIPv2
R3	Fa0/0	10.0.3.1	/24	Interfejs pasywny
	Fa0/1	192.168.2.1	/30	RIPv2
	Se0/2/0	192.168.3.2	/30	RIPv2
	Fa1/0	192.168.100.1	/30	RIPv2
R4	Fa0/0	172.16.30.1	/30	OSPF
	Fa0/1	172.16.50.1	/30	OSPF
	Fa1/0	10.10.10.1	/24	OSPF
	Fa1/1	192.168.100.2	/30	RIPv2
	Loopback1	192.168.255.252	/32	-
R5	Fa0/0	172.16.50.2	/30	OSPF
	Fa0/1	192.168.150.1	/30	OSPF
	Se0/2/0	172.16.40.1	/30	OSPF
	Fa1/0	172.16.100.1	/24	OSPF
	Loopback1	192.168.255.254	/32	-
R6	Fa0/0	172.16.30.2	/30	OSPF
	Fa0/1	10.20.20.0	/24	OSPF
	Se0/2/0	172.16.40.2	/30	OSPF
	Se0/2/1	192.168.190.253	/30	OSPF
	Loopback1	192.168.255.251	/32	-
R7	Fa0/0	192.168.150.2	/30	OSPF
	Fa0/1	192.168.120.1	/30	EIGRP
	Se0/2/0	192.168.180.1	/30	EIGRP
	Se0/2/1	192.168.190.254	/30	OSPF
	Fa1/0	192.168.200.253	/30	EIGRP
	Loopback1	192.168.255.253	/32	-
R8	Fa0/0	10.50.0.1	/24	EIGRP
	Fa0/1	192.168.120.2	/30	EIGRP
	Fa1/0	192.168.110.2	/30	EIGRP
R9	Fa0/0	192.168.110.1	/30	EIGRP
	Fa0/1	10.60.0.1	/24	EIGRP
	Se0/2/0	192.168.180.2	/30	EIGRP
	Fa1/0	10.40.0.1	/24	EIGRP
R10	Fa0/0	83.72.100.1	/30	Statyczny
	Fa0/1	192.168.200.254	/30	EIGRP

Tabela 4. Adresacja IP interfejsów sieciowych routerów z rysunku 7.
Opracowanie własne.

W tabeli 4 przedstawiono adresacją IP interfejsów routerów z rysunku 7. Kolumna „Router” zawiera nazwę routera, kolumna „Interfejs” zawiera nazwy poszczególnych interfejsów sieciowych danych routerów. Kolumny „Adres IP” i „Maska” zawierają nadaną adresację IP interfejsom sieciowym, maska zapisana jest w zapisie bitowym. W kolumnie

„Protokół routingu” zawarta jest informacja jaki protokół routingu uruchomiony jest na danym interfejsie routera. Interfejs pasywny oznacza, że na danym interfejsie zostało wyłączone rozsyłanie aktualizacji RIP, ponieważ interfejsy te nie mają połączenia z innymi routerami.

Adresacja IP komputerów pracowników została umieszczona w załączniku 2 oraz znajduje się naniesiona na schemat sieci na rysunku 7.

6.2 Analiza działania protokołu RIP

Protokół RIP w wersji 2 został uruchomiony na routerach R1, R2, R3 i R4. (Rys.7). Router R1 ma bezpośrednie połączenie z routerem R2 za pośrednictwem interfejsu FastEthernet0/1 z routerem R2 i za pośrednictwem interfejsu szeregowego Serial0/2/0 z routerem R3 . Router R3 oprócz połączeń z routerami R1 i R2 połączony jest za pośrednictwem interfejsu FastEthernet1/0 z routerem R4.

Na listingu 1 przedstawiono skonfigurowany protokół RIPv2 na routerze R1.

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 19 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/1        2     2
  Serial0/2/0            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        192.168.1.0
        192.168.3.0
Passive Interface(s):
        FastEthernet0/0
Routing Information Sources:
        Gateway         Distance      Last Update
        192.168.3.2           120      00:00:02
        192.168.1.2           120      00:00:22
Distance: (default is 120)
R1#
```

Listing 1. Wynik polecenia „show ip protocols” routera R1

Opracowanie własne.

Działanie protokołu routingu na routerze można sprawdzić komendą „show ip protocols”. Z wyniku można odczytać, iż włączony jest protokół RIP w wersji 2. aktualizacje RIP wysyłane są w interwale czasowym 30 sekund, licznik uznania trasy za nieczynną ustawiony na 180 sekund, licznik wstrzymania na 180 sekund a licznik oczyszczania na 240 sekund. Włączona jest redystrybucja protokołu RIP, oraz że w routingu biorą udział wymienione sieci. Wyłączona jest funkcja automatycznego podsumowania tras. Włączona jest funkcja „Passive Interface**”** na interfejsie FastEthernet0/0, która powoduje to, iż z podanego interfejsu nie są rozsyłane aktualizacje protokołu RIP. Nie ma potrzeby rozsyłania aktualizacji z tego interfejsu, gdyż nie jest do niego podłączony inny router. Źródłem informacji o trasach dla routera R1 są sąsiednie routery o adresach 192.168.1.2 i 192.168.3.2. Odległość administracyjna dla protokołu RIP ma wartość 120.

Na listingu 2 przedstawiono tablicę routingu routera R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.3.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 4 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
R       10.0.2.0 [120/1] via 192.168.1.2, 00:00:08, FastEthernet0/1
R       10.0.3.0 [120/1] via 192.168.3.2, 00:00:13, Serial0/2/0
R       10.10.10.0 [120/6] via 192.168.3.2, 00:00:13, Serial0/2/0
     172.16.0.0/30 is subnetted, 2 subnets
R       172.16.30.0 [120/6] via 192.168.3.2, 00:00:13, Serial0/2/0
R       172.16.50.0 [120/6] via 192.168.3.2, 00:00:13, Serial0/2/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/1
     192.168.2.0/30 is subnetted, 1 subnets
R       192.168.2.0 [120/1] via 192.168.1.2, 00:00:08, FastEthernet0/1
                    [120/1] via 192.168.3.2, 00:00:13, Serial0/2/0
     192.168.3.0/30 is subnetted, 1 subnets
C       192.168.3.0 is directly connected, Serial0/2/0
     192.168.100.0/30 is subnetted, 1 subnets
R       192.168.100.0 [120/1] via 192.168.3.2, 00:00:13, Serial0/2/0
R*   0.0.0.0/0 [120/2] via 192.168.3.2, 00:00:13, Serial0/2/0
R1#
```

