POLITECHNIKA KRAKOWSKA
IM. TADEUSZA KOŚCIUSZKI
WYDZIAŁ FIZYKI MATEMATYKI I INFORMATYKI
KIERUNEK INFORMATYKA

KAROLINA JOPEK

PROBLEMATYKA DOBORU OPTYMALNEGO PROTOKOŁU ROUTINGU DLA WYBRANYCH TOPOLOGII SIECI KOMPUTEROWYCH

THE ISSUE OF SELECTION OF THE OPTIMAL ROUTING PROTOCOL FOR SELECTED COMPUTER NETWORK TOPOLOGY

PRACA INŻYNIERSKA
STUDIA STACJONARNE

Promotor: Dr inż. Mariusz Święcicki

Kraków 2013

Spis treści

1. Wstęp 4
1.1 Cel i zakres pracy 4
1.2 Układ pracy 4
2. Podstawowe wiadomości o sieciach komputerowych i protokołach routingu 6
2.1 Sieci komputerowe 6
2.1.1 Podział sieci 6
2.1.2 Topologie Sieci komputerowych 6
2.1.3 Zagadnienie routingu 14
2.1.4 Routing statyczny 15
2.1.5 Routing dynamiczny 16
2.2 Omówienie wybranych protokołów routingu dynamicznego 17
2.2.1 RIP wersja 1 17
2.2.2 RIP wersja 2 19
2.2.3 EIGRP 20
2.2.4 OSPF 24
3. Opis części praktycznej 27
3.1 Infrastruktura sieciowa wykorzystująca konfiguracje routingu statycznego 27
3.1.1 Opis i schemat zaprojektowanej sieci 27
3.1.2 Opis konfiguracji sprzętu dla poszczególnych protokołów routingu 28
3.1.3 Porównanie czasów działania sieci dla routingu statycznego i dynamicznego 30
3.1.4 Podsumowanie 31
3.2 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego RIPv1. 32
3.2.1 Opis i schemat zaprojektowanej sieci 32
3.2.2 Konfiguracja sprzętu dla poszczególnych protokołów routingu 33
3.2.3 Porównanie czasów działania sieci 36
3.2.4 Podsumowanie 37
3.3 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego RIPv2. 38
3.3.1 Schemat zaprojektowanej sieci 38
3.3.2 Badanie zawartości aktualizacji routingu 39
3.3.3 Porównanie czasów działania sieci 42
3.3.4 Podsumowanie 43
3.4 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego OSPF. 44
3.4.1 Schemat zaprojektowanej sieci 44

3.4.2 Badanie zawartości aktualizacji routingu 45
3.4.3 Porównanie czasów działania sieci 49
3.4.4 Podsumowanie 50
3.5 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego EIGRP. 51
3.5.1 Schemat zaprojektowanej sieci 51
3.5.2 Badanie zawartości aktualizacji routingu 52
3.5.3 Porównanie czasów działania sieci 54
3.5.4 Podsumowanie 56
Zakończenie 57
Spis rysunków 60
Spis tabel 61
Spis wzorów 62
Spis listingów 63
Spis załączników: 64
Bibliografia 65

1. Wstęp

W dzisiejszym świecie sieci komputerowe odgrywają bardzo ważną rolę ż życiu człowieka. Spotykamy się z nimi na każdym kroku. Potrzebują ich zarówno duże korporacje, małe firmy jak i typowe gospodarstwa domowe, posiadające wiele urządzeń połączonych w jedną sieć. Powstają sieci bardzo rozbudowane, które muszą w swojej strukturze obsłużyć wiele usług i zapewnić komunikację między różnymi urządzeniami tworzącymi daną topologię. Aby tego dokonać potrzebne jest stworzenie odpowiedniego środowiska, które sprosta tym wymaganiom, jak również konieczne jest zastosowanie odpowiednich technik, które będą wstanie pokierować całym ruchem w sieci. Opisanym powyżej wymaganiom są wstanie sprostać protokoły routingu, które w zależności od ich rodzaju, poradzą sobie z specyficznymi wymaganiami.

1.1 Cel i zakres pracy

Celem niniejszej pracy jest przegląd wybranych protokołów routingu dynamicznego pod względem: czasu osiągania zbieżności sieci, skalowalności sieci oraz funkcji umożliwiających ograniczenie zużycia zasobów routera lub zasobów sieci. Zostanie ona podzielona na część teoretyczną i praktyczną. W części teoretycznej znajdą się podstawowe informacje o topologiach sieci komputerowych jak również poruszone zostanie zagadnienie routingu. Część praktyczną natomiast stanowić będzie analiza porównawcza wybranych protokołów routingu.

1.2 Układ pracy

Poniższa praca składa się z trzech głównych rozdziałów: wstępu, podstawowych wiadomości o sieciach komputerowych i protokołach routingu oraz części praktycznej pracy wraz z opisem.

Pierwsze dwa rozdziały mają charakter teoretyczny. W rozdziale drugim opisano podstawowe zagadnienia dotyczące sieci komputerowych, niezbędne do zrozumienia zasady funkcjonowania protokołów routingu. W jego skład wchodzi także dokładne omówienie użytych w projekcie protokołów routingu- statycznego, RIP w wersji 1, RIP w wersji 2, EIGRP, OSPF.

Rozdział trzeci ma charakter praktyczny. Zawiera on opis i schemat zaprojektowanej sieci komputerowej dla każdego z analizowanych protokołów oraz opisy konfiguracji przykładowych routerów wchodzących w jej skład. W dalszej części tego rozdziału znajduje się analiza omawianych protokołów routingu pod względem: czasu osiągania zbieżności, zachowania sieci w przypadku awarii, funkcji umożliwiających ograniczenie zużycia zasobów routera i sieci.

Na samym końcu przedstawiono wnioski i przemyślenia dotyczące problematyki wyboru optymalnego protokołu routingu dla danej topologii sieci komputerowej.

2. Podstawowe wiadomości o sieciach komputerowych i protokołach routingu

2.1 Sieci komputerowe

2.1.1 Podział sieci

Sieci komputerowe można podzielić na kilka kategorii, w zależności od rozpatrywanego kryterium.

Ze względu na zasięg wyróżniamy:

- ➔ sieci rozległe (WAN- Wide Area Network)
- ➔ sieci lokalne (LAN- Local Area Network)

Ze względu na medium transmisyjne:

- ➔ Sieci bezprzewodowe
- ➔ Sieci przewodowe

2.1.2 Topologie Sieci komputerowych

Topologia sieci jest to zestaw zasad łączenia wszystkich elementów sieci komputerowej oraz reguł komunikacji przez różnego rodzaju medium transmisyjne. Możemy wyróżnić podział na topologie fizyczną i logiczną sieci komputerowej. Prawidłowy dobór topologii sieci w procesie jej projektowania decyduje o jej przyszłej niezawodności.

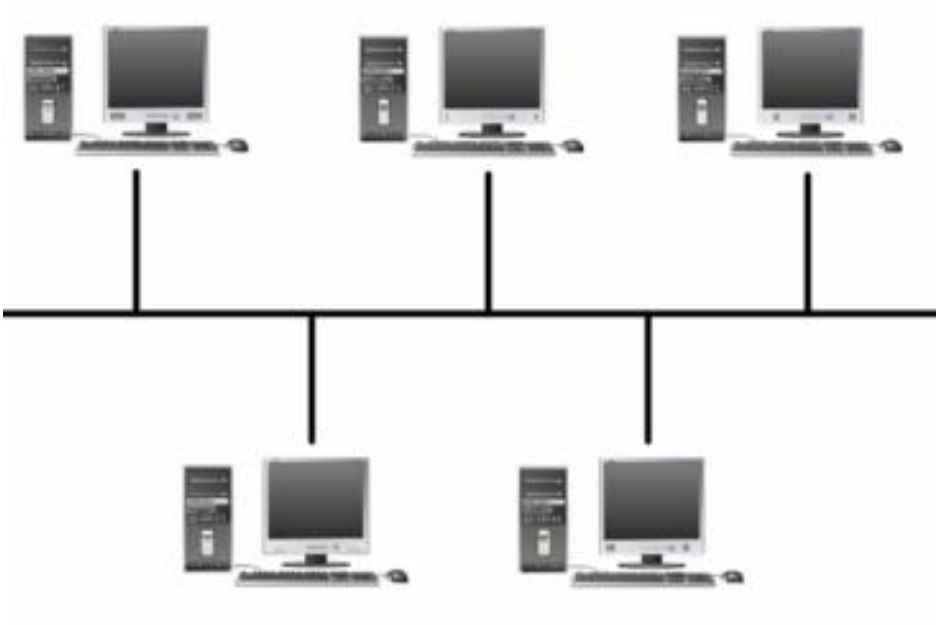
Topologia fizyczna opisuje sposoby fizycznej realizacji łączenia ze sobą komputerów i jest ściśle powiązana z topologią logiczną.

a) Topologia magistrali (ang. *bus topology)*

W topologii tej wszystkie urządzenia połączone są jednym przewodem (zwykle kablem koncentrycznym), który pełni rolę łącza. Kabel ten ma nadaną przez IEEE[1] kategorie 802.3 10b2 (10 base 2). Sieci 10b2 zazwyczaj przesyłają dane z przepustowością 4 Mb/s na

1 IEEE - Instytut Inżynierów Elektryków i Elektroników organizacja skupiająca profesjonalistów. Jednym z podstawowych zadań jest ustalanie standardów konstrukcji, pomiarów itp. dla urządzeń elektronicznych, w tym standardów dla urządzeń i formatów komputerowych. [http://pl.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers]

odległości nie przekraczające 185 metrów. Oba końce przewodu głównego, zwanego magistralą, są zakończone opornikami ograniczającymi o wartości 50Ω, nazywanymi również terminatorami. Chronią one przed odbiciami sygnału. Kiedy komputer wysyła sygnał, rozchodzi się on w przewodzie automatycznie w obu kierunkach. Gdyby sygnał nie napotkał na swojej drodze opornika, to dobiegłby on do końca przewodu głównego, gdzie zmieniłby kierunek. Mogłoby to doprowadzić do zablokowania wszystkich dostępnych szerokości pasma i uniemożliwić wysyłanie sygnałów pozostałym klientom w sieci.[6]

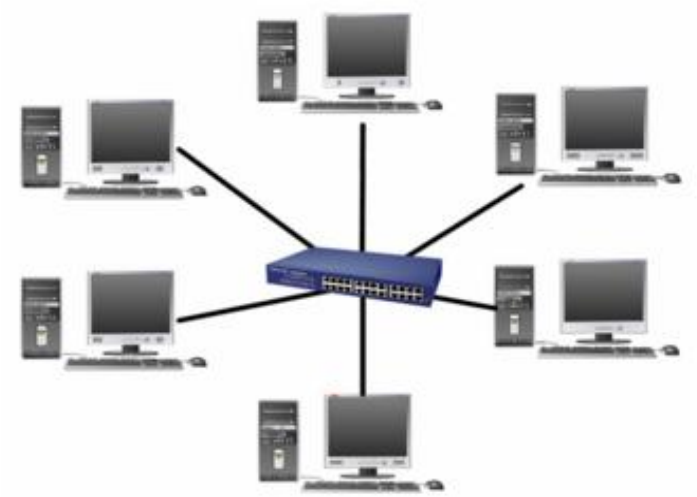


Rysunek 2.1. Topologia magistrali [13]

Zalety magistrali:	**Wady magistrali:**
- małe zużycie kabla - prosta instalacja - niska cena instalacji - bardzo prosta rozbudowa sieci - proste wykrywanie usterek - każdy komputer jest podłączony tylko do jednego kabla - awaria komputera nie powoduje unieruchomienia całej sieci	- konkurencja o dostęp, podział przewodu między wszystkie komputery - awaria kabla powoduje unieruchomienie całej sieci, żaden klient nie jest zdolny do komunikacji. -ograniczenia w odległości i przepustowości. - konieczność zachowania pewnej odległości między punktami przyłączenia poszczególnych stacji, ze względu na możliwość wystąpienia zakłóceń sygnałów.

b) Topologia gwiazdy

W strukturze tej wszystkie klienty łączą się z centralnym urządzeniem, którym zwykle jest koncentrator lub przełącznik. Urządzenie to przejmuje transmisje od nadawcy i przekierowuje dane do odbiorcy. Topologia ta została sklasyfikowana przez IEEE jako 802.3 10bT. Pozwala ona przesyłać dane z prędkością do 1 Gb/s. Natomiast maksymalna odległość pomiędzy komputerem, a urządzeniem centralnym jest ograniczona do 100 metrów, jednak może ona zostać zwiększona poprzez zastosowanie regeneratorów. Topologie te stały się dominujące we współczesnych sieciach LAN. Są one stosunkowo tanie oraz dość łatwe w wykonaniu. [6]

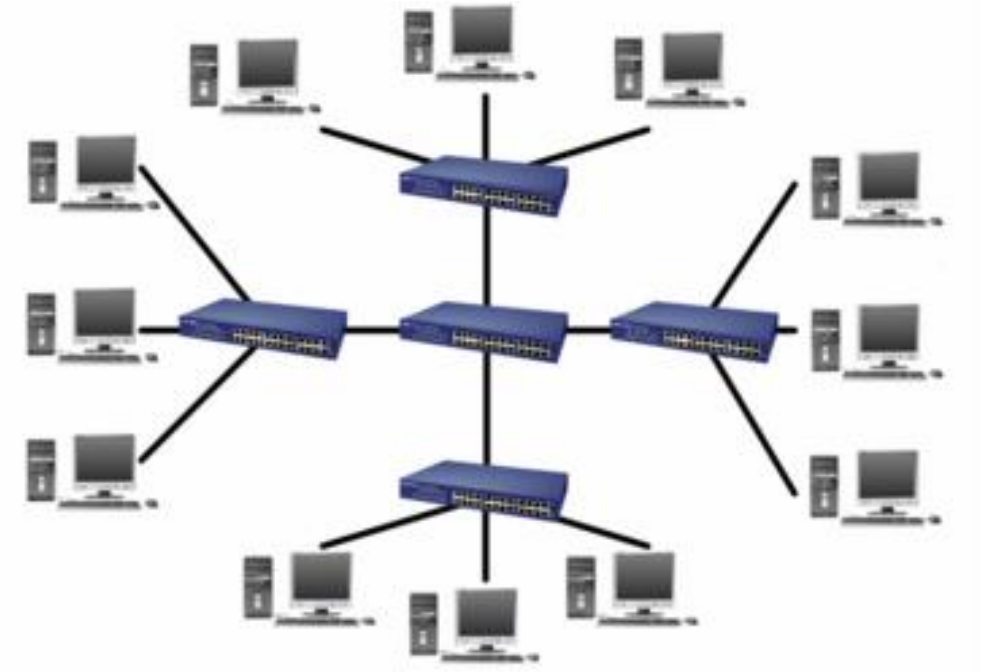


Rysunek 2.2 Topologia gwiazdy [13]

Zalety topologii gwiazdy:	**Wady topologii gwiazdy:**
- łatwa konserwacja i lokalizacja uszkodzeń - prosta rekonfiguracja - proste i szybkie oprogramowanie użytkowe sieci - centralne sterowanie i centralna programowa diagnostyka sieci - możliwe wysokie szybkości transmisji	-duża liczba kabli - wszystkie maszyny wymagają podłączenia wprost do głównego komputera - ograniczona możliwość rozbudowy sieci - działanie sieci zależy od sprawności komputera centralnego - ograniczenie odległości komputera od huba - w przypadku awarii huba przestaje działać cała sieć.

c) Topologia rozszerzonej gwiazdy

W tej topologii każde z urządzeń końcowych działa jako urządzenie centralne dla własnej topologii gwiazdy. Pojedyncze gwiazdy połączone są przy użyciu koncentratorów lub przełączników. Topologia ta ma charakter hierarchiczny i może być konfigurowana w taki sposób, aby ruch pozostawał lokalny. Jest ona stosowana głównie w przypadku rozbudowanych sieci lokalnych oraz sieci kampusowych.

