informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

informatyka+

Kuźnia Talentów Informatycznych: Sieci komputerowe

Konfiguracja protokołów routingu statycznego i dynamicznego

Dariusz Chaładyniak

Józef Wacnik

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Konfiguracja protokołów routingu statycznego i dynamicznego

Rodzaj zajęć: Kuźnia Talentów Informatycznych
Tytuł: Konfiguracja protokołów routingu statycznego i dynamicznego
Autor: dr inż. Dariusz Chaładyniak, mgr inż. Józef Wacnik

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+** – ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w zakresie technologii informacyjno-komunikacyjnych (ICT).
www.informatykaplus.edu.pl
kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa
www.wwsi.edu.pl
rektorat@wwsi.edu.pl

Skład: Recontra Studio Graficzne

Warszawa 2010

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Konfiguracja protokołów routingu statycznego i dynamicznego

Dariusz Chaładyniak
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Józef Wacnik
Warszawska Wyższa Szkoła Informatyki
j_wacnik@poczta.wwsi.edu.pl

STRESZCZENIE

Dynamika zmian o sieciach komputerowych wymusza stosowanie w pełni skalowalnych i wysoce wydajnych protokołów routingu, służących do wymiany informacji pomiędzy urządzeniami sieciowymi oraz określeniu optymalnej ścieżki do sieci docelowej. Wykład zawiera podstawowe informacje o budowie i działaniu routerów. Wyjaśnia wybrane możliwości i zastosowania routingu statycznego i dynamicznego. Dokonuje przeglądu wybranych protokołów routingu dynamicznego (RIP, IGRP, EIGRP, OSPF) wraz z praktycznymi sposobami ich konfiguracji, implementacji i weryfikacji.

Warsztaty będą okazją do praktycznego przećwiczenia materiału z wykładu.

Spis treści

1. WPROWADZENIE DO BUDOWY I KONFIGURACJI ROUTERÓW

WPROWADZENIE

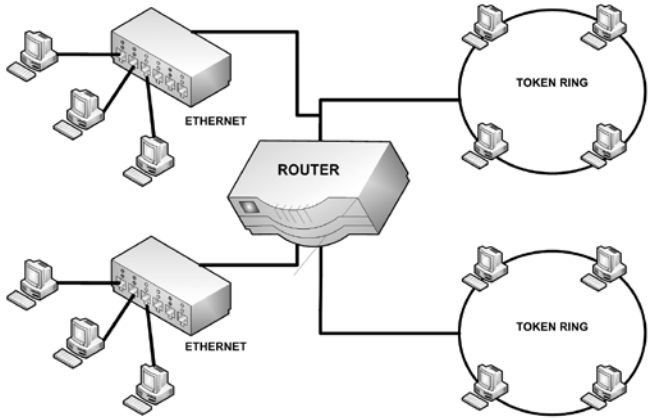
Router to specjalny typ komputera, zawiera te same podstawowe podzespoły, co zwykły komputer PC: procesor, pamięć, magistralę systemową oraz różne interfejsy wejścia/wyjścia. Routery to urządzenia sieciowe, realizujące usługi trasowania (tzn. wybierania optymalnej marszruty) i przełączania pakietów pomiędzy wieloma sieciami. Są one łącznikami sieci LAN z bardziej rozległymi sieciami WAN, tworząc rdzeń Internetu.

Tak samo jak komputery wymagają systemów operacyjnych do uruchamiania aplikacji, tak routery wymagają oprogramowania **IOS** (ang. *Internetwork Operating System*) do uruchamiania plików konfiguracyjnych. Pliki konfiguracyjne zawierają instrukcje i parametry sterujące przepływem komunikacji do routerów i z nich. Routery korzystają z protokołów routingu do określenia najlepszej ścieżki dla pakietów. Pliki konfiguracyjne określają wszystkie informacje konieczne do prawidłowej konfiguracji użycia przez router wybranych lub włączonych protokołów routingu.

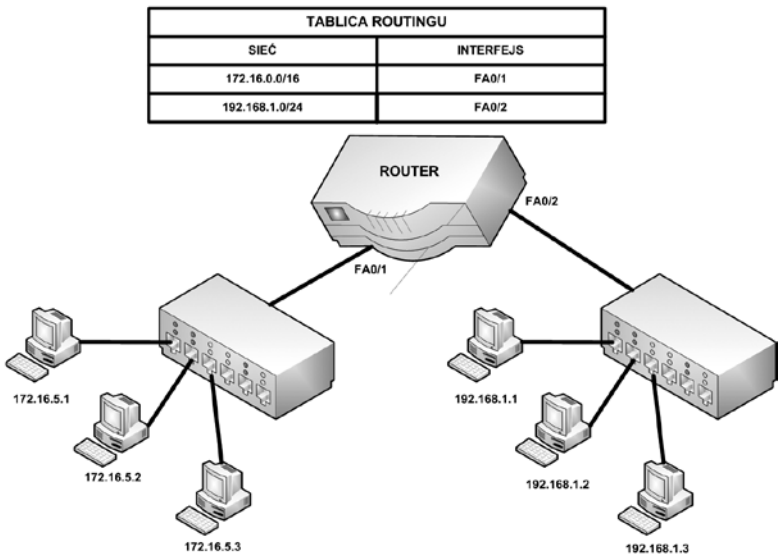
Routery służą do zwiększania fizycznych rozmiarów sieci poprzez łączenie jej segmentów (patrz rys. 1). Urządzenie to wykorzystuje logiczne adresy hostów w sieci, dzięki temu komunikacja, jako oparta na logicznych adresach odbiorcy i nadawcy, jest niezależna od fizycznych adresów urządzeń.

Oprócz filtracji pakietów pomiędzy segmentami, router określa optymalną drogę przesyłania danych po sieci. Dodatkowo eliminuje pakiety bez adresata i ogranicza dostęp określonych użytkowników do wybranych segmentów czy komputerów sieciowych.

Router jest konfigurowalny, umożliwia sterowanie przepustowością sieci oraz zapewnia pełną izolację pomiędzy segmentami.



Rysunek 1.
Przykładowe zastosowanie routera

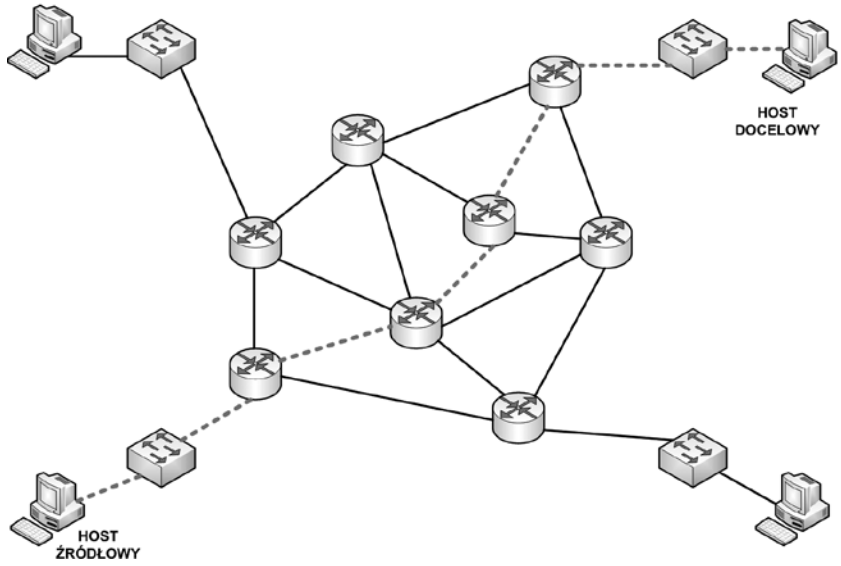


Rysunek 2.
Tablica routingu

Tablica routingu (ang. *routing table*) pokazana na rysunku 2 jest miejscem, w którym przechowywane są informacje o adresach logicznych sieci lub podsieci, maskach oraz interfejsach wyjściowych (ethernetowych lub szeregowych).

WYBÓR NAJLEPSZEJ ŚCIEŻKI DLA PAKIETÓW

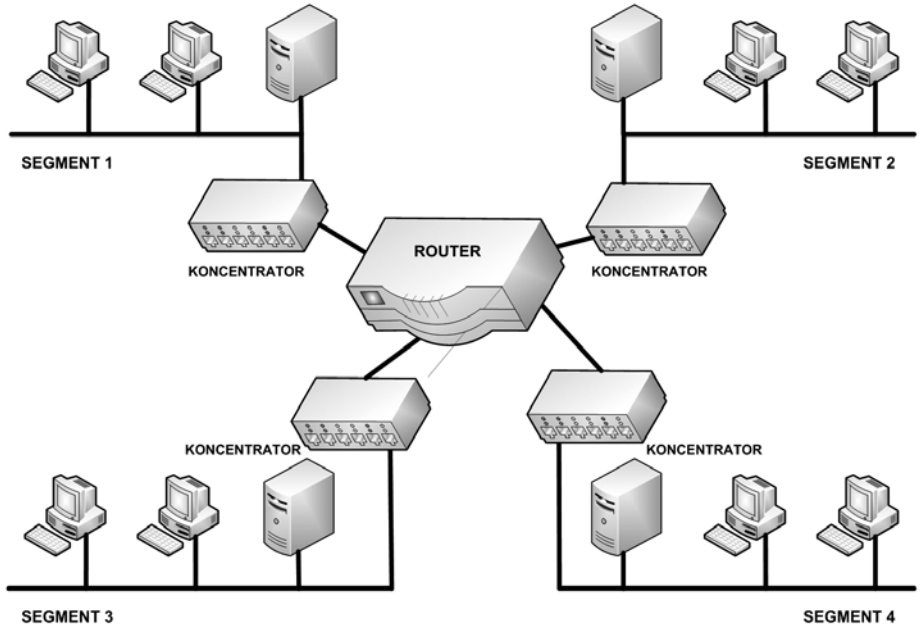
Podstawowym zadaniem routerów jest wybór optymalnej ścieżki dla pakietów na trasie od hosta źródłowego do hosta docelowego (patrz rys. 3). Routery do tego celu wykorzystują tablice routingu, które mogą być tworzone statycznie lub dynamicznie. Metoda statyczna polega na ręcznym budowaniu tablic routingu, natomiast metody dynamiczne wykorzystują odpowiednie algorytmy trasowania.



Rysunek 3.
Wybór optymalnej trasy dla pakietów

SEGMENTACJA ZA POMOCĄ ROUTERA

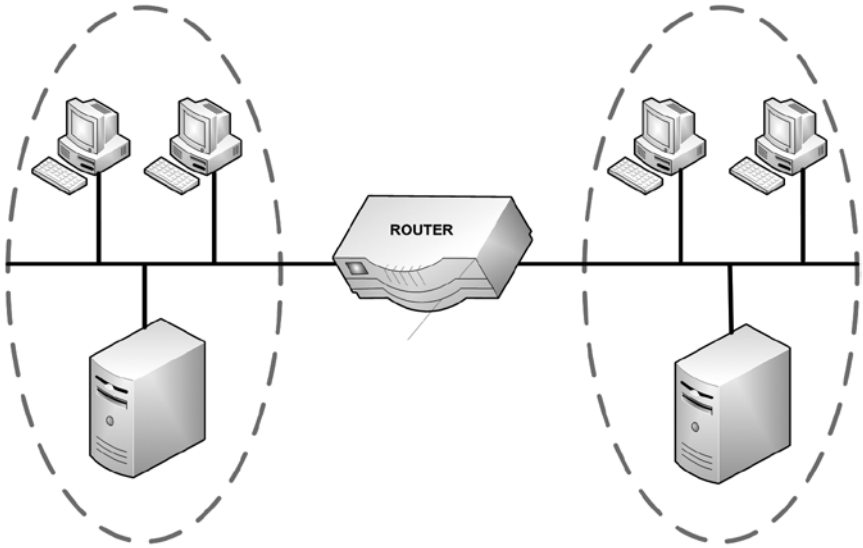
Segmentacja polega na podziale sieci na kilka mniejszych części (patrz rys. 4). Przy zastosowaniu segmentów oddzielonych routerami najintensywniej komunikujące się stacje robocze nie przeszkadzają sobie wzajemnie w pracy. Dzięki urządzeniom potrafiącym inteligentnie zatrzymać zbędny ruch sieć zostaje zrównoważona i znacznie odciążona.



Rysunek 4.
Przykład segmentacji sieci za pomocą routera

ROUTER – NIE PRZENOSI KOLIZJI

Przy zastosowaniu urządzeń sieciowych warstwy sieci, łączone ze sobą sieci stanowią osobne domeny kolizyjne (patrz rys. 5). Jest to bardzo pożądane rozwiązanie.



Rysunek 5.
Router nie powiększa domen kolizyjnych oraz rozgłoszeniowych

RODZAJE PAMIĘCI ROUTERA

Pamięć **RAM** ma następujące cechy i funkcje:
- przechowuje tablice routingu,
- zawiera pamięć podręczną protokołu ARP (ang. *Address Resolution Protocol*),
- zawiera aktualną konfigurację routera,
- buforuje pakiety (po odebraniu pakietu na jednym interfejsie, ale przed przekazaniem ich na inny interfejs są one okresowo składowane w buforze),
- traci zawartość po wyłączeniu lub restarcie routera.

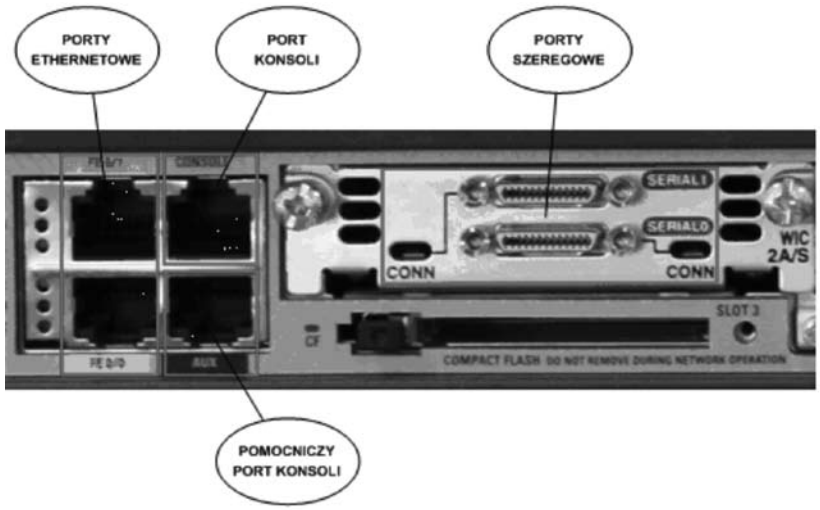
Pamięć **NVRAM** (ang. *nonvolatile RAM*) ma następujące cechy i funkcje:
- przechowuje pliki konfiguracji początkowej (o ile została zapisana, w nowych, pierwszy raz uruchomionych routerach, jest ona pusta) i ich kopie zapasowe,
- utrzymuje zawartość po wyłączeniu lub restarcie routera.

Pamięć **flash** (EPROM – ang. *Erasable Programmable ROM*) ma następujące cechy:
- przechowuje obraz IOS,
- umożliwia aktualizację oprogramowania bez konieczności wyjmowania i wymiany układów scalonych karty,
- utrzymuje zawartość po wyłączeniu lub restarcie routera,
- może przechowywać wiele wersji oprogramowania IOS.

Pamięć **ROM** ma następujące cechy i funkcje:
- zawiera instrukcje dla procedur diagnostycznych POST (ang. *Power-On Self Test*),
- przechowuje program uruchomieniowy (bootstrap) i podstawowe oprogramowanie systemu operacyjnego.

PORTY ROUTERA

Routery są wyposażone w następujące porty (patrz rys. 6):
- ethernetowe – do podłączania sieci LAN,
- szeregowe – do łączenia sieci WAN,
- konsoli – do lokalnego konfigurowania,
- pomocniczy konsoli – do zdalnego konfigurowania.



Rysunek 6.
Przykładowe porty routera

POŁĄCZENIA PORTU KONSOLI

Port konsoli jest portem służącym do konfiguracji początkowej routera i do jego monitorowania. Port konsoli jest również używany w procedurach stosowanych w razie awarii. Do połączenia komputera PC z portem konsoli routera (patrz rys. 7) służy kabel konsolowy (rollover) i przejściówka z RJ-45 na DB-9 (lub DB-25).

Komputer PC lub terminal muszą obsługiwać emulację terminala **VT100** (np. *HyperTerminal*). Aby podłączyć komputer do routera, należy wykonać następujące operacje:

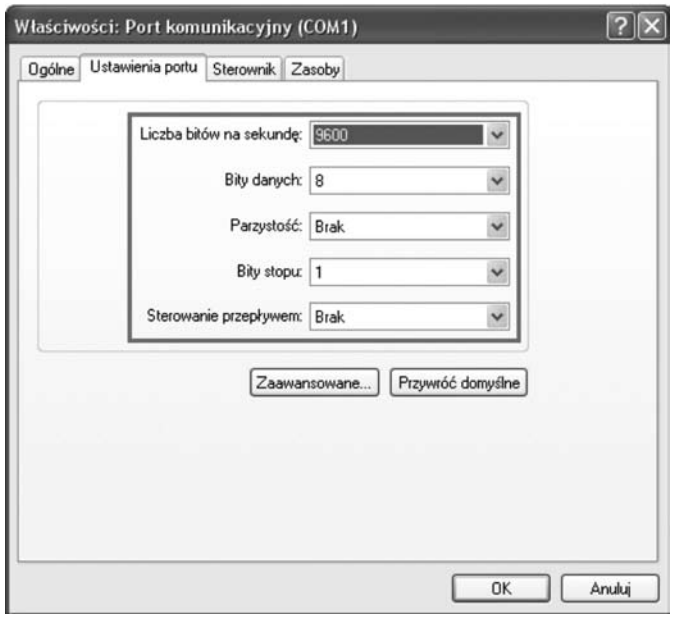
1. Podłącz złącze RJ-45 kabla rollover do portu konsoli routera.
2. Podłącz drugi koniec kabla rollover do przejściówki RJ-45 na DB-9 (lub DB-25).
3. Podłącz żeńskie złącze DB-9 (lub DB-25) przejściówki do komputera PC.