Listing 2. Tablica routingu routera R1

Opracowanie własne

Litera R przed wpisem w tablicy (Listing 2) oznacza, że informacja o trasie została przekazana przez protokół RIP, W tablicy znajdują się również informacje o trasie z literą C, są to sieci połączone bezpośrednio. Z zapisu tablicy routingu wynika też, że istnieje również trasa domyślna 0.0.0.0 do której droga prowadzi przez interfejs Serial0/2/0 o adresie IP 192.168.3.2

Komendą ping sprawdzono prawidłowość routingu z komputera PC2 o adresie IP 10.0.1.12/24 z komputerem należącym do innej podsieci – komputerem PC14 o adresie IP 10.0.2.14/24, wynik przedstawiony jest na listingu 3

```
PC>ping 10.0.2.14

Pinging 10.0.2.14 with 32 bytes of data:

Reply from 10.0.2.14: bytes=32 time=98ms TTL=126
Reply from 10.0.2.14: bytes=32 time=135ms TTL=126
Reply from 10.0.2.14: bytes=32 time=66ms TTL=126
Reply from 10.0.2.14: bytes=32 time=111ms TTL=126

Ping statistics for 10.0.2.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 135ms, Average = 102ms

PC>
```

Listing 3. Wynik działania komendy „ping 10.0.2.14” na komputerze PC2.
Opracowanie własne

Z listingu 3 wynika, że zachodzi komunikacja między komputerami należącym do różnych podsieci co świadczy o fakcie prawidłowego routingu pomiędzy tymi sieciami.

Sprawdzono prawidłowość działania trasy domyślnej. W tym celu wydano polecenie ping z komputera PC0 do interfejsu routera 83.72.100.1 routera R10, wynik przedstawiony jest na listingu 4.

```
PC>ping 83.72.100.1

Pinging 83.72.100.1 with 32 bytes of data:

Reply from 83.72.100.1: bytes=32 time=141ms TTL=250
Reply from 83.72.100.1: bytes=32 time=172ms TTL=250
Reply from 83.72.100.1: bytes=32 time=127ms TTL=250
Reply from 83.72.100.1: bytes=32 time=90ms TTL=250

Ping statistics for 83.72.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 90ms, Maximum = 172ms, Average = 132ms

PC>
```

Listing 4. Wynik działania komendy „ping 83.72.100.1" na komputerze PC0.
Opracowanie własne

Z listingu 4 wynika, że zachodzi komunikacja pomiędzy komputerem PC0 a interfejsem 83.72.100.1 routera R10. Ponieważ router R1 do którego należy podsieć z komputerem PC0 w swojej tablicy routingu (listing 2) nie posiada wpisu dotyczącego trasy do sieci 83.72.100.1, do wysyłania pakietów korzysta z wpisu tablicy routingu dotyczącego trasy domyślnej. Na podstawie powyższego stwierdzono, że router wysyła prawidłowo pakiety za pomocą trasy domyślnej do sieci, której nie posiada w swojej tablicy routingu.

Komendą „tracert" sprawdzono przebieg trasy od komputera PC0 do interfejsu 83.72.100.1 routera R10. Wynik przedstawia listing 5

```
Packet Tracer PC Command Line 1.0
PC>tracert 83.72.100.1

Tracing route to 83.72.100.1 over a maximum of 30 hops:

  1   63 ms     49 ms     33 ms     10.0.1.1
  2   33 ms     79 ms     62 ms     192.168.3.2
  3   109 ms    93 ms     109 ms    192.168.100.2
  4   112 ms    63 ms     81 ms     172.16.50.2
  5   127 ms    111 ms    83 ms     192.168.150.2
  6   143 ms    141 ms    188 ms    83.72.100.1

Trace complete.

PC>
```

Listing 5. Wynik komendy „tracert 83.72.100.1" na komputerze PC0.
Opracowanie własne

Z listingu 5 wynika, że droga pakietu od komputera PC0 do interfejsu 83.72.100.1 routera R10 przebiega kolejno przez routery:

- R1 – interfejs 10.0.1.1
- R3 – interfejs 192.168.3.2
- R4 – interfejs 192.168.100.2
- R5 – interfejs 172.16.50.2
- R7 - interfejs 192.168.150.2
- R10 – interfejs 83.72.100.1

Aby sprawdzić jak protokołów RIP zareaguje na zachodzące zmiany w topologii sieci, zostanie zasymulowana awaria poprzez wyłączenie interfejsu 192.168.3.2 routera R3, poprzez którą biegła droga pakietu od komputera PC0 do interfejsu 83.72.100.1 routera R10. Ze schematu sieci - Rys. 7 wynika, że istnieje inna trasa, poprzez router R2, ale trasa domyślna dla routera R1 przebiegała przez interfejs 192.168.3.2 dlatego, że protokół RIP wybrał trasę na podstawie korzystniejszej metryki - mniejszej liczby skoków.
Na listingu 6 przedstawiono tablicę routingu routera R1 po wyłączeniu interfejsu 192.168.3.2 routera R3. Kolorem zaznaczono zmieniony wpis dla trasy domyślnej, która teraz przebiega przez adres IP 192.168.1.2 routera R2.

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R       10.0.0.0/8 is possibly down, routing via 192.168.1.2, FastEthern
C       10.0.1.0/24 is directly connected, FastEthernet0/0
R       10.0.2.0/24 [120/1] via 192.168.1.2, 00:00:10, FastEthernet0/1
R       10.0.3.0/24 [120/2] via 192.168.1.2, 00:00:10, FastEthernet0/1
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/1
     192.168.2.0/30 is subnetted, 1 subnets
R       192.168.2.0 [120/1] via 192.168.1.2, 00:00:10, FastEthernet0/1
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.100.0/24 is possibly down, routing via 192.168.1.2, Fast
0/1
R       192.168.100.0/30 [120/2] via 192.168.1.2, 00:00:10, FastEthernet
R*   0.0.0.0/0 [120/3] via 192.168.1.2, 00:00:10, FastEthernet0/1
R1#
```

Listing 6. Tablica routingu routera R1 po symulacji awarii interfejsu 192.168.3.2 routera R3.

Opracowanie własne

Komendą „tracer” sprawdzono, czy zmiana trasy domyślnej w tablicy routingu faktycznie spowoduje, że pakiety z komputera R0 dotrą do interfejsu 83.72.100.1 routera R10. Wynik zaprezentowany jest na listingu 7.

