SPOŁECZNA WYŻSZA SZKOŁA
PRZEDSIĘBIORCZOŚCI I ZARZĄDZANIA W ŁODZI

KIERUNEK STUDIÓW: **SIECI I SYSTEMY KOMPUTEROWE**

Dariusz Sobieszek
Numer albumu: 27340

PROTOKOŁY ROUTINGU

- ROUTING STATYCZNY, RIP, OSPF, EIGRP -
PRZY WYKORZYSTANIU URZĄDZEŃ FIRMY CISCO

Praca inżynierska
napisana
w Instytucie Technologii
Informatycznych
pod kierunkiem
dr inż. Piotra Goetzena

Łódź 2010

Spis treści

Wstęp – założenia i cel pracy

Sieć komputerowa w firmie

Sprawna wymiana informacji to podstawa działania każdego przedsiębiorstwa. Rozwój firmy w dzisiejszych czasach jest wręcz niemożliwy bez wykorzystania wszelkich możliwości jakie dają sieci komputerowe i związane z nimi technologie.

Sieć komputerowa to system służący wymianie danych między dwoma lub więcej komputerami oraz urządzeniami peryferyjnymi. Jest to platforma wszystkich systemów teleinformatycznych w firmie i od jej właściwego wykonania zależy sprawne działanie firmy. Tworząc strukturę sieci musimy zwrócić szczególną uwagę na jej niezawodność i bezpieczeństwo. Nie można pozwolić sobie na dobranie urządzeń, które sprawiałyby problemy z kompatybilnością. Każda przerwa w pracy spowodowana awarią sieci to strata dla firmy więc powinniśmy wybrać sprzęt sprawdzonych producentów oraz stosować rozwiązania techniczne i technologiczne, które zapewniają niezawodność w działaniu.

W tej pracy wykorzystano sprzęt znanego i renomowanego na całym świecie producenta urządzeń sieciowych firmy CISCO.

Cel pracy

Celem tej pracy jest opracowanie konfiguracji urządzeń sieci komputerowej dla firmy XYZ składającej się z kilku podsieci. Sieć jest wykonana z zachowaniem odpowiedniej separacji miedzy poszczególnymi działami firmy a także możliwością udostępnienia danych dla wszelkich użytkowników i dostępu do sieci Internet. To wszystko zgodnie z zasadami bezpieczeństwa opracowanymi w firmie.

Podstawowym założeniem tej pracy jest pokazanie, że możliwe jest współistnienie kilku protokołów routingu w jednej sieci, a co za tym idzie połączenie kilku podsieci tak aby możliwa była wymiana danych i wykorzystanie wielu usług pomiędzy wszystkimi użytkownikami tych podsieci.

Protokoły jakie będą brane pod uwagę w tej pracy to:

- routing statyczny
- routing RIP
- routing EIGRP
- routing OSPF

Przegląd zawartości rozdziałów

Opracowanie to składa się z dwóch rozdziałów, wstępu i zakończenia-podsumowania. We wstępie przedstawiono istotę wykorzystywania sieci komputerowych w firmie oraz założenia projektowe jakie brano pod uwagę przy tworzeniu sieci.

Rozdział pierwszy to przybliżenie podstawowych wiadomości dotyczących sieci komputerowych oraz przedstawienie zagadnień związanych z routingiem w sieciach oraz przedstawienie użytych w projekcie protokołów routingu – statycznego, RIP, EIGRP, OSPF.

Rozdział drugi ma charakter praktyczny i zawiera opis wykonanej sieci komputerowej w firmie a także jej schemat. Zawarte są tutaj wszelkie wiadomości z praktycznego wykonania sieci. Pokazane są i wyjaśnione zastosowane rozwiązania techniczne i technologiczne jakie wykorzystano do budowy sieci. Są tam także opisy konfiguracji poszczególnych routerów.

Podsumowanie całej pracy inżynierskiej opisane jest w zakończeniu.

Rozdział I – Podstawowe wiadomości o sieciach i protokołach routingu

1.1 Sieci komputerowe

Sieć komputerowa to grupa komputerów lub innych urządzeń, które są połączone ze sobą w celu współdzielenia różnych zasobów lub wymiany danych. Połączenie komputerów pozwala użytkownikom na wspólne użytkowanie urządzeń peryferyjnych jak i też korzystanie z różnych usług oraz umożliwia wspólny i łatwy dostęp do programów i baz danych. Dzięki sieciom komputerowym możliwa jest wymiana informacji między różnym oprogramowaniem i różnymi systemami. [1]

1.1.1 Podział sieci

Sieci komputerowe można podzielić w zależności od ich wielkości i taki podział jest najczęściej stosowany:

a) **Local Area Network (LAN)** jest to najczęściej spotykany rodzaj sieci, które składają się z połączonych ze sobą kilku do nawet kilkuset komputerów znajdujących się na niewielkim obszarze obejmującym jedną firmę, jeden budynek (kilka budynków).

b) **Metropolitan Area Network (MAN)** to sieć miejska znajdująca się na obszarze jednego miasta lub regionu. Łączy ze sobą sieci LAN poszczególnych użytkowników takich jak uczelnie i instytucje. Przykładem takiej sieci są łódzka sieć LODMAN oraz warszawska sieć WARMAN.

c) **Wide Area Network (WAN)** są to sieci rozległe łączące urządzenia rozmieszczone na dużych obszarach geograficznych. Sieć WAN łączy ze sobą sieci miejskie MAN i lokalne LAN.

d) **Internet** zwana też „siecią sieci” jest to sieć globalna wykorzystująca protokół IP i łączy ze sobą wszystkie dostępne rodzaje sieci.

e) **Intranet** jest to sieć działająca najczęściej w ramach jednego przedsiębiorstwa oferująca podobne funkcje do sieci Internet. Nie musi być ograniczona terytorialnie ale najczęściej jest oddzielona od Internetu. [1]

1.1.2 Topologie sieci

Topologia sieci to zbiór reguł łączenia wszystkich elementów sieci komputerowych oraz zasad komunikacji przez różnego rodzaju medium transmisyjne. Topologie sieci możemy podzielić na topologie fizyczną i logiczną.

Topologia logiczna określa standardy komunikacji, dzięki którym poszczególne urządzenia bezbłędnie porozumiewają się w sieci. Topologia fizyczna jest związana z topologią logiczną. Przykładem jest specyfikacja Ethernet umożliwiająca skorzystanie z topologii fizycznej gwiaździstej albo magistrali, ale nie umożliwia zbudowania sieci w oparciu o topologię pierścienia.

Topologie logiczne definiowane są przez IEEE[1] (Institute of Electrical and Eletronics Engineers). Najczęściej spotykane specyfikacje sieci komputerowej to:

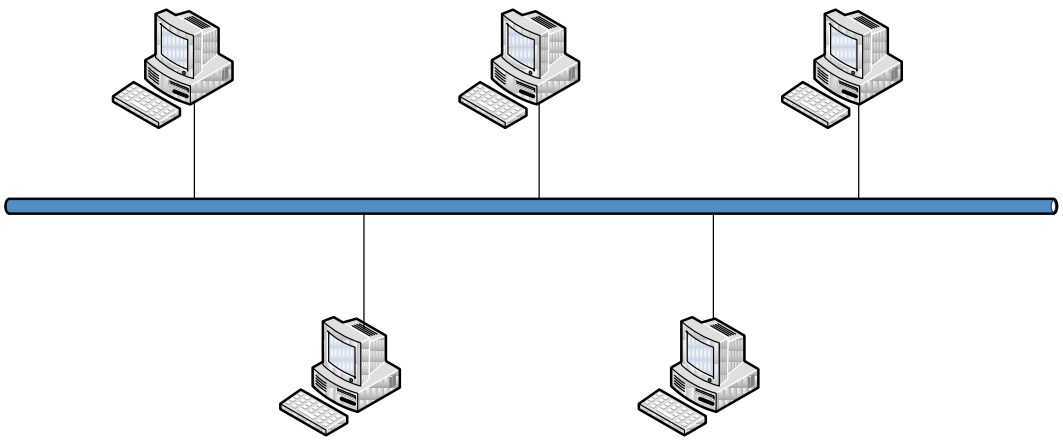
- IEEE 802.3 10 Mb Ethernet
- IEEE 802.3u 100 Mb Ethernet
- IEEE 802.3x Fuli Duplex Ethernet
- IEEE 802.3z 1 Gb Ethernet
- IEEE 802.5 Token Ring
- IEEE 802.11 Wireless LAN
- IEEE 802.12 100VG-AnyLAN
- IEEE 802.I4 Cable Modem

Topologie fizyczne:

a) **Topologia magistrali** - w topologii tej wszystkie urządzenia połączone są jednym przewodem do którego podłączone są hosty. Przewód główny zwany jest magistralą. Oba końce magistrali są zakończone opornikami ograniczającymi, zwanymi również często terminatorami. Chronią one przed odbiciami sygnału. Zawsze kiedy komputer wysyła sygnał, rozchodzi się on w przewodzie automatycznie w obu kierunkach. Jeśli sygnał nie napotka na swojej drodze opornika, to dobiega do końca magistrali, gdzie zmienia kierunek. W takiej przypadku pojedyncza transmisja może w całości zapełnić wszystkie dostępne szerokości pasma i uniemożliwić wysyłanie sygnałów pozostałym komputerom w sieci. Zaletą jest to, że wszystkie hosty mogą się bezpośrednio

[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]

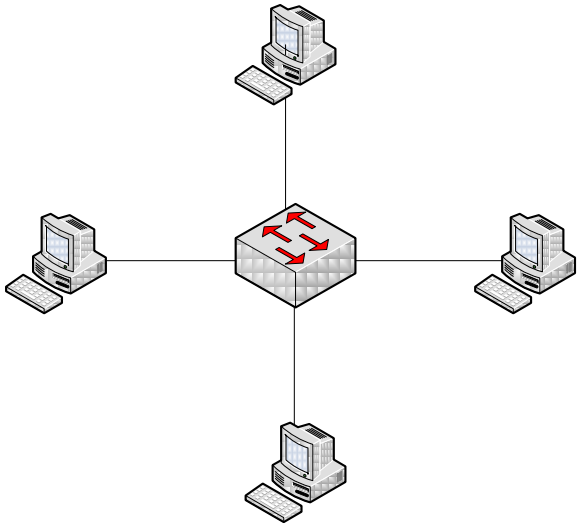
komunikować; wadą, że przerwanie kabla w jednym miejscu powoduje przerwanie działania sieci. Topologie taką stosuje się przeważnie przy wykorzystaniu kabla koncentrycznego. [1] [2]



Rysunek nr 1. Topologia magistrali [opracowanie własne]

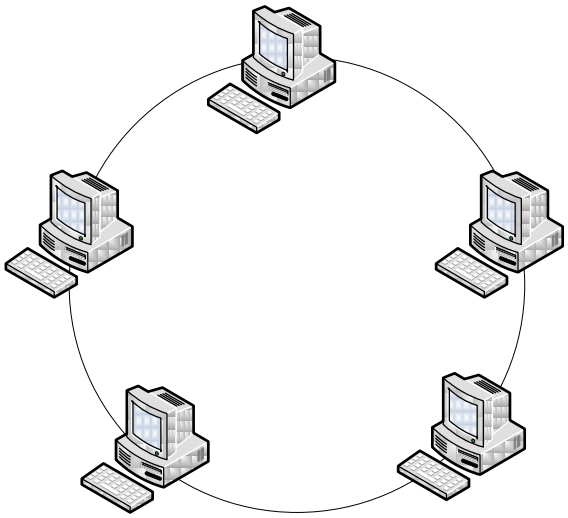
b) **Topologia gwiazdy** - połączenia sieci LAN w tej topologii z przyłączonymi do niej urządzeniami rozchodzą się z jednego punktu, którym jest przełącznik (SWITCH). Okablowanie całej sieci opiera się na skrętce czteroparowej i kart sieciowych z wyjściem z zakończeniami RJ-45[2]. Cechą tej topologii jest to, że każdy host (urządzenie) połączone jest do punktu centralnego za pomocą jednego osobnego przewodu. Zmniejsza to awaryjność całej sieci ponieważ w razie awarii jednego przewodu nie działa tylko jedno urządzenie a pozostałe mogą pracować bez żadnego problemu. W bardzo łatwy sposób można łączyć ze sobą kilka sieci w topologii gwiazdy. Wadą tej topologii jest to, że jeśli centralny punkt sieci (switch) ulegnie uszkodzeniu, cała sieć jest unieruchomiona. Topologie te stały się dominujące we współczesnych sieciach LAN. Są one dość łatwe w wykonaniu oraz stosunkowo tanie. [1] [2]

[2] RJ-45 – Typ złącza stosowany w sieciach teleinformatycznych



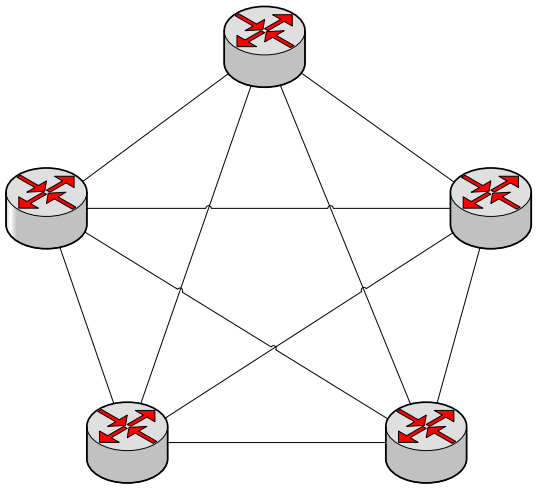
Rysunek nr 2. Topologia gwiazdy [opracowanie własne]

c) **Topologia pierścienia** - każdy przyłączony do sieci host w ramach takiej topologii ma dwa połączenia po jednym ze swoimi najbliższymi sąsiadami. Połączenie musi tworzyć fizycznie pierścień. Dane przesyłane są wokół pierścienia w jednym kierunku. Każdy host pobiera i odpowiada na pakiety do niego zaadresowane, i przesyła pozostałe pakiety do następnego hosta wchodzącego w skład sieci. Ujemną stroną tego rozwiązania jest to, że uszkodzenie jednego urządzenia najczęściej unieruchamia całą sieć pierścieniową. Aby temu zapobiec często stosuje się tzw. topologię podwójnego pierścienia. Dodaje się drugi niezależny pierścień, który łączy te same urządzenia i spełnia rolę pierścienia zapasowego. [1] [2]



Rysunek nr 3. Topologia pierścienia [opracowanie własne]

d) **Topologia MESH** - Założeniem topologii MESH jest możliwość bezpośredniego połączenia każdego węzła z innym węzłem sieci co jest podstawową zaletą tego rozwiązania. Daje to możliwość, w przypadku awarii jednego elementu sieci, przesłania informacji inną drogą i dane zawsze dotrą do określonego celu. Następna zaleta pozwala na przesłanie informacji wieloma ścieżkami sieciowymi. W praktyce topologia ta jest wykorzystywana do łączenia kilku sieci w topologii gwiazdy tak aby jej kluczowe elementy były połączone za pomocą sieci MESH. [1] [2]



Rysunek nr 4. Topologia MESH [opracowanie własne]

1.1.2 Media transmisyjne

Media transmisyjne to technologie pozwalające na komunikowanie się urządzeń podłączonych do sieci. Media transmisyjne dzielimy na przewodowe i bezprzewodowe.

Media przewodowe możemy podzielić na media miedziane i optyczne.

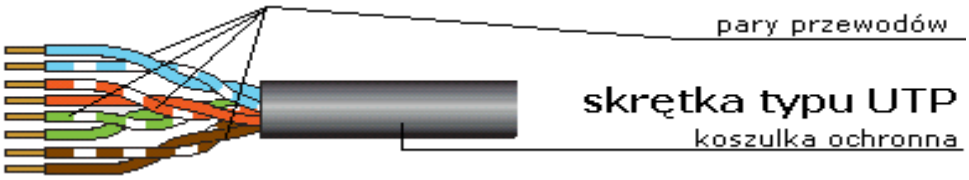
Media przewodowe miedziane

Najczęściej stosowanym w sieciach lokalnych jest tak zwana skrętka. Są to cztery pary przewodów we wspólnej osłonie. Podczas przesyłania sygnałów za pomocą skrętki uzyskuje się przepływności do 100 Mb/s (kat.5), a także 1000 Mb/s - Gigabit Ethernet. Do podłączania najczęściej służą złączki RJ-45.

Rozróżniamy następujące rodzaje przewodu:

a) UTP (ang. Unshielded Twisted Pair) - skrętka nieekranowana zbudowana z dwóch przewodów, ze zmiennym splotem co ochrania transmisję przed wpływem otoczenia. Podczas przesyłaniu sygnałów za pomocą skrętek UTP (cztery pary) uzyskuje się przepustowość do 100 Mb/s (kat.5), oraz 1 Gb/s - Gigabit Ethernet. Do przesyłania

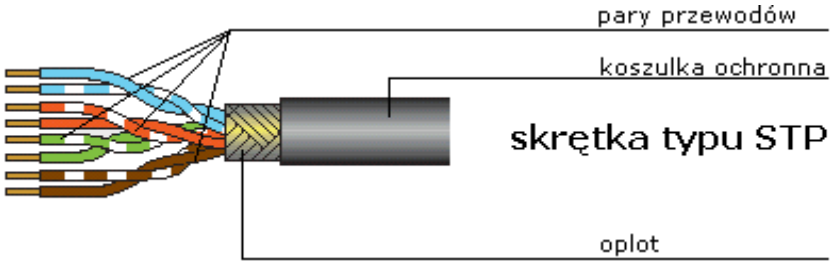
sygnałów w sieciach informatycznych konieczne są przewody kategorii 3 (10 Mb/s) i kategorii 5 (100 Mb/s), przy czym powszechnie stosowana jest tylko ta ostatnia.