Rysunek 7.
Przykład połączenia komputera (terminala) do portu konsuli routera

KONFIGURACJA PORTU KONSOLI

Należy skonfigurować następujące parametry w oprogramowaniu emulacji terminala na komputerze PC (patrz rys. 8):

1. Odpowiedni port COM – COM1 lub COM2.
2. Liczba bitów danych na sekundę – 9600.
3. Liczba bitów danych – 8.
4. Kontrola parzystości – brak bitu kontroli parzystości.
5. Liczba bitów stopu – 1.
6. Sterowanie przepływem – brak kontroli przepływu.



Rysunek 8.
Konfiguracja portu szeregowego komputera (terminala)

INTERFEJS WIERSZA POLECEŃ

Interfejs wiersza poleceń **CLI** (ang. *Command Line Interface*) jest tradycyjną konsolą wykorzystywaną przez oprogramowanie Cisco IOS. Istnieje kilka metod dostępu do środowiska CLI.

1. Zazwyczaj dostęp do interfejsu CLI jest realizowany poprzez sesję konsoli. Konsola korzysta z połączenia szeregowego o małej prędkości, które łączy bezpośrednio komputer lub terminal ze złączem konsoli w routerze.
2. Do sesji CLI można również uzyskać dostęp zdalny przy użyciu połączenia telefonicznego, wykorzystując modem dołączony do portu AUX routera. Żadna z tych metod nie wymaga skonfigurowania usług IP w routerze.
3. Trzecią metodą uzyskiwania dostępu do sesji CLI jest ustanowienie z routerem sesji Telnet. Aby ustanowić sesję Telnet z routerem, należy skonfigurować adres IP dla co najmniej jednego interfejsu, a dla sesji terminala wirtualnego trzeba ustawić login i hasła.

TRYBY PRACY NA ROUTERZE

W interfejsie CLI jest używana struktura hierarchiczna. Struktura ta wymaga przejścia do odpowiedniego trybu w celu wykonania określonych zadań. Na przykład, aby skonfigurować interfejs routera, należy włączyć tryb konfiguracji interfejsu. Wszystkie ustawienia wprowadzone w trybie konfiguracji interfejsu dotyczą tylko danego interfejsu. Każdy z trybów konfiguracji jest oznaczony specjalnym symbolem i umożliwia wprowadzenie tylko tych poleceń, które są właściwe dla danego trybu.

System IOS udostępnia usługę interpretacji poleceń o nazwie **EXEC**. Po wprowadzeniu każdego polecenia usługa EXEC sprawdza jego poprawność i wykonuje je. W celu zapewnienia bezpieczeństwa w IOS występują dwa poziomy dostępu do sesji EXEC. Są to tryb EXEC użytkownika oraz uprzywilejowany tryb EXEC. Uprzywilejowany tryb EXEC po angielsku jest również nazywany trybem *enable*.

Tryb EXEC użytkownika udostępnia jedynie ograniczony zestaw podstawowych poleceń do monitorowania. Z tego powodu jest on również nazywany trybem „tylko do odczytu". Tryb EXEC użytkownika nie udostępnia żadnych poleceń, które umożliwiają zmianę konfiguracji routera. Tryb EXEC użytkownika jest oznaczony symbolem >.

Uprzywilejowany tryb EXEC umożliwia dostęp do wszystkich poleceń routera. Do wejścia w ten tryb może być potrzebne hasło. Dodatkową ochronę można zapewnić, ustawiając żądanie podania identyfikatora użytkownika, tak aby dostęp do routera miały tylko uprawnione osoby. Aby z poziomu EXEC użytkownika uzyskać dostęp do uprzywilejowanego poziomu EXEC, należy po symbolu > wprowadzić polecenie **enable**. Jeśli skonfigurowane jest hasło, router zażąda jego podania. Po wprowadzeniu poprawnego hasła symbol zachęty routera zmieni się na symbol **#**. Oznacza to, że użytkownik jest w uprzywilejowanym trybie EXEC.

Tryb konfiguracji globalnej oraz wszystkie inne bardziej szczegółowe tryby konfiguracji są dostępne tylko z uprzywilejowanego trybu EXEC. Aby przejść do trybu konfiguracyjnego należy wprowadzić polecenie **configure terminal**. O tym, że pracujemy w trybie konfiguracyjnym zawiadamia nas znak gotowości np. **Router(config)#**. Zakończenie pracy w tym trybie realizowane jest poprzez wprowadzenie kombinacji klawiszy **CTRL+Z**. Ponadto tryb konfiguracyjny można opuścić, wprowadzając w linii poleceń: **end** lub **exit**.

PRZEŁĄCZANIE POMIĘDZY TRYBAMI EXEC

Aby przejść z trybu użytkownika do trybu uprzywilejowanego wpisujemy polecenie **enable** a następnie podajemy hasło. Aby powrócić z powrotem do trybu użytkownika wpisujemy polecenie **disable** (patrz rys. 9).

Rysunek 9.
Przełączanie pomiędzy trybami pracy routera

PRACA Z SYSTEMEM IOS

Istnieją trzy środowiska operacyjne (tryby) urządzeń z systemem IOS:

- tryb ROM monitor,
- tryb Boot ROM,
- tryb IOS.

Po uruchomieniu, router ładuje do pamięci RAM jedno z powyższych środowisk operacyjnych i rozpoczyna jego wykonywanie. Administrator systemu może przy użyciu ustawienia rejestru konfiguracji wybrać domyślny tryb uruchamiania routera.

Tryb **ROM monitor** realizuje proces uruchomieniowy udostępnia funkcje niskopoziomowe i diagnostyczne. Jest używany w przypadku awarii systemu oraz w celu odzyskania utraconego hasła. Tryb ROM monitor nie jest dostępny za pośrednictwem żadnego interfejsu sieciowego. Jedyną metodą dostępu jest bezpośrednie fizyczne połączenie przez port konsoli.

Podczas pracy w trybie **Boot ROM** na routerze dostępny jest tylko ograniczony zestaw funkcji systemu IOS. Tryb Boot ROM umożliwia operacje zapisu do pamięci błyskowej i jest używany głównie w celu zastąpienia obrazu systemu IOS znajdującego się w tej pamięci. W trybie Boot ROM można modyfikować obraz systemu IOS, używając polecenia **copy tftp flash**. Polecenie to powoduje skopiowanie obrazu systemu IOS przechowywanego na serwerze TFTP do pamięci flash routera.

Podczas normalnego działania routera jest wykorzystywany pełny obraz systemu IOS zapisany w pamięci flash. W przypadku niektórych urządzeń system IOS jest uruchamiany bezpośrednio z pamięci flash. Jednak w przypadku większości routerów Cisco kopia systemu IOS jest ładowana do pamięci RAM i z niej uruchamiana. Niektóre obrazy systemu IOS są zapisane w pamięci flash w postaci skompresowanej i podczas kopiowania do pamięci RAM muszą zostać zdekompresowane.

Aby zobaczyć informacje o obrazie i wersji uruchomionego systemu IOS, należy użyć polecenia **show version**, które wyświetla również ustawienie rejestru konfiguracyjnego. Aby sprawdzić, czy w systemie jest wystarczająca ilość pamięci do załadowania nowego obrazu systemu IOS, należy użyć polecenia **show flash**.

NAZWA ROUTERA

Jednym z pierwszych zadań konfiguracyjnych powinno być nadanie routerowi unikatowej nazwy (patrz rys. 10). Zadanie to wykonuje się w trybie konfiguracji globalnej za pomocą następującego polecenia:

Router(config)#hostname Darek

Po naciśnięciu klawisza Enter nazwa w symbolu zachęty zmieni się z domyślnej (**Router**) na nowo skonfigurowaną (**Darek**).

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# hostname Darek
Darek(config)#
```

Rysunek 10.
Zmiana nazwy routera

KONFIGUROWANIE HASEŁ ROUTERA

a) Hasło dla konsoli routera

Hasła ograniczają dostęp do routerów. Należy je zawsze konfigurować dla linii terminala wirtualnego (ang. **vty** – *virtual terminal lines*) oraz linii konsoli (ang. *line console*). Hasła służą także do określania praw dostępu do uprzywilejowanego trybu EXEC, tak aby zmian w pliku konfiguracyjnym mogli dokonywać wyłącznie uprawnieni użytkownicy.

W celu ustawienia opcjonalnego, ale zalecanego, hasła dla linii konsoli (patrz rys. 11) używa się następujących poleceń (cyfra 0 oznacza numer portu konsoli):

Router(config)#line console 0
Router(config-line)#password <*hasło*>

Aby wymusić logowanie do portu konsoli za pomocą zdefiniowanego hasła, należy użyć polecenia **login**. Brak tego polecenia daje swobodny dostęp do routera.

Router(config-line)#login

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password Darek
Router(config-line)# login
```

Rysunek 11.
Konfiguracja hasła dla konsoli routera

b) Hasło dla terminala wirtualnego

Aby użytkownicy mieli zdalny dostęp do routera przez połączenie Telnet, należy ustawić hasło dla jednej lub wielu linii vty. Większość routerów Cisco obsługuje pięć linii vty o numerach od 0 do 4. Inne platformy sprzętowe obsługują różne liczby połączeń vty. Zazwyczaj używa się tego samego hasła dla wszystkich linii vty. Można jednak ustawić inne hasło dla każdej z linii. Do ustawienia hasła dla wszystkich linii vty używa się następujących poleceń (patrz rys. 12):

Router(config)#line vty 0 4
Router(config-line)#password <*hasło*>
Router(config-line)#login

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# line vty 0 4
Router(config-line)# password Olek
Router(config-line)# login
```

Rysunek 12.
Konfiguracja hasła dla wirtualnych terminali

c) Hasła dla trybu uprzywilejowanego
Polecenia **enable password** i **enable secret** służą do ograniczania dostępu do uprzywilejowanego trybu EXEC (patrz rys. 13).

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# enable password Warszawa
Router(config)# enable secret Wroclaw
```

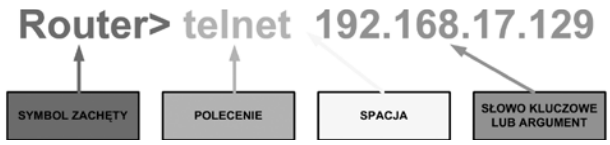
Rysunek 13.
Konfiguracja hasła dla trybu uprzywilejowanego

Polecenie **enable password** jest używane tylko wtedy, gdy nie zostało zastosowane polecenie **enable secret**. Należy korzystać z polecenia **enable secret**, ponieważ jest ono szyfrowane, podczas gdy polecenie **enable password** nie jest (zapisane jest otwartym tekstem i doskonale widoczne w konfiguracji routera). Do ustawienia haseł używa się następujących poleceń:

Router(config)#enable password <*hasło*>
Router(config)#enable secret <*hasło*>

PODSTAWOWA STRUKTURA POLECEŃ IOS

Każda komenda w IOS ma specyficzny format i składnię oraz jest wykonywana we właściwym wierszu poleceń. Ogólna składnia polecenia rozpoczyna się komendą, a po niej następują właściwe słowa kluczowe oraz argumenty (patrz rys. 14). Niektóre komendy zawierają podzbiór słów kluczowych i argumenty, które dostarczają dodatkową funkcjonalność. Na rysunku są pokazane wspomniane części polecenia.



Rysunek 14.
Struktura składni poleceń dla routera

Komenda jest początkowym słowem (lub słowami) wpisanym w wierszu poleceń. Komendy nie rozróżniają wielkości liter. Po komendzie występuje jedno lub więcej słów kluczowych i argumentów.

Słowa kluczowe opisują specyficzne parametry dla interpretera. Dla przykładu, polecenie **show** służy do wyświetlania informacji o urządzeniu. Komenda ta, może zawierać wiele słów kluczowych, które mogą być użyte do zdefiniowania wyniku, jaki ma zostać wyświetlony. Na przykład:

Router# show running-config

Komenda **show** została uzupełniona słowem kluczowym **running-config**. Wydanie polecenia wskazuje, że na wyjściu powinna zostać wyświetlona konfiguracja bieżąca urządzenia.

Komenda może wymagać jednego lub więcej argumentów. W przeciwieństwie do słowa kluczowego, argument nie jest słowem predefiniowanym. Argument jest wartością lub zmienną definiowaną przez użytkownika. Dla przykładu, gdy chcemy dołączyć opis do interfejsu korzystając z komendy **description**, wpisujemy:

Router(config-if)# description Sala komputerowa 213

Komenda to: **description**. Argument to: **Sala komputerowa 213**. Użytkownik definiuje argumenty. Dla tej komendy argument może być dowolnym ciągiem tekstowym o długości nieprzekraczającej 80 znaków.

Po każdej pełnej komendzie, ewentualnie uzupełnionej słowami kluczowymi oraz argumentami, należy nacisnąć klawisz Enter, aby przesłać komendę do interpretera poleceń.

KORZYSTANIE Z POMOCY WIERSZA POLECEŃ

IOS zawiera kilka rodzajów dostępu do pomocy:

1. Pomoc kontekstowa w postaci podpowiedzi
2. Weryfikacja składni komendy
3. Skróty i „gorące klawisze"

Ad.1. Pomoc kontekstowa w postaci podpowiedzi

Pomoc kontekstowa dostarcza wiersz komend i związanych z nimi słów kluczowych, pasujących do bieżącego trybu. Aby uzyskać pomoc należy wpisać znak zapytania ? w dowolnym miejscu wiersza poleceń. Następuje wówczas natychmiastowa odpowiedź – nie trzeba znaku ? potwierdzać klawiszem Enter.

Korzystając z pomocy kontekstowej otrzymujemy listę dostępnych komend. Takie rozwiązanie może być używane np. jeśli nie mamy pewności co do nazwy polecenia lub jeśli chcemy sprawdzić, czy IOS wspiera konkretną komendę. Dla przykładu, w celu uzyskania listy komend dostępnych w trybie EXEC użytkownika wprowadź ? w wierszu poleceń po znaku zachęty Router>.

Kolejnym przykładem pomocy kontekstowej jest wykorzystanie komendy do wyświetlenia listy komend rozpoczynających się od określonego znaku lub znaków. Po wpisaniu znaku lub sekwencji znaków, jeśli naciśniemy ? bez spacji, to IOS wyświetli listę poleceń lub słów kluczowych dla kontekstu rozpoczynającego się od podanych znaków. Na przykład, wpisz sh?, aby wyświetlić listę komend, które rozpoczynają się od ciągu sh.

Kolejnym zastosowaniem pomocy kontekstowej jest próba określenia, które opcje, słowa kluczowe czy argumenty są powiązane z określoną komendą. Aby sprawdzić, co może lub powinno zostać wprowadzone, po wpisaniu komendy należy nacisnąć spację i wprowadzić znak ?. Na przykład, po wpisaniu komendy **clock set 19:50:00** możemy wpisać znak ? i w ten sposób dowiedzieć się, jakie opcje lub słowa kluczowe pasują do tej komendy.

Ad.2. Weryfikacja składni komend

Po zatwierdzeniu komendy klawiszem Enter, w celu określenia żądanej akcji interpreter parsuje polecenie od lewej strony do prawej. IOS dostarcza informacji na temat błędów w składni. Jeśli interpreter zrozumie komendę, żądana akcja zostaje wykonana, a wiersz poleceń zwraca właściwy znak zachęty. Jednakże, jeśli interpreter nie rozumie wprowadzonego polecenia, to dostarczy informację zwrotną z opisem, co zostało wprowadzone błędnie.

Są trzy różne rodzaje komunikatów o błędach:

- niejednoznaczne polecenie,
- niekompletne polecenie,
- niepoprawne polecenie.

Ad.3. Skróty i „gorące klawisze"

Wiersz poleceń CLI dostarcza tzw. „gorące klawisze" (ang. *hot keys*) oraz skróty, które ułatwiają konfigurację, monitoring i rozwiązywanie problemów. Następujące skróty zasługują na specjalną uwagę:

Tab	– dopełnia komendę lub słowo kluczowe,
Ctrl-R	– odświeża linię,
Ctrl-Z	– wychodzi z trybu konfiguracji i wraca do trybu EXEC,
Strzałka w dół	– pozwala użytkownikowi na przewijanie do przodu wydanych komend,
Strzałka w górę	– pozwala użytkownikowi na przewijanie do tyłu wydanych komend,
Ctrl-Shift-6	– pozwala użytkownikowi na przerwanie procesu IOS takiego jak ping czy Traceroute,
Ctrl-C	– przerywa aktualną komendę i wychodzi z trybu konfiguracji.

KONFIGURACJA INTERFEJSU ETHERNETOWEGO

Każdy interfejs Ethernet musi mieć zdefiniowany adres IP i maskę podsieci, aby mógł przesyłać pakiety IP. Aby skonfigurować interfejs Ethernet, należy wykonać następujące czynności (patrz rys. 15):

1. Przejść do trybu konfiguracji globalnej.
2. Przejść do trybu konfigurowania interfejsu.
3. Podać adres interfejsu i maskę podsieci.
4. Włączyć interfejs.
5. Domyślnie interfejsy są wyłączone lub nieaktywne. Aby włączyć lub uaktywnić interfejs, należy użyć polecenia **no shutdown**. Jeśli zachodzi potrzeba wyłączenia interfejsu w celu przeprowadzenia czynności serwisowych lub rozwiązania problemu, należy użyć polecenia **shutdown**.