```
PC>tracert 83.72.100.1

Tracing route to 83.72.100.1 over a maximum of 30 hops:

  1    49 ms     47 ms     16 ms     10.0.1.1
  2    49 ms     63 ms     63 ms     192.168.1.2
  3    94 ms     47 ms     78 ms     192.168.2.1
  4    109 ms    80 ms     94 ms     192.168.100.2
  5    141 ms    146 ms    65 ms     172.16.50.2
  6    96 ms     143 ms    98 ms     192.168.150.2
  7    190 ms    127 ms    171 ms    83.72.100.1

Trace complete.

PC>
```

Listing 7. Trasa pakietu z PC0 do interfejsu 83.72.100.1 routera R10 po zmianie w tablicy routingu routera R1.

Opracowanie własne

Z listingu 7 wynika , że pomimo wystąpienia awarii sieci 192.168.3.0/30 protokół RIP zareagował prawidło, zmieniając tablicę routingu routera R1, umieszczając trasę domyślną wiodącą poprzez interfejs 192.168.1.2 routera R2, dzięki czemu komunikacja z routerem R10 została zachowana.

6.3 Analiza działania protokołu OSPF

Protokół OSPF uruchomiony jest na routerach R4, R5, R6 i R7. Pełna konfiguracja routerów zamieszczona jest w załączniku 1. Na każdym z wymienionych routerów uruchomiono interfejs pętli zwrotnej loopback, w celu nadania identyfikatorów ID poszczególnym routerom. W tym przypadku identyfikatorem ID routera będzie adres ip interfejsu loopback. Zaletą używania interfejsu pętli zwrotnej jest fakt, że nie może on ulec fizycznej awarii co zapewnia stabilność protokołu OSPF.

Sprawdzono komendą „show ip protocols” wydaną na routerze R5, czy protokół OSPF jest rzeczywiście uruchomiony. Wynik działania komendy przedstawiony jest na listingu 8.

```
R5#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.255.254
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.50.0 0.0.0.3 area 0
    172.16.100.0 0.0.0.255 area 0
    172.16.40.0 0.0.0.3 area 0
    192.168.150.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.50.1           110      00:02:00
    192.168.150.2         110      00:02:00
    172.16.40.2           110      00:02:02
  Distance: (default is 110)

R5#
```

Listing 8. Wynik działania komendy „show ip protocols" na routerze R5

Opracowanie własne

Z listingu 8 wynika, że na routerze uruchomiony jest protokół OSPF z identyfikatorem procesu 1. Identyfikator ten nie musi się zgadzać z innymi routerami aby zostały ustanowione przyległości, jednakże identyfikator o wartości 1 ustanowiony jest na każdym routerze z uruchomionym protokołem OSPF. Identyfikatorem ID routera jest adres IP interfejsu loopback – 192.168.255.254. W procesie routingu biorą udział cztery sieci o wymienionych na listingu adresach . Maska tych sieci zapisana jest w postaci maski odwrotnej tzw. „wildcart mask". Domyślna odległość administracyjna dla protokołu OSPF posiada wartość 110 – zgodnie z tabelą 1.

Komendą „show ip route" wyświetlono tablicę routingu routera R5. Wynik działania komendy znajduje się na listingu 9.

```
Gateway of last resort is 192.168.150.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 8 subnets
O E2    10.0.1.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
O E2    10.0.2.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
O E2    10.0.3.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
O       10.10.10.0 [110/2] via 172.16.50.1, 00:03:31, FastEthernet0/0
O       10.20.20.0 [110/3] via 172.16.50.1, 00:03:31, FastEthernet0/0
O E2    10.40.0.0 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
O E2    10.50.0.0 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
O E2    10.60.0.0 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.30.0/30 [110/2] via 172.16.50.1, 00:03:31, FastEthernet0/0
C       172.16.40.0/30 is directly connected, Serial0/2/0
C       172.16.50.0/30 is directly connected, FastEthernet0/0
C       172.16.100.0/24 is directly connected, FastEthernet1/0
     192.168.1.0/30 is subnetted, 1 subnets
O E2    192.168.1.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
     192.168.2.0/30 is subnetted, 1 subnets
O E2    192.168.2.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
     192.168.3.0/30 is subnetted, 1 subnets
O E2    192.168.3.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
     192.168.100.0/30 is subnetted, 1 subnets
O E2    192.168.100.0 [110/50] via 172.16.50.1, 00:03:31, FastEthernet0/0
     192.168.110.0/30 is subnetted, 1 subnets
O E2    192.168.110.0 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
     192.168.120.0/30 is subnetted, 1 subnets
O E2    192.168.120.0 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
     192.168.150.0/30 is subnetted, 1 subnets
C       192.168.150.0 is directly connected, FastEthernet0/1
     192.168.180.0/30 is subnetted, 1 subnets
O E2    192.168.180.0 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
     192.168.190.0/30 is subnetted, 1 subnets
O       192.168.190.252 [110/65] via 192.168.150.2, 00:03:31, FastEthernet0/1
     192.168.200.0/30 is subnetted, 1 subnets
O E2    192.168.200.252 [110/20] via 192.168.150.2, 00:03:31, FastEthernet0/1
     192.168.255.0/32 is subnetted, 1 subnets
C       192.168.255.254 is directly connected, Loopback1
O*E2 0.0.0.0/0 [110/1] via 192.168.150.2, 00:03:31, FastEthernet0/1
```

Listing 9. Tablica routingu routera R5.

Opracowanie własne

Na listingu 9 poszczególne wpisy tablicy routingu poprzedzone są literą O. Litera ta informuje, że źródłem informacji o danej trasie jest protokół OSPF. Oznaczenie E2 przy literze O informuje o tym, że trasa ta jest trasą zewnętrzną protokołu OSPF, czyli taką która do obszaru OSPF została dostarczona przez redystrybucję pomiędzy protokołami routingu. Proces redystrybucji jest opisany w dalszej części pracy. Wpis z literą C informuje o sieci połączonej bezpośrednio, w tym przypadku jest to interfejs pętli loopback o adresie 192.168.255.254, który został skonfigurowany po to aby stanowił identyfikator routera.

Poleceniem tracert sprawdzono drogę pakietu pomiędzy komputerem PC24 a serwerem o nazwie Serwer1. Wynik przedstawiono na listingu 10.