Rysunek nr 5. Skrętka UTP

[źródło: http://www.promanski.info/wp-content/photos/utp.png]

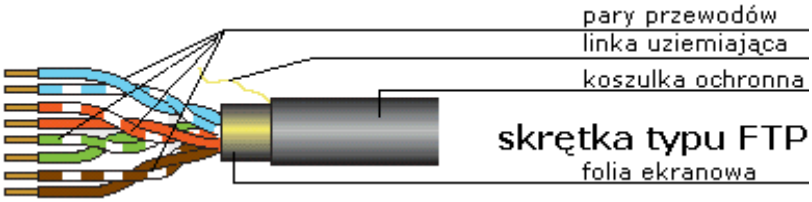
b) STP (ang. Shielded Twisted Pair) - skrętka ekranowana wykonana jest z dwóch skręconych przewodów wraz z ekranem w postaci oplotu. Jest bardziej odporna na zakłócenia od skrętki UTP.



Rysunek nr 6. Skrętka STP

[źródło: http://www.promanski.info/wp-content/photos/stp.png]

c) FTP (ang. Foiled Twisted Pair) - skrętka foliowana – jest to skrętka miedziana ekranowana folią wraz z przewodem uziemiającym. Przeznaczona jest przeważnie do tworzenia sieci komputerowych (Ethernet, Token Ring) o długości do nawet kilku kilometrów.



Rysunek nr 7. Skrętka FTP

[źródło: http://www.promanski.info/wp-content/photos/ftp.png]

Poza opisanymi wyżej rodzajami skrętek spotkać można także różne połączenia tych technologii:

- F-FTP – każda para przewodów jest otoczona osobnym ekranem z folii, a cały przewód jest również pokryty osłoną z folii,
- S-FTP – każda para przewodów jest otoczona osobnym ekranem z folii, a cały przewód pokryty jest oplotem,
- S-STP – każda para przewodów jest otoczona osobnym ekranem - oplotem, a cały przewód pokryty jest oplotem.

Zaletą skrętki komputerowej jest to, że posiada bardzo dobry stosunek możliwości do ceny, jest łatwa w montażu, charakteryzuje się duża przepustowością - do 1000Mb/s. [7]

Media przewodowe optyczne

Jednym z coraz częściej stosowanym medium transmisyjnym jest światłowód (ang. Fiber Optic Cable). Działanie światłowodu polega na transmisji impulsów świetlnych między nadajnikiem - przetwarzającym impulsy elektryczne na świetlne, a odbiornikiem przetwarzającym impulsy świetlne na elektryczne.

Światłowód zbudowany jest z powłoki zewnętrznej i płaszcza rdzenia.

Rysunek nr 8. Budowa światłowodu

[źródło: http://www.sieci-informatyczne.yoyo.pl/images/swiatlowod-budowa.gif]

Mówiąc o światłowodach musimy wyjaśnić pojęcie modu światłowodowego. Można pojęcie to określić jako tor ruchu promienia w włóknie. Liczba takich ruchów jest skończona i zależna od rodzaju światłowodu.

Rozróżniamy dwa rodzaje światłowodów:

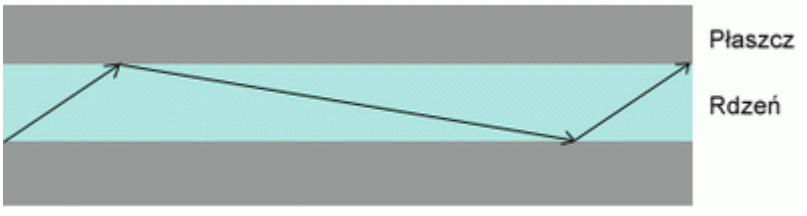
a) jednomodowy (ang. single mode) - światłowód taki posiada tylko jeden mod, ponieważ rozmiar rdzenia zbliżony jest do długości prowadzonej fali. Średnica włókna światłowodu jedno modowego to rząd wielkości kilku mikrometrów. Zasilane są

światłem spójnym generowanym przez lasery. Wykazują małe tłumienie i mogą przewodzić sygnały na odległości rzędu setek kilometrów.

Rysunek nr 9. Światłowód jednomodowy

[źródło: http://www.sieci-informatyczne.yoyo.pl/images/jednomod.gif]

b) wielomodowy (ang. multi mode) - posiada średnicę włókna rzędu kilkudziesięciu mikrometrów. Zasilanie może odbywać się przy pomocy diody świecącej LED. Sygnał w tych światłowodach ulega silniejszemu tłumieniu niż w światłowodach jednomodowych. Służą one do transmisji rzędu pojedynczych kilometrów (maksymalnie 5km).



Rysunek nr 10. Światłowód wielomodowy

[źródło: http://www.sieci-informatyczne.yoyo.pl/images/skokowy.gif]

Zaletami światłowodów jest całkowita odporność na zewnętrzne zakłócenia elektromagnetyczne, możliwość transmisji na duże odległości oraz bardzo duża szybkość transmisji. Wadą jest wysoka cena, skomplikowana i kosztowna instalacja oraz możliwość wykorzystania tylko jako połączenia punkt - punkt. [1] [8]

1.2 Technologie przesyłu danych

1.2.1 xDSL

xDSL (ang. X Digital Subscriber Line) jest to nazwa wspólna dla wszystkich technologii cyfrowych linii abonenckich, które używają istniejących sieci telefonicznych do przesyłania danych bez konieczności ich przebudowy. Technologie xDSL dzielimy na dwie grupy.

Pierwszą z nich jest to technika symetrycznego przesyłania informacji, W tym wypadku prędkość wysyłania i odbierania danych jest taka sama. Zaliczamy do niej:

- **HDSL** (ang. High data rate Digital Subscriber Line) - cyfrowa linia abonencka o wysokiej przepustowości. HDSL do transmisji danych wykorzystuje miedziane kable telefoniczne. Korzysta jednak nie tak jak telefony z pasma 300 - 3400 Hz, ale dużo szerszego - od 6 do 259 kHz. Technologia HDSL na początku swojego istnienia wykorzystywała do transmisji symetrycznej 2 Mb/s w obie strony aż 3 pary kabli miedzianych. W miarę rozwoju do przesyłu zredukowano najpierw do dwóch, a potem do jednej pary kabli koniecznych do uzyskania pełnej przepustowości 2 Mb/s. Zaletą HDSL jest wykorzystanie tradycyjnej infrastruktury telekomunikacyjnej do abonenta tzw. ostatniej mili. Wadą natomiast jest zależność przepustowości od długości przewodów oraz mały zasięg. Technika HDSL umożliwia przesyłanie w dwóch kierunkach strumieni E1 lub T1 na jednej, dwu, trzech parach kabli miedzianych. Jednoparowe łącze HDSL jest często wyróżniane jako transmisja SDSL. Charakteryzuje się mniejszym zasięgiem transmisji - do 3 kilometrów - niż HDSL kilkuparowy. Zaletą jest to, że korzysta z jednej pary przewodów miedzianych, którą zawsze jest u abonenta.
- **SDSL** (ang. Symmetric Digital Subscriber Line) to technologia przesyłu danych za pomocą linii telefonicznej, która pozwala użytkownikowi połączyć się z siecią Internet w sposób symetryczny. Pozwala na wideokonferencje czy budowanie korporacyjnych sieci wirtualnych. Prędkość transmisji to: 1,536 Mb/s (T1) lub 2 Mb/s (E1).

Druga grupa to technika niesymetrycznego przesyłania danych, dla której prędkość wysyłania danych jest znacznie mniejsza od prędkości pobierania. Zaliczamy do niej: ADSL i VDSL.

- **ADSL** (ang. asymetryczna cyfrowa linia abonencka) – umożliwia asymetryczny dostęp do sieci teleinformatycznych. Asymetria polega na tym, iż przesyłanie danych do użytkownika (z Internetu) jest szybsze niż z odwrotnego kierunku. Została stworzona z myślą o użytkownikach, którzy częściej odbierają dane niż je wysyłają. W ADSL wykorzystuje się przeważnie, miedziane kable telefoniczne. Standard ten pozwala na dużo szybszą komunikację niż technologia z użyciem modemów telefonicznych, w której sygnały są przetwarzane na sygnał analogowy u nadawcy, a następnie znowu przetwarzane na sygnał cyfrowy u odbiorcy. W standardzie ADSL sygnał po obu stronach jest cyfrowy. Umożliwia to wymianę danych, zarówno operator (ISP) jak i użytkownik, muszą posiadać na obu końcach linii telefonicznej odpowiednie modemy

ADSL. Technologia ta pozwala na prędkości transmisji od 16 kb/s do 24 Mb/s. Rodzaje technologii ADSL:

a) ADSL1 – jest najstarszą wersją i umożliwia transmisję rzędu 1536 Kb/s lub 2048 Kb/s, na odległość nie większą niż 5,5 kilometrów.
b) ADSL2 – transmisja w tym przypadku to 3072 Kb/s lub 4096 Kb/s, na odległość nie większą niż 3,7 kilometra.
c) ADSL2+ - stwarza możliwość transmisji z prędkością około 24 Mb/s, na odległość nie większą niż 2 kilometry.
d) ADSL3 – prędkości przesyłu to 200 Mb/s, na odległość nie większą niż 300 metrów. Prędkość wysyłania danych wynosi natomiast ok. 100 Mb/s

- **VDSL** (ang. Very High Speed DSL) jest to technologia umożliwiająca przesył danych za pomocą jednej pary kabla miedzianego. Prędkości uzyskiwane 12,96 Mb/s; 25,96 Mb/s; 51,84 Mb/s przy odległości do 1500m. Kanał zwrotny uzyskuje prędkość z zakresu 1,6 – 26 Mb/s.
- **RADSL** (ang. Rate Adaptive DSL) – jest to wersja DSL asymetrycznego, której cechą jest możliwość automatycznego dopasowania parametrów przesyłu danych do jakości łącza. Umożliwia automatyczne dostrojenie się współpracujących modemów do przepływności aktualnie dostępnych. Technologie ADSL, które są w tej chwili wykorzystywane są właśnie w większości w tej technologii. [5] [16]

1.2.2 Frame Relay

Jest to nowoczesna sieciowa technika transmisji danych, która opiera się na komutacji pakietów. Technologia ta dzieli przesyłaną informację na ramki przenoszące dane między sieciami LAN. Daje to możliwość budowy rozległych sieci - WAN. Ramki przesyłane są przez wiele węzłów sieci Frame Relay aż dotrą do miejsca docelowego. Węzły pośredniczące zajmują się jedynie przesyłaniem pakietów.

W sieci Frame Relay urządzenia końcowe same przeprowadzają procedurę kontroli błędów i w razie ich wykrycia żądają powtórzenia transmisji pakietów.

Sieć ta składa się z przełączników, które są połączone kanałami fizycznymi, w których są multipleksowane obwody wirtualne identyfikowane po niepowtarzalnych numerach DLCI. W skład sieci wchodzą także urządzenia dostępowe.

Technologia zwana jest często jako „chmura sieciowa" gdyż nie występuje w niej indywidualne fizyczne połączenie pomiędzy użytkownikami. Tworzona jest tylko logiczna

ścieżka nazwana połączeniem wirtualnym (ang. Virtual Circut). Pasmo przepustowe jest przydzielane dla danej ścieżki logicznej tylko wtedy, gdy dane są naprawdę przesyłane.

Połączenia wirtualne są połączeniami full-duplex[3] i są realizowane przez odpowiednie oprogramowanie węzłów sieci.

Oferowane są dwa typy połączeń wirtualnych:

- przełączane połączenia wirtualne (ang. switched virtual circuits) – SVCs. Przełączane połączenia wirtualne SVC są złączane i rozłączane na życzenie użytkownika, podobnie jak w tradycyjnej telefonii. Niektóre ustawienia takiego połączenia negocjuje się w czasie nawiązywania sesji. Komunikaty informujące o stanie połączenia SVC może zawierać jedną z niżej wymienionych informacji:
    a) Call Setup - połączenie wirtualne pomiędzy dwoma DT FR zostało ustalone
    b) Data Transfer – informuje, że trwa wymiana danych między DTE przez obwód wirtualny SVC
    c) Idle – połączenie ustalone, ale nieaktywne. Taki stan trwający przez ponad zdefiniowany czas może spowodować rozłączenie SVC
    d) Call Termination - oznacza, że połączenie między DTE zostało rozłączone

  Ustanowienie połączenia SVC pomiędzy nadawcą i siecią Freme Relay rozpoczyna sygnalizacja przez kanał typu D, zgodnie specyfikacją Q.933 dla ISDN.
- stałe połączenia wirtualne (ang. permanent virtual circuits) – PVCs. Stałe obwody wirtualne PVC, które odpowiadają dzierżawionym liniom. Są więc zestawiane na określony okres. Komunikat sieci Frame Relay o stanie PVC może zawierać jedną z dwu informacji:
    a) Data Transfer – informuje o trwającej wymianie danych między DTE przez obwód PVC
    b) Idle - połączenie jest ustalone, ale nieaktywne. Przedłużający się stan braku aktywności obwodu PVC nie ma wpływu na żadne decyzje.

  Urządzenie DTE nie nawiązuje połączenia PVC, wysyłane są dane bez uruchamiania procedur sygnalizacyjnych. Jest to typ połączeń dominujących sieciach Frame Relay WAN.

W technologii Frame Relay występują dwa poziomy protokołów:

- jeden do przesyłu danych między urządzeniami dostępowymi

[3] Full duplex - jednoczesna komunikacja w obu kierunkach.

- drugi do sygnalizacji (pozwala sprawdzić integralność interfejsu z siecią oraz przekazuje informacje o stanie obwodów wirtualnych)

Sieć Frame Relay zapewniają komunikację połączenia o przepustowości do 45 kb/s. Funkcjonują na łączach cyfrowych dobrej jakości, które odznaczają się małą ilością błędów. Lista zastosowań Frame Relay:

- wykorzystywane są do łączenia sieci LAN,
- umożliwiają dostęp do ATM,
- umożliwiają transmisję danych oraz głosu,
- umożliwiają wideokonferencje i telekonferencje,
- pozwalają na transport plików przez WAN pomiędzy stacjami wysokiej rozdzielczości a bazą danych,
- umożliwiają komunikację interaktywną pomiędzy terminalami a zasobami komputerów, lecz w ograniczonym zakresie przepływności.

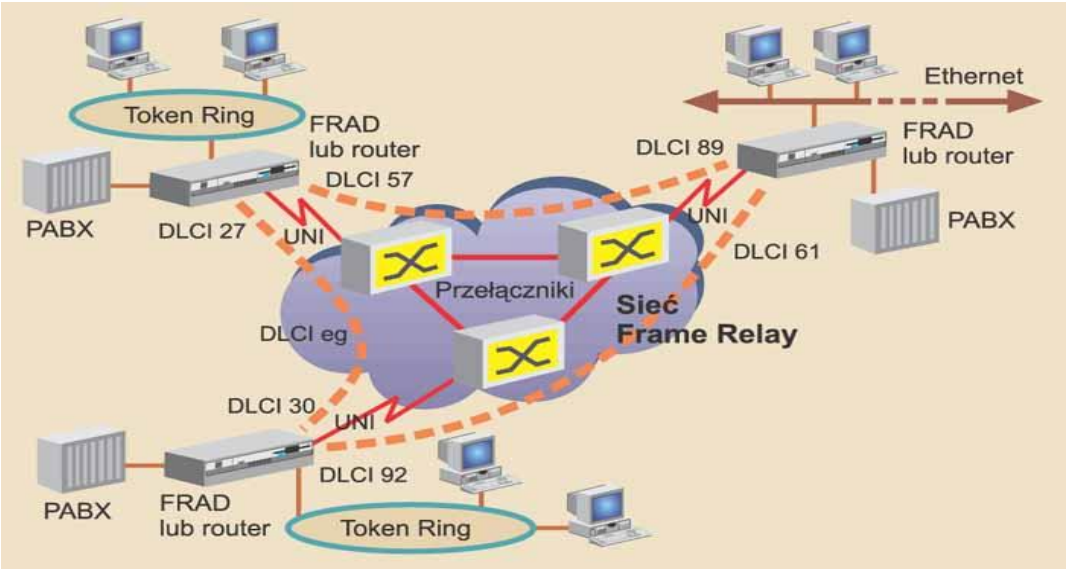
Zaletami sieci Frame Relay są:

- niskie koszty w porównaniu z sieciami opartymi na fizycznych łączach dzierżawionych
- duża elastyczność zmian połączeń
- łatwa integracja z innymi technologiami

Wady to:

- za korekcję błędów przesyłu muszą odpowiadać protokoły warstw wyższych
- wymagane są łącza o bardzo dobrej jakości

[9] [16]



Rysunek nr 11. Przykładowa sieć Frame Relay

[źródło: http://itpedia.pl/index.php/Grafika:Networld_vad_148_02.jpg]

1.2.3 ATM

Standard ATM (ang. Asynchronous Transfer Mode) można powiedzieć, że powstał z dwóch już istniejących technik cyfrowej transmisji szerokopasmowej: STM (Synchronous Transfer Mode) i PTM (Packet Transfer Mode). Połączył zalety tych technologii, a jednocześnie usunął większość wad tych systemów. STM stosowana jest w sieciach ISDN, zaś PTM w lokalnych sieciach komputerowych.