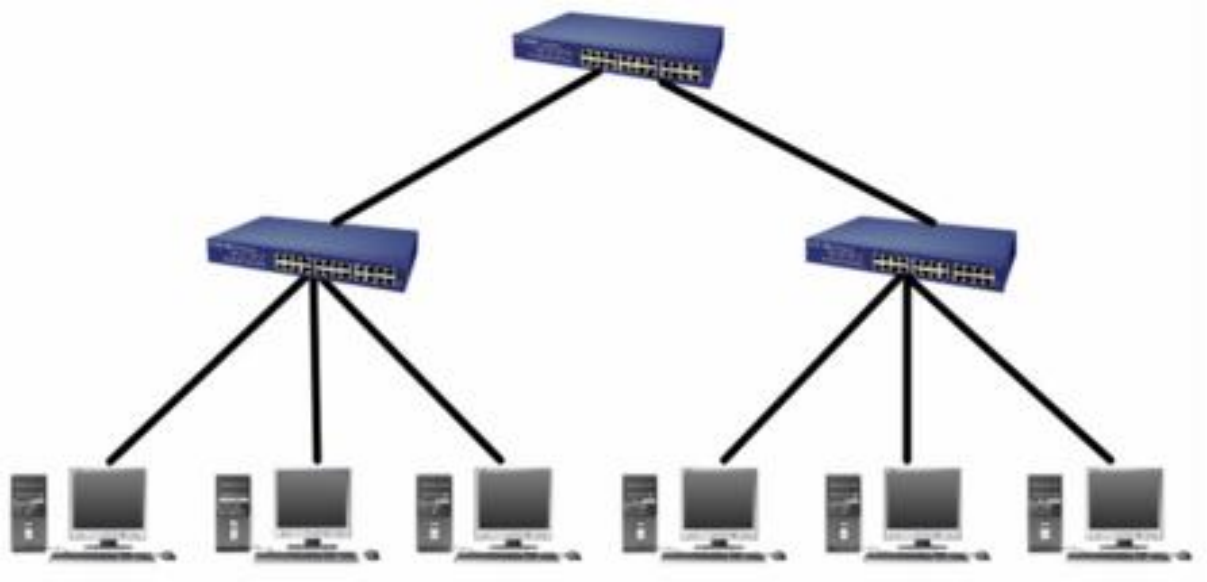


Rysunek 2.3. Topologia rozszerzonej gwiazdy [13]

Zalety rozszerzonej gwiazdy	**Wady rozszerzonej gwiazdy**
- przejrzystość konstrukcji, - praktycznie brak możliwości awarii całej sieci - pozwala na stosowanie krótszych przewodów. - ogranicza liczbę urządzeń, które muszą być podłączone z centralnym węzłem.	- Wysoki koszt związany z zakupem okablowania oraz dodatkowych koncentratorów.

d) Topologia drzewa (hierarchiczna)

Topologia hierarchiczna jest bardzo podobna do topologii rozszerzonej gwiazdy, jednak różni się sposobem działania. Jest ona utworzona z wielu magistrali liniowych, które są połączone łańcuchowo. W topologii tej urządzenia aktywne, oprócz regeneracji sygnału, pełnią rolę urządzeń sterujących dostępem do sieci. Topologia hierarchiczna przypomina strukturę drzewa, od którego odchodzą gałęzie. Budowa takiej topologii polega na tym, iż posiadamy jeden główny koncentrator, następnie od niego odchodzą kable do kolejnych koncentratorów oraz stacji roboczych. Natomiast od tych nowych koncentratorów odprowadzone są kolejne kable do kolejnych koncentratorów. W efekcie tworzone są w ten sposób kolejne poziomy drzewa. Na końcu takiego drzewa znajdują się pojedyncze urządzenia podłączone do magistral.

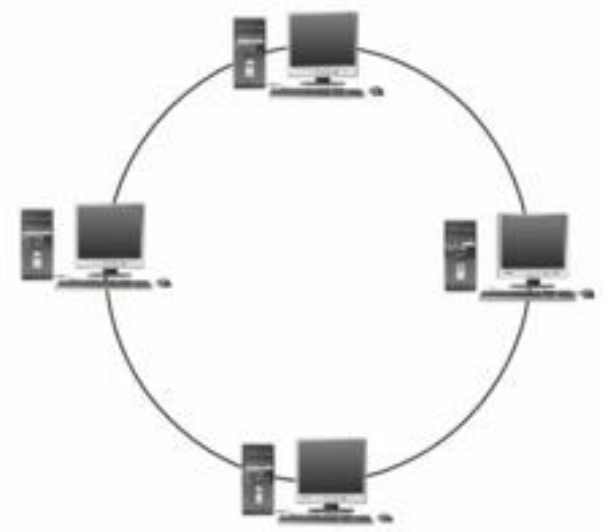


Rysunek 2.4. Topologia hierarchiczna [13]

Zalety topologii drzewa	**Wady topologii drzewa**
- prosta rozbudowa sieci poprzez dodawanie rozgałęźników - łatwa rekonfiguracja sieci - sieć zwykle może przetrwać uszkodzenie komputera lub kabla - łatwa lokalizacja uszkodzeń.	- duża liczba kabli - zależność pracy sieci od głównej magistrali.

e) Topologia pierścienia

Topologia pierścieniowa jest często stosowana przy łączeniu komputerów ze sobą za pomocą kabla światłowodowego. W topologii tej każdy przyłączony do sieci host ma dwa połączenia- po jednym z każdym swoim najbliższym sąsiadem. Połączenie takie tworzy fizycznie pierścień. Dane przesyłane są wokół pierścienia w jednym kierunku. Aby móc umieścić dane w sieci, klient musi posiadać żeton (ang. token) umożliwiający dostęp do sieci. W sieci dostępny jest tylko jeden żeton i przekazywany jest on w logicznym pierścieniu. Topologia ta jest stosowana np. w sieciach Token Ring, FDDI.



Rysunek 2.5. Topologia pierścienia [13]

Zalety topologii pierścienia	**Wady topologii pierścienia**
- małe zużycie kabla - możliwość zastosowania światłowodów - możliwe są wysokie osiągi sieci, gdyż każdy kabel łączy dwa konkretne komputery	- awaria pojedynczego kabla lub komputera powoduje przerwanie pracy całej sieci jeśli nie jest zainstalowany dodatkowy sprzęt - złożona diagnostyka sieci - trudna lokalizacja uszkodzeń - trudna rekonfiguracja sieci - problematyczna rozbudowa sieci, jeśli w pierścieniu jest wiele stacji

f) Topologia podwójnego pierścienia

Topologia podwójnego pierścienia jest odmianą topologii pierścienia. Działa ona na takiej samej zasadzie, co sieć opierająca się na topologii pierścienia. Różnica polega na dodaniu dodatkowego pierścienia łączącego te same urządzenia. W danej chwili działa tylko jeden pierścień. Drugi pierścień stanowi po prostu rolę kabla zapasowego, w razie awarii. Takie rozwiązanie umożliwia podtrzymanie działania sieci w przypadku awarii jednej z jej części.

Rysunek 2.6. Topologia podwójnego pierścienia.
Opracowanie własne na podstawie [13]

Zalety topologii podwójnego pierścienia	**Wady topologii podwójnego pierścienia**
- małe zużycie kabla - możliwość zastosowania światłowodów - odporność na awarie	- złożona diagnostyka sieci - trudna lokalizacja uszkodzeń - trudna rekonfiguracja sieci - problematyczna rozbudowa sieci, jeśli w pierścieniu jest wiele stacji

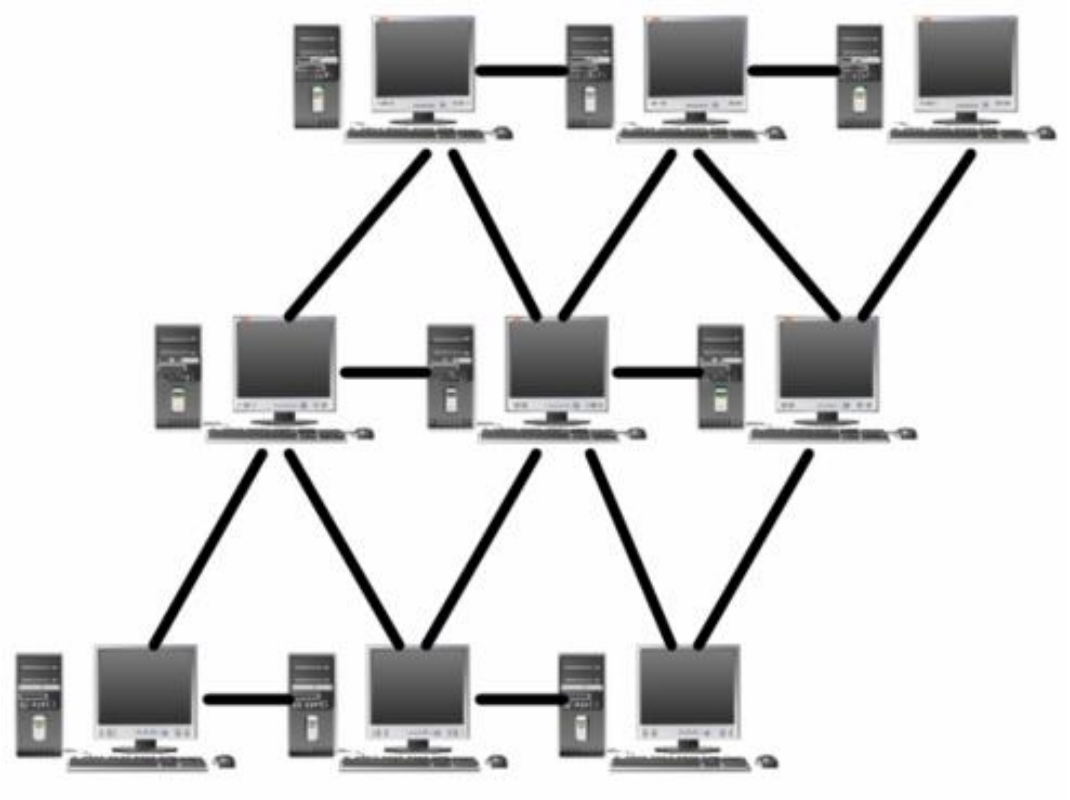
g) Topologia siatki (oczkowa)

W topologii siatki każdy host ma własne bezpośrednie połączenie z wszystkimi pozostałymi komputerami. Topologia ta bardzo przypomina pajęczynę . Sieć ta charakteryzuje się brakiem wymiany danych pomiędzy poszczególnymi komputerami, komunikacja następuje poprzez bezpośrednie połączenie.

Wyróżniamy dwa typy sieci opartych na topologii siatki:

- **pełna siatka** (*ang. Full Mesh*)- każdy węzeł sieci ma fizyczne, albo wirtualne połączenie z każdym innym węzłem,
- **częściowa siatka** (*ang. Partial Mesh*)- węzły mają różną ilość połączeń sieciowych do innych węzłów

Na podobnej zasadzie jest zbudowana cała sieć internetowa. Istnieje bardzo duża liczba ścieżek, które teoretycznie prowadzą do każdego miejsca w sieci.



Rysunek 2.7. Topologia siatki [13]

Zalety topologii siatki	**Wady topologii siatki**
- wysoka prędkość transmisji - odporność na uszkodzenia (niezawodność). - brak kolizji - przesyłanie danych wieloma ścieżkami	- wysokie koszty urządzeń sieciowych oraz okablowania - skomplikowana budowa - kłopotliwą rozbudowa

Topologia logiczna określa standardy umożliwiające bezbłędną komunikację poszczególnych komputerów w sieci. Jest ona zdefiniowana przez standard IEE (Institute of Electrical and Eletronics). W topologii logicznej możemy jeszcze wyróżnić:

Topologia rozgłaszania – polega na wysyłaniu przez host danych, do wszystkich hostów podłączonych do medium. Kolejność korzystania z medium określona jest według reguły „kto pierwszy wyśle, pierwszy zostanie obsłużony" (ang. first come, first serve). Siecią wykorzystującą tą topologie jest Ethernet.

- IEEE 802.3 – 10 Mb Ethernet
- IEEE 802.3u – 100 Mb Ethernet
- IEEE 802.3x – Full Duplex Ethernet
- IEEE 802.3z – 1 Gb Ethernet

Topologia przekazywania tokenu (żetonu) - polega na kontrolowaniu dostępu do sieci poprzez przekazywanie elektronicznego tokenu. Host posiadający w danym momencie token może skorzystać z medium. Gdy nie ma on aktualnie zadań, przekazuje token kolejnemu hostowi i cały cykl się powtarza.

- IEEE 802.5 – Token ring
- IEEE 802.6 – Sieci metropolitalne (MAN)
- FDDI

2.1.3 Zagadnienie routingu

Router jest urządzeniem sieciowym, pracującym w warstwie trzeciej modelu OSI. Składa się z tych samych podstawowych komponentów co zwykły komputer PC. Posiada procesor, pamięć, magistrale systemową oraz interfejsy wejścia/wyjścia. Tak jak komputery wymagają systemów operacyjnych do uruchamiania aplikacji, tak routery wymagają oprogramowania IOS (ang. Internetwork Operating Sytsem) do uruchamiania plików konfiguracyjnych zawierających instrukcje i parametry sterujące przepływem komunikacji do i z routerów. Mino iż routery mają wiele wspólnych cech z zwykłymi komputerami, są one tak zaprojektowane, aby wykonywać pewne specyficzne funkcje, które nie są przeznaczone dla zwykłych komputerów. Służą one między innymi do łączenia różnych sieci komputerowych, pełniąc tym samym rolę węzła komunikacyjnego, mającego za zadanie

przesyłania danych jak najlepszą i najszybsza drogą. Proces ten nosi nazwę routingu, trasowania lub rutowania.

Termin routingu posiada wiele znaczeń w zależności od kategorii, w której go rozpatrujemy. W informatyce routing odnosi się do sposobu wyznaczania drogi lub trasy, prowadzącej wysyłane dane do miejsca przeznaczenia. Żaden z hostów w sieci nie ma wpływu na przebieg całej trasy pakietu danych przesyłanego przez sieć. Za wyznaczanie tych tras odpowiedzialne są kolejne routery w sieci. Router podejmuje decyzje bazując na adresie IP hosta docelowego zawartym w pakiecie. Wszystkie urządzenia na całej drodze pakietu używają tego adresu IP, aby przesłać dane we właściwe miejsce. Aby router podejmował właściwe decyzje musi nauczyć się jaka jest trasa do odległej sieci. Routery są w stanie przeprowadzać routing na dwa podstawowe sposoby. Jednym ze sposobów jest wykorzystywanie wcześniej zaprogramowanych statycznych tras. Taką formę nazywamy routingiem statycznym. Innym rozwiązaniem jest zastosowanie routingu dynamicznego, który opiera się na obliczaniu tras z wykorzystaniem jednego z dynamicznych protokołów routingu (zagadnienie to omówiono dokładniej w dalszej części pracy).

2.1.4 Routing statyczny

Routing statyczny jest najprostszą forma trasowania. Konfiguracja routingu statycznego polega na ręcznym wprowadzaniu przez administratora tras definiujących routing. Router, który jest zaprogramowany na routing statyczny przesyła pakiety poprzez ściśle ustalone porty. Podczas tworzenia tras wymagane jest tylko podanie adresu sieci docelowej i interfejsu routera, przez który ma zostać wysłany pakiet. Router nie musi nawet podejmować prób odnalezienia dostępnych tras, ani uzyskiwać o nich informacji. W dużej sieci ręczne utrzymywani tablic routingu wymaga bardzo dużej ilości poświęconego czasu, gdyż każda zmiana w topologii sieci, czy też jej uszkodzenie, wymaga dokonania zmian w konfiguracji routingu. W małych sieciach, konfiguracja statycznego routingu wymaga mniejszego nakładu pracy administratora. Zaletą takiej formy trasowania jest większa wydajność zasobów, jak również wykorzystywanie mniejszej szerokości pasma transmisji. Statyczny routing wymaga znacznie mniej pamięci, gdyż nie są marnowane cykle procesora na obliczanie tras wędrówki pakietów danych. Jednak mimo swoich zalet, routing statyczny posiada wiele ograniczeń, stąd tez nawet w sieciach, gdzie jest planowany do wdrożenia, najczęściej współdziała z routingiem dynamicznym. [7]

2.1.5 Routing dynamiczny

Routingiem dynamicznym możemy nazwać zestaw komunikatów, procesów i algorytmów, służących do komunikacji między routerami, pozwalających na wymianę informacji o sieciach oraz umożliwiających budowanie tablicy routingu routerów [3].