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Rysunek 15.
Przykład konfiguracji interfejsu ethernetowego

KONFIGURACJA INTERFEJSU SZEREGOWEGO

Aby skonfigurować interfejs szeregowy, należy wykonać następujące czynności (patrz rys. 16):

1. Przejść do trybu konfiguracji globalnej.
2. Przejść do trybu konfigurowania interfejsu.
3. Podać adres interfejsu i maskę podsieci.
4. Ustawić częstotliwość zegara taktującego synchronizację połączenia (np. 56000).
5. Włączyć interfejs.

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# clock rate 56000
Router(config-if)# no shutdown
```

Rysunek 16.
Przykład konfiguracji interfejsu szeregowego

Jeśli podłączony jest kabel DCE, ustaw częstotliwość zegara. Pomiń tę czynność, jeśli podłączony jest kabel DTE. Interfejsy szeregowe wymagają sygnału zegarowego sterującego komunikacją. W większości środowisk sygnału zegarowego dostarcza urządzenie DCE, takie jak CSU/DSU (ang. *Channel Service Unit/Data Service Unit*). Domyślnie routery Cisco są urządzeniami DTE, ale można je skonfigurować jako urządzenia DCE.

W przypadku bezpośrednio połączonych ze sobą łączy szeregowych, na przykład w laboratorium, jedna ze stron musi być traktowana jako urządzenie DCE i dostarczać sygnału zegarowego. Polecenie clock rate powoduje włączenie zegara i określenie jego szybkości. Dostępne szybkości w bitach na sekundę to: 1200, 2400, 9600, 19 200, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000 i 4 000 000. W przypadku niektórych interfejsów szeregowych pewne szybkości mogą nie być dostępne.

Domyślnie interfejsy są wyłączone lub nieaktywne. Aby włączyć lub uaktywnić interfejs, należy użyć polecenia **no shutdown**. Jeśli zachodzi potrzeba administracyjnego wyłączenia interfejsu w celu przeprowadzenia czynności serwisowych lub rozwiązania problemu, należy użyć polecenia **shutdown**.

Do obejrzenia stanu pracujących interfejsów służą poniższe plecenia:

```
Router#show interfaces
Router#show ip interface
Router#show ip interface brief
```

OPIS INTERFEJSÓW ROUTERA

Opis interfejsu powinien zawierać istotne informacje, na przykład dotyczące sąsiedniego routera, numeru obwodu lub konkretnego segmentu sieci. Opis interfejsu może pomóc użytkownikowi sieci zapamiętać określone informacje na jego temat, na przykład do jakiej sieci jest on podłączony (patrz rys. 17).

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# description Podłączenie do pracowni komputerowej 111
```

Rysunek 17.
Przykładowy opis interfejsu routera

Chociaż opis jest umieszczony w plikach konfiguracyjnych przechowywanych w pamięci routera, nie wpływa on na funkcjonowanie routera. Opis zawiera jedynie informacje dotyczące interfejsu. Tworzy się go w oparciu o standardowy format, który ma zastosowanie do każdego interfejsu.

ODWZOROWANIE NAZW HOSTÓW

Odwzorowywanie nazw hostów jest procesem, za pomocą którego system komputerowy kojarzy nazwę hosta z adresem IP (patrz rys. 18). Aby móc używać nazw hostów do komunikowania się z innymi urządzeniami IP, urządzenia sieciowe, takie jak routery, muszą być w stanie powiązać te nazwy z odpowiednimi adresami IP. Lista nazw hostów i powiązanych z nimi adresów IP nosi nazwę **tablicy hostów**.

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# ip host Warszawa 192.168.10.15
Router(config)# ip host Wroclaw 192.168.30.49
Router(config)# ip host Torun 192.168.70.36
Router(config)# ip host Krakow 192.168.90.53
```

Rysunek 18.
Przykłady odwzorowania nazw hostów

2. WPROWADZENIE DO KONFIGURACJI ROUTINGU STATYCZNEGO

WPROWADZENIE DO ROUTINGU

Główne przeznaczenie routera jest przekazywanie pakietów z jednej sieci do drugiej. Aby router mógł wykonać to zadanie poprawnie musi wiedzieć, co zrobić z dostarczonym mu pakietem; gdzie go dalej przesłać, aby osiągnął on swoje przeznaczenie. Router wykorzystuje w tym celu tablicę routingu, czyli wskazówki, na który interfejs, pod jaki adres IP, przesłać pakiet.

Tablica routingu może być zbudowana na kilka sposobów:

- na pewno znajdują się tam adresy sieci bezpośrednio połączonych do interfejsów routera (np. fastethernet 0/0 i serial 0/0);
- inne sieci dostępne poprzez poszczególne interfejsy można wpisać ręcznie – routing statyczny;
- lub posłużyć się protokołami routingu dynamicznego (np. RIP, IGRP, OSPF).

ROUTING STATYCZNY

Najprostszą formą budowania informacji o topologii sieci są ręcznie podane przez administratora trasy. Przy tworzeniu takiej trasy wymagane jest jedynie podanie adresu sieci docelowej, maski podsieci oraz interfejsu, przez który pakiet ma zostać wysłany lub adresu IP następnego routera na trasie.

Routing statyczny ma wiele zalet:

1. Router przesyła pakiety przez z góry ustalone interfejsy bez konieczności każdorazowego obliczania tras, co zmniejsza zajętość cykli procesora i pamięci.
2. Informacja statyczna nie jest narażona na deformację spowodowaną zanikiem działania dynamicznego routingu na routerach sąsiednich.
3. Zmniejsza się zajętość pasma transmisji, gdyż nie są rozsyłane pakiety rozgłoszeniowe protokołów routingu dynamicznego.

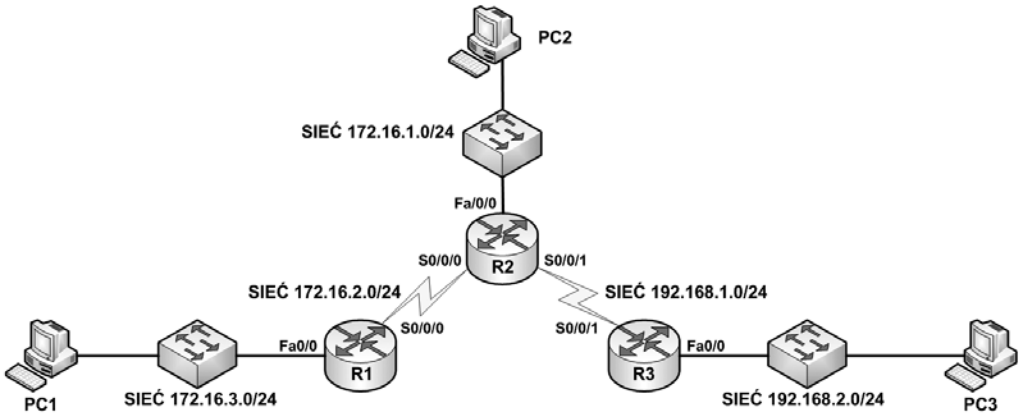
Dla małych sieci jest to doskonałe rozwiązanie, ponieważ nie musimy dysponować zaawansowanymi technologicznie i rozbudowanymi sprzętowo routerami.

Routing statyczny zapewnia również konfigurację tras domyślnych, nazywanych **bramami ostatniej szansy** (ang. *gateway of the last resort*). Jeżeli router uzna, iż żadna pozycja w tablicy routingu nie odpowiada poszukiwanemu adresowi sieci docelowej, korzysta ze statycznego wpisu, który spowoduje odesłanie pakietu w inne miejsce sieci. Routing statyczny wymaga jednak od administratora sporego nakładu pracy w początkowej fazie konfiguracji sieci, nie jest również w stanie reagować na awarie poszczególnych tras.

KONFIGUROWANIE TRAS STATYCZNYCH

Aby skonfigurować trasy statyczne, należy wykonać następujące czynności:

1. Określ sieci docelowe, ich maski podsieci oraz bramy. Brama może być zarówno interfejsem lokalnym, jak i adresem następnego przeskoku prowadzącym do sąsiedniego routera.
2. Przejdź do trybu konfiguracji globalnej.
3. Wpisz polecenie **ip route** z adresem i maską sieci oraz adresem określonym w kroku 1.
4. Powtórz krok 3 dla wszystkich sieci docelowych zdefiniowanych w kroku 1.
5. Opuść tryb konfiguracji globalnej.
6. Za pomocą polecenia **copy running-config startup-config** zapisz aktywną konfigurację w pamięci NVRAM.



URZĄDZENIE SIECIOWE	INTERFEJS	ADRES IP	MASKA PODSIECI	BRAMA DOMYŚLNA
ROUTER R1	Fa0/0 S0/0/0	172.16.3.1 172.16.2.1	255.255.255.0 255.255.255.0	
ROUTER R2	Fa0/0 S0/0/0 S0/0/1	172.16.1.1 172.16.2.2 192.168.1.2	255.255.255.0 255.255.255.0 255.255.255.0	
ROUTER R3	Fa0/0 S0/0/1	192.168.2.1 192.168.1.1	255.255.255.0 255.255.255.0	
HOST PC1	Karta sieciowa	172.16.3.10	255.255.255.0	172.16.3.1
HOST PC2	Karta sieciowa	172.16.1.10	255.255.255.0	172.16.1.1
HOST PC3	Karta sieciowa	192.168.2.10	255.255.255.0	192.168.2.1

Rysunek 19.
Przykładowy scenariusz połączeń sieciowych

Konfigurację routingu statycznego przeprowadzimy dla przykładowej sytuacji sieciowej pokazanej na rysunku 19. W przedstawionym przykładzie są 3 routery, które łączą ze sobą 5 sieci. Kolejne rysunki obrazują poszczególne etapy konfiguracji routingu statycznego.

SIECI PODŁĄCZONE BEZPOŚREDNIO

Zanim router będzie mógł przekazywać pakiety do innych (zdalnych) sieci, jego sieci połączone bezpośrednio muszą być aktywne. Sieci podłączone bezpośrednio do routera R1 sprawdzamy poleceniem – **R1# show ip route**, patrz rys. 20.

```
R1#show ip route
(**output omitted**)

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0


R2#show ip route
172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1


R3#show ip route
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Rysunek 20.
Podgląd konfiguracji sieci połączonych bezpośrednio do routerów R1, R2 i R3

KONFIGURACJA NA ROUTERZE R1 (Z WYKORZYSTANIEM ADRESU IP NASTĘPNEGO SKOKU)

Na rysunku 21 przedstawiono konfigurację routingu statycznego dla routera R1 z wykorzystaniem adresu IP następnego skoku.

```
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
```

Rysunek 21.
Konfiguracja routingu statycznego przeprowadzona dla routera R1

KONFIGURACJA NA ROUTERZE R2 I R3 (Z WYKORZYSTANIEM ADRESU IP NASTĘPNEGO SKOKU)

```
R2>
R2> enable
Password:
R2#
R2# configure terminal
R2(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/1


R3>
R3> enable
Password:
R3#
R3# configure terminal
R3(config)# ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Rysunek 22.
Konfiguracja routingu statycznego przeprowadzona dla routerów R1 i R2

SPRAWDZANIE ZMIAN W TABLICY ROUTINGU

Skonfigurowane statycznie sieci podłączone do routerów R1, R2 i R3 można sprawdzić poleceniami jak na rysunku 23.

```
R1#show ip route
***output omitted***
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2

R2#show ip route
***output omitted***
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 [1/0] via 172.16.2.1
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1

R3#show ip route
***output omitted***
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 192.168.1.2
S       172.16.2.0 [1/0] via 192.168.1.2
S       172.16.3.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Rysunek 23.
Podgląd tablic routingu dla routerów R1, R2 i R3

WERYFIKACJA POŁĄCZEŃ

Weryfikację połączeń przeprowadzamy za pomocą polecenia **ping**. Z rysunku 24 wynika, że wszystkie połączenia są poprawne.

```
R1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#
```

Rysunek 24.
Weryfikacja połączeń sieciowych za pomocą polecenia ping

KONFIGURACJA NA ROUTERZE R1 (Z WYKORZYSTANIEM INTERFEJSU WYJŚCIOWEGO)

```
R1(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

Rysunek 25.
Konfiguracja routingu statycznego dla routera R1 z wykorzystaniem interfejsu wyjściowego

KONFIGURACJA NA ROUTERZE R2 I R3 (Z WYKORZYSTANIEM INTERFEJSU WYJŚCIOWEGO)

```
R2>
R2> enable
Password:
R2#
R2# configure terminal
R2(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/1

R3>
R3> enable
Password:
R3#
R3# configure terminal
R3(config)# ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Rysunek 26.
Konfiguracja routingu statycznego dla routerów R2 i R3 z wykorzystaniem interfejsu wyjściowego

SPRAWDZANIE ZMIAN W TABLICY ROUTINGU

Skonfigurowane statycznie sieci podłączone do routerów R1, R2 i R3 można sprawdzić poleceniami jak na rysunku 27.

```
R1#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0

R2#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 is directly connected, Serial0/0/1

R3#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Rysunek 27.
Podgląd tablic routingu dla routerów R1, R2 i R3

TRASY STATYCZNE A ODLEGŁOŚĆ ADMINISTRACYJNA

Trasa statyczna używająca albo adresu IP następnego skoku, albo interfejsu wyjściowego domyślnie ma odległość administracyjną 1. Jednak, kiedy konfigurujemy trasę statyczną, określając interfejs wyjściowy, w wyniku polecenia **show ip route** nie ma wartości odległości administracyjnej. Kiedy trasa statyczna zostanie skonfigurowana z interfejsem wyjściowym, w wynikach widzimy sieć jako bezpośrednio połączoną z tym interfejsem. Domyślną wartością administracyjną każdej trasy statycznej, również tej skonfigurowanej z interfejsem wyjściowym jest 1. Pamiętajmy, że tylko sieć połączona bezpośrednio może mieć odległość administracyjną równą 0.

KONFIGUROWANIE TRASY DOMYŚLNEJ


```
R1(config)# ip route 0.0.0.0  0.0.0.0  192.168.1.5
LUB
R1(config)# ip route 0.0.0.0  0.0.0.0  S0/0/0
```

Rysunek 28.
Konfigurowanie trasy domyślnej

Trasy domyślne służą do routingu pakietów, których adresy docelowe nie odpowiadają żadnym innym trasom w tablicy routingu. Routery mają zazwyczaj skonfigurowaną trasę statyczną dla ruchu związanego z Internetem, ponieważ utrzymywanie tras do wszystkich sieci w Internecie jest zwykle niepotrzebne. Trasa domyślna to w rzeczywistości specjalna trasa statyczna zgodna z następującym formatem (patrz rys. 28):

ip route ***0.0.0.0 0.0.0.0*** [***adres-następnego-skoku*** | ***interfejs-wychodzący***]

Maska 0.0.0.0 poddana logicznej operacji AND z docelowym adresem IP pakietu przeznaczonego do przesłania zawsze da w wyniku sieć 0.0.0.0. Jeśli pakiet nie pasuje do trasy precyzyjniej określonej w tablicy routingu, zostanie przesłany do sieci 0.0.0.0.

Aby skonfigurować trasy domyślne, należy wykonać następujące czynności:

1. Przejść do trybu konfiguracji globalnej.
2. Wpisać polecenie **ip route**, podając 0.0.0.0 jako adres sieci i 0.0.0.0 jako maskę. Parametr adres oznaczający trasę domyślną może być interfejsem routera lokalnego połączonego z sieciami zewnętrznymi lub adresem IP routera następnego przeskoku. W większości przypadków należy określić adres IP routera następnego przeskoku.
3. Opuścić tryb konfiguracji globalnej.
4. Za pomocą polecenia **copy running-config startup-config** zapisać aktywną konfigurację w pamięci NVRAM.

SPRAWDZENIE ZMIAN W TABLICY ROUTINGU

Wydając polecenie **show ip route**, sprawdzamy zmiany wprowadzone do tablicy routingu. Należy zwrócić uwagę, że gwiazdka (*) obok kodu S oznacza trasę domyślną. Właśnie dlatego nazywana jest „domyślną trasą statyczną" (patrz rys. 29).