```
PC>tracert 172.16.100.10

Tracing route to 172.16.100.10 over a maximum of 30 hops:

  1    47 ms     33 ms     34 ms     10.20.20.1
  2    64 ms     62 ms     62 ms     172.16.30.1
  3    78 ms     94 ms     65 ms     172.16.50.2
  4    141 ms    94 ms     156 ms    172.16.100.10

Trace complete.

PC>
```

Listing 10. Wynik polecenia Tracer 172.16.100.10 na komputerze PC24. Opracowanie własne

Z listingu 10 wynika, że trasa do serwera Serwer1 przebiega kolejno przez routery: R6, R4 i R5. Ze schematu sieci (Rys. 7) można wywnioskować, że do tego samego serwera od komputera PC24 możliwe są inne trasy np. poprzez routery R6, R7, R5, lub poprzez routery: R6, R5. Dlaczego jednak trasa wiedzie poprzez routery R6, R4, R5?

Aby odpowiedzieć na to pytanie sprawdzono jaki jest łączny koszt dotarcia pakietu od komputera PC24 do serwera Serwer1. Łączny koszt dotarcia pakietu do celu jest sumą poszczególnych kosztów na drodze do celu. Aby sprawdzić jaki jest koszt danego interfejsu routera należy wydać polecenie „show ip ospf interface” . W tabeli 5 pokazano obliczony koszt do serwera Serwer1 w zależności od trasy .

Trasa	Interfejsy	Koszt interfejsu	Łączny koszt
R6-R4-R5	10.20.20.1	1	**4**
	172.16.30.1	1	
	172.16.50.2	1	
	172.16.100.1	1	
R6-R7-R5	10.20.20.1	1	**67**
	192.168.190.254	64	
	192.168.150.1	1	
	172.16.100.1	1	
R6-R5	10.20.20.1	1	**66**
	172.16.40.1	64	
	172.16.100.1	1	

Tabela 5. Łączny koszt ospf od komputera PC24 do Serwer1 w zależności od trasy.

Opracowanie własne

Z tabeli 5 wynika, że trasa R6-R4-R5 jest trasą z najniższym kosztem, dlatego właśnie ta trasa prowadzi do serwera Serwer1. Jeżeli zaś nastąpi awaria sieci 172.16.30.0/30 trasą aktualna stanie się trasa R6- R5. Aby to sprawdzić wyłączono interfejs 172.16.30.1 routera R4 symulując awarię. Trasa pakietów od komputera do serwera Serwer1 po awarii sieci 172.16.30.0/30 przedstawiona została na listingu 11

```
PC>tracert 172.16.100.10

Tracing route to 172.16.100.10 over a maximum of 30 hops:

  1    47 ms     49 ms     18 ms     10.20.20.1
  2    64 ms     33 ms     63 ms     172.16.40.1
  3    96 ms     94 ms     125 ms    172.16.100.10

Trace complete.
```

Listing 11. Wynik komendy tracert 172.16.100.10 po awarii sieci 172.16.30.0/30

Opracowanie własne

Z listingu 11 wynika, że trasa uległa zmianie, i przebiega przez interfejs 172.16.40.1 routera R5, czyli routery R6-R5, ponieważ teraz trasa ta jest trasą z najniższym kosztem..

Koszt łącza może zostać określony również przez administratora. Służy do tego polecenie „ip ospf cost”. W celu sprawdzenia działania tego polecenia zmieniono koszt interfejsu 172.16.40.1 i ustawiono go na wartość 128. Zmiana ta spowodowała, że trasą z najniższym kosztem stała się trasa R6-R7-R5 (której łączny koszt wynosi 67), czego dowodem jest listing 12.

```
PC>tracert 172.16.100.10

Tracing route to 172.16.100.10 over a maximum of 30 hops:

  1   18 ms     62 ms     31 ms     10.20.20.1
  2   94 ms     66 ms     49 ms     192.168.190.254
  3   52 ms     49 ms     110 ms    192.168.150.1
  4   141 ms    125 ms    94 ms     172.16.100.10

Trace complete.

PC>
```

Listing 12 Wynik działania komendy Tracer 172.16.100.10 po zmianie kosztu interfejsu 172.16.40.1

Opracowanie własne

Z listingu 12 można odczytać, że trasa pakietu przebiega przez interfejs o adresie IP 192.168.190.254 należący do routera R7 a cała trasa przebiega kolejno przez routery R6-R7-R5.

6.4 Analiza działania protokołu EIGRP.

Protokół EIGRP został uruchomiony na routerach R8, R9, oraz na interfejsie 192.168.180.1 routera R7 i interfejsie 192.168.200.254 routera R10.

Na listingu 13 przedstawiono tablicę routingu routera R8. Wpisy poprzedzone literą D informują że źródłem informacji o sieci jest protokół EIGRP. Oznaczenie EX oznacza, że trasa ta jest zewnętrzną trasą EIGRP z poza domeny routingu EIGRP. W związku z tym że protokół EIGRP w celu zminimalizowania tablicy routingu automatycznie podsumowuje trasy na granicy sieci, w przypadku prezentowanej sieci przedsiębiorstwa zostało wyłączone

automatyczne podsumowanie. Ostatni wpis w tablicy routing z listingu 13 informuje o trasie domyślnej, która prowadzi przez interfejs 192.168.120.1 a informacja o tej trasie pochodzi z zewnętrznego źródła EIGRP, o czym mówi odległość administracyjna ustawiona na wartość 170.

```
     10.0.0.0/24 is subnetted, 8 subnets
D EX    10.0.1.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
D EX    10.0.2.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
D EX    10.0.3.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
D EX    10.10.10.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
D EX    10.20.20.0 [170/284160] via 192.168.120.1, 00:08:07, FastEthernet0/1
D       10.40.0.0 [90/30720] via 192.168.110.1, 00:51:51, FastEthernet1/0
C       10.50.0.0 is directly connected, FastEthernet0/0
D       10.60.0.0 [90/30720] via 192.168.110.1, 00:51:51, FastEthernet1/0
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D EX    172.16.30.0/30 [170/284160] via 192.168.120.1, 00:08:54, FastEthernet0/1