ATM może być łatwo przetwarzane sprzętowo w samych urządzeniach. Dzięki temu możliwe jest uzyskanie dużych prędkości przesyłu. Sieci ATM oferują obecnie kilka klas szybkości: 25Mb/s, 100Mb/s, 155,52Mb/s, 622Mb/s, 2,5Gb/s, 10Gb/s. W miarę rozwoju możliwości technologia ATM może osiągnąć coraz większe prędkości transmisji.

Przesył danych w standardzie ATM charakteryzuje się:

- przesyłaniem informacji o stałym rozmiarze 53 bajty - w tym 48 bajtów informacji użytecznej - ułatwia to obróbkę w węzłach sieci ATM
- ustalaniem połączeń indywidualnych o dowolnej prędkości w obrębie istniejących standardów (25Mb/s, 100Mb/s, 155Mb/s, 622Mb/s, 2500Mb/s), dzięki dopasowaniu dowolnej liczby komórek do danego połączenia użytkownika
- obsługą transmisji izochronicznych[4] (głos, obraz ruchomy, HDTV) z opóźnieniem nie większym niż 10ms, przez zastosowanie przełączników ATM z szybkim przełączaniem komórek i połączeń
- skalowaniem przepływu ścieżek i węzłów ATM, dzięki temu wykorzystuje się w pełną maksymalną przepływność dowolnego medium transportowego.
- transmisją, która jest w trybie połączeniowym – oznacza to, że przed wysłaniem informacji występuje zestawienie łącza - według parametrów określonych przez abonenta (określenie typu usługi, określona przepływność, deklarowany adres), a po zakończeniu przekazu łącze jest kasowane
- wirtualizacją połączeń przez sieć zarówno dla pojedyńczych kanałów, jak i definiowanych grup kanałów zwanych ścieżkami. Umożliwia to istnienie identyfikatorów VCI (Virtual Channel Identifier) dla kanałów oraz identyfikatorów VPI (Virtual Path Identifier) dla ścieżek wirtualnych. Pola takich identyfikatorów znajdują się w nagłówku komórki ATM przesyłanej przez sieć

[4] Transmisja izochroniczna – jest to sposób komunikacji zapewniający stałą szybkość transmisji, niezależnie od wielkości ruchu generowanego w otaczającym go środowisku. Transmisja izochroniczna jest niezbędna do obsługi ruchu multimedialnego, zwłaszcza sygnałów głosowych i wideofonicznych, gdzie wymaga się uzyskania stałego ruchu ramek, przybywających w równomiernych odstępach czasu i w tej samej kolejności, w jakiej zostały nadane. Opóźnienia w przekazach pakietowych między skrajnymi punktami transmisji nie powinny przekraczać 50 ms dla przekazów obrazowych i nie więcej niż 150 ms dla głosu. [14]

- przypisaniem komórkom ATM określonej usługi, której parametry mogą być dynamicznie zmieniane w fazie nawiązywania łącza, jak i w trakcie wykonywania usługi komunikacyjnej;
- dostosowanie pracy sieci z różnymi protokołami i do realizacji różnych usług.

W sieci opartej na technologii ATM wyróżnia się następujące klasy interfejsów:

UNI (User to Network Interface) - styk użytkownika - z siecią szerokopasmową, znajduje się między urządzeniem użytkownika a zakończeniem sieci, w którym są realizowane protokoły dostępu do sieci (przełączniki dostępowe).

NNI (Network to Network Interface) styk sieciowy, który znajduje się między węzłami.

PNNI (Private Network to Network Interface), definiuje współpracę przełączników ATM wraz z możliwością „nauki" topologii sieci, przekaz i pamiętanie w przełącznikach dodatkowych informacji o stanie i parametrach poszczególnych łączy tj. szerokość pasma, opóźnienia przekazu komórek, poziom QoS uszkodzenia łączy i itp. Obniża to do minimum ilość przesyłanych aktualizacji. Dzięki temu zestawianie tras jest optymalne, i nie wymaga generowania dodatkowego (zbędnego) ruchu w sieci.

Połączenia w sieciach ATM nie oddają struktury fizycznej sieci lecz są one jedynie logiczne. Wyróżnia się dwa rodzaje połączeń:

- **VC** (Virtual Channel) - kanał wirtualny – jest to jednokierunkowe połączenie logiczne przez sieć między dwiema stacjami końcowymi, nawiązywane i przełączane dynamicznie przez węzły pośredniczące sieci czyli fizyczne przełączniki ATM.
- **VP** (Virtual Path) ścieżki wirtualne – jest to wiązka kanałów wirtualnych biegająca tą samą trasą co kanały wirtualne, która łączy dwóch użytkowników lub grupę abonentów końcowych w tych samych węzłach dostępu.

Koncepcja ścieżek i kanałów wirtualnych w topologii sieci jest zapewniona przez przydzielanie odpowiednich tzw. identyfikatorów ścieżki wirtualnej VPI (Virtual Path Identifier) oraz kanałów wirtualnych VCI (Virtual Channel Identifier) w zasięgu każdej ścieżki. Pola identyfikatorów VPI oraz VCI znajdują się w nagłówku pakietu przesyłanego w sieci ATM i są wypełniane i kasowane w węzłach dostępowych sieci oraz modyfikowane przez węzły pośredniczące.

Usługi sieciowe związane ze sposobem tworzenia połączeń wirtualnych wsieciach ATM:

- **PVC** (Permanent Virtual Connections) - stałe połączenia wirtualne - przydzielane są w przed komunikacją, a następnie dostępne przez dłuższy okres (miesiące, lata). Dla użytkownika, takie połączenie pełni rolę linii dzierżawionej o stałym opóźnieniu

- transmisji. W razie awarii tworzona jest droga zastępcza, która omija uszkodzony fragment sieci
- **SVC** (Switched Virtual Circuits) - dynamicznie przełączane połączenia wirtualne - na żądanie abonenta jest zestawiane i komutowane. Są to połączenia typu "punkt-punkt". Likwidowanie połączeń następuje natychmiast po zakończeniu przekazu, analogicznie do komutowania łączy w centrali telekomunikacyjnej
- **usługi bezpołączeniowe** (connectionless services) - nie wymagają organizacji trasy połączenia przed realizacją transmisji.

Aby zapewnić właściwe trasowanie przez sieci ATM stosuje się następujące sposoby wyznaczania połączeń:

- **Routing centralny** - polega na instalacji w sieci ATM jednego dużego i szybkiego routera, który jest włączony jednocześnie do wszystkich sieci wirtualnych. Rozwiązanie takie nie nadaje się do wyznaczania trasy w większych sieciach ATM, ponieważ ma ograniczoną wydajność, skalowalność i odporność pojedynczego routera centralnego oraz jego łącza
- **Routing rozproszony** - każde urządzenie dostępowe Ethernet/ATM jest jednocześnie przełącznikiem brzegowym i routerem. Urządzenia dostępowe, które mają możliwość trasowania są włączone do wszystkich sieci wirtualnych, w których uczestniczą, a wybór najlepszego routera jest wykonywany protokołem OSPF, stosowanym w sieciach TCP/IP. Wadami tego rozwiązania są: wysoki koszt urządzeń, trudności administracyjne sieci a także konieczność implementacji zabezpieczeń, ponieważ routing dokonuje się w wielu niezależnie konfigurowanych węzłach.
- **Protokół MPOA** (Multi-Protocol Over ATM) - ma on zalety routingu centralnego i pozbawiony jest jego wad. W tym sposobie routingu urządzeniami trasującymi są wybrane routery (nieliczne), lecz technicznie zaawansowane, które znajdują się w sieci ATM. Przy niewielkim obciążeniu całość tras w sieci jest kierowana przez te ustalone routery. Wzrost przepływności powyżej wyznaczonego progu powoduje tworzenie połączenia trasą krótszą i przekaz pakietów przez przełączniki ATM, które znajdują się na drodze między użytkownikami, a z pominięciem routera trasującego. Po ustalonym czasie braku aktywności urządzenia na brzegu zapominają o bezpośrednim połączeniu, a ustalenie komunikacji powtórnie dokonuje się przez router trasujący

[16]

1.3 Routing i protokoły routingu.

Wraz z rozwojem technologii komputerowych a co za tym idzie zwiększającą się ilością urządzeń połączonych za pomocą różnego rodzaju sieci zaszła potrzeba „kierowania ruchem" w sieciach, tak aby była zachowana odpowiednia komunikacja. Muszą być wyznaczone odpowiednie trasy, po których przesyłane są dane pomiędzy urządzeniami.
Routing (trasowanie) odpowiada, jak sama nazwa mówi, za wyznaczanie optymalnych tras dla przesyłanych informacji. Żaden z hostów w sieci nie ma wpływu na przebieg całej trasy pakietu danych przez sieć. Za wyznaczanie tras w sieciach informatycznych odpowiedzialne są kolejne routery w sieci.

Router wyznacza trasę w oparciu o docelowy adres IP przesyłanego pakietu. Wszystkie urządzenia, które w tym pośredniczą korzystają z docelowego adresu IP w celu wybrania właściwego kierunku wysyłania pakietów, aby zostały one dostarczone do właściwego miejsca docelowego.

Router odbierając pakiet sprawdza adres docelowy i wyszukuje w swojej tablicy routingu adresu sieci najbardziej zbliżonego do adresu docelowego. W tablicy routingu znajduje się także informacja o interfejsie routera, na który należy przekazać pakiet.
Protokół routingu można określić jako odpowiedni algorytm jaki jest potrzebny do optymalnego przesłania danych w sieci. Możemy je podzielić na kilka sposobów:

1. Ze względu na obszar działania:
    - Wewnętrzne (Interior Gateway Protocols - IGP). Działają one wewnątrz sieci lokalnych, są proste i mało obciążają routery. Zaliczamy do nich - RIP1, RIP2, EIGRP, OSPF.
    - Zewnętrzne (Exterior Routing Protocols - EGP). Działają na zewnątrz sieci lokalnych – BGP.
2. Ze względu na wykorzystanie maski sieci:
    - Routing klasowy - informacja o masce sieci nie jest rozsyłana między routerami. Klasa sieci rozpatrywana jest według danego adresu IP.
    - Routing bezklasowy - informacja o masce sieci jest rozsyłana przez routery.
3. Stosuje się też podział na:
    - 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, 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. Przykładem tego typu protokołów jest OSPF.

1.3.1 Routing statyczny

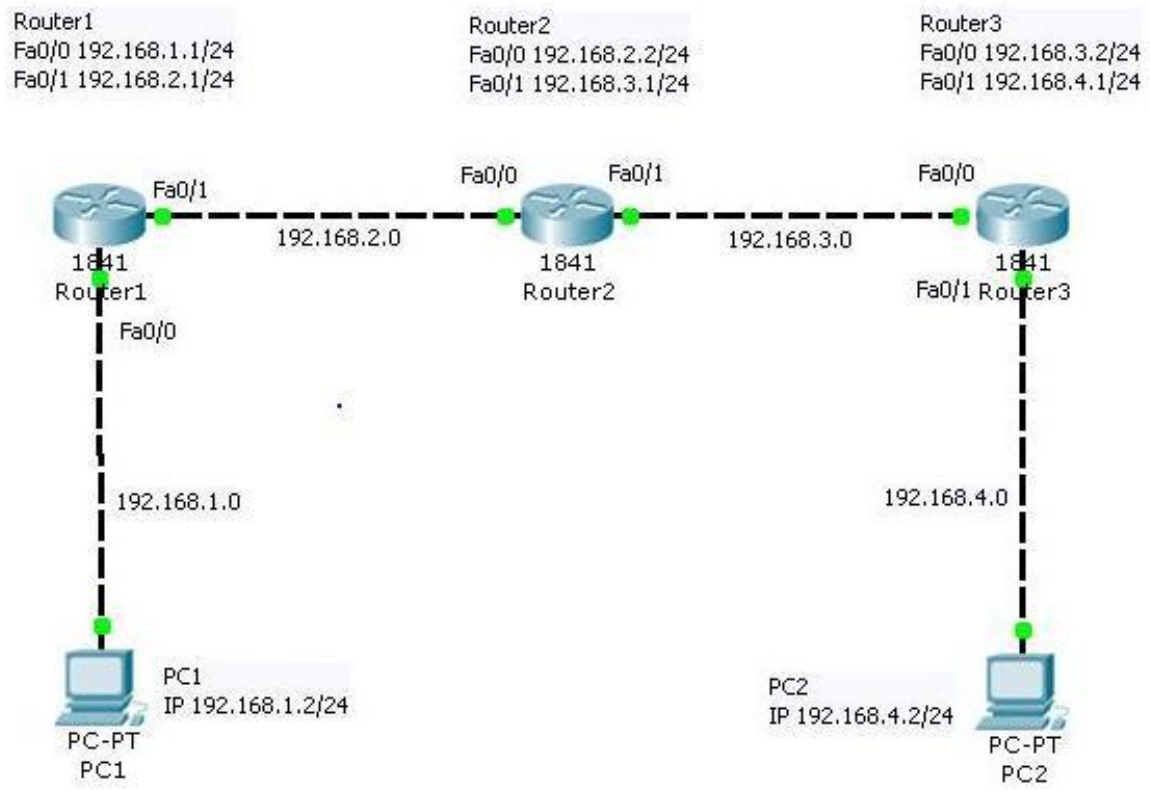
Przy konfiguracji routingu statycznego administrator wprowadza ręcznie trasy definiujące routing. Podczas tworzenia tras wymagane jest tylko podanie adresu sieci docelowej i interfejsu routera, przez który ma zostać wysłany pakiet.
Po konfiguracji routerów nie jest konieczne przesyłanie jakichkolwiek informacji na temat tras. Zadanie routera zostało ograniczone wyłącznie do przesłania pakietów po wcześniej zdefiniowanych trasach.

Przy zastosowaniu routingu statycznego zmiany w topologii sieci, zmiany parametrów lub awarie nie wpływają automatycznie na zmianę tablicy routingu. Wszystkie korekty muszą być wprowadzane przez administratora sieci.
Operacje routingu statycznego możemy skrótowo przedstawić w trzech punktach:

1. Konfiguracja routingu przez administratora.
2. Zapamiętanie tras wprowadzonych przez router.
3. Przesyłanie pakietów przez zapamiętane trasy.

Routing statyczny nie zapewnia wyboru optymalnej (w danej chwili) trasy przesłania pakietów w sieci. Sprawadza się w przypadku małych sieci, w których przesyłanie danych do wszystkich punktów docelowych odbywa się po tej samej trasie. Stosowany jest także jako trasy zapasowe. Na routerze można skonfigurować trasę statyczną, która używana będzie wtedy, gdy zawiedzie zapamiętana trasa dynamiczna. Aby użyć trasy statycznej jako zapasowej, należy ustawić dla niej wyższą wartość dystansu administracyjnego niż protokołu routingu dynamicznego. [4] [6]

Przykładowa konfiguracja routingu statycznego przedstawiona poniżej wykonana jest za pomocą oprogramowania Cisco Packet Tracert. Plik jest dołączony na płycie CD w katalogu „Lab” – nazwa pliku „routing_statyczny.pkt” – opracowanie własne.



Rysunek nr 12. Przykładowa sieć do konfiguracji routingu statycznego [opracowanie własne]

Podstawowa konfiguracja routing statycznego w sieci przedstawionej na rysunku nr 12: Przedstawiono także tablice routingu po zmianach w konfiguracji.

Router1

```
Router1(config)#ip route 192.168.3.0 255.255.255.0 fastEthernet 0/1
Router1(config)#ip route 192.168.4.0 255.255.255.0 fastEthernet 0/1
Router1(config)#do 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
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 is directly connected, FastEthernet0/1
S    192.168.4.0/24 is directly connected, FastEthernet0/1
```

Router2

```
Router2(config)#ip route 192.168.1.0 255.255.255.0 fastethernet 0/0
Router2(config)#ip route 192.168.4.0 255.255.255.0 fastethernet 0/1
Router2(config)#do 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
S    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
S    192.168.4.0/24 is directly connected, FastEthernet0/1
```

Router3

```
Router3(config)#ip route 192.168.2.0 255.255.255.0 fastethernet 0/0
Router3(config)#ip route 192.168.1.0 255.255.255.0 fastethernet 0/0
Router3(config)#do 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
S    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
```

1.3.2 RIP i RIP wersja 2

RIP jest jednym z najstarszych protokołów wektora odległości. Jest to standard otwarty.

Protokół RIP jest protokołem wewnętrznym (Interior Gateway Protocol) zaliczanym do protokołów wektora odległości (Distance Vector). Jest także wektorem klasowym co oznacza, że nie jest nim rozgłaszana maska sieci. Standardowy dystans administracyjny dla protokołu wynosi 120.

W protokole tym elementem wykorzystywanym do wyliczenia metryki jest liczba skoków przez kolejne routery na trasie do sieci docelowej. Jeśli do wybranej sieci prowadzi kilka tras z jednakową liczbą skoków, obie pokazywane są w tabeli routingu, inaczej pokazywana jest tylko trasa z najlepszą metryką. Standard protokołu RIP określa, że sieci w odległości większej niż 16 skoków są nieosiągalne co trzeba uwzględniać w konfiguracji sieci.

Tabela routingu ogłaszana jest do routerów sąsiadujących co 30 sekund a także po każdej zmianie konfiguracji sieci.