```
R1#show ip route
***output omitted***                                        PRZED

Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
R1#

R1#show ip route

       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0          PO
R1#
```

Rysunek 29.
Sprawdzenie zmian w tablicy routingu po konfiguracji tras domyślnych

3. WPROWADZENIE DO KONFIGURACJI PROTOKOŁÓW ROUTINGU DYNAMICZNEGO

PROTOKOŁY ROUTINGU

Protokoły routingu różnią się od protokołów routowanych (routowalnych) zarówno pod względem funkcjonowania, jak i przeznaczenia. Protokół routingu to metoda komunikacji pomiędzy routerami, umożliwia routerom współużytkowanie informacji na temat sieci i dzielących je odległości. Routery wykorzystują te

informacje do tworzenia i utrzymywania tablic routingu. Przykłady protokołów routingu:
- protokół RIP (ang. *Routing Information Protocol*),
- protokół IGRP (ang. *Interior Gateway Routing Protocol*),
- protokół EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*),
- protokół OSPF (ang. *Open Shortest Path First*).

PROTOKOŁY ROUTOWANE

Protokół routowany służy do kierowania ruchem użytkowym. Zawiera w adresie warstwy sieciowej wystarczającą ilość informacji, aby umożliwić przesłanie pakietu z jednego hosta do innego w oparciu o właściwy dla siebie schemat adresowania. Przykłady protokołów routowanych:
- IP (ang. *Internet Protocol*),
- IPX (ang. *Internetwork Packet Exchange*),
- DECnet (ang. *Digital Equipment Corporation network*),
- AppleTalk,
- Banyan VINES,
- XNS (ang. *Xerox Network Systems*).

Wyróżniamy dwie kategorie protokołów routingu:

1. Protokoły wewnętrznej bramy IGPs (ang. *Interior Gateway Protocols*):
   - RIP
   - IGRP
   - EIGRP
   - OSPF
   - IS-IS (ang. *Intermediate System-to-Intermediate System*).

2. Protokoły zewnętrznej bramy EGPs (ang. *Exterior Gateway Protocols*):
   - BGP (ang. *Border Gateway Protocol*).

Systemy te są sklasyfikowane w zależności od tego, jak współpracują one względem systemów autonomicznych. **System autonomiczny** to grupa sieci pozostających pod wspólną administracją i współdzielących tę samą strategię routingu. Z zewnątrz system autonomiczny jest widoczny jako pojedyncza jednostka. System autonomiczny może być prowadzony przez jednego lub kilku operatorów, prezentując jednocześnie spójny widok routingu dla świata zewnętrznego.

IANA (ang. *Internet Assigned Numbers Authority*) nadaje numery systemów autonomicznych regionalnym organizacjom rejestrującym. Numer systemu autonomicznego jest 16-bitowym (aktualnie 32-bitowym) numerem identyfikacyjnym. Protokół BGP (ang. *Border Gateway Protocol*) wymaga aby określić ten unikatowy, przypisany numer systemu autonomicznego w swojej konfiguracji.

PROTOKOŁY ROUTINGU DYNAMICZNEGO

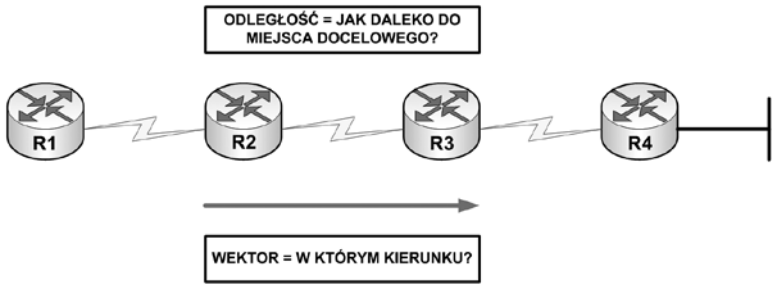
Celem protokołu routingu jest stworzenie i utrzymywanie tablicy routingu. Tablica ta zawiera sieci zapamiętane przez router oraz przypisane im interfejsy. Routery używają protokołów routingu do zarządzania informacjami odbieranymi od innych routerów i ich interfejsów oraz informacjami zawartymi w trasach skonfigurowanych ręcznie. Protokół routingu zapamiętuje wszystkie dostępne trasy, umieszcza najlepsze trasy w tablicy routingu i usuwa trasy, gdy te nie są już poprawne. Router korzysta z informacji zawartych w tablicy routingu do przesyłania pakietów protokołu routowanego.

Algorytm routingu stanowi podstawę routingu dynamicznego. Gdy topologia sieci zmieni się z powodu rozrostu, rekonfiguracji lub awarii sieci, baza wiedzy o sieci musi również ulec zmianie. Baza wiedzy o sieci musi odzwierciedlać dokładnie kształt nowej topologii.

Gdy wszystkie trasy w intersieci działają w oparciu o te same informacje, mówi się, że intersieć osiągnęła zbieżność (ang. *convergence*). Pożądane jest szybkie osiąganie zbieżności, ponieważ skraca to czas, w jakim routery podejmują niewłaściwe decyzje o routingu.

Systemy autonomiczne dzielą globalną intersieć na sieci mniejsze i łatwiejsze w zarządzaniu. Każdy system autonomiczny ma swój własny zbiór reguł i zasad oraz numer AS, który odróżnia go od innych systemów autonomicznych.

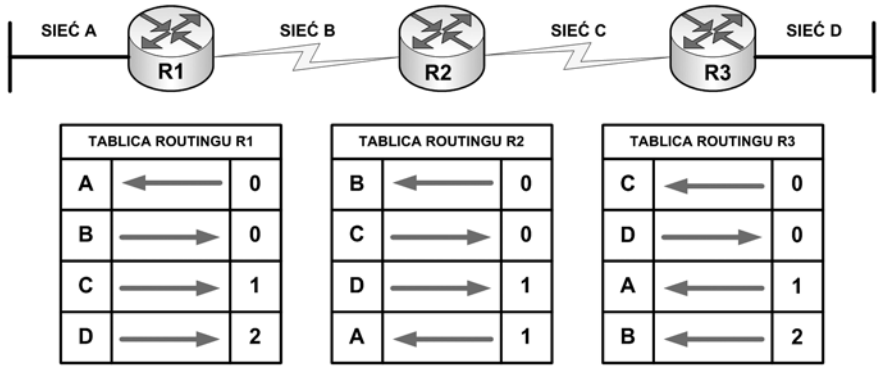
PROTOKOŁY ROUTINGU WEKTORA ODLEGŁOŚCI



Rysunek 30.
Parametry uwzględniane w protokołach routingu wektora odległości

Algorytm działający na podstawie wektora odległości okresowo przekazuje pomiędzy routerami kopie tablicy routingu. Takie regularne aktualizacje dokonywane pomiędzy routerami przekazują informacje o zmianach topologii. Algorytm routingu działający na podstawie wektora odległości znany jest jako **algorytm Bellmana-Forda**. Każdy router otrzymuje tablicę routingu od bezpośrednio z nim połączonych routerów sąsiednich. Router R2 odbiera informacje od routera R1, po czym dodaje wartość wektora odległości, na przykład liczbę przeskoków. Liczba ta zwiększa wektor odległości. Następnie router R2 przekazuje nową tablicę routingu innemu sąsiadowi, routerowi R3 a ten przekazuje dalej do routera R4. Ten sam proces zachodzi we wszystkich kierunkach pomiędzy sąsiednimi routerami (patrz rys. 30). Algorytm powoduje w efekcie zebranie sumarycznych informacji o odległościach dzielących sieci, dzięki czemu możliwe jest utrzymywanie bazy danych topologii sieci. Jednakże algorytm działający na podstawie wektora odległości nie umożliwia routerowi poznania dokładnej topologii sieci, ponieważ każdy router widzi jedynie swe routery sąsiednie.

DZIAŁANIE PROTOKOŁU ROUTINGU WEKTORA ODLEGŁOŚCI



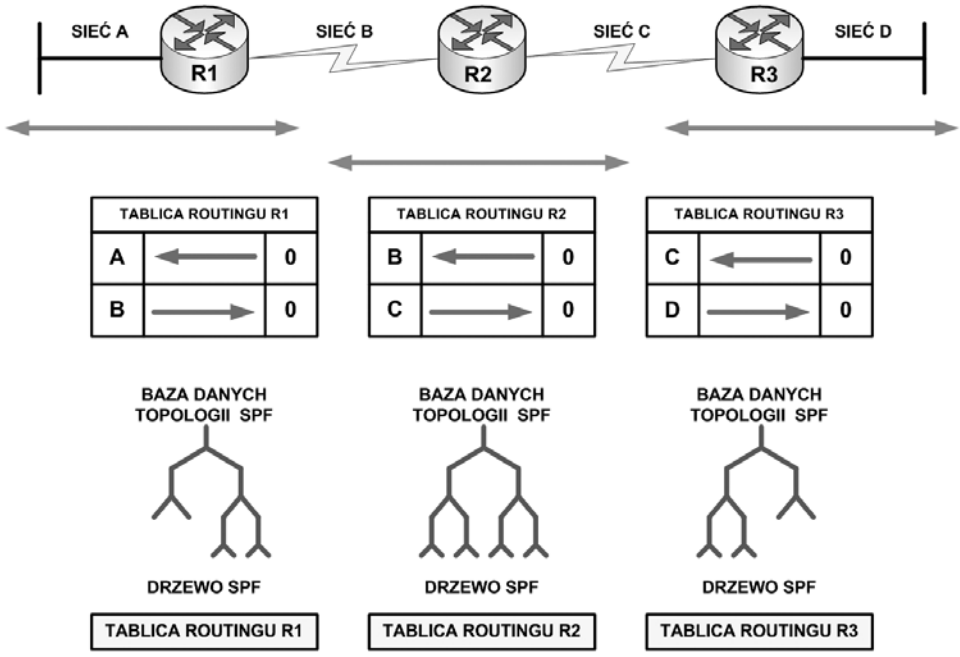
Rysunek 31.
Podgląd tablic routingu z wykorzystaniem algorytmu Bellmana-Forda

Każdy router korzystający z routingu działającego na podstawie wektora odległości w pierwszej kolejności identyfikuje swoich sąsiadów. Interfejs prowadzący do każdej bezpośrednio podłączonej sieci ma odległość administracyjną równą 0.

W miarę postępu procesu rozpoznawania opartego na algorytmie wektora odległości, na podstawie informacji otrzymanych od swoich sąsiadów, router ustala najlepsze trasy do sieci docelowych (patrz rys. 31). Router R1 zapamiętuje informacje o innych sieciach w oparciu o dane odebrane z routera R2 i tak dalej. Każda z pozycji reprezentujących inną sieć w tablicy routingu ma przypisany skumulowany wektor odległości pokazujący, jak daleko w danym kierunku znajduje się ta sieć. Aktualizacje tablic routingu następują w przypadku zmian topologii sieci. Tak jak w przypadku procesu wykrywania sieci, aktualizacje topologii sieci postępują od routera do routera.

Algorytmy działające na podstawie wektora odległości nakazują każdemu routerowi wysłanie swojej tablicy routingu do każdego z sąsiednich routerów. Tablice routingu zawierają informacje na temat całkowitego kosztu ścieżki zdefiniowanego przez jego metrykę oraz adresu logicznego pierwszego routera na drodze do każdej sieci zawartej w tablicy.

DZIAŁANIE PROTOKOŁU ROUTINGU STANU ŁĄCZA



Rysunek 32.
Parametry uwzględniane w protokołach routingu stanu łącza

Algorytm stanu łącza jest również znany jako **algorytm Dijkstry** lub algorytm **SPF** (ang. *Shortest Path First*). Routing stanu łącza wykorzystuje następujące elementy (patrz rys. 32):

1. Ogłoszenie LSA (ang. *Link-state advertisement*) – mały pakiet informacji o routingu wysyłany pomiędzy routerami.
2. Baza danych topologii – zbiór informacji zebranych na podstawie ogłaszania LSA.
3. Algorytm SPF – obliczenia wykonywane na podstawie informacji z bazy danych, dające w wyniku drzewo SPF.
4. Tablica routingu – lista znanych ścieżek i interfejsów.

Proces wymiany informacji LSA między routerami rozpoczyna się od bezpośrednio połączonych sieci, co do których zostały zgromadzone informacje. Każdy router tworzy bazę danych topologii składającą się z wszystkich informacji LSA.

Algorytm SPF oblicza osiągalność danej sieci. Router tworzy topologię logiczną w postaci drzewa, w którym sam zajmuje główną pozycję. Topologia ta składa się z wszystkich możliwych ścieżek do każdej sieci w intersieci protokołu stanu łącza. Następnie router sortuje ścieżki za pomocą algorytmu SPF – umieszcza najlepsze ścieżki i interfejsy do tych sieci docelowych w tablicy routingu. Utrzymuje również inną bazę danych elementów topologii i szczegółów stanu.

Pierwszy router, który otrzyma informację o zmianie topologii stanu łącza, przekazuje ją dalej, aby pozostałe routery mogły dokonać na jej podstawie aktualizacji. Wspólne informacje o routingu są wysyłane do wszystkich routerów w intersieci. Aby osiągnąć zbieżność, każdy router gromadzi informacje o sąsiednich routerach. Obejmują one nazwę każdego sąsiedniego routera, stan interfejsu oraz koszt łącza do sąsiada. Router tworzy pakiet LSA zawierający tę informację oraz dane o nowych sąsiadach, zmianach w koszcie łącza oraz o łączach, które nie są już aktualne. Pakiet LSA jest następnie wysyłany, aby pozostałe routery go odebrały. Gdy router odbierze pakiet LSA, aktualizuje tablicę routingu z użyciem bieżących informacji. Skumulowane dane służą do utworzenia mapy intersieci, a algorytm SPF jest używany do obliczenia najkrótszej ścieżki do innych sieci. Za każdym razem, gdy pakiet LSA powoduje zmianę bazy danych stanu łącza, za pomocą algorytmu SPF oblicza się najlepszą ścieżkę i aktualizuje tablicę routingu.

Z protokołami stanu łącza związane są następujące trzy zasadnicze problemy:

- zużycie czasu procesora,
- zapotrzebowanie na pamięć,
- zużycie pasma.

Routery wykorzystujące protokoły stanu łącza wymagają większej ilości pamięci i przetwarzają więcej danych, niż te wykorzystujące protokoły routingu działające na podstawie wektora odległości. Routery stanu łącza wymagają większej ilości pamięci do przechowywania wszystkich informacji z różnych baz danych, drzewa topologii i tablicy routingu. Początkowy rozpływ pakietów stanu łącza wymaga przesłania dużej ilości danych. W trakcie początkowego procesu wykrywania wszystkie routery korzystające z protokołów routingu według stanu łącza wysyłają pakiety LSA do pozostałych routerów. Powoduje to zalewanie intersieci i tymczasowo zmniejsza pasmo dostępne dla ruchu routowanego przenoszącego dane użytkowe. Po początkowym rozpływie protokoły routingu według stanu łącza wymagają minimalnej ilości pasma do sporadycznego lub wyzwalanego zdarzeniami wysyłania pakietów LSA odzwierciedlających zmiany topologii.

ODLEGŁOŚĆ ADMINISTRACYJNA TRASY

W miarę gromadzenia uaktualnień w procesie routingu, router wybiera najlepszą ścieżkę do dowolnego celu i próbuje dodać ją do tablicy routingu. Router decyduje, co zrobić z trasami dostarczanymi przez procesy routingu w oparciu o odległość administracyjną trasy. Jeśli dana ścieżka ma najmniejszą odległość administracyjną do danego celu, jest dodawana do tablicy routingu; jeśli tak nie jest, trasa jest odrzucana. W tabeli 1 zestawiono domyślne wartości dla protokołów obsługiwanych przez system Cisco IOS.

Tabela 1.
Wykaz wybranych wartości odległości administracyjnej trasy

Źródło trasy odległości administracyjnej	Odległość domyślna
DOŁĄCZONY BEZPOŚREDNIO INTERFEJS	0
TRASA STATYCZNA	1
SKONSOLIDOWANA TRASA PROTOKOŁU EIGRP	5
ZEWNĘTRZNA TRASA PROTOKOŁU BGP	20
WEWNĘTRZNA TRASA PROTOKOŁU EIGRP	90
PROTOKÓŁ IGRP	100
PROTOKÓŁ OSPF	110
PROTOKÓŁ IS-IS	115
PROTOKÓŁ RIP	120
ZEWNĘTRZNA TRASA PROTOKOŁU EIGRP	170
WEWNĘTRZNA TRASA PROTOKOŁU BGP	200
TRASA NIEZNANA	255

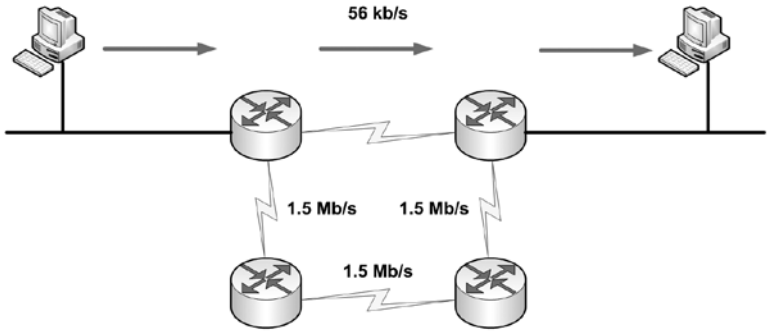
4. KONFIGURACJA PROTOKOŁÓW ROUTINGU RIPV1 I RIPV2

PROTOKÓŁ ROUTINGU RIP

Protokół RIP (ang. *Routing Information Protocol*) opisany po raz pierwszy w dokumencie RFC 1058 przeszedł ewolucję od klasowego protokołu routingu RIP w wersji 1 (RIP v1) do bezklasowego protokołu routingu RIP w wersji 2 (RIP v2). W celu zapobieżenia nieskończonym pętlom routingu, w protokole RIP ograniczono liczbę dopuszczalnych przeskoków na ścieżce od źródła do celu do 15. Gdy router otrzymuje aktualizację routingu zawierającą nową albo zmienioną pozycję, zwiększa wartość metryki o 1, aby uwzględnić siebie jako przeskok na ścieżce. Jeśli wartość metryki przekroczy 15, cel w sieci jest uznawany za niedostępny.

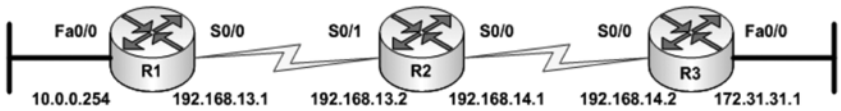
DZIAŁANIE PROTOKOŁU RIP

Na rysunku 33 ścieżka o prędkości 56 kb/s między dwoma hostami używającymi górnych routerów jest równa dwóm skokom. Niższa, zastępcza ścieżka, używająca trzech łączy T1 (1.5 Mb/s) jest równa czterem skokom. Ponieważ wybór ścieżki przez RIP jest oparty wyłącznie na liczbie skoków, w tym przypadku wybrane zostanie łącze o prędkości 56 kbps, a nie znacznie szybsze łącze T1.



Rysunek 33.
Działanie protokołu routingu dynamicznego RIP

KONFIGUROWANIE PROTOKOŁU RIPV1




```
R1(config)# router rip
R1(config-router)# network 10.0.0.0
R1(config-router)# network 192.168.13.0

R2(config)# router rip
R2(config-router)# network 192.168.14.0
R2(config-router)# network 192.168.13.0