D EX    172.16.40.0/30 [170/284160] via 192.168.120.1, 00:08:54, FastEthernet0/1

D EX    172.16.50.0/30 [170/284160] via 192.168.120.1, 00:50:51, FastEthernet0/1

D EX    172.16.100.0/24 [170/284160] via 192.168.120.1, 00:50:51, FastEthernet0/
1
     192.168.1.0/30 is subnetted, 1 subnets
D EX    192.168.1.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
     192.168.2.0/30 is subnetted, 1 subnets
D EX    192.168.2.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
     192.168.3.0/30 is subnetted, 1 subnets
D EX    192.168.3.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
     192.168.100.0/30 is subnetted, 1 subnets
D EX    192.168.100.0 [170/284160] via 192.168.120.1, 00:50:49, FastEthernet0/1
     192.168.110.0/30 is subnetted, 1 subnets
C       192.168.110.0 is directly connected, FastEthernet1/0
     192.168.120.0/30 is subnetted, 1 subnets
C       192.168.120.0 is directly connected, FastEthernet0/1
     192.168.150.0/30 is subnetted, 1 subnets
D EX    192.168.150.0 [170/284160] via 192.168.120.1, 00:51:51, FastEthernet0/1
     192.168.180.0/30 is subnetted, 1 subnets
D       192.168.180.0 [90/2172416] via 192.168.120.1, 00:51:42, FastEthernet0/1
     192.168.190.0/30 is subnetted, 1 subnets
D EX    192.168.190.252 [170/284160] via 192.168.120.1, 00:51:45, FastEthernet0/
1
     192.168.200.0/30 is subnetted, 1 subnets
D       192.168.200.252 [90/30720] via 192.168.120.1, 00:51:51, FastEthernet0/1
D*EX 0.0.0.0/0 [170/56320] via 192.168.120.1, 00:51:48, FastEthernet0/1
R8#
```

Listing 13. Tablica routingu routera R8.

Opracowanie własne

Obliczenie metryki EIGRP routera R8 do sieci 192.168.200.252.

Z listingu 13 wynika, że trasa do sieci 192.168.200.252 ma wartość 30720. Sprawdzono czy wartość ta zgadza się z przeprowadzonym poniżej obliczeniem.

Zgodnie ze wzorem (2):

Metryka EIGRP = Bw + delay

Bw(i) – łączem do sieci 192.168.200.252 jest łącze Fast Ethernet w związku z czym przepustowość pasma wynosi 100[Mb/s] czyli 100 000 [kb/s]

Bw = (10000000/Bw(i))*256 =(10000000/100000)*256 = 25600

delay(i) – suma opóźnień do sieci 192.168.200.250 dla łącza Fast Ethernet zgodnie z tabelą 2 wynosi dla jednego interfejsu 100 mikrosekund a trasa do sieci docelowej prowadzi przez dwa interfejsy: Fa0/1 routera R8 i interfejs Fa1/0 routera R9, czyli 200 [mikrosekundy]

delay = (delay(i)/10)*256 = (100+100)/10*256 = 5120

Metryka EIGRP = 25600+5120 = <u>30720</u>

Obliczona metryka EIGRP dla routera R8 do sieci 192.168.200.252 wynosi 30720 i jest identyczna z wartością metryki do tej sieci przedstawianą na listingu 13.

W celu sprawdzenia jakie przyległości sąsiedzkie ustanowił router R8 wydano polecenie „ show ip eigrp neighbors”. Wynik działania polecenia znajduje się na listingu 14

```
R8#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)       Cnt  Num
0   192.168.110.1   Fa1/0          14   00:15:48  40     1000  0   138
1   192.168.120.1   Fa0/1          11   00:15:48  40     1000  0   118

R8#
```

Listing 14. Wynik działania polecenia „show ip eigrp neighbors” na routerze R8.

Opracowanie własne

Z listingu14 wynika, że router R8 ustanowił relacje sąsiedzkie z routerem R9, do którego należy interfejs 192.168.110.1. oraz z routerem R7 do którego należy interfejs 192.168.120.1. Polecenie to dostarcza również innych informacji na temat działającego protokołu EIGRP. Kolumna „Hold” zawiera czas w sekundach pozostały do uznania sąsiada za nieczynnego. Każdorazowo kiedy zostanie odebrany pakiet hello, wartość czasu wstrzymania zostaje zresetowana i ustawiona na maksymalny czas wstrzymania i rozpoczyna się odliczanie tego czasu do zera. Kolumna „Uptime” wskazuje czas, jaki upłynął od czasu ustanowienia przyległości, w tym przypadku jest to 15 minut i 48 sekund.

Aby sprawdzić prawidłowość routingu w badanym obszarze routerów z uruchomionym protokołem EIGRP wydano polecenie ping z komputera PC34 z adresem IP 10.60.0.14 do serwera Serwer2 z adresem IP 172.16.100.20/24. Wynik działania polecenia przedstawiony jest w listingu 15.

```
PC>ping 172.16.100.20

Pinging 172.16.100.20 with 32 bytes of data:

Reply from 172.16.100.20: bytes=32 time=127ms TTL=124
Reply from 172.16.100.20: bytes=32 time=112ms TTL=124
Reply from 172.16.100.20: bytes=32 time=156ms TTL=124
Reply from 172.16.100.20: bytes=32 time=111ms TTL=124

Ping statistics for 172.16.100.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 111ms, Maximum = 156ms, Average = 126ms

PC>
```

Listing 15 Wynik komendy „ping 172.16.100.20 na komputerze PC34.

Opracowanie własne

Listing 15 informuje, że pakiety ICMP docierają do serwera Serwer2 prawidłowo, routing w obszarze EIGRP działa prawidłowo. W celu prześledzenia trasy pakietu wydano na komputerze PC34 komendę Tracer 172.16.100.20. Wynik jej działania zaprezentowano na listingu 16.

```
PC>tracert 172.16.100.20

Tracing route to 172.16.100.20 over a maximum of 30 hops:

  1   47 ms     47 ms     47 ms     10.60.0.1
  2   48 ms     64 ms     47 ms     192.168.110.2
  3   78 ms     94 ms     125 ms    192.168.120.1
  4   109 ms    125 ms    109 ms    192.168.150.1
  5   156 ms    172 ms    172 ms    172.16.100.20

Trace complete.

PC>
```

Listing 16. Wynik komendy „Tracer 172.16.100.20" na komputerze PC34

Opracowanie własne

Z listingu 16 wynika że trasa przebiega przez interfejsy routerów R9-R8-R7-R5. Ze schematu sieci (Rys. 7) wynika, że istnieje krótsza trasa przebiegająca z pominięciem routera R8. Dlaczego jednak protokół EIGRP zadecydował o tym, żeby trasa przebiegała przez router R8?

Aby odpowiedzieć na to pytanie wydano na routerze R9 polecenie „show ip eigrp topology". Wybrany fragment wyniku tego polecenia został zamieszczony na listingu 17.