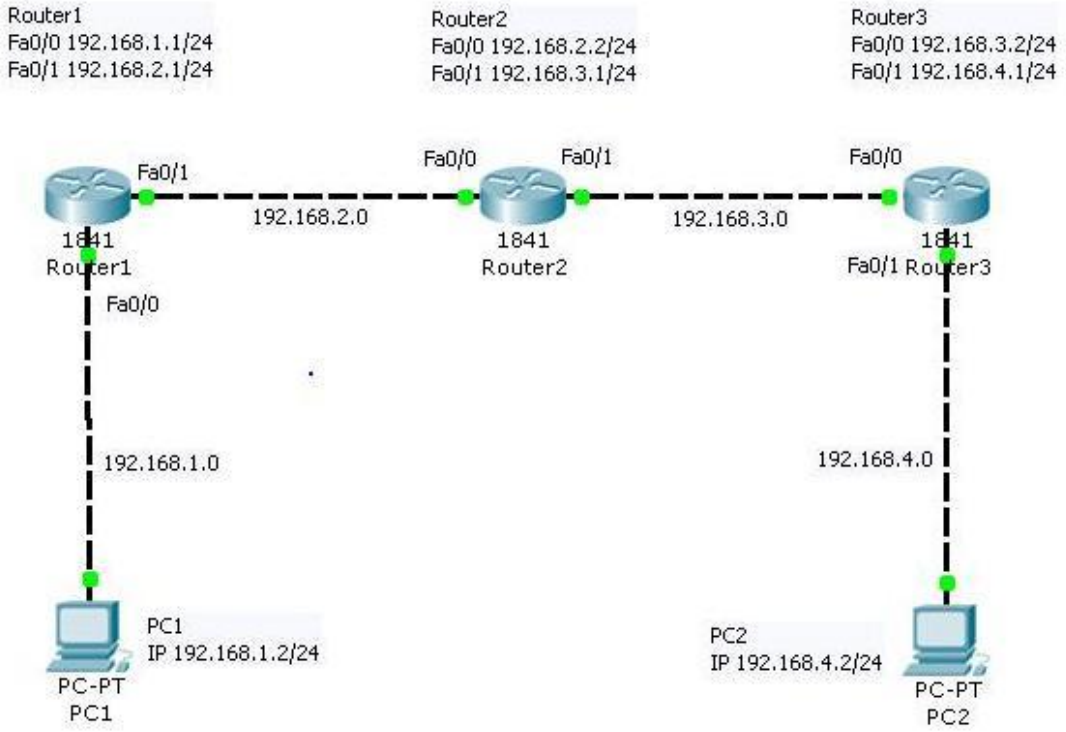
Protokół RIP nie ma własnego protokołu warstwy transportowej. Ogłoszenia realizowane są przez port 520 protokołem UDP. Routery rozgłaszają informacje metodą rozgłoszeniową na adres docelowy 255.255.255.255).

Zaletą protokołu jest łatwość konfiguracji i obsługi oraz dzięki ograniczeniu liczby skoków, uniemożliwienie przesyłania strumienia danych bez końca w pętli.

Schemat działania protokołu RIP przedstawia się następująco:

1. Żądanie aktualnych informacji o routingu od innych routerów i na tej podstawie aktualizacja tablicy routingu.
2. Odpowiedź na żądanie innych routerów.
3. W określonym czasie wysyłają informacje o swojej obecności, udzielając informacji innym routerom o aktualnej konfiguracji połączeń.
4. W przypadku wykrycia zmian w konfiguracji sieci rozsyłają aktualizację.

Przykładowa konfiguracja protokołu RIP przedstawiona poniżej wykonana jest za pomocą oprogramowania Cisco Packet Tracert. Plik jest dołączony na płycie CD w katalogu „Lab" – nazwa pliku „rip.pkt" – opracowanie własne.



Rysunek nr 13. Przykładowa sieć do konfiguracji protokołu RIP [opracowanie własne]

Podstawowa konfiguracja protokołu RIP w sieci przedstawionej na rysunku nr 13.

Przedstawiono także tablice routingu po zmianach w konfiguracji.

Router1

```
Router1(config)#router rip
Router1(config-router)#network 192.168.1.0
Router1(config-router)#network 192.168.2.0
Router1#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
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:23, FastEthernet0/1
R    192.168.4.0/24 [120/2] via 192.168.2.2, 00:00:23, FastEthernet0/1
```

Router2

```
Router2(config)#router rip
Router2(config-router)#network 192.168.2.0
Router2(config-router)#network 192.168.3.0
Router2#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 192.168.2.1, 00:00:03, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
R    192.168.4.0/24 [120/1] via 192.168.3.2, 00:00:20, FastEthernet0/1
```

Router3

```
Router3(config)#router rip
Router3(config-router)#network 192.168.3.0
Router3(config-router)#network 192.168.4.0
Router3#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 [120/2] via 192.168.3.1, 00:00:18, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:18, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
```

Protokół RIP2 jest ulepszoną wersją protokołu RIP. Przenosi informacje o masce sieci i wspiera VLSM[5]. Jest zaliczany go do protokołów bezklasowych.

Zmieniono także sposób komunikacji z urządzeniami sąsiednimi. Nadal wykorzystywany jest port 520 protokołu UDP ale transmisja realizowana jest w drodze emisji przy wykorzystaniu specjalnej grupy o adresie 224.0.0.9. Dzięki takiemu rozwiązaniu ruch związany z protokołem RIP nie obciąża wszystkich routerów w danym segmencie, a jedynie urządzenia należące do tej grupy.

Wprowadzono także możliwość wzajemnego uwierzytelniania routerów wymieniających informacje. Pozwala to wyeliminować z sieci routery nieautoryzowane, od których nie będą akceptowane ogłoszenia. Dla zapewnienia pełnej współpracy ze starszymi urządzeniami, które posługują się tylko wersją pierwszą RIP, dodano komendy pozwalające włączyć pełną zgodność z wersją pierwszą.

Konfiguracja praktycznie nie różni się od konfiguracji protokołu RIP. Po wydaniu polecenia **router rip** w następnej linii poleceń wpisujemy dodatkowo komendę **version 2.**

[4][10]

1.3.3 EIGRP

Protokół EIGRP jest protokołem firmy CISCO i można z niego korzystać wyłącznie w sieciach zbudowanych z urządzeń tej firmy. Został wprowadzony w 1994r. jako skalowalna, ulepszona wersja protokołu wektora odległości - IGRP.

EIGRP to protokół typu dystans-wektor i obsługuje bezklasowy routing międzydomenowy CIDR oraz technikę VLSM. Jest określany mianem protokołu hybrydowego, dlatego że łączy najlepsze cechy routingu według stanu łącza i wektora odległości.

W porównaniu z protokołem IGRP, który jest klasyfikowany jako klasowy protokół routingu, EIGRP zapewnia szybszą zbieżność, ma lepszą skalowalność i lepsze zarządzanie pętlami routingu. W protokole EIGRP maksymalna liczba przeskoków wynosi 224. Wystarcza to do zaprojektowania i obsługi dużych sieci,

Nad prawidłową pracą protokołu czuwa algorytm DUAL, który nadzoruje śledzenie wszystkich tras rozgłaszanych przez inne routery oraz na podstawie otrzymanych danych tworzy odpowiednią tablicą routingu. Umożliwia rozpoznanie i odrzucenie zapętlonych tras oraz pozwala na znalezienie alternatywnych.

[5] VLSM - (ang.Variable Length Subnet Masks) sposób adresacji IP pozwalający adresować sieci z maskami różnych długości.

EIGRP nie wysyła okresowych całych aktualizacji. Odświeżana jest informacja o sąsiedztwie z routerami przez wysłanie niewielkich pakietów oraz wysłanie częściowych aktualizacji w momencie wykrycia zmian w sieci. Zużywa mniej pasma od protokołów wektora odległości (np. RIP).

Routery skonfigurowane za pomocą EIGRP przechowują informacje o trasach i topologii w pamięci RAM urządzenia, dlatego mogą w szybki sposób reagować na zmiany.

Protokół EIGRP utrzymuje trzy tablice:

- tablica sąsiadów - każdy router w sieci utrzymuje tablicę sąsiadów. Zawarta w niej jest informacja o sąsiadujących z nim routerach. W momencie dodania nowego urządzenia w sąsiedztwie wykrywa i zapisuje informacje o jego adresie i interfejsie.
- tablica topologii zawiera wszystkie trasy jakie rozgłaszają sąsiadujące urządzenia.

  Routery EIGRP utrzymują osobną tablicę topologii dla każdego protokołu sieciowego, który jest skonfigurowany. Tablica topologii zawiera pola:

  Opłacalna odległość FD (Feasible Distance) - najniższa metryka do każdego z miejsc docelowych.

  Zgłaszana odległość RD (Reported Distance) - odległość do właściwego miejsca docelowego, która jest podana przez przylegającego sąsiada.

  Informacje o interfejsie - interfejs, przez który można dotrzeć do miejsca docelowego.

  Stan trasy - stan, w jakim jest się trasa.
- tablica routingu - przechowuje informacje o najlepszych trasach do danego miejsca docelowego. Dane te są pozyskane z tablicy topologii oraz tablicy sąsiadów. Routery EIGRP przechowują osobne tablice routingu każdego protokołu sieciowego.

Routery pracujące w protokole EIGRP tworzą tzw. relacje przylegania. Do tego celu wykorzystywane są małe pakiety „Hello”. Router zakłada, że dopóki otrzymuje pakiety „Hello” od znanych sąsiadujących urządzeń, to sąsiedzi oraz obsługiwane przez sąsiadów trasy funkcjonują prawidłowo.

Kiedy routery EIGRP tworzą relacje przylegania to:

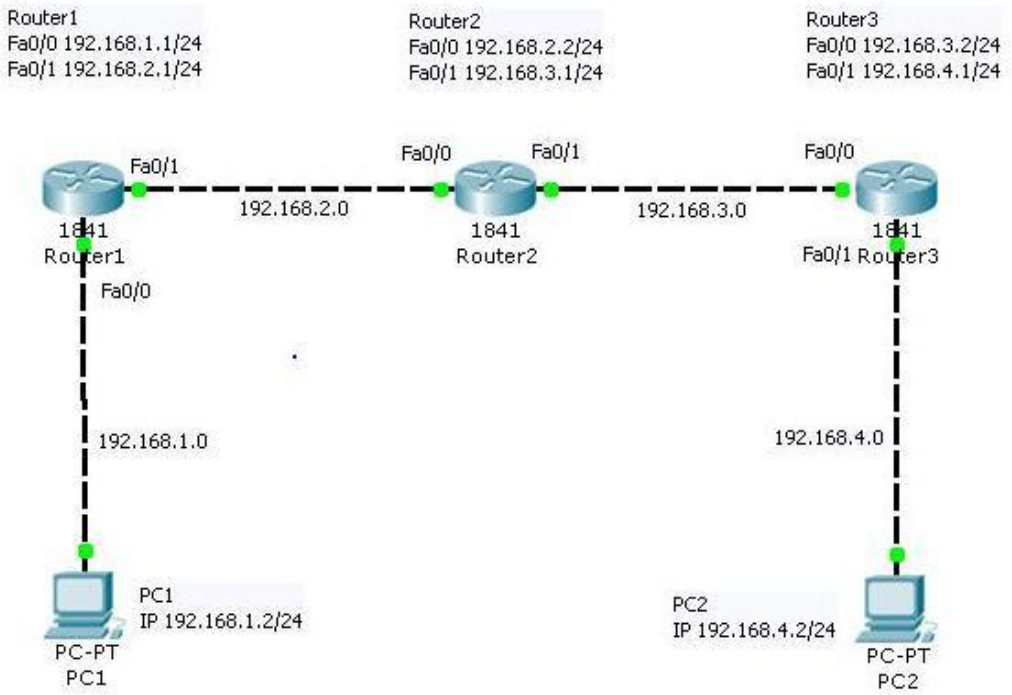
- dynamicznie uzyskują informację o nowych trasach pojawiających się w sieci
- wykrywają routery niedostępne lub takie, które przestały działać
- powtórnie wykrywają routery wcześniej niedostępne

W systemie działania protokołu EIGRP wyróżniamy 5 rodzajów pakietów:

1. **Pakiety HELLO** - wykorzystywane są do wykrywania i weryfikowania sąsiednich routerów. Routery EIGRP wysyłają pakiety Hello w jednakowych, ale możliwych do konfiguracji odstępach czasowych. - 5 sekund. Jeżeli router EIGRP nie otrzyma pakietu od sąsiada w określonym czasie, traktuje to jakby urządzenie to nie działało. W tej sytuacji algorytm DUAL zaczyna sprawdzanie tablicy routingu. Pakiety „Hello" w sieciach IP z routerami EIGRP wysyłane są pod adres grupowy 224.0.0.10.
2. **Pakiety potwierdzeń** (ang. acknowledgment) **–** są to pakiety „Hello" tylko pozbawione danych. Rozsyłane są pojedynczo jako potwierdzenie odbiorcy. Umożliwia to gwarantowaną komunikację między hostami EIGRP. Potwierdzenia takie mogą być dołączne do innych typów pakietów EIGRP, takich jak pakiety odpowiedzi
3. **Pakiety aktualizacyjne** (ang. update) **-** są używane w sytuacji, gdy router wykryje w sieci nowe urządzenie sąsiadujące. Wysyła wtedy do sąsiada pakiet aktualizujący, który umożliwia uzupełnienie tablicy topologii. Aby przekazać wszystkie informacje niejednokrotnie może to wymagać przesłania kilku pakietów. Pakiety aktualizacyjne wykorzystywane są również do wykrywania przez router zmian w topologii. W takiej sytuacji router wysyła do wszystkich sąsiadów pakiet w trybie multicast, z informacją o zmianie.
4. **Pakiety zapytań** (ang. query) – to pakiety z konkretnym zapytaniem wysyłanym do jednego lub wszystkich sąsiednich routerów.
5. **Pakiety odpowiedzi** (ang. reply) – to pakiety odpowiadające na pakiety zapytań. Pakiety odpowiedzi zawsze mają charakter transmisji pojedynczej

[3] [10]

Przykładowa konfiguracja protokołu EIGRP przedstawiona poniżej wykonana jest za pomocą oprogramowania Cisco Packet Tracert. Plik jest dołączony na płycie CD w katalogu „Lab" – nazwa pliku „eigrp.pkt"



Rysunek nr 14. Przykładowa sieć do konfiguracji protokołu EIGRP [opracowanie własne]

Podstawowa konfiguracja protokołu EIGRP w sieci przedstawionej na rysunku nr 14:

Przedstawiono także tablice routingu po zmianach w konfiguracji.

Router1

```
Router1(config)#router eigrp 55
Router1(config-router)#network 192.168.1.0
Router1(config-router)#network 192.168.2.0
Router1#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
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
D    192.168.3.0/24 [90/30720] via 192.168.2.2, 00:06:53, FastEthernet0/1
D    192.168.4.0/24 [90/33280] via 192.168.2.2, 00:05:12, FastEthernet0/1
```

Router2

```
Router2(config)#router eigrp 55
Router2(config-router)#network 192.168.2.0
Router2(config-router)#network 192.168.3.0
Router2#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
D    192.168.1.0/24 [90/30720] via 192.168.2.1, 00:11:40, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
D    192.168.4.0/24 [90/30720] via 192.168.3.2, 00:06:43, FastEthernet0/1
```

Router3

```
Router3(config)#router eigrp 55
Router3(config-router)#network 192.168.3.0
Router3(config-router)#network 192.168.4.0
Router3#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
D    192.168.1.0/24 [90/33280] via 192.168.3.1, 00:08:12, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 192.168.3.1, 00:08:12, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
```

1.3.4 OSPF

Protokół OSPF jest protokołem routingu stanu łącza zaliczanym jako bezklasowy obsługujący techniki VLSM i CIDR i jest protokołem wewnętrznym (IGP). Jest bardzo popularny ze względu, że rozwiązanie 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.
Jest protokołem skalowalnym i gwarantuje krótki czas konwergencji sieci oraz brak pętli.
OSPF korzysta z tzw. kosztów, przypisanych do każdego łącza - interfejsu o wartościach z przedziału: 1..65535.

Protokół ten dokonuje wyboru odpowiedniej ścieżki na podstawie kosztu, który jest metryką opartą na przepustowości. Do obliczenia najkrótszej ścieżki, wszystkie routery muszą dysponować pełnymi informacjami o sieciach dla każdego routera. Jest to algorytm bardzo złożony i dlatego protokół OSPF wymaga od routerów silnego procesora oraz większej ilości pamięci niż np. protokół RIP.

Protokół OSPF ma charakter hierarchiczny i pozwala podzielić jedną dużą sieć korporacyjną na mniejsze elementy zwane obszarami (ang. area). Obszar jest jakby samodzielnym elementem sieci, w której we wnętrzu odbywa się wymiana LSA (ang. Link State Advertisement) zakończona przeliczeniem ścieżek za pomocą algorytmu SPF (ang. Shortest Path First).