Routing dynamiczny umożliwia wymianę danych o aktualnych trasach i ich stanie pomiędzy routerami. Protokoły routingu dynamicznego wyznaczają najlepszą drogę do celu, jak również ustalają nową drogę (w sytuacji gdy na przykład zmieni się topologia sieci lub ulegnie ona awarii), co pozwala na bieżące reagowanie na zachodzące zmiany w sieci. Każdy router podczas uruchamiania wie tylko o jednej sieci. Następnie ogłasza on innym routerom do niego podłączonym to, co wie, inne routery natomiast odpowiadają tym co one wiedzą.[3]

Protokoły routingu możemy podzielić ze względu na:

- obszar działania:
    - wewnętrzne (Interior Gateway Protocols - IGP). Działają one wewnątrz sieci lokalnych. Są proste i mało obciążają routery. Zaliczamy do nich - RIPv1, RIPv2, EIGRP, OSPF.
    - zewnętrzne (Exterior Routing Protocols - EGP). Działają na zewnątrz sieci lokalnych. W tej kategorii wyróżniamy BGP.
- sposób działania/stosowany algorytm :
    - protokoły typu dystans-wektor (Distance Vector) - nawołują każdy router sąsiadujący do przesłania całej lub części swojej tablicy routingu. Protokoły bazują na znalezieniu dystansu, czyli liczby skoków i wektora oraz właściwego kierunku do celu. Przykładami tego typu są protokoły RIP i EIGRP
    - protokoły stanu łącza (Link State) - wysyłają informacje o trasach do wszystkich routerów tworząc w ten sposób mapę całej sieci. Osiągane jest to poprzez wymianę tak zwanych. LSA (ang. link-state advertisements) z innymi routerami w sieci. Przykładem tego typu protokołów jest OSPF

- hybrydowe protokoły routingu- mają cechy zarówno protokołów wektora odległości jak i stanu łącza. Przykładem tego typu protokołu jest EIGRP.

- wykorzystanie maski sieci:

  - Routing klasowy - informacja o masce sieci nie jest rozsyłana pomiędzy routerami. Klasa sieci rozpatrywana jest według danego adresu IP

  - Routing bezklasowy - informacja o masce sieci jest rozsyłana pomiędzy routerami

2.2 Omówienie wybranych protokołów routingu dynamicznego

2.2.1 RIP wersja 1

Routing Information Protocol jest jednym z najstarszych protokołów routingu, który do obliczania tras wykorzystuje algorytmy distance-vector. Został zaprojektowany z myślą o małych sieciach, o nieskomplikowanej topologii. Standard protokołu RIP jest opisany w dokumentach RFC[2] 1058 i 1723 (pierwszy z nich opisuje implementację protokołu, natomiast drugi jego zaktualizowaną wersję - RIPv2).

Działanie

Protokół RIP wykorzystuje dwa typy komunikatów: komunikaty żądania i odpowiedzi. Interfejs na którym został skonfigurowany omawiany protokół, zaraz po uruchomieniu wysyła komunikat ‘żądanie’ do wszystkich swoich sąsiadów, wymagając od nich aby wysyłali w odpowiedzi swoje pełne tablice routingu. Każdy sąsiad mający włączony protokół routingu RIP odsyła komunikat ‘odpowiedź’. Router odbierając odpowiedzi , ocenia każdy wpis trasy. W sytuacji gdy dany wpis trasy jest nowy, trasa ta jest instalowana w tablicy routingu routera. Jeżeli natomiast trasa ta znajduje się już w tablicy, a w nowym wpisie liczba skoków jest mniejsza, to wpis zostaje zaktualizowany. Komunikacja w działającej sieci polega na wysyłaniu przez routery, z wszystkich interfejsów z protokołem

[2] RFC (Request For Comments) to seria dokumentów wysyłanych do IETF (Internet Engineering Task Force) w celu zaproponowania internetowego standardu albo przekazywania nowych koncepcji , informacji.

RIP, aktualizacji z własną tablica routingu. Routery RIP wysyłają pełne tablice routingu co 30 sekund. Umożliwia to informowanie sąsiadów RIP o wszystkich aktualnych trasach.

Jedyną metryką protokołu RIP jest liczba skoków. Gdy osiąga ona wartość 16 skoków, oznacza to, że trasa jest nieosiągalna. Stad też łatwo zauważyć, że protokółu RIP można używać tylko w sieciach, w których pomiędzy dwiema dowolnymi sieciami znajduje się maksymalnie 15 routerów.

Format komunikatu

Protokół RIP nie ma własnego protokołu warstwy transportowej. Komunikaty RIP są enkapsulowane w segmencie pakietu UDP. Zarówno portem źródłowym, jak i docelowym jest port 520. Informacje przenoszone przez ten protokół, wysyłane są na adres rozgłoszeniowy 255.255.255.255. Sam pakiet został przedstawiony na poniższym rysunku:

+	Bity 0 - 7	8 - 15	16 - 31
0	Polecenie	Numer wersji	Pole zerowe (1)
32	Identyfikator Rodziny Adresów (AFI)		Pole zerowe (2)
64	Adres sieciowy		
96	Pole zerowe (3)		
128	Pole zerowe (4)		
160	Metryka		

Rysunek 2.8 Opis nagłówka protokołu RIPv1 [14]

- **Pole komendy**- wskazuje czy pakiet został wygenerowany jako odpowiedź, czy żądanie.

- **Pole numeru wersji**- Zawiera wersję protokołu RIP, która została wykorzystana do wygenerowania pakietu.

- **Pola zerowe**- początkowo puste pola zostały dodane z myślą z obsłudze większej przestrzeni adresowej w przyszłości. Mają zapewniać większa kompatybilność ze starszymi protokołami podobnymi do protokołu RIP.

- **Pole AFI-** określa rodzinę adresów reprezentowaną przez pole adresu IP.

- **Pole adresu IP-** zawiera adres sieciowy, który może być adresem hosta, sieci, lub bramy domyślnej.

- **Pole metryki**-zawiera licznik metryk pakietu. Wartość ta wzrasta przy każdym kolejnym przejściu przez router.

Cechy protokołu RIP

- Łatwy do skonfigurowania i wdrożenia
- Nie obsługuje VLSM ani CIDR
- Nie obsługuje uwierzytelniania
- Jako jedynej metryki przy wyborze drogi używa liczby skoków
- Niemożność przeskalowania go do użytku w dużych lub bardzo dużych intersieciach
- Stosuje aktualizacje niewyzwalane (czasowe)

2.2.2 RIP wersja 2

Jest ulepszoną wersją protokołu RIP. Format RIPv2 został opracowany na początku lat 90-tych XX wieku jako modyfikacja szeroko stosowanego protokołu RIPv1. Pierwsza wersja protokołu posiadała kilka wad, które ograniczały jego zastosowanie. Poprawiona wersja protokołu usuwa niektóre z tych ograniczeń.

Elementy wyróżniające protokół RIP ver 2:

-obsługuje routing bezklasowy

-umożliwia wysyłanie w aktualizacjach routingu adresów następnego skoku

- umożliwia wysyłanie aktualizacji przy użyciu adresów grupowych

- udostępnia opcje uwierzytelniania

- pozwala na przenoszenie informacji o masce podsieci, co umożliwia zastosowanie techniki VLSM[3]

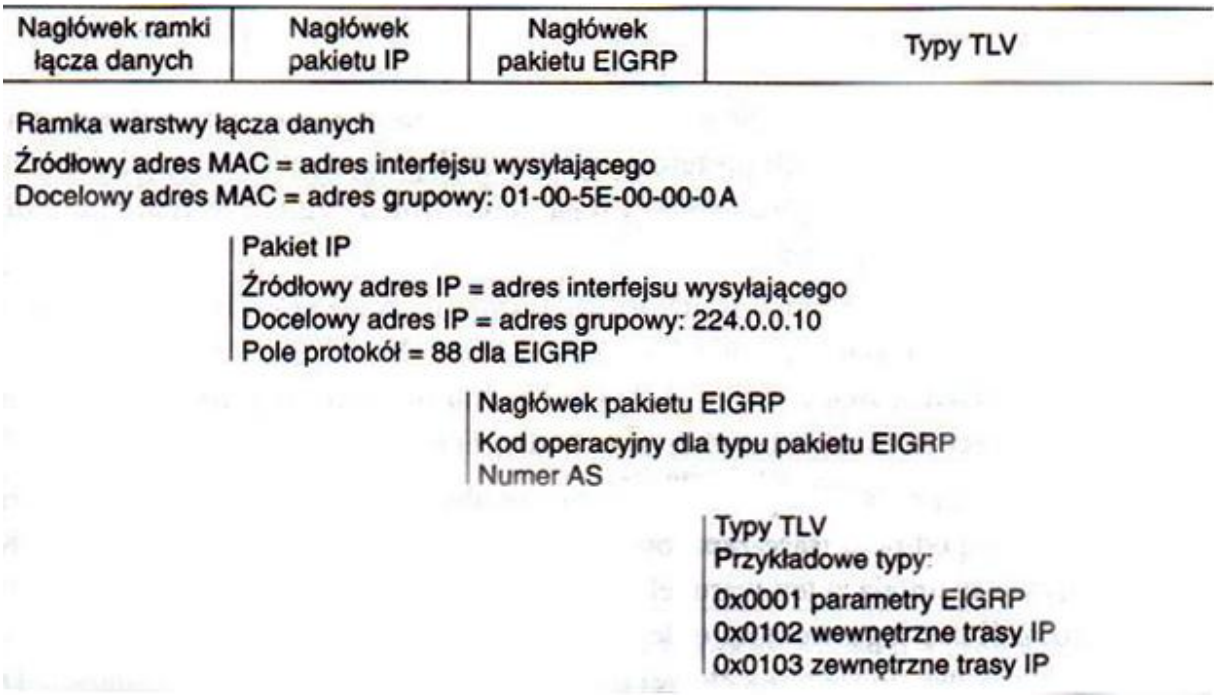
[3] VLSM (Variable Length Subnet Mask) – cecha niektórych protokołów trasowania umożliwiająca podzielenie i rozróżnianie podsieci z już istniejących podsieci.

2.2.3 EIGRP

EIGRP (ang. Enhanced Interior Gateway Routing Protocol). jest protokołem bezklasowym routingu wektora odległości. Stanowi rozwinięcie protokołu IGRP obsługującego jedynie sieci klasowe. Protokół ten został wprowadzony w 1992r przez firmę Cisco. Jedynie routery produkowane przez nią obsługują ten protokół.

W przeciwieństwie o protokołu RIP, EIGRP nie wysyła okresowych aktualizacji, a jedynie aktualizacje częściowe i ograniczone. Oznacza to, że zawierają one tylko informacje o zmianie trasy i wysyłane są tylko do tych routerów, których ta zmiana dotyczy. Do monitorowania stanu połączenia, EIGRP używa lekkiego protokołu hello. Router zakłada, że dopóki otrzymuje pakiety „Hello" od znanych sąsiadujących urządzeń, to sąsiedzi oraz obsługiwane przez sąsiadów trasy funkcjonują prawidłowo. Zjawisko to nazywane jest relacją przylegania.

Format pakietu EIGRP



Rysunek 2.9. Format nagłówka EIGRP [3]

Typy pakietów EIGRP

Do utrzymywania tabel i nawiązywania relacji z sąsiednimi routerami protokół EIGRP wykorzystuje różne rodzaje pakietów.

Wyróżniamy pięć rodzajów pakietów:

- hello
- potwierdzenie (Acknowledgment)
- aktualizacja (Update)
- zapytanie (Query)
- odpowiedź (Reply)

Pakiety hello służą do wykrywania sąsiednich routerów i do tworzenia między nimi relacji sąsiedzkich. Routery EIGRP wysyłają pakiety Hello co 5 sekund na adres grupowy 224.0.0.10. Jeżeli router EIGRP nie otrzyma pakietu od sąsiada w określonym czasie, traktuje to jakby urządzenie to nie działało. W tym momencie algorytm DUAL zaczyna sprawdzanie tablicy routingu.

P**akiety potwierdzeń** (ang. acknowledgment) – są to pakiety „Hello", które pozbawione są danych. Rozsyłane są pojedynczo jako potwierdzenie odbiorcy. Umożliwia to gwarantowaną komunikację między hostami EIGRP. Potwierdzenia takie mogą być dołączane do innych typów pakietów EIGRP, takich jak pakiety odpowiedzi

Pakiety aktualizacyjne (ang. update) używane są w sytuacji, gdy router wykryje nowe urządzenie sąsiednie oraz w przypadku wykrycia zmian w topologii. Routery EIGRP wysyłają wtedy do takiego routera pakiety aktualizacyjne w trybie transmisji pojedynczej (unicast). Umożliwią one uzupełnienie tablicy topologii lub powodują wysyłanie do wszystkich sąsiadów pakietu, w trybie multiemisji (multicast), z informacją o zaistniałej zmianie w topologii.

Pakiety zapytań (ang. query) – są to pakiety z konkretnym zapytaniem wysyłanym do jednego lub wszystkich sąsiednich routerów.

Pakiety odpowiedzi (ang. reply) – to pakiety odpowiadające na pakiety zapytań. Pakiety odpowiedzi zawsze mają charakter transmisji pojedynczej

Metryka protokołu EIGRP

Metryka protokołu EIGRP używana do wyznaczania najlepszej trasy jest bardzo złożona.

Do obliczania metryki protokołu EIGRP mogą być wykorzystane:

- szerokość (przepustowość) pasma,
- opóźnienie,
- niezawodność,
- obciążenie łącza.

Przy założeniu, że do obliczania metryki będziemy wykorzystywać wszystkie wartości, równanie na obliczenie metryki EIGRP będzie miało postać:

$$Metryka\ EIGRP = \left[K1 * szerokość\ pasma\ + \frac{K2 * szerokość\ pasma}{256 - obciążenie}\ +\ K3 * opóźnienie\right] * \left[\frac{K5}{niezawodność + K4}\right] \quad (2.1)$$

**Gdzie wartości od K1 do K5 oznaczają wagi metryki EIGRP*

W praktyce, domyślnie używane są tylko szerokość pasma i opóźnienie, a obliczenia polegają na dodaniu najwolniejszego pasma do sumy opóźnień interfejsów wyjściowych z routera do sieci docelowej, a domyślny wzór metryki EIGRP ma postać:

$$Metryka\ EIGRP = [K1 * szerokość\ pasma\ + K3 * opóźnienie] \quad (2.2)$$

Wartości domyślne:

K1 (szerokość pasma)=1

K2 (obciążenie)=0

K3 (opóźnienie)=1

K4 (niezawodność)= 0

K5 (niezawodność)= 0

Algorytm DUAL

Algorytmem używanym przez protokół EIGRP jest algorytm DUAL- Diffusing Update Algorithm. Pętle routingu, nawet tymczasowe, mogą mieć niekorzystny wpływ na wydajność sieci, a głównym zadaniem tego algorytmu jest zapobieganie tworzeniu się ich. Jego działanie polega na nadzorowaniu śledzenia wszystkich tras rozgłaszanych przez routery. DUAL wykorzystuje trzy oddzielne tabele dla obliczenia trasy. Tabele te są tworzone na podstawie informacji wymienianych między routerami. Wybrane ścieżki nie mogą tworzyć pętli routingu i musza posiadać najniższy koszt. Takie trasy umieszczane są przez protokół DUAL w tablicy routingu i wykorzystywane są w przesyłaniu datagramów. Ze względu na fakt, iż przeliczenia DUAL mogą być dużym obciążeniem dla procesora, należy ich unikać kiedy jest to tylko możliwe. Z tego powodu algorytm tworzy również listę zapasowych tras wolnych od pętli. W sytuacji, gdy podstawowa trasa w tablicy routingu zawiedzie, natychmiast umieszczana jest najlepsza trasa zapasowa.

Cechy protokołu EIGRP

- własnościowy protokół routingu Cisco
- prosty w konfiguracji
- obsługuje VLSM i CIDR
- krótki czas konwergencji.
- używa złożonej metryki
- nie używa liczników wstrzymania jak RIP
- używa algorytmu DUAL
- może działać jak protokół łącze-stan, pozostając protokołem routingu wektora odległości
- aktualizacje z ograniczeniami
- tworzenie przyległości
- tablice sąsiadów i topologii

2.2.4 OSPF

OSPF ang. Open Shortest Path First, podobnie jak RIP oraz EIGRP jest protokołem wewnątrzdomenowym- typu Interior Gateway Protocol (IGP). Jest to protokół bezklasowego routingu łacze-stan. Protokół ten został opracowany na przełomie lat 80-tych i 90-tych XX wieku. jako protokół otwarty, niezależny od producenta. W 1981 roku, w dokumencie RFC 1131 opublikowano pierwszą specyfikacje protokołu OSPF, nastepnie w 1991 roku w dokumencie RFC 1247, John Moy wprowadził OSPFv2. W 1998 roku w dokumencie RFC 2328 pojawiła się specyfikacja OSPFv2, która obowiązuje do dzisiaj.