R3(config)# router rip
R3(config-router)# network 192.168.14.0
R3(config-router)# network 172.31.0.0
```

Rysunek 34.
Przykład konfiguracji protokołu RIP w wersji 1

Polecenie **router rip** uaktywnia protokół RIP jako protokół routingu (patrz rys. 34). Następnie używane jest polecenie **network** określające, na których interfejsach ma działać protokół RIP.

Proces routingu wiąże określone interfejsy adresami sieciowymi rozpoczyna wysyłanie odbieranie aktualizacji RIP na tych interfejsach. Protokół RIP wysyła aktualizacje routingu w regularnych odstępach czasu. Po odebraniu aktualizacji tras zawierającej zmianę pozycji router aktualizuje swoją tablicę routingu, aby uwzględnić nową trasę. Odebrana wartość metryki dla ścieżki jest zwiększana o 1, a jako następny przeskok w tablicy routingu jest wskazywany interfejs źródłowy tej aktualizacji.

Na routerach RIP jest przechowywana informacja tylko o najlepszej ścieżce do celu, ale w przypadku ścieżek o równych kosztach przechowywanych może być ich kilka. W przypadku większości protokołów routingu aktualizacje są generowane czasowo oraz zdarzeniowo. Protokół RIP jest sterowany czasowo, ale w implementacji firmy Cisco tego protokołu w przypadku wykrycia zmiany wysyłane są wyzwalane aktualizacje.

Zmiany topologii wyzwalają natychmiastowe aktualizacje, które nie zależą od zegara aktualizacji, również w routerach IGRP. Bez takich aktualizacji protokoły RIP i IGRP działałyby mniej efektywnie. Po aktualizacji tablicy z powodu zmiany konfiguracji router natychmiast wysyła aktualizacje tras, aby poinformować inne routery o tej zmianie. Aktualizacje te, zwane aktualizacjami wyzwalanymi, są wysyłane dodatkowo oprócz aktualizacji zaplanowanych wysyłanych przez router RIP.Aby włączyć protokół RIP, należy w trybie konfiguracji globalnej użyć następujących poleceń:

Router(config)# router rip – włącza proces routingu RIP,
Router(config-router)# network *numer_sieci* – tworzy powiązanie sieci z procesem RIP

KONFIGUROWANIE PROTOKOŁU RIPV2

W wersji protokołu RIPv2 wprowadzono następujące rozszerzenia:

1. Możliwość przenoszenia dodatkowych informacji o routingu pakietów.

2. Mechanizm uwierzytelniania zabezpieczający tablice routingu.
3. Obsługa techniki masek podsieci o zmiennej długości (VLSM).

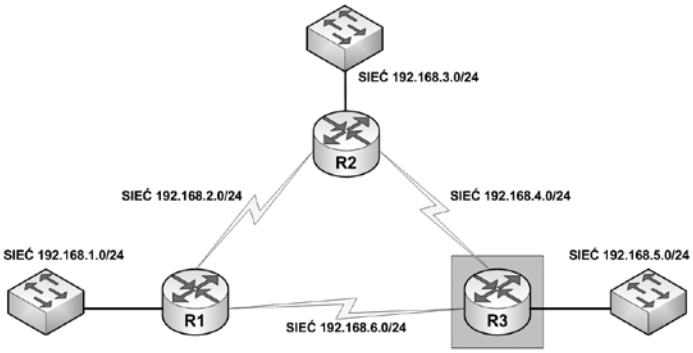

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 10.0.0.0
R1(config-router)# network 192.168.13.0

R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 192.168.14.0
R2(config-router)# network 192.168.13.0

R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# network 192.168.14.0
R3(config-router)# network 172.31.0.0
```

Rysunek 35.
Przykład konfiguracji protokołu RIP w wersji 2

Aby włączyć protokół RIPv2, należy w trybie konfiguracji globalnej użyć następujących poleceń (patrz rys. 35):

Router(config)# router rip – włącza proces routingu RIP
Router(config)# version 2
Router(config-router)# network *numer_sieci* – tworzy powiązanie sieci z procesem RIP

WERYFIKOWANIE KONFIGURACJI PROTOKOŁU RIP




```
R3#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 192.168.6.2, 00:00:05, Serial0/0/0
R    192.168.2.0/24 [120/1] via 192.168.6.2, 00:00:05, Serial0/0/0
                    [120/1] via 192.168.4.2, 00:00:05, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:05, Serial0/0/1
C    192.168.4.0/24 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
C    192.168.6.0/24 is directly connected, Serial0/0/0
```

Rysunek 36.
Przykład weryfikacji poprawności działania protokołu RIP

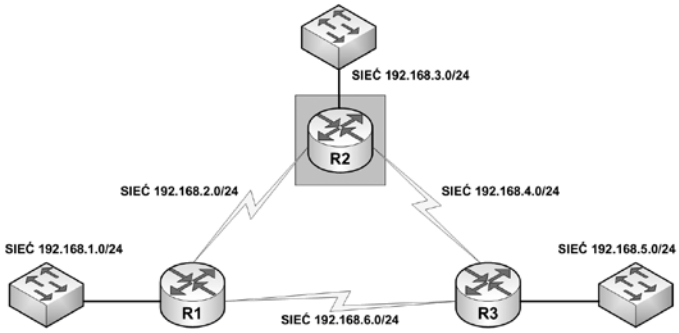
Polecenie **show ip route** umożliwia sprawdzenie, czy trasy odbierane od sąsiednich urządzeń używających protokołu RIP znajdują się w tablicy routingu (patrz rys. 36). W danych wyjściowych polecenia należy poszukać tras RIP, które są oznaczone literą R. Należy pamiętać o tym, że uzyskanie zbieżności trochę trwa, więc trasy mogą nie pojawić się natychmiast.

```
R3#show ip protocols
Routing Protocol is "rip"
(**output omitted**)

  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       1     1 2
    Serial0/0/0           1     1 2
    Serial0/0/1           1     1 2
  Automatic network summarization is in effect
  Routing for Networks:
    192.168.4.0
    192.168.5.0
    192.168.6.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.6.2          120      00:00:10
    192.168.4.2          120      00:00:18
  Distance: (default is 120)
```

Rysunek 37.
Podgląd wykonania polecenia **show ip protocols** na routerze R3

Polecenie **show ip protocols** pokazuje, które protokoły routingu przenoszą ruch IP w routerze. Danych tych można użyć do sprawdzenia ustawień konfiguracji protokołu RIP. Najczęściej sprawdzane są następujące elementy konfiguracji:

1. Konfiguracja protokołu RIP.
2. Wysyłanie i odbieranie aktualizacji protokołu RIP przez właściwe interfejsy.
3. Ogłaszanie właściwych sieci przez router.




```
R2#debug ip rip
RIP protocol debugging is on
RIP: received v1 update from 192.168.2.1 on Serial0/0/0
     192.168.1.0 in 1 hops
RIP: received v1 update from 192.168.4.1 on Serial0/0/1
     192.168.5.0 in 1 hops
RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.3.1)
RIP: build update entries
     network 192.168.1.0 metric 2
     network 192.168.2.0 metric 1
     network 192.168.4.0 metric 1
     network 192.168.5.0 metric 2
RIP: sending  v1 update to 255.255.255.255 via Serial0/0/1 (192.168.4.2)
RIP: build update entries
     network 192.168.1.0 metric 2
     network 192.168.2.0 metric 1
     network 192.168.3.0 metric 1
RIP: sending  v1 update to 255.255.255.255 via Serial0/0/0 (192.168.2.2)
RIP: build update entries
     network 192.168.3.0 metric 1
     network 192.168.4.0 metric 1
     network 192.168.5.0 metric 2
R2#undebug all
All possible debugging has been turned off
```

Rysunek 38.
Podgląd wykonania polecenia **debug ip rip** na routerze R2

Polecenie **debug ip rip** umożliwia diagnostykę takich problemów, jak nieciągłość podsieci lub powielone sieci. Objawem takich problemów może być router, który ogłasza metrykę mniejszą niż sam odebrał dla danej sieci.

5. KONFIGURACJA PROTOKOŁU ROUTINGU IGRP

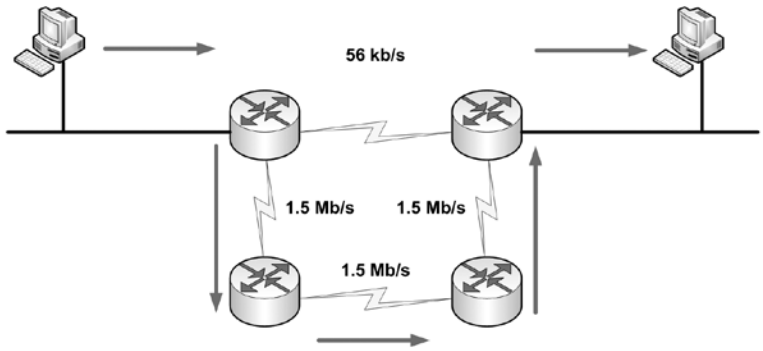
PROTOKÓŁ ROUTINGU IGRP

Protokół routingu IGRP (ang. *Interior Gateway Routing Protocol*) jest zaprojektowanym przez firmę Cisco protokołem routingu opartym na wektorze odległości. Protokół IGRP wysyła aktualizacje tras w odstępach 90-sekundowych. Aktualizacje te ogłaszają wszystkie sieci wchodzące w skład danego systemu autonomicznego (AS). Protokół IGRP ma następujące cechy:

1. Łatwość automatyzacji w przypadku niezdefiniowanych, złożonych topologii.
2. Elastyczność wymagana w przypadku segmentów o różnych przepustowościach i charakterystykach opóźnień.
3. Skalowalność umożliwiająca pracę w wielkich sieciach.
4. Obsługuje tylko routing klasowy.

Protokół IGRP używa złożonej metryki obliczanej przy użyciu pasma, opóźnienia, obciążenia i niezawodności. Domyślnie wykorzystywane jest tylko pasmo i opóźnienie; pozostałe parametry są brane pod uwagę tylko wtedy, gdy zostały auktywnione w procesie konfiguracji. Opóźnienie i pasmo nie są wartościami mierzalnymi, ale ustawianymi za pomocą poleceń **delay** i **bandwidth interface**.

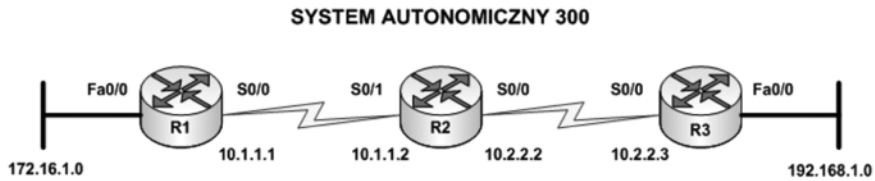
DZIAŁANIE PROTOKOŁU IGRP



Rysunek 39.
Działanie protokołu routingu dynamicznego IGRP

Na rysunku 39, ścieżka o prędkości 56 kb/s między dwoma hostami używającymi górnych routerów jest równa dwóm skokom. Niższa ścieżka używająca trzech łączy T1 (1.5 Mb/s) jest równa czterem skokom. Ponieważ wybór ścieżki przez IGRP jest oparty głównie na szybkości transmisji danych, w tym przypadku wybrane zostanie łącze o prędkości 1.5 Mb/s, a nie znacznie wolniejsze łącze (chociaż krótsze) o przepływności 56 kb/s.

KONFIGUROWANIE PROTOKOŁU IGRP




```
R1(config)# router igrp 300
R1(config-router)# network 172.16.0.0
R1(config-router)# network 10.0.0.0

R2(config)# router igrp 300
R2(config-router)# network 10.0.0.0

R3(config)# router igrp 300
R3(config-router)# network 192.168.1.0
R3(config-router)# network 10.0.0.0
```

Rysunek 40.
Przykład konfiguracji protokołu routingu dynamicznego IGRP

Aby skonfigurować proces **routingu IGRP**, należy użyć polecenia konfiguracyjnego **router igrp**. Aby usunąć proces routingu IGRP, należy poprzedzić to polecenie słowem kluczowym **no**. Polecenia te mają następującą składnię:

RouterA(config)#router igrp ***numer_as***
RouterA(config)#no router igrp ***numer_as***

Numer systemu autonomicznego (AS) jest identyfikatorem procesu IGRP. Jest on również używany do oznaczania informacji o routingu. Aby określić listę sieci dla procesów routingu IGRP, należy użyć polecenia konfiguracyjnego network. Aby usunąć pozycję, należy poprzedzić to polecenie słowem kluczowym **no**. Na rysunku 40 pokazano przykład konfiguracji protokołu IGRP dla systemu AS 300.

6. KONFIGURACJA PROTOKOŁU ROUTINGU EIGRP

PROTOKÓŁ ROUTINGU EIGRP

EIGRP to protokół routingu firmy Cisco oparty na protokole IGRP. EIGRP obsługuje bezklasowy routing międzydomenowy CIDR oraz technikę VLSM, dzięki czemu projektanci sieci mogą optymalizować wykorzystanie przestrzeni adresowej. W porównaniu z protokołem IGRP, który jest klasowym protokołem routingu, EIGRP zapewnia szybszą zbieżność, lepszą skalowalność i lepsze zarządzanie pętlami routingu. Jest on często określany mianem protokołu hybrydowego, jako że łączy najlepsze cechy algorytmów routingu z wykorzystaniem wektora odległości i według stanu łącza.

Protokół EIGRP to zaawansowany protokół routingu wykorzystujący funkcje typowe dla protokołów działających według stanu łącza. Niektóre najważniejsze funkcje protokołu OSPF, takie jak częściowe aktualizacje czy wykrywanie sąsiednich urządzeń, są wykorzystywane w podobny sposób w protokole EIGRP. Protokół EIGRP jest jednak łatwiejszy w konfiguracji.

EIGRP to idealne rozwiązanie dla dużych sieci korzystających z wielu protokołów i opartych głównie na routerach Cisco. Działanie protokołu EIGRP odbiega znacznie od funkcjonowania protokołu IGRP. EIGRP to zaawansowany protokół routingu wykorzystujący wektor odległości. Działa on jednak również jako protokół stanu łącza, ponieważ w podobny sposób wysyła aktualizacje do sąsiednich urządzeń i przechowuje informacje o routingu. Poniżej zestawiono zalety protokołu EIGRP w porównaniu z prostymi protokołami wektora odległości:

- szybsze osiąganie zbieżności,
- lepsze wykorzystanie pasma,
- obsługa techniki VLSM i protokołu CIDR,
- obsługa wielu warstw sieci,
- niezależność od protokołów routowanych.

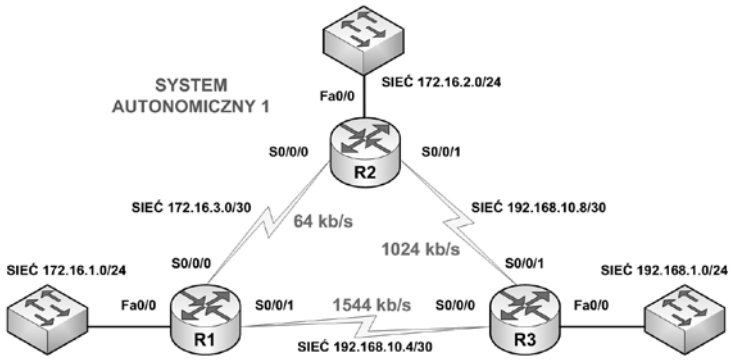
Routery wyposażone w protokół EIGRP szybciej osiągają zbieżność, ponieważ korzystają z algorytmu DUAL. Algorytm ten gwarantuje pracę bez zapętleń przez cały czas obliczania trasy, dzięki czemu wszystkie routery uczestniczące w zmianie topologii mogą dokonać synchronizacji w tym samym czasie.

Protokół EIGRP wysyła częściowe, ograniczone aktualizacje oraz efektywnie wykorzystuje pasmo. Gdy sieć jest stabilna, pasmo jest obciążane w minimalnym stopniu. Routery EIGRP nie wysyłają całych tablic, ale jedynie częściowe, przyrostowe aktualizacje. Przypomina to działanie protokołu OSPF. Różnica polega na tym, że routery EIGRP wysyłają częściowe aktualizacje tylko do routerów wymagających zawartych w nich informacji, a nie do wszystkich routerów w danym obszarze. Z tego względu aktualizacje te są nazywane aktualizacjami ograniczonymi. Do zachowania kontaktu między sobą routery EIGRP nie używają okresowych aktualizacji tras, ale niewielkich pakietów hello. Mimo iż pakiety te są przesyłane między routerami w regularnych odstępach czasu, nie zajmują one istotnej części pasma.

KONFIGUROWANIE PROTOKOŁU EIGRP

Aby skonfigurować protokół EIGRP dla protokołu IP, należy wydać następujące polecenie (patrz rys. 41):

Router(config)#router eigrp ***numer_as***




```
R1(config)# router eigrp 1
R1(config-router)# network 172.16.0.0
R1(config-router)# network 192.168.10.0

R2(config)# router eigrp 1
R2(config-router)# network 172.16.0.0
R2(config-router)# network 192.168.10.8

R3(config)# router eigrp 1
R3(config-router)# network 192.168.10.0
R3(config-router)# network 192.168.1.0
```

Rysunek 41.
Przykład konfiguracji protokołu routingu dynamicznego EIGRP

Numer systemu autonomicznego identyfikuje wszystkie routery należące do danej intersieci. Wartość ta musi być taka sama na wszystkich routerach w intersieci.

Wskaż na lokalnym routerze, które sieci należą do autonomicznego systemu EIGRP, wpisując następujące polecenie:

Router(config-router)#network ***numer_sieci***

Numer sieci określa, które interfejsy routera uczestniczą w systemie EIGRP i które sieci są ogłaszane przez router. Polecenie **network** powoduje skonfigurowanie tylko przyłączonych sieci.

Podczas konfigurowania łączy szeregowych za pośrednictwem protokołu EIGRP należy również skonfigurować ustawienia przepustowości interfejsu. Jeśli wartość przepustowości interfejsu nie zostanie zmieniona, protokół EIGRP przyjmie dla łącza pasmo domyślne zamiast faktycznego.