```
P 172.16.100.0/24, 1 successors, FD is 286720
         via 192.168.110.2 (286720/284160), FastEthernet0/0
         via 192.168.180.1 (20768000/281600), Serial0/2/0
```

Listing 17. Fragment polecenia „show ip eigrp topology"na routerze R9.

Opracowanie własne.

Listing 17 informuje, że w tablicy topologii dla sieci 172.16.100.0/24 istnieje jeden sukcesor a jego dopuszczalna odległość ma wartość 286720 i jest to jednocześnie metryka EIGRP do sieci 172.16.100.0/24. Sukcesorem jest router R8 do którego należy interfejs 192.168.110.2 a jego ogłaszana odległość to 284160. Dopuszczalnym sukcesorem jest router R7, do którego należy interfejs o adresie 192.168.180.1. Jeżeli router R8 stanie się niedostępny to nowa dopuszczalna odległość do sieci 172.16.100.0/24 będzie miała wartość 20768000. Wartość 281600 to ogłaszana odległość routera R7 do sieci 172.16.100.0/24 i jest mniejsza od wartości 286720 – bieżącej dopuszczalnej odległości, dzięki czemu zostaje spełniony warunek dopuszczalności i router R7 staje się dopuszczalnym sukcesorem dla routera R9.

Aby sprawdzić czy dopuszczalny sukcesor stanie się sukcesorem zasymulowano awarię sieci 192.168.110.0/30. W tym celu wyłączono interfejs 192.168.110.2 na routerze R8, poprzez który do tej pory prowadziła trasa do serwera Serwer2. Tablica topologii dla routera R9 po awarii sieci została zamieszczona na listingu 18.

```
P 172.16.100.0/24, 1 successors, FD is 20768000
         via 192.168.180.1 (20768000/281600), Serial0/2/0
```

Listing 18. Fragment polecenia „show ip eigrp topology" na routerze R9. po awarii sieci 192.168.110.0/30.

Opracowanie własne.

Listing 18 informuje, że do sieci 172.16.100.0/24 istnieje jeden sukcesor z dopuszczalną odległością 20768000, która jest jednocześnie teraz metryką EIGRP do sieci docelowej. Sukcesorem jest router R7, do którego należy interfejs o adresie IP 192.168.180.1. Brak jest sukcesora dopuszczalnego.

Poleceniem tracer sprawdzono trasę pakietów z komputera PC34 do serwera Serwer2. Wynik zaprezentowano na listingu 19.

```
PC>tracert 172.16.100.20

Tracing route to 172.16.100.20 over a maximum of 30 hops:

  1   63 ms     47 ms     63 ms     10.60.0.1
  2   94 ms     49 ms     51 ms     192.168.180.1
  3   94 ms     109 ms    62 ms     192.168.150.1
  4   111 ms    82 ms     141 ms    172.16.100.20

Trace complete.

PC>
```

Listing 19. Wynik polecenia :Tracer 172.16.100.20 po awarii sieci 192.168.110.0/30

Opracowanie własne.

Jak widać na listingu 19 trasa została zmieniona i prowadzi przez interfejs 192.168.180.1 routera R7.

Dzięki temu, iż w tablicy topologii umieszczony był dopuszczalny sukcesor, algorytm DUAL nie musiał ponownie wykonywać przeliczenia zapasowych tras do innych

routerów. Dzięki temu protokół EIGRP cechuje się szybką zbieżnością po zmianie topologii sieci.

6.5 Analiza redystrybucji tras pomiędzy protokołami RIP, OSPF, EIGRP

W przykładowej sieci przedsiębiorstwa (Rys.7) działają protokoły RIP, OSPF i EIGRP, oraz na routerze R10 ustawiona jest statyczna trasa domyślna, która jest redystrybuowana w całej sieci. Aby możliwy był routing pomiędzy różnymi protokołami routingu na routerach, na których uruchomione są różne protokołu routingu musi być skonfigurowana redystrybucja tras. Routery, na których działają różne protokoły routingu w przykładowej sieci przedsiębiorstwa (Rys. 7) to routery R4, R7, R10. Na routerze R4 działa protokół RIP i OSPF, na routerze R7 OSPF i EIGRP a na routerze R10 działa EIGRP i routing statyczny.

Na routerze R10 skonfigurowano domyślną trasę statyczną. Fragment listingu konfiguracji, który odpowiada za domyślną trasę statyczną zawiera listing 20.

```
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
```

Listing 20. Fragment konfiguracji routera R10 odpowiadający za domyślną trasę statyczną.

Opracowanie własne

Wszystkie pakiety, które nie pasują do żadnej z sieci docelowych zamieszczonych w tablicy routingu będą kierowane poprzez interfejs FastEthernet0/0 routera R10. Następnie dzięki komendzie konfiguracyjnej „redistribute static” informacja o domyślnej trasie statycznej jest redystrybuowana w głąb sieci, w tym przypadku za pomocą protokołu EIGRP, - listing 21.

```
!
router eigrp 1
 redistribute static
 network 192.168.200.252 0.0.0.3
 auto-summary
!
```

Listing 21. Fragment konfiguracji routera R10 odpowiadający za redystrybucję trasy statycznej do innych routerów.

Opracowanie własne

Pełny listing konfiguracji routera R10 znajduje się w załączniku 1.

Na routerze R7 uruchomione są protokoły OSPF i EIGRP. W celu zapewnienia routingu pomiędzy tymi protokołami została uruchomiona redystrybucja tras. Tablica routingu routera R7 została przedstawiona na listingu 23. Z listingu widać, że umieszczone są wpisy tras, których źródłem jest zarówno protokół OSPF jak i EIGRP – czego dowodem są litery O i D poprzedzające konkretne wpisy. Aby możliwe było uruchomienie redystrybucji tras koniecznym było wydanie odpowiednich poleceń konfiguracyjnych dla poszczególnych protokołów. Listing 22 zawiera fragment konfiguracji routera R7 odpowiedzialny za uruchomienie i redystrybucję protokołów EIGRP i OSPF.