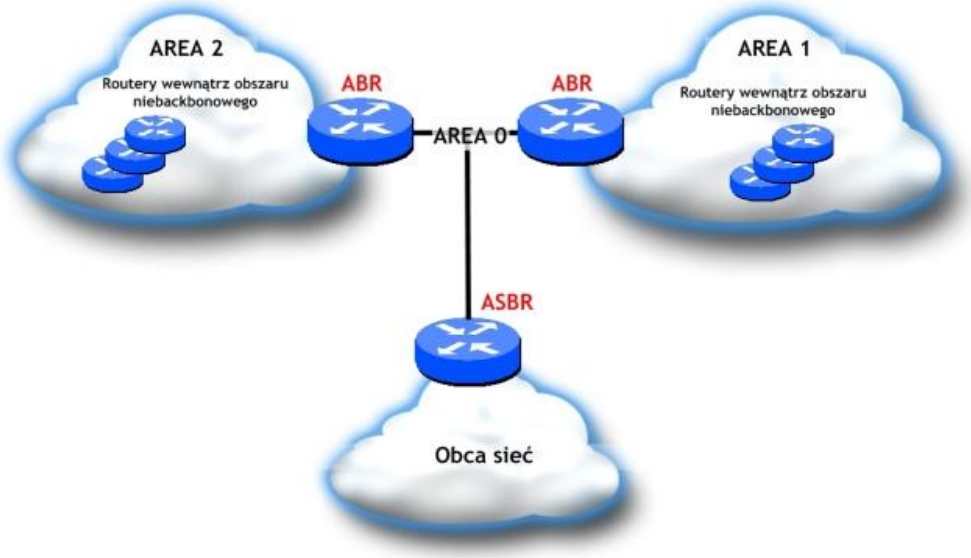
Algorytm SPF określa, że najlepszą trasę, która ma najniższy koszt. Algorytm przedstawia sieć jako zespół węzłów połączonych przez łącza punkt-punkt. Każde łącze ma przypisany koszt. Każdy węzeł ma określoną nazwę i dysponuje pełną wiedzą na temat wszystkich łączy.

Znana zatem jest pełna informacja o topologii fizycznej. Wszystkie bazy danych stanów łączy znajdujące się w danym obszarze są takie same.

Algorytm SPF wyznacza topologię pozbawioną zapętleń, używając konkretnego węzła jako punktu początkowego i odwołuje się do posiadanych informacji o przyległych węzłach.

Podział na obszary pozwala na zmniejszenie rozmiaru tablic routingu na routerach (sieci z jednego obszaru widziane są w innych obszarach w postaci sumarycznej). Routery w sieci OSPF mają przydzielone różne funkcje tj.:

- **Internal Router** jest to router, którego wszystkie interfejsy znajdują się w jednym obszarze. Jego zadanie to ogłaszanie LSA i utrzymywanie aktualnych informacji.
- **Backbone Router** – jest to router, którego wszystkie interfejsy znajdują się jednym obszarze tzw. area 0. Struktura protokołu OSPF określa istnienie specjalnego obszaru nazywanego area 0 bądź backbone area, który łączy inne obszary ze sobą.
- **Area Border Router** (ABR) - jest to router łączący dwa lub większą ilość obszarów - jednym z nich musi być routerem backbone area. Utrzymuje informacje o każdym z obszarów, do którego jest przyłączony i przesyła LSA między tymi obszarami. LSA zawierają zsumowane informacje o sieci w danym obszarze.
- **Autonomous System Border Router** (ASBR) – jest to router za pomocą , którego dochodzi do redystrybucji z OSPF na inny typ routingu np. redystrybucja.



Rysunek nr 15. Przykładowa sieć OSPF

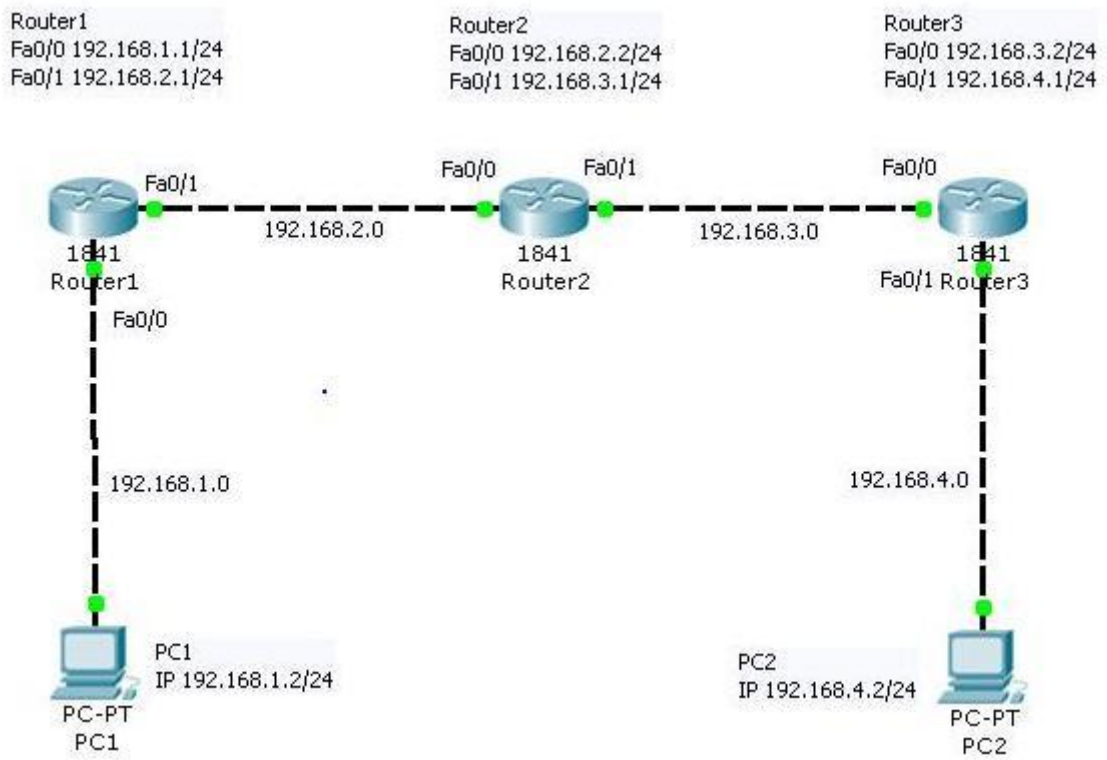
[źródło: http://cisco.howto.pl/artykuly,cisco-35-297-0.html]

Aby maksymalnie zmniejszyć ilość przesyłanych informacji w konkretnym segmencie sieci, OSPF wybiera router, który pełni rolę routera desygnowanego DR (ang. Designated Router). Wybierany jest także drugi router, który pełnić ma rolę zastępczego desygnowanego routera – BDR (ang. Backup Designated Router). Jeżeli router DR przestanie działać, to BDR przejmuje jego rolę. Takie rozwiązanie pozwala wyznaczyć punkt centralny z którym komunikują się wszystkie routery i wymieniają informacje o sieci, zamiast prowadzić wymianę informacji ze wszystkimi routerami osobno w danym segmencie.

Aby zagwarantować, że routery DR i BDR wiedzą o wszystkich stanach łącz wysyłanych przez wszystkie routery w segmencie, używany jest grupowy adres przeznaczony dla wszystkich routerów desygnowanych 224.0.0.6. Router DR przesyła informacje o stanie łącza do wszystkich pozostałych routerów OSPF za pomocą adresu grupowego 224.0.0.5.

[11] [12]

Przykładowa konfiguracja protokołu OSPF przedstawiona poniżej wykonana jest za pomocą oprogramowania Cisco Packet Tracert. Plik jest dołączony na płycie CD w katalogu „Lab" – nazwa pliku „ospf.pkt"



Rysunek nr 16. Przykładowa sieć do konfiguracji protokołu OSPF [opracowanie własne]

Podstawowa konfiguracja protokołu OSPF w sieci przedstawionej na rysunku nr 16:

Przedstawiono także tablice routingu po zmianach w konfiguracji.

Router1

```
Router1(config)#router ospf 100
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router1(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router1#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
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
O    192.168.3.0/24 [110/2] via 192.168.2.2, 00:06:52, FastEthernet0/1
O    192.168.4.0/24 [110/3] via 192.168.2.2, 00:04:47, FastEthernet0/1
```

Router2

```
Router2(config)#router ospf 100
Router2(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router2(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router2#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 [110/2] via 192.168.2.1, 00:08:43, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
O    192.168.4.0/24 [110/2] via 192.168.3.2, 00:06:38, FastEthernet0/1
```

Router3

```
Router3(config)#router ospf 100
Router3(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router3(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router3#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 [110/3] via 192.168.3.1, 00:07:55, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 192.168.3.1, 00:07:55, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
```

1.3.5 BGP

BGP czyli Border Gateway Protocol jest protokołem zewnętrznym i służącym przeważnie do komunikowania się routerów brzegowych różnych systemów autonomicznych. Protokół ten posiada mechanizmy ochrony przed zapętleniami pakietów i jest powszechnie stosowany do komunikacji między sieciami dostawców internetu IPS (Internet Service Providers) oraz w sieciach korporacyjnych do łączenia obszarów geograficznych lub administracyjnych.

Protokół BGP jak każdy protokół trasujący zarządza tablicami routingu i wymienia informacje o trasowaniu. Podstawową funkcją jest wymiana informacji o dostępności danej sieci zawierająca dane o liście ścieżek tzw. ASów. To może być wykorzystywane do skonstruowania grafu dostępności systemu autonomicznego. W informacjach rozgłaszanych urządzeniom BGP wysyłana jest tylko optymalna ścieżka do danej sieci. Informacja o routingu otrzymana jest od routera i jest przechowywana do czasu, gdy zostanie odebrane przyrostowe uaktualnienie. Każdy system autonomiczny posiada swój unikalny identyfikator ASN (Autonomic System Number), który jest nadawany przez odpowiednią organizację.
W Europie jest to RIPE[6]. Numer ten jest identyfikatorem wszystkich routerów BGP danego systemu.

BGP w warstwie transportowej wykorzystuje protokół TCP wraz z portem 179. Po nawiązaniu połączenia TCP dwa rutery utrzymują ze sobą sesję. Dzięki TCP protokół nie musi się martwić o utrzymywanie połączenia i sprawdzanie poprawności danych.

BGP powyżej warstwy transportowej posiada własne mechanizmy do zestawiania sesji i wymiany danych. Używane są pakiety do komunikowania się routerów, które potrzebne są do ustanawiania sesji, podtrzymywania jej, informowania routera sąsiada o zmianach oraz zamykania sesji.
Typy pakietów BGP:

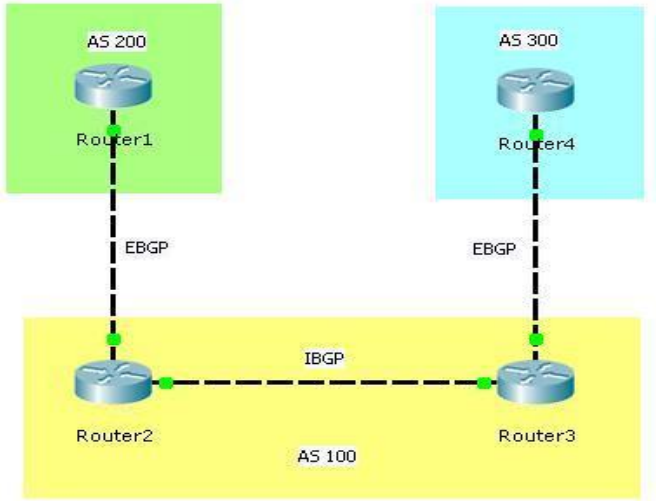
- **OPEN MESSAGE** - pakiet, który jest wymieniany pomiędzy routerami od razu po ustanowieniu sesji TCP. Zawiera podstawowe informacje, które są potrzebne do ustawienia połączenia.
- **UPDATE MESSAGE** - pakiet, który jest najczęściej wymieniany. Znajdują się w nim informacje o dodawanych lub usuwanych trasach i ich parametry

[6] RIPE – (fr. Réseaux IP Européens) Europejska Sieć IP stowarzyszenie zajmujące się rozwojem internetu. Zadaniem stowarzyszenia jest administracyjna i techniczna koordynacja zadań i prac związanych z rozwojem i utrzymaniem Internetu w Europie (www.ripe.net). [15]

- **NOTIFICATION MESSAGE –** pakiet ten wysyłany jest w razie wystąpienia jakiegoś błędu. Wysłanie takiego komunikatu skutkuje przerwaniem połączenia..
- **KEEPALIVE MESSAGE** –pakiety te podtrzymują sesję po jej zestawieniu. Routery za pomocą tych pakietów informują, że połączenie jest wciąż aktywne. Polega to na tym, że co 60 sekund przesyłany jest pakiet wielkości 19 bajtów. Jeżeli router otrzyma pakiet **UPDATE MESSAGE** to nie jest konieczne wysyłanie pakietu **KEEPALIVE MESSAGE** przez dany router.

Protokół BGP możemy podzielić na:

- eBGP (ang. exterior), gdy mamy sesję między dwoma różnymi AS. To właśnie takie połączenia wymieniają informacje pomiędzy przylegającymi do siebie sieciami i dzięki eBGP każda z tych sieci wie jak dotrzeć do dowolnego zakresu adresów rozgłaszanych w internecie W tym przypadku dystans administracyjny wynosi 20.
- iBGP (ang. interior), gdy sesja BGP nawiązana jest między dwoma takimi samymi AS. W tym wypadku dystans administracyjny wynosi 200.



Rysunek nr 17. Ilustracja IBGP oraz EBGP [opracowanie własne]

Protokół BGP nie korzysta przy wyborze najlepszej trasy z metryk technicznych, lecz wykorzystuje parametry administracyjne, zwane atrybutami. Atrybuty są związane z konkretną siecią IP i przesyłane razem z informacją o niej. Rozróżnia się następujące kategorie atrybutów BGP:

- well-known mandatory – muszą być rozpoznawane przez wszystkie implementacje protokołu (well-known) oraz muszą towarzyszyć każdej rozgłaszanej trasie (mandatory);

- well-known discretionary – są rozpoznawane przez wszystkie implementacje protokołu, ale nie muszą być przesyłane razem z ogłaszaną trasą (discretionary).
- optional transitive – nie muszą być rozpoznawane przez implementację (optional), ale jeśli towarzyszą ogłaszanej trasie są wraz z nią przekazywane do innych ruterów.
- optional non-transitive – ani nie muszą być rozpoznawane przez implementację, ani też przekazane do innych ruterów (non-transitive).

[4]

1.3.6 Redystrybucja

Redystrybucja (współużytkowanie) zachodzi wtedy, gdy przy wymianie pakietów do różnych sieci istnieje kilka różnych protokołów w tych sieciach i zachodzi konieczność wymiany między sobą informacji.

Jeśli na przykład dwie firmy łączą się, przy czym w jednej firmie jest wdrożona sieć wykorzystująca protokół EIGRP, a w drugiej sieć jest oparta na protokole RIP, to na routerach brzegowych tych sieci muszą być skonfigurowane oba protokoły routingu.

Obsługa wielu protokołów routingu na jednym routerze nie jest wystarczająca do wymiany informacji pomiędzy nimi. Aby routery przesyłały informacje między sobą muszą być w tym celu odpowiednio skonfigurowane.

Wyróżniamy dwa rodzaje redystrybucji:

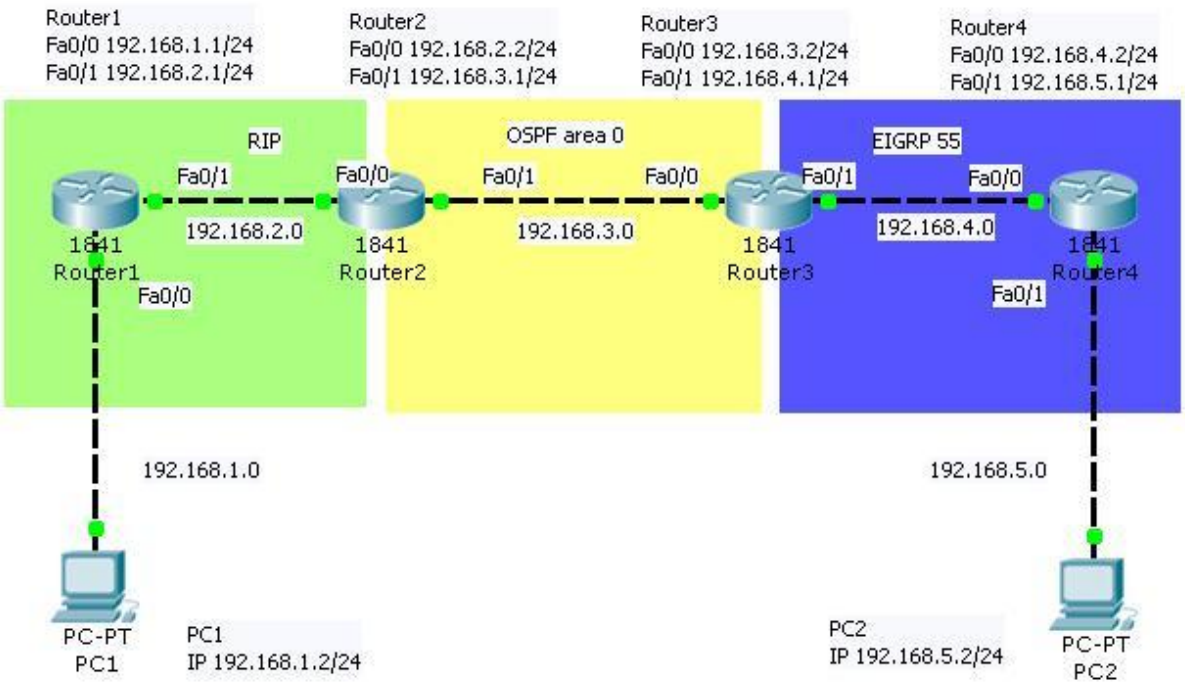
- jednokierunkową, w której tylko jeden z protokołów eksportuje trasy, a drugi je importuje,
- dwukierunkową, gdy każdy protokół jest zarówno eksporterem, jak i importerem informacji o trasach.