Gdy łącze będzie wolniejsze, router może nie być w stanie osiągnąć zbieżności, może następować utrata aktualizacji tras lub może mieć miejsce nieoptymalny wybór tras. Aby ustawić wartość przepustowości interfejsu, użyj następującego polecenia:

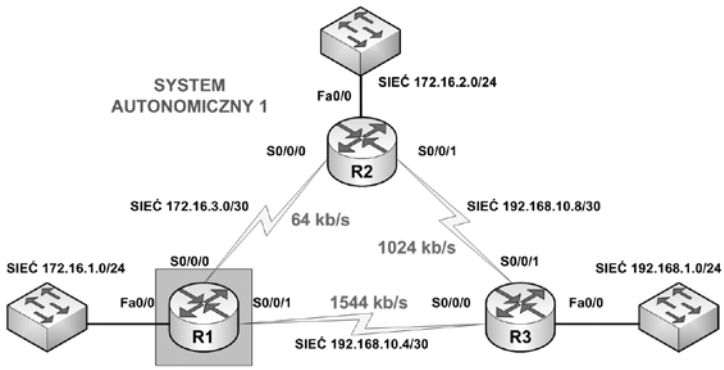
Router(config-if)#*bandwidth kbps*

Polecenie **bandwidth** jest wykorzystywane tylko przez proces routingu. Podawana wartość powinna odpowiadać szybkości łącza interfejsu.

WERYFIKOWANIE KONFIGURACJI PROTOKOŁU EIGRP

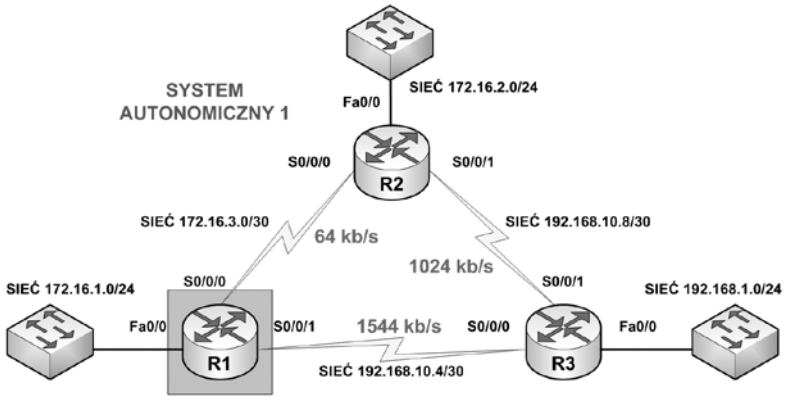
Polecenie **show ip route** umożliwia sprawdzenie, czy trasy odbierane od sąsiednich urządzeń używających protokołu EIGRP znajdują się w tablicy routingu. W danych wyjściowych polecenia należy poszukać tras EIGRP, które są oznaczone literą D. Należy pamiętać o tym, że uzyskanie zbieżności trochę trwa, więc trasy mogą nie pojawić się natychmiast. Na rysunku 42 pokazano wymienione informacje dla routera R1.

Polecenie **show ip protocols** wyświetla parametry i aktualny stan aktywnego protokołu routingu (patrz rys. 43). Użycie tego polecenia powoduje wyświetlenie numeru systemu autonomicznego protokołu EIGRP. Wyświetlane są również numery dla funkcji filtrowania i redystrybucji, jak również informacje o sąsiednich urządzeniach i odległościach.




```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
<Output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:03:50, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/2681856] via 192.168.10.6, 00:02:43, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:10:52, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/2172416] via 172.16.3.2, 00:10:47, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:02:31, Serial0/0/1
```

Rysunek 42.
Podgląd wydania polecenia **show ip route** na routerze R1




```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  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 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.10.0/24 for FastEthernet0/0, Serial0/0/0
      Summarizing with metric 2169856
    172.16.0.0/16 for Serial0/0/1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:03:29
    192.168.10.6          90      00:02:09
    Gateway         Distance      Last Update
    172.16.3.2            90      00:02:12
  Distance: internal 90 external 170
```

Rysunek 43.
Podgląd wydania polecenia **show ip protocols** na routerze R1

7. KONFIGURACJA PROTOKOŁU ROUTINGU OSPF

PROTOKÓŁ ROUTINGU OSPF

Zasada działania protokołów routingu według stanu łącza jest inna niż w przypadku protokołów działających na podstawie wektora odległości. Algorytm routingu według stanu łącza utrzymuje skomplikowaną bazę danych zawierającą informacje o topologii. Podczas gdy algorytmy działające w oparciu o wektor odległości gromadzą ogólne informacje na temat odległych sieci i nie dają wiedzy na temat odległych routerów, algorytm routingu według stanu łącza dysponuje pełną informacją o odległych routerach i ich wzajemnych połączeniach.

Protokoły routingu według stanu łącza zbierają informacje o trasach od pozostałych routerów znajdujących się w sieci lub w zdefiniowanym obszarze sieci. Po zgromadzeniu tych informacji każdy router oblicza najlepszą trasę do każdego miejsca docelowego w sieci. Ponieważ każdy z routerów ma własny obraz sieci, prawdopodobieństwo propagacji nieprawidłowych informacji dostarczonych przez któryś z sąsiednich routerów jest mniejsze.

Protokół routingu według stanu łącza spełnia między innymi następujące funkcje:

1. Szybko reaguje na zmiany w sieci.
2. Wysyła aktualizacje wyzwalane jedynie po wystąpieniu zmian w sieci.
3. Cyklicznie wysyła aktualizacje (tzw. odświeżanie stanu łącza).
4. Używa mechanizmu hello do określania dostępności sąsiadów.

Każdy z routerów rozgłasza pakiety hello, aby móc śledzić stan sąsiednich routerów. Każdy z routerów używa ogłoszeń LSA (ang. *link-state adverisement*) do śledzenia stanu wszystkich routerów znajdujących się w obsługiwanym obszarze sieci. Pakiety hello zawierają informacje o sieciach dołączonych do routera.

Routery używające protokołów działających według stanu łącza mają następujące cechy:

1. Używają informacji zawartych w pakietach hello i ogłoszeniach LSA otrzymywanych od innych routerów do tworzenia bazy danych informacji o sieci.
2. Korzystają z algorytmu SPF do obliczania najkrótszej trasy do każdej sieci.
3. Przechowują informacje o trasach w tablicy routingu.

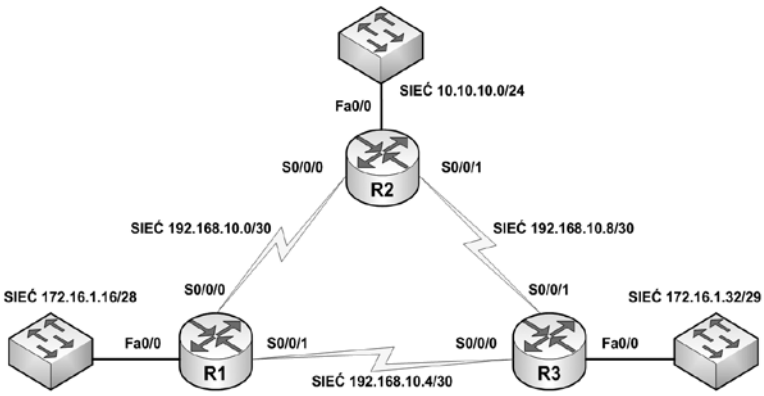
Protokoły routingu według stanu łącza mają następujące zalety:

1. Przy wyborze tras przez sieć protokoły routingu według stanu łącza używają metryki kosztu. Metryka kosztu odzwierciedla przepustowość łączy na tych trasach.
2. Protokoły routingu według stanu łącza używają wyzwalanych aktualizacji oraz rozpływowego przekazywania pakietów LSA, aby móc natychmiast powiadamiać wszystkie routery w sieci o zmianach jej topologii. Prowadzi to do szybkiej zbieżności.
3. Każdy router dysponuje pełnym i zsynchronizowanym obrazem sieci. Z tego powodu powstawanie pętli routingu jest bardzo utrudnione.
4. Routery dokonują wyboru najlepszych tras na podstawie najświeższych informacji.
5. Wielkość bazy danych stanu łączy można zmniejszyć, odpowiednio projektując sieć. Dzięki temu algorytm Dijkstry wymaga mniejszej ilości obliczeń, a osiągnięcie zbieżności zajmuje mniej czasu.
6. Każdy router dysponuje przynajmniej topologią własnego obszaru sieci. Ta cecha pozwala rozwiązywać pojawiające się problemy.
7. Protokoły routingu według stanu łącza obsługują notacje CIDR i VLSM.

Protokoły routingu według stanu łącza mają następujące wady:

1. Wymagają większej ilości pamięci i mocy obliczeniowej niż protokoły działające na podstawie wektora odległości. Na skutek tego koszty ich stosowania w organizacjach dysponujących mniejszym budżetem i starszym sprzętem są znacznie wyższe.
2. Wymagają ściśle hierarchicznego projektu sieci, gdzie sieć jest podzielona na mniejsze obszary w celu zmniejszenia tablic topologii.
3. Wymagają pracy administratora dobrze rozumiejącego działanie tych protokołów.
4. Podczas początkowego procesu wykrywania sieć jest zalewana pakietami LSA. Proces ten może znacząco zmniejszyć możliwość przesyłania danych w sieci. Może to w widoczny sposób obniżyć wydajność sieci.

KONFIGURACJA PROTOKOŁU OSPF




```
R1(config)# router ospf 1
R1(config-router)# network 172.16.1.16  0.0.0.15 area 0
R1(config-router)# network 192.168.10.0  0.0.0.3 area 0
R1(config-router)# network 192.168.10.4  0.0.0.3 area 0

R2(config)# router ospf 1
R2(config-router)# network 10.10.10.0  0.0.0.255 area 0
R2(config-router)# network 192.168.10.0  0.0.0.3 area 0
R2(config-router)# network 192.168.10.8  0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 172.16.1.32  0.0.0.7 area 0
R3(config-router)# network 192.168.10.4  0.0.0.3 area 0
R3(config-router)# network 192.168.10.8  0.0.0.3 area 0
```

Rysunek 44.
Przykładowa konfiguracja protokołu routingu dynamicznego OSPF

Do celów routingu, protokół OSPF wykorzystuje koncepcję obszarów. Każdy router zawiera pełną bazę danych stanów łączy dla danego obszaru. Obszarowi w sieci OSPF można przypisać dowolny numer z zakresu od 0 do 65 535. Jednemu z tych obszarów przypisuje się numer 0 – jest on znany jako „obszar zerowy". W sieci OSPF o wielu obszarach wszystkie obszary muszą łączyć się z obszarem 0. Obszar 0 nosi również nazwę obszaru szkieletowego.

Konfigurowanie protokołu OSPF wymaga włączenia procesu routingu OSPF na routerze oraz podaniu adresów sieci i informacji o obszarach. Adresy sieciowe są konfigurowane przy użyciu masek blankietowych, a nie masek podsieci. Maska blankietowa reprezentuje łącza lub adresy hostów, które mogą znajdować się w danym segmencie. Identyfikatory obszarów muszą być zapisywane w postaci pełnych liczb lub też w notacji kropkowo-dziesiętnej.

Aby włączyć routing OSPF, należy użyć polecenia konfiguracji globalnej o składni:

Router(config)#router ospf *id_procesu*

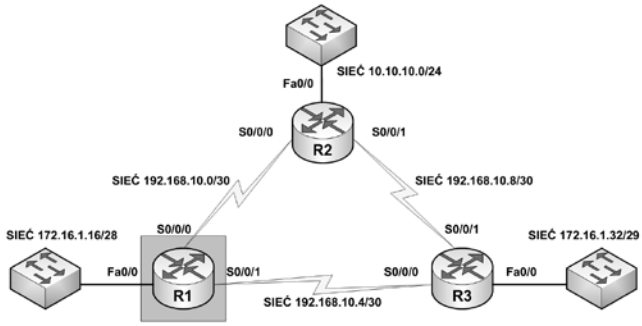
Identyfikator procesu jest liczbą używaną do identyfikacji procesu routingu OSPF na routerze. Na tym samym routerze można jednocześnie uruchomić wiele procesów OSPF. Liczba ta może przyjmować wartości z przedziału od 1 do 65 535. Większość administratorów sieci używa tego samego identyfikatora procesu w całym systemie autonomicznym, ale nie jest to obowiązkowe.

Rzadko zdarza się, że jest konieczne uruchomienie na routerze więcej niż jednego procesu OSPF. W protokole OSPF sieci IP są ogłaszane w następujący sposób:

Router(config-router)#network *adres maska odwrotna area id_obszaru*

Każda sieć musi być powiązana z obszarem, do którego należy. Adres sieci może być adresem całej sieci, podsieci lub adresem interfejsu. Maska odwrotna reprezentuje zbiór adresów hostów, które są obsługiwane w danym segmencie. Różni się ona od maski podsieci, która jest używana podczas konfigurowania adresów IP na interfejsach.

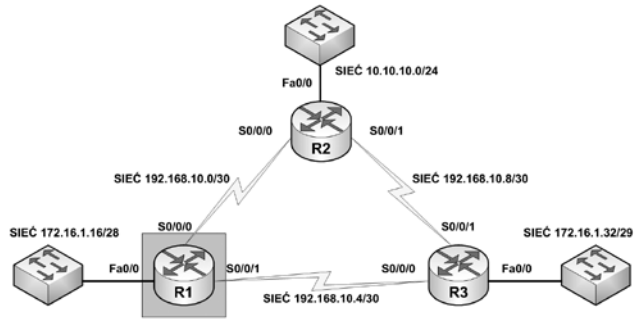
WERYFIKOWANIE KONFIGURACJI PROTOKOŁU OSPF




```
R1#show ip route
Codes:***output omitted***
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.2, 14:27:57, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/65] via 192.168.10.6, 14:27:57, Serial0/0/1
C       172.16.1.16/28 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.10.10.0/24 [110/65] via 192.168.10.2, 14:27:57, Serial0/0/0
C       10.1.1.1/32 is directly connected, Loopback0
```

Rysunek 45.
Weryfikacja konfiguracji protokołu OSPF

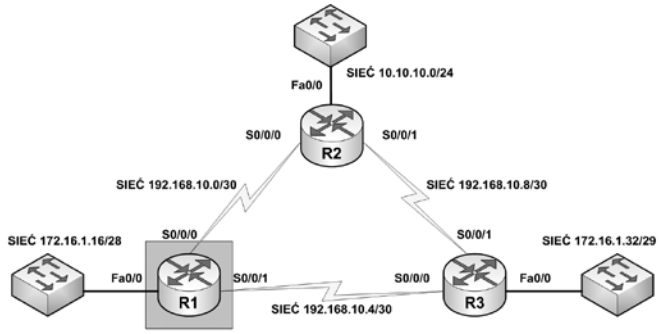
Polecenie **show ip route** służy do sprawdzenia, czy protokół OSPF wysyła i odbiera informacje o trasach. Litera O na początku każdego wpisu oznacza, że źródłem informacji o trasie jest protokół routingu dynamicznego stanu łącza OSPF (patrz rys. 45).




```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.16 0.0.0.15 area 0
    192.168.10.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2             110      11:29:29
    10.3.3.3             110      11:29:29
  Distance: (default is 110)
```

Rysunek 46.
Podgląd wydania polecenia **show ip protocols** na routerze R1

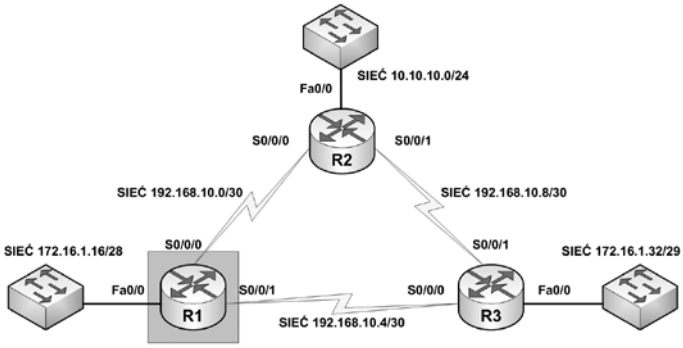
Polecenia **show ip protocols** używamy do sprawdzenia bieżącego identyfikatora routera. Ponadto polecenie to umożliwia sprawdzenie sieci rozgłaszanych przez dany router, sąsiadów od których router odbiera aktualizacje, oraz domyślną odległość administracyjną, która dla protokołu OSPF wynosi 110 (patrz rys. 46).




```
R1#show ip ospf
***output omitted***
 Routing Process "ospf 1" with ID 10.1.1.1
 Start time: 00:00:19.540, Time elapsed: 11:31:15.776
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 11:30:31.628 ago
        SPF algorithm executed 5 times
        Area ranges are
```

Rysunek 47.
Podgląd wydania polecenia **show ip ospf** na routerze R1

Polecenia **show ip ospf** używamy do sprawdzenia bieżącego identyfikatora routera. Ponadto polecenie to wyświetla informacje o obszarze OSPF oraz czas ostatniego przeliczenia algorytmu SPF (patrz rys. 47).




```
R1#show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
```

Rysunek 48.
Podgląd wydania polecenia **show ip ospf interface serial 0/0/0** na routerze R1

Najszybszym sposobem na sprawdzenie interwału hello i czasu uznania za nieczynny jest wydanie polecenia **show ip ospf interface**. Interwały te znajdują się w pakietach hello OSPF wymienianych między sąsiednimi routerami. Protokół OSPF może mieć różne interwały hello i czasy uznania za nieczynny na różnych interfejsach, ale żeby routery stały się sąsiadami, ich interwały hello i czasy uznania za nieczynny muszą być identyczne.

Na rysunku 48 widzimy, że na interfejsie serial 0/0/0 routera R1 skonfigurowano interwał hello o wartości 10 i czas uznania za nieczynny o wartości 40. Router R2 musi używać tych samych wartości na swoim interfejsie serial 0/0/0 aby routery te mogły utworzyć przyległość.