W przeciwieństwie do protokołu RIP, OSPF charakteryzuje się dobrą skalowalnością, wyborem optymalnych ścieżek, brakiem ograniczenia skoków powyżej 15 oraz przyspieszoną zbieżnością. Przeznaczony jest dla sieci posiadających do 500 routerów w wyznaczonym obszarze trasowania.

Typy pakietów OSPF

Routery korzystające z tego protokołu porozumiewają się ze sobą za pomocą pięciu komunikatów:

- Hello – pakiety hello służą do nawiązywania i utrzymywania relacji sąsiedzkich, czyli przyległości z innymi routerami OSPF.
- DBD (ang.database descriptions) – opis przechowywanych baz danych. Pakiet zawiera skróconą listę bazy danych łącze-stan routera wysyłającego. Wykorzystywany jest również przez routery odbierające do sprawdzania lokalnej bazy danych łącze-stan.
- LSR (ang. requests link-state) –routery odbierające, wysyłając żądanie LSR mogą żądać dodatkowych informacji o dowolnym wpisie z opisu DBD.
- LSU (ang. updates link-state)– pakiety aktualizacji stanów połączeń. Używane są do odpowiadania na LSR i ogłaszania nowych informacji.
- LSAck (ang. acknowledgments links-state)– pakiety potwierdzenia stanów połączeń. Router po odebraniu pakietu LSU, wysyła pakiet LSAck, w celu potwierdzenia odbioru pakietu LSU.

Algorytm OSPF

Każdy router OSPF prowadzi bazę danych łącze-stan, która zawiera wszystkie ogłoszenia LSA odebrane od pozostałych routerów. Po odebraniu przez router OSPF wszystkich ogłoszeń LSA i zbudowaniu lokalnej bazy danych łącze-stan, wykorzystywany jest algorytm SPF (shortest path first) w celu utworzenia drzewa SPF. Służy ono do zapełnienia tablicy routingu IP najlepszymi drogami do każdej sieci

Algorytm SPF określa najlepszą trasę- czyli taką która ma najniższy koszt (metrykę). Algorytm przedstawia sieć jako zespół węzłów połączonych przez łącza punkt-punkt. Każde łącze ma przypisany koszt, każdy węzeł ma określoną nazwę i dysponuje pełną wiedzą na temat wszystkich łączy. Oznacza to, ze znana jest pełna informacja o topologii fizycznej. Wszystkie bazy danych stanów łączy znajdujące się w danym obszarze są takie same. Po odebraniu zmian wprowadzonych w bazie danych stanu łączy, tabela routingu jest obliczana ponownie. Algorytm SPF wyznacza topologię pozbawioną zapętleń, używając konkretnego węzła jako punktu początkowego i odwołuje się do posiadanych informacji o przyległych węzłach.

Metryka OSPF

Metryką stosowaną przez protokół OSPF jest koszt. Dokument RFC 2328 definiuje koszt w następujący sposób:

Koszt jest związany ze stroną wyjściową każdego interfejsu routera. Może on zostać skonfigurowany przez administratora systemu (dokument nie precyzuje, jakich wartości należy używać do ustalenia kosztu).

System Cisco IOS jako kosztu używa łącznej szerokości pasma sieciowych interfejsów wyjściowych z routera do sieci docelowej, [3] zgodnie z poniższym wzorem :

$$Koszt\ OSPF = \frac{10^8}{szerokość\ pasma}\ [bps]$$

$$10^8 - referencyjna\ szerokość\ pasma \tag{2.3}$$

Koszt jest metryką opartą na przepustowości. Interfejsy z większą szerokością pasma mają niższy koszt.

Typ interfejsu	$\mathbf{10^8 b/s}$**=koszt**
Fast Ethernet i szybsze	$10^8/100\,000\ \ 000\ \ b/s\ = 1$
Ethernet	$10^8/10\,000\ \ 000\ \ b/s\ = 10$
E1	$10^8/2\,048\,000\ \ b/s\ = 48$
T1	$10^8/1\,544\,000\,b/s\ = 64$
128 kb/s	$10^8/128\ \ 000\,b/s\ = 781$
64 kb/s	$10^8/64\,000\,b/s\ = 1562$
56 kb/s	$10^8/56\ \ 000\,b/s\ = 1785$

Tabela 2.1. Wartości kosztów OSPF w systemie Cisco w zależności od typu interfejsu. Opracowanie własne na podstawie [3].

Cechy protokołu OSPF

Protokół OSPF ma następujące zalety w stosunku do protokołu RIP:

- trasy obliczone przez protokół OSPF są zawsze wolne od pętli.
- protokół OSPF można przeskalować do użytku w dużych i bardzo dużych intersieciach.
- szybka zbieżność. Ponowna konfiguracja po zmianach w topologii sieci odbywa się szybciej niż w RIP.
- brak ograniczeń dotyczących. liczby przeskoków
- obsługuje VLSM
- wykorzystuje adres rozsyłania grupowego do rozsyłania zmian
- bardziej skuteczna metryka
- możliwość równoważenia obciążenia
- możliwość uwierzytelnienia
- znaczniki tras zewnętrznych (podobnie jak RIPv2)
- podział sieci na obszary wielkości ok. 50 routerów

3. Opis części praktycznej

3.1 Infrastruktura sieciowa wykorzystująca konfiguracje routingu statycznego

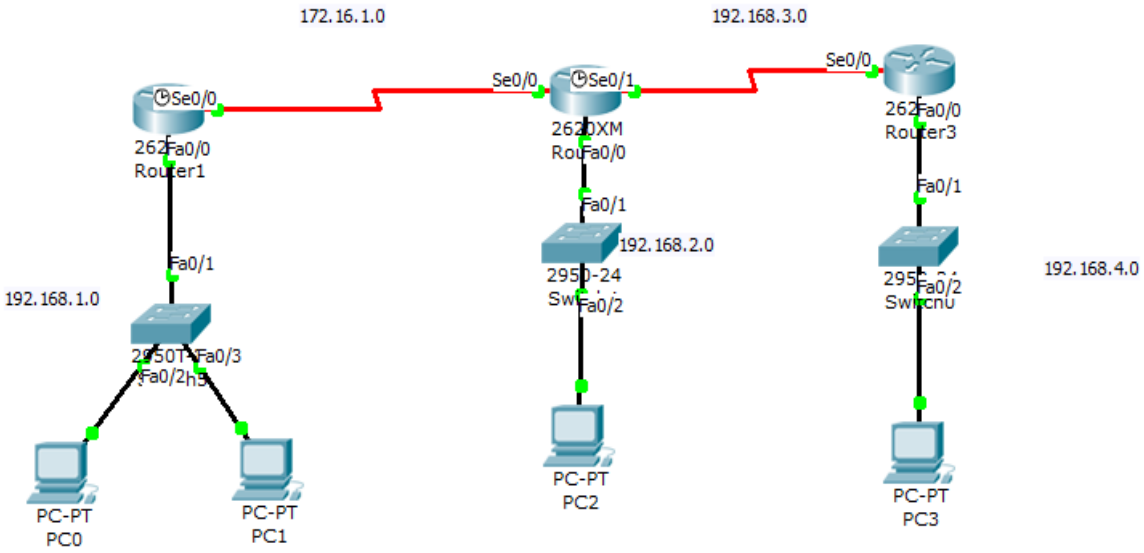
We współczesnym świecie na co dzień mamy do czynienia zarówno z małymi, lokalnymi sieciami danych jak i dużymi, globalnymi. Każda sieć ma swoją specyfikę oraz konkretne wymagania. Osoba zajmująca się sieciami komputerowymi jest odpowiedzialna za prawidłową konfiguracje protokołów routingu, tak aby działanie sieci było jak najbardziej wydajne. Do najważniejszych parametrów sieci można bez wątpienia zaliczyć złożoność topologii sieciowej, liczbę sieci, wymaganie automatycznego dostosowywania się do zmian itp..

Routing statyczny ma jednocześnie wiele zalet i wad. Istnieje wiele argumentów przemawiających za i przeciw używaniu routingu statycznego. Mówiąc o zaletach trasowania statycznego to bez wątpienia są nimi prostota konfiguracji oraz minimalne wykorzystanie procesora. Routing statyczny ma najczęściej zastosowanie w przypadku routingu do i z sieci szczątkowych, czyli sieci do których można dotrzeć tylko jedną trasą. W momencie rozrostu sieci, złożoność konfiguracji wzrasta i takie rozwiązanie przestaje być korzystne. Każda zmiana w topologii sieci wymaga interwencji administratora i „ręcznych" zmian w konfiguracji, co wiąże się z nieadekwatnym do zadania nakładem pracy administratora. Utrzymanie takiej sieci staje się uciążliwe. Są jednak sytuacje, gdy routing statyczny znajduje zastosowanie nawet w dużych i złożonych sieciach. Ma to miejsce w przypadku, gdy chcemy zapewnić wysokie bezpieczeństwo sieci np. dla firmowego połączenia z Internetem.

3.1.1 Opis i schemat zaprojektowanej sieci

Do wykonania sieci został użyty sprzęt firmy CISCO, dostępny w oprogramowaniu Cisco Packet Tracer. Wykorzystano trzy routery (2620XM) oraz trzy switch-e 24-portowe (2950) oznaczone odpowiednio Router 1, Router 2, Router 3 oraz Switch1, Switch2, Switch3.

Dla topologii przedstawionej na poniższym rysunku 13 skonfigurowano protokół routingu statycznego. Plik z konfiguracją został dołączony na płycie CD w katalogu „Packet_Tracer\Routing_statyczny" – nazwa pliku „routing_statyczny.pkt" – opracowanie własne.



Rysunek 3.10. Przykład topologii sieci dla routingu statycznego.

Opracowanie własne.

3.1.2 Opis konfiguracji sprzętu dla poszczególnych protokołów routingu

Na poniższych listingach przedstawiono wynik działania polecenia „show ip route”, prezentującego bieżąca konfiguracje tablic routingu.

Router 1

```
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 not set

       172.16.0.0/24 is subnetted, 1 subnets
       C       172.16.1.0 is directly connected, Serial0/0
       C    192.168.1.0/24 is directly connected, FastEthernet0/0
       S    192.168.2.0/24 is directly connected, Serial0/0
       S    192.168.3.0/24 is directly connected, Serial0/0
       S    192.168.4.0/24 is directly connected, Serial0/0
```

Listing 3.1. Tablica routingu routera R1.

Opracowanie własne.

Router 2

```
      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 not set

           172.16.0.0/24 is subnetted, 1 subnets
      C       172.16.1.0 is directly connected, Serial0/0
      S    192.168.1.0/24 is directly connected, Serial0/0
      C    192.168.2.0/24 is directly connected, FastEthernet0/0
      C    192.168.3.0/24 is directly connected, Serial0/1
      S    192.168.4.0/24 is directly connected, Serial0/1
```

Listing 3.2. Tablica routingu routera R2.

Opracowanie własne.

Router 3

```
      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 not set

           172.16.0.0/24 is subnetted, 1 subnets
      S       172.16.1.0 is directly connected, Serial0/0
      S    192.168.1.0/24 is directly connected, Serial0/0
      S    192.168.2.0/24 is directly connected, Serial0/0
      C    192.168.3.0/24 is directly connected, Serial0/0
      C    192.168.4.0/24 is directly connected, FastEthernet0/0
```

Listing 3.3. Tablica routingu routera R3.

Opracowanie własne.

3.1.3 Porównanie czasów działania sieci dla routingu statycznego i dynamicznego

Badanie przeprowadzono na przykładzie komputera PC1 (192.168.1.6) pingującego komputer PC3 (192.168.4.5).

	Routing statyczny (ms)	RIP wersja 1 (ms)	RIP wersja 2 (ms)	OSPF (ms)	EIGRP (ms)
1	25	33	32	33	31
2	33	43	24	37	44
3	16	22	17	85	36
4	31	36	27	44	31
5	32	32	28	34	31
6	16	34	23	36	32
7	29	26	28	61	44
8	32	19	21	55	40
9	28	35	28	104	32
10	26	34	23	47	31
11	26	32	37	24	30
12	22	33	26	47	33
13	21	21	29	51	34
14	30	37	29	46	29
15	24	31	55	62	19
16	34	37	35	37	25
17	32	29	24	64	35
18	18	30	31	26	44
19	21	38	47	48	25
20	19	25	46	57	61
Średnia	**25,75**	**31,35**	**30,5**	**49,9**	**34,35**

Tabela 3.1. Porównanie czasów działania sieci dla routingu statycznego i dynamicznego. Opracowanie własne.

3.1.4 Podsumowanie

Analizując powyższą tabelę można zauważyć, że w przypadku routingu statycznego opóźnienie było najmniejsze. Dla tak zaprojektowanej sieci routing statyczny okazał się być najkorzystniejszym rozwiązaniem, co było zgodne z wstępnymi oczekiwaniami. Jest to spowodowane tym, że routing statyczny mniej obciąża łącze, gdyż nie musi cyklicznie aktualizować tablic routingu. Ponadto dla routingu statycznego występuje dużo mniejsze zużycie czasu procesora i pamięci, gdyż nie ma konieczności przetwarzania informacji otrzymywanych od innych routerów, jak to ma miejsce w przypadku routingu dynamicznego. W momencie rozrostu sieci, złożoność konfiguracji znacznie by wzrosła i takie rozwiązanie przestałoby być korzystne. Zaprojektowana sieć wykorzystuje sieci szczątkowe, czyli sieci do których można dotrzeć tylko jedną trasą. Tak więc, brak któregokolwiek z routerów uniemożliwiłby dalszą komunikacje zarówno dla protokołów routingu statycznego jak i dynamicznego. Dlatego zbadanie zachowania sieci w przypadku awarii było niemożliwe.

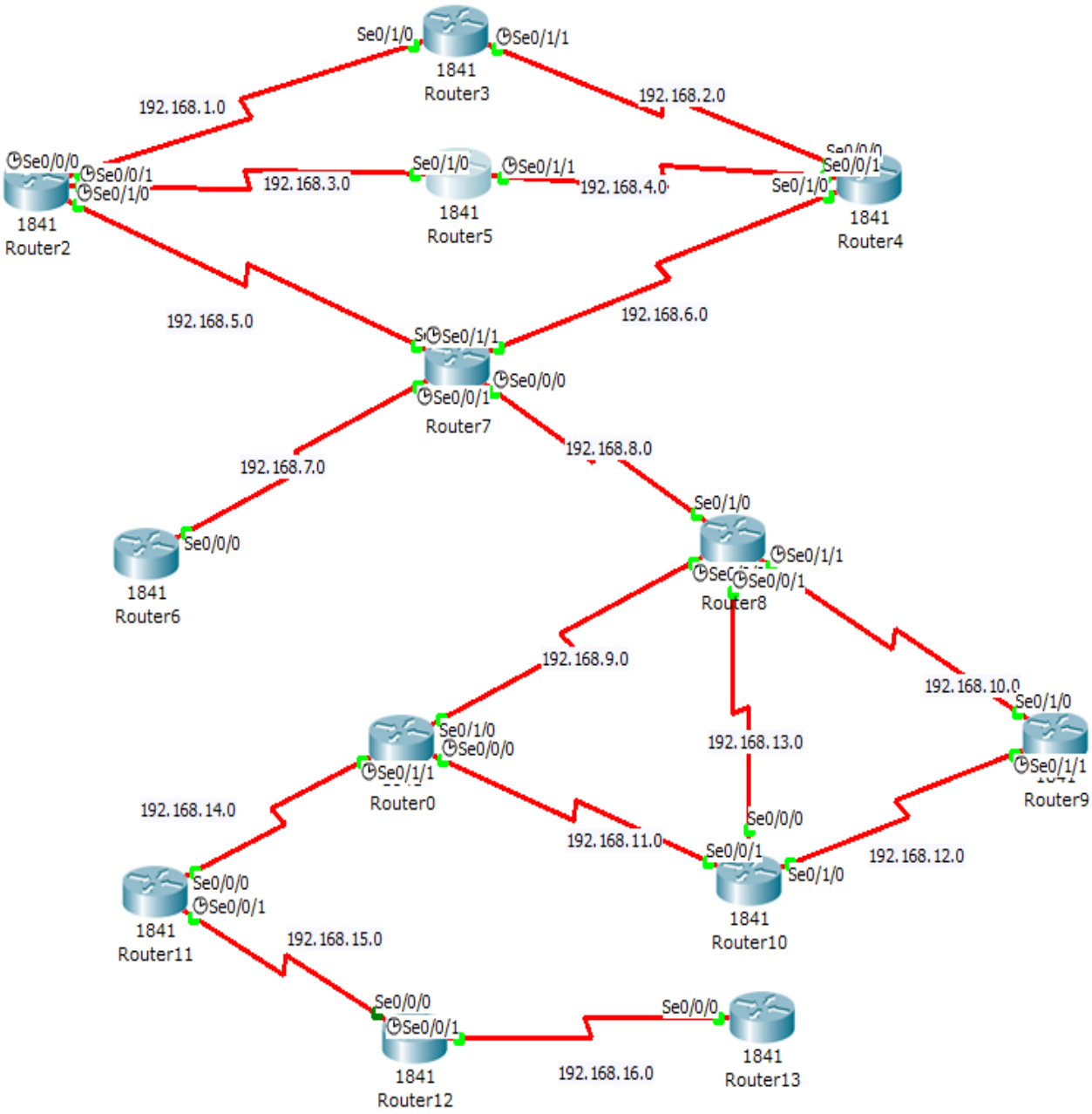
3.2 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego RIPv1.