Proces redystrybucji składa się z określenia źródła informacji trasowania, które mają być dystrybuowane, z protokołu trasowania, do którego informacja ma być redystrybuowana, oraz sposobu konwersji metryki podczas przesyłania informacji. Często informacje są przesyłane jednokierunkowo i jest to celowe i traktowane jako jeden z elementów zabezpieczenia sieci.

Z redystrybucji należy korzystać ostrożnie, gdyż nieumiejętne jej użycie może powodować powstanie pętli w trasach.

[4]

Przykładowa konfiguracja redystrybucji przedstawiona poniżej wykonana jest za pomocą oprogramowania Cisco Packet Tracert. Plik jest dołączony na płycie CD w katalogu „Lab” – nazwa pliku „redystrybucja.pkt”



Rysunek nr 18 . Przykładowa sieć do przedstawiająca redystrybucję [opracowanie własne]

Podstawowa konfiguracja redystrybucji w sieci przedstawionej na rysunku nr 18.

Przedstawiono także wynik polecenia *show ip protocols* aby przedstawić protokoły routingu na każdym z routerów.

Router 1

```
Router1(config)#router rip
Router1(config-router)#network 192.168.1.0
Router1(config-router)#network 192.168.2.0
Router1(config-router)#redistribute ospf 100 metric 10
Router1(config)#router ospf 100
Router1(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 9 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip, ospf 100
Default version control: send version 1, receive any version
  Interface         Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0   1     2 1
  FastEthernet0/1   1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        192.168.1.0
        192.168.2.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
        192.168.2.2          120      00:00:03
```

```
Distance: (default is 120)
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.2.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          110      00:20:09
  Distance: (default is 110)
```

Router 2

```
Router2(config)#router ospf 100
Router2(config-router)#redistribute rip metric 100000 subnets
Router2(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router2(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router2(config)#router rip
Router2(config-router)# redistribute ospf 100 metric 10
Router2(config-router)#network 192.168.2.0
Router2(config-router)# network 192.168.3.0
```

```
Router2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 2 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip, ospf 100
  Default version control: send version 1, receive any version
    Interface          Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0    1     2 1
    FastEthernet0/1    1     2 1
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
  Passive Interface(s):
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1          120      00:00:00
  Distance: (default is 120)
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.3.1
  Redistributing External Routes from,
    rip
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1          110      00:04:23
    192.168.3.2          110      00:04:22
  Distance: (default is 110)
```

Router 3

```
Router3(config)# router eigrp 55
Router3(config-router)# redistribute ospf 100 metric 100000 100000 100 100 55
Router3(config-router)# network 192.168.3.0
Router3(config-router)# network 192.168.4.0
Router3(config)# router ospf 100
Router3(config-router)# redistribute eigrp 55 subnets
Router3(config-router)# network 192.168.3.0 0.0.0.255 area 0
Router3(config-router)# network 192.168.4.0 0.0.0.255 area 0
```

```
Router3#show ip protocols
Routing Protocol is "eigrp  55 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum  hopcount 100
  EIGRP maximum  metric variance 1
Redistributing: eigrp 55, ospf 100
  Automatic network summarization  is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    192.168.3.0
    192.168.4.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.4.2     90            4
  Distance: internal 90 external 170
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.4.1
Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.3.0 0.0.0.255 area 0
    192.168.4.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.3.1         110       00:14:13
  Distance: (default is 110)
```

Router 4

```
Router4(config)# router eigrp 55
Router4(config-router)# network 192.168.4.0
Router4(config-router)# network 192.168.5.0
Router4#show ip protocols
Routing Protocol is "eigrp  55 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum  hopcount 100
  EIGRP maximum  metric variance 1
```

```
Router4(config)# router eigrp 55
Router4(config-router)# network 192.168.4.0
Router4(config-router)# network 192.168.5.0
Router4#show ip protocols
Routing Protocol is "eigrp  55 "
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 EIGRP maximum  hopcount 100
 EIGRP maximum  metric variance 1
Redistributing: eigrp 55
 Automatic network summarization  is in effect
 Automatic address summarization:
 Maximum path: 4
 Routing for Networks:
   192.168.4.0
   192.168.5.0
 Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.4.1     90            6
 Distance: internal 90 external 170
```

Rozdział II – Opis części praktycznej

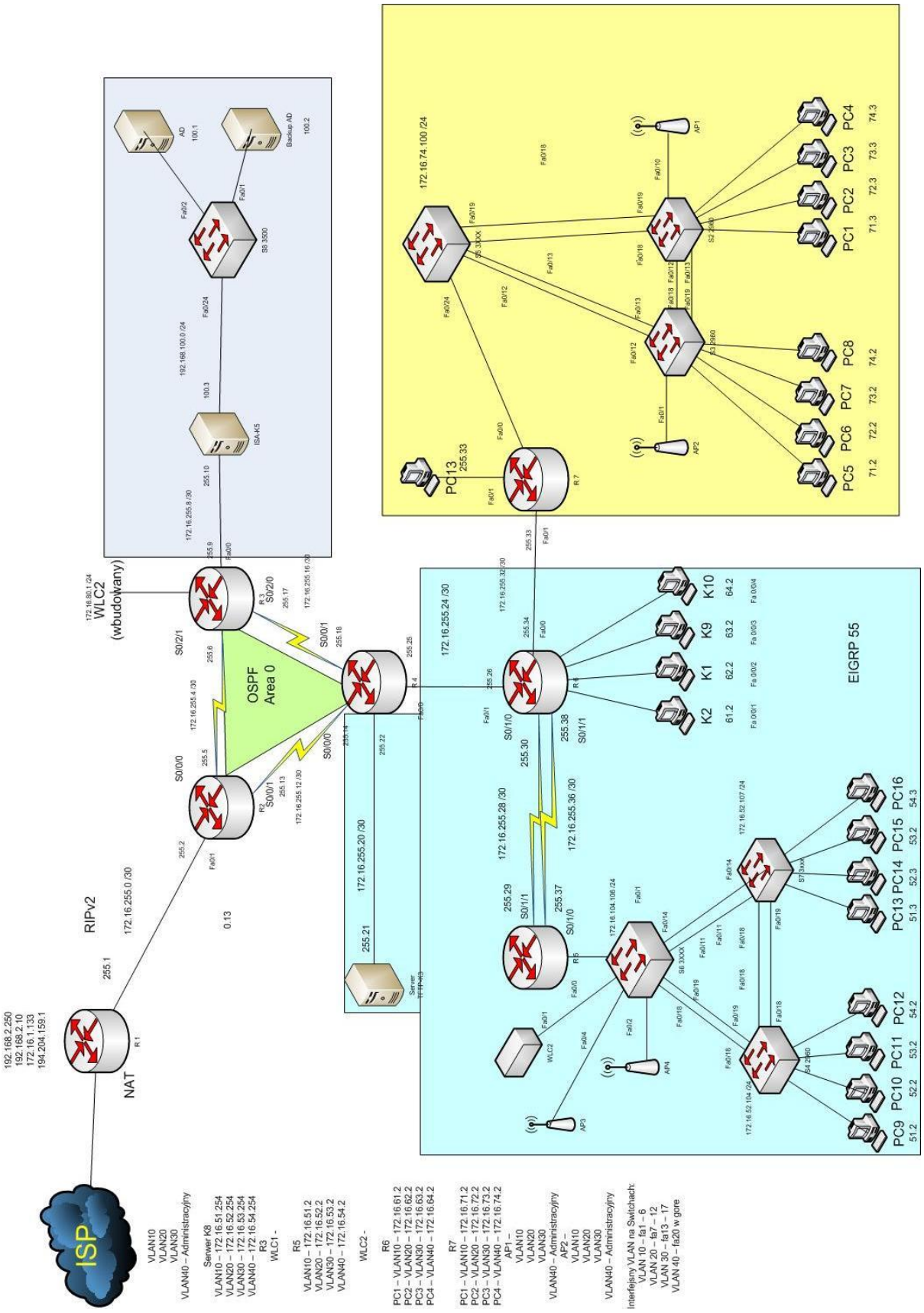
2.1 Opis i schemat wykonanej sieci

Do wykonania sieci został użyty sprzęt firmy CISCO. Wykorzystano siedem routerów (oznaczonych w dalszej części pracy jako R1, R2, R3, R4, R5, R6, R7) oraz siedem switch-y (oznaczonych jako S2, S3, S4, S5, S6, S7, S8). Aby sieć bardziej urozmaicić wprowadzono jeszcze kontrolery sieci bezprzewodowej oraz accesspointy Cisco.

Wykaz sprzętu przedstawia tabela nr 1

Lp.	Nazwa na schemacie	Nazwa i symbol urządzenia	Uwagi
1.	R1	CISCO ROUTER 2800 series (2811)	Specyfikacja w załączniku nr 1
2.	R2		
3.	R3		
4.	R4		
5.	R5	CISCO ROUTER 1800 series (1841)	Specyfikacja w załączniku nr 2
6.	R6		
7.	R7		
8.	S2	CISCO SWITCH 2960 catalyst	Specyfikacja w załączniku nr 3
9.	S3		
10.	S4		
11.	S5	CISCO SWITCH 3560 catalyst	Specyfikacja w załączniku nr 4
12.	S6		
13.	S7		
14.	S8		

Tabela nr 1. Routery i switche użyte do budowy sieci [opracowanie własne]



Rysunek nr 19. Schemat sieci [opracowanie własne]

Po właściwym podłączeniu wszystkich urządzeń przy pomocy odpowiedniego okablowania w celu sprawdzenia poprawności funkcjonowania całej sieci w środowisku laboratoryjnym konieczne było odpowiednie skonfigurowanie każdego urządzenia. W tym celu trzeba skonfigurować wszystkie urządzenia w jednym protokole routingu np. OSPF area 0 aby wykluczyć błędy połączeń między urządzeniami. Po sprawdzeniu działania jednego protokołu w całej sieci trzeba przystąpić do konfiguracji poszczególnych elementów sieci według następujących założeń:

- Router R1 w sieci pełni rolę routera brzegowego przypinającego całość do zewnętrznej sieci. Na tym routerze skonfigurowany jest także serwer DHCP[7], który pozwala przydzielić adresy IP dla hostów sieci bezprzewodowej.
- Routery R2, R3, R4 stanowią rdzeń sieci (OSPF).
- Router R2 ma za zadanie redystrybuować w dwie strony protokół RIPv2 i protokół OSPF.
- Router R3 nie ma żadnej zdefiniowanej statycznej trasy.
- Router R4 - zadaniem tego routera jest redystrybucja protokołu OSPF i protokołu EIGRP.
- Router R5 i R6 funkcjonuje tylko w protokole EIGRP.
- Router 6 ma za zadanie redystrybucję tras EIGRP i tras statycznych a także wysyłanie ich do routera R7.
- Do routera R5 przypięte są switch-e S4, S6, S7, na których uruchomione są VLAN-y: 10; 20; 30; 40.
- VLAN 40 jest VLAN-em natywnym (VLAN natywny to VLAN, w którym port trunkowany "rozumie" ramki nietagowane).
- Router R5 dzięki access control list-om dzieli ruch w taki sposób aby pomiędzy VLAN-ami był niemożliwy z wyjątkiem VLAN-u 40, który jest VLAN-em administracyjnym i gdzie ten ruch jest dozwolony.
- Identyczna konfiguracja jest na switch-ach S5, S6, S7, które podłączone są do routera R7.

W naszą sieć wpięty jest kontroler sieci bezprzewodowej, który jest podłączony do routera 6. Do tego kontrolera podłączone są 4 accesspoint-y (na schemacie oznaczone jako AP1 AP2, AP3, AP4).

[7] DHCP - (ang. Dynamic Host Configuration Protocol) protokół komunikacyjny, który umożliwia urządzeniom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci. Protokół DHCP jest zdefiniowany w RFC 2131

Accesspoint-y podłączone są w różnych punktach sieci (AP1 do switch-a S2, AP2 do switch-a S3 a AP3, AP4 do switch-a S6). Accesspoint-y pobierają adresy IP z serwera DHCP skonfigurowanego na routerze R1.

W naszej sieci znajduje się także niewielki serwer TFTP, którego zadaniem jest przechowywanie plików konfiguracyjnych wszystkich routerów i switch-y.

2.2 Adresacja

Sieć została podzielona na kilka podsieci i przydzielono adresy prywatne klasy B (zakres klasy B 172.16.0.0 – 172.31.255.255). Wybrana klasa adresów pozwalała zaadresować całą naszą sieć i zostawić jeszcze zapas w razie przyszłościowej rozbudowy. Dążono do wykorzystania jak najlepiej pulę adresów więc na poszczególne połączenia pomiędzy routerami tzw. punkt - punkt adresowano z maska 30 bitową. Pozostałe adresowano z maską 24 bitową.

Adres interfejsu S/0/0 na routerze R1 192.168.2.250/24 jest adresem sieci zewnętrznej (WAN).

Interfejs	Adres IP
Router R1	
S0/0/0	192.168.2.250/24
Fa 0/0	172.16.255.1/30
Router R2	
Fa 0/1	176.16.255.2/30
S0/0/0	172.16.255.5/30
S0/0/1	172.16.255.13/30
Router R3	
Fa 0/0	176.16.255.9/30
S0/2/0	172.16.255.17/30
S0/2/1	172.16.255.6/30
Router R4	
S0/0/0	176.16.255.14/30
S0/0/1	172.16.255.18/30
Fa 0/0	172.16.255.25/30

Fa 0/1	172.16.255.22/30
Router R5	
S0/1/1	176.16.255.29/30
S0/1/0	172.16.255.37/30
Fa 0/0.10	172.16.51.1/24
Fa 0/0.20	172.16.52.1/24
Fa 0/0.30	172.16.53.1/24
Fa 0/0.40	172.16.54.1/24
Router R6	
S0/1/0	176.16.255.30/30
S0/1/1	172.16.255.38/30
Fa 0/0	172.16.255.34/30
Fa 0/1	172.16.255.26/30
Hosty podłączone do routera R6	
K1 Vlan 10	172.16.61.1/24
K2 Vlan 20	172.16.62.1/24
K3 Vlan 30	172.16.63.1/24
K4 Vlan 40	172.16.64.1/24
Router R7	
Fa 0/1	172.16.255.33/30
Fa 0/0.10	172.16.71.1/24
Fa 0/0.20	172.16.72.1/24
Fa 0/0.30	172.16.73.1/24
Fa 0/0.40	172.16.74.1/24
Hosty podłączone do switch-a S2	
PC1 Vlan 10	172.16.71.3/24
PC2 Vlan 20	172.16.72.3/24
PC3 Vlan 30	172.16.73.3/24
PC4 Vlan 40	172.16.74.3/24
Hosty podłączone do switch-a S3	
PC5 Vlan 10	172.16.71.2/24
PC6 Vlan 20	172.16.72.2/24
PC7 Vlan 30	172.16.73.2/24

PC8 Vlan 40	172.16.74.2/24
Hosty podłączone do switch-a S4	
PC9 Vlan 10	172.16.51.2/24
PC10 Vlan 20	172.16.52.2/24
PC11 Vlan 30	172.16.53.2/24
PC12 Vlan 40	172.16.54.2/24
Hosty podłączone do switch-a S7	
PC13 Vlan 10	172.16.51.3/24
PC14 Vlan 20	172.16.52.3/24
PC15 Vlan 30	172.16.53.3/24
PC16 Vlan 40	172.16.53.4/24
Serwer 1	172.16.255.21/30

Tabela nr 2. Adresacja urządzeń [opracowanie własne]

2.3 Opis konfiguracji sprzętu

2.3.1 Router R1

Router R1 jest routerem brzegowym całej sieci i spoczywa na nim bardzo ważna rola odpowiedniego odseparowania naszej sieci od sieci zewnętrznej. Dlatego przez odpowiednią konfigurację oraz stworzenie właściwie skonfigurowanych list dostępu ACL musimy zapewnić jak najwięcej bezpieczeństwa.

Na tym routerze skonfigurowany jest także odpowiednio serwer DHCP dla całej sieci. Ustawiena serwera DHCP pozwalają na przydzielenie dla każdej podsieci adresów z zakresu 1 do 110. Ilość ta pozwoli nam w przyszłosci w razie potrzeby dodania dodatkowego sprzętu bez konieczności zmiany adresacji całej sieci.

Przypisano dla każdej podsieci domyślną bramę i zastosowano ustawienia NAT .

Na interfejsach tego routera zastosowano blokadę protokołu CDP[8] aby nie można było uzyskać wiadomości o tym routerze.