8. LITERATURA

1. Empson S., *Akademia sieci Cisco. CCNA Pełny przegląd poleceń*, WN PWN, Warszawa 2008
2. Graziani R., Johnson A., *Akademia sieci Cisco. CCNA Exploration. Semestr 2. Protokoły i koncepcje routingu*, WN PWN, Warszawa 2008
3. Józefiok A., *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2009
4. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
5. Mucha M., *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
6. Odom W., McDonald R., *CCNA semestr 2. Routery i podstawy routingu*, WN PWN, Warszawa 2007

WARSZTATY

1. RÓŻNE SPOSOBY ADRESOWANIA W SIECIACH KOMPUTEROWYCH

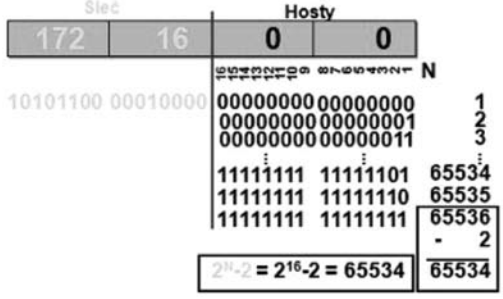
DZIAŁANIA NA PRZESTRZENI ADRESOWEJ IPV4

W celu zapewnienia poprawnego sposobu komunikacji pomiędzy urządzeniami w sieci komputerowej, każde z nich musi zostać zdefiniowane w jednoznaczny sposób. Niezbędnym jest również, aby każdy z pakietów tworzonych w warstwie sieciowej podczas komunikacji pomiędzy dwoma hostami zawierał zarówno adres urządzenia źródłowego jak i docelowego. W przypadku użycia protokołu IPv4 oznacza to, iż oba te 32-bitowe adresy zawarte są w nagłówku warstwy sieciowej. Dla użytkowników sieci, łańcuch 32-bitowy jest trudny do interpretacji i jeszcze trudniejszy do zapamiętania, zatem zwykle prezentujemy adresy IPv4 używając notacji dziesiętnej z kropkami.

OKREŚLANIE ADRESÓW SIECI, ADRESÓW ROZGŁOSZENIOWYCH ORAZ ADRESÓW HOSTÓW

ADRES SIECIOWY

Adres sieciowy jest standardowym sposobem odwoływania się do sieci. W przypadku sieci przedstawionej na rys. 49, możemy odwoływać się do niej używając nazwy „sieć 172.16.0.0". Adres sieci jest pierwszym (najniższym) adresem w zakresie adresów związanych z daną siecią. Jest to sposób jednoznacznie określający sieć oraz informujący, iż wszystkie hosty pracujące w sieci 10.0.0.0 będą miały takie same bity w polu sieciowym adresu. W zakresie adresów IPv4 związanych z daną siecią, pierwszy (najniższy) adres zarezerwowany jest dla adresu sieciowego. W adresie tym wszystkie bity w polu hosta mają wartość 0.



Rysunek 49.
Interpretacja zapisu adresu sieci i adresu rozgłoszeniowego

Ćwiczenie 1. Wyodrębnić z podanych przykładowych adresów, adresy sieci (uwzględniając klasowy schemat adresowania):

193.168.12.212
213.89.73.255
176. 16.0.0
11.10.10.10

ADRES ROZGŁOSZENIOWY

Adres rozgłoszeniowy IPv4 jest specjalnym adresem występującym w każdej sieci, umożliwiającym jednoczesne komunikowanie się ze wszystkimi hostami w danej sieci. Oznacza to, iż aby wysłać dane do wszystkich urządzeń końcowych w danej sieci, host wysyła pojedynczy pakiet zaadresowany adresem rozgłoszeniowym. Adres rozgłoszeniowy jest ostatnim (najwyższym) adresem w zakresie adresów związanych z daną siecią. Jest to adres, w którym wszystkie bity znajdujące się w polu hosta mają wartość 1. W przypadku sieci 172.16.0.0, adres rozgłoszeniowy będzie miał postać 172.16.255.255. Adres ten określany jest również jako rozgłoszenie skierowane (ang. *directed broadcast*).

Ćwiczenie 2. Wyodrębnić z podanych przykładów adresów, adresy rozgłoszeniowe (uwzględniając klasowy schemat adresowania):

199.12.13.254
173.100.0.0
100.255.255.255
1.10.1.255

OPERACJA KONIUNKCJI (AND)

W celu sprawdzenia w jakiej sieci znajduje się dany adres IP stosujemy logiczny AND między adresem IP a jego maską. Podstawowe działania na AND:

0 AND 0 = 0
0 AND 1 = 0
1 AND 0 = 0
1 AND 1 = 1

Zatem adres 192.168.1.1 z maską 255.255.255.0 potraktowany AND ma następująca postać:

11000000.10101000.00000001.00000001 (adres 192.168.1.1)
AND
11111111.11111111.11111111.00000000 (maska 24 bitowa)
wynik
11000000.10101000.00000001.00000000 (czyli 192.168.1.0)

Ćwiczenie 3. Wyodrębnić z podanych przykładów, za pomocą operacji koniunkcji, adresy sieci:

11.11.125.121/16
175.168.11.12/24
1.1.10.1/8

ADRESY HOSTÓW

Każde urządzenie końcowe (w rozumieniu sieci komputerowych) musi być jednoznacznie określone za pomocą unikatowego adresu, aby móc dostarczyć do niego wysyłany pakiet. W adresacji IPv4 urządzenia końcowe pracujące w danej sieci, mogą mieć przypisane adresy z zakresu ograniczonego adresem sieciowym oraz rozgłoszeniowym.

Ćwiczenie 4. Obliczyć z wykorzystaniem podanych przykładów adresów użyteczne zakresy adresów dla hostów (uwzględniając klasowy schemat adresowania):

192.168.0.0
172.16.0.0
199.199.199.255
10.10.10.10

Ćwiczenie 5. Projektowanie sieci o określonej liczbie hostów.
Założenia:

- przestrzeń adresowa 172.16.0.0/16
- sieć LAN1: 500 hostów
- siec LAN2: 150 hostów
- siec LAN3 100 hostów
- siec LAN4 100 hostów
- sieć LAN5 60 hostów
- sieć LAN6 20 hostów
- sieć WAN1, 2, 3, są to sieci point-to-point

Zadanie do wykonania:
Zaprojektować schemat adresacji zaczynając od sieci największej a kończąc na najmniejszej zachowując zasadę, że powinniśmy zachować jak najwięcej adresów na przyszły rozwój sieci. Określić adresy sieci, maski oraz zakresy dla adresów użytecznych.

Ćwiczenie 6. Projektowanie wymaganej liczby sieci przy opisanej przestrzeni adresowej.
Założenia:

- przestrzeń adresowa 192.168.1.0/24
- 5 maksymalnie dużych sieci LAN
- 4 point-to-point sieci WAN

Zadanie do wykonania:
Zaprojektować schemat adresacji zgodnie z wymaganiami. Określić adresy sieci, maski oraz zakresy dla adresów użytecznych.

DZIAŁANIA NA PRZESTRZENI ADRESOWEJ IPV6

IPv6 (ang. *Internet Protocol version 6*) to najnowsza wersja protokołu IP, będąca następcą IPv4, do którego stworzenia przyczynił się w głównej mierze problem małej, kończącej się ilości adresów IPv4. Dodatkowymi zamierzeniami było udoskonalenie protokołu IP: eliminacja wad starszej wersji, wprowadzenie nowych rozszerzeń (uwierzytelnienie, zlikwidowanie konieczności stosowania translacji adresów i adresów prywatnych w wielu sieciach, kompresja i inne), zminimalizowanie czynności wymaganych do podłączenia nowego węzła do Internetu (autokonfiguracja). IPv6 zapewnia większą spójność infrastruktury sieciowej, uproszczenie zasad adresowania, odporność na błędy oraz gotowe mechanizmy bezpieczeństwa.

STRUKTURA PRZESTRZENI ADRESOWEJ IPV6

Przestrzeń adresowa IPv6 została rozszerzona z 32 do 128 bitów. Tak długi adres byłby trudny do zapisania w sposób znany z IPv4, a tym bardziej do zapamiętania. Aby usprawnić operowanie nowymi adresami, wprowadzono pewne modyfikacje. Adres 128-bitowy grupuje się po 2 bajty i oddziela dwukropkiem. Tak wyodrębnione bloki 16-bitowe konwertuje się na postać szesnastkową:

0034:0000:A132:827C:0000:0000:19AA:2837

Aby skrócić otrzymany adres, pomija się zera występujące na początku danego członu:

34:0:A132:827C:0:0:19AA:2837

Chcąc jeszcze bardziej uprościć adres IPv6, sąsiadujące ze sobą bloki złożone z samych zer zastępuje się dwoma dwukropkami:

34:0:A132:827C::19AA:2837

Wybieg ten można zastosować tylko raz. Analizator adresu (parser) rozdziela adres w miejscu występowania podwójnego dwukropka i wypełnia go zerami do momentu wyczerpania 128 bitów. Opisane zabiegi czynią adres IPv6 bardziej czytelnym i mniej podatnym na błędy podczas zapisu przez użytkownika. Schemat adresowania IPv6 określono w RFC 2373.

Ze względu na długość adresu IPv6 szczególnie ważną funkcję spełniają serwery DNS. Jeżeli nadal chcemy zapisywać adresy URL, podając numer IP, należy umieszczać je w nawiasie kwadratowym. W przeciwnym razie parser URL nie będzie w stanie rozróżnić adresu IP do numeru portu. Przykład: http://[34:0: A132:827C::19AA:2837]:80/index.html

REPREZENTACJA ADRESU IPV6

Prefiks adresu tworzy określona liczba bitów wyznaczona od lewej strony adresu IPv6, które identyfikują daną sieć. Jego tekstowa reprezentacja jest analogiczna do notacji CIDR (*Classless InterDomain Routing*), znanej z IPv4, tj. adres IPv6/długość prefiksu:

0034:0000:A132:827C:0000:0000:19AA:2837/64

gdzie adres węzła to:

0034:0000:A132:827C:0000:0000:19AA:2837

adres podsieci to:

0034:0000:A132:827C:0000:0000: 0000:0000/64

lub po skróceniu:

34:0:A132:827C::/64

ZARZĄDZANIE ADRESACJĄ IPV6

Adresy zarezerwowane:

adres nieokreślony 0:0:0:0:0:0:0:0

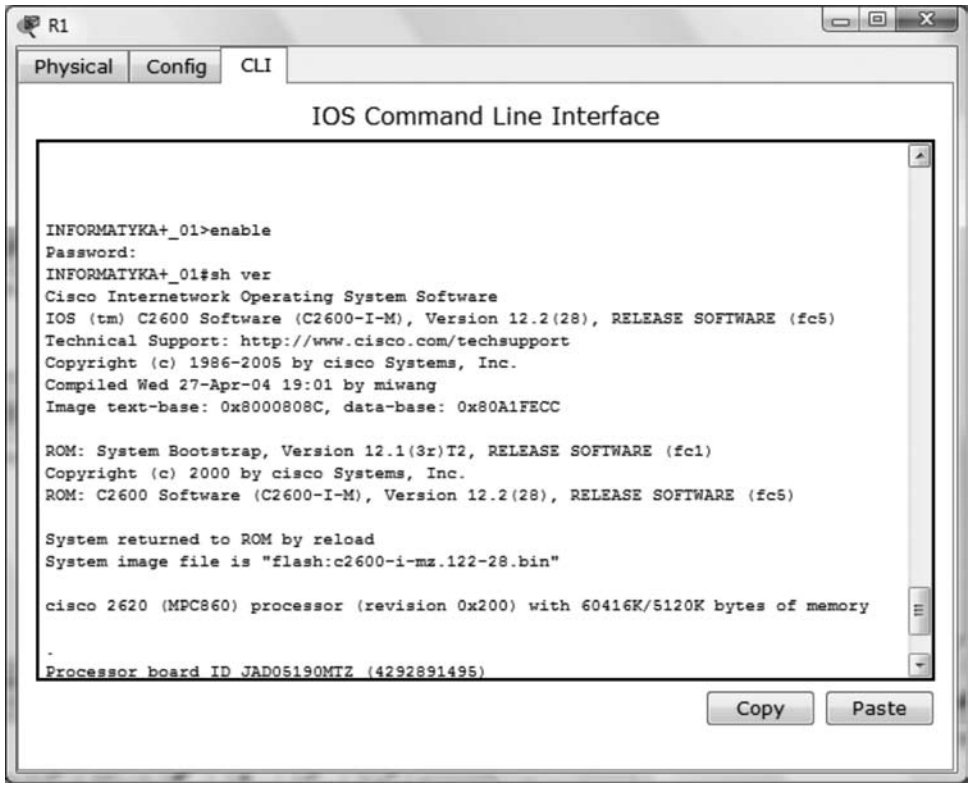
informuje o braku adresu. Jest wykorzystywany jako adres źródłowy podczas wysyłania pakietu z hosta, który jeszcze nie zdążył uzyskać swojego adresu;

adres Loopback 0:0:0:0:0:0:0:1

to adres typu pętla zwrotna, gdzie węzeł wysyła pakiet sam do siebie. Adresy tego typu nie powinny nigdy opuszczać danego węzła, a tym bardziej być przekazywane przez routery.

2. DZIAŁANIA NA SYSTEMACH OPERACYJNYCH AKTYWNYCH URZĄDZEŃ SIECIOWYCH. PODSTAWOWE FUNKCJE I MOŻLIWOŚCI

Okno terminala służy do konfiguracji podstawowych parametrów aktywnych urządzeń sieciowych (routerów) połączonych interfejsem konsoli do portu szeregowego komputera.



Rysunek 50.
Okno terminala

Ćwiczenie 7. Sprawdzenie podstawowych parametrów oraz ukompletowania (użycie polecenia **show version**).

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC
ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
System returned to ROM by reload
System image file is „flash:c2600-i-mz.122-28.bin” (plik z obrazem systemu operacyjnego)
cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
4 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Ćwiczenie 8. Sprawdzenie stanu interfejsów (użycie polecenia **show ip interface brief**).

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
Serial0/0              unassigned      YES manual administratively down down
Serial0/1              unassigned      YES manual administratively down down
Serial0/2              unassigned      YES manual administratively down down
Serial0/3              unassigned      YES manual administratively down down
```

Ćwiczenie 9. Sprawdzenie bieżącej konfiguracji (użycie polecenia **show running-config**).

```
Router#show running-config
Building configuration...
Current configuration : 424 bytes!
version 12.2
no service password-encryption
!
hostname Router
!
ip ssh version 1!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
 shutdown
!
interface Serial0/3
 no ip address
 shutdown
!
ip classless!
!
line con 0
line vty 0 4
 login
!
End
```

Ćwiczenie 10. Sprawdzenie aktywnych procesów (użycie polecenia **show processes**).

```
Router# show  processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID QTy       PC Runtime (ms)     Invoked  uSecs     Stacks TTY Process
   1 Csp 602F3AF0           0        1627       0 2600/3000    0 Load Meter
   2 Lwe 60C5BE00           4         136      29 5572/6000    0 CEF Scanner
   3 Lst 602D90F8        1676         837    2002 5740/6000    0 Check heaps
   4 Cwe 602D08F8           0           1       0 5568/6000    0 Chunk Manager
   5 Cwe 602DF0E8           0           1       0 5592/6000    0 Pool Manager
   6 Mst 60251E38           0           2       0 5560/6000    0 Timers
   7 Mwe 600D4940           0           2       0 5568/6000    0 Serial Backgrou
   8 Mwe 6034B718           0           1       0 2584/3000    0 OIR Handler
   9 Mwe 603FA3C8           0           1       0 5612/6000    0 IPC Zone Manage
  10 Mwe 603FA1A0           0        8124       0 5488/6000    0 IPC Periodic Ti
  11 Mwe 603FA220           0           9       0 4884/6000    0 IPC Seat Manage
  12 Lwe 60406818         124        2003      61 5300/6000    0 ARP Input
  13 Mwe 60581638           0           1       0 5760/6000    0 HC Counter Time
  14 Mwe 605E3D00           0           2       0 5564/6000    0 DDR Timers
  15 Msp 80164A38           0       79543       0 5608/6000    0 GraphIt
  16 Mwe 802DB0FC           0           2       011576/12000   0 Dialer event
  17 Cwe 801E74BC           0           1       0 5808/6000    0 Critical Bkgnd
  18 Mwe 80194D20           4        9549       010428/12000   0 Net Background
  19 Lwe 8011E9CC           0          20       011096/12000   0 Logger
  20 Mwe 80140160           8       79539       0 5108/6000    0 TTY Background
  21 Msp 80194114           0       95409       0 8680/9000    0 Per-Second Job
  22 Mwe 8047E960           0           2       0 5544/6000    0 dot1x
  23 Mwe 80222C8C           4           2    2000 5360/6000    0 DHCPD Receive
  24 Mwe 800844A0           0           1       0 5796/6000    0 HTTP Timer
  25 Mwe 80099378           0           1       0 5612/6000    0 RARP Input
  26 Mst 8022F178           0           1       011796/12000   0 TCP Timer
  27 Lwe 802344C8           0           1       011804/12000   0 TCP Protocols
  28 Hwe 802870E8           0           1       0 5784/6000    0 Socket Timers
  29 Mwe 80426048          64           3   21333 4488/6000    0 L2MM
  30 Mwe 80420010           4           1    4000 5592/6000    0 MRD
  31 Mwe 8041E570           0           1       0 5584/6000    0 IGMPSN
  32 Hwe 80429B40           0           1       0 2604/3000    0 IGMP Snooping P
  33 Mwe 804F43B0           0           5       0 5472/6000    0 Cluster L2
  34 Mwe 804F18D0           0          17       0 5520/6000    0 Cluster RARP
  35 Mwe 804EA650           0          23       0 5440/6000    0 Cluster Base
  36 Lwe 802A1158           4           1    4000 5592/6000    0 Router Autoconf
  37 Mwe 80022058           0           1       0 5624/6000    0 Syslog Traps
  38 Mwe 8031CE88           0           1       0 5788/6000    0 AggMgr Process
  39 Mwe 8035EF88           0         407       0 5592/6000    0 PM Callback
  40 Mwe 80437B58           0           3       0 5556/6000    0 VTP Trap Proces
  41 Mwe 80027D40           0           2       0 5676/6000    0 DHCPD Timer
```

Ćwiczenie 11. Konfiguracja podstawowych parametrów.