Protokoły routingu dynamicznego pozwalają administratorowi sieci uniknąć czasochłonnej konfiguracji tras statycznych. Od lat ulegają one ciągłej ewolucji, aby zaspokajać wzrastające zapotrzebowania dużych sieci. Jednym z pierwszych protokołów routingu dynamicznego opracowanych dla pakietów IP był RIPv1. Nie jest on wolny od wad, gdyż nie obsługuje ani sieci nieciągłych, ani VLSM, ale dzięki swojej prostocie i łatwości konfiguracji wciąż jest chętnie używany przez administratorów niewielkich sieci.

3.2.1 Opis i schemat zaprojektowanej sieci

Do wykonania poniższej intersieci został użyty sprzęt firmy CISCO, dostępny w oprogramowaniu Cisco Packet Tracer. Wykorzystano 13 routerów (1841) oznaczonych: Router 0, Router 2, Router 3, Router 4, Router 5, Router 6, Router 7, Router 8, Router 9, Router 10, Router11, Router 12, Router 13.

Dla topologii przedstawionej na poniższym rysunku skonfigurowano protokół routingu dynamicznego RIPv1. Plik z konfiguracją został dołączony na płycie CD w katalogu „Packet_Tracer\RIPv1” – nazwa pliku „RIPv1.pkt” – opracowanie własne.



Rysunek 3.11 Przykład topologii sieci dla routingu dynamicznego RIPv1.

Opracowanie własne.

3.2.2 Konfiguracja sprzętu dla poszczególnych protokołów routingu

Na poniższych listingach przedstawiono wynik działania polecenia „show ip route”, prezentującego tablicę routingu dla wybranych routerów.

Router 7

```
Router#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 not set

      R    192.168.1.0/24 [120/1] via 192.168.5.1, 00:00:15, Serial0/1/0
      R    192.168.2.0/24 [120/1] via 192.168.6.2, 00:00:15, Serial0/1/1
      R    192.168.3.0/24 [120/1] via 192.168.5.1, 00:00:15, Serial0/1/0
      R    192.168.4.0/24 [120/1] via 192.168.6.2, 00:00:15, Serial0/1/1
      C    192.168.5.0/24 is directly connected, Serial0/1/0
      C    192.168.6.0/24 is directly connected, Serial0/1/1
      C    192.168.7.0/24 is directly connected, Serial0/0/1
      C    192.168.8.0/24 is directly connected, Serial0/0/0
      R    192.168.9.0/24 [120/1] via 192.168.8.2, 00:00:20, Serial0/0/0
      R    192.168.10.0/24 [120/1] via 192.168.8.2, 00:00:20, Serial0/0/0
      R    192.168.11.0/24 [120/2] via 192.168.8.2, 00:00:20, Serial0/0/0
R    192.168.12.0/24 [120/2] via 192.168.8.2, 00:00:20, Serial0/0/0
```

Listing 3.4. Tablica routingu routera R7.

Opracowanie własne.

Router 0

```
      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 not set

      R    192.168.1.0/24 [120/3] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.2.0/24 [120/3] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.3.0/24 [120/3] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.4.0/24 [120/3] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.5.0/24 [120/2] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.6.0/24 [120/2] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.7.0/24 [120/2] via 192.168.9.1, 00:00:06, Serial0/1/0
      R    192.168.8.0/24 [120/1] via 192.168.9.1, 00:00:06, Serial0/1/0
      C    192.168.9.0/24 is directly connected, Serial0/1/0
```

```
      R    192.168.10.0/24 [120/1] via 192.168.9.1, 00:00:06, Serial0/1/0
      C    192.168.11.0/24 is directly connected, Serial0/0/0
      R    192.168.12.0/24 [120/1] via 192.168.11.2, 00:00:01, Serial0/0/0
      R    192.168.13.0/24 [120/1] via 192.168.9.1, 00:00:06, Serial0/1/0
                           [120/1] via 192.168.11.2, 00:00:01, Serial0/0/0
      C    192.168.14.0/24 is directly connected, Serial0/1/1
      R    192.168.15.0/24 [120/1] via 192.168.14.1, 00:00:04, Serial0/1/1
      R    192.168.16.0/24 [120/2] via 192.168.14.1, 00:00:04, Serial0/1/1
```

Listing 3.5. Tablica routingu routera R0.

Opracowanie własne.

Router 10

```
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 not set

      R    192.168.1.0/24 [120/3] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.2.0/24 [120/3] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.3.0/24 [120/3] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.4.0/24 [120/3] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.5.0/24 [120/2] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.6.0/24 [120/2] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.7.0/24 [120/2] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.8.0/24 [120/1] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.9.0/24 [120/1] via 192.168.11.1, 00:00:24, Serial0/0/1
                          [120/1] via 192.168.13.1, 00:00:00, Serial0/0/0
      R    192.168.10.0/24 [120/1] via 192.168.13.1, 00:00:00, Serial0/0/0
                           [120/1] via 192.168.12.2, 00:00:25, Serial0/1/0
      C    192.168.11.0/24 is directly connected, Serial0/0/1
      C    192.168.12.0/24 is directly connected, Serial0/1/0
      C    192.168.13.0/24 is directly connected, Serial0/0/0
      R    192.168.14.0/24 [120/1] via 192.168.11.1, 00:00:24, Serial0/0/1
      R    192.168.15.0/24 [120/2] via 192.168.11.1, 00:00:24, Serial0/0/1
      R    192.168.16.0/24 [120/3] via 192.168.11.1, 00:00:24, Serial0/0/1
```

Listing 3.6. Tablica routingu routera R10.

Opracowanie własne.

3.2.3 Porównanie czasów działania sieci

Wyniki testu ICMP Ping dla komunikacji w sieci przedstawione zostały w poniższej tabeli. Badanie przeprowadzono wywołując polecenie „ping 192.168.16.2” z adresu źródłowego 192.168.1.1.

	Routing statyczny (ms)	**RIP wersja 1 (ms)**	**RIP wersja 2 (ms)**	**OSPF (ms)**	**EIGRP (ms)**
1	22	29	19	25	27
2	20	22	22	34	23
3	19	20	18	20	25
4	25	22	21	27	25
5	24	18	20	23	37
6	20	29	24	35	26
7	20	21	20	20	23
8	29	22	23	27	25
9	20	20	20	29	25
10	29	22	37	37	27
11	21	20	20	37	23
12	22	25	20	42	27
13	19	27	22	25	33
14	23	20	17	25	31
15	24	22	24	54	19
16	20	27	23	29	20
17	18	20	21	43	29
18	23	22	22	25	23
19	33	31	21	30	36
20	21	21	24	20	21
Średnia	**22,6**	**23**	**21,9**	**30,3**	**26,25**

Tabela 3.1. Porównanie czasów działania sieci dla routingu statycznego i dynamicznego. Opracowanie własne.

3.2.4 Podsumowanie

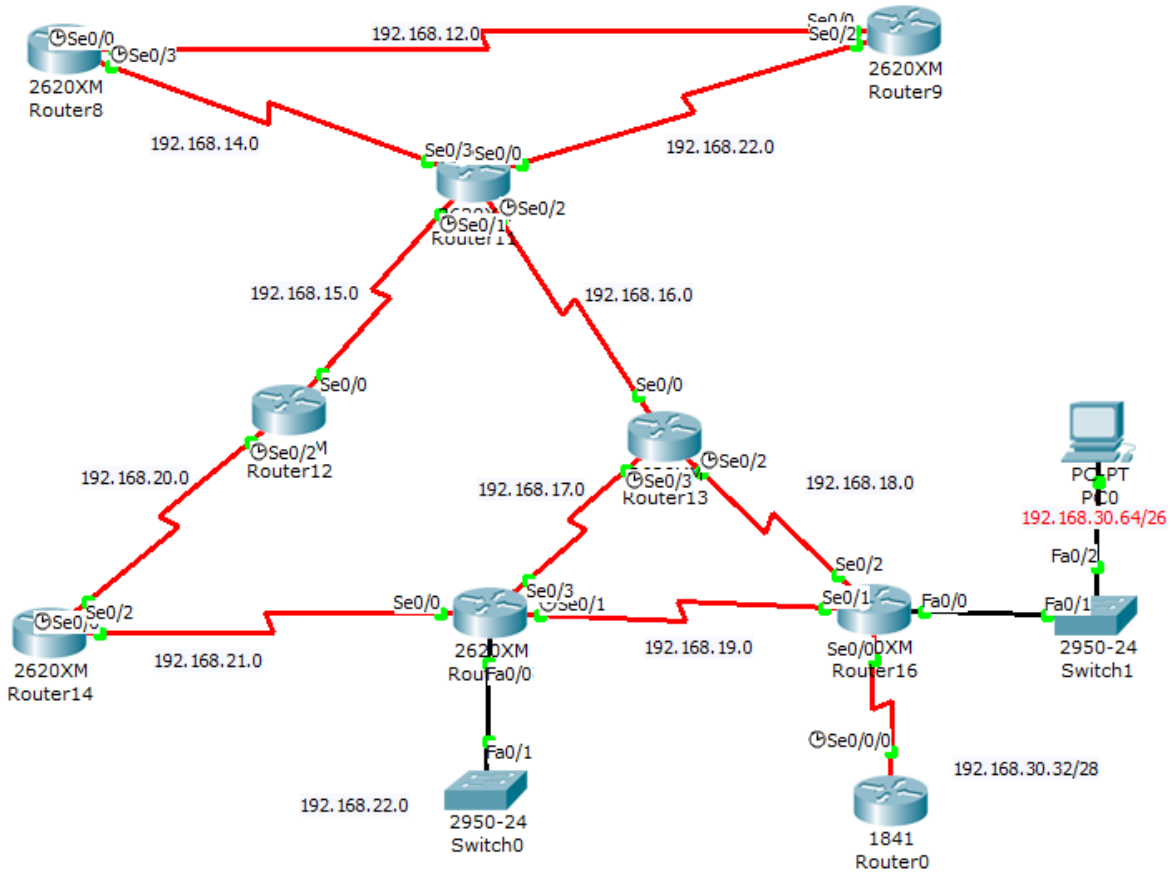
Analizując powyższą tabelkę, można łatwo zauważyć, że dla zaprojektowanej sieci najkorzystniejszym rozwiązaniem byłby routing statyczny lub routing dynamiczny RIP. Wydawać by się mogło, że zastosowanie routingu statycznego będzie najlepszym rozwiązaniem. Przyczyną takiego wrażenia może być fakt, że dla routingu statycznego trasy są z góry ustalone przez administratora i zużycie procesora oraz pamięci jest mniejsze, niż w routingu dynamicznym. Podobnie wygląda kwestia zajętości pasma transmisji, które dla routingu statycznego jest mniejsze, gdyż nie są rozsyłane pakiety rozgłoszeniowe protokołów routingu dynamicznego. Czynniki te znacznie wpływają na obniżenie czasu działania sieci. Jednak należy pamiętać, że ze względu na dużą złożoność sieci konfiguracja tras statycznych staje się problematyczna i takie rozwiązanie przestaje być korzystne. Szczególnie, gdy weźmiemy pod uwagę ewentualne błędy w konfiguracji lub awarie. Dynamiczny protokół RIP automatycznie reaguje na awarię jakiejś z tras routingu, czego nie można powiedzieć o routingu statycznym. Routery RIP standardowo rozgłaszają zawartość swej tablicy routowania średnio co 30 sekund. Jeśli router nie otrzyma od danego sąsiada pakietu RIP przez 180 sekund, zaznacza w swojej tablicy obsługiwane przez niego trasy jako bezużyteczne. Po kolejnych 240 sekundach ciszy router usuwa tę trasę ze swej tablicy. Dodatkowo natychmiast po zajściu zmiany w topologii sieci np. na skutek awarii lub przyłączenia nowego routera rozsyłane są informacje pakietu RIP, co nazywamy odświeżaniem wymuszonym. Stąd też dla sieci o takiej złożoności zalety routingu statycznego nie są wstanie zdominować jego wad. Należy jednak pamiętać, że RIP nie jest oczywiście idealnym protokołem, jednak w tym przypadku jego zastosowanie okazuje się być najkorzystniejszym rozwiązaniem (porównując do innych badanych protokołów routingu dynamicznego).

3.3 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego RIPv2.

Routing Informacjon Protocol w wersji drugiej stanowi rozszerzenie i uaktualnienie badanego wcześniej RIPv1, dlatego tez jego charakter i mechanizmy są podobne. Rozszerzenie to odnosi się głównie do przesyłania dodatkowych, ważnych informacji o trasach w wiadomościach aktualizacyjnych

3.3.1 Schemat zaprojektowanej sieci

Dla topologii przedstawionej na poniższym rysunku skonfigurowano protokół routingu dynamicznego RIPv2. Plik z konfiguracją został dołączony na płycie CD w katalogu „Packet_Tracer\RIPv2" – nazwa pliku „RIPv2.pkt" – opracowanie własne. Wykorzystano dziewięć routerów (2620XM) oraz dwa switch-e 24-potrowe (2950) oznaczone odpowiednio: Router 8, Router 9, Router 11, Router 12, Router 13, Router 14, Router 15, Router 16, Router 0 oraz Switch 0, Switch 1.



Rysunek 12. Przykład topologii sieci dla routingu dynamicznego RIPv2. Opracowanie własne.

3.3.2 Badanie zawartości aktualizacji routingu

Protokół RIP v1 jest protokołem klasowym, którego podstawową cecha jest to, że nie ogłasza on maski podsieci wraz z adresem sieci. Może to powodować pewne problemy przy przetwarzaniu adresów dotyczących sieci i hostów. Rozważmy sieć 192.168.30.0 obecną w zaprojektowanej infrastrukturze, ma ona maskę podsieci 255.255.255.0, tak więc 192.168.30.0 jest numerem sieci, 192.168.30.32 jest numerem podsieci, a 192.168.30.33 jest adresem hosta. Jednak, jeśli host nie zna maski podsieci to interpretacja adresu może być niejednoznaczna. Jeżeli część hosta ma wartość niezerową, nie można wyraźnie określić czy adres oznacza numer podsieci, czy adres hosta. Adres ten jako numer podsieci będzie bezużyteczny bez maski, dlatego przyjęte zostanie, że jest to adres reprezentujący hosta. W celu uniknięcia opisywanej dwuznaczności hosty nie mogą rozsyłać informacji o podsieciach do hostów, które przypuszczalnie nie znają odpowiedniej maski tej podsieci.[9]

Na poniższych listingach przedstawiono wynik polecenia **debug ip rip** dla routera „Router 16”, umożliwiającego zbadanie zawartości aktualizacji routingu, które są wysyłane i odbierane przez ten router. Poniższy listing zawiera wynik tego polecenia zarówno dla routera korzystającego z protokółu RIPv1 jaki i RIP v2, aby umożliwić zauważenie różnic między tymi protokołami.