[8] CDP- Protokół firmy CISCO umożliwiający identyfikowanie urządzeń oraz wymienianie danych identyfikacyjnych

Opis części pliku konfiguracyjnego routera R1 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 5).

```
no ip dhcp use vrf connected
ip dhcp excluded-address 172.16.54.1 172.16.54.110
ip dhcp excluded-address 172.16.51.1 172.16.51.110
ip dhcp excluded-address 172.16.52.1 172.16.52.110
ip dhcp excluded-address 172.16.53.1 172.16.53.110
ip dhcp excluded-address 172.16.61.1 172.16.61.110
ip dhcp excluded-address 172.16.62.1 172.16.62.110
ip dhcp excluded-address 172.16.63.1 172.16.63.110
ip dhcp excluded-address 172.16.64.1 172.16.64.110
ip dhcp excluded-address 172.16.71.1 172.16.71.110
ip dhcp excluded-address 172.16.72.1 172.16.72.110
ip dhcp excluded-address 172.16.73.1 172.16.73.110
ip dhcp excluded-address 172.16.74.1 172.16.74.110
ip dhcp excluded-address 172.16.80.1 172.16.80.110
```

Powyższe listingi definiują jakie adresy z poszczególnych podsieci powinny być wykluczone przez serwer DHCP. Zapobiega to brakowi adresów do późniejszej rozbudowy całej sieci.

```
ip dhcp pool Main
   network 172.16.0.0 255.255.0.0
   domain-name cisco.swspiz.pl
   dns-server 91.189.0.2
!
ip dhcp pool 172.16.51.0/24
   network 172.16.51.0 255.255.255.0
   default-router 172.16.51.1
!
ip dhcp pool 172.16.52.0/24
   network 172.16.52.0 255.255.255.0
   default-router 172.16.52.1
!
ip dhcp pool 172.16.53.0/24
   network 172.16.53.0 255.255.255.0
   default-router 172.16.53.1
!
ip dhcp pool 172.16.54.0/24
   network 172.16.54.0 255.255.255.0
   default-router 172.16.54.1
!
ip dhcp pool 172.16.61.0/24
   network 172.16.61.0 255.255.255.0
   default-router 172.16.61.1
!
ip dhcp pool 172.16.62.0/24
   network 172.16.62.0 255.255.255.0
   default-router 172.16.62.1
!
ip dhcp pool 172.16.63.0/24
   network 172.16.63.0 255.255.255.0
   default-router 172.16.63.1
!
ip dhcp pool 172.16.64.0/24
   network 172.16.64.0 255.255.255.0
   default-router 172.16.64.1
!
ip dhcp pool 172.16.71.0/24
   network 172.16.71.0 255.255.255.0
   default-router 172.16.71.1
```

```
ip dhcp pool 172.16.72.0/24
   network 172.16.72.0 255.255.255.0
   default-router 172.16.72.1
!
ip dhcp pool 172.16.73.0/24
   network 172.16.73.0 255.255.255.0
   default-router 172.16.73.1
!
ip dhcp pool 172.16.74.0/24
   network 172.16.74.0 255.255.255.0
   default-router 172.16.74.1
!
ip dhcp pool 172.16.80.0/24
   network 172.16.80.0 255.255.255.0
   default-router 172.16.80.1
```

Listingi powyżej odpowiadają za przydzielenie adresów za pomocą DHCP dla każdej podsieci oraz za odpowiednie utworzenie domyślnej bramy dla poszczególnych podsieci.

```
interface FastEthernet0/0
 ip address 172.16.255.1 255.255.255.252
 ip access-group 100 out
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 ip address 192.168.2.250 255.255.255.0
 ip access-group 101 in
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
```

Część pliku konfiguracyjnego odpowiedzialna za odpowiednią konfigurację poszczególnych interfejsów routera R1. Widać tu, że na interfejsach *FastEthernet0/0* i *FastEthernet0/1* włączono blokadę protokołu CDP celem nierozpowszechniania informacji o tym routerze.

```
router rip
 version 2
 redistribute static
 passive-interface FastEthernet0/1
 network 172.16.0.0
 distribute-list 99 in FastEthernet0/1
```

Listingi części pliku konfiguracyjnego odpowiedzialne za konfigurację protokołu RIP w wersji 2 oraz redystrybucję tras statycznych. Interfejs *FastEthernet0/1* jest interfejsem pasywnym i może być za jego pośrednictwem dystrybuowany ruch tylko na podstawie odpowiednio skonfigurowanych ACL, których to ustawienia są podane na listingach poniżej.

```
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.2.10
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 50 interface FastEthernet0/1 overload
ip nat inside source static 172.16.255.21 192.168.2.249
!
ip access-list extended VLAN10
 evaluate Z40TRAFFIC
 permit ip any 172.16.51.0 0.0.0.255
 permit ip any 172.16.61.0 0.0.0.255
 permit ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.0.0 0.0.255.255
 permit ip any any
ip access-list extended VLAN20
 evaluate Z40TRAFFIC
 permit ip any 172.16.52.0 0.0.0.255
 permit ip any 172.16.62.0 0.0.0.255
 permit ip any 172.16.72.0 0.0.0.255
 deny   ip any any
ip access-list extended VLAN30
 evaluate Z40TRAFFIC
 deny   ip any 172.16.51.0 0.0.0.255
 deny   ip any 172.16.61.0 0.0.0.255
 deny   ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.52.0 0.0.0.255
 deny   ip any 172.16.62.0 0.0.0.255
 deny   ip any 172.16.72.0 0.0.0.255
 deny   ip any 172.16.54.0 0.0.0.255
 deny   ip any 172.16.64.0 0.0.0.255
 deny   ip any 172.16.74.0 0.0.0.255
 permit ip any any
ip access-list extended VLAN40
 permit ip any any reflect Z40TRAFFIC
!
access-list 20 remark dostep do http/https
access-list 20 permit 192.168.2.112
access-list 20 deny   any
access-list 50 permit 172.16.0.0 0.0.255.255
access-list 99 deny   any
access-list 100 permit tcp any any
access-list 100 permit tcp any any established
access-list 100 permit icmp any any
access-list 100 permit udp any any
access-list 100 deny   ip any any
access-list 115 deny   ip any 192.0.0.0 35.255.255.255
access-list 115 deny   ip any 192.168.2.0 0.0.0.255
access-list 115 permit ip any any
no cdp run
```

2.3.2 Router R2

Router R2 jest jednym z trzech routerów, które tworzą rdzeń naszej sieci. Urządzenie to jest pierwszym urządzeniem, które musi pogodzić dwa protokoły routingu – protokół RIP2, który jest na interfejsie *FastEthernet 0/1* z protokołem OSPF skonfigurowanym na interfejsie *Serial0/0/0* i *Serial0/0/1*.
Poprzez odpowiednią konfigurację uzyskano redystrybucję protokołów w dwie strony.

Opis części pliku konfiguracyjnego routera R2 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 6).

```
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.255.2 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.255.5 255.255.255.252
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 ip address 172.16.255.13 255.255.255.252
 clock rate 2000000
```

Powyżej wpisy w konfiguracji routera odpowiadające za odpowiednie zaadresowanie poszczególnych interfejsów oraz przydzielenie odpowiedniej częstotliwości zegara dla połączeń sprzętowych przy wykorzystaniu interfejsów szeregowych

```
router ospf 1
 log-adjacency-changes
 network 172.16.255.0 0.0.0.3 area 0
 network 172.16.255.4 0.0.0.3 area 0
 network 172.16.255.12 0.0.0.3 area 0
 default-information originate
```

Wpisy odpowiadające za odpowiednie skonfigurowanie protokołu OSPF w obszarze 0. Została także włączona informacja o rozpowszechnianiu trasy domyślnej (*default-information originate*).

```
router rip
 version 2
 redistribute ospf 1 metric 1
 network 172.16.0.0
```

Wpis odpowiadający za redystrybucje protokołu RIP w wersji 2 do do protokołu OSPF. *Redistribute ospf 1 metric 1* wpis ten mówi nam także o metryce z jaką trasy OSPF będą rozgłaszane do protokołu RIP.

2.3.3 Router R3

Router R3 jest następnym routerem tworzącym nasz rdzeń sieci, który jest w całości oparty na protokole OSPF area 0.

Opis części pliku konfiguracyjnego routera R2 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 7).

```
interface FastEthernet0/0
 ip address 172.16.255.9 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2/0
 ip address 172.16.255.17 255.255.255.252
 clock rate 2000000
!
interface Serial0/2/1
 ip address 172.16.255.6 255.255.255.252
!
interface Integrated-Service-Engine1/0
 ip address 172.16.80.1 255.255.255.0
 ip helper-address 172.16.255.1
 no keepalive
```

Ustawienia poszczególnych interfejsów routera. Do tego routera podłączony jest kontroler sieci bezprzewodowej, pozwala na podłączenie komputerów mobilnych i pobranie adreu z DHCP (*ip helper-address 172.16.255.1*).

```
router ospf 1
 log-adjacency-changes
 network 172.16.80.0 0.0.0.255 area 0
 network 172.16.255.4 0.0.0.3 area 0
 network 172.16.255.8 0.0.0.3 area 0
 network 172.16.255.16 0.0.0.3 area 0
```

Wpisy odpowiadające za konfigurację protokołu OSPF na tym routerze.

2.3.4 Router R4

To kolejny router tworzący nasz rdzeń sieci. Zastosowano tu konfiguracje, która pozwala pogodzić dwa protokoły routingu OSPF (który jest protokołem wnętrza naszej sieci) a protokołem EIGRP co uzyskano poprzez redystrybucję w obie strony.
Do tego routera przypięty jest na interfejsie *FastEthernet0/1* serwer TFTP, którego zadaniem w tym środowisku laboratoryjnym jest przechowywanie plików konfiguracyjnych urządzeń.

Opis części pliku konfiguracyjnego routera R4 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 8).

```
interface FastEthernet0/0
 ip address 172.16.255.25 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.255.22 255.255.255.252
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 ip address 172.16.255.14 255.255.255.252
 no fair-queue
!
interface Serial0/0/1
 ip address 172.16.255.18 255.255.255.252
```

Wpisy konfiguracji routera odpowiadające za odpowiednie zaadresowanie poszczególnych interfejsów oraz przydzielenie odpowiedniej częstotliwości zegara dla połączeń sprzętowych przy wykorzystaniu interfejsów szeregowych. Na interfejsie *FastEthernet0/1* włączono blokadę protokołu CDP w celu nie rozpowszechniania informacji o tym routerze.

```
router eigrp 55
 redistribute connected
 redistribute ospf 1 metric 100000 1000 255 1 1500
 passive-interface FastEthernet0/1
 network 172.16.255.24 0.0.0.3
 no auto-summary
```

Wpisy powyższe odpowiadają za prawidłowe ustawienia protokołu EIGRP.
Redistribute connected oznacza redystrybuowanie wszystkich sieci przypiętych do tego routera.
Redistribute ospf 1 metric 100000 1000 255 1 1500 oznacza redystrybuowanie wszystkich sieci z OSPF 1 dla podanych metryk.

Passive-interface FastEthernet0/1 oznacza ze na podanym interfejsie została zablokowana możliwość wysyłania informacji o EIGRP.

No auto-summary oznacza, że została wyłączona autosumaryzacja.

```
router ospf 1
 log-adjacency-changes
 redistribute eigrp 55 subnets
 passive-interface FastEthernet0/1
 network 172.16.255.12 0.0.0.3 area 0
 network 172.16.255.16 0.0.0.3 area 0
 network 172.16.255.20 0.0.0.3 area 0
 default-information originate
```

Wpisy powyżej odpowiadają za prawidłową konfigurację protokołów oraz za redystrybucję OSPF.

Redistribute eigrp 55 subnets oznacza redystrybucje protokołu EIGRP z podsieciami.

Passive-interface FastEthernet0/1 oznacza ze na podanym interfejsie została zablokowana możliwość wysyłania informacji o OSPF.

Default-information originate oznacza że włączono rozgłaszanie trasy domyślnej

2.3.5 Router R5

Router R5 pracuje w protokole EIGRP. Opis części pliku konfiguracyjnego routera R2 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 9).

Charakterystyczną cechą konfiguracji tego routera jest, to że interfejs *FastEthernet0/0* nie ma skonfigurowanego osobnego adresu IP, ponieważ jest podzielony na kilka podinterfejsów odpowiadających odpowiednim v-lanom ze *enkapsulacją dot1q*.

Ruch na tym routerze dzięki zastosowaniu odpowiednio skonfigurowanych list dostępu ACL jest podzielony w taki sposób aby zapobiec ruchowi między tymi vlanami. Wyjątkiem jest VLAN 40, który jest vlanem natywnym do zarządzania.

```
interface FastEthernet0/0
 no ip address
 ip helper-address 172.16.255.1
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.51.1 255.255.255.0
 ip access-group VLAN10 in
 ip helper-address 172.16.255.1
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.52.1 255.255.255.0
 ip access-group VLAN20 in
```

```
 ip helper-address 172.16.255.1
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.53.1 255.255.255.0
 ip access-group VLAN30 in
 ip helper-address 172.16.255.1
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40 native
 ip address 172.16.54.1 255.255.255.0
 ip access-group VLAN40 in
 ip helper-address 172.16.255.1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface Serial0/1/0
 ip address 172.16.255.37 255.255.255.252
 clock rate 2000000
!
interface Serial0/1/1
 ip address 172.16.255.29 255.255.255.252
 clock rate 2000000
!
interface Vlan1
 no ip address
!
interface Vlan40
 no ip address
```

Powyższe wpisy odpowiadają za konfigurację poszczególnych interfejsów routera. Interfejsy *Serial0/1/0* i *Serial0/1/1* pełnią rolę redudantnego połączenia z routerem R6.

```
router eigrp 55
 passive-interface FastEthernet0/0
 network 172.16.51.0 0.0.0.255
 network 172.16.52.0 0.0.0.255
 network 172.16.53.0 0.0.0.255
 network 172.16.54.0 0.0.0.255
 network 172.16.255.28 0.0.0.3
 network 172.16.255.36 0.0.0.3
 auto-summary
```

Listingi odpowiedzialne za poprawną konfigurację protokołu EIGRP na tym routerze. *Passive-interface FastEthernet0/0* oznacza ze na podanym interfejsie została zablokowana możliwość wysyłania informacji o EIGRP.

Auto-summary oznacza, że została włączona autosumaryzacja.

Wpisy poniżej odpowiadają za odpowiednie skierowanie ruch na poszczególne VLAN-y (w tym separacja pomiędzy VLAN-mi za pomocą odpowiednich ACL).

```
ip access-list extended VLAN10
 evaluate Z40TRAFFIC
 permit ip any 172.16.51.0 0.0.0.255
 permit ip any 172.16.61.0 0.0.0.255
 permit ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.0.0 0.0.255.255
 permit ip any any
ip access-list extended VLAN20
 evaluate Z40TRAFFIC
 permit ip any 172.16.52.0 0.0.0.255
 permit ip any 172.16.62.0 0.0.0.255
 permit ip any 172.16.72.0 0.0.0.255
 deny   ip any any
ip access-list extended VLAN30
 evaluate Z40TRAFFIC
 deny   ip any 172.16.51.0 0.0.0.255
 deny   ip any 172.16.61.0 0.0.0.255
 deny   ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.52.0 0.0.0.255
 deny   ip any 172.16.62.0 0.0.0.255
 deny   ip any 172.16.72.0 0.0.0.255
 deny   ip any 172.16.54.0 0.0.0.255
 deny   ip any 172.16.64.0 0.0.0.255
 deny   ip any 172.16.74.0 0.0.0.255
 permit ip any any
ip access-list extended VLAN40
 permit ip any any reflect Z40TRAFFIC
!
access-list 110 permit ip any 172.16.51.0 0.0.0.255
access-list 110 permit ip any 172.16.61.0 0.0.0.255
access-list 110 permit ip any 172.16.71.0 0.0.0.255
access-list 110 deny   ip any 172.16.0.0 0.0.255.255
access-list 110 permit ip any any
access-list 120 permit ip any 172.16.52.0 0.0.0.255
access-list 120 permit ip any 172.16.62.0 0.0.0.255
access-list 120 permit ip any 172.16.72.0 0.0.0.255
access-list 120 deny   ip any any
access-list 130 deny   ip any 172.16.51.0 0.0.0.255
access-list 130 deny   ip any 172.16.61.0 0.0.0.255
access-list 130 deny   ip any 172.16.71.0 0.0.0.255
access-list 130 deny   ip any 172.16.52.0 0.0.0.255
access-list 130 deny   ip any 172.16.62.0 0.0.0.255
access-list 130 deny   ip any 172.16.72.0 0.0.0.255
access-list 130 deny   ip any 172.16.54.0 0.0.0.255
access-list 130 deny   ip any 172.16.64.0 0.0.0.255
access-list 130 deny   ip any 172.16.74.0 0.0.0.255
access-list 130 permit ip any any
```

2.3.6 Router R6

Router 6 skonfigurowany jest tak, aby pogodzić funkcjonowanie dwóch protokołów routingu a mianowicie protokół EIGRP oraz routing statyczny. Tutaj skonfigurowane są wszystkie trasy statyczne biegnące w kierunku routera R7.