```
router eigrp 1
 redistribute ospf 1 metric 100000 1000 100 100 55
 network 192.168.200.252 0.0.0.3
 network 192.168.120.0 0.0.0.3
 network 192.168.180.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 subnets
 network 192.168.150.0 0.0.0.3 area 0
 network 192.168.190.252 0.0.0.3 area 0
 default-information originate
!
```

Listing 22. Fragment konfiguracji routera R7 odpowiadający za redystrybucję protokołów.

Opracowanie własne

```
Gateway of last resort is 192.168.200.254 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 8 subnets
O E2    10.0.1.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
O E2    10.0.2.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
O E2    10.0.3.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
O       10.10.10.0 [110/3] via 192.168.150.1, 02:58:06, FastEthernet0/0
O       10.20.20.0 [110/4] via 192.168.150.1, 02:58:06, FastEthernet0/0
D       10.40.0.0 [90/33280] via 192.168.120.2, 00:10:43, FastEthernet0/1
D       10.50.0.0 [90/30720] via 192.168.120.2, 02:59:10, FastEthernet0/1
D       10.60.0.0 [90/33280] via 192.168.120.2, 00:10:43, FastEthernet0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.30.0/30 [110/3] via 192.168.150.1, 02:58:06, FastEthernet0/0
O       172.16.40.0/30 [110/65] via 192.168.150.1, 02:58:16, FastEthernet0/0
O       172.16.50.0/30 [110/2] via 192.168.150.1, 02:58:06, FastEthernet0/0
O       172.16.100.0/24 [110/2] via 192.168.150.1, 02:58:16, FastEthernet0/0
     192.168.1.0/30 is subnetted, 1 subnets
O E2    192.168.1.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
     192.168.2.0/30 is subnetted, 1 subnets
O E2    192.168.2.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
     192.168.3.0/30 is subnetted, 1 subnets
O E2    192.168.3.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
     192.168.100.0/30 is subnetted, 1 subnets
O E2    192.168.100.0 [110/50] via 192.168.150.1, 02:58:06, FastEthernet0/0
     192.168.110.0/30 is subnetted, 1 subnets
D       192.168.110.0 [90/30720] via 192.168.120.2, 00:10:44, FastEthernet0/1
     192.168.120.0/30 is subnetted, 1 subnets
C       192.168.120.0 is directly connected, FastEthernet0/1
     192.168.150.0/30 is subnetted, 1 subnets
C       192.168.150.0 is directly connected, FastEthernet0/0
     192.168.180.0/30 is subnetted, 1 subnets
C       192.168.180.0 is directly connected, Serial0/2/0
     192.168.190.0/30 is subnetted, 1 subnets
C       192.168.190.252 is directly connected, Serial0/2/1
     192.168.200.0/30 is subnetted, 1 subnets
C       192.168.200.252 is directly connected, FastEthernet1/0
     192.168.255.0/32 is subnetted, 1 subnets
C       192.168.255.253 is directly connected, Loopback1
D*EX 0.0.0.0/0 [170/53760] via 192.168.200.254, 02:59:10, FastEthernet1/0
```

Listing 23 Tablica routingu routera R7

Opracowanie własne.

Na routerze R4 została uruchomiona redystrybucja pomiędzy protokołami RIP i OSPF. Fragment konfiguracji zawierający komendy odpowiedzialne za uruchomienie i redystrybucję protokołów zawarty jest w listingu 24..