Wynik działania polecenia debug ip rip dla routera „Router 16” wykorzystującego protokół RIPv1(lewa kolumna) oraz RIPv2(prawa kolumna):

```
RIP: sending  v1 update to
255.255.255.255 via FastEthernet0/0
(192.168.30.65)
RIP: build update entries
      network 192.168.12.0 metric 4
      network 192.168.14.0 metric 3
      network 192.168.15.0 metric 3
      network 192.168.16.0 metric 2
      network 192.168.17.0 metric 2
      network 192.168.18.0 metric 1
      network 192.168.19.0 metric 1
      network 192.168.20.0 metric 3
      network 192.168.21.0 metric 2
      network 192.168.22.0 metric 2
```

```
RIP: sending  v2 update to 224.0.0.9 via
FastEthernet0/0 (192.168.30.65)
RIP: build update entries
  192.168.12.0/24 via 0.0.0.0, metric 4, tag 0
  192.168.14.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.15.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.16.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.17.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.18.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.19.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.20.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.21.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.22.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.30.32/28 via 0.0.0.0, metric 1, tag
```

```
RIP: sending  v1 update to
255.255.255.255 via Serial0/2
(192.168.18.2)
RIP: build update entries
      network 192.168.19.0 metric 1
      network 192.168.20.0 metric 3
      network 192.168.21.0 metric 2
      network 192.168.22.0 metric 2
      network 192.168.30.0 metric 1
RIP: received v1 update from
192.168.19.1 on Serial0/1
      192.168.12.0 in 4 hops
      192.168.14.0 in 3 hops
      192.168.15.0 in 3 hops
      192.168.16.0 in 2 hops
      192.168.17.0 in 1 hops
      192.168.20.0 in 2 hops
      192.168.21.0 in 1 hops
      192.168.22.0 in 1 hops
RIP: received v1 update from
192.168.18.1 on Serial0/2
      192.168.12.0 in 3 hops
      192.168.14.0 in 2 hops
      192.168.15.0 in 2 hops
      192.168.16.0 in 1 hops
      192.168.17.0 in 1 hops
      192.168.20.0 in 3 hops
      192.168.21.0 in 2 hops
      192.168.22.0 in 2 hops
```

```
RIP: sending  v2 update to 224.0.0.9 via
Serial0/2 (192.168.18.2)

RIP: build update entries
  192.168.19.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.20.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.21.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.22.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.30.0/24 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 192.168.19.1 on
Serial0/1
      192.168.12.0/24 via 0.0.0.0 in 4 hops
      192.168.14.0/24 via 0.0.0.0 in 3 hops
      192.168.15.0/24 via 0.0.0.0 in 3 hops
      192.168.16.0/24 via 0.0.0.0 in 2 hops
      192.168.17.0/24 via 0.0.0.0 in 1 hops
      192.168.20.0/24 via 0.0.0.0 in 2 hops
      192.168.21.0/24 via 0.0.0.0 in 1 hops
      192.168.22.0/24 via 0.0.0.0 in 1 hops
RIP: received v2 update from 192.168.18.1 on
Serial0/2
      192.168.12.0/24 via 0.0.0.0 in 3 hops
      192.168.14.0/24 via 0.0.0.0 in 2 hops
      192.168.15.0/24 via 0.0.0.0 in 2 hops
      192.168.16.0/24 via 0.0.0.0 in 1 hops
      192.168.17.0/24 via 0.0.0.0 in 1 hops
      192.168.20.0/24 via 0.0.0.0 in 3 hops
      192.168.21.0/24 via 0.0.0.0 in 2 hops
      192.168.22.0/24 via 0.0.0.0 in 2 hops
```

```
RIP: sending  v1 update to
255.255.255.255 via Serial0/1
(192.168.19.2)
RIP: build update entries
      network 192.168.12.0 metric 4
      network 192.168.14.0 metric 3
      network 192.168.15.0 metric 3
      network 192.168.16.0 metric 2
      network 192.168.18.0 metric 1
      network 192.168.30.0 metric 1
```

```
RIP: sending  v2 update to 224.0.0.9 via
Serial0/1 (192.168.19.2)
RIP: build update entries
  192.168.12.0/24 via 0.0.0.0, metric 4, tag 0
  192.168.14.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.15.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.16.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.18.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.30.0/24 via 0.0.0.0, metric 1, tag 0
```

```
RIP: sending  v1 update to
255.255.255.255 via Serial0/1
(192.168.19.2)
RIP: build update entries
      network 192.168.12.0 metric 4
      network 192.168.14.0 metric 3
      network 192.168.15.0 metric 3
      network 192.168.16.0 metric 2
      network 192.168.18.0 metric 1
      network 192.168.30.0 metric 1
```

```
RIP: sending  v2 update to 224.0.0.9 via
Serial0/1 (192.168.19.2)
RIP: build update entries
  192.168.12.0/24 via 0.0.0.0, metric 4, tag 0
  192.168.14.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.15.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.16.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.18.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.30.0/24 via 0.0.0.0, metric 1, tag 0
```

Listing 3.7. Wynik działania komendy „debug ip rip” dla routera R16 wykorzystującego protokół RIPv1
Opracowanie własne.

```
RIP: sending  v1 update to
255.255.255.255 via Serial0/0
(192.168.30.33)
RIP: build update entries
      network 192.168.12.0 metric 4
      network 192.168.14.0 metric 3
      network 192.168.15.0 metric 3
      network 192.168.16.0 metric 2
      network 192.168.17.0 metric 2
      network 192.168.18.0 metric 1
      network 192.168.19.0 metric 1
      network 192.168.20.0 metric 3
      network 192.168.21.0 metric 2
      network 192.168.22.0 metric 2
```

```
RIP: sending  v2 update to 224.0.0.9 via
Serial0/0 (192.168.30.34)
RIP: build update entries
  192.168.12.0/24 via 0.0.0.0, metric 4, tag 0
  192.168.14.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.15.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.16.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.17.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.18.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.19.0/24 via 0.0.0.0, metric 1, tag 0
  192.168.20.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.21.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.22.0/24 via 0.0.0.0, metric 2, tag 0
  192.168.30.64/26 via 0.0.0.0, metric 1, tag
```

Listing 3.8. Wynik działania komendy „debug ip rip” dla routera R16 wykorzystującego protokół RIPv2
Opracowanie własne.

W wyniku polecenia debug ip rip na powyższym listingu widzimy, że protokół RIPv2 uwzględnia w swoich aktualizacjach routingu sieci oraz odpowiadające im maski podsieci.

3.3.3 Porównanie czasów działania sieci

Wyniki testu ICMP Ping dla komunikacji w sieci przedstawione zostały w poniższej tabeli. Badanie przeprowadzono wywołując polecenie „ping 192.168.22.1” z adresu źródłowego 192.168.12.1.

	RIP wersja 1 (ms)	RIP wersja 2 (ms)	OSPF (ms)	EIGRP (ms)
1	2	3	5	3
2	3	2	4	5
3	9	2	7	13
4	9	3	8	6
5	5	3	6	2
6	11	5	7	1
7	3	7	5	6
8	3	5	3	11
9	3	6	2	11
10	9	4	9	6
11	12	3	3	6
12	4	3	5	4
13	3	2	11	5
14	2	3	2	9
15	4	11	6	6
16	3	4	5	3
17	8	6	4	14
18	5	2	3	6
19	7	5	7	8
20	9	7	13	5
Średnia	**5,7**	**4,3**	**5,75**	**6,5**

Tabela 3.1. Porównanie czasów działania sieci dla protokołów routingu dynamicznego
Opracowanie własne.

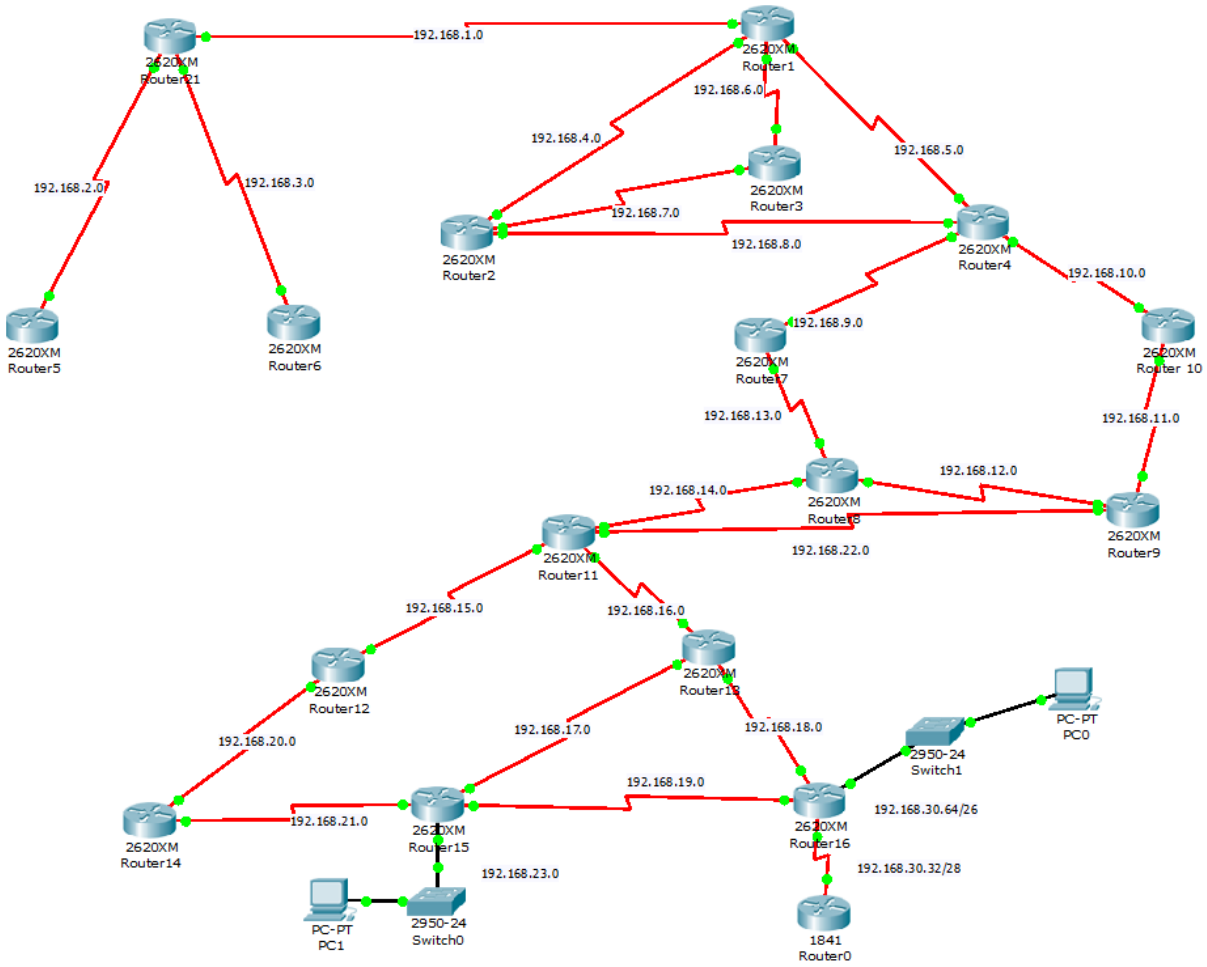
3.3.4 Podsumowanie

RIPv2 jest prostym i łatwym w użyciu protokołem, więc nie trzeba poświęcać mu zbyt dużo uwagi. Spotkał się on z się z ogromną akceptacją w obrębie małych sieci. Jednak ponieważ został opracowany jako zmodernizowana odmiana RIP v1 wciąż nie jest wstanie przezwyciężyć wszystkich ograniczeń swojego poprzednika. Standard RIP nakłada ograniczenia na środowiska, w których może być używany. Maksymalną liczbą przeskoków używaną przez routery RIP jest 15. Sieci znajdujące się w odległości 16 przeskoków lub większej są uważane za nieosiągalne. Tak więc, nie może on być używany w sieciach, które mają średnicę większą niż 15. Mimo to wiele niedoskonałości jego poprzednika zostało naprawione. W RIPv2 możliwe jest zastosowanie algorytmów uwierzytelniania, co nie jest przewidziane w wersji pierwszej protokołu. Ponadto RIPv2 wysyła w aktualizacjach routingu maskę podsieci. Dzięki temu może obsługiwać zarówno VLSM, jak i CIDR. Zmieniono także sposób komunikacji z urządzeniami sąsiednimi. Nadal wykorzystywany jest port 520, protokołu UDP, ale aktualizacje są wysyłane na adres grupowy 224.0.0.9. Natomiast RIPv1 wysyła aktualizacje na adres rozgłoszeniowy 255.255.255.255. Komunikaty grupowe zajmują mniej pasma sieciowego, dodatkowo wysyłanie aktualizacji jako komunikatów grupowych wymaga mniej obliczeń od urządzeń na których nie działa protokół RIP. Konfiguracja tego protokołu w odpowiednio małej intersieci pozwoli na wykorzystanie tańszego sprzętu (ze względu na mniejsze wymagania sprzętowe), przy jednoczesnym zachowaniu dobrej jakości pracy i szybkiej komunikacji.

3.4 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego OSPF.

OSPF jest bezklasowym protokołem routingu dynamicznego łącze-stan. Routery, na których zaimplementowany jest ten protokół utrzymują bazę danych, w której przechowują informacje na temat aktualnej topologii. Jest to bardzo popularny protokół, ponieważ rozwiązanie to stało się standardem otwartym i stosowne jest od dłuższego czasu. Większość producentów uwzględnia obsługę tego protokołu dlatego bardzo dobrze nadaje się do zastosowania w sieciach złożonych z urządzeń różnych firm.

3.4.1 Schemat zaprojektowanej sieci



Rysunek 13. Przykład topologii sieci dla routingu dynamicznego OSPF.

Opracowanie własne.

3.4.2 Badanie zawartości aktualizacji routingu

Pełna konfiguracja routerów zamieszczona jest w załączniku 4 w katalogu „Packet_Tracer\OSPF" – nazwa pliku „OSPF.pkt" – opracowanie własne W celach kontrolnych sprawdzono komendą „show ip protocols" wydaną na routerze Router16, czy protokół OSPF jest rzeczywiście uruchomiony. Wynik działania komendy przedstawiony jest na listingu 9.

```
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 192.168.30.65
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4       Routing for Networks:
    192.168.19.0 0.0.0.255 area 0
    192.168.18.0 0.0.0.255 area 0
    192.168.30.64 0.0.0.63 area 0
    192.168.30.32 0.0.0.15 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1           110      00:09:04
    192.168.3.1           110      00:09:04
    192.168.3.2           110      00:09:04
    192.168.6.1           110      00:09:02
    192.168.7.2           110      00:09:03
    192.168.8.1           110      00:09:02
    192.168.10.1          110      00:08:58
    192.168.11.2          110      00:08:53
    192.168.13.1          110      00:08:53
    192.168.14.1          110      00:09:03
    192.168.18.1          110      00:09:03
    192.168.20.1          110      00:09:03
    192.168.21.1          110      00:09:04
    192.168.22.1          110      00:09:02
    192.168.22.2          110      00:08:58
    192.168.23.1          110      00:08:48
    192.168.30.34         110      00:09:05
    192.168.30.65         110      00:09:05
  Distance: (default is 110)
```

Listing 3.9. Wynik działania komendy „show ip protocols" na routerze R16. Opracowanie własne.

Z listingu 3.9 wynika, że na routerze uruchomiony jest protokół OSPF z identyfikatorem procesu 1. Identyfikator o tej wartości ustanowiony jest na każdym routerze z uruchomionym protokołem OSPF, jednakże należy pamiętać, że nie musi się on zgadzać z innymi routerami, aby zostały ustanowione przyległości.

Komendą „show ip route" wyświetlono tablicę routingu routera Router16. Wynik działania komendy znajduje się na listingu 3.10.

```
Router#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 not set

O    192.168.1.0/24 [110/448] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.2.0/24 [110/512] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.3.0/24 [110/512] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.4.0/24 [110/448] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.5.0/24 [110/384] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.6.0/24 [110/448] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.7.0/24 [110/448] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.8.0/24 [110/384] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.9.0/24 [110/320] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.10.0/24 [110/320] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.11.0/24 [110/256] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.12.0/24 [110/256] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.13.0/24 [110/256] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.14.0/24 [110/192] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.15.0/24 [110/192] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.16.0/24 [110/128] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.17.0/24 [110/128] via 192.168.19.1, 00:11:51, Serial0/1
                     [110/128] via 192.168.18.1, 00:11:51, Serial0/2
```

```
C    192.168.18.0/24 is directly connected, Serial0/2
C    192.168.19.0/24 is directly connected, Serial0/1
O    192.168.20.0/24 [110/192] via 192.168.19.1, 00:11:51, Serial0/1
O    192.168.21.0/24 [110/128] via 192.168.19.1, 00:11:51, Serial0/1
O    192.168.22.0/24 [110/192] via 192.168.18.1, 00:11:51, Serial0/2
O    192.168.23.0/24 [110/65] via 192.168.19.1, 00:11:51, Serial0/1
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.32/28 is directly connected, Serial0/0
C       192.168.30.64/26 is directly connected, FastEthernet0/0
```

Listing 3.10. Tablica routingu routera Router16.

Opracowanie własne.

Na listingu 3.10 poszczególne wpisy tablicy routingu poprzedzone są literą O. Litera ta informuje, że źródłem informacji o danej trasie jest protokół OSPF, natomiast wpisy z litera C informują o sieciach połączonych bezpośrednio.