Opis części pliku konfiguracyjnego routera R7 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 10).

```
interface FastEthernet0/0
 ip address 172.16.255.34 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.255.26 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 switchport access vlan 10
 no cdp enable
 spanning-tree portfast
!
interface FastEthernet0/0/1
 switchport access vlan 20
 no cdp enable
 spanning-tree portfast
!
interface FastEthernet0/0/2
 switchport access vlan 30
 no cdp enable
 spanning-tree portfast
!
interface FastEthernet0/0/3
 switchport access vlan 40
 no cdp enable
 spanning-tree portfast
```

Na interfejsach FastEthernet0/0/0, FastEthernet0/0/1, FastEthernet0/0/2, FastEthernet0/0/3 włączona jest blokada protokołu CDP aby nie wypuszczać informacji o routerach z sieci.

```
interface Serial0/1/0
 ip address 172.16.255.30 255.255.255.252
 no fair-queue
!
interface Serial0/1/1
 ip address 172.16.255.38 255.255.255.252
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 172.16.61.1 255.255.255.0
 ip access-group VLAN10 in
 ip helper-address 172.16.255.1
!
```

```
interface Vlan20
 ip address 172.16.62.1 255.255.255.0
 ip access-group VLAN20 in
 ip helper-address 172.16.255.1
!
interface Vlan30
 ip address 172.16.63.1 255.255.255.0
 ip access-group VLAN30 in
 ip helper-address 172.16.255.1
!
interface Vlan40
 ip address 172.16.64.1 255.255.255.0
 ip access-group VLAN40 in
 ip helper-address 172.16.255.1
```

Wpisy odpowiadające za konfigurację poszczególnych interfejsów

```
router eigrp 55
 redistribute connected
 redistribute static
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/0/0
 passive-interface FastEthernet0/0/1
 passive-interface FastEthernet0/0/2
 passive-interface FastEthernet0/0/3
 network 172.16.255.24 0.0.0.3
 network 172.16.255.28 0.0.0.3
 network 172.16.255.32 0.0.0.3
 network 172.16.255.36 0.0.0.3
 no auto-summary
```

Wpisy odpowiadające za odpowiednie skonfigurowanie protokołu EIGRP.

Redistribute connected oznacza redystrybuowanie wszystkich sieci przypiętych do tego routera.

Redistribute static oznacz redystrybucję tras statycznych

Passive-interface FastEthernet0/0, FastEthernet0/0/0, FastEthernet0/0/1, FastEthernet0/0/2, FastEthernet0/0/3 oznacza że blokowany jest ruch na module switch-owym

No auto-summary wyłączona jest autosumaryzacja.

```
ip forward-protocol nd
ip route 172.16.71.0 255.255.255.0 172.16.255.33
ip route 172.16.72.0 255.255.255.0 172.16.255.33
ip route 172.16.73.0 255.255.255.0 172.16.255.33
ip route 172.16.74.0 255.255.255.0 172.16.255.33
```

Wpisy odpowiedzialne za skonfigurowanie tras w kierunku routera R7

```
ip http server
no ip http secure-server
!
ip access-list extended VLAN10
 evaluate Z40TRAFFIC
 permit ip any 172.16.51.0 0.0.0.255
 permit ip any 172.16.61.0 0.0.0.255
 permit ip any 172.16.71.0 0.0.0.255
```

```
 deny   ip any 172.16.0.0 0.0.255.255
 permit ip any any
ip access-list extended VLAN20
 evaluate Z40TRAFFIC
 permit ip any 172.16.52.0 0.0.0.255
 permit ip any 172.16.62.0 0.0.0.255
 permit ip any 172.16.72.0 0.0.0.255
 deny   ip any any
ip access-list extended VLAN30
 evaluate Z40TRAFFIC
 deny   ip any 172.16.51.0 0.0.0.255
 deny   ip any 172.16.61.0 0.0.0.255
 deny   ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.52.0 0.0.0.255
 deny   ip any 172.16.62.0 0.0.0.255
 deny   ip any 172.16.72.0 0.0.0.255
 deny   ip any 172.16.54.0 0.0.0.255
 deny   ip any 172.16.64.0 0.0.0.255
 deny   ip any 172.16.74.0 0.0.0.255
 permit ip any any
ip access-list extended VLAN40
 permit ip any any reflect Z40TRAFFIC
!
access-list 110 permit ip any 172.16.51.0 0.0.0.255
access-list 110 permit ip any 172.16.61.0 0.0.0.255
access-list 110 permit ip any 172.16.71.0 0.0.0.255
access-list 110 deny   ip any 172.16.0.0 0.0.255.255
access-list 110 permit ip any any
access-list 120 permit ip any 172.16.52.0 0.0.0.255
access-list 120 permit ip any 172.16.62.0 0.0.0.255
access-list 120 permit ip any 172.16.72.0 0.0.0.255
access-list 120 deny   ip any any
access-list 130 deny   ip any 172.16.51.0 0.0.0.255
access-list 130 deny   ip any 172.16.61.0 0.0.0.255
access-list 130 deny   ip any 172.16.71.0 0.0.0.255
access-list 130 deny   ip any 172.16.52.0 0.0.0.255
access-list 130 deny   ip any 172.16.62.0 0.0.0.255
access-list 130 deny   ip any 172.16.72.0 0.0.0.255
access-list 130 deny   ip any 172.16.54.0 0.0.0.255
access-list 130 deny   ip any 172.16.64.0 0.0.0.255
access-list 130 deny   ip any 172.16.74.0 0.0.0.255
access-list 130 permit ip any any
```

2.3.7 Router R7

Router R7 jest ostatnim w naszej sieci routerem, który obsługuje tylko trasy statyczne i są na nim skonfigurowane wszystkie trasy biegnące w kierunku routera R6.

Charakterystyczną cechą konfiguracji tego routera tak jak i routera R5 jest to, że interfejs *FastEthernet0/0* nie ma skonfigurowanego osobnego adresu IP, ponieważ jest podzielony na kilka podinterfejsów odpowiadających odpowiednim v-lanom ze *enkapsulacją dot1q*.

Ruch na tym routerze dzięki zastosowaniu odpowiednio skonfigurowanych list dostępu ACL jest podzielony w taki sposób aby zapobiec ruchowi między tymi vlanami. Wyjątkiem jest VLAN 40, który jest vlanem natywnym do zarządzania.

Opis części pliku konfiguracyjnego routera R2 odpowiadającej za routing (pełny plik konfiguracji w załączniku nr 11).

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.71.1 255.255.255.0
 ip access-group VLAN10 in
 ip helper-address 172.16.255.1
 no cdp enable
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.72.1 255.255.255.0
 ip access-group VLAN20 in
 ip helper-address 172.16.255.1
 no cdp enable
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.73.1 255.255.255.0
 ip access-group VLAN30 in
 ip helper-address 172.16.255.1
 no cdp enable
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40 native
 ip address 172.16.74.1 255.255.255.0
 ip access-group VLAN40 in
 ip helper-address 172.16.255.1
 no cdp enable
!
interface FastEthernet0/1
 ip address 172.16.255.33 255.255.255.252
 ip helper-address 172.16.255.1
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/1/1
 no ip address
 shutdown
```

```
 clock rate 125000
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.255.34
```

Wpis odpowiadający za odpowiednie wyłanie trasy domyślnej na adres 172.16.255.34 czyli w naszym przypadku w kierunku routera R6

```
ip http server
no ip http secure-server
```

Wpisy poniżej odpowiadają za odpowiednie skierowanie ruch na poszczególne VLAN-y (w tym separacja pomiędzy VLAN-mi za pomocą odpowiednich ACL).

```
ip access-list extended VLAN10
 evaluate Z40TRAFFIC
 permit ip any 172.16.51.0 0.0.0.255
 permit ip any 172.16.61.0 0.0.0.255
 permit ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.0.0 0.0.255.255
 permit ip any any
ip access-list extended VLAN20
 evaluate Z40TRAFFIC
 permit ip any 172.16.52.0 0.0.0.255
 permit ip any 172.16.62.0 0.0.0.255
 permit ip any 172.16.72.0 0.0.0.255
 deny   ip any any
ip access-list extended VLAN30
 evaluate Z40TRAFFIC
 deny   ip any 172.16.51.0 0.0.0.255
 deny   ip any 172.16.61.0 0.0.0.255
 deny   ip any 172.16.71.0 0.0.0.255
 deny   ip any 172.16.52.0 0.0.0.255
 deny   ip any 172.16.62.0 0.0.0.255
 deny   ip any 172.16.72.0 0.0.0.255
 deny   ip any 172.16.54.0 0.0.0.255
 deny   ip any 172.16.64.0 0.0.0.255
 deny   ip any 172.16.74.0 0.0.0.255
 permit ip any any
ip access-list extended VLAN40
 permit ip any any reflect Z40TRAFFIC timeout 300
!
access-list 110 permit ip any 172.16.51.0 0.0.0.255
access-list 110 permit ip any 172.16.61.0 0.0.0.255
access-list 110 permit ip any 172.16.71.0 0.0.0.255
access-list 110 deny   ip any 172.16.0.0 0.0.255.255
access-list 110 permit ip any any
access-list 120 permit ip any 172.16.52.0 0.0.0.255
access-list 120 permit ip any 172.16.62.0 0.0.0.255
access-list 120 permit ip any 172.16.72.0 0.0.0.255
access-list 120 deny   ip any any
access-list 130 deny   ip any 172.16.51.0 0.0.0.255
access-list 130 deny   ip any 172.16.61.0 0.0.0.255
access-list 130 deny   ip any 172.16.71.0 0.0.0.255
access-list 130 deny   ip any 172.16.52.0 0.0.0.255
```

```
access-list 130 deny   ip any 172.16.62.0 0.0.0.255
access-list 130 deny   ip any 172.16.72.0 0.0.0.255
access-list 130 deny   ip any 172.16.54.0 0.0.0.255
access-list 130 deny   ip any 172.16.64.0 0.0.0.255
access-list 130 deny   ip any 172.16.74.0 0.0.0.255
access-list 130 permit ip any any
!
```

Zakończenie – podsumowanie

W dzisiejszym świecie sieci komputerowe odgrywają bardzo ważną rolę i możemy się na nie natknąć na każdy kroku. Potrzebują ich małe firmy, wielkie korporacje a także typowe gospodarstwa domowe, w których jest już wiele urządzeń połączonych w jedną sieć.

Powstają sieci bardzo rozbudowane, które muszą w swojej strukturze obsłużyć wiele różnych usług i skomunikować wiele różnych urządzeń tworzących daną topologię. Aby tego dokonać potrzebne jest stworzenie odpowiedniego środowiska, które sprosta tym wymaganiom. Potrzebne są odpowiednie techniki, które pokierują całym ruchem w sieci niezależnie czy jest to sieć mała czy tez ogromna sieć korporacyjna. Technikami takimi są protokoły routingu, które w zależności od ich rodzaju poradzą sobie z tym wszystkim.

W zależności od zastosowań możemy użyć protokołów, które będą stosowane w sieci jako pojedyncze lub zastosować kilka protokołów w jednej sieci tak aby nie przeszkadzały sobie nawzajem.

Ta praca miała na celu pokazanie, że jest możliwe takie właśnie skonfigurowanie urządzeń w sieci aby protokołu współistniały obok siebie.

Niestety nie da się jednoznacznie określić, który protokół jest protokołem najlepszym. Każdy ma swoje zalety i wady. Każdy z nich spełnia się w określonych sytuacjach.

Protokół RIP jest bardzo dobrym rozwiązaniem do niewielkich sieci o jednakowym złożeniu technologicznym i nie wymagającym dużych mocy przeliczeniowych użytego w sieci sprzętu oraz jest łatwy w konfiguracji. Co za tym idzie koszt zbudowania niewielkiej sieci przy użyciu protokołu RIP jest mały. Co w niewielkim stopniu może zrekompensować, że RIP jest małoskalowalny a także wybiera czasami mało optymalne trasy.

W małych sieciach można pokusić się o zastosowani routingu statycznego ale jest to korzystne w sieciach składających się z bardzo małej ilości urządzeń ponieważ konfiguracja takiej sieci jest bardzo praco i czasochłonna. Przy choć najmniejszej zmianie topologii sieci wymagana jest nowa konfiguracja urządzeń.

Potrzebne więc są coraz to nowe rozwiązania. Pojawił się protokół EIGRP, który stosuje skuteczne mechanizmy trasowania ale niestety wiąże się to ze zwiększeniem mocy obliczeniowej procesorów i większym użyciem pamięci routerów w sieci co przekłada się na zwiększenie kosztów takiej sieci.

Powstał protokół OSPF, który na przykład ogranicza rozsyłanie pełnych tablic routingu co w przypadku innych protokołów nie było zastosowane. Protokół ten nie rozsyła cyklicznych rozgłoszeń a dodatkowy ruch generuje tylko podczas zmiany stanu łącza. OSPF

wprowadza podział na tzw. obszary co wpływa na jego optymalizację i sprawdza się jako zastosowanie w dużych sieciach. Niestety jak każdy protokół posiada wady tj. zwiększone zużycie mocy obliczeniowej procesora i pamięci operacyjnej routera a także zwiększenie pasma transmisji na początku swego działania.

Każdy z protokołów ma swoje zalety i wady, każdy sprawdza się w określonych warunkach. Rozwój technik informatycznych przyczyni się do dalszego rozwoju protokołów routingu, które to będą coraz to doskonalsze pracujące w coraz to szybszych sieciach spełniających wszelkie wymagania użytkowników.

Bibliografia

Pozycje książkowe:

1. Karol Krysiak „Sieci komputerowe" Wydawnictwo Helion Gliwice 2005 [1]
2. Mark A. Dye, Rick McDonald, Antoon „Tony" W. Rufi „Akademia sieci Cisco. CCNA Exploration. Semestr 1 – Podstawy sieci" Wydawnictwo Naukowe PWN Warszawa 2008 [2]
3. Rick Graziani, Allan Johnson „Akademia sieci Cisco. CCNA Exploration. Semestr 2 - Protokoły i koncepcje routingu" Wydawnictwo Naukowe PWN Warszawa 2008 [3]
4. Kevin Dooley, Ian J. Brown „ Cisco. Receptury" Wydawnictwo Helion Gliwice 2004 [4]
5. Sławomir Kula „Systemy i sieci dostępowe xDSL" Wydawnictwo WKŁ Warszawa 2009 [5]
6. Roland W. McCarty " Cisco WAN od podstaw" Wydawnictwo Mikom 2001 [6]

Strony internetowe:

7. http://www.promanski.info/?page_id=14 [7]
8. http://www.sieci-informatyczne.yoyo.pl/sieci.php?s=m2 [8]
9. http://itpedia.pl/index.php/Frame_Relay [9]
10. http://www.rogaski.org/cisco/ccna.html [10]
11. http://cisco.howto.pl/artykuly,cisco-35-297-0.html [11]
12. http://www.cisco.com/warp/public/104/1.pdf. [12]
13. http://cisco.howto.pl/artykuly,cisco-29-57-0.html [13]
14. http://www.wikit.pl/index.php/Transmisja_izochroniczna [14]
15. http://pl.wikipedia.org/wiki/Réseaux_IP_Européens [15]
16. http://www.networld.pl/artykuly/druk/20579/Technologie.sieci.rozleglych.html
17. http://www.cisco.com/web/PL/products/routers.html

Przypisy znajdujące się w tekście zawarte w nawiasach kwadratowych […] wskazują na źródło, na którego podstawie został opracowany dany fragment pracy.

Spis tabel i rysunków

Załączniki

Wszystkie załączniki znajdują się w katalogu „Załączniki” na płycie CD dołączonej do tej pracy, która jest jej integralną częścią.

Spis załączników:

1. Załącznik nr 1 - Specyfikacja ROUTER CISCO 2800 series (2811)
2. Załącznik nr 2 - Specyfikacja ROUTER CISCO 1800 series (1841)
3. Załącznik nr 3 - Specyfikacja SWITCH CISCO 2960 CATALYST
4. Załącznik nr 4 - Specyfikacja SWITCH CISCO 3560 CATALYST
5. Załącznik nr 5 - Plik z konfiguracją ROUTERA R1
6. Załącznik nr 6 - Plik z konfiguracją ROUTERA R2
7. Załącznik nr 7 - Plik z konfiguracją ROUTERA R3
8. Załącznik nr 8 - Plik z konfiguracją ROUTERA R4
9. Załącznik nr 9 - Plik z konfiguracją ROUTERA R5
10. Załącznik nr 10 - Plik z konfiguracją ROUTERA R6
11. Załącznik nr 11 - Plik z konfiguracją ROUTERA R7
12. Załącznik nr 12 - Plik z konfiguracją SWITCH S2
13. Załącznik nr 13 - Plik z konfiguracją SWITCH S3
14. Załącznik nr 14 - Plik z konfiguracją SWITCH S4
15. Załącznik nr 15 - Plik z konfiguracją SWITCH S5
16. Załącznik nr 16 - Plik z konfiguracją SWITCH S6
17. Załącznik nr 17 - Plik z konfiguracją SWITCH S7
18. Załącznik nr 18 - Plik z konfiguracją SWITCH S8

Łódź, dnia

Dariusz Sobieszek
Numer albumu: 27340
Specjalizacja: Sieci i systemy komputerowe

Oświadczenie

Świadomy odpowiedzialności oświadczam, że przedkładana praca inżynierska pt.: „Protokoły routingu- ROUTING STATYCZNY, RIP, OSPF, EIGRP –przy wykorzystaniu urządzeń CISCO" została napisana przeze mnie samodzielnie.

Jednocześnie oświadczam, że wyżej wymieniona praca nie narusza praw autorskich w rozumieniu Ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83) oraz dóbr osobistych chronionych prawem cywilnym.

Praca nie zawiera również danych i informacji, które uzyskałem w sposób niedozwolony. Przedkładana praca inżynierska nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadawaniem dyplomów wyższej uczelni lub tytułów zawodowych.

podpis studenta

Łódź, dnia

Dariusz Sobieszek
Numer albumu: 27340
Specjalizacja: Sieci i systemy komputerowe

Oświadczenie

Wyrażam zgodę na udostępnianie mojej pracy pod tytułem „Protokoły routingu - ROUTING STATYCZNY, RIP, OSPF, EIGRP – przy wykorzystaniu urządzeń CISCO”

podpis studenta