```
Router#configure terminal #przechodzimy w tryb konfiguracji z terminala#
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname INFORMATYKA+ _ 01 #wprowadzamy nazwę routera#
INFORMATYKA+ _ 01(config)#enable secret 12345678 #wprowadzamy hasło na tryb uprzywilejowany#
```

```
INFORMATYKA+ _ 01(config)#line vty 0 4
INFORMATYKA+ _ 01(config-line)#password 987654321  #wprowadzamy hasło na linie wirtualnego
terminala (telnet)#
INFORMATYKA+ _ 01(config-line)#exit
INFORMATYKA+ _ 01(config)#line console 0
INFORMATYKA+ _ 01(config-line)#password qwerty #wprowadzamy hasło na port konsoli#
INFORMATYKA+ _ 01(config-line)#^Z
%SYS-5-CONFIG _ I: Configured from console by console
INFORMATYKA+ _ 01#
INFORMATYKA+ _ 01#copy running-config startup-config #zapisanie konfiguracji#
Destination filename [startup-config]?
Building configuration...
[OK]
INFORMATYKA+ _ 01#
```

Ćwiczenie 12. Konfiguracja interfejsów LAN i WAN.

```
INFORMATYKA+ _ 01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
INFORMATYKA+ _ 01(config)#interface fastethernet 0/0 #wybór interfejsu#
INFORMATYKA+ _ 01(config-if)#ip address 192.168.1.1 255.255.255.0 #ustawienie adresu IP#
INFORMATYKA+ _ 01(config-if)#no shutdown #włączenie interfejsu#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
INFORMATYKA+ _ 01(config-if)#exit
INFORMATYKA+ _ 01(config)#interface serial 0/0
INFORMATYKA+ _ 01(config-if)#ip address 10.10.10.1 255.255.255.252
INFORMATYKA+ _ 01(config-if)#clock rate 128000 #ustawienie prędkości łącza WAN#
INFORMATYKA+ _ 01(config-if)#encapsulation ppp #ustawienie rodzaju protokołu WAN#
INFORMATYKA+ _ 01(config-if)#no shutdown
Serial0/0 LCP: State is Open
Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
INFORMATYKA+ _ 01(config-if)#
```

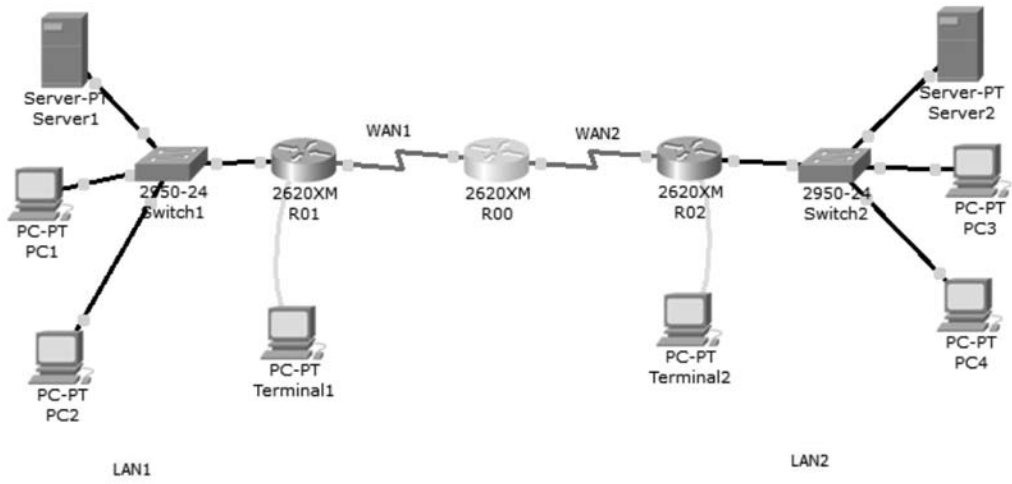
Ćwiczenie 13. Sprawdzenie działania interfejsu.

```
INFORMATYKA+ _ 01#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.9781.1a57 (bia 0001.9781.1a57)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of „show interface” counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 input packets with dribble condition detected
   0 packets output, 0 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

3. BUDOWANIE STATYCZNEJ I DYNAMICZNEJ TABLICY ROUTINGU

Ćwiczenie 14. Interaktywny model zostanie stworzony indywidualnie przez uczestników z wykorzystaniem oprogramowania Packet Tracer (firmy Cisco Systems). Celem jest opanowanie umiejętności konfigurowania tras statycznych pomiędzy routerami w celu umożliwienia transferu danych między nimi bez użycia dynamicznych protokołów routingu.



Rysunek 51.
Schemat topologii sieci dla routingu statycznego

SCHEMAT ADRESACJI:

LAN1: 192.168.1.0/24
LAN2: 172.16.0.0/16
WAN1: 10.10.10.0/30
WAN2: 10.10.10.4/30

KONFIGURACJA URZĄDZEŃ

Przejdź do trybu konfiguracji globalnej routera i skonfiguruj nazwę hosta, tak jak przedstawiono na rysunku. Następnie skonfiguruj konsolę, terminal wirtualny i hasła dostępu do trybu uprzywilejowanego. Wyświetl konfigurację bieżącą routera oraz sprawdź poprawność wprowadzonych parametrów:

Router#show running-config

Skonfiguruj interfejsy oraz sprawdź poprawność konfiguracji:

Router#show ip interface brief

KONFIGURACJA ROUTINGU STATYCZNEGO

```
INFORMATYKA+ _ 01(config)#ip route 172.16.0.0 255.255.0.0 10.10.10.2
INFORMATYKA+ _ 01(config)#ip route 10.10.10.4 255.255.255.252 10.10.10.2

INFORMATYKA+ _ 00(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
INFORMATYKA+ _ 00(config)#ip route 172.16.0.0 255.255.0.0 10.10.10.6

INFORMATYKA+ _ 02(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.5
INFORMATYKA+ _ 02(config)#ip route 10.10.10.0 255.255.255.252 10.10.10.5
```

ANALIZA TABLIC ROUTINGU

Tablicę routingu wyświetlamy poleceniem **show ip route** (poniższe przykłady prezentują tablice routingu dla trzech routerów w zadanej topologii:

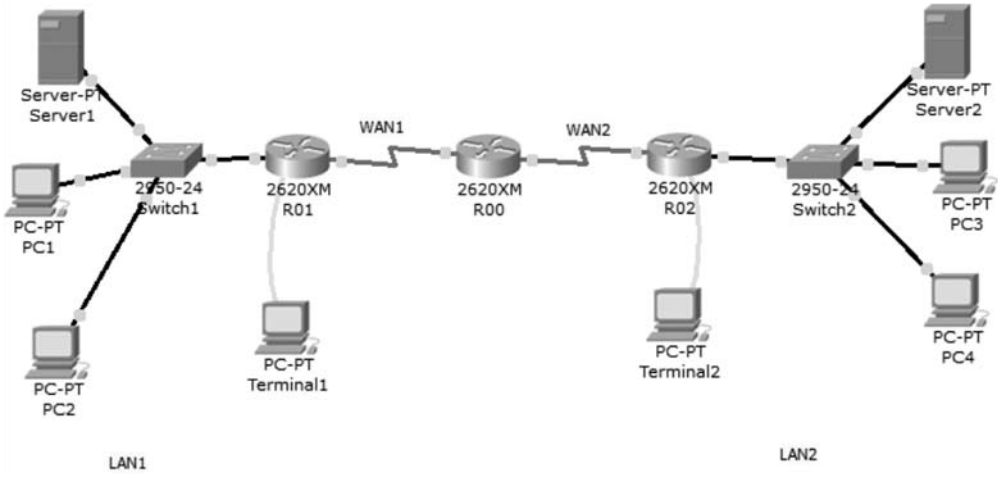
```
INFORMATYKA+ _ 00#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 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

     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Serial0/0
C       10.10.10.4 is directly connected, Serial0/1
S    172.16.0.0/16 [1/0] via 10.10.10.6
S    192.168.1.0/24 [1/0] via 10.10.10.1

INFORMATYKA+ _ 01#sh 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

     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Serial0/0
S       10.10.10.4 [1/0] via 10.10.10.2
S    172.16.0.0/16 [1/0] via 10.10.10.2
C    192.168.1.0/24 is directly connected, FastEthernet0/0

INFORMATYKA+ _ 02#sh 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

     10.0.0.0/30 is subnetted, 2 subnets
S       10.10.10.0 [1/0] via 10.10.10.5
C       10.10.10.4 is directly connected, Serial0/1
C    172.16.0.0/16 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 10.10.10.5
```

TESTY DZIAŁANIA SIECI

```
PC3>ping 192.168.1.11
Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=188ms TTL=125
Reply from 192.168.1.11: bytes=32 time=171ms TTL=125
Reply from 192.168.1.11: bytes=32 time=143ms TTL=125
Reply from 192.168.1.11: bytes=32 time=171ms TTL=125

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 143ms, Maximum = 188ms, Average = 168ms

PC3>tracert 192.168.1.101
Tracing route to 192.168.1.101 over a maximum of 30 hops:

  1    63 ms     62 ms     40 ms     172.16.0.1
  2    94 ms     93 ms     93 ms     10.10.10.5
  3    141 ms    94 ms     111 ms    10.10.10.1
  4    141 ms    173 ms    156 ms    192.168.1.101

Trace complete.
PC>
```

Ćwiczenie 15. Konfiguracja i weryfikacja działania protokołu RIP.



Rysunek 52.
Schemat topologii sieci dla konfiguracji protokołu RIP

SCHEMAT ADRESACJI:

LAN1: 192.168.1.0/24
LAN2: 172.16.0.0/16
WAN1: 10.10.10.0/30
WAN2: 10.10.10.4/30

KONFIGURACJA PROTOKOŁU

```
INFORMATYKA+ _ 01(config)#router rip
INFORMATYKA+ _ 01(config-router)#version 2
INFORMATYKA+ _ 01(config-router)#network 192.168.1.0
INFORMATYKA+ _ 01(config-router)#network 10.10.10.0

INFORMATYKA+ _ 00(config)#router rip
INFORMATYKA+ _ 00(config-router)#version 2
INFORMATYKA+ _ 00(config-router)#network 10.10.10.0

INFORMATYKA+ _ 02(config)#router rip
INFORMATYKA+ _ 02(config-router)#version 2
INFORMATYKA+ _ 02(config-router)#network 172.16.0.0
INFORMATYKA+ _ 02(config-router)#network 10.10.10.0
```

WERYFIKACJA TABLICY ROUTINGU

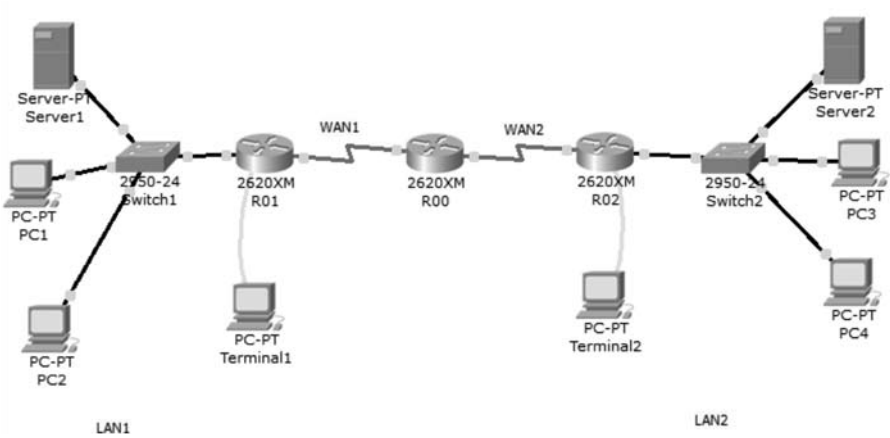
```
INFORMATYKA+ _ 01#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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

     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Serial0/0
R       10.10.10.4 [120/1] via 10.10.10.2, 00:00:13, Serial0/0
R    172.16.0.0/16 [120/2] via 10.10.10.2, 00:00:13, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

WERYFIKACJA DZIAŁANIA PROTOKOŁU ROUTINGU

```
INFORMATYKA+ _ 01#show ip protocols
Routing Protocol is „rip”
Sending updates every 30 seconds, next due in 18 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       1     2 1
  Serial0/0             1     2 1
```

```
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
     10.0.0.0
     192.168.1.0
Passive Interface(s):
Routing Information Sources:
     Gateway         Distance      Last Update
     10.10.10.2           120      00:00:12
Distance: (default is 120)
```

Ćwiczenie 16. Konfiguracja i weryfikacja działania protokołu EIGRP.



Rysunek 53.
Schemat topologii sieci dla konfiguracji protokołu EIGRP

SCHEMAT ADRESACJI:

LAN1: 192.168.1.0/24
LAN2: 172.16.0.0/16
WAN1: 10.10.10.0/30
WAN2: 10.10.10.4/30

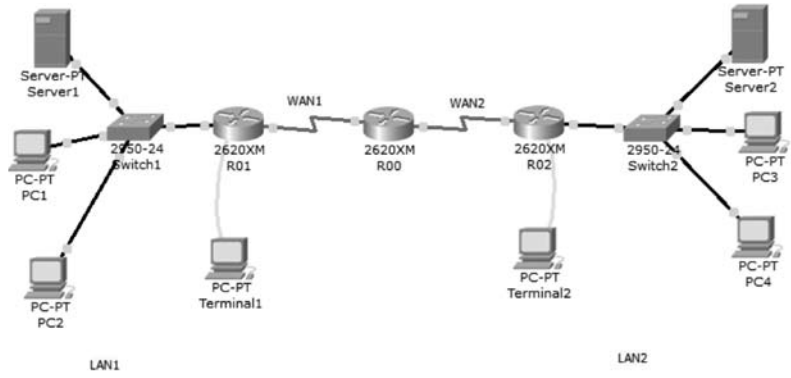
KONFIGURACJA PROTOKOŁU

```
INFORMATYKA+ _ 01(config)#router EIGRP 100
INFORMATYKA+ _ 01(config-router)#no auto-summary
INFORMATYKA+ _ 01(config-router)#network 192.168.1.0 0.0.0.255
INFORMATYKA+ _ 01(config-router)#network 10.10.10.0 0.0.0.3

INFORMATYKA+ _ 02(config)#router EIGRP 100
INFORMATYKA+ _ 02(config-router)#no auto-summary
INFORMATYKA+ _ 02(config-router)#network 172.16.1.0 0.0.255.255
INFORMATYKA+ _ 02(config-router)#network 10.10.10.4 0.0.0.3

INFORMATYKA+ _ 00(config)#router EIGRP 100
INFORMATYKA+ _ 00(config-router)#no auto-summary
INFORMATYKA+ _ 00(config-router)#network 10.10.10.0 0.0.0.3
INFORMATYKA+ _ 02(config-router)#network 10.10.10.4 0.0.0.3
```

WERYFIKACJA DZIAŁANIA PROTOKOŁU

```
INFORMATYKA+ _ 01#show ip protocols

Routing Protocol is „eigrp  100 „
  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 100
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
     10.10.10.0/30
     192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.2      90            16195
  Distance: internal 90 external 170

INFORMATYKA+ _ 01#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

     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Serial0/0
D       10.10.10.4 [90/2681856] via 10.10.10.2, 00:17:45, Serial0/0
D    172.16.0.0/16 [90/2684416] via 10.10.10.2, 00:17:45, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Ćwiczenie 17. Konfiguracja i weryfikacja działania protokołu OSPF.



Rysunek 54.
Schemat topologii sieci dla konfiguracji protokołu OSPF

SCHEMAT ADRESACJI:

LAN1: 192.168.1.0/24
LAN2: 172.16.0.0/16
WAN1: 10.10.10.0/30
WAN2: 10.10.10.4/30

KONFIGURACJA PROTOKOŁU

```
INFORMATYKA+ _ 01(config)#router ospf 200
INFORMATYKA+ _ 01(config-router)#network 10.10.10.0 0.0.0.3 area 0
INFORMATYKA+ _ 01(config-router)#network 192.168.1.0 0.0.0.255 area 0

INFORMATYKA+ _ 02(config)#router ospf 200
INFORMATYKA+ _ 02(config-router)#network 172.16.0.0 0.0.255.255 area 0
INFORMATYKA+ _ 02(config-router)#network 10.10.10.4 0.0.0.3 area 0

INFORMATYKA+ _ 00(config)#router ospf 200
INFORMATYKA+ _ 00(config-router)#network 10.10.10.0 0.0.0.3 area 0
INFORMATYKA+ _ 00(config-router)#network 10.10.10.4 0.0.0.3 area 0
```

WERYFIKACJA DZIAŁANIA PROTOKOŁU

```
INFORMATYKA+ _ 01#show ip protocols

Routing Protocol is „ospf 200”
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    10.10.10.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.2           110      00:00:08
  Distance: (default is 110)

INFORMATYKA+ _ 01#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

     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Serial0/0
O       10.10.10.4 [110/128] via 10.10.10.2, 00:00:15, Serial0/0
O    172.16.0.0/16 [110/129] via 10.10.10.2, 00:00:15, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

W projekcie **Informatyka +**, poza wykładami i warsztatami, przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
- nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
- konkursy dla uczniów, trzy w ciągu roku
- udział uczniów w pracach kół naukowych
- udział uczniów w konferencjach naukowych
- obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu **www.informatykaplus.edu.pl**