Poleceniem „**tracert**” sprawdzono drogę pakietu pomiędzy komputerem PC0, a komputerem PC1. Wynik przedstawiono na poniższym listingu 3.11.

```
PC>tracert 192.168.23.5

Tracing route to 192.168.23.5 over a maximum of 30 hops:

  1   4 ms      9 ms      5 ms      192.168.30.65
  2   7 ms      8 ms      8 ms      192.168.19.1
  3   13 ms     21 ms     14 ms     192.168.23.5

Trace complete.
```

Listing 3.11. Wynik polecenia tracert 192.168.23.5 na komputerze PC0.

Opracowanie własne

Z listingu 3.11 wynika, że trasa do komputera PC1 przebiega kolejno przez routery: Router16 i Router15. Ze schematu sieci (Rys. 3.4) można wywnioskować, że do tego samego komputera możliwe są inne trasy np. poprzez routery Router 16, Router 13, Router 15 lub poprzez routery: Router 16, Router 13, Router 11, Router 12, Router 14, Router 15. Wybór

trasy jest jednak zależny od łącznego kosztu dotarcia pakietu do celu, który jest sumą poszczególnych kosztów na drodze do niego. Aby sprawdzić jaki jest koszt danego interfejsu routera należy wydać polecenie „show ip ospf interface”. W poniższej tabeli przedstawiono zestawienie łącznych kosztów dotarcia pakietu z komputera PC0 do komputera PC1 dla poszczególnych tras:

Trasa	Łączny koszt
R16 i R15	1+64+1
R16, R13, R15	1+64+64+1
R16,R13, R11, R12, R14, R15	1+64+64+64+64+64+1

Tabela 3.1. Łączny koszt OSPF od komputera PC0 do komputera PC1 w zależności od trasy. Opracowanie własne

Z tabeli 3.4 wynika, że trasa Router 16, Router 15 posiada najniższy łączny koszt, dlatego właśnie ta trasa prowadzi do komputera PC1. Koszt łącza może zostać określony przez administratora, za pomocą polecenia „ip ospf cost”. Aby zbadać zachowanie sieci w specyficznych warunkach zmieniono koszt interfejsu 192.168.17.0, ustawiając go na wartość 1562. Dodatkowo zasymulowano awarie sieci 192.168.19.0/24, poprzez wyłączenie interfejsu 192.168.19.2 routera Router16. Trasa pakietów od komputera PC0 do komputera PC1 po awarii sieci 192.168.19.0/24 oraz modyfikacji kosztu interfejsu 192.168.17.0 przedstawiona została na listingu 12.

```
PC>tracert 192.168.23.5

Tracing route to 192.168.23.5 over a maximum of 30 hops:

  1   42 ms     5 ms      8 ms      192.168.30.65
  2   8 ms      8 ms      8 ms      192.168.18.1
  3   12 ms     12 ms     14 ms     192.168.16.1
  4   9 ms      10 ms     15 ms     192.168.15.2
  5   18 ms     26 ms     18 ms     192.168.20.2
  6   18 ms     24 ms     21 ms     192.168.21.2
  7   *         24 ms     29 ms     192.168.23.5
Trace complete.
```

Listing 3.12. Wynik polecenia tracert 192.168.23.5 na komputerze PC0. Opracowanie własne.

Łatwo zauważyć, iż zmiana ta spowodowała, że trasą z najniższym kosztem stała się trasa Router16, Router13, Router11, Router12, Router14, R Router15 (której łączny koszt wynosi 322), czego dowodem jest listing 12.

3.4.3 Porównanie czasów działania sieci

Wyniki testu ICMP Ping dla komunikacji w sieci przedstawione zostały w poniższej tabeli. Badanie przeprowadzono wywołując polecenie „ping 192.168.22.0" z adresu źródłowego 192.168.3.1.

	RIP wersja 1 (ms)	RIP wersja 2 (ms)	OSPF (ms)	EIGRP (ms)
1	84	76	20	50
2	78	90	12	25
3	67	85	27	22
4	104	70	21	30
5	78	56	26	26
6	79	58	25	18
7	73	78	22	31
8	62	79	39	46
9	70	81	33	28
10	77	78	32	22
11	82	105	25	18
12	111	57	28	19
13	115	81	30	33
14	85	63	24	27
15	74	72	22	33
16	70	73	26	28
17	58	90	34	21
18	91	50	24	33
19	77	91	17	18
20	104	48	26	16
Średnia	**82,95**	**74,05**	**25,65**	**27,20**

Tabela 3.2. Porównanie czasów działania sieci dla protokołów routingu dynamicznego z wyszczególnieniem protokołu OSPF.
Opracowanie własne.

3.4.4 Podsumowanie

Wraz ze wzrostem rozmiarów i stopnia skomplikowania sieci coraz wyraźniejsze stawały się ograniczenia protokołów działających na podstawie wektora odległości takich jak na przykład RIP. Routery wykorzystujące protokoły działające na podstawie wektora odległości poznają topologię sieci na podstawie aktualizacji tablic routingu otrzymanych od sąsiednich routerów. Okresowe aktualizacje informacji o routingu, wymagają szerokiego pasma, a zbieżność sieci jest osiągana powoli, czego rezultatem są nieoptymalne decyzje dotyczące routingu. Routery OSPF natomiast wysyłają ogłoszenia stanu łącza do wszystkich routerów w obrębie tego samego obszaru hierarchicznego poprzez transmisję IP w trybie rozgłoszeniowym, dzięki czemu każdy router ma pełen obraz topologii sieci. Stosowanie wyzwalanych aktualizacji umożliwia oszczędniejsze wykorzystanie pasma i zapewnia szybszą zbieżność. Ponadto, OSPF opiera się na koszcie trasy, dodatkowo umożliwiając użytkownikowi modyfikacje kosztu danego interfejsu, pozwalając na pierwszeństwo wybranych ścieżek. Daje to możliwość dostrojenia sieci do specyficznych potrzeb.

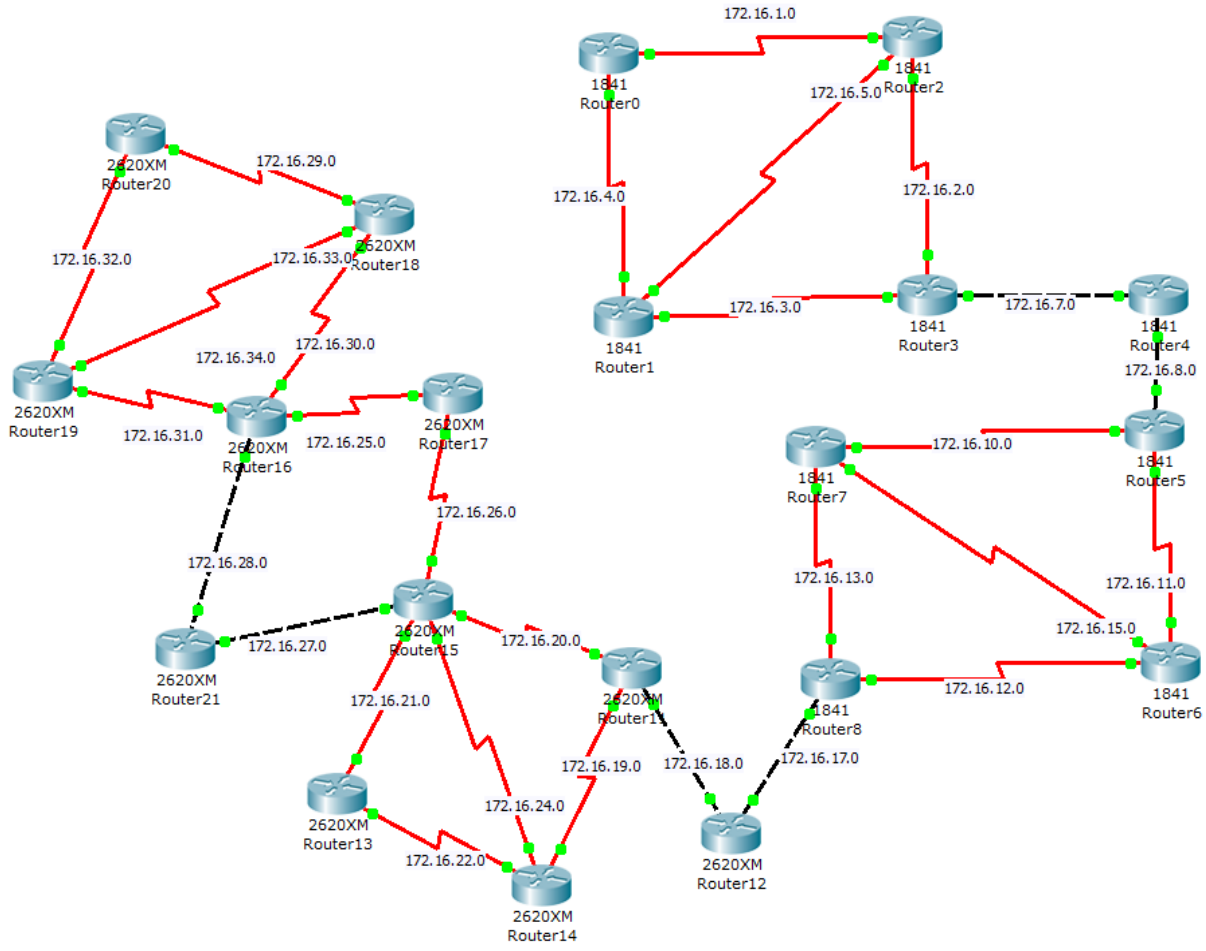
Podsumowując, OSPF jest jednym z najsilniejszych dostępnych protokołów routingu. Co implikuje fakt, iż budowanie i obsługiwanie sieci złożonej OSPF wymaga większego doświadczenia i wysiłku administratora niż w przypadku sieci wykorzystujących inne protokoły routingu. Właściwie zaprojektowana i wykonana sieć OSPF nagradza jednak swoich użytkowników niezawodnym i szybkim działaniem oraz czasem osiągania zbieżności.

3.5 Infrastruktura sieciowa wykorzystująca konfiguracje routingu dynamicznego EIGRP.

Internet jest bardzo dynamicznie rozwijającą się siecią, co wiąże się z tym, ze jego protokół IP musi charakteryzować się wysoka dynamiką. Firma Cisco Systems chcąc zaoferować nowoczesny i wysoce odporny protokół, zdecydowała się wprowadzić protokół EIGRP. Protokół ten charakteryzuje wydajne działanie, szybkie osiąganie zbieżności jak również wysokie bezpieczeństwo.

3.5.1 Schemat zaprojektowanej sieci

Dla topologii przedstawionej na poniższym rysunku skonfigurowano protokół routingu dynamicznego EIGRP. Plik z konfiguracją został dołączony na płycie CD w katalogu „Packet_Tracer\EIGRP" – nazwa pliku „EIGRP.pkt" – opracowanie własne. Wykorzystano 20 routerów (dziewięć typu 1841 oraz jedenaście typu 2620XM): Routery zostały oznaczone odpowiednio Router 0 - Router 8 oraz Router 11 - Router 21.



Rysunek 14. Przykład topologii sieci dla routingu dynamicznego EIGRP.

Opracowanie własne.

3.5.2 Badanie zawartości aktualizacji routingu

Pełna konfiguracja routerów EIGRP zamieszczona jest w załączniku 5 w katalogu „Packet_Tracer\EIGRP" – nazwa pliku „EIGRP.pkt" Komendą „show ip route" wyświetlono tablicę routingu routera Router 11. Wynik działania komendy znajduje się na listingu 3.13.

```
Router#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 not set

     172.16.0.0/24 is subnetted, 28 subnets
D       172.16.1.0 [90/3716096] via 172.16.18.2, 02:01:39, FastEthernet1/0
D       172.16.2.0 [90/3204096] via 172.16.18.2, 02:01:39, FastEthernet1/0
D       172.16.3.0 [90/3204096] via 172.16.18.2, 02:01:41, FastEthernet1/0
D       172.16.4.0 [90/4228096] via 172.16.18.2, 02:01:40, FastEthernet1/0
D       172.16.5.0 [90/3716096] via 172.16.18.2, 02:01:39, FastEthernet1/0
D       172.16.6.0 [90/3874816] via 172.16.18.2, 02:01:40, FastEthernet1/0
D       172.16.7.0 [90/2692096] via 172.16.18.2, 02:01:43, FastEthernet1/0
D       172.16.8.0 [90/2689536] via 172.16.18.2, 02:01:43, FastEthernet1/0
D       172.16.10.0 [90/2686976] via 172.16.18.2, 02:01:43, FastEthernet1/0
D       172.16.11.0 [90/3198976] via 172.16.18.2, 02:01:42, FastEthernet1/0
D       172.16.13.0 [90/2174976] via 172.16.18.2, 02:01:44, FastEthernet1/0
D       172.16.15.0 [90/2686976] via 172.16.18.2, 02:01:41, FastEthernet1/0
D       172.16.17.0 [90/30720] via 172.16.18.2, 02:02:33, FastEthernet1/0
C       172.16.18.0 is directly connected, FastEthernet1/0
C       172.16.19.0 is directly connected, Serial0/3
C       172.16.20.0 is directly connected, Serial0/0
D       172.16.21.0 [90/2681856] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.22.0 [90/2681856] via 172.16.19.1, 02:02:24, Serial0/3
D       172.16.24.0 [90/2681856] via 172.16.19.1, 02:02:24, Serial0/3
                    [90/2681856] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.25.0 [90/2686976] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.26.0 [90/2681856] via 172.16.20.1, 02:02:24, Serial0/0
```

```
D       172.16.27.0 [90/2172416] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.28.0 [90/2174976] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.29.0 [90/3198976] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.30.0 [90/2686976] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.31.0 [90/2686976] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.32.0 [90/3198976] via 172.16.20.1, 02:02:24, Serial0/0
D       172.16.33.0 [90/3198976] via 172.16.20.1, 02:02:24, Serial0/0
```

Listing 3.13. Tablica routingu routera Router 11.

Opracowanie własne.

Na listingu 3.13 poszczególne wpisy tablicy routingu poprzedzone są literą D. Litera ta informuje, że źródłem informacji o danej trasie jest protokół EIGRP, natomiast wpisy z litera C informują o sieciach połączonych bezpośrednio.

Obliczenie metryki EIGRP routera Router 11 do sieci 172.16.17.0

Z listingu 3.13 wynika, że trasa do sieci 172.16.17.0 ma wartość 30720. Sprawdzono czy wartość ta zgadza się z przeprowadzonymi poniżej obliczeniami.

Zgodnie ze wzorem (2.2)

$$Metryka\ EIGRP = [szerokość\ pas\ ma\ + opóźnienie]$$

W protokole EIGRP całkowita metryka jest obliczana przez skalowanie metryk szerokości pasma i opóźnienia. Do obliczenia pasma używany jest następujący wzór:

szerokość pasma = (10 000 000 / szerokość pasma(i)) * 256 (3.1)

gdzie szerokość pasma(i) to wyrażona w kilobitach, najmniejsza szerokość pasma wszystkich interfejsów wyjściowych znajdujących się na trasie prowadzącej do sieci docelowej. Łączem do sieci 172.16.17.0 jest łącze Fast Ethernet w związku z czym przepustowość pasma wynosi 100[Mb/s] czyli 100 000 [kb/s]

Wobec (3.1) uzyskujemy

Szerokość pasma = (10000000/ szerokość pasma(i)) * 256=(10000000/100000)*256 = 25600

Do obliczenia opóźnienia używany jest następujący wzór:

opóźnienie = opóźnienie(i) * 256 (3.2)

gdzie opóźnienie(i) to suma opóźnień określonych dla interfejsów znajdujących się na trasie prowadzącej do sieci docelowej. Wartość ta wyrażona jest w dziesiątkach milisekund. Wartość opóźnienia, którą możemy uzyskać wykonując polecenia show **ip eigrp topology** lub **show interface** jest wyrażona w mikrosekundach, zatem przed zastosowaniem tej wartości w równaniu należy podzielić ją przez 10. Suma opóźnień do sieci 172.16.17.0 dla łącza Fast wynosi dla jednego interfejsu 100 mikrosekund, a trasa do sieci docelowej prowadzi przez dwa interfejsy: Fast Ethernet routera Router 11 i interfejs Fast Ethernet routera Router12, co łącznie daje sumaryczną wartość 200 [mikrosekund].

Stosując (3.2) oraz (2.2) dostajemy odpowiednio

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

Metryka EIGRP = 25600+5120 = 30720

Obliczona metryka EIGRP dla routera Router 11 do sieci 172.16.17.0 wynosi 30720 i jest zgodna z wartością metryki do tej sieci widoczną na listingu 3.13.