```
!
router ospf 1
 log-adjacency-changes
 redistribute rip metric 50 subnets
 redistribute static subnets
 network 172.16.50.0 0.0.0.3 area 0
 network 172.16.30.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.255 area 0
 default-information originate
!
router rip
 version 2
 redistribute ospf 1 metric 5
 network 192.168.100.0
 default-information originate
 no auto-summary
!
```

Listing 24. Fragment konfiguracji routera R4 odpowiadający za uruchomienie i redystrybucję protokołów OSPF i RIPv2.

Opracowanie własne.

Redystrybucja protokołu RIP do obszaru OSPF odbywa się z metryką 50 (listing 24), redystrybucja obejmuje również podsieci, dzięki poleceniu „subnets”. Redystrybucja protokołu OSPF do obszaru RIP odbywa się z metryką 5. Dzięki temu redystrybucja jest dwukierunkowa i umożliwia wzajemną wymianę informacji o trasach między obszarami RIP i OSPF.

Podsumowanie

Protokoły routingu dynamicznego umożliwiają wymianę informacji o trasach do sieci zdalnych pomiędzy routerami, dzięki nim routery mogą dynamicznie umieszczać informacje o trasach w swoich tablicach routingu. Protokoły routingu dynamicznego potrafią znaleźć trasy alternatywne do sieci docelowych w sytuacji, kiedy w sieci wystąpi awaria łącza. W porównaniu z routingiem statycznym protokoły routingu dynamicznego pozwalają administratorom zaoszczędzić czas przy konfiguracji routingu, jednakże wymagają większych zasobów sprzętowych routera oraz większej szerokości pasma. Routing statyczny mimo wielu zalet routingu dynamicznego w dalszym ciągu znajduje zastosowanie w sieciach przedsiębiorstw. Routing statyczny stosowany jest w sieciach przedsiębiorstw o niewielkich rozmiarach, w sieciach, które nie są rozbudowywane. Routing statyczny jest dobrym rozwiązaniem wtedy, kiedy używa się jednej trasy domyślnej reprezentującej drogę do każdej sieci, dla której nie ma w tablicy routingu lepszej trasy. Niewątpliwą zaletą routingu statycznego jest bezpieczeństwo. Jest bardziej odporny od protokołów routingu dynamicznego na ataki związane ze zmianą tablic routingu. Fakt ten powoduje, że routing statyczny jest stosowany w sieciach, w których wymagane jest duże bezpieczeństwo kosztem dostępności po wystąpieniu awarii łącza prowadzącego do sieci docelowej. Przykładem stosowanie routingu statycznego ze względu na bezpieczeństwo są sieci, w których pracują bankomaty. Połączenie pomiędzy hostem transakcyjnym a bankomatem realizowanie jest z wykorzystaniem routingu statycznego.

Wybierając protokół routingu dynamicznego do zastosowania w danej sieci przedsiębiorstwa należy wziąć pod uwagę wymagania dotyczące skalowania sieci do większych rozmiarów, np. to czy na metryki są nałożone jakiekolwiek ograniczenia? Ograniczeniem protokołu RIP jest maksymalna liczba skoków – 15. W sieciach, w których trasy do sieci docelowych będą prowadzić przez więcej niż 15 routerów, protokół RIP nie może być zastosowany. Kolejnym ważnym czynnikiem jest czas zbieżności danego protokołu. W większości współczesnych sieci wymagany jest szybki stan zbieżności. Protokół RIP charakteryzuje się wolną zbieżnością, ponieważ stosuje aktualizacje okresowe, Nawet, jeżeli stosowane są zaawansowane techniki takie jak aktualizacje wyzwalane, całościowa zbieżność jest nadal wolniejsza niż protokołów stanu łącza. Kolejnym ograniczeniem stosowania protokołów wektora odległości w sieciach przedsiębiorstw jest zjawisko powstawania pętli routingu. Pętle routingu powstają wtedy, kiedy tablice routingu

nie są aktualizowane z powodu wolnej zbieżności na skutek występujących zmian w topologii sieci.

Protokołu routingu wektora odległości mają również swoje zalety i mogą być stosowane w sieciach o małych rozmiarach. Do działania nie wymagają routerów o dużych zasobach sprzętowych i nie wymagają dużych szerokości pasma do wysyłania aktualizacji routingu. Protokół RIPv2 z powodzeniem można zastosować w sieciach składających się od kilku do kilkunastu routerów (nie więcej niż 15), tam gdzie zmiana topologii nie występuje często. Jest protokołem prostym w implementacji i nie wymagającym od administratora dużej wiedzy do rozwiązywania występujących z nim problemów. Protokół EIGRP, który jest protokołem własnościowym Cisco jest protokołem o dużej skalowalności, może być stosowany do wielkości tysięcy węzłów routingu. Charakteryzuje się szybką zbieżnością w porównaniu do protokołu RIP. Wymagania sprzętowe w stosunku do routerów, na których działa protokół EIGRP są większe niż w przypadku pozostałych protokołów wektora odległości, ale mniejsze niż protokołów stanu łącza. Protokół EIGRP może być zastosowany tylko na routerach firmy Cisco. Jeżeli sieć jest zaprojektowana z użyciem wyłącznie routerów firmy Cisco, zastosowanie protokołu EIGRP zapewnia szybką zbieżność i stabilność procesu routingu. Protokół EIGRP wymaga jednak od administratora dużej wiedzy na temat sposobu zaimplementowania i sposobów diagnozowania i rozwiązywania problemów z nim związanych.

Protokoły routingu stanu łącza stosowane są w sieciach, w których wymagana jest szybka zbieżność. Protokół OSPF jest standardem otwartym, obsługiwanym przez wielu producentów urządzeń sieciowych, poprzez co może zostać zastosowany w sieciach wymagającej szybkiej zbieżności, których architektura oparta jest o routery różnych producentów. Pewnym problemem w sieciach, w których zastosowano OSPF może być sieć, która cyklicznie zmienia stan z czynnego na nieczynny i odwrotnie. Niestabilne łącze może powodować, iż routery na obszarze OSPF będą ciągle przeliczały algorytm SPF, uniemożliwiając osiągnięcie prawidłowego czasu zbieżności. Stąd na administratorach sieci, w których zastosowano protokół OSPF spoczywa duża odpowiedzialność za prawidłowo działającą warstwę sprzętową sieci. Protokół OSPF wymaga zastosowania wydajnych routerów, ponieważ zapotrzebowanie na zasoby sprzętowej jest większe niż w przypadku pozostałych protokołów routingu. Mniejszym zapotrzebowaniem od OSPF na zasoby sprzętowe cechuje się protokół IS-IS.

Wybierając protokołu routingu do zastosowania w sieci nie trzeba stosować tylko jednego protokołu routingu w całej sieci. Kryteria wyboru różnią się dla różnych części sieci

Jeżeli sieć przedsiębiorstwa projektowana jest od podstaw i jest to projekt hierarchiczny, czyli taki, w którym sieć składa się z warstwy rdzenia, warstwy dystrybucji i warstwy dostępu, warstwa rdzenia powinna zawierać łącza nadmiarowe oraz umożliwiać podział obciążenia pomiędzy trasy o jednakowym koszcie. Musi zapewniać natychmiastową reakcję na uszkodzenie łącza i bardzo szybko adoptować się do zmian. W warstwie rdzenia zastosować można EIGRP, OSPF i IS-IS. Protokół RIP nie nadaje się ze względu na wolną zbieżność. W pozostałych warstwach: dystrybucji i dostępu mogą być stosowane: RIPv2, EIGRP, OSPF i IS-IS.

Zastosowanie kilku protokołów routingu na obszarze jednej sieci możliwe jest dzięki procesowi redystrybucji. Redystrybucja pozwala routerom na obsługiwanie więcej niż jednego protokołu routingu, oraz dzielenie tras pomiędzy protokoły. Musi być starannie zaplanowana i wdrożona, ponieważ błędy podczas implementacji redystrybucji mogą doprowadzić do powstawania pętli routingu. Redystrybucja tras może być kłopotliwa, ponieważ każdy protokół routingu działa inaczej i protokoły nie mogą bezpośrednio wymieniać się informacjami dotyczącym tras, metryk, stanów łącz.

Podjęcie właściwej decyzji dotyczącej zastosowania właściwego protokołu routingu w sieci przedsiębiorstwa pozwoli zapewnić szybkość i stabilność działania sieci, poprzez co dostęp do informacji i zasobów przedsiębiorstwa będzie bezpieczny o bardzo dużym stopniu niezawodności.

.

Literatura

[1] Rick Graziani, Allan Johnson „Akademia sieci Cisco CCNA Exploration Semestr 2 Protokoły i koncepcje routingu” Wydawnictwo Naukowe PWN SA Warszawa 2008.

[2] Wendell Odom, Rick McDonald „Akademia sieci Cisco CCNA Semestr 2 Routery i podstawy routingu” Wydawnictwo Naukowe PWN SA Warszawa 2007.

[3] Priscilla Oppenheimer „Cisco Projektowanie sieci metodą Top-Down” Wydawnictwo Naukowe PWN SA Warszawa 2006.

[4] Wayne Lewis „Akademia sieci Cisco CCNA Semestr 3 Podstawy przełączania i routing pośredni” Wydawnictwo Naukowe PWN SA Warszawa 2007.

[5] Scott Muller „Rozbudowa i naprawa sieci Wydanie Drugie” Wydawnictwo Helion 2004

[6] Karol Krysiak „ Sieci komputerowe Kompendium” Wydawnictwo Helion 2003.

[7] Brian Komar „TCP/IP dla każdego” Wydawnictwo Helion 2002

[8] http://www.cisco.com. - Enhanced Interior Gateway Routing Protocol -Document ID: 16406 – stan na dzień 13.02.2011

Spis rysunków, tabel, listingów

Spis załączników