3.5.3 Porównanie czasów działania sieci

Aby sprawdzić prawidłowość i szybkość działania routingu w badanym obszarze routerów z uruchomionym protokołem EIGRP, wydano polecenie „ping 172.16.32.2” z routera Router 0 z adresem IP 172.16.1.1. Wyniki testu ICMP Ping dla komunikacji w sieci przedstawione zostały w poniższej tabeli 7.

	RIP wersja 1 (ms)	RIP wersja 2 (ms)	OSPF (ms)	EIGRP (ms)
1	62	123	59	49
2	76	64	55	38
3	66	52	65	41
4	51	51	62	56
5	66	56	63	65
6	56	58	49	47
7	62	52	60	40
8	73	54	70	45
9	66	48	78	51
10	50	53	66	63
11	70	50	50	48
12	61	61	47	56
13	81	60	72	51
14	62	57	78	49
15	67	48	49	51
16	51	57	51	40
17	78	62	59	40
18	79	65	62	47
19	70	87	44	56
20	68	71	49	48
Średnia	**66,75**	**61,45**	**59,4**	**57,7**

Tabela 3.1. Porównanie czasów działania sieci dla protokołów routingu dynamicznego z wyszczególnieniem protokołu EIGRP.
Opracowanie własne.

3.5.4 Podsumowanie

Protokół EIGP jest hybrydowym protokołem routingu, stanowiącym połączenie protokołów stanu łącz i protokołów wektora odległości, łącząc tym samym w sobie najlepsze cechy tych protokołów. Jest on łatwy do skonfigurowania i użycia. Charakteryzuje go szybka zbieżność sieci - protokół automatycznie reaguje na zmiany topologii. Znajduje zastosowanie w dużych sieciach, ze względu na wysoką zdolność skalowalności. Protokół EIGP domyślnie równoważy obciążenie, co powyższa wydajność jego działania. Dodatkowo, poprzez umożliwienie stosowania uwierzytelniania pomiędzy routerami, zwiększa bezpieczeństwo sieci. Zastosowanie protokołu warstwy transportu RTP, zapewnia mu także niezawodność dostarczania swoich własnych pakietów EIGRP i umożliwia łatwe dodanie w przyszłości obsługi innych routowalnych protokołów, takich jak IPv6.

Wymienione wyżej cechy powodują, iż jest on jednym z najbogatszych i najodporniejszych protokołów routingu. Pozostaje on jednak zastrzeżonym produktem firmy Cisco, co stanowi pewne ograniczenie dla potencjalnych jego użytkowników.

Zakończenie

Celem pracy było ukazanie wyników badań, dotyczących analizy wybranych protokołów routingu dynamicznego. Zrealizowanie tego celu było możliwe dzięki opracowaniu sieci na potrzeby każdego z omawianych protokołów routingu oraz odpowiedniej konfiguracji ich na routerach wchodzących w skład sieci. Zgodnie z założeniem pracy, protokoły zostały zbadane pod względem czasu osiągania zbieżności, skalowalności sieci oraz zużycia zasobów. Dodatkowo została również zwrócona uwaga na złożoność konfiguracji poszczególnych protokołów oraz ich bezpieczeństwo.

Analizując poszczególne protokoły trasowania można było łatwo zauważyć, iż stają się one doskonalsze, pracują w coraz to szybszych sieciach i spełniają już niemal wszelkie wymagania użytkowników. Mimo to stare protokoły nadal znajdują zastosowanie. Czynnikami mającymi na to wpływ, jest fakt, że każdy z protokołów ma swoje zalety i wady, każdy sprawdza się w określonych warunkach.

I tak, routing statyczny znajduje zastosowanie w niewielkich sieciach, które nie są rozbudowywane, ponieważ konfiguracja takiej sieci jest bardzo praco i czasochłonna, a utrzymanie staje się uciążliwe. Przy choć by najmniejszej zmianie topologii sieci, wymagana jest ponowna konfiguracja urządzeń. Tak więc nadaje się on do prostych topologii, gdyż nie skaluje się dobrze w powiększających się sieciach. Routing statyczny jest dobrym rozwiązaniem gdy, używa się jednej trasy domyślnej reprezentującej drogę do każdej sieci, dla której nie ma w tablicy routingu lepszej trasy. Ponadto niewątpliwą jego zaleta stanowi bezpieczeństwo. Jest dużo bardziej odporny na ataki związane ze zmiana tablic routingu. Znajduje więc on zastosowanie w sieciach, w których wymagane jest duże bezpieczeństwo kosztem dostępności po wystąpieniu awarii łącza prowadzącego do sieci docelowej. Niewątpliwą zaleta jest, minimalne zużycie procesora, gdyż żadne dodatkowe zasoby nie są wymagane.

Protokół routingu wektora odległości jakim jest RIP znalazł zastosowanie w małych sieciach o jednolitej topologii. Jest on łatwy w implementacji i utrzymaniu, dodatkowo nie wymaga dużej wiedzy od administratora. Zalety te, jednak okupione są wolna zbieżnością, która jest związana z używaniem okresowych aktualizacji. Dodatkowo, wolna zbieżność może ograniczać rozmiar sieci, gdyż większe sieci wymagają więcej czasu na propagację informacji o trasach. Podobnie jak w przypadku routingu statycznego, protokół RIP ma niewielkie zapotrzebowanie na zasoby. Protokoły routingu wektora odległości nie wymagają dużych ilości pamięci do składowania informacji, ani silnego procesora. Z reguły nie wymagają też dużych szerokości pasma do wysyłania aktualizacji routingu. Może to jednak

stanowić problem, gdy protokół ten zostanie wdrożony w dużej sieci. Zagraża to pojawieniem się pętli routingu, powstających kiedy niespójne tablice routingu nie są aktualizowane z powodu wolnej zbieżności w zmieniającej się sieci.

Wady protokołów RIP zostały wyeliminowane przez opracowanie protokołu stanu łącza OSPF, który nie rozsyła cyklicznych ogłoszeń, przez co nie jest generowany dodatkowy ruch w sieci. Szybko reaguje on na zmiany w topologii sieci. Dodatkowo, aby móc obsługiwać znacznie większe sieci, niż protokoły wektora odległości, OSPF wprowadził podział systemu autonomicznego na obszary. Pewnym problemem w sieciach, w których zastosowano OSPF może być sieć cyklicznie zmieniająca 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 też na administratorach sieci, w których zastosowano protokół OSPF spoczywa duża odpowiedzialność za prawidłowo działającą warstwę sprzętową sieci. Wymaga on również znacznie większego zapotrzebowania na zasoby sprzętowe, dotyczące procesora i pamięci operacyjnej.

Żadne narzędzie nie rozwiązuje jednak wszystkich problemów i pojawił się kolejny protokół trasowania jakim był EIGRP. Wprowadzał on nowe rozwiązania i algorytmy obliczeń. Łączy on w sobie najlepsze cechy protokołu routingu łącze-stan, pozostając protokołem routingu wektora odległości. Należy również pamiętać, że EIGRP jest zastrzeżonym produktem firmy Cisco i działa tylko na routerach Cisco, co stanowi jego ograniczenie. Wymagania sprzętowe w stosunku do routerów, na których działa protokół EIGRP są większe niż w przypadku pozostałych protokołów routingu wektora odległości, ale mniejsze niż dla protokołów stanu łącza. Charakteryzuje go wysoka skalowalność i może być stosowany do wielkości tysięcy węzłów routingu. Zastosowanie protokołu EIGRP zapewnia szybką zbieżność i stabilność procesu routingu. Wymaga jednak od administratora dużej wiedzy na temat sposobu zaimplementowania, sposobów diagnozowania i rozwiązywania problemów z nim związanych.

Każdy z protokołów ma swoje zalety i wady, każdy sprawdza się w określonych warunkach. Zalety jednej metody są wadami drugiej. Nie ma możliwości zaprojektowania optymalnego algorytmu wyznaczania trasy, dla każdego rodzaju fizycznej topologii. Nie ma też najlepszego protokołu, każdy ma swoje dobre i złe strony, w zależności od konkretnej sytuacji. Podjęcie właściwej decyzji dotyczącej zastosowania odpowiedniego protokołu routingu w sieci, pozwoli zapewnić szybkość i stabilność działania, przez co dostęp do informacji i zasobów będzie bezpieczny oraz niezawodny. Istnieje również możliwość

zastosowania redystrybucji, czyli współużytkowania protokołów routingu. Rozwiązanie to umożliwia routerom obsługę więcej niż jednego protokołu routingu oraz dzielenie tras pomiędzy protokoły. Temat ten jednak wykraczał poza ramy niniejszej pracy. Z powodzeniem jednak może być rozwijany, czy to w ramach pracy magisterskiej, czy też jako niezależny projekt.

Podsumowując, można stwierdzić, że badania i rozważania podjęte w niniejszej pracy nie wyczerpują całokształtu problematyki związanej z protokołami routingu dynamicznego. Temat ten jest nadal tematem otwartym i ciągle zmieniającym się. Ma na to wpływ dynamika rozwoju sieci i oprogramowania Wciąż są opracowywane techniki które mają na celu jak najlepiej wykorzystywać dostępne łącze. Nowo powstające protokoły routingu, będą coraz to doskonalsze, przystosowane do pracy w coraz to szybszych sieciach, dzięki czemu będą mogły spełniać wszelkie wymagania użytkowników.

Spis rysunków

Rysunek 2.1. Topologia magistrali [13] 7
Rysunek 2.2 Topologia gwiazdy [13] 8
Rysunek 2.3. Topologia rozszerzonej gwiazdy [13] 9
Rysunek 2.4. Topologia hierarchiczna [13] 10
Rysunek 2.5. Topologia pierścienia [13] 11
Rysunek 2.6. Topologia podwójnego pierścienia. 12
Rysunek 2.7. Topologia siatki [13] 13
Rysunek 2.8 Opis nagłówka protokołu RIPv1 [14] 18
Rysunek 2.9. Format nagłówka EIGRP [3] 20
Rysunek 3.1. Przykład topologii sieci dla routingu statycznego. 28
Rysunek 3.2 Przykład topologii sieci dla routingu dynamicznego RIPv1. 33
Rysunek 3.3. Przykład topologii sieci dla routingu dynamicznego RIPv2. 38
Rysunek 3.4. Przykład topologii sieci dla routingu dynamicznego OSPF. 44
Rysunek 3.5. Przykład topologii sieci dla routingu dynamicznego EIGRP. 51

Spis tabel

Tabela 2.1. Wartości kosztów OSPF w systemie Cisco w zależności od typu interfejsu. 26
Tabela 3.1. Porównanie czasów działania sieci dla routingu statycznego i dynamicznego. 30
Tabela 3.2. Porównanie czasów działania sieci dla routingu statycznego i dynamicznego. 36
Tabela 3.3. Porównanie czasów działania sieci dla protokołów routingu dynamicznego.....42
Tabela 3.4. Łączny koszt OSPF od komputera PC0 do komputera PC1 w zależności od trasy. 48
Tabela 3.5. Porównanie czasów działania sieci dla protokołów routingu dynamicznego z wyszczególnieniem protokołu OSPF. 49
Tabela 3.6. Porównanie czasów działania sieci dla protokołów routingu dynamicznego z wyszczególnieniem protokołu EIGRP. 55

Spis wzorów

Wzór 2.1. Pełny złożony wzór metryki EIGRP 23
Wzór 2.2. Domyślny złożony wzór metryki EIGRP. 23
Wzór 2.3. Koszt OSPF 26
Wzór 3.1. Szerokość pasma 54
Wzór 3.2. Opóźnienie interfejsu 55

Spis listingów

Listing 3.1. Tablica routingu routera R1. 28
Listing 3.2. Tablica routingu routera R2. 29
Listing 3.3. Tablica routingu routera R3. 29
Listing 3.4. Tablica routingu routera R7. 34
Listing 3.5. Tablica routingu routera R0. 35
Listing 3.6. Tablica routingu routera R10. 35
Listing 3.7. Wynik działania komendy „debug ip rip" dla routera R16 wykorzystującego protokół RIPv1 41
Listing 3.8. Wynik działania komendy „debug ip rip" dla routera R16 41
Listing 3.9. Wynik działania komendy „show ip protocols" na routerze R16. 45
Listing 3.10. Tablica routingu routera Router16. 47
Listing 3.11. Wynik polecenia tracert 192.168.23.5 na komputerze PC0. 47
Listing 3.12. Wynik polecenia tracert 192.168.23.5 na komputerze PC0. 48
Listing 3.13. Tablica routingu routera Router 11. 53

Spis załączników:

Wszystkie załączniki znajdują się w katalogu „Packet_Tracer” na płycie CD dołączonej do tej pracy.

1. Załącznik nr 1 – Pliki w katalogu „Routing statyczny” z konfiguracją routerów dla poszczególnych protokołów routingu dynamicznego i statycznego dla sieci z rysunku numer 3.1
2. Załącznik nr 2 – Pliki w katalogu „RIPv1” z konfiguracją routerów dla poszczególnych protokołów routingu dynamicznego dla sieci z rysunku numer 3.2
3. Załącznik nr 3 – Pliki w katalogu „RIPv2” z konfiguracją routerów dla poszczególnych protokołów routingu dynamicznego dla sieci z rysunku numer 3.3
4. Załącznik nr 4 – Pliki w katalogu „OSPF” z konfiguracją routerów dla poszczególnych protokołów routingu dynamicznego dla sieci z rysunku numer 3.4
5. Załącznik nr 5 – Pliki w katalogu „EIGRP” z konfiguracją routerów dla poszczególnych protokołów routingu dynamicznego dla sieci z rysunku numer 3.5

Bibliografia

Pozycje książkowe:

1. Donahue Gary A. „Wojownik sieci” Wydawnictwo Helion Gliwice 2012 [1]
2. Dye Mark A., McDonald Rick, Rufi Antoon „Tony” W. „Akademia sieci Cisco. CCNA Exploration. Semestr 1 – Podstawy sieci” Wydawnictwo Naukowe PWN Warszawa 2008 [2]
3. Graziani Rick, Johnson Allan „Akademia sieci Cisco. CCNA Exploration. Semestr 2 - Protokoły i koncepcje routingu” Wydawnictwo Naukowe PWN Warszawa 2008 [3]
4. Krysiak Karol „Sieci komputerowe” Wydawnictwo Helion Gliwice 2005 [4]
5. Lewis Chris „ Routing Cisco.TCP/IP dla profesjonalisty” Wydawnictwo PLJ Warszawa 1999 [5]
6. Scrimger Rob, LaSalle Paul, Leitzke Clay, Mridula Parihar, Meeta Gupta „TCP/IP. Biblia” Helion Gliwice 2002 [6]
7. Sportack Mark A. „Routing IP podstawowy podręcznik” Wydawnictwo Mikom Warszawa 2000 [7]
8. Stevens David L., Comer Douglas E. ” Sieci komputerowe TCP/IP. Tom 2. Projektowanie i realizacja protokołów” Wydawnictwo Naukowo-Techniczne Warszawa 1997 [8]

Strony internetowe:

9. http://www.faqs.org/rfcs/rfc1058.html [9]
10. http://technet.microsoft.com/pl-pl/library/cc778874(v=ws.10).aspx [10]
11. http://www.faqs.org/rfcs/rfc2453.html [11]
12. http://www.rogaski.org/cisco/sem2/6.html [12]
13. http://wazniak.mimuw.edu.pl/index.php?title=SK_Modu%C5%82_1 [13]
14. http://pl.wikipedia.org/wiki/Routing_Information_Protocol [14]

Oświadczenie

Ja, niżej podpisana Karolina Jopek studentka Wydziału Fizyki, Matematyki i Informatyki
oświadczam, że przedkładaną pracę dyplomową inżynierską pt.:

Problematyka doboru optymalnego protokołu routingu dla wybranych topologii sieci komputerowych.

wykonałam samodzielnie, tzn. nie zlecałam opracowania pracy dyplomowej, ani jej części osobom trzecim, jak również nie odpisywałam pracy dyplomowej, ani jej części od innych osób.

Jednocześnie przyjmuję do wiadomości, że w przypadku stwierdzenia popełnienia przeze mnie czynu polegającego na przypisaniu sobie autorstwa istotnego fragmentu lub innych elementów cudzej pracy lub ustalenia naukowego, właściwy organ stwierdzi nieważność postępowania w sprawie nadania mi tytułu zawodowego (art. 193 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym, Dz. U. Nr 164 poz. 1365 z późniejszymi zmianami).

.....

Data Podpis